Cisco Collaboration システム 12.*x* ソリューション リファレンス ネットワーク デザイン（SRND）

最終更新日：2018 年 3 月 1 日

Cisco Systems, Inc.
www.cisco.com

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

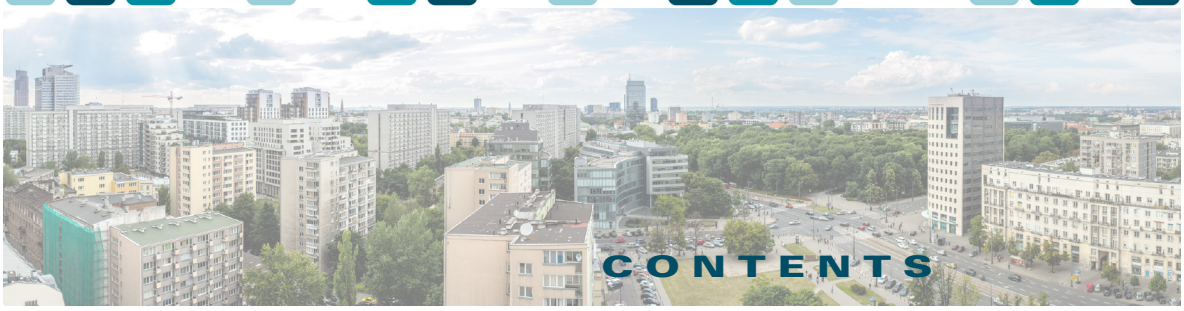
初版：2017 年 2 月 7 日

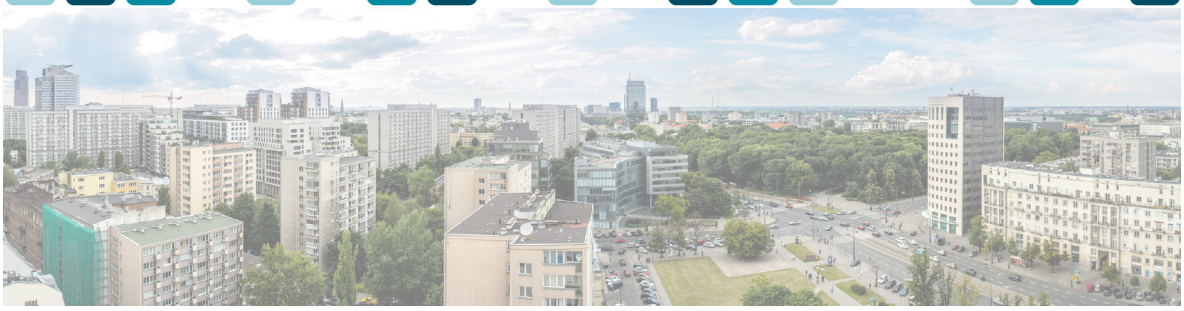
【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

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

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

Cisco Collaboration システム 12.x SRND





序文

改訂日：2018 年 3 月 1 日

このマニュアルでは、Cisco Unified Communications Manager 12.*x*、Cisco TelePresence System、および Cisco Collaboration システム リリース 12.*x* の他のコンポーネントを含む Cisco Collaboration ソリューションを配置する際の設計上の考慮事項およびガイドラインについて説明します。

このマニュアルは、シスコが過去 10 年以上にわたって作成してきたソリューション リファレンス ネットワーク デザイン（SRND）ガイドの長い系統から発展したものです。シスコの音声、ビデオ、コラボレーションのテクノロジーが時間とともに発展し、成熟するにつれて、こうしたテクノロジーの進展を文書に反映するように SRND の改訂と更新が行われています。SRND のこの最新バージョンには、Cisco Spark、TelePresence、WebEx、さまざまなエンドユーザ デバイスに対するサポートなどのシスコのコラボレーション テクノロジーのすべての範囲が含まれます。シスコはコラボレーション テクノロジーの開発と機能強化を継続的に行っており、それに伴って、コラボレーション ソリューションを作成するための最新のガイドライン、推奨事項、およびベスト プラクティスを提供するため、この SRND は引き続き発展し、更新されます。

このマニュアルは、次の Web サイトから入手できる他のマニュアルとあわせてお読みください。

- ソリューション リファレンス ネットワーク デザイン（SRND）に関するその他のマニュアル：
  https://www.cisco.com/go/srnd
- Cisco Collaboration 推奨アーキテクチャ（PA）の詳細：
  https://www.cisco.com/go/pa
- Cisco Collaboration ソリューションの詳細：
  https://www.cisco.com/c/en/us/solutions/collaboration/index.html
- Cisco Collaboration システム リリース（CSR）の詳細：
  https://www.cisco.com/go/unified-techinfo
- Cisco Unified Communications の詳細：
  https://www.cisco.com/c/en/us/products/unified-communications/index.html
  https://www.cisco.com/c/en/us/products/unified-communications/product-listing.html
  https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html
- Cisco Video Collaboration ソリューションの詳細：
  https://www.cisco.com/c/en/us/solutions/collaboration/video-collaboration/index.html

- その他のシスコ設計ガイド:
  https://www.cisco.com/go/designzone
- すべてのシスコ製品およびマニュアル:
  https://www.cisco.com

このリリースの新規または変更情報

(注) 特に指定のない限り、このマニュアルの情報は、すべての Cisco Collaboration システム 12.*x* リリースに適用されます。

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

このマニュアルの内容の多くは、以前のリリースの *Cisco Collaboration SRND* に似ていますが、最新の Cisco Collaboration システム リリースのアーキテクチャをより正確に反映するために、大幅に再編成および更新されています。テクノロジーとシステム アーキテクチャをよく理解するために、はじめに(1-1 ページ)から始めてマニュアル全体を確認することを推奨します。

変更履歴

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

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

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

次の表は、このマニュアルの改訂履歴を示したものです。

改訂日	説明
2018 年 3 月 1 日	Cisco Collaboration システム リリース(CSR)12.*x* を対象にしたこのマニュアルの初版です。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool(BST)の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。

シスコの新規および改訂版のテクニカル コンテンツを直接受信するには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

シスコ製品のセキュリティの概要

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

米国の輸出規制の詳細については、次の URL で参照できます。

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

表記法

このマニュアルでは、次の表記法を使用しています。

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

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

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

注意

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

ワンポイント アドバイス

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

警告

安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

警告

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

はじめに

改訂日：2018 年 3 月 1 日

コラボレーションは、共通の目標を達成するための共同作業を意味します。最近まで、コラボレーションする最適な方法は同じ時間に同じ場所に居て、お互いに直接対話することでした。ビジネス リソースやアウトソーシングされたサービスが分散され、オフィス設備や出張のコストが増加している現在のグローバル化された経済では、物理的に同じ場所に人を集めることはコラボレーションするための最も効率的で効果的な方法とは言えなくなりました。Cisco Collaboration Solutions を使用すると、時間と経費を大幅に節約しながら、いつでもどこでもお互いにコラボレーションすることができます。

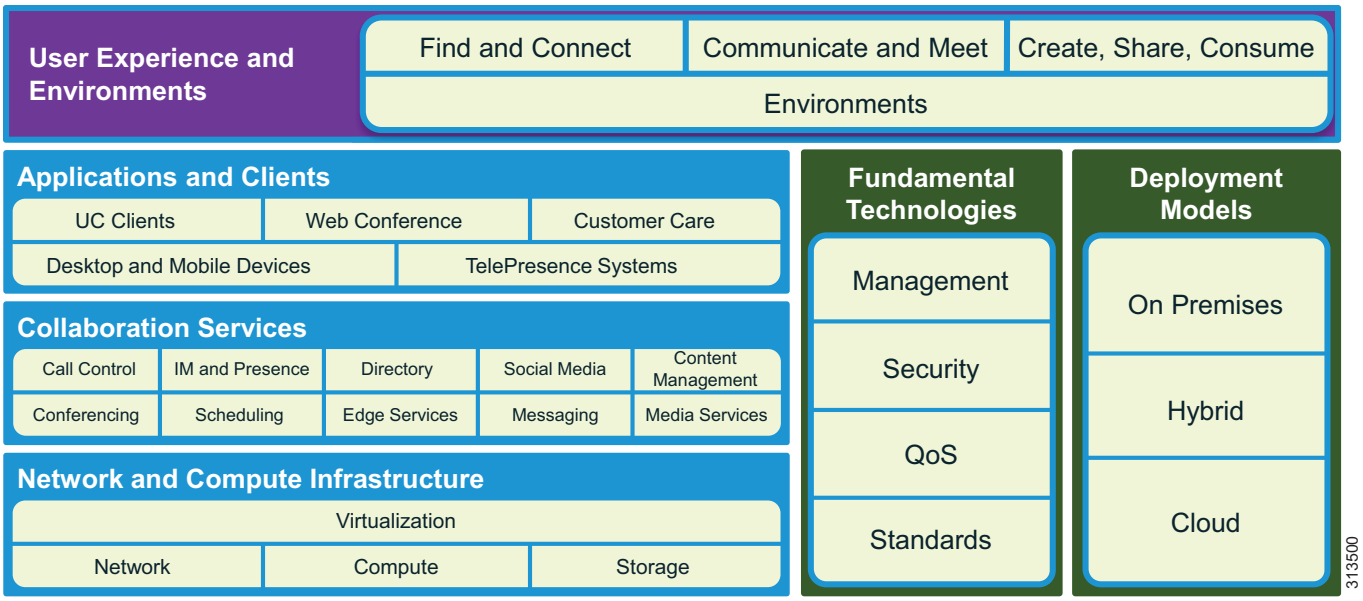
Cisco Collaboration Solutions は、モバイル通信やソーシャル メディアの最新技術など、音声、ビデオ、およびデータ通信を完全にサポートしています。Cisco Collaboration Solutions には、社内またはクラウドに配置できるアプリケーションとサービスの広範囲にわたるセットも用意されています。

Cisco End-to-End Collaboration ソリューション

Cisco Collaboration Technology は、あらゆる規模と種類の企業に対する完全なエンドツーエンドのコラボレーション ソリューションを作成するための多数の製品で構成されています。Cisco Collaboration Solutions は、概念的な形式で図 1-1 に示されているように、次の主な要素で構成されています。

- コラボレーション インフラストラクチャ（1-2 ページ）
- コラボレーション アプリケーションおよびサービス（1-3 ページ）
- コラボレーションのユーザ エクスペリエンス（1-4 ページ）

図 1-1　Cisco Collaboration アーキテクチャ（概念図）



コラボレーション インフラストラクチャ

シスコはルーティングおよびスイッチング テクノロジーのリーダー企業として、長年評価されてきました。このテクノロジーによって、Cisco Collaboration Solutions のネットワーク インフラストラクチャの中核が形成されます。Cisco スイッチおよびルータで使用できる Quality of Service（QoS）メカニズムにより、ネットワーク全体で、最高品質の音声、ビデオ、およびデータ通信が提供されます。さらに、Cisco ゲートウェイには、企業の内部ネットワークを、外部のワイド エリア ネットワーク（WAN）に加え、公衆電話交換網（PSTN）や PBX などのレガシー システムに接続するための多数の方法が備わっています。また、Cisco Hosted Collaboration Solution（HCS）を使用して、Cisco パートナーはお客様にクラウド ベースでホストされたコラボレーション サービスを提供できます。これらのサービスは安全で、柔軟性があり、低コストで、拡張可能であり、最新テクノロジーが常に取り入れられています。

Cisco Collaboration システム リリース 12.*x* は、VMware vSphere ESXi ハイパーバイザとの仮想化を使用して展開されます。Cisco Collaboration アプリケーションのノードは、サーバ上で 1 つまたは複数のアプリケーション ノードとして動作可能な仮想マシンとして展開されます。これらの仮想アプリケーションは中小企業にコラボレーション サービスを提供します。また、シスコなどの大規模なグローバル企業に対処できるように拡張できます。

通常、コラボレーション セッションは保護される必要があります。そのため、ネットワークの中核部分からエンド ユーザのデバイスまで、コラボレーション パスの各レベルを保護するために、シスコは多数のセキュリティ メカニズムを開発しました。

コラボレーション ソリューションが実行されると、それを監視および管理する必要があります。シスコは、コラボレーション ソリューションをプロビジョニング、運用、監視、および保守するシステム管理者を支援するために、さまざまなツール、アプリケーション、および製品を開発してきました。これらのツールを使用して、システム管理者はネットワーク コンポーネントの動作ステータスを監視し、システムに関する統計情報を収集および分析して、カスタム レポートを生成できます。

コラボレーション アプリケーションおよびサービス

Cisco Collaboration Solutions には、次のような多数の高度なアプリケーションおよびサービスが含まれています。

- **インスタンス メッセージング（IM）およびプレゼンス**：Cisco IM and Presence Service では、コラボレーションするパートナーと効率的にコミュニケーションを図れるため、Cisco Jabber、Cisco Unified Communications Manager アプリケーション、およびサードパーティ アプリケーションを使うユーザの生産性を高めることができます。
- **コラボレーティブ リッチ メディア会議**：Cisco WebEx には、音声、高解像度（HD）ビデオ、およびリアルタイムのコンテンツ共有がプラットフォームに組み込まれています。このプラットフォームを使用して、会議を簡単にセットアップおよび管理したり、会議で参加者と対話したり、IP フォン、タブレット デバイス、またはデスクトップ コンピュータなど、あらゆる種類のデバイスから会議に出席したりすることができます。オンプレミス型会議の場合、Cisco TelePresence Server を Cisco TelePresence Conductor と組み合わせて使用することで、TelePresence ビデオ エンドポイント、ビデオ対応デスク フォン、ソフトウェアベースのモバイルおよびデスクトップ クライアントへのコンテンツ共有とともに、アドホックでスケジューリングされた無期限の音声およびビデオの会議が可能になります。
- **Cisco Spark**：Cisco Spark デスクトップおよびモバイル クライアントは、1 対 1 およびチームのコラボレーションを容易にするクラウドベースの常設仮想チーム ルームを可能にします。Cisco Spark デスクトップ クライアントは、Windows および Mac のコンピュータ上で動作します。Cisco Spark モバイル クライアントは、Android および Apple iOS のデバイス上で動作します。Cisco Spark を使用すると、ユーザは Cisco Collaboration Cloud からコラボレーション サービスにアクセスできます。このサービスには、セキュアで暗号化されたパーシステント メッセージング、IP を介した音声/ビデオ通話、およびファイル共有などがあり、すべて仮想の 1 対 1 またはグループのコラボレーション ルーム内で利用できます。
- **テレプレゼンス**：Cisco TelePresence テクノロジーにより、ユーザは出張にまつわる経費や遅延を生じることなく、リアルタイムで集まることができます。Cisco TelePresence ポートフォリオには、個々のデスクトップ ユニットから会議室に最適な大型のマルチスクリーンによるイマーシブ ビデオ システムまでさまざまは高解像度（HD）ビデオ エンドポイントが含まれています。また、Cisco TelePresence 製品は、ビデオ機能を持つ Cisco WebEx や Cisco IP Phone など、他のシスコ コラボレーション製品と相互運用されるように設計されています。
- **音声メッセージ**：シスコ製品は大規模および小規模なコラボレーション システム用にいくつかの音声メッセージ オプションを提供し、さらに、標準プロトコルを使用したサードパーティ製ボイスメール システムと統合する機能を提供します。
- **カスタマー コンタクト**：Cisco Unified Contact Center 製品は、カスタマー コンタクト センターにインテリジェント コンタクト ルーティング、通話処理、およびマルチチャネル コンタクト管理を提供します。Cisco Unified Customer Voice Portal はスタンドアロンの対話式音声認識（IVR）システムとしてインストールしたり、コンタクト センターと統合して、パーソナライズされたセルフサービスをお客様に提供できます。また、Cisco SocialMiner はソーシャル メディアを介してお客様と関与するための強力なツールです。
- **コールの録音およびモニタリング**：Cisco Collaboration Solutions は、さまざまなテクノロジーを採用して、音声やビデオの会議だけでなく、コンタクト センター担当者と顧客との会話を録音およびモニタすることができます。コールの録音およびモニタリングの技術には、Cisco Unified Communications Manager、Cisco Agent Desktop、Cisco TelePresence Content Server、および Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の技術に基づくソリューションが含まれています。

コラボレーションのユーザ エクスペリエンス

コラボレーションとは、つまりユーザ エクスペリエンスです。ユーザがコラボレーション テクノロジーに関して良いエクスペリエンスを体験すると、ユーザはそのテクノロジーをより頻繁に使用し、それを使用してより良い成果を達成するようになります。コラボレーション テクノロジーを採用した企業は、これによってより大きな投資回収率（ROI）を得ることができます。そのため、シスコはコラボレーション テクノロジーを簡単、便利、および有益に使用できるようにすること目標に、特に次の拡張機能に重点を置いています。

- **さまざまなコラボレーション エンドポイントに対応**：シスコは基本的な音声のみの電話機から、ビデオやインターネット機能を持つ電話機、および高解像度のテレプレゼンスおよびイマーシブ ビデオ デバイスまで、完全なエンドポイント デバイスの製品ラインを提供しています。シスコのコラボレーション テクノロジーは、統合されたサードパーティ エンドポイント デバイスをコラボレーション ソリューションに統合する機能も提供します。
- **Cisco BYOD Smart Solution**：Cisco Bring Your Own Device（BYOD）Smart Solution により、ユーザはスマートフォン、タブレット、または PC など、独自のデバイスを使って仕事ができます。働き方のエクスペリエンスを拡大することに加え、Cisco BYOD Smart Solution では、組織全体に有線および Wi-Fi アクセス用の単一ポリシーを提供することで、より強力なネットワーク セキュリティが確保され、ネットワーク管理が簡素化されます。
- **モバイル コラボレーション**：シスコ モバイル コラボレーション ソリューションでは、モバイル ワーカーは持続的に到達可能性を得ることができ、さまざまな場所で、移動中や作業中の生産性を向上させることができます。シスコのモビリティ ソリューションには、次のような機能が含まれています。Extension Mobility を使用して、ユーザはシステム内のすべての電話機にログオンすることができ、その電話機でユーザのデフォルト電話機設定が想定されるようにできます。Cisco Jabber および Cisco Spark は、音声、ビデオ、およびインスタント メッセージ用のコア コラボレーション機能を、スマートフォンやタブレットなどのサードパーティ モバイル デバイスのユーザに提供します。Single Number Reach は、各ユーザのデスクにある電話機やモバイル電話の呼出音を同時に鳴らす単一の企業電話番号を提供します。
- **アプリケーションとサービス**：前述のとおり、シスコはエンド ユーザのコラボレーション エクスペリエンスを充実させるために、多数の高度なアプリケーションとサービスを開発してきました。（コラボレーション アプリケーションおよびサービス（1-3 ページ）を参照）。シスコのコラボレーション テクノロジーは業界標準に可能な限り準拠させているため、ユーザはサードパーティ製アプリケーションやサービスを独自のコラボレーション ソリューションに簡単に統合できます。また、シスコのコラボレーション製品で使用できるアプリケーション プログラミング インターフェイスを使用して、独自のカスタム アプリケーションを作成することができます。

このドキュメントについて

このマニュアルは、Cisco Collaboration ソリューション向けのソリューション リファレンス ネットワーク デザイン（SRND）ガイドです。ビジネス ニーズを満たすコラボレーション ソリューションを設計するためのシステム レベルの要件、推奨事項、ガイドライン、およびベスト プラクティスが示されています。

このマニュアルは、過去 10 年以上にわたりシスコが作成してきた SRND から発展したものです。シスコの音声、ビデオ、およびデータ コミュニケーションのテクノロジーが時間とともに発展し、成熟するにつれて、こうしたテクノロジーの進展を文書に反映するように SRND の改訂と更新が行われています。SRND の旧バージョンでは、シスコの Voice over IP（VoIP）テクノロジーのみに重点を置いていました。以降のバージョンでは、Cisco Unified Communications が文書化され、モバイル ボイス通信、会議、インスタント メッセージ（IM）、プレゼンス、ビデオ テレフォニーの新技術情報が追加されました。SRND のこの最新バージョンには、Cisco Spark、TelePresence およびすべてのタイプのエンド ユーザ デバイス（Bring Your Own Device、すなわち BYOD）に対するサポートなど、シスコ コラボレーション テクノロジーのすべての範囲が含まれています。シスコはコラボレーション テクノロジーの開発と機能強化を継続的に行っており、それに伴って、コラボレーション ソリューションを作成するための最新のガイドライン、推奨事項、およびベスト プラクティスを提供するため、この SRND は引き続き発展し、更新されます。

このマニュアルの構成

このマニュアルは、次の 4 つの主要部分で構成されています。

- **コラボレーション システムのコンポーネントとアーキテクチャ**

  マニュアルのこの部分の各章では、シスコ コラボレーション テクノロジーの主な構成要素が示されており、これらの構成要素がどのように連動して、完全なエンドツーエンドのコラボレーション ソリューションが形成されるかが説明されています。主な構成要素には、ネットワーク インフラストラクチャ、セキュリティ、ゲートウェイ、トランク、メディア リソース、エンドポイント、呼処理エージェント、配置モデル、およびリッチ メディア会議などがあります。詳細については、Cisco Collaboration システム コンポーネントとアーキテクチャの概要（2-1 ページ）を参照してください。

- **呼制御およびルーティング**

  マニュアルのこの部分の各章では、音声およびビデオ コールがコラボレーション システムでどのように確立、ルーティング、および管理されるかが説明されています。この部分で扱うトピックには、帯域幅管理、ダイヤル プラン、緊急サービス、ディレクトリ統合およびアイデンティティの管理などがあります。詳細については、呼制御およびルーティングの概要（12-1 ページ）を参照してください。

- **コラボレーション アプリケーションおよびサービス**

  マニュアルのこの部分の各章では、コラボレーション ソリューションに組み込めるコラボレーション クライアント、アプリケーション、およびサービスが説明されています。この部分で扱うトピックには、Cisco Unified Communications Manager 組み込みアプリケーション、音声メッセージ、IM およびプレゼンス、モバイル コラボレーション、コンタクト センター、およびコール録音などがあります。詳細については、コラボレーション アプリケーションとサービスの概要（17-1 ページ）を参照してください。

- **コラボレーション システムのプロビジョニングと管理**

  マニュアルのこの部分の各章では、コラボレーション ソリューションのコンポーネントをサイズ調整する方法、そのソリューションに移行する方法、およびそれを管理する方法が説明されています。この部分で扱うトピックには、サイジングの考慮事項、移行オプション、およびネットワーク管理などがあります。詳細については、コラボレーション システムのプロビジョニングと管理の概要（24-1 ページ）を参照してください。

追加情報の参照先

このマニュアルには、Cisco Collaboration 製品と可能なソリューション設計の全範囲が含まれているため、個々の製品、機能、または設定の詳細をすべて説明することはできません。そのような詳細情報については、次の Web サイトで入手可能な特定の製品マニュアルを参照してください。

https://www.cisco.com

このマニュアルには、シスコ コラボレーション テクノロジーを使用して独自のコラボレーション ソリューションを設計する方法に関する一般的なガイドラインが記載されています。また、シスコは、コラボレーション、音声およびビデオの導入に必要な特定の推奨されるアーキテクチャに関する開発、試験、および文書化も行ってきました。推奨されるアーキテクチャ（PA）では、エンジニアリングのベスト プラクティスに基づく規範的なソリューション設計が提供されており、それらは次の Web サイトで文書化されています。

https://www.cisco.com/go/pa

PART 1

コラボレーション システムのコンポーネントとアーキテクチャ

このパートの内容

マニュアルのこのパートに含まれる章は、次のとおりです。

Cisco Collaboration システム コンポーネントとアーキテクチャの概要

改訂日：2016 年 6 月 14 日

Unified Communications および Collaboration システムを企業環境に適切に構築するには、安定したネットワーク インフラストラクチャが必要となります。ネットワーク アーキテクチャでは、これ以外の重要な点として、適切なハードウェアおよびソフトウェアのコンポーネント、システム セキュリティおよび配置モデルの選択があります。

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

- ネットワーク インフラストラクチャ：QoS を有効にしながら、Unified Communications および Collaboration アプリケーションに対して冗長性と復元性を備えた基盤を保証します。
- 音声セキュリティ：Unified Communications および Collaboration アプリケーションの一般的なセキュリティ ポリシーを保証し、これらのアプリケーションが信頼する強固でセキュアなネットワーキング基盤を保証します。
- 配置モデル：Unified Communications および Collaboration 呼制御とアプリケーションの展開用にテストされたモデルと、Unified Communications および Collaboration の導入に適用するベスト プラクティスおよび設計ガイドラインを提供します。

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

SRND のこの部分に含まれる章は、次のとおりです。

- ネットワーク インフラストラクチャ（3-1 ページ）

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

- Cisco Collaboration Security（4-1 ページ）

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

- ゲートウェイ（5-1 ページ）

  この章では、パブリック ネットワークに接続するためのパスを提供するため、Unified Communications および Collaboration 配置の重要なコンポーネントである IP ゲートウェイについて説明します。この章では、ゲートウェイ トラフィックのタイプとパターン、プロトコル、キャパシティ プランニング、プラットフォームの選択、および FAX とモデムのサポートについて説明します。

- Cisco Unified CM トランク（6-1 ページ）

  この章では、IP 経由のコールをルーティングし、さまざまな Unified Communications および Collaboration 機能を活用できる機能を提供する、クラスタ間トランクとプロバイダー トランクの両方について説明しています。この章では、これらのトランクを経由する H.323 および SIP トランク、コーデック、および付加サービスについて説明します。

- メディア リソース（7-1 ページ）

  この章では、Unified Communications および Collaboration メディア リソースとして分類されるコンポーネントについて説明します。デジタル シグナル プロセッサ（DSP）と、それらの展開のためのコール終端、会議機能、トランスコーディング機能、および保留音（MoH）のすべてについて説明します。メディア ターミネーション ポイント（MTP）、その機能方法、および SIP トランクと H.323 トランクに関する設計上の考慮事項についても説明します。さらに、Trusted Relay Point、RSVP Agent、Annunciator、MoH、およびセキュア会議に関する設計上の考慮事項についても、この章で説明します。

- コラボレーション エンドポイント（8-1 ページ）

  この章では、シスコのポートフォリオで使用可能な Unified Communications および Collaboration のエンドポイントのさまざまなタイプについて説明します。対象のエンドポイントには、ソフトウェア ベースのエンドポイント、無線および有線の固定電話、ビデオ エンドポイント、時分割多重（TDM）に基づくアナログ接続のアナログ ゲートウェイとインターフェイス モジュールなどがあります。

- 呼処理（9-1 ページ）

  この章では、音声およびビデオ コール ルーティングを容易にする、さまざまなタイプの呼処理アプリケーションとプラットフォームについて説明します。この章では、プラットフォーム オプション、クラスタリング機能、呼処理に関するハイ アベイラビリティの考慮事項などの呼処理アーキテクチャについて説明します。

- コラボレーションの配置モデル（10-1 ページ）

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

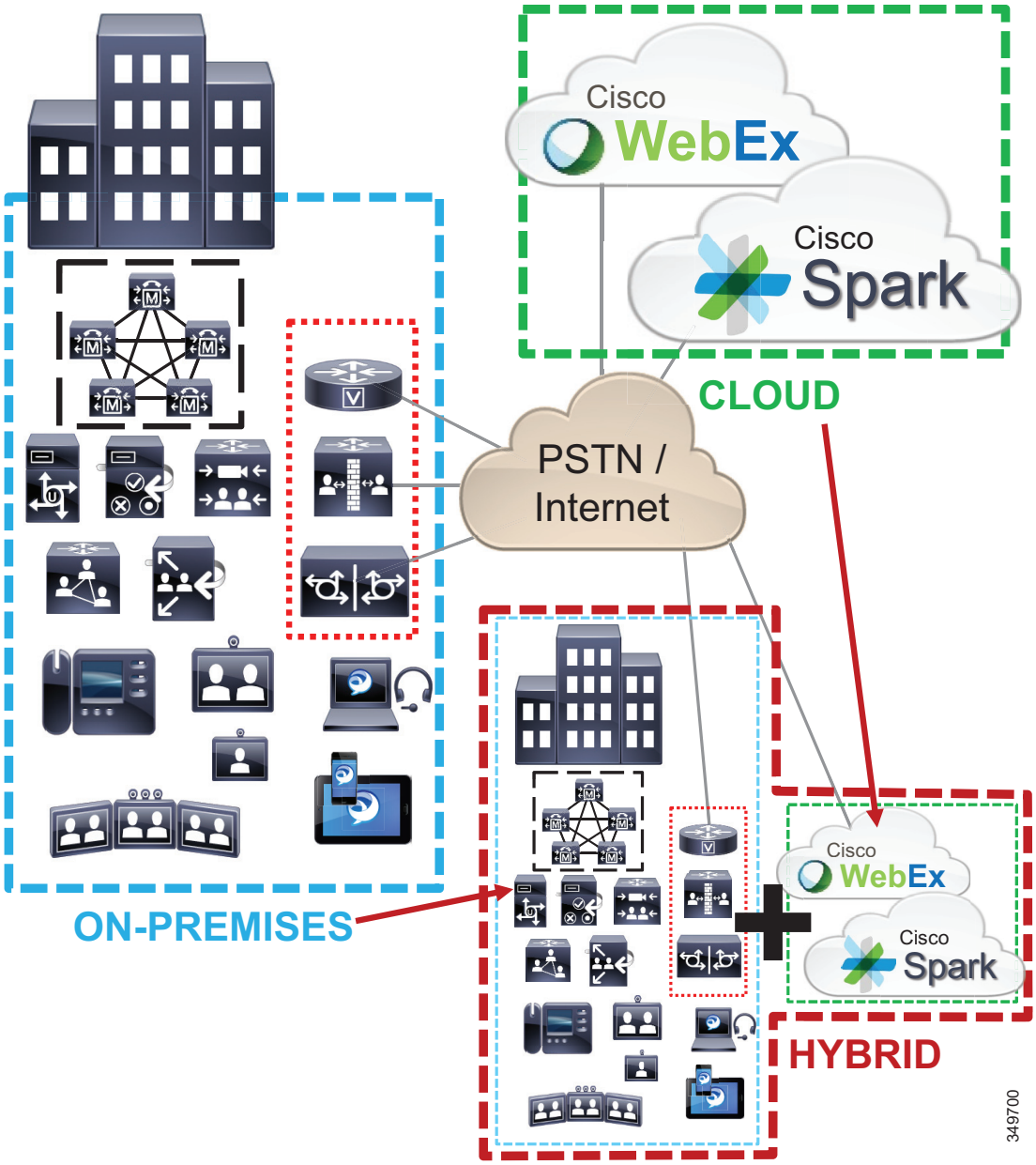
- Cisco Rich Media Conferencing（11-1 ページ）

  この章では、リッチ メディア会議について説明します。Unified Communications および Collaboration システムのユーザは、リッチ メディア会議を使用して、音声会議、ビデオ会議、および Web コラボレーション会議に対するスケジュール、管理、および参加を実行できます。この章では、ソフトウェアおよびハードウェア会議コンポーネントなどのさまざまな種類の会議とともに、Cisco TelePresence Video Communication Server（VCS）や Multipoint Control Unit（MCU）などについても説明します。また、配置モデル、ビデオ機能、H.323 と SIP の呼制御の統合、冗長性、さまざまな推奨ソリューションと設計のベスト プラクティスなど、リッチ メディア会議のさまざまな側面についても検討します。

アーキテクチャ

システム アーキテクチャによって、Unified Communications および Collaboration システムのすべてのコンポーネントが配置される基盤が構築されます。図 2-1 に、コラボレーション アプリケーションおよびサービスを社内のみ、クラウドのみ、または一連のハイブリッド サービス展開と組み合わせて提供できる仕組みについて概要を示します。

図 2-1　企業のコラボレーションの展開：オンプレミス、クラウド、およびハイブリッド



コール ルーティング、呼制御、アプリケーションとサービス、運用とサービスアビリティなどの Unified Communications および Collaboration システムのすべての要素が、システム アーキテクチャの適切な設計と配置に大きく依存しています。

ハイ アベイラビリティ

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

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

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

キャパシティ プランニング

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

システム サイジング、キャパシティ プランニング、およびサイジングに関連する配置上の考慮事項の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

ネットワーク インフラストラクチャ

改訂日：2018 年 3 月 1 日

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

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

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

図 3-1　　一般的なキャンパス ネットワーク インフラストラクチャ

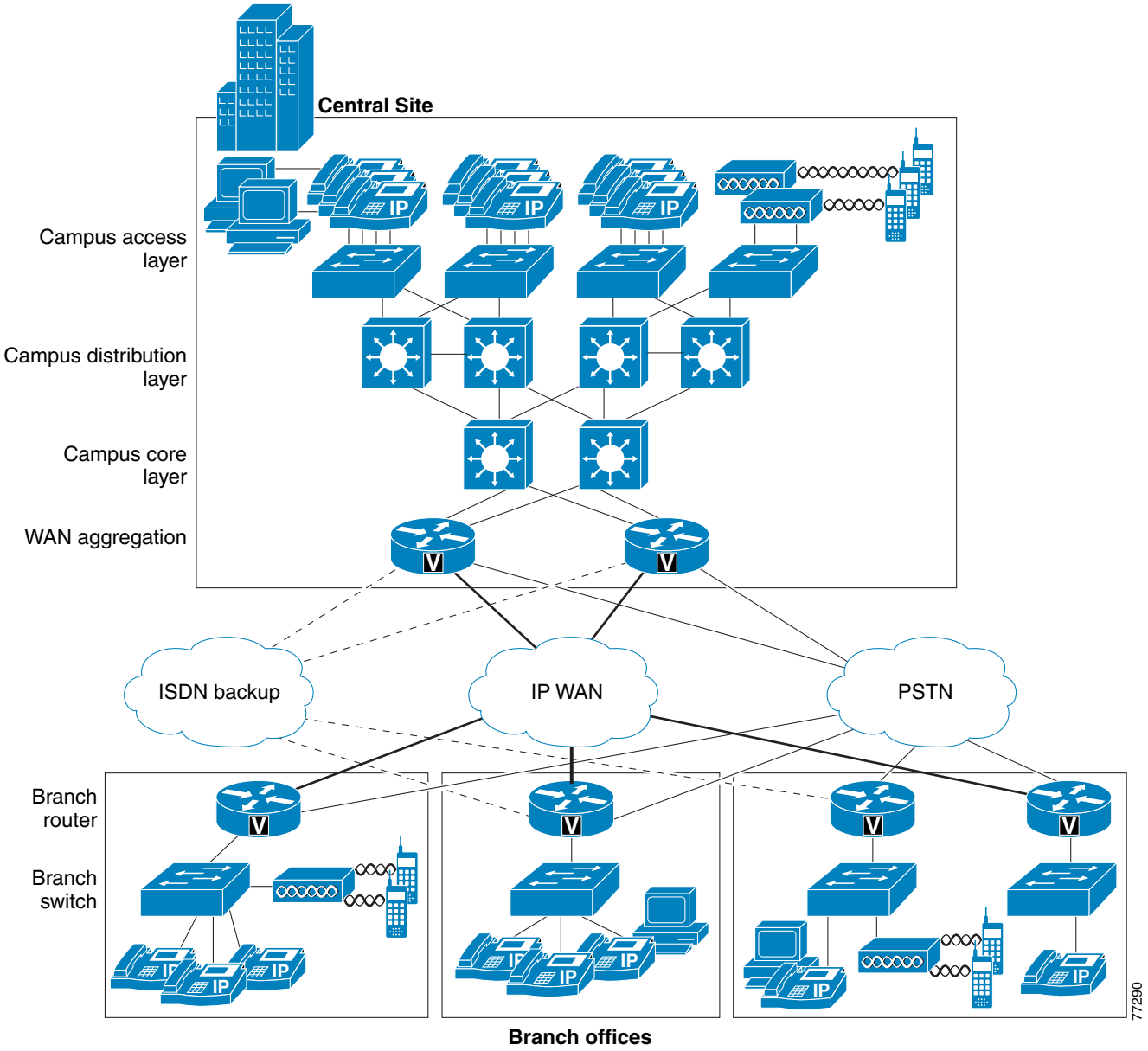


表 3-1　　ネットワーク インフラストラクチャ内の役割に必要な機能

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

1. 推奨作業です。
2. リンク速度が 786 kbps を下回る場合。

この章の変更点

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

表 3-2　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
コール制御トラフィックの帯域幅プロビジョニング	集中型コール処理による呼制御トラフィック用のプロビジョニング（3-61 ページ）	2018 年 3 月 1 日
この章から Cisco Nexus 1000V スイッチが削除されました	本書の対象外	2018 年 3 月 1 日

LAN インフラストラクチャ

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

- ハイ アベイラビリティのための LAN 設計（3-4 ページ）
- LAN の Quality of Service（QoS）（3-15 ページ）

ハイ アベイラビリティのための LAN 設計

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

- キャンパス アクセス レイヤ（3-5 ページ）
- キャンパス ディストリビューション レイヤ（3-10 ページ）
- キャンパス コア レイヤ（3-12 ページ）
- ネットワーク サービス（3-23 ページ）

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

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

キャンパス アクセス レイヤ

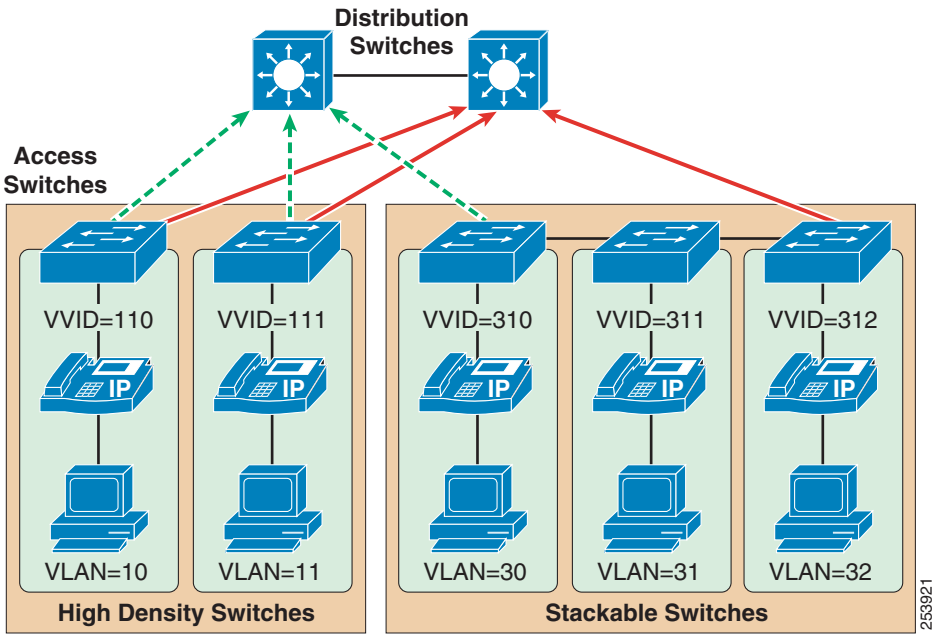
キャンパス LAN のアクセス レイヤに含まれるネットワーク部分は、デスクトップ ポートからワイヤリング クローゼット スイッチまでです。従来、アクセス レイヤ スイッチはディストリビューション レイヤへのレイヤ 2 アップリンクを持つレイヤ 2 デバイスとして設定されてきました。レイヤ 2 およびレイヤ 2 アクセス設計に対応するスパニングツリーの推奨事項は、十分に実証されており、次に簡単に説明します。レイヤ 3 プロトコルをサポートする最新の Cisco Catalyst スイッチでは、新しいルーテッド アクセス設計が可能となり、コンバージェンス時間と設計の簡素化における改善が行われていま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

レイヤ 2 アクセス設計の推奨事項

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

（注）　単一の Unified Communications VLAN におけるデバイス数を 512 ほどに制限する推奨事項は、ただ単に VLAN ブロードキャスト トラフィックの量を制御するためにだけ、必要な事項ではありません。1024 を超えるデバイスを含む IP サブネットのある VLAN に Unified CM をインストールすると、Unified CM サーバの ARP キャッシュがすぐに満杯になる可能性があり、Unified CM サーバとその他の Unified Communications のエンドポイント間の通信に深刻な影響を及ぼす場合があります。

図 3-2　　音声とデータに対応するアクセス レイヤ スイッチと VLAN



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

次の理由により、音声とデータの VLAN を分離することを推奨します。

- アドレス空間の確保と、外部ネットワークからの音声デバイスの保護

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

- 音声およびビデオ デバイスへの QoS 信頼性境界の拡張

  QoS 信頼性境界を音声およびビデオ デバイスに拡張し、同様にして、QoS 機能を PC や他のデータ デバイスに拡張できます。信頼できるデバイと信頼できないデバイスの詳細については、帯域幅管理（13-1 ページ）の章を参照してください。

- 悪質なネットワーク攻撃からの保護

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

- 管理および設定の容易性

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

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

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

スパニングツリー プロトコル（STP）

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

- PortFast

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

- ルート ガードまたは BPDU ガード

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

- UplinkFast と BackboneFast

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

- 単方向リンク検出（UDLD）

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

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

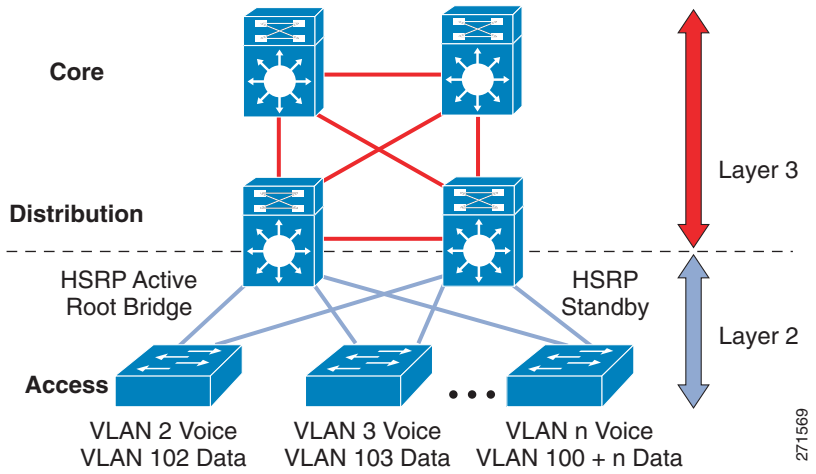
ルーテッド アクセス レイヤ設計

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

アクセス レイヤへの L2/L3 境界の移行

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

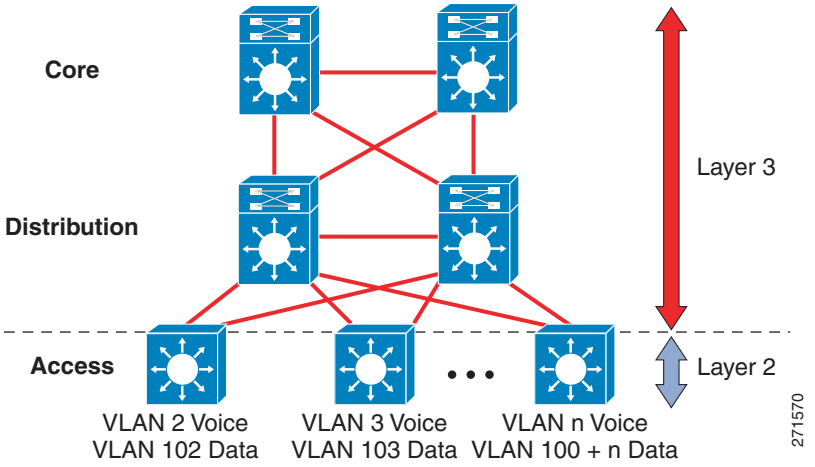
図 3-3　　従来のキャンパス設計：レイヤ 3 ディストリビューションを使用したレイヤ 2 アクセス



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

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

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



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

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

ルーテッド アクセス コンバージェンス

レイヤ 3 アクセス設計の使用には、次のような多くの潜在的利点があります。

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

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

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

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

キャンパス ディストリビューション レイヤ

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

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

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

ファーストホップ冗長プロトコル

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

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

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

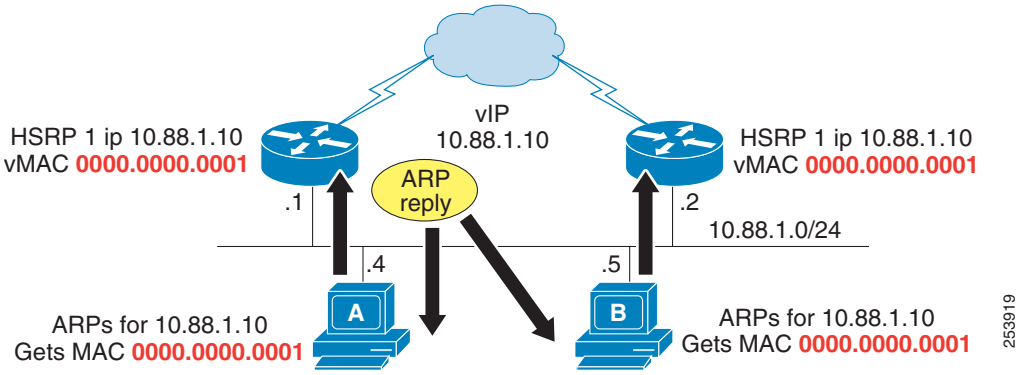
ゲートウェイ ロード バランシング プロトコル（GLBP）

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

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

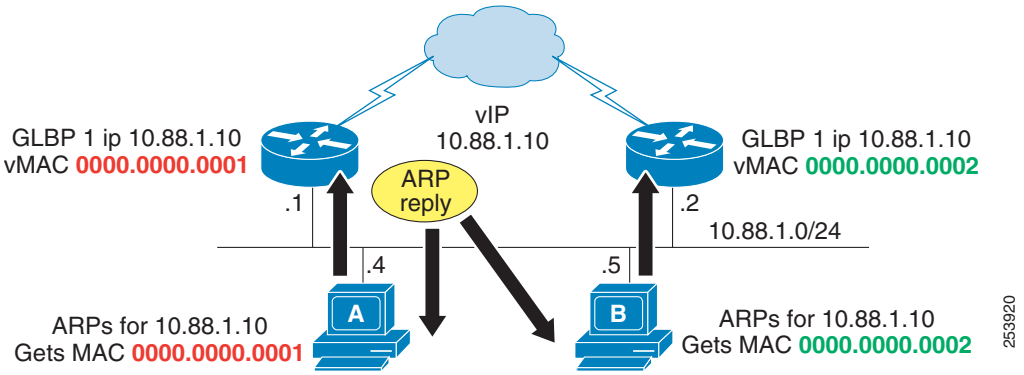
GLBP は HSRP と同じように設定され、機能します。HSRP では、アドレス解決プロトコル（ARP）を使用してデフォルト ゲートウェイの物理 MAC アドレスを取得するときに、単一の仮想 MAC アドレスがエンドポイントに指定されます（図 3-5 を参照）。

図 3-5　　HSRP では 1 つの仮想 MAC アドレスを使用



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

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



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

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

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

ルーティング プロトコル

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

キャンパス コア レイヤ

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

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

- 冗長なリンクまたはケーブル パス

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

- 冗長なデバイス

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

- 冗長なデバイス サブシステム

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

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

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

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

データセンターとサーバ ファーム

一般に、メディア リソース サーバなどの Cisco Unified Communications Manager（Unified CM）クラスタ サーバは、ファイアウォールで保護されたデータセンターまたはサーバ ファーム環境に配置されます。また、カンファレンス ブリッジ、DSP またはトランスコーダ ファーム、メディア ターミネーション ポイントなどの、集中型ゲートウェイと集中型ハードウェア メディア リソースも、データセンターまたはサーバ ファームに配置されることがあります。Cisco Unified Communications Manager（Unified CM）クラスタ サーバおよびメディア リソースに関連したファイアウォールの配置は、ネットワークにおけるセキュリティの設計および実装方法に影響を与える可能性があります。Unified Communications システムに関連したファイアウォール配置の設計ガイドラインについては、ファイアウォール（4-35 ページ）を参照してください。

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

Power over Ethernet（PoE）

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

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

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

Cisco PoE インライン パワーのほか、シスコでは、IEEE 802.3af PoE 標準および IEEE 802.3at 拡張 PoE 標準をサポートしています。802.3af 標準および 802.3at 標準に対応している Cisco Unified IP Phone の詳細については、ご使用の電話機モデルの製品マニュアルを参照してください。

IP Phone のエネルギー管理

Cisco EnergyWise テクノロジーを利用すると、Power over Ethernet（PoE）を使用する Unified Communications エンドポイントなど、IP ネットワーク上のデバイスのエネルギー使用をインテリジェントに管理できます。Cisco EnergyWise アーキテクチャでは、設定可能なスケジュールに基づいて、EnergyWise 対応スイッチ上の PoE 接続デバイスの電源をオンオフできます。EnergyWise の詳細については、次の URL にあるマニュアルを参照してください。

https://www.cisco.com/en/US/products/ps10195/index.html

EnergyWise 管理では、PoE スイッチにより IP Phone の電源をオフにすると、IP Phone の電源が完全に切れます。EnergyWise は IP Phone に接続しているポートのインライン パワーをシャット ダウンします。シャット ダウンは、スケジュールに従って実行されるか、ネットワーク管理ツールでコマンドを使用して実行されます。電源が無効になっている場合、電話機にアクティブ コールがあるかどうかを判断する検証は行われません。電源がオフになると、すべてのアクティブ コールが終了します。IP Phone の登録が Cisco Unified Communications Manager から失われ、この電話機とのコールの送受信は一切できなくなります。電話機には電源をオンにするメカニズムがないため、その電話機では緊急コールも使用できなくなります。

IP Phone は、スイッチの電源を再びオンにした場合にのみ再起動できます。電源が回復すると、IP Phone はリブートして、新しい IP アドレスの要求、設定ファイルのダウンロード、新しい設定パラメータの適用、新しいファームウェアまたはロケールのダウンロード、Cisco Unified CM への登録など、リカバリ プロセスを実行します。

EnergyWise スケジュールは、シスコのネットワーク インフラストラクチャで設定および管理されます。IP Phone または Cisco Unified CM での設定は一切必要はありません。ただし、電話機の電力消費は、Unified CM に設定したデバイス プロファイルでも管理できます。Unified CM で示されるエネルギー節約オプションは、次のとおりです。

- Power Save Plus モード（3-14 ページ）
- Power Save モード（3-15 ページ）

Power Save Plus モード

Power Save Plus モードでは、電話機のオンとオフの時間およびアイドル タイムアウト時間を IP Phone で設定できます。Cisco IP Phone の EnergyWise Power Save Plus 設定オプションでは、IP Phone がスリープする（電源が切れる）時間とウェイク アップする（電源が入る）時間のスケジュールを指定します。このモードには、EnergyWise 対応のネットワークが必要です。EnergyWise が有効な場合は、スリープ時間とウェイク アップ時間およびその他のパラメータを使用して、電話機の電源を管理できます。Power Save Plus のパラメータは、Cisco Unified CM Administration の製品固有のデバイス プロファイルで設定され、電話機設定 XML ファイルの一部として IP Phone に送信されます。

この省電力モードで設定された電源オフ中に、IP Phone は要求をスイッチに送信して、指定された時間にウェイク アップすることを要求します。スイッチが EnergyWise 対応の場合、スイッチは要求を受け入れて電話機ポートへの電力供給を低減し、電話機をスリープ状態にします。スリープ モードでは、電話機の電力消費が 1 ワット以下に低減されます。この場合、電話機は完全には電源オフになりません。電話機がスリープ状態になっている場合、PoE スイッチは電話機の Select キーが点灯するだけの最小限の電力を供給します。ユーザは Select ボタンを使用することで、IP Phone をウェイク アップできます。コールがアクティブになっている場合、IP Phone はスリープ モードになりません。オプションの音声および表示アラートを設定すると、電話機が Power Save Plus モードに入る前にユーザに警告することができます。スリープ状態のとき、電話機は Cisco Unified CM に登録されていないため、着信コールを受信できません。電話機のデバイス構成プロファイルの [未登録転送（Forward Unregistered）] 設定を使用して、電話機の番号への着信コールの処理方法を指定します。

（注）　Cisco EnergyWise Power Save Plus モードは、ほとんどの Cisco IP Phone と Collaboration Desk Endpoint でサポートされます。EnergyWise Power Save Plus をサポートしているエンドポイントについては、ご使用のエンドポイント モデルのデータ シートを参照してください。
https://www.cisco.com/c/en/us/products/collaboration-endpoints/product-listing.html

Power Save モード

省電力モードでは、電話機を使用していない間、スクリーンのバックライトが消灯します。このモードでは、電話機は Cisco Unified CM に登録されたままになるため、着信コールを受けたり発信コールを行うことができます。Cisco Unified CM Administration には製品固有の設定オプションがあり、曜日によってディスプレイを指定時間にオフにしたり、1 日中オフにすることができます。電話機は、ユーザがハンドセットを持ち上げるか、任意のボタンを押さない限り、スケジュールされた期間にわたって、電力節約モードのままになります。Power Save モードには、EnergyWise 対応ネットワークは必要ありません。タイムアウトになって電源が自動的にオフになるまでディスプレイをオンにしておくように、アイドル時間をスケジュールできます。このモードでは、電話機の電源はオンのままになるため、着信コールを受けることができます。

Power Save モードは、Power Save Plus モードと一緒に使用できます。両方とも使用すると、Cisco Unified IP Phone による総電力消費量が大幅に減少します。

これらのモードの設定の詳細については、次の URL から入手可能な Cisco IP Phone および Collaboration Desk Endpoint の管理ガイドを参照してください。

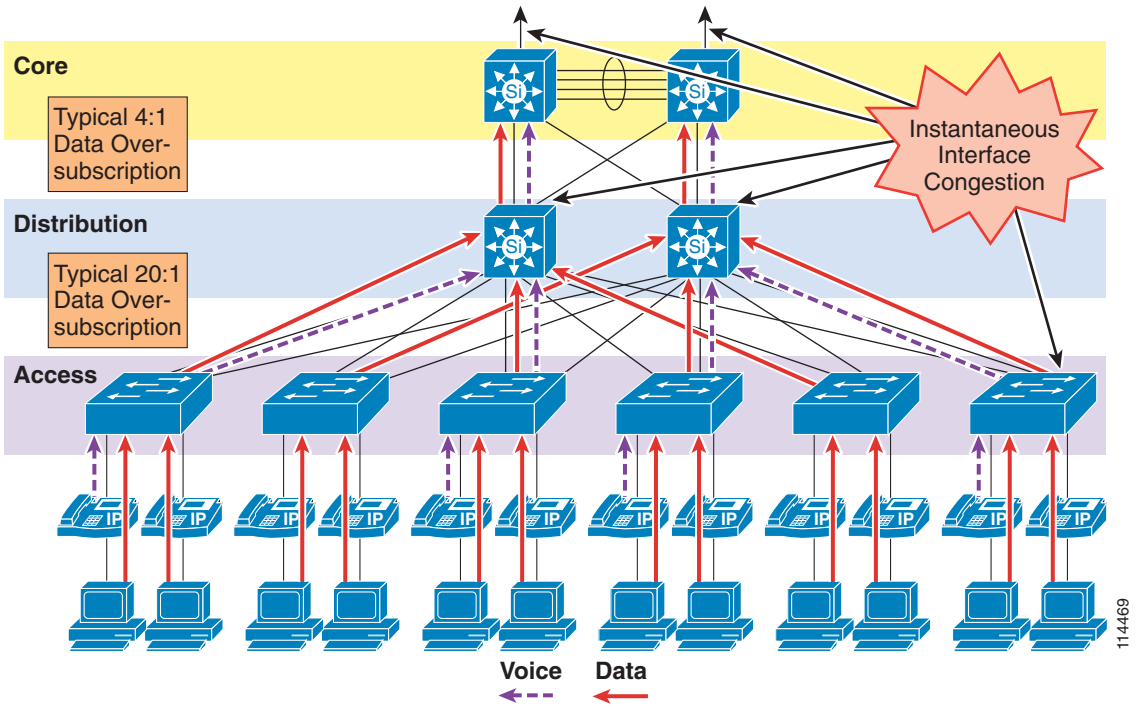
https://www.cisco.com/c/en/us/products/collaboration-endpoints/product-listing.html

LAN の Quality of Service（QoS）

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

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

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



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

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

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

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

トラフィックを管理して音声とビデオの品質を確保するには、ネットワーク全体で次のタイプの QoS ツールが必要です。

- トラフィック分類

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

- キューイングまたはスケジューリング

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

- 帯域幅のプロビジョニング

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

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

- トラフィック分類（3-17 ページ）
- インターフェイス キューイング（3-19 ページ）
- 帯域幅のプロビジョニング（3-20 ページ）
- QoS が使用されない場合の IP コミュニケーションの障害（3-20 ページ）

トラフィック分類

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

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

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

Application	レイヤ 3 分類			レイヤ 2 分類
	タイプ オブ サービス（ToS）IP Precedence（IPP）	Per-Hop Behavior（PHB）	Diffserv コード ポイント（DSCP）	サービス クラス（CoS）
ルーティング	6	CS6	48	6
音声 Real-Time Transport Protocol（RTP）	5	EF	46	5
ビデオ会議	4	AF41	34	4
IP ビデオ	4	AF41	34	4
イマーシブ ビデオ リアルタイム インタラクティブ	4	CS4	32	4

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

Application	レイヤ 3 分類			レイヤ 2 分類
	タイプ オブ サービス（ToS）IP Precedence（IPP）	Per-Hop Behavior（PHB）	Diffserv コード ポイント（DSCP）	サービス クラス（CoS）
ストリーミング ビデオ	3	AF31	26	3
コール シグナリング	3	CS3	24	3
トランザクション データ	2	AF21	18	2
ネットワーク管理	2	CS2	16	2
Scavenger	1	CS1	8	1
ベストエフォート型	0	0	0	0

トラフィック分類の詳細については、次の URL から入手可能な QoS 設計ガイドを参照してください。

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-ipv6/design-guide-listing.html

ビデオ テレフォニーのトラフィック分類

IP ビデオ テレフォニーに関係する主なクラスは、次のとおりです。

- 音声

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

- ビデオ会議

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

- コール シグナリング

  音声およびビデオ会議のコール シグナリングは、CoS 3（IP Precedence 3、PHB CS3、または DSCP 24）に分類されます。

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

ビデオ コールと音声専用コール間の QoS マーキングの相違点

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

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

シスコでは、ビデオ コールのオーディオ チャネルとビデオ チャネルを個別にマーキングできるように、エンドポイントに対するこの要件を変更中です。使用事例に応じて柔軟に、ビデオ コールのオーディオ チャネルとビデオ チャネルに同じ DSCP 値をマーキングしたり、異なる DSCP 値をマーキングできるようになります。DSCP マーキングの詳細については、帯域幅管理（13-1 ページ）の章を参照してください。

シグナリング クラスは、すべての音声シグナリング プロトコル（SCCP、MGCP など）、およびビデオ シグナリング プロトコル（SCCP、H.225、RAS、CAST など）に適用されます。

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

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

Trusted Relay Point（TRP）を使用した QoS の適用

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

TRP は、既存の Cisco IOS メディア ターミネーション ポイント（MTP）機能に基づくメディア リソースです。

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

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

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

インターフェイス キューイング

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

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

キャンパス内の送信インターフェイス バッファは、ネットワーク トラフィック自体にバースト性があるため、短い時間間隔で散発的に輻輳する傾向があります。輻輳が起きると、その送信インターフェイスを宛先とするすべてのパケットがドロップされます。音声トラフィックのドロップを防止する唯一の方法は、キャンパス スイッチ上で複数のキューを設定することです。このため、ポートごとに 2 つ以上の出力キューを持ち、レイヤ 2、レイヤ 3、またはその両方の QoS 分類に基づいてこれらのキューにパケットを送信する機能を持つスイッチを常に使用することを推奨します。大部分の Cisco Catalyst スイッチは、ポートごとに 2 つ以上の出力キューをサポートしています。Cisco Catalyst スイッチのインターフェイス キューイング機能の詳細については、https://www.cisco.com/en/US/products/hw/switches/index.html にあるマニュアルを参照してください。

帯域幅のプロビジョニング

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

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

QoS が使用されない場合の IP コミュニケーションの障害

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

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

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

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

Cisco UCS サーバを使用する仮想 Unified Communications に関する QoS 設計上の考慮事項

Cisco Unified Communications Manager（Unified CM）などの Unified Communications アプリケーションは、VMware Hypervisor の最上位で仮想マシンとして機能します。これらの Unified Communications 仮想マシンは、ハードウェアベースのイーサネット スイッチではなく、仮想ソフトウェア スイッチに接続されます。次のタイプの仮想ソフトウェア スイッチを使用できます。

- VMware vSphere 標準スイッチ

  VMware ライセンス スキームのタイプとは関係なく、すべての VMware vSphere Edition で使用できます。vSphere 標準スイッチは、それが設定されているホストにのみ存在します。

- VMware vSphere 分散スイッチ

  VMware vSphere の Enterprise Plus Edition でのみ使用可能です。vSphere 分散スイッチは、データセンターの関連するすべてのホスト全体に対して単一のスイッチとして動作し、ソフトウェア仮想スイッチの管理をシンプル化します。

仮想接続の観点から見ると、各仮想マシンは、ブレード サーバに配置されている上記の仮想スイッチのいずれかに接続できます。Cisco UCS B シリーズ ブレード サーバを使用する場合、ブレード サーバは、UCS シャーシ内のファブリック エクステンダから UCS ファブリック インターコネクト スイッチ（Cisco UCS 6200 シリーズなど）を経由して、ネットワークの他の個所に物理的に接続します。UCS ファブリック インターコネクト スイッチは、顧客のイーサネット LAN および FC SAN と物理的配線が接続される個所です。

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

輻輳シナリオ

Cisco UCS B シリーズ ブレード サーバと Cisco Collaboration アプリケーションのみの配置では、ネットワーク輻輳やオーバーサブスクリプションのシナリオが発生する可能性が非常に低くなります。これは、UCS ファブリック インターコネクト スイッチが高キャパシティのスイッチング ファブリックを備えており、さらにサーバ ブレードごとの使用可能帯域幅が一般的なコラボレーション アプリケーションの最大トラフィック要件を大幅に上回っているからです。

ただし、輻輳が発生する状況になる場合もあります。たとえば、多数の B シリーズ ブレード サーバとシャーシ、多数のアプリケーション、および高いネットワーク帯域幅を必要とするサードパーティ製アプリケーションが配置されている場合は、UCS B シリーズ システムのさまざまなネットワーク要素（アダプタ、I/O モジュール、ファブリック インターコネクト）で輻輳が発生する可能性があります。また、FCoE トラフィックは IP トラフィックと同じネットワーク要素を共有するので、アプリケーションが大量のストレージ転送を実行すると、ネットワーク要素での帯域幅使用量が増加し、輻輳が発生する可能性があります。

この潜在的な輻輳に対処するには、QoS を実行する必要があります。

Cisco UCS B シリーズでの QoS の実装

Cisco UCS ファブリック インターコネクト スイッチと Cisco VIC アダプタなどのアダプタは、レイヤ 2 CoS 値に基づいて QoS を実行します。トラフィック タイプは CoS 値によって QoS システム クラスに分類されます。QoS システム クラスによって、最小保障帯域幅や各クラスに対して使用するパケット ドロップ ポリシーなどが決まります。ただし、Cisco Collaboration アプリケーションは、レイヤ 2 ではなく、レイヤ 3 でのみ QoS マーキングを実行します。したがって、アプリケーションで使用される L3 値を Cisco UCS 要素で使用される L2 CoS 値にマッピングする必要があります。

VMware vSphere 標準スイッチ、vSphere 分散スイッチ、Cisco UCS ファブリック インターコネクト スイッチ、およびその他の UCS ネットワーク要素は、L3 と L2 値間でこのマッピングを実行できません。

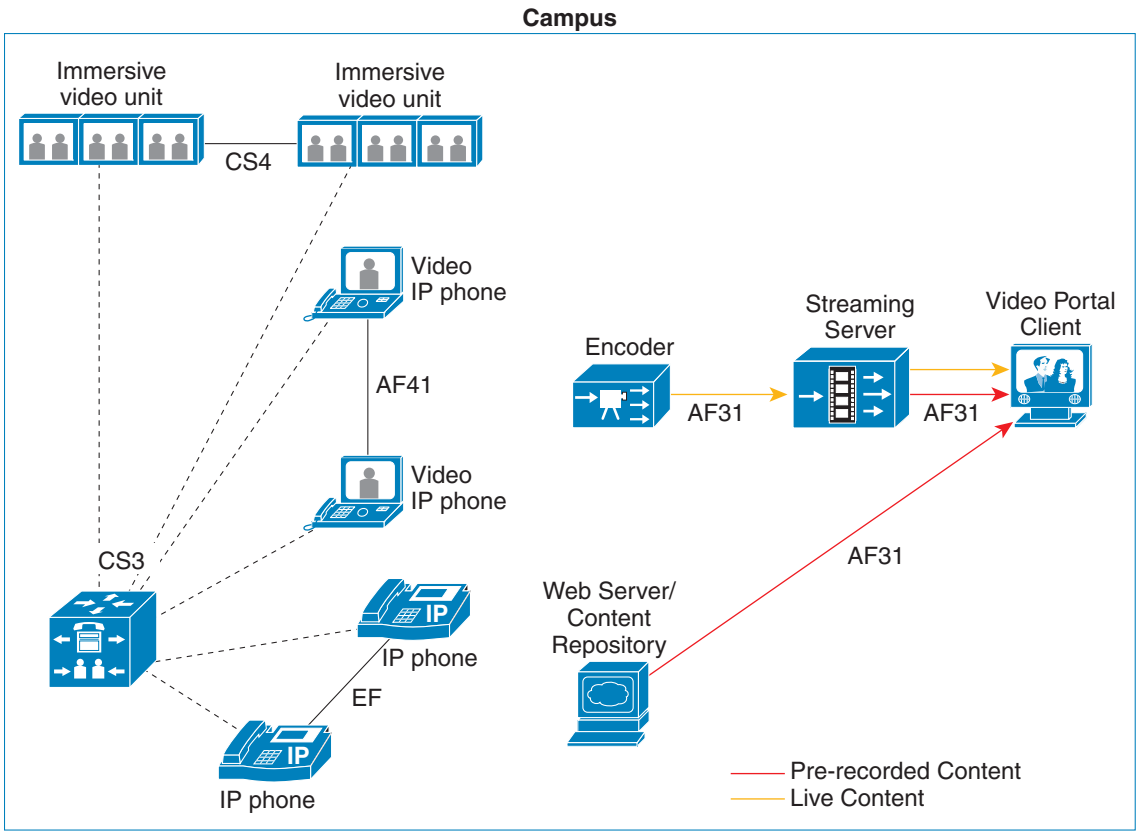
(注)　Fibre Channel over Ethernet（FCoE）トラフィックには、他のトラフィック タイプでは使用できない予約済み QoS システム クラスがあります。デフォルトでは、このシステム クラスの CoS 値は 3 です。この値は、上記の例で音声およびビデオ シグナリング トラフィックで使用されるシステム クラスに割り当てられた値と同じです。音声およびビデオ シグナリング トラフィックによって FCoE システム クラスが使用されないようにするには、FCoE システム クラスに異なる CoS 値を割り当てます（2 や 4 など）。

この問題を回避するには、複数の仮想スイッチを作成し、それらの各スイッチのアップリンク ポートに異なる CoS 値を割り当てることができます。たとえば、仮想スイッチ 1 のアップリンク ポートに CoS 値「1」を設定し、仮想スイッチ 2 のアップリンク ポートに CoS 値「2」を設定します。次に、必要な QoS システム クラスに応じて、アプリケーションの仮想マシンが仮想スイッチに割り当てられます。このアプローチの欠点は、仮想マシンからのすべてのトラフィック タイプに同じ CoS 値が使用されることです。たとえば、Unified CM 仮想マシンでは、MoH トラフィック、シグナリング トラフィック、音声以外のトラフィック（バックアップ、CDR、ログ、Web トラフィック）など、リアルタイム メディア トラフィックが同じ CoS 値を共有します。

ビデオに関する QoS 設計上の考慮事項

異なるビデオ アプリケーションに異なる DSCP マーキングを使用することを推奨します。Unified CM 9.*x* は、イマーシブ ビデオ トラフィックやビデオ会議（IP ビデオ テレフォニー）トラフィックに対する異なる DSCP マーキングをサポートしています。デフォルトでは、Unified CM 9.*x* は、推奨 DSCP 値として、TelePresence（イマーシブ ビデオ）コールに CS4、ビデオ（IP ビデオ テレフォニー）コールに AF41 を事前設定します。図 3-8 は、推奨 DSCP 値を使用した統合環境でのさまざまなビデオ アプリケーションを示しています。

図 3-8　　統合ネットワークでの推奨 QoS トラフィック マーキング



QoS のオーバーヘッドの計算

音声とは異なり、リアルタイム IP ビデオ トラフィックは通常、ややバースト性がある可変ビット レート ストリームです。音声とは異なり、ビデオにはネットワーク オーバーヘッドを計算するための明確な公式がありません。ビデオ パケットのサイズとレートがビデオ画像自体の動きの度合いに比例して異なるためです。ネットワーク管理者から見ると、帯域幅はレイヤ 2 で常にプロビジョニングされますが、パケット サイズの変動や、パケットがエンドツーエンドで移動するレイヤ 2 メディアの違いのため、レイヤ 2 でプロビジョニングすべき実際の帯域幅を計算するのは困難です。ただし、十分にテストされ広く用いられている慣習的ルールとして、ビデオ帯域幅を 20 % 多めにプロビジョニングするという方法があります。これの方法は、10 % のバーストとレイヤ 2 からレイヤ 4 へのネットワーク オーバーヘッドに対応します。

ネットワーク サービス

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

ドメイン ネーム システム（DNS）

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

多数のサービスを適切に動作させるために、コラボレーション ソリューション全体は DNS に依存しているので、可用性の高い DNS 構成を適切な場所に配置する必要があります。DNS への依存が不要な基本的な IP テレフォニー配置では、ホスト名ではなく IP アドレスを使用して Unified CM、ゲートウェイ、エンドポイント デバイス間の通信をサポートして確保するように、Unified CM を設定できます。

DNS を使用しない Unified CM の配置

DNS が不要な基本的な IP テレフォニー配置の場合は、ホスト名ではなく IP アドレスを使用するように、Unified CM、ゲートウェイ、エンドポイント デバイスを設定することを推奨します。これは、Unified CM クラスタのインストール時に実行する必要があります。パブリッシャとサブスクライバ ノードをインストールするときは、DNS を有効にするオプションを選択しないことを推奨します。Unified CM クラスタへのパブリッシャ ノードの初期インストールが完了すると、そのパブリッシャは、システムに提供したホスト名によってサーバ テーブルで参照されます。後続のサブスクライバ ノードをインストールして設定する前、またはエンドポイントを定義する前に、このサーバ エントリをパブリッシャのホスト名ではなく IP アドレスに変更する必要があります。クラスタに追加する各サブスクライバ ノードは、ホスト名ではなく IP アドレスで、同じサーバ テーブルに定義する必要があります。各サブスクライバ ノードは、1 デバイスずつこのサーバ テーブルに追加する必要があります。新しいサブスクライバ ノードをインストールするときを除き、いかなるときも存在しないサブスクライバ ノードは定義しないでください。

DNS を使用する Unified CM の配置

DNS サーバは地理的な冗長性を考慮して配置する必要があります。そのように配置すると、1 台の DNS サーバで障害が発生しても、IP テレフォニー デバイス間のネットワーク通信が妨げられることはありません。DNS サーバを冗長にすると、一方の DNS サーバで障害が発生しても、引き続き、DNS を利用してネットワーク上で通信するデバイスが、バックアップまたはセカンダリ DNS サーバから、ホスト名から IP アドレスへのマッピングを受信できることが保証されます。

Unified CM は DNS を使用して次を実行できます。

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

コラボレーション クライアントは DNS を使用して次を実行できます。

- シングル サインオン（SSO）
- ユーザ登録の自動検出を必要とする Jabber を配置
- セキュアなシグナリングとメディアのための証明書ベースのセキュリティ

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

表 3-4 の例は、Unified CM 環境で、DNS サーバが A レコード（ホスト名から IP アドレスへの解決）、Cname レコード（エイリアス）、SRV レコード（冗長性、ロード バランシング、およびサービス ディスカバリ用のサービス レコード）を使用できるしくみを示しています。

表 3-4　　Unified CM における DNS の使用例

ホスト名（Host Name）	タイプ（Type）	TTL	データ
CUCM-Admin.cluster1.cisco.com	ホスト（A）	12 時間	182.10.10.1
CUCM1.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.1
CUCM2.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.2
CUCM3.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.3
CUCM4.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.4
TFTP-server1.cluster1.cisco.com	ホスト（A）	12 時間	182.10.10.11
TFTP-server2.cluster1.cisco.com	ホスト（A）	12 時間	182.10.10.12
CUP1.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.15
CUP2.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.16
www.CUCM-Admin.cisco.com	エイリアス（CNAME）	デフォルト	CUCM-Admin.cluster1.cisco.com
_sip._tcp.cluster1.cisco.com	サービス（SRV）	デフォルト	CUCM1.cluster1.cisco.com
_sip._tcp.cluster1.cisco.com	サービス（SRV）	デフォルト	CUCM2.cluster1.cisco.com
_sip._tcp.cluster1.cisco.com	サービス（SRV）	デフォルト	CUCM3.cluster1.cisco.com
_sip._tcp.cluster1.cisco.com	サービス（SRV）	デフォルト	CUCM4.cluster1.cisco.com

Jabber クライアントについては、次の URL にある『*Cisco Jabber DNS Configuration Guide*』を参照してください。

https://www.cisco.com/web/products/voice/jabber.html

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）

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

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

DHCP オプション 150

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

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

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

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

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

電源復帰後の電話機による DHCP オペレーション

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

DHCP のリース期間

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

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

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

次のいずれかの方法によって、この状況を緩和できます。

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

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

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

  このアプローチは、WAN 接続の中断の影響を受けません。このアプローチを使用すると、IP アドレスの管理が分散されるため、各拠点で設定を更新する作業が発生します（詳細については、DHCP のネットワーク配置（3-28 ページ）を参照してください）。

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

DHCP のネットワーク配置

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

- 中央の DHCP サーバ

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

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

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

  集中型マルチサイト Unified CM 配置で使用する DHCP を設定する場合は、中央の DHCP サーバを使用して、中央にあるデバイスに DHCP サービスを提供できます。リモート デバイスは、ローカルに設置されたサーバから、またはリモート サイトにある Cisco IOS ルータから、DHCP サービスを受信できます。このタイプの配置では、WAN に障害が発生しても、リモートのテレフォニー デバイスから DHCP サービスを使用できることが保証されます。例 3-1 は、Cisco IOS DHCP サーバの基本的なコンフィギュレーション コマンドを示しています。

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

```
! Activate DHCP Service on the IOS Device

service dhcp

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

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

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

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

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

Unified CM DHCP サーバ（スタンドアロン サーバ対共存サーバ）

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

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

トリビアル ファイル転送プロトコル（TFTP）

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

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

- 電話機設定ファイル
- 電話機ファームウェア ファイル
- Certificate Trust List（CTL）ファイル
- ID 信頼リスト（ITL）ファイル
- トーン ローカリゼーション ファイル
- ユーザ インターフェイス（UI）ローカリゼーションおよび辞書ファイル
- リンガー ファイル
- ソフトキー ファイル
- SIP 電話機のダイヤル プラン ファイル

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

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

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

（注）　TFTP サーバは、共存するサブスクライバ サーバのデータベースからローカル データベースの読み取りを実行できます。ローカル データベースの読み取りは、パブリッシャが使用できない場合にユーザ方向機能を保持するなどの利点を提供するだけではなく、WAN を介したクラスタリングを通じて、複数の TFTP サーバの分散を可能にします（登録済み電話機があるサーバに適用されるのと同じ WAN を介したクラスタリングの遅延規則が TFTP サーバに適用されます）。この設定によって TFTP サービスがエンドポイントに近くなるため、遅延が低減され、サイト間で障害が確実に分離されます。

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

TFTP サーバが最大数の要求を処理しているときにデバイスが設定ファイルを要求すると、そのデバイスは、後で設定ファイルを要求するように指示するメッセージを TFTP サーバから受信します。Maximum Serving Count サービス パラメータは、TFTP サーバが同時に処理できる要求の最大数を指定し、設定できます（デフォルト値 = 2,500 件の要求）。同じサーバ上で TFTP サービスが他の Cisco CallManager サービスと一緒に実行されている場合は、デフォルト値を使用します。専用 TFTP サーバでは、Maximum Serving Count として、シングル プロセッサ システムの場合 2,500、デュアル プロセッサ システムの場合 3,000 の推奨値を使用します。

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

TFTP の動作の例

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

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

TFTP ファイル転送時間

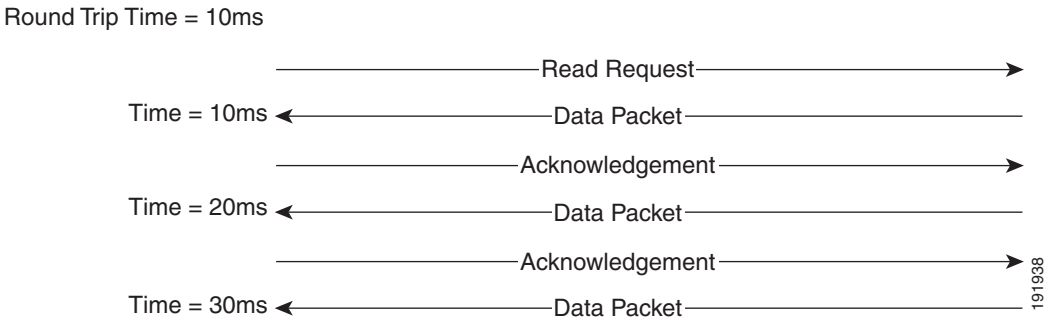
エンドポイントがファイルを要求するたびに、新しい TFTP 転送セッションが確立します。集中型呼処理配置の場合、これらの各転送が完了する時間は、エンドポイントを起動し、動作可能にするためにかかる時間と定期保守時にエンドポイントをアップグレードするためにかかる時間に影響を与えます。TFTP 転送時間は、これらの最終状態に影響を与える唯一の要因ではありませんが、重要なコンポーネントです。

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

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

TFTP はユーザ データグラム プロトコル（UDP）上で動作します。伝送制御プロトコル（TCP）とは異なり、UDP は信頼性の高いプロトコルではありません。つまり、UDP は本質的にパケット損失を検出する機能を備えていません。言うまでもなく、ファイル転送におけるパケット損失の検出は重要であるため、RFC 1350 は TFTP をロックステップ プロトコルとして規定しています。つまり、TFTP 送信側は 1 つのパケットを送信し、次のパケットを送信する前に応答を待ちます（図 3-9 を参照）。

図 3-9　TFTP パケット転送シーケンスの例

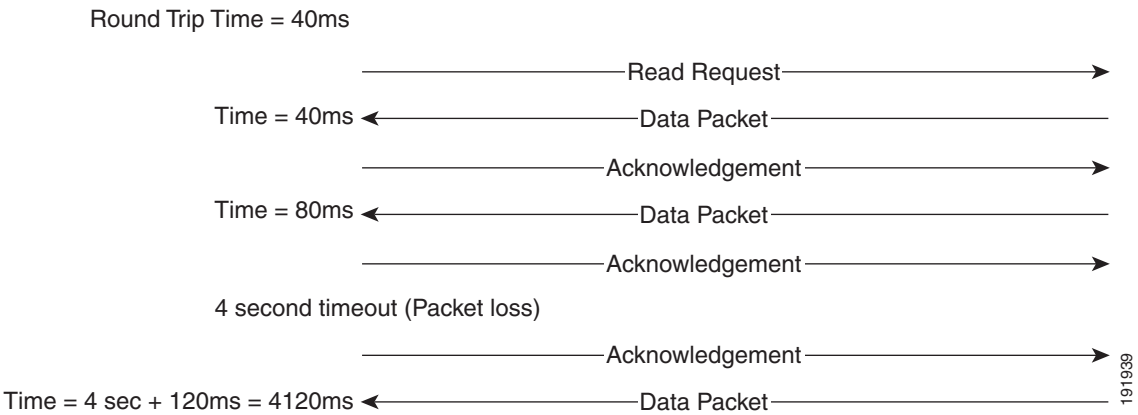


応答がタイムアウト時間（デフォルトでは 4 秒）内に受信されない場合、送信側はデータ パケットまたは確認応答を再送信します。5 回送信されても応答がない場合、TFTP セッションは失敗します。タイムアウト時間は常に同じであり、TCP タイムアウトのように適応できないので、パケット損失は、転送セッションを完了するのにかかる時間を大幅に増加させる可能性があります。

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

図 3-10 では、ラウンドトリップ時間が 40 ms に増加し、1 つのパケットが送信中に失われています。エラー率が 12 % と高い率である一方、セッションを完了する時間が 30 ms（図 3-9 を参照）から 4160 ms（図 3-10 を参照）に増加しているので、TFTP の遅延とパケット損失の効果が簡単にわかります。

図 3-10　　TFTP セッション完了時間におけるパケット損失の効果



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

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

ここで、

FileTransferTime は秒単位です。

FileSize はバイト単位です。

RTT はラウンドトリップ時間（ミリ秒単位）です。

ERR はエラー率または失われたパケットの比率です。

Timeout はミリ秒単位です。

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

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

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

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

TFTP サーバの冗長性

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

TFTP のロード シェアリング

TFTP サーバの順序が異なるリストを別のサブネットに付与して、ロード バランシングを実現することを推奨します。次に例を示します。

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

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

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

プロキシ TFTP

マルチクラスタ システムでは、プロキシ TFTP サービスは、1 つのプライマリ TFTP サーバを介して複数のクラスタから TFTP ファイルを提供できます。単一のサブネットまたは VLAN に複数のクラスタからの電話機が含まれている場合や、複数のクラスタが同じ DHCP TFTP オプション（150）を共有している場合、プロキシ TFTP はそれらの状況に対する単一の TFTP 参照として機能できます。

図 3-11 に示すように、プロキシ TFTP サービスは、シングルレベル階層として機能します。より複雑な複数レベル階層はサポートされません。

図 3-11　　プロキシ TFTP のシングル レベル階層

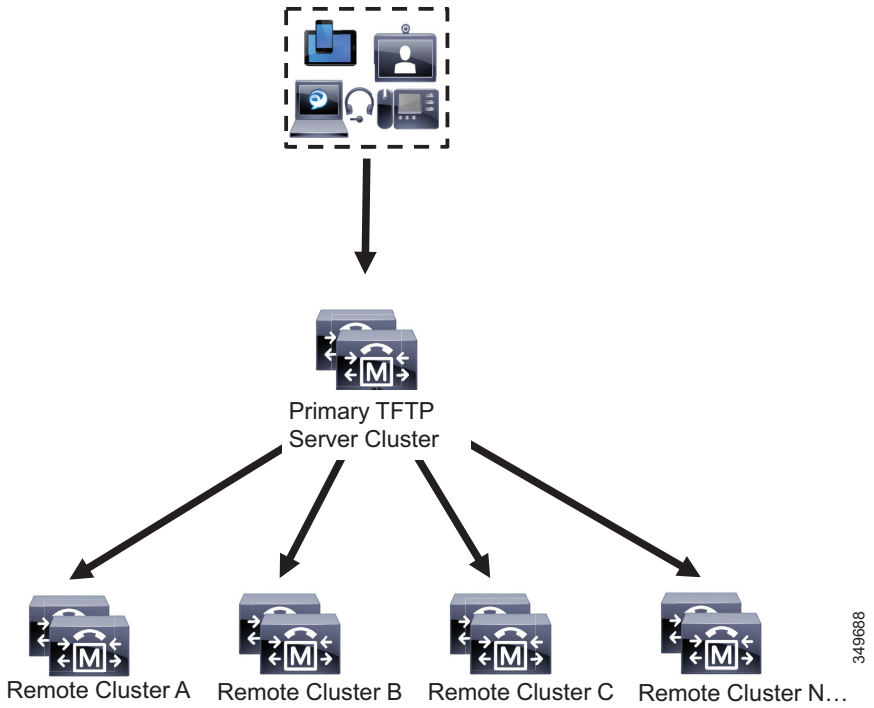


図 3-11 では、デバイス グループがプライマリ TFTP サーバに設定ファイルについて問い合わせています。デバイスから TFTP に対する要求を受信すると、プライマリ TFTP は自身のローカル キャッシュで設定ファイルを検索し、さらに、リモートで設定されている他のクラスタ（この例の Remote Cluster A、B、C、N など、設定されている他のリモート クラスタ）を調べます。

プライマリ TFTP サーバでは任意の数のリモート クラスタを設定可能ですが、各リモート クラスタには最大 3 つの TFTP IP アドレスのみを含めることができます。冗長性の推奨設計では、クラスタごとに 2 つの TFTP サーバを配置し、冗長性用のプライマリ TFTP サーバでリモート クラスタごとに 2 つの IP アドレスを設定します。

ネットワーク タイム プロトコル（NTP）

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

Unified CM での NTP 時刻同期

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

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

Windows Time Services を NTP サーバとして使用することは推奨できず、サポート対象にもなっていません。Windows Time Services では、多くの場合、簡易ネットワーク タイム プロトコル（SNTP）が使用されますが、Cisco Unified CM は SNTP と正常に同期できないからです。

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

Cisco IOS および CatOS での NTP 時刻同期

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

WAN インフラストラクチャ

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

- WAN の設計と設定（3-36 ページ）
- WAN の Quality of Service（QoS）（3-39 ページ）
- 帯域幅のプロビジョニング（3-56 ページ）

帯域幅管理の詳細については、帯域幅管理（13-1 ページ）の章を参照してください。

WAN の設計と設定

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

配置上の考慮事項

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

集中型および分散型マルチサイト配置モデルや、これらの配置モデルに対するマルチプロトコル ラベル スイッチング（MPLS）の影響に関する詳細については、コラボレーションの配置モデル（10-1 ページ）の章を参照してください。

可能であれば、WAN リンクを冗長にして、より高いレベルの耐障害性を実現する必要があります。冗長な WAN リンクを、別のサービス プロバイダーから入手するか、またはネットワーク内の物理的に異なる入力/出力点に配置すると、単一のリンクに障害が発生してもバックアップの帯域幅および接続性を利用できることが保証されます。障害のないシナリオでは、この冗長リンクを使用して、追加の帯域幅を利用し、WAN 内の複数のパスと機器を介してフローごとにトラフィックのロード バランシングを行うことができます。

音声、ビデオ、およびデータは、LAN で収束する場合とまったく同じように、WAN でも収束したままにしておく必要があります。一般的に、QoS プロビジョニングとキューイング メカニズムは、同じ WAN リンク上で音声、ビデオ、データを相互運用できるようにするために、WAN 環境で使用されます。音声、ビデオ、データを分離して別々のリンクで転送すると、多くの場合、問題が生じる可能性があります。これは、あるリンクで障害が発生すると、一般に、すべてのトラフィックが 1 つのリンクに集中するからです。その結果、トラフィックの各タイプでスループットが減少し、ほとんどの場合において音声品質が低下します。さらに、ネットワーク リンクまたはデバイスを別々に保守すると、最善を尽くしても、トラブルシューティングや管理が困難になります。

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

WAN 環境に音声を配置する場合は、WAN リンクを通過するすべての音声コールに対して低帯域幅の G.729 コーデックを使用すると、このような低速リンクでは帯域幅が節約されるので、帯域幅消費を低減することができます。さらに、可能な場合は、マルチキャスト トランスポート メカニズムを使用するように、MoH などのメディア リソースを設定することも可能です。この方法によって、さらに帯域幅が節約されます。

IP 音声ネットワークの遅延

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

保証帯域幅

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

- 専用回線
- フレーム リレー
- 非同期転送モード（ATM）
- ATM/フレームリレーのサービス インターワーキング
- マルチプロトコル ラベル スイッチング（MPLS）
- Cisco 音声およびビデオ対応 IP Security VPN（IPSec V3PN）

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

Dynamic Multipoint VPN（DMVPN）

スポークツースポーク DMVPN ネットワークは、ハブアンドスポーク トポロジと比較して、Cisco Unified Communications に対する利点を提供できます。スポークツースポーク トンネルは、WAN のホップ数と復号化/暗号化段階を削減することで、エンドツーエンドの遅延の低減をもたらします。また、DMVPN は、関連した管理および操作上のオーバーヘッドなしで、ポイントツーポイント トンネルのフル メッシュと同等の簡素化された設定方法を提供します。スポークツースポーク トンネルの使用はハブのトラフィックも削減し、その結果、帯域幅とルータ処理キャパシティを節約できます。ただし、スポークツースポーク DMVPN ネットワークは、スポークハブスポーク パスからスポークツースポーク パスへの RTP パケット ルーティングの転送時に発生する遅延変動（ジッタ）の影響を受けやすくなっています。この DMVPN パス転送時の遅延における変動は、コールの非常に早い段階で発生し、通常は気が付きません。ただし、遅延の差が 100 ms を超える場合、単一の瞬間的なオーディオのひずみが聞こえる場合があります。

集中型呼処理を使用したマルチサイト DMVPN WAN の導入に関する詳細については、https://www.cisco.com/go/designzone で入手可能な『*Cisco Unified Communications Voice over Spoke-to-Spoke DMVPN Test Results and Recommendations*』を参照してください。

ベストエフォート型の帯域幅

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

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

- インターネット
- DSL
- ケーブル
- 衛星
- ワイヤレス

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

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

（注）　アップストリームおよびダウンストリームの QoS メカニズムが、ワイヤレス ネットワークにおいてサポートされるようになりました。Voice over Wireless LAN の QoS の詳細については、https://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_wireless_uc.html で入手可能な『*Voice over Wireless LAN Design Guide*』を参照してください。

WAN の Quality of Service（QoS）

エンタープライズ WAN および VPN を介した QoS のケースについてはほぼ自明です。多くの場合、これらのリンクは、それらが接続している（ギガビットまたは 10 ギガビット イーサネットの）キャンパスまたはブランチ LAN リンクよりも桁違いに低速であるためです。そのため、これらの WAN および VPN エッジは通常、ネットワークのボトルネックであり、QoS 設計において最も注意を払う必要があります。

WAN/VPN QoS 設計には、戦略的 QoS 設計における次の 2 つの主要原則が該当します。

- 輻輳の可能性があるあらゆるノードでキューイング ポリシーを有効にする。これは、一般的に、WAN/VPN エッジごとに包括的なキューイング ポリシーを適用することと同等です。
- ネットワーク攻撃を緩和および抑制するために、（この機能をサポートしているプラットフォームで）コントロール プレーン ポリシングを有効にし、さらにデータ プレーン ポリシング（スカベンジャ クラス QoS）も有効にして、コントロール プレーンとデータ プレーンを保護する。

これを実現するために、この設計に関する項では、ワイド エリア ネットワーク全体で QoS を有効するベストプラクティスの推奨事項について説明します。ただし、この項の推奨事項は単独で完結しているわけではなく、すでに実装されている、LAN の Quality of Service（QoS）（3-15 ページ）の項に記載されているキャンパス QoS 設計の推奨事項に応じて異なるので注意してください。したがって、WAN を通過するトラフィックは、レイヤ 3 DSCP として正しく分類されマークされている（および必要に応じて、アクセス エッジでポリシングされている）と想定できます。

さらに、この設計に関する項では、ワイド エリア ネットワークに関する基本的な考慮事項についても説明します。WAN の戦略的 QoS 設計を行うには、その前に、以下に記載されている WAN 固有の考慮事項を検討する必要があります。コラボレーション ソリューションでの帯域幅管理の詳細については、帯域幅管理（13-1 ページ）の章を参照してください。

WAN QoS 設計上の考慮事項

WAN および VPN QoS 設計における考慮事項は以下のとおりです。

これらの WAN QoS 設計のそれぞれの考慮事項については、以降の項で説明します。

WAN アグリゲーション ルータ プラットフォーム

ワイド エリアにエンタープライズ キャンパス ネットワークを拡張して、他のキャンパスやブランチ ネットワークと相互接続するには、通常、2 種類のルータ（WAN アグリゲーション ルータとブランチ ルータ）を配置する必要があります。WAN アグリゲーション ルータは大規模キャンパス ネットワークを WAN/VPN に接続するために使用され、一方、ブランチ ルータは小規模ブランチ LAN を WAN/VPN に接続するために使用されます。

ハードウェアとソフトウェアの QoS

キャンパス内で使用され、ハードウェアでのみ QoS を実行する Cisco Catalyst スイッチとは異なり、シスコのルータは Cisco IOS ソフトウェアで QoS 操作を実行します。ただし、一部のプラットフォーム（Cisco Catalyst 6500 シリーズ、7600 シリーズ、Cisco ASR など）では、ソフトウェアとハードウェアのハイブリッド混合で QoS が実行されます。

Cisco IOS ソフトウェアで QoS を実行すると、次のような利点が得られます。

- プラットフォーム間での QoS 機能の一貫性

  たとえば、プラットフォームごとまたはラインカードごと（Cisco Catalyst スイッチの場合など）にハードウェア固有のキュー構造を持つのではなく、標準ソフトウェア キューイング機能（低遅延キューイング（LLQ）やクラスベース加重均等化キューイング（CBWFQ）など）を WAN およびブランチ ルータ プラットフォームで使用できます。

- 一貫性がある QoS 設定構文

  Cisco IOS QoS の設定構文であるモジュラ QoS コマンドライン インターフェイス（MQC）構文は、ごく少数の例外を除き、これらの WAN およびブランチ ルータ プラットフォーム全体で同一です。

- より多くの QoS 機能

  Network Based Application Recognition（NBAR）や階層型 QoS（HQoS）などの多くの Cisco IOS QoS 機能は、ほとんどの Catalyst ハードウェア プラットフォームで使用できません。

遅延とジッター

一部のリアルタイム アプリケーションでは遅延バジェットが固定されています。たとえば、ITU G.114 仕様では、リアルタイムの音声/ビデオ会話の一方向遅延の目標が 150 ミリ秒に設定されています。このような目標を達成するには、管理者がネットワーク遅延のコンポーネントを理解し、ネットワークと QoS の設計によって制御できる要因と制御できない要因を把握していることが大切です。ネットワーク遅延は、次のように固定コンポーネントと可変コンポーネントに分けることができます。

- シリアル化（固定）
- 伝搬（固定）
- キューイング（可変）

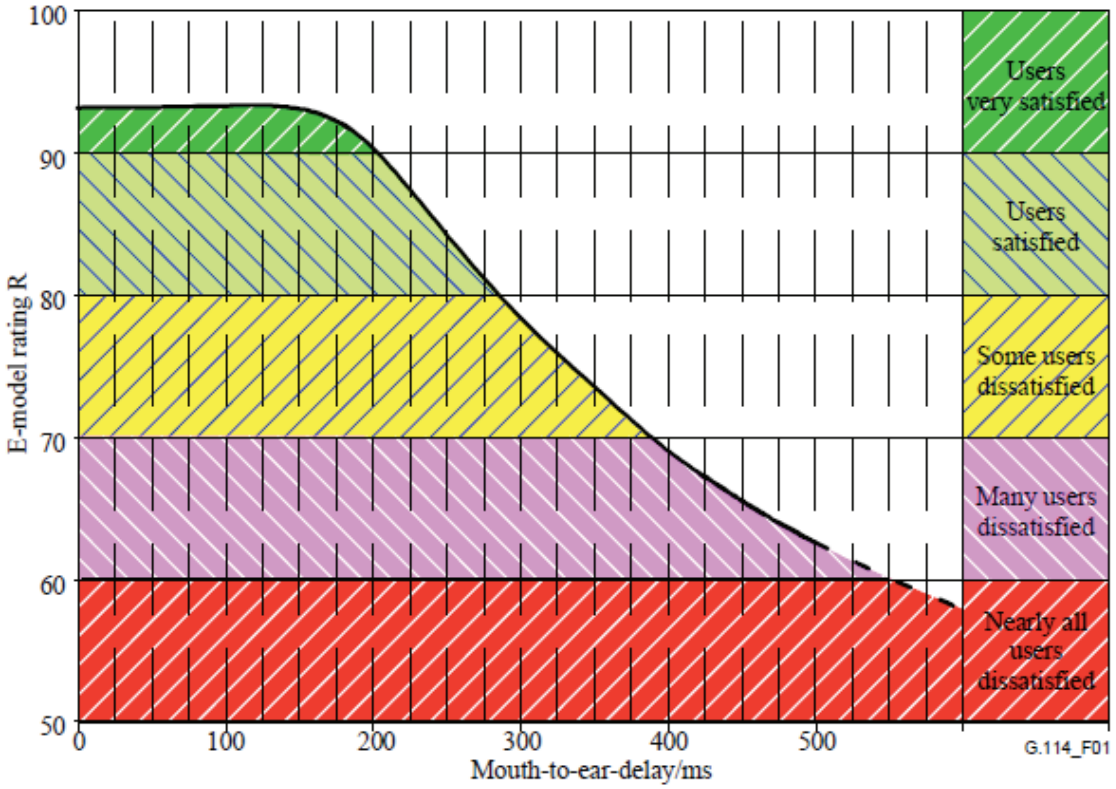
シリアル化は、伝送メディアに向けてレイヤ 2 フレームをレイヤ 1 電気パルスまたは光パルスに変換するのに要する時間を示します。したがって、シリアル化遅延は固定されており、回線レート（つまり、リンクのクロック速度）と相関しています。たとえば、（1.544 Mbps）T1 回線では、1,500 バイトのイーサネット フレームを有線用にシリアル化するのに約 8 ミリ秒かかりますが、（9.953 Gbps）OC-192/STM-64 回線では、同じフレームをシリアル化するのに 1.2 マイクロ秒しかかかりません。

通常、WAN を介した遅延目標を達成する上で最も重要なネットワーク要素は、伝搬遅延です。伝搬遅延がネットワーク遅延時間バジェットの 95 % 以上を占めることもあります。伝搬遅延は固定コンポーネントであり、発信側エンドポイントと受信側エンドポイント間で信号が移動する物理的距離と相関しています。伝搬遅延のゲーティング要素は光の速度であり、これは、真空状態で 300,000 km/秒（186,000 マイル/秒）になります。ただし、光ファイバにおける光の速度は、真空での光の速度の約 3 分の 1 になります。したがって、ほとんどのファイバ回線の伝搬遅延は 1 km あたり約 6.3 マイクロ秒（1 マイルあたり 8.2 マイクロ秒）です。

伝播遅延の計算で留意すべきもう 1 つの点は、光ファイバは物理的に、必ずしも 2 地点間の最短パスに敷設されるわけではないということです。これは、特に大洋横断リンクの場合に該当します。敷設の便宜上、回線は理論上必要な長さよりも数百マイル長くなり、場合によっては数千マイルも長くなることがあります。

それでもなお、G.114 リアルタイム通信ネットワークの遅延バジェット 150 ms は、約 24,000 km（15,000 マイル）相当の伝搬遅延に対応可能です（これは地球の円周の約 60 % になります）。理論上の最悪のシナリオ（地球の円周のちょうど半分）でも、126 ms の遅延しか必要ありません。したがって、伝送パスが比較的まっすぐな場合、この遅延目標は通常、ほぼあらゆる 2 地点で（地上パスを経由して）達成可能です。しかし、状況によっては、関係する距離とそれぞれの伝送パスの直線性が原因で、この目標を達成できないことがあります。そのような状況で、関係する距離が原因で G.114 150 ms の一方向遅延目標を達成できない場合、管理者は、ITU およびシスコ テクニカル マーケティングによる指摘に注意を払う必要があります。つまり、リアルタイムの音声品質と絶対遅延に関する ITU G.114 グラフ（図 3-12 に再現）に示されているように、一方向遅延が 200 ms を超えるまでリアルタイムの通信品質は大幅に低下しません。

図 3-12　　リアルタイムの音声品質と遅延に関する ITU G.114 グラフ



Source: *ITU-T Recommendation G.114* (05/2003), available at http://www.itu.int/rec/T-REC-G.114-200305-I/en

348825

（注） これまでは、地上パス経由の WAN 回線に重点を置いて説明してきました。衛星回線の場合、予測される遅延は 250 ～ 900 ミリ秒になります。たとえば、静止衛星でリレーされる信号は、（赤道から）海抜35,786 km（22,236 マイル）の高度に送信して宇宙に送り出し、再度地球に送り返す必要があります。光や無線波の速度の増加については対処できないので、このようなシナリオでは、遅延を低減するために管理者にできることは何もありません。このようなシナリオで遅延の影響に対処するために実行できることは、現実的なパフォーマンス予測を設定できるように、利用者を教育することです。

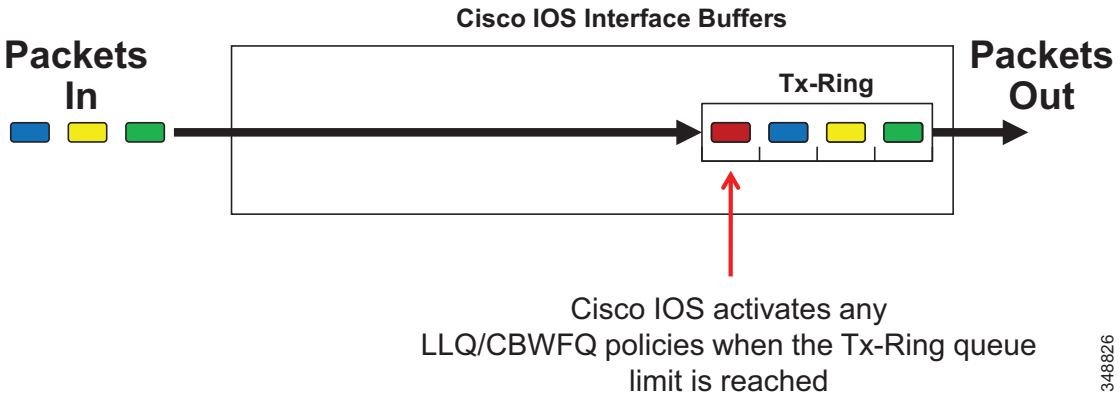
最後に考慮すべきネットワーク遅延のコンポーネントは、可変的なキューイング遅延です（可変遅延はジッターとも呼ばれます）。キューイング遅延は、ネットワーク ノードでの輻輳の有無と相関しており、遅延が発生している場合は、輻輳イベントの解決に適用されたスケジューリング ポリシーとも関連します。使い尽くされる前にパケットをデジッタ バッファで受信する必要があるため、リアルタイム アプリケーションは遅延よりもジッターに敏感です。デジッタ バッファで許可されている時間内にパケットが受信されなかった場合、そのパケットは実質的に失われ、全体的な音声またはビデオ コールの品質に影響を与える可能性があります。

ネットワーク遅延につながる要因の大部分が固定的な場合は、キューイング遅延に注意する必要があります。キューイング遅延は、キューイング ポリシーを介してネットワーク管理者が直接制御できる唯一の遅延要因であるからです。したがって、TX リングと LLQ/CBWFQ の運用を含めて、Cisco IOS キューイング システムを詳しく検討することは、管理者がこれらの重要なネットワーク ポリシーを最適化する上で役立ちます。

TX リング

TX リングは WAN インターフェイスの最終的な Cisco IOS 出力バッファ（比較的小さな FIFO キュー）であり、ルータ上の発信パケットのレートを物理インターフェイスのレートに一致させることによって、物理リンクの帯域幅利用を最大化します。図 3-13 は TX リングを示しています。

図 3-13　Cisco IOS の TX リングの動作



また、TX リングは、Cisco IOS ソフトウェアにインターフェイスの輻輳を示すのに役立ちます。インターフェイスの輻輳が発生する前に、パケットは TX リングを介して FIFO 方式でインターフェイスに送信されます。ただし、TX リングのキューが満杯になると、TX リングは Cisco IOS ソフトウェアに信号を送信して、インターフェイスに関連付けられている LLQ または CBWFQ ポリシーを使用するように求めます。後続のパケットは LLQ および CBWFQ ポリシーに従って Cisco IOS 内のキューに格納され、キューから TX リングへと取り出されて、FIFO 方式でインターフェイスから送信されます。

TX リングは、特定のプラットフォームで **tx-ring-limit** インターフェイス設定コマンドを使用して設定できます。TX リングのデフォルト値は、プラットフォーム、リンク タイプ、および速度に応じて異なります。詳細については、『*Understanding and Tuning the tx-ring-limit Value*』を参照してください。このマニュアルは次の URL から入手できます。

https://www.cisco.com/c/en/us/support/docs/asynchronous-transfer-mode-atm/ip-to-atm-class-of-service/6142-txringlimit-6142.html

TX リングのデフォルト設定の変更

シスコ テクニカル マーケティングによる設計検証では、一部のインターフェイスのデフォルトの TX リング制限によって、一部のリアルタイム アプリケーション クラス（特に、Cisco TelePresence トラフィックなどの HD ビデオ ベースのリアルタイム アプリケーション）で、やや高いジッター値が発生することが確認されています。その原因は、HD ビデオ トラフィックのバースト性です。たとえば、LLQ と CBWFQ ポリシーがアクティブになっている完全輻輳 T3 WAN リンク（Cisco PA-T3+ ポート アダプタ インターフェイスを使用）を想定してください。この場合、デフォルトの TX リングの深さは 64 パケットです。LLQ によって TelePresence トラフィックに優先順位が設定されている場合でも、送信する TelePresence パケットがないときは、デフォルトの深さ 64 パケットに達するまで FIFO TX リングに他のトラフィックが格納されます。新しい TelePresence パケットが到着すると、そのパケットは、スペースが空いたときに FIFO TX リングにデキューされます。パケットがレイヤ 3 LLQ/CBWFQ キューイング システムで優先的に扱われている場合でも同様です。ただし、デフォルト設定では、その TelePresence パケットの前に TX リング内に 63 ものパケットがある可能性があります。このような最悪のシナリオでは、これらの非リアルタイム パケットをこの（45 Mbps）T3 インターフェイスから送信するのに 17 ミリ秒かかる可能性があります。17 ミリ秒の即時かつ可変の遅延（ジッター）は、TelePresence のビデオ品質にエンドユーザの目に見えるほどの明らかな影響を与える可能性があります。ただし、このリンクの TX リングの値を小さくすると、Cisco IOS ソフトウェアは、即座にかつより頻繁に、輻輳管理ポリシーを使用するようになります。これによって、TelePresence などのリアルタイム アプリケーションの全体的なジッター値が小さくなります。

一方、TX リングの値が小さすぎると、キューイング ポリシーを使用するためにプロセッサが絶えず中断されるので、CPU 使用率が非常に高くなります。輻輳率の高さが一時的なもので、持続的ではない場合でも同様です。TX リングを調整する場合は、CPU の過剰使用を引き起こすことなく、ジッターを最小化するトレードオフ設定が必要です。

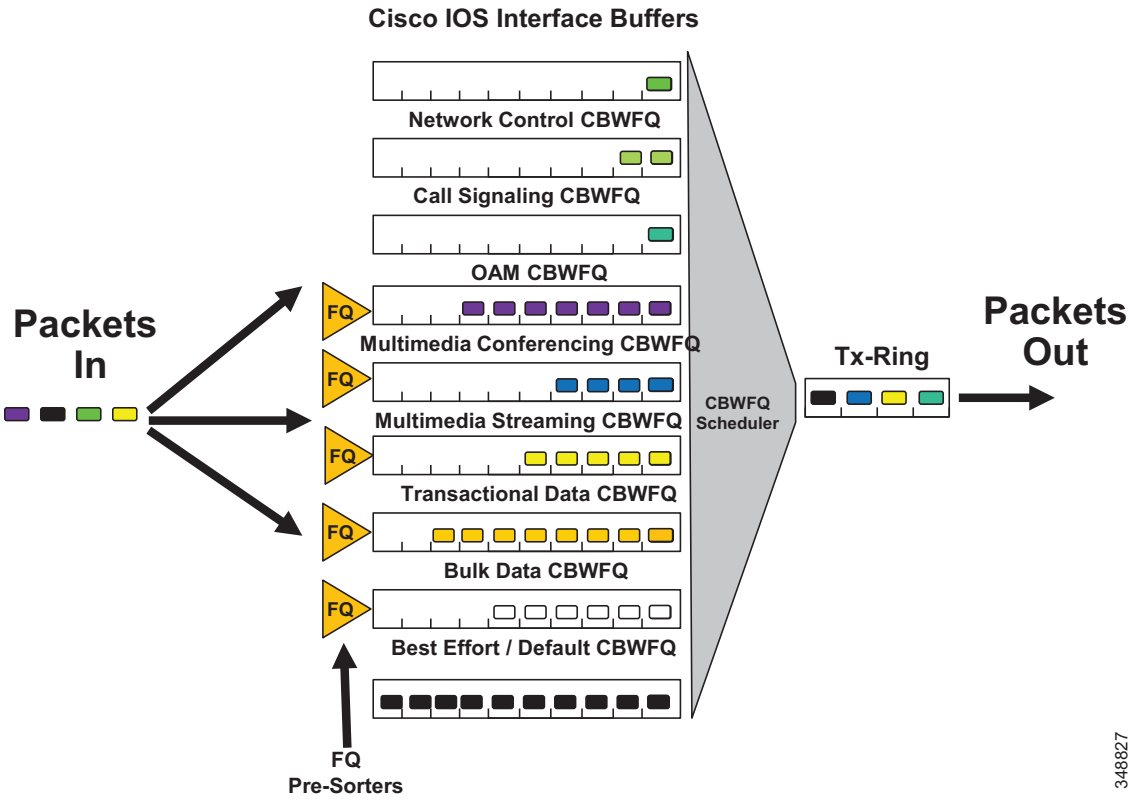
したがって、TX リングのデフォルト値を調整する場合は、リンクのタイプと速度に十分注意を払う必要があります。

クラス ベース加重均等化キューイング

クラスベース加重均等化キューイング（CBWFQ）は Cisco IOS キューイング アルゴリズムであり、帯域幅を保証する機能とトラフィック クラス内の他のフローの均等性を確保する機能とを兼ね備えています。

インターフェイスの TX リングが満杯状態（輻輳時にのみ発生）になった場合にのみ、Cisco IOS ソフトウェアは CBWFQ ポリシーを使用します（ポリシーがインターフェイスに関連付けられている場合）。輻輳の発生を示す信号がソフトウェアに送信されると、各 CBWFQ クラスにキューが割り当てられます。CBWFQ キューには均等化キューイングのプレソーターも適用されていることがあり、1 つのキューに対して競合している複数のフローが均等に処理されます。また、各 CBWFQ キューは、各クラスに割り当てられている帯域幅に基づいて、加重ラウンド ロビン（WRR）方式で処理されます。次に、CBWFQ スケジューラによって TX リングにパケットが転送されます。図 3-14 は CBWFQ の動作を示しています。

図 3-14　　Cisco IOS CBWFQ の動作



各 CBWFQ クラスは、**bandwidth** ポリシーマップ クラス コンフィギュレーション文によって帯域幅が保証されます。CBWFQ は、クラスに割り当てられている帯域幅からクラスに属するパケットのウェイトを導出します。次に、CBWFQ は WRR スケジューリングを介してこのウェイトを使用し、このクラスのキューが適正に処理されるようにします。

特定の CBWFQ クラスに割り当てられる帯域幅について重要な点は、割り当てられる帯域幅は、スタティックな帯域予約ではなく、クラス宛てのパケットがある場合にクラスに対して保証される最小帯域幅であるということです。クラス宛てのパケットがない場合、スケジューラは次のキューを処理し、未使用の帯域幅割り当てを必要に応じて動的に他のキューに再配分します。

また、**fair-queue** ポリシーマップ クラス コンフィギュレーション コマンドによって、特定の CBWFQ キューに均等化キューイング プレソーターを適用できます。機能名が示すように、このコマンドによって、フローベースの均等化キューイング プレソーターは有効化できますが、加重均等化キューイング プレソーターは有効にならないので注意してください（均等化キューイング プレソーターは、特定のクラスに送信されるパケットの IP プシデンス値を考慮しません）。たとえば、CBWFQ クラスに 1 Mbps の帯域幅が割り当てられており、このクラスに対して競合する 4 つのトラフィック フローがある場合、均等化キューイング プレソーターによって、各フローは「1/（合計フロー数）」の帯域幅を受け取ります。この例では、250 Kbps（1 Mpbs の 1/4）の帯域幅を受け取ります。

（注）　Cisco IOS リリース 12.4(20) よりも前では、class-default にのみ均等化キューイング プレソーターを適用できました。しかし、以降の Cisco IOS リリースでは、多数の QoS 機能強化の一環として階層型キューイング フレームワークのサポートが導入され、任意の CBWFQ クラスに均等化キューイング プレソーターを適用できるようになりました。HQF の詳細は、https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_hrhqf/configuration/15-mt/qos-hrhqf-15-mt-book.html に記載されています。

CBWFQ の深さはキュー制限によって定義されますが、キュー制限はリンク速度とプラットフォームに応じて異なります。このキュー制限は **queue-limit** ポリシーマップ クラス コンフィギュレーション コマンドで変更できます。CBWFQ での TelePresence トラフィックのプロビジョニング（バースト）など、状況によっては、キュー制限をデフォルト値から増加することを推奨します。これについては 加重ランダム早期検出（3-47 ページ）の項で詳しく説明します。

Cisco IOS ソフトウェアの旧バージョン（HQF 以前と 12.4(20) T 以前）に含まれている従来の機能では、LLQ/CBWFQ ポリシーが 75 % を超えるインターフェイス帯域幅をデフォルト以外のトラフィック クラスに明示的に割り当てる場合、それらのポリシーをインターフェイスに関連付けることはできません。この機能は、デフォルト クラスと制御トラフィック クラスが常に十分な帯域幅を得られるようにするための一種の安全機能であり、レイヤ 2 帯域幅オーバーヘッドのプロビジョニングを許可していました。この機能は、**max-reserved-bandwidth** インターフェイス コマンドを適用することで置き換えることができます。このコマンドは、明示的にプロビジョニングできる帯域幅の割合（通常、この値は 100 に設定される）をパラメータとして受け取ります。ただし、この安全機能を置き換える場合は、デフォルト クラスにリンク帯域幅の 25 % 以上を明示的に割り当てることを強く推奨します。

低遅延キューイング

低遅延キューイング（LLQ）は、基本的には CBWFQ に完全プライオリティ キューを組み合わせた機能です。図 3-15 は基本的な LLQ の動作を示しています。

図 3-15　Cisco IOS（シグナル）LLQ の動作

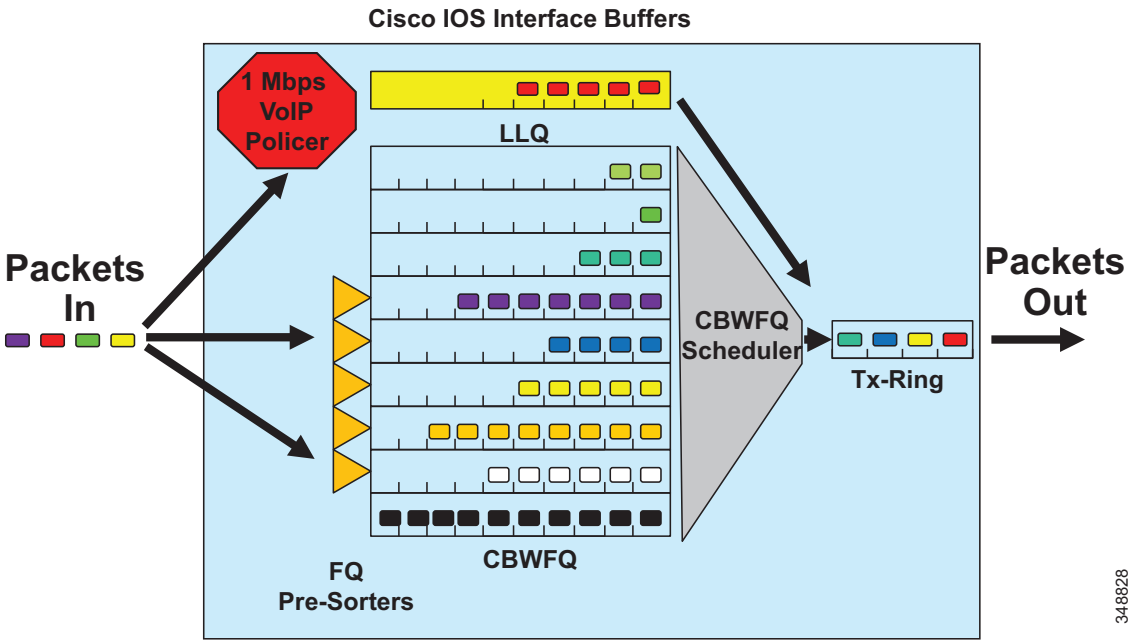


図 3-15 に示すように、LLQ は CBWFQ サブシステムに完全プライオリティ キューを追加します。LLQ に割り当てる帯域幅の量は、**priority** ポリシーマップ クラス コンフィギュレーション コマンドによって設定されます。Cisco IOS LLQ の興味深い点は、完全プライオリティ キューへのパケットを許可する暗黙的ポリサーが組み込まれていることです。この暗黙的ポリサーは、リアルタイム キューの処理で消費される帯域幅を制限して、CBWFQ スケジューラによって処理される非リアルタイム フローの帯域幅の枯渇を防ぎます。この暗黙的ポリサーのポリシング レートは、常に、完全プライオリティ キューの帯域幅割り当てと一致するように設定されます。プロビジョニングされた対応数よりも多くのトラフィックが LLQ クラスに送信された場合、超過トラフィックはポリサーによってドロップされます。LLQ/CBWFQ システムと同様、暗黙的ポリサーは輻輳の発生時（満杯状態の TX リングから Cisco IOS ソフトウェアに信号が送信された場合）にのみ有効になります。

加重ランダム早期検出

LLQ/CBWFQ などの輻輳管理機能はキューの先頭を処理し、一方、加重ランダム早期検出（WRED）などの輻輳回避機能はキューの末尾を処理します。選択的パケット廃棄によって、TCP ウィンドウ機能は「スロットルバック」し、フロー レートを管理可能なレートに調整するので、輻輳回避機能は TCP ベースのアプリケーションと最も適切に連携します。

Cisco IOS の主要な輻輳回避機能は WRED です。WRED はキューが最大容量に達するとランダムにパケットをドロップします。ただし、このランダムな選択はトラフィックの重みによって偏る可能性があります。低い IP プレシデンス（IPP）値を積極的にドロップするデフォルトの WRED と同様に、この重みは IPP 値である可能性があります（たとえば、統計的に IPP 1 は IPP 6 よりも積極的にドロップされます）。または、統計的に高い AF 廃棄優先度値を積極的にドロップする DSCP ベースの WRED と同様に、この重みは AF 廃棄優先度値である可能性があります（たとえば、AF AF43 は AF42 よりも積極的にドロップされ、AF42 は AF41 よりも積極的にドロップされます）。DSCP ベースの WRED は、**random-detect** ポリシーマップ クラス コンフィギュレーション コマンドとともに **dscp** キーワードを使用して有効にできます。図 3-16 は DSCP ベース WRED の動作を示しています。

図 3-16　Cisco IOS DSCP ベース WRED の動作

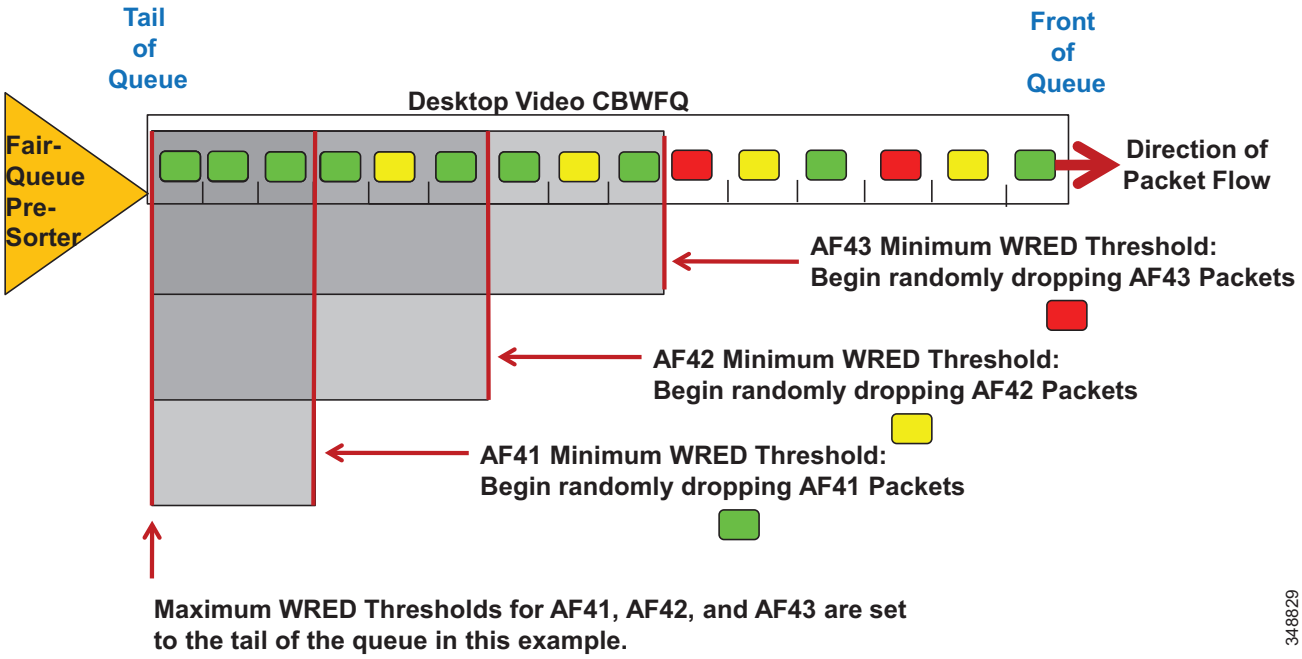


図 3-16 に示すように、特定の廃棄優先度（AF43、AF42、または AF41）がマーキングされたパケットは、キューの格納状態が廃棄優先度値の最小 WRED しきい値を超えた場合にのみドロップされ始めます。パケットは常にランダムにドロップされますが、キューの格納状態が廃棄優先度値の最小 WRED しきい値に近づくほど、ドロップされる確率が高くなります。図 3-16 に示すように、最大 WRED しきい値は通常、100 % に設定されます（キューの末尾）。ただし、このしきい値は設定可能であり、一部の上級管理者は、ニーズ、制約、および設定に応じて WRED しきい値を調整できます。

また、AF クラスの WRED しきい値を最適化できます。デフォルトでは、各 AF クラスの最小 WRED しきい値は、廃棄優先度値 3、2、1 に応じてそれぞれ 24、28、32 パケットとなります。これらのしきい値は、デフォルトのパケット キューの深さである 64 パケットの 60 %、70 %、および 80 % に相当します。また、デフォルトでは、最大 WRED しきい値は、各 AF クラスのすべての廃棄優先度値に対して 40 パケットに設定されます。デフォルトのキュー制限または深さ 64 パケットについて考えた場合、40 パケットのキューの深さを引き起こす可能性がある持続的な輻輳があるリンクでは、このデフォルト設定は不十分です（キューが 24 パケットに対応できるキャパシティを備えているにもかかわらず、その時点ですべてのコード ポイントがテールドロップされます）。そのため、管理者はこれらの WRED しきい値を調整して、各 AF クラスが廃棄優先度値 3、2、1 に応じてそれぞれ最小 WRED しきい値 40、45、50 パケットを持つようにすることができます。これらのしきい値は、デフォルトのキューの深さである 64 パケットの約 60 %、70 %、80 % に相当します。また、管理者は、各 AF クラスの各廃棄優先度値の最大 WRED しきい値をデフォルトのキューの深さ 64 パケットに調整することもできます。

設計例は 帯域幅管理（13-1 ページ）の章に記載されています。

低速リンクに関する考慮事項

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

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

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

これらの QoS メカニズムの目標は、音声トラフィックの遅延、パケット損失、およびジッタを削減することで、信頼性の高い、高品質の音声を保証することです。表 3-5 は、WAN リンク速度に基づいてこの目標を実現するために WAN インフラストラクチャで必要な QoS 機能とツールを示しています。

表 3-5　WAN テクノロジーとリンク速度ごとの Unified Communications のサポートに必要な QoS 機能とツール

WAN テクノロジー	リンク速度：56 ～ 768 kbps	リンク速度：768 kbps 以上
専用回線	• マルチリンク ポイントツーポイント プロトコル（MLP） • MLP LFI（リンク フラグメンテーション/インターリーブ） • LLQ（低遅延キューイング） • オプション：cRTP（RTP ヘッダー圧縮）	• LLQ
フレームリレー（FR）	• トラフィック シェーピング • LFI（FRF.12） • LLQ • オプション：cRTP • オプション：Voice-Adaptive Traffic Shaping（VATS） • オプション：Voice-Adaptive Fragmentation（VAF）	• トラフィック シェーピング • LLQ • オプション：VATS
非同期転送モード（ATM）	• TX-ring バッファ変更 • MLP over ATM • MLP LFI • LLQ • オプション：cRTP（MLP が必要）	• TX-ring バッファ変更 • LLQ
フレームリレーと ATM のサービス インターワーキング（SIW）	• TX-ring バッファ変更 • MLP over ATM と FR • MLP LFI • LLQ • オプション：cRTP（MLP が必要）	• TX-ring バッファ変更 • MLP over ATM と FR • LLQ
マルチプロトコル ラベル スイッチング（MPLS）	• インターフェイス テクノロジーに応じて、上記と同じ • サービス プロバイダーの仕様に従ってフローをリマークするには、通常クラスベースのマーキングが必要	• インターフェイス テクノロジーに応じて、上記と同じ • サービス プロバイダーの仕様に従ってフローをリマークするには、通常クラスベースのマーキングが必要

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

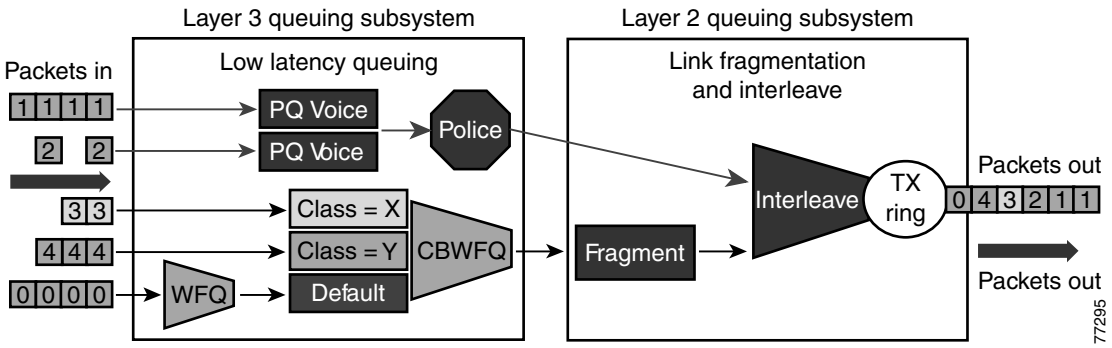
- トラフィックの優先順位（3-50 ページ）
- リンク効率化手法（3-51 ページ）
- トラフィック シェーピング（3-53 ページ）

トラフィックの優先順位

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

図 3-17 は、優先付け体系の例を示しています。

図 3-17　　WAN を介した VoIP 用の最適化キューイング



LLQ には、次の優先付けの基準を使用することを推奨します。

- *音声*がプライオリティ キューに格納される基準は、DSCP 値 46（EF）です。
- *ビデオ会議*トラフィックがプライオリティ キューに格納される基準は、DSCP 値 34（AF41）です。ビデオ トラフィックのパケット サイズが大きいと、768 Kbps 以下のリンク速度ではビデオのフラグメント化が必要になります。これは、ビデオが個別の CBWFQ に格納されている場合にのみ発生します。プライオリティ キュー（PQ）内のビデオはフラグメント化されません。
- WAN リンクが輻輳すると、*音声制御シグナリング* プロトコルが停止する可能性があります。したがって、IP Phone が IP WAN を介してコールできなくなります。そのため、音声制御プロトコル（たとえば、H.323、MGCP、および Skinny Client Control Protocol（SCCP））には、独自のクラスベース WFQ が必要です。このキューに格納される基準は、DSCP 値 24（CS3）です。
- 場合によっては、特定のデータ トラフィックで、ベストエフォート型よりも優れた処理が必要になることがあります。このトラフィックは、*ミッションクリティカル データ*と呼ばれ、必要な帯域幅を持つ 1 つ以上のキューに入ります。このクラス内のキューイング方式は、最小帯域幅が割り当てられたファーストインファーストアウト（FIFO）です。このクラスのトラフィックは、設定された帯域幅限界を超えると、デフォルト キューに入れられます。このキューへの入力基準は、伝送制御プロトコル（TCP）ポート番号、レイヤ 3 アドレス、または DSCP/PHB 値にすることができます。
- 残りの企業トラフィックはすべて、ベストエフォート型処理のデフォルト キューに入れることができます。キーワード **fair** を指定すると、キューイング アルゴリズムは WFQ になります。

Scavenger Class

Scavenger Class は、特定のアプリケーションに対してベストエフォート未満のサービスを提供することを目的としています。このクラスに割り当てられるアプリケーションは、企業の組織的目標にはほとんど、またはまったく貢献せず、本質的にエンターテイメント指向であることが一般的です。Scavenger トラフィックを最小帯域幅キューに割り当てることにより、輻輳期間中はこのトラフィックが抑制されて事実上発生しなかったことにされますが、オフピーク時に発生するなどで帯域幅が業務目的で使用されていない場合には、このトラフィックが使用可能になります。

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

リンク効率化手法

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

Compressed Real-Time Transport Protocol（cRTP）

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

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

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

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

cRTP 圧縮は、パケットが出力インターフェイスを通過する前、つまり、LLQ クラスベース キューイングが行われた後の最終段階として行われます。Cisco IOS Release 12.(2)2T からは、cRTP により、*音声* クラスの帯域幅を圧縮パケット値に基づいて設定できる LLQ クラスベース キューイング メカニズムへのフィードバック メカニズムを使用できるようになりました。12.(2)2T よりも前の Cisco IOS リリースでは、このメカニズムは使用されていないため、LLQ は圧縮帯域幅を認識しません。したがって、圧縮が行われないものとして *音声* クラスの帯域幅をプロビジョニングする必要があります。表 3-6 は、512 Kbps リンクで G.729 コーデックを使用して 10 コールに対応する場合の、*音声* クラスの帯域幅の設定における違いの例を示しています。

表 3-6 では、cRTP 以外の G.729 コールの場合が 24 Kbps で、cRTP の G.729 コールの場合が 10 Kbps であることを前提としていることに注意してください。これらの帯域幅の数値は、音声ペイロードと IP/UDP/RTP ヘッダーだけに基づいています。レイヤ 2 ヘッダーの帯域幅は考慮に入れていません。ただし、実際の帯域幅プロビジョニングでは、レイヤ 2 ヘッダーの帯域幅も、WAN リンクで使用されたタイプに基づいて考慮に入れられます。

表 3-6　512 Kbps リンク帯域幅と G.729 コーデックを使用する 10 件のコールに対応する場合の LLQ 音声クラスの帯域幅要件

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

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

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

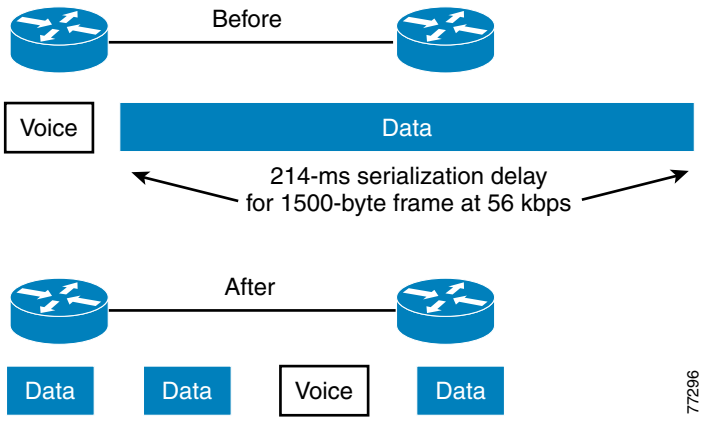
音声およびビデオに対応した IPSec VPN（V3PN）で cRTP を使用する場合の追加の推奨事項については、次の Web サイトで入手可能な V3PN 資料を参照してください。

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

リンク フラグメンテーション/インターリーブ（LFI）

低速リンク（768 Kbps 未満）の場合、許容できる音声品質を確保するには、LFI メカニズムを使用する必要があります。この手法は、図 3-18 に示されているように、大きなデータ フレームの背後で、音声トラフィックが遅延しないようにして、ジッタを制限します。この目的のための 2 つの手法は、マルチリンク ポイントツーポイント プロトコル（MLP）LFI（専用回線、ATM、および SIW 用）と、フレームリレー用の FRF.12 です。

図 3-18　リンク フラグメンテーション/インターリーブ（LFI）



Voice-Adaptive Fragmentation（VAF）

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

VAF は、一般に、Voice-Adaptive Traffic Shaping と組み合わせて使用されます（Voice-Adaptive Traffic Shaping（VATS）（3-55 ページ）を参照）。VAF はオプションの LFI ツールです。VAF を有効にする場合は注意が必要です。これは、音声アクティビティが検出されるタイミングと LFI メカニズムが連動するタイミングの間に多少の遅延が生じるためです。また、最後の音声パケットが検出されてから、VAF が非アクティブになるまでの間に、設定可能な非アクティブ化タイマー（デフォルトは 30 秒）が期限切れになる必要があります。そのため、この期間は LFI が不必要に発生します。VAF は、Cisco IOS Release 12.2(15)T 以降で使用できます。

トラフィック シェーピング

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

図 3-19 は、同一 IP WAN 上での音声とデータの転送時にトラフィック シェーピングが必要な主な理由を示しています。

図 3-19　　フレームリレーと ATM を使用したトラフィック シェーピング

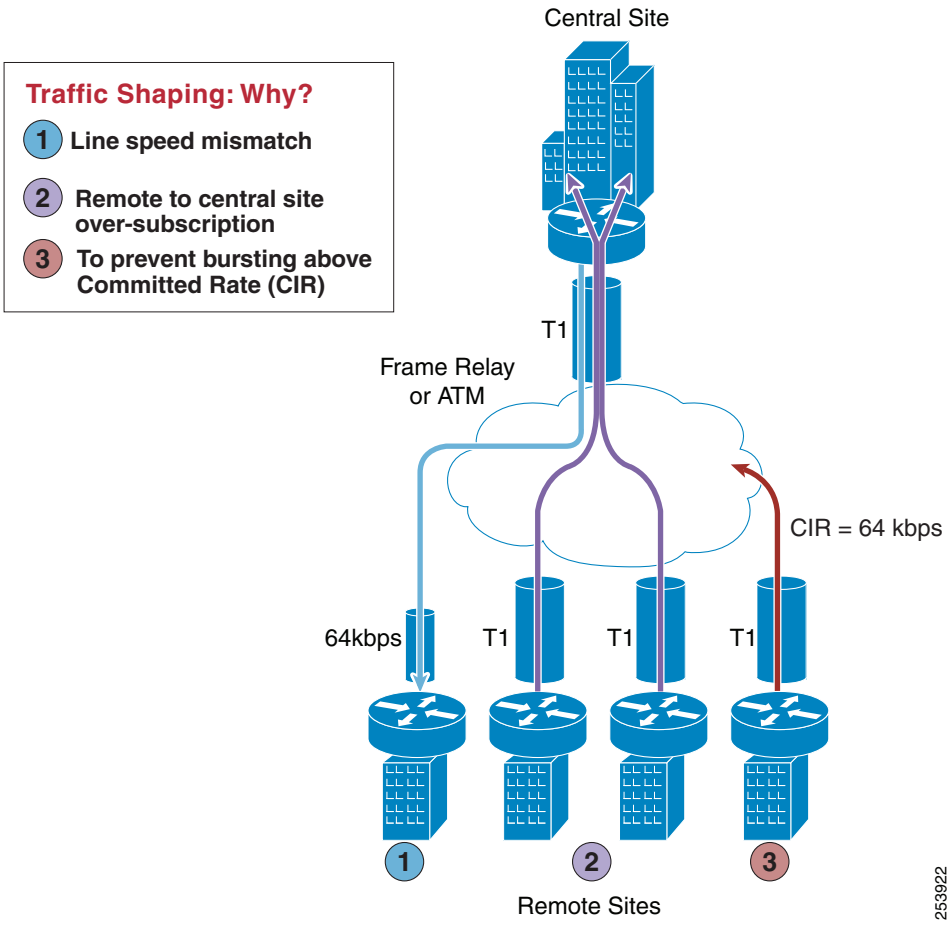


図 3-19 は、次の 3 つのシナリオを示しています。

1. 回線速度のミスマッチ

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

2. 中央サイトとリモート サイト間のリンクのオーバーサブスクリプション

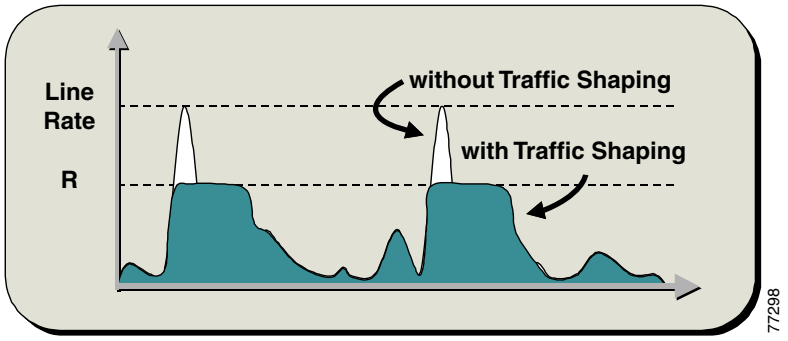
   複数のリモート サイトを 1 つの中央サイトに集約する場合、帯域幅をオーバーサブスクリプションにするのは、フレームリレーまたは ATM ネットワークでは一般的な方法です。たとえば、T1 インターフェイスで WAN に接続するリモート サイトが複数あるにもかかわらず、中央サイトには 1 つの T1 インターフェイスしかない場合があります。この設定により、配置されたネットワークは統計多重化による恩恵を受けますが、中央サイトのルータ インターフェイスが、トラフィックのバースト時に輻輳し、音声品質が低下することがあります。

3. 認定情報レート（CIR）を超えたバースト

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

トラフィック シェーピングは、インターフェイスから送出されるトラフィックを、回線レート未満のレートに制限して、WAN の両端で輻輳が起きないようにし、こうした問題を解決します。図 3-20 は、このメカニズムの一般的な例を説明しています。ここで、R は、トラフィック シェーピングが適用される場合のレートです。

図 3-20　　トラフィック シェーピングのメカニズム



Voice-Adaptive Traffic Shaping（VATS）

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

VATS を Voice-Adaptive Fragmentation（VAF）と組み合わせて使用する場合（リンク フラグメンテーション/インターリーブ（LFI）（3-52 ページ）を参照）、インターフェイス上で音声アクティビティが検出されたときは、音声以外のトラフィックはすべてフラグメント化され、トラフィックはすべて WAN リンクの CIR に合せてシェーピングされます。

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

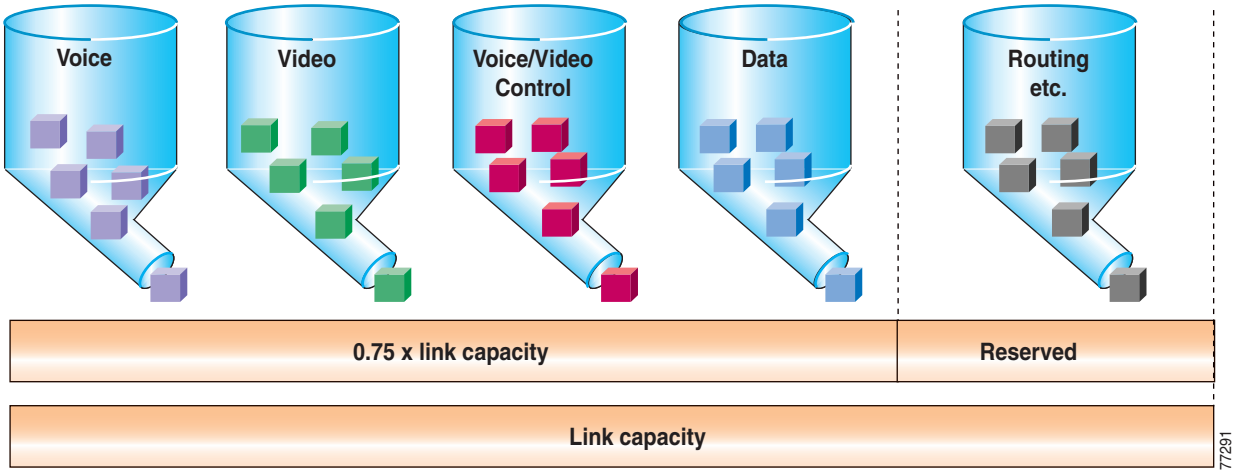
Voice-Adaptive Traffic Shaping 機能とフラグメンテーション機能の詳細、およびそれらの設定方法については、次の Web サイトで入手可能なドキュメントを参照してください。

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/wan_frly/configuration/15-mt/wan-frly-15-mt-book.html

帯域幅のプロビジョニング

成功する IP ネットワークを設計する主要部分は、ネットワーク帯域幅の適切なプロビジョニングです。主要なアプリケーション（たとえば、音声、映像、およびデータ）ごとの帯域幅必要量を加算すると、必要な帯域幅を計算できます。この合計値は、任意のリンクの最小帯域幅必要量を表します。この値は、そのリンクに使用可能な合計帯域幅の約 75 % 以下でなければなりません。この 75 % ルールは、ルーティングやレイヤ 2 キープアライブなどのオーバーヘッド トラフィックに、いくらかの帯域幅が必要であることを前提としています。図 3-21 は、こうした帯域幅のプロビジョニング プロセスを示しています。

図 3-21　　リンクの帯域幅プロビジョニング



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

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

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

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

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

- すべてのマルチサイト WAN 配置における音声およびビデオ ベアラ トラフィック（ベアラ トラフィック用のプロビジョニング（3-57 ページ）を参照）
- 集中型呼処理を使用するマルチサイト WAN 配置における呼制御トラフィック（集中型コール処理による呼制御トラフィック用のプロビジョニング（3-61 ページ）を参照）
- 分散型呼処理を使用するマルチサイト WAN 配置における呼制御トラフィック（分散型呼処理による呼制御トラフィック用のプロビジョニング（3-65 ページ）を参照）

ベアラ トラフィック用のプロビジョニング

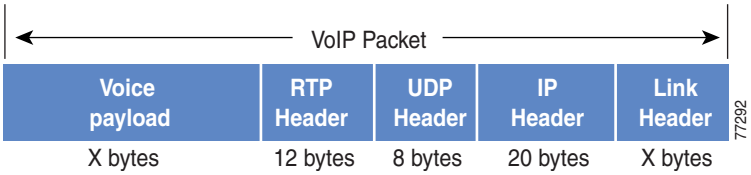
この項では、次のトラフィック タイプの帯域幅プロビジョニングについて説明します。

- 音声ベアラ トラフィック（3-58 ページ）
- ビデオ ベアラ トラフィック（3-60 ページ）

音声ベアラ トラフィック

図 3-22 に示されているように、VoIP（Voice-over-IP）パケットは、音声ペイロード、IP ヘッダー、ユーザ データグラム プロトコル（UDP）ヘッダー、Real-Time Transport Protocol（RTP）ヘッダー、およびレイヤ 2 リンク ヘッダーから構成されています。Secure Real-Time Transport Protocol（SRTP）暗号化を使用すると、各パケットの音声ペイロードは 4 バイト増加します。リンク ヘッダーの大きさは、使用されるレイヤ 2 メディアによって異なります。

図 3-22　　一般的な VoIP パケット



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

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

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

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

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

表 3-7 は、VoIP フローあたりのレイヤ 3 帯域幅を詳しく記述しています。表 3-7 は、音声ペイロードと IP ヘッダーだけによって消費される帯域幅を示しています。ここでは、パケット レートとして、デフォルトのパケット レートである 50 パケット/秒（pps）と、暗号化されていないペイロードと暗号化されたペイロードの両方のレートである 33.3 pps を使用しています。表 3-7 には、レイヤ 2 ヘッダーのオーバーヘッドは含まれていません。また、RTP ヘッダー圧縮（cRTP）などの可能な圧縮方式を考慮していません。Unified CM Administration の Service Parameters メニューを使用すると、コーデック サンプリング レートを調整できます。

表 3-7　　音声ペイロードと IP ヘッダーのみの帯域幅使用量

コーデック	サンプリング レート	音声ペイロード（バイト数）	1 秒あたりのパケット数	1 会話あたりの帯域幅
G.711 および G.722-64k	20 ms	160	50.0	80.0 kbps
G.711 および G.722-64k（SRTP）	20 ms	164	50.0	81.6 kbps
G.711 および G.722-64k	30 ms	240	33.3	74.7 kbps
G.711 および G.722-64k（SRTP）	30 ms	244	33.3	75.8 kbps
iLBC	20 ms	38	50.0	31.2 kbps
iLBC（SRTP）	20 ms	54	50.0	32.8 kbps
iLBC	30 ms	50	33.3	24.0 kbps

表 3-7　音声ペイロードと IP ヘッダーのみの帯域幅使用量（続き）

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

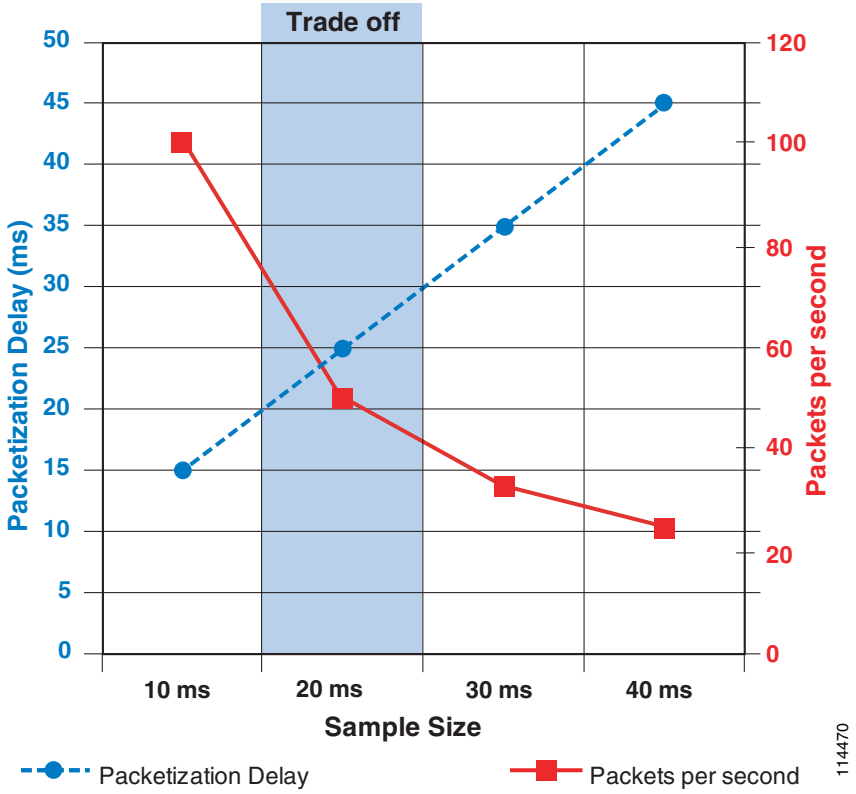
より正確な方法でプロビジョニングするには、帯域幅の計算にレイヤ 2 ヘッダーを含めます。表 3-8 は、レイヤ 2 ヘッダーを計算に含めたときの、音声トラフィックによって消費される帯域幅の量を示しています。

表 3-8　レイヤ 2 ヘッダーを含めた帯域幅使用量

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

30 ms を超えるサンプリング レートを設定することは可能ですが、これを行うと、通常、音声品質が非常に低下します。図 3-23 に示されているように、サンプリング サイズが増加すると、1 秒あたりのパケット数が減少するため、デバイスの CPU に与える影響は小さくなります。同様に、サンプル サイズが増加すると、1 パケットあたりのペイロードが大きくなるため、IP ヘッダーのオーバーヘッドが低下します。ただし、サンプル サイズが増加すると、パケット化の遅延も増加するため、音声トラフィックのエンドツーエンドの遅延が増加します。サンプル サイズを設定する場合は、パケット化の遅延と 1 秒あたりのパケット数とのトレードオフを考慮する必要があります。このトレードオフが 20 ms で最適化されている場合、30 ms のサンプル サイズでも、1 秒あたりのパケット数に対する遅延の比率は妥当なものになります。しかし、40 ms のサンプル サイズでは、パケット化の遅延が大きくなりすぎます。

図 3-23　　音声のサンプル サイズ:1 秒あたりのパケット数とパケット化の遅延との比較



ビデオ ベアラ トラフィック

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

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

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

呼制御トラフィック用のプロビジョニング

Unified Communications エンドポイントが WAN によって呼制御アプリケーションと分けられている場合、または相互接続された 2 つの Unified Communications システムが WAN によって分けられている場合、これらのエンドポイント間やシステム間の呼制御およびシグナリング トラフィック用にプロビジョニングする必要がある帯域幅の量について、考慮が必要です。ここでは、集中型または分散型の呼処理モデルが配置されている場合の、コール シグナリング トラフィック用の WAN 帯域幅プロビジョニングについて説明します。Unified Communications の集中型および分散型の呼処理配置モデルについては、コラボレーションの配置モデル（10-1 ページ）を参照してください。

集中型コール処理による呼制御トラフィック用のプロビジョニング

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

この配置モデルには、次の考慮事項が適用されます。

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

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

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

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

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

（注） この平均数が、特定の配置のニーズを満たさない場合、拡張公式（3-63 ページ）に記載されている拡張公式を使用して、推奨帯域幅を計算できます。

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

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

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

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

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

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

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

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

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

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

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

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

Cisco IOS ルータ上のキューに割り当てることができる最小帯域幅が 8 Kbps であるという事実を考慮すると、支店のさまざまな規模に対する最小帯域幅と推奨帯域幅の値を、表 3-9 のようにまとめることができます。

表 3-9　呼制御トラフィック用の推奨レイヤ 3 帯域幅（シグナリングの暗号化の有無別）

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

表 3-9 の値は、より多くの機能を備えた SIP シグナリングを実行する電話機のより新しいモデルには適合しません。これらのモデルでは、SIP スタック内のシグナリング オーバーヘッドが増える可能性があります。また、上記方程式の計算は、基本的な単一回線コールを前提としています。そのため、シグナリング キューの使用状況を監視およびテストして、一日の混雑する時間帯にキュー テール ドロップが発生した場合にどのような調整が必要かを決定することをお勧めします。帯域幅の高い WAN リンクでは、WAN 上の未使用の帯域幅を他のキューに使用できるように、キューの値を高く設定することをお勧めします。したがって、表 3-9 の暗号化を使用した SIP の値と暗号化を使用しない SIP の値を参考にして、電話機ごとの値を高めに調整するのがベストです。

(注)　上記の推奨事項は、LAN アクセス ポート ポリシング設定ではなく、WAN キューイング帯域幅設定に適用されます。LAN アクセス ポート ポリシングでは、さまざまなユースケースから想定されるシグナリング スパイクに応じて、値を 80 kbps 以上に設定することをお勧めします。（古いドキュメントでは 32 kbps が推奨されていますが、これは、既に多くのシグナリング ユースケースの基準ではありません）。たとえば、回線上の話中ランプ フィールド（BLF）が設定された電話機は、話中表示ごとに 1 つずつの SIP NOTIFY と SIP 200OK を生成します。つまり、大量の BLF が関連付けられた電話機は、SIP シグナリングでスパイクを引き起こし、1 秒間に何回もオンフックとオフフックを高速で繰り返す可能性があります。そのため、アクセス ポート スイッチ上のポリシングの前にシグナリングの最悪のシナリオを想定しておくことをお勧めします。

拡張公式

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

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

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

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

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

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

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

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

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

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

シェアド ライン アピアランスに関する考慮事項

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

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

  CHS = CHL *（ライン アピアランス数）/（回線数）

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

  回線数 = 5

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

  CHL = 6

  CHS = 6 * (11 / 5) = 13.2

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

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

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

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

  たとえば、SCCP と、同じ回線を共有する 6 台の電話機を使用する場合、トラフィックのシグナリング クラス用のキュー項目数は 78 以上に調整する必要があります。表 3-10 は、支店サイトでのシェアド ライン アピアランスの量に基づいた推奨されるキュー項目数を示しています。

表 3-10　支社サイトごとの推奨キュー項目数

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

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

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

分散型呼処理による呼制御トラフィック用のプロビジョニング

分散型呼処理配置では、Unified CM クラスタは、それぞれが単一サイト モデルまたは集中型呼処理モデルに従って、各 IP WAN を介して接続されます。WAN を介したコールの発信に使用されるシグナリング プロトコルは SIP です（H.323 トランクは Unified CM クラスタ間では推奨されなくなりました）。WAN を通過する SIP プロトコル制御トラフィックは、メディア ストリームに関連付けられるシグナリング トラフィックに属し、コールのセットアップ、終了、転送などが必要なときにクラスタ間トランクで交換されます。

制御トラフィックの合計数は、任意の時間にセットアップし、終了するコール数によって異なるので、コール パターンとリンク使用状況について、何らかの想定をする必要があります。従来型のテレフォニーから類推して、WAN リンクの音声およびビデオ用にプロビジョニングされた部分を複数の *仮想タイ ライン* と見なし、その仮想タイ ラインに関連するプロトコル シグナリング トラフィックを導出できます。

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

公式 6：仮想タイ ライン数に基づく推奨帯域幅

推奨帯域幅（bps）= 116 *（仮想タイ ライン数）

Cisco IOS ルータ上のキューに割り当て可能な最小帯域幅は、8 Kbps です。つまり、1 時間あたり最大 70 の仮想タイ ラインまたは 2,100 のコールによって生成される呼制御トラフィックを、8 Kbps の最小キュー サイズで受け入れ可能であると推測できます。クラスタ間の SIP シグナリング トラフィックに対して 8 kbps という量は、多くの大規模企業での展開において十分な量です。

ワイヤレス LAN インフラストラクチャ

統合ネットワークのワイヤレス LAN（WLAN）部分にコラボレーション エンドポイントを追加する場合は、ワイヤレス LAN インフラストラクチャの設計が重要になります。Cisco Unified Wireless エンドポイントが導入されている場合、音声およびビデオ トラフィックは WLAN 上に移動しているので、そこで既存のデータ トラフィックと合流します。有線 LAN および有線 WAN のインフラの場合と同様、WLAN に音声およびビデオを追加するには、基本的な設定と設計に関するベスト プラクティスに従って、可用性の高いネットワークを配置する必要があります。また、WLAN インフラストラクチャを適切に設計するには、ネットワーク全体でエンドツーエンドの音声品質とビデオ品質を確保するために、QoS を理解してワイヤレス ネットワーク上に配置する必要があります。次の項では、これらの要件について説明します。

- WLAN を介した音声およびビデオのアーキテクチャ（3-66 ページ）
- WLAN を介した音声およびビデオのハイ アベイラビリティ（3-70 ページ）
- WLAN を介した音声およびビデオのキャパシティ プランニング（3-72 ページ）
- WLAN を介した音声およびビデオの設計上の考慮事項（3-73 ページ）

ワイヤレス LAN を介した音声およびビデオの詳細については、『*Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide*』を参照してください。このマニュアルは次の URL から入手できます。

https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd.html

WLAN を介した音声およびビデオのアーキテクチャ

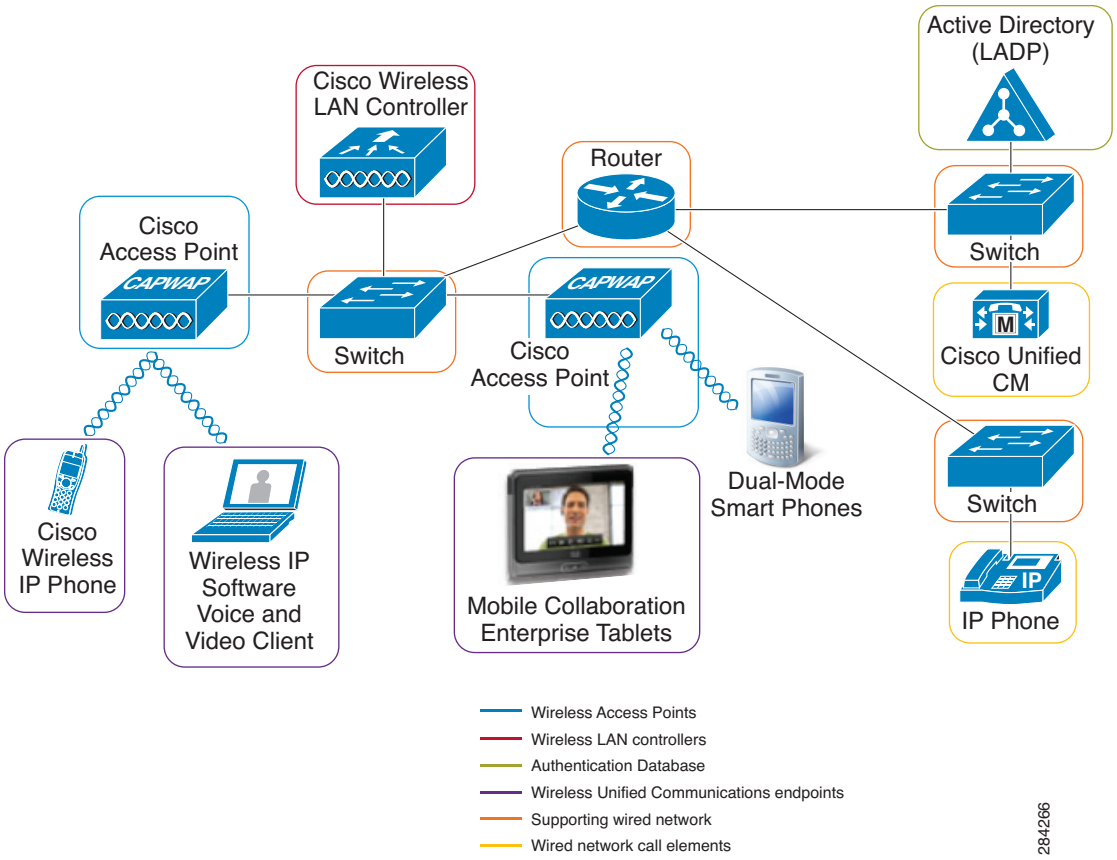
IP テレフォニー アーキテクチャでは当初から有線デバイスが使用されていますが、企業ユーザは長い間、会社構内を移動しながら通信できる機能を求め続けてきました。ワイヤレス IP ネットワークによって、IP テレフォニーは、ワイヤレス IP テレフォニー デバイスを持つユーザとのオンプレミス ローミング通信を提供し、企業モビリティを実現できるようになりました。

ワイヤレス IP テレフォニーおよびワイヤレス IP ビデオ テレフォニーは、同等の有線テレフォニーの拡張であり、同じコール要素を利用します。また、ワイヤレス IP テレフォニーと IP ビデオ テレフォニーではワイヤレス 802.11 対応メディアが利用されるため、IP 音声およびビデオをコードレスで使用できます。コードレスの使用は、ワイヤレス ネットワーク インフラストラクチャの要素を制御パケットとメディア パケットの送受信に利用することによって実現されます。

ワイヤレス LAN を介した音声およびビデオのアーキテクチャには、図 3-24 に示す次の基本要素が含まれます。

- ワイヤレス アクセス ポイント（3-67 ページ）
- ワイヤレス LAN コントローラ（3-68 ページ）
- 認証データベース（3-68 ページ）
- サポート有線ネットワーク（3-69 ページ）
- ワイヤレス コラボレーション エンドポイント（3-69 ページ）
- 有線のコール要素（3-69 ページ）

図 3-24　音声およびビデオのワイヤレス ネットワークの基本レイアウト

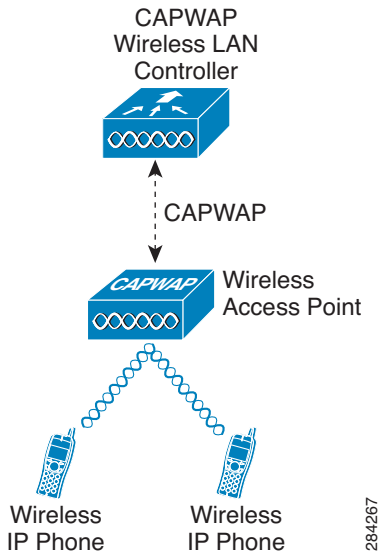


ワイヤレス アクセス ポイント

ワイヤレス アクセス ポイントにより、ワイヤレス デバイス（WLAN を介した音声およびビデオの場合は Unified Communications エンドポイント）は有線ネットワーク要素と通信できます。アクセス ポイントは、有線の世界とワイヤレスの世界の間にあるアダプタとして機能し、これら 2 つのメディア間に通路を築きます。シスコのアクセス ポイントは、ワイヤレス LAN コントローラ（WLC）で管理することもできますし、自律モードで機能することもできます。アクセス ポイントが WLC によって管理されている場合、それらは Lightweight アクセス ポイントと呼ばれます。このモードでは、コントローラのバージョンに応じて、WLC との通信時に Lightweight アクセス ポイント プロトコル（LWAPP）または Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルが使用されます。

図 3-25 は、Lightweight アクセス ポイントと WLC 間の基本的な関係を示しています。図 3-25 に示す例は CAPWAP WLC 用ですが、トラフィック フローおよび関係性の観点から見ると、CAPWAP と LWAPP の間に識別できる相違点はないので、この例はワイヤレス LWAPP ネットワークにも適用できます。ワイヤレス インフラストラクチャに WLC と Lightweight アクセス ポイントを利用する利点として、管理の容易性、ネットワークの動的な調整、およびハイ アベイラビリティがあります。ただし、アクセス ポイントで自律モードの代わりに管理モードを使用する場合は、ソリューションの設計時に LWAP-WLC 通信アーキテクチャのネットワーク トンネリング効果について検討する必要があります。このネットワーク トンネリング効果については、ワイヤレス LAN コントローラの設計上の考慮事項（3-78 ページ）の項で詳しく説明します。

図 3-25　Lightweight アクセス ポイント



ワイヤレス LAN コントローラ

多くの企業環境では、ワイヤレス ネットワークを大規模に展開する必要があります。ワイヤレス LAN コントローラ（WLC）は、ワイヤレス ネットワークの中心的な役割を担うデバイスであり、これにより大規模な展開を容易に行うことができます。ワイヤレス クライアントの関連付けや認証といったアクセス ポイントの従来の役割は WLC によって実行されます。Unified Communications 環境で Lightweight アクセス ポイント（LWAP）と呼ばれるアクセス ポイントは、WLC に自身を登録して、すべての管理パケットとデータ パケットを WLC にトンネリングします。すると、WLC はワイヤレス クライアントとネットワークの有線部分との間でパケットのスイッチングを行います。すべての設定は WLC で行います。LWAP は WLC から設定全体をダウンロードし、クライアントに対してワイヤレス インターフェイスとして機能します。

認証データベース

認証データベースは、ワイヤレス ネットワークの中心コンポーネントであり、ワイヤレス アソシエーションの進行中に認証されるユーザのクレデンシャルを保持します。認証データベースは、クレデンシャルを検証するための一元化されたリポジトリをネットワーク管理者に提供します。ネットワーク管理者は、ワイヤレス ネットワーク ユーザを認証データベースに追加するだけで済みます。ワイヤレス デバイスに関連するすべてのワイヤレス アクセス ポイントにユーザを追加する必要はありません。

一般的なワイヤレス認証シナリオでは、WLC は認証データベースと連携して、ワイヤレス アソシエーションの続行を許可するか、またはエラーにします。一般に使用される認証データベースは LDAP と RADIUS ですが、一部のシナリオでは、認証用として使用可能な小さなユーザ データベースを WLC でローカルに保存できます。

サポート有線ネットワーク

サポート有線ネットワークはシステムの一部であり、WLC、AP、および有線のコール要素間のパスとして機能します。AP は有線の世界と通信する必要があるので（または必要となる可能性があるので）、有線ネットワーク部分でこれらの通信を有効にしておく必要があります。サポート有線ネットワークは、スイッチ、ルータ、および有線メディア（WAN リンクと光リンク）から構成され、これらが連携して、WLAN を介した音声およびビデオのアーキテクチャを形成するさまざまなコンポーネントと通信します。

ワイヤレス コラボレーション エンドポイント

ワイヤレス コラボレーション エンドポイントは、WLAN を介した音声およびビデオのアーキテクチャのコンポーネントであり、ユーザはこれらを使用して互いに通信します。これらのエンドポイントは、音声専用にすることも、音声とビデオの両方に使用することもできます。エンド ユーザがワイヤレス通信エンドポイントを使用して目的の宛先にコールすると、エンドポイントはその要求を関連する呼処理サーバに転送します。コールが許可されると、エンドポイントは音声またはビデオを処理してエンコードし、受信側デバイスまたは処理のネクスト ホップに送信します。一般的なシスコのワイヤレス エンドポイントは、ワイヤレス IP Phone、デスクトップ コンピュータで実行されている音声およびビデオ ソフトウェア クライアント、ワイヤレス メディアを介して接続されているモバイル スマート フォン、およびモバイル コラボレーション エンタープライズ タブレットです。

有線のコール要素

ワイヤレス コラボレーション エンドポイントが互いの間でセッションを開始する場合でも、有線のエンドポイントとセッションを開始する場合でも、有線のコール要素が何らかの方法で関係します。有線のコール要素（ゲートウェイと呼処理エンティティ）は、サポート インフラストラクチャであり、音声およびビデオ エンドポイントはこのインフラストラクチャと連携します。

有線のコール要素は、一般的に次の 2 つの要件に対処するために必要です。

- コール制御（3-69 ページ）
- メディアの終端（3-69 ページ）

コール制御

コールを効率的にルーティングして、エンド ユーザに豊富な機能を体験してもらうために、シスコのワイヤレス エンドポイントは呼制御または呼処理サーバを必要とします。呼処理エンティティは、LAN または WAN 上の有線ネットワーク内のどこかに配置されます。

シスコのワイヤレス エンドポイントの呼制御は、SIP または SCCP のいずれかの呼制御プロトコルを通じて実行されます。

メディアの終端

有線エンドポイントのメディアの終端は、ワイヤレス エンドポイントのエンド ユーザが IP Phone、PSTN ユーザ、またはビデオ エンドポイントと通信する場合に発生します。音声ゲートウェイ、IP Phone、ビデオ端末、PBX トランク、およびトランスコーダはすべて、ユーザがそれらを通じて通信する場合にメディアの終端ポイントとして機能します。このようなメディアの終端は、ユーザ通信用の音声またはビデオ セッションのコーディングおよびデコーディングによって発生します。

WLAN を介した音声およびビデオのハイ アベイラビリティ

コラボレーション ソリューションでハイ アベイラビリティを実現することは、継続的な接続を求める現代の要求に沿った重要な要件です。ハイ アベイラビリティを目的として設計されたコラボレーションの配置によって、信頼性および使用可能時間が向上します。WLAN を介した音声またはビデオなどのリアルタイム アプリケーションをハイ アベイラビリティのない状態で使用すると、音声またはビデオ コールを発信できないなど、非常に悪い影響をエンド ユーザ エクスペリエンスに与える可能性があります。

ハイ アベイラビリティを備えた、WLAN を介した音声およびビデオ向けソリューションを設計するには、次の主要分野に重点を置く必要があります。

サポート有線ネットワークのハイ アベイラビリティ

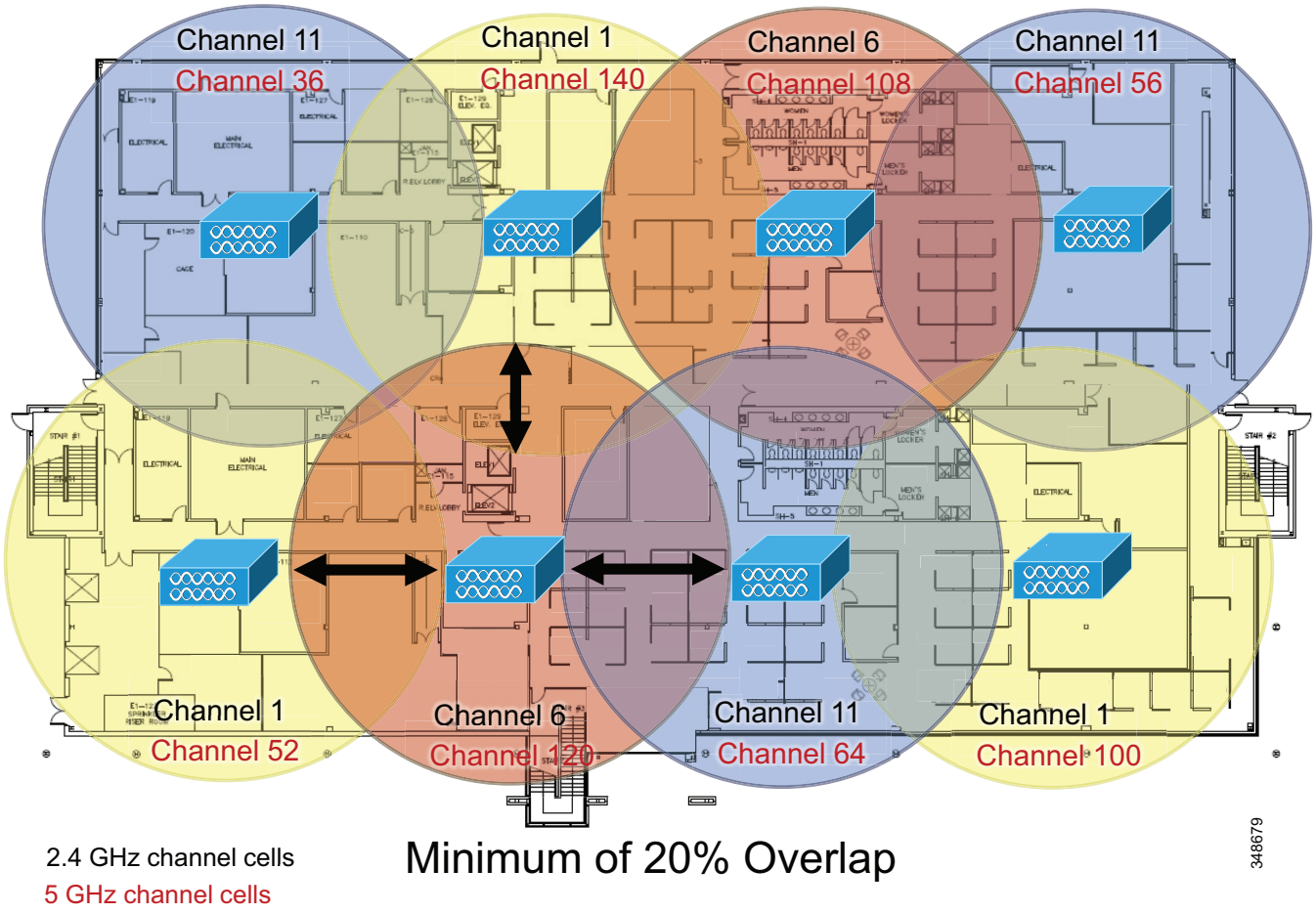
WLAN を介した音声およびビデオを配置する場合、有線ネットワークに使用されているハイ アベイラビリティ実現方法と同じ方法を、WLAN を介した音声およびビデオ向けソリューションの有線コンポーネントに適用できます。たとえば、ネットワーク内のレイヤ コンバージェンスを最適化して、中断を最小限に抑え、等コストの冗長パスを利用することができます。

可用性の高い有線ネットワークを設計する方法については、ハイ アベイラビリティのための LAN 設計 (3-4 ページ)を参照してください。

WLAN のハイ アベイラビリティ

WLAN を介した音声およびビデオのハイ アベイラビリティの特徴は、単一の WLAN 無線機に依存しない Wi-Fi チャネル カバレッジを提供する無線周波数 (RF) カバレッジのハイ アベイラビリティです。Wi-Fi チャネル カバレッジは、2.4 GHz および 5 GHz 周波数帯域の AP 無線機により提供されます。RF ハイ アベイラビリティを提供するための主要メカニズムは、セル境界オーバーラップです。一般的に、ワイヤレス ネットワークにハイ アベイラビリティを提供するには、非隣接チャネルのセル境界オーバーラップを 20 ～ 30 % にすることが推奨されています。ミッションクリティカルな環境では、必要な信号レベル (-67 dBm 以上) で認識可能な AP が 2 つ以上必要です。20 % のオーバーラップとは、非隣接チャネルを使用する AP の RF セルが、そのカバレッジ エリアの 20 % で互いにオーバーラップし、カバレッジ エリアの残りの 80 % が単一の AP によって処理されることを意味します。図 3-26 は、ハイ アベイラビリティを実現するために AP の非隣接チャネル セルのオーバーラップを 20 % にした場合の例をしています。さらに、AP の設置場所を決定する際は、(金属、ガラスなどの) 反射面に取り付けないようにします。このような反射面は、信号の歪みの原因となるマルチパス作用を引き起こす可能性があります。

図 3-26　　非隣接チャネルのアクセス ポイントのオーバーラップ



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

さらに、一般的に混雑が少なく、通常は干渉傾向が低い 5 GHz 周波数帯域の使用についても評価します。Bluetooth を使用する場合は、5 GHz 802.11a を使用することを強く推奨します。同様に、Cisco CleanAir テクノロジーを利用すると、無線周波数の干渉をリアルタイムで検出し、自己回復型および自己最適化型のワイヤレス ネットワークを提供することで、WLAN の信頼性が向上します。Cisco CleanAir テクノロジーの詳細については、次の URL で入手可能な製品マニュアルを参照してください。

https://www.cisco.com/en/US/netsol/ns1070/index.html

リッチ メディアをサポートする WLAN でのハイ アベイラビリティの実現方法については、『*Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide*』を参照してください。このマニュアルは次の URL から入手できます。

https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd.html

呼処理のハイ アベイラビリティ

呼処理の復元性に関する詳細については、呼処理のハイ アベイラビリティ（9-13 ページ）を参照してください。

WLAN を介した音声およびビデオのキャパシティ プランニング

WLAN を介した音声およびビデオを計画するうえで重要な点は、必要なコール キャパシティのソリューションを適切にサイジングすることです。キャパシティは、特定の領域でサポート可能な、WLAN を介した音声およびビデオの同時セッション数として定義されます。キャパシティは、RF 環境、コラボレーション エンドポイントの機能、WLAN システムの機能に応じて異なります。たとえば、最適化された WLAN サービス（Cisco Unified Wireless Network など）を提供する WLAN 上で Cisco Unified Wireless IP Phone 7925G を使用するソリューションは、802.11a と 802.11g の両方に対して 24 Mbps 以上のデータ レートで、チャネルごとに同時セッション数 27 の最大コール キャパシティを備えています。一方、WLAN 上でビデオ レート 2,500 kbps で 720p のビデオ コールを行うタブレットなどのワイヤレス デバイスによる同様のソリューションは（この場合、アクセス ポイントは 40 MHz チャネルの変調および符号化方式のデータ レート インデックス 7 で 802.11a/n として設定されます）、チャネルごとにビデオ コール数 7（2 つの双方向の音声およびビデオ ストリーム）の最大キャパシティを備えています。

これらのキャパシティを実現するには、ワイヤレス LAN のバックグラウンド トラフィックと無線周波数（RF）の使用を最小限に抑える必要があり、また、デバイスで Bluetooth を無効にする必要があります。さらに、制限要因はチャネル キャパシティであってアクセス ポイント（AP）数ではないため、コール キャパシティが非オーバーラップ チャネルごとに設定されることを理解することも重要です。

展開する際には、実際のワイヤレス エンドポイントで指定されているコール キャパシティを使用する必要があります。そのコール キャパシティが、そのエンドポイントでサポートされるキャパシティであるからです。ワイヤレス エンドポイントのキャパシティ情報については、ご使用のエンドポイント モデルの製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/product-listing.html

WLAN のコール キャパシティの計算方法については、『*Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide*』を参照してください。このマニュアルは次の URL から入手できます。

https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd.html

WLAN を介した音声およびビデオの設計上の考慮事項

ここでは、WLAN を介したコラボレーション エンドポイントの配置ソリューションに関するその他の設計上の考慮事項について説明します。WLAN 設定の詳細は、使用されている音声またはビデオ WLAN デバイスや WLAN 設計に応じて異なります。以下の項では、WLAN インフラストラクチャを設計するための一般的なガイドラインとベスト プラクティスについて説明します。

VLAN

有線 LAN インフラストラクチャの場合と同様、ワイヤレス LAN に音声またはビデオを配置する場合は、アクセス レイヤで 2 つ以上の仮想 LAN（VLAN）を有効にする必要があります。ワイヤレス LAN 環境のアクセス レイヤには、アクセス ポイント（AP）と最初のホップのアクセス スイッチが含まれます。AP とアクセス スイッチ上では、データ トラフィック用のネイティブ VLAN と、音声トラフィック用の Voice VLAN（Cisco IOS の場合）または Auxiliary VLAN（CatOS の場合）を設定する必要があります。この Auxiliary/Voice VLAN は、ネットワークにある他のすべての有線 Voice VLAN とは分離する必要があります。ただし、ワイヤレス クライアント（スマート フォン、ソフトウェア リッチメディア クライアントなど）が Auxiliary VLAN の概念をサポートしていない場合は、音声やビデオなどの重要なトラフィックを分離して優先的に処理するために、代替のパケット マーキング方法（ポートごとのパケット分類など）を適用する必要があります。無線インフラストラクチャを配置する場合は、WLAN AP の管理用に独立した管理 VLAN を設定することも推奨します。この管理 VLAN には WLAN アピアランスを設定しないでください。つまり、関連付けられた Service Set Identifier（SSID）を設定することも、WLAN から直接アクセスできるように設定することもしないでください。

ローミング

ユーザ エクスペリエンスを向上させるために、非隣接チャネルを 20 ～ 30 % オーバーラップさせてセル境界の配分を設計し、アクセス ポイント間でのワイヤレス クライアントのシームレスなローミングを容易にすることを推奨します。さらに、デバイスがレイヤ 3 でローミングする場合、デバイスはネイティブ VLAN の境界を越えて AP から別の AP に移動します。WLAN インフラストラクチャが自律 AP から構成されている場合は、Cisco Wireless LAN Controller を使用すると、Cisco Unified Wireless エンドポイントでそれらの IP アドレスを保持し、アクティブ コールを維持したままレイヤ 3 でローミングすることができます。シームレスなレイヤ 3 ローミングが行われるのは、クライアントが同じモビリティ グループ内でローミングする場合だけです。Cisco Wireless LAN Controller およびレイヤ 3 ローミングの詳細については、次の URL から入手可能な製品マニュアルを参照してください。

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

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

（注）　デュアルバンド WLAN（2.4 GHz と 5 GHz 帯域を装備）では、クライアントが両方の帯域をサポートする場合、同じ SSID によって 802.11b/g と 802.11a 間でローミングできます。ただし、これにより、音声パスにギャップが発生する場合があります。Cisco Unified Wireless IP Phone 7921 または 7925 が使用されている場合は、これらのギャップを回避できるようにファームウェア バージョン 1.3(4) 以上が電話機にインストールされていることを確認してください。インストールされていない場合は、音声用に 1 つの帯域のみを使用します。（Cisco Unified Wireless IP Phone 7926 では、最初のファームウェア バージョンからシームレスな帯域間ローミングが提供されています）。

ワイヤレス チャネル

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

2.4 GHz 802.11b/g/n 用にチャネル設定を最適化するには、設定するチャネルの間に 5 チャネル以上の間隔を設定して、チャネル間の干渉やオーバーラップを防止する必要があります。非オーバーラップ チャネルの間隔は 22 MHz です。チャネル 1 は 2.412 GHz、チャネル 6 は 2.437 GHz、チャネル 11 は 2.462 GHz です。許可されるチャネルが 1 ～ 11 の北米では、チャネル 1、6、および 11 が、AP とワイヤレス エンドポイント デバイスに使用可能な 3 つの非オーバーラップ チャネルです。それに対して、許可されるチャネルが 1 ～ 13 の欧州では、5 チャネルの間隔がある組み合わせは複数可能です。日本も許可されるチャネルが 1 ～ 14 なので、5 チャネルの間隔がある組み合わせは複数可能です。

5 GHz 802.11a および 802.11n 用にチャネル設定を最適化するには、1 チャネル以上の間隔を設定して、チャネル間の干渉やオーバーラップを防止する必要があります。北米では、次の 20 のオーバーラップのないチャネルを使用できます。36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、および 161。欧州および日本では、次の 16 の非オーバーラップ チャネルを使用できます。36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140。非オーバーラップ チャネルのセットは大きいため、802.11a および 5 Ghz 802.11n では WLAN をより密に配置できます。ただし、すべてのチャネルを有効にせずに、代わりに 12 チャネル設計を使用することを推奨します。

802.11a および 802.11n 帯域では（5.25 ～ 5.725 GHz で動作するチャネルを使用する場合、これらは使用可能な 24 チャネルのうちの 15 チャネル）、レーダー（軍事、衛星、および気象）による干渉を回避するために、一部のチャネルで動的周波数選択（DFS）と伝送パワー コントロール（TPC）のサポートが必要なので注意してください。規制により、チャネル 52 ～ 64、100 ～ 116、および 132 ～ 140 が DFS および TPC をサポートする必要があります。TPC は、これらのチャネル上の伝送が干渉を引き起こすほど強力にならないように制御します。DFC は、チャネルのレーダー パルスをモニタし、レーダー パルスを検出した場合、DFC はチャネル上の伝送を停止して、新しいチャネルに切り替えます。

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

高層オフィスビルや病院など、多階の建物にワイヤレス デバイスを配置する場合は、ワイヤレス AP とチャネル カバレッジのプランニングに 3 つめの次元が加わります。802.11 の 2.4 GHz と 5.0 GHz の波形は、いずれもフロア、天井、および壁を通過できます。このため、同一フロア上のオーバーラップ セルまたはチャネルを考慮するだけでなく、隣接フロア間のチャネル オーバーラップを考慮する必要もあります。2.4 GHz のワイヤレス スペクトルが 3 つの使用可能な非オーバーラップ チャネルに制限されている場合は、慎重に 3 次元の計画を立てることによってのみ、適切なオーバーラップ設計を実現できます。

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

ワイヤレス干渉とマルチパス歪み

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

可能性のある干渉源およびマルチパス歪みの源は、次のとおりです。

- オーバーラップ チャネル上にある他の AP
- 他の 2.4 GHz および 5 Ghz デバイス（2.4 GHz コードレス電話、個人用ワイヤレス ネットワーク デバイス、硫黄プラズマ照明システム、電子レンジ、不正 AP、2.4 GHz および 5 Ghz 帯域のライセンスフリーで動作するその他の WLAN 機器など）
- 金属機器、構造物、およびその他の金属面や反射面（金属 I ビーム、ファイリング キャビネット、機器ラック、ワイヤー メッシュまたは金属壁、防火扉と防火壁、コンクリート、および冷暖房のダクトなど）
- 高出力の電気装置（変圧器、強力電気モーター、冷蔵庫、エレベータ、およびエレベータ機器など）
- 高出力の電気装置（変圧器、強力電気モーター、冷蔵庫、エレベータ、エレベータ機器など）、および電磁干渉（EMI）を発生させる可能性があるその他の電源デバイス

Bluetooth 対応デバイスは 802.11b/g/n デバイスと同じ 2.4 GHz 無線帯域を使用するので、Bluetooth と 802.11b/g/n デバイスが相互に干渉して、接続に関する問題が発生する可能性があります。Bluetooth デバイスは 802.11b/g/n WLAN の音声およびビデオ デバイスに干渉して妨害する可能性があり、その結果、音声品質の低下、登録解除、コール セットアップの遅延、チャネル セルごとのコール キャパシティの低下が発生することがあります。そのため、可能な場合は、802.11a または 802.11n プロトコル（またはその両方）を使用してすべての WLAN 音声およびビデオ デバイスを 5 GHz Wi-Fi 帯域に配置することを推奨します。ワイヤレス クライアントを 5 Ghz 無線帯域に配置することで、Bluetooth デバイスによって引き起こされる干渉を回避できます。また、ワイヤレス インフラストラクチャ内で Cisco CleanAir テクノロジーを使用することを推奨します。これによって、リアルタイムの干渉検出が可能になるからです。Cisco CleanAir テクノロジーの詳細については、次の URL から入手可能な製品マニュアルを参照してください。

https://www.cisco.com/en/US/netsol/ns1070/index.html

（注）　802.11n は 2.4 GHz と 5 GHz 帯域の両方で動作できますが、Unified Communications には 5 GHz を使用することを推奨します。

WLAN 上のマルチキャスト

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

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

マルチキャスト アプリケーションまたはトラフィックが存在しない WLAN ネットワークでは、DTIM 周期を 2 以上の値に設定する必要があります。マルチキャスト アプリケーションが存在する WLAN ネットワークでは、可能な場合は常に、100 ms ビーコン周期で DTIM 周期の値を 2 に設定する必要があります。ただし、マルチキャスト トラフィックの品質が低下する場合や許容できない遅延が発生する場合は、DTIM 値を 1 に下げる必要があります。DTIM 値が 1 に設定されている場合、管理者は、バッテリ駆動式デバイスのバッテリ寿命が大幅に短縮されることに注意する必要があります。

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

マルチキャスト トラフィックに関するその他の考慮事項については、メディア リソース（7-1 ページ）の章を参照してください。

ワイヤレス AP の設定と設計

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

AP の選択

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

AP の配置

AP でアクティブになるデバイスの数は、各デバイスが転送メディアである Wi-Fi チャネルにアクセスできる時間に影響します。デバイスの数が増加すると、トラフィックの競合も増加します。より多くのデバイスを AP およびメディアの帯域幅に関連付けると、その AP に関連付けられているすべてのエンドポイント デバイスに対して、パフォーマンスが低下し、応答時間が長くなる可能性があります。

Cisco Wireless LAN Controller Release 7.2 よりも前のリリースには、限定された数のデバイスだけが単一の AP に関連付けられることを保証するメカニズムはありませんが、システム管理者は、定期的なサイト サーベイを実施し、ユーザとデバイスのトラフィック パターンを分析することによって、デバイスと AP の割合を管理できます。追加のデバイスおよびユーザを特定の領域でネットワークに追加した場合は、追加のサイト調査を行い、ネットワークにアクセスする必要があるエンドポイントの数に対応するために追加の AP が必要かどうかを判断する必要があります。

また、Cisco CleanAir テクノロジーをサポートしている AP では、Wi-Fi チャネルのリモート モニタリング機能が追加で提供されるため、これらの AP についても考慮する必要があります。

AP の設定

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

- アドレス解決プロトコル（ARP）キャッシングを有効にする

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

- AP 上のダイナミック伝送パワー コントロール（DTPC）を有効にする

  これにより、AP の送信電力が音声エンドポイントの送信電力と一致するようになります。伝送パワーの一致により、片方向オーディオ トラフィックの可能性を排除できます。音声エンドポイントは、関連付けられた AP の Limit Client Power（mW）設定に基づいて伝送パワーを調整します。

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

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

- AP で [ワイヤレス電話機の QoS 要素（QoS Element for Wireless Phones）] を有効にする。

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

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

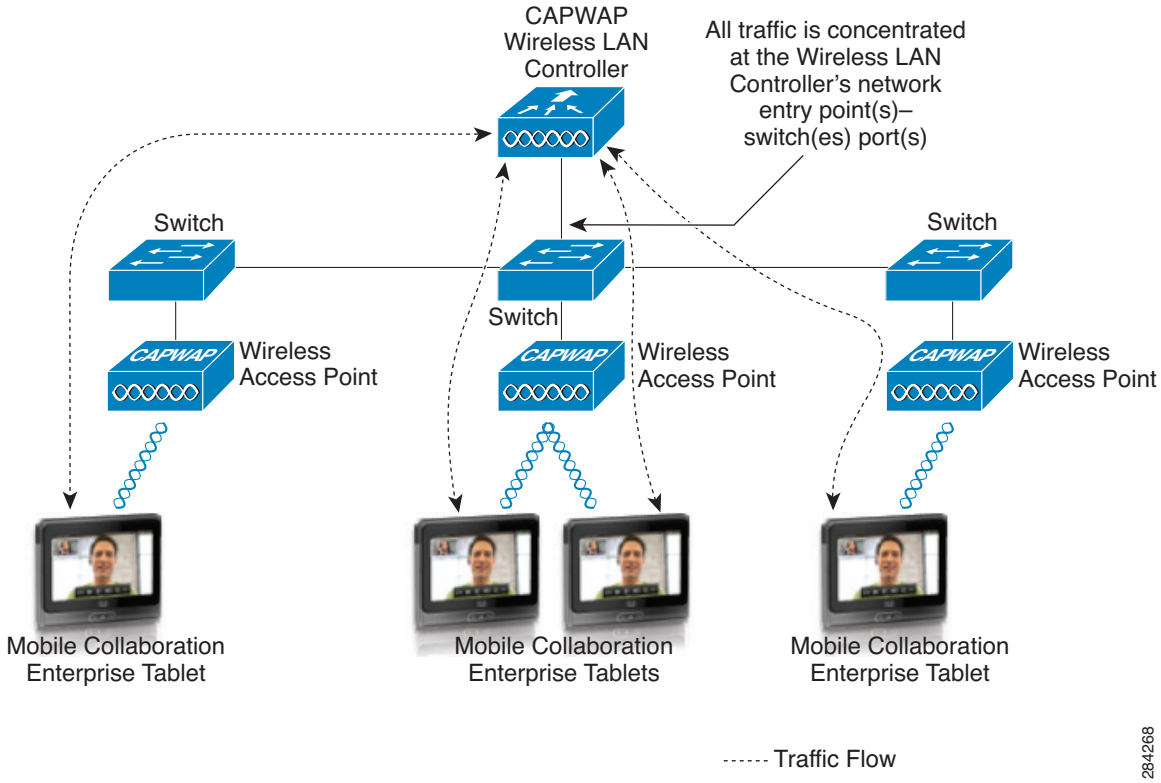
  音声トラフィックが確実にプライオリティ キューイング処理されるように、それぞれの VLAN のデフォルト分類で音声ポリシーとデータ ポリシーを設定します。（詳細については、インターフェイス キューイング（3-80 ページ）を参照してください）。

ワイヤレス LAN コントローラの設計上の考慮事項

音声またはビデオにサービスを提供するワイヤレス ネットワークを設計する際は、使用されるアクセス ポイントが自律型でもスタンドアロン型でもない場合の音声およびビデオのメディア パスに関して、ワイヤレス LAN コントローラが果たす役割を考慮することが重要です。すべてのワイヤレス トラフィックは、発信地点や宛先地点に関係なく、対応するワイヤレス LAN コントローラにトンネリングされるため、ワイヤレス コントローラのネットワーク接続エントリ ポイントを適切にサイジングすることが重要です。図 3-27 は、この問題を表したものです。モバイル デバイスが別のモバイル デバイスへのコールを試みた場合、トラフィックをワイヤレス LAN コントローラにヘアピン転送してから、受信側デバイスに送信する必要があります。この図には、両方のデバイスが同じ AP に関連付けられているというシナリオが含まれています。

ワイヤレス LAN コントローラが接続されているスイッチ ポートは、コラボレーション デバイスによって生成されたトラフィックに十分な帯域幅カバレッジを提供する必要があります。それらがビデオ エンドポイントであるか音声エンドポイントであるか、およびそれらのトラフィックが制御トラフィックであるかメディア トラフィックであるかは問いません。

図 3-27　　ワイヤレス LAN コントローラのネットワーク エントリ ポイントにおけるトラフィックの集中



また、スイッチ インターフェイスとスイッチ プラットフォームの出力バッファ レベルは、ワイヤレス ネットワークでサポートする予定の最大結合バーストと一致している必要があります。

適切なバッファ レベルを選択しないと、パケット ドロップが発生し、ワイヤレス LAN を介したビデオのユーザ エクスペリエンスに重大な影響を与える可能性があります。一方、帯域幅カバレッジの不足は、パケットのキューイングを引き起こし、極端な場合はパケットの遅延を引き起こします。

WLAN の Quality of Service（QoS）

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

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

ワイヤレスの QoS には、次の主要な設定領域があります。

- トラフィック分類（3-79 ページ）
- ユーザ優先度のマッピング（3-80 ページ）
- インターフェイス キューイング（3-80 ページ）
- ワイヤレス コール アドミッション制御（3-81 ページ）

トラフィック分類

有線ネットワーク インフラストラクチャの場合と同様、可能な限りネットワークのエッジ付近で適切なワイヤレス トラフィックを分類またはマークすることが重要です。トラフィック マーキングは、有線およびワイヤレス ネットワーク全体でキューイング方式の入力基準となるため、マーキングはできるだけワイヤレス エンドポイントで行われる必要があります。ワイヤレス ネットワーク デバイスによるマーキングまたは分類は、有線ネットワーク デバイスの場合（表 3-11 を参照）と同じである必要があります。

シスコのワイヤレス エンドポイントは、有線ネットワークのトラフィック分類ガイドラインに従って、音声メディア トラフィックまたは音声 RTP トラフィックを DSCP 46（または PHB EF）、ビデオ メディア トラフィックまたはビデオ RTP トラフィックを DSCP 34（または PHB AF41）、呼制御シグナリング トラフィック（SCCP または SIP）を DSCP 24（または PHB CS3）としてマークします。このトラフィックをマークしたら、ネットワーク全体でプライオリティ処理およびキューイング、またはベストエフォート型よりも優れた処理およびキューイングを行うことができます。トラフィックのマーキングが可能なすべてのワイヤレスの音声およびビデオ デバイスでは、この方法でマーキングする必要があります。ワイヤレス ネットワーク上の他のトラフィックはすべて、ベストエフォート型としてマークされるか、有線ネットワークのマーキング ガイドラインで規定されているいくつかの中間分類を使用してマークされる必要があります。音声またはビデオ ワイヤレス デバイスでパケット マーキングを実行できない場合は、ポートベースのマーキングなどの代替方法を実行して、ビデオおよび音声トラフィックのプライオリティを指定する必要があります。

ユーザ優先度のマッピング

802.1p および DiffServ コード ポイント（DSCP）が有線ネットワークに優先度を設定する標準であるのに対し、802.11e はワイヤレス ネットワークに使用される標準です。これは通常、ユーザ優先度（UP）と呼ばれ、UP を適切な DSCP 値にマッピングすることが重要です。表 3-11 は、コラボレーション トラフィックの値を示しています。

表 3-11　　QoS のトラフィック分類

トラフィックのタイプ	DSCP（PHB）	802.1p UP	IEEE 802.11e UP
音声	46（EF）	5	6
[ビデオ（Video）]	34（AF41）	4	5
音声およびビデオの制御	24（CS3）	3	4

802.11e およびその設定の詳細については、次の URL から入手可能な対応する製品マニュアルを参照してください。

https://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html

インターフェイス キューイング

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

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

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

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

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

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

（注） Wi-Fi マルチメディア（WMM）アクセスは Enhanced Distributed Channel Access（EDCA）に基づいているため、トラフィックに適切なプライオリティを割り当て、Arbitration Inter-Frame Space（AIFS）の変更および配信遅延を回避することが重要です。Cisco Unified Wireless の QoS の詳細については、『*Enterprise Mobility Design Guide*』の最新版を参照してください。このマニュアルは次の URL から入手できます。
https://www.cisco.com/en/US/netsol/ns820/networking_solutions_design_guidances_list.html。

ワイヤレス コール アドミッション制御

特定の AP チャネルのキャパシティ制限を超えないようにするには、ある種のコール アドミッション制御が必要です。Cisco AP およびワイヤレス Unified Communications クライアントでは、現在、コール アドミッション制御に、QoS Basic Service Set（QBSS）ではなく Traffic Specification（TSPEC）が使用されています。

Wi-Fi Multimedia Traffic Specification（WMM TSPEC）は QoS メカニズムであり、このメカニズムによって、WLAN クライアントはその帯域幅と QoS 要件を通知して、AP がその要件に対応できるようにします。クライアントが電話を掛けようと準備する場合、クライアントは TSPEC を示す Add Traffic Stream（ADDTS）メッセージを, 関連付けられた AP に送信します。次に、AP は、帯域幅とプライオリティ処理が使用できるかどうかに応じて、ADDTS 要求を受け入れるかまたは拒否します。コールが拒否された場合、クライアントは Network Busy メッセージを受信します。クライアントがローミングしている場合、TSPEC 要求は、アソシエーション プロセスの一部として新しい AP 宛の再アソシエーション要求メッセージに埋め込まれ、TSPEC 応答は再アソシエーション応答に埋め込まれます。

また、WMM TSPEC のサポートがなく、コール シグナリングとして SIP を使用しているエンドポイントは、AP によって管理できます。Service Set Identifier（SSID）に対してメディア スヌーピングを有効にしておく必要があります。クライアントの SIP 実装は、暗号化やポート番号など、ワイヤレス LAN コントローラの SIP 実装と一致している必要があります。メディア スヌーピングの詳細については、『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。このマニュアルは次の URL から入手できます。

https://www.cisco.com/en/US/docs/wireless/controller/7.0/configuration/guide/c70wlan.html

（注） 現在、ビデオに対するコール アドミッション制御のサポートはありません。QoS Basic Service Set（QBSS）情報要素が AP から送信されるのは、AP で [ワイヤレス電話機の QoS 要素（QoS Element for Wireless Phones）] が有効になっている場合だけです（ワイヤレス AP の設定と設計（3-76 ページ）を参照）。

Cisco Collaboration Security

改訂日：2018 年 3 月 1 日

音声およびビデオ コールの完全性と機密を保護するために、Cisco Collaboration ソリューションのさまざまなコンポーネントを保護する必要があります。

この章では、特にコラボレーション アプリケーションと音声およびビデオ ネットワークに関連したセキュリティ ガイドラインを示します。データ ネットワーク セキュリティの詳細については、次の URL で入手可能な Cisco SAFE Blueprint に関するマニュアルを参照してください。

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html

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

この章では、WAN 経由のクラスタリングを含む集中型呼処理と分散型呼処理について説明します。この章では、ヘッドエンド障害が発生したときに、すべてのリモート サイトが、ヘッドエンドまたはローカル呼処理バックアップへの冗長リンクを使用できることを前提としています。基本的にここでは、ネットワーク アドレス変換（NAT）と IP テレフォニーの間の対話については説明しません。この章では、すべてのネットワーク プライベート アドレスが指定されており、重複する IP アドレスが含まれていないことも前提としています。

この章の変更点

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

表 4-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
証明書管理	証明書管理（4-14 ページ）	2018 年 3 月 1 日
暗号化	暗号化（4-20 ページ）	2018 年 3 月 1 日
Cisco Unified Communications Manager（Unified CM）のセキュリティに関する考慮事項	Cisco Unified CM セキュリティ（4-22 ページ）	2018 年 3 月 1 日
その他の更新	この章のさまざまなセクション	2018 年 3 月 1 日
H.323 に関する情報を削除	本書の対象外	2018 年 3 月 1 日

セキュリティの概要

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

セキュリティ ポリシー

シスコは、自社内に導入されている各ネットワーク テクノロジーに関連付けられたセキュリティ ポリシーを作成することを推奨します。セキュリティ ポリシーは、ネットワーク内の機密データを特定し、ネットワーク内で転送する際にはデータを適切に保護します。セキュリティ ポリシーを配置すると、ネットワーク上のデータ トラフィックのタイプで要求されているセキュリティ レベルを定義するのに役立ちます。各データ タイプで独自のセキュリティ ポリシーが必要な場合もあれば、必要でない場合もあります。

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

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

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

音声およびビデオ トラフィックが含まれるセキュリティ ポリシーで困難な問題の 1 つは、通常、データ ネットワークと従来の音声ネットワークの両方に存在するセキュリティ ポリシーの結合です。ネットワークへのメディア統合のすべての側面が、導入済みのセキュリティ ポリシーまたは社内環境の適切なレベルで保護されていることを確認してください。

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

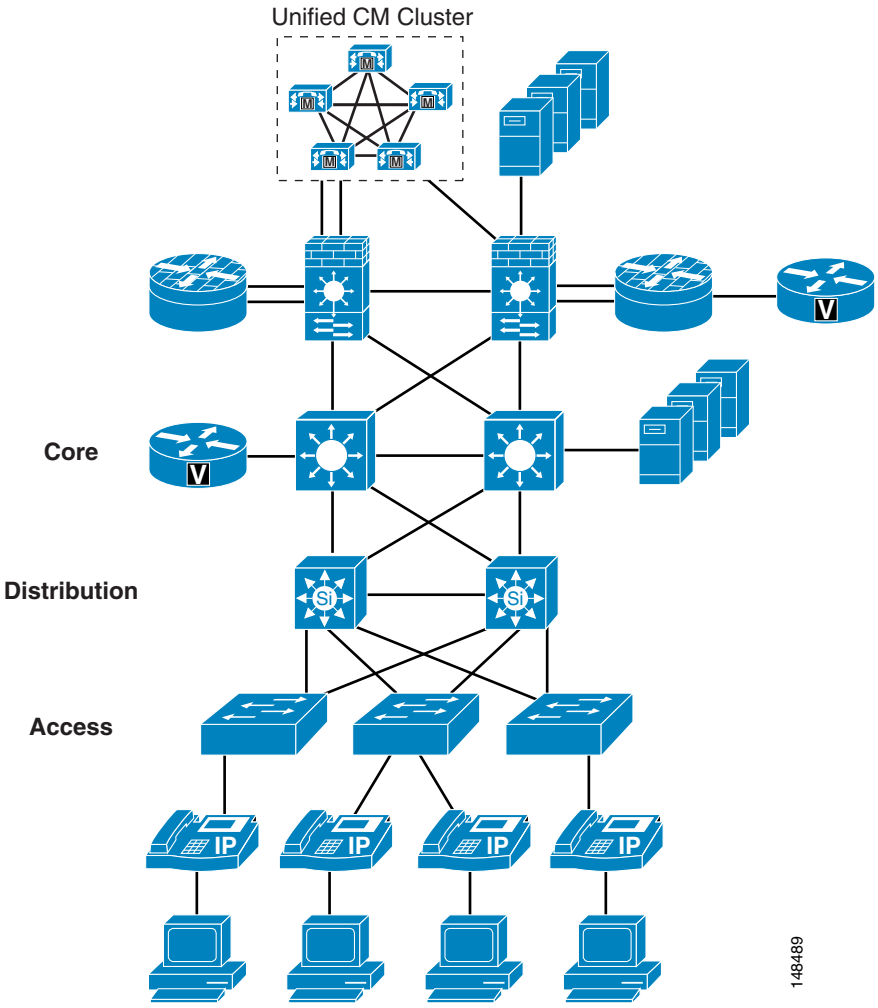
要約すると、セキュリティ ポリシーを定義するには、次のプロセスに従います。

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

レイヤ化したセキュリティ

この章では最初に、Cisco Unified Communications ソリューションにおける IP Phone エンドポイントの強化を示し、電話機からアクセス スイッチ、ディストリビューション レイヤ、コア、およびデータセンターへのネットワークについて説明します。(図 4-1 を参照)。シスコは、アクセスポートからネットワーク自体に至るまで、何層ものセキュリティを構築することを推奨します。このデザイン アプローチにより、ネットワーク アーキテクトはデバイスを配置して、そこに Cisco Unified Communications アプリケーションを物理的にも論理的にも簡単に導入できます。しかし、簡単に導入できるということは、セキュリティがより複雑になることを意味します。接続性があるところであればネットワーク内のどの場所にでも、デバイスを配置できるからです。

図 4-1　　セキュリティ レイヤ



セキュアなインフラストラクチャ

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

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

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

物理的なセキュリティ

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

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

- https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html
- https://www.cisco.com/c/en/us/products/security/service-listing.html

IP アドレッシング

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

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

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

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

ルート集約を正しく導入すると、ルーティング テーブルを、音声およびビデオ エンドポイントの導入の前と同じ大きさか、それよりわずかに大きい程度に保つことができます。

IPv6 アドレス指定

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

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

- 『*Deploying IPv6 in Campus Networks*』
  https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/CampIPv6.html
- 『*Deploying IPv6 in Branch Networks*』
  https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Branch/BrchIPv6.html

アクセス セキュリティ

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

音声 VLAN とビデオ VLAN

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

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

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

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

サードパーティ製のエンドポイントは、Cisco Discovery Protocol（CDP）または 802.1Q VLAN ID タギングをサポートしません。サードパーティ製デバイスが含まれる場合にデバイス検出を可能にするには、リンク層検出プロトコル（LLDP）を使用します。LLDP for Media Endpoint Devices（LLDP-MED）は、音声エンドポイントのサポートを向上させる LLDP の拡張です。LLDP-MED では、LLDP-MED 対応エンドポイントを検出したときに、スイッチ ポートが LLDP から LLDP-MED へどのように移行するかが定義されています。IP Phone および LAN スイッチでの LLDP と LLDP-MED 両方のサポートは、ファームウェアおよびデバイス モデルに依存します。特定の電話機またはスイッチ モデルで LLDP-MED がサポートされているかどうかを判断するには、特定の製品のマニュアル、リリース ノート、または速報を確認してください。

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

サーバやクライアントがファイアウォールで分断されている場合は、それらのエンドポイントとサーバ間で TCP ポートと UDP ポートを広範囲に許可する必要があります。各製品のポート利用ガイドを参照してください。詳細については、次の Web サイトで入手可能な『*System Configuration Guide for Cisco Unified Communications Manager*』の最新版を参照してください。

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

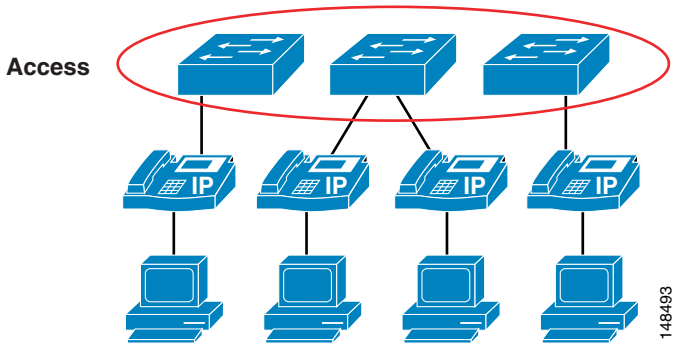
ゲートウェイとサーバはインフラストラクチャ デバイスと見なされ、通常は、データセンター内で Unified CM サーバに隣接して配置されます。一方、クライアントは、データ VLAN 上に配置されるのが一般的です。

スイッチ ポート

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

https://www.cisco.com

図 4-2　　電話機が接続される代表的なアクセス レイヤ設計



ポートセキュリティ：MAC CAM フラッディング

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

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

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

ポート セキュリティ：ポート アクセスの防止

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

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

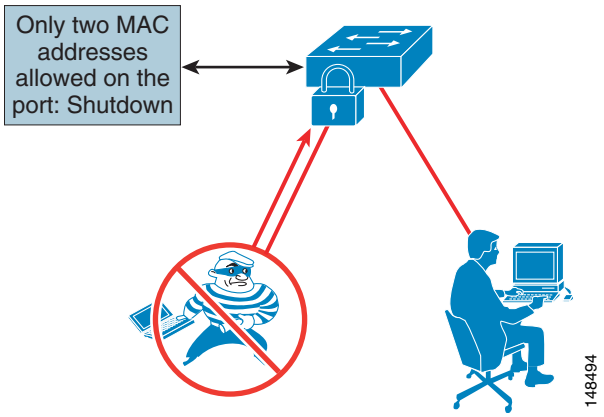
デバイス モビリティに対し、スタティック ポート セキュリティまたは持続性のあるダイナミック ポート セキュリティによるプロビジョニングは行われません。最重要の要件ではありませんが、MAC フラッディング攻撃は、特定の MAC アドレスへのアクセスを制限することを目的としているポート セキュリティにより暗黙的に防止されます。

セキュリティの観点から、MAC アドレス承認を使用するのではなく、802.1x に基づいてポート アクセスを認証して承認するより強力なメカニズムがあります。MAC アドレスだけでは、ほとんどのオペレーティング システムで簡単にスプーフィングまたは偽造されます。

ポート セキュリティ：不正なネットワーク拡張の防止

ポート セキュリティは、攻撃者がスイッチの CAM テーブルに対してフラッディングを実行したり、すべての受信トラフィックをすべてのポートに送信するハブに VLAN を転送したりするのを防止します。また、エンドポイントにハブまたはスイッチを追加することにより、認可されていないネットワークの拡張を防止します。ポート セキュリティは 1 つのポートでの MAC アドレスの数を制限するので、ポート セキュリティを、IT で作成されたネットワークへのユーザ拡張を抑制するためのメカニズムとして使用することもできます。たとえば、ユーザ方向のポート、または単一の MAC アドレス用にポート セキュリティが定義された電話機のデータ ポートに、ユーザがワイヤレス アクセス ポイント（AP）を接続した場合、ワイヤレス AP 自体がその MAC アドレスを占有し、背後にあるデバイスはネットワークにアクセスできません。（図 4-3 を参照）。一般的に、MAC フラッディングを停止するのに適切な設定は、不正アクセスを抑制するためにも適切です。

図 4-3　　MAC アドレス数の制限による不良ネットワーク拡張の防止



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

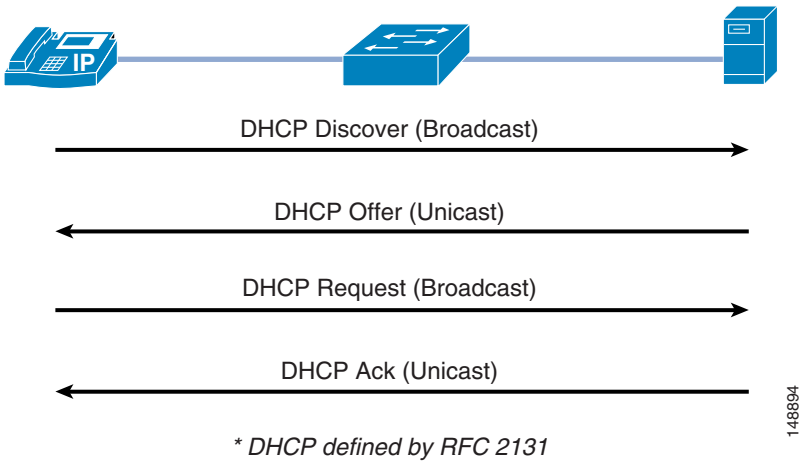
DHCP スヌーピング：不正な DHCP サーバ攻撃の防止

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

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

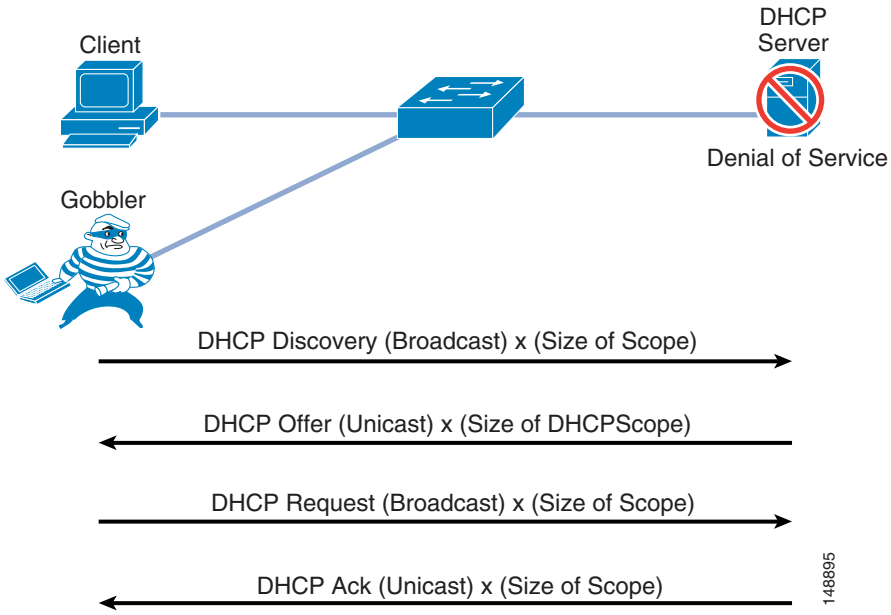
図 4-4 は、DHCP サーバに IP アドレスを要求するネットワーク接続デバイスの通常の操作を示しています。

図 4-4　　DHCP 要求の通常の操作



ただし、攻撃者は、単一の IP アドレスではなく、VLAN 内で使用可能なすべての IP アドレスを要求できます（図 4-5 を参照）。これは、ネットワークへのアクセスを試みている正当なデバイスのための IP アドレスが存在しないことを意味します。IP アドレスがないと、電話機は Unified CM に接続できません。

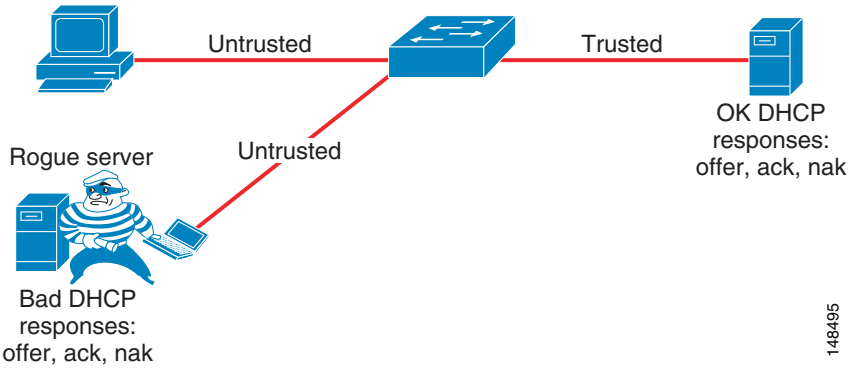
図 4-5　攻撃者は VLAN で使用可能なすべての IP アドレスを取得できる



DHCP スヌーピング：DHCP スターベーション攻撃の防止

Gobbler などのツールを使用した DHCP アドレス スコープ スターベーション攻撃は、DHCP サービス拒否（DoS）攻撃を仕掛けるために使用されます。Gobbler ツールは、ランダムに生成される異なる送信元 MAC アドレスから DHCP 要求を実行するので、ポート セキュリティを使用して MAC アドレスの数を制限することにより、Gobbler ツールが DHCP アドレス空間をスターピングするのを防止できます（図 4-6 を参照）。ただし、高度な DHCP スターベーション ツールでは、1 つの送信元 MAC アドレスから DHCP 要求を実行でき、DHCP ペイロード情報も多様です。DHCP スヌーピングを有効にすると、信頼されていないポートで、送信元 MAC アドレスと DHCP ペイロード情報が比較され、それらが一致しない場合は要求が失敗します。

図 4-6　DHCP スヌーピングを使用した DHCP スターベーション攻撃の防止



DHCP スヌーピングにより、任意の単一デバイスが特定範囲内のすべての IP アドレスをキャプチャすることを防止できますが、この機能が正しく設定されていないと、認定ユーザの IP アドレスが拒否される場合があります。

DHCP スヌーピング：バインディング情報

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

DHCP スヌーピングのために各タイプのスイッチに格納できるバインディング テーブル エントリには、最大制限があります（この制限を特定するには、スイッチの製品マニュアルを参照してください）。スイッチのバインディング テーブル内のエントリ数が気になる場合は、バインディング テーブルのエントリがより早くタイムアウトになるように、DHCP 範囲のリース時間を短縮できます。リースが期限切れになるまで、これらのエントリは DHCP バインディング テーブルに残されます。言い換えると、エンド ステーションがそのアドレスを持っていると DHCP サーバが判断する限り、これらのエントリは DHCP スヌーピング バインディング テーブルに残されます。ワークステーションまたは電話機を切断しても、これらのエントリはポートから除去されません。

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

ダイナミック ARP インスペクションの要件

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

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

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

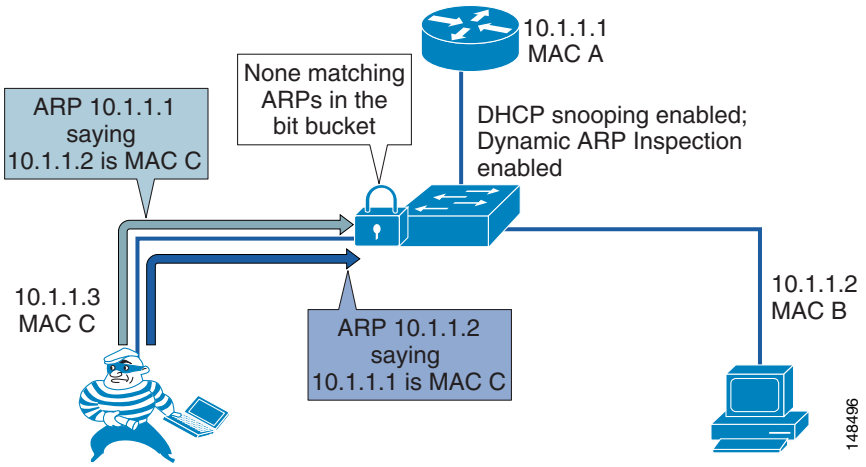
ただし、Gratuitous ARP は、別のステーションの身分を不正にかたること目的とした悪質なプログラムにより悪用される可能性もあります。悪質なステーションが、相互に通信しているその他の 2 つのステーションのトラフィックを自らにリダイレクトすると、GARP メッセージを送信したハッカーが中間者になります。ettercap などのハッカー プログラムは、このことを精密に行うため、GARP メッセージをブロードキャストするのではなく、「プライベートな」GARP メッセージを特定の MAC アドレスに発行します。これにより、攻撃の犠牲者は、自分のアドレスに対する GARP パケットを見ることが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

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

DAI の使用

ダイナミック ARP インスペクション（DAI）では、ARP 応答または Gratuitous ARP メッセージを正当化するために、DHCP バインディングが存在している必要があります。ホストで、アドレスを取得するための DHCP が使用されていない場合、そのホストを信頼するか、ホストの IP アドレスと MAC アドレスを対応付けるために ARP インスペクション用のアクセス コントロール リスト（ACL）を作成する必要があります（図 4-7 を参照）。DHCP スヌーピングと同様に、DAI は VLAN ごとに有効化されます。すべてのポートは、デフォルトで、信頼できないポートとして定義されます。DAI で DHCP スヌーピングからのバインディング情報を活用するには、DAI を有効化する前に、VLAN で DHCP スヌーピングを有効化する必要があります。DAI を有効化する前に DHCP スヌーピングを有効化しないと、VLAN 内のいずれのデバイスも、ARP を使用して、デフォルト ゲートウェイを含む VLAN 内の他のデバイスに接続できません。その結果、VLAN 内のすべてにデバイスに対するサービスを、自ら拒否することになります。

図 4-7　DHCP スヌーピングおよび DAI を使用した ARP 攻撃の防止



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

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

802.1X ポート ベースの認証

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

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

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

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

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

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

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

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

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

ほとんどの Cisco IP Phone では、EAP-Transport Layer Security（EAP-TLS）を使用した X.509 証明書による認証方式、または EAP-Flexible Authentication with Secure Tunneling（EAP-FAST）の認証方式をサポートしています。いずれの方式もサポートしていない一部の古いモデルでは、Cisco Catalyst スイッチが接続しているデバイスの MAC アドレスを認証方式として確認できるようにする MAC 認証バイパス（MAB）を使用して認証できます。

802.1X 機能設定のサポートを確認するには、https://www.cisco.com にある Cisco Unified IP Phone および Cisco Catalyst スイッチの製品ガイドを参照してください。

設定情報については、次の Web サイトで入手可能な『*IP Telephony for 802.1x Design Guide*』を参照してください。

https://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/IP_Tele/IP_Telephony_DIG.html

証明書管理

証明書は、シスコ コラボレーション導入でセキュアな接続を確立するために不可欠です。証明書を使用して、ネットワーク上の個人、コンピュータ、およびその他のサービスを認証することができます。証明書管理を適切に実装することにより、複雑さを軽減しながら、強力な保護を実現できます。

このセクションでは、最初に Public Key Infrastructure（PKI）の概要を示してから、一般的なガイダンスを提供します。

PKI の概要

Public Key Infrastructure（PKI）は、通信の安全を確保し、通信する両者の ID を検証するためのメカニズムを提供します。暗号化によって通信が保護され、公開/秘密キー ペアとデジタル アイデンティティ証明書を使用して ID が検証されます。

公開/秘密キーのペア

公開キーと秘密キーのペアは、数学的に相関された、2 つの一意に関連付けられた暗号キーで構成されます。公開キーで暗号化されたデータは、対応する秘密キー（一般に公開されない）でのみ復号化できます（逆も同様です）。

証明書

デジタル証明書は、ネットワーク上の個人、コンピュータ、およびその他のサービスの ID を認証するための電子クレデンシャルです。また、公開キーのラッパーでもあります。証明書は、公開キーの所有者に関する情報を提供します。通信相手を認証する TLS ハンドシェイクなどで使用されたり、ファイルにデジタル的に署名するために使用されたりします。シスコ コラボレーション製品と一緒に展開される証明書は、X.509 標準に基づいています。証明書には、次のような情報やその他の情報が含まれています。

- 公開キー
- 一般名 (CN)
- 組織名 (O)
- 発行元名
- 有効期間（それより前でも、それより後でもない）
- 拡張機能（オプション）：サブジェクト代行名（SAN）など

証明書は、自分で署名することも、認証局（CA）によって署名することもできます。

TLS ハンドシェイク中の証明書の検証

クライアントがサーバへの TLS 接続を開始すると、サーバはクライアントがサーバを認証できるように TLS ハンドシェイク中に自分の証明書を送信します。この動作は、管理者またはエンドユーザが Unified CM ページに接続したときに発生します。また、Jabber クライアントが起動して、Unified CM UDS サーバ、IM and Presence サーバ、Unity Connection サーバに接続したときなどに発生します。

サーバがクライアントを認証し、クライアントにその証明書の送信を依頼する場合もあります。これは相互認証（相互 TLS または MTLS）であり、暗号化モード（メディアとシグナリングの暗号化で設定）の Unified CM と Cisco エンドポイント間や、2 つの Unified CM クラスタを接続する SIP トランクや、Unified CM を Cisco Unity Connection、Cisco IOS ゲートウェイ、または Cisco Expressway（Expressway 上で TLS 検証が設定されている場合）に接続する SIP トランクで使用されます。

証明書の受信後の検証は、以下の項目のチェックで構成されます。

- ID — 証明書が発行される対象や ID は、セッションのイニシエータが意図した接続先の ID に一致しなければなりません。ホスト名（FQDN）は、共通名（CN）またはサブジェクト代行名（SAN）拡張機能に照らしてチェックされます。
- 有効期間 — 現在の時刻と日付が証明書の有効範囲内に収まっている必要があります。
- 証明書の失効ステータス。
- 信頼性 — 証明書が信頼できるものでなければなりません。署名（発行）当事者が信頼されている場合に、証明書は信頼できるものと見なされます。一般的に、署名当事者の信頼は、署名当事者の証明書を信頼できる証明書のストア（信頼ストア）にインポートすることにより確立されます。詳細については、自己署名証明書の代わりの CA 署名付き証明書（4-18 ページ）に関するセクションを参照してください。

証明書に関する一般的なガイダンス

Cisco Unified CM and IM and Presence Service などの一部のサーバは、システム サービスごとに異なる証明書を保持することができます。Cisco Expressway などの一部のサーバは、自分が提供しているサービスの証明書しか保持することができません。表 4-2 に、最も広く展開されている一部の製品のサーバ証明書を示します。ECDSA 証明書は掲載されていません。

表 4-2　一般的なシスコ コラボレーション コンポーネントのサーバ証明書

サービス	証明書	説明
Cisco Unified CM	Tomcat	セキュアな Web 接続に使用されます。LDAP、ILS、LBM などのサービスにも使用されます。
Cisco Unified CM	CallManager	CallManager サービスによるセキュアなシグナリングと、設定ファイルと ITL に署名する TFTP サービスに使用されます。
Cisco Unified CM	CAPF	エンドポイントが認証局プロキシ機能（CAPF）サービスに接続するときに必要です。
Cisco Unified CM	TVS	信頼検証サービス（TVS）に接続するときに必要です。
Cisco Unified CM	ITLRecovery	エンドポイントと Unified CM 間の信頼を回復するためのトラスト アンカーとして使用される証明書。ITL ファイルと CTL ファイルに保存されます。
Cisco Unified CM	ipsec	IPsec 接続用。IPsec を有効にすることができますが、このドキュメントでは説明しません。IPsec 証明書は、Cisco Unified CM ディザスタ リカバリ システム（DRS）にも使用されます。
Cisco Unified CM	authz	OAuth に使用されます
IM and Presence Service	Tomcat	SIP クライアント（Unified CM）、Web サービス、SOAP、LDAP 用
IM and Presence Service	cup	SIP プロキシ、プレゼンス エンジン、SIP フェデレーション用
IM and Presence Service	cup-xmpp	セキュア XMPP（IM）用
IM and Presence Service	cup-xmpp-s2s	セキュア XMPP フェデレーション用
IM and Presence Service	ipsec	IPsec 用。IPsec 証明書は、Cisco Unified CM ディザスタ リカバリ システム（DRS）にも使用されます。
Cisco Unity Connection	Tomcat	Unity Connection Web サービス証明書。ボイスメール ポート宛てのメディアとシグナリングの暗号化に使用されます。
Cisco Unity Connection	ipsec	IPsec 用
Cisco Expressway-C	サーバ	Expressway-C との間のセキュアな接続用
Cisco Expressway-E	サーバ	Expressway-E との間のセキュアな接続用
Cisco Meeting Server	データベース クライアント	データベースを備えていない Call Bridge サービスを使用した Cisco Meeting Server が、データベースを備えた Cisco Meeting Server ノードに安全に接続するために使用
Cisco Meeting Server	Web 管理、Call Bridge、XMPP、Web Bridge、データベース サーバ用の証明書	簡単にするために、すべての Cisco Meeting Server のノードとサービスに同じ証明書を使用することもできます。

表 4-2　一般的なシスコ コラボレーション コンポーネントのサーバ証明書（続き）

サービス	証明書	説明
Survivable Remote Site Telephony（SRST）、Cisco IOS ゲートウェイ、Cisco Unified Border Element	Cisco IOS 証明書	SRST を使用する場合は、SRST 証明書が各エンドポイントの設定ファイルに保存されます。
Cisco Prime Collaboration Deployment	Tomcat	Web サービス用
Cisco Prime Collaboration Provisioning	プロビジョニング	Web アクセスのプロビジョニング用

他にも ECDSA に基づく証明書があります。詳細については、RSA と ECDSA（4-17 ページ）に関するセクションを参照してください。

通常、シスコ コラボレーション サーバは、デフォルトで自己署名証明書と一緒にインストールされます。ただし、すべての製品に該当するわけではありません。たとえば、Cisco Meeting Server の場合は、デフォルトでは証明書がインストールされません。

Cisco Unified CM 自己署名証明書は 5 年間有効です。ただし、20 年間有効な ITLRecovery 証明書は除きます。この証明書はシステム全体のトラスト アンカーとして機能するため、その有効期間が長く設定されています。

RSA と ECDSA

通常、シスコ コラボレーション製品の証明書は、公開/秘密キーとデジタル署名用の RSA（Rivest、Shamir、and Adelman）に基づきます。一部の製品は楕円曲線デジタル署名アルゴリズム（ECDSA）証明書もサポートしており、自己署名証明書と CA 署名証明書の両方で使用できます。ECDSA 証明書と RSA 証明書の両方をサーバ上で共存させることができます。現時点では、エンドポイント上で ECDSA がサポートされていないことと、使いやすさや相互運用性を考慮すると、一般的に RSA 証明書を使用することが推奨されます。

（注）　キー交換が ECDHE に基づく暗号化アルゴリズム スイートには、ECDSA に基づく証明書は必要ありません。このスイートは、RSA に基づく証明書とネゴシエートできます。

自己署名証明書の代わりの CA 署名付き証明書

サーバのインストール時に、デフォルトで、自己署名証明書がほとんどのシスコ コラボレーション製品と一緒にインストールされます。自己署名証明書に基づいてサービスとの信頼性を確立するには、サービスへのセキュアな接続が必要なすべてのエンティティ（クライアント）の信頼できる証明書ストア（またはトラスト ストア）に、サーバの自己署名証明書をインポートする必要があります。インポートしていない場合は、接続を（Unified CM SIP トランクなどを使用して）開始するサーバを使用すると、接続に失敗します。Jabber と Web ブラウザを使用した場合は、警告メッセージが表示されますが、証明書を受け入れて信頼できる証明書ストアに追加することができます。ただし、クライアントの起動中に複数の証明書を受け入れるように何回もプロンプトが表示され、ユーザ エクスペリエンスが低下するため、この方法は使用しないでください。より重要なこととして、実際は、提示された証明書のフィンガープリントをチェックしてその証明書が正しいかどうかを検証することをほとんどのユーザは行わず、どの証明書もそのまま受け入れているのが現状です。これでは、セキュアなセッションを確立するための証明書ベースの認証のセキュリティの概念が成り立たなくなってしまいます。

通信する当事者のセットが少ない場合は自己署名証明書のインポートを処理できますが、通信ピアが多い場合は実用性に欠けます。これが、ほとんどのデフォルト自己署名証明書を CA 署名証明書に置き換えることが推奨されている主な理由です。これにより、証明書の管理が容易になります。CA 署名付き証明書を使用した場合は、クライアント トラスト ストアにそれぞれのサーバの証明書をインポートする必要がありません。代わりに、ルート CA 証明書をクライアント トラスト ストアにインポートするだけです。サーバ側では、通常、ルート CA 証明書もサーバ信頼ストアにインポートする必要があります。また、中間 CA が使用されている場合は、証明書チェーン内のすべての証明書もサーバ信頼ストアにインポートする必要があります。また、CA 署名付き証明書を使用すれば、署名する CA のルート証明書がすべてのクライアントの信頼できる証明書ストアにすでに追加されている限り、すべてのクライアントまたはサーバの信頼できる証明書ストアを更新しなくても、新しいサービス証明書を発行できます。CA 署名付き証明書は、マルチサーバ証明書を使用する場合の要件でもあります。

CA 署名付き証明書を使用するメリットの一例として、Jabber クライアントで自己署名証明書が使用されている場合は、すべてのノードの Unified CM Tomcat 証明書（UDS 用と TFTP 設定ファイルのダウンロード用）、IM and Presence Tomcat 証明書と cup-xmpp 証明書（ログインとセキュアなチャット用）、Unity Connection Tomcat 証明書（ビジュアル ボイス メール用）を Jabber を実行している各クライアントのトラスト ストアにインポートする必要があります。一方、CA 署名付き証明書を使用した場合は、署名する CA のルート証明書をインポートするだけで済みます。

一般に、自己署名証明書の代わりの CA 署名付き証明書の使用は、Tomcat 証明書に最もメリットがあります。これは、この証明書が、広く使用されている、ユーザが直接関わる証明書だからです。CallManager 証明書に CA 署名付き証明書を使用した場合もメリットがあります。これは、マルチサーバ証明書（詳細については、マルチサーバ証明書（4-19 ページ）を参照）を使用することができ、SIP トランク経由で Unified CM サブスクライバに接続するすべてのエンティティのすべての CallManager 証明書をインポートする必要がないためです。

さらに、CA を使用してすべての証明書に署名する必要がありません。一部の証明書は、内部操作にのみ使用され、ユーザの介入なしに、それらを必要とするエンティティに提供されます。たとえば、Trust Verification Service（TVS）証明書は、初期信頼リスト（ITL）ファイルに保存されており、エンドポイントの起動、再起動、またはリセット時に自動的にダウンロードされます。同様に、ITL 回復証明書は、証明書信頼リスト（CTL）と初期信頼リスト（ITL）に含まれています。つまり、外部 CA を使用してこれらの証明書に署名するメリットはありません。また、外部 CA によって CAPF 証明書に署名しても、実質的なメリットはありません。認証局プロキシ機能（CAPF）証明書またはエンドポイントのローカルで有効な証明書（LSC）の失効はサポートされません。また、電話機 VPN または 802.1 x を設定する場合は、ASA または RADIUS サーバのトラスト ストアにルート CA 証明書をインポートするだけでは不十分です。TLS ハンドシェイク中はエンドポイントが証明書チェーンを送信しない（そのため、CAPF 証明書が送信されない）ため、CAPF 証明書も引き続きインポートする必要があります。

表 4-3 に、CA によって署名するように推奨されている証明書を示します。

表 4-3　CA によって署名するように推奨されている証明書の例

製品	証明書	注記
Cisco Unified CM and IM and Presence Service	Tomcat	Web インターフェイスにアクセスする管理者とユーザや UDS にアクセスしてログインする Jabber などのさまざまな用途に使用されます。
Cisco Unified CM	CallManager	SIP トランクなどのさまざまな用途に使用されます。
Cisco Unified CM	ipsec	IPsec が使用されている場合のみ
IM and Presence Service	xmpp	
IM and Presence Service	xmpp-s2s	
Cisco Unity Connection	Tomcat	Web インターフェイスにアクセスする管理者とユーザやビジュアル ボイスメールにアクセスする Jabber などのさまざまな用途に使用されます。
Cisco Expressway-C	サーバ	
Cisco Expressway-E	サーバ	パブリック CA を使用します。
Survivable Remote Site Telephony（SRST）と Cisco IOS ゲートウェイ	SRST と Cisco IOS ゲートウェイ	
Cisco Unified Border Element	Cisco IOS	通常は、エンタープライズ CA を使用します。SIP サービス プロバイダーが暗号化をサポートしている場合は、パブリック CA を使用します。
Cisco Meeting Server	サーバ	
Cisco Meeting Server	データベース クライアント	
Cisco TelePresence Management Suite（TMS）	サーバ	
Cisco Prime Collaboration Deployment	Tomcat	
Cisco Prime Collaboration Provisioning	プロビジョニング	

マルチサーバ証明書

証明書の管理をさらに容易にするために、マルチサーバ証明書を使用することができます。ノードごとに証明書を使用する代わりに、クラスタ内のすべてのノード全体で 1 つの CA 署名証明書を使用することができます。1 つの対応する秘密キーもすべてのノードで使用され、自動的にノード全体に伝播されます。マルチサーバ証明書でカバーされるサーバは、サブジェクト代行名（SAN）拡張機能で一覧表示されます。マルチサーバ証明書を実装するには、導入でサードパーティ CA を使用する必要があります。

表 4-4 に示すように、可能な場合はマルチサーバ証明書の使用をお勧めします。

表 4-4　マルチサーバ証明書のサポート

製品	証明書	注記
Unified CM and IM and Presence Service	Tomcat	1 つのクラスタ内のすべての Unified CM および IM and Presence ノード全体で 1 つの Tomcat 証明書。証明書署名要求（CSR）を生成し、Unified CM パブリッシャ ノードに CA 発行証明書をアップロードします。
Unified CM	CallManager	
IM and Presence Service	xmpp	
IM and Presence Service	xmpp-s2s	
Unity Connection	Tomcat	

（注）　ワイルドカード証明書は、通常、シスコ コラボレーション製品ではサポートされません。

パブリック CA とプライベート CA の比較

Expressway-E 証明書にパブリック CA を使用するという要件に加えて、パブリック CA またはエンタープライズ CA（プライベート CA または内部 CA）を使用して、このドキュメント内のシスコ コラボレーション製品のさまざまな証明書に署名することもできます。パブリック CA を使用するメリットには、一部のクライアントとサーバがデフォルトで主要なパブリック CA をすでに信頼しているために、これらのデバイスとパブリック CA 間で信頼を確立する（CA 証明書をクライアント トラスト ストアにインポートする）必要がないという事実が含まれます。パブリック CA を使用すれば、IT 組織も内部 CA サーバを設置して維持する必要がありません。ただし、パブリック CA の主な欠点は、証明書を発行するコストと、一部のパブリック CA で課される制限です。

お勧めは、パブリック CA によって署名される必要がある Expressway-E 証明書と、SIP サービス プロバイダーが暗号化をサポートしている場合の Cisco Unified Border Element 証明書を除いて、表 4-2 内のすべての証明書に対してエンタープライズ CA を使用することです。詳細については、https://www.cisco.com/go/pa にある『*Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments CVD*』の最新版の「*Security*」の章を参照してください。

暗号化

内部ネットワークを越えて拡張するサービスが増えていることと、内部ネットワークが内部からの攻撃に晒される場合があることから、暗号化と認証がますます不可欠になりつつあります。

暗号化は、盗聴、改ざん、セッション リプレイなどの攻撃から保護します。権限のないユーザがトラフィックをキャプチャすることができても、暗号化キーを知らなければ、暗号化された通信の内容を復号化したり、変更したりすることができません。また、暗号化は、暗号化された通信のセットアップ時にデジタル証明書経由の認証も提供します。認証は、一方向の認証にすることができます。たとえば、管理者またはエンドユーザが Web ブラウザを使用して Web サービスにアクセスする場合です。この場合は、クライアント（ブラウザ）が Web サーバを認証しますが、サーバはクライアント（ブラウザ）を認証しません。または、相互 TLS（MTLS）を使用して認証を双方向にすることができます。この場合は、サーバもクライアントを認証します。MTLS は、エンドポイントとそれが登録されている Unified CM サーバ間のシグナリングや Unified CM SIP トランクなどで使用されます。

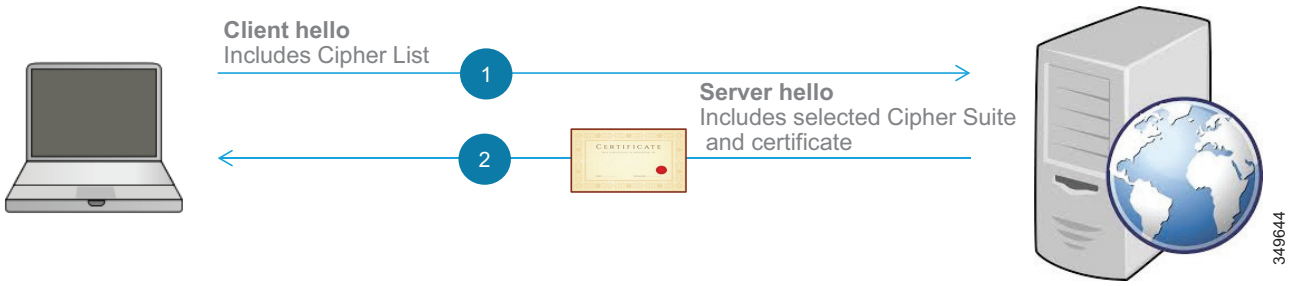
TLS の概要

Transport Layer Security（TLS）は、TCP トラフィックを暗号化するための方式で、Web サービス トラフィックや SIP シグナリングに広く使用されています。以下の手順は、TLS セッションの確立方法に関する概要を示しています。

1. TLS 接続が、TLS サーバに接続する TLS クライアントによって開始されます。クライアントは、最初に、乱数とその機能を含む Client Hello を送信して、サーバとの TCP 接続を確立します。これらの機能には、クライアントがサポートしている暗号スイートのリストが含まれます。
2. TLS サーバは、通常、クライアントの暗号スイートの設定を考慮して暗号スイートの 1 つを選択し、Server Hello で応答します。このメッセージには、クライアントが認証できるように、別の乱数とサーバ証明書も含まれています。

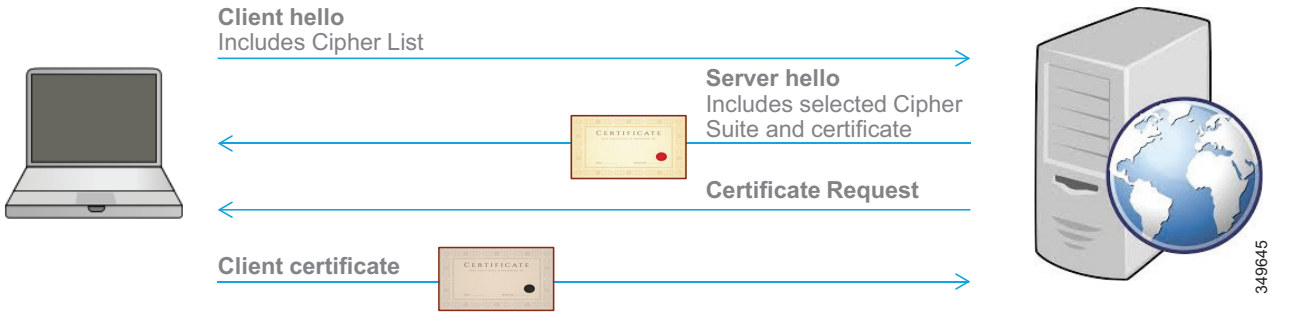
図 4-8 に、TLS セッションを確立するためのこの 2 つの手順を示します。簡略化するため、この図には TLS ハンドシェイクのすべてのメッセージと可能性のあるバリエーションが含まれているわけでありません。サーバ証明書は、Server Hello メッセージで送信することも、別に送信することもできます。

図 4-8　TLS ハンドシェイク



相互 TLS（MTLS）を使用すると、サーバもクライアントを認証します。サーバは、CertificateRequest をクライアントに送信し、クライアントからクライアント証明が送信されます。図 4-9 に、このフローの概要を示します。

図 4-9　MTLS ハンドシェイク



RSA を使用する場合は、クライアントがプリマスター シークレットをサーバの公開キーで暗号化して、サーバに送信します。Diffie-Hellman（DH）キー合意アルゴリズムを使用する場合は、プリマスター シークレットがネットワーク経由で送信されません。代わりに、クライアントとサーバが自力でプリマスター シークレットを抽出できるように、クライアントとサーバがデータ（乱数から計算され、認証用の秘密キーによって署名された）を交換します。DH と変化する乱数を組み合わせること（Diffie-Hellman Ephemeral）により、Perfect Forward Secrecy（PFS）が可能になります。

そうすれば、マスター シークレットが抽出され、セッション キーがマスター シークレットから計算されます。この時点から、クライアントとサーバが公開/秘密キーのペアの使用（非対称暗号化）を停止して、暗号化用の共有セッション キーの使用（対称暗号化）を開始します。

TLS は、セキュアなさまざまな通信リンクを保護するために使用されます。たとえば、SIP または Skinny Client Control Protocol（SCCP）シグナリングを保護するために使用されます。

現在のシスコ コラボレーション製品の多くが TLS バージョン 1.2 をサポートしています。これらの製品を使用すれば、TLS 1.0 と TLS 1.1 もサポートしていたとしても、TLS バージョン 1.2 が常にネゴシエートされるはずです。セキュリティやコンプライアンスの観点から、管理者は TLS のバージョンを 1.2 に固定し、TLS 1.0 と TLS 1.1 を無効にすることもできます。これは、多くのシスコ コラボレーション製品で行うことができます。この機能を備えた製品の一覧については、次の場所にある『*TLS 1.2 Compatibility Matrix for Cisco Collaboration Products*』を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html

また、TLS 1.2 のサポートと、TLS 1.0 または 1.1 の無効化の詳細については、次の場所にある『*TLS 1.2 for On-Premises Cisco Collaboration Deployments*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-configuration-examples-list.html

クレジットカード データ保護基準（PCI DSS）にも、TLS のバージョンに関する要件があります。詳細については、https://www.cisco.com/go/collabpci を参照してください。

メディアは、IETF RFC 3711 で定義されているセキュア RTP（SRTP）を使用して保護されます。

Cisco Unified CM セキュリティ

強化プラットフォーム

Cisco Unified CM と他のシスコ コラボレーション製品は、Linux OS に基づいて強化されたアプライアンスと同じプラットフォーム運用に基づいており、次のようなデフォルトの機能と制限があります。

- ルート アカウントが無効になっています。
- サードパーティ製ソフトウェアのインストールが許可されません。
- ホストベースの侵入からの保護（SELinux）とホストベースのファイアウォール（IPTables）がインストールされ、デフォルトで有効になっています。

  SELinux ソフトウェアは、サーバとの間のトラフィックの動作と、サーバ上でアプリケーションが実行される方法を調べて、すべてが正常かどうかを判別するポリシーを実行します。異常と見なされるものが見つかった場合、SELinux アクセス ルールは、そのアクティビティが発生するのを防ぎます。

  DoS 保護のための接続レート制限、および特定のポートをブロックするネットワーク シールドは、IPTables を使用して設定されます。ホストベースのファイアウォール設定には、Cisco Unified Communications サーバの [Operating System Administration] ページを使用してアクセスできます。

管理者は、SELinux をディセーブルにできませんが、許可モードに設定できます。厳密にトラブルシューティングの目的のためだけに許可モードにする必要があります。SELinux をディセーブルにするにはルート アクセスが必要で、Cisco Technical Assistance Center（TAC）からのリモート サポートによってのみ実行できます。

- 複雑なパスワード ポリシーが管理アカウントに適用されます。
- セキュアな管理インターフェイス（HTTPS、SSH、SFTP）が強制されます。さらに、ユーザをアクセス制御グループに割り当てることにより、特定の役割、管理者、エンドユーザ、アプリケーション ユーザに必要な権限のみを付与することができます。
- すべてのインストール パッケージは署名されて、OS とアプリケーションの両方を含めます。
- 問題発生時に現象を特定するために不可欠なシステム監査ロギングを利用できます。

メディアとシグナリングの暗号化用の Unified CM 混合モード

Unified CM を初めてインストールすると、「非セキュア モード」と呼ばれる状態になります。ほとんどのセキュリティ機能が実際にこのモードで利用可能であっても、そのように呼ばれます。たとえば、署名された TFTP 設定ファイル、暗号化された TFTP 設定ファイル、署名された電話ファームウェア、Web サービスへの HTTPS アクセス、ローカルで有効な証明書（LSC）をインストールするための CAPF 登録、SIP トランク暗号化、電話 VPN、802.1x のすべてをデフォルトで非セキュア モードの Unified CM で使用することができます。欠けている 1 つのセキュリティ機能がエンドポイント用のメディアとシグナリングの暗号化です。これを有効にするには、Unified CM を混合モードに設定する必要があります。そのためには、Unified CM をソフトウェアの米国輸出制限バージョンを使用してインストール（Unified CM の無制限バージョンではメディアとシグナリングの暗号化が使用できない）し、エクスポート制御機能を使用してシスコ スマート ソフトウェア ライセンスの登録トークンを作成する必要があります。

混合モードを有効にする方法には次の 2 つがあります。

- ハードウェア USB eToken

  これは、混合モードを有効するための従来の方法です。この方法では、最低でも 2 つのハードウェア USB eToken（KEY-CCM-ADMIN-K9= または新しい KEY-CCM-ADMIN2-K9=）が必要です。1 つの eToken は、証明書信頼リスト（CTL）ファイルの署名に使用されます。もう 1 つの eToken は、最初の eToken が失われたまたは使用できなくなった場合に冗長性を提供します。混合モードを有効にするには、CTL クライアント ソフトウェアを Microsoft Windows デスクトップにインストールする必要があります。この CTL クライアント ソフトウェアの動作中に、USB eToken をデスクトップに挿入する必要があります。混合モードの設定が完了すると、Unified CM クラスタ用の CTL ファイルが作成され、USB eToken が削除され、オフラインにされます。

- トークンレス（ソフトウェア eToken）

  この方法では、USB トークンや Microsoft Windows デスクトップが必要ありません。混合モードが CLI コマンド **utils ctl set-cluster mixed-mode** を介して簡単に有効になります。CTL ファイルは、ハードウェア USB eToken によって署名されませんが、Unified CM ITLRecovery 秘密キーによって署名されます。

トークンレス方式は、一般に推奨されており、次のようなメリットがあります。

- 混合モードの有効化と CTL ファイルの更新が容易です。混合モードを有効にするときや CTL ファイルを更新するときに、USB eToken を取得したり、Microsoft Windows デスクトップに CTL クライアントをインストールしたり、CTL クライアントを実行したりする必要がありません。1 つの CLI コマンドを発行する必要があるだけです。
- トークンレス方式では、CTL ファイルを署名するキーが長くなります。
- TLS 1.0 および 1.1 は、トークンレス オプションを使用して Unified CM 上で無効にすることができます。USB ハードウェア eToken を使用した場合は、CTL クライアントが TLS 1.1 または 1.2 をサポートしないため、TLS 1.0 を許可する必要があります。

Cisco Unified CM 12.0 以降では、トークンレス CTL ファイル（および ITL ファイル）が ITLRecovery 秘密キーによって署名されるため、CallManager 証明書の更新がもはや懸案材料ではなく、エンドポイントと Unified CM 間の信頼が失われないことに注意してください。

証明書信頼リスト（CTL）と初期信頼リスト（ITL）

証明書信頼リスト（CTL）と初期信頼リスト（ITL）は、Unified CM 証明書を含むファイルです。これらのファイルは、Cisco エンドポイントの起動、再起動、リセット時にダウンロードされます。これらの信頼リストを使用して、エンドポイントは、Unified CM サービスに対する信頼を構築するための Unified CM 証明書の最小セットを取得することができます。ITL ファイルは、Unified CM クラスタが非セキュア モードなのか混合モードなのかに関係なく、Unified CM クラスタ内に存在します。ただし、CTL ファイルは、Unified CM が混合モードの場合にのみ存在し、関連付けられます。

CTL ファイルと ITL ファイルは、システム管理者セキュリティ トークン（SAST、表 4-5 を参照）によって署名され、レコードのリストが保存されます。各レコードには、エンドポイントが容易に検索を行えるように、証明書、証明書の役割または機能、事前に抽出された証明書フィールドが含まれています。表 4-5 に、証明書の役割を示します。

表 4-5　CTL ファイルと ITL ファイル内の証明書の役割

証明書の役割	証明書	説明
TFTP	CallManager	Unified CM TFTP サーバを認証するため。たとえば、TFTP 設定ファイルの署名の確認に使用されます。この証明書の役割を持つレコードは、Unified CM が混合モードでないときに、ITL ファイルに保存されます。
CCM+TFTP	CallManager	シグナリングが暗号化された CallManager サービスを認証して、TFTP 設定ファイルの署名の確認時に Unified CM TFTP サーバを認証するため。この証明書の役割を持つレコードは、Unified CM が混合モードのときに、ITL ファイルと CTL ファイルに保存されます。
System Administrator Security Token（SAST）	ITLRecovery と CallManager	CTL、ITL、TFTP 設定ファイルに署名するエンティティである、SAST を認証するため。この種のレコードは、ITL ファイルと CTL ファイルに保存されます。ITL ファイルとトークンレス CTL ファイルは、ITLRecovery キーによって署名されます。TFTP 設定ファイルは、TFTP サーバの CallManager 秘密キーによって署名されます。
Certificate Authority Proxy Function（CAPF）	CAPF	CAPF とのセキュアな通信中に CAPF サービスを認証するため。この証明書の役割を持つレコードは、CAPF サービスが Unified CM パブリッシャでアクティブになっている場合に、ITL ファイルと CTL ファイルに保存されます。
信頼検証サービス（TVS）	TVS	TVS に接続するときに TVS サービスを認証するため。ITL ファイル内にのみ存在します。

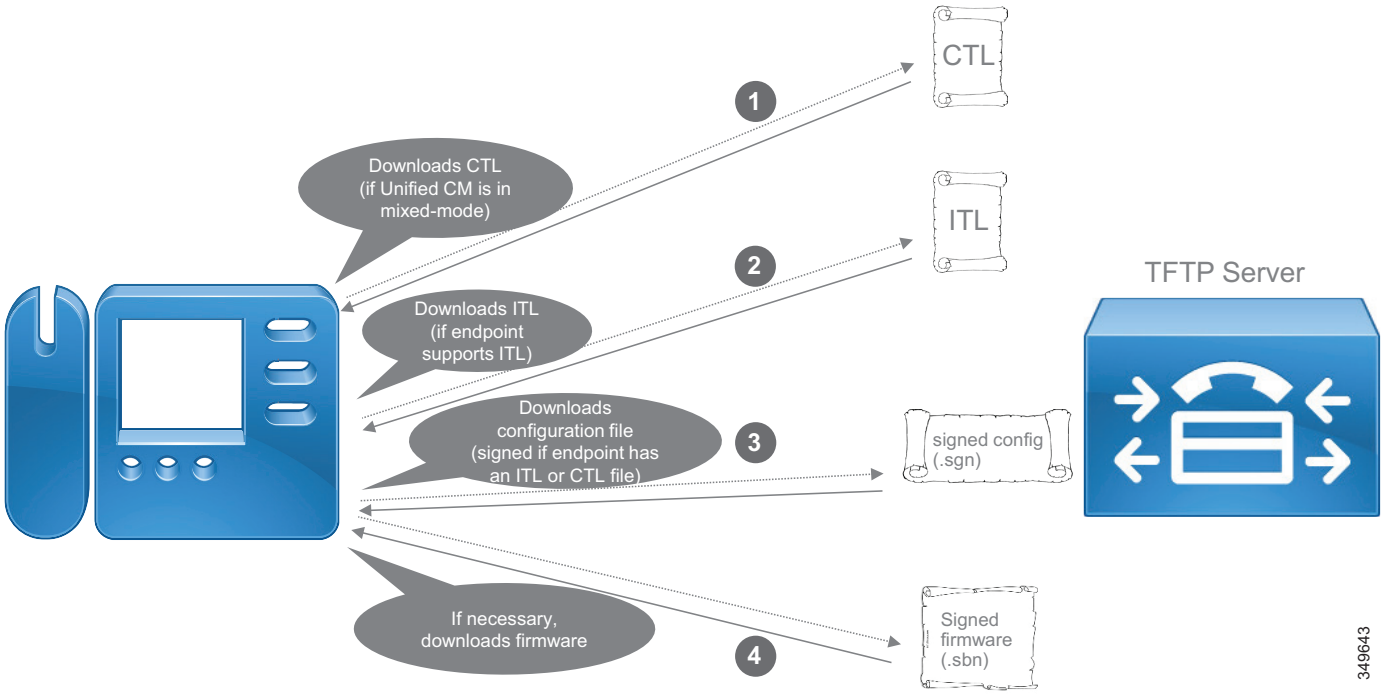
ITL は ITLRecovery 秘密キーによって署名されます。TFTP サービスを実行している Unified CM ノードごとに、エンドポイントに提供される個別の ITL ファイルが割り当てられます。

CTL ファイルは、システム管理者セキュリティ トークン（SAST）の秘密キーによって署名されます。トークンレス CTL を使用する場合は、SAST が ITLRecovery 秘密キーになります。Unified CM クラスタ全体で共有される CTL ファイルは 1 つだけです。

Unified CM が混合モードの場合は、エンドポイントを起動またはリセットすると、その設定ファイルがダウンロードされる前に、TFTP サーバから証明書信頼リスト（CTL）がダウンロードされます。ITL がエンドポイントによってサポートされている場合は、その後で、TFTP サーバの初期信頼リスト（ITL）がダウンロードされます。ほとんどの Cisco エンドポイントは、いくつかの稀な例外（主な例外は Jabber）を除いて、ITL ファイルをサポートします。エンドポイントが新しく展開され、エンドポイントが初めて Unified CM に接続した場合は、既存の CTL ファイルまたは ITL ファイルが存在しないため、CTL 署名または ITL 署名の検証に使用可能な証明書のリストも存在しません。その場合は、エンドポイントが、根拠はないものの 1 回だけ CTL/ITL ファイルを信用して受け入れ、それらのファイルの一部である証明書を保存します。エンドポイントに証明書の信頼できるリストが存在する場合は、それらを使用して、ダウンロードされる後続の CTL ファイルと ITL ファイルの署名を検証することができます。

エンドポイントが ITL をサポートしている場合または Unified CM が混合モード（エンドポイントによって CTL ファイルがダウンロードされる）の場合は、エンドポイントが ITL/CTL ファイルからの CallManager 証明書を所有しているため、Unified CM TFTP サーバ上で CallManager 秘密キーによって署名された設定ファイルを要求します。そうでない場合（Jabber を使用している場合や Unified CM が混合モードでない場合）は、署名されていない設定ファイルを要求します。その設定ファイルをダウンロードすると、エンドポイントは、正しいファームウェアが含まれているかどうかを確認します。正しいファームウェアが含まれていない場合は、該当するファームウェアをダウンロードして、その署名を検証し、それが改ざんされていないことを確認します。図 4-10 に、エンドポイントの起動時にダウンロードされるファイルを示します。

図 4-10　起動中にエンドポイントによってダウンロードされるファイル



TFTP 設定ファイルの暗号化

TFTP 設定ファイルの暗号化を使用しない場合は、任意の Unified CM TFTP サーバから TFTP 設定ファイルをプレーン テキスト形式で入手できます。TFTP 設定ファイルから入手可能な情報の種類には、電話ファームウェア情報や Unified CM クラスタに関する情報などが含まれます。さらに重要なことは、Unified CM Administration の電話ページでユーザ名とパスワードがプロビジョニングされた場合は、それらも TFTP 設定ファイルにプレーン テキストで保存されることです。したがって、一般的な推奨事項は、TFTP 設定ファイルの暗号化を有効にすることです。このことは、ユーザ名、パスワード、機密情報が Unified CM Administration の電話ページで設定される場合に特に重要です。

ただし、モバイルおよびリモート アクセス（MRA）エンドポイントを使用し、TFTP 設定ファイルの暗号化が設定されている場合は、MRA エンドポイントが、MIC を所有している場合でも、インターネットに展開されたり MRA 経由で接続されたりする前に、オンプレミスに展開されてから Unified CM に直接登録される必要があります。さらに、Jabber を使用している場合、エンドポイントはリセットされると、暗号化された設定ファイルを取得できなくなり、社内ネットワーク内に戻されるまで登録できなくなります。このような理由で、MRA 経由で接続しているエンドポイントの場合、特に、MRA 経由で接続している Jabber エンドポイントの場合は、TFTP 設定ファイルの暗号化を有効にしない方が簡単です。ただし、このようなエンドポイントに対して機密情報が設定されていないことを確認してください。結論として、このような MRA エンドポイントの場合は TFTP 設定ファイルの暗号化を無効にして（かつパスワードをプロビジョニングせず）、社内ネットワーク内のエンドポイントの場合は TFTP 設定ファイルの暗号化を有効にすることをお勧めします。これは、オンプレミス エンドポイントの場合は TFTP 設定の暗号化が有効になっている電話セキュリティ プロファイルを使用し、モバイルおよびリモート アクセス（MRA）経由で接続しているエンドポイントの場合は TFTP 設定が無効になっている別の電話セキュリティ プロファイルを使用することによって実現されます。

Survivable Remote Site Telephony（SRST）

Cisco IOS SRST は、Unified CM クラスタから離れたロケーションにあるエンドポイントに、可用性の高い呼処理サービスを提供します。エンドポイントが Unified CM 呼処理サーバとの通信を確立できない場合は、ローカル SRST ルータに登録されます。SRST は、非セキュアにもセキュアにも設定することができます。SRST がセキュアとして設定されている場合は、Unified CM で暗号化モードに設定されたエンドポイントが SRST ルータに登録したときにメディアとシグナリングが暗号化されます。

セキュア SRST が Unified CM で設定されると、Unified CM がデフォルトでポート 2445 の TLS 接続を介して SRST ルータ内の証明書プロバイダー サービスに接続し、SRST ルータの証明書を取得します。この証明書は、エンドポイントが SRST にフェールオーバーしたときに、SRST ルータを正しく認証できるように、エンドポイント TFTP 設定ファイルに追加されます。SRST ルータもエンドポイントを認証します。そのため、エンドポイント証明書に署名したエンティティの証明書を SRST 信頼ストアにインポートする必要があります。LSC 証明書がエンドポイントにインストールされており、CAPF によって署名されている場合は、CAPF 証明書を SRST 信頼ストアにインポートする必要があります。代わりに、電話機で MIC 証明書が使用されている場合は、Cisco Manufacturing 証明書を SRST 信頼ストアにインポートする必要があります。

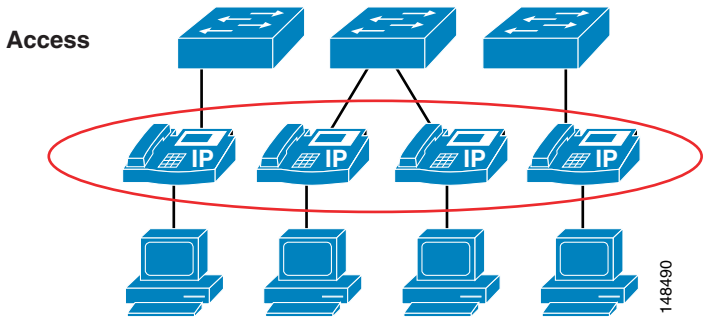
詳細については、次の場所にある『*Cisco Unified SCCP and SIP SRST System Administrator Guide*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-installation-and-configuration-guides-list.html

エンドポイント セキュリティ

Cisco Unified IP Phone には、IP テレフォニー ネットワーク上のセキュリティを強化するための組み込み型の機能があります。これらの機能を電話機単位で有効または無効にして、IP テレフォニー配置のセキュリティを強化できます。セキュリティ ポリシーは、電話機の配置に応じて、これらの機能を有効にする必要があるかどうか、および有効にする必要がある場所を判別するのに役立ちます（図 4-11 を参照）。

図 4-11　電話機レベルでのセキュリティ



次のセキュリティに関する留意点は IP 電話機に適用されます。

- 電話機の PC ポート（4-28 ページ）
- PC の音声 VLAN へのアクセス（4-28 ページ）
- 電話機経由の Web アクセス（4-29 ページ）
- 設定へのアクセス（4-29 ページ）
- 認証および暗号化（4-31 ページ）
- IP Phone の VPN クライアント（4-32 ページ）

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

https://www.cisco.com/c/en/us/support/collaboration-endpoints/index.html

Cisco Unified IP Phone 7800 および 8800 シリーズに関するセキュリティ情報の詳細については、次の場所にある『*Cisco IP Phone 7800 and 8800 Series Security Overview White Paper*』を参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html

電話機の PC ポート

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

セキュリティ ポリシーおよび電話機の配置状況によっては、特定の電話機の背面にある PC ポートを無効にする必要があります。このポートを無効にすると、電話機の背面にデバイスを接続したり、電話機自体を介してネットワークにアクセスしたりできなくなります。ロビーのような一般的なエリアに設置した電話機の場合、通常はポートを無効にします。ロビーでは物理的なセキュリティが非常に弱いため、ほとんどの企業では、制御されていないポートから不特定のユーザがネットワークにアクセスするのを許可しません。セキュリティ ポリシーで、電話機の PC ポートを経由してデバイスがネットワークにアクセスするのを許可しない場合は、通常の作業エリアに設置した電話機でも、ポートを無効にすることがあります。配置された電話機のモデルによっては、Cisco Unified Communications Manager（Unified CM）は、電話機の背面の PC ポートを無効にできます。この機能の有効化を試みる前に、次のリンクで入手可能なマニュアルを参照して、特定の Cisco Unified IP Phone モデルでこの機能がサポートされていることを確認してください。

https://www.cisco.com/c/en/us/support/collaboration-endpoints/index.html

PC の音声 VLAN へのアクセス

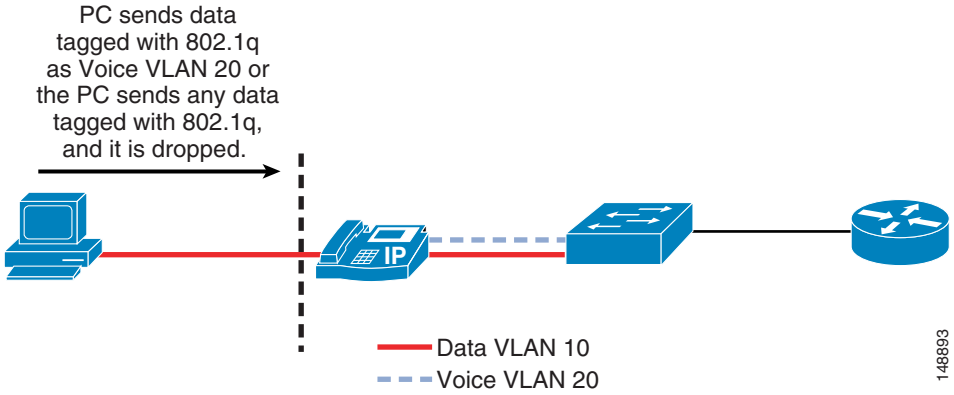
スイッチから電話機までに 2 つの VLAN が存在するので、電話機は、望まないアクセスから Voice VLAN を保護する必要があります。電話機では、電話機の背面から Voice VLAN に入り込む、望まないアクセスを防止できます。PC Voice VLAN Access 機能は、電話機の背面にある PC ポートから Voice VLAN への任意のアクセスを防止します。この機能を無効にすると、電話機の PC ポートに接続されたデバイスが、電話機の背面の PC ポートに到達する Voice VLAN を宛先とした 802.1q タグ付き情報を送信することにより、VLAN を「ジャンプ」して Voice VLAN にアクセスすることは許可されません。設定している電話機に応じて、この機能は 2 つの方法のいずれかで動作します。高機能の電話機では、電話機の背面の PC ポートに着信する Voice VLAN を宛先とした、すべてのトラフィックをブロックします。図 4-12 に示す例の場合、PC が、電話機の PC ポートに対して Voice VLAN トラフィック（このケースでは 200 の 802.1q タグ付き）の送信を試行すると、そのトラフィックはブロックされます。この機能が動作する他の方法は、電話機の PC ポートに着信する、802.1q タグ付きのすべてのトラフィック（Voice VLAN トラフィックに限らない）をブロックする方法です。

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

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

https://www.cisco.com/c/en/us/support/collaboration-endpoints/index.html

図 4-12　電話機の PC ポートから Voice VLAN へのトラフィックのブロック



電話機経由の Web アクセス

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

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

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

Unified CM は、IP フォンとの間の Web トラフィックに HTTPS のみ、もしくは HTTPS と HTTP の両方を使用するように設定できます。ただし、HTTPS だけが設定されている場合でも、IP フォンの Web サーバのポート 80 は自動的に閉じません。HTTP トラフィックを制限するために ACL を使用することが望ましい場合、Unified CM で HTTPS のみ使用するようにします。

設定へのアクセス

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

このアクセスを個々の電話機ごとに、または一括管理を使用して無効にすることにより、エンドユーザまたは攻撃者が、Unified CM IP アドレスや TFTP サーバ情報などの追加情報を取得することを防止できます。電話機設定ページへのアクセスを無効にすると、エンド ユーザは、スピーカー ボリューム、連絡先、呼び出しタイプなど、通常は制御可能な多くの電話機設定を変更できなくなります。電話機インターフェイスについてエンド ユーザに課される制限により、このセキュリティ機能を使用することが現実的ではない場合があります。このアクセスは制限付きとして設定することができます。これにより、ネットワーク設定情報へのアクセスはできなくなりますが、音量や呼出音などの設定はできます。

電話設定ページの詳細については、次の場所にある『*Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*』の最新版を参照してください。

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

Cisco TelePresence エンドポイントの強化

Cisco TelePresence のエンドポイントには攻撃に対してそれらを保護するための複数の設定オプションがあります。セキュリティ機能はエンドポイント間で異なり、デフォルトですべてが有効になっているわけではありません。これらの機能には、次のものがあります。

- HTTPS および SSH 経由の安全な管理
- 管理パスワード
- デバイス アクセス
- シグナリングおよびメディア暗号化

Cisco TelePresence のエンドポイントは、Secure Shell（SSH）および Secure Sockets Layer を介したハイパーテキスト転送プロトコル（HTTPS）経由の管理をサポートします。HTTP、HTTPS、SSH、または Telnet を使用したエンドポイントへのアクセスは、エンドポイント自体の [ネットワークサービス（Network Services）] の設定で設定できます。

エンドポイントはデフォルトの管理パスワード付きで出荷されますが、インストール時にパスワードを変更することを推奨します。管理機能へのアクセスは管理者権限を持つユーザに制限する必要があります。デフォルトの管理パスワードが使用されていると、ビデオ ストリームはこのパスワードで管理ページにアクセスできるすべてのユーザに表示されます。

エンドポイントは、定義済みの役割と権限に基づいてアクセスを提供されたユーザに割り当てることができます。こうしたユーザが SSH または Telnet および Web ベース アクセスを実現できるように、パスワードおよび PIN を指定できます。パスワードを定期的に失効させ、変更するとともに、アイドル状態のときにログインをタイムアウトにするために、クレデンシャル管理ポリシーを実装する必要があります。これは、デバイスへのアクセスを検証済みのユーザに限定するために必要です。

認証および暗号化

Cisco Collaboration ソリューションは、Transport Layer Security（TLS）および Secure Real-time Transport Protocol（SRTP）を使用し、シグナリングとメディア暗号化を行います。

トランスポート レイヤ セキュリティ（TLS）

Transport Layer Security（TLS）プロトコルは、2 つのアプリケーション間の通信の認証、データ整合性、および機密性を提供するように設計されています。TLS はクライアント/サーバ モードで動作し、「サーバ」として動作する側面と「クライアント」として動作する側面を持ちます。TLS には、信頼性の高いトランスポート層プロトコルとして動作する TCP が必要です。

シスコ コラボレーション デバイスは、Unified CM に接続するときに、TLS を使用して SIP または Skinny Client Control Protocol（SCCP）シグナリングを保護します。

Secure Real-Time Transport Protocol（SRTP）

IETF RFC 3711 に定義されている Secure RTP（SRTP）は、Real-time Transport Protocol（RTP）の音声メディアとビデオ メディアの両方と、対応する Real-time Transport Control Protocol（RTCP）ストリームの機密性およびデータの整合性を提供する方法を詳しく説明します。SRTP は、暗号化とメッセージ認証ヘッダーを使用してこれを実現します。

SRTP では、暗号化は RTP パケットのペイロードだけに適用されます。ただし、メッセージ認証は RTP のヘッダーと RTP のペイロードの両方に適用されます。ヘッダー内の RTP シーケンス番号にメッセージの認証が適用されるため、SRTP はリプレイ アタックに対しても間接的に保護を提供します。SRTP 暗号方式には、Advanced Encryption Standards（AES）256 または 128、およびセキュア ハッシュ アルゴリズム（SHA）2 での Encryption with Associated Data（AEAD）が含まれています。AES 128 および SHA-1 でのハッシュベースのメッセージ認証コードに基づく SRTP 暗号方式も、設定で禁止されていない場合は、ネゴシエートできます。

音声およびビデオ システム

Unified CM では、音声システム内の電話機に対して複数のレベルのセキュリティを実現するように設定できます。ただし、電話機でこれらの機能がサポートされている必要があります。これには、X.509 証明書を使用したデバイス認証およびメディアとシグナリングの暗号化が含まれます。導入済みのセキュリティ ポリシー、電話機の配置、および電話機サポートに応じて、社内の必要に合せてセキュリティを設定できます。

電話機と Unified CM クラスタでセキュリティを有効にするには、次の場所にある『*Security Guide for Cisco Unified Communications Manager*』の最新版を参照してください。

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

Unified CM で公開キー インフラストラクチャ（PKI）セキュリティ機能が正しく設定されている場合、サポートされているすべての電話機で、次の機能を使用できます。

- 完全性：この機能が有効な場合は、TFTP 署名ファイルを使用した TFTP ファイル操作は許可しませんが、電話機への Transport Layer Security（TLS）シグナリングは許可します。
- 認証：電話機のイメージは、Unified CM から電話機に対して認証され、デバイス（電話機）は Unified CM に対して認証されます。電話機と Unified CM の間のすべてのシグナリング メッセージは、認可されているデバイスから送信されるときに検証されます。
- 暗号化：サポートされているデバイスで、盗聴を防止するためシグナリングとメディアを暗号化できます。TFTP ファイルも暗号化することができます。
- Secure Real-time Transport Protocol（SRTP）：Cisco IOS ゲートウェイでサポートされています。電話機間通信でもサポートされています。Cisco Unity もボイスメールのための SRTP をサポートしています。

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

https://www.cisco.com/c/en/us/support/collaboration-endpoints/index.html

Unified CM では ID を保護し、暗号化を有効にするために証明書を使用します。エンドポイント上の証明書は、製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）のどちらかにすることができます。MIC はほとんどのハードウェア エンドポイント上にプレインストールされており、LSC は Unified CM の Cisco Certificate Authority Proxy Function（CAPF）によってインストールされます。MIC を使用する場合、Cisco CA 証明書および Cisco Manufacturing CA 証明書はルート証明書として機能します。ネイティブで登録されたエンドポイント用の LSC が生成された場合は、通常は CAPF によって署名され、CAPF 証明書がルート証明書になります。サードパーティ認証局（CA）を使用して LSC 証明書に署名することもできます（サードパーティ製の CA 証明書（4-32 ページ）に関するセクションを参照）。

シグナリングとメディアのエンドポイントでの暗号化には Unified CM での混合モードが必要です。Unified CM 混合モードの詳細については、Cisco Unified CM セキュリティ（4-22 ページ）に関するセクションを参照してください。

Cisco TelePresence Management Suite（TMS）は TLS 証明書を提供して、アウトバウンド接続を生成するときにその ID を確認します。

IP テレフォニー トラフィックがファイアウォールおよびネットワーク アドレス変換（NAT）を通過するのを可能にするアプリケーション層プロトコル検査およびアプリケーション層ゲートウェイ（ALG）も、シグナリングが暗号化されていると動作しません。暗号化されたメディアでは、一部のゲートウェイ、電話機、または会議はサポートされません。

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

サードパーティ製の CA 証明書

デフォルトで、エンドポイントに発行された LSC 証明書は Unified CM 内の CAPF サービスによって署名されます。ただし、サードパーティ製の CA 署名済み LSC もサポートしています。このようなサポートを実装するには、Unified CM の信頼ストアにサードパーティ製の CA 証明書をインポートし、エンドポイントの証明書発行者としてオフシステム CA を使用するように Unified CM の CAPF サービスを設定します。この方式では、すべての電話機の証明書署名要求（CSR）を処理し、サードパーティ CA でそれらに署名してもらってから、電話機に再びインポートするという手間もかかります。

IP Phone の VPN クライアント

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

Cisco Unified IP Phone 内の VPN クライアントは、Cisco SSL VPN テクノロジーを使用しており、Cisco ASA 5500 シリーズ VPN ヘッドエンドと Cisco IOS SSL VPN ソフトウェア機能を備えた Cisco サービス統合型ルータの両方に接続できます。音声トラフィックは VPN トンネルの一部として、UDP および Datagram Transport Layer Security（DTLS）プロトコルによって伝送されます。統合された VPN トンネルは、音声および IP Phone Service だけに適用されます。PC ポートに接続された PC はこのトンネルを使用できず、PC からのトラフィック用に独自の VPN トンネルを確立する必要があります。

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

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

VPN クライアント用の電話機の設定手順については、次の場所にある『*Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*』の最新版を参照してください。

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

(注)　テレワーカーおよび小規模オフィスまたはホーム オフィス（SOHO）の場合は、Cisco Expressway を使用した電話機ベースの VPN、ルータベースの VPN、または Mobile and Remote Access の導入を推奨します。

Quality of Service（QoS）

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

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

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

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

QoS の詳細については、ネットワーク インフラストラクチャ（3-1 ページ）と、次の Web サイトで入手可能な QoS の設計ガイドを参照してください。

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-ipv6/design-guide-listing.html

アクセス コントロール リスト

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

VLAN アクセス コントロール リスト

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

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

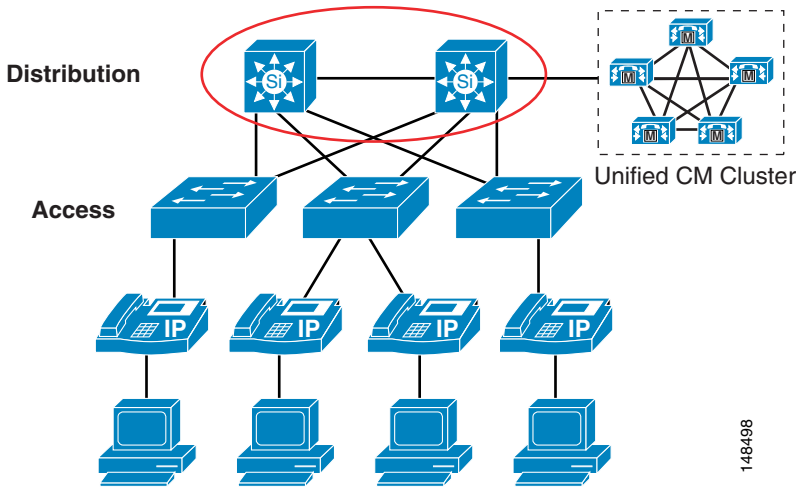
ACL は、VLAN に入るまたは VLAN から出るネットワーク トラフィックを制御する機能、および VLAN 内でトラフィックを制御する機能を提供します。

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

ルータのアクセス コントロール リスト

VLAN ACL と同様、ルータにも、ポートごとにインバウンド ACL およびアウトバウンド ACL の両方を処理する機能があります。最初のレイヤ 3 デバイスは、音声およびデータ VLAN を使用するときの音声データと別タイプのデータとの間の境界ポイントです。境界ポイントでは、2 つのタイプのデータが、相互にトラフィックを送信することが許可されます。VLAN ACL とは異なり、ルータ ACL は、ネットワーク内のすべてのアクセス デバイスには配置されません。その代わり、ネットワーク全体にルーティングするすべてのデータを準備する場所である、エッジ ルータで適用されます。これは、各 VLAN のデバイスがネットワーク内でアクセス可能なエリアを制御するために、レイヤ 3 ACL を適用するのに最適な場所です。レイヤ 3 ACL をネットワーク全体に配置することにより、トラフィックが収束する場所で、デバイスを相互に保護できます（図 4-13 を参照）。

図 4-13　　レイヤ 3 のルータ ACL



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

https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html

導入済みのセキュリティ ポリシーに応じて、レイヤ 3 ACL は、非 Voice VLAN からの IP トラフィックがネットワーク内の音声ゲートウェイにアクセスするのを禁止するという単純な設定にも、他のデバイスが IP テレフォニー デバイスと通信するために使用する個別のポートや時間帯を制御するという詳細な設定にもできます。ACL が高精度および詳細になると、ネットワーク内のポート使用法の変更が原因で、音声だけでなく、ネットワーク内の他のアプリケーションも遮断される場合があります。

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

特定のサブネットに制限され、音声 VLAN に限定される IP Phone の場合、Unified CM、音声ゲートウェイ、電話機、および音声のみのサービスに使用されるその他のあらゆる音声アプリケーションへの（IP アドレスまたは IP 範囲による）すべてのトラフィックをブロックするように ACL を記述できます。この方法により、レイヤ 3 ACL を、レイヤ 2 または VLAN ACL よりも簡素化できます。

ファイアウォール

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

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

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

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

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

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

（注）　ペイロード暗号化モジュールのない ASA は、ユニファイド コミュニケーション機能を無効にします。

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

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

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

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

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

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

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

https://www.cisco.com

ルーテッド ASA

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

https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html

ルーテッド ASA ファイアウォールは、QoS、NAT、およびボックスへの VPN 終端をサポートしています。これらの機能は、トランスペアレント モードではサポートされていません（トランスペアレント ASA（4-38 ページ）を参照）。ルーテッド設定では、ASA 上の各インターフェイスに IP アドレスが与えられます。トランスペアレント モードでは、ASA をリモートで管理するための IP アドレスの他には、インターフェイス上に IP アドレスは与えられません。

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

トランスペアレント ASA

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

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

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

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

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

トランスペアレント モードの詳細については、次の場所にある最新の ASA 構成ガイドを参照してください。

https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html

（注）　トランスペアレント モードで NAT を使用する場合は、ASA バージョン 8.0(2) 以降が必要です。詳細については、https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-release-notes-list.html にある『*Cisco ASA 5500 Series Release Notes*』を参照してください。

音声およびビデオのネットワーク アドレス変換

ネットワーク アドレス変換（NAT）デバイスは、社内のプライベート IP アドレスをパブリック インターネットで表示されるパブリック IP アドレスに変換します。社内のエンドポイントは内部エンドポイントであり、パブリック インターネットのエンドポイントは外部エンドポイントです。

社内デバイスが NAT 経由で接続する場合、NAT はそのデバイスにパブリック IP アドレスを動的に割り当てます。このパブリック IP アドレスは *public mapped address* または *reflexive transport address* とも呼ばれます。NAT がパブリック インターネット上のデバイスにこのパケットを転送すると、パケットはその割り当てられたパブリック アドレスから送信されたように見えます。外部デバイスがパブリック アドレスで NAT にパケットを返送する場合、NAT は、IP アドレスを内部プライベート アドレスに変換し、内部ネットワークにパケットを転送します。

NAT の機能は通常、ファイアウォールの一部であり、したがって、NAT/FW と呼ばれることがあります。NAT は、多数の内部のプライベート IP アドレスを少数の外部のパブリック IP アドレスにマッピングします。現在のパブリック IPv4 アドレス空間は限定的で、ユビキタスなプロトコルとして IPv6 が出現するまで、ほとんどの企業では利用可能なパブリック IPv4 アドレス数が制限されています。NAT により、多数のエンドポイントを持つ企業が少ないパブリック IP アドレスで運用できるようになります。NAT は、外部 IP アドレスに内部 IP アドレスを動的にマッピングすることにより、内部エンドポイントが NAT 経由で接続をするたびにこの機能を実行します。これらのマッピングはそれぞれ、NAT のバインディングと呼ばれます。

音声デバイスおよびビデオ デバイスに対して実行される NAT が複雑化する主な原因は、音声とビデオのシグナリング プロトコルがプロトコル シグナリング メッセージに送信元アドレスおよびポートを含むことにあります。これらの送信元アドレスは、リモート エンドポイントが応答パケットに使用する宛先アドレスを提供します。ただし、内部エンドポイントはプライベート アドレス空間のアドレスを使用し、アプリケーション層ゲートウェイ（ALG）を使用しない NAT はこれらの内部アドレスを変更しません。リモート エンドポイントがメッセージを受信しても、メッセージのプライベート IP アドレスへパケットをルーティングすることはできません。この問題を解決するには、パケットの内容を検査して、シグナリング メッセージにカプセル化されたメディアの IP アドレスとポート番号に対してアドレス変換を実行可能な NAT デバイスで ALG（SIP や SCCP などの「フィックスアップ」）を有効にする必要があります。

NAT ALG はファイアウォール ALG に似ていますが、NAT ALG はシグナリング メッセージのアドレスとポートを実際に変更します。NAT ALG は、暗号化されたシグナリング メッセージの内容は検査できません。

データセンター

データセンター内では、IP テレフォニー アプリケーション サーバで必要なセキュリティについて、セキュリティ ポリシーを定義する必要があります。Cisco Unified Communications サーバは IP に基づいているので、データセンター内にある、時間に敏感な他のデータに適用するセキュリティを、これらのサーバにも適用できます。

データセンターの間で WAN でのクラスタリングが使用されている場合、データセンター内とデータセンター間の両方に適用されている追加のセキュリティは、クラスタ内のノード間で許可されている最大往復時間に収まる必要があります。WAN を介したクラスタリングを使用するマルチサイトまたは冗長データセンター実装では、アプリケーション サーバに関する現行のセキュリティ ポリシーでデータセンターのファイアウォールをまたぐサーバ間のトラフィックを保護するように要求されている場合は、すでに展開済みのインフラストラクチャ セキュリティ システム間のこのトラフィックに対して IPSec トンネルを使用することを推奨します。

データ アプリケーションに適切なデータセンター セキュリティを設計するには、次の場所にある『*Data Center Technology Design Guide*』に記載されたガイドラインに従うことをお勧めします。

https://www.cisco.com/c/en/us/solutions/enterprise/data-center-designs-data-center-networking/index.html#~designs~tab-designs

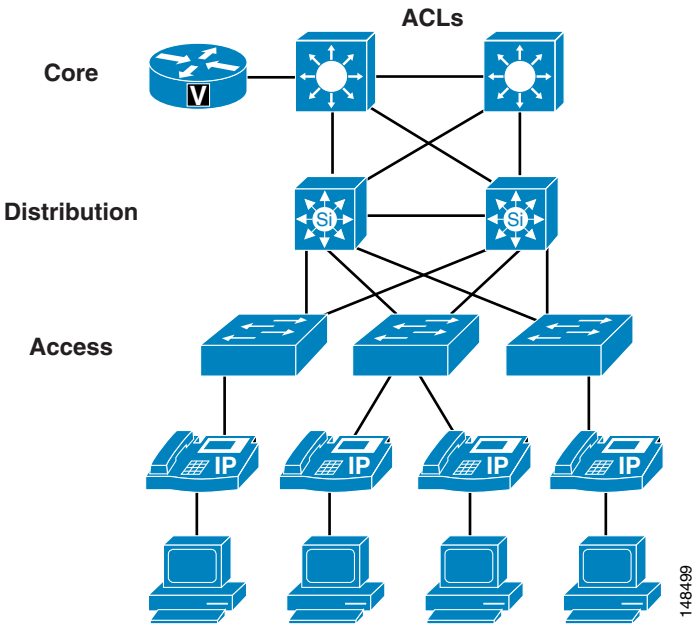
ゲートウェイ、トランク、およびメディア リソース

ゲートウェイおよびメディア リソースは、IP テレフォニー コールを PSTN コールに変換するデバイスです。外部コールがかけられた場合、ゲートウェイまたはメディア リソースは、IP テレフォニー ネットワークにおいてすべての音声 RTP ストリームが流れる数少ない場所の 1 つです。

IP テレフォニー ゲートウェイおよびメディア リソースは、ネットワーク内のほぼすべての場所に配置できるので、導入済みのセキュリティ ポリシーによっては、IP テレフォニー ゲートウェイまたはメディア リソースを保護することが、他のデバイスを保護することより難しいと見なされる場合があります。しかし、ネットワーク内のどこで信頼が確立されているかによりますが、ゲートウェイおよびメディア リソースを簡単に保護できる場合もあります。ゲートウェイおよびメディア リソースが Unified CM により制御される方法が関係していますが、シグナリングがゲートウェイまたはメディア リソースに到達するために通るパスがネットワーク内で安全と見なされている部分にある場合、単純な ACL を使用して、ゲートウェイまたはメディア リソースに送る、またはそこから戻るシグナリングを制御できます。ゲートウェイ（またはメディア リソース）と Unified CM のロケーションの間のネットワークが安全と見なされない場合は（ゲートウェイがリモートの支店に置かれている場合など）、インフラストラクチャを使用してゲートウェイおよびメディア リソースへの IPSec トンネルを構築することにより、シグナリングを保護できます。ほとんどのネットワークでは、通常、2 つの方式（ACL および IPSec）の組み合わせを使用して、これらのデバイスが保護されています。

ここでは、ネットワークのエッジで QoS を使用しているので、攻撃者が Voice VLAN に侵入してゲートウェイおよびメディア リソースの場所を判別できた場合、ポートの QoS により、攻撃者がゲートウェイまたはメディア リソースに送信できるデータの量が制限されます（図 4-14 を参照）。

図 4-14　IPSec、ACL、および QoS を使用したゲートウェイおよびメディア リソースの保護



電話機で SRTP を有効にしている場合、一部のゲートウェイおよびメディア リソースでは、電話機からのゲートウェイおよびメディア リソースに対する Secure RTP（SRTP）をサポートします。ゲートウェイまたはメディア リソースが SRTP をサポートしているかどうかを判別するには、次の Web サイトで入手可能な適切な製品マニュアルを参照してください。

https://www.cisco.com

IPSec トンネルの詳細については、次の場所にある『*IPSec VPN WAN Design Overview*』を参照してください。

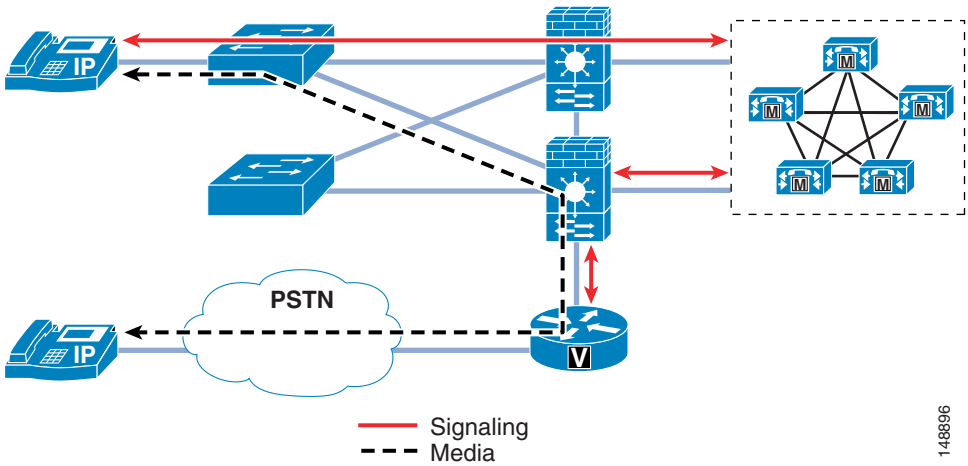
https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-ipv6/design-guide-listing.html

ゲートウェイの周囲へのファイアウォールの配置

コールの送信元である電話機と、PSTN ネットワークへのゲートウェイとの間にファイアウォールを配置する場合、注意が必要な問題が生じます。ステートフル ファイアウォールは、Unified CM、ゲートウェイ、および電話機の間のシグナリング メッセージの内容を参照し、コールの実行を許可するための RTP ストリーム用のピンホールを開けます。通常の ACL で同じことを行うには、RTP ストリームで使用されるポート範囲全体を、ゲートウェイに対して開放する必要があります。

ネットワーク内にゲートウェイを配置する方法は 2 つあります。つまり、ファイアウォールの背後に配置する方法と、ファイアウォールの前面に配置する方法です。ゲートウェイをファイアウォールの背後に配置する場合、そのゲートウェイを使用している電話機からのすべてのメディアは、ファイアウォールを通過する必要があります。また、これらのストリームがファイアウォールを通過するようにするには、追加の CPU リソースが必要です。次に、ファイアウォールでは、これらのストリームの制御が追加され、ゲートウェイが DoS 攻撃から保護されます（図 4-15 を参照）。

図 4-15　ファイアウォールの背後に配置されたゲートウェイ



ゲートウェイを配置する 2 番めの方法は、ファイアウォールの外側に配置する方法です。電話機からゲートウェイに送信される唯一のデータ タイプは RTP ストリームなので、そのゲートウェイに送信可能な RTP トラフィックの量は、アクセス スイッチの QoS 機能により制御されます。Unified CM からゲートウェイに送信されるのは、コールをセットアップするためのシグナリングだけです。ネットワーク内で、信頼できるエリアにゲートウェイが配置されている場合、Unified CM とゲートウェイの間で許可する必要がある唯一の通信は、そのシグナリングです（図 4-15 を参照）。RTP ストリームはファイアウォールを通過しないので、この配置方式では、ファイアウォールの負荷が低下します。

ACL とは異なり、ほとんどのファイアウォール設定では、シグナリングがファイアウォールを経由している限り、Unified CM が電話機とゲートウェイに対して、それらの 2 つのデバイスの間で使用するように指示している RTP ストリーム ポートだけが開放されます。また、ファイアウォールには、DoS 攻撃用の追加機能や、対象トラフィックを参照して、攻撃者が禁止動作を行っていないかどうかを判別するための Cisco 侵入防御システム（IPS）シグニチャがあります。

ファイアウォール（4-35 ページ）の項で説明するように、ファイアウォールが、電話機からゲートウェイへのすべてのシグナリングおよび RTP ストリームを調べる場合、キャパシティが問題になることがあります。また、音声データ以外のデータがファイアウォールを通過する場合、ファイアウォールを通過するコールがファイアウォールにより影響されないように、CPU 使用率をモニタする必要があります。

安全な音声およびビデオ会議

Cisco IOS Enhanced Conference Bridge と Cisco Meeting Server は、セキュアな会議を提供します。Unified CM、そのエンドポイント、および Cisco Meeting Server ノード間でメディアとシグナリングの暗号化を実装するには、Unified CM サーバと Cisco Meeting Server ノード間に SIP トランクをセキュア SIP トランクとして設定する必要があります。SIP トランク設定は、SRTP を許可するように設定する必要もあります。Cisco Meeting Server 証明書、つまり、CA 署名付き証明書が使用されている場合の CA 証明書は Unified CM CallManager と Tomcat の信頼ストアにアップロードする必要があり、SIP トランク プロファイルで証明書の共通名を X.509 サブジェクト名として設定する必要があります。同様に、CallManager 証明書、つまり、CA 署名付き証明書が使用されている場合の CA 証明書は、Cisco Meeting Server 信頼ストアにアップロードする必要があります。

この設定によって、Cisco Unified CM と Cisco Meeting Server 間の管理トラフィックのセキュアなシグナリングと HTTPS の両方が有効になります。

Cisco Unified Border Element と Unified CM トランクの統合

Unified CM トランクによって、企業ネットワークと外部ネットワークの間に IP 接続ポイントが追加されます。これらの相互接続に追加のセキュリティ対策を適用して、データおよび IP テレフォニー アプリケーションに固有の脅威を軽減する必要があります。Unified CM トランクと外部ネットワークの間に Cisco Unified Border Element を実装することが、より柔軟でセキュアな相互運用性オプションとなります。

Cisco Unified Border Element は、音声アプリケーション境界と音声トラフィックとデータ トラフィックの両方に適用できるセキュリティ脅威軽減技術を提供する Cisco IOS ソフトウェア機能です。Cisco Unified Border Element は、Cisco IOS ファイアウォール、認証、および VPN 機能とともに同じデバイス上で設定でき、サービス プロバイダー ネットワークまたはその他の外部ネットワークと統合された Unified CM トランクのセキュリティを強化できます。これらの Cisco IOS セキュリティ機能は、外部の攻撃に対する防御として、およびルータを通過してサービス プロバイダーのネットワークへ出ていく内部トラフィックのチェックポイントとしての役割を果たします。サービス プロバイダーまたはサービス プロバイダーのネットワークに接続されたネットワークから発生した不正アクセス、DoS 攻撃、または分散型 DoS（DDoS）攻撃を防ぐために、および侵入やデータ盗用を防ぐために、インフラストラクチャ アクセス コントロール リスト（ACL）を使用することもできます。

Cisco Unified Border Element は、シグナリングおよびメディアのネットワーク トポロジを隠蔽する機能を提供するバックツーバック ユーザ エージェント（B2BUA）です。ネットワークのセキュリティと処理上の独立性を有効にし、すべてのトラフィックで Cisco Unified Border Element IP アドレスを置き換えることで NAT サービスを提供します。

Cisco Unified Border Element は、ネットワーク間のメディアおよびシグナリング パケットで DSCP QoS パラメータを再マーキングするために使用できます。これにより、トラフィックはネットワーク内で QoS ポリシーに従うようになります。

Cisco IOS ファイアウォール機能は、Cisco Unified Border Element との組み合わせで使用され、シグナリング メッセージを一致させてトラフィックを管理するために Application Inspection and Control（AIC）を提供します。これは、SIP トランク DoS 攻撃を防ぐのに役立ち、コンテンツおよびレート制限に基づくメッセージ フィルタリングを可能にします。

Cisco Unified Border Element によって SIP トランク登録が可能です。この機能は、Unified CM SIP トランクでは使用できません。

Cisco Unified Border Element は、背後にあるエンドポイントに代わって、企業ネットワークの E.164 DID 番号をサービス プロバイダーの SIP トランクに登録できます。ネットワークの E.164 DID 番号をプロキシするために Cisco Unified Border Element を使用する場合、実際のエンドポイントのステータスはモニタされません。したがって、登録解除されたエンドポイントが引き続き使用可能として表示される場合があります。

Cisco Unified Border Element は、外部ネットワーク経由で SRTP を使用して RTP 企業ネットワークを接続できます。これにより、企業内に SRTP を配置しなくても安全な通信が可能になります。RTP-SRTP インターワーキングもサポートしますが、G.711 mulaw、G.711 alaw、G.729abr8、G.729ar8、G.729br8、G.729r8 など、少数のコーデックに制限されます。

特定の SIP サービス プロバイダーでは、コール サービスが許可される前に、SIP トランクへの登録が必要です。これにより、コールは既知のエンドポイントだけから発生するようになり、企業とサービス プロバイダー間のサービス ネゴシエーションはよりセキュアになります。Unified CM は、SIP トランクでの登録をネイティブにはサポートしませんが、Cisco Unified Border Element を使用することによってこのサポートを実現できます。Cisco Unified Border Element は、Cisco Unified Communications Manager に代わって、企業の電話番号を使用してサービス プロバイダーに登録します。

Cisco Unified Border Element の設定および製品詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

- https://www.cisco.com/c/en/us/products/unified-communications/unified-border-element/index.html
- https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html

DMZ 内の Cisco Expressway

Cisco Expressway は、企業のネットワークの外側にあるデバイスと、Expressway をコラボレーション エッジとして機能させたインターネットを介して、ビデオ コミュニケーション コールを確立できます。外部発信者がデバイスにアクセスできるようにするには、Cisco Expressway-E を Cisco Collaboration ソリューションで使用されるプライベート ネットワークの外側に配置する必要があります。これは、パブリック インターネット上または非武装地帯（DMZ）に配置できます。Expressway-E が DMZ 内に展開されている場合は、インターネットと Expressway-E 間のトラフィックを許可するようにファイアウォールを設定する必要があります。Expressway-C は Expressway-E とペア化され、通常は、データセンター内に展開されます。Expressway-E と組み合わせることにより、コラボレーション用のファイアウォール トラバーサルが容易になります。

Expressway-C は Cisco Unified CM 用の SIP プロキシおよびコミュニケーション ゲートウェイです。これには Expressway-E と通信するトラバーサル クライアント ゾーンが設定されており、NAT デバイスを通過するインバウンドおよびアウトバウンド コールを許可します。Expressway-E はリモート（エンタープライズ ネットワークの外部）に存在するデバイスの SIP プロキシです。これは、パブリック ネットワークのドメイン名で設定されます。

Cisco Expressway は、HTTPS、SIP TLS、ならびに Cisco Unified CM、LDAP、および syslog サーバへの接続に X.509 証明書を使用します。この導入では、信頼された CA 証明書のリストを使用し、サードパーティの CA が署名した証明書の使用が優先されます。これにより、Expressway-C、Expressway-E、および Unified CM との間での証明書の設定と交換が簡略化され、管理のオーバーヘッドが低減されます。物理エンドポイントがモバイルおよびリモート アクセス（MRA）を介して接続されている場合は、Expressway-E 証明書をパブリック サードパーティ CA によって署名する必要があります。これは、これらのエンドポイントがルート CA 証明書の組み込み信頼リストを使用して Expressway-E 証明書を検証するためです。

アプリケーション サーバ

Unified CM セキュリティ機能のリストとそれらの有効化方法については、次の場所にある『*Security Guide for Cisco Unified Communications Manager*』の最新版を参照してください。

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

任意の Unified CM セキュリティ機能を有効にする前に、それらの機能が、ネットワーク内のこれらのタイプのデバイスに関する企業セキュリティ ポリシーで指定されている、セキュリティ要件を満たしていることを確認してください。詳細については、次の Web サイトにある『*Cisco ASA 5500 Series Release Notes*』を参照してください。

https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-release-notes-list.html

シングル サインオン

シングル サイン オン（SSO）機能は、より強力な認証とより良いユーザ エクスペリエンスを可能にします。シスコ コラボレーション ソリューションで使用される SSO、SAML 認証、OAUTH プロトコルの詳細については、ディレクトリ統合とアイデンティティ管理（16-1 ページ）に関する章を参照してください。

Unified CM およびアプリケーション サーバの SELinux

Unified CM プラットフォームをベースにした Cisco Unified Communications システム アプリケーション サーバは、Security Enhanced Linux（SELinux）をホスト侵入防止ソフトウェアとして使用します。詳細については、Cisco Unified CM セキュリティ（4-22 ページ）の項を参照してください。

サーバに関する一般的なガイドライン

Cisco Unified CM とその他のコラボレーション アプリケーション サーバは、通常のサーバとして扱わないようにする必要があります。システムの設定時に行う任意の操作が、開始を試みているコール、または進行中のコールに影響する場合があります。他のビジネスクラス アプリケーションと同様、大規模な設定の変更は、電話の会話を遮断することがないようメンテナンス時間帯で行う必要があります。

アプリケーション サーバ用の標準のセキュリティ ポリシーは、コラボレーション サーバには適合しない可能性があります。電子メール サーバや Web サーバとは異なり、音声サーバでは、画面をリフレッシュしたり、メッセージを再送信したりすることは許可されていません。音声通信は、リアルタイムのイベントです。コラボレーション サーバ用のセキュリティ ポリシーでは、音声システムの設定または管理に関連しない作業がコラボレーション サーバで絶対に行われないことを保証する必要があります。ネットワーク内のアプリケーション サーバで通常のアクティビティと見なされるアクティビティ（インターネット サーフィンなど）は、コラボレーション サーバ上で実行しないようにする必要があります。

加えて、シスコはコラボレーション サーバ用に適切に定義されたパッチ システムを提供しています。IT 組織内のパッチ ポリシーに基づいて、このシステムを適用する必要があります。シスコにより承認されている場合を除き、OS ベンダーのパッチ システムを使用する通常の方法でシステムにパッチを適用しないでください。すべてのパッチは、シスコの指示に従ってシスコまたは OS ベンダーからダウンロードし、パッチ インストール プロセスに応じて適用する必要があります。

導入済みのセキュリティ ポリシーで、デフォルト インストールで提供された以上の OS のロック ダウンが要求されている場合は、OS の強化手法を使用する必要があります。

セキュリティ アラートを受信するには、次の Web サイトでシスコの通知サービスに登録できます。

https://www.cisco.com/go/support/

配置例

この項では、ロビーに設置された電話機およびファイアウォールの配置について、セキュリティ面を考慮した実施例を示します。このようなタイプと同様の配置を扱うには、適切なセキュリティ ポリシーを適用する必要があります。

ロビーに設置された電話機の例

この項の例は、物理的なセキュリティが低いロビー エリアのようなエリアで使用する、電話機およびネットワークを設定する 1 つの方法を示しています。この例に出てくる機能は、いずれもロビーに設置する電話機で要求されている機能ではありませんが、導入済みのセキュリティ ポリシーで、より強固なセキュリティが必要とされている場合は、この例でリストされている機能を使用できます。

いずれのユーザも電話機の PC ポートからネットワークにアクセスできないようにするため、電話機の背面の PC ポートを無効にして、ネットワーク アクセスを制限する必要があります（電話機の PC ポート（4-28 ページ）を参照）。また、攻撃を仕掛けようとしている人が、ロビーに設置された電話の接続先ネットワークの IP アドレスを参照できないように、電話機の設定ページも無効にする必要があります（設定へのアクセス（4-29 ページ）を参照）。電話機の設定を変更できないという欠点は、通常、ロビーに設置された電話機では問題になりません。

ロビーに設置された電話機が移動される可能性は非常に低いため、電話機には固定 IP アドレスを使用できます。固定 IP アドレスを使用すると、攻撃者が電話機を切断して接続することにより新しい IP アドレスを取得するのを防止できます（IP アドレッシング（4-4 ページ）を参照）。また、電話機が抜かれると、ポートの状態が変化し、電話機は Unified CM から登録解除されます。ロビーに設置された電話機のポートでこのイベントをトラッキングするだけで、誰かがネットワークへの接続を試行しているかどうかを判別できます。

電話機のスタティック ポート セキュリティを使用し、MAC アドレスを取得することを許可しない場合、攻撃者は、そのアドレスを発見できたときに、自らの MAC アドレスをその電話機の MAC アドレスに変更しなければなりません。ダイナミック ポート セキュリティを無制限タイマーと共に使用して、MAC アドレスを取得する（取得したアドレスは解除しない）場合、MAC アドレスを追加する必要はありません。これにより、電話機を交換しない限り、MAC アドレスをクリアするためにスイッチ ポートを変更せずに済みます。MAC アドレスは、電話機の底面のラベルにリストされています。MAC アドレスをリストすることがセキュリティの問題と見なされる場合は、ラベルを除去し、デバイスを識別するための Lobby Phone というラベルに置き換えることができます（スイッチ ポート（4-6 ページ）を参照）。

ポートまたはポートが接続されているスイッチに関する情報を攻撃者がイーサネット ポートから参照できないように、単一の VLAN を使用し、ポートで Cisco Discovery Protocol（CDP）を無効にできます。この場合、電話機の E911 緊急コール用のスイッチに CDP エントリは与えられません。緊急番号をダイヤルするときは、ロビーに設置された各電話機に、ラベル、またはローカル セキュリティ用の情報メッセージのいずれかが必要です。

ポート上に DHCP は存在しないため、DHCP スヌーピング バインディング テーブルに静的エントリを定義できます（DHCP スヌーピング：不正な DHCP サーバ攻撃の防止（4-9 ページ）を参照）。DHCP スヌーピング バインディング テーブルに静的エントリを定義すると、VLAN でダイナミック ARPインスペクションを有効にして、攻撃者が、ネットワーク上のレイヤ 2ネイバーの 1 つに関する他の情報を取得するのを防止できます（ダイナミック ARP インスペクションの要件（4-11 ページ）を参照）。

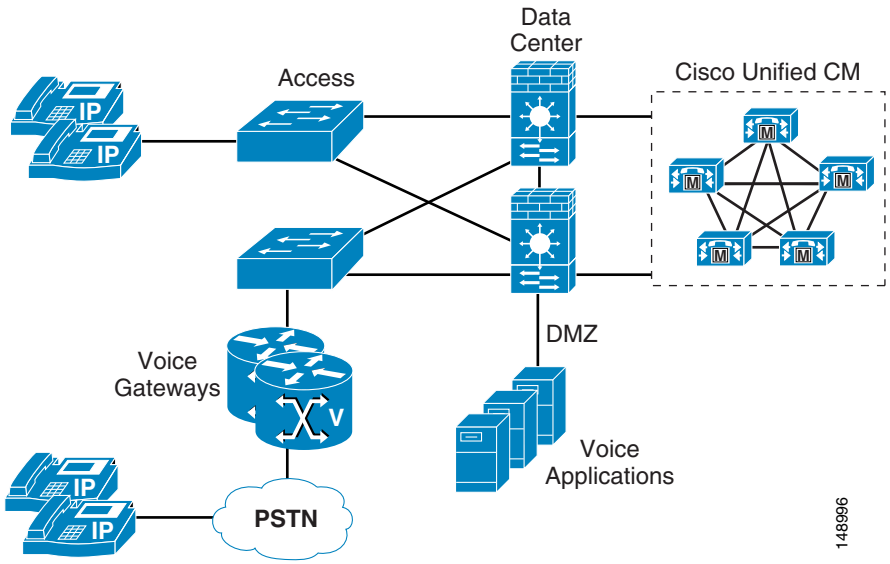
DHCP スヌーピング バインディング テーブルに静的エントリが定義されていると、IP ソースガードを使用できます。攻撃者が MAC アドレスと IP アドレスを取得でき、パケットの送信を開始した場合、正しい IP アドレスが設定されたパケットだけを送信できます。

電話機が動作するのに必要なポートと IP アドレスのみを許可する、VLAN ACL を書き込むことができます（VLAN アクセス コントロール リスト（4-34 ページ）を参照）。次の例には、ネットワークへのアクセスを制御するための、レイヤ 2 または最初のレイヤ 3 デバイスのポートに適用可能な非常に小規模な ACL が含まれています（ルータのアクセス コントロール リスト（4-34 ページ）を参照）。この例は、ロビー エリアで使用されている Cisco 7960 IP Phone に基づいています。電話機への保留音または電話機からの HTTP アクセスは使用しません。

ファイアウォール集中型の導入例

この項の例は、データセンター内において、背後に Unified CM を配置するファイアウォールの 1 つの展開方法を示しています（図 4-16 を参照）。この例では、Unified CM は、すべての電話機がファイアウォールの外側から 1 つのクラスタに接続される集中型配置として置かれています。この配置内のネットワークには、社内データセンター内でルーテッド モードで設定されたファイアウォールがすでに含まれているので、ゲートウェイの配置を決定する前に負荷が確認されます。ファイアウォールの平均的な負荷を確認した後、CPU に対するファイアウォールの負荷を 60% 未満に保つため、すべての RTP ストリームがファイアウォールを横断しないようにすることが決定されました（ゲートウェイの周囲へのファイアウォールの配置（4-42 ページ）を参照）。ゲートウェイはファイアウォールの外側に配置されています。Unified CM でゲートウェイとの間の TCP データ フローを制御するため、ネットワーク内の ACL を使用します。電話機の IP アドレスは適切に定義されているので、ACL は、電話機からの RTP ストリームを制御するためネットワークにも書き込まれます（IP アドレッシング（4-4 ページ）を参照）。音声アプリケーション サーバは非武装地帯（DMZ）に配置されています。Unified CM との間のアクセス、およびネットワーク上のユーザへのアクセスを制御するため、ファイアウォールで ACL を使用します。この設定では、インスペクションを使用してファイアウォールを通過する RTP ストリームの量を制限します。これにより、既存のネットワークに新しい音声アプリケーションを追加したときの、ファイアウォールに対する影響を最小限に抑えられます。

図 4-16　　ファイアウォールの配置例



まとめ

この章では、ネットワーク内の音声およびビデオ データを保護するために有効にできるセキュリティのうち、一部のみを取り上げました。ここで取り上げた手法は、ネットワーク内のすべてのデータを保護するためにネットワーク管理者が使用できる、すべてのツールのサブセットにすぎません。逆に、ネットワーク全体のデータで必要なセキュリティのレベルによっては、これらのツールでさえ、ネットワークで有効にする必要がない場合もあります。セキュリティの方法は、注意深く選択してください。ネットワーク内のセキュリティが高くなると、それに応じて、複雑度や問題のトラブルシューティングも増加します。各企業の責任で、リスクと組織の要件の両方を定義し、ネットワークとネットワークに接続されたデバイスに適切なセキュリティを適用する必要があります。

ゲートウェイ

改訂日：2018 年 3 月 1 日

ゲートウェイは、コラボレーション エンドポイントのネットワークを公衆電話交換網（PSTN）、従来型の PBX、または外部システムに接続するための複数の方法を提供します。音声およびビデオ ゲートウェイはエントリ レベルのスタンドアロン プラットフォームから、ハイエンドで機能が充実した統合ルータ、シャーシ ベースのシステム、および仮想化アプリケーションまであります。

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

この章の変更点

表 5-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 5-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Expressway のマイナー アップデート	Cisco Expressway（5-17 ページ）	2018 年 3 月 1 日

Cisco ゲートウェイのタイプ

2006 年頃までは、企業内部の音声およびビデオ ネットワークを外部の音声サービスに接続するには、従来の PSTN に接続された TDM またはシリアル ゲートウェイを経由する以外に方法はありませんでした。シスコの製品ラインナップには、PSTN をはじめ、PBX や外部システムにもアナログおよびデジタル接続できる各種 TDM およびシリアル ゲートウェイが揃っています。TDM 接続では、低密度アナログ（FXS、FXO）、低密度デジタル（BRI）、高密度デジタル（T1、E1、T3）など、さまざまなインターフェイスを選択できます。

2006 年ごろから、一般に「SIP トランク サービス」と呼ばれる企業向けの新しい音声およびビデオ サービス オプションがサービス プロバイダーから提供されるようになりました。PSTN やその他の企業外部の宛先に SIP トランクを使用して接続するには、企業のネットワークのエッジで IP-to-IP 接続が必要です。この相互接続ポイントでは、これまで TDM またはシリアル ゲートウェイによって実現されていたものと同じ機能（境界の設定、コール アドミッション制御、QoS、トラブルシューティングの境界の確保、セキュリティのチェックなど）が引き続き必要となります。音声およびビデオ SIP トランク接続では、Cisco Unified Border Element と Cisco Expressway シリーズが、企業とサービス プロバイダー ネットワーク間の相互接続ポイントとしてこれらの機能を実行します。

この章では、Cisco TDM および Serial ゲートウェイ プラットフォームと Cisco Expressway の詳細について説明します。Cisco Unified Border Element についても簡単に説明します。

Cisco TDM および Serial ゲートウェイ

Cisco ゲートウェイを使用すると、音声およびビデオ エンドポイントは外部通信デバイスと通信できるようになります。Cisco TDM ゲートウェイには、アナログとデジタルの 2 種類があります。両方のタイプが音声コールをサポートしますが、デジタル ゲートウェイのみがビデオをサポートします。

Cisco アナログ ゲートウェイ

Cisco アナログ ゲートウェイには、ステーション ゲートウェイとトランク ゲートウェイがあります。

- アナログ ステーション ゲートウェイ

  アナログ ステーション ゲートウェイは、Unified CM を一般電話サービス（POTS）のアナログ電話機、IVR システム、FAX マシン、およびボイスメール システムに接続します。ステーション ゲートウェイは、Foreign Exchange Station（FXS）ポートを備えています。

- アナログ トランク ゲートウェイ

  アナログ トランク ゲートウェイは、Unified CM を PSTN セントラル オフィス（CO）または PBX トランクに接続します。アナログ トランク ゲートウェイは、PSTN、PBX、またはキー システムへのアクセス用の Foreign Exchange Office（FXO）ポート、および従来型の PBX とのアナログ トランク接続用の E&M（受信（recEive）/送信（transMit）、または ear and mouth）ポートを備えています。アナログ Direct Inward Dialing（DID; ダイヤルイン方式）および Centralized Automatic Message Accounting（CAMA）も、PSTN 接続に使用できます。

Cisco アナログ ゲートウェイは、次の製品およびシリーズで使用できます。

- Cisco アナログ音声ゲートウェイ VG204XM および VG300 シリーズ（VG310、VG320、VG350）はすべて、SCCP をサポートしています。
- 該当する PVDM およびサービス モジュールまたはカード付きの Cisco Integrated Services Routers Generation 2（ISR G2）2900、3900、3900E、および 4000 シリーズ（4300 および 4400）。ISR 4000 シリーズによって使用される PVDM4 は現在、ビデオをサポートしていません。
- Cisco アナログ電話アダプタ（ATA）190（SIP のみ）は、ATA188 の代替品となります。

Cisco デジタル トランク ゲートウェイ

Cisco デジタル トランク ゲートウェイは、一次群速度インターフェイス（PRI）、基本速度インターフェイス（BRI）、シリアル インターフェイス（V.35、RS-449、および EIA-530）、または T1 個別線信号方式（CAS）などのデジタル トランクを経由して、Unified CM を PSTN または PBX に接続します。デジタル T1 PRI および BRI トランクは、ビデオおよび音声専用コールの両方に使用できます。

シスコのデジタル トランク ゲートウェイは、次の製品とシリーズで使用できます。

- 該当する PVDM およびサービス モジュールまたはカード付きの Cisco Integrated Services Routers Generation 2（ISR G2）1900、2900、3900、3900E、4300 および 4400 シリーズ
- Cisco TelePresence ISDN GW 3241 および MSE 8321
- Cisco TelePresence Serial GW 3340 および MSE 8330

Cisco TelePresence ISDN Link

Cisco TelePresence ISDN Link は、Cisco TelePresence EX、MX、SX、および C シリーズのエンドポイントをサポートする、室内 ISDN および外部ネットワーク接続用のコンパクトなアプライアンスです。従来の音声およびビデオ ゲートウェイは多数のエンドポイントの PSTN と IP ネットワークの間の接続を提供する共有リソースですが、各 Cisco ISDN Link は単一の Cisco エンドポイントとペアになっています。詳細については、次の URL から入手可能な Cisco TelePresence ISDN Link のマニュアルを参照してください。

https://www.cisco.com/en/US/products/ps12504/tsd_products_support_series_home.html

TDM ゲートウェイ選択

音声およびビデオ ネットワーク用のゲートウェイを選択する場合は、次の点を考慮してください。

- 呼制御用のゲートウェイ プロトコル（5-4 ページ）
- コア機能要件（5-5 ページ）

呼制御用のゲートウェイ プロトコル

Cisco Unified Communications Manager（Unified CM）は、ゲートウェイ用に次の IP プロトコルをサポートしています。

- Session Initiation Protocol（SIP）
- H.323
- メディア ゲートウェイ コントロール プロトコル（MGCP）
- Skinny Client Control Protocol（SCCP）

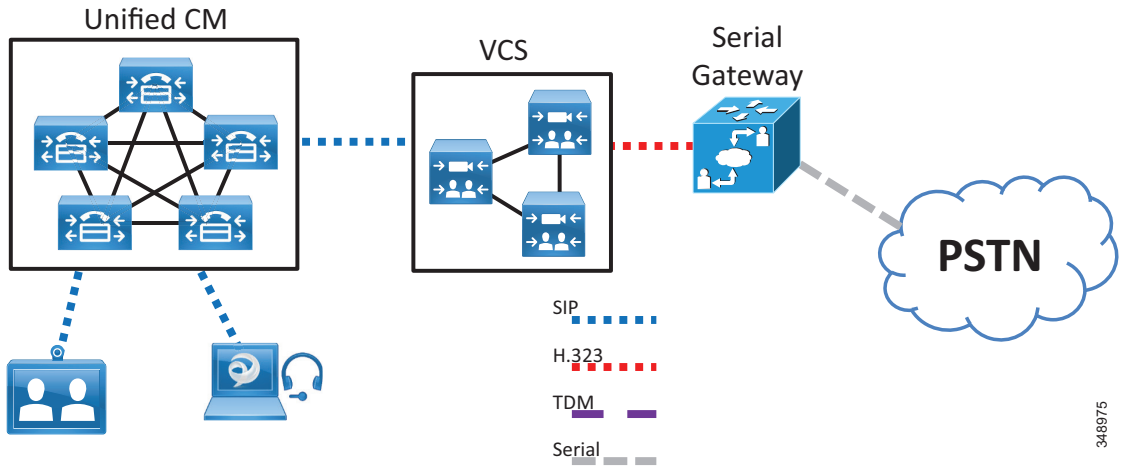
Cisco Expressway シリーズおよび Cisco TelePresence Video Communication Server（VCS）は、ゲートウェイに次の IP プロトコルをサポートしています。

- Session Initiation Protocol（SIP）
- H.323

SIP は、Cisco Collaboration ソリューション全体と新しい音声およびビデオ製品の方向性と一致しているため、コール シグナリング プロトコルとして推奨されます。ただし、プロトコルの選択は、サイト特有の要件と、現在の機器の設置ベースによって異なる場合があります。ゲートウェイ ハードウェアによって既存の配置が制限されたり、特定の機能用に別のシグナリング プロトコルが必要になったりすることがあります。

たとえば、ネットワーク内の Cisco ビデオ ゲートウェイの配置は、既存の呼制御アーキテクチャによって異なります。Cisco ISDN およびシリアル ゲートウェイは両方とも、ビデオ コール用に最適化され、Cisco VCS を使用するように設計されました。図 5-1 に示されているように、H.323 を使用して Cisco VCS に登録するには、Cisco TelePresence Serial Gateway 8330 および 3340 プラットフォームを使用することをお勧めします。

図 5-1　　Cisco VCS に登録されている Cisco TelePresence Serial Gateway



Cisco TelePresence ISDN Gateway 8321 および 3241 は、バージョン 2.2 から SIP をサポートしています。Cisco 8321 および 3241 ゲートウェイは H.323 を使用して VCS に登録したり（図 5-2 を参照）、SIP を使用して Unified CM に直接トランクしたり（図 5-3 を参照）することができます。

図 5-2　Cisco VCS にトランキングされている Cisco TelePresence ISDN Gateway

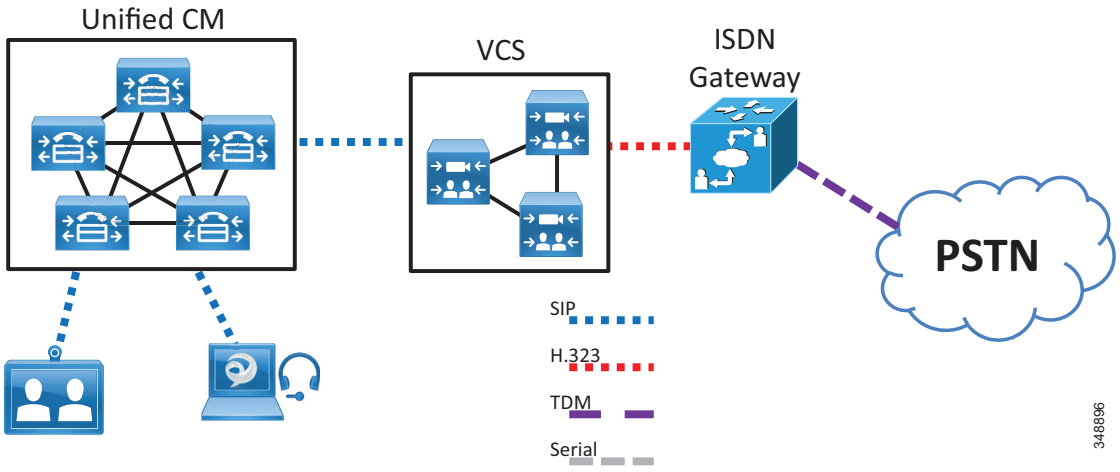
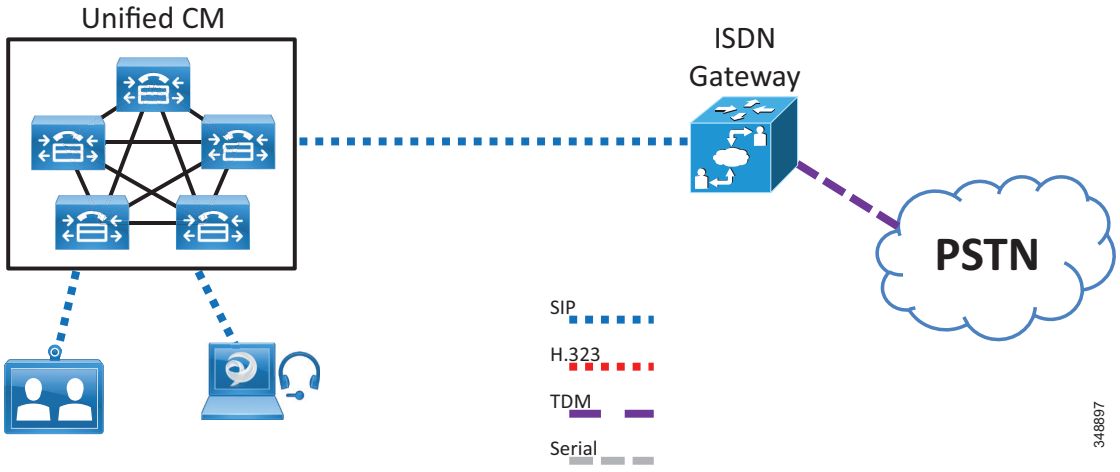


図 5-3　Cisco Unified CM に登録されている Cisco TelePresence ISDN Gateway



また、使用される Unified CM の配置モデルも、ゲートウェイ プロトコルの選択に影響を与える場合があります（コラボレーションの配置モデル（10-1 ページ）の章を参照してください）。

コア機能要件

音声およびビデオ エンドポイントで使用するゲートウェイは、次のコア機能要件を満たす必要があります。

- DTMF リレー（5-6 ページ）
- 付加サービス（5-7 ページ）

  付加サービスは、保留、転送、および会議などの基本的なテレフォニー機能です。
- Unified CM の冗長性（5-10 ページ）

Cisco Unified Communications は、分散モデルに基づき、高いアベイラビリティを確保しています。Unified CM クラスタには、Unified CM の冗長性が用意されています。ゲートウェイは、プライマリ Unified CM に障害が発生した場合に、セカンダリ Unified CM への「リホーム」機能をサポートする必要があります。一部のゲートウェイは Cisco VCS に登録されることがあります。この場合、ゲートウェイはプライマリ Cisco VCS に障害が発生した場合に、セカンダリへ「リホーム」する機能をサポートする必要があります。

企業での配置用に選択するゲートウェイがすべて、上記のコア要件を満たしていることを確認するには、ゲートウェイ製品の資料を参照してください。さらに、どのコラボレーションの実装についても、各サイト特有の機能要件（たとえば、アナログまたはデジタル アクセス、DID、およびキャパシティ要件）があります。

DTMF リレー

DTMF は、信号に音声帯域内の特定の周波数ペアを使用するシグナリング方式です。64 kbps のパルス符号変調（PCM）音声チャネルは、これらの信号を容易に伝送できます。しかし、音声圧縮に低ビット レート コーデックを使用する場合、DTMF 信号の損失または歪みの可能性があります。IP インフラストラクチャを介して DTMF トーンを伝送するアウトオブバンド シグナリング方式は、コーデックにより誘発されるこれらの症状を簡単に解決します。

SCCP ゲートウェイ

Cisco VG300 シリーズは、伝送制御プロトコル（TCP）ポート 2002 を使用して、DTMF 信号をアウトオブバンドで伝送します。アウトオブバンド DTMF は、VG310、VG320、および VG350 用のデフォルトのゲートウェイ コンフィギュレーション モードです。

H.323 ゲートウェイ

Cisco 4000 シリーズ製品などの H.323 ゲートウェイは、DTMF 信号をアウトオブバンドで交換するための拡張 H.245 機能を使用して、Unified CM と情報を交換できます。この機能は、4000 シリーズ ゲートウェイのコマンドライン インターフェイスと、そのダイヤル ピアで使用可能な **dtmf-relay** コマンドを使用して有効に設定されます。

MGCP ゲートウェイ

Cisco IOS ベースのプラットフォームでは、Unified CM 通信に MGCP を使用できます。MGCP プロトコルには、*パッケージ*の概念があります。MGCP ゲートウェイは、始動後、DTMF パッケージをロードします。MGCP ゲートウェイは、制御チャネルを介して、受信した DTMF トーンを表す *シンボル*を送信します。次に、Unified CM は、これらの信号を解釈し、アウトバンドでシグナリング エンドポイントに DTMF 信号を渡します。

DTMF に使用される方法は、ゲートウェイ CLI コマンドを使用して設定できます。

mgcp dtmf-relay voip codec all mode {*DTMF method*}

（注）　MGCP ゲートウェイを、インバンド DTMF のみをアドバタイズするように設定することはできません。インバンド DTMF リレーを有効にすると、MGCP ゲートウェイはインバンドおよびアウトオブバンド（OOB）両方の DTMF 方式をアドバタイズします。Unified CM は、どの方式を選択すべきかを判断し、MGCP シグナリングを使用してゲートウェイに通知します。両方のエンドポイントが MGCP である場合は、インバンド DTMF を有効にした後、両方のサイドでインバンドおよび OOB DTMF の方式を Unified CM にアドバタイズするため、DTMF リレー用のインバンドを呼び出す機能がありません。インバンドおよび OOB の機能がエンドポイントでサポートされている場合、Unified CM は常に OOB を選択します。

SIP ゲートウェイ

Cisco IOS および ISDN ゲートウェイでは、Unified CM 通信に SIP を使用できます。これらのプラットフォームはさまざまな方式の DTMF をサポートしていますが、Unified CM との通信に使用できるのは次の方式だけです。

- Named Telephony Events（NTE）、または RFC 2833
- Unsolicited SIP Notify（UN）（Cisco IOS ゲートウェイのみ）
- Key Press Markup Language（KPML）

DTMF に使用される方式は、ゲートウェイ CLI コマンド **dtmf-relay** をそれぞれの **dial-peer** の下で使用することで Cisco IOS で設定できます。Cisco ISDN ゲートウェイは、DTMF で RFC 2833 および KPML をサポートしています。

DTMF 方式の選択の詳細については、SIP トランク経由のコール（7-9 ページ）の項を参照してください。

付加サービス

付加サービスは、保留、転送、および会議などのユーザ機能を提供します。これらは、基本的なテレフォニー機能と見なされ、ビデオ コールよりも音声コールのほうでよく使用されます。

SCCP ゲートウェイ

Cisco SCCP ゲートウェイは、完全な付加サービス サポートを提供します。SCCP ゲートウェイは、ゲートウェイと Unified CM 間のシグナリング チャネル、および SCCP を使用して、呼制御パラメータを交換します。

H.323 ゲートウェイ

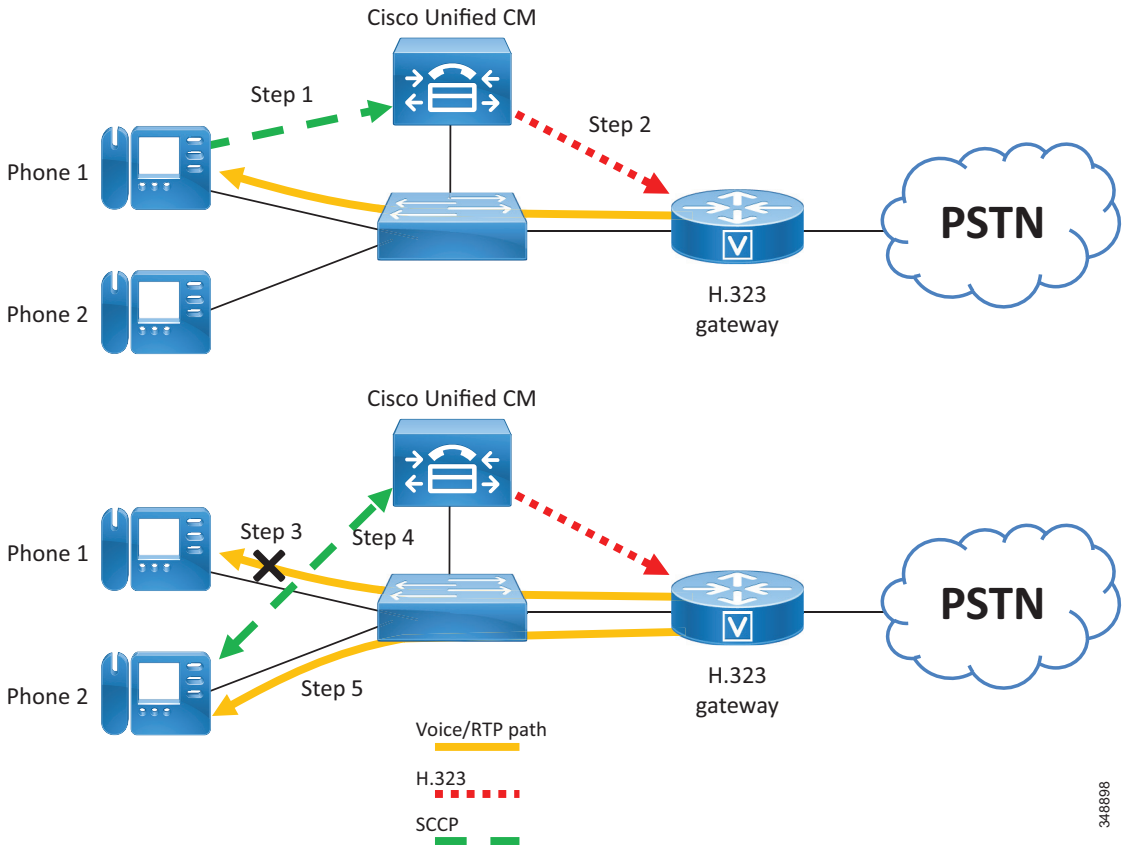
H.323v2 は、Open/Close LogicalChannel 機能と emptyCapabilitySet 機能を実行します。H.323 ゲートウェイによる H.323v2 の使用により、付加サービスを提供する際に MTP が必須ではなくなりました。トランスコーダは、WAN 全体で G.729 ストリームを維持しつつ、G.711 のみのデバイスへのアクセスを提供するコール中に必要な場合にのみ、動的に割り当てられます。

H.323v2 コールが Cisco IOS ゲートウェイと IP エンドポイントの間に Unified CM を H.323 プロキシとして使用してセットアップされると、エンドポイントはベアラ接続を変更する要求を行えます。Real-Time Transport Protocol（RTP）ストリームは、Cisco IOS ゲートウェイからエンドポイントに直接接続されるため、サポートされるメディア コーデックをネゴシエートできます。

図 5-4 と次の手順では、2 台の IP Phone 間のコール転送を示しています。

1. IP 電話機 1 が Cisco IOS ゲートウェイから電話機 2 にコールを転送しようとする場合、電話機 1 は、SCCP を使用して Unified CM に転送要求を出します。
2. Unified CM は、この要求を H.323v2 CloseLogicalChannel 要求に変換して、Cisco IOS ゲートウェイに送信して、適切な SessionID を求めます。
3. Cisco IOS ゲートウェイは、電話機 1 との RTP チャネルをクローズします。
4. Unified CM は、SCCP を使用して、Cisco IOS ゲートウェイとの RTP 接続をセットアップする要求を、電話機 2 に出します。同時に、Unified CM は、新しい宛先パラメータを指定して（ただし、同じ SessionID を使用）、Cisco IOS ゲートウェイに OpenLogicalChannel 要求を出します。
5. Cisco IOS ゲートウェイがこの要求を確認した後、RTP 音声ベアラ チャネルが、電話機 2 と Cisco IOS ゲートウェイとの間で確立されます。

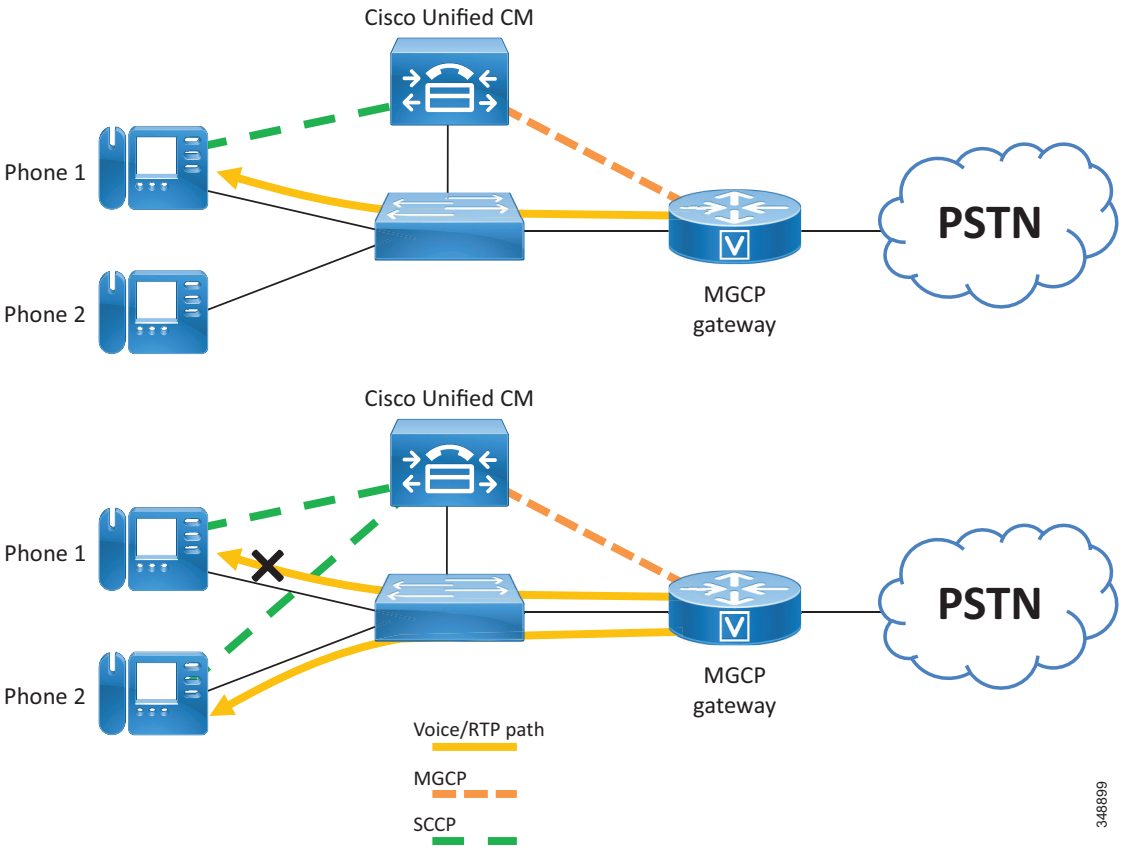
図 5-4　　H.323 ゲートウェイの付加サービス サポート



MGCP ゲートウェイ

MGCP ゲートウェイは、MGCP プロトコルを使用して、保留、転送、および会議機能を完全にサポートします。MGCP プロトコルは、すべてのセッション機能を制御する、Unified CM とのマスター/スレーブ プロトコルであるので、Unified CM は、MGCP ゲートウェイの音声接続を容易に操作できます。IP テレフォニー エンドポイント（たとえば、IP Phone）が、セッションの変更（たとえば、コールを別のエンドポイントに転送する）を必要とする場合、そのエンドポイントは、セッションの変更を SCCP を使用して Unified CM に通知します。次に、Unified CM は、Session ID に関連した現在の RTP ストリームを終了し、新しいエンドポイント情報を使用して新しいメディア セッションを開始することを、MGCP ユーザ データグラム プロトコル（UDP）制御接続を使用して、MGCP ゲートウェイに通知します。図 5-5 では、プロトコルが MGCP ゲートウェイ、エンドポイント、および Unified CM 間で交換される様子を示しています。

図 5-5　　MGCP ゲートウェイの付加サービス サポート



SIP ゲートウェイ

Cisco SIP ゲートウェイへの Unified CM SIP トランク インターフェイスは、保留、ブラインド転送、在席転送などの付加サービスをサポートしています。付加サービスのサポートは、INVITE や REFER などの SIP 方式によって実現されます。付加サービスを機能させるには、対応する SIP ゲートウェイによってこれらの方法がサポートされている必要もあります。詳細については、次のマニュアルを参照してください。

- 『*Cisco Unified Communications Manager System Guide*』
  https://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- 『*Cisco IOS SIP Configuration Guide*』
  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/sip/configuration/15-mt/sip-config-15-mt-book.html
- Cisco TelePresence ISDN Gateway のマニュアル
  https://www.cisco.com/en/US/products/ps11448/tsd_products_support_series_home.html

Unified CM の冗長性

コラボレーション ソリューション アーキテクチャに不可欠なことは、高価な専有の従来型の PBX システムの代わりに、低コストの分散型 PC ベース システムを提供することです。この分散型設計は、クラスタ化された Unified CM の堅固なフォールト トレラント アーキテクチャに適しています。最も単純な形式（2 システムのクラスタ）であっても、セカンダリ Unified CM は、最初にプライマリ Unified CM によって管理されていたすべてのゲートウェイの制御権を引き受ける必要があります。

SCCP ゲートウェイ

ブート後、Cisco VG310、VG320、および VG350 ゲートウェイには、Unified CM サーバ情報がプロビジョニングされます。これらのゲートウェイが初期設定されるときに、Unified CM のリストがゲートウェイにダウンロードされます。このリストでは、プライマリ Unified CM とセカンダリ Unified CM に優先順位が付けられています。プライマリ Unified CM が通信不能になった場合、ゲートウェイはセカンダリ Unified CM に登録されます。

WAN リンク障害用の H.323 VoIP コール プリザベーション

WAN リンク障害用の H.323 コール プリザベーション拡張機能を使用すると、対向のエンドポイントとは異なるエンティティ（シグナリングをルーティングするゲートキーパーや、接続している 2 者間でシグナリングを仲介するコール エージェント（Cisco Unified CM など）など）によってシグナリングが処理される H.323 トポロジにおいて、接続性が維持されます。コール プリザベーションが役立つのは、ゲートウェイと他のエンドポイントは同じサイトにあるものの、コール エージェントがリモート サイトにあり、接続障害が起こりやすいような場合です。

H.323 コール プリザベーションは、次の種類の障害と接続に対応します。

障害の種類：

- WAN リンクのフラッピングや性能低下などの WAN 障害
- Cisco Unified CM ソフトウェアの障害（Unified CM サーバでの ccm.exe サービスのクラッシュなど）
- LAN 接続の障害（障害がローカル ブランチで発生した場合を除く）

接続の種類：

- Cisco Unified CM で制御された 2 つのエンドポイント間のコールで、次の条件に該当する場合
  - Unified CM がリロード中の場合
  - 一方または両方のエンドポイントと Unified CM との間で H.225.0 または H.245 メッセージのシグナリングに使用される伝送制御プロトコル（TCP）接続が失われたか、フラッピングしている場合
  - エンドポイントがクラスタ内の異なる Unified CM に登録されていて、その 2 つの Unified CM 間の TCP 接続が失われた場合
  - IP Phone 間のコールで、PSTN が同じサイトにある場合
- ソフトスイッチによって制御されている Cisco IOS ゲートウェイとエンドポイント間のコールで、シグナリング（H.225.0、H.245、またはその両方）フローはゲートウェイとソフトスイッチ間で実行され、メディア フローはゲートウェイとエンドポイント間で実行される場合
  - ソフトスイッチがリロード中の場合
  - ゲートウェイとソフトスイッチ間の H.225.0 または H.245 TCP 接続が失われ、ソフトスイッチがエンドポイント上のコールをクリアしない場合
  - ソフトスイッチとエンドポイント間の H.225.0 または H.245 TCP 接続が失われ、ソフトスイッチがゲートウェイ上のコールをクリアしない場合

- メディア フローアラウンド モードで動作している Cisco Unified Border Element がコール フローに含まれていて、その Cisco Unified Border Element がリロードしているか、ネットワークの残りの部分との接続を失った場合

メディアが保持された後、一方の通話者が電話を切るか、メディアがアクティブでないことが検出されると、コールは終了します。コンピュータによって生成されたメディア ストリーム（メディア サーバからの音楽ストリーミングなど）が存在する場合は、メディア非アクティビティ検出が機能せず、コールが終了しない可能性があります。Cisco Unified CM はこの状況に対処するため、このようなコールは保持しないようにゲートウェイに指示しますが、サードパーティ製デバイスや Cisco Unified Border Element はそうしたことは行いません。

この機能において、フラッピングは「IP 接続の一時的な喪失が何度も繰り返されること」と定義されています。このような現象は、WAN または LAN の障害によって発生する可能性があります。Cisco IOS ゲートウェイと Cisco Unified CM 間の H.323 コールは、フラッピングが起こると終了する場合があります。Unified CM は、TCP 接続が失われたことを検出すると、コールをクリアし、TCP FIN を送信してコールで使用されていた TCP ソケットを閉じます。このとき、H.225.0 Release Complete メッセージまたは H.245 End Session メッセージは送信しません。これを *quiet clearing* と呼びます。ネットワークが短時間復帰した間に Unified CM から送信された TCP FIN がゲートウェイに到達すると、ゲートウェイはコールを終了します。TCP FIN がゲートウェイに到達しなくても、ネットワークが復帰すると、ゲートウェイから送信された TCP キープアライブが Unified CM に到達します。Unified CM はすでに TCP 接続を閉じているので、キープアライブに応答して TCP RST メッセージを送信します。ゲートウェイは RST メッセージを受け取ると、H.323 コールを終了します。

WAN リンク障害用の H.323 コール プリザベーション拡張機能の設定には、**call preserve** コマンドの設定を含める必要があります。Cisco Unified CM を使用している場合は、[サービス パラメータ（Service Parameters）] ウィンドウから Allow Peer to Preserve H.323 Calls パラメータを有効にする必要があります。

call preserve コマンドを発行すると、H.225.0 または H.245 接続でのアクティブ コールに関するソケットの終了またはソケット エラーがゲートウェイで無視されるため、これらの接続を使用しているコールを終了せずにソケットを閉じることができます。

MGCP ゲートウェイ

MGCP ゲートウェイにも、プライマリ Unified CM との通信が失われた場合に、セカンダリ Unified CM にフェールオーバーする機能があります。フェールオーバーが起きても、アクティブ コールは保持されます。

MGCP ゲートウェイのコンフィギュレーション ファイル内で、プライマリ Unified CM は、**call-agent <hostname>** コマンドを使用して指定され、セカンダリ Unified CM のリストは、**ccm-manager redundant-host** コマンドを使用して追加されます。プライマリ Unified CM とのキープアライブは、MGCP アプリケーション レベルのキープアライブ メカニズムを介して行われます。このメカニズムでは、MGCP ゲートウェイは、空の MGCP notify（NTFY）メッセージを Unified CM に送信し、確認応答を待ちます。バックアップ Unified CM とのキープアライブは、TCP キープアライブ メカニズムを介して行われます。

プライマリ Unified CM が後で使用可能になると、MGCP ゲートウェイは、元の Unified CM に「リホーム」（つまり復帰）できます。この復帰は、ただちに行われることもあれば、設定可能な時間が経過した後、または接続されているすべてのセッションが解除された後に行われることもあります。

SIP ゲートウェイ

Cisco IOS SIP ゲートウェイでの冗長性は、H.323 と同様の方法で実現できます。SIP ゲートウェイがプライマリ Unified CM との接続を確立できない場合、高い優先順位を持ち、別の dial-peer ステートメントで指定されるセカンダリ Unified CM との接続を試行します。

デフォルトでは、Cisco IOS SIP ゲートウェイは dial-peer で設定された Unified CM の IP アドレスに SIP INVITE 要求を 6 回送信します。SIP ゲートウェイは、その Unified CM から応答を受信しなかった場合、他の dial-peer で設定された、優先順位の高い Unified CM との接続を試行します。

Cisco IOS SIP ゲートウェイは、INVITE に対する SIP 100 応答を 500 ms 待ちます。デフォルトでは、Cisco IOS SIP ゲートウェイがバックアップ Unified CM に到達するまでに最大 3 秒かかります。SIP INVITE の再試行回数は、**sip-ua** 設定で **retry invite** <*number*> コマンドを使用して変更できます。また、Cisco IOS SIP ゲートウェイが SIP INVITE 要求に対する SIP 100 応答を待つ期間は、**sip-ua** 設定で **timers trying** <*time*> コマンドを使用して変更できます。

バックアップ Unified CM へのフェールオーバーを高速化する別の方法としては、**dial-peer** 文での **monitor probe icmp-ping** コマンドの設定があります。Unified CM がインターネット制御メッセージ プロトコル（ICMP）エコー メッセージ（ping）に応答しなかった場合、そのダイヤル ピアはシャットダウンされます。このコマンドが役に立つのは、Unified CM が到達不能のときだけです。ICMP エコーメッセージは、10 秒ごとに送信されます。

Unified CM リリース 9.0 および ISDN Gateway リリース 2.2 以降から、Cisco ISDN Gateway は Unified CM に SIP トランクを介して接続できます。ISDN Gateway SIP 設定は、IP アドレス、ホスト名、DNS A レコード、またはアウトバウンド SIP 接続の DNS SRV レコードの入力から開始します。冗長性は、適切な重みと優先順位を付けて DNS SRV レコードを使用することによって達成できるため、最初の Unified CM が失敗すると、ISDN Gateway はアウトバウンド SIP コールを 2 番目の Unified CM に送信します。

ビデオ テレフォニー用のゲートウェイ

ビデオゲートウェイは、IP テレフォニー ネットワークまたは PSTN へのビデオコールを終端します。ビデオ ゲートウェイは、ビデオをサポートし、そのコールを H.323 や SIP などのプロトコルを使用して IP ネットワーク上のビデオ コールに変換する ISDN またはシリアル リンクとデータをやり取りする必要がある点で音声ゲートウェイとは異なります。企業は、音声コールとビデオ コールでゲートウェイを分けることを検討することも、音声コールとビデオ コールの両方をルーティングする統合ゲートウェイを設置することもできます。

次の点を考慮することによって、音声とビデオで別々のゲートウェイが必要なのか、統合ゲートウェイが必要なのかを判断できます。

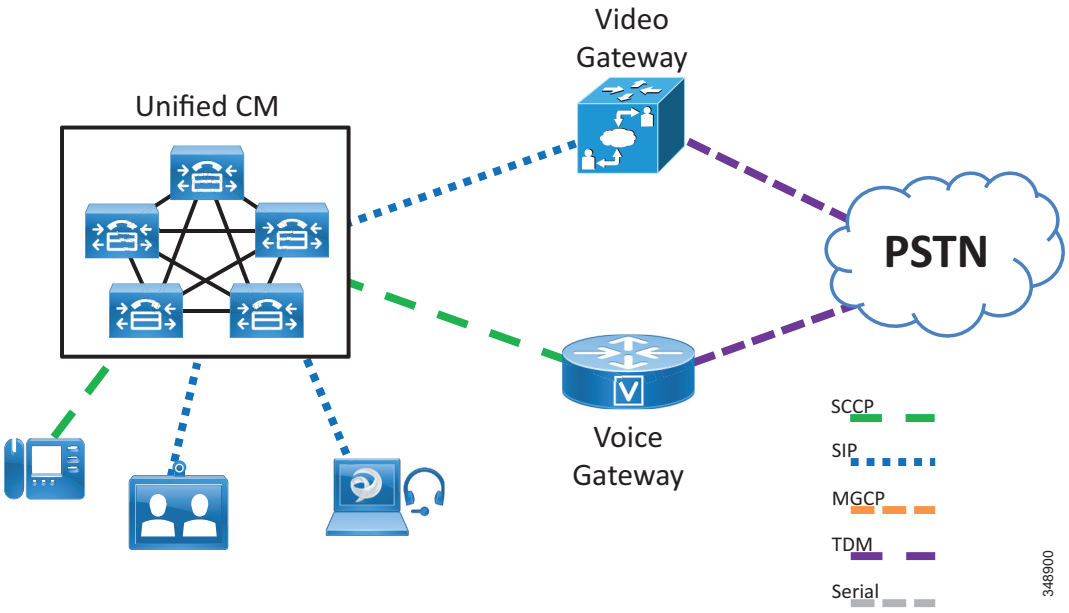
- ダイヤル プラン：ビデオ ユーザ用に別のダイヤル プランを用意できる場合は、既存のエンタープライズ ダイヤル プランを維持しながら、別のビデオ ゲートウェイを使用できます。
- ビデオ ユーザ：主にビデオよりも音声を使用するユーザの方が圧倒的に多い場合は、別のビデオ ゲートウェイを使用してビデオ コール ユーザにサービスを提供することを推奨します。
- ロケーション：多数のビデオ ユーザが地理的に分散している場合は、統合ゲートウェイを使用して総所有コスト（TCO）を削減することを推奨します。
- ビデオ IVR、自動応答、トランク上でのボンディングなどの付加的なビデオ機能：統合ゲートウェイでサポートされない高度な機能をサポートするには、専用ビデオ ゲートウェイが必要です。
- プロトコル：会社の方針や標準に合わせるために、ゲートウェイ プロトコルが重要な要素になる可能性があります。
- デバイス管理：保守、管理、およびトラブルシューティングを容易にしておくことは重要な要素になる可能性があります。専用ゲートウェイはどちらかと言えば管理/設定用のユーザ インターフェイス（GUI）として利用するのに適しており、統合ゲートウェイはトラブルシューティングに使用するのに適しています。ただし、こうした要素は製品によって異なります。

専用ビデオ ゲートウェイ

音声ゲートウェイを含む大規模な音声インフラストラクチャを所有する企業は、ユーザが専用ビデオ コールを PSTN に発信するためのビデオ ゲートウェイを追加できます。専用ビデオ ゲートウェイには、Cisco ISDN Gateway および Serial Gateways があります。これらの製品は音声のみのコールをサポートしていますが、これらはビデオ ユーザを特に念頭に置いて設計されました。さまざまなビデオ中心プロトコルおよび機能をサポートしています。

図 5-6 に、音声ゲートウェイ用に既存のプロトコルを使用しており、Unified CM ユーザが音声コールとビデオ コールを PSTN に発信できるようにビデオ ゲートウェイを追加できる、企業での展開の一例を示します。

図 5-6　　音声と IP ビデオ テレフォニーに別々の PSTN 回線を使用する Unified CM システム



シスコ ビデオ ゲートウェイはビデオ コール用としては優れていますが、シスコ音声ゲートウェイが提供するすべての機能をサポートしているわけではありません。シスコのビデオ ゲートウェイには次の特性があります。

- Serial Gateway は、IP 接続用に H.323 のみをサポートします。
- ISDN Gateway は、IP 接続用に H.323 および SIP（リリース 2.2 以降）をサポートします。
- T1/E1-PRI、BRI、V.35、RS-449、および EIA-530 をサポートします。
- H.261、H.263、H.263+、および H.264 ビデオ コーデックをサポートします。
- G.711、G.722、G.722.1、および G.728 をサポートしますが、G.729 オーディオはサポートしません。
- H.320、H.233、H.234、H.235（AES）、H.239、H.221、FTP、RTP、HTTP、HTTPS、DHCP、SNMP、および NTP をサポートします。

このように製品間の違いがあるため、Cisco TDM および Serial Gateway は Cisco 音声ゲートウェイの代わりとしては推奨できません。IP テレフォニーのユーザが通信環境にビデオを追加するには、両方のタイプのゲートウェイを配置して、すべての音声コールに Cisco 音声ゲートウェイを使用し、ビデオ コールのみに Cisco ビデオ ゲートウェイを使用する必要があります。また、配置する Cisco ゲートウェイのモデルによっては、PSTN サービス プロバイダーから音声とビデオに別個の回線を調達する必要がある場合もあります。

また、トール バイパスを設けるためには IP ネットワーク内でコールをどのようにリモート ゲートウェイへルーティングするのか、および IP ネットワークが使用不能になるか、コールを完了できるだけの帯域幅がない場合に、PSTN 上でコールをどのように再ルーティングするのかを考慮してください。具体的には、ビデオ コール用の自動代替ルーティング（AAR）を起動するのか、といったことです。

統合ビデオ ゲートウェイ

推奨はされていませんが、企業は音声とビデオ両方のゲートウェイ機能を備えた統合デバイスを検討できます。このデバイスは、管理対象デバイスの数が少なくなり、ダイヤル プランが単純になるというメリットを企業にもたらします。このゲートウェイは、コールが音声の場合は音声コールとして処理し、コールがビデオの場合はビデオ コールとして処理します。

Cisco IOS、ISDN、および Serial Video ゲートウェイには、次のような特徴があります。

- H.323 および SIP サポートを提供します（H.323 のみを提供する Serial Gateway を除く）。
- H.261、H.263、H.263+、および H.264 ビデオ コーデックをサポートします。
- さまざまな着信側および発信側変換機能を提供します。
- さまざまなロギングおよびトラブルシューティング機能を提供します。

次の留意点は、Cisco IOS、ISDN、および Serial Video ゲートウェイの配置に適用されます。

- 追加のビデオ コール用の PSTN リンクに必要な容量を考慮してください。
- Binary Flow Control Protocol（BFCP）などのコンテンツ共有を使用するためのデバイスが必要かどうかと、IP ネットワークで使用される追加の帯域幅を考慮してください。
- ゲートウェイでサポートされる会議で遠端カメラ制御や DTMF などの機能が必要かどうかを考慮してください。

Unified CM でのビデオ ゲートウェイの設定

次のいずれかの方法で Cisco TelePresence ISDN Gateway を設定できます。

- ISDN ゲートウェイを指す SIP トランクを設定し（図 5-3 を参照）、その SIP トランクを指す、該当する Unified CM ルート パターンを追加します。
- Unified CM から Cisco VCS に SIP トランクを設定します。H.323 を使用して VCS に ISDN ゲートウェイ（または、この場合は Serial ゲートウェイ）を登録します（図 5-2 を参照）。

Cisco TelePresence Serial Gateway を Unified CM に直接トランクさせることはできません。Cisco VCS に登録した後、SIP トランクを Unified CM に登録する必要があります。

どちらの方法でも最終的な目標は、各ゲートウェイが受信したすべての着信コールを Unified CM に送り、Unified CM がコールのルーティング方法を決定できるようにすることです。Unified CM と VCS の間で SIP トランクを設定する方法の詳細については、Cisco Unified CM トランク（6-1 ページ）の章を参照してください。

コール シグナリング タイマー

H.320 ボンディングに固有の遅延のため、ビデオ コールは音声コールよりも接続に時間がかかる場合があります。Unified CM のいくつかのタイマーは、デフォルトで音声コールをできるだけ高速に処理するように調整されているため、それが原因でビデオ コールが失敗する場合があります。したがって、H.320 ゲートウェイ コールをサポートするには、次のタイマーをデフォルト値から変更する必要があります。

- H.245TCSTimeout
- Media Exchange Interface Capability Timer
- Media Exchange Timer

これらの各タイマーを、Unified CM Administration の Service Parameters で 25 まで増やすことを推奨します。このパラメータはクラスタ全体のサービス パラメータであるため、既存の Cisco 音声ゲートウェイへの音声コールも含めて、あらゆるタイプのデバイスへのコールに影響を与えることに注意してください。

Cisco IOS 音声ゲートウェイのベアラ機能

H.323 コールは、どのタイプのコールを行うかを示すために、H.225/Q.931 Bearer Capabilities Information Element（bearer-caps）を使用します。音声専用コールでは、bearer-caps が「**speech**」または「**3.1 KHz Audio**」に設定され、ビデオ コールでは bearer-caps が「**Unrestricted Digital Information**」に設定されます。一部のデバイスでは、Unrestricted Digital Information の bearer-caps をサポートしていません。Unified CM が H.323 ビデオ コールとしてコールを試みると、これらのデバイスへのコールは失敗する場合があります。

Unified CM は、次の要因に基づいて、どの bearer-caps を設定するかを決定します。

- 発信側デバイスまたは着信側デバイス（あるいはその両方）がビデオ対応かどうか
- それらのデバイス間のコールにビデオを許可するように Unified CM のリージョンが設定されているかどうか

Unified CM では、ビデオ コールをオーディオとして再試行する機能をサポートしており、この機能は設定を介して有効にできます。Unified CM がビデオ コールの bearer-caps を「**Unrestricted Digital**」に設定し、コールが失敗すると、Unified CM は同じコールの bearer-caps を「**speech**」に設定したオーディオ コールとして再試行します。

H.323 を使用する場合、Cisco IOS ゲートウェイは、コールの設定で受信するベアラ機能に基づいて、コールを音声またはビデオとして処理できます。SIP を使用する場合、ゲートウェイはコールのネゴシエーションのため、ISDN 機能を SDP に変換します。

Cisco 音声ゲートウェイが Unified CM との通信に MGCP を使用している場合、この問題は発生しません。それは、Unified CM の MGCP プロトコル スタック上ではビデオがサポートされておらず、しかも、MGCP モードでは、Unified CM が PSTN への D チャネル シグナリングを完全に制御するためです。

IP ゲートウェイ

Cisco IP ゲートウェイには次のものが含まれます。

- Cisco Unified Border Element（5-16 ページ）
- Cisco Expressway（5-17 ページ）

Cisco Unified Border Element

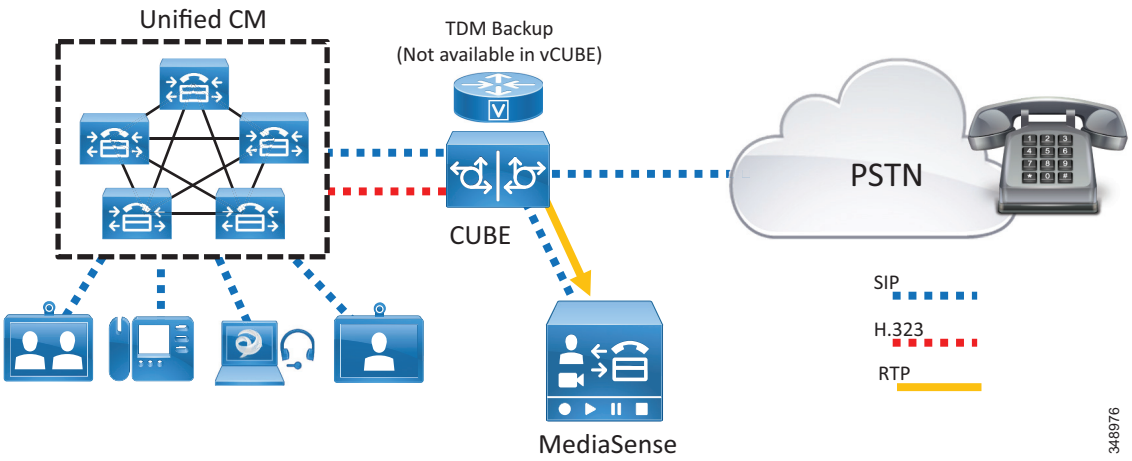
コラボレーション サービスの革新によって、従業員の生産性が大幅に向上し、また企業は、企業内での内部通話と外部の PSTN アクセスの両方で、IP ベースのユニファイド コミュニケーションを幅広く展開しています。これによって、企業およびテレフォニー サービス プロバイダー両方による TDM ベースの回線から、ユニファイド コミュニケーション用の IP ベース トランクへの大幅な移行が可能になりました。IP ベースのテレフォニー トランクの中核には、RFC 3261 に基づく業界標準の通信プロトコルであり、音声、ビデオ、ユニファイド メッセージング、ボイスメール、会議などのマルチメディア通信セッションの制御に幅広く使用されている Session Initiation Protocol（SIP）があります。

これらの PSTN SIP トランクは、ファイアウォールが 2 つのデータ ネットワークを分割する方法と同様に、企業側で企業とサービス プロバイダーの IP ネットワーク間の責任分界点として機能するセッション ボーダー コントローラ（SBC）で終端します。Cisco Unified Border Element（CUBE）Enterprise はシスコの SBC サービスであり、次を提供することで企業向けの豊富なマルチメディア コミュニケーションを実現します。

- セッション制御：コール アドミッション制御、トランク ルーティング、QoS、統計情報、請求、冗長性、スケーラビリティ、音声品質モニタリング
- セキュリティ：暗号化、認証、登録、SIP 保護、音声ポリシー、電話料金詐欺行為防止、テレフォニー Denial of Service（TDoS）攻撃からの保護
- インターワーキング：さまざまな SIP および H323 スタックの相互運用性、SIP の正規化、DTMF、トランスコーディング、トランスレーティング、コーデック フィルタリング
- 境界設定：障害分離、トポロジおよびアドレス隠蔽、L5/L7 プロトコルの境界設定、ネットワーク境界

CUBE は、IP トラフィックを SIP トランク経由でさまざまな企業およびサービス プロバイダーのネットワークに伝送する際に相互運用性、セキュリティ、およびサービス保証を確保するために必要な機能を提供します。これは Back-to-Back User Agent（B2BUA）で、Cisco ISR G2 800 シリーズ プラットフォームでの Cisco IOS インフラストラクチャ、ASR 1000 シリーズの Cisco IOS-XE、Cisco ISR 4000 シリーズ、およびシスコ クラウド サービス ルータ（CSR）1000V シリーズの CUBE（仮想 CUBE すなわち vCUBE）の一部です。図 5-7 に、企業の CUBE の展開を示します。

図 5-7　Cisco Unified Border Element の展開



Cisco Unified Border Element の詳細については、次のサイトで入手可能なマニュアルを参照してください。

https://www.cisco.com/go/cube

Cisco Expressway

インターネットを使用したコラボレーション サービスは、人気が高く、既存のレガシー ISDN ビデオ システムおよびゲートウェイがどんどん置き換えられています。インターネット ベースのコラボレーション サービスに使用されている 2 つの主なプロトコルは SIP と H.323 です。インターネットは、リモート ユーザとモバイル ユーザを、バーチャル プライベート ネットワーク（VPN）を使用せずに、音声、ビデオ、IM and Presence、およびコンテンツ共有サービスに接続するためにも使用されます。

Expressway-C と Expressway-E のペアは次の機能を実行します。

- モバイル & リモート アクセスだけでなく、Business-to-Business（B2B）サービスも、同じ Cisco Expressway-C と Expressway-E のソリューション ペアの一部として有効にできます。
- インターワーキング：音声、ビデオ、およびコンテンツ共有用の H.323 / SIP 間コールを相互接続する機能。
- 境界通信サービス：Expressway-C は社内ネットワーク内に配置されますが、Expressway-E は企業の DMZ 内に配置され、企業ネットワークとインターネット間の通信サービス専用の明確な接続点を提供します。
- セキュリティ：モバイル & リモート アクセスと Business-to-Business（B2B）コミュニケーションの両方に認証と暗号化を提供する機能。

Expressway-C と Expressway-E は、連携してインターネット経由の Business-to-Business（B2B）コミュニケーション用のコア コンポーネントであるファイアウォール トラバーサル ソリューションを形成するように設計されています。Expressway-C は、企業ネットワークの内部（信頼された側）に配置され、Expressway-E へのセキュアで信頼できる各種の標準規格に準拠した接続手段を提供する役割を果たします。また、その背後にあるすべてのデバイスへのトラバーサル クライアントとしての機能を果たします。このソリューションは、アウトバウンド通信用に開かれた少数のポートにすべてのメディアを多重化することによって、大量のメディア ポートを使用するデバイスの問題を解決します。また、Expressway-C から Expressway-E までのトラバーサル ゾーンに関するキープアライブを送信することによって、社内から社外への認証された信頼できる接続を実現します。また、すべてのインターネット通信に対して一括窓口を提供することで、セキュリティ リスクを最小化します。

SIP、H.323、XMPP などのリアルタイムや準リアルタイムの通信プロトコルでは、ファイアウォールの背後に設置されたデバイスとの通信ニーズは解決されません。このようなプロトコルを使用した典型的な通信には、シグナリングとメディア内にデバイス IP アドレスが含まれており、それぞれが TCP パケットと UDP パケットのペイロードになります。これらのデバイスが、内部的にルーティング可能な同じネットワーク上に存在する場合は、相互に直接通信することができます。TCP パケットのペイロードで伝送されるシグナリング IP アドレスは送信デバイスに戻すルーティングが可能であり、その逆もできます。ただし、送信デバイスがパブリックまたはネットワーク エッジ ファイアウォールの背後の別のネットワーク上に存在する場合は、2 つの問題が発生します。1 つ目の問題は、受信デバイスが、パケットの復号化後に、ペイロードで伝送された内部 IP アドレスに応答することです。この IP アドレスは、通常、ルーティング不可能な RFC 1918 アドレスであり、絶対に返信先に到達しません。2 つ目の問題は、返信先 IP アドレスがルーティング可能であっても、メディア（RTP/UDP）が外部ファイアウォールによってブロックされることです。このことは、Business-to-Business（B2B）コミュニケーションと、モバイル & リモート アクセスの通信の両方に当てはまります。

Expressway-E は DMZ 内のネットワーク エッジに配置されます。これは、標準の相互運用性を維持しながら、SIP、H323、および XMPP に関するシグナリングとメディアの両方のルーティング問題を解決する役割を果たします。Expressway-E は、ネットワーク内部のエンドポイント、デバイス、およびアプリケーション サーバの代わりにメディアとシグナリングを処理するために該当するヘッダーと IP アドレスを変更します。

Business-to-Business（B2B）コミュニケーション用の Expressway-C および Expressway-E の展開

Cisco Expressway シリーズの標準導入には、Business-to-Business（B2B）コミュニケーション用の少なくとも 1 つの Expressway-C と Expressway-E のペアの展開が必要です。復元力を高めるためには、Expressway-C と Expressway-E の両方をクラスタ内に展開する必要があります。各クラスタでのサーバ数は、同時コール数によって異なります。（詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください）。

しばしば、地理的範囲とスケーリングのために複数のペアの Expressway-C と Expressway-E が展開され、これにより、コラボレーション サービスの複数のインスタンスへのアクセスが可能になります。Unified CM がインターネット上のユニファイド ビジネス コミュニケーション アクセス用の SIP トランク経由で Expressway-C に接続されます。エンタープライズ セキュリティ ポリシーに基づいて、さまざまな展開モデルを実装できます。このマニュアルでは、デュアル ネットワーク インターフェイスを備えた Expressway-E の DMZ 展開を中心に説明します。これは、この展開が最も一般的でセキュアな展開モデルだからです。その他の展開モデルについては、次の URL から入手可能な最新バージョンの『*Cisco Expressway Basic Configuration Deployment Guide*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

Expressway-C と Expressway-E は、ファイアウォール トラバーサル機能を提供します。ファイアウォール トラバーサルは次のように動作します。

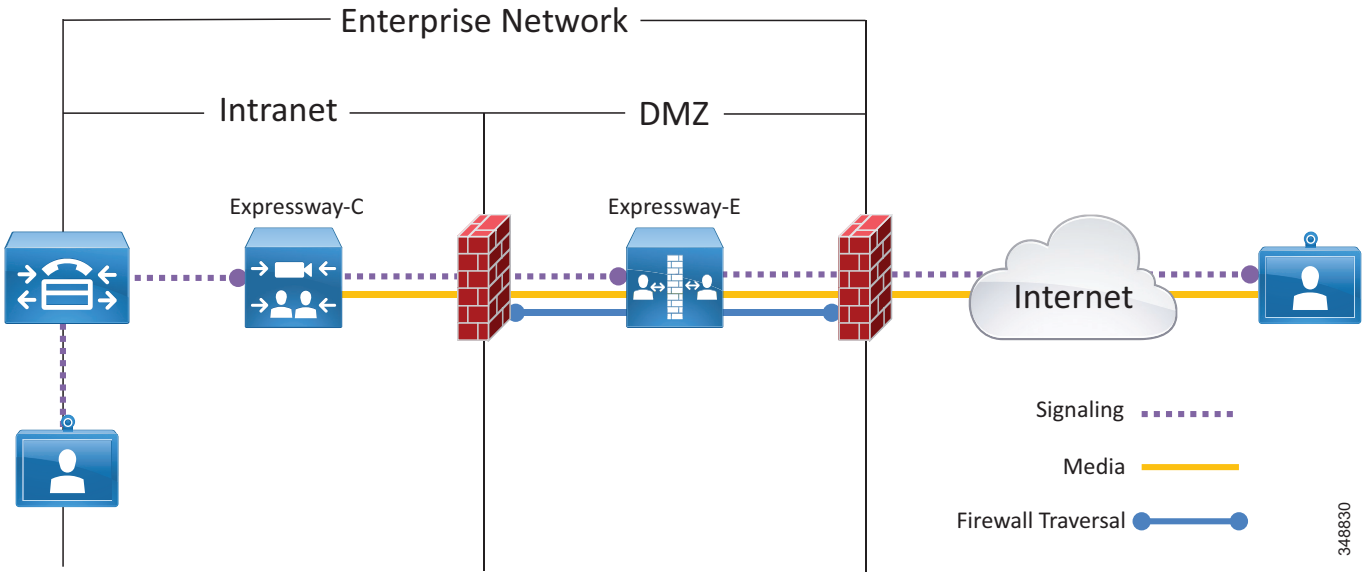
1. Expressway-E は企業の DMZ 内に設置されるトラバーサル サーバで、Expressway-C は企業ネットワーク内に設置されるトラバーサル クライアントです。
2. Expressway-C は、セキュアなログイン クレデンシャルを使用して、ファイアウォールを通って Expressway-E 上の特定のポートに至るトラバーサル アウトバウンド接続を開始します。ファイアウォールがほとんどの場合の動作と同様にアウトバウンド接続を許可している場合は、企業のファイアウォールで追加のポートを開く必要はありません。

   ポートの詳細については、最新バージョンの『*Unified Communications Mobile and Remote Access via Cisco Expressway Deployment Guide*』を参照してください。このマニュアルには、Business-to-Business（B2B）およびモバイル アクセスとリモート アクセスのシナリオで Expressway によって使用されるすべてのポートが含まれています。このガイドは、次の URL から入手できます。

   https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html
3. 接続が確立されると、Expressway-C がキープアライブ パケットを定期的に Expressway-E に送信して接続を維持します。
4. Expressway-E が着信コールやその他のコラボレーション サービス要求を受け取ると、着信要求を Expressway-C に発行します。
5. その後で、Expressway-C がその要求を Unified CM またはその他のコラボレーション サービス アプリケーションにルーティングします。
6. 接続が確立され、アプリケーション トラフィック（音声メディアとビデオ メディアを含む）が既存のトラバーサル接続経由で安全にファイアウォールを通過します。

ファイアウォール トラバーサルが機能するためには、Expressway-C 上でトラバーサル クライアント ゾーンを設定し、Expressway-E 上でトラバーサル サーバ ゾーンを設定する必要があります。図 5-8 に、Expressway-E のデュアル インターフェイスの展開シナリオにおけるファイアウォール トラバーサル プロセスをまとめます。

図 5-8　　デュアル インターフェイスの展開におけるファイアウォール トラバーサル



デュアルインターフェイス展開シナリオでは、Expressway-E が次の 2 つのファイアウォール間の DMZ 内に配置されます。インターネット ファイアウォールはインターネット向けの NAT サービスを提供し、イントラネット ファイアウォールは企業信頼ネットワークへのアクセスを提供します。

Expressway-E は次の 2 つの LAN インターフェイスを備えています。1 つはインターネット ファイアウォール向け（外部インターフェイスとも呼ばれる）で、もう 1 つはイントラネット ファイアウォール向け（内部インターフェイスとも呼ばれる）です。外部または内部インターフェイスにパケットをルーティングするには、Expressway-E でスタティック ルートを作成します。スタティック ルートを作成する最も簡単な方法は、Expressway-E のデフォルト ゲートウェイを外部の LAN インターフェイスのデフォルト ゲートウェイと同等に設定し、すべての内部ネットワークに対しスタティック ルートを作成することです。このようにして、内部トラフィックは内部インターフェイスに送信され、スタティック ルートで設定されたネットワーク範囲に一致しないすべてのトラフィックがインターネットに送信されます。

外部インターフェイスにパブリック IP アドレスを割り当てる必要はありません。これは、NAT によってアドレスを静的に変換できるためです。この場合は、Expressway-E 自体にパブリック IP アドレスを設定する必要があります。Expressway-E の外部インターフェイスは NAT によって静的に変換できますが、Expressway-E の内部インターフェイスは、Expressway がクラスタ化されていない場合にのみ NAT によって静的に変換できます。Expressway-C のインターフェイスは NAT によって変換できます。

Expressway-C とバックエンド アプリケーション サービス間の Business-to-Business（B2B）コミュニケーション用のインターネットからの接続は、その設定と会社の方針に基づいて暗号化される場合とされない場合があります。このケースでは、企業とリモート両方の Business-to-Business（B2B）パーティが公開証明書を使用した暗号化をサポートしている場合にのみ、通信がエンドツーエンドで暗号化されることに注意してください。これ以外のケースでは、ビデオ コールが暗号化されずに送信されるか、または Expressway-E の設定ポリシーに基づいて廃棄されます。

Business-to-Business（B2B）コール フロー

Business-to-Business（B2B）コミュニケーションには、URI ルーティングの目的でリモート組織のドメインを検索できる機能が必要です。これは、Expressway-E 上で DNS ゾーンを作成することによって実現されます。このゾーンはデフォルト設定で構成する必要があります。デフォルトで SIP と H.323 の両方が設定されます。Expressway-C と Expressway-E は、コールを開始するために使用されたプロトコルを使用しますが、Expressway 上で SIP/H.323 間ゲートウェイ インターワーキングが有効になっている場合は自動的に別のプロトコルを使用しようとします。

Expressway-E の場合、SIP/H.323 間のインターワーキングは [オン（On）] に設定する必要があります。これにより、コールが H.323 コールとして受信された場合に、Expressway-E がそのコールを SIP に接続し、Unified CM への残りのコール レッグにネイティブ SIP を使用できます。同様に、H.323 システムへの発信コールは、Expressway-E に到達して H.323 に接続されるまで SIP コールを維持します。

インターネット経由で Business-to-Business（B2B）コミュニケーションを受信するには、外部 SIP レコードと H.323 DNS レコードが必要です。これらのレコードを使用すれば、他の組織は URI のドメインをそのコール サービスを提供している Expressway-E に解決できます。シスコの検証済みデザインには、Business-to-Business（B2B）コミュニケーション用の SIP レコード、SIPS SRV レコード、および H.323 SRV レコードが含まれています。H.323 SRV レコードは、エンドポイントが登録用のゲートキーパーを探すために使用するもので、Expressway-E には必要ありません。

表 5-2 に、URI のドメインを解決するために使用される DNS SRV レコードを示します。

表 5-2　　URI ドメインの解決用の DNS SRV レコード

通信のタイプ	ドメイン	[ポート（Port）]	プロトコル
SIP Business-to-Business（B2B）	_sips._tcp.domain	5061	TLS
	_sip._tcp.domain	5060	TCP
	_sip._udp.domain	5060	UDP
H.323 Business-to-Business（B2B）	_h323ls._udp.domain	1719	RAS
	_h323cs._tcp.domain	1720	H.225
Mobile & Remote Access	_collab-edge._tls.domain	8443	Jabber ログイン
	_xmpp-server._tcp.domain	5269	XMPP フェデレーション

Expressway-E 上での DNS ゾーンの設定方法については、次の URL で入手可能な最新バージョンの『*Cisco Expressway Basic Configuration Deployment Guide*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

発信コールは、Cisco Unified CM で「*」に設定されている SIP ルート パターンを使用します。ローカルの Unified CM クラスタまたは ILS テーブル内に一致が見つからない SIP URI は、ダイヤル プラン（14-1 ページ）の章に定義されているルーティング ルール ロジックに従って、この SIP ルート パターンを介して送信されます。ターゲットとして Expressway-C クラスタに対するルート リストを含めるように、この SIP ルート パターンを設定します。

Business-to-Business（B2B）コミュニケーション用の次の 2 つのルールを含めるように Expressway-C を設定します。

- ドメインの一部が企業のドメインに一致する SIP URI を Cisco Unified Communications Manager に送信します。
- ドメインの一部が他のドメインに一致する SIP URI を Expressway-E に送信します。

Expressway-E で、Business-to-Business（B2B）コミュニケーション用の次の 2 つのルールを設定します。

- ドメインの一部が企業のドメインに一致する SIP URI を Expressway-C クラスタに送信します。
- ドメインの一部が他のドメインに一致する SIP URI を DNS SRV 解決に使用される DNS ゾーンに送信します。

ユーザが、Unified CM に接続されているエンドポイントから、ある文字列の後に外部ドメインをダイヤルすると、SIP ルート パターンに一致します。Unified CM は Expressway-C にコールを送信し、Expressway-C はそのコールを Expressway-E に送信します。Expressway-E はパブリック DNS で DNS SRV ルックアップを実行します。DNS は SRV レコードを解決し、Expressway-E はコールを未知のリモート エンドに転送できます。

着信コールは、デフォルト ゾーンで Expressway-E によって受信され、上記で指定した検索ルールに基づいて、Expressway-E はコールを Expressway-C に送信し、Expressway-C はそのコールを Cisco Unified CM に送信します。

モデル タイプまたは音声/ビデオ機能に関係なく、Cisco Unified CM に接続されている Cisco エンドポイントはすべて到達可能であることに注意してください。

エンドポイントに関連付けられている SIP URI がない場合は、文字列 <*DN*>@<*domain*> を介して到達可能です。<*DN*> は Cisco Unified CM に設定されているディレクトリ番号で、<*domain*> は企業の SIP ドメインです。

デバイスに、DN に関連付けられている対応する英数字の SIP URI がある場合、同じデバイスは英数字の SIP URI をダイヤルすることでも到達できます。

Business-to-Business（B2B）コールの IP ベース ダイヤリング

IP ベース ダイヤリングは、特に H.323 エンドポイントを使ってダイヤルする場合のほとんどのシナリオで使用されるよく知られた機能です。シスコ コラボレーション アーキテクチャでは、SIP URI を使用するため、IP ベース ダイヤリングは必要ありません。ただし、コールの発着信に IP アドレスしか使用できない他の組織のエンドポイントと対話する場合は、シスコ コラボレーション アーキテクチャで着信コールと発信コールの両方に IP ベース ダイヤリングを使用できます。

アウトバウンド コール

アウトバウンド IP ダイヤリングは Expressway-E と Expressway-C ではサポートされますが、Cisco Unified CM では完全なネイティブ サポートはありません。ただし、ここで説明するように、IP ベース ダイヤリングを使用するように Unified CM をセットアップすることができます。

IP アドレス単独でダイヤルする代わりに、Cisco Unified CM 上のユーザは、10.10.10.10@ip のように SIP URI ベースの IP アドレスにダイヤルすることができます。ここで、「@ip」は、リテラルで、「external」、「offsite」、またはその他の意味のある単語に置き換えることができます。

Unified CM は「ip」架空ドメインを Expressway-C にルーティングするように設定された SIP ルート パターンに一致します。Expressway-C はドメイン「@ip」を除外して、そのコールを IP アドレス ダイヤリング用にも設定されている Expressway-E に送信します。

Expressway -E 上の不明な IP アドレス宛てのコールは [直接（Direct）] に設定する必要があります。コール制御が展開されていない場合は IP ベース アドレス ダイヤリングのほとんどが H.323 エンドポイントで設定されるため、Expressway-E は H.323 コールをパブリック IP アドレスにあるエンドポイントに直接送信できます。コールは Expressway-E 上で接続されるまで SIP コールを維持します。

または、架空ドメインを追加する代わりに、ユーザはドットをアスタリスク文字に置き換えることができます。たとえば、10*10*10*10 のようになります。

Unified CM は、!*!*!*! と定義されたルート パターンに一致し、コールを Expressway-C に送信します。Expressway-C は「アスタリスク」文字をドットに置き換えます。この場合、検索ルールは正規表現 (\d\d?\d?)(*)(\d\d?\d?)(*)(\d\d?\d?)(*)(\d\d?\d?) に一致し、置換文字列として \1\.\3\.\5\.\7 を持ちます。

着信コール

IP ベースの着信コールは、Expressway-E に設定されたフォールバック エイリアスを使用します。インターネット上のユーザが Expressway-E 外部 LAN インターフェイスの IP アドレスにダイヤルすると、Expressway-E がそのコールを受信して、フォールバック エイリアス設定で設定されたエイリアスに送信します。たとえば、フォールバック エイリアスがコールを会議番号 80044123 または会議エイリアス meet@example.com に送信するように設定されている場合は、着信コールはその会議を担当するアプリケーションまたはデバイスに送信されます。

IP アドレスとフォールバック エイリアス間の静的マッピングが制限されている場合は、フォールバック エイリアスを Cisco Unity Connection または Cisco Unified Contact Center Express（UCCX）のパイロット番号に設定できます。この方法では、Unity Connection 自動応答機能または UCCX IVR の機能を使用して、DTMF 経由で、あるいは、Unity Connection でサポート可能な場合は音声認識によって、最終宛先を指定できます。Unity Connection が Expressway-E の IP アドレスにダイヤルする外部エンドポイントの自動応答機能として使用されている場合は、Unity Connection の Unified CM トランク設定で [再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）] に設定することを忘れないでください。

Expressway-C と Expressway-E のハイ アベイラビリティ

Expressway-C と Expressway-E はクラスタで展開することをお勧めします。クラスタごとに最大 6 つの Expressway ノードと最大 N+2 の物理冗長性を設定できます。クラスタ内のすべてのノードがアクティブです。クラスタ設定については、次の URL で入手可能な最新バージョンの『*Cisco Expressway Cluster Creation and Maintenance Deployment Guide*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

Expressway クラスタでは、設定の冗長性が提供されます。クラスタで設定された最初のノードがマスターとなります。設定はマスター内で実行され、自動的に他のノードにレプリケートされます。Expressway クラスタは、コール ライセンス共有と回復力を提供します。すべてのリッチ メディア セッション ライセンスがクラスタ内の全ノードで等しく共有されます。コール ライセンスはノードごとに設定されたライセンスによって供与されます。

仮想マシンとして展開された Expressway-C と Expressway-E は VMware VMotion をサポートします。VMwareVMotion は、物理サーバ間の実行中の仮想マシンのライブ マイグレーションを可能にします。仮想マシンの移動中は、Expressway-C サーバと Expressway-E サーバが、シグナリングのみを処理するとき、または、シグナリングとメディアの両方を処理するときにアクティブ コールを維持します。これにより、Expressway ノードのハイ アベイラビリティだけでなく、Cisco Unified Computing System（UCS）ホスト全体でのコール回復力も提供されます。

次のルールが Expressway クラスタリングに適用されます。

- Expressway-C ノード タイプと Expressway-E ノード タイプを同じクラスタ内に混在させることはできません。
- クラスタ内のすべてのノードには、同一の設定が必要です。
- 設定の変更はマスター ノードでのみ行う必要があり、この変更によってレプリケーション時にクラスタ内の他のノード上の設定が上書きされます。
- あるノードが使用できなくなった場合は、そのノードがクラスタに供与していたライセンスが 2 週間後に使用できなくなります。
- Expressway-C クラスタと Expressway-E クラスタには同じ数のノードを展開します。
- クラスタ全体に同じ OVA テンプレートを展開します。
- クラスタ内のすべてのノードは、他のすべてのクラスタ ノードへの最大ラウンドトリップ時間を 30 ms 以内にする必要があります。したがって、WAN 経由のクラスタリングは遅延の制約があるためお勧めできません。
- 同じクラスタ内のすべてのノードに対して同じクラスタ事前共有キーを使用する必要があります。
- 同じ Expressway-C と Expressway-E のペアでモバイル & リモート アクセスと Business-to-Business（B2B）コミュニケーションが有効になっている場合は、Unified CM と Expressway-C 間の SIP トランク上で使用されている SIP ポート番号をデフォルトの 5060 または 5061 から変更する必要があります（たとえば、5560 と 5561 を使用します）。
- DNS SRV レコードは、クラスタに対して使用可能にする必要があり、クラスタのノードごとに A レコードまたは AAAA レコードを含む必要があります。

Expressway-C は内部ネットワークに、Expressway-E は DMZ に展開されるため、Expressway-C は、Business-to-Business（B2B）コール用のトラバーサル ゾーンを介して Expressway-E に接続される必要があります。モバイルおよびリモート アクセスには、**Unified Communication トラバーサル ゾーン**と呼ばれる別のトラバーサル ゾーンが必要です。トラバーサル サーバ ゾーンとトラバーサル クライアント ゾーンには Expressway-C と Expressway-E のすべてのノードが含まれているため、ノードのいずれかが到達不能になった場合は、代わりにクラスタの別のノードが使用されます。

Expressway-C 上に設定されたトラバーサル クライアント ゾーンには、対応する Expressway-E クラスタのすべてのクラスタ ノードの完全修飾ドメイン名を含める必要があります。同様に、トラバーサル サーバ ゾーンはすべての Expressway-C クラスタ ノードに接続する必要があります。これは、Expressway-C 証明書のサブジェクトの別名に Expressway-C クラスタ ノードの FQDN を含め、TLS 検証サブジェクト名を Expressway-C クラスタの FQDN と同一に設定することによって実現されます。これにより、トラバーサル ゾーン全体にクラスタ ノードのメッシュ構成が形成され、最後のクラスタ ノードが使用不能になるまでトラバーサル ゾーンのハイ アベイラビリティが維持されます。

Expressway-C はネイバー ゾーン経由で Unified CM に接続して、Business-to-Business（B2B）の着信コールと発信コールをルーティングします。Unified CM は Expressway-C へのトランキングも行います。ハイ アベイラビリティを維持するために、各 Expressway-C クラスタ ノードの完全修飾ドメイン名を Unified CM 上のトランク設定に列挙する必要があります。Unified CM がクラスタ化されている場合は、クラスタの各メンバーの完全修飾ドメイン名（FQDN）を Expressway-C のネイバー ゾーン プロファイルにリストする必要があります。

ここでも、メッシュ状のトランク構成が形成されます。Unified CM は、SIP Options Ping 経由でトランク設定内のノードのステータスをチェックします。あるノードが使用できなくなると、Unified CM はそのノードを運用停止にして、そのノードに対するコールをルーティングしなくなります。Expressway-C も SIP OPTIONS Ping 経由で Unified CM からのトランクのステータスをチェックします。コールは、アクティブかつ使用可能として示されているノードにのみルーティングされます。これにより、トランク設定の両側にハイ アベイラビリティが提供されます。

DNS SRV レコードは、インバウンド Business-to-Business（B2B）トラフィックに対する Expressway-E の可用性を高めることができます。ハイ アベイラビリティを維持するためには、クラスタ内のすべてのノードを SRV レコード内に同じ優先度と重要度でリストする必要があります。これにより、すべてのノードを DNS クエリで返すことができます。DNS SRV レコードは、クライアントがルックアップに費やす時間を最小にするために役立ちます。これは、DNS 応答に SRV レコード内に列挙されたすべてのノードを含めることができるためです。通常は、遠端サーバまたは遠端エンドポイントが DNS 応答をキャッシュし、応答が受信されるまで DNS クエリで返されたすべてのノードを試します。これにより、コールが成功する確率が高まります。

さらに、Expressway クラスタは、クラスタ全体でのリッチ メディア ライセンス共有をサポートします。クラスタからノードが削除された場合は、そのコール ライセンスの共有が次の 2 週間だけ継続されます。

どの Expressway も、その物理能力を上回るライセンスを保持することはできても、その物理能力を上回る Rich Media ライセンスを処理することはできません。

Expressway-C と Expressway-E のセキュリティ

Expressway-C と Expressway-E 上のセキュリティは、ネットワーク レベルとアプリケーション レベルでさらに分割することができます。ネットワーク レベルのセキュリティにはファイア ウォール ルールや侵入からの保護などの機能が含まれるのに対して、アプリケーション レベルのセキュリティには認可、認証、および暗号化が含まれます。

ネットワーク レベル保護

Expressway-C と Expressway-E のネットワーク レベル保護は、2 つの主なコンポーネント（ファイアウォール ルールと侵入防御）で構成されます。ファイアウォール ルールは次の機能を有効にします。

- トラフィックを許可または拒否する送信元 IP アドレスのサブネットを指定する。
- 拒否対象のトラフィックを破棄または拒否するかを選択する。
- SSH や HTTP/HTTPS などの既知のサービスを設定する、または、トランスポート プロトコルとポート範囲に基づいてカスタマイズされたルールを指定する。
- Expressway-E 上の LAN 1 インターフェイスと LAN 2 インターフェイスで別々のルールを設定する。

悪意のあるトラフィックを検出およびブロックし、辞書ベースでの不正ログイン攻撃から Expressway を保護するためには、自動侵入保護機能を使用する必要があります。自動化された侵入保護は、システム ログ ファイルを解析して、SIP、SSH、Web/HTTPS などの特定のサービス カテゴリへのアクセスの連続的な失敗を検出することによって機能します。指定された時間内の失敗回数が設定されたしきい値を超えた場合は、送信元ホスト IP アドレス（侵入者）と宛先ポートが、指定された期間ブロックされます。その期間が過ぎると、自動的にホスト アドレスのブロックが解除されるため、一時的に設定が間違っていた正規のホストがロックアウトされなくなります。

アプリケーション レベルのセキュリティ

アプリケーション レベルのセキュリティは、次のように分割できます。

- 認証および暗号化（5-25 ページ）
- ダイヤル プランの保護と電話料金詐欺行為の緩和（5-26 ページ）

認証および暗号化

Business-to-Business（B2B）コミュニケーションの保護には、認証、暗号化、および認可が含まれます。Business-to-Business（B2B）コミュニケーションでは、デフォルトで、認証されたトラバーサル リンクが使用されます。トラバーサル リンクは、Expressway-C と Expressway-E の間で相互に認証された Transport Layer Security（MTLS）接続によって確認された公開キー インフラストラクチャ（PKI）の利用による恩恵を受けることもできます。Business-to-Business（B2B）トラバーサル リンクがモバイル & リモート アクセスと同じ Expressway-C および Expressway-E インフラストラクチャに展開される場合は、トラバーサル ゾーンが Expressway-C および Expressway-E のクラスタ ノードの FQDN を使用することを確認してください。これによって、トラバーサル接続用の証明書信頼に対して提供された証明書を検証するために各サーバの証明書を容易に使用できるようになります。

シグナリングとメディアの暗号化は Business-to-Business（B2B）コールにとって重要ですが、コールの受信機能を限定または制限しないように慎重に展開する必要があります。通信先の旧式の SIP または H.323 システムの中には、シグナリングまたはメディアの暗号化をサポートしていないものが多数含まれています。

ゾーン設定に基づいて、暗号化ポリシーを強制（[暗号化を強制（force encrypted）]）、推奨（[ベスト エフォート（best effort）]）、非許可（[非暗号化を強制（force unencrypted）]）に設定するか、またはエンドポイントの判断に任せる（[自動（auto）]）ようにすることができます。

[暗号化を強制（force encrypted）] がターゲット ゾーンで設定され、Expressway がそのリモート ゾーンでエンドポイントのコールを受信すると、Expressway は暗号化されたコールをセットアップします。リモート パーティが暗号化されていないコールのみを受け入れる場合、コールはドロップされます。発信側のエンドポイントが TCP を使用して暗号化されていないメディアを送信している場合に、[暗号化を強制（force encrypted）] がターゲット ゾーンに設定されると、Expressway はコール レッグを終了し、TLS および暗号化を使用して宛先に別のコール レッグをセットアップします。

Expressway は SRTP に対して RTP を実行するときに、Business-to-Business（B2B）コールに Back-to-Back User Agent（B2BUA）を使用します。B2BUA はシグナリングおよびメディアの両方を終了し、宛先への新しいコール レッグをセットアップします。B2BUA は、メディア暗号化モードが [自動（auto）] 以外に設定された場合に使用されます。SIP TLS と TCP のインターワーキングに B2BUA が必要となるのは、メディアが暗号化されて送信される場合だけです。そうでなければ、B2BUA は必要ありません。Expressway-E に影響する次のシナリオの場合にのみ、例外が発生します。インバウンド ゾーンとアウトバウンド ゾーンが同じ暗号化メディア タイプに設定され、これらのゾーンの 1 つがトラバーサル サーバ ゾーンである場合、Expressway-E は、関連付けられているトラバーサル クライアント ゾーンの値をチェックします。これら 3 つのゾーンがすべて同じ値に設定されている場合、Expressway-E は B2BUA を使用しません。この場合、B2BUA は Expressway-C でのみ使用されます。[ベスト エフォート（best effort）] に設定されている場合、Expressway は暗号化されたコールをセットアップできなければ、暗号化されていないコールにフォールバックします。

要件に応じて、さまざまなメディア暗号化ポリシーを設定できます。社内の適用ポリシーが設定されていない場合は、メディア暗号化モードとして [自動（auto）] が指定されているゾーンをセットアップすることを推奨します。[自動（auto）] に設定すると、エンドポイントに暗号化の決定が委託され、Expressway は RTP/SRTP 間の変換を実行しません。

暗号化ポリシーが Expressway で適用されると、次のシナリオに示すように、コールは B2BUA の関与によって多くのコール レッグに分けられます。

- [自動(auto)] に設定された Expressway-C ネイバー ゾーン ～ Unified CM
- [ベスト エフォート(best effort)] に設定された Expressway-C トラバーサル クライアント ゾーン
- [ベスト エフォート(best effort)] に設定された Expressway-E トラバーサル サーバ ゾーン
- [自動(auto)] に設定された Expressway-E DNS ゾーン
- 暗号化が設定された Unified CM、および混合モードに設定された Unified CM 上の発信エンドポイント
- 着信側エンドポイントまたはシステムは暗号化をサポートしません

たとえば、Unified CM が混在モードで使用されていて、発信エンドポイントが暗号化に対応するように設定されているとします。このシナリオでは、Unified CM 上のセキュアなエンドポイントがインターネット上の非暗号化エンドポイントを呼び出します。この呼び出しは、次のコール レッグからなります。

1. Unified CM エンドポイント～ Expressway-C B2BUA、暗号化される
2. Expressway-C B2BUA ～ Expressway-E B2BUA、暗号化される
3. Expressway-E B2BUA ～インターネット、未知のリモート エッジまたは最終宛先まで、暗号化されない
4. リモート エッジ～最終宛先、着信側パートナーの設定に応じて暗号化されるまたは暗号化されない

コール レッグ 1 ～ 3 が暗号化されると、ロック アイコンが正しく表示されます。これらのレッグの 1 つが暗号化されていない場合、ロック アイコンは表示されません。最後のコール レッグは他社の制御下にあり、ロック ステータスには影響しないことに注意してください。

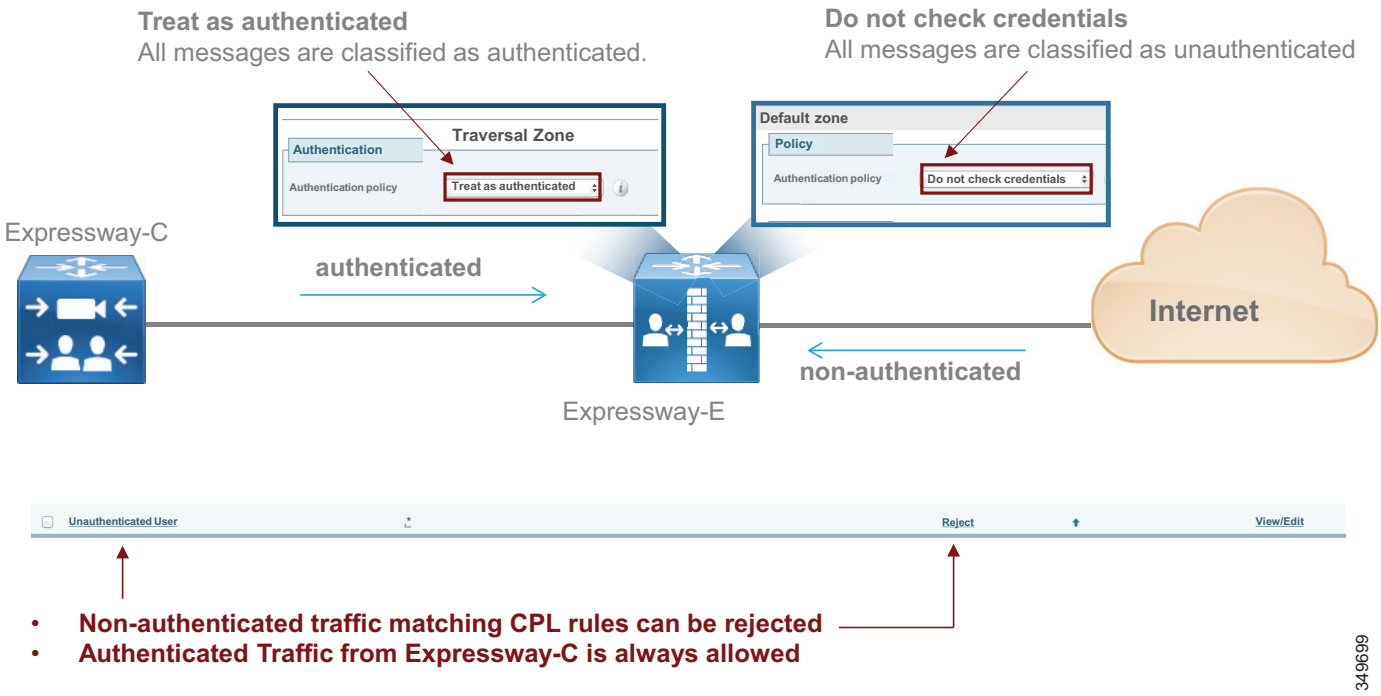
各企業は他の企業のエッジまでの暗号化を制御しており、エンドポイントはエンドポイントからリモート エッジへの暗号化されたコールを確立することができます。[暗号化を強制(force encrypted)] が Expressway で設定されている場合、暗号化ポリシーはインターネット上のメディアを保護できますが、コールがリモート エッジに達すると、コールが着信側エンドポイントに送信される前にエッジ レベルで復号化される可能性があります。

ダイヤル プランの保護と電話料金詐欺行為の緩和

インターネット上の望ましくないユーザからの合法的なコール試行、スパム コール、SIP または H.323 スキャンをブロックするために、呼処理言語(CPL)ルールを Expressway-E で使用することができます。CPL ルールはインターネットからのコール試行にのみ適用できます。

これを行うためには、トラバーサル クライアント ゾーンからのトラフィックを [認証(authenticated)] に設定し、インターネットからのトラフィックを [未認証(non-authenticated)] に設定します。CPL ルールは、認証されていないトラフィックのみに適用でき、内部ネットワークまたはインターネット上の信頼されたネイバーからのトラフィックの検査は回避されます。図 5-9 は、これについて説明しています。

図 5-9　　ゾーン認証ポリシー



CPL ルールはトップダウン方式を使用して処理されます。次の 2 つのポリシーのセットを作成できます。

- 許可ベースのポリシー

  許可ベースのポリシーは、正規表現（regex）を CPL に適用して、コールが内部的に設定された数字の範囲または英数字の URI 形式に一致する場合にのみ、そのコールを許可します。最後の CPL ルールはすべてのコールをブロックします。

- 拒否ベースのポリシー

  拒否ベースのポリシーは、ゲートウェイやボイスメールなどの特定のサービスに対するコールを拒否する一方で、ドメインが企業ドメインに一致する場合に残りのすべてを許可します。すべてのコールをブロックするデフォルトの CPL ルールは、最後のルールとして設定されます。

拒否ベースのポリシーの例として、コールが範囲 80XXXXXX にある一連のデバイスのみに許可され、ゲートウェイ アクセスや外部のインターネット宛先からの他のサービス（ここでは 0 と 9 で示す）は禁止される企業を想定します。この場合、ルールは 表 5-3 に示すように設定できます。

表 5-3　　拒否ベースのポリシーの例

ソース タイプ（Source Type）	[接続先（Destination）]	アクション
デフォルト ゾーン	**8[1-9]\d{6}@example\.com**	却下
デフォルト ゾーン	**[09]\d*@example\.com**	却下
デフォルト ゾーン	**\+\d*@example\.com**	却下
デフォルト ゾーン	**.*@example\.com**	許可（Allow）
デフォルト ゾーン	**.***	却下

さらに、発信側 ID に基づいてコールを拒否することも可能です。電気通信プロバイダーが発信者番号を確保する PSTN とは異なり、インターネットは自由であり、誰もユーザのアイデンティティをチェックしていません。したがって、発信側エイリアスに企業のドメインや Expressway-E の IP アドレスが含まれる場合は、Business-to-Business（B2B）の着信コールを拒否できます。

表 5-4 に記載する例は Cisco Expressway リリース 8.9 をベースにしています。

表 5-4　Expressway-E の IP アドレスを使用した拒否ベースのポリシーの例

ソース タイプ（Source Type）	接続元エイリアス（Source Alias）	接続先エイリアス（Destination Alias）	アクション
未認証	.*@10\.10\.10\.10.*	.*	却下
未認証	.*@example\.com.*	.*	却下

表 5-4 の 10.10.10.10 は、Expressway-E のパブリック アドレスを表します。これらのルールは、前のリストの「許可」ルール直前に追加できます。このようにすると、インターネットからのコールに企業のドメインや IP アドレスが含まれる場合、そのコールは拒否されるため、個人情報盗難が緩和されることになります。

デフォルト ゾーンが Business-to-Business（B2B）着信コールのターゲットであることから、デフォルト ゾーンの認証ポリシーは「クレデンシャルをチェックしない」ように設定する必要があります。このように設定すると、Business-to-Business（B2B）コールは認証されていないと見なされるため、ルールに照らし合わせてチェックされることになります。デフォルト ゾーンの認証ポリシーが「認証済みとして扱う」ように設定されている場合、トラバーサル ゾーンから発信された内部トラフィックは、このチェックをバイパスします（図 5-9 を参照）。

Expressway ソリューションのスケーリング

複数のインターネット エッジが展開されている場合は、コラボレーション トラフィックを最も近いインターネット エッジに送信するためのルーティング ルールを正しく設定することが重要です。

複数の Expressway-E と GeoDNS

Business-to-Business（B2B）コミュニケーションの拡張性は、複数の Expressway-C クラスタと Expressway-E クラスタを同じ物理位置にまたは地理的に分散して追加することによって解決できます。複数の Expressway-C と Expressway-E のペアが展開されている場合は、Unified CM が発信コールを発信側エンドポイントに最も近いエッジ サーバに転送できるため、内部 WAN トラフィックが最低限に抑えられます。大規模展開では、モバイル & リモート アクセスから分離した Expressway-C と Expressway-E のペア上で Business-to-Business（B2B）コミュニケーションをホストした方が適切な場合があります。これにより、サーバ リソースを外部インターネット通信専用にすることができます。

複数のインターネット エッジが展開されている場合は、それらの間の負荷分散方法を理解しておくことが重要です。インターネット エッジが同じデータセンターまたは同じエリアに展開されている場合は、DNS SRV レベルでロード バランシングを実行できます。たとえば、企業ネットワークに Business-to-Business（B2B）コミュニケーション用の 3 つのインターネット エッジが含まれており、それぞれが 2 つの Expressway-E ノードと Expressway-C ノードのクラスタで構成されている場合は、_sips._tcp.example.com レコードと _sip._tcp.example.com レコードに 6 つすべての Expressway-E レコードが同じ優先度と重要度で追加されます。これにより、登録とコールがさまざまな Expressway-E クラスタと Expressway-C クラスタに均等に分配されます。

ただし、Expressway クラスタが地理的地域全体に展開されている場合は、エンドポイントが確実に最も近い Expressway-E クラスタを使用するようにするため、DNS SRV の優先度と重要度のレコードに加えて何らかのインテリジェント メカニズムが必要になります。たとえば、ある企業が 2 つの Expressway クラスタを使用しており、1 つは米国（US）に、もう 1 つはヨーロッパ（EMEA）に設置されている場合、US に住んでいるユーザは US 内の Expressway-E クラスタに転送され、ヨーロッパに住んでいるユーザはヨーロッパ内の Expressway-E クラスタに転送されるのが理想的です。これは、GeoDNS サービスを実装することによって容易に実現できます。GeoDNS サービスはコスト効率が高く、設定が簡単です。GeoDNS を使用すれば、位置（IP アドレス ルーティング）や最小遅延などの複数のポリシーに基づいてトラフィックをルーティングできます。

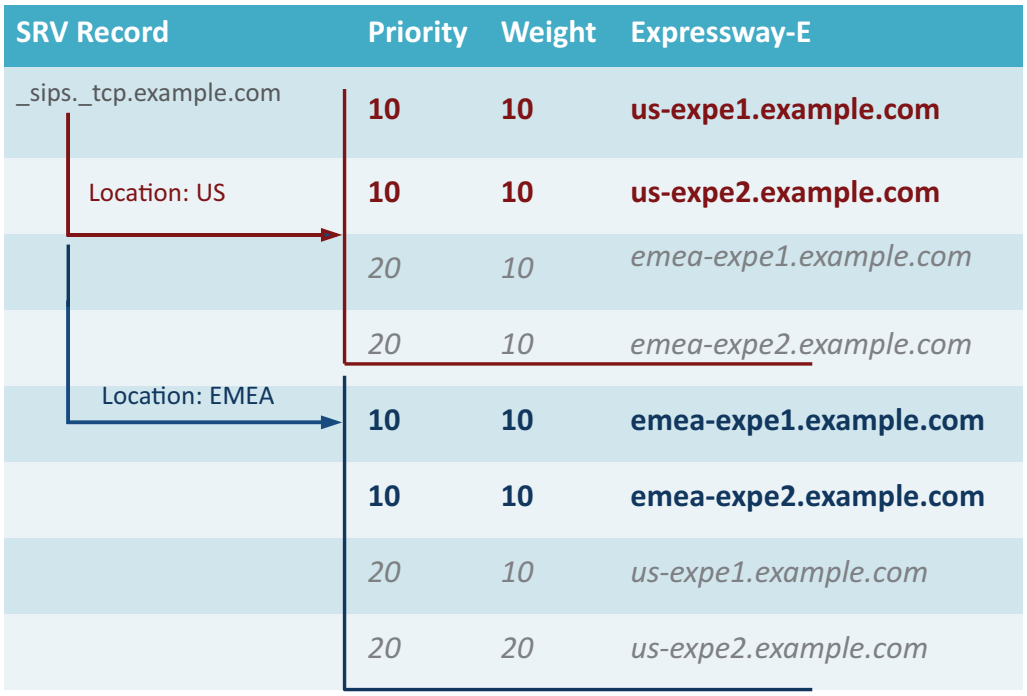
次に、GeoDNS サービス用の DNS を設定する例を示します。

このシナリオでは、2 つのインターネット エッジ Expressway クラスタを US とヨーロッパに 1 つずつ展開し、それぞれが 2 つの Expressway-C サーバと Expressway-E サーバで構成されます。発信側エンドポイントとヨーロッパ エッジ間で測定された遅延がエンドポイントと US エッジ間の遅延を下回っている場合、またはエンドポイントの IP アドレスが US の範囲に一致する場合、エンドポイントは設定されたポリシー（遅延または IP アドレス）に基づいてヨーロッパ エッジに転送されて登録されます。

一部の GeoDNS プロバイダーは、SRV レコードで GeoDNS サービスをサポートしていますが、多くのプロバイダーは CNAME または A レコードに対してのみ GeoDNS を許可しています。シンプルな構成と容易なトラブルシューティングを可能にするために、SRV レコードに GeoDNS サービスを実装することを推奨します。SRV レコードへの GeoDNS 設定を次の例に示します。

発信ユーザが米国にいる場合、コールは米国に送信されますが、米国のデータセンターが停止している場合、コールは EMEA に送信されます。この設定では、図 5-10 に示すように地理的冗長性が考慮されます。

図 5-10　SRV レコードへの GeoDNS 設定



CNAME レコードのみに対し GeoDNS サービスを指定し、SRV レコードに対しサービスを指定しないことを GeoDNS プロバイダーが許可している場合で、CNAME が GeoDNS サービスでサポートされている場合にのみ GeoDNS を設定する方法を次の例で示します。

このシナリオに従うと、DNS SRV レコードは CNAME レコードに解決されて、その CNAME レコードは A レコードに解決されます。CNAME レコードには地理的な場所を割り当てることができます。一例として、米国内に Expressway-E クラスタがあり、EMEA 内に別の Expressway-E クラスタがあるとします。SIP TLS の SRV レコード *_sips._tcp.example.com* や *_sip._tcp.example.com* は、Business-to-Business（B2B）コール用に設定されています。このレコードは CNAME レコード *alias1.example.com* に解決されます。

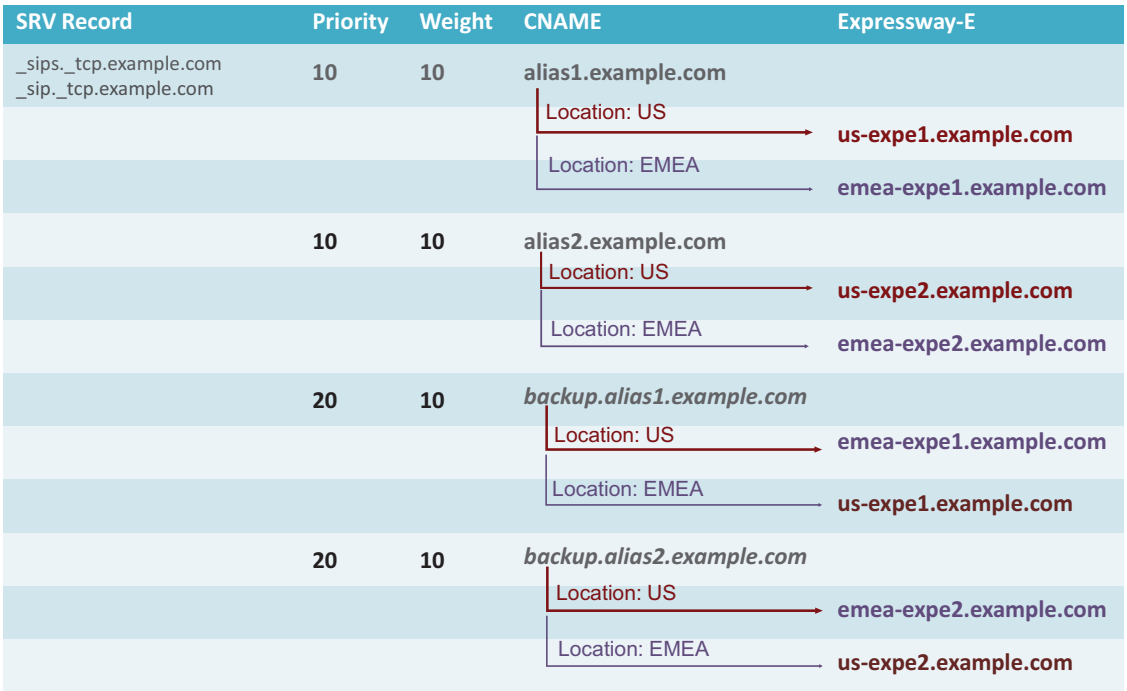
GeoDNS 設定に基づき、CNAME レコードには、そのレコードが有効な地域を識別するラベルが適用されます。この例では、CNAME は、優先度が高い（この例では 10）米国の A レコードと EMEA の別の A レコードに解決されます。これらの A レコードが、両方の地域にあるクラスタの最初のピアに対応します。

2 番目の CNAME レコードは、次に優先度が高い、米国および EMEA クラスタのピアに解決されます。このプロセスは、クラスタ内のすべてのピアが含まれるまで繰り返す必要があります。

地理的な冗長性を持たせるために、バックアップ CNAME エイリアスを作成する必要があります。図 5-11 の例では、*backup-alias1.example.com* が米国ユーザ用に最初の EMEA Expressway ピアに、EMEA ユーザ用に最初の US Expressway ピアに解決されることによって、両方の地域で地理的な冗長性が生まれます。バックアップ エイリアスのプロセスも、クラスタのすべてのピアが含まれるまで繰り返す必要があります。DSN SRV は低い優先度（この例では 20）に設定されているため、これらのバックアップ レコードが使用されるのは、最初のレコードが応答しない場合のみです。

図 5-11 に、CNAME レコードに適用される GeoDNS サービスの DNS レコード構造を示します。

図 5-11　　地理的な冗長性を持つ CNAME レコードの GeoDNS レコード構造



GeoDNS がない 2 つの異なる Expressway エッジ

GeoDNS 方式を採用することが推奨されますが、GeoDNS を展開できない場合があります。たとえば、DNS レコードが GeoDNS サービスを提供していないサービス プロバイダーによって管理されている場合、または複数のエッジがエッジ間で選択する GeoDNS の容量より少ない地域で展開される場合などです。たとえば、GeoDNS は発信側エンドポイントの場所がカリフォルニアにあるかペンシルバニアにあるかを識別することはできても、発信側ロケーション エンドポイントがサンノゼにあるかサンディエゴにあるかを識別することはできない場合があります。したがって、2 つの Expressway クラスタがサンノゼとサンディエゴにある場合、GeoDNS は使用できないことがあります。

別のソリューションとしては、宛先のエンドポイントまたはデバイスに最も近いエッジを返すように設計します。この場合は、宛先エンドポイントの位置を検索または確認して、該当するエッジを返す必要があります。このソリューションのメリットは、最短の内部パスをエンドポイントに提供することによって顧客ネットワーク上の帯域幅の使用が最小限に抑えられることです。

このシナリオでは、Business-to-Business（B2B）SRV レコードはすべての Expressway サーバで同じ優先度と重要度で設定されます。

たとえば、EMEA 内の 2 つの Expressway-C クラスタと Expressway-E クラスタと、APJC 内の別の 2 つの Expressway-C クラスタと Expressway-E クラスタについて考えます。EMEA 内の Expressway-C トランク上の Unified CM インバウンド コーリング サーチ スペースには、EMEA 電話機のパーティションは含まれますが、APJC 電話機のパーティションは含まれません。同様に、APJC 内の Expressway-C トランク上のインバウンド コーリング サーチ スペースには、APJC 電話機のパーティションは含まれますが、EMEA 電話機のパーティションは含まれません。EMEA 内のインターネット上のユーザが APJC にある企業エンドポイントにコールした場合は、そのコールが EMEA または APJC の Expressway クラスタに送信されます。

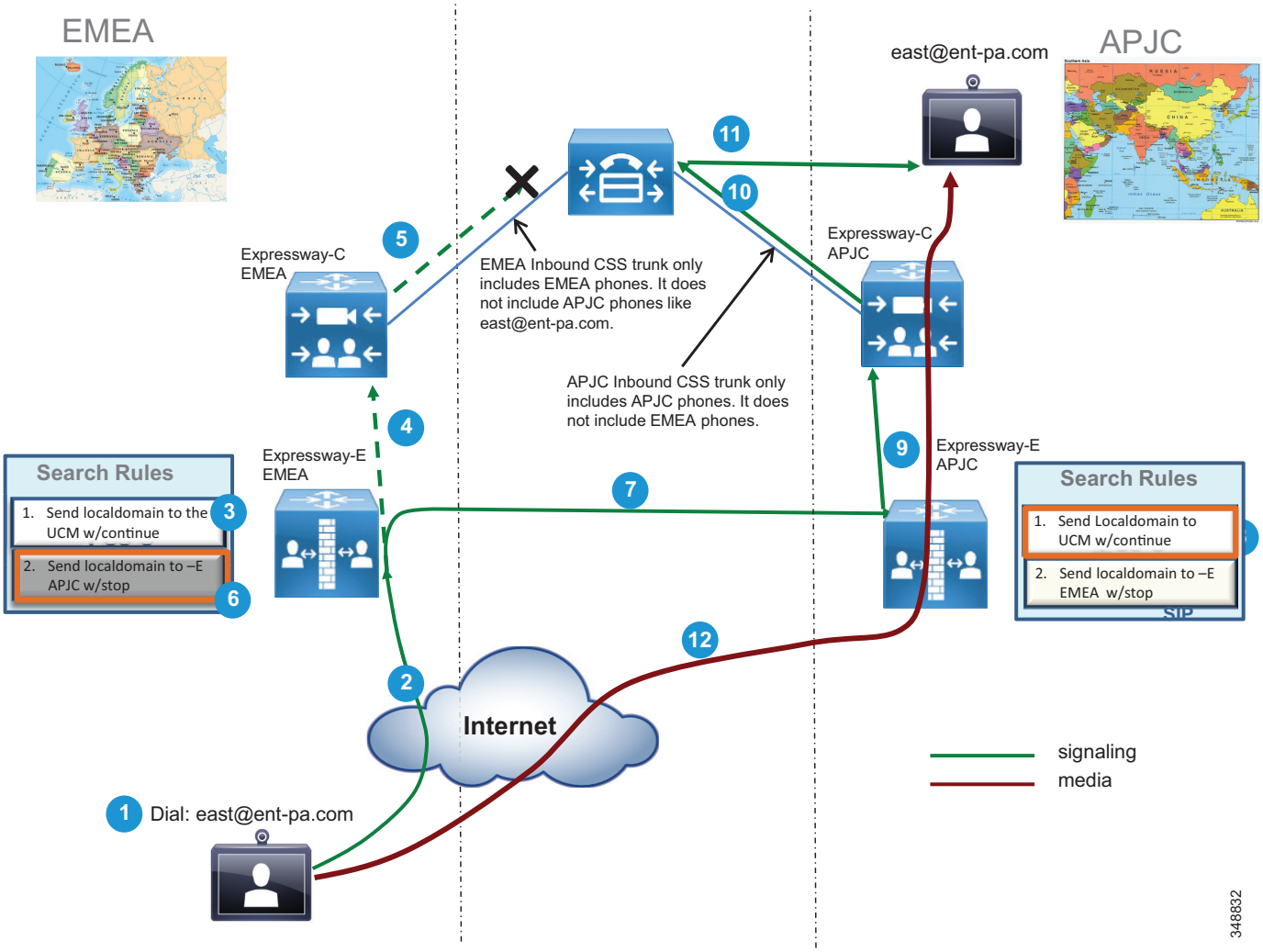
この例では、コールが EMEA Expressway-E クラスタに送信されると仮定します。EMEA Expressway-E と Expressway-C はそのコールを宛先に送信しようとしますが、Expressway-C トランクのインバウンド コーリング サーチ スペースがそのコールをブロックします。次に EMEA Expressway-E はそのコールを APJC Expressway E に転送します。こうして、コールが宛先に配信されます。これは、APJC Expressway-C のインバウンド コーリング サーチ スペースに APJC エンドポイントのパーティションが含まれているためです。

EMEA 内の Expressway-E がシグナリングとメディアのパスからそれ自体を削除できるようにするには、Expressway-E EMEA クラスタ上に TCP/TLS 変換または RTP/SRTP 変換が確実に存在しないようにし、すべての Expressway-C と Expressway-E ノードでコール シグナリング最適化パラメータを確実に [オン（On）] に設定することが重要です。

これは確定的プロセスではないため、Expressway エッジが 3 つ以上の場合は、検索メカニズムに時間がかかりすぎることがあります。したがって、この設定は Expressway エッジが 2 つ以下の場合にお勧めします。3 つ以上のエッジが必要な場合は、Directory Expressway アーキテクチャを導入することを推奨します。Directory Expressway アーキテクチャについては、このマニュアルでは説明しません。

図 5-12 に、宛先エンドポイントに最も近いエッジの選択を可能にする Expressway エッジ設計を示します。

図 5-12　　宛先に最も近い Expressway クラスタの選択

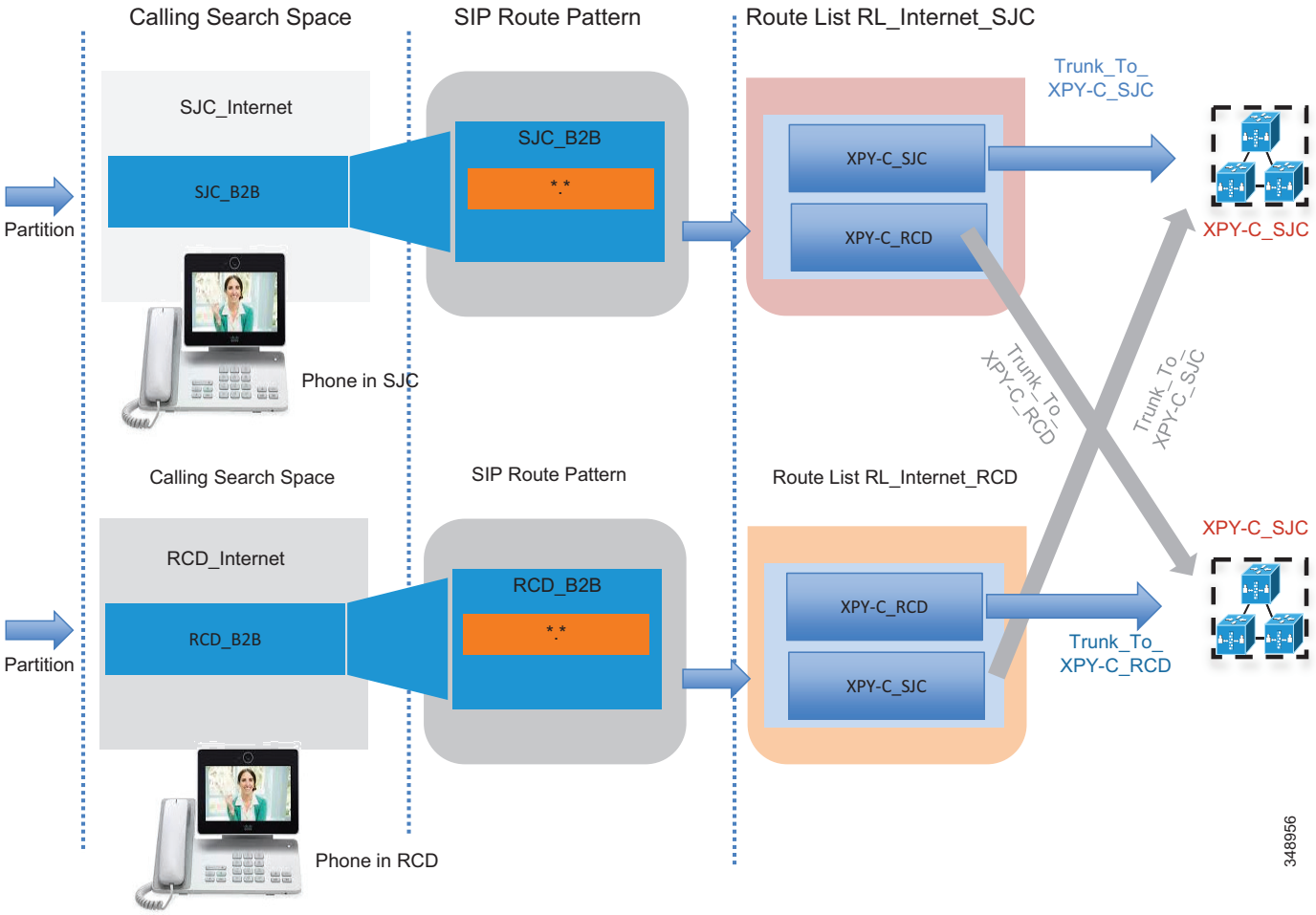


このアーキテクチャは、3 つ以上のサイトに拡張でき、Directory Expressway と呼ばれる中央の Expressway ノードが必要です。Directory Expressway は、異なる地域の Expressway 間でトランジット ノードとして機能する Expressway です。Directory Expressway アーキテクチャについては現在、このマニュアルでは説明していません。

発信コールに関する留意点

発信コールは発信側のエンドポイントに最も近い Expressway-C に転送する必要があります。これは、コーリング サーチ スペースやパーティションなどの Cisco Unified CM メカニズムを使用して実現できます。図 5-13 に、Unified CM の設定を示します。

図 5-13　最も近い Expressway-C クラスタに発信コールを転送し、最も近いクラスタが使用できない場合にバックアップ クラスタを使用する Unified CM の設定



Unified CM ローカル ルート グループ機能は、複数のサイトが複数の Expressway-C クラスタにアクセスする場合にこのソリューションのスケーリングに役立ちます。このメカニズムは、ISDN ゲートウェイおよび Cisco Unified Border Element にも適用されます。設定の詳細は、Cisco Unified Border Element や音声ゲートウェイにも当てはまるため、次の 2 つのセクションで説明します。

ゲートウェイのベスト プラクティス

ここでは、ゲートウェイに関する次のベスト プラクティスについて取り上げます。

ゲートウェイ ゲイン設定の調整

ゲートウェイを介して Cisco Unified Communications ネットワークを PSTN に接続するには、停電、インピーダンスの不整合、および遅延などによるエコーや信号の減衰から生じる、メディア品質問題に適切に対処する必要があります。このため、予期されるすべての音声パスに信号損失の状況を詳細に提供する Network Transmission Loss Plan（NTLP）を確立する必要があります。このプランを使用して、最適な声の大きさと効果的なエコー キャンセレーションを得るために信号の強さを調整する必要があるロケーションを識別できます。すべての通信事業者が同じ損失プランを使用するわけではないこと、また、セルラー ネットワークの存在が NTLP の作成をさらに複雑にすることに注意してください。このような NTLP を作成する前に、ゲートウェイで入力ゲインや出力衰退を調整することは推奨できません。詳細については、次の Web サイトで入手可能な『*Echo Analysis for Voice Over IP*』を参照してください。

https://www.cisco.com/en/US/docs/ios/solutions_docs/voip_solutions/EA_ISD.pdf

PSTN からの着信コールのルーティング

PSTN からの着信コールをルーティングするには、次のいずれかの方法を使用します。

- ビデオおよび音声コールの両方に対して、単一のディレクトリ番号を各ユーザに割り当てます。この方法では、音声のみのコールを含む、ビデオ ゲートウェイの PSTN からすべてのコールが受信されるため、推奨されません。貴重なビデオ ゲートウェイ リソースが浪費され、拡張が困難です。
- Unified CM クラスタ内にあるビデオ対応デバイスごとに、少なくとも 2 つの異なる電話番号を割り当て、1 つの回線を音声用、もう 1 つをビデオ用とします。この方法では、外部の（PSTN）発信者はビデオを有効にするために、正しい番号をダイヤルする必要があります。
- ビデオ コールの場合は、外部の発信者にビデオ ゲートウェイのメイン番号をダイヤルしてもらいます。Cisco ISDN および Serial ゲートウェイは統合された自動応答機能を提供し、発信者に相手側の内線番号の入力を求めます。次に、Unified CM は、それがビデオ コールであることを認識し、宛先デバイスを呼び出します。この方法では、発信者はそれぞれの着信側ごとに 2 つの異なる DID 番号を覚える必要はありませんが、着信ビデオ コールをダイヤルするという余分な手順が増えます。

（注）　外部のビデオ エンドポイントは、IVR プロンプトに着信側の内線番号を入力するために、DTMF をサポートしている必要があります。

次の例は、2 番めの方法を示しています。

ユーザは、ビデオ機能が有効になっている Cisco Unified IP Phone を所有しています。IP Phone の内線番号は 51212 で、完全修飾 DID 番号は 1-408-555-1212 です。DID 番号をダイヤルするだけで、音声専用コールの PSTN からそのユーザに到達できます。CO は、Cisco 音声ゲートウェイに接続した T1-PRI 回線（複数の場合もある）を通じて、その DID 番号にコールを送信します。ゲートウェイでコールが受信されると、Unified CM はゲートウェイが音声専用であることを認識し、そのコール用に 1 つの音声チャネルのみのネゴシエーションを行います。逆に、PSTN からビデオ コールのためにそのユーザに到達するには、ビデオ ゲートウェイのメイン番号をダイヤルした後、ユーザの内線番号を入力する必要があります。たとえば、1-408-555-1000 をダイヤルするとします。CO は、Cisco ISDN ビデオ ゲートウェイに接続されている T1-PRI 回線（複数の場合もある）を通じて、その番号にコールを送信します。ゲートウェイでコールが受信されると、自動応答プロンプトが発信元に、到達すべき相手の内線番号の入力を求めます。発信者が DTMF トーンで内線番号を入力すると、Unified CM はゲートウェイにビデオ機能があることを認識し、そのコール用に音声とビデオの両方のチャネルをネゴシエートします。

ゲートウェイの番号操作

Cisco TelePresence ISDN Gateway 8321 および 3241、Cisco TelePresence Serial Gateway 8330 および 3340 にはすべて、番号操作の機能があります。これらのビデオ ゲートウェイには、複数のダイヤル プラン ルールを設定できます。これらのルールは、発信番号および/または着信番号に基づいて照合され、IP から PSTN または PSTN から IP の方向のいずれかで機能します。着信コールが設定されたダイヤル プラン ルールと一致すると、ISDN または Serial ゲートウェイは次のいずれかの処理を実行できます。

- コールの拒否
- 自動応答の開始
- 番号（または PSTN から IP へのコールの場合、IP アドレス、ホスト名、または URI）にコールする

アクションがある番号へのコールである場合、元の着信番号またはその一部を、コールする新しい番号に使用できます。

詳細については、次のマニュアルを参照してください。

- 次の URL から入手可能な Cisco TelePresence ISDN Gateway のマニュアル
  https://www.cisco.com/en/US/products/ps11448/tsd_products_support_series_home.html
- 次の URL から入手可能な Cisco TelePresence Serial Gateway のマニュアル
  https://www.cisco.com/en/US/products/ps11605/tsd_products_support_series_home.html

PSTN への発信コールのルーティング

発信コールを PSTN へルーティングするには、次のいずれかの方法を使用します。

- 音声コールとビデオ コールに異なるアクセス コード（異なるルート パターン）を割り当てます。たとえば、ユーザが 9 の後にコール先の PSTN 電話番号をダイヤルすると、それがコールを音声ゲートウェイに送るルート パターンと一致します。同様に、数字の 8 を、ビデオ ゲートウェイにコールを渡すルート パターンとして使用することもできます。
- Unified CM クラスタ内にあるビデオ対応デバイスごとに、少なくとも 2 つの異なる電話番号を割り当て、1 つの回線を音声用、もう 1 つをビデオ用とします。その後、2 つの回線に異なるコーリング サーチ スペースを指定します。ユーザが第 1 の回線上でアクセス コード（たとえば 9）をダイヤルすると音声ゲートウェイにつながり、同じアクセス コードを第 2 の回線上でダイヤルするとビデオ ゲートウェイにつながります。この方法では、ユーザが 2 つの異なるアクセス コードを覚える必要がありませんが、コールの発信時に電話機で正しい回線を押す必要があります。ただし、すべてのシスコ ビデオ エンドポイントが現時点で複数回線をサポートしているわけではなく、その場合は、発信コールを PSTN にルーティングする方法として、プレフィックスの使用をお勧めします。

ビデオ ゲートウェイ コールの帯域幅

特定のプレフィックスを持つコールが PSTN への ISDN 接続で特定の最大消費帯域に制限されるように、Cisco TelePresence ISDN Gateway のダイヤル プラン ルールを設定できます。これは、1 つのコールが PRI リンク全体を独占できないようにする際に便利です。ゲートウェイにサービス プレフィックスを設定するときは、次のいずれかの最大速度を選択できます。

- 128 kbps
- 192 kbps
- 256 kbps
- 320 kbps
- 384 kbps
- 512 kbps
- 768 kbps
- 1152 kbps
- 1472 kbps

IP エンドポイントから PSTN へ向かうコールは、ゲートウェイがそのコールにどのサービスを使用するかを決定できるように、着信番号の先頭にサービス プレフィックスを含めることができます。オプションとして、番号の先頭にサービス プレフィックスを含んでいないコールに使用する、デフォルト プレフィックスを設定できます。この方法は、非常に複雑になる可能性があります。ユーザは、求めるコール速度を得るためにダイヤルすべきプレフィックスを覚えておく必要があるからです。また、管理者は、Unified CM で複数の（速度ごとに 1 つずつ）ルート パターンを設定する必要があります。

（注）　Cisco TelePresence ISDN Gateway の 2 つのグローバル設定を使用して、着信および発信 ISDN コールの帯域幅の最小値または最大値を設定できます。ダイヤル プランによって、これよりも大きい最大帯域幅に上書きすることはできません。ただし、ダイヤル プランによって、特定のコールに対し、より小さい帯域幅を強制することはできます。

自動代替ルーティング（AAR）

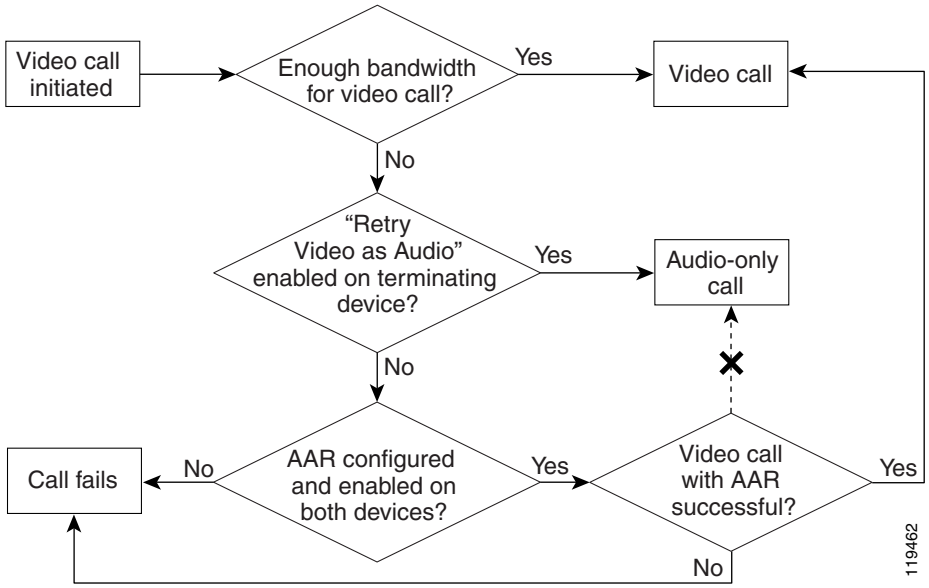
IP ネットワークにコールを処理できるだけの帯域幅がない場合、Unified CM はコール アドミッション制御メカニズムを使用して、コールの処理方法を決定します。Unified CM は設定に従って、次のいずれかの処理を実行します。

- コールに失敗し、発信側に対してビジー トーンを再生し、発信側の画面に「帯域幅が使用できません（Bandwidth Unavailable）」メッセージを表示します。
- ビデオ コールを音声のみのコールとして再試行します。
- Automated Alternate Routing（AAR; 自動代替ルーティング）を使用し、PSTN ゲートウェイなどの代替パス上でコールを再ルーティングします。

Retry Video Call as Audio オプションは、終端（着信側）デバイスでのみ有効です。そのため、発信側デバイスでは宛先ごとに異なるオプション（再試行または AAR）を使用できる柔軟性があります。

帯域幅の制限が原因でビデオ コールが失敗した場合、自動代替ルーティング（AAR）が有効であれば、Unified CM は失敗したコールをビデオ コールとして AAR の宛先に再ルーティングしようとします。AAR が有効でない場合、失敗したコールによって、発信者にビジー トーンとエラー メッセージが送信されます（図 5-14 を参照）。

図 5-14　　ビデオ コールで起こり得るシナリオ



音声コールまたはビデオ コールに AAR を使用できるようにするには、発信側デバイスと着信側デバイスを AAR グループのメンバーとして設定し、着信側デバイスに外部電話番号マスクを設定する必要があります。外部電話番号マスクによって、ユーザの内線用の完全修飾 E.164 アドレスが指定されます。また、AAR グループによって、コールが PSTN 上で正しくルーティングされるために、着信側デバイスの外部電話番号マスクの前に付加すべき数字が示されます。

たとえば、ユーザ A が San Jose AAR グループに属し、ユーザ B が San Francisco AAR グループに属しているとします。ユーザ B の内線番号は 51212 で、外部電話番号マスクは 6505551212 です。AAR グループは、San Jose と San Francisco の AAR グループ間のコールに対して、番号の前に 91 を付加するよう設定されています。この場合、ユーザ A が 51212 をダイヤルし、2 つのサイト間の IP WAN 上にそのコールを処理できるだけの帯域幅がない場合、Unified CM はユーザ B の外部電話番号マスクである 6505551212 を選択し、その前に 91 を付加して 916505551212 への新規コールを生成し、ユーザ A 用の AAR コーリング サーチ スペースを使用します。

Unified CM のデフォルトでは、すべてのビデオ対応デバイスで Retry Video Call as Audio オプションが有効（オン）になります。したがって、ビデオ コールで AAR を使用できるようにするには、Retry Video Call as Audio オプションを無効（オフ）にする必要があります。また、ロケーション間でリソース予約プロトコル（RSVP）に基づいたコール アドミッション制御ポリシーが使用されている場合は、RSVP ポリシーを音声ストリームとビデオ ストリームの両方について Mandatory に設定する必要があります。

さらに、Unified CM は、着信側デバイスだけを見て Retry Video Call as Audio オプションが有効か無効かを判断します。したがって、上記のシナリオで AAR プロセスが実行されるためには、ユーザ B の電話機で Retry Video Call as Audio オプションが無効にされている必要があります。

最後に、デバイスは 1 つの AAR グループだけに所属できます。AAR グループによって、どの数字を前に付加するかが決定されるため、再ルーティングされたコールにどのゲートウェイが使用されるかにも影響があります。前項で述べたように、PSTN への発信コール ルーティングの設定に何を選択したかに応じて、AAR によって再ルーティングされるビデオ コールは、ビデオ ゲートウェイでなく音声ゲートウェイに送られる可能性もあります。したがって、AAR グループと AAR コーリング サーチ スペースの構築は入念に行い、必ず正しい数字が付加され、AAR に正しいコーリング サーチ スペースが使用されるようにしてください。

こうした考慮事項により、大規模な企業環境での AAR の設定がかなり複雑になる可能性がありますが、エンドポイントのタイプが 2 つのどちらかに限定されている場合には、AAR の実装が容易です。エンドポイントが音声とビデオの両方のコールに対応している場合（Cisco Unified IP Phone 9971 または Cisco TelePresence System EX90）は、AAR の設定が非常に複雑になることがあります。したがって、音声とビデオのエンドポイントが混在する大企業では、ユーザごとに AAR の重要性をよく考え、専用のビデオ会議室や経営幹部用ビデオ システムなど、一部のビデオ デバイスだけに AAR を使用してください。表 5-5 に、さまざまなデバイス タイプで AAR を使用するのが適切なシナリオのリストを示します。

表 5-5　デバイス タイプ別の AAR 使用条件

デバイスタイプ（Device Type）	デバイスを使用したコールの宛先	AAR の必要性	説明
IP Phone	他の IP Phone およびビデオ対応デバイス	○	ビデオ対応デバイスにコールするときでも、発信元デバイスが音声専用なので、コールを音声ゲートウェイにルーティングするように AAR を設定できます。
Cisco Jabber または Cisco Unified IP Phone 9971	他のビデオ対応デバイスのみ	○	デバイスは必ずビデオ コールに使用されるので、AAR グループを設定できます。
	IP Phone およびその他のビデオ対応デバイス	なし	音声専用コールではビデオ コールと異なるルーティングを行うように AAR グループを設定するのは困難です。
H.323 または SIP クライアント	他のビデオ対応デバイスのみ	○	デバイスは必ずビデオ コールに使用されるので、AAR グループを設定できます。
	IP Phone およびその他のビデオ対応デバイス	なし	音声専用コールではビデオ コールと異なるルーティングを行うように AAR グループを設定するのは困難です。

最低料金選択機能

最低料金選択機能（LCR）とテールエンド ホップオフ（TEHO）は、VoIP ネットワークでは非常によく知られており、ビデオ コールにも利用できます。一般的にどちらの用語も、長距離電話番号へのコールが IP ネットワークを通じて宛先に最も近いゲートウェイにルーティングされ、通話料金が安くなるような、コール ルーティング ルールの設定方法を指しています。Unified CM は、次のような豊富な番号分析機能と番号操作機能のセットを使用して、この機能をサポートします。

- パーティションとコーリング サーチ スペース
- トランスレーション パターン
- ルート パターンとルート フィルタ
- ルート リストとルート グループ

LCR をビデオ コール用に設定するのは、音声コールの場合よりも少し複雑で、その理由は次のとおりです。

- この章ですでに述べたように、ビデオ コールには独自の専用ゲートウェイが必要です。
- ビデオ コールには、音声コールをはるかに上回る帯域幅が必要です。

専用ゲートウェイに関しては、LCR をビデオ コールに使用するかどうかを決めるための基礎となるロジックは、自動代替ルーティング（AAR）（5-37 ページ）の項で説明したロジックとほとんど同じです。音声とビデオ用にさまざまなタイプのゲートウェイが必要になるため、LCR で音声コールを 1 つのゲートウェイに送り、ビデオ コールを別のゲートウェイに送るために必要なすべてのパーティション、コーリング サーチ スペース、トランスレーション パターン、ルート パターン、ルート フィルタ、ルート リスト、およびルート グループを設定するのは、かなり複雑な作業になる可能性があります。

帯域幅の要件に関しては、LCR を使用するかどうかは、特定のロケーションとの間を結ぶビデオ コールの LCR をサポートできるだけの帯域幅が、使用している IP ネットワークにあるかどうかで決まります。現在の帯域幅が十分でない場合は、IP ネットワークをアップグレードしてビデオ コール用の空きを作ったり、ローカル ゲートウェイを導入して PSTN 上でコールをルーティングしたりするためのコストと、ビデオ コールの利点を比較する必要があります。たとえば、ある中央サイトに 1.544 Mbps の T1 回線を介して支社が接続されているとします。その支店内には、20 人のビデオ機能を持つユーザがいます。1.544 Mbps の T1 回線は、最大でほぼ 4 つの 384 kbps ビデオ コールを処理できます。この場合、中央サイトまでビデオ コールをルーティングして、通話料金を節約することに意味があるかどうかが問題です。サポートするコールの数に応じて、1.544 Mbps の T1 回線をもっと高速のものにアップグレードしなければならない場合もあります。ビデオには、そうしたアップグレードに要する毎月の追加料金に見合うだけの重要性があるのでしょうか。ない場合は、その支社に Cisco ビデオ ゲートウェイを導入すると、LCR に煩わされずに済みます。しかし、各支社へのローカル Cisco ビデオ ゲートウェイの配置も安価には行えないため、最終的には、ビデオから公衆網へのコールがビジネスにとってどれほど重要であるかを判断しなければなりません。ビデオが重要でないなら、帯域幅をアップグレードしたりビデオ ゲートウェイを購入したりするよりも、Retry Video Call as Audio 機能を使用し、使用可能な帯域幅を超過した場合にビデオ コールを音声専用コールとして再ルーティングした方がよいこともあります。コールが音声専用までダウングレードされると、LCR を実行するためのローカル ゲートウェイ リソースと帯域幅は、もっと手ごろな価格で設定しやすいものになります。

FAX とモデムのサポート

Cisco ゲートウェイ全体に対する FAX とモデムのサポートについては、次のマニュアルを参照してください。

- 次の URL から入手可能な『*Cisco Unified Communications System 9.0 SRND*』の「*Gateways*」の章を参照してください。

  https://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/9x/gateways.html

- 次の URL から入手可能な『*Fax, Modem, and Text Support over IP Configuration Guide*』

  https://www.cisco.com/en/US/docs/ios-xml/ios/voice/fax/configuration/15-mt/vf-15-mt-book.html

Cisco Unified CM トランク

改訂日：2017 年 2 月 7 日

トランクとは、Cisco Unified Communications Manager（Unified CM）における通信チャネルであり、Unified CM はトランクを使用することによって他のサーバと接続できます。1 つ以上のトランクを使用して、音声コール、ビデオ コール、および暗号化されたコールの送受信やリアルタイム イベント情報の交換など、Unified CM から呼制御サーバおよびその他の外部サーバとのさまざまな通信を行うことができます。

トランクは、Cisco Collaboration システムの導入における重要かつ不可欠な部分であるため、利用可能なトランクの種類、それらの機能に加え、障害復旧力、容量、ロード バランシングといった設計および導入時に考慮すべき事項について理解することが重要となります。

Unified CM で設定できる基本的なトランクには、次の 2 種類があります。

- SIP トランクと H.323 トランク。いずれも、外部通信に使用できます。
- クラスタ間トランク（ICT）。

H.323 トランクは引き続きサポートされていますが、SIP トランクが Unified Communications の導入で推奨されるトランク タイプになります。これは、SIP トランクが H.323 トランクでは使用できない追加の機能を提供するためです。この章では、H.323 と SIP トランク機能の比較の概要を示しますが、重点は置くのは SIP トランクであり、その操作と、Unified Communications 導入向けの機能を説明します。H.323 トランクの機能と操作の詳細については、次の Web サイトで入手可能な『*Cisco Collaboration 9.x SRND*』の「*Cisco Unified CM Trunks*」の章を参照してください。

https://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/collab09/trunks.html

Unified CM トランクのアプリケーションの詳細については、このマニュアルの次の章の各項を参照してください。

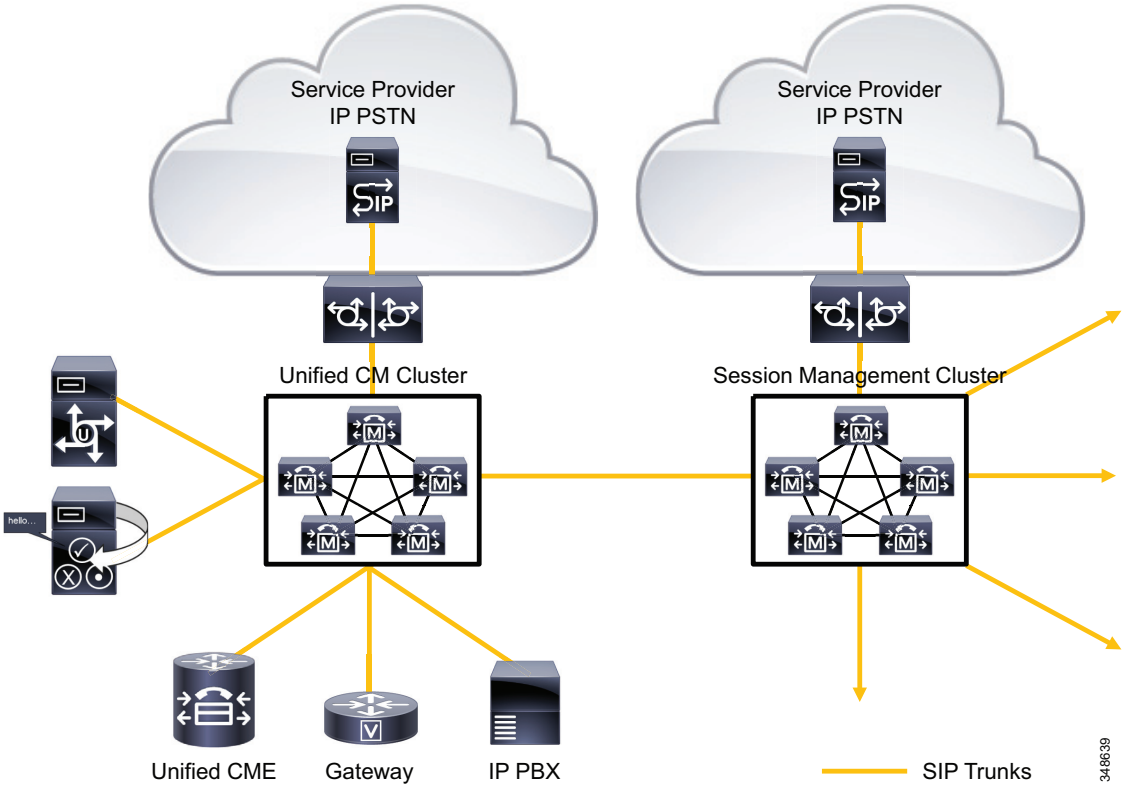
- コラボレーションの配置モデル（10-1 ページ）
- メディア リソース（7-1 ページ）
- 帯域幅管理（13-1 ページ）
- コラボレーションのインスタント メッセージングとプレゼンス（20-1 ページ）

Unified CM トランク ソリューション アーキテクチャ

Cisco Unified CM では、IP トランクのメカニズムを使用して、Unified Communications ソリューションの他のコンポーネントとコール関連情報を交換します。この点においてトランクは重要であるため、プロトコル、期待される機能およびサービス、パフォーマンス要件などを適切に考慮して IP トランクのシステム アーキテクチャを開発することが重要です。

図 6-1 に、システムの接続性の観点から IP トランクの役割を示します。この図には、Unified CM クラスタからのすべての接続が示されているわけではありません。

図 6-1　　IP トランクによって提供される Unified CM への接続



コールは、ダイヤル プランでの定義に従って、ルート パターン コンストラクトを使用してトランクに転送されます。ルート パターンでは、直接トランクを使用することも、ルート リストを通してトランクを使用することもできます。ルート リストが使用される場合、そのルート リストは、それぞれが 1 つ以上のトランクを含む 1 つ以上のルート グループから構成されます。ルート グループ内の個別のトランクは、トップダウン的に選択されるように設定することも、循環的に選択されるように設定することもできます。発信コールでは、ルート パターンを使用して、このように関連付けられたトランクの 1 つが Unified CM によって選択されます。Unified CM では、着信コールを受け付ける前に、コールの発信元のリモート アドレスにトランクが定義されているかどうかが確認されます。

SIP トランクおよび H.323 トランクの比較

Cisco Unified CM トランク接続は、SIP と H.323 の両方のトランクをサポートしています。SIP または H.323 のどちらを使用するかの決定は、それぞれのプロトコルで提供される固有な機能に大きく影響されます。過去のいくつかのリリースでは、Unified Communications ベンダーおよびお客様の両方の間で SIP の人気が拡大するにつれ、SIP トランクがサポートする機能も拡大して H.323 トランクよりも豊富な機能セットを提供できるようになり、Unified Communications の導入で推奨されるようになりました。現在多くのお客様が、H.323 トランクおよびゲートキーパーベースの Unified Communications の導入から、SIP トランクのみを使用し、トランクとダイヤルプランの集約プラットフォームとして Cisco Unified Communications Manager Session Manager Edition を使用する導入へ移行しています。

表 6-1 に示されるように、SIP および H.323 トランクがシスコ デバイス間のトランク接続で同じ機能を多数共有していますが、SIP トランクは H.323 トランクでサポートされていない複数の機能をサポートします。他のベンダーの製品およびサービス プロバイダー ネットワークへのトランク接続では、SIP が今日最もよく使用されているプロトコルで、H.323 などのプロトコルを使用している Unified Communications の製品およびネットワークが SIP に移行するにともない、その使用が拡大しています。

表 6-1 に、Unified CM クラスタ間での SIP および H.323 トランクを介して提供される機能の一部についての比較を示します。

表 6-1　Cisco Unified CM トランクでの SIP および H.323 機能の比較

機能	SIP	H.323
発呼回線（番号）ID 表示	○	○
発呼回線（番号）ID 表示禁止	○	○
発信者名 ID 表示	○	○
発信者名 ID 表示禁止	○	○
接続回線（番号）ID 表示	○	○
接続回線（番号）ID 表示禁止	○	○
接続者名 ID 表示	○	○
接続者名 ID 表示禁止	○	○
[呼び出し表示（Alerting Name）]	○	***X***
転送（ブラインドまたは在席）	Yes/Yes	Yes/Yes
すべてのコールの転送	○	○
話中転送	○	○
自動転送（無応答）	○	○
QSIG 呼完了（ビジー サブスクライバ）	○	○
QSIG 呼完了（無応答）	○	○
QSIG パス置換	○	○
サブスクライブ/通知、パブリッシュ - 表示	○	***X***
メッセージ待機インジケータ（MWI：ランプ点灯/消灯）	○	***X***
コール保留/復帰	○	○
保留音（ユニキャストおよびマルチキャスト）	○	○

表 6-1　Cisco Unified CM トランクでの SIP および H.323 機能の比較（続き）

機能	SIP	H.323
DTMF リレー	RFC 2833、KPML（OOB）、Unsolicited Notify（OOB）	H.245 アウトオブバンド（OOB）[1]
SIP アーリー オファー	はい：MTP が必要な場合があります	該当なし
ベスト エフォートのアーリー オファー	はい：MTP は使用されません。可能な場合、SIP アーリー オファーが送信されます。それ以外の場合は、SIP ディレイド オファーが送信されます。	該当なし
SIP ディレイド オファー	○	該当なし
H.323 Fast Start	該当なし	はい：発信 Fast Start のために常に MTP が必要：音声コールのみがサポート対象
受信オファーのオーディオ コーデック プリファレンスの受け入れ	○	***X***
SIP アーリー オファー/H323 Fast Start に対する MTP によるコーデック	[音声コールとビデオ コールに対する早期オファーのサポート：必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls - Mandatory (insert MTP if needed)）] または [音声コールとビデオ コールに対する早期オファーのサポート：ベスト エフォート（MTP の挿入なし）（Early Offer support for voice and video calls - Best Effort (no MTP inserted)）] が選択されている場合は、すべてのコーデックがサポートされます。 [MTP が必須（MTP Required）] がオンの場合は、G.711、G.729	G.711、G.723、G.729 のみ
[ビデオ（Video）]	○	○
ビデオ コーデック	H.261、H.263、H.263+、H.264 AVC	H.261、H.263、H.263+、H.264 AVC

表 6-1　Cisco Unified CM トランクでの SIP および H.323 機能の比較（続き）

機能	SIP	H.323
ビデオ プレゼンテーション共有（BFCP）	○	*X*
Multi-Level Precedence and Preemption（MLPP）	○	○
T.38 Fax	○	○
シグナリング認証	ダイジェスト、TLS	*なし*
シグナリング暗号化	TLS	*なし*
メディア暗号化（音声）	SRTP	SRTP
RSVP ベースの QoS およびコール アドミッション制御	○	*X*
+ 文字のサポート	○	*X*
着信の着呼側変換	○	○
着信の発呼側変換	○	○
接続先変換	○	○
発信の発呼側変換	○	○
発信の着呼側変換	○	○
発信の発呼側/着呼側番号タイプの設定	SIP は番号タイプをサポートしません	Unified CM、Unknown、National、International、Subscriber
発信の着呼側/発呼側番号計画の設定	SIP は番号計画をサポートしません	Unified CM、ISDN、National Standard、Private、Unknown
トランクの宛先：状態検出メカニズム	OPTIONS ping	*コール別の試行*
IPv6、デュアル スタック、ANAT	○	*X*
相互運用性のためのプロトコル変更スクリプト	○	*X*
すべての Unified CM ノードで実行	○	○
最大 16 の宛先アドレス	○	○
URI ベースのコール	○	X
地理的位置のサポート	○	○

1. H.323 トランクは、特定の接続の種類で、RFC 2833 に規定されたシグナリングをサポートします。

SIP トランクの概要

SIP トランクによって、ゲートウェイ、Cisco Unified CM Session Management Edition、SIP プロキシ、Unified Communications アプリケーション、その他の Unified CM クラスタなど、他の SIP デバイスに接続できます。現在、サービス プロバイダーや Unified Communications アプリケーションに接続するときに、最も一般的に選択されるプロトコルは、ほぼ間違いなく SIP です。Cisco Unified CM では、次の SIP トランクとコール ルーティングの機能が提供されています。

- すべての Unified CM ノードで実行
- 各トランクで最大 16 の宛先 IP アドレスをサポート

- SIP OPTIONS ping キープアライブ
- 音声コールとビデオ コールに対する早期オファーのサポートが必須（必要に応じて MTP を挿入）
- 音声コールとビデオ コールに対する早期オファーのサポートはベストエフォート（MTP の挿入なし）：ベスト エフォートのアーリー オファーとも呼ばれます
- オーディオ コーデック プリファレンス（および受信オファーのオーディオ コーデック プリファレンス受け入れ）
- 相互運用性の SIP トランクの正規化および透過性スクリプト
- SIP REFER 透過
- デスクトップ プレゼンテーション（Binary Floor Control Protocol（BFCP）および遠端カメラ制御（FECC）を備えた H.264 ビデオ

最新リリースの Unified CM で使用できる SIP トランク機能によって、SIP は新規のトランク接続にも既存のトランク接続にも適した選択肢になりました。QSIG over SIP 機能は H.323 クラスタ間トランクにおけるものと同等を提供します。また、Cisco IOS ゲートウェイ（および QSIG ベースの TDM PBX）に対する QSIG over SIP トランク接続を提供するためにも使用されます。すべての Unified CM ノードで実行され、最大 16 の宛先 IP アドレスを処理できる機能によって、Unified CM クラスタからの発信の分配が改善され、クラスタおよびデバイス間に必要な SIP トランク数が減ります。SIP OPTIONS ping には、コール別の到達可能性の判断ではなく、SIP トランクの宛先に関するダイナミックな到達可能性を検出する機能があります。[音声コールとビデオ コールに対する早期オファー サポートが必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）] および [ベスト エフォートのアーリー オファー（Best Effort Early Offer）] を使用すると、SIP トランクを経由する音声コール、ビデオ コールおよび暗号化されたコールに対するアーリー オファーを作成するために MTP を使用する必要がなくなります。[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] を使用すると、発信側デバイスのメディア特性（たとえば、ベスト エフォートのアーリー オファー トランクを介した SIP ベースの IP 電話からのコールなど）を判別できる場合、Unified CM は SIP アーリー オファーのみを送信します。発信側デバイスのメディア特性（たとえば、ベスト エフォートの SIP アーリー オファー トランクを介して転送された着信 SIP ディレイド オファー コールなど）を判別できない場合は、SIP ディレイド オファーが代わりに送信されます。

Lua スクリプトを使用した SIP トランクの正規化および透過性によって、サードパーティのユニファイド コミュニケーション システム間のネイティブ Unified CM の相互運用性が改善されます。正規化によって、着信および発信の SIP メッセージおよび SDP 情報を SIP トランクごとに変更できます。通過するメッセージの部分を Unified CM が理解またはサポートしていない場合でも、透過性によって、Unified CM は SIP ヘッダー、パラメータ、コンテンツ本文を SIP トランク コール レッグから別の宛先に渡すことができます。

これらの機能については、この項で詳しく後述します。

SIP トランクの新規拡張機能の全リストについては、次の Web サイトで入手可能な Cisco Unified Communications Manager の製品リリース ノートを参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html

Session Initiation Protocol（SIP）の操作

ここでは、Unified CM SIP トランクの設計および配置時に考慮する必要がある Unified CM SIP トランクの操作と、いくつかの主要な SIP トランク機能について説明します。

SIP オファー/アンサー モデル

Cisco Unified CM は、RFC 3264 で規定されているように、SIP セッションの確立に SIP オファー/アンサー モデルを使用します。この場合、オファーは、SIP メッセージのボディ部で送信されるセッション記述プロトコル（SDP）フィールドに含まれます。このオファーは、通常、デバイスでサポートされるメディア特性（メディア ストリーム、コーデック、方向メディア属性、IP アドレス、使用されるポート）を定義します。オファーを受信するデバイスは、対応する一致メディア ストリーム、コーデック、方向メディア属性、および IP アドレス/ポート番号（メディア ストリームの受信に使用）とともに、SIP 応答の SDP フィールドでアンサーを送信します。オファーおよびアンサーが入れ替わると、双方向メディアが発信側と着信側のエンドポイント間で確立されます。Unified CM は、このオファー/アンサー モデルを使用して、主要な SIP 標準、RFC 3261 で規定されているように、SIP セッションを確立します。

RFC 3261 は、SDP メッセージをオファーおよびアンサーで送信できる 2 つの方式を規定しています。これらの 2 つの方式は、一般的にディレイド オファーおよびアーリー オファーとして知られていて、ユーザ エージェント クライアント/サーバによる両方の方式のサポートが RFC 3261 規格で必要となります。簡単に言うと、メッセージ ボディで SDP を使用して送信される初期 SIP Invite は、アーリー オファーを定義し、メッセージ ボディで SDP を含まずに送信される初期 SIP Invite は、ディレイド オファーを定義します。

ディレイド オファーおよびアーリー オファーは、メディア機能の交換にすべての標準ベースの SIP スイッチで使用できる 2 つのオプションです。ほとんどのベンダーは、ディレイド オファーまたはアーリー オファーのいずれかを選択しています。また、それぞれに独自の利点や制限事項があります。

Unified CM SIP トランクは、SIP ディレイド オファーおよび SIP アーリー オファーの両方をサポートします。デフォルトでは、SIP トランクはディレイド オファーとして設定されており、音声、ビデオ、および暗号化されたコールをサポートします。アーリー オファー コールでは、次の 3 つのトランク設定オプションを使用できます。

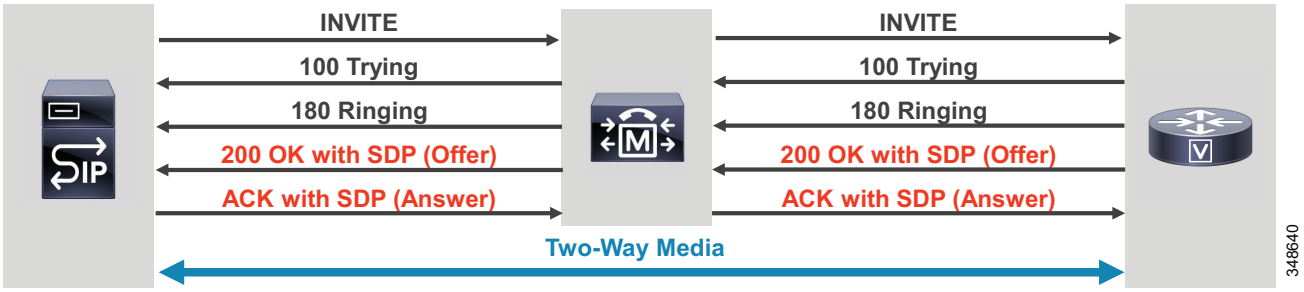
- SIP トランクでオンになっている [MTP が必須（MTP Required] オプション：MTP がすべてのコールに挿入されます。
- [音声コールとビデオ コールに対する早期オファー サポートが必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）]：SIP プロファイルのオプション。発信側デバイスのメディア特性（たとえば、アーリー オファー SIP トランクを介して転送される着信ディレイド オファー コールなど）を判別できない場合、Unified CM はメディア ターミネーション ポイント（MTP）を挿入します。
- [音声コールとビデオ コールに対する早期オファーのサポートはベスト エフォート（MTP の挿入なし）（Early Offer support for voice and video calls Best Effort (No MTP inserted)）]：SIP プロファイルのオプション。発信側デバイスのメディア特性を判別できる場合にのみ、アーリー オファーが送信されます。メディア特性を判別できない場合は、ディレイド オファーが送信されます。

ディレイド オファー、アーリー オファー、およびベスト エフォートのアーリー オファーに関する Unified CM アーリー オファー トランク設定については、Unified CM SIP トランク：ディレイド オファー、アーリー オファー、およびベスト エフォートのアーリー オファー（6-19 ページ）の項で説明します。

SIP ディレイド オファー

ディレイド オファーでは、セッションの開始側（発信側デバイス）は、その機能を初回の Invite で送信せず、着信側デバイスからその機能（たとえば、着信デバイスでサポートされるコーデックのリスト）が送られるまで待機します（これにより、発信デバイスは、セッションで使用されるコーデックを選択できます）。図 6-2 では、SIP ディレイド オファーの例を示します。

図 6-2　SIP ディレイド オファー

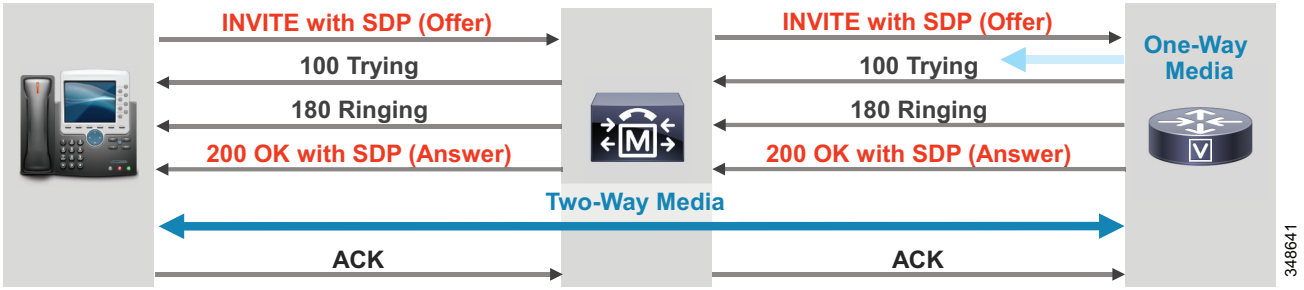


SIP アーリー オファー

アーリー オファーでは、セッションの開始側（発信側デバイス）は、その機能（たとえば、サポート対象のコーデック、IP アドレス、および RTP の UDP ポート番号）を初回の Invite に含まれる SDP ボディで送信します（これにより、セッションで使用されるコーデックを着信側デバイスで選択できるようになります）。アーリー オファーおよびディレイド オファーは、どちらも SIP 規格の必須となる部分ですが、アーリー オファーは、サードパーティのユニファイド コミュニケーション ベンダーが優先的に使用することが多く、IP PSTN サービス プロバイダーではほとんどの場合に使用されています。サービス プロバイダーは、初回の INVITE の SDP オファーが受信されると、発信側デバイスに一方向メディアが確立されるようになるアーリー オファー機能を使用します。この一方向メディア機能は、通話の課金が始まる前に、発信者に（たとえば、不明な番号）対するアナウンスを再生するために使用されます（通話の課金が開始されるのは通常、双方向メディアが確立され、トランザクションの最終確認応答（ACK）が受信された後です）。

（注）　SIP ベースの Cisco Unified IP Phone は、アーリー オファーを送信します。（図 6-3 を参照）。

図 6-3　SIP アーリー オファー



Provisional Reliable Acknowledgement（PRACK）

SIP は、最終応答と暫定応答の 2 つのタイプの応答を SIP 要求で定義します。

最終応答（たとえば、2XX、3XX、および 4XX 応答）は、処理された要求（INVITE など）の結果を伝達し、確実に送信されます（確認応答されたことを意味します）。

暫定応答（すべての 1XX 応答）は、要求の経過に関する情報を提供しますが、確実には送信されません。そのため、暫定応答の送信者は、受信されたことを認識しません。この理由から、信頼できない 1XX 応答で SDP 情報は送信されません。

Provisional Reliable Acknowledgements（PRACK）は、確実に 1XX 応答を送信できる SIP プロトコルの拡張機能です。PRACK は、PSTN との相互運用シナリオに 1XX 応答の信頼性を提供するため実用的です。また、双方向メディアを設定する前に交換する必要がある SIP メッセージ数を減らすために使用することもできます（図 6-4 および図 6-5 を参照）。

PRACK は、アーリー オファーまたはディレイド オファーを使用する SIP トランク上で使用できます。アーリー メディアとも呼ばれます。PRACK は Cisco Collaboration 製品の大半でサポートされており、一般に推奨される機能です。

図 6-4　アーリー メディア（PRACK）を使用した SIP アーリー オファー

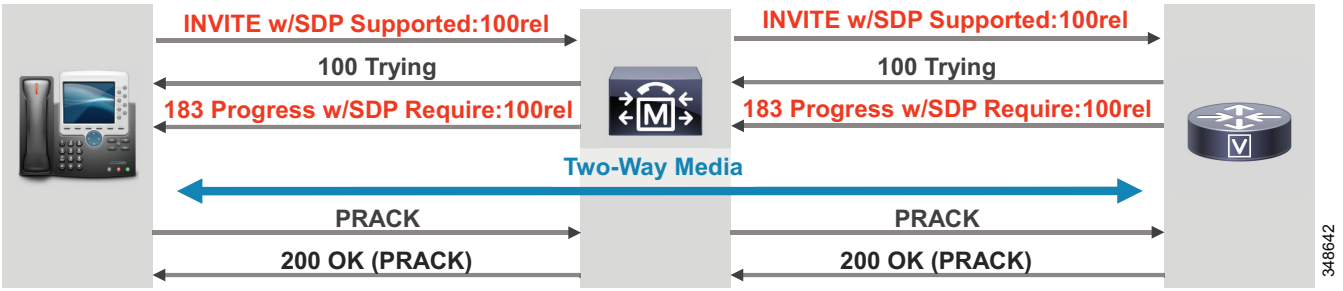
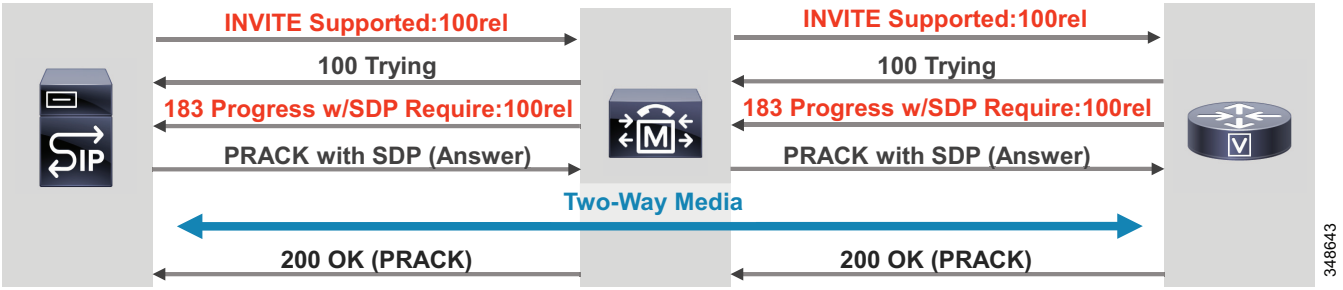


図 6-5　アーリー メディア（PRACK）を使用した SIP ディレイド オファー



（注）　100 Trying 応答は、Unified CM が INVITE を受信したことを示します。180 Ringing および 183 Session in Progress 応答は、ユーザが呼び出しを受けていることを示し、SIP ヘッダー メッセージ（PRACK が使用されている場合は、SIP メッセージ本文内の SDP コンテンツ）で着信側ユーザに関する情報を送信するのに使用されます。

Session Description Protocol（SDP）およびメディア ネゴシエーション

SDP は、SIP のコンパニオン プロトコルです。RFC 4566 に規定されているように、SDP はメディア特性について記載し、エンドポイント間のマルチメディア セッションのメディア タイプ、形式、および関連付けられたパラメータをネゴシエートするために使用されます。これらのメディア特性は、SDP メッセージで一連の 1 行フィールドに記載されます。

Session Description Protocol（SDP）および音声コール

表 6-2、表 6-3、および図 6-6 の例では、音声コールの SDP オファーとアンサーを示します。

表 6-2　　音声コール：SDP オファー

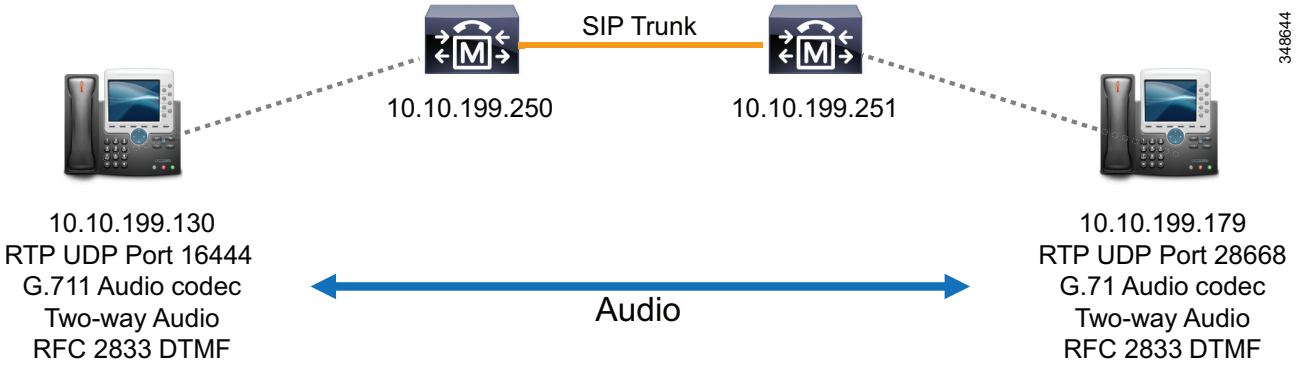
SDP メッセージのフィールド	説明
v=0	SDP バージョン（現在はバージョン 0）
o=CiscoCCM-SIP 2000 1 IN IP4 10.10.199.250	発信元（Unified CM IP アドレスを含む）
s=SIP Call	セッション名
c=IN IP4 10.10.199.130	接続データ（エンドポイントの IP アドレス）
t=0 0	タイミング（0 0 = 永続セッション）
m=audio 16444 RTP/AVP 0 8 18 101	メディア記述：UDP ポート、提供されたビデオ コーデックの RTP ペイロード タイプ（選好順序）、および DTMT
a=rtpmap:0 PCMU/8000	G.711 mu-law コーデック
a=ptime:20	パケット化（サンプリング）の時間間隔（ミリ秒）
a=rtpmap:8 PCMA/8000	G.711 a-law コーデック
a=ptime:20	パケット化（サンプリング）の時間間隔（ミリ秒）
a=rtpmap:18 G729/8000	G.729 コーデック
a=ptime:20	パケット化（サンプリング）の時間間隔（ミリ秒）
a=sendrecv	メディア方向
a=rtpmap:101 telephone-event/8000	RFC 2833 インバンド DTMF
a=fmtp:101 0-15	サポート対象の DTMF 文字

対応する SDP アンサーは、オファーを受信するエンドポイントのメディア特性および双方向音声メディアのエンドポイントによって選択される音声コーデックについて記載します（表 6-3 を参照）。

表 6-3　音声コール：SDP アンサー

SDP メッセージのフィールド	説明
v=0	SDP バージョン（現在はバージョン 0）
o=CiscoCCM-SIP 2000 1 IN IP4 10.10.199.251	発信元（Unified CM IP アドレスを含む）
s=SIP Call	セッション名
c=IN IP4 10.10.199.179	接続データ（エンドポイントの IP アドレス）
t=0 0	タイミング（0 0 = 永続セッション）
m=audio 28668 RTP/AVP 0 101	メディア記述：UDP ポート、選択したコーデックの RTP ペイロード タイプ、および DTMF
a=rtpmap: 0 PCMU/8000	G.711 mu-law コーデック
a=ptime:20	パケット化（サンプリング）の時間間隔（ミリ秒）
a=sendrecv	メディア方向
a=rtpmap:101 telephone-event/8000	RFC 2833 インバンド DTMF
a=fmtp:101 0-15	サポート対象の DTMF 文字

図 6-6　ネゴシエートされた音声コール



Session Description Protocol（SDP）およびビデオ コール

音声コールの場合、共通の音声コーデックの対称のメディア フローがエンドポイントによってネゴシエートされます。ビデオ メディア フローの場合、通常、送受信メディア機能が非対称であることが望まれます。非対称の要件は、アップロードとダウンロード速度が異なるブロードバンド サービスなどのいくつかの使用例に由来します（大きさ順が用いられることが多い）。さらに、ビデオの符号化は復号化より CPU を使用でき、ビデオ エンドポイントは、一般に符号化することが可能な解像度より高い解像度で復号化できます。このような要件から、SDP オファーおよびアンサーで送信されるビデオ コーデック機能は、それぞれのエンドポイントの受信機能と見なされ、一般に非対称である必要があります。

表 6-4 は、音声コールおよびビデオ コールの SDP オファーを示します。

表 6-4　音声コールおよびビデオ コール:SDP オファー

SDP メッセージのフィールド	説明
v=0	SDP バージョン（現在はバージョン 0）
o=CiscoCCM-SIP 161095 1 IN IP4 10.10.199.250	発信元（Unified CM IP アドレスを含む）
s=SIP Call	セッション名
t=0 0	タイミング（0 0 = 永続セッション）
m=audio 16444 RTP/AVP 0 8 18 101	音声メディア:選好順序のペイロード タイプによって表示されているポート番号とオーディオ コーデック、および DTMF ペイロード タイプ
c=IN IP4 10.10.199.130	接続データ（エンドポイントの IP アドレス）
….	複数のオーディオ コーデックおよび DTMF の属性
m=video 16446 RTP/AVP 98 99	メディア記述:UDP ポート、および提供されたビデオ コーデックの RTP ペイロード タイプ（選好順序）
c=IN IP4 10.10.199.130	エンドポイントの IP アドレス
a=rtpmap:98 H264/90000	H.264 ビデオ コーデック
a=fmtp:98 profile-level-id=428016;packetization-mode=1;max-mbps=245000;max-fs=9000;max-cpb=200;max-br=5000;max-rcmd-nalu-size=3456000;max-smbps=245000;max-fps=6000	H.264 コーデック メディア属性
a=rtpmap:99 H263-1998/90000	H.263 ビデオ コーデック
a=fmtp:99 QCIF=1;CIF=1;CIF4=1;CUSTOM=352,240,1	H.263 コーデック メディア属性
a=rtcp-fb:* nack pli	パケット損失表示の RTCP
a=rtcp-fb:* ccm tmmbr	ビデオ レート適合の RTCP

この SDP メッセージで提供される H.263 および H.264 コーデックには、エンドポイントの受信機能について記載する追加のパラメータの範囲が含まれます。SDP アンサーのネゴシエートされた H.264 コーデックに対して 表 6-5 に示されるように、これらのパラメータは対称的である必要はありません。

表 6-5　音声コールおよびビデオ コール:SDP アンサー

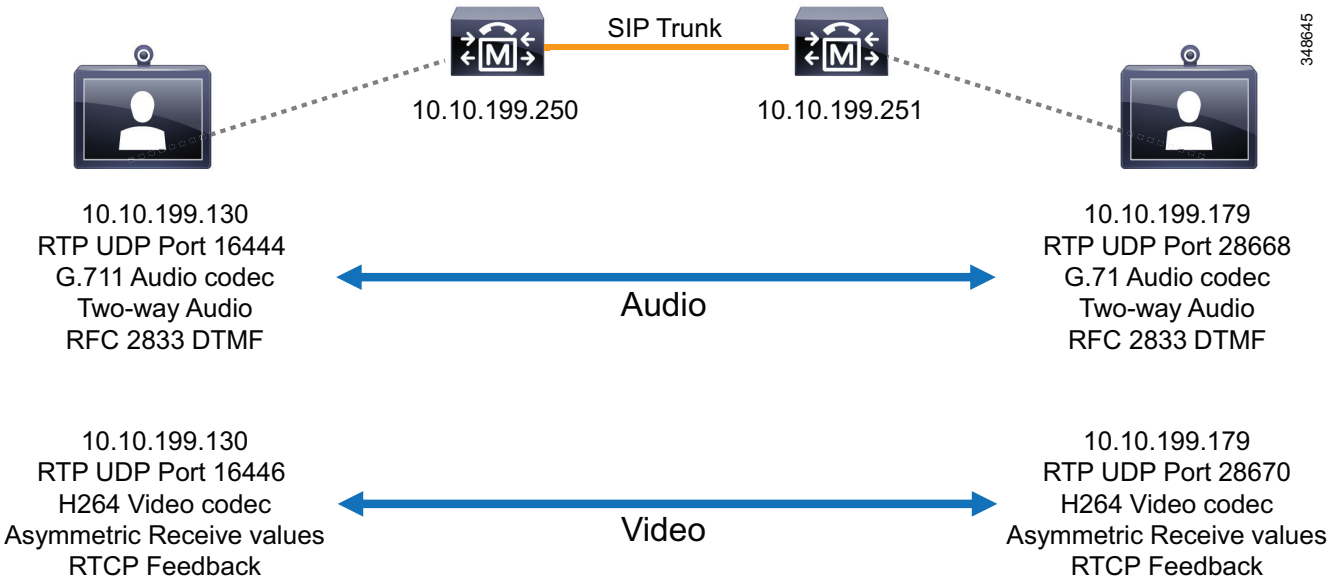
SDP メッセージのフィールド	説明
v=0	SDP バージョン（現在はバージョン 0）
o=CiscoCCM-SIP 112480 1 IN IP4 10.10.199.251	発信元（Unified CM IP アドレスを含む）
s=SIP Call	セッション名
t=0 0	タイミング（0 0 = 永続セッション）
m=audio 28668 RTP/AVP 0 101	音声メディア:ポート番号、選択したオーディオ コーデック、および DTMF ペイロード タイプ

表 6-5　音声コールおよびビデオ コール：SDP アンサー（続き）

SDP メッセージのフィールド	説明
c=IN IP4 10.10.199.179	接続データ（エンドポイントの IP アドレス）
….	選択した G.711 オーディオ コーデックおよび DTMF の属性
m=video 28670 RTP/AVP 98	ビデオに選択した H.264 コーデック
c=IN IP4 10.10.199.179	エンドポイントの IP アドレス
a=rtpmap:98 H264/90000	H.264 コーデックの詳細
a=fmtp:98 profile-level-id=428016;packetization-mode=1;max-mbps=108000;max-fs=3600;max-cpb=200;max-br=5000;max-rcmd-nalu-size=1382400;max-smbps=108000;max-fps=6000	選択した H.264 コーデックのメディア属性。 プロファイル レベル ID とパケット化モードは、ネゴシエートされたコールで対称的である必要があります。その他の属性では、対称的である必要はなく、エンドポイントの受信機能を表します。
a=rtcp-fb:* nack pli	パケット損失表示の RTCP
a=rtcp-fb:* ccm tmmbr	ビデオ レート適合の RTCP

プロファイル レベル ID およびパケット化モードは、ネゴシエートされたビデオ コールで対称的である必要があります。プロファイル レベル ID は、エンドポイントでサポートされる H.264 機能、解像度、フレーム レート、およびビット レットの最小サブセットについて記載します。パケット化モードは、ビデオ サンプルをどのようにカプセル化し、RTP パケットで送信できるかについて記載します。プロファイル レベル ID とパケット化モードの後のメディア属性は、対称的である必要はなく、表 6-5 および 図 6-7 に示されるように、実際にネゴシエートされたビデオ コールですべてが対称的でありません。

図 6-7　ネゴシエートされた音声コールおよびビデオ コール



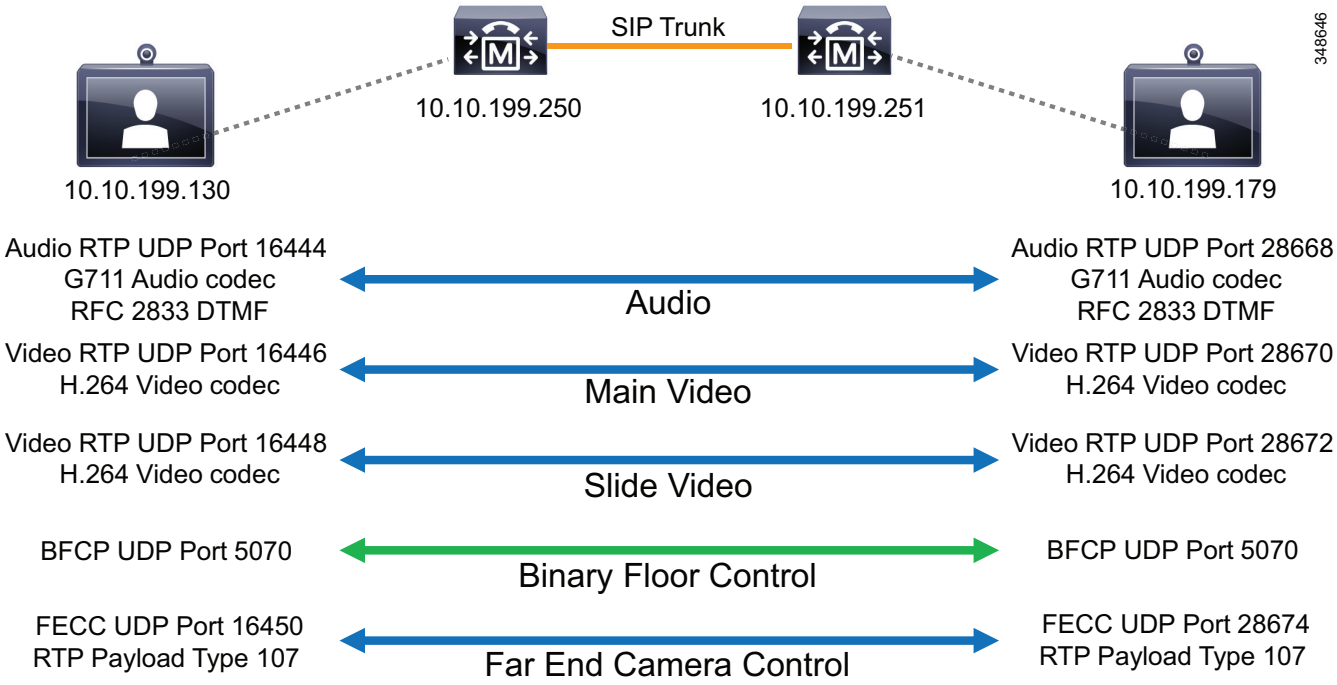
ビデオ デスクトップ共有および Binary Floor Control Protocol（BFCP）

ビデオ デスクトップおよびプレゼンテーション共有では、エンドポイントは追加の RTP ビデオ チャネルをネゴシエートして、共有されるコンテンツ（たとえば、プレゼンテーションのスライド）と、ビデオまたは会議コール内のリソースへの共有アクセスを管理する BFCP の UDP チャネルを送信します。（図 6-8 を参照）。BFCP は、RFC 4582 および RFC 4583 に記載されています。

遠端カメラ制御（FECC）

遠端カメラ制御を使用すると、ユーザはビデオ ソースを選択して、パン、チルト、ズームおよびフォーカスなどのカメラのアクションを制御できます。FECC を使用したエンドポイントは、カメラ制御に対して追加の RTP チャネルをネゴシエートします。（図 6-8 を参照）。FECC は、H.281、H.224、および RFC 4573 に記載されています。

図 6-8　　プレゼンテーション共有および遠端カメラ制御を使用した音声コールおよびビデオ コール



Unified CM の SIP トランクの機能と操作

ここでは、Unified CM SIP トランクの設計および配置時に考慮する必要がある Unified CM SIP トランクの操作と、いくつかの主要な SIP トランク機能について説明します。

すべての Unified CM ノードで実行

Cisco Unified CM は、クラスタ内のコール処理サブスクライバ ノードで SIP トランク コールが発信または受信されるようにする設定オプションを提供しています。

SIP トランク：すべてのノードおよびルート ローカル ルールで実行

SIP トランクで [すべてのアクティブな Unified CM ノードで実行（Run on all Active Unified CM Nodes）] オプションをオンにすると、Unified CM は、クラスタ内のコール処理サブスクライバごとに SIP トランク デーモンのインスタンスを作成します。そのため、どのコール処理サブスクライバでも SIP トランク コールを発信または着信できます。（この機能の前は、Unified CM グループを使用して最大 3 つのノードがトランクごとに選択可能でした）。[すべてのアクティブな Unified CM ノードで実行（Run on all Active Unified CM Nodes）] をオンにすると、発信 SIP トランク コールは、（たとえば電話またはトランクから）着信コールを受信したのと同じノードから発信します（ルート ローカル ルールに基づいて）。[すべてのアクティブな Unified CM ノードで実行（Run on all Active Unified CM Nodes）] 機能は、トランクの Unified CM グループ設定を無効にします。

SIP トランクでは、ルート ローカル ルールは次のように動作します。

> 発信 SIP トランク コールでは、登録されている電話または着信トランクからのコールが Unified CM ノードに到達すると、着信コールが着信した同じノードに選択した発信トランクのインスタンスが存在するかどうかが Unified CM によって確認されます。存在する場合、Unified CM はそのノードを使用して発信トランク コールを確立します。

SIP トランクで [すべてのアクティブな Unified CM ノードで実行（Run on all Active Unified CM Nodes）] をオンにすることが推奨されます。この機能を使用すると、発信コールがクラスタ内のコール処理ノードで発信されたり、受信されたりできるからです。[すべてのアクティブな Unified CM ノードで実行（Run on all Active Unified CM Nodes）] は、発信 SIP トランク上で確立される前に、コールが同じクラスタ内のコール処理ノード間でセットアップされないようにすることもできます。

すべての Unified CM SIP トランクと同様に、トランクに関連付けられている SIP デーモンは、トランクの宛先アドレス フィールドに定義された IP アドレスを持つエンド システムからの着信コールのみを受け入れます。同じ宛先への複数の SIP トランクが同じコール処理ノードを使用している場合、各トランクが一意に識別されるように、トランクごとに一意の着信および発信のポート番号を定義する必要があります。

ルール リスト：すべてのノードおよびルート ローカル ルールで実行

これは具体的には SIP トランク機能ではありませんが、すべてのノードでルート リストを実行すると、ルート リストおよびルート グループ内のトランクに利点があります。すべてのノードでルート リストを実行すると、ルート ローカル ルールを使用した発信の分配が改善され、不要なクラスタ内コール セットアップ トラフィックを回避できます。

ルート リストの場合、ルート ローカル ルールは次のように動作します。

> ルート リスト（および関連するルート グループとトランク）を使用する発信の場合、登録されている電話からのコールまたは着信トランクが、ルート リスト インスタンスがあるノードに到達したときに、選択した発信トランクのインスタンスがルート リストと同じノードに存在するかどうかが Unified CM によって確認されます。存在する場合、Unified CM はそのノードを使用して発信トランク コールを確立します。

ルート リストとトランクの両方で [すべてのアクティブな Unified CM ノードで実行（Run on all Active Unified CM Nodes）] が有効の場合、発信のコール分配は、着信コールが到達したノードによって決定されます。すべてのノードでの実行ではなく、選択した発信トランクが Unified CM グループを使用する場合、選択した発信トランクのインスタンスが、着信コールが到達した同じノードに存在する場合に、Unified CM はルート ローカル ルールを適用します。トランクのインスタンスがそのノードに存在しない場合、Unified CM は（クラスタ内の）コールを、トランクがアクティブなノードに転送します。

ルート リストで [すべてのアクティブな Unified CM ノードで実行（Run on all Active Unified CM Nodes）] をオンにしていない場合、ルート リストのインスタンスはクラスタ内の 1 つのノード（ルート リストの Unified CM グループのプライマリ ノード）でアクティブになります。選択した発信トランクが、ルート リストの Unified CM グループのプライマリ ノードでもアクティブな場合、ルート ローカル ルールが適用され、結果として発信コールの分配が最適ではなくなります。これは、すべての発信トランク コールがこのノードから発信されるためです。

すべてのルート リストおよび SIP トランクで、[すべてのアクティブな Unified CM ノードで実行（Run on all Active Unified CM Nodes）] をオンにすることを強く推奨します。

最大 16 の SIP トランク宛先 IP アドレス

SIP トランクは、最大 16 の宛先 IP アドレス、16 の完全修飾ドメイン名、または単一の DNS SRV エントリを使用して設定できます。追加の宛先 IP アドレスをサポートしているため、2 つの Unified Communications システム間のコール分配のために、ルート リストおよびルート グループに関連付けられた複数のトランクを作成する必要性が軽減されます。結果として、Unified CM トランク設計が単純になりますこの機能は、[すべてのアクティブな Unified CM ノードで実行（Run on all Active Unified CM Nodes）] 機能と併用できます。（図 6-9 および図 6-10 を参照）。ただし、Unified CM SIP トランクと関連付けられた SIP デーモンは、トランクの宛先アドレス フィールドに定義された IP アドレスを持つエンド システムからの着信のみを受け入れる点に注意してください。1 つ以上の宛先アドレスで 1 つの SIP トランクを使用して、Unified CM クラスタをもう 1 つのユニファイド コミュニケーション システムに接続します。トランクのフェールオーバーが必要な場合は、フェールオーバーのユニファイド コミュニケーション システムに追加のトランクを作成し、ルート リストとルート グループを使用して、トランクの選択を順序付けします。Unified CM は、設定された SIP トランク宛先アドレスで発信コールをランダムに分配します。

図 6-9　[すべての Unified CM ノードで実行（Run on All Unified CM Nodes）] および複数の宛先アドレスを使用した SIP トランク

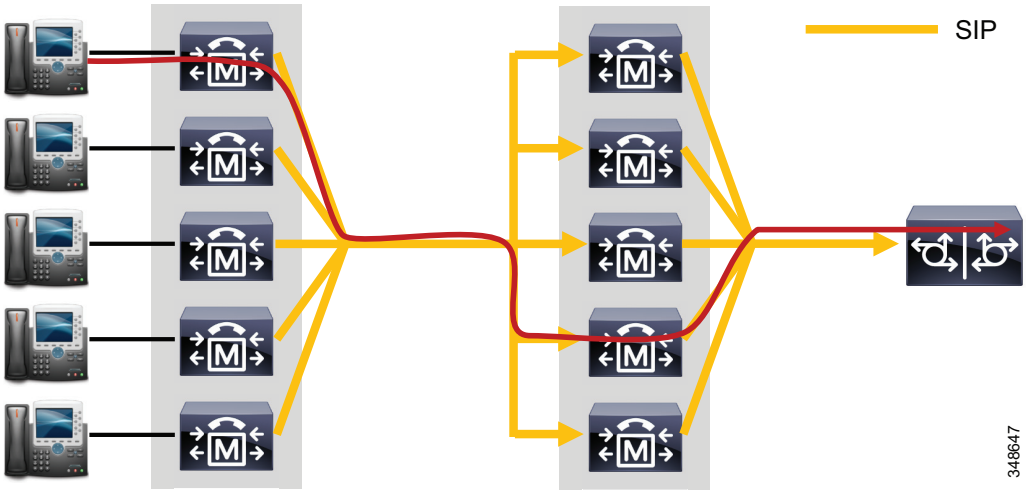
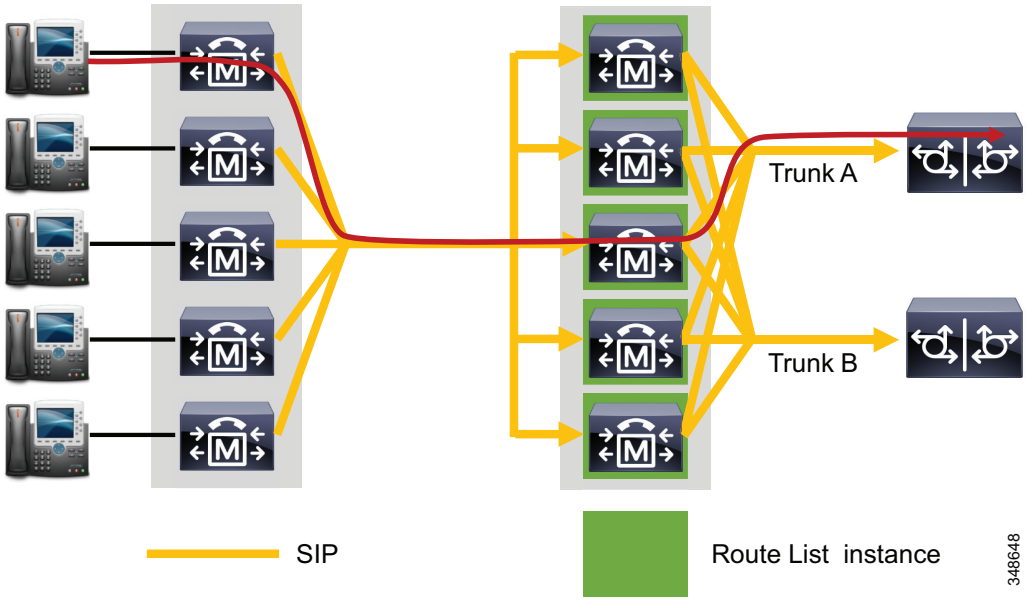


図 6-10　[すべての Unified CM ノードで実行(Run on All Unified CM Nodes)] をオンにした SIP トランクおよびルート リスト



DNS を使用する SIP トランク

次のような特定の状況では、複数の宛先 IP アドレスを定義するよりも、SIP トランクの宛先として DNS SRV エントリを使用する方が推奨されます。

- SRV ホストの優先順位付けが必要な場合
- SRV ホストの重み付けが必要な場合
- 必要な宛先 IP アドレス数が 16 を超える場合
- DNS SRV の解決が、宛先 Unified Communications システムの要件の場合

(注)　設定オプション [接続先アドレスは SRV(Destination Address is an SRV)] が選択されている場合、トランクの宛先として単一の SRV エントリのみを追加できます。(たとえば、Destination Address = cluster1.cisco.com、Port = 0 です)。

図 6-11 に、DNS SRV を使用して、アドレスを宛先 Unified CM クラスタに解決する SIP トランクのコール フローを示します。ただし、この宛先は、サードパーティのユニファイド コミュニケーション システムの場合もあります。

図 6-11　DNS SRV を使用したクラスタ間 SIP トランクのコール フロー

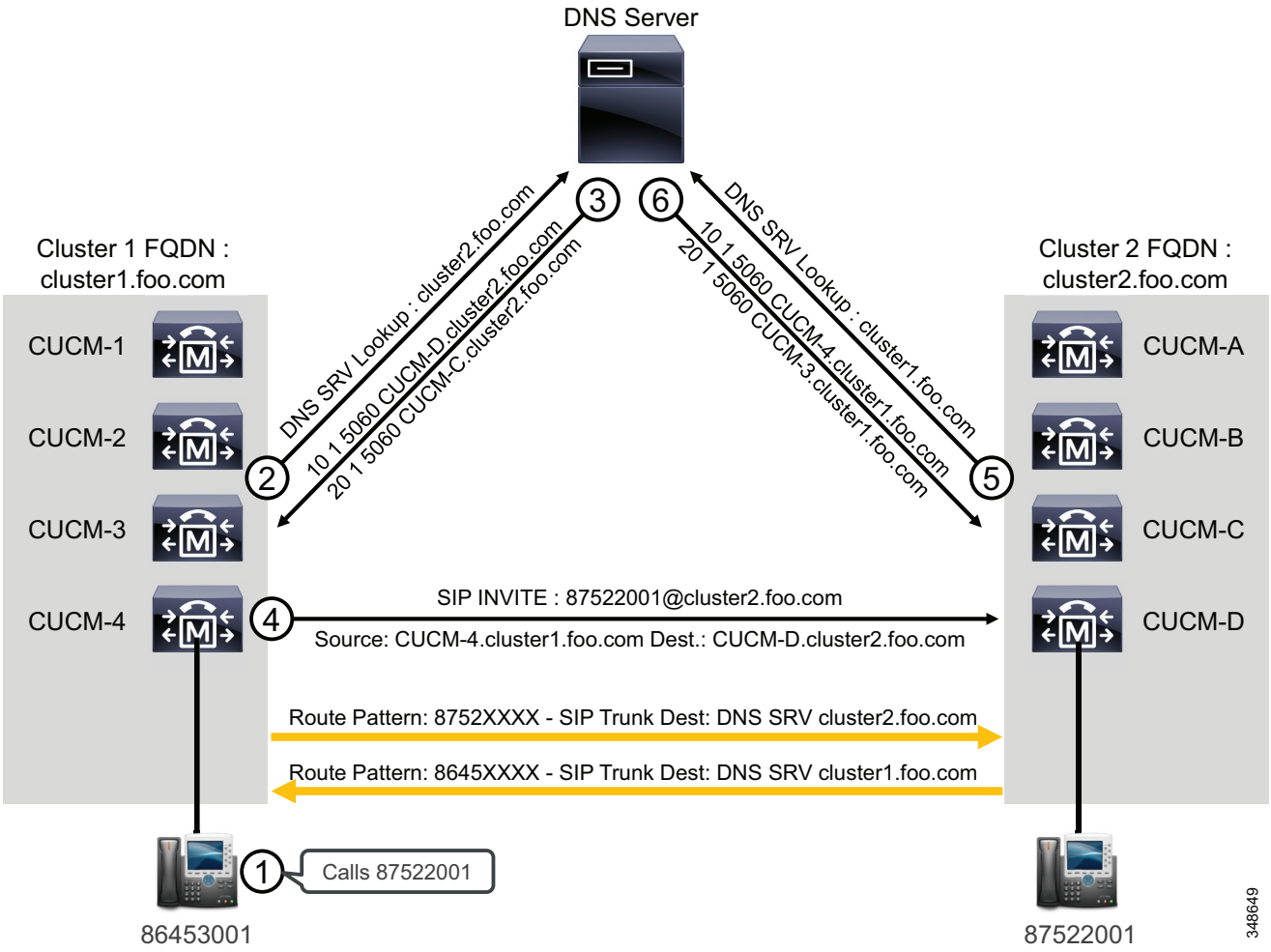


図 6-11 は、このコール フローにおける次の手順を示しています。

1. クラスタ 1 内の IP Phone が 87522001 にコールします。
2. コールはルート パターン 8752XXXX と一致し、このパターンは cluster2.foo.com の DNS SRV を使用した SIP トランクを指しています。電話機と SIP トランクの両方が登録されているため、クラスタ 1 の CUCM-4 はこのコールに対処するノードです。CUCM-4 は、cluster2.foo.com の DNS SRV ルックアップを送信します。
3. DNS サーバは、CUCM-D.cluster2.foo.com と CUCM-C.cluster2.foo.com の 2 つのレコードで応答します。CUCM-D.cluster2.foo.com のプライオリティの方が高いため、コールはその Unified CM に対して試みられます。SIP INVITE が送信される前に、CUCM-D.cluster2.foo.com に関して別の DNS ルックアップが行われます。
4. CUCM-4 は、SIP INVITE を 87522001@cluster2.foo.com に送信します。宛先アドレスは CUCM-D の IP アドレスに設定されます。

5. Unified CM は、このコールをローカル コールとして解釈します。ユニフォーム リソース識別子（URI）のホスト部分が Cluster FQDN エンタープライズ パラメータと一致しているためです。クラスタ 2 には、CUCM-4 の宛先が設定された SIP トランクがありません。したがって、DNS SRV を使用する SIP トランクに設定されたすべてのドメインに対して、DNS SRV ルックアップを行います。その場合、例では cluster1.foo.com の DNS SRV の宛先を持つ単一のトランクが示されています。
6. DNS サーバは 2 つのエントリを返し、そのうちの 1 つが INVITE の送信元 IP アドレスと一致します。クラスタはコールを受け入れ、内線 87522001 にコールをルーティングします。

（注）　DNS A ルックアップは、このコール フローでは表示されません。

SIP OPTIONS ping

SIP トランクに関連付けられた SIP プロファイルで SIP OPTIONS ping 機能を有効にして、トランクの宛先の状態をダイナミックに追跡できます。この機能を有効にすると、トランクの SIP デーモンを実行する各ノードは、トランクの各宛先 IP アドレスに対して OPTIONS 要求を定期的に送信して到達可能性を判断し、到達可能なノードにのみコールを送信します。宛先アドレスが OPTIONS 要求に応答しない場合、Service Unavailable（503）応答または Request Timeout（408）応答を送信する場合、または TCP 接続を確立できない場合、そのアドレスは「アウト オブ サービス」と見なされます。1 つ以上のノードが、1 つ以上の宛先アドレスから（408 または 503 以外の）応答を受信した場合、トランク全体の状態は「イン サービス」と見なされます。SIP トランク ノードは、トランクの設定済み宛先 IP アドレス、またはトランクの DNS SRV エントリの解決済み IP アドレスに対して OPTIONS 要求を送信できます。すべての SIP トランクで SIP OPTIONS Ping を有効にすることを推奨します。有効にすることで、Unified CM は、ノードごと、コールごと、およびタイムアウトごとにトランク宛先の状態を判別するのではなく、ダイナミックにトランクの状態を追跡できるためです。

Unified CM SIP トランク：ディレイド オファー、アーリー オファー、およびベスト エフォートのアーリー オファー

ここでは、Unified CM SIP トランクでのディレイド オファー、アーリー オファー、およびベスト エフォートのアーリー オファーの使用に関するガイドラインを示します。

Unified CM SIP ディレイド オファー

Unified CM SIP トランクのデフォルト設定では、ディレイド オファー（SDP コンテンツなしで送信される SIP INVITE）を使用します。このデフォルト設定を使用して、SIP トランクを経由するすべての発信コールは SIP ディレイド オファーを送信します。メディア ターミネーション ポイント（MTP）は、送信 INVITE で使用されません。つまり、受信オファーに応答して送信されるアンサー内の SDP コンテンツを生成するのに使用されません。ただし、DTMF 転送の不一致に対応するために MTP を使用できます。SIP トランクを介して送信されるすべてのコールがディレイド オファーを送信するようにするには、このデフォルト設定を使用します。音声コール、ビデオ コール、および暗号化されたコールがサポートされます。

Unified CM SIP アーリー オファー

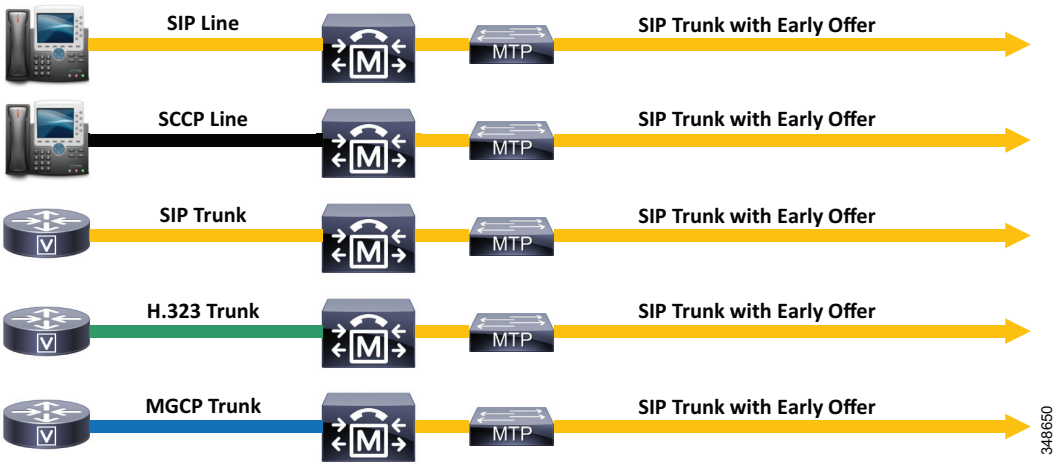
Unified CM SIP トランクを経由するすべての発信コールにアーリー オファーを有効にするには、2 つの設定可能なオプションがあります。

- メディア ターミネーション ポイントが必須（Media Termination Point Required）
- 音声コールとビデオ コールに対する早期オファーのサポートが必須（必要に応じて MTP を挿入）

[メディア ターミネーション ポイントが必須（Media Termination Point Required）] を使用したアーリー オファー

SIP トランクで [メディア ターミネーション ポイントが必須（Media Termination Point Required）] オプションをオンにすると、トランクのメディア リソース グループ（MRG）からの MTP が各着信コールおよび発信コールに割り当てられます。（図 6-12 を参照）。この処理でスタティックに割り当てられた MTP は G.711 または G.729 コーデックのみをサポートするため、選択したコーデック タイプを使用して、メディアは音声コールにのみ限定されます。[メディア ターミネーション ポイントが必須（Media Termination Point Required）] を使用したアーリー オファーの有効化は、[音声コールとビデオ コールに対する早期オファー サポートが必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）] および [音声コールとビデオ コールに対する早期オファーのサポートはベスト エフォート（MTP の挿入なし）（Early Offer support for voice and video calls Best Effort (No MTP inserted)）] に変更されています。[メディア ターミネーション ポイントが必須（Media Termination Point Required）] を使用したアーリー オファーは、着信コールと発信コールの音声メディアが MTP の 1 つの IP アドレスにアンカーされる必要がある場合に有効です。

図 6-12　[メディア ターミネーション ポイントが必須（Media Termination Point Required）] を使用した SIP アーリー オファー



[音声コールとビデオ コールに対する早期オファー サポートが必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）] を使用したアーリー オファー

SIP トランクに関連付けられた SIP プロファイルで [音声コールとビデオ コールに対する早期オファー サポートが必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）] を有効にして MTP が挿入されるのは、発信デバイスがアーリー オファーの作成に必要なメディア特性を Unified CM に提示できない場合のみです。一般的に、[メディア ターミネーション ポイントが必須（Media Termination Point Required）] よりも [音声コールとビデオ コールに対する早期オファー サポートが必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）] が推奨されるのは、この設定オプションによって MTP の使用量が減り、音声コール、ビデオ コール、および暗号化されたコールをサポートできるためです。（図 6-13 を参照）。

[音声コールとビデオ コールに対する早期オファー サポートが必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）] に設定されている SIP トランクを介した発信コールの場合、Unified CM は、次の場合にのみ MTP を挿入して、SDP オファーを作成します。

- Unified CM への着信コールがディレイド オファー SIP トランクを介して受信される場合
- Unified CM への着信コールが H.323 Slow Start トランクを介して受信される場合
- 着信コールが Unified CM に登録されている古い SCCP ベースの IP Phone から受信される場合

一般に、MTP を使用するこのタイプのアーリー オファー コールは音声のみをサポートしますが、単一の音声コーデックに制限されていません（必要に応じて MTP を使用したアーリー オファーである場合）。これらのコールは、最初のコール セットアップでのみ音声をサポートしますが、コール メディアが再ネゴシエートされる場合（保留/再開後など）、ビデオおよび SRTP をサポートするためにコール中にエスカレーションできます。

（注）　着信 INVITE メッセージに初回のオファー SDP が含まれているかどうかにかかわらず、着信 INVITE メッセージに MTP リソースは必須ではありません。

図 6-13　音声コールとビデオ コールに対する早期オファー サポート：必須（必要な場合は MTP を挿入）

Unified CM に対する着信を次のいずれかの手段で受信した場合、SIP トランク上で発信アーリー オファー コールを作成するために、Unified CM が MTP を挿入する必要はありません。

- アーリー オファーを使用する SIP トランク上
- Fast Start を使用する H.323 トランク上
- MGCP トランク上
- Unified CM に登録されている SIP ベースの IP フォンから
- Unified CM に登録されている、SCCP ベースの新しい Cisco Unified IP Phone モデルから

上記のデバイスの場合、Unified CM はエンドポイントのメディア機能を使用して、発信デバイスと発信 SIP トランクのリージョンペアに基づいてコーデック フィルタリング ルールを適用し、発信 SIP トランク コールのオファー SDP を作成します。ほとんどの場合、オファー SDP には、コールを発信したエンドポイントの IP アドレスとポート番号が含まれます。そのため、発信デバイスと SIP トランクの間に共通のコーデックがない場合でも、DTMF の不一致、TRP の要件、またはトランスコーダの要件など、他の理由で Unified CM が MTP を挿入する必要はありません。

トランクの SIP プロファイルで [音声コールとビデオ コールに対する早期オファー サポートが必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）] を設定している場合、古い SCCP ベースの電話、SIP ディレイド オファー トランク、および H.323 Slow Start トランクからのコールに対して Unified CM では MTP を割り当てます。MTP は、有効なメディア ポートおよび IP アドレスを含むオファー SDP を生成するために使用されます。MTP は、発信 SIP トランクのメディア リソースではなく、発信デバイスに関連付けられたメディア リソースから割り当てられます。（この処理で、メディア パスが発信 SIP トランクの MTP にヘアピンされるのを回避します）。発信デバイスのメディア リソース グループ リスト（MRGL）から MTP を割り当てることができない場合、MTP の割り当ては SIP トランクの MRGL から試行されます。

Unified CM に登録されているより古い SCCP 電話からのコールの場合、発信デバイスの一部のメディア機能（サポート対象の音声コーデック、ビデオ コーデック、暗号化キーなど、サポートされる場合）は、セッション記述プロトコル（SDP）を介したメディア交換に使用できます。Unified CM は、エンドポイントおよび MTP コーデック機能のスーパーセットを作成し、適用可能なリージョンペア設定に基づいてコーデックのフィルタリングを適用します。発信オファー SDP は、MTP の IP アドレスとポート番号を使用します。また、音声メディア、ビデオ メディア、および暗号化されたメディアをサポートできます。パススルー コーデックをサポートするには、Cisco IOS ベースの MTP を使用して、設定する必要があります。

（注）　Cisco Unified IP Phone 7902、7905、7910、7912、7920、7935、7940、7960 など古い SCCP ベースの IP Phone では、[音声とビデオに対する早期オファーが必須（必要に応じて MTP を挿入）（Early Offer for voice and video Mandatory (insert MTP if needed)）] 機能を有効にして SIP トランクを介したコールを発信するときに、MTP を使用する必要があります。クラスタにこれらの電話機タイプが多数配置されている場合は、[音声とビデオに対する早期オファーが必須（必要に応じて MTP を挿入）（Early Offer for voice and video Mandatory (insert MTP if needed)）] ではなく、ディレイド オファー トランクを配置することを検討してください。[音声とビデオに対する早期オファーが必須（必要に応じて MTP を挿入）（Early Offer for voice and video Mandatory (insert MTP if needed)）] トランクを使用する場合は、このアーリー オファー機能を使用する SIP トランクを介した最繁時のコール数と同等の MTP リソースをクラスタ内にプロビジョニングします。

Unified CM が H.323 Slow Start または SIP ディレイド オファー トランクで着信を受信した場合、コールの開始時に発信デバイスのメディア機能を使用できません。この場合、Unified CM が MTP を挿入する必要があります。また、IP アドレスと UDP ポート番号を使用して、（リージョンペアのフィルタリング後に）発信 SIP トランクで送信された最初の INVITE のオファー SDP で、サポート対象のすべての音声コーデックをアドバタイズします。アンサー SDP を SIP トランクで受信し、発信エンドポイントでサポートされるコーデックが含まれる場合、追加のオファー/アンサー トランザクションは不要です。コーデックが一致しない場合、Unified CM は、トランスコーダを挿入してその不一致に対処するか、Re-INVITE または UPDATE を送信してメディア ネゴシエーションをトリガーできます。H.323 Slow Start または SIP ディレイド オファー トランクからのコールは、最初のコール セットアップでのみ音声をサポートしますが、コール メディアが再ネゴシエートされる場合（保留または再開後など）、ビデオおよび SRTP をサポートするためにコール中にエスカレーションできます。

ベスト エフォートのアーリー オファー [音声コールとビデオ コールに対する早期オファーのサポートはベスト エフォート（MTP の挿入なし）（Early Offer support for voice and video calls Best Effort (No MTP inserted)）]

[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] は、SIP トランクに関連付けられた SIP プロファイルで有効にでき、すべての Unified CM および Unified CM Session Management Edition（SME）トランクに対して推奨される設定です。[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] のトランクでは、アーリー オファーを作成するために MTP を使用しません。発信側デバイスに応じて、アーリー オファーかディレイド オファーのいずれかを使用して発信 SIP トランク コールを開始できます。[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] の SIP トランクは、音声コール、ビデオ コール、および暗号化されたコールをサポートしています。

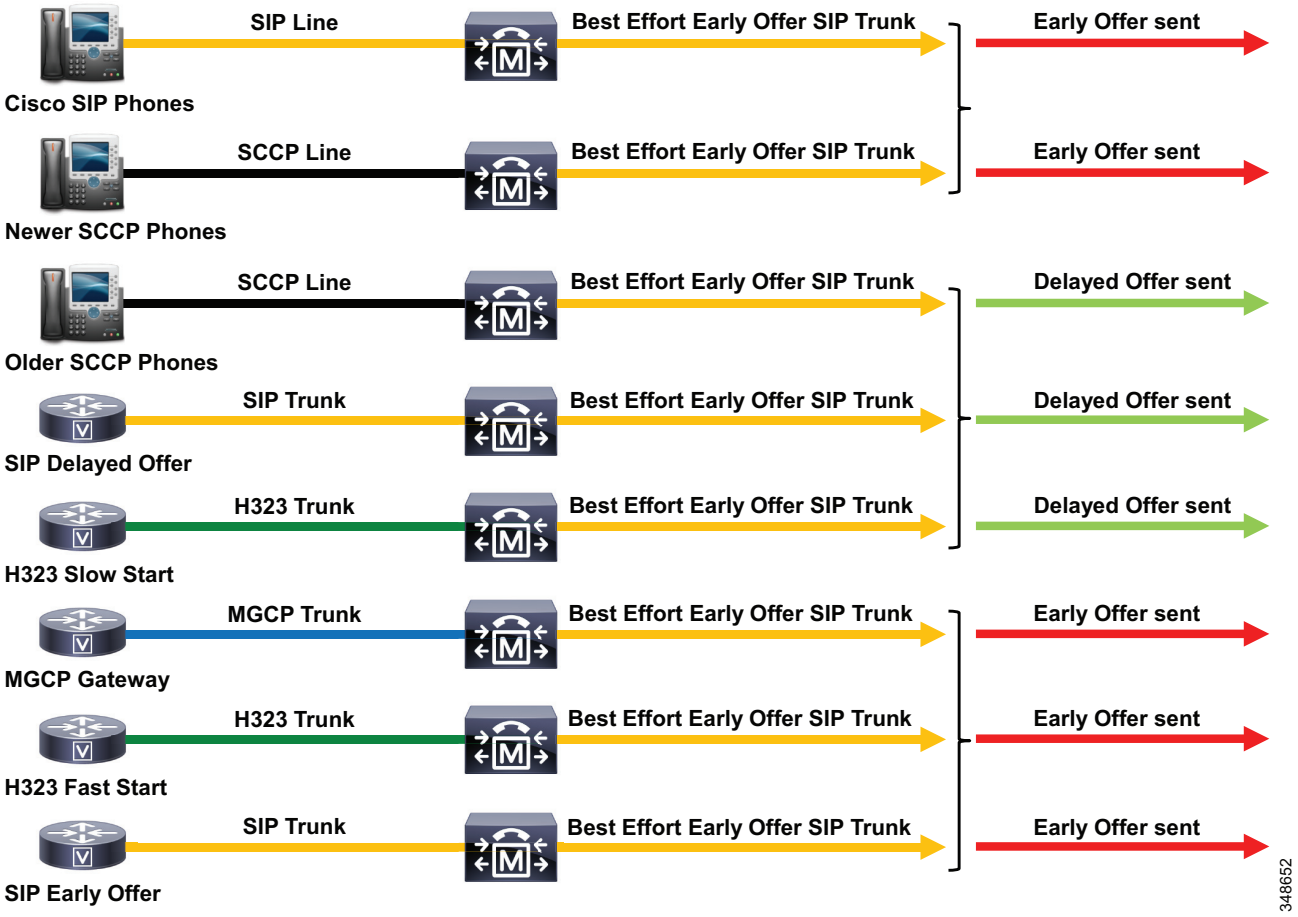
[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] の SIP トランクは、次の状況において、アーリー オファー（SDP コンテンツを含む INVITE）を使用して発信コールを送信します。

- Unified CM または SME への着信コールがアーリー オファーを使用した SIP トランクを介して受信される場合。
- Unified CM または SME への着信コールが Fast Start を使用した H.323 トランクを介して受信される場合。
- Unified CM または SME への着信コールが MGCP トランクを介して受信される場合。
- コールが Unified CM に登録されている SIP ベースの IP 電話から開始される場合。
- コールが Unified CM に登録されている新しいモデルの SCCP ベースの Cisco Unified IP Phone から開始される場合。

[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] のトランクは、次の状況において、ディレイド オファー（SDP コンテンツを含まない INVITE）を使用して発信コールを送信します。

- Unified CM または SME への着信コールがディレイド オファー SIP トランクを介して受信される場合。
- Unified CM または SME への着信コールが H.323 Slow Start トランクを介して受信される場合。
- コールが Unified CM に登録されている古いモデルの SCCP ベースの IP 電話から開始される場合。

図 6-14　　ベスト エフォートのアーリー オファー



DTMF 変換用の MTP などのメディア リソース、Trusted Relay Point（TRP; トラステッド リレー ポイント）、およびコーデックの不一致用のトランスコーダは、引き続き [ベスト エフォートのアーリー オファー（Best Effort Early Offer）] のトランクに関連付けてそのトランクで使用できます。[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] を使用すると、アーリー オファーの作成または、受信したオファーに応答したアンサーの作成に MTP が使用されなくなることに注意してください。

企業内のすべての SIP トランクで [ベスト エフォートのアーリー オファー（Best Effort Early Offer）] を使用することで、Cisco Collaboration システムのネットワーク設計と展開が簡略化され、オファーの作成に MTP を使用する必要がなくなります。ただし、Cisco Collaboration のコール制御システム、アプリケーション、およびゲートウェイは、[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] のトランクを介してアーリー オファー コールまたはディレイド オファー コールを受信することができ、また、そのどちらかを受信できる必要があることに注意してください。すべての Cisco Collaboration システム アプリケーションは、アーリー オファー コールまたはディレイド オファー コールの受信をサポートしています。

特定のケース（たとえば、Cisco Unified Border Element Session Border Controller（SBC）を介したサービス プロバイダーの IP PSTN へのコールなど）では、アーリー オファーが常に IP PSTN に送信される必要があります。このような状況では、Cisco Unified Border Element のディレイド オファーからアーリー オファーへの変換機能を使用して、受信したディレイド オファーをアーリー オファーに変換します。

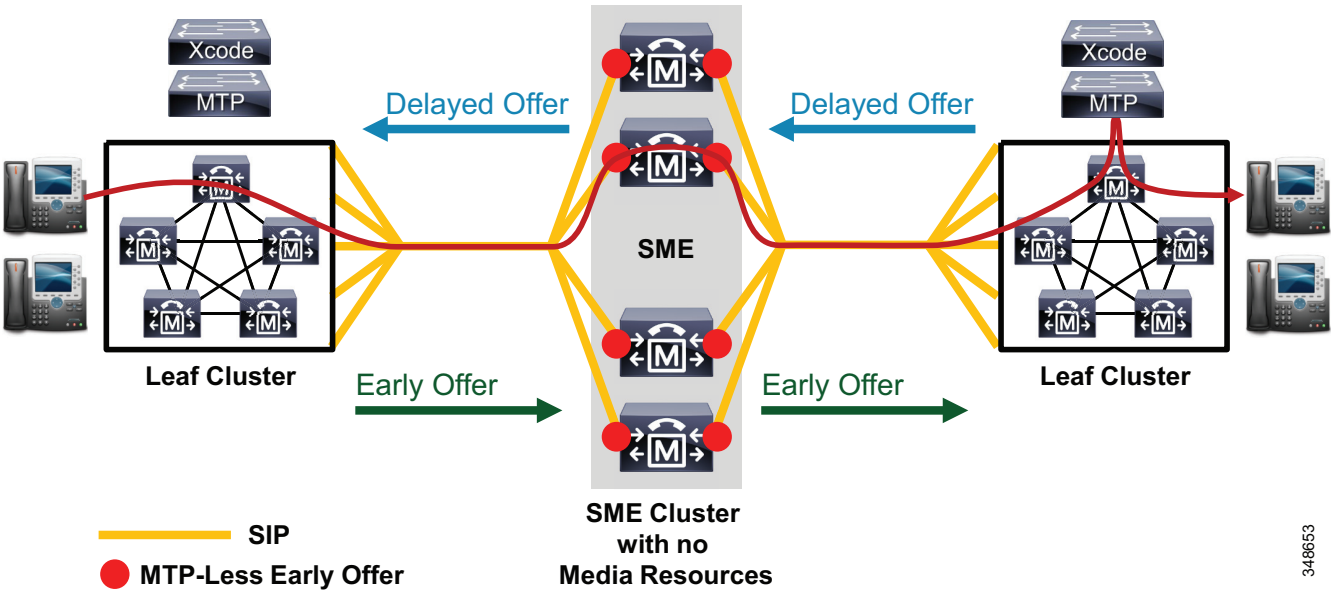
Cisco Collaboration システム アプリケーションがアーリー オファーまたはディレイド オファーのみを受信する必要がある場合は、それぞれアーリー オファー（[音声コールとビデオ コールに対する早期オファー サポートが必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）] または [MTP が必須（MTP Required）] を使用）またはディレイド オファーに設定された Unified CM SIP トランクを使用して、このアプリケーションに接続できます。単一の Unified CM クラスタの展開では、これらのトランクの選択は簡単です。Unified CM Session Management Edition 経由で相互接続されているマルチクラスタ展開で、多数のエンド Cisco Collaboration システムへの到達に単一の SIP トランクを共有できる場合は、すべての SME トランクに対して [ベスト エフォートのアーリー オファー（Best Effort Early Offer）] が推奨されます。[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] の設計上の考慮事項については、マルチクラスタ SME 配置の SIP トランクの推奨事項の概要（6-52 ページ）を参照してください。

MTP なしのアーリー オファー、ベスト エフォートのアーリー オファー、および SME メディアの透過性

[MTP なしのアーリー オファー（MTP-Less Early Offer）] は、[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] 機能をサポートしない Unified CM Session Manager Edition（SME）クラスタ バージョンの特別な SIP トランク設定です。[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] では、[MTP なしのアーリー オファー（MTP-Less Early Offer）] と同じ機能が提供されるのに対し、[MTP なしのアーリー オファー（MTP-Less Early Offer）] の展開では、メディア リソースが SME クラスタで設定されていないことが必要です。[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] を使用する場合は、メディア リソースを必要に応じて設定できます。[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] または [MTP なしのアーリー オファー（MTP-Less Early Offer）] の SIP トランクのみを使用した SME 展開の場合、メディアに透過的な SME クラスタを配置することができます（SME クラスタでメディア リソースは不要）。これは、すべてのメディア ネゴシエーションがリーフ Unified Communications システムで行われるためで、メディア リソース（MTP、トランスコーダなど）は必要に応じて挿入されます。（図 6-15 を参照）。

[MTP なしのアーリー オファー（MTP-Less Early Offer）] は、Unified CM SIP サービス パラメータ [MTP 割り当てが失敗した場合 SIP トランク経由のコールが失敗する（Fail Call Over SIP Trunk if MTP Allocation Fails）] を利用します。このサービス パラメータのデフォルト設定は [いいえ（False）] であるので、MTP リソースを使用できない場合は、着信ディレイド オファー コールがディレイド オファー コールとして（アーリー オファーで設定された）発信 SIP トランクを経由することができます。

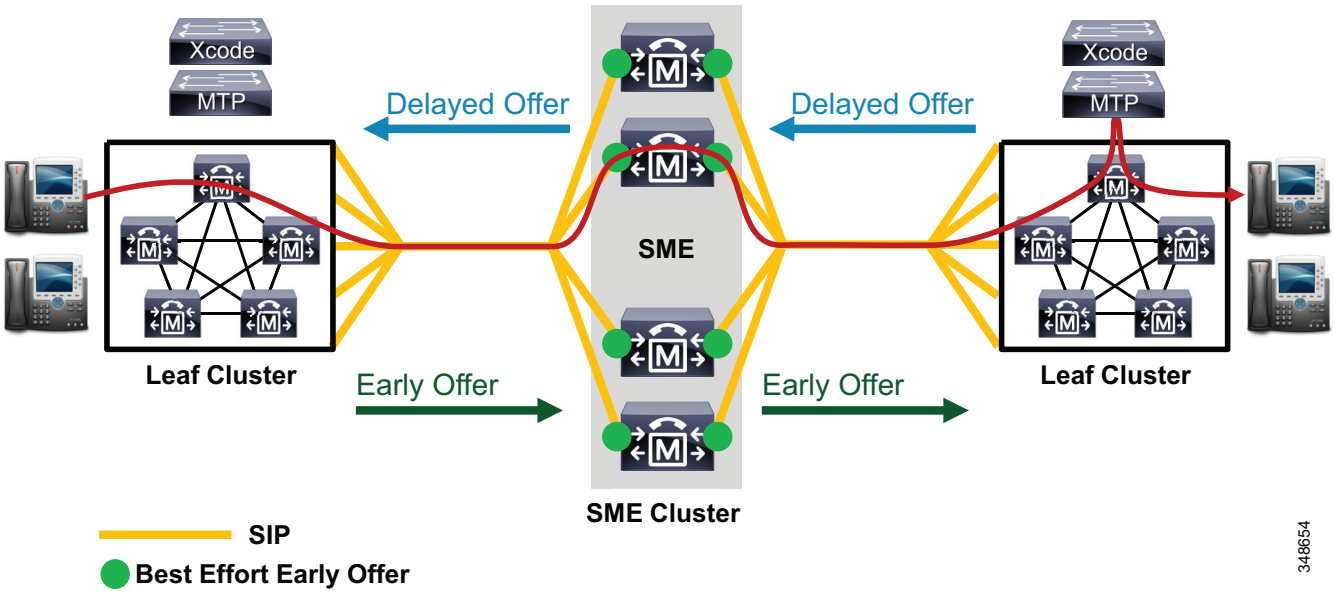
図 6-15　SME メディアの透過性に対する MTP なしのアーリー オファーの使用



MTP なしのアーリー オファーを使用してメディアに透過的な SME クラスタを設定するには、次の内容を実行します。

- SME クラスタで SIP トランクのみを使用する。
- [音声コールとビデオ コールに対する早期オファー サポートが必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）] を使用して、すべてのトランクを有効にする。
- すべての SME ノードの IPVMS サービスを無効にする。これにより、Unified CM メディア ターミネーション ポイント、会議、保留音、およびアナンシエータ リソースが無効になります。
- SME クラスタと Cisco IOS メディア リソースを関連付けしない。
- SIP トランク DTMF 設定を [初期設定なし（No Preference）]（デフォルト設定）に設定する。
- すべての SME SIP トランクで [受信オファーのオーディオ コーデック初期設定を承認（Accept Audio Codec Preference in Received Offer）] をオンにする。

図 6-16　SME メディアの透過性に対するベスト エフォートのアーリー オファーの使用



[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] を使用してメディアに透過的な SME クラスタを設定するには、次の内容を実行します。

- SME クラスタで SIP トランクのみを使用する。
- すべてのトランクで [ベスト エフォートのアーリー オファー（Best Effort Early Offer）] を有効にする。
- SIP トランク DTMF 設定を [初期設定なし（No Preference）]（デフォルト設定）に設定する。
- すべての SME SIP トランクで [受信オファーのオーディオ コーデック初期設定を承認（Accept Audio Codec Preference in Received Offer）] をオンにする。

（注）　メディア リソースは、[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] の SIP トランクが設定されている SME クラスタに展開できますが、これらのリソースが使用されるのは、1 つ以上の SIP トランクがディレイド オファーまたはアーリー オファーとして設定されている場合のみです。このような場合、アーリー オファー トランクまたはディレイド オファー トランクに発着するコールは、メディアに透過的ではなく、DTMF またはコーデックの不一致が見つかった場合はメディア リソースを呼び出すことができます。

メディア ターミネーション ポイント

MTP は次の用途で Unified CM に使用されます。

- SIP トランク上で SIP アーリー オファーを配信する場合
- DTMF 転送の不一致に対処する場合
- RSVP エージェントとして動作する場合
- 信頼されたリレー ポイント（TRP）として動作する場合
- RTP ストリームに対して IPv4 と IPv6 の変換を提供する場合

MTP は、次の 3 種類の形式で利用できます。

- Cisco IOS ゲートウェイのソフトウェア MTP：任意の Cisco IOS T-train ソフトウェア リリースで使用できます。また、Route Processor RP2 を搭載した Cisco Aggregation Services Router（ASR）1000 シリーズでは、5,000 セッション（コール）まで拡張できます。
- Cisco IOS ゲートウェイでのハードウェア MTP：任意の Cisco IOS T-train ソフトウェア リリースで使用できます。ハードウェア MTP は、オンボード DSP リソースを使用し、Cisco ルータ プラットフォームでサポートされる DSP の数に従ってコールを拡張します。
- Unified CM サブスクライバ ノードで Cisco IP Voice Media Streaming Application を使用する Cisco Unified CM ソフトウェア MTP。

Cisco IOS MTP は Unified CM MTP で推奨されます。Cisco IOS MTP が追加のコーデック タイプ、複数のメディア ストリーム、およびパススルー コーデックのサポートなど、追加拡張性と優れた機能を提供するためです。（詳細については、メディア ターミネーション ポイント（MTP）（7-7 ページ）の項を参照してください）。

次の設定例は、Cisco IOS ソフトウェア MTP の場合の例です。

```
!
sccp local Vlan5
sccp ccm 10.10.5.1 identifier 5 version 8.6.2
! Communications Manager IP address (10.10.5.1)
sccp
!
sccp ccm group 5
 bind interface Vlan5
 associate ccm 5 priority 1
 associate profile 5 register MTP000E83783C50
! MTP name (MTP000E83783C50) ... must match the Unified CM MTP name.
!
dspfarm profile 5 mtp
 description software MTP
 codec g711ulaw
 codec pass-through
 maximum sessions software 500
 associate application SCCP
```

SIP トランク上の DTMF トランスポート

DTMF 情報を SIP エンドポイント間で転送する方法はいくつかあります。一般的に、これらの方法は、アウトオブバンドおよびインバンド シグナリングに分類できます。インバンド DTMF 転送方式では、RTP ストリーム内でそのままの、またはシグナリングされた DTMF トーンのいずれかが送信されます。これらは、発信側または着信側、あるいはその両方のエンドポイントで処理および解釈される必要があります。アウトオブバンド シグナリング方式では、DTMF トーンは RTP パス外で、エンドポイントに対して直接転送されるか、必要に応じてこれらのトーンの解釈または転送、あるいはその両方を行う Cisco Unified CM などのコール エージェントを介して転送されます。

アウトオブバンド（OOB）SIP DTMF シグナリング方式には、Unsolicited Notify（UN）、Information（INFO）および Key Press Mark-up Language（KPML）が含まれます。KPML（RFC 4730）は、シスコが推奨する OOB シグナリング方式ですが、Cisco Unified CM、Cisco IOS プラットフォーム（リリース 12.4 以降）、および大半の Cisco Unified IP Phone モデルでサポートされます。INFO は、Unified CM ではサポートされていません。

インバンド DTMF 転送方式は、RTP メディア ストリームのそのままのトーン、または RFC 2833 を使用した RTP ペイロードのシグナリングされたトーンのいずれかで DTMF トーンを送信します。RFC 2833 は、SIP 製品ベンダーにおいて、主流の DTMF トーン送受信方式となっていて、シスコ音声製品の大部分でサポートされています。

インバンド シグナリング方式では、RTP メディア ストリームの DTMF トーンが送信されるため、セッションの SIP エンドポイントは、使用される転送方式（たとえば、RFC 2833）をサポートするか、このインバンド シグナリングを解釈し変換する方式を提供しなければなりません。2 つのエンポイントで、呼制御にバックツーバック ユーザ エージェント（B2BUA）サーバ（たとえば、Cisco Unified CM）が使用されていて、これらのエンドポイントで、各デバイスと呼制御エージェント間で異なる DTMF 方式がネゴシエートされる場合、DTMF の違いをどのように扱うか、つまり、MTP 挿入または OOB 方式のいずれを介するかが、コール制御エージェントにより決定されます。Unified CM では、DTMF 転送方式の不一致（たとえば、インバンドとアウトオブバンド DTMF）は、メディア ターミネーション ポイント（MTP）を挿入することで解決されます。MTP は、インバンド DTMF シグナリング（RFC 2833）で RTP ストリームを終端させ、RTP ストリームから DTMF トーンを抽出して、これらのトーンをアウトオブバンドで Unified CM に転送します。ここで、これらのトーンは、アウトオブバンド シグナリングをサポートするエンドポイントに転送されます。DTMF の不一致の場合、挿入された MTP は 2 つのエンドポイント間で常にメディア パスに存在します。RTP メディア パケットは MTP を透過的に通過しますが、インバンド DTMF パケットは RTP ペイロード タイプによって識別され、Unified CM に抽出され、アウトオブバンド DTMF に変換されます。

インバンド DTMF トーンは、RTP メディア ストリームでそのままの（可聴）トーンとして転送することもできます。ただし、この転送方式は、シスコ製品では広くサポートされていないため、通常、エンドツーエンド DTMF 転送メカニズムとしては推奨できません。インバンド オーディオ DTMF トーンは通常、G.711 a-law や mu-law などの高帯域幅コーデックを使用する場合に確実に再生成されますが、G.729 などの低帯域幅コーデックとの使用には適していません。インバンド オーディオだけが、唯一使用できる DTMF 転送メカニズムである場合、Cisco Unified Border Element を使用して、インバンド オーディオ DTMF シグナリングを RFC 2833 シグナリングに変換できます。

Unified CM SIP トランクでは、3 つの DTMF オプションを使用できます。

- DTMF Signaling Method：No Preference

  このモードでは、Unified CM は、コールに対して最も適切な DTMF シグナリング方式を選択することで、MTP リソースの使用を最小限に抑えようとします。

  両方のエンドポイントが RFC 2833 インバンド DTMF をサポートしている場合は、MTP は必要ありません。

  両方のデバイスがアウトオブバンド DTMF メカニズムをサポートしている場合、Unified CM は SIP トランク上で KPML を使用します。

  両方のデバイスが RFC 2833 インバンド DTMF とアウトオブバンド DTMF の両方をサポートしている場合は、RFC 2833 が優先されます。

  MTP が必要となる唯一のケースは、エンドポイントの 1 つがアウトオブバンド DTMF のみをサポートし、もう一方が RFC 2833 インバンド DTMF のみをサポートする場合です。

  Cisco Collaboration システムのエンドポイントの大半は、インバンドおよびアウトオブバンドの両方の DTMF をサポートします。

- DTMF Signaling Method：RFC 2833

  トランク全体の DTMF シグナリング方式を制限することにより、一方または両方のエンドポイントが RFC 2833 インバンド DTMF をサポートしていない場合に Unified CM は MTP を強制的に割り当てます。この設定では、MTP が割り当てられないのは、両方のエンドポイントが RFC 2833 インバンド DTMF をサポートしている場合だけです。

- DTMF Signaling Method：OOB and RFC 2833

  このモードでは、SIP トランクを通じてアウトオブバンド（OOB）DTMF（KPML または Unsolicited NOTIFY）と RFC 2833 インバンド DTMF の両方が送信され使用されます。これは MTP の使用される可能性が最も高いモードです。MTP リソースが必要ないのは、両方のエンドポイントが RFC 2833 インバンド DTMF およびアウトオブバンド DTMF をサポートしている場合だけです。

DTMF シグナリング方式を、Unified CM SIP トランクで [初期設定なし（No Preference）] に設定することを推奨します。このように設定することで、Unified CM は、最適な DTMF 転送方式を選択し、MTP 割り当てを最小に抑えることができます。

Cisco Unified Border Element は、VoIP ダイヤル ピア上で SIP ベースの DTMF リレー転送方式（RFC 2833（rtp-nte）、Unsolicited Notify（sip-notify）、および KPML（sip-kpml））のいずれかまたはすべてをサポートします。

SIP トランク上でのコーデック選択

通信エンティティ間でメディアを確立するには、これらのエンティティが、使用するコーデックに同意する必要があります。このコーデック（音声とビデオの両方が使用される場合には複数のコーデック）は、該当する通信エンティティでサポートされているコーデックのうち共通するもの、および設定されている Unified CM のポリシー（*リージョン*設定で設定）から導出されます。

Unified CM のリージョン設定は、設定可能なオーディオ コーデックのプリファレンス リストを提供しています。リージョンの [リンク損失タイプ（Link Loss Type）] で選択できるデフォルトの [高損失（Lossy）] および [低損失（Low Loss）] オーディオ コーデック プリファレンス リストに加え、複数のカスタム オーディオ コーデック プリファレンス リストも作成できます。オーディオ コーデック プリファレンス リストは、リージョン内およびリージョン間のコールのコーデック選択に使用できます。[最大オーディオ ビット レート（Maximum Audio Bit rate）] は依然としてリージョン内およびリージョン間のコールに適用されますが、（以前の Unified CM リリースのように）最大ビット レート設定に基づいて音声品質が最も高いコーデックを使用するのではなく、オーディオ コーデック プリファレンス リストとエンドポイントがサポートするコーデックに基づいてコーデックが選択されます。（図 6-17 および図 6-18 を参照）。

オーディオ コーデック プリファレンス リストは、Unified CM でサポートされているすべてのコーデック タイプのリストです。コーデック リストの優先順位は、カスタム プリファレンス リストとして変更して保存できます。（オーディオ コーデック プリファレンス リストからコーデックは削除できないことに注意してください）。コール セットアップ時のコーデック ネゴシエーションに使用されるコーデックのリストは、デバイスによってサポートされコーデック プリファレンス リストに存在するコーデックのサブセットで、リージョンまたはリージョン ペアの最大オーディオ ビット レートによって制限されます。

図 6-17 および図 6-18 は、コール セットアップ中にコーデックがコーデック ネゴシエーションにどのように選択されるかを示す例です。

図 6-17　最大オーディオ コーデック ビット レートが 64 kbps のコーデック選択

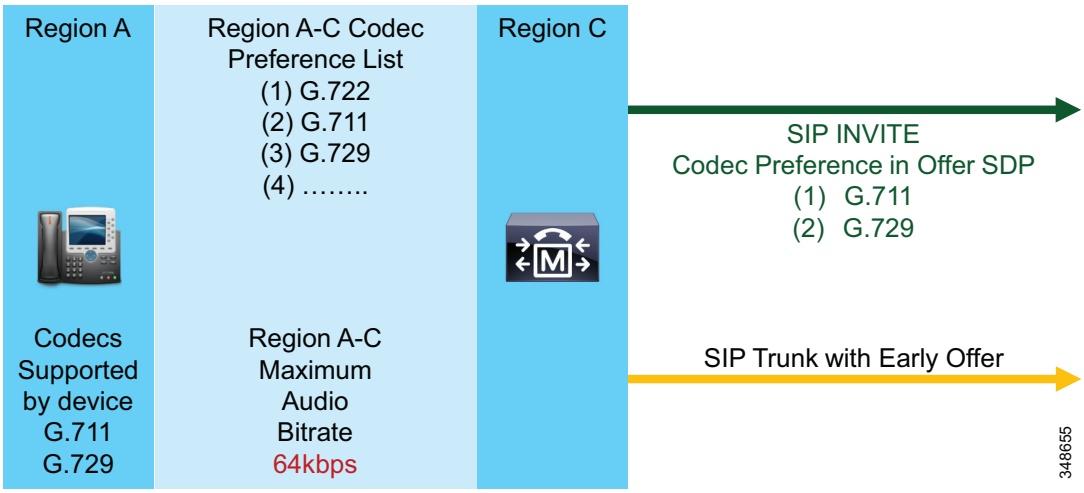
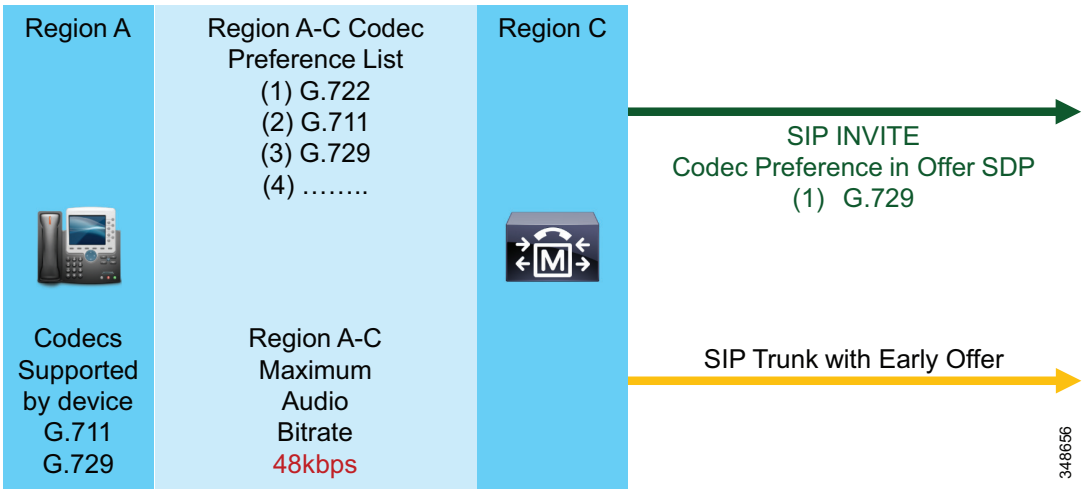
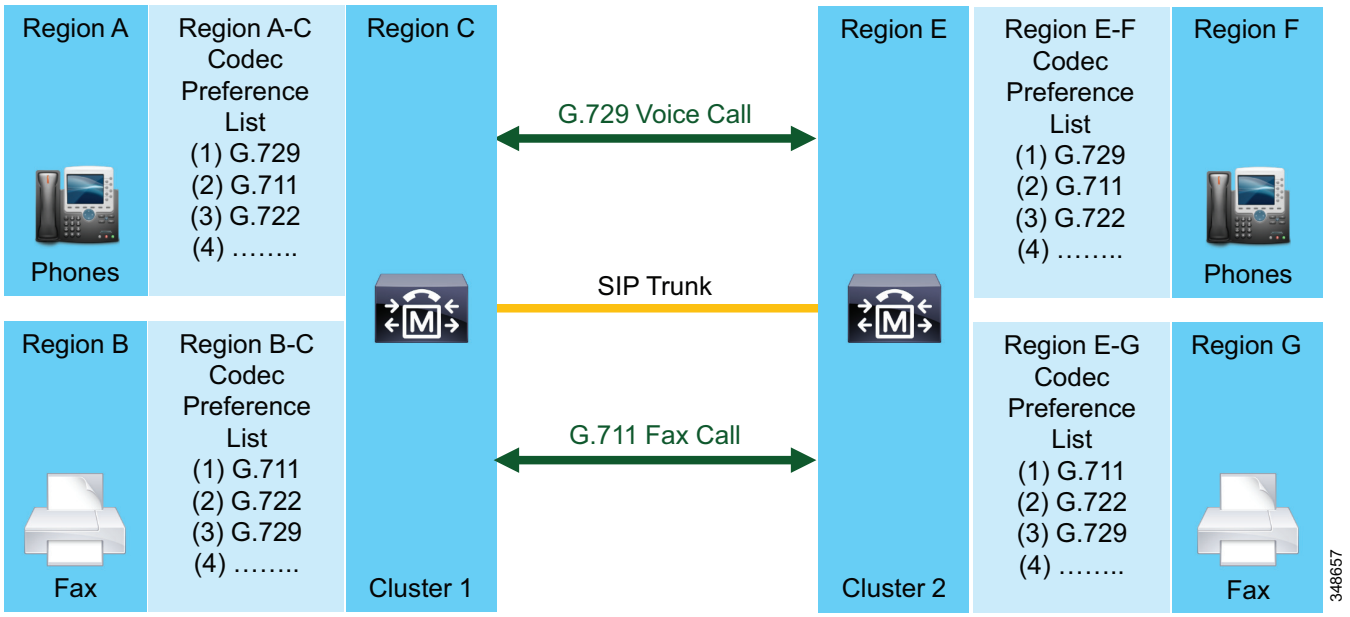


図 6-18　最大オーディオ コーデック ビット レートが 48 kbps のコーデック選択



SIP クラスタ間トランクでの 2 つの Unified CM クラスタ間のコールでは、オーディオ コーデック プリファレンス リストを使用することで、発信側と着信側デバイスのコーデック プリファレンスに基づいてコールのコーデックを選択することができます。各クラスタ内のデバイスをコーデック プリファレンスに基づいてリージョンにグループ化することで、単一のクラスタ間トランクを、優先コーデックを使用する各コール タイプで複数のコールをサポートするために使用できます。(図 6-19 を参照)。

図 6-19　　2 つの Unified CM クラスタ間の音声コールと FAX コール用のオーディオ コーデック プリファレンス リスト



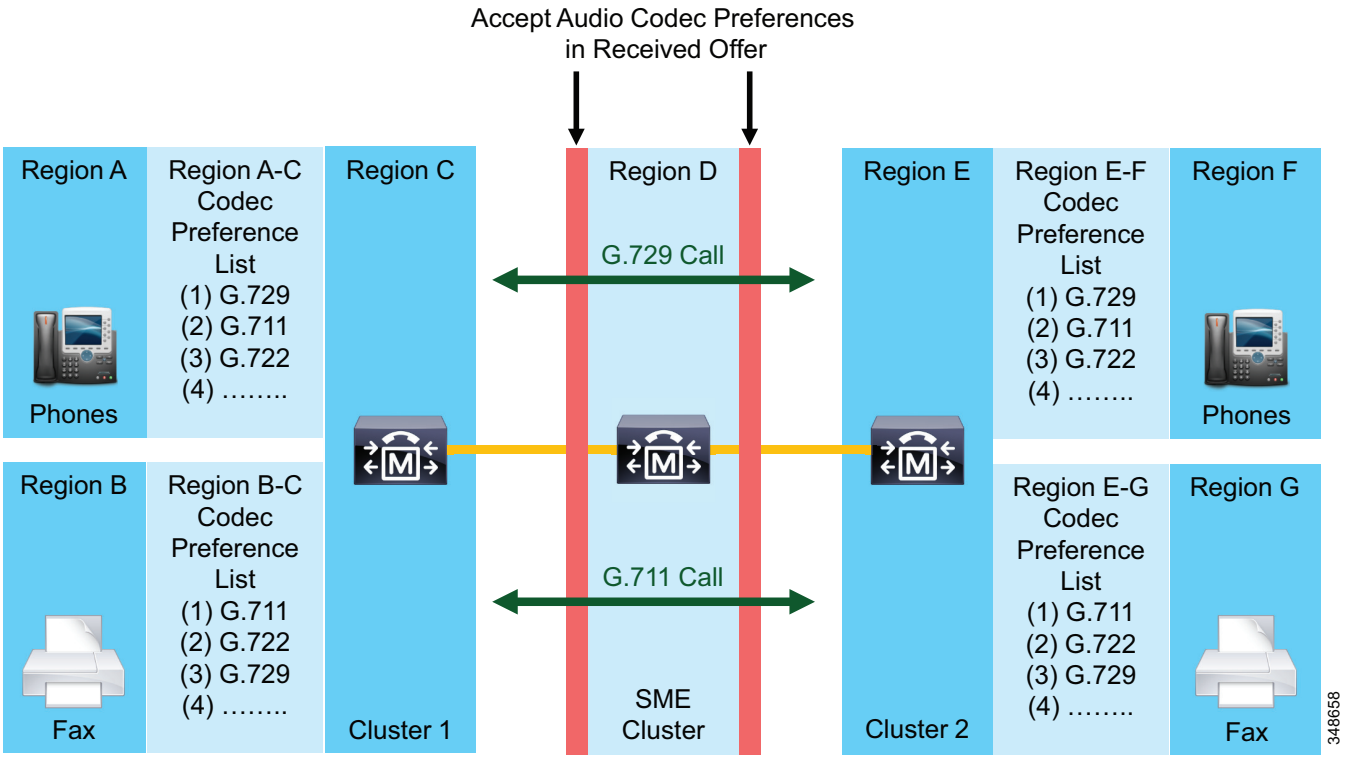
(注)　それぞれのクラスタで、各デバイス タイプに同等のリージョン間オーディオ コーデック プリファレンス リストを設定して、コールの向きやトランク設定にかかわらず各デバイス タイプに共通のコーデックが選択されるようにする必要があります。各クラスタのオーディオ コーデック プリファレンス リストが同等でない場合、コールごとに使用されるコーデックはコールの方向とトランク設定によって異なる場合があります。（通常、コーデックの優先順位はコーデックの優先順位リストを受信するクラスタによって遵守されません）。

(注)　コーデック プリファレンスが必要な場合、[MTP が必須（MTP Required）] をオンにしたアーリーオファーに設定された SIP トランクを使用しないでください。このトランク設定は、1 つのオーディオ コーデックだけに限定されている着信コールと発信コールに MTP を挿入するので、コーデック プリファレンスと選択を無効にします。

受信オファーのオーディオ コーデック初期設定を承認

コールが複数の Unified CM クラスタを通過する配置（SME 配置など）では、中間 Unified CM（SME）クラスタのリージョン間オーディオ コーデック プリファレンス リストで、発信側と着信側のデバイス間の優先コーデック選択を無効にできます。コールが SME を通過するときにエンドポイントのコーデックの優先順位が尊重されるようにするには、SIP プロファイル機能 [受信オファーのオーディオ コーデック初期設定を承認（Accept Audio Codec Preferences in Received Offer）] をすべての SME SIP トランクでオンにします。（図 6-20 を参照）。

図 6-20　SIP トランクで [受信オファーのオーディオ コーデック初期設定を承認 (Accept Audio Codec Preferences in Received Offer)] を使用する SME 配置



（注） [受信オファーのオーディオ コーデック初期設定を承認 (Accept Audio Codec Preferences in Received Offer)] 機能は、SIP トランクでのみ利用できます (SIP プロファイル機能)。SME クラスタが SIP、H.323 や MGCP トランクの組み合わせを使用する SME 配置で使用された場合、この機能は一貫した結果になりません。したがって、[受信オファーのオーディオ コーデック初期設定を承認 (Accept Audio Codec Preferences in Received Offer)] 機能は、SME クラスタが SIP トランクのみを使用して配置されている場合に使用する必要があります。

Cisco Unified CM と Cisco Unified Border Element SIP トランクのコーデック プリファレンス

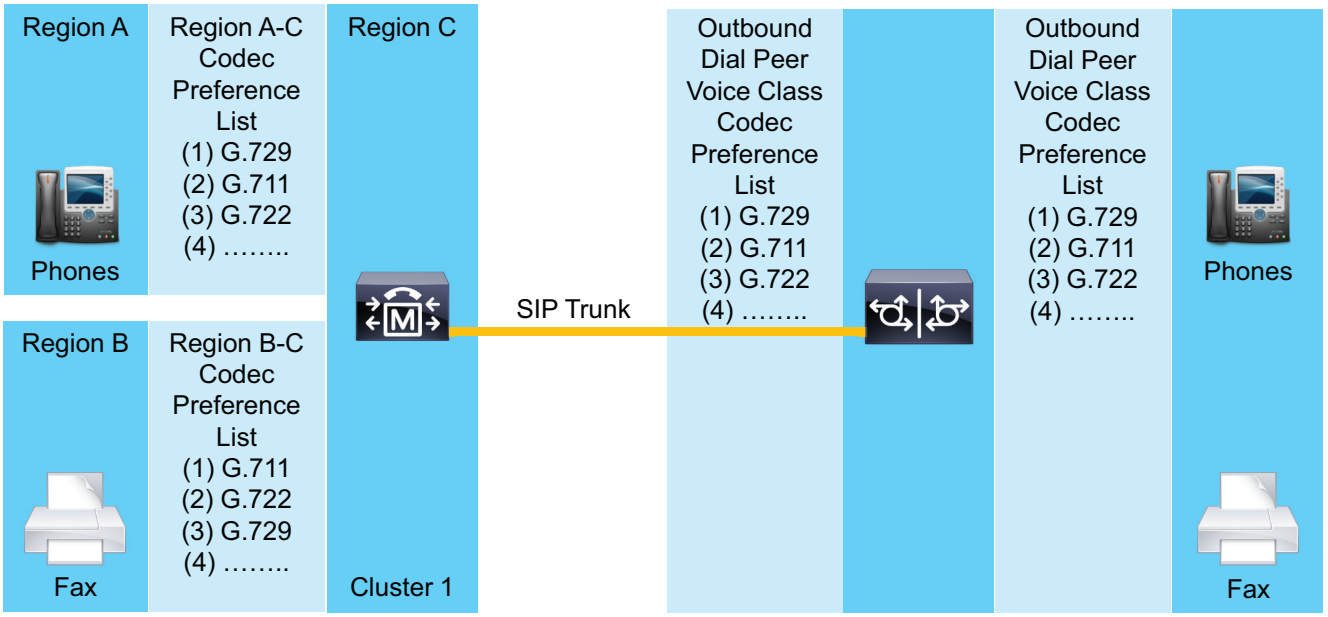
Unified CM オーディオ コーデック プリファレンス リストは、Cisco Unified Border Element を使用した Unified Communications の導入で使用して、Unified CM と Unified Border Element 間の SIP トランクの設定を簡素化できます。たとえば、音声および FAX コール用に Unified Border Element への専用 SIP トランクを使用する代わりに、単一の Unified CM SIP トランクを使用して、コールが Unified Border Element を通過するときに、デバイス タイプごとのコーデック プリファレンスを考慮できるようになります。

図 6-21 では、Cisco Unified Border Element の着信と発信のダイヤル ピアに定義された音声クラスのコーデック プリファレンス リストは、受信したオファーでリストされたコーデックの優先順位を変更しません。Cisco Unified Border Element は受信したオファーに対し、着信と発信のダイヤル ピア両方にコーデック フィルタリングを行い、ピア レッグへの着信オファーで受信したのと同じ優先順位で共通コーデックを伝えます。

オファー内で受信したものに加え、音声クラスのコーデック リストでコーデックが定義されている場合、それらのコーデックは順序付きリストで受け取ったものに付加され、送信オファーで送出されます。

したがって、単一の着信および発信ダイヤル ピアを、すべてのデバイス タイプについて Cisco Unified Border Element で設定できます。シスコでは、着信および発信両方のダイヤル ピアに、サービス プロバイダーとのネゴシエートに使用するコーデックを含む同一の音声クラス コーデック プリファレンス リストを使用することを推奨します。前述のように、コーデックの順序はまず着信オファーで受信した順序に左右され、その後音声クラス コーデック プリファレンス リストで定義された順番に左右されることになります。

図 6-21　Cisco Unified CM と Cisco Unified Border Element SIP トランクのコーデック プリファレンス



SIP Trunk Transport Protocol

SIP トランクは、メッセージ トランスポート プロトコルとして TCP、TLS（TCP を介して実行）、または UDP のいずれかを使用できます。Unified CM は、異なる転送プロトコルを使用して SIP トランクのネイティブ インターワーキング機能を提供します。TCP は、大きな SIP メッセージを分割し、再構成する機能を備えた信頼性の高い接続指向のプロトコルであるため、Cisco Collaboration システム ネットワーク内で使用することを推奨します。UDP は接続指向ではなく、信頼性も高くありません（メッセージの伝送が保証されない）。遠端デバイスの障害の検出と応答は SIP INVITE の再試行回数と SIP Trying タイマーに依存しています。SIP OPTIONS ping を使用して、ダイナミックに各 SIP トランク上の各宛先 IP アドレスの状態、およびトランク全体の総合的な状態を追跡することを推奨します。

SIP トランク タイマーの調整の詳細については、次に示す設定例およびテクニカル ノートを参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example09186a008082d76a.shtml

（注）　TCP が Cisco Collaboration システム ネットワーク内で推奨される転送プロトコルですが、ほとんどのサービス プロバイダーは、処理オーバーヘッドが TCP より低い UDP の使用を好みます。Cisco Unified Border Element は、Cisco Collaboration システム ネットワークに TCP ベースの SIP トランク接続を、サービス プロバイダー ネットワークに UDP ベースの SIP トランク接続を提供するために使用できます。

安全な SIP トランク

安全な SIP トランクには次の 2 つのプロセスが必要です。

- メディアを暗号化するようにトランクを設定する（メディア暗号化（6-36 ページ）を参照）
- シグナリングを暗号化するようにトランクを設定する（シグナリング暗号化（6-36 ページ）を参照）

メディア暗号化

メディア暗号化を SIP トランクで設定するには、トランクの [SRTP 許可（SRTP allowed）] チェックボックスをオンにします。[SRTP 許可（SRTP allowed）] をオンにすると、コールのメディアは暗号化されますが、トランクのシグナリングは暗号化されない点に注意してください。結果として、安全なメディア ストリームの確立に使用されるセッション キーは暗号化されていない状態で送信されます。そのため、Unified CM と宛先 SIP トランク デバイス間のシグナリングも暗号化し、キーや他のセキュリティ関連の情報がコールのネゴシエーション中に漏洩しないようにすることが重要です。

シグナリング暗号化

SIP トランクはシグナリング暗号化に TLS を使用します。TLS は SIP トランクに関連付けられた SIP セキュリティ プロファイルで設定します。また、TLS は X.509 証明書の交換を使用してトランク デバイスを認証し、シグナリング暗号化を可能にしています。

証明書は、次のいずれかの処理が実行されます。

- 各 Unified CM ノードの SIP トランク デーモンに対して TLS 接続を確立したい各デバイスから、そのノードに対してインポートします。
- 認証局（CA）から署名されます。この場合、リモート デバイスの証明書をインポートする必要はありません。インポートする必要があるのは CA 証明書のみです。

Unified CM には、証明書の一括インポートおよびエクスポート機能があります。ただし、[すべてのアクティブな Unified CM ノードで実行（Run on all Active Unified CM Nodes）] および最大 16 の宛先アドレスを使用する SIP トランクの場合、認証局を使用するほうが、管理上の負荷の少ない集中管理的な方法で SIP トランクにシグナリング暗号化を設定できます。

SIP トランクの TLS の詳細については、次のサイトで入手可能な最新バージョンの『*Cisco Unified Communications Manager Security Guide*』を参照してください。

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

認証局については、次のサイトで入手可能な最新バージョンの『*Cisco Unified Communications Operating System Administration Guide*』で認証局（CA）の情報を参照してください。

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

システムが安全なメディアまたはシグナリング パスを確立でき、さらにエンド デバイスが SRTP をサポートする場合、システムは SRTP 接続を使用します。システムが安全なメディアまたはシグナリング パスを確立できないか、1 つ以上のデバイスが SRTP をサポートしない場合、システムは RTP 接続を使用します。SRTP から RTP へのフォールバック（またはその逆）は、安全なデバイスから安全ではないデバイスへの転送の場合、または会議、トランスコーディング、保留音などの場合に発生する可能性があります。

SRTP が設定されたデバイスでは、デバイスの [SRTP Allowed] チェックボックスがオンで、そのコールでデバイスの SRTP 機能が正常にネゴシエートされた場合、Unified CM はコールを暗号化済みと分類します。これらの条件を満たさない場合、Unified CM はコールを安全ではないと分類します。デバイスが、セキュリティ アイコンを表示できる電話に接続されている場合、コールが暗号化されているときは電話機に鍵アイコンが表示されます。

（注）　[MTP が必須（MTP Required）] チェックボックスを使用して、スタティックに SIP トランクに割り当てられている MTP は、パススルー コーデックをサポートしないため、SRTP をサポートしません。

すべてのコールで SRTP をサポートするには、ディレイド オファーまたは [ベスト エフォートのアーリー オファー（Best Effort Early Offer）] について SIP トランクを設定します。

[音声コールとビデオ コールに対する早期オファーのサポートが必須（必要に応じて MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）] が暗号化をサポートするデバイスで設定されている場合、MTP を使用する必要のないすべてのコールが SRTP をサポートできます。MTP をコール パスに挿入する場合、このダイナミックに挿入された MTP はパススルー コーデックをサポートするため、次の場合に暗号化されたコールがサポートされます。

- 古い SCCP ベースの電話が発信元デバイスとして Unified CM に登録されている場合、最初のコール セットアップ時に SRTP をネゴシエートできます。
- ディレイド オファー SIP トランクまたは H.323 Slow Start トランクで Unified CM に対してコールを着信した場合、最初のコール セットアップ時に SRTP はネゴシエートされません。これは、使用できるセキュリティ キーがないためです。ただし、コール メディアを再ネゴシエートする場合（保留または再開後など）、SRTP をサポートするようにコール中にコールをエスカレーションできます。

アーリー オファー以外の理由（信頼されたリレー ポイントのためや、RSVP エージェントとしてなど）で、Unified CM がダイナミックに MTP を挿入する場合、パススルー コーデック（Cisco IOS MTP）をサポートする MTP で SRTP がサポートされます。

（注）　MTP を使用したインバンドからアウトオブバンド DTMF への変換は、SRTP 暗号化メディア ストリームに機能しません。MTP が DTMF パケットを復号化できないからです。

ユーザ ID および SIP トランク

発信側ユーザの名前と番号は、次の SIP メッセージ ヘッダーで Unified CM SIP トランクを介して送信できます。

送信者 : (From:)	From: "Jim Bob" <sip:1000@10.10.199.250> From: "Anonymous" <sip:localhost>
送信先	To: "Nick Cave" <sip:2000@10.10.100.251>
P-Asserted-Identity:	P-Asserted-Identity: "Jim Bob" <sip:1000@10.10.199.250>
Remote-Party-ID:	Remote-Party-ID: "Jim Bob" <sip:1000@10.10.199.250>

SIP 要求と応答で送信される From メッセージと From メッセージのヘッダーは、コールの方向を示します。(From ヘッダーが発信側ユーザを表し、To ヘッダーが着信側ユーザを表します)。From ヘッダーおよび To ヘッダーは、コールのすべての SIP 要求と応答で同じ状態のままです。

SIP では、From ヘッダーが匿名で行われることを可能にするので、発信側のユーザ情報が着信側のユーザに表示されません。

P-Asserted-Identity および Remote-Party-ID ヘッダー(ある場合)には、常にユーザの ID が含まれます。これらの ID ヘッダーを持つ SIP メッセージに含まれるユーザ情報は方向性を持つので、ヘッダーは発信側のユーザの ID を初期 INVITE に含み、着信側のユーザの ID を応答に含みます。P-Asserted-Identity および Remote-Party-ID ヘッダーは、匿名コールの ID を追跡するために使用できます。

デフォルトでは、P-Asserted-Identity および Remote-Party-ID ヘッダーの両方は、Unified CM SIP トランクを介して送信されますが、無効にできます。P-Asserted-Identity および Remote-Party-ID ヘッダーの使用は、Unified CM SIP トランクが接続されているデバイスによって異なります。P-Asserted-Identity は、最新の標準で、Remote-Party-ID より広く使用されています。P-Asserted-Identity 標準(RFC 3325)は、信頼できない SIP レルム間の認証をサポートするため、Remote-Party-ID より安全であると見なされます。信頼できないネットワークへの SIP トランク接続の場合、P-Asserted-Identity ヘッダーではなく、P-Preferred-Identity ヘッダーを送信するように Unified CM を設定します。Unified CM は、送信された P-Preferred-Identity ヘッダーのダイジェスト認証チャレンジに応答します。

発信者 ID の表示と表示禁止

上記のように、発信側のユーザ名および番号は、SIP トランクで送信される SIP メッセージの From ヘッダーで匿名にできます。発信者名および番号の表示と表示禁止は、3 つの方法で有効にできます。

- 発信デバイスに関連付けられたトランスレーション パターンの発信者名と番号の表示または表示禁止の設定
- Unified CM トランクへの発信者名と番号の表示または表示禁止の設定
- Unified CM SIP トランクへの P-Asserted-Identity 関連の SIP プライバシー値の設定

これらの発信者 ID の表示と表示禁止の設定オプションは、次の優先順位（プライオリティが高いものを最優先）で実行します。

1. SIP プライバシー値
2. トランクの設定
3. デバイス設定

発呼側番号と着呼側番号の正規化および SIP トランク

パブリック PTSN または IP PTSN と、企業のプライベート ネットワークの間のエッジをコールが通過する際、コール セットアップ メッセージで送信される着信側番号と発信側番号は、+E.164 などのグローバルにルーティング可能な国際フォーマットに可能な限り正規化されている必要があります。これらの番号をどのようにして、どこで正規化するかは、企業が接続されている PSTN ネットワークのタイプに左右されます。

ISDN および Q.931 PSTN ネットワーク

ISDN Q.931 および PSTN ネットワーク内のコールは、着信番号と発信番号を分類するために、コール セットアップ メッセージの番号タイプ フィールドに追加の情報を提供します。番号タイプは、Unknown、Subscriber、National、または International のいずれかです。PSTN から企業ネットワークへのコールの場合、適切な数字を前に付けて、+E.164 値に発信側番号をグローバル化するために、番号タイプのパラメータを企業で使用できます。企業内のグローバル化された PSTN 発信側番号を使用すると、追加の番号操作をほとんど（もしくはまったく）することなく、PSTN の発信者にコールを返すことができます。サービス プロバイダーによって送信される番号形式によっては、企業の着信側番号を企業のダイヤル プランの番号と一致するように変更しなければならない場合もあります。企業内に +E.164 ダイヤル プランを配置することを推奨します。

これらの番号タイプがどのように使用されるかについての詳細および例、そしてダイヤル プランの推奨事項については、ダイヤル プラン（14-1 ページ）の章を参照してください。

SIP ベースの IP PSTN ネットワーク

SIP ベースの IP PSTN ネットワークからのコールには、SIP メッセージに番号タイプ情報は含まれません。この場合、IP PSTN サービス プロバイダーは、グローバルにルーティング可能な国際表現（たとえば、+E.164 番号）を使用して PSTN 発信側番号を示す必要があります。サービス プロバイダーによって送信される番号形式に応じて、企業の着信側番号が企業のダイヤル プランの番号と一致するように変更しなければならない場合があります。企業内に +E.164 ダイヤル プランを配置することを推奨します。

サービス プロバイダーが PSTN 発信側番号を +E.164 形式で送信し、着信側番号を、企業のダイヤル プラン（+E.164 を推奨）で使用される番号に一致する形式で送信する場合、企業内でこれらの番号に変更を加える必要はほとんどありません（もしくはまったくありません）。

SIP では番号タイプを転送できないため、発信側番号の正規化は、コールが Unified CM のコール ルーティング プロセスに送られる前に実行する必要があります。この変換は、たとえば、着信 SIP ゲートウェイで実行できます。次の設定例は、このような変換を実行するために Cisco IOS ゲートウェイで定義できる変換ルールを示しています。

```
voice translation-rule 1
 rule 1 // /+4940/ type subscriber subscriber
 rule 2 // /+49/ type national national
 rule 3 // /+/ type international international
...
voice translation-profile 1
 translate calling 1
...
dial-peer voice 300 voip
```

```
 translation-profile outgoing 1
 destination-pattern T
 session protocol sipv2
 session target ipv4:9.6.3.12
...
```

上記の例のように設定されている場合、Unified CM との通信に SIP を使用する Cisco IOS ゲートウェイは、+ 記号を含む、E.164 形式に正規化された発信側情報番号を送信します。この Unified CM 設定では、番号タイプが「unknown」のすべてのコールが、このゲートウェイから受信されます。プレフィックスを追加する必要はありません。

変換ルールの設定の詳細については、次のサイトから利用できる『*Voice Translation Rules*』マニュアルを参照してください。

https://www.cisco.com/en/US/tech/tk652/tk90/technologies_tech_note09186a0080325e8e.shtml

Unified CM は、発信コールの発番号を、正規化されたグローバル形式に設定できます。SIP トランクから発信されるコールの番号タイプは「unknown」になります。Cisco IOS ゲートウェイは、除去が行われない場合はこの番号タイプを International に変更し、接続サービス プロバイダーにより要求された場合は除去と番号タイプ変更の両方を実行しなければなりません。

Cisco Collaboration システムの配置で SIP トランクのみを使用する理由

1 つ以上の Unified CM クラスタで構成される Cisco Collaboration Systems ネットワークの場合、Unified Communications アプリケーション、セッション ボーダー コントローラ、およびゲートウェイは、SIP を唯一の相互接続トランク プロトコルとして使用して、一般的な機能を十分に備えたシンプルな Collaboration Systems ネットワークを構築できます。

他のトランク プロトコルと比べて、今日の SIP トランクは、次のような多数の独自の機能をサポートします。

- トランクの全体的な動作ステータスおよび各トランクの宛先ノードの状態を追跡する SIP OPTIONS ping。
- コーデック プリファレンス リストおよび SDP オファーで受信されるコーデック プリファレンスを受け入れる機能。
- BFCP ベースのプレゼンテーション共有および遠端カメラ制御を使用した H.264 ビデオのサポート。
- SIP メッセージの正規化および透過性。Unified CM を通過するときに SIP メッセージおよびメッセージ ボディ（SDP）の内容を透過的に転送または変更できる SIP トランクに強力なスクリプトベースの機能を提供します。正規化および透過性のスクリプトは、SIP の相互運用性の問題に対処するように設計されているため、Unified CM は SIP ベースのサードパーティ PBX、アプリケーション、および IP PSTN サービスと相互運用できます。
- IPv4 のみ、IPv6 のみ、またはデュアル スタック（IPv4 および IPv6）ANAT 対応 SIP トランクに対するサポート。

SIP トランクの設計と設定の推奨事項

SIP ベースの Cisco Collaboration システム ネットワークを設計および導入する場合、次の SIP トランク機能を使用することを推奨します。

Unified CM リーフ クラスタおよび SME クラスタに対するベスト エフォートのアーリー オファー

[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] に設定された SIP トランクのみを使用すると、リーフ クラスタでのアーリー オファーの作成に MTP を使用する必要がなくなり、SME クラスタがメディア ネゴシエーションに対して透過的になります。[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] を使用すると、発信側デバイスのオファーを作成するためのメディア機能に関する十分な情報を持っている場合にのみ、SIP トランクはアーリー オファーを送信します。この情報を持っていない場合は、代わりにディレイド オファーを送信します。

[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] の前に、リーフ クラスタ トランクでディレイド オファーまたはアーリー オファーのどちらを使用するかの判断は通常、クラスタに登録されている古い SCCP エンドポイントの数に基づきます。古い SCCP エンドポイントでは、多数の SCCP エンドポイントがクラスタ内に存在する、アーリー オファー SIP トランクを介するコールに対しオファーを作成するには MTP の挿入が必要なため、MTP の使用を避けるためにディレイド オファーが推奨されていました。[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] を使用すると、クラスタに登録されているエンドポイントのタイプに基づいてアーリー オファーまたはディレイド オファーの SIP トランク設定を決定する必要がなくなります。

Cisco Collaboration システムの展開では、Cisco Unified Communications 以外のアプリケーションとサービスで、アーリー オファーのみの受信が必要な場合があります。アーリー オファーを常に受信する要件に対処するオプションが 2 つあります。

- Cisco Unified Border Element では、SIP ディレイド オファーからアーリー オファーへの変換機能を音声コールに対して提供します。着信ディレイド オファーのコールが発信アーリー オファーのコールに変換されるので、Unified CM および SME で、[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] のトランクを使用できるようになります。この使用例で代表的と言えるのは、通常は SIP アーリー オファーを常に受信する必要があるサービス プロバイダーの IP PSTN 接続です。
- SIP アーリー オファーのみを受け入れる企業の Unified Communications アプリケーションの場合、専用のアーリー オファー SIP トランクを Unified CM リーフ クラスタから Unified Communications アプリケーションに使用できます。多数の MTP がアーリー オファー SIP トランクで必要な場合は、Cisco Unified Border Element のディレイド オファーからアーリー オファーへの変換機能を使用することを検討してください。

SME クラスタでは、[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] は SME クラスタをメディア ネゴシエーションに透過的にすることで [MTP なしのアーリー オファー（MTP-Less Early Offer）] と同じ役割を果たします。次にメディアの決定を末端の Unified Communications システムで行われるように強制します。このシステムでは、必要に応じて、DTMF またはコーデックの不一致問題に対処するためにメディア リソースを挿入できます。メディア リソースは、MTP なしのアーリー オファー SME トランクに関連付けないでください。必要に応じて、メディア リソースを [ベスト エフォートのアーリー オファー（Best Effort Early Offer）] のトランクに関連付けることができます。

すべての Unified CM ノードで実行

この機能は、SIP トランクおよびルート リストでサポートされ、Unified CM および SME クラスタから、そして Unified CM および SME クラスタを介してコール ルーティングを大幅に簡素化します。すべての SIP トランクおよびルート リストで、[すべての Unified CM ノードで実行（Run on all Active Unified CM Nodes）] 機能をオンにすることを強く推奨します。コール ルーティングは、[すべての Unified CM ノードで実行（Run on all Unified CM nodes）] とルート ローカル機能の組み合わせで簡略化されます。ここでは、SIP トランクを介した電話は、電話機が登録されている Unified CM ノードから常に発信されます。トランク間のコールと同様に、発信 SIP トランク コールは、着信トランク コールが到達した Unified CM ノードから常に発信されます。すべての SIP トランクおよびルート リストに対して [すべての Unified CM ノードで実行（Run on all Unified CM nodes）] をオンにすると、クラスタ内のコール処理ノード間でコールをセットアップする必要がなくなります。これは、WAN を介したクラスタリングが Unified CM または SME クラスタで配置されるときに実用的です。

最大 16 の SIP トランク宛先 IP アドレス

SIP トランクは、最大 16 の宛先 IP アドレス、16 の完全修飾ドメイン名、または単一の DNS SRV エントリを使用して設定できます。追加の宛先 IP アドレスをサポートしているため、2 つの Unified Communications システム間のコール分配のために、ルート リストおよびルート グループに関連付けられた複数のトランクを作成する必要性が軽減されます。結果として、Unified CM トランク設計が単純になりますIP アドレスが SIP トランクで宛先として使用される場合、Unified CM は定義されたすべての宛先 IP アドレス間でコールをランダムに配信します。

SIP OPTIONS ping

SIP トランクに関連付けられた SIP プロファイルで SIP OPTIONS ping 機能を有効にして、トランクの宛先の状態およびトランクの全体の状態をダイナミックに追跡できます。

PRACK

PRACK は、PSTN との相互運用シナリオに 1XX 応答の信頼性を提供します。また、双方向メディアを設定する前に交換する必要がある SIP メッセージ数を減らすのに使用することもできます。トランクに関連付けられた SIP プロファイルで [SIP Rel1XX オプション（SIP Rel1XX Options）] パラメータを介して PRACK を有効にします。

SIP トランクの DTMF シグナリング方式：初期設定なし

[DTMF シグナリング方式：初期設定なし（DTMF Signaling Method: No Preference）] の使用は、SIP トランクでは推奨されません。このモードでは、Unified CM は、コールに対して最も適切な DTMF シグナリング方式（インバンドまたはアウトオブバンド）を選択することで、MTP リソースの使用を最小限に抑えようとします。

Unified CM Session Management Edition

Cisco Unified Communications Manager Session Management Edition（Unified CM SME）は、マルチサイト分散型呼処理配置で推奨されるトランクとダイヤル プランの集約プラットフォームです。SME は基本的に、トランク インターフェイスだけを使用し、IP エンドポイントを使用しない Unified CM クラスタです。このクラスタには、リーフ システムと呼ばれる、複数のユニファイド コミュニケーション システムを集約できます（図 6-22 を参照）。

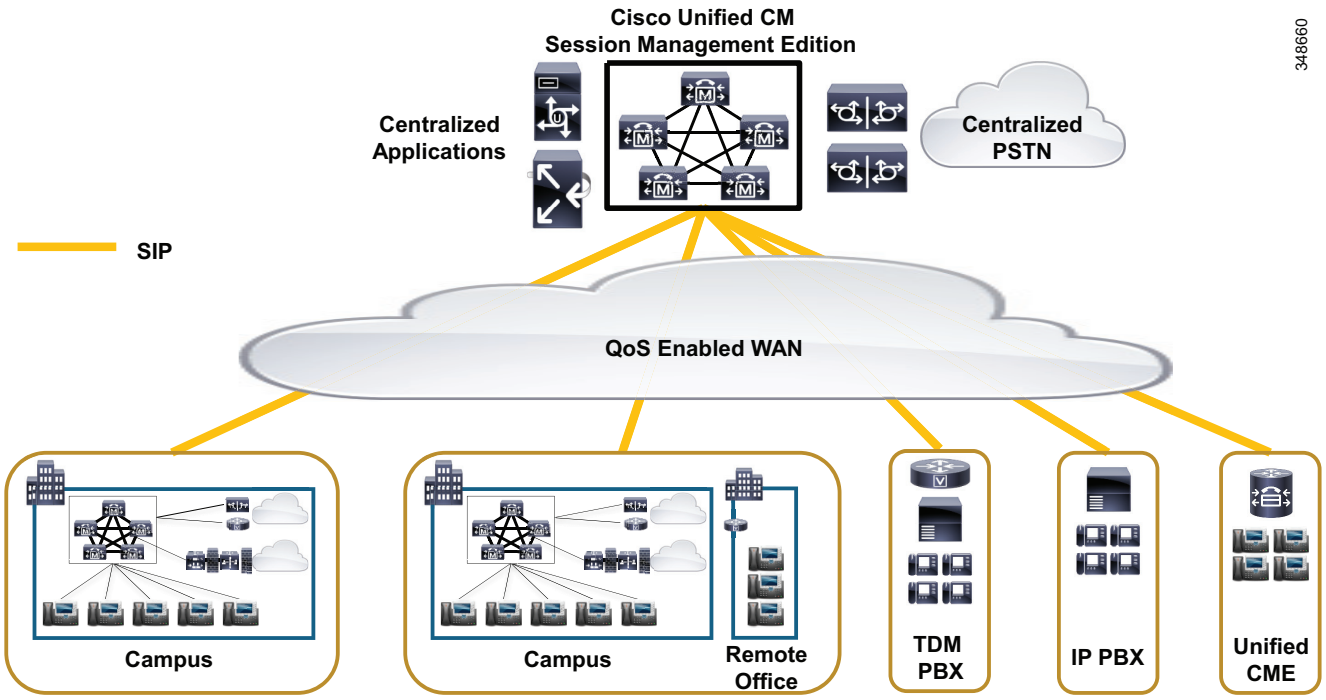
SIP が H.323 および MGCP トランクで使用できない追加の機能を提供するため、SIP トランクは、SME およびリーフ Unified Communications システムで大いに推奨されます。この項の後半で述べられるように、SIP トランクのみを使用する SME 設計専用の特定のトランク機能があります。Unified Communications ネットワークが、ゲートウェイまたは他の Unified Communications アプリケーションへの H.323 または MGCP トランク接続をサポートする必要がある場合、SME クラスタで SIP 専用トランク機能を保持するために、SME ではなく、リーフ Unified Communications システムにこれらの H.323 および MGCP トランク（もしくはどちらか一方）を接続します。

Cisco Unified CM Session Management Edition（SME）は、次のコール タイプをサポートします。

- ボイス コール
- ビデオ コール
- 暗号化されたコール
- FAX コール

また、Unified CM Session Management Edition を使用して、PSTN のほか、PBX、集中型のユニファイド コミュニケーション アプリケーションなどのサードパーティのユニファイド コミュニケーション システムに接続できます。

図 6-22　Unified CM Session Management Edition を使用したマルチサイト分散型呼処理配置



Unified CM Session Management Edition を配置する状況

次のいずれかの操作を行う場合は、Unified CM Session Management Edition を配置することを推奨します。

- 集中型ダイヤル プランの作成および管理

  他のすべてのユニファイド コミュニケーション システムに接続するために各ユニファイド コミュニケーション システムに別個のダイヤル プランおよびトランクを設定するのではなく、Unified CM Session Management Edition を使用すると、SME クラスタを指す簡潔なダイヤル プランおよびトランクをリーフのユニファイド コミュニケーション システムに設定できます。Unified CM Session Management Edition には、集中型ダイヤル プランと、他のすべてのユニファイド コミュニケーション システムに到達するためのこのプランに対応する情報が含まれています。

  （注）　SME および Unified CM リーフ クラスタで ILS GDPR を実行すると、ダイヤル プランの管理をさらに簡略化できます。これは、個々のディレクトリ番号、DN に対応する E.164 番号、ルート パターン（たとえば、内線番号範囲および外線番号範囲）、および URI は、ILS サービスを使用して配信できるためです。このアプローチでは、必要なルート パターンの数を減らし、それぞれ一意の番号範囲のルート パターンではなく、呼制御システム（Unified CM クラスタなど）ごとに 1 つの SIP ルート パターンにすることで、ダイヤル プランの管理を簡略化します。ILS および GDPR の詳細については、クラスタ間検索サービス（ILS）および Global Dial Plan Replication（GDPR）（10-34 ページ）を参照してください。

- 集中型 PSTN アクセスの提供

  Unified CM Session Management Edition を使用すると、1 つ（または複数）の集中型 PSTN トランクに PSTN アクセスを集約できます。集中型 PSTN アクセスには一般に、ブランチベースの PSTN 回線の削減または排除を伴います。

- アプリケーションの集中化

  Unified CM Session Management Edition の導入によって、会議やボイス メールなどの一般に使用されるアプリケーションを直接 SME クラスタに接続できるため、複数のトランクの管理によるリーフ システムへのオーバーヘッドが軽減されます。

- Unified Communications システムに移行するために PBX を集約

  Unified CM Session Management Edition は、レガシー PBX から Cisco Unified Communications システムへの移行の一環として、複数の PBX の集約ポイントを提供できます。ILS GDPR を導入する場合、各サードパーティ製システムでサポートされている番号範囲や URI を ILS GDPR にインポートし、SIP ルート パターンおよび対応する SIP トランクを介して到達できるようにすることもできます。

Unified CM Session Management Edition と標準の Unified CM クラスタの相違

Unified CM Session Management Edition ソフトウェアは、Unified CM と同じです。ただし、Unified CM ソフトウェアは、この新しい導入モデルの要件を満たすために強化されています。Unified CM Session Management Edition は、多数のトランクツートランク接続をサポートするように設計されているため、次に示す設計上の考慮事項に従う必要があります。

容量とサイジング

Unified CM Session Management クラスタは、リーフ Unified Communications システム間（たとえば、Unified CM クラスタと PBX 間）、集中型 PSTN 接続間、および集中型アプリケーションへの予想される BHCA トラフィック ロードに基づいて正確にサイジングすることが重要です。使用している Unified Communications システムでのユーザの平均的な BHCA およびコール保留時間を判断し、その情報をシスコ アカウント システム エンジニア（SE）またはシスコ代理店と共有して、Unified CM Session Management Edition クラスタの規模を適切に決定してください。SME サイジングの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

SME トランク

SME は SIP、H.323、および MGCP トランクをサポートしますが、Cisco Unified Communications System Release 8.5 およびそれ以降のバージョンを実行する SME および Unified CM リーフ クラスタのトランク プロトコルとして SIP を使用することを推奨します。

SME クラスタで SIP トランクのみを使用すると、「メディア トランスペアレント」クラスタを展開できます。ここでは必要に応じて、メディア リソースが SME ではなく、エンドまたはリーフ Unified Communications システムによって挿入されます。WAN を介してクラスタリングする場合、SIP トランクのみを使用すると、SME ノード間で拡張ラウンド トリップ時間（RTT）を使用できるようにもなります。

SME SIP トランクは、[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] トランクとして設定する必要があります。リーフ Unified CM クラスタ SIP トランクもまた、[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] として設定する必要があります。

メディア ネゴシエーション用の SME の透過性

MTP またはトランスコーダなどのメディア リソースは、コールが正常に続行するために必要で、これらのリソースがエッジまたはリーフ Unified Communications システムで割り当てられる必要があります。SME トランク メディア リソースが SME クラスタを通過するコールに使用される場合、メディア パス コールが SME メディア リソースを介してヘアピンします。SIP トランクのみ、そして [ベスト エフォートのアーリー オファー（Best Effort Early Offer）]（または [MTP なしのアーリー オファー（MTP-Less Early Offer）]）を使用して、メディア リソースを使用せずに、SME クラスタを配置できます。メディア リソースが必要な場合は、リーフ Unified Communications システムで提供することができます。

SME CoW+ による WAN を介したクラスタリング

Cisco Unified CM 9.1 およびそれ以降のリリースでは、SME の配置では、SME クラスタ ノード間で最大 500 ミリ秒のラウンドトリップ時間（RTT）をサポートします。（図 6-23 を参照）。この拡張 RTT は SME クラスタのみに適用され（標準の Unified CM クラスタ設計の最長 RTT は 80 ミリ秒です）に適用され、次の設計上の制限があります。

- WAN（CoW+）を介したクラスタリングの拡張ラウンドトリップ時間使用した SME の配置は、SIP トランクだけでサポートされます。すべての SIP トランクは、コールが SME クラスタ内のノード間でルーティングされないように、すべて [ベスト エフォートのアーリー オファー（Best Effort Early Offer）]（推奨）またはすべて [MTP なしのアーリー オファー（MTP-Less Early Offer）] として設定され、[すべての Unified CM ノードで実行（Run on all Unified CM Nodes）] 機能を使用する必要があります。H.323、MGCP、および SCCP プロトコルは、WAN のラウンドトリップ時間を介した拡張クラスタリングの SME 配置ではサポートされていません。
- エンドポイントまたは CTI デバイスは SME クラスタに設定、または登録されません。
- MTP、信頼されたリレー ポイント（TRP）、RSVP エージェント、トランスコーダなどのメディア リソースは、SME クラスタに設定または登録されません。（Unified CM ノードでホストされているメディア リソースを無効にするには、クラスタ内の各ノードの IPVMS サービスを非アクティブにします）。
- サイト間の Intra-Cluster Communication Signaling（ICCS）トラフィックに最低 1.544 Mbps（T1）の帯域幅が必要です。
- Intra-Cluster Communication Signaling（ICCS）トラフィックに必要な帯域幅に加え、パブリッシャ ノードとあらゆるリモート サブスクライバ ノード間のデータベースおよびその他のサーバ間トラフィック用に、最低でも 1.544 Mbps（T1）の帯域幅が必要になります。

（注）　すべての SME 設計を使用して、SME 設計は、配置前にシスコの SME チームによる確認と承認が必要になります。

SME クラスタのアップグレード プロセスは、2 つの主要な部分で構成されています。

- バージョンのスイッチングオーバー：コール処理ノードが新しいソフトウェア バージョンで再起動され、初期化されます（サーバあたり約 45 分かかります）。
- データベース複製：サブスクライバのデータベースは、パブリッシャ ノードのデータベースと同期化されます。

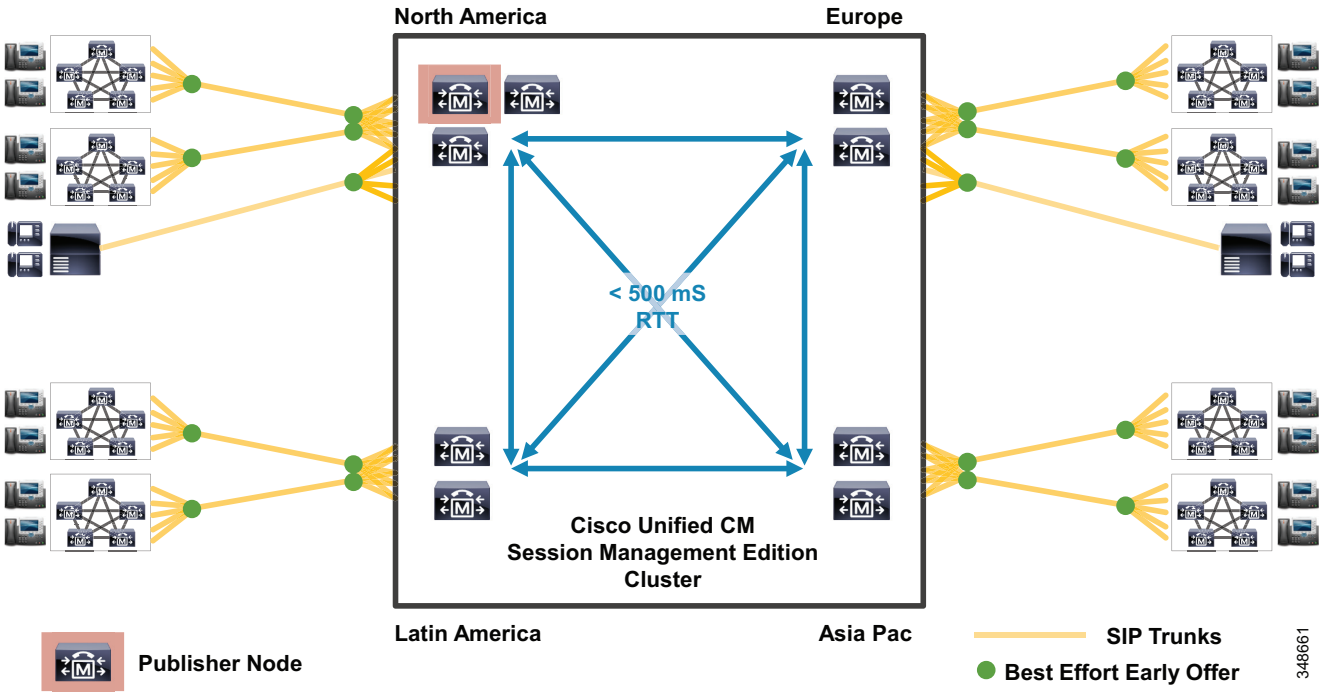
このデータベース複製フェーズを完了するのにかかる時間は、クラスタ内のサブスクライバ ノードの数とパブリッシャおよびサブスクライバ ノード間の RTT によって異なります。データベース複製プロセスにはサブスクライバの呼処理機能への影響はほとんどなく、通常の SME クラスタ処理中にバックグラウンド処理として実行できます。データベース複製フェーズ中に SME クラスタ設定に変更を加えないようにしてください。これにより、複製が完了するまでの時間が遅くなります。

拡張 RTT を使用して SME クラスタを配置する場合、クラスタをアップグレードする前に、パブリッシャ ノードで次の管理者レベル CLI コマンドを実行します。

utils dbreplication setprocess 40

このコマンドは、複製設定のパフォーマンスを向上させ、データベース複製に要する時間が短縮されます。

図 6-23　Unified CM Session Management Edition：拡張ラウンド トリップ時間を使用した WAN を介したクラスタリング



Unified CM バージョン

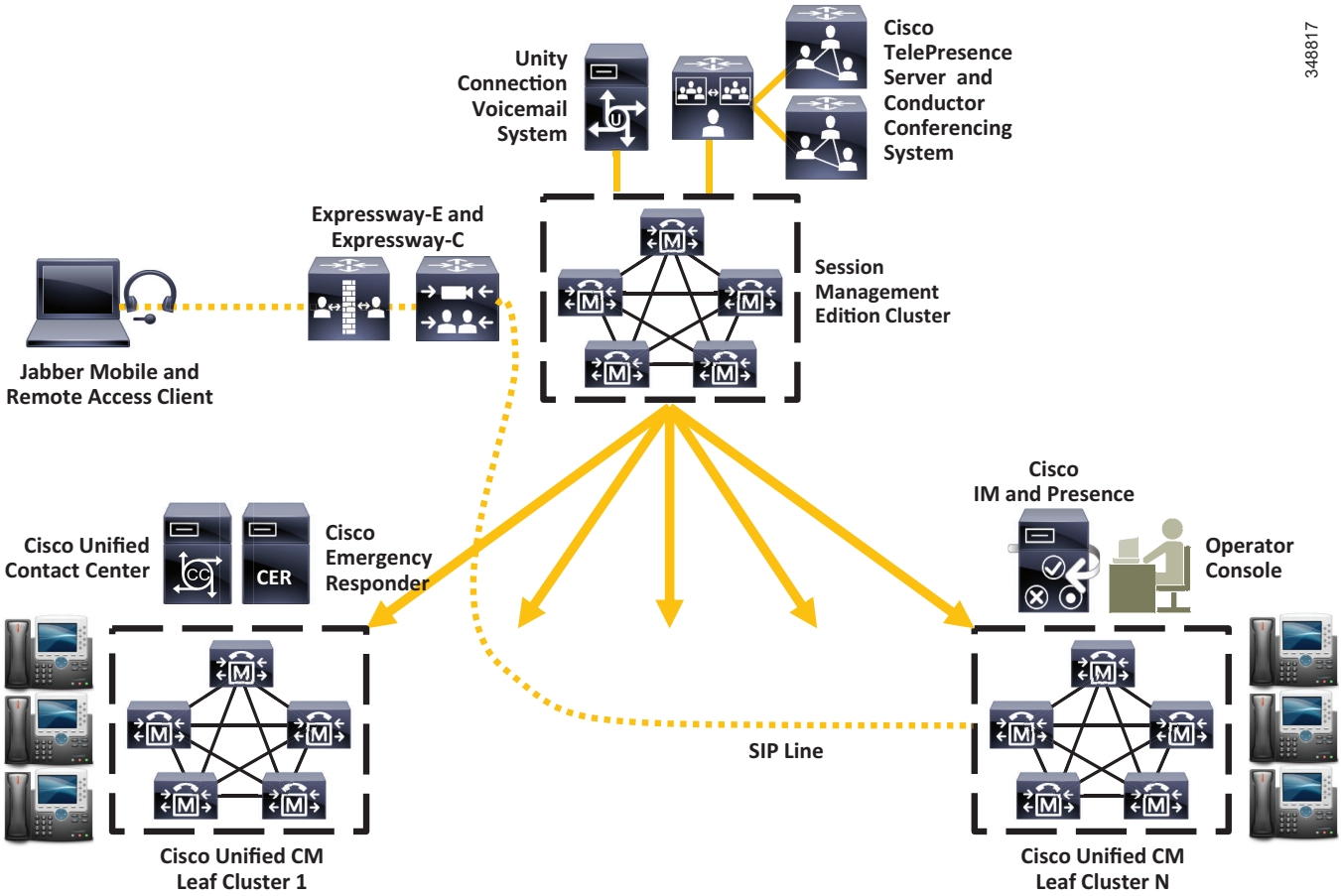
最新の Cisco Collaboration システムのリリースと SIP トランクを、すべての Unified CM リーフ クラスタと SME クラスタで使用すると、コーデックのプリファレンス リスト、ILS、GDPR、および Enhanced Locations Call Admission Control（CAC）といった一般的なクラスタ間機能のメリットを導入環境で享受できるようになります。最新の Unified CM バージョンへのアップグレードをすべてのクラスタ上で行いたくない場合、最小推奨バージョンは SIP トランクを使用する Cisco Unified CM 8.5 となります。これは、Unified CM および Session Management Edition クラスタを介したコール ルーティングを改善し、簡略化する機能がこのバージョンに含まれているためです。

Session Management Edition での Unified Communications アプリケーションの一元化に関するガイダンス

Session Management Edition クラスタへの Unified Communications（UC）アプリケーションの同時配置と接続では、各リーフ UC システムに関連付けられた複数のインスタンスではなく、1 つの集中型アプリケーション インスタンスを使用することで、規模を節約して、管理上のオーバーヘッドを縮小できます。ここでは、Session Management Edition クラスタと同時配置できる UC アプリケーションの設計ガイドラインの一部について説明します。

一般的なルールとして、コールを確立するために番号に基づいたコール ルーティングのみに依存するアプリケーションは、Unified CM Session Management Edition に接続できます。デバイス状態を追跡するために追加のインターフェイス（CTI など）を必要とするアプリケーション（たとえば、ユニファイド コンタクト センターやリーフ クラスタ）は、リーフ クラスタに接続する必要があります。（図 6-24 を参照）。

図 6-24　　集中型 UC アプリケーションと Session Management Edition



集中型ボイス メール：Unity Connection

Cisco Unity Connection などのボイスメール アプリケーションは、SME クラスタに接続し、すべてのリーフ UC システム上のユーザにボイスメール サービスを提供できます。

リーフ クラスタと SME 間のクラスタ間トランク、およびボイスメール アプリケーションとのトランク接続では、ボイスメールにルーティングされるコールとともに、元の着信側/リダイレクト番号が送信されることを確認してください。

QSIG 非対応トランクの場合、元の着信側またはリダイレクト番号の転送は以下の方法で有効にできます。

- MGCP ゲートウェイ、H.323 ゲートウェイ、および H.323 トランクで着信および発信の [番号 IE 配信のリダイレクト（Redirecting Number IE Delivery）] を有効にします
- SIP トランクで着信および発信の [Diversion ヘッダー配信のリダイレクト（Redirecting Diversion Header Delivery）] を有効にします。

QSIG 対応 SIP、MGCP および H323 トランクの場合、元の着信側番号は、QSIG 転送元レッグ情報 APDU で送信されます。QSIG 対応トランクを介して QSIG APDU で送信される転送情報は、発信側の変更をピックアップせず、ボイス メール ボックスのマスク設定にも対応しません。Unified CM により送信された QSIG 転送情報は、変換の適用なしでリダイレクト元の DN に常に送信されます。

リダイレクト元 DN が +E.164 として設定されている場合は、先頭の「+」が削除され、QSIG 転送情報は「+」文字を含まない E.164 番号のみを保持します。

すべての QSIG トランク タイプの考慮事項

UC ネットワークでの QSIG の使用は、得られる機能のメリットが少ないため、通常は推奨されていません。QSIG を使用する主な理由は、コールバック機能を提供することです。(代替として、Collaboration ユーザは、Cisco IM and Presence サービスによって提供されるプレゼンス情報を使用して、他のユーザの状態を追跡できます)。リーフ UC システムから SME へのトランクで QSIG を有効にする場合は、すべてのクラスタ間トランクでも QSIG を有効にする必要があります。これによって、電話ユーザがコール バックが一部の(QSIG 対応の)着信側ユーザには機能しているがその他のユーザには機能していないことに気づくといった、低品質のエンド ユーザ エクスペリエンスが回避されます。

QSIG トンネリングが有効になっている H.323、MGCP、および SIP トランクでは、発信側、着信側、およびリダイレクト元の番号情報を含むすべての番号情報が、外部の H.323 メッセージや SIP ヘッダーからではなく、常にカプセル化された QSIG メッセージから取得されます。この QSIG トランクの動作には、SME に集中化され、複数のリーフ システムにサービス提供するボイスメール システムに特別な設計上の考慮が必要となる場合があります。

一般的な推奨事項として、円滑なエンドツーエンドの QSIG 実装を可能にするためには、すべての UC システムにわたって統一された、グローバルに一意なダイヤル プランが実装される必要があります。

QSIG トランクが使用されている場合、集中型ボイスメール システムに送信される前にリダイレクト番号を正規化することはできません。この制限により、各リーフ UC システムのユーザ用の集中型ボイスメール システム メールボックス番号は、各リーフ システムで使用される電話番号の番号形式に対応している必要があります。次に例を示します。

- E.164 形式の電話番号を持つユーザには、同じ E.164 形式を使用した、対応するボイスメール システム メールボックス番号を設定する必要があります。
- +E164 形式の電話番号を持つユーザには、同じ E.164 形式を使用した、対応するボイスメール システム メールボックス番号と、+E.164 形式を使用した代替のボイス メールボックス番号を設定する必要があります。

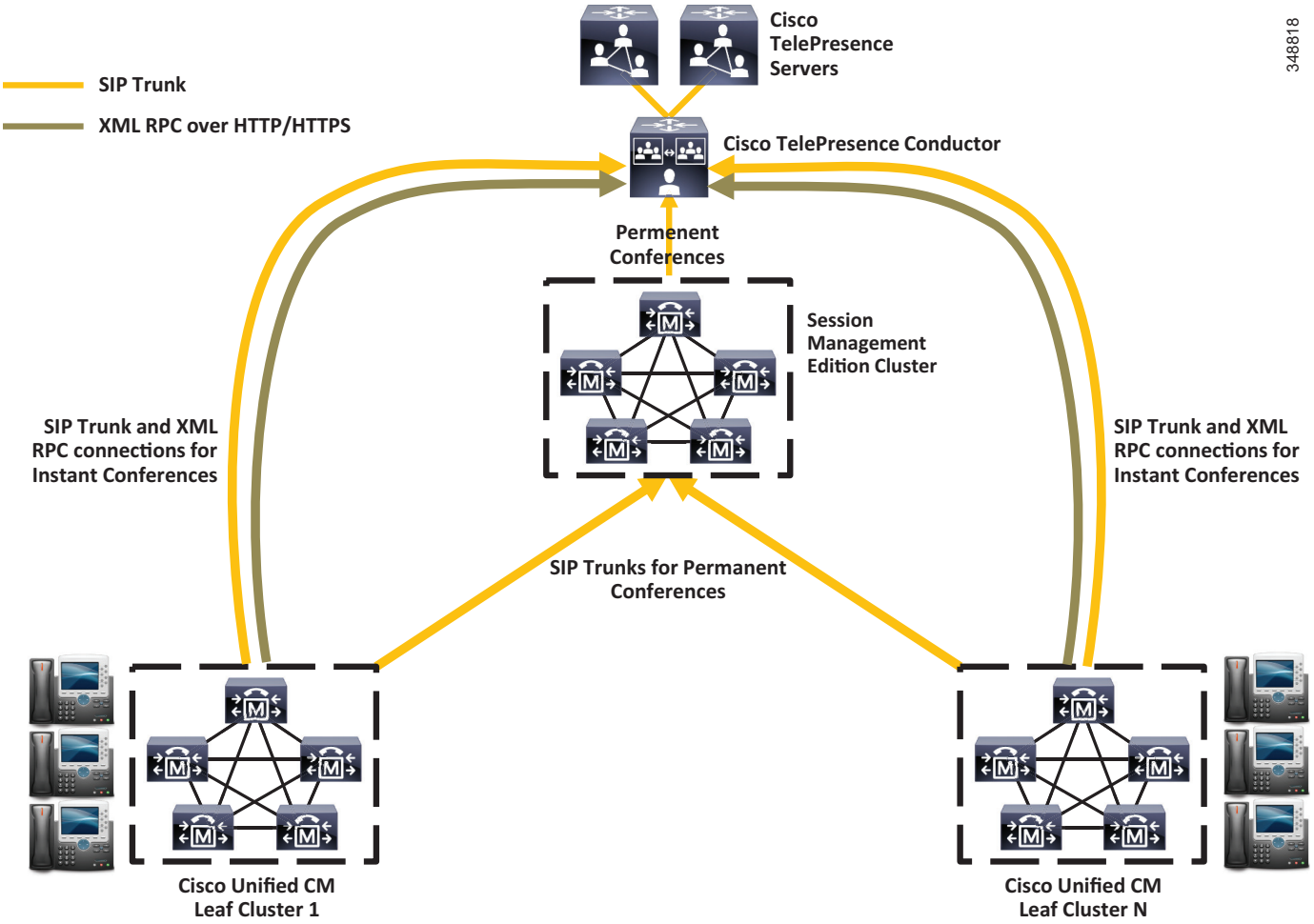
TelePresence Server および TelePresence Conductor

会議システムは、Session Management Edition クラスタに接続できます。Cisco TelePresence Conductor および TelePresence Server を使用した導入では、SIP トランクのシグナリング接続を超える追加のシグナリング接続がインスタント会議に必要なことに留意してください。会議リソースに到達するためにルート パターンと SIP トランクを使用する相手先固定会議とは異なり、Unified CM は、インスタンス会議をメディア リソースとして定義し、HTTP/HTTPS 経由の XML RPC を使用して、電話ユーザが「会議」ボタンを押したときにインスタント会議を作成するように TelePresence Conductor または TelePresence Server に指示します。インスタント会議では、HTTP/HTTPS XML RPC メッセージおよび SIP INVITE メッセージは、同じ送信元 IP アドレスから発信される必要があるので、インスタント会議接続(HTTP XML RPC および SIP トランク)は、SME クラスタではなくリーフ Unified CM クラスタで設定する必要があります。TelePresence Conductor および TelePresence Server は、SME と引き続き同じ場所に配置できますが、相手先固定会議のみが SME クラスタから直接接続された SIP トランク接続を使用でき、インスタント会議 SIP トランクおよび HTTP XML RPC 接続は、リーフ Unified CM クラスタから直接接続される必要があります。(図 6-25 を参照)。

詳細については、次の URL から入手できる最新バージョンの『*Cisco TelePresence Conductor with Unified CM Deployment Guide*』を参照してください。

https://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html

図 6-25　集中型 TelePresence Server および TelePresence Conductor



Expressway-C および Expressway-E

Cisco Expressway プラットフォームは、Session Management Edition クラスタに接続できます（図 6-26 を参照）。導入タイプによって、Expressway-C は SME への接続に SIP トランクを使用できる場合とできない場合があります。

- モバイル & リモート アクセス

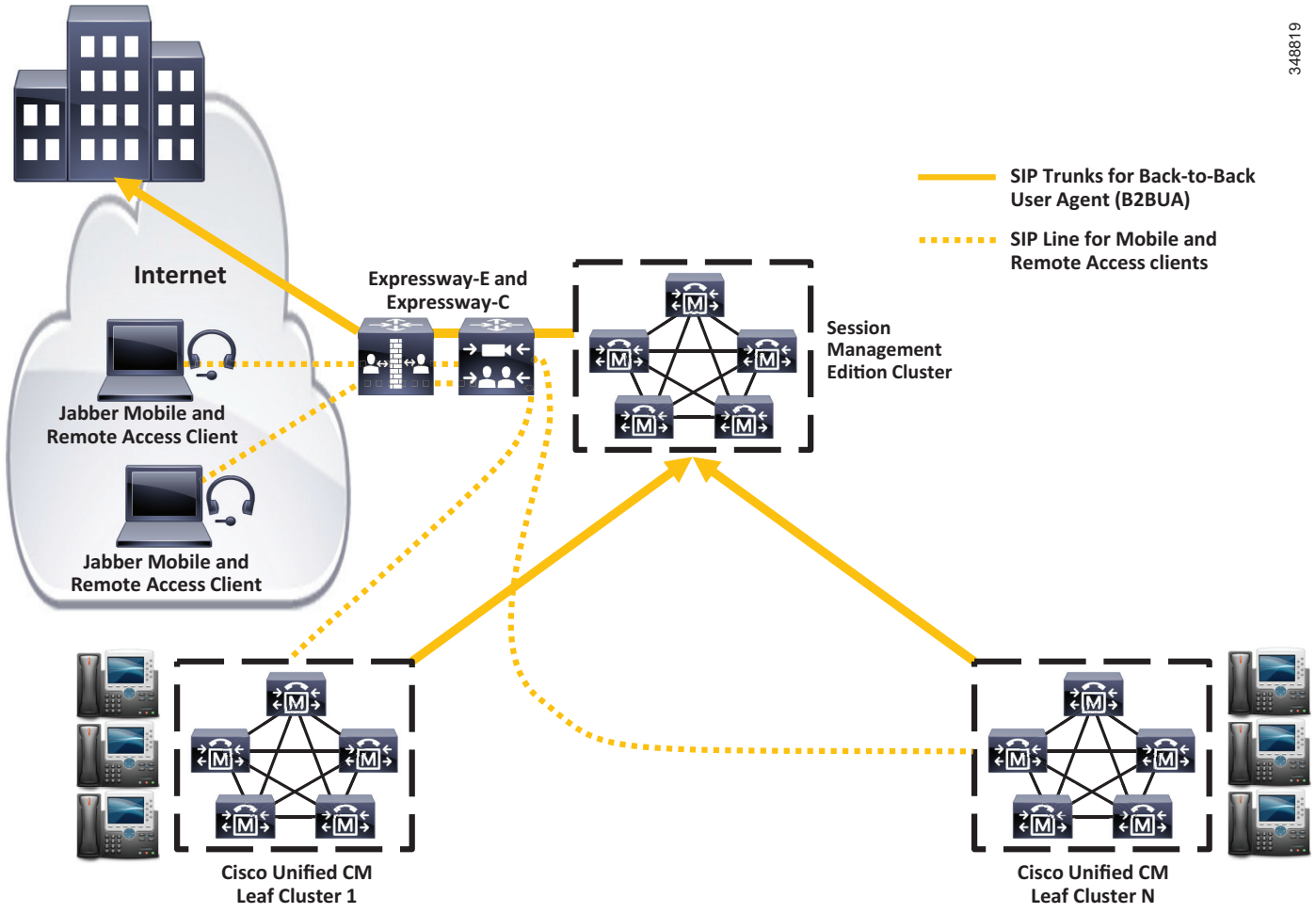
  企業の UC ネットワークへの接続にモバイルおよびリモート アクセス機能を使用しているデバイスは、SME クラスタへの SIP 接続を確立しません。そのデバイスは、UDS を使用して、ホーム クラスタを検出して直接登録します。UDS ホーム クラスタ ルックアップ要求の受信に SME が使用されている場合は、ホーム クラスタの検出のために他の Unified CM クラスタと通信するために ILS サービスを使用する必要もあります。詳細については、次の URL から入手できる最新バージョンの『*Mobile and Remote Access via Cisco Expressway Deployment Guide*』を参照してください。

  https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

- トランキングされた Expressway アプリケーション

  Business-to-Business（B2B）Collaboration などの Expressway アプリケーションの場合、Expressway は SME クラスタへの直接 SIP トランク接続を使用します。

図 6-26　　集中型 Expressway-C と Expressway-E



マルチクラスタ SME 配置の SIP トランクの推奨事項の概要

ここでは、SIP トランクの推奨事項、および Unified CM Session Management Edition を使用したマルチ クラスタ配置の動作に関する概要を示します。

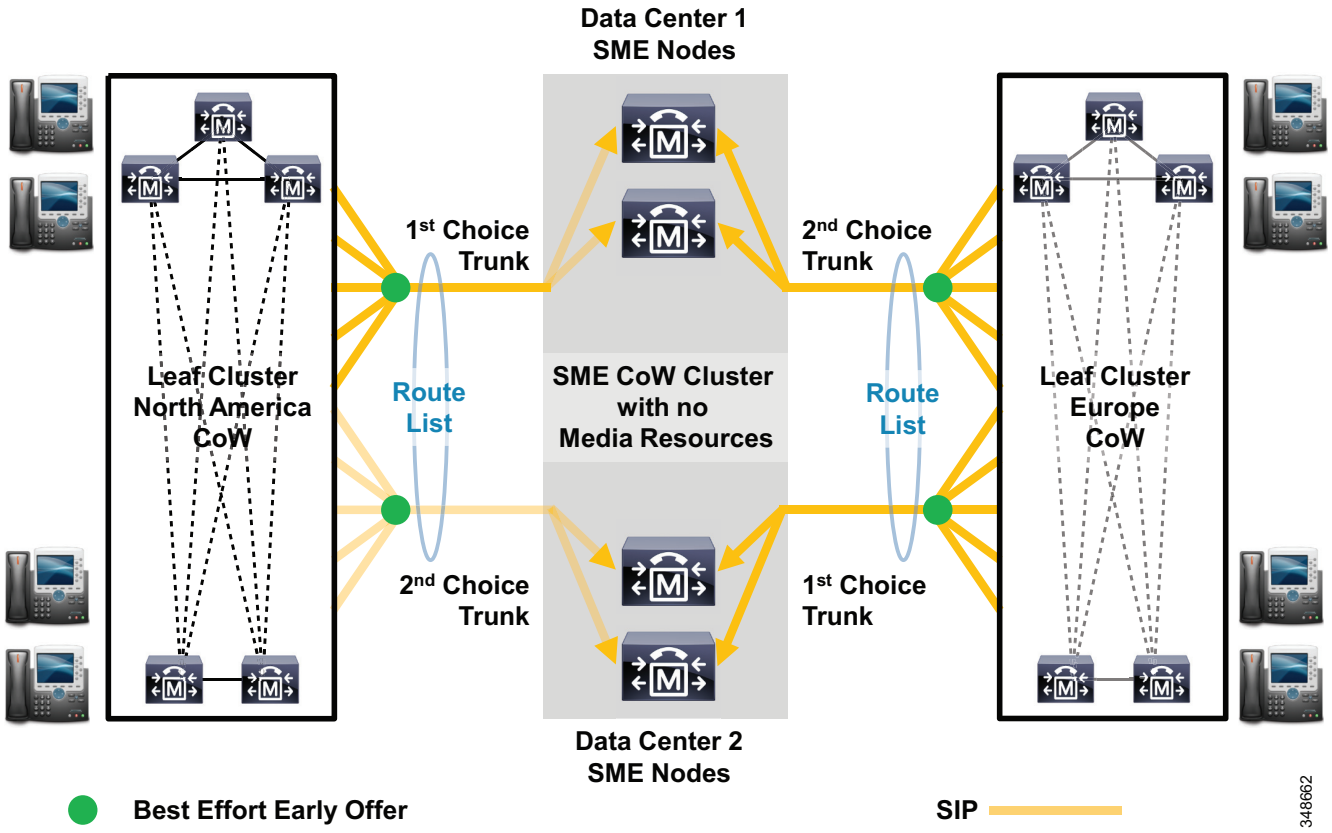
Unified CM リーフ クラスタの推奨事項:

- 各地域データセンターの SME ノードのセットごとに 1 つの SIP トランクを設定する。たとえば、4 つの地域 SME データセンターがある場合、各リーフ クラスタに 4 つの SIP トランクを作成します（図 6-27 を参照）。これにより、すべての SME ノードからのコールがリーフ クラスタによって受信され、受け入れられるようになります。これらのすべてのトランクで [すべての Unified CM ノードで実行（Run on all Unified CM nodes）] をオンにします。
- SME CoW+ クラスタへのパスの冗長性のために、ルート リストおよびルート グループにこのようなリーフ クラスタの SIP トランクを 2 つ以上置く。
- [ベスト エフォートのアーリー オファー（Best Effort Early Offer）] がすべてのリーフ クラスタ SIP トランクに推奨されます。

  Unified Communications の展開では、Cisco Unified Communications 以外のアプリケーションとサービスで、アーリー オファーのみの受信が必要な場合があります。リーフ クラスタの場合は、アーリー オファーが常に受信される要件に対応するオプションが 2 つあります。

  - Cisco Unified Border Element では、SIP ディレイド オファーからアーリー オファーへの変換機能を音声コールに対して提供します。着信ディレイド オファーのコールが発信アーリー オファーのコールに変換されるので、Unified CM および SME で、[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] のトランクを使用できるようになります。この使用例で代表的と言えるのは、通常は SIP アーリー オファーを常に受信する必要がある、Cisco Unified Border Element 経由のサービス プロバイダーの IP PSTN 接続の場合です。
  - SIP アーリー オファーのみを受け入れる企業の Unified Communications アプリケーションの場合、専用のアーリー オファー SIP トランクを Unified CM リーフ クラスタから Unified Communications アプリケーションに使用できます。多数の MTP がアーリー オファー SIP トランクで必要な場合は、Cisco Unified Border Element のディレイド オファーからアーリー オファーへの変換機能を代わりに使用することを検討してください。
- すべてのリーフ クラスタ ノードで IPVMS サービスを有効にする。必要に応じて、会議、保留音、およびアナンシエータ リソースをアクティブにします。（IPVMS ベースの MTP を非アクティブにすることが推奨されます）。
- 必要に応じて、リーフ クラスタに Cisco IOS メディア リソース（MTP、会議、およびトランスコーディング）を設定して、関連付ける。
- SIP トランク DTMF 設定を [初期設定なし（No Preference）]（デフォルト設定）に設定する。
- SIP OPTIONS ping および PRACK を有効にする。
- 必要に応じて、コーデックのプリファレンス リストを設定し、適用する。

図 6-27　　CoW リーフ クラスタ トランクに対する推奨トランク設定



Session Management Edition クラスタの推奨事項:

- SME クラスタで SIP トランクのみを使用する。
- SME クラスタから各リーフ クラスタに 1 つの SIP トランクを設定する（図 6-28 を参照）。これらのトランクで [すべての Unified CM ノードで実行（Run on all Unified CM Nodes）] をオンにし、リーフ クラスタ内のすべてのコール処理ノードにトランク宛先を設定する。
- [ベスト エフォートのアーリー オファー（Best Effort Early Offer）] がすべての SME クラスタ SIP トランクに推奨されます。

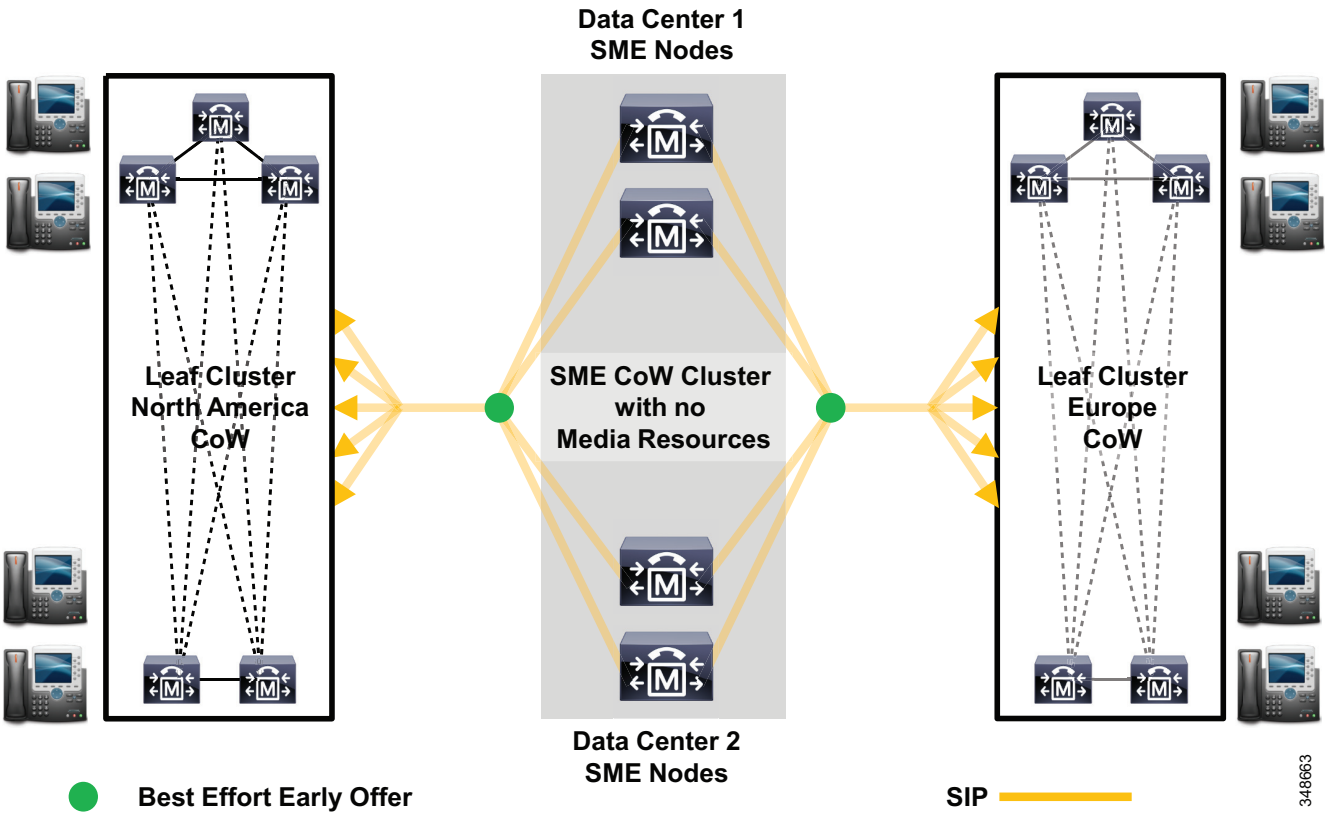
  アーリー オファーのみの受信が SME クラスタに接続されている Cisco Unified Communications 以外のアプリケーションとサービスで必要な場合、この要件に対応するオプションが 2 つあります。

  - Cisco Unified Border Element では、SIP ディレイド オファーからアーリー オファーへの変換機能を音声コールに対して提供します。着信ディレイド オファーのコールが発信アーリー オファーのコールに変換されるので、Unified CM および SME で、[ベスト エフォートのアーリー オファー（Best Effort Early Offer）] のトランクのみを使用できるようになります。この使用例で代表的と言えるのは、通常は SIP アーリー オファーを常に受信する必要がある、Cisco Unified Border Element 経由のサービス プロバイダーの IP PSTN 接続の場合です。

  - SIP アーリー オファーのみを受け入れる企業の Unified Communications アプリケーションで、専用のアーリー オファー SIP トランクが SME クラスタから Unified Communications アプリケーションに使用されている場合、メディア リソースは SME トランクに関連付けられる必要があり、それが使用されると、不要なメディアのヘアピニングの原因となります。通常このケースで使用されるメディア リソースは、アーリー オファーの作成または DTMF 不一致に対応するための MTP、またはコーデックの不一致に対応するためのトランスコーダです。SME クラスタでメディア リソースを使用することは一般に推奨されません。代わりに、SME と Unified Communications アプリケーション間で Cisco Unified Border Element のディレイド オファーからアーリー オファーへの機能を使用することを検討するか、またはリーフ クラスタからアプリケーションへの直接トランクを使用します。

- すべての SME ノードの IPVMS サービスを無効にする。これにより、Unified CM メディア ターミネーション ポイント、会議、保留音、およびアナンシエータ リソースが無効になります。
- SME クラスタと Cisco IOS メディア リソースを関連付けしない。
- SIP トランク DTMF 設定を [初期設定なし（No Preference）]（デフォルト設定）に設定する。
- すべての SME SIP トランクで [受信オファーのオーディオ コーデック初期設定を承認（Accept Audio Codec Preference in Received Offer）] をオンにする。
- SIP OPTIONS ping および PRACK を有効にする。

図 6-28　CoW+ SME クラスタ トランクに対する推奨トランク設定



リーフおよび SME クラスタを介したコール ルーティングの推奨事項:

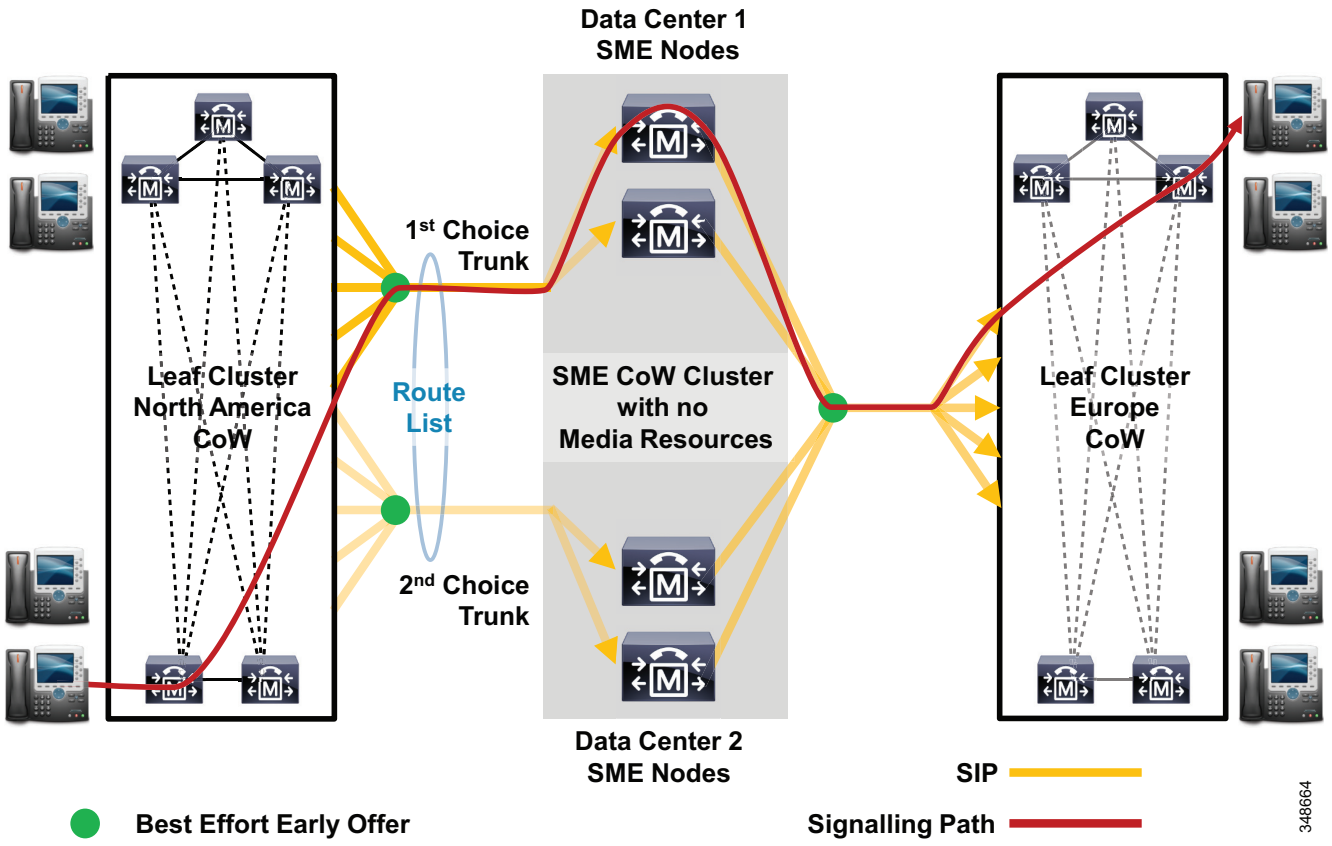
発信リーフ クラスタは、発信デバイスが登録されている同じノードから SIP トランク コールを発信します(ルート ローカル ルールを使用)。リーフ クラスタは、SIP トランクのルート リストから宛先アドレスをランダムに選択します。(図 6-29 の例では、第一希望のトランクが選択されます)。

SME クラスタからの発信コールは、着信コールが到達した同じノードから発信されます(ルート ローカル ルールを使用)。すべての SME トランク上で [すべての Unified CM ノードで実行(Run on all Unified CM nodes)] がオンにされている場合、SME クラスタ内のコール処理ノード間でコールがセットアップされることはありません。SME クラスタは、宛先リーフ クラスタを指す SIP トランクの宛先アドレスをランダムに選択します。

宛先リーフ クラスタへの着信 SIP トランク コールの場合、着信コールが到達したコール処理ノードから、着信側デバイスが登録されているノードに、コールが拡張される場合があります。

必要に応じて、メディア リソースは、リーフ クラスタ(またはエンド Unified Communications システム)によって挿入されます。発信側リーフ クラスタの SIP トランクのデバイスがディレイド オファーを使用する場合、メディアの決定は、このクラスタによって行われます。必要に応じて、メディア リソース(MTP およびトランスコーダ、またはどちらか一方)を挿入します。発信側リーフ クラスタの SIP トランクのデバイスがアーリー オファーを送信する場合、メディアの決定は、宛先リーフ クラスタによって行われます。必要に応じて、メディア リソース(MTP およびトランスコーダ、またはどちらか一方)を挿入します。

図 6-29　　リーフおよび SME クラスタを介したコール ルーティングで推奨されるトランクの設定



Unified CM SIP トランクのマイナー機能

ここでは、Unified CM SIP トランクで使用可能な複数のマイナー機能の機能と用途を説明します。

[通話中 INVITE で sendrecv を送信（Send sendrecv in Mid-Call INVITE）]

この機能は、サードパーティ製品との相互運用性の問題を処理するために使用されます。Unified CM が SIP トランクを介してコールを保留に置く場合、SDP 本文の音声方向のメディア属性 a=inactive で通話中の INVITE を送信して、メディア接続を切断します。コールの再開では、SDP オファーでメディア特性を取得するために、Unified CM は保留デバイスにディレイド オファー INVITE（SDP なし）を送信します。RFC 3261（セクション 14.2）に応じて、保留デバイスは、新しいコールを発信したかのように（つまり、サポート対象のすべてのコーデックと a=sendrecv のリストで）オファーを構築する必要があります。一部のサードパーティ製品は、コールが常に非アクティブ状態で、メディアを再開できない結果に応じて、最後に使用されたコーデックとメディア方向属性のみで応答します。[通話中 INVITE で sendrecv を送信（Send "sendrecv" in mid call INVITE）] が有効な場合、この機能では、発信側デバイス間のメディア パスに MTP を挿入することにより、a=sendrecv により MTP と保留デバイス間のメディアを確立し、維持しながら、Unified CM デバイスと MTP 間でメディア接続を切断することができるようになります。コールの再開中、MTP がメディア パスから削除されます。この機能は、音声方向の通話中のディレイド オファー INVITE 問題に対処しますが、サポートされているすべてのコーデックの詳細なリストではなく、最後に使用されたコーデックを使用して応答するデバイスの問題を解決できません。この問題は、G.729 コールを保留中にし、G711 が望まれる保留音ソースに接続するなどのメディアの再構築でコーデックの変更が必要な場合は、問題になる可能性があります。

通話中のメディア交換で SDP 非アクティブを必要とする

SIP では、メディア接続を中断することなく、通話中のコーデックの更新や、IP アドレス、UDP ポート番号などの接続情報の更新を処理できます。一部のサードパーティ製デバイスはこの方法を使用してメディア変更を受け入れることができないので、正常にメディア パスを閉じてから、再び開いてメディア変更を行う必要があります。この機能が有効な場合、通話中のコーデックまたは接続の更新中に、Cisco Unified CM が INVITE a=inactive SDP メッセージをエンドポイントに送信して、メディア交換を中断させます。

（注） アーリー オファー対応の SIP トランクの場合、このパラメータは [通話中 INVITE で送受信 SDP を送信（Send send-receive SDP in mid-call INVITE）] パラメータによって上書きされます。

[180 で早期メディアを無効化（Disable Early Media on 180）]

デフォルトでは、SDP が 180 Ringing または 183 Session Progress Response で受信されなかった場合、Cisco Unified CM は、ローカル リングバックを再生するように、登録された発信側電話機に通知します。

180 または 183 Response に SDP が含まれる場合、リングバックをローカルで再生する代わりに、Cisco Unified CM ではメディアを接続し、発信側電話機がメディア ストリームで送信しているもの（リングバックまたはビジー信号）をすべて着信側電話機で再生します。

リングバックが受信されない場合、接続しているデバイスが 180 Response に SDP を含んでいる可能性がありますが、200 OK 応答の前にメディアを送信していません。この場合、このチェックボックスをオンにして、発信側の電話機でローカル リングバックを再生し、200 OK 応答の受信時にメディアを接続します。

アプリケーションによるリダイレクト（Redirect by Application）

オンにした場合、アプリケーションによるリダイレクト機能により、Unified CM は次の内容を実行できます。

- リダイレクトされたコンタクトが 3xx 応答で受信された場合に、特定のコーリング サーチスペースを適用します。
- リダイレクトされたコンタクトに対して番号分析を適用し、コールが正しくルーティングされていることを確認する。
- リダイレクション（再帰リダイレクション）要求の数を制限することによって、DOS 攻撃を防止する。
- リダイレクションの実行中にその他の機能を起動できるようにします。

[アプリケーションによるリダイレク（Redirect by Application）] チェックボックスがオフの場合、発信 SIP トランク コールを制限付きの電話番号（国際電話など）にリダイレクトできます。これは、リダイレクトが SIP スタック レベルで処理およびルーティングされ、Unified CM の番号解析とサービス クラスによる介入がないためです。

新しいトランクへの着信要求の再ルーティング

発信側デバイスの送信元 IP アドレスとポート番号が、設定された SIP トランクの宛先 IP アドレスとポート番号に一致する場合にだけ、Unified CM への着信 SIP トランク コールが受け入れられます。コールが受け入れられると、受信した SIP メッセージ ヘッダーに含まれる情報に基づいて、別の Unified CM SIP トランクに任意で再ルーティングできます。

デフォルトでは、IP アドレスとポート番号に基づいて SIP トランクが照合されると、コールは再ルーティングされることはありません。

任意で、次の内容の受信に基づいて新しいトランクに着信要求を再ルーティングできます。

- Contact ヘッダー

  コールは、Contact ヘッダーで受信された IP アドレスとポート番号に基づいて別の SIP トランクに再ルーティングされます。この機能は、通常、SIP プロキシから特定のエンド ユーザまたはシステムに割り当てられている Unified CM SIP トランクにコールを再ルーティングするために使用されます。

- [purpose=x-cisco-origIP のコール情報ヘッダー（Call-Info Header with purpose=x-cisco-origIP）]

  このオプションは、Cisco Unified Customer Voice Portal（CVP）からの着信コールを、コール情報ヘッダーのパラメータ purpose=x-cisco-origIP に含まれる IP アドレスとポート番号に基づいた特定のトランクに照合するために使用されます。この機能は、コール アドミッション制御に対して Unified CVP からのコールを Unified CM トランクにマッピングするために通常使用されます。

発信トランク コールでの発信者 ID 番号および発信者名の上書き

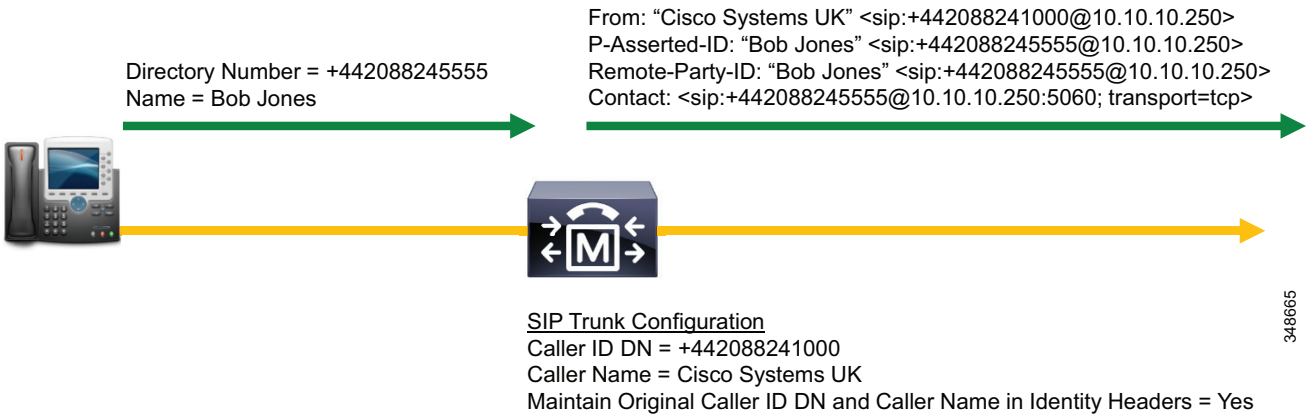
この機能はたとえば、SIP トランクで送信されるコールの SIP メッセージの発信者の番号と名前ではなく、企業のスイッチボードの番号と企業名を送信する場合に、実用的です（図 6-30 を参照）。この機能は、デバイス レベル（集中型 SIP トランクを使用した支社の場合）またはトランク レベルに適用できます。

デバイス レベルでは、デバイスに関連付けられている SIP プロファイルの [URI からの着信要求の設定（Incoming Requests FROM URI Setting）] セクションの [発信者 ID DN（Caller ID DN）] および [発信者名（Caller Name）] フィールドを使用します。

トランク レベルでは、トランク設定ページの [発信コール：発信者情報（Outbound Calls - Caller Information）] セクションの [発信者 ID DN（Caller ID DN）] および [発信者名（Caller Name）] フィールドを使用します。

デフォルトでは、From ヘッダー、Contact ヘッダー、および P-Asserted-Identity ヘッダー、および Remote-Party-ID ヘッダーで送信される [発信者 ID DN（Caller ID DN）] と [発信者名（Caller Name）] は、発信 SIP トランク コールで変更されます。P-Asserted-Identity および Remote-Party-ID ヘッダーの元の発信者 ID を保持したい場合は、トランク設定ページで [元の発信者 ID DN と発信者名を ID ヘッダーに維持する（Maintain Original Caller ID DN and Caller Name in Identity Headers）] チェックボックスをオンにします。このチェックボックスをオンにすると、コールの発信者を追跡することができます。

図 6-30　　発信 SIP トランク コールでの発信者 ID の番号および発信者名の上書き



SIP トランク メッセージの正規化および透過性

正規化および透過性は、SIP トランクに強力なスクリプトベースの機能を提供します。この機能を使用すると、Unified CM を通過するときに SIP メッセージおよびメッセージ ボディ（SDP）の内容を透過的に転送または変更できます。正規化および透過性のスクリプトは、SIP の相互運用性の問題に対処するように設計されているため、Unified CM は SIP ベースのサードパーティ PBX、アプリケーション、および IP PSTN サービスと相互運用できます。

SIP トランクの正規化

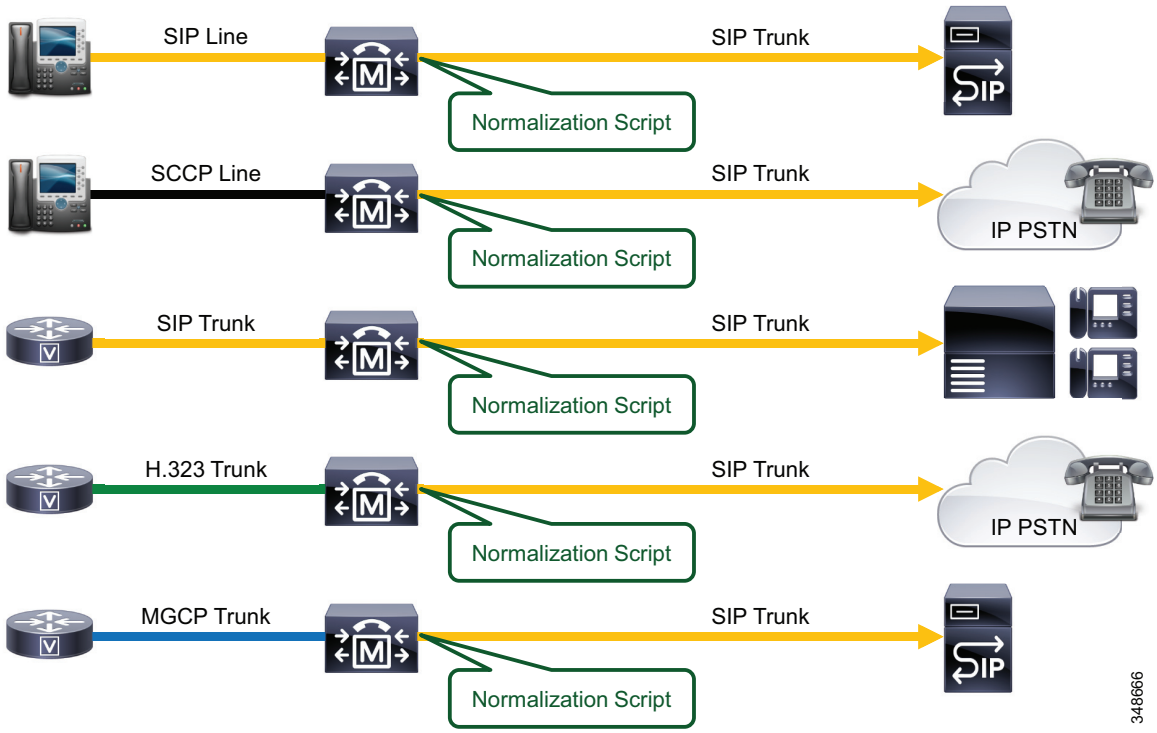
正規化によって、Unified CM を通過するときに着信および発信 SIP メッセージを変更できます。たとえば、Unified CM では、リダイレクト番号情報を伝達するための Diversion ヘッダーがサポートされます。Unified CM に接続される一部の SIP デバイスでは、この目的で History-Info ヘッダーが使用されます。着信の正規化スクリプトは、Cisco Unified CM でリダイレクト情報が認識されるように、History-Info ヘッダーを Diversion ヘッダーに変換するために使用できます。同様に、発信の正規化スクリプトは、外部 SIP デバイスでリダイレクト情報が認識されるように、Diversion ヘッダーを History-Info ヘッダーに変換するために使用できます。

正規化スクリプトは、SIP トランクまたは SIP 回線に関連付けられています。スクリプトは、発着信 SIP メッセージで動作するメッセージ ハンドラのセットとして示されます。正規化では、スクリプトによって、次のものを含む SIP メッセージのほとんどの状態が操作されます。

- 要求 URI
- 応答コードとフレーズ
- SIP ヘッダー
- SIP パラメータ
- コンテンツ本文
- SDP

正規化は、コールに関係する他のエンドポイントで使用されるプロトコルに関係なく、スクリプトが関連付けられた SIP トランクを通過するすべてのコールに適用されます。たとえば、SIP トランクの正規化スクリプトは、SIP ライン デバイスから SIP トランクに対するコール、SCCP デバイスから SIP トランクに対するコール、MGCP トランクから SIP トランクに対するコール、H.323 トランクから SIP トランクに対するコールなどで実行できます（図 6-31 を参照）。

図 6-31　SIP トランクの正規化



SIP トランクの透過性

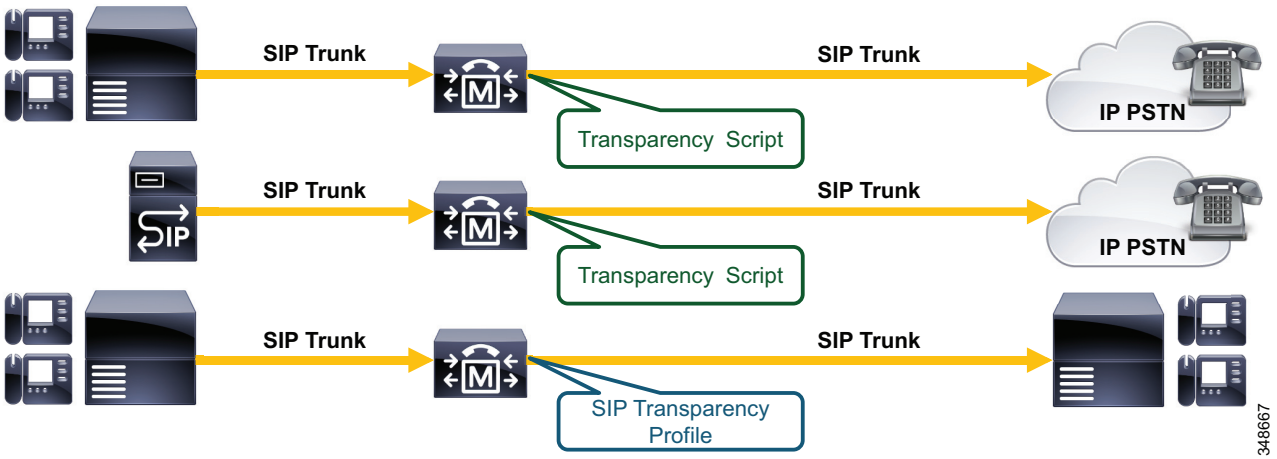
通過するメッセージの部分を Unified CM が理解またはサポートしていない場合でも、透過性 Lua スクリプトによって、Unified CM は SIP ヘッダー、パラメータ、メッセージ ボディの内容を SIP トランク コール レッグから別の宛先に渡すことができます。透過性（または透過的なパススルー）は、Unified CM を介した SIP 間のコールでのみ適用されます。（図 6-32 を参照）。

透過性スクリプトは、SIP トランクまたは SIP 回線に関連付けられています。スクリプトは、発着信 SIP メッセージで動作するメッセージ ハンドラのセットとして示されます。透過性では、スクリプトによって、次のものを含む SIP メッセージのほとんどの情報が渡されます。

- SIP ヘッダー
- SIP パラメータ
- コンテンツ本文

SIP プロファイルは、SDP 透過性プロファイルもサポートしています。そのプロファイルは、すべての不明な SDP パラメータ（デフォルト）または Unified CM によってネイティブでサポートされていない選択された SDP パラメータを 1 つの SIP トランク（または SIP エンドポイント）から別のトランクに Lua 透過性スクリプトを使用せずに渡すために使用できます。

図 6-32　SIP トランクの透過性



正規化と透過性のスクリプトは、強力、高速、軽量、そして埋め込み可能なスクリプティング言語である Lua を使用して、SIP トランク上の SIP メッセージと SDP 本文の内容を変更します。（Lua の詳細については、https://lua-users.org/wiki/LuaOrgGuide で入手可能なマニュアルを参照してください）。

SIP トランクの正規化および透過性のスクリプトについて詳しくは、次のサイトで入手可能な最新バージョンの『*Developer Guide for SIP Transparency and Normalization*』を参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html

この開発者ガイドでは、SIP メッセージ情報を操作し、渡すために使用される、スクリプト環境および API について説明します。

スクリプト管理の詳細については、次のサイトで入手可能な最新バージョンの『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

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

プリロードされた Unified CM 正規化および透過性スクリプト

多数の正規化および透過性スクリプトが Unified CM にプリロードされており、次のスクリプトはそのうちの代表的な例です。

- Refer-passthrough スクリプト：このスクリプトを使用して、ブラインド転送（ダイアログ内参照使用）が 2 つの SIP トランク間で呼び出されたときに、Unified CM をコール シグナリング パスから削除できます。
- ContactHeader スクリプト：このスクリプトは、着信ディレイド オファーの通話中再参加内の Contact ヘッダーから音声とビデオの属性を削除します。
- HCS PCV PAI パススルー スクリプト：このスクリプトは、IP Multimedia Subsystem（IMS）ネットワークとの統合で使用され、INVITE、UPDATE、および 200 OK メッセージの P-Charging-Vector ヘッダーをパススルーまたは追加します。
- Diversion-Counter スクリプト：このスクリプトは、さまざまなコール転送シナリオ用に転送カウンタを調整する機能を提供します。
- VCS-interop スクリプト：このスクリプトは、Cisco TelePresence Video Communication Server（VCS）に登録されたエンドポイントの相互運用性を提供します。

サービス プロバイダー ネットワークへの IP PSTN および IP トランク

サービス プロバイダーは、企業の顧客に対して非 TDM PSTN 接続のサービスを増やしています。非 TDM インターフェイスを配置することで得られるコスト削減という重要なメリットのほかに、これらの IP ベース PSTN 接続では、従来の PSTN インターフェイスと比較して優れた音声機能も提供されます。

SIP のサービスは今日の使用可能なサービスの中で優位を占め、旧 H.323 サービスは特定の地域で使用できましたが、段階的に使用されなくなっています。これは、主にユニファイド コミュニケーションのベンダーおよび企業内で、SIP がプロトコルとして人気が高まったことによるものです。

サービス プロバイダーの IP PSTN ネットワークに接続する場合、エンタープライズ エッジ セッション ボーダー コントローラとして Cisco Unified Border Element を使用し、企業ネットワークとサービス プロバイダーのネットワーク間に制御された境界およびセキュリティ ポイントを用意することが強く推奨されます。

Cisco Unified Border Element

Cisco Unified Border Element は、次の機能とサービスを提供する Session Border Controller です。

- アドレスおよびポート トランスレーション（プライバシーおよびレベル 7 のトポロジ隠蔽）
- SIP ディレイド オファーからアーリー オファーへの変換
- プロトコルのインターワーキング（H.323 および SIP）および正規化
- メディアのインターワーキング（DTMF 変換、Fax、トランスコーディング、トランスレーティング、音量と制御取得）
- コール アドミッション制御（合計のコール、メモリ、コール到達のスパイク検出、または宛先あたりの最大コール数）

- セキュリティ（RTP と SRTP 間のインターワーキング、SIP の不正パケット検出、非ダイアログの RTP パケット ドロップ、SIP リスニング ポートの設定、ダイジェスト認証、同時コール数制限、コール レート制限、料金詐欺の防止、および複数のシグナリングとメディアの暗号化オプションなど）
- PPI/PAI/プライバシーおよび RPID：サービス プロバイダーとの ID ヘッダー インターワーキング
- QoS および帯域幅管理（ToS/DSCP を使用した QoS マーキング、および RSVP やコーデック フィルタリングによる帯域幅拡張）
- 複数のサービス プロバイダーからの SIP トランクに対する同時接続
- ボックス内またはボックス間のフェールオーバー オプションによるハイ アベイラビリティ（プラットフォームによって変わります）
- ダイヤル ピアに照合するために URI ルーティングによる GDPR ルート文字列の使用
- ドメインベースのルーティング
- マルチキャスト保留音からユニキャスト保留音
- 音声およびビデオ メディア フォーキング
- 企業の電話プロキシ：Unified CM から Cisco Unified Border Element への VPN-Less IP Phone の登録
- 請求の統計情報と CDR の収集

Cisco Unified Border Element は、Cisco ルータおよびゲートウェイ プラットフォームの広い範囲で使用できる認可を受けた Cisco IOS アプリケーションです。選択したハードウェア プラットフォームに応じて、Cisco Unified Border Element は、ボックス内またはボックス間のフェールオーバー オプションで、4 ～ 16,000 の同時音声コールについてセッション スケーラビリティを提供できます。

Cisco Unified Border Element の詳細については、次のサイトで入手可能なマニュアルを参照してください。

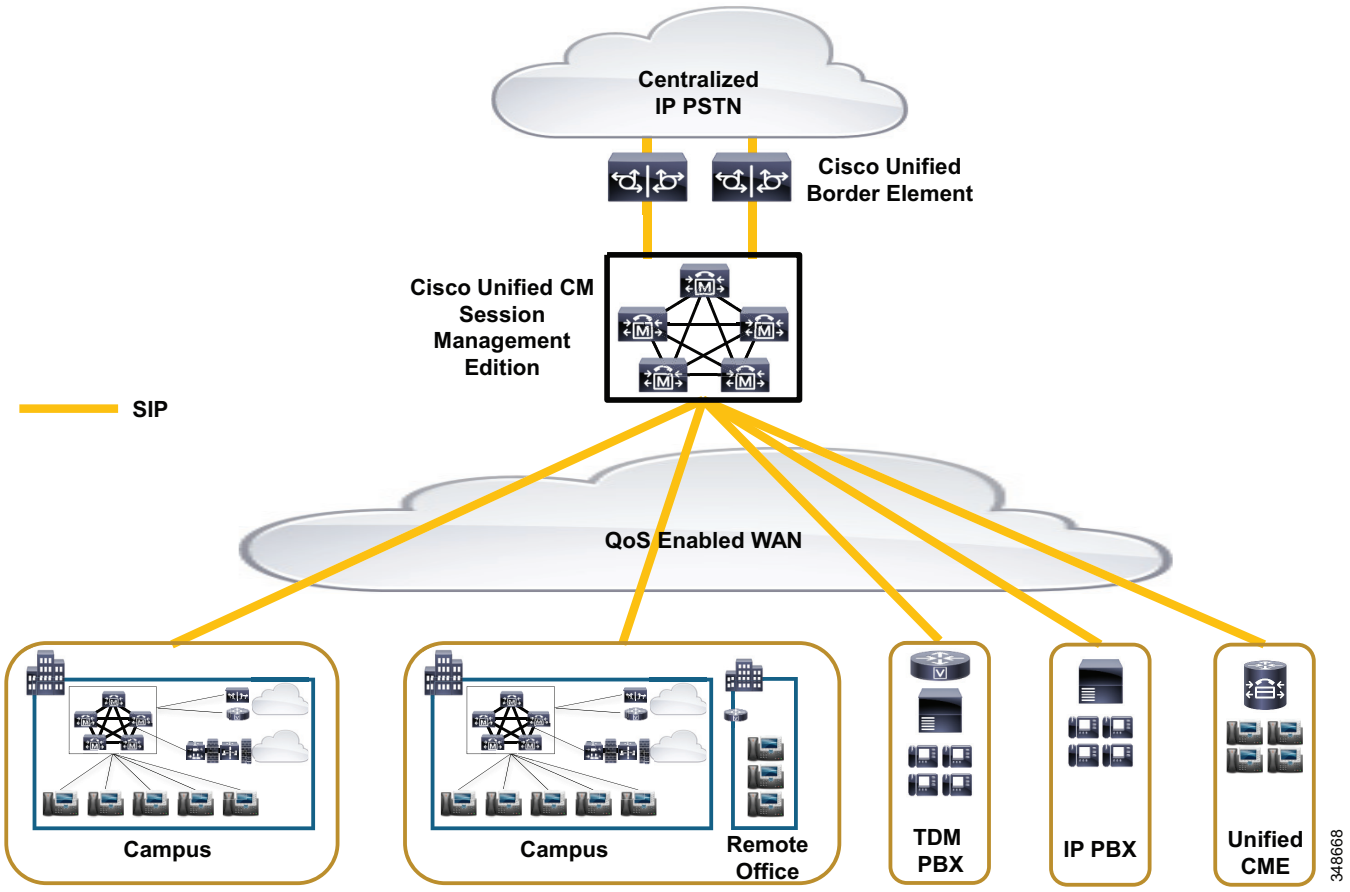
https://www.cisco.com/go/cube

IP-PSTN トランク接続モデル

トランクは、必要なアーキテクチャに応じて、さまざまな方法で IP PSTN サービス プロバイダーに接続されます。この接続における最も一般的なアーキテクチャには、中央集中型トランクと分散型トランクの 2 つがあります。

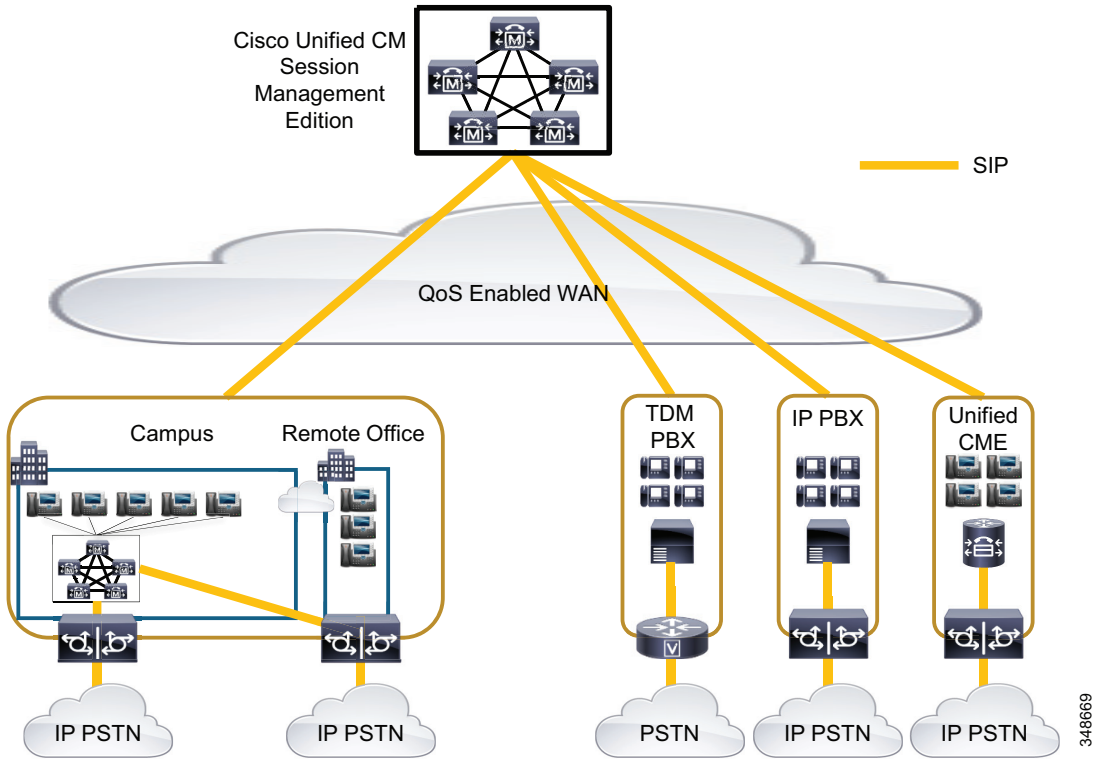
中央集中型トランクは、Cisco Unified Border Element などのセッション ボーダー コントローラ（SBC）を使用し、1 つの論理接続を通して企業ネットワークをサービス プロバイダーに接続します（ただし、冗長性を確保するために複数の物理接続が存在する場合があります）。（図 6-33 を参照）。IP PSTN へのすべてのコール、および IP PSTN からのすべてのコールでは、このトランクのセットが使用されます。集中型 IP PSTN 接続からのすべてのリモート サイトでは、PSTN コールのメディアおよびシグナリングは、企業 IP WAN を通過する必要があります。

図 6-33　　中央集中型または集約型 SIP トランク モデル



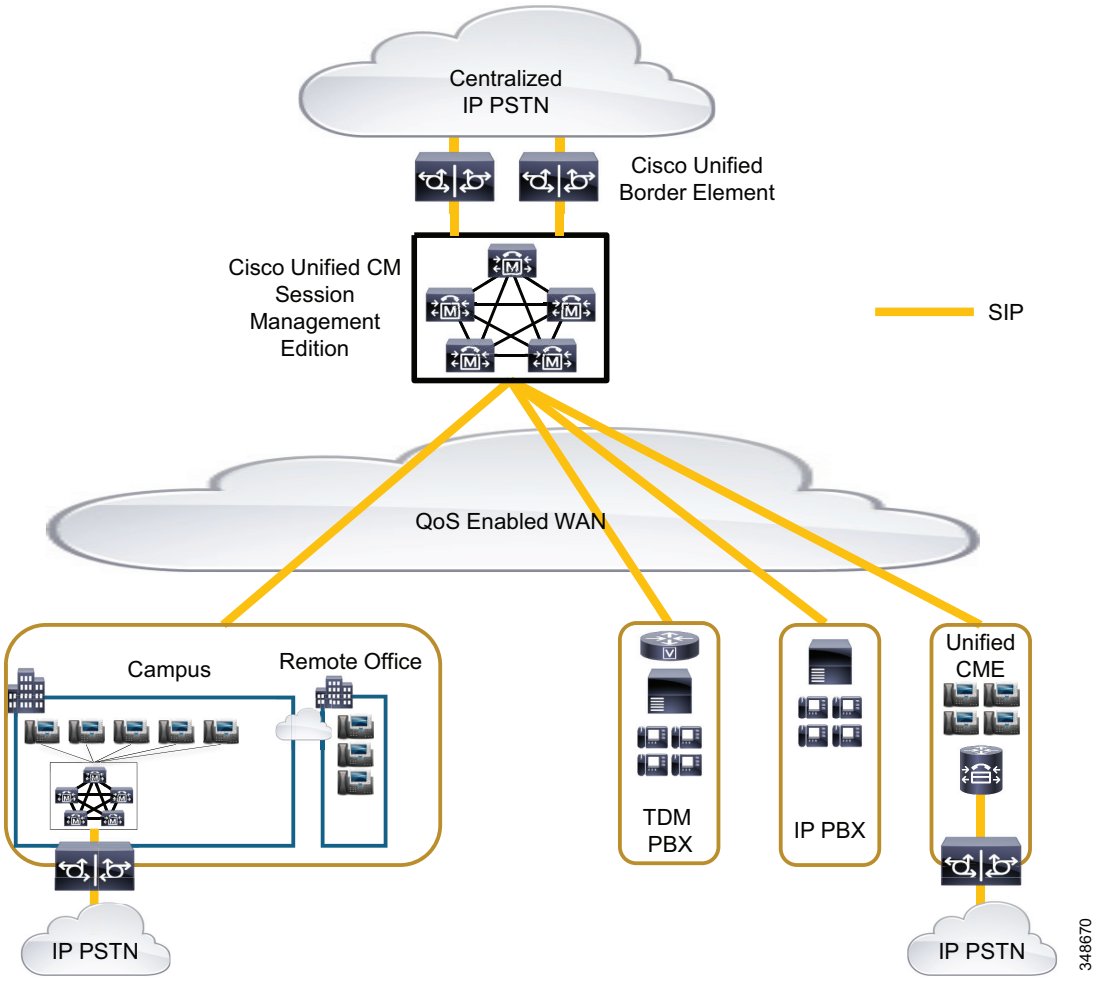
分散型トランクは、複数の地理的に分散された論理接続経由でサービス プロバイダーに接続します。（図 6-34 を参照）。会社の各支社は、サービス プロバイダーへの独自のローカル トランクを保有できます。各支社サイトで分散型トランクを使用する場合、メディアは企業 WAN を通過する必要はなくなりましたが、ローカル SBC 経由でサービス プロバイダー インターフェイスへと流れます。

図 6-34　　分散型 SIP トランク モデル



これらの接続モデルには、それぞれ利点と欠点があります。通常、中央集中型トランクは、物理的な機器および設定の複雑さの面でより容易に展開できますが、ディアおよびシグナリングは PSTN に到達するために企業を通過する必要があるので、企業 WAN でハイ アベイラビリティが必要になります。分散型トランクには、メディアをローカル ハンドオフできる利点があり、またローカル プロバイダーからの番号の可搬性が高まります。図 6-35 に示すように、いくつかの支社をグループ化して接続したり、マルチクラスタ配置で各 Unified CM クラスタからトランクを提供したりするハイブリッド接続モデルでは、両方の配置モデル形式の利点が実現されます。

図 6-35　　リージョンによる集約を行ったハイブリッド SIP トランク モデル



IP PSTN トランクと緊急サービス

IP トランクは、緊急 911 コールを送信できない場合があります。また、中央集中型 PSTN トランクのように、発信側のロケーションに適した Public Safety Answering Point（PSAP）に緊急 911 コールを送信できない場合があります。そのため、お客様は、緊急 911 コールおよび発信側のロケーションを適切な PSAP に送信できるかどうか、IP トランク サービス プロバイダーの機能を注意して調査する必要があります。Cisco Emergency Responder を使用すると、緊急 911 コールに対する、ロケーションに固有な発番号を IP トランク サービス プロバイダーに提供できる場合があります。

また、中央集中型 IP または PSTN トランクが、WAN 輻輳または障害のために、リモート ロケーションからの緊急 911 コールに一時的に応答できなくなることもあります。そのため、リモート ロケーションでは、常に、緊急 911 コールを送信できる PSTN へのローカル ゲートウェイを使用できなければなりません。詳細については、緊急サービス（15-1 ページ）の章を参照してください。

メディア リソース

改訂日：2018 年 3 月 1 日

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

この章では、Cisco Unified CM メディア リソース アーキテクチャおよび Cisco IP Voice Media Streaming Application サービスについての概要を説明し、さらに次のメディア リソースについて重点的に説明します。

- 音声インターフェイス（7-4 ページ）
- トランスコーディング（7-5 ページ）
- メディア ターミネーション ポイント（MTP）（7-7 ページ）
- Trusted Relay Point（7-17 ページ）
- Annunciator（7-17 ページ）
- Cisco RSVP Agent（7-19 ページ）
- 保留音（7-19 ページ）

この章を使用して、Unified CM で使用可能な各メディア リソース タイプの機能を理解し、配置に必要なリソースを確認してください。会議リソースの詳細については、Cisco Rich Media Conferencing（11-1 ページ）の章を参照してください。

Cisco Integrated Service Router（ISR）ゲートウェイの DSP サイジングを適切に行うために、有効なログイン アカウントを持つシスコの従業員およびシスコ パートナーは次のツールを使用できるようになっています。

- Cisco Collaboration Sizing Tool（https://cucst.cloudapps.cisco.com/landing から入手可能）
- DSP Calculator（https://www.cisco.com/c/en/us/applications/dsp-calc.html から入手可能）

メディア リソースのアーキテクチャ

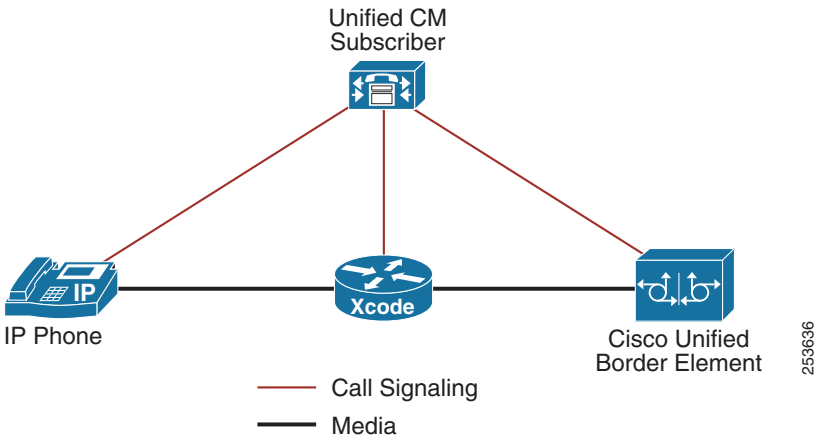
会社のメディア リソース割り当て方針を適切に策定するには、さまざまなメディア リソースコンポーネントの Cisco Unified CM アーキテクチャを理解しておくことが重要です。次の各項では、Unified CM を使用したメディア リソース設計の重要な特徴を中心に説明します。

メディア リソース マネージャ

Unified CM のソフトウェア コンポーネントであるメディア リソース マネージャ（MRM）は、メディア リソースの割り当ておよびメディア パスの挿入が必要であるかどうかを判別します。このメディア リソースは、Unified CM IP Voice Media Streaming Application サービスまたはデジタル シグナル プロセッサ（DSP）カードによって提供されます。MRM は、メディア リソースのタイプを判別および特定すると、当該デバイスに関連付けられているメディア リソース グループ リスト（MRGL）およびメディア リソース グループ（MRG）の構成の設定値に応じて、使用可能なリソース全体を検索します。MRGL および MRG は、割り当てを行うためにメディア リソースの関連するグループをまとめて保持する構成概念です。詳細については、メディア リソース グループとメディア リソース グループ リスト（7-37 ページ）の項を参照してください。

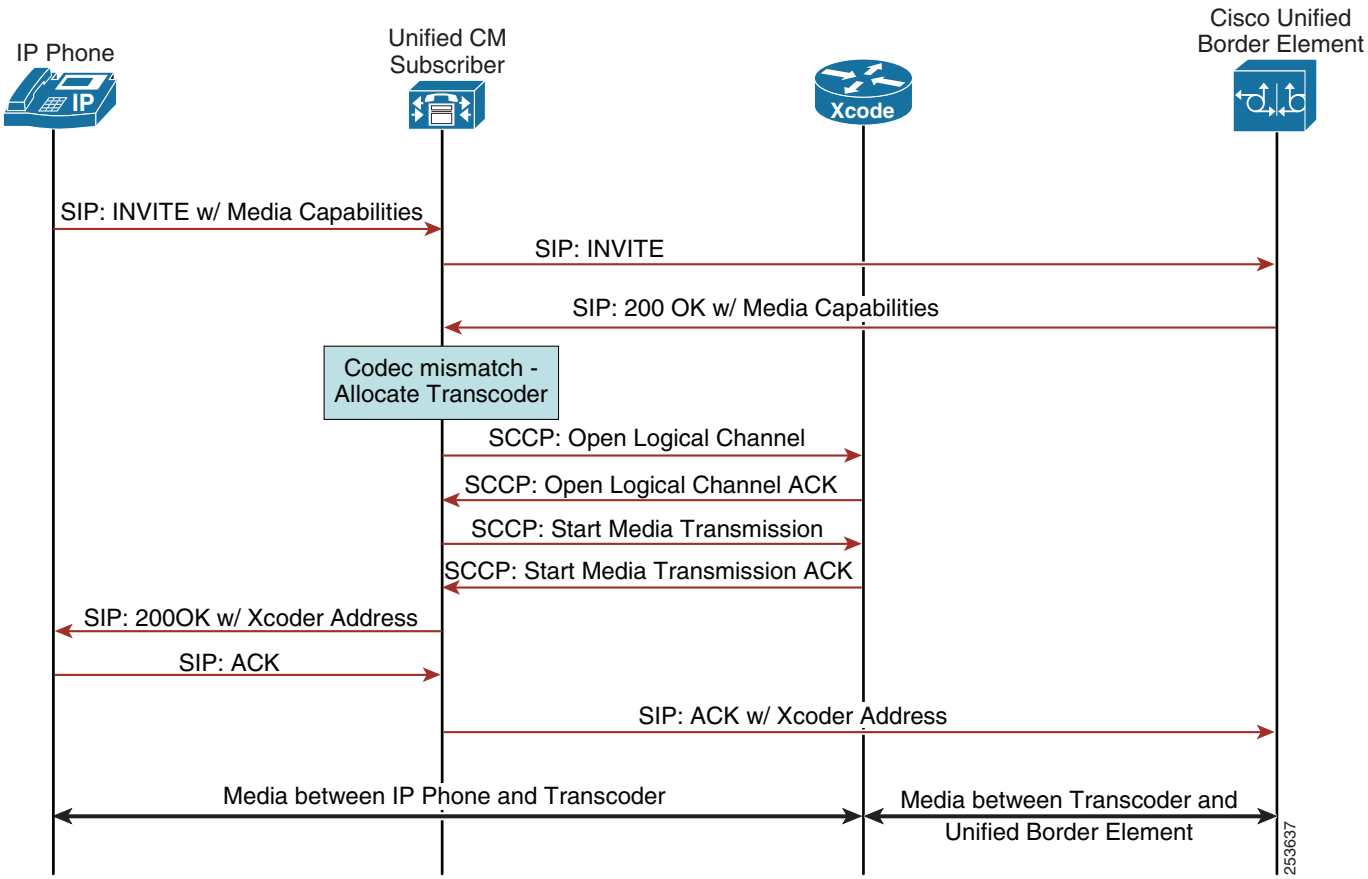
図 7-1 は、IP フォンと Cisco Unified Border Element 間で一般的なコーデックが使用できない場合に、トランスコーダなどのメディア リソースが、これらの間のメディア パスにどのように配置されるかを示しています。

図 7-1　　一般的なコーデックが使用できない場合のトランスコーダの使用



Unified CM は、Skinny Client Control Protocol（SCCP）を使用して、メディア リソースと通信します。このメッセージングは、Unified CM と通信エンティティ間で使用されている可能性のあるプロトコルに依存しません。図 7-2 にメッセージ フローの例を示します。ただし、この例は、エンティティ間で交換されるすべての SCCP メッセージおよび SIP メッセージを示しているわけではありません。

図 7-2　　コンポーネント間のメッセージ フロー



Cisco IP Voice Media Streaming Application

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

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

IP Voice Media Streaming Application をアクティブにすると、上記の各リソースが 1 つずつ自動的に設定されます。必要に応じて、会議、Annunciator、IVR、および MTP サービスを無効にできます。これらのリソースが不要な場合は、Unified CM 設定で適切なサービス パラメータを変更して無効にすることを推奨します。サービス パラメータには、各メディア サービスが処理できる最大接続数がデフォルトで設定されています。サービス パラメータの変更方法については、次の URL で入手可能な適切なバージョンの『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

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

複数のリソースが必要になる状況や、それらのリソースによって IP Voice Media Streaming Application にかかる負荷を慎重に検討してください。メディア リソースは、Unified CM と同じサーバ、または Unified CM 呼処理サービスを実行していない専用サーバを設置することができます。デフォルト数よりも多いリソースが必要な場合は、専用のサーバで実行するように設定することを推奨します。Cisco Unified CM のパフォーマンスに悪影響が及ぼされる可能性があるため、呼処理の負荷が大きい Cisco Unified CM ノードでは Cisco IP Voice Streaming Media Application をアクティブにしないことを強くお勧めします。展開内でメディア リソースを頻繁に使用することが予測される場合は、専用の Unified CM メディア リソース ノード（クラスタ内で呼処理を実行しない非パブリッシャ ノード）を配置するか、ハードウェアベースのメディア リソースに依存することを推奨します。Unified CM ノード上のソフトウェアベースのメディア リソースは、メディア リソースの必要性が限られている小規模な展開向けです。

音声インターフェイス

音声インターフェイスは、時分割多重（TDM）インターフェイス上のレッグと VoIP（Voice over IP）接続上のレッグの 2 つのコール レッグを持つコールに適用されます。TDM レッグは、エンコーディング/デコーディングとストリームのパケット化を実行するハードウェアで必ず終端します。この終端機能は、同じハードウェア モジュール、ブレード、またはプラットフォーム上にあるデジタル シグナル プロセッサ（DSP）リソースによって実行されます。

Cisco TDM ゲートウェイ上の DSP ハードウェアはすべて、音声ストリームを終端できます。また、特定のハードウェアは、会議やトランスコーディングなどの他のメディア リソース機能を実行することもできます（トランスコーディング（7-5 ページ）およびトランスコーディング（7-5 ページ）を参照）。DSP ハードウェアには、アップグレードまたは変更ができない固定 DSP リソース、またはアップグレード可能なモジュラ DSP リソースのどちらかが搭載されています。

DSP ごとにサポートされるコール数は、コールに使用されるコーデックの計算の複雑度や、DSP に設定された複雑度モードによって異なります。Cisco IOS を使用すると、ハードウェア モジュールの複雑度モードを設定できます。PVDM2、PVDM3、PVDM4 DSP のようなハードウェア プラットフォームは、3 つの複雑度モード（中複雑度モード、高複雑度モード、フレックス モード）をサポートします。他のハードウェア プラットフォームには、中複雑度モードと高複雑度モードのみをサポートするものもあります。

中複雑度モードと高複雑度モード

各 DSP は、中複雑度モード、高複雑度モード、またはフレックス モード（PVDM3 DSP および C5510 に基づく DSP）のいずれかとして個別に設定できます。DSP は、コールのコーデックに関する実際の複雑度に関係なく、設定されている複雑度に応じてすべてのコールを処理します。着信コールの実際の複雑度と同じかそれ以上の複雑度が設定されたリソースが使用可能になっている必要があります。そうでない場合、コールは失敗します。たとえば、コールに高複雑度コーデックが必要な場合、DSP リソースが中複雑度モードに設定されていると、コールは失敗します。しかしながら、高複雑度モードに設定された DSP に対して中複雑度コールが試行された場合、コールは成功し、Cisco IOS は高複雑度モードのリソースを割り当てます。

フレックス モード

フレックス モードは、C5510 チップセットを使用するハードウェア プラットフォーム上、および PVDM3 DSP 上だけで使用可能であり、このモードでは、設定時にコーデックの複雑度を指定する必要がありません。フレックス モードの DSP は、処理能力が足りる限り、サポートされているすべてのコーデック タイプのコールを受け入れます。

C5510 ベースの DSP の場合は、Millions of Instructions Per Second（MIPS）単位の処理能力を計算することで動的にトラッキングされます。Cisco IOS は、受信されたコールごとに MIPS の計算を実行し、新しいコールが開始されるたびにそのバジェットから MIPS クレジットを差し引きます。コールで消費される MIPS 数は、コールのコーデックによって異なります。着信コールに必要な MIPS 以上の MIPS クレジットが残っている限り、DSP は新しいコールを許可します。

同様に、PVDM3 DSP モジュールでは、クレジットベースのシステムを使用します。各モジュールには、メディア ストリームを処理するモジュールのキャパシティの単位を表す固定数の「クレジット」が割り当てられています。音声インターフェイス、トランスコーディングなどの各メディア動作には、クレジットによるコストが割り当てられています。DSP リソースはメディア処理用に割り当てられているため、そのコスト値は、使用可能なクレジットから差し引かれます。使用可能なクレジットが使い果たされると、DSP モジュールのキャパシティがなくなり、要求された操作に対応できなくなります。PVDM3 DSP のクレジット割り当て規則は、より複雑です。

フレックス モードは、同じハードウェアで複数のコーデックのコールをサポートする必要がある場合に便利です。これは、フレックス モードでは、DSP が中複雑度または高複雑度として設定されている場合よりも多くのコールをサポートできるためです。ただし、フレックス モードではリソースのオーバーサブスクリプションが許可されています。オーバーサブスクリプションになると、すべてのリソースが使用された場合にコール障害が発生するリスクが生じます。フレックス モードを使用すると、物理 TDM インターフェイスを使用する場合よりも DSP リソースの数を削減できます。

中複雑度モードまたは高複雑度モードと比べると、フレックス モードには、DSP ごとに最も多くの G.711 コールをサポートできるという利点があります。たとえば、PVDM2-16 DSP は、中複雑度モードで 8 つの G.711 コールを、フレックス モードでは 16 の G.711 コールをサポートできます。

トランスコーディング

トランスコーダは、あるコーデックからの入力ストリームを、別のコーデックを使用する出力ストリームに変換するデバイスです。Cisco IOS Release 15.0.1M から、トランスコーダは、同じコーデックを異なるパケット サイズで利用する 2 つのストリームを接続するトランスレーティングもサポートします。

G.711 から他のコーデックへのトランスコーディングは、従来のトランスコーディングと呼ばれます。2 つの非 G.711 コーデック間のトランスコーディングは、ユニバーサル トランスコーディングと呼ばれ、Universal Cisco IOS トランスコーダが必要です。ユニバーサル トランスコーディングは、Cisco IOS Release 12.4.20T からサポートされます。ユニバーサル トランスコーディングは、従来のトランスコーディングよりも DSP の密度が低いです。

Unified CM システムでは、通常、G.711 音声ストリームと低ビットレート圧縮音声ストリームの G.729a との間の変換を行うために、トランスコーダを使用します。次の場合には、どのようなときにトランスコーダ リソースが必要かが決まります。

- システム全体で単一のコーデックが使用されている。

  一般に、単一のコーデックは、帯域幅の節約を通常必要としない単一サイト配置で使用されます。システムのすべてのコールに対して単一のコーデックが設定されている場合、トランスコーダ リソースは必要ありません。このシナリオでは、すべてのベンダーでサポートされている G.711 を選択するのが最も一般的です。

- システムで複数のコーデックが使用され、すべてのエンドポイントがすべてのコーデック タイプに対応している場合

  複数のコーデックを使用する最も一般的な理由は、LAN コールには G.711 を使用してコール品質を最大にし、帯域幅が制限されている WAN を通過するコールには低帯域幅コーデックを使用して帯域幅効率を最大にするためです。低帯域幅コーデックには、G.729a を使用することを推奨します。G.729a は、すべての Cisco Unified IP Phone モデル、およびその他のほとんどの Cisco Unified Communications デバイスでサポートされるため、トランスコーディングの必要がなくなります。Unified CM では、リージョン間でその他の低帯域幅コーデックも設定できますが、一部の電話機モデルはこのコーデックをサポートしないため、トランスコーダが必要になります。ゲートウェイへのコールには 1 つのトランスコーダが必要で、別の IP Phone へのコールには 2 つのトランスコーダが必要です。すべてのデバイスが G.711 と G.729 の両方をサポートし、両方で設定されている場合は、デバイスがコールごとに適切なコーデックを使用するため、トランスコーダを使用する必要はありません。

- システムで複数のコーデックが使用され、一部のエンドポイントが G.711 だけをサポートしているか、または G.711 だけを使用するように設定されている。

  この条件は、システムで G.729a を使用し、このコーデックをサポートしないデバイスがある場合、または G.729a をサポートするデバイスが G.729a を使用するように設定されていない場合に発生します。この場合はトランスコーダが必要です。サードパーティ ベンダーのデバイスは、G.729 をサポートしない場合があります。

トランスコーダは、メディア ターミネーション ポイント（MTP）と同じ機能も実行できます。トランスコーダ機能と MTP 機能の両方が必要な場合、トランスコーダがシステムによって割り当てられます。MTP 機能が必要な場合、Unified CM はトランスコーダまたは MTP をリソース プールから割り当てます。リソースの選択はメディア リソース グループによって決まります（メディア リソース グループとメディア リソース グループ リスト（7-37 ページ）の項を参照）。

設計を最終決定するには、必要なトランスコーダの数と、トランスコーダを配置する場所を検討する必要があります。マルチサイト配置の場合は、トランスコーダを必要な各サイトにローカルに配置することを推奨します。複数のコーデックが必要な場合は、すべてのコーデックをサポートしないエンドポイントの数、これらのエンドポイントを配置する場所、これらのリソースにアクセスする他のグループ、これらのデバイスがサポートする同時コールの最大数、およびネットワーク上でこれらのリソースを配置する場所を検討する必要があります。

オーディオ変換リソース

トランスコーディングを実行するには、デジタル シグナル プロセッサ（DSP）リソースが必要です。DSP リソースは、音声モジュールまたは、Cisco サービス統合型ルータ（ISR）で使用可能なオンボード Cisco Packet Voice/Fax Digital Signal Processor（PVDM2、PVDM3、または PVDM4）のスロットに配置できます。

音声ゲートウェイとサポートされる音声モジュールの詳細については、次の URL で入手可能なシスコ音声モジュールおよびインターフェイス カードに関する情報を参照してください。

https://www.cisco.com/c/en/us/products/interfaces-modules/voice-modules-interface-cards/index.html

ビデオの相互運用性

ビデオの相互運用性とは、Cisco TelePresence System（CTS）エンドポイント、他の Cisco Unified Communications ビデオ エンドポイント、およびサードパーティ製ビデオ エンドポイント間でポイントツーポイント コールの音声とビデオをサポートすることです。Cisco Unified CM 8.5 よりも前のリリースでは、さまざまなビデオ エンドポイント間におけるビデオの相互運用性は、ビデオ トランスコーダやマルチポイント コントロール ユニット（MCU）などのビデオ コンポーネントをエンドポイントの間に挿入した場合にのみ実現できました。

Cisco Unified CM 8.5 以降のリリースでは、さまざまなタイプのエンドポイント間（ポイントツーポイント）のネイティブなビデオの相互運用性が提供されるだけでなく、SIP および H.323 プロトコルでの H.264 コーデック ネゴシエーションによってビデオの相互運用性が全体的に向上し、利用可能な場合は高品位（HD）解像度でネゴシエートできるようになりました。ただし、ビデオの相互運用性は相互運用をサポートするエンドポイントによって異なります。詳細については、次の URL で入手可能な『*Interoperability Between CTS Endpoints and Other Cisco Endpoints or Devices*』を参照してください。

https://www.cisco.com/en/US/docs/telepresence/interop/endpoint_interop.html

メディア ターミネーション ポイント（MTP）

メディア ターミネーション ポイント（MTP）は、2 つの全二重メディア ストリームを受け入れるエンティティです。MTP はこの 2 つのストリームをブリッジし、これらのストリームを個々にセットアップおよび終了できるようにします。ある接続の入力ストリームから受信されるストリーミング データは、他の接続の出力ストリームに渡され、逆も同様です。MTP には次のような多くの用途があります。

- ストリームの再パケット化（7-7 ページ）
- DTMF 変換（7-8 ページ）
- プロトコル固有の使用（IPv4 エンドポイントと IPv6 エンドポイント間のブリッジング）
  - SIP トランク経由のコール（7-9 ページ）
  - H.323 付加サービス（7-14 ページ）
  - H.323 発信時の Fast Connect（7-14 ページ）

ストリームの再パケット化

MTP は、G.711 a-law 音声パケットから G.711 mu-law パケット（およびその逆）にトランスコードしたり、パケット化周期が異なる（使用するサンプル サイズが異なる）2 つの接続をブリッジしたりできます。

DTMF 変換

コール中にメニュー システムのナビゲート、データの入力、またはその他の操作の目的で遠端のデバイスに信号を送信する際は、DTMF トーンが使用されます。これらは、呼制御の一部としてコール セットアップ中に送信される DTMF トーンとは異なる方法で処理されます。IP 上で DTMF を送信する方法はいくつかありますが、2 つの通信エンドポイントで共通の手順がサポートされていない場合があります。このような場合、Unified CM はメディア パスに動的に MTP を挿入して、DTMF 信号をエンドポイント間で変換できます。残念ながら、このようなコールには MTP リソースが 1 つずつ必要となるため、この方法は拡張性に欠けています。必要な MTP リソースの最適な量は、以降の項に従い、システム内のエンドポイント、トランク、およびゲートウェイの組み合わせに基づいて判断してください。

MTP の挿入が必要であると判断された場合に使用可能な MTP リソースがないとき、Unified CM はサービス パラメータ [MTP 割り当てが失敗した場合コールが失敗する（Fail call if MTP allocation fails）] の設定に従って、そのコールを続行するかどうかを決定します。このサービス パラメータは、[いいえ（False）] のデフォルト値に設定されています。このデフォルト設定では、SIP アーリー オファー トランクの着信コールは、発信側でディレイド オファーになります。

エンドポイント間の DTMF リレー

次の方法を使用して、DTMF を 1 つのエンドポイントから別のエンドポイントにリレーします。

Named Telephony Event（RFC 2833）

RFC 2833 で規定されている Named Telephony Event（NTE）は、コール メディアが確立された後で、あるエンドポイントから別のエンドポイントに DTMF を送信する方式です。トーンは、すでに確立されている RTP ストリームを使用して、パケット データとして送信されます。これらのトーンは、RTP ペイロード タイプ フィールドによってオーディオとは区別されます。たとえば、コールのオーディオをセッションで送信する際は、そのオーディオを G.711 データとして識別する RTP ペイロード タイプを使用できます。DTMF パケットの送信時には、そのパケットを NTE として識別する RTP ペイロード タイプが使用されます。ストリームの受信側は、G.711 パケットと NTE パケットを別々に利用します。

Key Press Markup Language（RFC 4730）

Key Press Markup Language（KPML）は RFC 4730 で規定されています。DTMF をインバンドで送信する NTE とは異なり、KPML はシグナリング チャネルを使用して（つまり、アウトオブバンド（OOB）で）、DTMF 番号を含む SIP メッセージを送信します。

KPML 手順では、DTMF 番号の登録に SIP SUBSCRIBE メッセージが使用されます。DTMF 番号自体は、XML で符号化された本体を含む NOTIFY メッセージで送信されます。

Unsolicited Notify（UN）

Unsolicited Notify 手順は、主に Cisco IOS SIP ゲートウェイにおいて、SIP NOTIFY メッセージを使用して DTMF 番号を転送するために使用されます。KPML とは異なり、これらの NOTIFY メッセージは非請求メッセージで、これらのメッセージを受信するために事前に SIP SUBSCRIBE メッセージで登録が行われることはありません。ただし、KPML と同様に、Unsolicited Notify メッセージもアウトオブバンドです。

また、KPML には XML で符号化されたメッセージ本体が含まれますが、Unsolicited Notify の NOTIFY メッセージの本体はそれとは異なり、DTMF イベントを表す 10 文字の符号化された数字、ボリューム、および継続時間です。

H.245 Signal、H.245 Alphanumeric

H.245 は、H.323 ネットワークで使用されるメディア制御プロトコルです。メディア特性のネゴシエートに使用されるほか、DTMF 転送用のチャネルも提供します。H.245 はシグナリング チャネルを利用するため、DTMF 番号はアウトオブバンド（OOB）で送信されます。Signal 方式は、Alphanumeric 方式よりも多くの DTMF イベント情報（DTMF イベントの実際の継続時間など）を伝送します。

シスコ独自の RTP

この方法は DTMF 番号をインバンドで（つまり、RTP パケットと同じストリームで）送信します。ただし、DTMF パケットはメディア パケットとは符号化方法が異なり、別のペイロード タイプが使用されます。この方法は Unified CM ではサポートされていませんが、Cisco IOS ゲートウェイではサポートされています。

Skinny Client Control Protocol（SCCP）

SCCP は、Unified CM により、Unified CM に登録されている SCCP ベースの各種デバイスを制御するために使用されます。SCCP は、Unified CM と制御デバイス間で DTMF 番号を転送するアウトオブバンド メッセージを定義します。

同じ Unified CM クラスタのエンドポイント間での DTMF リレー

同じクラスタ内の Unified CM サーバに登録されたエンドポイントには、次の規則が適用されます。

- SIP 以外の 2 つのエンドポイント間のコールには、MTP は必要ありません。

  SIP 以外のすべての Cisco Unified Communications エンドポイントはさまざまなシグナリング パスによって DTMF を Unified CM に送信し、Unified CM は受け取った DTMF を異なるエンドポイント間で転送します。たとえば、IP Phone は Unified CM への SCCP メッセージを使用して DTMF を送信します。この DTMF は H.245 シグナリング イベントによって H.323 ゲートウェイに送信されます。Unified CM は、異なるシグナリング方式の間で DTMF を転送できます。

- 2 つの Cisco SIP エンドポイント間のコールには、MTP は必要ありません。

  Cisco SIP エンドポイントはすべて NTE をサポートしているため、DTMF はエンドポイント間で直接送信され、変換は不要です。

- SIP エンドポイントと SIP 以外のエンドポイントの組み合わせの場合、MTP が必要になることがあります。

  ご使用のデバイスで NTE がサポートされるかどうかは、そのデバイスの製品マニュアルを参照してください。NTE のサポートは SIP に限定されていないため、その他の呼制御プロトコルを使用するデバイスでサポートされていることがあります。Unified CM は、エンドポイントのペアの機能に基づき、MTP をコール単位に動的に割り当てることができます。

SIP トランク経由のコール

SIP トランク設定は、SIP ユーザ エージェント（別の Cisco Unified CM クラスタや SIP ゲートウェイなど）との通信をセットアップする際に使用されます。

SIP はセッション記述プロトコル（SDP）によってメディア情報をネゴシエートします。これにより、一方が提示したメディア セットに他方が応答する形で、使用するメディアがある組み合わせに決定します。SIP では、発信側が初期 INVITE メッセージ（アーリー オファー）によって初期のオファーを送信するか、発信側がそうしなかった場合は着信側が最初の信頼性のある応答（ディレイド オファー）で初期のオファーを送信できます。

デフォルトで、Unified CM SIP トランクは、初期のオファー（ディレイド オファー）を伴わない INVITE を送信します。Unified CM には、SIP トランクが INVITE でオファー（アーリー オファー）を送信できるようにする次の 3 つの設定可能なオプションがあります。

メディア ターミネーション ポイントが必須（Media Termination Point Required）

SIP トランク上でこのオプションを有効にすると、すべての発信コールに対して 1 つの MTP が割り当てられます。このオプションは、SIP トランク上で単一のコーデック（G.711 または G.729）の制限を課すコーデックのパススルー モードをサポートしないので、メディアを音声コールのみに制限します。このオプションが有効な場合、トランクを介したコールは、同じシグナリング パスに従うようにメディアを強制する発信デバイス MTP を使用せずに、トランクに割り当てられている MTP を使用します。

（注）　SIP トランク上で [メディア ターミネーション ポイントが必須（Media Termination Point Required）] オプションを有効にすると、MTP 使用率が上がります。必要に応じてではなく、すべての着信コールおよび発信コールに対して MTP が割り当てられるためです。

[音声コールとビデオ コールに対する早期オファー サポートが必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）]

SIP トランクに関連付けられた SIP プロファイルでこの Unified CM 設定オプションを有効にすると、MTP が挿入されるのは、発信デバイスが発信アーリー オファーの作成に必要なメディア特性を Unified CM に提示できない場合のみです（たとえば、Unified CM への着信コールがディレイド オファー SIP トランクまたは Slow Start H.323 トランクで受信される場合、Unified CM に登録された Cisco Unified IP Phone 7940 または 7960 などの古い SCCP ベースの電話機からコールなど）。Unified CM は、エンドポイントおよび MTP コーデック機能のスーパーセットを作成し、適用可能なリージョンペア設定に基づいてコーデックのフィルタリングを適用します。発信オファー SDP は、MTP の IP アドレスとポート番号、発信電話でサポートされる音声コーデックを使用します。

Unified CM が H.323 Slow Start または SIP ディレイド オファー トランクで着信を受信した場合、コールの開始時に発信デバイスのメディア機能を使用できません。この場合、Unified CM は、MTP を挿入し、その IP アドレスと UDP ポート番号を使用して、（リージョンペアのフィルタリング後の）サポートされるすべてのオーディオ コーデックを、発信 SIP トランク上で送信される初期 INVITE のオファー SDP にアドバタイズする必要があります。アンサー SDP が SIP トランク上で受信される場合、その SDP に発信エンドポイントでサポートされるコーデックが含まれていれば、追加のオファー/アンサー トランザクションは不要です。コーデックが一致しない場合、Unified CM は、トランスコーダを挿入してその不一致に対処するか、Re-INVITE または UPDATE を送信してメディア ネゴシエーションをトリガーできます。H.323 Slow Start トランクまたは SIP ディレイド オファー トランクからのコールは、初期コール セットアップ時に音声のみをサポートしますが、コール メディアが再ネゴシエートされれば（保留/再開後など）、ビデオと SRTP をサポートするようにコール中にアップグレードされる可能性があります。

トランクの SIP プロファイルに [音声コールとビデオ コールに対する早期オファー サポートが必須（必要な場合は MTP を挿入）（Early Offer support for voice and video calls Mandatory (insert MTP if needed)）] を設定した場合、古い SCCP ベースの電話機、SIP ディレイド オファー トランク、および H.323 Slow Start トランクからのコールは、すでに別の理由で MTP またはトランスコーダが割り当てられていなければ、Unified CM によって MTP が割り当てられます。この MTP を使用して、有効なメディア ポート番号と IP アドレスを含むオファー SDP が生成されます。この MTP は、発信 SIP トランクのメディア リソースからではなく、発信デバイスに関連付けられているメディア リソースから割り当てられます。（この処理で、メディア パスが発信 SIP トランクの MTP にアンカーされるのを回避します）。発信デバイスのメディア リソース グループ リスト（MRGL）から MTP を割り当てることができない場合、MTP の割り当ては SIP トランクの MRGL から試行されます。

（注）　MTP リソースを使用できない場合、コールは、ディレイド オファー コールとして処理されます。

Unified CM は、次のいずれかの手段で着信コールを受信する場合は、SIP トランク上で発信アーリー オファー コールを作成するために MTP を挿入する必要はありません。

- アーリー オファーを使用する SIP トランク上
- Fast Start を使用する H.323 トランク上
- MGCP トランク上
- Unified CM に登録されている SIP ベースの IP フォンから

[音声コールとビデオ コールに対する早期オファーのサポートはベスト エフォート（MTP の挿入なし）（Early Offer support for voice and video calls Best Effort (No MTP inserted)）]

この Unified CM SIP プロファイルの設定オプションが有効になっている場合、SIP トランクは MTP を使用してアーリー オファーを作成することはありませんが、発信側デバイスの機能に応じて、アーリー オファーまたはディレイド オファーを送信します。

ベスト エフォートのアーリー オファー SIP トランクは、次の状況において発信コールをアーリー オファー（SDP コンテンツを含む INVITE）として送信します。

- Unified CM または SME への着信コールがアーリー オファーを使用して SIP トランク経由で受信される場合。
- Unified CM または SME への着信コールが Fast Start を使用した H.323 トランクを介して受信される場合。
- Unified CM または SME への着信コールが MGCP トランクを介して受信される場合。
- コールが Unified CM に登録されている SIP ベースの IP 電話から開始される場合。
- コールが Unified CM に登録されている新しいモデルの SCCP ベースの Cisco Unified IP 電話から開始される場合。

ベスト エフォートのアーリー オファー トランクは、次の状況において発信コールをディレイド オファー（SDP コンテンツを含まない INVITE）として送信します。

- Unified CM または SME への着信コールがディレイド オファー SIP トランクを介して受信される場合。
- Unified CM または SME への着信コールが H.323 Slow Start トランクを介して受信される場合。
- コールが Unified CM に登録されている古いモデルの SCCP ベースの IP 電話から開始される場合。

ベスト エフォートのアーリー オファー SIP トランクを介したコールは、音声、ビデオ、および暗号化されたメディアをサポートしています。

通常、すべての Unified CM および Unified CM Session Management Edition の SIP トランクに対し、[音声コールとビデオ コールに対する早期オファーのサポートはベスト エフォート（MTP の挿入なし）（Early Offer support for voice and video calls Best Effort (No MTP inserted)）] が推奨されます。

このオプションの詳細については、ベスト エフォートのアーリー オファー [音声コールとビデオ コールに対する早期オファーのサポートはベスト エフォート（MTP の挿入なし）（Early Offer support for voice and video calls Best Effort (No MTP inserted)）]（6-24 ページ）の項を参照してください。

SIP トランクの MTP に関する要件

デフォルトでは、SIP トランク パラメータの [メディア ターミネーション ポイントが必須（Media Termination Point Required）] と SIP プロファイル パラメータの [音声コールとビデオ コールに対する早期オファー サポート（Early Offer support for voice and video calls）] は選択されていません。

SIP トランクで MTP リソースが必要かどうかを判断するには、次の手順に従います。

1. この SIP トランクで定義されている対向の SIP デバイスが、SIP アーリー オファーを含まない着信コールを受け入れられるかどうかを確認します。

   受け入れられない場合、このトランクに関連付けられた SIP プロファイルで、[音声コールとビデオ コールに対する早期オファーのサポート（必要な場合は MTP を挿入）（Early Offer support for voice and video calls (insert MTP if needed)）] チェックボックスをオンにします。発信 SIP トランク コールでは、アーリー オファーの作成に必要なメディア特性を持つ Unified CM を発信側デバイスが提供できない場合、または DTMF 変換が必要な場合にのみ、MTP が挿入されます。

   その場合は、[音声コールとビデオ コールに対する早期オファーのサポートはベスト エフォート（MTP の挿入なし）（Early Offer support for voice and video calls Best Effort (No MTP inserted)）] をオンにして、ステップ 2. に進んで、MTP が DTMF 変換に対して動的に挿入されるかどうかを判断します。MTP による DTMF 変換は、どのコーデックを使用している場合でも実行できます。

2. トランクの DTMF Signaling Method を選択します。このパラメータは、そのトランクでの DTMF 選択の動作を制御します。すべてのコールについて、DTMF 方式を一致させるために、必要に応じて使用可能な MTP が割り当てられます。

   a. DTMF Signaling Method：No Preference

      このモードでは、Unified CM は、エンドポイントによってサポートされる DTMF シグナリング方式を選択することで、MTP の使用を最小限に抑えようとします。

      両方のデバイスが RFC 2833 をサポートしている場合は、MTP は必要ありません。

      両方のデバイスがいずれかのアウトオブバンド DTMF メカニズムをサポートしている場合、Unified CM は SIP トランク上で KPML を使用します。MTP が必要となる唯一のケースは、エンドポイントの 1 つがアウトオブバンドのみをサポートし、もう一方が RFC 2833 のみをサポートする場合です。

      両方のデバイスが RFC 2833 とアウトオブバンド DTMF メカニズムをサポートしている場合、Unified CM は RFC 2833 と KPML の両方をネゴシエートしますが、番号を受信する際は RFC 2833 に依存します。

      （注）　Unified CM の DTMF 設定で SIP トランクが [設定なし（No Preference）] に設定されている場合、Unified CM は Unsolicited Notify に対してネゴシエーションを行いません。たとえば、遠端の SIP ゲートウェイまたは Cisco Unified Border Element が **dtmf-relay sip-notify** 用に設定されていて、Cisco Unified Border Element に接続する Unified CM SIP トランクが [設定なし（No Preference）] に設定されていると、DTMF は機能しません。この場合に推奨される方法は、DTMF 設定で Unified CM SIP トランクを OOB および RFC 2833 に接続するよう設定することです。こうすることで、Unified CM が SIP ゲートウェイまたは Cisco Unified Border Element と Unsolicited Notify で DTMF 方式をネゴシエートできるようになります。

b. DTMF Signaling Method：RFC 2833

トランク全体の DTMF シグナリング方式を制限することにより、Unified CM は、一方または両方のエンドポイントが RFC 2833 をサポートしていない場合に MTP を強制的に割り当てます。この設定では、MTP が割り当てられないのは、両方のエンドポイントが RFC 2833 をサポートしている場合だけです。

c. DTMF Signaling Method：OOB and RFC 2833

このモードでは、SIP トランクを通じて KPML 方式と RFC 2833 DTMF 方式の両方が送信されます。これは MTP の使用される可能性が最も高いモードです。MTP リソースが必要とされない唯一のケースは、両方のエンドポイントが RFC 2833 といずれかの OOB DTMF 方式（KPML または SCCP）をサポートしている場合です。

（注）　Cisco Unified IP Phone は、DTMF を SCCP 経由で受信した場合、エンド ユーザに対して DTMF を再生しますが、RFC 2833 で受信したトーンは再生しません。ただし、DTMF を別のエンド ユーザに送信する必要はありません。DTMF を必要とするエンドポイント（PSTN ゲートウェイ、アプリケーション サーバなど）と対応するコールを発信するエンドポイントについてのみ検討する必要があります。

SIP ゲートウェイおよび Cisco Unified Border Element での DTMF リレー

Cisco SIP ゲートウェイは、その設定に応じて、DTMF メカニズムとして KPML、NTE、または Unsolicited Notify をサポートします。システムにはさまざまなエンドポイントが混在している場合があるため、複数の方式をゲートウェイに同時に設定することで、MTP の要件を最小限に抑えることができます。

Cisco SIP ゲートウェイでは、SIP ダイヤル ピアの DTMF リレー方式として、**sip-kpml** と **rtp-nte** の両方を設定します。このように設定すると、NTE だけをサポートするものや OOB 方式だけをサポートするものも含めて、すべてのタイプのエンドポイント間で MTP リソースなしに DTMF 交換を実現できます。この設定では、ゲートウェイは NTE と KPML の両方を Unified CM とネゴシエートします。Unified CM のエンドポイントで NTE がサポートされていない場合は、DTMF 交換に KPML が使用されます。両方の方式のネゴシエーションが成功した場合、ゲートウェイは NTE を使用して DTMF 番号を受信し、KPML へのサブスクライブは行いません。

Cisco SIP ゲートウェイでは、DTMF に独自の Unsolicited Notify（UN）方式を使用することもできます。UN 方式は、DTMF トーンを表すテキストをメッセージ本体に含む SIP Notify メッセージを送信します。この方式は Unified CM でもサポートされており、**sip-kpml** が有効でない場合に使用されます。DTMF リレー方式として **sip-notify** を設定します。この方式はシスコ独自のものである点に注意してください。

NTE だけをサポートする SIP ゲートウェイでは、NTE をサポートしないエンドポイントと通信する場合、MTP リソースの割り当てが必要となります。

H.323 トランクおよびゲートウェイ

H.323 ゲートウェイおよびトランクでは、次の 3 つの理由で MTP が呼び出されます。

- H.323 付加サービス（7-14 ページ）
- H.323 発信時の Fast Connect（7-14 ページ）
- DTMF 変換（7-14 ページ）

H.323 付加サービス

H.323v2 で規定された Empty Capabilities Set（ECS）で使用する OpenLogicalChannel および CloseLogicalChannel 要求機能をサポートしていない H.323 エンドポイントでも、MTP を利用することでこれらの機能をサポートすることができます。この要件はあまり発生しません。すべての Cisco H.323 エンドポイント、およびほとんどのサードパーティのエンドポイントが ECS をサポートしています。必要に応じて、MTP が割り当てられ、H.323 エンドポイントに代わってコールに接続されます。MTP が H.323 コールで要求され、使用できるものがない場合、コールは処理されますが、付加サービスを呼び出すことはできません。

H.323 発信時の Fast Connect

H.323 では、Fast Connect という手順が定義されています。これは、コール セットアップ時に交換されるパケット数を削減し、メディアを確立する時間を短縮します。この手順では、制御チャネルのシグナリングに Fast Start 要素を使用します。H.323 を利用する 2 つのデバイスのネットワーク遅延が高いときは、この遅延がメディアを確立する時間に影響を与えるため、この手順が役立ちます。Unified CM は、コール セットアップの方向に基づき、着信 Fast Start と発信 Fast Start を区別します。MTP 要件が同じではないため、この区別は重要です。着信 Fast Start の場合、MTP は必要ありません。H.323 トランクの発信コールは、Fast Start が有効なとき、MTP を必要とします。多くの場合、問題になるのは、着信コールだけです。問題を解決するには、発信 Fast Start を有効にせずに着信 Fast Start を使用します。

DTMF 変換

H.323 トランクは、H.245 アウトオブバンド方式による DTMF のシグナリングをサポートします。H.323 クラスタ間トランクは、NTE による DTMF もサポートします。H.323 トランクには DTMF 設定オプションはありません。DTMF 転送方式は Unified CM によって動的に選択されます。

異なるクラスタにある 2 つのエンドポイントが H.323 トランクを使用して接続する場合は、次のケースが起こり得ます。

- 両方のエンドポイントが SIP の場合は、NTE が使用されます。DTMF のために MTP は必要ありません。
- 一方のエンドポイントが SIP で、KPML と NTE の両方をサポートしていて、他方のエンドポイントが SIP でない場合は、SIP エンドポイントから Unified CM に KPML で DTMF が送信され、トランクでは H.245 が使用されます。DTMF のために MTP は必要ありません。
- 一方のエンドポイントが SIP で、NTE だけをサポートしていて、他方のエンドポイントが SIP でない場合は、トランクで H.245 が使用されます。この場合はコールに対して使用可能な MTP が割り当てられます。MTP は、SIP エンドポイントがある Unified CM クラスタで割り当てられます。

たとえば、SIP を使用する Cisco Unified IP Phone 7970 が、SCCP を使用する Cisco Unified IP Phone 7970 と通信する場合は、SIP トランク経由で接続されるときは NTE が使用され、H.323 トランク経由で（H.245 方式を使用するトランクを使用して）通信するときは OOB 方式が使用されます。

コールがある H.323 トランクから着信し、そのコールを別の H.323 トランクにルーティングする場合、両方のエンドポイントが SIP のときは、DTMF 用に NTE が使用されます。どちらか一方のエンドポイントが SIP でないときは、H.245 が使用されます。一方が NTE だけをサポートする SIP エンドポイントで、他方が SIP でない場合は、MTP が割り当てられます。

H.323 ゲートウェイおよび Cisco Unified Border Element での DTMF リレー

H.323 ゲートウェイは、H.245 Alphanumeric、H.245 Signal、NTE、およびメディア ストリームのオーディオによる DTMF リレーをサポートします。現時点では、H.323 ゲートウェイ用の Unified CM において NTE オプションはサポートされていないため、使用できません。これに適したオプションは H.245 Signal です。他のエンドポイントに Unified CM と共通のシグナリング機能がない場合、H.323 ゲートウェイへのコールを確立するために、MTP が必要です。たとえば、SIP スタックを実行している Cisco Unified IP Phone 7960 は NTE だけをサポートするため、H.323 ゲートウェイを使用する場合は MTP が必要です。

CTI ルート ポイント

CTI ルート ポイントは、CTI イベントを使用して CTI アプリケーションと通信します。DTMF の観点では、CTI ルート ポイントは、すべての OOB 方式をサポートし、RFC 2833 はサポートしないエンドポイントと見なすことができます。そのようなエンドポイントで DTMF 変換に MTP が必要となるケースは、RFC 2833 だけをサポートする別のエンドポイントと通信する場合だけです。

電話コールのファーストパーティ制御を持つ CTI ルート ポイントは、コールのメディア ストリームに参加し、MTP の挿入を必要とします。CTI によるコールのサードパーティ制御が可能で、メディアが CTI で制御されているデバイスを通過する場合、MTP が必要かどうかは制御されるデバイスの機能によって異なります。

例 7-1　NTE 変換用に MTP を必要とするコール フロー

例として、ファーストパーティ制御（CTI ポートがメディアの終端）の CTI ルート ポイントがあり、IVR メニューをナビゲートするために DTMF を使用するシステムに統合されているシステムを考えます。システムのすべての電話機が SCCP を実行している場合、MTP は必要ありません。この場合、Unified CM が CTI ポートを制御し、IP Phone からの DTMF を SCCP 経由で受信します。Unified CM が、DTMF 変換を提供します。

ただし、SIP スタックを実行している電話機（NTE だけをサポートしていて、KPML をサポートしていない電話機）がある場合は、MTP が必要です。NTE はメディア ストリームの一部なので、Unified CM は受信しません。MTP がメディア ストリームの中に呼び出され、SCCP を使用する 1 つのコール レッグと NTE を使用する 2 番めのコール レッグを持ちます。MTP は Unified CM によって SCCP 制御下に置かれ、NTE から SCCP への変換を実行します。KPML をサポートしている新しい電話機では、MTP は必要ありません。

カンファレンス ブリッジでの MTP の使用

MTP は、会議の参加者のデバイスの中に RFC 2833 を使用するデバイスがある場合に使用されます。会議機能が呼び出されると、Unified CM が、コールに含まれており、RFC 2833 だけをサポートするすべての会議参加者のデバイスに MTP リソースを割り当てます。これは、カンファレンス ブリッジの DTMF 機能が使用されているかどうかにかかわらず行われます。

MTP リソース

次のタイプのデバイスは、MTP として使用できます。

ソフトウェア MTP（Cisco IP Voice Media Streaming Application）

ソフトウェア MTP とは、Unified CM サーバ上で Cisco IP Voice Media Streaming Application を有効にすることによって実装されるデバイスです。インストールされたアプリケーションが、MTP アプリケーションとして設定されると、そのアプリケーションは、Unified CM ノードに登録され、サポートする MTP リソース数を Unified CM に知らせます。ソフトウェア MTP デバイスは、G.711 ストリームまたはコーデックでのパススルー モードのみをサポートします。IP Voice Media Streaming Application は、複数の機能に使用することもできるリソースで、設計ガイダンスではすべての機能を同時に考慮する必要があります（Cisco IP Voice Media Streaming Application（7-3 ページ）を参照）。

ソフトウェア MTP（Cisco IOS に基づく）

- ルータでソフトウェアベースの MTP を提供する機能は、Cisco 3800 シリーズ ルータでは Cisco IOS Release 12.3(11)T、Cisco 2900 シリーズおよび 3900 シリーズ ルータでは Release 15.0(1)M、ASR1002、1004、および 1006 ルータでは Release IOS-XE、ASR1001 ルータでは Release IOS-XE 3.2、その他のルータ モデルでは Release 12.3(8)T4 から使用できるようになりました。
- この MTP によって、G.711 mu-law および a-law、G.729a、G.729、G.729ab、G.729b、およびパススルーのコーデックを設定できます。ただし、同時に設定できるコーデックは 1 つだけです。これらの内の一部のコーデックは、Unified CM では実装していません。
- ルータ設定では、最大 1,000 の個別ストリームが可能で、500 のトランスコーディングされたセッションをサポートします。この数の G.711 ストリームを使用すると、10 MB のトラフィックが生成されます。Cisco ISR G2 および ASR ルータでは、これよりもはるかに大きな数をサポートできます。

ハードウェア MTP

音声モジュールまたは、Cisco サービス統合型ルータ（ISR）で使用可能なオンボード Cisco Packet Voice/Fax Digital Signal Processor（PVDM2、PVDM3、または PVDM4）のスロットに配置された DSP リソースは、MTP リソースとしても使用できます。

各 PVDM モジュールでサポートされるセッションの詳細については、メディア リソースのキャパシティ プランニング（7-33 ページ）の項を参照してください。

（注）　Cisco IOS MTP リソースがコール フローのために Unified CM によって呼び出されると、コール フローのメディア レッグにトランスレーティングを必要とする場合を除き、ハードウェア DSP セッション以外のソフトウェア セッションが消費されます。したがって、MTP を呼び出すフローの場合、トランスレーティング（コーデックは同じだがパケット化の時間が異なるメディア レッグ間の変換）が必要な場合にのみ DSP セッションが使用されます。

Trusted Relay Point

Trusted Relay Point（TRP）はメディア ストリームに挿入可能なデバイスの一種で、そのストリームのコントロール ポイントとして機能します。TRP を使用すると、そのストリームにさらに処理を加えることができます。また、ストリームが任意の特定のパスを通るようにする手段として TRP を使用することも可能です。TRP 機能を使用するためには 2 つの要素が存在します。1 つは CUCM 上で論理的に TRP を設定すること。もう 1 つは実際に TRP として動作するコールのアンカーポイントとなるデバイスです。TRP 機能は MTP デバイスをアンカーポイントとして使用する際に使うことができます。

Unified CM の個々の電話機に関する設定に、その電話機へのコールまたはその電話機からのコールに対して TRP を呼び出すための設定パラメータが新しく追加されました。TRP リソースの管理には、メディア リソース プール メカニズムが利用されます。その電話機のメディア リソース プールには、TRP として呼び出し可能なデバイスが含まれている必要があります。

TRP を QoS 強制メカニズムとして使用する例については、ネットワーク インフラストラクチャ（3-1 ページ）の章を参照してください。冗長ファイアウォールを備えた冗長なデータセンターでメディア ストリームのアンカー ポイントとして TRP を利用する例については、Cisco Collaboration Security（4-1 ページ）の章を参照してください。

Annunciator

アナンシエータは Cisco IP Voice Media Streaming Application のソフトウェア機能で、これを使用すると、音声メッセージや各種コール プログレス トーンをシステムからユーザに流すことができます。これは、SCCP メッセージを使用して RTP ストリームを確立し、また、Cisco IP Phone またはゲートウェイなどのデバイスに複数の片方向 RTP ストリームを送信できます。ほとんどの SIP デバイスでは、コール プログレス トーンは登録時にデバイスにダウンロード（プッシュ）され、必要に応じて Unified CM からの SIP シグナリング メッセージで呼び出せるようにします。クラスタ間 SIP トランクなどの一部の SIP デバイスは、引き続きコール プログレス トーンに Annunciator を使用する場合があります。Annunciator は、SIP を使用しているか SCCP を使用しているかに関係なく、ほとんどのデバイスで口頭メッセージに使用できます。

一部のインストールでは、Annunciator との双方向メディア接続を確立する必要がある場合があります。この機能を有効にするには、Cisco Unified CM サービス パラメータ [デュプレックス ストリーミング有効（Duplex Streaming Enabled）] を [はい（True）] に設定します。これは、ファイアウォール トラバーサルまたは SIP アーリー オファーのシナリオで必要となる場合があります。

トーンとアナウンスは、システムで事前に定義されています。アナウンスでは、ローカリゼーションがサポートされており、また、適切な .wav ファイルを置き換えて、アナウンスをカスタマイズすることもできます。Annunciator は、トランスコーディング リソースを使用しないで、G.711 a-law および mu-law、G.729、および Cisco L16 Wideband コーデックをサポートできます。

次の機能には、Annunciator リソースが必要です。

- Cisco Multilevel Precedence Preemption（MLPP）

  この機能には、次のようなコール失敗の状態に応じて再生されるストリーミング メッセージが用意されています。

  - 優先順位の高い既存のコールが原因で、プリエンプション処理できない。
  - 優先順位アクセス制限に到達した。
  - 試行された優先順位レベルが許可されていない。
  - 着信番号が、プリエンプション処理またはコール ウェイティングに対応していない。

- SIP トランクを介した統合

  SIP エンドポイントには、トーンを生成し、RTP ストリームでインバンドで送信する機能があります。SCCP デバイスにはこの機能がないため、SIP エンドポイントと統合した場合、DTMF トーンの生成または受け入れ時には Annunciator と MTP が併用されます。次のタイプのトーンがサポートされます。

  - コール プログレス トーン（ビジー、アラート、順番の変更、およびリングバック）
  - DTMF トーン

- Cisco IOS ゲートウェイとクラスタ間トランク

  これらのデバイスには、コール プログレス トーン（リングバック トーン）のサポートが必要です。

- システム メッセージ

  次のようなコール失敗の状態では、システムはエンド ユーザにストリーミング メッセージを再生します。

  - ダイヤル番号をシステムが認識できない。
  - サービスが中断したためコールがルーティングされない。
  - 番号が通話中で、その番号がプリエンプション処理またはコール ウェイティング用に設定されていない。

- [会議（Conferencing）]

  電話会議の間、システムは、参加者がブリッジに参加、またはブリッジから退出したことをアナウンスするときに、割り込み音を再生します。

Cisco IP Voice Media Streaming Application をサーバ上でアクティブにすると、Annunciator がシステム内に自動的に作成されます。Media Streaming Application を非アクティブにすると、Annunciator も非アクティブになります。単一の Annunciator インスタンスは、パフォーマンス要件を満たす場合は、Unified CM クラスタ全体にサービスを提供できます（Annunciator のパフォーマンス（7-18 ページ）を参照）。そうでない場合は、追加の Annunciator をクラスタ用に設定する必要があります。追加の Annunciator を設定するには、クラスタ内の他のサーバ上で Cisco IP Voice Media Streaming Application をアクティブにします。

Annunciator は、そのデバイス プールおよび CM グループで定義されたとおり、一度に 1 つの Unified CM に登録されます。デバイス プールに対してセカンダリが設定されている場合、Annunciator は自動的にセカンダリ Unified CM にフェールオーバーします。障害発生時に再生されるアナウンスはいずれも保持されません。

Annunciator はメディア デバイスと見なされるため、メディア リソース グループ（MRG）に含めて、電話機およびゲートウェイで使用される Annunciator の選択を制御できます。

Annunciator のパフォーマンス

デフォルトでは、Annunciator は 48 のストリームを同時にサポートするように設定されています。この設定値は、Unified CM サービスが同一のサーバ（共存）上で動作する Annunciator に推奨される最大値です。サーバの接続性が 10 Mbps しかない場合は、設定を下げて同時ストリームを 24 にします。

各サーバ プラットフォームでサポートされる Annunciator セッションの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章で、メディア リソース（25-30 ページ）の項を参照してください。

Cisco RSVP Agent

トポロジ対応型のコール アドミッション制御を提供するために、Unified CM は 1 つまたは 2 つの RSVP Agent をコール セットアップ中に呼び出し、IP WAN を介して RSVP 予約を実行します。これらのエージェントは、RSVP 機能を提供するように設定された MTP またはトランスコーダ リソースです。RSVP リソースは、Unified CM による MTP またはトランスコーダ リソースの割り当てという観点から見て、通常の MTP またはトランスコーダと同様に処理されます。

Cisco RSVP Agent 機能は、Cisco IOS Release 12.4(6)T で最初に導入されました。RSVP および Cisco RSVP Agent の詳細については、帯域幅管理（13-1 ページ）の章を参照してください。

保留音

保留音（MoH）機能を利用するには、各 MoH サーバが Unified CM クラスタに含まれ、データ レプリケーション スキーマに参加している必要があります。特に、MoH サーバは、データベース レプリケーション プロセスを通じて、次の情報を Unified CM クラスタと共有する必要があります。

- オーディオ ソース：設定されたすべての MoH オーディオ ソースの数と ID
- マルチキャストまたはユニキャスト：これらのソースそれぞれに設定されたトランスポートの種類
- マルチキャスト アドレス：マルチキャストとしてストリーミングするように設定されたソースのマルチキャスト ベース IP アドレス

MoH サーバを設定するには、1 つ以上の Unified CM ノードで Cisco IP Voice Media Streaming Application サービスを有効にします。MoH サーバは、Unified CM とともに同じサーバに配置することも、スタンドアロン モードで配置することもできます。

ユニキャストおよびマルチキャスト MoH

Unified CM は、ユニキャストおよびマルチキャストの MoH トランスポート メカニズムをサポートしています。

ユニキャスト MoH ストリームは、MoH サーバから MoH を要求しているエンドポイントへの、ポイントツーポイントの片通話のリアルタイム転送プロトコル（RTP）ストリームです。これは、ユーザまたは接続ごとに別々のソース ストリームを使用します。したがって、20 台のデバイスが保留になっている場合、サーバとこれらのエンドポイント デバイス間のネットワーク上で、ストリームが 20 本生成されます。ユニキャスト MoH が非常に役立つのは、マルチキャストが使用可能になっていないネットワークの場合や、デバイスがマルチキャスト対応になっていないネットワークの場合です。このようなときに、管理者はユニキャスト MoH を使用することで、MoH 機能を利用できます。ただし、このような MoH ストリームが生成されると、ネットワークのスループットと帯域幅に対してマイナスの影響を与える可能性があります。

マルチキャスト MoH ストリームは、MoH サーバとマルチキャスト グループ IP アドレス間の、ポイントツーマルチポイント片方向オーディオ RTP ストリームです。MoH オーディオ ストリームを必要とするエンドポイントは、必要に応じてマルチキャスト グループに参加できます。このモードの MoH では、複数のユーザが同じオーディオ ソース ストリームを使用して保留音を提供できるようになるので、システム リソースと帯域幅を節約できます。このため、マルチキャストは、ソース デバイスに対する CPU の影響を大幅に削減し、共通パス上の伝送の帯域幅使用量も大幅に削減するので、MoH などのサービスの配置に非常に魅力的なトランスポート メカニズムです。しかし、ネットワークがマルチキャスト対応になっていない状況や、エンドポイント デバイスがマルチキャストを処理できない状況では、マルチキャスト MoH に問題が生じます。

コール フローの動作に関して、ユニキャストとマルチキャストの MoH には明らかな相違点があります。ユニキャスト MoH コール フローは、Unified CM から MoH サーバへのメッセージによって始まります。このメッセージは、被保留側デバイスの IP アドレスにオーディオ ストリームを送信するように、MoH サーバに指示します。一方、マルチキャスト MoH コール フローは、Unified CM から被保留側デバイスへのメッセージによって始まります。このメッセージは、設定されたマルチキャスト MoH オーディオ ストリームのマルチキャスト グループ アドレスに加わるように、エンドポイント デバイスに指示します。マルチキャスト MoH サーバは、どの発信者が保留状態であるかどうかに関係なく、設定されたマルチキャスト MoH オーディオ ソースをそれぞれ連続してストリーミングします。

マルチキャスト MoH は、IPv4 でのみ使用可能です。IPv6 でのマルチキャストは、MoH サーバで現在サポートされていません。

MoH コール フローの詳細については、MoH コール フロー（7-26 ページ）の項を参照してください。

MoH 選択プロセス

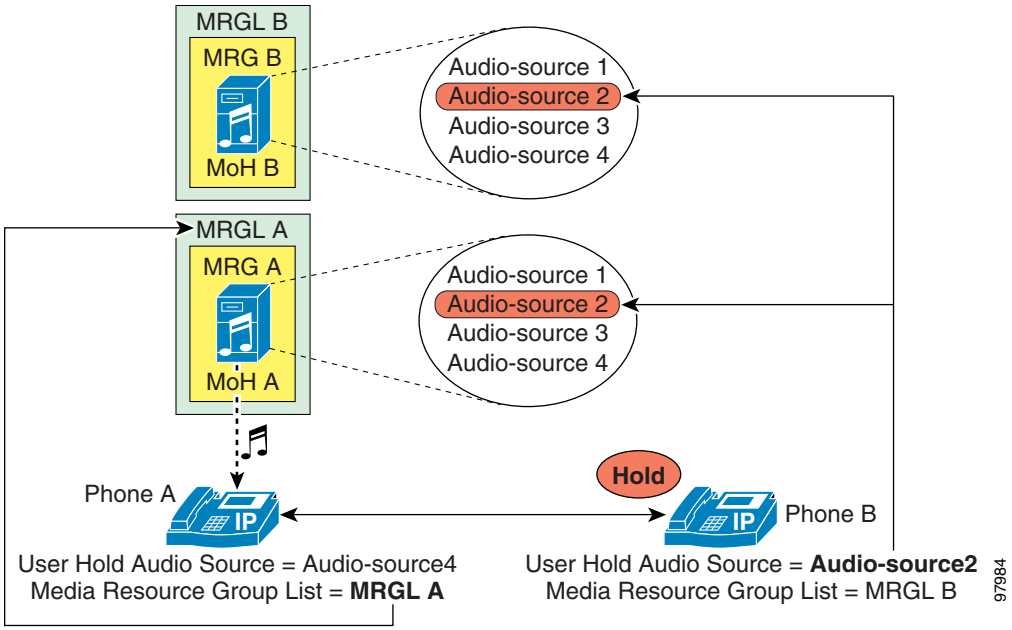
この項では、Unified CM に実装するときの MoH 選択プロセスについて説明します。

Cisco Unified Communication 環境における基本的な MoH の動作は、保留側と被保留側から構成されます。*保留側*とは、通話を保留にするエンドポイント ユーザまたはネットワーク アプリケーションです。一方、*被保留側*とは、保留にされたエンドポイント ユーザまたはデバイスです。

エンドポイントが受信する MoH ストリームは、エンドポイントを保留にするデバイス（保留側）のユーザ保留 MoH オーディオ ソースと、保留にされたエンドポイント（被保留側）に設定されたメディア リソース グループ リスト（MRGL）との組み合わせによって決まります。保留側に対して設定されたユーザ保留 MoH オーディオ ソースによって、保留側が通話を保留にしたときに流されるオーディオ ファイルが決まります。被保留側に設定された MRGL は、被保留側が MoH ストリームを受信する元のリソースまたはサーバを指定します。

図 7-3 の例に示すように、電話機 A および B が通話中であるときに、電話機 B（保留側）で電話機 A（被保留側）を保留にする場合、電話機 A には、電話機 B に対して設定された MoH オーディオ ソース（オーディオソース 2）が聞こえます。ただし、電話機 A はこの MoH オーディオ ストリームを、電話機 A に対して設定された MRGL（リソースまたはサーバ）（MRGL A）から受信します。

図 7-3　　ユーザ保留オーディオ ソースとメディア リソース グループ リスト（MRGL）



設定した MRGL により、ユニキャスト専用デバイスが MoH ストリームを受信するサーバが決まるので、ユニキャスト専用デバイスを設定する場合は、ユニキャスト MoH リソースまたはメディア リソース グループ（MRG）を指定する MRGL を使用する必要があります。同様に、マルチキャスト機能を持つデバイスは、マルチキャスト用に設定された MoH サーバが含まれたマルチキャスト MRG を指定する MRGL を使用して設定する必要があります。

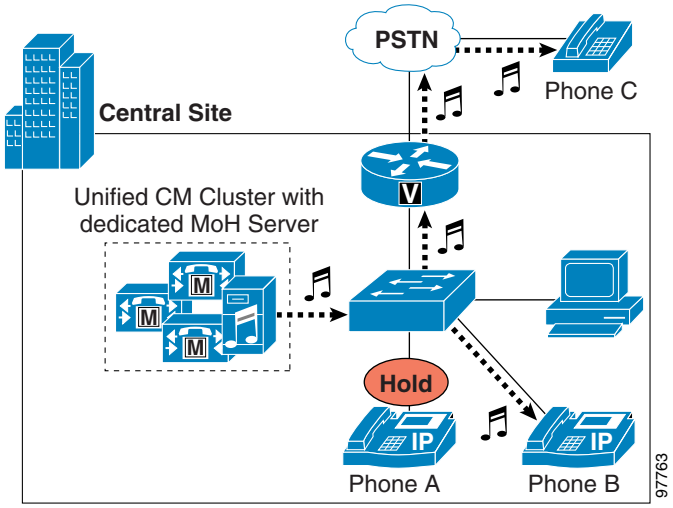
ユーザ保留とネットワーク保留

ユーザ保留には次のタイプがあります。

- IP Phone またはその他のエンドポイント デバイスでのユーザ保留
- MoH がゲートウェイにストリーミングされる PSTN でのユーザ保留

図 7-4 は、これらの 2 つのタイプのコール フローを示しています。電話機 A が電話機 B と通話中であるときに、電話機 A（保留側）で [Hold] ソフトキーを押すと、MoH サーバから電話機 B（被保留側）に音楽ストリームが送信されます。この音楽ストリームは、IP ネットワーク内の被保留側だけでなく、電話機 A が電話機 C を保留にする場合と同様に、PSTN 上の被保留側にも送信できます。電話機 C の場合、MoH ストリームは音声ゲートウェイ インターフェイスに送信され、PSTN 電話機に適したフォーマットに変換されます。電話機 A が [Resume] ソフトキーを押すと、被保留側（電話機 B または C）は、音楽ストリームから切り離され、電話機 A に再び接続されます。

図 7-4　　ユーザ保留の基本的な例



ネットワーク保留は、次のようなシナリオで発生する可能性があります。

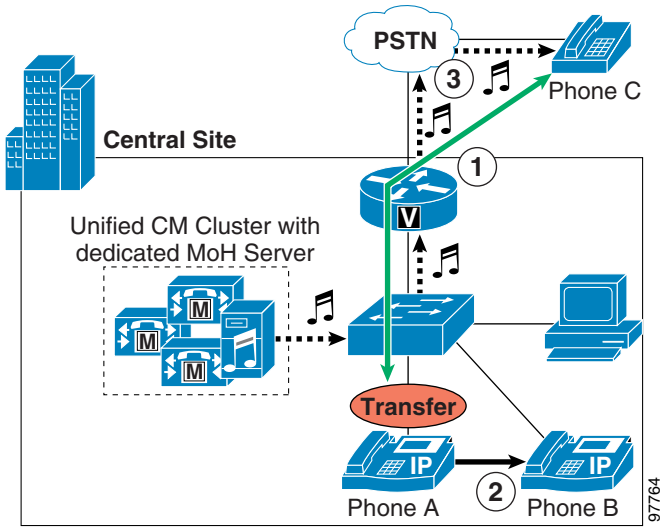
- コール転送
- コール パーク
- 会議セットアップ
- アプリケーションベースの保留

図 7-5 に、コール転送中のネットワーク保留の例を示します。コール フローは、次の手順で構成されます。

1. 電話機 A が PSTN 電話機 C からのコールを受信します。
2. 電話機 A がコールに応答し、電話機 B に転送します。転送プロセスの進行中に、電話機 C はネットワーク保留になります。
3. 電話機 C は、MoH サーバからゲートウェイ経由で MoH ストリームを受信します。電話機 A が転送アクションを完了したあと、電話機 C は音楽ストリームから切り離され、電話機 B に転送されます。

このプロセスは、コール パークや会議セットアップなどの他のネットワーク保留操作の場合と同じです。

図 7-5　　コール転送のネットワーク保留の基本的な例



MoH ソース

Unified CM MoH サーバでは、2 つのタイプのソースから MoH ストリームを生成できます。

- Unified CM MoH サーバにアップロードされたオーディオ ファイル。
- マルチキャストをサポートする Cisco IOS ルータまたはサードパーティのデバイス サポートからのライブ固定オーディオ ソースまたはオーディオ ファイル。Unified CM では、外部のマルチキャスト オーディオ ソースを Unified CM MoH オーディオ ソースとして使用して、CD、ラジオ、ジュークボックスなどの外部オーディオ ソースからライブ保留音を提供することができます。

Unified CM クラスタごとに最大で 501 個の MoH オーディオ ソースを設定できます。そのうちの 1 つ（51 番目）は固定ライブ ソースとして識別されます。IPv4 またはデュアルモードの IPv4/IPv6 メディア アドレスのサポートを提供するために、MoH サーバは Unified CM クラスタに登録します。

オーディオ ファイル

オーディオ ファイル（.wav 形式）を Unified CM にアップロードし、MoH コーデックの MoH オーディオ ソース ファイルを自動的に生成することができます。Unified CM では、MoH ストリーム用に G711（a-law および mu-law）、G.729 Annex A、および Cisco L16 ワイドバンド コーデックをサポートしています。アップロードしたオーディオ ファイルは、16 ビットの PCM 形式または 8 ビットの G.711（a-law/mu-law）形式にする必要があります。

(注)　MoH オーディオ ソースを設定する前に、Unified CM Administration インターフェイスのファイルのアップロード機能を使用して、クラスタ内のすべての MoH サーバに .wav 形式のオーディオ ソース ファイルをアップロードする必要があります。最初にオーディオ ソース ファイルをクラスタ内の各 MoH サーバにアップロードし、次にそのオーディオ ファイルをパブリッシャ（MoH サーバでなくてもかまいません）にアップロードし、最後にそのパブリッシャ上の Unified CM Administration インターフェイスで MoH オーディオ ストリーム番号を割り当て、MoH オーディオ ソースを設定することを推奨します。これによって、各 MoH サーバは、MoH オーディオ ストリーム番号に割り当てられている場合に MoH オーディオ ファイルを使用できるようになります。

固定ソース

録音されたオーディオまたはライブ オーディオが必要な場合、マルチキャストをサポートする Cisco IOS ルータまたはサードパーティ デバイスのアナログ インターフェイスに接続されている固定ライブ ソースからマルチキャスト MoH を生成できます。

(注)　Unified CM ノードが仮想化される際の MoH 用の USB ポートがサポートされていないため、Cisco Unified CM は、MOH サーバへの固定ライブ オーディオ ソース接続用 USB サウンド カードをサポートしなくなりました。

このメカニズムにより、ラジオ、CD プレーヤー、または互換性があるその他のサウンド ソースを使用して、マルチキャスト MoH をストリーミングできます。固定オーディオ ソースからのストリームは、Cisco IOS ルータによってリアルタイムにトランスコードされます。

(注)　保留音を送信するときに固定オーディオ ソースを使用する場合は、事前に、著作権のあるオーディオ素材の再ブロードキャストについて、その適法性および問題を検討しておく必要があります。起こりうる問題については、貴社の法務部門に相談してください。

Cisco IOS ルータからのライブ MoH の詳細については、次の URL で入手可能な最新バージョンの『*Cisco Unified SCCP and SIP SRST System Administrator Guide*』の「*MoH from a Live Feed*」の項を参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html

外部マルチキャスト ソースの再ブロードキャスト

Cisco Unified CM 11.5 から、Cisco IOS ルータは .wav ファイルまたは外付けオーディオ ソースからマルチキャスト オーディオ RTP ストリームを提供するように設定できるようになりました。オーディオ ソースは .wav ファイル、CD プレーヤー、ラジオ、または Cisco IOS ルータに接続されている他のオーディオ デバイスから取得できます。

(注)　この機能は、既存の Unified CM の「固定オーディオ ソース」（#51）に影響しません。そのソースはそのまま維持され、Cisco IOS ルータからストリームされる固定ライブ ソースまたはオーディオ ファイル マルチキャストとして使用できます。

この機能では、Unified CM MOH オーディオ ソース設定オプション内に 1 つ以上の外部マルチキャスト ソースを設定する機能が提供されます。この機能を使用して、Unified CM は外部オーディオ ソースが接続されている Cisco IOS ルータから 1 つ以上のマルチキャスト RTP ストリームを受信します。次に、Unified CM は、受信したマルチキャスト RTP ストリームを保留された発信者に送信します。

Unified CM MoH オーディオ ソースの設定内で、.wav ファイルをオーディオ ソースとして使用するように MoH オーディオ ソースを設定する代わりに、外部（マルチキャスト）の IP: PORT をオーディオ ソースとして使用するように割り当てることができます。これによって、発信者は Cisco IOS ルータの E&M ポートに接続された外部マルチキャスト ソースからストリーミングされた保留音を聞くことができます。（図 7-6 を参照）。複数の Unified CM MoH オーディオ ソースで同じ外部マルチキャスト オーディオ ソースを使用できます。

図 7-6　　外部マルチキャスト MoH ソース

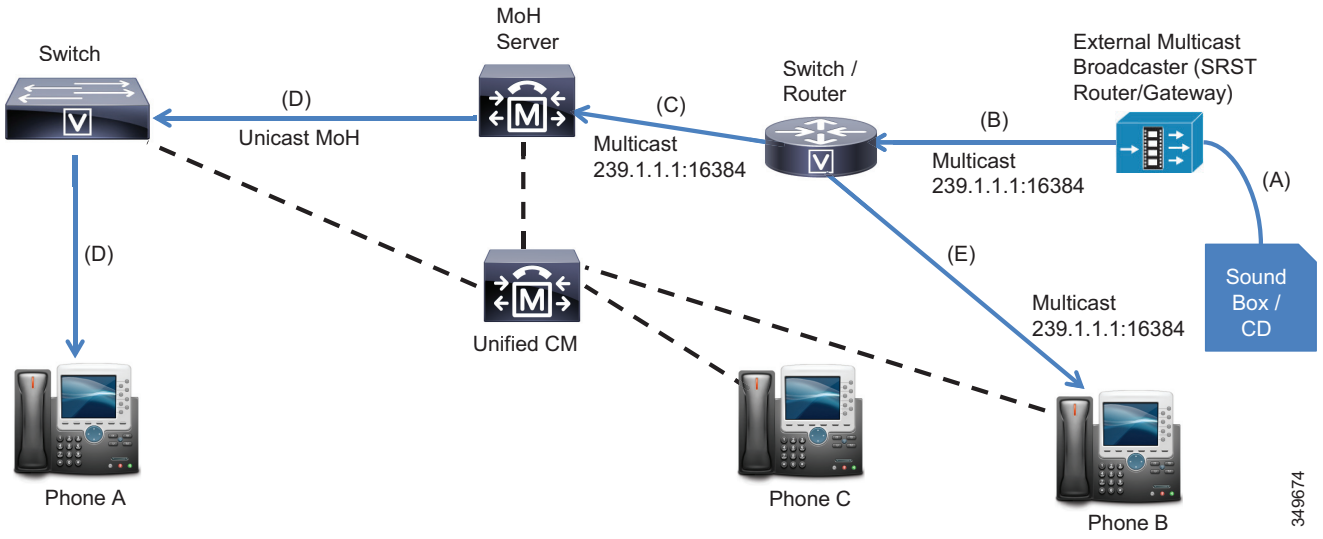


図 7-6 に、外部マルチキャスト MoH ソースを使用する場合のネットワーク フローを示します。示されているように、音楽ソースが Cisco SRST ルータの E&M ポートに接続され（A）、ネットワーク マルチキャスト グループ 239.1.1.1:16384（B）に音声がブロードキャストされるように設定されています。MoH サーバは、マルチキャスト グループ（C）を受信し、ユニキャスト RTP MoH ストリーム（D）を保留された電話機 A に再ブロードキャストするように設定されています。

オプションで、MoH サーバは、Cisco SRST ルータが外部オーディオ ソースをブロードキャストするために使用しているものと同じマルチキャスト グループ アドレスで設定されたオーディオ ソースを持つことができます。マルチキャスト MoH サーバとオーディオ ソースが同じマルチキャスト グループ アドレスで設定されている場合、電話機 B が保留中になると、電話機 B は SRST ルータ経由の元のマルチキャスト ストリーム（B）ブロードキャストからのマルチキャスト RTP オーディオ ストリーム（E）を受信します。この場合、宛先マルチキャスト IP アドレス グループが SRST ルータ経由の外部オーディオ ソース マルチキャスト ストリーム（B）ブロードキャストと同じであることが認識されるため、MoH サーバは音声を送信しません。また、Unified CM でオーディオ ソースに対して別のマルチキャスト IP アドレスを指定することもできます。この場合、MoH サーバは、ネットワークから受信する元のマルチキャスト ブロードキャスト オーディオ ストリーム（C）を使用して別個のマルチキャスト ストリームを再ブロードキャストします。

MoH の選択

個々のケースにユーザ オーディオ ソース設定値とネットワーク オーディオ ソース設定値のいずれかを適用するか決定するために、Unified CM は、次の優先順位で、*保留側*デバイスに対するこれらの設定値を使用します。

1. ディレクトリまたは回線設定（ゲートウェイなど、回線定義のないデバイスには、このレベルはありません）
2. デバイス設定値
3. 共通のデバイス設定
4. クラスタ全体のデフォルト設定

Unified CM は、*被保留側*デバイスの MRGL 設定値も、次の優先順位で使用します。

1. デバイス設定値
2. デバイス プールの設定値
3. システムのデフォルト MoH リソース

システムのデフォルト MoH リソースは、MRG に割り当てられていないリソースで、常にユニキャストであることに注意してください。

MoH コール フロー

次の各項では、SCCP および SIP エンドポイントの両方について、ユニキャストとマルチキャスト MoH コール フローの詳細な図と説明を示します。次に示すすべてのコール フローは、Unified CM MOH サーバの MoH ストリーミングを示しています。Cisco IOS ルータからのマルチキャスト MoH のストリーミングは示されていませんが、これらのマルチキャスト シナリオのコール フローは通常、Unified CM MoH サーバのマルチキャスト コール フローと同じです。

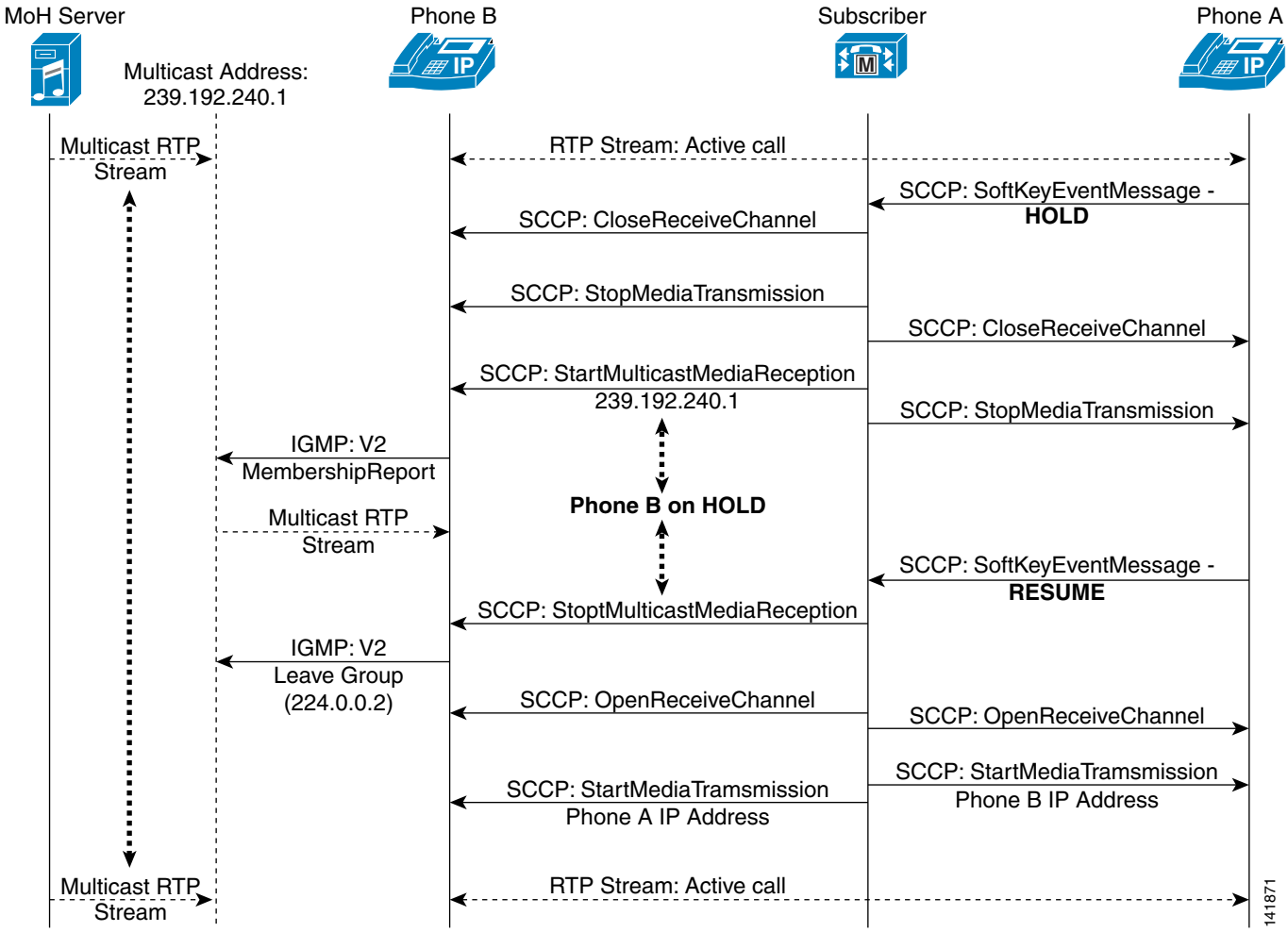
SCCP コール フロー

ここでは、Skinny Client Control Protocol（SCCP）エンドポイントでの、保留音のマルチキャストおよびユニキャストのコール フローについて説明します。

SCCP マルチキャスト コール フロー

図 7-7 は、標準的な SCCP マルチキャスト コール フローを示しています。この図に示されているように、電話機 A で [Hold] ソフトキーが押されると、Unified CM は、Close Receive Channel（受信チャネルのクローズ）と Stop Media Transmission（メディア送信の停止）を電話機 A と電話機 B の両方に指示します。このアクションは、実質的に、RTP 双方向オーディオ ストリームを停止させます。次に、Unified CM は、マルチキャスト グループ アドレス 239.192.240.1 から、Start Multicast Media Reception（マルチキャスト メディア受信の開始）を電話機 B（被保留側）に指示します。その後、電話機 B はインターネット グループ管理プロトコル（IGMP）V2 の Membership Report メッセージを発行して、電話機 B がこのグループに加わることを示します。

図 7-7　SCCP マルチキャスト MoH コール フローの詳細



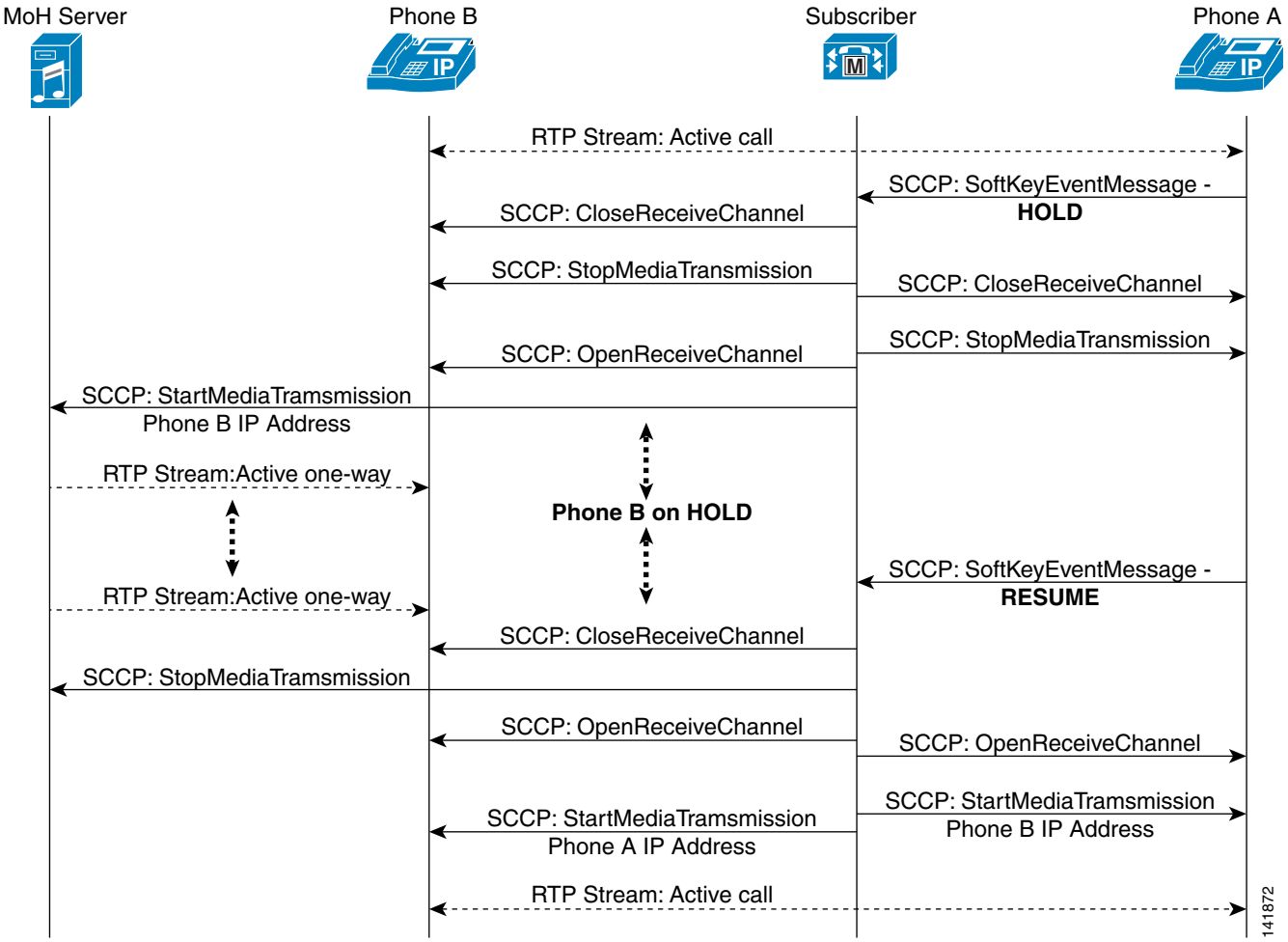
一方、MoH サーバがこのマルチキャスト グループ アドレスに RTP オーディオを送信しているので、電話機 B はそのマルチキャスト グループに加わった後、MoH ストリームの受信を開始します。電話機 A で [Resume] ソフトキーが押されると、Unified CM は、電話機 B に Stop Multicast Media Reception（マルチキャスト メディア受信の停止）を指示します。電話機 B は、マルチキャスト ストリームが必要なくなったことを示すために、IGMP V2 の Leave Group メッセージを 224.0.0.2 に送信します。これにより、実質的に MoH セッションが終了します。次に、Unified CM は、電話機 A と電話機 B 間の通話の開始時に送信するように、両方の電話機に一連の Open Receive Channel（受信チャネルのオープン）メッセージを送信します。その後すぐに、Unified CM は、互いの IP アドレスへの Start Media Transmission（メディア送信の開始）を両方の電話機に指示します。電話機は、RTP 双方向オーディオ ストリームによって再び接続されます。

（注） 図 7-7 と図 7-8 のコール フロー図では、電話機 A と電話機 B の間に双方向 RTP オーディオ ストリームがあるコールを前提としています。これらの図は、コール フローを示しているので、適切な MoH 動作に必要な関連トラフィックのみが記載されています。したがって、インタラクションがわかりやすいように、キープアライブ、確認応答、およびその他のトラフィックは省略されています。各図の初期化イベントは、電話機 A によって実行される [Hold] ソフトキー アクションです。

SCCP ユニキャスト コール フロー

図 7-8 は、SCCP ユニキャスト MoH コール フローを示しています。このコール フロー図では、電話機 A で [Hold] ソフトキーが押されると、Unified CM は、Close Receive Channel（受信チャネルのクローズ）と Stop Media Transmission（メディア送信の停止）を電話機 A と電話機 B の両方に指示します。このアクションは、実質的に、RTP 双方向オーディオ ストリームを停止させます。この時点まで、ユニキャストとマルチキャストの MoH コール フローは、まったく同じように動作します。

図 7-8　SCCP ユニキャスト MoH コール フローの詳細



次に、Unified CM は、Open Receive Channel（受信チャネルのオープン）を電話機 B（被保留側）に指示します。（これは、マルチキャストの場合とまったく異なっています。マルチキャストでは、Unified CM は、Start Multicast Media Reception（マルチキャスト メディア受信の開始）を被保留側に指示します）。次に、Unified CM は、MoH サーバに、電話機 B の IP アドレスへの Start Media Transmission（メディア送信の開始）を指示します。（これもまた、マルチキャスト MoH コール フローの動作とは異なります。マルチキャストでは、マルチキャスト グループ アドレスに参加するように電話機にプロンプト表示されます）。この時点で、MoH サーバは電話機 B に一方向のユニキャスト RTP 音楽ストリームを送信しています。電話機 A で [再開（Resume）] ソフトキーが押されると、Unified CM は、Stop Media Transmission（メディア送信の停止）を MoH サーバに指示し、Close Receive Channel（受信チャネルのクローズ）を電話機 B に指示して、実質的に MoH セッションを終了させます。マルチキャスト シナリオの場合と同じように、Unified CM は、一連の Open Receive Channel（受信チャネルのオープン）メッセージおよび Start Media Transmissions（メディア送信の開始）メッセージを電話機 A と電話機 B に相互の IP アドレスを使用して送信します。電話機は、RTP 双方向オーディオ ストリームによって再び接続されます。

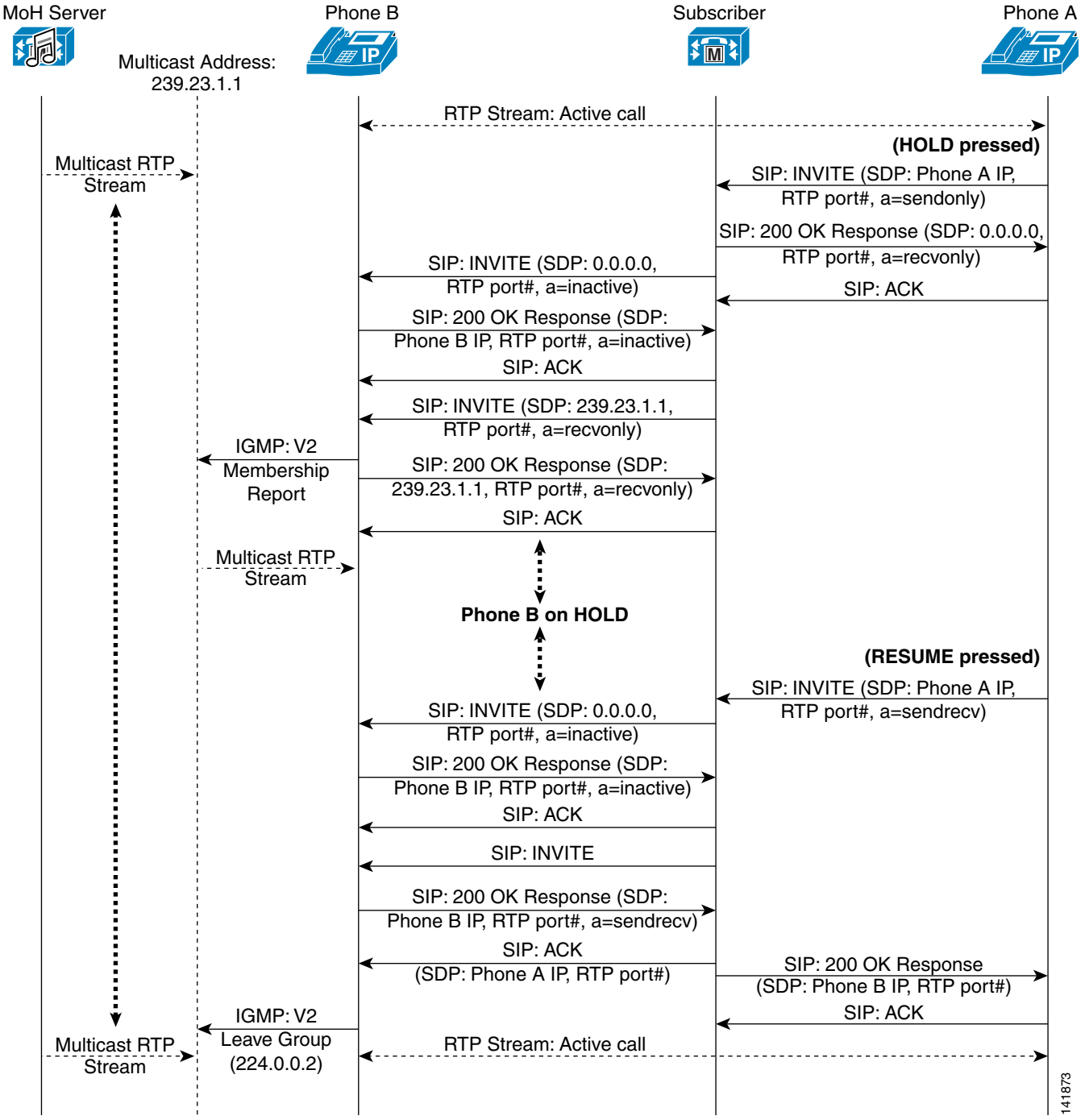
SIP コール フロー

ここでは、Session Initiation Protocol（SIP）エンドポイントでの、保留音のマルチキャストおよびユニキャストのコール フローについて説明します。

SIP マルチキャスト コール フロー

図 7-9 は、標準的な SIP マルチキャスト コール フローを示しています。この図に示されているように、電話機 A で [Hold] ソフトキーが押されると、電話機 A は SIP INVITE を送信します。このときのセッション記述プロトコル（SDP）接続情報は電話機 A の IP アドレスを示し、メディア属性は sendonly を示しています。Unified CM は、SDP 接続情報が 0.0.0.0、メディア属性が recvonly を示す SIP 200 OK Response によって、RTP ストリームを切断するよう電話機 A に指示します。電話機 B は、Unified CM からの SIP INVITE によって RTP ストリームを切断するように指示されます。このときの SDP 接続情報は 0.0.0.0 を示し、メディア属性は inactive です。電話機 B から Unified CM に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されると、Unified CM は SIP INVITE を電話機 B に送信します。このときの SDP 接続情報は MoH マルチキャスト グループ アドレス（この場合は 239.23.1.1）を示し、メディア属性は recvonly です。

図 7-9　　SIP マルチキャスト MoH コール フローの詳細



次に、図 7-9 の電話機 B は IGMP V2 の Membership Report メッセージを発行して、電話機 B がこのマルチキャスト グループに加わることを示します。さらに、電話機 B は、前の SIP INVITE に応答して、SDP メディア属性が sendonly を示す SIP 200 OK Response を Unified CM に返します。一方、MoH サーバがこの MoH マルチキャスト グループ アドレスに RTP オーディオを送信しているので、電話機 B はそのマルチキャスト グループに加わった後、一方向 MoH ストリームの受信を開始します。

電話機 A のユーザが [再開（Resume）] ソフトキーを押すと、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は電話機 A の受信 RTP ポートおよび sendrecv を示しています。Unified CM は、SDP 接続情報が 0.0.0.0、メディア属性が inactive を示す SIP INVITE によって、電話機 B にマルチキャスト MoH ストリームから切断するように指示します。電話機 B から Unified CM に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されます。

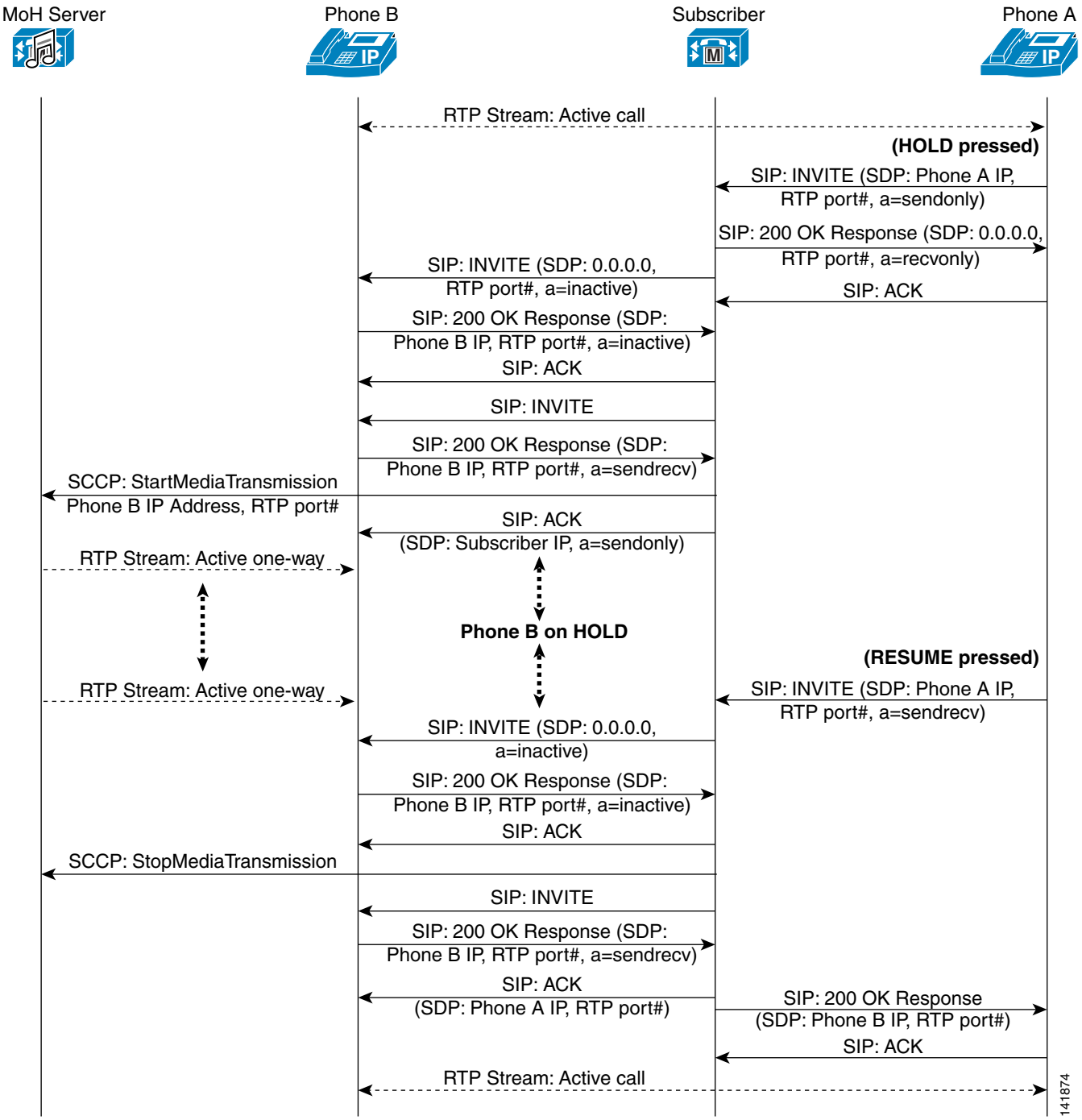
次に、Unified CM は電話機 B に SIP INVITE を送信し、電話機 B はそれに対して、SDP 接続情報が電話機 B の IP アドレスを示し、メディア属性が電話機 B の受信 RTP ポートおよび sendrecv を示す SIP 200 OK Response で応答します。Unified CM はそれに応答し、SDP 接続情報が電話機 A の IP アドレスを示し、メディア属性が電話機 A の受信 RTP ポート番号の SIP ACK を電話機 B に送信します。同様に、Unified CM は、SIP 200 OK Response を電話機 A の最初の保留解除 SIP INVITE に転送します。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポート番号です。電話機 B は、マルチキャスト ストリームが必要なくなったことを示すために、IGMP V2 の Leave Group メッセージを 224.0.0.2 に送信します。最後に、電話機 A と電話機 B の間に RTP 双方向オーディオ ストリームが再確立されます。

（注） 図 7-9 と図 7-10 のコール フロー図では、電話機 A と電話機 B の間に双方向 RTP オーディオ ストリームがあるコールを前提としています。これらの図は、コール フローを示しているので、適切な MoH 動作に必要な関連トラフィックのみが記載されています。したがって、インタラクションがわかりやすいように、キープアライブ、一部の確認応答、進行状況表示、およびその他のトラフィックは省略されています。各図の初期化イベントは、電話機 A によって実行される [Hold] ソフトキー アクションです。

SIP ユニキャスト コール フロー

図 7-10 は、SIP ユニキャスト MoH コール フローを示しています。この図に示されているように、電話機 A で [Hold] ソフトキーが押されると、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は sendonly を示しています。Unified CM は、SDP 接続情報が 0.0.0.0、メディア属性が recvonly を示す SIP 200 OK Response によって、RTP ストリームを切断するよう電話機 A に指示します。電話機 B は、Unified CM からの SIP INVITE によって RTP ストリームを切断するように指示されます。このときの SDP 接続情報は 0.0.0.0 を示し、メディア属性は inactive です。次に、電話機 B から Unified CM に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されます。この時点まで、ユニキャストとマルチキャストの MoH コール フローはまったく同じです。

図 7-10　SIP ユニキャスト MoH コール フローの詳細



Unified CM は電話機 B に SIP INVITE を送信し、電話機 B は、それに対して、SDP 接続情報が電話機 B の IP アドレスを示し、メディア属性が電話機 B の受信 RTP ポート番号および sendrecv を示す SIP 200 OK Response で応答します。Unified CM は、SCCP の StartMediaTransmission メッセージを MoH サーバに送信して、電話機 B のアドレスおよび受信 RTP ポート番号を伝えます。この後、Unified CM から電話機 B への SIP ACK が続き、このときの SDP 接続情報には Unified CM の IP アドレス、メディア属性には sendonly が示されます。一方、MoH サーバが RTP オーディオを送信しているので、電話機 B は一方向 MoH ストリームの受信を開始します。

電話機 A のユーザが [Resume] ソフトキーを押すと、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は電話機 A の受信 RTP ポートおよび sendrecv を示しています。Unified CM は、SDP 接続情報が 0.0.0.0、メディア属性が inactive を示す SIP INVITE によって、電話機 B にマルチキャスト MoH ストリームから切断するように指示します。電話機 B から Unified CM に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されます。その後、Unified CM は、SCCP の StopMediaTransmission メッセージを MoH サーバに送信します。これによって、MoH サーバは電話機 B への MoH ストリームの転送を停止します。

次に、Unified CM は電話機 B に SIP INVITE を送信し、電話機 B はそれに対して、SDP 接続情報が電話機 B の IP アドレスを示し、メディア属性が電話機 B の受信 RTP ポートおよび sendrecv を示す SIP 200 OK Response で応答します。Unified CM はそれに応答し、SDP 接続情報が電話機 A の IP アドレスを示し、メディア属性が電話機 A の受信 RTP ポート番号の SIP ACK を電話機 B に送信します。同様に、Unified CM は、SIP 200 OK Response を電話機 A の最初の保留解除 SIP INVITE に転送します。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポートです。最後に、電話機 A と電話機 B の間に RTP 双方向オーディオ ストリームが再確立されます。

デュプレックス ユニキャスト MoH メディア接続

一部のシナリオでは、保留にされたデバイス（被保留側）と MOH サーバ間に双方向のメディア接続が必要です。Cisco Unified CM サービス パラメータ [デュプレックス ストリーミング有効（Duplex Streaming Enabled）] は、このタイプの接続を有効にするために使用可能です。MoH サーバは、保留にされたエンドポイントから受信した音声をすべて破棄します。たとえば、MoH メディア ストリームが保留にされたデバイスに到達するためにファイアウォールを通過する必要がある場合に、この [デュプレックス ストリーミング有効（Duplex Streaming Enabled）] オプションが必要になります。

メディア リソースのキャパシティ プランニング

この項では、DSP を含む各種ネットワーク モジュールおよびシャーシのキャパシティ、ネットワーク モジュールを含むシャーシのキャパシティ、およびハードウェアに対するソフトウェアの依存性に関する情報を提供します。

すべての Cisco ISR G1 および G2 のキャパシティ プランニングには、https://www.cisco.com/go/dspcalculator から入手できる DSP Calculator を使用します。

ユニファイド コミュニケーション ソリューションの DSP リソースは、NM-HD、NM-HDV、および PVDM モジュールによって提供されます。NM-HD および NM-HDV2 モジュールは、Cisco ISR G1 および G2 シリーズのプラットフォームでサポートされています。これらのモジュールのキャパシティ情報については、それぞれの製品データ シートを参照してください。

PVDM モジュールは、PVDM-256K、PVDM2、PVDM3、および PVDM4 の 4 つのモデルで使用できます。それぞれのモデルに、異なる密度をサポートする複数のモジュールがあります。

ハードウェアベースのメディア リソースに対してキャパシティ プランニングを行う場合に考慮する点として、モジュールの密度、基盤となるプラットフォーム（Cisco ISR G1 または G2）、および必要な Cisco IOS の最小バージョンがあります。

PVDM2 モジュールのキャパシティ情報については、次の URL で入手可能な『*High-Density Packet Voice Digital Signal Processor Module for Cisco Unified Communications Solutions*』データシートを参照してください。

https://www.cisco.com/en/US/prod/collateral/routers/ps5854/product_data_sheet0900aecd8016e845_ps3115_Products_Data_Sheet.html

PVDM3 モジュールのキャパシティ情報については、次の URL で入手可能な PVDM3 プロビジョニング情報を参照してください。

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-ip-service-level-agreements-slas/whitepaper_C11-718333.html

PVDM4 モジュールのキャパシティ情報については、次の URL で入手可能な『*Cisco Fourth-Generation Packet Voice Digital Signal Processor Module for Cisco Unified Communications Solutions Data Sheet*』を参照してください。

https://www.cisco.com/c/en/us/products/routers/4000-series-integrated-services-routers-isr/datasheet-listing.html

保留音のキャパシティ プランニング

MoH リソースのキャパシティ プランニングを行う場合は、MoH リソースのハードウェア キャパシティを認識し、このキャパシティとの関連からマルチキャストとユニキャストの MoH の役割を考慮することが重要です。MoH サーバのキャパシティは、配置モデル（共存またはスタンドアロン）、基盤となるサーバ プラットフォームなどの複数の要因に依存します。

共存 MoH サーバとスタンドアロン MoH

MoH 機能を利用するには、Unified CM クラスタに含まれているサーバを使用する必要があります。MoH サーバは、次のいずれかの方法で設定できます。

- 共存配置

  「*共存*」という用語は、同じサーバ上で複数のサービスまたはアプリケーションが実行されている状態を指します。共存配置では、MoH 機能は Unified CM ソフトウェアも実行している、クラスタ内の任意のサーバ（パブリッシャまたはサブスクライバ）で実行されます。

- スタンドアロン配置

  スタンドアロン配置では、MoH 機能は Unified CM クラスタ内の専用のメディア リソース サーバ ノードに置かれます。このサーバは、パブリッシャとしてもサブスクライバとしても機能しません。つまり、Cisco IP Voice Media Streaming Application サービスが、そのサーバ上で使用できる唯一のサービスとなります。この専用サーバの機能は、MoH ストリームをネットワーク内のデバイスに送信することだけです。

サーバ プラットフォームの制限

Cisco Unified Communications Manager は、スタンドアロン配置で 7.5K または 10K の Open Virtualization Archive（OVA）テンプレートを使用して、Cisco Unified Computing System（UCS）の C シリーズまたは B シリーズで最大 1,000 の MoH ストリームをサポートします。他のプラットフォームでは、Unified CM は、その他のサービスがサーバでアクティブであるかによって、その量の半分以下をサポートできます。MoH セッションがこの最大同時セッション数を超えてから、さらに負荷が増えると、MoH 品質の低下、不規則な MoH 動作、または MoH 機能の喪失までも発生するおそれがあるので、ネットワークのコール量が最大同時セッション数を超えないようにしてください。Unified CM クラスタごとに最大 500 の固有オーディオ ソースを設定できることに注意してください。

各サーバ プラットフォームでサポートされる MoH オーディオ ソースおよびセッションの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章で、メディア リソース（25-30 ページ）の項を参照してください。

次の 2 つの MoH サーバ設定パラメータは、MoH サーバのキャパシティに影響を与えます。

- **最大半二重ストリーム (Maximum Half Duplex Streams)**

  このパラメータにより、ユニキャスト MoH に配置できるデバイスの数が決まります。デフォルトでは、この値は 250 に設定されています。

  Maximum Half Duplex Streams パラメータは、次の公式から得られた値に設定する必要があります。

  （サーバおよび配置キャパシティ）–（（マルチキャスト MoH ソースの数）＊（有効な MoH コーデックの数））

  次に例を示します。

10K OVA スタンドアロン MoH サーバを使用した Cisco Unified Computing System（UCS）	マルチキャスト MoH オーディオ ソース	有効な MoH コーデック（G.711 mu-law と G.729）	Maximum Half Duplex Streams
1,000	- (12	＊ 2)	= **976**

  したがって、この例では、Maximum Half Duplex Streams パラメータは 976 未満の値で設定されます。マルチキャスト MoH オーディオ ソースのそれぞれに、有効な各 MoH コーデック用に作成された自動マルチキャスト RTP ストリームがあります。

- **Maximum Multicast Connections**

  このパラメータにより、マルチキャスト MoH に配置できるデバイスの数が決まります。

  Maximum Multicast Connections パラメータは、必要に応じてすべてのデバイスを確実にマルチキャスト MoH に配置できるような数に設定する必要があります。MoH サーバはマルチキャスト ストリームの有限数だけを生成することができますが、多数の保留デバイスを各マルチキャスト ストリームに加えることもできます。このパラメータは、同時にマルチキャスト MoH に配置される可能性のあるデバイスの数、またはそれよりも大きい数に設定する必要があります。一般的なマルチキャスト トラフィックは、生成されるストリームの数に基づいて決まりますが、Unified CM では、マルチキャスト MoH に実際に配置されたデバイスの数または各マルチキャスト MoH ストリームに加えられたデバイスの数が適用されます。この方式は、マルチキャスト トラフィックが通常トラッキングされる方法と異なりますが、このパラメータを適切に設定することが重要です。

これらのパラメータを適切に設定しないと、MoH サーバ リソースが十分に使用されない、またはサーバがネットワーク負荷を処理できないといった問題が発生する可能性があります。サービス パラメータの設定方法については、次の URL で入手可能な『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

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

（注）　MOH サーバごとに 1,000 セッションの最大限度数は、ユニキャスト、マルチキャスト、またはユニキャストとマルチキャストの同時 RTP ストリームに適用されます。制限は、トランスポート メカニズムに関係なく、プラットフォームがサポートできる MoH ストリームの推奨最大数を表します。

リソースのプロビジョニング

共存またはスタンドアロンの MoH サーバ設定のプロビジョニングを行う場合、ネットワーク管理者は、MoH オーディオ ストリームに使用されるトランスポート メカニズムのタイプを考慮する必要があります。ユニキャスト MoH を使用する場合、保留される各デバイスには、別々の MoH ストリームが必要です。しかし、マルチキャスト MoH と単一のオーディオ ソースのみを使用する場合、保留にするタイプのデバイス数に関係なく、設定されている MoH コーデック タイプごとに必要な MoH ストリームは 1 つだけです。

たとえば、30,000 台の電話機のあるクラスタがあり、保留率が 2 % である（すべてのエンドポイント デバイスの 2 % だけが、常に保留になる）場合、600 の MoH ストリームまたはセッションが必要です。ユニキャスト専用の MoH 環境の場合、この負荷を処理するために、10K OVA テンプレートを使用した Cisco Unified Computing System（UCS）で動作する 1 つの共存（またはスタンドアロン）MoH サーバが必要です。

比較すると、36 の固有 MoH オーディオ ストリームがあるマルチキャスト専用 MoH 環境は、たとえば、1 つの共存 MoH サーバが必要です。36 の固有マルチキャスト ストリームは、次のいずれかの方法でプロビジョニングできます。

- 単一のコーデックを使用して 36 の固有オーディオ ソースをストリーミングする。
- 2 つのコーデックだけを使用して 18 の固有オーディオ ソースをストリーミングする。
- 3 つのコーデックだけを使用して 12 の固有オーディオ ソースをストリーミングする。
- 4 つのコーデックすべてを使用して 9 つの固有オーディオ ソースをストリーミングする。

上記の例では、2 % の保留率は、30,000 台の電話機に基づくものであり、保留になる可能性があるネットワーク内のゲートウェイまたはその他のエンドポイント デバイスを考慮していません。こうしたその他のデバイスは、電話機と同じように保留になる可能性があるので、保留率を計算するときは、これらのデバイスも考慮する必要があります。

上記の計算では、MoH サーバの冗長性を見込んでいません。MoH サーバに障害が発生する場合、またはユーザの 2% 以上が同時に保留になる場合、このシナリオでは、オーバーフローが発生したり負荷が増えたときに処理するための MoH リソースがありません。MoH リソースの計算には、冗長性に配慮して十分に余裕のあるキャパシティを含める必要があります。追加の MoH サーバは、メディア リソースのハイ アベイラビリティ（7-37 ページ）の項で説明されているように、冗長性またはハイ アベイラビリティ用にプロビジョニングできます。

メディア リソースのハイ アベイラビリティ

Unified CM のメディア リソース グループ（MRG）とメディア リソース グループ リスト（MRGL）のコンストラクトは、この章で説明されているリソースの編成とアクセスの方法を制御するために使用されます。この項では、これらのコンストラクトを効率的に利用する方法について説明します。

メディア リソース グループとメディア リソース グループ リスト

メディア リソース グループ（MRG）とメディア リソース グループ リスト（MRGL）は、リソースの割り当て方法を制御する方式を提供するもので、リソースに対するアクセス権、リソースの場所、特定のアプリケーションのリソース タイプが含まれます。この項では、読者がメディア リソース グループおよびメディア リソース グループ リストを理解しているものとして、次の設計上の考慮事項について詳しく説明します。

- ユーザ インターフェイスに表示されないデフォルトのメディア リソース グループがシステムによって定義されます。すべてのリソースが、作成時にこのデフォルトの MRG のメンバーになります。MRG を使用してリソースへのアクセスを制御する場合は、リソースを明示的に別の MRG に設定することによって、デフォルト MRG の外に移動する必要があります。すべてのコールに対する最後の手段としてのみリソースを使用できるようにする場合は、そのリソースをデフォルト グループに残しておくことができます。また、リソースの制御が必要ない場合も、デフォルト グループに残しておくことができます。
- メディア リソースの使用側は、まず、設定で指定されている任意のメディア リソース グループ（MRG）またはメディア リソース グループ リスト（MRGL）のリソースを使用します。必要なリソースが使用できない場合、デフォルト MRG でリソースが検索されます。単純な配置では、デフォルトの MRG だけを使用することがあります。
- メディア リソース グループ（MRG）とメディア リソース グループ リスト（MRGL）を使用して、複数の Unified CM 間でリソースを共有します。MRG と MRGL を使用しない場合、リソースは、1 つの Unified CM からしか使用できません。
- MRGL は、設定にリストされている順序で MRG を使用します。ある MRG に必要なリソースがない場合、次の MRG が検索されます。すべての MRG が検索され、リソースが見つからない場合、検索は終了します。
- Unified CM Administration で MRG 内のデバイスがアルファベット順に表示されていても、MRG 内では、リソースは設定順序に基づいて割り当てられます。メディア リソースを特定の順序で割り当てるには、リソースごとに別の MRG を作成し、MRGL を使用して割り当て順序を指定することを推奨します。
- MRG 内に同じタイプのリソースを提供するデバイスが複数存在する場合、そのリソースを割り当てるアルゴリズムによって、これらすべてのデバイス間でロード バランシングが行われます。Cisco Unified CM は、設定された MTP またはトランスコーダ リソースの数のパーセンテージを定義する、[MTP およびトランスコーダ リソース スロットリング パーセンテージ（MTP and Transcoder Resource Throttling Percentage）] サービス パラメータを使用して、MTP およびトランスコーダ リソース全体でロード バランシングを行うスロットリング メカニズムを使用します。アクティブな MTP またはトランスコーダ リソースの数がこのパラメータに設定されている割合以上である場合、Cisco Unified CM はコールの両端で一致するコーデックを使用するリソースを検出するために、1 回このリソースおよびハントに MRGL（デフォルトを含む MRG）によるコールの送信を停止します。Cisco Unified CM が一致するコーデックの使用可能なリソースを検出できない場合、調整された状態にコールの機能の小さいサブセットと一致し、これらのリソースを含む検索を繰り返す場合は、MRGL の最上位に戻されます。Cisco Unified CM は、コールに最適な一致であるリソースにこのようなリソースが使用可能なときにコールをリソースに発信します。コールは、Cisco Unified CM がコールのリソースを割り当てることができない場合に失敗します。

- Unified CM サーバベースのソフトウェア MTP はデフォルトでパススルー モードがイネーブルです。Cisco IOS Enhanced MTP デバイスは、コーデック パススルー モードまたは非コーデック パススルー モードをサポートするように設定できます。コーデック パススルーの MTP が必要な場合、Unified CM は Real-Time Transport Protocol パススルー（RTCP PT）機能を持つ MTP を見つけるために、最初の繰り返し処理で MRGL（デフォルト MRG を含む）を検索します。必要な RTCP パススルー機能を持つ MTP が見つからなければ、Unified CM は今度はパススルー機能を対象に再度 MTP リストを調べます。必要なパススルー機能を持つ MTP が見つからなければ、Unified CM はパススルー機能を対象とせずに再び MTP リストを調べます。
- MRG には、複数のタイプのリソースが含まれていることがあります。必要な機能に基づいて、適切なリソースがグループから割り当てられます。MTP とトランスコーダは、特別な例です。トランスコーダは MTP としても使用できます。たとえば、MTP とトランスコーダの両方が同じ MRG に存在していて MTP が要求されている場合、リソースが MRG に出現する順序に基づいて割り当てが行われます。トランスコーダ デバイスが MRG 内で MTP よりも前に出現している場合、トランスコーダ リソースが使い果たされるまでトランスコーダ リソースが MTP 要求に割り当てられ、その後、MTP の割り当てが開始されます。このため、MRG および MRGL を作成するときにリソースの順序を考慮することが重要です。
- MRG を使用して、同様のタイプのリソースをグループ化することもできます。上記の例で説明したように、トランスコーダがより高価なリソースであるため、シスコでは、トランスコーダおよび MTP を別の MRG にグループ化し、適切な順序で MRGL に MRG を追加して、正しいリソースを呼び出すことを推奨します。
- また、MRG と MRGL を使用すると、地理的なロケーションに基づいてリソースを分離できます。その結果、WAN 帯域幅を節約できる場合もあります。
- メディア リソース自身には、別のメディア リソースを呼び出さない設定が必要です。たとえば、MTP がコールに挿入され、この MTP で設定されているコーデックが、このコールに対して Unified CM が必要とするコーデックと異なる場合、トランスコーダも呼び出されます。よくある間違いは、Unified CM が G.729a を必要とする場合に、MTP を G.729 または G.729b に設定することです。

Cisco IOS ベースのメディア リソースの冗長性とフェールオーバーに関する考慮事項

メディア リソースに関するハイ アベイラビリティ設計には、冗長なメディア リソースを含める必要があります。これらのリソースが Cisco IOS ベースのリソースである場合は、単一プラットフォームの障害を防ぐために各リソースを複数の Cisco IOS プラットフォームに分散できます。また、各リソースを異なるプライマリ Unified CM サーバに登録することも可能です。

Cisco IOS は、フェールオーバー機能のモードとして「グレースフル」と「即時」の 2 種類をサポートしています。デフォルトのフェールオーバー方法はグレースフルで、この場合はすべてのメディア アクティビティが停止して初めてリソースがバックアップ Unified CM サーバに登録されます。それに対して即時フェールオーバーでは、プライマリの障害が検出されるとすぐにリソースがバックアップ Unified CM サーバに登録されます。冗長性のない 1 組のメディア リソースしかない状況では、即時フェールオーバーを使用することを推奨します。

トランスコーダのハイ アベイラビリティ

次のトランスコーダのフェールオーバー プロセスは、デバイスが登録されている Cisco Unified CM が使用できなくなると実行されます。

プライマリ Unified CM に障害が発生した場合、トランスコーダ デバイスは、そのデバイスの Cisco Unified CM グループに定義されているセカンダリ Unified CM ノードに登録しようとします。トランスコーダ デバイスは、プライマリ Unified CM が再度使用可能になるとすぐにフォールバックします。その Unified CM にあったコールがリスト内の次の Unified CM に登録されます。

保留音のハイ アベイラビリティ

完全な冗長性のある MoH 動作を確保するために複数の MoH サーバを設定し、配置することを推奨します。最初の MoH サーバに障害が発生したり、要求を処理するために必要なリソースがなくなったために使用不能になると、2 番めのサーバが自動的に MoH 機能を引き継ぎ、要求に応答します。適切な冗長構成のために、クラスタ内の 2 つ以上の MoH サーバから各 MRG にリソースを割り当ててください。

マルチキャストとユニキャストの両方の MoH が必要な環境では、ネットワーク内のすべてのエンドポイントの MoH 冗長性が確保されるように、必ず両方のトランスポート タイプに冗長性をもたせてください。

メディア リソースの設計に関する留意点

この項では、さまざまな Unified CM 配置モデルと一緒に使用するメディア リソースの配置に関する留意点について検討します。また、Unified CM 実装でのメディア リソース割り当てに関する堅牢なソリューションの設計に役立つ、設定上の留意点とベスト プラクティスについても取り上げます。

配置モデル

ここでは、MTP リソースとトランスコーディング リソースが、いつどの場所で使用されるかについて説明します。具体的には、次の 3 つの企業 IP テレフォニー配置のモデルで示します。

- 単一サイト配置（7-39 ページ）
- 集中型呼処理を使用するマルチサイト配置（7-40 ページ）
- 分散型呼処理を使用するマルチサイト配置（7-41 ページ）

単一サイト配置

単一サイト配置では、低ビット レート（LBR）コーデックを使用する根拠となっている低速リンクが不要のため、トランスコーディングの必要はありません。H.323v2 に準拠していない相当数のデバイス（旧バージョンの Microsoft NetMeeting や特定のビデオ デバイスなど）が存在する場合、何らかの MTP リソースが必要なことがあります。SIP エンドポイントがある場合は、DTMF 変換用に MTP リソースが必要になることがあります（Named Telephony Event（RFC 2833）（7-8 ページ）を参照）。

単一サイト展開では、Unified CM が SCCP ベースの Cisco Unified IP Phone 7940 または 7960 からの着信コールを受信した場合、コールが開始されると発信デバイスのメディア機能を使用できず、SIP PSTN サービス プロバイダーのほとんどにアーリー オファーが必要になります。この場合、Unified CM は、MTP を挿入し、その IP アドレスと UDP ポート番号を使用して、(リージョン ペアのフィルタリング後の) サポートされるすべてのオーディオ コーデックを、発信 SIP トランク上で送信される初期 INVITE のオファー SDP にアドバタイズする必要があります。

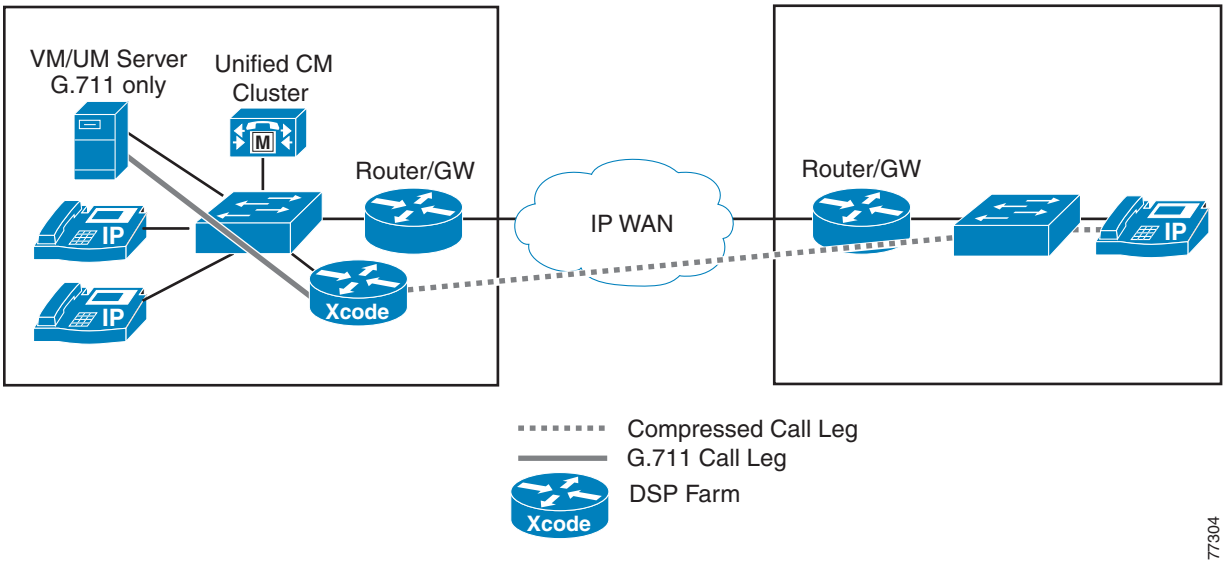
集中型呼処理を使用するマルチサイト配置

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

WAN 帯域幅は一般に制限されるので、WAN を通過するときは、G.729 などの低ビット レート コーデックを使用するようにコールが設定されます (図 7-11 を参照)。

IP Phone 間の音声圧縮は、Unified CM の *リージョン*と *ロケーション*を使用して簡単に設定されます。リージョンは、そのリージョン内のデバイスが使用する圧縮のタイプ (たとえば、G.711 または G.729) を指定します。ロケーションは、そのロケーションのデバイスに出入りするコールに使用可能な、合計帯域幅量を指定します。

図 7-11　　集中型呼処理を使用する WAN のトランスコーディング



Unified CM は、MRG (メディア リソース グループ) を使用して、クラスタ内の Unified CM サーバ間で、MTP リソースとトランスコーディング リソースの共有を可能にします。さらに、異なるリージョンを通過するコールに LBR コーデック (たとえば、G.729a) を使用する場合、トランスコーディング リソースが使用されるのは、エンドポイントの一方 (または両方) が、LBR コーデックを使用できない場合だけです。

図 7-11 では、Unified CM がトランスコーダが必要であることを認識し、高帯域幅コーデックを使用するデバイスの MRGL または MRG に基づいてトランスコーダを割り当てます。この場合、VM/UM サーバが、使用するトランスコーダ デバイスを決定します。この Unified CM の動作は、トランスコーダ リソースが高帯域幅デバイスの近くに正しく配置されていることを前提としています。VM/UM サーバ用のトランスコーダがリモート サイトに配置されるようにこのシステムが設計されていた場合、G.711 は WAN を経由して送信されるため、設計の意図が失われます。結果として、G.711 のみのデバイスを使用する複数のサイトがある場合に WAN で LBR が実行されていると、これらの各サイトがトランスコーダ リソースを必要とします。

その他のリソースの配置も重要です。たとえば、リモート サイトの 3 つの電話機で会議が発生し、会議リソースが中央（呼処理）サイトにある場合、3 つのメディア ストリームが WAN で伝送されます。会議リソースがローカルにあれば、コールは WAN を経由しません。WAN の帯域幅とコール アドミッション制御を設計するときは、この要素を考慮する必要があります。

分散型呼処理を使用するマルチサイト配置

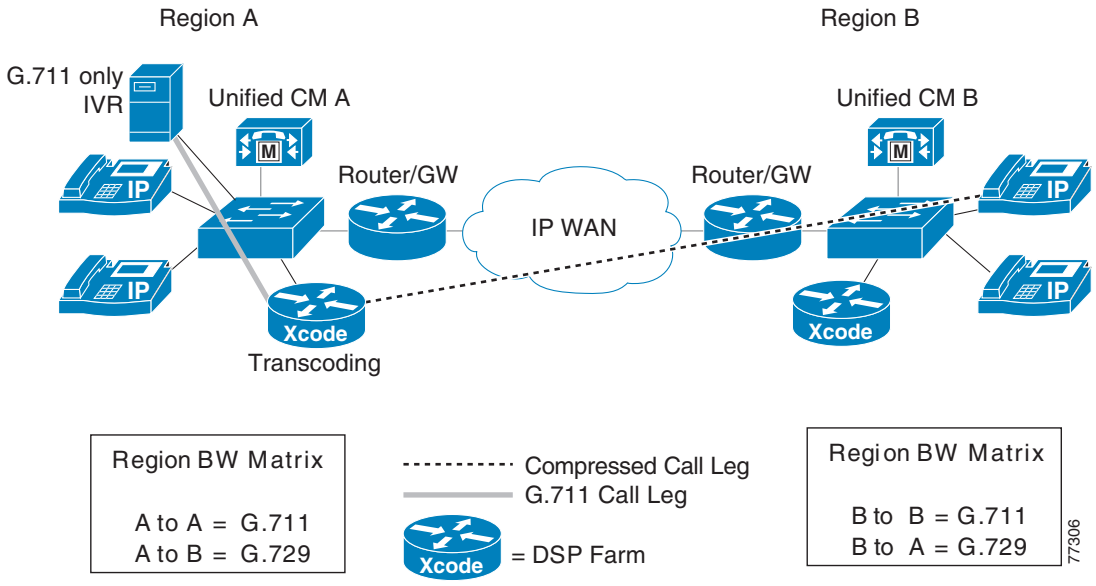
分散型呼処理配置では、IP WAN を介して複数のサイトが接続されます。各サイトには Unified CM クラスタが含まれ、単一サイト モデルか、集中型呼処理モデルになります。サイト間のコール アドミッション制御には、ゲートキーパーを使用できます。

WAN 帯域幅は一般に制限されているので、WAN を通過するときは、LBR コーデック（たとえば、G.729a）を使用するように、サイト間のコールが設定されていることがあります。H.323v2 クラスタ間トランクは、Unified CM クラスタの接続に使用されます。Unified CM は、ハードウェア MTP が使用される場合、MTP サービスを通じた圧縮音声コール接続もサポートします（図 7-12 を参照）。

次の状況では、分散型呼処理配置に、トランスコーディング サービスと MTP サービスが必要になる場合があります。

- 現行バージョンの Cisco アプリケーションを使用する場合は、トランスコーディング リソースの使用を回避できるため、回避することを推奨します。特別な例として、特定のデバイスの G.711 を回避できないことがあります。
- 一部のエンドポイント（たとえば、映像エンドポイント）が、H.323v2 機能をサポートしません。

図 7-12　トランスコーディングを使用したクラスタ間コール フロー



Unified CM は、MRG（メディア リソース グループ）を使用して、クラスタ内の Unified CM サーバ間で、MTP リソースとトランスコーディング リソースの共有を可能にします。さらに、クラスタ間トランクを介したコールの場合、MTP リソースとトランスコーディング リソースは、必要な場合だけ使用されます。したがって、LBR コーデックをサポートしないアプリケーションに対して MTP サービスを設定する必要がなくなります。

次の特性が、分散型呼処理配置に適用されます。

- トランスコーディングを必要とするクラスタ間コールだけが、MTP サービスを使用します。たとえば、コールの両方のエンドポイントが G.729 コーデックを使用できる場合、トランスコーディング リソースは使用されません。
- クラスタ内のサーバ間で MTP リソースを共有すると、リソースの使用効率が向上します。

メディアの機能と音声品質

メディアを操作するいずれのプロセスも、メディアの品質を低下させる可能性があります。たとえば、ネットワーク（IP または TDM）上で送信するための音声ストリームのエンコーディングと、相手側でのデコーディングは情報の損失を招き、結果として音声ストリームは元の音声を正確に再生しません。同じ音声ストリームの複数のエンコーディングおよびデコーディングの手順を含む、ネットワーク経由のメディア通過パスが存在する場合、エンコーディングおよびデコーディングの操作が繰り返されるたびに音声品質は低下していきます。通常、このようなパスは回避する必要があります。このことは特に、G.729 などの低帯域幅コーデック（LBC）に当てはまります。

このようなパスが回避できない場合には、G.711 または G.722 コーデックなどの帯域幅が比較的高く、低圧縮のコーデックを使用することによって通常、音声品質を向上させることができます。このようなパスが予想される場合には、これらのコーデックの使用を推奨します。このようなシナリオで、低帯域幅で高圧縮のコーデックを使用することは推奨できません。

保留音の設計に関する留意点

ここでは、堅牢な MoH ソリューションの設計に役立つ、MoH 設定上の考慮事項とベスト プラクティスについて説明します。

コーデックの選択

MoH 配置に複数のコーデックが必要な場合、クラスタ全体の Unified CM サービス パラメータ設定にある IP Voice Media Streaming Application サービス パラメータ [サポートされる MoH コーデック（Supported MoH Codecs）] で設定します。[クラスタ全体のパラメータ（Clusterwide Parameters）] の下の [サポートされる MoH コーデック（Supported MoH Codecs）] リストの中から、MoH ストリームに許可する、目的のコーデック タイプをすべて選択します。デフォルトでは、G.711 mu-law のみが選択されています。別のコーデック タイプを選択するには、リストをスクロールさせて該当するコーデックをクリックしてください。複数選択する場合は、CTRL キーを押したまま、マウスを使用して、リストをスクロールさせて複数のコーデックを選択します。MoH イベントに使用される実際のコーデックは、MoH サーバおよび保留にされるデバイス（IP 電話、ゲートウェイなど）のリージョン設定によって決まります。したがって、適切なリージョン設定を MoH サーバに割り当て、必要なリージョンの関係を設定して、MoH インタラクションのコーデック選択を制御します。

（注）　MoH オーディオ ストリームに G.729 コーデックを使用する場合、このコーデックは会話用に最適化されているので、音楽用としては最低限のオーディオ品質であることに注意してください。

マルチキャスト アドレッシング

マルチキャスト MoH を設定するには、適切な IP アドレッシングが重要です。IP マルチキャストのアドレス範囲は 224.0.1.0 ～ 239.255.255.255 です。しかし、IANA（Internet Assigned Numbers Authority）は、公衆マルチキャスト アプリケーション用に 224.0.1.0 ～ 238.255.255.255 の範囲のアドレスを割り当てています。公衆マルチキャスト アドレスを MoH に使用しないことを強く推奨します。代わりに、プライベート ネットワーク上の管理制御アプリケーション用に予約されている、239.1.1.1 ～ 239.255.255.255 の範囲内の IP アドレスを使用するように、マルチキャスト MoH オーディオ ソースを設定することを推奨します。

さらに、次の理由で、ポート番号ではなく、IP アドレスでインクリメントするように、マルチキャスト オーディオ ソースを設定することも必要です。

- 保留にされた IP Phone は、ポート番号ではなく、マルチキャスト IP アドレスに加わる。

  Cisco IP Phone には、マルチキャスト ポート番号という概念はありません。したがって、特定のオーディオ ストリームに対して設定されているすべてのコーデックが、同じマルチキャスト IP アドレス（別々のポート番号であっても）に送信される場合、1 本のストリームしか必要ない場合であっても、すべてのストリームが IP Phone に送信されます。IP Phone は 1 本の MoH ストリームしか受信できないので、不必要なトラフィックでネットワークが飽和状態になる可能性があります。

- IP ネットワーク ルータは、ポート番号ではなく、IP アドレスに基づいて、マルチキャストをルーティングする。

  ルータには、マルチキャスト ポート番号という概念はありません。したがって、同じマルチキャスト グループ アドレス（別々のポート番号であっても）に送信される複数のストリームを検出すると、ルータは、そのマルチキャスト グループのすべてのストリームを転送します。必要なストリームは 1 本だけなので、ネットワーク帯域幅が過剰に利用され、その結果、ネットワークの輻輳が発生する可能性があります。

複数のマルチキャスト MoH サーバを設定する場合は、各 MoH サーバに異なる基本のマルチキャスト IP アドレスおよび/または範囲を割り当てます。複数の MoH サーバが同じマルチキャスト IP アドレスに送信している場合、エンドポイントがマルチキャスト グループ アドレスに追加されると、そのエンドポイントは（異なる MoH サーバからの）複数の MoH ストリームを受信します。

Unified CM MoH オーディオ ソース

オーディオ ソースは、Unified CM クラスタ内の*すべての* MoH サーバ間で共有されるため、各オーディオ ソース ファイルはクラスタ内の各 MoH サーバにアップロードしておく必要があります。クラスタごとに最大 500 の固有オーディオ ソースを設定できます。

マルチキャスト ストリームに使用するこれらのオーディオ ソースには、[マルチキャスティングを許可（Allow Multicasting）] を必ず有効にしてください。

同一 Unified CM クラスタ内のユニキャストとマルチキャスト

管理者は、1 つの Unified CM クラスタでユニキャストとマルチキャスト両方の MoH ストリームを処理するように設定できます。この設定が必要なのは、マルチキャストをサポートしないデバイス、またはエンドポイントがテレフォニー ネットワークに含まれている場合、あるいはネットワークの一部でマルチキャストが使用可能になっていない場合です。

クラスタがユニキャストとマルチキャストの両方の MoH オーディオ ストリームをサポートできるようにするには、次のいずれかの方法を使用してください。

- 別々の MoH サーバを配置します。一方のサーバをユニキャスト MoH サーバとして設定し、もう一方のサーバをマルチキャスト MoH サーバとして設定します。
- 2 つのメディア リソース グループ（MRG）を備えた 1 台の MoH サーバを配置します。各グループには同じ MoH サーバが含まれますが、1 つの MRG はオーディオストリームはマルチキャスト用に設定し、もう 1 つはユニキャスト用に設定します。

どちらの場合も、少なくとも 2 つの MRG、および少なくとも 2 つのメディア リソース グループ リスト（MRGL）を設定する必要があります。ユニキャスト MoH を必要とするエンドポイントには、1 つのユニキャスト MRG と 1 つのユニキャスト MRGL を設定します。同様に、マルチキャスト MoH を必要とするエンドポイントには、1 つのマルチキャスト MRG と 1 つのマルチキャスト MRGL を設定します。

別々の MoH サーバを配置する場合、一方のサーバをマルチキャスト無効（ユニキャスト専用）に設定し、もう一方の MoH サーバをマルチキャスト有効に設定してください。ユニキャスト専用 MoH メディア リソースとマルチキャスト使用可能 MoH メディア リソースを、ユニキャスト MRG とマルチキャスト MRG にそれぞれ割り当てます。マルチキャスト MRG には [Use Multicast for MoH Audio] ボックスにチェックマークが付き、ユニキャスト MRG にはチェックマークが付いていないことを確認してください。また、これらのユニキャスト MRG とマルチキャスト MRG をそれぞれの MRGL に割り当てます。この場合、MRG がマルチキャストを使用するように設定されているかどうか、また MoH ストリームを流す元のサーバに基づいて、MoH ストリームのユニキャストまたはマルチキャストが行われます。

単一の MoH サーバをユニキャスト MoH とマルチキャスト MoH の両方に対して配置する場合は、サーバをマルチキャスト用に設定します。同じオーディオ ソースをユニキャスト MRG とマルチキャスト MRG の両方に割り当て、マルチキャスト MRG に対して [Use Multicast for MoH Audio] ボックスにチェックマークを付けます。この場合は、MRG がマルチキャストを使用するように設定されているかどうかだけで、MoH ストリームがユニキャストかマルチキャストかが決まります。

(注)　ユニキャスト MRG を設定する場合は、混乱しないようにしてください。これは、MoH メディア リソースをユニキャスト MRG に追加する場合であっても、リソース名の最後に、[Multicast] が追加されるからです。このラベルは、リソースがマルチキャスト対応であるという単なる表示です。リソースがユニキャストとして送信されるか、マルチキャストとして送信されるかを決定するのは、[Use Multicast for MoH Audio] ボックスのチェックの有無です。

さらに、適切な MRGL を使用するように、個々のデバイスまたはデバイス プールを設定する必要があります。1 つまたは複数のデバイス プールにすべてのユニキャスト デバイスを含め、ユニキャスト MRGL を使用するようにこれらのデバイス プールを設定できます。あるいは、1 つまたは複数のデバイス プールにすべてのマルチキャスト デバイスを含め、マルチキャスト MRGL を使用するようにこれらのデバイス プールを設定することもできます。オプションとして、該当するユニキャスト MRGL またはマルチキャスト MRGL を使用するように、個々のデバイスを設定できます。最後に、個々のデバイス、または（電話デバイスの場合）個々の回線かディレクトリ番号ごとに、ユーザ保留オーディオ ソースおよびネットワーク保留オーディオ ソースを設定して、適切なオーディオ ソースを割当ます。

マルチキャスト MoH とユニキャスト MoH の両方を同じクラスタに配置する方法を選択する場合は、必要なサーバの数を考慮することが重要です。単一の MoH サーバをユニキャストとマルチキャストの両方に使用すると、クラスタ全体に必要な MoH サーバの数が減ります。マルチキャスト MoH サーバとユニキャスト MoH サーバを別々に配置すると、クラスタ内に必要なサーバの数が明らかに増えます。

Quality of Service（QoS）

時間に依存する重要なリアルタイム アプリケーション（音声など）に遅延または損失がないように、1 つのネットワーク上のデータと音声のコンバージェンスには、適切な QoS が必要です。音声トラフィック用の適切な QoS を確保するには、ストリームがネットワークに入り、通過するときに、ストリームのマーク付け、分類、およびキューイングを行って、音声ストリームを重要度の低いトラフィックよりも優先的に処理する必要があります。MoH サーバは、Diffserv コード ポイント（DSCP）値 46 または PHB（Per Hop Behavior）値 EF（ToS 値 0xB8 に相当）を使用して、オーディオ ストリーム トラフィックに、音声ベアラトラフィックと同じマークを自動的に付けます。したがって、ネットワーク上で QoS が適切に設定されている限り、MoH ストリームは、音声 RTP メディア トラフィックとして分類され、プライオリティ キューイングとして扱われます。

MoH サーバと Unified CM サーバ間のコール シグナリング トラフィックは、デフォルトで DSCP 値 24 または PHB 値 CS3（ToS of 0x60 に相当）を使用して自動的にマーキングされます。したがって、ネットワーク上で、QoS が適切に設定されている限り、他のすべてのコール シグナリングと同様、ネットワーク内で、このコール シグナリング トラフィックは、適切に分類されキューに入れられます。

コール アドミッション制御と MoH

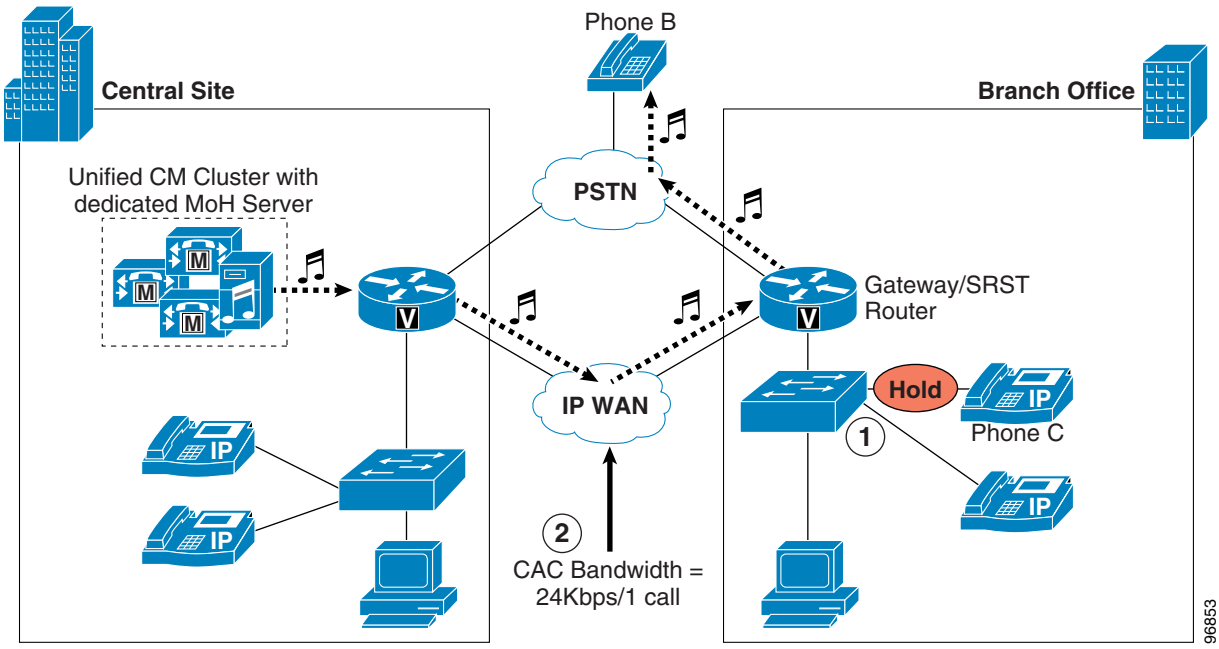
IP テレフォニー トラフィックが WAN リンク上を流れる場合は、コール アドミッション制御（CAC）が必要です。このようなリンク上では使用可能な帯域幅が制限されているので、適切なコール アドミッション制御がないと、音声メディア トラフィックの遅延または損失が起きる可能性が高くなります。詳細については、帯域幅管理（13-1 ページ）を参照してください。

Unified CM の（静的ロケーションまたは RSVP 対応ロケーションのいずれかに基づく）コール アドミッション制御は、WAN を通過するユニキャスト MoH ストリームをトラッキングできますが、マルチキャスト MoH ストリームはトラッキングできません。したがって、WAN 帯域幅が完全にサブスクライブされた場合であっても、マルチキャスト MoH ストリームは、コール アドミッション制御によって WAN へのアクセスを拒否されません。ストリームは WAN を介して送信され、その結果、オーディオ ストリームの品質が低下し、WAN を通過するその他のすべてのコールの品質も低下する可能性があります。マルチキャスト MoH ストリームがこのオーバーサブスクリプション状態にならないようにするには、帯域幅を追加して低遅延キューイング（LLQ）音声プライオリティ キューを設定することによって、すべてのダウンストリーム WAN インターフェイス上で QoS 設定に余裕を持ってプロビジョニングする必要があります。MoH ストリームは単方向であるため、ダウンストリーム インターフェイス（中央サイトからリモート サイトへ）の音声プライオリティ キューのみを余分にプロビジョニングする必要があります。WAN リンクを通過する可能性があるすべての固有マルチキャスト MoH ストリームに対して、十分な帯域幅を追加してください。たとえば、4 つの固有マルチキャスト オーディオ ストリームが WAN を通過する可能性がある場合、音声プライオリティ キューに 96 Kbps を追加します（4 * 24 Kbps（G.729 オーディオ ストリームごと）= 96 Kbps）。

図 7-13 は、集中型マルチサイト配置におけるコール アドミッション制御と MoH の例を示しています。この例の場合、IP Phone C が PSTN 電話機（電話機 B）とコール中であると想定します。この時点では、WAN 上で帯域幅は消費されていません。電話機 C で [Hold] ソフトキーを押すと（ステップ 1）、電話機 B は、WAN を介して中央サイトの MoH サーバから MoH ストリームを受信するので、リンク上の帯域幅を消費します。コール アドミッション制御でこの帯域幅を考慮すべきかどうかは、MoH ストリームのタイプに応じて決まります。マルチキャスト MoH が流れる場合、コール アドミッション制御は、24 Kbps が消費されているとは見なしません（したがって、ダウンストリーム WAN インターフェイス上の QoS はそれに応じてプロビジョニングされなければなりません）。しかし、ユニキャスト MoH が流れる場合、コール アドミッション制御は、使用可能な WAN 帯域幅から 24 Kbps を差し引きます（ステップ 2）。

（注）　上記の例では、ユニキャスト MoH を WAN 上で流すことを示唆しているように見えますが、これは、MoH とのロケーションベースのコール アドミッション制御をわかりやすく示すための例に過ぎません。また、この設定の推奨または保証を意味するものではありません。前述のように、WAN を介した MoH オーディオ ストリームの送信用のトランスポート メカニズムには、マルチキャスト MoH を推奨します。

図 7-13　　ロケーションベースのコール アドミッション制御と MoH



保留音の配置モデル

各種 Unified Communications 呼処理配置モデルにより、MoH の構成設計にはさらに考慮事項が発生します。配置モデルの選択が、MoH のトランスポート メカニズム（ユニキャストまたはマルチキャスト）、リソースのプロビジョニング、およびコーデックの決定に影響を与える場合があります。ここでは、各種配置モデルに関連した問題について説明します。

配置モデルの詳細については、コラボレーションの配置モデル（10-1 ページ）の章を参照してください。

単一サイト キャンパス（すべての配置に関連）

単一サイト キャンパス配置は、通常、LAN インフラストラクチャに基づくものであり、大量のトラフィックに対して十分な帯域幅が用意されています。LAN インフラストラクチャでは一般に帯域幅が制限されないので、単一サイト配置内のすべての MoH オーディオ ストリームには、G.711（A-law または mu-law）コーデックの使用を推奨します。G.711 は、IP テレフォニー環境に、最適な音声と音楽のストリーミング品質を提供します。

MoH サーバの冗長性も考慮する必要があります。MoH サーバが過負荷になるか、使用不能になった場合でも、複数の MoH サーバを設定し、それらのサーバを優先順に MRG に割り当てておくと、別のサーバが制御を引き継いで、MoH ストリームを流すことができます。

ネットワーク テクノロジーの多様性が増すにつれて、大規模な単一サイト キャンパスでは、一部のエンドポイント デバイスまたはネットワーク領域がマルチキャストをサポートできなくなる可能性があります。このため、ユニキャストとマルチキャストの両方の MoH リソースを配置する必要があります。詳細については、同一 Unified CM クラスタ内のユニキャストとマルチキャスト（7-44 ページ）の項を参照してください。

オフネット コールとアプリケーション処理コールが、保留時に期待された MoH ストリームを受け取るには、適切な MRGL とオーディオ ソースを使用してすべてのゲートウェイとその他のデバイスを設定するか、それらを適切なデバイス プールに割り当ててください。

集中型マルチサイト配置

集中型呼処理を使用するマルチサイト IP テレフォニー配置には、一般的に、中央以外の複数のサイトとの WAN 接続が含まれます。これらの WAN リンクは、通常、帯域幅とスループットの障害になります。これらのリンク上での帯域幅使用量を最小限にするには、WAN を通過するすべての MoH オーディオ ストリームとして G.729 コーデックを使用することを推奨します。G.729 コーデックは、音楽アプリケーションではなく、音声用に最適化されています。したがって、MoH トランスポートに G.729 がもたらす品質の低下よりも、帯域幅の節約がはるかに重要な問題である WAN 上でのみ、G.729 を使用してください。さらに、マルチキャスト トラフィックにより、帯域幅を大幅に節約できるので、WAN を介してエンドポイントにオーディオを流す場合は、常にマルチキャスト MoH を使用する必要があります。

WAN を介して G.729 を使用するときに MoH ストリームの音声品質が問題になる場合は、WAN を介した MoH オーディオ ストリームに G.711 コーデックを使用し、音声コールには引き続き G.729 を使用します。WAN を介した MoH ストリームの送信に G.711 コーデックを使用し、WAN を介した音声コールの送信に G.729 コーデックを使用するには、Unified CM リージョンにすべての MoH サーバだけを配置し、そのリージョンが他のリージョンとの間で G.711 を使用するように設定します。この設定により、WAN の一方の側にある 2 つの電話機間でコールを発信するときは、それぞれのリージョンの間で G.729 コーデックが使用されます。ただし、一方の通話者がコールを保留にした場合、MoH オーディオ ストリームは G.711 を使用して符号化されます。これは、G.711 が、MoH サーバのリージョンと、保留にされた電話機のリージョンとの間で使用するコーデックとして設定されているためです。

集中型 PSTN の展開

PSTN アクセス用の単一のゲートウェイまたはゲートウェイ セットによる集中型 PSTN 展開では、500 を超える固有オーディオ ソースを設定する方法はありません。ゲートウェイに割り当てられたメディア リソース グループ リスト（MRGL）は、PSTN 発信者が保留されるときに MoH ストリーミングで使用される MoH サーバを判別し、コールを保留中にしている電話機はオーディオ ソースを判別します。集中型 PSTN 配置では、PSTN ゲートウェイがローカル サイトにないため、支社ロケーションに基づいて複数の MoH サーバを指すように MRGL を使用することはできません。そのためこのケースでは、最大 500 の支社サイトの固有 MoH ソースを有効にするために、最大 500 の一意のサイト固有の MoH ソースまたはマルチキャスト ストリーミングがあります。

次の例は、MOH ストリーミングが最大 500 のロケーションでどのように機能するかを示します。

1 ～ 500 の支社の場合、MOH サーバ ノード MoH_1（239.1.1.1 の基本のマルチキャスト アドレスを使用）を指している MRGL で集中型 PSTN ゲートウェイまたはゲートウェイのセットが設定されます。各支社のすべての電話機が、クラスタに設定された 500 のオーディオ ソースの 1 つを指します。そのため、支社 1 の電話機は MoH_1 サーバが 239.1.1.1 ～ 4 のオーディオ ソース 1 を指します（コーデックに応じて、そしてオーディオ ソースが順に設定されていることを想定して）。支社 2 の電話機は MoH_1 サーバが 239.1.1.5 ～ 8 のオーディオ ソース 2 を指し、支社 3 の電話機は MoH_1 サーバが 239.1.1.9 ～ 12 のオーディオ ソース 3 を指します。そして最後に、支社 500 の電話機は MoH_1 サーバが 239.1.8.197 ～ 200 のオーディオ ソース 501 を指します。

支社ルータからのマルチキャスト MoH

Cisco Unified Survivable Remote Site Telephony（SRST）機能を使用して配置された支社ルータは、支社の SRST ルータのフラッシュ、またはアナログ ポートに接続されているライブ フィードからの MoH ストリーミングを使用して、リモート サイトや支社サイトでマルチキャスト MoH を提供できます。これらの 2 つの方式によって支社のルータから MoH をマルチキャストすると、Unified CM MoH の機能が次のシナリオの両方において向上します。

- 非フォールバック モード

  WAN が稼働中で、電話機が Unified CM で制御されている場合、この設定では、ローカルに発信される MoH を提供し、WAN を介してリモート支社サイトに MoH を転送する必要がなくなります。

- フォールバック モード

  SRST がアクティブで、支社のデバイスが中央サイトの Unified CM との接続を失った場合、支社のルータが継続して MoH をマルチキャストします。

いずれかのシナリオでライブ フィード オプションを使用している場合、ライブ フィードの入力をモニタすることにより、SRST ルータでは冗長性が確保され、ライブ フィードの接続が切断されても、フラッシュ内のファイルから MoH をストリームするようになります。マルチキャスト MoH を流す際に使用できるマルチキャスト アドレスとポート番号は、SRST ルータごとに 1 つのみです。このため SRST ルータではライブフィードとフラッシュ ファイルの両方からのストリーミングを同時に実行することはできません。また、SRST ルータでは、フラッシュから流すことのできるオーディオ ファイルは 1 つのみです。

（注）　SRST 機能が実際に使用されるかどうかに関係なく、SRST ライセンスが必要です。ライセンスが必要なのは、支社ルータのフラッシュから MoH を流すための設定が SRST コンフィギュレーション モードで行われるため、および SRST 機能が使用されない場合でも少なくとも 1 つの **max-ephones** と 1 つの **max-dn** を設定する必要があるためです。

非フォールバック モード

非フォールバック モード中（WAN が稼働していて、SRST がアクティブでない場合）、支社の SRST または E-SRST ルータは、マルチキャスト MoH をすべてのローカル Cisco Unified Communications デバイスに流すことができます。これを実現するには、支社ルータ上で設定された内容と同じマルチキャスト IP アドレスとポート番号をもつオーディオ ソースを使用して、Unified CM MoH サーバを設定する必要があります。ブランチ ルータで使用されるオーディオ ソースのマルチキャスト IP アドレスとポート番号は、集中型 Unified CM MoH サーバのオーディオ ソース ファイルまたは固定オーディオ ソースのマルチキャスト アドレスとポート番号に対応できます。このシナリオでは、マルチキャスト MoH オーディオ ストリームが、常に SRST または E-SRST ルータから発信されるので、中央サイトの MoH サーバのオーディオ ソースが WAN を通過する必要はありません。

中央サイトのオーディオ ストリームが WAN を通過しないようにするには、次のいずれかの方法を使用してください。

- 最大のホップ カウントを設定する

  中央サイトの MoH オーディオ ソースが、中央サイトの LAN より先に流れないように、最大ホップ カウントまたは TTL を十分に小さく設定します。

- WAN インターフェイス上でアクセス コントロール リスト（ACL）を設定する

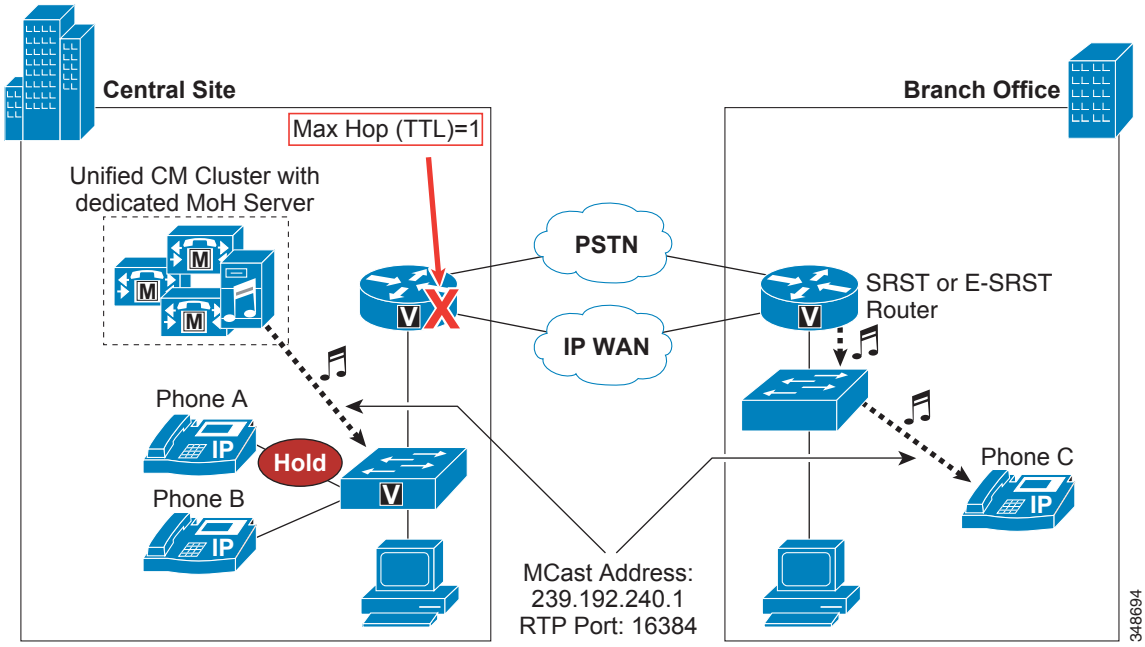
  中央サイトの WAN インターフェイス上で ACL を設定して、マルチキャスト グループ アドレス宛のパケットがインターフェイスから発信されないようにします。

- WAN インターフェイス上でマルチキャスト ルーティングを無効にする

  WAN インターフェイス上ではマルチキャスト ルーティングを設定しないでください。設定しなければ、マルチキャスト ストリームが WAN に転送されないことが保証されます。

図 7-14 は、フォールバック モードでないときに支社のルータからマルチキャスト MoH を流す仕組みを示しています。電話機 A で電話機 C を保留にすると、電話機 C は、ローカル SRST ルータからマルチキャスト MoH を受信します。この図では、MoH サーバは、(RTP ポート 16384 上で) 239.192.240.1 にマルチキャスト オーディオ ソースを流します。しかし、最大ホップ数が 1 に制限されているので、このストリームは、ローカル MoH サーバのサブネットから WAN を通過して外に出ないことが保証されています。同時に、支社の SRST ルータまたはゲートウェイは、フラッシュまたはライブ フィードからオーディオ ストリームをマルチキャストします。このストリームも、マルチキャスト アドレスとして 239.192.240.1 を使用し、RTP ポート番号として 16384 を使用します。電話機 A で [Hold] ソフトキーを押すと、電話機 C は、SRST ルータから発信された MoH オーディオ ストリームを受信します。

図 7-14　　支社ルータのフラッシュからのマルチキャスト MoH



この方法を使用してマルチキャスト MoH を配信する場合は、Unified CM クラスタ内のすべてのデバイスが、同じユーザ保留およびネットワーク保留オーディオ ソースを使用するように設定し、すべての支社ルータに同じマルチキャスト グループ アドレスとポート番号を設定します。保留側のユーザまたはネットワーク保留オーディオ ソースは、オーディオ ソースを特定するときに使用されるため、クラスタ内に複数のユーザまたはネットワーク保留オーディオ ソースを設定する場合、リモートの被保留側が常にローカルの MoH ストリームを受信することを保証する手段はありません。たとえば、中央サイトの電話機に設定されているオーディオ ソースが、そのユーザおよびネットワーク保留オーディオ ソースとして、グループ アドレス 239.192.254.1 を使用するものとします。この電話機がリモート デバイスを保留にすると、ローカル ルータのフラッシュの MoH ストリームがマルチキャスト グループ アドレス 239.192.240.1 に送信される場合でも、リモート デバイスは 239.192.254.1 に加わろうとします。代わりに、ネットワーク内のすべてのデバイスがマルチキャスト グループ アドレス 239.192.240.1 でユーザ/ネットワーク保留オーディオ ソースを使用するように設定し、すべての支社ルータが 239.192.240.1 でフラッシュからマルチキャストするように設定すると、リモート デバイスはすべて、そのローカル ルータから MoH を受信します。

フォールバック モード

フォールバック モード中（WAN がダウンしていて SRST がアクティブな場合）、支社の SRST ルータはシャーシ内のすべてのアナログ ポートとデジタル ポートに、マルチキャスト MoH を流すことができます。これによりアナログ電話機および PSTN 電話機に MoH を流すことができます。

支社のルータに対して、フォールバック モードのマルチキャスト MoH を設定する方法は、通常の設定方法と同じです。ただし、ルータに対して設定するマルチキャスト アドレスは、目的の動作によって異なります。支社のルータから、デバイスにマルチキャスト MoH をフォールバック モードでのみ流す必要がある場合（たとえば、リモート デバイスで受信する MoH が非フォールバック モード中に中央サイトの MoH サーバから発信される場合）、SRST ルータに設定したマルチキャスト アドレスとポート番号が、中央サイトの MoH サーバのいずれのオーディオ ソースと重複しないようにする必要があります。重複していると、リモート デバイスは、設定されているユーザ/ネットワーク保留オーディオ ソースに応じて、ローカル ルータのフラッシュから MoH を継続的に受信することがあります。

支社の SRST/ゲートウェイ ルータに、マルチキャスト MoH を設定すると、ルータはフォールバック モードでないときにも、MoH ストリームのマルチキャストを継続することに注意してください。

フォールバック モードを設定して、拡張 SRST（E-SRST）と呼ばれる SRST モードで Cisco Unified Communications Manager Express（Unified CME）を使用することもできます。フォールバック モードの動作は同じですが、コンフィギュレーション コマンドが多少異なります。SRST コマンドは、Cisco IOS **call-manager-fallback** コンストラクトで入力しますが、E-SRST モードでは、コマンドは **telephony-service** で入力します。

SRST を介して MoH をマルチキャストする方法は 4 つあります。

- 支社ルータのフラッシュからの SRST マルチキャスト MoH
- ライブ フィードからの SRST マルチキャスト MoH
- ブランチ ルータのフラッシュからのマルチキャスト MoH による E-SRST モード
- ライブ フィードからのマルチキャスト MoH による E-SRST モード

Cisco Unified SRST と E-SRST の設定方法については、次のマニュアルを参照してください。

- 次のサイトで入手可能な『*Cisco Unified SRST System Administrator Guide*』

  https://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html

- 次の Web サイトで入手可能な『*Cisco Unified Communications Manager Express System Administrator Guide*』

  https://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_and_configuration_guides_list.html

- マルチキャスト MoH リソースとして Cisco Unified SRST を使用する場合の詳細については、次の URL で入手可能な最新バージョンの『*Cisco Unified SCCP and SIP SRST System Administrator Guide*』の「*Integrating Cisco Unified Communications Manager and Cisco Unified SRST to Use Cisco Unified SRST as a Multicast MoH Resource*」の項を参照してください。

  https://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html

分散型マルチサイト配置

分散型呼処理を使用するマルチサイト IP テレフォニー配置には、通常、サイト間の WAN または MAN 接続が含まれます。これらの低速リンクは、通常、帯域幅とスループットの障害になります。リンク上での帯域幅使用量を最小限にするには、リンクを通過するすべての MoH オーディオ ストリームとして G.729 コーデックを使用することを推奨します。ただし G.729 コーデックは、音楽用ではなく、音声用に最適化されているので、MoH トランスポートに G.729 がもたらす品質の低下よりも、帯域幅の節約がはるかに重要な問題である WAN/MAN 上でのみ、G.729 を使用してください。

集中型マルチサイト配置の場合とは異なり、WAN を介して流れる MoH オーディオ ストリーム用に G.711 が必要になる可能性がある状況では、分散型マルチサイト環境で MoH オーディオ ストリームが G.711 を使用するように強制することはできません。MoH サーバが別の Unified CM リージョンに配置されている状況で、このリージョンとクラスタ間トランクまたは SIP トランクのリージョンとの間で G.711 コーデックが設定されている場合でも、2 つのクラスタ間のコールが一方の電話機によって保留にされたときは、元の音声コールのコーデックが保持されます。これらのクラスタ間コールは、一般に、帯域幅の節約のために G.729 を使用して符号化されるため、一方のクラスタからの MoH ストリームも G.729 を使用して符号化されます。

もう 1 つのオプションでは、マルチキャスト MoH をクラスタ間トランク（ICT）または SIP トランク経由でクラスタ間コールにプロビジョニングします。これにより、1 つの Unified CM クラスタ内のエンドポイントで別の Unified CM クラスタからストリーミングされたマルチキャスト MoH を聞くことができるようになるとともに、クラスタ間帯域幅をより効率的に使用できるようになります。この機能を活かすには、適切に設計された IP マルチキャスト環境が必要です。IP マルチキャストの詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

https://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html

分散型クラスタ間環境では、適切なマルチキャスト アドレス管理も、設計上の重要な考慮事項です。分散型ネットワーク全体で流れるリソースの重複を防止するために、いかなる MoH オーディオ ソース マルチキャスト アドレスも、配置内のすべての Unified CM クラスタに対して一意でなければなりません。

WAN を介したクラスタリング

その名前が示すように、クラスタオーバー WAN 配置には、他のマルチサイト配置と同様、低速 WAN リンクを含みます。したがって、これらの配置にも、G.729 コーデック、マルチキャスト トランスポート メカニズム、および低速 WAN リンクを介した MoH トラフィックに対して欠かせない安定した QoS の、3 つの要件が必要です。

さらに、このタイプの設定では、WAN の各端部に MoH サーバ リソースを配置することも必要です。WAN に障害が発生した場合には、WAN の各端部のデバイスは、ローカルに配置された MoH サーバから、引き続き MoH オーディオ ストリームを受信できます。さらに、適切な MoH 冗長設定がきわめて重要です。WAN の各端部のデバイスには、MRGL を指定する必要があります。この MRGL の MRG には、少なくとも 1 つのローカル リソースが最優先になった MoH リソースの優先順位リストが必要です。プライマリ サーバが使用不能になるか、要求を処理できない場合に備えて、この MRG に対して、MoH リソースを追加設定しておく必要があります。WAN のローカル側のリソースは使用不能になった場合に備えて、リスト内で他に少なくとも 1 つの MoH リソースは、リモート側の MoH リソースを指定しておく必要があります。

コラボレーション エンドポイント

改訂日：2018 年 3 月 1 日

Cisco Collaboration の配置では、さまざまなエンドポイントを使用できます。これらのエンドポイントは、通常のアナログ電話機をサポートする IP 環境内のゲートウェイから、さまざまな機能を提供する拡張的なネイティブ IP Phone セットに至るまで、多岐にわたります。

エンドポイントを配置する際は、認証、アップグレード、シグナリング プロトコル、Quality of Service（QoS）などのいくつかの要素を考慮する必要があります。コラボレーション システムは、これらの要素に対応するように適切に設計する必要があります。

この章では、さまざまなタイプのコラボレーション エンドポイントを要約し、ハイ アベイラビリティ、キャパシティ プランニングなどの設計および配置について説明します。この章で説明するコレボレーション エンドポイントは、次の主要なタイプに分類できます。

上記に示される各項では、配置に関する考慮事項を含む各エンドポイント タイプに関する情報を提供します。この情報の後に、エンドポイントを効率的に導入するための高可用性、キャパシティ プランニング、および設計に関する留意点の説明が続きます。

この章は、使用可能なエンドポイント タイプの範囲とそれらの導入に伴う高レベルの設計上の留意点を理解するために使用してください。

この章の変更点

表 8-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

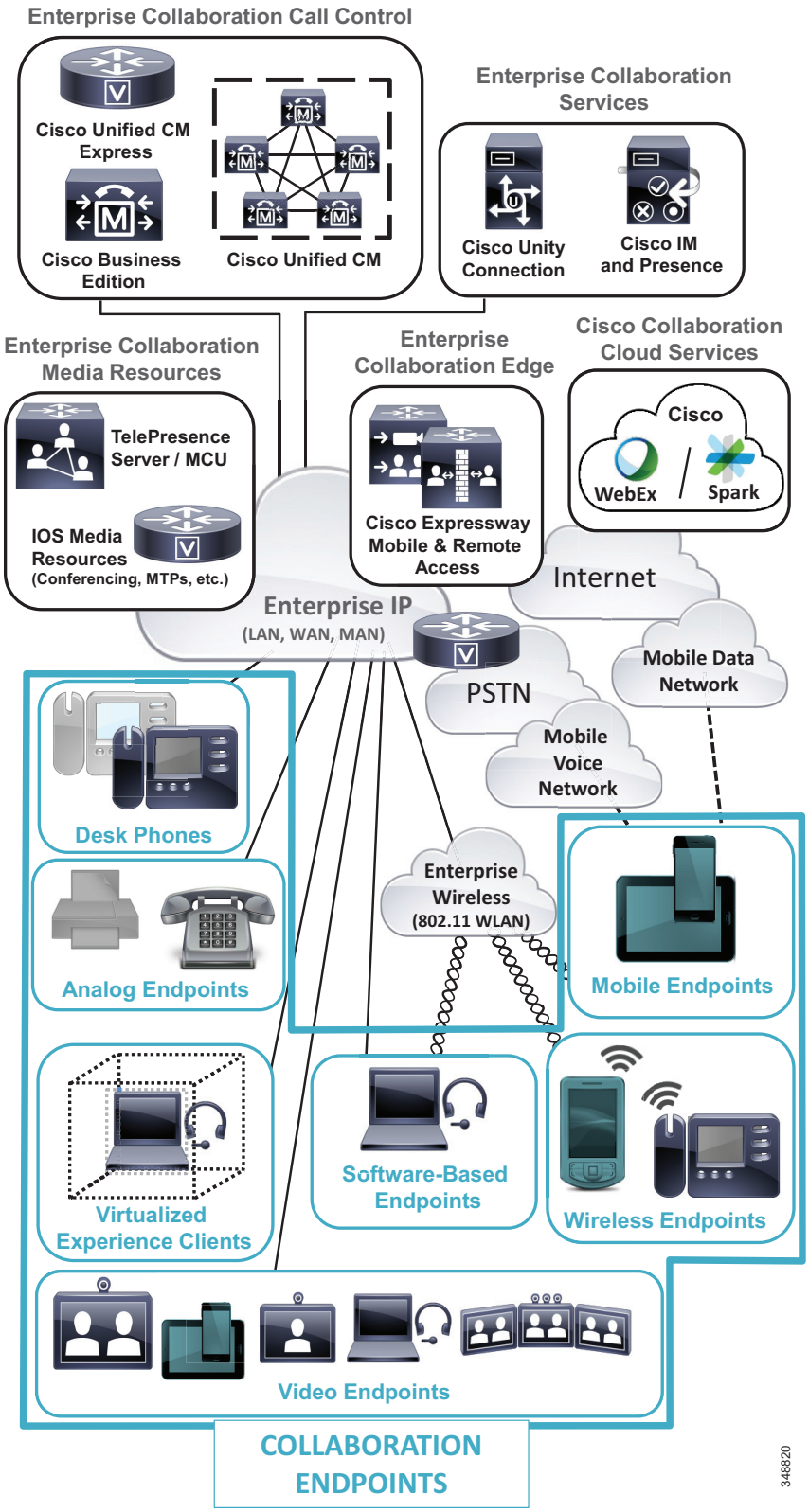
表 8-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Jabber および Cisco Spark Apple iOS クライアント対応の Apple プッシュ通知サービス（APNs）	モバイル エンドポイントとクライアントの配置に関する考慮事項（8-42 ページ）	2018 年 3 月 1 日
Cisco Jabber でのリフレッシュ トークンを使用した OAuth 2.0	ソフトウェア ベースのエンドポイントの配置に関する一般的な考慮事項（8-32 ページ） モバイル エンドポイントとクライアントの配置に関する考慮事項（8-42 ページ）	2018 年 3 月 1 日
Cisco Spark Room シリーズ	Cisco Spark Room シリーズ（8-18 ページ）	2018 年 3 月 1 日
Cisco IP Phone 8800 シリーズ	Cisco IP Phone 8800 シリーズ（8-10 ページ）	2018 年 3 月 1 日

コラボレーション エンドポイントのアーキテクチャ

図 8-1 に示されているようなさまざまなタイプのエンドポイントと同様に、コラボレーション エンドポイントを配置する場合に考慮する必要のあるさまざまな呼制御、コラボレーション サービス、およびメディア リソース オプションがあります。コラボレーション エンドポイントは、音声およびビデオ通話サービス用のエンタープライズ呼制御および/またはクラウド ベースのコラボレーションに依存します。コラボレーション エンドポイントは、ボイス メッセージ、インスタント メッセージ、およびプレゼンスなど、社内とクラウドベースの両方のコラボレーション サービスを利用します。さらに、これらのエンドポイントは、ビデオおよび音声会議、トランスコーディング、保留音などのエンタープライズ メディア リソースから主な付加サービスを取得します。

図 8-1　　シスコ コラボレーション エンドポイント アーキテクチャ



音声およびビデオ サービスにコラボレーション呼制御を配置するときは複数のオプションを使用できます。各呼制御プラットフォームによってエンドポイント登録、コールのセットアップ、およびルーティング サービスと、プロビジョニングされたメディア リソースへのアクセスが提供されます。エンドポイントとエンタープライズ Cisco Unified Communications Manager 間の高レベルの呼制御相互作用については、次のサブセクションで説明します。

Cisco Unified Communications Manager（Unified CM）呼制御

Cisco Unified Communications Manager（Unified CM）、Cisco Business Edition、および Cisco Unified Communications Manager Express（Unified CME）のコール シグナリングでは、回線側シグナリングとトランク側シグナリングが区別されます。トランク側シグナリングは他のサーバおよびゲートウェイに全体の呼処理クラスタまたはルータを接続するために使用されますが、回線側は呼処理プラットフォームにエンドポイント デバイスを接続するために使用されます。この 2 つのインターフェイスはそれぞれ、提供するサービスが異なります。回線側は、ユーザ指向の豊富な機能セットを提供します。

Session Initiation Protocol（SIP）と Skinny Client Control Protocol（SCCP）は、Cisco 呼処理プラットフォームでサポートされる 2 種類の主要な回線側シグナリング プロトコルです。すべての Cisco エンドポイントは、このうち一方または両方のプロトコルをサポートしています。どちらのプロトコルでも、サポートされる機能セットはおおよそ同じであるため、いずれのプロトコルの使用を選択するかは、基本的には導入における個人的な好みによります。ただし、SIP はすべての新しい機能とシスコのエンドポイントのサポート用に選択できるプロトコルです。

Cisco エンドポイントを使用してコールの発信や受信、またはアプリケーションの実行を行うには、いくつかの操作パラメータを使用して Cisco エンドポイントを設定しておく必要があります。この設定は、呼処理サーバまたはルータで事前に実行する必要があります。設定されると、呼処理プラットフォームは使用されるエンドポイントの設定ファイルを生成し、トリビアル ファイル転送プロトコル（TFTP）サーバにそのファイルを保存します。エンドポイント自体は、電源が投入されると、ブートアップ シーケンスを通過します。エンドポイントは、この設定ファイルを取得した後、適切なサーバに登録されます。これにより、エンドポイントは使用できる状態になります。エンドポイントは、ブートアップ シーケンスの一部として次のステップを実行します。

1. エンドポイントが電源に差し込まれていない場合、アクセス スイッチに接続されていれば、スイッチからの電力の獲得を試行します（Power over Ethernet）。無線および移動式エンドポイントはイーサネットを介して企業ネットワークに接続されていないため、常にバッテリまたは電源コンセントから電力を取得します。
2. デバイスのセキュリティが有効になっている場合、電力を取得すると、エンドポイントはそのクレデンシャルをセキュリティ サーバまたはネットワーク認証インフラストラクチャに示します。
3. エンドポイントは、ネットワークを使用できる場合、エンドポイント内の静的プロビジョニングによって、または動的ホスト制御プロトコル（DHCP）によって、ネットワーク パラメータ（IP アドレス、ドメイン ネーム サービス（DNS）サーバ、ゲートウェイ アドレスなど）を取得します。
4. また、エンドポイントは、エンドポイント内の静的プロビジョニングによって、または DHCP オプションによって、TFTP サーバ アドレスも取得します。
5. 続いてエンドポイントは、TFTP サーバ アドレスを使用して、その設定ファイルを取得します。これらのファイルには、そのエンドポイントが関連付けられるか登録されることがある呼処理サーバまたはルータ、エンドポイントがサポートする必要があるディレクトリ番号などが、他のパラメータとともに説明されています。
6. エンドポイントが呼処理プラットフォームに登録され、使用できる状態になります。

どのエンドポイントが Cisco Unified CM への登録をサポートしているかを確認するには、この章の各項に表示されているエンドポイント データ シートを参照してください。

コラボレーション エンドポイントのセクション 508 への準拠

選択した呼制御プラットフォームに関係なく、エンドポイントを選択して、Cisco Collaboration ネットワークを設計する場合は、Telecommunications Act のセクション 255 と U.S. セクション 508 に準拠して、障害を持つユーザがより利用しやすい電話機能を作成するように努める必要があります。

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

- Quality of Service（QoS）とコール アドミッション制御をネットワーク上で有効にして、企業での通信が可能な限りクリアで正確になるように、音声とビデオの品質を最適化します。
- ターミナル テレタイプ（TTY）デバイスまたは Telephone Device for the Deaf（TDD）に接続する電話には、G.711 コーデックのみを設定します。G.729 のような低ビット レートのコーデックを音声通信に適用している場合でも、Total Character Error Rate（TCER）が 1 % を超えている場合は、TTY/TDD デバイスが適切に作動しないことがあります。
- 必要に応じて、TTY/TDD デバイスに G.711 を設定し、WAN に対応します。
- Echo Cancellation を使用可能（ON）にし、パフォーマンスを最適化します。
- 音声アクティビティ検出（VAD）は、TTY/TDD 接続に影響を与えるため、使用されることはありません。したがって、設定は使用可能、使用不可のどちらであっても関係ありません。ただし、Unified CM 呼制御で VAD（無音圧縮）を無効にしたままにし、**no vad** コマンドを H.323 および Cisco IOS SIP ダイヤル ピアで使用することをお勧めします。
- Unified CM 内の *リージョン*および*デバイス プール*を適切に設定して、TTY/TDD デバイスが常時 G.711 コードを使用するようにします。
- TTY/TDD の Cisco Unified Communications ネットワークへの接続は、次のいずれかの方法で行います。
  - 直接接続（推奨方式）

    RJ-11 アナログ回線用 TTY/TDD を直接 Cisco FXS ポートに接続します。FXS ポートを備える Cisco 音声ゲートウェイであれば動作します。シスコは、この接続方式を推奨します。
  - アコースティック カップル

    IP Phone のハンドセットを TTY/TDD に接続しているカップリング機器に置きます。アコースティック カップルは、RJ-11 接続に比較すると信頼性が劣ります。カップリング方式は部屋の周囲の雑音やその他の要素で、一般的に通信エラーを起こしやすい方式です。
- 可聴メッセージ待機インジケータ（AMWI）の断続ダイヤル トーンが必要な場合は、アナログ電話機を Cisco VG アナログ ゲートウェイまたは Analog Telephony Adaptor（ATA）上に備えている FXS ポートに接続します。ほとんどの Cisco IP Phone が断続ダイヤル トーンをサポートします。
- Cisco TelePresence 専用ルームを配置する場合は、車いすや他の補助乗り物の動きが妨げられることのない十分に広い部屋を用意してください。

アナログ エンドポイント

アナログ ゲートウェイは、通常、アナログ信号が IP ネットワーク上でパケット化されて送信できるように、FAX 機、モデム、Deaf（TDD）/テレタイプライタ（TTY）用の通信デバイス、アナログ電話機などのアナログ デバイスを VoIP ネットワークに接続するために使用されます。また、アナログ ゲートウェイは、PSTN および、PBX やキー システムなどの他の従来のテレフォニー機器への物理的な接続も提供します。アナログ ゲートウェイには、Cisco IOS ルータベースのアナログ インターフェイスまたはサービス モジュール、および固定ポートのスタンドアロン ゲートウェイが含まれます。一般に、アナログ ゲートウェイは、呼制御、付加サービス、そして場合によってはインターフェイスの登録と設定のために Cisco Unified CM、Cisco Business Edition、Unified CM Express、および Survivable Remote Site Telephony（SRST）に依存します。シスコ アナログ ゲートウェイを介してサポートされる呼制御プロトコルには、SIP、H.323、SCCP、および Media Gateway Control Protocol（MGCP）が含まれます。

スタンドアロン アナログ ゲートウェイ

Cisco Analog Telephony Adapter（ATA）、Cisco VG シリーズ ゲートウェイなどのシスコのスタンドアロン アナログ ゲートウェイは、FAX 機、モデム、TDD/TTY、ページング システム、アナログ電話機、IP ネットワークに接続するための 1 つ以上のイーサネット ポートなどのアナログ デバイスに接続を提供します。シスコのスタンドアロン アナログ ゲートウェイは、FXS アナログ テレフォニー インターフェイスのポート タイプだけをサポートします。

Cisco ATA の詳細については、次の URL で ATA 190 シリーズに関するデータ シートとマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/ata-190-series-analog-telephone-adapters/index.html

Cisco VG シリーズ ゲートウェイの詳細については、次の URL でデータ シートとマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/vg-series-gateways/index.html

アナログ インターフェイス モジュール

Network Module（NM）および Voice Interface Card（VIC）などの Cisco IOS ルータ ベースのアナログ インターフェイス モジュールは、PBX、アナログ電話機、FAX 機、キー システムなどの PSTN やその他の従来の電話機器を、Cisco Integrated Services Router（ISR）などの Cisco マルチサービス アクセス ルータに接続します。Cisco IOS アナログ インターフェイス モジュールは、FXS、FXO、T1/E1、E&M、BRI などの広範囲のアナログ テレフォニー インターフェイスのポート タイプをサポートします。

Cisco IOS バージョンのサポートは、アナログ インターフェイス モジュールに正常に展開するために重要です。インターフェイス ポート タイプや Cisco IOS バージョンのサポートを含む Cisco IOS ベースのアナログ インターフェイス モジュールに関する詳細については、次の Web サイトにリストされているデータシートおよびマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-733646.html

アナログ エンドポイントの配置に関する考慮事項

次の項では、アナログ エンドポイントを導入するための重要な設計上の留意点について説明します。

アナログ接続タイプ

多くの場合、確立されるアナログ接続のタイプによって、どのアナログ接続タイプを選択するかが決まります。たとえば、基本的な受話器の呼出音とダイヤル トーンは、FXS または E&M インターフェイスによって提供されますが、PSTN または企業の PBX へのトランクまたはタイ ライン接続には FXO インターフェイスが使用されます。いずれの場合も、これらのインターフェイスによって、電話回線のオン フックまたはオフフック状態が指定されます。

FXO および FXS アナログ接続には、ループ スタートまたはグラウンド スタートという 2 種類のアクセス シグナリング方法があります。使用されるシグナリング タイプは、PSTN からのサービスのタイプによって最終的に決定されます。通常、標準的な電話回線はループ スタートを使用しますが、ビジネス電話回線とトランクは多くの場合グラウンド スタートに依存します。ループ スタート回線はその回線が使用されるまで回路に電流を維持しませんが、グラウンド スタート回線は回線にある程度の電流を維持します。グラウンド スタート回線で一定の電流を使用するには、通常、PSTN 側に特殊な機器が必要ですが、多くの場合、これによってループ スタート回線よりもグラウンド スタート回線のコストのほうが高くなります。ただし、グラウンド スタート回線を使用すると、回線上の電流損失はアナログ接続の遠端で即時に検出され、ゲートウェイまたは PBX は接続と切断に関して即時に指示を受け取るため、接続をより適切に制御できます。さらに、グラウンド スタート トランクは「グレア」、つまり、回線上の同時着信および発信コールの衝突の可能性を低減します。

E&M インターフェイスは、ウインク スタートや即時スタートなど、さまざまなシグナリング方式をサポートしています。ウインク スタートは E&M シグナリングの最も一般的な形式であり、インターフェイスを介して番号を送信できるようになるまで、応答の遠端から発信元の初期オフフック指示まで「ウインク」順序（オンフック、オフフック、オンフック）を使用します。一方、即時スタート シグナリングは、初期オフフック指示の後、番号が送信されるまで、終端からの応答ではなく短い一時停止を使用します。

特定の配置で使用されるアナログ インターフェイス タイプは、PSTN プロバイダー、または内部アナログ接続用に配置された機器によってサポートされるインターフェイスによって最終的に指定されます。いずれの場合も、回線の最大の可視性と制御を提供するアナログ接続タイプ用にサポートされているシグナリング方式を使用する必要があります。たとえば、FXS または FXO を使用する場合は、エンドツーエンドの回線電流の障害を即時に検出できるため、グラウンド スタートのほうがループ スタートよりも適しています。同様に、E&M を使用する場合は、番号を送信可能という遠端からの肯定的な指示により、即時スタートよりもウインク スタートのほうが優先されます。

シスコのアナログ テレフォニー シグナリングの詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

https://www.cisco.com/c/en/us/tech/voice/telephony-signaling/index.html

ページング システム

一部の IP テレフォニー配置では、エンタープライズ IP PBX はページング システムに統合され、ユーザは音声ブロードキャストをオーバーヘッド スピーカーに転送するシステムで内線を呼び出すことができます。これらのオーバーヘッド ページング システムは、着信側が受話器の近くにいないワークショップ、駐車場、および広い工場エリアなどで便利です。これらのページング システムへの統合は、アナログ インターフェイス モジュール ポートを使用して実行されます。

Cisco アナログ ゲートウェイとインターフェイス モジュールは、FXO、FXS、および E&M など、ページング システムの統合に使用するすべての従来型アナログ ポート タイプをサポートします。オーバーヘッド ページング システムと統合する場合は、必要に応じて、統合されるページング システムによって適切なアナログ インターフェイス モジュール タイプ、シグナリング、および設定が使用されていることを確認します。ポート タイプ、シグナリング、および設定は、ページング システムによって最終的に決定されます。

オーバーヘッド ページング システムへの E&M インターフェイスの統合の例は、次の Web サイトから入手できます。

https://www.cisco.com/c/en/us/support/docs/voice/analog-signaling-e-m-did-fxs-fxo/27627-e-mpaging.html

Quality of Service

ネットワーク レベルの Quality of Service（QoS）を設定すると、スタンドアロン Cisco VG シリーズや Cisco IOS ベースのアナログ インターフェイス モジュールなどの Cisco アナログ ゲートウェイが信頼され、そのパケット マーキングが尊重されます。アナログ ゲートウェイはデフォルトで、音声メディアおよびシグナリング パケットに対して適切なレイヤ 3 値（音声メディアは DSCP 46 または PHB EF、コール シグナリングは DSCP 24 または PHB CS3）でマーキングを行います。これは、統合されたネットワークでエンドツーエンドの音声品質を確保するためであり、適切な音声メディアおよびシグナリング マーキングについてのシスコの QoS 推奨事項と一致しています。

デスク フォン

Cisco IP Phone ポートフォリオには、次のデスク フォンの製品群があります。

- Cisco Unified IP Phone 7900 シリーズ（8-9 ページ）
- Cisco IP Phone 8800 シリーズ（8-10 ページ）
- Cisco Unified SIP Phone 3900 シリーズ（8-10 ページ）
- Cisco DX シリーズ（8-11 ページ）

Cisco Unified IP Phone 7900 シリーズ

Cisco Unified IP Phone 7900 シリーズのエンドポイントは、複数のモデルと機能セットで構成されます。一般に、Unified IP Phone 7900 シリーズ内のすべての電話機が、コール保留、コール転送などのエンタープライズ IP テレフォニー機能を提供します。ただし、7900 シリーズは、プレゼンス、メッセージング、モビリティ、セキュリティ、およびその他のネットワークベースのアプリケーションとサービスを可能にする IP ベースの電話サービスのサポートを含む、従来のエンタープライズ IP テレフォニー機能セットを上回る機能も提供します。Cisco Unified IP 7900 シリーズでは、シスコの呼処理プラットフォームに登録して通信するための SCCP と SIP の両方のシグナリング プロトコルをサポートします。

場合によっては、Cisco Unified IP Phone Expansion Module 7916 などのキー拡張モジュールを物理的に接続することにより、追加の回線キーを Unified IP Phone 7900 シリーズ デバイスに追加できます。これによって、管理スタッフおよびその他のユーザは、デスクトップフォンの現在の回線容量を超える回線数に応答したり、または回線の状態を確認できるようになります。一部の Unified IP Phone 7900 シリーズ モデルは 2 つまでの Cisco Unified IP Phone 拡張モジュールをサポートできますが、外部電源アダプタの使用が必要になる場合があります。

（注） 1 台の電話機で 2 つの拡張モジュールを使用する場合、2 番めのモジュールを 1 番めのモジュールと同じモデルにする必要があります。

Cisco Unified IP Phone 7900 シリーズの詳細については、次の Web サイトのデータ シートおよびマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-7900-series/index.html

Cisco IP Phone 7800 シリーズ

Cisco IP Phone 7800 シリーズのエンドポイントには、1 回線の Cisco IP Phone 7811 から、大規模でより高度な 16 回線の Cisco IP Phone 7861 まで、さまざまなモデルが含まれます。これらの電話機モデルには LCD ディスプレイ、内蔵スピーカー フォン、および PC ポートがあります。IP Phone 7800 シリーズ内のすべての電話機が、保留、コール転送、自動転送などのエンタープライズ IP テレフォニー機能を提供します。Cisco IP 7800 シリーズは、シスコ呼処理プラットフォームに登録して通信するための SIP シグナリング プロトコルをサポートします。

（注） Cisco IP Phone 7800 シリーズ ファームウェア バージョン 11.0(1) と Cisco Expressway X8.7 以降のバージョンの 7800 シリーズは、VPN アクセスの代替手段として Cisco Expressway を正式にサポートします。Expressway は、7800 シリーズの音声コールにエンタープライズ ファイアウォール トラバーサルを提供します。

Cisco IP Phone 7800 シリーズの詳細については、次の URL で入手可能なデータ シートと製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-7800-series/index.html

Cisco IP Phone 8800 シリーズ

Cisco IP Phone 8800 シリーズのエンドポイントは、広帯域オーディオのサポートと一緒に高度にセキュアで包括的な機能セットを提供します。たとえば、新しい Cisco IP Conference Phone 8832 では、歪みが少なく周波数が低くても鮮明な、動的できめ細かいサウンドを提供します。有線マイクと Digital Equipment Cordless Telephony（DECT）ワイヤレス拡張マイクの両方を使用して、会議室導入環境全体をカバーできます。さらに、IP Phone 8800 シリーズのパーソナル エンドポイント（8811 ～ 8865）でも広範な機能を揃えています。このシリーズの一部のモデル（8845、8851、8861、8865 など）は、Bluetooth と Intelligent Proximity for Mobile Voice に加えて、オンボード USB ポートを介したスマートフォンまたはタブレットの充電もサポートします。8800 シリーズに導入された新しいキー拡張モジュール（KEM）は、表示領域を最大化しユーザ エクスペリエンスを向上させるデュアル LCD サポートを提供します。新しいオーディオ KEM とビデオ KEM が導入されています。また、8845 と 8865 は、HD 720p の組み込みビデオ カメラをサポートします。一般に、IP Phone 8800 シリーズ内のすべての電話機に、保留、コール転送、自動転送などのエンタープライズ IP テレフォニー機能一式が備わっています。これらのエンドポイントでは、シスコの呼処理プラットフォームに登録して通信するための SIP シグナリング プロトコルをサポートします。

（注）　Cisco IP Phone 8800 シリーズ ファームウェア バージョン 11.0(1) と Cisco Expressway X8.7 以降のバージョンの 8800 シリーズ電話機モデルは、VPN アクセスの代替手段として Cisco Expressway を正式にサポートします。Expressway は、8800 シリーズの音声コールとビデオ コールにエンタープライズ ファイアウォール トラバーサルを提供します。

（注）　Cisco IP Phone 8800 シリーズ ファームウェア バージョン 11.5 以降の 8800 シリーズ電話機モデルでは、拡張回線モードをサポートしています。これにより、短縮ダイヤルなどのプログラム可能な回線または機能を 10 個すべての回線キーに割り当てられるようになっています。このファームウェア機能拡張が導入される前は、電話機で使用できるプログラム可能な回線キーは 5 つだけでした。また、ファームウェア バージョン 12.0 では拡張回線モードに、コール パーク、Extension Mobility Cross Cluster、グループ ピックアップ、ハント グループのサポートが追加されています。

Cisco IP Phone 8800 シリーズの詳細については、次の URL でデータ シートとその他のマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/index.html

Cisco Unified SIP Phone 3900 シリーズ

Cisco Unified SIP Phone 3900 シリーズは、単一回線をサポートするコスト効率の高い、エントリレベルのエンド ポイントを提供し、エンタープライズ IP テレフォニー機能の基本的なセットおよび、ミュート、コール保留、コール転送などの基本的な付加機能を提供します。Cisco Unified SIP Phone 3900 シリーズには、2 行の液晶ディスプレイ（LCD）画面および半二重または全二重スピーカーフォン（モデルによって異なる）があります。Cisco Unified SIP Phone 3900 シリーズでは、シスコの呼処理プラットフォームに登録して通信するのための SIP シグナリング プロトコルをサポートします。

(注)　Cisco Unified SIP Phone 3900 シリーズは、CTI（Jabber 電話機制御用）、短縮ダイヤル、サイレント モニタリングおよび録音用の組み込みブリッジなどの機能をサポートしていません。Cisco IP Phone 7800 シリーズおよび 8800 シリーズは、エンタープライズ クラスの IP テレフォニー機能のフル セットが必要な環境向けに推奨されています。

Cisco Unified SIP Phone 3900 シリーズの詳細については、次の URL でデータ シートとマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-sip-phone-3900-series/index.html

Cisco DX シリーズ

DX シリーズのエンドポイントは、ユニファイド コミュニケーション、高解像度（HD）ビデオ、コラボレーション アプリケーションおよびサービスの統合を実現します。Cisco DX シリーズ エンドポイントでは、エンタープライズクラスのコミュニケーション用の広帯域オーディオと HD ビデオに、統合された 7 ～ 23 インチ（モデルにより異なる）のマルチタッチ LCD ディスプレイと前面カメラが用意されています。このデバイスは、セキュアな Android オペレーティング システムを実行し、予定表管理、社内ディレクトリ検索、電子メール、Jabber IM and Presence、ビジュアル ボイスメール、WebEx 会議、およびセキュアなネットワーク アタッチメントのための AnyConnect VPN を含む、統合されたさまざまなコラボレーションおよびコミュニケーション アプリケーションへのアクセスを可能にします。また、オープンな Android プラットフォームとして、Google Play ストアにアクセスして、さまざまなサードパーティ アプリケーションを入手することにより、機能の追加を可能にします。このエンドポイントは、ラップトップや外部ディスプレイなどの外部デバイス（モデルによって異なる）を接続するための HDMI や、キーボード、マウス、または有線ヘッドセット アタッチメント用の USB、および無線ヘッドセット、キーボード、マウスを接続したり、Intelligent Proximity for Mobile Voice を利用したりするための Bluetooth を含む、アクセサリを接続するためのさまざまな外部インターフェイスも提供します。

DX シリーズ エンドポイントは、シスコ呼処理プラットフォームに登録して通信するための SIP シグナリング プロトコルをサポートします。DX シリーズの導入とサポートには、Cisco Unified Communications Manager が必要です。

(注)　Cisco DX シリーズ ファームウェア バージョン 10.2.4 以降の DX シリーズは、VPN アクセスの代替手段として Cisco Expressway をサポートします。Expressway は、DX シリーズの音声とビデオ用のエンタープライズ ファイアウォール トラバーサルだけでなく、組み込みの Jabber IM アプリケーションも提供します。

Cisco DX シリーズの詳細については、次の URL でデータ シートとマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/desktop-collaboration-experience-dx600-series/index.html

シスコ デスク フォンの導入に関する考慮事項

次の項では、シスコのデスク フォンを配置するときに重要な設計上の考慮事項について説明します。

ファームウェアのアップグレード

通常、IP フォンは、デフォルトで、1 つ以上の呼処理プラットフォームに統合された TFTP サービスから、ポート 6970 を使用する HTTP を使用してイメージをアップグレードします。HTTP が使用できない場合、IP フォンは、同じ TFTP サービスから、UDP ベースのプロトコルである TFTP を使用します。この配置では、すべての電話機がこれらの TFTP サービスから直接イメージを取得します。この方法は、電話機の数が比較的少ない場合や、すべての電話機が実質的に帯域幅の制限がない LAN 環境を持つ単一のキャンパス領域に存在する場合に効果的です。

集中型呼処理を使用する大規模な配置の場合は、低速 WAN リンクで中央データセンターに接続された支社の電話機をアップグレードするのに WAN を介した大量のデータ トラフィックが必要になることがあります。それぞれの電話機に対して同じファイル セットが WAN を複数回通過することになります。このような大量のデータを転送することは WAN 帯域幅を浪費するだけでなく、各データ転送がお互いに帯域幅を求めて競合するため長時間かかることがあります。また、TFTP プロトコルの特性により、一部の電話機でアップグレードが強制的に中止され、既存のバージョンのコードに戻る場合があります。

（注）　7900 シリーズの電話機と違って、Cisco IP Phone 7800、8800、および DX シリーズは稼働したままアップグレードすることができます。7800、8800、および DX シリーズの電話機は、アクティブな状態を維持しながら、新しいファームウェアをメモリにダウンロードして保存し、ダウンロードが正常に行われた場合にのみ新しいファームウェアでリブートします。

WAN を介して電話機をアップグレードすることが必要なため生じた問題を緩和するのに 2 つの方法が存在します。1 つの方法はアップグレードのためだけにローカル TFTP サーバを使用することです。管理者は TFTP サーバを支社（特に大量の電話機が存在する支社あるいは WAN リンクが高速または堅牢でない支社）に設置し、支社の電話機がその特定の TFTP サーバを新しいファームウェアのためだけに使用するように設定できます。この変更により、電話機が新しいファームウェアをローカルに取得します。このアップグレード方法では、管理者が支社の TFTP サーバに電話機のファームウェアを事前にロードし、影響を受ける電話機の設定の **load server** パラメータの TFTP サーバ アドレスを手動で設定する必要があります。支店のルータを TFTP サーバとして使用できることに注意してください。

WAN リソースを大量に使用せずに電話機をアップグレードする 2 つめの方法は、ピア ファイル共有（PFS）機能を使用することです。この機能を使用した場合、通常は、支店内の各モデルの電話機が 1 台ずつ新しいファームウェア ファイルを中央の TFTP サーバからダウンロードします。電話機がファームウェア ファイルをダウンロードしたら、この電話機はそのファイルを支社の他の電話に配布します。この方法では、load server の方法で必要な手動によるロードと設定を回避できます。

アップグレードが要求された際、同じ支社のサブネット内の同じ電話機モデルが自身の階層形式（チェーン形式）で配置されると、PFS 機能が動作します。これは、電話機間でメッセージを交換し、実際にダウンロードを実行する「ルート」電話機を選択することによって行われます。ルート電話機は TCP 接続を使用してチェーンの 2 つめの電話機にファームウェア ファイルを送信し、2 つめの電話機はチェーンの 3 つめの電話機にファームウェア ファイルを送信し、というようにチェーンのすべての電話機がアップグレードされるまでこの作業が繰り返されます。ルート電話機は完全な電話ファームウェアを構成するファイルに応じて異なる場合があることに注意してください。

Power Over Ethernet

インライン パワー対応スイッチを備えたデスクフォンを配置すると、これらのエンドポイントは、イーサネット ネットワーク接続を介して電力を取得できます。これによって、外部電源および壁面コンセントが不要になります。インライン パワー対応のスイッチに無停電電源装置（UPS）を付けると、Power over Ethernet（PoE）対応の IP デスクフォンが電源障害の発生中も電力を継続して受けることが保証されます。この電源障害の発生中にテレフォニー ネットワークの残りの部分が使用可能であれば、IP Phone はコールの発信および受信を継続して行うことができます。

デスクフォンのタイプおよび、デスクフォンとインライン パワー対応スイッチの両方でサポートされる PoE 規格により、場合によっては、インライン パワースイッチ ポートの電力バジェットが超過することがあります。これは通常、キー拡張モジュールを取り付けたり、USB カメラなどの電力消費アタッチメントを接続した場合に発生します。この場合、電話機に壁面コンセントまたは外部電源を使用して電力を供給する必要があり、あるいは電源を供給するスイッチをアップグレードする必要があります。

（注）　Cisco Unified IP Phone は、アクセス スイッチからのインライン パワー、またはローカルの壁面コンセントからの電源供給を使用することに加えて、Cisco Unified IP Phone パワー インジェクタによる電源供給も可能です。Cisco Unified IP Phone パワー インジェクタを使用すると、インライン パワーをサポートしない Cisco スイッチまたは Cisco 以外のスイッチに、Cisco Unified IP Phone を接続できます。Cisco Unified IP Phone パワー インジェクタは、ほとんどの Cisco Unified IP Phone と互換性があります。Cisco Unified IP Phone パワー インジェクタは、2 つの 10/100/1000 Base-T イーサネット ポートを備えています。一方のイーサネット ポートをスイッチのアクセス ポートに接続し、もう一方を Cisco Unified IP Phone に接続します。

Quality of Service

ネットワーク レベルの Quality of Service（QoS）を設定すると、Cisco Unified IP Phone 7900、8800、DX シリーズなどのシスコ デスク フォンが信頼され、そのパケット マーキングが尊重されます。このエンドポイントは、デフォルトで、音声メディアおよびシグナリング パケットに対して適切なレイヤ 3 値（音声メディアは DSCP 46 または PHB EF、コール シグナリングは DSCP 24 または PHB CS3）でマーキングを行います。これは、コンバージド ネットワーク上のエンドツーエンドの音声品質を確保するためであり、適切な音声メディアおよびシグナリング マーキングに関するシスコの QoS 推奨事項と一致します。多くのシスコのデスクフォンがデスクトップ コンピュータの接続をサポートしますが、シスコのデスクフォンは、音声およびデータ トラフィックを分離し、音声トラフィックを音声 VLAN に配置し、デスクトップからのデータ トラフィックをデータ VLAN に配置することができます。これにより、ネットワークが信頼性を電話機まで拡張します。ただ、電話機の PC ポートまでではありません。ただし、デスクトップ コンピュータと接続せずに音声トラフィックとデータ トラフィックの両方を生成可能な Cisco DX シリーズ エンドポイントのような多目的デバイスでは、音声トラフィックとデータ トラフィックの両方が同じ VLAN を通過します。このような場合、デバイスが音声またはデータ VLAN に接続されていても、これらのデバイスに信頼性を拡張することは得策でない可能性があります。代わりに、ポートおよびプロトコルに基づいてトラフィックを再マーキングすると、すべてのトラフィックが通過する VLAN に関係なく適切にマーキングされるようになります。

Cisco DX シリーズなどの多目的デバイスによって生成される可能性があるデータ トラフィック量やリアルタイムの音声およびビデオ トラフィックに悪影響を及ぼす可能性が懸念される導入では、これらのデバイスをデータ VLAN または個別の VLAN に導入する必要があります。これにより、音声とビデオ専用デバイスのコール品質に影響する不安が軽減されます。さらに、ポートおよびプロトコルに基づいたパケットの再マーキングでは、多目的デバイスによって生成されるリアルタイム トラフィックに対してプライオリティ処理が VLAN 内で引き続き提供されます。

（注）　多くの Cisco デスクフォンで Link Layer Discovery Protocol for Media Endpoint Devices（LLDP-MED）がサポートされますが、これは VLAN および Power over Ethernet ネゴシエーションのためにのみ行われます。Cisco Unified IP Phone では、LLDP-MED によって提供される DSCP および CoS マーキングは受け入れられません。

SRST と拡張 SRST

低速な、または信頼できない WAN リンクにより集中型呼処理プラットフォームから隔てられた支社のロケーションに Cisco デスク フォンを展開する場合、ローカル呼処理の冗長化を検討することが重要です。各支社ロケーションの Cisco IOS ルータ上で Survivable Remote Site Telephony（SRST）または拡張 SRST を使用することで、集中型呼処理プラットフォームへの接続が失われた場合でもデスクフォンのエンドポイントの基本的な IP テレフォニー サービスは維持できます。ただし、デバイスが SRST に登録された場合に使用可能な一連の対ユーザ機能は、電話が Unified CM に登録された場合よりもずっと少なくなります。

リモート エンタープライズ接続の保護

Cisco デスクトップフォンは、VPN または VPN-less ソリューションを使用してリモート ロケーションから企業ネットワークに安全に接続できます。

VPN ベース接続の場合、エンタープライズ エッジに Cisco Adaptive Security Appliance（ASA）または他の VPN ヘッドエンド コンセントレータへの安全な VPN トンネルを作成する VPN ルータの後ろにデスクトップフォンを配置することができます。また、一部の電話機モデルは、PC またはデータ トラフィックではなく、デバイスの音声トラフィック（メディアおよびシグナリング）に対して電話機内で VPN 接続を提供するネイティブの内蔵 VPN クライアントをサポートします。この場合、電話機は社内の Cisco ASA への安全な VPN トンネルを作成します。ネイティブの組み込み VPN クライアントは、Cisco Unified IP Phone 7945、7965、および 7975 のほか、8800 シリーズの電話機を含む特定の電話機モデルでのみサポートされます。Cisco Unified IP Phone の内蔵 VPN の詳細については、次のサイトで入手可能な最新バージョンの『*Security Guide for Cisco Unified Communications Manager*』を参照してください。

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

（注）　7800 シリーズは、組み込み VPN をサポートしません。また、7800 シリーズは、ファームウェア バージョン 11.0(1) 以降と Expressway X8.7 以降のバージョンの Expressway Mobile and Remote Access をサポートします。

Cisco IP Phone 7800 シリーズ、IP Phone 8800 シリーズ、および DX シリーズ エンドポイントは、Cisco Expressway ソリューションのモバイルおよびリモート アクセス機能を利用できます。このファイアウォール トラバーサル ソリューションは、Cisco Expressway-E サーバおよび Expressway-C サーバによって規定されているように、音声通話とビデオ通話の Unified CM 呼制御への登録をエンタープライズへの TLS リバース プロキシ接続に依存します。Cisco Expressway ソリューションのモバイルおよびリモート アクセス機能の詳細については、次の Web サイトのソリューション情報および製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html

インテリジェント プロキシミティ

インテリジェント プロキシミティは、シスコ ハードウェア エンドポイントとモバイル デバイス間のプロキシミティベースの接続を利用する機能を意味します。

Cisco DX シリーズと一部の 8800 シリーズ エンドポイント上で使用可能な Intelligent Proximity for Mobile Voice 機能は、DX または 8800 エンドポイントとセルラーまたはスマートフォン間の Bluetooth ペアリングの使用に依存します。

Bluetooth でペアリングされたモバイル デバイスは、次の 2 つの機能を呼び出すことができます。

- DX シリーズ、8845、8851、8861、または 8865 IP エンドポイントのスピーカーまたはハンドセット経由でセルラー終端コールの音声を送信可能なハンズフリー音声。セルラー終端コールの音声再生は、DX、8845、8851、8861、または 8865 とモバイル デバイス間で移動できます。加えて、8845、8851、8865、または DX シリーズ エンドポイントでは Bluetooth でペアリングされたモバイル デバイスが別の回線として認識されるため、Bluetooth でペアリングされたモバイル デバイス上のセルラー コールは DX または 8800 IP エンドポイントを使用して発信できます。
- DX シリーズ、8845、8851、8861、または 8865 エンドポイントと、モバイル デバイス連絡先および通話履歴共有を共有する機能を提供する、モバイル連絡先および通話履歴共有。

Intelligent Proximity for Mobile Voice は Bluetooth ペアリングに依存しているため、モバイル デバイス上でアプリケーションまたはクライアントを実行する必要がありません。すべての通信と相互作用が標準ベースの Bluetooth インターフェイス経由で発生します。

DX シリーズ エンドポイントと 8845、8851、8861、および 8865 IP フォン上の Intelligent Proximity for Mobile Voice 機能セットは、シングル ナンバー リーチ（SNR）、リモート接続先とデスク フォン ピックアップ、2 段階エンタープライズ ダイヤリング、およびモバイル ボイスメール回避を含む、Unified Mobility 機能セットと互換性があります。8845、8851、8861、および 8865 IP フォンの場合は、Intelligent Proximity for Mobile Voice が Cisco Jabber モバイル クライアントと互換性があります。モバイル デバイス上で実行中の Jabber クライアントが 8845、8851、8861、または 8865 IP フォンとペアリングされている場合は、Jabber コールの音声部分が 8845、8851、8861、または 8865 のハンドセットまたはスピーカーを使用して再生されるのに対して、コールのビデオ部分は引き続き Jabber モバイル クライアント上で再生されます。DX シリーズ エンドポイントの場合、Intelligent Proximity for Mobile Voice 機能は、Bluetooth でペアリングされた Jabber を実行しているモバイル デバイスのセルラー回線のみに制限されます。

DX シリーズと一部の 8800 シリーズ エンドポイント上の Intelligent Proximity for Mobile Voice 機能セットには、ファームウェア　バージョン 10.1.1 以降が必要です。

（注）　Cisco IP Phone 8800 シリーズ ファームウェア バージョン 11.0(1) 以降の 8845、8851、8861、および 8865 電話機は、Cisco VoIP ネットワーク経由のインポートされたスマートフォン連絡先へのダイヤリングを許可する Cisco Unified CM アプリケーション ダイヤル ルールをサポートします。

Intelligent Proximity for Mobile Voice の詳細については、Cisco DX シリーズおよび 8800 シリーズ エンドポイントの製品マニュアルと、以下のリンク先ページに記載されている情報を参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html

ビデオ エンドポイント

Cisco ビデオ エンドポイントは、IP 音声テレフォニーと同じような機能を IP 音声テレフォニーに提供し、ユーザがポイント ツー ポイントおよびポイントツーマルチポイントのビデオ コールができるようになります。シスコでは、次のビデオ対応エンドポイントを提供します。

- Cisco Jabber for Windows などの Cisco Jabber ソフトウェア ベース デスクトップ クライアント
- カメラ内蔵 Cisco Unified IP Phone 8800 シリーズ（8845 または 8865）
- カメラ内蔵 Cisco DX シリーズ
- Cisco TelePresence System EX、MX、SX、および IX シリーズ
- Cisco Spark Room Kit シリーズ

シスコのビデオ エンドポイントは、組織内のどこにおいても、すべてのユーザおよび環境に高品質ビデオを提供します。シスコのビデオ エンドポイントは、サポートする機能、ハードウェアの画面サイズ、およびエンドポイントが配置される環境に基づいて複数のファミリに分類されます。ここでは、シスコ ビデオ エンドポイントのファミリをパーソナル、多目的、およびイマーシブ エンドポイントのグループに分類します。

パーソナル ビデオ エンドポイント

パーソナル ビデオ エンドポイントは、パーソナル ワークスペースに高品質で対面型のビデオ通話エクスペリエンスを提供します。

Cisco Jabber デスクトップ ビデオ

Cisco Jabber for Windows などの Cisco Jabber ソフトウェアベース デスクトップ クライアントは、組み込みカメラまたは USB で接続されたカメラを持つデスクトップ コンピュータで実行すると、ビデオの送受信が行えます。これらのビデオ対応ソフトウェア ベースのエンドポイントは、Unified CM 呼制御で登録および通信を行い、SIP の単一回線の音声とビデオ対応の電話機として動作します。これらのエンドポイントは、Unified CM によってプライマリおよびバックアップの登録の冗長性メカニズムをサポートします。Cisco Jabber ソフトウェア ベースのエンドポイントは、インストールされているコンピュータ上のビデオを処理します。デコーディングとエンコーディングの品質は、コンピュータの CPU とメモリ リソースの可用性によって決まります。

Cisco Jabber デスクトップ デスクトップの詳細については、ソフトウェアベースのエンドポイント（8-24 ページ）を参照してください。

Windows 用の Cisco Jabber のビデオ機能の詳細については、次の Web サイトで入手可能なデータ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/jabber-windows/index.html

Cisco IP Phone 8800 シリーズ

このシリーズに含まれる一部のモデル、特に、8845 と 8865 は、内蔵のビデオ カメラで HD 720p をサポートします。8845 と 8865 の主な違いは、8865 はオンボード USB ポート経由でスマートフォンやタブレットの充電もサポートすることです。また、8865 は、最大 3 つのキー拡張モジュールをサポートします。通常、8845 と 8865 は、コール保留、コール転送、自動転送などのエンタープライズ IP テレフォニー機能と一緒に内蔵ビデオ体験を提供します。これらのエンドポイントでは、シスコの呼処理プラットフォームで登録および通信するための SIP シグナリング プロトコルをサポートします。

Cisco IP Phone 8800 シリーズの詳細については、次の URL でデータ シートとマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/index.html

Cisco DX シリーズ

Cisco DX シリーズ エンドポイントは、内蔵の前面カメラを使ってビデオを送信できます。これらのエンドポイントは、さまざまなビデオ解像度とフレーム レートで画面にビデオをネイティブに受信したり、表示したりできます。これらの電話機のビデオ機能は、シスコの呼制御プラットフォーム設定ページから、必要に応じて有効化、無効化、または調整できます。

これらのデバイスは SIP シグナリング プロトコルを使用して Unified CM で登録および通信を行います。

Cisco DX シリーズのビデオ機能の詳細については、次の URL で入手可能なデータ シートと製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/desktop-collaboration-experience-dx600-series/index.html

Cisco TelePresence System EX90

Cisco TelePresence System EX90 ビデオ エンドポイントは、パーソナル デスクトップ ソリューションを、フル高解像度（HD）ビデオ コールと、コンテンツ シェアリングなどの追加機能をサポートすることによって次のレベルのエクスペリエンスに高めます。EX90 には、参加者を Cisco TelePresence コールに追加する機能を提供するマルチサイト機能をサポートする大きい画面と、コンテンツ共有用のデュアル ディスプレイが備わっています。

Cisco TelePresence System EX90 ビデオ エンドポイントは、SIP シグナリング プロトコルを使用して Unified CM に登録して通信します。

Cisco TelePresence EX90 ビデオ エンドポイントの詳細については、次の URL で入手可能なデータ シートと製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-system-ex-series/index.html

多目的ビデオ エンドポイント

多目的ビデオ エンドポイントを使用すると、どのような規模の会議室でも、高品質なポイントツーポイントまたはマルチポイントのビデオ コラボレーションとコンテンツ共有を提供することで、テレプレゼンス ルームとして使用することができます。

Cisco TelePresence System MX シリーズ

MX シリーズの Cisco TelePresence エンドポイントは、多目的ルーム システムに分類される高度に統合されたコラボレーション ルーム システムを提供します。これらのビデオ エンドポイントは使用しやすく、容易にインストールでき、プレゼンテーション中にビデオ コールとコンテンツ共有を提供します。これらはコスト効率の良いエンドポイントであり、どのような部屋や既存の会議スペースでも、フルハイデフィニション（HD）ビデオ コールを提供することで、多目的会議室に転換できます。MX シリーズには次の 4 種類があります。

- MX800 は、シングルまたはデュアル 70 インチ画面内蔵 TelePresence システムです。
- MX700 は、デュアル 55 インチ画面内蔵 TelePresence システムです。
- MX300 G2 は、55 インチ画面内蔵 TelePresence システムです。
- MX200 G2 は、42 インチ画面内蔵 TelePresence システムです。

これらのエンドポイントは SIP シグナリング プロトコルを使用して Unified CM に登録されます。

Cisco TelePresence System MX シリーズ ビデオ エンドポイントの詳細については、次の Web サイトで入手可能なデータ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-mx-series/index.html

Cisco TelePresence SX シリーズ

Cisco TelePresence SX シリーズは、任意のフラットパネル ディスプレイを強力な Cisco TelePresence システムに変換する柔軟なインテグレータです。SX シリーズ ビデオ エンドポイントは、HD ビデオとマルチパーティ会議用に設計されており、さまざまな部屋のサイズに柔軟に対応します。これは、小規模から中規模の企業や、コスト効率の良い TelePresence 対応の会議室のソリューションを探している企業にとって理想的なソリューションです。SX シリーズ ビデオ エンドポイントは次のオプションを備えています。

- SX10 は、カメラが内蔵されたオールインワン システム コーデックです。
- SX20 は、3 つのカメラ オプションの 1 つを備えたコーデックであり、1 つの Cisco TelePresence コールで最大 3人の参加者を追加できるマルチサイト機能をサポートします。
- SX80 は、さまざまなカメラとタッチパネル オプションをサポートするインテグレータ パッケージを含むコーデックです。

これらのエンドポイントは SIP シグナリング プロトコルを使用して Unified CM に登録されます。

Cisco TelePresence SX シリーズ ビデオ エンドポイントの詳細については、次の URL で入手可能なデータ シートと製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-quick-set-series/index.html

Cisco Spark Room シリーズ

Cisco Spark Room シリーズ エンドポイントには、どんな部屋や既存の会議スペースでも多目的会議室に変換できる高度に統合されたコラボレーション ルーム システムと、任意のフラットパネル ディスプレイを強力な Cisco TelePresence システムに変換できる柔軟なインテグレータの両方が組み込まれています。Cisco Spark Room シリーズ ビデオ エンドポイントは 4K の超高解像度ビデオと画面共有およびマルチパーティ会議用に設計されており、さまざまな部屋のサイズに柔軟に対応します。

Cisco Spark Room シリーズには 4 つのバリエーションがあります。

- Cisco Spark Room Kit は、カメラが内蔵されたオールインワン システム コーデックです。
- Cisco Spark Room Kit Plus は、それぞれが独立したコーデックを使用するクアッド カメラ システムです。
- Cisco Spark Room 55 は、55 インチ画面が統合された TelePresence システムです。
- Cisco Spark Room 70 は、70 インチのシングルまたはデュアル画面が統合された TelePresence システムです。

これらのエンドポイントは、Cisco Unified CM（SIP シグナリング プロトコルを使用する場合）または Cisco Collaboration Cloud（HTTPS を使用する場合）に登録されます。

Cisco Spark Room シリーズ ビデオ エンドポイントの詳細については、次の URL で入手可能なデータ シートと製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/spark-room-series/index.html

イマーシブ ビデオ エンドポイント

イマーシブ ビデオ エンドポイントを使用して、可能な限り最適な対面テレプレゼンス ビデオ コラボレーションを行うことができます。ここでは、さまざまな場所に居る出席者がまるで同じ部屋にいるかのように感じます。

Cisco TelePresence IX5000 シリーズ

Cisco TelePresence IX5000 シリーズは、業界初の H.265 3 画面 TelePresence システムを使用した「対面式」コラボレーションの水準を高めます。このイマーシブ システムは、使いやすいだけでなく、設定も非常に簡単です。このシステムには、1 列 6 シート IX5000 システムと 2 列 18 シート IX5200 システムの 2 種類があります。これらのシステムは、3 つの同時高解像度（1080p、60 fps）ビデオ ストリームと 2 つのコンテンツ シェアリング ストリーム（1080p、30 fps）を配信できます。これらのエンドポイントは SIP シグナリング プロトコルを使用して Unified CM に登録されます。

Cisco TelePresence IX5000 シリーズ イマーシブ ビデオ システムの詳細については、次の URL で入手可能なデータ シートと製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/ix5000-series/index.html

ビデオ エンドポイントの配置に関する一般的な考慮事項

次の項では、ビデオ エンドポイントを配置するための重要な設計上の考慮事項について説明します。

Quality of Service

ネットワーク レベルの Quality of Service（QoS）を設定すると、シスコ ビデオ エンドポイント（Cisco DX シリーズと Cisco TelePresence System デバイスを含む）の多くが音声およびビデオ パケット マーキング（音声メディアは DSCP 46 または PHB EF、デスクトップ ビデオ メディアは DSCP 34 または PHB AF41、テレプレゼンス ビデオ メディアは DSCP 32 または PHB CS4、コール シグナリングは DSCP 24 または PHB CS3）に関連したシスコ汎用 QoS ガイドラインに従ってレイヤ 3 でトラフィックをマーキングするため、これらのデバイスは信頼できます。Cisco DX シリーズ デバイスを含むパーソナル デスクトップ ビデオ エンドポイントの場合は、音声メディア パケットとビデオ メディア パケットの両方が DSCP 34 または PHB AF41 とマーキングされ、ビデオ コール中のリップシンクが維持されます。

適切なネットワーク QoS 設定は不可欠ですが、エンドポイントのマーキングが信頼される場合でも、ネットワーク上に十分な帯域幅が用意されていることを確認し、ネットワーク ベースのポリシングとレート制限を使用して、すべてのエンドポイントが必要以上のネットワーク帯域幅を消費しないようにすることをお勧めします。ソフトウェア ベースのビデオ対応エンドポイントは、トラフィックを適切にマークしない、またはマークできない場合の課題になります。この場合、一般的なガイダンスは、プロトコルまたはポート番号に基づいて、ネットワーク内のメディアおよびシグナリング トラフィックを、ベスト エフォートから適切な推奨値（音声メディアは DSCP 46 または PHB EF、ビデオ コールに対するデスクトップ ビデオおよび音声メディアは DSCP 34 または PHB AF41、テレプレゼンス ビデオ メディアは DSCP 32 または PHB CS4、コール シグナリングは DSCP 24 または PHB CS3 として）に再マークすることです。

ソフトウェア ベースの Cisco Jabber for Windows の場合、Microsoft Windows グループ ポリシーを使用して、音声およびビデオ メディア ソース ポート番号に基づき、該当するレイヤ 3 DSCP QoS マーキングを音声およびビデオ ストリームに適用できます。

Microsoft Windows グループ ポリシーを使用した Cisco Jabber for Windows QoS の詳細については、次の URL で入手可能な最新バージョンの『*On-Premises Deployment for Cisco Jabber*』で Quality of Service 設定に関する情報を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

（注）　一部のシスコのビデオ対応エンドポイントで Link Layer Discovery Protocol for Media Endpoint Devices（LLDP-MED）がサポートされていますが、これは VLAN および Power over Ethernet ネゴシエーションのためにのみ行われます。Cisco ビデオ エンドポイントでは、LLDP-MED によって提供される DSCP および CoS マーキングは受け入れられません。

ビデオ エンドポイント ネットワーク帯域幅の消費と、QoS のマーキングおよび分類の詳細については、WAN の Quality of Service（QoS）（3-39 ページ）の当該項を参照してください。

VLAN 間ルーティング

音声 VLAN とデータ VLAN を分離したネットワークでビデオ エンドポイントを配置する場合は、ソフトウェア ベースのビデオ対応エンドポイント、およびリソースにアクセスする必要があるハードウェア ベースのビデオ エンドポイントを考慮することが重要です。デスクトップ コンピュータで実行されるソフトウェア ベースのエンドポイントがデータ VLAN に主に接続されるため、VLAN 間ルーティングでは、データ VLAN 上のこれらのエンドポイントから音声トラフィックを音声 VLAN 上のエンドポイントに到達できるように設定および許可される必要があります。同様に、Cisco TelePresence System エンドポイントなどのハードウェア ベースのビデオ エンドポイントが、データ VLAN 上に配置されるディレクトリや管理サービスなどのネットワーク リソースにアクセスする必要がある場合、VLAN 間ルーティングを許可する必要があります。

SRST と拡張 SRST

低速と信頼性の低い WAN リンクで集中型呼処理プラットフォームから分離された支社ロケーションにビデオ エンドポイントを配置する場合は、ローカル呼処理の冗長性を考慮することが重要です。各支社ロケーションの Cisco IOS ルータ上で SRST または拡張 SRST を配置することで、集中型呼処理プラットフォームへの接続が失われた場合でもほとんどのビデオ エンドポイントの基本的な IP テレフォニー サービスは維持できます。使用可能なユーザ機能セットは、アプリケーションが Unified CM に登録されている場合に比べ、ビデオ エンドポイントが SRST に登録されている場合は少なくなります。具体的には、SRST に登録されたビデオ エンドポイント デバイスは音声コールのみ（音声のみ）を送受信できます。SRST は、Cisco TelePresence System ビデオ エンドポイントではサポートされません。ただし、電話機ロード ファームウェア 9.4.1 以降を使用する Cisco IOS リリース 15.3(3)M 以降の Enhanced SRST は、WAN 障害時の一部のビデオ エンドポイントによるビデオ コールの発信と受信をサポートします。さまざまな電話機モデルの拡張 SRST ビデオ サポートの詳細については、次の Web サイトの Cisco Unified IP Phone マニュアルを参照してください。

https://www.cisco.com/

リモート エンタープライズ接続の保護

Cisco ビデオ エンドポイントは、VPN または VPN-less ソリューションを使用してリモート ロケーションから企業ネットワークに安全に接続できます。

VPN ベース接続の場合、エンタープライズ エッジに Cisco Adaptive Security Appliance（ASA）または他の VPN ヘッドエンド コンセントレータへの安全な VPN トンネルを作成する VPN ルータの後ろにすべてのビデオ エンドポイントを配置することができます。加えて、Cisco Unified IP Phone 8800 シリーズは、VPN ルータを使用することなく、音声トラフィックとビデオ トラフィック（メディアとシグナリング）に対して電話機内部の VPN 接続を提供する、ネイティブの組み込み VPN クライアントをサポートします。

VPN-less 接続の場合は、TC ファームウェアを実行している Cisco TelePresence エンドポイント（EX、MX、C、および SX シリーズ エンドポイント）だけでなく、DX シリーズ エンドポイントも Cisco Expressway ソリューションのモバイルおよびリモート アクセス機能を利用できます。このファイアウォール トラバーサル ソリューションは、Cisco Expressway-E サーバおよび Expressway-C サーバによって規定されているように、音声通話とビデオ通話の Unified CM 呼制御への登録をエンタープライズへの TLS リバース プロキシ接続に依存します。Cisco Expressway ソリューションのモバイルおよびリモート アクセス機能の詳細については、次の Web サイトのソリューション情報および製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html

インテリジェント プロキシミティ

前述したように、インテリジェント プロキシミティは、シスコ ハードウェア エンドポイントとモバイル デバイス間のプロキシミティベースの接続を利用する機能を意味します。

Cisco IP Phone 8800 シリーズまたは Cisco DX シリーズ上で使用可能な Intelligent Proximity for Mobile Voice 機能は、DX エンドポイントとセルラーまたはスマートフォン間の Bluetooth ペアリングに依存し、ハンズフリーの音声/モバイル連絡先および通話履歴共有を可能にします。

インテリジェント プロキシミティと Bluetooth ペアリングの詳細については、インテリジェント プロキシミティ（8-15 ページ）を参照してください。

ビデオの相互運用性

ビデオの相互運用性とは、Cisco TelePresence System ビデオ エンドポイント、他の Cisco Collaboration ビデオ エンドポイント、およびサードパーティ製ビデオ エンドポイント間でポイントツーポイント コールの音声とビデオをサポートすることです。以前は、異なるファミリのビデオ エンドポイント間におけるビデオの相互運用性は、ビデオ トランスコーダやマルチポイント コントロール ユニット（MCU）などのビデオ コンポーネントをエンドポイントの間に挿入した場合にのみ実現できました。

Cisco Unified CM は、異なるエンドポイント ファミリ タイプ間のネイティブ ビデオの相互運用性が提供されるだけでなく、SIP および H.323 プロトコルでの H.264 コーデック ネゴシエーションによってビデオの相互運用性が全体的に向上し、利用可能な場合は高品位（HD）解像度をエンドポイントでネゴシエートできるようになりました。ただし、ビデオの相互運用性は相互運用をサポートするエンドポイントによって異なります。

Unified CM のビデオの相互運用性により、Cisco TelePresence System ビデオ エンドポイントはビデオ以外のエンドポイントと通信できます。ただし、インストールされているファームウェアでそのような相互運用性がサポートされている場合に限ります。詳細については、次の Web サイトで入手可能な『*Cisco TelePresence Interoperability Database*』を参照してください。

https://tp-tools-web01.cisco.com/start/

また、Cisco Unified CM には、Unified CM 以外のコール エージェントとの相互運用性を強化するためのサポートが提供されています。スクリプトを使用して、Unified CM は次の機能をサポートします。

- SIP 透過性：既知および未知のメッセージ コンポーネントをパススルーすることが可能
- SIP の正規化：着信および発信 SIP メッセージおよびコンテンツ本文の変換

このビデオ相互運用性サポートの主な目的は、他の方法で必要になる高価なハードウェア ベースの DSP インフラストラクチャを配置することなく、さまざまなエンドポイントの相互作用を促進することです。高度な会議およびトランスコーディング リソースを使用することによって、さらに利益を得ることができます（たとえば、マルチ ポイント会議の参加者がアクティブなスピーカーを観ることができるアクティブ プレゼンスなど）。ただし、目的の機能セットとビデオ コールのニーズによって、それらの高度なリソースが必要になる条件と場所が決定されます。

次の項では、ビデオの相互運用性の使用に関する一般的な考慮事項と推奨事項を示します。

- ビデオの相互運用性アーキテクチャ（8-22 ページ）
- ビデオの相互運用性に関する設計上の考慮事項（8-23 ページ）

ビデオの相互運用性アーキテクチャ

ビデオの相互運用性アーキテクチャには、次の要素が含まれます。

- Cisco Unified CM で使用可能なビデオ相互運用性サポート
- ビデオ コールに参加している 2 種類のビデオ エンドポイント ファミリ タイプ（Cisco TelePresence System ビデオ エンドポイント、Cisco DX80 などのその他の Cisco Collaboration ビデオ エンドポイント、またはサードパーティ エンドポイント）

次の項では、ビデオの相互運用性サポートの範囲について詳しく説明します。

- ビデオの相互運用性のテスト ケース（8-23 ページ）
- ビデオの相互運用性の制限（8-23 ページ）

ビデオの相互運用性のテスト ケース

ほとんどの場合、独自のシグナリングを使用せずに SIP または H.323 をサポートするビデオ エンドポイントは、ビデオの相互運用性をサポートする Cisco Collaboration ビデオ エンドポイントと相互運用できます。導入されたデバイスの共通セット間の相互運用性の範囲に関する特定の情報と、相互運用性のより一般的な例を検証するために実施されたテストに関する一般情報については、次の URL で入手可能な Cisco Collaboration System のマニュアルを参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/ucstart.html

ビデオの相互運用性の制限

ビデオの相互運用性のサポートでは、任意間のポイントツーポイント ビデオ コールの相互運用性を実現しようとしますが、別のエンドポイントと相互運用するときに、個々のビデオ エンドポイントのすべての機能がサポートされるとは限りません。これにはさまざまな理由があります。たとえば、異なる呼制御プロトコル間の非互換性は、機能の使用不能や別の表示につながる可能性があります。別の例として、H.264 ビデオ メディア パラメータは、H.323 では SIP と異なる表現になることがあります。また、H.323 ではプレゼンスがサポートされませんが、SIP ではプレゼンスは一般的にサポートされています。Skinny Client Control Protocol（SCCP）には、SIP および H.323 のエンドポイント実装で一般的に利用可能なアプリケーション共有の概念がありません。たとえば、PC 画面を共有しようとしている SCCP ユーザはその操作を阻止されます。これは、SCCP で Binary Flow Control Protocol（BFCP）と H.239 が使用できないためです。

ビデオの相互運用性に関する設計上の考慮事項

Unified CM のビデオの相互運用性機能を実装するときに、次の領域を考慮する必要があります。

- ビデオの相互運用性に関するガイドラインと制約事項（8-23 ページ）
- ビデオの相互運用性のための Quality of Service（QoS）とコール アドミッション制御に関する考慮事項（8-24 ページ）

ビデオの相互運用性に関するガイドラインと制約事項

Unified CM 配置におけるビデオの相互運用性に関しては、次のガイドラインと制約事項が適用されます。

- H.323 または SCCP プロトコルをビデオの相互運用性と併用する場合は、Unified CM によって単一の H.264 ペイロードのみがサポートされ、パケット化モードは 0 として処理されます。この状況の副次的な影響（1 つだけではありません）の例として、1080p 解像度にはパケット化モード 1 が必要になるため、これらのプロトコルでは 1080p を利用できないということがあります。
- ビデオの相互運用性コールに参加している H.323 または SCCP エンドポイントによって複数のペイロードが提示される場合、Unified CM ではコーデック プロファイルが最も低いペイロードのみが使用されます。これにより、サポートされている最高の解像度より低い解像度がコールに選択される可能性があります。
- SIP エンドポイントでセッション記述プロトコル（SDP）の **level-asymmetry-allowed** パラメータが省略されると、シスコ製品はエンドポイントが非対称の解像度送信をサポートできると想定します。したがって、受信側と送信側で異なるビデオ解像度もコール中にネゴシエートできます。

- Unified CM で SIP と H.323 によるプロトコル インターワーキングが実行されている間にコールをビデオの相互運用性で処理する場合、H.323 ビデオ エンドポイントは SIP 側で指定されたダイナミック ペイロード番号を受け入れます。つまり、別のペイロードへの再ネゴシエーションはサポートされません。
- ビデオ コールによってメディア ターミネーション ポイント（MTP）またはトランスコーダが呼び出された場合、Unified CM は Real-Time Transport Control Protocol（RTCP）のフィードバックをネゴシエートしません。

ビデオの相互運用性のための Quality of Service（QoS）とコール アドミッション制御に関する考慮事項

ビデオの相互運用性がサポートされても、Unified CM のリージョンとロケーションの設定に変更はありません。ただし、リージョンはエンドポイントのグループ間の解像度を決定するときに重要な役割を果たし、これらのデバイスで相互運用時に使用される解像度の最大化または最小化に使用できます。リージョン設定の [ビデオ コールの最大ビットレート（Max Video Call Bit Rate）] フィールドは、帯域幅およびエンドポイントがネゴシエートできる解像度を決定するために使用されます。

ネイティブ ビデオの相互運用性による QoS とコール アドミッション制御の詳細については、ビデオの展開に関するコール アドミッション制御の設計上の推奨事項（13-85 ページ）の項を参照してください。

ソフトウェアベースのエンドポイント

ソフトウェア ベースのエンドポイントは、音声およびビデオ サービスのシスコの呼処理プラットフォームで登録および通信するクライアント デスクトップ コンピュータにインストールされたアプリケーションです。また、これらのエンドポイントのソフトウェア クライアント アプリケーションは、メッセージング、プレゼンス、ディレクトリ アクセスや会議などのコラボレーション機能およびサービスを提供することがあります。ソフトウェアベースのエンドポイント デスクトップ クライアント アプリケーションには、Cisco IP Communicator と Cisco Jabber が含まれます。

Cisco IP Communicator

Cisco IP Communicator は、デスクトップ コンピュータにエンタープライズ IP Phone の機能を提供する Microsoft Windows ベースのアプリケーションです。このアプリケーションは、リモート ユーザ、在宅勤務者、および他のモバイル ユーザにエンタープライズ クラスの IP ボイスコールを提供します。Cisco IP Communicator は、Cisco 呼処理プラットフォームで登録および通信するための SCCP と SIP の両方のシグナリング プロトコルをサポートします。Cisco IP Communicator の詳細については、次の Web サイトのデータ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-communicator/index.html

Cisco Jabber デスクトップ クライアント

Cisco Jabber デスクトップ クライアントを使用して、音声、ビデオ、Web コラボレーション、ビジュアル ボイス メールなどのコラボレーション サービスをソフトウェア ベースのデスクトップ アプリケーションに統合できます。Cisco Jabber では、デスクトップ アプリケーションのユーザは、Cisco Unified Communications Manager（Unified CM）、Cisco IM and Presence、Cisco Unity Connection、Cisco WebEx、および Lightweight Directory Access Protocol（LDAP）対応ディレクトリなどのバック エンドのコラボレーション アプリケーション サーバによって提供されるさまざまな通信およびコラボレーション サービスにアクセスできます。Cisco Jabber は、オンプレミスの Cisco IM and Presence または Cisco WebEx Messenger クラウド サービスのいずれかにより提供される IM およびプレゼンス機能を利用できます。

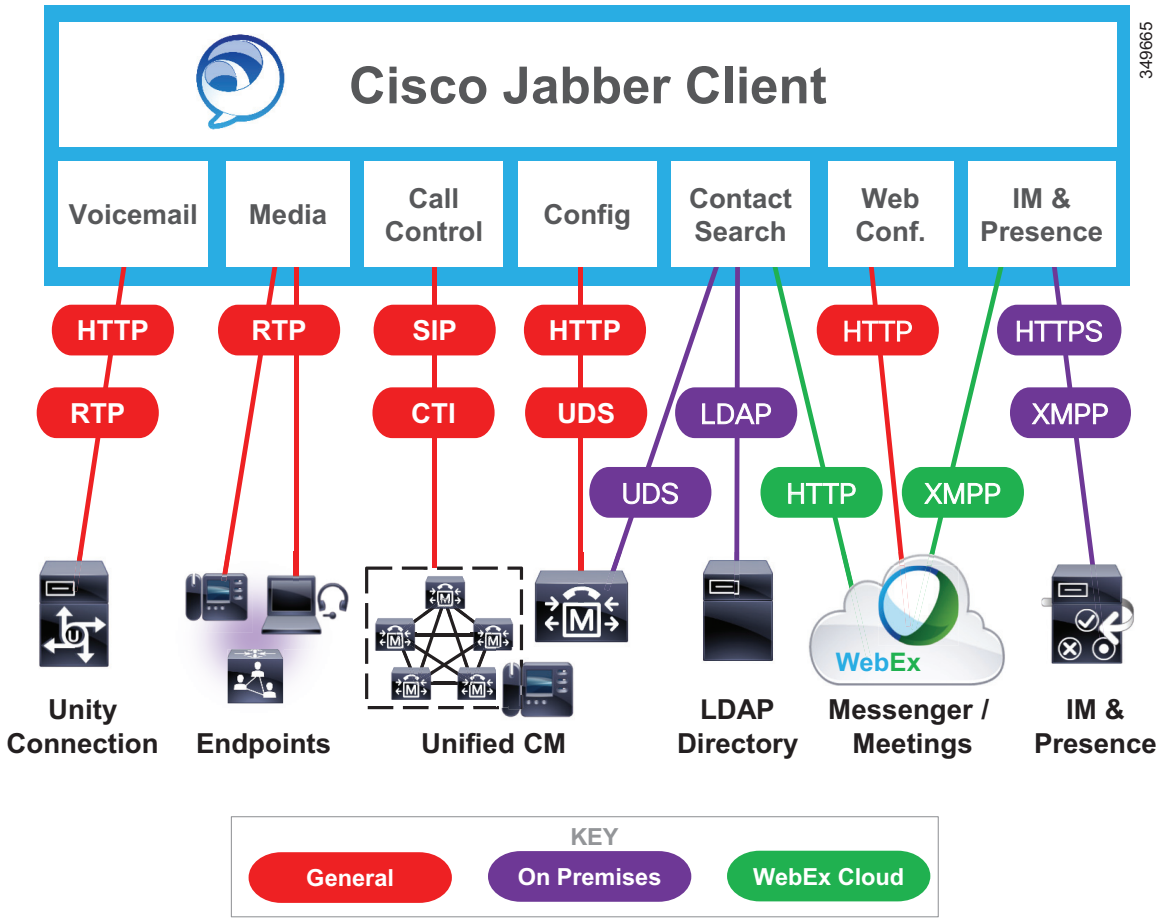
Cisco Jabber デスクトップ クライアントのアーキテクチャ

Cisco Jabber for Windows と Cisco Jabber for Mac は、インスタント メッセージング、プレゼンス、音声、ビデオ、Web コラボレーション、ビジュアル ボイスメールなど、さまざまなシスコ コラボレーション機能を提供するために、共通インターフェイスを使用します。この共通インターフェイスによって、単純化されたクライアント インターフェイスと、次の基本となるコミュニケーション サービスへのアクセスが提供されます。

- Unified CM からの音声およびビデオ ソフトフォン クライアント用 SIP ベースの呼制御
- Unified CM の CTI インターフェイスからのデスクフォンの呼制御と「クリック通話」サービス
- ソフトフォン クライアントの音声およびビデオ メディアの終端
- Cisco IM and Presence サービスまたは Cisco WebEx Messenger サービスのいずれかからの、XMPP を使用したインスタント メッセージングおよびプレゼンス サービス。Cisco WebEx Meeting Center は、オンラインミーティングやイベントなどのホステッド コラボレーション サービスも提供します。
- スケジュールされた音声、ビデオ、および Web 会議サービスの参照
- ビデオ デスクトップ共有（BFCP）または WebEx デスクトップ共有のいずれかを使用したデスクトップ共有
- Internet Message Access Protocol（IMAP）または Representational State Transfer（REST）を使用した Cisco Unity Connection からのビジュアル ボイスメール サービス
- Unified CM User Data Service（UDS ）、Microsoft Active Directory、およびその他のサポートされている LDAP ディレクトリを使用したコンタクトの管理。クラウド ベース統合の場合は WebEx Messenger サービス
- ユーザのアベイラビリティ ステータスおよびメッセージング機能を Microsoft Outlook などの Microsoft Office アプリケーションのユーザ インターフェイスで直接提供する Microsoft Office 統合

通信機能、サービスおよび API（図 8-2 を参照）は、Jabber Desktop Client がプロトコルの管理をこれらのサービスおよび API に対して行い、イベント通知を処理し、ローカル システム リソースのための簡易的な接続ロジックを制御することを可能にします。導入☆のタイプによっては、一部の機能がサポートされない場合があります。

図 8-2　Cisco Jabber デスクトップ クライアントのアーキテクチャ



Jabber Desktop Client：インスタント メッセージングおよびプレゼンス サービス

Jabber クライアントのインスタント メッセージングおよびプレゼンス サービスは XMPP インターフェイスを通じて提供されます。シスコでは、次の製品にインスタント メッセージングおよびプレゼンス サービスを提供します。

- Cisco IM and Presence
- WebEx Messenger サービス

インスタント メッセージングおよびプレゼンス サービスのために Cisco IM and Presence と WebEx Messenger サービスのどちらを選択するかは、多くの要素に依存しています。WebEx Messenger サービスで導入した場合、インターネットからアクセス可能なクラウドベースのサービスを使用します。Cisco IM and Presence をベースとしたオンプレミスで導入した場合、管理者が IM およびプレゼンスのプラットフォームを直接制御でき、SIP/SIMPLE を使用して他のプレゼンス サービスに対するプレゼンス フェデレーションが可能になります。

各 IM およびプレゼンスのプラットフォームでサポートされている機能の詳細については、次のマニュアルを参照してください。

- Cisco IM and Presence

  https://www.cisco.com/c/en/us/products/unified-communications/unified-presence/index.html

- WebEx Messenger サービス

  https://www.cisco.com/c/en/us/products/unified-communications/webex-messenger/index.html

Jabber Desktop Client：呼制御

Cisco Jabber Desktop Client は、2 種類の呼制御モードいずれかで動作します。

- ソフト フォン モード：コンピュータ上で音声とビデオを使用

  Jabber Desktop Client がソフトフォン モードの場合、音声およびビデオ呼制御可能な SIP エンドポイントとして Unified CM に直接登録され、デバイス タイプ Client Services Framework として Unified CM で設定します。

- デスクフォン制御モード：音声（サポートされる場合、ビデオも）に Cisco IP Phone を使用

  Jabber Desktop Client がデスクフォン制御モードの場合、SIP を使用して Unified CM に登録されることはありませんが、Cisco Unified IP Phone を制御しながら CTI/JTAPI を使用してコールの開始、モニタ、終了を行い、ライン ステートをモニタし、コール履歴を提供します。各ユーザに関連付けられたデバイスのリストの取得には、Unified CM の Cisco CallManager Cisco IP Phone（CCMCIP）または UDS サービスが Jabber Desktop Client によって使用されます。デバイスのリストが、デスクフォン モードのクライアントが制御対象の Cisco IP Phone を選択するために使用されます。

ソフトフォン モード

Jabber Desktop Client は、ソフトフォン モードで動作している場合、Unified CM 上の SIP 回線側登録デバイスで、登録の設定、冗長性、リージョン、ロケーション、ダイヤル プラン管理、認証、暗号化、ユーザの関連付けなど、すべての呼制御機能と Cisco Unified IP Phone の機能を使用します。Jabber Desktop Client は、ユーザに対して単一のライン アピアランスをサポートします。

Unified CM クラスタのサイジングの計算では、Jabber Desktop Client の SIP 登録デバイスは、その他のあらゆる SIP 登録エンドポイントと同じく、正規の SIP エンドポイントとして考慮しなければなりません。ソフトフォン モードの Jabber Desktop Client は、Unified CM への登録のデバイス名を検出するために CCMCIP または UDS サービスを使用します。

デスクフォン制御モード

デスクフォン制御モードで動作している場合、Jabber Desktop Client は CTI/JTAPI を使用して、Cisco Unified IP Phone を使用したコールの発信、モニタ、および受信の機能を提供します。このモードでコールが受信または発信されると、音声パスが Cisco Unified IP Phone を通過します。ビデオ コールでは、ビデオ ストリームは Cisco IP Phone（カメラ付きの場合）または承認済みのカメラを使用するコンピュータのいずれかで発信および終了できます。Jabber Desktop Client はユーザの関連付けられているデバイスを検出するために、Unified CM 上の CCMCIP または UDS サービスを使用します。

Jabber Desktop Client のデスクフォン制御モードを使用する場合は、CTI のトラフィックを Unified CM 導入計算に組み入れてください。キャパシティ プランニングの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章参照してください。

Jabber Desktop Client：音声、ビデオ、および Web 会議サービス

スケジュールされた会議サービスへのクライアントのアクセスは HTTP インターフェイス経由で提供できます。シスコの音声、ビデオ、および Web ベースのスケジュール会議サービスは、クラウドベースの WebEx Meeting Center サービスを使用するか、または音声およびビデオ会議サービスと WebEx クラウドベース Web 会議サービスのオンプレミス WebEx Meeting Server の組み合わせを使用して提供されます。WebEx Meeting Center の詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/conferencing/webex-meeting-center/index.html

Jabber Desktop Client：コンタクトの管理

Jabber Desktop Client は、コンタクトの検索および情報に、次のコンタクト ソースのいずれかを使用できます。

- User Data Service（UDS）を介した Cisco Unified CM User データベース
- LDAP directory integration
- WebEx Messenger サービス

コンタクトは、次のいずれかを使用して保存し、ローカルで取得できます。

- Jabber Desktop Client キャッシュ
- Microsoft Outlook などのローカルのアドレス帳とコンタクト リスト

Jabber Desktop Client は、電話取得に加え、逆番号ルックアップを使用して着信電話番号をマッピングします。Jabber Desktop Client のコンタクト管理では、LDAP クエリーに定義する最大 5 個の検索ベースを使用できます。

Cisco Unified CM ユーザ データ サービス（UDS）

UDS は Cisco Unified Communications Manager でのコンタクト検索サービスをクライアントに提供します。Microsoft Active Directory または他の LDAP ディレクトリ ソースから Cisco Unified CM データベースにコンタクト データを同期させることができます。その後、クライアントはコンタクト データを Unified CM から UDS REST インターフェイスを使用して直接取得できます。

ローカルの Unified CM ユーザ データベースから連絡先情報を取得する代わりの手段として、UDS-to-LDAP Proxy 機能を使用することができます。UDS-to-LDAP Proxy では、コンタクト検索は UDS により処理されますが、社内 LDAP ディレクトリにプロキシされ、UDS は結果を Jabber クライアントに戻します。これにより Jabber クライアントは、Unified CM データベースでサポートされている最大ユーザ数を超える社内ディレクトリを検索できます。

LDAP ディレクトリ

次のような多くの異なる要件を満たすように、社内 LDAP ディレクトリを設定できます。

- ユーザ プロビジョニング：ディレクトリ統合を使用して、Cisco Unified Communications Manager データベースに LDAP ディレクトリからユーザを自動的にプロビジョニングできます。Cisco Unified CM は LDAP ディレクトリの内容と同期されるため、LDAP ディレクトリに変更が発生するたびに手動でユーザ情報の追加、削除、変更を行う必要はありません。
- ユーザ認証：LDAP ディレクトリのクレデンシャルを使用してユーザを認証できます。Cisco IM and Presence は、Cisco Unified Communications Manager からすべてのユーザ情報を同期してクライアント ユーザを認証します。
- ユーザ ルックアップ：LDAP ディレクトリの参照を有効にして、シスコのクライアントまたはサードパーティの XMPP クライアントが LDAP ディレクトリで連絡先を検索できるようにします。

WebEx ディレクトリ統合

WebEx ディレクトリ統合を実装するには WebEx 管理ツールを使用します。WebEx は WebEx Messenger サービスに企業ディレクトリ情報のカンマ区切り形式（CSV）ファイルをインポートします。詳細については、次のサイトで入手可能な最新バージョンの『*Cisco WebEx Messenger Administration Guide*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/webex-messenger/products-installation-guides-list.html

Jabber Desktop Client キャッシュ

Jabber Desktop Client は、ローカルのアドレス帳やコンタクト リストだけでなく、前のディレクトリ照会から派生したコンタクト情報およびすでにリストされているコンタクトのローカル キャッシュを保持しています。コールのコンタクトがすでにキャッシュに存在する場合、Jabber Desktop Client はディレクトリを検索しません。コンタクトがキャッシュに存在しない場合、Jabber Desktop Client は、ディレクトリ検索を実行します。

ディレクトリ検索

ローカル Jabber Desktop Client キャッシュでコンタクトが見つからない場合、コンタクトの検索を実行できます。WebEx Messenger のユーザは、コンタクト名が入力されるとともに Outlook のキャッシュ、コンタクト リストとローカル コンタクト リストを照会する予測検索を使用できます。一致が見つからない場合、検索は社内ディレクトリ（WebEx Messenger データベース）への照会を続けます。

Windows 用 Cisco Jabber の詳細については、次の Web サイトのデータ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/jabber-windows/index.html

Mac 用の Cisco Jabber の詳細については、次の URL のデータ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/jabber-mac/index.html

Cisco Spark デスクトップ クライアント

Cisco Spark デスクトップ クライアントにより、1 対 1 のコラボレーションとチーム コラボレーションを促進する永続的なクラウド ベースの仮想チーム スペースが実現します。Cisco Spark デスクトップ クライアントは Windows および Mac コンピュータ上で動作します。Cisco Spark では、デスクトップ アプリケーションのユーザが、1 対 1 またはグループの仮想コラボレーション スペース内で Cisco Collaboration Cloud のコラボレーション サービス（セキュアな暗号化パーシステント メッセージング、IP 経由の音声およびビデオ コール、ファイル共有など）にアクセスできます。クライアントはメッセージングおよびファイル共有では HTTPS を使用して Cisco Collaboration Cloud と通信し、IP 経由の音声およびビデオ メディアでは SRTP を使用します。

Cisco Spark クライアントが適切に動作できるようにするには、デスクトップ コンピュータが有線またはワイヤレス ネットワーク（802.11 WLAN またはモバイル プロバイダー データ ネットワーク）に接続してインターネットにアクセスできる必要があります。

Cisco Spark デスクトップ クライアントの詳細、追加機能の詳細、およびサポートされているハードウェアとソフトウェアのバージョンについては、次の Web サイトで入手可能な Cisco Spark の資料を参照してください。

https://support.ciscospark.com/

Cisco UC Integration™ for Microsoft Lync

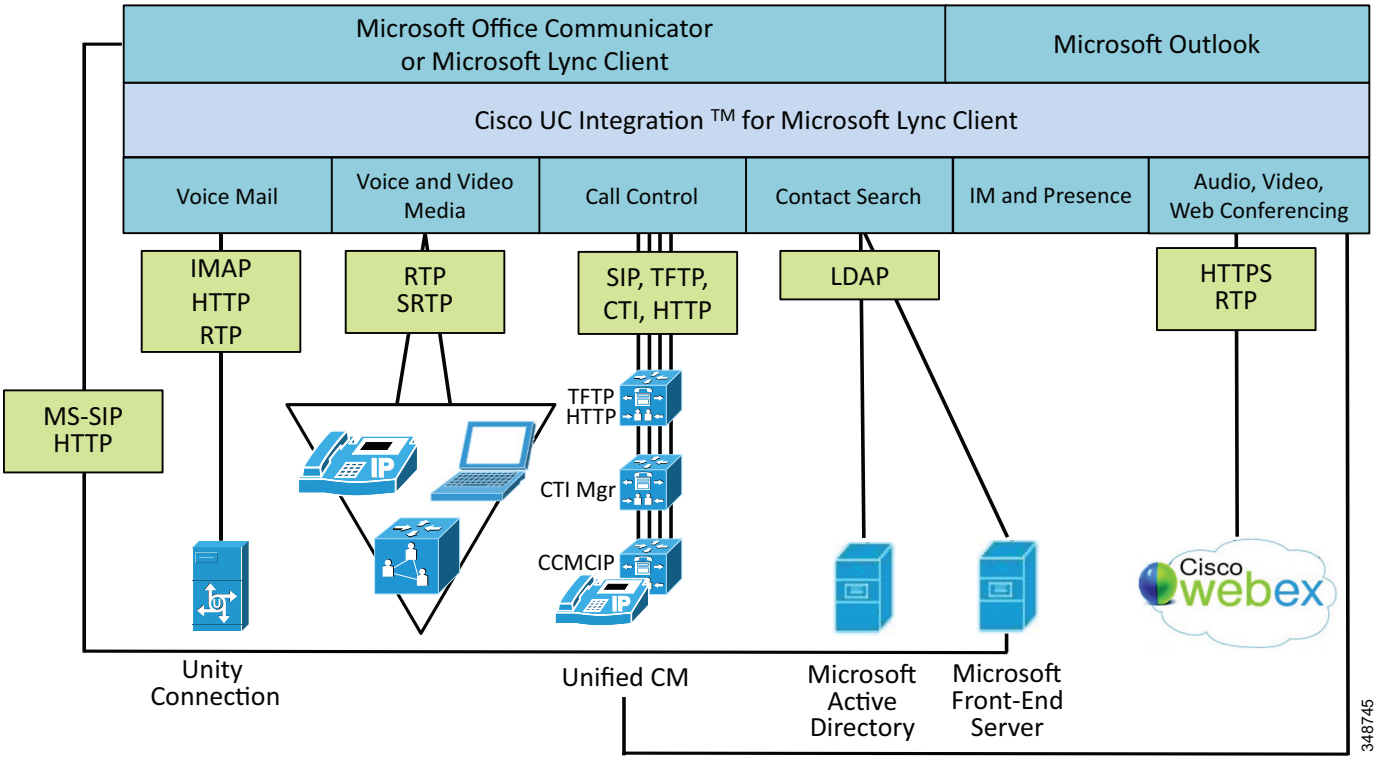
Cisco UC Integration™ for Microsoft Lync クライアントは、さまざまなオンプレミス導入モデルをサポートし、IM およびプレゼンス サービスは Cisco IM and Presence ではなく Microsoft Applications によって提供されます。

Cisco UC Integration™ for Microsoft Lync によって、基盤となる Unified Communications サービスとの統合による Cisco Unified Communications サービスと Microsoft Lync の緊密な統合が可能になります。このソリューションは、一貫したユーザ エクスペリエンスを保ちつつ、標準ベースの音声とビデオ、ユニファイド メッセージング、Web 会議、デスクトップ制御、テレフォニー プレゼンスなどの幅広い一連の Cisco Unified Communications サービスへのアクセスを提供することにより、Microsoft Lync のプレゼンスとインスタント メッセージングの機能を拡張します。

Cisco UC Integration™ for Microsoft Lync アーキテクチャ

Cisco UC Integration™ for Microsoft Lync の導入のソリューション アーキテクチャ（図 8-3 を参照）には、音声およびビデオ サービスのための Cisco Unified Communications Manager、プレゼンスおよびインスタント メッセージング サービスのための Microsoft Office Communications Server 2007、ユーザ アカウント情報のための Microsoft Active Directory、PC 音声またはデスクフォン制御のための Cisco Unified Communications サービス、および Microsoft Lync が含まれます。

図 8-3　Cisco UC Integration™ for Microsoft Lync アーキテクチャ



Cisco UC Integration™ for Microsoft Lync の導入により、クライアントは、クライアントにダウンロードされた Office Communications Server Address Book からのユーザ情報を使用できます。いったんユーザがプレゼンスとインスタント メッセージングについて有効になると、アドレス帳が Office Communications Server から生成され、クライアントに配布されます。ユーザ アカウントの一貫性のために、管理者がユーザのディレクトリ番号情報を E.164 値（例：+18005551212）で入力し、Unified CM での LDAP の同期化と認証を有効にすることをお勧めします。Cisco UC Integration™ for Microsoft Lync が Cisco Unified CM と Microsoft Active Directory の両方に接続され、アカウント クレデンシャルの同期規則を提供します。

（注）　Cisco UC Integration™ for Microsoft Lync では、Cisco Unified Communications サービスではなく、Microsoft のインスタント メッセージングおよびプレゼンス サービスが提供されます。

Cisco UC Integration™ for Microsoft Lync の配置と設定

Cisco UC Integration™ for Microsoft Lync を配置すると、Cisco Unified Communications Manager がコール制御を提供し、Microsoft Lync がインスタント メッセージングおよびプレゼンス機能を提供します。

Cisco UC Integration™ for Microsoft Lync は、そのコンフィギュレーション設定を、管理者が設定する必要がある一連のレジストリ エントリから読み取ります。これらのレジストリ コンフィギュレーション設定は、Microsoft Active Directory からグループ ポリシーを使用してプッシュして、コンフィギュレーション設定をクライアント コンピュータに自動的に配布することを推奨します。グループ ポリシーが推奨されるインストール メカニズムですが、サードパーティ製のソフトウェア配置ツール、バッチ ファイル、Vbscrip、手動での設定など、その他の方法も利用可能です。

Microsoft Active Directory グループ ポリシーは管理テンプレートを使用して拡張でき、Cisco UC Integration™ for Microsoft Lync は管理者がグループ ポリシーをサポートするために追加できるテンプレートを提供します。管理者は、管理テンプレートをロードした後、レジストリ コンフィギュレーション設定（TFTP サーバ、CTI サーバ、CCMCIP サーバ、ボイスメール、LDAP サーバ）のための Cisco UC Integration™ for Microsoft Lync 設定ポリシーを作成できます。

これらのグループ ポリシーがどこでどのように個々の組織単位に適用されるかを制御するために、グループ ポリシー管理コンソールを使用できます。クライアント ポリシーの観点から、Cisco UC Integration™ for Microsoft Lync を配置する際には、Microsoft Telephony Mode Policy を [IM and Presence Only] および [DisableAVConferencing] に設定することを推奨します。このクライアント ポリシー変更により、Microsoft Lync のユーザ エクスペリエンスで単一セットのコール オプションだけを表示できるようになります。

Cisco UC Integration™ for Microsoft Lync 配置では、インストールされる cisco-presence-states-config.xml ファイルでカスタム プレゼンス状態の定義と展開を行うことも可能です。ただし、次のレジストリの場所に基づいて Microsoft Lync がこのカスタム プレゼンス状態ファイルを使用できるように、管理者がこのファイルを Microsoft Office Communications Server などの HTTP ロケーションに置き直すことを推奨します。

HKLM\Software\Policies\Microsoft\Communicator\CustomStateURL

ソフトウェア ベースのエンドポイントの配置に関する一般的な考慮事項

次の項では、ソフトウェアベースのエンドポイントを配置するための重要な設計上の考慮事項について説明します。

Quality of Service

シスコのソフトウェアベースのクライアント アプリケーションは、QoS マーキングのベスト プラクティスに従ってレイヤ 3 のトラフィックをマーキングしますが、アプリケーションがトラフィックを適切にマーキングしても、基盤となるオペレーティング システムまたはハードウェアがマーキングを受け入れないことがあります。デスクトップ コンピュータから着信するトラフィック マーキングの一般的な予測不可能性および不信頼性を考慮すると、一般的に、これらのトラフィック マーキングは、信頼する必要があります。これは、すべてのトラフィック フローがプロトコルまたはポート番号に基づくネットワークによってマークされる必要があり、リアルタイム トラフィック フローがベスト プラクティスに基づいてマークされることを意味します。これには、DSC 46 または PHB EF の音声のみのコールのメディア マーキング、DSCP 34 または PHB AF41 のビデオ コールのメディア（音声を含む）、および DSCP 24 または PHB CS3 のコール シグナリングが含まれます。正しく設定されたネットワーク インフラストラクチャとともにこれらのマーキングは、音声のみのコールのメディアの優先処理およびビデオコールのメディアとコールシグナリングの専用帯域幅を保証します。ソフトウェア ベースのエンドポイント トラフィックの再マーキングに加えて、ネットワーク ベースのポリシングとレート制限を使用してソフトウェア ベースのエンドポイントが大量のネットワーク帯域幅を消費しないようにすることを推奨します。これは、デスクトップ コンピュータが大量のデータ トラフィックを生成する場合、またはエンドポイント アプリケーションが不正な動作をして一般的なコールに対して予測を超える音声、またはビデオ メディアとシグナリングのトラフィックを生成する場合に発生する可能性があります。完全にデスクトップ コンピュータのネットワーク トラフィック マーキングを制御するためにサードパーティ製ソフトウェアが使用されている場合、管理者はデスクトップ コンピュータのマーキングを信頼することを決定でき、その場合はパケットの再マーキングが不要であることがあります。ネットワーク ベースのポリシングおよびレート制限は、動作の不正なエンドポイントの場合はネットワーク全体を保護するために依然として推奨されます。

ソフトウェア ベースの Cisco IP Communicator および Cisco Jabber for Windows の場合、Microsoft Windows グループ ポリシーを使用して、音声およびビデオ メディア ソース ポート番号に基づき、該当するレイヤ 3 DSCP QoS マーキングを音声およびビデオ ストリームに適用できます。

Microsoft Windows グループ ポリシーを使用した Cisco Jabber for Windows QoS の詳細については、次の URL で入手可能な最新バージョンの『*On-Premises Deployment for Cisco Jabber*』で Quality of Service 設定に関する情報を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

VLAN 間ルーティング

ソフトウェア ベースのエンドポイントは、通常はデータ VLAN に配置されるデスクトップ コンピュータで実行されるため、音声 VLAN とデータ VLAN が分離されたネットワークにソフトウェア ベースのエンドポイントが配置されると、VLAN 間ルーティングを設定および許可して、データ VLAN のこれらのエンドポイントからの音声トラフィックが音声 VLAN のエンドポイントに到達できるようにする必要があります。

SRST と拡張 SRST

低速と信頼性の低い WAN リンクで集中型呼処理プラットフォームから分離された支社ロケーションにシスコのソフトウェア ベースのエンドポイントのデスクトップ アプリケーションを配置する場合は、ローカル呼処理の冗長性を考慮することが重要です。各支社ロケーションの Cisco IOS ルータ上で SRST または拡張 SRST を使用することで、集中型呼処理プラットフォームへの接続が失われた場合でもソフトウェア ベースのエンドポイントの基本的な IP テレフォニー サービスは維持できます。ただし、使用可能なユーザ機能セットは、アプリケーションが Unified CM に登録されている場合に比べ、デスクトップ ソフトウェア ベースのエンドポイントが SRST に登録されている場合は少なくなります。

リモート エンタープライズ接続の保護

シスコのソフトウェアベースのエンドポイントは、VPN または VPN-less ソリューションを使用してリモート ロケーションから企業ネットワークに安全に接続できます。

VPN ベース接続の場合、エンタープライズ エッジに Cisco Adaptive Security Appliance（ASA）または他の VPN ヘッドエンド コンセントレータへの安全な VPN トンネルを作成する VPN ルータの後ろにソフトウェアベースのエンドポイントを配置することができます。このセキュア リモート接続は、音声およびビデオ メディアおよびシグナリング トラフィックだけでなく、パーソナル コンピュータから着信するトラフィックすべてのトラフィックも保護します。その結果、コンピュータからのすべてのトラフィックは、そのトラフィックの宛先が最終的にインターネットである場合でも、企業のネットワークのエッジを通過します。

また、Cisco Jabber デスクトップ クライアントは Cisco Expressway ソリューションのモバイル デバイスとリモート アクセス機能を利用できます。このファイアウォール トラバーサル ソリューションは、音声およびビデオ コールに対する Unified CM 呼制御の登録や、企業のコラボレーション アプリケーションおよびサービスへのアクセス（IM and Presence、ボイス メール、ディレクトリ アクセスなど）で、Cisco Expressway E および Expressway C サーバによって提供される、企業への TLS リバース プロキシ接続を使用します。Cisco Expressway ソリューションのモバイルおよびリモート アクセス機能の詳細については、次の Web サイトのソリューション情報および製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html

ダイヤル プラン

ソフトウェアベースのエンドポイントを配置する際には、ダイヤル プランと番号の正規化に関する考慮事項を念頭に置いて作業してください。Jabber Desktop Client は通常、コンタクトの検索、解決、および追加にディレクトリを使用します。これらのコンタクトに関連付けられている番号は、クライアントが認識し、解決し、ダイヤルできる形式になっていなければなりません。

配置は、ディレクトリおよび Unified CM の設定によって変わってくる場合があります。ビジネス、モバイル、および自宅の電話番号用に E.164 の番号指定（例：+18005551212）がディレクトリに含まれており、Unified CM にも E.164 ダイヤル プランが含まれている場合は、すべてのルックアップ、解決、およびダイヤルされたイベントが E.164 形式のダイヤル ストリングになるため、追加のダイヤル規則の必要性が最小限に抑えられます。

Unified CM 配置環境でプライベート ダイヤル プラン（5551212 など）を実装している場合は、Unified CM 上で E.164 番号をプライベート ディレクトリ番号に変換する必要が生じます。発信は、Unified CM のトランスレーション パターンによって変換することができます。これにより、ダイヤルされた番号（+18005551212 など）をプライベート番号（この例では 5551212）でエンドポイントに表示させることができます。着信コールは、ディレクトリのルックアップ規則によって変換できます。これにより、着信した番号の 5551212 が、逆番号ルックアップ発信者 ID に +18005551212 で示されます。

企業で使用されるダイヤルプランおよび LDAP ディレクトリに格納された電話番号情報において、番号形式の相違に対応するため Cisco Unified Communications Manager にトランスレーション パターンとディレクトリ ルックアップ規則を設定する必要がある場合、独自のダイヤル プランの導入が発生する可能性があります。ディレクトリ ルックアップ規則は、ディレクトリ ルックアップ キーとして使用される着信コール ID を再フォーマットする方法を定義します。トランスレーション パターンは、発信ダイヤル用に LDAP ディレクトリから取得した電話番号を変換する方法を定義します。

トランスレーション パターンは、コールがルーティングされる前にダイヤルされた数字を操作するために、Unified CM によって使用されます。これらは、Unified CM によって厳密に処理されます。トランスレーション パターンは、着信番号の処理に推奨される方法です。トランスレーション パターンの使用方法およびダイヤル プラン管理に関するその他のガイドラインについては、ダイヤル プラン（14-1 ページ）の章を参照してください。

トランスレーション パターンの代用として、アプリケーション ダイヤリング規則を使用して、ダイヤルされた番号を処理できます。アプリケーション ダイヤリング規則を適用すると、ユーザがダイヤルする電話番号に対して数字の追加と削除を自動的に実行できます。アプリケーション ダイヤリング規則は、Unified CM 上で設定され、Unified CM からクライアントにダウンロードされます。トランスレーション パターンは、着信番号の処理に推奨される方法です。

ディレクトリ検索ルールは、発信者の識別情報をディレクトリで検索可能な番号に変換します。定義する各ディレクトリ ルックアップ規則には、先頭の数字および番号の長さに基づいてどの数字を変換するかを指定します。ディレクトリ ルックアップ規則は、Unified CM 上で設定され、Unified CM からクライアントにダウンロードされます。

コンタクト情報を通じてコールが発信される前に、クライアント アプリケーションがダイヤルされる電話番号から文字と数字以外のすべてのものを取り除きます。アプリケーションは、文字を数字に変換し、ダイヤリング規則を適用します。文字と数字のマッピングは、ロケール固有で、その場所の標準的な電話機のキーパッドにある文字に対応します。たとえば、US English ロケールでは、1-800-4UCSRND は 18004827763 に変換されます。コールがアプリケーションによって発信される前に、ユーザがクライアントの変換された番号を見たり変更したりすることはできません。

コンタクト ソース

Cisco Jabber for Windows と Cisco Jabber for Mac は、デフォルトで Cisco ディレクトリ統合（CDI）を使用します。CDI ではサービス検出を使用して、Microsoft Active Directory を含む LDAP v3 対応のディレクトリに自動的に接続し、認証を行います。

カスタム属性のマッピングを必要とする LDAP ディレクトリとの統合では、これらの属性マッピングは Unified CM サーバからクライアントにダウンロードできるコンフィギュレーション ファイルで作成できます。

Cisco Jabber デスクトップ クライアントでは、Unified CM User Data Service（UDS）もサポートされています。これにより、クライアントが Unified CM ユーザ データベース（LDAP ディレクトリと同期している場合もある）を使用してコンタクト情報を検索できます。企業のファイアウォールの外部にあり Expressway モバイル & リモート アクセスを使用して接続している Jabber デスクトップ クライアントは、コンタクトの解決に UDS を自動的に使用します。

また、Jabber for Windows は Microsoft Outlook のローカル連絡先をサポートしており、ユーザは自分の Microsoft Outlook クライアントにある連絡先を検索できます。

Extend and Connect

Cisco Jabber デスクトップ クライアントは Extend and Connect をサポートしており、サードパーティの電話機を使用して Jabber からコールを発信および受信することができます。これによって、Cisco Collaboration 機能を活用しながら、既存のサードパーティの PBX 電話機を使用することができます。Extend and Connect には複数のモードがあり、モードごとに別のトランクを使用する必要があります。Extend and Connect を使用する場合、ダイヤル プランを慎重に設計する必要があります。ダイヤル プランの設計の詳細については、ダイヤル プラン（14-1 ページ）の章を参照してください。Jabber クライアントが企業ネットワークの外部にあり Expressway モバイル & リモート アクセスを使用して接続している場合、Extend and Connect はサポートされません。

リフレッシュ トークンを使用した OAuth でのログイン フロー

Cisco Jabber 11.9 以降、OAuth 2.0 承認フレームワークを使用して、クライアント承認と認証を容易に行えるようになっています。これにより、ログインが迅速化されるとともに、起動時やネットワーク遷移時の再認証も迅速化されます。Cisco Unified CM 12.0 および Unified CM 11.5(1) SU3 の前までは、導入環境内でシングル サインオン（SSO）が有効にされている場合、Cisco Jabber は OAuth のみを使用していました。OAuth 実装は、認証を行い承認トークンをクライアントに発行する承認サーバとしての役割を果たす Unified CM パブリッシャに依存します。このトークンとリフレッシュ トークンにより、クライアントがコラボレーション サービスに要求を行い承認を取得することが可能になります。また、リフレッシュ トークンを使用して、期限切れの承認トークンを素早く更新できます。OAuth 2.0 フレームワークの詳細については、承認フレームワーク（16-46 ページ）の項を参照してください。

OAuth を Jabber クライアントの承認と認証に使用するには、Cisco Unified CM、Unified CM IM and Presence、Unity Connection で、**OAuth with Refresh Login Flow** サービス パラメータを有効にする必要があります。同様に、Jabber クライアントが Expressway モバイルおよびリモート アクセスで OAuth を使用するには、**Authorize by OAuth token with refresh** 設定を Expressway-C で有効にする必要があります。

Cisco Jabber での OAuth 展開の詳細については、次の URL で入手可能な最新バージョンのホワイト ペーパー『*Deploying OAuth with Cisco Collaboration Solution Release 12.0*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

ワイヤレスエンドポイント

Cisco ワイヤレス エンドポイントは、ネットワーク接続のため、また IP テレフォニー機能を提供するために 802.11 Wireless LAN（WLAN）インフラストラクチャに依存しています。このタイプのエンドポイントは、単一の企業ロケーション内や複数の企業ロケーション間、または従来の有線電話機では望ましくない、または問題のある環境間で移動するモバイル ユーザに理想的です。シスコでは、Voice and Video over WLAN（VVoWLAN）IP Phone を介した次の音声およびビデオを提供します。

- Cisco Unified Wireless IP Phone 8821、7925G、7925G-EX、および 7926G を含む Cisco Unified Wireless IP Phone
- Cisco IP Phone 8861 および 8865
- Cisco DX シリーズ

すべてが、組み込み型の無線アンテナを備えた、ハードウェアベースの電話機です。Cisco Unified Wireless IP Phone 7925G、7925G-EX、および 7926G では、ネットワークへの 802.11b、802.11g、または 802.11a 接続が可能です。Cisco Unified Wireless IP Phone 8821、Cisco IP Phone 8861 および 8865 では、802.11a、802.11b、802.11g、802.11n、および 802.11ac ワイヤレス接続が可能であり、Cisco DX シリーズ エンドポイントでは 802.11a、802.11b、802.11g、および 802.11n ワイヤレス接続が可能です。Cisco Unified Wireless IP Phone 7925G、7925G-EX、および 7926G は、SCCP シグナリング プロトコルを使用して、シスコの呼処理プラットフォームで登録および通信します。Cisco Unified Wireless IP Phone 8821、Cisco IP Phone 8861 と 8865、および DX シリーズ エンドポイントは、SIP シグナリング プロトコルを使用して、シスコの呼処理プラットフォームで登録および通信します。

Cisco Unified Wireless IP Phone の詳細については、次の Web サイトで入手可能なデータ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-7900-series/index.html

Cisco IP Phone 8800 シリーズの詳細については、次の Web サイトのデータ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/index.html

Cisco DX シリーズ エンドポイントの詳細については、次の Web サイトのデータ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/desktop-collaboration-experience-dx600-series/index.html

ワイヤレス エンドポイントの配置に関する一般的な考慮事項

次の項では、ワイヤレス エンドポイントを配置する場合に重要な設計上の考慮事項について説明します。

ネットワークの無線周波数の設計とサイト サーベイ

ワイヤレス エンドポイントを配置する前に、WLAN 無線周波数（RF）の設計によって同じチャネルの干渉を最小限に抑えるようにすると同時に、十分な無線信号レベルを維持しながら、デバイスをあるロケーションから別のロケーションに移動しても許容可能な音声およびビデオ画質が維持されるように、十分な無線信号レベルおよび非隣接チャネルのオーバーラップを提供する必要があります。また、WLAN サイト全体のサーベイを実行することで、ネットワーク RF 設計を検証して、適切なデータ レートとセキュリティ メカニズムが整っているようにする必要があります。サイト調査では、最適なカバレッジを提供するアンテナ タイプや RF 干渉の送信元が存在している可能性がある場所を考慮する必要があります。サードパーティのサイト サーベイ ツールを使用している場合でも、各エンドポイントまたはクライアント無線の動作がアンテナの感度およびサーベイ アプリケーションの制限によって動作が異なるため、無線エンドポイント デバイス自体を使用してサイト サーベイの実施を強く推奨します。シスコでは、音声およびビデオ トラフィックを生成することができるワイヤレス エンドポイント接続するために、可能であれば、5 GHz WLAN 帯域（802.11a/n）の利用を推奨します。5 GHz WLAN は、音声コールとビデオ コールに対し、スループットを改善して干渉を低減します。無線ネットワークの設計の詳細については、ワイヤレス LAN インフラストラクチャ（3-66 ページ）を参照してください。

セキュリティ：認証および暗号化

ワイヤレス エンドポイントを配置する場合、ネットワークへのアクセスの制御およびネットワーク トラフィックの保護のために使用されるセキュリティ メカニズム考慮することが重要です。Cisco ワイヤレス エンドポイントは、WPA、WPA2、EAP-FAST、PEAP などを含む広範囲の認証および暗号化プロトコルをサポートします。WLAN インフラストラクチャ、配置されるエンドポイント デバイス、および IT セキュリティ ポリシーと一致しているものによって、サポートされる認証および暗号化方式を選択します。さらに、デバイスがネットワーク内のあるロケーションから別のロケーションに移動しているときにアクティブな音声およびビデオ コールが保持できるように、選択した認証および暗号化方式が Cisco Centralized Key Management（CCKM）などの高速キー再生成方式をサポートする必要があります。

（注）　二重帯域 WLAN（2.4 GHz と 5 GHz の両方の帯域を持つ WLAN）では、同じ SSID の 802.11b/g と 802.11a との間でのローミングは、クライアントが両方のボードをサポートできれば可能です。ただし、一部のデバイスでは、これにより、音声またはビデオ経路にギャップが発生する可能性があります。これらのギャップを回避するために、音声およびビデオ通信用に帯域を 1 つだけ使用します。

ワイヤレス コールのキャパシティ

企業 WLAN 内にワイヤレス デバイスを配置し、ワイヤレス デバイス ローミングを有効にする場合、WLAN インフラストラクチャのデバイスの接続性とコール キャパシティを考慮することも重要です。デバイス数またはアクティブ コール数の面での WLAN インフラストラクチャのオーバーサブスクリプションは、無線接続のドロップ、音声とビデオの品質の低下、またはコール セットアップの遅延や失敗の原因となります。Voice and Video over WLAN の配置をオーバーサブスクライブする可能性は、必要なコール キャパシティを処理するように WLAN アクセス ポイント（AP）の十分な数の配置によって著しく最小限に抑えられます。AP のコール キャパシティは、単一チャネル セル領域内でサポートできる同時双方向ストリーム数に基づきます。VVoWLAN のコール キャパシティの一般的なルールは次のとおりです。

- Bluetooth が無効で 802.11g/n（2.4 GHz）チャネル セルあたり最大 27 の同時 VoWLAN 双方向ストリーム、または 24 Mbps 以上のデータ レートが有効で 802.11a/n/ac（5 GHz）チャネルあたり最大 27 の同時 VoWLAN 双方向ストリーム。
- Bluetooth が無効で 802.11 g/n（2.4 GHz）チャネル セルあたり最大 8 の同時 VVoWLAN 双方向ストリーム、または 720p のビデオ解像度（高解像度）および最大 1 Mbps のビデオ ビットレートとした場合の 802.11 a/n/ac（5 GHz）チャネル セルあたり最大 8 の同時 VVoWLAN 双方向ストリーム。

これらのコール キャパシティ値は、RF 環境、無線ハンドセット機能、および基礎となる WLAN システム機能に大きく依存します。一部の配置では、実際のキャパシティはこれよりも小さくなることもあります。

（注）　同じ AP に関連付けられている 2 台のワイヤレス エンドポイント間の単一のコールは、2 つの同時双方向ストリームであると見なされます。

上記のキャパシティは、音声アクティビティ検出（VAD）が無効で、パケット化のサンプル サイズが 20 ミリ秒（ms）であることに基づいています。VAD とは、コール中に音声が発生しないときに RTP パケットを送信しないことにより、帯域幅を節約するメカニズムです。ただし、無音圧縮とも呼ばれる VAD を有効または無効にすることは、シスコの呼制御プラットフォームに応じてグローバル設定になることがあります。そのため、VAD が無線で接続された Cisco Unified IP Phone で有効にされると、VAD は配置内のすべてのデバイスで有効にされていることがあります。全体の音声品質を良好に保つため、VAD（無音圧縮）を disabled のままにすることを推奨します。

サンプリング レートを 20 ms に設定すると、片方向の音声コールで 50 パケット/秒（pps）が生成されます。ほどんどすべての場合、サンプル レートを 20 ms に設定するように推奨します。それより大きいサンプル サイズ（30 または 40 ms）を使用すると、AP あたりの同時コールの数を増分できますが、エンドツーエンドの遅延も大きくなります。また、サンプル サイズを大きくすると、1 つのパケットが失われたときに欠落する会話の量が大きくなるため、ワイヤレス環境で許容される音声パケットの損失率は大幅に減少します。音声サンプリング サイズの詳細については、帯域幅のプロビジョニング（3-56 ページ）を参照してください。

Bluetooth のサポート

Cisco Unified Wireless IP Phone 8821、7925G、7925G-EX、および 7926G、Cisco IP Phone 8861 と 8865、および Cisco DX シリーズ エンドポイントは、Bluetooth 対応デバイスです。ワイヤレス Cisco IP Phone 内の Bluetooth 無線またはモジュールにより、Bluetooth ヘッドセットのサポートが有効になります。また、前述したように Cisco IP Phone 8845、8851、8861、8865、および DX シリーズ エンドポイントでは、ハンズフリー音声および携帯電話のコンタクトと通話履歴の共有のために、Intelligent Proximity for Mobile Voice と Bluetooth のペアリングがサポートされます。Bluetooth デバイスは、802.11b/g デバイスと同じ 2.4 GHz 無線帯域を使用するので、Bluetooth および 802.11b/g 対応デバイスが相互に干渉し、その結果、接続に関する問題が起きる可能性があります。

Bluetooth と 802.11 WLAN 無線が Cisco Unified Wireless IP Phone、Cisco IP Phone 8861、8865、および Cisco DX シリーズ エンドポイントでネイティブに共存し、Bluetooth と 802.11b/g 無線との間の無線干渉が大幅に減少して回避される一方で、これらの無線で接続された電話機の Bluetooth 無線は近くに配置されている他の 802.11 b/g デバイスおよび Bluetooth 無線デバイスと干渉を起こすことがあります。802.11b/g WLAN 音声およびビデオ デバイスの干渉と中断が発生する可能性があるため（これが原因で音質および画質の低下、登録解除、コール セットアップの遅延が発生する可能性があるため）、すべての WLAN 音声およびビデオ デバイスを、5 GHz 無線帯域を使用する 802.11a、802.11n、または 802.11ac に配置することを推奨します。ワイヤレス電話機を 5 GHz 無線帯域に配置することで、Bluetooth デバイスによって引き起こされる干渉を回避できます。

802.11 WLAN デバイスを 5 GHz 無線帯域に配置する必要があり、2.4 GHz 無線帯域の緩衝が原因で接続、機能、または音声とビデオの品質に関する問題が発生する場合は、Bluetooth ヘッドセットや Bluetooth に依存する機能（Intelligent Proximity for Mobile Voice など）をこの配置で使用することを制限または禁止することを検討してください。

Cisco 8851、8861、および DX シリーズ エンドポイントの Intelligent Proximity for Mobile Voice と Bluetooth のペアリングの詳細については、インテリジェント プロキシミティ（8-15 ページ）を参照してください。

（注）　バッテリ駆動式 Cisco Unified Wireless IP Phone で Bluetooth ワイヤレス ヘッドセットを使用すると、電話機のバッテリ電力消費が増加し、バッテリ寿命が短くなります。

（注）　Bluetooth ヘッドセットと Bluetooth 機能（Intelligent Proximity for Mobile Voice など）を使用すると、干渉が発生し、2.4 GHz 帯域（802.11b/g/n）を使用する隣接ワイヤレス クライアントおよびエンドポイントでサービスの中断が発生する可能性があります。

Quality of Service

ネットワーク レベルの Quality of Service（QoS）を設定する場合、シスコのワイヤレス エンドポイント（Cisco Unified Wireless IP Phone、Cisco IP Phone 8861、および Cisco DX シリーズ エンドポイントなど）は信頼でき、それらのパケット マーキングは受け入れられます。これらのエンドポイントはデフォルトで、音声/ビデオ メディアとコール シグナリングに対して推奨されている適切なレイヤ 3 値（音声メディアは DSCP 46 または PHB EF、音声/ビデオ メディアはビデオ コールに対して DSCP 34 または PHB AF41、音声シグナリングは DSCP 24 または PHB CS3）でマーキングを行います。同様に、これらのデバイスは、レイヤ 2 で適切にマークします（6 の音声メディア WMM User Priority（UP）、5 のビデオ コール WMM UP に対する音声およびビデオ メディア、4 のコール シグナリング WMM UP）。これらのパケット マーキングによって、統合されたネットワークでエンドツーエンドの音声品質が許容可能です。

レイヤ 2 およびレイヤ 3 の両方の適切なパケット マーキングにもかかわらず、Cisco DX80 などの多目的デバイスは、大量の非リアルタイム トラフィックを生成できます。したがって、同じ WLAN SSID または VLAN でのこれらのデバイスの混在に関連する懸念があげられることがあります。レイヤ 2 QoS マーキングと 802.11e WMM は、リアルタイム トラフィックに対してワイヤレス媒体へのより多くの帯域幅とより高い頻度のアクセスが確保されるように作用しますが、緻密で、頻繁に使用されている配置では、DX シリーズ エンドポイントなどの多目的デバイスを別個の SSID に分離することで、何らかの対策になる場合があります。ただし、これらのデバイスによって生成されるリアルタイム トラフィックがワイヤレス インフラストラクチャでまだ所定のプライオリティ処理を与えられるようにするには、多目的デバイスのこの別個の SSID が Platinum QoS プロファイルに引き続き設定される必要があります。

SRST と拡張 SRST

低速または信頼性の低い WAN リンクで集中型呼処理プラットフォームから分離された支社ロケーションにワイヤレス エンドポイントを配置する場合は、ローカル呼処理の冗長性を考慮することが重要です。各支社ロケーションの Cisco IOS ルータ上で SRST または拡張 SRST を配置することで、集中型呼処理プラットフォームへの接続が失われた場合でもワイヤレス エンドポイントの基本的な IP テレフォニー サービスは維持できます。ただし、使用可能なユーザ方向セットは、ワイヤレス エンドポイントが Unified CM に登録されている場合に比べ、SRST に登録されている場合は少なくなります。

デバイスのモビリティ

ワイヤレス エンドポイントがマルチ サイト集中型呼処理配置のロケーション間で移動する場合、デバイスが Unified CM に登録するために使用する IP アドレスに基づいてデバイスのロケーションを更新するために Cisco Unified CM デバイス モビリティ機能を使用できます。これにより、デバイスがロケーション間で移動するときのコール ルーティング、PSTN の出力、および通常遭遇するコーデックおよびメディア リソースの選択に関する問題を回避できます。デバイス モビリティに関する詳細については、デバイス モビリティ（21-15 ページ）の項を参照してください。

Cisco Unified Wireless IP Phone 7925G などの無線 IP エンドポイントの展開の詳細については、次の Web サイトの展開ガイドを参照してください。

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-implementation-design-guides-list.html

ワイヤレス Cisco 8800 シリーズ エンドポイントの展開の詳細については、次の Web サイトの展開ガイドを参照してください。

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

Cisco DX シリーズ エンドポイントのワイヤレスでの展開の詳細については、次の Web サイトの展開ガイドを参照してください。

https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-implementation-design-guides-list.html

モバイル エンドポイント

シスコのモバイル エンドポイント デバイスとモバイル エンドポイント クライアント アプリケーションは、音声およびビデオ通話サービス用の Unified CM で登録および通信します。これらのデバイスおよびクライアントは、Cisco Unity Connection、Cisco IM and Presence、および LDAP ディレクトリなどの他のバック エンド システムと通信することによって、エンタープライズ メッセージング、プレゼンス、社内ディレクトリ統合などの追加機能およびサービスを有効にします。シスコは、次のモバイル エンドポイント デバイスおよびクライアントを提供します。

- Cisco Jabber for Android および Apple iOS（8-40 ページ）
- Cisco Spark モバイル クライアント（8-41 ページ）
- Cisco WebEx Meetings（8-41 ページ）（Android、BlackBerry および Apple iOS デバイス用）
- Cisco AnyConnect セキュア モビリティ クライアント（8-41 ページ）（Android、および Apple iOS デバイス用）

Cisco Jabber for Android および Apple iOS

iPhone と iPad を含む Android および Apple iOS デバイスの Cisco Jabber モバイル クライアントによって、スマート フォンとタブレットは IP 経由で音声およびビデオを使用してエンタープライズ コールを発信または受信できます。Android または Apple iOS デバイスで実行される Cisco Jabber モバイル クライアントアプリケーションは、SIP シグナリング プロトコルを使用して Unified CM に登録および通信します。Cisco Jabber モバイル クライアントは、社内ディレクトリ アクセス、エンタープライズ ビジュアル ボイス メール、XMPP ベースのエンタープライズ インスタント メッセージングとプレゼンス、および Cisco Expressway モバイル & リモート アクセスを使用したリモート接続の保護などの追加機能を有効にします。

Cisco Jabber for Android の詳細については、次の Web サイトのデータ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/jabber-android/index.html

Cisco Jabber for iPhone and iPad の詳細については、次の Web サイトのデータ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/jabber-iphone-ipad/index.html

Cisco Spark モバイル クライアント

Cisco Spark モバイル クライアントにより、1 対 1 のコラボレーションとチーム コラボレーションを促進する永続的なクラウド ベースの仮想チーム スペースが実現します。Cisco Spark では、モバイル アプリケーション ユーザが Cisco Collaboration Cloud のコラボレーション サービスにアクセスできます。Cisco Spark for Android クライアントおよび Cisco Spark for iPad and iPhone クライアントにより、1 対 1 またはグループ コラボレーション スペース内でセキュアな暗号化パーシステント メッセージング、IP 経由の音声およびビデオ、およびファイル共有がすべて提供されます。これらのクライアントは Cisco Collaboration Cloud と通信するときに、メッセージングおよびファイル共有では HTTPS を使用し、IP メディア トラフィックでの音声およびビデオでは SRTP を使用します。

Cisco Spark クライアントが適切に動作するには、モバイル クライアント デバイスが 802.11 WLAN またはモバイル プロバイダー データ ネットワークへの接続によってインターネットにアクセスできる必要があります。

Cisco Spark モバイル クライアントの詳細、追加機能の詳細、およびサポートされているハードウェアとソフトウェアのバージョンについては、次の Web サイトで入手可能な Cisco Spark の資料を参照してください。

https://support.ciscospark.com/

Cisco WebEx Meetings

Cisco WebEx Meetings モバイル クライアントは、特定の Android、Apple iOS、BlackBerry、および Windows Phone のモバイル スマート フォンやタブレットで稼働します。このクライアントによって、モバイル エンドポイントはデスクトップ ブラウザ ベースの Cisco WebEx 会議と同様に、同様の機能を持つ Cisco WebEx 会議に参加できます。このクライアントによって、Cisco WebEx 音声およびビデオ会議へのアクティブな参加（参加者リストや共有コンテンツを表示する機能を含む）が可能になります。

Cisco WebEx モバイル クライアントに関する詳細情報については、次の URL にある製品情報を参照してください。

https://www.cisco.com/c/en/us/products/conferencing/webex-meetings/index.html

Cisco AnyConnect セキュア モビリティ クライアント

Cisco AnyConnect Secure Mobility Client によって、Cisco Jabber モバイル デバイス クライアントに対する安全なリモート接続が有効になり、モバイル データ ネットワークと非企業 WLAN 経由の永続的企業アクセスを行えるようになります。このクライアント アプリケーションは、Cisco Adaptive Security Appliance（ASA）ヘッドエンドで利用可能な Cisco AnyConnect VPN ソリューションを使用して、Apple iOS および Android モバイル デバイスに SSL VPN 接続を提供します。

Cisco AnyConnect を使用したセキュアなリモート VPN 接続の詳細については、次の Web サイトで入手可能な Cisco AnyConnect Secure Mobility Client マニュアルを参照してください。

https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html

モバイル エンドポイントとクライアントの配置に関する考慮事項

次の項では、モバイル エンドポイントとクライアントを配置するための重要な設計上の考慮事項について説明します。

WLAN 設計

Cisco Jabber モバイル クライアントは WLAN に接続される場合が多いため、前述のすべての WLAN 配置に関する考慮次回は、サイト調査による WLAN RF 設計および検証など、モバイル クライアントとデバイスに適用されます。特に、音声およびビデオ トラフィックを生成することができるワイヤレス エンドポイントを接続するために、可能であれば、5 GHz WLAN 帯域（802.11a/n/ac）の利用が推奨されます。5 GHz WLAN は、音声コールとビデオ コールに対し、スループットを改善して干渉を低減します。2.4 GHz 帯域がモバイル クライアントとデバイスに使用される場合、Bluetooth は避ける必要があります。同様に、これらのクライアントおよびデバイスを配置する場合、ワイヤレス コールのキャパシティ（8-37 ページ）の項で説明する音声だけの WLAN チャネル セルおよびビデオ コール容量数を考慮する必要があります。

リモート エンタープライズ接続の保護

正常に展開された場合は、パブリックまたはプライベート 802.11 Wi-Fi ホット スポットを使用することによって、シスコのモバイル エンドポイントとクライアントをリモート ロケーションからモバイル データ ネットワーク経由で企業にも接続できます。このようなシナリオでは、モバイル エンドポイントとクライアントは、VPN または VPN-less ソリューションを使用して安全に接続できます。VPN の場合、Cisco AnyConnect Mobile VPN クライアントを使用すると、セキュア SSL デバイスまたはクライアントをトンネル経由で企業に接続できます。

Cisco Jabber および Cisco AnyConnect の配置で重要な考慮事項は、保護対象のトラフィックです。Cisco AnyConnect モバイル VPN クライアントを Cisco Jabber とともにモバイル デバイスで使用する場合、デフォルトでデバイスへのすべてのトラフィックは暗号化された VPN トンネルを介して企業に送信されます。この動作は、一部の配置では望ましくない場合があります。Cisco Jabber の場合、VPN トンネルを介して企業に Jabber 固有のトラフィックのみが送信され、他のトラフィックはそのトンネル以外を介して送信される動作が適しています。これは、Split-Tunnel 機能を使用して実行できます。この機能を使用して、管理者は（宛先サブネットに基づき）VPN トンネルを通過するトラフィックと、平文で送信されるトラフィックを指定できます。Jabber トラフィックのみを保護するには、管理者は Cisco Unified Communications Manager クラスタ、IM および Presence クラスタ、ボイスメール サーバ、ディレクトリ サーバ、および Trivial File Transfer Protocol（TFTP）サーバの IP サブネットに加え、接続する可能性のあるすべてのエンドポイントの IP サブネットをトンネルに含めるように設定する必要があります。したがって、Split-Include ポリシーには、企業ネットワークの IP アドレス範囲を含める必要があります。大企業の IP スペースは、取得やその他のイベントのため連続的ではないため、この設定はすべての導入には適用されないことがあります。

Split-Tunnel に含める Cisco Jabber および Cisco AnyConnect の詳細については、次の Web サイトで入手可能な『*Cisco AnyConnect Deployment Guide for Cisco Jabber*』を参照してください。

https://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/guide_c07-717020.pdf

VPN-less 接続の場合、Cisco Jabber モバイル クライアントは Cisco Expressway ソリューションのモバイルとリモート アクセス機能を利用できます。このファイアウォール トラバーサル ソリューションは、音声およびビデオ コールに対する Unified CM 呼制御の登録や、企業のコラボレーション アプリケーションおよびサービスへのアクセス（IM and Presence、ボイス メール、ディレクトリ アクセスなど）で、Cisco Expressway E および Expressway C サーバによって提供される、企業への TLS リバース プロキシ接続を使用します。Cisco Expressway ソリューションのモバイルおよびリモート アクセス機能の詳細については、次の Web サイトのソリューション情報および製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html

Quality of Service

シスコのモバイル クライアントのアプリケーションおよびデバイスは、シスコのコラボレーション QoS マーキング推奨事項に従って、一般にレイヤ 3 QoS パケット値をマークします。これには、DSCP 46 または PHB EF のマーキング音声のみのコールのメディア トラフィック、DSCP 34 または PHB AF41 のビデオ コールのメディア（音声を含む）トラフィック、および DSCP 24 または PHB CS3 のコール シグナリング トラフィックが含まれます。適切なモバイル クライアントおよびデバイス アプリケーションのレイヤ 3 パケット マーキングにかかわらず、レイヤ 2 802.11 WLAN パケット マーキング（ユーザ優先度、または UP）はさらに課題を示します。一部のデバイスは、適切に無線レイヤ 2 802.11 ユーザ プライオリティ（UP）値（音声のみのコールのメディア UP 6、ビデオ コールのメディア UP 5、およびコール シグナリング UP 3）をマークします。しかし、シスコのモバイル クライアントがさまざまなモバイル デバイスで実行されている場合、レイヤ 2 ワイヤレス QoS マーキングには一貫性がありません。レイヤ 2 ワイヤレス QoS マーキングに依存した状態では、WLAN のトラフィックを適切に処理できません。Cisco Unified Wireless LAN Controller を使用した配置では、ワイヤレス SIP コール アドミッション制御（CAC）を有効にすると、適切でないか、または存在しないレイヤ 2 WLAN マーキングに対する何らかの対策になる場合があります。SIP CAC はメディア セッションのスヌーピングを使用し、ダウンストリームの音声およびビデオ フレームが適切に優先順位を付けられて処理できるようになります。モバイル クライアントのアプリケーション レイヤ 3 やレイヤ 2 のパケット マーキングが適切であるとしても、データとリアルタイム トラフィックの両方を含むさまざまなタイプのトラフィック生成の面で、モバイル デバイスはデスクトップ コンピュータと同じ多数の課題を示します。これを考えると、一般にモバイル デバイスはコラボレーション エンドポイントの信頼できないカテゴリに分類されます。モバイル クライアント デバイスが信頼されているエンドポイントとして見なされない配置の場合、ネットワークのプライオリティ キューイングと専用帯域幅が適切なトラフィックに適用されるように、トラフィック タイプおよびポート番号に基づいたパケット再マーキングが必要です。モバイル デバイスのトラフィックを再マーキングするだけでなく、ネットワーク ベースのポリシングとレート制限を使用してモバイル クライアント デバイスが大量のネットワーク帯域幅を消費しないようにすることを推奨します。

（注）　モバイル クライアントとデバイスは、モバイル データ ネットワークまたはパブリックやプライベートの Wi-Fi ホット スポット経由で Cisco AnyConnect クライアントを使用できるサーバがある企業にリモート接続できる場合があります。これらの接続は、インターネットを通過するため、IP パスにエンドツーエンドの QoS が存在しないことから、すべてのトラフィックはすべて、ベスト エフォートとして処理されます。音声およびビデオの品質には、これらのタイプの接続では保証できません。

SRST と拡張 SRST

低速または信頼性の低い WAN リンクで集中型呼処理プラットフォームから分離されている支社ロケーションに、Cisco Jabber for iPhone などのモバイル エンドポイントおよびクライアントを配置する場合は、ローカル呼処理の冗長性を考慮することが重要です。Cisco Jabber モバイル クライアントは SRST をサポートしませんが、ほとんどの Cisco Jabber モバイル クライアントは携帯電話の音声を使用するスマート フォンで動作するため、ユーザはモバイル プロバイダー ネットワークを使用して電話をかけられる場合があります。

Cisco Jabber モバイル クライアントに関する追加設計および配置については、シスコのモバイル クライアントおよびデバイス（21-81 ページ）を参照してください。

インテリジェント プロキシミティ

前述したように、インテリジェント プロキシミティは、シスコ ハードウェア エンドポイントとモバイル デバイス間のプロキシミティベースの接続を利用する機能を意味します。

Cisco 8851、8861、および DX シリーズ エンドポイントで利用可能な Intelligent Proximity for Mobile Voice 機能は、IP エンドポイトと携帯電話またはスマートフォンの間の Bluetooth ペアリングを使用し、ハンズフリー音声および携帯電話のコンタクトと通話履歴の共有を可能にします。

前述のとおり、8851、8861、および DX シリーズ エンドポイントでの Intelligent Proximity for Mobile Voice と Unified Mobility 機能セットには互換性があります。また、8851 および 8861 IP Phone の Intelligent Proximity for Mobile Voice は Cisco Jabber と互換性があるため、IP Phone 8851 および 8861 で音声を再生でき、Jabber クライアント デバイスでビデオが再生されます。

インテリジェント プロキシミティと Bluetooth ペアリングの詳細については、インテリジェント プロキシミティ（8-15 ページ）を参照してください。

コンタクト ソース

Cisco Jabber for Android および Cisco Jabber for iOS は、デフォルトで Cisco ディレクトリ統合（CDI）を使用します。この場合、Microsoft Active Directory などの LDAP v3 対応ディレクトリとの統合が使用されます。

カスタム属性のマッピングを必要とする LDAP ディレクトリとの統合では、これらの属性マッピングは Unified CM サーバからクライアントにダウンロードできるコンフィギュレーション ファイルで作成できます。

Cisco Jabber モバイル クライアントでは、Unified CM User Data Service（UDS）もサポートされています。これにより、クライアントが Unified CM ユーザ データベース（LDAP ディレクトリと同期している場合もある）を使用してコンタクト情報を検索できます。企業のファイアウォールの外部にあり Expressway モバイル & リモート アクセスを使用して接続している Jabber モバイル クライアントは、コンタクトの解決に UDS を自動的に使用します。

ローカルの Unified CM ユーザ データベースから連絡先情報を取得する代わりの手段として、UDS-to-LDAP Proxy 機能を使用することができます。UDS-to-LDAP Proxy では、コンタクト検索は UDS により処理されますが、社内 LDAP ディレクトリにプロキシされ、UDS は結果を Jabber クライアントに戻します。これにより Jabber クライアントは、Unified CM データベースでサポートされている最大ユーザ数を超える社内ディレクトリを検索できます。

リフレッシュ トークンを使用した OAuth でのログイン フロー

Cisco Jabber 11.9 以降、OAuth 2.0 承認フレームワークを使用して、クライアント承認と認証を容易に行えるようになっています。これにより、ログインが迅速化されるとともに、起動時やネットワーク遷移時の再認証も迅速化されます。Cisco Unified CM 12.0 および Unified CM 11.5(1) SU3 の前までは、導入環境内でシングル サインオン（SSO）が有効にされている場合、Cisco Jabber は OAuth のみを使用していました。OAuth 実装は、認証を行い承認トークンをクライアントに発行する承認サーバとしての役割を果たす Unified CM パブリッシャに依存します。このトークンとリフレッシュ トークンにより、クライアントがコラボレーション サービスに要求を行い承認を取得することが可能になります。また、リフレッシュ トークンを使用して、期限切れの承認トークンを素早く更新できます。OAuth 2.0 フレームワークの詳細については、承認フレームワーク（16-46 ページ）の項を参照してください。

OAuth を Jabber クライアントの承認と認証に使用するには、Cisco Unified CM、Unified CM IM and Presence、Unity Connection で、**OAuth with Refresh Login Flow** サービス パラメータを有効にする必要があります。同様に、Jabber クライアントが Expressway モバイルおよびリモート アクセスで OAuth を使用するには、**Authorize by OAuth token with refresh** 設定を Expressway-C で有効にする必要があります。

Cisco Jabber での OAuth 展開の詳細については、次の URL で入手可能な最新バージョンのホワイト ペーパー『*Deploying OAuth with Cisco Collaboration Solution Release 12.0*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

Apple プッシュ通知サービス（APNs）

Cisco Jabber for iPhone and iPad 11.9 以降では、Apple プッシュ通知サービス（APNs）がサポートされるようになっています。APNs を使用して、クライアントが実行している間も、バックグラウンドで着信コールとメッセージを受信できます。

これまでは、Jabber for Apple iOS クライアント（iPhone および iPad）は他の Jabber クライアントと同じように、クライアントがバックアップに移行すると、Voice and Video over IP（VVoIP）と IM およびプレゼンス サービス用の接続を維持するために定期的なダイレクト IP ソケット キープアライブを利用していました。Apple がダイレクト IP ソケットによる通知のサポートを終了するので、Apple iOS デバイスのバックグラウンドで実行中の Jabber for iOS クライアントに通知を送信するには近日中に APNs が必要になります。

Cisco Spark for Apple iOS でも、クライアントがバックグラウンドで実行中に、着信コールとメッセージ通知の受信を APNs でサポートしています。

（注）　非 iOS の Cisco Spark クライアント（Cisco Spark for Android、Cisco Spark for Windows、Cisco Spark for Mac）と非 iOS の Cisco Jabber クライアント（Jabber for Android、Jabber for Windows、Jabber for Mac）では、APNs による影響は*ありません*。

Cisco Jabber クライアント対応の APNs の詳細については、Cisco Jabber for iPhone and iPad 対応の Apple プッシュ通知サービス（APNs）（21-108 ページ）を参照してください。

Cisco Virtualization Experience Media Engine

Cisco Virtualization Experience Media Engine（VXME）は、Virtual Desktop Infrastructure（VDI）環境に Cisco Jabber コラボレーション エクスペリエンスを拡張することにより、不可欠なコラボレーション ソフトウェア コンポーネントを提供します。VXME はローカル プラットフォーム（シンクライアント）にインストールされるソフトウェア パッケージであり、完全に統合されたユーザ エクスペリエンスを確保しながら仮想デスクトップを介してリアルタイム メディアのルーティングをバイパスし、ローカルで終了した音声およびビデオによるリアルタイム通信を含めるために VDI セッションを拡張します。ホストされた仮想デスクトップは、ローカルにインストールされた Citrix Receiver または VMware View Client をそれぞれ介して、Citrix XenDesktop、Citrix XenApp Published Desktop または VMware VIEW でサポートされます。ホスト VDI プラットフォームに関係なく、ユーザには VXME のユニファイド コミュニケーションおよびシームレスな統合に対応した完全に統合されたアクセサリ付きの仮想デスクトップ上で Cisco Jabber を使用して、一貫した音声、ビデオ、仮想デスクトップ エクスペリエンスが提供されます。

Cisco Virtualization Experience Media Engine（VXME）の詳細については、次の Web サイトのデータ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/collaboration-endpoints/virtualization-experience-media-engine/index.html

Cisco Virtualization Experience Media Engine の配置に関する考慮事項

次の項では、Cisco Virtualization Experience Media Engine（VXME）を配置するときに重要な設計上の考慮事項について説明します。

Quality of Service

ネットワークが 8021.q Dual VLAN 用に設定されている場合、Cisco Virtualization Experience Media Engine（VXME）に追加の設定は必要ありません。ネットワークが 802.1q Dual VLAN 用に設定されていない場合、QoS はベスト エフォート型であり、シン クライアントはデータ VLAN に配置する必要があります。トラフィック マーキングの詳細については、次の Web サイトで入手可能な QoS 設計ガイドを参照してください。

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-ipv6/design-guide-listing.html

音声およびビデオのコール アドミッション制御は、既存の Cisco Unified IP Phone ガイドラインに従っており、仮想デスクトップの帯域幅制御は、接続ブローカ設定を介して提供されます。

SRST と拡張 SRST

低速または信頼性の低い WAN リンクで集中型呼処理プラットフォームから分離された支社ロケーションに Cisco VXME を配置する場合は、ローカル呼処理の冗長性を考慮することが重要です。Jabber がデスクフォン制御モードで動作している場合、WAN の障害時は、Cisco Jabber クライアントが実行される、ホストされた仮想デスクトップ（HVD）はデータセンターと共に配置されている Cisco Unified CM と通信し続けます。ただし、VXC ゼロ クライアントとペアになっているデスクトップ フォンへの Cisco Unified CM 接続は失われます。各支社ロケーションの Cisco IOS ルータ上で Survivable Remote Site Telephony（SRST）または拡張 SRST を使用することで、集中型呼処理プラットフォームへの接続が失われた場合でも VXC クライアントとペアになっているデスクフォンのエンドポイントの基本的な IP テレフォニー サービスは維持できます。

VXME は SRST または拡張 SRST をサポートしていません。

サードパーティ製 IP Phone

この項で説明されているように、一部のサードパーティ製 IP Phone およびデバイスは、基本的な IP テレフォニー機能を提供するためにシスコの呼制御と統合されている場合があります。

サードパーティ製 SIP IP Phone

サードパーティ製電話機には、機能アクセス ボタン（固定または可変）など、呼制御シグナリング プロトコルとは関係しない、固有のローカル機能が備わっています。基本的な SIP RFC サポートでは、特定のデスクトップ機能が Cisco Unified IP Phone と同じになるように対応し、特定機能の相互運用性にも対応します。ただし、これらのサードパーティ製 SIP 電話機は、Cisco Unified IP Phone の機能をフル装備しているわけではありません。

シスコは、Cisco Developer Network に参加している、Cisco Unified CM と Unified CME SIP の機能を利用するソリューションを開発している主要なサードパーティ ベンダーと協力しています。たとえば Tenacity Operating は accessaphone ipTTY という名前のソフトウェア ベースのエンドポイントを提供しています。このエンドポイントにより、IP テレフォニー用のターミナル テレタイプ（TTY）またはテキスト ベースの通信が有効になります。このソフトウェア ベースのエンドポイントは、サードパーティ製の SIP 電話機として Cisco Unified CM に登録および通信できます。

シスコの回線側 SIP の相互運用性の詳細については、次の Web サイトの『Cisco Unified Communications Manager programming guide』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html

Cisco Developer Network およびサードパーティの開発パートナーの詳細については、次の Web サイトの Cisco Developer Community で入手可能な情報を参照してください。

https://developer.cisco.com

コラボレーションのエンドポイントのハイ アベイラビリティ

呼制御プラットフォームの障害発生時にもサービスを維持するため、シスコのエンドポイントは登録および呼制御サービスの冗長性に応じて、複数のノードまたは複数のサーバを使用して設定できます。

Cisco Unified CM 呼制御を使用する場合、直接設定によって、またはブートアップ フェーズ中の DHCP によって、コラボレーション エンドポイントは複数の TFTP サーバ アドレスを受け入れて処理できます。エンドポイントのブートアップ中にプライマリ TFTP サーバが停止した場合、エンドポイントはセカンダリ TFTP サーバから設定ファイルを取得できます。

各エンドポイントは、デバイス プールとも関連付けられています。デバイス プールには、1 つ以上の Unified CM サブスクライバを持つ Unified CM Group が含まれます。これらのサブスクライバのリストが、各エンドポイントの設定ファイル内に送信されます。エンドポイントは、リスト内の最初の（プライマリ）サブスクライバへの登録を試行します。その Unified CM サブスクライバが使用できない場合、エンドポイントは、リスト内の 2 番めのサブスクライバ（セカンダリ）への登録を試行します。3 番め以降も同様に続きます。サブスクライバへの登録後は、現在のサブスクライバに障害が発生すると、エンドポイントは、Unified CM Group 内の優先順位リスト内の別のサブスクライバにフェールオーバーできます。優先順位の高いサブスクライバが復旧されると、エンドポイントはそのサブスクライバに再登録します。

CTI を利用するエンドポイント（デスクフォン制御モードで稼働する Cisco Jabber デスクトップ クライアントなど）の場合、CTI サービスの冗長性が必要です。この場合、Unified CM Group 設定によってノードでの障害発生時にクライアントがプライマリ CTIManager ノードからセカンダリ CTIManager ノードにフェールオーバーできるように、複数の Unified CM ノードで Cisco CTIManager サービスが稼働している必要があります。

Unified CM クラスタから WAN を介して配置されているエンドポイントのネットワーク障害に備えるために、エンドポイントの登録に使用するサーバ リスト内に、SRST または拡張 SRST を備えた、ローカルで使用可能な Cisco Integrated Services Router（ISR）または他の Cisco IOS ルータを構成することもできます。WAN の障害発生時には、エンドポイントは SRST ルータに登録し、継続して音声テレフォニー サービスを提供します（SRST モードでは、サポートされる機能セットがこれより小さい場合もあります）。Cisco Jabber および Cisco TelePresence System ビデオ エンドポイントなど、一部のエンドポイントでは SRST がサポートされないことに注意してください。

コラボレーション エンドポイントのキャパシティ プランニング

Cisco 呼制御プラットフォームは、次のハイレベル エンドポイント機能をサポートします。

- Cisco Unified CM クラスタは、Cisco Business Edition 7000 の一部として配置されている場合でも、最大 40,000 の SCCP または SIP エンドポイントをサポートします。
- Cisco Business Edition 6000 の一部として配置されている Cisco Unified CM クラスタは、サーバ タイプに応じて最大 2,500 の SCCP または SIP エンドポイントをサポートします。
- Cisco Business Edition 4000 は、最大 200 の SIP エンドポイントをサポートします。
- Cisco Unified CM Express は、最大 450 の SCCP または SIP エンドポイントをサポートします。
- Cisco Expressway-C クラスタと Expressway-E クラスタのペアでは、最大 10,000 のリモート エンドポイント プロキシ登録がサポートされます。

上記の数字は、通常の最大キャパシティです。呼制御プラットフォームで実際にサポートされる最大エンドポイント数は、プラットフォームが実行しているその他すべての機能や、ユーザの最繁時呼数（BHCA）などによって決まります。このため、実際のキャパシティは公称の最大キャパシティよりも小さくなることがあります。Jabber デスクトップ クライアントとその他のデスクフォン制御アプリケーションが動作できる十分な CTI キャパシティを確保できるようにするため、システムのサイジング時には Unified CM CTI キャパシティを検討する必要もあります。CTI サイジングの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

呼制御プラットフォームのキャパシティの他に、帯域幅とコールのキャパシティに関してネットワークの容量を考慮する必要があります。Cisco Unified Wireless IP Phone 7925G や Cisco Jabber が稼働する Android スマートフォンなど、ネットワーク エンドポイントのキャパシティが物理ポートの数ではなく、共有ワイヤレス ネットワークで使用可能な帯域幅とスループットの量によって決まる 802.11 ワイヤレス接続デバイスでは、特に注意が必要です。802.11 チャネル セルあたりの音声およびビデオ コールのキャパシティについては、ワイヤレス コールのキャパシティ（8-37 ページ）を参照してください。

Cisco 呼制御でのエンドポイント キャパシティ（プラットフォーム固有のノードごとのエンドポイント キャパシティなど）の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

コラボレーションのエンドポイントの設計上の考慮事項

次に、シスコ エンドポイントを配置するための大まかな設計上の推奨事項を要約したリストを示します。

- アナログ ゲートウェイは、スタンドアロン デバイスと Cisco IOS マルチサービス ルータの統合インターフェイス モジュールの両方として使用でき、両方のタイプともに、同じ配置内で使用できます。会社のロケーション間のアナログ ポート密度の要件を満たすゲートウェイまたはアナログ ゲートウェイを 1 つまたは複数選択します。必要なアナログ デバイスに対応するために適切なポート容量がすべてのロケーションに提供されていることを確認します。
- Cisco IP Phone 8800 シリーズおよび Cisco DX シリーズのエンドポイントの CTI モニタリングおよび制御を可能にするために、デバイスに関連付けられたエンドユーザ設定の [標準 CTI による接続時の転送および会議をサポートする電話の制御（Standard CTI Allow Control of Phones supporting Connected Xfer and conf）] のロールを有効にします。CTI アプリケーションがこれらの電話機をモニタリングまたは制御できるのは、このロールが有効にされた後です。
- リモート ブランチに対して WAN 経由のエンドポイントのファームウェアのアップグレードにかかる時間を最小にするために、リモート ロケーションでローカル TFTP サーバを配置することを考慮し、**load server** パラメータを使用して、このローカル TFTP サーバに対してその支社のエンドポイントを指定します。または、特定のリモート ロケーションにあるすべて、またはほとんどのデバイスがと同じ電話モデルである場合に、ピアのファイル共有（PFS）機能の使用を検討します。
- Cisco Unified IP デスクトップフォンは、インライン パワー対応のスイッチに接続された場合、またはインライン パワー インジェクタで配置された場合、Power over Ethernet（PoE）によって電力を受けることができます。ダウン タイムを短縮し、外部電源および壁面コンセントを不要にするために、インライン パワーの使用を検討します。
- 低速または信頼性の低い WAN リンクで集中型呼処理プラットフォームから分離された支社ロケーションにシスコのエンドポイントを配置する場合は、ローカル呼処理の冗長性を考慮することが重要です。各支社ロケーションの Cisco IOS ルータ上で SRST または拡張 SRST を使用することで、集中型呼処理プラットフォームへの接続が失われた場合でもデスクフォンの基本的な IP テレフォニー サービスは維持できます。ただし、デバイスが SRST に登録された場合に使用可能な一連の対ユーザ機能は、電話が Unified CM に登録された場合よりもずっと少なくなります。
- ネットワークの音声とデータ VLAN を分離した配置の場合、通常、データ VLAN に接続されたデスクトップ コンピュータ上で実行されているシスコのソフトウェア ベースのエンドポイントが音声 VLAN 上のエンドポイントと通信できるように VLAN 間ルーティングが設定および許可されていることを確認します。これは、ディレクトリや管理などのサービスを VLAN ベースで提供するデータ リソースに依存する可能性がある音声 VLAN 上のエンドポイントの場合でも重要です。
- ワイヤレス ネットワークのリアルタイム トラフィックを生成できるワイヤレス エンドポイントおよびモバイル エンドポイントを配置する前に、WLAN サイト サーベイを実行して、適切な RF 設計の確認、および干渉源の特定と除去を行う必要があります。これは、WLAN を通過するコールに対する許容可能な音声およびビデオの品質を保証するために必要です。
- ワイヤレス エンドポイントがあるロケーションから別のロケーションに移動するときに音声コールとビデオ コールが中断されないように、会社のセキュリティ ポリシーに準拠するだけでなく、高速キー再生成または認証を有効にする WLAN の認証および暗号化方式を選択します。

- シスコでは、音声およびビデオ トラフィックを生成できるワイヤレス エンドポイントとモバイル クライアント デバイスに接続するために、可能であれば、5 GHz WLAN 帯域（802.11a/n/ac）を利用することを推奨します。5 GHz WLAN は、音声コールとビデオ コールに対し、スループットを改善して干渉を低減します。2.4 GHz 帯域が無線クライアント デバイスとエンドポイントを接続するために使用されている場合は、Bluetooth は避ける必要があります。
- 適切なネットワークおよび呼制御機能を提供し、配置されたエンドポイントの数をサポートします。まず、呼制御プラットフォームあたりのエンドポイント登録と設定のキャパシティを検討します（Cisco Business Edition 7000 の一部として配置される場合を含め、最大で Unified CM クラスタあたり 40,000 のエンドポイント。Cisco Business Edition 6000 の一部として配置される場合はクラスタあたり 2,500 のエンドポイント。Cisco Business Edition 4000 に配置する場合は 200 の SIP エンドポイント。または Cisco Expressway 経由での 10,000 リモート エンドポイント登録）。次に、無線で接続されたエンドポイントのワイヤレス チャネル セルあたりのコール キャパシティを考慮し、WLAN チャネルあたり最大 27 の双方向音声専用ストリーム、または最大 8 の同時音声ビデオ ストリームまたはコールであることを確認します。
- エンドツーエンドのネットワーク インフラストラクチャが、該当するマーキングと再マーキング、信頼境界、優先および専用の両方の帯域幅クエリを使用したクエリ、レート制限、およびポリシングなど、適切な QoS ポリシーを使用して設定されていることを確認し、コレボレーション エンドポイントで高品質の音声およびビデオがエンド ユーザに提供されるようにします。

呼処理

改訂日:2018 年 3 月 1 日

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

この章では、シスコの呼処理製品によってスケーラブルで復元性のある呼処理システムを設計するためのガイドラインを示します。このような製品には、Cisco Unified Communications Manager(Unified CM)、および Cisco Unified Communications Manager Express(Unified CME)があります。主に次の要素を中心に説明します。

- 規模:ユーザ、ロケーション、ゲートウェイ、アプリケーションなどの数
- パフォーマンス:コールのレート
- 復元性:冗長性の規模

この章では、特に次のトピックについて説明します。

- 呼処理アーキテクチャ (9-2 ページ)

  ここでは、一般的な呼処理アーキテクチャおよびさまざまな呼処理ハードウェア オプションについて説明します。また、Unified CM クラスタリングについても説明します。

- 呼処理のハイ アベイラビリティ (9-13 ページ)

  ここでは、ネットワークの冗長性、サーバの冗長性、ロード バランシングなど、呼処理のハイ アベイラビリティに関する考慮事項について説明します。

- 呼処理のキャパシティ プランニング (9-22 ページ)

  ここでは、呼処理配置のサイジングの概要を示します。

- 呼処理の設計上の考慮事項 (9-26 ページ)

  ここでは、基本設計のガイドラインと呼処理を配置するためのベスト プラクティスの要約リストを示します。

- コンピュータ テレフォニー インテグレーション（CTI）（9-29 ページ）

  ここでは、Cisco コンピュータ テレフォニー インテグレーション（CTI）アーキテクチャについて説明し、CTI のコンポーネントとインターフェイス、CTI 機能、CTI のプロビジョニングとキャパシティ プランニングについて説明します。

- 複数の呼処理エージェントの統合（9-36 ページ）

  ここでは、Cisco Unified CM Session Management Edition（SME）で通常実行される、複数の呼処理エージェントの統合について説明します。また、Cisco Unified Communications Manager Express（Unified CME）との Cisco Unified CM の直接的統合についても扱います。

この章の変更点

表 9-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 9-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
マイナー アップデートと修正	この章の各項で説明	2018 年 3 月 1 日

呼処理アーキテクチャ

ユニファイド コミュニケーション システムの設計と配置を成功させるには、コール ルーティング機能を提供する基盤の呼処理アーキテクチャを理解することが重要です。この機能は、次のシスコの呼処理エージェントによって提供されます。

- Cisco Unified Communications Manager（Unified CM）

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

  VPN や Cisco Expressway などのコラボレーションに関する様々な先端ソリューションを使えば、インターネットからエンタープライズ コラボレーション ネットワークおよび Unified CM にアクセスして、リモート アクセスおよび Business-to-Business のセキュアなテレプレゼンスとビデオ コミュニケーションが可能になります。

- Cisco TelePresence Video Communication Server（VCS）

  Cisco TelePresence VCS は、ビデオ エンドポイントの登録、呼処理、および SIP および H.323 エンドポイントの帯域幅管理を行うことができるビデオ アプリケーションです。VCS は SIP レジストラ、SIP プロキシ サーバ、H.323 ゲートキーパー、および SIP から H.323 へのゲートウェイ サーバとして機能し、SIP と H.323 デバイスの間にインターワーキングを提供します。また Cisco TelePresence VCS は、VCS Expressway と組み合わせることによって、NAT/ファイアウォール トラバーサルを使用した外部通信を提供します。

SIP をサポートする TelePresence エンドポイントおよびルーム ベースの TelePresence 会議システムなどの、すべてのエンドポイントのメイン呼処理エージェントとして Unified CM を配置し、十分な機能を有する H.323 Telepresence エンドポイントとの相互運用性またはサードパーティ製ビデオ エンドポイントとの統合のためにのみ VCS を使用することを推奨します。これは、二重呼制御によりダイヤル プランおよびコール アドミッション制御が複雑になることを避けるためです。そのため、この章では VCS の詳細については説明しません。VCS の詳細については、『Cisco Collaboration System 10.*x* SRND』または Cisco VCS 製品のドキュメントを参照してください。

- Cisco Business Edition 4000 および Cisco Unified Communications Manager Express（Unified CME）

  Cisco Business Edition 4000（BE4K）は、中小企業向けに最適化された、新しいオンプレミスの完全クラウドマネージ型オーディオ テレフォニー プラットフォームです。Cisco Unified Communications Manager Express（Unified CME）と Cisco Unity Express Virtual（vCUE）を備えた Business Edition 4000 は、最大 200 台のデバイスの手頃な価格の統合 IP テレフォニーおよびボイスメール ソリューションを提供します。Cisco Business Edition 6000 および 7000 と同様に、Business Edition 4000 は、構成済みのハードウェア、インストール済みのライセンス、プリロードされたシスコ コラボレーション アプリケーションの提供により、見積もりと発注のプロセスを簡素化し、迅速な導入を実現します。

  Cisco Business Edition 4000 および Cisco Unified CME は、小規模な単一サイト導入と大規模な分散マルチサイト導入向けに呼処理サービスを提供します。Cisco Unified CME は、Cisco Unified CM の集中型呼処理導入でリモート サイトにおいてローカル呼処理をバックアップする機能を提供するための呼処理サービスも提供します。

Cisco Unified Communications Manager（Unified CM）および Cisco TelePresence Video Communication Server（VCS）は、標準のシスコ コラボレーション製品として、または、呼処理サービスおよび管理、会議、コンタクト センターなどのその他のサービスを含むパッケージ化されたコラボレーション ソリューションである Cisco Business Edition 6000 および Cisco Business Edition 7000 から使用可能です。

Cisco Business Edition 6000 および 7000 ソリューションにより、見積もり/発注のプロセスが簡素化され、事前に設定されたハードウェア、事前にインストールされた認可を受けたハイパーバイザ、事前にロードまたはインストールされたシスコ コラボレーション アプリケーションが用意されているため、導入が高速化されます。Cisco Business Edition 6000M および Cisco Business Edition 6000H は、最大で 1,000 人のユーザ向けの導入を対象としています。Cisco Business Edition 7000 は、1,000 人を超えるユーザ向けの導入を対象としています。シスコ コラボレーション アプリケーションの設計およびサイジングは、Cisco Business Edition 6000 では簡素化されています。ただし、Cisco Business Edition 7000 では、通常の Unified CM の設計およびサイジングのガイドラインが適用されます。

呼処理の仮想化

仮想化により、複数のシスコ コラボレーションの「サーバ」または「仮想マシン」を 1 つの物理サーバで実行できます。シスコ コラボレーションのサーバまたは仮想マシンは、このドキュメントで VM、ノード、またはインスタンスとも呼ばれています。

このアーキテクチャには、アプリケーションがハードウェア プラットフォーム上で直接動作している従来の導入と比べて、明らかなメリットがあります。たとえば、コスト（サーバ、電力、冷却、ラック スペースのコストなど）を大幅に削減できます。そして、ハードウェア プラットフォームの運用および保守を簡素化できます。仮想化は、物理サーバに直接インストールされ、仮想マシンを管理するハイパーバイザにより実現されます。シスコ コラボレーションに必要なハイパーバイザは、VMware ESXi Hypervisor です。

各仮想マシンには、仮想 CPU、仮想メモリ、仮想ディスクなどの仮想ハードウェア リソースが関連付けられています。これらのリソースは、仮想マシン テンプレートをパッケージおよび配布するオープン スタンダード ベースの方式である Open Virtualization Archive（OVA）を介して配布される事前定義されたテンプレートの各コラボレーション アプリケーションに定義されます。多くのシスコ コラボレーション アプリケーションでは、さまざまなキャパシティ オプションを提供するために、OVA の導入時に複数の VM 設定オプションが使用可能です。シスコ コラボレーション アプリケーションをインストールするときは、正しい仮想ハードウェア リソースを定義するためだけでなく、ホストの物理ディスクによって仮想ディスクに不整合が生じないようにするために（ストレージのパフォーマンスに影響します）、OVA を使用する必要があります。

シスコ コラボレーション呼処理エージェントの仮想化サポートは、次のとおりです。

- Cisco Unified CM は、仮想アプリケーションとしてのみ動作します。たとえば、Cisco UCS サーバへの直接の配置はできません。
- Cisco Unified CME は、Cisco サービス統合型ルータ上の Cisco IOS や IOS-XE ソフトウェア内で実行し、仮想化をサポートしていません。
- Cisco Business Edition 4000 は、Cisco 4321 サービス統合型ルータ（ISR）上の Cisco IOS-XE ソフトウェア内で実行し、仮想化をサポートしていません。

Cisco Unified Communications アプリケーションの仮想化の設計上および配置上の考慮事項については、次の URL で入手可能な情報を参照してください。

https://www.cisco.com/go/virtualized-collaboration

呼処理ハードウェア

Cisco Unified CM のハードウェア オプションには、3 種類があります。Tested Reference Configuration、Cisco Business Edition 6000 および 7000、仕様ベースのハードウェアです。

- Tested Reference Configuration（TRC）

  TRC は、Cisco Unified Computing System（UCS）サーバに基づいて選択されたハードウェア構成です。固定されたハードウェア構成を持ち、特定のアドバタイズされたパフォーマンス、キャパシティ、アプリケーションが混在するシナリオのためにシスコ コラボレーション アプリケーションでテストおよび検証されています。明確に検証されたインフラストラクチャを必要とする顧客や、必ずしも仮想化の経験があるわけではない顧客を対象としています。

  各 TRC のハードウェア構成が明確に定義され、このハードウェア構成から逸脱することは非常に限られています。たとえば、CPU モデルやコア数を変更したり、TRC の RAID 設定を変更すると、サーバ資格が変更されてサーバが TRC として見なされなくなり、仕様ベースのハードウェアとして見なされます。

- Cisco Business Edition 6000 および 7000

  Cisco Business Edition 6000 および 7000 は、ハードウェア プラットフォーム、仮想化ソフトウェア、シスコ アプリケーションを含むパッケージ化されたコラボレーション ソリューションです。ハードウェア プラットフォームは事前に構成されています（たとえば、ファームウェア、ドライバ、RAID コントローラは工場で構成済みです）。TRC と同様に、ハードウェア プラットフォームは特定のキャパシティとパフォーマンス向けにシスコ コラボレーション アプリケーションでテストおよび検証されています。

  Cisco Business Edition 6000 では、BE6000M および BE6000H の 2 つのハードウェア プラットフォーム オプションが使用可能です。Cisco Business Edition 7000 でも、BE7000M および BE7000H の 2 つのハードウェア プラットフォーム オプションが使用可能です。

  TRC および Cisco Business Edition 6000 および 7000 ハードウェア プラットフォームの詳細については、https://www.cisco.com/go/virtualized-collaboration のドキュメントを参照してください。

- 仕様ベースのハードウェア

  仕様ベースのハードウェア（単純に「仕様ベース」とも呼ばれます）は、より柔軟なハードウェア構成を提供します。たとえば、Cisco UCS TRC に基づいてプラットフォームを選択したり、CPU モデル、コア数、および RAID 構成を変更したり、iSCSI または NAS ストレージを使用することができます。必要に応じて、シスコ以外のサーバ ベンダーも使用できます。シスコ製品かどうかに関係なく、仕様ベースのハードウェア サーバが、次の『*VMware Compatibility Guide*』に記載されている必要があります。

  https://www.vmware.com/resources/compatibility/search.php

  仕様ベースのハードウェアはより柔軟なハードウェア構成を提供しますが、一部の要件も満たす必要があります。たとえば、CPU のモデルおよび最小 CPU 速度に関して要件があり、ログおよび統計情報を収集するために vCenter が必要となります。仕様ベースのハードウェアでは、シスコによってシスコ コラボレーション アプリケーションのハードウェア構成が明示的に検証されていない点に注意してください。したがって、コラボレーション アプリケーションはハードウェアの互換性に関する規範的なガイダンスを提供することができず、保証はされません。また、シスコ コラボレーション アプリケーションのパフォーマンスはガイダンスの目的に限定されています（https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-system/115955-uc-specs-tshoot-00.html でトラブルシューティングのテクニカル ノートを参照してください）。

  仕様ベースのハードウェアを使用したシスコ コラボレーション アプリケーションのパフォーマンスに関するガイドラインを入手するには、TRC または Cisco Business Edition 6000 および 7000 ハードウェア プラットフォームを参照用に使用します。詳細については、https://www.cisco.com/go/virtualized-collaboration のドキュメントを参照してください。

Cisco Unified CME は、Cisco 2900、3900、4000 シリーズ ISR などの Cisco サービス統合型ルータ（ISR）で実行されます。Cisco Unified CME は、仮想アプリケーション、またはクラウド サービス ルータ 1000V の一部としては実行されません。Cisco Business Edition 4000 は Cisco 4321 サービス統合型ルータ（ISR）上でのみ実行されます。Cisco Unity Express Virtual（vCUE）を利用するボイスメールは Cisco ISR 4321 のサービス コンテナ内でのみ実行可能で、UCS-E モジュール上では実行できません。

必要な規模、パフォーマンス、および冗長性に応じて、特定の配置に適した呼処理タイプとプラットフォームを決定します。一般に、Unified CM は非常に幅広いキャパシティ オプションと高い可用性を提供し、Cisco Unified CME は低いレベルのキャパシティと冗長性を提供します。冗長性とスケーラビリティの詳細については、呼処理のハイ アベイラビリティ（9-13 ページ）および呼処理のキャパシティ プランニング（9-22 ページ）を参照してください。

Unified CM クラスタのサービス

Cisco Unified CME はスタンドアロン呼処理アプリケーションですが、Unified CM はクラスタリングの概念をサポートしています。Unified CM アーキテクチャでは、サーバ ノードのグループを 1 つの呼処理エンティティまたは IP PBX システムとして連携させることができます。このサーバ ノード グループを*クラスタ*と呼びます。Unified CM サーバ ノードのクラスタは、設計上の制限事項を遵守している限り、IP ネットワークを介して分散していてもかまわず、空間的な冗長性、およびそれに伴う復元性をユニファイド コミュニケーション システムの設計にもたらすことができます。

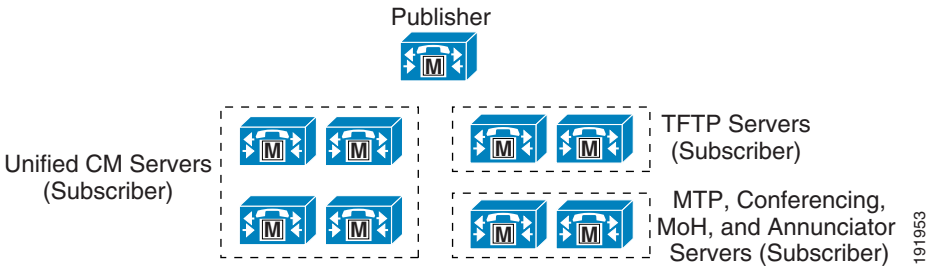
Unified CM クラスタの内部には、それぞれ固有のサービスを提供するサーバ ノードが存在します。これらの各サービスは、同じサーバ ノード上で他のサービスと共存できます。たとえば、小規模なシステムでは、データベース サービス、呼処理サービス、およびメディア リソース サービスを単一のサーバ ノードで提供できます。クラスタの規模とパフォーマンスを強化する必要が高まった場合は、これらのサービスの多くを専用サーバ ノードに移行する必要があります。

次の項では、Unified CM クラスタを形成しているサーバ ノードが実行する各種の機能について説明し、必要な規模、パフォーマンス、および復元性を達成するようにサーバ ノードを配置する方法について、ガイドラインを示します。

クラスタ サーバ ノード

図 9-1 に、複数のサーバ ノードで構成された一般的な Unified CM クラスタを示します。パブリッシャとサブスクライバという、2 つのタイプの Unified CM サーバ ノードがあります。これらの用語は、データベース間の関係をインストール時に定義するために使用されています。

図 9-1　　一般的な Unified CM クラスタ



パブリッシャ

パブリッシャはすべてのクラスタに必要なサーバ ノードであり、図 9-1 に示すように、クラスタごとに 1 つのパブリッシャだけを配置できます。このサーバ ノードは、最初にインストールする必要があります。クラスタ内の他のすべてのサブスクライバに対して、データベース サービスを提供します。パブリッシャ ノードは、コンフィギュレーション データベースに完全な読み取りと書き込みのアクセスができる唯一のサーバ ノードです。

1,250 ユーザを超える大規模なシステムの場合には、管理操作によるテレフォニー サービスへの影響を防止するために、専用パブリッシャを推奨します。専用パブリッシャのノード上で、呼処理または TFTP サービスが提供されることはありません。代わりに、これらのサービスはクラスタ内の他のサブスクライバ ノードによって提供されます。

パブリッシャ用の VM 設定は、クラスタで必要な規模とパフォーマンスを基準として選択する必要があります。パブリッシャは、呼処理サブスクライバと同等のサーバ ノード パフォーマンスを持つものにすることを推奨します。

サブスクライバ

ソフトウェアを初期インストールしたときに使用可能になるのは、データベース サービスとネットワーク サービスだけです。すべてのサブスクライバ ノードは、パブリッシャにサブスクライブして、データベース情報のコピーを取得します。ただし、Unified CM クラスタの初期化時間を短縮するために、クラスタ内のすべてのサブスクライバ ノードは、初期化時にデータベースのローカル コピーの使用を試みます。これにより、Unified CM クラスタの全体的な初期化時間は短縮されます。すべてのサブスクライバ ノードは、パブリッシャまたは他のサブスクライバ ノードからの変更通知によって、データベースのローカル コピーを更新された状態に保ちます。

図 9-1 に示すように、複数のサブスクライバ ノードが同じクラスタのメンバーになることができます。サブスクライバ ノードには、Unified CM 呼処理サブスクライバ ノード、TFTP サブスクライバ ノード、および会議や保留音（MoH）などの機能を提供するメディア リソース サブスクライバ ノードがあります。

呼処理サブスクライバ

呼処理サブスクライバは、Cisco CallManager サービスが有効になっているサーバ ノードです。このサービスが有効になった時点で、このノードは呼処理機能を実行できるようになります。電話、ゲートウェイ、メディア リソースなどのデバイスが登録やコール発信を実行できるのは、このサービスが使用可能になっているサーバに対してのみです。図 9-1 に示すように、複数の呼処理サブスクライバが同じクラスタのメンバーになることができます。実際、Unified CM は、クラスタごとに最大 8 つの呼処理サブスクライバ ノードをサポートします。

TFTP サブスクライバ

TFTP サブスクライバまたはサーバ ノードは、Unified CM クラスタの一部として、次の 2 つの主要な機能を実行します。

- サービスのためのファイルの提供。電話やゲートウェイなどのデバイスのコンフィギュレーション ファイル、電話および一部のゲートウェイのアップグレード用バイナリ ファイル、さまざまなセキュリティ ファイルなど。
- コンフィギュレーション ファイルおよびセキュリティ ファイルの生成。通常は署名済みであり、ダウンロード用として提供する前に暗号化されることもあります。

この機能を提供する Cisco TFTP サービスは、クラスタ内の任意のサーバ ノードで有効にできます。ただし、何らかの設定を変更すると、TFTP サービスがコンフィギュレーション ファイルを再生成するため、1,250 ユーザを超えるクラスタでは、他のサービスが影響を受ける場合があります。このため、1,250 ユーザを超えるクラスタまたは頻繁な設定変更を伴う機能を備えたクラスタでは、図 9-1 に示すように、特定のサブスクライバ ノードを TFTP サービス専用にすることを推奨します。

TFTP サブスクライバの VM 設定には、呼処理サブスクライバと同じものを使用することを推奨します。

メディア リソース サブスクライバ

メディア リソース サブスクライバまたはサーバ ノードは、会議や保留音などのメディア サービスをエンドポイントとゲートウェイに提供します。これらのタイプのメディア リソース サービスは、Cisco IP Voice Media Streaming Application サービスによって提供されます。このサービスは、クラスタ内の任意のサーバ ノードで使用可能にできます。

メディア リソースには、次のものがあります。

- 保留音（MoH）：保留状態になっているデバイス、会議に転送または追加されるデバイスに対して、マルチキャストまたはユニキャストの保留音を提供できます（保留音（7-19 ページ）を参照）。
- Annunciator サービス：電話番号を間違えていることや、コール ルーティングが使用不可になっていることを伝える場合に、トーンの代わりに音声アナウンスを流します（Annunciator（7-17 ページ）を参照）。
- カンファレンス ブリッジ：インスタント会議とパーマネント会議のための、ソフトウェア ベースの会議を提供します（トランスコーディング（7-5 ページ）を参照）。
- メディア ターミネーション ポイント（MTP）サービス：H.323 クライアント、H.323 トランク、および Session Initiation Protocol（SIP）エンドポイントおよびトランク用の機能を提供します（メディア ターミネーション ポイント（MTP）（7-7 ページ）を参照）。

クラスタ内でメディア リソースを実行する場合は、メディア リソース サービスの処理とネットワークに関する要件が追加される場合に備えて、すべてのガイドラインに準拠することが重要です。一般に、マルチキャスト MoH とアナンシエータ サービスには専用のメディア リソース サブスクライバを使用せず、ユニキャスト MoH およびソフトウェア ベースの大規模な会議と MTP に、図 9-1 に示すような専用のメディア リソース サブスクライバを使用することを推奨します（これらのサービスが、メディア リソース（7-1 ページ）の章で説明している設計ガイドラインの範囲内にある場合は除きます）。

その他のクラスタ サービス

Unified CM クラスタ内の特定のタイプのサブスクライバ ノード以外に、Unified CM 呼処理サブスクライバ ノードで実行できるその他のサービスもあり、追加機能を提供して使用可能にできます。

Computer Telephony Integration（CTI）Manager

CTI Manager サービスは、Cisco CallManager サービスと TAPI または JTAPI 統合アプリケーションの仲介者として機能します。このサービスは、CTI を利用するアプリケーションのクラスタで必要です。CTI Manager サービスは、CTI アプリケーションの認証を提供し、アプリケーションがエンドポイントの回線をモニタおよび制御できるようにします。CTI Manager は、呼処理サブスクライバ上だけで使用可能にできます。したがって、クラスタ内では最大で 8 つのノードで CTI Manager サービスを実行できます。

CTI Manager の詳細については、コンピュータ テレフォニー インテグレーション（CTI）（9-29 ページ）を参照してください。

Unified CM のアプリケーション

Unified CM 上では、Cisco Unified CM Assistant、エクステンション モビリティ、Web Dialer などのさまざまなタイプのアプリケーション サービスを使用可能にできます。これらのアプリケーションに関する設計ガイドラインの詳細については、Cisco Unified CM アプリケーション（18-1 ページ）の章を参照してください。Cisco IM and Presence サービスを追加することもできます（コラボレーションのインスタント メッセージングとプレゼンス（20-1 ページ）の章を参照）。

Unified CM の VM 設定の混在

Unified CM クラスタ内に VM 設定を混在させることはできますが、クラスタ内のすべての Unified CM ノードに同じ VM 設定を使用することを推奨します。また、Unified CM パブリッシャに使用する VM 設定が同じクラスタ内で使用されている他の Unified CM VM 設定を下回ることや、バックアップ サブスクライバに使用する VM 設定がプライマリ サブスクライバに使用する VM 設定を下回ることがないように設定することを推奨します。

クラスタ内の VM 設定を混在させる場合は、サポートされる全体のクラスタ キャパシティはクラスタ内の最小の VM 設定に対応するクラスタ キャパシティによって制限されるため、各 VM 設定間のキャパシティの違いを考慮する必要があります。

たとえば、7.5k VM 設定を使用する 1 つの Unified CM 呼処理ペアと、10k VM 設定を使用する 2 つの Unified CM 呼処理ペアを混在させる場合、サポートされる全体のクラスタ キャパシティは、7.5k VM 設定を使用したすべてのノードのクラスタ キャパシティに対応します。この例の 3 つの呼処理ペアについては、クラスタ キャパシティは 22.5k エンドポイント（3 * 7,500）に制限されます。このクラスタ キャパシティの制限をなくすための 1 つのオプションは、別のクラスタを展開し、そのクラスタを SIP トランクと接続することです。

ハードウェア プラットフォームおよび Business Edition プラットフォームの混在

Unified CM クラスタ内にさまざまなタイプのハードウェア プラットフォームを混在させることも許可されていますが、すべての VM 設定がすべてのサーバ ハードウェアでサポートされていないため、VM 設定が混在することにより、クラスタ キャパシティ全体に影響する場合があります（詳細については、Unified CM の VM 設定の混在（9-8 ページ）を参照してください）。また、混在するプラットフォームの一部が Business Edition 6000 の場合には、Business Edition 6000 ソリューション固有のルールを考慮する必要があります。

例 9-1　BE6000M および BE7000 の混在

BE6000M の一部として展開された Unified CM は、クラスタ ノードの数に関係なく 1,000 人のユーザと 1,200 台のデバイスに制限されます。ノードが BE7000 の一部かどうか、および追加ノードがより大きい VM 設定を使用するかどうかにかかわらず、他のノードを追加することができます。これにより冗長性や地理的な分散が提供されますが、BE6000 のサイジング ルールにより、クラスタ キャパシティは増加しません。BE6000M の Unified CM クラスタ キャパシティは、ノードが追加されても 1,000 人のユーザと 1,200 台のデバイスに制限されたままです。BE6000H にも同様の制限が適用され、ノード数に関係なく、最大 1,000 人のユーザと 2,500 台のデバイスに制限されます。

例 9-2　小規模 TRC および BE7000

Cisco Business Edition 6000M または 6000H ソリューションの一部でない Small Tested Reference Configuration（TRC）の場合、ノードのキャパシティは 1,000 ユーザまたはデバイスに制限されますが、Unified CM クラスタのキャパシティは 1,000 ユーザまたはデバイスに制限されません。クラスタに複数のノードを追加すると、1,000 を超えるユーザとデバイスをサポートできます。ただし、小規模 TRC ハードウェア プラットフォームでは、1,000 人のユーザ用の VM 構成のみがサポートされています。そのため、小規模 TRC で一部の Unified CM ノードが実行されていて、（Unified CM の VM 設定の混在（9-8 ページ）の項に記載されているように）同じクラスタ内に混在する BE7000 で一部が実行されている場合、サポートされる全体のクラスタ キャパシティは、最小の VM 設定を使用するノード（この場合は 1,000 人のユーザ用の VM 構成）に対応するクラスタ キャパシティによって制限されます。たとえば、1 つの Unified CM 呼処理ペアが小規模 TRC（1,000 人のユーザ用の VM 構成）で実行されていて、別の Unified CM 呼処理ペアが BE7000 で実行されている場合は、1k より大きい Unified CM VM 設定が BE7000 で展開されている場合でも、サポートされる Unified CM クラスタ キャパシティは 2,000 のユーザおよびデバイスに制限されます（2*1,000）。

別のベンダーからのサーバを混在させることはできますが、これは仕様ベースのハードウェアのポリシーである可能性があり、Unified CM パフォーマンスは、このタイプのプラットフォームの組み合わせでは保証されません。

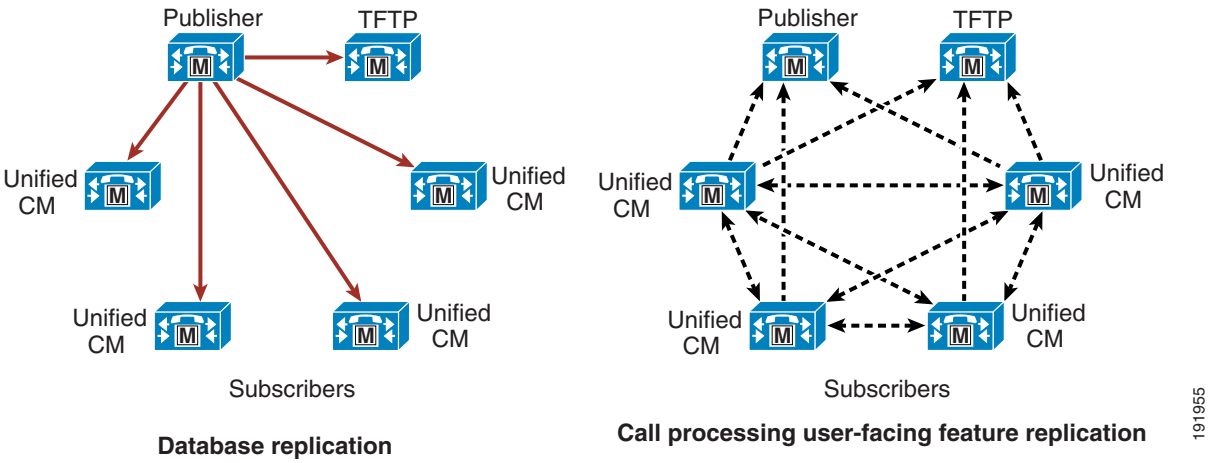
クラスタ内通信

2 種類の主要なクラスタ内通信（Unified CM クラスタ内の通信）があります（図 9-2 および図 9-3 を参照）。1 つ目は、すべてのデバイス構成情報を含むデータベースを配布するためのメカニズムです（図 9-2 の「データベース レプリケーション」を参照）。コンフィギュレーション データベースは、パブリッシャ ノードに保存され、コピーがクラスタのサブスクライバ ノードに複製されます。データベースの変更のほとんどはパブリッシャで加えられ、サブスクライバ データベースに伝達されます。そのため、クラスタのメンバー全体で設定の一貫性が確保され、データベースの空間的な冗長性が容易になります。

ユーザ方向の呼処理機能に対するデータベースの変更は、エンド ユーザ デバイスが登録されるサブスクライバ ノードで行われます。次にサブスクライバ ノードが、これらのデータベース変更をクラスタにある他のすべてのノードに複製し、ユーザ方向機能に冗長性を提供します（図 9-2 の「呼処理のユーザ方向機能の複製」を参照）。これらの機能には、次のものがあります。

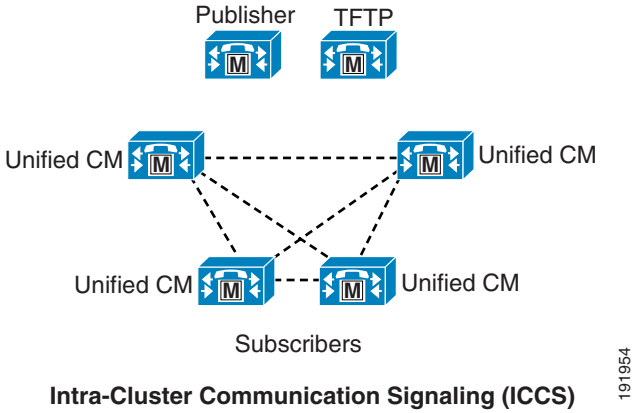
- 不在転送（CFA）
- メッセージ待機インジケータ（MWI）
- プライバシーの有効/無効
- エクステンション モビリティのログイン/ログアウト
- ハント グループのログイン/ログアウト
- デバイス モビリティ
- エンド ユーザおよびアプリケーション ユーザの Certificate Authority Proxy Function（CAPF）ステータス
- クレデンシャルのハッキングと認証

図 9-2　データベースおよびユーザ方向機能の複製



Intra-Cluster Communication Signaling（ICCS）と呼ばれる、もう 1 つのクラスタ内通信は、デバイスの登録、ロケーションの帯域幅、共有メディア リソースなどのランタイム データの伝搬と複製です（図 9-3 を参照）。この情報は、Cisco CallManager サービス（呼処理サブスクライバ）を実行している、クラスタのすべてのメンバー全体で共有されます。クラスタのメンバーと関連ゲートウェイとの間で、コールの最適なルーティングが確保されます。

図 9-3　Intra-Cluster Communication Signaling (ICCS)

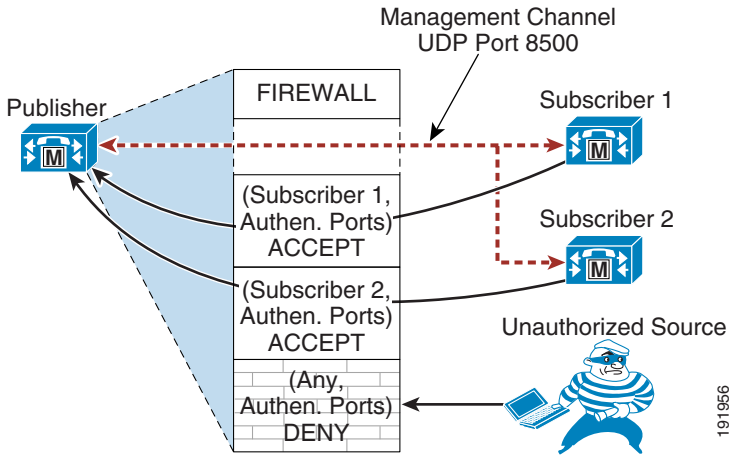


Intra-Cluster Communication Signaling (ICCS)

クラスタ内セキュリティ

Unified CM クラスタ内の各サーバ ノードが内部で動的ファイアウォールを実行します。Unified CM のアプリケーション ポートは、送信元 IP フィルタリングによって保護されます。動的ファイアウォールは、認証済みサーバまたは信頼できるサーバ ノードに対してだけ、これらのアプリケーション ポートを開きます（図 9-4 を参照）。

図 9-4　クラスタ内セキュリティ



このセキュリティ メカニズムは、単一の Unified CM クラスタ内のサーバ ノード間だけに適用できます。Unified CM のサブスクライバは、パブリッシャのデータベースにアクセスする前に、クラスタ内で認証されます。クラスタ内通信およびデータベース レプリケーションは、認証済みサーバ ノード間だけで発生します。インストール時にサブスクライバ ノードは、事前共有キー認証メカニズムでパブリッシャに対して認証されます。認証プロセスに必要な手順は次のとおりです。

1. セキュリティ パスワードを使用してパブリッシャ ノードをインストールします。
2. Unified CM Administration を使用することによって、パブリッシャ上にサブスクライバ ノードを設定します。

3. パブリッシャ サーバのインストール時に使用されたのと同じセキュリティ パスワードを使用して、サブスクライバ ノードをインストールします。
4. サブスクライバのインストール後、サーバ ノードは、UDP 8500 を使用する管理チャネル上でパブリッシャとの接続を確立しようとします。サブスクライバは、ホスト名、IP アドレスなどのすべてのクレデンシャルをパブリッシャに送信します。クレデンシャルは、インストール時に使用されたセキュリティ パスワードを使用して認証されます。
5. パブリッシャは、独自のセキュリティ パスワードを使用してサブスクライバのクレデンシャルを確認します。
6. その情報が有効な場合、パブリッシャは、自身の動的ファイアウォール テーブルに、信頼できる送信元としてサブスクライバを追加します。サブスクライバは、データベースへのアクセスを許可されます。
7. サブスクライバは、パブリッシャから他のサブスクライバ ノードのリストを取得します。すべてのサブスクライバが互いに管理チャネルを確立し、メッシュ トポロジが作成されます。

クラスタリングに関する一般的なガイドライン

すべての Unified CM クラスタに次のガイドラインが適用されます。

- クラスタ内のすべてのノードで同じ VM 設定を使用することを推奨します。Unified CM の VM 設定を混在させることができますが、設計に影響と制限があります。詳細については、Unified CM の VM 設定の混在（9-8 ページ）の項を参照してください。
- 通常の環境では、同一 LAN または MAN 内にクラスタのすべてのメンバーを入れます。
- クラスタが IP WAN にわたって構築されている場合、IP WAN を介したクラスタリング（10-46 ページ）の項を参照して、IP WAN を介したクラスタ化のガイドラインに従ってください。
- Unified CM クラスタには、20 のサーバ ノードを組み込めます。20 のサーバ ノードのうち、呼処理サブスクライバ（Cisco CallManager サービスを実行するノード）は最大で 8 つです。クラスタ内の残りのサーバ ノードは、専用データベース パブリッシャ、専用 TFTP サブスクライバ、またはメディア リソース サブスクライバとして設定できます。
- ノードが 2 つのクラスタを配置する場合も、クラスタ内のユーザ数が 1,250 を超えないようにすることを推奨します。1,250 ユーザを超える場合は、専用パブリッシャと別個のサーバ ノードをプライマリおよびバックアップの呼処理サブスクライバ用に推奨します。
- Business Edition 6000 は、Unified CM の単一のインスタンス（呼処理も扱う Unified CM パブリッシャ）を提供します。増設の Business Edition 6000 サーバは、Unified CM およびその他の共存するアプリケーションに対してサブスクライバの冗長性を提供するために、アクティブ/スタンバイ方式またはロード バランシング方式で配置できます。ただし、新しいノードと新しいハードウェア プラットフォームを追加してもキャパシティは増加しません。たとえば、ユーザおよびデバイスのキャパシティは増加しません。
- 各 Unified CM ノード インスタンスは、パブリッシャ ノード、呼処理サブスクライバ ノード、TFTP サブスクライバ ノード、またはメディア リソース サブスクライバ ノードのいずれかになります。クラスタごとに 1 つのパブリッシャ ノードだけがサポートされます。

- 仮想化により、Unified CM は、Simplified Message Desk Interface（SMDI）統合の Cisco Messaging Interface（CMI）サービス、オーディオ カード（MOH-USB-AUDIO=）を使用したライブ MoH オーディオ フィードの固定 MoH オーディオ ソースの統合、またはこれらのサーバへのフラッシュ ドライブをサポートしなくなっています。代わりに、次のオプションを使用できます。
  - MoH ライブ オーディオ ソース フィードの場合は、ライブ オーディオ ソース接続に Cisco IOS ベースのマルチキャスト MoH を使用することを検討してください。
  - システムのインストール ログの保存には、仮想フロッピー ソフトメディアを使用します。
  - Simplified Message Desk Interface（SMDI）の統合に対する Cisco Messaging Interface（CMI）サービスの代替オプションはありません。

呼処理のハイ アベイラビリティ

呼処理サービスは、可用性が高くなるように Unified Communications システム内に配置して、1 つの呼処理コンポーネントの障害によってすべての呼処理サービスが使用不可にならないようにする必要があります。

ハードウェア プラットフォームのハイ アベイラビリティ

呼処理のプラットフォームは、特定の配置のサイズとスケーラビリティだけでなく、プラットフォーム ハードウェアの冗長性にも基づいて選択する必要があります。

可能な場合は二重化電源を備えたプラットフォームを選択して、1 つの電源の障害によってプラットフォームが失われないようにします。二重化電源を備えたプラットフォームを 2 つの異なる電力源に接続して、1 つの電源回路が故障しただけでプラットフォーム全体に障害が発生することを回避します。二重化電源の使用と無停電電源（UPS）の使用を組み合わせると、電力の可用性は最大になります。二重化電源プラットフォームを実現できない配置でも、建物の電力が必要なレベルの電力の可用性を備えていない状況では、UPS の使用を推奨します。

プラットフォームで障害が発生すると、そのハードウェア プラットフォームで実行しているすべての仮想マシンで障害が発生する可能性があるため、仮想化を導入するときは、ハードウェア プラットフォームのハイ アベイラビリティを提供することがさらに重要になります。可能であれば、同じ物理サーバ上で同様の機能を持つ同じアプリケーションのインスタンスを複数実行することは避けます。代わりに、Cisco UCS B-Series Blade Server を使用している場合は、それらの仮想マシンを複数のサーバに割り振り、可能であれば複数のシャーシにも割り振ります。

ネットワーク接続のハイ アベイラビリティ

IP ネットワークへの接続性も、最大限のパフォーマンスとハイ アベイラビリティにとって重要な考慮事項です。Cisco Unified CME では、ネットワーク接続に最低 2 つ以上のポートを使用します。Unified CM では、ネットワーク接続のハイ アベイラビリティは、複数のアップリンクを介してハイパーバイザ仮想スイッチを設定し、ハードウェア プラットフォーム上で複数の物理ポートを使用することにより実現されます。そのため、OVA 設定に定義された 1 つの仮想 NIC で十分です。たとえば VMware vSphere 仮想スイッチを使用している場合は、スイッチ アップリンクに対して NIC チーミングを設定します。また、複数のこれらのポートを最低 2 台のアップストリーム スイッチに接続して、アップストリーム スイッチで障害が発生したときに復元力を提供します。

最高速度でプラットフォームをネットワークに接続し、最大スループット（UCS B シリーズ プラットフォームを使用する場合は、通常 1 Gbps または 10 Gbps）を確保します。プラットフォームが全二重でネットワークに接続されていることを確認します。

IP ネットワーク接続の速度とデュプレックス モード以外に、このネットワーク接続の復元性も同じように重要です。ユニファイド コミュニケーションの配置は、実際の冗長性に関して、基盤となるネットワーク接続に大きく依存します。このため、復元性が高い方法で基盤となるネットワーク インフラストラクチャを配置および設定することが重要です。可用性の高いネットワーク インフラストラクチャの設計の詳細については、ネットワーク インフラストラクチャ（3-1 ページ）の章を参照してください。すべての場合で、インフラストラクチャ内でスイッチまたはルータの障害が発生しても、ほとんどのユーザは配置内で提供されているほとんどのサービスにアクセスできるように、ネットワークを設計する必要があります。

呼処理の可用性を最大にするには、可能な場合は呼処理プラットフォームを別々の建物および別々のネットワーク スイッチに置いて接続し、建物またはネットワーク インフラストラクチャ スイッチの障害が発生したときの呼処理への影響を最小にします。Unified CM 呼処理では、このことは、可能な場合は常に、クラスタ サーバ ノードを LAN または MAN 配置内の複数の建物またはロケーション間で分散させることを意味します。最低限でも、同じロケーション内の異なる物理ネットワーク スイッチ間でネットワーク接続を物理的に分散させることを意味します。

さらに、Cisco Unified CME がスタンドアロンの呼処理エンティティであっても、物理的な分散とこの呼処理エンティティによる冗長性を提供することは、複数の呼処理エンティティを配置する場合にやはり意味を持ちます。そのようなシナリオで可能な場合は常に、Unified CME の各インスタンスをネットワーク内の異なる物理ロケーションにインストールするか、または最低限でも異なるネットワーク スイッチに物理的に接続します。

Unified CM のハイ アベイラビリティ

基盤となる Unified CM クラスタリングメカニズムのため、Unified Communications システムには、ハードウェア プラットフォームのディスクおよび電力コンポーネントの冗長性、物理ネットワーク ロケーション、および接続の冗長性以外にも、ハイ アベイラビリティに関する考慮事項があります。ここでは、呼処理サブスクライバの冗長性の考慮事項、呼処理のロード バランシング、およびその他のクラスタ サービスの冗長性について説明します。

呼処理の冗長性

Unified CM には、次の呼処理の冗長性設定オプションまたは冗長性方式があります。

- 2:1 冗長性方式：プライマリ呼処理サブスクライバ 2 台ごとに、1 つの共用セカンダリまたはバックアップ呼処理サブスクライバを設置します。
- 1:1 冗長性方式：プライマリ呼処理サブスクライバごとに、1 つのセカンダリまたはバックアップ呼処理サブスクライバを設置します。

これらの冗長性方式は、Unified CM クラスタ アーキテクチャ内の組み込み登録フェールオーバー メカニズムによって実施され、エンドポイントのプライマリ呼処理サブスクライバ ノードに障害が発生したときに、エンドポイントはバックアップ呼処理サブスクライバ ノードに再登録されます。この登録フェールオーバー メカニズムは、Skinny Client Control Protocol（SCCP）IP Phone のフェールオーバー レート、毎秒約 125 台の登録を実現できます。Session Initiation Protocol（SIP）電話機の登録フェールオーバー レートでは、毎秒約 40 台の登録です。

選択した呼処理の冗長性方式によって、配置の耐障害性だけでなく、アップグレードの耐障害性も決まります。

1:1 冗長性方式では、プライマリ呼処理サブスクライバで複数の障害が発生しても、呼処理機能に影響はありません。それに対して 2:1 冗長性方式では、バックアップ呼処理サブスクライバを共用する 2 つのプライマリ呼処理サブスクライバのうちの 1 つだけで障害が発生した場合、呼処理に影響はありません。ただし、両方のプライマリ サブスクライバに登録されているエンドポイントの合計数と、それら 2 つのプライマリ サブスクライバが処理するトラフィック量が、バックアップ サブスクライバのキャパシティ制限以内である場合、バックアップ サブスクライバで両方のプライマリ サブスクライバの障害を処理できます。

（注） 2 つのプライマリ サブスクライバの合計キャパシティ使用率がバックアップ サブスクライバのキャパシティを超える場合は、2:1 冗長性を導入しないでください。たとえば、呼処理キャパシティまたはエンドポイント キャパシティ使用率が両方のプライマリ サブスクライバで 50 % を超えると、両方のプライマリ サブスクライバに障害が発生した場合、バックアップ サブスクライバは呼処理サービスを適切に処理できなくなります。これらのシナリオでは、バックアップ サブスクライバ システムのキャパシティが超過したことが原因で、一部のエンドポイントが登録できない、一部の新しいコールを処理できない、一部のサービスおよび機能が適切に機能しないなどの状況が生じる可能性があります。

同様に、1:1 冗長性方式では、クラスタのアップグレードは、1 つのエンドポイント登録フェールオーバー期間だけが呼処理サービスに影響するように実行できます。それに対して 2:1 冗長性方式では、クラスタのアップグレードには複数の登録フェールオーバー期間が必要になる場合があります。

Unified CM クラスタは、サービスへの影響を最小限に抑えてアップグレードできます。2 つのバージョン（リリース）の Unified CM を同じサーバ ノード上に置いて、一方をアクティブ パーティションに、もう一方を非アクティブ パーティションに入れることができます。すべてのサービスとデバイスで、すべての Unified CM 機能に対して、アクティブ パーティションの Unified CM バージョンが使用されます。アップグレード時に、クラスタ操作はアクティブ パーティションにある現在のリリースの Unified CM を使用して続行されながら、アップグレード バージョンが非アクティブ パーティションにインストールされます。アップグレード プロセスの完了後は、サーバ ノードをリブートし非アクティブ パーティションをアクティブ パーティションに切り替えて、新しいバージョンの Unified CM を実行できます。

1:1 冗長性方式では、次の手順を使用して、ダウンタイムを最小限に抑えてクラスタをアップグレードできます。

手順 1 新しいバージョンの Unified CM を非アクティブ パーティションにインストールします。最初にパブリッシャにインストールしてから、すべてのサブスクライバ（呼処理サブスクライバ、TFTP サブスクライバ、およびメディア リソース サブスクライバ）にインストールします。リブートはしないでください。

手順 2 パブリッシャをリブートして、新しいバージョンに切り替えます。

手順 3 TFTP サブスクライバ ノードを 1 つずつリブートして、新しいバージョンに切り替えます。

手順 4 専用メディア リソース サブスクライバ ノードを 1 つずつリブートして、新しいバージョンに切り替えます。

手順 5 バックアップ呼処理サブスクライバを 1 つずつリブートして、新しいバージョンに切り替えます。

手順 6 プライマリ呼処理サブスクライバを 1 つずつリブートして、新しいバージョンに切り替えます。デバイス登録は、前にアップグレードおよびリブートされたバックアップ呼処理サブスクライバにフェールオーバーします。各プライマリ呼処理サブスクライバがリブートされると、デバイスはプライマリ呼処理サブスクライバへの再登録を開始します。

このアップグレード方法では、異なるバージョンの Unified CM ソフトウェアを実行しているサブスクライバ ノードにデバイスが登録される期間（登録フェールオーバー期間を除く）がありません。これらの手順はすべて Cisco Prime Collaboration を使用して自動化することができます。

2:1 冗長性方式では、クラスタ内のサーバ ノード数を少なくできますが、アップグレード時の登録フェールオーバーの発生頻度が多くなり、アップグレードの全体的な時間および特定のエンドポイントの呼処理サービスが使用不可になる時間が長くなります。プライマリ呼処理サブスクライバのペアごとにバックアップ呼処理サブスクライバは 1 つだけであるため、1 つのバックアップ呼処理サブスクライバのオーバーサブスクリプションを回避するために、一度にペアのうちの 1 つのプライマリ呼処理サブスクライバだけで新しいバージョンへリブートできます。その結果、各ペアの最初のプライマリ呼処理サブスクライバが新しいバージョンに切り替わった後、エンドポイント登録をバックアップ サブスクライバから新しくアップグレードされたプライマリ サブスクライバに移動するための時間が発生し、その後で 2 番めのプライマリ サブスクライバでのエンドポイント登録をバックアップ サブスクライバに移動して新しいバージョンへリブートできるようになります。この間、2 番めのプライマリ呼処理サブスクライバのエンドポイントは、バックアップ サブスクライバへの再登録中に使用不可になるだけでなく、新しいバージョンを実行するノードに再登録されるまでは、すでにアップグレード済みの他のサブスクライバ ノード上のエンドポイントに到達することもできません。

（注）　アップグレードを行う前に、ディザスタ リカバリ フレームワークを使用して、Unified CM およびコール詳細レコード（CDR）データベースを外部ネットワーク ディレクトリにバックアップすることを推奨します。このようにしておくと、アップグレードが失敗した場合のデータ損失を防止できます。

（注）　Unified CM クラスタのアップグレードでは、一部またはほとんどのデバイスから一時的に登録サービスおよび呼処理サービスが失われるため、アップグレードは前もって計画し、定期保守時に実装する必要があります。1:1 冗長性方式を選択すると、デバイスのダウンタイムおよびサービス停止を最小にできますが、それでも、一部またはすべてのユーザが呼処理サービスを使用できない時間が発生します。

Unified CM のアップグレードの詳細については、次の URL で入手可能なインストールおよびアップグレード ガイドを参照してください。

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

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

Cisco IOS SRST は、Unified CM クラスタから離れたロケーションにあるエンドポイントに、可用性の高い呼処理サービスを提供します。Unified CM クラスタリングの冗長性方式は確かに、LAN または MAN 環境内の呼処理などのアプリケーション サービスに高レベルの冗長性をもたらします。一方で、WAN などの低速リンクによって中央の Unified CM クラスタから分離されたリモート ロケーションの場合、冗長性方式として SRST を使用することにより、リモート サイトと中央サイトの間でネットワーク接続が失われたときに、基本的な呼処理サービスをこれらのリモート ロケーションに提供できます。呼処理サービスが重要であり、Unified CM クラスタへの接続が失われた場合にも呼処理サービスを維持する必要がある各リモート サイトには、SRST 対応の Cisco IOS ルータを配置することを推奨します。これらのリモート ロケーションのエンドポイントは、Unified CM 内の適切な SRST リファレンスとともに設定する必要があります。Unified CM サブスクライバへの接続を使用できない場合に、呼処理サービス用にどのアドレスを使用して SRST ルータに接続するかをエンドポイントが認識するようにするためです。

Cisco IOS ルータの Cisco Unified 拡張 SRST（E-SRST）は、中央の Unified CM クラスタへの接続が失われると、バックアップ呼処理機能を提供するためにリモート サイトで使用することもできます。E-SRST は、ルータの通常の SRST で使用できる機能よりも多くのテレフォニー機能を IP Phone に提供します。ただし、Unified E-SRST のエンドポイント キャパシティは、通常は基本的な SRST よりも低下します。SRST および E-SRST の両方が Cisco Unified SRST Manager でサポートされています。これは、SRST および E-SRST で Unified CM から設定を同期するので、ブランチの SRST または E-SRST ルータに必要な手動の設定が減り、ユーザが SRST および通常モードでも同様のコール操作を行えるようにします。

呼処理サブスクライバの冗長性

選択した冗長性方式に応じて（呼処理の冗長性（9-14 ページ）を参照）、呼処理サブスクライバは、プライマリ（アクティブ）サブスクライバまたはバックアップ（スタンバイ）サブスクライバのどちらかになります。ロード バランシングを実装する場合は、サブスクライバがプライマリ サブスクライバとバックアップ サブスクライバの両方を兼ねることもあります。クラスタの設計を計画するときは、通常は呼処理サブスクライバにこの機能を割り当てます。大規模なクラスタや高性能クラスタでは、呼処理サービスをパブリッシャおよび TFTP サブスクライバ ノード上で使用可能にしないでください。1:1 冗長性方式は、プライマリ サブスクライバとバックアップ サブスクライバの専用ペアを使用します。2:1 冗長性方式は、1 つのバックアップ サブスクライバを共用するプライマリ サブスクライバのペアを使用します。

次の図では、Unified CM で呼処理の冗長性を実現するための一般的なクラスタ構成を示しています。

図 9-5　　基本的な冗長性方式

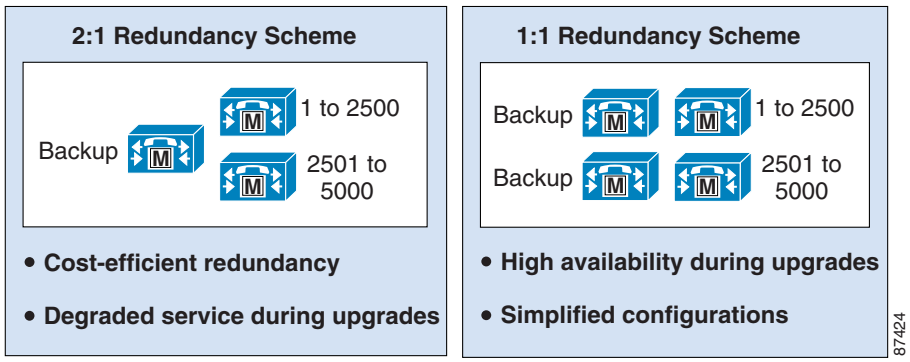


図 9-5 では、利用できる 2 つの基本的な冗長性方式を示しています。どちらの場合でも、バックアップ サーバ ノードは、障害の発生するプライマリ呼処理サーバ ノード 1 台分以上の処理能力を備えている必要があります。2:1 冗長性方式の場合、バックアップ サーバは、個々の配置の要件に応じて、障害の発生する呼処理サーバ ノード 1 台分、または両方のプライマリ呼処理サーバ ノードに相当する処理能力を備えている必要があります。キャパシティ サイジングと VM 設定の選択の詳細については、呼処理のキャパシティ プランニング（9-22 ページ）の項を参照してください。

（注） 2:1 冗長性では、バックアップ サブスクライバが過負荷の状態になることがあるので、10,000 人のユーザ用の VM 構成でサポートされません。

図 9-6　　1:1 冗長構成のオプション

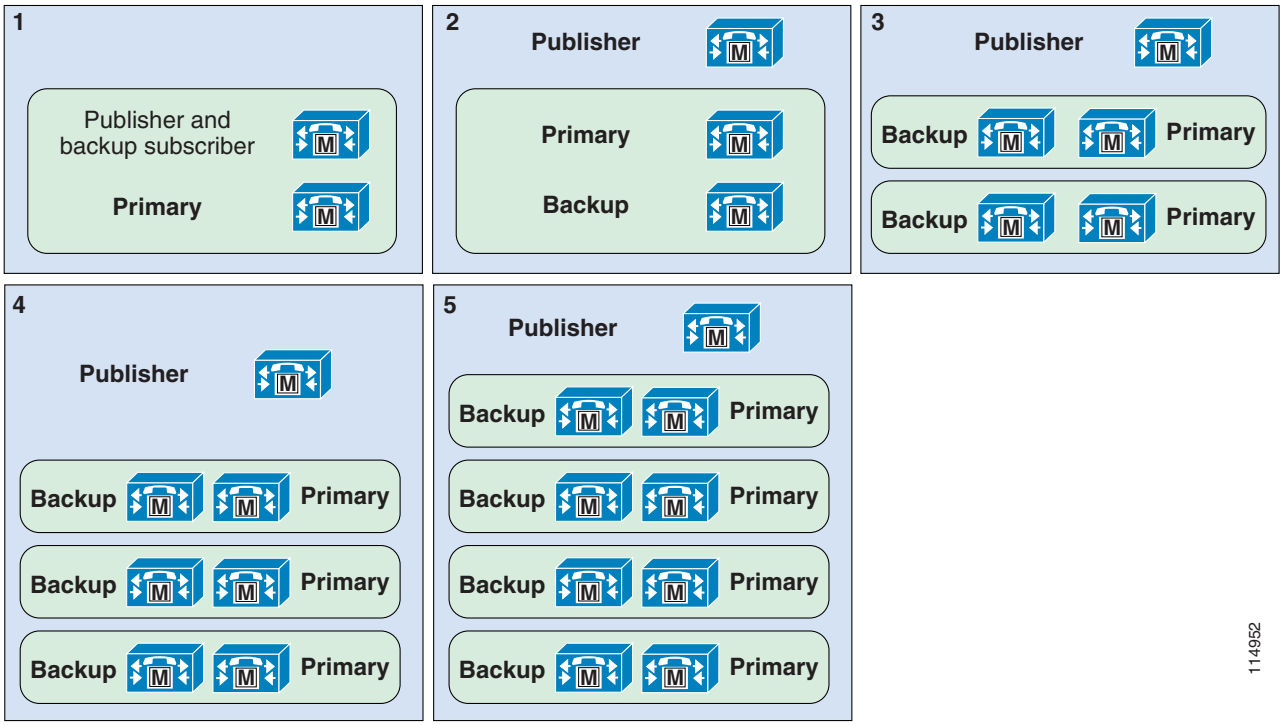


図 9-7　　2:1 冗長構成のオプション

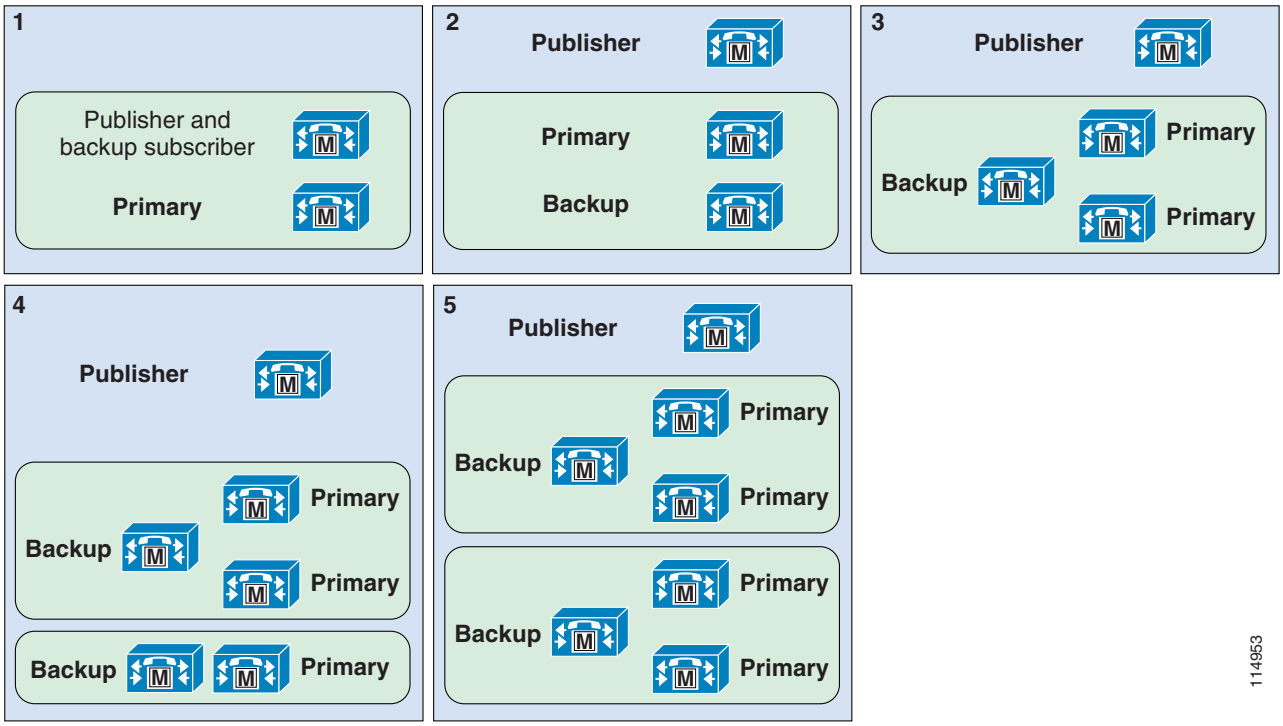


図 9-6 に示した 5 つは、すべて 1:1 冗長性のオプションを示しています。図 9-7 に示した 5 つは、すべて 2:1 冗長性のオプションを示しています。どちらの場合も、1,250 よりも少ないユーザをサポートし、Cisco Business Edition 6000 の Unified CM の展開を含むクラスタでは、オプション 1 を使用します。オプション 2 ～ 5 は、それぞれの冗長性方式でクラスタを徐々に拡張した様子を示しています。正確な規模は、選択したハードウェア プラットフォームや必要なハードウェア プラットフォームによって異なります。

これらの図では、パブリッシャと呼処理サブスクライバだけを示していることに注意してください。TFTP やメディア リソースなどの他のサブスクライバ ノードは示していません。

(注)　Unified CM グループあたり最大 3 つの呼処理サブスクライバを定義できます。追加のバックアップ用に 3 次サブスクライバを追加すると、上記の冗長性方式は 2:1:1 または 1:1:1 冗長性に拡張されます。ただし、WAN を介したクラスタリングの展開（リモート フェールオーバー配置モデル（10-57 ページ）を参照）で 3 次サブスクライバ ノードを使用する場合を除き、リモート サイトに設置するエンドポイント デバイスには 3 次サブスクライバの冗長性は推奨しません。エンドポイントが 3 次サブスクライバへの接続性をチェックする必要があると、SRST へのフェールオーバーがさらに遅延するためです。3 次サブスクライバは、クラスタ内の呼処理サブスクライバの最大数に対してもカウントされます（8 つの呼処理サブスクライバ ノード）。

図 9-6 または図 9-7 では示していませんが、シングルノード クラスタを配置することもできます。シングルノード クラスタのエンドポイント設定および登録が 1,000 を超えないようにする必要があります。シングル ノード構成では、バックアップ呼処理サブスクライバがないため、クラスタの冗長性メカニズムはありません。このようなタイプの配置では、冗長性メカニズムとして Survivable Remote Site Telephony（SRST）を使用して、Unified CM が使用できない際に最低限の呼処理サービスを提供する必要があります。

ロード バランシング

1:1 冗長性方式の Unified CM クラスタでは、プライマリ呼処理サブスクライバとバックアップ呼処理サブスクライバ間で、デバイス登録および呼処理サービスのロード バランシングを行うことができます。

通常、プライマリが使用可能な場合、バックアップ サーバ ノードに登録されたデバイスはありません。このことにより、所定の時間に呼処理の負荷を処理するプライマリ呼処理サブスクライバ ノードは最大で 4 つであるため、配置のトラブルシューティングは容易になります。さらに、Unified CM の冗長性グループとデバイス プールの数を減らすことにより、構成が簡素化される可能性もあります。

ロードバランスされた配置では、Unified CM の冗長性グループとデバイス プールの設定値を使用して、デバイス登録と呼処理にかかる負荷の半分までをプライマリ サブスクライバからセカンダリ サブスクライバに移すことができます。この方法で、各プライマリおよびバックアップ呼処理サブスクライバ ペアは、この呼処理サブスクライバ ペアによってサービスを提供される全デバイスの半数に、デバイス登録および呼処理サービスを提供します。これは、50/50 ロード バランシングと呼ばれます。50/50 ロード バランシング モデルには、次の利点があります。

- ロード シェアリング：登録と呼処理の負荷が複数のサーバ ノード上に分散され、応答時間をより速くできます。
- フェールオーバーとフェールバックが高速：すべてのデバイス（IP Phone、CTI ポート、ゲートウェイ、トランク、ボイスメール ポートなど）がすべてのアクティブ サブスクライバにわたって分散されるため、プライマリ サブスクライバに障害が発生した場合に、セカンダリ サブスクライバにフェールオーバーするデバイスは一部だけです。この方法で、サーバ ノードが使用不能になる影響を 50 % 減らすことができます。

50/50 ロード バランシングを計画するには、ロード バランシングを使用しない場合のクラスタのキャパシティを計算し、次に、デバイスおよびコールの量に基づいて、負荷をプライマリ サブスクライバとバックアップ サブスクライバに分散します。プライマリ サーバ ノードやバックアップ サーバ ノードの障害に対処できるようにするには、プライマリとセカンダリのサブスクライバの合計負荷が、サブスクライバ ノード 1 台分の負荷を超えないようにします。

(注)　50/50 ロード バランシングが設定された Unified CM クラスタのアップグレード中、バックアップ呼処理サブスクライバのアップグレードによって、そのサブスクライバに登録されているデバイス（プライマリ サブスクライバとバックアップ サブスクライバのペアによってサービスを提供される全デバイスの半数）は、プライマリ呼処理サブスクライバにフェールオーバーします。

TFTP の冗長性

大規模な Unified CM クラスタには複数の専用 TFTP サブスクライバ ノードを配置して、TFTP サービスの冗長性を提供することを推奨します。通常は 2 つの TFTP サブスクライバで十分ですが、クラスタに 3 つ以上の TFTP サーバ ノードを配置することもできます。

1 つ以上の冗長 TFTP サブスクライバを提供する以外に、これらの冗長 TFTP ノードを利用するためのエンドポイントを設定する必要があります。DHCP を使用するかまたは静的に TFTP オプションを設定する場合、クラスタ内の両方の TFTP サブスクライバ ノードの IP アドレスを含む TFTP サブスクライバ ノード IP アドレス アレイを定義します。この方法では、2 つの異なる IP アドレス アレイで 2 つの DHCP スコープを作成することによって（または、2 つの異なる TFTP サブスクライバ ノード IP アドレスでエンドポイントを手動で設定することによって）、TFTP サブスクライバ A をプライマリ、TFTP サブスクライバ B をバックアップとして使用する半分のエンドポイント デバイスと、TFTP サブスクライバ B をプライマリ、TFTP サブスクライバ A をバックアップとして使用するもう半分のエンドポイント デバイスを割り当てることができます。1 つの TFTP サブスクライバの障害時の冗長性を提供する以外に、複数の TFTP サブスクライバにわたってエンドポイントを分散させるこの方法はロード バランシングをもたらし、1 つの TFTP サブスクライバですべての TFTP サービス負荷を処理しないようにします。

(注)　電話やゲートウェイの個々のバイナリまたはファームウェア ロードを追加する場合は、ファイルをクラスタ内の各 TFTP サブスクライバ ノードに追加する必要があります。

CTI Manager の冗長性

すべての CTI 統合アプリケーションは、CTI Manager サービスを実行している呼処理サブスクライバ ノードと通信します。さらに、ほとんどの CTI アプリケーションには、冗長 CTI Manager サービス ノードを指定する機能があります。そのため、クラスタ内の少なくとも 2 つの呼処理サブスクライバで CTI Manager サービスをアクティブにすることを推奨します。プライマリとバックアップ両方の CTI Manager が設定されている場合、障害が発生すると、アプリケーションはバックアップ CTI Manager に切り替えて CTI サービスを受けます。

すでに説明したように、CTI Manager サービスは呼処理サブスクライバ上だけで使用可能にできます。したがって、クラスタごとに最大で 8 つの CTI Manager があります。復元性、パフォーマンス、および冗長性を最大限まで高めるには、CTI アプリケーションの負荷をクラスタ内で使用可能な CTI Manager に分散することを推奨します。

一般に、CTI アプリケーションによって制御またはモニタされるデバイスは、CTI Manager サービスに使用するものと同じサーバ ノード ペアに関連付けることを推奨します。たとえば、音声自動応答装置（IVR）アプリケーションでは 4 つの CTI ポートが必要になります。1:1 冗長性と 50/50 ロード バランシングを使用する場合は、これらを次のように設定します。

- 2 つの CTI ポートは、サーバ ノード A をプライマリ呼処理サブスクライバ、サーバ ノード B をバックアップ サブスクライバとする Unified CM 冗長性グループを持つようにします。残りの 2 つの CTI ポートは、サーバ ノード B をプライマリ サブスクライバ、サーバ ノード A をバックアップ サブスクライバとする Unified CM 冗長性グループを持つようにします。
- IVR アプリケーションは、サブスクライバ A 上の CTI Manager をプライマリ、サブスクライバ B をバックアップとして使用するように設定します。

上の例は、サブスクライバ A 上の CTI Manager で障害が発生した場合の冗長性を備えており、IVR コールの負荷を 2 台のサーバ ノードに分散することもできています。この方法では、Unified CM サブスクライバ ノードの障害による影響も最小限に抑えることができます。

CTI および CTI Manager の詳細については、コンピュータ テレフォニー インテグレーション（CTI）（9-29 ページ）を参照してください。

仮想マシンの配置およびハードウェア プラットフォームの冗長性

仮想化を使用する場合、物理サーバ間にわたる Unified CM サーバ ノードのインストールと常駐というサーバ ノードの仮想的特徴があるため、冗長性に関する考慮事項があります。

図 9-8 に示すように、たとえば、Unified CM を配置して最大レベルの呼処理の冗長性を確保する場合は、次のガイドラインに従ってください。

- 各プライマリ呼処理サブスクライバ ノード インスタンスは、バックアップ呼処理サブスクライバ ノード インスタンスとは異なる物理サーバ上に存在する必要があります。これにより、プライマリ呼処理ノード インスタンスを含むサーバで障害が発生しても、バックアップ呼処理サブスクライバ ノードへのアクセスをエンドポイントに提供するシステムの機能に影響は及ぼされません。
- サービスの冗長性のために複数の TFTP またはメディア リソース サブスクライバ ノード インスタンスを配置する場合は、冗長サブスクライバ ノードを常に複数のサーバに分散させて、1 つのサーバの障害によってそれらのサービスが排除されないようにします。これにより、TFTP またはメディア リソース サブスクライバを含むブレードで障害が発生しても、エンドポイントは別のサーバ上に存在するサブスクライバ ノードで TFTP およびメディア リソース サービスにアクセスできます。障害のないシナリオでは、エンドポイントも冗長 TFTP およびメディア リソース サブスクライバ ノード インスタンス間で分散させて、システムをロードバランスできます。
- CTI アプリケーションを配置する場合は、CTI Manager サービスを実行する呼処理サブスクライバ ノード インスタンスを常に複数のサーバに分散させて、1 つのサーバの障害によって CTI サービスが排除されないようにします。さらに、CTI アプリケーションは、1 つのサーバ上のサブスクライバ ノード インスタンスで実行されている CTI Manager サービスをプライマリ CTI Manager として使用し、別のサーバ上のサブスクライバ ノードで実行されている CTI Manager サービスをバックアップ CTI Manager として使用するように設定する必要があります。

図 9-8　　UCS での Unified CM サーバ ノードの分散

シャーシでブレード サーバを使用する場合（たとえば、Cisco UCS 5100 ブレード シャーシでは B シリーズ ブレード サーバ）、サブスクライバ ノード インスタンスを複数のブレードに分散させる以外に、複数のブレード シャーシにサブスクライバ ノード インスタンスを分散させて、冗長性と拡張性を追加できます。

仮想マシンのホスト リソースの冗長性とプロビジョニングの詳細については、https://www.cisco.com/go/virtualized-collaboration にあるドキュメントを参照してください。

Cisco Business Edition のハイ アベイラビリティ

Cisco Business Edition 6000M、Cisco Business Edition 6000H、Cisco Business Edition 7000 では、追加の Cisco Unified CM ノードのクラスタリングによりハイ アベイラビリティが提供されます。追加の Business Edition サーバは、呼処理のほか、その他のアプリケーションおよびサービスに対するハイ アベイラビリティを提供するために配置できます。

（注）　WAN 配置でのクラスタリングと同様に、追加の冗長性と地理的な分散、あるいはそのいずれかを提供するために、2 台を超える物理サーバをクラスタリングできます。ただし、Cisco Business Edition 6000 では、サーバの追加により冗長性のみが提供され、キャパシティは増加しません。たとえば、BE6000M と BE6000H では、クラスタ全体でユーザの合計数は 1,000 を超えることができません。この制限値を超える配置は、標準の Unified CM クラスタと見なされます。このため、展開は標準の Unified CM のハイ アベイラビリティ設計ガイダンスに従う必要があります（Unified CM のハイ アベイラビリティ（9-14 ページ）を参照）。Cisco Business Edition 7000 では、キャパシティは 1,000 ユーザに制限されていません。正確には、標準アプリケーションのキャパシティ プランニングおよび設計ルールが適用されます。

呼処理のキャパシティ プランニング

呼処理のキャパシティ プランニングは、ユニファイド コミュニケーションの配置を成功させるために重要です。このセクションでは、Cisco Business Edition 6000 または 7000 の一部であるかどうかに関係なく、Cisco Unified CM のキャパシティ プランニングについて説明します。また、Cisco Business Edition 4000 および Unified CME も扱います。

Unified CM のキャパシティ プランニング

Unified CM のキャパシティは、ハードウェア プラットフォーム、VM 設定、展開要件によって異なります。また、Unified CM が Cisco Business Edition 6000 の一部として展開されているかどうかによっても異なります。表 9-2 に、一般的な Unified CM のキャパシティ制限を示します。

表 9-2　Cisco Unified CM のキャパシティ制限

容量情報	Cisco Business Edition 6000M	Cisco Business Edition 6000H	Cisco Business Edition 7000 および Enterprise Cisco Unified CM
最大ユーザ数	クラスタごとに 1,000	クラスタごとに 1,000	ノードごとに最大 10,000、クラスタごとに最大 40,000[1]
最大エンドポイント数	クラスタごとに 1,200	クラスタごとに 2,500	ノードごとに最大 10,000、クラスタごとに最大 40,000[1]
キャパシティ プランニングの実行方法	製品マニュアルのキャパシティ情報[2]	製品マニュアルのキャパシティ情報[2]	製品マニュアル、SRND ガイドライン、Cisco Collaboration Sizing Tool[3]

1. メガクラスタ展開ではより多くなる場合があります。
2. 必要に応じて、Business Edition 製品マニュアルの固定キャパシティ数の代わりに、Cisco Collaboration Sizing Tool に基づいたキャパシティ プランニングを使用することができます。ただし、この場合も Unified CM クラスタは 1,000 ユーザに制限されます。
3. 最大 10,000 のユーザまたはエンドポイント（いずれかの制限に先に到達）の展開では、Cisco Preferred Architecture for Enterprise Collaboration で使用可能な簡素化されたサイジングを使用してキャパシティ プランニングを行うことができます。

Cisco Business Edition 6000M/H のキャパシティ プランニング

Cisco Business Edition 6000 では、Unified CM は特定の VM 設定で展開され、Unified CM キャパシティは固定されます。Cisco Unified CM キャパシティ プランニングはシンプルで、Cisco Collaboration Sizing Tool には依存しません。

Cisco Business Edition 6000M で展開された Unified CM では、最大 1,000 のユーザ、1,200 のデバイス、5,000 の BHCA がサポートされます。Business Edition 6000H では、最大 1,000 のユーザ、2,500 のデバイス、5,000 の BHCA がサポートされます。

BE6000 では、ハイ アベイラビリティを提供するためのノードまたはハードウェア プラットフォームの追加がサポートされていますが、これによりキャパシティは増加しません。Business Edition 6000 に固有の VM 設定を使用する必要があります。2,500、7,500、または 10,000 ユーザのためのより大きな VM 設定は、Business Edition 6000 では使用できません。

Business Edition 6000 の一部として展開された Unified CM には、いくつかの追加の制限事項があります。たとえば、Cisco Business Edition 6000M/H では、最大 50 のサイトと最大 100 のコンタクト センター エージェントがサポートされています（詳細については、https://www.cisco.com/go/be6000 で利用可能な Cisco Business Edition 6000 の製品マニュアルを参照してください）。これらの要件を満たすことができず、ユーザ数が 1,000 を下回る場合には、Cisco Business Edition 6000M/H のキャパシティ プランニングに対して別のアプローチを取ることができます。Business Edition 6000 に固有の固定されたキャパシティに依存する代わりに、製品マニュアルのサイジングのガイドライン、この SRND、Cisco Collaboration Sizing Tool に基づいて、Business Edition 7000 および企業 Unified CM と同じ方法でサイジングを行うことができます。サイジング ツールを使用するときは、1,000 人のユーザ用の VM 構成を選択する必要があります。

Cisco Business Edition 7000M/H および Cisco Unified CM のキャパシティ プランニング

Cisco Business Edition 7000 または（Business Edition 以外の）企業バージョンの Cisco Unified CM では、さまざまな VM 設定を、さまざまな対応するキャパシティとともに使用することができ、ノードを追加するとキャパシティが増加します。キャパシティ プランニングは、このドキュメントのガイドラインと Cisco Collaboration Sizing Tool に基づいて行います。ただし、*Cisco Preferred Architecture for Enterprise Collaboration CVD*（https://www.cisco.com/go/pa で利用可能）に簡素化されたキャパシティ プランニング方法が説明されています。Unified CM 展開のユーザまたはデバイスの数が 10,000 未満で（いずれかの制限に先に到達）、特定のサイジングの前提条件が満たされている場合に、この簡素化されたサイジング方法を使用することができます。サイジングの前提条件を満たすことができない場合は、簡素化されたキャパシティ プランニングを使用することはできず、製品マニュアルのガイドライン、この SRND、Cisco Collaboration Sizing Tool に基づく通常のキャパシティ プランニングを代わりに行う必要があります。サイジング ツールではさらに多くのパラメータが考慮されます。たとえば、電話のタイプ（SCCP、SIP、またはモバイル）や電話のセキュリティ モードが考慮されます。これはより複雑なサイジング プロセスですが、特定の展開に対してカスタマイズできます。

一部の Unified CM 機能の利用を可能にしたり増やしたりすると、システムの呼処理機能に影響を与える可能性があり、全体的なキャパシティを低下させる場合もあります。これらの機能には、トレース、コール詳細レコード、複雑なダイヤル プラン、および Unified CM プラットフォーム上に共存するその他のサービスが含まれます。複雑なダイヤル プランには、複数のライン アピアランス、多くのパーティション、コーリング サーチ スペース、ルート パターン、変換、ルート グループ、ハント グループ、ピックアップ グループ、ルート リスト、自動転送、共存サービス、およびその他の共存アプリケーションが含まれています。こうした機能はすべて、Unified CM システム内の追加リソースを消費します。

次の手法を使用して、システム パフォーマンスを向上させることができます。

多数のゲートウェイ、ルート パターン、トランスレーション パターン、およびパーティションを含む非常に大きなダイヤル プランを持つ Unified CM クラスタでは、Cisco CallManager サービスの初回始動時に、初期化に長い時間がかかる場合があります。デフォルトの時間内にシステムが初期化されない場合、システム初期化タイマー（Unified CM サービス パラメータ）を変更して、設定を初期化するための時間を追加できます。システム初期化時間の詳細については、Unified CM Administration の *サービス パラメータ*に関するオンライン ヘルプを参照してください。

Unified CM のキャパシティ プランニング ガイドラインおよびエンドポイントの制限

次のキャパシティのガイドラインは、Cisco Business Edition 7000 の一部である Cisco Unified CM、または Business Edition 以外の Cisco Unified CM に適用されます。

- クラスタ内では、Cisco CallManager サービスを使用して最大 8 つの呼処理サブスクライバ ノードを使用可能にできます。それ以外のサーバ ノードは、パブリッシャ、TFTP サブスクライバ、メディア リソース サブスクライバなどの専用機能に使用できます。
- 各 Unified CM ノードは、最大 10,000 台のセキュアまたはセキュアでない SCCP または SIP エンドポイントの登録をサポートできます。各クラスタは、最大 40,000 台のセキュアまたはセキュアでない SCCP または SIP エンドポイントの設定および登録をサポートできます。

- 必要なキャパシティに応じて、OVA で使用可能ないくつかの Cisco Unified CM 用の VM 設定オプションがあります。VM 設定の名前は、各ユーザが 1 台の電話機を所有していることを前提として、各ノードで最大ユーザ数に対応しています。ユーザごとの電話の数の比率が 1 ではない場合には、VM 設定名がノードごとのエンドポイントの最大数に実際に対応します。使用される BHCA および機能セットなどのさまざまな変数に応じて、実際のユーザまたはエンドポイントの数が下回る場合があります。導入のサイジングを検証するには、https://www.cisco.com/go/cst で利用可能な Cisco Collaboration Sizing Tool を使用してください。
- CallManager サービスのデフォルトのトレース設定は、Signaling Distribution Layer（SDL）トレースで 10 MB の 1,500 ファイルになります。コール レートの高い環境での特定のトラブルシューティングでファイルの最大数を増やす必要がある場合を除き、ほとんどの環境ではデフォルト設定で十分なトレースを収集できます。

サイジングの制限や、システム サイジング、キャパシティ プランニング、および配置の考慮事項に関する詳しい説明など、Unified CM キャパシティ プランニングの考慮事項の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

メガクラスタ

*メガクラスタ*という用語は、拡張性をさらに増大させることが可能な特定の Unified CM 配置を定義および識別します。メガクラスタでは、追加の Unified CM サブスクライバ ノードのサポートにより、さらに多くのデバイス キャパシティが提供されます。メガクラスタごとに最大 8 つの Unified CM サブスクライバ ペア（1:1 冗長性）を設定でき、これにより、最大で 80,000 台のデバイスを使用できます。

また、顧客が単純に非ローカルの冗長性を備えた呼処理機能を必要としている場合に、Survivable Remote Site Telephony（SRST）を使用せずにメガクラスタを展開し、標準クラスタ展開で可能な最大 8 サイトを超えて、メガクラスタあたり最大 16 の Unified CM サブスクライバ ノードまで拡張できます。たとえば、12 のロケーションがある大きな病院で、各ロケーションに 1,000 台のデバイスしかないとします。この合計 12,000 というデバイス数だけでいうと、標準クラスタの最大デバイス キャパシティが 40,000 であるため、標準クラスタで提供できます。しかし、この場合で必要なのは、デバイス キャパシティの追加ではなく、Unified CM サブスクライバの追加です。これにはメガクラスタ配置が必要です。この例では、Unified CM サブスクライバ ノードは各ロケーションに配置され、各 Unified CM サブスクライバは、ローカル エンドポイントのプライマリ サブスクライバとして、また、別のロケーションのリモート エンドポイントのバックアップ サブスクライバとして動作できます。

メガクラスタ配置を検討する場合、キャパシティに影響を与える主な領域は次のとおりです。

- メガクラスタには、16 台のサブスクライバ ノード、2 台の TFTP サーバ ノード、2 台の保留音（MoH）サーバ ノード、および 1 台のパブリッシャ ノードで構成される合計 21 台のサーバ ノードを含めることができます。
- Unified CM は、7,500 人のユーザまたは 10,000 人のユーザ用の VM 構成オプションで展開する必要があります。
- 冗長性モデルは 1:1 である必要があります。

標準クラスタに関連する他のすべてのキャパシティがメガクラスタにも適用されます。メガクラスタ導入のサポートは、Cisco Collaboration Sizing Tool の結果の送信など、詳細設計の確認が成功した後でのみ与えられることに注意してください。Cisco Collaboration Sizing Tool および Unified CM 標準クラスタとメガクラスタのサイジングの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

メガクラスタ配置に関しては複雑な考慮事項が多数あるので、このような配置の実現を望むお客様は、シスコのアカウント チーム、シスコ アドバンスド サービス、または認定された Cisco Unified Communications パートナーに関与してもらう必要があります。

(注)　特に明記されていない限り、この SRND 内に含まれる呼処理配置に関連するすべての情報（キャパシティ、ハイ アベイラビリティ、一般的な設計上の考慮事項など）は、標準クラスタにのみ適用されます。

呼処理サイジングの詳細や、システム サイジング、キャパシティ プランニング、および配置の考慮事項に関する詳しい説明については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

Cisco Business Edition 4000 のキャパシティ プランニング

Cisco Business Edition 4000 は、最大で 200 のエンドポイントをサポートします。詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章および次の Web サイトにある Business Edition 4000 のドキュメントを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/business-edition-4000/index.html

Unified CME のキャパシティ プランニング

Unified CME を配置する場合、必要となるサポート対象エンドポイント数という観点で、目的に合ったキャパシティを提供する Cisco IOS ルータ プラットフォームを選択することが重要です。また、Unified CME ルータが、呼処理以外のサービス（IP ルーティング、DNS ルックアップ、Dynamic Host Configuration Protocol（DHCP）アドレス サービス、VXML スクリプトなど）を提供する場合は、プラットフォームのメモリ キャパシティも考慮する必要があります。

Unified CME は、単一の Cisco IOS プラットフォーム上で最大 450 エンドポイントをサポートできます。ただし、各ルータ プラットフォームのエンドポイントのキャパシティは、システムのサイズによって異なります。Unified CME は Cisco Collaboration Sizing Tool ではサポートされないため、次の Web サイトで入手可能な Unified CME の製品データ シートに記載されているキャパシティ情報に従う必要があります。

https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-express/datasheet-listing.html

呼処理の設計上の考慮事項

シスコの呼処理を配置する際は、次の設計上の推奨事項およびガイドラインに従ってください。

Cisco Unified CM

- Cisco Unified CM は、VMware Hypervisor 上で仮想化アプリケーションとしてのみ動作します。また、VMware Hypervisor を使用しない場合、ハードウェア プラットフォーム上で直接動作しません。
- Cisco Unified CM クラスタ内で最大 8 つの呼処理サブスクライバ ノード（Cisco CallManager サービスを実行するノード）を使用可能にできます。その他のサーバ ノードは、パブリッシャ、TFTP、およびメディア リソース サービス専用で使用できます。承認されたメガクラスタ配置は、最大で 16 個の呼処理サブスクライバ ノードをサポートします。

- 各 Unified CM クラスタは、最大 40,000 台のセキュアまたはセキュアでないエンドポイントの設定および登録をサポートできます。プラットフォームごとのサイジングの制限など、Unified CM のキャパシティ プランニングの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。
- ノードが 2 つのクラスタを配置する場合も、クラスタ内のユーザ数が 1,250 を超えないようにすることを推奨します。1,250 ユーザを超える場合は、専用パブリッシャと別個のノードをプライマリおよびバックアップの呼処理サブスクライバ用に推奨します。
- クラスタ内のすべてのノードで同じ VM 設定を使用することを推奨します。Unified CM の VM 設定を混在させることができますが、設計に影響と制限があります。詳細については、Unified CM の VM 設定の混在（9-8 ページ）の項を参照してください。
- 10,000 人のユーザ用の VM 構成オプションを使用する場合、バックアップ サブスクライバが過負荷の状態になることがあるので、2:1 冗長性はサポートされません。
- 仮想マシンのネットワーク トラフィックにハードウェア プラットフォームの複数の物理ポートを使用し、最低 2 台のアップストリーム スイッチを使用して、ネットワーク接続の冗長性を提供します。VMware vSphere 仮想スイッチを使用している場合は、VMware NIC チーミングを使用します。
- 可能な場合は常に、ハードウェア プラットフォームをネットワーク内の複数の物理スイッチおよび同じネットワーク内の複数の物理ロケーションに分散させて、スイッチの障害または特定のネットワーク ロケーションの損失による影響を最小限に抑えます。
- SRST または E-SRST をリモート ロケーションの Cisco IOS ルータに配置して、これらのロケーションで Unified CM クラスタへの接続が失われた場合にフォールバック呼処理サービスを提供します。
- Unified CM クラスタ内で音声アクティビティ検出（VAD）を使用不可にしておくことを推奨します。デフォルトでは、Unified CM サービス パラメータで VAD は使用不可になっています。Cisco IOS ゲートウェイで設定されている H.323 および SIP ダイヤル ピア上で使用不可にするには、**no vad** コマンドを使用してください。
- バックアップまたは冗長サブスクライバ ノードがプライマリ サブスクライバ ノードとは別の物理サーバ上に置かれるように、Unified CM ノードが異なる物理サーバに分散されていることを確認します。
- 低速の CPU を搭載したサーバは、サポートされる Open Virtualization Archive（OVA）VM 構成の点で制限される場合があります。そうしたサーバは「*制限された UC パフォーマンス*」CPU と呼ばれます。たとえば、Cisco Unified CM 1000 ユーザ OVA VM 構成はそうしたサーバにインストール可能なただ 1 つの Unified CM OVA VM 構成です。ただし、一部の小規模なサーバは小規模な VM 設定のみをサポートします。適切な VM 設定の選択と、Cisco Collaboration Sizing Tool の使い方の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。
- ハードウェア プラットフォームの USB ポートおよびシリアル ポートへのアクセスは、Unified CM 仮想マシンではサポートされていません。そのため、MoH 用の固定ライブ オーディオ ソースを接続すること、レガシー ボイスメール システムへのシリアル SMDI 接続を行うこと、またはログ ファイルの書き込みのために USB フラッシュ ドライブを接続することもできません。次の代替オプションを使用できます。
  - MoH ライブ オーディオ ソース フィードの場合は、ライブ オーディオ ソース接続に Cisco IOS ベースのマルチキャスト MoH を使用することを検討してください。
  - システムのインストール ログの保存には、仮想フロッピー ソフトメディアを使用します。
  - SMDI シリアル接続に対するサポートはありません。

- Cisco Business Edition 6000 では、Unified CM は単一の Unified CM パブリッシャ ノードとして展開され、呼処理も扱います。Unified CM の冗長性を提供するために、SRST を展開するか、Unified CM サブスクライバ ノードをホスティングする追加のハードウェア サーバを展開することができます。

（注）　BE6000 展開のために 2 台を超えるサーバをクラスタ化して、追加の冗長性や地理的な分散を提供することができます。ただし、キャパシティ制限は増加しません。たとえば、クラスタ全体のユーザの総数は、BE6000M または BE6000H では 1,000 を超えることはできません。

- 同じ配置で複数の Business Edition 6000 サーバが必要な場合は、複数の物理スイッチに分散します。
- 特にサーバに電源装置が 1 台しかない場合、可用性を最大限まで高めるために、無停電電源装置（UPS）を使用します。
- Business Edition 6000 をハイ アベイラビリティ用に 2 台のサーバで配置する場合は、1 つのサーバに障害が発生した場合にハイ アベイラビリティを提供するように、Unified CM ノードを各サーバで実行する必要があります。また、サブスクライバ ノードをプライマリ呼処理サーバとして、パブリッシャ ノードをバックアップ呼処理サーバとして Unified CM クラスタを設定することを推奨します。
- Cisco Business Edition 7000 では、Unified CM は企業（Cisco Business Edition の一部でない）Unified CM 展開と同じルール、キャパシティ、設計上の考慮事項を持ちます。
- Business Edition 6000 ソリューションの一部ではなく、別のハードウェアで実行されるアプリケーションを Business Edition 6000 展開に統合することができます。ただし、このアプリケーションが Business Edition 6000 のキャパシティ制限を超えないことを確認する必要があります。たとえば、全体の BHCA およびコンタクト センター エージェントの数は、Unified CM の Business Edition 6000 のキャパシティ制限を超えることはできません。Business Edition 6000 のキャパシティ制限の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。また、このアプリケーションが Business Edition 6000 によって提供されるシスコ コラボレーション VM 設定をサポートしていることを確認します。たとえば、Cisco Unified Contact Center Enterprise では Unified CM の 7.5k ユーザまたはより大規模な VM 設定が必要なため、Business Edition 6000 で実行される Unified CM 展開と統合することはできません。

Cisco Unified CME

- Unified CME は、最大で 450 のエンドポイントをサポートします。ただし、Cisco IOS ルータ モデルによっては、エンドポイント キャパシティは大幅に低下する場合があります。Unified CME のプラットフォームおよびキャパシティの詳細については、次の Web サイトにある Cisco Unified Communications Manager Express の互換性情報を参照してください。https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/products-device-support-tables-list.html。
- 可能な場合は、複数の IP インターフェイスを使用して Unified CME ルータをネットワークに二重接続し、ネットワークの可用性を最大限まで高めます。同様に、同じ配置で Unified CME の複数のインスタンスが必要な場合は、複数の物理スイッチまたはロケーションに分散します。
- 可能な場合は、二重化電源および無停電電源（UPS）を備えた Unified CME ルータを配置し、プラットフォームの可用性を最大限まで高めます。

コンピュータ テレフォニー インテグレーション(CTI)

Cisco コンピュータ テレフォニー インテグレーション(CTI)を利用すると、Cisco Unified CM で使用可能な豊富なフィーチャ セットだけでなく、サードパーティ製のアプリケーションも使用できるようになります。CTI 対応アプリケーションによって、ユーザの生産性が向上し、コミュニケーションが活発になるとともに、高品質なカスタマー サービスを提供できるようになります。Cisco CTI を使用すると、サードパーティ製デスクトップ アプリケーションで Microsoft Outlook 内から通話を行ったり、着信コールの発信者 ID に基づいてウィンドウを開いたり、アプリケーションを起動したりできます。また、課金のためにコールと連絡先をリモートで追跡することもできます。Cisco CTI 対応のサーバ アプリケーションでは、企業ネットワーク全体での適切な対応先のルーティングや、自動応答や音声自動応答装置(IVR)などの自動発信者サービスの提供に加えて、対応先の記録および分析に役立つメディアの取り込みも行えます。

CTI アプリケーションは一般に、次の 2 つの主なカテゴリに分類できます。

- ファーストパーティ製のアプリケーション:モニタ、制御、メディア ターミネーション

  ファーストパーティ製の CTI アプリケーションは、コールのセットアップ、終了、およびメディア ターミネーション用の CTI ポートおよびルート ポイントなどのデバイスを登録するように設計されています。これらのアプリケーションはメディア パスに直接配置されているので、インバンド DTMF などのメディア レイヤのイベントに応答できます。ファーストパーティ製の CTI アプリケーションには音声自動応答装置や Cisco Attendant Console などがあり、これらのアプリケーションはコールをモニタおよび制御しながら、コール メディアとも対話します。

- サードパーティ製のアプリケーション:モニタおよび制御

  サードパーティ製の CTI アプリケーションもコールをモニタおよび制御しますが、メディア ターミネーションは直接制御しません。

  - モニタリング アプリケーション

    Cisco IP デバイスの状態をモニタする CTI アプリケーションは、モニタリング アプリケーションと呼ばれます。オンフックまたはオフフックのステータスを表示する、またはその情報を使用してユーザの可用性をプレゼンスの形式で示すビジーランプフィールド アプリケーションは、どちらもサードパーティ製の CTI モニタリング アプリケーションの例です。

  - 呼制御アプリケーション

    Cisco CTI を使用して、アウトバンド シグナリングを使用する Cisco IP デバイスをリモート制御するアプリケーションは、呼制御アプリケーションです。Cisco IP デバイスをリモート制御するように設定された Cisco Jabber は、呼制御アプリケーションのよい例です。

  - モニタリング + 呼制御アプリケーション

    これらは、Cisco IP デバイスをモニタおよび制御するすべての CTI アプリケーションです。Cisco Unified Contact Center Enterprise は、エージェントのステータスをモニタして、エージェント デスクトップを介してエージェント電話機を制御するため、モニタと制御を兼ね備えたアプリケーションのよい例です。

(注) ここでモニタリング アプリケーション、呼制御アプリケーション、モニタリング + 呼制御アプリケーションの違いを列挙しましたが、この細かな違いはアプリケーション開発者には見えないようになっています。Cisco CTI を使用するすべての CTI アプリケーションは、モニタリングおよび制御の両方に有効です。

次のデバイスは CTI 経由でモニタまたは制御できます。

- CTI ルート ポイント
- CTI ポート
- CTI をサポートする Cisco Unified IP Phone
- CTI リモートデバイス

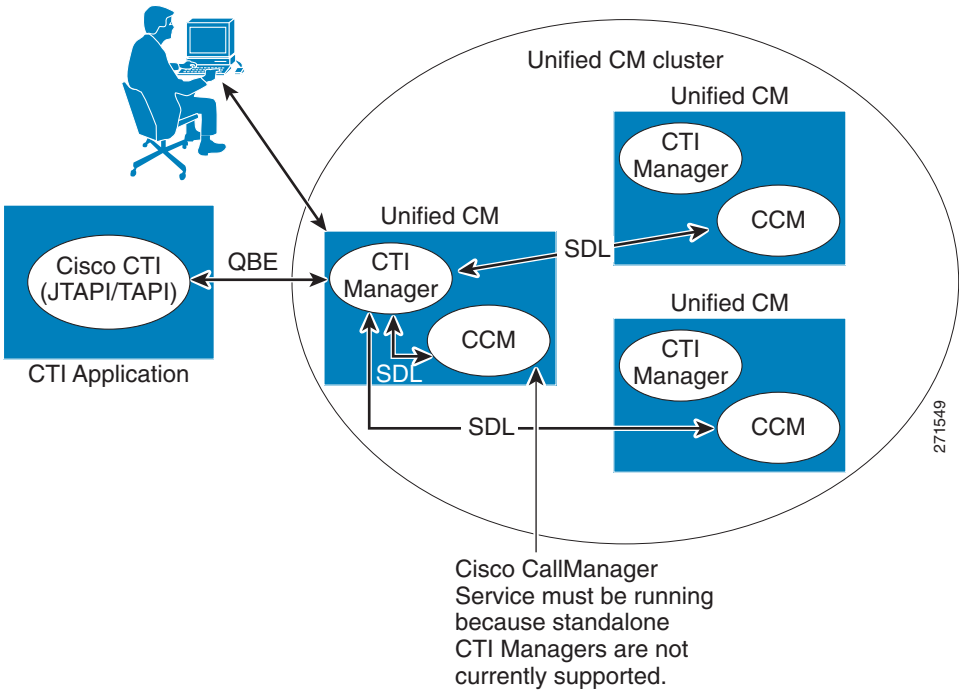
CTI リモート デバイスにより、従来の PSTN 電話機、携帯電話、サードパーティ電話、または サードパーティ PBX に接続されている電話機などの、CTI をサポートしない電話機上のモニタリング機能および制限された呼制御機能を CTI アプリケーションが持つことができるようになります。

CTI のアーキテクチャ

Cisco CTI は、次のコンポーネントで構成されます(図 9-9 を参照)。これらは互いに対話し、Cisco Unified CM で使用可能なテレフォニーフィーチャ セットを各アプリケーションで利用できるようにします。

- CTI 対応アプリケーション:特定のテレフォニー機能を提供するために作成されたシスコ製またはサードパーティ製のアプリケーション。
- JTAPI および TAPI:Cisco CTI でサポートされる 2 つの標準インターフェイス。開発者は、好みの方式のライブラリを使用してアプリケーションを作成できます。
- Unified JTAPI および Unified TSP クライアント:外部メッセージを Cisco Unified CM で使用される内部の Quick Buffer Encoding(QBE)メッセージに変換します。
- Quick Buffer Encoding(QBE):Unified CM の内部通信メッセージ。
- プロバイダー:アプリケーションと CTI Manager との接続の論理的な表現であり、通信を容易にするために使用されます。プロバイダーは、アプリケーションにデバイス イベントおよびコール イベントを送付しながら、アプリケーションによるデバイスのリモート制御を可能にする制御命令を受け付けます。
- Signaling Distribution Layer(SDL):Unified CM の内部通信メッセージ。
- パブリッシャおよびサブスクライバ:Cisco Unified Communications Manager(Unified CM)サーバ ノード。
- CCM:Cisco CallManager サービス(ccm.exe)。テレフォニー処理エンジンです。
- CTI Manager(CTIM):プライマリまたはセカンダリ モードで動作する 1 つ以上の Unified CM サブスクライバで実行され、Cisco IP デバイスを制御およびモニタできるようにテレフォニー アプリケーションを認証および許可するサービス。

図 9-9　　Cisco CTI のアーキテクチャ



アプリケーションを認証および許可すると、CTIM は、テレフォニー アプリケーションと Cisco CallManager サービスの仲介者として機能します(このサービスは呼制御エージェントです。全体の製品名である Cisco Unified Communications Manager と混同しないようにしてください)。CTIM はテレフォニー アプリケーションからの要求に応答し、Unified CM システムで内部的に使用される Signaling Distribution Layer(SDL)メッセージに変換します。Cisco CallManager サービスからのメッセージも CTIM によって受信され、処理のために適切なテレフォニー アプリケーションに転送されます。

CTIM は、Cisco CallManager サービスがアクティブになっているクラスタ内の Unified CM サブスクライバ ノードでアクティブにできます。これによって、Unified CM クラスタ内で 8 つまでの CTIM をアクティブにできます。スタンドアロンの CTIM は現在サポートされていません。

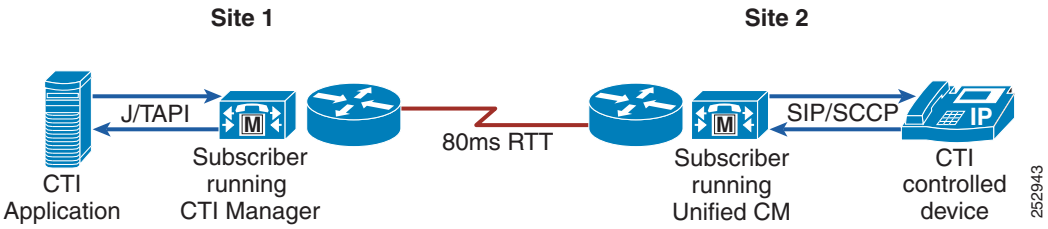
WAN を介した CTI アプリケーションおよびクラスタリング

WAN を介したクラスタリングを採用した配置では、次の 2 つのシナリオがサポートされます。

- WAN を介した CTI Manager(図 9-10 を参照)

  このシナリオでは、CTI アプリケーションとそれに関連付けられた CTI Manager が WAN の一方の側(サイト 1)に配置され、Unified CM サブスクライバに登録されるモニタおよび制御対象のデバイスが他方の側(サイト 2)に配置されます。WAN を介したクラスタリングのラウンドトリップ時間(RTT)は、現在サポートされている限度値 80 ms を超えることはできません。CTI トラフィックに必要な帯域幅を計算するには、ローカル フェールオーバー配置モデル(10-50 ページ)にある公式を使用します。この帯域幅は、ローカル フェールオーバー配置モデル(10-50 ページ)の説明に従って計算した Intra-Cluster Communication Signaling (ICCS)帯域幅や、音声に必要な帯域幅(RTP トラフィック)とは別に必要であることに注意してください。

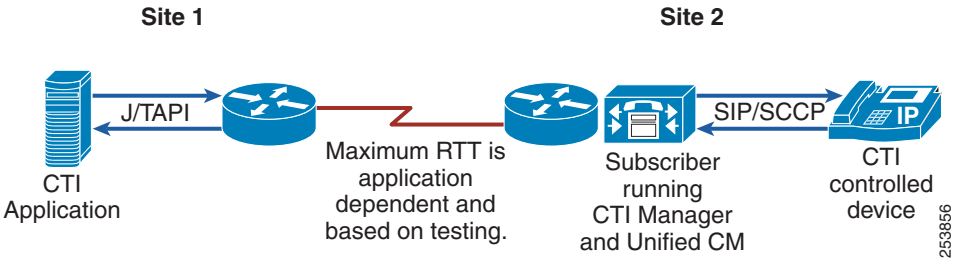
図 9-10　WAN を介した CTI



- WAN を介した TAPI および JTAPI アプリケーション(WAN を介した CTI アプリケーション)(図 9-11 を参照)

  このシナリオでは、CTI アプリケーションが WAN の一方の側(サイト 1)に配置され、関連付けられた CTI Manager が他方の側(サイト 2)に配置されます。このシナリオでは、CTI アプリケーション開発者またはプロバイダーの責任において、アプリケーションが実装された RTT に適応できるかどうかを確認します。場合によっては、アプリケーションが CTI Manager と同じ場所にある場合よりも、フェールオーバー時間およびフェールバック時間が長くなることがあります。このような場合、アプリケーション開発者またはプロバイダーは、そのような状況におけるアプリケーションの動作に関するガイダンスを示す必要があります。

図 9-11　WAN を介した JTAPI



(注)　WAN を介した TAPI および JTAPI のサポートは、アプリケーションに依存します。ユーザとアプリケーション開発者またはプロバイダーの両者が、使用するアプリケーションに WAN を介したクラスタリングが含まれる配置との互換性があることを確認する必要があります。

CTI のキャパシティ プランニング

サポートされている CTI 制御デバイスの最大数は、クラスタごとに 40,000 です。プラットフォームごとのノードおよびクラスタの CTI キャパシティや、CTI リソースの計算式および例など、CTI のキャパシティ プランニングの詳細については、コラボレーション ソリューション サイジング ガイダンス(25-1 ページ)の章を参照してください。

CTI のハイ アベイラビリティ

ここでは、ハイ アベイラビリティのための CTI プロビジョニングについて、いくつかのガイドラインを提供します。

CTI Manager

CTI Manager は、Unified CM クラスタ内の少なくとも 1 つ(おそらくすべて)の呼処理サブスクライバで有効にする必要があります。クライアント側のインターフェイス(TAPI TSP または JTAPI クライアント)では IP アドレスを 2 つずつ使用できます。これらの IP アドレスは、CTIM サービスを実行している Unified CM サーバ ノードを指します。CTI アプリケーションの冗長性を確保するため、図 9-12 のとおり、クラスタの少なくとも 2 つの Unified CM サーバ ノードで、CTIM サービスをアクティブにすることを推奨します。

冗長性、フェールオーバー、およびロード バランシング

冗長性が必要な CTI アプリケーションでは、TAPI TSP または JTAPI クライアントは 2 つの IP アドレスで設定できるため、障害発生時には代替の CTI Manager を使用できます。ここで注意すべきは、2 つの CTI Manager 間で情報が共有されていないため、この冗長性はステートフルではありません。そのため、フェールオーバーの際に、再初期化が必要になることがあります。

CTI Manager がフェールオーバーした場合、必要な処理は、現在アクティブになっている CTI Manager で CTI アプリケーションのログイン プロセスをやり直すことだけです。ただし、Unified CM サーバ ノード自体に障害が発生した場合は、障害が発生した Unified CM や現在アクティブになっている Unified CM などのすべてのデバイスを再登録し、その後で CTI アプリケーションのログイン プロセスを実行する必要があるため、再初期化プロセスは時間がかかります。

ロード バランシングが必要な CTI アプリケーションや、この設定を利用できる CTI アプリケーションは、図 9-12 に示すように、2 つの CTI Manager に同時に接続できます。

図 9-12　　冗長性とロードバランシング

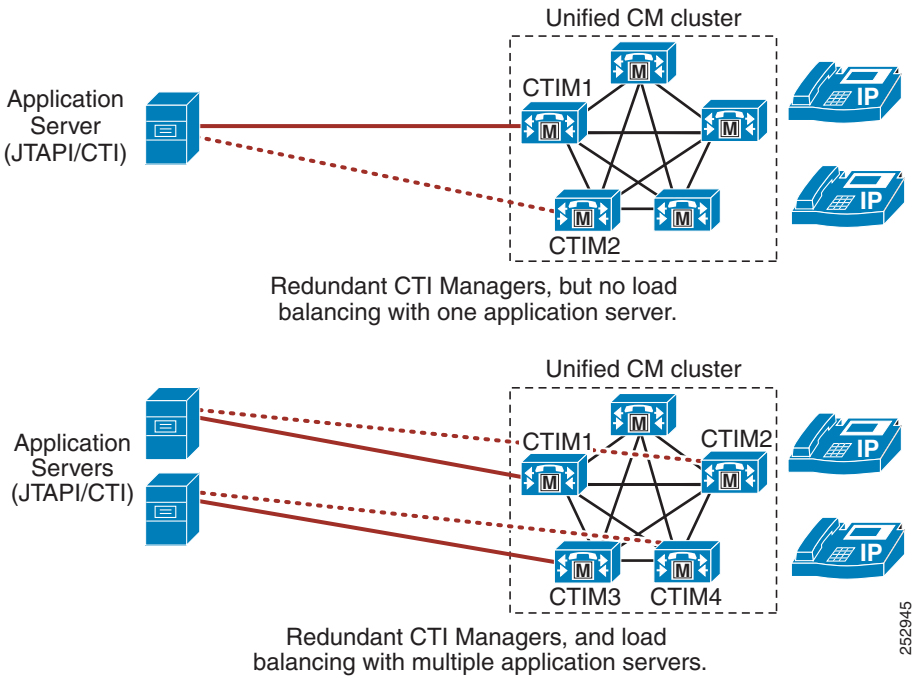


図 9-13 は、このタイプの Cisco Unified Contact Center Enterprise（Unified CCE）の設定例を示しています。このタイプの設定には、次の特性があります。

- Unified CCE は冗長性のために 2 つのペリフェラル ゲートウェイ（PG）を使用します。
- 各 PG は異なる CTI Manager にログインします。
- 一度に 1 つの PG しかアクティブになりません。

図 9-13　Cisco Unified Contact Center Enterprise での CTI の冗長性

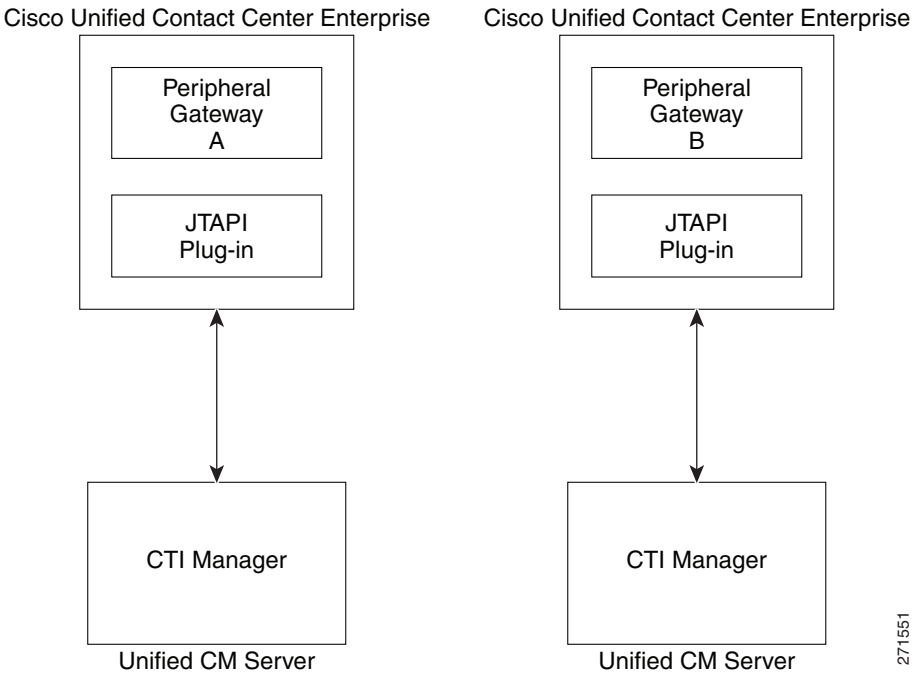
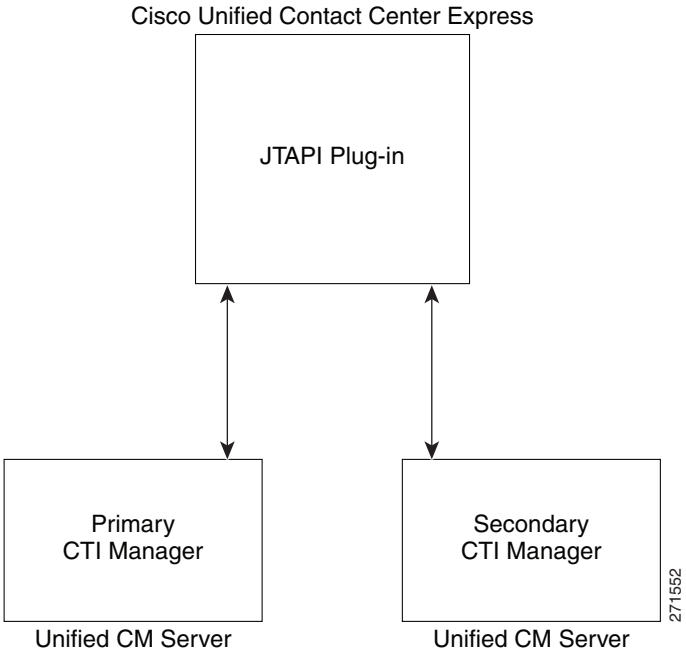


図 9-14 は、このタイプの Cisco Unified Contact Center Express（Unified CCX）の設定例を示しています。このタイプの設定には、次の特性があります。

- Unified CCX では、各 CTI Manager 用に 1 つずつ、合計で 2 つの IP アドレスを設定できます。
- プライマリ CTI Manager への接続が失われた場合、Unified CCX はセカンダリ CTI Manager にフェールオーバーします。

図 9-14　Cisco Unified Contact Center Express での CTI の冗長性



実装

アプリケーションの作成に関するガイダンスとサポートについて、アプリケーション開発者は次の Web サイトの Cisco Developer Network（DevNet）で相談してください。

https://developer.cisco.com/site/devnet/home

複数の呼処理エージェントの統合

複数の Unified CM クラスタを 1 つに統合するか、Cisco TelePresence Video Communication Server（VCS）と Unified CM クラスタを統合するには、Cisco Unified CM Session Management Edition（SME）を使用します。SME は、マルチサイト分散型呼処理配置で推奨されるトランクとダイヤルプランの集約プラットフォームです。SME は基本的に、トランク インターフェイスだけを使用し、IP エンドポイントを使用しない Unified CM クラスタです。このクラスタには、リーフシステムと呼ばれる、複数のユニファイド コミュニケーション システムを集約できます。

また、Unified CM Session Management Edition を使用して、PSTN 接続、PBX、集中型のユニファイド コミュニケーション アプリケーションなど、サードパーティのユニファイド コミュニケーション システムに接続できます。

SME の詳細については、Unified CM Session Management Edition（10-28 ページ）の項を参照してください。

複数の呼処理エージェントの直接的統合も可能です。この項では、SIP トランキング プロトコルを使用している Cisco Unified CM と Cisco Unified Communications Manager Express（Unified CME）に関して、マルチサイト IP テレフォニー配置における相互運用性およびインターネットワーキングの要件について説明します。ここでは、Unified CM の制御する電話機と Unified CME の制御する電話機との間での推奨する配置を中心に説明します。

この項では、次の項目について説明します。

- Unified CM と Unified CME 間の相互運用性の概要（9-37 ページ）
- 分散型呼処理を使用したマルチサイト配置における SIP 経由の Unified CM と Unified CME の相互運用性（9-38 ページ）

Cisco Unified CM および Cisco Unified Communications Manager Express（Unified CME）は、H.323 を使用して統合することもできますが、ここではこの統合について詳しく説明しません。H.323 統合の詳細については、次の Web サイトで入手可能な『*Cisco Collaboration 9.x SRND*』を参照してください。

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

Unified CM と Unified CME 間の相互運用性の概要

H.323 または SIP をトランキング プロトコルとして使用して、Unified CM と Unified CME を相互接続できます。本社または中央サイトに Unified CM を配置して、支店の Unified CME システムと連携させる場合、ネットワーク管理者は、プロトコルの仕様と WAN トランク全体でサポートされる機能を慎重に検討して、SIP または H.323 のいずれかのプロトコルを選択する必要があります。以前は、H.323 トランクを使用して Unified CM と Unified CME を接続する方法が主流でしたが、SIP 電話機と SIP トランクのより高度な機能が Unified CM と Unified CME に追加されたことで、この状況は変わりました。この項ではまず、Unified CM と Unified CME の相互運用性のトランキング プロトコルとは無関係のいくつかの機能について説明し、次に SIP トランクを使用するための最も一般的な設計シナリオとベスト プラクティスを紹介します。

コール タイプとコール フロー

一般に、Unified CM と Unified CME のインターワーキングを使用すると、SIP トランクまたは H.323 トランク全体で、SCCP IP Phone から SIP IP Phone へのコール、またはその逆のコールをすべて組み合わせることができます。コールは、Unified CM と Unified CME SIP 間、または SCCP IP Phone との間で、転送（ブラインドまたは打診）または自動転送できます。

H.323 トランク経由で Unified CM に接続していると、Unified CME は Unified CM のコールを自動検出できます。Unified CME を終端とするコールが転送または自動転送されると、Unified CME はコールを再生成し、ヘアピン コールによって他の Unified CME または Unified CM に適切にコールをルーティングします。Unified CME は必要に応じて、SIP トランクまたは H.323 トランク全体の VoIP コールについて、Unified CM からのコール レッグをヘアピンします。H.450 以外でサポートされる Unified CM ネットワークで自動検出を可能にする方法と、H450.2、H450.3、または SIP の付加サービスを有効または無効にする方法の詳細については、次の Web サイトで入手可能な Unified CME の製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/tsd-products-support-series-home.html

SIP トランク経由で Unified CM に接続すると、Unified CME は Unified CM のコールを自動検出しません。デフォルトでは、Unified CME は常に、コール転送の SIP Refer メッセージまたは自動転送の SIP 302 Moved Temporarily メッセージを使用して、コールをリダイレクトしようとします。リダイレクトが失敗すると、Unified CME はヘアピン コールを試みます。

保留音

Unified CM では G.711 形式と G.729 形式の両方で MoH ストリームを有効にできますが、Unified CME で MoH をストリームできるのは G.711 形式のみです。そのため、保留になったコールの MoH オーディオを Unified CME で制御する場合は、G.711 MoH ストリームと G.729 コールレッグの間でトランスコーディングするためのトランスコーダが必要です。

インスタントおよびパーマネント ハードウェア会議

インスタント会議とパーマネント会議の両方に、ハードウェアの DSP リソースが必要です。SIP、H.323、PSTN のいずれを経由して接続している場合でも、Unified CM 電話機と Unified CME 電話機は、ネットワークから到達できる限り、インスタント会議に招待または追加されて、会議の参加者になることができます。アクティブな会議のセッション中にコールを保留にしても、その会議のセッションの参加者には音楽は聞こえません。

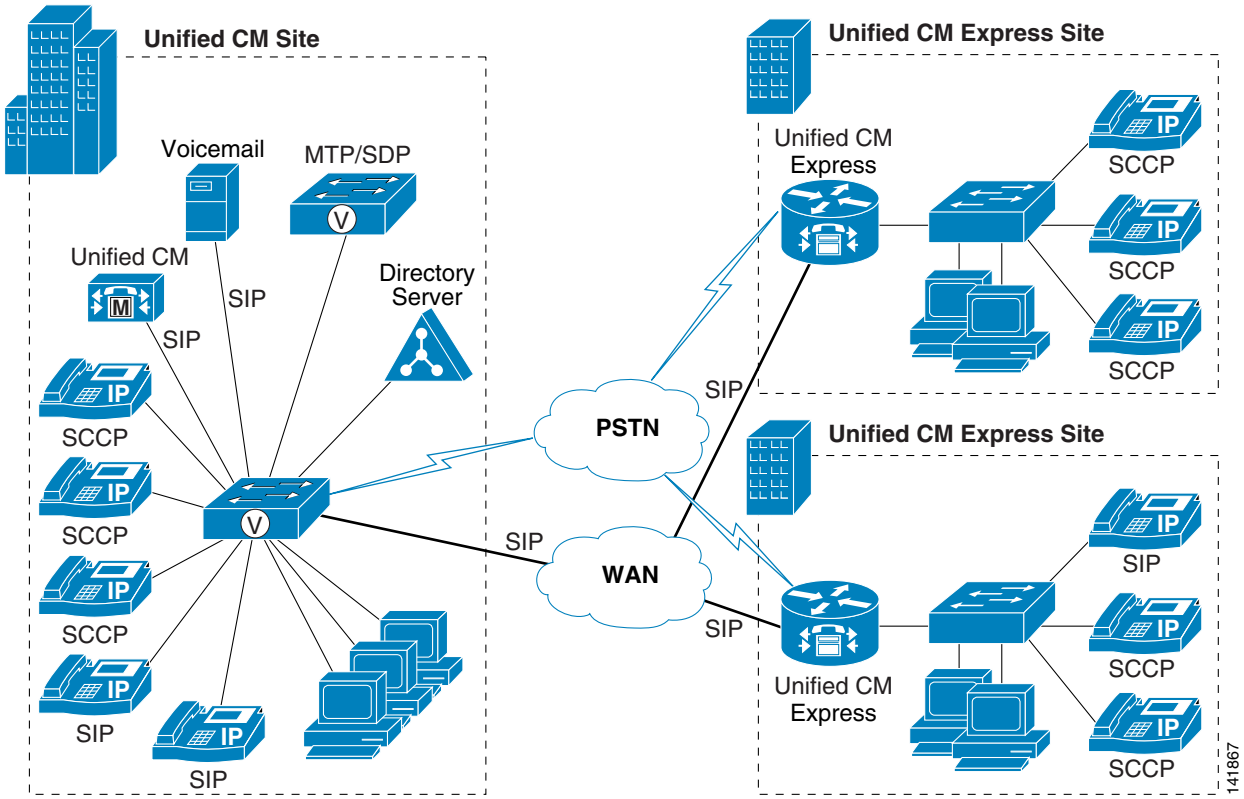
インスタント会議とパーマネント会議に必要でサポートされる DSP リソースと、会議に参加できる最大人数については、次の Web サイトで入手可能な Unified CME の製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/tsd-products-support-series-home.html

分散型呼処理を使用したマルチサイト配置における SIP 経由の Unified CM と Unified CME の相互運用性

Unified CM は、SIP インターフェイスを使用する Unified CME と直接通信できます。図 9-15 に、SIP トランクを使用して Unified CM が Cisco Unified CME と直接ネットワーク接続されている Cisco Unified Communications マルチサイト配置を示します。

図 9-15　SIP トランクを使用して Unified CM と Unified CME を接続したマルチサイト配置



ベスト プラクティス

図 9-15 に示した配置モデルを使用する場合は、次のガイドラインに従い、ベスト プラクティスを参考にしてください。

- [Accept Replaces Header] を選択した SIP トランク セキュリティ プロファイルを設定します。
- 作成した SIP トランク セキュリティ プロファイルを使用して SIP トランクを Unified CM 上に設定し、再ルーティング CSS も指定します。再ルーティング CSS は、どこで SIP ユーザ（転送者）が別のユーザ（被転送者）を第三者ユーザ（転送先）に振り向けることができるか、および SIP 302 Redirection Response と Replaces を持つ INVITE を使用して SIP ユーザがどの機能を呼び出せるかを決定するために使用します。
- SIP トランクの場合、Unified CME 上で SCCP エンドポイントを使用しているときに、メディア ターミネーション ポイント（MTP）を使用可能にする必要はありません。ただし、Unified CME 上に SIP エンドポイントがある場合は、メディア ターミネーション ポイントを Unified CM 上で使用して、SIP プロトコルでディレイド オファー/アンサー交換の処理（セッション記述プロトコルなしの INVITE 受信）ができるようにする必要があります。
- Unified CM ダイヤル プラン設定（ルート パターン、ルート リスト、ルート グループ）を使用して、SIP トランク経由で Unified CME にコールをルーティングします。
- Unified CM のデバイス プールとリージョンを使用して、サイト内では G.711 コーデックを設定し、リモートの Unified CME サイトに対しては G.729 コーデックを設定します。

- Unified CME の **voice services voip** で **allow-connections sip to sip** コマンドを設定して、SIP-to-SIP コール接続を許可します。
- SIP エンドポイントの場合は、**voice register global** で **mode cme** コマンドを設定し、Unified CME の SIP 電話機ごとに **voice register pool** コマンドで **dtmf-relay rtp-nte** を設定します。
- SCCP エンドポイントの場合は、Unified CME の **telephony-service** で **transfer-system full-consult** コマンドと **transfer-pattern .T** コマンドを設定します。
- Unified CME の **session protocol sipv2** および **dtmf-relay [sip-notify | rtp-nte]** により、SIP WAN インターフェイスの voip ダイヤル ピアを設定し、Unified CM を宛先としてコールを転送またはリダイレクトします。

設計上の考慮事項

この項ではまず、一部の主要な領域における SIP 経由での Unified CM と Unified CME の相互運用性に関するいくつかの特徴と設計上の考慮事項について説明します。主要な領域には、コール転送や自動転送のための付加サービス、スピード ダイヤル ボタンや電話帳のコール リストの Busy Lamp Field（BLF）通知のためのプレゼンス サービス、パートナー アプリケーションとの統合や、Unified CM 電話機と Unified CME 電話機間のクリックダイヤルに対するサードパーティ製電話による制御のための Out-Of-Dialog Refer（OOD-Refer）などが含まれます。この項では、SIP 経由での Unified CM と Unified CME の相互運用性に関する設計上の一般的な考慮事項についても説明します。

付加サービス

SIP Refer メッセージや SIP 302 Moved Temporarily メッセージを Unified CME または Unified CM でのコール転送や自動転送などの付加サービスに使用して、転送先または自動転送先に対して新しいコールを開始するよう、被転送者または自動転送される電話機（被転送者）に指示できます。SIP Refer メッセージまたは SIP 302 Moved Temporarily メッセージがサポートされている場合、コール転送や自動転送のシナリオにはヘアピンは不要です。

ただし、DID マッピングがない内線が存在する場合や、Unified CM または Unified CME に、SIP 302 Moved Temporarily メッセージの DID にコールをルーティングするダイヤル プランがない場合は、**supplementary-service** を無効にする必要があります。**supplementary-service** が無効になっていると、Unified CME はコールをヘアピンするか、re-INVITE の SIP メッセージを Unified CM に送信して、新しい着信者 ID へメディア パスを置き換えます。それ以降のコール転送に複数の Unified CME が関係する場合でも、シグナリングとメディアの両方がヘアピンされます。転送されたコールでも、**supplementary-service** は無効にできます。この場合、SIP Refer メッセージは Unified CM に送信されませんが、被転送者と転送先がヘアピンされます。

（注）　付加サービスを無効にするには、**voice service voip** または **dial-peer voice xxxx voip** で **no supplementary-service sip moved-temporarily** コマンドか **no supplementary-service sip refer** コマンドを実行します。

次の例は、付加サービスが無効になっているときのコール フローを示しています。

- Unified CM の電話機 B が Unified CME の電話機 A にコールします。電話機 A は電話機 C（Unified CM 電話機、同一または異なる Unified CME 上にある Unified CME 電話機、PSTN 電話機のいずれか）に自動転送（[Forward All]、[Forward Busy]、[Forward No Answer]）するように設定されています。

  Unified CME は Unified CM に SIP 302 Moved Temporarily メッセージを送信しませんが、Unified CM 電話機 B と電話機 C の間でコールをヘアピンします。

- Unified CM の電話機 B が Unified CME の電話機 A にコールします。電話機 A はコールを電話機 C（Unified CM 電話機、Unified CME 電話機、PSTN 電話機のいずれか）に転送します。

  Unified CME は Unified CM に SIP Refer メッセージを送信しませんが、Unified CM 電話機 B と電話機 C の間でコールをヘアピンします。

SIP 経由での Unified CM と Unified CME の相互運用性に関する設計上の一般的な考慮事項

- SIP 302 Moved Temporarily メッセージまたは SIP Refer メッセージが Unified CM でサポートされていない場合は、**supplementary-service** を無効にします。無効にしないと、Unified CM はコールを転送先または自動転送先にルーティングできません。
- SIP-to-SIP コール シナリオでは、Refer メッセージがデフォルトで転送者から被転送者に送信され、被転送者は転送先への新しいコールをセットアップします。コールが転送先につながるまで、転送者にはデフォルトでリングバック トーンが聞こえます。Unified CME の **supplementary-service** が無効になっている場合、Unified CME は、被転送者と転送先の間でコールが接続されるとすぐにインバンドのリングバック トーンを提供します。
- プレゼンス サービスは、SIP トランク経由の Unified CM と Unified CME でのみサポートされます。
- OOD-Refer 機能を使用すると、サードパーティ製アプリケーションで SIP REFER メソッドを使用して、Unified CM または Unified CME の 2 つのエンドポイントを接続できます。OOD-Refer を使用する場合は、次の点を考慮してください。
  - Unified CM と Unified CME はどちらも、OOD-Refer 機能が有効になるよう設定する必要があります。
  - 保留、転送、および会議は、OOD-Refer トランザクション中はサポートされませんが、Unified CME によってブロックされることもありません。
  - コール転送がサポートされるのは、OOD-Refer コールが接続状態になった後のみで、コールの接続前はサポートされません。そのため、接続前はコールの transfer-at-alert はサポートされません。
- TLS のシグナリング制御はサポートされますが、SRTP は SIP トランク経由ではサポートされません。
- SIP トランク経由の SRTP は、Unified CM 用 Cisco IOS のゲートウェイ機能です。SRTP サポートは、SIP トランク経由での Unified CM と Unified CME のインターワーキングでは使用できません。

（注） 複数の PSTN 接続（Unified CM に 1 つと Unified CME に 1 つ）が存在する場合、PSTN エンドポイントに対する Unified CM エンドポイントと Unified CME エンドポイント間の完全在席転送は失敗します。複数の PSTN 接続を使用する場合にはブラインド転送の使用を推奨し、この設定は **telephony-service** で **transfer-system full-blind** として行います。

コラボレーションの配置モデル

改訂日：2018 年 3 月 1 日

この章では、Cisco Collaboration システムの配置モデルについて説明します。

この章の旧版では、Cisco Unified Communications Manager（Unified CM）向けの呼処理配置モデルのみに基づいて、配置モデルを説明しました。この章の最新版では、単なる呼処理サービスではなく多くの機能を備えた Cisco Unified Communications および Cisco Collaboration システム全体の設計ガイドラインを提供します。

以前のリリースの Cisco Unified Communications での設計ガイドラインについては、次の Web サイトで入手可能な Cisco Unified Communications ソリューション リファレンス ネットワーク デザイン（SRND）のマニュアルを参照してください。

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

この章の変更点

表 10-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 10-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
マイナー アップデートと修正	この章の各項で説明	2018 年 3 月 1 日

Unified Communications および Collaboration の配置

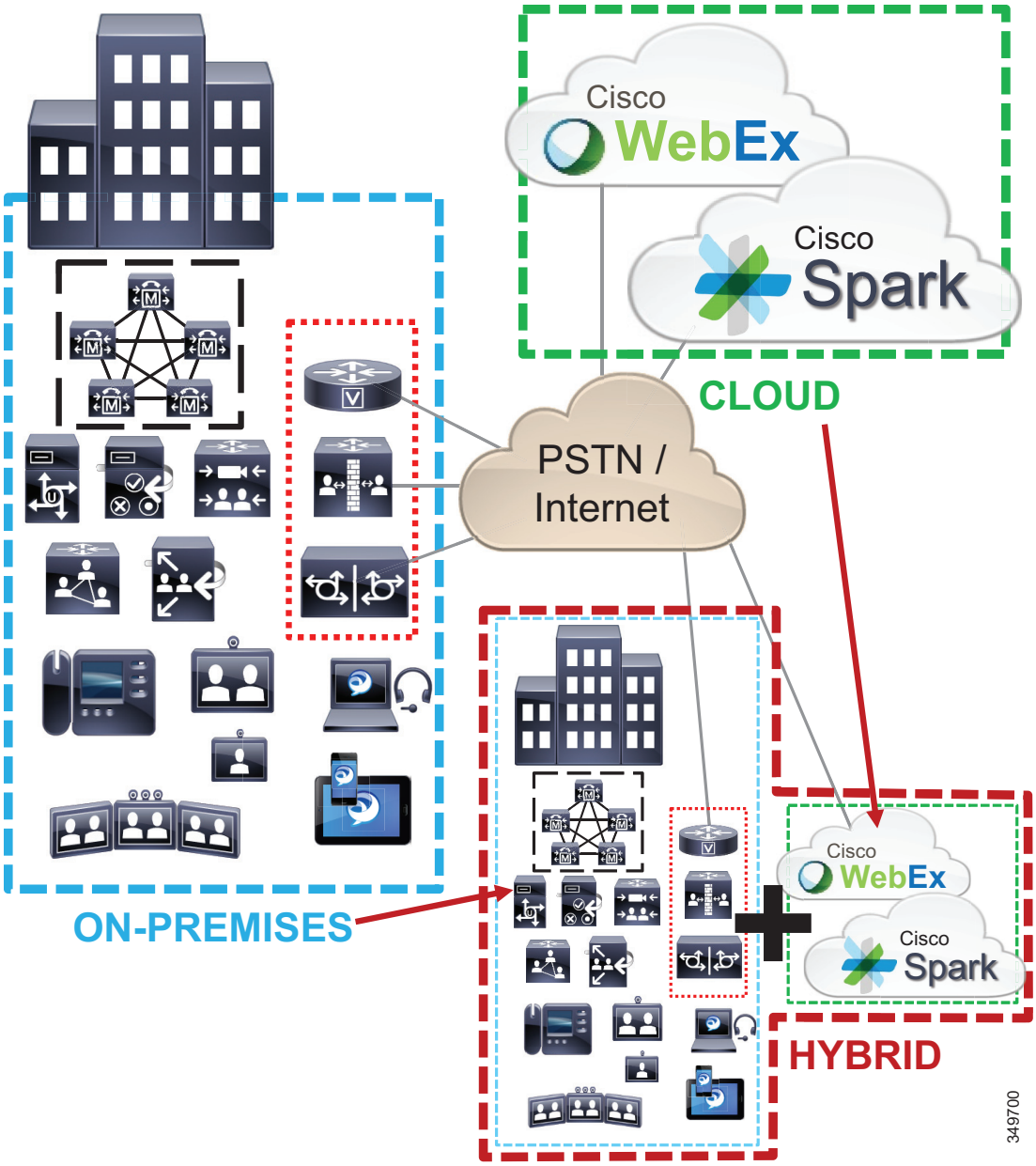
今から 15 年以上前に初めて Voice over IP（VoIP）と IP テレフォニーが公開されてから、現在の Unified Communications および Collaboration に至るまで、ユーザは多様な機能を備えたさまざまなデバイスを駆使して、いろいろな方法でコミュニケーションを図ることができるようになりました。現在、Unified Communications および Collaboration システムは、IM and Presence 向け Jabber クライアントのみの導入から開始し、必要に応じて段階的に音声、ビデオ、Web 会議、モバイル ボイス アプリケーション、ソーシャル メディア、ビデオ会議とテレプレゼンスを追加できます。Unified Communications ユーザ単位で使用可能なデバイスの数と、コミュニケーションの形態が増加するにつれ、Unified Communications アーキテクチャを緊密に統合する必要が生じました。シスコの Unified Communications および Collaboration アーキテクチャは、急速に変化し拡大を続ける Unified Communications 環境の要件に対応できる柔軟性とスケーラビリティを備えています。Unified Communications 環境では、複数の Unified Communications デバイスを持つユーザを通信の形式に関係なく単一のユーザ名で識別したいと考えるため、より URI が中心となってきています。

企業のコラボレーションの配置

従来、企業のコラボレーションと Unified Communications（UC）の配置では、アプリケーションおよびサービスは、企業ネットワーク境界内かオンプレミスで提供されてきました。近年では、コラボレーションおよび UC のサービスは、「サービスとして（aaS）」パラダイム（Collaboration as a Service、Communication Platform as a Service、UC as a Service など）を使用してクラウドから提供されるようになり、企業は、1 つ以上のサービスをクラウドで利用できます。オンプレミス サービスの利点（既存の投資、高品質の音声とビデオの通話など）とクラウド サービスの利点（継続的な配信、モバイルおよび Web 配信など）の両方が必要な企業は、ほとんどの場合、オンプレミスとクラウドベースのコラボレーション アプリケーションおよびサービスを組み合わせたハイブリッド配置を実装しています。

図 10-1 に示すように、コラボレーション アプリケーションおよびサービスの提供形態は、オンプレミスのみ、クラウドのみ、または、ますます一般的になっているハイブリッド サービス配置セット、という 3 形態のいずれかになる場合があります。

図 10-1　エンタープライズ コラボレーションの配置：オンプレミス、クラウド、ハイブリッド



たとえば、オンプレミス配置では、コラボレーション アプリケーションは企業の事業所内に配置されて、音声やビデオのコール、テキスト、音声、およびビデオのメッセージング、プレゼンス、ビデオ会議、デスク共有、画面共有、およびコンテンツ共有のサービスが提供されます。アプリケーションおよびサービスには、次が含まれます。

- Unified CM
- Unified CM - IM and Presence
- Unity Connection
- Cisco Meeting Server and TelePresence Management Suite（TMS）

クラウド配置の場合、クラウドから提供されるコラボレーション サービスには、音声やビデオのコール、メッセージング、ビデオ会議、コンテンツ共有や画面共有などがあります。クラウドから提供されるサービスには、次のものがあります。

- Cisco Spark のメッセージ、会議、コール：Cisco Spark 1:1 およびチーム メッセージング。モバイル、Web、およびデスクトップ プラットフォームすべてにわたる音声会議、ビデオ会議、Web 会議、音声およびビデオ コール
- WebEx での会議およびメッセージング：WebEx Messenger および WebEx Meetings（モバイル、Web、およびデスクトップ。Collaboration Meeting Rooms（CMR）など）

Cisco WebEx の詳細については、https://help.webex.com/welcome で入手可能なマニュアルを参照してください。Cisco Spark の詳細については、https://support.ciscospark.com/ で入手可能なマニュアルを参照してください。

コラボレーションに関するその他のクラウド実装として、従来型のオンプレミスのコラボレーション アプリケーションおよびサービスをクラウドから提供するサードパーティ管理型サービス プロバイダーおよびインテグレータにより提供されるコラボレーション プラットフォーム ベースのサービスなどがあります。このタイプのクラウド プラットフォームベース サービスの例としては、Cisco Hosted Collaboration Solution（HCS）があります。

Cisco Hosted Collaboration Solution の詳細については、https://www.cisco.com/c/en/us/solutions/hosted-collaboration-solution/index.html で入手可能なマニュアルを参照してください。

また、オンプレミスとクラウドベースの両方のサービスを組み合わせてハイブリッド配置を実装し、組織が両方の配信メカニズムの利点を活用できるようにすることもできます。ハイブリッド配置の例を次に示します。

- クラウドのメッセージングと会議の機能を備えた企業コール：コール制御、ボイス メッセージング、およびビデオ メッセージング用の Cisco Unified IM と Unity Connection。IM とプレゼンス、ボイスとビデオ、固定コラボレーション会議室などの Web ベースの会議用に WebEx Messenger と WebEx Meetings も実装。
- クラウドの通話とメッセージング機能を備えた企業コール：音声とビデオ通話用の Cisco Unified CM オンプレミス。Cisco Spark のメッセージングと会議、およびオンプレミスとクラウド間の音声とビデオを統合するためのハイブリッド サービスも実装。

この章で説明している配置モデルは、主にオンプレミス配置を扱っています。ただし、すべての場合において、クラウドベースのアプリケーションおよびサービスをさまざまな配置モデルと統合して、ハイブリッド配置を実現できます。

配置モデル アーキテクチャ

一般に、配置モデル アーキテクチャは、サービスを提供する企業のアーキテクチャに従います。配置モデルは、企業の代表的なトポロジにおける Unified Communications ニーズを満たす参照アーキテクチャを記述します。たとえば、集中型呼処理配置モデルは、1 箇所または数箇所の中央集中型の本社に接続された多数のサイトで業務の大部分が行われる企業に向いたモデルです。

場合によっては、技術的制約のために技術の配置モデルが企業の配置モデルから逸脱することがあります。たとえば、企業に 1 つあるキャンパスのスケールが 1 つのサービス インスタンス（Cisco Unified Communications Manager が提供する呼処理サービスなど）のスケールを超えている場合、1 つのキャンパスに複数の呼処理クラスタ インスタンスまたは複数のメッセージング製品が必要になることがあります。

標準クラスタのサイジング制限を超えるお客様は、別の選択肢として、拡張性を向上できるメガクラスタの配置を検討できます。メガクラスタの詳細については、メガクラスタ（9-25 ページ）を参照してください。

(注)　特に明記されていない限り、この SRND 内に含まれる呼処理配置に関連するすべての情報（キャパシティ、ハイ アベイラビリティ、一般的な設計上の考慮事項など）は、最大 8 個の呼処理サブスクライバ ノードを持つ標準クラスタにのみ適用されます。

Unified Communications 配置モデルの概要

この章では、Unified Communications およびコラボレーションの 3 種類の基本的なオンプレミスの配置モデルについて説明します。

- キャンパス配置モデル

  Unified Communications および Collaboration サービス、これらに関連するエンドポイント、ゲートウェイ、ボーダー コントローラ、メディア リソース、その他のコンポーネントがすべて 1 つの高速 LAN または MAN 上に位置しています。

- 集中型配置モデル

  Unified Communications および Collaboration サービスは中央キャンパス サイトまたはデータセンターに位置しますが、エンドポイント、ゲートウェイ、メディア リソース、その他のコンポーネントは、QoS 対応の WAN によって相互接続される複数のリモート サイトに分散されます。

- 分散型配置モデル

  複数のキャンパスおよび集中型配置、またはこの一方が、Cisco Unified Communications Manager Session Management Edition クラスタなどのトランクとダイヤル プランの集約プラットフォームで QoS 対応 WAN 経由で相互接続されます。

集中型または分散型 PSTN アクセスやサービスの配置など、この 3 種類の基本的な配置モデルに無制限のバリエーションがありますが、この章で説明する基本的な設計のガイドラインが、対象の大部分に引き続き適用されます。

配置モデルのハイ アベイラビリティ

Unified Communications サービスは、ハイ アベイラビリティを実現するための機能を数多く備えています。その実装には、次のようにさまざまな方法があります。

- フェールオーバー冗長性

  不可欠なサービスの場合、設計に単一障害点が存在しないように冗長な要素を配置します。2 つ（またはそれ以上）の要素間の冗長性が自動的に確保されます。たとえば、Cisco Unified Communications Manager（Unified CM）に使用されているクラスタリング技術では、最大 3 台のサーバがお互いをバックアップできます。このタイプの冗長性は、技術的境界を越えて実現される場合もあります。たとえば、1 台の電話機に対して、優先順位 3 番めまでの呼制御エージェントとして、同じ呼処理クラスタに属する 3 台の独立した Unified CM サーバを設定できます。そして 4 番めの選択肢として、Cisco IOS ルータを利用して呼処理サービスを提供するように電話機を設定することもできます。

- リンクの冗長性

  1 つの WAN リンクでの障害に対処するために、IP WAN リンクなどの冗長な IP リンクを配置すると有益な場合があります。

- 地理的多様性

  一部の製品は、冗長なサービス ノードを WAN リンク越しに分散させて、（あらかじめ設定しておいた UPS および発電バックアップ システムの機能を超えて長時間停電が発生するなど）サイト全体がオフラインになっても、別の場所にある別のサイトで事業を継続できるようにしています。

配置モデルのキャパシティ プランニング

さまざまな配置モデルのキャパシティは、一般にその基となる製品のキャパシティと切り離すことができません。この章では、適宜キャパシティについて説明します。サービスをサポートしている製品をこのドキュメントの他の項で詳しく取り上げている場合、その項でその製品のキャパシティについて説明します。

共通の設計基準

Cisco Unified Communications システムを構成するどの技術でも、設計時に検討する基準として次のものがあります。

Size

このコンテキストでのサイズとは一般にユーザ数を指し、これが IP 電話、ボイスメールボックス、プレゼンス ウォッチャなどの数量に読み換えられます。また、データセンターなど、ユーザがほとんど（あるいはまったく）存在しないサイトでは、処理キャパシティの点からサイズを考えることもできます。

ネットワーク接続

サイトをシステムの他の部分への接続を設計する際に考慮が必要な主な要素が 3 つあります。

- Quality of Service（QoS）を確保できる帯域幅
- 遅延
- 信頼性

多くの場合、ローカル エリア ネットワーク（LAN）ではこれらの要素は十分達成されています。すべての LAN 機器で QoS が達成されており、帯域幅は一般にギガビット範囲、遅延は最小限（数ミリ秒程度）で、優れた信頼性が標準で確保されています。

メトロポリタン エリア ネットワーク（MAN）では、3 つの要素とも LAN に近いものとなっています。帯域幅は一般にまだ数メガビット範囲、遅延は一般に数十ミリ秒で、優れた信頼性が確保されています。一般にパケット処理ポリシーが MAN プロバイダーから提供されるため、エンドツーエンドの QoS を実現できます。

ワイド エリア ネットワーク（WAN）では、これらの要素に特に注意する必要があります。帯域幅はコストが何よりも重視され、遅延は実効的な送出速度だけでなく物理的な距離にかかわる実際の伝搬遅延にも左右されることがあり、信頼性はさまざまな要因の影響を受けます。また、QoS 実現のために、余分な運用コストと設定作業が必要になることもあります。

帯域幅は、サイトで利用できる Unified Communications サービスのタイプおよびサービスの提供方法に大きな影響を与えます。たとえば、20 人のユーザにサービスを提供するサイトがシステムの他の部分に 1.5 Mbps の帯域幅で接続している場合、サイトの音声、プレゼンス、インスタント メッセージング、電子メール、およびビデオ サービスをリモートのデータセンター サイトに問題なくホストできます。その同じサイトが 1000 人のユーザをホストしている場合、比較的限られた帯域幅がシグナリングおよびメディア フローで飽和状態になるのを避けるために、サービスの一部をローカルにホストするのが最善です。これ以外にもう 1 つ、リモートのデータセンター サイトから WAN 全体にサービスを配信できるよう帯域幅を拡大する方法もあります。

遅延が設計に与える影響は、リモートに配置する Unified Communications サービスのタイプに応じて異なります。たとえば、片方向の遅延が 200 ms である WAN 全体に音声サービスを提供する場合、ダイヤルトーン遅延やメディア カットスルー遅延増大などの問題が発生することがあります。プレゼンスなど他のサービスでは、200 ms の遅延があっても問題が発生しない可能性があります。

サイトからネットワークの他の部分への接続の信頼性は、技術に適した配置モデルを決定する際の基本的な考慮事項です。信頼性が高い場合は、ほとんどの Unified Communications コンポーネントではリモート サイトからホストされるサービスを配置できます。信頼性が安定しない場合、一部の Unified Communications コンポーネントはリモートからホストされる際に正しく実行されないことがあります。信頼性が低いと、サイトに Unified Communications サービスのコロケーションが必要になることがあります。

ハイ アベイラビリティ要件

サービスのハイ アベイラビリティは常に設計の目標となるものです。信頼性の必要性とその実現に伴うコストとのバランスを保つには、実際的な設計の判断が必要です。次のいずれの要素も、設計がハイ アベイラビリティを実現できるかどうかに影響を与えます。

- 帯域幅の信頼性。Unified Communications サービスの配置モデルに直接影響を与えます。
- 電源の可用性

  停電は、どんなシステムでも極めて破壊的な事象です。停電中はサービスが利用できなくなるだけでなく、電力復旧によってリプル効果がもたらされるためです。電力の可用性が高いサイト（たとえば、無停電電源（UPS）および発電装置によるバックアップを備えて、電力グリッド接続が安定しているサイト）は、一般に Unified Communications サービスのホストに選択できます。サイトの電力可用性に一貫性がない場合、そのサイトをホスト用のサイトとして使用するのは賢明な判断ではありません。

- 熱、湿度、振動などの環境要因

  一部の Unified Communications サービスは、サーバなど定期的な保守を必要とする機器を使用して配信されます。Unified Communications コール エージェント サーバのホストなど、一部の Unified Communications 機能は、能力ある人材が配属されているサイトに配置するのが最善です。

サイトベースの設計ガイドライン

このドキュメント全体を通して、さまざまな Unified Communications サービスおよび技術の系列に沿って設計ガイドラインを編成しています。たとえば、呼処理の章では、呼処理サービスを実際に説明するだけでなく、サイトのサイズ、ネットワーク接続、およびハイ アベイラビリティの要件に基づいて IP Phone および Cisco Unified Communications サーバを配置するための設計ガイドラインも示します。同様に、コール アドミッション制御の章では、技術自体の説明に焦点を当てるだけでなく、サイトベースの設計考慮事項も示します。

一般に、特定の Unified Communications サービスまたは技術のほとんどの側面が、サイトのサイズまたはネットワーク接続とは関係なく、すべての配置に関係しています。必要に応じて、サイトベースの設計考慮事項について説明します。サービスは集中化、分散化、インターネットワーク化、および地理的多様化が可能です。

サービスの集中化

企業の支店サイトが地理的に分散し、ワイド エリア ネットワークで相互接続されている用途では、Cisco Unified Communications サービスを中央に配置しつつ、WAN 接続でエンドポイントにサービスを提供できます。たとえば、呼処理サービスを集中的に配置できます。テレフォニー サービスの配信に必要なのは、リモート サイトとの IP 接続だけです。同様に、Cisco Unity Connection プラットフォームから提供されるようなボイス メッセージ サービスも中央にプロビジョニングして、IP WAN で接続されたリモートからサービスをエンドポイントに配信できます。

中央にプロビジョニングした Unified Communications サービスは、WAN 接続中断の影響を受けます。そのため、サービスごとに、ローカル サバイバビリティ オプションを計画すべきです。たとえば、Cisco Unified CM から提供されるような呼処理サービスには、Survivable Remote Site Telephony（SRST）や拡張 SRST などのローカル サバイバビリティ機能を設定できます。同様に、Unity Connection Survivable Remote Site Voicemail（SRSV）を使用してローカル ボイス メール サービスにアクセスするには、SRST 下でリモート サイトの操作を許可するように、Cisco Unity Connection のような集中型ボイス メッセージ サービスをプロビジョニングできます。

すべての Unified Communications サービスでサービスの集中化を統一する必要はありません。たとえば、複数のサイトが 1 つの集中型呼処理サービスを利用する場所にシステムを配置し、一方で Cisco Unity Express などの非集中型（分散型）ボイス メッセージ サービスでそのシステムをプロビジョニングすることもできます。同様に、Cisco Unity Connection などの集中型ボイス メッセージ サービスとともに、Cisco Unified Communications Manager Express（Unified CME）を使用して呼処理が各サイトでローカルにプロビジョニングされるように Unified Communications システムを配置することもできます。

多くの場合、各サービスの設計時に考慮すべき主要な基準は、サイト間の IP ネットワークの可用性と品質です。サイト間の IP 接続が次の特性を備えている場合、Unified Communications サービスの集中化は、機器のホストと運用に伴う資本費用と運用費用のどちらの面でもスケールメリットが得られます。

- 予想されるトラフィック負荷に十分対応できる帯域幅。ボイスメールへのアクセス、集中型の PSTN 接続へのアクセス、音声やビデオを含むサイト間オンネット通信などによって発生する、ピーク時のアクセス負荷も含めます。
- ハイ アベイラビリティ。WAN サービス プロバイダーがサービス レベル契約に従って接続を迅速に保守および復旧することによりもたらされます。
- 低遅延。主要な中央サイトへのラウンドトリップ時間のためにシステムの応答時間に遅延が発生しても、リモート サイトのローカルなイベントは損害を受けません。

また、特定のサービスを中央に配置して複数のサイトのエンドポイントにサービスを提供した場合、複数のサイトでユーザに同じ処理リソースを使用することから、機能の透過性という利点が得られます。たとえば、2 つのサイトに同じ集中型 Cisco Unified Communications Manager（Unified CM）クラスタからサービスを提供する場合、ユーザは 2 つのサイト間でライン アピアランスを共有できます。各サイトに異なる（分散した）呼処理システムからサービスを提供する場合には、この利点は得られません。

機能の透過性およびスケール メリットという利点は、Unified Communications トラフィックの需要に応えるために WAN ネットワークを構築および運用する際の相対的コストに照らして評価する必要があります。

サービスの分散化

Unified Communications サービスは、複数のサイトに分散させて個別に配置することもできます。たとえば、2 つ（またはそれ以上の）のサイトを独立した呼処理 Cisco Unified CME ノードでプロビジョニングできます。同じ場所にあるエンドポイントに対するサービスの可用性を確保するために WAN を利用する必要はありません。同様に、サイトを Cisco Unity Express などの独立したボイス メッセージング システムでプロビジョニングできます。

Unified Communications サービスを分散させた場合の主な利点は、配置方法が WAN 接続の相対的な可用性およびコストに依存しないことです。たとえば、WAN 接続が使用できないか、きわめて費用がかかるか、または信頼性が高くないリモートの場所でサイトを運用している場合、そのリモート サイト内で Cisco Unified CME などの独立した呼処理ノードをプロビジョニングすると、WAN がダウンしても呼処理の中断が回避されます。

サービスのインターネットワーク化

2 つのサイトを独立したサービスでプロビジョニングした場合でも、両サイトを相互接続してサイト間で機能の透過性をある程度実現できます。たとえば、Cisco Unified CME でプロビジョニングした分散型呼処理サービスを SIP または H.323 トランクでインターネットワーク化して、サイト間で IP コールを許可できます。同様に、Cisco Unity Connection または Cisco Unity Express の独立したインスタンスを同じメッセージング ネットワークに参加させることによって、ユニファイド メッセージ ネットワーク内でメッセージをルーティングしたり、サブスクライバ情報およびディレクトリ情報を交換したりできます。

Unified Communications サービスの地理的多様性

一部のサービスを IP WAN 越しで複数の冗長なノードにプロビジョニングできます。使用中の設計および機能では、これは停電やネットワーク障害でサイトが中断したり、火事や地震などの重大な災害でサイトの物理的な整合性が損なわれたりしても、サービスを継続できます。

このような地理的多様性を実現するには、個々のサービスが冗長なノードをサポートするだけでなく、IP WAN の遅延と帯域幅の制約を越えてこれらのノードを配置できる必要があります。たとえば、ノード間のエンドツーエンドの合計ラウンドトリップ時間が 80 ms を超えず、適度な容量の QoS 対応帯域幅をプロビジョニングしている限り、Unified CM の呼処理サービスは単一クラスタの呼処理ノードを IP WAN 越しに配置できます。これに対して、Unified CME は冗長性を備えていないため、地理的に多様な構成に配置できません。

表 10-2 に、各 Cisco Unified Communications サービスを上記の方法で配置できるかどうかをまとめます。

表 10-2　Cisco Unified Communications サービスに使用可能な配置オプション

サービス	集中型	分散型	インターネットワーク化	地理的多様性
Cisco Unified CM： • Enterprise Edition • Business Edition 6000 • Business Edition 7000	○	○	○	○
Cisco Business Edition 4000	○	X	X	X
Cisco Unified CME	なし	○	○	X
Cisco Unity Express	なし	○	はい（Voice Profile for Internet Mail（VPIM）ネットワーキング経由）	なし
Cisco Unity Connection	○	可（サイトごとに 1 つの Cisco Unity Connection）	はい（VPIM ネットワーキング経由）	○
Cisco Emergency Responder	○	可（サイトごとに 1 つの Emergency Responder グループ）	可（Emergency Responder クラスタリングを使用）	○
Cisco IM and Presence	○	はい（サイトごとに 1 つの Cisco IM and Presence サービス）	可（ドメイン間フェデレーションを使用）	○

表 10-2　Cisco Unified Communications サービスに使用可能な配置オプション(続き)

サービス	集中型	分散型	インターネットワーク化	地理的多様性
Cisco Unified Mobility	○	はい(Unified CM シングル ナンバー リーチとして)	なし	○
Cisco Expressway	○	○	○	○
Cisco Meeting Server	○	○	○	○

呼処理は基本的なサービスであるため、この章では基本呼処理配置モデルについて説明します。Cisco Unified Communications Manager 呼処理の技術的詳細については、呼処理(9-1 ページ)の章を参照してください。

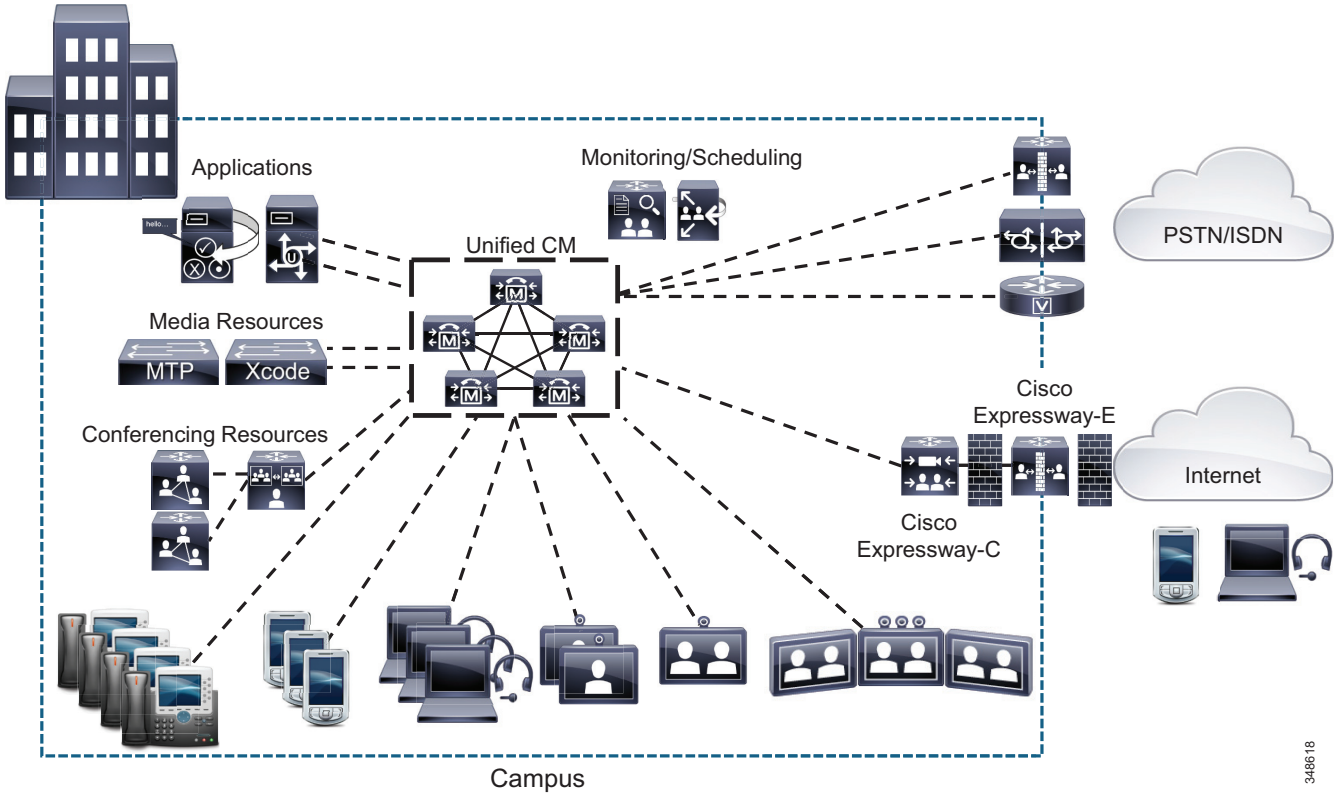
配置モデルの設計上の特徴とベスト プラクティス

ここでは、Cisco Collaboration と Unified Communications システムの基本的な配置モデルを説明し、各モデルのベスト プラクティスを示します。

キャンパス配置

この呼処理配置モデルでは、Unified Communications サービスとエンドポイントはキャンパスの同じ場所にあります。サービス ノード、エンドポイント、およびアプリケーションの間の QoS 対応ネットワークは高い可用性を実現しており、ギガビット単位の帯域幅を提供し、エンドツーエンドの遅延は 15 ms 未満です。同様に、電源の品質および可用性はきわめて高く、サービスは適切なデータセンター環境にホストされます。エンドポイント間の通信は、LAN または MAN を通過し、企業外部の通信は PSTN などの外部ネットワークを経由します。企業は、一般に LAN または MAN で接続された 1 つまたは複数のまとまったビルにキャンパス モデルを配置します。(図 10-2 を参照)。

図 10-2　　キャンパス配置の例



キャンパス モデルの設計上の特長は、次のとおりです。

- 単一の Cisco Unified CM クラスタ（Enterprise または Business Edition 7000）。一部のキャンパス呼処理配置では、複数の Unified CM クラスタが必要になる場合があります。たとえば、コールの対象となるエンドポイントの数が多すぎて単一のクラスタでは対応できない場合や、クラスタをコール センターなどの用途に限る必要がある場合などです。
- 一方、小規模な導入では、Cisco Business Edition 4000 または Business Edition 6000 をキャンパスに配置できます。
- Unified CM クラスタごとに最大 40,000 の設定済みおよび登録済み Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone、ソフトフォン、アナログ ポート、ビデオ エンドポイント、SIP ベースの TelePresence エンドポイント、ルームベースの TelePresence 会議システム、モバイル クライアント、および Cisco Virtualization Experience Clients（VXC）。
- Unified CM クラスタごとに最大 2,100 のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H.323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）。
- キャンパスの外部にある宛先へ向かうすべてのコール用のトランクやゲートウェイ（IP または PSTN）。
- マルチポイント会議には、マルチポイント コントロール ユニット（MCU）、Telepresence Server、または他のマルチポイント リソースなどの、マルチポイント会議リソースが必要です。
- 会議、トランスコーディング、およびメディア ターミネーション ポイント（MTP）に対応する、同じ場所のデジタル シグナル プロセッサ（DSP）リソース。

- メッセージング（ボイスメール）、プレゼンス、モビリティなどその他の Unified Communications サービスも一般に同じ場所に設置されます。
- PBX やボイスメール システムなどレガシー音声サービスへのインターフェイスがキャンパス内に接続されるため、帯域幅または接続に運用コストがかかりません。
- SIP ベースのビデオ ISDN ゲートウェイは、公衆 ISDN 網上のビデオ会議デバイスと通信するために必要です。
- Cisco Expressway-C および Cisco Expressway-E は、安全な Business-to-Business Telepresence およびビデオ コミュニケーションを実現するコラボレーション エッジ機能のほか、インターネット経由のリモートおよびモバイル ワーカーに対する企業アクセスを提供します。
- Cisco TelePresence Video Communication Server（VCS）は、レガシー H.323 およびサードパーティ製 TelePresence エンドポイントの登録にも使用できます。ただし、デュアル呼制御によって生じるダイヤル プランおよびコール アドミッション制御の複雑さを回避するには（デュアル呼制御配置の設計上の考慮事項（10-43 ページ）を参照）、SIP を使用して、Cisco Unified CM にすべての TelePresence エンドポイントとルームベースの TelePresence 会議システムを登録することを推奨します。
- 広帯域オーディオ（たとえば、G.711 または G.722）はサイト内のデバイス間で使用できます。
- 広帯域ビデオ（たとえば、4CIF または 720p では 1.5 Mbps、1080p では 2 Mbps）はサイト内のデバイス間で使用できます。

キャンパス モデルのベスト プラクティス

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

- インフラストラクチャがハイ アベイラビリティで、QoS に対応し、復元性、高速コンバージェンス、およびインライン パワーを備えていることを確認します。
- 自社内のコール パターンを知っておく必要があります。キャンパス モデルは、大部分のコールが社内の同一サイトから発信されている場合、または社外の PSTN ユーザ宛てに発信されている場合に適用します。
- すべてのエンドポイントに G.711 コーデックを使用します。この方式を実施すると、トランスコーディングに対してデジタル シグナル プロセッサ（DSP）リソースを消費する必要がなくなり、その分のリソースは、会議やメディア ターミネーション ポイント（MTP）などの他の機能に割り当てることができます。
- ハイ アベイラビリティ、電話機用の接続オプション（インライン パワー）、Quality of Service（QoS）メカニズム、およびセキュリティ用の推奨ネットワーク インフラストラクチャを実装しています（ネットワーク インフラストラクチャ（3-1 ページ）を参照）。
- 呼処理（9-1 ページ）の章にリストされているプロビジョニングの推奨事項を実行します。

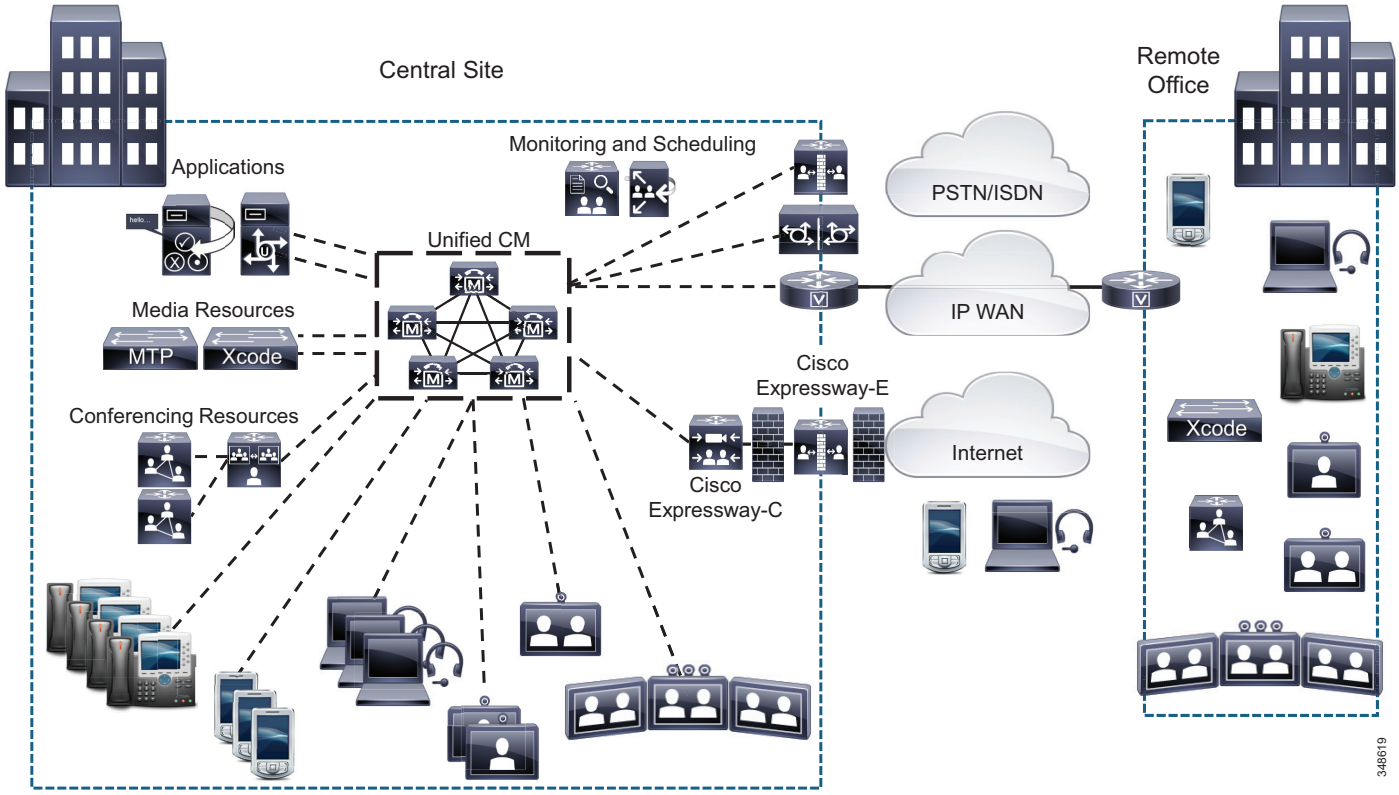
集中型呼処理を使用するマルチサイト配置

この呼処理配置モデルでは、少なくとも一部のエンドポイントは QoS 対応のワイド エリア ネットワークを越えて呼処理サービスとは離れた場所に置かれます。WAN 全体で利用できる帯域幅の容量が限られているため、特定の WAN リンクで認められるコールの数を管理して、負荷を使用可能な帯域幅の制限内に収めるには、コール アドミッション制御メカニズムが必要です。エンドポイント間のオンネット通信は、LAN/MAN（エンドポイントが同じサイトにある場合）または WAN（エンドポイントが異なるサイトにある場合）のいずれかを通過します。企業外部の通信は、エンドポイントと同じ場所または異なる場所に配置できるゲートウェイまたは Cisco Unified Border Element（CUBE）セッション ボーダー コントローラ（SBC）を介して PSTN などの外部ネットワークを経由します（たとえば、メイン サイトで集中型ゲートウェイを使用する場合、またはエンタープライズ ネットワーク全体でテールエンド ホップオフ（TEHO）を行う場合）。

IP WAN は、中央サイトとリモート サイト間の呼制御シグナリングも伝送します。図 10-3 は、一般的な集中型呼処理配置を示しています。この配置では、中央サイトの呼処理エージェントとして Unified CM クラスタを使用し、すべてのサイトを接続するために、QoS 対応の IP WAN を使用します。この配置モデルでは、管理と保守全体のコストを削減するために、ボイス メッセージ、プレゼンス、モビリティなど他の Unified Communications サービスも中央サイトにホストすることがよくあります。WAN の信用性が低い場合や、WAN 帯域幅のコストが高い場合には、サービスの可用性が WAN の障害の影響を受けないように、ボイス メッセージング（ボイスメール）など一部の Unified Communications サービスを分散させることができます。

（注）　このマニュアルで説明する集中型呼処理モデル用のソリューションでは、さまざまなサイトが QoS に対応した IP WAN に接続されます。

図 10-3　　集中型呼処理を使用するマルチサイト配置



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

- 単一の Unified CM クラスタ（Enterprise または Business Edition 7000）。一部の集中型呼処理配置では、複数の Unified CM クラスタが必要になる場合があります。たとえば、コールの対象となるエンドポイントの数が多すぎて単一のクラスタでは対応できない場合や、クラスタをコール センターなどの用途に限る必要がある場合などです。
- Cisco Business Edition 6000 は、最大 49 のリモート サイトに対応する集中型呼処理構成で配置できます。
- Cisco Business Edition 4000 は、集中型呼処理構成で配置できます。
- Unified CM クラスタごとに最大 40,000 の設定済みおよび登録済み Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone、ソフトフォン、アナログ ポート、ビデオ エンドポイント、SIP ベースの TelePresence エンドポイント、ルームベースの TelePresence 会議システム、モバイル クライアント、および Cisco Virtualization Experience Clients（VXC）。
- Unified CM クラスタあたり最大 2,000 のロケーションまたは支店サイト。
- Unified CM クラスタごとに最大 2,100 のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H.323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）。
- すべてのオフネット コールのための PSTN 接続。
- 会議、トランスコーディング、およびメディア ターミネーション ポイント（MTP）用のデジタル シグナル プロセッサ（DSP）リソースを各サイトにローカルに分散させて、DSP を必要とするコールが消費する WAN 帯域幅の容量を削減します。

- マルチポイント会議には、マルチポイント コントロール ユニット（MCU）または他のマルチポイント会議リソースが必要です。これらのリソースは中央サイトにあっても、ローカル会議リソースが必要な場合はリモート サイトに分散していてもかまいません。
- レガシー構内交換機（PBX）システムおよびボイスメール システムとの統合機能。PBX やボイスメール システムなど従来の音声サービスへの接続を中央サイト内に行うことができるため、帯域幅または接続に運用コストがかかりません。リモート サイトにある従来のシステムに接続するには、余分な WAN 帯域幅のプロビジョニングに伴う運用コストが必要になる場合があります。
- SIP ベースのビデオ ISDN ゲートウェイは、公衆 ISDN 網上のビデオ会議デバイスと通信するために必要です。ISDN ビデオ ゲートウェイは、各リモート サイトで一元的に管理、または配置できます。
- Cisco Expressway C および Cisco Expressway E は、安全な Business-to-Business Telepresence およびビデオ コミュニケーションを実現するコラボレーション エッジ機能のほか、インターネット経由のリモートおよびモバイル ワーカーに対する VPN-less 企業アクセスを提供します。
- Cisco TelePresence Video Communication Server（VCS）は、レガシー H.323 およびサードパーティ製 TelePresence エンドポイントの登録にも使用できます。ただし、デュアル呼制御によって生じるダイヤル プランおよびコール アドミッション制御の複雑さを回避するには（デュアル呼制御配置の設計上の考慮事項（10-43 ページ）を参照）、SIP を使用して、Cisco Unified Communications Manager にすべての TelePresence エンドポイントとルームベースの TelePresence 会議システムを登録することを推奨します。
- システムは、サイト内のデバイス間の広帯域オーディオ（たとえば、G.711 または G.722）の自動選択を異なるサイトのデバイス間の狭帯域オーディオ（たとえば、G.729）選択中に可能にします。
- システムは、同じサイト内のデバイス間の広帯域ビデオ（4CIF または 720p での 1.5 Mbps から 1080p での 2 Mbps など）、および異なるサイトのデバイス間の狭帯域ビデオ（448p または CIF での 384 kbps）の自動選択を可能にします。
- WAN でビデオを発信するときには、WAN リンク速度を最低でも 1.5 Mbps 以上にする必要があります。
- コール アドミッション制御は、Enhanced Locations CAC によって実現されます。
- 音声およびビデオ コールの場合、コール アドミッション制御が、帯域幅不足によるクラスタ内のエンドポイント間でコールを拒否する場合、Automated Alternate Routing（AAR）は、PSTN 経由で自動的にコールを再ルーティングします。AAR は、ゲートウェイを利用して発信側電話機から PSTN へ向かうコールをルーティングし、着信側電話機に接続される別のゲートウェイを利用してリモート サイトで PSTN からのコールを受け付けます。
- リモート WAN リンク障害のためにエンドポイントが未登録であると見なされたときには、Call Forward Unregistered（CFUR）機能により、PSTN 経由で自動的にコールを再ルーティングできます。CFUR は、ゲートウェイを利用して呼び出し元の電話機から PSTN へ向かうコールをルーティングし、呼び出し先の電話機に接続される別のゲートウェイを利用してリモート サイトで PSTN からのコールを受け付けます。
- リモート サイトに位置するビデオ エンドポイント用 Survivable Remote Site Telephony（SRST）は、WAN 接続に障害が発生した場合、すべてのデバイスを音声専用にします。拡張 SRST により、WAN 障害時でも SIP ビデオ エンドポイント（Cisco Unified IP Phone 9900 など）でビデオを存続させることができます。特定の電話機モデルでの SRST ビデオ サポートについては、https://www.cisco.com で入手可能な『Cisco Unified IP Phone Administration Guide』を参照してください。
- SRST の代わりに Cisco Unified Communications Manager Express（Unified CME）を使用して、リモート サイトのサバイバビリティ（拡張 SRST）を確保することもできます。

- Cisco Unified Communications Manager Express（Unified CME）は、支社またはリモート サイトで Cisco Unity サーバと統合が可能です。Cisco Unity Connection サーバは、中央サイトの Unified CM に通常モードで登録され、Unified CM が到達不能の場合や WAN の障害時は、拡張 SRST に CM モードでフォールバックできます。これにより支社のユーザは、MWI を使用してボイスメールにアクセスできます。
- マルチサイト集中型呼処理モデルを使用している場合、本社およびリモート サイト ゲートウェイの両方を経由した PSTN ルーティングがサポートされています。ローカル PSTN ブレークアウト用にリモート サイトのローカル ゲートウェイを提供することは、リモート サイトのユーザに緊急サービスを提供する場合にその国の要件を満たす必要があります。この場合、リモート サイトのローカル ゲートウェイは、緊急コール用のローカル PSAP にコール ルーティングを提供します。PSTN から IP テレフォニー ネットワークを分離する必要がある規制の厳しい国には、リモート サイトのローカル PSTN ブレークアウトも必要な場合があります。規制で許可されていれば、リモート サイト ゲートウェイを経由するローカル PSTN ブレークアウトを使用して、トール バイパスまたは Tail-end Hop Off（TEHO; テールエンド ホップ オフ）を有効にできます。

IP WAN の接続オプションは、次のとおりです。

- 専用回線
- フレーム リレー
- 非同期転送モード（ATM）
- ATM とフレーム リレーのサービス インターワーキング（SIW）
- マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）
- Voice and Video Enabled IP セキュリティ プロトコル（IPSec）音声およびビデオ対応 IPSec VPN（V3PN）

WAN エッジに置かれているルータには、プライオリティ キューイングやトラフィック シェーピングなどの Quality of Service（QoS）メカニズムが装備されていて、WAN の帯域幅が恒常的に不足している場合に、データ トラフィックから音声トラフィックおよびビデオ トラフィックを保護しています。加えて、音声トラフィックおよびビデオ トラフィック、またはこの一方による WAN リンクのオーバーサブスクリプションや確立されたコールの品質低下を防止するために、コール アドミッション制御方式が必要です。集中型呼処理配置の場合は、Unified CM 内に設定された拡張ロケーション CAC または RSVP ロケーションは、コール アドミッション制御（CAC）を提供します（ロケーションの詳細については、帯域幅管理（13-1 ページ）の章を参照してください）。

さまざまな Cisco ゲートウェイは、TDM または IP ベースの PSTN アクセスをリモート サイトで提供できます。IP WAN で障害が発生した場合や、IP WAN 上で使用可能な帯域幅がすべて消費されてしまった場合でも、リモート サイトのユーザからのコールは、PSTN 経由で再ルーティングできます。Cisco Unified Survivable Remote Site Telephony（SRST）機能は、SCCP および SIP 電話機の両方で使用可能です。Cisco Unified IP Phone が、リモートの 1 次、2 次、および 3 次 Unified CM への接続を失った場合、または WAN 接続がダウンした場合に、支店での呼処理を提供します。Cisco IOS ゲートウェイおよびルータでは、Cisco Unified SRST、および拡張 SRST を実行する Unified CME を使用できます。拡張 SRST を実行する Unified CME では、標準の Unified SRST よりも電話に関する多くの機能を提供されます。

集中型呼処理モデルのベスト プラクティス

マルチサイトの集中型呼処理配置を実装する際は、次のガイドラインおよびベスト プラクティスに従ってください。

- 音声のカットスルー遅延（クリッピングとも呼ばれます）を減らすために、Unified CM とリモート ロケーション間の遅延を最小限に抑えます。
- リモート ブランチとの間でコール アドミッション制御をやり取りするために、Unified CM で Enhanced Locations CAC を設定します。このメカニズムをさまざまな WAN トポロジに適用する方法については、帯域幅管理（13-1 ページ）の章を参照してください。
- 各リモート サイトでの Survivable Remote Site Telephony（SRST）モードでサポートされている IP Phone およびライン アピアランスの数は、その支店内にあるルータのプラットフォーム、取り付け済みメモリ容量、および Cisco IOS Release により異なります。SRST では最大 1,500 台の電話機がサポートされますが、拡張 SRST を実行する Unified CME の場合は、最大 450 台です（最新の SRST または Unified CME プラットフォームおよびコードの仕様については、https://www.cisco.com で入手可能な SRST および Unified CME のマニュアルを参照してください）。ただし、一般的には、特定サイトに対して集中型呼処理か、分散呼処理かを決定するには、次に示す種々の要素を考慮する必要があります。
  - IP WAN 帯域幅、または遅延制限
  - 音声ネットワークに関する臨界状況
  - フィーチャ セットの必要性
  - 拡張性
  - 管理の容易さ
  - コスト

  お客様のビジネス ニーズに分散型呼処理モデルがふさわしいと判断する場合は、2 つの選択肢があります。各サイトに Unified CM クラスタをインストールする方法と、リモート サイトで Unified CME を稼働する方法です。
- リモート サイトでは、次の機能を使用して、WAN 障害が発生した場合の呼処理のサバイバビリティを確保します。
  - SCCP 電話機の場合は、SRST または拡張 SRST を使用します。
  - SIP 電話機の場合は、SIP SRST または拡張 SRST を使用します。
  - 集中型ボイス メールの配置の場合、Survivable Remote Site Voicemail（SRSV）を使用します。

  SRST、拡張 SRST、SIP SRST、SRSV、および MGCP ゲートウェイ フォールバックは、同一の Cisco IOS ゲートウェイに相互に存在することができます。

リモート サイトのサバイバビリティ

集中型呼処理モデルで WAN を介した Cisco Unified Communications を配置する場合、リモート サイトのデータ サービスと音声サービスのハイ アベイラビリティを確保するために、追加の処置が必要です。表 10-3 では、リモート サイトでのハイ アベイラビリティを実現するためのさまざまな方法をまとめています。これらの方法のいずれを選択するかは、ビジネスまたはアプリケーションの特殊な要件、可用性が高いデータ サービスと音声サービスに関連した優先順位、コストの考慮事項などの複数の要素によって異なります。

表 10-3　リモート サイトのハイ アベイラビリティを実現する方法

方法	データ サービスのハイ アベイラビリティ	音声サービスのハイ アベイラビリティ
支店ルータにおける冗長 IP WAN リンク	○	○
支店ルータの冗長プラットフォーム + 冗長 IP WAN リンク	○	○
データのみの ISDN バックアップ + SRST または拡張 SRST	○	○
データと音声の ISDN バックアップ	○	あり（下記の規則を参照）
Cisco Unified Survivable Remote Site Telephony（SRST）または拡張 SRST	なし	○

表 10-3 にリストされている最初の 2 つのソリューションは、IP WAN アクセス ポイントに冗長性を追加して、リモート IP Phone と中央の Unified CM との間の IP 接続を常に保持することによって、ネットワーク インフラストラクチャ層に高い可用性を提供します。これらのソリューションは、データ サービスと音声サービスの両方に適用され、呼処理層からはまったく見えません。このオプションは、支店ルータでの冗長 IP WAN リンクの追加から、冗長 IP WAN リンクを備えた別の支店ルータ プラットフォームの追加までにわたります。

表 10-3 の 3 番めと 4 番めのソリューションでは、ISDN バックアップ リンクを使用して、WAN 障害時の存続可能性を提供します。ISDN バックアップ用には、次の 2 つの配置オプションがあります。

- データのみの ISDN バックアップ

  このオプションでは、ISDN はデータのみの存続可能性の確保に使用され、一方 SRST または拡張 SRST は音声のサバイバビリティの確保に使用されます。Skinny Client Control Protocol（SCCP）、H.323、メディア ゲートウェイ コントロール プロトコル（MGCP）、Session Initiation Protocol（SIP）などのテレフォニー シグナリング プロトコルからのトラフィックが ISDN インターフェイスに入らないように支店ルータにアクセス コントロール リストを設定して、IP Phone からの信号が中央サイトの Unified CM に到達しないようにする必要があることに注意してください。これにより、支社にあるテレフォニー エンドポイントは WAN の障害を検出し、ローカル SRST リソースを利用するようになります。

- データと音声の ISDN バックアップ

  このオプションでは、ISDN はデータと音声の両方の存続性を確保するのに使用されます。この場合、IP Phone は常に Unified CM クラスタとの IP 接続を保持するので、SRST または拡張 SRST の Unified CME は使用されません。しかし、データと音声のトラフィックの転送に ISDN を使用するのは、次の条件がすべて満たされる場合だけにすることをシスコは推奨しています。

  - ISDN リンク上で音声トラフィックに割り当てられた帯域幅が、IP WAN リンク上で音声トラフィックに割り当てられた帯域幅と同じである。
  - ISDN リンクの帯域幅が固定されている。
  - 必要なすべての QoS 機能が、ルータの ISDN インターフェイスに配置されている。QoS の詳細については、ネットワーク インフラストラクチャ（3-1 ページ）の章を参照してください。

表 10-3 にリストされている 5 番めのソリューションでは、WAN 障害が検出された場合、Survivable Remote Site Telephony（SRST）または拡張 SRST が、リモート オフィスのルータ内で呼処理機能のサブセットを提供し、IP Phone を拡張して、ローカル ルータ内の呼処理機能に「re-home」機能を提供することによって、音声サービスのみのハイ アベイラビリティを提供します。図 10-4 では、SRST または拡張 SRST を使用した典型的なコールのシナリオを示しています。

図 10-4　Survivable Remote Site Telephony（SRST）または拡張 SRST、通常の動作

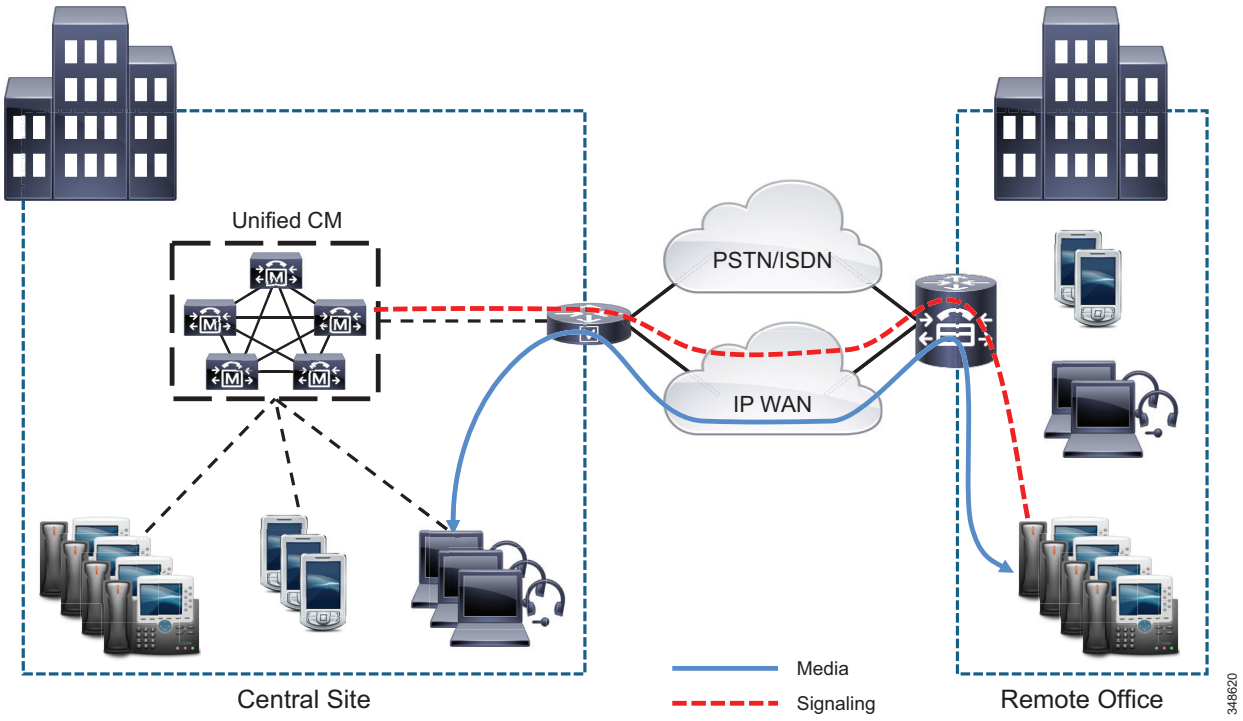
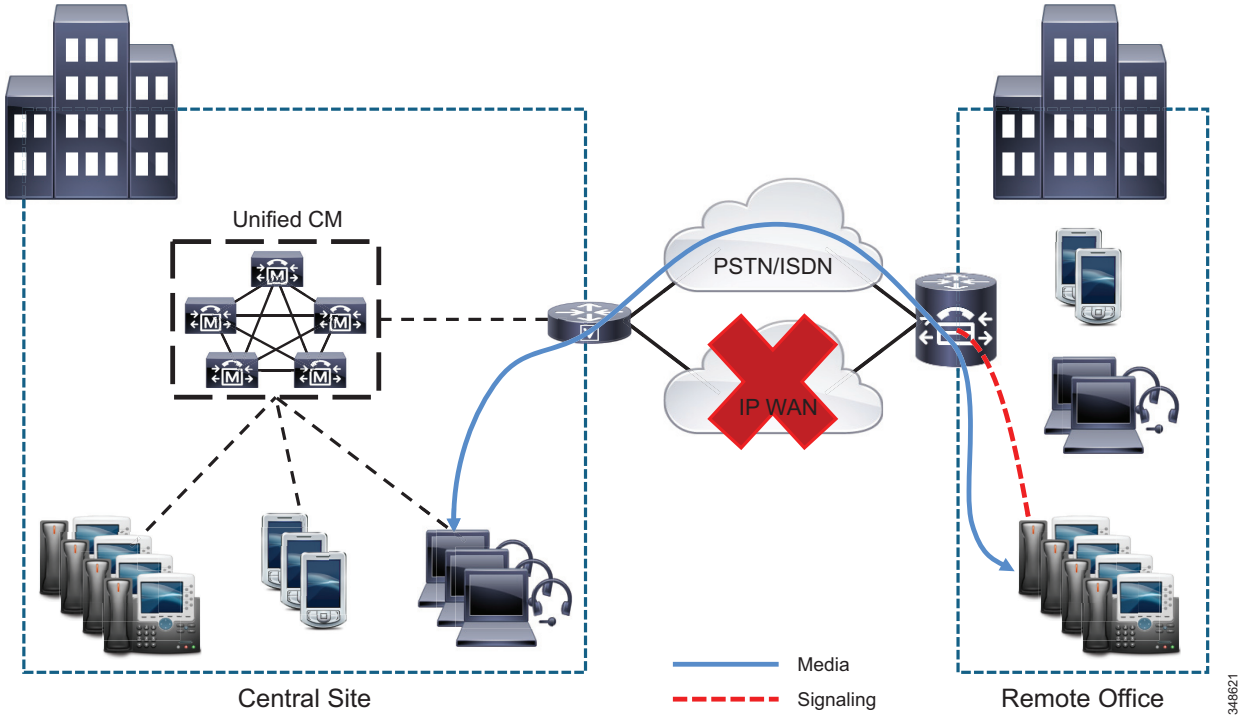


図 10-4 の通常の動作では、リモート オフィスは、データ トラフィック、音声トラフィック、およびコール シグナリングを伝送する IP WAN を経由して、中央サイトに接続されます。リモート オフィスの IP Phone は、中央サイトの Unified CM クラスタとコール シグナリング情報を交換し、IP WAN を介してコールを発信します。リモート オフィスのルータまたはゲートウェイは、両方のタイプのトラフィック（コール シグナリングと音声）を透過的に転送し、IP Phone を認識しません。

図 10-5 に示されるように、リモート オフィスとの WAN リンクに障害が起きた場合、またはその他の何らかのイベントにより、Unified CM クラスタとの接続が失われた場合、リモート オフィスの IP Phone はリモート オフィスのルータに SRST モードで再登録されます。リモート オフィスのルータは、SRST または拡張 SRST を使用して、設定について IP Phone に照会し、この情報を使用して独自の設定を自動的に作成します。リモート オフィスの IP Phone は、リモート オフィスのネットワーク内か、または PSTN を介してコールの発信と受信を行うことができます。電話機は「Unified CM フォールバック モード（Unified CM fallback mode）」というメッセージを表示し、Unified CM の一部の拡張機能が利用不能になり、電話機のディスプレイでグレー表示されます。

図 10-5　Survivable Remote Site Telephony（SRST）または拡張 SRST：WAN の障害



中央サイトとの WAN 接続が再度確立されると、リモート オフィスの IP Phone は、Unified CM クラスタに自動的に再登録され、正常な動作に戻ります。リモート オフィスの SRST ルータは、IP Phone についての情報を削除し、標準のルーティングまたはゲートウェイ設定に戻ります。リモート オフィスで拡張 SRST を使用するルータは、自動プロビジョニング オプションを使用することで、取得した電話機および回線の設定を、Unified CME ルータの実行コンフィギュレーションに保存できます。**auto-provision none** が設定されている場合、自動でプロビジョニングされた電話機または回線の設定情報は、Unified CME ルータの実行コンフィギュレーションに保存されません。そのため、IP Phone を交換して MAC アドレスが変更された場合でも、Unified CME での設定変更は必要ありません。

（注）　中央サイトとの WAN 接続が再度確立された場合、または Unified CM が再度到達可能になった場合でも、アクティブ コールを持つ SRST モードの電話機がただちに Unified CM に再登録されるわけではありません。再登録されるのは、そのようなアクティブ コールが終了してからです。

拡張 SRST

拡張 SRST は、ルータの SRST で使用できる機能よりも多くの呼処理機能を IP Phone に提供します。コール プリザベーションや自動プロビジョニング、フェールオーバーといった SRST の機能に加え、拡張 SRST では、電話機用に用意されている次のような Unified CME テレフォニー機能のほとんどを使用できます。

- ページング
- [会議（Conferencing）]
- ハント グループ

- 基本自動着信呼分配（B-ACD）
- コール パーク、コール ピックアップ、コール ピックアップ グループ
- オーバーレイ DN、ソフトキー テンプレート
- Cisco IP Communicator
- Cisco Jabber Clients
- Cisco Unified Video Advantage
- エンドポイントのビデオ コール

拡張 SRST では、WAN 障害が発生した場合に、SCCP および SIP 電話機に対する呼処理がサポートされます。ただし、拡張 SRST では、MGCP 電話機またはエンドポイントに対するフォールバックはサポートしていません。Unified CM への接続が失われた場合や、WAN 接続に障害が発生した場合に、MGCP 電話機がフォールバックできるようにするために、SRST フォールバック サーバとして動作している同じ Unified CME サーバに、MGCP ゲートウェイ フォールバック機能を追加で設定できます。

拡張 SRST のベスト プラクティス

- Unified CM での SRST 参照の IP アドレスとして、Unified CME の IP アドレスを使用します。
- Connection Monitor Duration は、SRST から Unified CM へのフォールバックを開始するまでに、電話機が WAN リンクをモニタする時間を指定するタイマーです。ほとんどの場合は、デフォルト設定の 120 秒を使用します。ただし、SRST モードの電話機が、フラッピングが発生しているリンクで Unified CM にフォールバックしたり復帰したりするのを防ぐために、Unified CM の Connection Monitor Duration パラメータをより長い期間に設定できます。これにより、電話機が SRST ルータと Unified CM の間で登録と再登録を繰り返すことがなくなります。電話機が長期間にわたって SRST から Unified CM にフォールバックしなくなるため、この値を極端に長い期間に設定しないでください。
- SRST フォールバック モードの電話機は、アクティブ状態になっても Unified CM に復帰しません。
- SRST フォールバック モードの電話機は、セキュア会議から非セキュア モードに戻ります。
- **auto-provision none** を設定し、取得された ephone-dn または ephone 設定が、Unified CME ルータの実行コンフィギュレーションに書き込まれないようにします。これにより、IP Phone が交換された場合や、MAC アドレスが変更された場合に、設定を変更する必要がなくなります。

拡張 SRST の詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Express System Administrator Guide*』を参照してください。

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

MGCP ゲートウェイ フォールバックの詳細については、次の Web サイトで入手可能な『*CCisco Unified Communications Manager and Interoperability Configuration Guide, Cisco IOS Release 15M&T*』の MGCP ゲートウェイ フォールバックに関する情報を参照してください。

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cminterop/configuration/15-mt/cminterop-15-mt-book.html

SRST ルータのベスト プラクティス

次の配置シナリオでは、拡張 SRST ではなく、Cisco Unified SRST ルータを使用します。

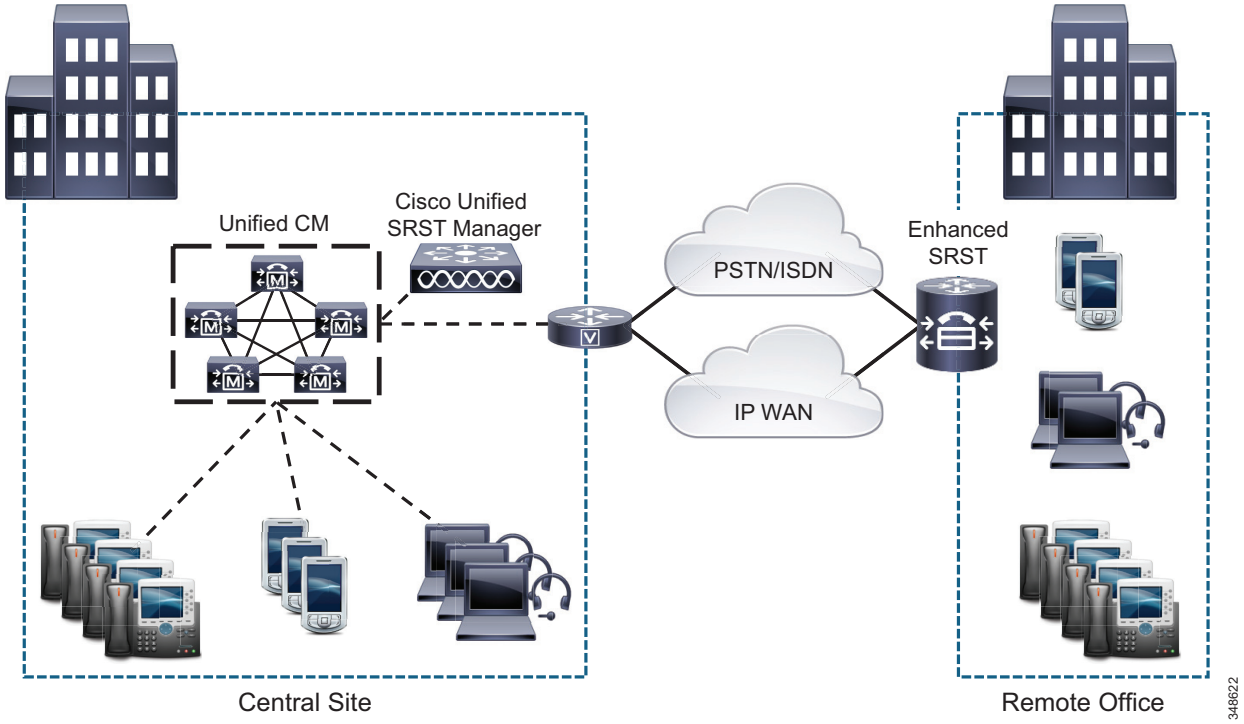
- 1 台の SRST ルータで、最大 1,500 台の電話機をサポートする場合。(拡張 SRST は、最大で 450 台の電話機をサポートします)。
- 最大 3,000 台の電話機をサポートする場合は、2 台の SRST ルータを使用。各 SRST ルータ間でコールが相互にルーティングされるように、ダイヤル プランを正しく設定する必要があります。
- 基本的な SRST 機能の、単純な 1 回限りの設定を行う場合。
- Cisco Unified SRST(セキュア SRST)でのみ使用可能な SRTP メディア暗号化を使用する場合。

到達不能または SRST ルータに登録されていない電話機のコールをルーティングする場合は、**alias** コマンドを使用。

Cisco Unified Survivable Remote Site Telephony Manager

Cisco Unified Survivable Remote Site Telephony(SRST)Manager は、支社の拡張 SRST および従来の SRST の配置を簡素化します(図 10-6 を参照)。Cisco Unified SRST Manager は、シスコがサポートする仮想プラットフォーム(たとえば、Cisco UCS)の仮想マシン内で実行される Linux ベースのソフトウェアです。Cisco Unified SRST Manager は、Cisco Unified CM クラスタが中央のロケーションで動作する集中型呼処理配置モデルのみをサポートしています。Cisco Unified SRST Manager は、Cisco Unified CM クラスタとともに中央ロケーションで、またはリモート支社ロケーションで展開できます。図 10-6 は、中央ロケーションにある Cisco Unified SRST Manager の配置を示しています。通常の動作中に、Cisco Unified SRST Manager は Cisco Unified CM から定期的に設定(たとえば、コーリング サーチ スペース、パーティション、ハント グループ、コール パーク、コール ピック アップなど、設定されている場合)を取得し、SRST モードの使用についても同様の機能のブランチ ルータをプロビジョニングするためにアップロードします。したがって、Cisco Unified SRST Manager は支社の SRST ルータで必要な手動の設定を減らし、SRST と通常モードでも同様のコール操作を実現できるようにします。

図 10-6　　中央ロケーションに配置された Cisco Unified SRST Manager



Cisco Unified SRST Manager はリモート オフィスのルータをプロビジョニングするために Unified CM 設定をアップロードするときに WAN リンクからの帯域幅を消費します。Cisco Unified SRST Manager ソフトウェアはパケットのマーキングを実行しないため、Cisco Unified SRST Manager のトラフィックは、ネットワークのベスト エフォートとして伝送されます。シスコでは、このベスト エフォート型マーキングを維持することを推奨します。これは IP Precedence 0（DSCP 0 または PHB BE）であり、リアルタイムの高優先度音声トラフィックに干渉しません。Cisco Unified SRST Manager トラフィックによる輻輳の発生を回避し、パケットのドロップ率を軽減するために、ピーク時以外の間（夜間や週末など）に設定のアップロードをスケジュールすることを推奨します。設定のアップロード スケジュールは、Cisco Unified SRST Manager の Web インターフェイスから設定できます。

Cisco Unified SRST Manager を配置する場合は、次の注意事項に従ってください。

- Cisco Unified SRST Manager は、Cisco Unified Communications 500 シリーズ プラットフォームではサポートされません。
- リモート オフィスの音声ゲートウェイは、SRST ルータと共存する（ルータに存在する）必要があります。
- Cisco Unified SRST Manager は、冗長化には対応していません。Cisco Unified SRST Manager が使用できない場合、設定のアップロードは不可能です。
- Cisco Unified SRST Manager は、NAT が本社と支社の間で使用される展開ではサポートされていません。

集中型呼処理のバリエーションとしての Voice Over the PSTN

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

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

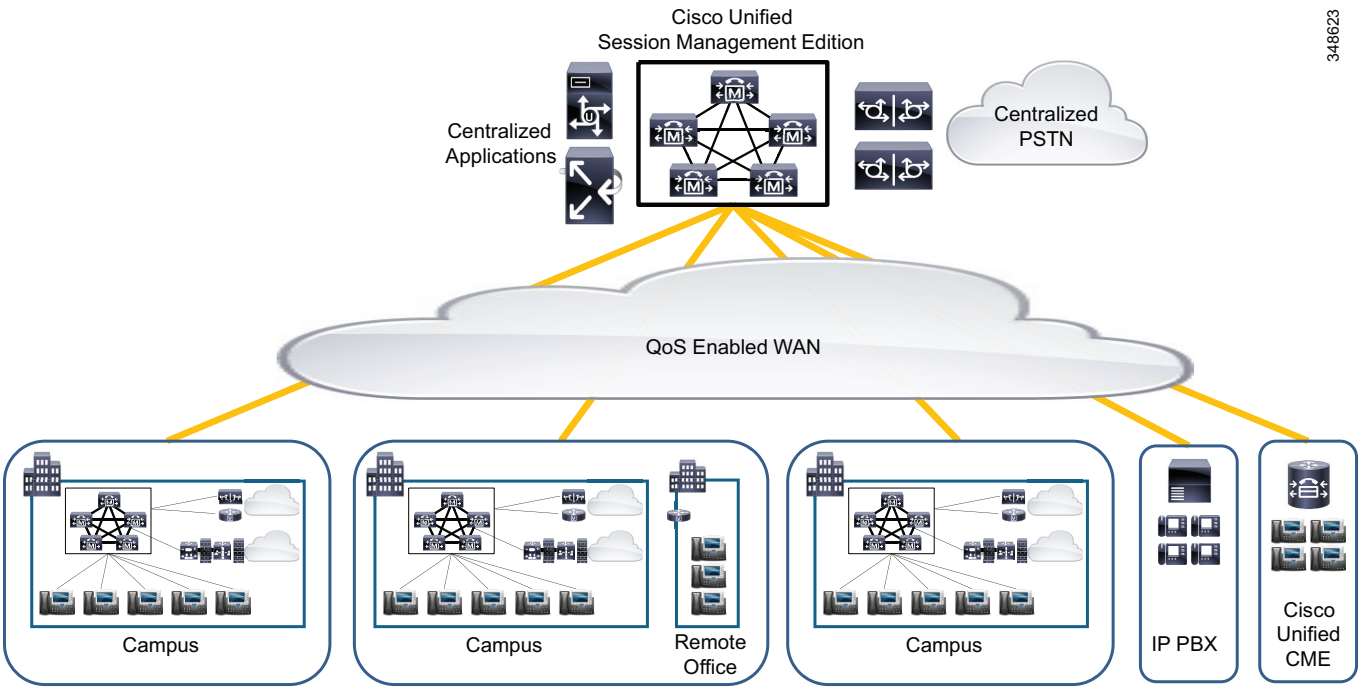
VoPSTN 配置オプションの詳細情報および設計ガイドラインについては、次の URL で入手可能な『*Cisco Unified Communications System 9.0 SRND*』の「*Unified Communications Deployment Models*」の章の「VoPSTN」の項を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/9x/uc9x/models.html

分散型呼処理を使用するマルチサイト配置

分散型呼処理を使用するマルチサイト配置のモデルは、複数の独立したサイトから構成されています。各サイトには独自の呼処理エージェント クラスタがあり、そのエージェント クラスタは、分散されたサイト間の音声トラフィックを伝送する IP WAN に接続されます。図 10-7 は、標準的な分散型呼処理配置を示しています。

図 10-7　　分散型呼処理を使用するマルチサイト配置



分散型呼処理モデルの各サイトは、次のいずれかになります。

- 独自の呼処理エージェントを使用する単一サイト。呼処理エージェントは、次のいずれかになります。
  - Cisco Unified Communications Manager（Enterprise または Business Edition 7000）
  - Cisco Business Edition 6000
  - Cisco Unified Communications Manager Express（Unified CME）
  - サードパーティ製 IP PBX
  - Voice over IP（VoIP）ゲートウェイを備えたレガシー PBX。
- 集中型呼処理サイトと、それに関連したすべてのリモート サイト。

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

- 一般的に、トランクおよびダイヤル プラン集約のための集中型プラットフォームが導入されます。このプラットフォームには、マルチサイトの分散型呼処理配置におけるクラスタ間コール ルーティングおよびダイヤル プランを集約するために Session Initiation Protocol（SIP）プロキシ サーバも使用できますが、通常は Cisco Unified Communications Manager Session Management Edition（SME）のクラスタです。
- 集中型サービスには以下のものがあります。
  - 集中型 PSTN アクセス
  - 集中型ボイスメール
  - 集中型会議

  これらのサービスは中央に配置できるため、一元管理とスケール上の利点があります。エンド ユーザの状態（たとえば、Cisco IM and Presence）を追跡する必要のあるサービスは、サービスを提供するユーザに対して Unified CM クラスタに接続されている必要があります。
- 同じサイト内のデバイス間の広帯域オーディオ（G.711 または G.722 など）、異なるサイトのデバイス間の狭帯域オーディオ（G.729 など）。
- 同じサイト内のデバイス間の広帯域ビデオ（4CIF または 720p での 1.5 Mbps から 1080p での 2 Mbps など）、異なるサイトのデバイス間の狭帯域ビデオ（448p または CIF での 384 kbps）。
- 最大 1.5 Mbps 以上の WAN リンク速度。速度が 1.5 Mbps 未満の WAN 接続ではビデオを *推奨しません*。
- コール アドミッション制御は、Enhanced Locations CAC によって実現されます。

IP WAN は、分散型呼処理のサイトをすべて相互接続します。一般に、PSTN は、IP WAN 接続に障害が起きたか、使用可能な帯域幅がすべて消費されてしまった場合に、サイト間のバックアップ接続の役目を果たします。PSTN のみで接続されているサイトは、独立サイトであり、分散型呼処理モデルには含まれません（キャンパス配置（10-10 ページ）を参照）。

IP WAN の接続オプションは、次のとおりです。

- 専用回線
- フレーム リレー
- 非同期転送モード（ATM）
- ATM とフレーム リレーのサービス インターワーキング（SIW）
- マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）
- Voice and Video Enabled IP セキュリティ プロトコル（IPSec）音声およびビデオ対応 IPSec VPN（V3PN）

分散型呼処理モデルのベスト プラクティス

分散型呼処理を使用するマルチサイト配置には、単一サイトと同じ、または集中型呼処理を使用するマルチサイト配置と同じ要件が少なからずあります。分散型呼処理モデルについては、ここでリストされているベスト プラクティスに加えて、他のモデルのベスト プラクティスにも従ってください（キャンパス配置（10-10 ページ）および集中型呼処理を使用するマルチサイト配置（10-13 ページ）を参照）。

分散型呼処理配置のダイヤル プラン集約プラットフォーム

Cisco Unified Communications Manager Session Management Edition（SME）クラスタまたは Session Initiation Protocol（SIP）プロキシ サーバを使用して、マルチサイト分散型呼処理配置におけるクラスタ間コール ルーティングおよびダイヤル プランの集約を提供できます。これらのトランクおよびダイヤル プラン集約デバイスの使用には、次のベスト プラクティスが適用されます。

Unified CM Session Management Edition クラスタ

Cisco Unified Communications Manager Session Management Edition は、分散型呼処理配置におけるクラスタ間コール ルーティングおよびダイヤル プランの集約で一般的に使用されています。クラスタ間コール ルーティングは、標準の数字ルート パターンの使用に基づく数値、またはクラスタ間検索サービス（ILS）および Global Dial Plan Replication（GDPR）の使用に基づく URI と数値にすることができます（グローバル ダイヤル プラン レプリケーション（14-51 ページ）を参照）。Unified CM Session Management Edition は Unified CM と同じコードとユーザ インターフェイスを使用しますが、複数のトランク プロトコル（SIP、H.323、および MGCP）、ならびに高度なトランク、ディジット操作機能、およびコール アドミッション制御機能のサポートを利用します。Unified CM Session Management Edition クラスタ配置は、通常は多くのトランク（SIP トランクを推奨。Cisco Unified CM トランク（6-1 ページ）を参照）で構成され、Unified Communications エンドポイントはありません。Unified CM Session Management Edition クラスタでは、Unified CM クラスタに利用できるすべてのハイ アベイラビリティ機能（WAN を介したクラスタリング、および [すべての Unified CM ノードで実行（Run on all Unified CM Nodes）] など）を使用できます。

SIP プロキシの配置

Cisco Unified SIP Proxy など、SIP プロキシは、コール ルーティングおよび SIP シグナリング正規化を提供します。

SIP プロキシの使用には、次のベスト プラクティスが適用できます。

- SIP プロキシの適切な冗長性を確保します。
- SIP プロキシのキャパシティが、ネットワークに必要なコール レートおよびコール数に対応していることを保証します。

（注）　Session Management Edition（SME）は Unified CM と同じコードと GUI を使用し、ILS、GDPR、および Enhanced Locations Call Admission Control（ELCAC）などのクラスタ間機能も共有できるため、SME は、マルチサイトの分散型コール処理配置の推奨されるトランクとダイヤル プランの集約プラットフォームです。

分散型呼処理モデルのリーフ Unified Communication システム

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

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

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

表 10-4 は、推奨される呼処理エージェントを示しています。

表 10-4　推奨される呼処理エージェント

呼処理エージェント	推奨規模	説明
Cisco Unified Communications Manager Express（Unified CME）	最大 450 台の電話機	• 小規模なリモート サイト用 • キャパシティは Cisco IOS プラットフォームに依存する • SIP トランクを推奨
Cisco Business Edition 6000	最大 2,500 台の電話機	• 小中規模サイト用 • 集中型呼処理をサポートする • 分散型呼処理をサポートする • SIP トランクを推奨
Cisco Business Edition 4000	最大 200 台の電話機	• 小規模なサイト用 • 集中型呼処理をサポートする
Cisco Unified Communications Manager（Enterprise または Business Edition 7000）	50 ～ 40,000 台の電話機	• Unified CM クラスタの規模に応じて、小規模から大規模までのサイト • 集中型呼処理をサポートする • 分散型呼処理をサポートする • SIP トランクを推奨
IP PBX	PBX に依存する	• 一般に IP PBX は、SME への接続に使用できる SIP トランクを使用
VoIP ゲートウェイを備えた従来の PBX	PBX に依存する	• IP WAN コール数と機能は、PBX と VoIP ゲートウェイを接続するプロトコルおよびゲートウェイ プラットフォームによって異なる • SIP トランクは、VoIP ゲートウェイと SME の間で推奨

Unified CM Session Management Edition

Cisco Unified CM Session Management Edition（SME）は、マルチサイト分散型呼処理配置で推奨されるトランクとダイヤル プランの集約プラットフォームです。SME は基本的に、トランク インターフェイスだけを使用し、IP エンドポイントを使用しない Unified CM クラスタです。このクラスタには、リーフ システムと呼ばれる、複数のユニファイド コミュニケーション システムを集約できます

Cisco Unified CM Session Management Edition は、次のトランク プロトコルをサポートします。

- SIP クラスタ間トランク
- SIP トランク
- H.323 Annex M1 クラスタ間トランク
- ゲートウェイへの H.323 トランク
- ゲートウェイへの MGCP トランク

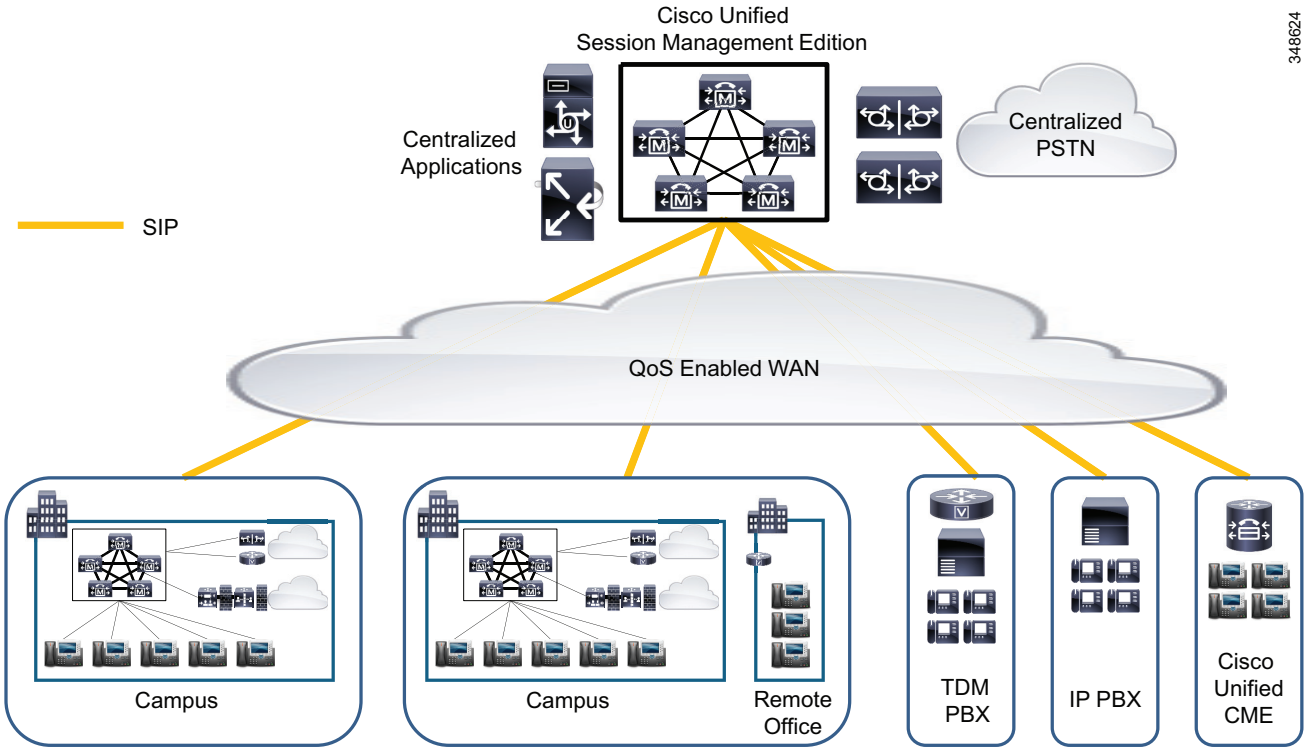
SIP が H.323 および MGCP トランクを介して追加の機能を提供するため、SIP トランクは推奨される SME およびリーフ Unified Communications システムです（詳細については、Cisco Unified CM トランク（6-1 ページ）の章を参照してください）。

Cisco Unified CM Session Management Edition は、次のコール タイプをサポートします。

- ボイス コール
- ビデオ コール
- 暗号化されたコール
- FAX コール

また、Unified CM Session Management Edition を使用して、PSTN のほか、PBX、集中型のユニファイド コミュニケーション アプリケーションなどのサードパーティのユニファイド コミュニケーション システムに接続できます（図 10-8 を参照）。標準の Unified CM クラスタと同様に、サードパーティ デバイスからの Unified CM Session Management Edition への接続は、実稼働環境で使用する前に相互運用性をテストしたシステムである必要があります。

図 10-8　Unified CM Session Management Edition を使用したマルチサイト分散型呼処理配置



Unified CM Session Management Edition を配置する状況

次のいずれかの操作を行う場合は、Unified CM Session Management Edition（SME）を配置することを推奨します。

- 集中型ダイヤル プランの作成および管理

  他のすべてのユニファイド コミュニケーション システムに接続するために各ユニファイド コミュニケーション システムに別個のダイヤル プランおよびトランクを設定するのではなく、Unified CM Session Management Edition を使用すると、Session Management クラスタを指す簡潔なダイヤル プランおよびトランクをリーフのユニファイド コミュニケーション システムに設定できます。Unified CM Session Management Edition には、集中型ダイヤル プランと、他のすべてのユニファイド コミュニケーション システムに到達するためのこのプランに対応する情報が含まれています。

（注）　SME および Unified CM リーフ クラスタでクラスタ間検索サービス（ILS）および Global Dial Plan Replication（GDPR）を実行すると、ダイヤル プランの管理をさらに簡略化できます。これは、個々のディレクトリ番号、DN に対応する E.164 番号、ルート パターン（たとえば、内線番号範囲および外線番号範囲）、および URI を ILS サービスを使用して配信できるためです。このアプローチでは、必要なルート パターンの数を減らし、それぞれ一意の番号範囲のルート パターンではなく、呼制御システム（Unified CM クラスタなど）ごとに 1 つの SIP ルート パターンにすることで、ダイヤル プランの管理を簡略化します。ILS および GDPR の詳細については、クラスタ間検索サービス（ILS）および Global Dial Plan Replication（GDPR）（10-34 ページ）を参照してください。

- 集中型 PSTN アクセスの提供

  Unified CM Session Management Edition を使用すると、1 つ（または複数）の集中型 PSTN トランクに PSTN アクセスを集約できます。集中型 PSTN アクセスには一般に、ブランチベースの PSTN 回線の削減または排除を伴います。

- アプリケーションの集中化

  Unified CM Session Management Edition の配置によって、会議やボイスメールなどの一般に使用されるアプリケーションを直接 Session Management クラスタに接続できるため、複数のトランクの管理によるリーフ システムへのオーバーヘッドが軽減されます。

- Unified Communications システムに移行するために PBX を集約

  Unified CM Session Management Edition は、レガシー PBX から Cisco Unified Communications システムへの移行の一環として、複数の PBX の集約ポイントを提供できます。ILS GDPR を導入する場合、各サードパーティ製システムでサポートされている番号範囲や URI を ILS GDPR にインポートし、SIP ルート パターンおよび対応する SIP トランクを介して到達できるようにすることもできます。

Unified CM Session Management Edition と標準の Unified CM クラスタの相違

Unified CM Session Management Edition ソフトウェアは、Unified CM と同じです。Unified CM Session Management Edition は、多数のトランクツートランク接続をサポートするように設計されているため、次に示す設計上の考慮事項に従う必要があります。

容量（Capacity）

Unified CM Session Management クラスタは、リーフ Unified Communications システム間（たとえば、Unified CM クラスタと PBX 間）、集中型 PSTN 接続間、および集中型アプリケーションへの予想される BHCA トラフィック ロードに基づいて正確にサイジングすることが重要です。使用している Unified Communications システムでのユーザの平均的な BHCA およびコール保留時間を判断し、その情報をシスコ アカウント システム エンジニア（SE）またはシスコ代理店と共有して、Unified CM Session Management Edition クラスタの規模を適切に決定してください。SME サイジングの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

トランク

SME は SIP、H.323、および MGCP トランクをサポートしますが、Cisco Unified CM 8.5 およびそれ以降のリリースを実行する SME および Unified CM リーフ クラスタのトランク プロトコルとして SIP を使用することを推奨します。

SIP トランクは、次のようなトランク設計と Unified Communications 配置を大幅に簡素化する独自の機能を多数提供します。

- すべての Unified CM ノードで実行
- OPTIONS ping
- 受信オファーのコーデック プリファレンスの受け入れ
- 相互運用のために SIP メッセージと Session Description Protocol（SDP）の内容の変更を可能にする Lua スクリプト

SME クラスタで SIP トランクのみを使用すると、「メディア トランスペアレント」クラスタを展開できます。ここでは必要に応じて、メディア リソースが SME ではなく、エンドまたはリーフ Unified Communications システムによって挿入されます。WAN を介してクラスタリングする場合、SIP トランクのみを使用すると、SME ノード間で拡張ラウンド トリップ時間（RTT）を使用できるようにもなります。

Unified CM リーフ クラスタの SIP トランクと SME SIP トランクは両方ともに、[ベスト エフォート Early Offer（Best Effort Early Offer）] トランクとして設定する必要があります。SIP トランクと [ベスト エフォート Early Offer（Best Effort Early Offer）] の詳細については、Cisco Unified CM トランク（6-1 ページ）の章を参照してください。

メディア リソース

MTP またはトランスコーダなどのメディア リソースは、コールが正常に続行するために必要で、これらのリソースがリーフ Unified Communications システムで可能な限り割り当てられる必要があります。SME トランク メディア リソースが SME クラスタを通過するコールに使用される場合、メディア パス コールが SME メディア リソースを介してヘアピンします。SIP トランクのみと、[ベスト エフォート Early Offer（Best Effort Early Offer）] または [MTP-less Early Offer] のいずれかを使用することにより、メディア リソースを使用せずに、SME クラスタを配置できます。メディア リソースが必要な場合は、リーフ Unified Communications システムで割り当てることができます。

WAN を介したクラスタリング

SME の配置では、SME クラスタ ノード間で最大 500 ミリ秒の拡張ラウンドトリップ時間（RTT）をサポートできます（図 10-9 を参照）。この拡張 RTT は SME クラスタのみに適用され（標準の Unified CM クラスタ設計の最長 RTT は 80 ミリ秒です）に適用され、次の設計上の制限があります。

- WAN を介したクラスタリングによる SME 配置の拡張ラウンドトリップ時間は、SIP トランクが SME クラスタで設定されている場合のみサポートされます。すべての SIP トランクは、[ベスト エフォート Early Offer（Best Effort Early Offer）] または [MTP-less Early Offer] のいずれかとして設定され、コールが SME クラスタ内のノード間でルーティングされないように [すべての Unified CM ノードで実行（Run on all Unified CM Nodes）] 機能を使用する必要があります（詳細については、Cisco Unified CM トランク（6-1 ページ）の章を参照してください）。MGCP、SCCP、および H.323 プロトコルは、WAN を介したクラスタリングによる SME 配置の拡張ラウンドトリップ時間をサポートしていません。
- エンドポイントまたは CTI デバイスは SME クラスタに設定、または登録されません。
- MTP、信頼されたリレー ポイント（TRP）、RSVP エージェント、トランスコーダなどのメディア リソースは、SME クラスタに設定または登録されません（Unified CM ノードでホストされているメディア リソースを無効にするには、クラスタ内の各ノードの IPVMS サービスを非アクティブにします）。
- サイト間の Intra-Cluster Communication Signaling（ICCS）トラフィックに最低 1.544 Mbps（T1）の帯域幅が必要です。
- Intra-Cluster Communication Signaling（ICCS）トラフィックに必要な帯域幅に加え、パブリッシャとあらゆるリモート サブスクライバ ノード間のデータベースおよびその他のサーバ間トラフィック用に、最低でも 1.544 Mbps（T1）の帯域幅が必要になります。

  他のすべての SME 設計と同様に、SME 設計は、配置前にシスコの SME チームによる確認と承認が必要になります。

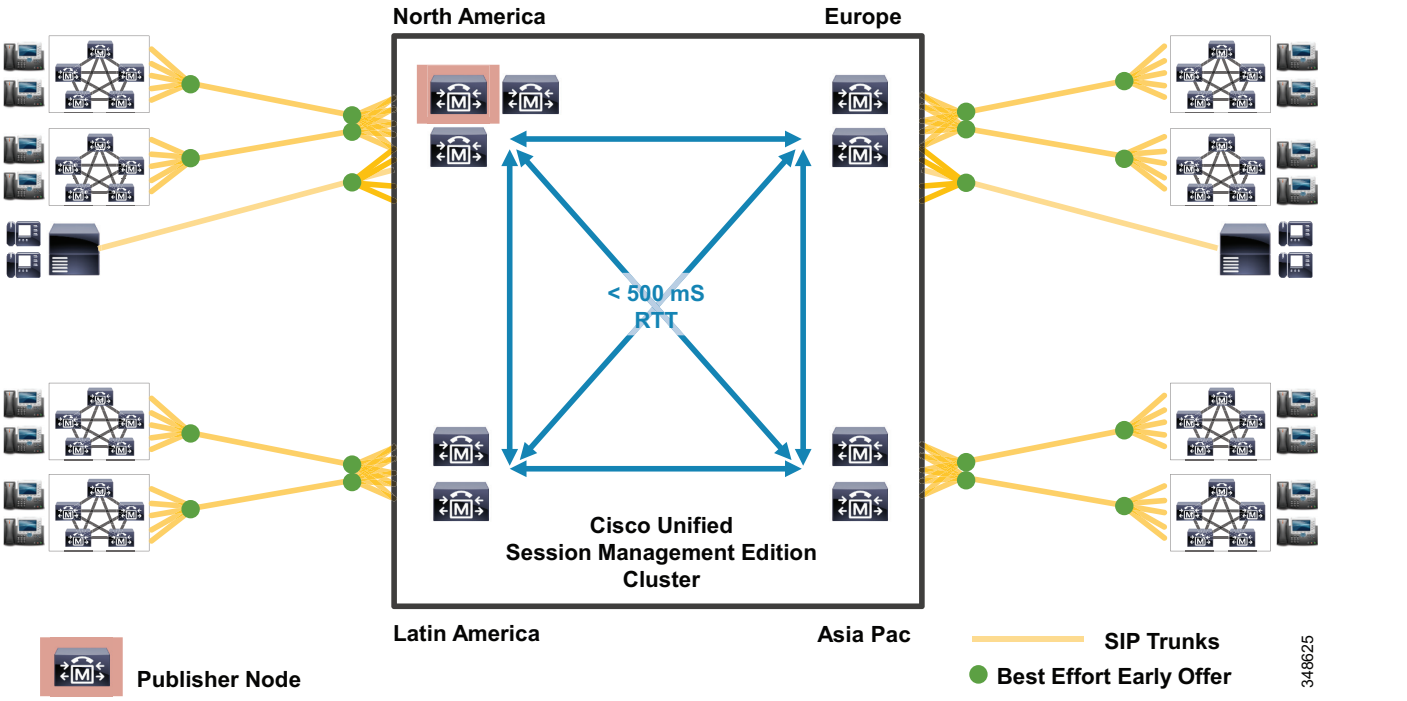
（注）　SME クラスタのアップグレード プロセスは 2 つの主要部分で構成されています。1 つめはバージョンのスイッチオーバーで、呼処理ノードがリブートされ、新しいソフトウェア バージョンで初期化され（サーバあたり約 45 分かかります）。2 つめはデータベースの複製で、サブスクライバのデータベースがパブリッシャ ノードのデータベースと同期化されます。このデータベース複製フェーズの完了にかかる時間は、パブリッシャ ノードとサブスクライバ ノードの間の RTT とクラスタ内のサブスクライバの数によって異なります。データベース複製プロセスにはサブスクライバの呼処理機能への影響はほとんどなく、通常の SME クラスタ処理中にバックグラウンド処理として実行できます。データベース複製フェーズ中に SME クラスタ設定に変更を加えないようにしてください。これにより、複製が完了するまでの時間が遅くなります。

拡張 RTT を使用して SME クラスタを配置する場合、クラスタをアップグレードする前に、パブリッシャ ノードで次の Admin レベル CLI コマンドを実行します。

```
utils dbreplication setprocess 40
```

このコマンドは、複製設定のパフォーマンスを向上させ、データベース複製に要する時間が短縮されます。

図 10-9　拡張ラウンド トリップ時間を使用した WAN を介した Unified CM Session Management Edition のクラスタリング



Unified CM バージョン

すべての Unified CM リーフ クラスタおよび SME クラスタで最新の Cisco Unified Communications システム リリースと SME クラスタを使用すると、Unified Communications 配置は、Codec Preference Lists、クラスタ間検索サービス（ILS）、Global Dial Plan Replication（GDPR）、Enhanced Locations Call Admission Control（ELCAC）などの共通のクロス クラスタ機能からメリットを得ることができます。すべてのクラスタ上で最新の Unified Communications バージョンにアップグレードしない場合には、最小推奨バージョンは SIP トランクを使用した Cisco Unified CM 8.5 です。このバージョンには、Unified CM および Session Management Edition クラスタを介したコール ルーティングを改善し、簡略化する機能が含まれているからです。

相互運用性

ほとんどのベンダーが標準に準拠していますが、各ベンダーによるプロトコルの実装には相違があります。標準の Unified CM クラスタの場合と同様に、実稼働環境にシステムを配置する前に、サードパーティの未検証のユニファイド コミュニケーション システムとのエンドツーエンドの相互運用性テストを実施することを強く推奨します。相互運用性テストでは、Unified CM Session Management クラスタを介したシスコおよびサードパーティのリーフ システムからのコール フローと機能を検証します。シスコの相互運用性チームによってテストされたサードパーティのユニファイド コミュニケーション システムの情報を得るには、次の Cisco Interoperability Portal サイトで提供している情報を参照してください。

https://www.cisco.com/c/en/us/solutions/enterprise/interoperability-portal/interOp_ucSessionMgr.html

SIP トランクの相互運用性の問題に対して、Lua スクリプトは、発着信 SIP メッセージおよび SDP の内容を変更するために使用できます。

着信コールと発信コールのロード バランシング

Session Management クラスタ内の Unified CM サーバ間に着信コールと発信コールが均等に分散されるよう、Unified CM Session Management Edition およびリーフのユニファイド コミュニケーション システムのトランクを設定します。原則として、使用可能な場合は、[すべての Unified CM ノードで実行（Run on All Unified CM Nodes）] を常に有効にしてください。トランク コールのロード バランシングの詳細については、Cisco Unified CM トランク（6-1 ページ）の章を参照してください。

設計のガイドラインとサポート

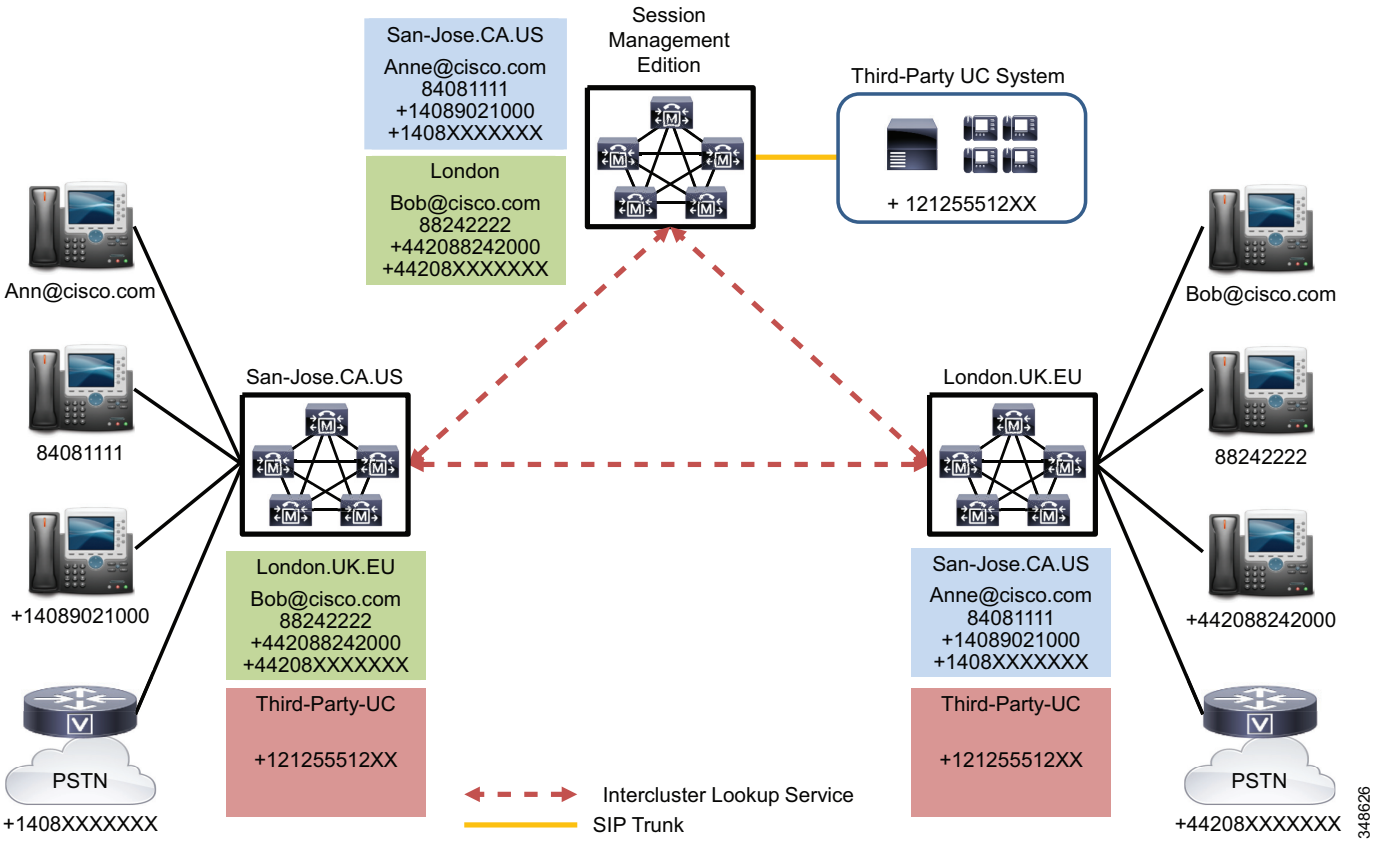
Unified CM Session Management Edition の設計と配置のトランク設定の詳細については、Cisco Unified CM トランク（6-1 ページ）の章を参照してください。

（注）　配置する前に、Unified CM Session Management Edition の設計は、担当のシスコ SE が Cisco Unified CM Session Management チームと一緒に確認します。

クラスタ間検索サービス（ILS）および Global Dial Plan Replication（GDPR）

Global Dial Plan Replication（GDPR）は、クラスタ間検索サービス（ILS）を使用して、参加している ILS 対応クラスタ間のダイヤル プラン情報を共有します。GDPR を使用すると、関連付けられた URI、+E.164 番号、企業番号、+E.164 パターン、企業パターン、および PSTN フェールオーバー番号に関する情報を各クラスタが配信できるようになります。参加している各クラスタは、番号または URI が存在するクラスタ（またはエンド Unified Communications システム）を識別する GDPR および対応するルート文字列によってアドバタイズされたすべての番号と URI を含む共通の Global Dial Plan カタログを共有します（図 10-10 を参照）。

図 10-10　ILS および GDPR の番号、パターン、および URI 配信



GDPR を使用した場合、各クラスタはダイヤル プラン情報（番号と URI）を*ルート文字列*として知られるロケーション属性にアドバタイズします。コールが英数字の URI に対して発信されると、Unified CM はその URI がクラスタ内のデバイスに関連付けられているかどうかを確認します。関連付けられていない場合、Unified CM は GDPR カタログでその URI を検索します。Global Dial Plan カタログで一致が検索されると、GDPR は番号または URI が存在するクラスタに対応するルート文字列を返します。Unified CM は、返されたルート文字列を既存の SIP ルート パターンおよび対応する SIP トランクに照合するための候補として使用します数値の宛先の場合、best-match 番号分析によって GDPR から学習した宛先との一致結果が返されると、学習した宛先が存在するクラスタに対応するルート文字列を再度使用して、コールのルーティング先とする SIP トランクが決定されます。（図 10-11 および図 10-12 を参照。）

図 10-11　ILS および GDPR の番号、パターン、および URI ルックアップ

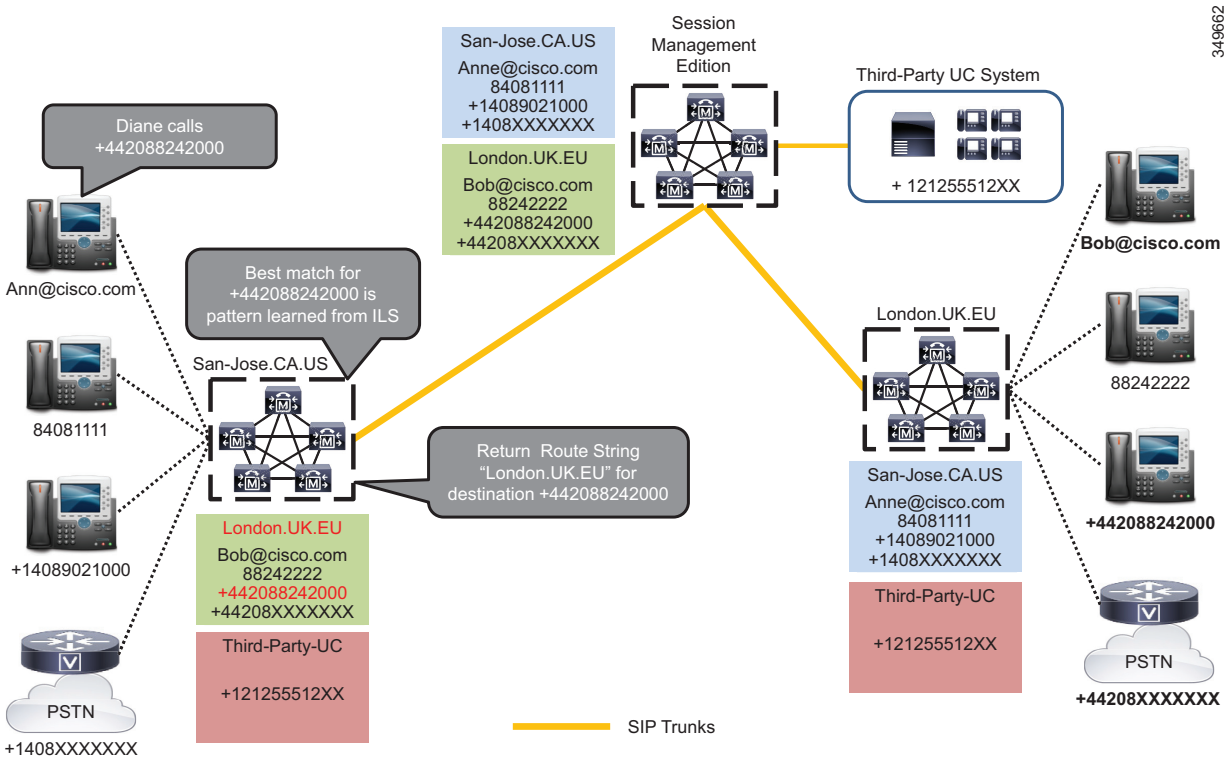
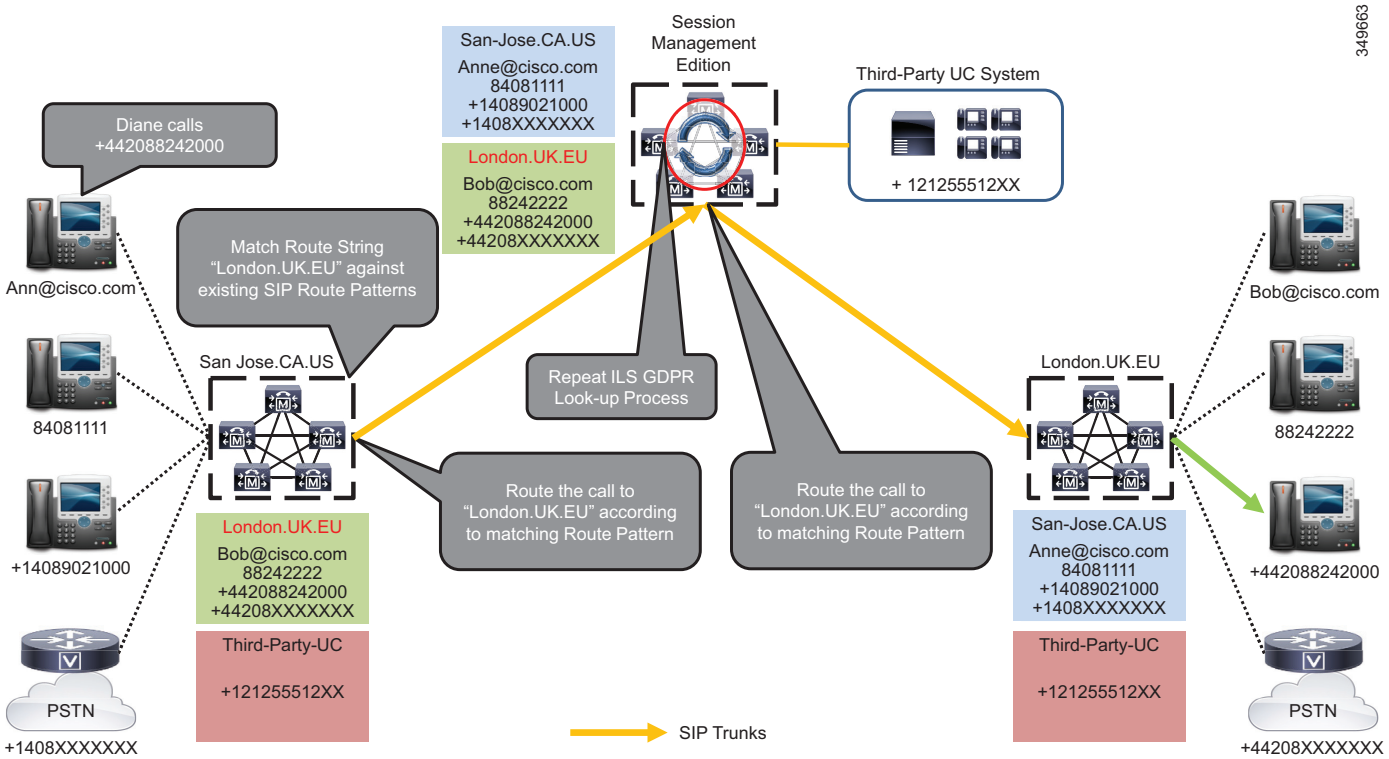


図 10-12　ILS および GDPR のコール ルーティング



ILS および GDPR の利点

GDPR を使用することは、数字ルート パターンで標準のダイヤル プランを使用することとは大きく異なります。Unified Communications ネットワーク内でそれぞれの一意の番号範囲のルート パターンを必要とする代わりに、GDPR は、番号、番号パターン、および URI を配信し、1 つの SIP ルート パターンだけが Unified Communications ネットワーク内の各クラスタで必要になります。サードパーティ製ユニファイド コミュニケーション システム（および ILS と GDPR をサポートしない Unified CM クラスタ）に関連付けられた番号および URL は、GDPR にカタログとしてインポートされ、各ユニファイド コミュニケーション システムに対応するルート文字列で ILS を介して配信できます。番号グループに対応する個々の番号とルート パターンの両方が GDPR でアドバタイズできるため、番号と番号範囲をこの数字ルート パターンから取り除くと、GDPR は単純かつ簡潔に、多くの番号範囲で高度に細分化されたダイヤル プランをサポートできます。ILS と GDPR を使用している各クラスタは、参加している他のクラスタからアドバタイズされた個々の番号と番号範囲をブロックし、消去できます。

各 GDPR の番号タイプ（+E.164 番号、企業番号、+E.164 パターン、または企業パターン）は、ILS で学習したときに特定のパーティションに置かれ、ユーザ単位またはデバイス単位のサービス クラスが番号タイプのパーティションおよびコーリング サーチ スペースに基づいて適用されるようにします。

Cisco Unified Border Element は、Unified CM SIP トランクを介したコール セットアップ時に、Cisco Unified Border Element に送信される GDPR ルート文字列値に一致するダイヤル ピアを使用した番号および URI のコール ルーティングもサポートしています。Cisco IOS ダイヤル ピアと一致する GDPR ルート文字列は、Cisco IOS releases 15.3(3)M、15.4(1)T（ISR）、15.3(3)S（ASR）およびそれ以降のリリースでサポートされます。

コラボレーション エッジの配置

Enterprise Unified Communications ネットワークと外部の間の境界は、*コラボレーション エッジ*とも呼ばれます。外部から企業ネットワークへのアクセスには、いくつかの形式があります。たとえば、ユーザは自宅勤務の在宅勤務者、企業への Wi-Fi インターネット アクセスが可能なモバイル ワーカー、または IP PSTN 間でコールを発信するユーザやインターネットを介して他のビジネス間でコールを発信するユーザである可能性があります。コラボレーション エッジに必要な Unified Communications 機器は、必要とされる企業アクセスのタイプに大きく左右されます。これは、大きく 3 つのカテゴリに分類できます。

- VPN ベースのアクセス
- VPN-less アクセス
- Business-to-Business（B2B）コミュニケーション
- IP PSTN アクセス

コラボレーション エッジのこれら 4 つの配置オプションについては、これ以降の項で説明します。

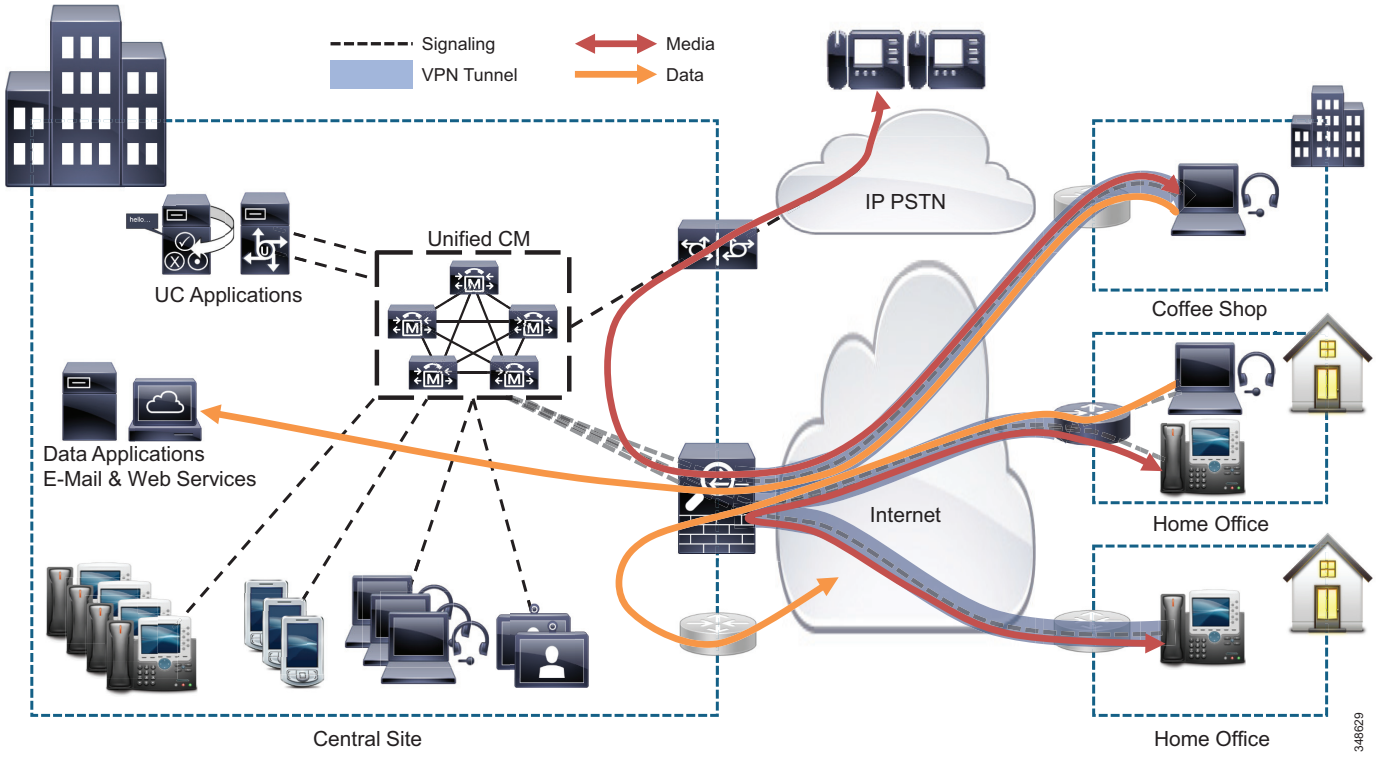
VPN ベースの企業アクセスの配置

企業ネットワークへの VPN アクセスは、今日の最も一般的な企業アクセスの形式で、いくつかの方法で提供することが可能です。

- ラップトップ、タブレット、およびスマート フォンなどのモバイル デバイスを企業ネットワーク内の Unified Communications サービス（Unified CM、Cisco IM and Presence、Cisco Unity など）およびビジネス アプリケーション サービス（社内 E メール システムおよび内部 Web サイトなど）にアクセスするように Cisco AnyConnect VPN クライアントを配置できます。この VPN 接続が確立されている状態で、Cisco Jabber および Cisco IP Communicator などの Unified Communications ソフト クライアントは Unified CM に登録し、企業デバイス間で音声、ビデオ、および暗号化されたコールを発信できます。
- 1 つ以上の企業デバイスを持つホーム オフィス ワーカーは、Cisco Virtual Office（CVO）の Integrated Services Router（ISR）を配置して、VPN を介して企業ネットワークを自宅に拡張できます。CVO VPN 接続は、接続デバイスを企業ネットワーク内の Unified Communications サービス（Unified CM、Cisco IM and Presence、Cisco Unity など）およびビジネス アプリケーション サービス（社内 E メール システムおよび内部 Web サイトなど）にアクセスできるようにします。CVO VPN 接続が確立されている状態で、Unified Communications ソフト クライアントと IP Phone は Unified CM に登録し、企業デバイス間で音声、ビデオ、および暗号化されたコールを発信できます。
- Cisco Unified IP Phone の Cisco VPN クライアントは、Cisco Unified IP Phone モデルのサブセットの企業アクセスを提供します。Cisco Unified IP Phone の Cisco VPN クライアントをサポートするデバイスの詳細については、コラボレーション エンドポイント（8-1 ページ）の章を参照してください。電話機の VPN クライアントは電話機専用のトンネルを作成し、Unified CM との登録、さらに企業デバイス間での音声、ビデオ、および暗号化されたコールを発信できるようにします。電話機の PC ポートに接続されたコンピュータは、VPN クライアント ソフトウェアを使用して、企業への独自のトンネルの認証と確立を受け持ちます。

VPN アクセスは、デバイスから VPN ヘッドエンドへの安全で暗号化されたトンネルを作成して、企業内のすべての Unified Communications とビジネス アプリケーションへのアクセスをユーザに与えます。VPN ユーザ間のコールのインターネットおよびメディア宛てのトラフィックを含むすべてのトラフィックは、インターネットを介してデバイスから宛先に直接確立されるのではなく、企業ネットワークを常に通過する必要があります（図 10-13 を参照）。

図 10-13　VPN ベースのアクセス



上記のデバイスはすべて VPN クライアントを使用して、Cisco Adaptive Security Appliance（ASA 5500）または Cisco VPN 集約ルータなどの VPN ヘッドエンド プラットフォームを介して企業ネットワークに接続します。

VPN アクセス ソリューションの詳細については、次の URL で入手可能なユニファイド アクセスおよび BYOD のソリューション ガイド [英語] を参照してください。

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

VPN-less 企業アクセス

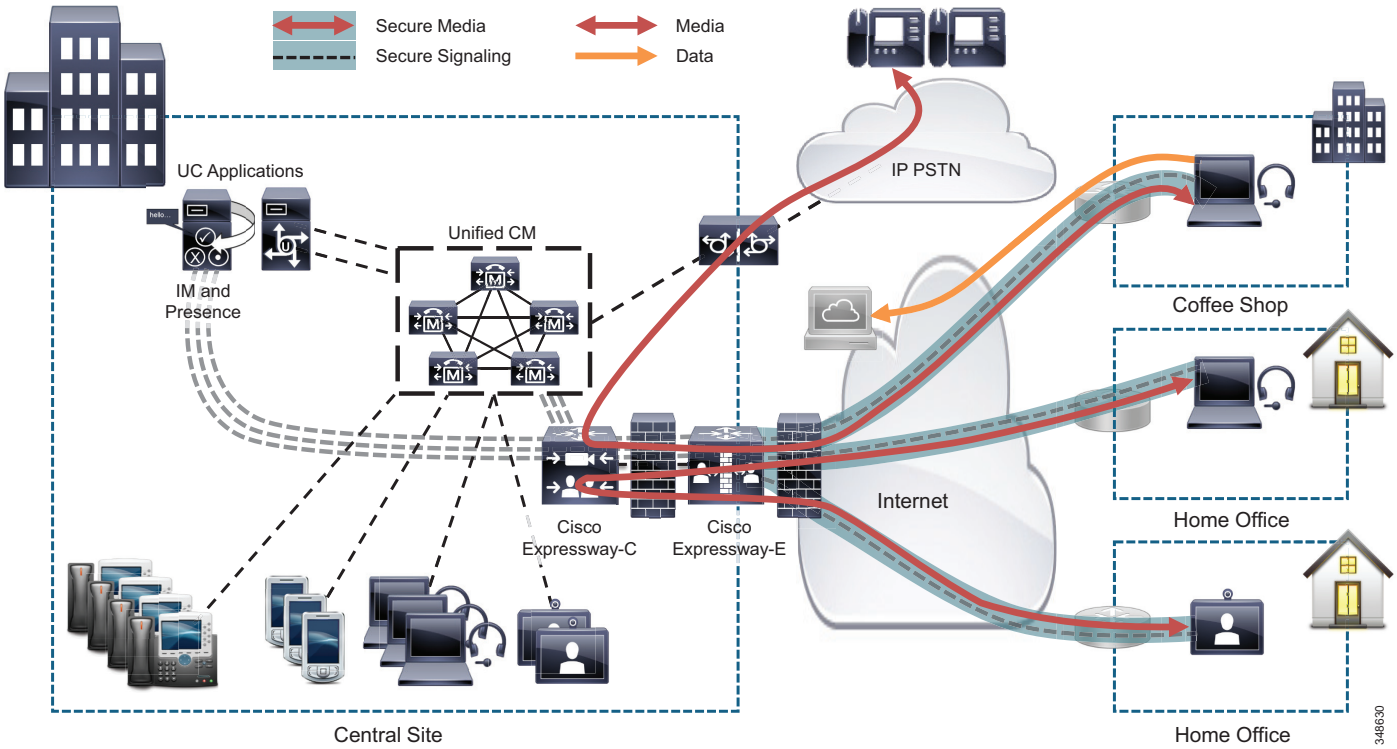
VPN-less クライアントは VPN トンネルを使用する代わりに、Cisco Expressway などの企業エッジ トラバーサル プラットフォームに安全で暗号化されたシグナリング パスを確立します。VPN-less クライアントは企業内で Unified CM に登録し、クライアントはエッジ トラバーサル プラットフォームへのセキュア チャネルを使用することによって、他の企業デバイスへのコールまたは企業 PSTN ゲートウェイを介する PSTN へのコールに対してインターネット経由の暗号化されたメディア パスを確立できるようになります。メディアはオプションで暗合されたままの状態にしておくことができますが、企業シグナリング内では通常、暗号化されていません。

VPN クライアントとは異なり、VPN-less クライアントは、Collaboration アプリケーションへのアクセスのみを提供します。企業内のビジネス アプリケーション（社内 E メールおよび内部 Web サイトなど）にはアクセスできず、インターネットへの接続は企業を介さず、デバイスから直接行われます。シスコの VPN-less クライアント アクセスは、エッジ トラバーサル プラットフォームとして Cisco Expressway を使用して配置できます。

この配置タイプは、Cisco Expressway-C および Expressway-E を使用します。Cisco Expressway E は、DMZ または公共のインターネットのどちらかに配置し、Cisco Expressway C から企業ネットワークの Unified CM クラスタで通信できます（図 10-14 を参照）。Cisco Expressway は、主に Cisco Jabber クライアントおよび TelePresence エンドポイントの VPN-less アクセスをサポートしています。音声、ビデオ、暗号化されたコール、および IM and Presence は、企業エンドポイント間でサポートされています。リモート VPN-less デバイス間のコールのメディアとシグナリングは、Cisco Expressway-C および Expressway-E を通過します。Cisco Expressway VPN-less 企業アクセスでサポートされているエンドポイント範囲固有の情報については、コラボレーション エンドポイント（8-1 ページ）の章を参照してください。Cisco Expressway の VPN-less クライアント アクセスの詳細については、次のサイトで入手可能なマニュアル [英語] を参照してください。

- https://www.cisco.com/c/en/us/solutions/collaboration/collaboration-edge-architecture/index.html
- https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html
- https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

図 10-14　Cisco Expressway とのコラボレーション エッジの VPN-less アクセス



Business-to-Business（B2B）コミュニケーション

Cisco Expressway と Cisco Unified Border Element（CUBE）の両方で、企業間におけるインターネットベースの Business-to-Business（B2B）ユニファイド コミュニケーション接続がサポートされます。Cisco Expressway と CUBE の両方で、Business-to-Business（B2B）コミュニケーション シグナリング用に SIP トランクまたは H.323 トランクが使用されます。Cisco Expressway では、ボイス コール、ビデオ コール、および IM とプレゼンスのフェデレーションがサポートされます（図 10-15 を参照）。CUBE では、ボイス コールとビデオ コールのみがサポートされます（図 10-16 を参照）。

図 10-15　Cisco Expressway による Business-to-Business（B2B）コミュニケーション

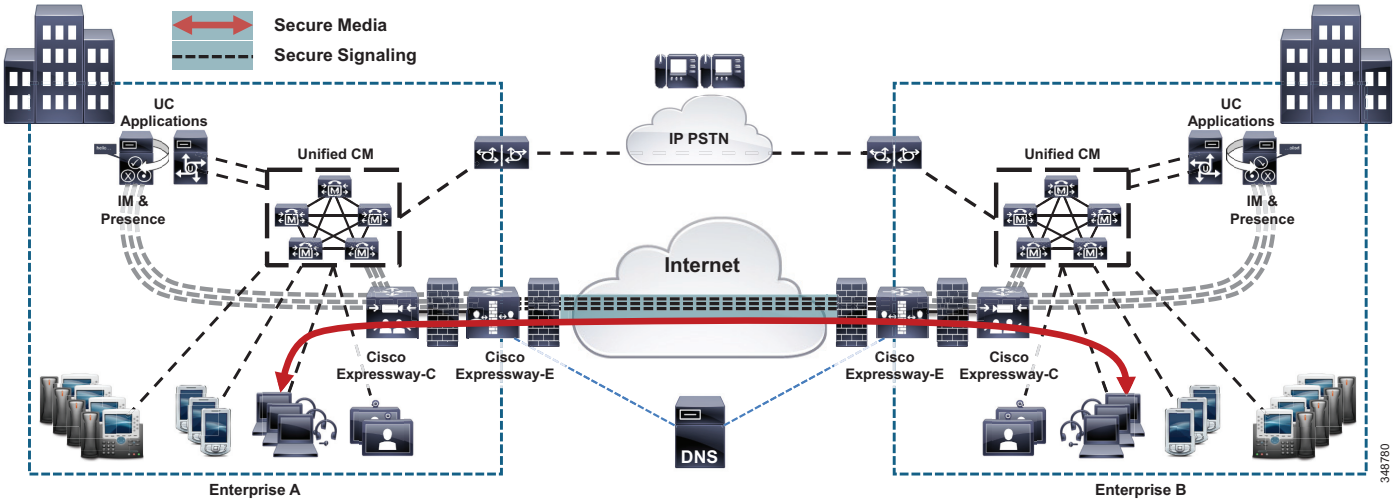
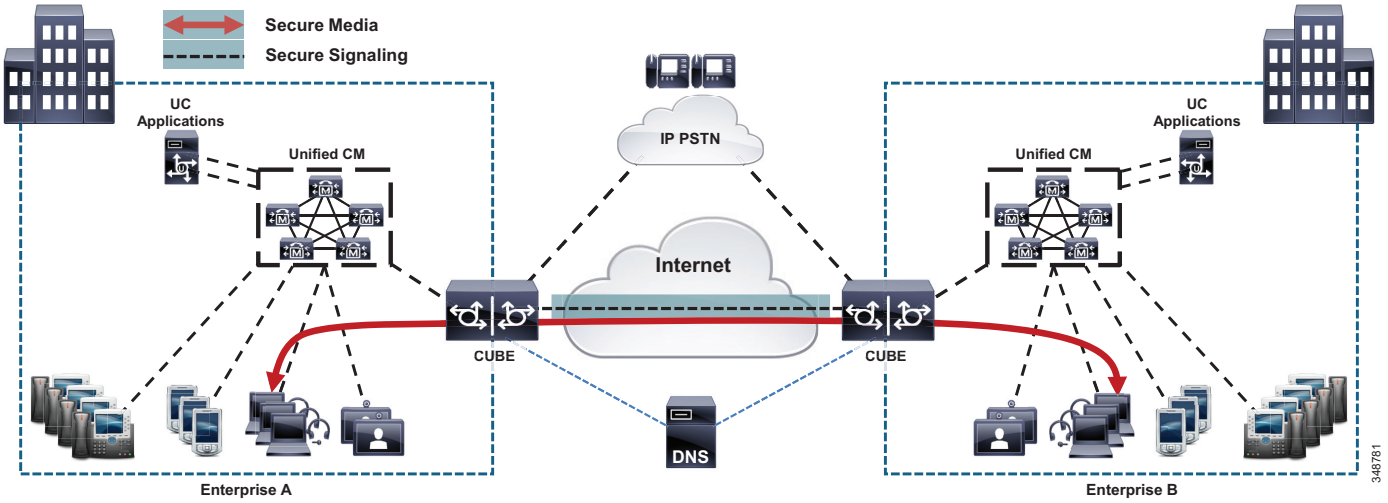


図 10-16　Cisco Unified Border Element（CUBE）による Business-to-Business（B2B）コミュニケーション



Cisco Expressway および Unified Border Element を使用する Business-to-Business（B2B）コミュニケーションの配置に関する詳細については、IP ゲートウェイ（5-15 ページ）を参照してください。

IP PSTN の配置

IP PSTN の配置はますます増大しており、徐々に既存の TDM ベースの PSTN アクセスを置き換えつつあります。SIP は、IP PSTN アクセス プロトコルとして一般に使用されており、現在多くのサービス プロバイダーが Cisco Unified Border Element などのセッション ボーダー コントローラを介して IP PSTN に音声専用のサービスを提供しています。セッション ボーダー コントローラは、SIP Back-to-Back User Agent（B2BUA）で、通常、各コールの音声メディアと SIP シグナリングの両方が Cisco Unified Border Element を流れるフロースルー モードで使用されます（図 10-17 を参照）。B2BUA がフロースルー モードであることから、Cisco Unified Border Element は、トランスレーティング、暗号化、コール録音アプリケーション用のメディア フォーキング、および相互運用に対して SIP メッセージや SDP 本文の内容を変更できるスクリプトのサポートも提供しながら、高度な QoS マーキングおよびコール アドミッション制御ポリシーを実行できます。Cisco Unified Border Element の機能の詳細については、次の URL で入手可能な『*Cisco Unified Border Element Data Sheet*』の最新バージョンを参照してください。

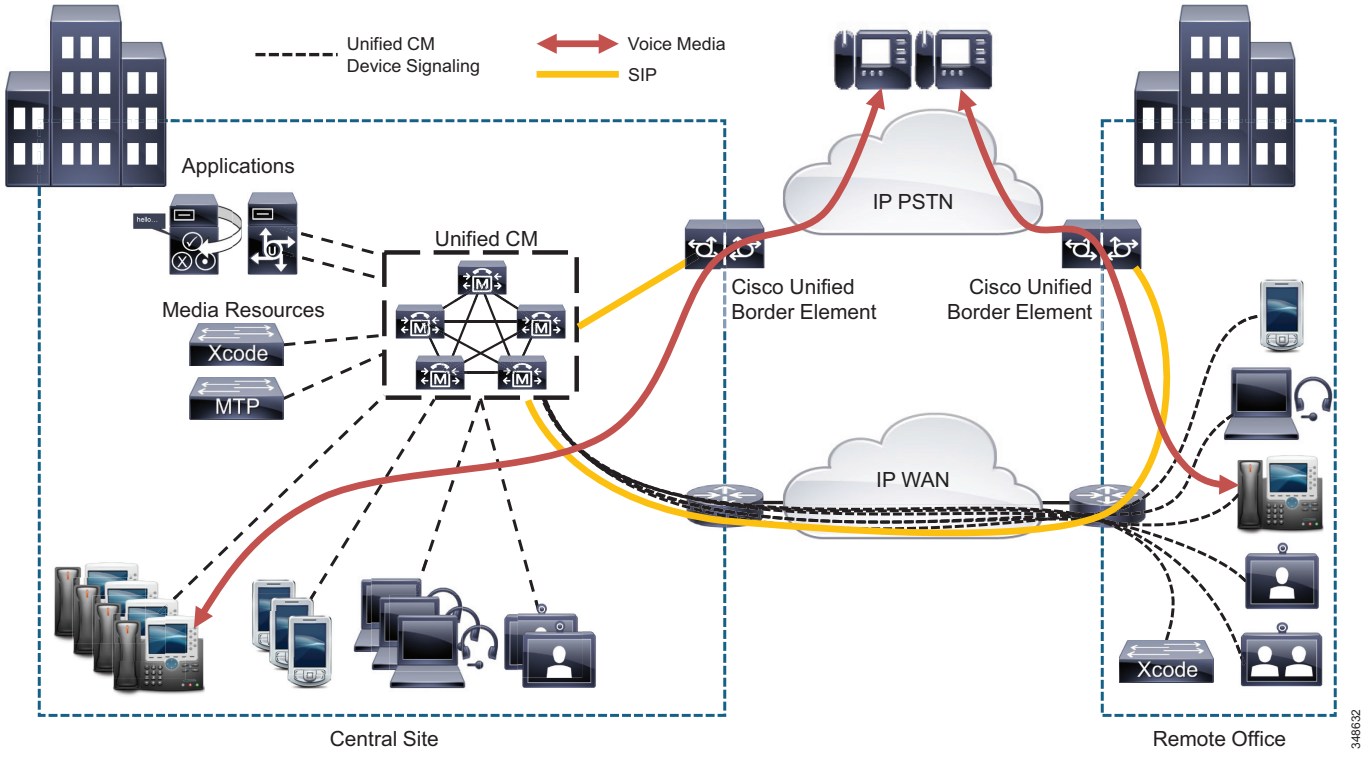
https://www.cisco.com/c/en/us/products/unified-communications/unified-border-element/index.html

Cisco Unified Border Element は、Cisco Integrated Services Router（ISR）から Cisco アグリゲーション サービス ルータ（ASR）までの幅広いシスコのルーティング プラットフォームでサポートされます。Cisco Unified Border Element は、ハードウェア プラットフォームに応じて、4 ～ 16,000 本の同時ボイス コールが可能なセッション拡張性を提供できます。Cisco Unified Border Element は、次のプラットフォームで冗長性も提供します。

- Cisco ISR プラットフォームでは、安定したアクティブ コールのメディア保護を含むボックス ツー ボックス冗長性を提供できます。
- Cisco ASR プラットフォーム。安定したアクティブ コールのために、メディアおよびシグナリングの保護（ステートフル フェールオーバー）によるボックス間またはボックス内の冗長性を提供できます。

（注） IP PSTN へのアクセスと VPN-less クライアントの企業へのアクセスを同じ Cisco Unified Border Element プラットフォームに配置できます。

図 10-17　コラボレーション エッジの IP PSTN アクセス



IP PSTN の地理的な配置オプション

SIP トランクは、必要なアーキテクチャに応じて、さまざまな方法で IP PSTN サービス プロバイダーに接続されます。この接続における最も一般的なアーキテクチャには、中央集中型トランクと分散型トランクの 2 つがあります。

中央集中型トランクは、Cisco Unified Border Element などのセッション ボーダー コントローラ（SBC）を使用し、1 つの論理接続を通してサービス プロバイダー（SP）に接続します（ただし、冗長性を確保するために複数の物理接続が存在する場合があります）。企業へのすべての IP PSTN コール、および企業からのすべての IP PSTN コールでは、このトランクのセットが使用され、ほとんどのコールに対して、メディアおよびシグナリングは企業 WAN を横断して、企業のデバイスを PSTN のものに接続します。

分散型トランクは、複数の論理接続経由でサービス プロバイダーに接続します企業の各支社は、サービス プロバイダーへの独自のローカル トランクを保有しています。分散型トランクでは、支社からのメディアは企業 WAN を通過する必要はなくなりましたが、ローカル SBC 経由でサービス プロバイダーへと直接流れることができます。

これらの接続モデルには、それぞれ利点と欠点があります。通常、中央集中型トランクは、物理的な機器および設定の複雑さの面でより容易に展開できます。分散型トランクには、メディアをローカル ハンドオフできる利点があり、またローカル プロバイダーからの番号の可搬性が高まります。また、一部の集中型および分散型 IP PSTN アクセスを結合するハイブリッド接続モデルでは、IP PSTN 配置形式の両方の利点が実現されます。

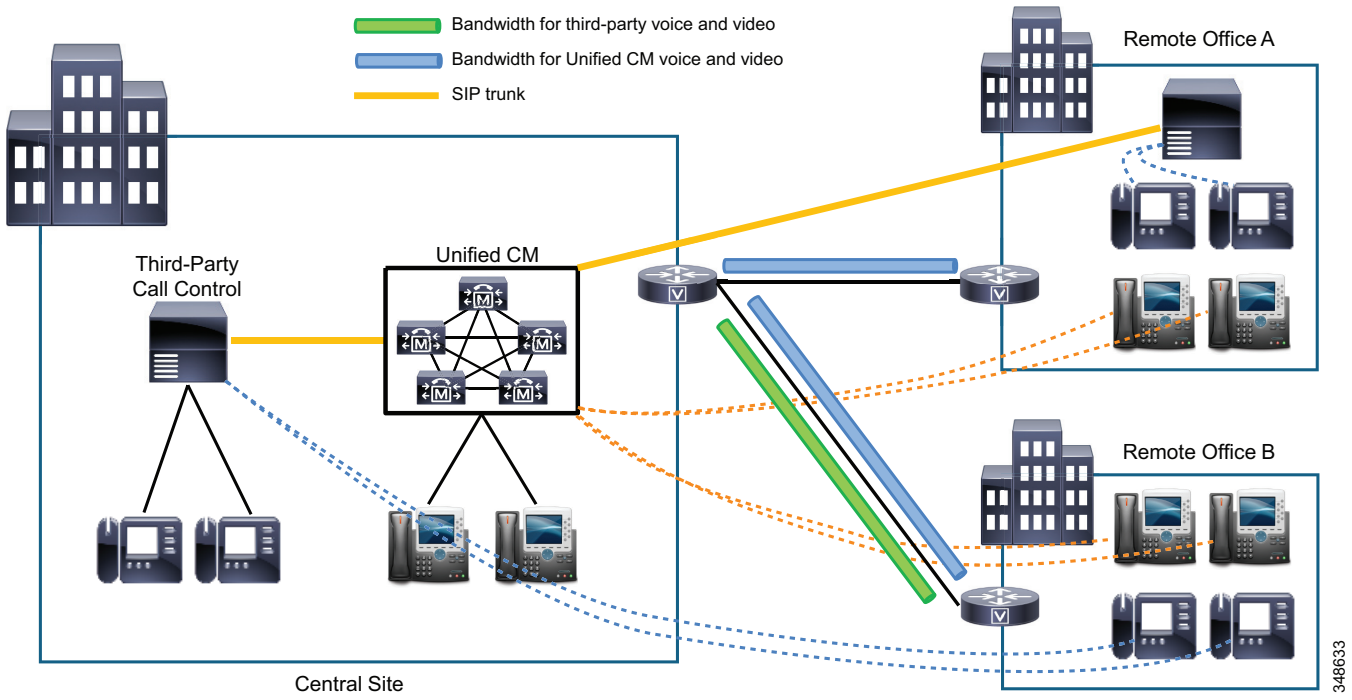
デュアル呼制御配置の設計上の考慮事項

一般に、エンドポイントが Cisco Unified CM とサードパーティ呼制御プラットフォームに登録された配置は、ダイヤル プランおよびコール アドミッション制御に関する任意のコラボレーション ソリューションの設計を複雑なものにします。これらのデュアル呼制御配置では、Unified CM とサードパーティ呼制御プラットフォームは、いずれもコール アドミッション制御に独立した機能を使用し、独立したダイヤル プランがあるため、複雑さの度合いは使用される配置モデルによって決まります（図 10-18 を参照）。

デュアル呼制御を備えたキャンパス配置では、コール アドミッション制御は必要なく、各呼制御システムのダイヤル プランは比較的単純です。つまり、エンドポイントが 1 台のシステムで検出できない場合は、コールは別のシステムに転送されます。標準のダイヤル プラン設定（コーリング サーチ スペースおよびパーティション）は、システム間のルーティング ループを防止するために使用できます。

マルチサイトの集中型呼処理配置では、通常、コール アドミッション制御の複雑さとダイヤル プランの複雑さとの間でトレードオフが発生します。Unified CM クラスタとサードパーティ呼制御プラットフォームが中央サイトのみに配置されている場合、ダイヤル プランは比較的単純ですが、各システムでコール アドミッション制御に使用される WAN 帯域幅を別個に考慮し、WAN に対してプロビジョニングする必要があります。サードパーティ製エンドポイントがあるリモート サイトに追加でサードパーティ製呼制御サーバを配置する場合、コール アドミッション制御の複雑さは、ダイヤル プランをより細分化すると回避されます。こうしたトレードオフについては、次の項で詳しく説明します。

図 10-18　集中型および分散型サードパーティ システムを使用したデュアル呼制御配置



デュアル呼制御配置のコール アドミッション制御に関する考慮事項

コール アドミッション制御では、呼処理コンポーネントの全体的なコール キャパシティおよびネットワーク帯域幅に基づいて、所定の時間にネットワーク上で許可するコール数を制限することにより、ネットワーク帯域幅のオーバーサブスクリプションを回避するメカニズムを提供します。

デュアル呼制御配置では、Unified CM とサードパーティ呼制御プラットフォームは、いずれもコール アドミッション制御に独立した機能を使用します。

Unified CM クラスタとサードパーティ呼制御プラットフォームが中央サイトのみに配置されたマルチサイトの集中型呼処理配置では、各プラットフォームがコール アドミッション制御に使用する帯域幅の WAN に考慮する必要があります。サードパーティ製エンドポイントがローカルに配置されたサードパーティ製呼制御システムに登録されたリモート サイトでは、これらのコール アドミッション制御の考慮事項を回避できます。

分散サードパーティ呼制御によるマルチサイト集中型 Unified CM 配置

サードパーティ エンドポイントが存在するすべてのサイトで、サードパーティ製呼制御システムを使用するデュアル呼制御配置モデルは、Unified CM コール アドミッション制御と強固に統合できます。これは、サードパーティ呼制御システムから Unified CM への SIP トランクを各サイトに使用し、そのサイトにある Unified CM エンドポイントと同じ Unified CM ロケーションでこの SIP トランクを設定することによって実行できます。しかし、この方法で Unified CM とサードパーティ呼制御のコール アドミッション制御の問題を解決する一方で、多数のサードパーティ製呼制御システムがプロビジョニングされ、ネットワークのダイヤル プランが細分化します。

集中型サードパーティ呼制御によるマルチサイト集中型 Unified CM 配置

Unified CM のように WAN を介して複数のサイトに存在するサードパーティ エンドポイントを提供するため、サードパーティ呼制御システムが中心になる場合があります。このタイプの配置では、サードパーティ呼制御システムは異なるサイトのサードパーティ製エンドポイント間のコールにコール アドミッション制御を提供します。同様に、集中型 Unified CM クラスタが、異なるサイトの Unified CM エンドポイント間のコールにコール アドミッション制御を提供します。Unified CM クラスタとサードパーティ製呼制御システムは独立したコール アドミッション制御機能を使用するため、Unified CM とサードパーティ製エンドポイントの両方が集中型呼制御配置にあるサイトで、Unified CM コール アドミッション制御とサードパーティ呼制御用の WAN に別々の帯域幅の量をプロビジョニングする必要があります。コールが同じサイトの Unified CM エンドポイントとサードパーティ製のエンドポイント間で発信された場合、コール アドミッション制御の帯域幅は、コールのメディア パスが WAN を通過しない場合でも、サードパーティ製呼制御システムと Unified CM クラスタの両方で減少します。この集中型コール処理設計は、コール アドミッション制御の点から見ると理想的ではありませんが、ハードウェアに関して、(エンドポイントが集中型 Unified CM クラスタまたは集中型サードパーティ製呼制御システムのみに登録されるため) コスト効率が高く、ダイヤル プランの細分化が軽減されます。

実践的なアプローチが各デュアル呼制御配置に適用する必要があります。戦略的な観点から、あらゆる支社にサードパーティ製呼制御システムを配置することは、現在では商用的に意味を成さない場合があります。ただし正確なコール アドミッション制御が設計の優先順位の場合、この配置モデルが適切なことがあります。同様に、集中型サードパーティの呼制御および集中型 Unified CM クラスタを使用した配置の場合、独立したコール アドミッション制御ドメインの問題は WAN のプロビジョニング帯域幅を超えた方法で対応できます。

デュアル呼制御配置におけるダイヤル プランに関する考慮事項

配置内に呼制御システムが 2 つしかなく、エンドポイントに対し番号が使用され、着信番号がローカル Unified CM クラスタまたはサードパーティ製呼制御システムのローカル パターンに一致した場合、コールはローカルに接続されたエンドポイントに送信されます。番号が別の（リモート）呼制御のパターンに一致した場合、コールは相互接続 SIP トランクを介した非ローカル エンドポイントに送信する必要があります。重複するダイヤル プランの場合、Unified CM クラスタとサードパーティ呼制御システムの両方が、内部に登録されているどのエンドポイントにも一致しないコールを他の呼制御クラスタに送信することができます。

配置内の呼制御システムが増加すると、ダイヤル プランの細分化も進みます。この問題は、複数の呼制御からのエンドポイントが同じサイト内に存在し、このエンドポイントに別の、または簡単な集約番号の範囲が設定されていない場合にさらに状況が悪化する可能性があります。この場合、デフォルト ルートを使用することはできませんが、2 つのオプションのいずれかを配置して、複数の呼制御システムと高度に細分化されたダイヤル プランを使用した Unified Communications システムにコールをルーティングできます。

- 各呼制御に関連付けられた一意の番号範囲ごとに明示的なルート パターンおよび対応するトランクを使用します。
- Unified CM（および使用している場合は、SME）配置内では、クラスタ間検索サービス（ILS）と Global Dial Plan Replication（GDPR）を使用して、各 Unified CM クラスタとサードパーティのユニファイド コミュニケーション システムでサポートされる番号範囲に関する情報を共有します。サードパーティ システムと関連するデバイスの場合、それぞれの一意の番号範囲を GDPR にインポートし、インポートされたそれぞれの番号範囲をルート文字列（呼制御システムを識別するラベル）に関連付けます。Unified CM ユーザが番号にダイヤルすると、Unified CM は番号がクラスタに登録されているかどうかを確認します。番号が Unified CM クラスタに登録されていない場合、Unified CM は着信側番号および対応するルート文字列について ILS を検索します。ルート文字列は、番号が存在する呼制御クラスタを識別し、SIP ルート パターンとの照合に使用され、その後宛先へ SIP トランクを介してコールを転送します。

英数字 URI が Unified CM とサードパーティ製呼制御システムに登録されたエンドポイントのアドレス指定とコールに使用される場合、コール ルーティングは配置に応じて、次のいずれかの方法で実施されます。

- 単一のサードパーティ製呼制御システムのみが、単一の SIP トランク経由で Unified CM クラスタとなって配置されている場合、1 つの呼制御にないエンドポイントへのコールが他の呼制御に送信されるように、デフォルト SIP ルートは Unified CM とサードパーティ製呼制御システムで設定できます。
- 複数のサードパーティ製呼制御システムを配置する場合は、クラスタ間検索サービス（ILS）と Global Dial Plan Replication（GDPR）を使用して、各 Unified CM クラスタとサードパーティのユニファイド コミュニケーション システムでサポートされる URI に関する情報を共有します。Unified CM ユーザが URI にダイヤルするときの URI ベースのコール ルーティングでは、Unified CM は URI がクラスタに登録されているかどうかを確認します。登録されていない場合、Unified CM は着信側 URI および対応するルート文字列について ILS を検索します。ルート文字列は、URI が存在する呼制御クラスタを識別し、SIP ルート パターンとの照合に使用され、その後宛先 URI へ SIP トランクを介してコールを転送します。サードパーティ製呼制御システムに登録された URI ベースのエンドポイントの場合、サードパーティ製呼制御システムの対応ルート文字列とともに、サードパーティ呼制御システムに登録された URI のリストを ILS に手動でインポートする必要があります。

IP WAN を介したクラスタリング

QoS 機能に対応している IP WAN によって相互接続される複数サイト間で、単一の Unified CM クラスタ（Enterprise Edition、Business Edition 7000、または Business Edition 6000）を配置できます。ここでは、WAN を介したクラスタリングの概要を簡潔に説明します。詳細については、呼処理（9-1 ページ）の章を参照してください。

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

- ローカル フェールオーバー配置モデル（10-50 ページ）

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

- リモート フェールオーバー配置モデル（10-57 ページ）

  リモート フェールオーバーでは、WAN を介して分割されたプライマリとバックアップの呼処理サーバを配置できます。このタイプの配置を使用すると、Unified CM サブスクライバを備えた複数のサイトを、別のサイトにある Unified CM サブスクライバでバックアップすることが可能です。

（注） リモート フェールオーバーの配置では、サブスクライバ サーバ間で大量のクラスタ内トラフィックが流れるため、広い帯域幅が必要になる場合があります。

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

WAN を介したクラスタリングの主な利点として、次のようなものが挙げられます。

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

これらの機能により、このソリューションは、ビジネスが継続して行われるサイトのディザスタ リカバリ プランとして、または複数の中小規模サイト用の単一ソリューションとして理想的なものになります。

WAN の考慮事項

WAN を介したクラスタリングが成功するには、WAN 自体のさまざまな特性を慎重に計画し、設計し、実装する必要があります。Unified CM サーバ間の Intra-Cluster Communication Signaling（ICCS）は、複数のトラフィック タイプから構成されます。ICCS のトラフィック タイプは、優先またはベストエフォートのどちらかとして分類されます。優先 ICCS トラフィックには、IP Precedence 3（DSCP 24 または PHB CS3）が付けられます。ベストエフォート型 ICCS トラフィックには、IP Precedence 0（DSCP 0 または PHB BE）が付けられます。さまざまなタイプの ICCS トラフィックについては、クラスタ内通信（10-48 ページ）で説明されています。この項では、プロビジョニングについてのさらに詳しいガイドラインも記述されています。WAN の特性には、次の設計上のガイドラインが適用されます。

- 遅延

  任意の 2 台の Unified CM サーバ間の片方向の最大遅延は 40 ミリ秒、つまり 80 ミリ秒ラウンドトリップ時間（RTT）以下でなければなりません。遅延の測定については、遅延のテスト（10-49 ページ）を参照してください。2 つのサイト間の伝搬遅延は、他のネットワーク遅延を考慮しない場合、1 キロメートルあたり 6 マイクロ秒になります。これは、40 ミリ秒遅延に対して理論的な最大距離約 6,000 km、つまり約 3,720 マイルに相当します。この距離は、相対的なガイドラインとしてのみ記載されています。実際には、ネットワーク内の他の遅延により、これより短くなります。

- ジッタ

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

- パケット損失とエラー

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

- 帯域幅

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

- Quality of Service

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

クラスタ内通信

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

サーバ間のクラスタ内トラフィックは、次のものから構成されます。

- 主な設定情報を提供する IBM Informix Dynamic Server（IDS）データベースからのデータベース トラフィック。IDS トラフィックは、Cisco QoS の推奨事項に沿って再優先順位付けが行われ、より高い優先順位のデータ サービスになります（たとえば、特定のビジネス ニーズによって必要な場合は IP Precedence 1）。この一例は、IDS データベース設定を使用する、エクステンション モビリティの拡張使用です。
- サブスクライバをパブリッシャに認証し、パブリッシャのデータベースにアクセスするために使用されるファイアウォール管理トラフィック。管理トラフィックは、クラスタ内のすべてのサーバ間を通過します。管理トラフィックは、Cisco QoS の推奨事項に沿って優先順位付けが行われ、より高い優先順位のデータ サービスになります（たとえば、特定のビジネス ニーズによって必要な場合は IP Precedence 1）。
- ICCS リアルタイム トラフィック。このトラフィックは、シグナリング、コール アドミッション制御、および開始と終了時のコールについてのその他の情報から構成されます。ICCS は、Cisco CallManager Service が使用可能になっているすべてのサーバ間で、伝送制御プロトコル（TCP）接続を使用します。この接続は、これらのサーバ間でフルメッシュです。このトラフィックは、優先 ICCS トラフィックであり、Cisco CallManager リリースおよびサービス パラメータ設定に応じてマークされます。
- CTI Manager リアルタイム トラフィック。このトラフィックは、コールに関係する CTI デバイスに使用されるか、Unified CM サーバ上のその他のサードパーティ製デバイスの制御またはモニタに使用されます。このトラフィックは、優先 ICCS トラフィックとしてマークされ、CTI Manager を備えた Unified CM サーバと、CTI デバイスを備えた Unified CM サーバとの間に存在します。

（注）　Unified CM サーバ間のさまざまなタイプのトラフィックの詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html で入手可能な『*System Configuration Guide for Cisco Unified Communications Manager*』の最新バージョンを参照してください。

Unified CM パブリッシャ

パブリッシャ サーバは、部分的なマスター データベースの読み取り専用コピーをクラスタ内の他のすべてのサーバに複製します。データベースのほとんどの変更は、パブリッシャで行われます。クラスタ内の別のサーバが到達不能である期間に、パブリッシャのマスター データベースに管理目的の更新などの変更が加えられた場合、パブリッシャは、通信が再確立されたときに、更新されたデータベースを複製します。ユーザ方向の呼処理機能に対するデータベースの変更は、IP Phone が登録されるサブスクライバ サーバで行われます。これらの機能には、次のものがあります。

- 不在転送（CFA）
- メッセージ待機インジケータ（MWI）
- プライバシーの有効/無効
- Do Not Disturb（DND）の有効/無効

- エクステンション モビリティ（EM）のログイン
- モニタ（将来的に使用、現在ユーザ レベルの更新はありません）
- ハント グループのログアウト
- デバイス モビリティ
- エンド ユーザおよびアプリケーション ユーザの CTI Certificate Authority Proxy Function（CAPF）ステータス
- クレデンシャルの確認と認証

各サブスクライバ サーバは、これらの変更をクラスタ内の他のすべてのサーバに複製します。パブリッシャが到達不能またはオフラインの間は、他のいかなる設定変更もデータベースに加えることはできません。パブリッシャに障害が発生している場合でも、次のものをはじめとするクラスタの通常の操作の大部分は、影響を*受けません*。

- 呼処理
- フェールオーバー
- 設定済みデバイスの登録

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

コール詳細レコード（CDR）およびコール管理レコード（CMR）

コール詳細レコードとコール管理レコードが使用可能である場合、各サブスクライバによって収集され、定期的にパブリッシャにアップロードされます。パブリッシャが到達不能である間、CDR および CMR は、サブスクライバのローカル ハードディスクに保存されます。パブリッシャとの接続が再確立されると、未処理の CDR はすべて、パブリッシャにアップロードされます。パブリッシャは、レコードを CDR 分析とレポート（CAR）データベースに格納します。

遅延のテスト

任意の 2 台のサーバ間の最大ラウンドトリップ時間（RTT）は、80 ミリ秒以下でなければなりません。この制限には、この 2 台のサーバ間の伝送パスの遅延がすべて含まれる必要があります。Unified CM サーバで **ping** ユーティリティを使用してラウンドトリップの遅延を確認しても、正確な結果は得られません。ping は、ベストエフォート型のパケットとして送信されます。ICCS トラフィックと同じ QoS 対応パスを使用して転送されません。したがって、遅延を確認するには、Unified CM サーバに最も近いネットワーク デバイスを使用することを推奨します。理想的には、サーバが接続されているアクセス スイッチです。Cisco IOS は、ICCS トラフィックが通過するのと同じ QoS 対応パス上で ping パケットが送信されるように、レイヤ 3 タイプ オブ サービス（ToS）ビットを設定できる拡張 ping を備えています。拡張 ping によって記録される時間は、ラウンドトリップ時間（RTT）、つまり通信パスを通過して戻るのに要する時間です。

次に、IP precedence を 3 に設定した Cisco IOS 拡張 ping の例を示します（ToS バイトは 96 に設定）。

```
Access_SW#ping
Protocol [ip]:
Target IP address: 10.10.10.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]: 96
Set DF bit in IP header? [no]:
Validate reply data? [no]:
```

```
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

エラー率

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

トラブルシューティング

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

- クラスタ内のリモート Unified CM サーバ上にある IP Phone、ゲートウェイ、またはその他のデバイスが、一時的に通信不能になることがあります。
- コールの接続が切断されたり、コールのセットアップ中に失敗する場合があります。
- ユーザにダイヤル トーンが聞こえるまでに、予想以上に長い遅延が起こる場合があります。
- Busy Hour Call Completions（BHCC）が低い場合があります。
- ICCS（SDL セッション）がリセットされたり、接続が切断されることがあります。
- サブスクライバをアップグレードし、パブリッシャとデータベースの同期をとることにかかる時間が増加します。

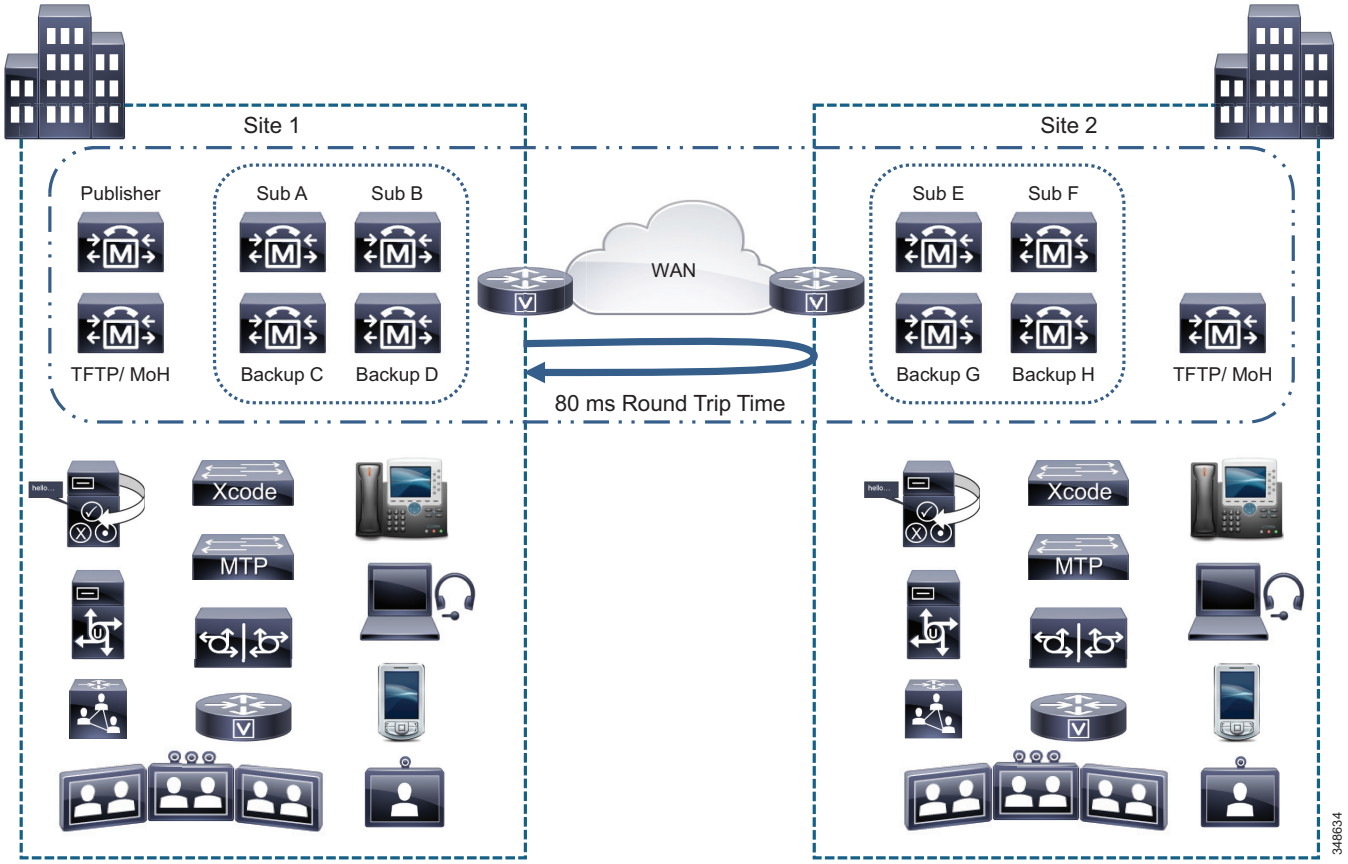
要約すると、クラスタ間の通信の問題のトラブルシューティングを行うには、次のタスクを実行します。

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

ローカル フェールオーバー配置モデル

ローカル フェールオーバー配置モデルは、WAN を介したクラスタリングに対する最大の復元性があります。このモデルの各サイトには、少なくとも 1 つのプライマリ Unified CM サブスクライバと 1 つのバックアップ サブスクライバがあります。この設定では、最大 4 つのサイトをサポートできます。電話機および他のデバイスの最大数は、配置されているサーバの数とタイプによって異なります。全サイトの IP Phone の最大総数は 40,000 です（図 10-19 を参照）。

図 10-19　ローカル フェールオーバー モデルの例



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

- 少なくとも 1 つのプライマリ Unified CM サブスクライバと 1 つのバックアップ サブスクライバを含むように、各サイトを設定します。
- Unified CM の *グループ*と *デバイス プール*を設定して、サイト内のデバイスが、あらゆる状況でそのサイトのサーバだけに登録されるようにします。
- 各サイトで主要なサービス（TFTP、DNS、DHCP、LDAP、および IP Phone サービス）、すべてのメディア リソース（トランスコーダ、会議リソース、アナンシエータ、および保留音）、およびゲートウェイを複製します。複製を確実に行い、最大レベルの復元性を得るよう、シスコは強く推奨します。また、この方法を拡張して、各サイトにボイスメール システムを組み込むこともできます。
- WAN 障害が発生した場合、パブリッシャ データベースへのアクセスがないサイトでは、いくつかの機能を使用できないことがあります。たとえば、リモート サイトのシステム管理者は、設定を一切追加、変更、または削除することができません。ただし、ユーザは、Unified CM パブリッシャ（10-48 ページ）の項にリストされているユーザ方向の機能に、引き続きアクセスできます。
- WAN 障害が発生した状態では、コールを発信するサブスクライバと現在通信していない電話番号にコールを発信すると、ファーストビジー トーンが聞こえるか、またはコール転送されます（ボイスメールまたは Call Forward Unregistered で設定された宛先に転送される可能性があります）。

- Unified CM クラスタ内の任意の 2 台のサーバ間に可能な最大ラウンドトリップ時間（RTT）は、80 ミリ秒です。

（注）　ラウンドトリップ遅延時間が長く、最繁時呼数（BHCA）が多い状況では、音声のカットスルー遅延が大きくなる場合があり、音声コール確立時の初期音声クリッピングの原因となる場合があります。

- WAN を介してクラスタリングされている各サイトと他のすべてのサイト間の Intra-Cluster Communication Signaling（ICCS）に最低 1.544 Mbps（T1）の帯域幅が必要です。たとえば、3 ヵ所のサイトが WAN を介してクラスタリングされると、各サイトで呼制御トラフィック用の WAN 帯域幅の 2 * 1.544 Mbps が必要です。呼制御トラフィック用のこの最小帯域幅要件は、1 つのサイトから別のサイトへの最大 10,000 の最繁時呼数（BHCA）から構成され、電話番号が WAN を介してクラスタリングされるサイト間で共有されない配置にのみ適用されます。特定の遅延が発生している共有されていないディレクトリ番号間での、10,000 BHCA を超えるトラフィックの帯域幅を計算する場合は、次の計算式をガイドラインとして使用できます。

  合計帯域幅（Mbps）=（合計 BHCA/10,000）*（1 + 0.006 * 遅延）、遅延 = RTT 遅延（ミリ秒単位）

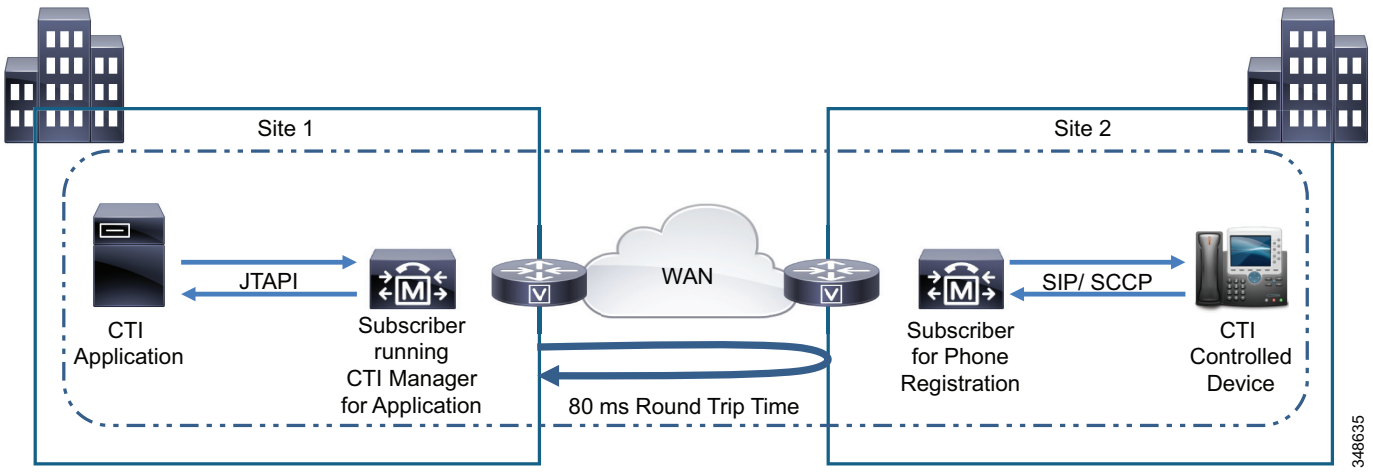
  この呼制御トラフィックは、優先トラフィックに分類されます。優先 ICCS トラフィックには、IP Precedence 3（DSCP 24 または PHB CS3）が付けられます。

- Intra-Cluster Communication Signaling（ICCS）トラフィックに必要な帯域幅に加え、パブリッシャとクラスタ内のあらゆるサブスクライバ ノード間のデータベースおよびその他のサーバ間トラフィック用に、最低でも 1.544 Mbps（T1）の帯域幅が必要になります。

- WAN を介して CTI Manager も配置するお客様の場合（図 10-20 を参照）、次の式を使用して、CTI Manager サービスが実行されている Unified CM サブスクライバと CTI エンドポイントの登録先 Unified CM サブスクライバ間の CTI Intra-Cluster Communication Signaling（ICCS）トラフィックの帯域幅（Mbps）を計算できます。

  CTI ICCS 帯域幅（Mbps）=（合計 BHCA/10,000）* 0.53

図 10-20　WAN を介した CTI

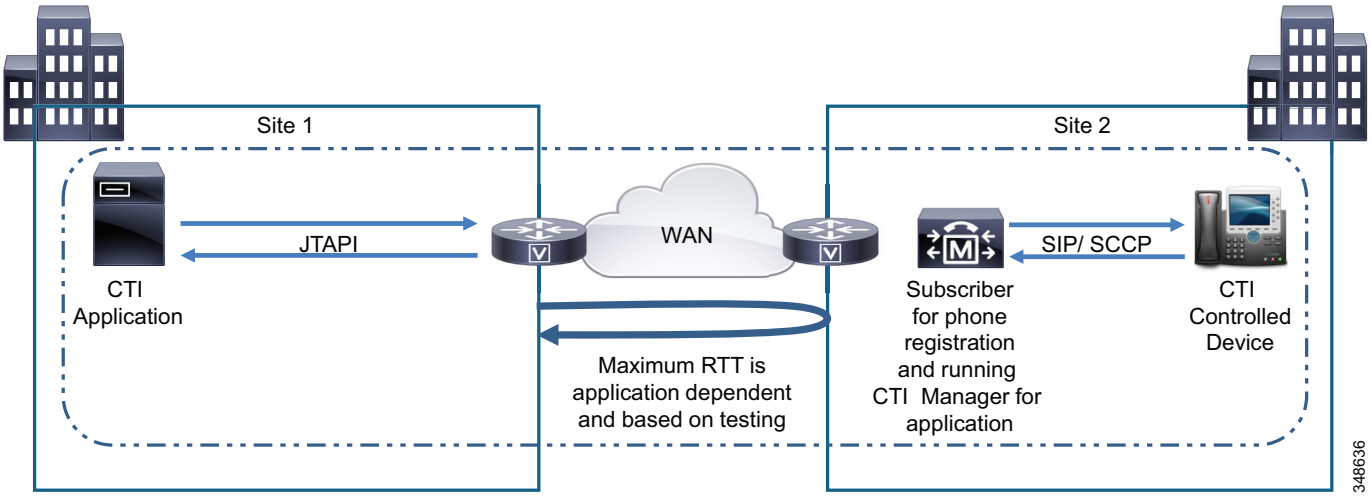


- J/TAPI アプリケーションが Unified CM サブスクライバから離れている配置では（図 10-21 を参照）、次の式を使用して、一般的な J/TAPI アプリケーションの Quick Buffer Encoding（QBE）J/TAPI 帯域幅を計算できます。

  J/TAPI 帯域幅（Mbps）=（合計 BHCA/10,000）* 0.28

  帯域幅は、J/TAPI アプリケーションによって異なる場合があります。帯域幅要件については、アプリケーションの開発者またはプロバイダーに確認してください。

図 10-21　WAN を介した J/TAPI



例 10-1　2 つのサイトの帯域幅の計算

Unified CM を配置した 2 つのサイト（サイト 1、サイト 2）があると仮定します。2 つのサイトは WAN を介してクラスタリングされており、ラウンドトリップ時間は 80 ミリ秒です。サイト 1 にはパブリッシャが 1 つと、TFTP および保留音（MoH）を組み合わせたサーバが 1 つ、そして 2 つの Unified CM サブスクライバ サーバが配置されています。サイト 2 には TFTP/MoH サーバが 1 つと、Unified CM サブスクライバ サーバが 2 つ配置されています。サイト 1 には 5000 台の電話機があり、それぞれ 1 つの DN を持っています。サイト 2 にも 5000 台の電話機があり、それぞれ 1 つの DN を持っています。最繁時は、サイト 1 の 2500 台の電話機がサイト 2 の 2500 台の電話機を呼び出します。それぞれのコールは、3 BHCA です。同じ最繁時に、サイト 2 の 2500 台の電話機もサイト 1 の 2500 台の電話機を呼び出します。それぞれのコールは、3 BHCA です。この場合、次のように計算します。

最繁時の合計 BHCA = 2500 * 3 + 2500 * 3 = 15,000

サイト間に必要な合計帯域幅 = 合計 ICCS 帯域幅 + 合計データベース帯域幅

合計 BHCA が 15,000 であり、10,000 を超えているため、合計 ICCS 帯域幅 =（15,000/10,000）*（1 + 0.006*80）= 2.22 Mbps という計算式を使用できます。

合計データベース帯域幅 =（パブリッシャからリモートとなるサーバの数）* 1.544 = 3 * 1.544 = 4.632 Mbps

サイト間で必要な帯域幅 = 2.22 Mbps + 4.632 Mbps = 6.852 Mbps（およそ 7 Mbps）

- WAN を介してクラスタリングされているサイト間でディレクトリ番号が共有されている場合は、さらに帯域幅を確保する必要があります。最低限必要な 1.544 Mbps の帯域幅に加え、このようなオーバーヘッドと追加帯域幅が必要になります。共有 DN 間での 10,000 BHCA のトラフィックの場合、次の計算式を使用して計算できます。

  オーバーヘッド =（0.012 * 遅延 * シェアド ライン）+（0.65 * シェアド ライン）。各値の意味は次のとおりです。

  遅延 = IP WAN を介した RTT 遅延（ミリ秒単位）

  シェアド ライン = WAN 経由でディレクトリ番号が共有されている追加の電話機の平均数

  特定の遅延が発生している共有されているディレクトリ番号間での、10,000 BHCA を超えるトラフィックの帯域幅を計算する場合は、次の計算式をガイドラインとして使用できます。

  合計帯域幅（Mbps）=（合計 BHCA/10,000）*（1 + 0.006 * 遅延 + 0.012 * 遅延 * シェアド ライン + 0.65 *）。各値の意味は次のとおりです。

  遅延 = RTT 遅延（ミリ秒単位）

  シェアド ライン = WAN 経由でディレクトリ番号が共有されている追加の電話機の平均数

例 10-2　ディレクトリ番号を共有する 2 つのサイトの帯域幅の計算

Unified CM を配置した 2 つのサイト（サイト 1、サイト 2）があると仮定します。2 つのサイトは WAN を介してクラスタリングされており、ラウンドトリップ時間は 80 ミリ秒です。サイト 1 にはパブリッシャが 1 つと、TFTP および保留音（MoH）を組み合わせたサーバが 1 つ、そして 2 つの Unified CM サブスクライバ サーバが配置されています。サイト 2 には TFTP/MoH サーバが 1 つと、Unified CM サブスクライバ サーバが 2 つ配置されています。サイト 1 には 5000 台の電話機があり、それぞれ 1 つの DN を持っています。サイト 2 にも 5000 台の電話機がありますが、それぞれがサイト 1 の 5000 台の電話機と DN を共有しています。そのため、各 DN は WAN 経由で共有され、平均して 1 台の追加の電話機を持つことになります。最繁時は、サイト 1 の 2500 台の電話機がサイト 2 の 2500 台の電話機を呼び出します。それぞれのコールは、3 BHCA です。これにより、サイト 1 の電話機も呼び出すことになります。同じ最繁時に、サイト 2 の 2500 台の電話機がサイト 1 の 2500 台の電話機を呼び出します。それぞれのコールは、3 BHCA です。これにより、サイト 2 の電話機も呼び出すことになります。この場合、次のように計算します。

最繁時の合計 BHCA = 2500 * 3 + 2500 * 3 = 15,000

サイト間に必要な合計帯域幅 = 合計 ICCS 帯域幅 + 合計データベース帯域幅

合計 BHCA が 15,000 であり、10,000 を超えているため、合計 ICCS 帯域幅 =（15,000/10,000）*（1 + 0.006*80 + 0.012*80*1 + 0.65*1）= 4.635 Mbps という計算式を使用できます。

合計データベース帯域幅 =（パブリッシャからリモートとなるサーバの数）* 1.544 = 3 * 1.544 = 4.632 Mbps

サイト間で必要な帯域幅 = 4.635 Mbps + 4.632 Mbps = 9.267 Mbps（およそ 10 Mbps）

（注）　上記の帯域幅は、ICCS、データベース、およびその他のサーバ間トラフィックに限定したものです。コールが IP WAN を経由する場合は、コールに使用する音声およびビデオ コーデックに応じて、音声またはメディア トラフィック用に追加の帯域幅をプロビジョニングする必要があります。詳細については、帯域幅のプロビジョニング（3-56 ページ）を参照してください。

- クラスタ内のサブスクライバ サーバは、ローカル データベースを読み取ります。データベースの変更は、変更のタイプに応じて、ローカル データベースとパブリッシャのデータベースの両方で発生する可能性があります。クラスタ内のさまざまなサーバの同期には、Informix Dynamic Server（IDS）のデータベース複製が使用されます。そのため、長期間にわたる WAN 接続の喪失など、障害状態から回復する場合は、障害時に行われた可能性があるあらゆる変更と Unified CM データベースを同期する必要があります。このプロセスは、パブリッシャとクラスタ内のその他のサーバへのデータベース接続が復元されると、自動的に実行されます。低帯域幅のリンクや遅延が大きいリンクでは、このプロセスに時間がかかる場合があります。また、まれなケースですが、手動によるリセットやサーバ間でのデータベース複製の修復が必要になる場合もあります。この操作は、コマンドライン インターフェイス（CLI）で **utils dbreplication repair all** や **utils dbreplication reset all** などのコマンドを使用して実行します。WAN を経由して、リモートのサブスクライバでデータベース複製の修復またはリセットを実行すると、クラスタ内のすべての Unified CM データベースが再同期されます。パブリッシャおよびサブスクライバ ノード間の長い遅延、低帯域幅では、データベース複製の修復またはリセットが完了するまで時間がかかることがあります。

（注）　同一のリモート ロケーションにある複数のサブスクライバに対して、データベース複製の修復またはリセットを実行すると、データベース複製の完了に時間がかかる場合があります。このようなリモートのサブスクライバのデータベース複製を修復またはリセットする場合は、1 つずつ実行することを推奨します。異なるリモート ロケーションにあるサブスクライバのデータベース複製を修復またはリセットする場合は、同時に実行できます。

- WAN を介したクラスタリングを使用してクラスタリングで集中型呼処理を使用するリモート支社を、WAN トラフィックを介したクラスタリングに使用される同じ WAN パス経由で中央サイトに接続する場合は、WAN を介したクラスタリングに使用されるリンクがオーバーサブスクリプションにならないよう、慎重にコール アドミッション制御を設定します。
  - WAN を介したクラスタリングに使用されるリンク上で帯域幅が制限されていない場合（つまり、リンクへのインターフェイスが OC-3s または STM-1s で、コール アドミッション制御に関する要件がない場合）は、リモート サイトがメイン サイトのいずれかに接続される場合があります。これは、すべてのメイン サイトでロケーションを Hub_None として設定する必要があるためです。この設定が行われても、コール アドミッション制御に使用するハブアンドスポーク トポロジは保持されます。
  - マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）機能を使用している場合は、Unified CM ロケーションとリモート サイトにあるすべてのサイトが、メイン サイトのいずれかに登録される場合があります。
  - メイン サイト間の帯域幅が制限されている場合は、サイト間でコール アドミッション制御を使用し、ロケーションが Hub_None として設定されているメイン サイトにすべてのリモート サイトを登録する必要があります。このメイン サイトはハブ サイトと見なされ、それ以外のリモート サイトと、クラスタオーバー WAN サイトはすべて、スポーク サイトとなります。
- ソフトウェア アップグレード時は、ソフトウェア リリース ノートで説明されている標準のアップグレード手順を使用して、クラスタ内のすべてのサーバを同じ保守期間内にアップグレードする必要があります。IP WAN 経由のラウンドトリップ遅延時間が大きい場合は、ソフトウェア アップグレードにかかる時間が長くなります。パブリッシャからサブスクライバへの帯域幅が各サブスクライバ ノードに必要な 1.544 Mbps より低いと、ソフトウェア アップグレード プロセスが完了するまで時間がかかる場合があります。アップグレード時間を短縮するには、アップグレード中にリモート サブスクライバごとに必要な 1.544 Mbps を超える追加の帯域幅をプロビジョニングできます。

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

ローカル フェールオーバー モデルに対する Unified CM クラスタのプロビジョニングは、呼処理 (9-1 ページ) の章で説明されているキャパシティについての設計上のガイドラインに従う必要があります。WAN を介してサイト間の音声コールまたはビデオ コールが可能である場合、サイト間のコール アドミッション制御を提供するために、他のサイトのデフォルト ロケーションに加えて、Unified CM の *ロケーション*も設定する必要があります。デバイス数に対して帯域幅が余分にプロビジョニングされる場合でも、ロケーションに基づくコール アドミッション制御を設定するのが最良の方法です。ロケーションベースのコール アドミッション制御によってコールが拒否された場合は、自動代替ルーティング (AAR) 機能によって PSTN への自動フェールオーバーを行うことができます。

冗長性とアップグレード時間を改善するために、2 台の Unified CM サーバで Cisco Trivial File Transfer Protocol (TFTP) サービスを使用可能にすることを推奨します。クラスタ内には 3 台以上の TFTP サーバを配置できますが、そのような構成ではすべての TFTP サーバ上ですべての TFTP ファイルを再構築するために時間がかかります。

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

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

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

ローカル フェールオーバー用のゲートウェイ

ゲートウェイは、通常、どのサイトにも配置されていて、PSTN へのアクセスに対応しています。ゲートウェイを同一サイトの Unified CM サーバに登録するために、デバイス プールを設定する必要があります。サイトのローカル ゲートウェイを PSTN アクセス用の第一選択肢として選択し、他のサイトのゲートウェイをオーバーフロー用の第二選択肢として選択するために、コール ルーティング (ルート パターン、ルート リスト、およびルート グループ) も設定する必要があります。各サイトで緊急用サービスへのアクセスを確保するように特に注意してください。

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

ローカル フェールオーバー用のボイスメール

Cisco Unity Connection や他のボイスメール システムは、すべてのサイトに配置が可能で、Unified CM クラスタに組み込むことができます。この設定では、WAN 障害時に PSTN を使用しなくても、ボイスメールにアクセスできます。ボイスメール プロファイルを使用すると、同じロケーションにある IP Phone に、サイトに適したボイスメール システムを割り当てることができます。Unity Connection および WAN を介したクラスタリングの詳細については、分散型メッセージングと WAN を介したクラスタリング (19-17 ページ) を参照してください。

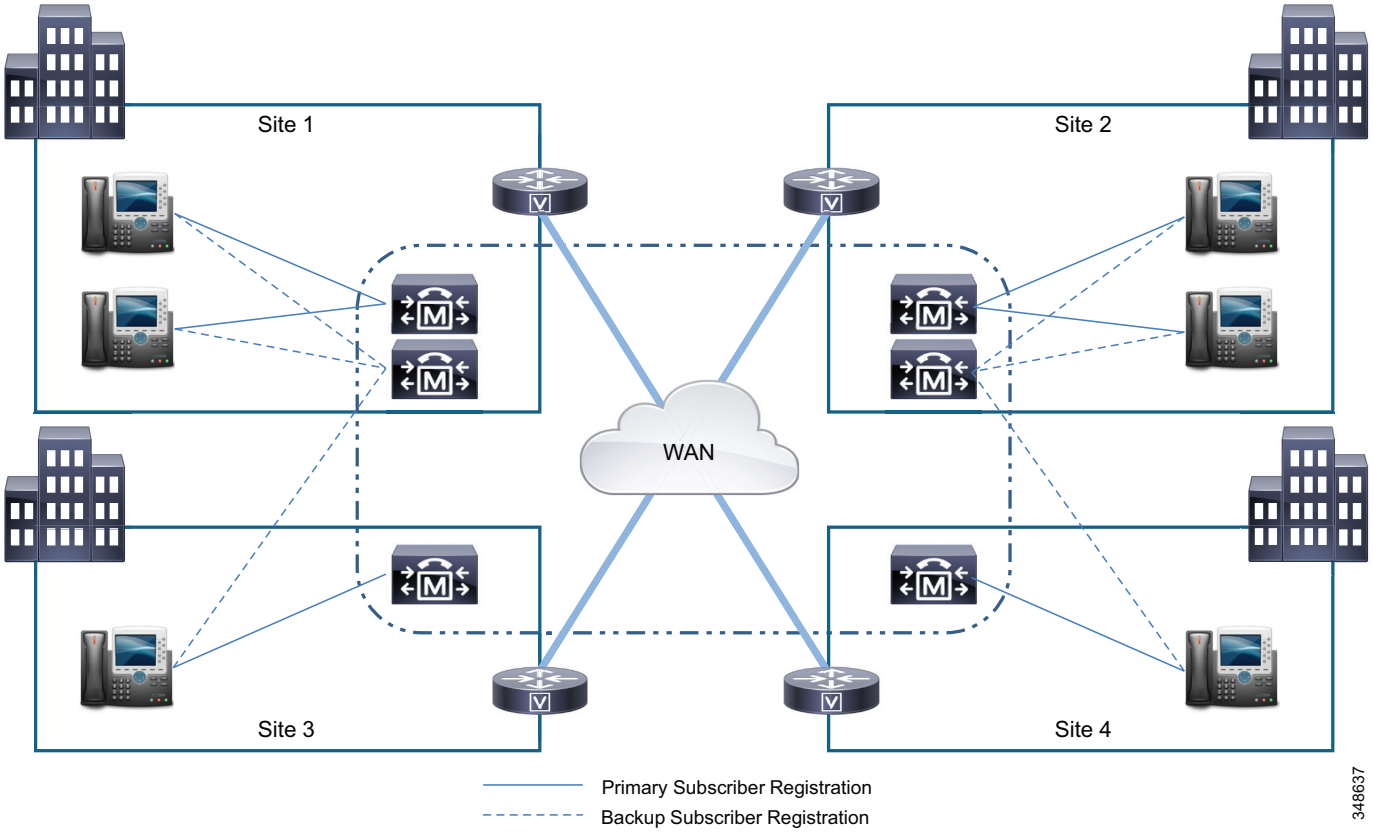
ローカル フェールオーバーに対する保留音とメディア リソース

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

リモート フェールオーバー配置モデル

リモート フェールオーバー配置モデルでは、バックアップ サーバを柔軟に配置できます。各サイトには、少なくとも 1 つのプライマリ Unified CM サブスクライバを含め、バックアップ サブスクライバを必要に応じて配置します。このモデルでは、呼処理（9-1 ページ）の章で説明されている 1:1 冗長性と 50/50 ロード バランシングを使用する場合、IP Phone と他のデバイスが通常ローカル サブスクライバに登録されている複数のサイトを配置できます。バックアップ サブスクライバは、他の 1 つ以上のサイトで、WAN を介して配置されます（図 10-22 を参照）。

図 10-22　WAN を介したクラスタリング：4 つのサイトでのリモート フェールオーバー



リモート フェールオーバー モデルを実装する場合は、ローカル フェールオーバー モデルのガイドライン（ローカル フェールオーバー配置モデル（10-50 ページ）を参照）と、次の変更点に従ってください。

- 少なくとも 1 つのプライマリ Unified CM サブスクライバと、必要に応じてオプションのバックアップ サブスクライバを含むように、各サイトを設定します。IP WAN を経由したバックアップ サブスクライバを設定しない場合は、Survivable Remote Site Telephony（SRST）ルータをバックアップの呼処理エージェントとして使用できます。
- Unified CM の *グループ*と *デバイス プール*を設定して、デバイスが第 2 または第 3 の選択肢として WAN を越えたサーバに登録できるようにします。
- デバイスが、WAN を介して同じクラスタ内のリモート Unified CM サーバに登録される場合、シグナリング トラフィックまたは呼制御トラフィックのために帯域幅を追加する必要があります。この帯域幅は、ICCS トラフィックより大きくなる場合があります。また、シグナリングに関する帯域幅のプロビジョニング計算を使用して計算する必要があります（帯域幅のプロビジョニング（3-56 ページ）を参照）。

（注）　ディザスタ リカバリを目的として、これら 2 つのタイプの配置の機能を組み合わせることもできます。たとえば、Unified CM のグループでは、最大 3 台のサーバ（1 次、2 次、3 次）を設定できます。そのため、同一のサイトに 1 次および 2 次のサーバを配置し、ターシャリ サーバを WAN 経由でリモート サイトに配置するように Unified CM のグループを設定できます。

仮想サーバでの Unified Communications の配置

仮想化については、Cisco Collaboration アプリケーションのノードは、ハイパーバイザを介して物理サーバ（ホスト）上で実行する仮想マシン（VM）として配置されます。通常、複数の仮想マシンを単一のホストで実行できます。これは、アプリケーションがハードウェア プラットフォーム上で直接動作している従来のソリューションと比べて、明らかなメリットがあります。たとえば、コスト（ハードウェア、エネルギー、ケーブリング、ラック スペースのコストなど）を大幅に削減できます。さらに、仮想化ソフトウェアの能力を活用することにより、ハードウェア プラットフォームの運用および保守を簡素化できます。

ここでは、Cisco Unified Computing System（UCS）アーキテクチャ、アプリケーション仮想化のハイパーバイザ テクノロジー、およびストレージ エリア ネットワーキング（SAN）の概念の詳細について、簡単に説明します。また、仮想サーバで Unified Communications アプリケーションを配置するための設計考慮事項も示します。

ここでの説明は、次の場所で入手できる製品固有の詳細な設計ガイドライン [英語] に置き換わるものではありません。

- https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html
- https://www.cisco.com/go/virtualized-collaboration

仮想サーバでの Unified Communications システムのサイジングについては、Cisco Collaboration Sizing Tool を使用してください。このツールは、（有効なログイン認証を持つ）シスコ代理店および従業員が次の URL から入手できます。

https://cucst.cloudapps.cisco.com/landing

ハイパーバイザ

ハイパーバイザはサーバ ハードウェアで直接動作してハードウェアを制御するシン ソフトウェア システムであり、複数のオペレーティング システム（ゲスト）がサーバ（ホスト コンピュータ）で同時に動作できます。ゲスト オペレーティング システム（Cisco Unified CM のオペレーティング システムなど）はハイパーバイザ上の別のレベルで動作します。ハイパーバイザはクラウド コンピューティングおよび仮想化テクノロジーの基盤要素のいずれかであり、アプリケーションを統合するサーバの数が少なくて済みます。

ほとんどの Cisco Collaboration システム アプリケーションは、仮想化によってのみサポートされます。これは、VMware vSphere ESXi ハイパーバイザを配置するには、これらのアプリケーションで必要であり、サーバ（ベア メタル）に直接インストールすることができないことを意味します。

VMware vCenter は、仮想環境の管理を支援するツールです。テスト済みリファレンス構成では、VMware vCenter は必須ではありません。ただし、多くのホストを配置する場合には強く推奨されます。仕様ベースのハードウェアでは、VMware vCenter が必要になります。

サーバ ハードウェア オプション

仮想化を使用して Cisco Collaboration アプリケーションを配置する際には、次の 2 つのハードウェア構成オプションを利用できます。

- テスト済みリファレンス構成（TRC）：Cisco Unified Computing System（UCS）プラットフォームに基づいて選択されたハードウェア設定テストされ、具体的に保証された性能、キャパシティ、Cisco Collaboration システム仮想マシンを満載して稼働するアプリケーションの組み合わせシナリオが文書化されています。
- 仕様ベースのハードウェア：ハードウェアの柔軟性が向上します。また、たとえば、『*VMware Compatibility Guide*』（https://www.vmware.com/resources/compatibility/search.php で入手可能）に記載されている他の Cisco UCS およびサードパーティ製サーバのサポートを追加します。

Cisco Unified Computing System

Unified Computing は、コンピューティング リソース（CPU、メモリ、および I/O）、IP ネットワーキング、ネットワークベースのストレージ、および仮想化を単一のハイ アベイラビリティ システムに統合するアーキテクチャです。このレベルの統合により、電力および冷却の費用を節約し、ネットワークへのサーバ接続を簡易化し、物理ホスト間でアプリケーション インスタンスを動的に再配置し、ディスク ストレージ容量をプールできます。

Cisco Unified Computing System は、多くのコンポーネントで構築されていますが、サーバの観点からすると、UCS アーキテクチャは次の 2 つのカテゴリに分割されます。

- Cisco UCS B シリーズ ブレード サーバ（10-60 ページ）
- Cisco UCS C シリーズ ラックマウント（10-62 ページ）

Cisco Unified Computing System アーキテクチャの詳細については、次の URL から入手可能な資料を参照してください。

https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html

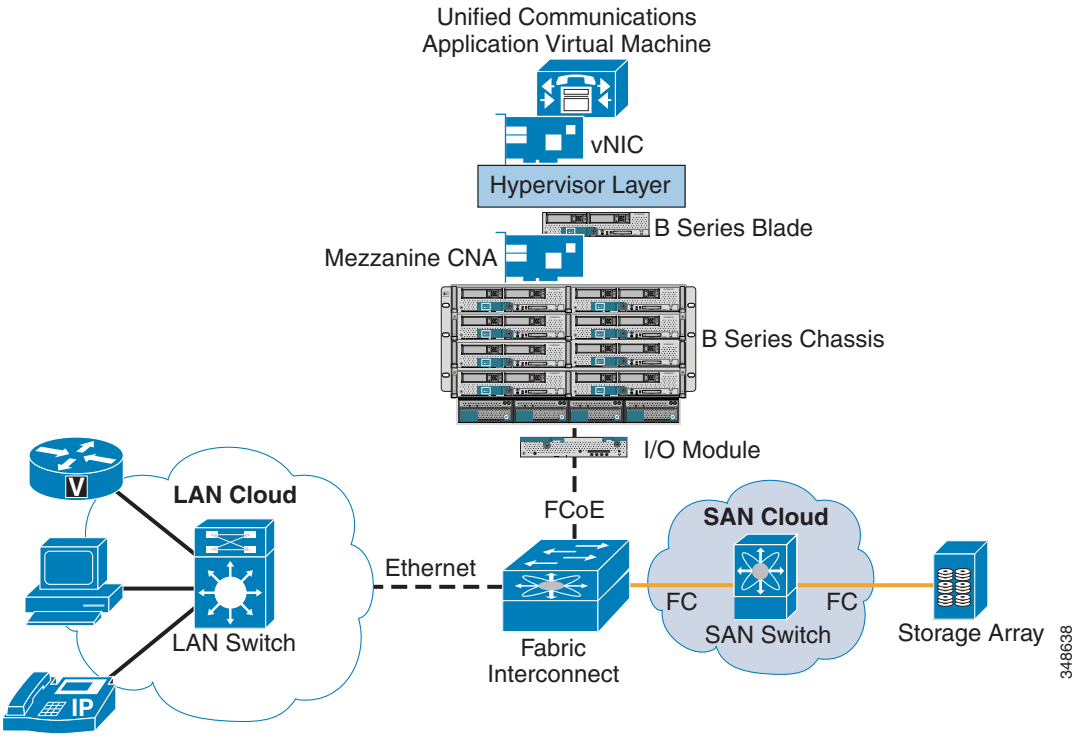
Cisco UCS E シリーズ サーバ モジュールは、Cisco Integrated Services Routers Generation 2（ISR G2）に配置されるように設計されたブレード サーバです。一部の Cisco Collaboration アプリケーションが Cisco UCS E シリーズでサポートされていますが、サポートが制限されている場合があります（たとえば、TRC ではなく、仕様ベースのハードウェア サポートなど）。

Cisco UCS B シリーズ ブレード サーバ

Cisco Unified Computing System（UCS）機能ブレード サーバは、x86 アーキテクチャに基づいています。ブレード サーバは、コンピューティング リソース（メモリ、CPU、および I/O）をオペレーティング システムおよびアプリケーションに提供します。ブレード サーバは、メザニン フォーム ファクタの統合型ネットワーク アダプタ（CNA）を介してユニファイド ファブリックにアクセスできます。

このアーキテクチャでは、Fibre Channel over Ethernet（FCoE）などの技術を利用して、単一のインフラストラクチャで LAN、ストレージ、および高性能コンピューティング トラフィックを転送するユニファイド ファブリックを採用しています（図 10-23 を参照）。シスコのユニファイド ファブリック技術は 10 Gbps イーサネットを基盤とするため、LAN、SAN、およびハイパフォーマンス コンピューティング ネットワークのためにアダプタ、ケーブル、およびスイッチをいくつも用意する必要がありません。

図 10-23　Cisco UCS B シリーズ ブレード サーバでのユニファイド コミュニケーションの基本的なアーキテクチャ



ここでは、プライマリ UCS コンポーネントと、そのコンポーネントが Unified Communications ソリューションで機能する方法について簡単に説明します。Cisco UCS B シリーズ ブレード サーバの詳細については、次の URL で入手可能なモデル比較を参照してください。

https://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-b-series-blade-servers/models-comparison.html

Cisco UCS 5100 シリーズ ブレード サーバ シャーシ

Cisco UCS 5100 シリーズ ブレード サーバ シャーシは、B シリーズ ブレード サーバをホストするだけでなく、Cisco UCS ファブリック エクステンダによってアップリンク ファブリック インターコネクト スイッチへの接続を提供します。

Cisco UCS 2100 および 2200 シリーズ I/O モジュール

Cisco UCS 2100 および 2200 シリーズ I/O モジュール（またはファブリック エクステンダ）は、B シリーズ シャーシに挿入され、Cisco UCS 5100 シリーズ ブレード サーバ シャーシを Cisco UCS ファブリック インターコネクト スイッチに接続します。ファブリック エクステンダは、Fibre Channel over Ethernet（FCoE）プロトコルを使用して、ブレード サーバの FCoE 対応 CNA 間のトラフィックをファブリック インターコネクト スイッチに渡すことができます。

Cisco UCS 6100 および 6200 シリーズ ファブリック インターコネクト スイッチ

Cisco UCS 6100 および 6200 シリーズ ファブリック インターコネクト スイッチは、10 ギガビット FCoE 対応スイッチです。B シリーズ シャーシ（およびブレード サーバ）はファブリック インターコネクトに接続し、ファブリック インターコネクトはデータセンター内の LAN または SAN スイッチング要素に接続します。

Cisco UCS Manager

管理がシステムのすべてのコンポーネントに統合されるため、Cisco UCS Manager を使用して UCS システム全体を単一のエンティティとして管理できます。Cisco UCS Manager では、直観的なユーザ インターフェイスを使用して、すべてのシステム設定操作を管理できます。

ストレージ エリア ネットワーキング

ストレージ エリア ネットワーキング（SAN）を使用すると、リモート ストレージ デバイスまたはストレージ アレイをサーバに接続して、ストレージがサーバにローカルに接続されているようにオペレーティング システムに認識させるようにできます。SAN ストレージは、複数のサーバ間で共有できます。

B シリーズ ブレード サーバ上で仮想 Unified Communications アプリケーションを実行する場合の設計上の考慮事項

ここでは、仮想サーバで Unified Communications サービスを実行する場合に従う必要がある設計規則および考慮事項を示します。

ブレード サーバ

Cisco B シリーズ ブレード サーバは、複数の CPU ソケットをサポートし、各 CPU ソケットは複数のマルチコア プロセッサをホストできます。たとえば、1 つの B200 ブレードには、最大 2 つのマルチコア プロセッサをホストできる CPU ソケットが 2 つあります。また、1 つのブレード サーバで複数の Unified Communications アプリケーションを実行する機能もあります。各 Unified Communications アプリケーションは、専用の処理およびメモリ リソースに割り当てて、リソースがオーバーサブスクリプションにならないようにする必要があります。

SAN およびストレージ アレイ

Cisco UCS B シリーズ プラットフォームに基づいたテスト済みリファレンス構成では、ファイバチャネル SAN ストレージ アレイから実行するために仮想マシンが必要になります。SAN ストレージ アレイは、VMware ハードウェア互換リストの要件を満たす必要があります。iSCSI、FCoE SAN、および NFS NAS などのその他のストレージ オプションは、仕様ベースのハードウェア サポートによりサポートされています。詳細については、次の URL で入手可能なマニュアルを参照してください。

https://www.cisco.com/go/virtualized-collaboration

Cisco UCS C シリーズ ラックマウント

B シリーズ ブレード サーバだけでなく、Cisco Unified Computing System（UCS）も、x86 アーキテクチャに基づいた汎用ラックマウント サーバを特徴としています。C シリーズ ラックマウント サーバは、コンピューティング リソース（メモリ、CPU、および I/O）およびローカル ストレージをハイパーバイザおよびアプリケーションに提供します。C シリーズ サーバの詳細については、次の Web サイトにある資料を参照してください。

https://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html

C シリーズ ラックマウント サーバ上で仮想 Unified Communications アプリケーションを実行する場合の設計上の考慮事項

UCS B シリーズとは異なり、UCS C シリーズに基づいたテスト済みリファレンス構成では、直接接続されたストレージ ドライブでのローカルなハイパーバイザおよびアプリケーションの仮想マシンの保存がサポートされています。FC SAN ストレージ アレイではサポートされていません。C シリーズ サーバで外部ストレージ アレイを使用することができますが、サーバは TRC ではなく、仕様ベースのハードウェアとして見なされるようになります。

詳細については、次の URL で入手可能なマニュアルを参照してください。

https://www.cisco.com/go/virtualized-collaboration

仮想サーバが配置モデルに及ぼす影響

仮想サーバでの Cisco Unified Communications アプリケーションの配置では、物理サーバが使用されるときと同じ配置モデルがサポートされます。ただし、仮想化にはいくつかの考慮事項があります。たとえば、Unified CM VMware 仮想アプリケーションは、ホスト USB およびシリアル ポートにアクセスできません。そのため、Unified CM は、Simplified Message Desk Interface（SMDI）統合の Cisco Messaging Interface（CMI）サービス、オーディオ カード（MOH-USB-AUDIO=）を使用したライブ MoH オーディオ フィードの固定 MoH オーディオ ソースの統合、またはこれらのサーバへのフラッシュ ドライブをサポートしなくなっています。次の代替オプションを使用できます。

- MoH ライブ オーディオ ソース フィードの場合は、ライブ オーディオ ソース接続に Cisco IOS ベースのマルチキャスト MoH を使用することを検討してください。
- システムのインストール ログの保存には、仮想フロッピー ソフトメディアを使用します。

Simplified Message Desk Interface（SMDI）の統合に対する Cisco Messaging Interface（CMI）サービスの代替オプションはありません。

ネットワーク インフラストラクチャ（3-1 ページ）の章では、Cisco UCS B ブレード仮想サーバの QoS 機能をネットワークに統合する方法に関する設計ガイドラインを示します。

Service Advertisement Framework（SAF）の呼制御ディスカバリ（CCD）を使用したコール ルーティングおよびダイヤル プラン配信

Cisco Service Advertisement Framework（SAF）は、呼処理プラットフォームの間でコール ルーティングおよびダイヤル プラン情報を自動的に共有するために使用できる Cisco IOS サービス ルーティング プロトコルです。SAF を使用すると、シスコ以外の呼処理プラットフォーム（TDM PBX など）も Cisco IOS ゲートウェイを介して相互接続して Service Advertisement Framework に参加させることができます。

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

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

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

SAF が Call Control Discovery（CCD）をアドバタイズできるサービス

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

（注）　SAF CCD は、社内 DN 範囲、外部（PSTN）DN 範囲、および URI の配信をサポートする GDPR とは異なり、社内 DN 範囲の配信のみをサポートします。

SAF の動的な特性、およびコール エージェントがホストする DN 範囲と To PSTN プレフィックスの可用性を SAF ネットワーク内の他のコール エージェントにアドバタイズできることにより、静的でより労働集約的な他のダイヤル プラン配布方式を大幅に上回るメリットを提供します。

次のシスコ製品が、SAF に対応した Call Control Discovery（CCD; 呼制御ディスカバリ）サービスをサポートしています。

- Cisco Unified Communications Manager（Unified CM）
- Cisco Integrated Services Router（ISR）上の Cisco Unified Communications Manager Express（Unified CME）
- Cisco ISR プラットフォーム上の Survivable Remote Site Telephony（SRST）
- Cisco ISR プラットフォーム上の Cisco Unified Border Element
- Cisco ISR プラットフォーム上の Cisco IOS ゲートウェイ

CCD は、Cisco IOS Release 15.0(1)M 以降で動作する Cisco ISR プラットフォームでサポートされます。

Unified Communications ネットワーク内の SAF CCD の詳細情報については、次の URL にある『*Cisco Unified Communications System 9.0 SRND*』の「*Unified Communications Deployment Models*」の章の「SAF」の項を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/9x/uc9x/models.html

SAF 自体の詳細については、次の URL にある『*Cisco Collaboration 9.x Solution Reference Network Designs (SRND)*』の「*Network Infrastructure*」の章の「*Service Advertisement Framework (SAF)*」の項を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab09/clb09/netstruc.html

SAF CCD 配置の考慮事項

次のスケーラビリティ制限が、Unified CM および Cisco IOS SAF CCD 製品に適用されます。

- アドバタイズする DN パターンは Unified CM クラスタあたり最大 2,000
- 学習する DN パターンは Unified CM クラスタあたり最大 100,000（デフォルト値 = 20,000 学習パターン）
- アドバタイズする DN パターンは Unified CME、Cisco Unified Border Element、または Cisco IOS ゲートウェイあたり最大 125
- 学習する DN パターンは Unified CME、Cisco Unified Border Element、Cisco IOS ゲートウェイ、または SRST あたり最大 6,000（プラットフォーム依存）

（注）　単一の SAF 自律システム（AS）を使用し、Cisco IOS プラットフォームで実行される Cisco Unified CM および SAF CCD で構成されている SAF 配置では、SAF CCD のシステム全体のスケーラビリティが 6,000 の学習 DN パターンに制限されます。

Cisco Rich Media Conferencing

改訂日：2018 年 3 月 1 日

会議は、特にリモート ユーザや大規模なユーザ ベースのサービスを提供する場合は、コラボレーション システムの基本コンポーネントです。Cisco Rich Media Conferencing は、インスタント、永続的、およびスケジュールされた音声とビデオによる会議、コンテンツ共有などの機能を提供します。

カンファレンス ブリッジは会議機能を提供します。カンファレンス ブリッジとは、複数の参加者を 1 つのコール（音声またはビデオ）に参加させるリソースです。そのデバイス上で 1 つの会議に許可される最大キャパシティまで、所定の会議用に任意の数の接続を受け入れることができます。特定の参加者の出力表示には、表示者自身の入力を除く、接続しているすべての参加者が表示されます。

Cisco Rich Media Conferencing ソリューションでは、さまざまなインフラストラクチャを活用して、音声とビデオによる会議機能およびコンテンツ共有を提供します。会議インフラストラクチャは、ソフトウェアまたは DSP リソースを使用した Cisco Unified CM、Cisco Meeting Server、または Cisco WebEx Collaboration Cloud であり、この章では各ソリューションに関連する設計上の詳細を説明します。

Cisco Rich Media Conferencing ソリューションは、オンプレミス、クラウド、またはハイブリッドの導入環境として使用できます。これにより組織は、すでに投資しているコラボレーション ソリューションとの統合、または「クラウドで」ホストされるサービスの実装を行うことができます。これは、さまざまなソリューション間の重要な違いの 1 つで、組織に最適なソリューションを決定するときに最初に意思決定すべきポイントです。

Cisco WebEx Software as a Service（SaaS）は完全にオフプレミスなソリューションを提供しますが、Cisco Collaboration Meeting Rooms（CMR）Hybrid はオンプレミス機器とオフプレミス機器が混在するハイブリッド ソリューションです。Cisco Collaboration System を導入している組織は、オンプレミス ソリューションを利用することで最も利益を得ます。この章の以降の項では、各会議ソリューションの詳細な導入オプションについて説明します。

表 11-1 は、オンプレミス クラウドの観点から利用可能なソリューションを要約したものです。

表 11-1　Cisco コラボレーティブ ソリューションのオンプレミス、クラウド、およびハイブリッド機能

ソリューション	音声		ビデオ		コンテンツ共有	
	オンプレミス	クラウド	オンプレミス	クラウド	オンプレミス	クラウド
Cisco WebEx Meetings Server	○	X	○[1]	X	○	X
Cisco WebEx SaaS	X	○	X	はい 1	X	○
Cisco Meeting Server	○	X	○	X	○	X
Cisco CMR Hybrid	○	○	○	○	○	○
Cisco WebEx Meeting Center Video Conferencing	X	○	X	○	X	○

1. Cisco WebEx Web カメラのみ。標準ベースのビデオはサポート外。

十分なエンドユーザ エクスペリエンスを実現するには、Cisco Conferencing ソリューションを導入する際に、ユーザが必要な会議機能を使用できるように、慎重な計画と設計を行う必要があります。

設計に役立てるため、この章では Cisco Conferencing ソリューションでサポートされるさまざまなタイプの会議の概要を示すことから始め、その後で、各ソリューションについて次の主要なトピックを詳細に説明します。

- アーキテクチャ

  ここでは、会議ソリューションの主要なコンポーネントの概要を示し、その利点、およびコラボレーション システムのさまざまなコンポーネントを通じて利用可能なさまざまな会議機能について説明します。サポートされる導入モデル、ソリューション、および推奨事項についても、ここで説明します。

- ハイ アベイラビリティ

  ここでは、復元力のある Cisco Conferencing ソリューションの設計に関するベスト プラクティスについて説明しています。また、冗長性とロード バランシングのためのガイダンスが含まれます。

- キャパシティ プランニング

  ここでは、Cisco Conferencing ソリューションのキャパシティ制限と拡張性に関するベスト プラクティスと設計情報を提供します。

- 設計上の考慮事項

  ここでは、Cisco Conferencing ソリューションの設計に関する一般的な推奨事項とベスト プラクティスについて説明します。

この章では、以下の Cisco Conferencing ソリューションについて説明します。

- Cisco WebEx Software as a Service（SaaS）
- Cisco WebEx Meetings Server（プライベート クラウド向け）
- Cisco WebEx Meeting Center Video Conferencing
- Cisco Meeting Server
- Cisco Collaboration Meeting Rooms（CMR）Hybrid

この章の変更点

この章には、Cisco Collaboration System Release（CSR）12.*x* の新規サポートおよび更新された設計が記載されています。Cisco Collaboration System に Conferencing を導入する前に、この章全体をお読みください。

表 11-2 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 11-2　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Collaboration Meeting Rooms（CMR）Premises が Cisco Meeting Server で置き換えられました。	Cisco Meeting Server（11-7 ページ）	2018 年 3 月 1 日
Cisco Collaboration System Release（CSR）12.*x* のコンテンツを再編成した他、いくつかの更新を加えました。	この章の各項で説明	2018 年 3 月 1 日

会議のタイプ

Cisco Rich Media Conferencing ソリューションは次の会議のタイプをサポートします。

- インスタント会議

  音声またはビデオによるインスタント会議（アドホック会議とも呼ばれる）は、臨時会議です。インスタント会議は、会議前にスケジュールまたは用意されません。たとえば、マルチポイント会議にエスカレートされたポイントツーポイント コールは、インスタント会議と見なされます。

- パーマネント会議

  パーマネント会議（ミートミー会議、スタティック会議、またはランデブー会議とも呼ばれる）は、前もってスケジュールすることなく会議を行えるようにする事前定義のアドレスです。会議ホストはその他のユーザとアドレスを共有します。それらのユーザは、いつでもそのアドレスにコールインできます

  パーマネント会議のリソースは先着順に使用されます（確保されません）。会議リソースを保証（確保）するには、スケジュール済み会議を使用する必要があります。

- スケジュール済み会議

  スケジュール済み会議は、Cisco TelePresence Management Suite（TMS）と呼ばれるスケジュール管理システムを使用して開催者によって開始されます。会議は、開始時刻と終了時刻、および任意で事前定義の参加者のセットを指定して、Cisco TMS を介して予約されます。

Cisco Rich Media Conferencing は、以下で説明する会議ソリューションで構成されています。各ソリューションに関する詳細は、それぞれの項で説明しています。

- Cisco Unified CM 音声会議（11-4 ページ）

  このソリューションを採用することで、Unified CM がその内部ソフトウェア コンポーネントまたは外部ハードウェアのデジタル信号プロセッサ（DSP）をリソースとして使用して音声会議を実行できるようになります。

- Cisco Meeting Server（11-7 ページ）

  Cisco Meeting Server は、オンプレミスのビデオ会議ソリューションです。各ユーザには、会議を主催するために使用できるパーソナル スペースがあります。ユーザは Cisco Meeting App から、スペースの作成、スペースへのメンバー追加、PIN の作成などの作業項目を管理できます。

- Cisco Collaboration Meeting Rooms Hybrid（11-54 ページ）

  Cisco CMR Hybrid は、オンプレミス ビデオ会議と WebEx Meeting Center 会議を単一の会議に組み合わせます。これにより、TelePresence および WebEx の参加者が参加し、音声、ビデオ、およびコンテンツを共有できるようになります。CMR Hybrid 会議は、スケジュール済み会議またはスケジュールされない会議のいずれかです。

- Cisco WebEx Meeting Center Video Conferencing（11-37 ページ）

  Cisco WebEx Meeting Center Video Conferencing（旧称 Cisco Collaboration Meeting Rooms（CMR）Cloud）は、オンプレミスの会議リソースや管理インフラストラクチャを必要としない、代替会議導入モデルです。これは、スケジュール済み会議とスケジュールされない会議の両方をサポートし、単一コールで TelePresence、音声、および WebEx の参加者（すべてクラウドでホスト）をサポートします。

- Cisco WebEx Meetings Server（11-44 ページ）

  クラウドベースの Web および音声会議が適していない場合に、オンプレミス WebEx Meetings Server ソリューションを使用できます。この製品は、スタンドアロンの音声、ビデオ、およびコラボレーション Web 会議プラットフォームを提供します。

Cisco Unified CM 音声会議

Cisco Unified CM では、以下のいずれかの手法を使用して音声会議をサポートします。

- ソフトウェア音声会議（11-4 ページ）
- ハードウェア音声会議（11-5 ページ）
- ビルトイン ブリッジ（11-5 ページ）
- Cisco Conference Now（11-6 ページ）

ソフトウェア音声会議

ソフトウェア ベースの音声会議ブリッジは Unified CM の IP Voice Media Streaming Application によって提供されます。このアプリケーションは、クラスタ内の各ノード上でイネーブルにする必要があります。ソフトウェア ユニキャスト カンファレンス ブリッジは、G.711 音声ストリームと Cisco Wideband オーディオ ストリームを混合できる標準の会議ミキサーです。Wideband または G.711 a-law および mu-law ストリームの任意の組み合わせが、同じ会議に接続される場合があります。所定の設定でサポートできる会議数は、カンファレンス ブリッジ ソフトウェアが実行されるサーバと、アプリケーションで有効になっている他の機能によって決まります。ただし、256 はこのタイプのオーディオ ストリームの最大数です。ストリーム数が 256 あれば、ソフトウェア電話会議のメディア リソースで、1 つの電話会議あたり 256 人のユーザに対応できます。また、1 つの電話会議のユーザ数が 4 人の場合は、最大 64 の会議リソースに対応できます。Cisco IP Voice Media Streaming Application サービスおよび Cisco CallManager サービスが同一サーバ上で実行されている場合、ソフトウェア電話会議の最大参加者数は、48 人に限定されます。

Cisco IP Voice Media Streaming Application は、複数の機能に使用することもできるリソースで、設計ではすべての機能を同時に考慮する必要があります（Cisco IP Voice Media Streaming Application（7-3 ページ）を参照）。ソフトウェア音声会議ブリッジの機能は限られているため、このブリッジは、集中型導入環境、またはインスタント音声会議とミートミー音声会議で G.711 コーデックを使用できる導環境でのみ使用することをお勧めします。Unified CM でソフトウェア音声会議ブリッジを使用すると、システムに高い負荷が発生することにも注意が必要です。

ハードウェア音声会議

Cisco IOS によって会議リソースとして設定されるデジタル シグナル プロセッサ（DSP）は、会議機能のみに特化した DSP にファームウェアをロードします。このような DSP は、他のメディア機能には使用できません。単一のシャーシで任意の Cisco PVDM ハードウェアを音声インターフェイスとして同時に使用することはできますが、他のメディア リソース機能として同時に使用することはできない場合があります。PVDM ハードウェアの DSP はそれぞれ個別に音声インターフェイス、会議、メディアの終端、トランスコーディングとして設定されます。そのため、1 つの PVDM の複数の DSP を異なるリソース タイプとして使用できます。DSP は、まず音声インターフェイスに割り当ててから、必要に応じて他の機能に割り当ててください。会議用の DSP リソースは、プロファイル属性に基づいて、実際の参加者数に関係なく、設定の間予約されています。

ハードウェア音声会議ブリッジは、ソフトウェア会議ブリッジより多くの機能およびコーデック形式をサポートします。より多目的な音声会議ブリッジ、および帯域幅を削減するために G.729 のようにより複雑なコーデックのサポートが必要な企業では、ハードウェア音声会議ブリッジを使用することを推奨します。

ビルトイン ブリッジ

ビルトイン ブリッジとは、コール内のエンドポイントのいずれかによってホストされる DSP リソースのことを指します。一部の Cisco IP Phone には、組み込みブリッジ機能用のオンボード DSP が搭載されています。IP Phone の組み込みブリッジは Cisco Rich Media Conferencing アーキテクチャの唯一の組み込み音声リソースです。ただし、組み込みブリッジの会議機能は限定的で、完全な会議の起動には使用できません。Cisco IP Phone の組み込みブリッジで、ユーザは次のことができます。

- IP フォンが使用する複数の異なる回線上のコールを結合し、それらのコールをビルトイン ブリッジでホストされる 1 つの会議に変換します。
- 回線を共有する別のエンドポイントのコールに割り込み（コールがプライベートにセットされていない場合）、そのコールをビルトイン ブリッジでホストされる会議に変換します。
- コールに関与するエンドポイントからサイレント録音またはモニタリング セッションを開始し、この機能を呼び出した IP フォンによって生成および受信されたメディアを分岐します。

Cisco IP Phone の組み込みブリッジは、G.711 および G.729 コーデック形式のエンコードとデコードができます。ただし、一度コールのコーデックが選択されると、組み込みブリッジのコーデック選択はロックされ、電話機で使用するコーデックを変更することはできません。したがって、ベスト プラクティスとして、コールのドロップを避けるために組み込みブリッジが呼び出される可能性があるコール フローを慎重に分析します。

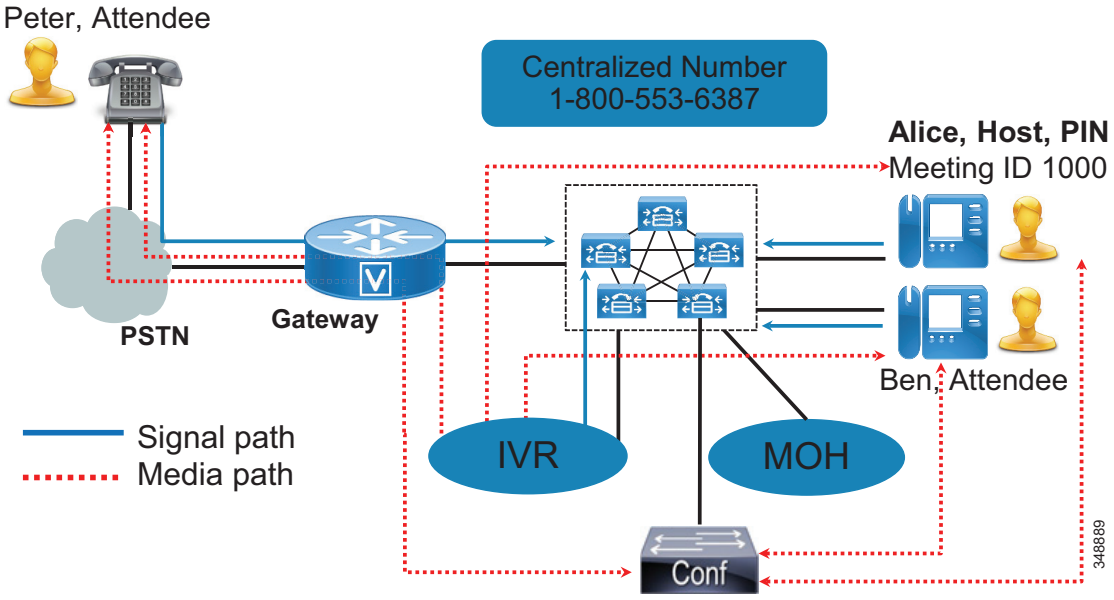
組み込みブリッジは最大 2 コールを混合し、1 コール（2 ストリーム）のみを分岐できます。

Cisco Conference Now

Cisco Conference Now は、Meet-Me に類似したパーマネント会議機能を提供する Unified CM ネイティブ アプリケーションです。このアプリケーションは、基本的な音声会議ソリューションを必要とする小規模なビジネス顧客を対象にしています。Cisco Conference Now で会議に参加するには、ユーザは、一元化された番号にコールインし、音声でガイドされたシステムにより尋ねられたときに、適切な会議 ID と、ホストまたは参加者の PIN を入力するだけです。

図 11-1 に、Cisco Conference Now のアーキテクチャと、関係するコンポーネントを示します。Conference Now では、外部と内部両方の発信者が Conference Now IVR ディレクトリ番号（一元化された会議のアシスタント番号）をダイヤルすることにより会議に参加できます。アナウンスを再生することで会議に参加する参加者をガイドして情報を収集するために、IVR デバイスが使用されます。IVR は、Cisco IP Phone やゲートウェイなどのデバイスに事前に録音されたアナウンス（.wav ファイル）を Unified CM が再生できるようにするメディア リソース デバイスです。

図 11-1　Cisco Conference Now のアーキテクチャ



管理者は、ユーザに対して Conference Now オプションを有効にすることができます。有効にすると、ユーザは会議番号を取得し、会議を開始するホスト PIN を設定する必要があります。また、参加者が会議に参加するためのオプションの参加者アクセス コードを設定できます。会議前に、会議のホストは、すべての参加者に会議番号とオプションのアクセス コードを配布します。会議を開始するには、ホストが Conference Now にダイヤルし、会議番号とホスト PIN の両方を入力します。会議に参加するには、参加者が Conference Now にダイヤルし、会議番号とオプションの参加者アクセス コードを入力します。ホストより前に参加者が会議にダイヤルすると、参加者には保留音（MoH）が流されます。Conference Now は、ホストの発信デバイスに関連付けられているメディア リソース グループ（MRG）およびメディア リソース グループ リスト（MRGL）で設定されているカンファレンス ブリッジを使用して、会議機能を実行します。Conference Now 機能を使用するには、カンファレンス ブリッジと IVR リソースの両方を Unified CM が使用できることを確認してください。

ソフトウェアベースの Cisco IP Voice Media Streaming Application（IPVMS）以外のカンファレンス ブリッジを Unified CM から使用すると、会議参加者の入室音と退出音が提供されない可能性があります。ユーザ エクスペリエンスを快適にするため、Conference Now にソフトウェアベースの Cisco IPVMS カンファレンス ブリッジを使用することを推奨します。会議参加者の入室音と退出音のサポートの詳細については、次の Web サイトで入手可能な『*Feature Configuration Guide for Cisco Unified Communications Manager*』の最新バージョンを参照してください。

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

Cisco Conference Now を実装する際は、次の点を考慮してください。

- IVR はアウト オブ バンド DTMF のみをサポートします。DTMF 機能の不一致を変換するには MTP を使用します。
- IVR は、G.711（A-law および μ-law）、G.729、およびワイドバンド 256K をサポートします。IPVMS は、G.711 およびワイドバンド 256K をサポートします。その他のコーデック サポートでは、トランスコーダを使用します。
- Conference Now は、名簿リストや参加者のミュート/ミュート解除などの高度な機能はサポートしていません。

Cisco Meeting Server

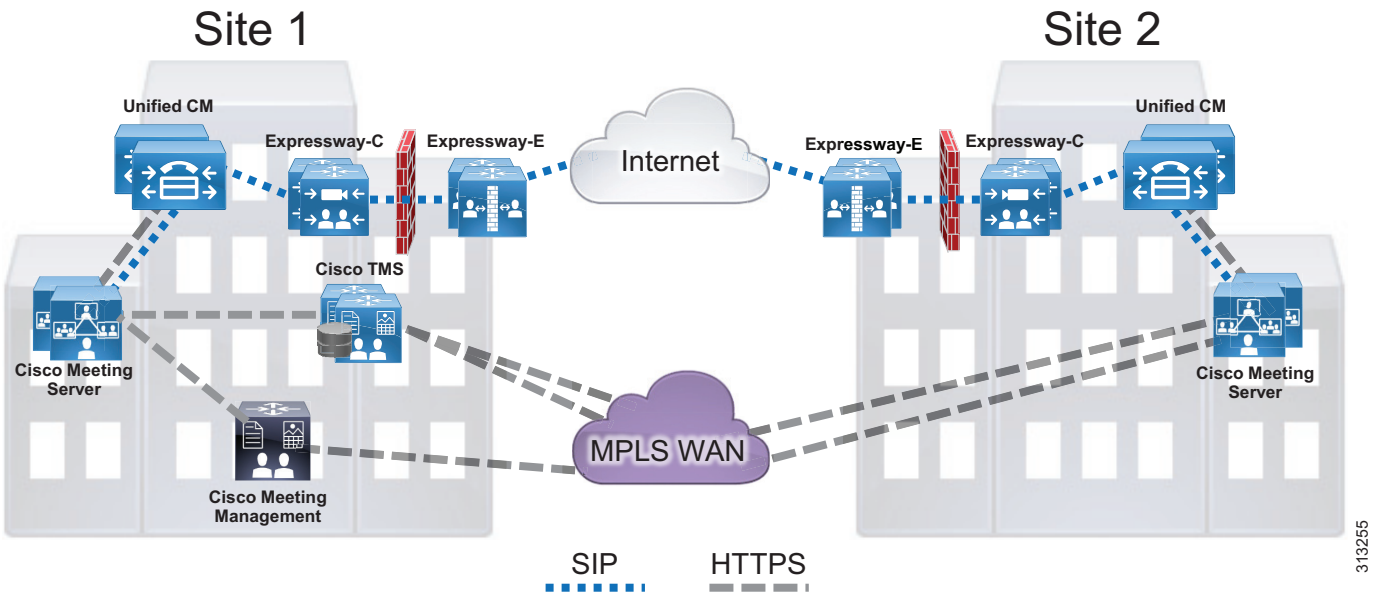
Cisco Meeting Server ではオンプレミスの Cisco インフラストラクチャを使用して、ビジネス品質のビデオ会議と音声会議ならびにコンテンツ共有を可能にします。システム内の各ユーザには、ビデオ アドレス（DN または URI）を関連付けた Always-On のパーソナル スペースを割り当てることができます。参加者はこのビデオ アドレスにダイヤルインして会議に参加できます。Cisco Meeting Server では、Cisco Unified Communications Manager（Unified CM）または Cisco Expressway に登録されたエンドポイントのリッチ会議コラボレーション機能、および音声とビデオの Business-to-Business（B2B）システムとレガシー H.323 ビデオ システムを Cisco Expressway を介して統合する機能を使用できます。このアーキテクチャは、会議ソリューションのさまざまなコンポーネントに依存して、豊富な機能セットを提供します。ここでは、Cisco Meeting Server 会議ソリューションの各コンポーネントを紹介し、それぞれの役割を概説しします。

アーキテクチャ

図 11-2 に、Cisco Meeting Server を使用した会議ソリューションのアーキテクチャを示します。Cisco Meeting Server が会議リソースを提供して管理します。Cisco TelePresence Management Suite（TMS）が会議リソースのプロビジョニング機能とスケジューリング機能を提供し、Cisco Meeting Management が会議の制御機能と管理機能を提供します。Cisco Unified Communications Manager（Unified CM）はコール制御システムとして機能します。または、Cisco Unified CM の代わりに Cisco Expressway をコール制御システムとして使用することできます。Cisco Meeting Server がサポートするのは SIP コール制御のみですが、Cisco Expressway を使用することでレガシー H.323 ビデオ システムとの連動が可能になります。Cisco Meeting Server はあらゆるタイプの会議をサポートする会議ブリッジであり、ここに、SIP トランク経由で Unified CM が接続されます。

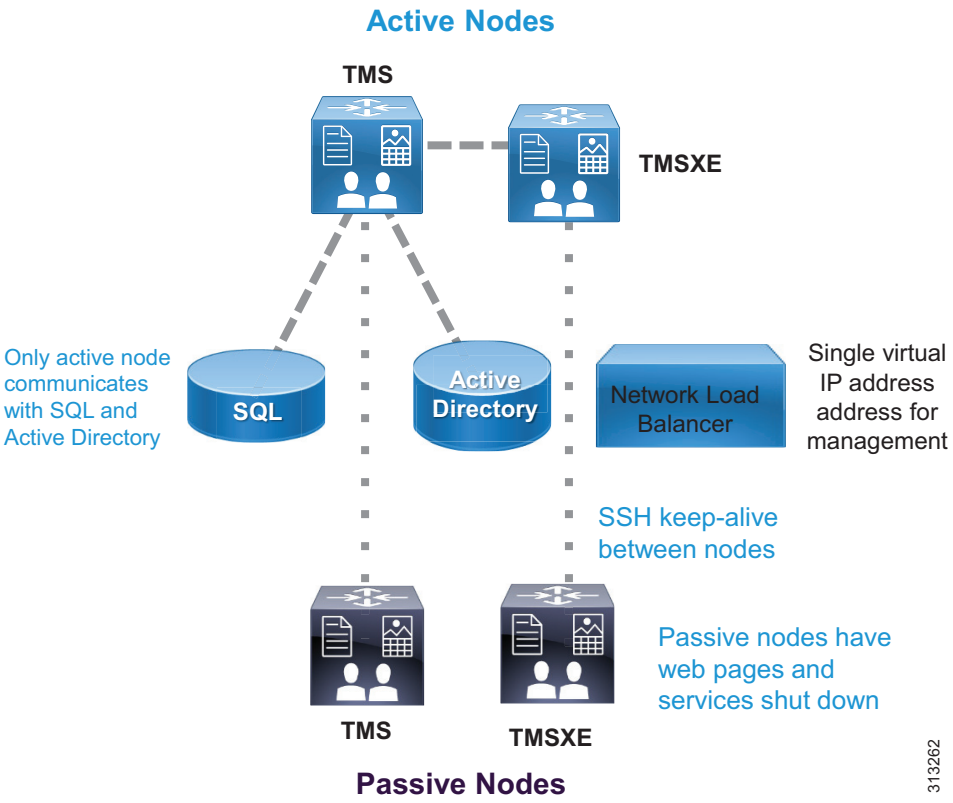
Cisco Unified CM は XML-RPC over HTTPS を使用して Cisco Meeting Server と通信し、インスタント会議の会議ブリッジを制御します。Cisco TMS は REST API 接続を使用して Cisco Meeting Server にリンクし、会議リソースのプロビジョニングとスケジューリングを行います。Cisco Meeting Management が使用する Cisco Meeting Server とのインターフェイスには、REST API と呼詳細レコード（CDR）の 2 つがあります。REST API インターフェイスは Cisco Meeting Server で操作を実行する際に使用し、CDR インターフェイスは Cisco Meeting Server からコール イベントを受信する際に使用します。

図 11-2　Cisco Meeting Server のアーキテクチャ概要



スケジューリング アーキテクチャは、Cisco TMS および TelePresence Management Suite Extension for Microsoft Exchange（TMSXE）それぞれのアクティブ ノードとパッシブ ノードで構成されています。これらのノードは、ネットワーク ロード バランサの背後に導入されます。アクティブ ノードが着信要求を処理する一方、パッシブ ノードはスタンバイ モードで稼働し、その Web ページとサービスをロックした状態に維持して着信トラフィックを拒否します。大規模な導入環境では、Cisco TMS と TMSXE を別々の仮想マシン上にインストールする必要があります（図 11-3 を参照）。Cisco TMS サーバを設置する場所は、組織の SQL 導入環境もホストしている顧客データ センターです。すべてのサーバ ノードは、1 つの外部 Microsoft SQL データベースから機能します。さらに、エンドポイント、Cisco Meeting Server、Unified CM を合わせると完全な会議コンポーネントとなりスケジューリングに対応できます。

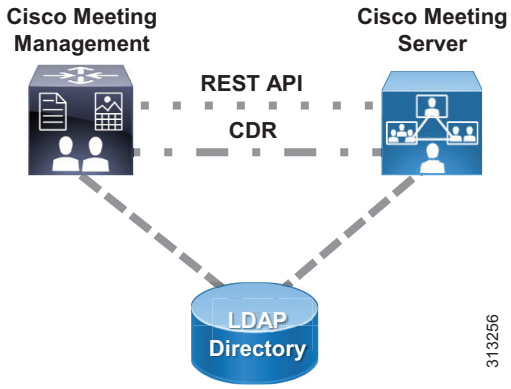
図 11-3　　スケジューリング アーキテクチャの概要



Cisco Meeting Management は Cisco Meeting Server の外部にある別個のサーバ上で、Cisco Meeting Server 導入環境専用として稼働します。前述したように、Cisco Meeting Management は REST API リンクを使用して Cisco Meeting Server で操作を実行します。Cisco Meeting Management は CDR インターフェイスを使用して、Cisco Meeting Server からコール関連のイベントを受信するため、会議がいつ開始または終了したのかということや、その他のコール アクティビティを認識します。ユーザがポータルにログインする際は、LDAP ディレクトリに対してユーザの認証が行われます。さらに、Cisco Meeting Management はディレクトリ内部に設定されたグループを使用して、ユーザのロール（ビデオ オペレータまたは管理者）を判別します。Cisco Meeting Management ポータル上で使用可能なオプションは、ユーザのロールに応じて異なります。（図 11-4 を参照）。

（注） Cisco Meeting Management を導入するために最低限必要なバージョンは Cisco Meeting Server 2.1.5 ですが、バージョン 2.2 以降を使用することをお勧めします。

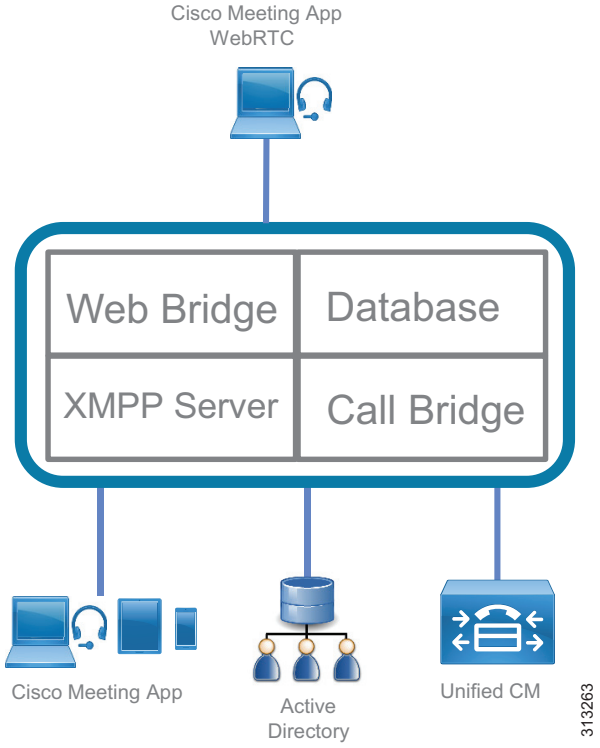
図 11-4　Cisco Meeting Management のアーキテクチャ



Cisco Meeting Server の役割

図 11-5 に、ビデオ会議機能を提供する Cisco Meeting Server のコア会議コンポーネントを示します。コール ブリッジ コンポーネントにはコールを制御するための Cisco Unified CM が統合され、会議機能を実行するためのリソースがここから提供されます。すべての Cisco Meeting Server 会議はスペース上でホストされます。スペースとは、音声、ビデオ、コンテンツ共有機能を備えた仮想会議室のことです。スペースには、スペース URI または電話電話番号を使ってアクセスできます。ユーザをシステムにインポートするために、Cisco Meeting Server には Microsoft Active Directory などのディレクトリ サーバを統合する必要があります。ユーザのインポート プロセス中に、フィールド マッピング式の設定に従ってスペースが作成されます。ユーザとスペースに関するすべての情報はデータベースに格納されます。参加者が会議に参加するには、シスコまたはサードパーティ製の標準の SIP ビデオ エンドポイント、Cisco Jabber Clients、または Cisco ミーティング アプリケーションを使用できます。Cisco ミーティング アプリケーションを使用してログインする場合、ユーザの認証は XMPP サーバによって行われます。WebRTC クライアントのユーザは、ログイン後に Web ブリッジによってコール ブリッジに接続されます。

図 11-5　Cisco Meeting Server のコア会議コンポーネント



Cisco ミーティング アプリケーションは、Cisco Meeting Server のクライアントです。このアプリケーションは、ネイティブ デスクトップ/モバイル アプリケーションである場合も、WebRTC ブラウザ アプリケーションである場合もあります。ユーザは Cisco ミーティング アプリケーションを使用して、会議にログインして参加し、音声とビデオならびにコンテンツ共有を使用できます。WebRTC クライアントを使用すると、Cisco Meeting Server 上にアカウントがないユーザでも、互換性のあるブラウザを使用することで、ゲストとして会議に参加できます。さらに、ユーザは Cisco ミーティング アプリケーションを使用して会議を実行し、アクション（参加者の表示、参加者のミュート/削除、録音の開始/停止、独自のスペースの作成/編集など）を実行することができます。

（注） WebRTC アプリケーションは、互換性のある特定のブラウザ上でのみ稼働します。サポートされているブラウザについて詳しくは、https://kb.acano.com/content/37/4/en/what-versions-of-browsers-do-we-support-for-webrtc-app.html に掲載されている情報を参照してください。

（注） Cisco ミーティング アプリケーションをエンタープライズ ネットワークの内部または外部のどちらに導入しても、会議に参加できます。導入の詳細については、https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html から入手できる Cisco Meeting Server のコンフィギュレーション ガイドを参照してください。

会議に Cisco Meeting Server を使用すると、以下のことをはじめとしいくつかの利点があります。

- 小規模な導入環境でも大規模な導入環境でも、必要に応じて簡単に拡張して、キャパシティを徐々に追加できます。
- あらゆるタイプのデバイスで、簡素化された直感的かつ最適な会議エクスペリエンスを創出できます。
- マルチパーティ ランセンスを使用する場合、基盤となるハードウェアで対応可能な限り、参加者が何人でも会議に参加できます。
- 単一の導入モデルをあらゆる会議タイプに適用できます。

Cisco TelePresence Management Suite（TMS）の役割

Cisco TelePresence Management Suite（TMS）は、会議のスケジューリングならびに会議室システムの予約を行います。Cisco Unified CM でエンドポイントの設定管理が維持されていれば、Cisco TMS はそれらのエンドポイントにカレンダーをプッシュできます。管理者は、組織のデフォルト会議のパラメータを設定してから、そのテンプレートに基づいて個々の会議を作成することができます。

Cisco TelePresence Management Suite Extension for Microsoft Exchange（TMSXE）の役割

エンドユーザが Microsoft Outlook で複数の会議室リソースを使用して 1 つの会議をスケジュールすると、Microsoft Exchange の Exchange Web Service（EWS）機能により、そのイベントが Cisco TMS にスケジュール済み会議として同期されます。この同期は双方向であるため、管理者またはサポート担当員が、会議主催者の Outlook イベントにアクセスせずに、会議を更新できます。組織内のエンドポイント リソースのうち、この会議に使用する予定のエンドポイント リソースはすべて、同じ 1 つの Microsoft Exchange 会議要求内にリストされている必要があります。

Cisco Meeting Management の役割

Cisco Meeting Management は Cisco TMS を必要としないスタンドアロンのツールですが、Cisco TMS と併せて使用することで、Cisco Meeting Sever を完全に管理するための機能が揃うことになります。お客様に対するコンシェルジュ サービスを提供する Meeting Manager が Cisco Meeting Management に備わっています。Meeting Manager は、すべてのアクティブな会議をそれぞれの詳細と併せてリストします。また、特定の会議内では、その会議の参加者全員がリストされ、録音またはストリーミングの開始/停止、レイアウトの変更、参加者の追加/除外、会議の終了などの操作を実行できます。個々の参加者は、音声/ビデオのミュート/ミュート解除、レイアウトの変更、コール統計の表示といった操作を行うことができます。

Cisco Meeting Server エッジ

Cisco Meeting Server エッジを使用することで、外部ユーザがインターネットから Cisco ミーティング アプリケーションを使用して会議に参加できるようになります。この導入環境では、外部ユーザはエッジ ソフトウェア コンポーネントとやり取りを行い、これらのコンポーネントがコア ソフトウェア コンポーネントと通信します。エッジ コンポーネントは DMZ 内に配置され、コア コンポーネントはエンタープライズ ネットワーク内に配置されます。外部ユーザが接続すると、そのコールはエッジ コンポーネントにルーティングされてから、コア コンポーネントにルーティングされます。エッジ コンポーネントの導入オプションとしては、単一の統合導入環境（図 11-6）と単一の分割導入環境（図 11-7）の 2 つがあります。

単一の統合導入環境では、エッジ コンポーネントとコア コンポーネントを両方とも同じサーバ内に展開します。ただし、エッジ コンポーネントは DMZ ネットワーク内に配置され、コア コンポーネントはファイアウォール内部のエンタープライズ ネットワークに配置されます。単一の分割導入環境では、エッジ コンポーネントとコア コンポーネントをそれぞれ異なる 2 つのサーバに導入して分離します。エッジ コンポーネントは、DMZ 内に物理的に置かれたサーバに導入し、コア コンポーネントは企業のファイアウォール内に置かれた別個のサーバに導入することになります。

図 11-6　　単一の統合導入環境

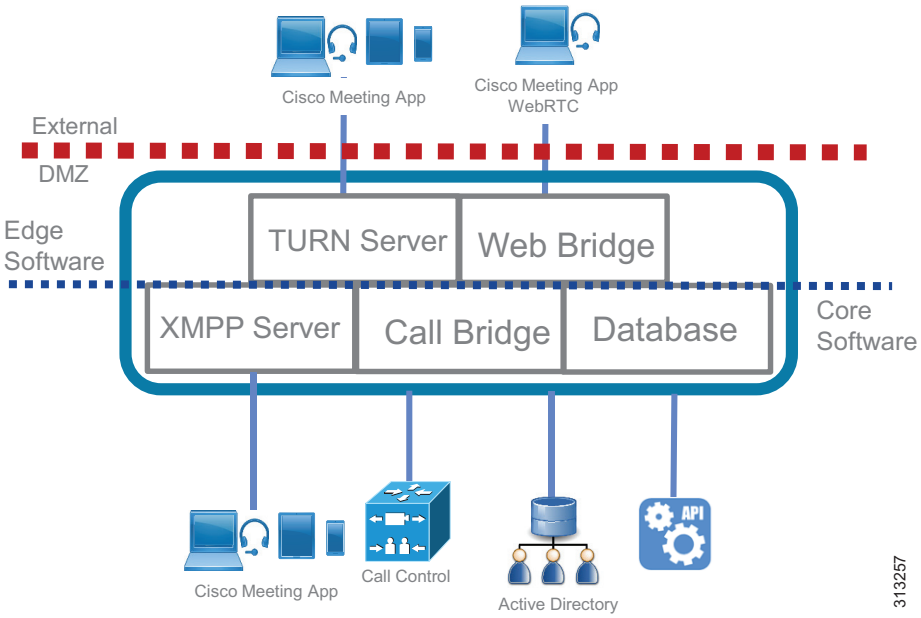
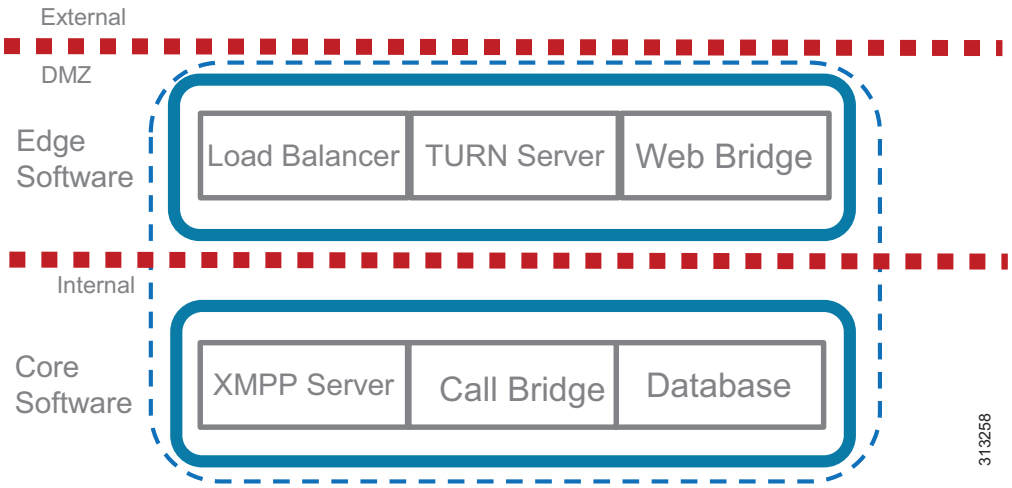


図 11-7　　単一の分割導入環境



WebRTC クライアントを使用する外部ユーザは、DMZ 内の Web ブリッジに直接接続します。TURN サーバで提供されるファイアウォール メディア トラバーサル技術により、Cisco Meeting Server をファイアウォールまたは NAT の背後に導入することができます。TURN は Cisco Meeting Server 導入環境に組み込まれており、追加のライセンスは不要です。

分割導入環境においては、ロード バランサが、外部 Cisco ミーティング アプリケーションの単一の接続ポイントを提供します。ロード バランサは外部インターフェイスとポートで着信接続をリッスンします。ロード バランサはまた、XMPP サーバからの着信 TLS 接続も受け入れます。この接続では、ロード バランサが外部クライアントからの TCP 接続を多重化できます。これにより、コア コンポーネントとエッジ コンポーネント間に TLS トランクが形成されます。ロード バランサにも追加のライセンスは必要ありませんが、Call Bridge が有効にされている必要があります。

単一の統合導入環境および単一の分割導入環境について詳しくは、以下のリンク先から入手できる該当する導入ガイドを参照してください。

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

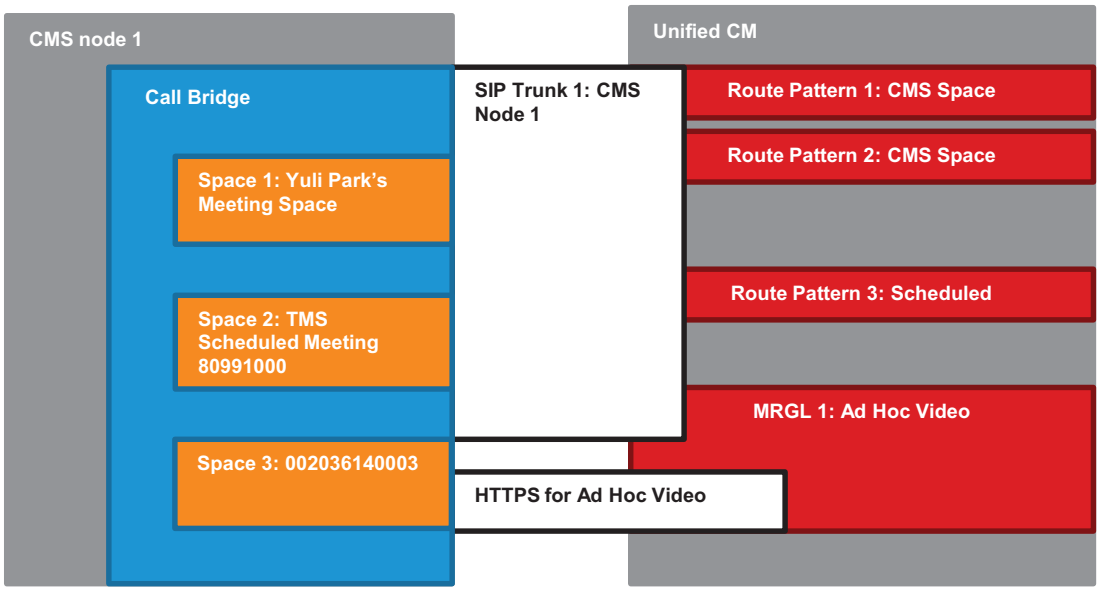
Cisco Meeting Server 2.1.2 および Cisco Expressway X8.10 からは、WebRTC クライアントを使用する外部ユーザが Expressway を介して Cisco Meeting Server に接続できるようになっています。導入環境について詳しくは、以下のリンク先から入手できる最新バージョンの *Cisco Expressway Web Proxy for Cisco Meeting Server* 導入ガイドを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

会議のコール フロー

Cisco Unified CM により、デバイス登録と、接続されたエンドポイント間での音声およびビデオ コールのルーティングが行われます。パーマネント会議、インスタント会議、スケジュール済み会議のコールは、いずれも単一の SIP トランク経由で Cisco Meeting Server 上のコール ブリッジにルーティングされます。各コール ブリッジには、個別の SIP トランクが必要です。インスタント会議の XML-RPC 要求を Cisco Meeting Server ノードに送信する HTTPS 接続が Unified CM ノード上に設定されます（図 11-8 を参照）。ユーザがデバイス上の会議ソフトキーを押して 2 者間通話を 3 者間通話にエスカレートする際は、会議をホストするための一時スペースを作成するために、Unified CM が API リクエストをこの HTTPS 接続を介して Cisco Meeting Server に送信します。インスタント会議、パーマネント会議、スケジュール済み会議をホストするスペースは、さまざまなコンポーネントによって作成されます。

図 11-8　Cisco Unified CM と Cisco Meeting Server の SIP トランク

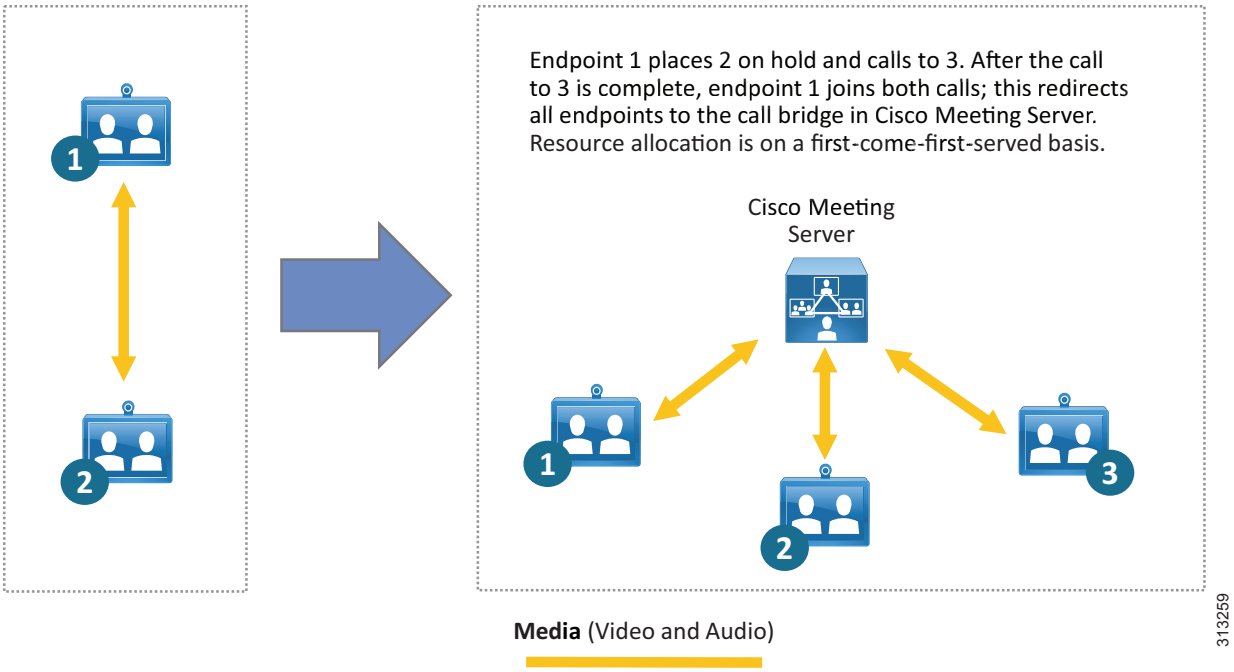


Unified CM によって管理されるインスタント コール フローは、スケジュール会議など、その他の方法で作成された会議への参加者を追加するために使用できません。また、他のコール フローを使用して、インスタント会議への参加者を追加することもできません。インスタント コール エスカレーション方式は、その方法で作成されたインスタント会議でのみサポートされます。その他の方法で生成された会議をインスタント メカニズムで拡張することはできません。これにより、チェーン会議の可能性を回避できます。

インスタント会議

インスタント会議では、2 者間のポイントツーポイント コールに関与するエンドポイントを、Unified CM 会議ブリッジ リソースを使用して 3 者間のマルチポイント コールにエスカレートさせることができます。インスタント会議では、Unified CM と Cisco Meeting Server 上のコール ブリッジの間にある SIP トランクに関連付けられた HTTPS XML-RPC 接続を使用します。ユーザが会議ソフトキーを押してインスタント会議を開始すると、Unified CM は Cisco Meeting Server 上に一時スペースを作成するために、HTTPS 接続を使用して API 要求を発行します。一時スペースが作成されると、Unified CM はそのスペースに、SIP トランク経由ですべての参加者をルーティングします。会議が終了した時点で、Unified CM はそのスペースを Cisco Meeting Server から削除するために、別の API 要求を発行します。図 11-9 に、Cisco Meeting Server を使用してインスタント会議を開始する例を示します。

図 11-9　Cisco Meeting Server を使用したインスタント会議の開始



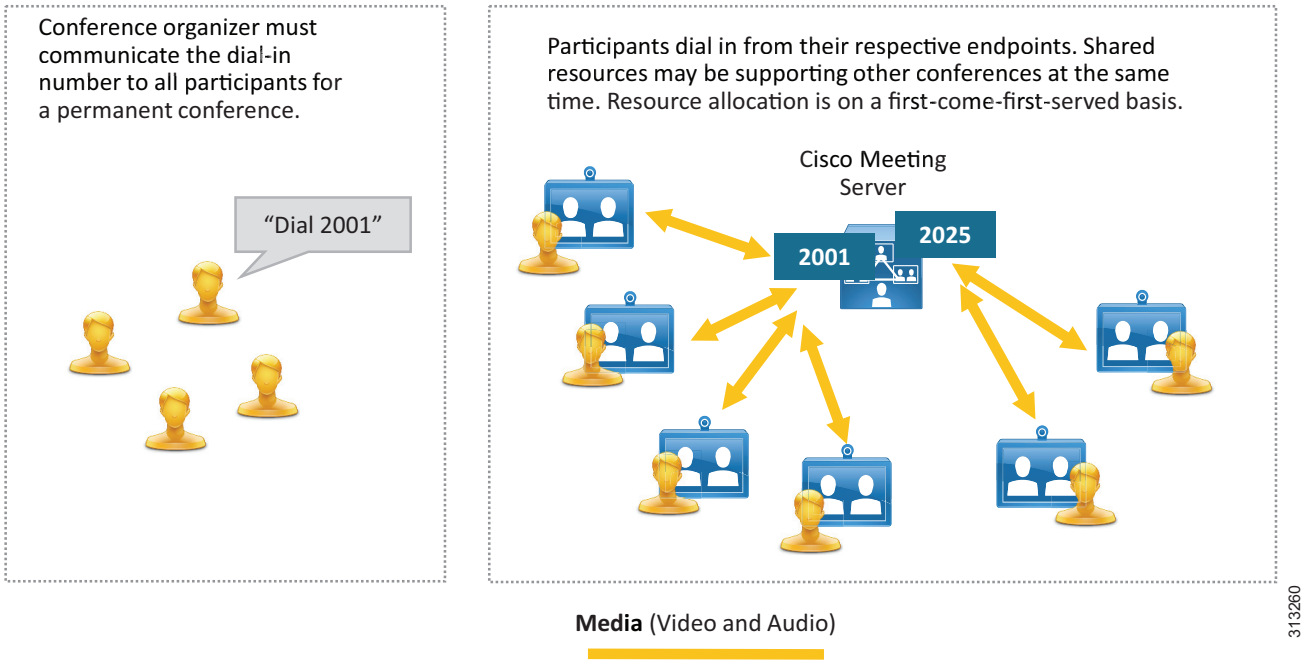
Cisco Meeting Server スペースを使用したパーマネント会議

パーマネント会議は、Cisco Meeting Server スペースを使用して展開されます。パーマネント タイプの会議を提供するスペースは、LDAP からのユーザ インポート プロセスの一環として作成されます。各スペースにはビデオ アドレス（URI または DN、あるいはその両方）が関連付けられ、ユーザはこのビデオ アドレスを使用して会議に参加できるようになっています。管理者はフィールド マッピングを使用してスペースの属性（名前、ユーザ名、URI など）を指定し、これらのマッピングを使用してスペースを作成できます。ユーザは作成されたスペースに Cisco ミーティング アプリケーションを使用してログインし、そのスペースにメンバーを追加することができます。ユーザは Cisco ミーティング アプリケーションにログインして、他のスペースを作成し、メンバーを追加することもできます。このタイプの会議には、Unified CM と Cisco Meeting Server 上のコール ブリッジとの間に SIP トランクが必要です。

パーマネント会議を開始するには、会議開催者が使用するコール制御に応じて、いくつかの方法（IVR ダイヤルイン、事前設定されたビデオ アドレスなど）があります。図 11-10 に、ビデオ アドレスをダイヤルしてパーマネント会議を行う例を示します。

管理者によってパーマネント会議のビデオ アドレスが事前設定された後は、そのビデオ アドレスが恒久的に使用可能になります。ユーザはそのビデオ アドレスをダイヤルすることで、会議を開始したり、会議に参加したりできます。

図 11-10　　パーマネント会議の例



別の方法として、ユーザは Cisco Meeting Server に組み込まれている自動音声応答（IVR）を使用して会議にダイヤルインすることもできます。この場合、IVR により、参加対象の会議の会議 ID と、パスワード（設定されている場合）の入力がユーザに求められます。

スケジュール済み会議

Cisco Meeting Server は、Cisco TMS での会議のスケジューリングをサポートしています。スケジュール済み会議には、Unified CM と Cisco Meeting Server 上のコール ブリッジとの間に SIP トランクが必要です。Unified CM は、スケジュール済み会議の参加者を SIP トランクの接続先にルーティングします。Cisco Meeting Server に対する REST API 要求を HTTPS 接続で送信するには、Cisco Meeting Server を Cisco TMS に追加する必要があります。管理者がスケジュール済み会議用の数値による ID の範囲を指定すると、Cisco TMS は API リンクを使用して、数値による ID ごとに Cisco Meeting Server 上に非アクティブのスペースを作成します。開催者が会議をスケジュールすると、Cisco TMS は、指定された範囲からランダムにダイヤルイン番号を選択します。スケジュール済み会議の開始時刻になると、Cisco TMS は API を使用してスペースをアクティブ化し、参加者が参加できるようにします。スケジュール済み会議にはさまざまな方法で参加できます（表 11-3 を参照）。

表 11-3　　スケジュール済み会議のコール起動オプション

起動方式	説明
ワンボタン機能（OBTP）（One Button to Push）	• 会議のダイヤルイン情報は OBTP をサポートするエンドポイントに自動的に表示されます。OBTP をサポートしないシステムの場合、参加者に転送するための会議情報の電子メールが会議のオーナーに送信されます。
自動接続（Automatic Connect）	• すべてのエンドポイントは、指定された日時に自動的に接続されます。

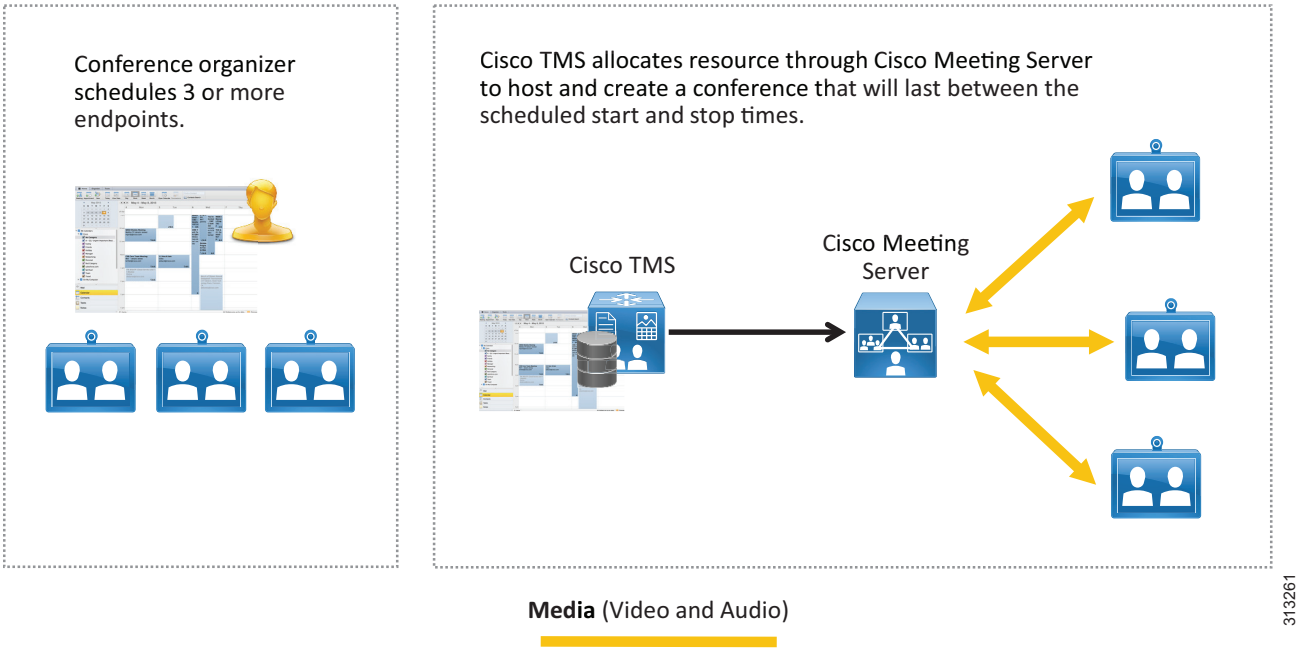
表 11-3　スケジュール済み会議のコール起動オプション（続き）

起動方式	説明
手動接続（Manual Connect）	• 会議は、特定のエンドポイント（通常は、会議開催者のエンドポイント）が接続されるまで開始できません。その特定のエンドポイントが接続されると、残りのエンドポイントが自動的に接続されるか、それらのエンドポイントが手動によってダイヤルインすることが可能になります。
予約（Reservation）	• この方法では、エンドポイントは予約されますが、接続が開始されることはありません。

スケジューリングは、エンドポイントおよびポート リソースの可用性が保証されるよう試みられるため、会議に接続する便利な方法を提供します。大部分の企業は、カレンダー アプリケーションを使用して会議のスケジュール作成しています。この場合、カレンダー統合によって、ユーザが既存のカレンダー クライアントを使用して会議をスケジュールすることが可能となります。TelePresence 導入環境には、多くの場合、大量のエンドポイントと各種のインフラストラクチャ コンポーネントが組み込まれます。一元管理を行わなければ、不可能ではないにしても、コンポーネントのプロビジョニングやリソースのモニタリングが困難になります。管理プラットフォームは、これらのプロセスを大幅に簡素化します。

スケジュール済み会議は、会議リソースとエンドポイントに企業のカレンダー アプリケーションを統合することによって機能するようになります（図 11-11 を参照）。Cisco TelePresence Management Suite（TMS）は、エンドポイントとカレンダー アプリケーションの間に存在し、各スケジュール済み会議に適したブリッジ リソースを特定します。スケジュール済み会議を TelePresence Management Suite で導入し、3 つ以上のエンドポイントをスケジューリングして会議を作成することを推奨します。

図 11-11　カレンダー アプリケーションとの統合を使用したスケジュール済み会議



会議のセキュリティ

Cisco Unified CM は、Cisco Meeting Server との間でセキュリティ保護された SIP トランクを使用することによって、セキュリティな会議をサポートします。セキュアな会議では、Unified CM はコール シグナリングに TSL を使用し、メディア ペイロード暗号化に SRTP を使用します。ただし、会議全体がセキュアになるのは、すべての参加者エンドポイントがビデオ暗号化をサポートしている場合に限られます。Cisco Unified CM と Cisco Meeting Server 間の API インターフェイスを暗号化して、HTTPS が使用されるようにする必要があります。

（注）　Cisco Meeting Server リリース 2.3 以降では、デフォルトで、すべての接続に TLS バージョン 1.2 を使用します。

Cisco Meeting Server は外部コンポーネントとの通信にも内部コンポーネント間の通信にもセキュアな接続を使用するために、証明書が必要です。自己署名証明書と認証局（CA）署名付き証明書の両方がサポートされますが、導入環境では CA 署名付き証明書を使用することをお勧めします。証明書の導入と要件について詳しくは、以下のリンク先から入手できる最新バージョンの『*Cisco Meeting Server Certificate Guidelines*』を参照してください。

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

PIN やパスワードを使用して会議へのアクセスを制限するため、別レベルのセキュリティを追加できます。どのスケジュール済み会議またはパーマネント会議でも、PIN を設定して、すべての参加者がその PIN を入力しなければ接続が許可されないようにすることができます。

セキュア会議の詳細については、Cisco Collaboration Security（4-1 ページ）を参照してください。

会議のハイ アベイラビリティ

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

スケジュール済み会議でも、スケジュールされていない会議でも、ハイ アベイラビリティには Cisco Unified CM、Cisco Meeting Server、Cisco TMS が関与します。

Cisco Unified CM のハイ アベイラビリティ

会議サービスでハイ アベイラビリティを実現するには、Cisco Meeting Server と Cisco Unified CM 間のリンクを冗長構成にして、Cisco Meeting Server への一方のリンクがダウンしても、バックアップ リンクでサービスを提供できるようにする必要があります。これらのリンクには、インスタント会議のメディア リソース グループとメディア リソース グループ リスト、および Cisco Meeting Server にコールをルーティングするためのルート グループとルート リストを組み込みます。

メディア リソース グループとメディア リソース グループ リスト

コール制御として Cisco Unified CM を使用している Cisco Collaboration エンドポイントで、ユーザが CONF ソフトキーをアクティブにすると、Unified CM はメディア リソース マネージャを使用して会議ブリッジを選択します。会議ブリッジ リソースは、メディア リソース グループ（MRG）で設定されます。メディア リソース グループ リスト（MRGL）は、優先順位順に並べられた MRG のリストを指定するものであり、エンドポイントと関連付けることができます。メディア リソース マネージャでは、エンドポイントの MRGL を使用して、会議ブリッジを選択します。リソースをグループ化する方法は完全に自由ですが、所定のサイトのすべてのエンドポイントが最も近いカンファレンス ブリッジを使用するように、可能な限り地理的な配置の論理モデルを使用して、リソースをグループ化することを推奨します。

Cisco Unified CM では、以下の基準に基づき（記載されている順）、会議ブリッジを選択します。

1. メディア リソース グループ リスト（MRGL）にリストされているメディア リソース グループ（MRG）の優先順位
2. 選択された MRG の中で、最も使用されていないリソース

メディア リソースの設計の詳細については、メディア リソース（7-1 ページ）の章を参照してください。

ルート グループとルート リスト

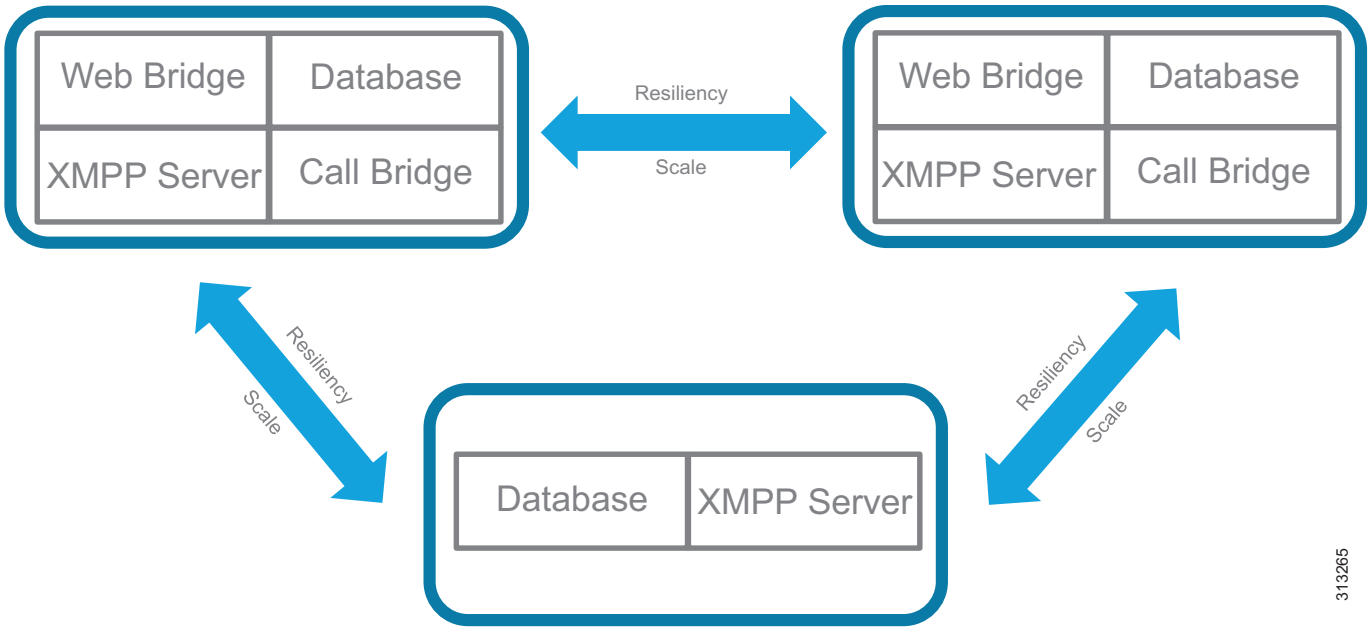
ルート リストおよびルート グループは、Cisco Unified CM ドメインから出て行くコールの信頼性を確保する共通のコール ルーティング メカニズムです。バックアップ会議ブリッジが存在する場合、Cisco Unified CM がトランクとして統合されているメディア リソースでは、ルート リストおよびルート グループを使用してハイ アベイラビリティを実現する必要があります。コール アドミッション制御は、コールに使用されるトランクに基づいてメディア リソースの場所を設定することで維持できます。

ルート リストおよびルート グループの復元力メカニズムについては、ダイヤル プラン（14-1 ページ）の章を参照してください。

Cisco Meeting Server のハイ アベイラビリティ

1 つ以上のサーバに追加のコンポーネント インスタンスを導入して、これらのコンポーネント インスタンスの間で負荷を共有し、あるインスタンスで障害が発生しても、バックアップ インスタンスでその負荷を引き継げるようにすることで、Cisco Meeting Server の復元力を実現できます。さらに、XMPP サーバ、コール ブリッジ、データベースをまとめてクラスタ化し、単一のインスタンスとして動作させることも可能です（図 11-12 を参照）。

図 11-12　ハイ アベイラビリティ対応 Cisco Meeting Server クラスタの最小構成



標準的な Cisco Meeting Server クラスタは、コール ブリッジ サービスが有効にされた 2 つ以上（最大 8 個）のノードで構成されます。ノード間の最大ラウンド トリップ時間（RTT）は 300 ミリ秒です。コール ブリッジ クラスタのピアは、フル メッシュ構成で分散リンクを使用して相互接続されます。分散リンクとは、ノード間でコール シグナリングおよび制御状況メッセージを受け渡しするために使用される HTTPS 接続です。コールは、クラスタ内のどのノードにも送信できます。ある 1 つのノードがダウンした場合、Unified CM は残りのコール ブリッジ ノードにコールをルーティングして会議に参加させることができます。会議の開催中にコール ブリッジで障害が発生した場合は、それらのコールがドロップされるため、参加者は同じ番号をダイヤルして、新しいコール ブリッジ上の会議に参加する必要があります。Unified CM のルート グループおよびルート リスト コンストラクトを使用して、コールを SIP トランク経由で Cisco Meeting Server に分配することができます。

データベース クラスタを構成するのは 1 つのマスターと複数のスレーブ（最大 5 つのノード）で、ノード間の最大 RTT は 200 ミリ秒です。データベース マスターは読み取り操作と書き込み操作の両方を実行する一方、スレーブは読み取り操作のみを実行します。コール ブリッジは読み取り/書き込み操作を行うためにデータベース マスターに常に接続され、マスター上で行われた変更のすべてがスレーブに複製されます。ローカル データベースを使用するコール ブリッジは、ローカル データベース クラスタのマスターに自動的に接続されますが、ローカル データベースがないコール ブリッジについては手動でデータベース クラスタに接続する必要があります。マスターで障害が発生した場合、スレーブのうちの 1 つが新しいマスターになり、残りのスレーブはこの新しいマスターに再登録されます。元のマスターで障害が解消されると、それはスレーブとして新しいマスターに登録されます。ネットワーク パーティションが発生した場合、クラスタ メンバーの過半数を認識できるデータベース ノードのみが、マスターに昇格する対象と見なされます。同様に、過半数のクラスタ メンバーを認識できない既存のマスターはスレーブに降格されます。これは、複数のマスターが作成されないようにするための仕組みです。したがって、データベース クラスタが偶数（2 または 4）のノードで構成されている場合、ネットワークがノード数を均等に分けた 2 つのセグメントにパーティション化されると、どちらのセグメントでもマスターがクラスタ メンバーの過半数を認識することはできなくなるため、マスターはスレーブに降格されます。この場合、クラスタ内にマスターは存在しなくなります。それでもコール ブリッジはコールを受け取ることができますが、データベースへの書き込み操作は不可能になります。このことから、常にマスターが選出されるよう、奇数のノードでデータベース クラスタを構成することを推奨します。つまり、クラスタを構成するデータベース ノードの最小数は 3 になるということです。

XMPP の復元力により、特定の XMPP サーバにアクセスできないクライアントに対するフェールオーバー保護が講じられます。XMPP サーバ クラスタは、奇数の XMPP サーバ ノード（最小 3 つのノード）を使用して構成されていなければなりません。これは、Cisco Meeting Server で XMPP サーバ マスターを選出するためには、クラスタ ノードの過半数が使用可能でなければならないという、マスター選出アルゴリズムの要件によるものです。クラスタ内で使用可能な XMPP サーバ マスターがなければ、Cisco ミーティング アプリケーション ユーザはログインできません。XMPP サーバのそれぞれは、XMPP サーバ間に確立されたリンクによって、互いの場所を把握します。サーバはキープアライブ メッセージを使用して互いをモニタし、マスターを選出します。XMPP メッセージは任意のサーバに送信できます。どのサーバに送信したとしても、マスター XMPP サーバに転送されるためです。マスターで障害が発生した場合、新しいマスターが選出されて、他の XMPP サーバはその新しいマスターにメッセージを転送します。コール ブリッジでは、DNS SRV レコード（_xmpp-component）で設定された優先度と重みに基づいて、使用可能な XMPP サーバに接続します。コール ブリッジが接続する XMPP サーバは一度に 1 つであるため、ネットワークの問題によってコール ブリッジが XMPP サーバに接続できなくなると、コール ブリッジは別の XMPP サーバへの接続を試みます。したがって、各 XMPP サーバ内にすべてのコール ブリッジを設定する必要があります。

図 11-12 には、ハイ アベイラビリティ対応 Cisco Meeting Server クラスタの最小構成が示されています。この構成では、データベースと XMPP サーバそれぞれの 3 つのインスタンスをホストするために、少なくとも 3 台のサーバが必要です。個々のサーバで、各コンポーネント サービス（Web ブリッジとコール ブリッジ）の 2 つ以上のインスタンスを有効にして、コール ブリッジをグループに含めてください。各サーバ内のすべてのサービスを有効にする必要はありません。必要なものだけを有効にします。導入環境に必要なキャパシティが 2 つのコール ブリッジで処理可能なキャパシティを超える場合、3 つ目のサーバに追加のコール ブリッジを設定することで対処できます（コール ブリッジのためだけに 4 台目のサーバを購入する必要はありません）。

Cisco TMS のハイ アベイラビリティ

大規模な Cisco TMS 導入環境でハイ アベイラビリティを実現するには、2 台の TMS フロントエンド サーバ、TMSXE を実行する 2 台のサーバ、1 つのネットワーク ロード バランサ、1 つの Microsoft SQL データベースが必要です（図 11-3 を参照）。TMS の復元力でサポートできるのは 2 台のサーバ（1 つのアクティブ ノードと 1 つのパッシブ ノード）に限られるため、このモデルでは TMS 導入環境のキャパシティが増減することはありません。ネットワーク ロード バランサー（NLB）は、TMS サーバの前面に導入します。TMS への着信トラフィックは NLB を経由し、NLB によってアクティブ ノードに転送されます。TMS からの発信トラフィックは、NLB を経由せずに直接宛先に送信されます。NLB は既存のアクティブ ノードで障害を検出すると、ユーザによる介入なしで、自動的に新しいアクティブ ノードに切り替えます。

Cisco Meeting Management のハイ アベイラビリティ

Cisco Meeting Management には、復元力を提供するクラスタ機能が組み込まれていません。ただし、ハイ アベイラビリティを必要とするお客様は、同じ Cisco Meeting Server インスタンスを管理する、まったく同じ設定の 2 つの別個の Cisco Meeting Management インスタンスを構成し、この 2 つの Cisco Meeting Management インスタンスの前面にネットワーク ロード バランサを配置するという方法を取ることができます。この場合、ユーザはロード バランサを介して Cisco Meeting Management ポータルに接続できます。Cisco Meeting Management サーバのロード バランサの設定と可用性は、どの Cisco Meeting Management サーバを使用するかを決めます。

会議ソリューションの拡張

標準的な Cisco Meeting Server クラスタにコール ブリッジ（最大 8 つ）を追加することで、会議ソリューションを拡張できます。

この導入環境では、Unified CM 内の SIP トランクでのダイヤル プランとルート グループおよびルート リストの設定に応じて、クラスタ内の任意のコール ブリッジにコールをルーティングできます。同じ会議の複数のコールが異なるコール ブリッジにルーティングされる場合、最後の 4 つの通話中のスピーカーの音声とビデオがそれらのコール ブリッジ間で交換されるため、あるブリッジ上の参加者は他のブリッジ上の通話中のスピーカーを認識できます。

（注）　Cisco Meeting Server では 8 つを超えるコール ブリッジを使用したクラスタ化をサポートしますが、このような導入にはシスコによる事前の承認が必要です。詳細については担当のシスコ アカウント チームにお問い合わせください。

各コール ブリッジでは 450 人の参加者をサポートできます。したがって、単一のサーバを使用する場合は、会議ごとの最大参加者数は 450 人となります。単一のクラスタ内に含まれる複数のサーバを使用する場合は最大 2,600 人の参加者をサポートできます。拡張性についての詳細は、以下のリンク先から入手できる最新のバージョンの『*Cisco Meeting Server and Cisco Meeting App Data Sheet*』を参照してください。

https://www.cisco.com/c/en/us/products/conferencing/meeting-server/datasheet-listing.html

Cisco Meeting Server クラスタはコール ブリッジ グループを使用して、同じ場所にあるコール ブリッジ間または異なる場所にあるノード間でインテリジェントにコールをロード バランシングし、1 つの導入環境内で拡張を行えます。コールの転送先を決定するためのインテリジェントな判断は、Cisco Meeting Server によって行われます。コール制御システムがコールを適切な場所に移動するためには、Cisco Meeting Server からの SIP メッセージを処理できなければなりません。クラスタとして構成されているコール ブリッジは、1 つ以上のコール ブリッジ グループに含めることができます。グループに含まれるコール ブリッジについては、Cisco Meeting Server はそれらのコール ブリッジの間でコールをインテリジェントにロード バランシングし、コール ブリッジ間の分散リンクの作成を最小限に抑えるために、同じ会議のコールを可能な限り同じコール ブリッジに送信します。

コール ブリッジへの着信 SIP コールの場合、そのコール ブリッジの現在の負荷に応じて、Cisco Meeting Server はコールを拒否するか受け入れるか判断します。現在の負荷が事前設定されたしきい値を下回っていれば、コールは受け入れられます。そうでない場合、コールは拒否され、Unified CM により、ダイヤル プランの設定に従ってコールがコール グループ内の別のコール ブリッジに再ルーティングされます。Unified CM がコールを受け入れるコール ブリッジを見つけられなければ、コール全体が拒否されます。Cisco Meeting Server で受け入れられたコールは、その Cisco Meeting Server のコール ブリッジでホストされる場合もあれば、会議の内部順序付けリストに従って、最大の優先度が設定された別のコール ブリッジに移動される場合もあります。コールが移動されると、コール ブリッジが有効にされたターゲット Cisco Meeting Server は、コールを引き継ぐために、Replaces を設定した INVITE を Unified CM に送信します。デフォルトでは、コール ブリッジ グループに含まれるコール ブリッジは、負荷が 80 % になった時点で新しい参加者のすべてのコールを拒否し、新しい分散コールのみを許可するようになります。

アウトバウンド SIP コールについては、Cisco Meeting Server はアウトバウンド ダイヤル ルールを使用して、ドメインと一致する最大優先度のルールを特定し、コール ブリッジ グループを使用してコールのロード バランシングを行います。ルールがローカル コール ブリッジに適用される場合、コールのロード バランシングはローカル コール ブリッジ グループを使用して行われます。適用されない場合は、リモート コール ブリッジがメンバーとなっているコール ブリッジ グループを使用してコールのロード バランシングが行われます。また、API を使用して発信されるコールについては、コール ブリッジ グループまたはコール ブリッジをパラメータとして指定できます。コール ブリッジ グループの場合は、そのグループに含まれるコール ブリッジの間でコールのロード バランシングが行われます。コール ブリッジの場合は、そのコール ブリッジを使用してコールが実行されます。

Cisco ミーティング アプリケーション（WebRTC を含む）クライアントの場合、ユーザはスペースのメンバーとして、またはスペースの非メンバーとして（Cisco Meeting Server 上にアカウントがある場合）、あるいはゲストとして会議に参加できます。API を使用してユーザをメンバーとしてスペースに追加する際は、コール ブリッジ グループまたはコール ブリッジをパラメータとして指定できます。コール ブリッジ グループの場合、Cisco ミーティング アプリケーション ユーザが会議に参加すると、そのグループを使用してコールのロード バランシングが行われます。コール ブリッジの場合、Cisco ミーティング アプリケーション ユーザが会議に参加すると、そのコール ブリッジによってコールが処理されます。ユーザがスペースのメンバーではない場合、あるいは Cisco ミーティング アプリケーションを使用してゲストとして会議に参加する際は、そのユーザが最初に接続するコール ブリッジが判断されます。そのコール ブリッジがコール ブリッジ グループに属している場合は、そのグループを使用してコールのロード バランシングが行われます。Cisco ミーティング アプリケーション コールのロード バランシングを行うためには、コール ブリッジ グループに含まれるコール ブリッジのそれぞれが、XMPP クラスタまたは単一の XMPP サーバに接続できるようにしてください。

コール ブリッジ グループに含まれるコール ブリッジ間で正常にコールを移動するには、満たさなければならないネットワーク要件がいくつかあります。グループに含まれるコール ブリッジ間の最大 RTT は 100 ミリ秒、クラスタ内の 2 つコール ブリッジ間の最大 RTT は 300 ミリ秒でなければなりません。

コール ブリッジ グループの設定と導入について詳しくは、以下のリンク先から入手できる最新バージョンのホワイト ペーパー『*Load Balancing Calls Across Cisco Meeting Servers*』を参照してください。

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

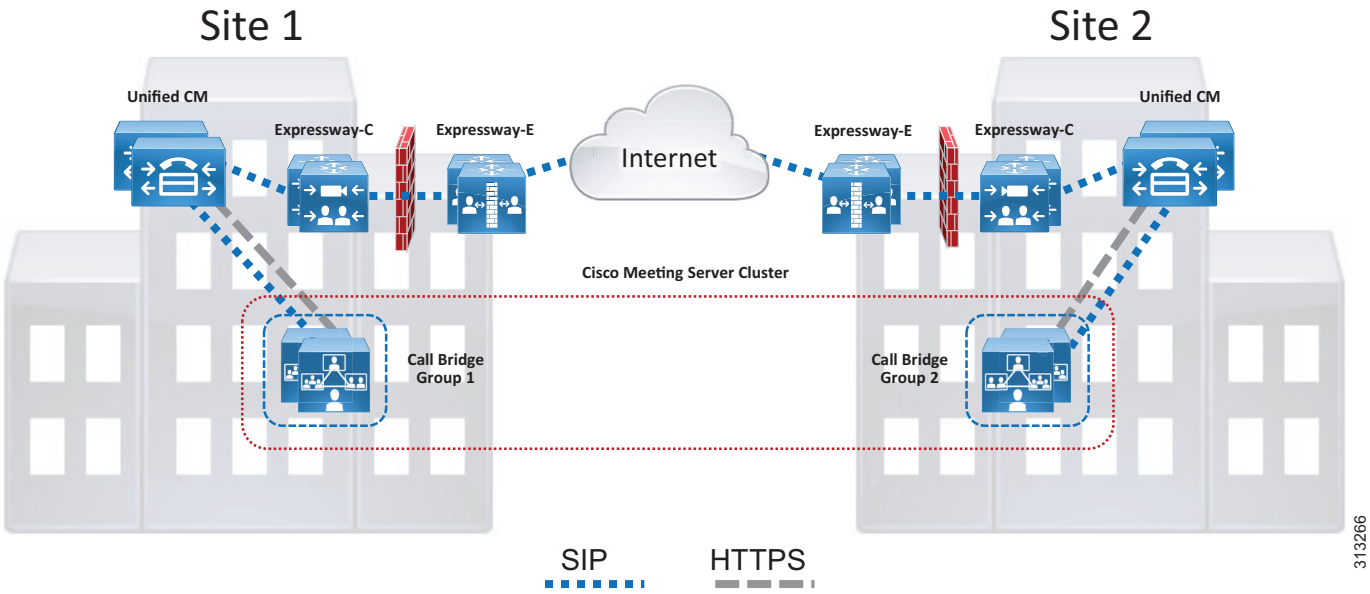
（注）　コール ブリッジ グループとロード バランシングが使用されていなければ、コールが拒否されることはありませんが、負荷の上限に達すると、すべてのコールの品質が低下します。品質低下が頻繁に発生する場合は、追加のハードウェアを導入することをお勧めします。

複数の Unified CM クラスタに関する考慮事項

複数の Cisco Unified CM クラスタを使用する大規模な導入環境では、単一の Cisco Meeting Server クラスタに複数のコール ブリッジ グループを設定し、それぞれのグループを各 Unified CM クラスタ専用にしてください。

たとえば、導入環境に 3 つの Unified CM クラスタがある場合、3 つのコール ブリッジ グループ（Unified CM クラスタごとに 1 つ）を設定した単一の Cisco Meeting Server クラスタを導入します。Unified CM クラスタごとに、そのローカル コール ブリッジ グループ内の各コール ブリッジに接続する SIP トランクが必要です。Unified CM クラスタへのすべて着信会議コールは、ローカル コール ブリッジ グループによって処理されます。コール ブリッジの分散リンクは、グループ内外にあるそれぞれのピアにフル メッシュ トで接続されている必要があります。同じ会議に複数のユーザが Unified CM クラスタからダイヤルインしてそのローカル コール ブリッジ グループに到達した場合、他のコール ブリッジ グループに含まれるコール ブリッジにより最後の 4 つの通話中のスピーカーの音声とビデオがピアと交換されるため、参加者はこれらのブリッジを介して互いを認識することができます。（図 11-13 を参照）。

図 11-13　複数の Unified CM クラスタを使用した Cisco Meeting Server 導入環境



複数の地域に Cisco Meeting Server クラスタを拡張して複数の Unified CM クラスタに対応する場合は、以下のガイドラインが適用されます。

- 1 つ以上の Cisco Unified CM クラスタの導入環境に対して、単一の Cisco Meeting Server クラスタを使用する必要があります。
- 標準的な Cisco Meeting Server クラスタには、最大 8 つのコール ブリッジを導入できます。クラスタのコール ブリッジが 8 つを超える場合は、導入前にシスコ アカウント チームの承認が必要です。
- 最大 5 つのデータベースと奇数のノードを Cisco Meeting Server クラスタに導入します。
- 奇数の XMPP サービス ノードを Cisco Meeting Server クラスタに導入します。
- ラウンドトリップ時間（RTT）に関するネットワーク要件：
  - Cisco Meeting Server クラスタ内のコール ブリッジ間では最大 300 ミリ秒、データベース間では最大 200 ミリ秒
  - グループ内のコール ブリッジ間では最大 100 ミリ秒

ライセンシング

Cisco Meeting Server は、マルチパーティ ランセンスと Cisco Meeting Server キャパシティ ユニットの両方をサポートしていますが、マルチパーティ ランセンスを使用することを推奨されています。マルチマーティ ライセンスはユーザベースのランセンス モデルであり、コール ブリッジが有効にされたすべてのノードに適用する必要があります。このライセンスには、Personal と Shared の 2 つのバージョンがあります。Personal Multiparty Plus（PMP+）は特定のネームド ホスト用であり、Shared Multiparty Plus（SMP+）は会議室システム用またはユーザ間で共有されるものです。デフォルトでは、システム内のすべてのユーザが Shared Multiparty Plus（SMP+）を使用します。Personal Multiparty Plus（PMP+）が必要な場合は、Cisco Meeting Server API を使用して PMP+ をユーザに割り当ててください。各ライセンスでは、ユーザは、参加者数無制限、ビデオの最大解像度 1080p の会議をホストできます。表 11-4 で、Personal Multiparty および Shared Multiparty の各ライセンスに含まれる機能を要約します。

表 11-4　シスコの Personal Multiparty Plus ライセンスと Shared Multiparty Plus ライセンスの機能

機能	Personal Multiparty Plus（PMP+）	Shared Multiparty Plus（SMP+）
ネームド ホストとの関連付け	○	X
アベイラビリティ	Cisco UWL Meeting に付属	個別に購入するか、またはルーム システムと共に割引価格で購入
最小発注数	25	1
会議の最大参加者数	無制限（利用可能なハードウェア キャパシティの制限内）	
最大解像度	シングルスクリーンまたはマルチスクリーン エンドポイントで、ビデオに対しては 1080p60（フル HD）、コンテンツに対しては 1080p30	
Business-to-Business（B2B）または Business-to-Customer（B2C）のリッチ メディア セッション	同梱	同梱
Cisco TMS、TMS、TMSXE、および Skype for Business/Lync 相互運用ライセンス	含む	新規顧客は Starter Pack を購入[1]
インスタント会議、パーマネント会議、スケジュール済み会議のサポート	○	○

1. Cisco TMS および関連する製品ライセンスのみが必要な場合は、TMS Starter Pack を購入していただけます。

ライセンスの詳細については、以下のリンク先から入手できる製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/conferencing/meeting-server/index.html?dtid=osscdc000283

Cisco Meeting Management では、Cisco Meeting Server のお客様用の追加ライセンスは不要です。https://www.cisco.com から Cisco Meeting Management をダウンロードできます。

キャパシティ プランニング

Cisco Meeting Server のキャパシティは、選択したプラットフォームや導入環境内で実行する会議ノードの数によって異なります。導入のサイジングの主な目的は、必要な Cisco Meeting Server への同時接続数を決定することです。次のような検討事項があります。

- 地理的なロケーション：Cisco Unified CM のサービスを提供する地域ごとに、会議専用のリソースを確保する必要があります。たとえば米国と EMEA それぞれの中央ロケーションに、Unified CM、Cisco Meeting Server、およびその他のサーバを設置するという方法が考えられます。
- Cisco Meeting Server プラットフォームの選択：仮想化またはアプライアンス
- Cisco Meeting Server プラットフォームのキャパシティ：キャパシティの詳細については、https://www.cisco.com/c/en/us/products/conferencing/meeting-server/datasheet-listing.html から入手できる Cisco Meeting Server のデータ シートを参照してください。
- 会議のタイプ：音声またはビデオ（あるいはその両方）。スケジュール済み会議またはスケジュールされない会議（あるいはその両方）
- 会議のビデオ解像度：高品質の会議ほど多くのリソースを消費します。
- 大規模な会議の要件：オールハンズ ミーティングなど

地域ネットワークの会議メディアをできるだけ多く確保するために、会議リソースは一般に 1 つの地域専用となります。したがって、サイジングは地域単位で検討することができます。会議の導入環境を適切にサイジングするには、Cisco Collaboration Sizing Tool を使用してください。このツールは、有効なログイン アカウントがあれば https://cucst.cloudapps.cisco.com から入手できます。

(注)　特定の環境での会議リソースのサイジングにあたっては、代理店にご相談ください。

サイジングの詳細については、コラボレーティブ会議（25-47 ページ）を参照してください。

Cisco Meeting Server プラットフォームのタイプと、Cisco Meeting Management で管理する Cisco Meeting Server クラスタの数によって、必要となる導入サイズは異なります。詳細については、以下のリンク先から入手できる最新の Cisco Meeting Management リリース ノートを参照してください。

https://www.cisco.com/c/en/us/support/conferencing/meeting-management/products-release-notes-list.html

設計上の考慮事項

要約すると、Cisco Meeting Server を導入する際は、以下の推奨事項を考慮する必要があります。

- Cisco Meeting Server の導入環境には、マルチパーティ ランセンス（PMP+/SMP+）を使用してください。
- Cisco Meeting Server の導入環境では、内部接続と外部接続の両方をセキュリティ保護するために証明書が必要です。証明書には、CA 署名付き証明書を使用してください。
- Cisco Meeting Server クラスタは、コール ブリッジを使用して最大 8 つのノードをサポートします。8 つを超えるノード（最大 24）を導入することも可能ですが、それには導入前にシスコの承認が必要になります。

- 導入環境でデータベースまたは XMPP サービスをクラスタ化する場合、クラスタのマスター選出アルゴリズムの要件により、少なくとも 3 つのデータベースまたは XMPP ノードが必要になります。
- 大規模な分散型 Cisco Meeting Server 導入環境では、コール ブリッジ グループを使用して地域内のコール ブリッジをグループ化し、コール ブリッジ間での分散リンクの作成を最小限に抑えてください。
- Cisco Meeting Server クラスタ導入環境でのネットワーク要件は、コール ブリッジ間では 300 ミリ秒、データベース間では 200 ミリ秒、コール ブリッジ グループに含まれるコール ブリッジ間では 100 ミリ秒です。
- Cisco TelePresence Management Suite（TMS）は会議のスケジューリングとエンドポイントの管理を提供し、Cisco Meeting Management は会議の管理を提供します。この 2 つのアプリケーションによって、Cisco Meeting Server の完全な管理ソリューションが実現します。
- Cisco Meeting Management は追加ライセンスなしで導入できますが、Cisco Meeting Server とは別のサーバが必要となります。

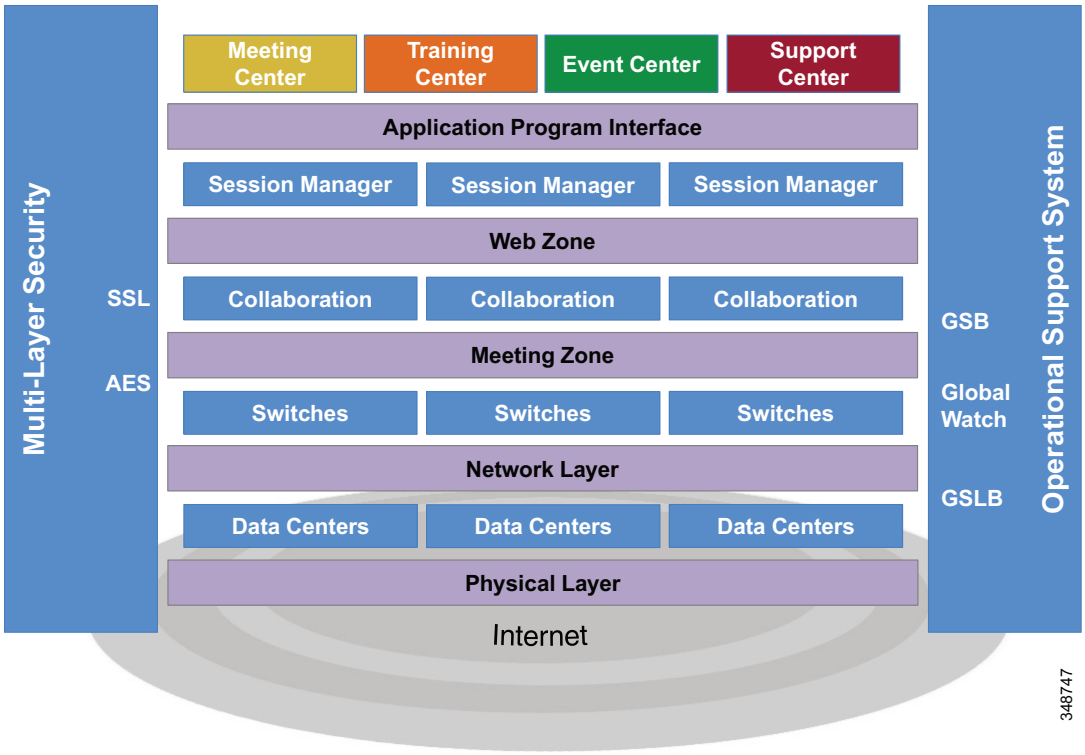
Cisco WebEx Software as a Service

Cisco WebEx は、ハードウェアをオンサイトに配置する必要がないコラボレーション会議ソリューションです。すべてのサービス（音声、ビデオ、およびコンテンツ共有）は、Cisco WebEx Collaboration Cloud を介してインターネットでホストされます。これは、多くの場合、Software-as-a-Service（SaaS）と呼ばれます。インターネットに接続できる環境であれば、会議の開始と会議への参加は、いつでもどこでも、どのデバイスからでも行うことができます。企業に接続する必要はありません。ここでは、ソリューションの特性について説明し、WebEx SaaS の配置の設計ガイドラインを示します。

アーキテクチャ

Cisco WebEx SaaS は、Cisco WebEx Collaboration Cloud を使用して顧客に会議ソリューションを提供します。Cisco WebEx Collaboration Cloud は、キャリアクラス情報スイッチング アーキテクチャで作成されたグローバル ネットワークであり、このネットワーク上ではシスコ コラボレーション トラフィックのみが流れます。図 11-14 は、Cisco WebEx Collaboration Cloud のアーキテクチャを示しています。

図 11-14　Cisco WebEx Collaboration Cloud のアーキテクチャ



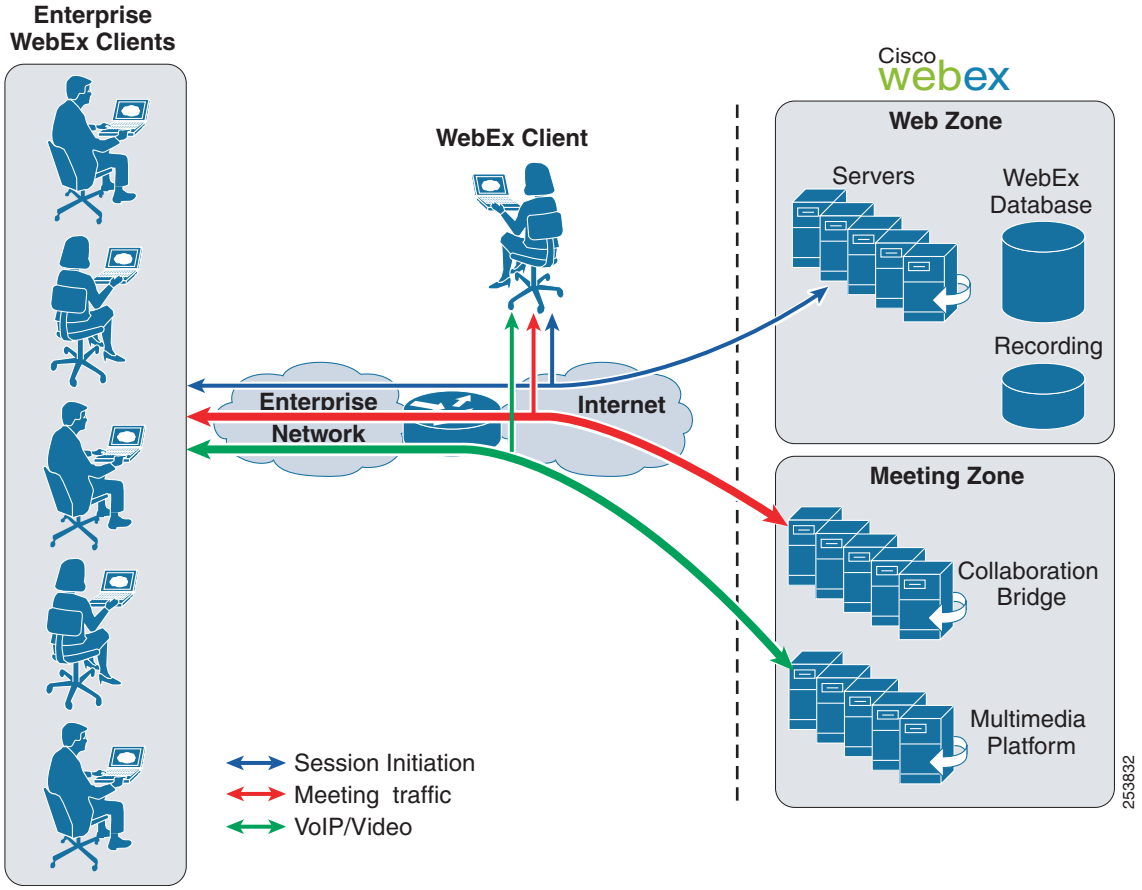
このネットワークは、リアルタイム通信専用に作成されており、TCP レイヤのフローに関連する遅延を最小化するように特別に構成されています。ネットワークは、主要なピアリング ポイントにおいてアプリケーション固有のマルチメディア スイッチで構成されており、WebEx 会議に関して高速のセッション トラフィックを処理し、また高品質のサービスを保証します。これらのスイッチは、公衆インターネットを避けて専用線で相互接続された安全性の高いシスコ データセンターに格納されています。これらのデータセンターは、主要なインターネット アクセス ポイントの近くに配置されており、会議トラフィックを世界中に安全かつ確実にルーティングします。主要な会議ノードを格納するこれらの大規模なデータセンターに加えて、シスコは、世界中にノードを展開しています。ネットワークは、グローバル サイト バックアップを備えた完全冗長クラスタ上に構築されます。これらのサービスおよびその他の機能は、Cisco WebEx Collaboration Cloud 運用サポート システムの一部を形成します。

ユーザが WebEx ミーティングに接続するには、コンピュータやモバイル デバイス上で稼働する会議アプリケーションを使用することも、さらには HTML5 ブラウザベースの Web アプリケーションを使用することもできます。接続が確立されると、図 11-14 に示すように、WebEx Collaboration Cloud は、WebEx 会議を構成するすべての同期リアルタイム対話を管理します。ユーザは、Web ゾーン内に存在する WebEx Collaboration Cloud を使用して、ブラウザで WebEx アプリケーションにアクセスします。アプリケーション プログラミング インターフェイス（API）により、WebEx Collaboration Cloud コア内の会議ゾーンで WebEx アプリケーションをスイッチング プラットフォームに関連付けます。相互接続および分散型コラボレーション スイッチの多数のクラスタ、関連付けられたデータベース、および論理的および物理的なネットワーク インフラストラクチャにより、WebEx Collaboration Cloud コアが構成されます。多層セキュリティ コンポーネントと WebEx 運用サポート システムでネットワークを囲むことにより、保護が強化されます。

WebEx Collaboration Cloud は、インテリジェントなルーティング、グローバル サイト バックアップ（GSB）、およびグローバル サーバ ロードバランシング（GSLB）を使用してリアルタイム トラフィックを確実に提供します。WebEx 会議出席者の地理的な位置に基づいて、WebEx Collaboration Cloud は、最小の遅延と最高のパフォーマンスを提供するポイントオブプレゼンスを決定します。WebEx 会議ホストは、同じ領域内の地理的に離れたシスコ データセンターに物理的に配置されるバックアップ サイトを自動的に取得します。ほとんどないことですが、プライマリ WebEx サイトが使用不可になること、GSB は、すべての会議アクティビティを自動的にバックアップ サイトに切り替えます。GSLB はロードバランシング設計であり、遅延が最小になるように、WebEx Collaboration Cloud 内の最も輻輳が低いスイッチにトラフィックを振り向けます。したがって、1 台の会議スイッチで輻輳が発生すると、トラフィックは代替スイッチに振り向けられて、参加者の間で迅速な画面の更新と同期が実現され、より効果的な会議環境となります。

図 11-15 に示す WebEx 配置モデルでは、すべてのクライアントからのすべてのコンテンツ、音声、およびビデオ トラフィックは、インターネットを通過し、クラウド内で WebEx データセンターでミキシングおよび管理されます。WebEx データセンターは、論理的には、会議ゾーンと Web ゾーンに分割されます。Web ゾーンは、Web 会議の前後に発生することを処理します。スケジューリング、ユーザ管理、課金、レポート、ストリーミング レコーディングなどのタスクが組み込まれています。会議ゾーンは、実際の会議がエンドポイント間で進行中になると、その切り替えを処理します。

図 11-15　WebEx の導入



会議ゾーンは 2 つのサブシステムで構成されます。会議ゾーンには、会議コンテンツを切り替えるコラボレーション ブリッジがあります。マルチメディア プラットフォームは、会議内の VoIP ストリームおよびビデオ ストリームすべてのミキシングを処理します。WebEx セッションに参加するには、参加者は最初に Web ゾーンに接続する必要があります。Web ゾーンのトラフィックは、会議の前後にだけ流れ、比較的低い帯域幅であり、主にリアルタイムではありません。リアルタイムの会議コンテンツ共有は、会議ゾーンへ、または会議ゾーンから流れ、帯域幅に大きな影響を与える可能性があります。そのリアルタイムという性質から、企業のアクセス インフラストラクチャに大きな負荷がかかる場合があります。ネットワーク トラフィック プランニングの詳細については、キャパシティ プランニング（11-36 ページ）を参照してください。

Meeting Center では H.264 AVC/SVC コーデックが使用され、高画質ビデオを会議で使用できます。このような環境を展開するには、より広いネットワーク帯域幅が必要です。高画質ビデオのネットワーク トラフィック最適化の詳細については、キャパシティ プランニング（11-36 ページ）を参照してください。

各 WebEx Meeting Center ホストには、カスタマイズ可能な固定 URL を持つパーソナル ルームがあります。ホストは、自身のルームを使用して会議を主催し、参加者はその固定 URL を使用してルームに入出します。ホストは、ルームをロックして会議の進行中に他者が入らないようにしてプライバシーを維持するなどのロビー管理機能を使用できます。

Cisco WebEx Meeting Center バージョン WBS32.4 以降、Meeting Center で雑音検出機能をサポートするようになっています。この機能では、会議で発言中のユーザの声と背景雑音を区別することができます。[コンピュータを使用して通話（Call Using Computer）] オプションを使用して音声が接続されている場合、アクティブな背景雑音（ノック、タイプ、サイレン、犬の吠え声など）が検出されると、Meeting Center は自動的にユーザに警告を出して、ミュートにするよう求めることができます。ただし、ユーザは必要に応じて雑音検出機能を無効にすることもできます。

（注）　雑音検出機能では、[コンピュータを使用して通話（Call Using Computer）] 音声オプションのみをサポートしています。

セキュリティ

デフォルトでは、すべての WebEx 会議データは、128 ビット SSL 暗号化を使用してクライアントとシスコの Collaboration Cloud の間で暗号化されます。クラウド内の SSL アクセラレータによって、コンテンツ共有情報は復号化され、コンテンツを処理して SSL アクセラレータを介して返信する WebEx カンファレンス ブリッジに送信されます。情報は SSL アクセラレータで再度暗号化されてから、参加者に返信されます。Web ゾーンと会議ゾーンのトラフィックはすべて、128 ビット SSL を使用して暗号化されます。SSL 機能を Web ゾーンと会議ゾーンのサーバからオフロードするために、SSL アクセラレータが使用されます。

会議の終了後は、WebEx クラウドまたは参加者のコンピュータにセッション データは保持されません。2 種類のデータだけが長期的に保持されます。これらのデータは、課金とレポート情報、およびオプションのネットワーク ベースのレコーディングであり、どちらも許可された企業ユーザだけがアクセスできます。

会議データの一部の制限されたキャッシュが、会議ゾーンで実行されます。これは、接続に問題のあるユーザまたは開始されたあとで会議に参加するユーザが、最新の完全に同期がとれたバージョンの会議コンテンツを受信できるようにするために実行されます。

文書化されたセキュリティのベスト プラクティスに WebEx クラウドが準拠していることを保証するために、独立した第三者によって、商業的および政治的なセキュリティ要件を対象とした外部監査が実行されます。WebEx では、AICPA によって確立された標準に従って、SSAE Type 16 監査を年次で Price Waterhouse Coopers によって実行しています。WebEx に対して監査される制御は、ISO-27002 の標準に基づきます。この重視および認知されている監査によって、顧客データの処理に関して、WebEx サービスが制御の目的および制御のアクティビティ（情報技術およびセキュリティ関連プロセスの制御を含む場合もあります）に対して詳細に監査されていることが検証されます。

セキュリティの強化を必要とするお客様の場合、クラウド内でトラフィックが復号化されないように、コラボレーション ブリッジおよびマルチメディア コンテンツに対してエンドツーエンド 256 ビット AES 暗号化を実行するオプションもあります。エンドツーエンド暗号化の結果、NBR などの一部の機能は失われます。拡張 WebEx セキュリティ オプションの詳細については、次の Web サイトで入手可能なホワイト ペーパー『*Unleash the Power of Highly Secure, Real-Time Collaboration*』を参照してください。

https://www.cisco.com/en/US/products/ps12584/prod_white_papers_list.html

（注）　エンドツーエンドの暗号化オプションは、追加コストなしで Meeting Center および Support Center の会議で使用できます。

サイト管理者は、ネットワークベースの録音へのアクセスに対し、パスワードの使用を強制することができます。開催者は会議をスケジュールする際に、会議の参加者全員にシングル サインオン（SSO）認証によるサインインを必須事項としたり、招待した参加者だけに会議を制限したりすることができます。さらに、サイト管理者は開催者がロック解除したパーソナル ルームへの入室を、認証済み参加者だけに許可するオプションを有効にすることもできます。この場合、認証されていない参加者は、開催者が入室を許可するまではロビーで待たなければなりません。

スケジューリング

会議のスケジューリングと開始に関して、WebEx にはクラウドベースの Web スケジューリング機能がありますが、ほとんどの組織は企業電子メール システム（Exchange、Lotus Notes など）またはその他の企業アプリケーションからスケジューリングします。WebEx Productivity Tools は、単一のアプリケーションに組み込まれた既知のデスクトップ ツールとの統合のバンドルです。WebEx 管理者は、組織のユーザにツールを介して提供される特定の統合を制御できます。WebEx サイトからダウンロードしてインストールすることも、標準的なデスクトップ管理ツールを使用してローカルでプッシュすることもできます。WebEx Productivity Tools の詳細については、次の Web サイトを参照してください。

https://www.webex.com/support/productivity-tools.html

ユーザ プロファイル

クラウド内に組織の WebEx ユーザ プロファイルを作成するためのオプションがいくつかあります。実際のユーザ名とパスワード、および大量のユーザ アカウントの処理について、セキュリティ上の考慮事項を検討する必要があります。WebEx 管理者は、CSV テンプレートのバルク インポートによって手動で、またはプログラムによるアプローチによって、ユーザ プロファイルを作成できます。プログラムによるアプローチでは、WebEx API、URL、および XML のいずれかまたは組み合わせ、あるいはフェデレーション SSO ソリューションが使用されます。プログラムによるアプローチはカスタマー ポータルで使用できます。カスタマー ポータルは、WebEx に直接統合される CRM ツールや Learning Management System などのアプリケーションです。また、ユーザは、会社の WebEx サイトからアカウントにサインアップできます。要求の承認後に、ユーザ プロファイルが作成されます。

組織の LDAP ディレクトリとの直接統合の場合、Security Assertion Markup Language（SAML）を使用したフェデレーション SSO が望ましいアプローチです。フェデレーション SSO の詳細情報については、次の URL にあるホワイト ペーパーおよびテクニカル ノートを参照してください。

https://developer.cisco.com/site/webex-developer/develop-test/sso/reference/

ハイ アベイラビリティ

Cisco WebEx Collaboration Cloud には、非常に高レベルの冗長性が組み込まれており、シスコによって管理されています。これは、停止時に冗長な会議ノードに対して非常に堅牢なカットオーバーを行うことによりサービスを継続するように設計されています。すべてのお客様に対して、プライマリ WebEx サイトに加えて、同じ領域内の地理的に離れた WebEx データセンターに物理的に配置されたバックアップ サイトが準備されています。お客様のプライマリ サイトが使用できない場合、グローバル サイト バックアップ（GSB）は、すべての会議アクティビティを自動的にバックアップ サイトに移動します。ホストと参加者は、どちらもバックアップ サイトにリダイレクトされたことに気付きません。GSB システムは、WebEx 会議に対する継続的なアクセシビリティをグローバルに実現し、すべての属性、アドレス帳、プリファレンス、会議スケジュール、およびその他のリアルタイム データを、プライマリ サイトとバックアップ サイト間で同期して保持します。この同期により、GSB は、会議の前後で冗長性とディザスタ リカバリを提供します。

Cisco WebEx Cloud Connected Audio

Cisco WebEx Cloud Connected Audio（CCA）は、オンプレミス IP テレフォニー ネットワークを使用するハイブリッド導入モデルに基づく音声会議ソリューションであり、組織の WebEx 会議に統合化された音声エクスペリエンスを提供します。WebEx CCA は、組織の IP テレフォニー ネットワークから WebEx クラウド インフラストラクチャへの SIP トランク接続を実装します（図 11-16 を参照）。音声会議トラフィックは、サービス プロバイダー PSTN 接続の代わりにこの SIP 接続を通過します。したがって、WebEx CCA により、オーディオ コストが大幅に節約され、また他の WebEx オーディオ オプションと同様の統合化された直感的なユーザ エクスペリエンスを維持できます。

図 11-16　Cisco WebEx Cloud Connected Audio の概要設計

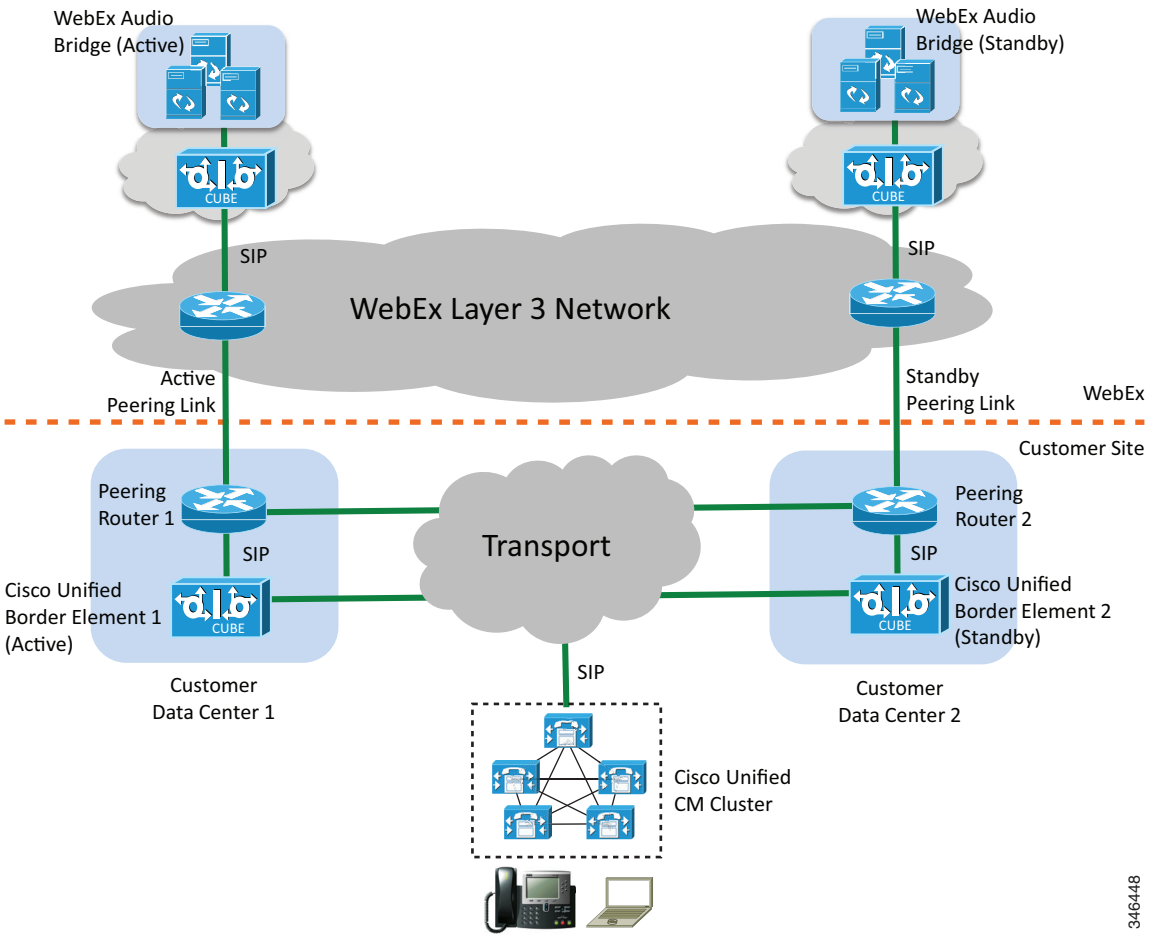


図 11-16 に示すように、一般的な WebEx CCA 概要設計は、お客様が提供する専用 IP ピアリング接続を介して接続されるオンプレミス IP テレフォニー ネットワークと WebEx クラウド インフラストラクチャで構成されます。オンプレミス IP テレフォニー ネットワークは、Cisco Unified Communications Manager（Cisco Unified CM）クラスタおよび Cisco Unified Border Element で構成されます。Cisco Unified Border Element は、WebEx クラウド インフラストラクチャに導入され、組織の IP テレフォニー ネットワークのエントリ ポイントを示します。クラウド内および顧客サイトの Cisco Unified Border Element は、SIP 経由で互いに通信します。WebEx CCA では、冗長性を目的として、地理的に離れた場所に存在する別々の WebEx データセンターに接続する 2 つの IP ピアリング接続が必要です。冗長 IP リンクは、アクティブ/スタンバイ モードで設定されます。すべての会議のオーディオ トラフィックがプライマリ リンクを経由して流れ、またプライマリ リンクがダウンした場合には、セカンダリ リンクにフェールオーバーします。また、WebEx CCA では、ゲートウェイ ルータが Border Gateway Protocol（BGP）と Bidirectional Forwarding Detection（BFD）プロトコルもサポートする必要があります。BGP と BFD により、ネットワーク障害が発生した場合の再コンバージェンス時間が大幅に速くなります。

（注）　WebEx データセンター機器、オーディオ ブリッジおよびサーバは、WebEx CCA ソリューションの他のカスタマーとともに共有インフラストラクチャ上で実行されます。

Cisco Unified CM は、顧客サイトの Cisco Unified Border Element を介して WebEx クラウドと SIP 接続され、テレフォニー信号を処理します。会議のダイヤルイン番号は顧客が所有し、顧客サイトを終端とします。コール ルーティングは顧客サイトで処理され、コール シグナリングとオーディオ トラフィックは冗長 IP ピアリング接続で処理され、コール ミキシングはクラウドで処理されます。ユーザが企業内の会議番号にダイヤルすると、Cisco Unified CM は、PSTN を経由することなく、Cisco Unified Border Element を通して専用 SIP トランク経由で WebEx クラウドにコールをルーティングします。会議ユーザがコールバックを要求すると、WebEx は、そのコールを顧客サイトの Cisco Unified Border Element に送信し、そこから宛先エンドポイントにルーティングされます。会議ユーザが企業ネットワークの外部にいる場合、コールは顧客の IP テレフォニー ネットワークの終端の前または出た後に、PSTN 経由でルーティングされます。WebEx CCA は、G.711 オーディオ コーデック、RFC 2833 DTMF、および SIP シグナリングのみをサポートします。

WebEx CCA は、継続的にサービスを運用できるように設計された、可用性が高い完全冗長アーキテクチャを持っています。すべての主要コンポーネントには、相互にバックアップするアクティブ モードとスタンバイ モードの 2 つのインスタンスがあります。2 つの独立したルータのペア、2 つの Cisco Unified Border Element のペア、および 2 つの音声カンファレンス ブリッジで処理される 2 つの IP ピアリング接続があります。これらのいずれかのコンポーネントに障害が発生すると、スタンバイ側が引き継ぎます。アクティブ ピアリング リンクに障害が発生した場合、ネットワークはスタンバイ接続を介して収束します。すべての既存のコールは継続しますが、メディア フローが非常に短時間中断します。Cisco Unified Border Element は、Out-of-Dialog OPTIONS ping メカニズムを使用して互いの動作状態をモニタします。また、顧客サイトの Cisco Unified Border Element も、Out-of-Dialog OPTIONS ping メカニズムを使用して Cisco Unified CM クラスタをモニタします。ping への応答に失敗すると、送信側のダイヤルピア リストから無応答要素が削除され、すべての新しいコールがスタンバイ インスタンスを介してルーティングされるようになります。アクティブ WebEx オーディオ ブリッジに障害が発生すると、ブリッジに関連付けられたすべてのコールが終了し、スタンバイ WebEx オーディオ ブリッジがアクティブになります。次に、WebEx は、ユーザに対して新しくアクティブになったブリッジに接続するための新しい番号を要求します。また、障害発生前にシステムから発信されたすべてのコール（コールバック）がリダイヤルされます。

Cisco WebEx Cloud Connected Audio を導入する場合には、次のガイドラインを考慮してください。

- WebEx CCA の導入で Cisco Unified CM 8.5 以降のリリースを使用することを推奨します。
- WebEx CCA の導入で専用の Cisco Unified Border Element を使用して、健全なアーキテクチャと容易なトラブルシューティングを保証することを推奨します。
- Cisco Unified Border Element は、音声ポートのキャパシティ要件に応じて、Cisco サービス統合型ルータ（ISR）またはアグリゲーション サービス ルータ（ASR）上に導入できます。
- パケット インスペクションの代わりにアクセス コントロール リスト（ACL）を使用して、IP ピアリング リンク上のファイアウォール トラフィックを制限します。
- システム管理者は、ゲスト ダイヤルイン用に少なくとも 1 つの有料通話番号と 1 つの無料通話番号を提供する必要があります。
- G.711 以外のオーディオ コーデックが望ましい場合は、トランスコーダを使用して、WebEx に送信する前に G.711 にオーディオ ストリームを変換します。
- すべての会議番号に関して、Cisco Unified Border Element を介して、少なくとも 1 つのダイヤルイン方式（DID）デジタル番号識別サービス（DNIS）を WebEx クラウドに渡す必要があります。

Cisco WebEx Cloud Connected Audio の詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

https://www.cisco.com/go/cwcca

キャパシティ プランニング

特定のお客様について、同時会議の実際の数は本質的には無制限です。WebEx 会議のタイプが異なると、参加者数に関するキャパシティも異なります。詳細な製品比較表については、次の Web サイトで入手可能な『*Cisco WebEx Web Conferencing Product Comparison*』を参照してください。

https://www.cisco.com/en/US/prod/ps10352/product_comparison.html

ネットワーク トラフィック プランニング

インターネットへのトラフィックが増加するにつれて、ネットワーク トラフィック プランニングを考慮することが重要になります。ネットワーク トラフィックを計画する場合、ユーザが WebEx を使用する方法によって、会議で生成されるトラフィック量が大きく異なります。たとえば、参加者がネイティブ プレゼンテーション共有（ドキュメントは共有の前に WebEx サイトにロードされます）を使用する場合、生成されるデータはデスクトップを共有する場合よりも大幅に少なくなります。大企業の場合、特にインターネット アクセス ポイントなどのネットワーク内の混雑するポイントで、このことを理解して正しいトラフィック エンジニアリングを確保することが重要です。最繁時にホストされる平均会議数と平均参加者数を事前に見積もる必要があります。そのあとで、これらの会議のタイプと特性に応じて、帯域幅の要件を見積もることができます。ネットワーク トラフィック プランニングの詳細については、次の Web サイトで入手可能なホワイト ペーパー『*Cisco WebEx Network Bandwidth* 』を参照してください。

https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white_paper_c11-691351.html

設計上の考慮事項

Cisco WebEx SaaS ソリューションを実装する場合は、次の設計上の考慮事項に従ってください。

- 通常、コラボレーティブ会議システムによって、正時の呼処理の負荷が大きくなります。シスコ代理店と従業員は、コラボレーティブ会議固有のパラメータが設定されたキャパシティ プランニング ツールにアクセスして、大規模構成の Cisco Unified Communications システムのキャパシティを計算できます。システムのサイジングでサポートが必要な場合は、シスコ代理店またはシスコのシステム エンジニア（SE）にお問い合わせください。シスコ パートナーと従業員は、Cisco Collaboration Sizing Tool を https://cucst.cloudapps.cisco.com/landing から入手できます。
- WebEx クライアントからのすべての接続は、クラウドに対して開始されます。通常、イントラネット デバイスがインターネットへの TCP 接続を開始することをファイアウォールが許可するかぎり、ネットワーク ファイアウォール内の開いているピンホールは必要ありません。
- 会議のビデオおよびデータのトラフィックに対して十分な帯域幅をプロビジョニングします。詳細については、ネットワーク トラフィック プランニング（11-52 ページ）を参照してください。
- ビジネス要件に基づき、以下の点について設計上の意思決定を行う必要があります。
  - ユーザの作成および認証オプション（詳細についてはユーザ プロファイル（11-32 ページ）を参照してください）
  - 会議のスケジュール オプション（詳細についてはスケジューリング（11-32 ページ）を参照してください）

- Cisco WebEx SaaS では多層セキュリティ モデルが使用され、セキュリティは WebEx インフラストラクチャから組織および個々の会議レイヤに拡張されます。さまざまなセキュリティ オプションが使用可能であり、ビジネス要件に応じて、組織は異なるレベルのセキュリティを導入できます。セキュリティ オプションと考慮事項については、次の Web サイトで入手可能なホワイト ペーパー『*Unleash the Power of Highly Secure, Real-Time Collaboration*』を参照してください。

  https://www.cisco.com/en/US/products/ps12584/prod_white_papers_list.html

- さまざまなシスコ コラボレーション クライアント製品の詳細と、それらがシスコの会議ソリューションにどのように適しているかについては、コラボレーション エンドポイント（8-1 ページ）の章を参照してください。

Cisco WebEx Meeting Center Video Conferencing

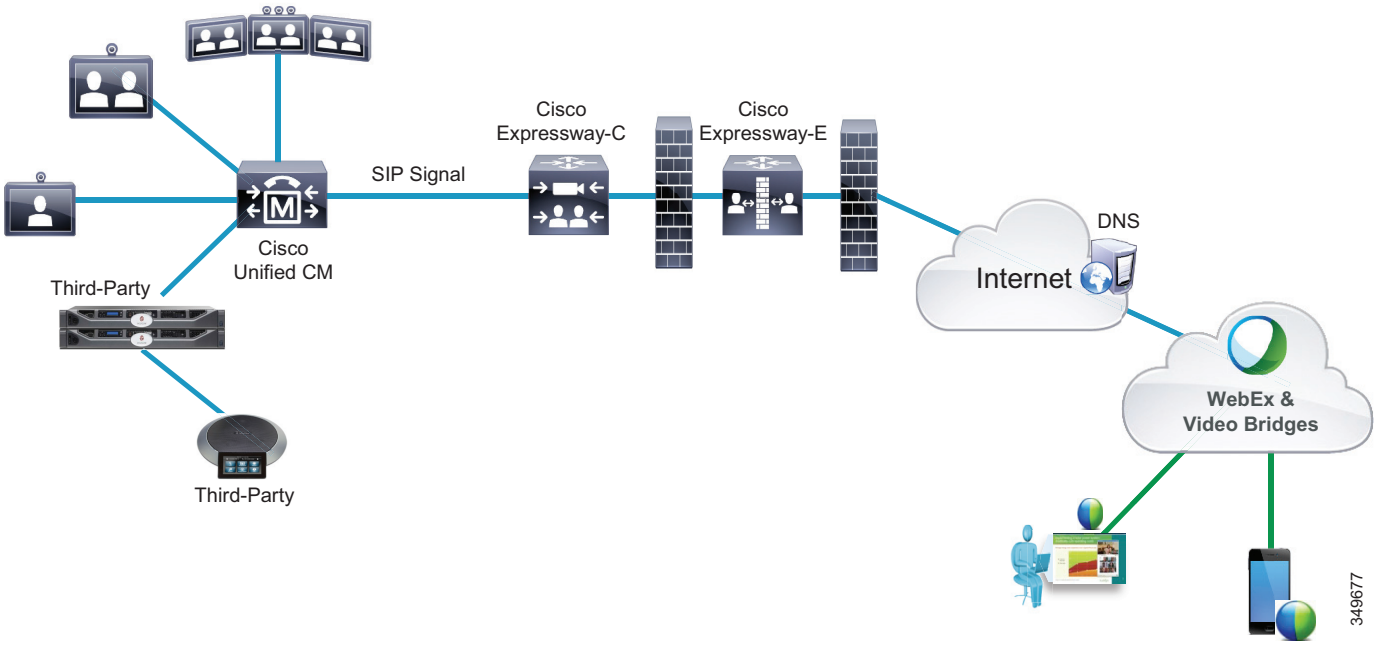
Cisco WebEx Meeting Center Video Conferencing は、一貫性のあるスケーラブルな仮想会議室エクスペリエンスを提供するエンタープライズ クラスのコラボレーション サービスです。このサービスは、ビジネス品質のビデオ、音声、データ共有機能を 1 つに統合したソリューションを、Cisco WebEx Collaboration Cloud を介して提供します。Cisco WebEx Meeting Center Video Conferencing は、Cisco WebEx Meeting Center サブスクリプションを購入すると、その一部として提供されます。これは、Cisco Unified CM や Cisco Expressway などのシスコ コラボレーション インフラストラクチャおよびアプリケーションに統合されます。参加者は、WebEx クライアント、Cisco TelePresence、Cisco Jabber、またはその他のサードパーティ製の標準ベースのエンドポイント（SIP または H.323）を使用して Cisco WebEx Meeting Center Video Conferencing 会議に参加できます。また、Cisco WebEx Collaboration Cloud のシンプルで安全性の高いコラボレーション ソリューションが提供され、参加者はどこにいるかに関係なく、任意のデバイス（デスクトップ、モバイル、ビデオ エンドポイント）を使用して会議に参加できます。Cisco WebEx Meeting Center Video Conferencing では、ユーザがパーソナライズされた常時使用可能な会議室にその他のユーザをいつでも招待して参加させたり、会議主催者が生産性向上ツールを使用してスケジュール済み会議に必要なルームとリソースを予約したりできます。

アーキテクチャ

図 11-17 に、SIP ビデオを使用した Cisco WebEx Meeting Center Video Conferencing のアーキテクチャを示します。このアーキテクチャは、エンタープライズ コラボレーション ネットワーク、およびすべての会議リソースがホストされる WebEx Collaboration Cloud で構成されており、それらはインターネットを介して接続されています。エンタープライズ コラボレーション ネットワークには Cisco Unified Communications Manager（Unified CM）と Cisco Expressway が含まれ、Unified CM は SIP トランクを介して Cisco Expressway-C と接続します。Cisco Unified CM は、登録されたビデオ デバイスのコール ルーティングおよび呼制御機能を提供します。Cisco Expressway は、企業と WebEx Collaboration Cloud の間にセキュアなファイアウォール トラバーサル メカニズムを提供し、Cisco Expressway-E 内で設定された DNS ゾーンを介して WebEx Collaboration Cloud へのビデオ コールをルーティングします。さらに、Cisco Expressway はサポートされるシスコのビデオ エンドポイントへのモバイルおよびリモート アクセス機能を提供するため、それらのエンドポイントは企業外の Unified CM に登録できます。参加者が会議および共有コンテンツに参加するためには、SIP デバイスが URI ダイヤリングおよび Binary Floor Control Protocol（BFCP）をサポートしている必要があります。BFCP を使用しなければ、コンテンツを共有できません。その場合、コンテンツはメイン ビデオに埋め込まれたように表示されます。

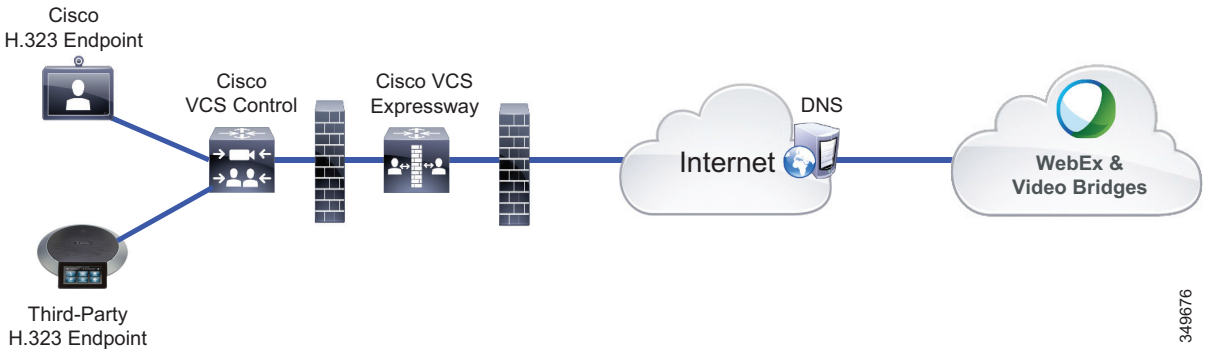
（注）　Cisco VCS の既存顧客の場合、VCS Control を SIP エンドポイント用の SIP レジストラおよびファイアウォール トラバーサル用の VCS Expressway として使用することは、導入でサポートされます。

図 11-17　SIP ビデオを使用した Cisco WebEx Meeting Center Video Conferencing のアーキテクチャ



Cisco WebEx Meeting Center Video Conferencing のアーキテクチャでは、H.323 ビデオ デバイスもサポートされます（図 11-18 を参照）。このアーキテクチャでは、Cisco VCS Control はゲートキーパーであり、登録された H.323 エンドポイントの呼制御を提供します。Cisco VCS Expressway は、企業と WebEx クラウドの間のコールにセキュアなファイアウォール トラバーサル メカニズムを提供し、Cisco VCS Expressway 内で設定された DNS ゾーンを介して WebEx クラウドへのビデオ コールをルーティングします。参加者が会議および共有コンテンツに参加するためには、H.323 デバイスが URI ダイヤリング用の Annex O およびコンテンツ共有用の H.239 をサポートしている必要があります。H.239 を使用しなければ、コンテンツを共有できません。その場合、コンテンツはビデオに埋め込まれたように表示されます。さらに、ホストとして会議を開始するため、またはホストが参加する前に会議に参加するために自動音声応答（IVR）を使用するには、H.323 デバイスが DTMF シグナリングの RFC 2833 方式または H.245 ユーザ入力のいずれかをサポートしている必要があります。

図 11-18　H.323 ビデオを使用した Cisco WebEx Meeting Center Video Conferencing のアーキテクチャ



また、コール制御システムなしで H.323 ビデオを使用して Cisco WebEx Meeting Center Video Conferencing を導入することもできます（図 11-19 を参照）。このアーキテクチャでは、H.323 デバイスはゲートキーパーに登録せず、ユーザが URI をダイヤルすると、そのコールは DNS を使用してファイアウォールを通して WebEx クラウドにルーティングされます。シグナリングおよびメディアが通過できるように、必要なファイアウォールのポートが開いていることを確認してください。ポート範囲の詳細については、https://collaborationhelp.cisco.com/article/en-us/WBX264 でアクセスできる Collaboration Help の記事を参照してください。

図 11-19　コール制御システムなしで H.323 ビデオを使用した Cisco WebEx Meeting Center Video Conferencing のアーキテクチャ

Cisco WebEx Meeting Center バージョン WBS32.9 以降、ユーザは会議の招待に記載されている地域の IP アドレスをダイヤルして、H.323 ビデオシステムから会議に参加できるようになっています。ただし、ユーザが別の地域の IP アドレス（会議の招待には記載されていない IP アドレス）をダイヤルした場合は、会議への参加は許可されません。

導入で使用される SIP デバイスまたは H.323 デバイスに関係なく、WebEx クラウドはプロトコル間のインターワーキングを実行できます。Cisco WebEx Meeting Center Video Conferencing 導入環境でビデオ デバイスを使用するには、いくつかの要件があります。詳細については、以下のリンク先から入手できる『*Cisco WebEx Meeting Center Enterprise Deployment Guide for Video Device-Enabled Meetings*』を参照してください。

https://collaborationhelp.cisco.com/article/en-us/nmdp0hq

ビデオ デバイス上の各参加者について、音声、ビデオ、およびコンテンツ共有が IP 接続を介して WebEx クラウドに送信されます。そこでメディアはその他の参加者と混合され、混合された音声、通話中のスピーカーのビデオ、およびコンテンツ共有がデバイスに戻されて表示されます。

Cisco WebEx Meeting Center Video Conferencing では、通話中のスピーカーとコンテンツ共有に H.264 ビデオを使用します。デバイスの能力および使用可能な帯域幅に応じて、Cisco WebEx Meeting Center Video Conferencing は、ビデオ デバイス上および WebEx クライアントで、最大 720p、30 フレーム/秒（fps）の通話中のスピーカーのビデオ、および最大 720p のコンテンツ ビデオをサポートします。WebEx 会議クライアントでは、通話中のスピーカーのビデオのビデオ フロアは 180p、最小ビットレート 1.2 Mbps です。ネットワークの状態が原因で最小ビット レートを維持できない場合（重度のパケット損失など）、WebEx クライアントは通話中のスピーカーのビデオの受信を停止しますが、コンテンツ共有および会議の音声は受信し、そのビデオを他の参加者に送信します。WebEx クライアントは定期的に帯域幅の再テストを実行し、ネットワークの状態が安定すると自動的に通話中のスピーカーのビデオを再確立します。会議中に、WebEx は、会議内のすべての WebEx クライアントの中で最小能力デバイスに基づいて（ビデオ フロア未満で実行されているデバイスを除く）、最大帯域幅 4 Mbps で帯域幅を割り当てます。ただし、最小能力デバイスが会議を離脱した場合、帯域幅は、WebEx 会議クライアントを実行している次の最小能力デバイスに基づいて再割り当てされます。割り当てられた帯域幅によって、WebEx クライアント上のビデオの表示に使用する解像度が決まります。

Cisco WebEx Meeting Center Video Conferencing セッションごとに、ビデオ アドレスの URI と URL が関連付けられます。参加者は、URI をダイヤルするか、ビデオ デバイスでコールバックを受信するか、または URL をクリックして WebEx 会議クライアントを開き、会議に参加します。Cisco WebEx Meeting Center Video Conferencing 会議は、以下のいずれかのタイプにすることができます。

スケジュール済み会議

ユーザは WebEx Productivity Tools（PT）を使用して Cisco WebEx Meeting Center Video Conferencing 会議をスケジュールできます。Productivity Tools は Outlook プラグインを含むツール スイートであり、ユーザが電子メール クライアント内で迅速かつ簡単に会議をスケジュールできるようにします。このツール スイートはユーザのカレンダーとのシームレスな統合を提供し、ユーザは会議をスケジュールし、1 つのトランザクションで電子メール クライアントからすべての参加者に招待状を直接送信できます。また、ユーザは WebEx ポータルから Cisco WebEx Meeting Center Video Conferencing 会議をスケジュールすることもできます。ただし、会議の開催者は、WebEx から会議をスケジュールした後、会議の詳細を添付した招待状を作成して参加者全員に送信する必要があります。

Cisco TMS 15.2 および TMSXE 5.2 を使用している場合は、WebEx Productivity Tools により、ワンボタン機能（OBTP）で Cisco WebEx Meeting Center Video Conferencing 会議をスケジュールできます。Cisco TMS は内部で Cisco WebEx Meeting Center Video Conferencing への SIP URI をダイヤル文字列として使用して、外部でホストされる会議を作成します。また、Cisco TMS ではデフォルトの会議タイプを OBTP に設定する必要があります。

（注）　Cisco WebEx Meeting Center Video Conferencing OBTP に Cisco TMS および TMSXE を使用する場合、オンプレミスのビデオ会議インフラストラクチャを統合する必要はありません。一方、TMS と TMSXE がオンプレミスのビデオ会議インフラストラクチャと統合されている場合は、この 2 つを同時に Cisco WebEx Meeting Center Video Conferencing OBTP で使用できます。

Cisco WebEx Meeting Center バージョン WBS32.6 以降、ユーザが Google カレンダーから直接、WebEx Personal Room で会議をスケジュールしたり開始したりできるようになっています。この機能を使用するには、ユーザが Google Web ストアから Cisco WebEx Scheduler 拡張機能をインストールし、さらにサイト管理者が WebEx サイトで Google カレンダー オプションを有効にする必要があります。ユーザが自分の WebEx アカウントを使って Cisco WebEx Scheduler 拡張機能にサインインすると、そのユーザの Google アカウントで WebEx サービスを使用できるようになります。ユーザの Google アカウントにリンクできる WebEx アカウントは 1 つだけです。Google カレンダー対応 Cisco WebEx Scheduler の設定と制約事項について詳しくは、以下のリンク先の記事を参照してください。

- https://collaborationhelp.cisco.com/article/en-us/j5bm2v
- https://collaborationhelp.cisco.com/article/en-us/9pq6jc

パーマネント会議

会議はユーザのパーソナル ルームでホストできます。パーソナル ルームは、サイト レベル、または WebEx サイトのユーザ単位レベルで有効にすることができます。パーソナル ルームが有効になっている場合、固定 URI および URL が各ユーザに割り当てられ、参加者はそれらを使用してユーザのパーソナル ルームに参加できます。このパーソナル ルームは指定されたユーザに属しており、常にオンです。したがって、ユーザは自身のルームを自身の会議に使用し、ルームの URI と URL を添付した招待状をすべての参加者に送信できます。Cisco Spark のカレンダー サービスを使用すると、Outlook カレンダーの招待状の [場所] フィールドに @webex を追加することができ、カレンダー コネクタがユーザのパーソナル ルーム情報を招待状に自動的に追加します。詳細については、モバイル コラボレーション（21-1 ページ）の章を参照してください。

インスタント会議

ユーザは、WebEx ポータルから、または WebEx Productivity Tools を使用してインスタント会議を作成することができ、会議は即時に開始されます。[今すぐミーティング] 設定オプションを使用すると、Meeting Center、ユーザのパーソナル ルーム、Cisco Jabber Desktop からインスタント会議を開始できます。

セキュリティ

Cisco WebEx Meeting Center Video Conferencing は、エンタープライズ ネットワークと WebEx クラウドの間で、暗号化されたシグナリングとメディア、または暗号化された/非セキュア シグナリングとメディアの組み合わせをサポートします。エンドツーエンドの暗号化の場合、エンタープライズで暗号化されたシグナリングとメディアをオンにし、エンタープライズ ネットワークと WebEx クラウドの間で暗号化されたシグナリングとメディアを使用することができます。暗号化されたシグナリングが機能するためには、証明書を Cisco Expressway-E にアップロードして、適切なハンドシェイクが行われるようにする必要があります。この証明書は、自己署名するか、信頼できるルート認証局（CA）の署名を受けることができます。詳細については、以下のリンク先から入手できる最新バージョンの『*Cisco WebEx Meeting Center Video Conferencing Enterprise Deployment Guide*』を参照してください。

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

SIP ベースのコールについては、Cisco WebEx Meeting Center Video Conferencing は以下の 4 レベルのセキュリティ（優先順に記載）をサポートしています。

- CA 署名付き証明書および SRTP メディア暗号化で暗号化された TLS シグナリング
- 自己署名証明書および SRTP メディア暗号化で暗号化された TLS シグナリング
- SRTP メディア暗号化を使用した非セキュア TCP シグナリング
- 非セキュア RTP メディアを使用した非セキュア TCP シグナリング

必ずファイアウォールのネットワーク ポートを開いて、シグナリングおよびメディアの着信トラフィックと発信トラフィックが通過できるようにしてください。ポート範囲の詳細については、https://collaborationhelp.cisco.com/article/en-us/WBX264 でアクセスできる WebEx の記事を参照してください。

すべての Cisco WebEx Meeting Center Video Conferencing 会議では、会議を開始する開催者のプレゼンスが必要となります。ゲストは、ホストより前に参加すると待合室にとどまり、ホストが参加するまでは互いに会話することはできません。さらに、ホストがビデオ デバイスから会議に参加するときにホスト PIN が必要となります。

ユーザのパーソナル ミーティング ルーム内には、ルームをロックして他の参加者がユーザのパーソナル ルームに入らないようにするために使用できる [ルームをロック（Lock Room）] ボタンがあります。ルームがロックされているときに参加者がそのルームに入ろうとすると、ホストが許可するかルームをロック解除するまでは、その参加者はブロックされます。このボタンは、ユーザのパーソナル ルームが連続した会議に使用され、ホストがまだ最初の会議を終えていない場合に役立ちます。ホストは、最初の会議が終了してロック解除されるまでは 2 番目の会議の参加者が入るのを防ぐために、ルームをロックできます。

オーディオ導入オプション

ビデオ デバイスを使用した Cisco WebEx Meeting Center Video Conferencing 参加者の場合、音声、ビデオ、コンテンツ共有は WebEx クラウドとビデオ デバイス間の IP 接続を介して送受信されます。WebEx クライアントの参加者に対しては、Cisco WebEx Meeting Center Video Conferencing は従来の WebEx Meeting Center で使用可能なすべてのオーディオ オプションをサポートします。つまり、以下のようなオプションです。

- WebEx Cloud Connected Audio
- VoIP を使用した WebEx Audio
- PSTN を使用した WebEx Audio
- Teleconferencing Service Provider Audio

ハイ アベイラビリティ

エンタープライズ コラボレーション ネットワークでは、Cisco Unified CM および Cisco Expressway のクラスタリング オプションを使用して、ビデオ デバイスとファイアウォール トラバーサル コールを使用した呼制御に冗長性を提供します。プライマリ サーバで障害が発生すると、バックアップ サーバは呼制御および呼処理機能を引き継ぐことができます。

Cisco Unified CM クラスタリングについては、呼処理（9-1 ページ）の章を参照してください。

Cisco Expressway クラスタリングについては、次の Web サイトで入手可能な『*Cisco Expressway Cluster Creation and Maintenance Deployment Guide*』の最新バージョンを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

キャパシティ プランニング

Cisco WebEx Meeting Center Video Conferencing 会議は、最大で 25 台の標準ベースのビデオ デバイス、ビデオを有効にした 500 人の WebEx 参加者、および音声のみの 500 人の WebEx 参加者をサポートします。

(注)　マルチスクリーン ビデオ デバイスの各画面が、1 つのビデオ デバイスとしてカウントされます。たとえば、トリプル スクリーン イマーシブ システムが Cisco WebEx Meeting Center Video Conferencing 会議に参加すると、ビデオ デバイス キャパシティ制限から 3 つのビデオ デバイスを消費します。

Cisco WebEx Meeting Center Video Conferencing のキャパシティ プランニングには、企業内で稼働するコンポーネントのサイジングが含まれます。コンポーネントには、以下が含まれます。

- Cisco Unified CM

  Cisco WebEx Meeting Center Video Conferencing 会議のビデオ エンドポイントおよび IP Phone によって生成されるトラフィックを処理するために十分なリソースとキャパシティが Unified CM にあることを確認してください。キャパシティの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

- Cisco Expressway

  Cisco Expressway は、導入環境のトラバーサル コール トラフィックを処理するのに十分なリソースを提供する必要があります。キャパシティの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

ネットワーク トラフィック プランニング

Cisco WebEx Meeting Center Video Conferencing のネットワーク トラフィック プランニングは、次の要素で構成されます。

- WebEx クライアントの帯域幅

  WebEx 会議クライアントは、Scalable Video Coding（SVC）テクノロジーを使用してビデオを送受信します。ビデオの送信にマルチレイヤ フレームが使用され、受信クライアントは可能な最善の解像度を自動的に選択してビデオを受信します。これには、通常 1.2 ～ 3 Mbps の使用可能帯域幅が必要です。WebEx クライアントのネットワーク トラフィック プランニングの詳細については、次の Web サイトで入手可能なホワイトペーパー『*Cisco WebEx Network Bandwidth*』を参照してください。

  https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white_paper_c11-691351.html

- 企業から WebEx クラウドへのビデオ デバイスの帯域幅

  最適な SIP 音声およびビデオの品質のために、Cisco Unified CM に登録するエンドポイントに関連付けられた地域内のデバイスの画面ごとにビデオ帯域幅を少なくとも 1.5 Mbps に設定することを推奨します。トリプル スクリーン デバイスが Unified CM に登録する場合、4.5 Mbps のビデオ帯域幅を関連地域に割り当てる必要があります。

設計上の考慮事項

Cisco WebEx Meeting Center Video Conferencing を導入する際は、以下の推奨事項を考慮してください。

- ビデオ エクスペリエンスを最適にするために、ファイアウォールでメディア ストリーミングに対して UDP を有効にします。
- シグナリングおよびメディアの着信トラフィックおよび発信トラフィックを許可するために、ファイアウォールのネットワーク ポートを開きます。詳細については、以下のリンク先から入手できる最新バージョンの『*Cisco WebEx Meeting Center Video Conferencing Enterprise Deployment Guide*』を参照してください。

  https://www.cisco.com/c/en/us/support/conferencing/webex-meeting-center/products-installation-and-configuration-guides-list.html
- Cisco Expressway-C 内の Unified CM ネイバー ゾーンが Binary Floor Control Protocol（BFCP）を有効にして設定されていること、および Unified CM と Expressway-C の間の SIP トランクに関連付けられた SIP プロファイルで BFCP が有効になっていることを確認してください。
- Cisco WebEx Meeting Center Video Conferencing でテスト済みのデバイスについては、以下のリンク先でアクセスできる記事「*WebEx Video Compatibility and Support*」を参照してください。

  https://collaborationhelp.cisco.com/article/en-us/ipxxr2

Cisco WebEx Meetings Server

Cisco WebEx Meetings Server は、非常に安全で、完全に仮想化された、プライベート クラウドの会議ソリューションで、音声、ビデオ、Web 会議を 1 つのソリューションに統合しています。Cisco WebEx Meetings Server は、従業員の生産性を高め、さらにダイナミックなコラボレーションと柔軟な働きかたをサポートするために必要なすべてのツールを備えた、包括的な会議ソリューションを提供することで、現代の企業のニーズに応えます。既存ユーザは、導入済みの Cisco Unified Communications をベースにしながら、既存の Cisco Unified Communications Manager の実装を拡張して SIP アーキテクチャを使用した会議の機能を組み込むことができます。また、次の例のように、Cisco WebEx Meetings Server は Cisco Unified CM の多くの機能を活用してその機能を実行します。

- SIP トランク接続と Unified CM を使用して電話会議を主催する
- セキュア会議に Unified CM の SIP トランクのセキュア接続サポートを利用する
- Unified CM によってレガシーまたはサードパーティ製 PBX を統合する
- IPv6 をサポートするために Unified CM のデュアル スタック（IPv4 および IPv6）機能を活用する

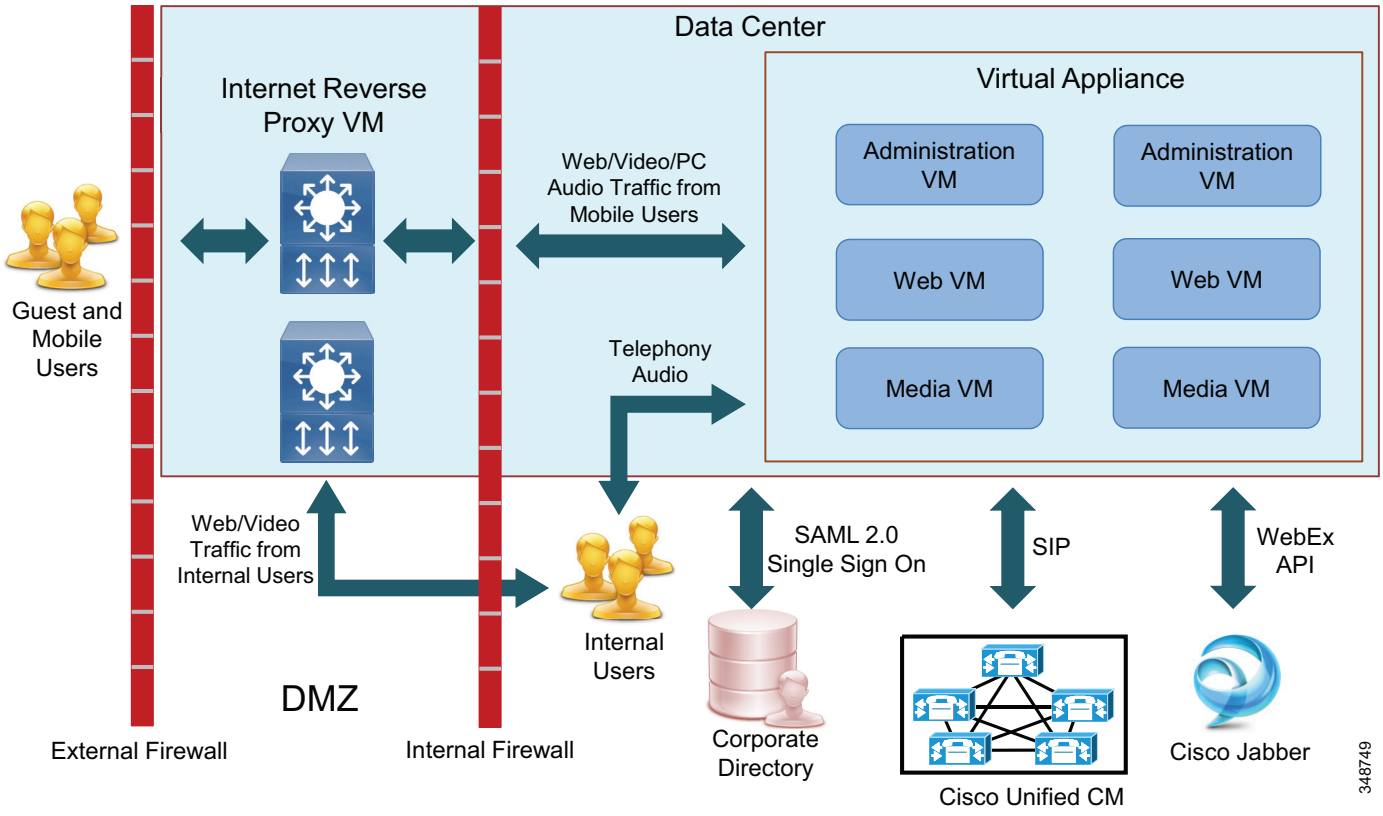
これらの機能については、以下の項で詳しく説明します。

アーキテクチャ

Cisco WebEx Meetings Server は、Cisco Unified Computing System（UCS）で動作する、完全に仮想化された、ソフトウェア ベースのソリューションです。サービスを迅速に導入するために、仮想アプライアンス テクノロジーを使用します。仮想アプライアンスは、システムの管理タスクを簡素化します。たとえば、ハイパーバイザ テクノロジーを使用することで、メンテナンスのためにシステム コンポーネントを簡単に移動したり、問題が発生したときにシステム コンポーネントを正常動作するバージョンに簡単にロール バックすることが可能です。仮想アプライアンスは、業界標準の形式、オープン仮想アプライアンス（OVA）で配布されます。WebEx Meetings Server をインストールするために必要なすべてのソフトウェア コンポーネントが OVA 内部にパッケージ化されています。従来、実行ファイルのインストーラを使用して個々のソフトウェア コンポーネントをインストールする場合は、ソフトウェアの展開に時間がかかりました。しかし、OVA を使用すれば、すべてのソフトウェア コンポーネントがファイル内にあらかじめパッケージ化されているため、ソフトウェアを展開するのに必要な時間を大幅に短縮できます。したがって、仮想アプライアンス テクノロジーは Cisco WebEx Meetings Server の展開にかかる時間の短縮に非常に役立ちます。

図 11-20 に、非分割水平ネットワーク トポロジを使用した Cisco WebEx Meetings Server のアーキテクチャの概要を示します（非分割水平ネットワーク トポロジの詳細については、https://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html から入手できる『*Cisco WebEx Meetings Server Planning Guide*』を参照してください）。仮想アプライアンス内では、1 つまたは複数の仮想マシン（VM）を実行できます。管理、Web、メディアの仮想マシンです。管理仮想マシンおよび Web 仮想マシンは、管理や WebEx サイトのバックエンド処理として機能します。これらのサイトは、設定、会議のスケジューリングや参加、録音の再生といった、会議の前後に発生するタスクを処理します。メディア仮想マシンは、会議中にリソース割り当て、テレビ会議の呼制御、およびメディア処理（音声、ビデオ、データ）を提供します。仮想アプライアンス内で動作する仮想マシンの数は、必要なキャパシティと、ハイ アベイラビリティの必要性によって決まります。これにより、導入サイズにさまざまなオプションが提供されます。

図 11-20　Cisco WebEx Meetings Server のアーキテクチャの概要

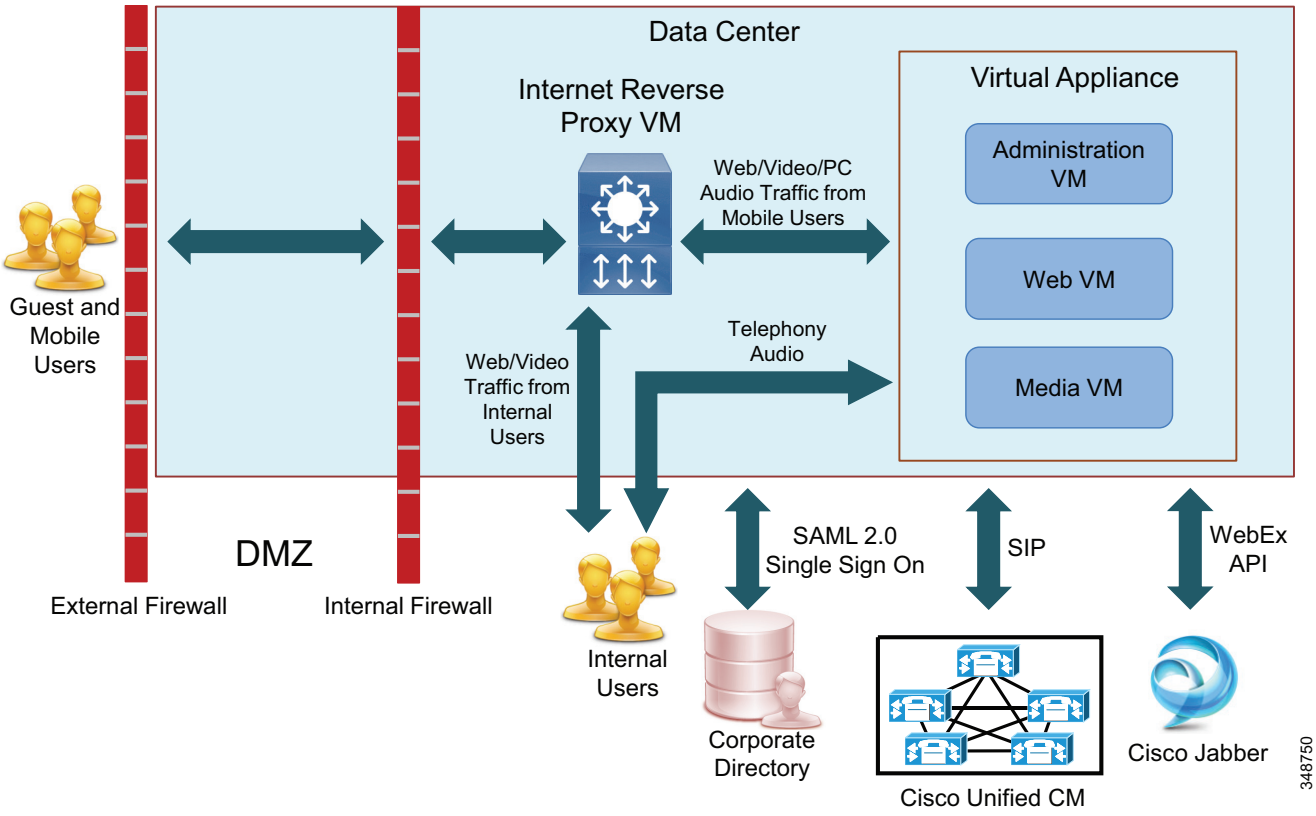


Cisco WebEx Meetings Server には、外部アクセスを容易にするため、DMZ 内にインターネット リバース プロキシ（またはエッジ サーバ）を配置するというオプションがあります。このオプションには、2 つの利点があります。まず、すべての外部参加者はインターネットから VPN を通過せずに、安全に WebEx 会議にアクセスできます。2 番目に、モバイル ユーザは、インターネット接続が存在する限り、どこにいてもモバイル デバイスから会議に参加できます。モバイル クライアント アクセスが有効になっている場合、インターネット リバース プロキシが必須であることに注意してください。

インターネット リバース プロキシは、インターネットからのすべての着信トラフィックを DMZ 内で終端させるために使用されます。コンテンツは暗号化された Secure Socket Layer（SSL）または Transport Layer Security（TLS）トンネルを介して内部仮想マシンに転送されます。この暗号化されたトンネルは、インターネット リバース プロキシに外向き接続する内部仮想マシンによって確立されます。したがって、DMZ から内部ファイアウォールの内部ネットワークへの着信 TCP ポートを開く必要はありません。ただし、DMZ 内のインターネット リバース プロキシとの通信を許可するには、内部ファイアウォールで内部ネットワークからの一部の発信ポートを開く必要があります。

すべてのエンドユーザ セッションは、業界標準の Secure Socket Layer（SSL）および Transport Layer Security（TLS）を使用して、100% 暗号化されます。仮想マシン間のすべてのトラフィックは、セキュアなチャネルを介して送信されます。米国の国防総省（DoD）レベルのセキュリティを提供する連邦情報処理標準（FIPS）暗号化も、単一のポリシー設定によってオンにできます。または、図 11-21 のように、インターネット リバース プロキシを内部ファイアウォールの後方に配置することもできます。

図 11-21　内部ファイアウォール後方のインターネット リバース プロキシ



組織では一般に、セキュリティ上の理由から、DMZ の内側にコンポーネントを展開する許可の取得に何ヵ月もかかります。この方法を使用して、DMZ コンポーネントを排除して承認プロセスをバイパスすることで、WebEx Meetings Server の導入を迅速に実施できます。外部ファイアウォールへのすべてのインターネット トラフィック（ポート 80 上の HTTP およびポート 443 上の SSL）は、内部ファイアウォールに転送される必要があります。これにより、外部および内部のファイアウォールに開く必要があるポート数が最小限になります。ただし、内部ネットワーク内にインターネット リバース プロキシを配置することは、着信インターネット トラフィックが内部ネットワークで終端することを意味します。内部ネットワークへの直接のインターネット アクセスはファイアウォールによって制御できますが、すべての組織が内部ネットワークでインターネット トラフィックを直接終端させることを許可しているわけではありません。このオプションを選択する前に、この導入が組織の IT ポリシーに違反していないことを確認してください。

大規模企業の導入環境では、エンド ユーザが企業の資格情報を使用してサイン インできるよう、シングル サイン オン（SSO）機能が必要になることがあります。Cisco WebEx Meetings Server は、SSO 用の業界標準 SAML 2.0 を使用して、社内 LDAP ディレクトリに接続できます。

（注）　Cisco WebEx Meetings Server は、Meeting Center だけをサポートします。

（注）　Cisco WebEx Meetings Server 1.1 以降、Cisco Unified CM IM and Presence サービスと統合された Cisco Jabber を使用して、WebEx Meetings Server 上でホストされた会議に参加または開始することができます。Cisco Jabber のサポートの詳細については、https://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html から入手できる『*Cisco WebEx Meetings Server System Requirements*』を参照してください。

Cisco Unified CM の統合

Cisco WebEx Meetings Server は、Cisco Unified CM と Session Management Edition（SME）の両方をサポートします。Cisco Unified CM は、WebEx Meetings Server アーキテクチャの中心部分で、次の操作を可能にします。

- 会議参加者が Cisco IP Phone または PSTN によって電話会議に参加する
- Cisco WebEx Meetings Server とレガシーまたはサードパーティ製 PBX との統合

Cisco Unified CM は、着信およびコールバックの呼制御を行う SIP トランクによって WebEx Meetings Server と統合されます。顧客は、セキュリティをオンにして、SIP トランク接続上で Transport Layer Security（TLS）および Secured Real-time Transport Protocol（SRTP）を実行できます。SIP トランクは、WebEx Meetings Server 内のロード バランサの宛先アドレスを使用して Unified CM 上で設定され、SIP トランク経由のコールをルーティングするために、ルート パターン（WebEx Meetings Server で設定されたコールインのアクセス番号と一致）を使用する必要があります。2 番目の SIP トランクは、WebEx Meetings Server のアプリケーション サーバの宛先アドレスを使用して Unified CM 上で設定され、SIP トランク経由のコールをルーティングするためには SIP ルート パターンを使用する必要があります。会議に参加するために参加者がアクセス番号をダイヤルすると、コール送信に最初の SIP トランクが使用されます。コールが接続され、発信者が会議 ID を入力した後、ロード バランサは SIP REFER を Unified CM に発行して、2 番目の SIP トランク経由で会議をホストするアプリケーション サーバに発信者を転送します。

システム管理者は、コールバックを実行するよう、Unified CM をポイントする WebEx Meetings Server 内の SIP トランクを設定できます。参加者は、コールバック番号を入力して、ブリッジに参加するようシステムから参加者の番号へ外線ダイヤルさせることができます。参加者がコールバックを要求している場合、WebEx Meetings Server は設定済み SIP トランク経由でコールバック番号とともに、Unified CM に SIP 要求を送信します。会議参加のコールバック要求から受信したすべてのダイヤル ストリングを Unified CM が解決できることが不可欠です。サイト管理設定により、コールバックをシステム全体で無効にすることもできます。Unified CM は、さまざまな国に対するすべての料金制限や、ほとんどの企業がブロックするその他の番号も制御します。WebEx Meetings Server には、それ自体をブロックする料金制限がないためです。

WebEx Meetings Server は双方向 SIP OPTIONS ping メカニズムをサポートします。リモート エンドからの ping 応答は、リモート エンドがアクティブかどうか、コールを受け入れることができるかどうかを示します。応答に基づいて、WebEx Meetings Server または Unified CM は、現在の SIP トランク上でコールを送信するか、代替 SIP トランク（設定されている場合）を探してコールを送信するかを判断できます。SIP OPTIONS ping は Cisco Unified CM 8.5 以降のリリースでサポートされていることに注意してください。この理由から、Cisco WebEx Meetings Server 導入には、SIP OPTIONS ping をサポートする、互換性のある Cisco Unified CM バージョンを使用することを推奨します。互換性のある Unified CM バージョンのリストについては、次の Web サイトで入手可能な『*Cisco WebEx Meetings Server System Requirements*』の互換性マトリックスを参照してください。

https://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html

（注）　Cisco WebEx Meetings Server は Cisco Unified CM との SIP トランク接続のみをサポートします。

レガシー PBX の統合

レガシー PBX があり、Cisco Unified Communications ソリューションに完全移行する準備ができていない組織では、会議用システムに Cisco WebEx Meetings Server を使用することができます。Cisco Unified CM は、レガシー PBX と Cisco WebEx Meetings Server とのブリッジ接続に使用できます。Cisco WebEx Meetings Server は、Unified CM だけを認識でき、PBX が Unified CM の背後にあることは認識しません。Unified CM が組織の PBX と相互運用できるのであれば、Cisco WebEx Meetings Server を組織の PBX と統合できます。この統合によって複数の利点が得られます。

- レガシー システムのユーザも新しいテクノロジーを体験できる
- 組織が新しいテクノロジーを段階的に自分のペースで導入できる
- シスコのテクノロジーに徐々に移行しつつ、既存のテクノロジーに対する顧客の投資を保護する

PBX と Unified CM との相互運用性の詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

https://www.cisco.com/en/US/solutions/ns340/ns414/ns728/networking_solutions_products_genericcontent0900aecd805b561d.html

IPv6 のサポート

Cisco WebEx Meetings Server は、テレフォニー オーディオについて、IPv4 のみ、またはデュアル スタック（IPv4 および IPv6）アドレッシングをサポートします。テレフォニーのシグナリングは IPv4 のままです。オーディオ ストリームは、IPv4、IPv6 に加え、同じ会議で IPv4 と IPv6 を混合して使用できます。Cisco WebEx Meetings Server は、代替ネットワーク アドレス タイプ（ANAT）をサポートし、SIP トランクと Unified CM とが優先アドレッシング方式を使用したメディア接続を確立するために SIP Offer と Answer を交換する間、Session Description Protocol（SDP）内での IPv4 と IPv6 両方のメディア アドレッシングを有効にします。

電話会議には、IPv4 と IPv6 の両方のデバイスを使用できます。IPv6 デバイスの場合、Cisco WebEx Meetings Server は IPv6 シグナリングを IPv4 に変換し、SIP トランクを介して Cisco WebEx Meetings Server に伝送する Unified CM の機能を活用します。テレフォニー メディア アドレッシングを使用すると、Cisco WebEx Meetings Server は IPv4 と IPv6 の間での変換を実行できます。したがって、Cisco WebEx Meetings Server は高価な MTP リソースなしで IPv6 をサポートできます。

ANAT を使用すると、Cisco WebEx Meetings Server は IPv6 テレフォニー シグナリングのサポートなしで IPv6 テレフォニー オーディオをサポートできます。ただし、ANAT が Unified CM SIP トランクの両側でサポートされている必要があります。Unified CM SIP トランクの ANAT を必ず有効にしてください。有効にしないと、参加者のコールバック要求やダイヤル イン試行のときのコール確立に失敗します。

WebEx Meetings Server で IPv6 が有効になると、ANAT ヘッダーがメディア オファーに含まれます。メディア オファーに ANAT ヘッダーが含まれる場合、WebEx Meetings Server は必ず ANAT ヘッダーで応答します。次に、ANAT ヘッダーを使用した、IPv6 対応 WebEx Meetings Server とデュアル スタック Unified CM との間でのメディア アドレスのバージョン選択プロセスについて説明します。

WebEx Meetings Server が Unified CM にコールを発信するとき、SDP オファーには IPv6 と IPv4 の両方のメディア アドレスが含まれます。着信側デバイスが IPv6 の場合、Unified CM はメディア接続に IPv6 を選択して SDP の IPv6 メディア アドレスに応答します。着信側デバイスがデュアル スタックの場合、Unified CM は [メディア用の IP アドレッシングモード設定（IP Addressing Mode Preference for Media）] パラメータを使用して応答 SDP でのアドレス バージョンを決定します。パラメータが IPv6 に設定されている場合、IPv6 がメディア接続に使用されます。

Unified CM が SIP トランクによって WebEx Meetings Server にコールを送信すると、WebEx Meetings Server は ANAT ヘッダーが付いた SDP オファーを受信します。SDP オファーに IPv6 と IPv4 両方のメディア アドレスが含まれている場合、WebEx Meetings Server は ANAT ヘッダーで高い優先順位が指定されたバージョンで応答します。この場合は IPv6 になります。SDP に IPv6 アドレスだけが含まれている場合、WebEx Meetings Server は IPv6 メディア アドレスを使用して応答します。

Cisco Unified Communications システムでの IPv6 の導入の詳細については、次の Web サイトで入手可能な『*Deploying IPv6 in Unified Communications Networks with Cisco Unified Communication Manager*』の最新バージョンを参照してください。

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

ハイ アベイラビリティ

Cisco WebEx Meetings Server は、コンポーネントの障害が発生した場合にシステム可用性を確保するために N+1 冗長性方式を使用します。同じデータセンター内のプライマリ システムにローカル冗長システムを追加することにより、ハイ アベイラビリティを実現できます。システム レベルでは、内部の仮想マシンとコンポーネントはアクティブ/アクティブ モードで動作します。あるコンポーネントがダウンすると、システムはそのコンポーネントを再起動します。ステータス情報が、システム コンポーネントの間で交換されます。このステータス情報を使用して、システムはアクティブなコンポーネント間で要求を均等に分配することができます。導入サイズに応じて、バックアップまたは冗長システムの仮想マシンの数は、プライマリ システムと同じ場合も、同じでない場合もあります。

ハイ アベイラビリティ システムでは、会議をホストする仮想マシンがダウンした場合、影響を受けた会議クライアントは短時間のうちに利用可能なサービスに自動的に再接続します。ただし、障害の性質や障害の起きたコンポーネントによっては、すべてのクライアントと会議が影響を受けるわけではありません。コンポーネント障害後のハイ アベイラビリティ システムの動作の詳細については、次の Web サイトで入手可能な『*Cisco WebEx Meetings Server Administration Guide*』の最新バージョンを参照してください。

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

仮想 IP アドレス

ハイ アベイラビリティ システム内には、アクティブな管理内の 2 つ目のネットワーク インターフェイスと、仮想 IP アドレスで設定されたインターネット リバース プロキシ仮想マシンがあります。管理サイトと WebEx サイトの URL では、管理サイトと WebEx サイトへのアクセスにこの仮想 IP アドレスを使用します。フェールオーバーが発生した場合、仮想 IP アドレスは新しいアクティブ仮想マシンに移行します。このように、管理および WebEx サイトにアクセス冗長性を提供します。

複数データセンター設計

地理的な冗長性やディザスタ リカバリのために、Cisco WebEx Meetings Server を複数のデータセンターに導入できます（最大で 2 つ）。この導入では、同じ導入サイズの 2 つの WebEx Meetings Server システムが存在し（各データセンターに 1 つ）、結合されて、アクティブ/アクティブ モードで実行される単一の論理システムを形成しています。マルチデータセンター システムに追加される最初のシステムはプライマリであり、その後で追加されるシステムはセカンダリです。マルチデータセンター システムにセカンダリ システムが追加されると、そのグローバル データがすべてプライマリ システムのデータで上書きされ、そのデータセンターにローカルな設定パラメータのみが保持されます。上書きされるデータと保持されるデータのタイプの詳細については、『*Cisco WebEx Meetings Server Administration Guide*』を参照してください。各データセンター内に、電話会議を処理するためのローカル Unified CM インスタンスがあります。システム ステータスが交換され、暗号化された SSL リンクを介してユーザと会議に関する情報をデータセンターのピア間で同期させます。管理者は単一 URL を使用してシステムを管理し、参加者は単一 URL または 1 つのダイヤルイン番号セットを使用して会議に参加します。参加者がクライアントを介して会議に参加すると、システムはその参加者に最も近いデータセンターを自動的に選択して会議をホストし、会議はデータセンター間でカスケードされます。

障害が発生した場合、データセンターで 1 つのコンポーネントがダウンすると、システムはそのコンポーネントを再起動します。データセンター全体がダウンすると、稼働中のデータセンターが手動での介入を必要とせずに引き継ぎ、システムは依然としてフル キャパシティで稼働しています。この場合、影響を受けた会議クライアントは、短時間の間に自動的に稼働中のデータセンターのサービスに再接続されます。ただし、障害の性質とクライアントの状態に応じて、リカバリ メカニズムが異なる場合があり、ハイ アベイラビリティ システムと同じ動作に従います。詳細については、次の Web サイトで入手可能な『*Cisco WebEx Meetings Server Administration Guide*』の最新バージョンを参照してください。

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

複数データセンター設計を使用する際は、次の点を考慮してください。

- すべてのデータセンターに NTP を設定します。
- WebEx Meetings Server システムのマルチデータセンター ライセンスが各データセンターに必要です。データセンターに参加する前に、プライマリ データセンター システムにライセンスをインストールします。
- システムあたり 50 ユーザの導入サイズはサポートされませんが、より大きいシステム サイズがサポートされます。
- データセンター内でハイ アベイラビリティ システムを実行することはサポートされていません。
- 各データセンターにローカル Unified CM インスタンスを導入します。
- システムを結合しても、システム全体のキャパシティは増加しません。
- インターネット リバース プロキシは、両方のデータセンターに導入するか、どちらのデータセンターにも導入しないかのいずれかです。

キャパシティ プランニング

WebEx Meetings Server のキャパシティは、選択したプラットフォームや導入環境内で実行する会議ノードの数によって異なります。キャパシティ プランニングの詳細については、コラボレーティブ会議（25-47 ページ）を参照してください。

ストレージ プランニング

会議を記録することが必要な場合、録音を維持するのに十分なディスク領域を Network Attached Storage（NAS）デバイスで割り当てる必要があります。ディスク領域割り当ての詳細については、次の Web サイトで入手可能な『*Cisco WebEx Meetings Server Planning Guide*』の「*Meeting Recordings*」の項を参照してください。

https://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html

ネットワーク トラフィック プランニング

WebEx Meetings Server コラボレーションのネットワーク トラフィック プランニングは、次の要素で構成されます。

- 呼制御帯域幅

  呼制御帯域幅は非常に狭いですが、重要です。WebEx Meetings Server と Unified CM を同じ場所に設置することによって、呼制御に伴う問題の回避が容易になります。離れた場所に設置する場合は、信頼できる動作を保証するための適切な QoS プロビジョニングが必要になります。呼制御帯域幅は、WebEx Meetings Server と Unified CM の間のコールの確立に使用され、各コールに必要な帯域幅の大きさは、参加者が会議に参加する方法によって決まります。会議にダイヤルインする参加者では、コールによって、2 つの SIP コールを実行するのとほぼ同量の帯域幅が消費されます。コールバックを要求している参加者では、コールによって、1 つの SIP コールを実行するのとほぼ同量の帯域幅が消費されます。SIP コールに関する呼制御帯域幅の概算および QoS プロビジョニングの詳細については、ネットワーク インフラストラクチャ（3-1 ページ）の章を参照してください。

- リアルタイム トランスポート プロトコル（RTP）トラフィック帯域幅

  RTP トラフィックは、音声とビデオのトラフィックで構成されます。音声帯域幅の計算は、各デバイスで使用するオーディオ コーデックによって異なります（コーデック タイプ別の帯域幅使用量については、ネットワーク インフラストラクチャ（3-1 ページ）の章を参照）。ビデオ帯域幅は WebEx SaaS と同じ方法で計算できます。（ネットワーク トラフィック プランニング（11-36 ページ）を参照）。

- Web コラボレーション帯域幅

  WebEx Meetings Server の Web コラボレーション帯域幅は WebEx SaaS と同じ方法で見積もることができます（ネットワーク トラフィック プランニング（11-36 ページ）を参照）。

- 複数データセンター導入

  この導入環境における適切な運用と最適なユーザ エクスペリエンスのために、最大ラウンドトリップ遅延時間（RTT）、および各カスケード会議でのデータセンター間の最小保証帯域幅と追加帯域幅のネットワーク要件があります。ネットワーク要件の詳細については、次の Web サイトで入手可能な最新の『*Cisco WebEx Meetings Server Planning Guide and System Requirements*』を参照してください。

  https://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html

設計上の考慮事項

WebEx Meetings Server の導入では、以下の設計上の考慮事項が追加で適用されます。

- WebEx Meetings Server のコンポーネントがネットワーク ファイアウォールで分離されるシナリオでは、必要なすべてのトラフィックに対して適切なピンホールが開かれていることが不可欠です。
- 通常、コラボレーティブ会議システムによって、正時の呼処理の負荷が大きくなります。WebEx Meetings Server 用の特定のパラメータを設定したキャパシティ プランニング ツールは、シスコ代理店と従業員が使用できる機能であり、大規模構成の Cisco Unified Communications システムのキャパシティの計算に役立ちます。システムのサイジングでサポートが必要な場合は、シスコ代理店またはシスコのシステム エンジニア（SE）にお問い合わせください。シスコ パートナーと従業員は、Cisco Collaboration Sizing Tool を https://cucst.cloudapps.cisco.com/landing から入手できます。
- Transport Layer Security（TLS）および Secured Real-time Transport Protocol（SRTP）の使用は、WebEx Meetings Server のキャパシティに影響しません。ただし、TLS と SRTP の使用は Cisco Unified CM のキャパシティに影響を与えます。
- WebEx Meetings Server には、回線エコー キャンセレーションが組み込まれていません。エコー キャンセレーション機能を提供するには、Cisco Integrated Service Router（ISR）などの外部デバイスを使用します。
- さまざまなシスコ コラボレーション クライアント製品の詳細と、それらがシスコの会議ソリューションにどのように適しているかについては、コラボレーション エンドポイント（8-1 ページ）の章を参照してください。
- WebEx Meetings Server を使用したコール アドミッション制御は、Unified CM によって実行されます。ロケーションベースのコール アドミッション制御では、Unified CM は、WebEx Meetings Server 固有の SIP トランクを一定量の音声帯域幅が許可されたロケーションに置くことによって、WebEx Meetings Server システムへの帯域幅を制御できます。また、Unified CM は、コール アドミッション制御も提供可能なリソース予約プロトコル（RSVP）の使用をサポートします。コール アドミッション制御戦略の詳細については、帯域幅管理（13-1 ページ）の章を参照してください。
- シスコでは、リップシンク維持のため、WebEx Meetings Server からのオーディオ ストリームとビデオ ストリームの両方を AF41（DSCP 0x22）としてマークすることを推奨します。これらの値は、WebEx Meetings Server Administration で設定できます。
- Web 会議トラフィックは SSL で暗号化され、常にベストエフォート（DSCP 0x00）とマークされます。

参照資料

WebEx Meetings Server のネットワーク要件、ネットワーク トポロジ、導入サイズのオプション、および他の導入要件とオプションについては、次の Web サイトで入手可能な『*Cisco WebEx Meetings Server Planning Guide*』を参照してください。

https://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html

Cisco Collaboration Meeting Rooms Hybrid

Cisco Collaboration Meeting Rooms（CMR）Hybrid は、Cisco TelePresence 会議のビデオ エクスペリエンスと Cisco WebEx Meeting のプレゼンテーション エクスペリエンスを単一の会議に統合するコラボレーション会議プラットフォームです。Cisco WebEx と TelePresence は、標準ベースのビデオ エンドポイントおよび WebEx 会議クライアントで動作するように最適化されています。これらは、会議の範囲の拡張、およびすべての参加者のエクスペリエンスの簡素化に役立ちます。TelePresence エンドポイントおよび WebEx クライアント上の出席者は、お互いの間で双方向ビデオ、音声、コンテンツを安全に共有できます。このプラットフォームは、2 つの会議システムのユーザ エクスペリエンスを集約し、より多くの場所のより多くのデバイス上のより多くのユーザにコラボレーションを拡張します。

Cisco CMR Hybrid では、主催者は、WebEx Productivity Tools または Cisco TelePresence Management Suite（TMS）で対応可能となる Microsoft Outlook の使い慣れたインターフェイスを使用して会議をスケジュールすることができます。ホストは、参加者を選択し、優先エンドポイントおよび WebEx 情報を追加し、参加者全員に招待を送信します。参加者は、生産性向上ツールを使用して、TelePresence または WebEx を通して参加する方法に関するすべての情報が含まれる単一の会議招待を受信します。会議は、TelePresence エンドポイントからワンボタン機能（OBTP）を使用して起動するか、またはスケジュールされた開始時刻に Cisco TMS で自動的にエンドポイントに接続できます。

アーキテクチャ

図 11-22 に示すように、Cisco CMR Hybrid の上位レベル アーキテクチャは、IP 接続を介して接続される WebEx クラウド インフラストラクチャとエンタープライズ コラボレーション ネットワークで構成されます。エンタープライズ コラボレーション ネットワークは、Cisco Unified Communications Manager（Unified CM）、Cisco Expressway-C および Expressway-E、TelePresence Conductor で管理される TelePresence Bridge プール、および Cisco TelePresence Management Suite（TMS）で構成されます。Cisco Unified CM は、企業内の TelePresence エンドポイントにコールルーティングと呼制御を提供する呼処理プラットフォームです。Cisco Expressway-C および Expressway-E は、企業ネットワークと WebEx クラウドの間のコールをルーティングします。Cisco Unified CM は、個別のベスト エフォート早期オファー SIP トランクを介して Cisco Expressway-C および Cisco TelePresence Conductor に接続します。

Cisco Unified CM と Cisco Expressway の統合の詳細については、次の Web サイトで入手可能な『*Cisco Expressway and CUCM via SIP Trunk Deployment Guide*』の最新バージョンを参照してください。

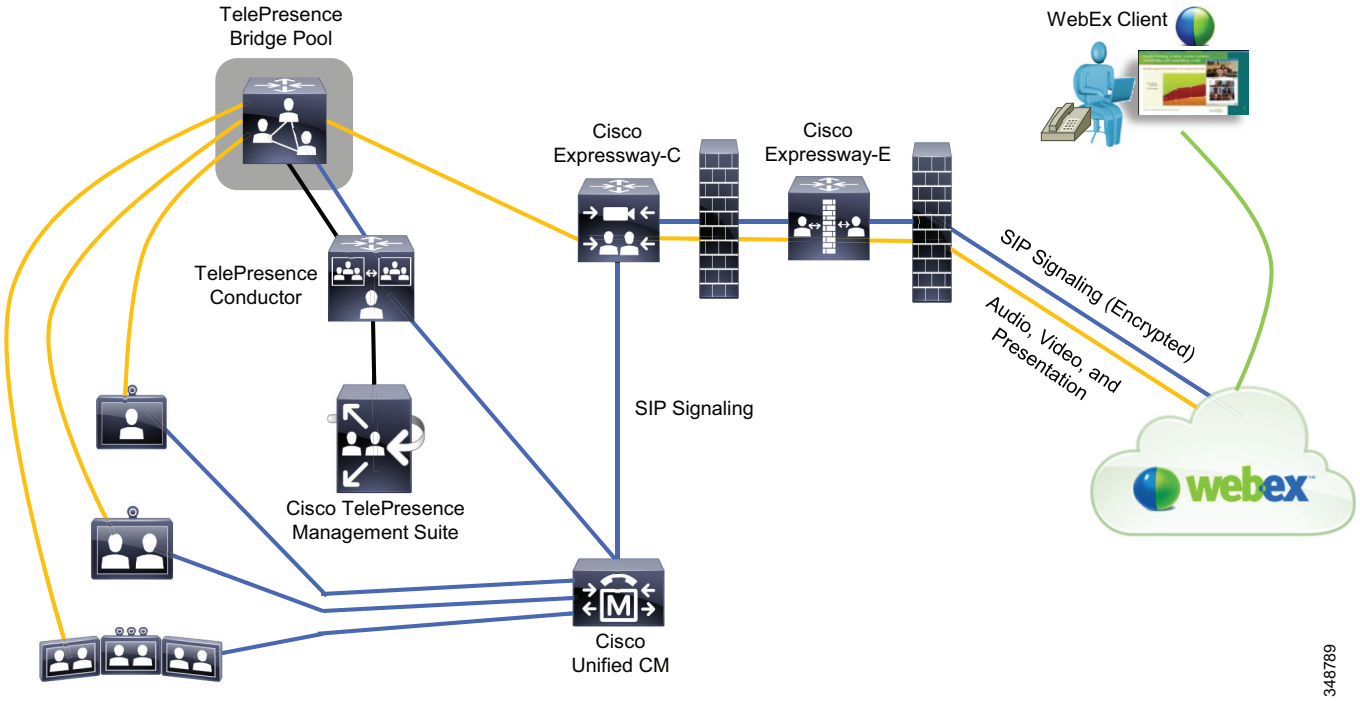
https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

（注） 既存の Cisco VCS の顧客の場合、Cisco Expressway-C および Expressway-E の代わりに Cisco VCS Control と Expressway を使用した導入がサポートされます。

（注） TelePresence Conductor を使用せずに Unified CM と TelePresence Bridge の間でベスト エフォート早期オファー SIP トランクを使用した導入はサポートされていますが、TelePresence Conductor を使用することを推奨します。

Cisco TelePresence Conductor は、TelePresence 会議をホストする TelePresence Bridge をプールから選択します。TelePresence Bridge は、TelePresence エンドポイント参加者からの音声を混合し、混合オーディオ、通話中のスピーカーのビデオ、およびコンテンツ共有ビデオを SIP を使用して WebEx クラウドに送信します。同様に、TelePresence Bridge は、WebEx クラウドからメディア（混合オーディオ、通話中のスピーカーとコンテンツ共有）を受信し、そのオーディオを TelePresence 会議にカスケードし、コンテンツ共有ビデオを TelePresence エンドポイントに送信します。TelePresence Bridge は、通話中のスピーカーが WebEx 側からであると検出した場合、TelePresence エンドポイントを通話中のスピーカーのビデオに切り替えます。通話中のスピーカーが TelePresence 側からの場合、TelePresence Bridge は、前の通話中のスピーカーのビデオを現在の通話中のスピーカーの TelePresence エンドポイントに送信します。

図 11-22　SIP による WebEx 音声を使用した Cisco CMR Hybrid



DMZ では、Cisco Expressway-E は、企業と WebEx クラウド間のトラバーサル コールを処理し、また信号とメディアが内部および外部ファイアウォールを横断するのを許可します。Cisco Expressway-E は、設定された DNS ゾーンを介して WebEx クラウドに接続し、DNS ルックアップを介してコールを WebEx にルーティングします。Cisco Expressway-E は、SIP 信号とメディアについて、TLS およびセキュア RTP を使用した暗号化接続を介して WebEx クラウドと通信します。顧客には、企業内で SIP 信号およびメディア トラフィックの暗号化をオンにするオプションがあります。企業外の TelePresence エンドポイントは、Expressway-C および Expressway-E を介して Unified CM に登録できるため、これらのエンドポイントの参加者は CMR Hybrid 会議に参加できます。

WebEx クラウドが、企業ネットワークから送信されたトラバーサル コールおよびメディアを受信すると、WebEx オーディオ ブリッジは WebEx 会議に音声をカスケードし、WebEx は通話中のスピーカーのビデオに切り替え、WebEx 会議クライアントにコンテンツ共有を表示します。同様に、WebEx クラウドは、Cisco Expressway-E および Expressway-C を介して WebEx 側から企業に、会議混合オーディオ、通話中のスピーカー、およびコンテンツ共有ビデオを送信します。それらは、そこで TelePresence Bridge にルーティングされます。

Cisco CMR Hybrid は、通話中のスピーカーとコンテンツ共有に対して H.264 ビデオをサポートします。また、コンテンツ共有に対して Binary Floor Control Protocol（BFCP）、およびオーディオに対して G.711 コーデックを使用します。Cisco WebEx は H.264 ビデオおよび G.711 オーディオ コーデックを使用しますが、TelePresence は、エンドポイントでサポートされるその他のビデオ形式またはコーデックを使用することもできます。TelePresence Bridge は、TelePresence エンドポイントと WebEx 会議クライアントの間で音声およびビデオの相互運用性を処理します。さらに、TelePresence Bridge と WebEx クラウド間のリンクに対してフロー制御が行われ、メディアの処理に使用可能な帯域幅を調整します。WebEx からのメディアの場合、TelePresence Bridge は、常に 4 Mbps を割り当てて、WebEx が TelePresence ブリッジに可能な最高品質のビデオを送信するようにします。TelePresence Bridge からのメディアの場合、WebEx 会議クライアントでは、通話中のスピーカーのビデオ フロアは 180p で、最小ビット レートは 1.2 Mbps です。ネットワークの状態が原因で最小ビット レートを維持できない場合（重度のパケット損失など）、WebEx クライアントは通話中のスピーカーのビデオの受信を停止しますが、コンテンツ共有および会議の音声は受信し、そのビデオを他の参加者に送信します。WebEx クライアントは定期的に帯域幅の再テストを実行し、ネットワークの状態が安定すると自動的に通話中のスピーカーのビデオを再確立します。WebEx 会議クライアントを実行するデバイスの能力および使用可能な帯域幅に応じて、WebEx クライアントは、最大 HD 720p、30 フレーム/秒（fps）の通話中のスピーカーのビデオ、および最大 1080p のコンテンツ ビデオをサポートします。会議中に、WebEx は、会議内のすべての WebEx クライアントの中で最小能力デバイスに基づいて（ビデオ フロア未満で実行されているデバイスを除く）、最大帯域幅 4 Mbps で帯域幅を割り当てます。ただし、最小能力デバイスが会議を離脱した場合、帯域幅は、WebEx 会議クライアントを実行している次の最小能力デバイスに基づいて再割り当てされます。割り当てられた帯域幅によって、WebEx クライアント上の TelePresence ビデオの表示に使用する解像度とフレーム レートが決まります。導入された TelePresence エンドポイント、必要なビデオ解像度、目的の画面レイアウト、および選択した導入オプションに応じて、顧客は、Cisco TelePresence Server（アプライアンスまたは仮想プラットフォーム）を使用した TelePresence Bridge または Cisco TelePresence MCU を導入できますが、プールは同じタイプのブリッジのみで構成されている必要があります（TelePresence Server または TelePresence MCU のいずれか）。TelePresence Conductor 導入の詳細については、以下のリンク先から入手できる『*Cisco Rich Media Conferencing* chapter of the *Cisco Collaboration System 11.x SRND*』の *Cisco Collaboration Meeting Rooms Premises* に関するセクションを参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/confernc.html

WebEx および TelePresence 参加者は、企業内から、またはインターネット上の任意の場所から CMR Hybrid 会議に参加できます。WebEx 参加者の場合、PSTN または VoIP オーディオのいずれかで WebEx 会議クライアントを使用して会議に参加します。TelePresence 参加者の場合、サポートされるエンドポイントでワンボタン機能（OBTP）または Auto Connect 機能を介するか、または TelePresence Bridge に直接コールすることにより会議に参加します。参加者は、正常に会議に参加すると、エンドポイントおよび会議クライアントからのライブ ビデオを相互に表示できます。WebEx ユーザと共有するプレゼンテーションの場合、ユーザ自身がプレゼンタとなるか、またはプレゼンテーションを共有する前にホストがユーザにプレゼンタ権限を割り当てることができます。この動作を制御する WebEx サイトの設定があります。TelePresence ユーザと共有するプレゼンテーションの場合、ユーザは、自分のコンピュータにビデオ ディスプレイ ケーブルを接続するか、またはエンドポイントのボタンを押して、ホストを経由せずに自分のプレゼンテーションの共有を開始することができます。

（注）　Cisco TMS 14.6 および TMSPE 1.4 以降、Cisco Collaboration Meeting Rooms Premises を Cisco WebEx と統合し、参加者が WebEx 会議クライアントからユーザのパーソナル ルームで会議に参加できるようにすることができます。

スケジューリング

Cisco TelePresence Management Suite（TMS）は、Cisco CMR Hybrid 会議をスケジュールするための主要コンポーネントです。これは、Cisco WebEx 会議スケジューラに制御リンクを提供します。このリンクにより、Cisco TMS は、Cisco WebEx カレンダーに新しい会議を作成すること、また会議参加者に配布される Cisco WebEx 会議情報を取得することができます。CMR Hybrid 会議をスケジュールするときに使用できるオプションを次に示します。

- WebEx Productivity Tools

  WebEx Productivity Tools は、ユーザが WebEx セッションを迅速かつ容易にスケジュールできるようにする一連のツールです。Productivity Tools には Outlook プラグインが含まれており、主催者は、WebEx 会議、TelePresence リソース、および CMR Hybrid 会議をスケジュールできます。生産性ツールで会議を予約するために Cisco TMS とインターフェイスする場合は、Cisco TelePresence Management Suite Extension for Microsoft Exchange（TMSXE）が必要です。このオプションは、CMR Hybrid 会議をスケジュールするユーザ、および電子メール クライアント内ですべての参加者に直接招待を単一トランザクションで送信するユーザに対して、シームレスな統合を提供します。

- Smart Scheduler

  Smart Scheduler は、Cisco TelePresence Management Suite Provisioning Extension（TMSPE）でホストされる Web ベースのツールであり、ユーザはブラウザを使用して CMR Hybrid 会議をスケジュールできるようになります。これにより、モバイル デバイスで会議をスケジュールするユーザにオプションが提供されます。

  （注）　Cisco TMSPE オプション キーがインストールされている場合、Smart Scheduler を使用するのに余分なライセンスは必要ありません。

- WebEx Scheduling Mailbox

  このオプションでは、ネットワーク管理者は Microsoft Exchange Server に特別なメール ボックス アカウントを作成する必要があります。主催者は、CMR Hybrid 会議をスケジュールするときに、招待者リストにこの特別なメール ボックス アカウントを含める必要があります。Cisco TMSXE は、このアカウントをモニタして、受信者リストにこのアカウントがある場合、Cisco TMS に対して CMR Hybrid 会議を予約するよう要求します。このオプションでは、設定の制御は制限されますが、Outlook Web Access（OWA）など、Exchange によってサポートされる任意の電子メール クライアントを使用して、簡単に会議をスケジュールできます。

- Cisco TMS Booking インターフェイス

  このオプションでは、会議主催者は、Cisco TMS ポータルにログインして、Booking インターフェイスから CMR Hybrid 会議をスケジュールする必要があります。このインターフェイスでは、会議の詳細設定を制御します。通常、ヘルプ デスクや IT 担当者がこのオプションを使用して、会議をスケジュールします。

これらのオプションでの Cisco TMS 設定の詳細については、次の Web サイトで入手可能な『*Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide*』を参照してください。

https://www.cisco.com/en/US/products/ps11338/products_installation_and_configuration_guides_list.html

CMR Hybrid 会議のスケジューリングは 2 段階のプロセスです。最初に、WebEx カレンダーで会議をスケジュールするための要求が WebEx クラウドに送信され、WebEx クラウドが Cisco TMS に渡される会議の詳細で応答します。2 番目に、Cisco TMS が、そのカレンダーに TelePresence 会議をスケジュールします。会議の開始時間になると、Cisco TMS は TelePresence Bridge に WebEx 上の会議に参加するための会議の詳細を提示します。WebEx から返される会議の詳細には、会議の日時、ダイヤルイン情報、件名、会議番号、会議に参加するための URL などが含まれます。会議がスケジュールされると、会議の WebEx および TelePresence の部分の詳細がホストに送信され、ホストはすべての参加者に詳細を転送できます。ただし、生産性ツールを使用する場合、会議の詳細は、ホストが作成して会議の参加者に送信する招待に自動的に含まれます。

シングル サインオン

Cisco CMR Hybrid は、シングル サインオン（SSO）を使用して、Cisco TMS 内の会議の WebEx 部分のスケジュールをサポートします。この機能では、WebEx サイトで、Cisco TMS が委任パートナーとしてプロビジョニングされており、またパートナー委任認証が設定されている必要があります。Cisco TMS で SSO が有効になっている場合、ユーザの WebEx ユーザ名のみ、WebEx パスワードを必要とすることなく Cisco TMS ユーザ プロファイルに保存されます。ユーザが CMR Hybrid 会議をスケジュールすると、WebEx は Cisco TMS を信頼し、WebEx カレンダーで会議をスケジュールするためには、Cisco TMS に保存されている WebEx ユーザ名だけが必要です。SSO での Cisco TMS 設定の詳細については、以下のリンク先から入手できる最新バージョンの『*Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide*』を参照してください。

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-and-configuration-guides-list.html

Cisco WebEx での SSO の詳細については、次の URL にあるホワイト ペーパーおよびテクニカル ノートを参照してください。

https://developer.cisco.com/site/webex-developer/develop-test/sso/reference

セキュリティ

企業ネットワークと WebEx クラウドの間の通信はすべて暗号化されます（TLS およびセキュア RTP を使用）。また、顧客には、企業内で SIP 信号およびメディアの暗号化をオンにするオプションがあります。TLS 接続が機能するためには、証明書を Cisco Expressway-E にアップロードして、適切なハンドシェイクが行われるようにする必要があります。その証明書は、信頼できるルート認証局によって署名される必要があります。信頼できるルート認証局のリストについては、次のページで入手可能な『*Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide*』を参照してください。

https://www.cisco.com/en/US/products/ps11338/products_installation_and_configuration_guides_list.html

会議に参加するために TelePresence Bridge が WebEx にコールする場合、パスワードが必要です。パスワードは、WebEx カレンダーでスケジュールされた各 CMR Hybrid 会議に割り当てられ、WebEx クラウドから会議の詳細の一部として返される SIP URI に組み込まれます。このパスワードは 22 バイトに符号化され、セキュリティ基準を満たしています。会議の開始時に、TelePresence Bridge がこの SIP URI を使用して WebEx にコールし、WebEx がパスワードを検証してコールが会議に参加するのを許可します。

導入オプション

CMR Hybrid 会議の開始時間になると、Cisco TMS は、TelePresence 参加者に対して TelePresence Conductor を介して TelePresence Bridge で会議を開始します。TelePresence Bridge は、スケジュール プロセスの一部として返された、WebEx 側で会議に参加するための SIP URI を使用して、WebEx クラウドに対して TelePresence Conductor を介した SIP コールを行います。その結果、TelePresence Bridge は、会議用のクラウドと、オーディオ、通話中のスピーカー ビデオ、およびコンテンツ共有ビデオの個別ストリームを確立します。通話中のスピーカーのビデオ、コンテンツ共有のビデオ、会議制御は常に IP ネットワークを介して送信されますが、オーディオは、選択した導入オプションに応じて IP ネットワークまたは PSTN を介して送信できます。CMR Hybrid では、次の各種オーディオ オプションを利用できます。

- SIP を使用した WebEx Audio（11-59 ページ）（Cloud Connected Audio を含む）
- PSTN を使用した WebEx Audio（11-59 ページ）
- Teleconferencing Service Provider Audio（11-60 ページ）

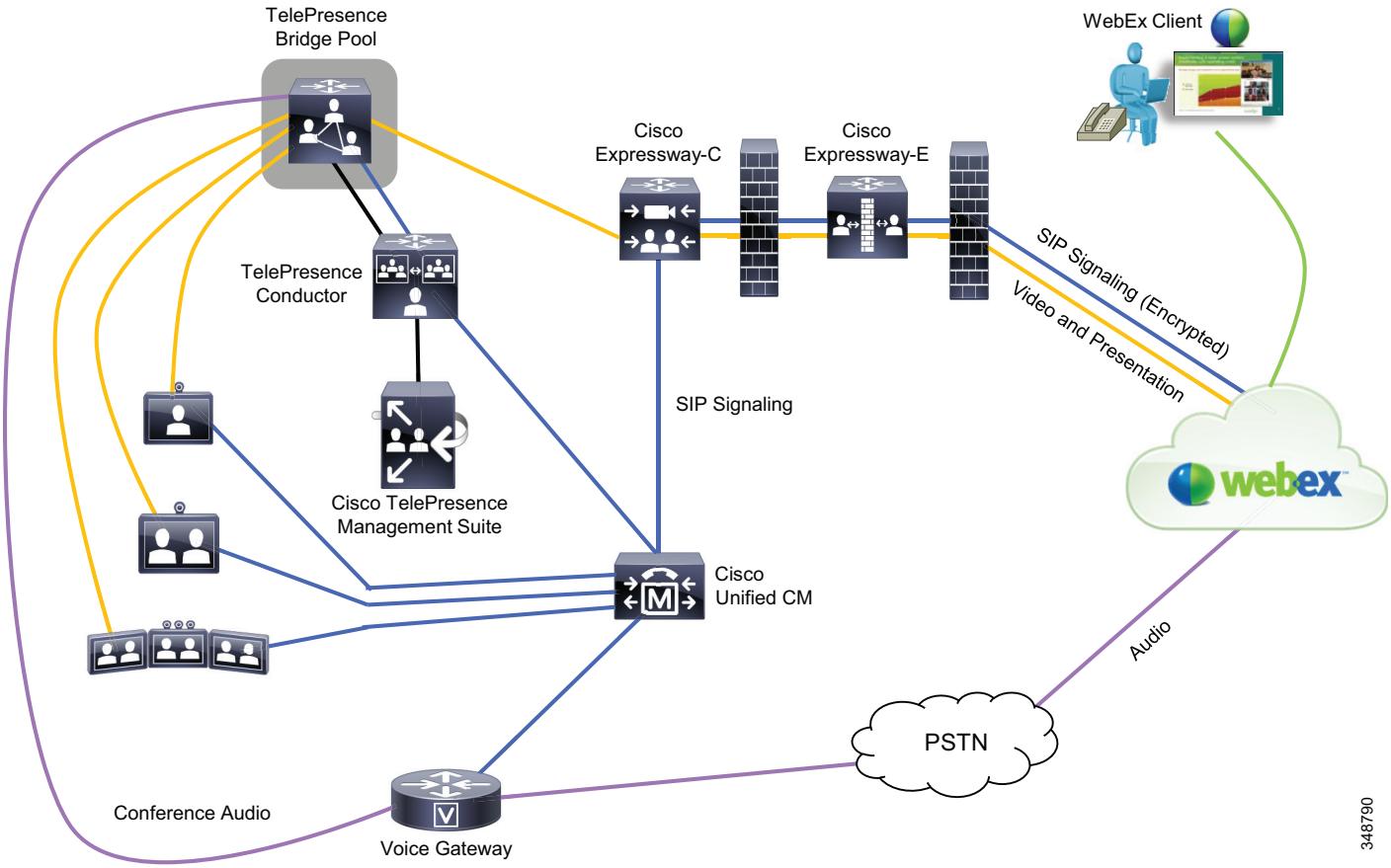
SIP を使用した WebEx Audio

図 11-22 は、SIP での WebEx Audio を使用した Cisco CMR Hybrid の導入を示しています。このオプションでは、会議の開始時に TelePresence Bridge が WebEx にクラウドにコールしたときに、会議の音声が WebEx オーディオ ブリッジで SIP 接続を介して確立されます。音声、通話中のスピーカーのビデオ、コンテンツ共有ビデオ、および会議制御は、Cisco Expressway-C および Expressway-E を介して TelePresence Bridge から WebEx クラウドに IP ネットワークで送信されます。その結果、TelePresence Bridge からの音声接続は WebEx オーディオ ブリッジにカスケードされます。

PSTN を使用した WebEx Audio

国内ルールでトール バイパスが許可されない Cisco CMR Hybrid 導入では、PSTN を使用した WebEx Audio はオプションです。図 11-23 は、この導入を示しています。このオプションでは、通話中のスピーカーのビデオ、コンテンツ共有ビデオ、および会議制御は IP ネットワークを介して送信されますが、音声は PSTN を通して WebEx オーディオ ブリッジで確立されます。このオプションでは、IP ネットワークと PSTN 間で音声コールを接続するために、音声ゲートウェイの導入が必要です。スケジューリング プロセスで、WebEx カレンダーで会議をスケジュールするときに、WebEx は Cisco TMS にダイヤルアウト番号と会議番号を渡します。会議の開始時に、TelePresence Bridge は、WebEx クラウドへの SIP コールを開始して通話中のスピーカーのビデオおよびコンテンツ共有ビデオを確立します。同時に、TelePresence Bridge は、PSTN 経由でダイヤルアウトして WebEx オーディオ ブリッジとの音声接続を確立します。WebEx オーディオ ブリッジと接続した後、TelePresence Bridge は、会議番号を DTMF ダイヤル シーケンスとして送信して、WebEx が音声およびビデオ コール レッグを関連付けられるようにします。その結果、TelePresence Bridge からの音声接続は WebEx オーディオ ブリッジにカスケードします。

図 11-23　PSTN で WebEx Audio を使用した Cisco CMR Hybrid

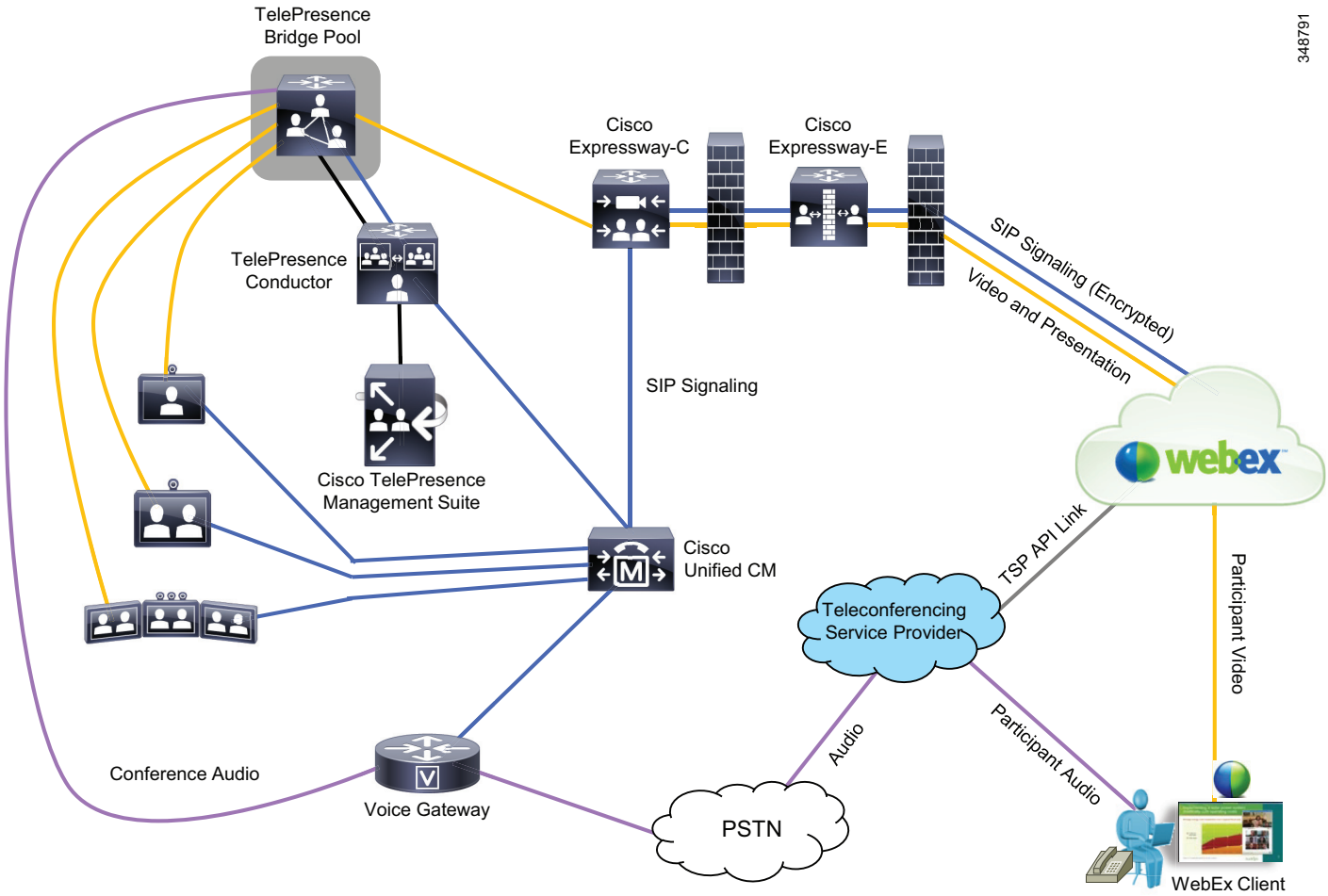


WebEx から返されるダイヤル アウト番号は、完全な E.164 番号形式です（例：+14085551212）。Cisco Unified CM のダイヤル プランの設計では、E.164 番号の処理を考慮に入れる必要があります。Cisco Unified CM でのダイヤル プランの設計については、ダイヤル プラン（14-1 ページ）の章を参照してください。

Teleconferencing Service Provider Audio

Teleconferencing Service Provider（TSP）Audio オプションは、サードパーティの電話会議サービス プロバイダーがホストするオーディオ ブリッジの使用を希望する顧客用です。TSP Audio 設定は、PSTN 設定を使用する WebEx 音声と非常によく似ていますが、オーディオ ブリッジは電話会議サービス プロバイダーによってホストされる点が異なります（図 11-24 を参照）。WebEx と TSP 間の TSP リンクは、高度な会議制御機能を提供します。

図 11-24　Teleconferencing Service Provider（TSP）Audio を使用した Cisco CMR Hybrid



スケジューリング プロセスでは、ダイヤルアウト番号と会議番号に加えて、TSP オーディオ ブリッジに対する IVR プロンプトを通してナビゲートするための追加の番号が、WebEx から Cisco TMS に渡されます。スケジュール済み会議の開始時に、TelePresence Bridge は WebEx クラウドへの SIP コールを開始してビデオ接続を確立します。同時に、TelePresence Bridge は PSTN 経由で TSP オーディオ ブリッジにダイヤルアウトします。次に、TelePresence Bridge は、DTMF 桁を付加した会議番号を DTMF ダイヤル シーケンスとして再生し、オーディオ ブリッジの IVR をナビゲートして会議を開始します。WebEx 側では、WebEx 参加者が会議クライアントを使用して WebEx セッションを開始し、TSP オーディオ ブリッジにダイヤルするか、オーディオ ブリッジからのコールバックを受けます。このため、TelePresence および WebEx の参加者からのオーディオ ストリームがカスケードされます。この時点より先では、WebEx 側の最も声が大きなスピーカーや参加者リストなどに関する情報が、TSP から WebEx に TSP リンクを通して渡され、その後エンタープライズ コラボレーション ネットワークに渡されます。

WebEx から返されるダイヤル アウト番号は、完全な E.164 番号形式です（例：+14085551212）。Cisco Unified CM のダイヤル プランの設計では、E.164 番号の処理を考慮に入れる必要があります。Cisco Unified CM でのダイヤル プランの設計については、ダイヤル プラン（14-1 ページ）の章を参照してください。

ハイ アベイラビリティ

CMR Hybrid のハイ アベイラビリティの設計では、検討すべき 2 つの領域として、エンタープライズ コラボレーション ネットワークと WebEx クラウドがあります。WebEx クラウドはシスコによって管理されており、すでに冗長性がインフラストラクチャに組み込まれています。詳細については、Cisco WebEx Software as a Service（11-28 ページ）の項を参照してください。

エンタープライズ コラボレーション ネットワークでは、Cisco Unified CM および Cisco Expressway のクラスタリング オプションを使用して、TelePresence エンドポイントでの呼制御およびコール ルーティングに冗長性を提供します。プライマリ サーバで障害が発生すると、バックアップ サーバは呼制御およびコール ルーティング機能を引き継ぐことができます。さらに、カンファレンス ブリッジの障害を処理するために、TelePresence 会議インフラストラクチャの復元力を考慮する必要があります。

Cisco Unified CM クラスタリングについては、呼処理（9-1 ページ）の章を参照してください。

Cisco Expressway クラスタリングについては、次の Web サイトで入手可能な『*Cisco Expressway Cluster Creation and Maintenance Deployment Guide*』の最新バージョンを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

TelePresence 会議インフラストラクチャの復元力については、Cisco Meeting Server（11-7 ページ）の項を参照してください。

キャパシティ プランニング

WebEx クラウドには、しきい値を超えた場合にトラフィックを均等に分散して動的に容量を追加する機能が組み込まれています。Cisco CMR Hybrid のキャパシティ プランニングには、企業内で稼働するコンポーネントのサイジングが含まれます。コンポーネントには、以下が含まれます。

- 呼処理プラットフォーム

  Cisco Unified CM は、TelePresence エンドポイントで生成されたトラフィックを処理するのに十分なリソースを提供する必要があります。詳細については、コラボレーション エンドポイントのキャパシティ プランニング（8-48 ページ）の項を参照してください。

- TelePresence 会議

  Cisco TelePresence Conductor、Cisco TelePresence Server、または Cisco TelePresence MCU は、会議トラフィックを処理するのに十分なリソースを提供する必要があります。キャパシティ プランの詳細については、以下のリンク先から入手できる『*Cisco Collaboration System 11.x SRND*』の「*Cisco Rich Media Conferencing*」の章の *Cisco Collaboration Meeting Rooms Premises* に関するセクションを参照してください。

  https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/confernc.html

- Cisco Expressway

  Cisco Expressway は、導入環境のトラバーサル コール トラフィックを処理するのに十分なリソースを提供する必要があります。キャパシティの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

ネットワーク トラフィック プランニング

Cisco CMR Hybrid のネットワーク トラフィック プランニングは、以下の要素で構成されます。

- WebEx クライアントの帯域幅

  WebEx 会議クライアントは、Scalable Video Coding（SVC）テクノロジーを使用してビデオを送受信します。これは、多層フレームを使用してビデオを送信し、受信側クライアントが自動的に最適な解像度を選択してビデオを受信できるようにします。WebEx クライアントのネットワーク トラフィック プランニングの詳細については、次の Web サイトで入手可能なホワイトペーパー『*Cisco WebEx Network Bandwidth*』を参照してください。

  https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white_paper_c11-691351.html

- 企業から WebEx クラウドへの帯域幅

  WebEx クラウドへの各コールでは、企業と WebEx クラウド間で 1.1 Mbps 以上のネットワーク帯域幅が必要です。たとえば、顧客が 5 つの同時 CMR Hybrid 会議を想定している場合、5.5 Mbps のネットワーク帯域幅が必要です。同時に、コールごとに最大 4 Mbps の帯域幅がサポートされます。

TelePresence Bridge と WebEx クラウド間で最適な SIP 音声およびビデオの品質を提供するため、シスコは、Cisco Unified CM に登録する各エンドポイントに関連付けられた領域で少なくとも 1.3 Mbps のビデオ帯域幅を設定するよう推奨しています。

設計上の考慮事項

Cisco CMR Hybrid の導入には、次の設計上の考慮事項が適用されます。

- Cisco TelePresence MultiPoint Switch インフラストラクチャを使用する、以前のバージョンの CMR Hybrid からのアップグレードはサポートされておらず、これらの以前のバージョンを使用するカスタマーは移行を計画する必要があります。
- CMR Hybrid 会議をスケジュールするすべてのユーザは、WebEx サイトで Cisco TelePresence セッション タイプのホスト アカウントが割り当てられている必要があります。
- Cisco Unified CM に登録でき、TelePresence Bridge でサポートされる任意のエンドポイントを使用して、Cisco CMR Hybrid 会議に参加できます。
- Cisco TelePresence Management Suite（TMS）によって管理されているデバイスのみ、ワンボタン機能（OBTP）または Auto Connect 機能を使用して CMR Hybrid 会議に参加できます。
- Cisco Expressway-C 内の Cisco Unified CM ネイバー ゾーンが、Binary Floor Control Protocol（BFCP）を有効にして設定されていることを確認します。
- TelePresence Bridge に対して SIP 音声、および WebEx 参加者に対して PSTN オーディオを使用できるように、WebEx サイト内のハイブリッド オーディオをプロビジョニングします。
- Cisco CMR Hybrid は Cisco WebEx Meetings Server をサポートしていません。
- CMR Hybrid 会議に参加するときにホストが存在しない場合は TelePresence Bridge がデフォルトのホストになり、ホストが WebEx 会議クライアントを使用して参加すると、そのホストにホスト権限が再割り当てされます。
- TelePresence または WebEx 参加者がまだ参加していない場合であっても、TelePresence Bridge は、会議の開始時に WebEx クラウドにコールします。

- 主催者の WebEx アカウントと Outlook のタイム ゾーンが一致する必要があります。一致しない場合、WebEx と Cisco TMS カレンダーでスケジュール済み会議で、開始時刻が異なります。
- ビデオ エクスペリエンスを最適にするために、ファイアウォールでメディア ストリーミングに対して UDP を有効にします。

PART 2

呼制御およびルーティング

このパートの内容

マニュアルのこのパートに含まれる章は、次のとおりです。

呼制御およびルーティングの概要

改訂日:2015 年 6 月 15 日

ネットワーク インフラストラクチャが Cisco Unified Communications および Collaboration システムに配置されると、呼制御およびルーティングのアプリケーション、コンポーネント、およびサービスをネットワーク インフラストラクチャの最上位で階層化できるようになります。ネットワーク インフラストラクチャ上に配置できる、また場合によっては配置する必要があるアプリケーションと機能は、数多く存在します。

- 帯域幅管理:所定の時間にネットワーク上で許可するコール数を制限することで、音声およびビデオ品質を保証してネットワーク帯域幅のオーバーサブスクリプションを回避するメカニズムを提供します。パケット マーキングと再マーキングの組み合わせ、および低遅延やプライオリティ キューイングなどの高度なキューイング メカニズムによって、音声およびビデオ品質が保証されます。同様に、コール アドミッション制御は、呼処理コンポーネントおよび使用可能なネットワーク帯域幅の総合的なコール キャパシティを確保します。
- ダイヤル プラン:ユーザが行うことができるコールのタイプを制限するために、エンドポイントの番号、ダイヤルされる番号の分析、および制限クラスを提供します。
- 緊急サービス:発信者が迅速な応答と必要なヘルプを受け取ることができるように(警察、消防、救急チームなど)、適切な Public Safety Answering Point(PSAP)に発信者のロケーションおよび緊急状態に関して重要な情報を提供します。
- ディレクトリ サービスおよびアイデンティティ管理サービス:Lightweight Directory Access Protocol(LDAP)はディレクトリに保存されている情報にアクセスし、変更するための標準方式をアプリケーションに提供します。同様に、アイデンティティ管理とシングル サインオンによってユーザ識別およびアクセスの安全性が保証されます。これらの機能により、企業は、すべてのユーザ情報を、複数のアプリケーションで利用できる単一リポジトリに集中化させることができます。追加、移動、および変更が簡単なので、情報へのアクセスが向上し、保守コストが削減されます。

本 SRND のこの章では、上記の機能、コンポーネント、およびサービスについて説明します。各章では、コンポーネントまたはサービスの概要を示したあと、アーキテクチャ、ハイ アベイラビリティ、および設計上の考慮事項について説明します。各章では、アプリケーションおよびサービスの設計関連の側面を中心に説明します。製品固有のサポートおよび設定情報については、関連する製品マニュアルを参照してください。

SRND のこの部分に含まれる章は、次のとおりです。

- 帯域幅管理（13-1 ページ）

  この章では、帯域幅管理方法と、コールの音声およびビデオ品質が許容できなくなる原因となる、IP リンクの潜在的なオーバーサブスクリプションについて説明します。また、オーバーサブスクリプションを回避するために、所定の時間にネットワーク上で特定の数の同時コールだけを許可するためのコール アドミッション制御の使用についても説明します。この章では、Quality of Service（QoS）およびコール アドミッション制御タイプ（ロケーションベースのコール アドミッション制御など）、さらに QoS とアドミッション制御サービスを適切に配置するための設計と配置のガイドラインについて説明します。

- ダイヤル プラン（14-1 ページ）

  この章では、呼処理アプリケーションがコールを適切な宛先にルーティングできるようにする、ダイヤル プランの機能と機能性について説明します。この章では、ダイヤル プラン サービスのさまざまな側面（ダイヤル プラン構成要素、ダイヤル プラン番号オプションと設計上の考慮事項、制限クラス、着信コールと発信コールの機能、ダイヤル プランとコール ルーティング冗長メカニズムなど）について検討します。

- 緊急サービス（15-1 ページ）

  この章では、企業の IP コミュニケーション環境から PSTN 上の Public Safety Answering Point（PSAP）を介して緊急サービスにアクセスする方法について説明します。この内容は、医療、火災、およびその他の緊急応答サービスが重要なニーズとなる可能性があるため、ほとんどの配置において重要となります。この章では、企業の内外におけるさまざまな緊急サービス コンポーネントの概要について説明します。また、立案、911 ネットワーク サービス プロバイダー、ゲートウェイ インターフェイス、および番号とロケーションのマッピングについても説明します。

- ディレクトリ統合とアイデンティティ管理（16-1 ページ）

  この章では、Cisco Unified Communications Manager のディレクトリ アーキテクチャ自体や LDAP の同期化および認証に関する設計上の考慮事項など、Unified Communications および Collaboration と LDAP ディレクトリとの統合について説明します。Unified Communications および Collaboration エンドポイントからのディレクトリ アクセス、およびシングル サインオンなどのセキュリティ上の考慮事項についても説明します。

アーキテクチャ

コール ルーティング コンポーネントとサービス（呼処理エージェント、IP ゲートウェイと PSTN ゲートウェイなど）は、基盤となるネットワーク インフラストラクチャを使用して、ネットワークに接続およびアクセスします。コール ルーティングのコンポーネントおよび機能は、基盤となるネットワーク インフラストラクチャに接続することで、エンドツーエンドのネットワーク接続および Quality of Service を利用して、企業ネットワークと公衆電話網の両方にアクセスできます。一方、コール ルーティングのアプリケーションとサービスは、基本的な Unified Communications および Collaboration 機能（呼制御、ダイヤル プラン、コール アドミッション制御、ゲートウェイ サービスなど）を配置内のその他のアプリケーションとサービスに提供します。たとえば、Unified CM クラスタは、スイッチを介して IP ネットワークに接続し、ネットワーク内のその他のデバイスおよびアプリケーションと通信する以外に、その他のロケーション内のその他のデバイスおよびサービスにアクセスします。同時に、Unified CM クラスタは、IP Phone などの呼制御コンポーネントとサービスに対して、電話登録、メディア リソースのプロビジョニングと割り当てなどのサービスを提供します。

また、コール ルーティング コンポーネントがネットワーク インフラストラクチャに依存してネットワーク接続を行っているのと同様、コール ルーティングのコンポーネントとサービスも、多くの場合、完全に機能するために相互依存しています。たとえば、Unified CM は、ネットワーク内のさまざまな IP エンドポイントに登録サービスおよびコール ルーティング サービスを提供する一方で、企業の外側にコールをルーティングするために、ゲートウェイおよびゲートウェイ サービスに完全に依存しています。

ハイ アベイラビリティ

ネットワーク インフラストラクチャの場合と同様に、重要な Unified Communications および Collaboration コール ルーティング サービスでは、ネットワークまたは個々のコール ルーティング コンポーネントで障害が発生した場合でも必要な機能を引き続き使用できるように、ハイ アベイラビリティを実現する必要があります。発生する可能性のあるさまざまなタイプの障害、およびこれらの障害に関する設計上の考慮事項を理解することが重要となります。Unified CM クラスタリング メカニズムには冗長な性質が備えられているため、単一のサーバまたはコンポーネント（Unified CM クラスタのサブスクライバ ノードなど）に障害が発生しても、その影響がほとんどまたはまったくない場合があります。ただし、その他の場合には、単一の障害が複数のコンポーネントまたはサービスに影響を及ぼすことがあります。たとえば、PSTN ゲートウェイまたは IP ゲートウェイの障害によって、公衆電話網にアクセスできなくなる可能性があります。また、Unified CM など呼処理エージェントが引き続き使用可能で、ほとんどの機能とサービスを提供できる場合でも、ゲートウェイに障害が発生してパスを使用できなくなると、コールを PSTN にルーティングできません。このようなタイプの状況を回避するためには、複数の PSTN ゲートウェイを配置して、冗長なゲートウェイ サービスを提供し、コール ルーティングを必要に応じて両方のゲートウェイで処理できるように、呼処理エージェントを設定する必要があります。

ダイヤル プランや帯域幅管理などの機能とサービスの場合、ハイ アベイラビリティに関する考慮事項には、ネットワーク接続または呼処理エージェント アプリケーション サーバの障害によって機能が一時的に失われ、コール エージェントがコールをルーティングできなくなり、これにより、発信者がコールを発信できなくなることが含まれます。また、QoS などのコール アドミッション制御サービスが、コールを開始するエンドポイントで使用できない場合は、ネットワークのオーバーサブスクリプションが発生することもあります。たとえば、コール アドミッション制御エージェントに障害またはネットワークへの接続の切断が発生すると、コールは依然として通過できますが、コール アドミッション制御サービスではそのコールが認識されないため、品質が低下する可能性があります。このようなタイプのシナリオを回避するには、複数のコール アドミッション制御エージェントを配置することにより、コール アドミッション制御の復元性を提供します。

また、ハイ アベイラビリティの考慮事項は、ビデオ エンドポイントやリモート サイトのサバイバビリティなどのコンポーネントとサービスに関する考慮事項でもあります。デバイスが中央サイトのエージェントから呼処理サービスを利用する、ネットワーク接続リモート サイトが含まれた配置の場合、たとえば、SRST を使用するリモート サイトのサバイバビリティによって、中央サイトへの接続が切断された場合でも、リモート サイト内のローカル電話機が引き続き呼処理サービスを受信するようにできます。同様に、ビデオ エンドポイントのハイ アベイラビリティを確保するために、複数のマルチポイント コントロール ユニット（MCU）を配置して、いずれかに障害が発生した場合に備えることができます。

キャパシティ プランニング

ネットワーク インフラストラクチャは、個々のコンポーネントおよびシステム全体のキャパシティとスケーラビリティを考慮して設計および配置する必要があります。同様に、コール ルーティング コンポーネントとサービスの配置についても、キャパシティとスケーラビリティを考慮して設計する必要があります。さまざまなコール ルーティング アプリケーションとサービスを配置する場合、それらのアプリケーションとサービス自体のスケーラビリティの考慮が重要となるだけでなく、基盤となるネットワーク インフラストラクチャのスケーラビリティを考慮する必要があります。ネットワーク インフラストラクチャは、使用可能な帯域幅を持ち、コール ルーティング コンポーネントによって発生する追加のトラフィック負荷を処理できる必要があります。同様に、コール ルーティング インフラストラクチャおよびそのコンポーネントは、必要なすべてのデバイス設定と登録以外に、コール負荷または最繁時呼数（BHCA）を処理できる必要があります。

たとえば、Unified CM などの呼処理エージェントの場合は、ユーザ数、エンドポイント数、および時間あたりのユーザごとのコール数という観点で配置のサイズを評価し、必要な負荷を処理するために十分なリソースを配置することが重要です。呼処理エージェントのサイズが小さく、十分なリソースがない場合は、負荷の増加に伴い、機能とサービスが失敗するようになります。呼処理の配置のサイズを設定する場合の 2 つの主な考慮事項は、呼処理タイプと呼処理ハードウェアです。これらは両方とも、ユーザ、ロケーション、デバイスなどの数を考慮して、システムのサイジングを適切に設定するために重要です。例として、Cisco Unified Communications Manager は、Cisco Unified Communications Manager Express よりもキャパシティが大幅に高いため、大規模な配置への使用に適しています。また、呼処理エージェントを実行するために選択されたサーバ プラットフォームによって、多くの場合、最大の負荷が決まります。

リモート サイトのサバイバビリティのためのキャパシティ プランニングは、バックアップ呼処理ハードウェアに依存するという点で、ほとんど同じです。バックアップまたは存続可能な呼処理サービスを提供するために、適切な Cisco IOS プラットフォームを選択する場合は、通常、中央サイトへの接続が切断されたときにそのサイトでサポートする必要があるデバイスとユーザの数を決定することから開始します。このサイジングで同等に重要となるのは、ローカル PSTN ゲートウェイ サービスです。中央サイトへの接続が切断された場合、ローカル PSTN ゲートウェイには、最も忙しい時間に、すべてのコールをブロックされることなくルーティングできる十分な回線がありますか。これに対する回答がいいえである場合、呼処理をバックアップできるようにリモート サイトを適切にサイジングするには、ゲートウェイまたはトランクを追加する必要があります。

PSTN ゲートウェイと IP ゲートウェイについても、配置のサイズを適切に設定して、最も忙しい時間におけるすべてのコールを処理するために、十分なキャパシティを使用できるようにする必要があります。場合によっては、十分なリソースを提供するために、複数の PSTN ゲートウェイまたは IP ゲートウェイを配置する必要がある場合があります。

QoS およびコール アドミッション制御サービスの設定とサイジングを行う場合は、必要なコール数をサポートするために、ネットワーク接続上およびプライオリティ キューで十分な帯域幅を使用できるようにしてください。十分な帯域幅を使用できない場合、追加のネットワーク キャパシティ、ゲートウェイ、および IP トランクまたはテレフォニー トランクが必要となる場合があります。

ダイヤル プラン サービスのサイジングも重要となります。ただし、多くの場合、エンドポイントや電話番号の数、ルート パターン、またはその他のダイヤル プラン構成要素の観点からのダイヤル プラン キャパシティは、使用される呼処理エージェントおよびプラットフォームに完全に依存します。

ビデオ テレフォニーなどのコンポーネントおよびサービスの場合、適切なサイジングが同様に重要となります。ビデオ テレフォニーのキャパシティ プランニングに関する考慮事項では、主に、ネットワークの帯域幅、使用可能なビデオ ポート、および MCU セッションが重要となります。基盤となるネットワーク インフラストラクチャが追加の負荷を処理できると想定すると、ほとんどの場合、アプリケーション サーバおよび MCU を増やしたり、サーバまたは MCU ハードウェアを大容量モデルにアップグレードしたりすることで、キャパシティを追加できます。

システム サイジング、キャパシティ プランニング、およびサイジングに関連する配置上の考慮事項の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

帯域幅管理

改訂日：2018 年 3 月 1 日

帯域幅管理とは、コラボレーション ソリューション内の音声とビデオ対応エンドポイント、クライアント、およびアプリケーションのすべてで、エンドツーエンドの最高のユーザ エクスペリエンスを実現することです。この章では帯域幅管理の包括的なアプローチについて説明します。帯域幅管理では、エンドツーエンドのサービス品質（QoS）アーキテクチャ、コール アドミッション制御、ビデオ レート アダプテーション、復元力メカニズムを導入し、マネージドおよびアンマネージド ネットワークでパーベイシブ ビデオを展開する際に最高のユーザ エクスペリエンスを実現します。

始めに、コラボレーション メディアの説明、音声とビデオの違い、ネットワークに与える影響について説明します。次に、信頼されているエンドポイントと信頼されていないエンドポイント、クライアント、アプリケーションのコラボレーション メディアとシグナリングを識別および分類する方法について説明し、コラボレーションのエンドツーエンドの QoS アーキテクチャについても説明します。WAN キューイングとスケジューリングの戦略、帯域幅のプロビジョニングとアドミッション制御についても解説します。

（注） ネットワーク インフラストラクチャ（3-1 ページ）の章では、LAN および WAN の QoS の基礎について説明します。この章を確認し、その概念について十分理解することが重要です。この章は、それらの概念を理解していることを前提としています。

この章の変更点

表 13-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

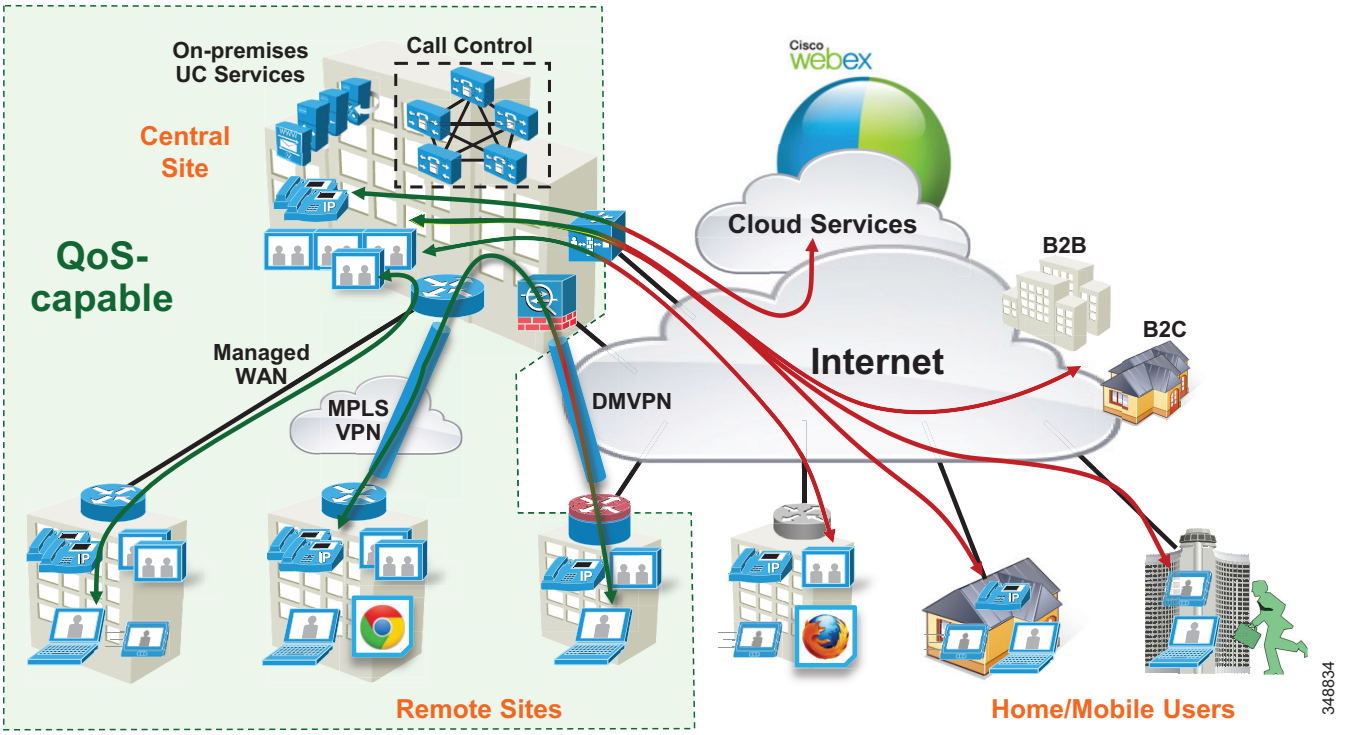
表 13-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
QoS ポリシーの一致と DSCP 再マーキング	信頼されているエンドポイント（13-100 ページ）	2018 年 3 月 1 日
その他の小さな修正および更新	この章の各項で説明	2018 年 3 月 1 日

はじめに

コラボレーション環境は絶えず進化し、アプリケーションとネットワークの 2 つの領域が大きく変化しています。Unified Communications が初めて導入されたときは、メディアが通過するネットワーク全体で管理者がサービス品質（QoS）を実装できる、完全なマネージド ネットワークに接続されている IP Phone とルーム システム エンドポイントなど、主に固定ハードウェア エンドポイントから構成されていました。時間の経過に合わせて、インターネットと WebEx などのクラウドベース サービスを使用できるようになり、コラボレーション インフラストラクチャの一部はマネージド ネットワーク外およびクラウド内に配置できるようになりました。また、オフィス接続オプションも進化しています。企業は、Cisco Expressway 経由で直接接続されたインターネット、または Dynamic Multipoint VPN（DMVPN）などの技術を経由したインターネット上のリモート サイトとモバイル ユーザを相互接続しています。図 13-1では、クラウド サービスを使用するマネージド（QoS 対応）ネットワーク内の従来のオンプレミス コラボレーション ソリューションと、インターネットなどのアンマネージド（QoS 非対応）ネットワーク上に配置されたサイトをまとめています。オンプレミス リモート サイトは、管理者が QoS でコラボレーション メディアとシグナリングの優先順位を設定できる MPLS マネージド ネットワークを経由して接続されます。他のリモート サイトとブランチは、コラボレーション メディアとシグナリングの優先順位を設定できるまたはサイトからの発信に対してのみ優先順位を設定できる場合、インターネットを経由して企業に接続します。また、多くのさまざまなモバイル ワーカーおよびテレワーカーも、インターネットを経由してオンプレミス ソリューションに接続します。そのため、企業、リモート サイト、家庭、モバイル ユーザ、他のビジネス、消費者を結ぶソースとしてインターネットは普及し、帯域幅管理およびユーザ エクスペリエンスに大きな影響を与えています。

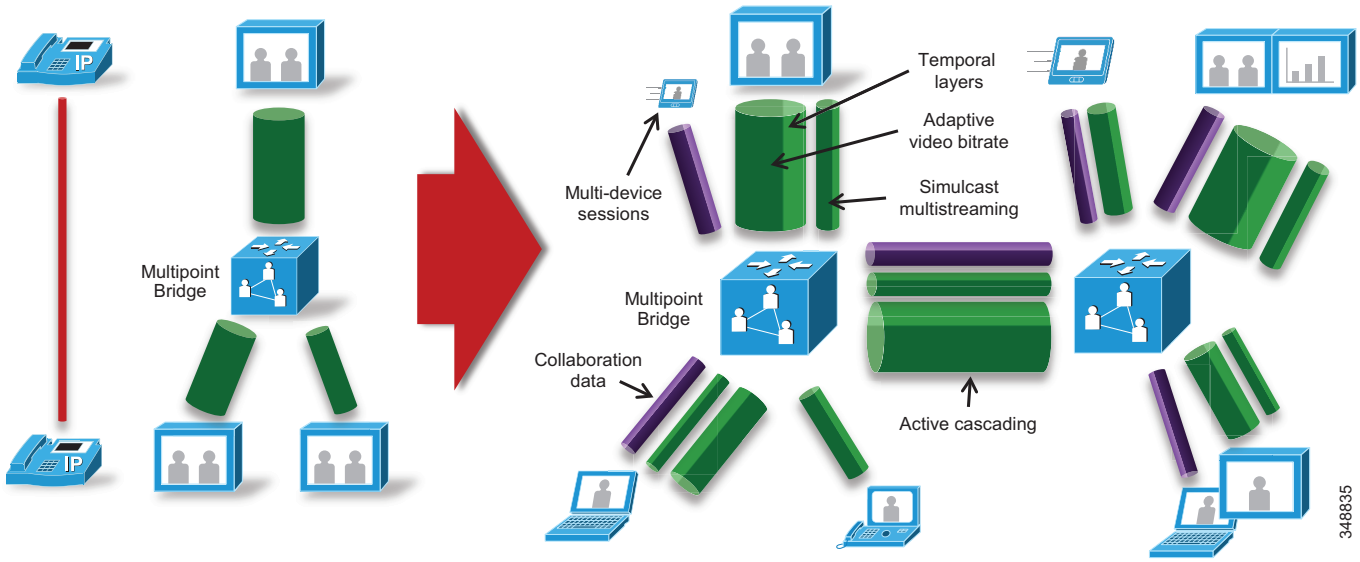
図 13-1　　マネージド ネットワークとアンマネージド ネットワーク



新しい技術および動向とは、エンドポイントとユーザ エクスペリエンスの進化、大量のコラボレーション デバイスとオプションを意味しています。企業は、ハウジングの単一目的型シングル メディア通信デバイスから多目的型マルチメディア オプションに移行しています。これは、Bring Your Own Device（BYOD）などの動向にも明確に表れています。ユーザは会社に自分の高性能なコンパクト モバイル デバイスを持ち込み、インスタント メッセージ、ビデオ コラボレーション、会議機能、デスクトップ共有機能などのコラボレーション技術を業務プロセスに導入しているため、業務プロセスの協調性と効率性が改善されています。

コラボレーション メディアは、固定シングル ストリームで固定ビット レートの音声とビデオ ストリームに接続したポイントツーポイントまたはマルチポイント ブリッジから、さまざまなデバイスと相互接続するマルチポイント ブリッジ全体でカスケードされたマルチレイヤで適応型ビット レートのビデオ セッションに大幅に進化しました。図 13-2 はこの進化を示しています。

図 13-2　コラボレーション メディア ストリームの進化



コラボレーション ソリューションで現在積極的に適用されているその他の傾向および技術は、次のとおりです。

- モビリティ、Bring Your Own Device（BYOD）、ユビキタス ビデオ
- Web ベースのコラボレーションと WebRTC
- 標準とイマーシブ ビデオ
- クラウド、オンプレミス、およびハイブリッド会議
- ワイド エリア ネットワーク：所有型とオーバーザトップ
- 企業間コラボレーション：Business-to-Business および Business-to-Customer
- マルチデバイスのマルチストリーム セッション：音声、ビデオ、データ共有、およびインスタント メッセージ

マネージド ネットワークとアンマネージド ネットワークのこのような進化、新しいエンドポイント、ユーザ エクスペリエンス、新しい技術と動向には、次のような課題があります。

- 帯域幅を制御し、マネージド ネットワークとアンマネージド ネットワーク上で優れたユーザ エクスペリエンスを実現する方法
- 企業全体でビデオを広範囲に導入し、使用可能なネットワーク リソースの帯域利用率を最適化する方法

この章では、利用可能なネットワーク リソースに基づいて最高のユーザ エクスペリエンスを実現できるように、Cisco ビデオ エンドポイントでのスマート メディア技術の活用、エンドツーエンドの QoS アーキテクチャの構築、最新デザインと導入推奨事項および帯域幅管理のベスト プラクティスの活用に関する戦略について説明します。ネットワーク コラボレーション メディアのタイプが強制的に通過するようになりました。

コラボレーション メディア

このセクションでは、Cisco ビデオ エンドポイントが、パケットの損失、遅延、ジッターに直面しながらも高品質のビデオを実現するために導入するリアルタイム メディア技術とスマート メディア技術を使用した音声ストリームとビデオ ストリームの特性について説明します。

デジタル ビデオの基礎

ビデオは企業のトラフィック ミックスの主要コンポーネントです。ストリーミング ビデオと事前に配置したビデオの両方がネットワークに影響を与え、パフォーマンス全体にも大きく影響します。ビデオ データグラムの構造とネットワークに配置する際の要件を理解すると、ネットワーク管理者がメディア対応ネットワークを実装する場合に役立ちます。

さまざまなタイプのビデオ

ビデオの説明にはさまざまな属性を使用できます。たとえば、ビデオは、リアルタイムまたは録画、ストリーミングまたは事前配置、高解像度または低解像度に分類できます。ネットワーク負荷は、送信されるビデオのタイプによって異なります。録画、事前配置、低解像度のビデオはファイル転送とほとんど同じですが、リアルタイム ストリーミング ビデオには高性能ネットワークが必要です。一般的なビデオ アプリケーションの多くはこのどこかに当てはまります。このため、リアルタイム ストリーミング ビデオ アプリケーションはパブリック インターネット上で適切に動作できます。ネットワークおよびメディア エンコーダの調整は、IP ネットワークでビデオを導入する際の重要な側面です。

H.264 コーディングとデコードの影響

ビデオ コーデックは、過去 15 年間にわたって進化を続けています。現在のコーデックは、強力な処理能力を使用してストリーミング サイズを適切に最適化します。一般的な手順は、元の MPEG1 標準規格のリリースからほとんど変わっていません。画像は、ブロックにグループ化されたピクセルのマトリックスから構成されます。ブロックはマクロ ブロックにまとめられます。マクロ ブロックの 1 行が 1 つのスライスです。スライスは画像を形成し、画像は画像グループ（GOP）にまとめられます。

各ピクセルには、赤、緑、青のコンポーネントがあります。エンコーディング プロセスでは、RGB を luma と 2 色のカラー コンポーネント（一般には YCrCb と呼ばれる）に分けることから始まります。エンコーディングではわずかな色情報は無視され、後で補間されます。YCrCb 形式になると、各コンポーネントは変換に進みます。変換は元に戻すことができ、データが圧縮されることはありません。その代わり、効率的な量子化と圧縮を実現できるように、データは異なる方法で表されます。データの細部を補完するには、量子化が使用されます。品質を設定するには、この補完が使用されます。品質を下げると、圧縮率が上がります。量子化の後、共通ビットをバイナリ コードで置き換えて、無損失圧縮を適用します。画像の各マクロ ブロックがこのプロセスを通過すると、ビットの基本的なストリームが生成されます。このストリームは、PES（Packetized Elementary Stream）と呼ばれる 188 バイトのパケットにスライスされます。次に、このストリームは IP パケットにロードされます。IP パケットには 1,500 バイトの MTU が含まれ、PES パケットは 188 バイトに固定されているため、1 つの IP パケットに収めることができる PES は 7 つのみです。生成された IP パケットは 1,316 バイトで、ヘッダーは含まれません。その結果、IP フラグメンテーションの問題はありません。一般的なパケット数は 45 ～ 65 ですが、高解像度ビデオのすべてのフレームの基本ストリーム パケットをすべて伝送するのに必要な IP パケット数は 100 になることがあります。量子化および画像の複雑性は、伝送に必要なパケット数を決定する上で重要な要因となります。消失情報の見積りには、前方誤り訂正を使用できます。ただし多くの場合、複数の IP パケットが連続して消失します。このため、フレームの復元がほぼ不可能になります。正常に送信されたパケットは使われない帯域幅を表します。新しいフレームを要求するには RTCP を使用できます。有効な最初のフレームがないと、後続フレームが正しくデコードされません。

フレーム タイプ

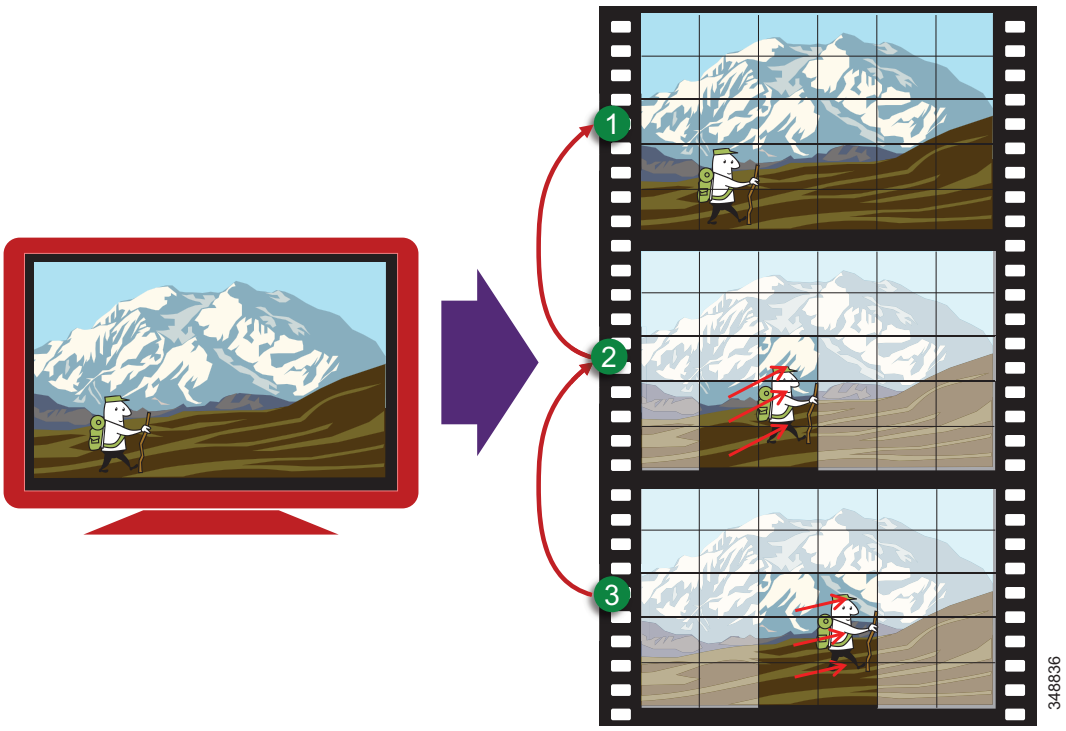
最新世代のビデオ コーディングは、H.264、MPEG4 パート 10、および Advanced Video Coding（AVC）の 3 つの名前で知られています。以前のコーデックと同様に、H.264 は空間的かつ時間的圧縮を使用します。空間的圧縮は、これまでに説明したようにビデオの単一フレームで使用します。これらのタイプのフレームは I フレームと呼ばれています。I フレームは GOP の最初の画像です。時間的圧縮は、後続フレーム間の情報がほとんど変わらない点を利用します。拡大率を変更したり、カメラを移動したりすると、ほぼすべてのピクセルが変化しますが、変化は移動が原因です。ベクトルはこの移動を表すために使用され、ブロックに適用されます。カメラの旋回と同じように、すべてのピクセルが一緒に移動したとエンコーダが判断した場合は、グローバル ベクトルが使用されます。さらに、発生するエラーを微調整するために、差分信号が使用されます。H.264 では可変ブロック サイズが有効で、¼ ピクセル相当に動きをコーディングできます。デコーダはこの情報を使用して、現在のフレームが前のフレームと比べてどのように表示されるかを決定します。動きのベクトルとエラー信号を含むパケットは P フレームと呼ばれます。通常、P フレームが失われると、後続フレームに組み込まれるアーティファクトが発生します。アーティファクトが長期間発生する場合、その原因は P フレームの消失の可能性があります。

図 13-3 は基本的な仕組みを示します。

1. I フレーム（イントラコード化画像）は静止画像としてエンコードされた画像全体で、パケットのグループとして送信されます。このフレームは他のフレームを参照しません。デコーダで画像全体を生成するのに必要なのはこのフレームのみです。この場合、画像は山をハイキングする小さなハイカーです。
2. 次に P フレーム（予測画像）が送信されます。これは前にエンコードしたフレーム（この場合は I フレーム）に基づくフレームです。I フレームとの差異のみがエンコードされます。デコーダはこれらの差異を取得し、すでにある I フレームにこの差異を適用します。この場合、小さなハイカーが丘を登っています。小さなハイカーとその動きのみが最後の I フレームから変化するため、この P フレームは非常に小さくなり、送信するパケットおよび帯域幅は少なくなります。

3. 次の P フレームが送信され、最後の P フレームの予測が送信されます。ステップ 2 の P フレームと同様に、この P フレームでは、丘を登るハイカーの最後の動きとこの新しい動きとの差異を示します。前の画像からの変化量が大きくなるまで、この一連の操作は継続するため、新しい I フレームが必要になります。

図 13-3　　エンコーディングの基本



H.264 は B フレームも実装します。このタイプのフレームには、P フレーム間の情報が含まれます。つまり、B フレームの情報を使用する前に、次の P フレームが到着するまで B フレームを保持する必要があります。B フレームは H.264 のどのモードでも使用されません。エンコーダは最適なフレーム タイプを決定します。通常、I フレームよりも P フレームが多くなります。ラボの分析では、TelePresence の I フレームは通常 64 K バイト長（1,316 バイトで 50 パケット）で、P フレームの平均は 8 K バイト長（900 バイトで 9 パケット）です。I フレームが大きくなるため、P フレームと比較してビット レートに急激に上昇します。

音声とビデオ

多くの場合、音声とビデオは従兄弟のような関係と考えられています。両方ともリアルタイム プロトコル（RTP）アプリケーションですが、同じ点はこれだけです。通常、各パケットのサイズとレートは固定されているため、音声は適切に動作すると考えられています。ビデオ フレームは複数のパケットに広がり、グループとして移動します。1 つのパケットが失われると、P フレームが無駄になり、1 つの P フレームが無駄になると、永続的なアーティファクトが生成されるため、通常、ビデオには音声よりも厳密な損失要件があります。ビデオは非対称です。音声も非対称ですが、通常は対称です。ミュートの場合でも、IP Phone は同じサイズのフローを送受信します。

ビデオでは、平均リアルタイム パケット サイズが増え、ネットワークのトラフィック プロファイルを素早く変更する可能性があります。計画的に行わないと、ネットワーク パフォーマンスに悪影響を与える可能性があります。図 13-4 では、一定の時間送信される一連の音声パケットとビデオ パケットの差異を示します。

図 13-4　音声とビデオ

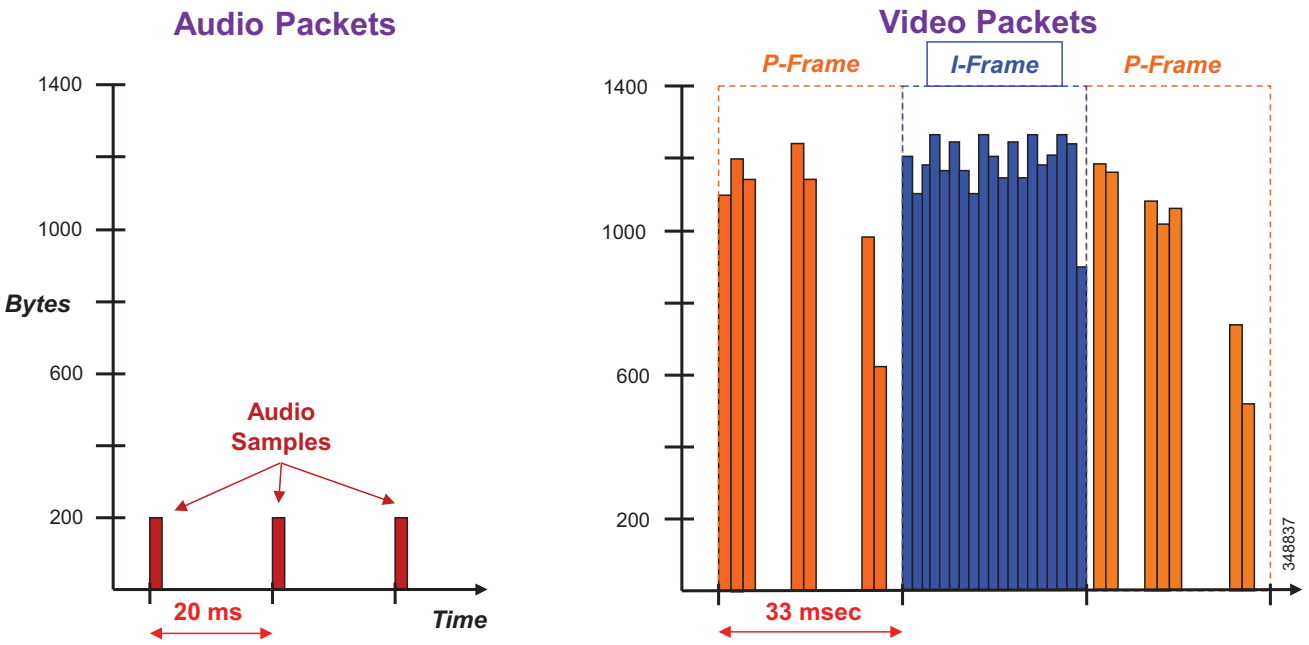


図 13-4 から分かるように、音声パケットは同じサイズで、正確に同間隔で送信され、非常にスムーズなストリームです。一方、ビデオは一定の間隔で大量のパケットを送信し、フレームごとに大きく異なります。図 13-4 では、I フレームと P フレームを比較した場合の、パケット数とパケット サイズの差異を示します。音声と比較すると、非常にバースト性のあるメディア ストリームに変換されます。図 13-5 では、HD ビデオ ストリームの帯域幅プロファイルを段階的に示します。I フレームの送信時にはバーストが大きくなることに注意してください。

図 13-5　帯域幅の使用：高解像度ビデオ コール

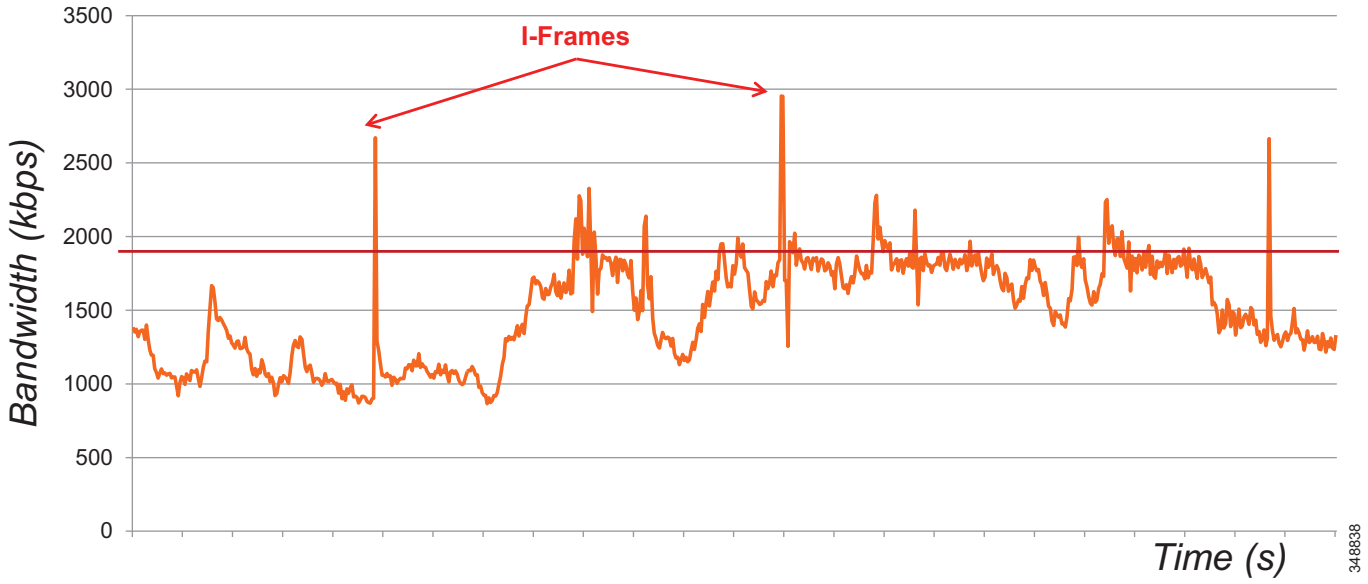
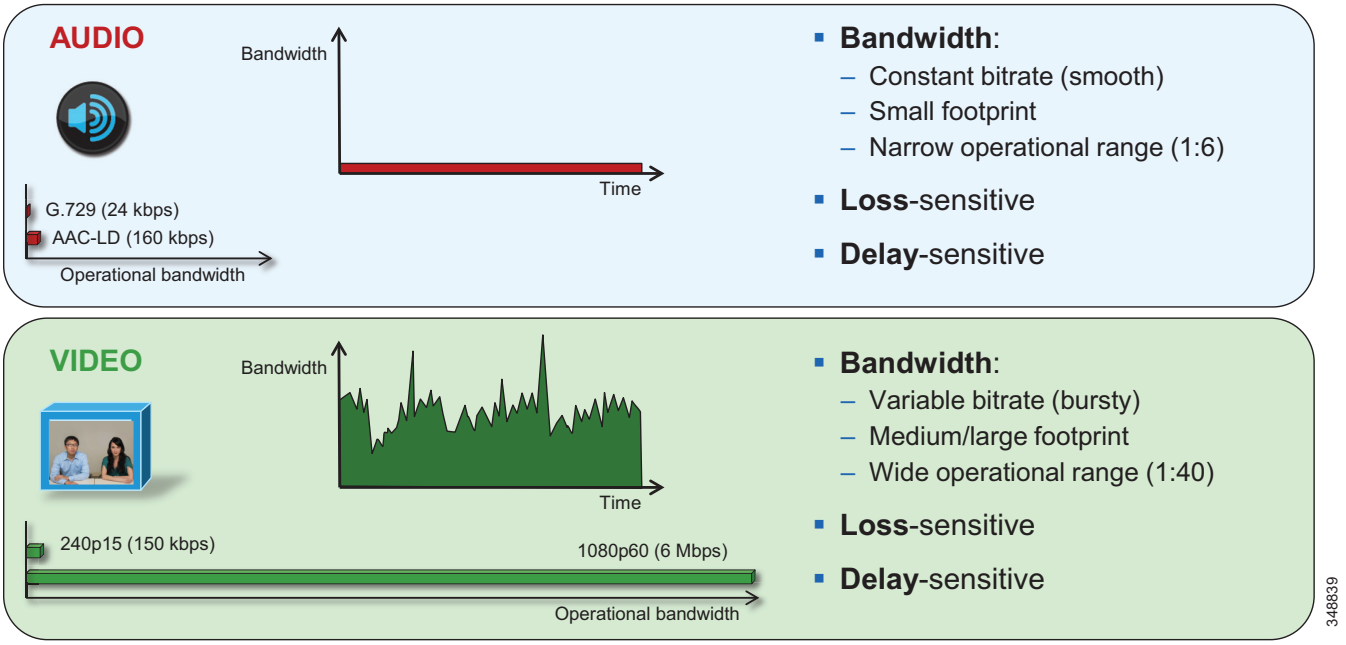


図 13-5 では、1,920 kbps で 720p30 の HD ビデオ コール（1,792 kbps ビデオ + 128 kbps 音声）を示します。このグラフはビデオ帯域幅（L3 オーバーヘッドを含む）を表し、赤色の線は平均ビット レートを示します。

音声とビデオの両方とも UDP 経由で転送され、損失と遅延の影響を受けやすいですが、それぞれのネットワーク要件とプロファイルは大きく異なります。音声のビット レートは一定で、ビデオと比較して密度が低いです。また、最小ビット レート オーディオ コーデックと最大ビット レート コーデックの 1 つを比較しても、運用範囲の比率は 1:6 と狭いです。一方、ビデオのビット レートは可変（バースト性がある）で、音声と比較して密度が高いです。また、運用範囲は 1:40 と広いです（15 fps で 250p と 60 fps で 1080p）。図 13-6 では、これらの差異の一部を示します。

図 13-6　ビデオ トラフィック要件とプロファイル



注意すべき重要な点は、音声とビデオは、転送、および損失と遅延の影響については似ていますが、ネットワークにおけるそれぞれの帯域幅要件の管理については大きく異なります。また、ビデオはコラボレーション エクスペリエンス全体に関連し、音声が重要であることにも注意してください。たとえば、ネットワークの停止または他のネットワーク関連イベントにより、ビデオがビデオ コール中に失われた場合、音声がこの停止中に失われなければ、通信は継続できます。QoS の分類とマーキングのようなコラボレーション設計のネットワーク要件を考える場合、これは重要な概念になります。

解像度

送信側ステーションはビデオ解像度を決定するため、ネットワークの負荷も決まります。これは、ビデオの表示に使用するモニタのサイズとは関係ありません。負荷を推定するのに、ビデオを調査するのは信頼性のある方法ではありません。一般的な高解像度形式は、720i、1080i、1080p などです。高解像度に加えて、HTTP（または一部で HTTPS）および SSL（表 13-2 を参照）でトンネリングされることの多い低解像度のビデオも急増しています。一般的な解像度には、CIF（352x288）と 4CIF（704x576）があります。これらの数値は、DCT（22x18）と（44x36）マクロ ブロックでそれぞれ使用される、16x16 マクロ ブロックの整数値として選択されています。

表 13-2　形式、解像度、および帯域幅

フォーマット（Format）	解像度	標準帯域幅
QCIF（1/4 CIF）	176x144	260 kbps
CIF	352x288	512 kbps
4CIF	704x576	1 Mbps
SD NTSC	720x480	アナログ、4.2 MHz
720 HD	1280x720	1 ～ 8 Mbps
1080 HD	1080x1920	5 ～ 8 Mbps H.264 12+ Mbps MPEG-2

ネットワーク負荷

解像度がネットワーク負荷に与える影響は、一般的に係数の二乗です。画像の大きさが 2 倍のときは、4 倍の帯域幅が必要になります。また、カラー サンプリング、量子化、およびフレーム レートも、ネットワークのトラフィック量に影響を与えます。標準レートは 30 フレーム/秒（fps）ですが、これは AC 電源の周波数に基づいて選択した任意の値です。ヨーロッパでは、従来のアナログ ビデオは 25 fps です。シネプレックス向けの映画は 24 fps で撮影されています。フレーム レートが下がるにつれて、ネットワークの負荷も少なくなりますが、動きの臨場感は低下します。ビデオが 24 fps を超えても、動きが大幅に改善されることはありません。

また、エンコーダの高性能化も、ビデオの負荷に大きく影響します。H.264 エンコーダは、最適なエンコード方法を決定するときに優れた柔軟性を発揮するため、最適な方法を決定するときに複雑になります。たとえば、MPEG4.10 では、エンコーダが周辺ピクセルに応じて最適なブロック サイズを選択できます。効率的なエンコードはデコードよりも難しく、送信者がネットワークの負荷を判断するため、通常の低コストのエンコーダは高性能なエンコーダよりも多くの帯域幅を必要とします。リアルタイム CIF ビデオの H.264 コーディングではすべてを使用しますが、専用のメディア プロセッサを装着しないと、最も強力なラップトップの CPU 使用率は 90 % になります。

表 13-3 から表 13-5 では、エンドポイントと解像度に基づいた帯域幅の平均使用範囲を示します。次の表では、一般的な TelePresence エンドポイントおよびデスクトップ ビデオ エンドポイントの解像度に基づいた帯域幅範囲の例のみを示します。対象のエンドポイントに関連する最新の数値については、最新の製品マニュアルを参照してください。

表 13-3　Cisco TelePresence エンドポイント – 帯域幅の使用例[1]

	MX200		SX20		EX90		TX9000	
解像度	低品質	高品質	低品質	高品質	低品質	高品質	低品質	高品質
720p30（1280x720）	736 kbps	1.2 Mbps	812 kbps	1.2 Mbps	812 kbps	1.2 Mbps	3.1 Mbps	6.4 Mbps
1080p30（1920x1080）	2.6 Mbps	5.7 Mbps	2.6 Mbps	6.2 Mbps	2.5 Mbps	6.1 Mbps	8.8 Mbps	11.9 Mbps
720p60（60 fps）	該当なし	2.3 Mbps	該当なし	2.3 Mbps	該当なし	2.4 Mbps	該当なし	該当なし

1. TelePresence エンドポイントの詳細については、https://www.cisco.com/c/dam/en/us/products/collateral/collaboration-endpoints/tested_bandwidth_whitepaperx.pdf で入手可能な帯域幅使用に関するホワイト ペーパーを参照してください。

表 13-4　Cisco DX シリーズ – 帯域幅の使用例[1]

解像度	DX シリーズ ビデオ帯域幅
240p30（432x240）	150 ～ 299 kbps
360p30（640x360）	300 ～ 599 kbps
480p30（848x480）	600 ～ 799 kbps
576p30（1024x576）	800 kbps ～ 1.29 Mbps
720p30（1280x720）	1.3 ～ 1.99 Mbps
1080p30（1920x1080）	2 ～ 4 Mbps

1. DX シリーズの詳細については、https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html で入手可能な最新版の『*Cisco DX Series Administration Guide*』を参照してください。

表 13-5　Cisco Jabber – 帯域幅の使用例[1]

解像度	Jabber ビデオ帯域幅（G.711 音声付き）
w144p30（256x144）	156 kbps
w288p30（512x288）	320 kbps
w448p30（768x448）	570 kbps
w576p30（1024x576）	890 kbps
720p30（1280x720）	1.3 Mbps

1. Jabber の詳細については、https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html で入手可能な最新版の『Cisco Jabber Deployment and Installation Guide』を参照してください。

マルチキャスト（Multicast）

ブロードキャスト ビデオは、マルチキャストで提供される帯域幅節減の活用に役に立ちます。これは長年にわたり、多くのネットワークに導入されています。マルチキャストの最近の改善により、ネットワークへの導入が簡単になりました。マルチキャストは今後も使用されますが、すべての状況で使用されるわけではありません。マルチポイント TelePresence など、一部のアプリケーションはビデオの複製専用の MCU を使用します。MCU は、どの参加者が各送信者を表示するかについて判断することができます。また、MCU は表示されていない送信者を抑制することもできます。

転送

MPEG4 は MPEG2 と同じ転送を使用します。PES は IP にロードされる 188 バイト データグラムで構成されます。ビデオ パケットは RTP/UDP/IP または HTTP(S)/TCP/IP にロードできます。

UDP 経由のビデオは、マルチメディア会議や TelePresence などの専用リアルタイム アプリケーションで使用されます。この場合、RTCP チャネルは受信者から送信者に対して設定できます。これを使用すると、ビデオ セッションを管理できます。RTCP を使用すると、I フレームを要求したり、送信者に機能を報告したりできます。UDP および RTP はそれぞれ多重チャネルの手段を提供します。通常、音声およびビデオは異なる UDP ポートを使用しますが、RTP ペイロード タイプも固有です。ディープ パケット インスペクション（DPI）をネットワークで使用すると、現在のビデオ音声のタイプを特定できます。また、H.264 ビデオは、ビデオの多重レイヤに関するメカニズムも提供しています。

バッファリング

ジッターおよび遅延はすべての IP ネットワーク内に存在します。ジッターは遅延の変動です。一般的に遅延は、インターフェイスのキューイングが原因で発生します。ビデオ デコーダで再生バッファを使用すると、ネットワーク内のジッターを抑えることができます。このバッファの深さには制限があります。浅すぎると、廃棄されてしまいます。深すぎると、ビデオが遅延するため、TelePresence などのリアルタイム アプリケーションで問題が発生する場合があります。再生バッファが深いことの多い廃棄パケットを処理するために別の制限があります。RTCP を使用して新しい I フレームを要求する場合、再同期化のときに多くのフレームがスキップされます。その結果、失われたパケットが見つかった場合に与える影響よりも、廃棄パケットがビデオの品質低下に与える影響のほうが若干大きくなります。ほとんどのコーデックがダイナミック再生バッファを使用します。

要約

この追加負荷を適切に考慮して計画しないと、ビデオはネットワークのパフォーマンスに大きな影響を与える場合があります。この章は、管理者が企業ネットワークでリアルタイム ビデオを管理する場合に役立ちます。

「スマート」メディア テクニック（メディアの復元力とレート調整）

シスコの企業向けビデオ エンドポイントは過去数年間で大きく進化しました。シスコのすべてのビデオ エンドポイントでは多くのメディアの復元力手法を使用して、ネットワークの輻輳の回避、パケット損失からの回復、ネットワーク リソースの最適化を行います。このセクションでは、シスコのビデオ エンドポイントで使用されている次のスマート メディアの手法についてします。

- エンコーダ ペーシング（13-11 ページ）
- Gradual Decoder Refresh（GDR）（13-12 ページ）
- 長時間参照フレーム（LTRF）（13-13 ページ）
- 前方誤り訂正（FEC）（13-14 ページ）
- レート調整（13-15 ページ）

エンコーダ ペーシング

パケット数は、フレーム タイプ（I または P）と必要なパケットの数に応じて変化します。つまり、始まり、途中、または最後で 33 ミリ秒間隔のパケットのバーストが発生します。これにより、パケットがネットワークを流れると、帯域幅が急激に上昇します。エンコーダ ペーシングは、帯域幅のバーストのピークをスムーズにするために、33 ミリ秒間隔でパケットを可能な限り均等に分散する簡単な手法です。図 13-7 はこの手法を示します。

図 13-7　エンコーダ ペーシング

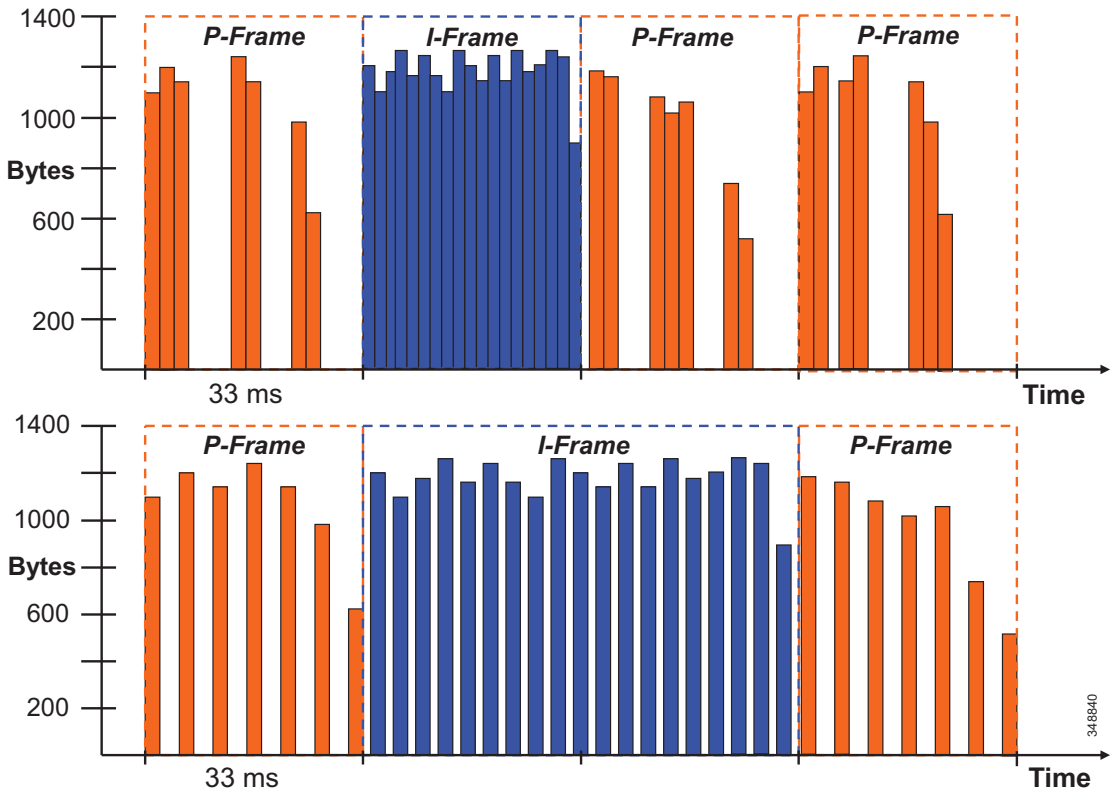


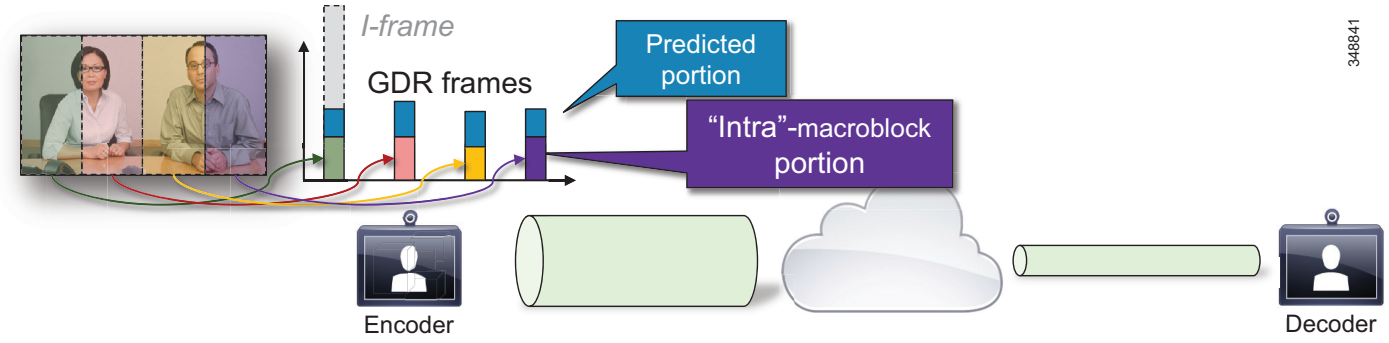
図 13-7 上部のグラフは、エンコーダ ペーシングを使用せずにネットワーク上を流れるパケットを示し、下部のグラフはエンコーダ ペーシングを使用した場合を示しています。各フレームが 33 ミリ秒間隔でネットワーク上でパケット化されるため、エンドポイント パケット スケジューラは、単一間隔でパケットを可能な限り均等に分散します。大きな I フレームは、2 つまたは 3 つのフレーム間隔に「分ける」必要があり、エンコーダはビット レート範囲内に収めるために 1 つまたは 2 つのフレームをスキップすることがあります。このため、同じ期間での帯域幅使用率のピークが分散されます。

Gradual Decoder Refresh（GDR）

GDR は、エンコードされたビット ストリームの開始点または更新を提供します。GDR は、多数のフレームで画像を徐々にリフレッシュして、よりスムーズでバースト性の低いビット ストリームを提供する方法です。

新しい I フレームではトラフィックのバーストが起こるため、特に会議の切り替え時に輻輳が発生します。I フレーム パケットが 1 つ廃棄されると、フレーム全体を再送信する必要があります。図 13-8 で示すように、Gradual Decoder Refresh は N フレームに対して「内部的」にエンコードした画像データを拡散します。GDR フレームには、「内部的」なマクロブロックの部分と予測したマクロブロックの部分が含まれます。GDR のすべてのフレームを受信したら、デコーダは画像を完全に更新できます。

図 13-8　Gradual Decoder Refresh (GDR)



長時間参照フレーム (LTRF)

長時間参照フレーム (LTRF) は、エンコーダおよびデコーダが別の方法で明示的な信号を受信するまで、エンコーダおよびデコーダに保存される参照フレームです。(H.264 では最大 15 LTRF がサポートされます。) 通常 (LTRF 未使用時)、パケットの損失後、エンコーダ/デコーダの再同期化には内部フレームが使用されます。

LTRF は、エンコーダとデコーダの再同期化の代替手法として、通常の内部フレームよりも優れています。通常、エンコーダは LTRF を一定の間隔で挿入し、それと同時にその LTRF を 1 つ以上を保存するようにデコーダに指示します (図 13-9 を参照)。

修正 P フレームは、参照として正しくデコードされた以前の LTRF を使用します。修正 P フレームは、損失フレームまたはその参照フレームに応じて使用されます。確認 LTRF がデコーダで適切に受信されていると分かっているため、デコーダが修正 P フレームを適切にデコードできる場合は、同期状態に戻ることが確認されています。

図 13-9　長時間参照フレーム (LTRF)

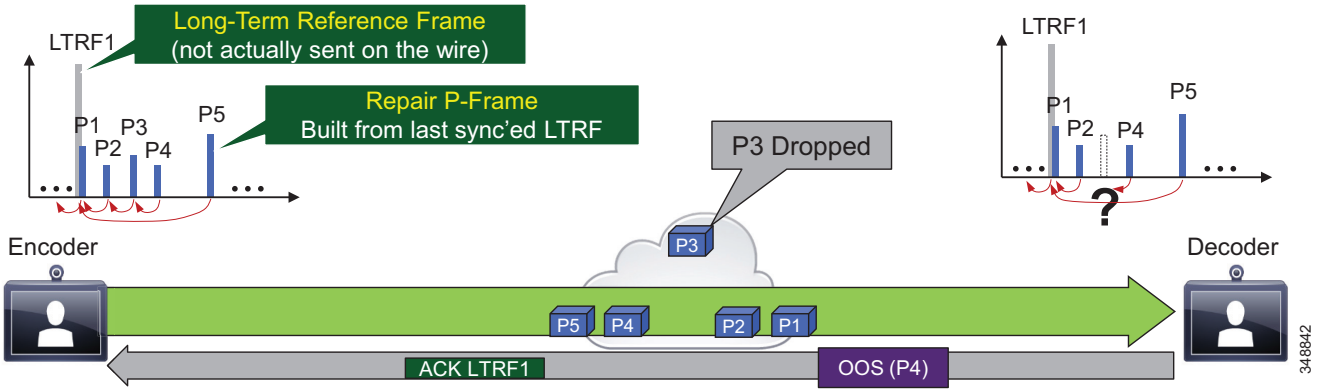


図 13-9 から分かるように、LTRF は、アクティブ フィードバック メッセージを使用して、エンコーダとデコーダの同期を維持します。エンコーダは、長時間参照フレーム (H.264 標準の一部) として特定の同期ポイントで未処理のフレームを保存するようにデコーダに指示します。デコーダは「バック チャネル」(RTCP) を使用して LTRF を確認します。フレームが失われると、エンコーダは、新しい I フレームの代わりに、最後に同期した LTRF に基づいて修正 P フレームを作成するため、帯域幅が保存されます。

前方誤り訂正（FEC）

前方誤り訂正（FEC）では、所定のアルゴリズムを使用して、転送される情報に冗長性を付与します（図 13-10 を参照）。この冗長性により、受信側では、メッセージのいずれかの箇所でエラーが発生した場合でもそれが一定数であれば、送信側に追加データを要求することなく、そのエラーを検出し訂正することができます。FEC では、受信側でエラーを訂正する場合、データの再送信を要求するためのリバース チャネルは必要ありませんが、その代わりとして、より高い転送チャネル帯域幅が常に必要となります。FEC では最も重要なデータ（通常は修正 P フレーム）が保護されます。これにより、それらのフレームは受信側で確実に受信されます。エンドポイントでは、帯域幅が 768 kbps を下回る場合 FEC は使用されません。また、1.5 % 以上のパケット損失が発生していない場合も FEC は適用されません。通常、FEC の有効性はエンドポイントによりモニタリングされます。FEC が有効でない場合は、エンドポイントにより FEC の実行が中止されます。

図 13-10　前方誤り訂正（FEC）

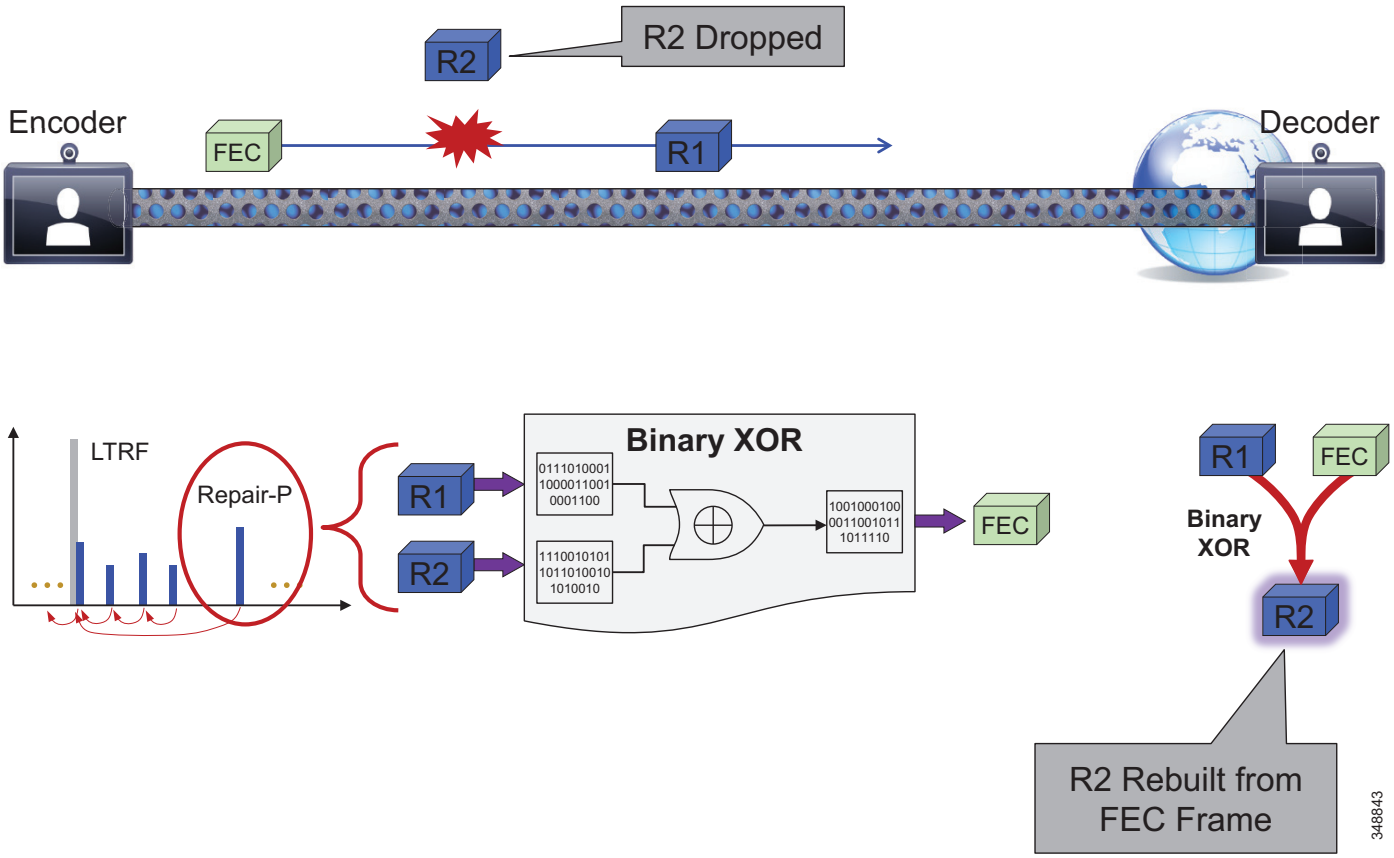


図 13-10 から分かるように、FEC により、同期化が失われることなく、デコーダは一定量のパケット損失から復元できます。これは、損失の多い環境で「重要」なフレームを保護するために、さまざまなレベル（*N* データ パケットごとの *X* FEC パケットなど）で適用できます。修正コードには、基本（バイナリ XOR）または高度（Reed-Solomon）があります。帯域幅の使用ではトレードオフが増えているため、非バースト損失に最適です。

レート調整

レート調整またはダイナミック ビット レート調整は、使用できる可変帯域幅に合わせてコール レートを調整します。これにより、パケット損失の状況に基づいてビデオ ビット レートの速度が上下します（図 13-11 を参照）。パケット損失が減少すると速度が上昇します。一部のエンドポイントでは、RTCP を介して送信側プロアクティブ方式が使用されます。この場合、送信側では常に RTCP レシーバー レポートの確認が行われ、その内容に従ってビット レートが調整されます。その他のエンドポイントでは、受信側方式が使用され、コール シグナリング（H.323 フロー制御、TMBRR、SIP Re-invite）または RTCP メッセージ内の明示的な要求を介して調整されます。

図 13-11　レート調整

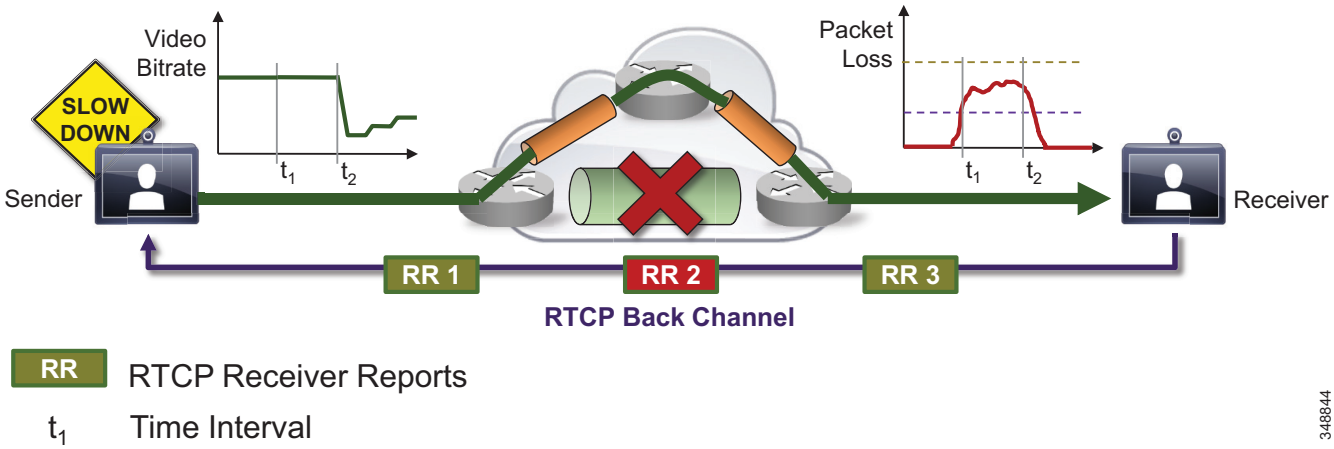


図 13-11 から分かるように、受信側は長時間にわたって遅延とパケット損失を観察し、RTCP レシーバ レポート（RR）を使用して信号を返します。このレポートにより、送信側は、ネットワークの状況に合わせてビット レートを調整します（ビット レートの速度の上下）。

レート調整には、次の 2 つの方式があります。

- RTCP レシーバ レポートに基づいた送信側調整
- コール シグナリング（H.323 フロー制御、TMBRR、SIP Re-invite）または RTCP メッセージ内の明示的な要求を介した受信側調整

要約

- トラフィックのバースト性およびエンドポイントのモビリティ性は、インタラクティブ ビデオの確実なプロビジョニングをネットワーク管理者にとって困難なものにします。
- メディアの復元力 メカニズムにより、ネットワークに対するビデオ トラフィックの影響およびビデオに対するネットワーク障害の影響が軽減されます。（表 13-6 を参照）。
- ダイナミック レート調整により、企業のネットワークでインタラクティブ ビデオを柔軟にプロビジョニングするモデルの機会が生まれます。
- メディアの復元力およびレート調整により、ビデオ トラフィックがインターネットまたは QoS 未対応ネットワークを通過する場合、ユーザ エクスペリエンスが維持されます。

表 13-6　シスコ コラボレーション ビデオ エンドポイントのメディア復元力のサポート

エンドポイントまたはブリッジ	エンコーダペーシング	レート調整	FEC	LTRF 修正
8800 シリーズ	○	X	X	X
9900 シリーズ	X	X	X	X
DX シリーズ	○	○	X	X
WebEx	○	○	○	X
TX シリーズ	○	○	X	○
Jabber	○	○	○	○
C、EX、MX、SX、およびプロファイル シリーズ	○	○	○	○
TelePresence Server	○	○	○	○
MCU	○	○	○	○
Cisco Meeting Server	○	○	○	○

コラボレーション用の QoS アーキテクチャ

サービス品質（QoS）により、メディア エンドポイントおよびアプリケーションの遅延、パケット損失、ジッターの削減し、信頼性のある高品質な音声とビデオを実現します。QoS は、音声、ビデオ、データ ネットワークの透過的なコンバージェンスをサポートするのに必要な基本的なネットワーク インフラストラクチャ技術を提供します。インタラクティブ アプリケーション（特に音声、ビデオ、およびイマーシブ アプリケーション）の増加に伴い、多くの場合、ネットワークのリアルタイム サービスが求められます。これらのリソースは限られているため、効率的かつ効果的に管理する必要があります。優先リソースのフロー数に制限がない場合は、これらのリソースがオーバーサブスクライブされるため、すべてのリアルタイム トラフィック フローの品質が低下し、最終的には役に立たなくなります。「スマート」メディアの手法、QoS、およびアドミッション制御により、リアルタイム アプリケーションとその関連メディアが、これらのアプリケーションにプロビジョニングされたネットワークおよび帯域幅をオーバーサブスクライブしないようにします。QoS に関連するこれらのスマート メディアの手法と、必要に応じたアドミッション制御は、リアルタイム メディアを非リアルタイム ネットワーク トラフィックから保護し、ネットワークをオーバーサブスクリプションから保護して、音声とビデオのすべてのアプリケーションの潜在的な品質低下を回避するための強力なツール セットです。

アドミッション制御と QoS は相互に補完します。アドミッション制御には QoS が必要ですが、QoS はアドミッション制御がなくても導入できます。この章の後半では、アドミッション制御と QoS との関係について詳しく説明します。

図 13-12 は、この章で使用する QoS の手法について示しています。この手法は次のフェーズで構成されており、このセクションの後半で詳しく説明します。

- 識別と分類（13-17 ページ）

  このフェーズでは、信頼されているエンドポイントおよび信頼されていないエンドポイントに対するメディアとシグナリングの識別に関する信頼と手法の概念について説明します。信頼されているエンドポイントと信頼されていないエンドポイントの両方のネットワーク全体に、エンドツーエンドの適切な Per-Hop Behavior を使用してメディアとシグナリングを提供するために、識別したトラフィックを適切な DSCP にマッピングするプロセスが含まれます。

- WAN キューイングとスケジューリング（13-35 ページ）

  このフェーズは、一般的な WAN のキューイングとスケジューリング、各種キューイング、およびコラボレーション メディアとシグナリングが WAN への出力で正しくキューイングするための推奨事項で構成されています。

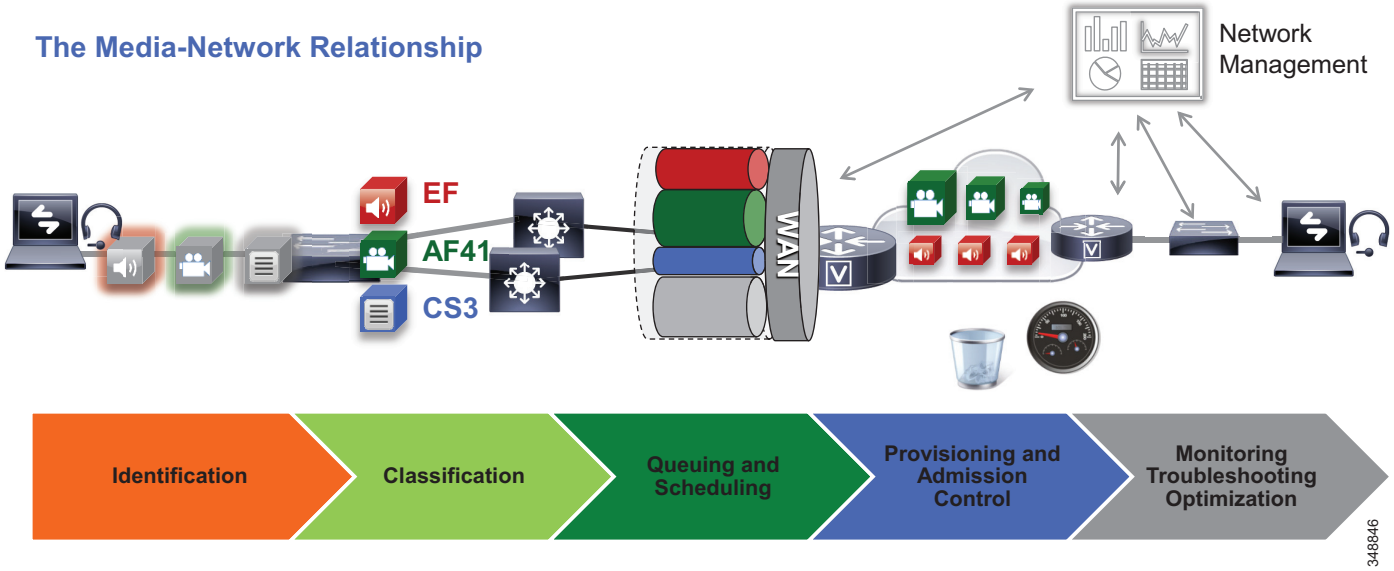
- プロビジョニングとアドミッション制御（13-39 ページ）

  このフェーズでは、ネットワークでの帯域幅のプロビジョニング、およびエンドポイント グループが使用する最大ビット レートの測定について説明します。また、コール アドミッション制御を必要なネットワーク領域に実装することもできます。

- モニタリング、トラブルシューティング、および最適化

  このフェーズは、ネットワークでの音声とビデオの適切な操作および管理に必要不可欠ですが、この章では説明しません。これらの作業の詳細については、ネットワーク管理（27-1 ページ）の章を参照してください。

図 13-12　コラボレーション用の QoS アーキテクチャの要素



識別と分類

このセクションでは、信頼されているエンドポイントおよび信頼されていないエンドポイントに対するメディアとシグナリングの識別に関する信頼と手法の概念について説明します。信頼されているエンドポイントと信頼されていないエンドポイントの両方のネットワーク全体に、エンドツーエンドの適切な Per-Hop Behavior を使用してメディアとシグナリングを提供するために、識別したトラフィックを適切な DSCP にマッピングするプロセスが含まれます。

QoS の信頼と適用

QoS の適用は、リアルタイムの音声、ビデオ、またはイマーシブ ビデオ エクスペリエンスに必要不可欠です。ネットワークで QoS（分類、優先順位付け、およびキューイング）を適切に処理しないと、リアルタイム メディアに過度の遅延またはパケット損失が発生する可能性があり、リアルタイム メディア フローの品質が低下します。QoS の適用のパラダイムでは、信頼の問題と信頼境界が同様に重要です。信頼は、トラフィックの QoS マーキング（レイヤ 2 CoS またはレイヤ 3 IP DSCP）を許可または「信頼」し、ネットワークを介して継続できるエンドポイントまたはデバイスを示しています。信頼境界は信頼するネットワーク内の場所です。これはネットワーク内のあらゆる場所で設定できますが、LAN アクセス入力や WAN エッジ、または必要に応じてその両方など、ネットワーク エッジで信頼を適用することをお勧めします。WAN エッジはトラフィック入力の別の分野で、サービス プロバイダーはネットワーク（サービス プロバイダー ネットワーク）全体の使用方法についてトラフィックを再度マーキングすることがあります。このため、エンドツーエンドの企業ネットワーク全体の継続性を確保するために、トラフィックを再度マーキングして適切な値に戻すことが重要です。

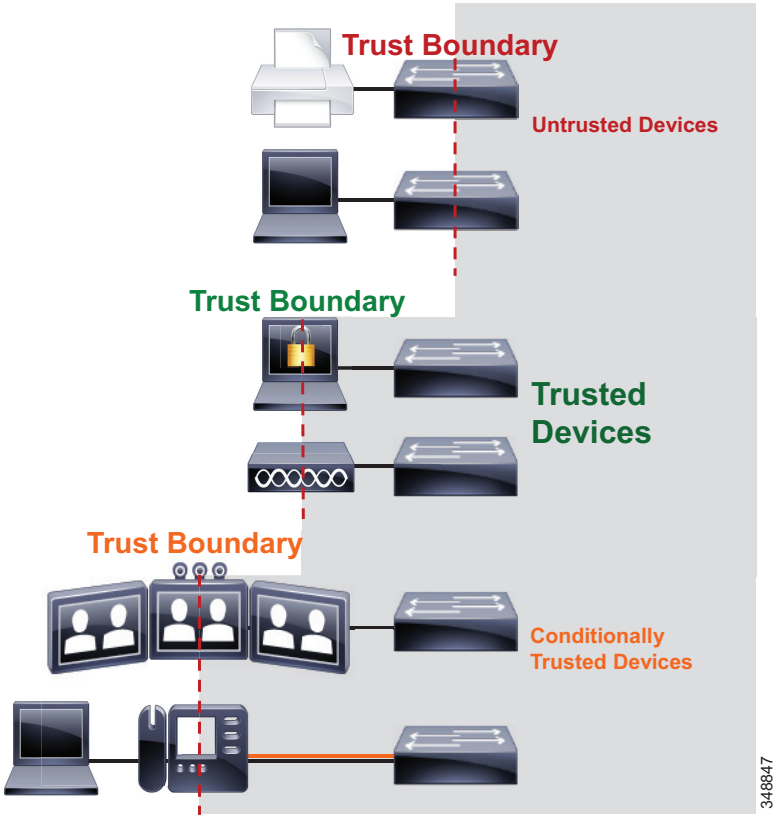
Cisco IP Phone およびビデオ エンドポイントを使用したシスコのコンバージド ネットワークでは、Cisco Discovery Protocol（CDP）を使用して IP Phone を検出するようにスイッチを設定できます。その後は、IP Phone またはビデオ エンドポイントのスイッチ ポートに接続された PC のマーキングを信頼していなくても、Cisco IP Phone およびビデオ エンドポイントが送信するパケットの DiffServ コード ポイント（DSCP）マーキングをスイッチは信頼できます。これは条件付き信頼と呼ばれます。Cisco IP Phone のみが許可され（音声 VLAN と呼ばれる）、そのパケット マーキングがスイッチによって信頼され、変更されていないネットワークを介して送られる、保護された VLAN では一般的です。一般的に、信頼されていないクライアント（PC や Mac など）が通常配置された VLAN（データ VLAN と呼ばれる）から配信されるトラフィックは信頼しません。通常、データ VLAN またはネットワーク内の同等の領域にあるデバイスから配信されるパケットは、ベスト エフォート（IP DSCP 0）に再マーキングされます。

信頼の観点から、エンドポイントには次の 3 つの主なカテゴリがあります。

- **信頼されていないエンドポイント**：保護されていない PC、Mac、または 携帯型モバイル デバイス
- **信頼されているエンドポイント**：保護された PC とサーバ、ビデオ会議エンドポイント、アクセス ポイント、アナログとビデオ会議ゲートウェイ、CDP が使用できない他の同様なデバイス
- **条件付きで信頼されるエンドポイント**：Cisco IP Phone、CDP をサポートする Cisco TelePresence エンドポイント

図 13-13 では、次の 3 つのタイプのデバイスについて説明します。

図 13-13　信頼境界



信頼境界は、管理上技術的に実現可能なエンドポイントのできるだけ近くに設定する必要があります。推奨事項は、スイッチで信頼を設定し、コラボレーション メディアとシグナリング用の音声 VLAN を使用し、コラボレーション以外のデータ トラフィック用のデータ VLAN を使用するためのものです。レイヤ 2 アクセス設計の詳細については、キャンパス アクセス レイヤ (3-5 ページ)を参照してください。

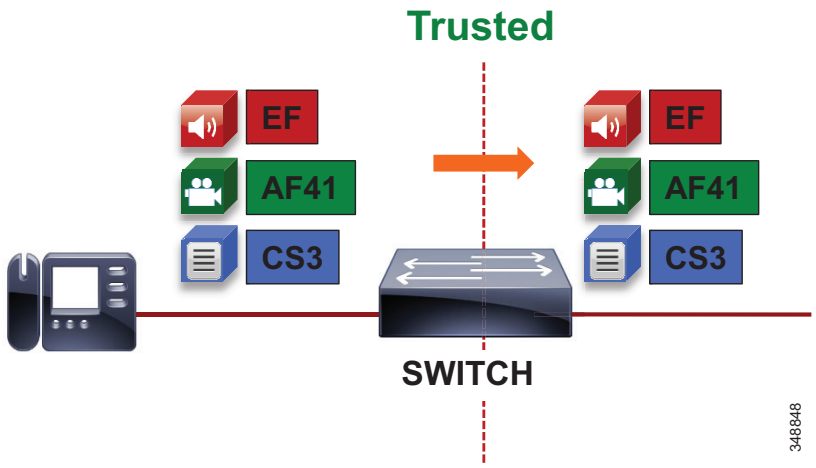
分類とマーキング

信頼境界が確立されると、QoS の適用はデバイスの 2 つのカテゴリ（信頼されていると信頼されていない）に分類されます。このセクションは、信頼されているデバイスと信頼されていないデバイスの分類およびマーキングについて説明します。

信頼されているエンドポイント

信頼されているエンドポイントおよび条件付きで信頼されているエンドポイントの場合、スイッチへの入力パケットの DSCP マーキングは信頼されており、出力で同じ値に再び書き換えられます。図 13-14 では、信頼されているエンドポイントの音声、ビデオ、信号トラフィックのマーキング、およびそのマーキングを信頼しているスイッチについて示します。

図 13-14　信頼されているエンドポイントの再マーキング



信頼されているポートまたは条件付きで信頼されているポートで設定されたシスコのスイッチの場合、スイッチは、CoS を使用して DSCP にマッピングするか、または元の DSCP を使用して、この DSCP を送信パケットの IP ヘッダー DSCP にマッピングします。図 13-15 では、レイヤ 2（CoS）およびレイヤ 3（DSCP）の受信パケット マーキングを示します。信頼のタイプには、信頼されている（CoS 信頼または DSCP 信頼）または信頼されていないがあります。内部スイッチ パケット上書きプロセスは、CoS 信頼または DSCP 信頼に基づいています。

図 13-15　受信と送信のスイッチ パケット マーキング

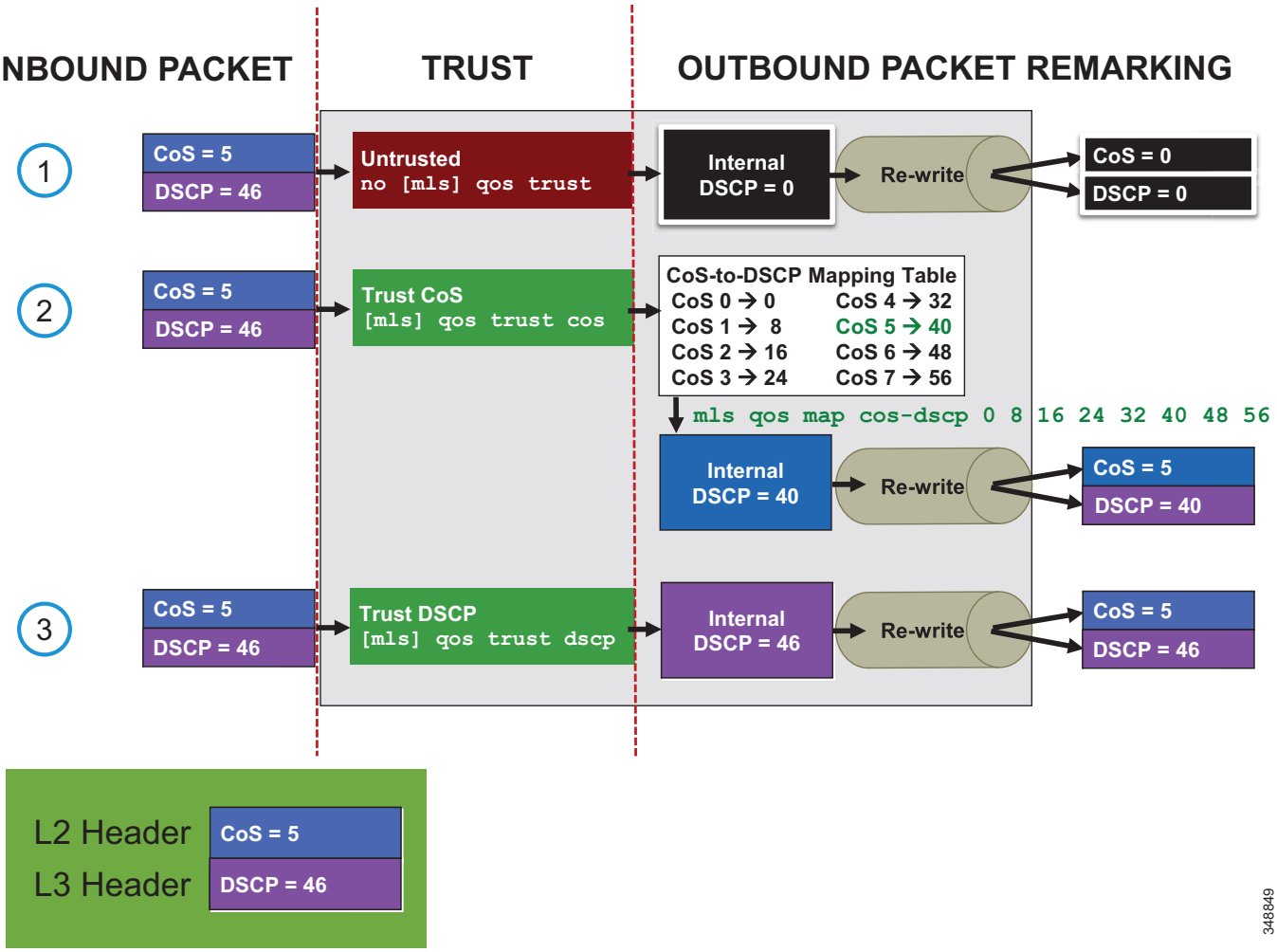


図 13-15 には、マルチレイヤ スイッチング（MLS）コマンドのほんの一例が示されています。MLS プラットフォームには、Cisco 2960、3560、および 3750 シリーズ スイッチ プラットフォームがあります。現在出荷されている他のすべてのスイッチ プラットフォーム（Cisco 3650、3850、4500、6500、および 6800 シリーズ スイッチ プラットフォームなど）の信頼はデフォルトで有効になっています。

図 13-15 では、次の 3 つのイベントを示しています。

1. CoS 5 および DSCP 46 とマーキングされたパケットは、信頼されていないポートで受信されます。0（BE）の内部 DSCP を使用して、送信パケット CoS および DSCP を 0 に書き換えます。
2. CoS 5 および DSCP 46 とマーキングされたパケットは、信頼されているポート（CoS 信頼）で受信されます。CoS-to-DSCP マッピング テーブルで参照が実行され、CoS 5 が内部 DSCP 40 にマッピングされます。40 の内部 DSCP を使用して、送信パケット CoS を 5 に、DSCP を 40 に書き換えます。CoS-to-DSCP マッピング テーブルにはデフォルト値が設定されていますが、静的 CoS-to-DSCP マッピングに変更することができます。たとえば、CoS 5 は DSCP 46 にマッピングできます（EF）。
3. CoS 5 および DSCP 46 とマーキングされたパケットは、信頼されているポート（DSCP 信頼）で受信されます。46（EF）の内部 DSCP を使用して、送信パケット CoS を 5 に、DSCP を 46（EF）に書き換えます。

CDP 対応 Cisco IP Phone、Cisco CTS、Cisco IP Video Surveillance カメラ、Cisco Digital Media Player（Jabber などのソフトウェア クライアントとは対照的）の場合、CDP の条件付き信頼を使用し、ネットワークを介して信頼されているエンドポイントのマーキングを転送することをお勧めします。Cisco IP Phone を信頼するように選択した場合は、IP Phone がレイヤ 2 で PC トラフィックのみを再マーキングできるため、CoS を信頼する必要があります。信頼されているエンドポイントは、Unified CM から DSCP マーキングを取得します。エンドポイントの DSCP は、[クラスタ全体のパラメータ（システム：QoS）（Clusterwide Parameters (System - QoS)）] の Unified CM サービス パラメータで設定されます。

Unified CM では、CallManager サービスのサービス パラメータと SIP デバイスにのみ適用される SIP プロファイルの 2 つの場所にエンドポイントの QoS 設定が保存されます。QoS 設定の SIP プロファイル設定により、サービス パラメータ設定が上書きされます。これにより、Unified CM の管理者はエンドポイント グループの異なる QoS ポリシーを設定することができます（帯域幅管理の設計例（13-97 ページ）を参照）。エンドポイント登録時、Unified CM は、この QoS 設定を TFTP 経由で設定ファイルとしてエンドポイントに転送します。この設定ファイルには、QoS パラメータと、他の多くのエンドポイント固有のパラメータが含まれます。QoS のために、ビデオ エンドポイントには 2 つのカテゴリがあります。TelePresence エンドポイント（電話タイプ名で TelePresence のエンドポイント）と、このマニュアル内で「UC ビデオ エンドポイント」と呼ばれている他のすべての TelePresence 以外のビデオ エンドポイントです。図 13-16 では、シスコのビデオ エンドポイントの 2 つのカテゴリが DSCP を取得する方法について示します。これらのカテゴリは QoS とコール アドミッション制御にのみ適用されることに注意してください（Telepresence イマーシブ ビデオの Enhanced Location CAC（13-64 ページ）を参照）。

図 13-16　　シスコのエンドポイントによる DSCP の取得方法

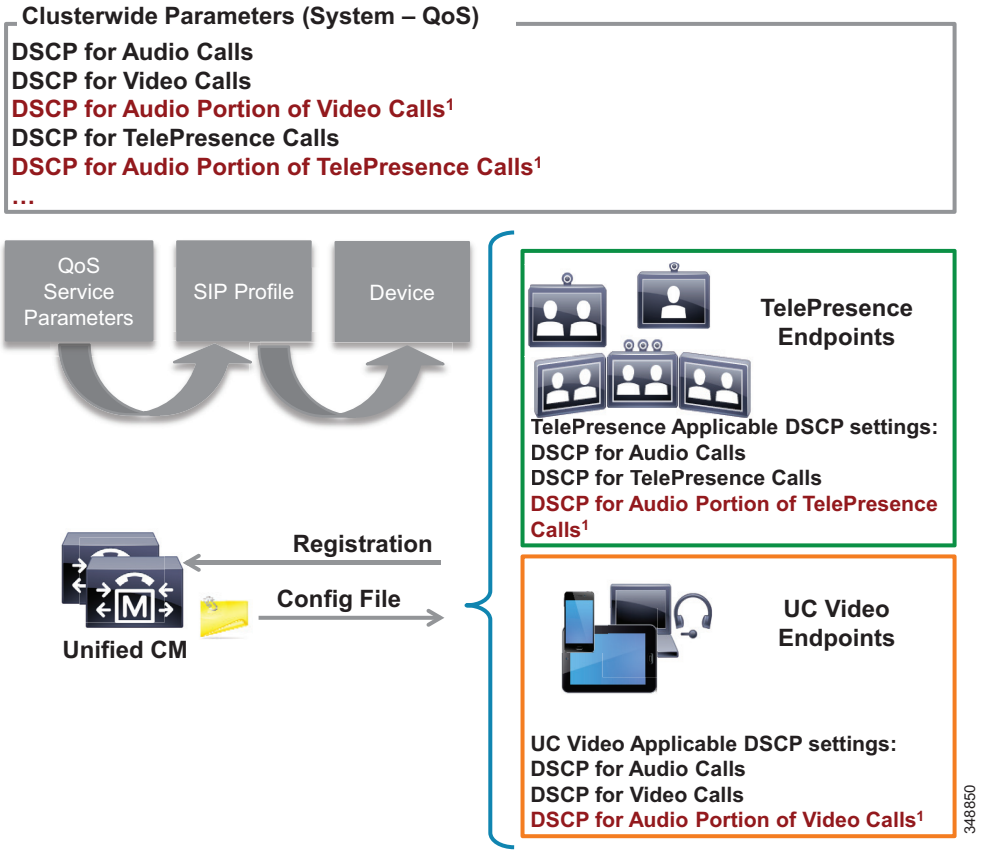


図 13-16 に示されている [ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）] および [TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）] のパラメータは、すべてのビデオ エンドポイントでは現在サポートされていません。これらのパラメータをサポートするエンドポイントのタイプについては、表 13-8 を参照してください。

設定ファイルは、設定時に CallManager サービス パラメータまたは SIP プロファイルの QoS パラメータと統合され、登録時にエンドポイントに送信されます。次に、エンドポイントは、エンドポイントのカテゴリに応じて、メディア ストリームの各タイプに正しい DSCP パラメータを使用します。表 13-7 に、DSCP パラメータ、エンドポイントのタイプ、ストリームの DSCP マーキングを決定するコール フローのタイプの一覧を示します。

表 13-7　基本的なコール フローの DSCP[1]

DSCP パラメータ	TelePresence エンドポイント	UC ビデオ エンドポイント	コール フロー
音声コールの DSCP（DSCP for Audio Calls）	○[2]	○	音声のみ
ビデオ コールの DSCP（DSCP for Audio Calls）	該当なし	○	ビデオ：ビデオ コールの音声とビデオ ストリーム。ただし、エンドポイントは [ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）] パラメータをサポートします。
ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）[3]	該当なし	○	ビデオ コールのオーディオ ストリーム：このパラメータをサポートするエンドポイントのみに適用されます
TelePresence コールの DSCP（DSCP for TelePresence Calls）	○	該当なし	イマーシブ ビデオ：イマーシブ ビデオ コールの音声とビデオ。ただし、エンドポイントは [TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）] パラメータをサポートします。
TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）[3]	○	該当なし	ビデオ コールのオーディオ ストリーム：このパラメータをサポートするエンドポイントのみに適用されます

1. マルチレベルのプライオリティおよびプリエンプション（MLPP）の DSCP 設定について、このドキュメントでは説明しません。MLPP 設定および QoS 設定の詳細については、最新版の『System Configuration Guide for Cisco Unified Communications Manager』を参照してください。
2. TelePresence ビデオ エンドポイントの中で、DX シリーズ エンドポイントのみが [音声コールの DSCP（DSCP for Audio Calls）] と対応する [TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）] をサポートします。ただし、エンドポイントが CE ソフトウェアを実行している場合に限ります。
3. このパラメータは、すべてのビデオ エンドポイントでは現在サポートされていません。このパラメータをサポートするエンドポイントのタイプについては、表 13-8 を参照してください。

表 13-8　ビデオと TelePresence コールのオーディオ部分の DSCP パラメータのエンドポイント サポート

ビデオ エンドポイント	ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）	TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）
8800 シリーズ	○	該当なし
8900 シリーズ	なし	該当なし
9900 シリーズ	なし	該当なし
Jabber	○[1]	なし
DX650、CE 以外のソフトウェアを持つ DX70 および DX80	○	○[2]
TX シリーズ	該当なし	○
IX シリーズ	該当なし	なし
CE 8.x ソフトウェア シリーズ（DX70、DX80、SX シリーズ、MX シリーズ G2、MX700、MX800）	該当なし	○
TC 7.1.4 ソフトウェア シリーズ（C シリーズ、プロファイル シリーズ、EX シリーズ、MX シリーズ G1）	該当なし	○
EX シリーズ（TC ソフトウェア）	該当なし	○

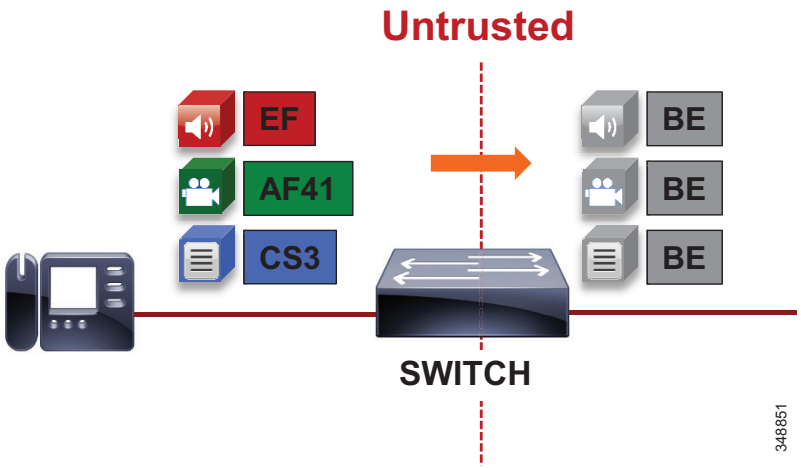
1. Jabber for Windows はグループ ポリシー オブジェクトを使用して PC のトラフィックをマーキングします。他のすべての Jabber クライアントは DSCP をネイティブにマーキングできます。
2. DX70 および DX80 が TelePresence コールの DSCP や TelePresence コールのオーディオ部分の DSCP を使用できるようにするには、CE ソフトウェアにアップグレードする必要があります。

次の新機能とシステム全体の機能が原因により、現在の DSCP のデフォルト値が推奨値であるとは限りません。この詳細については、帯域幅管理の設計例（13-97 ページ）で説明します。

信頼されていないエンドポイントとクライアント

信頼されていないエンドポイントの場合、スイッチ入力のパケットの DSCP マーキングは信頼されておらず、0（BE）に書き換えられます。図 13-17 では、音声、ビデオ、信号トラフィックをマーキングする信頼されていないエンドポイントと、送信パケットのこの値を書き換えるスイッチを示します。

図 13-17　信頼されていないエンドポイントの再マーキング



一般的に、PC、Mac、または携帯型モバイル デバイスでユーザが設定できるマーキングの信頼はお勧めしません。ユーザは自分のトラフィックをマーキングする場合（OS の管理権限を持つ場合）、プロビジョニングされた QoS ポリシーを悪用できます。たとえば、EF の DSCP がネットワークでプロビジョニングされている場合、PC ユーザはすべてのトラフィックを EF にマーキングするように設定できるため、ネットワーク プライオリティ キューをハイジャックしてリアルタイム以外のトラフィックを処理できます。このように悪用すると、企業全体のリアルタイム アプリケーションのサービス品質を簡単に台無しにできる可能性があります。一方、Windows 環境のグローバルポリシーオブジェクトなど、PC の QoS マーキングを一括で管理するように企業のコントロールをまとめると、PC のマーキングを信頼することも可能です。OSX が動作する Mac および携帯型モバイル クライアントの場合、マーキングを信頼するかどうかという問題が残ります。この方法については、「QoS の信頼、分類、マーキングでのオペレーティング システムの使用」セクションで説明します。一般的なルールでは、個人のコンピューティング デバイスは信頼しませんが、トラフィックを再マーキングする方法が必要です。

Jabber などのソフトウェア クライアントからのメディアおよびシグナリング ストリームが、適切に分類およびマーキングされるようにするため、信頼とは異なる方法が必要です。ある方法では、UDP と TCP ポートなどの特定のプロトコル ポートに応じて識別可能なメディアとシグナリング ストリームをマッピングし、ネットワーク アクセス リストを使用して、そのプロトコル ポート範囲に応じたシグナリングとメディア ストリームの QoS を再マーキングします。この方法は、メディアとシグナリング ポート範囲の割り当て時、Cisco Jabber クライアントがすべて同じように動作するため、すべての Cisco Jabber クライアントに適用されます。この方法は、パケット DSCP 再マーキングを実現するためのアクセス リストに応じたポリシーを作成するネットワークの使用から、Windows OS 自体（ここでは Jabber for Windows クライアントのみ適用）を使用したネットワーク内の PC のマーキングの信頼までカバーします。

また、信頼の問題のため、Cisco Jabber クライアントで QoS を簡単に実現できる方法として最も幅広く導入および推奨されています。Jabber クライアントには、Cisco Jabber for Windows、Cisco Jabber for Mac OS、Cisco Jabber for iPhone、Cisco Jabber for iPad、および Cisco Jabber for Android があります。

この概念はシンプルです。PC からのトラフィックがすべて信頼できるわけでないため、UDP ポート範囲に応じたメディアとシグナリング ストリームを特定し、それらを適切な値に再マーキングするために、ネットワーク アクセス レイヤ装置でアクセス リストが使用されます。この手法は実装が簡単で、幅広く導入できますが、安全な方法ではありません。

図 13-18 では、ネットワーク アクセス コントロール リスト（ACL）を使用した、DSCP への識別可能なメディアとシグナリング ストリームのマッピングを示します。

図 13-18　DSCP への UDP/TCP ポート範囲のマッピング

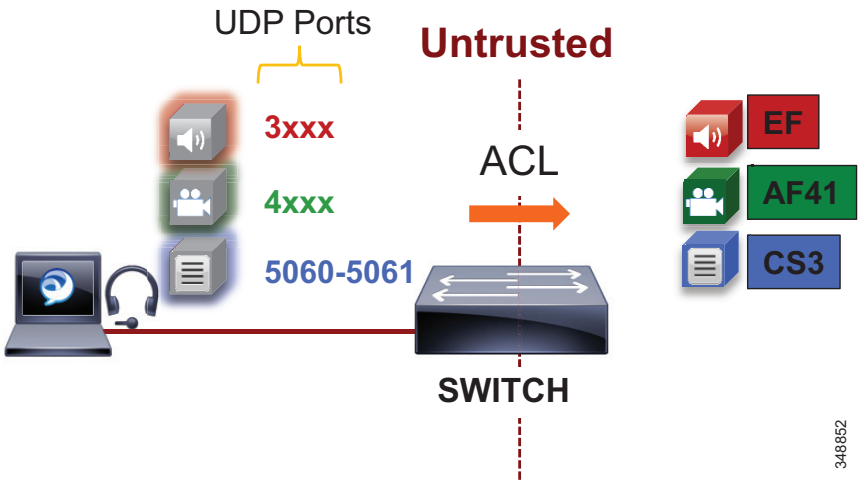


図 13-18 では、次の Jabber クライアントの ACL ベースの QoS ポリシー例を示します。

- DSCP EF への UDP ポート範囲 3xxx のマーキング
- DSCP AF41 への UDP ポート範囲 4xxx のマーキング
- DSCP CS3 への TCP ポート 5060-5061 のマーキング

（注）　次のアクセス コントロール リストの例は、Cisco Common Classification Policy Language（C3PL）に基づいています。C3PL をサポートしていないシスコ デバイスまたは C3PL の更新済みコマンドに対して同じポリシーを実現するには、特定のスイッチまたはルータの設定ガイドを参照してください。この設定は、モジュール型 QoS CLI-MQC、マルチレイヤ スイッチング（MLS）、および C3PL などの現在出荷されているすべてのスイッチに適用できます。

```
! ここでは、UDP ポート範囲と一致するように ACL を設定します。
   access-list 100 permit udp any range 3000 3999 any
   access-list 101 permit udp any range 4000 4999 any
   access-list 102 permit tcp any range 5060 5061 any

! ここでは、ACL と一致するようにクラスを設定します。
   class-map JABBER-VOICE
     match access-group 100
   class-map JABBER-VIDEO
     match access-group 101
   class-map JABBER-SIP
     match access-group 102

! ここでは、上記で設定したクラスと一致し、入力で JABBER の音声、ビデオ、および SIP シグナリングの DSCP を設定する policy-map を設定します。（一般的なデフォルト DSCP 値が使用されます。Jabber の推奨値については、設計上の考慮事項を参照してください。）
policy-map INGRESS-MARKING
   class JABBER-VOICE
     set dscp ef
   class JABBER-VIDEO
     set dscp af41
   class JABBER-SIP
     set dscp cs3
```

```
   class class-default

! ここでは、policy-map をインターフェイスに適用します。
  Switch (config-if)# service-policy input INGRESS-MARKING
```

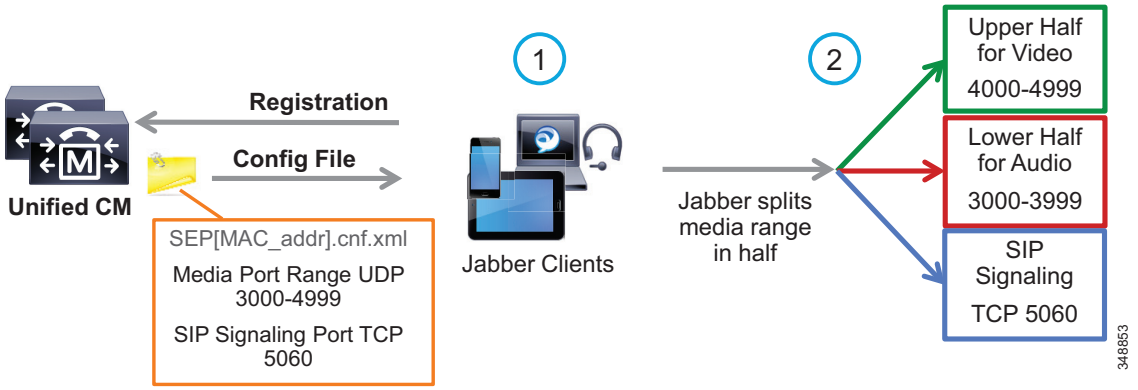
Cisco Jabber クライアントの QoS

前述したように、この方法では、IP アドレス、プロトコル、プロトコル ポート範囲に応じて Jabber クライアントからのさまざまなストリームを特定することで、メディアとシグナリングを分類します。いったん特定されると、シグナリングとメディア ストリームは、対応する DSCP で分類および再マーキングできます。プロトコル ポート範囲は Unified CM で設定し、デバイス登録時に使用するエンドポイントに転送されます。次にネットワークをアクセス コントロール リスト（ACL）経由で設定し、IP アドレス、プロトコル、プロトコル ポート範囲に応じてトラフィックを分類し、前述の適切な DSCP で分類したトラフィックを再マーキングできます。

Cisco Jabber は、UDP プロトコル ポート範囲に応じて識別可能なメディア ストリームおよび TCP プロトコル ポート範囲に応じて識別可能なシグナリング ストリームを提供します。Unified CM では、エンドポイントのシグナリング ポートは SIP セキュリティ プロファイルで設定しますが、メディア ポート範囲は Cisco Unified CM の管理ページの SIP プロファイルで設定します。

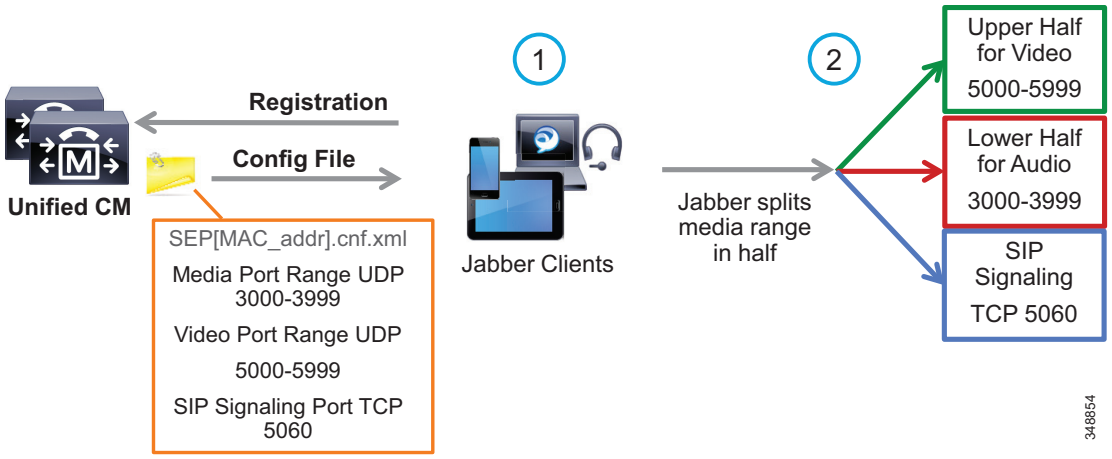
メディア ポート範囲の場合、すべてのエンドポイントおよびクライアントは、SIP プロファイル パラメータの [メディアポートの範囲（Media Port Range）] を使用して、メディアで使用される UDP ポートを取得します。デフォルトでは、メディア ポート範囲は [オーディオおよびビデオ用コモンポートの範囲（Common Port Range for Audio and Video）] で設定します。Jabber クライアントが Config ファイルでこのポート範囲を受け取ると、ポート範囲を半分に分割し、オーディオとビデオの両方のコールのオーディオ ストリームに下半分を使用し、ビデオ コールのビデオ ストリームに上半分を使用します。[メディアポートの範囲（Media Port Range）] > [オーディオおよびビデオ用コモンポートの範囲（Common Port Range for Audio and Video）] の設定を使用する場合、Jabber はビデオ UDP ポート範囲にビデオ コールのオーディオを配置しません。図 13-19 でこれについて説明します。

図 13-19　メディアとシグナリングのポート範囲：共通



Jabber は、[メディアポートの範囲（Media Port Range）] > [オーディオとビデオのポート範囲の分割（Separate Port Range for Audio and Video）] の設定も使用できます。この設定では、Unified CM の管理者は、図 13-20 に示すように連続しないオーディオとビデオ ポートの範囲を設定できます。

図 13-20　メディアとシグナリングのポート範囲:分割

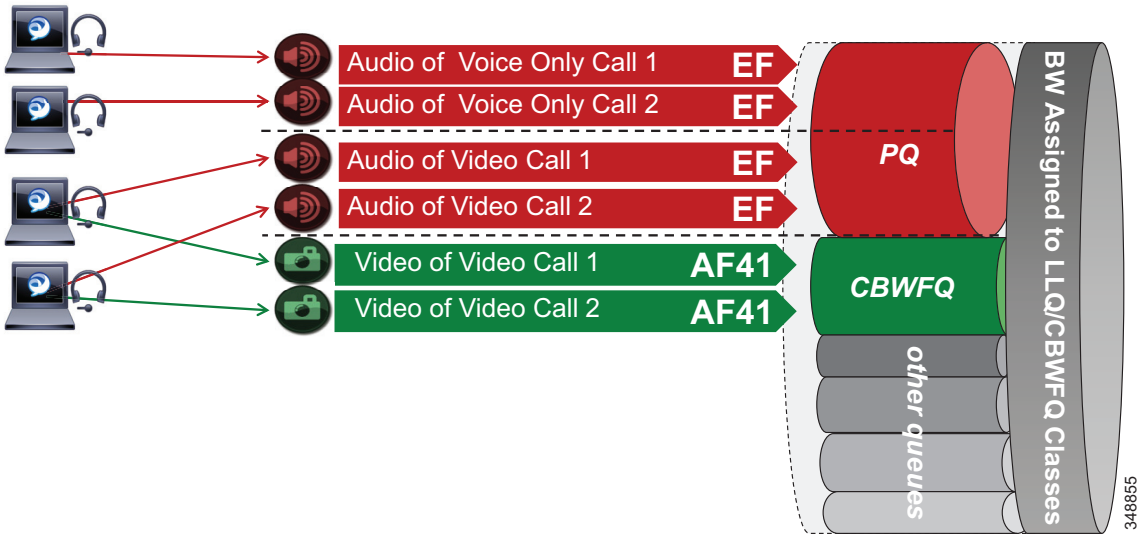


UDP ポート範囲の割り当てに関する Jabber クライアントの動作が原因で、QoS マーキングで Enhanced Locations Call Admission Control（EL-CAC）の帯域幅削減を適切にマッピングできないことがあります。CAC は音声プールからオーディオ専用コールの帯域幅を削減しますが、ビデオ コールのオーディオとビデオの両方の帯域幅がビデオ プールから削減されます。アドミッション制御ロジックに一致させるには、音声専用コールのオーディオ ストリームを EF としてマーキングする必要がありますが、ビデオ コールのオーディオとビデオの両方のストリームは AF41 とマーキングする必要があります。Cisco Jabber クライアントおよび UDP ポート範囲を使用して識別可能なメディア ストリームをマッピングする場合、音声専用コールのオーディオとビデオ コールのオーディオを区別することはできません。そのため、この手法は QoS のみを実現する場合に効果的です。したがって、EF としてオーディオを送信する Jabber クライアントからのビデオ セッションのオーディオを考慮するには、EF トラフィックのプライオリティ キューをオーバープロビジョニングするか、または代わりの DSCP を使用することをお勧めします。帯域幅管理の設計例（13-97 ページ）では、いくつかの方法について説明します。

注意　**セキュリティ警告**：ネットワーク レベルで QoS 分類に識別可能なメディア ストリームを使用すると、信頼モデルがアプリケーション自体に拡張されることは*ありません*。目的のアプリケーションのストリームに優先順位を付けること以外に、同じ識別基準（メディア ポート範囲）を使用するように他のアプリケーションを潜在的に設定できるため、ネットワークの優先順位付けを実現できる「可能性」があります。この目的外のトラフィックは CAC またはネットワークのプロビジョニングで考慮されないため、リアルタイムの会話全体に深刻な影響を与える可能性があります。制限付きポート範囲を定義して、必要に応じてメディア ストリームを特定することをお勧めします。

この手法を使用する場合、オーディオ トラフィック クラス（EF）に再マーキングされるこれらのビデオ コールのオーディオ部分、およびビデオ トラフィック クラス（AF4）に再マーキングされるビデオ部分が、状況に応じてネットワーク内でプロビジョニングされるようにすることが重要です。図 13-21 では、プライオリティ キュー（PQ）へのオーディオ トラフィックの配置、およびクラス ベースの重み付け均等化キュー（CBWFQ）へのビデオ トラフィックの配置の例を示します。Cisco Jabber エンドポイントのポート範囲で音声専用コールのオーディオとビデオ コールのオーディオを識別することはできないため、この手法を使用するオーディオはすべて EF と再マーキングされます。音声専用とビデオ コールの音声部分をサポートするには、PQ を適切にプロビジョニングすることが重要です。図 13-21 では、このプロビジョニングの例を示します。ネットワーク内でキューイングとスケジューリングをプロビジョニングするときの設計および導入に関する推奨事項については、WAN キューイングとスケジューリング（13-35 ページ）を参照してください。

図 13-21　ネットワークでの Jabber QoS のプロビジョニング



RFC 3551 に準拠して、RTCP がエンドポイントで有効な場合は、次に大きな奇数のポートが使用されます。たとえば、ポート 3500 で RTP ストリームを確立するデバイスは、ポート 3501 で同じストリームの RTCP を送信します。RTCP のこの機能は、すべての Jabber クライアントにも当てはまります。RTCP はほとんどのコール フローに共通しており、ストリームの統計情報用として一般的に使用され、ビデオ コールのオーディオとビデオを同期して適切なリップシンクを実現します。ほとんどの場合、ビデオおよび RTCP は、エンドポイント自体または電話の共通プロファイル設定で有効または無効にできます。

分類とマーキングでのネットワークの活用

Jabber クライアントで作成した識別可能なメディアおよびシグナリング ストリームに基づいて、共通ネットワーク QoS ツールを使用して、これらのクラスに従ってトラフィック クラスを作成し、パケットを再マーキングできます。

これらの QoS メカニズムは、アクセス レイヤ（アクセス スイッチ）などの異なるレイヤで適用できます。これは、ディストリビューション、コア、またはサービスの WAN エッジのエンドポイントおよびルータ レベルに最も近いレイヤです。分類および再マーキングの実行場所に関係なく、エンドツーエンドの Per-Hop Behavior を実現するために DSCP を使用することをお勧めします。

前述したように、Cisco Unified CM により、SIP エンドポイントで利用されるポート範囲は、SIP プロファイルで設定できます。一般的なルールとして、ポート範囲が最小 100 ポート（たとえば、3000 ～ 3099）あれば、ほとんどのシナリオで足ります。さまざまなオーディオ、ビデオ、および関連する RTCP ポートに十分なポートを割り当てられるのであれば、範囲を狭く設定することができます（RTCP は範囲内で奇数のポート上で実行されます）。

（注）　SCCP 音声専用エンドポイントが導入されたネットワークで Jabber クライアントを導入する場合、SCCP エンドポイントは、音声専用コールに対して設定不可能なハードコードされた範囲（16384 ～ 32767）を使用します。このため、SIP デバイスのメディア ポート範囲を変更しない場合は、SCCP 音声専用コールが SIP ビデオ対応エンドポイント コールと同じ範囲上で実行されます。SCCP を使用するように設定されたエンドポイントでコラボレーション ソリューションを導入する場合、16384 ～ 32767 の範囲外にある Jabber クライアントのメディア ポート範囲を設定することをお勧めします。3000 ～ 4999 のビデオ対応 Jabber クライアントと 3000 ～ 3999 の音声専用 Jabber クライアントの上記の例は、SCCP エンドポイントの重複を回避するのに非常に役立ちます。

重複を回避するための推奨事項は、他の SIP ベースのビデオ エンドポイントにも適用されます。SCCP ベースのオーディオ エンドポイント範囲での重複を回避するには、SIP ベースのビデオ エンドポイントを、SCCP ベースのオーディオ ポート範囲（16384 ～ 32767）または Jabber クライアント メディア ポート範囲で重複しないポート範囲に割り当てる必要もあります。

アクセス レイヤ（レイヤ 2 定義）

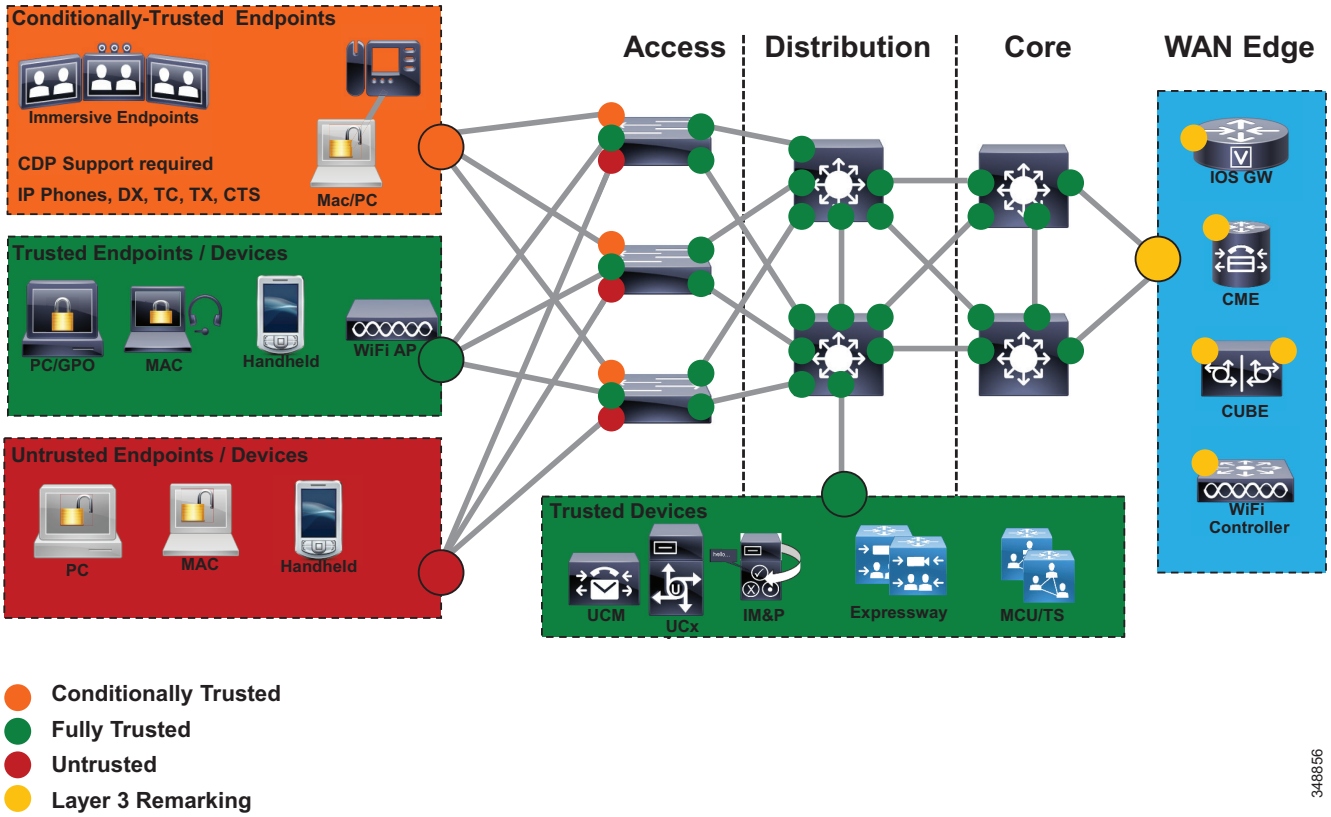
トラフィックの分類にアクセス レイヤを使用する場合、ネットワークへのトラフィックの入力時に分類が行われるため、入力に合わせてフローが識別されます。QoS ポリシーが WAN と LAN 内にも適用される環境では、すべてのアップストリーム コンポーネントが、処理時にトラフィック マーキングを使用できます。入力時の分類により、各種エンドポイントに応じてさまざまな方法を使用できます。IP Phone などの物理的なエンドポイントは、Cisco Discovery Protocol（CDP）または Link Layer Discovery Protocol-Media Endpoint Discovery（LLDP-MED）のようなメカニズムを使用して信頼関係を確立することができます。デバイスが信頼済みと識別されると、そのデバイスから受信する QoS マーキングはネットワーク全体で信頼されます。

ネットワークのアクセス レイヤで QoS ポリシーを設定すると、大量のデバイスの設定が必要になる場合があるため、新たな運用上のオーバーヘッドが発生する可能性があります。QoS ポリシー設定は、テンプレートを通じてアクセス レイヤの各種スイッチ全体で標準化する必要があります。設定導入ツールを使用すると、手動設定の負担を軽減できます。

ディストリビューション、コア、サービスの WAN エッジ（レイヤ 3 定義）

QoS マーキングが行われる場所は、レイヤ 3 のルート設定済み境界にあります。キャンパス ネットワークでは、レイヤ 3 は、アクセス、ディストリビューション、コア、またはサービス WAN エッジ レイヤでもかまいません。信頼境界を構築し、アクセスで分類および再マーキングすることをお勧めします。次に、ネットワークのディストリビューションとコア経由で信頼し、WAN エッジで最終的に再分類および再マーキングします。レイヤ 3 スイッチング コンポーネントを導入していない支店などの小規模なネットワークの場合、QoS マーキングは WAN エッジ ルータで適用できます。レイヤ 3 では、QoS ポリシーがレイヤ 3 ルーティング インターフェイスに適用されます。ほとんどのキャンパス ネットワークでは、VLAN インターフェイスですが、ファスト イーサネットまたはギガビット イーサネット インターフェイスの場合もあります。図 13-22 では、ネットワーク内の場所（アクセス、ディストリビューション、コア、および WAN エッジ）に関連して、さまざまなタイプの信頼が適用されるネットワークの領域を示します。

図 13-22　信頼と適用：ネットワーク内の場所



QoS の信頼、分類、およびマーキングに対するオペレーティング システムの活用

Cisco Jabber クライアントの QoS の信頼で別の方法を使用すると、アプリケーションが実行されるオペレーティング システムが、アプリケーションの要求に応じてメディアとシグナリングの QoS をマーキングできます。この方法の利点は、ネットワーク オペレータがオペレーティング システム自体に QoS の信頼モデル拡張して、次に QoS マーキングを「信頼」し、ネットワークを介してそのマーキングを送れるようにネットワークを設定できることです。これは、企業が QoS 信頼を Windows PC、Mac OS、携帯型デバイスに拡張する際の一般的な方法ではありません。それは、この方法では、認証されたアプリケーション通信のトラフィックだけでなく、デバイスのトラフィックをすべて信頼するためです。このようなアプリケーションをこれらのデバイスにインストールして使用すると、プライオリティ QoS が「ハイジャック」され、QoS 導入の本来の目的が失われることがあります。管理上のグローバル ポリシーを介して、管理者は、OS が不要なアプリケーションまたは設定を受け入れないように、Windows OS など、一部のオペレーティング システムまたはユーザ アクセス コントロールを管理できます。このような場合、QoS 信頼でこの方法の使用が許可される場合があります。

Windows 7 および 8 オペレーティング システムでは、特定のポリシーを設定する必要があります。Mac OS、Apple iOS、および Android デバイスでは、OS は、特定のポリシーを設定する必要はなく、アプケーションの要求時にネイティブにマーキングします。

次のセクションでは、Cisco Jabber クライアントと、各オペレーティング システムがアプリケーションの QoS 分類とマーキングに対してどのように機能するかについて説明します。これらのセクションで説明する内容はすべて、レイヤ 2 サービス クラス（CoS）ではなく、レイヤ 3 DSCP マーキングに関連しています。

Windows 7 と 8 での分類

Microsoft Windows 7 と Windows 8 では異なる手法が採用されています。オペレーティング システムによる QoS マーキングでは、Microsoft のセキュリティ強化が原因で、ユーザ アカウント制御（UAC）により、通常のアプリケーションが IP パケットの DSCP マーキングを設定できません。これはセキュリティ上の問題と見なされます。QoS/DSCP マーキングの許可に推奨されるオプションでは、グループ ポリシー オブジェクト（GPO）と呼ばれる Microsoft グループ ポリシーを使用して、特定のアプリケーションがプロトコル数およびポート範囲に基づいてトラフィックをマーキングできるようにします。このマニュアルですでに説明したように、Cisco Jabber で作成された識別可能なトラフィック ストリームを GPO とともに使用すると、Windows オペレーティング システムが特定のアプリケーション（CiscoJabber.exe など）で送信されたトラフィックをマーキングするように指示できます。すべての GPO と同様に、QoS GPO を設定できるのは管理者のみであるため、GPO によって許可されたアプリケーションのみが、オペレーティング システムを経由して QoS をマーキングできます。

ほとんどの企業のネットワーク管理者は、PC など、データ VLAN のデバイスの QoS マーキングを信頼しません。通常、データ VLAN のトラフィックはすべて、アクセス レイヤの入力で DSCP が 0（ベスト エフォート）に再マーキングされ、次に、UCP ポート範囲またはプロトコルなどの他の基準に基づいた DSCP に再マーキングされます。非常に厳格な OS ポリシーおよびネットワーク アクセス ポリシーを持つ一部の企業は、完全に制御できるオペレーティング システムのマーキングを信頼することがあります。この場合、Windows 7 または 8 のオペレーティング システムが Cisco Jabber クライアントなどの特定のアプリケーションの QoS トラフィックをマーキングできるようにすることで、QoS GPO に利点があります。

Cisco Jabber for Windows を導入する企業で、QoS 信頼のこのレベルを提供する場合、この方法を選択することもできます。

⚠
注意　**セキュリティ警告**：純粋な Windows 7（およびそれ以降のバージョン）環境で、GPO のみを使用すると、企業はこの Windows デバイスから送信されるすべてのデータを無条件で信頼できます。実際の環境でこのような同種環境が存在することはほとんどないため、同一の VLAN またはアクセス レイヤの類似ポートにある他のオペレーティング システムとデバイスから GPO ベースのデバイスの信頼モデルを分離するには、特別な努力が必要です。

GPO は、オペレーティング システムが、プロトコル、ポート、およびアプリケーションの実行可能ファイルに基づいて、特定のアプリケーションの QoS をマーキングできるようにするネットワーク アクセス リストに非常に類似しています。図 13-23 では、Jabber for Windows を使用した Windows 7 および 8 での QoS 再マーキングのプロセスについて説明します。

図 13-23　グループ ポリシー オブジェクト

図 13-23 で説明しているプロセスは、IP アドレス範囲（または任意のアドレス）、プロトコル（UDP）、およびポート範囲（オーディオは 3000 ～ 3999、ビデオは 4000 ～ 4999）を定義する QoS グループ ポリシーから始まります。一度設定して OS に適用したら、Jabber for Windows クライアントは登録時に Unified CM からその設定をダウンロードし、SIP プロファイル メディア ポート範囲として共通を適用します。そこから、Jabber for Windows クライアントがコールを行う場合、Unified CM から提供されるメディア ポート範囲します。ただし、Windows OS に適用された GPO はそのポリシーを適用し、UDP ポート 3000 ～ 3999 からオーディオのメディア トラフィックを取得して EF に再マーキングし、UDP ポート 4000 ～ 4999 から取得して AF41 に再マーキングします。トラフィックが OS に残らないため、パケットには適用したマーキングが含まれます。これらのマーキングを信頼し、ネットワーク経由で送れるかはネットワーク次第です。図 13-23 では、メディア ポート範囲について SIP プロファイルで非連続ポート範囲として分割ポートを使用する場合の類似した GPO も示します。

Mac OS での分類

Cisco Jabber for Mac は、オペレーティング システムに対して DSCP QoS マーキングをネイティブに要求し、特定のポリシーを設定せずにトラフィックをマーキングします。

Apple iOS での分類（iPhone と iPad）

Cisco Jabber for iPad および Cisco Jabber for iPhone は、オペレーティング システムに対して DSCP QoS マーキングをネイティブに要求し、特定のポリシーを設定せずにトラフィックをマーキングします。

Android での分類

Cisco Jabber for Android は、オペレーティング システムに対して DSCP QoS マーキングをネイティブに要求し、特定のポリシーを設定せずにトラフィックをマーキングします。

エンドポイントの識別と分類の考慮事項と推奨事項

設計と導入の考慮事項と推奨事項:

- IP レイヤにエンドツーエンドで適用され、レイヤ 2マーキングよりも詳細で拡張性に優れているため、DSCP マーキングをできるだけ使用します。
- できるだけエンドポイントの近くにマーキングします。LAN スイッチ レベルがお勧めです。
- SCCP ベースのオーディオ エンドポイントが導入された環境に音声用およびビデオ用の Jabber を導入する場合は、16384 ～ 32767 の範囲（SCCP デバイス用にハードコードされた範囲）外で使用できるように Cisco Jabber エンドポイントのメディア ポート範囲を変更します。これは、UDP ポート範囲に基づいて DSCP を再マーキングするためにネットワーク ポリシーを作成するときの潜在的な重複を回避するためです。たとえば、音声専用（ビデオ無効）Jabber クライアントに 3000 ～ 3999 のポートを使用し、ビデオ対応 Cisco Jabber エンドポイントに 3000 ～ 4999 を使用します。
- Cisco Jabber クライアントで使用するメディア ポート数を最小化する場合、最小範囲として 100 個のポートを使用します。これは、RTCP、オーディオとビデオ用の RTP、BFCP、デスクトップ共有セッションのセカンダリ ビデオ用の RTP など、すべてのストリームに十分なポートを割り当て、同一コンピュータ上の他のアプリケーションと重複しないようにするためです。
- Enhanced Locations CAC を導入する場合は、AF41 *ではなく* EF がマーキングされた Jabber クライアントからのビデオのオーディオを考慮するようにオーディオ クラス（EF）をオーバープロビジョニングします。

レイヤ 3 DSCP の値にレイヤ 4 ポート範囲の識別可能なメディアおよびシグナリング ストリームをマッピングすると、Cisco Jabber クライアントに QoS を導入できます。Jabber クライアントでネットワーク アクセス コントロール リスト（ACL）またはオペレーティング システムを使用して、PC、Mac、または携帯型デバイスの QoS マーキングを信頼してネットワーク経由で送信すると、識別可能なメディアおよびシグナリング ストリームをマッピングできます。ネットワークの ACL 方式は OS の信頼方式を上書きするだけで、すべてのオーディオの再マーキングを強制し、信頼方式の使用目標を放棄するため、両方の方式を組み合わせることはお勧めしません。

WAN キューイングとスケジューリング

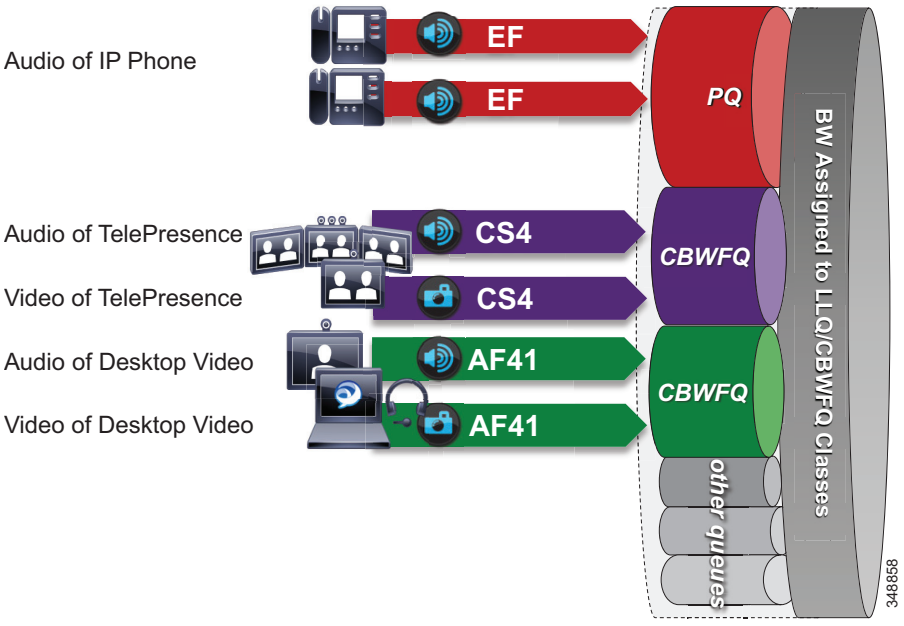
QoS に関するシスコの推奨事項は、ビデオについて過去数年間で少し変化しています。従来のビデオは、デスクトップ ビデオとイマーシブ TelePresence ビデオの 2 種類に分類されています。識別と分類（13-17 ページ）セクションで説明されているように、Unified CM はこれらのエンドポイントのビデオ エンドポイント タイプとビデオ ストリームを区別できます。このため、ネットワーク管理者は、これら 2 種類のエンドポイントのビデオを別々に処理できます。従来、推奨 DSCP マーキングは、デスクトップ ビデオには AF41、TelePresence ビデオ（イマーシブ ビデオ）には CS4 が割り当てられています。これらの値は RFC 4594 に準拠しています。図 13-24 では、WAN での分類およびスケジューリングの一般的な手法について説明します。この識別と分類の手法は長年にわたり導入されていますが、これら 2 つのクラスのトラフィックが、Cisco IOS のクラスベースの重み付け均等化キューなど、レートベースのキューを分離するために適用される場合には欠点があります。

（注）　このセクションでは、WAN の Quality of Service（QoS）（3-39 ページ）セクションで詳細に説明している、Cisco IOS の異なるキューイングとスケジューリング技術について解説します。ここでは技術を十分に理解していることを前提として、これらの技術のいくつかについて説明し、その内容は Cisco IOS のさまざまなキューイングとスケジューリングのメカニズムを使用する際のベスト プラクティスおよび推奨事項に焦点を当てます。

デュアル ビデオ キュー手法

WAN 内のトラフィックのスケジューリングとキューイングに関するこの手法では、音声コールのオーディオは EF とマーキングされ、PQ がこのトラフィックに割り当てる帯域幅に関する厳格なポリサーを使用して、プライオリティ キュー（PQ）に配置されます。ビデオ コールは、デスクトップ タイプ ビデオ用の AF41 クラスと、TelePresence ビデオ（イマーシブ）用の CS4 クラスの 2 つのクラスに分けられます。これらのクラスはそれぞれ個別のクラスベースの重み付け均等化キューに分けれます。

図 13-24　デュアル ビデオ キュー手法



デュアル ビデオ キュー手法には次の欠点があります。

- TelePresence（イマーシブ）ビデオとデスクトップ ビデオで異なるキュー
- 複雑なプロビジョニング：複数のビデオ キューを管理し、ビデオ全体ではなく、各ビデオ タイプで帯域幅割り当てを分ける必要があります
- 準最適な帯域幅の使用：あるクラスのビデオがすべての帯域幅を使用していない場合、他のビデオ キューではなく、インターフェイス上の他のすべてのキューで残りの帯域幅を使用できるようになります。そのため、2 つの異なるクラスのビデオが、すべてのビデオ帯域幅割り当てを効率的に共有するのに最適ではありません。

ビデオ コールのオーディオ部分に関連する、この手法のその他の考慮事項は次のとおりです。

- ビデオ コールのオーディオは、ビデオ キューのパケット損失の影響を受ける可能性があります。
  - ビデオ コールのオーディオとビデオ ストリームに同一の DSCP

    デフォルトでは、ビデオ コールのオーディオとビデオの両方とも同じ DSCP 値がマーキングされます。その結果、オーディオとビデオ ストリームの両方が、ビデオ キューの輻輳で均等に影響を受けます。ビデオのパケット損失が発生すると、パケット損失が発生しなくなるまで、ビデオ エンドポイントがレート調整を許容レベルまで下げるときに、ビデオ品質が少し低下する場合があります。オーディオは一定のビット レート メディアであり、ビデオと同じレート調整機能はありません。そのためオーディオの場合、この低下は、ビデオ キューのパケット損失がなくなるまで、ユーザが通信できなくなることを意味します。オーディオへの影響は、ビデオへの影響よりもユーザ エクスペリエンスに大きな影響があります。ビデオが影響を受けている場合、ビデオのパケット損失が発生しても、ユーザは会議や会話を継続することができます。両方のメディアの特性に関する詳細については、音声とビデオ（13-6 ページ）を参照してください。
  - これまで、ビデオ コールのオーディオおよびビデオ ストリームでは、2 つのストリーム間で大きな遅延差が生じないようにするため、同じ DSCP 値がマーキングされていました。そうしないと、ビデオ エンドポイントはオーディオとビデオを適切に同期できませんでした。すべてのシスコ エンドポイントに RTCP を実装することで、RTCP がビデオ コールのオーディオとビデオ間の同期化を適切に実行するため、心配する必要がなくなりました。当然ですが、これにはビデオ エンドポイントで RTCP を有効にする必要があります。
- 信頼されていないデバイスのオーディオ ストリームの分類は、音声専用コールとビデオ コール間で区別することはできません。
  - メディア ストリームの識別は、信頼されていないエンドポイントおよびクライアントには困難です。前述のように、エンドポイントまたはクライアントが信頼されていない場合は、別の方法で識別する必要があります。アクセス リストなどの別の方法では、多くの場合、ビデオ コールのオーディオから音声専用コールのオーディオを区別し、2 種類のオーディオを別々に分類することは困難です。そのため、両方の種類のコールのオーディオすべてを単一の DSCP 値でマーキングする必要があります。これにより、包括的な手法を作成できますが、マーキングがさらに難しくなります。

単一ビデオ キュー手法

統合したコラボレーション メディアおよびデータ ネットワーク全体での複数の種類のビデオの管理では、廃棄率の異なる複数の DSCP を持つ単一レートベースのキューを使用することを新たにお勧めします。WAN のビデオ トラフィックをスケジューリングするこの新しい手法では、単一のビデオ キューを、AF41、AF42、および AF43 を使用して 2 または 3 の AF4 廃棄率に設定します。この場合、AF43 の廃棄優先度または廃棄率は AF42 よりも高く、AF42 の廃棄優先度または廃棄率は AF41 よりも高くなります。階層型廃棄優先のこのサービス クラスを持つ単一のビデオ キューの前提は、あるクラスのビデオがキュー内の帯域幅を使用していない場合、キューの残りの帯域幅を他の DSCP で使用できるというものです。これにより、2 つの異なるレートベースのキューの CS4 TelePresence ビデオおよび AF41 デスクトップ ビデオを使用した以前のキューイング手法の最適ではない帯域幅使用率の主な欠点の 1 つが解決されます。

最適化されたビデオ帯域幅使用率に関する多くの異なる戦略は、階層型 DSCP 廃棄率を使用するこの単一ビデオ キューに基づいて設計することができます。単一クラスベースの重み付け均等化キュー（CBWFQ）で AF41 と AF42 の 2 つの DSCP 値を持つ、TelePresence ビデオとデスクトップ ビデオの 2 種類の同じビデオを使用すると、この新しい QoS キューイング手法の例を簡単に説明できます。図 13-25 に、このアプローチを示します。

図 13-25　単一ビデオ キュー手法

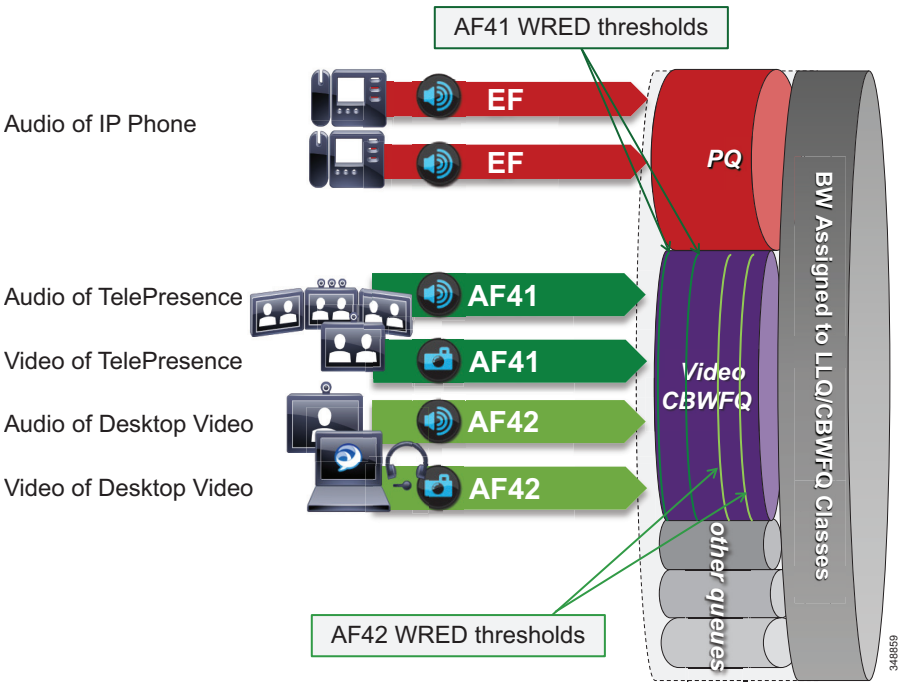


図 13-25 では、音声コールのオーディオは EF とマーキングされ、PQ がこのトラフィックに割り当てる帯域幅に関する厳格なポリサーを使用して、プライオリティ キュー（PQ）に配置されます。ビデオ コールは、TelePresence ビデオの AF41 とデスクトップ ビデオの AF42 の 2 つのクラスに分けられます。重み付けランダム早期検出（WRED）で CBWFQ を使用すると、管理者は、AF41 に対して AF42 の廃棄優先度を調整できるため、キューがいっぱいになって輻輳が発生したとき、AF42 パケットが AF41 よりも高い確率でキューから廃棄されます。WRED の機能の詳細については、WAN の Quality of Service（QoS）（3-39 ページ）を参照してください。

この例では、すべてのビデオに対して DSCP ベースの WRED と単一 CBWFQ を使用する管理者が、輻輳時のパケット損失から、別の種類のビデオ（デスクトップ）よりも、ある種類のビデオ（TelePresence ビデオ）を保護する方法について説明します。この「単一」ビデオ キュー手法では、デュアル ビデオ キュー手法とは異なり、ある種類のビデオがキューの帯域幅を使用していない場合、他の種類のビデオが、必要に応じてキューの帯域幅全体の完全なアクセス権を得られます。これは、パーベイシブ ビデオの導入を考える際の重要なポイントです。

ビデオ コールのオーディオに関する考慮事項

上記の単一ビデオ キューの例では、あるクラスと別のクラスの CBFWQ が同じである場合、あるクラスのビデオの未使用帯域幅を、別のクラスのビデオがすべて使用できる方法についてのポイントを簡単に説明しています。これにより、デュアル ビデオ キュー手法の欠点の 1 つが解決されます。ただし、これにより、ビデオ コールのオーディオ部分の他の考慮事項が解決されるわけではありません。前述のとおり、2 つの主な欠点があります。

- ビデオ コールのオーディオは、ビデオ キューのパケット損失の影響を受ける可能性があります。
- 信頼されていないデバイスのオーディオ ストリームの分類は、音声専用コールとビデオ コール間で区別することはできません。

これらの問題を解決する戦略とは、すべてのオーディオがソリューション全体で完全優先転送（EF）の単一の値でマーキングされるようにすることです。この方法では、オーディオ ストリームが音声専用コールまたはビデオ コールに関連付けられるかどうかに関係なく、常に同じ単一の値にマーキングされます。この方法では、ビデオ コールのオーディオの優先順位はビデオよりも上位になるため、ビデオ キューでパケット損失の対象にはなりません。また、Jabber クライアントなどの信頼されていないデバイスでの識別問題も解決します。クライアントのマーキングはネットワーク アクセス レイヤで信頼されないため、ネットワークで音声専用コールのオーディオ ストリームとビデオ コールのオーディオを区別する効果的な方法はありません。そのため、すべてのオーディオが同じ単一の値でマーキングされるこの新しいモデルに移行すると、ネットワークの優先順位付けおよびトラフィックの処理が簡単になります。

（注）　信頼されているエンドポイントが DSCP を取得する方法、ビデオのオーディオ部分または TelePresence エンドポイントに DSCP を設定する方法、この差別化をサポートするエンドポイントに関する詳細については、信頼されているエンドポイント（13-19 ページ）を参照してください。また、信頼されていないエンドポイントとクライアント（13-24 ページ）では、Jabber クライアントに DSCP を設定する方法についても説明します。

ソリューション全体でこれを総合的に実現するのは、すべてのオーディオを EF の DSCP にマーキングするのに必要ないくつかの条件次第です。

- エンドポイントは、すべてのオーディオを EF とマーキングできるように、Unified CM で [ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）] および [TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）] の QoS 設定をサポートする必要があります。エンドポイント サポートの詳細については、表 13-8 を参照してください。
- Jabber クライアントは、信頼されているまたは信頼されていない実装ですべてのオーディオを EF にマーキングするようにサポートできます。

- Enhanced Locations CAC は、すべてのオーディオを EF にマーキングしながら実装できます。ELCAC は適切な DSCP 設定を使用し、音声およびビデオ CAC プールが表すキューを保護します。ビデオ コールのオーディオ ストリームの DSCP を変更するには、ELCAC がビデオ コールの帯域幅を差し引く方法を更新する必要があります。[ビデオ コールのオーディオ プールからオーディオ帯域幅を差し引く（Deduct Audio Bandwidth from Audio Pool for Video Call）] と呼ばれる CallManager サービスのコール アドミッション制御セクションにあるサービス パラメータを設定すると、これを実行できます。このパラメータは、[True] または [False] に設定できます。
  - [True]：Cisco Unified CM は、ビデオ コールのオーディオとビデオの帯域幅割り当てを個別のプールに分けます。ビデオ コールのオーディオ部分の帯域幅割り当てはオーディオ プールから差し引かれ、ビデオ コールのビデオ部分はビデオ プールから差し引かれます。
  - [False]：Cisco Unified CM は従来の動作を適用します。ビデオ コールのオーディオとビデオの帯域幅割り当てをビデオ プールから差し引きます。これがデフォルトの設定です。

ビデオのすべてのオーディオを EF にマーキングする際のアドミッション制御機能の詳細については、音声プールからのすべてのオーディオの差し引き（13-54 ページ）の ELCAC セクションを参照してください。

状況対応型ビデオ

組織全体でビデオを広範囲に導入しようとする場合、帯域幅の一般的な制約により、利用可能な帯域幅および最繁時のビデオ コールの数に基づいて、一日の最繁時に実現できるビデオ解像度のレベルが決定されます。この問題を解決するために、コラボレーション メディアの識別および分類に関する戦略を考慮しながら DSCP ベースの WRED を持つ単一のビデオ キューを使用して、ビデオの種類を状況対応型ビデオに限定します。

状況対応型ビデオとは、任意の時点で利用可能な WAN 帯域幅リソースに応じて、最適な品質を実現したビデオを示します。これを実現するには、いくつかの要件を満たす必要があります。

- 状況対応型ビデオ エンドポイント グループの選択
- WAN の確保は、廃棄優先度が AF41、AF42、および AF43 の AF4 DSCP クラス サービスで DSCP ベースの WRED を使用して、単一のビデオ キューで設定されます。
- AF42 を使用する状況対応型エンドポイントのビデオの識別と分類
- AF41 を使用する他のすべてのビデオ エンドポイントの識別と分類

プロビジョニングとアドミッション制御

帯域幅をプロビジョニングし、適切なビット レートがさまざまなエンドポイント グループ間でネゴシエートされるようにすることは、帯域幅管理の重要な側面です。Unified CM 環境では、ビット レートは Unified CM 経由でネゴシエートされます。リージョンの概念を使用し、特定のコール フローの最大オーディオ ビット レートおよび最大ビデオ ビット レートを設定します。ここでは、ビデオおよび TelePresence の最大ビット レートに注目します。

Unified CM のリージョン

Unified CM のロケーション（Enhanced Locations Call Admission Control（13-42 ページ）を参照）は、*リージョン*とともに、コール フローの特性を定義します。リージョンは、2 つのデバイス間で使用される圧縮とビット レートの種類（8 kbps または G.729、64 kbps または G.722/G.711 など）を定義します。ロケーション リンクは、デバイス間のパスで利用可能な帯域幅の容量を定義します。システム内の各デバイスおよびトランクを（デバイス プールを使用して）リージョンに割り当て、（デバイス プールまたはデバイス自体に直接設定した値を使用して）ロケーションに割り当てます。

- リージョンにより、ビデオ コールの帯域幅を設定できます。リージョンのオーディオ制限により、高いビット レートのコーデックが除外される可能性があります。ただしビデオ コールでは、ビデオの制限により、ビデオの品質（解像度と転送速度）が抑制されます。
- ロケーションは、対象のリンクのすべてのコールで利用可能な総帯域幅の容量を定義します。リンク上でコールが確立すると、そのリンクで許可された総帯域幅からそのコールのリージョンの値を差し引く必要があります。

デバイス グループの最大ビデオ ビット レート（ビデオ解像度）を管理するリージョン マトリックスを作成すると、特定のデバイス グループがネットワーク帯域幅を過剰に使用しないようにすることができます。リージョン マトリックスを作成するためのガイドラインは次のとおりです。

- 最大ビデオ ビット レート カテゴリにデバイスをまとめます。
- グループの数が少ないほど、帯域幅要件の計算が簡単になります。
- デフォルトのリージョン設定を検討し、マトリックスを簡単にして、リージョン内およびリージョン間のデフォルト値を入力します。

リージョン設定の詳細については、Enhanced Locations Call Admission Control（13-42 ページ）を参照してください。

表 13-9 では、4 つのデバイス グループについて最大ビデオ ビット レートのリージョン マトリックスの例を示します。

（注） 表 13-9 は、デバイスのグループ化方法と、デバイス グループ間の通常の解像度に適した最大ビット レートのほんの一例です。

表 13-9　グループ リージョン マトリックスの例

エンドポイント グループ	従来（小型画面）	Jabber	ルーム システム + スマート デスクトップ	イマーシブ + MCU
従来（小型画面）	800 kbps	800 kbps	800 kbps	800 kbps
Jabber	800 kbps	1,500 kbps	1,500 kbps	1,500 kbps
ルーム システム + スマート デスクトップ	800 kbps	1,500 kbps	2,500 kbps	2,500 kbps
イマーシブ + MCU	800 kbps	1,500 kbps	2,500 kbps	12,000 kbps

表 13-9 の 4 つのグループは次のとおりです。

- 従来（小型画面）：小型の低解像度画面を備えた従来のエンドポイント、またはビット レートが 800 kbps に制限された他のデバイスです。
- Jabber：通常、導入されているビデオ対応エンドポイントの最大グループにあたるため、状況対応型ビデオ手法の利点があります。状況対応ビデオと分類されると、レートが 1,500 kbps（720p@30fps）まで上がり、パケット損失に応じてレートが下方調整されます。
- ルーム システム + スマート デスクトップ：Cisco MX、SX、C、またはプロファイル シリーズなどのルーム システムです。また、Cisco DX および EX シリーズなどのスマート デスクトップ エンドポイントです。最大ビデオ ビット レートが 2,500 kbps あり、通常、これらのエンドポイントは 720p@30fps に対応しています。
- イマーシブ + MCU：大規模な Cisco TX または IX シリーズ エンドポイントおよび MCU で、最大 12 Mbps に設定されています。他の TelePresence デバイスおよび MCU に変換すると約 1080p@30fps です。

帯域幅のプロビジョニングに関するリージョンの他の考慮事項：

- 最初の考慮事項は、異なるリージョン内設定とリージョン間設定を指定するかどうです。これは、サイトごとのリージョン設定が必要かどうかによって決まります。ここでの考え方は、リージョン内とリージョン間でオーディオまたはビデオの異なるビット レートを設定する場合、サイトごとにリージョンを設定する必要があります。このため、リージョン設定が、サイト数（N）にビデオ グループ数（X）を掛けた値まで増えます。N*X = 必要な平均リージョン数。リージョン内およびリージョン間のオーディオとビデオのビット レートが同じ場合、必要になるのはビデオ グループのリージョン数（X）のみです。
- 可能であれば、音声専用 IP Phone に設定されたリージョンを再使用します。
  - オーディオ コーデック設定は共有されるため、複数のビデオ コールで異なるオーディオ コーデックを使用する必要がある場合は、新しいリージョンを設定する必要があります。たとえば、音声専用デバイスが WAN 上の G.729 オーディオ コーデックを、LAN 上の G.711 または LAN G.722 を使用する場合、ビデオ デバイスは G7.11 または G.722 を常に使用しますが、音声専用エンドポイントおよびビデオ エンドポイントはリージョンを共有できません。そのため、各サイトはデバイス グループごとにリージョンが必要になります。サイト数 = N で、ビデオ リージョン グループ数 = 4 + 音声専用リージョン グループのため、N*4 が必要なリージョン数になります。設定サポート用に Prime Collaboration のプロビジョニング ツールまたは一括管理ツールを使用します。
  - リージョン内とリージョン間の両方のコールと音声専用コールに対して単一のオーディオ コーデックを使用する場合、サイトごとのリージョンは不要の可能性があります。オーディオとビデオの両方のエンドポイントで、音声専用コールまたはビデオ コールに WAN と LAN を経由した G.711 または G.722 を使用する場合、音声専用 IP Phone およびビデオ エンドポイントは同じリージョンを使用します。
- デフォルト リージョン設定を検討し、マトリックスを単純にします。次に、図 13-25 のリージョン グループに基づいた有効なデフォルト設定例を示します。リージョン間ビット レートよりも大きなリージョン内ビット レートを設定する場合は、サイトごとのリージョンが必要になります。
  - [リージョン内のデフォルトの最大ビデオ コール ビット レート（オーディオ含む）（Default Intraregion Max Video Call Bit Rate (Includes Audio)）]：768 に設定します。リージョン内のコールに対してデバイスの最大ビデオ ビット レート機能を 768 kbps に設定します。
  - [リージョン間のデフォルトの最大ビデオ コール ビット レート（オーディオ含む）（Default Interregion Max Video Call Bit Rate (Includes Audio)）]：768 に設定します。リージョン間のコールに対してデバイスの最大ビデオ ビット レート機能を 768 kbps に設定します。

- [リージョン内のデフォルトの最大イマーシブ ビデオ コール ビット レート（オーディオ含む）（Default Intraregion Max Immersive Video Call Bit Rate (Includes Audio)）]：12000 に設定します。リージョン内のコールに対してデバイスの最大ビデオ ビット レート機能を 12,000 kbps に設定します。
- [リージョン間のデフォルトの最大イマーシブ ビデオ コール ビット レート（オーディオ含む）（Default Interregion Max Video Call Bit Rate (Includes Audio)）]：12000 に設定します。リージョン間のコールに対してデバイスの最大ビデオ ビット レート機能を 12,000 kbps に設定します。
- デフォルト設定以外に、各ビデオ エンドポイント グループに対して 1 つずつ、4 つのリージョンを設定する必要があります。

Enhanced Locations Call Admission Control

コール アドミッション制御機能は、特に複数のサイトが IP WAN 経由で接続され、オーディオ コールとビデオ コールで使用可能な帯域幅リソースが制限されている場合、コラボレーション システムの重要なコンポーネントとなります。コール アドミッション制御の機能と必要性をわかりやすく説明するために、図 13-26 の例について考えます。

図 13-26　　コール アドミッション制御が必要な理由

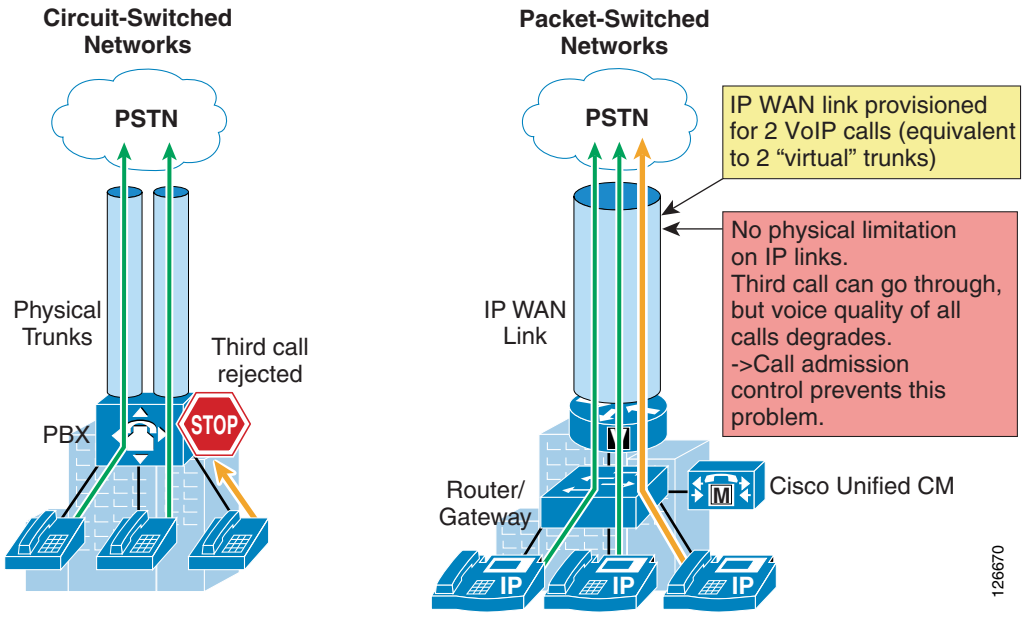


図 13-26 の左側で示すように、従来の TDM ベースの PBX は、回線交換ネットワークの一部として動作します。このネットワークでは、回線はコールがセットアップされるたびに確立されます。このため、レガシー PBX が PSTN または他の PBX に接続されている場合は、一定数の物理トランクを設定する必要があります。PSTN または他の PBX 宛てのコールをセットアップする必要があるとき、PBX は、使用可能なトランクの中からトランクを選択します。使用可能なトランクがない場合、コールは PBX によって拒否され、発信者にはネットワーク ビジー信号が聞こえます。

次に、図 13-26 の右側に示している IP 接続 Unified Communications システムについて考えます。このシステムは、パケット交換ネットワーク（IP ネットワーク）を基盤としているため、IP テレフォニー コールをセットアップするために回線を確立する必要はありません。サンプリング音声を含んでいる IP パケットが、他のタイプのデータ パケットとともに、IP ネットワーク経由でルーティングされるだけです。音声パケットは、Quality of Service（QoS）を使用してデータ パケットと区別されますが、帯域幅リソースは、特に IP WAN リンクでは無限ではありません。このため、ネットワークの管理者が、一定量の「優先」帯域幅を各 IP WAN リンク上の音声トラフィック専用として割り当ててください。ただし、設定した帯域幅がすべて使用される状態になった場合は、IP テレフォニー システムで以後のコールを拒否して、IP WAN リンク上のプライオリティ キューのオーバーサブスクリプションを防止する必要があります。オーバーサブスクリプションが発生すると、すべての音声コールで品質が低下します。この機能はコール アドミッション制御と呼ばれ、IP WAN を利用したマルチサイト配置で良好な音声品質とビデオ品質を保証するために不可欠なものです。

エンド ユーザ エクスペリエンスの満足度を維持するには、コール アドミッション制御機能を常にコール セットアップ段階で実行する必要があります。このようにすることで、ネットワーク リソースを使用できない場合に、エンド ユーザにメッセージを表示したり、異なるネットワーク（PSTN などの）を通じてコールを再ルーティングしたりすることができるようになります。

この章では、次の主要トピックについて説明します。

- コール アドミッション制御のアーキテクチャ（13-43 ページ）

  ここでは、Enhanced Location Call Admission Control と呼ばれる Cisco Unified Communications Manager で使用可能なコール アドミッション制御のメカニズムについて説明します。Cisco IOS ゲートキーパー、RSVP、および RSVP SIP プレコンディションの詳細については、次の Web サイトから入手可能な『*Cisco Unified Communications System 9.0 SRND*』の「*Call Admission Control*」の章を参照してください。

  https://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/9x/cac.html

- コール アドミッション制御の設計上の考慮事項（13-79 ページ）

  ここでは、IP WAN トポロジに基づいて Enhanced Location Call Admission Control を適用する例を示します。

コール アドミッション制御のアーキテクチャ

ここでは、Cisco Unified CM に基づいて Enhanced Location Call Admission Control の設計と設定のガイドラインを提供します。

Unified CM Enhanced Location Call Admission Control

Cisco Unified CM では、Enhanced Location Call Admission Control（ELCAC）を提供し、複数のクラスタが同じ物理サイトのデバイスを同じ WAN アップリンクを使用して管理している、複雑な WAN トポロジと、Unified CM の分散型配置でのコール アドミッション制御をサポートします。Enhanced Location CAC 機能はイマーシブ ビデオもサポートし、管理者は TelePresence などのイマーシブ ビデオ コールに対してコール アドミッションを他のビデオ コールと別に制御することができます。

より複雑な WAN トポロジをサポートするために、Unified CM はロケーション ベースのネットワーク モデリング機能を実装しています。これは、発信側と着信側の間のマルチ ホップ WAN 接続をサポートする機能を Unified CM に提供します。このネットワーク モデリング機能は、段階的にマルチ クラスタの分散型 Unified CM 配置をサポートするように強化されました。これは、クラスタ全体で同じロケーションに割り当てられた帯域幅を予約、解放、および調整するためにクラスが相互に通信できるようにすることによって、管理者が効果的にクラスタ間の場所を「共有」することが可能になります。また、管理者は**イマーシブ ビデオ帯域幅**と呼ばれる [ロケーション(Location)] 設定に新しいフィールドを割り当てることによって、TelePresence などのイマーシブ ビデオ コールの帯域幅を個別にプロビジョニングできます。

ツールを使用して、Enhanced Location CAC を管理し、トラブルシューティングすることができます。CAC の拡張機能と設計は、この章で詳しく説明していますが、トラブルシューティング、およびサービスアビリティ ツールは個別の製品マニュアルで説明します。

ロケーション、リンク、および重みによるネットワーク モデリング

Enhanced Location CAC はモデル ベースのスタティック CAC メカニズムです。Enhanced Location CAC では、「ルーテッド WAN ネットワーク」をモデリングするロケーションとリンクを設定するのに、Unified CM で管理インターフェイスを使用する必要があります。このモデルは、WAN ネットワーク トポロジがエンドツーエンドの音声、ビデオ、およびイマーシブ コールに対するエンドポイント グループ間のメディアをどのようにルーティングするのかを表します。ネットワークをモデル化するために Unified CM は設定インターフェイスおよびサービスアビリティ インターフェイスを提供しますが、まだ再ルーティングしているネットワーク障害とネットワーク プロトコルを考慮しない「静的」CAC メカニズムです。したがって、モデルは、WAN ネットワーク トポロジが変更されたらアップデートする必要があります。Enhanced Location CAC もコール指向であり、帯域幅の差し引きはストリームごとではなくコールごとであるため、片方向のストリームのビットレートが反対方向のビットレートよりも高いようなメディア フローの場合、必ず高い方のビットレートに対して差し引かれます。また、単方向メディア フロー アラウンドは双方向メディア フローであるかのように差し引かれます。

管理者がロケーションとリンクを使用してネットワーク モデルを構築できるように、Enhanced Locations CAC は次の設定コンポーネントを組み込みます。

- ロケーション:ロケーションは LAN を表します。これは、エンドポイントを含み、または単に WAN ネットワークのモデル化に対してリンク間の中継場所として機能します。たとえば、MPLS プロバイダーはロケーションで表される可能性があります。
- リンク:リンクはロケーションを相互接続し、ロケーション間で利用可能な帯域幅を定義するために使用されます。リンクは論理的に WAN リンクを表し、ロケーションのユーザ インターフェイス(UI)に設定されます。
- 重み:重みは、ロケーションのペア間に*有効なパス*を構成するリンクの相対的なプライオリティを与えます。有効なパスは、帯域幅の計算に Unified CM で使用するパスであり、すべての可能なパスにある最小の累積重みが設定されます。重みは、「有効なパス」に「コスト」を提供するためにリンクで使用され、任意の 2 地点間に複数のパスがある場合にだけ該当します。
- パス:パスはロケーション ペアを接続するリンクおよび中間場所のシーケンスです。Unified CM では、各ロケーションから他のすべてのロケーションへの最小コスト パス(最も小さい累積的な重み)をパス計算し、さまざまなパスへのマップを構築します。1 つの「有効なパス」だけがロケーションの任意のペア間で使用されます。
- 有効なパス:有効なパスは最小の累積重みのパスです。
- 帯域割り当て:音声、ビデオ、およびイマーシブ ビデオ(TelePresence)の各トラフィック タイプ用のモデルで割り当てられる帯域幅。

- Location Bandwidth Manager（LBM）：1 つ以上のクラスタで設定されたロケーションおよびリンク データからネットワーク モデルを構築する Unified CM のアクティブ サービス。ロケーションのペア間の有効なパスを決定して、各タイプのコールに対する帯域幅の可用性に基づいてロケーションのペア間のコールを許可するか決定し、そして許可された各コールの時間分の帯域幅を差し引きます（予約します）。
- Location Bandwidth Manager ハブ：固定ロケーション、リンクのデータおよびダイナミック帯域幅割り当てのデータのクラスタ間のレプリケーションに直接参加するように指定された Location Bandwidth Manager（LBM）サービス。LBM のハブ グループに割り当てられている複数の LBM は、共通の接続を介して互いに探索し、フル メッシュ構造のクラスタ間のレプリケーション ネットワークを形成します。LBM ハブを持つクラスタ内の他の LBM サービスはクラスタの LBM のハブを介してクラスタ間のレプリケーションに間接的に参加します。

ロケーションおよびリンク

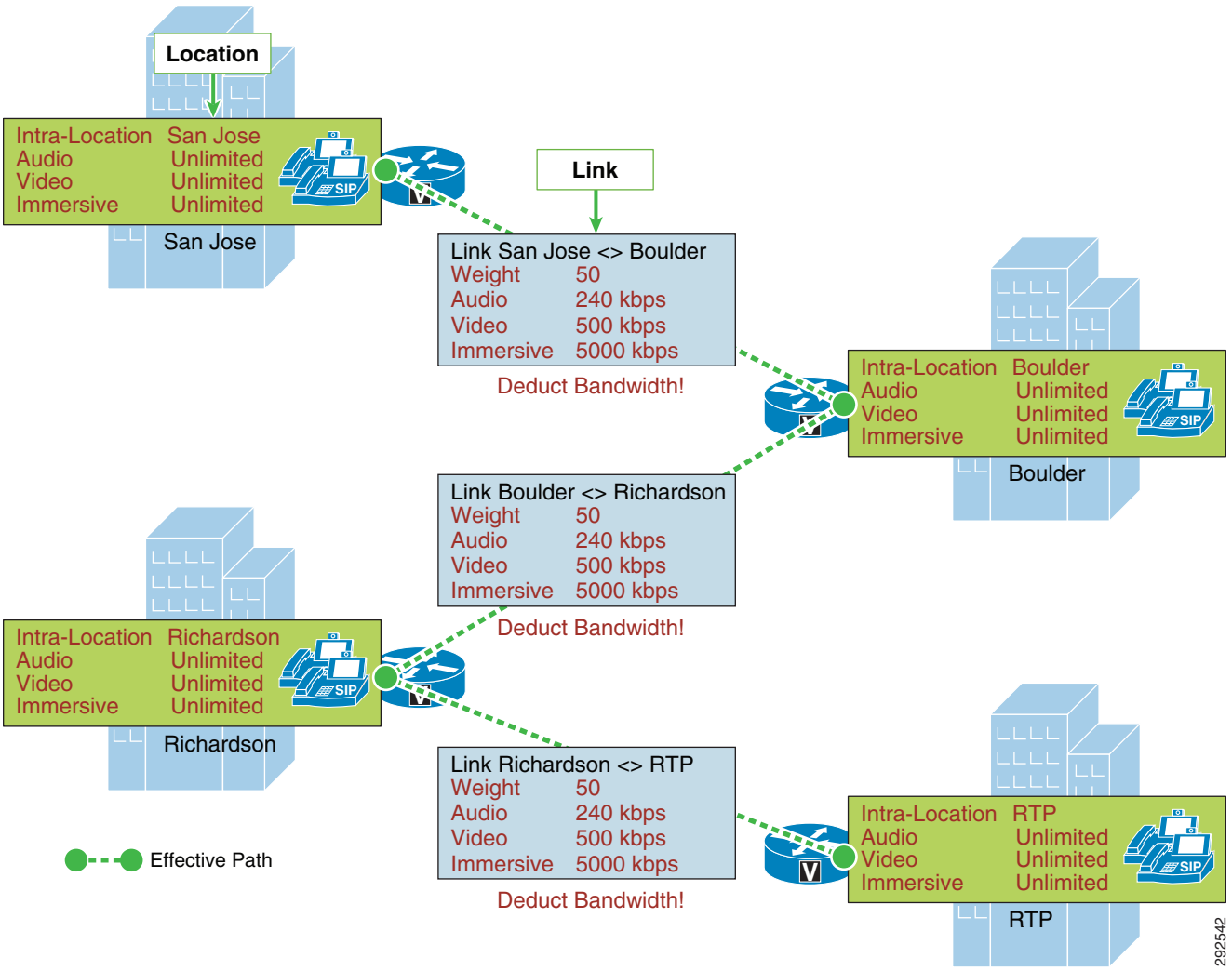
Unified CM は、ロケーションの概念を使用して物理的なサイトを表し、エンドポイント、ボイス メッセージ ポート、トランク、ゲートウェイなどのメディア デバイスとの関連付けを作成します。これは、デバイス自体に直接設定した値、デバイス プール、またはデバイス モビリティを通じて行われます。Unified CM は、*links* と呼ばれる新しいロケーション設定パラメータも使用します。リンクはロケーションを相互接続し、ロケーション間で利用可能な帯域幅を定義するために使用されます。リンクは論理的に WAN リンクを表します。ここでは、ロケーションおよびリンクおよびその使用方法について説明します。

ロケーション設定自体は、リンク、ロケーション間の帯域幅パラメータ、および RSVP ロケーションの設定の 3 つの主要部分で構成されます。Enhanced Location CAC に対する RSVP ロケーションの設定は、RSVP 実装にのみ適用されるため、ここでは考慮されません。設定では、ロケーション間の帯域幅パラメータが Show によって [詳細を表示（Show advanced）] リンクの選択で非表示または表示される間、リンク帯域幅パラメータが最初に表示されます。

ロケーション間の帯域幅パラメータは、管理者が音声、ビデオ、およびイマーシブの 3 つのコール タイプの帯域幅割り当てを設定することができます。これらは、トラフィックの量を、指定されたロケーション内およびロケーションとの間で制限します。どのデバイスでもコールを発信または受信すると、帯域幅がそのコール タイプに適用可能な帯域割り当てから差し引かれます。この機能により管理者は、LAN または中継ロケーションで使用される帯域幅の量を制限することができます。ギガビット LAN で構成される現在ほとんどのネットワークでは、これらの LAN 帯域幅を制限する原因がほとんどないか、まったくありません。

リンク帯域幅パラメータは、管理者が「隣接ロケーション」（つまり、その間で設定されたリンクがあるロケーション）間の音声、ビデオ、およびイマーシブ コール用にプロビジョニングされた帯域幅を特徴付けることができます。この機能により管理者にマルチ ホップ WAN ネットワークをモデル化するロケーションの組み合わせのストリングを作成する機能を提供します。これに図解するために、図 13-27 に示すように 4 つの物理的なサイトを接続する単純な 3 ホップ WAN トポロジを検討します。このトポロジでは、San Jose と Boulder 間、Boulder と Richardson 間、および Richardson と RTP 間のリンクを作成します。たとえば、San Jose から Boulder へのリンクの作成時、逆のリンク（Boulder から San Jose）も存在することに注意してください。したがって、管理者はいずれかのロケーション設定のページから一度だけペア リンクを作成する必要があります。図 13-27 の例では、3 つの各リンクは同じ設定で、重みが 50、音声帯域幅が 240 kbps、ビデオ帯域幅が 500 kbps、イマーシブ帯域幅が 5000 kbps（または 5 Mbps）です。

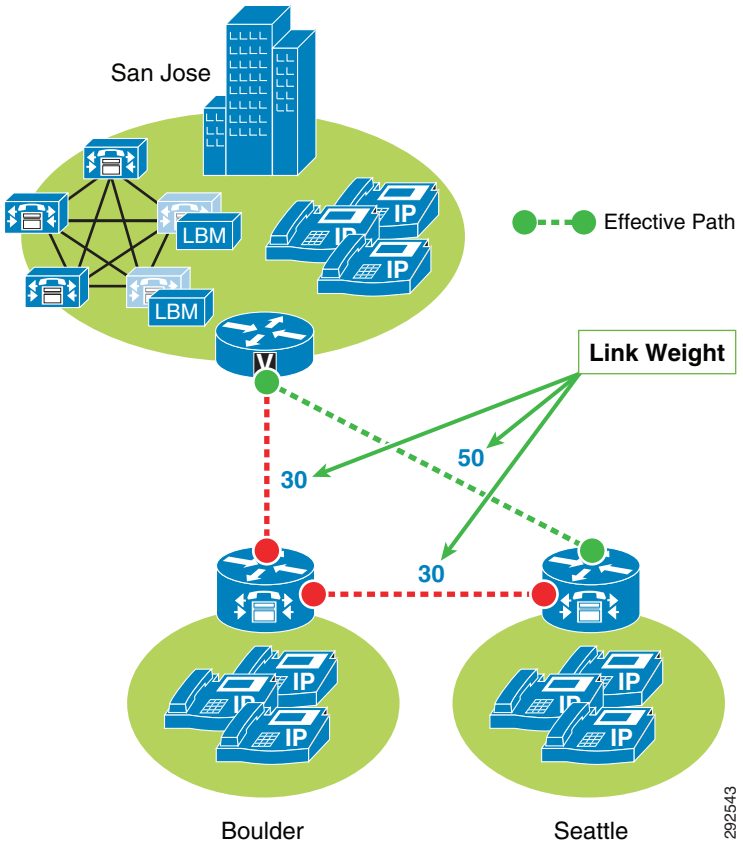
図 13-27　3 WAN のホップを持つ単一リンクの例



コールが San Jose と RTP の間で確立されると、Unified CM は、2 つのデバイス間のリージョン ペアによって決定される要求されたコールの帯域幅を計算し（ロケーション、リンクとリージョンの設定（13-50 ページ）を参照）、2 地点間の有効なパスを確認します。つまり、Unified CM は 2 地点間のパスを構成するリンクと場所を確認し、各リンクと（該当する場合）パスの各場所からそれに応じて帯域幅を差し引きます。ロケーション内の帯域幅も、ロケーションのいずれかが無制限以外の帯域幅値を設定した場合はパスに沿って差し引かれます。

2 地点間で複数のパスが使用可能である場合に、重みがリンクだけで設定可能で、特定のパスの選択を強制する機能を提供します。複数のパスが設定されている場合、累積重みに基づいて 1 つだけが選択され、このパスが *有効なパス* と呼ばれます。この重みはスタティックであり、有効なパスを動的に変更されません。図 13-28 は San Jose、Boulder および Seattle の 3 地点間のリンクで設定された重みを示しています。

図 13-28　累積パスの重み



San Jose から Seattle は 2 つのパスがあり、1 つはロケーション間の直接リンクで、もう 1 つは Boulder ロケーション経由（San Jose/Boulder リンクと Boulder/Seattle リンク）のパスです。San Jose と Seattle 間の直接リンクで設定された重みは 50 で、リンク San Jose/Boulder および Boulder/Seattle の累積重み 60（30+30）未満です。したがって、直接リンクが、累積リンクの重みが 50 であるため有効なパスとして選択されます。

Unified CM でデバイスを設定するときは、そのデバイスをロケーションに割り当てることができます。ロケーションは、トポロジを構築するために他のロケーションへのリンクで設定できます。Unified CM で設定するロケーションは、仮想ロケーションであり、実際の物理ロケーションではありません。前述のように、Unified CM は、ネットワーク内の実際の物理トポロジを認識しません。したがって Unified CM ロケーション モデルの実際の基本ネットワーク トポロジをマッピングするには、Unified CM の物理ネットワークへの変更は手動で実行する必要があります。デバイスが 1 つの物理ロケーションから他のロケーションに移動されると、システム管理者は、Unified CM がそのデバイスとの間で正しくコールの帯域幅割り当てを計算できるように、ロケーション設定の手動アップデートを実行するかデバイス モビリティ機能を実装する必要があります。各デバイスは、デフォルトでは **Hub_None** ロケーションに配置されます。ロケーション Hub_None は、通常、複数のロケーションをリンクするハブとして動作し、音声、ビデオ、およびイマーシブ帯域幅の無制限のロケーション内帯域幅割り当てがデフォルトで設定されるロケーションの例です。

Unified CM は、各ロケーションおよびロケーション間のリンクに別の音声、ビデオ、およびイマーシブ ビデオの帯域幅プールを定義することができます。通常、ロケーションのロケーション内の帯域幅設定はデフォルトの**無制限**のままであるのに対し、物理的なサイト間の WAN リンクの容量に合わせて、ロケーション間のリンクは有限数のキロ ビット/秒（kbps）に設定されます。ロケーションのロケーション内の音声、ビデオ、およびイマーシブ帯域幅が**無制限**として設定されている場合、そのロケーション内のコールおよびそのロケーションを通り抜けるすべてのコール（音声、ビデオ、およびイマーシブ）に使用できる無限の帯域幅があります。一方、帯域幅の値が有限数のキロ ビット/秒（kbps）に設定されている場合、Unified CM はロケーション内のすべてのコール、および中継ロケーション（計算パス内にあるが、パス内の発信または着信ロケーションではないロケーション）としてロケーションを使用するすべてのコールをトラッキングします。

ビデオ コールでは、ビデオ ロケーションの帯域幅は、ビデオ コールの音声およびビデオ部分の両方を考慮に入れます。したがって、ビデオ コールの場合、帯域幅が音声帯域幅プールから差し引かれることは一切ありません。同じことがイマーシブ ビデオ コールにも適用されます。

ロケーションでメンバーシップを指定できるデバイスには、次のものがあります。

- IP Phone
- CTI ポート
- H.323 クライアント
- CTI ルート ポイント
- カンファレンス ブリッジ
- 保留音（MoH）サーバ
- ゲートウェイ
- トランク
- メディア ターミネーション ポイント（デバイス プールを使用）
- 信頼されたリレー ポイント（デバイス プールを使用）
- アナンシエータ（デバイス プールを使用）

Enhanced Location Call Admission Control メカニズムでは、通話中のコール タイプ変更も考慮されます。たとえば、サイト間でビデオ コールを確立する場合、Unified CM は、パスのそれぞれのロケーションおよびリンクから適切なビデオ帯域幅を差し引きます。このビデオ コールが、ビデオ非対応のデバイスへの転送の結果、音声のみのコールに変更された場合、Unified CM はビデオ プールに割り当てられた帯域幅を返却し、同じパスに沿って音声プールから適切な帯域幅を割り当てます。音声からビデオに変更されるコールについては、これとは逆の帯域幅割り当て変更が発生します。

表 13-10 に、さまざまなコールのタイプ（ビット レート）において静的ロケーション アルゴリズムが要求する帯域幅を示します。音声コールでは、Unified CM はメディア ビット レートに IP および UDP オーバーヘッドを加えてカウントします。たとえば、G.711 音声コールは、ロケーションとリンクのオーディオ帯域幅割り当てから差し引かれた 80 kbps（64k ビット レート + 16k IP/UDP ヘッダー）を消費します。ビデオ コールでは、Unified CM は、音声ストリームとビデオ ストリームの両方に対して、メディア ビット レートだけを計算します。たとえば、384 kbps のビット レートのビデオ コールに対して、Unified CM はビデオ帯域幅割り当てから 384 kbps を割り当てます。

表 13-10　ロケーションおよびリンクの帯域幅の差し引きアルゴリズムが要求する帯域幅の量

コールのビット レート	静的ロケーションとリンク帯域幅値
G.711 音声コール（64 kbps）	80 kbps
G.729 音声コール（8 kbps）	24 kbps
128 kbps ビデオ コール	128 kbps
384 kbps ビデオ コール	384 kbps
512 kbps ビデオ コール	512 kbps
768 kbps ビデオ コール	768 kbps

コーデックおよびロケーションとリンクの帯域幅値のリストについては、次の Web サイトで入手可能な『*Cisco Unified Communications Manager System Guide*』の「*Call Admission Control*」の項の帯域幅計算情報を参照してください。

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

たとえば Hub_None への支社 1 のロケーションのリンク設定が使用可能なビデオ帯域幅 256 kbps および音声帯域幅 384 kbps を割り当てるとします。この場合支社 1 から Hub_None へのパスは、最高 3 つの G.711 音声コール（コールごとに 80 kbps）、または 10 の G.729 音声コール（コールごとに 24 kbps）、または 256 kbps を超えない両方の組み合わせをサポートできます。このロケーション間のリンクでは、使用されているビデオ コーデックおよびオーディオ コーデックに応じて、さまざまな数のビデオ コールをサポートすることもできます（たとえば、384 kbps の帯域幅を要求する 1 つのビデオ コール、またはそれぞれ 128 kbps の帯域幅を要求する 3 つのビデオ コールをサポートできます）。

あるロケーションから他のロケーションにコールが発信されると、Unified CM は、ロケーションおよびあるロケーションから他のロケーションへのリンクの有効なパスから適切な帯域幅を差し引きます。例として図 13-27 を使用すると、San Jose と RTP ロケーション間の G.729 コールによって、Unified CM は、San Jose と Boulder 間、Boulder と Richardson 間、Richardson と RTP 間のリンクで使用可能な帯域幅から 24 kbps を差し引きます。コールが完了すると、Unified CM は有効なパス上でこれらの同じリンクに帯域幅を返却します。十分な帯域幅がパス上のリンクのいずれかにない場合、コールは Unified CM によって拒否され、発信者はネットワーク ビジー トーンを受信します。発信側デバイスが、ディスプレイを備えた IP Phone である場合、そのデバイスには、「Not Enough Bandwidth」というメッセージも表示されます。

ロケーション間コールがコール アドミッション制御によって拒否された場合、Unified CM は自動代替ルーティング（AAR）機能を使用して、PSTN 接続を通じて宛先にコールを自動的に再ルーティングできます。AAR 機能の詳細については、自動代替ルーティング（14-85 ページ）を参照してください。

（注） AAR は、有効なパスに沿ってネットワーク帯域幅が不足しているために、Enhanced Location Call Admission Control によってコールが拒否される場合のみ、呼び出されます。IP WAN が使用不可の場合や、接続に関するその他の問題によって着信側デバイスが Unified CM に登録されない状態になった場合には、AAR は呼び出されません。このような場合、コールは着信側デバイスの [Call Forward No Answer] フィールドで指定されている宛先に転送されます。

デバイス間のビデオ コールが CAC に失敗した場合にビデオ デバイスを [ビデオコールをオーディオとして再試行（Retry Video Call as Audio）] にイネーブルにできることも注意すべき点です。このオプションは、Unified CM のビデオ エンドポイントの設定ページで設定され、コールを受信するビデオ エンドポイントまたはトランクに適用できます。一部のビデオ エンドポイントは、デフォルトでは [ビデオコールをオーディオとして再試行（Retry Video Call as Audio）] がイネーブルにされ、エンドポイントで設定できないことにも注意する必要があります。

ロケーション、リンクとリージョンの設定

ロケーションは、リージョンとともに機能してロケーションおよびリンクに有効なパス上でコールの特性を定義します。リージョンはデバイス間で使用される圧縮のタイプまたはビットレート（8 kbps または G.729、64 kbps または G.722/G.711 など）を定義し、ロケーション リンクはデバイス間の有効なパスで使用可能な帯域幅の量を定義します。システム内の各デバイスを（デバイス プールを使用して）リージョンに割り当て、（デバイス プールまたはデバイス自体に直接設定した値を使用して）ロケーションに割り当てます。

Unified CM では、ロケーションを設定することにより、次の要素を定義できます。

- 物理的なサイト（たとえば、ブランチ オフィス）または中継サイト（たとえば、MPLS クラウド）：場所は LAN を表します。これは、エンドポイントを含み、または単に WAN ネットワークのモデル化に対してリンク間の中継場所として機能します。
- 隣接するロケーション間のリンク帯域幅：リンクはロケーションを相互接続し、ロケーション間で利用可能な帯域幅を定義するために使用されます。リンクは物理的なサイト間の WAN リンクを論理的に表します。
  - 音声帯域幅：ロケーションデバイスから設定された隣接した場所に行われる音声および FAX コールの WAN リンクで使用可能な帯域幅の量。Unified CM は、Enhanced Location Call Admission Control にこの帯域幅値を使用します。
  - ビデオ帯域幅：ロケーション デバイスから設定された隣接した場所に行われたビデオ コール用の WAN リンクで使用可能なビデオ帯域幅の量。Unified CM は、Enhanced Location Call Admission Control にこの帯域幅値を使用します。
  - イマーシブ ビデオ帯域幅：ロケーション デバイスから設定された隣接した場所に行われた TelePresence コールの WAN リンクで使用可能なイマーシブ帯域幅の量。Unified CM は、Enhanced Location Call Admission Control にこの帯域幅値を使用します。
- ロケーション内の帯域幅
  - 音声帯域幅：ロケーション内のデバイスから行われる音声および FAX コールの LAN で使用可能な帯域幅の量。Unified CM は、Enhanced Location Call Admission Control にこの帯域幅値を使用します。
  - ビデオ帯域幅：ロケーション内のデバイスから行われるビデオ コールの LAN で使用可能なビデオ帯域幅の量。Unified CM は、Enhanced Location Call Admission Control にこの帯域幅値を使用します。
  - イマーシブ ビデオ帯域幅：ロケーション内のデバイスから行われる TelePresence コールの LAN で使用可能なイマーシブ帯域幅の量。Unified CM は、Enhanced Location Call Admission Control にこの帯域幅値を使用します。

Unified CM では、リージョンを設定することにより、次の要素を定義できます。

- リージョン内およびリージョン間のコールに使用する最大オーディオ ビット レート設定
- リージョン内およびリージョン間のコールに使用するビデオ コールの最大セッション ビット レート（オーディオ含む）
- リージョン内およびリージョン間のコールに使用するイマーシブ ビデオ コールの最大セッション ビット レート（オーディオ含む）
- オーディオ コーデック プリファレンス リスト

Unified CM によるロケーションおよびリージョンのサポート

Cisco Unified Communications Manager は、クラスタごとに 2,000 のロケーションと 2,000 のリージョンをサポートします。最大 2,000 のロケーションおよびリージョンを配置するには、[クラスタ全体のパラメータ（Clusterwide Parameters）] >（[システム（System）] > [ロケーションとリージョン（Location and Region）]）および [クラスタ全体のパラメータ（Clusterwide Parameters）] >（[システム（System）] > [RSVP]）の設定メニューで次のサービス パラメータを設定する必要があります。

- リージョン内のデフォルトの最大オーディオ ビット レート（Default Intraregion Max Audio Bit Rate）
- リージョン間のデフォルトの最大オーディオ ビット レート（Default Interregion Max Audio Bit Rate）
- リージョン内のデフォルトの最大ビデオ コール ビット レート（オーディオ含む）（Default Intraregion Max Video Call Bit Rate (Includes Audio)）
- リージョン間のデフォルトの最大ビデオ コール ビット レート（オーディオ含む）（Default Interregion Max Video Call Bit Rate (Includes Audio)）
- リージョン内のデフォルトの最大イマーシブ コール ビット レート（オーディオ含む）（Default Intraregion Max Immersive Call Bit Rate (Includes Audio)）
- リージョン間のデフォルトの最大イマーシブ ビデオ コール ビット レート（オーディオ含む）（Default Interregion Max Video Call Bit Rate (Includes Audio)）
- リージョン間のデフォルト オーディオ コーデック プリファレンス リスト（Default Audio Codec Preference List between Regions）
- リージョン内のデフォルト オーディオ コーデック プリファレンス リスト（Default Audio Codec Preference List within Regions）

リージョンを追加するときは、ビデオ コールの最大オーディオ ビット レートと最大セッション ビット レートの値として [システム デフォルトの使用（Use System Default）] を選択してください。

個別のリージョンに応じてデフォルト値からこれらの値を変更すると、サーバ初期化とパブリッシャー アップグレードの時間に影響を与えます。合計 2,000 のリージョンと 2,000 のロケーションを使用する場合、最大 200 リージョンでデフォルト以外の値を使用するように変更できます。合計 1,000 以下のリージョンおよびロケーションを使用する場合、最大 500 リージョンでデフォルト以外の値を使用するように変更できます。表 13-11 は、これらの制限を要約したものです。

表 13-11　許可されたロケーションとデフォルト値以外のリージョンの数

デフォルト値以外のリージョンの数	リージョンの最大数	ロケーションの最大数
0 ～ 200	2,000	2,000
200 ～ 500	1,000	1,000

（注）　[最大オーディオビットレート（Max Audio Bit Rate）] は、音声コールと FAX コールの両方に使用されます。リージョン間コーデックとして G.729 を使用する場合、FAX コールには T.38 FAX リレーを使用してください。WAN で FAX パススルーを使用する場合、オーディオ プリファレンス リストを使用して、音声のみのコールには G.729、FAX コールには G.711 を使用します。

Location Bandwidth Manager

Location Bandwidth Manager（LBM）は、サービスアビリティ Web ページから管理し、Enhanced Location CAC 帯域幅の機能すべてを担当する Unified CM 機能サービスです。LBM は、Unified CM サブスクライバ ノードまたはクラスタの専用の Unified CM ノードのスタンドアロン サービスとして実行できます。クラスタで Enhanced Location CAC を有効にするには、LBM の 1 つ以上のインスタンスが各クラスタで実行される必要があります。ただし、Cisco CallManager サービスも実行しているクラスタ内の各サブスクライバ ノードで LBM を実行することを推奨します。

LBM では次の機能が実行されます。

- ロケーションおよびリンク パスのトポロジを組み合わせる
- トポロジにわたる有効なパスの計算
- Cisco CallManager サービス（Unified CM 呼制御）からのサービスの帯域幅要求
- 他の LBM への帯域幅情報の複製
- 設定済みのダイナミック情報をサービスアビリティに提供
- Location Real-Time Monitoring Tool（RTMT）カウンタの更新

LBM サービスは、従来のロケーション CAC のみをサポートする以前のリリースから Cisco Unified CM をアップグレードすると、デフォルトで有効です。新規インストールの場合、LBM サービスは手動でアクティブにする必要があります。

初期化中に LBM は、ロケーションの音声、ビデオ、およびイマーシブ帯域幅値などのデータベース、ロケーション内の帯域幅データ、ロケーションごとのリンク音声、ならびにイマーシブ帯域幅の値と重みからローカル ロケーション情報を読み取ります。リンク データを使用して、クラスタ内の各 LBM は、あるロケーションから他のすべてのロケーションまでのパスのローカル アセンブリを作成します。これは、*アセンブルされたトポロジ*と呼ばれます。クラスタでは、各 LBM は同じデータにアクセスし、初期化中にアセンブルされるトポロジと同じローカル コピーを作成します。

実行時、LBM は、ロケーションとリンクのローカルで組み立てられたトポロジの計算されたパスの予約を適用し、クラスタ内の他の LBM に予約を複製します。クラスタ間の Enhanced Location CAC が設定され、アクティブになると、LBM は他のクラスタにアセンブルされたトポロジを複製するように設定できます（詳細についてはクラスタ間の Enhanced Location CAC（13-55 ページ）を参照してください）。

デフォルトでは、Cisco CallManager サービスはローカル LBM サービスと通信しますが、この通信を管理するために LBM グループを使用できます。LBM グループは Unified CM の呼制御の冗長性を作成するために、アクティブなスタンバイ LBM を提供します。図 13-29 は LBM の冗長性を示します。

図 13-29　Location Bandwidth Manager の冗長性

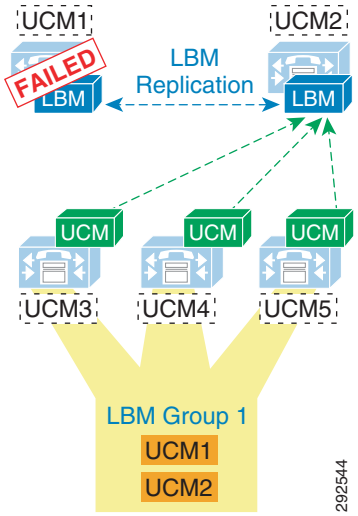


図 13-29 は 5 つの Unified CM サーバを示します。UCM1 および UCM2 は専用 LBM サーバ（LBM サービスがイネーブルの場合だけ）、UCM3、UCM4 および UCM5 は Unified CM サブスクライバ（Cisco CallManager サービスがイネーブルの場合）です。LBM グループは UCM1 でアクティブとして、UCM2 でスタンバイとして設定されており、UCM3、UCM4 および UCM5 サブスクライバに適用されます。この設定は UCM3、UCM4 および UCM5 がすべての帯域幅の要求に対して UCM1 にクエリーを実行できるようになります。UCM1 が何らかの理由で失敗し、サブスクライバはスタンバイ UCM2 にフェールオーバーします。この例を使用して、LBM グループ設定の仕組みを説明します。これは推奨設定ではありません（以下の推奨事項を参照）。

LBM は、動作している CallManager サービスによって処理されるコールすべての要求の処理に直接関係しているため、LBM の最適な機能を確保するために次のシンプルな設計推奨事項に従うことが重要です。

推奨設定は、Cisco CallManager サービス（呼処理）で LBM 共存を実行することです。LBM サービスの冗長性が必要な場合、特定の LBM をオーバーサブスクライブしないことが重要です。また、LBM が特定の導入でプライマリおよびセカンダリにすぎないようにすることも重要です。つまり、障害シナリオでは複数の CallManager サービスの負荷を LBM にかけないようにし、通常の動作時にかける負荷は 1 つの CallManager サービスのみにします。LBM グループを使用すると、共存 LBM をプライマリとして、別のローカル（同一 LAN 上の）LBM をセカンダリとして、最後にサービス パラメータをフェールセーフ メカニズムとして設定し、この CallManager サービスによって処理されたすべてのコールが失敗しないようにすることができます。これらの推奨事項にはさまざまな理由があります。LBM は、動作している CallManager サービスの呼処理負荷に直接関係しているため、LBM の負荷を特定するのは困難です。遅延には考慮事項もあります。LBM が CallManager サービスからオフボックスになるとすぐに、CallManager サービスで処理されるコールすべてのパケット化と処理によって遅延が発生します。呼処理遅延を組み合わせると、呼び出し状態に対して特定のコール フローの許容不可能なレベルに総遅延量が増えるため、ユーザ エクスペリエンスが低下する可能性があります。これらの設計推奨事項を順守すると、総呼処理遅延が削減されます。

Unified CM Cisco CallManager サービスが LBM を使用する順序は次のとおりです。

- LBM グループの指定
- ローカル LBM（共存）
- サービス パラメータ [利用可能な LBM がない場合のコール処理（Call Treatment when no LBM available）]（デフォルト = [コールの許可（allow calls）]）

Enhanced Location CAC の設計および配置の推奨事項と考慮事項

- Location Bandwidth Manager（LBM）は Unified CM 機能サービスです。LBM はトポロジのモデリングおよび Unified CM 帯域幅要求のサービスを行う役割があります。
- クラスタ内の LBM は、LBM 間の帯域幅の変更通知のレプリケーションを行うために、TCP 経由の XML でフル メッシュ通信ネットワークを作成します。
- Cisco CallManager 呼処理サービスを実行している Unified CM サブスクライバで LBM サービス共存を展開することをお勧めします。
- LBM サービスに冗長性が必要な場合は、Cisco CallManager 呼処理サービスを実行している Unified CM サブスクライバごとに LBM グループを作成します。共存 LBM サービスをプライマリ LBM として、同一 LAN 上の別の Unified CM サブスクライバからの LBM をセカンダリ LBM として追加します。これにより、Cisco CallManager 呼処理サービスが、共存 LBM をプライマリとして、別のローカル（同一 LAN）Unified CM サブスクライバ上の LBM をセカンダリとして、サービス パラメータ [利用可能な LBM がない場合のコール処理（Call Treatment when no LBM available）] を LBM 要求のターシャリ ソースとして使用するようになります。

（注）　LBM で複数の Cisco CallManager サービスをバックアップすることをお勧めします。LBM が共存 CallManager サービスの負荷を処理し、別の CallManager サービスが失敗したと仮定すると、これは単一の LBM 上にある 2 つの呼処理サーバの負荷に相当します。

- WAN 上のクラスタでの展開およびローカル フェールオーバーでは、クラスタ内 LBM トラフィックが WAN の帯域幅計算であらかじめ計算されます。帯域幅計算の詳細については、ローカル フェールオーバー配置モデル（10-50 ページ）の WAN 経由のクラスタリングのセクションを参照してください。

音声プールからのすべてのオーディオの差し引き

Unified CM には、管理者がビデオと TelePresence コールのオーディオ帯域幅を音声プールから差し引く機能が追加されました。ELCAC は音声とビデオ CAC プールが表示するキューを確実に保護するために適切な DSCP 設定を使用するため、Unified CM がビデオ プールから帯域幅を差し引く方法を変更するには、ビデオ コールのオーディオ ストリームの DSCP をオーディオ専用コールのオーディオ ストリームと同じようにマーキングする必要があります。アドミッション制御と QoS の整合に関する詳細については、ビデオ コールのオーディオに関する考慮事項（13-38 ページ）を参照してください。

Unified CM でこの機能をイネーブルにするには、CallManager サービスのコール アドミッション制御セクションで、サービス パラメータ [ビデオ コールのオーディオ プールからオーディオ帯域幅を差し引く（Deduct Audio Bandwidth from Audio Pool for Video Call）] を [True] に設定します。デフォルト設定は [False] であり、デフォルトでは、Unified CM はビデオ プールからビデオ コールのオーディオとビデオの両方のストリームを差し引きます。

クラスタ間の Enhanced Location CAC

クラスタ間の Enhanced Location CAC は、複数のクラスタにわたるネットワーク モデリングの概念を拡張します。クラスタ間の Enhanced Location CAC では、各クラスタは、ロケーションとリンク上でローカルに設定されたトポロジを管理し、LBM クラスタ間のレプリケーション ネットワーク内にある他のリモート クラスタにこのローカル トポロジを伝播します。リモート クラスタのトポロジを受け取ると、LBM は独自のローカル トポロジにこれを再構成し、グローバル トポロジを作成します。このプロセスによって、グローバル トポロジはすべてのクラスタ間で同じになり、エンドツーエンド CAC に対する企業ネットワーク トポロジの全体的視野を各クラスタに提供します。図 13-30 は、単純なハブアンドスポーク ネットワーク トポロジを持つグローバル トポロジの概念を例として示します。

図 13-30　単純なハブアンドスポーク ネットワークのグローバル トポロジの例

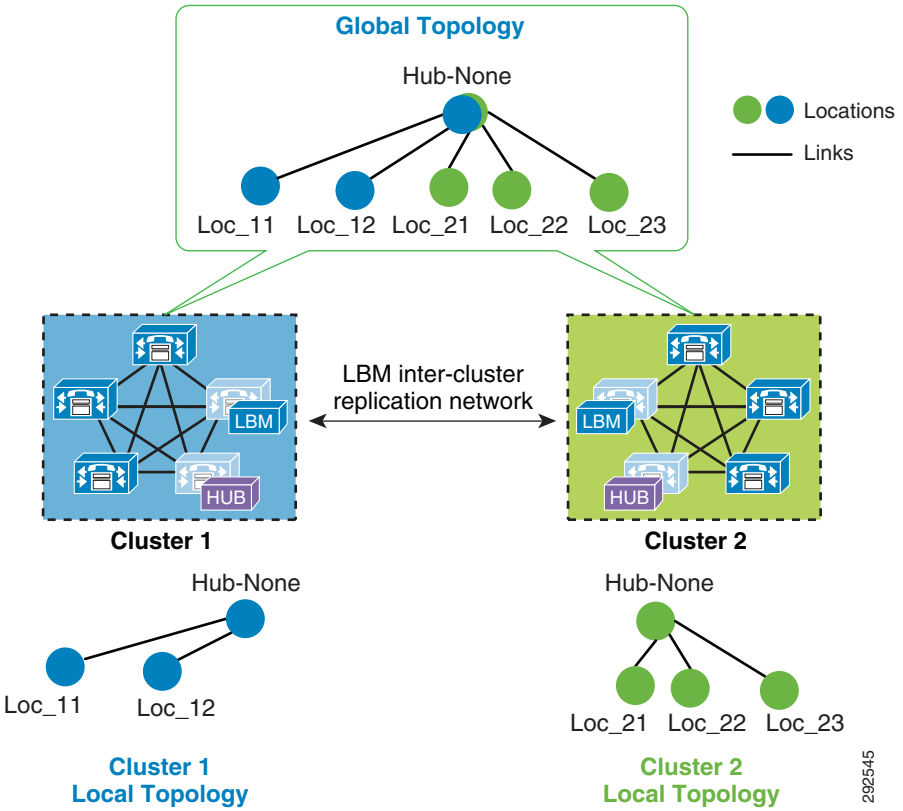


図 13-30 はクラスタ 1 とクラスタ 2 の 2 つのクラスタを示し、それぞれにローカルに設定されたハブアンドスポーク ネットワーク トポロジがあります。クラスタ 2 は Loc_21、Loc_22 および Loc_23 へのリンクで Hub_None を設定し、クラスタ 1 は Loc_11 および Loc_12 へのリンクで Hub_None を設定しました。クラスタ間の Enhanced Location CAC をイネーブルにすると、クラスタ 1 は、クラスタ 2 がクラスタ 1 にするように、そのローカル トポロジをクラスタ 2 に送信します。各クラスタはリモート クラスタのトポロジのコピーを取得した後、各クラスタはオーバーレイ独自上のリモート クラスタのトポロジを自身の上にオーバーレイします。オーバーレイは、同じ名前で設定されたロケーションの一般的な場所によって実現されます。クラスタ 1、クラスタ 2 の両方に同じ名前の共通のロケーション Hub_None があるため、各クラスタは、共通の場所として Hub_None により他方のネットワーク トポロジをオーバーレイし、Hub_None がハブで Loc_11、Loc_12、Loc_21、Loc_22、および Loc_23 がすべてスポーク ロケーションであるグローバル トポロジを作成します。これは単純なネットワーク トポロジの例ですが、より複雑なトポロジは同じ方法で処理されます。

LBM のハブのレプリケーション ネットワーク

クラスタ間 LBM のレプリケーション ネットワークは、LBM ハブと呼ばれる指定 LBM の個別のレプリケーション ネットワークです。LBM ハブは、個別のフル メッシュを相互に作成し、ローカル クラスタのトポロジを他のリモート クラスタに複製します。各クラスタは、グローバル トポロジを作成するために、他のすべてのリモート クラスタからトポロジを効果的に受信します。クラスタ間のレプリケーション ネットワークの指定 LBM は、*LBM ハブ*と呼ばれます。クラスタ内でだけ複製する LBM は *LBM スポーク*と呼ばれます。LBM のハブは、LBM **クラスタ間のレプリケーション グループ**による設定で指定されます。クラスタ内の任意の LBM ロールの割り当てを、クラスタ間のレプリケーション グループ設定のハブまたはスポークのロールに変更することもできます（LBM ハブ グループ設定の詳細については、https://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html で入手可能な Cisco Unified Communications Manager の製品マニュアルを参照してください）。

LBM クラスタ間のレプリケーション グループでは、ブートストラップ LBM の概念もあります。ブートストラップ LBM は、他のすべての LBM ハブに、フル メッシュのハブ レプリケーション ネットワークを作成するために必要な接続の詳細を提供する LBM ハブです。ブートストラップ LBM は、すべての LBM ハブが持つことができるロールです。すべての LBM ハブが 1 つの LBM ハブを指す場合、その 1 つの LBM ハブが他のすべての LBM ハブに相互に接続する方法を伝えます。各レプリケーション グループは、最大 3 つのブートストラップ LBM を参照できます。

LBM のハブ グループが各クラスタに設定されると、指定 LBM ハブはフル メッシュのクラスタ間のレプリケーション ネットワークを作成します。図 13-31 は、クラスタ間のレプリケーション ネットワークを形成するために 3 つのクラスタ（リーフ クラスタ 1、リーフ クラスタ 2 および Session Management Edition（SME）クラスタ）の間に設定された LBM のハブ グループによるクラスタ間のレプリケーションのネットワーク構成を示します。SME クラスタは例としてのみ使用され、この特定の設定には必要ありません。SME クラスタは、エンドポイント登録を処理する別の通常のクラスタである可能性があります。

図 13-31　3 つのクラスタのクラスタ間レプリケーション ネットワークの例

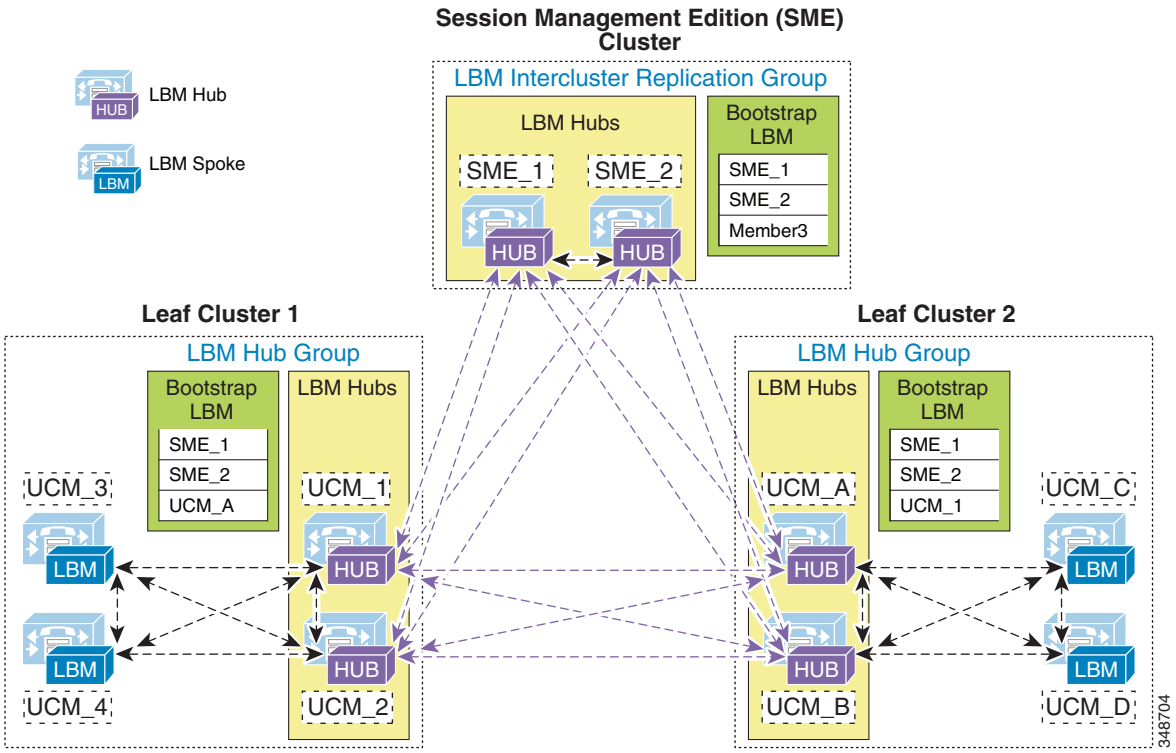


図 13-31 では、各クラスタから 2 つの LBM がクラスタの LBM のハブとして指定されます。これらの LBM ハブは、クラスタ間の LBM レプリケーション ネットワークを形成します。各 LBM クラスタ間のレプリケーション グループに設定されたブートストラップ LBM は、SME_1 および SME_2 と見なされます。SME クラスタからのこれら 2 つの LBM ハブは、クラスタ間 LBM のレプリケーション ネットワーク全体の窓口またはブートストラップ LBM として機能します。これは、各クラスタの各 LBM が SME_1 に接続し、SME_1 にローカル トポロジを複製し、SME_1 からリモート トポロジが取得されることを意味します。また、SME_1 から他のリーフ クラスタの接続情報を取得し、その他のリモート クラスタに接続し、トポロジを複製します。これは、フル メッシュのレプリケーション ネットワークを作成します。SME_1 が使用できない場合、LBM のハブは SME_2 に接続します。SME_2 が使用できない場合、リーフ クラスタ 1 LBM は UCM_A に接続し、SME クラスタが使用できない場合のバックアップ手段として、リーフ クラスタ 2 LBM は UCM_1 に接続します。これは、クラスタ間 LBM のレプリケーション ネットワークのコンポーネントを説明する設定例です。

LBM には、LBM クラスタ間のレプリケーション ネットワークに関する次の役割があります。

- ブートストラップ LBM
  - レプリケーション ネットワークのすべての LBM のハブを相互接続するリモート LBM ハブ
  - ネットワーク内のどのハブにも存在できます
  - LBM クラスタ間のレプリケーション グループごとに最大 3 つのブートストラップ LBM ハブを表示できます

- LBM ハブ（ローカル LBM）
  - クラスタ間 LBM のレプリケーション ネットワークの一部として他のリモート ハブと直接通信します
- LBM スポーク（ローカル LBM）
  - クラスタのローカル LBM のハブと直接通信し、ローカル LBM のハブを介してリモート LBM のハブと間接的に通信します
- LBM のハブのレプリケーション ネットワーク：帯域幅の差し引きと調整メッセージ
  - LBM は各クラスタから送信元および受信者を選択して、LBM メッセージを最適化します。
  - クラスタの LBM の送信者と受信者は、最も小さい IP アドレスによって決まります。
  - リモート クラスタからメッセージを受信する LBM ハブは次に、ローカル クラスタの LBM のスポークに受信メッセージを転送します。

LBM ハブは、通信を暗号化するように設定することもできます。これは、クラスタ間のリンクが保護されていないネットワークに存在する可能性があるためにクラスタ間のトラフィックの暗号化が欠かせない環境に、クラスタ間 ELCAC を配置することを可能にします。暗号化されたシグナリングを LBM ハブ間に設定する方法の詳細については、次の Web サイトで入手可能な Cisco Unified Communications Manager の製品マニュアルを参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

共通ロケーション（共有ロケーション）およびリンク

前述のとおり、共通ロケーションはクラスタ全体で同じ名前のロケーションです。共通ロケーションは、LBM がグローバル トポロジを作成する方法、および複数のクラスタ間で 1 つのロケーションを関連付ける方法において重要な役割を果たします。複数のクラスタ間で同じ名前のロケーションは、同じロケーションと見なされため、これらのクラスタ間では共有ロケーションです。したがって、ロケーションが複数のクラスタ間で共有されることを意味する場合、まったく同じ名前である必要があります。複製後も、LBM は、ロケーションとリンクでの設定の矛盾点について確認します。帯域幅値の不一致、または共通ロケーションとリンク間の重みはサービスアビリティで表示でき LBM は、重みの帯域幅と最小値（最低コスト）の最も厳しい値のロケーションおよびリンク パスを計算します。

共通のロケーションとリンクは、いくつかの異なる理由でクラスタ全体に対して設定できます。同じ物理サイトのデバイスを管理し、同じ WAN アップリンクを使用するいくつかのクラスタを使用することがあるため、同じロケーションは、各クラスタのローカル デバイスにそのロケーションを関連付けるために各クラスタに設定する必要があります。独自のトポロジを管理するクラスタがある場合もありますが、これらのトポロジは、特定のロケーションにおいて相互接続されるため、これらのロケーションを各クラスタ間の共通ロケーションとして設定する必要が生じます。そうすることで、グローバル トポロジが作成されている際に、クラスタでは、各クラスタで共通の相互接続ロケーションとリンクを持ち、各リモート トポロジをともに効果的にリンクさせることができるようになります。図 13-32 はトポロジをリンクすることを示し、各クラスタが共有する共通トポロジを示します。

図 13-32　グローバル トポロジを作成する共通のロケーションとリンクの使用

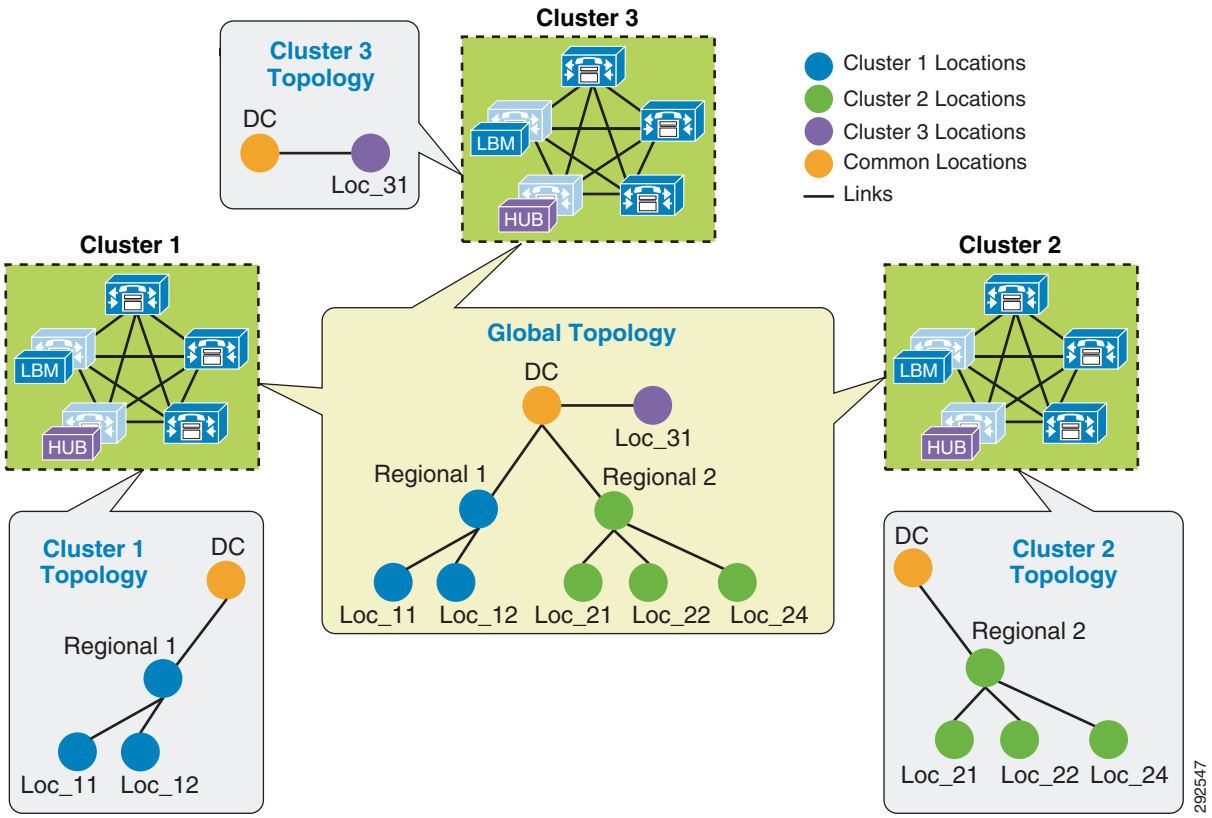
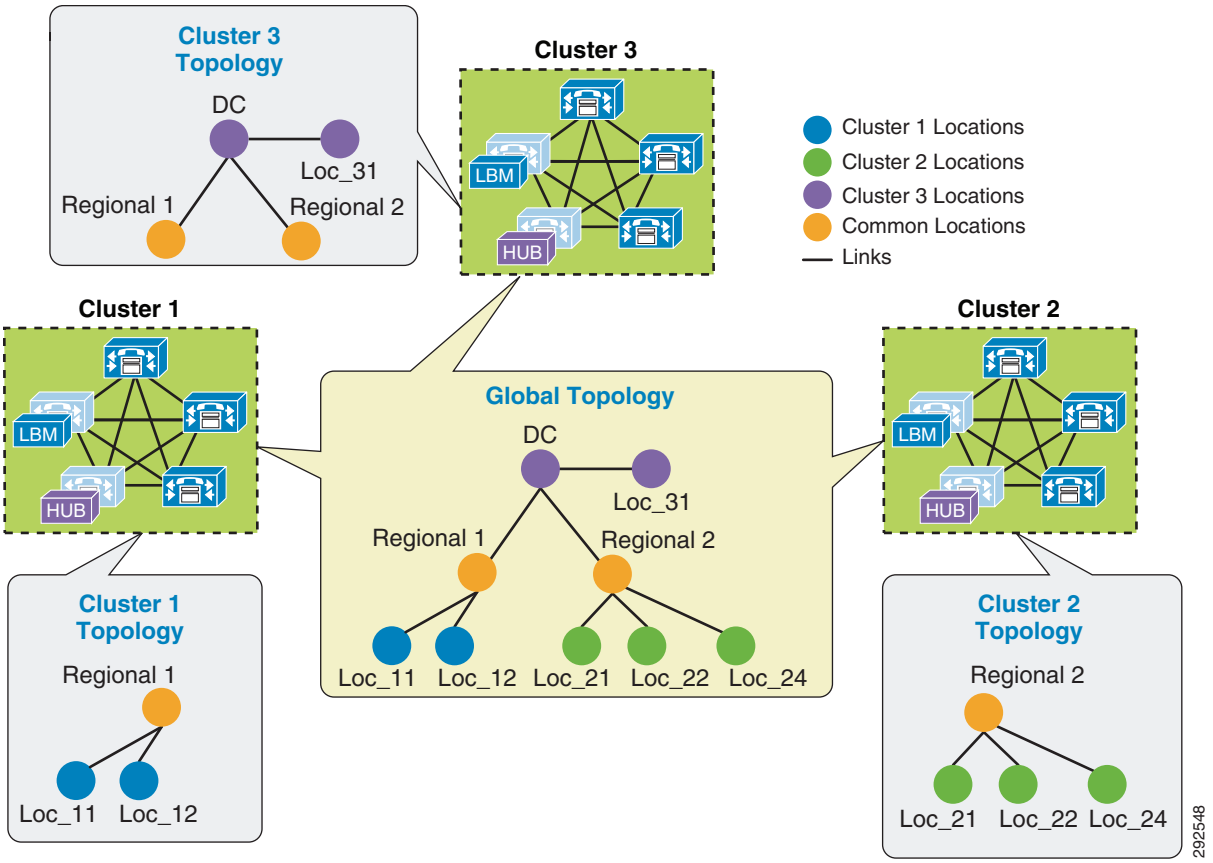


図 13-32 では、クラスタ 1 は Regional 1、Loc_11 および Loc_12 のロケーションにデバイスがありますが、グローバル トポロジの他にリンクするために、DC および Regional 1 から DC へのリンクの設定が必要です。クラスタ 2 も同様に、Regional 2、Loc_21、Loc_22 および Loc_23 にデバイスがあり、グローバル トポロジにマッピングするように DC および DC から Regional 2 へのリンクの設定が必要です。クラスタ 3 には Loc_31 だけにデバイスがあり、クラスタ 1 とクラスタ 2 のトポロジにマッピングするように DC および Loc_31 から DC へのリンクの設定が必要です。また、図 13-33 で示されているように、Regional 1 および Regional 2 を DC の代わりに、すべてのクラスタで設定された共通ロケーションにすることができます。

図 13-33　異なる共通ロケーションを使用する代替トポロジ



クラスタからクラスタへのトポロジ マッピングのキーは、トポロジを相応に相互接続するように少なくとも 1 つのクラスタに別のクラスタの共通ロケーションがあることを確認します。

シャドウ ロケーション

*シャドウ ロケーション*は、Enhanced Location CAC がクラスタ間で機能するために必要な、ロケーションの名前、ビデオ トラフィック クラス（後述）などの、Enhanced Location CAC 情報を他のものに渡すように SIP トランクをイネーブルにするために使用されます。クラスタ全体でこのロケーション情報を渡すためには、SIP クラスタ間トランク（ICT）は「シャドウ」ロケーションに割り当てる必要があります。シャドウ ロケーションは他の場所へのリンクを持つことができないため、帯域幅はシャドウ ロケーションと別のロケーションの間で予約できません。Hub_None に関連付けられたように、シャドウ ロケーションに割り当てられた SIP ICT 以外のいずれかのデバイスが処理されます。SIP ICT 以外のデバイスがシャドウ ロケーションに行きついたら、帯域幅の差し引きは Hub_None 内にあるようにそのデバイスから行われ、ロケーションおよびリンク設定に応じてさまざまな影響を受けるため、これを理解することは重要です。

SIP ICT は Enhanced Location CAC で有効になっている場合、SIP Call-Info ヘッダーによって情報を渡します。これにより、発信側と着信側のクラスタは、ロケーションの帯域幅の差し引きをエンドツーエンドで処理できるようになります。図 13-34 は、渡された情報に関する 2 クラスタと一部の詳細の間のコールの例を示します。これは、ロケーション情報をクラスタからクラスタに渡す方法、また帯域幅の差し引きを行う方法を単に示します。

図 13-34　SIP を介してクラスタ間で渡されるロケーション情報

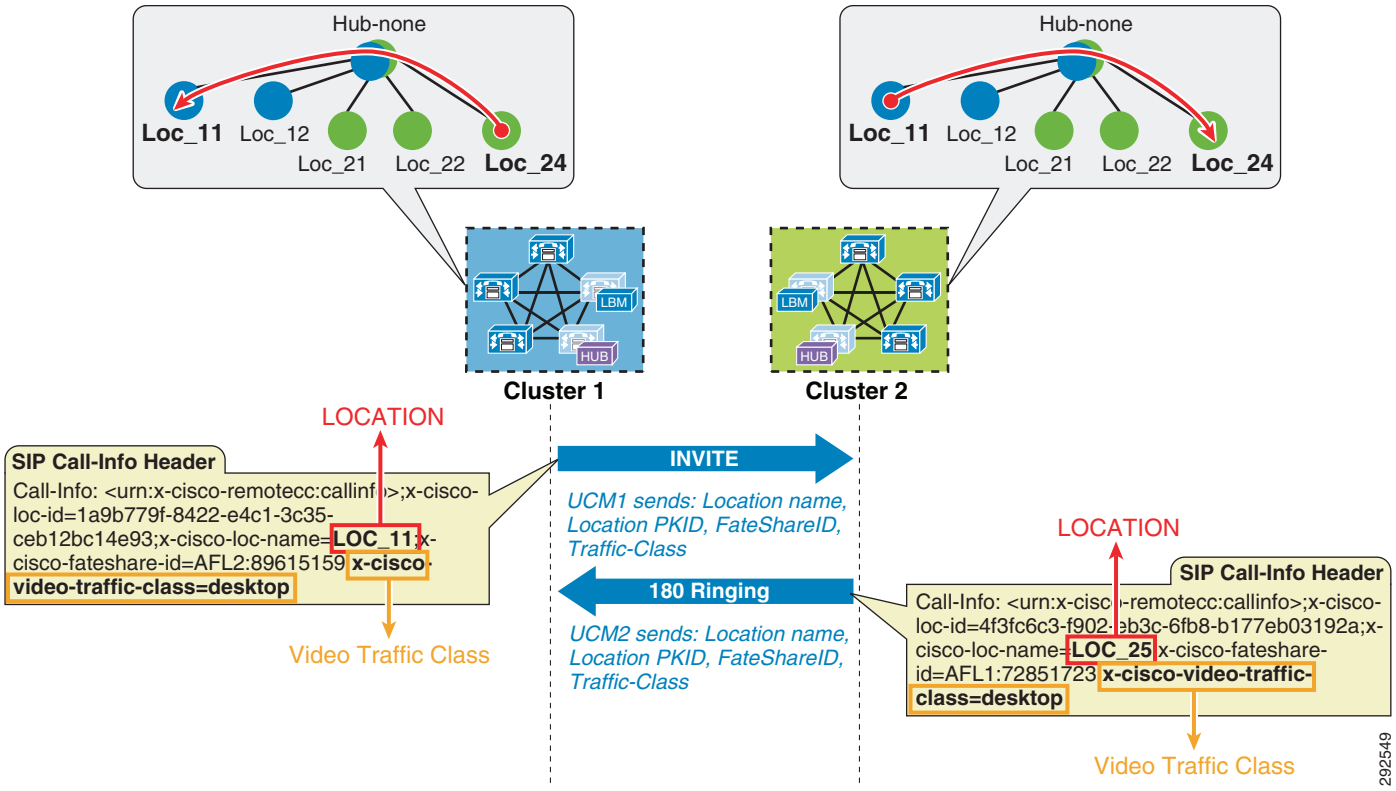


図 13-34 では、Cluster 1 は Cluster 2 に invite を送信し、call-info ヘッダーに、一意のコール ID など、その他の関連情報間の発信側のロケーション名およびビデオ トラフィック クラスを入力します。クラスタ 2 は情報の invite を受信すると、着信側を検索し、LBM レプリケーションからのメモリ内にあるグローバル トポロジから、発信側のロケーションと着信側のロケーション間のパスで CAC 要求を実行します。これが成功すると、クラスタ 2 は予約を複製し、着信デバイスにコールを拡張し、着信側のロケーション情報によって 180 の呼び出し音をクラスタ 1 に返します。クラスタ 1 は 180 の呼び出し音を受信すると着信デバイスのロケーション名を取得し、call-info ヘッダーに渡された情報から計算された同じ固有コール ID を使用して同じ帯域幅のルックアップ プロセスを通過します。成功した場合、コール フローも継続されます。両方のクラスタは call-info ヘッダーに同じ情報を使用するため、同じ call-ID を使用して同じコールの帯域幅を差し引きするため、二重の帯域幅の差し引きを回避できます。

ロケーションおよびリンク管理クラスタ

設定のオーバーヘッドを回避するために、ロケーションおよびリンク管理のクラスタは、グローバル トポロジのすべてのロケーションおよびリンクを管理するように設定できます。他のすべてのクラスタはロケーションからデバイスへの関連付けに必要なロケーションを一意に設定し、無制限以外のリンクまたは帯域幅値を設定しません。ロケーションおよびリンク管理のクラスタは設計概念で、ロケーションおよびリンクの全体のグローバル トポロジに設定された単なるクラスタですが、LBM のレプリケーション ネットワーク上の他のクラスタはすべて、帯域幅の値が無制限で、かつリンクを設定されていないロケーションのみで構成されていることに注意すべきです。クラスタ間の Enhanced Location CAC がイネーブルになり、LBM のレプリケーション ネットワークが設定されている場合、すべてのクラスタがネットワーク ビューを複製します。指定したロケーションおよびリンク管理のクラスタには、ロケーション、リンクおよび帯域幅の値を持つグローバル トポロジ全体があります。これらの値は、複製されると最も制限的になるため、すべてのクラスタで使用されます。この設計によって、多数の共通のロケーションが複数のクラスタ間で必要な配置の設定オーバーヘッドが軽減されます。

推奨事項

- ロケーションおよびリンク管理クラスタ：
  - 1 つのクラスタをクラスタ管理（ロケーションとリンクを管理するために選択したクラスタ）として選択する必要があります。
  - クラスタ管理は次のように設定する必要があります。

    企業内のすべてのロケーションは、このクラスタに設定されます。

    すべてのロケーションとリンクの帯域幅値と重みは、このクラスタで管理されます。
- 企業内の他のすべてのクラスタ：
  - 企業内の他のすべてのクラスタは、デバイスへの関連付けに必要なロケーション*のみ*を設定する必要があります。ロケーション間のリンクを設定して*はなりません*。このリンク情報は、クラスタ間の Enhanced Location CAC が有効な場合に管理クラスタから取得されます。
  - クラスタ間の Enhanced Location CAC が有効な場合、すべてのロケーションとリンクは管理クラスタから複製され、LBM は最小で、最も限定的な帯域幅と重み値を使用します。
- LBM は、複製後で最小の最も限定的な帯域幅と最も小さい重み値を常に使用します。

利点

- 単一クラスタから企業 CAC トポロジを管理します。
- クラスタが複数の共通のロケーションを共有する場合のロケーションとリンク設定のオーバーヘッドを軽減します。
- クラスタ間でロケーションおよびリンクの設定の誤りを軽減します。
- 企業の他のクラスタは、ロケーションからデバイスやエンドポイントへの関連付けに必要なロケーションにだけ設定を必要とします。
- グローバル ロケーション トポロジのモニタリングに単一のクラスタを提供します。

図 13-35 は、3 つのリーフ クラスタのロケーションおよびリンクの管理クラスタとして Cisco Unified Communications Manager Session Management Edition（SME）について説明します。

（注）　前述のように、クラスタはロケーションとリンクの管理クラスタとして機能できます。この例では、SME はロケーションとリンクの管理クラスタです。

図 13-35　ロケーションおよびリンクの管理クラスタとしての SME の例

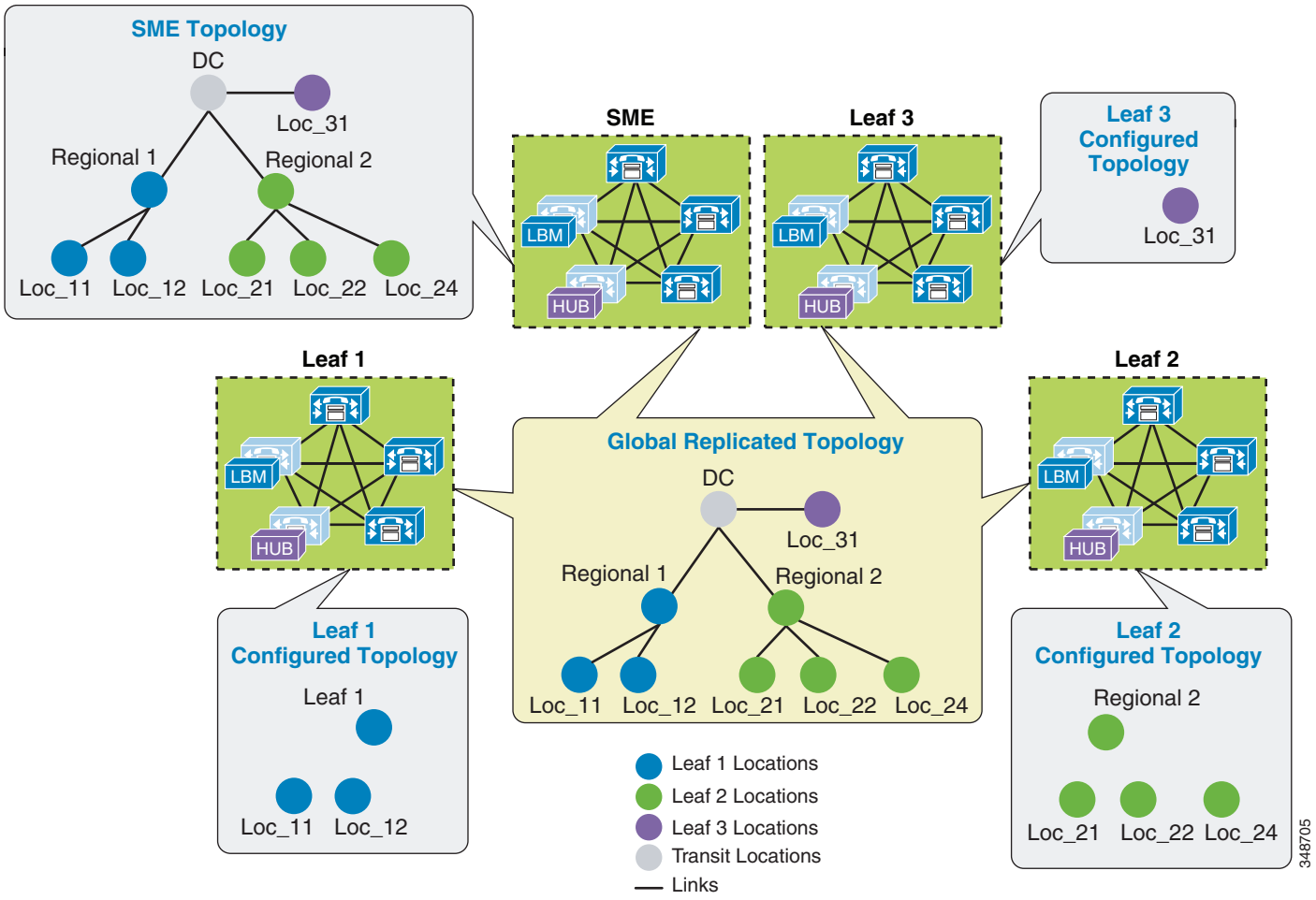


図 13-35 では 3 つのリーフ クラスタがあり、それぞれは、リージョン ロケーションおよびリモート ロケーションだけにデバイスがあります。SME にはロケーションおよびリンクで設定されているグローバル トポロジ全体があり、クラスタ間 LBM の複製は 4 つのすべてのクラスタの間でイネーブルです。SME がロケーションとリンク トポロジの全体を設定するため、すべてのロケーションが共通のロケーションですが、この例ではロケーションを共有するクラスタはありません。SME ではグローバル トポロジ全体が設定されていますが、リーフ 1、リーフ 2 とリーフ 3 は、デバイスやエンドポイントに関連付ける必要があるロケーションだけを設定することに注意してください。クラスタ間レプリケーション後に、すべてのクラスタはグローバル トポロジを持つようになります。

クラスタ間の Enhanced Location CAC の設計および配置の推奨事項と考慮事項

- クラスタは、ロケーションからデバイスへの関連付けに対してロケーションをローカルに設定することを要求します。
- 各クラスタはすぐにネイバー ロケーションで設定されて、各クラスタのトポロジが相互接続できるようにする必要があります。これは、ロケーションとリンクの管理クラスタの配置には適用されません。
- リンクは、リモート トポロジ間の相互接続ポイントを確立するように設定する必要があります。これは、ロケーションとリンクの管理クラスタの配置には適用されません。
- 共通のロケーションとリンクの帯域幅制限および重みの不一致は、帯域幅および重みの最小値を使用して解決されます。
- クラスタ全体でのロケーションの一貫した命名は重要です。「同じロケーション、同じ名前、および、異なるロケーション、異なる名前」の方法に従ってください。
- Hub_None ロケーションは各クラスタで一意であるように名前変更される必要があります。そうしないと、他のクラスタによって共通（共有）ロケーションになります。
- クラスタ ID は、サービスアビリティ レポートが使用できるように各クラスタで一意である必要があります。
- すべての LBM のハブはクラスタ間でフル メッシュです。
- LBM のハブは、リモート クラスタのハブに通信する責任があります。
- LBM のスポークは、他のリモート クラスタと直接通信することはありません。LBM のスポークはローカル LBM のハブを経由してリモート クラスタとの間でメッセージを送受信します。
- LBM のハブのグループ
  - ハブのロールに LBM を割り当てるために使用されます
  - LBM のハブのレプリケーション ネットワークの全ハブのハブ連絡先情報を複製する 3 つのリモート ハブのメンバーを定義するために使用されます
  - LBM は、LBM のハブのグループに割り当てられる場合のハブです。
  - LBM は LBM のハブのグループに割り当てられていない場合、スポークになります。
- クラスタに LBM のハブがない場合、または LBM のハブが実行されていない場合、クラスタは分離されて、クラスタ間 LBM のレプリケーション ネットワークに参加しません。

パフォーマンスのガイドライン

- 最大 2,000 のローカルに設定されたロケーション。2,000 ロケーションの制限は、ロケーションとリンクの管理クラスタにも適用されます。
- クラスタ間 CAC を持つ複製された最大 8,000 の合計ロケーション

Telepresence イマーシブ ビデオの Enhanced Location CAC

TelePresence エンドポイントがデスクトップから会議室といった広範囲に多様なコラボレーション エクスペリエンスを提供できるようにするため、Enhanced Location CAC には、TelePresence イマーシブ ビデオ コールに CAC を提供するサポートが含まれています。ここでは、TelePresence イマーシブ ビデオ CAC をサポートする Enhanced Location CAC の機能について説明します。

[ビデオコールトラフィッククラス（Video Call Traffic Class）]

[ビデオコールトラフィッククラス（Video Call Traffic Class）] は、すべてのエンドポイントに割り当てられた属性で、エンドポイントまたはトランクのビデオ分類タイプを確認するために SIP トランクでイネーブルにもできます。これは、Unified CM が、さまざまなコール フローをイマーシブまたは、デスクトップ ビデオ、またはその両方として分類し、ビデオ帯域幅またはイマーシブ帯域幅、またはその両方の適切なロケーションやリンク帯域幅の割り当てから、それに応じて差し引くことを可能にします。TelePresence エンドポイントには、エンドポイントに割り当てられた**イマーシブ**の設定不可能な [ビデオコールトラフィッククラス（Video Call Traffic Class）] があります。SIP トランクは、SIP トランク コールの帯域幅予約を差し引きするためにデスクトップ、イマーシブ、または混合ビデオとして分類できます。他のエンドポイントおよびトランクにはすべて、**デスクトップ ビデオ**の設定不可能な [ビデオコールトラフィッククラス（Video Call Traffic Class）] があります。エンドポイントおよびトランクの分類の詳細は、次の項で説明します。

TelePresence イマーシブ エンドポイントは CS4 の DSCP 値のメディアをデフォルトで表示し、デスクトップ ビデオ エンドポイントは推奨される QoS 設定によって AF41 のメディアをデフォルトで表示します。Cisco エンドポイントの場合、これは、設定可能な Unified CM QoS サービス パラメータの [ビデオ コールの DSCP（DSCP for Audio Calls）] および [TelePresence コールの DSCP（DSCP for TelePresence Calls）] によって実現されます。Cisco TelePresence エンドポイントは、Unified CM に登録されている場合、設定ファイルをダウンロードし、[TelePresence コールの DSCP（DSCP for TelePresence Calls）] の設定に QoS 設定を適用します。Unified Communications ビデオ対応エンドポイントは、Unified CM に登録されている場合、設定ファイルをダウンロードし、[ビデオ コールの DSCP（DSCP for Audio Calls）] の設定に QoS 設定を適用します。すべてのサードパーティ製ビデオ エンドポイントは、エンドポイントの手動設定自体を必要とし、静的に設定され、コール タイプによって QoS マーキングを変更しないことを意味します。したがって、正しい DSCP に Enhanced Location CAC の帯域割り当てを一致させることが重要です。Unified CM は、**デスクトップ**の [ビデオコールトラフィッククラス（Video Call Traffic Class）] を持つデバイスのビデオ帯域幅のロケーションとリンクの割り当てからデスクトップ ビデオ コールを差し引くことによって、これを実現します。エンドツーエンド TelePresence イマーシブ ビデオ コールは、**イマーシブ**の [ビデオコールトラフィッククラス（Video Call Traffic Class）] を持つデバイスまたはトランクのイマーシブ ビデオ帯域幅のロケーションとリンクの割り当てから差し引かれます。これによって、エンドツーエンド デスクトップ ビデオとイマーシブ ビデオ コールが正しくマーキングされ、コール アドミッション制御に正しくカウントできます。デスクトップ デバイスと TelePresence イマーシブ デバイス間のコールでは、帯域幅はビデオ帯域幅とイマーシブ ビデオ帯域幅の両方のロケーションとリンクの割り当てから差し引かれます。

エンドポイントの分類

Cisco TelePresence エンドポイントには**イマーシブ**の固定された設定不可能な [ビデオコールトラフィッククラス（Video Call Traffic Class）] があり、Unified CM でイマーシブとして識別されます。テレプレゼンス エンドポイントはデバイス タイプによって Unified CM に定義されます。デバイスを Unified CM に追加する場合、一般的なシングル スクリーンおよびマルチスクリーンのルーム システムがあるため、デバイス タイプの名前が TelePresence のデバイスは**イマーシブ**に分類されます。Unified CM のエンドポイントの機能を確認する別の方法として、Cisco Unified Reporting Tool に移動し、[システムレポート（System Reports）] > [Unified CM 電話機能リスト（Unified CM Phone Feature List）] を選択します。機能ドロップダウン リストで [TelePresence デバイスのイマーシブビデオサポート（Immersive Video Support for TelePresence Devices）] を、製品ドロップダウン リストで [すべて（All）] を選択します。ここには、**イマーシブ**に分類されているデバイス タイプがすべて表示されます。他のすべてのエンドポイントは、設定不可能なイマーシブ属性が不足しているため、[ビデオコールトラフィッククラス（Video Call Traffic Class）] が**デスクトップ**に固定されています。

帯域予約はビデオ コールのエンドポイントの分類によって決定され、表 13-12 に示されるようにロケーションおよびリンクの帯域幅プールから帯域幅を差し引きます。

表 13-12　エンドポイント タイプごとの帯域幅プールの使用

エンド ポイント A	エンド ポイント B	使用されるロケーションとリンクのプール
イマーシブ ビデオ（Immersive video）	イマーシブ ビデオ（Immersive video）	イマーシブ帯域幅（Immersive bandwidth）
イマーシブ ビデオ（Immersive video）	デスクトップ ビデオ（Desktop video）	イマーシブ帯域幅およびビデオ帯域幅（Immersive and video bandwidth）
デスクトップ ビデオ（Desktop video）	デスクトップ ビデオ（Desktop video）	ビデオ帯域幅（Video bandwidth）
オーディオ専用コール（Audio-only call）	任意（Any）	音声帯域幅（Audio bandwidth）

SIP トランクの分類

SIP トランクは、SIP トランク コールの帯域幅予約を差し引きするためにデスクトップ、イマーシブ、または混合ビデオとして分類できます。分類は発信側デバイス タイプと SIP トランクの Video Call Traffic Class によって決定されます。SIP トランクは、SIP プロファイルのトランク固有の情報によって次のように設定できます。

- イマーシブ：高解像度イマーシブ ビデオ
- デスクトップ：標準デスクトップ ビデオ
- 混合：イマーシブ ビデオとデスクトップ ビデオの組み合わせ

SIP トランクはこれらの 3 つの分類のいずれかに分類でき、ビデオまたは TelePresence マルチポイント コントロール ユニット（MCU）、固定ロケーションのビデオ デバイス、従来のロケーション CAC をサポートする Unified CM クラスタ、または Cisco TelePresence System Video Communications Server（VCS）を分類する場合に主に使用されます。

帯域予約はエンドポイントの分類およびビデオ コールの SIP トランクの分類によって決定され、表 13-13 に示されるようにロケーションおよびリンクの帯域幅プールから帯域幅を差し引きます。

表 13-13　SIP トランクおよびエンドポイント タイプごとの帯域幅プールの使用

エンドポイント（Endpoint）	SIP トランク	使用されるロケーションとリンクのプール
TelePresence エンドポイント	イマーシブ	イマーシブ帯域幅（Immersive bandwidth）
TelePresence エンドポイント	Desktop	イマーシブ帯域幅およびビデオ帯域幅（Immersive and video bandwidth）
TelePresence エンドポイント	混合	イマーシブ帯域幅およびビデオ帯域幅（Immersive and video bandwidth）
デスクトップ エンドポイント	イマーシブ	イマーシブ帯域幅およびビデオ帯域幅（Immersive and video bandwidth）

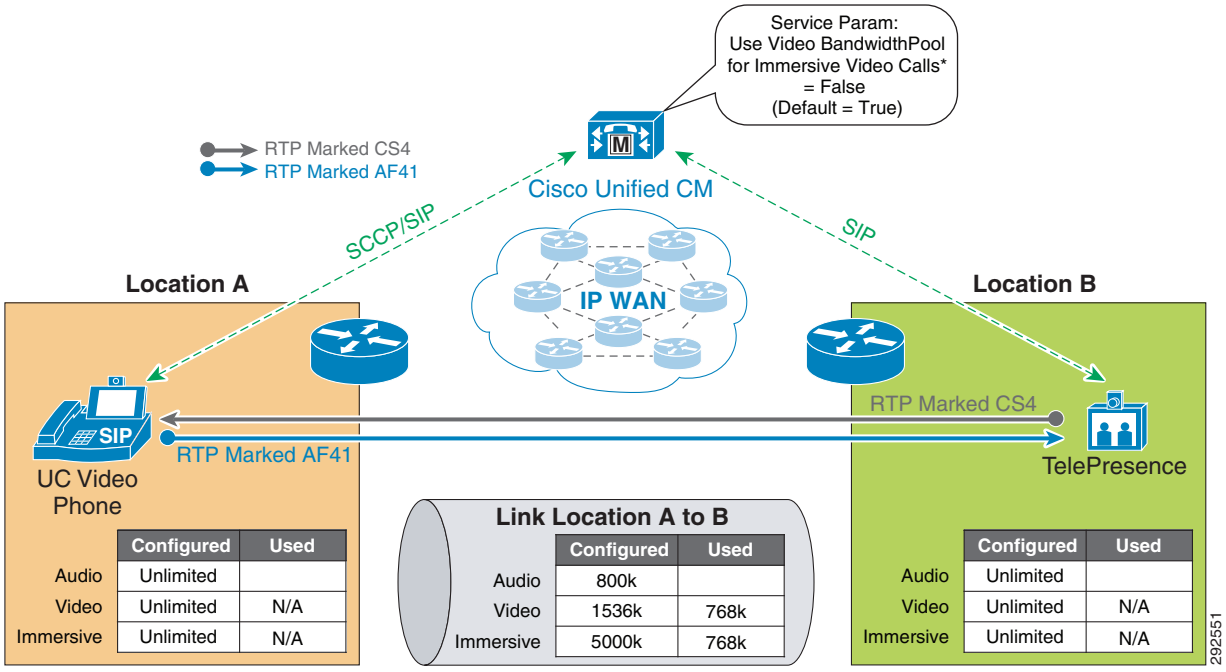
表 13-13　SIP トランクおよびエンドポイント タイプごとの帯域幅プールの使用（続き）

エンドポイント（Endpoint）	SIP トランク	使用されるロケーションとリンクのプール
デスクトップ エンドポイント	Desktop	ビデオ帯域幅（Video bandwidth）
デスクトップ エンドポイント	混合	イマーシブ帯域幅およびビデオ帯域幅（Immersive and video bandwidth）
ビデオ以外のエンドポイント	任意（Any）	音声帯域幅（Audio bandwidth）

デフォルトでは、イマーシブ エンドポイントまたはデスクトップ エンドポイントからのすべてのビデオ コールは、ロケーションおよびリンクのビデオ帯域幅プールから差し引かれます。この動作を変更するには、Unified CM の CallManager サービス パラメータの [イマーシブ ビデオ コールにビデオ帯域幅プールを使用（Use Video BandwidthPool for Immersive Video Calls）] を [False] に設定すると、イマーシブ ビデオ帯域幅の差し引きがイネーブルになります。これを有効にすると、イマーシブとデスクトップのビデオ コールが、それぞれのプールから差し引かれます。

前述したように、Unified Communications ビデオ エンドポイント（デスクトップ Video Call Traffic Class）と TelePresence エンドポイント（イマーシブ Video Call Traffic Class）の間のビデオ コールは、メディアを非対称にマーキングし、イマーシブ ビデオ CAC がイネーブルな場合、ビデオとイマーシブのロケーションおよびリンクの帯域幅プールから帯域幅を差し引きます。図 13-36 は、これについて説明しています。

図 13-36　マルチ サイト配置の Enhanced Location CAC 帯域幅の差し引きおよびメディア マーキング



さまざまなコール フローおよびロケーションとリンクの帯域幅プールの差し引きの例

次のコール フローは、Unified CM サービス パラメータの [イマーシブ ビデオ コールにビデオ帯域幅プールを使用（Use Video BandwidthPool for Immersive Video Calls）] が [False] に設定される場合の、ロケーションおよびリンクの帯域幅の差し引きの予想される動作を示します。

図 13-37 は、ロケーション L1 の TP-A とロケーション L2 TP-B 間のエンドツーエンド TelePresence のイマーシブ ビデオ コールについて説明します。エンドツーエンド イマーシブ ビデオ エンドポイントのコールは、有効なパスに沿ったロケーションおよびリンクのイマーシブ帯域幅プールから帯域幅を差し引きます。

図 13-37　エンドツーエンド TelePresence イマーシブ ビデオのコール フロー

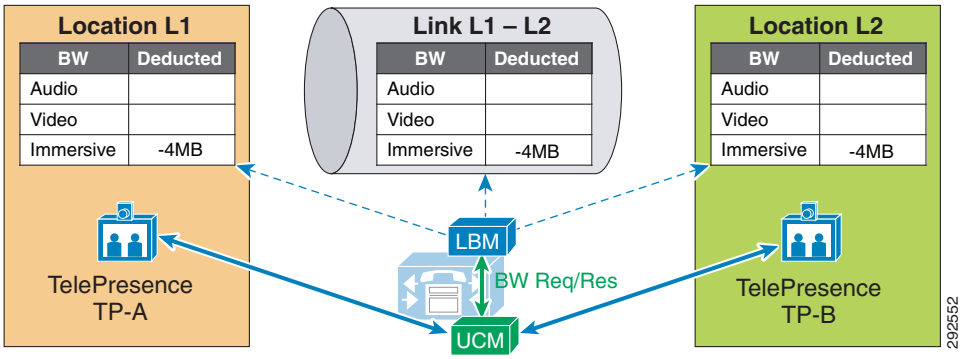


図 13-38 は、ロケーション L1 の DP-A とロケーション L2 DP-B 間のエンドツーエンド デスクトップ ビデオ コールについて説明します。エンドツーエンド デスクトップ ビデオ エンドポイントのコールは、有効なパスに沿ったロケーションおよびリンクのビデオ帯域幅プールから帯域幅を差し引きます。

図 13-38　エンドツーエンド デスクトップ ビデオのコール フロー

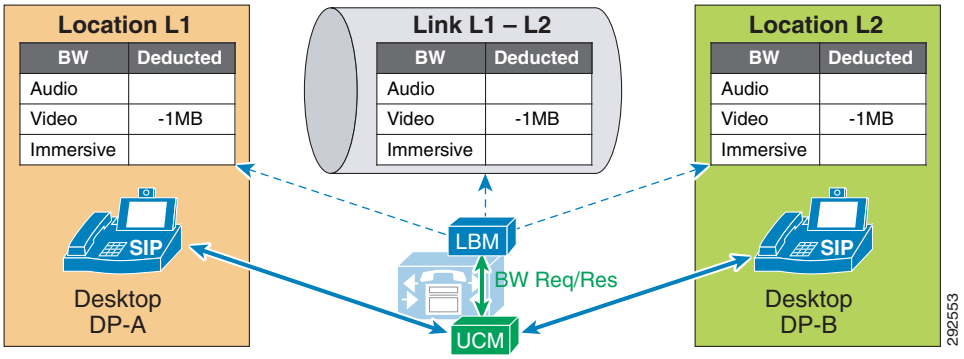


図 13-39 は、ロケーション L1 のデスクトップ ビデオ エンドポイント DP-A とロケーション L2 の TelePresence ビデオ エンドポイント TP-B 間のビデオ コールについて説明します。デスクトップ ビデオ エンドポイントと TelePresence ビデオ エンドポイント間の相互運用性コールは、有効なパスに沿ってビデオとイマーシブのロケーションおよびリンクの帯域幅プールから帯域幅を差し引きます。

図 13-39　デスクトップから TelePresence ビデオへのコール フロー

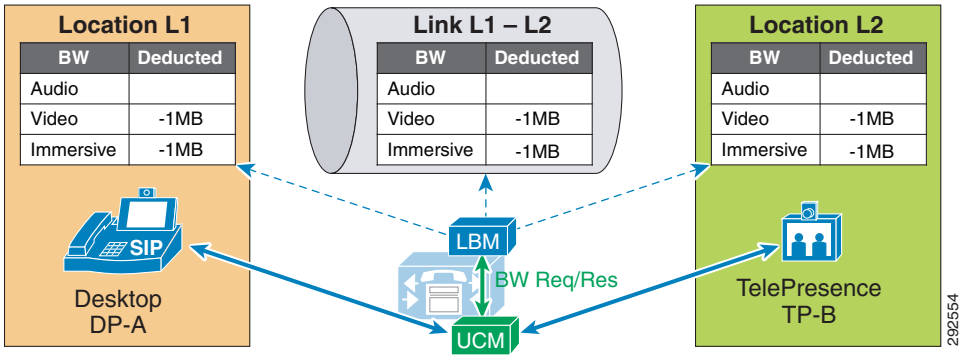


図 13-40 では、1 つのデスクトップ ビデオ エンドポイントと 2 つの TelePresence エンドポイントが、TelePresence MCU を指定するイマーシブの Video Traffic Class で設定した SIP トランクをコールします。エンドツーエンド イマーシブであるコールのイマーシブのロケーションおよびリンクの帯域幅プールから、およびデスクトップからイマーシブへのコールのビデオとイマーシブのロケーションおよびリンクの帯域幅プールから有効なパスに沿って帯域幅が差し引かれます。

図 13-40　MCU を使用したビデオ会議のコール フロー

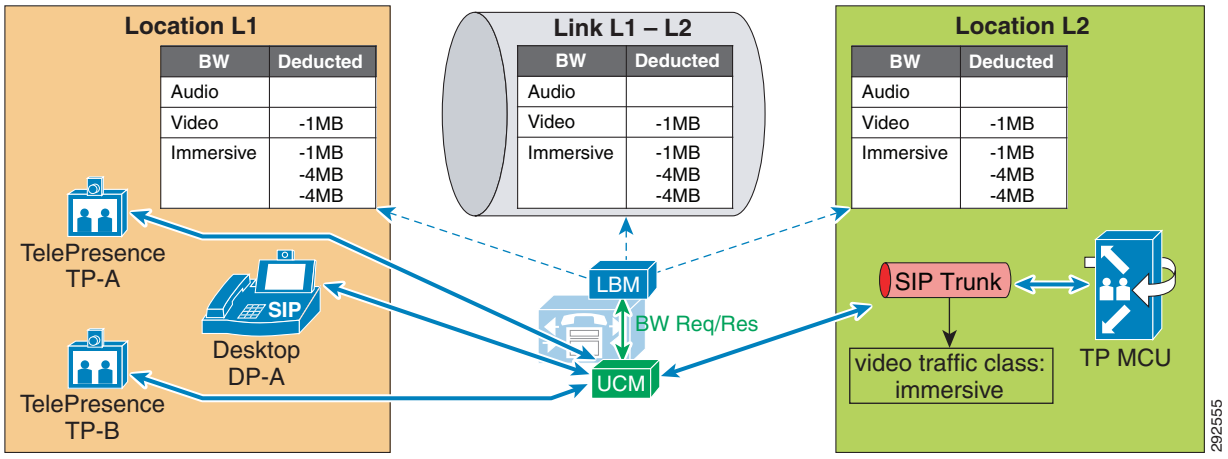


図 13-41 は、有効なパスに沿ったロケーションおよびリンクのイマーシブ帯域幅プールから帯域幅を差し引く、クラスタ全体でエンドツーエンド イマーシブ ビデオ コールを説明します。

図 13-41　クラスタ間のエンドツーエンド TelePresence ビデオのコール フロー

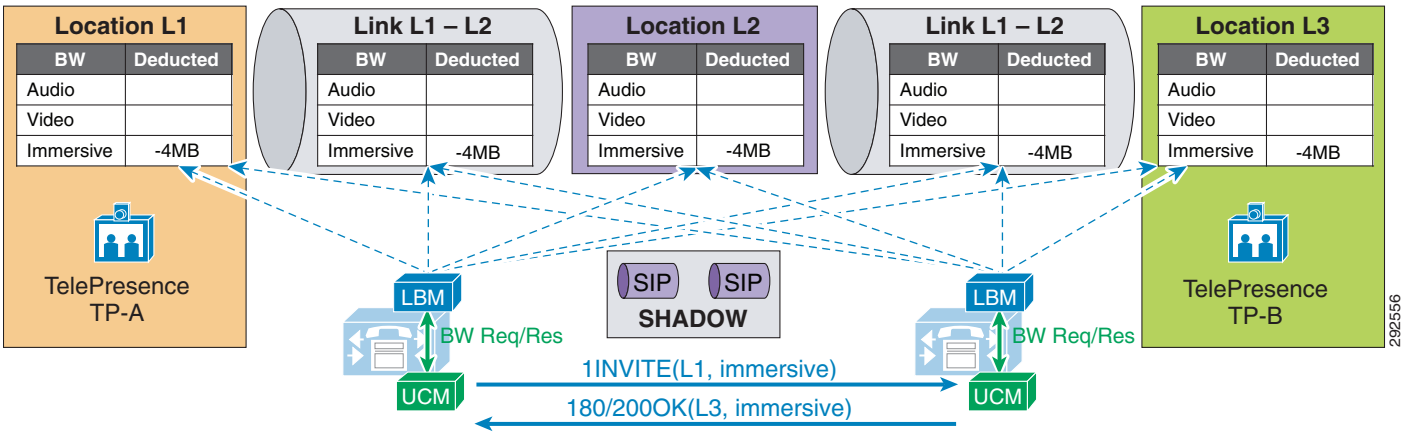


図 13-42 は、有効なパスに沿ったロケーションおよびリンクのビデオ帯域幅プールから帯域幅を差し引きする、クラスタ間のエンドツーエンド デスクトップ ビデオ コールについて説明します。

図 13-42　クラスタ間のエンドツーエンド デスクトップ ビデオ コールのコール フロー

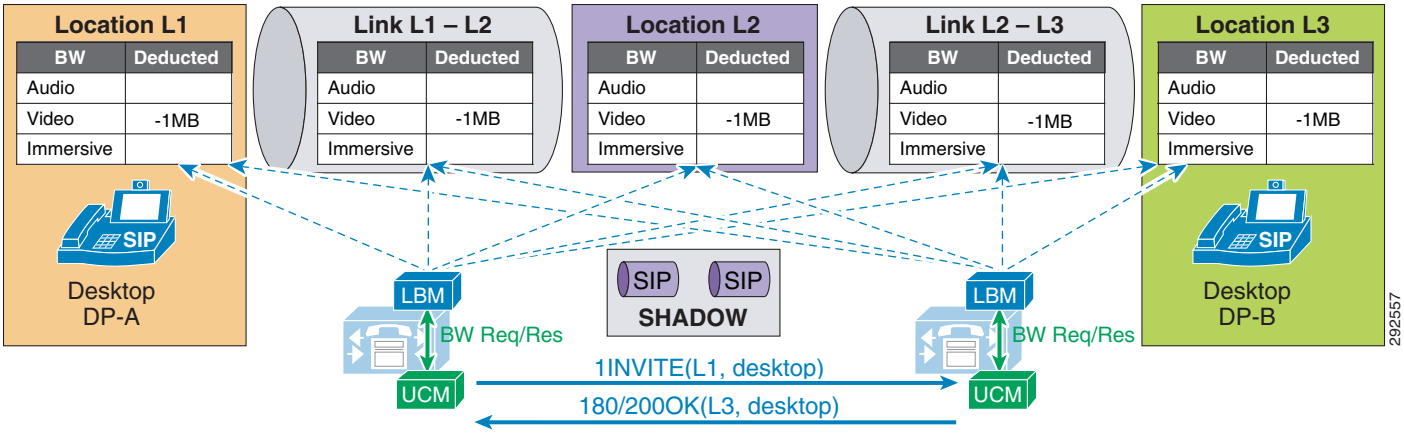
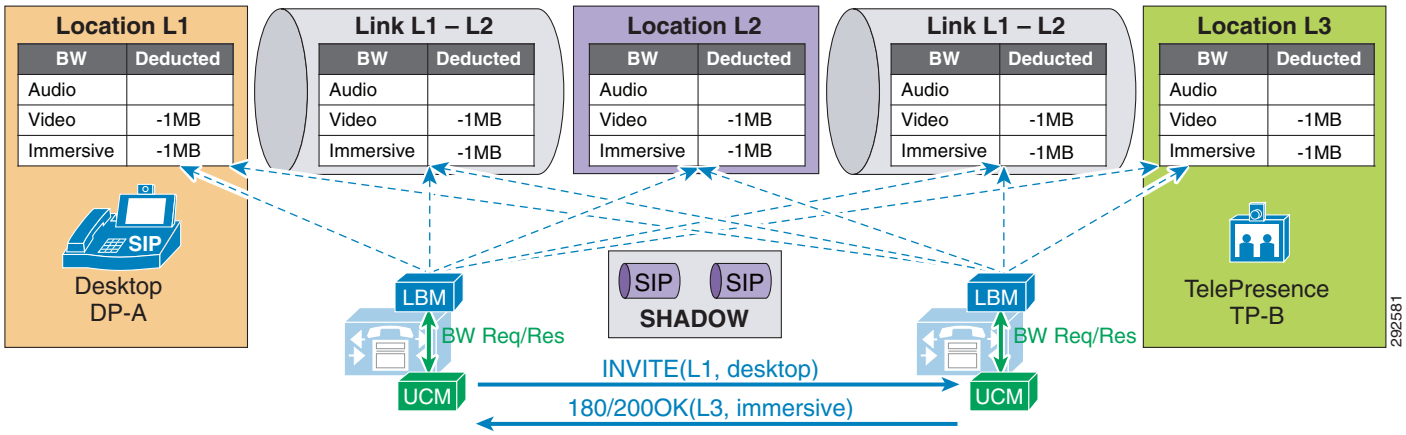


図 13-43 は、クラスタ全体で TelePresence エンドポイントをコールするデスクトップ ビデオ エンドポイントを示します。このコールは、有効なパスに沿ってロケーションおよびリンクのビデオとイマーシブ帯域幅の両方のプールから帯域幅を差し引きます。

図 13-43　クラスタ間のデスクトップから TelePresence ビデオへのコール フロー



ビデオ帯域幅の使用率とアドミッション制御

Unified CM で音声またはビデオ コールをネゴシエートすると、複数の異なるストリームがコールに関係するエンドポイント間で確立されます。コンテンツ共有のあるビデオ コールの場合、これにより、8 つ（またはそれ以上）もの単方向ストリームが生じる可能性があります。音声のみのコールの場合は、通常、最低でも 2 つのストリームが各方向に生成されます。ここでは、ネットワークでの帯域幅使用率と、Unified CM がアドミッション制御帯域幅アカウンティングでこれに対処する方法を説明します。

この項の説明を理解するために、次の点に注意してください。

- この項の図では、両方向矢印（<-->）を使用して 2 つの単方向ストリームを表します。
- 次のポイントは、Unified CM Enhanced Location CAC が設定済みの音声、ビデオ、およびイマーシブな割り当てから帯域幅を差し引く方法を要約したものです。詳細については、ロケーションおよびリンク（13-45 ページ）の項を参照してください。
  - オーディオ（音声のみのコール）：RTP ビット レートと IP、および UDP ヘッダーのオーバーヘッド
  - ビデオ（ビデオ コール）：RTP ビット レートのみ
  - イマーシブ（Cisco TelePresence エンドポイントによるビデオ コール）：RTP ビット レートのみ

- Enhanced Location CAC での帯域幅の差し引き：
  - 帯域幅の差し引きは二方向 RTP ストリームに対して行われ、対称的にルーティングされると想定されます（両方のストリームが同じパスを介してルーティングされる）。たとえば、80 kbps の G.711 音声コールは全二重ネットワークを介した各方向で 80 kbps です。つまり、送信ペアのワイヤの 80 kbps と受信ペアのワイヤの 80 kbps で、全二重の 80 kbps と等しくなります（図 13-44 を参照）。WAN では、トラフィックがに常に対称的にルーティングされるわけではありません。WAN を介したネットワークでルーティングする際に、アドミッション制御がメディアを正しく処理するように、必要に応じてネットワーク管理者に確認してください。
  - Real-Time Transport Control Protocol（RTCP）帯域幅オーバーヘッドは Unified CM 帯域幅割り当てには含まれません。これは、ネットワーク プロビジョニングに含まれる必要があります。RTCP は、ほとんどのコール フローで非常に一般的であり、ストリームに関する統計情報によく使用されます。また、リップシンクを適切に行えるように、ビデオ コールで音声を同期するためにも使用されます。場合によっては、エンドポイントで有効または無効に設定できます。RFC 3550 では、RTCP 用に追加されるセッション帯域幅の割合を 5 % に固定することが推奨されます。これは、RTCP セッションの場合、関連する RTP セッションの最大 5 % までであることが一般的であることを意味します。したがって、ネットワークで帯域幅使用率を計算する場合は、RTP セッションごとに RTCP のオーバーヘッドを追加する必要があります。たとえば、RTCP が有効な状態で G.711 音声コールが 80 kbps である場合、RTP と RTCP の両方に対してセッションごとに最大 84 Kbps を使用します（RTCP のオーバーヘッドは 4 kbps）。この計算は Enhanced Location CAC の差し引きには含まれませんが、ネットワーク プロビジョニングには含まれる必要があります。

（注）　ただし、別の DiffServ コード ポイント（DSCP）にこのトラフィックを再マーキングする方法があります。たとえば、RTCP では奇数の UDP ポートを使用し、RTP は偶数の UDP ポートを使用します。このため、UDP ポート範囲に基づいて分類できます。Network-Based Application Recognition（NBAR）を使用し、RTP ヘッダー [ペイロード タイプ（Payload Type）] フィールドに基づいて分類と再マーキングを行うこともできます。NBAR の詳細については、https://www.cisco.com を参照してください。ただし、エンドポイント マーキングがネットワークで信頼されている場合、RTCP オーバーヘッドは音声 RTP と同じ QoS クラス内のネットワークでプロビジョニングする必要があります（デフォルト マーキングは EF）。また、RTCP は RTP と同じマーキングを使用してエンドポイントでマークされることにも注意してください。デフォルトで、これは EF です（RTCP も EF とマークされます）。

図 13-44　RTCP が有効に設定された基本的な音声のみのコール

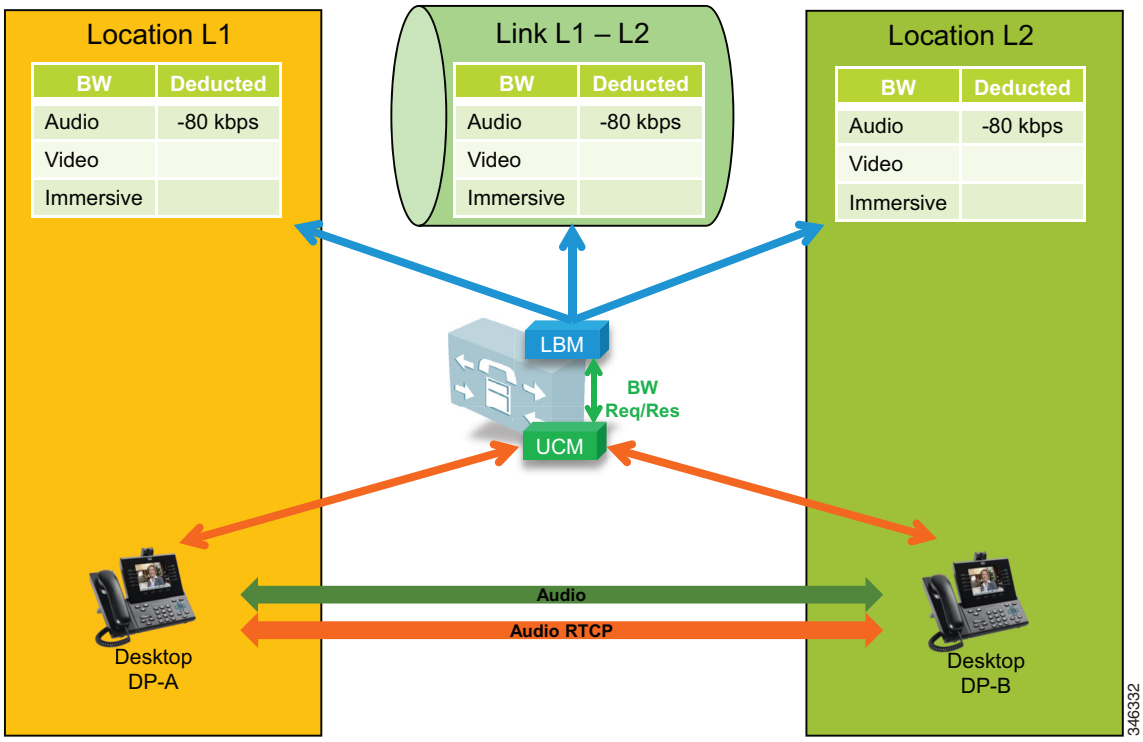


図 13-44 には、2 つのデスクトップ ビデオ電話が音声のみのコールに確立されています。このコール フローでは 4 つのストリームはネゴシエートされます。つまり、単一の二方向矢印によって記述される 2 つのオーディオ ストリームと、同様に二方向矢印で示されている 2 つの RTCP ストリームです。このコールについて、Location Bandwidth Manager（LBM）は、デスクトップ電話 DP-A と DP-B の間で確立されたコールのロケーション L1 と ロケーション L2 間から 80 kbps（ビット レート + IP/UDP のオーバーヘッド）を差し引きます。RTCP が有効なネットワークのレイヤ 3 で消費される実際の帯域幅は、このセクションの前半で説明したように、80 kbps ～ 84 kbps の間です。

図 13-45 には、2 つのデスクトップ ビデオ電話がビデオ コールに確立されています。このコール フローでは 8 つのストリームがネゴシエートされます。つまり、2 つのオーディオ ストリーム、2 つの音声関連 RTCP ストリーム、2 つのビデオ ストリーム、および 2 つのビデオ関連 RTCP ストリームです。この図でも、両方向矢印を使用して 2 つの単方向ストリームが表されます。この特定のコールは、64 kbps の G.711 音声、および 960 kbps のビデオを持つ 1024 kbps です（ビデオ コールの音声およびビデオ割り当てのみに対するビット レート）。この場合、LBM はデスクトップ電話 DP-A と DP-B の間で確立されたビデオ コールのロケーション L1 と L2 の間から 1024 kbps を差し引きます。RTCP は、ネットワークによるマーキングまたは再マーキングの方法に応じたプロビジョニングを考慮する必要のあるオーバーヘッドです。

図 13-45　RTCP が有効に設定された基本的なビデオ コール

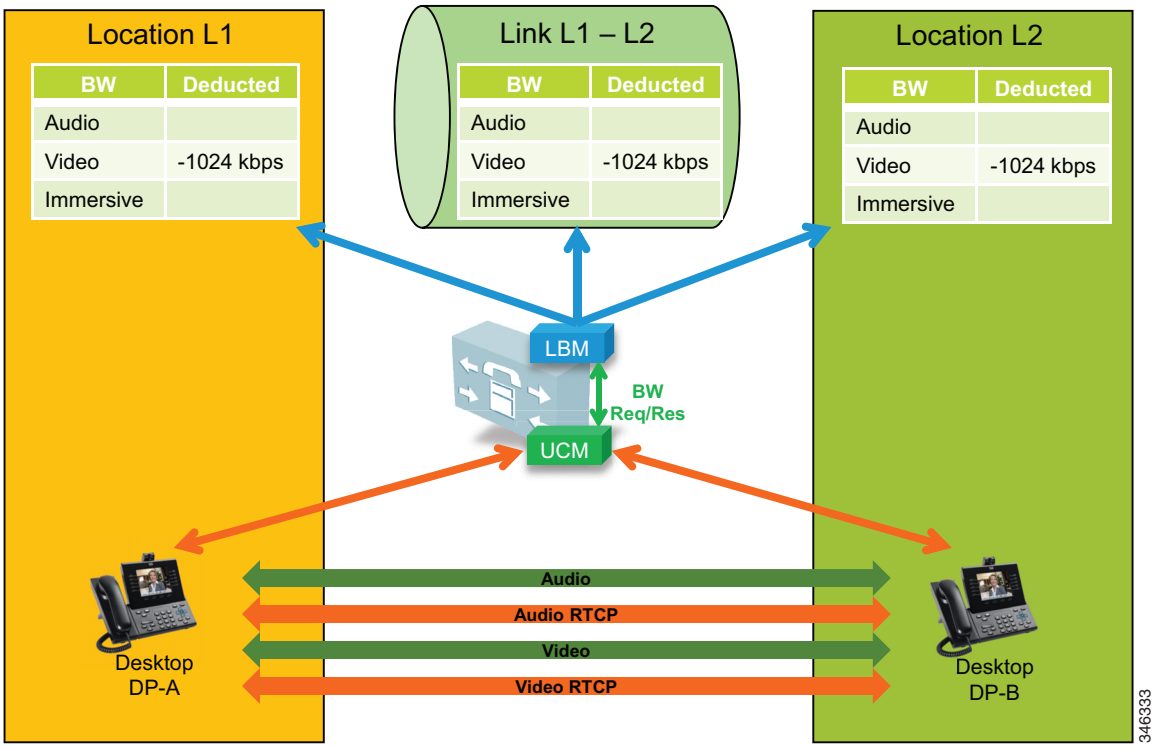
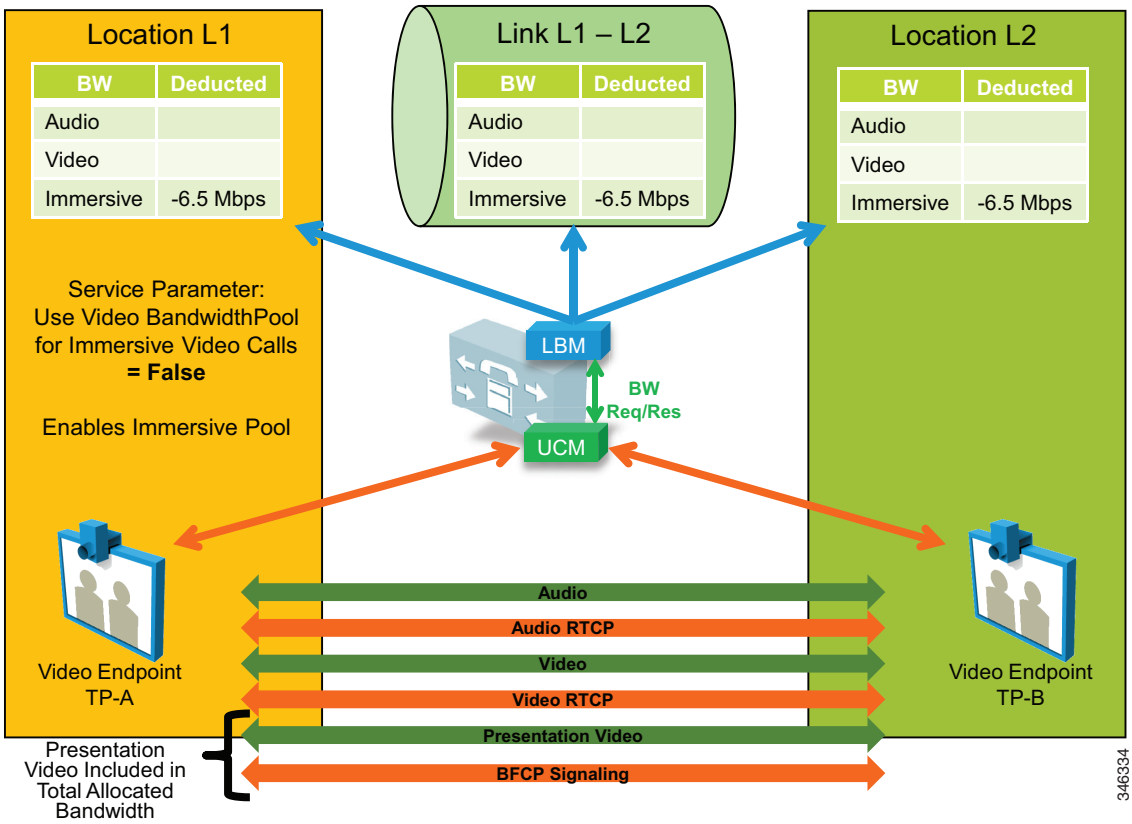


図 13-46 は、プレゼンテーション共有のあるビデオ コールの例です。これは、ネットワーク上で使用される帯域幅と比較すると、関連付けられたストリーム数と帯域幅の割り当てがより複雑なコールであるため、ネットワークでプロビジョニングする必要があります。図 13-46 は、プレゼンテーション共有に関して Binary Floor Control Protocol（BFCP）を有効にし、RTCP を有効にしているビデオ コールを示しています。Cisco TelePresence System EX、MX、SX、C、および Profile シリーズなど、SIP が有効に設定されているすべてのテレプレゼンス多目的またはパーソナル エンドポイントは同じように機能します。

図 13-46　RTCP および BFCP が有効なビデオ コールとプレゼンテーション共有



2 つのビデオ エンドポイント間でビデオ コールが確立されている場合、音声およびビデオ ストリームが確立され、ネゴシエートされたレートに応じて帯域幅が差し引かれます。Unified CM はリージョンを使用してコールに対する最大ビット レートを決定します。たとえば、最高の詳細度が 1 秒あたり 30 フレーム（fps）で 1080p の Cisco TelePresence System EX90 の場合、リージョン間でネゴシエートされるレートは 6.5 Mbps に設定する必要があります。このシナリオで使用する EX90s は、このセッションに対して約 6.1 Mbps を要します。エンドポイントがセッション中にプレゼンテーション共有を開始すると、BFCP はエンドポイント間でネゴシエートされ、新しいビデオ ストリーム間はエンドポイント設定に応じて 5 fps または 30 fps のいずれかで有効になります。このような場合、エンドポイントはメインのビデオ ストリームをスロットル ダウンして、プレゼンテーション ビデオを組み込み、セッション全体が、割り当てられた 6.5 Mbps の帯域幅を超えてセッション全体が使用しないようにできます。このため、プレゼンテーション共有の有無にかかわらず、平均帯域幅使用量は変わりません。

(注)　通常、プレゼンテーション ビデオ ストリームはプレゼンテーションを表示している 1 人以上のユーザの方向で単方向です。

お互いの間でコールをネゴシエーションする Cisco TelePresence System 500、1000、3000、および TX9000 シリーズなどのテレプレゼンス イマーシブおよびオフィス エンドポイントは、プレゼンテーション共有用のビデオがメインのビデオ セッションに割り当てられたもの以上の追加帯域幅であるため、Enhanced Location CAC から差し引かれないという点で少し異なる動きをします。図 13-47 は、これについて説明しています。

図 13-47　RTCP および BFCP が有効なビデオ コールとプレゼンテーション

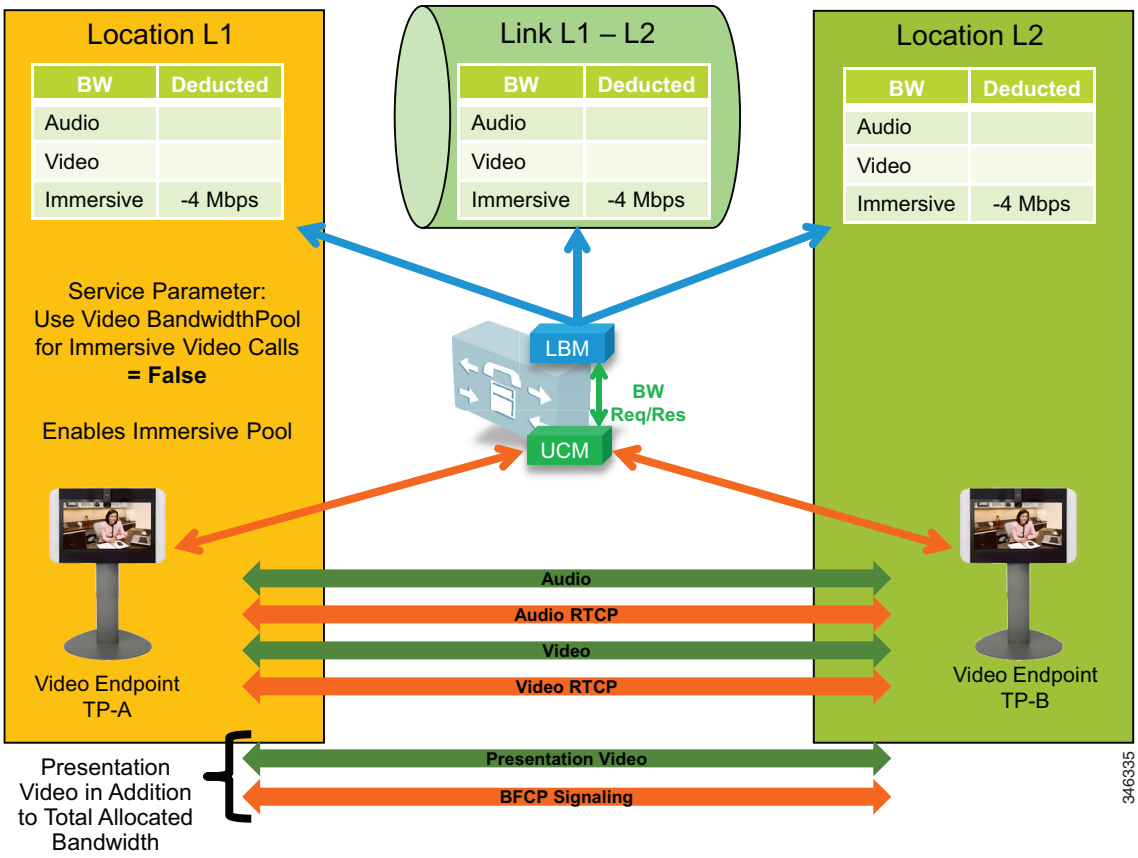


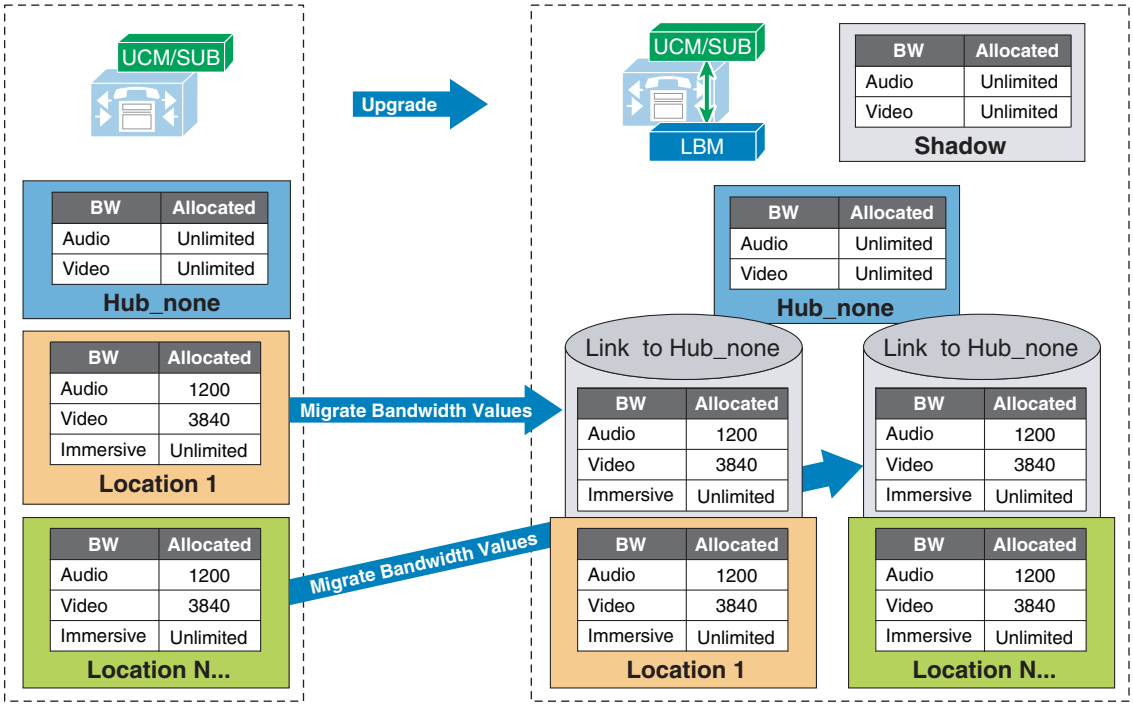
図 13-47 では、テレプレゼンス イマーシブ ビデオ エンドポイントがビデオ コールを確立し、プレゼンテーション共有を有効にしています。LBM はメインの音声およびビデオ セッション用に 4 Mbps をコール用のイマーシブ プールから差し引き、ビデオがエンドポイント間に確立されます。プレゼンテーション共有がアクティブ化されると、2 つのエンドポイントが BFCP を交換し、エンドポイントの設定に基づいて一方向で 5 fps または 30 fps でプレゼンテーション ビデオ ストリームをネゴシエーションします。5 fps で、使用される平均帯域幅は追加帯域幅オーバーヘッドの 500 kbps です。この帯域幅は、ビデオ コールに割り当てられた 4 Mbps 以上であり、ネットワークでプロビジョニングされる必要があります。30 fps で、プレゼンテーション ビデオの平均ビット レートは約 1.5 Mbps です。

（注） Cisco TelePresence System エンドポイントは、Telepresence Interoperability Protocol（TIP）を使用して、各方向で 2 つの音声およびビデオ RTP ストリームにマルチスクリーンと音声を多重化します。このため、回線上の実際のストリームは図に示されているものと異なる場合がありますが、プレゼンテーション ビデオ用の追加帯域幅オーバーヘッドの概念は同じです。

Location CAC から Enhanced Location CAC へのアップグレードおよび移行

従来のロケーション CAC のみをサポートする以前のリリースから Cisco Unified CM にアップグレードすることによって、Location CAC は Enhanced Location CAC に移行します。移行は、音声およびビデオ帯域幅のすべての以前に定義されたロケーションの帯域幅限度の取得と、ユーザ定義のロケーションと Hub_None の間のリンクへの移行で構成されます。これにより、実質的に、Unified CM ロケーション CAC の以前のバージョンがサポートするハブ アンド スポーク モデルが再作成されます。図 13-48 は、帯域幅情報の移行について説明します。

図 13-48　Unified CM アップグレード後の Location CAC から Enhanced Location CAC への移行



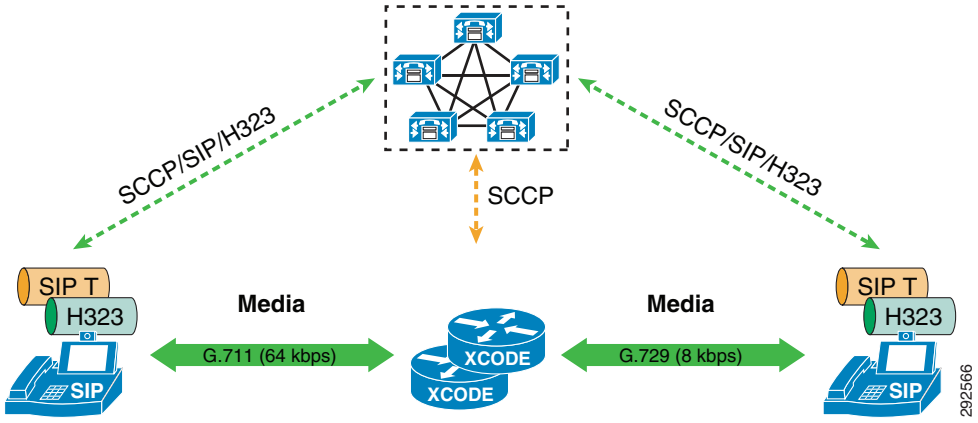
Enhanced Location CAC をサポートする Cisco Unified CM リリースへのアップグレード後の設定

- LBM は、Cisco CallManager サービスを実行している各 Unified CM サブスクライバでアクティブになります。
- Cisco CallManager サービスはローカル LBM と直接通信を行います。
- LBM グループまたは LBM ハブ グループは作成されません。
- すべての LBM サービスはフル メッシュです。
- クラスタ間の Enhanced Location CAC はイネーブルになりません。
- すべてのロケーション内の帯域幅値は無制限に設定されます。
- ロケーションに割り当てられる帯域幅値は、ユーザが定義したロケーションと Hub_None を接続するリンクに移行されます。
- イマーシブの帯域幅は無制限に設定されます。
- シャドウ ロケーションが作成されます。

- Phantom ロケーションおよびシャドウ ロケーションにはリンクがありません。
- MTP とトランスコーダの Enhanced Location CAC 帯域幅調整

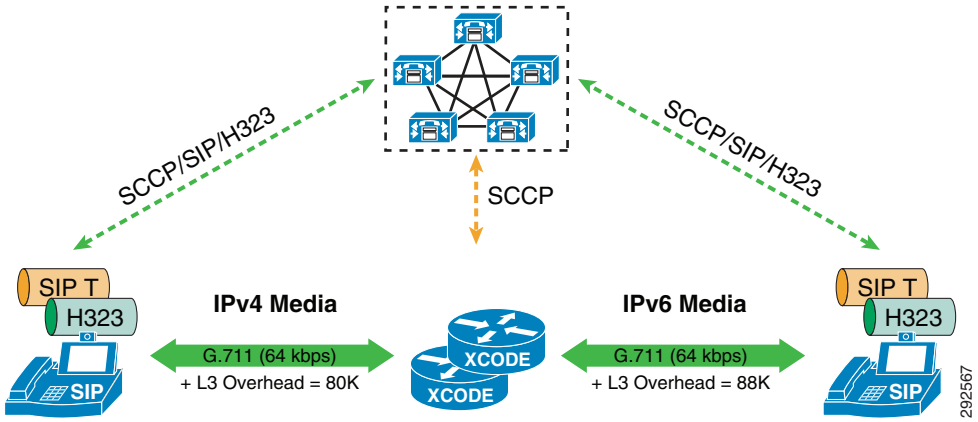
  挿入をトランスコードするために、ビット レートは接続の各レッグで異なります。図 13-49 は、これについて説明しています。

図 13-49　トランスコードのための異なるビット レートの例



デュアル スタック MTP 挿入の場合、ビット レートは各接続で異なりますが、帯域幅は IP ヘッダーのオーバーヘッドによって異なります。図 13-50 は、デュアル スタック MTP 挿入に IPv4 および IPv6 ネットワークで使用される帯域幅の違いについて説明します。

図 13-50　デュアル スタック MTP 挿入の帯域幅の違い



Enhanced Location CAC は、MTP とトランスコーダ間の帯域幅でこれらの違いを考慮しません。サービス パラメータの [ロケーション メディア リソース オーディオ ビット レート ポリシー (Locations Media Resource Audio Bit Rate Policy)] は最大帯域幅または最小帯域幅がロケーションおよびリンクのパスに沿って使用される必要があるかを決定します。最低ビット レート (デフォルト) または最高ビット レートは、帯域幅の使用量のこれらの違いを管理するために使用できます。

Enhanced Location CAC によるクラスタ間のエクステンション モビリティ

Enhanced Location CAC は、クラスタ間のエクステンション モビリティ（EMCC）を使用した設計をサポートしています。Unified CM は、クラスタ間のエクステンション モビリティ（EMCC）という機能によって、企業内のクラスタ間でエクステンション モビリティ ログインを実行する機能を提供します。詳細については、クラスタ間のエクステンション モビリティ（EMCC）（18-11 ページ）の項を参照してください。

EMCC 設計に Enhanced Location CAC を使用すると、Visiting クラスタが Visiting 電話機のロケーションをホーム クラスタに渡します。これにより、ホーム クラスタは登録時に Visiting 電話機に正しいロケーションを関連付けることができるようになります。EMCC 設計で Enhanced Location CAC を機能させるためには、次の要件を満たす必要があります。

- ホーム クラスタおよび Visiting クラスタの両方で、Cisco Unified CM 10.0 以降のリリースであること
- Visiting クラスタおよびホーム クラスタが同じクラスタ間 LBM のレプリケーション ネットワークにあること

Enhanced Location CAC および EMCC の両方を、製品マニュアルおよびこの SRND のガイドラインに従って設計および導入することができます。必要とする他の要件や特定の設定情報はありません。

コール アドミッション制御の設計上の考慮事項

この項では、さまざまな IP WAN トポロジに対して、コール アドミッション制御メカニズムを適用する方法について説明します。Unified CM Enhanced Location CAC のネットワーク モデル化のサポートによって、Unified CM は単純なハブ アンド スポークまたは MPLS トポロジのサポートに制限されませんが、現在はクラスタ間の拡張ロケーションとともに、Unified CM 配置モデルのほとんどのネットワーク トポロジをサポートできます。Enhanced Location CAC は依然としてネットワークを参照しない静的に定義されたメカニズムであるため、ネットワークの変更がアドミッション制御に影響するたびに、管理者は適宜 Unified CM をプロビジョニングする必要があります。これは、ネットワーク障害が発生し、メディア ストリームがネットワークの異なるパスを取る場合などに RSVP などのネットワーク対応のメカニズムが、その間隔を埋めてネットワークの動的変化をサポートできる場合です。これは、ロード バランシングされた二重またはマルチホーム WAN アップリンク、あるいは不等サイズのプライマリおよびバックアップ WAN アップリンクがある設計の場合がよくあります。

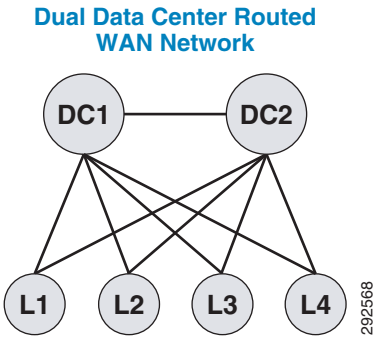
Enhanced Location CAC がどのように機能するか、および Enhanced Location CAC の設計および配置方法について確認するには、Unified CM Enhanced Location Call Admission Control（13-43 ページ）の項を参照します。

ここでは、いくつかの一般的なトポロジを調べ、それらのトポロジを管理するために Enhanced Location CAC を設計する方法について説明します。

デュアル データセンター設計

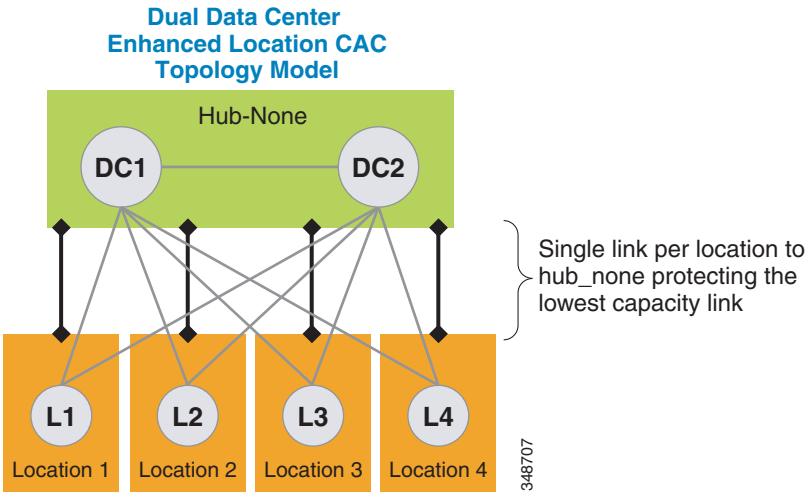
図 13-51 は、各リモート サイトに単一の WAN アップリンクがある単純なデュアル データセンター WAN ネットワーク設計について説明します。データセンターは、データ トラフィック用に余裕を持ってプロビジョニングされた高速 WAN 接続を介して相互接続します。

図 13-51　デュアル データセンター WAN ネットワーク



通常、リモート サイトからデータセンターへのこれらの WAN アップリンクは、ロードバランシングされているかプライマリ/バックアップ設定にあり、これらのシナリオを処理するスタティック CAC メカニズム用の制限方法があります。Enhanced Location CAC のこのマルチパス トポロジを設定できますが、重みのメトリックが変更されるまで 1 つのパスだけが有効なパスとして計算されてスタティックのままになります。このタイプのネットワーク トポロジをサポートする、よりよい方法は、2 つのデータセンターを Enhanced Location CAC の 1 つのデータセンターまたはハブ ロケーションとして設定し、各リモート サイト ロケーションに対して単一リンクを設定することです。図 13-52 は、Enhanced Location（E-L）CAC のロケーションとリンクのオーバーレイについて説明します。

図 13-52　デュアル データセンターの Enhanced Location CAC のトポロジのモデル



設計に関する推奨事項

リモート ロケーションへのリモート デュアルまたはより多くのリンクを持つリモートのデュアル データセンターに関する次の設計上の推奨事項は、ロードバランシング WAN 設計、プライマリ/バックアップ WAN 設計の両方に適用されます。

- 1 つのロケーション（Hub_None）は、両方のデータセンターを表します。
- リモート ロケーションと Hub_None 間の単一リンクは、通常の状態または最高帯域幅容量のリンクの障害時にリモート サイトのアップリンクをオーバーサブスクリプションから保護します。
- リモート サイトと Hub_None 間のリンク帯域幅割り当て容量は、単一リンクの適切な Unified Communications メディア用の最低帯域幅容量と同じです。たとえば、各 WAN アップリンクが音声トラフィックによってマークされた EF の 2 Mbps をサポートできる場合、障害状態または等コスト パスのルーティングをサポートするために、リンクの音声帯域幅値は 2 Mbps 以下である必要があります。

MPLS クラウド

Enhanced Location CAC ネットワークのモデルでマルチ プロトコル ラベル スイッチング（MPLS）の Any-to-Any 接続タイプのクラウドを設計する場合、1 つのロケーションは MPLS クラウドとして動作できます。このロケーションに関連付けられているデバイスはありませんが、このクラウドにアップリンクを持つすべてのサイトには、ロケーションに設定されたリンクがあります。このように、MPLS クラウドは、他のリモート ロケーションに複数の可変サイズの帯域幅 WAN アップリンクを相互接続するための中継ロケーションとして機能します。ここでは、多数の異なる MPLS ネットワークおよびその同等のロケーションとリンクのモデルを示します。

図 13-53 では、Hub_None は、サーバ、エンドポイントおよびデバイスが配置され、エンドポイントとデバイスだけ配置されているリモート ロケーションがあるキャンパス ロケーションを相互接続する中継ロケーションとして動作する MPLS クラウドを表します。リモート ロケーションから Hub_None への各リンクは、音声、ビデオ、およびイマーシブ メディア用に割り当てられた WAN アップリンクの帯域幅に従ってサイジングできます。

図 13-53　　単一 MPLS クラウド

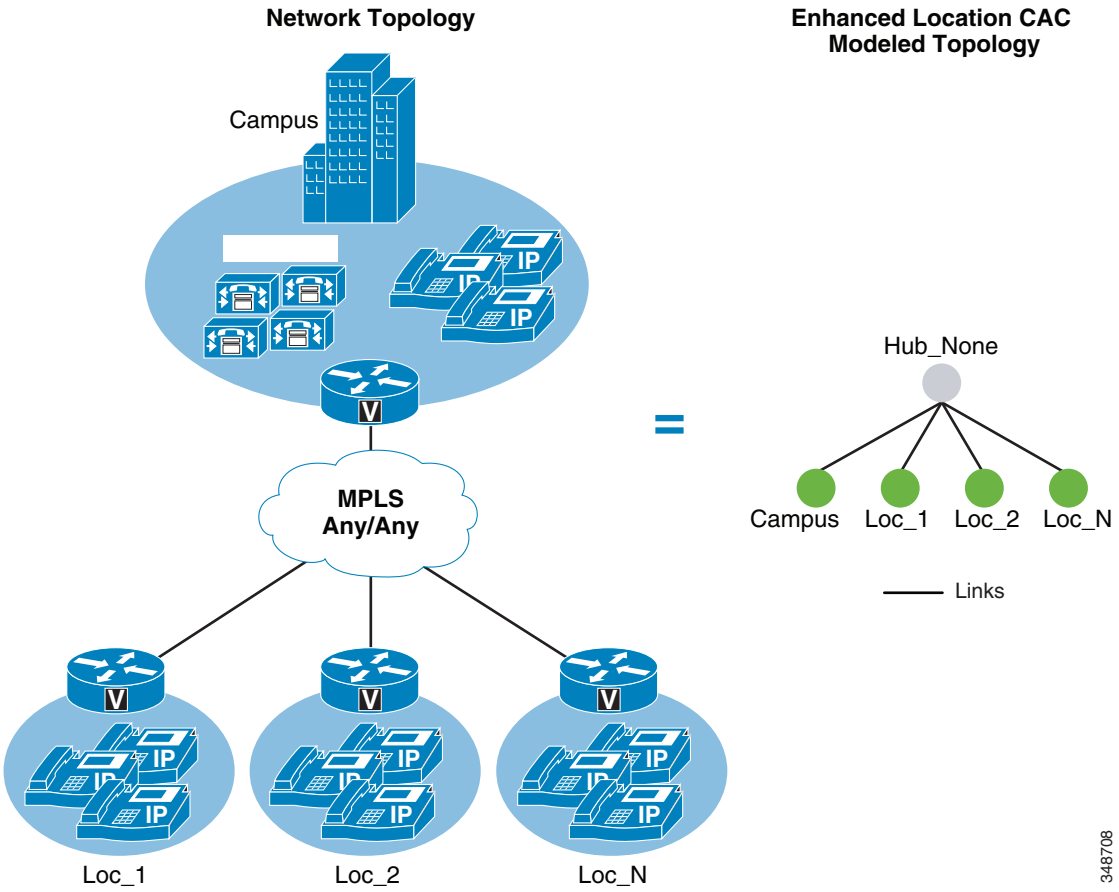


図 13-54 は、サーバ、エンドポイントおよびデバイスが配置され、エンドポイントとデバイスだけ配置されているリモート ロケーションがあるキャンパス ロケーションを相互接続する中継ロケーションとして動作する 2 つの MPLS クラウドを示します。キャンパスは、両方のクラウドにも接続されています。リモート ロケーションから MPLS クラウドへの各リンクは、音声、ビデオおよびイマーシブ メディア用に割り当てられた WAN アップリンクの帯域幅に従ってサイジングできます。この設計は、各地理的ロケーションで異なるプロバイダーからの個別の MPLS クラウドを持つ、大陸間にまたがる企業で一般的です。

図 13-54　個別の MPLS クラウド

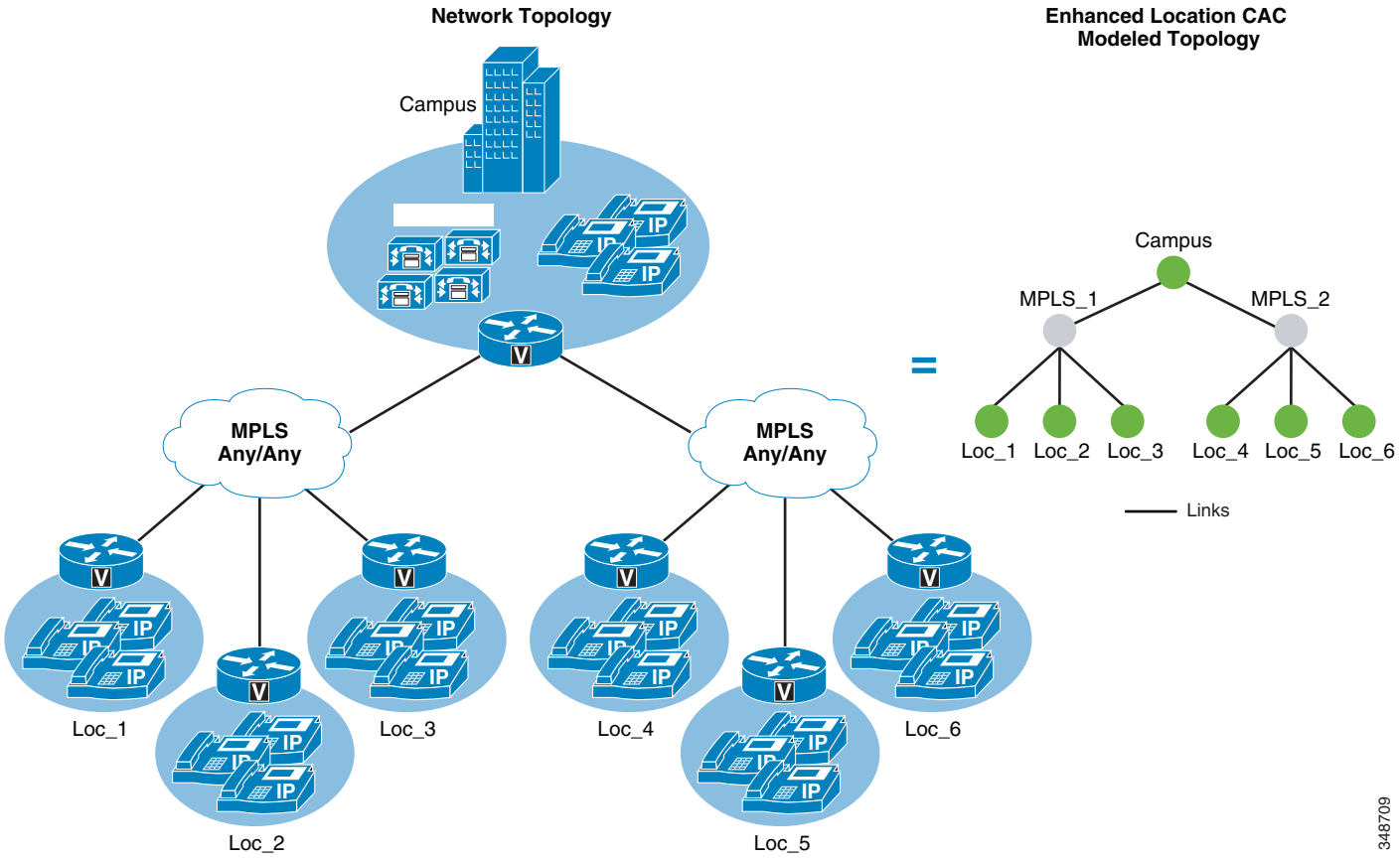
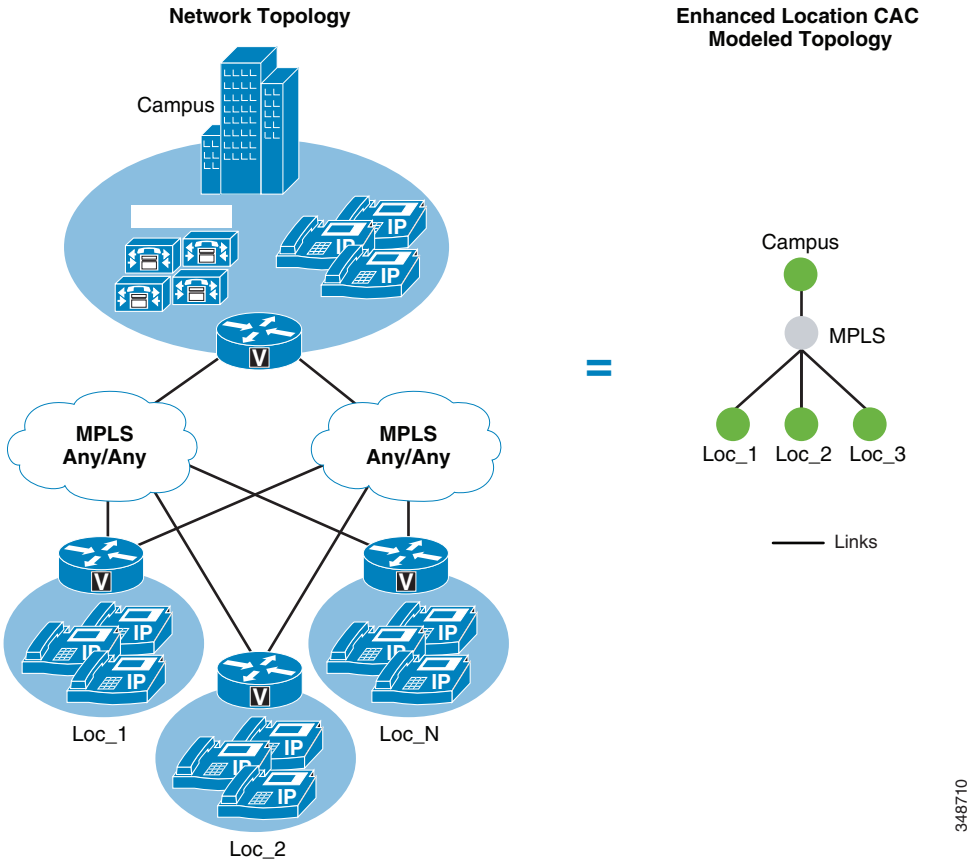


図 13-55 は、各サイトが各クラウドへの 1 の接続を持ち、等コストのロード バランシングされた方法またはプライマリ/バックアップ シナリオで MPLS クラウドを使用する、異なるプロバイダーから複数の MPLS クラウドを示します。どちらの場合でも、この設計は、1 つのロケーションが両方のクラウドを表して単一リンクが 2 つの最低容量のリンクを表すデュアル データセンター設計と同等です。

図 13-55　デュアル MPLS クラウドに接続されたリモート サイト



設計に関する推奨事項

- MPLS クラウドは、エンドポイントを含まなくてもロケーションを相互接続するハブとして使用されるロケーションとして設定する必要があります。
- MPLS クラウドは、他のリモート ロケーションに複数の可変サイズの帯域幅 WAN アップリンクを相互接続するための中継場所として機能します。
- デュアル MPLS クラウドへの接続を持つリモート サイトは、その接続を単一リンクとして扱い、ネットワーク障害状態時のオーバーサブスクリプションを回避するためにリンクの最低容量までサイジングする必要があります。

ビデオの展開に関するコール アドミッション制御の設計上の推奨事項

ここでは、Enhanced Location CAC、およびビデオの展開を設計する際に Quality of Service（QoS）に適用できる設計上の考慮事項と推奨事項について説明します。

アドミッション制御と QoS は相互に補完し、多くの場合は共存します。オーディオとビデオのエンドポイント、音声とビデオのゲートウェイ、音声メッセージ、会議など、最新のシスコ製品サービスは、IP DiffServ コード ポイント（IP DSCP）に基づいてネイティブ QoS パケット マーキングをすべてサポートします。ただし、Jabber for Windows クライアントは、Windows オペレーティング システムが、アプリケーション、IP アドレス、および UDP/TCP ポート範囲を使用するグループ ポリシー オブジェクト（GPO）を使用して DSCP のトラフィックをマーキングする必要があるため、他のクライアントと同じようにネイティブ マーキング機能に厳密に従うことはありません。グループ ポリシー オブジェクトは、トラフィックをマーキングする機能という点で、ネットワーク アクセス リストと非常に類似した機能です。

QoS を使用しないと、許可されたトラフィックが許可されていないトラフィックまたは他のトラフィックの分類よりも上位を求めるネットワーク リソースを使用できるように、ネットワークがメディアの優先順位を付けられないため、QoS はアドミッション制御に必要不可欠です。Unified CM では、QoS の CallManager サービス パラメータに主な 5 つの QoS 設定があります。これらは、エンドポイント メディア分類に適用可能で、イマーシブおよびデスクトップで分類されたエンドポイント（Telepresence イマーシブ ビデオの Enhanced Location CAC（13-64 ページ）の項を参照）が、イマーシブまたはデスクトップのビデオ分類に基づいたメディアに対して異なる QoS マーキングも設定できるようにします。表 13-14 では、デフォルト設定および Per-Hop Behavior（PHB）相当とともに、主な 5 つの DSCP 設定を示します。

表 13-14　エンドポイント メディア分類の QoS 設定

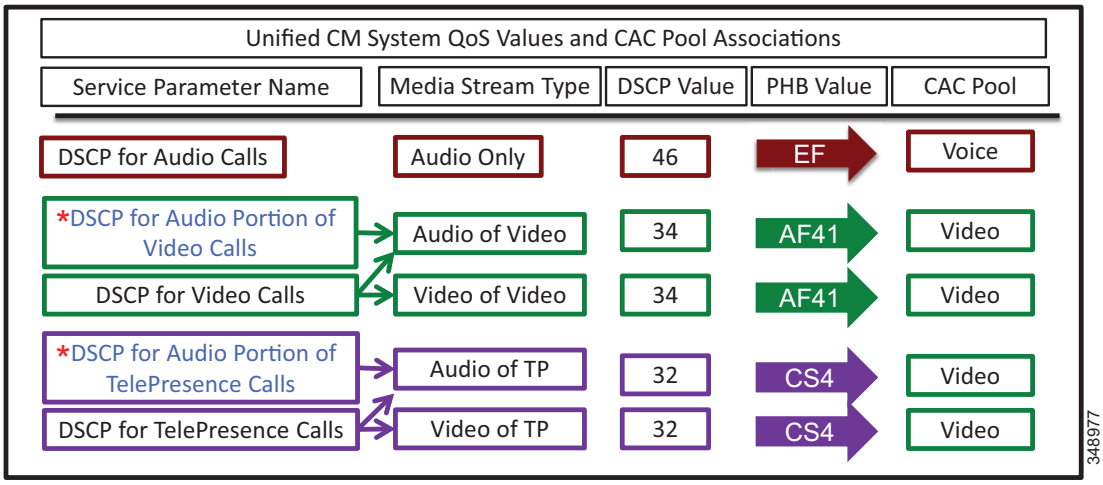
[Cisco CallManager サービス パラメータ（Cisco CallManager Service parameters）] > [クラスタ全体のパラメータ（システム：QoS）（Clusterwide Parameters（System - QoS））]	デフォルト値（Default Value）	PHB 相当
音声コールの DSCP（DSCP for Audio Calls）	46	EF
ビデオ コールの DSCP（DSCP for Audio Calls）	34	AF41
ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）	34	AF41
TelePresence コールの DSCP（DSCP for TelePresence Calls）	32	CS4
TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）	32	CS4

[音声コールの DSCP（DSCP for Audio Calls）] 設定は、オーディオ専用コールを発信するデバイスに使用されます。[ビデオ コールの DSCP（DSCP for Audio Calls）] 設定は、「デスクトップ」に分類されるデバイスのオーディオとビデオのトラフィックに使用されます。[TelePresence コールの DSCP（DSCP for TelePresence Calls）] は、「イマーシブ」に分類されるデバイスのオーディオとビデオのトラフィックに使用されます。[ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）] および [TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）] がビデオ エンドポイントのサブセットに現在適用可能で、分類に基づいてビデオ コール タイプを使用するビデオ コールのオーディオ部分のみを区別します。詳細については、信頼されているエンドポイント（13-100 ページ）の項を参照してください。

Telepresence イマーシブ ビデオの Enhanced Location CAC（13-64 ページ）の項で説明したように、Cisco Unified CM E-LCAC には、他のビデオ コールと別に TelePresence コールのアドミッション制御を実行する機能があります。E-LCAC は、エンドポイントと SIP トランクを「イマーシブ」または「デスクトップ」に分類することでこの機能を実行します。このように分類すると、イマーシブに分類されたデバイスおよびトランクの個別のイマーシブ帯域幅プールから帯域幅を差し引く機能が Unified CM に付与されます。デフォルトでは、LBM は、分類に関係なくビデオ帯域幅プールからビデオをすべて差し引きます（Unified CM's CallManager サービス パラメータ [イマーシブ ビデオ コールにビデオ帯域幅プールを使用（Use Video BandwidthPool for Immersive Video Calls）] を [True] に設定）。

また、デフォルトでは、イマーシブと分類されたすべてのエンドポイントの DSCP が CS4 に設定されており（DSCP 32：[TelePresence コールの DSCP（DSCP for TelePresence Calls）]）、デスクトップ エンドポイントの DSCP は AF41 に設定されています（DSCP 34：[ビデオ コールの DSCP（DSCP for Audio Calls）]）。QoS および E-LCAC のデフォルト設定は DSCP を区別しますが、同じ E-LCAC 帯域幅プールからすべてのビデオを差し引きます。図 13-56 では、QoS と E-LCAC 帯域幅プールの関連性、およびイマーシブとデスクトップに分類されたデバイスのデフォルト設定を示します。

図 13-56　CAC 帯域幅プールのデフォルト QoS 設定



[TelePresence コールの DSCP（DSCP for TelePresence Calls）] はイマーシブ分類で、[ビデオ コールの DSCP（DSCP for Audio Calls）] はデスクトップ分類です。

Enhanced Location CAC の設計上の考慮事項と推奨事項

ビデオの Enhanced Location CAC を設計する場合は、この項に示す設計上の推奨事項と考慮事項に従ってください。

設計に関する推奨事項

次の設計上の推奨事項は、Enhanced Location CAC を使用するビデオ ソリューションに適用されます。

- デスクトップ ビデオと Telepresence ビデオの区別が必要な場合に Unified Communications ビデオ（デスクトップ分類）と TelePresence ビデオ（イマーシブ分類）を配置する場合、Unified CM サービス パラメータの [イマーシブ ビデオ コールにビデオ帯域幅プールを使用（Use Video Bandwidth Pool for Immersive Video Calls）] が [false] に設定されていることを確認してください。これは、TelePresence コールのイマーシブ帯域幅プールをイネーブルにします。
- Enhanced Location CAC では、TelePresence エンドポイントを、Unified Communications ビデオ エンドポイントと同じロケーションで管理できます。TelePresence コールが Enhanced Location CAC によって追跡されない場合は、イマーシブ ロケーションとリンクの帯域幅プールを [無制限（unlimited）] に設定します。これにより、イマーシブに分類された TelePresence または SIP トランクで CAC が行われないようにします。TelePresence コールが Enhanced Location CAC によって追跡される場合は、イマーシブのロケーションおよびリンクの帯域幅プールを、ロケーションとリンク パスで許容される使用ビット レートおよびコール数に応じた値に設定します。
- クラスタ間 SIP トランクはシャドウ ロケーションに関連付けられている必要があります。
- Cisco Unified CM では、UC ビデオ エンドポイントと TelePresence エンドポイントの DiffServ コード ポイント（DSCP）設定を区別するために、2 つの異なる、クラスタ全体の QoS サービス パラメータが使用されます。TelePresence では [TelePresence コールの DSCP（DSCP for TelePresence Calls）] QoS パラメータが使用され、Cisco UC ビデオ エンドポイントでは [ビデオ コールの DSCP（DSCP for Audio Calls）] QoS サービス パラメータが使用されます。
- デフォルトの QoS マーキングでビデオをマーキングする場合は、次の推奨事項が適用されます。
  - UC エンドポイントのみを配置し、TelePresence エンドポイントを配置しないサイトの場合、着信 CS4 とマークされたトラフィックに対応し、CS4 とマークされたメディアの QoS 処理を行うために、着信 WAN QoS 設定で CS4 DSCP クラスが AF41 QoS トラフィック クラスに追加されていることを確認します。
  - UC TelePresence エンドポイントのみを配置し、UC エンドポイントを配置しないサイトの場合、着信 AF41 とマークされたトラフィックに対応し、AF41 とマークされたメディアの QoS 処理を行うために、着信 WAN QoS 設定で AF41 DSCP クラスが CS4 QoS トラフィック クラスに追加されていることを確認します。

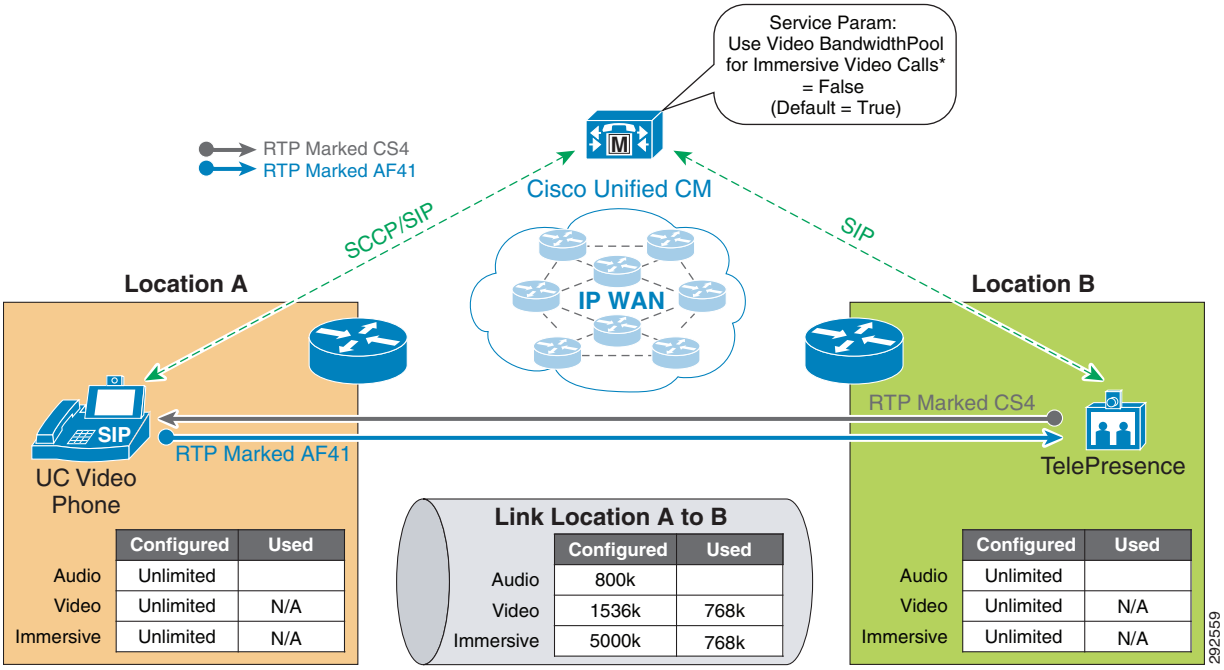
設計上の考慮事項

イマーシブ ビデオ コールに Enhanced Location CAC を展開すると、イマーシブに分類されたエンドポイントがデスクトップに分類されたエンドポイントに接続された場合に相互運用可能なコールが、デフォルトで非対称にマーキングされるため、DSCP のマーキングが両方の QoS クラスに与える影響を考慮します。

DSCP QoS マーキング

TelePresence ビデオの相互運用可能なコールの DiffServ コード ポイント（DSCP）QoS マーキングは、非対称です。UC エンドポイントには AF41 が使用され、TelePresence エンドポイントには CS4 が使用されます。AF41 と CS4 は Unified CM でのデフォルト設定であり、これらのデフォルトの変更は、ネットワーク インフラストラクチャの QoS 設定と整合している必要があります（該当する場合）。TelePresence エンドポイントは、ビデオ コールを DSCP 値 CS4 でマークします。これは、デフォルトの [TelePresence コールの DSCP（DSCP for TelePresence Calls）] 設定と整合性が取れています。UC エンドポイントは、コールを DSCP 値 AF41 でマークします。これは、デフォルトの [ビデオ コールの DSCP（DSCP for Audio Calls）] 設定と整合性が取れています。図 13-57 に、メディア マーキングと帯域幅アカウンティングを示します。

図 13-57　Enhanced Location CAC を使用したマルチサイト配置での帯域幅の差し引きとメディア マーキング



TelePresence ビデオの相互運用性コールの帯域幅アカウンティング

TelePresence および UC で相互運用可能なビデオ コールに対する Enhanced Location CAC は、図 13-57 に示されるように、ビデオとイマーシブのロケーションおよびリンクの帯域幅プールから帯域幅を差し引きます。これは、QoS で分類されたストリームの両方のタイプが、エンドポイント間のパスの両方向においてメディアに必要な帯域幅を確保するよう設計されたことによります。

Enhanced Location CAC は、AF41 クラス トラフィックと CS4 クラス トラフィックの両方の双方向メディアに対応します。ただし、非対称にマークされたフローでは、AF41 クラスの十分に割り当てられたビット レートは一方向で使用されますが、他方向で使用されません。一方の方向では、完全な割り当て済みビット レートは CS4 にマーキングされます。これは、追加の帯域幅消費というわけではなく、単に各 QoS クラスのネットワークでのマーキングおよびキューイングの相違です。この方式の帯域幅アカウンティングでは、各方向の各フローを保護する必要があります。

TelePresence ビデオ（CS4）が Unified Communications ビデオ（AF41）とは別個にネットワーク パス上でプロビジョニングされ、TelePresence の大部分がスケジューリングされており、コールのスケジューリングが制御されて TelePresence の使用率が決定論的である環境の場合、ロケーションとリンクのイマーシブ ビデオ帯域幅を [無制限（unlimited）] に設定して、二重帯域幅 CAC が計算されるのを回避できます。これにより、TelePresence 間のコールが常にスムーズに行き来し、アドミッション制御の影響を受けないようにしつつ、デスクトップ ビデオ、および TelePresence とデスクトップ間のビデオ コールがアドミッション制御の影響を受けず、ビデオ帯域幅割り当てで対処されるようになります。

Enhanced Location CAC と TelePresence の相互運用可能なコールのコール フローの詳細については、Telepresence イマーシブ ビデオの Enhanced Location CAC（13-64 ページ）を参照してください。

Enhanced Location CAC を使用する Unified CM Session Management Edition の配置に関する設計上の推奨事項

Unified CM Session Management Edition（SME）は通常、複数の Unified CM クラスタ、サードパーティ製 UC システム（IP および TDM ベースの PBX）、PSTN 接続、および集中型 UC アプリケーションを相互接続するために使用され、また、ダイヤル プランおよびトランク集約にも使用されます。次に、Enhanced Location CAC で Unified CM SME を配置する場合に従うべき推奨事項と設計上の考慮事項のリストを示します。Unified CM SME の詳細については、コラボレーションの配置モデル（10-1 ページ）の章を参照してください。

推奨事項と設計上の考慮事項

- Enhanced Location CAC をサポートするすべてのリーフ クラスタは、クラスタ間 Enhanced Location CAC を SME でイネーブルにしている必要があります。
- SME は、Enhanced Location CAC のクラスタ間ハブ レプリケーション ネットワークにおける中央のブートストラップ ハブとして使用できます。詳細については、LBM のハブのレプリケーション ネットワーク（13-56 ページ）を参照してください。
- Enhanced Location CAC をサポートするリーフ クラスタへのすべてのトランクは、シャドウ ロケーションに配置された SIP トランクである必要があります。これは、Enhanced Location CAC をサポートするリーフ クラスタと SME 間のトランクで Enhanced Location CAC をイネーブルにするためです。
- TelePresence ビデオの相互運用性については、ビデオの展開に関するコール アドミッション制御の設計上の推奨事項（13-85 ページ）を参照してください。
- Enhanced Location CAC をサポートする Unified CM 以外のトランクまたはデバイス（例：サードパーティ製の PBX、ゲートウェイ、従来のロケーション CAC のみをサポートする Unified CM クラスタ、カンファレンス ブリッジへのボイス メッセージ ポートまたはトランク、Cisco Video Communications Server など）への SME からの接続は、ファントム ロケーションまたはシャドウ ロケーション以外のロケーションで設定される必要があります。この理由はファントム ロケーションとシャドウ ロケーションの両方が非終端のロケーションであることです。つまり、ロケーションに関する情報を中継し、他のクラスタのユーザ定義のロケーションの効果的なプレースホルダとなります。ファントム ロケーションは、従来のロケーション CAC のみをサポートする Unified CM のバージョンでロケーション情報の伝送を可能にするレガシー ロケーションですが、Unified CM Enhanced Location CAC ではサポートされません。シャドウ ロケーションは、Enhanced Location CAC をサポートする Unified CM クラスタ間トランクでエンドツーエンドを実現する特別なロケーションです。

- SME は、ロケーションおよびリンクの管理クラスタとして使用できます。この例として、図 13-58 を参照してください。
- SME はローカルに設定された最大 2,000 のロケーションをサポートできます。

図 13-58　ロケーションおよびリンクの管理クラスタとしての Unified CM SME

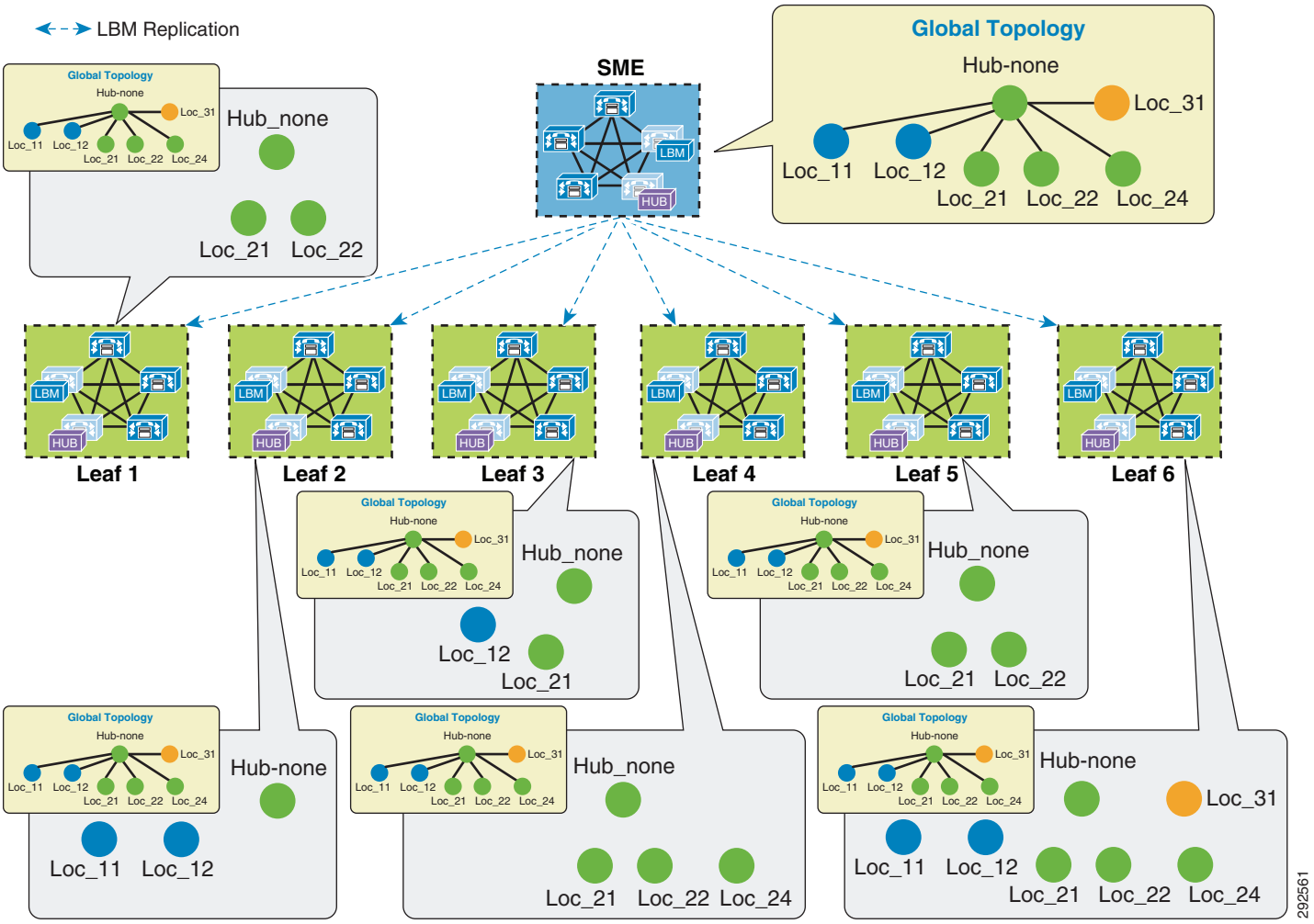
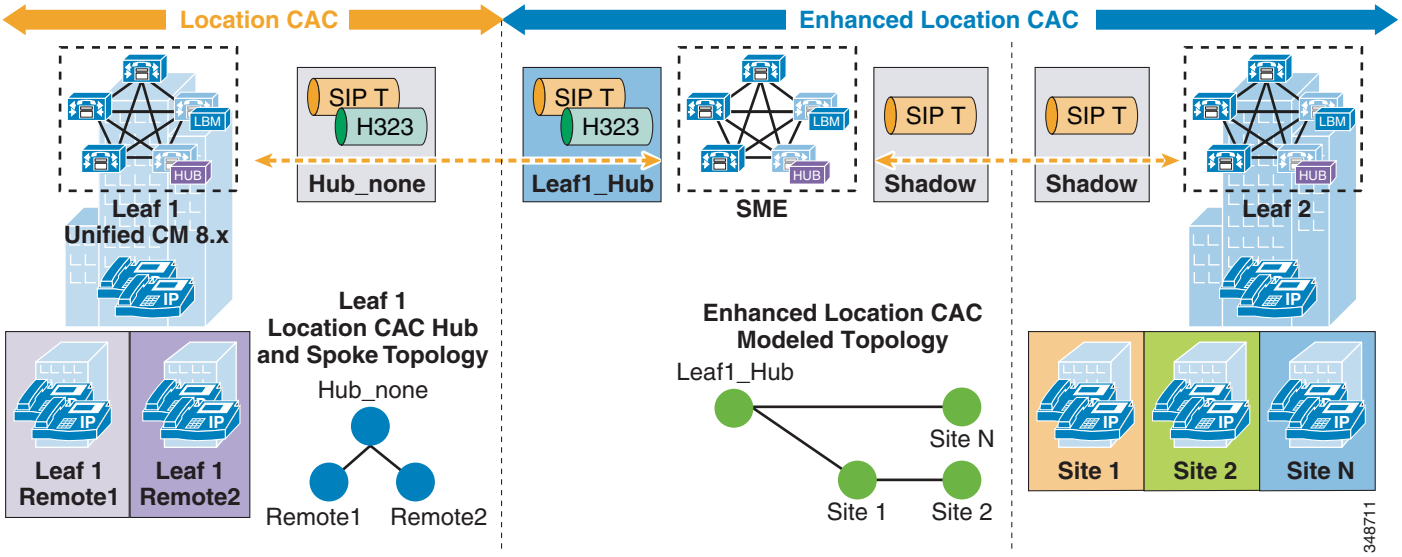


図 13-58 は、ロケーションおよびリンクの管理クラスタとしての SME について説明しています。ロケーションおよびリンクのグローバル トポロジ全体は SME で設定および管理され、リーフ クラスタは、エンド デバイスに関連付ける必要があるロケーションだけをローカルに設定します。クラスタ間 Enhanced Location CAC がイネーブルで、ロケーションおよびリンクが複製される場合、各リーフ クラスタは SME からグローバル トポロジを受信します。これを自らの設定済みのトポロジの上にオーバーレイし、コール アドミッション制御にグローバル トポロジを使用します。これは、複数のクラスタ間での設定およびロケーション/リンク管理を簡素化し、クラスタ間の設定ミスの可能性を少なくします。設計および展開の詳細については、ロケーションおよびリンク管理クラスタ（13-62 ページ）の項を参照してください。

図 13-59 は、クラスタ間 Enhanced Location CAC が 1 つ以上のリーフ クラスタでイネーブルにされている場合（右）、および 1 つ以上のリーフ クラスタが従来のロケーション CAC のみをサポートする Unified CM のバージョンを実行している場合（左）の SME デザインについて示しています。この種類の展開では、従来型のロケーション CAC で管理されるロケーションを、Enhanced Location CAC で有効なクラスタ間での共通または共有のロケーションとすることはできません。リーフ 1 は、従来型のハブ アンド スポークに設定され、デバイスがさまざまなリモート サイトで管理されています。クラスタ間 Enhanced Location CAC をイネーブルにしている SME および他のリーフ クラスタは、E-L CAC モデル化トポロジで示されるように、グローバル トポロジを共有します。Leaf1_Hub は、リーフ 1 トポロジのハブを表しており、SIP または H.323 クラスタ間トランクに割り当てられた SME のユーザ定義のロケーションです。これにより、リーフ 1 と Leaf1_Hub との間のコールの帯域幅を SME が差し引きできるようになります。このように、リーフ 1 は従来型のロケーション CAC でリモート ロケーションを管理し、一方で SME とリーフ 2 は Enhanced Location CAC のロケーションとリンクを管理します。

図 13-59　Enhanced Location CAC およびリーフ クラスタの従来のロケーション CAC を使用する SME の設計



Enhanced Location CAC を使用する Cisco Expressway の配置に関する設計上の推奨事項

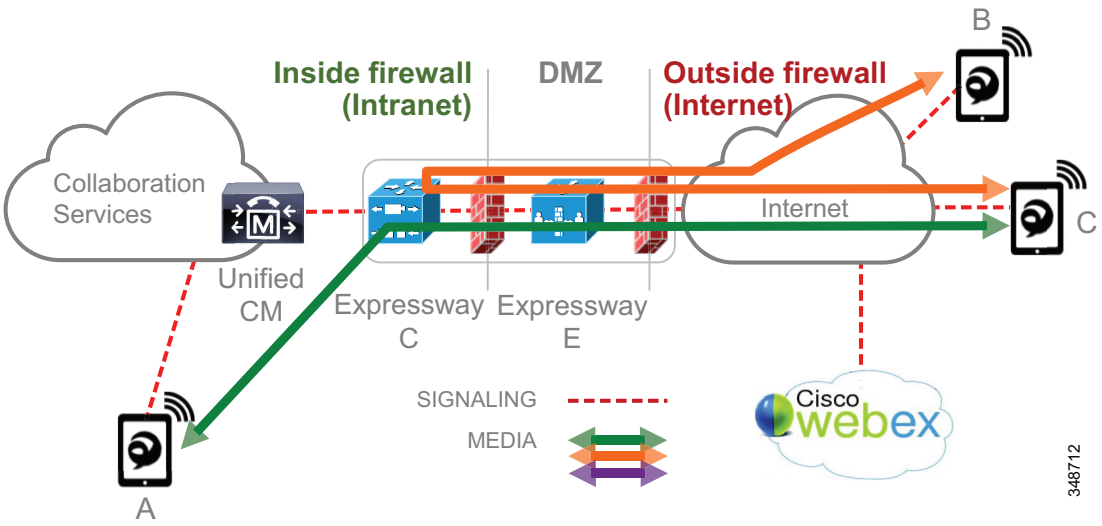
Cisco Expressway のモバイルとリモート アクセス機能は、VPN を使用しない Unified CM へのインターネット ベースのデバイスの登録を提供します。別名、VPN-less エンタープライズ アクセスとして知られています。これにより、企業ネットワークにアクセスできるようにオペレーティング システム全体がアプリケーションをホストする必要なく、エンドポイントまたはクライアント アプリケーションが Unified CM に安全に登録されるようになります。ここでは、Enhanced Location Call Admission Control（ELCAC）を使用してモバイルおよびリモート アクセスを配置する推奨事項と設計上の考慮事項を示します。モバイルとリモート アクセスの詳細については、VPN-less 企業アクセス（10-38 ページ）の項を参照してください。

推奨事項と設計上の考慮事項

Cisco Expressway の VPN-less モバイルとリモート アクセス ソリューションでは、この機能をサポートするエンドポイントは、VPN を使用せずに Cisco Expressway 配置を介して Unified CM に登録できます。Cisco Expressway C および Expressway E サーバは、それぞれがハイ アベイラビリティの冗長性を備えて配置されます。Expressway E はファイアウォールからインターネット（外側）とファイアウォールから企業（内側）間の DMZ に配置されますが、Expressway C は企業内に配置されます。図 13-60 に、この配置を示します。また、次のメディア フローを示しています。

1. お互いをコールするインターネットベースのエンドポイントでは、図 13-60 のエンドポイント B と C の間に示されるように、メディアは Expressway E と Expressway C を経由してルーティングされ、インターネットに戻されます。
2. 内部エンドポイントをコールするインターネットベースのエンドポイントでは、図 13-60 のエンドポイント A と C の間に示されるように、メディアは Expressway E と Expressway C を流れます。

図 13-60　VPN-less アクセス用の Cisco Expressway の配置



同じ企業内で VPN-less アクセス用の Cisco Expressway を複数配置する場合、1 つの Expressway ペアを介して登録されるインターネットベースのエンドポイントが別の Expressway ペアを介して登録されるインターネットベースのエンドポイントをコールすることで、メディアが企業を経由してルーティングされます。これは、図 13-61 のエンドポイント D とエンドポイント C 間のコールに示されます。両方がインターネットから登録されますが、2 つの異なる Expressway ペアを経由します。メディア フローは、エンドポイントが同じ Unified CM クラスタまたは異なる Unified CM クラスタに登録されているかどうかに関係なく同じになります。

図 13-61　複数の Cisco Expressway ペアの配置でのメディア フロー

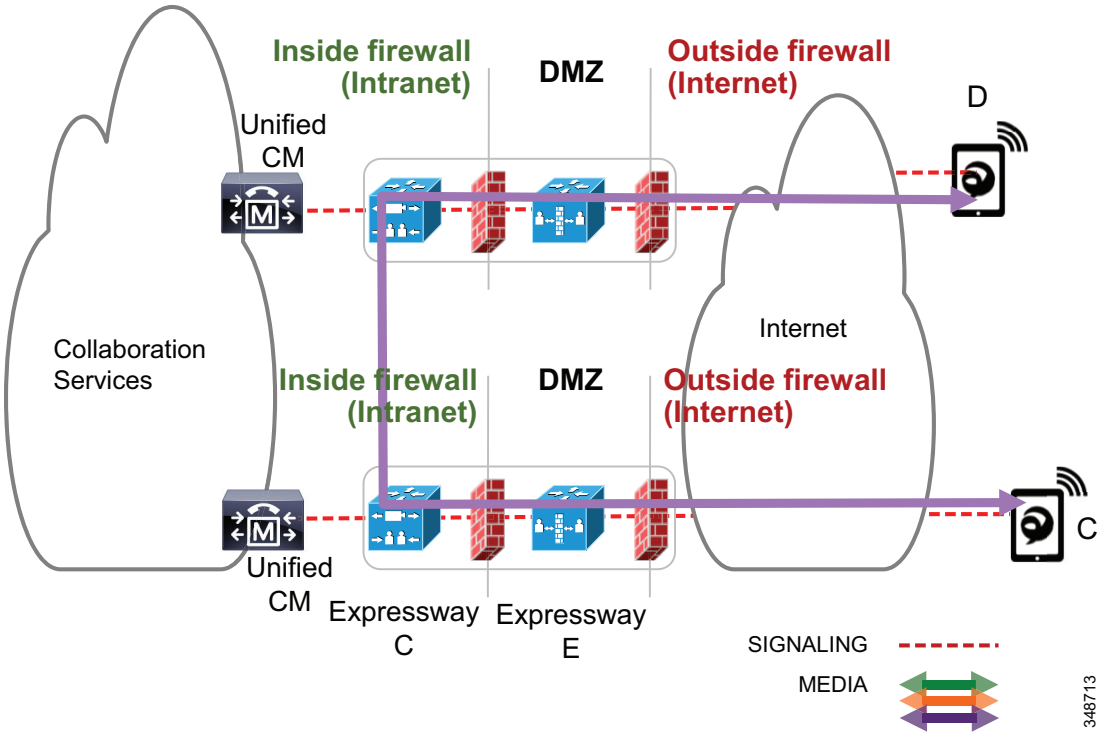


図 13-62 は、企業を通過するメディア フローの帯域幅のトラッキングを統合しながら、アドミッション制御なしでメディアがインターネット上を流れることを拒否しないロケーションとリンクの設定例を示します。

図 13-62　リモートとモバイル アクセスのロケーションとリンク

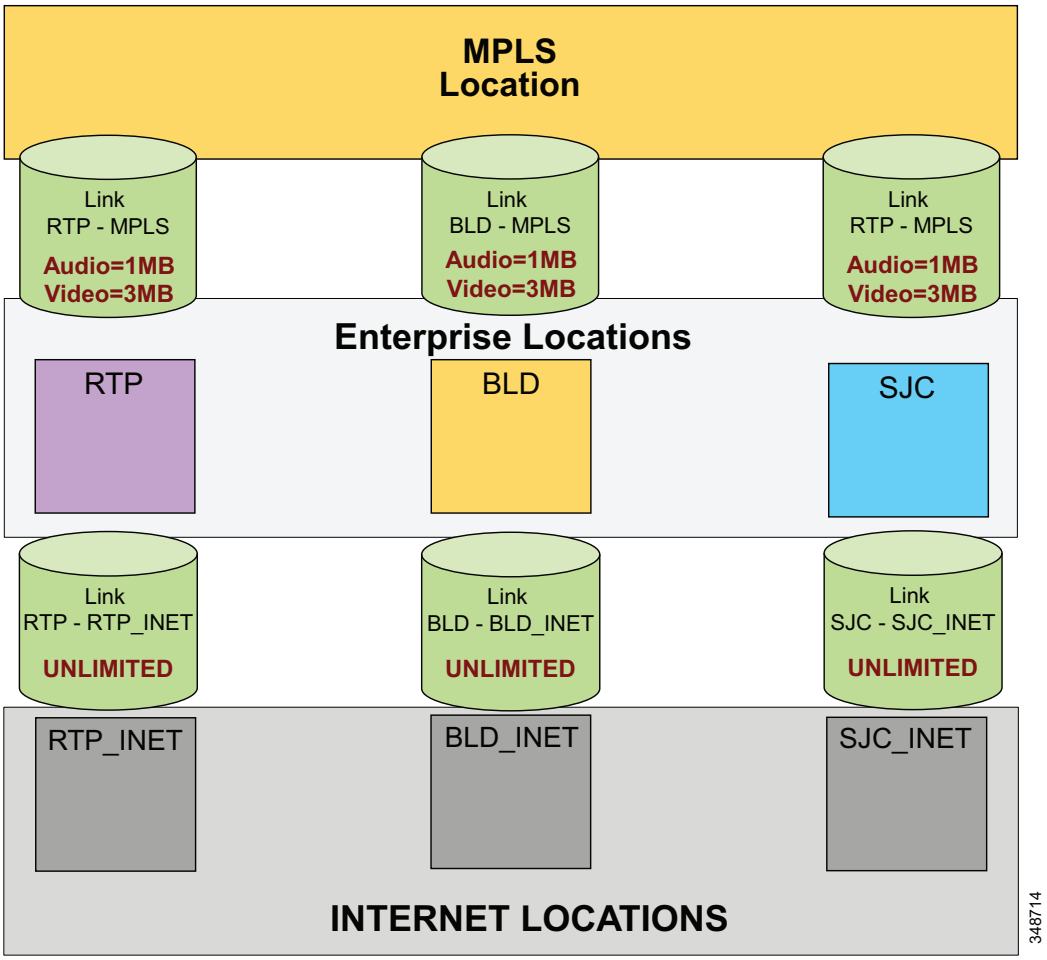


図 13-62 に、3 つの主要なサイト（RTP、BLD、および SJC）で構成される ELCAC の展開例を示します。これらのサイトはすべて MPLS プロバイダーに接続されるため、それぞれに MPLS クラウドへの別個の WAN 接続があります。帯域幅リンクがネットワーク トポロジにマッピングする音声コールおよびビデオ コールに限定された状態で、企業ロケーションが MPLS と呼ばれるロケーションに直接リンクされるように、適宜ロケーションとリンクが作成されます。企業内にあるとき、デバイスは 3 つのサイトの 1 つに置かれるため、関連付けられたロケーションを持ちます。これらの各サイトには、Unified CM に登録されるインターネットベースのエンドポイントの VPN-less リモートおよびモバイル アクセス用の Cisco Expressway ソリューションがあります。新しい 3 つのロケーションは、RTP_INET、BLD_INET、および SJC_INET の名前で各 Expressway ソリューション サイトに対して 1 つずつ、インターネットベースのデバイスに設定されます。これらの 3 つのロケーションは、Expressway ペアを介してインターネットから Unified CM に登録されるデバイスのロケーションであることから、「インターネット ロケーション」と表現されます。これらのロケーションは、直接のリンクで相互接続されません。これは、Expressway 間のコールが企業を経由してルーティングされ、MPLS クラウドを介して流されるからです。その代わりに、このようなインターネット ロケーションには、関連付けられた企業ロケーションへのリンクがあります。たとえば、RTP_INET には RTP へのリンク、BLD_INET には BLD へのリンクなどがあります。インターネット ロケーションと企業ロケーション間のこれらのリンクは、[無制限（unlimited）] の帯域幅に設定されている必要があります。

前述のように、Cisco Expressway 配置の Enhanced Location CAC には、デバイス モビリティと呼ばれる Unified CM の機能を使用する必要があります（この機能の詳細については、デバイス モビリティ（21-15 ページ）の項を参照してください）。エンドポイントでデバイス モビリティを有効にすると、Unified CM は、デバイスが Cisco Expressway を介して登録されたときや企業内で登録されたときを認識できるようになります。またデバイス モビリティを使用すると、企業とインターネット間をローミングするときに、Unified CM がアドミッション制御をデバイスに提供できるようになります。デバイス モビリティは、エンドポイントが Expressway C の IP アドレスを使用して Unified CM に登録されるときを認識することによりこれを実行し、Unified CM が適切なインターネット ロケーションを関連付けます。ただし、エンドポイントが他の IP アドレスで登録されている場合、Unified CM は、デバイスに直接設定されている（またはデバイスに直接設定されたデバイス プールから）企業ロケーションを使用します。この機能が作用するために企業全体にわたってデバイス モビリティを配置する必要がないことに注意してください。Unified CM のデバイス モビリティ設定は Expressway の IP アドレスでのみ必要となり、この機能を必要とするデバイス（つまり、インターネット経由で登録するデバイス）上だけでこの機能が有効にされます。図 13-63 は、デバイスのモビリティ設定の概要を示します。これは ELCAC がインターネットベースのデバイスで機能するためのデバイス モビリティの最小設定要件ですが、企業内の同一のエンドポイントのモビリティをサポートするために、デバイス モビリティを設定することができます（詳細については、デバイス モビリティ（21-15 ページ）の項を参照してください）。

図 13-63　デバイスのモビリティ設定とロケーションの関連付け

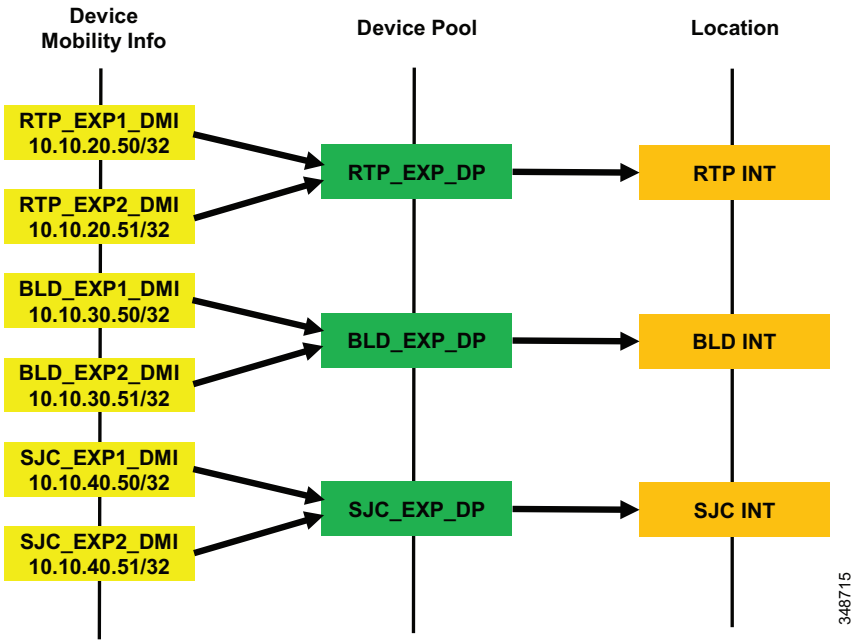
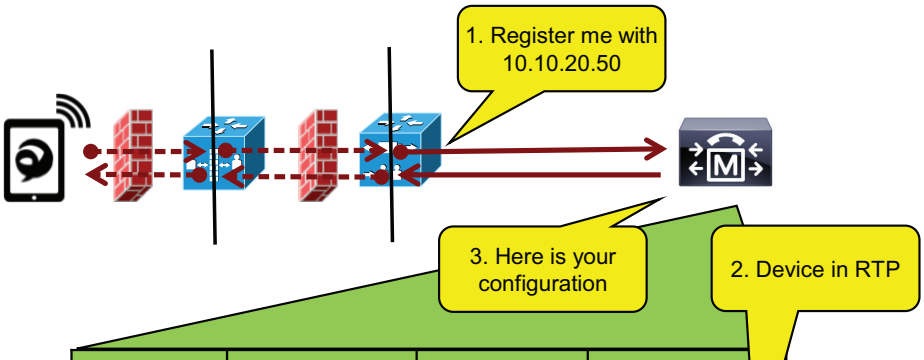


図 13-63 は、図 13-62 で説明された ELCAC の展開例に対するデバイス モビリティの簡易バージョンを示します。Expressway C サーバの IP アドレスは、デバイスのモビリティ情報に設定されています。この例では、3 つのサイト（RTP、BLD、および SJC）のそれぞれに Expressway C サーバの冗長ペアがあります。RTP_EXP1_DMI および RTP_EXP2_DMI は、RTP Expressway C サーバのサーバ IP アドレスでそれぞれ設定されています。これらの 2 つは、ロケーション RTP_INET が設定されている RTP_EXP_DP と呼ばれる新しいデバイス プールに関連付けられます。各サイトが同様に設定されます。この設定では、任意のデバイスが RTP_EXP1_DMI または RTP_EXP2_DMI のデバイス モビリティ情報に対応する IP アドレスで Unified CM に登録されるデバイス モビリティで有効にされている場合、RTP_EXP_DP デバイス プール、そして RTP_INET ロケーションに関連付けられます。

上記の設定では、インターネット ベースのデバイスが Expressway を介して Unified CM に登録される場合、Expressway C の IP アドレスを使用して登録されます。次に、Unified CM は、デバイス モビリティ情報に設定された IP アドレスを使用して、デバイス プールとこのデバイス プールに関連するインターネット ロケーションを関連付けます。図 13-64 に、このプロセスを示します。

図 13-64　Expressway IP アドレスに基づいたデバイス プールとロケーションの関連付け



IP Subnet	Device Mobility Info	Device Pool	Location
10.10.20.50	RTP_EXP1_DMI	RTP_EXP_DP	RTP_INET
10.10.30.50	BLD_EXP1_DMI	BLD_EXP_DP	BLD_INET
10.10.40.50	SJC_EXP1_DMI	SJC_EXP_DP	SJC_INET

348716

図 13-64 では、クライアントは RTP の Expressway を介して Unified CM に登録します。シグナリングが RTP の Expressway C で変換されるため、デバイスは Expressway C の IP アドレスを使用して登録されます。デバイ スプール RTP_EXP_DP は、この IP アドレスに基づいてデバイスに関連付けられます。RTP_EXP_DP プールは RTP_INET ロケーションで設定されているため、そのロケーションがデバイスに関連付けられます。そのため、デバイスが Expressway に登録されると、デバイス モビリティを介して正しいロケーションの関連付けを取得します。エンドポイントが企業に移動する場合、静的ロケーションの設定に戻ります。また、たとえばエンドポイントが SJC の別の Expressway に移動する場合、デバイス モビリティを介して正しいロケーションの関連付けを取得します。

Enhanced Location CAC による Cisco Expressway VPN-less アクセスの設定と設計に関するベスト プラクティス

- Cisco Expressway ソリューションが常駐するインターネット アクセスがある各サイトには、インターネット ロケーションと企業ロケーションが必要です。各 Cisco Expressway の配置には、これらのロケーション ペアが必要です。企業ロケーションは、デバイスが企業内に存在するときにデバイスに関連付けられます（図 13-62 の RTP、BLD、および SJC のロケーションを参照）。エンドポイントがインターネットから登録されている場合、インターネット ロケーションはデバイス モビリティ機能を介してエンドポイントに関連づけられます（図 13-62 の RTP_INET、BLD_INET、および SJC_INET のロケーションを参照）。たとえば、図 13-62 では、RTP および RTP_INET は、物理サイト RTP のロケーションのペアを形成します。
- 企業ロケーションは、該当する企業 ELCAC の設計に従って設定されます。
- インターネット ロケーションには、ペアリングされた企業ロケーションへのリンクが常に 1 つあります。たとえば、図 13-62 では、RTP および RTP_INET は、企業ロケーションとインターネット ロケーションのペアを形成します。
- インターネット ロケーションから企業ロケーションへのリンクは、[無制限（unlimited）] 帯域幅に設定されます。これらのロケーション ペア間の無制限の帯域幅によって、帯域幅がインターネット ロケーションからのローカルの企業ロケーションへのコール、またその逆の場合のコールに対してカウントされないようになります（たとえば、図 13-62 の RTP から RTP_INET へのコール）。
- 複数の Cisco Expressway のサイトが展開され、複数のインターネット ロケーションを必要とする Cisco Expressway ソリューションでは、必ずインターネット ロケーションが互いの直接リンクが持たないようにします。インターネット ロケーション間の直接リンクは、ELCAC で複数のパスを作成するため、推奨されません。
- Cisco Expressway で DSCP を設定する場合は、エンドポイント マーキング ポリシーと整合性があることを確認します。Cisco Expressway リリース 8.9 以降、DSCP はシグナリング、オーディオ、ビデオ、XMPP に対して個別に設定できます。このため、シグナリングに CS3（24）、オーディオに EF（46）、ビデオに AF41（32）、XMPP に CS3（24）を設定することが可能で、Expressway-C はインターネットから企業に入ってくるメディアおよびシグナリング トラフィックに適切なマーキングを行います。8.9 より前のリリースから Expressway サーバをアップグレードする場合、以前のリリースで使用された単一の設定済み DSCP 値が新しい Expressway リリースの 4 つのすべての値に設定されます。

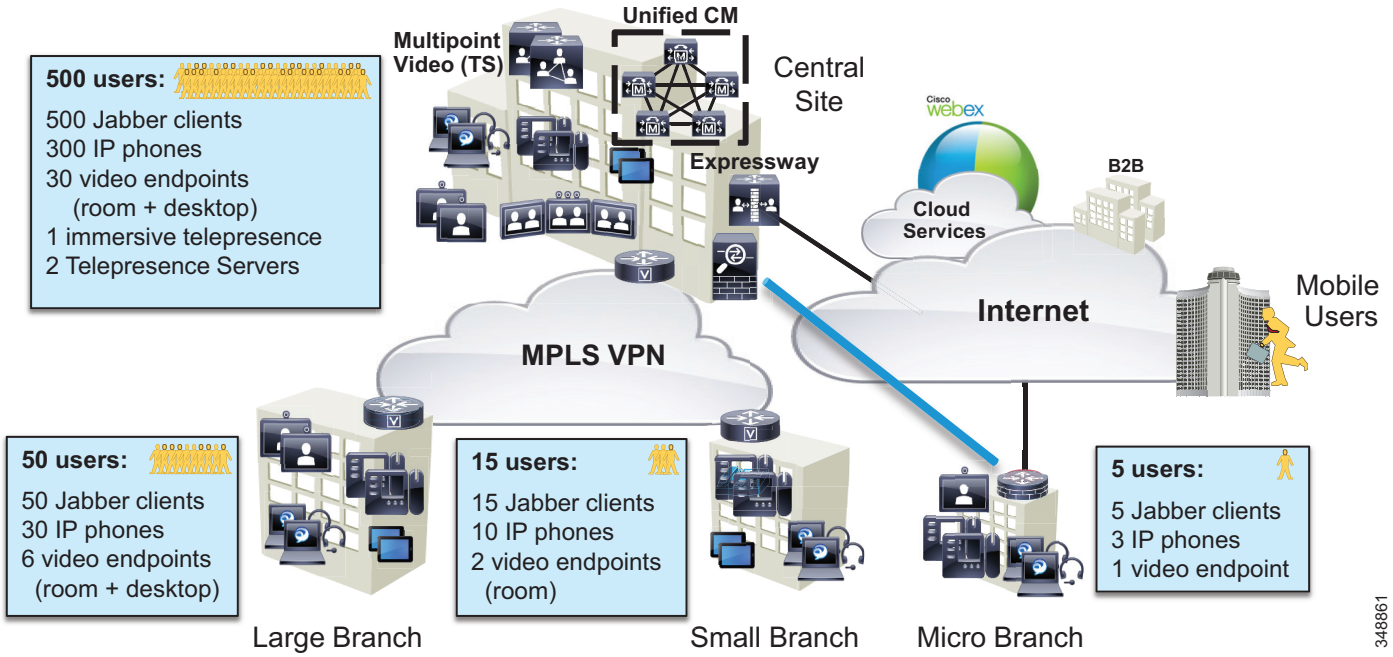
帯域幅管理の設計例

ここでは設計例を示し、本章で説明したすべての側面について取り上げます。識別と分類、WAN キューイングとスケジューリング、プロビジョニングとリソース管理、帯域幅割り当てのガイドラインについて、各項目の例で詳細に説明します。

企業例 #1

企業例 #1 は、広範囲の地域にユーザを持ち、本社にはデータ センター（DC）が設置され、あらゆる規模（約 500 人、50 人、15 人）の支社が複数あり、各支店にはそれぞれ 5 人のユーザがいる大企業です。ネットワーク図を簡略化するため、これらのサイトのカテゴリ（HQ、大、小、事務所）をテンプレートとして使用し、同様のユーザとエンドポイントの密度を持つ各サイトに応じた帯域幅の考慮事項を決定します。図 13-65 では、各サイト タイプについて説明します。この企業は、ビデオのために Jabber を導入し、ユーザが会議でビデオ端末にアクセスできるようにしています。TelePresence ビデオ会議リソースは HQ の DC に配置されています。IP Phone は音声専用通信用です。ビデオ エンドポイントには、Jabber クライアント、コラボレーション デスクトップ エンドポイント（DX シリーズ）、およびルーム エンドポイント（MX、プロファイル、および SX シリーズ）を使用しています。大規模なサイトには、IX シリーズなどのイマーシブ TelePresence ユニットが用意されています。

図 13-65　企業例 #1



IT 部門は、企業例 #1 の各サイト タイプに応じた WAN エッジの帯域幅要件の決定を任されています。次に要件を一覧で表示し、QoS の適用方法と、帯域幅、キューイング、アドミッション制御の要件の決定方法について説明します。

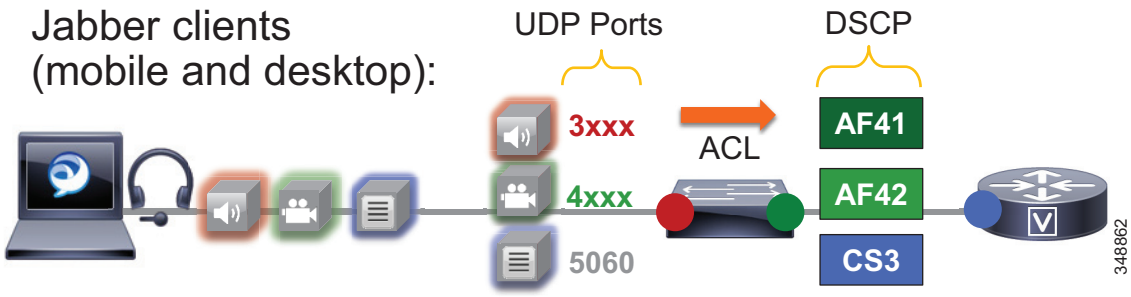
識別と分類

ここでは、企業全体の QoS 要件を確立します。

信頼されていないエンドポイント（Jabber）

Jabber エンドポイントは信頼されておらず、データ VLAN 内に配置されています。アクセス レイヤ スイッチでシグナリングおよびメディアを再マーキングするには、特定の UDP ポート範囲が使用されます。この場合、Unified CM の設定には、共通メディアおよび 3000 ～ 4999 のシグナリング ポート範囲を使用するすべての Jabber クライアント専用の SIP プロファイルを使用します。これにより、すべての Jabber エンドポイントが、3000 ～ 3999 の ソース UDP ポートをオーディオ ストリームとして、4000 ～ 4999 をビデオ ストリームとして使用するように設定されます。5060 のデフォルト SIP ポートは SIP シグナリング（SIP セキュリティ プロファイルで設定）に使用されます。図 13-66 でこれについて説明します。

図 13-66　信頼されていない（Jabber）エンドポイント QoS



管理者は、次の DSCP 値に UDP ポートを再マーキングするデータ VLAN にアクセス スイッチの ACL を作成します。

- オーディオ：AF41 にマーキングされる UDP ポート 3000 ～ 3999
- ビデオ：AF42 にマーキングされる UDP ポート 4000 ～ 4999
- シグナリング：CS3 にマーキングされる TCP ポート 5060

Jabber の分類概要：

- すべての Jabber コールのオーディオ ストリーム（音声専用とビデオ コール）は AF41 にマーキングされています。
- Jabber ビデオ コールのビデオ ストリームは AF42 にマーキングされています。

Jabber エンドポイントの場合、Jabber SIP プロファイルでデフォルトの QoS 値も変更することをお勧めします。何らかの理由で、Jabber クライアントの QoS がワイヤレス ルータまたは他の有線ルータ経由で信頼されている場合は、信頼されている QoS と ACL で 再マーキングされた QoS との間で信頼された値の一貫性が適切に確保されます。そのため、Jabber クライアント用の SIP プロファイルの QoS パラメータは、表 13-15 に示すように設定する必要があります。

表 13-15　Jabber クライアント用の SIP プロファイルの QoS パラメータ

QoS サービス パラメータ名（SIP プロファイル）	システム デフォルト値	変更値
音声コールの DSCP（DSCP for Audio Calls）	EF	AF41
ビデオ コールの DSCP（DSCP for Audio Calls）	AF41	AF42
ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）	AF41	
TelePresence コールの DSCP（DSCP for TelePresence Calls）	CS4	該当なし
TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）	CS4	該当なし

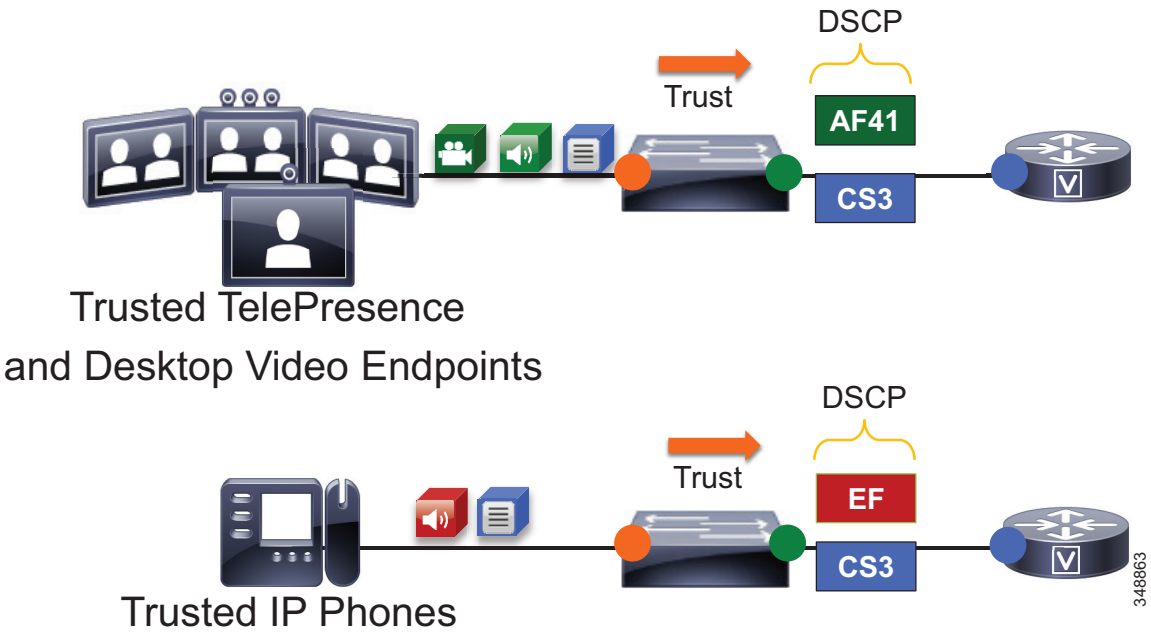
表 13-15 の構成時の設定は、何らかの理由で、トラフィックが信頼されているネットワーク パスを流れているのに、信頼されていないネットワーク パス内の UDP ポート範囲を介して再マーキングされない場合、Jabber クライアントのビデオが AF42 に設定されるようにします。ビデオ コールのオーディオ部分の DSCP は、AF41 のデフォルト設定のままです。これは単に、UDP ポート範囲を使用するネットワーク経由で信頼されているまたは再マーキングされているか、Jabber エンドポイント間で一貫して設定するようにするためです。

信頼されているエンドポイント

信頼されているエンドポイントの場合、Cisco Discovery Protocol（CDP）が使用され、IP Phone およびビデオ エンドポイントの QoS は、アクセス スイッチで設定された条件付き信頼メカニズムを使用して信頼されます。この設定では、Unified CM デフォルト システム設定として、音声専用コールのオーディオに EF、ビデオ コールのオーディオとビデオに AF41、TelePresence のオーディオとビデオに CS4、シグナリングに CS3 を使用します。そのため、TelePresence エンドポイントの QoS がその設定に従って調整されるようにするには、管理者が、SIP プロファイルで信頼されているエンドポイントについて、Unified CM の QoS デフォルト設定を変更する必要があります。

図 13-67 では、アクセス スイッチの条件付き信頼（CDP ベース）およびパケット マーキングを示します。

図 13-67　信頼されているエンドポイント QoS



管理者は、次に分類されるように、IP Phone およびビデオと TelePresence エンドポイントの条件付き QoS 信頼ですべてのアクセス スイッチを設定します。

- ビデオ コールのオーディオおよびビデオ ストリームは AF41 にマーキングされます。
- 音声専用コールは EF にマーキングされます。

また、管理者は、表 13-16 の値を使用する SIP プロファイルで信頼されているエンドポイントに対して、Unified CM の QoS デフォルト設定を変更する必要もあります。

表 13-16　信頼されているエンドポイントの SIP プロファイルの QoS パラメータ

QoS サービス パラメータ名（SIP プロファイル）	システム デフォルト値	変更値
音声コールの DSCP（DSCP for Audio Calls）	EF	
ビデオ コールの DSCP（DSCP for Audio Calls）	AF41	
ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）	AF41	
TelePresence コールの DSCP（DSCP for TelePresence Calls）	CS4	AF41
TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）	CS4	AF41

WAN エッジの入力に到着する特定の DSCP 値を持つパケットは、アクセス レイヤで信頼されているか、またはアクセス スイッチで信頼されていない場合は適宜再マーキングされていることが予想されます。入力のフェールセーフ プラクティスとして、アクセス レイヤで再マーキングできなかった信頼されていないトラフィックは、WAN エッジで再マーキングすることが重要です。QoS は LAN で重要ですが、WAN では最も重要です。ルータは入力トラフィックが信頼されていると見なすため、ビジネス要件およびユーザ エクスペリエンスに応じた適切な QoS ポリシーを設定することが重要です。WAN エッジの再マーキングは、ルータへの入力インターフェイスで常に実行されます。キューイングおよびスケジューリングは出力インターフェイスで実行されます。次に、WAN 入力 QoS ポリシーと出力キューイング ポリシーの例を示します。図 13-68 では、設定と再マーキングのプロセスを説明します。

図 13-68 では、ネットワークの信頼されている領域と信頼されていない領域の両方から送られるパケットは、前述の信頼方法または UDP ポート範囲に一致する簡単な ACL を経由し、適切な DSCP マーキングを使用して識別および分類されます。この ACL は、IP アドレスと、マーキング範囲を細かに制限する他のいくつかの属性にも細部にわたって一致する可能性があることに注意してください。

図 13-68　　ルータ入力 QoS ポリシー プロセス例：ステップ 1

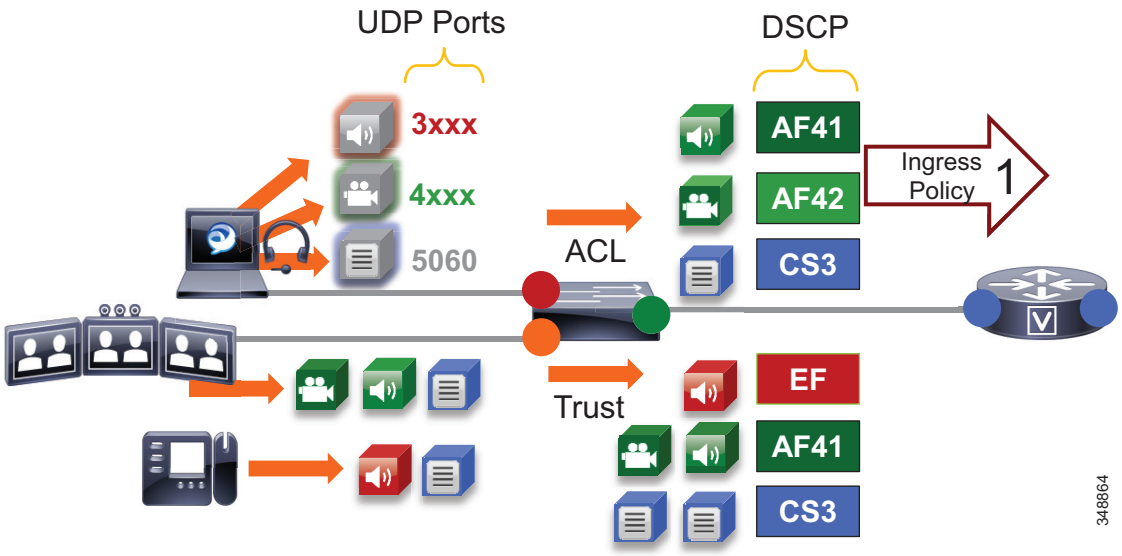
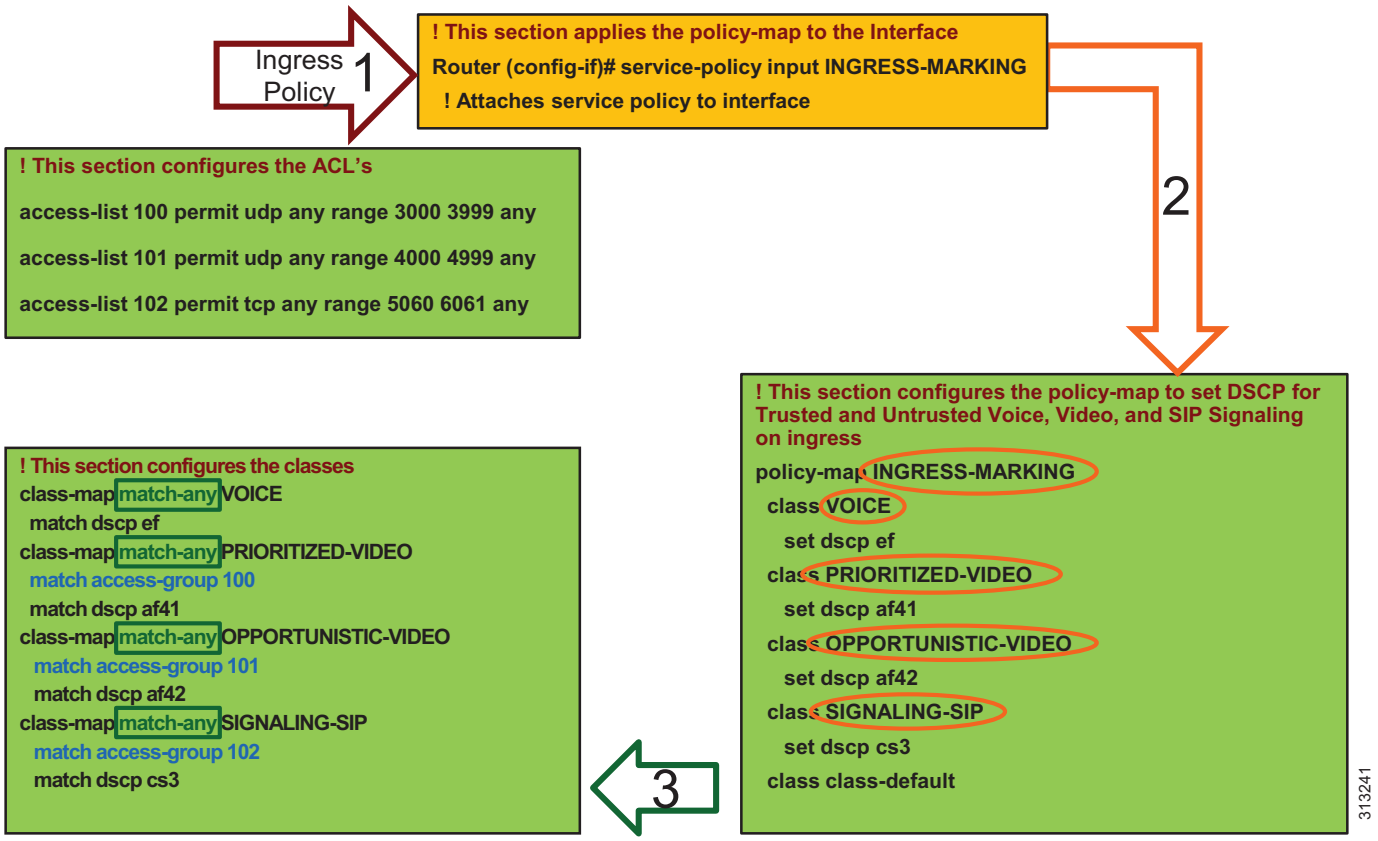


図 13-68 ～ 図 13-73 では、入力 QoS ポリシーの一致基準および DSCP 再マーキングについて説明します。このプロセスには、図に示された次のステップが含まれます。

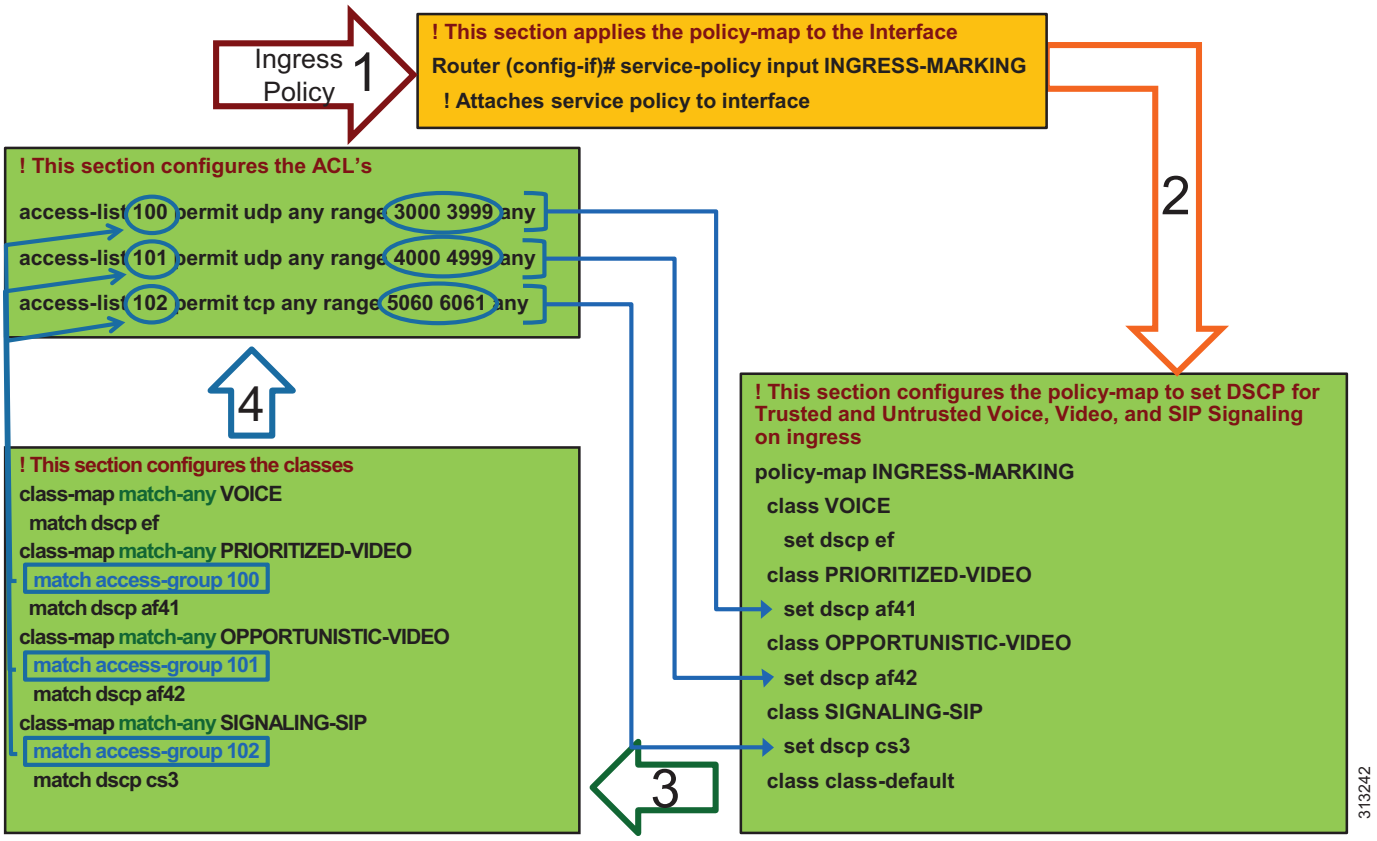
1. ステップ 1 で、パケットがルータ入力インターフェイスに到着し、入力サービス ポリシーで設定されます（図 13-69）。
2. ステップ 2 で、policy-map は 4 つのクラスのトラフィックで設定され、次の適切な DSCP を設定します。VOICE = EF、PRIORITIZED-VIDEO = AF41、OPPORTUNISTIC-VIDEO = AF42、SIGNALING-SIP = CS3（図 13-69）。
3. ステップ 3 で、これらの各クラスは match-any 基準で設定されている同じ名前の class-map に一致します（図 13-69）。この [いずれかに一致（match-any）] 基準の場合、プロセスはトップダウン方式で開始され、policy-map ステートメントの各クラスに従って最初に一致した基準が実行されます。

図 13-69　ルータ入力 QoS ポリシー プロセス例：ステップ 1～3



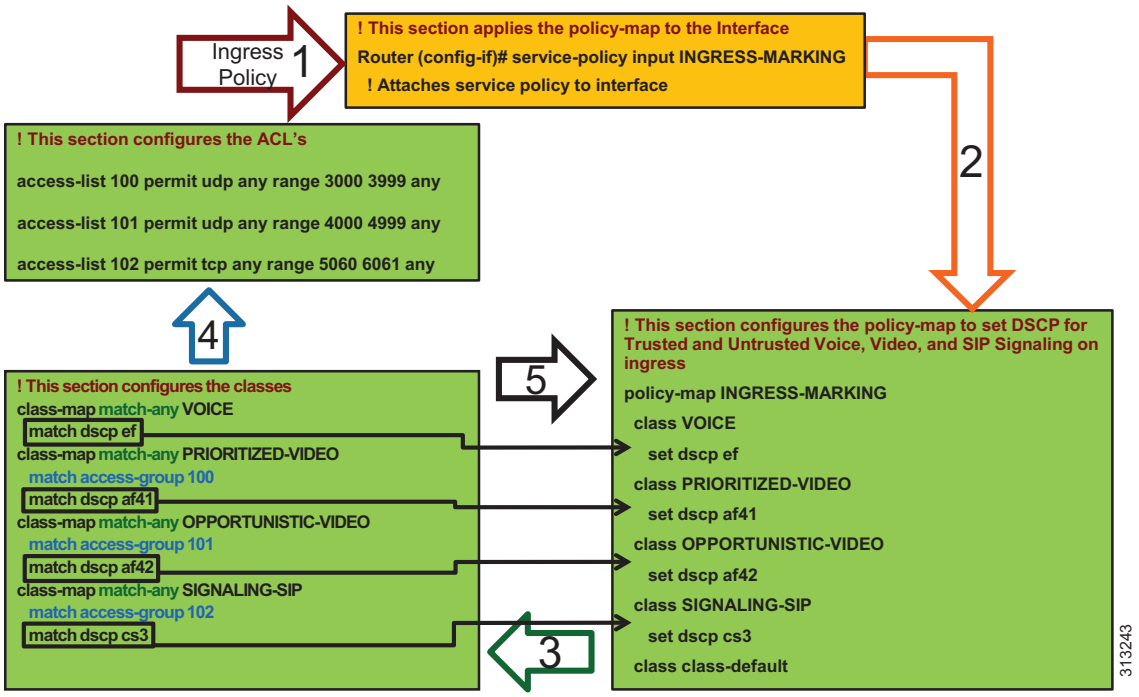
4. ステップ 4 で、class-map ステートメントの最初の行が解析されます。これは Unified CM の識別と分類セクションに設定されている UDP ポートに一致する ACL です。ACL 基準（プロトコルとポート範囲）が一致する場合は、対応する policy-map ステートメントで設定されているとおりにトラフィックがマーキングされます（図 13-70）。図 13-68 のポリシーに従って、Jabber Audio は AF41 とマーキングされ、Jabber Video は AF42 とマーキングされることに注意してください。

図 13-70　ルータ入力 QoS ポリシー プロセス例：ステップ 4



5. ステップ 5 で、最初のステートメントに一致しないトラフィックは class-map 内の次の match ステートメント、**match dscp** に移動します（図 13-71）。トラフィックが DSCP と単純に一致する場合、DSCP はすでに一致したものと同じ値に再び設定され、policy map ステートメントで設定されたかのようになります。この場合、ルータは単純に DSCP に一致し、DSCP を同じ値にリセットします。これはサーバおよびアプリケーションから WAN ルータに入ってくる信頼された DSCP の catch-all 設定です。

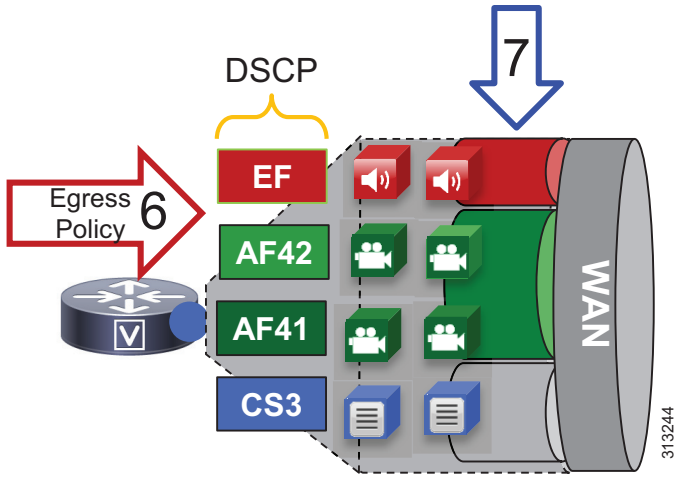
図 13-71　ルータ入力 QoS ポリシー プロセス例：ステップ 5



（注）　これは、モジュラ QoS CLI（MQC）に基づいた QoS 入力マーキング ポリシー例です。MQC をサポートするシスコ ルータで同様のポリシーを実現する方法と、更新されたコマンドについては、特定ルータ設定ガイドを参照してください。

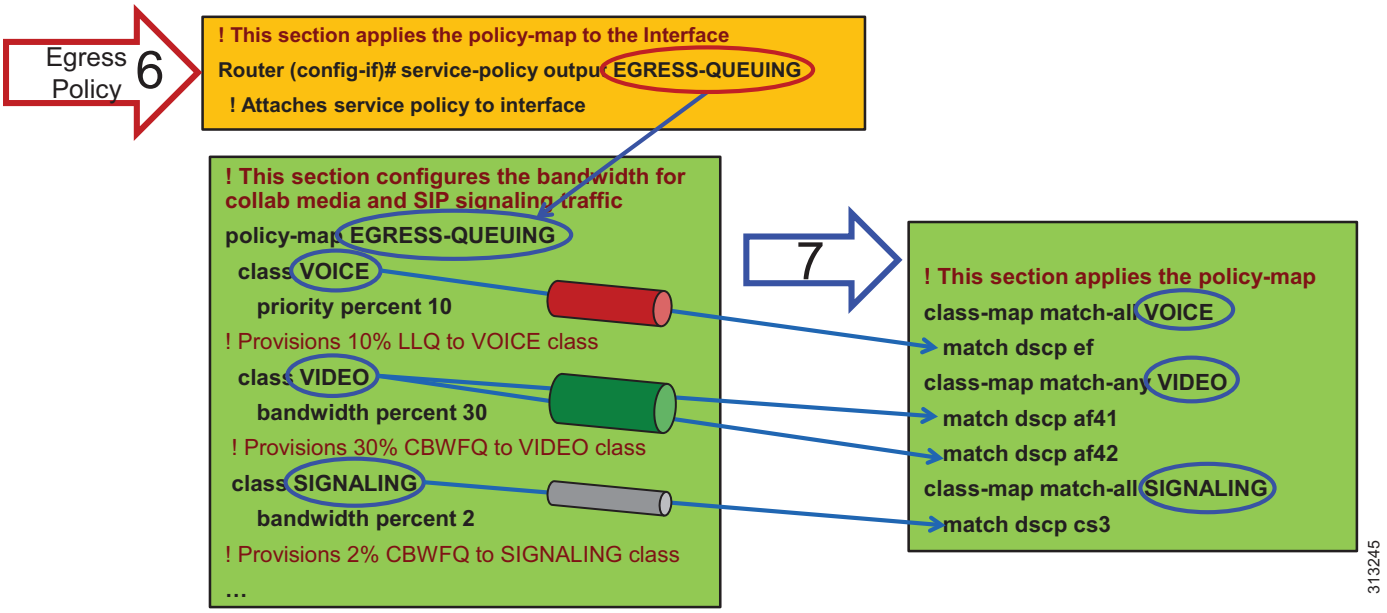
6. ステップ 6 で、トラフィックは 3 つのキュー（VOICE と呼ばれる Priority Queue、VIDEO と呼ばれる CBWFQ、SIGNALING と呼ばれる CBWFQ）が作成された出力サービス ポリシーによってキュー登録およびスケジューリングされた送信インターフェイスに移動します。これについて図 13-72 および図 13-73 に示します。これは、この出力キューイング ポリシーが、アクセス スイッチや WAN ルータ入力インターフェイスへの入力で発生するネットワーク マーキングとして DSCP のみに基づいている点を強調しています。これは、一致基準およびキューを説明するための単なる例であり、WRED 機能は含まれていません。WRED の詳細については、WAN キューイングとスケジューリング（13-107 ページ）の項を参照してください。

図 13-72　ルータ出力キューイング ポリシー プロセス例：ステップ 6



7. ステップ 7 で、トラフィックが class-map 一致ステートメントと一致します（図 13-73）。EF とマーキングされたトラフィックはすべて VOICE PQ に送られ、AF41 と AF42 のトラフィックは VIDEO CBWFQ に、CS3 のトラフィックは SIGNALING CBWFQ に送られます。

図 13-73　ルータ出力キューイング ポリシー プロセス例：ステップ 7



（注）　これは、Cisco Common Classification Policy Language（C3PL）に基づいた出力キューイング ポリシー例です。C3PL をサポートするシスコ ルータで同様のポリシーを実現する方法と、更新されたコマンドについては、特定のルータの設定ガイドを参照してください。

WAN キューイングとスケジューリング

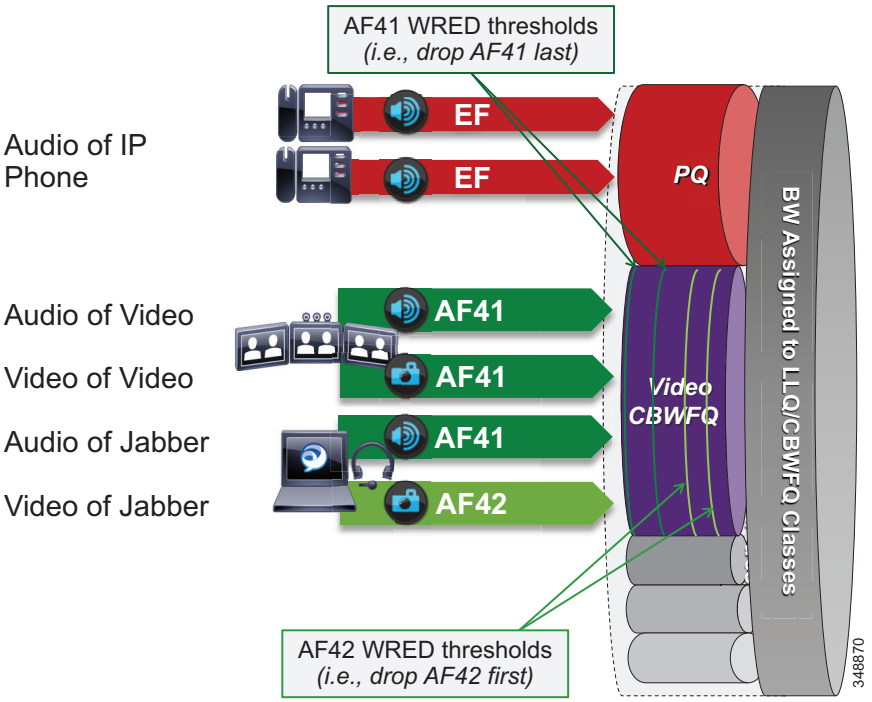
ここでは、インターフェイス キューイングについて説明します。図 13-74 では、CBWFQ で使用される音声 PQ、ビデオ CBWFQ、および WRED のしきい値について説明します。

- 信頼されているエンドポイント（EF）の音声専用コールは PQ にマッピングされます。
- 優先順位付けされたビデオ コールおよび Jabber は同じ CBWFQ を共有します。
  - 信頼されているエンドポイントからのビデオ コールのオーディオとビデオのストリームには AF41
  - Jabber クライアントからのすべてのコールのオーディオ ストリームには AF41
  - Jabber クライアントからビデオ コールのビデオ ストリームには AF42
- WRED はビデオ キューで設定されます。
  - AF42 の最小および最大のしきい値:

    キュー制限の約 10 % ～ 30 %
  - AF41 の最小および最大のしきい値:

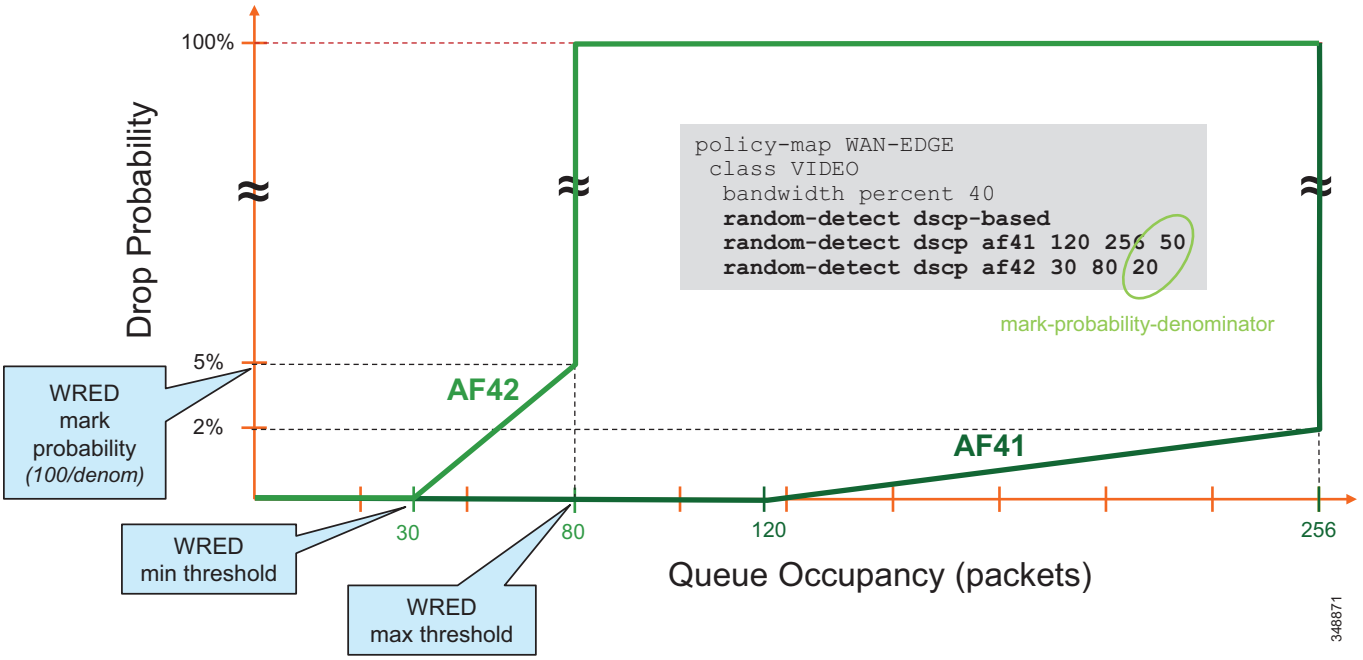
    キュー制限の約 45 % ～ 100 %

図 13-74　キューイングとスケジューリングのコラボレーション メディア



重み付けランダム早期検出（WRED）の最小および最大しきい値は、Video CBWFQ でも設定されます。WRED のしきい値の設定方法を説明するため、インターフェイスはキューの深さが 256 パケットで設定されていると仮定します。次に、上述のガイドラインに従って、AF42 および AF41 の WRED の最小しきい値および最大しきい値が、図 13-75 の説明とおりに設定します。

図 13-75　WRED のしきい値を持つビデオ CBWFQ の例



プロビジョニングとアドミッション制御

ここでは、各サイト タイプのキューに対してアドミッション制御およびプロビジョニング帯域幅を指定します。

前述のとおり、このような場合、アドミッション制御をビデオ帯域幅の管理には使用しませんが、その代わり、PQ がオーバーサブスクライブされないようにするために、オーディオ トラフィックの管理には使用します。これは音声専用コールです。

図 13-76 では、さまざまなコール フロー、それに対応するオーディオとビデオ ストリーム、そのダイレクト先のキューについて説明します。

図 13-76　プロビジョニングとアドミッション制御

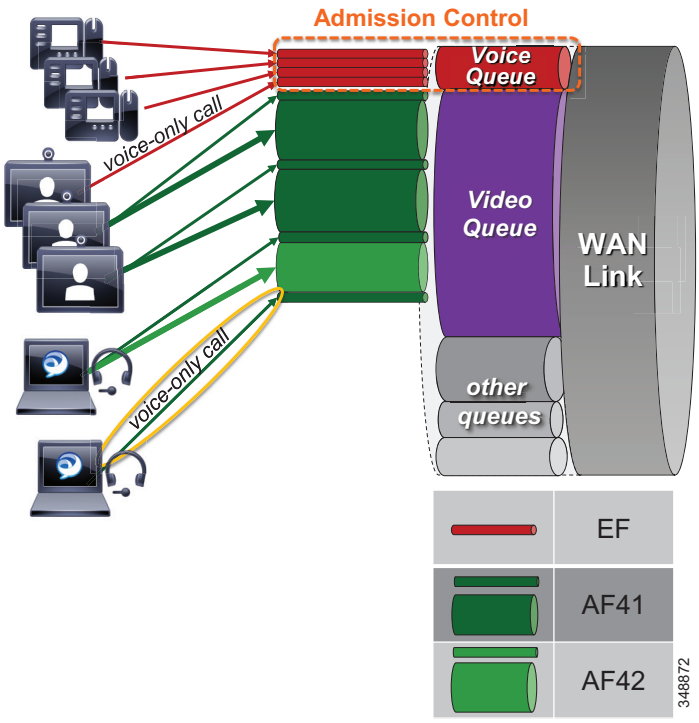


図 13-76 の例では、次の設定を使用します。

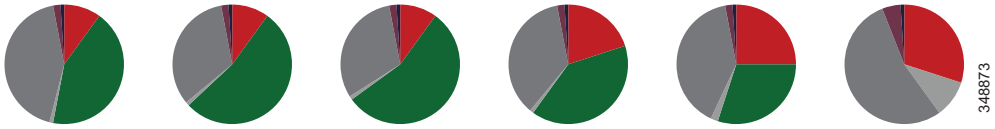
- プライオリティ キューは信頼されているエンドポイントからの音声コールにプロビジョニングされ、アドミッション制御（ELCAC 音声帯域幅プール）によって保護されます。
- ビデオ キューは、会議室ベースのビデオ システムにオーバープロビジョニングされます。
  - 比率は、デスクトップ ビデオ エンドポイントの帯域幅使用率に適用されます。
  - Jabber ビデオ コールは、ビデオ ルーム システムで使用されていない帯域幅を使用できます。
  - 輻輳の発生時、Jabber コールのビデオ ストリームでは、WRED が低下するため、ビデオ ビット レートが動的に下がります。

帯域幅割り当てのガイドライン

図 13-77 の帯域幅割り当ては、この企業例 #1 だけに基づいたガイドラインです。コラボレーション トラフィックのさまざまな共通クラスで利用可能な帯域幅の割合について説明しています。帯域幅のプロビジョニングは使用率に大きく依存しており、それぞれの展開と、各サイトで割り当てられるユーザ ベースごとに異なることを理解することが重要です。次の例では、帯域幅のプロビジョニングに使用するプロセスを説明します。帯域幅のプロビジョニング後、最適なユーザ エクスペリエンスに必要な最高の帯域幅のプロビジョニングと割り当てを維持するには、帯域幅の監視および再調整が常に必要です。

図 13-77　帯域幅割り当てのガイドライン

WAN Link Speed / Class	622 Mbps (OC12)	155 Mbps (OC3)	34-44 Mbps (E3/DS3)	10 Mbps	5 Mbps	<2 Mbps (T1/E1)
Control (%)	1	1	1	1	2	10
Voice (%)	10	10	10	20	25	30
Video (%)	43	53	55	40	30	--
Signalling (%)	2	2	2	2	2	5
Scavenger (%)	1	1	1	1	1	1
Default (%)	43	33	31	36	40	54



ここでは、各サイト（中央、大規模支社、小規模支社、営業所）と、各クラスのユーザ数と利用可能な帯域幅に基づいてクラスごとにプロビジョニングされたリンク帯域幅について説明します。これらの値は、レイヤ 3 以上用に計算された帯域幅に基づいていることに注意してください。そのため、リンク タイプ（イーサネット、フレーム リレー、MPLS など）に依存しているレイヤ 2 のオーバーヘッドは含まれていません。レイヤ 2 のオーバーヘッドの詳細については、ネットワーク インフラストラクチャ（3-1 ページ）の項を参照してください。

中央サイト リンク（100 Mbps）帯域幅の計算

図 13-78 で示すように、中央サイトには次の帯域幅要件があります。

- 音声キュー（PQ）：10 Mbps（L3 帯域幅）

  G.711/G.722 で 125 コール
- 音声プール用の Unified CM ロケーション リンク帯域幅：

  125 * 80 kbps = 10 Mbps
- ビデオ キュー：55 Mbps（L3 帯域幅）
  - イマーシブ エンドポイント：2 Mbps * 1 コール = 2 Mbps
  - ビデオ エンドポイント：1.2 Mbps * 30 コール * 0.2 = 7.2 Mbps
  - TelePresence Servers：1.5 Mbps * 40 コール * 0.5 = 30 Mbps
  - 55 Mbps – (2 Mbps + 7.2 Mbps + 30 Mbps) = Jabber メディア用 15.8 Mbps

    576p で 18 Jabber ビデオ コール、または 288p で 50

    （さらに残りの帯域幅）

計算上の注意

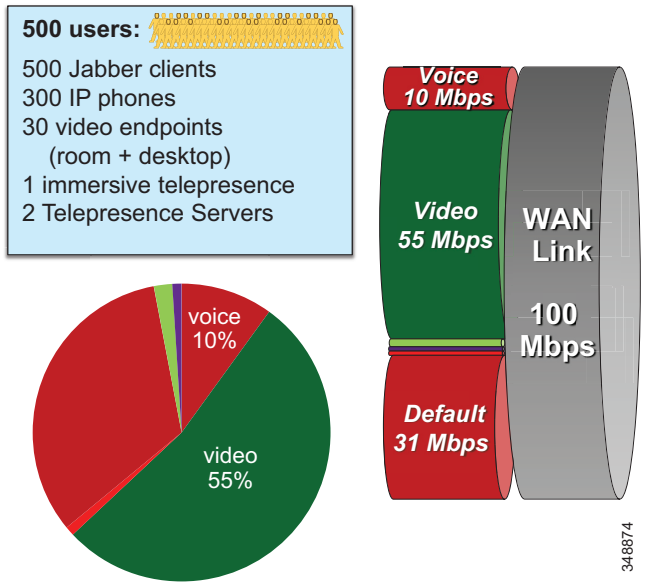
イマーシブ エンドポイントは最繁時に応じて決定されます。あるエンドポイントで WAN 経由のコールがあるとします。会議コールは TelePresence サーバでローカルに終了するため、これはポイントツーポイント コールになります。最頻時の最悪のシナリオを考慮することが重要です。

ビデオ エンドポイントの WAN 使用率は 20 %（*0.2）に指定されます。1.2 Mbps での有効な総コール数は 30 で、エンドポイントの数に基づいています。ただし、WAN 経由のアクティブ コールの WAN 使用率が 20 % しかないとすると、アクティブ ローカル コールと比較して、WAN 使用レートは 7.2 Mbps 以上になります。

TelePresence Server では、リモート サイトにあるエンドポイントのさまざまな解像度の平均を考慮して、平均ビット レートは 1.5 Mbps に指定されます。その場合、TelePresence Server は、最大 40 コール（ローカルとリモート）をサポートできます。このコールの 50 %（0.5 倍）は、WAN 経由で転送される TelePresence コールの半分に対応し、残りの半分はローカル エンドポイント用です。

さらに、Jabber コールが 15.8 Mbps の場合、576p で 18 コールや 288p で 50 コールなど幅広く対応します。このことから、Jabber ビデオ コールが帯域幅に応じて利用できることがわかります。15.8 Mbps 以上で多くの Jabber ビデオ コールが発生すると、パケット損失が起こり、すべての Jabber クライアントでビット レートが下方調整されます。これは、新しいコールが追加されても損失レートは低く、ユーザ エクスペリエンスに明確な影響を与えない非常に軽微なプロセスなのか、パケットの即時損失が発生した場合に Jabber ビデオに多大な影響を与えるかのどちらかです。新しいビデオ コールが追加されるときの予想パケット損失レートは、この状況対応型ビデオのユーザ エクスペリエンスが中断されるレベルを決定するのに役立ちます。

図 13-78　　中央サイト

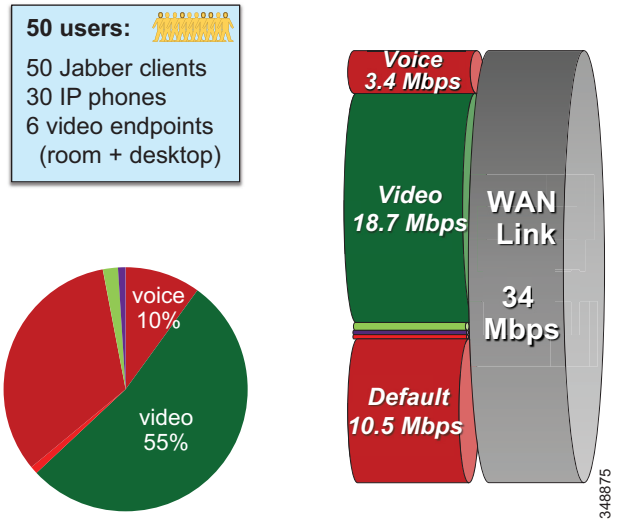


大規模支店リンク（34 Mbps）帯域幅の計算

図 13-79 で示すように、大規模支店サイトには次の帯域幅要件があります。

- 音声キュー（PQ）：3.4 Mbps（L3 帯域幅）
  G.711/G.722 で 42 コール
- 音声プール用の Unified CM ロケーション リンク帯域幅：
  42 * 80 kbps = 3.360 Mbps
- ビデオ キュー：18.7 Mbps（L3 帯域幅）
  - ビデオ エンドポイント：1.2 Mbps * 6 コール = 7.2 Mbps
  - 18.7 Mbps – 7.2 Mbps = 11.5 Mbps（Jabber メディア用）
    576p で 13 Jabber ビデオ コール、または 288p で 36
    （さらに残りの帯域幅）

図 13-79　大規模支店

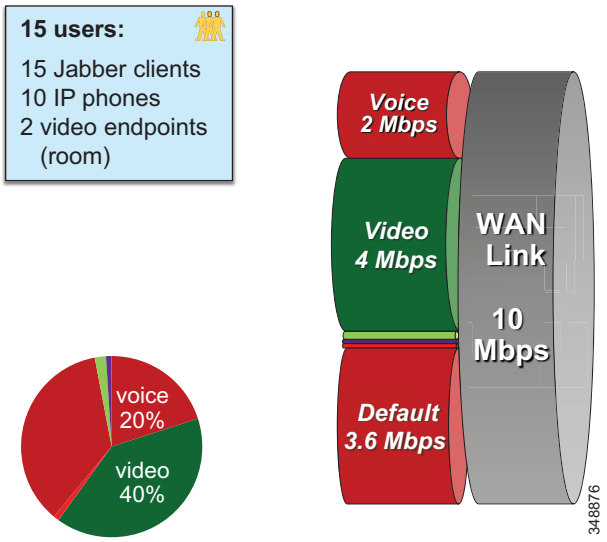


小規模支店リンク（10 Mbps）帯域幅の計算

図 13-80 で示すように、小規模支店サイトには次の帯域幅要件があります。

- 音声キュー（PQ）：2 Mbps（L3 帯域幅）
  G.711/G.722 で 25 コール
- 音声プール用の Unified CM ロケーション リンク帯域幅：
  25 * 80 kbps = 2 Mbps
- ビデオ キュー：18.7 Mbps（L3 帯域幅）
  - ビデオ エンドポイント：1.2 Mbps * 2 コール = 2.4 Mbps
  - 4 Mbps – 2.4 Mbps = 1.6 Mbps（Jabber メディア用）
    576p で 2 Jabber ビデオ コール、または 288p で 5
    （さらに残りの帯域幅）

図 13-80　小規模支店

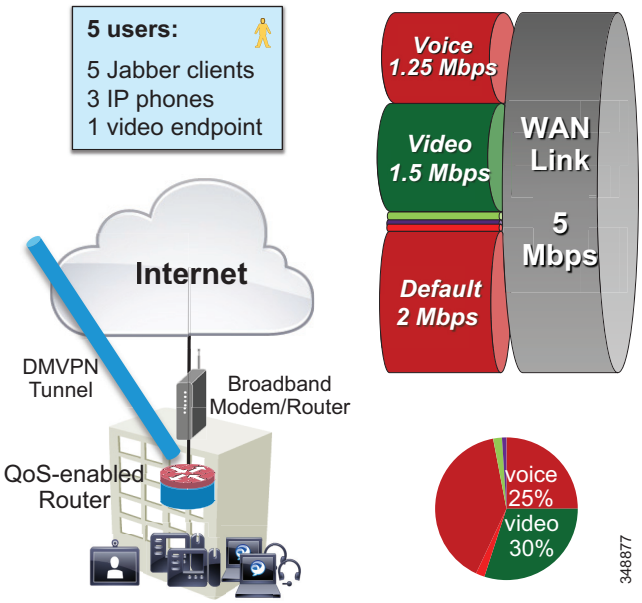


営業所ブロードバンド インターネット接続（5 Mbps）帯域幅の計算

図 13-81 で示すように、営業所サイトには次の帯域幅要件があります。

- ブロードバンド インターネット接続 + 中央サイトへの DMVPN
- ブロードバンド アップリンク速度に対応するように VPN ルータのインターフェイスを設定する
- TCP フローの bufferbloat を回避するために VPN ルータで QoS を有効にする
- 非対称ダウンロード/アップロードのブロードバンド: ビデオ エンドポイントでのビットレートの制限を検討する

図 13-81　営業所



制限付き WAN リンクを使用する大規模支店（ビデオに対応する Enhanced Locations CAC）

低速 WAN リンクを持つ特定の支店サイトでは、ビデオ キューのオーバープロビジョニングは実現不可能です（図 13-82 を参照）。ELCAC は、ビデオ コールがリンク帯域幅をオーバーサブスクライブしないように、ビデオのこれらのロケーション リンクに適用できます。このテンプレートでは、サイト固有のリージョン設定を使用して、ビデオ エンドポイントおよび Jabber クライアントで使用される最大帯域幅を制限する必要があります。また、Jabber ユーザがサイト間でローミングする場合には、デバイス モビリティも必要になることに注意してください。

（注）　音声専用 Jabber コールの帯域幅は「音声」ELCAC から差し引かれますが、（AF41 にマーキングされているため）ビデオ キューに影響します。ビデオ ELCAC 帯域幅とビデオ キュー サイズの差分を調整します。

図 13-82　制限付き WAN リンクを使用する大規模支店（ビデオに対応する Enhanced Locations CAC）

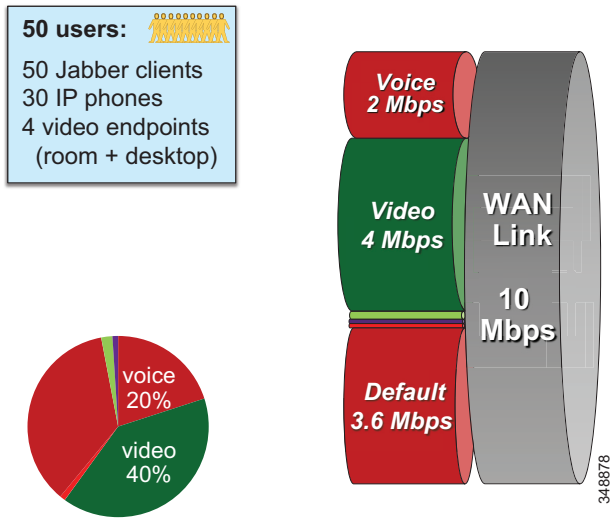


図 13-82 の説明のとおり、制限付き WAN リンク（10 Mbps）の大規模支店サイトには次の帯域幅要件があります。

- 音声キュー（PQ）：2 Mbps（L3 帯域幅）

  G.711/G.722 で 25 コール
- 音声プール用の Unified CM ロケーション リンク帯域幅：

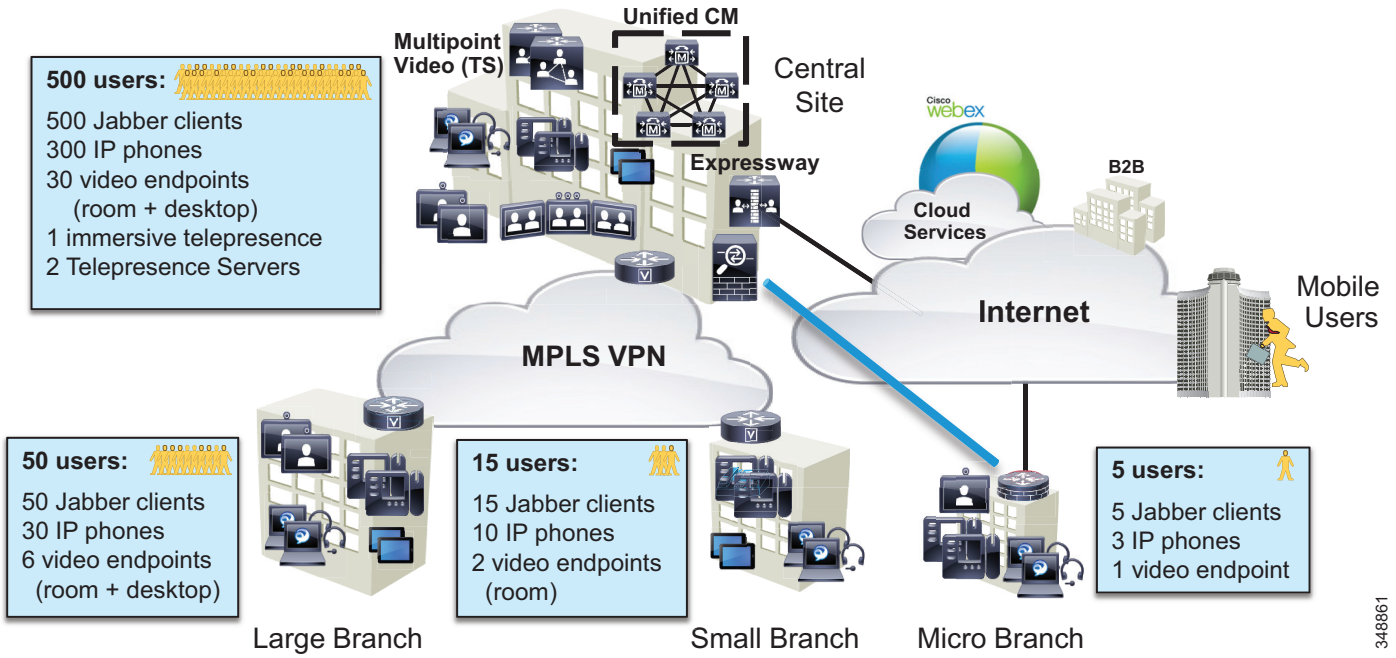
  25 * 80 kbps = 2 Mbps
- ビデオ キュー：4 Mbps（L3 帯域幅）
  - 有効な使用方法：576p（768 kbps）で 2 コール + 288p（320 kbps）で 5 コール = 3,136 kbps
  - ビデオ コールの Unified CM ロケーション リンク帯域幅：3.2 Mbps（L3 帯域幅）
  - L2 オーバーヘッド、バースト性、AF41 とマーキングされた Jabber オーディオ専用コールのために帯域幅を確保する

企業例 #2

企業例 #2 は、広範囲の地域にユーザを持ち、本社にはデータ センター（DC）が設置され、あらゆる規模（約 500 人、50 人、15 人）の支社が複数あり、各支店にはそれぞれ 5 人のユーザがいる大企業です。ネットワーク図を簡略化するため、これらのサイトのカテゴリ（HQ、大、小、事務所）をテンプレートとして使用し、同様のユーザとエンドポイントの密度を持つ各サイトに応じた帯域幅の考慮事項を決定します。図 13-83 では、各サイト タイプについて説明します。この企業は、ビデオのために Jabber を導入し、ユーザが会議でビデオ端末にアクセスできるようにしています。TelePresence ビデオ会議リソースは HQ の DC に配置されています。IP Phone は音声専用通信用です。ビデオ エンドポイントには、Jabber クライアント、コラボレーション デスクトップ エンドポイント（DX シリーズ）、およびルーム エンドポイント（MX、プロファイル、および SX シリーズ）を使用しています。大規模なサイトには、IX シリーズなどのイマーシブ TelePresence ユニットが用意されています。

（注）　企業例 #2 のすべてのエンドポイント（信頼済みと非信頼）では、すべてのオーディオ（音声専用コールとビデオ コール）を EF にマーキングし、Jabber ビデオを AF41 または AF42 にマーキングするように設定されている点で、企業例 #2 は企業例 #1 と大きく異なります。また、企業例 #2 は、オーディオ部分のビデオ キューの保護に Enhanced Locations CAC も使用しています。Cisco Collaboration System Release（CSR）12.*x* には、ビデオ プールからすべてのオーディオを差し引くことができる機能があります。詳細については、Enhanced Locations Call Admission Control（13-42 ページ）の項を参照してください。

図 13-83　企業例 #2



IT 部門は、企業例 #2 の各サイト タイプに応じた WAN エッジの帯域幅要件の決定を任されています。次に要件を一覧で表示し、QoS の適用方法と、帯域幅、キューイング、アドミッション制御の要件の決定方法について説明します。

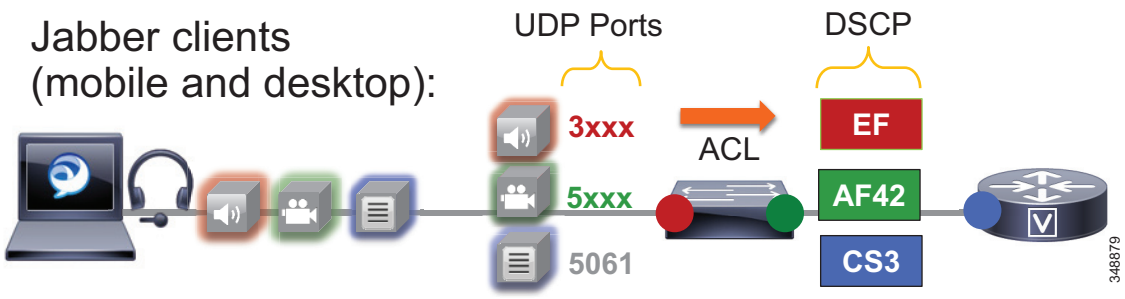
識別と分類

ここでは、企業全体の QoS 要件を確立します。

信頼されていないエンドポイント（Jabber）

Jabber エンドポイントは信頼されておらず、データ VLAN 内に配置されています。企業例 #2 では、アクセス レイヤ スイッチでシグナリングおよびメディアを再マーキングするのに特定の UDP ポート範囲を使用します。この場合、Unified CM の設定には、個別のメディアおよび 3000 ～ 3999 のオーディオ用と 5000 ～ 5999 のビデオ用のシグナリング ポート範囲を使用するすべての Jabber クライアント専用の SIP プロファイルを使用します。セキュア SIP シグナリング ポート 5061 は、Secure SIP シグナリング ポートとして使用されます。図 13-84 でこれについて説明します。

図 13-84　信頼されていない（Jabber）エンドポイント QoS



管理者は、次の DSCP 値に UDP ポートを再マーキングするデータ VLAN にアクセス スイッチの ACL を作成します。

- オーディオ：EF にマーキングされる UDP ポート 3000 ～ 3999
- ビデオ：AF42 にマーキングされる UDP ポート 5000 ～ 5999
- シグナリング：CS3 にマーキングされる TCP ポート 5060 ～ 5061

Jabber の分類概要：

- すべての Jabber コールのオーディオ ストリーム（音声専用とビデオ）は EF にマーキングされています。
- Jabber ビデオ コールのビデオ ストリームは AF42 にマーキングされています。

Jabber エンドポイントの場合、Jabber SIP プロファイルでデフォルトの QoS 値も変更することをお勧めします。これは、何らかの理由で QoS がワイヤレス ルータ経由または他の方法で「信頼されている」場合、適切な「信頼されている」値が再マーキング値と同じになるようにするためです。そのため、SIP プロファイルの QoS パラメータは、表 13-17 に示すように設定する必要があります。

表 13-17　信頼されていない Jabber エンドポイントの SIP プロファイルの QoS パラメータ

QoS サービス パラメータ名（SIP プロファイル）	システム デフォルト値	変更値
音声コールの DSCP（DSCP for Audio Calls）	EF	
ビデオ コールの DSCP（DSCP for Audio Calls）	AF41	AF42
ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）	AF41	EF
TelePresence コールの DSCP（DSCP for TelePresence Calls）	CS4	AF41
TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）	CS4	EF

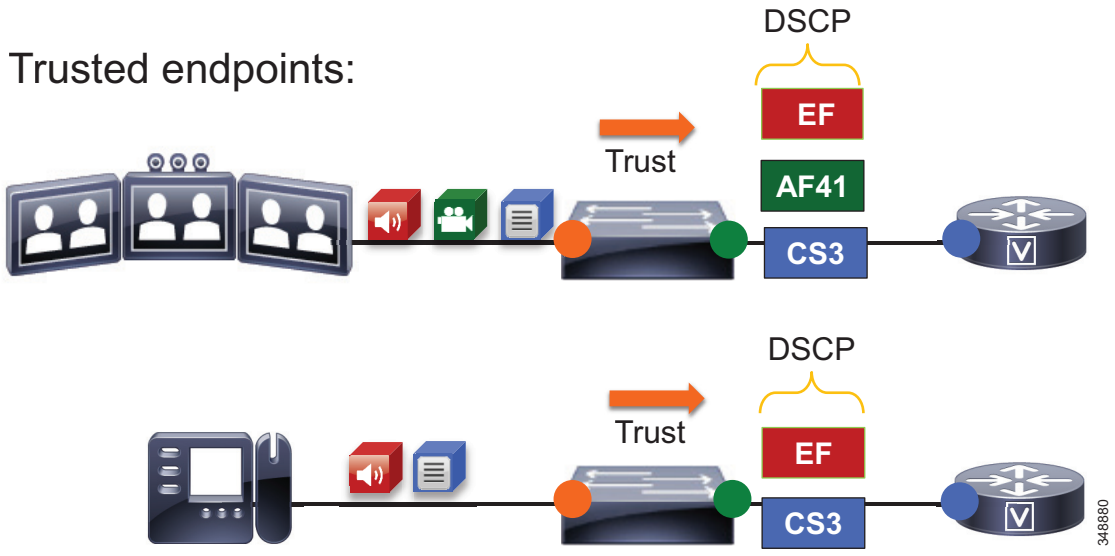
表 13-17 の設定により、何らかの理由で Jabber クライアントのオーディオとビデオが信頼され、アクセス スイッチで UDP ポート範囲経由で再マーキングされない場合、Jabber クライアントのオーディオは EF に設定され、ビデオは AF42 に設定されます。これは単に、Jabber エンドポイント間で設定の一貫性を確保するためです。

信頼されているエンドポイント

信頼されているエンドポイントの場合、Cisco Discovery Protocol（CDP）が使用され、IP Phone およびビデオ エンドポイントの QoS は、アクセス スイッチで設定された条件付き信頼メカニズムを使用して信頼されます。すべてのエンドポイントのオーディオすべてが EF に設定されるように、デフォルト設定を変更する必要があります。この場合、Unified CM の設定には、ビデオ コールと TelePresence コールのオーディオをそれぞれ EF に変更する SIP プロファイルを使用します。

図 13-85 では、アクセス スイッチの条件付き信頼（CDP ベース）およびパケット マーキングを示します。

図 13-85　信頼されているエンドポイント QoS



管理者は、次に分類されるように、IP Phone およびビデオと TelePresence エンドポイントの条件付き QoS 信頼ですべてのアクセス スイッチを設定します。

- 音声専用コールとビデオ コールのオーディオ ストリームは EF にマーキングされています。
- ビデオ コールのビデオ ストリームは AF41 にマーキングされています。

管理者は、表 13-18 に記載された DSCP 値を使用して、信頼されているエンドポイントの Unified CM の SIP プロファイルを設定します。

表 13-18　信頼されているエンドポイントの SIP プロファイルの QoS パラメータ

QoS サービス パラメータ名（SIP プロファイル）	システム デフォルト値	変更値
音声コールの DSCP（DSCP for Audio Calls）	EF	
ビデオ コールの DSCP（DSCP for Audio Calls）	AF41	
ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）	AF41	EF
TelePresence コールの DSCP（DSCP for TelePresence Calls）	CS4	AF41
TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）	CS4	EF

WAN エッジの入力に到着する特定の DSCP 値を持つパケットは、アクセス レイヤで信頼されているか、またはアクセス スイッチで信頼されていない場合は適宜再マーキングされていることが予想されます。入力のフェールセーフ プラクティスとして、アクセス レイヤで再マーキングできなかった信頼されていないトラフィックは、WAN エッジで再マーキングすることが重要です。QoS は LAN で重要ですが、WAN では最も重要です。ルータは入力トラフィックが信頼されていると見なすため、ビジネス要件およびユーザ エクスペリエンスに応じた適切な QoS ポリシーを設定することが重要です。WAN エッジの再マーキングは、ルータへの入力インターフェイスで常に実行されます。キューイングおよびスケジューリングは出力インターフェイスで実行されます。次に、WAN 入力 QoS ポリシーと出力キューイング ポリシーの例を示します。図 13-86 では、設定と再マーキングのプロセスを説明します。

図 13-86 では、ネットワークの信頼されている領域と信頼されていない領域の両方から送られるパケットは、前述の信頼方法または UDP ポート範囲に一致する簡単な ACL を経由し、適切な DSCP マーキングを使用して識別および分類されます。この ACL は、IP アドレスと、マーキング範囲を細かに制限する他のいくつかの属性にも細部にわたって一致する可能性があることに注意してください。

図 13-86　ルータ入力 QoS ポリシー プロセス例：ステップ 1

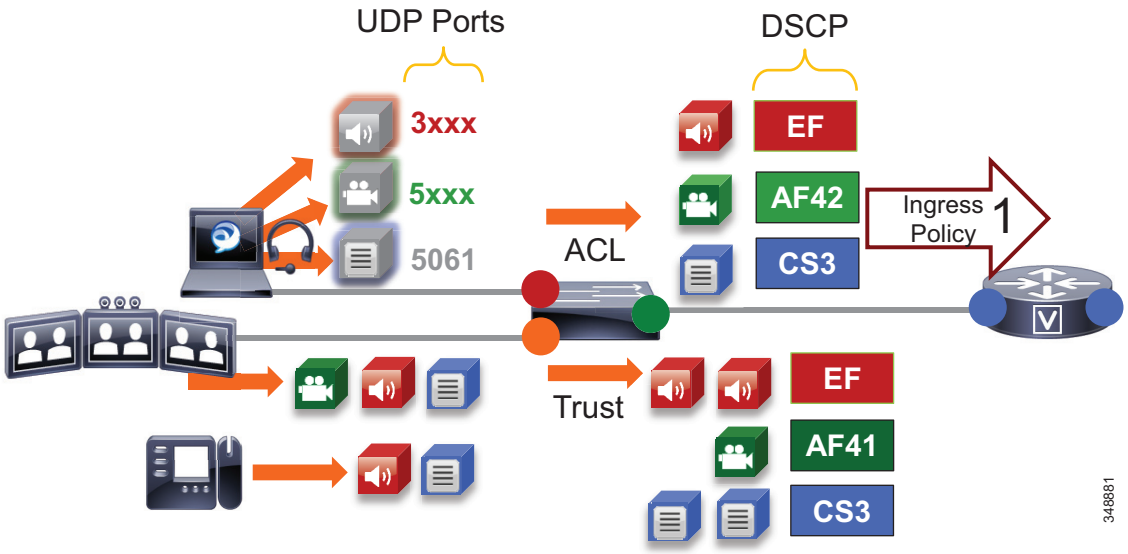
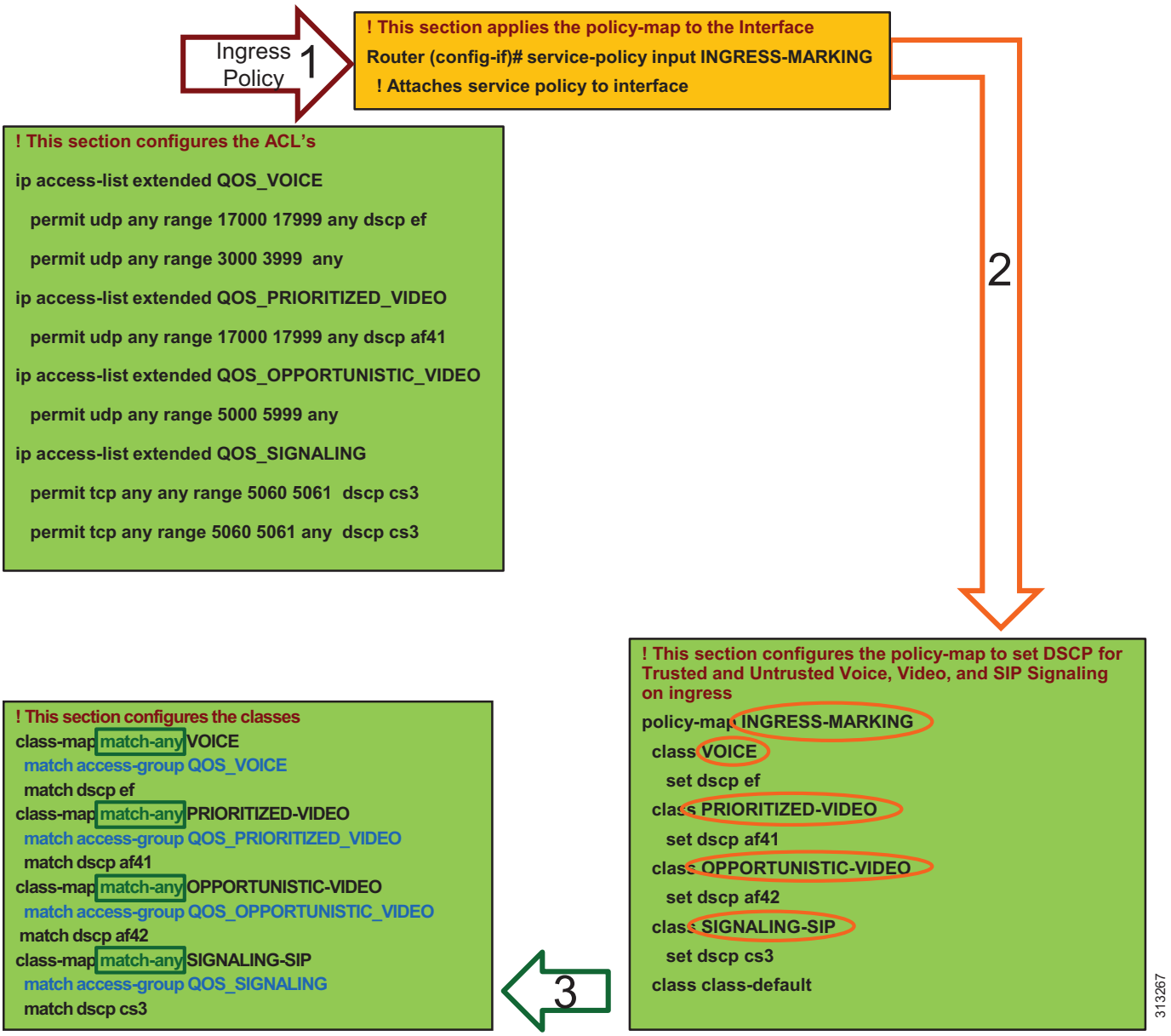


図 13-87 では、ポリシー一致基準および DSCP 再マーキングについて説明します。このプロセスには、図に示された次のステップが含まれます。

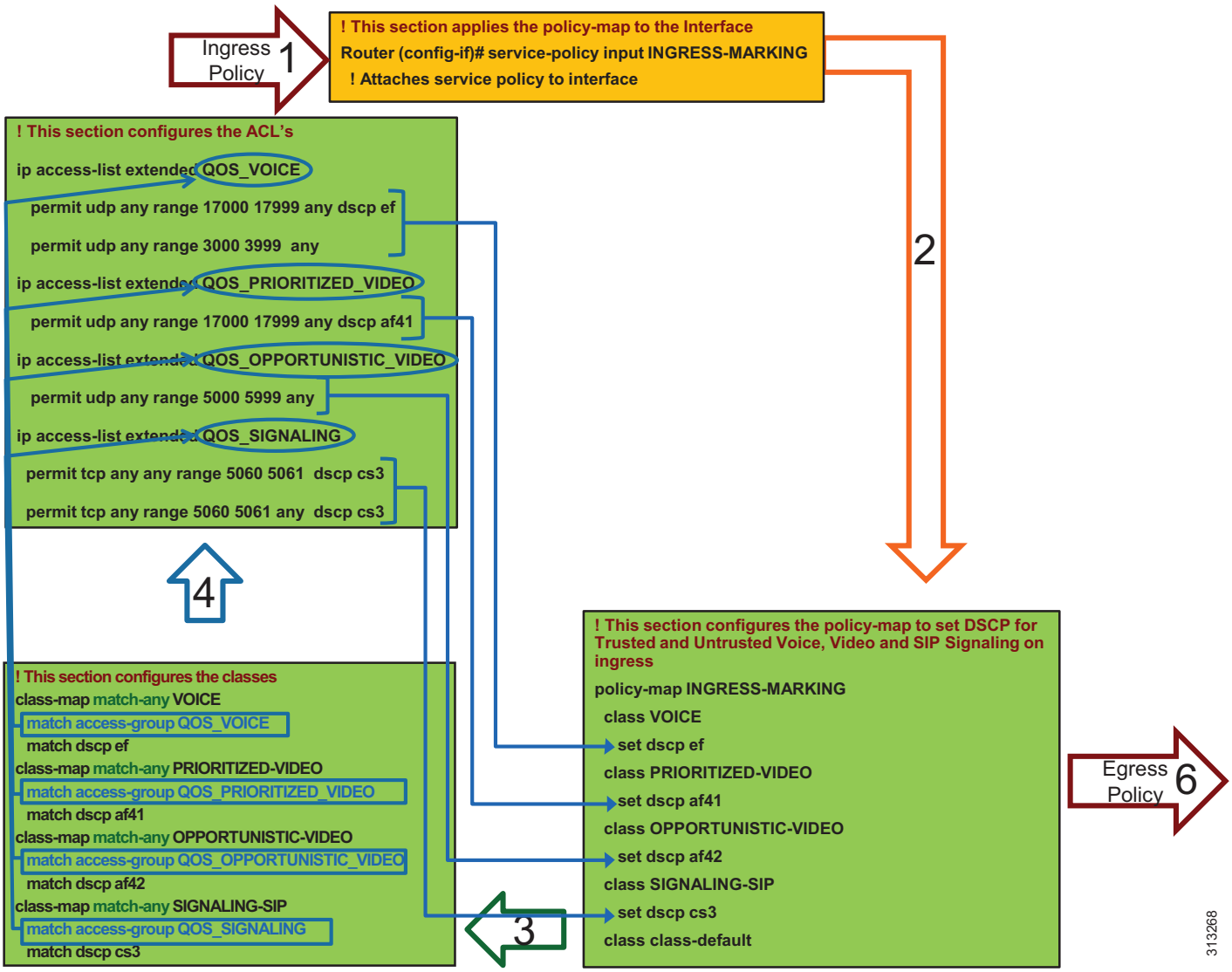
1. パケットがルータ入力インターフェイスに到着し、入力サービス ポリシーで設定されます（図 13-87）。
2. policy-map は、適切な DSCP を設定するトラフィックの 4 つのクラスで設定されます。EF の DSCP を設定する VOICE、AF41 の DSCP を設定する PRIORITIZED-VIDEO、AF42 の DSCP を設定する OPPORTUNISTIC-VIDEO、CS3 の DSCP を設定する SIGNALING-SIP（図 13-87）です。
3. 各クラスは、[いずれかに一致（match-any）] 基準、DSCP 一致、ACL 一致が設定された同名の class-map と一致します。この [いずれかに一致（match-any）] 基準の場合、プロセスはトップダウン方式で、最初に一致した基準が実行され、次に policy-map ステートメントの各クラスに従って DSCP を設定します。[すべてに一致（match-all）] はもう 1 つの方法で、すべての基準に一致する必要があります。つまり、DSCP *および* ACL と一致します。ただし、マーキングされたトラフィック *または* マーキングされていないトラフィックのいずれかを再マーキングするための機能ではありません。

図 13-87　ルータ入力 QoS ポリシー プロセス例：ステップ 1～3



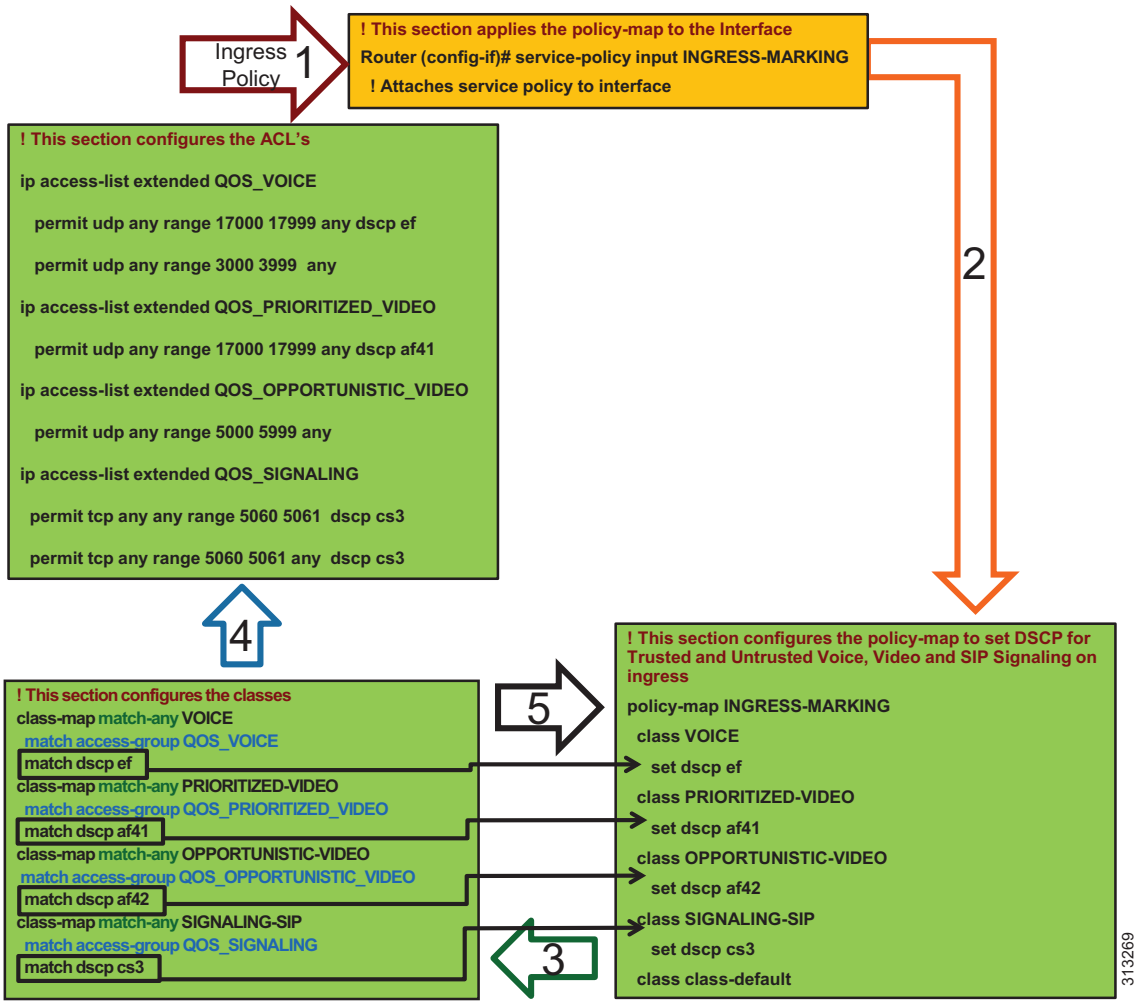
4. ステップ 4 で、class-map ステートメントの最初の行が解析されます。これは Unified CM の識別と分類セクションに設定されている UDP ポートに一致する ACL です。ACL 基準（プロトコル、ポート範囲、および場合により DSCP）が一致する場合は、対応する policy-map ステートメントで設定されているとおりにトラフィックがマーキングされます（図 13-88）。
図 13-86 のポリシーに従って、Jabber Audio は EF とマーキングされ、Jabber Video は AF42 とマーキングされることに注意してください。

図 13-88　ルータ入力 QoS ポリシー プロセス例：ステップ 4



5. ステップ 5 で、最初のステートメントに一致しないトラフィックは class-map 内の次の match ステートメント、**match dscp** に移動します（図 13-89）。トラフィックが DSCP と単純に一致する場合、DSCP はすでに一致したものと同じ値に再び設定され、policy map ステートメントで設定されたかのようになります。この場合、ルータは単純に DSCP に一致し、DSCP を同じ値にリセットします。これはサーバおよびアプリケーションから WAN ルータに入ってくる信頼された DSCP の catch-all 設定です。

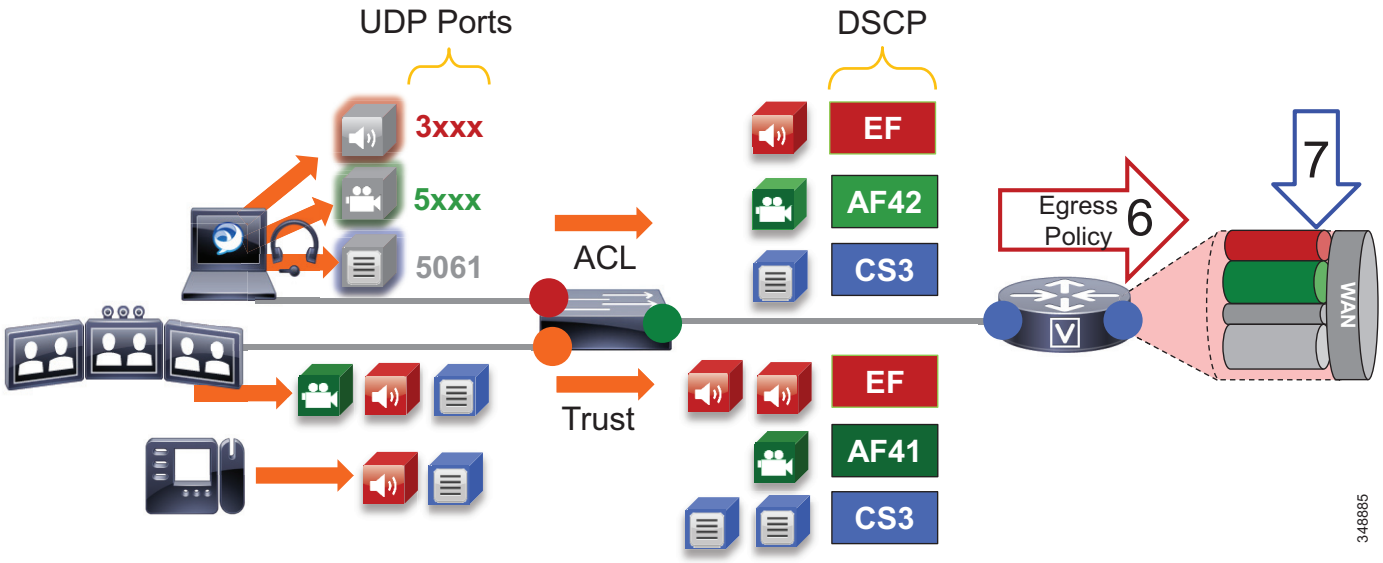
図 13-89　ルータ入力 QoS ポリシー プロセス例：ステップ 5



(注)　これは、Cisco Common Classification Policy Language（C3PL）に基づいた QoS 入力マーキング ポリシー例です。C3PL をサポートするシスコ ルータで同様のポリシーを実現する方法と、更新されたコマンドについては、特定のルータの設定ガイドを参照してください。

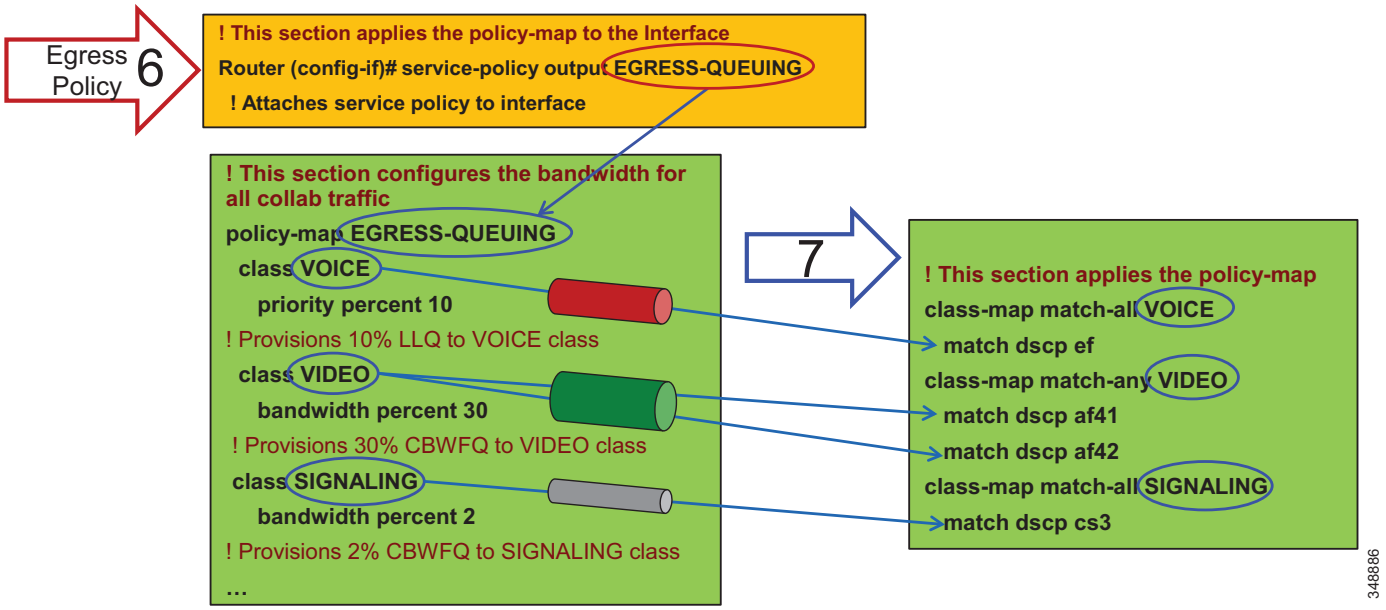
6. トラフィックは、3 つのキュー（VOICE と呼ばれる Priority Queue、VIDEO と呼ばれる CBWFQ、SIGNALING と呼ばれる CBWFQ）が作成された出力サービス ポリシーによってキュー登録およびスケジューリングされた送信インターフェイスに移動します。（図 13-90）。これは、この出力キューイング ポリシーが、アクセス スイッチや WAN ルータ入力インターフェイスへの入力で発生するネットワーク マーキングとして DSCP のみに基づいている点を強調しています。これは、一致基準およびキューを説明するための単なる例であり、WRED 機能（次の項で説明）は含まれていません。WRED の詳細については、WAN キューイングとスケジューリング（13-124 ページ）の次の項を参照してください。

図 13-90　ルータ出力キューイング ポリシー プロセス例:ステップ 6



7. トラフィックが class-map 一致ステートメントと一致します。EF とマーキングされたトラフィックはすべて VOICE PQ に送られ、AF41 と AF42 のトラフィックは VIDEO CBWFQ に、CS3 のトラフィックは SIGNALING CBWFQ に送られます（図 13-91）。

図 13-91　ルータ出力キューイング ポリシー プロセス例:ステップ 7



（注）　これは、Cisco Common Classification Policy Language（C3PL）に基づいた出力キューイング ポリシー例です。C3PL をサポートするシスコ ルータで同様のポリシーを実現する方法と、更新されたコマンドについては、特定のルータの設定ガイドを参照してください。

WAN キューイングとスケジューリング

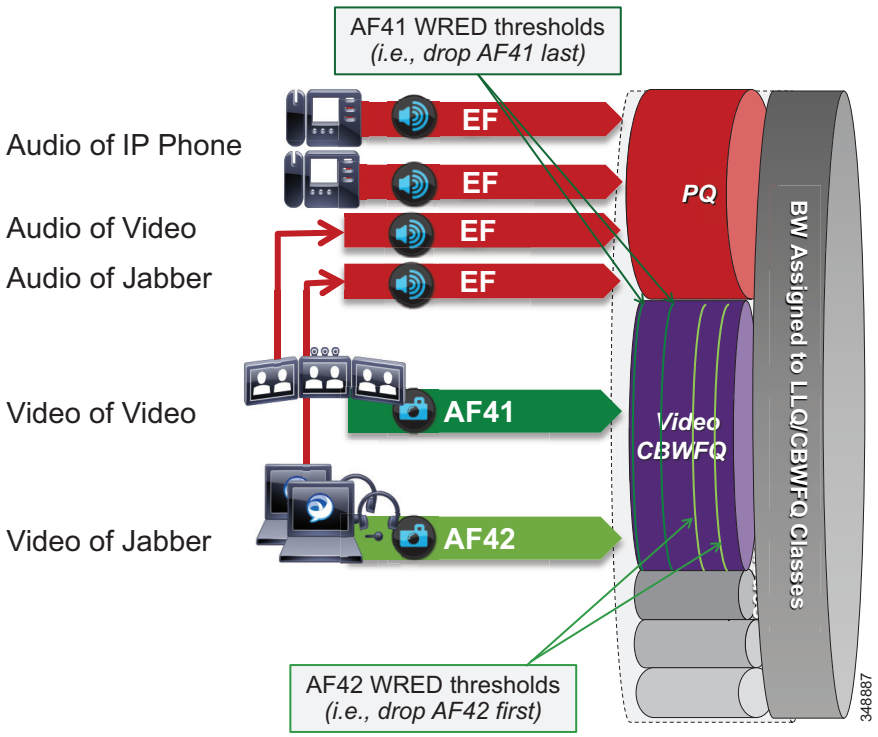
ここでは、インターフェイス キューイングについて説明します。図 13-92 では、CBWFQ で使用される音声 PQ、ビデオ CBWFQ、および WRED のしきい値について説明します。

- EF とマーキングされたすべてのエンドポイント（信頼済みと非信頼）からのオーディオはすべて、PQ にマッピングされます。
- ビデオ コールおよび Jabber は同じ CBWFQ を共有します。
  - 信頼されているエンドポイントからのビデオ コールのオーディオ ストリームには EF
  - 信頼されているエンドポイントからのビデオ コールのビデオ ストリームには AF41
  - Jabber クライアントからのすべてのコールのオーディオ ストリームには EF
  - Jabber クライアントからビデオ コールのビデオ ストリームには AF42
- WRED はビデオ キューで設定されます。
  - AF42 の最小および最大のしきい値:

    キュー制限の約 10 % ～ 30 %
  - AF41 の最小および最大のしきい値:

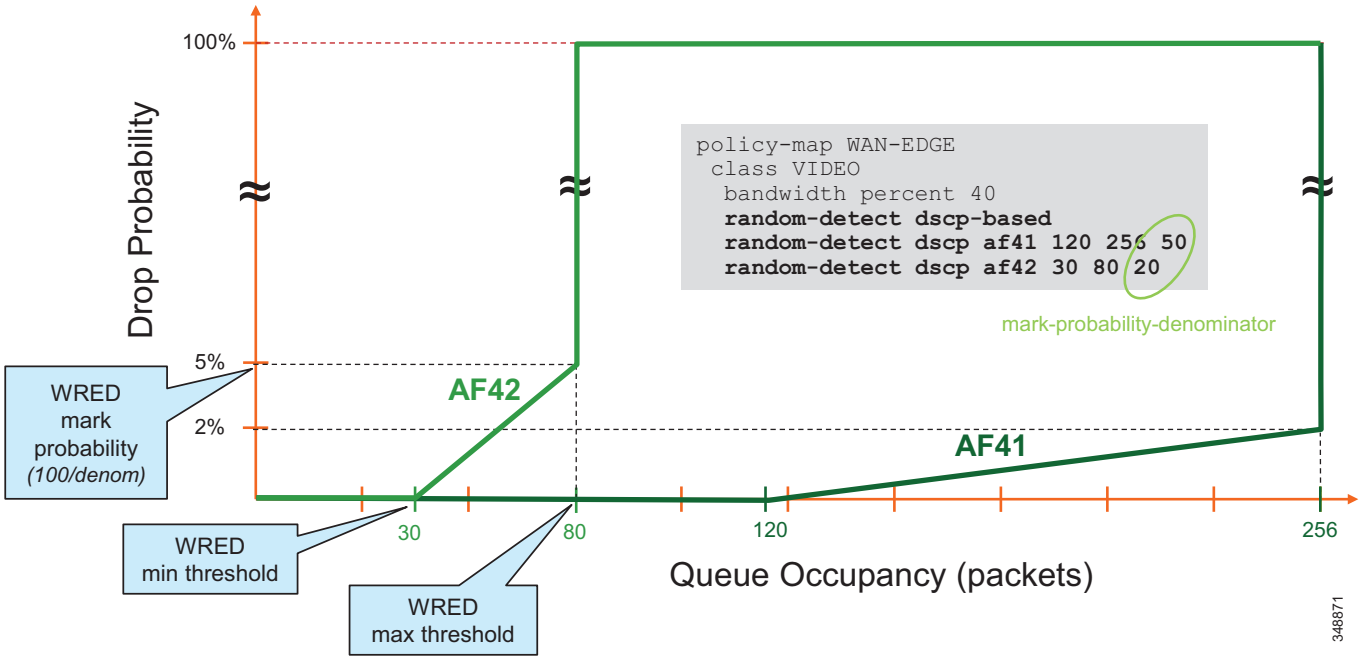
    キュー制限の約 45 % ～ 100 %

図 13-92　キューイングとスケジューリングのコラボレーション メディア



重み付けランダム早期検出（WRED）の最小および最大しきい値は、Video CBWFQ でも設定されます。WRED のしきい値の設定方法を説明するため、インターフェイスはキューの深さが 256 パケットで設定されていると仮定します。次に、上述のガイドラインに従って、AF42 および AF41 の WRED の最小しきい値および最大しきい値が、図 13-93 の説明とおりに設定します。

図 13-93　WRED のしきい値を持つビデオ CBWFQ の例



プロビジョニングとアドミッション制御

ここでは、各サイト タイプのキューに対してアドミッション制御およびプロビジョニング帯域幅を指定します。

前述のとおり、このような場合、アドミッション制御をビデオ帯域幅の管理には使用しませんが、その代わり、PQ がオーバーサブスクライブされないようにするために、オーディオ トラフィックの管理には使用します。この企業例 #2 では、Enhanced Locations CAC の音声プールは、音声専用コールとビデオ コールの両方のオーディオを許可しています。

Unified CM でこの機能をイネーブルにするには、コールした CallManager サービスのコール アドミッション制御セクションで、サービス パラメータ [ビデオ コールのオーディオ プールからオーディオ帯域幅を差し引く (Deduct Audio Bandwidth from Audio Pool for Video Call)] を [True] に設定します。デフォルト設定は [False] であり、デフォルトでは、Unified CM はビデオ プールからビデオ コールのオーディオとビデオの両方のストリームを差し引きます。このパラメータはその動作を変更するため、企業例 #2 の QoS の変更に不可欠です。

図 13-94 では、さまざまなコール フロー、それに対応するオーディオとビデオ ストリーム、そのダイレクト先のキューについて説明します。

図 13-94　プロビジョニングとアドミッション制御

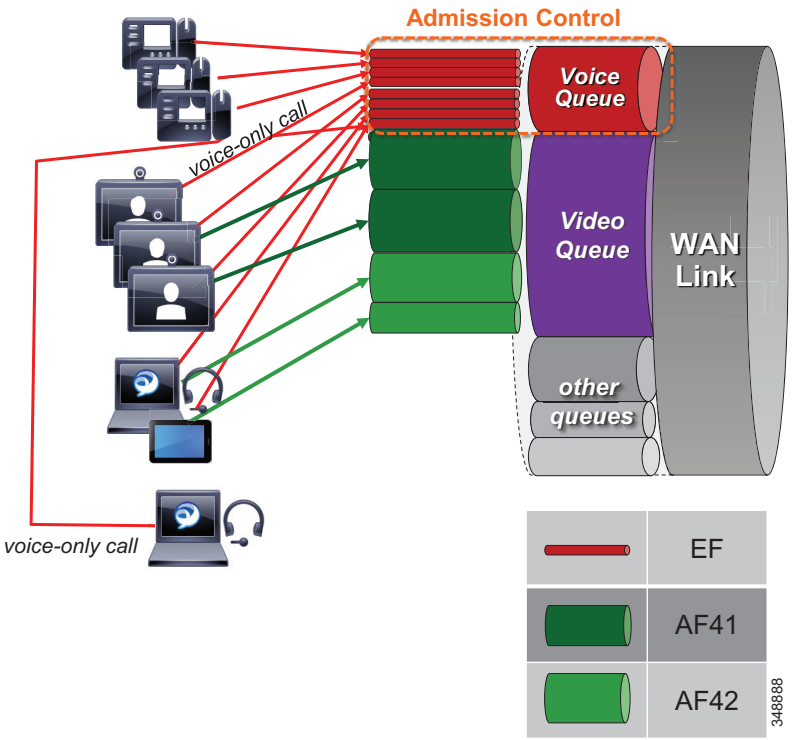


図 13-94 の例では、次の設定を使用します。

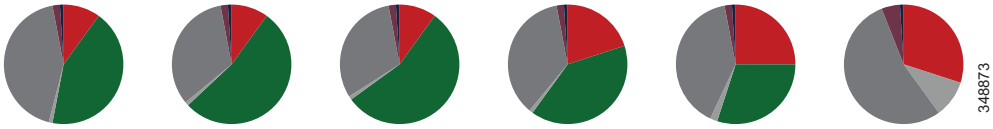
- プライオリティ キューは信頼されているおよび信頼されていないエンドポイント両方からのコールすべてにプロビジョニングされ、アドミッション制御（E-LCAC 音声 BW プール）によって保護されます。
- ビデオ キューは、会議室ベースのビデオ システムにオーバープロビジョニングされます。
  - 比率は、デスクトップ ビデオ エンドポイントの帯域幅使用率に適用されます。
  - Jabber ビデオ コールは、ビデオ ルーム システムで使用されていない帯域幅を使用できます。
  - 輻輳の発生時、Jabber コールのビデオ ストリームでは、WRED が低下するため、ビデオ ビット レートが動的に下がります。

帯域幅割り当てのガイドライン

図 13-95 の帯域幅割り当ては、この企業例 #2 だけに基づいたガイドラインです。コラボレーション トラフィックのさまざまな共通クラスで利用可能な帯域幅の割合について説明しています。帯域幅のプロビジョニングは使用率に大きく依存しており、それぞれの展開と、各サイトで割り当てられるユーザ ベースごとに異なることを理解することが重要です。次の例では、帯域幅のプロビジョニングに使用するプロセスを説明します。帯域幅のプロビジョニング後、最適なユーザ エクスペリエンスに必要な最高の帯域幅のプロビジョニングと割り当てを維持するには、帯域幅の監視および再調整が常に必要です。

図 13-95　帯域幅割り当てのガイドライン

WAN Link Speed / Class	622 Mbps (OC12)	155 Mbps (OC3)	34-44 Mbps (E3/DS3)	10 Mbps	5 Mbps	<2 Mbps (T1/E1)
Control (%)	1	1	1	1	2	10
Voice (%)	10	10	10	20	25	30
Video (%)	43	53	55	40	30	--
Signalling (%)	2	2	2	2	2	5
Scavenger (%)	1	1	1	1	1	1
Default (%)	43	33	31	36	40	54



ここでは、各サイト（中央、大規模支社、小規模支社、営業所）と、各クラスのユーザ数と利用可能な帯域幅に基づいてクラスごとにプロビジョニングされたリンク帯域幅について説明します。これらの値は、レイヤ 3 以上用に計算された帯域幅に基づいていることに注意してください。そのため、リンク タイプ（イーサネット、フレーム リレー、MPLS など）に依存しているレイヤ 2 のオーバーヘッドは含まれていません。レイヤ 2 のオーバーヘッドの詳細については、ネットワーク インフラストラクチャ（3-1 ページ）の項を参照してください。

また、ビデオ コールの帯域幅のオーディオ部分が音声プールから差し引かれるようになったことにも注意してください。音声キューをプロビジョニングするときは、音声専用コールとビデオ コールの両方のオーディオ帯域幅が含まれます。これらは企業例 #1（13-98 ページ）の例と同じです。唯一の違いは、企業例 #2 の場合、ビデオ コールの帯域幅のオーディオ部分は音声アドミッション制御プールから差し引かれ、オーディオ ストリームは音声キューに入ります。

中央サイト リンク（100 Mbps）帯域幅の計算

図 13-96 で示すように、中央サイトには次の帯域幅要件があります。

- 音声キュー（PQ）：10 Mbps（L3 帯域幅）

  G.711/G.722 で 125 コール
- 音声プール用の Unified CM ロケーション リンク帯域幅：

  125 * 80 kbps = 10 Mbps
- ビデオ キュー：55 Mbps（L3 帯域幅）
  - イマーシブ エンドポイント：2 Mbps * 1 コール = 2 Mbps
  - ビデオ エンドポイント：1.2 Mbps * 30 コール * 0.2 = 7.2 Mbps
  - TelePresence Servers：1.5 Mbps * 40 コール * 0.5 = 30 Mbps
  - 55 Mbps – (2 Mbps + 7.2 Mbps + 30 Mbps) = Jabber メディア用 15.8 Mbps

    576p で 18 Jabber ビデオ コール、または 288p で 50

    （さらに残りの帯域幅）

計算上の注意

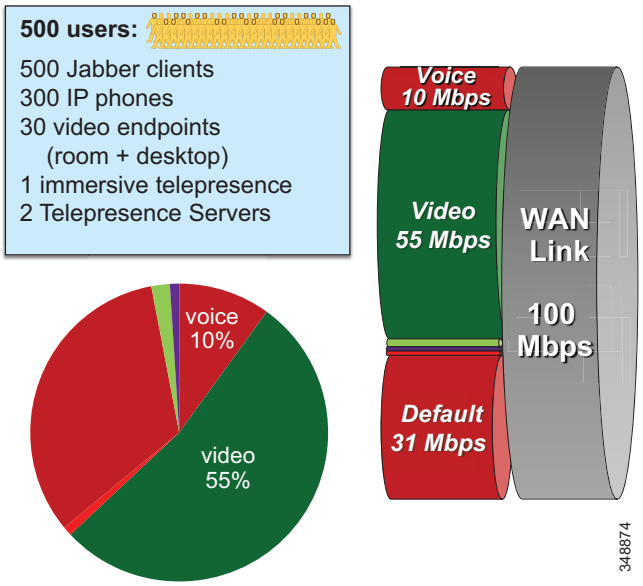
イマーシブ エンドポイントは最繁時に応じて決定されます。あるエンドポイントで WAN 経由のコールがあるとします。会議コールは TelePresence サーバでローカルに終了するため、これはポイントツーポイント コールになります。最頻時の最悪のシナリオを考慮することが重要です。

ビデオ エンドポイントの WAN 使用率は 20 %（*0.2）に指定されます。1.2 Mbps での有効な総コール数は 30 で、エンドポイントの数に基づいています。ただし、WAN 経由のアクティブ コールの WAN 使用率が 20 % しかないとすると、アクティブ ローカル コールと比較して、WAN 使用レートは 7.2 Mbps 以上になります。

TelePresence Server では、リモート サイトにあるエンドポイントのさまざまな解像度の平均を考慮して、平均ビット レートは 1.5 Mbps に指定されます。その場合、TelePresence Server は、最大 40 コール（ローカルとリモート）をサポートできます。このコールの 50 %（0.5 倍）は、WAN 経由で転送される TelePresence コールの半分に対応し、残りの半分はローカル エンドポイント用です。

さらに、Jabber コールが 15.8 Mbps の場合、576p で 18 コールや 288p で 50 コールなど幅広く対応します。このことから、Jabber ビデオ コールが帯域幅に応じて利用できることがわかります。15.8 Mbps 以上で多くの Jabber ビデオ コールが発生すると、パケット損失が起こり、すべての Jabber クライアントでビット レートが下方調整されます。これは、新しいコールが追加されても損失レートは低く、ユーザ エクスペリエンスに明確な影響を与えない非常に軽微なプロセスなのか、パケットの即時損失が発生した場合に Jabber ビデオに多大な影響を与えるかのどちらかです。新しいビデオ コールが追加されるときの予想パケット損失レートは、この状況対応型ビデオのユーザ エクスペリエンスが中断されるレベルを決定するのに役立ちます。

図 13-96　　中央サイト

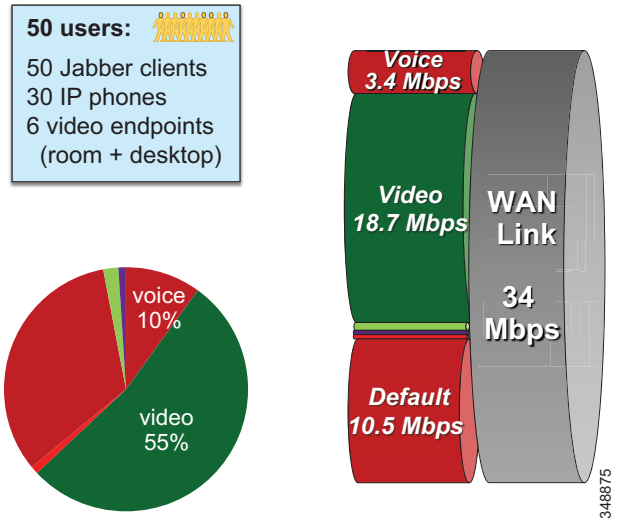


大規模支店リンク（34 Mbps）帯域幅の計算

図 13-97 で示すように、大規模支店サイトには次の帯域幅要件があります。

- 音声キュー（PQ）：3.4 Mbps（L3 帯域幅）
  G.711/G.722 で 42 コール
- 音声プール用の Unified CM ロケーション リンク帯域幅：
  42 * 80 kbps = 3.360 Mbps
- ビデオ キュー：18.7 Mbps（L3 帯域幅）
  - ビデオ エンドポイント：1.2 Mbps * 6 コール = 7.2 Mbps
  - 18.7 Mbps – 7.2 Mbps = 11.5 Mbps（Jabber メディア用）
    576p で 13 Jabber ビデオ コール、または 288p で 36
    （さらに残りの帯域幅）

図 13-97　大規模支店

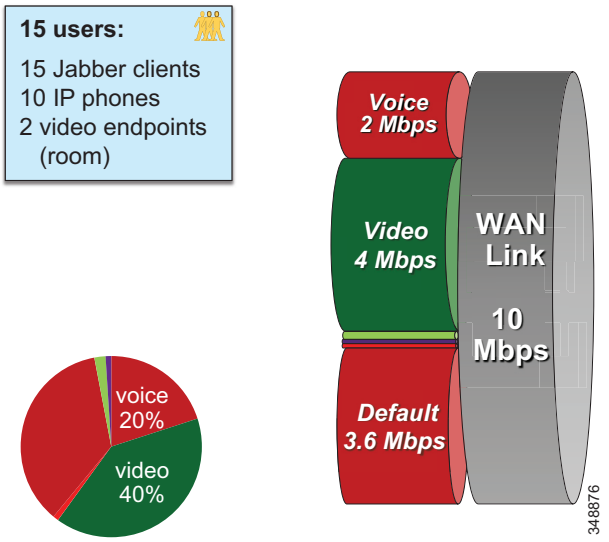


小規模支店リンク（10 Mbps）帯域幅の計算

図 13-98 で示すように、小規模支店サイトには次の帯域幅要件があります。

- 音声キュー（PQ）：2 Mbps（L3 帯域幅）
  G.711/G.722 で 25 コール
- 音声プール用の Unified CM ロケーション リンク帯域幅：
  25 * 80 kbps = 2 Mbps
- ビデオ キュー：18.7 Mbps（L3 帯域幅）
  - ビデオ エンドポイント：1.2 Mbps * 2 コール = 2.4 Mbps
  - 4 Mbps – 2.4 Mbps = 1.6 Mbps（Jabber メディア用）
    576p で 2 Jabber ビデオ コール、または 288p で 5
    （さらに残りの帯域幅）

図 13-98　小規模支店

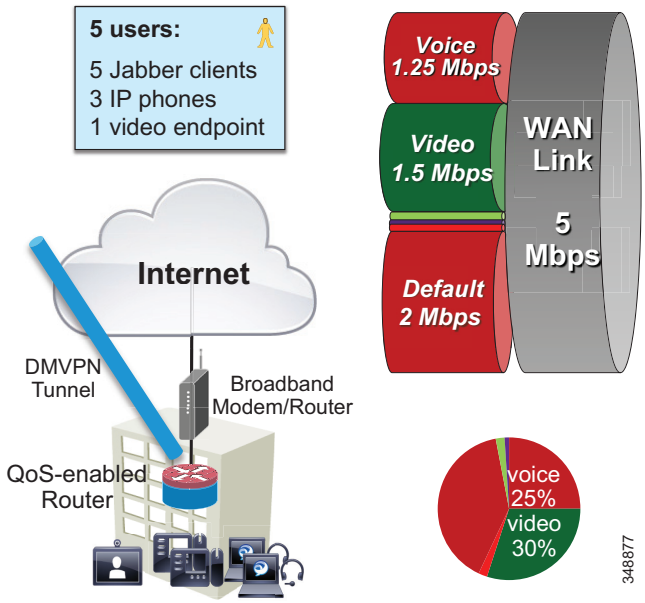


営業所ブロードバンド インターネット接続（5 Mbps）帯域幅の計算

図 13-99 で示すように、営業所サイトには次の帯域幅要件があります。

- ブロードバンド インターネット接続 + 中央サイトへの DMVPN
- ブロードバンド アップリンク速度に対応するように VPN ルータのインターフェイスを設定する
- TCP フローの bufferbloat を回避するために VPN ルータで QoS を有効にする
- 非対称ダウンロード/アップロードのブロードバンド: ビデオ エンドポイントでのビットレートの制限を検討する

図 13-99　営業所



制限付き WAN リンクを使用する大規模支店（ビデオに対応する Enhanced Locations CAC）

低速 WAN リンクを持つ特定の支店サイトでは、ビデオ キューのオーバープロビジョニングは実現不可能です（図 13-100 を参照）。ELCAC は、ビデオ コールがリンク帯域幅をオーバーサブスクライブしないように、ビデオのこれらのロケーション リンクに適用できます。このテンプレートでは、サイト固有のリージョン設定を使用して、ビデオ エンドポイントおよび Jabber クライアントで使用される最大帯域幅を制限する必要があります。また、Jabber ユーザがサイト間でローミングする場合には、デバイス モビリティも必要になることに注意してください。

（注）　音声専用コールとビデオ コールの両方のオーディオ帯域幅は音声 CAC プールから差し引かれるため、企業例 #1 の場合のように、キューの帯域幅調整は必要がありません。

図 13-100　制限付き WAN リンクを使用する大規模支店（ビデオに対応する Enhanced Locations CAC）

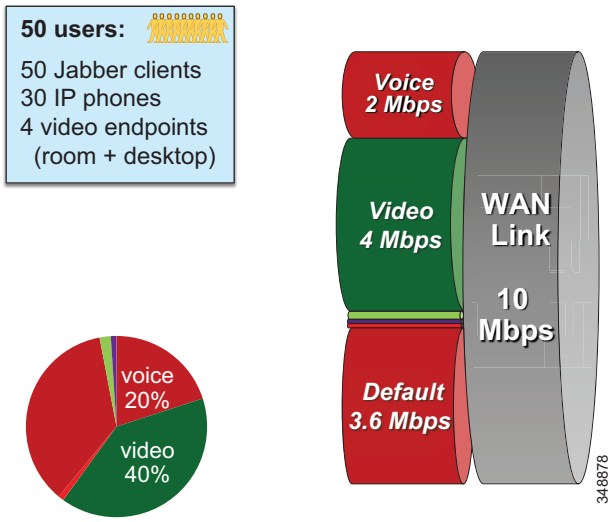


図 13-100 の説明のとおり、制限付き WAN リンク（10 Mbps）の大規模支店サイトには次の帯域幅要件があります。

- 音声キュー（PQ）：2 Mbps（L3 帯域幅）

  G.711/G.722 で 25 コール
- 音声プール用の Unified CM ロケーション リンク帯域幅：

  25 * 80 kbps = 2 Mbps
- ビデオ キュー：4 Mbps（L3 帯域幅）
  - 有効な使用方法：576p（768 kbps）で 2 コール + 288p（320 kbps）で 5 コール = 3,136 kbps
  - ビデオ コールの Unified CM ロケーション リンク帯域幅：3.2 Mbps（L3 帯域幅）
  - L2 オーバーヘッド、バースト性、AF41 とマーキングされた Jabber オーディオ専用コールのために帯域幅を確保する

ダイヤル プラン

改訂日 : 2018 年 3 月 1 日

ダイヤル プランは、ユニファイド コミュニケーションおよびコラボレーション システムの重要な要素の 1 つであり、すべての呼処理エージェントにとって不可欠となる部分です。概説すると、ダイヤル プランは、コールをどのようにルーティングするかを呼処理エージェントに指示する役割を果たします。具体的には、ダイヤル プランは次の機能を実行します。

- エンドポイントのアドレッシング

  呼処理エージェントに登録された宛先に、到達可能性を実現するためにアドレスが割り当てられます。これらの内部の宛先には、すべてのエンドポイント（IP Phone、ビデオ エンドポイント、ソフト クライアント、アナログ エンドポイントなど）とアプリケーション（ボイスメール システム、自動転送、会議システムなど）が含まれます。

- パスの選択

  発信元デバイスとダイヤルされた宛先に応じて、ダイヤルされた宛先へのパスが選択されます。セカンダリ パスを使用できる場合、このパスもプライマリ パスに障害が発生したときに検討対象になります。

- コール特権

  特定の宛先へのアクセスを許可または拒否することによって、複数のデバイス グループにそれぞれ別のサービス クラスを割り当てることができます。たとえば、ロビーにある電話からはシステム内部および市内の PSTN 宛先にしか到達できないようにし、その一方で、幹部社員の電話からは無制限に PSTN アクセスできるようにします。

- ダイヤルされた宛先の操作

  ダイヤルしているデバイスからダイヤルされた宛先へのパスで、ダイヤル プランはダイヤルされた宛先に操作を適用できます。たとえば、ドイツの PSTN の宛先に到達するために、米国のユーザは 9011496901234 をダイヤルしますが、一方でフランスのユーザは 000496901234 をダイヤルすることで同じ宛先に到達することができる場合があります。このダイヤルされる宛先は、米国のゲートウェイの PSTN トランクには 011496901234 として示され、フランスにあるゲートウェイの PSTN トランクには 00496901234 として示される必要があります。

- コールに関連する ID 情報の表示

  セッションの確立中とコール中に、発信側および着信側デバイスで、他のデバイスに関する情報が表示されます。コールの状態および方向に応じて、発信元、転送元、アラート側、接続先の情報が含まれます。ダイヤル プランで、表示される情報の形式と内容に影響するマッピングを定義できます。

この章では、システム設計者が、連絡先からのダイヤル、コンピュータやスマート フォンからのクリックツーコール アクション、モビリティ関連機能の採用などの、コンピューティング テクノロジーとテレフォニーがより緊密に統合された新機能を利用しつつ、テレフォニーおよびビデオ ユーザの従来のダイヤリング手順に対応するダイヤル プランを設計するために役立つ情報を示します。この章では、次の主要な領域に関する情報を示します。

- ダイヤル プランの基本（14-3 ページ）

  ここでは、企業向け音声およびビデオ ダイヤル プランでよく使用される一般的な概念について説明します。

- ダイヤル プランの要素（14-14 ページ）

  ここでは、Cisco Unified Communications Manager（Cisco Unified CM）と Cisco TelePresence Video Communication Server（VCS）を含む企業向けコラボレーション ソリューションのアーキテクチャ要素で使用できる各ダイヤル プラン要素を説明します。

- 推奨される設計（14-60 ページ）

  ここでは、マルチ サイト コラボレーション ネットワーク、エンドポイントのアドレッシング、サービス クラスの構築に関連する設計ガイドラインを説明します。また、Unified CM と VCS のダイヤル プランの統合についても説明します。

- 特記事項（14-84 ページ）

詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』、『*Feature Configuration Guide for Cisco Unified Communications Manager*』、『Cisco IOS Voice and Video Configuration ガイド』、次の URL から利用できるその他の製品マニュアルを参照してください。

https://www.cisco.com

この章の変更点

表 14-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 14-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
1 つのルート フィルタをあまりに多くのルート パターンに割り当てないでください。	ルート フィルタ（14-28 ページ）	2018 年 3 月 1 日
コーリング サーチ スペースの最大長	コーリング サーチ スペース（14-46 ページ）	2018 年 3 月 1 日
SIP ルート ヘッダー	Unified CM での SIP 要求のルーティング（14-52 ページ）	2018 年 3 月 1 日

ダイヤル プランの基本

エンドツーエンドの企業のダイヤル プランの開発には、特定の製品に依存しないいくつかの概念の確実な知識が必要です。ここでは、次のような、これらの概念の概要を提供します。

エンドポイントのアドレッシング

呼処理エージェントに登録されているエンドポイント、ユーザ、およびアプリケーションの到達可能性は、アドレス指定可能なエンティティに割り当てられたアドレスによって提供されます。エンタープライズ コラボレーション ネットワークで、数値アドレスと英数字の Uniform Resource Identifier（URI）は区別されます。

数値アドレス（番号）

数値アドレスは一連の数字で表されます。呼制御エージェントでは、数値アドレスに対して、特殊な構造を前提としたり、排除したりせず、必須のものでもありません。ダイヤル プランで使用される数値アドレス構造の決定は、ダイヤル プランの設計プロセスの一部です。

ITU 勧告 E.164 は、図 14-1 に示すように、PSTN で使用される数値の地理的アドレス（電話番号）の基本構造を定義します。

図 14-1　　地理的な番号の E.164 形式

<table>
<tr><td rowspan="2">1 ～ 3 桁</td><td colspan="2">最大 15-n 桁（n = CC の桁）</td></tr>
<tr><td>国内番号計画によって定義</td><td>国内番号計画によって定義</td></tr>
<tr><td colspan="3">最大 15 桁</td></tr>
</table>

図 14-1 には、次の定義が適用されます。

- CC = 国番号
- NSN = 国内の最上位番号
- NDC = 国内の宛先コード
- SN = 加入者番号

ITU 勧告 E.164 に従って、電話番号の最大長は 15 桁です。地理的な E.164 番号の最初の部分は、国番号です。国番号の長さは、1 ～ 3 桁です（1 桁の国番号は、国番号 1 および 7 だけです）。地理的な E.164 番号の残りの部分は、国内の最上位番号（NSN）です。NSN の一般的な構造は、最初の数桁が国内の宛先コード（NDC）またはエリア コードを表し、最後の数桁が加入者番号を表します。ITU 勧告 E.164 は国内番号計画を定義しないため、特定の国で NSN に使用するスキーマを規定していません。これは、国内番号計画の機関に任されます。次の URL で、さまざまな国別番号計画のドキュメントを入手できます。

https://www.itu.int/oth/T0202.aspx?parent=T0202

国内番号計画の構造は大きく異なる場合があります。例として、表 14-2 で、米国とドイツで使用される番号計画を比較します。

表 14-2　米国とドイツの番号計画の比較

国コード（Country Code）	NSN 長	NDC 長	SN 長
1（米国）	10	3	7
49（ドイツ）	3 ～ 13	2 ～ 5	4 ～ 11（エリア コードによって異なる）

ITU 勧告 E.164 には、国際プレフィックスが必要な場合、それを示すために先頭に「+」を使用する必要があることも記載されています。この設計ガイドでは、一貫して、「E.164」は E.164 番号を表し、「+E.164」は先頭に「+」が付いた E.164 番号を表します。

数値アドレスとして +E.164 番号を使用することには、これらの数値は本質的に一義的であり、企業のダイヤル プランでサポートする必要がある慣習的なダイヤリングと +E.164 のマッピングが非常に容易であるというメリットがあります。

一義的な数値の +E.164 アドレスを使用する代わりに、企業の番号計画に従って数値アドレスを使用することもできます。複数サイトの展開で企業アドレス計画または番号方式を確立するには、次の特性で一般的な階層型アドレス構造を定義します。

- 企業内のすべてのエンドポイント、ユーザ、アプリケーションに一義的な数値アドレスを提供します。
- 番号付け方式は、既存のエンドポイント、ユーザ、アプリケーションのアドレスの再割り当てなど、番号付け方式全体を再設計することなく新しいサイトを追加できるように拡張可能であることが必要です。

一般的な企業の番号計画では、数値アドレスはサイト コードとサイトの加入者番号で構成されます。企業の番号計画を設計するとき、サイトを必要に応じて追加でき、十分な加入者番号をサイトごとに定義できるようにするために、サイト コードとサイトの加入者番号の両方に十分な桁数を予約します。企業の番号計画は、通常は固定長で設計します。

企業の番号計画によって定義されるアドレスのダイヤリングをダイヤリング手順として直接サポートする必要がある場合、通常、1 桁のアクセス コードが選択され、会社の番号に前に付けられます。この場合、完全な会社の番号アドレスは、企業のアドレス アクセス コード（例：8）、サイト コード（例：496）、サイトの加入者番号（例：9123）の 3 つの部分で構成されます。この例では、8-496-9123 になります。

この場合、企業のアドレス アクセス コードは、他のダイヤリング手順とオーバーラップしないように選択する必要があります（ダイヤリング手順（14-6 ページ）を参照してください）。

アドレス指定可能なエンティティを一義的に識別できるように、すべてのアドレスが一義的か、少なくとも呼処理エージェントが管理する定義済みサブ ドメイン内で一義的でなければなりません。同じアドレスを使用して 2 つの独立したエンティティをアドレス指定する必要がある場合、2 つの同一のアドレスは、個別に管理される分離したアドレッシング ドメインに存在しなければなりません。数値アドレスの場合、この状況はサイトの最上位数値アドレス（たとえば、4 桁の内線番号）を使用し、異なるサイトにあって同じサイトの最上位アドレス（同じ 4 桁の内線番号）を使用する 2 個のエンドポイントに、同じ呼制御エージェントでアドレス指定する必要がある場合に発生する可能性があります。表 14-3 に、この状況の例を示します。

表 14-3　　オーバーラップする数値アドレッシング

[+E.164番号（Advertised Failover Number）]	サイト（サブドメイン）	サイトの DID 範囲	4 桁の DN（アドレス）
+49 690 773 3001	Frankfurt	+49 690 773 3XXX	3001
+1 408 555 3001	San Francisco	+1 408 555 3XXX	3001

表 14-3 で、2 つの E.164 番号が、それぞれのサイトの DID 範囲に基づいて、同じサイト固有の 4 桁のディレクトリ番号になります。これは、4 桁の DN を数値エンドポイント アドレスとして直接使用できないことを意味します。

企業の番号計画に従うアドレスは、Enterprise Significant Number（ESN）とも呼ばれ、PSTN 番号（E.164 番号）が存在しない宛先にアドレスを指定するために使用できます。これらの宛先には、次のものが含まれます。

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

英数字のアドレス

SIP URI に基づく英数字のアドレスも、エンドポイント、ユーザ、アプリケーションのアドレス指定に使用できます。英数字のアドレスに広く使用されている方式は、*ユーザ@ホスト*という簡略化された SIP URI で、左側（LHS、ユーザ部分）は英数字、右側（RHS、ホスト部分）はドメイン名です。次の例で、SIP URI に基づく有効な英数字のアドレスを示します。

- bob@example.org
- bob.home-office@example.org
- bob@de.eu.example.org
- bob.ex60@example.org
- bob.vmbox@example.org
- voicemail@de.eu.example.org

これらの URI はすべて、個々のエンドポイント、ユーザ、アプリケーションに対する個々の英数字のアドレスとして使用できます。アドレッシングの観点から見て、ドットで区切られた ID（bob.ex60、de.eu.example.org）の使用によって意味される階層が、任意の 2 つの URI が同等であると見なされるかどうかに影響を与えることはありません。

RFC 3261 に準拠して、SIP URI の LHS の比較は大文字と小文字を区別し、RHS は大文字と小文字を区別しないで比較しなければなりません。この標準化された動作に従い、Alice@example.com と alice@example.com は同等とは見なされず、その結果、別のアドレスを示します。実際には、ユーザ部分の大文字と小文字の区別に依存するエンドポイント、ユーザ、アプリケーションのアドレッシング方式を使用することは、トラブルシューティングが複雑になるため、望ましくないとされています。また、RFC 2543（RFC 3261 に先行する RFC 仕様）では、SIP URI（ホストおよびユーザ部分）は大文字と小文字を区別しないと明示的に定義されていることに注意してください。URI の等価性における大文字と小文字の区別に関して動作が異なることはよくあります。問題を回避するために、英数字のアドレスとしてすべて小文字の URI を常に使用することを推奨します。

Unified CM の URI ルックアップ ポリシーは、必要に応じてエンタープライズ パラメータ [URI ルックアップ ポリシー（URI Lookup Policy）] を設定することで、大文字と小文字を区別するか（デフォルト）、区別しないかを設定することができます。

ダイヤリング手順

ユーザ、エンドポイント、アプリケーションなどの宛先へのダイヤリングは、さまざまな形式を使用して行うことができます。数値の +E.164 アドレス +496907739001 は、たとえば、次のいずれかとしてダイヤルできます。

- +496907739001
- 米国の内線から 9011496907739001
- 米国の固定電話から 011496907739001
- ドイツの内線から 006907739001
- イタリアの内線から 000496907739001
- 同じオフィスの電話から 9001

これらの例は、ダイヤル文字列は通常、コンテキストで解釈されることを示しています。+E.164 アドレスを直接ダイヤルする場合を除き、ダイヤルされた文字列とコンテキストの組み合わせだけが適切な ID を目的の宛先アドレスに提供します。

「ダイヤリング手順」は、通常、特定の宛先のセットに到達するために使用される特定のダイヤリング動作を示します。いくつかの「ダイヤリング手順」の例を示します。

- 米国内から海外の宛先へのダイヤルは、9-0-1-1 に加え E.164
- ドイツの国内通話は、0-0 に加え NSN
- 米国の国内通話は、9-1 に加え 10 桁
- オフィスのサイト内コールは、4 桁

ダイヤリング手順は、ダイヤルされる文字列の形式（ダイヤリング構造）と、到達する宛先アドレス クラスの両方を指定することで説明されます。通常、企業のダイヤル プランで使用される宛先アドレス クラスの例は次のとおりです。

- オンネット/サイト内
- オンネット/サイト間
- オフネット/市内
- オフネット/国内
- オフネット/国際
- オフネット/緊急
- サービス（ボイス メール、ピックアップなど）

ダイヤル プランでサポートする必要があるダイヤリング手順を特定することは、企業ダイヤル プランの設計を開始する際の最初の手順の 1 つです。特定の発信者にサポートされる 2 つのダイヤリング手順間で重複が生じないようにダイヤリング手順を定義する必要があるため、サポートするすべてのダイヤリング手順の全体を把握してダイヤル プラン設計を開始することが不可欠です。これを守らない場合、呼制御において、番号が 1 つずつダイヤルされたときにその番号を分析することにより重複するダイヤリング手順を確定的に区別することができないため、ユーザ エクスペリエンスが損なわれます。これは最終的に、桁間タイムアウトにつながります。

英数字のダイヤリングでは、通常、完全修飾アドレスと非完全修飾アドレスだけを区別します。完全修飾アドレスには SIP URI のユーザ部分とホスト部分が含まれます。一方、英数字の非完全修飾アドレスはアドレスのユーザ部分だけを表し、ホスト部分は発信側のダイヤリング コンテキストから取得する必要があります。たとえば、発信側のダイヤリング コンテキストで、すべての英数字の非完全修飾アドレスに「@example.com」を追加する必要があると定義されている場合、「bob」とダイヤリングすることは「bob@example.com」とダイヤリングすることと同等です。

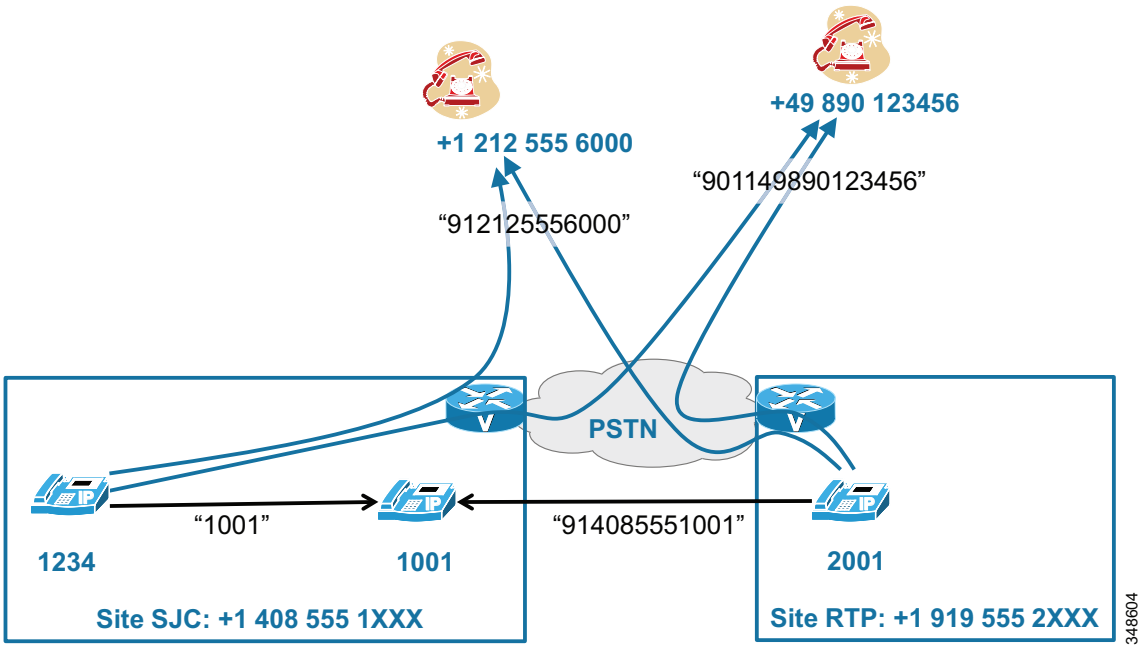
ダイヤル ドメイン

前のセクションで説明したように、ユーザごとに異なる文字列を使用して特定の宛先をダイヤリングできます。ダイヤル ドメインは、ダイヤリング手順の同じセットを共有する（同一の宛先に到達するために同じ文字列をダイヤリングする）ユーザまたはデバイスのグループを指定します。企業のダイヤル プランでは、各ダイヤル ドメインで同じ処理を実装しなければならないため、ダイヤル ドメインの概念が重要です。特定のダイヤル ドメインに属するすべてのユーザが同じダイヤリング処理を共有します。

ダイヤル ドメインを特定するには、すべてのダイヤリング手順を考慮することが重要です。米国の 2 つのサイトのユーザが、同じ PSTN ダイヤリング手順を共有する場合でも、オンネット コールの実行方法を考慮すると異なるダイヤル ドメインに属する場合もあります。通常の環境では、オンネットのサイト内コールは 4 桁のダイヤルによってサポートされ、オンネット サイト間コールは PSTN のダイヤリング手順に対応するダイヤル文字列を使用して実行されます（強制オンネットは、コールをオンネットのままにします）。

図 14-2 に、この例を示します。サイト SJC のエンドポイント 1234 とサイト RTP のエンドポイント 2001 では、国内の接続先（PSTN の接続先 +1 212 555 6000 に到達するために 91212555600 をダイヤル）と海外の接続先（PSTN の接続先 + +49 890 123456 に到達するために 901149890123456 をダイヤル）について同じダイヤリング手順を共有していますが、サイト SJC のエンドポイント 1001 に到達するダイヤリング手順は、RTP のエンドポイントと SJC のエンドポイントでは異なります。サイト SJC のエンドポイント 1234 では 1001 をダイヤルし、サイト RTP のエンドポイント 2001 では 914085551001 をダイヤルする必要があります。この例では、サイト RTP とサイト SJC のエンドポイントは異なるダイヤル ドメインに属します。

図 14-2　　ダイヤル ドメイン



サービス クラス

企業内のすべてのユーザ、アプリケーション、エンドポイントが同じ宛先のセットに到達できるわけではありません。到達可能な宛先のセットを制限する理由には、コストの回避、セキュリティ上の考慮事項、プライバシーなどがあります。たとえば、一部のユーザが国際通話を発信できない場合があります。ボイス メール システムは、電話料金の詐欺行為を防止するために、PSTN 宛先にコールできない場合があります。非常に限られたユーザだけが、会社の CEO に直接コールすることが許可される場合があります。許可される宛先の制限またはクラスのセットを示すためによく使用される用語が、*サービス クラス*、または CoS です。

コスト重視のサービス クラスの要件は、関連付けられた電話料金とコスト構造に大きく依存します。音声サービスが安価になる（または無料で使用できるようになる）に従い、より多くのサービス クラスの管理に関連する複雑さの増大と、削減可能なコールのコストの間のトレード オフは変化しています。たとえば、市内通話と国内通話の両方のコール タイプの料金が完全に同じになり、区別する意味がなくなる場合があります。

サービス クラスの定義は、時間のスケジュールに基づく場合もあります。特定の宛先へのアクセスが、特定の時間にのみ許可される場合があります。

企業ダイヤル プランの複雑さを軽減するために、区別されるサービス クラスの数を最小限にすることを推奨します。これは、有用性が低い、または有用性がないサービス クラスを削除するか（国内通話が原則無料にもかかわらず「国内」と「市内」のサービス クラスが区別されているなど）、（ほとんど）同等のサービス クラスを単一のサービス クラスに結合させることで実現できます。

通常、コストが発生する特定のユーザ、デバイス、アプリケーションによる特定のコール タイプへのアクセスとは別に、緊急サービス（911、112 など）へのアクセスは常にすべてのユーザに提供されなければなりません。したがって、すべてのサービス クラスで緊急サービスへのアクセスを常に可能にしなければなりません。

コール ルーティング

コールのルーティングには複数の側面があります。

- ダイヤル文字列の構造に基づいてダイヤリング手順を特定します。
- 発信エンティティのサービス クラスに基づいてコールを許可/ブロックします。
- ダイヤル文字列に変更を適用します。
- 発信者 ID に変更を適用します。
- 着信先へのルートを選択し、コールを確立し、期待される形式で関連する ID を示します。ルート選択には、何らかの理由でプライマリ ルートが使用可能でない場合の、代替ルートの選択が含まれます。

エンドツーエンドの企業ダイヤル プランでは、これらの側面をすべて考慮する必要があり、発信側と着信側のエンティティ間でルートを確立することだけに限定されません。

ダイヤリング手順の特定と、オーバーラップの回避

発信エンティティからの入力を受信した後、コール ルーティング プロセスの最初の手順は、使用されるダイヤリング手順を一義的に特定することです。英数字のダイヤリングの場合、完全修飾 SIP URI と非完全修飾 SIP URI を区別するだけなので、これは通常、小さなタスクです。ダイヤルされた文字列の単純な文字分析によって容易に実現できます。

番号のダイヤリングの場合、特にダイヤルされる番号が 1 桁ずつ入力される場合は、少し注意が必要です。この場合、呼制御は発信エンティティから桁単位で宛先を受信し、十分な桁数を受信したときに、宛先への正しいルートを選択する部分を正確なタイミングで決定し、桁間のタイムアウトが発生するまで待たずにコールをルーティングする必要があります。

図 14-3 に、PSTN および緊急通話用の一般的な米国でのダイヤリング手順を示します。これらのダイヤリング手順のすべてで同一の先頭数字 9 を共有しますが、国際ダイヤリングと最初の緊急ダイヤリング文字列は、2 桁目（0 または 9）がダイヤルされるとすぐに、容易に区別できます。北米番号計画（NANP）では 1 で始まる NPA コード（番号計画エリア コード）が許可されていないため、3 番目の数字がダイヤルされるとすぐに、911 のダイヤリングと国内の宛先へのダイヤリングはオーバーラップしなくなります。

図 14-3　　PSTN および緊急通話用の一般的な米国のダイヤリング手順

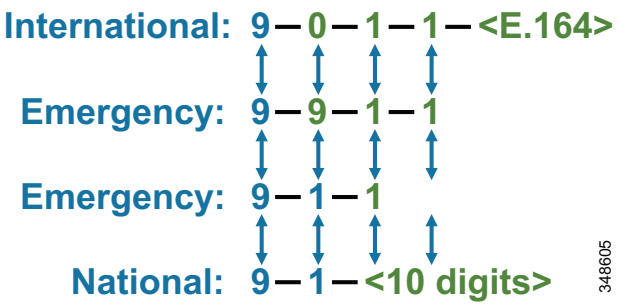


図 14-3 の PSTN ダイヤリング手順を考慮すると、9 で始まる内線への 4 桁のサイト内ダイヤリングは部分的にオーバーラップする可能性があるため、回避する必要があります。たとえば、内線番号 9113 は緊急通話とオーバーラップし、呼制御は 911 を受信した後、発信者が 3 をダイヤルするか（内線 9113）、ダイヤリングが 911 で完了したかを判断しなければなりません。これは、すべての緊急通話を遅らせます。同様に、9140 などの内線は国内の PSTN コールとオーバーラップし、これらの内線番号へのコールが遅れます。

オーバーラップを最小限に抑えるには、ダイヤリング手順の 1 桁目は宛先クラスを一義的に識別するアクセス コードとして定義します。PSTN またはトランク アクセス コードはこの方式の最適な例です。最も一般的なトランク アクセス コードは 9（米国、英国など）および 0（欧州諸国のほとんどで一般的に使用）です。

前述のように、オーバーラップしないダイヤリング手順を選択することは桁間タイムアウトによるユーザ エクスペリエンスの低下を回避する鍵です。企業のダイヤル プランでよく見られるオーバーラップには、次のものがあります。

- 10 桁のダイヤリングと短縮サイト内ダイヤリング（たとえば、4 桁）

  米国の NPA コードは 0 または 1 以外のあらゆる数字で始まる可能性があります。これは、10 桁のダイヤリングの最初の数桁が、ほとんどすべての短縮サイト内ダイヤリングとオーバーラップすることを意味します。

- PSTN アクセス コード（米国の 9 など）と短縮サイト内ダイヤリング

  PSTN アクセス コード 9 は、9 で始まる内線へのすべての短縮サイト内ダイヤリングとオーバーラップします。

- 短縮オンネット サイト間ダイヤリングと短縮サイト内ダイヤリング

  企業の短縮オンネット番号計画用に選択されたアクセス コードが、同じ数字で始まるサイト間ダイヤリングの範囲とオーバーラップする可能性があります。たとえば、短縮オンネット サイト内ダイヤリングにアクセス コード 8 を使用した場合、8 で始まる短縮サイト内ダイヤリングを使用できなくなります。

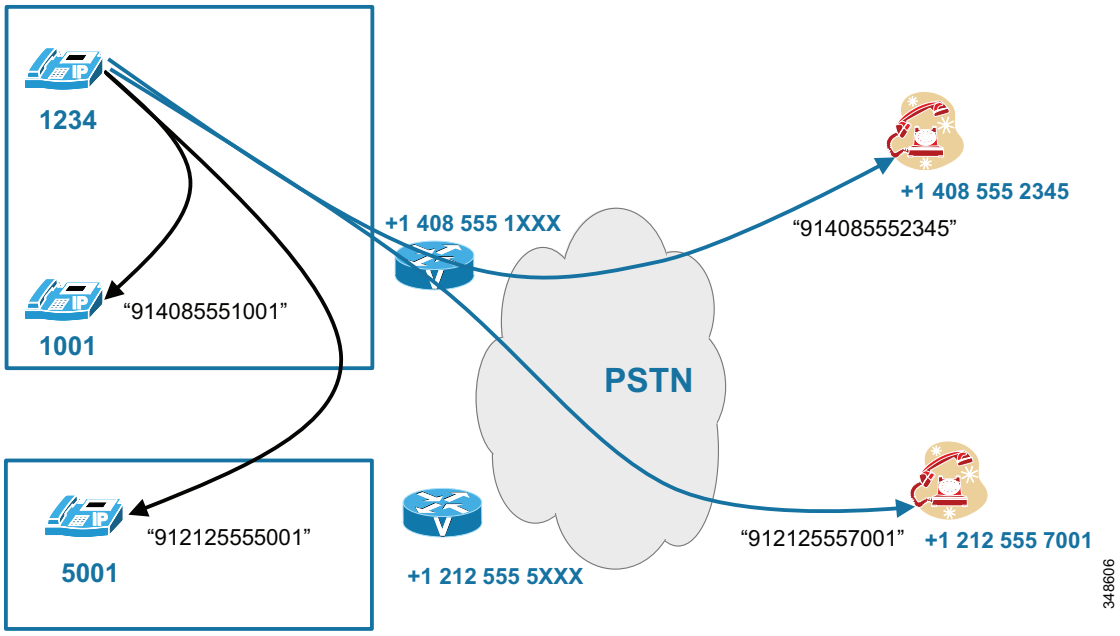
コール パーク番号やボイス メールなどの機能へのアクセスも、定義されたダイヤリング手順のセットにマッピングする必要があります。これらの機能へのダイヤリングは、通常、短縮ダイヤル手順だけを必要とします。これを実現するには、機能アクセス コードを短縮サイト内ダイヤリングにマップするか、専用の機能アクセス コードを定義する必要があります。

強制オンネット ルーティング

オンネット/サイト間の宛先とオフネットの宛先へのダイヤリング手順で、同じダイヤリング構造を使用することは珍しくありません。この場合、呼制御が、アドレス指定されたエンドポイント、ユーザ、アプリケーションがオンネットかオフネットかをダイヤルされたアドレスに基づいて決定し、コールをそれぞれオンネットまたはオフネットとして扱います。

図 14-4 に、強制されたオンネット ルーティングの例を示します。この例の 4 つのコールは、91 プラス 10 桁としてダイヤルされます。ただし、+ 1 408 555 2345 と + 1 212 555 7000 へのコールは、実際にはオフネット コールとして PSTN ゲートウェイを介してルーティングされますが、他の 2 つのコールは呼制御がオンネット宛先として最終的な宛先を識別するため、オンネット コールとしてルーティングされます。強制オンネット ルーティングは、特定の宛先のダイヤルに使用されるダイヤリング手順が必ずしもコールのルーティング方法を決定するわけではないことも明確に示します。この例で、使用された PSTN ダイヤリング手順でオフネットの宛先が呼び出されることが示されている場合でも、一部のコールはオンネット コールとしてルーティングされます。

図 14-4　　強制オンネット ルーティング



強制オンネット ルーティングは、ディレクトリからの +E.164 宛先のダイヤリングが実装されている場合に、特に重要です。正規化されたディレクトリでは、番号に関連付けられているユーザが内部か外部かに関係なく、すべての宛先が +E.164 番号として定義されます。この場合、強制オンネット ルーティングは、PSTN を通じて内部コールをルーティングすることで発生する料金を回避するために必須です。

1 つの呼制御のコール ルーティング

すべてのエンドポイントが単一の呼制御に登録された場合、この呼制御がすべての既知のオンネット宛先を完全に認識できます。定義されたダイヤリング手順のいずれかを使用してユーザ、エンドポイント、またはアプリケーションが宛先をダイヤルしたときに、呼制御はダイヤルされた宛先がオンネットかオフネットかを容易に判断できます。これは、使用されたダイヤリング手順またはダイヤルされた正規化アドレスに基づきます（強制オンネット ルーティング（14-10 ページ）を参照してください）。

ダイヤルされた宛先が外部だと判断されると、呼制御は、コールをセット アップするために正しい外部ルートを選択する必要があります。1 台の外部（PSTN）接続だけがある場合、これは簡単に決定できます。複数の外部接続がある場合は、次の要因を任意に組み合わせて出力ルートを選択できます。

- コールの発信側
- ダイヤルされた宛先
- リソースの可用性
- リソースの優先順位

ダイヤルされた宛先に基づいて外部接続を選べるように、ダイヤルされる宛先を分類する必要があります。前述したとおり、E.164 番号は番号が地理的な関係を意味する階層構造になっていて、出力接続の選択が宛先に（E.164 番号の地理的な意味で）「最も近い」出力ポイントを選択するプレフィックス ベースの階層型ルーティング スキームに基づきます。この動作はテールエンド ホップオフ（TEHO）と呼ばれます。テールエンド ホップオフを実装するときは、地域の規制を考慮しなければなりません。

市内電話（州内）より国内通話（州間など）のほうが低価格になる変わった通話料金では、TEHO の特別なケースが発生します。この場合は、ダイヤルされた宛先に「近すぎる」出力接続を実際には選択しないように、出力ポイント選択ポリシーを実装する必要が生じる場合があります。電話料金が下がれば、このようなルーティング スキームの有効性は低下します。

左側の英数字に最も重要な情報がある、明確に階層化された地理的な構造を持つ E.164 番号とは対照的に、SIP URI では、URI のホスト部分（RHS）でアドレスを階層化できます。RHS として使用されるドメイン名によっては、URI のアドレス階層は、特に user@example.org などのフラットな URI スキームが使用されている場合、必ずしもルーティング トポロジのロケーションに対して URI の地理的なマッピングが許可されるわけではありません。より興味深い点として、SIP URI の最も重要な要素は、ホスト部分の右端のデータです（トップ レベル ドメイン）。

複数の呼制御のコール ルーティング

大規模な企業ネットワークでは、多数の呼制御が導入されている場合があります。これらの独立した呼制御は、トランクを使用して相互に接続されます。可能なトポロジには、ハブ アンド スポーク、フル メッシュ、およびこれらの組み合わせがあります。これらの呼制御のいずれかが個別に、エンドポイント、ローカルに登録されたアプリケーション、または内部および外部トランクによって提供されたコールをルーティングします。

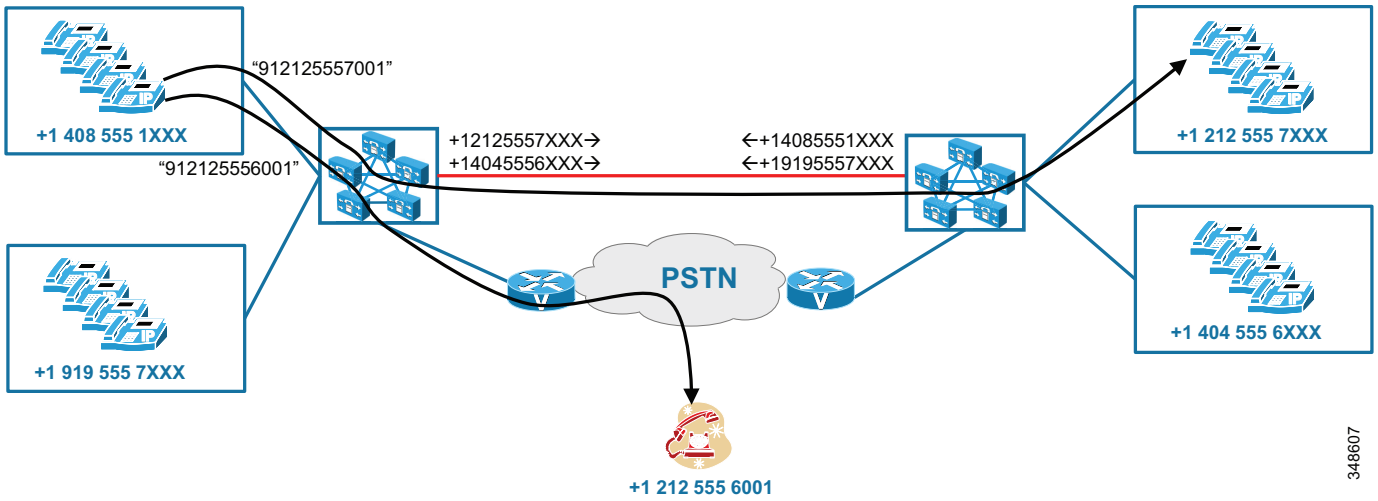
このような環境では、前の項で説明したオンネット/オフネットの決定が少し複雑になります。コールを外部接続にルーティングする前に、各呼制御が、ダイヤルされた宛先がほんとうにオフネットであることを確認する必要があります。しかし、ローカルに登録されたアドレスだけを確認しても、呼制御は、実際には信頼性の高いローカル/リモートの決定ができるだけで、リモート（ローカルに登録されていない）として分類された宛先がオンネットであり、導入されている他のエンタープライズ呼制御のいずれかでホストされている可能性があります。

個々の呼制御に数値アドレスを設定し、エンドポイントを厳密に地理的に割り当てて、特定の呼制御で正しい内部または外部接続を選択するには、E.164 プレフィックスに基づくルーティング方式を実装する必要があります。これは基本的に、プレフィックス ベースのルーティングに使用する接続の一部が外部接続（たとえば、PSTN への接続）ではなく、企業の他の呼制御エンティティへの内部接続であるという点を除いて、単一の呼制御の例で説明したコール ルーティング プロセスと同じです。リモート オンネットの宛先へのコールだけがリモート呼制御にルーティングされるようにするために、リモート呼制御に対してローカルな特定のアドレス範囲に基づき、コール ルーティングを決定する必要があります。

図 14-5 に、独立した呼制御間のプレフィックス ベースのルーティングをごく限定的にする必要がある理由を示します。この例では、左側の呼制御が 912125556001 をオンネット コールとして処理する必要があるかどうかを判断できるようにするために、左側の呼制御が、右側の呼制御エンティティによって提供されたすべての数値アドレスに対して特別な数字プレフィックス ルートを持っていなければなりません。

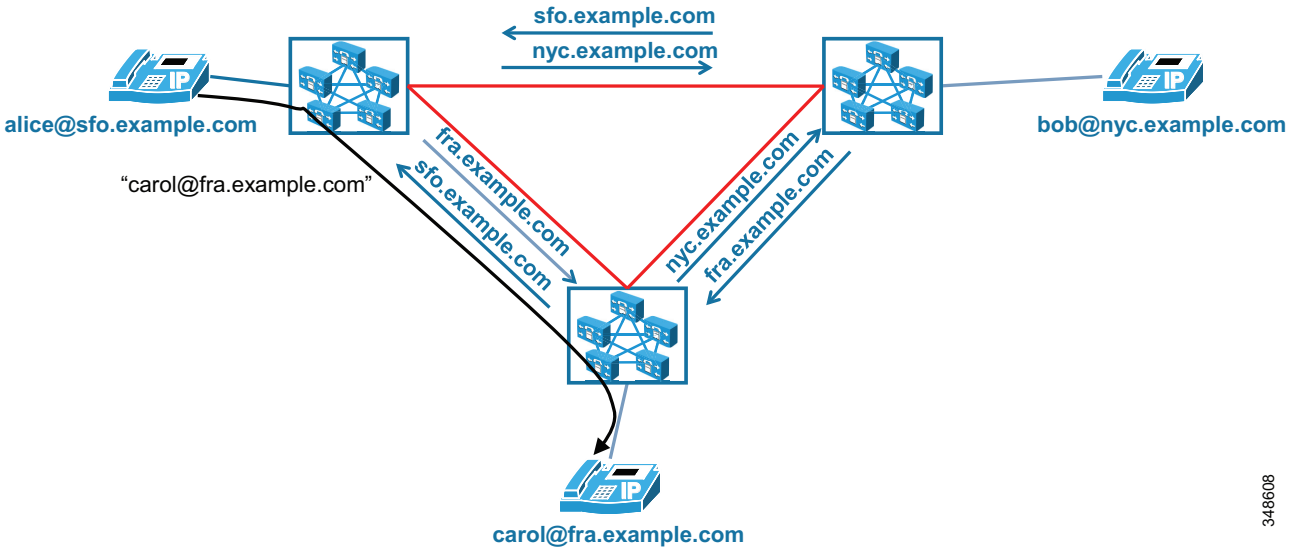
各呼制御でプロビジョニングされたオンネット プレフィックス ルートのメンテナンスは、関係する呼制御数や、考慮すべきサイト数と DID 範囲の増加により、より複雑になりました。リモート宛先のダイナミック学習は、この複雑さを解消するのに役立ちます。グローバル ダイヤル プラン レプリケーション（GDPR）は、呼制御がリモート呼制御に存在する宛先を自動的に学習できるようにするアーキテクチャの 1 例です。

図 14-5　　呼制御間のプレフィックス ベースのルーティング



英数字 URI の数値アドレス プレフィックス ベース ルーティングは、ドメインの階層を使用して、URI のホストまたはドメイン部分に基づいてルーティングを実行することと同じです。図 14-6 に、アルファベット URI を使用する階層型ルーティングの例を示します。この例では、階層的なドメイン構造に基づいてオンネット ルーティングを容易に実装できるように、3 個の独立した呼制御がすべて専用（サブ）ドメインを使用します。

図 14-6　　アルファベット URI の階層型ルーティング



URI のアドレッシング方式が非階層の場合、各呼制御はリモート呼制御でホストされているすべての URI を認識する必要があります。グローバル ダイヤル プラン レプリケーション（GDPR）は、フラットな URI の命名方式でも確定的なルーティングを可能にするために、各呼制御でホストされている URI に関する情報を交換するために呼制御のためのメカニズムを提供します。

ダイヤル プランの要素

ここでは、次のソリューション コンポーネントで使用可能なダイヤル プラン要素について説明します。

Cisco Unified Communications Manager

Cisco Unified Communications Manager（Unified CM）に含まれている次のダイヤル プラン要素について、設計と設定のガイドラインを示します。

IP Phone でのユーザ インターフェイス

（注）　さまざまな種類の IP 電話で、キーパッド入力が使用でき、視覚的な情報をさまざまな方法で提供します。この章では説明のため、次のタイプの電話機を定義します。

- **タイプ A 電話機**：Cisco Unified IP Phone 7905、7912、7940、および 7960
- **タイプ B 電話機**：Cisco Unified IP Phone 6901、6911、6921、6941、6945、6961、7906、7911、7921、7925、7931、7941、7942、7945、7961、7962、7965、7970、7971、7975、8961、9951、9971、およびそれ以降の新しい電話

IP Phone での発信側トランスフォーメーション

発信側トランスフォーメーション パターンによって、システムは発信者番号をさまざまな形式に適応させることができます。最も一般的な用途は、グローバル化された発信者番号からローカル化された番号に適応させること、およびその逆です。

トランスフォーメーション パターンは、照合される発番号の数値表現で構成されます。使用される構文は、ルート パターン、着信側トランスフォーメーション パターン、ディレクトリ番号などのその他パターンの構文と同じです

トランスフォーメーション パターンの変換演算子には、数字破棄命令（ドット前の番号など）、発信側トランスフォーメーション マスク、プレフィックス番号、発信側の外線電話番号マスクを適用するオプションが含まれます。また、発信側のプレゼンテーション インジケータ（[デフォルト（Default）]、[許可（Allowed）]、または [制限（Restricted）]）を設定できます。

パーティションおよびコーリング サーチ スペースによって、どの発信側トランスフォーメーション パターンをどの電話機に適用するかどうかが制御されます。電話機では、デバイス プールの発信側トランスフォーメーション コーリング サーチ スペース（CSS）またはデバイス固有の発信側トランスフォーメーション CSS を優先順位の低い順に使用できます。

IP Phone では、発信側トランスフォーメーションを電話機から発信されたコールと電話機で終了したコール用に設定できます。

- 設定されたディレクトリ番号がグローバル化された番号（+E.164）形式ではない電話から発信されたコールの場合、着信コールの発信側トランスフォーメーション CSS を使用して適切なグローバリゼーションを定義できます。この CSS は [番号表示トランスフォーメーション（Number Presentation Transformation）] セクションの [電話の設定（Phone Configuration）] ページ、または [この電話からのコールの発信者 ID（Caller ID For Calls From This Phone）] の下の [デバイス プール設定（Device Pool Configuration）] ページにある [電話の設定（Phone Settings）] セクションにあります。
- 電話機で終了するコールについては、発信コールの発信側トランスフォーメーション CSS を使用して、発信者番号に適用するローカリゼーション方式を定義できます。この CSS は、[リモート番号（Remote Number）] の下の [番号表示トランスフォーメーション（Number Presentation Transformation）] セクションの [電話の設定（Phone Configuration）] ページ、または [発信側トランスフォーメーション CSS としてのデバイス モビリティ関連情報（Device Mobility Related Information as Calling Party Transformation CSS）] の下の [デバイス プール設定（Device Pool Configuration）] ページにあります。

電話機の場合、電話が鳴っている間に表示される番号が、発信またはリモート番号の発信側トランスフォーメーションの影響を受けます。

発信コールの発信側トランスフォーメーション CSS（ローカリゼーションやリモート番号の発信側トランスフォーメーション CSS とも呼ばれる）を使用して、リモート接続されている通話者情報をローカライズすることもできます。この機能を有効にするには、拡張サービス パラメータ [リモート番号にトランスフォーメーションを適用（Apply Transformations On Remote Number）] を有効にする必要があります。

ローカライズされた通話者情報を電話機に提供できることで、通話切換機能が呼び出された場合でも一貫したリモートの通話者情報を IP Phone に表示できます。

電話機での + ダイヤリングのサポート

タイプ A 電話機では、キーパッドを使用して + 記号をダイヤルすることはできません。タイプ B 電話機では、0 キー（Cisco Unified IP Phones 7921 および 7925）または * キー（他のすべての電話機モデル）のいずれかを押したままにして + 記号をダイヤルできます。Cisco Unified Personal Communicator エンドポイントでは、+ 記号はコンピュータのキーボードを使用して入力するか、エンドポイントのクリックツーダイヤル機能の使用時に入力文字列の一部として入力します。

タイプ A の電話機では、+ 記号のダイヤルはサポートされていません。+ 記号は、着信コールの発呼側情報としてディレクトリ内に表示できますが、エントリが不在着信のディレクトリからダイヤルされる場合、電話は + 記号を除去します。かけ間違いを回避するために、タイプ A の電話機は、不在着信ディレクトリに変換された番号を置き、コールバックも変換された番号を使用します。変換された番号は、ディレクトリからのかけ間違いを回避するため、ダイヤル プランによってサポートされるダイヤリング手順の形式にする必要があります。

一部のエンドポイントでは、着信コールで発信者番号を + を番号の一部に含めて表示することができます。コールが電話機に提供されたとき、呼び出し中の電話機に表示される番号は、設定された発信者番号トランスフォーメーション パターンによって処理されます。不在コールと受信コールのディレクトリは、元の変換前の番号と変換された番号の両方を保持できます。一部のエンドポイントでは、リストに表示される番号は変換された番号になり、変換前の番号はエントリの詳細を確認したときにだけ表示されます。ダイヤル プランが + ダイヤリングをサポートする限り、一部のエンドポイントのディレクトリからダイヤルされた番号は元の変換前の番号であり、発信者番号の一部として + 記号が使用された以前の受信コールをワンタッチでダイヤルできるようになります。他のエンドポイントでは、ディレクトリからダイヤルされる番号は変換された番号です。ワンタッチでのダイヤリングを許可するには、この番号をダイヤル プランでサポートされているダイヤリング手順の形式にする必要があります。

例 14-1　+ ダイヤリングを使用する発番号

New York にあるタイプ B 電話機が +1 408 526 4000 からのコールを受信します。発信側トランスフォーメーション パターンは、電話機のデバイス プールの発信側変換 CSS に配置されています。パターンの 1 つは \+1.!（ドットの前の番号を削除）と設定されています。

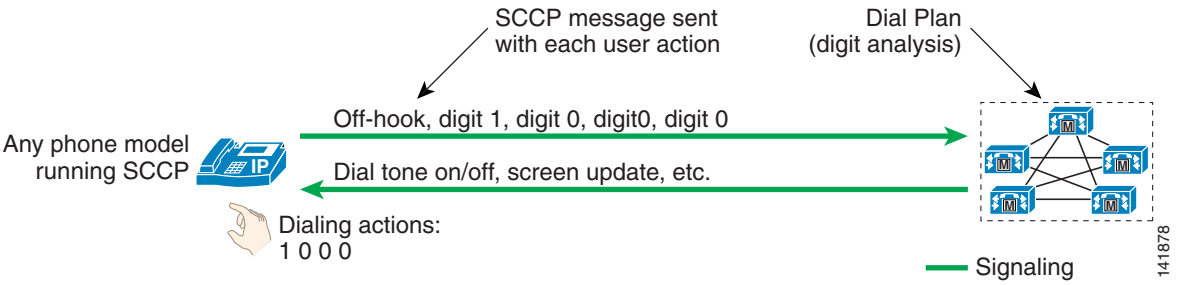
コールが鳴ると、着信側電話機に着番号 4085264000 が表示されます。コールに応答し、コールを解放した後、受信コール ディレクトリには最後のコールが 408 526 4000 として表示されますが、ユーザがディレクトリ エントリからコールバックを開始したときの着信番号は +1 408 526 4000 です。

SCCP 電話機でのユーザ入力

SCCP を使用する IP Phone は、すべてのユーザ入力イベントをただちに Unified CM に報告します。たとえば、ユーザがオフフックにするとすぐに、その電話機が登録されている Unified CM サーバに電話機からシグナリング メッセージが送信されます。電話機は 1 つの端末と考えることができ、設定されたダイヤル プランに従い、ユーザ入力に起因するすべての決定がその端末で Unified CM によって下されます。

その他のユーザ イベントが電話機で検出されると、そのイベントは個別に Unified CM にリレーされます。オフフックして 1000 をダイヤルしたユーザは、電話機から Unified CM に 5 つの独立したシグナリング イベントをトリガーすることになります。その結果としてユーザに提供されるフィードバック、たとえば画面メッセージ、ダイヤル トーンの再生、2 次ダイヤル トーン、リングバック、リオーダーなどは、Unified CM がダイヤル プラン設定に基づいて電話機へ発行するコマンドです（図 14-7 を参照）。

図 14-7　SCCP 電話機でのユーザ入力とフィードバック



SCCP を実行する IP Phone 上にダイヤル プラン情報を設定する必要はなく、また設定できません。ダイヤル プラン機能は、ユーザ入力が収集されたときのダイヤリング パターンの認識も含めて、すべて Unified CM クラスタに含まれています。

ユーザのダイヤルしたパターンが Unified CM に拒否された場合は、そのパターンが Unified CM の番号分析でベストマッチになるとすぐに、そのユーザに対してリオーダー トーンが再生されます。たとえば、1 分刻みで課金される番号計画エリア（または市外局番）976 へのコールがすべて拒否される場合は、ユーザが 91976 をダイヤルするとすぐに、そのユーザの電話機にリオーダー音が送信されます。

タイプ A の SIP 電話機でのユーザ入力

タイプ A 電話機はタイプ B 電話機と動作が少し異なり、タイプ B 電話機では Key Press Markup Language（KPML）がサポートされていますが、タイプ A 電話機ではサポートされません（タイプ B の SIP 電話機でのユーザ入力（14-19 ページ）を参照）。

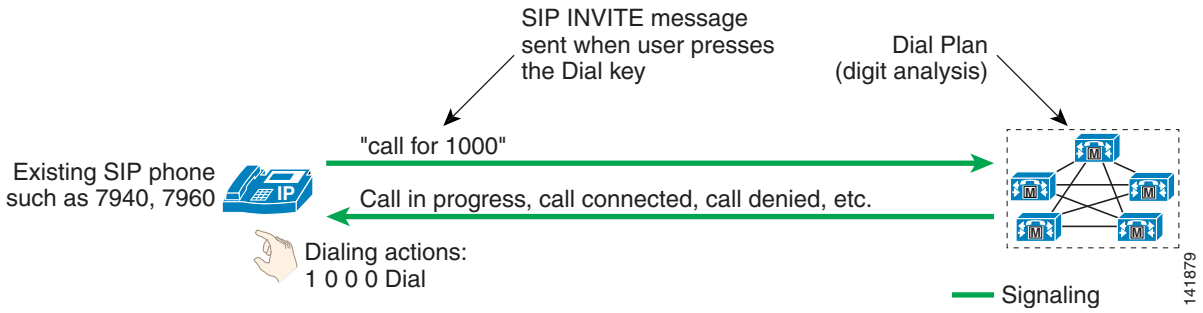
SIP を使用するタイプ A の IP Phone には、次の 2 つの異なる動作モードがあります。

- 電話機に SIP ダイヤル規則が設定されていない場合（14-17 ページ）
- 電話機に SIP ダイヤル規則が設定されている場合（14-18 ページ）

電話機に SIP ダイヤル規則が設定されていない場合

図 14-8 は、電話機にダイヤル プラン規則が設定されていない SIP タイプ A 電話機の動作を表しています。このモードでは、電話機はユーザが # キーを押すか [Dial] ソフトキーを押すまで、すべてのユーザ入力イベントを蓄積します。この機能は、多くの携帯電話で使用されている「送信」ボタンによく似ています。たとえば、内線 1000 にコールするユーザは、1、0、0、0 を押した後に [Dial] ソフトキーまたは # キーを押す必要があります。その後、電話機は Unified CM に SIP INVITE メッセージを送信し、内線 1000 へのコールの要求を示します。コールが Unified CM に到達すると、Unified CM のダイヤル プランに実装されているすべてのサービス クラスおよびコール ルーティング ロジックの対象になります。

図 14-8　　ダイヤル規則が設定されていないタイプ A の SIP 電話機でのユーザ入力とフィードバック



ユーザが番号をダイヤルした後に [Dial] ソフトキーや # キーを押さなかった場合、電話機は桁間タイムアウト（デフォルトでは 15 秒）だけ待ってから、SIP INVITE メッセージを Unified CM に送信します。図 14-8 の例では、1、0、0、0 をダイヤルして桁間タイムアウトの時間だけ待つと、電話機は 15 秒後に内線 1000 にコールをつなぎます。

（注）　ユーザが [Redial] ソフトキーを押した場合は、ただちに処理が行われるため、ユーザは Dial キーを押したり、桁間タイムアウトを待ったりする必要がありません。

ユーザが Unified CM に拒否されるパターンをダイヤルした場合、そのユーザはパターン全体を入力して Dial キーを押し、INVITE メッセージを Unified CM に送信した後でなければ、コールが拒否されたという通知（リオーダー トーン）は発信元に送信されません。たとえば、NPA 976 へのコールがすべて拒否される場合は、リオーダー音が再生される前に 919765551234 をダイヤルして [ダイヤル（Dial）] を押す必要があります。

電話機に SIP ダイヤル規則が設定されている場合

SIP ダイヤル規則を使用すると、ユーザがダイヤルしたパターンを電話機が認識できます。認識作業が完了すると、SIP INVITE メッセージが Unified CM に自動的に送信され、ユーザは Dial キーを押したり、桁間タイムアウトを待ったりする必要がありません（詳細については、SIP ダイヤル規則（14-20 ページ）を参照してください）。

たとえば、企業の支店で同一支店内の電話機間のコールに 4 桁の内線番号をダイヤルする必要がある場合は、4 桁のパターンを認識するように電話機を設定すれば、ユーザが Dial キーを押したり、桁間タイムアウトを待ったりする必要がありません（図 14-9 を参照）。

図 14-9　ダイヤル規則が設定されているタイプ A の SIP 電話機でのユーザ入力とフィードバック

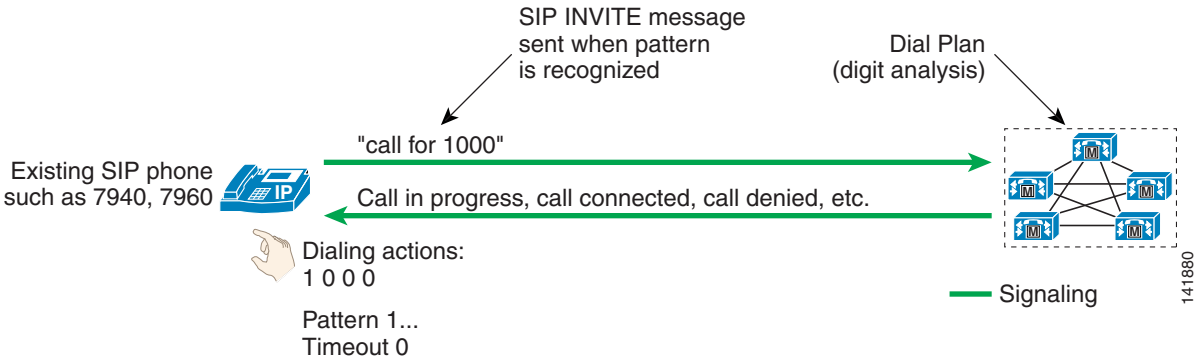


図 14-9 で、電話機は 1 で始まる 4 桁のパターンをすべて認識するように設定され、それに対応するタイムアウト値が 0 に設定されています。このパターンと一致するすべてのユーザ入力操作によって、SIP INVITE メッセージがすぐに Unified CM に送信され、ユーザが Dial キーを押す必要はありません。

SIP ダイヤル規則を使用するタイプ A 電話機では、電話機上に明示的に設定されていないパターンをダイヤルすることもできます。ダイヤルされたパターンが SIP ダイヤル規則と一致しない場合、ユーザは Dial キーを押すか、桁間タイムアウトを待ちます。

特定のパターンが電話機で認識され、それが Unified CM によってブロックされる場合、ユーザがダイヤル ストリング全体をダイヤルした後でなければ、コールがシステムで拒否されたという通知を受け取ることができません。たとえば、電話機に 919765551234 という形式でダイヤルされたコールを認識するように SIP ダイヤル規則が設定され、そのコールが Unified CM ダイヤル プランによってブロックされる場合、ユーザはダイヤリングの終了時（最後の 4 のキーを押した後）にリオーダー トーンを受信します。

タイプ B の SIP 電話機でのユーザ入力

タイプ B 電話機はタイプ A 電話機と動作が少し異なり、タイプ B 電話機では Key Press Markup Language（KPML）がサポートされていますが、タイプ A 電話機ではサポートされません（タイプ A の SIP 電話機でのユーザ入力（14-17 ページ）を参照）。

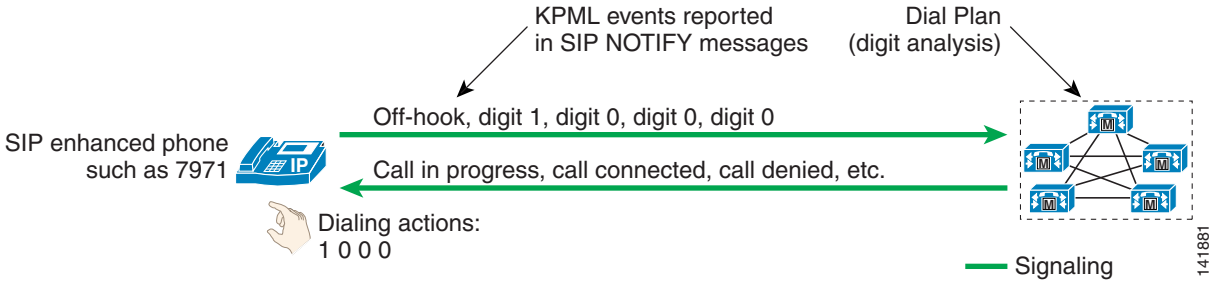
SIP を実行するタイプ B の IP Phone には、次の 2 つの異なる動作モードがあります。

- 電話機に SIP ダイヤル規則が設定されていない場合（14-19 ページ）
- 電話機に SIP ダイヤル規則が設定されている場合（14-19 ページ）

電話機に SIP ダイヤル規則が設定されていない場合

タイプ B の IP Phone は、Key Press Markup Language（KPML）に基づいて、ユーザによるキー操作を報告する機能を提供します。ユーザ入力イベントの 1 つ 1 つにより、Unified CM に対して KPML をベースとした独自のメッセージが生成されます。ユーザの個々の操作をすぐに Unified CM にリレーするという点では、この操作モードは SCCP を実行している電話機の操作モードと非常によく似ています（図 14-10 を参照）。

図 14-10　ダイヤル規則が設定されていないタイプ B の SIP 電話機でのユーザ入力とフィードバック



ユーザのすべてのキー操作によって、Unified CM に対する SIP NOTIFY メッセージがトリガーされることで、ユーザが押したキーに対応する KPML イベントが報告されます。このメッセージ機能により、Unified CM の番号分析はユーザが合成する部分パターンをその都度認識し、無効な番号がダイヤルされるとすぐにリオーダー トーンを再生するなど、適切なフィードバックを提供できます。

ダイヤル規則なしに SIP を実行しているタイプ A の IP Phone とは異なり、タイプ B の SIP 電話機には、ユーザ入力の終わりを示す Dial キーがありません。図 14-10 では、1000 をダイヤルするユーザは、最後の 0 をダイヤルした後、Dial キーを押さなくても、コール プログレス トーン（リングバック トーンかリオーダー トーン）を受け取ります。この動作は、SCCP プロトコルを実行する電話機のユーザ インターフェイスとの整合性が取れています。

電話機に SIP ダイヤル規則が設定されている場合

タイプ B の IP Phone では、ダイヤルされたパターンの認識が電話機によって行われるように SIP ダイヤル規則を設定できます（図 14-11 を参照）。

図 14-11　ダイヤル規則が設定されているタイプ B の SIP 電話機でのユーザ入力とフィードバック

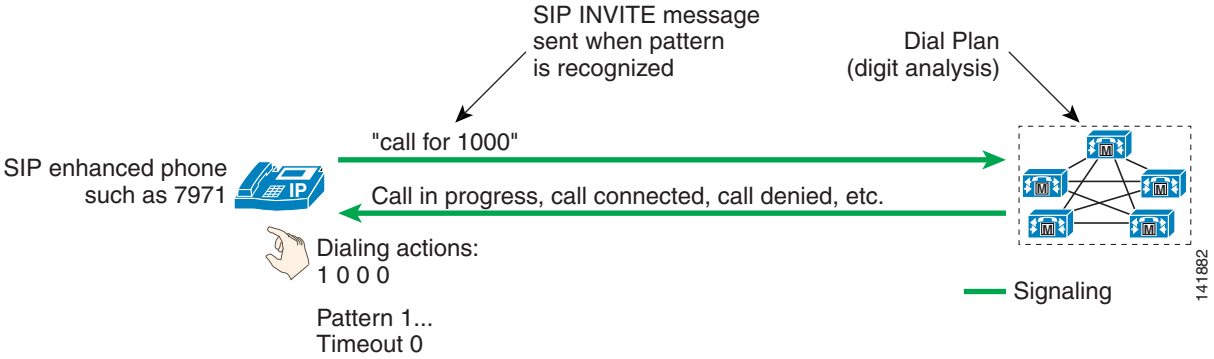


図 14-11 で、電話機は 1 で始まる 4 桁のパターンすべてを認識するように設定され、それに対応するタイムアウト値が 0 に設定されています。このパターンと一致するすべてのユーザ入力操作によって、Unified CM への SIP INVITE メッセージの送信がトリガーされます。

（注） SIP ダイヤル規則がタイプ B の IP Phone に実装されるとすぐに、KPML ベースのダイヤリングは無効になります。ユーザが SIP ダイヤル規則と一致しない番号ストリングをダイヤルした場合は、個々の桁のイベントが、いずれも Unified CM にリレーされません。その代わり、ダイヤリングが完了すると（桁間タイムアウトの発生後）、ダイヤルされたストリング全体が Unified CM にまとめて送信されます。

SIP ダイヤル規則を使用するタイプ B 電話機では、電話機上に明示的に設定されていないパターンをダイヤルする方法は 1 つだけです。ダイヤルされたパターンが SIP ダイヤル規則と一致しない場合、ユーザは桁間タイムアウトを待った後でなければ、Unified CM に SIP NOTIFY メッセージが送信されません。タイプ A の IP Phone とは異なり、タイプ B の IP Phone にはオンフック ダイヤルを使用した場合を除いて、ダイヤリングの終わりを示す Dial キーがありません。その場合、ユーザはいつでも [ダイヤル（Dial）] キーを押すことで、ダイヤルしたすべての桁の Unified CM への送信をトリガーできます。

（注） タイプ B 電話機を SRST ルータに登録した場合、設定した SIP ダイヤル規則は無効になります。

特定のパターンが電話機で認識され、それが Unified CM によってブロックされる場合、ユーザがダイヤル ストリング全体をダイヤルした後でなければ、コールがシステムで拒否されたという通知を受け取ることができません。たとえば、電話機に 919765551234 という形式でダイヤルされたコールを認識するように SIP ダイヤル規則が設定され、そのコールが Unified CM ダイヤル プランによってブロックされる場合、ユーザはダイヤリングの終了時（4 のキーを押した後）にリオーダー トーンを受信します。

SIP ダイヤル規則

Cisco Unified CM には、ユーザ入力が収集されたときに電話機でパターン認識を実行できるように、SIP ダイヤル規則機能が備わっています。たとえば、誰もが知る 911 というパターンを認識したら Unified CM にメッセージを送信し、すぐに緊急コールが開始されるように電話機を設定できます。それと同時に、ユーザが国際電話番号の可変長のパターンを入力できるようにも設定できます。

注意すべき重要な点は、SIP ダイヤル規則を使用して電話機にパターン認識を設定しても、Unified CM のサービス クラスとルート プランの設定の方が優先されることです。ある電話機が長距離通話のパターンを認識するように設定されていても、その電話機がローカル コールのみを許可するサービス クラスに割り当てられていると、Unified CM がそのコールをブロックします。

SIP ダイヤル規則には、それらの規則を設定する電話機のモデルに基づいて、次の 2 つのタイプがあります。

- 7905_7912（Cisco Unified IP Phone 7905 および 7912 に使用）
- 7940_7960_OTHER（上記以外のすべての IP Phone モデルに使用）

ダイヤル規則の一部として使用できる基本的なダイヤル パラメータは、次の 4 つです。

- パターン

  このパラメータは、パターンの実際の数値表現です。数字、ワイルドカード、2 次ダイヤル トーンを再生する命令を含めることができます。次の表は、2 つのタイプのダイヤル規則について、値とその効果を示しています。

	ダイヤル規則のタイプ	
パターン	7905_7912	7940_7960_OTHER
数字の 0 ～ 9	対応する数字。	対応する数字。
.	任意の数字（0 ～ 9）と一致します。	任意の文字（0 ～ 9、*、#）と一致します。
-	続けて追加の数字が入力される場合があることを示します。個々の規則の末尾に置く必要があります。	適用対象外
#	入力終了キー。ダイヤル規則の中に文字位置を示す > 文字を置くと、その文字位置以後は # キーが入力終了として認識されます。たとえば、9>#... と指定すると、9 が押された後は、いつでも # 文字が認識されます。	適用対象外
t*n*	*n* 秒のタイムアウト値を示します。たとえば、1…t3 は 1000 と一致し、3 秒後に Unified CM への招待の送信をトリガーします。	適用対象外
r*n*	最後の文字を *n* 回繰り返します。たとえば、1.r3 は 1…に相当します。	適用対象外
S	パターンに修飾子 S が含まれていると、このパターン以後の他のダイヤル規則がすべて無視されます。実質的に、S によって規則照合が終了します。	適用対象外

パターン	ダイヤル規則のタイプ	
	7905_7912	7940_7960_OTHER
*	入力終了キー。ダイヤル規則の中に文字位置を示す > 文字を置くと、その文字位置以後は * キーが入力終了として認識されます。	1 文字以上と一致します。たとえば、パターン 1* は 10、112、123456 などと一致します。
,	適用対象外	電話機で 2 次ダイヤル トーンを再生します。たとえば 8,.... の場合、ユーザには 8 を押した後に 2 次ダイヤル トーンが聞こえます。

- IButton

  このパラメータは、ダイヤル パターンの適用対象となるボタンを指定します。ユーザが回線ボタン 1 でコールを開始しようとしている場合は、ボタン 1 用に指定されたダイヤル パターンのみが適用されます。このオプション パラメータを設定しなかった場合、ダイヤル パターンは電話機のすべての回線に適用されます。このパラメータは、Cisco SIP IP Phone 7940、7941、7942、7945、7960、7961、7962、7965、7970、7971、および 7975 のみに適用されます。ボタン番号は、画面横にあるボタンの上から下の順に対応し、一番上のボタンが 1 になります。

- Timeout

  このパラメータは、システムがタイムアウトになり、ユーザが入力した番号にダイヤルするまでの時間を秒単位で指定します。ダイヤルされた番号がすぐにダイヤルされるようにするには、0 を指定します。このパラメータは、7940_7960_OTHER ダイヤル規則にのみ適用されます。このパラメータを省略した場合は、電話機のデフォルトの桁間タイムアウト値（デフォルトは 10 秒）が使用されます。

- ユーザ（User）

  このパラメータは、ダイヤルされた番号に自動的に追加されるタグを表します。有効な値は、**IP**（Unified CM 以外の SIP コール エージェントが配置される場合）と **Phone** です。このパラメータは、7940_7960_OTHER ダイヤル規則にのみ適用されます。このパラメータはオプションであり、Unified CM が唯一のコール エージェントとなる配置では省略してください。Unified CM に送信される SIP リクエスト内の user=phone タグは、SIP URI を数値 URI として扱うよう Unified CM に強制することに注意してください。alice@cisco.com;user=phone 形式の SIP URI のルーティングは成功しません。user=phone タグは数値扱いを強制し、alice は Unified CM にプロビジョニングされたどの数値パターンにもマッチしないからです。

（注） Cisco Unified IP Phone 7905 および 7912 は、パターンを SIP ダイヤル規則内で作成された順に選択します。これに対し、その他の電話機モデルでは、最長一致のパターンが選択されます。次の表は、ユーザが 95551212 をダイヤルした場合に選択されるパターンを示しています。

SIP ダイヤル規則	7905_7912	7940_7960_OTHER
…… 9…….	最初に一致するパターンの ……. が選択されます。	最長一致パターンの 9……が選択されます。

Unified CM におけるコール ルーティング

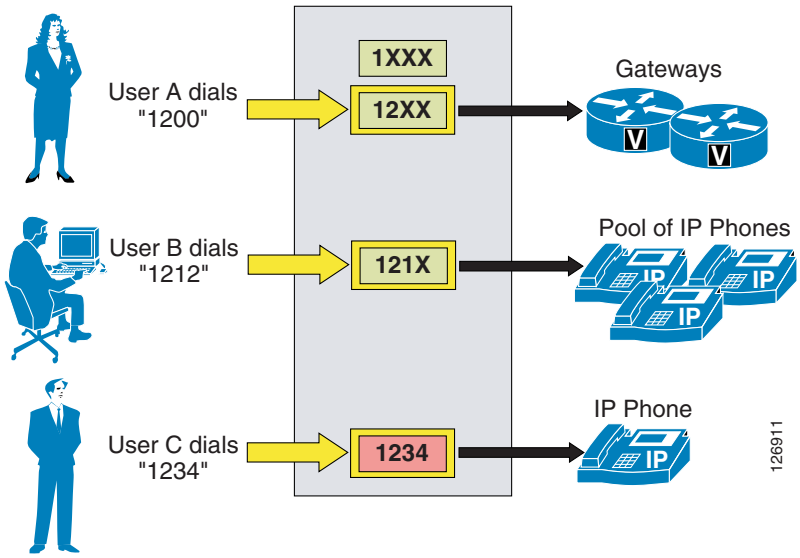
Unified CM 内に設定される数字のダイヤリング宛先およびディレクトリ URI は、すべて内部のコール ルーティング テーブルにパターンとして追加されます。このような宛先としては、IP Phone 回線、ボイスメール ポート、ルート パターン、トランスレーション パターン、および CTI ルート ポイントがあります。Unified CM は、数字ダイヤル先とディレクトリ URI に 2 つの異なるルーティング テーブルを使用します。

ディレクトリ URI がダイヤルされたとき、Unified CM は完全一致ロジックを使用して、ディレクトリ URI ルーティング テーブル内の設定済みディレクトリ URI から一致を検索します。[URI ルックアップ ポリシー（URI Lookup Policy）] エンタープライズ サービス パラメータ設定は URI のユーザ部分（左側）の完全一致ロジックが大文字と小文字を区別するかしないかを決定します。大文字と小文字を区別するマッチングがデフォルトです。番号がダイヤルされると、Unified CM は best-match ロジックを使用し、数字のコール ルーティング テーブルにあるすべてのパターンの中から一致パターンを選択します。一致する可能性のある数字パターンが複数ある場合は、次の基準に基づいて宛先パターンを選択します。

- ダイヤルされたストリングに一致するもの。
- 一致する可能性のあるパターンのうち、ダイヤルされたストリング以外に一致するパターンが最も少ないもの。

たとえば、図 14-12 の場合を考えます。ここでは、コール ルーティング テーブルにパターン 1XXX、12XX、および 1234 が保持されています。

図 14-12　Unified CM のコール ルーティング ロジックの例



ユーザ A がストリング 1200 をダイヤルすると、Unified CM は、この番号をコール ルーティング テーブル内のパターンと比較します。この場合は、一致する可能性のあるパターンが 2 つあります（1XXX と 12XX）。両方ともダイヤルされたストリングに一致していますが、1XXX は合計 1,000 個のストリングに一致する一方で（1000 ～ 1999）、12XX は 100 個のストリングに一致します（1200 ～ 1299）。したがって、12XX がこのコールの宛先として選択されます。

ユーザ B がストリング 1212 をダイヤルした場合、一致する可能性のあるパターンは 3 つあります（1XXX、12XX、および 121X）。上で説明したように、1XXX に一致するストリングは 1,000 個あり、12XX に一致するストリングは 100 個あります。しかし、121X に一致するストリングは 10 個しかありません。したがって、このパターンがコールの宛先として選択されます。

ユーザ C がストリング 1234 をダイヤルした場合、一致する可能性のあるパターンは 3 つあります（1XXX、12XX、および 1234）。上で説明したように、1XXX に一致するストリングは 1,000 個あり、12XX に一致するストリングは 100 個あります。しかし、1234 に一致するストリングは 1 個しかありません（ダイヤルされたストリング）。したがって、このパターンがコールの宛先として選択されます。

可変長パターンの一致文字列の数を判断する必要がある場合、Unified CM はダイヤルされた桁数と同じ長さの一致文字列だけを考慮に入れます。次の表で、ユーザが 1311 とダイヤルし、パターン 1XXX、1[2-3]XX、13! がある場合に、これらの一致する可能性があるパターンの一致する文字列の数を示します。

パターン	一致する文字列の数	一致する可能性のある文字列
1XXX	1000	1000 ～ 1999
1[2-3]XX	200	1200 ～ 1299、1300 ～ 1399
13!	100	1300 ～ 1399。ダイヤルされた桁数に基づいて、4 桁の文字列のみカウント

この例では、変数長パターン 13! がベストマッチとして選択されています。

（注）　Cisco Unified CM でディレクトリ番号（DN）を設定すると、それぞれのデバイス（IP Phone など）が登録済みかどうかにかかわらず、その番号はコール ルーティング テーブルに配置されます。この仕様によって、デバイス（およびそのプライマリ パターン）が未登録である場合は、セカンダリの一致パターンを利用してフェールオーバー機能をアプリケーションに提供することができなくなりました。プライマリ パターンがコール ルーティング テーブルに必ず存在するため、セカンダリ パターンに一致するかどうかは検索されません。

パターンにおける + 記号のサポート

Unified CM 内のすべてのパターン（ルート パターン、トランスレーション パターン、ディレクトリ番号など）では、+ 記号を使用できます。+ を文字どおりの意味で使用するには、+ の前にエスケープ文字 \ を入力することで、先行文字の 1 つ以上のインスタンスを意味する正規表現演算子の + と区別します。次に例を示します。

- \+14085264000 は +14085264000 を意味します。
- 2+ は 2、22、222 などを意味します。

これによって、Unified CM の +E.164 ダイヤル プランのシームレスな実装が可能になります。

ディレクトリ URI

Unified CM に登録されているすべてのエンドポイントは、1 つ以上の数字（先頭に + が付く場合もある）を含むディレクトリ番号でプロビジョニングされます。最大 5 つのディレクトリ URI を各ディレクトリ番号に関連付けることができます。この関連付けは、ディレクトリ URI をディレクトリ番号に明示的に関連付けることで作成できます。ディレクトリ URI がエンド ユーザに設定されている場合、そのエンドユーザにプライマリ内線番号が定義されるとすぐに、このディレクトリ URI が自動的にそのエンドユーザのプライマリ内線番号と関連付けられます。すべての自動的に関連付けられたディレクトリ URI はパーティション **ディレクトリ URI** に作成されますが、手動設定されたディレクトリ URI はどのパーティションにも置くことができます。手動で設定されたディレクトリ URI は、関連付けられているディレクトリ番号と同じパーティションに配置できますが、そうしなくてもかまいません。ディレクトリ URI はパーティションごとに一義的でなければなりません。

正確には、ディレクトリ番号に関連付けられたディレクトリ URI の 1 つが、そのディレクトリ番号のプライマリ ディレクトリ URI としてマークされる必要があります。ユーザ ディレクトリ URI がそのユーザのプライマリ内線番号に自動的に関連付けられる場合、そのディレクトリ URI は自動的にそのディレクトリ番号のプライマリ ディレクトリ URI にもなります。自動的に関連付けられたディレクトリ URI がない場合、設定されたディレクトリ URI の 1 つがプライマリ ディレクトリ URI として選択される必要があります。プライマリ ディレクトリ URI の目的は、このディレクトリ URI がそれぞれのディレクトリ番号から発信されたコールについて、発信 ID ディレクトリ URI として使用されることです。

ディレクトリ URI をどのディレクトリ番号とも関連付けすることが可能なため、関連付けられたディレクトリ URI をダイヤルすることで、発信者はどのディレクトリ番号にも到達できます。着信側ディレクトリ番号は、任意のプロトコルを使用して Unified CM に登録された任意のデバイスになります。同様に、Unified CM は、ディレクトリ URI が発信側ディレクトリ番号に関連付けられている限り、どのディレクトリ番号からのコールにもディレクトリ URI 発信者 ID を提供できます。

ディレクトリ URI のクラスタ間ルーティングを有効にするために、クラスタ間検索サービス（ILS）で他のクラスタとディレクトリ URI カタログを交換するように Unified CM をプロビジョニングできます。他のクラスタとディレクトリ URI カタログを交換するように設定された各クラスタは、ロケーション属性、SIP ルート文字列とともに、すべてのローカルに設定されたディレクトリ URI を 1 つのディレクトリ URI カタログでアドバタイズします。マルチ クラスタ環境では、ディレクトリ URI のホスト部分を使用して SIP 要求を確実にルーティングすることができない場合に、ディレクトリ URI へのコールを正しいクラスタに転送するために、このロケーション属性が使用されます。これは、たとえば、*<user>@example.com* などのフラットな URI スキームを使用する場合です。ホスト部分の「example.com」は、この URI をホストするリモートの Unified CM クラスタを一義的に識別しません。

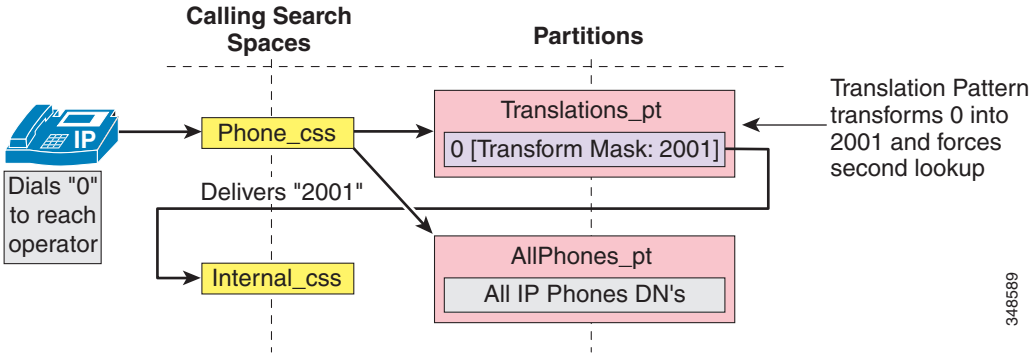
リモート クラスタから学習したディレクトリ URI へのコールをルーティングする方法の詳細については、Unified CM での SIP 要求のルーティング（14-52 ページ）の項を参照してください。

トランスレーション パターン

トランスレーション パターンは、Unified CM で最も強力な番号操作ツールであり、あらゆるタイプのコールに対して使用できます。トランスレーション パターンは、ルート パターンと同じ一般規則に従い、同じワイルドカードを使用します。ルート パターンと同じように、トランスレーション パターンをパーティションに割り当てます。しかし、ダイヤルされた数字がトランスレーション パターンと一致する場合、Unified CM は、ゲートウェイなどの外部エンティティにコールをルーティングしません。代わりに、まず変換を実行した後、トランスレーション パターン内で設定されたコーリング サーチ スペースを使用して、コールを再度ルーティングします。

トランスレーション パターンは、図 14-13 の例に示すように、さまざまな用途に使用できます。

図 14-13　トランスレーション パターンの応用例



この例では、管理者は、0 をダイヤルすると到達できるオペレータ サービスをユーザに提供し、一方で定型の内部番号計画をそのまま維持することを考えています。IP Phone は、Translations_pt パーティションを（他のパーティションとともに）含んでいる Phone_css コーリング サーチ スペースを使用して設定されています。このパーティションには、トランスレーション パターン 0 が定義されています。設定済みの Called Party Transform Mask によって、ダイヤルされたストリング（0）を新しいストリング 2001 で置き換えるように Unified CM に指示しています。2001 は、オペレータの電話機の DN に対応しています。2 回めの（この場合は 2001 の）ルックアップが、Internal_css コーリング サーチ スペースを使用して、コール ルーティング エンジンを通じて強制的に実行されます。この時点で、AllPhones_pt パーティションに含まれている実際のオペレータ DN（2001）までコールを伸ばすことができます。

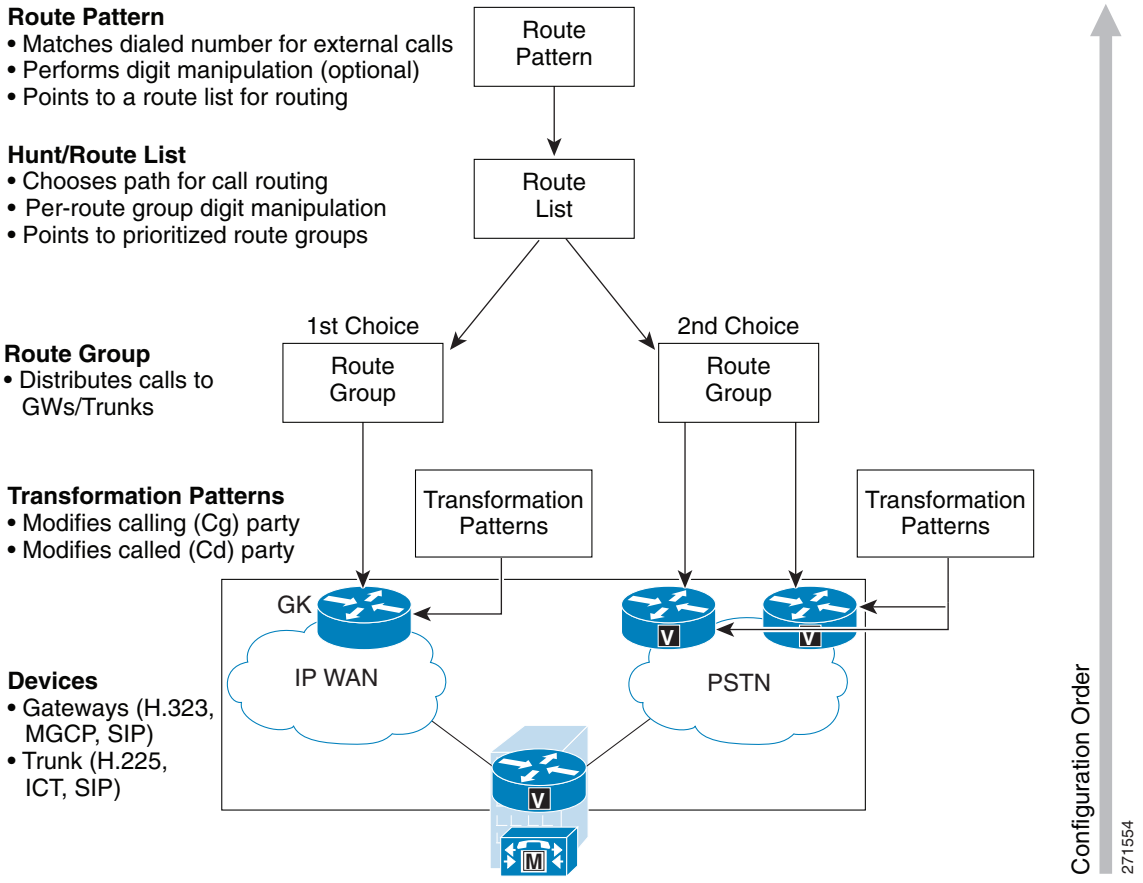
（注）　ダイヤルされた番号をトランスレーション パターンを使用して操作すると、その変換後の番号が、コール詳細レコード（CDR）に記録されます。ただし、番号操作がルート リスト内で発生した場合、CDR には変換後の番号ではなく、ダイヤルされた元の番号が表示されます。IP Phone の Placed Calls ディレクトリには、常にユーザがダイヤルしたストリングがそのまま表示されます。

トランスレーション パターンの一般的な使用例は、特定のダイヤル文字列の形式から他のダイヤル プラン要素がマッチする文字列でマッピングを作成することです。このマッピングは、ルート パターン、ディレクトリ番号などのその他パターンによって作成された「ネイティブ」ダイヤリング手順にオーバーレイのダイヤリング手順を実装します。セカンダリ ルックアップでは通常、ダイヤリングの正規化を実行するトランスレーション パターンはトランスレーション パターンをアクティブにするコーリング サーチ スペースを単純に使用する必要があります。CSS 継承と呼ばれるこの動作は、トランスレーション パターンのオプション [発信側コーリング サーチ スペースを使用（Use Originator's Calling Search Space）] で選択します。このオプションを有効にすると、別のコーリング サーチ スペースによってそれぞれ定義された異なるサービス クラスのダイヤリングの正規化トランスレーション パターンを再利用できるようになります。

Unified CM の外部ルート

Unified CM は、同じクラスタ内の内部宛先にコールをルーティングする方法を自動的に「認識」します。PSTN ゲートウェイ、SIP トランク、またはその他の Unified CM クラスタなどの外部宛先の場合、外部ルート コンストラクト（次の項で説明）を使用して、明示的にルーティングを設定する必要があります。このコンストラクトは、3 層式のアーキテクチャに基づいています。このアーキテクチャでは、複数層のコール ルーティングと共に、番号操作も可能です。Unified CM は、外部ダイヤル ストリングと一致する設定済みルート パターンを検索し、それを使用して、対応するルート リストを選択します。ルート リストには、コールに使用可能なパスが優先順位順に並べられています。これらのパスは、ルート グループと呼ばれ、従来の PBX でトランク グループと呼ばれていたものに非常によく似ています。図 14-14 では、Unified CM 外部ルート コンストラクトの 3 層式アーキテクチャを示しています。

図 14-14　外部ルート パターンのアーキテクチャ



次の各項では、Unified CM の外部ルート コンストラクトの個々の要素について説明します。

- ルート パターン（14-28 ページ）
- ルート リスト（14-31 ページ）
- ルート グループ（14-32 ページ）
- ルート グループ デバイス（14-32 ページ）

ルート パターン

ルート パターンは、コールを外部エンティティにルーティングするために Unified CM で設定された、数字とワイルドカードを組み合わせたストリング（たとえば、9.[2-9]XXXXXX）です。ルート パターンでは、コールをルーティングするゲートウェイを直接指すことも、ルート リストを指すこともできます。ルート リストはルート グループを指しており、最終的にゲートウェイを指します。

ルート パターン、ルート リスト、およびルート グループ コンストラクトを完全パスで指定することを強く推奨します。その理由は、この構造を使用するとコール ルーティング、番号操作、および将来のダイヤル プランの拡張を最も柔軟に行うことができるからです。

@ ワイルドカード

- @ ワイルドカードは、特殊なマクロ関数であり、特定の国の番号計画全体を表す一連のパターンに拡張されます。たとえば、フィルタ処理されていない単一のルート パターン（たとえば、9.@）を北米番号計画を使用して設定すると、実際には、Unified CM の内部ダイヤル プラン データベースに 166 個の個別ルート パターンが追加されます。
- その他の国別番号計画を受け入れるように Unified CM を設定できます。この作業が完了すると、[Route Pattern] 設定ページの [Numbering Plan] フィールドで選択した値に応じて、同じ Unified CM クラスタ内で、複数の番号計画に対して @ ワイルドカードを使用できるようになります。詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Dial Plan Deployment Guide*』を参照してください。

  https://www.cisco.com/en/US/products/sw/voicesw/ps5629/prod_maintenance_guides_list.html
- @ ワイルドカードは、いくつかの中小規模の配置では十分に実務で使用できますが、大規模な配置では、管理とトラブルシューティングが困難になる可能性があります。これは、@ ワイルドカードを利用する場合、ルート フィルタを使用して、管理者が特定のパターンをブロックする必要があるためです（ルート フィルタ（14-28 ページ）を参照してください）。

ルート フィルタ

- ルート フィルタは、@ ワイルドカードによって作成されるルート パターン数を減らすために、@ ルート パターンと一緒にのみ使用します。@ ワイルドカードを含まないパターンに適用されるルート フィルタは、発生するダイヤル プランに影響を与えません。
- ルート フィルタと一緒に入力する論理式は、NOT-SELECTED フィールドを除いて、最大 1024 文字にできます。
- ルート フィルタ内の論理文節数が増えるにつれて、設定ページのリフレッシュ時間も増え、容認できないほど長くなる場合があります。
- コール ルーティングを設定する際は、1 つのルート フィルタをあまりに多くのルート パターンに割り当てないようにしてください。数百のルート パターンが関連付けられたルート フィルタを編集した場合、システム コアに発生します。これは、ルート フィルタを使用するすべてのルート パターンのコール ルーティングの更新に新たなシステム処理が必要になるためです。発生しないようにするには、重複するルート フィルタを作成します。
- 大規模な配置の場合、@ ワイルドカードとルート フィルタではなく、明示ルート パターンを使用してください。この方法を利用すると、管理とトラブルシューティングも容易になります。これは、Unified CM で設定されているすべてのパターンが、[Route Pattern] 設定ページから簡単に参照できるからです。

国際および可変長ルート パターン

- 国際間の宛先は、通常、任意の桁数を表す ! ワイルドカードを使用して設定されます。たとえば、北米では通常、国際コール用にルート パターン 9.011! が設定されています。欧州諸国のほとんどでは、0.00! ルート パターンを使用することで同じ結果を実現しています。
- ! ワイルドカードは、ダイヤルされた番号の長さが変化する国では配置にも使用されます。このような場合、Unified CM は、ダイヤルがいつ完了するかわからないので、コールの送信前に 15 秒待機します。この遅延は、次の方法のいずれかで短縮できます。
  - ダイヤルの終わりを指定する T302 タイマー（サービス パラメータ TimerT302_msec）の値を減らします。ただし、ユーザがダイヤルを終了する前のコールの早期送信を防止するために、4 秒以上に設定します。
  - # ワイルドカードで終了する同じパターンのルートパターンを設定し（たとえば、北米の場合 9.011!#、欧州の場合 0.00!#）、ダイヤルの終わりを示すために # をダイヤルするようにユーザに指示します。この処理は、携帯電話で送信ボタンを押すことに相当します。

重複送信と重複受信

国内の番号計画をスタティック ルート パターンで定義することが難しい国では、Unified CM に重複送信および重複受信を設定できます。

重複送信とは、エンド ユーザがダイヤルする番号を Unified CM で収集しながら、番号がダイヤルされると同時に PSTN に渡すことを意味します。重複送信を可能にするには、[Route Pattern] 設定ページの [Allow Overlap Sending] チェックボックスをオンにします。ルート パターンには、PSTN アクセス コードだけを含める必要があります（北米では「9」、多くのヨーロッパ諸国では「0」）。

重複受信とは、ダイヤルされる番号を PRI PSTN ゲートウェイから Unified CM で 1 つずつ受信し、ストリングのダイヤルが完了するまで待機し、その後でコールを内部宛先にルーティングすることを意味します。重複受信を可能にするには、OverlapReceivingFlagForPRI サービス パラメータを True に設定します。

ルート パターンにおける番号操作

- コールで最終的に利用するルート グループに関係なく、ルート パターンで設定する番号操作は、発番号および着番号に影響を与えます。ルート リスト ビューにあるそのメンバーのルート グループに設定される番号操作が影響するのは、ルートに対してだけです。つまり、コールの発信に使用するルート グループに設定されている変換のみが実行されます。
- ルート リスト ビューにあるそのルート グループの番号操作は、ルート パターンに設定される番号操作よりも優先されます。
- コールをルーティングするために選択されたデバイス（またはそのデバイスのデバイス プール）で設定されたトランスフォーメーション パターンが、ルート パターンやルート リストで設定された発信側および着信側トランスフォーメーションよりも優先されます。コールをルーティングするために選択されたデバイス（またそのデバイスのデバイス プール）でトランスフォーメーション コーリング サーチ スペース（CSS）が設定されている場合には、ルート パターンまたはルート リストで設定されているトランスフォーメーションは、それぞれのトランスフォーメーション CSS を使用して一致が見つからなかった場合にのみ考慮されます。トランスフォーメーション CSS への入力は常に、ルート パターンまたはルート リストのトランスフォーメーションを適用する前の、変換されていない番号です。
- ルート パターンで番号操作を設定する場合、コール詳細レコード（CDR）は、番号操作が行われた後のダイヤル番号を記録します。ルート グループまたはデバイス レベルのみで番号操作を設定する場合、CDR は、番号操作が行われる前の実際のダイヤル番号を記録します。
- 同様に、ルート パターンでの番号操作を設定すると、発信側の IP Phone ディスプレイには、操作後の番号が示されます。ルート グループのみで番号操作を設定する場合、この操作はエンド ユーザには見えなくなります。

発信側回線 ID

- 発呼回線 ID の表示は、ゲートウェイで使用可能または使用不可にできます。また、サイトの要件に基づいて、ルート パターンで操作することもできます。
- [Use Calling Party's External Phone Number Mask] オプションを選択する場合、外部コールは、コールを発信する IP Phone に指定された発呼回線 ID を使用します。このオプションを選択しない場合、[Calling Party Transform Mask] フィールドに指定されたマスクが、発信者番号識別の生成に使用されます。

コールの分類

- このルート パターンを使用しているコールは、オンネットまたはオフネットのコールとして分類できます。このルート パターンを使用すると、オフネット間でのコール転送を禁止したり、オンネット通話者がいないカンファレンス ブリッジを終了したりすることによって、料金詐欺を防止できます（これらの機能は、どちらも Unified CM Administration の Service Parameters を使用して制御します）。
- [Allow device override] チェックボックスをオンにすると、コールは、関連するゲートウェイまたはトランク上で、コール分類設定に基づいて分類されるようになります。

強制承認コード（FAC）

- [強制承認コード（FAC）（Forced Authorization Codes（FAC））] チェックボックスを使用すると、個々のルート パターンを使用するときに発信コールが制限されます。ルート パターンに対して FAC を有効にすると、ユーザは、目的のコール受信者に到達するための承認コードを入力するように要求されます。
- ユーザのダイヤルした番号が、FAC が有効になったルート パターンを通じてルーティングされるものである場合、システムは承認コードの入力を求めるトーンを再生します。コールを確立するには、ユーザ承認コードが、ダイヤルされた番号のルーティングに必要となる承認レベルを満たしているか、そのレベルを超えている必要があります。
- コール詳細レコード（CDR）に表示されるのは、承認名のみです。承認コードは CDR には表示されません。
- FAC 機能は、[Allow overlap sending] チェックボックスがオンの場合は使用できません。

クライアント識別コード（CMC）

- [Client Matter Code] チェックボックスを使用すると、個々のルート パターンを使用して特定番号へのコールがトラッキングされます。たとえば、企業で使用すると、特定のクライアントへのコールをトラッキングできます。
- ルート パターンに対して CMC を有効にすると、ユーザは目的の宛先に到達するためのコードを入力するように要求されます。
- ユーザのダイヤルした番号が、CMC が有効になったルート パターンを通じてルーティングされるものである場合、システムはコードの入力を求めるトーンを再生します。コールを確立するには、ユーザが正しいコードを入力する必要があります。
- クライアント識別コードは、コール詳細レコードに表示されます。これは、クライアントの課金およびアカウンティングに関するレポートを生成するための、CDR の分析およびレポート ツールで使用できるようにするためです。
- CMC 機能は、[Allow overlap sending] チェックボックスがオンの場合は使用できません。
- CMC と FAC を両方とも有効にすると、ユーザは番号をダイヤルするとき、FAC の入力を求められたら入力し、次のプロンプトで CMC を入力します。

SIP ルート パターン

SIP ルート パターンは、Unified CM で設定され、SIP URI のホスト部分（右側）に基づいて外部エンティティへのコールをルーティングまたはブロックします。SIP ルート パターンは、SIP トランクまたは 1 つ以上のルート グループに続いて最後に SIP トランクを参照するルート リストを直接ポイントすることができます。いっそうの柔軟性のために、フル SIP ルート パターン、ルート リスト、ルート グループ コンストラクトの使用を推奨します。

SIP URI のホスト部分に一致する SIP ルート パターンは、ドメイン名または IP アドレス（両方とも SIP URI の右側にある可能性がある）と一致する場合があります。ドメイン名の SIP ルート パターンでワイルドカードを使用して、複数のドメインに一致させることができます（たとえば、*.cisco.com や ccm[1-4].uc.cisco.com）。IP アドレスの SIP ルート パターンでは、サブネット表記を使用できます（たとえば、192.168.10.0/24）。

ルート リスト

ルート リストは、発信コールに使用できるパス（ルート グループ）が優先順位順に並べられたリストです。ルート リストの標準的な用途は、リモートの宛先に 2 つのパスを指定することです。この場合、第一選択のパスは、IP WAN を介したパスであり、第二選択のパスは、PSTN ゲートウェイを介したパスです。

ルート リストには次の特性があります。

- 複数のルート パターンが同一ルート リストを指すことができます。
- ルート リストは、所定の宛先への代替パスの役目をするルート グループが、優先順位順に並べられたリストです。たとえば、ルート リストを使用して最低料金選択機能をサポートできます。この場合、リスト内のプライマリ ルート グループが、コールあたりのコストがより低くなるようにします。プライマリ ルート グループが「all trunks busy（全トランク使用中）」状態、または IP WAN リソースの不足により使用できない場合だけ、セカンダリ ルート グループが使用されます。
- ルート リスト内の各ルート グループは、独自の番号操作を行うことができます。たとえば、ルート パターンが 9.@ であるときに、ユーザが 9 1 408 555 4000 をダイヤルした場合、IP WAN ルート グループは 9 1 を削除し、PSTN ルート グループは 9 だけを削除することが可能です。
- 複数のルート リストに、同じルート グループを含むことができます。ルート グループの番号操作は、そのルート グループを指定する特定のルート リストに関連しています。
- ルート パターンまたはルート グループ内で複数の番号操作を実行すると、変換が実行される順序が、コールに使用される、変換結果の発番号および着番号に影響を与える可能性があります。Unified CM は、次に示す主要なタイプの番号操作を表示されている順に実行します。
  1. 番号を破棄する
  2. ルート パターンまたはルート グループで定義されている発信側および着信側トランスフォーメーション
  3. 番号をプレフィックスとして付加する

出力デバイス（ゲートウェイまたはトランク）に定義された発信側および着信側トランスフォーメーションは、ルート パターンとルート グループで定義された発信側および着信側トランスフォーメーションを上書きすることに注意してください。

ルート グループ

ルート グループは、一般にゲートキーパーまたはリモート Unified CM クラスタとのゲートウェイ（MGCP、SIP、または H.323）、H.323 トランク、または Cisco Unified Border Element である特定のデバイスを制御し、それを指定します。Unified CM は、割り当てられている分配アルゴリズムに従ってコールをデバイスに送信します。Unified CM では、トップダウン アルゴリズムと循環アルゴリズムをサポートしています。

ルート グループ デバイス

ルート グループ デバイスは、ルート グループによってアクセスされるエンドポイントであり、一般に、ゲートキーパーまたはリモート Unified CM とのゲートウェイまたはトランクで構成されます。次のタイプのデバイスは、Unified CM で設定できます。

- メディア ゲートウェイ コントロール プロトコル（MGCP）ゲートウェイ
- SIP ゲートウェイ
- H.323 ゲートウェイ
- H.225 トランク、ゲートキーパー制御：ゲートキーパーを介した標準 H.323 ゲートウェイとのトランク
- クラスタ間トランク、非ゲートキーパー制御：別の Unified CM クラスタとの直接トランク
- クラスタ間トランク、ゲートキーパー制御：ゲートキーパーを介した他の Unified CM クラスタまたは H.323 ゲートウェイとのトランク
- SIP トランク：別の Unified CM クラスタとのトランク、Cisco Unified Border Element、Session Border Controller、または SIP プロキシ

（注）　H.225 トランクとクラスタ間トランク（ゲートキーパー制御）はどちらも、相手方エンドポイントが標準 H.323 ゲートウェイであるか、Unified CM であるかを自動的に検出し、それに応じて H.225 または Intercluster Trunk プロトコルを選択します。

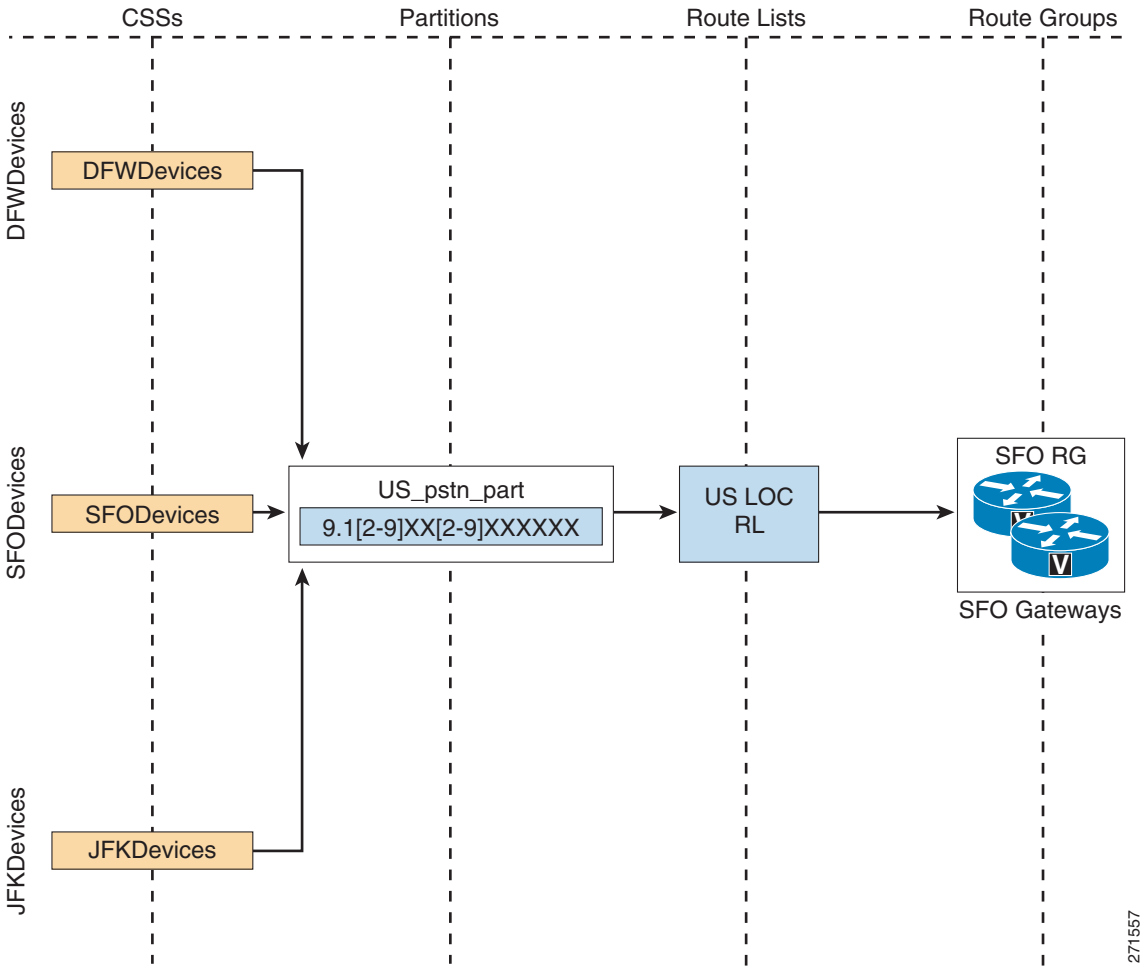
ローカル ルート グループ

デバイス プールは、複数のローカル ルート グループに関連付けることができます。ローカル ルート グループを使用したルート パターンには固有の特性があります。つまり、コールの発信元デバイスに基づいて出口ゲートウェイを動的に選択できます。それに対し、スタティック ルート グループを使用したルート パターンによってルーティングされるコールでは、コールの発信元デバイスに関係なく、コールが同じゲートウェイにルーティングされます。

例 14-2　ローカル ルート グループと非ローカル ルート グループの比較

図 14-15 では、9.1[2-9]XX[2-9]XXXXXX と定義されたルート パターンは、San Francisco ゲートウェイを含む非ローカル ルート グループを参照するルート リストを指しています。このルート パターンが Dallas、San Francisco、および New York の電話機のコーリング サーチ スペースに含まれているパーティションにある場合、それらの 3 つの都市にあるデバイスからの国内コールの出口は San Francisco の PSTN となります。

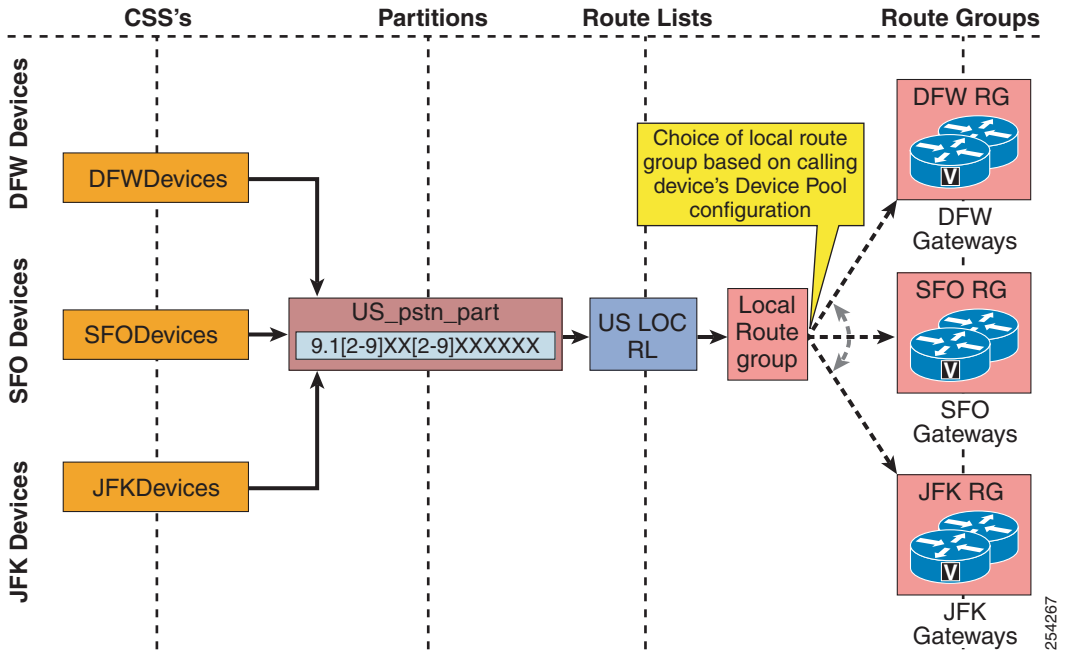
図 14-15　非ローカル ルート グループの動作



一方、図 14-16 に示すように、同じルート パターンを変更して、標準ローカル ルート グループを含むルート リストを指すようにした場合、Dallas サイトから発信されるコールの出口は Dallas ゲートウェイを経由した公衆網となり、New York サイトから発信されるコールの出口は New York ゲートウェイを経由した公衆網となり、San Francisco サイトから発信されるコールの出口は San Francisco ゲートウェイを経由した公衆網となります。

ローカル ルート グループを使用すると、発信元デバイスに基づいて出力ゲートウェイを選択できます。これにより、すべてのサイトの電話機のコーリング サーチ スペースによって再利用が可能な、サイトに依存しないルート パターンが使用できるようになります。

図 14-16　ローカル ルート グループの動作



デバイス モビリティ機能を使用すると、ローミングしている現在のサブネットに基づいて、デバイス プールをエンドポイントに割り当てることができます。これにより、電話機の現在のサイトに基づいた、ローカル ルート グループの割り当てが可能になります。

例 14-3　デバイス モビリティ

電話機を San Francisco サイトから New York サイトに移動するとします。電話機の新しい IP アドレス（New York サイトに関連付けられた IP サブネット部分）に基づいて、New York のデバイス プールがその電話機に割り当てられます。ローミング電話機によって発信される次のコールは、標準ローカル ルート グループを含むルート リストを使用したルートと一致し、New York ゲートウェイを経由してルーティングされます。

ローカル ルート グループが転送コール シナリオで使用されている場合（たとえば、電話機 A から電話機 B にコールし、B が PSTN 内の宛先に転送される場合）、電話機 B のコール転送コーリング サーチ スペースのルート パターンによって、電話機 B から転送されるコールのサービス クラスが特定されます。一方、デフォルトでは電話機 A のデバイス プールに関連付けられたローカル ルート グループは、電話機 B のコール転送コーリング サーチ スペースを使用して見つかったルート パターンで選択されているルート リスト内の標準ローカル ルート グループにヒットする場合、出力ゲートウェイの特定に使用されます。その結果、一般的には電話機 A に対してローカルなゲートウェイが転送コールに使用されます。これにより、最初の発信者（電話機 A）の発信者 ID を PSTN に送信でき、この発信者 ID はプロバイダーによってスクリーニングされません。管理者による転送コールのローカル ルート グループの選択ポリシーの設定を許可するサービス パラメータがあります。サービス パラメータは次のように設定できます。

- [発信者のローカル ルート グループ（Calling Party's Local Route Group）]：下位互換性のあるデフォルト。最初の発信者のデバイス プールに関連付けられたローカル ルート グループが選択されます（上の例では電話機 A）。
- [着信者（Original Called Party）]：着信側電話機のデバイス プールに関連付けられたローカル ルート グループが選択されます（上の例では電話機 B）。
- [最終的な転送者（Last Redirecting Party）]：PSTN にコールを転送している電話機のデバイス プールに関連付けられたローカル ルート グループが選択されます（上の例では電話機 B）。これらの最後の 2 通りの方法は、PSTN に最後に転送される前に、コールが複数のホップを介して転送される場合にのみ異なります。

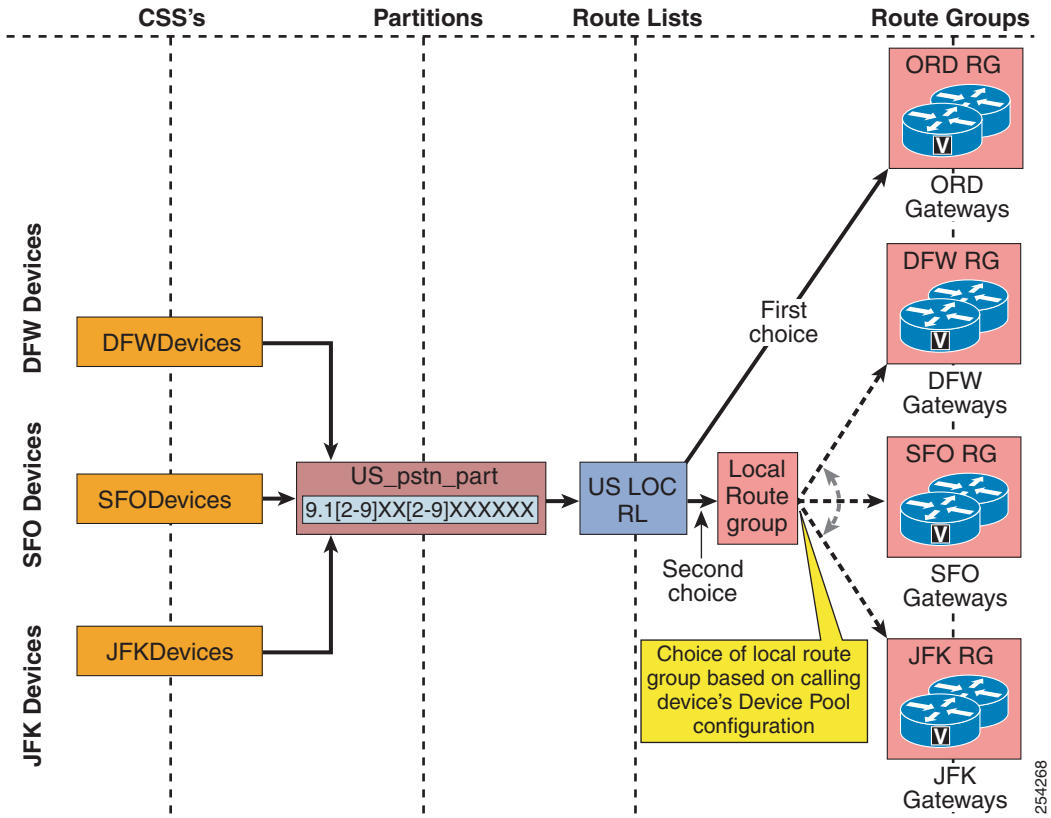
PSTN へのローカル フェールオーバーを使用した中央ゲートウェイ

中央ゲートウェイが設定されているシステムの場合、ローカル ルート グループによって、PSTN へのローカル フェールオーバーが簡素化されます。発信側サイトでゲートウェイへのローカル フェールオーバーが許可されているときに、単一のルート リストを使用することで、複数サイトの PSTN コールをルーティングできます。

例 14-4　中央ゲートウェイとローカル フェールオーバー

ある会社が、Chicago にあるトランクのグループに有利な PSTN 相互接続レートをネゴシエートするとします。ルート リストに、1 番めの項目として Chicago にあるゲートウェイを含むルート グループが含まれ、2 番めの項目として標準ローカル ルート グループが含まれている場合、処理されるコールは最初に Chicago にある低コストの推奨ゲートウェイに送信されます。Chicago ゲートウェイが使用可能でない、フリー ポートがない、あるいは発信側電話機と Chicago ゲートウェイ間で使用できる帯域幅が十分でない場合は、発信側電話機のデバイス プール設定でローカル ルート グループによって決定されている、2 番めの項目を使用して、発信側電話機と同じ場所にあるゲートウェイを経由したコールのルーティングが試行されます（図 14-17 を参照）。

図 14-17　PSTN へのローカル フェールオーバーを使用した中央ゲートウェイ



複数のローカル ルート グループ

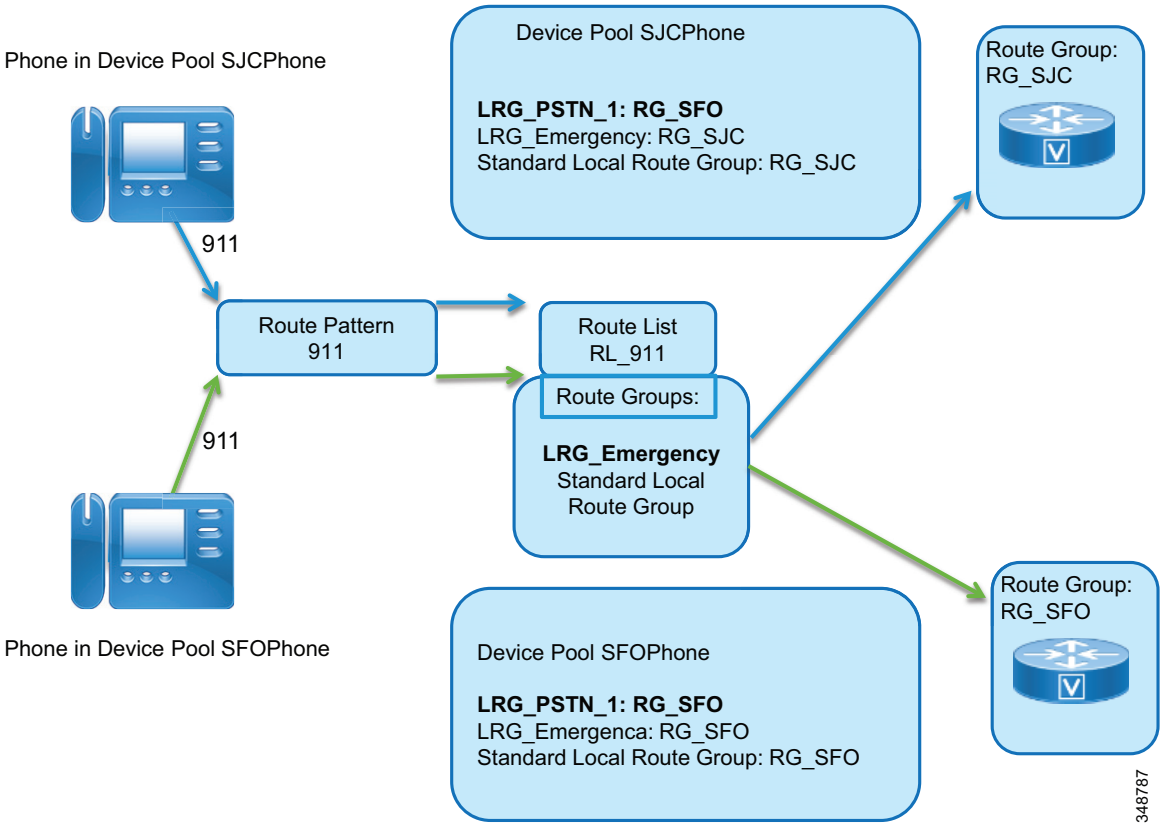
発信側デバイス固有の複数のルート グループ要素を持つルート リストをサポートするために、複数の名前付きローカル ルート グループを Unified CM で設定できます。すべてのローカル ルート グループの名前をシステム レベルで定義した後、名前付きローカル ルート グループあたりのルート グループをデバイス プール レベルで設定できます。これによって、たとえば、緊急通話、国内 PSTN 宛先およびその他の宛先に使用する異なるローカル ルート グループを定義できます。複数のローカル ルート グループを使用することによって、異なるゲートウェイをさまざまなコールのタイプに選択することができます。たとえば、緊急通話に対してのみ使用すべき小規模な PSTN ゲートウェイがある小規模サイトで、その小規模サイトの PSTN コールが主要なハブの PSTN リソースを使用する必要がある場合は、次のローカル ルート グループの設定を使用することもできます。

サイト	[ローカルルートグループ(Local Route Groups)]	
	LRG_PSTN	**LRG_Emergency**
SJC(ブランチ)	RG_SFO	RG_SJC
OAK(ブランチ)	RG_SFO	RG_OAK
SFO(ハブ)	RG_SFO	RG_SFO
TPA(ブランチ)	RG_MCO	RG_TPA
MIA(ブランチ)	RG_MCO	RG_MIA
MCO(ハブ)	RG_MCO	RG_MCO

この例では、主要なハブ（SFO または MCO）のゲートウェイは、ハブに関連付けられたハブ サイトとブランチ サイトのユーザによって PSTN コールに使用され（SJC および OAK は SFO、TPA および MIA は MCO を使用）、緊急通話は常にローカル PSTN リソースを使用します。

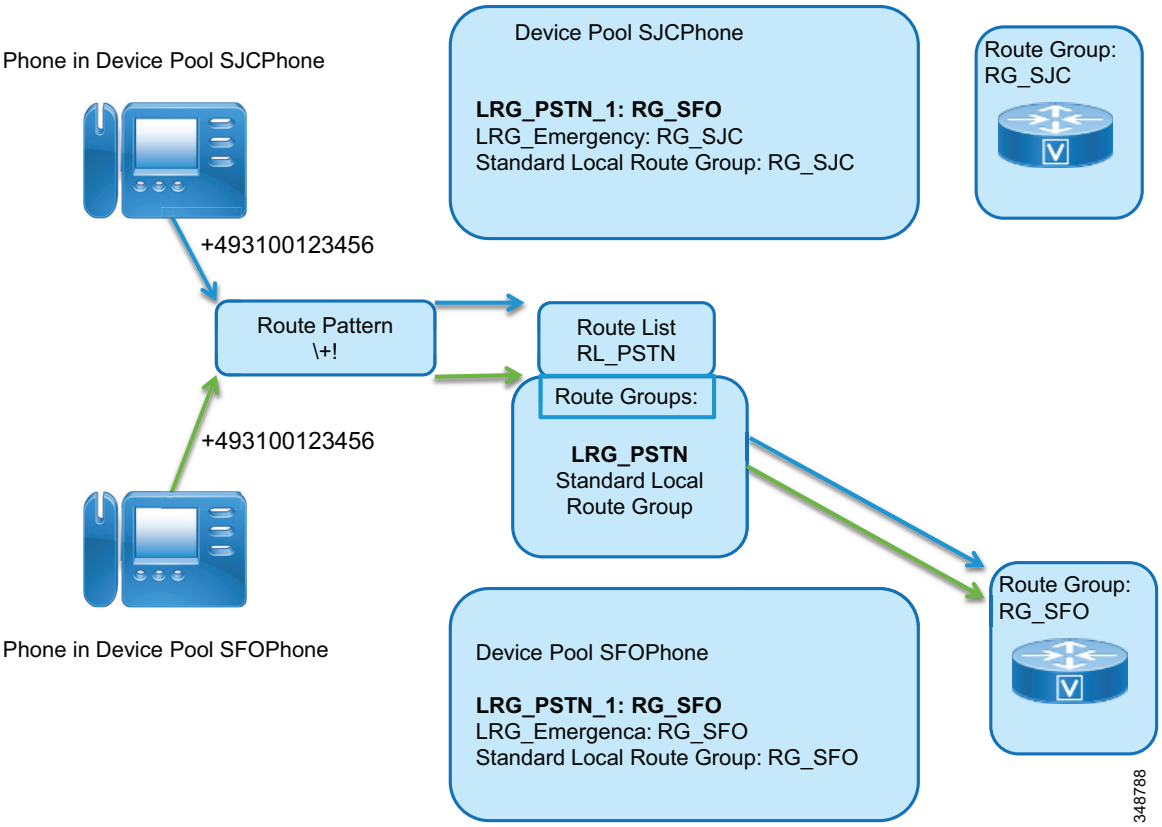
図 14-18 に緊急通報のコール ルーティングとローカル ルート グループの選択を示します。緊急ルート パターンによって使用されるルート リスト RL_911 には、最初のルート グループ エントリとして LRG_Emergency があります。ルート リストの 2 番目のエントリは標準ローカル ルート グループを参照し、デバイス プールで定義されたデフォルト PSTN リソースがフェールオーバーとして選択されていることを確認します。緊急通話が発信され、ルート リスト エントリ LRG_Emergency が選択されるたびに、Unified CM はプレースホルダ LRG_Emergency の参照を解除し、代わりに発信側デバイスのデバイス プールで LRG_Emergency に設定したルート グループを使用します。緊急通報用のサイト SFO および SJC の電話、ローカル PSTN ゲートウェイがどのように選択されるかを例に示します。

図 14-18　　複数のローカル ルート グループによる緊急通報ルーティング



同様の概念を利用して、サイトに依存しない PSTN ルート パターンは LRG_PSTN を使用するルート リストを指すように定義できます。LRG_PSTN は、名前付きローカル ルート グループ LRG_PSTN のデバイス プール レベルで定義されたルート グループへの参照が解除されます。サイト SJC および SFO からの PSTN コールが、デバイス プール ローカル ルート グループ設定に基づいて、どのようにサイト SFO の中央 PSTN ゲートウェイにルーティングされるかを図 14-19 に示します。

図 14-19　　複数のローカル ルート グループによる PSTN コール ルーティング



未定義のローカル ルート グループは、出力ルーティング デバイスの選択中にスキップされます。ルート リストに、発信側デバイスのデバイス プールにルート グループが割り当てられていないローカル ルート グループが含まれていると、ルート リストのこのエントリはスキップされ、ルート リストの次のルート グループのメンバーが考慮されます。ローカル ルート グループのみを含むルート リストを使用する場合、実ルート グループに一度も到達せずルート リストが枯渇することによって出力コールがドロップされないよう、すべての発信元デバイスのすべてのデバイス プールで一貫してルート グループを定義することが重要です。

すべてのルート リストの最後のエントリとして常に標準ローカル ルート グループを使用し、すべてのデバイス プールで標準ローカル ルート グループのルート グループが選択されるようにすることは、上記のルート リストの枯渇の問題を回避するための安全対策メカニズムとして使用できます。

緊急パターン

トランスレーション パターン、ルート パターン、DN は緊急パターンとして設定できます。緊急パターンのデフォルト値は、トランスレーション パターンでは緊急、ルート パターンと DN では非緊急になります。ルート パターン、トランスレーション パターン、DN の緊急パターンのみが設定できます。他のパターンは、すべて非緊急状態になります。

パターンを緊急としてマーキングすることは、一般に、パターンに一致したコールを T302 タイマーの満了を待たずにすぐにルーティングする目的で使用されます。たとえば、北米でパターン 9.911 と 9.[2-9]XXXXXX が設定されている場合、ユーザが 9911 をダイヤルすると、Unified CM は T302 タイマーが終了するまで待機し、その後でコールをルーティングします。これは、9911 の後に数字が入力されると、パターン 9.[2-9]XXXXXX に一致する場合があるためです。9.911 ルート パターンについて緊急プライオリティを有効にすると、Unified CM はユーザが 9911 とダイヤルした直後にルーティング処理を実行し、T302 タイマーの満了までは待機しません。

パターンを緊急にすると、設定済みのパターンがダイヤルされた番号とのベストマッチになったとき、その直後に T302 タイマーが満了します。つまり、緊急パターンが他のパターンよりも高い優先順位を持っているわけではありません。Unified CM におけるコール ルーティング（14-23 ページ）の項で説明した closest-match ロジックは、依然として有効です。

たとえば、ルート パターン 1XX が緊急パターンとして設定され、パターン 12! が非緊急のルート パターンとして設定されているとします。ユーザが 123 をダイヤルした場合、Unified CM は 3 番めの数字を受信した直後にルーティングの判断を実行しません。これは、1XX は緊急パターンであっても、ベストマッチではないからです（12! が合計 10 個のパターンに一致するのに対して、1XX は 100 個のパターンに一致）。パターン 12! では、ユーザがさらに番号を入力できるため、Unified CM は桁間タイムアウトを待ってから、コールをルーティングする必要があります。

別の例として、パターン 12[2-5] に緊急のマークが付けられ、12! が非緊急パターンとして設定されているとします。ユーザが 123 とダイヤルすると、パターン 12[2-5] はベストマッチになります（12[2-5] が合計 4 個のパターンに一致するのに対し、12! は 10 個のパターンに一致）。緊急プライオリティ パターンがベストマッチなので、T302 タイマーは打ち切られ、それ以上のユーザ入力は想定されません。Unified CM は、パターン 12[2-5] を使用してコールをルーティングします。

図 14-20 の 9011.! のような可変長緊急トランスレーション パターンは、桁間タイムアウトを強制しません。ダイヤルされた番号が受信され、数字ごとに分析されて、緊急トランスレーション パターンが唯一の一致（またはベストマッチ）になるとすぐに、トランスレーション パターンで定義された番号変換が実行され、トランスレーション パターンの CSS によって定義されるセカンダリ ルックアップがただちに実行されます。

図 14-20　緊急トランスレーションでの桁間タイムアウト

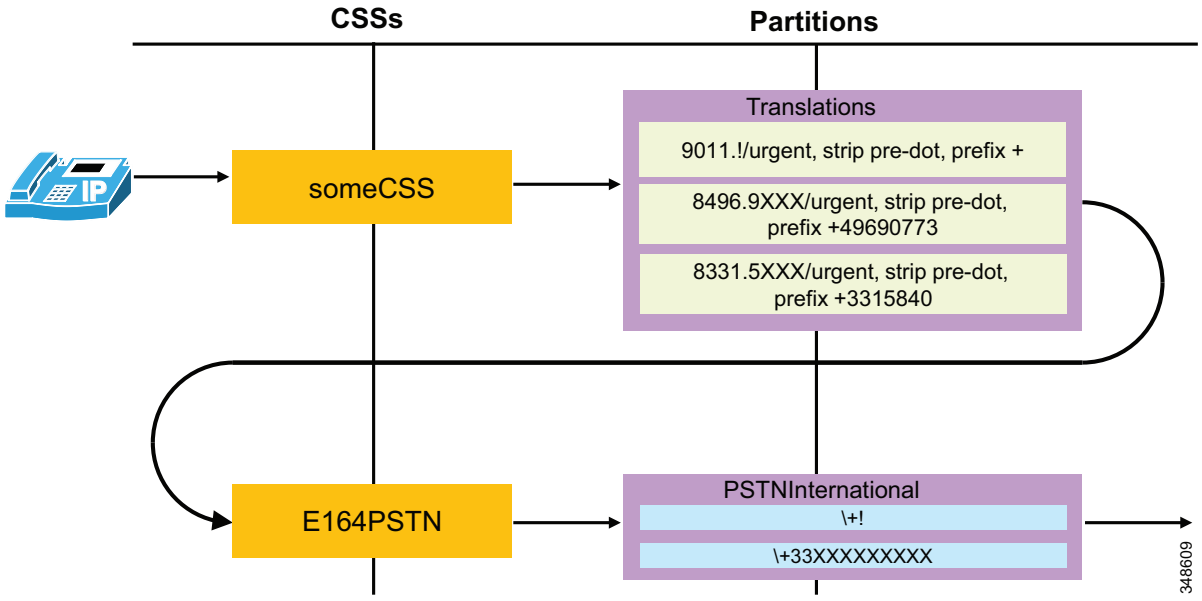


図 14-20 で示す設定がある場合、ユーザが 901133158405858 とダイヤルすると、コールは最後の数字がダイヤルされた直後にルーティングされます。コールはトランスレーション パターン 9011.! と一致し、ダイヤルされた番号は +3333158405858 に変換され（9011 が廃棄され、+ が前に付きます）、固定長の PSTN ルート パターン \+33XXXXXXXXX（フランスで使用される 9 桁の NSN）に一致します。

一方、ユーザが 9011496907739001 とダイヤルすると、桁間タイムアウトが発生します。9011.! との一致後、結果の番号 +496907739001 はルート パターン \+! に一致し、Unified CM は、発信者が以降の番号をダイヤルするつもりがないことを確認するために、次の番号を待機する必要があります。以降にダイヤルされた番号も同じルート パターンに一致します。

図 14-20 では、緊急トランスレーション パターンを使用して短縮オフネット ダイヤリング手順を実装するいくつかの例も示します。8 で始まる両方のトランスレーション パターンが 8 桁をそのまま受け入れ、ダイヤルされた番号を +E.164 にトランスフォームし、セカンダリ ルックアップを実行します。

83315858 にダイヤリングすると、桁間タイムアウトなしで、すぐにルーティングされます。ダイヤルされた番号は固定長のトランスレーション パターン 8331.5XXX と一致し、変換された着信者番号 +33158405858 は固定長のルート パターン \+33XXXXXXXXX に一致します。

ただし、84969001 にダイヤリングしても、デフォルトではただちにルーティングされません。ダイヤルされた番号が固定長のトランスレーション パターン 8496.9XXX に一致し、変換された着信者番号 +496907739001 は可変長の PSTN ルート パターン \+! に一致します。この例は、中間トランスレーションパターン一致の緊急パターンでも固定長でもない特性が、中間トランスレーション パターンに設定されている CSS によって定義されたセカンダリ ルックアップで継承されることを示します（E164PSTN）。セカンダリ ルックアップで一致するルート パターンが可変長パターンのため、桁間タイムアウトを待機するように Unified CM が強制されます。中間トランスレーション パターンが固定長のトランスレーション パターンである場合は、これ以上の数字によって中間トランスレーション パターンが一致しない状態になるため、以降の数字をセカンダリ ルックアップで待機してもあまり意味を成しません。したがって、固定長のトランスレーション パターンに対しては、セカンダリ ルックアップでの桁間タイムアウト処理を変更することが適切です。そのためには、トランスレーション パターンのオプション [後続のホップで番号間タイムアウトを待機しない（Do Not Wait For Interdigit Timeout On Subsequent Hops）] を設定する必要があります。このオプションが設定されている場合、トランスレーション パターンに一致すると、Unified CM はそれ以上の数字を待機せず、中間トランスレーション パターンで定義された CSS によって識別されたパターンに対して、変換された着信者番号を照合します。原則として、[後続のホップで番号間タイムアウトを待機しない（Do Not Wait For Interdigit Timeout On Subsequent Hops）] はすべての固定長トランスレーション パターンで有効にする必要があります。

[後続のホップで番号間タイムアウトを待機しない（Do Not Wait For Interdigit Timeout On Subsequent Hops）] オプションのその他の一般的な使用例は、桁間タイムアウトを回避するために番号収集を終了させる特殊キーを使用する、ダイヤリング正規化トランスレーション パターンのセカンダリ ルックアップです。たとえば、米国ダイヤル プランで終了文字 # を持つ国際間宛先を照合するダイヤリング正規化トランスレーション パターン（9011.!# など）は、可変長国際ダイヤリングと一致することができ、ユーザは # を押すことでダイヤリングを終了することができます。このトランスレーション パターンのセカンダリ ルックアップは通常、\+[^1]! などの可変長ルート パターンで一致し、このセカンダリ ルックアップの一致でも番号分析が行われ、追加の番号が待機されます。この場合も、このタイムアウトを避けるための最も簡単な方法は、ダイヤリング正規化トランスレーション パターン 9011.!# で [後続のホップで番号間タイムアウトを待機しない（Do Not Wait For Interdigit Timeout On Subsequent Hops）] オプションを設定することです。

発信側および着信側トランスフォーメーション パターン

発信側トランスフォーメーション パターンを使用すると、発番号のグローバル形式を、ゲートウェイ、トランクなどのルート グループ デバイスに接続されているオフクラスタ ネットワークで必要となるローカル形式に適応させることができます。

着信側トランスフォーメーション パターンを使用すると、着番号のグローバル形式を、ゲートウェイ、トランクなどのルート グループ デバイスに接続されているオフクラスタ ネットワークで必要となるローカル形式に適応させることができます。

(注)　着信側トランスフォーメーション パターンは、電話機に影響を与えません。また、デバイス プールの着信側トランスフォーメーション パターン CSS も、そのパターンが割り当てられている電話機に影響を与えません。

両方のトランスフォーメーション パターン タイプは、一致する発番号または着番号の数値表現で構成されます。使用される構文は、ルート パターン、トランスレーション パターン、ディレクトリ番号などのその他パターンの構文と同じです（図 14-21 を参照）。

変換演算子には、数字破棄命令（ドット前の番号など）、発信側トランスフォーメーション マスク、プレフィックス番号が含まれます。この演算子によって、発信側電話番号表示（Default、Allowed、または Restricted）が制御されます。発信側トランスフォーメーション パターンを設定することで、発信側の外部電話番号マスクを発番号として使用できます。

パーティションおよびコーリング サーチ スペースによって、どの発信側トランスフォーメーション パターンをどのゲートウェイまたはトランクに適用するかどうかが制御されます。ゲートウェイまたはトランクでは、関連するデバイス プールの発信側変換 CSS またはデバイス固有の発信側変換 CSS を優先順位の低い順に使用できます。同じメカニズムを使用して、着信側トランスフォーメーション パターンの適用を制御します。

[Call Routing Information] > [Outbound Calls] の [Gateway Configuration] ページで設定された発信側および着信側トランスフォーメーション パターンは、ゲートウェイに送信される発番号または着番号と、発信側または着信側の番号タイプおよび番号計画に影響します。[着信側の設定（Incoming Calling Party Settings）] で適用される発信側および着信側トランスフォーメーション パターンは、ゲートウェイから送信されるコールに適用されます。

図 14-21　発信側および着信側トランスフォーメーション パターン

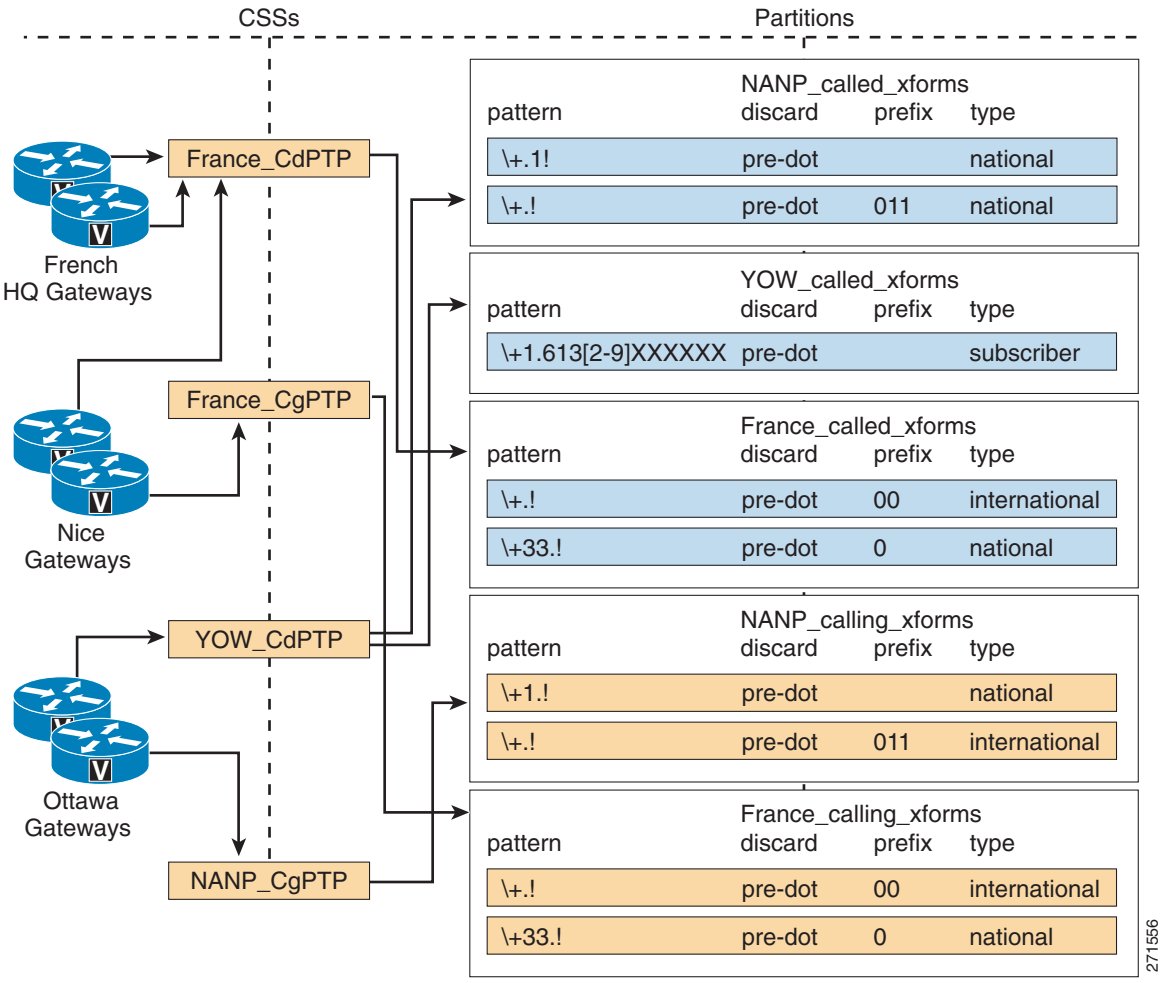


図 14-21 は、発信側および着信側トランスフォーメーション パターンを、さまざまな PSTN で PSTN に接続しているゲートウェイの異なるグループに適用する方法を示しています（フランスおよび NANP エリア）。

北米番号計画（NANP）では、カナダの Ottawa（空港コード YOW）にあるゲートウェイは、パーティション NANP_calling_xforms が含まれている、発信側変換 CSS NANP_CgPTP に割り当てられます。発番号が +1 で始まる（つまり、NANP 内から発信される）コールは、パーティション NANP_calling_xforms 内で設定されている両方のパターンに一致します。best-match ロジックの後、最初のパターンが選択され、発番号から + 記号と NANP 国コード 1 が削除されます。残りの発番号部分は PSTN に送信される発番号として使用され、番号タイプは National に設定されます。

たとえば、+1 613 555 1234 からのコールを YOW ゲートウェイに送信した場合、その発番号は 613 555 1234 に変換され、番号タイプは National に設定されます。

同じ発信側からのコールをフランスにあるゲートウェイに送信した場合には、一連の異なる発信側トランスフォーメーション パターンが適用されます。たとえば、+1 613 555 1234 からのコールをフランスの Nice（空港コード NCE）にあるゲートウェイに送信した場合、パーティション France_calling_xforms に含まれている発信側トランスフォーメーション パターンが適用されます。この場合、発番号は 001 613 555 1234 に変換され、番号タイプは International に設定されます。

(注)　コールをゲートウェイに送信すると、発番号変換が無効になることがあります。多くのサービス プロバイダーでは、現地のサービス契約や規制で定められているように、特定の範囲外で発番号を使用することを許可していません。

同じプロセスは、着番号トランスフォーメーション パターンにも適用されます。Ottawa ゲートウェイの場合、割り当てられた受信側変換 CSS は YOW_CdPTP です。これは、パーティション NANP_Called_xforms および YOW_Called_xforms に含まれています。番号計画エリア 613 内の宛先番号に発信されるコールは、これらの 2 つのパーティションに含まれているすべてのパターンに一致します。ただし、ベストマッチ プロセスによってパターン \+1.613[2-9]XXXXXX が選択されます。

たとえば、Ottawa ゲートウェイ経由で +1 613 555 9999 にコールを発信すると、着番号は 516 555 9999 に変換され、番号タイプは Subscriber に設定されます。

着信側の設定（ゲートウェイまたはトランク別）

個々のゲートウェイまたはトランクで、優先順位に従ってデバイス プール レベルまたはサービス パラメータ レベルで着信側の設定を行うことができます。各番号タイプ（Subscriber、National、International、または Unknown）には、Unified CM で適切なプレフィックス番号を設定できます。デバイス プール、ゲートウェイまたはトランク設定では、削除桁数の方法の定義と、発信側トランスフォーメーション パターンに基づいた柔軟な変換が可能なため、サービス パラメータ設定の使用は推奨されません。さらに、番号を削除したり、着番号として指定した番号にプレフィックス番号を付けたりできます。最初に番号削除操作が着信側の番号で実行され、次にその結果の番号にプレフィックス番号が付加されます。たとえば、削除する桁数を 1 に設定し、プレフィックス番号を +33 と設定し、着信側の番号が 01 58 40 58 58 である場合、+33 1 58 40 58 58 となります。

発信側トランスフォーメーション パターンをコールに適用するために使用するコーリング サーチ スペースを各番号タイプに設定できます。コーリング サーチ スペースには、発信側トランスフォーメーション パターンだけが存在するパーティションが保持される必要があります。これによって、厳密に番号タイプに基づくのではなく、発番号の構造に基づいた変更を発番号に適用できます。発信側トランスフォーメーション パターンでは、正規表現を使用して発番号が照合されます。複数の一致項目から選択するには、best-match プロセスが使用され、選択されたパターンの発信側トランスフォーメーションがコールに適用されます。

着信の着呼側設定（ゲートウェイまたはトランク別）

前のセクションで説明されている着信側の設定と同じで、着信の着呼側の変換も設定できます。これらの着信の着信側トランスフォーメーションによって、コールを実際にルーティングする前に、着信の着呼側の情報を正規化できます。

着信側トランスフォーメーション パターンをコールに適用するために使用するコーリング サーチ スペースを各番号タイプに設定できます。コーリング サーチ スペースには、着信側トランスフォーメーション パターンだけが存在するパーティションが保持される必要があります。これによって、厳密に番号タイプに基づくのではなく、着信者番号の構造に基づいた変更を着信者番号に適用できます。着信側トランスフォーメーション パターンでは、正規表現を使用して着信者番号が照合されます。複数の一致項目から選択するには、best-match プロセスが使用され、選択されたパターンの着信側トランスフォーメーションがコールに適用されます。

Unified CM におけるコール特権

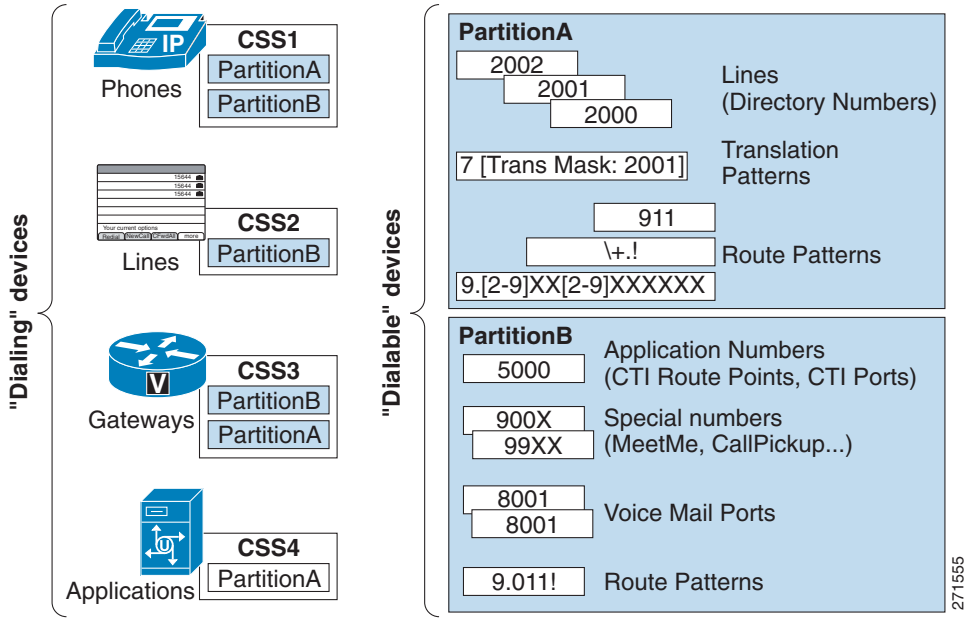
ダイヤリング特権は、特定のエンドポイント（電話、ゲートウェイ、または CTI アプリケーションなど）にどのタイプのコールを許可する（または禁止する）かを制御するために設定されます。Unified CM で処理されるすべてのコールは、次の要素の設定で実装されたダイヤリング特権の対象になります。

- パーティション（14-45 ページ）
- コーリング サーチ スペース（14-46 ページ）

*パーティション*は、同様のアクセシビリティを持つディレクトリ番号（DN）またはディレクトリ URI のグループです。*コーリング サーチ スペース*は、特定のデバイスからどのパーティションがアクセス可能であるかを指定します。デバイスは、コーリング サーチ スペースに含まれているパーティション内の DN およびディレクトリ URI だけを呼び出すことができます。

図 14-22 に示すように、パーティション内に配置できるすべての項目は、ダイヤリングの対象となるパターンを持っています。このような項目としては、電話回線、ルート パターン、トランスレーション パターン、CTI ルート グループ回線、CTI ポート回線、ボイスメール ポート、および Meet-Me 会議番号があります。逆に、コーリング サーチ スペースを持つ項目は、コールをダイヤルできるすべてのデバイスです。たとえば、電話機、電話回線、ゲートウェイ、アプリケーション（CTI ルート グループまたはボイスメール ポート経由）などです。

図 14-22　パーティションとコーリング サーチ スペース

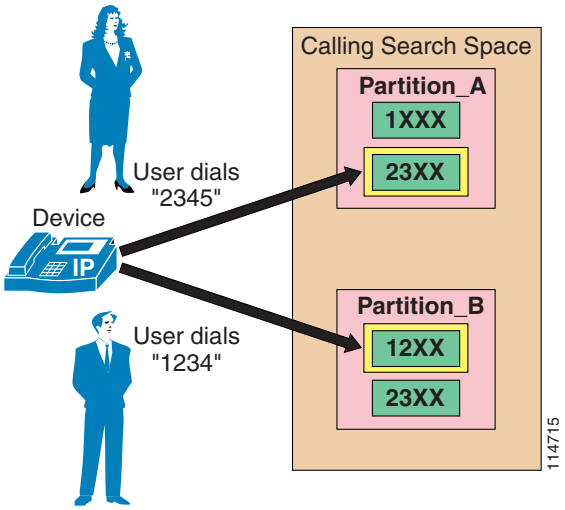


パーティション

パーティションに含めることができるダイヤル プラン項目には、IP Phone のディレクトリ番号、ディレクトリ URI、トランスレーション パターン、ルート パターン、CTI ルート ポイント、およびボイスメール ポートがあります。Unified CM におけるコール ルーティング（14-23 ページ）で説明するように、複数の数値のダイヤル プラン項目（ディレクトリ番号、ルート パターンなど）が重複する場合、Unified CM は、ダイヤルされた番号と一致するか、または最も近い（最も固有性の高い一致）項目を選択します。2 つのダイヤル プラン項目が、ダイヤルされたパターンに等しく一致した場合、Unified CM は、コールを発信するデバイスのコーリング サーチ スペース内で最初に表示されているダイヤル プラン項目を選択します。ディレクトリ URI は、常に完全に一致している必要があります。ディレクトリ URI に部分一致の概念はありません。

たとえば、図 14-23 について考えます。ルート パターン 1XXX と 23XX はパーティション A の一部であり、ルート パターン 12XX と 23XX はパーティション B の一部です。発信側デバイスのコーリング サーチ スペースには、パーティション A:パーティション B の順にパーティションがリストされています。このデバイスのユーザが 2345 をダイヤルすると、Unified CM では、パーティション A のルート パターン 23XX を一致項目として選択します。これは、このパターンが発信側デバイスのコーリング サーチ スペースで最初に示されているためです。ただし、ユーザが 1234 をダイヤルした場合には、Unified CM ではパーティション B のルート パターン 12XX を一致項目として選択します。これは、パーティション A の 1XXX よりも一致率が大きいためです。コーリング サーチ スペースに含まれているパーティションの順序は、closest-match ロジックに基づいて均等一致項目が複数あった場合に、競合を解消する要素としてのみ使用されます。

図 14-23　　マッチング ロジックにおけるパーティション順序の影響



（注） 均等一致項目が同じパーティションに複数ある場合、Unified CM は、ローカルのダイヤル プラン データベース内で最初にリストされている項目を選択します。ダイヤル プラン データベース内でダイヤル プラン項目がリストされる順序は、設定することができません。したがって、同じパーティション内で均等一致項目が共存しないようにすることを強く推奨します。これはこのような場合に発生するダイヤル プラン ロジックが予測できないからです。

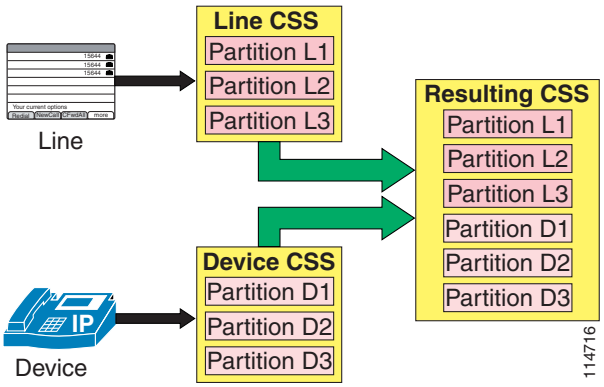
日時に基づいてパーティションをアクティブまたは非アクティブにできます。パーティションをアクティブまたは非アクティブにするには、まず、Unified CM Administration で期間とスケジュールを設定し、次に個々のタイム スケジュールを各パーティションに割り当てます。スケジュールに指定した日時の範囲外では、このパーティションは非アクティブになります。このパーティションに含まれているパターンは、Unified CM コール ルーティング エンジンによってすべて無視されます。この機能の詳細については、時間帯ルーティング（14-97 ページ）を参照してください。

コーリング サーチ スペース

コーリング サーチ スペースは、特定のデバイスからどのパーティションがアクセス可能であるかを指定します。所定のコーリング サーチ スペースが割り当てられるデバイスは、そのコーリング サーチ スペースにリストされているパーティションだけにアクセスできます。そのコーリング サーチ スペース以外のパーティション内の DN またはディレクトリ URI へのダイヤルは失敗します。発信者にはビジー信号が聞こえます。

IP Phone 回線とデバイス（電話機）自体の両方でコーリング サーチ スペースを設定する場合、Unified CM は、この 2 つのコーリング サーチ スペースを図 14-24 に示すように連結し、デバイスのコーリング サーチ スペースの前に、回線のコーリング サーチ スペースを置きます。

図 14-24　IP Phone の回線とデバイスのコーリング サーチ スペース（CCS）の連結



（注）　デバイス モビリティを使用しない場合、デバイスのコーリング サーチ スペースは静的となり、デバイスをネットワークの別の場所に移動しても同じままです。デバイス モビリティを有効にした場合、電話機の IP アドレスによって決定されている、ネットワークで電話機が物理的に配置されている場所に基づいて、デバイスのコーリング サーチ スペースを動的に決定できます。詳細については、デバイス モビリティ（14-89 ページ）を参照してください。

同じパターンが、2 つのパーティション（回線のコーリング サーチ スペースに含まれているパーティションとデバイスのコーリング サーチ スペースに含まれているパーティション）に指定されている場合、Unified CM は、パーティション（14-45 ページ）の項で説明している規則に従って、パーティションの連結リスト内で最初にリストされているパターン（この場合、回線のコーリング サーチ スペースに関連したパターン）を選択します。

あらゆるコーリング サーチ スペースの最大長は、各パーティション名の区切り文字を含めて、1024 文字です。（たとえば、「partition_1:partition_2:partition_3」という文字列には 35 文字が含まれています）。そのため、コーリング サーチ スペース内のパーティションの最大数は、パーティション名の長さによって異なります。したがって、パーティションとコーリング サーチ スペースを作成するときは、コーリング サーチ スペースに含める予定のパーティション数を基準にして、パーティション名を短くしてください。コーリング サーチ スペースの設定の詳細は、次の Web サイトで入手可能なオンラインの『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

https://www.cisco.com

パーティションまたはコーリング サーチ スペースを設定する前に、すべての DN は、<None> という名前が付いた特別なパーティションに置かれ、すべてのデバイスには、<None> という名前が付いたコーリング サーチ スペースが割り当てられます。カスタム パーティションとコーリング サーチ スペースを作成する場合は、作成するどのコーリング サーチ スペースにも、<None> パーティションが含まれています。一方、<None> コーリング サーチ スペースには、<None> パーティション*だけ*が入っています。

（注） <None> パーティションに残っているどのダイヤル プラン項目も、コールを発信する*任意*のデバイスから暗黙的に到達可能です。したがって、予期しない結果を避けるために、<None> パーティションにダイヤル プラン項目を残さないように強く推奨します。

（注） <None> と定義されたままのコーリング サーチ スペースを残さないでください。そのままにしておくと、ダイヤル プランの動作が予測困難になる可能性があります。

トランスフォーメーション パターンの特別な考慮事項

発信側および着信側トランスフォーメーション パターンは、パーティションにも配置されます。それらのパーティションは、コーリング サーチ スペース（CSS）に含まれますが、コール特権を制御するためのものではありません。トランスフォーメーション パターンのパーティションの役割は、どの変換をどのゲートウェイ、トランク、または電話機に適用するかを選択することです。発信側トランスフォーメーション パターン CSS に含まれるパーティションには、発信側トランスフォーメーション パターンのみが含まれていなければなりません。同様に、着信側トランスフォーメーション パターン CSS に含まれるパーティションには、着信側トランスフォーメーション パターンのみが含まれていなければなりません。

自動転送コーリング サーチ スペース

（注） この機能が電話機によってアクティブになっている場合、Call Forward All 動作は、宛先番号が個々のユーザによって入力されるその他の自動転送動作とは異なります。

自動転送コーリング サーチ スペースを有効にする方法を決定できます。Calling Search Space Activation Policy（コーリング サーチ スペースのアクティベーション ポリシー）によって指定されている、選択可能なオプションは次の 3 つです。

- [システムデフォルトの使用（Use System Default）]

  Calling Search Space Activation Policy を Use System Default に設定した場合、クラスタ全体のサービス パラメータである CFA CSS Activation Policy によって、使用される Forward All コーリング サーチ スペースが決定されます。CFA CSS Activation Policy サービス パラメータを With Configured CSS または With Activating Device/Line CSS に設定できます（下記を参照してください）。デフォルトでは、CFA CSS Activation Policy サービス パラメータは With Configured CSS に設定されています。

- With Configured CSS

  With Configured CSS オプションを選択した場合、Directory Number Configuration ウィンドウで明示的に設定されている Forward All コーリング サーチ スペースと Forward All のセカンダリ コーリング サーチ スペースによって、不在転送のアクティブ化と自動転送が制御されます。Forward All コーリング サーチ スペースを None に設定した場合、Forward All に対して CSS は設定されません。そのため、パーティションおよびディレクトリ番号に対する不在転送のアクティブ化の試行は失敗します。不在転送のアクティブ化中に、Forward All コーリング サーチ スペースおよび Forward All のセカンダリ コーリング サーチ スペースの変更は発生しません。

- With Activating Device/Line CSS

  Forward All コーリング サーチ スペースを明示的に設定せずに、ディレクトリ番号のコーリング サーチ スペースとデバイスのコーリング サーチ スペースの組み合わせを使用する場合には、Calling Search Space Activation Policy に対して With Activating Device/Line CSS を選択します。Forward All が電話機によってアクティブになっている場合にこのオプションを選択すると、Forward All コーリング サーチ スペースと Forward All のセカンダリ コーリング サーチ スペースに、ディレクトリ番号のコーリング サーチ スペースとアクティブ化デバイスのデバイス コーリング サーチ スペースが自動的に入力されます。Unified CM Administration から宛先への Forward All を設定した場合、Forward All コーリング サーチ スペースとセカンダリ コーリング サーチ スペースは自動的にはデータが格納されず、明示的に設定しなければなりません。その 2 つのコーリング サーチ スペースが連結され、連結されたコーリング サーチ スペースを使用することで、不在転送宛先として入力されている番号を検証します。

  不在転送が電話機によってアクティブになっているときに、Forward All コーリング サーチ スペースを None に設定した場合にこの設定（Calling Search Space Activation Policy を With Activating Device/Line に設定）を使用すると、ディレクトリ番号のコーリング サーチ スペースとアクティブになっているデバイス コーリング サーチ スペースを使用することで、不在転送の試行を検証します。

SIP を実行しているタイプ A の IP Phone では、Call Forward All がその電話機自体から起動された場合、転送されるコールにデバイスの Rerouting Calling Search Space が使用されます。Forward All 動作が [Unified CM User] ページまたは [Unified CM Administrative] ページから起動される場合、その電話機から開始される Forward All 動作とは無関係になります。

たとえば、SIP を実行するタイプ A の IP Phone に、[Unified CM] ページで内線 3000 への Forward All が指定されているとします。同時に、その電話機自体には、内線 2000 への Forward All が設定されています。この場合、その電話機に対するすべてのコールは、内線 3000 に転送されます。

（注）　SIP を実行するタイプ A の IP Phone では、[Unified CM User] ページまたは [Administrative] ページからの Forward All の起動は、電話機に反映されません。電話機には、コールの転送に関する確認は何も表示されません。

SCCP を実行する IP Phone または SIP を実行するタイプ B の IP Phone から Forward All が起動された場合、ユーザ入力は入力と同時に、設定済みの Forward All コーリング サーチ スペースの中で許可されるパターンと比較されます。無効な宛先パターンが設定されていると、ユーザにはリオーダー トーンが聞こえます。SIP を実行するタイプ A の IP Phone から Forward All が起動された場合、Forward All ユーザ入力は電話機上にローカルに保管され、Unified CM 内のコーリング サーチ スペースとは照合されません。ユーザ入力が無効な宛先に対応している場合でも、ユーザへの通知はありません。その電話機へのコールに対しては、電話機が無効な宛先番号に対して SIP 再ルーティング動作を開始しようとしたときに、リオーダー トーンが再生されます。

その他の自動転送タイプ

さまざまな自動転送タイプ（Forward Busy、Forward No Answer、Forward No Coverage、Forward on CTI Failure、Forward Unregistered）に対して設定されているコーリング サーチ スペースは、他のどのコーリング サーチ スペースとも連結されないスタンドアロン値です。

Call Forward 設定（Forward All を除く）は、内部または外部のコール タイプ別に設定できます。たとえば、電話機で外部発信者のボイスメールに Call Forward No Answer を設定しても、発信者がネットワーク上の別の IP Phone から発信している社員である場合には、ボイスメールを携帯電話番号に転送できます。これを可能にするには、内線と外線の Call Forward 設定に対して、異なる設定を使用します。

Forward All コーリング サーチ スペースが <None> のままになっている場合、処理の結果は Unified CM のリリースによって異なり、予想することは困難です。このため、自動転送コーリング サーチ スペースを設定する場合は、次のベスト プラクティスに従うことを推奨します。

- 自動転送コーリング サーチ スペースは、常に <None> 以外の値を使用して設定する。この設定により混乱を避けることができ、トラブルシューティングが容易になります。転送されるコールにどのコーリング サーチ スペースが使用されるかについて、ネットワーク管理者が正確に把握できるためです。
- Call Forward Busy コーリング サーチ スペースと Call Forward No Answer コーリング サーチ スペースは、ボイスメール パイロットおよびボイスメール ポートの DN に到達可能で、かつ外部 PSTN 番号以外の値を使用して設定する。
- Call Forward All コーリング サーチ スペースと Forward All のセカンダリ コーリング サーチ スペースは、どちらも企業のポリシーに従って設定する。多くの企業では、コールを社内の番号にしか転送できないように制限しています。この方法によって、ユーザが IP Phone の回線を長距離電話の番号に転送したり、私用電話の長距離通話料金がかからないようにするためにローカル IP Phone の番号に PSTN からダイヤルしたりすることを防止します。

Call Forward Unregistered（CFUR）機能は、一時的に登録から外されている宛先の電話機に発信されたコールを再ルーティングする手段です。CFUR の設定は、主に次の 2 つの要素で構成されます。

- 宛先の選択

  DN が登録から外されているときに、コールを次のいずれかの宛先に再ルーティングできます。

  - [ボイスメール（Voicemail）]

    ボイスメールのチェックボックスをオンにし、CFUR コーリング サーチ スペースを設定して、ボイスメールのパイロット番号を含めることで、コールをボイスメールに送信できます。

  - PSTN を経由した電話機への到達に使用するディレクトリ番号

このアプローチが適切となるのは、WAN リンクがダウンするサイト内に電話機がある場合です。そのサイトに Survivable Remote Site Telephony（SRST）が装備されている場合は、電話機（および同じ場所にある PSTN ゲートウェイ）が同じ場所にある SRST ルータに再登録されます。その後、電話機は、その PSTN DID 番号に発信されたコールの受信を行うことができます。

この場合、適切な CFUR 宛先は、対応する元の宛先 DN の PSTN DID 番号です。宛先フィールドにこの PSTN DID を設定します。+ 記号を含む E.164 形式で設定することを推奨します（たとえば、+1 415 555 1234）。これによって、同じオフネット アクセス コードと PSTN プレフィックスを登録から外された電話機として使用するかどうかに関係なく、発信側電話機のローカル ルート グループによる CFUR 宛先の処理が可能になります。

- コーリング サーチ スペース

  Unified CM では、着信側 DN の CFUR コーリング サーチ スペースを使用することで、設定済みの宛先番号へのコールのルーティングを試行します。CFUR コーリング サーチ スペースは、対象の電話機に設定され、登録から外されている電話機に発信するすべてのデバイスで使用されます。つまり、すべての発信側デバイスでは、ルート パターン、ルート リスト、ルート グループの同じ組み合わせを使用して、コールを発信します。標準ローカル ルート グループを参照するルート リストを指すパターンを使用して、コールを CFUR 宛先にルーティングするために、CFUR コーリング サーチ スペースを設定することを推奨します。これによって、発信側デバイスに基づいて PSTN への出口ゲートウェイが選択されるようになります。

電話機が単にネットワークから切断されている場合と同様に、電話機が登録から外されている一方で、電話機の DID 番号に関連付けられているゲートウェイが依然として Unified CM の制御下にある場合に、Call Forward Unregistered 機能を使用すると、テレフォニー ルーティング ループが発生することがあります。このような場合、電話機への初期化コールによって、電話機の DID への最初のコールが PSTN 経由で試行されます。次に、同じ電話機の DN に到達するために、その結果の着信 PSTN コールによって、別の CFUR 試行がトリガーされ、さらに、PSTN を経由して PSTN の中央ゲートウェイから別の CFUR コールがトリガーされます。システム リソースが使い果たされるまで、このサイクルが繰り返されます。

サービス パラメータ **MaximumForwardUnRegisteredHopsToDn** によって、DN に対して同時に許可される CFUR コールの最大数が制御されます。デフォルト値 0 は、カウンタが無効であることを意味します。PSTN 経由で CFUR を再ルーティングするように DN を設定した場合には、ループを防止する必要があります。このサービス パラメータを値 1 に設定すると、CFUR のメカニズムで 1 つのコールを発信するとすぐに、CFUR 試行が停止されます。CFUR が設定されている場合には、この設定によって、1 つのコールだけをボイスメールに転送することも可能です。このサービス パラメータを値 2 に設定すると、最大 2 人の同時発信者が、ボイスメールに対して CFUR 設定が設定されている DN のボイスメールに到達でき、CFUR 設定によって PSTN を経由してコールが送信される DN に対して、発生する可能性があるループを 2 つに制限できます。

（注）　Call Forward Unregistered コールを DN に関連付けられている PSTN DID に送信するために、エクステンション モビリティの DN を設定しないでください。ログアウト状態になっている、エクステンション モビリティ プロファイルの DN は登録から外されていると見なされます。そのため、ログアウト状態の DN の PSTN DID 番号へのコールによって、ルーティング ループがトリガーされます。ログアウト状態になっている、エクステンション モビリティの DN へのコールがボイスメールに確実に送信されるように、対応する Call Forward Unregistered パラメータを設定してコールがボイスメールに送信されることを確認します。

グローバル ダイヤル プラン レプリケーション

グローバル ダイヤル プラン レプリケーション（GDPR）により、独立した Unified CM クラスタはクラスタ間検索サービス（ILS）を使用して URI、+E.164 番号、エンタープライズ番号、+E.164 パターン、エンタープライズ パターン、PSTN フェールオーバー番号などのダイヤル プラン要素を共有できます。Unified CM クラスタからアドバタイズされたすべてのローカル ダイヤル プラン情報は、単一 GDPR カタログの一部としてアドバタイズされます。アドバタイズされたダイヤル プラン要素の到達可能性は、各 GDPR カタログとともにロケーション属性（SIP ルート文字列）をアドバタイズすることで実現されます。

エンタープライズ固有の番号とパターンは、オンネット サイト間の短縮ダイヤルを許可するグローバルなエンタープライズ固有のダイヤリング手順を表します。GDPR を通じて交換されるエンタープライズ固有の番号とパターンは、グローバルに有効である必要があります。E.164 番号付け方式の特性に基づいた +E.164 番号とパターンは、定義上、グローバルに有効です。

マルチ クラスタ環境におけるこのロケーション属性は、GDPR を介して学習した正しいクラスタへの任意の宛先に対するダイレクト コールに使用されます。確定的に SIP 要求をルーティングするためにディレクトリ URI のホスト部分を使用できない場合、ディレクトリ URI にこれを使用することができます。これは、たとえば、<user>@example.com などのフラットな URI スキームを使用する場合です。example.com というホスト部分は、特定の URI をホストするリモート Unified CM クラスタを一意に識別しませんが、適切に選択された SIP ルート文字列は識別します。

Unified CM 内の各 DN に対して、+E.164 代替番号やエンタープライズ代替番号は設定された DN に適用されるマスクに基づいて定義できます。これらの代替番号はローカル パーティションにオプションで追加できます。各代替番号は GDPR を使用してリモート クラスタにアドバタイズされるように個別に設定できます。

Unified CM 内の各 DN に対して、最大 5 つの URI をエイリアスとして定義できます。個別の URI はそれぞれ、GDPR を使用してリモート クラスタにアドバタイズされるように設定できます。

Unified CM 内の各 DN に対して、エンタープライズまたは +E.164 の代替番号を PSTN フェールオーバー番号としてアドバタイズするために選択できます。リモート クラスタで、この PSTN フェールオーバー番号は +E.164 の代替番号、エンタープライズ代替番号または URI へのコールの PSTN フェールオーバーに使用できます。PSTN フェールオーバーは、GDPR が学習した宛先へのコールが [未割り当ての番号（unallocated number）]、[ユーザがビジー（user busy）]、[通常のコールの消去（normal call clearing）]、[問題のある宛先（destination out of order）]、[サービス使用不可（service not available）] 以外の原因コードで失敗するとトリガーされます。PSTN フェールオーバー番号も、コール アドミッション制御に障害が発生した場合には、自動代替ルーティング（AAR）に使用されます。PSTN フェールオーバー番号へのコールの場合、発信側デバイスの AAR CSS は、リモート クラスタで使用されます。

DN の関連情報（ディレクトリ URI、エンタープライズ代替番号、+E.164 代替番号、PSTN フェールオーバー番号）に加えて、GDPR もエンタープライズ パターンと +E.164 パターンのアドバタイズを有効にします。パターンは DN に関連付けられていないため、ワイルドカードを使用して定義できます（固定長および可変長）。エンタープライズおよび +E.164 パターンの PSTN フェールオーバー番号は削除手順およびプレフィックス手順に基づいて定義されます。

GDPR はローカル ルーティング情報のアドバタイズを許可するだけでなく、URI、エンタープライズ パターンおよび +E.164 パターンを含むことのできるインポートされた GDPR カタログをサポートします。インポートされた GDPR カタログごとに、一意のロケーション属性（SIP ルート文字列）がアドバタイズされます。これにより、クラスタはローカル以外の宛先にルーティング情報を挿入できます。

受信側では、GDPR から学習されたすべてのディレクトリ URI は、数字以外の URI へのルーティングでローカル URI の一致が見つからない場合に参照される単一ローカル リポジトリに挿入されます。すべての学習された URI はサービス クラスの観点から同等として扱われます。

これとは異なり、GDPR が学習した数字パターンと番号は情報のタイプに基づいてローカル パーティションに挿入されます。4 つの独立したパーティションは +E.164 代替番号、エンタープライズ代替番号、+E.164 パターンとエンタープライズ パターンに設定できます。学習された情報の各タイプのデフォルト パーティションは、[グローバル学習 E164 番号（Global Learned E164 Numbers）]、[グローバル学習 E164 パターン（Global Learned E164 Patterns）]、[グローバル学習エンタープライズ番号（Global Learned Enterprise Numbers）]、[グローバル学習エンタープライズ パターン（Global Learned Enterprise Patterns）] です。GDPR を介して学習したリモートの宛先にダイヤルする場合、不要な桁間タイムアウトを回避するために、学習した宛先の緊急パターンをクラスごとに設定できます。

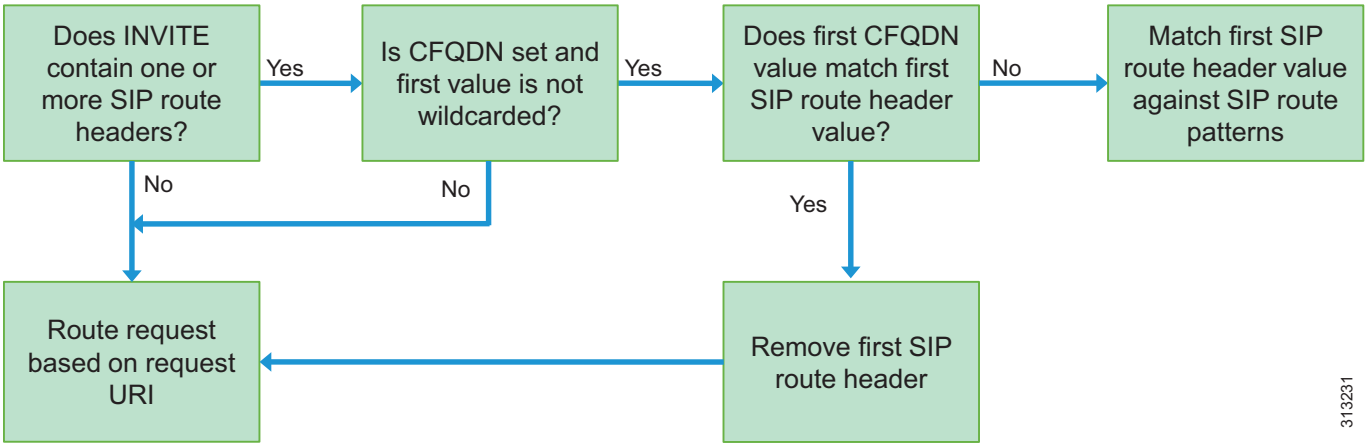
シスコでは、パターン**緊急**としてローカル番号分析に挿入される +E.164 番号と固定長 +E.164 パターンを設定することを推奨します。

ディレクトリ URI および GDPR を介して学習した数値の宛先へのコールのルーティング方法については、Unified CM での SIP 要求のルーティング（14-52 ページ）の項を参照してください。

Unified CM での SIP 要求のルーティング

SIP トランクまたは SIP エンドポイントから受信した SIP 要求のルーティングは、特定のルールに従い、ローカルとクラスタ間の両方のルーティング要件が満たされます。SIP 要求に SIP ルート ヘッダーが含まれている場合、Unified CM は図 14-25 に示されているように処理します。

図 14-25　SIP ルート ヘッダー ベースのルーティング



Unified CM は SIP 要求のリクエスト URI を分析する前に、SIP ルート ヘッダー（例：Route: <sip:ucm.example.com;lr>）の有無をチェックします。SIP ルート ヘッダーがなければ、Unified CM は SIP リクエスト URI に基づいて SIP 要求をルーティングします。

1 つ以上の SIP ルート ヘッダーが存在する場合、[クラスタ完全修飾ドメイン名（Cluster Fully Qualified Domain Name）]（CFQDN）エンタープライズ パラメータが設定されていて、このパラメータの最初の値がワイルドカードでなければ、Unified CM は最初の SIP ルート ヘッダーに含まれている最初のルート ヘッダー値をルーティング対象と見なします。Unified CM は、SIP ルート ヘッダー値に指定されているホスト（上記の例では、ucm.example.com）が [クラスタ完全修飾ドメイン名（Cluster Fully Qualified Domain Name）] エンタープライズ パラメータに指定されている最初のエントリと一致するかどうかをチェックします。一致する場合、Unified CM は最上位の SIP ルート ヘッダーを削除し、リクエスト URI に基づいて要求をルーティングします。

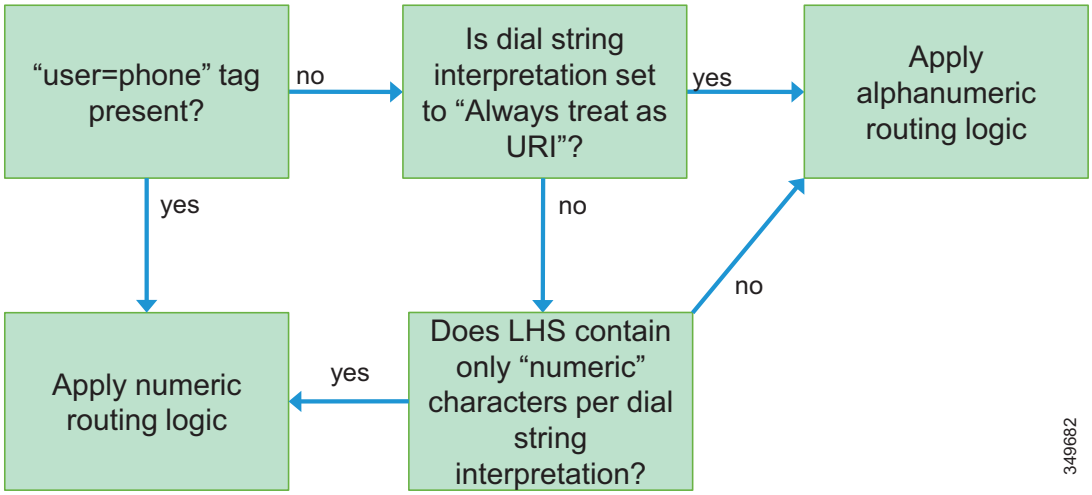
SIP ルート ヘッダーが存在し、最初の SIP ルート ヘッダー値に指定されているホストが [クラスタ完全修飾ドメイン名（Cluster Fully Qualified Domain Name）] エンタープライズ パラメータで指定されている最初のエントリと一致しなければ、Unified CM は要求をルーティングするために、SIP ルート ヘッダー値を設定済み SIP ルート パターンと照合します。このルーティング動作により、Cisco Spark ハイブリッド コール サービス導入環境内の Cisco Expressway-C とその他のエンタープライズ Unified CM クラスタとの間の中継ルーティング エンティティとして、Unified CM SME を使用できるようになります。Cisco Spark ハイブリッド コール サービス導入環境では、コール サービス接続用に設定されたユーザが Cisco Spark アプリケーションで発信したコールの場合、コール レッグが Cisco Collaboration Cloud から発信側ユーザの Unified CM クラスタにフォークされて、発信側ユーザの Cisco Spark リモート デバイスに固定されます。このコール レッグの SIP 要求では、リクエスト URI に、ダイヤルされた宛先が組み込まれ、Cisco Collaboration Cloud によって要求に追加された SIP ルート ヘッダーに、発信側ユーザの Unified CM クラスタのクラスタ完全修飾ドメイン名が組み込まれます。

Unified CM は、数値および英数字の SIP リクエスト URI に異なるルーティング ロジックを適用します。

数値 URI とディレクトリ URI

図 14-26 に、受信 SIP 要求 URI を英数字 URI として扱うか、数値 URI として扱うかを分類するために Unified CM によって使用される意思決定ツリーを示します。

図 14-26　　数値 URI と英数字 URI の分類



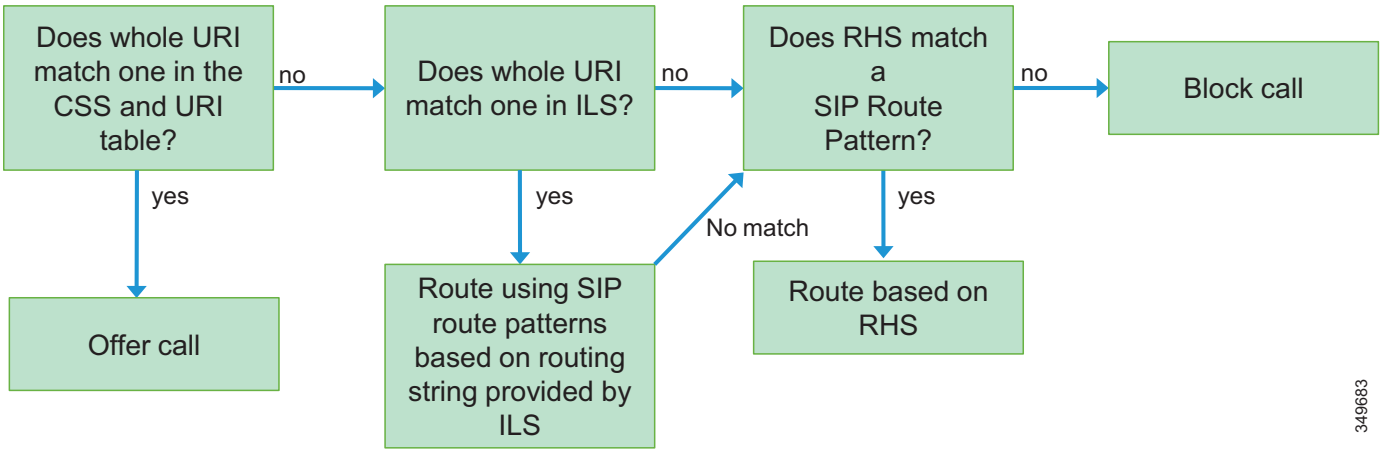
SIP 要求に user=phone タグがある場合、SIP URI は常に数値 SIP URI として解釈されます。user=phone が存在しない場合、発信側デバイス（エンドポイントまたはトランク）の SIP プロファイルのダイヤル文字列解釈の設定に基づいて決定されます。この設定は、Unified CM が数値 SIP URI として受け入れる文字セット（0 ～ 9、*、#、+ およびオプションとして A ～ D）を定義するか、またはディレクトリ URI としての解釈を強制します。

数値および英数字の URI に適用されるルーティング ロジックについては、次の項で説明します。

英数字ディレクトリ URI のルーティング

図 14-27 に、Unified CM によって英数字 URI に適用されるルーティング ロジックのフローチャートを示します。

図 14-27　SIP 要求のコール ルーティング ロジック



最初の手順では、発信側デバイスのコーリング サーチ スペースに基づいて SIP 要求のルーティングを試みます。Unified CM は、発信側デバイスのコーリング サーチ スペースによって指定されたパーティションに設定されたすべてのディレクトリ URI に対して SIP URI の完全一致を検索します。一致が見つかった場合、コールは一致したローカル ディレクトリ URI に関連付けられたディレクトリ番号に伝送されます。

一致するローカル ディレクトリ URI が存在しない場合、Unified CM はインポートされた GDPR カタログまたはリモート システムから学習した GDPR カタログで、再び完全一致によって SIP URI を探します。一致が見つかった場合、SIP 要求は GDPR カタログに関連付けられた SIP ルート文字列（ロケーション ID）を照合することによりルーティングされます。この一部として、発信側デバイスのコーリング サーチ スペースによって指定された設定済み SIP ルート パターンに対して、見つかったディレクトリ URI は学習されています。（図 14-28 を参照）。

SIP URI がローカル ディレクトリ URI で一致せず、どの GDPR カタログ内のディレクトリ URI ともマッチしない場合、Unified CM は SIP URI の右側のみと設定済み SIP ルート パターンとの一致に基づいて SIP 要求をルーティングします。この最終手段のルーティングは、ローカルや GDPR に参加する他の呼制御で不明なすべての SIP URI のためのデフォルト ルートを作成するために使用できます。一般的な例は、Cisco Expressway Business-to-Business（B2B）構成要素への SIP ルートです。

図 14-28　ディレクトリ URI のルーティング例

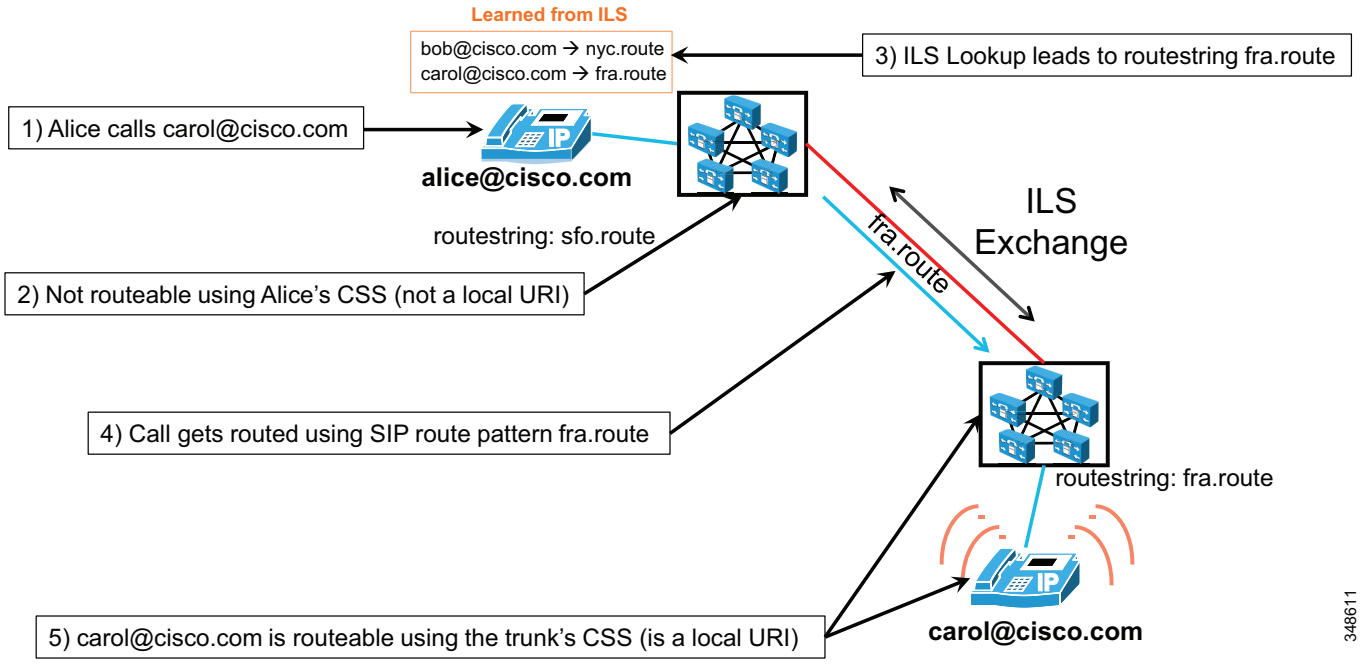


図 14-28 に、ダイヤルされたディレクトリ URI が Unified CM によってルーティングされる例を示します。この例では、下の Unified CM クラスタがローカル ディレクトリ URI「carol@cisco.com」をアドバタイズします。この Unified CM クラスタのすべてのローカル ディレクトリ URI は、SIP ルート文字列「fra.route」のもとにアドバタイズされます。GDPR を介したこの情報交換の一部として、最上部の Unified CM クラスタは学習したディレクトリ URI テーブルに「carol@cisco.com」から SIP ルート文字列「fra.cisco.com」への関連付けを読み込みました。最上部のクラスタに登録された電話機からディレクトリ URI「carol@cisco.com」コールがなされた場合、ディレクトリ URI「carol@cisco.com」のローカル ルックアップは失敗します。「carol@cisco.com」はローカル ディレクトリ URI ではないからです。ルーティング プロセスの次の手順は、GDPR が学習したテーブルでディレクトリ URI「carol@cisco.com」を検索することです。この検索では、下部のクラスタから学習した情報を見つけることができ、最上部の発信元クラスタは学習した SIP ルーティング「fra.cisco.com」を使用し、SIP ルート文字列「fra.cisco.com」と発信側デバイスのコーリング サーチスペースで指定した設定済み SIP ルート パターンのマッチングでルートを探します。SIP ルート パターン「fra.route」が設定され、ルート リストをポイントします。ルートリストは最終的にはターゲット Unified CM クラスタをポイントする SIP トランクに到達します。発信元 Unified CM クラスタは、こうして宛先 Unified CM クラスタにコールをルーティングします。送信された SIP 要求の宛先は「carol@cisco.com」になります。宛先クラスタでは、図 14-26 に示したのと同じルーティング ロジックが、「carol@cisco.com」を宛先クラスタ上のすべてのローカル ディレクトリ URI とマッチングし、完全一致が見つかってターゲット デバイスが鳴ります。

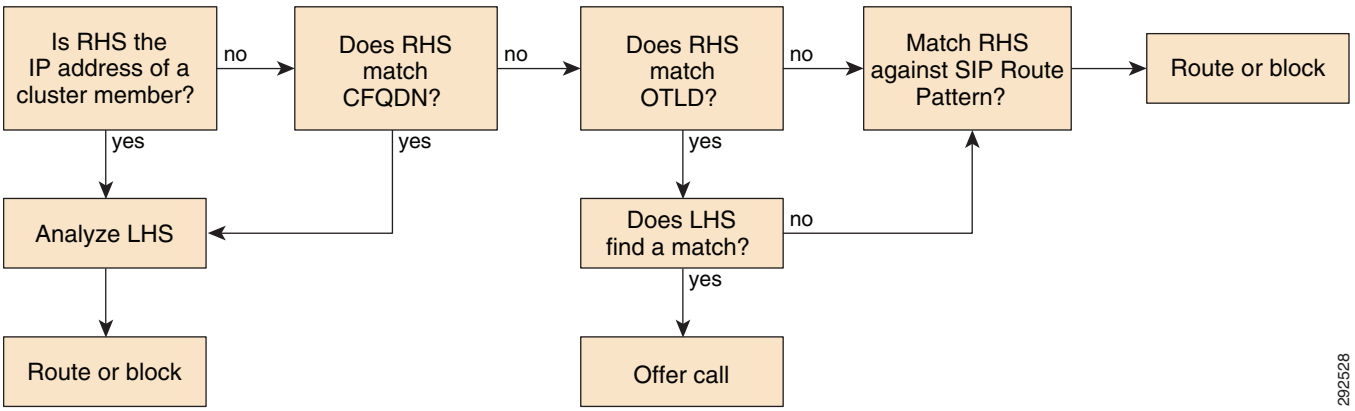
上記の例は、SIP ルート文字列のネーム スペースが、ディレクトリ URI のネーム スペースから完全に独立していることを示します。ディレクトリ URI のホスト部分に使用するネーム スペースの構造と何らかの方法で関連する SIP ルート文字列を使用する必要はありません。これによって望ましいルーティング トポロジに基づいて SIP ルート文字列のネーム スペースを最適化することができます。直接 URI のホスト部分との一致に使用する SIP ルート パターンと、SIP ルート文字列に基づいてディレクトリ URI のルーティングを行うために使用される SIP ルート パターンを区別するために、SIP ルート文字列のルート パターンに対して独立したネーム スペースを使用することを強く推奨します（「.route」、「.ils」など）。

上記の例では、基本的に、選択した SIP ルート文字列が個々の呼制御（fra.route、nyc.route）を識別し、学習した SIP ルート文字列に基づいてディレクトリ URI SIP 要求のルーティングに使用される SIP ルート パターンのグリッドが、明示的なパターン（fra.route、nyc.route）を使用して目的の到達可能性を実現します。階層型トポロジでは、階層的な SIP ルート文字列（sjc.us.route、nyc.us.route、fra.de.route、muc.de.route など）を、Unified CM クラスタのセットにアドレスを指定するそれぞれの統合 Cisco Unified Communications Manager Session Management Edition（SME）クラスタにルーティングするワイルドカード SIP ルート パターン（*.de.route、*.us.route）とともに使用できます。

数値 URI のルーティング

SIP URI が数値 URI と見なされた場合（図 14-26 を参照）、コールは図 14-29 のフローチャートに従って処理されます。リリース 9.0 以前の Unified CM では、これが SIP 要求の標準ルーティング手順です。

図 14-29　数値 SIP 要求のコール ルーティング ロジック



最初の手順では、SIP URI の右側が Unified CM クラスタのメンバーであるサーバの IP アドレスまたはホスト名であるか、または Unified CM エンタープライズ パラメータに設定されているクラスタの完全修飾ドメイン名（CFQDN）に一致するかを確認します。この場合、URI の左側はローカル数字パターンと見なされ、発信側デバイスのコーリング サーチ スペースを使用してローカル番号分析にある数字のパターンに一致します。

次の手順では、SIP URI の右側が、Unified CM エンタープライズ パラメータに設定されている組織のトップレベルのドメイン（OTLD）に一致するかどうかを確認します。一致する場合、Unified CM は発信側デバイスのコーリング サーチ スペースを使用してコールを再度数値的にルーティングしようとします。一致するものが見つからない場合、ルーティングはフォールバックし、設定されている SIP ルート パターンに SIP URI の右側を照合することによってコールがルーティングされます。

Unified CM クラスタに、IP アドレスが 192.168.10.10、192.168.10.11、192.168.20.10、および 192.168.20.11 のメンバー、ucm1.cisco.com として設定されているクラスタの完全修飾ドメイン名、および cisco.com として設定されている組織のトップレベルのドメインが含まれていると仮定すると、次の SIP URI はすべて市内電話番号 1234 にルーティングされます。

- 1234@192.168.10.10
- 1234@192.168.10.11
- 1234@192.168.20.10

- 1234@192.168.20.11
- 1234@ucm1.cisco.com
- 1234@cisco.com

市内電話番号 1234 が存在しないと仮定すると、最初の 5 つのコールはすぐに失敗し、Unified CM は、設定されている SIP ルート パターンに cisco.com を照合することによって、6 番めのコールをルーティングしようとします。

数値による一致は、ローカルに存在する数字パターンのどのタイプとも一致する可能性があります。これには、ディレクトリ番号とルート パターンおよびその他の通常の数字パターンは含まれませんが、GDPR が学習したすべての数字パターン マッチと一致する可能性があります（+E.164 番号またはパターン、または会社の電話番号またはパターン）。GDPR が学習した宛先が一致した場合、設定された SIP ルート パターンに一致した GDPR 情報の SIP ルート文字列と照合するセカンダリ ルックアップがすぐに行われます。SIP ルート文字列と照合するセカンダリ ルックアップ用に、最初の数値ルックアップに使用するものと同じコーリング サーチ スペースが使用されます。この動作は、関連する SIP ルート文字列をルーティングする SIP ルート パターンへのアクセスを提供しない CSS を定義して、特定の GDPR カタログの一部として学習された情報へのアクセスを制限するために使用できます。

（注）　GDPR が学習した宛先に到達できるように、発信側デバイスのコーリング サーチ スペースは GDPR が学習したパターンが存在するパーティションと、GDPR が学習した宛先に関連付けられた SIP ルート文字列に一致する SIP ルート パターンが存在するパーティションを含める必要があります。

Cisco TelePresence Video Communication Server

この項では、Cisco TelePresence Video Communication Server（VCS）で利用可能なコール ルーティング メカニズムの概要を示します。詳細な説明については、次の URL にある『*Cisco TelePresence Video Communication Server Administrator Guide*』および各種 Cisco VCS の導入ガイドを参照してください。

https://www.cisco.com/en/US/products/ps11337/tsd_products_support_series_home.html

この項では、次の項目について説明します。

- Cisco VCS アドレッシング方式：SIP URI、H.323 ID、E.164 エイリアス（14-58 ページ）
- Cisco VCS アドレッシング ゾーン（14-58 ページ）
- Cisco VCS のパターン マッチング（14-59 ページ）
- Cisco VCS のルーティング プロセス（14-60 ページ）

Cisco VCS アドレッシング方式：SIP URI、H.323 ID、E.164 エイリアス

Cisco TelePresence Video Communication Server（VCS）は、H.323 と SIP を使用する通信を可能にし、本質的にこれらのプロトコルでサポートされているアドレッシング方式を可能にします。

ダイヤル可能なアドレスの形式は次のとおりです。

- IPv4/IPv6 アドレス

  IPv4 または IPv6 の IP アドレスを使用してエンドポイントとマルチポイント デバイスを呼び出すことができます。

- H.323 ID

  H.323 ID は H.323 エンドポイントの英数字の識別子です。任意の英数字の文字列を割り当てることができます。エンドポイントに SIP と H.323 の登録が必要な場合（デュアル登録）、このエイリアスは通常、SIP URI に一致します。

- E.164 エイリアス（E.164 alias）

  E.164 は PSTN と同じ番号設定方式を使用します。これは、H.323 ID とともに H.323（PSTN で使用される番号計画）で設定できるオプションです。

- SIP URI

  これは、常に*ユーザ名@ドメイン*の形式を取るエイリアスです。

- ENUM

  ENUM ダイヤリングでは、そのエンドポイントが異なる形式のエイリアスを使用して登録されていても、E.164 番号（電話番号）にダイヤリングした発信者がエンドポイントに接続できます。

基本的に、SIP URI は E.164 エイリアスを使用して作成できます。エイリアスのユーザ名部分は E.164 番号で、ホスト名部分がドメインになります。SIP を使用してこのタイプの E.164 マッピングを設定すると、エイリアスからユーザの情報が失われます。この場合、適切なエイリアス、*ユーザ名@ドメイン*で FindMe を設定し、多くの異なるアドレッシング スキームから生じる複雑さを隠します。FindMe エイリアスはアドレッシング方式に関係なく、ダイヤル可能な任意のデバイスに関連付けることができます。

Cisco VCS アドレッシング ゾーン

VCS は、ローカルに登録されたエンドポイント、ネイバー システム、およびパブリック インターネットのエンドポイントからコールを受信します。

VCS に登録されているエンドポイント、ゲートウェイ、マルチポイント デバイス、およびコンテンツ サーバは、ローカル ゾーンの一部と見なされます。ローカル ゾーンはサブゾーンにさらに分割されます。デフォルトで存在するものも、管理者が設定するものもあります。

より一般的に言うと、ゾーンは同じダイヤリング動作と帯域幅の設定を共有するエンドポイントの集合です。ゾーンは VCS に対してローカルでもリモートでもかまいません。

ダイヤル可能なエンティティが VCS に登録されていない場合、他の呼制御またはシステムによって管理されるリモート ゾーンで使用可能な場合があります。これらのリモート ゾーンには、ネイバー ゾーン、トラバーサル クライアントおよびトラバーサル サーバ ゾーン、DNS ゾーン、および ENUM ゾーンがあります。

ネイバー ゾーンの概念は、Cisco Unified CM のトランクの概念と似ています。別の VCS、Unified CM サーバまたはクラスタ、サードパーティの呼制御システム、マルチポイント デバイス、またはゲートウェイへの SIP または H.323 トランク側接続です。

DNS ゾーンは DNS サービス（SRV）を使用して検出できるローカル以外の宛先です。トラバーサル クライアントおよびサーバは、VCS Control および VCS Expressway を使用してインターネット経由の通信にアクセスするためのゾーンです。ENUM ゾーンは、ENUM サービスを使用して到達できるローカル以外の宛先です。

Cisco VCS のパターン マッチング

VCS のルーティング ロジックの重要な概念が、トランスフォーム（検索前のトランスフォームとも呼ばれます）と検索ルール（検索とも呼ばれます）です。トランスフォームと検索の違いは、検索には宛先のターゲット ゾーンがありますが、トランスフォームはシステム レベルで設定され、単一ゾーンごとの適用ができないことです。

検索とトランスフォームは管理者が設定した優先順位に従って適用され、パターン分析と文字列操作に正規表現を使用します。

検索前のトランスフォームの概念は、Unified CM のトランスレーション パターンに似ていますが、正規表現を使用して英数字のトランスフォームができるという点が異なります。

検索ルールは、Unified CM のルート パターンに似ています。ルート パターンはトランクまたはルート リストに適用されますが、検索ルールにはターゲットとして宛先ゾーンがあります。

検索ルールとトランスフォームの両方に、次の主な特徴があります。

- VCS がルールまたはトランスフォームの解析に使用する順番を定義する優先順位
- ダイヤルされたパターンが検査される一致式（パターン文字列）
- 宛先エイリアスの取得に使用される表現である、置換文字列

正規表現で複雑な文字列操作が可能ですが、非常に一般的な、シンプルな適用例がいくつかあります。VCS の最も一般的な文字列操作の 1 つは、エイリアスのドメイン部分を追加するか削除することによって発生します。この例を示します。

エイリアス：88302

検索ルールの一致式（正規表現を使用）：(\d+)

検索ルールの置換文字列：\1@cisco.com

このシンプルなルールに従って、VCS に到達するダイヤルされたすべての番号が、number@domain に変換されます。この場合、88302 は 88302@cisco.com に変換されます。

検索ルールには、ダイヤリング方式の作成時に役立つ次の特性があります。

- ターゲット ゾーン（必須）。ターゲット ゾーンは、VCS 内のコール用にローカル ゾーンにすることも、ネイバー、トラバーサル クライアントまたはサーバ、または DNS ゾーンとしてとして他のゾーンにすることもできます。ポリシー サーバが含まれる場合もあります。宛先ゾーンはユーザがダイヤルしたパターンに基づいて選択されます。
- 送信元ゾーン（オプション）。Cisco VCS リリース 7.2 から、特定のゾーンまたはサブゾーンから発信したエンドポイントにだけルールを適用することができます。
- 検索ルールに一致した場合の設定可能な動作（必須）。

VCS では、パターンに一致したエイリアスと、検出され、コールに応答できるデバイスに対処するエイリアスは異なります。

エイリアスが検索ルールの一致式に対して検査され、式がエイリアスと一致した場合、VCS は、そのエイリアスがターゲット ゾーンにあるかどうかを判断します。

検索ルールがエイリアスに一致し、エイリアスが検出された場合、コールはターゲット ゾーンに送信されます。

検索ルールがエイリアスに一致し、エイリアスが検出されない場合、ターゲット ゾーンにないことを意味します。この場合の VCS の動作は、検索ルールの [正常に一致する場合（On Successful Match）] フィールドの設定によって異なります。このフィールドが [停止（stop）] に設定されている場合、エイリアスが見つからなくてもルーティング エンジンは停止し、コールが宛先ゾーンに送信されます。フィールドが [続行（continue）] に設定されている場合、エイリアスが見つかるか、[正常に一致する場合（On Successful Match）] フィールドが [停止（stop）] に設定されているエイリアスにルールが一致するか、すべてのルールが分析されるまで検索プロセスは残りの優先順位が低いルールの分析を継続します。

この動作は、複数の呼制御プラットフォームに同じドメインを含む英数字 SIP URI が登録されているため、特定のエイリアスがある場所を管理者が知らない場合に役立ちます。たとえば、同じ企業内で複数の VCS が、同じドメイン company.com を共有する場合があります。user1@company.com へのコールは、宛先 VCS がわからない場合、正しくルーティングできません。ただし、VCS のルーティング ロジックを使用して、複数の VCS または他の呼制御システムでそのエイリアスを検索して、エイリアスが見つかったときにだけコールを送信することが可能です。

Cisco VCS のルーティング プロセス

Cisco VCS がコールを受信すると、設定された検索前のトランスフォームがすべて適用されます。検索前のトランスフォームの後は、呼処理言語（CPL）ロジックが適用されます。このポリシーは、高度なルーティング ルール用の CPL スクリプトを使用して設定され、外部ポリシー サーバを含めることができます。ただし、大半のシナリオでは、CPL を使用する必要はありません。

FindMe エイリアスが設定されている場合、次にユーザ ポリシーが適用されます。FindMe ID は 1 つ以上のターゲット エイリアスに解決され、ターゲット エイリアスを正しく見つけるために、もう一度呼処理ロジックが開始されます。

VCS はその後、優先度順に検索ルールを照会することで、エイリアスに一致する式を検索します。検索ルールが新しい宛先（SIP URI またはエイリアス）を返すと、プロセスが再開します。これは、コールが DNS サービス、ENUM サービス、またはポリシー サービスに送信される場合に発生することがあります。

エイリアスがいずれかのゾーン（ローカル ゾーン、ネイバーなど）で見つかるか、ルーティングの宛先がポリシー サービスによって返された場合、VCS はコールの発信を試行します。

一致がない場合は、コールが失敗したことを示すために、VCS はメッセージを返します。

ルーティング ロジックが最長一致に基づく Unified CM に対して、VCS では、ロジックは優先度ベースです。Unified CM でトランスレーション パターンまたはルート パターンの順序を変更しても、ルーティング アルゴリズムの結果は影響を受けませんが、VCS でルールの優先順位を変更すると、ルーティング動作が変わる原因になります。

推奨される設計

ここでは、設計ガイダンスと、エンドツーエンドの企業のダイヤル プランを実装する方法の概要を示します。

Unified CM のグローバル化されたダイヤル プラン アプローチ

この項では、グローバル化された番号に基づいて簡素化されたコール ルーティングを実装するために使用されるダイヤル プラン機能について説明します。主に、オフネット コールに対して発信元にかかわらず単一のルーティング構造を使用することによって、ルーティングが簡素化されます。たとえば、異なる国にいる 2 人のユーザは、それぞれのダイヤリング手順に一致するように設定されたサイト固有のルート パターンの代わりに、同じルート パターンを使用して、それぞれのローカル ゲートウェイに対してコールを伝送できます。

このようなグローバル化を実現するためのアーキテクチャ上の主要なアプローチは、次のようにまとめることができます。

- コールがシステムに着信する場合、宛先番号および発信番号はローカル形式で受け付けられますが、すぐにシステムによってグローバル化されます。Unified CM に登録されたエンドポイントから発信されたコールの場合、ダイヤルされた宛先のグローバリゼーションはダイヤリング正規化トランスレーション パターンにより行われ、発信側情報のグローバリゼーションは、+E.164 ディレクトリ番号の場合は必要ないか、この回線からのコール用の電話の発信側トランスフォーメーションにより対処される適切な発信側トランスフォーメーションによって行われます。トランクでの着信コールの場合、着信コールと発信側トランスフォーメーションが同じ目的のために使用されます。
- グローバル形式で表現されたルート パターンを使用してコールを宛先にルーティングするために、グローバル化された着信者番号が使用されます。グローバル形式は、81001234 のようなグローバルな企業固有の内部形式や、+E.164 形式（たとえば +12125551234）などの DID 番号のグローバル化された PSTN 表現の組み合わせとなります。
- 宛先が特定されると、発信番号および着信番号は、コール伝送先のエンドポイント、ネットワーク、またはシステムで必要とされる形式にローカル化されます。

したがって、設計指針は次のようになります。

> コールの入力ではローカライズ化された形式で受け付け、それらをグローバル化します。グローバル化された形式に基づいてコールをルーティングし、宛先で必要とされる形式に従ってコールをローカライズします。

Cisco Unified Communications Manager（Unified CM）には、次のダイヤル プラン グローバル化機能が備えられています。

- ローカル ルート グループ（14-62 ページ）
- + ダイヤリングのサポート（14-62 ページ）
- 発信者番号変換（14-63 ページ）
- 着信者番号変換（14-63 ページ）
- 着信側の設定（ゲートウェイ別）（14-64 ページ）
- 論理パーティション（14-65 ページ）

また、これらの新機能により Unified CM システムで次のことができるようになりました。

- 発信者の物理的な場所に基づいたコールのルーティング。
- 国際電気通信連合（ITU）の E.164 勧告に記載されているようなグローバル形式で発番号および着番号を表示する。
- ローカル ダイヤリング手順に基づいた形式でユーザへのコールを表示する。
- 発番号、着番号、それらに対応する番号タイプのローカル要件に適合する形式で外部ネットワークへのコール（たとえば PSTN）を表示する。

- 発信番号の数字と番号タイプに基づき、ゲートウェイからの着信コールについての発番号をグローバル形式で生成する。
- 一部の国の法的要件に準拠するため、各エンドポイントのジオロケーションに適用されるポリシーに基づいて、エンドポイント間のコールの確立と通話切替機能の開始を制御する。

ローカル ルート グループ

ローカル ルート グループでは、発信側のローカル ルート グループ定義に基づいて選択されたゲートウェイへのオフネット コールをルーティングするパターンを作成する機能を提供します。これにより、たとえば、発信側に近いイーグレス ゲートウェイを選択することができます。たとえば、ルート オフネット、特定の国のすべてのサイトに対する国内通話に対して、1 つのパターンを定義できます。すべてのサイトの電話機をこのパターンに一致するように設定できます。このパターンはその後、発信側電話機に関連付けられたローカル ルート グループと、それぞれのローカル ルート グループに設定された電話機のデバイス プール レベルに基づいて、コールをルーティングします。これによって、サイト 1 の電話機がサイト 1 のゲートウェイを介してコールをルーティングできるようにします。一方、サイト 2 の電話機（こちらも同じパターンを使用）はサイト 2 のゲートウェイを介してコールをルーティングします。この機能は、オフネット コールのサイト固有のルーティング設定を簡素化します。

複数のローカル ルート グループの定義により、異なるコール タイプのイーグレス ゲートウェイの選択を差別化することができるため、たとえば、緊急、国内、国際のコール用にデバイス プールごとに異なるイーグレス ゲートウェイを定義することができます。

+ ダイヤリングのサポート

電話番号には、他の国から宛先に到達するのに必要な国際ダイヤル アクセス コードを表すために、+ 記号を使用できます。たとえば、+1 408 526 4000 は、米国にあるシスコ本社の国際表記です。この番号にコールするには、フランスの企業テレフォニー ユーザは通常 0 00 1 408 526 4000 とダイヤルする必要がありますが、英国の発信者は 9 00 1 408 526 4000 とダイヤルする必要があります。いずれの場合でも、+ をそれぞれの発信者に関連のある、適切なオフネット アクセス コード（企業テレフォニー システムで定められているとおり）に、また国際アクセス コード（PSTN キャリアで定められているとおりに）に置き換える必要があります。

システムは + で定義された宛先に直接、コールをルーティングできます。たとえば、ユーザは、シスコの米国本社の WiFi 電話のスピード ダイヤル エントリを +1 408 526 4000 とプログラムし、フランス、英国、または企業内の任意の場所でローミングしているときに、直接ダイヤルできます。それぞれの場所で、システムは宛先番号を地域で定められた番号ストリングに変換して、コールが正しくルーティングされるようにします。

同様に、着信番号が +E.164 形式で表現されている場合、デュアルモード電話からダイヤルされた電話番号は、電話機が GSM モードの場合には携帯電話キャリア ネットワーク経由で、電話機が WiFi モードの場合には企業ネットワーク経由で、直接ルーティングできます。これにより、ユーザは、特定の連絡先エントリに対して宛先番号を 1 つ保存するだけで済み、電話機が現在接続されているネットワークにかかわらずその番号にダイヤルできます。

この機能によりユーザは、システムを使用して ITU E.164 勧告に記述されている形式で表現される電話番号に変換し、正しくルーティングできます。ユーザが番号を手動で編集してローカル ダイヤリング手順に適合させる必要はありません。

発信者番号変換

Unified CM を介してルーティングされるコールに関連付けられている発番号は、電話機または PSTN に表示される前に適合させることが必要な場合があります。たとえば、+1 408 526 4000 からのコールは、宛先の電話機が米国またはカナダにある場合は、発信元が 408 526 4000 と表示されるようにする必要があります。一方、同じ番号からのコールで、宛先の電話機がフランスにある場合は、発信元が 00 1 408 526 4000 と表示されるようにする必要があります。これは主に、地域の PSTN によって定められる慣習的形式で発信側番号が表示されるようにするのが目的で、慣れ親しんだ形式でコールの発信元を識別できます。

ゲートウェイに配信されるコールでは、ゲートウェイが接続している電話通信業者の要件に、発信者番号を適合させる必要があります。たとえば、フランスにあるゲートウェイに提示される +1 408 526 4000 からのコールでは、発信者番号を 1 408 526 4000 と表し、発信者番号タイプを [国際（International）] に設定することが必要な場合があります。同様に、カナダにあるゲートウェイに提示される同じ番号からのコールでは、発信側番号を 408 526 4000 とし、発番号タイプを National に設定することが必要な場合があります。

この機能では、発番号を Unified CM システム内のコール ルーティングで使用される形式から、電話機のユーザまたはオフクラスタ ネットワークで定められる形式に適合させることができます。

（注）　一部のサービス プロバイダーでは、機器に技術的な制限、または企業ポリシーや政府の規制の理由から、外国の電話番号を表す発番号を受け付けない場合があります。プロバイダーが発信者番号を受け付けない場合は、発信者番号をスクリーニングして上書きするか、コールを拒否します。一部のネットワークでは、コールに 2 つの発信者識別子（ユーザ指定とネットワーク指定）が存在する場合があります。

着信者番号変換

Unified CM を介してルーティングされるコールに関連付けられている着信番号は、PSTN に提示される前に適合させる必要がある場合があります。たとえば、カナダにあるゲートウェイを介して PSTN に出る場合、+1 408 526 4000 に対して発信されるコールでは、着番号を 1 408 562 4000 に変換し、番号タイプを National に設定する必要があります。同じコールがフランスのゲートウェイに対して再ルーティングされた場合、着信者番号を 1 408 526 4000 に変換し、番号タイプを [国際（International）] に設定する必要があります。

着番号を操作し、着信番号の番号タイプを設定することによって、この機能では着番号がオフクラスタ ネットワークで定められる形式に適合するようにします。

同時に、着信の着信側トランスフォーメーションは、コールをルーティングする前に着信の着信側情報を共通のグローバル化形式に正規化できるようにします。Unified CM では、この機能でゲートウェイごとの設定を取り入れたことにより、番号タイプごとのさまざまなプレフィックスを、異なるゲートウェイに入るコールに適用できるようになりました。設定は優先度順にゲートウェイ自体またはゲートウェイのデバイス プールに設定できます。空白のエントリはプレフィックスとして数字が付加されないことを意味します。より優先順位の低い設定から設定を継承するには、エントリを [Default] に設定する必要があります。より複雑な着信側変換には、番号タイプごとの着信側変換コーリング サーチ スペースが使用できます。SIP はタイプされた番号の概念をサポートしないため、SIP ではタイプ [不明（Unknown）] のデバイス プール設定が考慮されます。

着信側の設定（ゲートウェイ別）

デジタル インターフェイス（たとえば、ISDN PRI）を介してゲートウェイに着信するコールには、発信者番号、および発信者番号の番号タイプを [不明（Unknown）]、[サブスクライバ（Subscriber）]、[国内（National）]、または [国際（International）] のいずれかに区別する属性が関連付けられています。組み合わせると、着信コールの発信番号と、それに関連付けられた番号タイプにより、発信者の識別情報を特定できます。これは、着信コールの発番号に対して適切な数字を除去したり、プレフィックスを付加したりすることにより実行されます。着信側の設定では、4 つの発信番号タイプのそれぞれで、発番号に対して数字を除去したり、プレフィックスを付加したりする個別の組み合わせを適用できるようにします。

たとえば、2 つのコールがドイツのハンブルグにあるゲートウェイに入るとします。どちらのコールも発番号は 691234567 です。最初のコールは、番号タイプ Subscriber に関連付けられています。これは、発信者がハンブルグにいることを意味します。このためシティ コードはハンブルグの（40）となり、国コードはドイツの（49）になります。そのため、着信コールを完全に表すと +49 40 69 1234567 となります。この番号は、番号タイプ Subscriber の着信コールの発番号に対して +49 40 をプレフィックスとして付加することにより得られます。

2 つめのコールは、番号タイプ National に関連付けられています。これは、発信者がドイツにいることを意味します。そしてこの番号にはすでに適切なシティ コード（69 がフランクフルトのシティ コード）が含まれていますが、国コードはドイツ（49）になります。2 つめの着信コールを完全に表すと +49 69 1234567 となります。この番号は、番号タイプ National の 2 つめの着信コールの発番号に対して +49 をプレフィックスとして付加することにより得られます。

番号の削除は、グローバル化された番号の一部であってはならない着信番号文字列から番号を削除するために必要です。たとえば、オーストリアの一部の ISDN トランクでは国内宛先からのコールの着信の発信者番号には先頭にゼロが付き、+E.164 にグローバル化するにはこのゼロを削除する必要があります。たとえば、ウィーンからのコールは、発信者番号が 01666001234、発信者番号タイプが [国内（National）] で受信することがあります。このコールではオーストリアの国番号（43）が示され、番号にはすでにウィーンのシティ コード（1）が含まれています。この場合の正規化では、1 桁（先頭のゼロ）の削除と、正規化された +E.164 番号 +43 1 666001234 を得るためのプレフィックス +43 の追加が必要です。

Unified CM では、この機能でゲートウェイごとの設定を取り入れたことにより、番号タイプごとのさまざまなプレフィックスを、異なるゲートウェイに入るコールに適用できるようになりました。設定は、優先順位順にゲートウェイ上、ゲートウェイのデバイス プール上、またはクラスタ全体のサービス パラメータ上で設定できます。空白のエントリはプレフィックスとして数字が付加されないことを意味します。より優先順位の低い設定から設定を継承するには、エントリを [Default] に設定する必要があります。

サービス パラメータ レベルの設定はグローバルな重要度を持つため、特別な変換のセットを使用しなければならないゲートウェイが 1 つだけ存在する場合は、デバイス プール レベルの設定を使用し、これらの設定が同じデバイス プールを共有するすべてのゲートウェイで共有されるようにするか、ゲートウェイのレベルの設定を使用することを強く推奨します。混乱を避けるために、特定のインストールではデバイス プール レベルの設定またはデバイス レベルの設定だけを常に使用し、混在させないことを推奨します（一部にはデバイス レベルの設定を使用し、残りにはデバイス プール レベルの設定を使用することは避けてください）。

所定の番号タイプ内のすべてのコールに対しては、最初に受信された発番号に関係なく、プレフィックスの付加および番号削除の動作が適用されます。

（注）　SIP トランク、または SIP ゲートウェイからのコールはすべて発番号タイプ Unknown に関連付けられています。

特に、SIP ゲートウェイおよび SIP トランクに実装された SIP プロトコルによって、実質的にすべてのコールの着信の発信者番号の番号タイプが [不明（Unknown）] になります。このため、Unified CM では、異なる発番号カテゴリに異なる発番号変更を適用できません。

Unified CM では、番号タイプごとに、着信側の設定コーリング サーチ スペース（CSS）を使用できます。これらの CSS を使用することで、発信側トランスフォーメーション パターンに基づいて発信側に変更を適用できます。これらのパターンでは、正規表現を使用して大文字と小文字を区別したサブセットが照合され、各サブセットに別個の番号操作が実施されます。この新しい機能によって、Unified CM は異なる発番号カテゴリに異なる発番号変更を適用できます。たとえば、PSTN への接続に使用される SIP トランクから、番号タイプが [不明（Unknown）] に設定されたローカル、国内、および海外からのコールが送信されることがあります。このような場合、各コールの発信者番号を使用して、番号タイプ [不明（Unknown）] に関連付けられたトランクの CSS 内の発信側トランスフォーメーション パターンが照合され、Unified CM で異なる発信者番号カテゴリに異なる発信者番号変更が適用されます。

論理パーティション

インドなどの一部の国には、企業外部でコールを接続するときに、企業の音声インフラストラクチャにローカル PSTN だけを使用することを義務付けた電気通信規制があります。このため、音声システムを 2 つのシステムに論理的にパーティション化する必要があります。2 つのシステムとは、企業内の非公開ユーザ グループ（CUG）通信用とローカル PSTN へのアクセス用です。ロケーション A の企業ユーザからロケーション B の別の企業ユーザへのコールは、CUG システム内で確立できますが、ロケーション A の企業ユーザから PSTN の宛先へのコールは、そのロケーションにかかわらず、ロケーション A の PSTN へのローカル アクセスを経由する必要があります。

既存のダイヤル プラン ツールを使用すると、コールが CUG の外側のエンドポイント間で行われる場合にそのコールを防止できますが、コールが進行しているときにはその新しいコール レッグの確立を防止できません。たとえば、英国ロンドンの企業ユーザが企業ネットワークを介してインドのデリにある同僚にコールするとします。コールが確立されると、デリのユーザは、ロンドンからのコールを受信した回線と同じ回線からインドのカスタマーとの会議に切り替えることになります。この非公開ユーザ グループ以外の宛先への通話切替（同じ回線上）は、Unified CM 内の既存のダイヤル プラン ツール（コーリング サーチ スペースやパーティションなど）を使用するだけでは防止できません。Unified CM 7.1 以降のリリースには、論理パーティション機能が導入されています。この機能を利用することにより、発信側だけでなく、会議や転送などの通信切替機能にも適用されるポリシーを確立し、実施できます。

Unified CM で使用可能なグローバリゼーション機能の組み合わせにより、発信元ユーザとキャリアで定められるローカル形式のコールを受け入れることができるようになり、着信者番号と発信者番号のグローバル表現を使用してコールをオンネットでルーティングできるようになります。また、宛先のユーザまたはネットワークで必要なローカル形式で電話機またはゲートウェイにコールを送信できます。ダイヤル デザイン アプローチの 3 つの側面は、次のように要約できます。

- ローカル化されたコールの着信（14-66 ページ）
- グローバル化されたコール ルーティング（14-68 ページ）
- ローカル化されたコールの発信（14-68 ページ）

ローカル化されたコールの着信

Unified Communications システム（複数のサイトがさまざまなリージョンまたは国に存在する）では、ユーザのさまざまなダイヤリング手順や、ゲートウェイの接続先のサービス プロバイダーのさまざまなシグナリング要件を満たす必要があります。各地域で異なる場合があるため、システムはローカル ダイヤリング手順とシグナリング要件を、コールが正しくルーティングされる形式に「変換」できるようにする必要があります。そのため、システムは多くのローカル化された着信要件を満たすだけではなく、あらゆる宛先パターンをグローバル化した 1 つの形式も作成する必要があります。

ローカル化されたコールの電話機への着信

電話機またはビデオ端末などのエンドポイントから発信されるコールは通常、ローカル ダイヤリング手順に慣れているユーザによってダイヤルされます。米国内の企業ユーザは、カリフォルニア州 San Jose にあるシスコ本社に到達するために 9 1 408 526 4000 とダイヤルするのに慣れていますが、一方で英国のユーザは 9 00 1 408 526 4000 とダイヤルし、フランスのユーザは 0 00 1 408 526 4000 とダイヤルします。これら 3 つのダイヤル形式は、企業のオフネット アクセス コード（9 は米国、英国、0 はフランス）、国際アクセス コード（00 は英国とフランス、米国の場合、宛先は国内のため必要なし）、宛先番号の表現（国コード（1）を含む）を表します。これら 3 つの各ユーザ グループは、同じグローバル化された宛先番号（+1 408 526 4000）をダイヤルしますが、それぞれのローカル ダイヤリング手順を付加します。これら 3 つの各手順で、ローカル ダイヤリング手順のグローバルな記号として + を使用できます。

Unified CM のトランスレーション パターンはローカル化されたユーザ入力を電話機からダイヤルされたものとして、Unified Communications システム内のコールのルーティングに使用するグローバル形式に変換します。これらのパターンでは、ローカライズされたすべてのダイヤリング手順が認識されるようにする必要があります。これらの、トランスレーション パターンに基づくダイヤリングの正規化を実装する方法の詳細については、グローバル化されたダイヤル プランのコール ルーティング（14-70 ページ）を参照してください。

電話機でも、グローバル形式のダイヤル番号でダイヤルされたストリングを提供します。Cisco Unified Personal Communicator などのソフトウェア エンドポイントの場合、+ ダイヤリングは直接、電話機のテレフォニー ユーザ インターフェイス（TUI）から調整でき、ユーザによるクリック ダイヤル アクションから生成できます。タイプ B の IP Phone の場合、キーパッドから + をダイヤルするには、電話機のモデルに応じて、* または 0 キーを押したままにします。また、不在コールと受信コールのディレクトリには、番号に + が含まれるエントリがある場合があります。ユーザがそれらのディレクトリからダイヤルするとき、Unified CM に入るコールは、+ で始まる着信者番号になります。

（注）　タイプ A およびタイプ B 電話機の定義については、ダイヤル プランの要素（14-14 ページ）を参照してください。

電話機から発信されたコールの発信者番号は、コールの発信元回線のディレクトリ番号として設定されている番号に設定されます。グローバル化されたダイヤル プランのデザイン アプローチの概念に従って、すべてのコールの発信者情報をグローバル化する必要があります。ディレクトリ番号の形式がグローバル化された内部発信者情報用に選択された形式（+E.164 を推奨）と同じでない場合、[この電話からのコールの発信者 ID（Caller ID for Calls from this Phone）] 発信側変換 CSS を使用してディレクトリ番号を正しくグローバル化することで、発信者情報の適切な処理を実現する必要があります。これは、電話機から +E.164 へのコールの発呼側情報のグローバル化に推奨される方法です。この方法は、トランスレーション パターンの発信側トランスフォーメーションが適用されない URI でダイヤルされたコール フローとも互換性があるためです。

ローカル化されたコールのゲートウェイへの着信

外部ネットワーク（たとえば、PSTN）による Unified Communications システムに送信される着信番号と発信番号は通常、ローカル化されます。番号の形式は、トランクのサービス プロバイダーの設定によって異なります。ゲートウェイが PSTN トランクに接続されると、システム管理者は PSTN サービス プロバイダーに問い合わせて、この特定のトランクで使用される、適切なシグナリング ルールを決定します。トランクからシステムにコールが送信されると、発信者番号と着信者番号についての一部の情報は明示的に、一部の情報は暗黙的に示されます。この情報を使用して、システムはコールのグローバル化された発番号および着番号を生成する必要があります。

着番号のグローバル化は、次の方法のいずれかによって実行できます。

- ゲートウェイ設定で、[Call Routing Information] > [Inbound Calls] の設定を行います。ここで有効桁数を元の着信番号から取得し、プレフィックスをストリング（着信番号のグローバル化に使用する）に追加します。プレフィックスの数字は、適用可能な + 記号および国コード、エリア コード、シティ コードの追加に使用されます。
- ゲートウェイのコーリング サーチ スペースによって参照される、トランスレーション パターンをパーティションに配置します。トランスレーション パターンは、ゲートウェイに接続されているトランクで使用する着番号の形式に一致するよう設定する必要があります。また、グローバル形式に変換する必要があります。プレフィックスの数字は、適用可能な + 記号および国コード、エリア コード、シティ コードの追加に使用されます。
- ゲートウェイとゲートウェイのデバイス プールで使用可能な着信コールの着信側トランスフォーメーション設定を使用します。削除番号およびプレフィックス番号の命令を定義するか、または番号タイプごとに着信側トランスフォーメーション コーリング サーチ スペースを設定できます。これは推奨される方法です。

発番号のグローバル化は、着信側の設定を使用して行う必要があります。この設定は、直接ゲートウェイ上で、またはゲートウェイを制御するデバイス プールのいずれかで設定します。

（注） 管理者がプレフィックスを **Default** に設定した場合、呼処理で次のレベル設定（デバイス プールまたはサービス パラメータ）を使用することを示します。それ以外の場合、フィールドが空白でなければ、設定された値がプレフィックスとして使用されます。フィールドが空白の場合、プレフィックスは何も割り当てられません。

たとえば、シスコの米国本社（+1 408 526 4000）に対して、米国の番号からコールが発信されるとします。そうするとコールはカリフォルニア州 San Jose にあるゲートウェイに送信されます。ゲートウェイに送信された着信番号は 526 4000 です。この情報は、Cisco Unified Communications システムがコールの完全な宛先番号を生成するのに十分です。この特定のトランク グループのサービス プロバイダーによって送信されたコールは、ゲートウェイに接続されたトランク グループの特性に基づいて暗示される国番号とエリア コードを継承します。これは、トランク グループによって処理されたすべての宛先 DID 番号が北米番号計画の国番号（1）、エリア コード 408 を継承していることを前提とします。そのため、この番号の生成されたグローバル形式は +1 408 526 4000 です。ゲートウェイに送信された発信番号は 555 1234 で、番号タイプは Subscriber に設定されています。この番号タイプは、国コードとエリア コードが、トランク グループで設定済みの特性から継承されたものであることを示します。このようにして、システムは発信番号が +1 408 555 1234 であると認識します。

別のコールで、発信番号が 33158405858、番号タイプが International の場合、これは発信番号のグローバル形式が +33158405858 と表現されるということを示します。

グローバル化されたコール ルーティング

すべてのケースに共通のグローバル形式で表現される宛先の場合、すべてのローカル形式を生成できる宛先番号のグローバル形式を採用する必要があります。+ 記号は ITU の E.123 勧告で使用されるメカニズムで、すべてのグローバルな E.164 PSTN 番号をグローバル一意形式で表現できます。この形式は、完全修飾 PSTN 番号と呼ばれることもあります。このドキュメントでは、この表記を +E.164（+ 記号が前に付く E.164）と示します。

システムはルーティング パターン（+ 記号を含むグローバル化された着信番号とマッチングする）を使用して設定できます。このような同一のルーティング パターンは、標準ローカル ルート グループを示すルーティング リストとルーティング グループを指します。このため、コール時に発信エンドポイントのデバイス プールからイーグレス ゲートウェイを特定できるため、グローバルのルーティング パターンを作成できます。宛先が選択されると、地域設定と要件にコールを適合させるのに必要なすべてのタスク（発番号と着番号）が実行されます。

ローカル化されたコールの発信

着信番号および発信番号のグローバル形式を使用して、コールが宛先にルーティングされる場合、コールが宛先に送信されるときに次のローカル化の操作について考慮する必要がある場合があります。

電話機の発信者番号のローカリゼーション

コールが電話機に送信されると、発信番号はグローバル形式に変換されます。これは着信側からは認識できません。ユーザは通常、国内の発信者からのコールでは、発信者の番号が短縮形式で表示されることを望みます。

たとえば、米国にいるユーザは、米国の発信者からの着信コールが、10 桁の国番号で表示され、+ 記号または国コード（1）がないものを好みます。グローバル電話番号が +1 408 555 1234 のユーザは、+1 408 526 4000 とコールすると、着信番号は、電話が鳴っている間、発番号として 408 555 1234 と表示されます。これを実現するために、システム管理者は発信側トランスフォーメーション パターンを \+1.!（ドットの前の番号を削除）と設定する必要があります。発信側トランスフォーメーション パターンは、宛先電話機の発信側トランスフォーメーション パターン CSS（デバイス プール レベルで設定）に含まれるパーティションに配置されます。+1 408 555 1234 からのコールが電話機に送信されると、設定済みの発信側トランスフォーメーション パターンとマッチングされます。これにより +1 が削除され、電話が鳴っているときに発番号が 408 555 1234 と表示されます。

（注） 一部の新しい電話では、不在コールと受信コールのディレクトリに格納されている発信者番号は、グローバル化された形式のままのため、ディレクトリに格納された番号文字列を手動で編集せずに、ワンタッチでダイヤルできます。その他の電話では、不在コールと受信コールのディレクトリには変換された発信者番号が格納されます。ディレクトリからのワンタッチでのダイヤルによる問題を回避するには、変換された発信者番号と変換されていない発信者番号の形式を両方ともサポートされているダイヤリング手順に合わせる必要があります。特に、一般的な企業のダイヤル プランでは、10 桁のダイヤリングは通常、短縮サイト内ダイヤリングなどのその他のダイヤリング手順とオーバーラップすることなく企業のダイヤリング手順としてサポートすることができないため、国内番号からのコールの発信者情報の 10 桁へのローカリゼーションを使用できません。

(注)　多くの電話機ユーザは PSTN 番号のグローバル化形式に慣れつつあります。それは主に、国境を越える携帯電話が一般に使われているためです。システム管理者は、着信番号をグローバル形式で表示させたい場合は、発信者トランスフォーメーション パターンの設定を控えて、電話機の発信者情報をローカライズすることができます。

ゲートウェイの発番号のローカル化

コールがゲートウェイに送信されると、発番号は、トランク グループを提供する PSTN サービス プロバイダーの要件に合せる必要があります(このトランク グループにはゲートウェイが接続されています)。発番号トランスフォーメーション パターンは、発信側番号の番号ストリングと番号タイプの変更に使用できます。通常、ゲートウェイの国コードを示す発番号では、+ 記号を削除し、国コードを明示するように変更する必要があります。また、それらを国のプレフィックスに置き換える必要があります。また、発番号の番号タイプを National に変更する必要があります。ゲートウェイが特定のエリア、シティ コードを示すトランク グループに接続されている場合、+ 記号、国コード、ローカル エリア コードの特定の組み合わせは通常、適切なローカル プレフィックスに置き換える必要があります。また、番号タイプは Subscriber にする必要があります。

たとえば、San Francisco のユーザからのコール(+1 415 555 1234)が、最初の選択肢として San Francisco のゲートウェイ、別の選択肢として Chicago のゲートウェイを指定したルーティング リストを介してルーティングされるとします。San Francisco のゲートウェイは 2 つの発信側トランスフォーメーション パターンを使用して設定されます。

- \+1415.XXXXXXX(ドットの前の番号を削除)、番号タイプ:サブスクライバ
- \+1.!,(ドットの前の番号を削除)、番号タイプ:国内

コールが San Francisco のゲートウェイに送信されると、発番号は両方の発信側トランスフォーメーション パターンとマッチングされます。ただし、最初のパターンの方がより正確に一致しているため、発番号の処理にはこちらが選択されます。このようにして、変換された番号は 5551234、発信側タイプは Subscriber に設定されます。

ゲートウェイがコールを処理できなかった場合(たとえば、すべてのポートがビジーだった、など)、コールは PSTN に発信するために Chicago のゲートウェイに送信されます。Chicago ゲートウェイは次の 2 つの発信側トランスフォーメーション パターンを使用して設定されます。

- \+1708.XXXXXXX(ドットの前の番号を削除)、番号タイプ:サブスクライバ
- \+1.!,(ドットの前の番号を削除)、番号タイプ:国内

コールが Chicago のゲートウェイに送信されると、発番号は 2 番めの発信側トランスフォーメーション パターンのみとマッチングされます。そのため、ゲートウェイに送信される発番号は 4155551234 となり、発番号タイプは National に設定されます。

ゲートウェイの着番号のローカル化

コールがゲートウェイに送信されると、着番号は、ゲートウェイが接続されているトランク グループを提供する PSTN サービス プロバイダーの要件に合せる必要があります。着番号トランスフォーメーション パターンは、着番号と着番号タイプの変更に使用できます。通常、ゲートウェイの国コードを示す着番号では、+ 記号を削除し、国コードを明示するように変更する必要があります。また、それらを国のプレフィックスに置き換える必要があります。また、着番号の番号タイプを National に変更する必要があります。ゲートウェイが特定のエリア、シティ コードを示すトランク グループに接続されている場合、+ 記号、国コード、ローカル エリア コードの特定の組み合わせは通常、適切なローカル プレフィックスに置き換える必要があります。また、番号タイプは Subscriber にする必要があります。

たとえば、San Francisco のユーザへのコール（+1 415 555 2222）が、最初の選択肢として San Francisco のゲートウェイ、別の選択肢として Chicago のゲートウェイを指定したルーティング リストを介してルーティングされるとします。San Francisco のゲートウェイは 2 つの着信側トランスフォーメーション パターンを使用して設定されます。

- \+1415.XXXXXXX（ドットの前の番号を削除）、番号タイプ：サブスクライバ
- \+1.!,（ドットの前の番号を削除）、番号タイプ：国内

コールが San Francisco のゲートウェイに送信されると、着番号は両方の着信側トランスフォーメーション パターンとマッチングされます。ただし、最初のパターンの方がより正確に一致しているため、着番号の処理にはこちらが選択されます。このようにして、変換された番号は 5552222、着信側タイプは Subscriber となります。

ゲートウェイがコールを処理できなかった場合（たとえば、すべてのポートがビジーだった、など）、コールは PSTN に発信するために Chicago のゲートウェイに送信されます。Chicago ゲートウェイは次の 2 つの着信側トランスフォーメーション パターンを使用して設定されます。

- \+1708.XXXXXXX（ドットの前の番号を削除）、番号タイプ：サブスクライバ
- \+1.!,（ドットの前の番号を削除）、番号タイプ：国内

コールが Chicago のゲートウェイに送信されると、着番号は 2 番めの着信側トランスフォーメーション パターンのみとマッチングされます。そのため、ゲートウェイに送信される着番号は 4155552222 となり、着番号タイプは National に設定されます。

（注）　コールがゲートウェイに発信されると、発信側および着信側トランスフォーメーション パターンが、発信および着信番号にそれぞれ適用されます。

（注）　SIP では番号タイプが示されません。そのため、SIP ゲートウェイでは、Unified CM によって設定された着信側または発信側の番号タイプの表示を受信できません。

グローバル化されたダイヤル プランのコール ルーティング

ユーザ入力を認識するようにシステムを設定し、コールが正しい宛先にルーティングされ、送信されるようにします。コールはさまざまな形式で発信される可能性があるため、システムはそれらの各形式に一致するパターン認識を用意する必要があります。

グローバル化されたダイヤル プラン アプローチのコア ルーティングは、+E.164 パターンのルーティングに基づいているため、このダイヤル プラン アプローチのネイティブ ダイヤリング手順はグローバルな +E.164 ダイヤリングです。

Unified CM のトランスレーション パターンはローカライズされたユーザ入力を電話機からダイヤルされたものとして、Unified Communications システム内のコールのルーティングに使用するグローバル +E.164 形式に変換します。

サイトごとに設定されているコーリング サーチ スペースでは通常、次のことができます。

- サイトの、ローカル化されたサイト内のダイヤリング手順
- サイトにいるユーザの、ローカル化されたオフネットのダイヤリング手順
- 緊急通話などの適用可能なローカル テレフォニー サービス、ディレクトリおよびオペレータ サービス
- オンネットおよびオフネット番号のグローバル化された形式

図 14-30 で、米国のサンプル サイトのローカルなダイヤリング手順を使用してグローバル化された形式のダイヤリングをサポートする方法を示します。

図 14-30　ローカライズおよびグローバル化されたダイヤリング

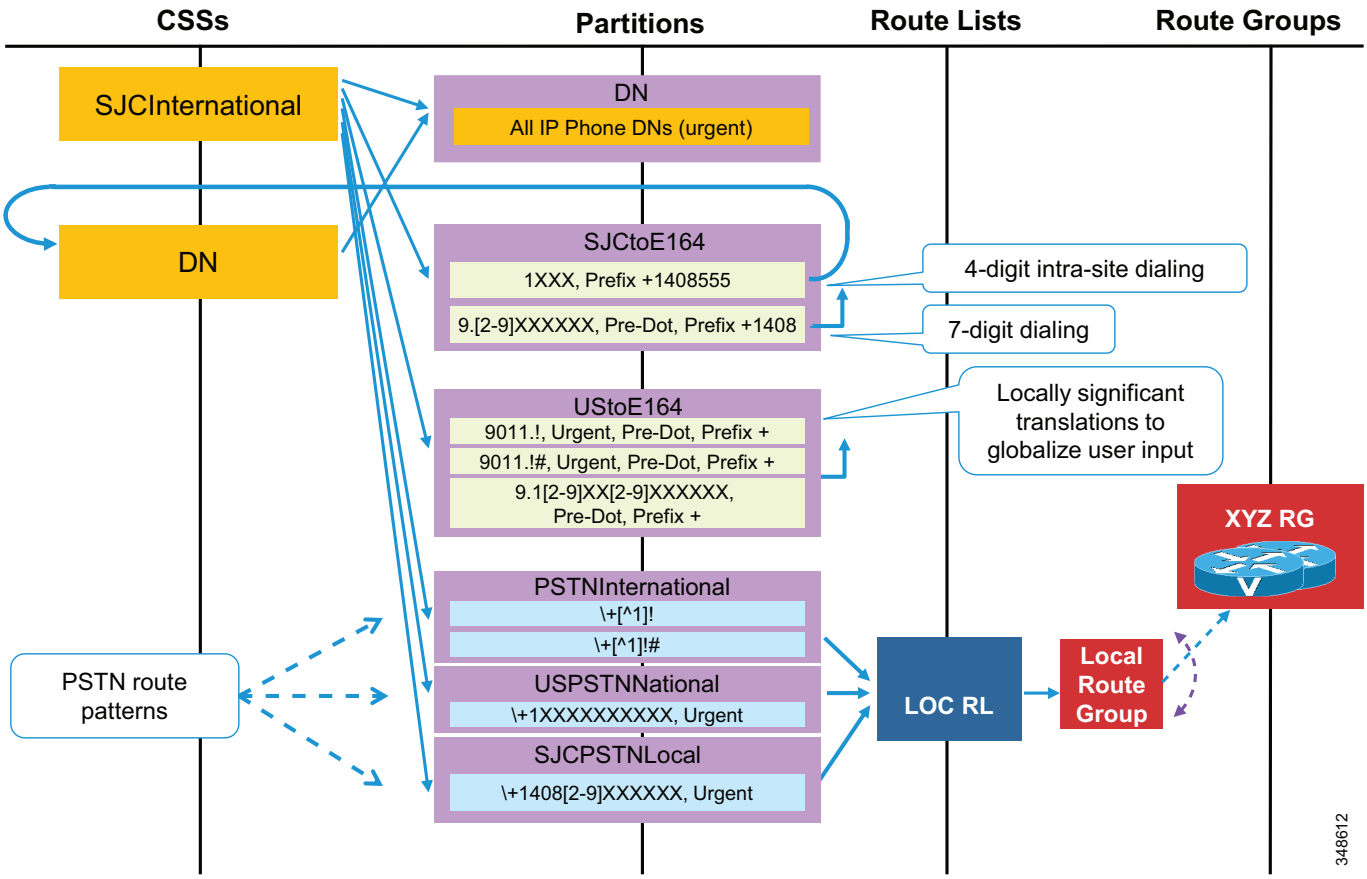


図 14-30 で、米国の IP Phone ユーザは 9011496100773 をダイヤルし、ドイツの宛先に接続してからコールを解除します。ドイツの着信側は米国のユーザにコール バックし、接続してから、コールを解除します。その後米国のユーザは Received コール ディレクトリに移り、最後の受信コールのエントリ（+49 6100 773）を選択し、[ダイヤル（Dial）] を押します。

この例では、米国のユーザは別々の 2 つのコールを同じ宛先（+496100773）に向けて開始します。最初のコールの場合、米国のダイヤリング手順に合せてローカライズされた宛先番号の形式が使用されます。対応するトランスレーション パターン 9011.! に対してユーザ入力がマッチングされます。変換されると、同じコーリング サーチ スペースがセカンダリ ルックアップ（トランスレーション パターンに設定される [発信側コーリングサーチスペースを使用（Use Originator's Calling Search Space）]）に使用され、ルート パターン \+[^1]! がコールのルーティングに使用されます。2 つめのコールの場合、宛先番号のグローバル化された形式が使用され、ルーティング パターン \+[^1]! が直接使用されます。

これらのコール フローを比較すると、このダイヤル プラン アプローチで実装される 2 ステップのルーティング プロセスが明確に示されます。最初にすべてのダイヤリング手順を +E.164 に正規化し、+E.164 パターンに基づいてルーティングします。有効な PSTN アクセス レベルは、コーリング サーチ スペースによって指定された PSTN ルート パターンで定義されます。より詳細なアクセス レベルは、特定のルート パターンを追加することによって実装できます。

パーティション DN のすべてのディレクトリ番号は、オンネット宛先が呼び出され、ダイヤルされたオンネット宛先がパーティション PSTNInternational の可変長のオフネット ルート パターンと重なった場合に、桁間タイムアウトの可能性を回避するために緊急 DN として設定されます。

パーティション SJCtoE164 での最初のトランスレーションでは、サイトのすべてのローカル DID が +1 408 555 1XXX の範囲内であると想定して、4 桁のサイト内ダイヤリングが実装されています。San Jose のサイトのローカル ダイヤリング(9+7)は、同じパーティションの 2 番目のトランスレーション パターンによって、ローカル ダイヤリング手順を +E.164 に再び変換することで実装されています。海外と国内の宛先に対する米国の PSTN ダイヤリング手順のグローバリゼーションを実装するパーティション UStoE164 にも、同じことが当てはまります。

すべてのダイヤリングの正規化トランスレーション パターンには [発信側コーリングサーチスペースを使用(Use Originator's Calling Search Space)] が設定されるため(CSS 継承)、トランスレーション パターンで定義された着信側変換を適用した後は、セカンダリ ルックアップに使用されるコーリング サーチ スペースはアクティブ化コーリング サーチ スペースと同じです。

要求されたサービス クラスを作成する単一のコーリング サーチ スペースは、回線/デバイス コーリング サーチ スペースとして使用できます。エクステンション モビリティやデバイス モビリティなどのモビリティ機能をサポートする配置では、回線コーリング サーチ スペースを使用してユーザがローミング時にサービス クラスを保持できるようにする必要があります。

これで、内線番号が +1 408 555 1234 であるユーザに、他のユーザからコーリング サーチ スペースを使用して到達できるようになります。この例では、次の番号をダイヤルします。

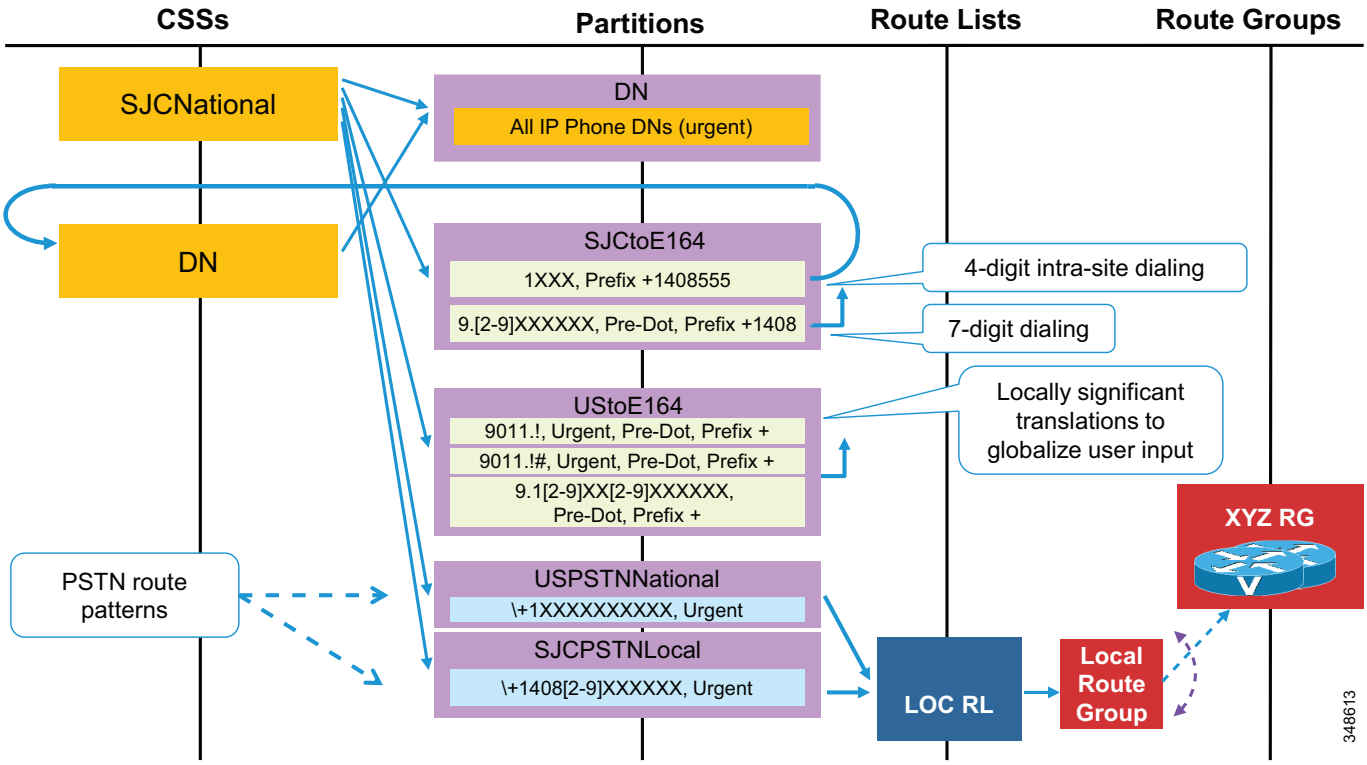
- 1234: ダイヤルされた番号は、パーティション SJCtoE164 のトランスレーション パターンによって +14085551234 に変換され、パーティション DN でディレクトリ番号と一致します。
- 95551234: ダイヤルされた番号は、パーティション SJCtoE164 のトランスレーション パターンによってグローバル化され、パーティション DN のディレクトリ番号が照合されます。
- 914085551234: ダイヤルされた番号は、パーティション UStoE164 のトランスレーション パターンによってグローバル化され、パーティション DN のディレクトリ番号が照合されます。
- +14085551234: パーティション DN のディレクトリ番号とのダイレクト マッチ。

その他のサービス クラス

図 14-30 では、サービス クラス「国際」の +E.164 ダイヤリング手順の正規化を作成するすべてのトランスレーション パターンで CSS 継承を使用するため、着信側トランスフォーメーション(+E.164 へのグローバル化)適用後にセカンダリ ルックアップのために CSS のアクティブ化も使用されます。これにより、他のサービス クラスに対して同じダイヤリングの正規化トランスレーション パターンを再使用できるようになります。

図 14-31 に、サービス クラス「国際」に使用されるスキーマと同じスキーマに基づいてサービス クラス「国内」を定義する方法を示します。図 14-30 のこのスキーマとサービス クラス「国際」との比較では、ダイヤリング正規化および PSTN ルート パターンを含むすべてのパーティションが再使用できることが確認できます。実質的に、唯一の違いは、コーリング サーチ スペース SJCNational にパーティション PSTNInternational の国際 PSTN ルート パターンへのアクセスがないことです。

図 14-31　サービス クラス間でのダイヤリングの正規化の共有



サービス クラス「国内」についても、国際ダイヤリング 9011 のローカル手順に対するダイヤリング正規化パターンへのアクセスが必要です。これは、国際オンネット宛先（米国外のパーティション DN のディレクトリ番号）への国際ダイヤリングをサポートする必要があるためです。

「市内」や「社内」などのより制限の厳しいサービス クラスが、不適切な PSTN ルート パターンを保持するパーティションへのアクセスを単に削除する同じスキーマの後に組み込まれています。

前の図で、パーティションおよびコーリング サーチ スペースに使用されている命名規則は、複数のサービス クラス、サイト、およびダイヤリング ドメインをサポートするために複製する必要があるダイヤル プランを特定するのに役立ちます。名前にサイトの指定（たとえば、パーティション名 SJCtoE164 の SJC）が含まれている場合は、すべてのサイトについてこの要素を複製する必要があります。名前にサービス クラスの指定（たとえば、SJCInternational の International）が含まれている場合は、すべてのサービス クラスについてこの要素を複製する必要があります。名前にサイトの指定が含まれていない場合は（たとえば、パーティション USPSTNNational）、同じダイヤリング手順を共有するすべてのサイト（この例では、米国のすべてのサイト）で再利用できます。

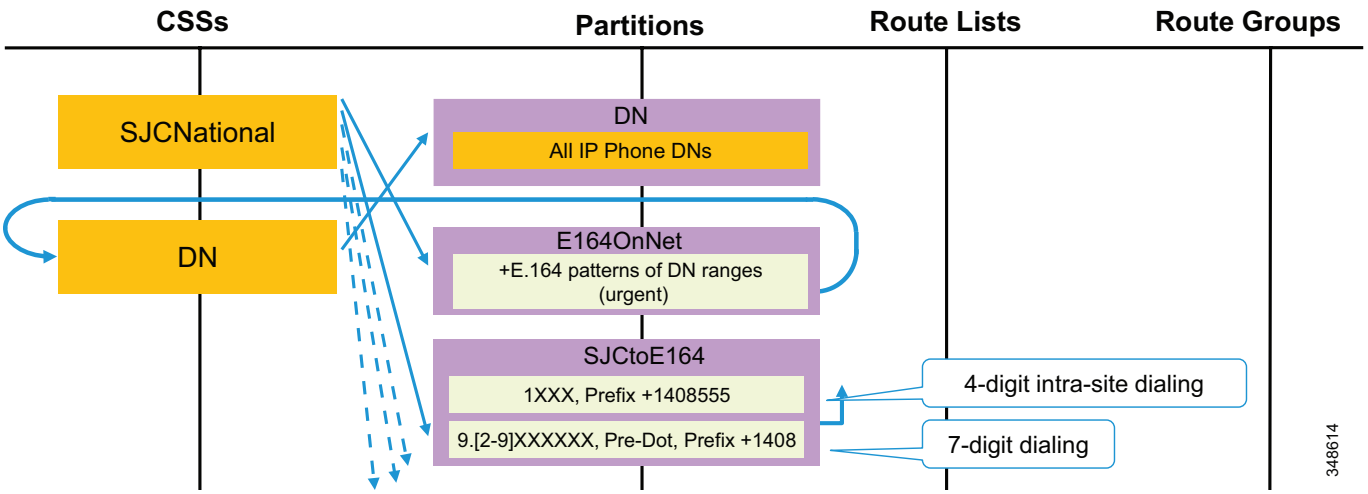
未定義 DN の呼び出し

パーティション SJCtoE164 で 4 桁ダイヤリングの正規化のトランスレーション パターン 1XXX は CSS 継承を使用しません。代わりに、このトランスレーション パターンはセカンダリ ルックアップのためのコーリング サーチ スペース DN を使用します。これは、ユーザが 1234 とダイヤルし、ディレクトリ番号 \+14085551234 が存在しない場合に、原因「未割り当ての番号」でコールが拒否されるようにするためです。パターン 1XXX で CSS 継承が使用されている場合、コールは代わりにパーティション USPSTNNational のルート パターンと一致した後で PSTN にルーティングされます。PSTN はコールをすぐに拒否するか、着信側ディレクトリ番号がないため、着信コールとして見なされて拒否されるエンタープライズの PSTN ゲートウェイにルーティングするため、最終的に同じ結果になります。どのゲートウェイにおいても、着信コーリング サーチ スペースルーティング ループは通常、内部の宛先のみにアクセスがあり、PSTN の宛先にはアクセスがないことに注意してください。これは、ルーティング ループを遮断し、電話料金の詐欺行為を回避するためです。

未定義 DN へのコールでの同じ PSTN へアピニング問題は、CSS 継承を使用したダイヤリングの正規化トランスレーション パターンによって実装される他のダイヤリング手順と、+E.164 ダイヤリングにも発生します。これらのダイヤリング手順に、DN パーティションに対するループバックへの DN コーリング サーチ スペースを使用するオプションはありません。これは、オンネットの宛先が、単にこれらのダイヤリング手順を介して到達可能になる宛先のサブセットにすぎないためです。

このヘアピニングを回避する必要のある場合、図 14-32 のスキーマを使用できます。ここでは、パーティション E164OnNet がすべてのオンネット宛先の +E.164 プレフィックスに一致する緊急トランスレーション パターンを保持します。DID 範囲が + 1 408 555 1XXX のサイトでは、E164OnNet に緊急トランスレーション パターン \+14085551XXX が存在します。これらのオンネットのインターセプト パターンは、最終的にプロビジョニングされた DN へのアクセスを提供する DN コーリング サーチ スペースにポイントし返します。すべてのダイヤリングの正規化パターン（短縮されたサイト内ダイヤリングのダイヤリング正規化パターンも含む）は CSS 継承を使用します。未定義 DN へのコールはオンネット パターンによってインターセプトされるため、PSTN にルーティングされなくなります。ダイヤルされた DN が DN パーティションにない場合、コールは原因「未割り当ての番号」によって拒否されます。

図 14-32　未定義 DN への PSTN へアピニングの回避と非 +E.164 DN のサポート



E164OnNet でのインターセプト パターンの目的としては、+E.164 からディレクトリ番号の形式へのマップがあります。たとえば、DID 範囲が +1 408 555 1XXX のサイトに対して E.164（プラスなし）としてディレクトリ番号を設定する場合、着信側変換「strip pre-dot」（+ を削除）のトランスレーション パターン \+.14085551XXX は、E164OnNet に設定する必要があります。

+E.164 としてディレクトリ番号を設定することを強く推奨しますが、ディレクトリ番号は E.164（プラスなし）などの別のグローバル化形式、簡潔な企業の番号付けスキーム、または米国の 10 桁で設定することもできます。+E.164 としてディレクトリ番号を設定しない場合、グローバル化された発信者 ID 用に、追加の番号の正規化を設定する必要があります。また、CTI アプリケーション（たとえば、アテンダント コンソール アプリケーション）によっては、設定されたディレクトリ番号がグローバル ディレクトリに格納されている形式に一致しない場合、追加の番号の正規化が必要になる場合があります。

+E.164 DN が使用され、未定義の DN へのオンネット コールの稀なヘアピニングがクリティカルであると見なされない場合、パーティション E.164OnNet にオンネット DN のリストを維持するための取り組みは避け、図 14-30 と図 14-31 に示す簡素化されたダイヤル プラン アプローチを導入する必要があります。

緊急通話

緊急サービスへのアクセスは、すべてのユーザに許可する必要があります。そのためには、緊急番号ルート パターンのパーティションを各コーリング サーチ スペースに追加するか、デバイス レベルのコーリング サーチ スペースを介した緊急番号ルート パターンへのアクセスを有効にします。デバイス コーリング サーチ スペース経由の緊急番号へのアクセスが許可されている場合は、ローミング シナリオ（たとえば、エクステンション モビリティ）において、ユーザは訪問したサイトのダイヤリング手順を使用して、緊急サービスをダイヤルする必要があります。一方、回線コーリング サーチ スペース経由の緊急番号へのアクセスの場合、ユーザはホーム サイトのダイヤリング手順を使用して緊急サービスをダイヤルできます。この違いが明らかに重要になるのは、ホーム サイトと訪問したサイトで緊急サービスのダイヤリング手順が異なる場合のみです。たとえば、欧州のユーザ（緊急番号 112）が米国の電話機（緊急番号 911）にログインする場合などです。

通常、推奨される方式は、発信側デバイスの物理的な場所にローカルな緊急番号で、緊急通話サービスを提供することです。これによって緊急番号と他のダイヤリング手順との間でオーバーラップが発生する場合がありますが（たとえば、短縮ダイヤリングが 9XXX のサイトから米国の電話機にログインした米国以外のユーザのための 9 で始まる 4 桁のサイト内ダイヤリングと、911）、少なくとも、指定された場所の電話機は、いつでも、別の緊急番号を使用する地域のリモート ユーザがログインしているかどうかに依存せずに、現地の慣習的な緊急ダイヤリングを使用して緊急通話を発信できることが保証されます。

この動作を実装するには、緊急パターンをデバイス コーリング サーチ スペースで処理できる必要があります。

デザイン アプローチの利点

新しいグローバリゼーション機能により有効になったダイヤル プラン デザイン アプローチの利点は、次のとおりです。

- コールのルーティング、特にローカルから PSTN に発信する場合の簡素化された設定。
- システム機能の簡素化された設定と拡張機能。次のものがあります。
  - 自動代替ルーティング（AAR）
  - Emergency Responder サイト固有のフェールオーバー
  - Call Forward Unregistered（CFUR）

- テールエンド ホップオフ（TEHO）
- Cisco Jabber などのソフト クライアントからの E.164 番号のクリックツーダイヤル
- ローミング中のエクステンション モビリティ ユーザまたはローミング デバイスから発信されたスピード ダイヤルの適合コール ルーティング
- 電話機ディレクトリ エントリ（デュアルモードの電話機を含む）からのワンタッチ ダイヤリング
- IP Phone ディレクトリの Missed Calls および Received Calls リストからのワンタッチ ダイヤリング

自動代替ルーティング

自動代替ルーティング（AAR）宛先マスクがグローバル化された形式に入力されている場合、およびすべての AAR CSS がグローバル化された形式で宛先にコールをルーティングできる場合、システム管理者は AAR グループを設定できます。それは、この機能が、特定の宛先に到達するために、発信電話機の PSTN アクセスの地域要件に基づいてどの数字をプレフィックスとして付加するかを決定する唯一の機能であるためです。プレフィックス番号が設定されていない単一の AAR グループはプロビジョニングしたすべてのデバイスに対して使用できます。

（注）　AAR を有効にするには、着信側ディレクトリ番号がグローバル化された形式ですでに設定されている場合でも、着信先で AAR マスクまたは外部電話番号マスクをグローバル化された形式で設定する必要があります。AAR は AAR マスクまたは外部電話のマスクが設定されている場合にだけアクティブになります。

さらに、ほとんどの場合、この AAR CSS の唯一の機能では、コールを発信電話機と同じ場所にあるゲートウェイにルーティングします。そのため、標準ローカル ルート グループを含むルーティング リストを指す 1 つだけのルート パターン（\+!）を使用して設定できます。この 1 つのルーティング パターンを使用してルーティングされるコールは常に発信エンドポイントに関連付けられたローカル ルート グループを介してルーティングされるため、どのリージョン、どの国にいるとしても、すべてのサイトのすべての電話でこの 1 つの AAR CSS を使用できます。

Cisco Emergency Responder

Cisco Emergency Responder へのコールのルーティングは通常、911 CTI ルート ポイントをプライマリ Emergency Responder サーバに接続し、また 912 CTI ルート ポイントをバックアップ Emergency Responder サーバに接続するように設定することによって行われます。

どちらの Emergency Responder サーバも利用できない場合、911 コールは、PSTN が発信側電話機と同じ場所にあるゲートウェイに発信されるように指示できます。設定は次のようにします。

- Call Forward No Answer（CFNA）への 911 CTI ルート ポイントおよび 912 への Call Forward Busy（CFB）、912 CTI ルート ポイントのパーティションを含むコーリング サーチ スペースを介して。
- CFNA への 912 CTI ルート ポイントおよび 911 への CFB、グローバル パーティションを含むコーリング サーチ スペースを介して。グローバル パーティションは標準ローカル ルート グループを含むルート リストを指すルート パターン 911 を含む。

どちらの CTI ルート ポイントも登録解除された場合、911 へのコールは、発信電話機のデバイス プールで決定されたとおりにローカル ルート グループに転送されます。デバイス モビリティが設定されている場合、ローミング電話機は訪問したサイトのデバイス プールと関連付けられます。このため訪問したサイトのローカル ルート グループと関連付けられます。

Call Forward Unregistered（CFUR）

Call Forward Unregistered 機能によって処理されるコールが、発信側電話機と同じ場所にあるゲートウェイを使用するようにするには、電話機の CFUR 宛先を、PSTN 番号のグローバル化された+ 形式を使用して設定します。CFUR CSS は、標準ローカル ルート グループを含むルート リストを指す 1 つのルート パターン（\+!）のみを使用して設定できます。この 1 つのルーティング パターンを使用してルーティングされるコールは常に発信エンドポイントに関連付けられたローカル ルート グループを介してルーティングされるため、どのリージョン、どの国にいるとしても、すべてのサイトのすべての電話で同じ CSS を使用できます。

テールエンド ホップオフ（TEHO）

PSTN 接続料金を低くするため、システム管理者は、IP ネットワークを使用してオフネットの宛先にコールをルーティングし、PSTN への出口点を着信番号のできるだけ近くにします。同時に、コールの優先 TEHO ルートが使用できない場合、発信電話のローカル ゲートウェイを使用してコールを PSTN に送信する必要がある場合もあります。これは、特定の番号タイプの TEHO ルーティングに参加しているすべての電話で、特定の宛先番号に一致するルート パターンと一致するように設定し、その番号が最初のエントリとして、選択した TEHO 出口ゲートウェイを含むルート リストを、2 番めのエントリとして標準ローカル ルート グループを指すように設定することによって実現できます。

グローバル ダイヤル プラン レプリケーション（GDPR）でのダイヤル プラン

+E.164 の代替番号とエンタープライズ代替番号はマスクを使用してディレクトリ番号に定義され、ローカル番号分析に挿入されて、リモート呼制御にアドバタイズされます。ローカル番号分析への挿入とリモート呼制御へのアドバタイズは個別に有効化できるオプションです。番号をローカル番号分析に挿入し、リモート呼制御にアドバタイズするか、リモート呼制御の PSTN フェールオーバー番号として使用する必要がある場合にのみ、+E.164 またはエンタープライズ代替番号を定義する必要があります。

ローカル番号分析にエンタープライズまたは +E.164 の代替番号を挿入することによって、実質的にディレクトリ番号へのダイヤリングの代替手段を作成します。サイト SJC のディレクトリ番号 \+14085551234 に対しては、マスク 1XXX を使用してパーティション SJCToE164 のエンタープライズ代替番号を定義することもできます。これは、このパーティションでローカル パターン 1234 を作成します。サイトのすべての DN に対して同じエンタープライズ代替番号方式を使用して、SJC は、図 14-30 と図 14-31 に示す 4 桁のサイト内ダイヤリング トランスレーション パターン 1XXX の削除を実質的に許可します。このスキーマは、ローカル サイトだけで有効なエンタープライズ代替番号が曖昧さを避けるためにサイト固有のパーティションに挿入されるため、複数のサイトに拡張できます（たとえば、表 14-4 を参照）。

表 14-4　　ローカル サイトのエンタープライズ代替番号

サイト	DID 範囲	エンタープライズ代替番号マスク	エンタープライズ代替番号パーティション
SJC	+14085551XXX	1XXX	SJCToE164
RTP	+19195552XXX	2XXX	RTPToE164
NYC	+12125551XXX	1XXX	NYCToE164

ディレクトリ番号 +14085551234 および +12215551234 に対し、表 14-4 に示す設定を使用してまったく同じエンタープライズ代替番号 1234 が作成されますが、サイトの特性が維持されるように、それぞれ異なるパーティション内にあります。

表 14-4 のスキーマは、ローカルの番号分析に追加された GDPR エンタープライズ代替番号が、このダイヤリング手順のダイヤリングの正規化トランスレーション パターンを追加せずに、どのように短縮されたサイト内ダイヤリングの実行に使用できるかを示していますが、ローカル サイトでだけ有効なエンタープライズ代替番号は GDPR にはアドバタイズされません。受信するクラスタでは、重複する（および同一の可能性のある）エンタープライズ代替番号は、ルーティングに曖昧さを生じるため学習する必要があります。

（注）　シスコは GDPR でグローバルに有効なエンタープライズ代替番号だけをアドバタイズすることを推奨します。通常、これらのエンタープライズ代替番号は企業の短縮オンネット番号付けプランに沿っています。

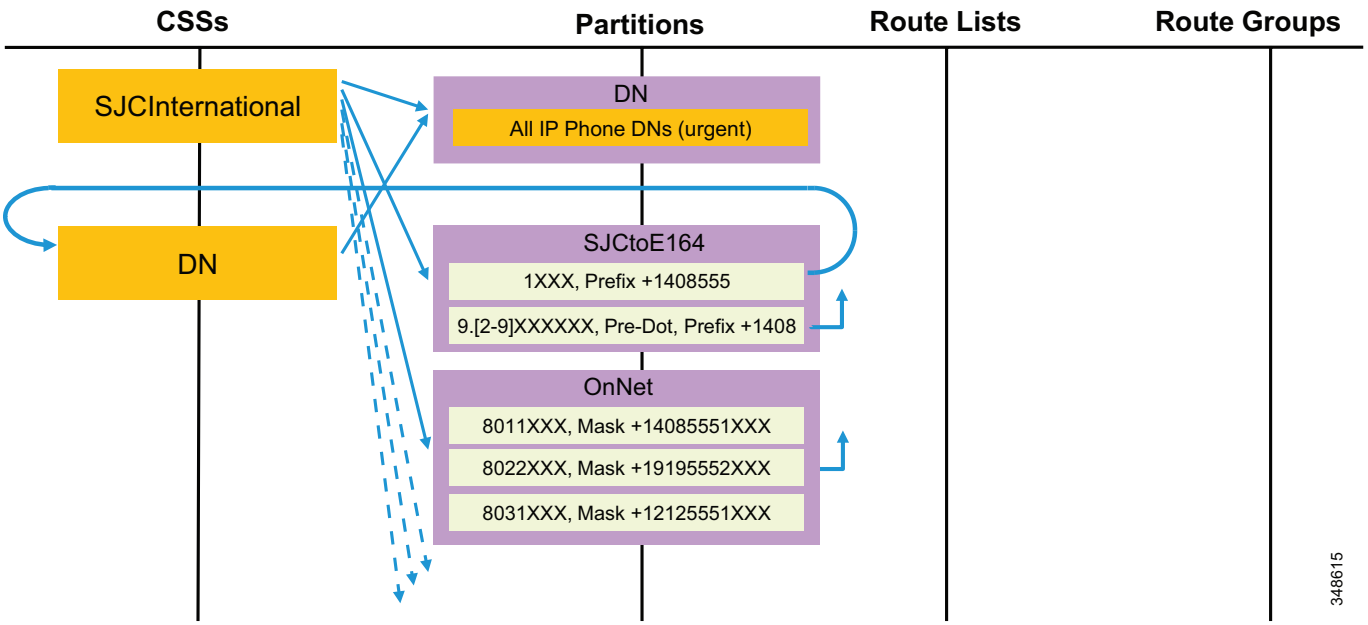
表 14-5 は、アクセス コードとして 8 と 2 桁のサイト番号を使用する企業の短縮オンネット番号プランに基づいて、潜在的なエンタープライズ代替番号スキーマを示します。

表 14-5　グローバル エンタープライズ代替番号

サイト	DID 範囲	エンタープライズ代替番号マスク	エンタープライズ代替番号パーティション
SJC	+14085551XXX	8011XXX	DN
RTP	+19195552XXX	8022XXX	DN
NYC	+12125551XXX	8031XXX	DN

これらのエンタープライズ代替番号はグローバルで有効になったため、すべての市内電話番号に対する短縮サイト間のダイヤリング手順を実行する DN のパーティションに簡単に追加できます。ダイヤリングの正規化トランスレーション パターンに基づいて同等に短縮サイト間オンネット ダイヤリング手順を実行するための従来のアプローチを図 14-33 に示します。

図 14-33　短縮されたサイト内のオンネット ダイヤリングの正規化トランスレーション パターン



（エンタープライズ代替番号をローカル番号分析に追加するか、ダイヤリングの正規化を使用する）どちらのスキームも同等のユーザ エクスペリエンスを実装します。唯一の違いは、ダイヤリングの正規化パターンでは、このオーバーレイ ダイヤリング手順を使用してダイヤルされた未定義番号へのコールは PSTN にルーティングされてから、ヘアピンし返されることです。一方で、ローカル番号分析に各電話番号の明示的なエンタープライズ代替番号を追加すると、ローカル ダイヤル プランのトラブルシューティングをより複雑にする可能性のあるローカル ダイヤル プランを大幅に拡大します。

エンタープライズ代替番号と同様に、+E.164 代替番号も電話番号をマスキングすることによって定義されます。+E.164 DN の +E.164 代替番号を定義するには、マスクを単に空のままにしておくことができます。+E.164 DN の +E.164 代替番号はローカルのダイヤル プランに追加すべきではありませんが、リモート呼制御に +E.164 代替番号または +E.164 PSTN フェールオーバー番号をアドバタイズできる必要があります。

ダイヤリングの正規化トランスレーション パターンを使用して、各電話番号に対するエンタープライズ代替番号を定義する代わりに、短縮されたオンネットのダイヤリング手順を実行することは、より少ないパターンが実際に番号分析に追加されるため、番号分析の複雑さが軽減されます。同様に、ディレクトリごとの個々の代替番号の代わりに、+E.164 とエンタープライズ代替パターンをアドバタイズすることによって、アドバタイズされたダイヤル プラン要素の数を最小限にし、GDPR からアドバタイズされた情報をインポートするリモート呼制御のダイヤル プランの複雑さを軽減します。+E.164 とエンタープライズ パターンの形式でサマリーだけをアドバタイズすることを強くお勧めします。

GDPR からダイヤル プラン情報を学習する呼制御は、タイプによって異なるパーティションに学習された情報を挿入できます（+E.164 代替番号、エンタープライズ代替番号、+E.164 パターン、エンタープライズ パターン）。必要なサービス クラスを実行するためにこのタイプ ベースの差別化が必要ない場合、GDPR から学習したすべての数値のダイヤル プラン情報は、リモート オンネットの宛先にアクセスできるサービス クラスを実行するすべてのコーリング サーチ スペースに追加される単一のパーティションに送信できます（図 14-33 に示すオンネットのパーティションなど）。

差別化されたサービス クラスも、GDPR にアドバタイズされる SIP ルート文字列の形式でロケーション情報のルーティング スキーマを作成する SIP ルート パターンへのアクセスの制限に基づいて行うことができます。これにより、アドバタイズされた SIP ルート文字列の到達可能性に基づいて、特定の呼制御または特定のインポートされた GDPR カタログの一部としてアドバタイズされた宛先の到達可能性を制限できます。

Unified Communications Manager と TelePresence Video Communication Server の統合

Cisco Unified Communications Manager（Cisco Unified CM）は、Cisco TelePresence System C シリーズ、EX シリーズ、Profile シリーズ、SX シリーズのコーデック登録および英数字 URI ダイヤリングをサポートします。このシナリオで、Cisco TelePresence Video Communication Server（VCS）は、2 個の主要な機能を実行できます。

- ビデオおよびコンテンツの H.323 と SIP の相互運用性
- VCS Control および VCS Expressway を使用した Business-to-Business（B2B）アクセス

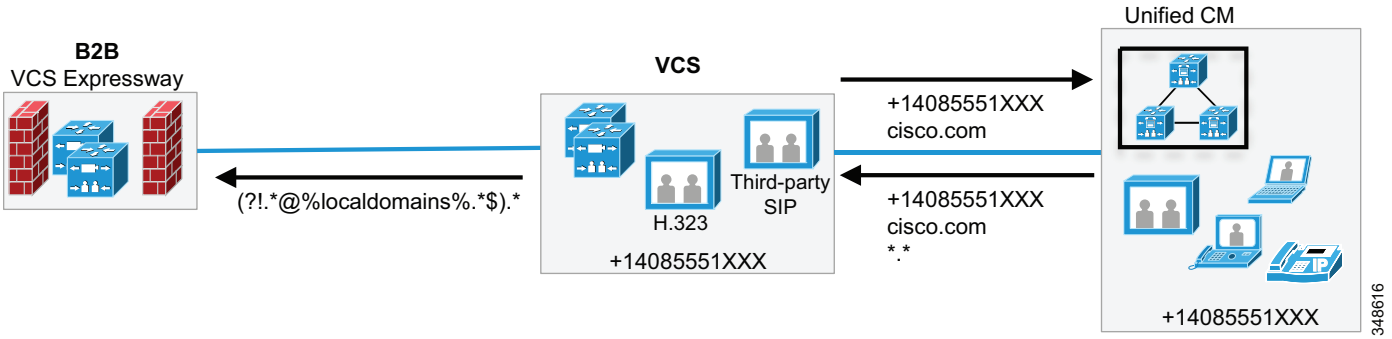
H.323 レガシー エンドポイントを VCS に登録でき、これにより、H.323/H.239 と SIP Binary Flow Control Protocol（BFCP）との間のプロトコル変換とコンテンツの相互運用性を実現します。このシナリオで、VCS はシグナリングおよびメディア ゲートウェイとして機能し、メディアを処理する必要もあるため、インターワーキング機能をオンにしなければならないことに注意してください。

VCS に接続されている H.323 エンドポイントは、Unified CM と同じ番号計画を共有します。

エイリアスの操作および正規化は、標準ベースの Portable Operating System Interface for Unix（POSIX）形式の正規表現構文を使用して VCS で行われます。POSIX は、オペレーティング システム（UNIX）がサポートする必要がある照合および置換機能のいくつかを定義する標準のコレクションです。

図 14-34 に、Unified CM と VCS に登録された音声およびビデオ エンドポイント間のエンドツーエンド通信、および VCS Expressway による企業の外部のピアとの通信を可能にする Cisco VSC と Unified CM の相互接続のトポロジ例を示します。

図 14-34　Cisco VCS と Unified CM を相互接続するためのサンプル トポロジ



+E.164 番号計画

Unified CM と VCS との間でグローバル化されたコール ルーティングを可能にするには、Unified CM のグローバル化されたダイヤル プラン アプローチ（14-61 ページ）の項で説明したグローバル化されたダイヤル プランを Unified CM で実装し、+E.164 アドレスを VCS にプロビジョニングする必要があります。また、VCS に登録された各エンドポイントの H.323 ID が、+E164 番号とともに設定され、ローカル ゾーンに登録されなければなりません。

エイリアスの正規化と操作

エイリアスの正規化の目的は、エンドポイントをダイヤリングするときに、正しいエイリアスを示すことです。エイリアスの正規化は、システム レベルまたはゾーン レベルで発生する可能性があります。

システム レベルの正規化の例は、H.323 エンドポイントと SIP エンドポイントが VCS に登録されている混在環境でダイヤル プランの透過性を実装するときに発生します。H.323 エンドポイントは、VCS のローカル ゾーンに H.323 ID と E.164 エイリアスを登録します。ただし、SIP エンドポイントが E.164 エイリアスをダイヤルすると、ユーザが E.164 番号をダイヤルしただけでも、自動的にドメインが追加されます。E.164 番号が相手側の VCS にとってローカルまたはリモートのいずれであっても、正規化ルールによってコールの転送前に、ドメインが削除されます。これは、トランスフォームを使用して行うことができます。

ゾーン レベルの正規化の例は VCS を Unified CM クラスタに接続したときに発生します。この場合、Unified CM が、登録されているエンドポイントのエイリアスに一致しないエイリアス形式を使用している可能性があります。これは、Unified CM から受信したコールでだけ発生するため、宛先への転送前に検索ルールを適用して、エイリアスを標準化できます。

正規化後に、操作も発生する可能性があります。コールが VCS のエイリアス形式をサポートしない非 VCS システムに送信される際に、正規化の後で操作が発生する可能性があります。

次の例で、H.323 エンドポイント接続および B2B 接続に使用される VCS クラスタに接続された Unified CM クラスタについて考えます（図 14-34 を参照してください）。

この場合、エイリアスの正規化は必要ありません。すべてのエンドポイントは +E164 エイリアスと同じ H.323 ID で到達可能です。ただし、Unified CM との間で送受信されるコールは、最終的な宛先にルーティングされる前に操作を必要とします。

H.323 エンドポイントが VCS に登録されている別の H.323 エンドポイントをコールするとき、H.323 ID と同じに設定されている +E.164 番号を使用し（図 14-34 の +14085551001）、コールは正しく発信されます。

ただし、コールが Unified CM に送られるときは、SIP-to-H.323 インターワーキングが発生し、結果としてドメインを追加する検索ルールが必要になります。範囲 +14085551XXX の +E.164 番号がローカル VCS で使用されていると仮定すると、例 14-5 の検索ルールが必要です。

例 14-5　VCS のローカル +E.164 宛先用の検索ルール

```
検索ルール「To VCS」
[説明(Description)]:ローカル +E164 へ
[優先度(Priority)]:50
[モード(mode)]:[エイリアスのパターン マッチ(alias pattern match)]
[パターン タイプ(pattern type)]:[正規表現(regex)]
[パターン文字列(pattern string)]:(\+14085551\d{3})(@.*)
[パターン動作(pattern behavior)]:[文字列の置換(replace string)]:\1
[正常に一致する場合(On successful Match)]:[停止(Stop)]
[ターゲット(Target)]:[ローカル ゾーン(Local Zone)]
```

内部の範囲をダイヤルする VCS に登録された各 H.323 クライアントは、このルールに一致します。

+E.164 コールが Unified CM から VCS に着信した場合、ダイヤルされたアドレスは次のいずれかの形式になります。

- +14085551XXX@10.10.10.10:5060（@ に続いて VCS の IP アドレスとポート番号。ポート番号は 5060 か、Unified CM のトランク設定でピアとして VCS の IP アドレスを使用する場合は 5061）
- +14085551XXX@vcs1.cisco.com:5060（@ に続いて VCS の DNS 名とポート番号。ポート番号は 5060 か、Unified CM のトランク設定で VCS の DNS 名を使用する場合は 5061）
- +14085551XXX@cisco.com:5060（@ に続いてドメインとポート番号。ポート番号は 5060 か、Unified CM のトランク設定でドメイン名と DNS SRV レコードを使用する場合は 5061）

Unified CM から VCS へのトランクを設定する推奨される方法は、Unified CM の IP アドレスを使用して、VCS をピアとして定義する方法です。

例 14-5 のパターン文字列 (\+14085551\d{3})(@.*) は、上の 3 つの形式のすべてと一致し、定義された置換文字列で受信した SIP URI の右側が削除されます。これによって、受信した +E.164 アドレスは VCS で設定された H.323 ID と正しく一致するようになります。

より優れたパターン選択が必要な場合には、より厳しいパターン マッチングを使用することが可能です。たとえば、([^@]*)@(%ip%|[^@]*cisco.com(.*)) を使用します。このパターンは、@ を含まれない文字シーケンスで始まり、@ と、VCS クラスタの VCS ピアの IP アドレスまたは「cisco.com」とポート番号を含む文字列が続くすべての URI と一致します。

いくつかの SIP エンドポイントが VCS に登録されている場合、自動的にドメインが追加されます。この場合も、上記の検索ルールでドメインが削除されます。

VCS から Unified CM にルーティングされる数字の +E.164 コールの場合、H.323 エンドポイントが自動的にドメインを追加しないため、発信要求の SIP URI にドメインを追加しなければなりません。Unified CM に送信されるコールのドメインを追加するために、例 14-6 に示すような検索ルールを作成しなければなりません。

例 14-6 検索ルール「To UCM」

```
検索ルール「To UCM」
[説明(Description)]:UCM +E164 へ
[優先度(Priority)]:100
[モード(mode)]:[エイリアスのパターン マッチ(alias pattern match)]
[パターン タイプ(pattern type)]:[正規表現(regex)]
[パターン文字列(pattern string)]:(\+14085551\d{3})(.*)
[パターン動作(pattern behavior)]:[文字列の置換(replace string)]:\1@cisco.com
[正常に一致する場合(On successful Match)]:[停止(Stop)]
[ターゲット(Target)]:[UCM ゾーン(UCM Zone)]
```

例 14-6 の検索ルールによって、\+14085551XXX に一致し、ローカル クライアントに一致しない VCS からのすべての数字のダイヤリングが Unified CM に送信され、Unified CM に送信される SIP URI のホスト部分が「cisco.com」に設定されます。Unified CM での SIP 要求のルーティング（14-52 ページ）の項、特に図 14-29 に記載されているように、Unified CM 内の SIP ルーティング メカニズムに従って、Unified CM が Unified CM で設定された番号の +E.164 ダイヤル プランに従ってこれらの数字の SIP URI のパスを指定するように Unified CM の組織のトップ レベル ドメイン（OTLD）は「cisco.com」に設定されていなければなりません。このルールは、VCS に登録された SIP エンドポイントがある場合、これにも一致します。

B2B 接続を可能にするには、VCS が、B2B 構築ブロックにローカル以外の SIP URI のホスト部分があることで識別されるすべての B2B コールを VCS Expressway にルーティングしなければなりません。例 14-7 の検索ルールは、cisco.com 以外のドメインを持つものすべてに一致し、一致したものを VCS Expressway およびインターネットへ送信することによって、これを実現します。

例 14-7 B2B の検索ルール

```
検索ルール「External」
[説明(Description)]:B2B 用
[優先度(Priority)]:110
[モード(mode)]:[エイリアスのパターン マッチ(alias pattern match)]
[パターン タイプ(pattern type)]:[正規表現(regex)]
[パターン文字列(pattern string)]:[^@]*@[^@]*(?<!cisco.com)
[パターン動作(pattern behavior)]:[変更なし(leave)]
[正常に一致する場合(On successful Match)]:[停止(Stop)]
[ターゲット(Target)]:[VCS-E]
```

Unified CM で、VCS でホストされる +E.164 プレフィックスは、特定の +E.164 ルート パターンを Unified CM ダイヤル プランに追加し、適切なルート リストおよびルート グループ設定によってこのルート パターンが VCS へのトランクに対応することを確認することによって、追加されなければなりません。

VCS に登録されたエンドポイントが Unified CM に登録されたエンドポイントと同じ DN 範囲を共有している場合、Unified CM のダイヤル プラン設定は、Unified CM で不明であるローカル プレフィックスのすべての +E.164 番号が VCS にルーティングされることを保証しなければなりません。図 14-35 に、グローバル化されたダイヤル プラン アプローチでこれを実現する方法を示します。

図 14-35　未割り当てのディレクトリ番号の代行受信

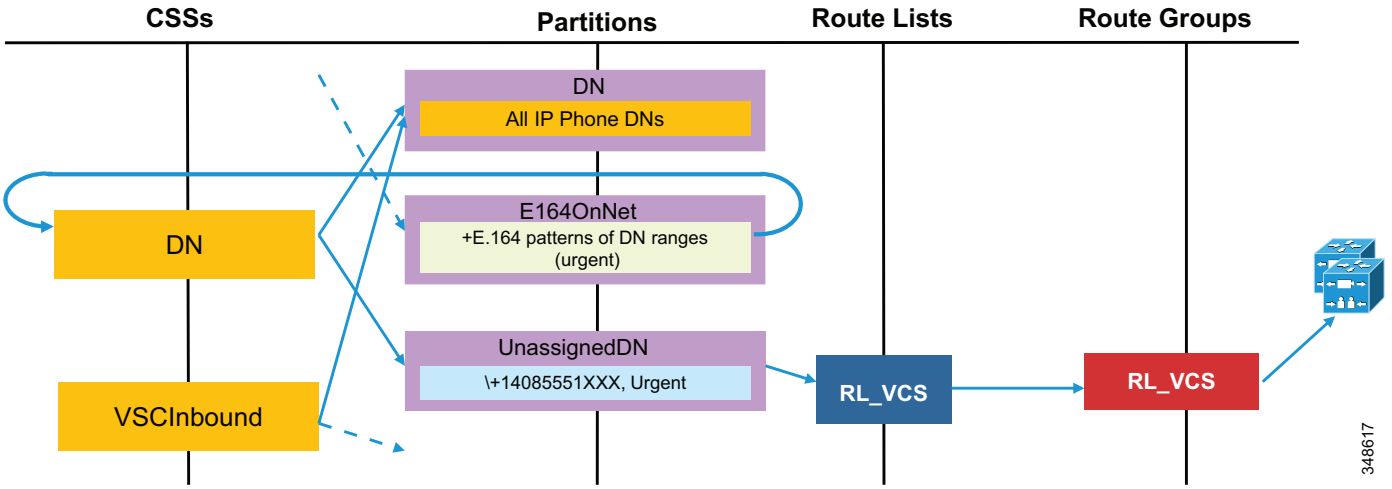


図 14-35 のグローバル化されたダイヤル プランは、Unified CM のグローバル化されたダイヤル プラン アプローチ (14-61 ページ) の項で説明したアプローチを使用します。端的に言えば、既知のオンネット +E.164 プレフィックスで一致する、すべてのダイヤリングの正規化のトランスレーション パターンおよび緊急トランスレーション パターンから参照される DN コーリング サーチ スペースは、VCS と共有する +E.164 プレフィックスで一致するルート パターンを含むように拡張しなければなりません。Unified CM のディレクトリ番号と一致しなかったこの範囲のすべての +E.164 パターンは、このルート パターンに一致し、VCS に送信されます。ルーティング ループが発生しないように、VCS から着信するトランクの着信コーリング サーチ スペースは、このルート パターンにアクセスして戻らないようにしてください。

また、Unified CM のダイヤル プランは、Unified CM にとってローカルなディレクトリ URI に対応しない、URI (数字でない) としてダイヤルされたすべてのコールが VCS にルーティングされるようにする必要があります。これを実現する最も簡単な方法は、Unified CM で、適切なルート リストおよびルート グループ設定を通じて VCS へのトランクにも対応する「catch-all」SIP ルート パターン (*.* など) を追加することです。ここでも、ルーティング ループが発生しないように、VCS から着信するトランクの着信コーリング サーチ スペースは、この「catch-all」SIP ルート パターンにアクセスしないようにしてください。

エンドポイント SIP URI の実装

Unified CM のエンドポイントに SIP URI および +E164 番号を使用して到達できる場合、例 14-8 に示すように、VCS から Unified CM に正しくルーティングする別の検索ルールを追加できます。

例 14-8　VCS から Unified CM への URI ダイヤリングの検索ルール

```
検索ルール「URI To UCM」
[説明(Description)]:SIP URI から UCM
[優先度(Priority)]:100
[モード(mode)]:[エイリアスのパターン マッチ(alias pattern match)]
[パターン タイプ(pattern type)]:[サフィックス(suffix)]
[パターン文字列(pattern string)]:cisco.com
[パターン動作(pattern behavior)]:[変更なし(leave)]
[正常に一致する場合(On successful Match)]:[停止(Stop)]
[ターゲット(Target)]:[UCM ゾーン(UCM Zone)]
```

H.323 エンドポイントが、+E.164 エイリアスを使用する代わりに同じ SIP URI 形式の英数字のエイリアスを使用してアドレス指定されている場合、例 14-5 の「To VCS」検索ルールは、例 14-9 のいずれかに置き換えることができます。

例 14-9　H.323 登録エンドポイントの URI ダイヤリングをサポートするように変更された検索ルール「To VCS」

```
検索ルール「To VCS」
[説明(Description)]:ローカル H.323 エイリアスへ
[優先度(Priority)]:50
[モード(mode)]:[エイリアスのパターン マッチ(alias pattern match)]
[パターン タイプ(pattern type)]:[サフィックス(suffix)]
[パターン文字列(pattern string)]:cisco.com
[パターン動作(pattern behavior)]:[変更なし(leave)]
[正常に一致する場合(On successful Match)]:[続行(Continue)]
[ターゲット(Target)]:[ローカル ゾーン(Local Zone)]
```

エイリアスがローカル ゾーンにない場合、これはエイリアスではなくローカルであることを意味し、優先度 100 の次のルール(「To CUCM」)に従って Unified CM に送信されるため、「続行(Continue)」を有効にしなければなりません。ただし、コールが Unified CM から送信された場合は、コールの発信元である CUCM ゾーンに戻されないため、ルーティング ループが防止されます。

Unified CM で、+E.164 が VCS にルーティングするために使用する同じルート リストを指す「cisco.com」に一致する SIP ルート パターンを作成しなければなりません。

Unified CM のユーザが alice@cisco.com をダイヤルすると、Unified CM は最初に、ローカルに設定された SIP URI とこの URI を照合し、次にフォール バックとして、設定された SIP ルート パターンとホスト部分(cisco.com)を照合し、上記の SIP ルート パターンが一致して、コールは VCS にルーティングされます。VCS で URI がわかっている場合は、コールがエンドポイントにルーティングされますが、URI が未知である場合、コールはそのゾーンから送信され、操作されていないため、Unified CM に戻されません。

特記事項

この項では、次のような多くの Cisco Unified CM の機能に関連する、ダイヤル プランに関する考慮事項を説明します。

- 自動代替ルーティング(14-85 ページ)
- デバイス モビリティ(14-89 ページ)
- エクステンション モビリティ(14-90 ページ)
- 時間帯ルーティング(14-97 ページ)
- 論理パーティション(14-98 ページ)

自動代替ルーティング

自動代替ルーティング（AAR）機能を使用すると、Unified CM で音声メディア用の代替パスを確立できます。このパスが確立されるのは、同じクラスタ内の 2 つのエンドポイント間にある優先パスで、コール アドミッション制御用のロケーション メカニズムによって決定される使用可能な帯域幅が使い果たされたときです。

AAR 機能の主な適用対象は、WAN 経由で接続されているサイトを使用する配置です。たとえば、支店 A の電話から支店 B の電話にコールする場合、支店間の WAN リンクで使用可能な帯域幅（ロケーション メカニズムによって計算）が不足しているときは、AAR によって PSTN 経由でコールを再ルーティングできます。コールの音声パスは、発信元の電話からローカルの（支店 A の）PSTN ゲートウェイまでは IP ベース、このゲートウェイから PSTN を経由して支店 B のゲートウェイまでは TDM ベース、支店 B のゲートウェイから宛先の IP Phone までは IP ベースです。

AAR による処理は、ユーザには見えません。ユーザが着信側電話のオンネット（たとえば 4 桁の）ディレクトリ番号にしかダイヤルできないように AAR を設定すると、PSTN などの代替ネットワーク経由で宛先に到達するときに、ユーザによる追加入力が不要になります。

（注）　AAR では、CTI ルート ポイントがコールの発信元や宛先になることはサポートしていません。また、ユーザが複数のサイトにわたってローミングする場合、AAR はエクステンション モビリティ機能と共存できません。詳細については、エクステンション モビリティ（14-90 ページ）を参照してください。

AAR を正常に動作させるには、AAR の次の主要要素を指定する必要があります。

- 宛先 PSTN 番号の確立（14-85 ページ）
- 必要なアクセス コードの付加（14-86 ページ）
- 適切なダイヤル プランおよびルートの選択（14-88 ページ）

宛先 PSTN 番号の確立

コールを再ルーティングするには、PSTN などの代替ネットワーク経由でルーティングできる宛先番号を使用する必要があります。AAR では、ダイヤルされた番号を使用してコールのオンクラスタでの宛先を特定し、その番号を着信側の AAR 宛先マスクと結合します。AAR 宛先マスクが設定されていない場合には、その代わりに外部電話番号マスクが使用されます。ダイヤルされた番号と適切なマスクを結合することで、代替ネットワークによってルーティング可能な、完全修飾番号を生成する必要があります。

または、AAR 設定でボイスメールのチェックボックスをオンにすることで、コールをボイスメールのパイロット番号に転送できます。この選択では、発信者によってダイヤルされた元の番号を利用しませんが、ボイスメール プロファイル設定に従ってコールがルーティングされます。

（注）　デフォルトでは、ディレクトリ番号設定によってコールの AAR レッグがコール履歴に保持されます。これによって、ボイス メッセージング システムへの転送で適切なボイスメールボックスが選択されます。「Remove this destination from the call forwarding history」を選択した場合には、コールの AAR レッグがコール履歴に保持されません。そのため、ボイスメールボックスが自動的に選択されなくなり、発信者に汎用ボイスメール グリーティングが提供されます。

AAR 宛先マスクを使用することで、外部電話番号マスクと無関係に、宛先の電話番号を決定できます。たとえば、会社の発信者 ID ポリシーに基づいて、電話機の外部電話番号マスクをオフィスの代表電話番号（415 555 1000 など）にする必要がある場合、AAR に電話機固有の PSTN 番号を提供するために、AAR 宛先マスクを +1 415 555 1234 に設定できます。

たとえば、San Francisco にある電話機 A（DN = 2345）から、New York にある電話機 B 上に設定されているオンネット DN（1234）にダイヤルするとします。ロケーションベースのコール アドミッション制御によってコールが拒否された場合、AAR は New York の電話機の AAR 宛先マスク（+1212555XXXX）を取得して使用し、PSTN 上でルーティング可能な番号（+12125551234）を導出します。

AAR 宛先マスクを設定して + 記号を含む完全修飾 E.164 番号を生成することが最善の方法となります。その理由は、この方法によって AAR 設定全体が大幅に簡素化されるためです。たとえば、パリにある電話機は AAR 宛先マスク +33 1 58 04 58 58 で設定されます。この番号は完全修飾 E.164 番号であるため、発信側電話機がフランスやカナダにあるか、世界のどこにあるかに関係なく、発信側電話機の PSTN へのゲートウェイによって要求されるルーティング可能な PSTN 番号を導出するために、Cisco Unified Communications システムに必要なすべての情報がこの番号に含まれています。次の項では、このアプローチについて詳しく説明します。

必要なアクセス コードの付加

AAR 宛先で + 記号を含む完全修飾 E.164 番号を生成する場合

これが最も単純なケースです。AAR 宛先には、ワイルドカードとして + が含まれています。+ は、各ゲートウェイで必要となる適切なアクセス コードに置き換えられます。適切なルート パターンにルーティングされるように宛先番号が準備されます。その後、適切な着信側トランスフォーメーション パターンによって宛先番号が PSTN への出口点で変換されます。

例 1：カナダの Ottawa にある電話機が Paris にある電話機に発信していますが、WAN の帯域幅が不足しているために AAR がトリガーされます。AAR 宛先は +33 1 58 04 58 58 です。発信側電話機の AAR コーリング サーチ スペースには、コールを標準ローカル ルート グループにルーティングするルート パターン \+! が含まれています。コールは、Ottawa にあるローカル ゲートウェイにルーティングされ、そこで、着信側トランスフォーメーション パターンによって + が適切な国際アクセス コード 011 に置き換えられます。その結果、011 33 1 58 04 58 58 にコールが発信されます。

例 2：フランスの Nice にある電話機が Paris にある電話機に発信していますが、WAN の帯域幅が不足しているために AAR がトリガーされます。AAR 宛先は +33 1 58 04 58 58 です。発信側電話機の AAR コーリング サーチ スペースには、コールを標準ローカル ルート グループにルーティングするルート パターン \+! が含まれています。コールは、Nice にあるローカル ゲートウェイにルーティングされ、そこで、着信側トランスフォーメーション パターンによって + 33 が適切な国内アクセス コード 0 に置き換えられます。その結果、01 58 04 58 58 にコールが発信されます。

AAR 宛先マスクで国コードを含む番号を生成する場合

宛先番号（国コードが含まれると前提）が元の支店のダイヤル プランによって正常にルーティングされるためには、プレフィックスが必要になる場合があります。また、発信地点が別のエリア コードまたは別の国に配置されている場合、ダイヤルされたストリングの一部として、国際ダイヤル アクセス コード（たとえば、00、011）などの他のプレフィックスが必要になる場合があります。

AAR を設定する場合は、DN を AAR グループ内に配置します。AAR グループのペアごとに、同じ AAR グループ内で発信または終端するコールのプレフィックス番号も含めて、その 2 グループ間のコールで DN に追加するプレフィックス番号を設定できます。

一般的な規則として、複数の DN が各国間で同じダイヤリング構造を共有している場合は、それらの DN を同じ AAR グループに配置します。たとえば、UK 国外にある UK ダイヤル番号のすべての電話機は、9 を PSTN アクセス コードとして使用し、その後に国際アクセス コードの 00 が続きます。フランスおよびベルギーにあるすべての電話機は、0 を PSTN アクセス コードとして使用し、その後に国際アクセス コードの 00 が続きます。NANP にあるすべての電話機は、9 を PSTN アクセス コードとして使用し、その後に国際アクセス コードの 011 が続きます。

これによって、AAR グループ設定は次のようになります。

[AARグループ(AAR Group)]	NANP	Cent_EU	UK
NANP	9	9011	9011
Cent_EU	000	000	000
UK	900	900	9

例 3: カナダの Ottawa にある電話機が Paris にある電話機に発信していますが、WAN の帯域幅が不足しているために AAR がトリガーされます。AAR 宛先は 33 1 58 04 58 58 です。発信側電話機の AAR グループは NANP であり、宛先番号の AAR グループは Cent-EU です。したがって、プレフィックス 9011 が付加されます。発信側電話機の AAR コーリング サーチ スペースには、コールを Ottawa のルート リストにルーティングして 9 を削除する、サイト固有のルート パターン 9011! が含まれています。コールは、Ottawa にあるローカル ゲートウェイにルーティングされます。その結果、011 33 1 58 04 58 58 にコールが発信されます。

例 4: ベルギーの Brussels にある電話機が Paris にある電話機に発信していますが、WAN の帯域幅が不足しているために AAR がトリガーされます。AAR 宛先は 33 1 58 04 58 58 です。発信側電話機および宛先番号の AAR グループは Cent-EU です。したがって、プレフィックス 000 が付加されます。発信側電話機の AAR コーリング サーチ スペースには、コールを Brussels のルート リストにルーティングして先行する 0 を削除する、サイト固有のルート パターン 000! が含まれています。コールは、Brussels にあるローカル ゲートウェイにルーティングされます。その結果、00 33 1 58 04 58 58 にコールが発信されます。

これらの例で、特定の AAR グループを設定する必要のない +E.164 ダイヤル プランのメリットがはっきりとわかります。

これらの例で、+E.164 ディレクトリ番号によるダイヤル プランのメリットがはっきりとわかります。特定の AAR グループまたは PSTN プレフィックスを設定する必要がありません。ダイヤルされたオンネット宛先がすでにダイヤル プランのコア ルーティングで使用される形式(+E.164)のため、ダイヤルされたディレクトリ番号を代替コールの PSTN アドレスとして直接使用することができます。

ボイスメールの考慮事項

AAR は、コールをボイスメールに転送できます。通常、オフネット アクセス コードなしでボイスメールのパイロット番号がダイヤルされます(ボイスメールのパイロット番号が 8 555 1000 などの完全修飾のオンネット番号である場合)。コールをボイスメールに送信するために AAR を設定すると、AAR グループ メカニズムによって、設定済みのアクセス コードも付加されます。この設定には、AAR グループを作成する必要があります。AAR グループは、必要な AAR 宛先がボイスメール(たとえば、vmail_aar_grp)となっているすべての DN によって使用されます。他の AAR グループの DN からコールを受信するときに、このボイスメールの AAR グループでプレフィックス番号を使用しないことを確認してください。

例：San Francisco サイトおよび New York サイトにある DN が、AAR グループ NANP で設定され、そのグループにある任意の 2 つの DN 間のコールに 9 が付加されるとします。San Francisco にある DN を設定して AAR コールをボイスメールに送信した場合（たとえば、8 555 1000）、985551000 にコールが発信されますが、そのコールは失敗します。その代わりに、San Francisco にある DN を AAR グループ vmail で設定します。次の表に示すように、AAR グループ NANP から AAR グループ vmail へのコールのプレフィックス番号は <none> です。これで、コールが正常に 85551000 に発信されます。

[AARグループ（AAR Group）]	NANP	Cent_EU	UK	vmail
NANP	9	9011	9011	<none>
Cent_EU	000	000	000	<none>
UK	900	900	9	<none>

（注） デバイス モビリティを使用しない場合、DN ドメインの AAR グループ設定は、デバイスがネットワークの別の場所に移動しても同じままです。デバイス モビリティを使用した場合、電話機の IP アドレスによって決定された、ネットワークで電話機が物理的に配置されている場所に基づき、ARR グループを動的に決定できます。詳細については、デバイス モビリティ（14-89 ページ）を参照してください。

適切なダイヤル プランおよびルートの選択

AAR コールは、発信元の電話と同じロケーションにあるゲートウェイを通じて出力する必要があります。これによって、完成されたダイヤル ストリングが、発信元サイトのダイヤル プランを通じて送信されます。このように設定するには、Unified CM Administration のデバイス設定ページで、適切な AAR コーリング サーチ スペースを選択します。AAR コーリング サーチ スペース内で、オフネット ダイヤル プラン項目（たとえば、ルート パターン）を、同じ場所にあるゲートウェイを指し、PSTN にコールを転送する前にアクセス コードを削除するように設定します。

たとえば、San Francisco サイトの電話を設定する場合は、91-NPA-NXX-XXXX としてダイヤルされた長距離電話を許可し、アクセス コード（9）を削除して San Francisco のゲートウェイに送信する AAR コーリング サーチ スペースを使用します。

ローカル ルート グループを使用し、さらに完全修飾 E.164 アドレス（+ 記号を含む）を AAR 宛先として使用すると、AAR コーリング サーチ スペース設定を大幅に簡素化することできます。これは、+E.164 AAR 宛先マスクまたは +E.164 ディレクトリ番号のいずれかを使用することで実現することができます。単一のパーティションで設定され、単一のルート パターン \+! が含まれ、さらに標準ローカル ルート グループを備えた単一のルート リストを指している単一のコーリング サーチ スペースを使用することで、クラスタ全体のすべてのサイトですべてのコールをルーティングできます。これは、適切なゲートウェイ固有の着信側トランスフォーメーション パターンを利用して、宛先番号のユニバーサル形式を、各サイトでコールが送信されるサービス プロバイダー ネットワークで必要となるローカル形式に適応させます。

（注） オンネット社内コールを強制的に PSTN コールとしてダイヤルする追加のルート パターンを設定した場合は、それらのパターンが AAR 機能のものと一致しないことを確認します。+E.164 ディレクトリ番号によるグローバル化されたダイヤル プランでは、これらの +E.164 ディレクトリ番号を保持するパーティションは、AAR コーリング サーチ スペースの一部にしてはなりません。

(注)　コール アドミッション制御による再ルーティングされたコールの拒否を避けるため、AAR 機能は、各エンドポイントとそれに関連する PSTN へのゲートウェイとの間で、IP パスとして LAN を使用する必要があります。したがって、AAR ダイヤル プランでは、PSTN へのアクセスに集中型ゲートウェイを使用することはできません。

(注)　デバイス モビリティを設定した場合、電話機の IP アドレスによって決定されている、ネットワークで電話機が物理的に配置されている場所に基づいて、ARR コーリング サーチ スペースを動的に決定できます。詳細については、デバイス モビリティ（14-89 ページ）を参照してください。

デバイス モビリティ

デバイス モビリティには、IP ネットワーク内にあるデバイスのモビリティが向上するように設計された機能が備わっています（San Francisco で使用するために初期設定された電話が New York に物理的に移動されるなど）。デバイスは同じ Unified CM クラスタに登録されたままですが、置かれている新しいサイトに基づいて、動作の一部が順応します。これらの変更は、電話機のある IP サブネットによってトリガーされます。

ローミングするとき、電話機はデバイスの現在のサブネットに関連付けられているデバイス プールに関連付けられているパラメータを継承します。ダイヤル プランから見て、次の 5 つの主要な設定パラメータの機能は、電話機の物理的な場所により変更できます。変更するこれらのパラメータについて、デバイスはホーム ロケーションの外部をローミングしているが、ホーム デバイスのモビリティ グループ内にいると見なされます。

- ローカル ルート グループ

  ローミング デバイス プールのローカル ルート グループが使用されます。たとえば、San Francisco から New York にデバイスがローミングする場合、パターンが標準ローカル ルート グループを呼び出すルート リストを指している場合は常に、PSTN へのコールのルーティングに New York デバイス プールのローカル ルート グループが使用されます。

- 発信側変換 CSS

  ローミング デバイス プールの発信側変換 CSS が使用されます。これにより、電話機は発信側電話番号表示モード（訪問した場所にある電話機の慣習的表示モード）を継承できます。

- デバイス コーリング サーチ スペース

  デバイス設定ページで設定されているデバイス コーリング サーチ スペースではなく、ローミング デバイス プールのデバイス モビリティ コーリング サーチ スペースが使用されます。たとえば、デバイスが San Francisco から New York にローミングしているとき、New York デバイス プールのデバイス モビリティ コーリング サーチ スペースが、ローミング電話機のデバイス コーリング サーチ スペースとして使用されます。サービス クラスに対して回線/デバイス アプローチを使用している場合、このアプローチは PSTN コールが取るパスを確立し、ローカルな New York ゲートウェイにルーティングします。

- AAR コーリング サーチ スペース

  デバイス設定ページで設定されている AAR コーリング サーチ スペースではなく、ローミング デバイス プールの AAR モビリティ コーリング サーチ スペースが使用されます。たとえば、デバイスが San Francisco から New York にローミングしているとき、New York デバイス プールの AAR コーリング サーチ スペースが、ローミング電話機の AAR コーリング サーチ スペースとして使用されます。このコーリング サーチ スペースは発信 AAR PSTN コールが取るパスを確立し、ローカルな New York ゲートウェイにルーティングします。

- DN の AAR グループ

  着信 AAR コールの場合、DN のホスト電話機がローミングしているかどうかにかかわらず、DN に割り当てられている AAR グループが保持されます。これにより、AAR 宛先番号に対して確立された到達可能性の特性が保持されます。

  発信 AAR コールの場合、発信 DN の AAR グループでは、DN の設定ページで選択された AAR グループではなく、ローミング デバイス プールの AAR グループが使用されます。この AAR グループは、ローミング デバイス上のすべての DN に適用されることに注意してください。たとえば、New York から Paris にローミングするデバイス上のすべての DN（どちらの場所も同じデバイス モビリティ グループであることを前提とする）は、Paris デバイス プールの発信コールに対して設定されている AAR グループを継承します。この AAR グループはローミング デバイス上のすべての DN に割り当てられます。また、ローミング電話機上の DN から行われた AAR コールに対して適切なプレフィックスを付加することを許可します。

ローミング中の Call Forward All

デバイスが同一のデバイス モビリティ グループ内をローミングしているとき、Unified CM ではローカル ゲートウェイへの到達にデバイス モビリティ CSS を使用します。ユーザが電話機で Call Forward All を設定している場合、CFA CSS が None に設定されていて、CFA CSS Activation Policy が With Activating Device/Line CSS に設定されていると、次のようになります。

- デバイスがホーム ロケーションにあるときに CFA CSS としてデバイス CSS と回線 CSS が使用されます。
- デバイスが同一のデバイス モビリティ グループ内をローミングしているとき、CFA CSS としてローミング デバイス プールからのデバイス モビリティ CSS と回線 CSS が使用されます。
- デバイスが別のデバイス モビリティ グループ内をローミングしているとき、CFA CSS としてデバイス CSS と回線 CSS が使用されます。

デバイス モビリティ（21-15 ページ）の項で、この機能について詳しく説明します。

エクステンション モビリティ

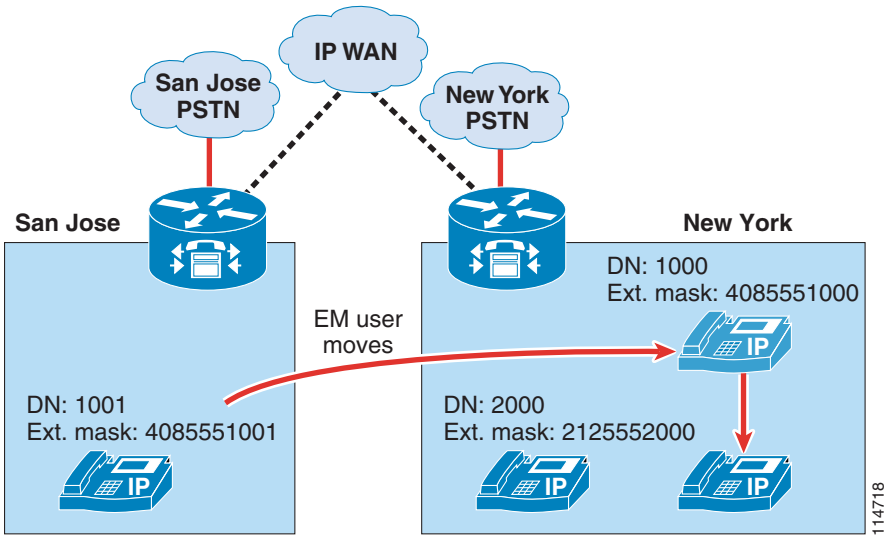
エクステンション モビリティ機能を使用すると、ユーザが IP Phone にログインしたとき、内線番号、スピード ダイヤル、メッセージ待機インジケータ（MWI）ステータス、コール特権を含めて、そのユーザのプロファイルが自動的にその電話機に適用されるようになります。このメカニズムは、それぞれのエクステンション モビリティ ユーザに関連付けられる、デバイス プロファイルを作成することで成り立っています。デバイス プロファイルは、実質的には仮想 IP Phone であり、1 つまたはそれ以上の回線を設定したり、コール特権やスピード ダイヤルなどを定義したりできます。

IP Phone がログアウト状態になっている（つまり、エクステンション モビリティ ユーザがログインしていない）とき、この IP Phone の特性は、デバイス設定ページと回線設定ページによって決まります。ユーザが IP Phone にログインすると、デバイス設定は変更されませんが、既存の回線設定は Unified CM データベースに保存され、ユーザのデバイス プロファイルの回線設定によって置き換えられます。

エクステンション モビリティの重要な利点の 1 つは、ユーザがどこにいるかにかかわらず、同じ Unified CM クラスタによって制御されている IP Phone にユーザがログインできれば、そのユーザに対して、そのユーザ固有の内線番号で到達できることです。集中型呼処理を使用しているマルチサイト配置に対してエクステンション モビリティを適用すると、地理的に互いに分離している複数のサイトに対して、この機能を展開できます。

ただし、エクステンション モビリティ機能を自動代替ルーティング（14-85 ページ）の項で説明している AAR 機能と組み合わせる場合は、一定の制限事項があります。図 14-36 に示した例について考えます。エクステンション モビリティと AAR を集中型呼処理の Unified CM クラスタに配置していて、San Jose と New York にそれぞれ 1 つのサイトがあります。

図 14-36　エクステンション モビリティと AAR



この例では、通常、San Jose を拠点としているエクステンション モビリティ ユーザが、DN 1000 と DID 番号 (408) 555-1000 を持っているとします。このユーザの外部電話番号マスク（または AAR マスク）は、4085551000 と設定されています。ユーザが New York のサイトに移動してログインします。また、San Jose と New York の間の IP WAN 帯域幅が完全に使用されていると仮定します。

San Jose にいる内線番号 1001 のユーザが 1000 にコールすると、AAR がトリガーされ、発信側の AAR コーリング サーチ スペースと発信側、着信側の AAR グループに基づいて、914085551000 への新しいコールが、San Jose の電話機によって試行されます。このコールは、San Jose のゲートウェイを使用して PSTN にアクセスしますが、DID（408）555-1000 が同じゲートウェイによって所有されているため、PSTN はコールをこのゲートウェイに戻します。San Jose のゲートウェイは、内線番号 1000 を持つ電話へのコールを確立しようとしますが、この電話は現在 New York にあります。New York にアクセスするための帯域幅を使用できないため、AAR 機能がもう一度呼び出され、次の 2 つのうち、いずれかのシナリオが発生します。

- ゲートウェイの AAR コーリング サーチ スペースに外部 PSTN ルート パターンが含まれている場合、ループが開始され、San Jose サイトにあるすべての PSTN トランクが使い果たされる。
- 逆に、ゲートウェイの AAR コーリング サーチ スペースに内部の番号のみが含まれている場合は、コールが失敗し、発信者にはファーストビジー トーンが聞こえる。この場合は、1 つの PSTN コールが発生して 1 つが受信されるため、コールのセットアップ中、San Jose のゲートウェイでは 2 つの PSTN トランクが使用されます。

ヒント　ここで説明したようなルーティング ループを防止するには、ゲートウェイ設定ページでコーリング サーチ スペースを設定するときに、必ず内部の宛先のみを含め、同じゲートウェイを含んでいるルート グループやルート リストを指すルート パターンを一切含めないようにします。

この例では、エクステンション モビリティが Cisco Unified Communications の動的な側面を利用しているため、サイト間のコール ルーティングで IP ネットワークを使用する必要があることを中心に説明しています。PSTN に定義されている E.164 番号は静的なものであり、PSTN ネットワークはエクステンション モビリティ ユーザの移動を認識しません。AAR 機能は、コール ルーティングを PSTN に依存しているため、ホーム サイト以外のサイトに移動したエクステンション モビリティ ユーザに対して、この機能を使用して到達することはできません。

(注)　ただし、エクステンション モビリティ ユーザが自分のホーム サイトと同じ AAR グループに属するリモート サイトに移動した場合には、使用可能な IP WAN 帯域幅が十分にないとき、そのユーザは AAR 機能を使用して他のサイトへのコールを発信できます。これは、コールの発信元の電話機の AAR コーリング サーチ スペースによってそれらのコールのパスが決定されるためです。この AAR コーリング サーチ スペースはユーザがエクステンション モビリティにログイン、またはログアウトしても変更されません。また、このスペースは訪問したリモート サイトのゲートウェイを使用するように設定する必要があります。

ヒント　登録解除されたエクステンション モビリティ プロファイル DN がボイスメールにコールを送信するように設定してください。詳細については、自動転送コーリング サーチ スペース (14-47 ページ)を参照してください。

Cisco Unified Mobility 固有の考慮事項

Cisco Unified Mobility（Cisco Unified Mobility（21-51 ページ）についての項を参照）では、コールのルーティングに直接影響を与える機能に依存しています。ダイヤル プランに関連する Cisco Unified Mobility パラメータの影響を理解するには、次の例について考えてみます。

(注)　この説明で必要なパラメータのみを、ここで示しています。

ユーザ Paul は、次のように設定された IP Phone を所有しています。

DN：8 555 1234

DID 番号：+1 408 555 1234

外部電話番号マスク：408 555 1234

回線コーリング サーチ スペース：P_L_CSS

デバイス コーリング サーチ スペース：P_D_CSS

Paul の DN は、次のように設定されたリモート宛先プロファイル（RDP）に関連付けられています。

コーリング サーチ スペース：P_RDP_CSS

再ルーティング コーリング サーチ スペース：P_RDP_Rerouting_CSS

発信側変換 CSS：P_CPT_CSS

Paul の RDP は、次のように設定されたリモート宛先に関連付けられています。

宛先番号：+1 514 000 9876（これは Paul の携帯電話番号。シングルモードまたはデュアルモードのいずれかの電話機）

Paul または Ringo の DID 番号にかけられた PSTN からのコールは、次のように設定されたゲートウェイによって処理されます。

コーリング サーチ スペース：GW_CSS

有効桁：7

プレフィックス DN：8

ユーザ Ringo は、次のように設定された IP Phone を所有しています。

DN：8 555 0001

DID 番号：408 555 0001

外部電話番号マスク：408 555 0000（これは企業の代表番号）

回線コーリング サーチ スペース：R_L_CSS

デバイス コーリング サーチ スペース：R_D_CSS

次の項では、コール ルーティングでの上記のモビリティ パラメータの影響について説明します。

リモート宛先プロファイル

リモート宛先プロファイル（RDP）はディレクトリ番号（たとえば、ユーザの IP Phone の DN）およびリモート宛先（たとえば、ユーザの携帯電話番号）と関連付けられています。RDP は IP Phone と、リモート宛先として設定された外部番号（たとえば、携帯電話）間のやり取りを制御します。

（注）　リモート宛先は、オンクラスタ DN を宛先番号として設定することはできません。

リモート宛先プロファイルの再ルーティング コーリング サーチ スペース

リモート宛先プロファイルに関連付けられている DN にコールが発信された場合、コールは DN と、リモート宛先として設定されている番号の両方にコールします。

発信者が宛先 IP Phone に到達できるかどうかは、発信者のコーリング サーチ スペース設定によって制御されます。ただし、コールがリモート宛先に分岐（転送）されるかどうか（たとえば、携帯電話）は、着信側モビリティ ユーザの再ルーティング コーリング サーチ スペースによって制御されます。

次に例を示します。
Ringo は、自分の IP Phone から 8 555 1234 とダイヤルすることによって Paul にコールします。Paul の IP Phone が鳴り、彼の携帯電話も鳴ります。

Ringo が Paul の DN に到達できるかどうかは、Ringo の IP Phone の回線およびデバイス コーリング サーチ スペースによって制御されています。ダイヤルした宛先（8 555 1234）は、連結されたコーリング サーチ スペース R_L_CSS および R_D_CSS にあるパーティションにあります。

このコールが Paul の携帯電話に分岐（転送）されるようにするには、設定されたリモート宛先（+1 514 000 9876）がコーリング サーチ スペース P_RDP_Rerouting_CSS にあるパターンと一致する必要があります。

（注）　Ringo の電話機に割り当てられたダイヤリング特権で外部コールが許可されていなくても、リモート宛先へのコールは、Paul のリモート宛先プロファイルに関連付けられた再ルーティング コーリング サーチ スペースによって処理されます。

リモート宛先プロファイルのコーリング サーチ スペース

新しいサービス パラメータ（[リモート宛先用の着信コーリング サーチ スペース（Inbound Calling Search Space for Remote Destination）]）が、クラスタのリモート宛先のいずれかから発信されたコールのルーティングに使用されるコーリング サーチ スペースを制御します。デフォルト設定は [トランクまたはゲートウェイの着信コーリング サーチ スペース（Trunk or Gateway Inbound Calling Search Space）] です。これはすべての着信コールをトランクまたはゲートウェイの設定済み CSS を使用してルーティングします。サービス パラメータが [リモート宛先プロファイル + 回線コーリング サーチ スペース（Remote Destination Profile + Line Calling Search Space）] に設定されると、コールをルーティングするために、一致したリモート宛先に関連付けられた DN の回線 CSS と、リモート宛先に関連付けられたリモート接続先プロファイルの CSS を連結したものが使用されます。

同じクラスタ内のリモート宛先として定義されているすべての番号は、クラスタに着信する任意の外部コールで一致するものを検索します。

次の例では、[リモート宛先用の着信コーリング サーチ スペース（Inbound Calling Search Space for Remote Destination）] サービス パラメータが [トランクまたはゲートウェイの着信コーリング サーチ スペース（Trunk or Gateway Inbound Calling Search Space）] に設定されていることを前提としています。

次に例を示します。
Paul は、Ringo の卓上電話にコールするために自分の携帯電話を使用しています。コールは PSTN からゲートウェイに着信します。発番号は 514 000 9876 で着番号は 408 555 0001 です。コールは Ringo の電話機にルーティングされます。Ringo の電話機に発番号として表示される番号は、Paul の卓上電話番号 8 555 1234 です。これにより、Paul の携帯電話番号は表示されず、Missed および Received コール リストから発信された Ringo のコールが Paul の IP Phone を鳴らします。このようにして企業モビリティ機能の完全なセットが使用できるようになります。

コールがゲートウェイに着信するとき、PSTN では発番号を 514 000 9876、着番号を 408 555 0001 と表示します。ゲートウェイの設定は着信者番号の末尾から 7 桁の有効桁を保持し、先頭に 8 のプレフィックスを付加して、宛先番号として 8 555 0001 を生成します。

システムは発番号が Paul のリモート宛先番号と一致するかどうかを検出します。一致を検出すると、次の処理が行われます。

1. 発番号を Paul の DN、8 555 1234 に変更します。
2. 着信ゲートウェイのコーリング サーチ スペースを使用して、コールを着信番号にルーティングします。具体的には、ルーティングは GW_CSS コーリング サーチ スペースを介して行われます。

ゲートウェイにより提示される宛先（着信）番号は、電話機の DN である必要があります。また、上記の手順 1 で示した発信側の置換では、Missed/Received コール リストからワンタッチ ダイヤルを使用した方法を示しています。

（注） リモート宛先番号をパーティションに分類する方法はありません。複数のユーザ グループ（異なる会社、請負業者など）で同じクラスタを使用している場合、この点に注意する必要があります。[リモート宛先用の着信コーリング サーチ スペース（Inbound Calling Search Space for Remote Destination）] サービス パラメータが [トランクまたはゲートウェイの着信コーリング サーチ スペース（Trunk or Gateway Inbound Calling Search Space）] に設定されている場合、発信者番号がリモート宛先に一致するかどうかにかかわらず、コールのルーティングは、着信トランクまたはゲートウェイの CSS に基づきます。ただし、発番号の置換は、発信側がリモート宛先に一致した場合でも行われます。これは、テナントのリモート宛先番号から別のテナントの DID 番号へのコールが、発信側のオンネット エクステンション DN と一致する、変換済み発番号で提示されることを意味します。

(注)　発番号が使用できない着信外部コールは、着信ゲートウェイの CSS に従ってルーティングされます。これは、SIP または H.323 トランクなどの IP トランクからの着信コールにも当てはまります。

リモート宛先プロファイルの発信側変換 CSS とトランスフォーメーション パターン

企業の IP Phone からモビリティ対応の DN に発信されたコールは、企業の宛先 IP Phone の DN と、1 つの（または複数の）外部宛先の両方に分岐（転送）されます。これによる 1 つの課題は、それぞれの宛先電話機のダイヤル プランに適合した発番号を送信することです。これは、Missed および Received コール リストからのコールのリダイヤルを可能にするために必要です。企業の電話機の場合、発番号はリダイヤル可能な企業の電話番号である必要があります。PSTN のリモート宛先の場合（自宅の電話機または携帯電話）、発番号は、発信側 IP Phone と関連付けられている企業の番号から、PSTN からリダイヤル可能な番号（一般に、発信側電話機の DID 番号）に変換する必要があります。

コールがモビリティ対応の企業 DN に発信された場合、発信者の発番号に一致するものを検索するために、関連付けられたリモート宛先プロファイルのコーリング サーチ スペースが使用されます。このスペースには、トランスフォーメーション パターンを含むパーティションが含まれています。

トランスフォーメーション パターンは、企業形式から PSTN 形式への発番号の適合を制御しています。トランスフォーメーション パターンは、着信番号ではなく、発番号をマッチングするという点で、Unified CM の他のすべてのパターンと異なります。マッチング処理は、正規表現（たとえば、8 555 XXXX）を使用して行われます。そして変換処理では、発信側 DN の外部電話番号マスクのほかに、トランスフォーメーション パターンを使用し、番号をプレフィックスとして付加できます。

一致すると、設定済みのすべての変換が実行されます。そして一致したリモート宛先プロファイルに関連付けられているすべてのリモート宛先への到達に、変換後の発番号が使用されます。

次に例を示します。
Ringo が Paul にコールすると、Paul の IP フォンには発番号が 8 555 0001 と表示され、Paul の携帯電話には 408 555 0001 と表示されるようにします。

この場合、次のパラメータを使用してトランスフォーメーション パターンを作成します。

Pattern：8 555 XXXX

Partition：SJ_Calling_Transform

Use calling party's external phone number mask：チェックしない

Calling Party Transformation mask：555 XXXX

Prefix Digits (outgoing calls)：408

パーティション SJ_Calling_Transform がコーリング サーチ スペース P_CPT_CSS に配置されていることを確認する必要もあります。

Ringo からのコールが Paul の電話機に固定されている場合、2 つの別々のコール レッグが試行されます。最初のコール レッグは Paul の IP Phone を鳴らし、発信者の DN を発番号（つまり 8 555 0001）と表示します。2 番めのコール レッグは Paul のリモート宛先プロファイルを介して試行されます。参照されるすべてのパーティションのトランスフォーメーション パターン内にある 8 555 0001 の一致を検索するために、RDP の発信側変換 CSS（P_CPT_CSS）が使用されます。パターン 8 555 XXXX はパターン SJ_Calling_Transform でマッチングされます。トランスフォーメーション マスクが発番号に適用され、555 0001 が生成されます。プレフィックス番号が追加され、リモート宛先にコールが発信された場合に変換された発番号 408 555 0001 が使用されます。

この例では、Ringo の DID 番号と異なる番号に設定されているため、外部電話番号マスクを使用していないことに注意してください。これにより、オフネットの宛先に提示される発番号が発信者と着信側で異なっている必要がある場合に、柔軟性が提供されます。Ringo から Paul へのコールは同僚間のものであるため、Ringo の DID 番号が公開されるのは許容されると見なされます。Ringo の次のコールは顧客に対するものである可能性があります。この場合、企業の代表番号 408 555 0000 が、宛先に提示されるのに最も望ましい発番号です。

(注)　発信側トランスフォーメーション コーリング サーチ スペースには <none> パーティションが暗黙的に含まれていません。そのため、<none> パーティションに残っているトランスフォーメーション パターンはどの発信側トランスフォーメーション コーリング サーチ スペースにも適用されません。これは Unified CM 内の他のすべてのパターンと異なります。Unified CM では、<none> パーティション内に残るすべてのパターンは暗黙的にすべてのコーリング サーチ スペースに含まれます。

アプリケーション ダイヤル ルール（Application Dial Rules）

リモート宛先と定義される番号は、着信コールを企業のモビリティ コールとして識別し、固定するためにも使用されます。PSTN がコールを識別する形式は、企業のダイヤル プランがコールを外部番号にダイヤルする場合の形式と異なることがよくあります。適用ダイヤル規則は、リモート宛先で、コールをリモート宛先に分岐（転送）する際に必要な形式に設定するために使用できます。これらの規則では、リモート宛先として設定された番号から、数字を削除したり、数字をプレフィックスとして付加したりできます。

次に例を示します。
番号 514 000 9876 は Paul のリモート宛先番号として設定されています。この番号は、企業に着信するコールを識別するために PSTN が使用する形式に対応します。ただしこれは、発信コールで企業のダイヤル プランが使用する形式（91 をプレフィックスとして付加する必要があります）とは異なります。この場合、リモート宛先の形式を企業ダイヤル プランの形式に適合させるために、適用ダイヤル規則を作成する必要があります。

適用ダイヤル規則:

名前:514000_ten

説明:プレフィックス 91 を 514000 で始まる 10 桁の番号に付加するために使用

番号の先頭:514000

桁数:10

削除する桁数:0

パターンで付加するプレフィックス:91

この例では、Paul の携帯電話から企業へかけられたコールは、514 000 9876 からのものと識別されます。これは、Paul の番号がリモート宛先と設定されている形式に一致します。このため、マッチングが行われ、Paul の卓上電話コールの固定をトリガーします。またオンネットの宛先に表示される発番号の最適化も行われます（たとえば、コールが Ringo の DID 番号に対して行われた場合、Ringo にはその着信が 8 555 1234 から来たものと表示されます）。

コールが Paul の企業 DN 番号に対して行われた場合、Paul のリモート宛先番号に分岐（転送）されたコール レッグは、上記の適用ダイヤル規則によって処理されます。ストリング 514 000 は Paul のリモート宛先番号の先頭と一致します。また、この番号は 10 桁であるため、数字は削除されず、91 がプレフィックスとして付加されます。これにより、Paul のリモート宛先プロファイル コーリング サーチ スペース（この場合は P_RDP_CSS）を介してルーティングされる番号として、91 514 000 9876 が生成されます。

(注)　このアプローチでは、IP Phone から行われたコールのルーティングのためにすでに定義済みのコーリング サーチ スペースを再利用する機能を提供します。発信コールに対してプレフィックスを付加する必要のない新しいコーリング サーチ スペース（つまり、直接 514 000 9876 にコールをルーティングできる）は好ましくありません。外部パターンとオンネット パターンが重複する状況が発生する可能性があるためです。

時間帯ルーティング

この機能を使用するには、次の要素を設定します。

- 期間
- タイム スケジュール

期間を利用すると、営業開始時刻と終了時刻を設定できます。この開始時刻と終了時刻は、コールをルーティングできる期間を示しています。これらの時刻に加えて、毎週または毎年発生するイベントを設定することもできます。さらに、Start Time オプションと End Time オプションにある No business hours を選択して、休業時間を設定することもできます。このオプションを選択した場合は、すべての着信コールがブロックされます。

タイム スケジュールは、パーティションに割り当てられている特定の期間をグループにまとめたものです。このタイム スケジュールによって、指定した期間中にパーティションがアクティブまたは非アクティブのどちらになっているかが判断されます。一致したパターンやダイヤリング パターンには、そのダイヤリング パターンの配置されているパーティションがアクティブになっている場合のみ到達できます。

図 14-37 では、同じコール パターン（8000）を持つ 2 つのハント パイロットが、2 つのパーティション（RTP_Partition、SJC_Partition）内に設定されています。これらのパーティションには、一連の定義済み期間を保持したタイム スケジュールがそれぞれ割り当てられています。たとえば、RTP の電話には、ハント パイロット 1 を使用することで、月曜日から金曜日の午前 8 時～午後 12 時（東部標準時。GMT - 5.00）まで、および日曜日の午前 8 時から午後 5 時まで到達できます。同様に、SJC の電話には、ハント パイロット 2 を使用することで、月曜日から金曜日の午前 8 時～午後 5 時（太平洋標準時。GMT - 8.00）まで、および土曜日の午前 8 時～午後 5 時まで到達できます。この例では、どちらのハント パイロットも 7 月 4 日は非アクティブです。

図 14-37　　時間帯ルーティング

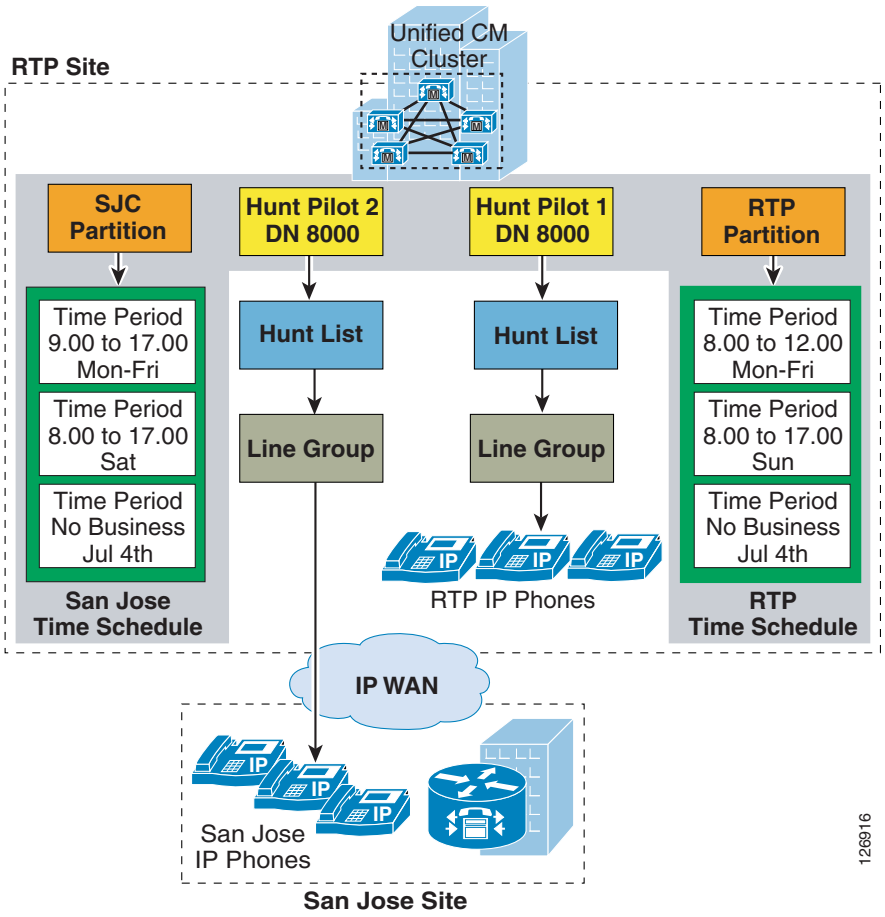


図 14-37 の例では、水曜日の午後 3 時にハント パイロット（8000）に着信したコールは、SJC の電話に転送されます。一方、このハント パイロットに 7 月 4 日にコールした人は、別のパターンが 8000 に一致しない限り、ファースト ビジー トーンを受信します。

論理パーティション

論理パーティションには、次の要素が含まれます。

- デバイス タイプ。電話機は *interior* として分類され、ゲートウェイとトランクは *border* として定義されます。表 14-6 に、各デバイスのエンドポイント タイプを示します。
- ジオロケーション。エンドポイントにはポリシーの決定に使用される住所が割り当てられます。
- ジオロケーション フィルタ。ポリシーの決定は、ジオロケーション オブジェクトのサブセットに対して行うことができます。
- ポリシー。エンドポイント間の通信は、それらの相対的な（フィルタ処理された）ジオロケーションとデバイス タイプに基づいて許可または拒否されます。

(注)　コールのすべての参加者が *interior* として分類されないと、ポリシーは適用されません。つまり、同じクラスタにある電話機間のコールに論理パーティション ポリシーが適用されることはありません。

(注)　ジオロケーションは、Unified CM で設定するコール アドミッション制御用のロケーションや、デバイス モビリティに使用される物理ロケーションと混同されることはありません。

表 14-6　デバイス タイプ

論理パーティションのデバイス タイプ	Cisco Unified Communications Manager デバイス
Border	• ゲートウェイ（H.323 ゲートウェイなど） • クラスタ間トランク（ICT）、ゲートキーパー制御および非ゲートキーパー制御 • H.225 トランク • SIP トランク • MGCP ポート（E1、T1、PRI、BRI、FXO）
Interior	• 電話機（SCCP、SIP、またはサードパーティ） • CTI ルート ポイント • Cisco VG シリーズ ゲートウェイに接続されたアナログ電話 • MGCP ポート（FXS） • Cisco Unity ボイスメール（SCCP）

論理パーティションのデバイス タイプ

Unified CM は、エンドポイントを *interior* または *border* に分類します。この分類は固定されており、システム管理者が変更することはできません。

ジオロケーションの作成

(RFC) 4119 規格には、ジオロケーションの基本情報が記載されています。ジオロケーションには、次のオブジェクトによって指定される住所形式が使用されます。

- [名前（Name）]
- 説明
- 2 文字の短縮形を使用した国名
- 州、地区、または地域（A1）
- 国または行政区（A2）
- 市町村（A3）
- 自治区（A4）
- 地区（A5）

- 街（A6）
- N や W など、街の先頭の方角指示（PRD）
- SW など、街の末尾のサフィックス（POD）
- 通りや区画など、住所のサフィックス（STS）
- 番地（HNO）
- A、1/2 など、番地のサフィックス（HNS）
- ランドマーク（LMK）
- 部屋番号など、ロケーションの補足情報（LOC）
- フロア（FLR）
- 会社または居住者の名前（NAM）
- 郵便番号（PC）

（注）　Unified CM では、ジオロケーションを手動で定義する必要があります。

ジオロケーションの割り当て

デバイスには、優先順位に従ってデバイス ページ、デバイス プール、またはエンタープライズ パラメータで設定されたデフォルトのジオロケーションのいずれかからジオロケーションが割り当てられています。

ジオロケーション フィルタの作成

ジオロケーション フィルタでは、異なるエンドポイントのジオロケーションを比較するときに使用するジオロケーション オブジェクトを定義します。たとえば、電話機のグループには、それらの電話機が置かれている部屋やフロアを除いて、同じジオロケーションが割り当てられる可能性があります。ポリシーによっては、同じ建物内のエンドポイントを同じ非公開ユーザ グループに所属するものと見なし、通信を許可する場合もあります。各電話の実際のジオロケーションは異なりますが、フィルタ処理されたジオロケーションは同じになります。この方法は、ジオロケーションの最上位のフィールドだけにポリシーを適用する必要がある場合に役立ちます。たとえば、異なる都市にある電話機とゲートウェイ間の通信を拒否し、同じ都市内の電話機とゲートウェイ間の通信は許可するポリシーは、都市よりも詳細なオブジェクトを無視してフィルタ処理された相対的なジオロケーションを基にできます。

ジオロケーション フィルタの割り当て

電話機は、デバイス プールのフィルタの割り当てを継承します。ゲートウェイとトランクには、優先順位に従ってデバイスまたはデバイス プール レベルでジオロケーション フィルタを設定できます。

論理パーティション ポリシーの設定

論理パーティション ポリシーは、ジオロケーション ID 間に設定されます。ジオロケーション ID は、フィルタ処理されたジオロケーションとデバイス タイプの組み合わせになります。フィルタ処理されたジオロケーションを取得するには、デバイスのジオロケーションを呼び出し、デバイスに関連付けられたジオロケーション フィルタを適用します。

ポリシーは、ジオロケーション オブジェクトのセットとデバイス タイプの組み合わせ（ソース ジオロケーション ID）として、そのようなもう 1 つの組み合わせ（ターゲット ジオロケーション ID）と関係付けて作成されます。関係が一致すると、設定されている「許可」または「拒否」の処理がコール レッグに適用されます。

(注)　ポリシーに設定されているジオロケーション オブジェクトのセットはそれぞれ、1 つのデバイス タイプに関連して考慮されます。たとえば、国 = インド、州 = カルナタカ、市 = バンガロールのようなジオロケーション オブジェクトのセットは、バンガロールの電話機に対する処理に関してはデバイス タイプ Interior に関連付ける必要があり、バンガロールのゲートウェイに対する処理に関してはデバイス タイプ Border に別に関連付ける必要があります。

論理パーティション ポリシーの適用

ユーザの操作によって新しいコール レッグが作成された場合（たとえば、ユーザが第 3 の発信者を既存のコールに参加させる場合）、Unified CM は各参加者ペアのジオロケーション ID と事前に設定されたポリシーのジオロケーション ID を照合します。

(注)　2 つのデバイスのジオロケーション ID が論理パーティションによって評価されている場合、両方のデバイスのデバイス タイプが Interior であれば、ポリシーは適用されません。つまり、同じクラスタ内の IP 電話間のコール、会議、転送などが論理パーティション ポリシーによって拒否されることはありません。

たとえば、インドのバンガロールにある電話機 A と B、およびカナダのオタワにあるゲートウェイ C について考えます。電話機 A が電話機 B にコールします。どちらのデバイスもタイプ [内部（Interior）] のため、ポリシーは呼び出されません。コールが確立された後に、電話機 A のユーザが電話会議を呼び出すと、ゲートウェイ C に移されます。アクションが許可される前に、Unified CM が A と C、および B と C のジオロケーション ID をチェックし、事前設定済みポリシーとの一致を確認します。ポリシーの一致によって処理が拒否された場合、新しいコール レッグは確立できません。

(注)　Unified CM のデフォルト ポリシーは拒否です。つまり、コール レッグを許可するように明示的にポリシーを設定していなければ、コール レッグは拒否されます。

この例では、バンガロールの Interior デバイスがオタワの Border デバイスに接続できるように明示的にポリシーを設定していない限り、コール レッグは拒否されます。

緊急サービス

改訂日：2016 年 6 月 14 日

通信システムを適切に導入するには、緊急サービスが非常に重要です。この章では、緊急コールの計画に不可欠な次の主要な設計上の考慮事項について説明します。

この章では、カナダおよび米国で配置されている 911 緊急ネットワークに固有の情報について説明します。ここで説明する概念の多くは、他の地域にも適応できます。緊急コール機能の適切な実装については、ローカル テレフォニー ネットワーク プロバイダーにご相談ください。

米国の一部の州では、Multi-Line Telephone System（MLTS）のユーザに必要な 911 機能を対象にした法律がすでに制定されています。また、National Emergency Number Association（NENA）が『*NENA Technical Requirements Document on Model Legislation E9-1-1 for Multi-Line Telephone Systems*』を制作しています。これは、次のサイトからオンラインで入手できます。

https://www.nena.org/

この章は、北米在住の PSTN ユーザに使用可能な汎用 911 機能について十分に理解している読者を対象にしています。

（注） この章で説明する内容は、Cisco Emergency Responder が Cisco Unified Communications Manager（Unified CM）と共に使用される場合のみ適用されます。Cisco TelePresence Video Communication Server（VCS）は現在、緊急サービスをサポートしていません。

911 緊急サービスのアーキテクチャ

この項では、Multi-Line Telephone Systems（MLTS）における緊急コールの機能要件の一部について説明します。ここでの緊急コールとは、北米の公衆電話交換網（PSTN）によって提供される 911 コールのことです。

緊急サービスのアーキテクチャは、通常次の要素から構成されます。

- 緊急事態にある発信者は、固定回線、携帯電話機、公衆電話、または音声コールを行うことができる任意のデバイスから緊急サービスをダイヤルできる必要があります。
- 緊急サービス コール ハンドラが緊急要求に応答し、警察、消防、医療などの必要なサービスを派遣できる必要があります。
- 援助を提供するには、コール ハンドラは、緊急事態にある発信者のロケーションをできるだけ正確に特定できる必要があります。
- 発信者のロケーションに最も近い緊急サービス コール ハンドラにコールをルーティングするには、緊急サービス ネットワークが必要です。

次の項では、911 緊急サービス アーキテクチャの重要なアーキテクチャ コンポーネントのいくつかについて説明します。

Public Safety Answering Point（PSAP）

Public Safety Answering Point（PSAP）は、911 コールに応答して、適切な緊急対応（警察、消防署、救急チームの派遣など）を手配する機関です。911 コールを発信する電話機の物理的なロケーションは、そのコールに応答する適切な PSAP を決定する基本要素です。一般に、各建物を、1 つのローカル PSAP が担当します。

所定のロケーションを担当する PSAP を確認するには、地域の防火管理者や警察署などの地域の公衆安全情報サービス機関に問い合わせてください。また、通常、地域通信事業者のディレクトリにも、所定地域内の 911 コールを処理する機関がリストされています。

標準的な状況

- 1 つの番地に対して、1 つの PSAP だけが指定されます。
- 1 つの番地の 911 コールはすべて、同じ PSAP にルーティングされます。

例外的な状況

- キャンパスの物理的な規模により、一部の建物が別の PSAP の管轄になります。
- 一部の 911 コールをオンネット ロケーション（キャンパスのセキュリティ、建物のセキュリティ）にルーティングする必要があります。

選択ルータ

選択ルータは、発信者の地理的な場所と自動番号識別（ANI）に基づいたコール送信のために適切な PSAP を決定する緊急サービス ネットワークのノードです。通常、地域通信事業者（LEC）が選択ルータを運用します。したがって、発信者がそのロケーションに基づいて適切な選択ルータにルーティングされるようエンタープライズ IP 通信ネットワークが設計されている必要があります。

自動ロケーション識別データベース

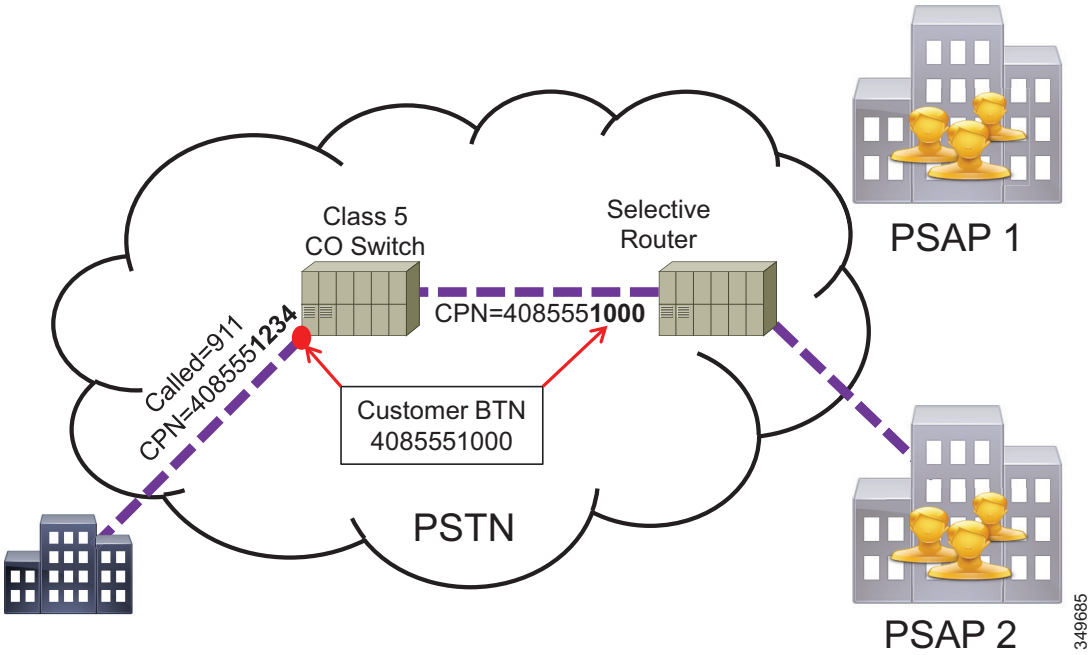
発信者のロケーション情報は、911 サービス インフラストラクチャの重要な部分です。自動ロケーション識別（ALI）データベースには LEC により提供された特定の地理的なロケーションに関する情報が保持されます。各 911 コールに対して、PSAP は ALI データベースを検索し、発信者番号の ANI に基づいて発信者のロケーションを取得します。ALI データベースでは、アドレスが Master Street Address Guide（MSAG）形式で保存されます。ALI データベースは、ローカル緊急サービス管理側の代わりに、契約を締結したサード パーティ（通常は現在の地域通信事業者（LEC））によって保守されます。

サービス プロバイダー ALI

サービス プロバイダー ALI（SP-ALI）は、サービス プロバイダーが接続上のすべての緊急コールに対する ALI 情報を定義し、維持するための構成です。SP-ALI サービスは、LEC での物理的な相互接続を使用して、コールの発信元ロケーションを決定します。居住者顧客については、ALI 情報はサブスクライバの住所とその居住者のディレクトリ番号に関連付けられます。ALI 情報は LEC の物理的な相互接続に基づいてサービス プロバイダーによって決定されるため、サブスクライバは ALI 情報の変更または設定を行うことはできません。

回線またはトランクの相互接続の物理的な場所に基づく ALI 情報の設定は、PRI トランク接続にも適用されます。デフォルトでは、PSTN アクセス用に PRI トランクを使用する MLTS オペレータは、SP-ALI サービスを所有します。LEC は、緊急コール用の発信者番号（CPN）および ALI アドレスを定義します。通常、緊急コールで使用される発信者番号は顧客の請求先番号（BTN）または MLTS オペレータの代表番号です。緊急コール番号に関連付けられる物理アドレスは、顧客の施設での PRI の境界のアドレスです。PRI トランクが SP-ALI サービス用に設定されている場合、911 へのすべてのコールには、ALI レコードと顧客の一致処理を行うために LEC により置き換えられた発信者番号が付随します（図 15-1 を参照）。

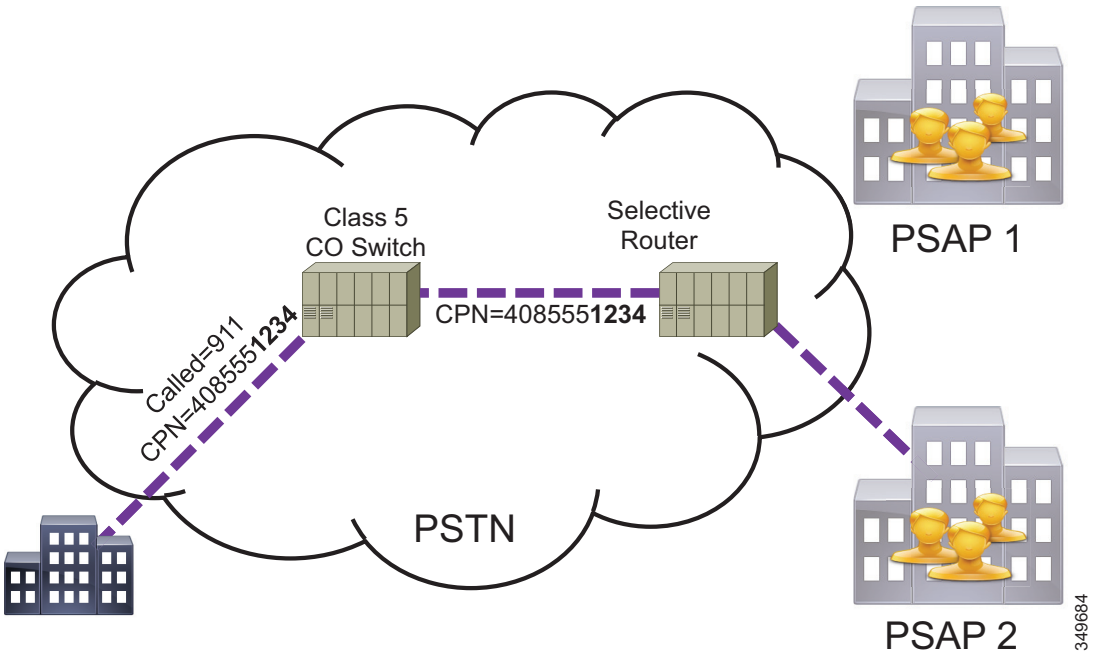
図 15-1　　サービス プロバイダー ALI



Private Switch ALI

Private Switch ALI（PS/ALI）は、MLTS オペレータが各エンドポイントに詳細なアドレスとロケーション情報を提供できるようにする 911 緊急応答システムの拡張機能です。このサービスにより、顧客が生成したアドレス テーブルを ALI データベースにロードできるようになります。この結果、MLTS システムの各ステーションの電話番号から 911 にコールが行われた場合に、MLTS システムの各ステーションを一意に識別できるようになります。通信システムにより生成されたステーション固有またはロケーション固有の自動番号識別（ANI）は、発信者の正確なロケーションを特定するために直接 E911 システムに渡すことができます（図 15-2 を参照）。次に、PSAP オペレータは、正確な住所、建物、階、部屋、またはパーティションにさえも緊急対応人員を派遣できます。この結果、作業が簡略化され、精度が高まります。

図 15-2　Private Switch ALI



911 ネットワーク サービス プロバイダー

担当 PSAP を確認したあと、各 PSAP が接続されている 911 ネットワーク サービス プロバイダーも特定する必要があります。通常、PSAP は PSTN から 911 コールを受信すると想定されますが、実際はそうではありません。実際は、911 コールは、地域の重要な専用ネットワークを経由して伝送され、各 PSAP は 1 つ以上のこうした地域ネットワークに接続されます。大半の場合、既存の地域通信事業者（LEC）が PSAP の 911 ネットワーク サービス プロバイダーです。例外として、軍事施設、大学構内、国立や州立の公園、または公衆安全の責任が地方自治体の管轄外であるロケーション、もしくは公共の地域通信事業者以外のエンティティによってプライベート ネットワークが運営されているロケーションがあります。

所定の PSAP の 911 ネットワーク サービス プロバイダーについて疑問がある場合は、その PSAP に直接連絡して、情報を確認してください。

標準的な状況

- 所定の番地に対する 911 ネットワーク サービス プロバイダーは、既存の地域通信事業者（LEC）です。電話会社 X がサービスを提供するロケーションの場合、対応する PSAP も、電話会社 X からサービスが提供されます。
- すべての 911 コールは、オフネット ロケーションに直接ルーティングされるか、オンネット ロケーションに直接ルーティングされます。

例外的な状況

- MLTS インターフェイスから PSTN へ接続するために使用する地域通信事業（LEC）と、PSAP に対して 911 ネットワーク サービス プロバイダーの役目をする LEC が*異なる*場合があります（たとえば、通信システムは電話会社 X からサービスを受け、PSAP は電話会社 Y に接続されている場合です）。この状況では、LEC 間の特別な調整、または電話システムと PSAP の 911 ネットワーク サービス プロバイダー間に特別な専用トランクが必要な場合があります。
- 一部の LEC は、ネットワーク上で 911 コールを受け入れることができません。この場合、LEC を変更するか、911 コールを適切な PSAP にルーティングできる LEC に接続されたトランク（911 コール ルーティング専用）を確立するかの 2 つのオプションしかありません。
- 一部（または全部）の 911 コールをオンネット ロケーション（キャンパスのセキュリティや建物のセキュリティなど）にルーティングする必要があります。各電話機の 911 コールの宛先が正しく計画され、文書化されていれば、この状況には、設計および実装の段階で簡単に対応できます。

適切な 911 ネットワークへのインターフェイス ポイント

大規模な通信システムでは、911 接続に多数のインターフェイス ポイントが必要になる場合があります。一般に、複数の E911 選択ルータが LEC の管轄地区内で使用されます。これらのルータは、通常、相互接続*されません*。

たとえば、大規模なキャンパスを備えた企業に、次のような状況があるとします。

- 建物 A はサンフランシスコにある。
- 建物 B はサンノゼにある。
- サンフランシスコ警察とサンノゼ警察が、該当する PSAP である。
- サンフランシスコ警察とサンノゼ警察は、同じ 911 ネットワーク サービス プロバイダーのサービスを利用している。
- しかし、サンフランシスコ警察とサンノゼ警察は、同じ 911 ネットワーク サービス プロバイダーが運営する異なる E911 選択ルータのサービスを受けている。

このタイプの状況では、2 つの別々のインターフェイス ポイント（E911 選択ルータごとに 1 つずつ）が必要です。E911 選択ルータの管轄地区に関する情報は、一般に、担当 LEC が保持しています。また、その LEC の地域アカウント担当者が、企業顧客に関連情報を提供できる必要があります。多くの LEC は、911 問題を担当する専門家のサービスも用意しています。この専門家は、911 アクセス サービスの適切なマッピングについてアカウント担当者と協議できます。

標準的な状況

- 単一サイト配置またはキャンパス配置では、通常、911 コール用に 1 つだけの PSAP があります。
- 1 つの PSAP だけへのアクセスが必要であれば、必要なインターフェイス ポイントは 1 つだけです。複数の PSAP へのアクセスが必要な場合でも、同じ集中インターフェイスを介して、同じ E911 選択ルータから到達可能です。集中型呼処理で企業の支社サイトが WAN を介して接続されており、Survivable Remote Site Telephony（SRST）操作がアクティブであるときに WAN 障害が発生した場合の 911 孤立を防止するため、911 へのローカル（つまり、各支社内の）アクセスを各ロケーションに指定することが推奨されます。

例外的な状況

- キャンパスの物理的な規模により、一部の建物が別の PSAP 管轄になります。また、
- 一部の 911 コールは、異なるインターフェイス ポイントを通じて、異なる E911 選択ルータにルーティングされる必要があります。

（注）　PSAP と E911 選択ルータの地理的な管轄地区の設定に必要な情報は、オンライン、または各種の競争的地域通信事業者（CLEC）の Web サイトから部分的に情報を入手できます（たとえば、https://clec.att.com/clec/hb/shell.cfm?section=782 [英語] では、カリフォルニア州およびネバダ州の AT&T がカバーする管轄地区についての貴重なデータが提供されています）。ただし、911 コール ルーティングを設計および実装する前に、該当するインターフェイス ポイントの適切な情報を LEC から入手しておくことを強く推奨します。

インターフェイス タイプ

ネットワークへの 911 コールの発信に使用されるインターフェイスは、音声通信の提供に加えて、発信側についての識別データも提供する必要があります。

自動番号識別（ANI）は、ネットワークが適切な宛先へ 911 コールをルーティングするために使用する、発信側の北米番号計画の番号を参照します。この番号は、PSAP がコールの自動ロケーション識別（ALI）を検索するためにも使用されます。

911 コールは、ソースルートされます。つまり、911 コールは発信者番号に応じてルーティングされます。別々のロケーションからすべて同じ番号（911）をダイヤルする場合でも、ANI（発信者番号）によって表される起点ロケーションに基づいて、別々の PSAP に到達します。

911 コール機能は、次のいずれかのインターフェイス タイプを使用して実装できます。

- 動的 ANI 割り当て
- 静的 ANI 割り当て

動的 ANI 割り当ては、（複数の ANI をサポートするので）スケーラビリティに優れていますが、小規模のシステム配置には適していません。これに対し、静的 ANI 割り当ては、最小のシステムから最大のシステムまで、より広範囲にわたる環境で使用できます。

動的 ANI（トランク接続）

動的 ANI では、通信システムの 1 つのインターフェイスを、911 ネットワークにアクセスする多数のエンドポイントが共用します。また、ネットワークに送信される ANI がコールごとに異なっていることが必要な場合があります。

動的 ANI インターフェイスには、次の 3 つの主なタイプがあります。

- Integrated Services Digital Network Primary Rate Interface（ISDN-PRI、または単に PRI）
- Session Initiation Protocol（SIP）トランク
- Centralized Automatic Message Accounting（CAMA）

PRI

このタイプのインターフェイスは、通常、通信システムを PSTN Class 5 スイッチに接続します。発信者番号（CPN）は、発信側の E.164 番号を識別するためにコール セットアップ時に使用されます。

911 にコールする場合、LEC によって CPN を扱う方法が異なります。Class 5 スイッチ機能の制限、または LEC や地方自治体の方針によっては、CPN が 911 コール ルーティング用の ANI として使用されない場合があります。この場合、代わりに Listed Directory Number（LDN）または請求先番号（BTN）を ANI の目的で使用するように、ネットワークをプログラムできます。

CPN が ANI に使用されない場合、PRI インターフェイスから発信する 911 コールはすべて、911 ネットワークには同じように見えます。これらの 911 コールはすべて、同じ ANI を持ち、同じ宛先（適切な宛先でない場合があります）にルーティングされるためです。LEC による CPN の置換は通常、サービス プロバイダー ALI（SP-ALI）と呼ばれます。これは、ALI ルックアップの際にサービス プロバイダーが CPN を指定するためです。

一部の LEC は、911 コールの CPN が PRI インターフェイスを通過するようにする機能を備えています。この機能を使用すると、コールのセットアップ時に Class 5 スイッチに提示された CPN は、コールをルーティングするために ANI として使用されます。この機能の名称は、LEC によって異なります（たとえば、SBC はカリフォルニア州でこの機能を Inform 911 と呼びます）。

（注）　SP-ALI サービスが使用されている場合、CPN は、ルーティング可能な北米番号計画の番号である必要があります。つまり、CPN は、関連付けられた E911 選択ルータのルーティング データベースに入力されている必要があります。

（注）　ダイヤルイン方式（DID）の電話機の場合、DID 番号は、911 の目的で ANI として使用できますが、これは、911 サービス プロバイダーのネットワーク内で、緊急サービス番号に適切に関連付けられている場合だけです。DID 以外の電話機の場合は、別の番号を使用してください（詳細については、緊急ロケーション識別番号のマッピング（15-14 ページ）を参照してください）。

多くの Class 5 スイッチは、1 つのエリア コードしかサポートしないトランクを通じて、E911 選択ルータに接続されています。このような場合、PRI が 911 コールの伝送に使用されるとき、Class 5 スイッチと同じ番号計画エリア（NPA）のある CPN（または ANI）を持つ 911 コールだけが、適切にルーティングされます。

例

MLTS が、エリア コード 514（NPA = 514）の Class 5 スイッチに接続されるとします。MLTS が PRI トランク上で 911 コールを送信し、CPN が **450**.555.1212 である場合、Class 5 スイッチは、（正しい **450**.555.1212 ではなく）ANI **514**.555.1212 として E911 選択ルータにそのコールを送信するため、不適切なルーティングと ALI ルックアップが発生します。

PRI を 911 インターフェイスとして適切に使用するには、システムの設計担当者が、CPN が ANI に使用されることを確認し、リンク上で受け入れ可能な番号の範囲（NPA NXX TNTN の形式）を適切に指定する必要があります。たとえば、PRI リンクが、範囲 514 XXX XXXX 内の ANI 番号を受け入れるように指定されている場合、NPA = 514 の発信者番号を持つコールだけが適切にルーティングされます。

SIP トランク

SIP トランキングは、セッション ボーダー コントローラ（SBC）を通常経由して、コミュニケーション システムをサービス プロバイダーに接続する IP のみのインターフェイスです。SIP トランクを使用すると、同じ動的発信者番号を PRI トランクとしてキャリアに送信できますが、PRI トランクとは異なり、SIP トランクには同時に確立可能なコール数の物理的な制限はありません。

緊急サービスが SIP トランク経由でコールされる場合、正しい選択ルータにコールが送信されることをプロバイダーと一緒に確認する必要があります。ローカル LEC で終端する PRI 回線と異なり、SIP トランクはローカル LEC と物理接続されていないことがあり、その場合、911 コールは発信者の自治体の選択ルータに自動的にルーティングされません。また、各 SIP トランク プロバイダーは、それぞれ異なる E911 ルーティング能力を持つことがあります。たとえば、あるサービス プロバイダーは、発信者番号に基づいて（ローカル エリア以外の）米国全土の選択ルータにコールを送信でき、別のサービス プロバイダーは、顧客が指定した選択ルータに対してのみ E911 コールの送信を許可する場合もあります。Cisco Unified CM の管理者は、特に SIP トランクが集中型コール ルーティングを提供する場合、911 コール送信機能をキャリアと一緒に確認する必要があります。

SIP サービス プロバイダーは、それらが SIP トランク経由でサービスを提供するすべての DID 番号用の適切な料金算出地点または PSAP に 911 コールをルーティングする必要があります。たとえば、テキサス州ダラスのデータ センターで物理的に終端する SIP トランクがあると仮定します。このデータ センターは、415-555-1xxx の範囲を持つサンフランシスコ オフィスと 212-448-2xxx の範囲を持つニューヨーク オフィスに DID のサービスを提供します。911 へのコールが 415-555-1800 で発生した場合、SIP プロバイダーは PSAP を提供するために、サンフランシスコの選択ルータにコールをルーティングする必要があります。ニューヨーク オフィスの内線 212-448-2840 のユーザが 911 をダイヤルした場合、コールは同じ SIP トランクを経由してニューヨーク エリアの適切な選択ルータにルーティングされ、発信者にとって適切な PSAP に到達します。

CAMA

Centralized Automatic Message Accounting（CAMA）トランクも、MLTS がコールを 911 ネットワークに送信することを可能にします。PRI 方式との相違点は、次のとおりです。

- CAMA トランクは、E911 選択ルータに直接接続されます。E911 選択ルータと MLTS ゲートウェイ ポイント間の距離をカバーするために、マイレージ追加料金が適用される場合があります。
- CAMA トランクは、911 コールだけをサポートします。CAMA トランクの設置と操作に関連した資産コストと運営コストは、911 トラフィックのサポートだけに使用されます。
- MLTS 業界の CAMA トランクは、固定エリア コードに制限されることがあります。このエリア コードは、一般に、リンク プロトコルで暗黙的に示されます（つまり、明示的に送信されません）。接続には、すべてのコールが同じ固定エリア コードを共用するため、7 桁または 8 桁だけが ANI として送信されます。

静的 ANI（回線接続）

静的 ANI は、PSTN との回線（トランクではなく）接続をサポートし、発信側の電話機の CPN に関係なく、回線の ANI が、その回線で発信されるすべての 911 コールに関連付けられます。静的 ANI は、LEC の物理的な相互接続ポイントに基づきます。静的 ANI はキャリアによって、LEC の相互接続ポイント上に定義されるため、静的 ANI の緊急コール ルーティングは、サービス プロバイダー ALI（SP-ALI）とも呼ばれます。単純な旧式の電話サービス（POTS）回線は、この用途に使用される接続の最も一般的なタイプです。

POTS 回線は、最も単純で、かつ広くサポートされている PSTN インターフェイスの 1 つです。POTS 回線は、通常、911 コールを受け入れるように設定されています。さらに、既存の E911 インフラストラクチャは、POTS 回線からの 911 コールを適切にサポートします。

POTS アプローチには、次の特徴があります。

- POTS 回線に関連する運用コストが低くなります。
- POTS 回線に、電源障害に備えたバックアップ回線の役割を持たせることができます。
- POTS 回線番号を、ALI データベースに入力されるコールバック番号として使用できます。
- POTS 回線は、PSTN へのローカル PRI、または CAMA アクセスに見合うユーザ密度を持たないロケーションに対して、最低コストで最適な 911 サポートを実現します。
- PSTN の敷設に伴い、POTS 回線は広く普及しています。

このタイプのインターフェイスを介した 911 発信コールはすべて、E911 ネットワークによって同じものとして扱われます。ANI は単なる POTS 回線番号の可能性があるため、E911 ネットワークに提示される ANI 操作を制御できるようにするツール（トランスレーションまたはトランスフォーメーションなど）は、無関係です。

Cisco Emergency Responder

IP 通信テクノロジーの主な利点の 1 つは、移動、追加、および変更の管理が容易であることです。ユーザが介入することなく自動的に 911 情報を更新する移動、追加、および変更をサポートするために、シスコは Cisco Emergency Responder（Emergency Responder）と呼ばれる製品を開発しました。

Cisco Emergency Responder は、次の主な機能を備えています。

- 検出された電話機の物理ロケーションに基づいて、電話機を緊急応答ロケーション（ERL）に動的に関連付けます。
- コールバックのために緊急ロケーション識別番号（ELIN）を発信側電話機に動的に関連付けます。上記の項で説明されている一般的な緊急サービスのシナリオと異なり、Cisco Emergency Responder は、911 コールを発信した電話機にコールバックできるようにします。
- 緊急コールが進行中であることを知らせるために、指定された通話者へのオンサイト通知が可能です（ポケットベル、Web ページ、電子メール、または電話を使用）。電子メール、ポケットベル、および Web ページによる通知には、発信者の名前と電話番号、ERL、およびそのコールに関連した日時の詳細が含まれます。電話による通知では、緊急コールの発信番号に関する情報が提供されます。

ERL と ELIN の詳細については、緊急応答ロケーションのマッピング（15-13 ページ）と緊急ロケーション識別番号のマッピング（15-14 ページ）を参照してください。Cisco Emergency Responder の詳細については、Cisco Emergency Responder の設計に関する考慮事項（15-19 ページ）と、次の Web サイトで入手可能な Cisco Emergency Responder 製品のマニュアルを参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html

Cisco Emergency Responder のデバイス ロケーション検出方法

Cisco Emergency Responder は、複数の方法を使用して、デバイスの物理的なロケーションを特定します。より具体的なロケーションが検出されるほど、より短い時間に緊急事態の場所を位置付けて緊急サービスを提供できるので、Emergency Responder は次の方法（優先順位の降順に記載）を使用して、緊急発信者のロケーションを特定します。

1. スイッチ ポート検出
2. アクセス ポイント アソシエーション
3. IP サブネット
4. 静的 DN 割り当て
5. デフォルト ルート（Default route）

スイッチ ポート検出

Cisco Emergency Responder でロケーションを特定するために使用される第 1 の方法は、スイッチ ポート レベルでのレイヤ 2 検出によるエンドポイントの検出です。レイヤ 2 の Cisco Discovery Protocol（CDP）検出を通してエンドポイントを検出することで、Emergency Responder は、ブースやオフィスのネットワーク ジャックへのネットワーク ケーブルの物理終端に基づいて発信側デバイスの正確な物理的ロケーションを判断できます。接続デバイスの検出メカニズムの信頼性は高いものですが、その物理ロケーションが精度を保つためには次の 2 点が主要な前提となります。

- 企業の有線インフラストラクチャは適切に確立されており、散発的に変化しないこと。また、ワイヤリング クローゼットが変化した場合は常に、Emergency Responder の管理者に、そのことを伝える通知がトリガーされること。
- Cisco Emergency Responder が、このインフラストラクチャをブラウズできること。つまり、Cisco Emergency Responder は、敷設されたネットワーク インフラストラクチャとの簡易ネットワーク管理プロトコル（SNMP）セッションを確立でき、接続された電話機を検出するためにネットワーク ポートをスキャンできること。

Cisco Emergency Responder はコールの発信ポートを検出すると、そのコールを、そのポートのロケーション用として事前に確立された ERL に関連付けます。このプロセスは、ロケーションに事前に確立された ELIN との関連付けと、発信 ERL に基づく、E911 インフラストラクチャの適切な出口点の選択も行います。

アクセス ポイント アソシエーション

ワイヤレス デバイスは、有線のエンドポイントとは異なる検出機能とトラッキング特性を持つため、Cisco Emergency Responder はワイヤレス クライアントをトラッキングする際に、Unified CM 11.5 以降で利用可能なロケーション認識機能を使用します。ロケーション認識機能を使用することにより、Emergency Responder は、Unified CM で展開されたすべてのアクセスポイントを同期し、AP を適切な ERL に割り当てることができます。また、AP 間のモバイル デバイスの移動に関する情報も更新できます。

Emergency Responder は、Unified CM のロケーション認識機能を通して、企業全体でワイヤレス クライアントをトラッキングできます。モバイル クライアントが企業内の AP に関連付けられると、デバイスはコール制御を通してその AP の基本サービス セット識別子（BSSID）を Unified CM に送信します。Unified CM は次に、新しい AP アソシエーションの情報を使用してデータベースを更新します。Emergency Responder は、最後の要求以降に AP アソシエーションを更新したすべてのデバイスに関して、Unified CM からのデバイス更新を定期的に要求します。Emergency Responder は、最後の要求以降に移動したデバイスの情報のみを受信します。Unified CM 11.5 では、要求間隔は 2 分です。

IP サブネット（IP Subnet）

また、Cisco Emergency Responder は、IP サブネットに対して ERL を設定し、IP アドレス別に IP エンドポイントのロケーションを割り当てる機能を提供します。この機能は、接続されたスイッチ ポートで Cisco Emergency Responder が見つけることができない、Cisco Unified CM に登録されたワイヤレス IP フォン、IP ソフトフォン、Cisco Discovery Protocol（CDP）をサポートしていないコラボレーション エンドポイント、およびサードパーティの SIP エンドポイントを見つけるために使用できます。また、この機能は、有線の Cisco Collaboration エンドポイントに対して接続されたスイッチ ポート ロケーションの代わりに使用したり、これらのスイッチ ポート ロケーションに追加して使用したりできます。Cisco Collaboration エンドポイントに対して接続されたスイッチ ポートと IP サブネット ロケーションの両方が利用可能である場合、Cisco Emergency Responder は接続されたスイッチ ポートを優先して利用します。これは、接続されたスイッチ ポートは通常 IP サブネット ロケーションよりも具体的であるためです。接続されたスイッチ ポートの検出で遅延やエラーが発生した場合であっても適切な ERL が割り当てられるように、接続されたスイッチ ポートと IP サブネット ロケーションの両方を使用することを推奨します。

Cisco Emergency Responder では、1 つの ERL に対して 2 つ以上の ELIN を使用できます。この機能拡張の目的は、次の例に示されているように、同じ期間内に 1 つの ERL から複数の 911 コールが発信される特定のケースに対応することです。

例 1

- 電話機 A と電話機 B はどちらも ERL X 内に存在し、ERL X は ELIN X に関連付けられています。
- 電話機 A は午後 1 時に 911 にコールします。ELIN X は、そのコールを PSAP X にルーティングするために使用され、PSAP X はそのコールに応答し、コールを解除します。その後、午後 1 時 15 分に電話機 B が 911 にコールします。再び ELIN X が、コールを PSAP X にルーティングするために使用されます。
- PSAP X は、電話機 B からのコールを解除したあと、電話機 A の最初のコールに関連する詳細情報を取得するために、電話機 A にコールバックすることを決定します。PSAP は ELIN X にダイヤルしますが、（目的の電話機 A ではなく）電話機 B につながります。

この状況を回避するために、Cisco Emergency Responder では、各 ERL に ELIN のプールを定義できます。このプールにより、後続のコールごとに別個の ELIN をラウンドロビン方式で使用できます。この例で ERL X に対して 2 つの ELIN を定義すると、例 2 で説明する状況になります。

例 2

- 電話機 A と電話機 B はどちらも ERL X 内に存在し、ERL X は ELIN X1 と ELIN X2 の両方に関連付けられています。
- 電話機 A は午後 1 時に 911 にコールします。ELIN X1 は、そのコールを PSAP X にルーティングするために使用され、PSAP X はそのコールに応答し、コールを解除します。その後、13:15 に電話機 B が 911 にコールし、このコールを PSAP X にルーティングするために ELIN X2 が使用されます。
- PSAP X は、電話機 B からのコールを解除したあと、電話機 A の最初のコールに関連する詳細情報を取得するために、電話機 A にコールバックすることを決定します。PSAP は ELIN X1 にダイヤルし、電話機 A につながります。

3 番めの 911 コールが発信されたが ERL に 2 つの ELIN しかない場合、コールバック機能が、最後の 2 人の発信者にしか正しく到達できません。

緊急サービスのハイ アベイラビリティ

最も危機的な状況であってもユーザが緊急サービスを利用できることは非常に重要です。したがって、企業で緊急サービスを配置する場合は、ハイ アベイラビリティの計画を慎重に行う必要があります。

Cisco Emergency Responder は、アクティブ/スタンバイ モードで最大 2 台のサーバを使用するクラスタリングをサポートします。データは、プライマリ Cisco Emergency Responder サーバとセカンダリ Cisco Emergency Responder サーバ間で同期されます。プライマリ サーバが利用できない場合にコールがセカンダリ サーバにルーティングされるようにするために、システム管理者は特定のプロビジョニング ガイドラインに従って、CTI ルート ポイントと、Cisco Unified CM でこれらの CTI ルートポイントに関連付けられたディレクトリ番号（DN）を設定する必要があります。設定の詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』を参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

両方の Cisco Emergency Responder サーバが利用できない場合は、ローカル ルート グループ（LRG）を使用して適切な ELIN/ERL（Cisco Emergency Responder が提供したものよりも具体的でない可能性があります）を持つ適切な PSAP にコールをルーティングできます。また、別の方法として、コールを内部セキュリティ オフィスにルーティングして発信者のロケーションを決定できます。いずれの場合であっても、このプロビジョニングは Cisco Unified CM で実行する必要があります。

Cisco Emergency Responder の冗長性以外に、911 緊急コールをルーティングし、シングル ポイント障害を回避できるように Cisco Unified CM の冗長性とゲートウェイ/トランクの冗長性も考慮する必要があります。

Cisco Emergency Responder クラスタリングのキャパシティ プランニング

Cisco Emergency Responder クラスタでは、ホーム Cisco Emergency Responder グループのトラッキング ドメイン外部でローミングするエンドポイントの数が、スケーラビリティ ファクタとなります。このような電話機の数は、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「*Network Hardware and Software Requirements*」に記載されている制限内に収める必要があります。

https://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

Emergency Responder の最大ローミング キャパシティ制限を超える必要のある配置（たとえば、複数の Unified CM クラスタを含む大規模なキャンパス配置）では、IP サブネットによって電話機の移動をトラッキングできます。各 Cisco Emergency Responder グループで IP サブネットを定義し、Cisco Emergency Responder グループごとに各 ERL を 1 つの ELIN に割り当てることによって、実質的にローミング電話機をなくすことができます。これは、キャンパス内のすべての電話機が、それぞれの Cisco Emergency Responder グループのトラッキング ドメインに含まれるためです。

適切なサイジングになるよう、Cisco Collaboration Sizing Tool を使用してください。このツールは、シスコのパートナーと従業員だけが利用できます（https://cucst.cloudapps.cisco.com/landing で適切なログインが必要）。このサイジング ツールにアクセスできない場合は、シスコ アカウント チームまたはパートナー インテグレータと協力してシステムのサイジングを適切に行ってください。

911 緊急サービスの設計に関する考慮事項

Multi-Line Telephone System（MLTS）配置の 911 緊急サービスを計画している場合は、最初に電話サービスが必要なすべての物理ロケーションを確立します。これらのロケーションは、次のように分類できます。

- 単一ビル配置：すべてのユーザは同じ建物に存在しています。
- 単一キャンパス配置：ユーザは近距離にある建物のグループに存在しています。
- マルチサイト配置：ユーザは地理的に広い範囲に分散しており、WAN 接続を介して呼処理サイトにリンクされています。

これらのロケーション（つまり、配置のタイプ）は、911 サービスの設計と実装に使用される基準に影響を与えます。次の各項で、主要な基準を、それぞれの一般的な状況および例外的な状況とともに説明します。これらの基準を分析し、適用する際には、ネットワーク内の電話機ロケーションによって受ける影響を考慮してください。

緊急応答ロケーションのマッピング

National Emergency Number Association（NENA）は、企業通信システムで 911 を管理する規則を制定する際に、州および連邦機関が使用すべき法律モデルを提案しています。NENA 提案の概念の 1 つは、次のように定義される緊急応答ロケーション（ERL）の概念です。

> *911 緊急応答チームの派遣先ロケーション：このロケーションは、緊急応答チームがそのロケーション内で発信者の位置をすばやく確認するための妥当な機会を提供できる、明確なものでなければならない。*

この要件は、各エンドポイントのロケーションを個々に識別するのではなく、エンドポイントを「ゾーン」(ERL)にグループ化することを見込んでいます。ERL の最大サイズは、この法律の地域ごとの実施に応じて異なる可能性がありますが、ここでは説明の基準として 7000 平方フィートを使用します(ここで説明する概念は、任意の州または地域で許可される最大 ERL サイズとは無関係です)。

緊急ロケーション識別番号(ELIN)が、各 ERL に関連付けられます。ELIN は、E911 ネットワーク内でコールのルーティングに使用される完全修飾 E.164 番号です。関連した ERL から発信するすべての 911 コールで、ELIN が E911 ネットワークに送信されます。このプロセスは、911 の目的で、複数の電話機を同じ完全修飾 E.164 番号に関連付けることを可能にし、DID 電話機と非 DID 電話機にも同様に適用できます。

(注)　このマニュアルは、法律の実際の要件を提示しようとするものではありません。ここで提示する情報や例は、説明だけを目的としています。システムの設計担当者の責任において、適用されるローカル要件を確認してください。

たとえば、ある建物に 70,000 平方フィートの作業領域があり、100 台のエンドポイントがあるとします。911 機能を計画する際に、この建物を 7000 平方フィートごとの 10 個のゾーン(ERL)に分割し、そこに置かれた各エンドポイントを ERL に関連付けることができます。911 コールが発信されると、関連した ELIN を PSAP に送信することによって、ERL(複数のエンドポイントに対して同一)が識別されます。この例のように、エンドポイントが均等に分散されている場合、10 台のエンドポイントを持つ各グループには、同じ ERL があり、したがって同じ ELIN を持ちます。

各種法律により、最小台数のエンドポイント(たとえば 49)と最低作業領域(たとえば、40,000 平方フィート)が定義されます。この数を下回ると、MLTS 911 の要件は適用されません。しかし、法律が企業の 911 機能を要求しない場合であっても、911 機能をプロビジョニングすることが常に最善の方法です。

緊急ロケーション識別番号のマッピング

一般的に、緊急ロケーション識別番号(ELIN)と呼ばれる 1 つの完全修飾 E.164 番号を、各 ERL に関連付ける必要があります(ただし、Cisco Emergency Responder を使用する場合は、ERL ごとに複数の ELIN を設定できます)。ELIN は、E911 インフラストラクチャ全体でコールをルーティングするために使用されます。また、PSAP により、ALI データベースへのインデックスとして使用されます。

ELIN は次の要件を満たす必要があります。

- ELIN は、E911 インフラストラクチャ全体でルーティング可能である必要があります(インターフェイス タイプ(15-6 ページ)の項の例を参照)。ELIN がルーティング不能である場合、関連した ERL からの 911 コールは、E911 選択ルータでプログラムされたデフォルト ルーティングに応じて処理されます。
- 企業の ERL-to-ELIN マッピングが定義されたあとは、LEC を使用して、対応する ALI レコードを設定する必要があります。その結果、PSAP にサービスを提供する ANI と ALI データベース レコードを正確に更新できます。
- ELIN はコールバック用に PSAP から到達可能である必要があります。

ELIN マッピング プロセスは、所定の ERL に対する E911 インフラストラクチャとのインターフェイスのタイプに応じて、次のいずれかを選択できます。

- 動的 ANI インターフェイス

  このタイプのインターフェイスを使用すると、ネットワークに渡される発番号識別は MLTS によって制御されます。MLTS のテレフォニー ルーティング テーブルは、発信側エンドポイントの ERL に基づいて、正しい ELIN をコールに関連付けます。Cisco Emergency Responder が配置されていないシナリオの場合、Unified CM によりトランスフォーメーション マスクを使用して、911 へのコールの発信者番号を変更できます。たとえば、所定の ERL 内にあるすべてのエンドポイントが、トランスレーション パターン（911）と発呼側トランスフォーメーション マスク（エンドポイントの CPN をそのロケーションの ELIN に置き換えます）を含むパーティションをリストする同じコーリング サーチ スペースを共有できます。一方、Cisco Emergency Responder が配置されている場合、発信者番号の変更は Emergency Responder システムで実行する必要があります。

- 静的 ANI インターフェイス

  このタイプのインターフェイスを使用すると、ネットワークに渡される発信者番号識別は PSTN によって制御されます。これは、インターフェイスが POTS 回線である場合に該当します。ELIN は POTS 回線の電話番号であり、電話機の発信者識別番号をさらに操作することはできません。

PSAP コールバック

最初の会話の完了後、または PSAP オペレータがコールに応答する前に発信者が電話を切った場合に、PSAP が発信者に到達できなくてはらなない場合があります。PSAP がコールバックできるかどうかは、PSAP が最初の着信コールとともに受信する情報によって決まります。

この情報は、次の 2 段階のプロセスによって PSAP に送信されます。

1. 最初に、自動番号識別（ANI）が PSAP に送信されます。ANI は、コールをルーティングするために使用される E.164 番号です。この説明では、PSAP で受信された ANI は、MLTS が送信した ELIN を指しています。
2. PSAP は ANI を使用して、データベースを照会し、自動ロケーション識別（ALI）を取得します。ALI は、次のような情報を PSAP 担当者に知らせます。
   - 発信企業名
   - 物理アドレス
   - 該当する公衆安全機関
   - コールバック情報を組み込むことができる、その他のオプション情報。たとえば、救援活動の調整に役立てるために、企業のセキュリティ サービスの電話番号がリストされています。

標準的な状況

- ANI 情報が PSAP コールバックに使用されます。ここでは、ELIN が PSTN ダイヤル可能な番号であると想定します。
- ELIN は、MLTS に関連した PSTN 番号です。PSTN から ELIN にコールすると、そのコールは、MLTS によって制御されるインターフェイス上で終端します。
- システム内の任意の ELIN に発信されたコールが、関連した ERL のすぐ近くにある電話機（または複数の電話機）を鳴らすように、コール ルーティングをプログラムするのは、MLTS システム管理者の責任です。
- ERL-to-ELIN マッピングが設定されたあと、修正が必要なのは、企業の物理的な状況に変更があった場合だけです。電話機が単にシステムに追加、システム内で移動、またはシステムから削除された場合、ERL-to-ELIN マッピングと、それに関連する ANI/ALI データベース レコードを変更する必要はありません。

例外的な状況

- 発信 ERL のすぐ近くへのコールバックを、オンサイト緊急デスクへのコールバックのルーティングと組み合わせる（または置き換える）ことができます。これは、PSAP が最初の発信者を呼び出し、緊急事態に対してただちに支援を要請するときに役立ちます。
- たとえば、エリア コードの分割、公衆安全業務の新しい配分を必要とする地方自治体業務の変更、新しい建物の追加、または 911 の目的でコールの望ましいルーティングに影響を与えるその他の変更により、企業の状況が変わる場合があります。こうした状況では、企業の ERL-to-ELIN マッピングおよび ANI/ALI データベース レコードの変更が必要です。

ダイヤル プランに関する考慮事項

アクセス コード（たとえば、9 など）を使用するかどうかにかかわらず、システムが緊急コールを認識しやすいようにダイヤル プランを設定することを強く推奨します。北米の緊急ストリングは、通常、911 です。ストリング 911 と 9911 の両方を認識するようにシステムを設定することを強く推奨します。

また、緊急ルート パターンに Urgent Priority のマークを明示的に付けて、Unified CM が、コールのルーティング前に、桁間タイムアウト（Timer T.302）を待機*しない*ようにすることも強く推奨します。

これ以外の緊急コール ストリングを、システム上で同時にサポートできます。システム ユーザには、選択した緊急コール ストリングを想定した訓練を行うことを強く推奨します。

また、ユーザが誤って緊急ストリングをダイヤルした場合に適切な対応ができるように訓練することも必要です。北米では、アクセス コード 9 を使用して長距離番号にアクセスしようとするユーザが、誤って 911 をダイヤルする可能性があります。このような場合、ユーザは、緊急事態ではないため、緊急人員を派遣する必要がないことを確認するために、回線を保持する必要があります。Cisco Emergency Responder のオンサイト通知機能では、誤って発信されたコールを含め、911 に発信されたすべてのコールの詳細なアカウント情報を提供することによって、そのような疑わしい 911 コールの起点にある電話機を識別できます。緊急派遣センターは、911 へのコールが誤って発信されたものだと確認できない場合、緊急サービスを現場に派遣する必要があります。1 ヵ月に 4 回以上の緊急サービス派遣が単一の顧客に行われると、多くの場合、その会社への罰金が発生します。

マルチサイト配置では、ダイヤル プラン設定により、緊急コールがサイトに対してローカルな PSTN ゲートウェイを介して常にルーティングされ、緊急コールが該当する地域で最も近い PSAP にルーティングされるようにする必要があります。これを実現するメカニズムの 1 つとして、Cisco Unified CM のローカル ルート グループ機能を使用することがあります。集中型 PSTN アクセスによるマルチサイト配置の場合、市内電話による PSAP へのルーティングはできません。集中型 PSTN アクセスによる配置では、Unified CM 管理者は、PSTN プロバイダーが ANI または ELIN に基づいて適切な PSAP に緊急コールをルーティングすることを確認する必要があります。サービス プロバイダーが複数サイトに対して緊急コール ルーティング サービスを提供できない場合、E911 対応範囲に含まれていないすべてのサイトはロケーション接続（アナログ回線）を持つか、または集中型 PSTN アクセスがリモート サイト（SIP トランク）用の 911 コール配信をサポートする必要があります（インターフェイス タイプ（15-6 ページ）の項の例を参照）。

また、マルチサイト配置では、緊急番号が、常に到達可能であり、実装されたサービス クラス（CoS）に関係なくモビリティ ユーザ（拡張モビリティおよびデバイス モビリティ）のためにローカル PSTN ゲートウェイを介してルーティングされることが非常に重要です。サイト/デバイス方法が使用される場合は、緊急コールをルーティングするためにデバイスのコーリング サーチスペース（CSS）を使用できます。

シスコは、Cisco Emergency Responder で発信側変更を有効にすることを推奨しています。この機能が有効な場合は、発信者番号が Cisco Emergency Responder によって緊急コールを表す ELIN で置き換えられます。発信側変更が有効でない場合は、DID が PSAP に送信されます。または、発信側がルート パターンまたはゲートウェイで定義されている ELIN で置き換えられるように Cisco Unified CM を設定する必要があります。

ゲートウェイに関する考慮事項

システムの緊急コールを処理するゲートウェイを選択する際には、次の要素を考慮してください。

ゲートウェイの配置

地域通信事業者（LEC）ネットワーク内で、911 コールは、コールの起点に基づいて、ローカル側で有効なインフラストラクチャ上でルーティングされます。サービスを提供する Class 5 スイッチは、ロケーションに関連した PSAP に直接接続されるか、E911 選択ルータに接続されます。この選択ルータ自体は、その地域に有効な PSAP 群に接続されます。

シスコの IP ベースの企業通信アーキテクチャでは、リモート側に置かれているゲートウェイに、オンネットでコールをルーティングすることが可能です。たとえば、サンフランシスコに置かれているエンドポイントは、IP ネットワークを介して、サンノゼにあるゲートウェイにコールを伝送してから、LEC のネットワークに送信できます。

911 コールの場合、緊急コールが適切なローカル PSAP にルーティングされるように、LEC ネットワークへの出口点を選択することが重要です。前述の例では、サンフランシスコのエンドポイントからの 911 コールが、サンノゼのゲートウェイにルーティングされてしまうと、サンフランシスコの PSAP に到達できません。これは、そのコールを受信するサンノゼの LEC スイッチには、サンフランシスコ PSAP にサービスを提供する E911 選択ルータへのリンクがないためです。さらに、サンノゼ地域の 911 インフラストラクチャは、サンフランシスコの発信者番号に基づいてコールをルーティングすることができません。

一般的に、911 コールは、発信側エンドポイントと物理的に同じ場所にあるゲートウェイにルーティングしてください。共通ゲートウェイを使用して、複数のロケーションからの 911 コールを集約できるかどうかは、LEC に問い合わせてください。所定の地域の 911 ネットワークが、911 コールに中央ゲートウェイを使用しやすい場合でも、911 コール ルーティングが WAN 障害中の影響を受けないように、発信側電話機と同じ場所にあるゲートウェイを使用することが望ましいことに注意してください。

ゲートウェイのブロック

911 コールが「全トランク ビジー」状況にならないようにする必要があります。911 コールを接続する必要がある場合、トランキング リソースの不足により他のタイプのコールがブロックされる場合でも、911 コールは処理可能にしておく必要があります。このような状況に備えて、明示トランク グループを 911 コール専用にできます。

緊急コールを独占的に緊急トランク グループにルーティングするのが、好ましい方法です。もう 1 つの方法は、通常の PSTN コールと同じトランク グループに緊急コールを送信し（インターフェイスが許可する場合）、専用緊急トランク グループへの代替パスを用意するものです。後者の方法では、最大限の柔軟性が得られます。

たとえば、緊急コールを PRI トランク グループに向け、オーバーフロー状態になったときに備えて POTS 回線への代替パス（緊急コール専用に予約済み）を指定できます。代替トランク グループに 2 つの POTS 回線を配置すると、メインのトランク グループで許可されたすべてのコール以外に、少なくとも 2 つの 911 コールを同時にルーティングできることが保証されます。

優先ゲートウェイが使用不能になった場合、代替ゲートウェイが使用されるように、緊急コールを代替番号にオーバーフローできます。たとえば、北米で 911 にダイヤルされたコールは、E.164（911 以外）ローカル緊急番号にオーバーフローできます。この方法は、北米の 911 ネットワーク インフラストラクチャを利用しません（つまり、選択ルーティング、ANI、または ALI サービスを使用しません）。この方法は、該当する公衆安全機関によって受け入れられる場合にかぎり、ネットワーク リソースの不足による緊急コールのブロックを回避する最後の手段としてだけ使用してください。

応答監視

通常の状態では、緊急番号に発信されたコールは、PSAP との接続後、応答監視を返す必要があります。応答監視は、他のコールと同じように、オンネット発信者と、LEC ネットワークへの出口インターフェイスとの間の全二重音声接続をトリガーできます。

一部の北米 LEC では、「無料」コールを行う場合、応答監視が返されないことがあります。これは、一部の通話無料番号（たとえば、800 番など）にも該当します。例外的な状況では、緊急コールは「無料」コールと見なされるため、PSAP との接続後、応答監視が返されないことがあります。この状況は、911 テスト コールを発信するだけで検出できます。PSAP との接続後、音声が存在する場合、コール タイマーが発信コールの所要時間を記録します。コール タイマーがない場合は、応答監視が返されなかった可能性があります。応答監視が返されない場合、LEC に連絡して、この状況を報告することを強く推奨します。望ましい機能ではない可能性があります。

この状況が地域通信事業者（LEC）によって修正できない場合、LEC ネットワークにコールが発信されるときに応答監視を必要とし*ない*ようにイーグレス ゲートウェイを設定することを推奨します。また、応答監視が返されない場合でも、プログレス インジケータ トーン、代行受信メッセージ、および PSAP との通信が可能であるように、両方向で音声をカットスルーすることも推奨します。

デフォルトでは、Cisco IOS ベースの H.323 ゲートウェイは、両方向で音声を接続するために、応答監視を受信する必要があります。これらのゲートウェイ上で応答監視が必要ないようにするには、次のコマンドを使用してください。

- **progress_ind alert enable 8**

  このコマンドは、アラートの受信時にプログレス インジケータ 8（インバンド情報が使用可能）を受信することに相当します。このコマンドを使用すると、ゲートウェイの POTS 側が、コールの起点方向の音声を接続できます。

- **voice rtp send-recv**

  このコマンドは、宛先スイッチから Connect メッセージを受信する前に、逆方向と順方向の両方の音声カットスルーを可能にします。このコマンドは、すべての Voice over IP（VoIP）コール（使用可能である場合）に影響を与えます。

応答監視が提供されない場合は、コール詳細レコード（CDR）に 911 コールの接続時間または期間が正確に反映されません。その結果、コール レポーティング システムが、911 コール関連の統計情報を正しく表すことができない場合があります。

いかなる場合でも、すべてのコール パスからの 911 コール機能をテストし、PSAP との接続後、応答監視が返されることの確認を行うことを強く推奨します。

Cisco Emergency Responder の設計に関する考慮事項

デバイス モビリティにより、緊急コールに特別な設計上の考慮事項が生じます。Cisco Emergency Responder（Emergency Responder）は、デバイスの動的な物理ロケーションに基づいて、デバイス モビリティをトラッキングし、システムによる緊急コールのルーティングを適合させるために使用できます。

コール アドミッション制御ロケーション間のデバイス モビリティ

集中型呼処理配置では、Cisco Emergency Responder は Cisco エンドポイントの移動を検出し、移動したエンドポイントを適切な ERL に自動的に再び割り当てることができます。ただし、移動したエンドポイントに対する Cisco Unified CM のロケーションベースのコール アドミッション制御は、新しいロケーションの電話機の WAN 帯域幅使用量を正しく把握できず、WAN 帯域幅リソースのオーバーサブスクリプションやアンダーサブスクリプションが発生する可能性があります。たとえば、電話機を支社 A から支社 B に物理的に移動したにもかかわらず、エンドポイントのコール アドミッション制御ロケーションが同じままである（たとえば、Location_A など）場合、Location_A に使用可能な帯域幅がすべて他のコールで使用中であれば、そのエンドポイントから 911 に発信するコールは、コール アドミッション制御拒否によりブロックされる可能性があります。このようなコールのブロックを回避するために、デバイスのロケーションとリージョン パラメータを使用するよう手動で設定する必要がある場合があります。

Cisco Unified CM デバイス モビリティを使用すると、新しい物理ロケーションを反映するよう Unified CM でエンドポイントの設定（コーリング サーチ スペースとロケーション情報を含む）を自動的に更新できます。デバイス モビリティを使用しないと、Cisco Unified CM で設定を手動で変更することが必要になる場合があります。

デバイス モビリティ機能の詳細については、デバイス モビリティ（21-15 ページ）の項を参照してください。

デフォルトの緊急応答ロケーション

Cisco Emergency Responder は、エンドポイントの物理的なロケーションを直接判別できない場合、コールにデフォルトの緊急応答ロケーション（ERL）を割り当てます。デフォルトの ERL は、こうしたすべてのコールを特定の PSAP に導きます。この状態が発生した場合、コールの送信先について共通の推奨事項はありませんが、通常、中央に置かれ、最大の公衆安全管轄権を提示する PSAP を選択するのが望ましい方法です。また、デフォルト ERL の緊急ロケーション識別番号（ELIN）の ALI レコードに、企業の緊急番号の連絡先情報を取り込み、発信者のロケーションの不確実性についての情報を提供することも推奨します。さらに、緊急コールのデフォルト ルーティングが発生したというマークを ALI レコードに付けることも推奨します。また、別の方法として、コールを内部セキュリティ オフィスにルーティングして発信者のロケーションを決定できます。

ワイヤレス クライアント向けの Cisco Emergency Responder とロケーション認識

Cisco Emergency Responder 11.5 以降のリリースでは、企業のアクセスポイントまでワイヤレス エンドポイントやクライアントをトラッキングできます。Cisco Emergency Responder での構成変更を最小限に抑えるために、すべてのアクセスポイントは Cisco Unified Communications Manager から同期される必要があります。また、同期プロセスでは、Cisco Unified CM で発生するアクセス ポイントに関する追加、更新、削除もすべて処理されます。Unified CM でのすべてのアクセス ポイント変更は、変更後 2 分以内に Emergency Responder に反映されます。アクセス ポイントは Emergency Responder 内で定義できません。また、Emergency Responder 内でロケーション識別用に使用されるすべてのアクセス ポイントは Unified CM で定義する必要があります。Unified CM は、シスコ ワイヤレス LAN コントローラの同期サービスを使用して、アクセス ポイントを Unified CM データベースに自動的に同期することで、アクセス ポイントを管理しています。シスコ ワイヤレス LAN コントローラの同期サービスは、シスコ ワイヤレス LAN コントローラ（WLC）と連携してアクセスポイント情報を管理します。他のベンダーを WLC サービス用に使用する場合は、一括管理ツール（BAT）を使用して、アクセス ポイントを Cisco Unified CM データベースに一括してインポートする必要があります。

ワイヤレス アクセス ポイントに関連付けられるモバイル クライアントまたはワイヤレス デバイスは、関連付けられたアクセス ポイントの基本サービス セット識別子（BSSID）を Unified CM に送信する必要があります。モバイル クライアントでの更新生成頻度の関係上、Unified CM では、モバイル デバイスおよびワイヤレス クライアントのロケーション更新の頻度について、ノードあたりの更新回数を毎秒 90 回に制限しています。ロケーション更新の回数が長時間にわたってこのレートを超えると、Unified CM はそれ以上の更新を遅延し、480「ビジー状態（Busy Here）」メッセージを表示します。この場合、クライアントは一定時間待機した後に、ロケーション更新を再送信します。更新を再送信するまでの合計遅延時間は、Cisco Emergency Responder または Unified CM ではなく、クライアントに依存します。

モバイル クライアントまたはワイヤレス デバイスのロケーションが Cisco Unified CM で更新されると、その更新は 2 分以内に Cisco Emergency Responder に反映されます。

Cisco Emergency Responder および Extension Mobility

Cisco Emergency Responder は、Cisco Unified CM クラスタ内で Extension Mobility をサポートします。また、両方の Cisco Unified CM クラスタが、共通の Cisco Emergency Responder サーバまたはグループによってサポートされるか、Cisco Emergency Responder クラスタとして設定された 2 つの Cisco Emergency Responder サーバまたはグループによってサポートされる場合、Cisco Emergency Responder は、Extension Mobility Cross-Cluster（EMCC）もサポートします。いずれの場合でも、Cisco Unified CM クラスタが、911 コールに対する EMCC に関連付けられた付加コーリング サーチ スペース（CSS）を使用しないよう設定し、両方の Cisco Unified CM クラスタですべての 911 コールに対して Cisco Emergency Responder を使用するよう設定する必要があります。

Cisco Emergency Responder およびビデオ

Cisco Emergency Responder は、Cisco Video Collaboration エンドポイントを、その機能に応じて次の方法で検出できます。

- CDP をサポートするビデオ コラボレーション エンドポイント（15-21 ページ）
- CDP をサポートしないビデオ コラボレーション エンドポイント（15-21 ページ）

ビデオ エンドポイントが検出された方法にかかわらず、ビデオは、PSAP への緊急コールのメディアとしてサポートされていないことに注意する必要があります。

(注)　この章で説明する内容は、Cisco Emergency Responder が Cisco Unified Communications Manager（Unified CM）と共に使用される場合のみ適用されます。Cisco TelePresence Video Communication Server（VCS）は現在、緊急サービスをサポートしていません。

CDP をサポートするビデオ コラボレーション エンドポイント

Cisco Discovery Protocol（CDP）をサポートしている社内にあるビデオ コラボレーション エンドポイントについて、次の URL で入手可能な『*Cisco Emergency Responder Administration Guide*』の最新バージョンにある Emergency Responder のスイッチ設定情報に示されているように、それらのエンドポイントを、CDP を通して Cisco Emergency Responder によってトラッキングされる他のコラボレーション エンドポイントと同様に扱うことをシスコでは推奨しています。

https://www.cisco.com/en/US/partner/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

社外にある CDP をサポートするビデオ コラボレーション エンドポイントについて、次の URL で入手可能な『*Off-Premise Location Management User Guide for Cisco Emergency Responde*』の最新バージョンにある IP Phone の構外サポートに関する情報に示されているように、それらのビデオ コラボレーション エンドポイントを音声コラボレーション エンドポイントと同様に扱うことをシスコでは推奨しています。

https://www.cisco.com/en/US/partner/products/sw/voicesw/ps842/products_user_guide_list.html

CDP をサポートしないビデオ コラボレーション エンドポイント

Cisco Discovery Protocol（CDP）をサポートしないビデオ コラボレーション エンドポイントについて、音声コラボレーション エンドポイントに専用回線を使用することをシスコでは推奨しています。ビデオ コラボレーション エンドポイントをトラッキングする必要がある場合、次の URL で入手可能な『*Cisco Emergency Responder Administration Guide*』の最新バージョンにある IP サブネットベースの ERL の設定に関する情報に示されているように、IP サブネット ERL を設定することをシスコでは推奨しています。

https://www.cisco.com/en/US/partner/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

Cisco Emergency Responder と構外エンドポイント

エンドポイントが企業の境界外に配置されており、VPN または VPN 以外のソリューションを使用して企業に接続されている場合（ホーム オフィスまたはホテルからの Cisco Expressway モバイルおよびリモート アクセスなど）、Cisco Emergency Responder は発信者のロケーションを特定できません。さらに、システムで、発信者のロケーションに該当する PSAP にコールを送信できるように、適切な位置にゲートウェイが配置されている可能性はほとんどありません。

構外エンドポイントを 911 コール用に使用して企業を経由することを許可するか、許可しないかは、企業ポリシーの問題です。VPN または Cisco Expressway 経由でインターネットに接続しているエンドポイント向けのポリシーでは、911 コールを許可しないことを推奨します。それにもかかわらず、このようなユーザが 911 をコールした場合、ベストエフォート型のシステム応答では、オンサイト保安部隊、またはシステムのメイン サイトに近い大規模 PSAP のどちらかに、コールをルーティングします。

次のパラグラフは、構外のエンドポイントおよびユーザに対して緊急コール機能が保証されていないことを警告するために、ユーザに発行できる通知の例を示しています。

> *緊急コールは、設定されているサイト（オフィスなど）に設置されているデバイスから発信する必要があります。地域保安当局は、設定されたサイトから移動されたデバイスからの緊急コールには応答しない可能性があります。設定済みのサイトから離れているときに、このデバイスを緊急コールに使用する必要がある場合は、応答した公共安全機関に、現在のロケーションに関する具体的な情報を伝えられるように準備してください。旅行または在宅勤務時の緊急コールには、サイトに対してローカル側で設定されているデバイス（たとえば、ホテルの電話機や自宅の電話機など）を使用してください。*

また、Cisco Emergency Responder は Intrado V9-1-1（米国でほとんどすべての PSAP に到達できる緊急コール配信サービス）との統合をサポートします。Cisco Emergency Responder と Intrado V9-1-1 の組み合わせにより、企業の外部の IP フォンとソフトフォンは、ほとんどの Cisco IP Phones および Cisco IP Communicator に搭載されている表示画面、または Cisco Emergency Responder で提供されている Web ページを使用してロケーションを更新できます。構外ロケーションからの緊急コールは、Cisco Emergency Responder を経由して Intrado に配信され、その後、発信者のロケーションに該当する PSAP に配信されます。

テスト コール

企業テレフォニー システムでは、911 コール機能のテストは、初期インストール後だけでなく、予防手段として定期的に実施することを推奨します。

テストを実施する際は、次の推奨事項を参考にしてください。

- PSAP に連絡して、テスト前に許可を要請し、テスト実施者の連絡先情報を伝えます。
- 各コール発信時に、実際の緊急事態 *ではなく*、単なるテストであることを伝えます。
- 通話者の画面上に表示される ANI と ALI を確認します。
- コールがルーティングされた先の PSAP を確認します。
- エンドポイント上のコール所要時間タイマーを調べることによって、応答監視が受信されたことを確認します。アクティブ コール タイマーは、応答監視が正しく機能していることを示します。

共用ディレクトリ番号への PSAP コールバック

Cisco Emergency Responder は、緊急ロケーション識別番号（ELIN）に対するインバウンド コールのルーティングを処理します。911 コールの発信元の回線が、共用ディレクトリ番号である場合、PSAP コールバックにより、すべての共用ディレクトリ番号アピアランスが鳴ります。その後、共用アピアランスのいずれかがコールに応答できます。これは、911 コールが発信された電話機とはかぎりません。

Cisco Unified CM 11.5 以降のリリースでは、共有 DN への PSAP コールバックは、PSAP へのコールを行ったデバイスのみを呼び出します。Unified CM は、デバイスと回線の設定（不在転送、応答不可など）を上書きして、緊急サービスからのコールバックを配信します。

Cisco Emergency Responder の配置モデル

複数の Unified CM クラスタに基づく企業通信システムは、Cisco Emergency Responder（Emergency Responder）の機能のメリットを受けられます。

ここで使用する用語の詳細、および次の説明を理解するために必要な背景情報については、『*Cisco Emergency Responder Administration Guide*』を参照してください。「*Planning for Cisco Emergency Responder*」の章は特に重要です。このマニュアルは、次の Web サイトで入手できます。

https://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

（注）　Cisco Emergency Responder は、Cisco Unified Communications Manager Express（Unified CME）または Survivable Remote Site Telephony（SRST）をサポートしません。SRST 配置の場合は、サイト公開番号を使用して 911 コールを PSTN にルーティングするよう適切なダイヤルピアを設定してください。Unified CME は、E911 をネイティブにサポートします。

単一の Cisco Emergency Responder グループ

単一の Emergency Responder グループを配置して、複数の Unified CM クラスタからの緊急コールを処理できます。この設計の目標は、どの電話機からの緊急コールでも、その Cisco Emergency Responder グループにルーティングされるようにすることです。その Cisco Emergency Responder グループが ELIN を割り当て、エンドポイントのロケーションに基づいてコールを適切なゲートウェイにルーティングします。

単一の Cisco Emergency Responder グループを使用する 1 つの利点は、すべての ERL と ELIN が単一のシステムに設定されることです。単一の Cisco Emergency Responder グループがシステムのすべてのアクセス スイッチのポーリングを担当しているため、どのクラスタに登録されているエンドポイントでも、そのグループによって位置が確認されます。図 15-3 は、2 つの Unified CM クラスタとインターフェイスする単一の Cisco Emergency Responder グループを示しています。

図 15-3　2 つの Unified CM クラスタに接続されている単一の Cisco Emergency Responder グループ

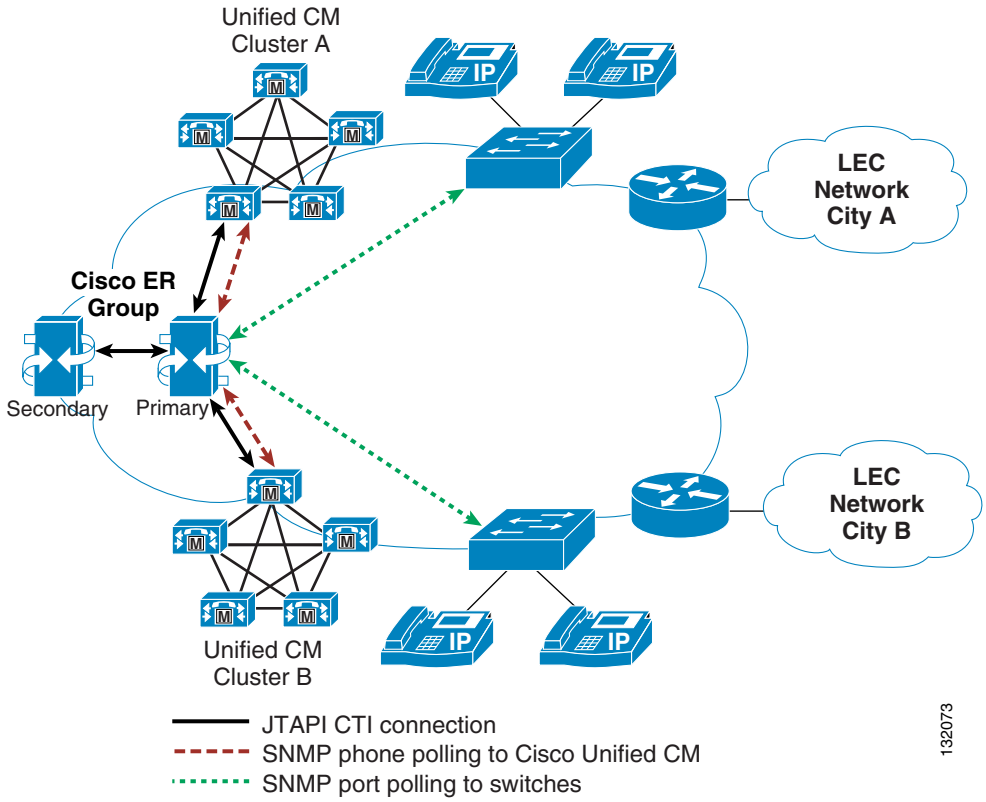


図 15-3 の単一の Cisco Emergency Responder グループは、次のコンポーネントとインターフェイスします。

- 各 Unified CM クラスタ（SNMP 経由）。それぞれに設定されているエンドポイントに関する情報を収集します。
- IP テレフォニー エンドポイントが接続されている企業のアクセス スイッチ（SNMP 経由）。エンドポイントのロケーションが IP サブネットに基づいて識別される場合、この接続は不要です。IP サブネットベースの ERL を設定する方法の詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「*Cisco Emergency Responder Configuration*」の章を参照してください。

  https://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html
- 各 Unified CM クラスタ（JTAPI 経由）。911 をダイヤルするエンドポイントのすべてに対して必要な呼処理を可能にする必要があります。その呼処理とは、発信側エンドポイントの ERL の識別、ELIN の割り当て、（発信側エンドポイントのロケーションに基づく）適切なゲートウェイへのコール リダイレクション、PSAP コールバック機能の処理などです。
- 各 Unified CM クラスタ（SNMP 経由）。アクセスポイントの情報を Cisco Wireless LAN Controller（WLC）から収集します。

Cisco Emergency Responder によって使用される JTAPI インターフェイスのバージョンは、Cisco Emergency Responder が接続される Unified CM ソフトウェアのバージョンによって決まります。システムの初期化時に、Cisco Emergency Responder は Unified CM クラスタに問い合わせて、適切な JTAPI テレフォニー サービス プロバイダー（TSP）をロードします。Cisco Emergency Responder サーバ上には 1 つのバージョンの JTAPI TSP しか存在できないため、単一の Cisco Emergency Responder グループがインターフェイスするすべての Unified CM クラスタが、同じバージョンの Unified CM ソフトウェアを実行する*必要があります*。

配置によっては、このソフトウェア バージョン要件によって問題が生じる場合があります。たとえば、Unified CM のアップグレード中は、クラスタが異なると、実行されているソフトウェアのバージョンが異なり、一部のクラスタが、Cisco Emergency Responder サーバ上で実行されているバージョンと互換性のないバージョンの JTAPI を実行していることがあります。このような場合、Cisco Emergency Responder グループの JTAPI バージョンとは異なるバージョンを実行しているクラスタからの緊急コールは、緊急番号の CTI ルート ポイントのコール転送設定によって提供されるコール処理を受けることができます。

複数の Unified CM クラスタに対して単一の Cisco Emergency Responder グループが適切であるかどうかを検討する場合は、次のガイドラインを適用してください。

- Unified CM のアップグレードは、緊急コールの数ができるだけ少ない許容可能なメンテナンス時間帯（たとえば、営業時間後や、システムの使用量が最小限のとき）に行う。
- クラスタの数とサイズから判断して、ソフトウェアのアップグレード中に異なるバージョンの JTAPI が使用される時間を最小限に抑えることができる場合にだけ、単一の Cisco Emergency Responder グループを使用する。

たとえば、8 台のサーバで構成される 1 つの大規模なクラスタと、2 台のサーバで構成される 1 つの小規模なクラスタを同時に配置し、単一の Cisco Emergency Responder グループとともに使用するとします。この場合、大規模なクラスタを最初にアップグレードすることを推奨します。これにより、アップグレードのメンテナンス時間帯に Cisco Emergency Responder サービスを使用できないユーザ（小規模なクラスタからサービスを受けるユーザ）の数を最小限に抑えられます。さらに、小規模なクラスタのユーザは、Cisco Emergency Responder に到達できない間、実際には、緊急コールの一時スタティック ルーティングによって適切にサービスを受けられます。これは、そのユーザが、その時間中に発信されるすべての非 ER コールに割り当てられている単一の ERL/ELIN によって識別されることが可能なためです。

複数の Cisco Emergency Responder グループ

マルチクラスタ システムをサポートするために、複数の Cisco Emergency Responder グループを配置することもできます。この場合は、各 ER グループが次のコンポーネントとインターフェイスします。

- Unified CM クラスタ。次の方式を使用します。
  - SNMP：クラスタに設定されているエンドポイントに関する情報を収集します。
  - JTAPI：適切なゲートウェイへの、またはローミング エンドポイントの場合は適切な Unified CM クラスタへの、コール リダイレクションに関連する呼処理を可能にします。
- その Cisco Emergency Responder グループの Unified CM に関連付けられているほとんどのエンドポイントの接続先となるアクセス スイッチ（SNMP 経由）。
- 各 Unified CM クラスタ（SNMP 経由）。アクセスポイントの情報を Cisco Wireless LAN Controller（WLC）から収集します。

この方法を使用すると、Unified CM クラスタが、異なるバージョンのソフトウェアを実行できます。これは、各クラスタが、別の Cisco Emergency Responder グループとインターフェイスするためです。

エンドポイントがネットワーク上のさまざまな場所をローミングし、Cisco Emergency Responder がその電話機をトラッキングできるようにするには、Cisco Emergency Responder グループを 1 つの Cisco Emergency Responder クラスタに設定する必要があります。Cisco Emergency Responder クラスタおよびグループの詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「*Planning for Cisco Emergency Responder*」の章を参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

図 15-4 は、Cisco Emergency Responder クラスタリングの背後にある基本的な概念を表すトポロジの例を示しています。

図 15-4　　複数の Cisco Emergency Responder グループ

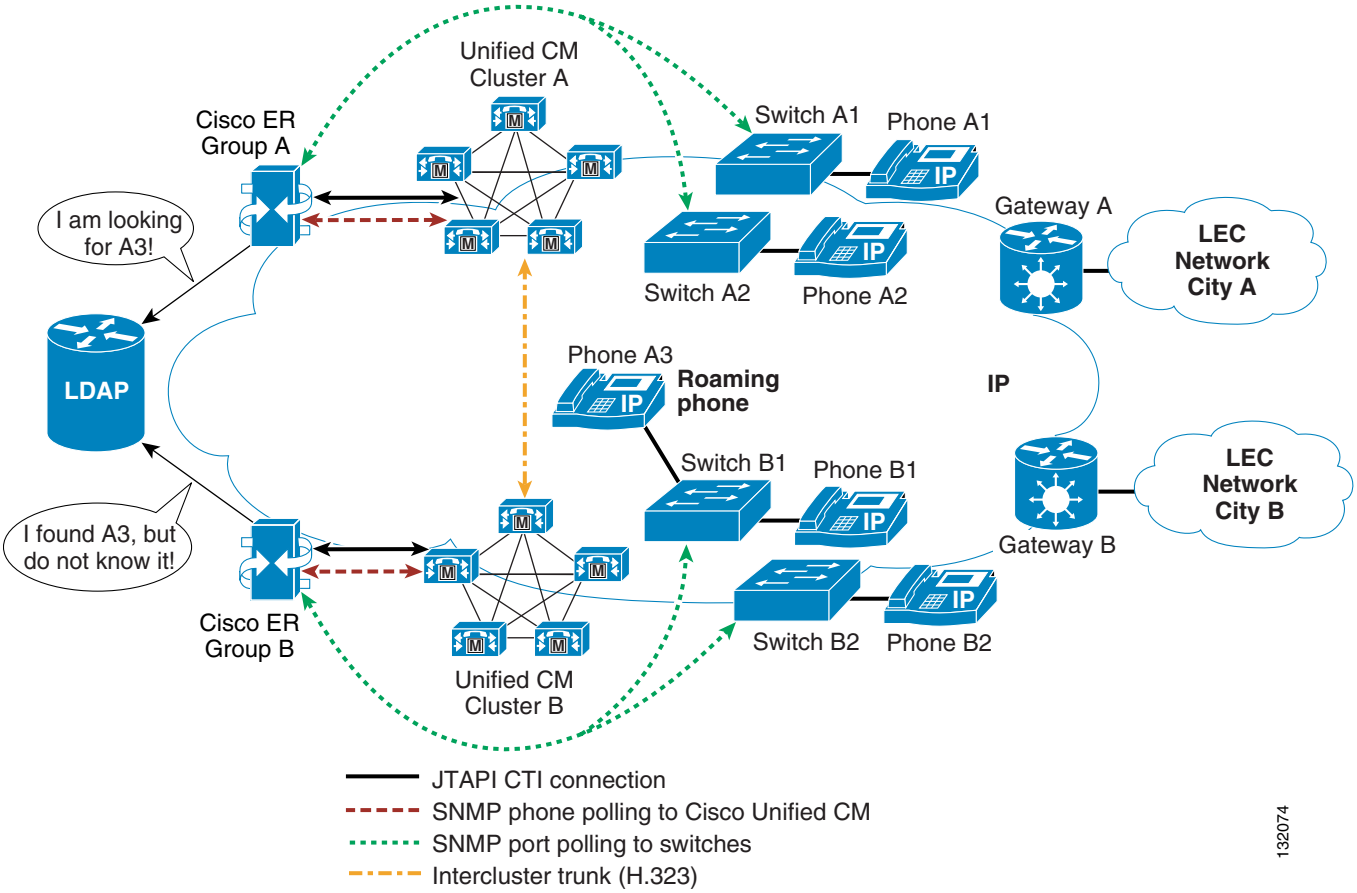


図 15-4 は、次のトポロジを示しています。

- Cisco Emergency Responder グループ A は、Unified CM クラスタ A とインターフェイスして、スイッチ A1 および A2 にアクセスする。このグループは、Unified CM クラスタ A に登録されているすべてのエンドポイントのホーム Cisco Emergency Responder グループであると見なされます。
- 同様に、Cisco Emergency Responder グループ B は、Unified CM クラスタ B とインターフェイスして、スイッチ B1 および B2 にアクセスする。このグループは、Unified CM クラスタ B に登録されているすべてのエンドポイントのホーム Cisco Emergency Responder グループであると見なされます。

Cisco Emergency Responder グループのトラッキング ドメイン内のエンドポイント移動

エンドポイントが、同じホーム Cisco Emergency Responder グループによって制御されるアクセス スイッチ間を移動する場合、そのエンドポイントの緊急コール処理は、単一の Unified CM クラスタを使用する配置で行われる処理と同じです。たとえば、アクセス スイッチ A1 と A2 の間を移動するエンドポイントは、Unified CM クラスタ A に登録されたままで、移動前も移動後もそのエンドポイントのロケーションは Cisco Emergency Responder グループ A によって決定されます。Unified CM クラスタ A によるエンドポイント検出と、Cisco Emergency Responder のスイッチ A2 によるエンドポイントのロケーション特定の両方で、エンドポイントは引き続き Cisco Emergency Responder グループ A の完全な制御下にあります。したがって、エンドポイントは位置未確認の電話機と見なされません。

Cisco Emergency Responder クラスタのさまざまなトラッキング ドメイン間のエンドポイント移動

Cisco Emergency Responder クラスタは、実質的に、ロケーション情報を共有する Cisco Emergency Responder グループのコレクションです。各グループは、アクセス スイッチ上または IP サブネット内で検出するすべてのエンドポイントのロケーションを共有します。

また、Cisco Emergency Responder グループは、Cisco Emergency Responder グループのトラッキング ドメイン内（スイッチまたは IP サブネット内）で位置を確認できないが、そのグループに関連付けられている Unified CM クラスタに登録されていることがわかっているエンドポイントに関する情報も共有します。このようなエンドポイントは、*位置未確認*と見なされます。

異なる Cisco Emergency Responder グループによってモニタされるアクセス スイッチ間をエンドポイントがローミングする場合、それらのグループは、エンドポイントのロケーションに関する情報を交換できるように、1 つの Cisco Emergency Responder クラスタに設定される必要があります。たとえば、エンドポイント A3 が Unified CM クラスタ A に登録されているが、Cisco Emergency Responder グループ B によって制御されているアクセス スイッチに接続されている場合、Cisco Emergency Responder グループ A は、エンドポイント A3 が Unified CM クラスタ A に登録されていることを認識しますが、サイト A のどのスイッチもエンドポイント A3 の位置を確認することはできません。したがって、エンドポイント A3 は Cisco Emergency Responder グループ A によって*位置未確認*と見なされます。

これに対し、Cisco Emergency Responder グループ B は、モニタ対象のスイッチの 1 つで、エンドポイント A3 の存在を検出します。エンドポイント A3 は、Unified CM クラスタ B に登録されていないため、*不明*なエンドポイントとして Cisco Emergency Responder データベースを介してアドバタイズされます。

2 つの Cisco Emergency Responder グループは、複製されたデータベース テーブルを介して通信しているため、Cisco Emergency Responder グループ B の*不明*なエンドポイント A3 が Cisco Emergency Responder グループ A の*位置未確認*のエンドポイント A3 と同じであることがわかります。

Cisco Emergency Responder グループ A の [位置未確認の電話機（Unlocated Phone）] ページには、このエンドポイントの MAC アドレスが、リモート Cisco Emergency Responder グループ（この場合は Cisco Emergency Responder グループ B）とともに表示されます。

Cisco Emergency Responder クラスタ内の緊急コール ルーティング

Cisco Emergency Responder クラスタリングは、1 つの Unified CM クラスタと 1 つの Cisco Emergency Responder で構成されるペア間で緊急コールをリダイレクトできるようにするルート パターンにも依存します。詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「*Creating Route Patterns for Inter-Cisco Emergency Responder Group Communications*」の項を参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

エンドポイント A3 が緊急コールを発信した場合、コール シグナリング フローは次のようになります。

1. エンドポイント A3 が、処理のために緊急コール ストリングを Unified CM クラスタ A に送信します。
2. Unified CM クラスタ A が、リダイレクションのためにコールを Cisco Emergency Responder グループ A に送信します。
3. Cisco Emergency Responder グループ A が、エンドポイント A3 の位置を Cisco Emergency Responder グループ B のトラッキング ドメイン内であると確認し、Unified CM クラスタ B を指すルート パターンにコールをリダイレクトします。
4. Unified CM クラスタ A がコールを SIP トランクまたはクラスタ間トランクを介して Unified CM クラスタ B に送信します。
5. Unified CM クラスタ B が、リダイレクションのためにコールを Cisco Emergency Responder グループ B に送信します。
6. Cisco Emergency Responder グループ B がエンドポイント A3 のロケーションに関連付けられている ERL と ELIN を（発信者番号に基づいて）識別し、コールを Unified CM クラスタ B にリダイレクトします。発信者番号は、エンドポイント A3 の ERL に関連付けられている ELIN に変換されます。着信者番号は、コールが適切なゲートウェイにルーティングされるように変更されます。
7. Unified CM クラスタ B が、Cisco Emergency Responder グループ B から入手した新しい着信番号情報に従ってコールをルーティングします。
8. Unified CM クラスタ B が、ゲートウェイを通じてコールを緊急 PSTN ネットワークに送信します。

（注）　ステップ 6 の ERL と ELIN の一致処理は、911 へのコールを行ったエンドポイントの発信者番号に基づいて行われます。SIP トランクまたはクラスタ間トランクが発信者番号を（完全な +E.164 番号などに）変更すると、グループ B の Emergency Responder は、トランク上の発信者番号を、アクセス スイッチ Cisco Discovery Protocol（CDP）ネイバーから取得したディレクトリ番号と一致させることができません。したがって、SIP トランクまたはクラスタ間トランクで転送される緊急コールは、発呼側トランスフォーメーションの処理を受けないようにする必要があります。

Cisco Emergency Responder の WAN 配置

Cisco Emergency Responder は、WAN を介したクラスタリングを使用して、2 つのメイン サイトをサポートします。各サイトに Emergency Responder サーバを 1 つずつインストールし、一方のサーバをパブリッシャとして、もう一方のサーバをサブスクライバとして設定します。Emergency Responder パブリッシャはプライマリ Unified CM CTI Manager とともに配置し、Emergency Responder サブスクライバはセカンダリ Unified CM CTI Manager とともに配置する必要があります。いずれかの Emergency Responder サーバとリモート接続しているすべての Unified CM サーバは、両方の Emergency Responder サーバから 80 ミリ秒のラウンドトリップ時間（RTT）の範囲内に配置されている必要があります。Emergency Responder パブリッシャと Emergency Responder サブスクライバも、相互に 80 ms RTT 内に配置されている必要があります。Cisco Emergency Responder サーバ間で必要な最小帯域幅は 1.544 Mbps です。

Unified CM のネイティブ緊急コール ルーティングによる緊急コール ルーティング

正確なロケーション識別を必要とするが、サイトが 1 つだけ、または識別する必要のあるロケーションが少数である顧客は、Cisco Unified Communications Manager のネイティブ緊急コール ルーティング機能を使用できます。ネイティブ緊急コール ルーティング機能を使用すると、管理者は緊急ロケーション識別番号（ELIN）をデバイス プール レベルまたはデバイス レベルで定義できます。このため、デバイスのロケーションは、Public Safety Answering Point（PSAP）で特定および識別できます。

Cisco Unified CM のネイティブ緊急コール ルーティングは、次の機能を提供します。

- 静的デバイス割り当てまたはデバイス プール割り当てに基づく ELIN アソシエーション
- コールバックを目的とした、発信側電話機への ELIN の動的アソシエーション
- モバイル デバイスをネイティブ緊急コール ルーティングでトラッキングするために使用されるデバイス モビリティ グループ
- 適切な ELIN への発信者番号の自動置換
- 緊急コールを完了するための適切なゲートウェイへの緊急コールのルーティング

911 ネイティブ緊急コール ルーティング サービスの設計に関する考慮事項

Cisco Unified CM ネイティブ緊急コール ルーティング サービスを使用する緊急コール ルーティング プランを設計する際には、ビルディング内の緊急ロケーションの境界に関して、特別に考慮する必要があります。緊急サービスが緊急事態にあるユーザの位置付けにかかる時間を短縮できるように、緊急ロケーションは、物理境界または論理境界を使用して識別できるロケーションにしておく必要があります。物理境界または論理境界の例としては、ビルディングの単一のフロア、ラボ、オフィス、またはフロア位置インジケータ（1 階の西側など）があります。

ネイティブ緊急コール ルーティングの設計では、ELIN を定義してデバイスまたはデバイス プールに割り当てる必要がありますが、ネイティブ緊急コール ルーティング機能では、管理者は ERL 情報を定義して ELIN に関連付けることはできません。特定の ELIN 用の ERL 定義は、Cisco Unified CM の外部で行い、ローカル PSAP にアップロードする必要があります。アップロードの手順は、E911 サービスを設定する際に地域通信事業者により提供された指示に従う必要があります。

Cisco Emergency Responder の配置と同様に、ネイティブ緊急コール ルーティングも、同じロケーションから緊急サービスに対する複数の一意な同時発生コールをサポートできます。ネイティブ緊急コール ルーティングでは、単一の緊急ロケーションに関連付けられる ELIN のプールを作成できます。定義できるロケーションの数は、個々の緊急ロケーション（ELIN）グループに割り当てられた ELIN の数に基づきます。ネイティブ緊急コール ルーティングは、最大 100 の ELIN をサポートします。対象となる配置で、ロケーションあたり 1 つの同時発生コールのみを必要とする場合、システムは、100 の一意な緊急ロケーション グループをサポートできます。対象となる配置で、同じロケーションからの 2 つの同時発信者をトラッキングする能力が必要である場合、管理者は、単一の緊急ロケーション（ELIN）グループに対して 2 つの ELIN を定義する必要があります。単一のロケーションに対して 2 つの ELIN が必要である場合、Unified CM は 50 ロケーションをサポートできます（2 ELIN * 50 ERL = 100 ELIN）。1 つのロケーションからの同時かつ一意に識別される発信者をサポートするためにさらに多くの ELIN を使用すると、定義可能なロケーションの総数が少なくなります。次の公式を使用すると、ERL からの同時かつ一意な発信者の数に基づいて、定義できるロケーションの最大数を確認できます。

100/（ERL あたり同時かつ一意な発信者の数）= 最大 ERL 数

ELIN は、各緊急ロケーション（ELIN）グループに対して同じである必要はありません。1 つの ERL が非常に多くのユーザをカバーする場合、緊急ロケーション（ELIN）グループは、4 人の同時かつ一意の緊急発信者をサポートするために、4 つの ELIN を含むことがあります。ただし、同じビルディングに、定常的に勤務する社員が少ない大きなラボ フロアまたは保管倉庫がある場合は、1 つの ELIN のみを緊急ロケーション（ELIN）グループに割り当てるだけで済むことがあります。

PSAP が発信者にコールバックして追加情報を入手する必要がある場合、コールはコールの発信元である ELIN を使用して Unified CM に折り返されます。折り返しコールが正しくルーティングされるようにするために、インバウンド着信者番号が Unified CM で定義されている ELIN に一致するよう、ダイヤル プランを構成する必要があります。インバウンド トランクが着信側の最後の 5 桁のみを配信する場合、管理者は ELIN に一致するようにトランスレーション パターンを含めて収集した数値を拡張する必要があります。折り返しコールが適切に機能するようにするために、着信者番号は Unified CM で定義された ELIN 番号に正確に一致する必要があります。ELIN には顧客の DID 範囲の任意の番号を割り当てることができますが、使用するコール トランスレーション パターンの数を可能な限り少なくするために、連続した番号を使用することをシスコでは推奨しています。

ALI フォーマット

マルチクラスタ構成では、単一の Cisco Emergency Responder グループに定義されている ERL と ELIN の物理ロケーションが、複数の電話会社の管轄地区にまたがることがあります。これにより、複数の LEC 用のレコードを含む共通ファイルから、さまざまな電話会社用のレコードを抽出する必要が生じることがあります。

Cisco Emergency Responder は、この情報を、National Emergency Number Association（NENA）2.0、2.1、および 3.0 のフォーマットに準拠する ALI レコードでエクスポートします。ただし、多くのサービス プロバイダーは NENA 標準を使用しません。そのような場合は、ALI Formatting Tool（AFT）を使用して、Cisco Emergency Responder によって生成された ALI レコードを、サービス プロバイダーによって指定されたフォーマットに準拠するように変更できます。これにより、サービス プロバイダーは、再フォーマットされたファイルを使用して、ALI データベースを更新できます。

ALI Formatting Tool（AFT）では、次の機能を実行できます。

- レコードを選択し、ALI フィールドの値を更新する。AFT では、ALI フィールドを編集し、さまざまなサービス プロバイダーの要件を満たすようにカスタマイズできます。これにより、サービス プロバイダーは、再フォーマットされた ALI ファイルを読み取り、そのファイルを使用して ELIN レコードを更新できます。
- 複数の ALI レコードに対するバルク更新を実行する。一括更新（バルク更新）機能を使用すると、選択したすべてのレコードに対して共通の変更を適用できます。
- エリア コード、シティ コード、または 4 桁のディレクトリ番号に基づいて ALI レコードを選択してエクスポートする。たとえば、あるエリア コードのすべての ALI レコードを選択してエクスポートすることにより、各サービス プロバイダーのすべての ELIN レコードにすばやくアクセスできるため、複数のサービス プロバイダーを簡単にサポートできます。

AFT の柔軟性を利用して、単一の Cisco Emergency Responder グループから、複数の ALI データベース フォーマットで ALI レコードをエクスポートできます。2 つの LEC の管轄地区内に複数のサイトがある Unified CM クラスタに対して単一の Cisco Emergency Responder グループがサービスを提供する場合、基本的な方法は次のとおりです。

1. Cisco Emergency Responder からの ALI レコード ファイル出力を標準の NENA フォーマットで入手します。このファイルには、複数の LEC に宛てられたレコードが含まれています。
2. 必要な ALI 形式ごとに元のファイルの 1 つのコピーを作成します（LEC ごとに 1 つのコピー）。
3. 最初の LEC（たとえば、LEC-A）の AFT を使用して、NENA 形式のファイルのコピーをロードし、他の LEC に関連付けられているすべての ELIN のレコードを削除します。削除する情報は、通常、NPA（またはエリア コード）によって識別できます。
4. 結果として生成されたファイルを、LEC-A に必要な ALI 形式で保存し、適宜ファイル名を付けます。
5. 各 LEC に対してステップ 3 と 4 を繰り返します。

ALI Formatting Tools の詳細については、次の Web サイトで入手可能なオンライン マニュアルを参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

この URL にリストされていない LEC の場合、スプレッドシート プログラムや標準のテキスト エディタなど、標準のテキスト ファイル編集ツールを使用して Emergency Responder からの出力をフォーマットできます。

ディレクトリ統合とアイデンティティ管理

改訂日：2018 年 3 月 1 日

アイデンティティ管理は、どのアプリケーションにも必要な基本概念です。アイデンティティ管理では、個々のプリンシパルの管理とこれらのプリンシパルの認証および認可を行います。従来、各アプリケーションは、アイデンティティ管理を個々に処理していました。このため、ユーザは個々のアプリケーションに対して認証を実施しなければいけませんでした。アイデンティティ管理、認証、認可を集中化することにより、シングル サインオン（SSO）などのサービスを提供することで、ユーザ エクスペリエンスを大幅に向上できます。

アイデンティティ管理の集中化の最初のステップは、エンタープライズのプリンシパルに関する情報のストレージを一元化することです。これらの一元化された企業全体のデータストアは、一般的にディレクトリとして知られています。

ディレクトリ（電話帳）は、多数の読み取りや検索、および随時の書き込みや更新用に最適化される特殊なデータベースです。ディレクトリには、一般に、社員の情報、ユーザ特権、グループ メンバーシップなど、頻繁に変更されないデータが企業ネットワーク上に保存されます。

ディレクトリは拡張可能です。つまり、ディレクトリに保存された情報のタイプを変更し、拡大できます。「*ディレクトリ スキーマ*」という語は、保存されている情報のタイプ、そのコンテナ（または属性）、およびユーザやリソースとの関係を定義します。

Lightweight Directory Access Protocol（LDAP）は、ディレクトリに保存されている情報にアクセスし、変更するための標準方式をアプリケーションに提供します。この機能により、企業は、すべてのユーザ情報を、複数のアプリケーションで利用できる単一リポジトリに集中化させることができます。追加、移動、および変更が簡単なので、保守コストも大幅に削減されます。

この章では、Cisco Unified Communication Manager（Unified CM）に基づく Cisco Unified Communications システムを社内 LDAP ディレクトリと統合する場合の、設計上の主な原則について説明しています。この章の構成は、次のとおりです。

- ディレクトリ統合とは（16-3 ページ）

  ここでは、一般的な企業の IT 部門における社内 LDAP ディレクトリとの統合に関して、さまざまな要件を分析します。

- Unified Communications エンドポイントのディレクトリ アクセス（16-4 ページ）

  ここでは、Cisco Unified Communications エンドポイントのディレクトリ アクセスを有効にする技術的なソリューションについて説明し、そのソリューションに基づく設計上のベストプラクティスを示します。

- Unified CM とのディレクトリ統合（16-7 ページ）

  ここでは、LDAP 同期機能や LDAP 認証機能などを含む、Cisco Unified CM でのディレクトリ統合に関して、技術的なソリューションについて説明し、設計上の考慮事項を示します。

- VCS 登録エンドポイントのディレクトリ統合（16-34 ページ）

  ここでは、Cisco TelePresence Video Communication Server（VCS）に登録されたビデオ エンドポイントのディレクトリ アクセスを有効にする技術的なソリューションを簡単に紹介します。
- アイデンティティ管理アーキテクチャの概要（16-35 ページ）

  ここでは、アイデンティティ管理アーキテクチャについて説明します。
- シングル サインオン（SSO）（16-36 ページ）

  ここでは、SAML 2.0 シングル サインオン（SSO）の概要を示します。
- 承認フレームワーク（16-46 ページ）

  ここでは、Cisco Unified CM で利用できる Oauth 承認サービスについて説明します。

この章で説明する考慮事項は、Cisco Unified CM とそれにバンドルされているアプリケーション（Cisco エクステンション モビリティ、Cisco Unified Communications Manager Assistant、WebDialer、Bulk Administration Tool、および Real-Time Monitoring Tool）に適用されます。

Cisco Unity については、次の Web サイトで入手可能な『*Cisco Unity Design Guide*』、および『*Cisco Unity Data and the Directory*』、『*Active Directory Capacity Planning*』、『*Cisco Unity Data Architecture and How Cisco Unity Works*』の各ホワイト ペーパーを参照してください。

https://www.cisco.com

この章の変更点

表 16-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

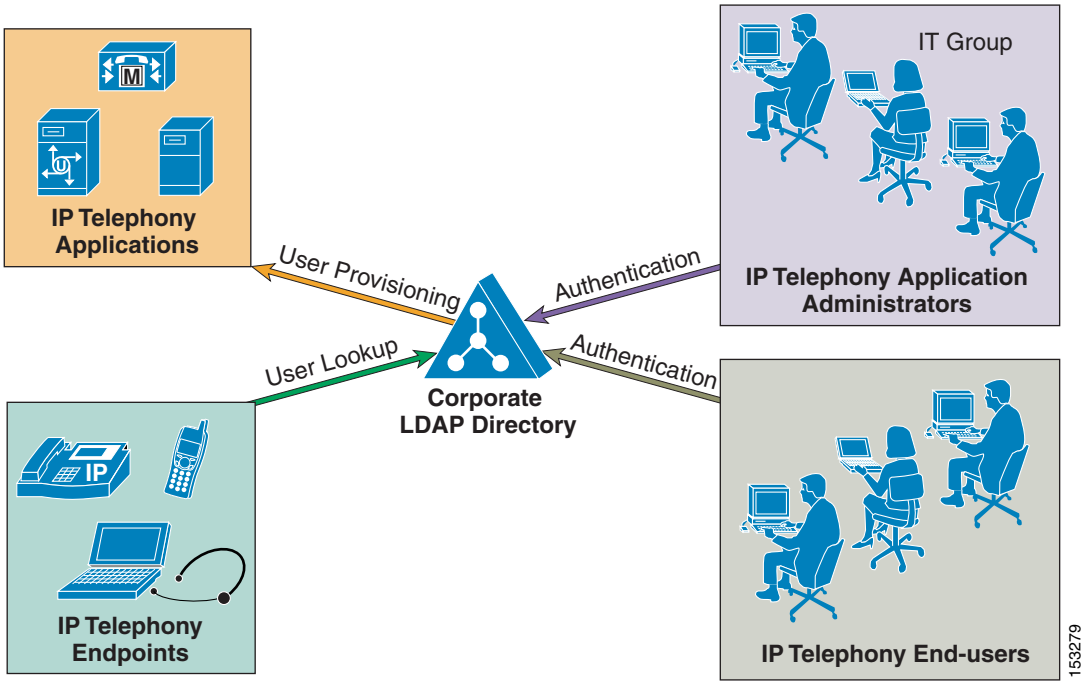
表 16-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
ユーザ データ サービス（UDS）を使用したディレクトリ アクセス	Cisco ユーザ データ サービス（UDS）を使用した Unified Communications エンドポイントのディレクトリ アクセス（16-6 ページ）	2018 年 3 月 1 日
アイデンティティ管理	アイデンティティ管理アーキテクチャの概要（16-35 ページ）	2018 年 3 月 1 日
シングル サインオン（SSO）	Cisco Jabber の SSO（16-45 ページ） SSO の設計上の検討事項（16-45 ページ）	2018 年 3 月 1 日
認証と OAuth 2.0	承認フレームワーク（16-46 ページ）	2018 年 3 月 1 日

ディレクトリ統合とは

音声アプリケーションと社内 LDAP ディレクトリとの統合は、多くの企業の IT 部門にとって一般的な作業です。ただし、統合の正確な範囲は企業によって異なるため、図 16-1 に示すように、1 つ以上の具体的かつ独立した要件として表すことができます。

図 16-1　　ディレクトリ統合のさまざまな要件



たとえば、1 つの一般的な要件は、IP 電話またはその他の音声エンドポイントやビデオ エンドポイントからユーザ ルックアップ（「個人別電話帳」サービスと呼ばれることもあります）を有効にし、ユーザがディレクトリで番号を検索した後に、連絡先に迅速にダイヤルできるようにすることです。

もう 1 つの要件は、社内ディレクトリからアプリケーションのユーザ データベースを、ユーザに自動的に提供することです。この方法により、社内ディレクトリの変更のたびにコア ユーザ情報を手動で追加、削除、または修正する必要がなくなります。

一般に、社内ディレクトリ クレデンシャルを使用して、音声アプリケーションやビデオ アプリケーションのエンド ユーザと管理者を認証することも必要です。ディレクトリ認証を有効にすることで、IT 部門は 1 つのログイン機能を提供し、さまざまな企業アプリケーションに対して各ユーザが保持する必要のあるパスワードの数を減らすことができます。

表 16-2 に示すように、Cisco Unified Communications システムに関係する場合、*ディレクトリ アクセス*という用語は、Cisco Unified Communications エンドポイントのユーザ ルックアップの要件を満たすメカニズムおよびソリューションを意味します。また、*ディレクトリ統合*という用語は、ユーザ プロビジョニングおよび（エンド ユーザと管理者の両方の）認証の要件を満たすメカニズムおよびソリューションを意味します。

表 16-2　ディレクトリの要件とシスコのソリューション

要件	シスコのソリューション	Cisco Unified CM の機能
エンドポイントのユーザ ルックアップ	ディレクトリ アクセス	Cisco Unified IP Phone Services SDK Cisco ユーザ データ サービス（UDS）
ユーザ プロビジョニング	ディレクトリ統合	LDAP 同期
Unified Communications エンド ユーザの認証	ディレクトリ統合	LDAP 認証
Unified Communications アプリケーション管理者の認証	ディレクトリ統合	LDAP 認証

この章では、これ以降、Cisco Unified CM に基づく Cisco Unified Communications システムで、これらの要件にどのように対処するかについて説明します。

（注）「*ディレクトリ統合*」という用語については、管理ポリシーおよびセキュリティ ポリシーを集中化するために、Microsoft Active Directory ドメインにアプリケーション サーバを追加する機能といった解釈もあります。Cisco Unified CM は、カスタマイズした組み込みオペレーティング システムで実行するアプライアンスであり、Microsoft Active Directory ドメインに追加できません。Cisco Unified CM のサーバ管理は、Cisco Real-Time Monitoring Tool（RTMT）によって行われます。アプリケーションに合わせた強力なセキュリティ ポリシーが組み込みオペレーティング システム内にすでに実装されています。

Unified Communications エンドポイントのディレクトリ アクセス

この項では、Cisco Unified Communications エンドポイント（Cisco Unified IP Phone など）からユーザ ルックアップを実行するように、LDAP 準拠のディレクトリ サーバへの社内ディレクトリ アクセスを設定する方法について説明します。Unified CM やその他の Unified Communications アプリケーションがユーザ プロビジョニングおよび認証のために社内ディレクトリに統合されているかどうかに関係なく、この項で説明しているガイドラインが適用されます。

ディスプレイ画面を持つ Cisco Unified IP Phone では、ユーザが電話機の Directories ボタンを押すと、ユーザ ディレクトリを検索できます。IP Phone は、ハイパーテキスト転送プロトコル（HTTP）を使用して、要求を Web サーバに送信します。Web サーバからの応答には、電話機が解釈して表示する特定の Extensible Markup Language（XML）オブジェクトが含まれています。

デフォルトでは、Cisco Unified IP Phone は、Unified CM の組み込みデータベースに対してユーザ ルックアップを実行するように設定されます。ただし、社内 LDAP ディレクトリでルックアップを実行するように、この設定を変更できます。変更した場合、電話機は HTTP 要求を外部 Web サーバに送信します。このサーバはプロキシとして動作し、要求を LDAP 照会に変換します。その後、その LDAP 照会は社内ディレクトリによって処理されます。LDAP 応答は、Web サーバによって XML オブジェクトにカプセル化され、HTTP を使用して電話機に返信されて、エンド ユーザに伝えられます。

図 16-2 では、Unified CM が社内ディレクトリに統合されていない配置において、このメカニズムを示しています。このシナリオでは、Unified CM がメッセージ交換にかかわっていないことに注意してください。図 16-2 の右側に表示されている Unified CM Web ページの認証メカニズムは、ディレクトリ ルックアップの設定とは関係ありません。

図 16-2　Cisco Unified IP Phone Services SDK を使用する Cisco Unified IP Phone のディレクトリ アクセス

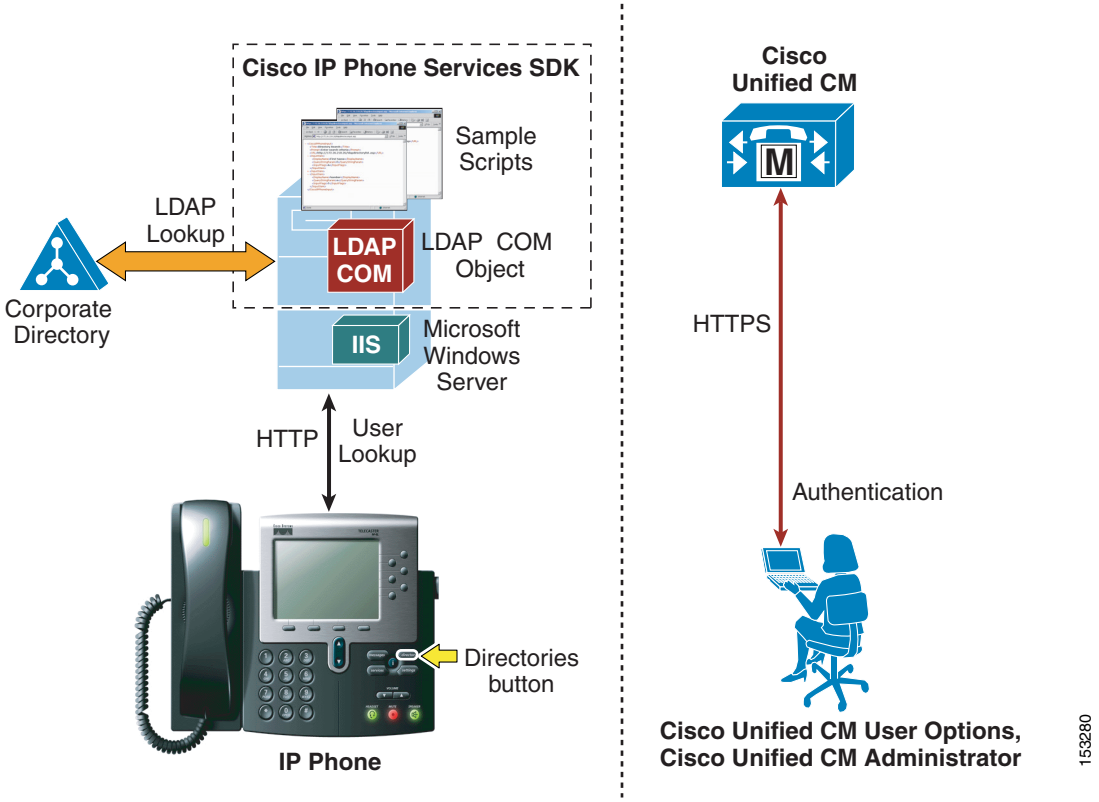


図 16-2 に示す例では、Web サーバのプロキシ機能は、Cisco Unified IP Phone Services ソフトウェア開発キット（SDK）に組み込まれている Cisco LDAP Search コンポーネント オブジェクト モデル（COM）サーバによって提供されます。次の URL の Cisco DevNet（シスコの開発者コミュニティ）から最新の Cisco Unified IP Phone Services SDK をダウンロードできます。

https://developer.cisco.com/site/devnet/home/index.gsp

IP Phone Services SDK は、IIS 4.0 以降を実行する Microsoft Windows Web サーバにはインストールできますが、Unified CM サーバにはインストールできません。SDK には、単純なディレクトリ ルックアップ機能を提供するサンプル スクリプトが入っています。

IP Phone Services SDK を使用する社内ディレクトリ ルックアップ サービスを設定するには、次の手順を実行します。

手順 1　社内 LDAP ディレクトリを指すようにサンプル スクリプトのいずれかを修正するか、SDK に付属の『LDAP Search COM Programming Guide』を使用して独自のスクリプトを作成します。

手順 2　Unified CM で、外部 Web サーバ上のスクリプトの URL を指すように URL Directories パラメータ（[System] > [Enterprise Parameters]）を設定します。

手順 3　変更を有効にするために電話機をリセットします。

（注）　ユーザのサブセットだけにサービスを提供する場合は、[Enterprise Parameters] ページではなく、[Phone Configuration] ページ内で URL Directories パラメータを直接設定します。

まとめると、Cisco Unified IP Phone Services SDK によるディレクトリ アクセスには、次の設計上の考慮事項が適用されます。

- ユーザ ルックアップは、LDAP 準拠の社内ディレクトリに対してサポートされる。
- Microsoft Active Directory に照会する場合、スクリプトがグローバル カタログ サーバを指すようにし、スクリプト設定でポート 3268 を指定することにより、グローバル カタログに対してルックアップを実行できる。この方法では、通常はルックアップが高速化します。グローバル カタログに記載されているユーザの属性がすべてではないことに注意してください。詳細については、Microsoft Active Directory のマニュアルを参照してください。
- この機能が有効であっても Unified CM に影響はなく、LDAP ディレクトリ サーバに最小限の影響しか及ばない。
- SDK に付属のサンプル スクリプトでは、最小限のカスタマイズだけが可能である（たとえば、返送されたすべての番号の前に番号ストリングを付けられる）。もっと高度な操作のためには、カスタム スクリプトを作成する必要があり、スクリプトの作成に役立つプログラミング ガイドが SDK に付属しています。
- この機能は、社内ディレクトリに対する Unified CM ユーザのプロビジョニングまたは認証を必要としない。

Cisco ユーザ データ サービス（UDS）を使用した Unified Communications エンドポイントのディレクトリ アクセス

ここでは、前のセクションで説明した Web サービスの代わりに UDS を使用した、ユーザ データにアクセスするためのエンドポイントのディレクトリ アクセスのメカニズムとベスト プラクティスについて説明します。ユーザ データ サービス（UDS）API は、ユーザのデバイス、加入サービス、スピード ダイヤルをはじめ、Unified Communication 設定データベース内の各ユーザ リソースおよびエンティティに対する認証済みアクセスを提供する、REST ベースの操作を集めたものです。

現在のエンドポイント（CE ソフトウェアを実行するすべてのエンドポイントを含む）は、ユーザがエンドポイントで検索機能を呼び出すときはいつでも、UDS REST ベースのディレクトリ検索メソッドに直接アクセスして検索結果を取得します。UDS の検索メソッドから返された結果は、エンドポイントのディスプレイに表示されます。UDS LDAP プロキシ機能が使用されない限り、UDS の検索機能でリストされるのは、Unified CM データベース内にあるディレクトリ エントリだけです。UDS LDAP プロキシ機能を使用する場合、エンドポイントが UDS を介して Cisco Unified CM にディレクトリ情報を要求することに変わりはありませんが、結果は、設定済みの外部 LDAP ディレクトに UDS サービスによって要求されてから、UDS 要求の結果としてエンドポイントに返されます。

Unified CM とのディレクトリ統合

この項では、社内 LDAP ディレクトリに対するユーザ プロビジョニングと認証を考慮した、Cisco Unified CM でのディレクトリ統合のメカニズムおよびベスト プラクティスについて説明します。この項では、次の項目について説明します。

- Cisco Unified Communications Directory のアーキテクチャ（16-7 ページ）

  ここでは、Unified CM ユーザ関連アーキテクチャの概要を示します。

- LDAP 同期（16-11 ページ）

  ここでは、LDAP 同期の機能について説明し、この機能の配置に関する設計上のガイドラインを Microsoft Active Directory に関する追加の考慮事項と共に示します。

- LDAP 認証（16-23 ページ）

  ここでは、LDAP 認証の機能について説明し、この機能の配置に関する設計上のガイドラインを Microsoft Active Directory に関する追加の考慮事項と共に示します。

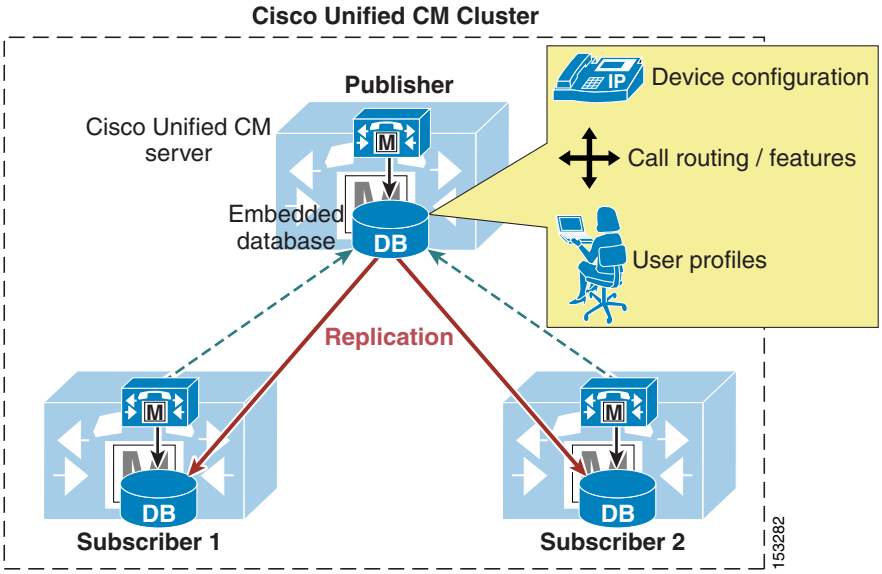
サポートされる LDAP ディレクトリの一覧については、次の Web サイトで入手可能な『*System Configuration Guide for Cisco Unified Communications Manager*』の最新版を参照してください。

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

Cisco Unified Communications Directory のアーキテクチャ

図 16-3 は、Unified CM クラスタの基本アーキテクチャを示しています。組み込みデータベースには、デバイス関連データ、コール ルーティング、機能のプロビジョニング、およびユーザ プロファイルなど、すべての設定情報が保存されます。データベースは CM クラスタ内のすべてのサーバ上に存在し、パブリッシャ サーバからすべてのサブスクライバ サーバに自動的に複製されます。

図 16-3　Cisco Unified CM のアーキテクチャ



デフォルトでは、Unified CM Administration Web インターフェイスを介してすべてのユーザを手動でパブリッシャ データベースにプロビジョニングします。Cisco Unified CM には、次の 2 つのユーザ タイプがあります。

- エンド ユーザ：実在の人間でかつ対話形式のログインに関連付けられているすべてのユーザ。このカテゴリには、すべての Unified Communications ユーザのほか、User Groups and Roles 設定（以前のバージョンの Unified CM にある Cisco Multilevel Administration 機能に相当）を使用する場合の Unified CM 管理者も含まれます。
- アプリケーション ユーザ：Cisco Unified Communications の他の機能またはアプリケーション（Cisco Attendant Console、Cisco Unified Contact Center Express、Cisco Unified Communication Manager Assistant など）に関連付けられているすべてのユーザ。これらのアプリケーションは Unified CM に対して認証する必要がありますが、この内部「ユーザ」は対話形式のログインを行わず、単にアプリケーション間の内部通信だけを処理します。

表 16-3 では、Unified CM データベースにデフォルトで作成されるアプリケーション ユーザのリストを、それらのユーザが使用される機能またはアプリケーションと共に示しています。Cisco Unified Communications の他のアプリケーションを統合する場合に、追加のアプリケーション ユーザを手動で作成できます（たとえば、Cisco Attendant Console の **ac** アプリケーション ユーザ、Cisco Unified Contact Center Express の **jtapi** アプリケーション ユーザなど）。

表 16-3　Unified CM のデフォルトのアプリケーション ユーザ

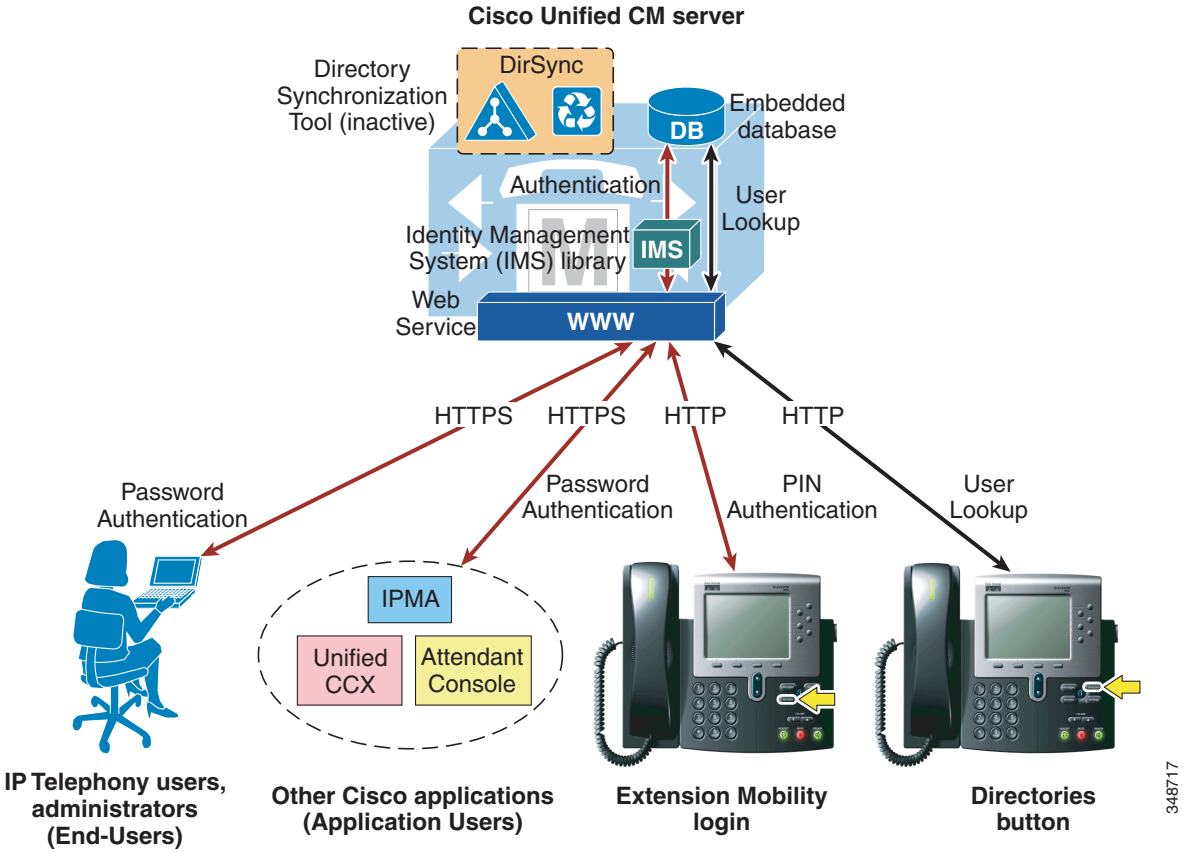
アプリケーション ユーザ	使用される機能またはアプリケーション
CCMAdministrator	Unified CM Administration（デフォルトは「スーパー ユーザ」）
CCMQRTSecureSysUser	Cisco Quality Reporting Tool
CCMQRTSysUser	
CCMSysUser	Cisco エクステンション モビリティ

表 16-3　Unified CM のデフォルトのアプリケーション ユーザ(続き)

アプリケーション ユーザ	使用される機能またはアプリケーション
IPMASecureSysUser	Cisco Unified Communications Manager Assistant
IPMASysUser	
WDSecureSysUser	Cisco WebDialer
WDSysUser	

これらの考慮事項に基づいて、図 16-4 に、ルックアップ、プロビジョニング、認証などのユーザ関連操作に対する Unified CM でのデフォルト動作を示します。

図 16-4　Unified CM のユーザ関連操作に対するデフォルト動作



エンド ユーザは、HTTPS 経由で [Unified CM User Options] ページにアクセスし、ユーザ名およびパスワードで認証します。ユーザ グループと役割によって管理者として設定されている場合、エンド ユーザは同じクレデンシャルで Unified CM Administration のページにもアクセスできます。

同様に、シスコの他の機能とアプリケーションは、それぞれのアプリケーション ユーザに関連付けられたユーザ名およびパスワードで、HTTPS 経由で Unified CM に対して認証します。

HTTPS メッセージによって伝送される認証確認は、Unified CM の Web サービスにより、Identity Management System（IMS）という内部ライブラリにリレーされます。デフォルト設定では、IMS ライブラリは、組み込みデータベースに対してエンド ユーザとアプリケーション ユーザの両方を認証します。このように、Unified Communications システムにおける「現実の」ユーザと内部アプリケーション アカウントの両方が、Unified CM に設定されたクレデンシャルを使用して認証されます。

エンド ユーザは、IP Phone からエクステンション モビリティ サービスにログインするときに、ユーザ名と数値パスワード（PIN）で認証することもできます。この場合、認証確認は HTTP 経由で Unified CM に伝送されますが、やはり Web サービスにより IMS ライブラリにリレーされ、IMS ライブラリは組み込みデータベースに対してクレデンシャルを認証します。

さらに、Directories ボタンを介して Unified Communications エンドポイントによって実行されるユーザ ルックアップでは、HTTP 経由で Unified CM の Web サービスと通信し、組み込みデータベースのデータにアクセスします。

エンド ユーザとアプリケーション ユーザの区別の重要性は、社内ディレクトリとの統合が必要な場合に明らかになります。前の項で説明したように、この統合は次の 2 つの独立したプロセスによって実現されます。

- LDAP 同期

  このプロセスでは、Unified CM の Cisco Directory Synchronization（DirSync）という内部ツールを使用して、社内 LDAP ディレクトリから多数のユーザ属性を（手動または定期的に）同期します。この機能がイネーブルの場合、ユーザは Unified CM 管理 GUI を介して、ローカル ユーザのプロビジョニングに加えて社内ディレクトリから自動的にプロビジョニングされます。この機能はエンド ユーザだけに適用され、アプリケーション ユーザは独立したままで、引き続き Unified CM Administration インターフェイスを介してプロビジョニングされます。要約すると、エンド ユーザは社内ディレクトリで定義され、Unified CM データベースに同期されますが、アプリケーション ユーザは Cisco Unified CM データベースに保存されるだけで、社内ディレクトリで定義する必要はありません。

- LDAP 認証

  このプロセスは、LDAP の標準的な Simple_Bind 操作を使用して、IMS ライブラリが社内 LDAP ディレクトリに対して LDAP 同期エンド ユーザのユーザ クレデンシャルを認証できるようにします。この機能がイネーブルの場合、LDAP 同期されたエンド ユーザは社内ディレクトリに対して認証される一方、アプリケーションのユーザ パスワードとローカル エンド ユーザのパスワードは引き続き Unified CM データベースに対してローカルで認証されます。Cisco エクステンション モビリティの PIN も引き続きローカルで認証されます。

Unified CM データベースに対して内部でアプリケーション ユーザを維持および認証すると、社内 LDAP ディレクトリの可用性とは無関係に、これらのアカウントを使用して Unified CM と通信するすべてのアプリケーションと機能に対して復元性が提供されます。

Cisco エクステンション モビリティの PIN も Unified CM データベース内で維持されます。これは、これらの PIN はリアルタイム アプリケーションの必須部分であり、リアルタイム アプリケーションは社内ディレクトリの応答性に依存しないようにする必要があるためです。

次の 2 つの項では、LDAP 同期と LDAP 認証についてさらに詳しく説明し、両方の機能に関して設計上のベスト プラクティスを示します。

（注）　Unified Communications エンドポイントのディレクトリ アクセス（16-4 ページ）の項で説明したように、外部 Web サーバで Cisco Unified IP Phone Services SDK を設定することにより、エンドポイントからのユーザ ルックアップを社内ディレクトリに対して実行することもできます。

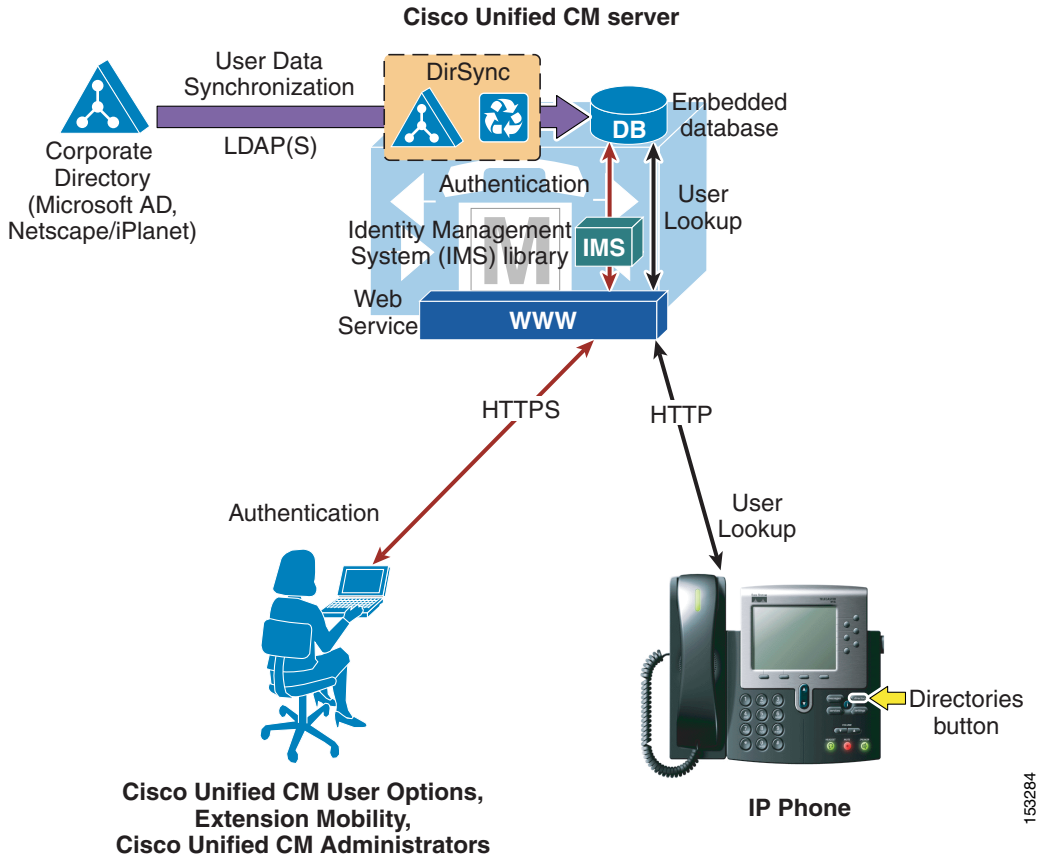
LDAP 同期

Unified CM を社内 LDAP ディレクトリに同期すると、管理者は Unified CM データ フィールドをディレクトリ属性にマッピングすることにより、ユーザを容易にプロビジョニングできるようになります。LDAP ストアに保持されている重要なユーザ データは、スケジュールまたはオンデマンド ベースで Unified CM データベース内の対応する適切なフィールドにコピーされます。社内 LDAP ディレクトリのステータスは、中央リポジトリのままとなります。Unified CM は、ユーザ データを保存するための統合データベースを備え、またユーザ アカウントおよびデータを作成して管理するための Web インターフェイスを、Unified CM Administration 内に備えています。LDAP 同期を有効にすると、ローカル データベースは引き続き使用され、追加のローカル エンド ユーザ アカウントを作成できます。エンドユーザ アカウントは、LDAP ディレクトリのインターフェイスおよび Unified CM 管理 GUI で管理できます。（図 16-5 を参照）。アプリケーション ユーザのアカウントは、Unified CM Administration Web インターフェイスのみで作成と管理を実行できます。

ユーザ アカウント情報は、LDAP ディレクトリから Unified CM パブリッシャ サーバにあるデータベースにインポートされます。LDAP ディレクトリからインポートされた情報は、Unified CM から変更できません。Cisco Unified Communications に固有の追加のユーザ情報は、Unified CM によって管理され、ローカル データベースだけに保存されます。たとえば、デバイスとユーザのアソシエーション、スピード ダイヤル、自動転送設定、およびユーザ PIN はすべて Unified CM が管理するデータの例であり、社内 LDAP ディレクトリには存在しません。次に、ユーザ データは組み込みデータベース同期メカニズムによって、Unified CM パブリッシャ サーバからサブスクライバ サーバに伝達されます。

LDAP ディレクトリから同期されたユーザ情報は、ユーザ情報を Unified CM でローカルで編集できるよう、ローカル ユーザ情報に変換できます。ローカル エンド ユーザは、Unified CM Administration GUI を使用して手動で追加できます。LDAP 同期信号中、ローカル エンド ユーザはアクティブ LDAP ユーザに変わり、同じユーザ ID のユーザが LDAP で見つかった場合、ローカルで設定済みのデータはディレクトリのデータに置き換えられます。

図 16-5　　ユーザ データ同期の有効化



LDAP 同期をアクティブにすると、一度に 1 つのタイプの LDAP ディレクトリだけをクラスタ用にグローバルに選択できます。また、LDAP ディレクトリ ユーザの 1 つの属性が選択されて [Unified CM User ID] フィールドにマッピングされます。Unified CM はデータへのアクセスに標準 LDAPv3 を使用します。

Cisco Unified CM は、標準属性からデータをインポートします。ディレクトリ スキーマの拡大は必要ありません。表 16-4 に、Unified CM の各フィールドへのマッピングに使用できる属性を示します。[Unified CM User ID] フィールドにマッピングされるディレクトリ属性のデータは、そのクラスタのすべてのエントリ内で一意のものである必要があります。[Unified CM UserID] フィールドにマッピングされる属性はディレクトリに格納される必要があり、**sn** 属性はデータと一緒に格納される必要があります。そうしないと、このインポート処理時にこれらのレコードはスキップされます。エンドユーザ アカウントのインポート中に使用するプライマリ属性が Unified CM データベースのいずれかのアプリケーション ユーザと一致する場合、そのユーザは LDAP ディレクトリからインポートされません。

表 16-4 では、LDAP ディレクトリから対応する Unified CM ユーザ フィールドにインポートされた属性を示していて、またこれらのフィールド間のマッピングについて説明しています。Unified CM ユーザ フィールドの中には、複数の LDAP 属性の 1 つからマッピングされるものもあります。

表 16-4　同期化された LDAP 属性と対応する Unified CM フィールド名

Unified CM のユーザ フィールド	Microsoft Active Directory	Microsoft Active Directory アプリケーション モード（ADAM）または Active Directory ライトウェイト ディレクトリ サービス（AD LDS）	Oracle DSEE および Sun	OpenLDAP およびその他の LDAPv3 タイプ
ユーザ ID（User ID）	*次のいずれかになります。* sAMAccountName mail employeeNumber telephoneNumber userPrincipalName	*次のいずれかになります。* uid mail employeeNumber telephoneNumber userPrincipalName	*次のいずれかになります。* uid mail employeeNumber telephonePhone	*次のいずれかになります。* uid mail employeeNumber telephonePhone
名（First Name）	givenName	givenName	givenName	givenName
ミドル ネーム（Middle Name）	*次のいずれかになります。* middleName initials	*次のいずれかになります。* middleName initials	initials	initials
姓（Last Name）	sn	sn	sn	sn
マネージャ ID（Manager ID）	manager	manager	manager	manager
部署名（Department）	department	department	departmentnumber	departmentnumber
電話番号（Phone Number）	*次のいずれかになります。* telephoneNumber ipPhone	*次のいずれかになります。* telephoneNumber ipPhone	telephoner	telephonenumber
メール ID（Mail ID）	*次のいずれかになります。* mail sAMAccountName	*次のいずれかになります。* mail uid	*次のいずれかになります。* mail uid	*次のいずれかになります。* mail uid
objectGUID	objectGUID	objectGUID	適用されない	適用されない
OCSPrimaryUser アドレス（OCSPrimaryUser Address）	msRTCSIP-PrimaryUser Address	適用されない	適用されない	適用されない
役職（Title）	title	title	Title	title
自宅電話番号（Home Phone Number）	homePhone	homePhone	Homephone	hometelephonenumber
携帯電話番号（Mobile Phone Number）	mobile	mobile	Mobile	Mobiletelephonenumber

表 16-4　同期化された LDAP 属性と対応する Unified CM フィールド名（続き）

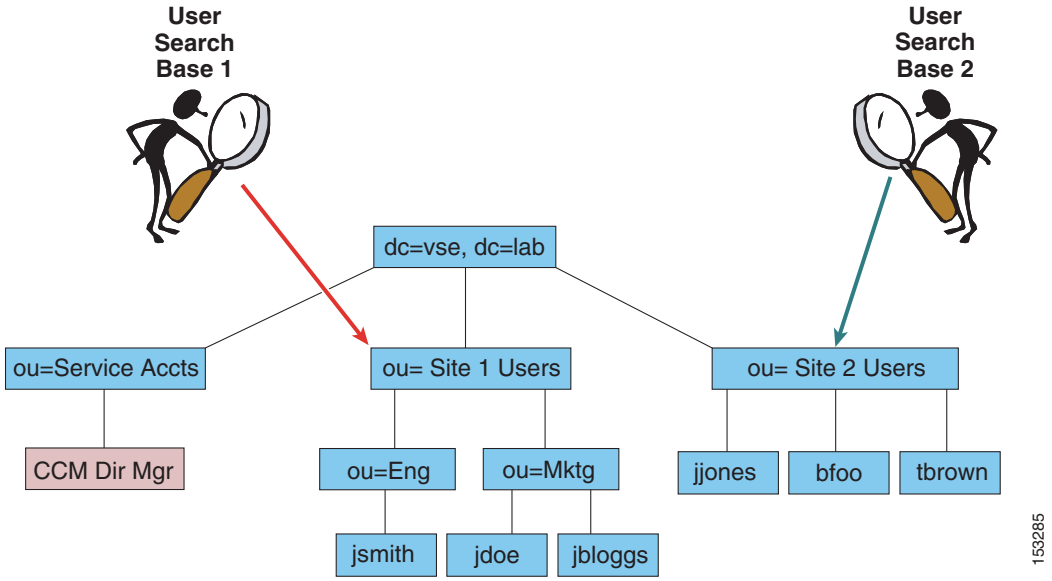
Unified CM のユーザ フィールド	Microsoft Active Directory	Microsoft Active Directory アプリケーション モード（ADAM）または Active Directory ライトウェイト ディレクトリ サービス（AD LDS）	Oracle DSEE および Sun	OpenLDAP およびその他の LDAPv3 タイプ
ポケットベル番号（Pager Number）	pager	pager	Pager	Pagertelephonenumber
ディレクトリ URI（Directory URI）	*次のいずれかになります。* msRTCSIP-PrimaryUserAddress mail none	*次のいずれかになります。* mail none	*次のいずれかになります。* mail none	*次のいずれかになります。* mail none
表示名（Display Name）	displayName	displayName	displayName	displayName

ディレクトリ属性とローカル ユーザ属性の直接マッピングに加えて、同期されたユーザの他の特性は、LDAP ディレクトリ同期アグリーメントの設定によって決まります。LDAP 同期によって作成されたユーザのアクセス制御グループ メンバーシップは、LDAP ディレクトリ構成設定で直接設定されます。これ以上の機能は、選択した機能グループ テンプレートによって決まります。LDAP ディレクトリ同期アグリーメントにおける機能グループ テンプレートの選択はオプションです。機能グループ テンプレートを使用すると、管理者は、ユーザの特性を定義できます（ホーム クラスタ選択、IM and Presence 機能、モビリティ機能、サービス プロファイル、ユーザ プロファイルなど）。ユーザ プロファイルを使用すると、管理者は、Unified CM で LDAP 同期されたユーザのディレクトリ電話番号を自動作成するために対象となるユニバーサル回線テンプレートを定義できます。

同期は、Serviceability Web ページで有効にする Cisco DirSync というプロセスによって実行されます。このプロセスを有効にすることで、システムに 1 ～ 20 件の同期アグリーメントを設定できます。80,000 人以上のユーザが同期される場合、この数は 10 に減少します。アグリーメントでは、LDAP ツリー内で Unified CM がインポートするユーザ アカウントの検索を開始する場所となる検索ベースを指定します。Unified CM は、特定の同期アグリーメントについて検索ベースで指定したドメインの領域に存在するユーザだけをインポートできます。

図 16-6 は、2 つの同期アグリーメントを示しています。一方の同期アグリーメントでは、User Search Base 1 を指定し、ユーザ jsmith、jdoe、jbloggs をインポートします。もう一方の同期アグリーメントでは、User Search Base 2 を指定し、ユーザ jjones、bfoo、tbrown をインポートします。CCMDirMgr アカウントは、ユーザ検索ベースで指定した場所の下位に存在しないので、インポートされません。ユーザを LDAP ディレクトリの構造に編成すると、その構造を使用して、どのユーザ グループをインポートするかを制御できます。この例では、単一の同期アグリーメントを使用してドメインのルートを指定することもできましたが、その検索ベースでは Service Accts もインポートしていたと考えられます。検索ベースではドメイン ルートを指定する必要はなく、ツリーのどの場所でも指定できます。

図 16-6　ユーザ検索ベース



データを Unified CM データベースにインポートするために、LDAP Manager Distinguished Name として設定で指定されたアカウントを使用して、システムが LDAP ディレクトリへのバインドを実行し、データベースの読み取りがこのアカウントで実行されます。Unified CM のログインのために、LDAP ディレクトリでアカウントが使用可能である必要があります。ユーザ検索ベースで指定したサブツリー内のすべてのユーザ オブジェクトの読み取り可能な権限を持つ、固有のアカウントを作成することをお勧めします。同期アグリーメントでは、そのアカウントがドメイン内の任意の場所に存在できるように、アカウントの完全認定者名を指定します。図 16-6 の例では、CCMDirMgr が同期に使用するアカウントです。

アカウントのインポートは、LDAP Manager Distinguished Name アカウントの権限を使用して制御できます。この例では、ou=Eng への読み取りアクセスはできるが ou=Mktg への読み取りアクセスはできないようにこのアカウントを制限した場合、Eng の下位にあるアカウントだけがインポートされます。

同期アグリーメントには、複数のディレクトリ サーバを指定して冗長性を実現する機能があります。同期の試行時に使用するディレクトリ サーバを 3 つまで、順序付きのリストにして設定に指定できます。これらのサーバでの試行が、リストの最後まで順に行われます。どのディレクトリ サーバも応答しない場合、同期には失敗しますが、設定済みの同期スケジュールに従って再試行されます。

同期のメカニズム

同期アグリーメントでは、同期を開始する時刻を指定し、再同期の期間を時間、日、週、月のいずれかの単位（最小値は 6 時間）で指定します。同期アグリーメントは、特定の時刻に 1 回だけ実行するように設定することもできます。

Unified CM パブリッシャ サーバで同期を初めて有効にすると、社内ディレクトリに存在するユーザ アカウントが Unified CM データベースにインポートされます。そして、その後のプロセスに従って、既存の Unified CM エンド ユーザ アカウントがアクティブになってデータが更新されるか、新しいエンド ユーザ アカウントが作成されます。

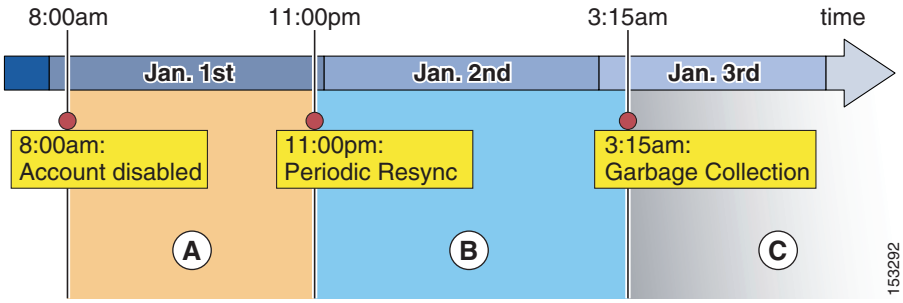
1. エンド ユーザ アカウントがすでに Unified CM データベースに存在するときに同期アグリーメントを設定した場合、以前に LDAP から同期されたすべての既存のアカウントは Unified CM で非アクティブとマークされます。同期アグリーメントの設定で、Unified CM UserID への LDAP データベース属性のマッピングを指定します。同期中に LDAP データベースのアカウントが既存の Unified CM アカウントと一致すると、その Unified CM アカウントは再びアクティブとマークされます。
2. 同期の完了後、アクティブに設定されなかった LDAP 同期アカウントは、ガーベッジ コレクション プロセスの実行時に Unified CM から永続的に削除されます。ガーベッジ コレクションは、午前 3 時 15 分の定時に自動的に実行されるプロセスで、設定はできません。
3. 後で社内ディレクトリに変更を加えると、スケジューリングされた次回の同期期間に、完全な再同期として Microsoft Active Directory から同期が行われます。これに対して、Sun ONE のディレクトリ製品は、ディレクトリに変更が加えられると差分同期を実行します。次の項では、2 つのシナリオのそれぞれの例を示します。

（注）　ユーザを LDAP から Unified CM データベースに同期した後で同期設定を削除すると、その設定によってインポートされたユーザには、データベース内で非アクティブのマークが付きます。その後、これらのユーザはガーベッジ コレクションによって削除されます。

Active Directory でのアカウント同期

図 16-7 は、LDAP 同期と LDAP 認証の両方を有効にした Unified CM 配置について、イベントのスケジュールの例を示しています。再同期は、毎日午後 11 時に設定されています。

図 16-7　Active Directory での変更の伝達



最初の同期の後、アカウントの作成、削除、または無効化は、図 16-7 に示すスケジュールに従って、次の手順で説明するように Unified CM に伝達されます。

1. 1 月 1 日の午前 8 時に、AD でアカウントを無効にするか削除します。これ以降、期間 A 中は、Unified CM が認証を AD にリダイレクトするため、このユーザのパスワード認証（たとえば、[Unified CM User Options] ページ）は失敗します。ただし、PIN は Unified CM データベースに保存されているため、PIN 認証（たとえば、エクステンション モビリティ ログイン）は今までどおり成功します。

2. 定期的な再同期が 1 月 1 日午後 11 時にスケジュールされています。このプロセス中に、Unified CM がすべてのアカウントを検証します。AD で無効にするか削除したアカウントは、この時点で Unified CM データベースでは非アクティブとしてタグ付けされます。1 月 1 日の午後 11 時より後に、アカウントが非アクティブとマークされると、Unified CM による PIN 認証とパスワード認証は両方とも失敗します。
3. アカウントのガーベッジ コレクションは毎日午前 3 時 15 分の定時に発生します。このプロセスは、24 時間以上非アクティブとマークされたレコードの Unified CM データベースからユーザ情報を永続的に削除します。この例では、1 月 2 日の午前 3 時 15 分に実行するガーベッジ コレクションでは、アカウントが非アクティブになってまだ 24 時間が経過していないので、アカウントを削除しません。したがって、アカウントは 1 月 3 日の午前 3 時 15 分に削除されます。この時点で、ユーザ データは Unified CM から永続的に削除されます。

期間 A の開始時にアカウントを AD で作成していた場合、そのアカウントは期間 B の開始時に実行される定期的な再同期で Unified CM にインポートされ、Unified CM ですぐにアクティブになります。

Sun ONE でのアカウント同期

Sun ONE 製品は差分同期アグリーメントをサポートし、Microsoft Active Directory とは異なる同期スケジュールを使用します。同期には、多くの LDAP 実装でサポートされている永続検索メカニズムが使用されます。図 16-8 では、LDAP 同期と LDAP 認証の両方を有効にした Unified CM 配置について、この同期スケジュールの例を示しています。

図 16-8　Sun ONE での変更の伝播

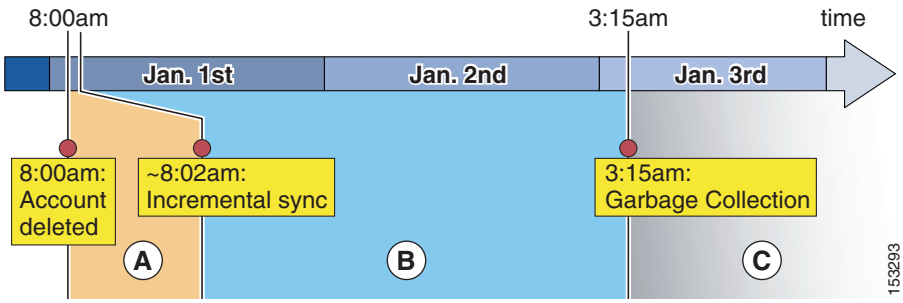


図 16-8 の例は、次の手順から構成されます。

1. 1 月 1 日の午前 8 時にアカウントが社内ディレクトリから削除され、これにより、差分更新データが LDAP サーバから Unified CM に送信されます。Unified CM は、データに対応するコピーを非アクティブに設定します。LDAP 認証が設定されているので、LDAP サーバがレコードを削除するとすぐに、ユーザはパスワードによるログインができなくなります。また、Unified CM レコードが非アクティブとマークされると、PIN をログインに使用できません。
2. 期間 B 中は、ユーザのレコードは非アクティブですが、まだ Unified CM に存在します。
3. 1 月 2 日の午前 3 時 15 分にガーベッジ コレクションが実行されるときは、レコードが非アクティブになってまだ 24 時間が経過していません。データは 1 月 3 日の期間 C の開始時まで Unified CM データベースに残り、ガーベッジ コレクション プロセスがこの日の午前 3 時 15 分に再び実行され、レコードが 24 時間以上にわたって非アクティブであったことを確認します。その結果、レコードはデータベースから永続的に削除されます。

ディレクトリで新規に作成したアカウントは、差分更新データによって同様に Unified CM に同期し、差分更新データが受信されるとすぐに使用できます。

自動回線作成

LDAP 同期中に作成されたユーザに対して、Unified CM は自動的にディレクトリ番号を作成できます。これらの自動生成されたディレクトリ番号は、ディレクトリで見つかった情報のうちディレクトリで見つかった電話番号に適用されるマスクに基づいて定義されたものに基づくか、または LDAP 同期アグリーメントで定義されたディレクトリ番号プールから取得されます。マスクが同期アグリーメントで定義されるている場合は、可変長 +E.164 ディレクトリ番号を生成できるようにするため、次のルールが適用されます。

- マスクを空白のままにしておくと、Unified CM はすべての数字と先頭の「+」（存在する場合）をディレクトリから取得します。
- X は、マスクのワイルドカード文字として使用されます。
- ワイルドカードは、数字および「+」に一致します。
- マスクのワイルドカードは、右側から使用されます。
- マスクの使用されないワイルドカードは削除されます。

表 16-5 に、いくつかの例を示します。

表 16-5　マスクに基づいて LDAP 電話番号からディレクトリ番号を作成する例

LDAP の番号	マスク	結果
14085551234		14085551234
14085551234	+XXXXXXXXXX	+14085551234
14085551234	+XXXXXXXXXXXXXXXXX	+14085551234
14085551234	XXXX	1234
+14085551234		+14085551234
+14085551234	+XXXXXXXXXXXXXXXXX	+14085551234
+496100123	+XXXXXXXXXXXXXXXXX	+496100123

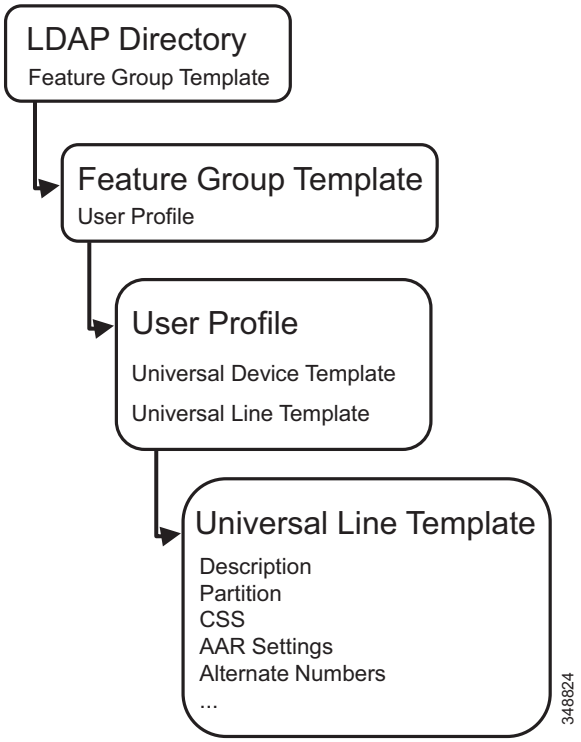
LDAP からの情報に基づいてディレクトリ番号を作成する代わりに、新しいユーザのディレクトリ番号は、事前に定義された番号プールから取得することもできます。各プールは開始番号と終了番号によって決まります。ディレクトリ番号プールは、+E.164 番号をサポートします。最大 5 つのプールを定義できます。番号は、最初のプールのすべての番号が割り当てられるまで、最初のプールから割り当てられます。その後、番号の割り当てには次のプールの番号を使用し始めます。

自動回線作成は、次の*両方*の条件を満たしたときにのみ有効になります。

- 機能グループ テンプレートがディレクトリ同期アグリーメントで割り当てられる。**および**
- ユニバーサル回線テンプレートが機能グループ テンプレートで選択したユーザ プロファイルで選択されている。

図 16-9 に、自動回線作成の回線レベル設定を定義するために必要な構成要素の階層を示します。

図 16-9　LDAP ディレクトリ設定、機能グループ テンプレート、ユーザ プロファイル、およびユニバーサル回線テンプレートの関係



最終的に、ユニバーサル回線テンプレートは、対応する LDAP 同期定義によって追加されたユーザに対して自動的に作成されるすべてのディレクトリ番号の特性を定義します。

設計上の考慮事項

ユニバーサル回線テンプレートで定義されたコーリング サーチ スペースによって、自動生成されたディレクトリ番号のいずれかを使用するデバイスのサービス クラスが決まります。これは、同じ LDAP 同期アグリーメントによって作成されたすべてのディレクトリ番号が同じサービス クラスを共有すること、およびそのために、複数のサイトや複数のサービス クラスのディレクトリ番号が自動生成される必要がある場合は、複数の LDAP 同期アグリーメント（サイトやサービス クラスごとに 1 つ）が必要なことを意味します。これらの同期アグリーメントごとに、個別の LDAP フィルタを定義する必要があります。それぞれのフィルタは、サイト固有およびサービス クラス固有のユーザ グループのいずれかに属するユーザで完全一致します。サイトおよびサービス クラスに基づくグループ メンバーシップが少数の LDAP 属性で明示的にエンコードされない限り（それがカスタム属性内の場合でも）、LDAP 属性からサイトやサービス クラス グループへのこのようなマッピングは困難なものになることがあります。また、サポートされる LDAP アグリーメントの最大数は限られています。これは、自動的にディレクトリ番号を作成できるユーザ グループの数を制限します。

ディレクトリ番号の自動作成は、LDAP ディレクトリ同期中に作成されたユーザにのみ適用されます。特定の LDAP 同期アグリーメントのユニバーサル回線テンプレートを追加、変更、または更新しても、既存のユーザのディレクトリ番号は作成されず、既存のディレクトリ番号の設定は変更されません。

ユニバーサル回線テンプレートを使用すると、管理者は未登録の接続先へのコール転送を定義できます。その際、ボイスメールを転送先として選択するか、または明示的な接続先を定義できます。WAN の障害時に登録済みのエンドポイントからリモート サイト内のエンドポイントに到達するには、リモート サイトの電話機に対する未登録の接続先へのコール転送を、リモート電話機の PSTN エイリアス（+E.164 番号）に設定する必要があります。これは、ユニバーサル回線テンプレート設定では実現できません。割り当てられたディレクトリ番号（および該当する場合は適用されたマスク）に基づいて未登録の接続先へのコール転送を設定する必要が生じるためです。

社内グループのサポート

Jabber クライアントが Microsoft Active Directory 内のグループを検索できるようにするため、Active Directory からエンド ユーザを同期するように Unified CM を設定するだけでなく、Active Directory に定義された配布グループを含めるように設定できます。社内グループの同期は、データ ソースとして Microsoft Active Directory を使用する場合のみサポートされます。Active Directory ライトウェイト ディレクトリ サービス（AD LDS）またはその他の社内ディレクトリではサポートされません。社内グループの同期は、Unified CM の LDAP ディレクトリ設定で有効になります。社内グループの最大数は 15,000 で、グループあたりのメンバーの最大数は 100 です。グループおよびメンバーを Cisco Unified CM Administration で追加または変更することはできませんが、Active Directory から同期されたグループは [ユーザ管理（User Management）]/[ユーザ設定（User Settings）]/[ユーザ グループ（User Group）] メニューで確認できます。

グループ メンバーごとに、次の情報が Jabber クライアントで使用できます。

- 表示名（Display Name）
- ユーザ ID（User ID）
- 役職（Title）
- 電話番号（Phone number）
- メール ID（Mail ID）

セキュリティに関する考慮事項

アカウントのインポート中は、LDAP ディレクトリから Unified CM データベースに、パスワードも PIN もコピーされません。Unified CM で LDAP 認証が有効でなく、シングル サインオンが使用されていない場合、エンド ユーザのパスワードは Unified CM Administration を使用して管理されます。パスワードと PIN は、暗号化形式で Unified CM データベースに保存されます。PIN は常に Unified CM で管理されます。LDAP ディレクトリ パスワードを使用してエンド ユーザを認証する場合は、LDAP 認証（16-23 ページ）の項を参照してください。

Unified CM および LDAP サーバで Secure LDAP（SLDAP）を有効にすることにより、Unified CM パブリッシャ サーバとディレクトリ サーバ間の接続を保護できます。Secure LDAP を使用すると、Secure Socket Layer（SSL）接続で LDAP 送信ができます。Unified CM Platform Administration 内で LDAP サーバを Tomcat 信頼ストアに追加することにより、Secure LDAP を有効にできます。詳細な手順については、https://www.cisco.com から入手できる Unified CM の製品マニュアルを参照してください。SLDAP を有効にする方法については、LDAP ディレクトリ ベンダーのドキュメンテーションを参照してください。

LDAP 同期に関する設計上の考慮事項

Cisco Unified CM で LDAP 同期を配置する場合は、設計と実装に関する次のベスト プラクティスに従ってください。

- 社内ディレクトリ内で特定のアカウントを使用し、Unified CM 同期アグリーメントがそのディレクトリに対して接続および認証できるようにする。目的の検索ベース内にあるすべてのユーザ オブジェクトを最低限の「読み取り」権限を設定し、期限切れにならないようにパスワードを設定した状態で、Unified CM 専用のアカウントを使用することを推奨します。ディレクトリ内のこのアカウントのパスワードは、Unified CM 内のアカウントのパスワード設定と同期し続ける必要があります。サービス アカウントのパスワードがディレクトリ内で変更された場合は、必ず Unified CM でアカウント設定をアップデートしてください。
- 所定のクラスタにあるすべての同期アグリーメントは、同じ LDAP サーバ ファミリと統合する必要がある。
- 複数のアグリーメントが同時に同じ LDAP サーバに照会することがないように、同期アグリーメントのスケジューリングに時間差を設ける。待機期間中（オフピーク時間）の同期時刻を選択します。
- ユーザ データのセキュリティが必要である場合、Unified CM Administration の [LDAP ディレクトリ（LDAP Directory）] 設定ページで [SSL を使用（Use SSL）] フィールドのチェックボックスをオンにして、Secure LDAP（SLDAP）を有効にする。
- [Unified CM UserID] フィールドへのマッピングのために選択した LDAP ディレクトリ属性が、そのクラスタのすべての同期アグリーメント内で一意であることを確認する。
- UserID として選択した属性は、Unified CM で定義したアプリケーション ユーザのいずれかの属性と同じであってはならない。
- LDAP 属性 sn（姓）は、ユーザの LDAP 同期の必須属性である。
- 同期前の Unified CM データベースにある既存のアカウントは、LDAP ディレクトリからインポートされたアカウントの属性に一致する場合だけ維持される。Unified CM UserID に一致する属性は、同期アグリーメントによって確認されます。
- エンド ユーザ アカウントは LDAP ディレクトリの管理ツールによって管理し、これらのアカウントのシスコ固有データは Unified CM Administration Web ページによって管理する。
- AD の配置については、ObjectGUID がユーザの主要属性として Unified CM で内部的に使用される。[Unified CM User ID] に対応する AD 内の属性は、AD 内で変更できます。たとえば、sAMAccountname を使用している場合、ユーザは自分の sAMAccountname を AD で変更することができ、Unified CM 内で対応するユーザ レコードは更新されます。

  その他すべての LDAP プラットフォームでは、User ID にマッピングされる属性が Unified CM におけるそのアカウントの主要属性となります。LDAP 内の属性を変更すると、Unified CM に新しいユーザが作成され、元のユーザには非アクティブのマークが付きます。

Microsoft Active Directory に関する追加の考慮事項

ドメインの同期アグリーメントでは、ドメイン外のユーザや子ドメイン内のユーザは同期されません。同期プロセス中は Unified CM が AD 照会に従わないためです。図 16-10 の例では、すべてのユーザをインポートするために 3 つの同期アグリーメントが必要です。Search Base 1 ではツリーのルートを指定しますが、子ドメインのいずれかに存在するユーザはインポートしません。範囲は VSE.LAB に限定されており、残りの 2 つのドメインに対し、そのユーザをインポートするように別々のアグリーメントが設定されています。

図 16-10　複数の Active Directory ドメインでの同期

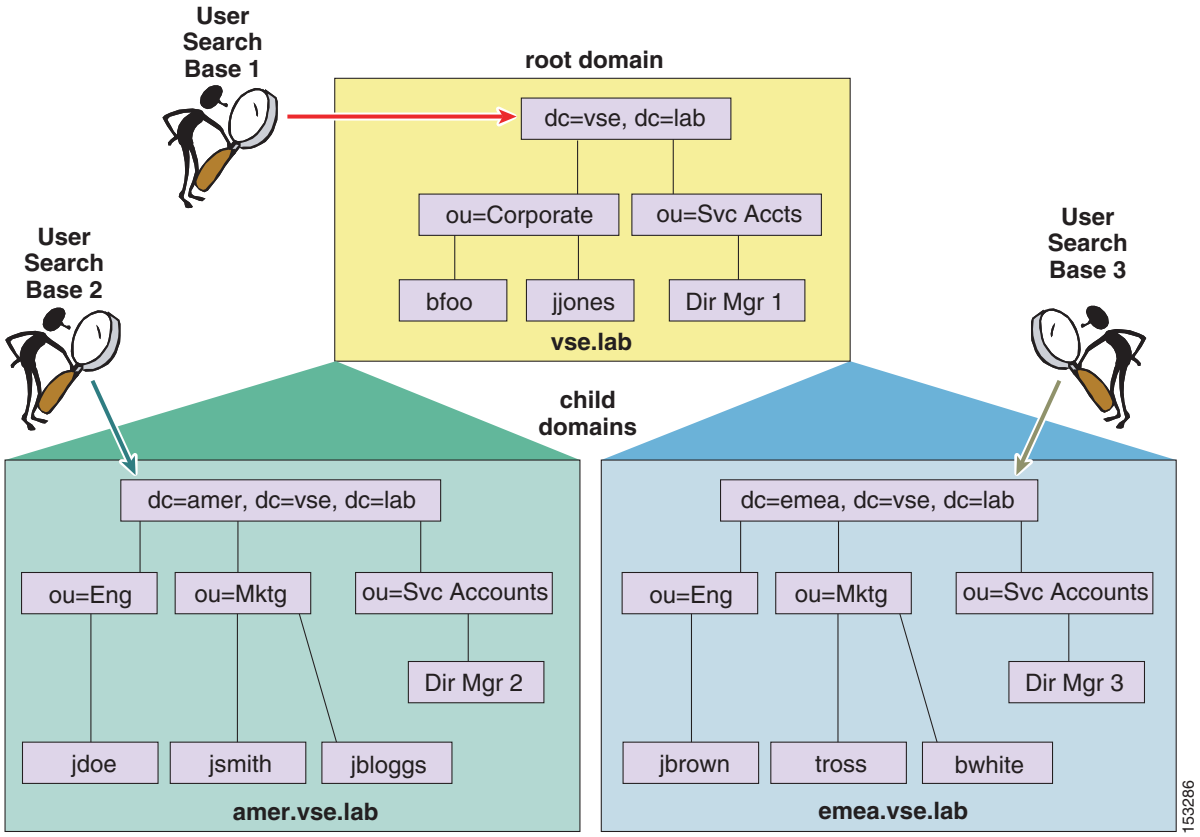
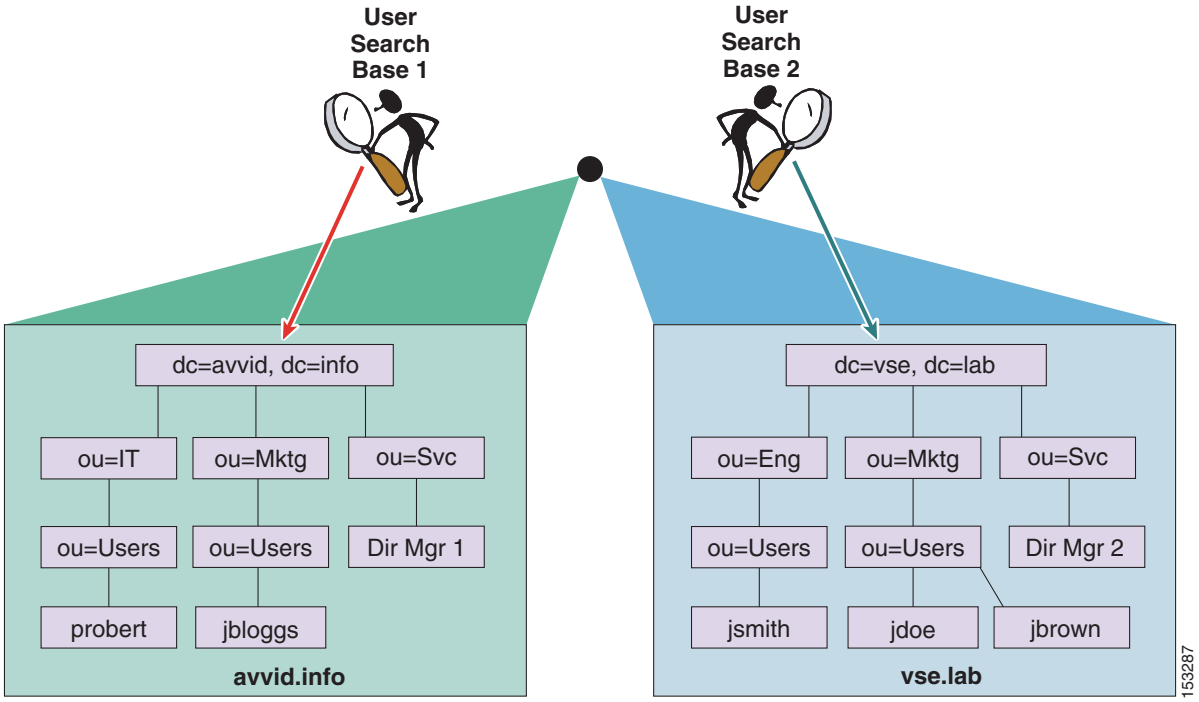


図 16-10 では、ドメインとサブドメインのそれぞれに少なくとも 1 つのドメイン コントローラ（DC）が関連付けられ、3 つの同期アグリーメントはそれぞれ適切なドメイン コントローラを指定します。DC にある情報は、その DC が存在するドメイン内のユーザの情報だけなので、すべてのユーザをインポートするために 3 つの同期アグリーメントが必要です。

図 16-11 に示すように、複数のツリーを含む AD フォレストで同期を有効にした場合も、上記と同じ理由で複数の同期アグリーメントが必要です。さらに、UserPrincipalName（UPN）属性がフォレスト全体で一意であることが Active Directory によって保証され、この属性は Unified CM UserID にマッピングする属性として選択する必要があります。マルチツリーの AD シナリオで UPN 属性を使用する場合の追加の考慮事項については、Microsoft Active Directory に関する追加の考慮事項（16-27 ページ）の項を参照してください。

図 16-11　　複数の AD ツリー（不連続なネームスペース）での同期



アカウントの同期を実行すると、Unified CM から AD にデフォルトの LDAP 検索フィルタ ストリングが送信されます。その中に、AD で無効のマークが付いているアカウントを戻さないという条件があります。ログインの失敗回数を超えた場合など、AD によって無効のマークが付けられたアカウントには、そのアカウントが無効である間に同期が実行された場合に非アクティブのマークが付けられます。

Unified CM マルチフォレスト LDAP 同期

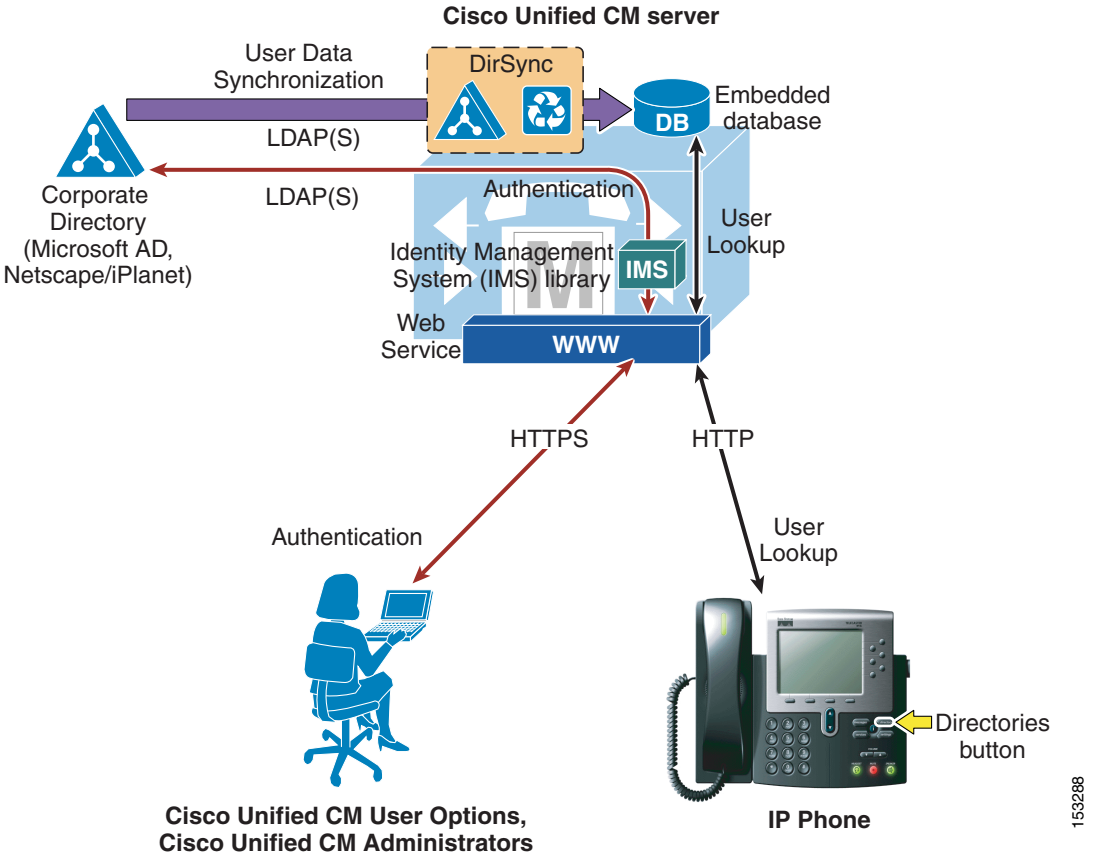
マルチフォレスト LDAP インフラストラクチャを使用した Unified CM 展開は、複数の異種フォレストを統合する単一のフォレスト ビューとして AD LDS を使用することによって、サポートできます。この統合では、LDAP フィルタリングを使用する必要があります（ディレクトリ同期および認証のユーザ フィルタリング（16-29 ページ）を参照）詳細については、次の URL で入手可能な『*How to Configure Unified Communication Manager Directory Integration in a Multi-Forest Environment*』を参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example09186a0080b2b103.shtml

LDAP 認証

LDAP 認証機能により、Unified CM が LDAP で同期されたユーザを社内 LDAP ディレクトリに対して認証できます。アプリケーション ユーザとローカルに設定されたユーザは、ローカル データベースに対して常に認証されます。また、すべてのエンド ユーザの PIN も、常にローカル データベースで確認されます。図 16-12 に示すように、Unified CM 内の Identity Management System（IMS）モジュールと社内ディレクトリ サーバ間で確立した LDAPv3 接続によって、この認証が実現されます。

図 16-12　LDAP 認証の有効化



認証を有効にするために、クラスタ全体に単一の認証アグリーメントを定義できます。認証アグリーメントは、冗長性を得るために LDAP サーバを 3 つまで設定でき、必要に応じて保護接続 Secure LDAP（SLDAP）もサポートします。認証は、LDAP 同期が正しく設定され、使用されている場合にのみ有効にできます。LDAP 認証設定は、SSO を有効にすることによって上書きされます。SSO が有効になると、エンド ユーザは常に SSO を使用して認証され、LDAP 認証設定は無視されます。

認証を有効にした場合の Unified CM の動作説明を、次に示します。

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

この動作は、リアルタイム Unified Communications システムの操作を社内ディレクトリの可用性に依存しないようにしながら、シングル ログイン機能をエンド ユーザに提供するという原則に従ったものです。図 16-13 に図示します。

図 16-13　エンドユーザパスワード、アプリケーションユーザパスワード、エンドユーザ PIN の認証

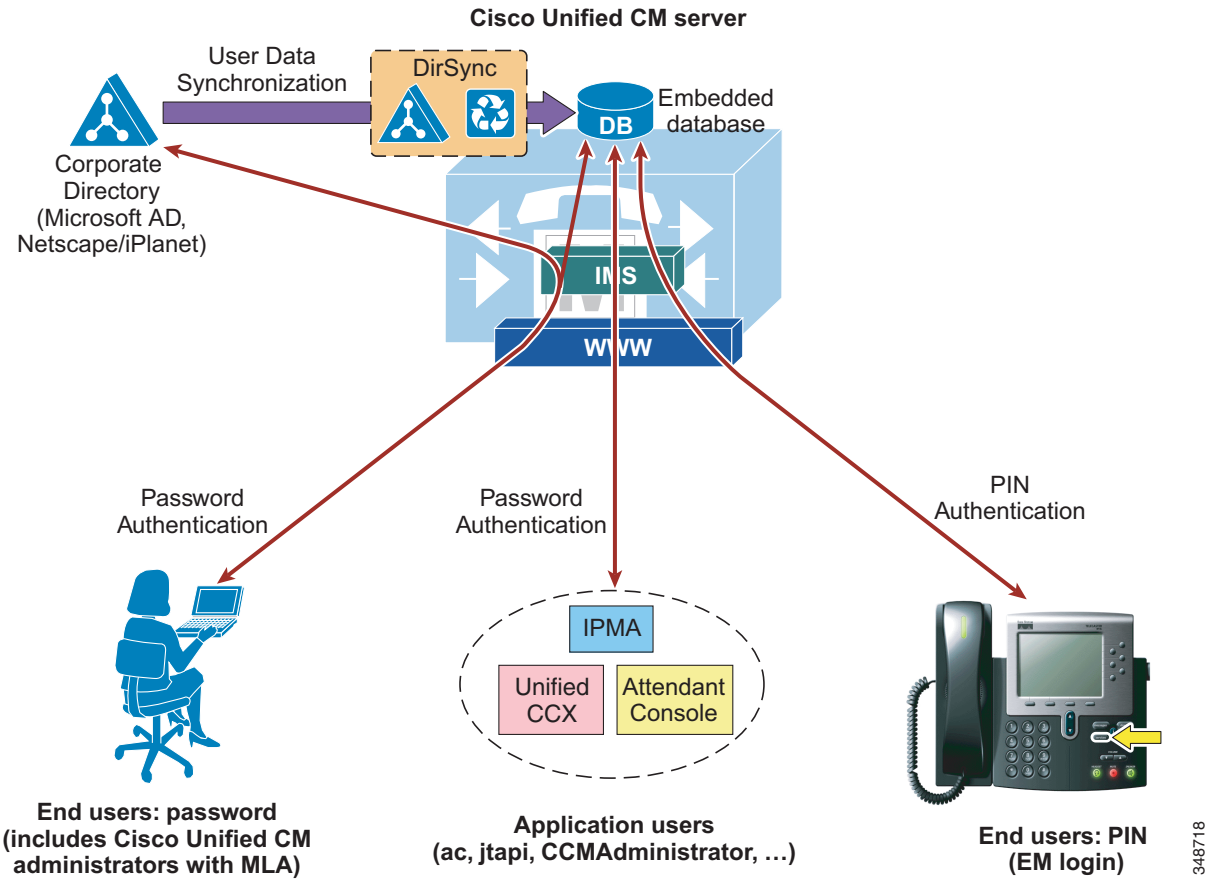


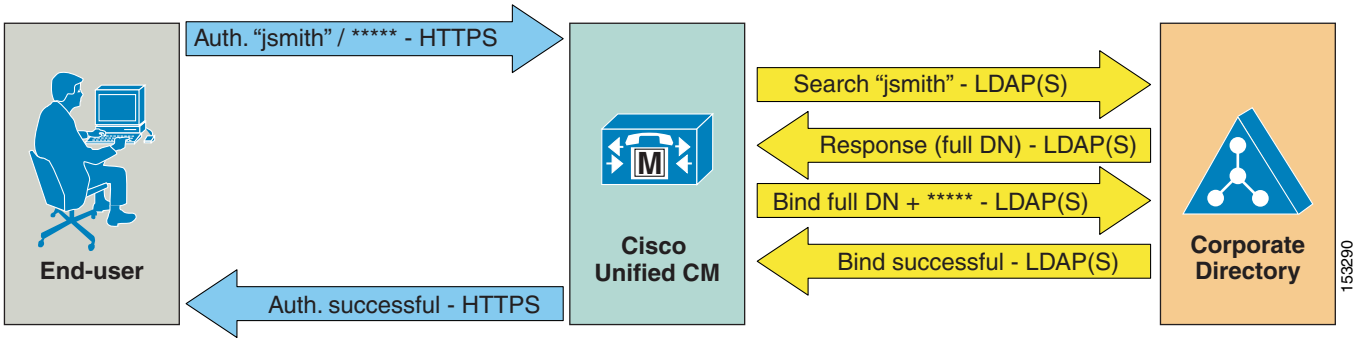
図 16-14 は、LDAP から同期化されたエンドユーザを社内 LDAP ディレクトリに対して認証するために Unified CM で採用された、次のプロセスを示しています。

1. ユーザは、HTTPS 経由で [Unified CM User Options] ページに接続し、ユーザ名とパスワードで認証を試行します。この例では、ユーザ名は jsmith です。
2. ユーザがローカル ユーザの場合、パスワードはローカル データベースに対して検査されます。

次の手順は、LDAP 同期ユーザにのみ適用されます。

1. ユーザが LDAP 同期ユーザの場合、Unified CM はユーザ名 jsmith に関する LDAP 照会を発行し、[LDAP 認証（LDAP Authentication）] 設定ページの [LDAP 検索ベース（LDAP Search Base）] で指定された値を、この照会の範囲として使用します。SLDAP を有効にした場合、この照会は SSL 接続を通じて行われます。
2. 社内ディレクトリ サーバは、LDAP 経由で、ユーザ jsmith の完全認定者名（DN）で応答します（たとえば、「cn=jsmith, ou=Users, dc=vse, dc=lab」）。
3. 次に Unified CM は、LDAP バインド操作を使用して、ユーザに提供された完全な DN とパスワードを渡すことにより、ユーザのクレデンシャルの検証を試みます。
4. LDAP バインドが成功した場合、Unified CM は、要求された設定ページにユーザが進むことを許可します。

図 16-14　認証プロセス



LDAP 認証に関する設計上の考慮事項

Cisco Unified CM で LDAP 認証を配置する場合は、設計と実装に関する次のベスト プラクティスに従ってください。

- 社内ディレクトリ内に特定のアカウントを作成し、Unified CM がそのディレクトリに対して接続および認証できるようにする。目的の検索ベース内にあるすべてのユーザ オブジェクトを「読み取る」ように最小権限を設定し、期限切れにならないようにパスワードを設定した状態で、Unified CM 専用のアカウントを使用することを推奨します。ディレクトリ内のこのアカウントのパスワードは、Unified CM 内のアカウントのパスワード設定と同期し続ける必要があります。アカウントのパスワードがディレクトリ内で変更された場合は、必ず Unified CM でアカウント設定を更新してください。LDAP 同期も有効にする場合、両方の機能に同じアカウントを使用できます。
- LDAP Manager Distinguished Name および LDAP Password で前述のアカウントのクレデンシャルを指定し、LDAP User Search Base ですべてのユーザが存在するディレクトリ サブツリーを指定することにより、Unified CM で LDAP 認証を有効にする。
- この方法は、LDAP から同期化されたすべてのエンド ユーザにシングル ログイン機能を提供します。これらは [Cisco Unified CM ユーザ オプション（Unified CM User Options）] ページにログインするために、社内ディレクトリ クレデンシャルを使用できます。
- 社内ディレクトリ インターフェイスで LDAP 同期ユーザのエンドユーザ パスワードを管理する。認証を有効にすると、Unified CM Administration のページの LDAP 同期ユーザにパスワード フィールドが表示されなくなります。
- Unified CM Administration の Web ページまたは [Unified CM User Options] ページでエンドユーザ PIN を管理する。
- Unified CM Administration の Web ページでアプリケーション ユーザのパスワードを管理する。アプリケーション ユーザは他の Cisco Unified Communications アプリケーションとの通信やリモート呼制御を容易にすること、また、実際のユーザには関連付けられないことに留意してください。
- 対応するエンド ユーザを Unified CM Administration の Web ページから Unified CM Super Users ユーザ グループに追加することにより、Unified CM 管理者のシングル ログインを有効にする。カスタマイズしたユーザ グループおよびロールを作成することにより、複数レベルの管理者権利を定義できます。

Microsoft Active Directory に関する追加の考慮事項

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

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

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

Microsoft AD から同期するユーザが複数のドメインに属していると、認証へのグローバル カタログの使用がさらに効率的になります。Unified CM は、照会に従う必要がなく、すぐにユーザを認証できるためです。このような場合は、Unified CM がグローバル カタログ サーバを指すようにし、LDAP User Search Base をルート ドメインの最上位に設定します。

複数のツリーを含む Microsoft AD フォレストの場合には、追加の考慮事項が適用されます。単一の LDAP 検索ベースでは複数のネームスペースを扱えないので、Unified CM は別のメカニズムを使用して、これらの不連続なネームスペース間でユーザを認証する必要があります。

LDAP 同期（16-11 ページ）の項で説明したように、複数のツリーがある AD フォレストで同期をサポートするために、UserPrincipalName（UPN）属性を Unified CM 内でユーザ ID として使用してください。ユーザ ID が UPN の場合、Unified CM Administration の [LDAP Authentication] 設定ページで [LDAP Search Base] フィールドへの入力はできませんが、その代わりに「LDAP user search base is formed using userid information.」という注意が表示されます。

実際には、図 16-15 に示すように、ユーザごとに UPN サフィックスからユーザ検索ベースが導き出されます。この例では、Microsoft Active Directory フォレストは avvid.info と vse.lab という 2 つのツリーで構成されます。同じユーザ名が両方のツリーに表示される場合があるため、同期プロセス中および認証プロセス中は UPN を使用してデータベースのユーザを一意に識別するように、Unified CM が設定されています。

図 16-15　複数のツリーがある Microsoft AD フォレストでの認証

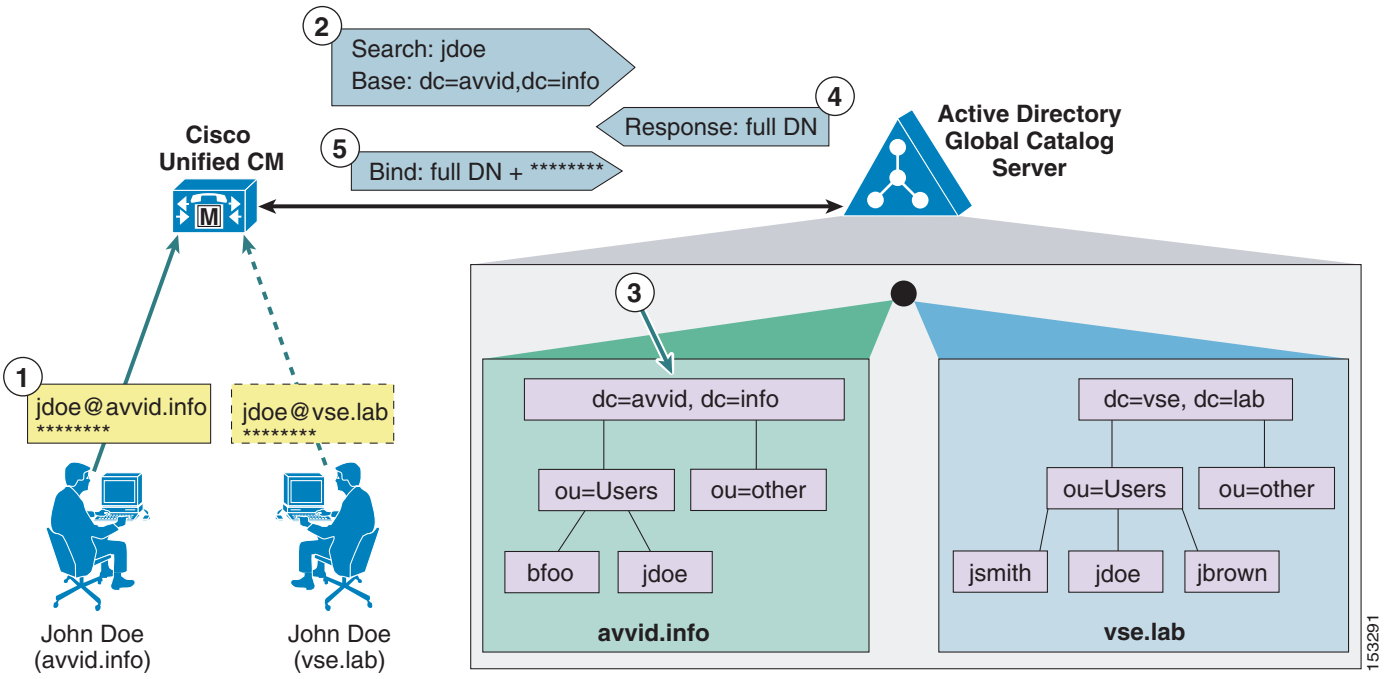


図 16-15 に示すように、John Doe という名前のユーザが avvid.info ツリーと vse.lab ツリーの両方に存在します。次の手順は、UPN が jdoe@avvid.info となる第 1 のユーザに対する認証プロセスを示しています。

1. ユーザは、ユーザ名（UPN に対応するもの）とパスワードを使用し、HTTPS 経由で Unified CM に対して認証します。
2. Unified CM は、Microsoft Active Directory グローバル カタログ サーバに対して LDAP 照会を実行し、UPN で指定したユーザ名（@ 記号よりも前の部分）を使用して、UPN サフィックス（@ 記号より後の部分）から LDAP 検索ベースを得ます。この場合、ユーザ名は jdoe で、LDAP 検索ベースは「dc=avvid, dc=info」です。
3. Microsoft Active Directory は、LDAP 照会で指定したツリーのユーザ名に対応する正しい認定者名を識別します。この場合は、「cn=jdoe, ou=Users, dc=avvid, dc=info」です。
4. Microsoft Active Directory は LDAP 経由で、このユーザの完全認定者名を使用して Unified CM に応答します。
5. Unified CM は、提供された認定者名とユーザが最初に入力したパスワードで LDAP バインドを試行し、その後は図 16-14 に示す標準的な場合と同様に、認証プロセスが続行されます。

（注）　複数のツリーを含む Microsoft AD フォレストでの LDAP 認証のサポートは、上記の方法だけで行われます。したがってサポートは、ユーザの UPN サフィックスが、そのユーザが存在するツリーのルート ドメインに対応する配置だけに限定されます。AD では、異なる UPN サフィックスが許可されたエイリアスを使用できます。UPN サフィックスがツリーの実際のネームスペースから分離されている場合は、Microsoft Active Directory フォレスト全体で Unified CM ユーザを認証できなくなります（ただし、その場合でも、別の属性をユーザ ID として使用し、統合をフォレスト内の単一のツリーに限定することはできます）。

ディレクトリ同期および認証のユーザ フィルタリング

Unified CM は、ディレクトリ同期のパフォーマンスを最適化するために、LDAP 照会フィルタを提供します。Unified Communications リソースに割り当てられるディレクトリ ユーザ アカウントをインポートすることを推奨します。企業全体で UDS ベースのサービス検出を有効にするには、企業内のすべてのクラスタの Unified Communications リソースに割り当てられているすべてのユーザが企業内のすべてのクラスタにインポートされる必要があります。ローカル ユーザとリモート ユーザの差別化は、使用される LDAP 同期アグリーメントに関連付けられた機能グループ テンプレートの [ホーム クラスタ(Home Cluster)] 設定によって行われます。ディレクトリ ユーザ アカウントの数が、各クラスタに対してサポートされている数を超える場合は、フィルタリングを使用して、そのクラスタに関連付けられるユーザのサブセットを選択する必要があります。Unified CM 同期機能は、大規模な社内ディレクトリに置き換わるものではありません。

多くの場合、同期対象のアカウントを制御するために必要となるのは、固有の検索ベースだけです。固有の検索ベースを使用できない場合は、カスタム LDAP フィルタが必要となることがあります。以降の項では、ディレクトリ同期の最適化に使用できる両方の方法について説明します。いずれかのメカニズムを使用して Unified CM へのアカウントのインポートを制限する場合、デフォルトのディレクトリ ルックアップの設定では、UDS LDAP プロキシ機能が使用されない限り、Unified CM データベースに存在するディレクトリ エントリだけが表示されます。ディレクトリ全体にアクセスするディレクトリ ルックアップの場合は、外部 Web サーバを使用するように Unified CM を設定することもできます。この設定の詳細については、ここでは説明しませんが、次の Web サイトで入手可能な Unified CM 製品マニュアルで説明しています。

https://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Unified CM データベース同期の最適化

Unified CM データベース同期機能には、LDAP ディレクトリ ストアから Unified CM パブリッシャ データベースへユーザ設定データ(属性)のサブセットをインポートするメカニズムがあります。ユーザ アカウントの同期が発生すると、各ユーザの LDAP アカウント情報が、そのユーザの特定の Unified Communications 機能を有効にするために必要な追加データと関連付けられることがあります。認証も有効な場合、パスワード確認のための LDAP ストアへのバインドに、ユーザのクレデンシャルを使用します。同期や認証が有効な場合に、エンド ユーザのパスワードは Unified CM データベースには格納されません。

ユーザ アカウント情報はクラスタ固有です。各 Unified CM パブリッシャ サーバは、このクラスタから Unified Communications サービスを受けているユーザの一意のリストを保持しています。同期アグリーメントはクラスタ固有で、各パブリッシャにはユーザ アカウント情報の独自コピーがあります。Unified Communications リソースが割り当てられるユーザだけが Unified CM と同期します。LDAP ディレクトリに定義されているユーザのセット全体が Unified CM クラスタにインポートされない共通の理由の一部を、次に示します。

- Unified Communications リソースが割り当てられないユーザのインポートにより、ディレクトリ同期時間が増加する。
- Unified Communications リソースが割り当てられていないユーザのインポートにより、Unified CM 検索とデータベース全体のパフォーマンスが遅くなる可能性がある。
- 多くの場合、LDAP ディレクトリ ストアのユーザ アカウント数が、Unified CM データベースの合計ユーザ容量を大幅に超過する。

Unified CM には、システムに追加できるアカウント数の制限がありません。シスコは、ユーザの数をサポートされているエンドポイントの 2 倍に制限することを推奨します。アプリケーション用のアカウントが必要な場合や、設計によっては追加のアカウントが必要な場合があります。

シスコは、ここで説明している制御メカニズムを使用して、LDAP データベース サイズに関係なく、インポートされるユーザ アカウントを最小限にすることを推奨します。これによって、最初とそれ以降の定期同期化の速度が改善され、ユーザ アカウントの管理可能性も向上します。

同期を制御するための LDAP 構造の使用

多数の LDAP ディレクトリの配置には、組織ユニット名（OU）を使用して、ユーザを論理的順序や、場合によっては階層的順序でグループ化します。ユーザを複数の OU に編成する構造が LDAP ディレクトリにある場合、インポートされるユーザのグループを制御するためにこの構造を使用することもできます。各個別 Unified CM 同期アグリーメントは、単一の OU を指定します。サブ OU 内であっても、指定 OU の下にある全アクティブ アカウントがサポートされます。OU 内のユーザだけが同期されます。ユーザを含む複数の OU がクラスタで必要な場合、複数の同期アグリーメントが必要です。Unified Communications リソースを割り当てられていないユーザが OU に含まれている場合は、これらの OU をディレクトリ同期から省くことを推奨します。

AD に同じ手法を使用して、コンテナを定義できます。同期アグリーメントでは、ディレクトリ ツリーの特定のコンテナを指定でき、それによってインポートの範囲を制限できます。

使用できる同期アグリーメントの数は限られているため、多数の OU やコンテナを持つ LDAP の配置では、この手法はすぐに使い果たされてしまいます。複数の OU がある環境でユーザを同期するには、同期サービス アカウントに割り当てる権限を制御するという方法があります。複数のユーザが存在するツリー ノードに同期アグリーメントを設定してから、システム アカウントの読み取りアクセスをサブツリーの選択部分に制限します。このアクセスを制限する方法については、LDAP ベンダーのドキュメンテーションを参照してください。

LDAP 照会

次のいずれかの理由により、フィルタリングに対して追加の制御が必要となる場合があります。

- LDAP ディレクトリがフラット構造となっており、同期アグリーメントの設定によって適切に制御できない。すべての同期アグリーメントによってインポートされるユーザの集約数が、Unified CM クラスタでサポートされる最大ユーザ数を超える場合は、フィルタを介してインポートされるユーザの数を制御する必要があります。
- 管理目的でユーザをセグメント化するために、ユーザ アカウントのサブセットを Unified CM クラスタにインポートし、クラスタへのアクセス権および認証を持つユーザのサブセットを制御する必要がある。クラスタにインポートされるいずれかのアカウントが、Web ページへのあるレベルのアクセス権および認証メカニズムを持ち、このことが適切でない場合があります。
- LDAP ディレクトリ構造が、Unified CM クラスタにユーザをマッピングする方法を正確に反映していない。たとえば、OU は組織階層に応じて設定されているものの、ユーザは地理的に Unified CM にマッピングされている場合、これら 2 つの間で重複する部分はほとんどありません。

このような場合、LDAP 照会フィルタを使用して、同期アグリーメントに対して追加の制御を提供できます。

LDAP 照会フィルタ構文およびサーバ側フィルタリング

Unified CM は、標準の LDAP メカニズムを使用して、LDAP ディレクトリ ストアのデータを同期します。Unified CM は、RFC 4510 などで規定されているように、検索メカニズムを使用して要求を送信し、LDAP サーバからデータを取得します。このメカニズムでは、検索メッセージ内のフィルタ ストリング指定する機能も定義されています。LDAP サーバはフィルタ ストリングを使用して、データを返すデータベースのエントリを選択します。フィルタ ストリングの構文は、RFC 4515 の The String Representation of Search Filters で規定されています。この RFC を参照用として使用して、より複雑なフィルタ ストリングを作成できます。

フィルタ ストリングは、Unified CM から LDAP サーバに送信される検索メッセージに組み込まれ、LDAP サーバはそれを実行して、応答で提供するユーザ アカウントを選択します。

単純なフィルタ構文

標準の属性名と、それらの属性に必要な値を指定して、フィルタを設定できます。属性は、名前の代わりに DN 要素で指定することもできます。Unified CM によって LDAP 照会で使用されるフィルタ ストリングは、ldapfilter テーブルの内部に格納され、検索メッセージに挿入されます。

フィルタは、次の構文を持つ UTF-8 形式のストリングです。

(*attribute operator value*)

or

(*operator*(*filter1*)(*filter2*))

ここで、*filter1* および *filter2* には、最初の行で示した構文が含まれ、*operator* は、表 16-6 に示す演算子のいずれかとなります。*attribute* は、ディレクトリ内に存在する LDAP 属性に対応し、*operator* は、表 16-6 に示す演算子のいずれかとなり、*value* は、その属性に必要な実際のデータ値に対応します。

表 16-6　フィルタ ストリングの基本的な演算子

演算子	機能の意味
!	論理否定
&	論理積
|	論理和
*	ワイルドカード
=	次の値と等しい（Equal to）
>=	辞書順における以上
<=	辞書順における以下

フィルタでは、LDAP ディレクトリ ストアに存在する任意の属性を指定できます。この属性は、Unified CM によって認識およびインポートされる属性である必要はありません。属性は、LDAP サーバでデータを選択するためにだけ使用され、対応するエントリには、Unified CM にインポートされるデータのサブセットが含められます。

例 16-1　単一の条件

(givenName=Jack)

例 16-1 のフィルタでは、指定された名前 Jack を持つすべてのユーザが選択されます。

例 16-2　複数の条件（論理文字を使用して結合）

(&(objectclass=user)(department=Engineering))

例 16-2 のフィルタでは、エンジニアリング部門のすべてのユーザが選択されます。

デフォルトのフィルタ ストリング

カスタム フィルタ ストリングが定義されていない場合、Unified CM は次のようにデフォルト LDAP フィルタ ストリングを使用します。

- Active Directory（AD）のデフォルトのフィルタ ストリング

  (&(objectclass=user)(!(objectclass=Computer))(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))

  このデフォルト フィルタでは、オブジェクト クラスがコンピュータではなくユーザであり、かつアカウントに無効のフラグが付いていないエントリが選択されます。

- Active Directory アプリケーション モード（ADAM）または Active Directory ライトウェイト ディレクトリ サービス（AD LDS）のデフォルトのフィルタ ストリング

  (&(objectclass=user)((objectclass=Computer))(!(msDS-UserAccountDisabled=TRUE)))

- その他すべてのディレクトリ タイプのデフォルトのフィルタ ストリング

  (objectclass=inetOrgPerson)

デフォルト フィルタの拡張

デフォルトのフィルタ ストリングを使用して、そこに追加の条件を付加することを推奨します。次に例を示します。

(&(objectclass=user)(!(objectclass=Computer))(!(UserAccountControl:1.2.840.113556.1.4.803:=2))(telephonenumber=+1919*))

このフィルタでは、電話番号フィールドのプレフィックスが +1919 であるユーザだけが選択されます。同期アグリーメントによって、米国でエリア コード 919 を持つユーザだけがインポートされます。この例では、すべてのエントリが +E.164 形式であることを前提としています。

検索フィルタに対して、既存の任意の属性を使用できます。または、LDAP ディレクトリ ストアで定義したカスタム属性を使用することもできます。フィルタ ストリングでは、LDAP サーバによって選択され、Unified CM に返されるレコードが制御されますが、インポートされる属性は、フィルタ ストリングの影響を受けません。

カスタム LDAP フィルタ ストリングの長さは 2048 文字です。最初にカスタム LDAP フィルタを作成する必要があり、その後既存のカスタム LDAP フィルタを LDAP 同期アグリーメントに割り当てることができます。それぞれの LDAP 同期アグリーメントに、別のカスタム LDAP フィルタを使用できます。

ハイ アベイラビリティ

Unified CM LDAP 同期を使用すると、ディレクトリ同期アグリーメントごとに最大 3 つの冗長 LDAP サーバを設定できます。Unified CM LDAP 認証を使用すると、認証アグリーメントごとに最大 3 つの冗長 LDAP サーバを設定できます。冗長性を確保するには、最低限 2 つの LDAP サーバを設定する必要があります。これらの LDAP サーバでは、ホスト名の代わりに IP アドレスを設定することで、ドメイン ネーム システム（DNS）の可用性への依存を排除できます。

Unified CM データベース同期のキャパシティ プランニング

Unified CM データベース同期機能には、LDAP ストアから Unified CM パブリッシャ データベースへユーザ設定データ（属性）のサブセットをインポートするメカニズムがあります。ユーザ アカウントの同期が発生すると、各ユーザの LDAP アカウント情報が、そのユーザの特定の Unified Communications 機能を有効にするために必要な追加データと関連付けられることがあります。認証も有効な場合、パスワード確認のための LDAP ストアへのバインドに、ユーザのクレデンシャルを使用します。同期や認証が有効な場合に、エンド ユーザのパスワードは Unified CM データベースには格納されません。

ユーザ アカウント情報はクラスタ固有です。各 Unified CM パブリッシャ サーバは、このクラスタから Unified Communications サービスを受けているユーザの一意のリストを保持しています。同期アグリーメントはクラスタ固有で、各パブリッシャにはユーザ アカウント情報の独自コピーがあります。

Unified CM クラスタが処理できる最大ユーザ数は、クラスタのメンバー間で複製される内部コンフィギュレーション データベースの最大サイズによって制限されます。設定または同期化可能なユーザの最大数は 160,000 です。80,000 人以上のユーザの場合、LDAP 同期アグリーメントの最大数は 10 に制限されますが、80,000 人未満のユーザの場合、LDAP 同期アグリーメントの合計数は 20 に制限されます。ディレクトリ同期のパフォーマンスを最適化するには、次の点を考慮してください。

- 電話機および Web ページからのディレクトリ ルックアップでは、Unified CM データベース、IP Phone サービス SDK、または UDS LDAP プロキシ機能を使用できます。ディレクトリ ルックアップ機能に Unified CM データベースを使用する場合、LDAP ストアから設定された、または同期されたユーザだけがディレクトリに表示されます。ユーザのサブセットを同期すると、ユーザのそのサブセットだけがディレクトリ ルックアップに表示されます。
- ディレクトリ ルックアップに IP Phone Services SDK を使用する場合に、LDAP に対する Unified CM ユーザの認証が不要であれば、Unified CM クラスタにログインするユーザのサブセットだけに同期を制限できます。
- クラスタが 1 つしか存在せず、LDAP ストア内のユーザ数が Unified CM クラスタでサポートされている最大ユーザ数よりも少なく、ディレクトリ ルックアップが Unified CM データベースに実装されている場合、LDAP ディレクトリ全体をインポートできます。
- 複数のクラスタが存在し、LDAP 内のユーザ数が Unified CM クラスタでサポートされている最大ユーザ数よりも少ない場合、すべてのユーザを各クラスタにインポートし、ディレクトリ ルックアップにすべてのエントリを確実に含めることができます。
- LDAP のユーザ アカウントの数が Unified CM クラスタでサポートされている最大ユーザ数を超え、ユーザ セット全体をすべてのユーザに表示する必要がある場合は、Unified IP Phone Services SDK を使用して Unified CM からディレクトリ ルックアップをオフロードする必要があります。
- 同期と認証の両方を有効にすると、Unified CM データベースに設定または同期されたユーザ アカウントはそのクラスタにログインできるようになる。同期するユーザの決定は、ディレクトリ ルックアップ サポートの決定に影響します。

（注）　シスコは、上記で説明している制限までユーザ アカウントの同期をサポートしていますが、この制限を強制しているわけではありません。多くのユーザ アカウントを同期化すると、ディスク容量のスターベーション、データベース パフォーマンスの低速化、およびアップグレードの長時間化を招くことがあります。

LDAP の UDS プロキシ

連絡先ソース アクセスのためにユーザ データ サービス（UDS）を使用するクライアントは、Unified CM エンドユーザ データベースに存在するユーザにのみアクセスが制限されます。このデータベースは LDAP 同期によって社内ディレクトリからデータを格納できますが、検索されるユーザの数は、Unified CM でサポートされるユーザの最大数によって制限されます（詳細については、Unified CM データベース同期のキャパシティ プランニング（16-33 ページ）の項を参照してください）。この制限に対処するため、Cisco Unified CM 11.5 以降のリリースでは、UDS ベースのユーザ検索で UDS から LDAP へのプロキシとして動作するように設定できます。このモードでは、UDS で要求されるユーザ検索ごとに、Unified CM は社内ディレクトリに接続して検索を実行し、その結果を UDS 経由でクライアントにリレーします。UDS 検索要求を直接実行する代わりに、このモードの Unified CM は社内 LDAP ディレクトリから返される情報に依存します。

（注）　オンプレミスの Jabber 導入環境に推奨される連絡先ソースは、Cisco Directory Integration（CDI）です。LDAP の UDS プロキシは、エンドポイントが連絡先検索で UDS に依存したり、社内ディレクトリのユーザ数が Cisco Unified CM でサポートされるエンド ユーザの最大数を超えたりする導入でのみ使用してください。

UDS プロキシ機能は、Unified CM でグローバルにイネーブルになります。プロキシ機能用に LDAP データ ソースを定義するために、最大 3 つのディレクトリ Unified Communications サービスを選択できます。Unified CM は LDAP バインドを使用して検索操作を実行します。このバインド操作に使用するユーザとパスワードは、この機能専用として設定されます。UDS プロキシは、最大 3 つの LDAP ユーザ検索ベースをサポートします。

VCS 登録エンドポイントのディレクトリ統合

Cisco TelePresence Video Communication Server（VCS）のエンドポイントは VCS によって管理され、Cisco TelePresence Management Suite（TMS）からディレクトリ情報を受信できるようになります。Cisco TelePresence Management Suite は、Unified CM および VCS 登録エンドポイントのスケジューリングのような多くのサービスと、VCS 登録エンドポイントの管理を提供します。

Cisco TelePresence Management Suite は、複数のソースから取得する複数の電話帳を管理できます。

Cisco TMS 14.1 は、Cisco Unified Communications Manager との統合も可能で、Unified CM からディレクトリ情報を受信できます。これは Unified CM および VCS エンドポイント用の統合されたディレクトリを用意する場合に推奨される構成です。

複数の Unified CM クラスタは、Cisco TMS に複数のディレクトリ ソースとして追加され、1 つのディレクトリに編成できます。TMS は、TMS に接続され、単一または複数の VCS に登録されたエンドポイントにディレクトリ情報をプッシュできます。

詳細については、次の URL にある『*Cisco TelePresence Management Suite Administrator Guide*』と『*Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*』の最新バージョンを参照してください。

https://www.cisco.com/en/US/products/ps11338/tsd_products_support_series_home.html

アイデンティティ管理アーキテクチャの概要

図 16-16 は、アイデンティティ管理アーキテクチャの概要を示します。すべてのシスコ コラボレーション アプリケーション（Cisco Unified CM with IM and Presence、Cisco Unity Connection など）は、個々の ID ストアを維持します。これらの ID ストアのユーザは個々の LDAP 同期アグリーメントによって社内ディレクトリから同期できますが、ローカルに設定することもできます。すべての関連プリンシパル（ユーザ）が社内ディレクトリと個々の ID ストアの両方に存在するようにするため、LDAP から同期することを強く推奨します。

LDAP 同期は、管理インターフェイスにアクセスするコラボレーション クライアントおよびワークステーションや、コラボレーション アプリケーションで提供されるさまざまなユニファイドコミュニケーション サービスが、シングル サインオン（SSO）を使用できるための条件です。SSO は、Security Assertion Markup Language（SAML）バージョン 2.0（SAML 2.0）に基づいて実装されています。SAML 2.0 認証では、サービスにアクセスするクライアント、これらのサービスを提供するコラボレーション アプリケーション、およびアイデンティティ プロバイダー（IdP）の間で、SAML 認証フローを使用します。IdP は実際のユーザ認証を行うコンポーネントです。IdP は、LDAP に対するユーザ/パスワード ベース認証、Kerberos 認証、スマートカード ベース認証など、さまざまな認証メカニズムをサポートできます。IdP は、SAML 2.0 仕様に準拠するマーケットで利用可能な IdP になることができます。シスコは、OpenAM、Ping Federate、Microsoft Active Directory Federated Services（ADFS）など、一部の IdP で SSO を検証しています。

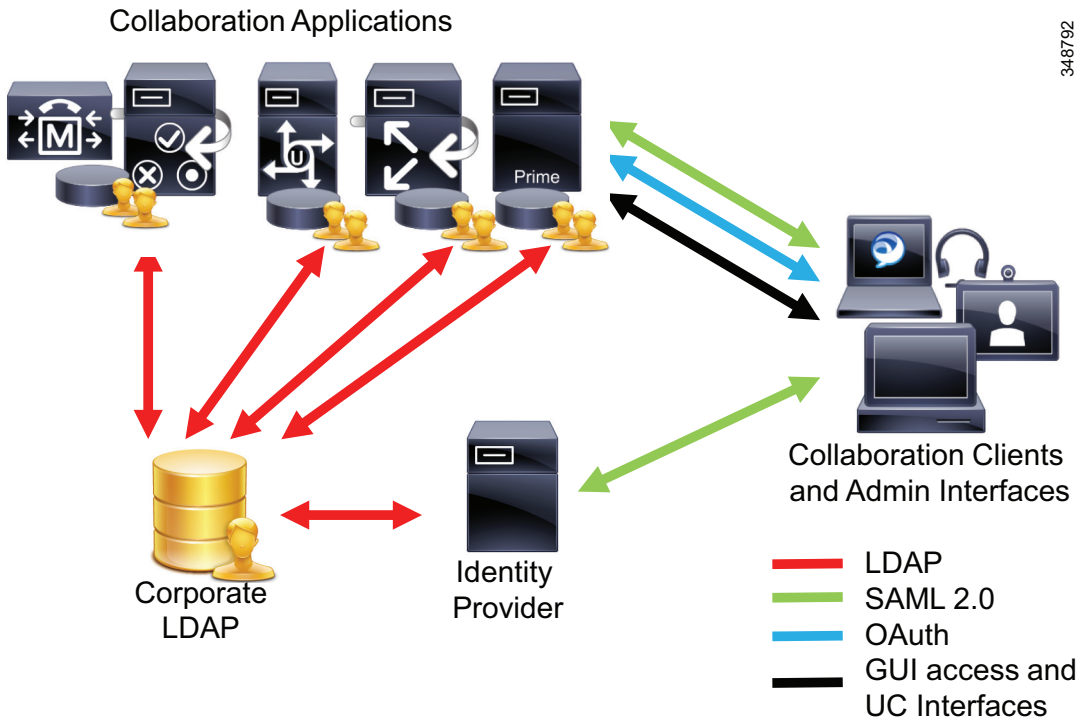
シングル サインオン（SSO）に対して、Unified Communications サービスへの認証は、SAML 2.0 による IdP で処理されます。この機能を使用すると、任意のユーザは Unified Communications サービスを提供するどのエンティティについても必要な認証は一度のみになり、再び認証しないで他のすべての Unified Communications サービス プロバイダーの GUI にアクセスできます。

SAML 2.0 はユーザ認証のみを提供し、ブラウザ ベースです。SAML 2.0 は、UC インターフェイス（Unified CM UDS、Unified CM SIP、Unified CM CTI、Unified CM IM and Presence SOAP、Unified CM IM and Presence XMPP、Unity Connection VMRest など）を使用するための分散型承認の要件に対処しません。

Unified CM 上で実行される集中型承認サービスが、Unified CM、Unified CM IM and Presence、Unity Connection によって提供される UC サービスの認証を提供します。この集中型承認機能は、OAuth 2.0 の仕様に基づいています。OAuth 2.0 は、リソース所有者に代わってサービスへの委任アクセスを提供する、承認用のオープン フレームワークです。このプロトコルは、クライアントが認証に使用するクレデンシャルを共有せずに、クライアントがリソースにアクセスすることを承認できるようにします。基本的に OAuth では中央承認インスタンスがクライアントにアクセス トークンを発行できるようにします。クライアントはこのトークンを、承認された証拠としてサービスを提供するサーバに提示します。アクセス トークンは、特定のリソースに対するアクセス権の付与レベルと有効期間を表す文字列値です。アクセス トークンは、承認サービスから承認の詳細を取得するために使用できる識別子を表しているか、実際の承認内容を格納しているかのいずれかです。後者の場合、アクセス トークンは*自己完結型*と呼ばれます。自己完結型アクセス トークンのコンテンツには署名を付けて、承認内容の信ぴょう性を検証できるようにする必要があります。必要に応じて、自己完結型アクセス トークンのコンテンツを暗号化することもできます。アクセス トークンが自己完結型でない場合、サービス プロバイダーは承認の有効性を確認するために、提示されたトークンの検証を承認サービスに要請する必要があります。このプロセスにおいて、承認トークンの内容、およびクライアント認証とトークン発行に使用するメカニズムは、サービス プロバイダーに対して完全に透過的です。

シスコ コラボレーション ソリューションの承認フレームワークでは、自己完結型アクセス トークンを使用しています。アクセス トークンの署名と暗号化に使用されたキーは、Unified CM から Unified CM IM and Presence にプッシュされ、Cisco Unity Connection および Cisco Expressway からプルされます。

図 16-16　アイデンティティ管理アーキテクチャ



シングル サインオン（SSO）

SAML 2.0 による SSO は、既存の LDAP バインドとローカル認証に追加された認証オプションです。SAML 2.0 SSO では、OAuth 承認サービスを含むすべての Unified Communications サービスは、SAML 2.0 を使用して社内アイデンティティ管理システムと直接統合します。

SSO に使用されるプライマリ プロトコルは、SAML です。プロトコル仕様、使用例、認証フローなどの SAML の詳細情報は、インターネットで公開されています。ここでは、SAML の重要な点だけを紹介します。

SAML を使用したアイデンティティ プロバイダー（IdP）とのすべての対話は、クライアント側の Web ブラウザを経由する必要があります。SAML の認証がユーザに Web GUI を公開しないクライアントに使用する場合、これらのクライアントは、内部の WebView クライアントを使用します。この例では、SSO をサポートする Jabber ソフトクライアントおよびコラボレーション エンドポイントが含まれます。

Security Assertion Markup Language（SAML）は、サービス プロバイダー（SP）と IdP との間のデータ交換用に特別に設計された XML データ形式です。SAML は IdP と SP 間で認証関連情報を渡すためにアサーションを含むセキュリティ トークンを使用します。この交換では、IdP が SAML 認証局のロールを担い、SP は SAML ユーザとなります。SAML の仕様は次の URL から入手できます。

https://saml.xml.org/saml-specifications

SAML 認証を行う前に、サービス プロバイダー（SP）と ID プロバイダー（Idp）間に信頼関係が確立されていなければなりません。これは、SP と IdP 間でメタデータを交換することによって行われます。

一般的に、単一の SAML メタデータ インスタンスに単一の SAML エンティティまたは複数のエンティティが記述されています。複数の SAML インスタンスを記述する SAML メタデータ インスタンスには、単一エンティティの記述のリストが含まれます。Cisco Unified CM リリース 11.5 以前では、シスコ コラボレーション ソリューションによって作成された SAML メタデータ インスタンスは、常に単一の SAML インスタンスのみを記述します。

SAML メタデータ インスタンスに記述されているどの SAML インスタンスについても、メタデータには以下が含まれます。

- 固有識別子
- 部門
- この情報の有効期限
- キャッシング期間
- この情報の XML シグニチャ
- 担当者
- エンティティ（エンティティ ID）の固有識別子
- この SAML インスタンスの SAML ロールの記述（ID プロバイダー、サービス プロバイダーなど）

これらのうち固有識別子以外は SAML 仕様でオプションであり、シスコ コラボレーション SP によって作成されたメタデータに含まれません。

SAML メタデータ インスタンスに含まれる各ロールの記述はサポートされるプロトコルを定義します。また、オプションで SSO キー情報も含まれます。これらのキーは、後で SAML エンティティ間で交換される SAML メッセージに署名するために使用されます。

SAML サービス プロバイダーの SAML メタデータは、SAML ID プロバイダーがこれらの 2 つのエンティティ間における SAML 交換に関連するサービス プロバイダーについて理解するために必要です。サービス プロバイダーに固有の SAML メタデータには、サービス プロバイダーが SAML 認証要求に署名するかどうかや、サービス プロバイダーが署名するためにサービス プロバイダーに返される SAML アサーションを要求するかどうかを示します。また、サービス プロバイダー SAML メタデータは、認証応答のポスト先を定義します。この認証コンシューマ サービス（ACS）の定義は基本的に URL です。また、サービス プロバイダー SAML のメタデータは、SAML 認証プロセスの一部として SAML サービス プロバイダーと SAML ID プロバイダーの間で交換される属性を定義する場合があります。

同様に、ID プロバイダーのメタデータは IdP と SP 間の SAML 交換に関連する IdP 特性を定義します。IdP のメタデータも、認証要求の署名要件と、SAML 認証プロセスの一部として IdP と SP 間で交換する必要がある属性を定義できます。

SAML のメタデータ形式に関する詳細情報は次の URL から入手できます。

https://saml.xml.org/saml-specifications

シスコ コラボレーション SP によって作成された SAML メタデータには、以下のみが含まれます。

- ID、entityID：どちらも、ノードの FQDN に設定されます。クラスタ全体の SSO の場合は、パブリッシャ ノードの FQDN に設定されます。
- AuthnRequestSigned: **false**。IdP によって要求されない限り、このエンティティによって送信される認証要求は署名されないことを示します。
- WantAssertionsSigned: **false**。このエンティティで承認されるために SAML アサーションが署名される必要がないことを示します。ただし、署名されたアサーションも承認できます。
- 暗号キーおよび署名キー：メタデータには、両方のキーに対するノードの Tomcat 証明書が含まれます。クラスタ全体の SSO の場合、マルチサーバ Tomcat 証明書が使用されます。これには、マルチサーバ Tomcat 証明書を使用するようにクラスタを設定する必要があります。

- nameIDFormat: **transient**。SAML アサーションのサブジェクトを特定するために使用される名前識別子が一時的なものであることを示します。IdP は次に同じサブジェクトの認証が成功したときに特定された新しい固有 Opaque を発行するため、これらの識別子をサブジェクトの特定に使用できません。代わりに、認証済みサブジェクトは、IdP によって返された **uid** 属性に基づいて特定されます。
- AssertionConsumerService：1 つまたは複数の Assertion Consumer Service 定義が含まれます。Cisco Unified CM リリース 11.5 以前では、HTTP-POST バインディングの Assertion Consumer Service 定義が 1 つのみ含まれます。Unified CM リリース 11.5 以降では、ノードおよびバインド（HTTP-POST および HTTP-Redirect）ごとに 1 つの Assertion Consumer Service 定義が含まれます。各 Assertion Consumer Service 定義は、バインド（HTTP-POST または HTTP-Redirect）および Assertion Consumer Service の URL（例：https://ucm.example.org:8443/ssosp/saml/SSO/alias/ucm.example.org）を指定します。

SAML 認証

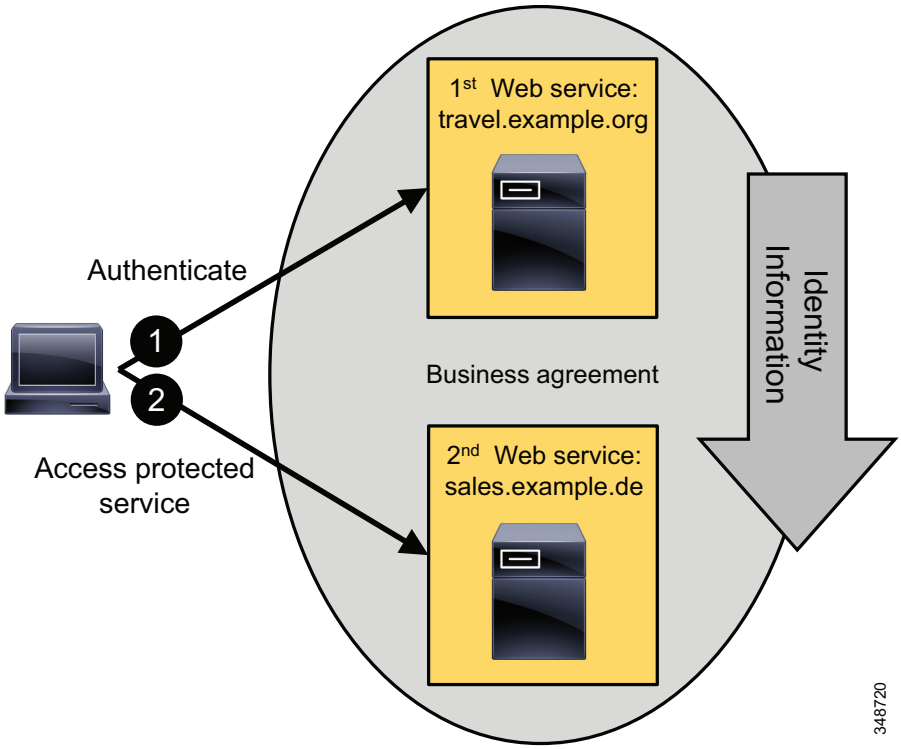
一般的な SAML 認証フローのアクターは次のとおりです。

- クライアント：サービスへのアクセスに使用するブラウザ ベースのユーザ クライアント
- SP：ユーザがサービスへのアクセスに使用するアプリケーションまたはサービス
- IdP：ユーザ クレデンシャルに基づいてユーザ認証を実行するエンティティ。実際のクレデンシャルと実際のクレデンシャル認証メカニズムは IdP によって非表示となります。IdP は、認証プロセスの結果に基づいて SAML アサーションを発行します。

SAML は、一般的な使用例を解決するための SAML の用途を記述するプロファイル数を定義します。シスコ コラボレーション サービスで SSO に使用される関連プロファイルは、SAML V2.0 の Web ブラウザ SSO プロファイルです。

このプロファイルによって解決する使用例は、図 16-17 に示すマルチドメイン Web のシングル サインオンです。この使用例では、ユーザはすでに何らかの Web サービスでログイン セッションを行っており（たとえば、travel.example.org）、このサービスを使用しています。ログイン プロセスの一環として、セキュリティ コンテキストが travel.example.org に確立されました。同じユーザが別の Web サービス（たとえば、sales.example.de）に移動し、travel.example.org と sales.example.de の間にこれらのサービス間でユーザにフェデレーション ID を確立するビジネス契約が存在する場合、そのユーザは認証クレデンシャルを再び提供せずに Web サービス sales.example.de にアクセスできます。この場合、ID プロバイダーのサイト（travel.example.org）は、このユーザは既知であり、適切に認証されており、特定の ID 属性を持っていることを、サービス プロバイダーのサイト（sales.example.de）にアサートします。サービス プロバイダーのサイト（sales.example.de）は、これらのサイト間の既存のビジネス契約に基づきこのアサーションを信頼し、このサービスへのアクセスを許可します。

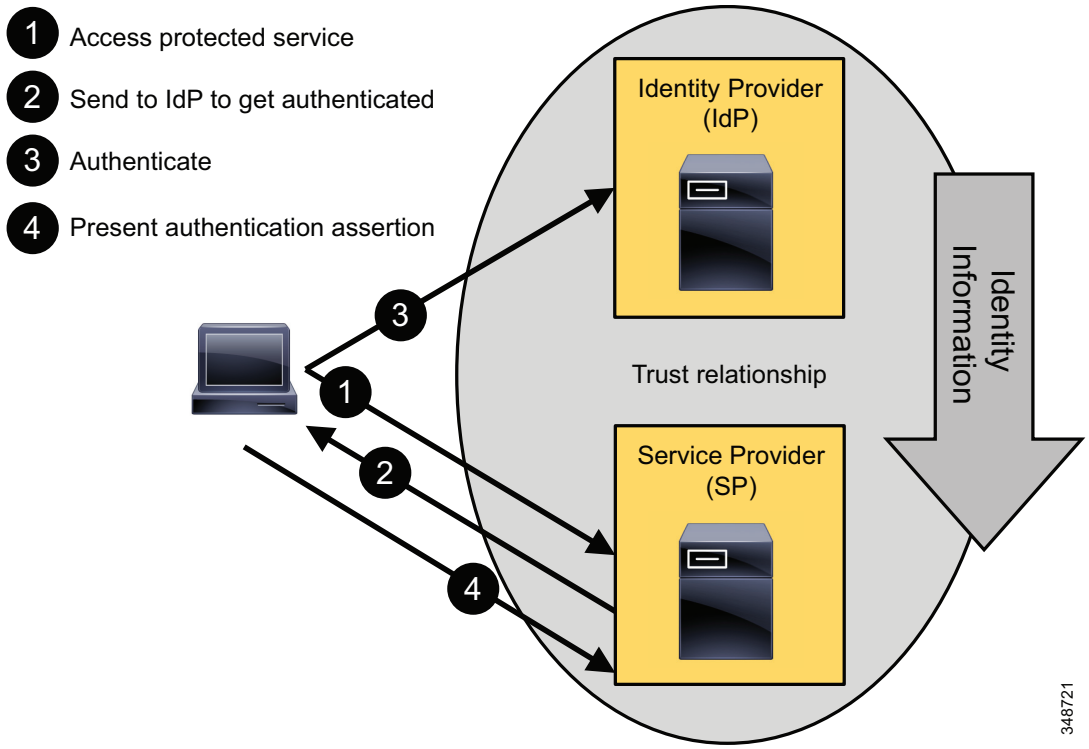
図 16-17　マルチドメイン Web のシングル サインオン



この説明は、ユーザが最初に Web サービスによって認証され、その最初の Web サービスはユーザが 2 つ目の Web サービスにアクセスできるように ID アサーションを提供することを示しています。最初にアクセスした Web サービス（travel.example.org）は、SP sales.example.de の IdP として機能します。これは IdP 起動の Web SSO と呼ばれます。

図 16-18 に示す、シスコ コラボレーション サービスで使用されるより一般的な Web SSO のフローは、SP 起動の Web SSO です。この場合、ユーザは直接（最初に IdP にアクセスせずに）SP の保護されているリソースにアクセスしようとします。SP は IdP にユーザを送信して認証させ、次にユーザは IdP から受け取った認証アサーションを SP に提示してアクセスします。

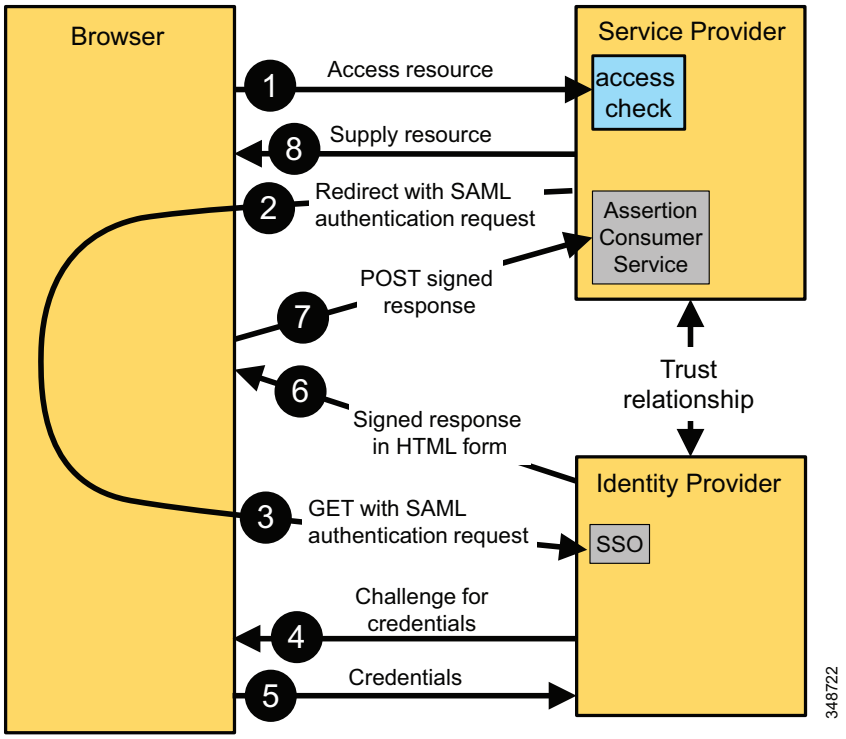
図 16-18　サービス プロバイダーによって起動される Web SSO



SAML の Web ブラウザ SSO プロファイルは、認証が IdP と SP のどちらによって起動されるのかや、IdP と SP 間のメッセージの交換方法によって、さまざまなオプションを提供します。前述のとおり、シスコ コラボレーション サービスは、サービス プロバイダーとのアクティブなセッションを行っていないユーザが保護されているリソースにアクセスしようとした場合に、SP がユーザを IdP に送信して最初に認証させる場合に限り、SP 起動の SSO を使用します。IdP は、認証アサーションを作成して、ユーザをそのアサーションとともに SP に戻します。

シスコ コラボレーション サービスの IdP と SP 間のメッセージ交換に使用されるバインディングは、図 16-19 に示す Redirect/POST バインディングです。ここでは HTTP 302 リダイレクトを使用し SP から IdP に SAML 認証要求メッセージが送信され、認証応答は HTTP POST メッセージを使用して IdP から SP に送信されます。

図 16-19　SP 起動の SSO（Redirect/POST バインディング）



SAML 認証フローの一般的な手順は次のとおりです。

1. ユーザが、アプリケーション サーバでホストされている URL をブラウザに入力して、サービスまたはリソースにアクセスしようとします。この時点でブラウザにそのサービスとのアクティブなセッションはありません。

2. SP は、要求元のクライアントにアクティブなセッションがないことがわかると、HTTP はステートレスなので、クライアントが事前に SP によって発行されたセッション Cookie を送信する場合にのみ、アクティブ セッションは SP によって検出できます。SSO の設定に基づいて、SP は、SSO 設定の一部として定義されている適切な IdP に送信される SAML 認証要求を生成します。この SAML 要求には、要求を生成した SP に関する情報が含まれています。この情報は、IdP が SAML 要求の送信元 SP を識別できるようにするために必要です。

   SP は、直接 IdP と通信してユーザを認証するのではなく、代わりに SP は、ブラウザを IdP にリダイレクトします。リダイレクトに使用する URL は、事前に交換した IdP のメタデータから取得します。IdP に送信される SAML 要求は Base64 エンコードを使用して URL のクエリー パラメータとしてリダイレクトに含まれます。

   この HTTP 302 のリダイレクトは次のようになります。

```
HTTP/1.1 302 Found
Location:
https://pingsso.example.com:9031/idp/SSO.saml2?SAMLRequest=nZLNbtswEITveQqCd1m0pKo
WY
RlwYxQ1kDZK5OaQG02tYwISqXLJtH37kkra%2FBjwodflcPab3V2iGPqRr7076lv44QEdIb%2BGXiOfXm
rqreZGoEKuxQDIneTt%2BusVz2aMj9Y4I01PL7abmmJWVCxnku07sYCqFAu2KGWVdaycV1AWRbnPPjJZl
Dkld2BRGV3TYEPJFtHDVqMT2oUSm%2BcJq5Ks2LGK5x84K%2B8p2QQ0pYWbfh2dG5Gn6aj0A6KZHc0AM2
MfeACYp6ob07a9nsUEGSWfjZUwJazpQfQIsWEjENUj%2FKs0z1E%2BKd0F0%2FO5908i5F92uyZprtsdJ
WtEsJHu0mj0A9gW7KOS8P326oVXejkk4F94F0WRpyEBjmmkjdip6JXAEyldXSyjhE%2FDsq%2BWdJ5V%2
```

```
FOWiq%2FeWy%2FSV4bP9yL8Fi%2B2mMb2Sv%2F%2FnFuK8B%2BHOq2NFdclhknJnhUYF2lHSNrH%2FjQ9
DOCiwNT2ZA1n3vfl5aUG4sD5nPdDVU5K37CFQenrdqz8%3D&RelayState=s249030c0bda8e96a8086c
92d0619e6446b270c463
```

上記のエンコードされた SAML 認証要求は以下にデコードできます。

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    ID="s249030c0bda8e96a8086c92d0619e6446b270c463"
    Version="2.0"
    IssueInstant="2013-09-19T09:35:06Z"
    Destination="https://pingsso.example.com:9031/idp/SSO.saml2"
    ForceAuthn="false"
    IsPassive="false"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    AssertionConsumerServiceURL="https://cucm-eu.example.com:
8443/ssosp/saml/SSO/alias/cucm-eu.example.com"
    >
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
cucm-eu.example.com</saml:Issuer>
<samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
    SPNameQualifier="cucm-eu.example.com"
    AllowCreate="true"
     />
</samlp:AuthnRequest>
```

認証パラメータを指定し、要求 SP を識別する他の詳細の中でも、上記の SAML 認証要求は、アサーション コンシューマ サービス（ACS）URL も指定します。ACS の URL は、認証プロセス終了時に SAML 認証応答を POST する必要がある URL です。

3. ブラウザはリダイレクトを受信し、URL に続き、IdP に対応する GET を発行します。SAML 要求は維持されます。この時点ではブラウザは IdP のアクティブなセッションがありません。
4. アクティブなセッションがないブラウザから新しい要求を受信したら（ブラウザは事前に IdP で発行された Cookie を送信しない）、IdP は事前に設定された認証メカニズムに基づいてユーザを認証します。利用可能な認証メカニズムには、ユーザ/パスワード、PKI/CAC、または Kerberos が含まれます。ユーザ/パスワード認証のため、IdP はユーザにクレデンシャルを入力するようにフォームをプッシュすることがあります（たとえば、IdP ログイン フォーム付きの「200 OK」メッセージなど）。実際の認証の場合、IdP はユーザ/パスワード認証のために LDAP サーバなど、バックエンド システムに依存する可能性があります。

   ここで重要な点は、認証のためのクレデンシャルの交換が IdP とブラウザの間で行われることです。SP は関与せず、クレデンシャルを目にすることもありません。
5. 認証プロセスに必要な詳細情報がブラウザから提供されます。ユーザ/パスワード認証の場合、この情報は POST で提供されます。その他の認証メカニズムの場合は、ブラウザが IdP にその他の詳細を送信する必要があります。
6. 提供されたクレデンシャルを IdP が確認および検証します。この確認には、それぞれのバックエンド システム（LDAP に対するユーザ/パスワード認証の LDAP バインド、チケットを検証する Kerberos サーバとの通信などです。

   最終的に IdP は SP に対して SAML 応答を生成します。この応答には、認証プロセスの結果を記録した SAML アサーションが含まれます。SAML アサーションには、基本的な Yes/No 情報に加えて、有効性の情報と認証されたエンティティを記述する属性に関する情報が含まれます。認証されたエンティティのユーザ ID は、よく知られている属性 **uid** に最低限含まれている必要があります。これは、SP がこの情報をアサーションから抽出し、認証されたエンティティをローカルのデータベースに存在するユーザに関連付けるためです。

   SAML アサーションは、IdP のメタデータで公開されている SSO キーの情報に従って、IdP によって署名され、場合によっては暗号化されます。これにより、SAML アサーションが本物であることを SP が確認できます。

IdP は 200 OK メッセージで非表示フォームの SAML アサーションをブラウザに返します。非表示のフォームは、SP のアサーション コンシューマ サービス（ACS）URL に SAML アサーションを POST するようブラウザに指示します。

IdP は、今後、クレデンシャルの交換を実行せずに同じブラウザからの認証要求に応答できるようにセキュリティ コンテキストを確立する必要があります。IdP は、ブラウザで有効なセッションがすでにあることを認識し、再度クレデンシャルを要求することなく、前に認証されたユーザの認証をアサートします。このコンテキストは、IdP によってブラウザで設定されたセッション Cookie によって確立されます。これにより、複数の SP に対する SSO がおおむね実現されます。

7. ブラウザは 200 OK メッセージで受信した非表示の POST に続き、SP のアサーション コンシューマ サービスに SAML アサーションを POST します。
8. SP は、SAML アサーションを POST から抽出して、アサーションの署名を検証します。これにより、SAML アサーションと IdP が本物であることが保証されます。その後、属性ステートメントの一部として SAML アサーションの属性 **uid** で受け取ったユーザ ID を使用して、そのユーザが要求したサービスへのアクセスを許可されているかどうかを判断します。この判断は、SP のローカル アクセス制御の設定に基づいて行われます。SAML アサーションで受け取った **uid** 値は、要求されたサービスで承認されたエンド ユーザの Unified CM ユーザ ID と一致する必要があります。SAML アサーションで IdP から送信されたユーザ識別子を Unified CM のユーザ ID に関連付けるため、SSO 認証は LDAP からで同期されたエンド ユーザでのみサポートされます。ここでは、IdP が同じディレクトリに統合されているため、IdP によって返される **uid** 値は Unified CM のエンド ユーザ情報と同じデータ ソースに基づいているという前提があります。

   SP は要求されたリソースへのアクセス権を付与し、ブラウザに 200 OK メッセージの内容を返信します。SP はまた、同じブラウザから同じ SP へのそれ以降のアクセス要求に対して SP が IdP との交換をそれ以上開始する必要がないように、ブラウザにセッション Cookie を設定します。IdP は、SP セッションの期限が切れた後にのみ、同じブラウザからの追加要求に関与します。

Web ベース アプリケーションの認証機能

SSO がコラボレーション サービスで有効になっている場合、各サービスへのすべてのアクセスは、SSO を使用して認証されます。フォールバック手段として、バニティ URL またはリカバリ URL もランディング ページに存在します。バニティ URL は SSO メカニズムをバイパスし、すべての管理者 GUI へのアクセスを提供します。バニティ URL による管理者 GUI へのアクセスは、ローカル ユーザ データベースに対して認証されます。バニティ URL による GUI へのアクセスは **utils sso recovery-url disable** コマンドを使用して CLI で無効にできます。

IdP に到達できないか IdP がダウンしている、メタデータに問題がある（たとえば、期限切れの署名付き証明書）、IdP の設定が変更されるなど、SAML のインフラストラクチャに問題がある場合はバニティ URL をリカバリのバック ドアとして使用できます。

コラボレーション サービスは現在、次の種類のユーザをサポートしています。

- OS ユーザ

  このユーザはインストール中に指定され、CLI、Disaster Recovery System（DRS）GUI、および OS Admin GUI にもアクセスできます。OS ユーザのクレデンシャルは、他のユーザのクレデンシャルとは別に維持されます。SSO を有効にすると、ローカル データベースに格納されているパスワードを使用して、CLI に対するアクセスが常にローカルで認証されます。一方、DRS および OS 管理 GUI に対するアクセスは SSO によって認証され、プラットフォーム データベースに照らし合わせて承認されます。CLI で **set account name** コマンドを使用することで、SSO UID 値からプラットフォーム ユーザへのマッピングを作成できます。

- アプリケーション ユーザ

  これらはローカルで作成および管理される機能ユーザです。パスワードは、ローカル データベースに保存されます。アプリケーション ユーザは SSO に対してイネーブルになっていません。SSO がイネーブルになっている場合、アプリケーション ユーザはランディング ページのバニティ URL から Admin GUI のみにアクセスできます。

- ローカル エンド ユーザ

  これらのユーザはローカルで作成および管理されます。パスワードはローカルに保存されます。これらのユーザはエンタープライズ ID 管理システムに存在しません。SSO がイネーブルの場合、ローカル エンド ユーザを正常に認証できません。SSO がイネーブルでないと、ローカル エンド ユーザと LDAP 同期ユーザは引き続きサポートされます。

- LDAP 同期エンド ユーザ

  これらのユーザは、社内 LDAP ディレクトリで管理され、LDAP 同期アグリーメントにより Unified Communications サービスに同期されます。ローカル データベースのどの LDAP 同期エンド ユーザにも、社内 LDAP ディレクトリに一致するユーザがあります。SSO がディセーブルの場合、LDAP 同期エンド ユーザのパスワードは、LDAP バインド操作を使用して検証されます。SSO がイネーブルになっている場合、LDAP 同期ユーザの認証は IdP で定義された認証メカニズムに基づき、認証はローカル設定に基づきます。LDAP 同期エンド ユーザは、要求されたリソースにアクセスするためにローカルに割り当てられた適切な権限が必要です。

PIN ベースの認証は常に（SSO が有効になっている場合でも）ローカル設定に基づきます。複数のコラボレーション サービスは個別の PIN を維持します。Cisco Unified CM リリース 11.5 以降、PIN は Unified CM と Cisco Unity Connection との間で同期させることができます。

次の Web サービスは、SAML IdP リダイレクトに基づいて SSO で有効になります。

- Cisco Unified Communications Manager Admin GUI
- Cisco Unified CM セルフ ケア ポータル
- Cisco Unified Communications Manager Serviceability GUI
- Cisco Unified Communications Manager Reporting Tool GUI
- Cisco Unified Communications Manager Platform Admin GUI
- Cisco Unified Communications Manager Disaster Recovery GUI
- Cisco Unified Communications Manager IM and Presence Admin GUI
- Cisco Unified Communications Manager IM and Presence Platform Admin GUI
- Cisco Unity Connection Admin GUI
- Cisco Unity Connection Platform Admin GUI
- Cisco Unified Personal Communicator Assistant
- Cisco Unity Connection WebInBox

Cisco Jabber の SSO

すべての Jabber プラットフォームは、SSO に組み込みのブラウザ制御を使用します。この制御は、基盤となるオペレーティング システム ブラウザ技術に依存します（表 16-7 を参照）。Jabber で使用する組み込みブラウザのコントロールがシステム ブラウザと同じテクノロジーに基づいているとしても、この 2 つの間で Cookie が共有されることは決してありません。これは、ユーザがシステム ブラウザを使用してすでに同じ IdP に対して認証されているとしても、Jabber には常に SSO を使用した専用の認証が必要であることを意味します。この問題を回避する唯一の方法は、セッション Cookie の代わりに永続的な Cookie を使用するように IdP を設定しないことです。ただし、この方法はベスト プラクティスであるとは見なせません。永続的な Cookie を使用すると IdP 認証状態が一般に公開されることから、同じ Cookie 保管場所にアクセスできる他のアプリケーションによってハイジャックされる可能性があるためです。

表 16-7　　ブラウザ技術と Cookie の共有

OS	Windows	Mac OS	Apple iOS	Android
基盤となるブラウザ	Internet Explorer	Safari	WebKit または Safari	WebKit
ネイティブ OS ブラウザとの Cookie 共有の制御	X	X	X	X

Apple iOS 上の Jabber の場合、ブラウザの選択（WebKit または Safari）は、[iOS での SSO ログイン動作（SSO Login Behavior for iOS）] エンタープライズ パラメータによって決まります。Apple iOS 上で SSO のブラウザとして Safari を選択すると、Apple 製アプリケーションだけがアクセスできる iOS 証明書ストアやその他の保護されたリソースにもアクセスできるようになります。SSO で証明書ベースの認証スキームを使用しなければならない場合は、このように選択する必要があります。

SSO の設計上の検討事項

SAML SSO は、クラスタ内のすべてのノードに対して常にイネーブルまたはディセーブルにする必要があります。クラスタ内のすべてのノードが SSO に対してイネーブルになるか、どのノードも SSO に対してイネーブルになりません。Admin GUI 経由で SSO をイネーブルにすると、自動的にすべての既存のノードが同時に SSO をイネーブルにします。このプロセスの一部として SP メタデータがダウンロードされて、IdP とクラスタ ノードの間の信頼の範囲を確立するために使用されます。

Cisco Unified CM リリース 11.5 より前、IdP では各クラスタ ノードを個々の SP として表現する必要がありました。すでに SSO モードに入っているクラスタに後でノードが追加されると、その追加されたノードのメタデータは IdP で定義された SP のリストを完成するために IdP にインポートされる必要がありました。

Cisco Unified CM リリース 11.5 以降では、SSO をクラスタ全体モードで有効にできます。この場合、IdP と交換する必要があるメタデータ ファイルは 1 つのみです。クラスタの SAML メタデータには暗号化および署名キーを 1 つだけ含めることができるため、クラスタ全体の SSO は単一のマルチサーバ Tomcat 証明書がクラスタで使用される場合だけ使用できます。マルチサーバ証明書は、CA 署名付き証明書である必要があります。新しいノードがクラスタ全体の SSO に対応したクラスタに追加されると、追加されたノードの新しい Assertion Consumer Service URL を IdP が認識できるように、更新されたメタデータは IdP と交換される必要があります。

シスコ コラボレーション SP の SP メタデータには、HTTP-POST および HTTP-Redirect バインドの Assertion Consumer Service 定義が含まれます。これらのバインドは、IdP によってサポートされ、IdP で有効である必要があります。クラスタ全体モードの SSO の場合、IdP が単一 SP に対する複数の Assertion Consumer Service 定義をサポートできる必要があります。

IdP のメタデータはすべての SAML SP にインポートされる必要があります。SSO が Admin GUI でイネーブルの場合、プロセスで提供される IdP のメタデータは、クラスタ内のすべてのノードに自動的にインポートされます。アサーションの署名または暗号化が IdP によって使用される場合、シスコ コラボレーション SP と交換した IdP のメタデータに署名および暗号化キーを含める必要があります。

SP メタデータはオプションの ContactPerson 情報を含まないため、IdP はシスコ コラボレーション SP の連絡先情報を表示できません。

SAML SP は、SAML AuthnRequest に WantAssertionsSigned を含めることで、IdP から署名されるアサーションを要求できます。現在、シスコ コラボレーション SP はこの情報を送信せず、SP メタデータで同じパラメータが **False** に設定されます。これによって、IdP はアサーションの署名を完全に制御できます。シスコは IdP で署名する SAML アサーションを実行することを推奨します。

そうでない場合は、IdP によって要求されないと、シスコ コラボレーション SP は SAML 認証要求を暗号化したり署名したりしません。これは IdP によってサポートされている必要があります。

シスコ コラボレーション SP は、メタデータと SAML 認証要求の両方で、namedid-format:transient を要求します。IdP はこの形式をサポートし、適切に設定される必要があります。

SAML アサーションの一部として、IdP は AttributeStatement で属性 **uid** を返す必要があり、この属性の値は Unified CM の各エンド ユーザのユーザ ID と一致している必要があります。

IdP の可用性は SSO を使用するうえでの重要な要件です。IdP は完全な冗長性と耐障害性とともに導入する必要があります。このタイプの導入に重要なのは、IdP が単一の論理 URL を使用して導入され、単一の IdP URL の可用性が高くなるように適切なロード バランサと Web サーバ ファームが導入されることです。単一の IdP URL は IdP のメタデータに含まれ、すべてのシスコ コラボレーション SP にインポートされます。1 つの要素の障害（たとえば、1 つの Web サーバ）は、コラボレーション サービスでは非表示にする必要があります。

SAML 要求およびアサーションは、SP および IdP の証明書を使用して署名されます。SAML SSO のメカニズムが引き続き機能することを確認するために、これらの証明書の有効期間を厳密に監視する必要があります。

SAML アサーションには、有効性の情報（NotBefore、NotOnOrAfter）が含まれます。有効なアサーションがタイミングの問題で拒否されないようにするには、Network Time Protocol（NTP）などの適切なメカニズムを使用してすべてのサービスを同期することが必須です。

承認フレームワーク

Web インターフェイスにアクセスするユーザの場合、認証はローカル設定または LDAP に基づいて行われるか、あるいは（SSO の場合）ユーザのブラウザ、Web サーバ、IdP 間の SAML 交換に基づいて行われるかのいずれかです。認証に成功すると、Web サーバ（Unified CM Administration GUI にアクセスする場合は、Unified CM で実行している管理アプリケーション）は、ローカル設定を確認して、認証済みユーザに特定のリソースへのアクセスが承認されているかどうかを判断します。たとえば、ユーザ Bob が IdP に有効なクレデンシャルを提供して SSO 認証が成功したとしても、Bob が「Standard CCM Super Users」グループのメンバでなければ、Unified CM は引き続き Unified CM Administration インターフェイスへのアクセスを拒否できます。この場合 Bob は、Unified CM Administration へのアクセスを取得する代わりに、システムにアクセスするために必要な権限を持っていないことを示すメッセージだけを受け取ります。Unified CM 管理 GUI やエンドユーザのページなどの Web サービスに対するアクセスの承認は、常にアプリケーションで定義されたアクセス レベルに基づいて行われます。

Jabber クライアントおよびその他のエンドポイントは、多数のコラボレーション インターフェイス（Unified CM SIP、Unified CM CTI、Unified CM IM and Presence SOAP、Unity Connection VMRest など）へのアクセスが必要です。（各インターフェイスで）多重認証メカニズムにならないよう、Cisco Collaboration システムでは単一の認証に基づく一元化された承認フレームワークとして OAuth を使用しています。

OAuth 2.0

Oauth 2.0 認証フレームワークは、IETF OAuth 作業グループによって定義されたオープン スタンダードです。現在のバージョンは RFC 6749 としてリリースされています。

アプリケーションがユーザに代わって複数のサービスにアクセスしなければならない場合、OAuth を使用しなければ常に、サービスごとに個別の認証および承認が必要になります。これはエンドユーザにとって、準最適なユーザ エクスペリエンスになります。なぜなら、エンド ユーザが複数のクレデンシャルのセットを管理せざるを得ないためです（ただし、SSO を使用することで部分的に対処できます）。しかも、アクセス クレデンシャルを複数のアプリケーションで共有しなければならないという信頼に関する問題があります。

OAuth はこのような課題に対処するために、アプリケーションがエンド ユーザの代理としてサービスに対するアクセス権を取得できるよう、エンド ユーザとサービスの間で行われる承認インタラクションを調整します。この承認インタラクションの一環として、エンド ユーザは認証後に、承認を求めるアプリケーションにアクセス トークンを付与するよう OAuth 承認サービスに指示します。アクセス トークンを受け取ったアプリケーションは、サービスにアクセスする際に、承認された証拠としてそのトークンを提示します。

アクセス トークンには有効期限があるため、アプリケーションでアクセス トークンを使用できる期間は限られます。OAuth 仕様では、OAuth 承認サービスがアクセス トークンと併せてリフレッシュ トークンも付与できるようになっています。通常、リフレッシュ トークンの有効期間はアクセス トークンよりも長くなっていて、リフレッシュ トークンが有効な限り、アプリケーションはこれを使用して OAuth 承認サービスから新しいアクセス トークンを取得することができます。完全な承認手順に従ってアクセス トークンを取得する場合とは対照的に、リフレッシュ トークンと引き換えに新しいアクセス トークンを取得する場合、エンド ユーザのインタラクションも、さらにはエンド ユーザの認証も必要ありません。リフレッシュ トークンの概念により、エンド ユーザに代わってサービスへのアクセスがアプリケーションに承認される期間は（リフレッシュ トークンが有効な期間だけ）長くなりますが、リフレッシュ トークンを失効できるようにすることによってアクセス トークンの露出をその有効期間に制限しています。アプリケーションが現在使用しているアクセス トークンの有効期間の終了時に新しいアクセス トークンを取得しようとする場合、OAuth 承認サービスとのインタラクションが必要になります。リフレッシュ トークンが失効していると、OAuth 承認サービスは、アプリケーションが引き続き承認されていることを表す新しいアクセス トークンの発行を拒否します。

インターネットでは、さまざまなサービスで OAuth が一般的に使用されています。一部のサービスでは、Web アプリケーションに独自の承認ロジックを組み込む代わりに、Facebook、Google、Twitter などのサイトの OAuth 承認サービスにこのプロセスを委任しています。その場合、メインの Web サイトで、ユーザがたとえば Facebook による OAuth 承認リンクを表すアイコンをクリックするだけで、メインの Web サイト（クライアント）が OAuth 承認フローを開始します。これにより、エンド ユーザのユーザ エージェント（Web ブラウザ）は承認サーバ（たとえば Facebook）にリダイレクトされます。承認サーバに対し、エンド ユーザが自分のクレデンシャルを使用して認証を行った後、承認サーバはエンド ユーザに対し、このフローでクライアントが要求したアクセス レベル（スコープ）（たとえば、ユーザのメール アドレスに対するアクセス）を承認するよう求めます。エンド ユーザがアクセスを承認すると、それと同時に承認サーバはアクセスを要求しているクライアントにアクセス権を付与し、アクセス トークンを発行します。クライアントがアクセス トークンを取得する実際のプロセスは、そのクライアントで使用する OAuth 承認フローのタイプによって異なります。

Oauth ロール

OAuth の動作を理解するには、以下のロール定義が参考になります。

- リソース所有者またはエンド ユーザ

  保護されたリソースの所有者。OAuth フレームワークでのリソース所有者とは、保護されたリソースに対するアクセス権を付与するエンティティのことです。リソース所有者が個人の場合は、エンド ユーザとも呼ばれます。

- リソース サーバ

  保護されたリソースは、リソース サーバでホストされます。リソースに対するアクセスの要求では、承認された証拠としてアクセス トークンを使用します。要求に含めて提示されたアクセス トークンに基づいて、リソース サーバはアクセス権を付与するか要求を拒否します。シスコ コラボレーション ソリューションのコンテキストでは、保護されたリソースとは、Cisco Jabber クライアントおよびエンドポイントで使用する UDS、Unity Connection VMRest などのインターフェイスを指します。

- クライアント

  リソース所有者に代わり、保護されたリソースに対して要求を行うアプリケーション。クライアントとしては、デスクトップ マシンやモバイル デバイス上で稼働するアプリケーション、サーバ アプリケーション、クラウド サービスなどが考えられます。「クライアント」という用語は、OAuth フレームワークのコンテキストにおけるロールを単に意味します。

  一部の使用例では、OAuth クライアントはシスコ コラボレーション サービス（たとえばコラボレーション エッジ）またはエンド ユーザ クライアント（たとえば Jabber）になります。コラボレーション エッジがユーザに代わって OAuth トークンを要求する場合、コラボレーション エッジは OAuth クライアントとして機能します。企業内の Jabber クライアント ログイン フローの場合、Jabber クライアントが OAuth クライアントとして動作します。

  各 OAuth クライアントには、OAuth client_id と呼ばれる固有識別子があります。この OAuth client_id は、クライアント タイプを一意に識別します。たとえば、Jabber for Windows と Jabber for Android は、異なる client_id を使用します。しかし、明確な理由から変更された client_id によって異なるクライアント リリースを認証サービスが区別できることが要求される（たとえば、クライアント リリース別に OAuth 交換のバリエーションをサポートする）場合を除き、Jabber for Windows ではすべてのリリースで同じ client_id を使用します。シスコ製品およびサードパーティ クライアント用に、一連の client_id が事前定義されています。

  保護されたリソースに対する承認を要求すると、OAuth クライアントは特定の範囲のトークンを要求できます。この範囲は、アクセスするために OAuth トークンを使用できるサービスの範囲を表します。

  OAuth アクセス トークンは、承認サービスによって提供され、ベアラー（クライアント）によって保護されたリソースへのアクセスに使用されます。通常、アクセス トークンは、特定のユーザに対して発行され、特定の有効期限があります。アクセス トークンが期限切れになると、クライアントは新しいアクセス トークンを取得する必要があります。

- 許可サーバ

  リソース所有者の認証が完了し、そのリソース所有者から承認を得ると、承認サーバはクライアントが使用するアクセス トークンを発行します。

リソース サーバと承認サーバは必ずしも別々のエンティティである必要はありません。これらの機能は、同じサーバ上に存在することができます。さらに、単一の承認サーバが複数のリソース サーバのアクセス トークンを発行することもできます。

Cisco Unified Communications アーキテクチャでは、承認サーバは Unified CM 上で実行される機能です。承認サーバによって発行されたアクセス トークンは、Cisco Jabber クライアントやその他のエンドポイントがさまざまなコラボレーション インターフェイス（Unified CM SIP、Unified CM CTI、Unified CM IM and Presence SOAP、Unity Connection VMRest など）のアクセス権を取得するために使用します。

一般的な OAuth フロー

OAuth では、多種多様な承認フローを定義していますが、このすべてのフローの間で共有する共通点がいくつかあります（図 16-20 を参照）。

図 16-20　一般的な OAuth プロトコルのフロー

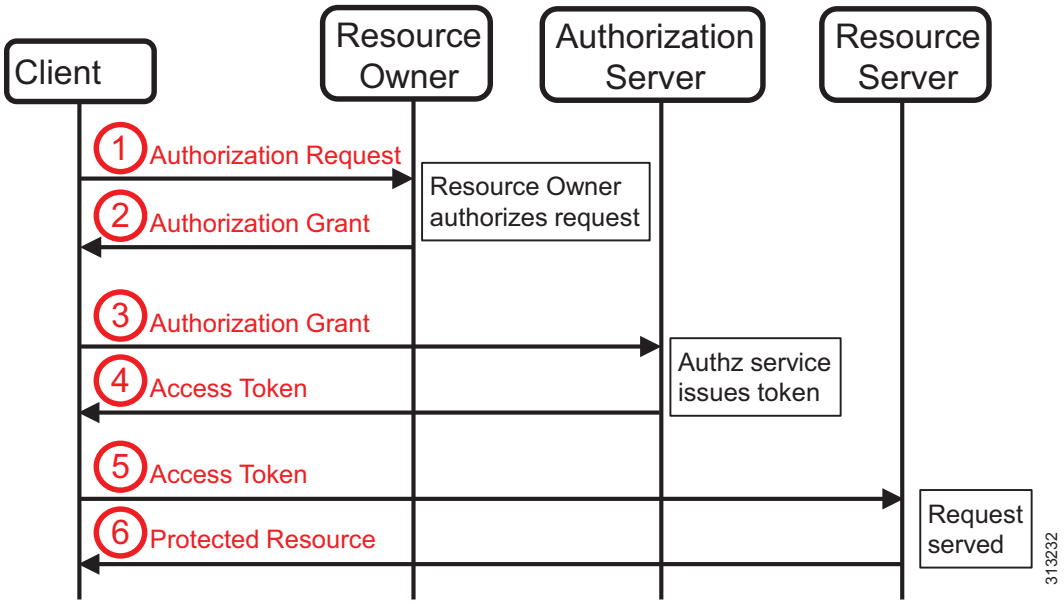


図 16-20 に示されている OAuth フローは、4 つのロールと、それらのロール間での以下のインタラクションを説明しています。

1. クライアントがリソース所有者（エンド ユーザ）に、保護されたリソースへのアクセスを承認するよう求めます。図 16-20 では、これはクライアントとリソース所有者間で直接行われるインタラクションとして示されていますが、実際には、この要求は承認サーバの仲介によって行われるのが通常です。その場合、承認サーバはリソース所有者の認証が成功した後、承認フローを開始したクライアントを承認するよう、リソース所有者に求めます。図 16-20 に示されているように、クライアントを承認するかどうかの決定は、リソース所有者（エンド ユーザ）の手に委ねられています。
2. クライアントが、リソース所有者の承認を表す承認付与を受け取ります。この付与は、OAuth 仕様で定義されている付与の 4 つのタイプのうちの 1 つによって表現されます。付与のタイプは、そのクライアントが承認を要求するために使用した手段と、承認サーバでサポートされているタイプによって決まります。
3. クライアントは承認付与を使用して、承認サーバにアクセス トークンを要求できます。それには、クライアントが認証を行って、取得済みの承認付与を提示する必要があります。クライアントの認証が必要となるのは、信頼されていない仲介者によって承認付与が悪用されないようにするためです。

4. 承認サーバはクライアントを認証する際に、承認付与を検証します。承認付与が有効であれば、アクセス トークンと（オプションで）リフレッシュ トークンを発行します。承認サーバによるクライアント認証では、クライアントの認証クレデンシャルが事前に承認サーバに登録されていることが必要になります。
5. この段階で、クライアントは保護されたリソースへのアクセスを要求し、取得済みの承認トークンを承認の証拠として使用できます。
6. リソース サーバはアクセス トークンを検証し、有効であれば、要求を処理します。この検証では、自己完結型アクセス トークンが使用されていない場合は特に、リソース サーバと承認サーバの間でのトランザクションが必要になることがあります。

ステップ 1 の説明で述べたように、承認サーバから承認付与を取得する方法として優先されるのは、承認サーバを仲介として使用することです。OAuth 承認コード付与フローは、この手順の一例です（詳細については、承認コード付与フロー（16-51 ページ）を参照）。

承認付与

図 16-20 の一般的な OAuth 承認フローの説明に示されているように、承認付与は、保護されたリソースへのアクセスの承認がリソース所有者によって付与されていることを表すクレデンシャルです。クライアントは承認付与を使用してアクセス トークンを取得します。OAuth 仕様では、承認付与のタイプとして、承認コード、暗黙、リソース所有者パスワード クレデンシャル、クライアント クレデンシャルの 4 つを定義しています。このドキュメントでは、以下に説明する 2 つのフローのみが関連します。

暗黙の付与フロー

暗黙の付与フローは、承認コード付与フローを単純化したものです。このフローでは、承認コード付与を発行する代わりに、承認サーバが直接、アクセス トークンをクライアントに発行します。中間クレデンシャルが発行されないことから。これは「暗黙」と呼ばれます。

このフローは、スクリプト言語を使用してブラウザに実装されたクライアントに対して最適化されています。このフローではアクセス トークンが直接発行されるため、クライアントの認証は行われません。したがって、アクセス トークンがリソース所有者だけでなく、リソース所有者のブラウザにアクセス可能な他のアプリケーションに漏れる可能性があります。

暗黙の付与フローは応答性に優れていますが（アクセス トークンの承認コード付与を交換するための追加トランザクションが不要であるため）、それほどセキュアではないフローとして見なすべきです。

また、シスコ ユニファイド コミュニケーション ソリューションのコンテキストでは、Jabber クライアントやその他のエンドポイントが OAuth 承認フローによって取得したアクセス トークンを使用して各種のシステム インターフェイスにアクセスします。そのため、暗黙の付与フローを使用する場合、それまで使用していたアクセス トークンの有効期限に達した時点で新しいアクセス トークンを取得するには、常に新しい承認手順が必要になることに注意してください。承認コード付与フローであれば、クライアントはリフレッシュ トークンも取得するため、エンド ユーザの認証を繰り返すことなく、リフレッシュ トークンを使用して新しいアクセス トークンを取得できます。

SAML ベアラー アサーション付与フロー

エンティティ（通常はサービス）は、エンド ユーザに代わり、発行されたアサーションを使用して、そのエンド ユーザに関連付けられた OAuth トークンを入手します。コラボレーション エッジでは、このフローのバリエーションを使用して、承認コードを取得するためにエッジ外部から接続するクライアントに代わってトークンを取得します。

承認コード付与フロー

このフローでは、クライアントとリソース所有者との間の仲介として承認サーバを使用します（図 16-21 を参照）。

図 16-21　承認コード付与フロー

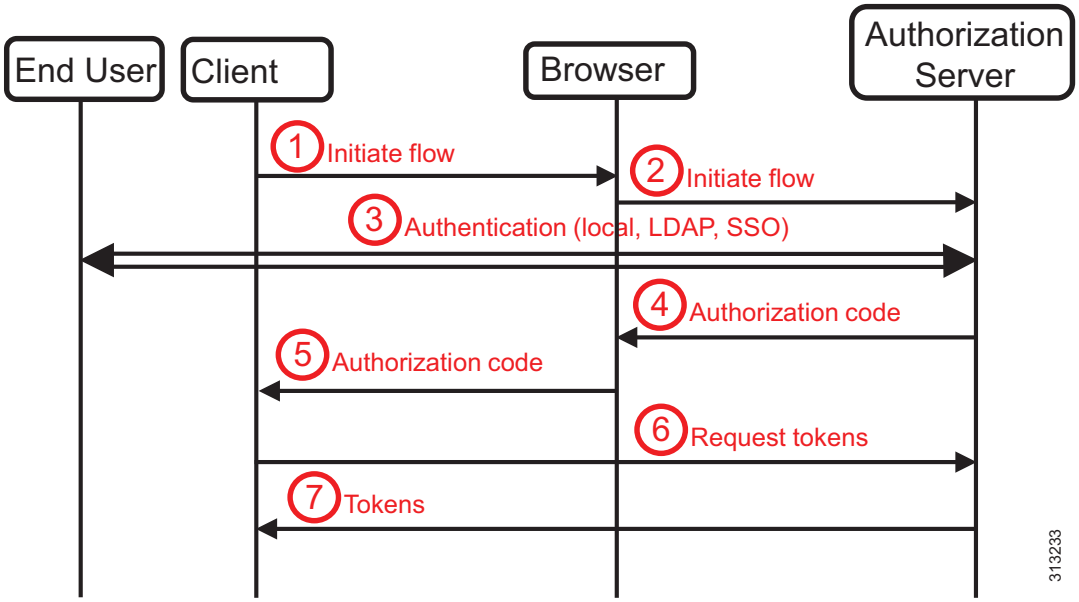


図 16-21 に、承認コード付与フローの詳細を示します。クライアントはエンド ユーザに直接承認付与（承認コード）を要求することはしません。代わりに、クライアントはエンド ユーザを承認サーバにリダイレクトします。フローではその後、承認コードが付与されエンド ユーザはクライアントに戻されます。このリダイレクションでは、エンド ユーザの Web ブラウザが使用されます。つまり、承認コード付与フローはブラウザ ベースです。このフローでのエンド ユーザのブラウザのリダイレクションでは、HTTP 302 リダイレクトを使用できるだけでなく、ブラウザに返される Web コンテンツでは JavaScript コードベースのリダイレクションも使用できます。

1. クライアント（たとえば Cisco Jabber）が承認フローを開始するために、エンド ユーザのブラウザを承認エンドポイントにリダイレクトします。シスコ ユニファイド コミュニケーション ソリューションでは、これは Unified CM 上の /ssosp/oauth/authorize です。
2. ブラウザが承認サーバ上のエンドポイントにアクセス（GET）します。この要求で、いくつものパラメータが渡されます。具体的には、クライアント ID、要求するアクセス レベル（スコープ）、一意の要求 ID、フローの最後に結果の承認コードを送信するリダイレクト URI などです。
3. 承認サーバがエンド ユーザを認証します。Unified CM 上のローカル エンド ユーザ テーブルに照らし合わせた認証、または LDAP バインドを使用した認証の場合は、エンド ユーザにユーザ名とパスワードの入力が求められます。ユーザ名とパスワードに基づく認証の場合は、承認エンドポイントに対する GET リクエストの結果として承認サーバが Web フォームを返します。エンド ユーザがこのフォームにクレデンシャルを入力すると、承認サーバがそのクレデンシャルを、ローカル エンド ユーザ テーブルに照らし合わせて検証するか、LDAP バインドをして設定済み LDAP サーバに照らし合わせて検証します。

   SSO が設定されていれば、承認サーバは SAML 2.0 Redirect/Post フローを開始します。この場合、Redirect/Post フローの終了時に SAML アサーションが承認サービスに送信されると、承認手順が完了します。

認証が成功した後、Cisco 承認サービスは、直ちに承認コード付与の発行を進めます。これは、エンド ユーザが、要求されたリソースを使用することをクライアント（たとえば Cisco Jabber）に承認したことを示します。

4. 承認コードをクライアントに付与するために、承認サーバはエンド ユーザのブラウザを、ステップ 1 と 2 で指定されたリダイレクト URI にリダイレクトします。リダイレクト URI には、承認コードと、ステップ 2 で識別された要求が組み込まれます。
5. ブラウザはこの URL にアクセスすることで、承認コードと指定された要求をクライアントに示します。クライアントは指定された要求を使用して、このイベントと、フローをトリガーした未処理のイベントを関連付けることができます。
6. クライアントは、前のステップで取得した承認コードを使用して、承認サービスにアクセス トークンを要求します。承認サービスに対するトークン要求は、クライアントのクレデンシャル（クライアント ID とシークレット）を使用して認証されます。また、ここでもクライアントはリダイレクション URI を渡します。
7. 承認サーバがクライアント認証を行って、リダイレクション URL をチェックします。有効であれば、応答としてアクセス トークンとリフレッシュ トークンを返します。

重要な点として、承認サーバはローカル認証、LDAP バインド、SSO を使用してエンド ユーザ認証を取得するため、リソース所有者の認証詳細（認証のタイプ、リソース所有者のクレデンシャルなど）がクライアントと共有されることは決してありません。クライアントが取得するのは承認コード付与のみです。

このフローには、他にも以下の利点があります。

- アクセス トークンは、クライアントが直接取得するため、リソース所有者のブラウザには公開されません。
- 承認コード付与をアクセス トークンと交換するためのトランザクションは、クライアント クレデンシャルを使用して認証されます。クライアント クレデンシャルを知らない限り、承認コード付与を単独で使用して、保護されたリソースにアクセスすることはできません。

承認コード付与フローは、Cisco Unified CM リリース 11.5(1) SU3 で導入されました。承認コード付与フローでリフレッシュ トークンを使用するには、[リフレッシュを使用した Oauth ログイン フロー（OAuth with Refresh Login Flow）] エンタープライズ パラメータを使用する必要があります。このパラメータはデフォルトで [無効（disabled）] に設定されていますが、このフローを有効にすることをお勧めします。リフレッシュ トークンを使用した承認コード付与フローを有効にした場合でも、後方互換性のために暗黙の付与フローは常にサポートされます。

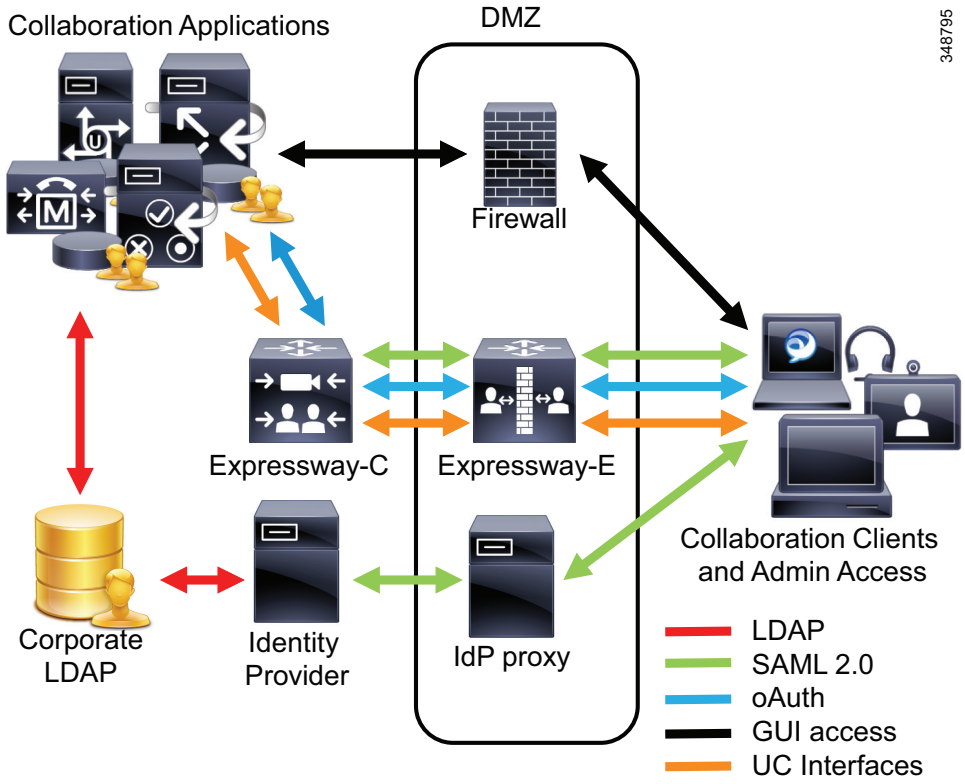
トークン

シスコ コラボレーション ソリューションで使用されるアクセス トークンのデフォルトの有効期間は、1 時間（3,600 秒）です。期限切れのアクセス トークンを使用すると、リソース サーバがサービスを拒否して、トークンが失効していることを示すエラーを返します。この場合、クライアントは新しいアクセス トークンを取得する必要があります。このような強制的なアクセス トークン更新を回避するため、シスコ コラボレーション クライアントは、トークン有効期間の 75% が経過するとトークン更新を開始するようになっています。アクセス トークンの有効期限が切れても、XMPP や SIP などのプロトコルを使用した既存のセッションに影響はありません。このようなセッションでは、セッションを確立する際（たとえば、SIP 登録の際）にだけ、アクセス トークンに基づく認証が行われるためです。

モバイルおよびリモート アクセス（MRA）の認証と承認

モバイルおよびリモート アクセス（MRA）を使用してコラボレーション エッジ経由で接続された企業外部のクライアントに OAuth でアクセスを承認するには、図 16-22 に示すように Cisco Expressway-E および Expressway-C 導入します。

図 16-22　コラボレーション エッジを使用した OAuth



コラボレーション エッジを介したエンドポイントとコラボレーション クライアントの登録では、（Expressway-E によってプロキシされる）Expressway-C の承認 API を使用することにより、OAuth を使用してアクセス トークンを取得できます。クライアントがこの承認エンドポイントを呼び出す際は、client_id、要求固有の状態 ID、ユーザ ID と併せて承認コード付与フローを使用するように指定する必要があります。ユーザを識別するには、ユーザ名、電子メール アドレス、またはユーザ ID を使用できます。Expressway-C 上の承認 API は、ユーザの認証方式に応じて、ブラウザを IdP にリダイレクトして SAML Redirect/Post 認証フローを開始するか、ローカル認証ページを表示します。ユーザの認証方式は、Expressway-C 上の MRA アクセス制御設定およびユーザのホーム クラスタ設定によって決まります。

- [認証パス（Authentication path）] 設定は、Unified CM LDAP、SAML SSO、またはこの両方を使用した認証が許可されるかどうかの設定を反映します。
- [OAuth トークンとリフレッシュ トークンによる承認（Authorize by OAuth token with refresh）] は、リフレッシュ トークンを使用した承認コード付与フローを有効にします。
- [OAuth トークンによる承認（Authorize by OAuth token）] は、レガシーの暗黙の承認付与フローを有効にします。Unified CM 12.*x* および現在の Jabber クライアントでは、このパラメータは必要ありません。

- すべての IP フォンおよび Cisco TelePresence エンドポイントで MRA の機能を使用できるようにするには、[ユーザ クレデンシャルによる承認（Authorize by user credential）] を有効にする必要があります。
- [内部認証の可用性をチェックする（Check for internal authentication availability）] を有効にしなければならないのは、すべての Unified CM クラスタが、リフレッシュ トークンを使用した OAuth をサポートする Unified CM のリリースに移行され、すべてのクラスタが共通の認証（SSO または Unified CM LDAP 基本認証）を使用するようになるまでの間だけです。このパラメータを有効にすると、Expressway-C はユーザのホーム Unified CM クラスタを判断してから、そのホーム クラスタでの認証設定を決定します。

必要とされる認証方式にしたがって、該当する承認フローが開始されます。

ローカル認証を使用した MRA サインオン

図 16-23 に、ユーザ名とパスワードに基づく認証で Cisco Expressway を使用してアクセス トークンを取得する場合に使用されるフローを示します。

図 16-23　ローカル認証での Expressway を使用した OAuth 承認

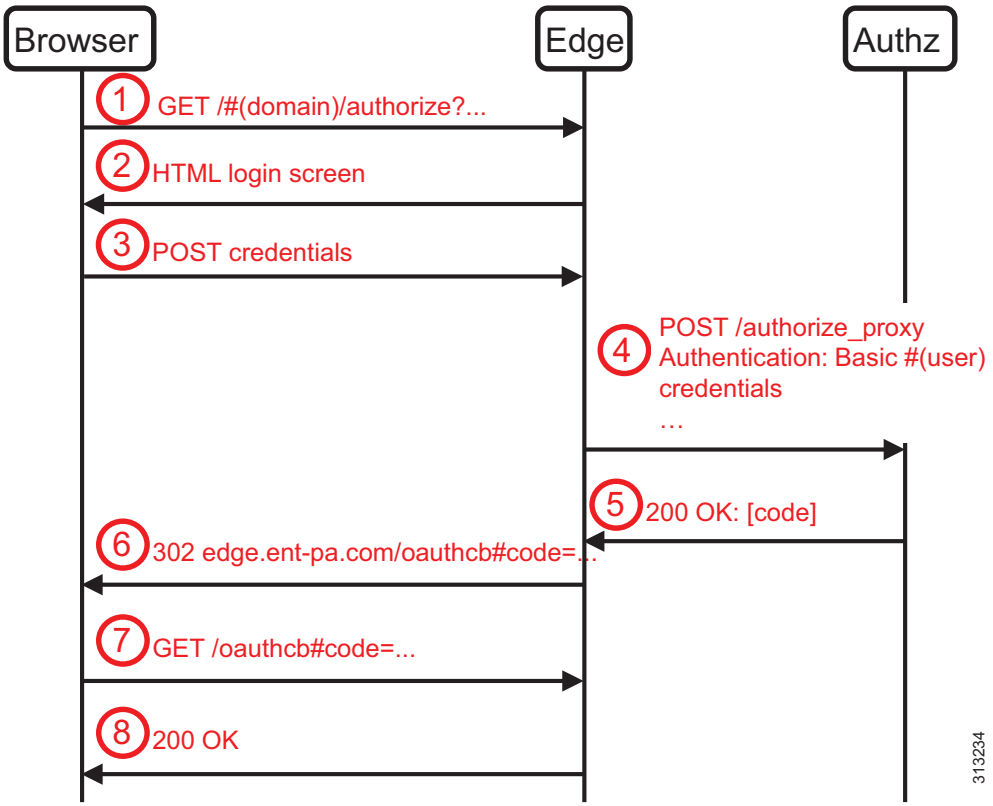


図 16-23 に示されているフローのステップは、以下のとおりです。

1. Jabber クライアントが Expressway 上の承認 API にアクセスするために Web ブラウザをリダイレクトします。要求には、その要求を一意に識別する状態情報、client_id、ユーザ ID が格納されます。
2. ユーザ ID に基づいて、Expressway はユーザ名とパスワードによる認証が必要であることを判別し、ユーザ クレデンシャルを入力するための Web フォームを表示する Web ページを返します。この Web フォームの非表示の入力フィールドを介して、ステップ 1 で取得したすべてのパラメータが渡されます。
3. ユーザ クレデンシャルが入力された後、Web フォームが Expressway に送り返されます。
4. Expressway が Unified CM 上の承認サービスに設定されている /authorize_proxy エンドポイントを使用して、承認コードを取得します。これは、SAML ベアラー アサーション付与フローのバリエーションです。この要求は、アプリケーション ユーザのユーザ名とパスワードを使用して認証されます。参照元アプリケーション ユーザは、Unified CM 上の承認サービスの AXL API にアクセスする権限が必要です。/authorize_proxy 要求には、先ほどキャッシュされたすべての承認パラメータが含まれています。
5. 承認サービスがクレデンシャルを検証します。それには、クレデンシャルをローカル エンドユーザ テーブルに照合するという方法、または LDAP バインドという方法が使用されます。検証後、承認サービスは承認コードを（コラボレーション）エッジに返します。
6. エッジはそのコードをキャッシュできますが、そのコードをクライアントに返す必要もあります。そのために、クライアントに 302 メッセージを返して、クライアント上のブラウザ インスタンスをエッジ上の OAuth コールバックにリダイレクトします。リダイレクトのターゲット URL には、承認コードに関する必要な情報が含まれています。
7. クライアント上のブラウザは、リダイレクションに従い、エッジ上の OAuth コールバック リソースにアクセスします。
8. 200 OK メッセージによって、エッジを使用した SSO フローが完了します。これで、クライアントは最終的な URL から承認コードを抽出できます。

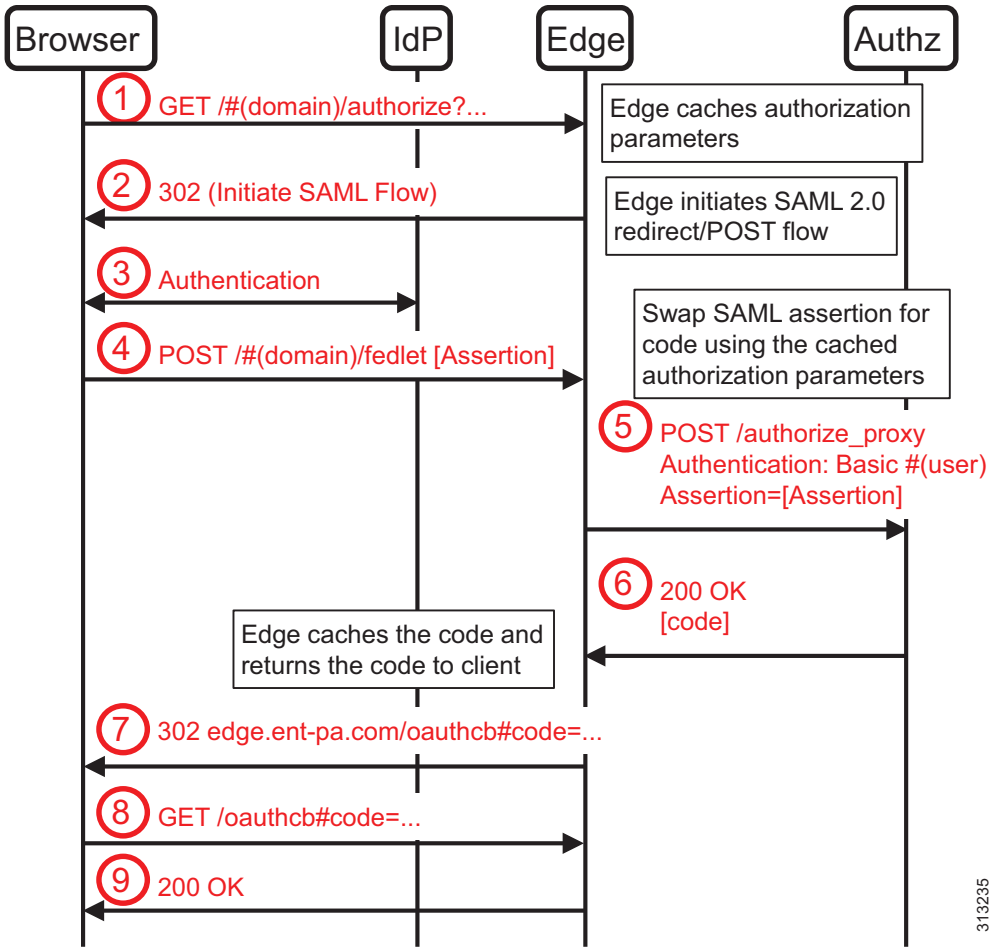
その結果、承認パラメータが Expressway 上でキャッシュされ、Jabber クライアントが承認コードを所有することになります。

Jabber は、再び Expressway の承認 API にアクセスすることで、この承認コードをアクセス トークンと交換できます。この場合の Expressway は、上記のフローのステップ 4 と 5 と同じように、承認サービスの access_token エンドポイントへの要求をプロキシします。

SSO 認証を使用した MRA サインオン

このフローは、ユーザ名とパスワードに基づく認証フローと非常によく似ています。このフローの場合、Cisco Expressway は SAML 2.0 Redirect/Post フローを使用して認証を取得し、クライアント上のブラウザが一般にアクセス可能な ID プロバイダーにリダイレクトされます。これは一般に顧客の DMZ 内にある IdP プロキシであり、企業内に導入された IdP のプロキシとして機能します。基本的に、DMZ 内の IdP プロキシは、企業 IdP 用の汎用 HTTPS リバース プロキシです。一部の IdP のベンダーは、IdP プロキシとして DMZ 内に IdP インスタンスをインストールするオプションを提供します。Expressway-E および Expressway-C プロキシはコラボレーション アプリケーションのサービスへのコラボレーション クライアント要求のみをプロキシします。パブリック DNS が企業 IdP の DNS 名を DMZ 内の IdP プロキシのパブリック IP アドレスに解決したことを確認することで、SAML 認証フローは DMZ 内の IdP プロキシにリダイレクトされますが、OAuth トークンを実現する OAuth 交換は Expressway-C および Expressway-E をパススルーし、Expressway-E は実際のクライアントのプロキシとして OAuth トークンを要求します。これは、図 16-24 に示すように、OAuth SAML ベアラー付与フローの一種です。

図 16-24　SSO 認証での Expressway を使用した OAuth 認証



1. OAuth トークンを取得するため、ブラウザは Edge 上の /authorize エンドポイントに HTTP GET リクエストを送信します。Edge 上の /authorize エンドポイントは、顧客ドメインを参照するプレフィックス エンコーディングを使用してアクセスされます。この説明でのエッジはコラボレーション エッジを実装する Expressway-C と Expressway-E のペアを指します。
2. Expressway が、ブラウザから IdP にリダイレクトする 302 応答を返すことによって、SP 起点の SAML 2.0 Redirect/POST 認証フローを開始します。さらに Edge は、後で実際の OAuth プロキシ要求で必要になるため、クライアント要求の承認パラメータをキャッシュします。
3. ブラウザと IdP は、ユーザを認証するために必要なメッセージを交換します。メッセージ交換は、IdP に設定されている認証方式によって異なります。
4. SAML 認証が成功すると、SAML 交換の最後の手順として、ブラウザはエッジ上のアサーションを使用するサービスに SAML アサーションを POST します。エッジは、この SAML アサーションを承認コードと交換する必要があります。
5. そのために、エッジは承認サービス上の /authorize_proxy エンドポイントを使用します。この要求は、アプリケーション ユーザのユーザ名とパスワードを使用して認証されます。参照元アプリケーション ユーザは、Unified CM 上の承認サービスの AXL API にアクセスする権限が必要です。/authorize_proxy 要求には、先ほどキャッシュされたすべての承認パラメータが含まれています。

6. このため、承認サービスは、認証されたエンド ユーザに必要な権限があるかどうかを確認できます。要求したサービスへのアクセスが認証されたユーザに承認されると、承認サービスは承認コードを発行し、その承認コードを 200 OK メッセージで返します。
7. エッジそのコードをキャッシュできますが、そのコードをクライアントに返す必要があります。そのために、クライアントに 302 メッセージを返して、クライアント上のブラウザ インスタンスをエッジ上の OAuth コールバックにリダイレクトします。リダイレクトのターゲット URL には、承認コードに関する必要な情報が含まれています。
8. クライアント上のブラウザは、リダイレクションに従い、エッジ上の OAuth コールバック リソースにアクセスします。
9. 200 OK メッセージによって、エッジを使用した SSO フローが完了します。これで、クライアントは最終的な URL から承認コードを抽出できます。

その結果、承認パラメータが Expressway 上でキャッシュされ、Jabber クライアントが承認コードを所有することになります。

Jabber は、再び Expressway の承認 API にアクセスすることで、この承認コードをアクセス トークンと交換できます。この場合の Expressway は、上記のフロー同じように、承認サービスの access_token エンドポイントへの要求をプロキシします。

OAuth トークンについて

ここでは、アクセス トークンとリフレッシュ トークン、トークンの有効期限、トークンの管理について説明します。

アクセス トークン

アクセス トークンは、認証サービスによってクライアントに発行されます。アクセス トークンの内容は、クライアントには判読できないものとなっていますが、クライアントがアクセス トークンの意味を理解する必要はありません。クライアントはアクセス トークンを、任意の文字列値として扱うためです。アクセス トークンは、クライアントからサービスに送信される要求を承認するためだけに使用されます。

Cisco Unified CM 上の承認サービスによって発行されるアクセス トークンは、自己完結型トークンです。これらの自己完結型トークンは、承認サービスにアクセスすることなく Unified Communications サービスにより検証できます。これらのアクセス トークンは RFC 7519 で規定されている JSON Web トークンであり、承認されたユーザ、有効期限、承認されるスコープに関する情報が含まれています。アクセス トークンは承認サービスによって暗号化され、デジタル署名が付けられます。

Unified Communications サービスは許可サーバにアクセスせずに、自己完結型トークンに基づいて承認をチェックするため、アクセス トークンの有効期間中に事前に承認されたアクセスを一元的に失効させる手段はありません。露出を制限するために、通常は、自己完結型アクセス トークンの有効期間は短くなっています。Cisco Unified CM 上の承認サービスによって発行されるアクセス トークンの有効期間は、デフォルトで 60 分に設定されます。この値は、1 分から 1440 分（1 日）までの範囲で設定できます。

Jabber では通常、現在のアクセス トークンの有効期間が残り 25 % になると新しいアクセス トークンの取得を試みます。つまり、有効期間が 60 分のトークンは 45 分後に更新されるということです。

リフレッシュ トークン

リフレッシュ トークンは、Cisco Unified CM 上の承認サービスによってクライアントに発行されます。リフレッシュ トークンの有効期間内であれば、クライアントは Cisco Unified CM 上の承認サービスにリフレッシュ トークンを提示することで、アクセス トークンを取得できます。その際、エンド ユーザの認証は必要にならないため、新しいアクセス トークンを取得するためのトランザクションは、ユーザ エクスペリエンスに影響を与えることなく非常に短時間で実行できます。リフレッシュ トークンの場合も、クライアントはその内容を判読することはできません。新しいアクセス トークンを取得するための要求は、クライアント クレデンシャル（クライアント ID、クライアント シークレット、およびリダイレクト URI）を使用して認証されます。

Unified CM 上の承認サービスによって発行されるリフレッシュ トークンの有効期間は、デフォルトで 60 日に設定されます。この値は、1 日から 1825 日（5 年）までの範囲で設定できます。

（注）　リフレッシュ トークンの有効期間を変更すると、承認サービスによって現在発行されているすべてのリフレッシュ トークンが無効になります。したがって、すべてのユーザが再認証を行って新しいリフレッシュ トークンを取得しなければならなくなります。

新しいリフレッシュ トークンを取得するには、改めて初めから最後まで承認フローに従わなければなりません。これには、エンド ユーザの認証が必要になります。Jabber クライアントはリフレッシュ トークンの有効期限が近づくとエンド ユーザに通知するため、エンド ユーザは新たに承認フローを開始することができます。

管理者は、特定のユーザのすべてのリフレッシュ トークンを失効させることができます。それには、Unified CM 上の **https://<*unifed_cm*>:8443/ssosp/token/revoke?user_id=<*uid*>** エンドポイントを使用します。ここで、*unified_cm* は Unified CM パブリッシャの IP アドレスまたはホスト名で置き換え、*uid* はリフレッシュ トークンを失効させる対象のユーザのユーザ ID で置き換えます。この要求の認証には、管理者ユーザのクレデンシャルを使用する必要があります。

トークンの署名キーと暗号キー

自己完結型アクセス トークンは、Cisco Unified CM 上の承認サービスによって暗号化され、デジタル署名されます。必要なキーは、Unified CM パブリッシャ ノードで作成されて、クラスタのすべてのノードに配布されます。Unified CM IM and Presence はクラスタ内のレプリケーションによってキーを取得しますが、Cisco Expressway と Unity Connection は Unified CM からキーをプルして、アクセス トークンの検証を有効にする必要があります。これらのキーにアクセスするには、Unified CM 上のトークン キー API を使用します。この API にアクセスするには、AXL アクセス権限を持つアプリケーション ユーザのクレデンシャルを使用した認証が必要です。Cisco Unity Connection では、Cisco Unity Connection 管理の [システム設定（System Setting）] タブにある [承認サーバ（Authz Server）] セクションで、承認サーバが定義されます。

管理者は、署名キーや暗号キーのセキュリティが侵害されていると判断した場合、キーを再生成することができます。これらのキーのいずれかを再生成すると、承認サービスによって発行されたすべてのアクセス トークンが無効になります。したがって、すべてのクライアントが新しいトークンを取得しなければならなくなり、それによってすべてのエンド ユーザの再認証が必要になります。

署名キーを再生成するには、**set key regen authz signing** CLI コマンドを使用します。暗号キーを再生成するには、**set key regen authz encryption** CLI コマンドを使用します。現在の署名キーと暗号キーに関する情報は、**show key authz signing** と **show key authz encryption** CLI コマンドを使用して表示することができます。

スコープ

アクセス トークンには、スコープ要素が含まれています。スコープは、アクセス トークンの所有者に使用を許可する Unified Communications サービスを定義するものです。どのユーザに対しても、発行するアクセス トークンのスコープを定義するには、Cisco Unified CM 上のユーザ プロファイル設定の [モバイルおよびリモート アクセス ポリシー（Mobile and Remote Access Policy）] にある [Jabber デスクトップ クライアント ポリシー（Jabber Desktop Client Policy）] と [Jabber モバイル クライアント ポリシー（Jabber Mobile Client Policy）] を設定します。この 2 つの設定を使用して、管理者は Jabber デスクトップ クライアントと Jabber モバイル クライアントにそれぞれ異なるスコープを定義することができます。使用可能な値は、[サービスなし（No Service）]、[IM&Presence のみ（IM&Presence only）]、[IM&Presence コール、音声コール、ビデオ コール（IM&Presence, Voice and Video calls）] です。

クライアントが接続を確立する際は常に Expressway によってスコープがチェックされます。Expressway はアクセスが承認されているサービスへの接続だけを確立します。

PART 3

コラボレーション アプリケーションおよびサービス

このパートの内容

マニュアルのこのパートに含まれる章は、次のとおりです。

コラボレーション アプリケーションとサービスの概要

改訂日：2015 年 6 月 15 日

ネットワーク、コール ルーティング、および呼制御のインフラストラクチャを Cisco Unified Communications および Collaboration システム用に配置すると、追加のアプリケーションおよびサービスをそのインフラストラクチャの最上位に追加または階層化できます。既存の Cisco Unified Communications および Collaboration インフラストラクチャに配置できるアプリケーションおよびサービスは多数存在します。通常は、次のアプリケーションおよびサービスを配置します。

- Cisco Unified Communications Manager アプリケーション：IP テレフォニーに拡張機能を提供します。
- ボイス メッセージング：ボイスメール サービスおよびメッセージ待機インジケータを提供します。
- プレゼンス サービス：ユーザ デバイスおよびクライアントでのユーザの応答可能性を確認します。
- モビリティ サービス：企業外部のユーザに対して、企業レベルの Unified Communications および Collaboration 機能を提供します。
- コンタクト センター：大規模コールの呼処理、キューイング、およびモニタリングを行います。
- コール録音：後から検索したり再生したりするため、音声コールとビデオ コールを録音できます。

本 SRND のこの章では、上記のアプリケーションおよびサービスについて説明します。各章では、アプリケーションまたはサービスの概要を示したあと、アーキテクチャ、ハイ アベイラビリティ、キャパシティ プランニング、および設計上の考慮事項について説明します。各章では、アプリケーションおよびサービスの設計関連の側面を中心に説明します。製品固有のサポートおよび設定情報については、関連する製品マニュアルを参照してください。

SRND のこの部分に含まれる章は、次のとおりです。

- Cisco Unified CM アプリケーション（18-1 ページ）

  この章では、基礎的な IP テレフォニーに多数の動作および機能の拡張を提供する、Cisco Unified Communications Manager（Unified CM）アプリケーションについて説明します。外部の eXtensible Markup Language（XML）生産性向上アプリケーションまたは IP Phone Service は、Web サーバまたはほとんどの Cisco Unified IP Phone 上のクライアント（あるいはその両方）で実行できます。この章では、Cisco Extension Mobility、Cisco Unified Communications Manager Assistant、Cisco WebDialer などの追加の機能を提供する多数の Unified CM 統合アプリケーションについても説明します。

- シスコのボイス メッセージング（19-1 ページ）

  この章では、ボイス メッセージングについて説明します。ボイス メッセージングは、ほとんどの Unified Communications および Collaboration 導入において一般的に普及しているアプリケーションです。ボイス メッセージングを使用して、発信者はメッセージを送信し、システムのサブスクライバはメッセージを取得できます。この章では、ボイス メッセージング アプリケーションに関するメッセージング配置モデル、ボイス メッセージングの機能、ボイス メール ネットワーキング、および設計と配置のベスト プラクティスについて説明します。

- コラボレーションのインスタント メッセージングとプレゼンス（20-1 ページ）

  この章では、プレゼンス サービスについて説明します。生産性はユーザの応答可能性ベースのアプリケーションによって向上できるため、ほとんどの Unified Communications および Collaboration 配置において、プレゼンス サービスの重要性が高まっています。この章では、プレゼンスを定義し、プレゼンスのさまざまなコンポーネントと機能、プロトコル、配置モデル、冗長性、キャパシティ、および一般的な設計ガイドラインについて説明します。

- モバイル コラボレーション（21-1 ページ）

  この章では、モビリティ アプリケーションについて説明します。モビリティ アプリケーションは、モバイル従業員の増加、および Unified Communications および Collaboration 機能およびサービスに関する企業の境界があいまいになっていることからその重要性は非常に高く、モビリティ アプリケーションとサービスに対する需要が高まる結果となっています。この章では、モビリティのソリューション アーキテクチャ、機能、および設計と導入に関する考慮事項について説明します。

- Cisco Unified Contact Center（22-1 ページ）

  この章では、大容量コール センター アプリケーションを必要とする大規模な Unified Communications および Collaboration 導入にとって重要かつ不可欠な部分である、コンタクト センター ソリューションについて説明します。この章では、コール センター ソリューションのアーキテクチャ、機能、および設計と配置が及ぼす影響について説明します。

- コール録音とモニタリング（23-1 ページ）

  この章では、音声コールとビデオ コールの両方について、Cisco Unified Communications および Collaboration システムで使用可能なさまざまなコール録音ソリューションおよびモニタリング ソリューションの概要を示します。また、Cisco Unified Communications および Collaboration ソリューション内に組み込まれたコール録音ソリューションおよびモニタリング ソリューションの基本的な設計の考慮事項についても説明します。

アーキテクチャ

他のネットワークおよびアプリケーション テクノロジー システムの場合と同様に、Unified Communications および Collaboration アプリケーションとサービスは、基盤となるネットワーク インフラストラクチャとシステム インフラストラクチャの最上位で階層化する必要があります。音声メッセージ、リッチ メディア会議、プレゼンス、モビリティ、コンタクト センター、およびコール録音などの Unified Communications および Collaboration アプリケーションおよびサービスは、ネットワーク接続から呼制御、付加サービス、ダイヤル プラン、帯域幅管理、ゲートウェイ サービスなどの基本的な Unified Communications および Collaboration 機能までのすべての基礎となる Unified Communications および Collaboration のコール ルーティング、呼制御のインフラストラクチャ、およびネットワーク インフラストラクチャに依存します。たとえば、ボイス メッセージング アプリケーションとプレゼンス アプリケーションでは、ネットワーク インフラストラクチャを利用して、キャンパス サイト、支社サイト、およびインターネット上のユーザに到達します。また、これらのアプリケーションは、コール ルーティングと呼制御インフラストラクチャによって提供される、Unified Communications および Collaboration の音声とビデオのエンドポイント、コール ルーティング、PSTN 接続、およびメディア リソースに依存します。アプリケーションとサービスは、これらのインフラストラクチャ レイヤおよび基本的な Unified Communications および Collaboration サービスに依存しているだけでなく、多くの場合、完全に機能するために相互依存もしています。

ハイ アベイラビリティ

ネットワーク、コール ルーティング、および呼制御の各インフラストラクチャの場合と同様に、重要な Unified Communications および Collaboration アプリケーションとサービスでは、ネットワークやアプリケーションに障害が発生した場合でも必要な機能を引き続き使用できるように、ハイ アベイラビリティを実現する必要があります。発生する可能性のあるさまざまなタイプの障害、およびこれらの障害に関する設計上の考慮事項を理解することが重要となります。多くの Unified Communications および Collaboration アプリケーションが他のアプリケーションやサービスに依存しているため、場合によっては、単一のサーバまたは機能の障害が、複数のサービスに影響を及ぼすことがあります。たとえば、コンタクト センター配置のさまざまなアプリケーション サービス コンポーネントが適切に機能できる場合でも、この配置において、コール センター アプリケーションへのコールのルーティングが呼制御サーバに依存していると、すべての呼制御サーバに障害が発生したとき、コンタクト センターが事実上使用できなくなる場合があります。

ボイス メッセージングやモバイル コラボレーションなどのアプリケーションとサービスの場合、ハイ アベイラビリティに関する考慮事項には、ネットワーク接続やアプリケーション サーバの障害が原因で機能が一時的に失われ、その結果、発信者がメッセージを残すことができない、ユーザがメッセージを取得できない、ユーザが会議をスケジュールできない、およびユーザが会議に参加できない、などの状況が発生することが含まれます。また、ボイス メッセージングおよびモバイル コラボレーション アプリケーションの発信者とユーザのフェールオーバーに関する考慮事項には、特定の障害が発生した場合に、エンド ユーザがサービスに引き続きアクセスできるように、冗長なリソースによって一部の機能を処理できるようにするというシナリオが含まれます。

また、ハイ アベイラビリティの考慮事項は、プレゼンスやモビリティなどのサービスに関する考慮事項でもあります。ネットワーク接続の中断またはサーバの障害が発生すると、通常、機能が低下し、場合によっては、機能が完全に失われます。プレゼンス サービスの場合、このことは、一部またはすべてのデバイスおよびクライアントで、プレゼンスや可用性の更新を送受信できなくなることを意味することがあります。モビリティ サービスの場合、ハイ アベイラビリティの考慮事項には、2 ステージ ダイヤリングまたは Dial-via-office などの特定の機能の喪失の可能性、またはシングル ナンバー リーチなどの機能の低下（会社の電話または携帯電話のいずれかだけが鳴る結果となる）が含まれます。さらに、一部の障害シナリオでは、完全な機能を再度使用するために、会社のエンドポイントおよびモバイル クライアントを再登録し、再接続や最認証を行うことが必要となります。

コンタクト センターの配置の場合、数多くのサーバとコンポーネントに対して、ハイ アベイラビリティを考慮する必要があります。通常、独立した単一サーバまたは単一コンポーネントの障害は、そのサーバまたはコンポーネントに冗長性がある限り、機能や機能性を失うことなく対処できます。これ以外の場合には、複数のサーバまたはコンポーネントの損失によって、通常、一部の機能や機能性が失われます。すべての呼制御サーバなどの特定のコンポーネントが完全に失われたシナリオでは、より深刻な機能の喪失が発生することがあります。

コラボレーション クライアントおよびアプリケーションについて考慮する場合は、ハイ アベイラビリティが特に重要となります。特定のコラボレーション機能や機能性が障害シナリオで使用できなくなるだけでなく、場合によっては、プレゼンス対応クライアントがネットワークに接続できなくなり、登録およびコールの発信や受信などの基本的な機能でさえ使用できなくなる可能性があります。また、クライアントやデバイスが、サービスを再度提供するために、再接続および再認証する必要がある場合もあります。

キャパシティ プランニング

ネットワーク、コール ルーティング、および呼制御インフラストラクチャは、個々のコンポーネントとシステム全体のキャパシティおよびスケーラビリティを理解したうえで、設計および展開する必要があります。同様に、Unified Communications および Collaboration アプリケーションとサービスの配置は、キャパシティとスケーラビリティの考慮事項に注意して設計する必要があります。さまざまな Unified Communications および Collaboration アプリケーションを配置する場合は、アプリケーション自体のスケーラビリティの考慮が重要となるだけでなく、基盤となるインフラストラクチャのスケーラビリティについても考慮する必要があります。ネットワーク インフラストラクチャは、使用可能な帯域幅を持ち、アプリケーションによって発生する追加のトラフィック負荷を処理できる必要があります。同様に、コール ルーティングと呼制御のインフラストラクチャでは、ユーザとデバイスの設定および登録以外に、プロトコルと接続に関するアプリケーション統合の負荷を処理できる必要があります。たとえば、モビリティ、プレゼンス、コンタクト センターなどのアプリケーションとサービスでは、ユーザ、デバイス、および機能に関して、これらの個々のアプリケーションに対するキャパシティの暗黙的要件がありますが、コンピュータ テレフォニー インテグレーション（CTI）などの接続とプロトコルを処理する基盤インフラストラクチャのスケーラビリティも、同様に重要となります。モビリティ、プレゼンス、またはコンタクト センター アプリケーションが、多数の CTI 接続をサポートできる一方で、基盤となる呼制御およびコール ルーティングのインフラストラクチャが、アプリケーションまたはサービスによって追加された CTI 負荷を処理するために使用できるキャパシティを持っていない場合があります。

ボイス メッセージングやリッチ メディア会議などのアプリケーションとサービスの場合、キャパシティ プランニングの考慮事項には、メールボックスまたはユーザの数、メールボックス サイズ、音声ポートとビデオ ポート、MCU セッションなどが含まれます。基盤となるネットワーク、コール ルーティング、および呼制御の各インフラストラクチャが追加の負荷を処理できると想定すると、ほとんどの場合、アプリケーション サーバや MCU を増やしたり、サーバや MCU ハードウェアを大容量モデルにアップグレードすることで、キャパシティを追加できます。

また、キャパシティ プランニングの考慮事項は、プレゼンスやモビリティなどのサービスに関する考慮事項でもあります。スケーラビリティを考慮する必要があるのは、設定済みまたはサポート対象のユーザとデバイスの数などの項目だけでなく、アプリケーションとサービス間の統合と接続の数も含まれます。2 ステージ ダイヤリングおよび Dial-via-office コールの量は、呼制御機能および PSTN ゲートウェイ機能の両方の観点から、モビリティ アプリケーションにとって特別な考慮事項になります。一方、プレゼンス サービスの場合、スケーラビリティに関する重要な考慮事項には、プレゼンス ステータスの変更の頻度、およびネットワークへのこれらの変更の伝達以外に、テキストまたはインスタント メッセージの量が含まれます。通常、追加のアプリケーション サーバまたはハードウェアのアップグレードによって、これらのアプリケーションおよびサービスのキャパシティは増加しますが、基盤となるコール ルーティング インフラストラクチャと呼制御インフラストラクチャが、増加したすべての負荷を処理できる必要があります。

コンタクト センターの配置は、スケーラビリティの考慮事項という点では、他のアプリケーションおよびサービスと変わりません。当然、コールを処理するエージェントとエージェント デバイスの数は、ユーザとデバイスの設定および登録において重要となります。ただし、コンタクト センターの配置のキャパシティという観点となると、主要な考慮事項は、コンタクト センターでは一般的な多数の最繁時呼数（BHCA）、および呼制御インフラストラクチャとルーティング インフラストラクチャへの CTI 統合の数です。

コラボレーション クライアントおよびアプリケーションのキャパシティ プランニングを考慮する場合は、デバイスの登録および設定が、スケーラビリティの考慮事項として最も重要となります。ただし、プレゼンスやメッセージングなどのバックエンド アプリケーションおよびサービスには、スケーラビリティに関する他の暗黙的要件があります。また、さまざまなクライアントをサードパーティ製のアプリケーションおよびインフラストラクチャとともに配置または統合する場合は、これらのサードパーティ製の配置でサポートされているキャパシティを考慮することも必要となります。

システム サイジング、キャパシティ プランニング、およびサイジングに関連する配置上の考慮事項の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

Cisco Unified CM アプリケーション

改訂日：2018 年 3 月 1 日

Cisco Unified CM アプリケーションは、基礎的な IP テレフォニーに多数の動作および機能の拡張を提供します。外部の eXtensible Markup Language（XML）生産性向上アプリケーションまたは IP Phone Service は、Web サーバまたはほとんどの Cisco Unified IP Phone 上のクライアント（あるいはその両方）で実行できます。たとえば、ユーザのデスク上の IP Phone を使用して、株式相場、天気情報、フライト情報など各種の Web ベースの情報を取得できます。また、カスタム IP Phone サービス アプリケーションを作成すると、ユーザが在庫を追跡したり、時間単位で顧客に課金したり、会議室の環境（照明、ビデオ画面、室温など）を制御できます。Cisco Unified CM には、次に示すような追加機能を提供する統合アプリケーションも多数あります。

- Cisco Extension Mobility（EM）

  エクステンション モビリティ（EM）機能では、モバイル ユーザがその電話機にログインすることで、一時的に Cisco Unified IP Phone をそのユーザ用に設定できます。

- Cisco Unified Communications Manager Assistant（Unified CM Assistant）

  Unified CM Assistant は、アシスタントが 1 人以上のマネージャあて着信電話コールを処理できるようにする Cisco Unified CM に統合されたアプリケーションです。

- Cisco WebDialer

  WebDialer は Cisco Unified CM のクリックコール アプリケーションで、ユーザはサポートされる任意の電話デバイスを使用して自分の PC から簡単にコールを発信できます。

場合によっては、これらの統合アプリケーションが追加機能を提供するために、IP Phone Service を呼び出すこともあります。

この章では、次の Cisco Unified CM アプリケーションについて説明します。

- IP Phone サービス（18-2 ページ）
- エクステンション モビリティ（18-9 ページ）
- Unified CM Assistant（18-23 ページ）
- WebDialer（18-38 ページ）

またこの章では、次についても説明します。

- Cisco Unified Attendant Consoles（18-47 ページ）
- Cisco Paging Server（18-53 ページ）

この章の変更点

表 18-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 18-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Unified Attendant Consoles	Cisco Unified Attendant Consoles（18-47 ページ）	2018 年 3 月 1 日
その他の小さな更新と修正	この章の各項で説明	2018 年 3 月 1 日

IP Phone サービス

Cisco Unified IP Phone Service は、Web クライアントやサーバ、および Cisco Unified IP Phone の XML 機能を利用するアプリケーションです。Cisco Unified IP Phone のファームウェアには、限定的な Web ブラウジング機能を可能にするマイクロブラウザが含まれています。これらの電話サービス アプリケーションをユーザのデスクトップ電話機上で直接実行することで、付加価値サービスが提供され、生産性も向上する可能性があります。この章で *phone service* という用語は、Cisco Unified IP Phone を宛先および発信元としてコンテンツを送受信するアプリケーションを指します。

ここでは、IP Phone Service 機能の設計について次の項目を説明します。

- IP Phone サービスのアーキテクチャ（18-2 ページ）
- IP Phone サービスのハイ アベイラビリティ（18-6 ページ）
- IP Phone サービスのキャパシティ プランニング（18-8 ページ）
- IP Phone サービスの設計上の考慮事項（18-8 ページ）

IP Phone サービスのアーキテクチャ

IP Phone サービスは、次のような複数の方法で開始できます。

- ユーザ起動（プル）

  IP Phone ユーザが [サービス（Services）] または [アプリケーション（Applications）] ボタンを押すと、ユーザ加入電話サービスのリストを表示するために、HTTP GET メッセージが Cisco Unified CM に送信されます。図 18-1 は、この機能を示しています。

- 電話機起動（プル）

  IP Phone ファームウェア内で、アイドル時間の値は URL Idle Time パラメータによって設定できます。このタイムアウト値を超えた場合、IP Phone のファームウェア自体が URL Idle パラメータで指定されるアイドル状態の URL の場所に対して、HTTP GET を開始します。

- 電話サービス起動（プッシュ）

  電話サービス アプリケーションは、電話機に HTTP POST メッセージを送信することによって、IP Phone にコンテンツをプッシュできます。

(注)　電話サービスを呼び出すために電話機の Web クライアントが使用されるユーザ起動および電話機起動のプル機能とは異なり、電話サービス起動のプッシュ機能は、電話機の（クライアントではなく）Web サーバに（HTTP POST を通じて）コンテンツをポストすることによって、電話機上の処理を呼び出します。

図 18-1 は、ユーザが開始する IP Phone サービス処理の詳細を示しています。ユーザが [サービス（Services）] または [アプリケーション（Applications）] ボタンを押したとき、[サービスのプロビジョニング（Services Provisioning）] が [外部 URL（External URL）] または [両方（Both）] に設定されている場合、デフォルトでは、HTTP GET メッセージが IP Phone から Cisco Unified CM の getservicesmenu.jsp スクリプトに送信されます（ステップ 1）。URL Services パラメータを変更することによって、異なるスクリプトを指定できます。getservicesmenu.jsp スクリプトは、個々のユーザが加入している電話サービス URL ロケーションのリストを返します（ステップ 2）。HTTP 応答は、IP Phone にこのリストを返します（ステップ 3）。ユーザによって選択される追加の電話サービス メニュー オプションは、ユーザと選択された電話サービス アプリケーションを含む Web サービス間で HTTP メッセージングを継続します（ステップ 4）。

[サービスのプロビジョニング（Services Provisioning）] パラメータは、デフォルトで [内部（Internal）] に設定されます。この設定では、IP Phone は Unified CM に HTTP GET メッセージを送る代わりに、コンフィギュレーション ファイルから電話サービスのリストを取得します。

(注)　Service Provisioning エンタープライズ パラメータが内部にセットされる場合は、ステップ 1 からステップ 3 までがバイパスされ、電話サービスの処理はステップ 4 から開始します。

(注)　Cisco Unified IP Phone 7960 はコンフィギュレーション ファイルから電話サービスのリストを解析する機能を持たないため、[サービスのプロビジョニング（Service Provisioning）] エンタープライズ パラメータが [内部（Internal）] に設定されている場合でも、HTTP GET を Unified CM に送ってリストを取得します。

図 18-1　　ユーザ起動の IP Phone Service のアーキテクチャ

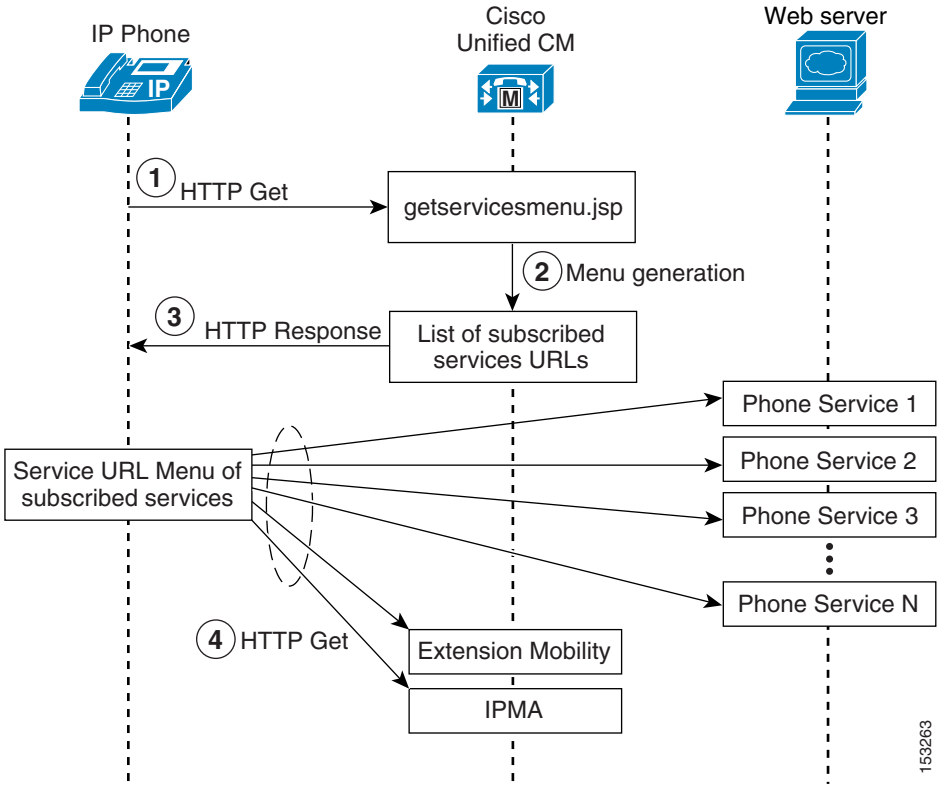
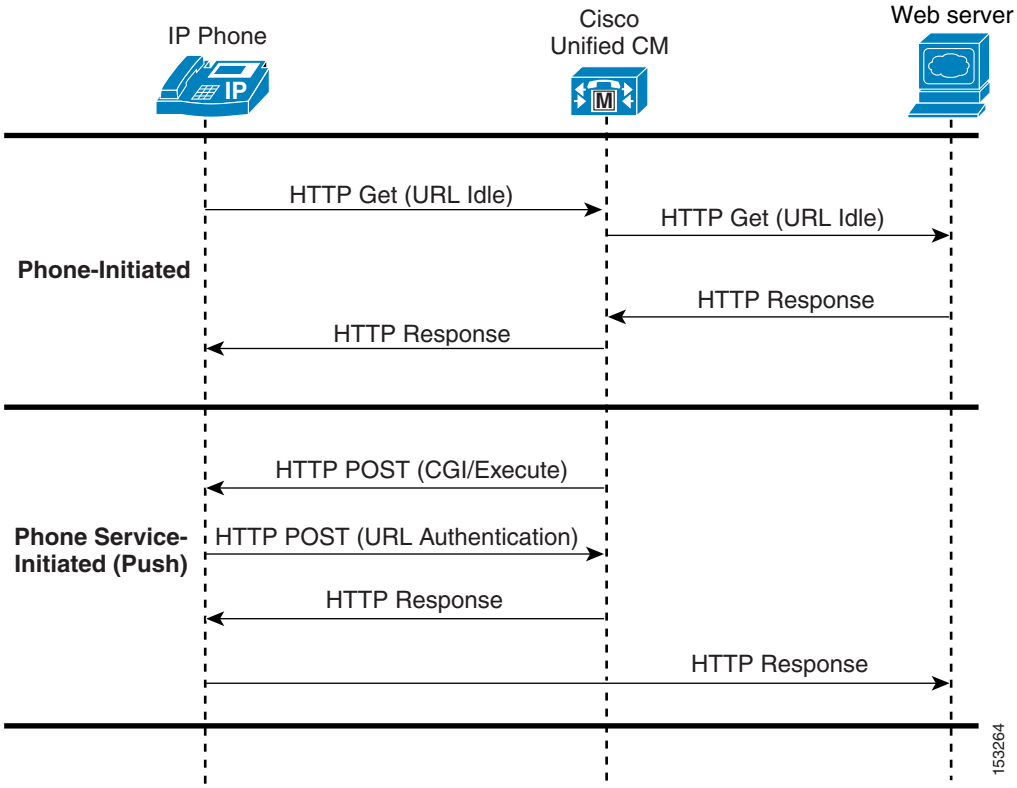


図 18-2 は、電話機起動と電話サービス起動の両方のプッシュ機能の例を示しています。電話機起動の例では、URL Idle Time に到達した時点で、自動的に、電話機から URL Idle パラメータで指定されたロケーションに HTTP GET が送信されます。HTTP GET は、Cisco Unified CM を通じて外部 Web サーバに転送されます。この Web サーバは HTTP 応答を返し、この応答は Cisco Unified CM によって電話機にリレーされ、電話機は画面にテキストまたはイメージ（あるいはその両方）を表示します。

電話サービス起動のプッシュの例で、外部 Web サーバ上の電話サービスは電話機の Web サーバに対して、Common Gateway Interface（CGI）または Execute 呼び出しで HTTP POST を送信します。CGI または Execute 呼び出しを実行する前に、電話機は URL Authentication パラメータで指定されるプロキシ認証サービスを使用して要求を認証します。このプロキシ認証サービスは、電話機に対する直接の要求を検証するための、電話機と Cisco Unified CM ディレクトリ間のインターフェイスを提供します。要求が認証された場合、Cisco Unified CM は電話機に HTTP 応答を転送します。次に、電話機の Web サーバは要求された処理を実行し、電話機は外部 Web サーバに HTTP 応答を返します。認証に失敗した場合、Cisco Unified CM は、HTTP 否定応答を転送し、電話機は要求された CGI または Execute 処理を実行しないで、HTTP 否定応答を外部 Web サーバに転送します。

図 18-2　電話機起動および電話サービス起動の IP Phone サービスのアーキテクチャ



XML Services に加えて、[Service Category] が [Java MIDlet] の新しいサービスを作成できます。Java MIDlet タイプのサービスが起動されると、設定された Service URL には、MIDlet JAD ファイルを取得できる URL を含みます。アプリケーション サーバは JAD ファイルの要求を受信すると、そのサーバは適切な JAR ファイルを対応デバイスに返します。この対応デバイスでは、電話の MIDlet インストーラがダウンロードし、処理しまします。

Cisco IP Phone の Java MIDlet サポートの詳細については、https://www.cisco.com の Cisco IP Phone データ シートを参照してください。

(注) 電話機は、設定ファイルをダウンロードした後、リストのサービスが変わっていないかどうか判断するためサービス設定を解析し、変わっている場合にはそのローカル（持続）サービス設定を更新します。変更されたサービスが Java MIDlet（これは明示的にプロビジョニングされ、電話機に保存されます）の場合は、次に、電話機は必要なインストール処理、アップグレード処理、ダウングレード処理、およびアンインストール処理を、設定ファイルにプロビジョニングされたものに応じて順次実行します。MIDlet インストールが失敗の場合、電話機がその設定ファイルをチェックする次回（ブート、リセット、または再スタート時）に MIDlet インストールを再試行します。

管理者は、設定されたサービスの [Service Type] を [IP Phone Services]、[Directories]、または [Messages] のいずれかに指定する追加機能を使用できます。これは、ユーザが IP phone で新しいサービスにアクセスするため押すボタンを管理する柔軟性を管理者に与えます。新しいサービスはオプションとして Enterprise Subscriptions と同様に設定できます。これにより、それらサービスは個々の電話機ごとに加入を更新する必要がなく、自動的にすべての IP phone に表示されます。さらに、サービスは Unified CM データベースからそのサービスを削除する必要がなく有効にできたり無効にできたりします。

（注）　Missed Calls、Placed Calls、および Corporate Directory などのデフォルトのサービスも無効にできます。これは、管理者が Service URL で指定されたデフォルト サービスをもとにしてカスタム サービスを作成できるようにします。

Unified CM は、非セキュア URL 以外に、HTTPS を使用してセキュア IP Phone サービス URL を設定する機能を提供します。HTTPS をサポートする電話機は、自動的にセキュア URL を使用します。IP Phone の信頼検証サービスとセキュリティ認証処理の詳細、および HTTPS をサポートする電話機の全リストについては、次の Web サイトで入手可能な最新バージョンの『*Security Guide for Cisco Unified Communications Manager*』で、HTTPS の情報を参照してください。

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

IP Phone サービスのハイ アベイラビリティ

電話機のユーザに対して信頼性の高いサービスを確保するには、システムの障害時に冗長システムにシームレスに移行することにより、高レベルのシステムの可用性を維持する必要があります。

[サービスのプロビジョニング（Services Provisioning）] で [内部（Internal）] にセットされる場合、電話機は加入した電話サービスが設定された設定ファイルを受信し、これら（および対応するサービス URL）をフラッシュ メモリに保存します。これにより電話機は、最初に Cisco CallManager IP Phone Service を参照せずにサービス URL に直接アクセスできます。Services Provisioning で内部にセットされる場合、Corporate および Personal Directories デフォルト サービスには電話機に組み込まれた追加レベルの冗長性もあります。これらサービスが選択された場合、電話機は適切な URL ストリングを使用して現在登録されている Unified CM に、HTTP メッセージの送信を試行します。したがって、電話機のデバイス プールの Unified CM Group の設定が、これらサービスの冗長性を提供します。

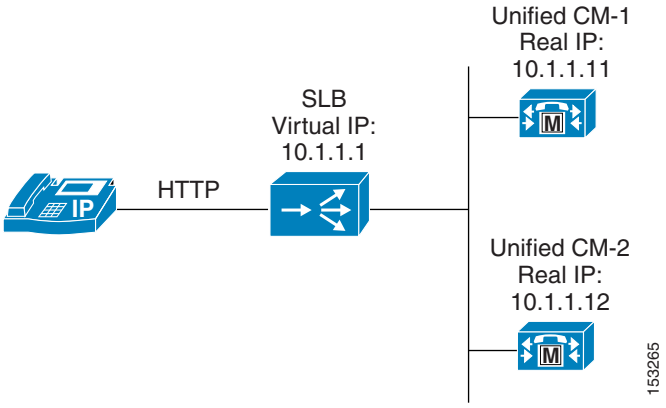
Services Provisioning が External URL、または両方にセットされる場合、電話サービスのほとんどのバックエンド処理は Web サーバで発生しますが、電話機はやはり加入電話サービスのそれらサービス URL を通知するには Unified CM に依存します。図 18-1 および図 18-2 に示す IP Phone サービス機能のアーキテクチャおよびメッセージ フローでは、次の 2 つの主な障害のシナリオを検討する必要があります。

障害シナリオ 1：Cisco Unified CallManager の Cisco Unified IP Phone Service サーバの障害

この場合の冗長性は、図 18-3 に示すように、ある種のサーバ ロード バランシング（SLB）に依存します。この SLB では、1 つ以上の Unified CM サーバを指すために仮想 IP アドレス（または DNS による解決可能なホスト名）が使用されます。この仮想 IP アドレス（または DNS による解決可能なホスト名）は、[URL サービス（URL Services）] パラメータの設定時に使用されます。SLB デバイスは、Unified CM サブスクライバ ノードの実 IP アドレスを使用して設定されます。このため、Cisco Unified CM サーバに障害が発生しても、電話機の [サービス（Services）] または [アプリケーション（Applications）] ボタンが押されたときに、IP Phone サービス加入リストは電話機に正常に返されます。また、Cisco Unified CM サーバで実行されるエクステンション モビリティおよび Unified CM Assistant などの電話サービスも、この方法によって冗長性を持つ可能性があります（エクステンション モビリティのハイ アベイラビリティ（18-17 ページ）および Unified CM Assistant のハイ アベイラビリティ（18-27 ページ）を参照）。

多くの SLB デバイスは、障害発生時の複数のサーバと自動転送要求のステータスをモニタするように設定できます。

図 18-3　電話サービスに冗長性を提供する方法



障害シナリオ 2：特定の IP Phone Service をホストしている外部 Web サーバの障害

このシナリオでは、Cisco Unified CM サーバへの接続は保持されますが、ユーザ加入電話サービスをホストしている Web サーバへのリンクに障害が発生します。[サービス（Services）] または [アプリケーション（Applications）] ボタンが押された場合でも IP Phone は引き続き Cisco Unified CM サーバにアクセスできるため、これは冗長性を提供するための比較的容易なシナリオです。この場合、IP Phone は Web サーバにアクセスする他の任意 HTTP クライアントに似ています。このため、（図 18-3 に示すような）SLB 機能を再び使用して、電話機から、ユーザ加入電話サービスをホストしている 1 つ以上の冗長 Web サーバに HTTP 要求を転送できます。

IP Phone サービスのキャパシティ プランニング

Cisco Unified IP Phone サービスの大部分は、HTTP クライアントとして機能します。ほとんどの場合、Unified CM は加入サービスのロケーションへの転送サーバとしてのみ使用されます。Unified CM は電話サービスへの転送サーバとして機能するため、ユーザが [サービス（Services）] キーを押して電話サービスを要求したときに、Unified CM へ与えるパフォーマンスの影響は通常最小限になります。しかし、多数の要求（1 分間に数百の要求）はサーバのパフォーマンスに影響する可能性があります。サーバ パフォーマンスへの影響をできる限り小さくするため、IP Phone サービスの外部 URL を指定する必要がない場合、通常は [サービスのプロビジョニング（Services Provisioning）] エンタープライズ パラメータを [内部（Internal）] 設定のままにすることを推奨します。[サービスのプロビジョニング（Services Provisioning）] を [外部 URL（External URL）] または [両方（Both）] に設定する必要がある場合、またはコンフィギュレーション ファイルからサービスのリストを取得する機能を持たない電話機（Cisco Unified IP Phone 7960 など）を大量に使用する場合は、Cisco Unified IP Phone のサービス リスト提供ノードを慎重に選択してください。たとえば、すでにパブリッシャの負荷が高くなっているのであれば、Unified CM パブリッシャの代わりに Unified CM TFTP サーバを使用することや、あまり多くのトラフィックを扱っていない Unified CM サブスクライバを使用することを検討してください。

（注）　エクステンション モビリティおよび Unified CM Assistant 電話サービスの場合、Unified CM は転送サーバ以上の役割を果たすので、パフォーマンスへのさらなる影響を検討する必要があります。これらのアプリケーションの特定のパフォーマンスおよびスケーラビリティの考慮事項については、エクステンション モビリティ（18-9 ページ）および Unified CM Assistant（18-23 ページ）の項を参照してください。

IP Phone はクライアントまたはサーバのいずれかであるため、IP Phone サービスで使用される必要帯域幅の推定は、Web 運用サーバにある HTTP コンテンツと同じテキストにアクセスする HTTP ブラウザの帯域幅の推定に似ています。

IP Phone サービスの設計上の考慮事項

統合されたエクステンション モビリティおよび Unified CM Assistant アプリケーションの電話サービスを除き、IP Phone サービスは独立したオフクラスタの Unified CM 以外の Web サーバに存在する必要があります。Unified CM サーバ ノードで、エクステンション モビリティおよび Unified CM Assistant 以外の電話サービスを実行することはサポートされていません。

ほとんどの Cisco IP Phone がテキストとグラフィックスを含むコンテンツをサポートしています。Cisco Unified IP Phone 7911G などの一部の電話機は、テキストベースの XML アプリケーションしかサポートしていません。Cisco TelePresence エンドポイントなどの一部のシスコのエンドポイントは Cisco IP Phone サービスをサポートしない場合があります。

エクステンション モビリティ

Cisco エクステンション モビリティ（EM）機能では、ユーザがその電話機にログインすることで、一時的に Cisco Unified IP Phone をユーザ個別の設定に設定することが可能です。ユーザがログインすると、IP Phone には、回線番号、スピード ダイヤル、サービス リンク、およびその他のユーザ固有の電話機のプロパティなど、ユーザの個別のデバイス プロファイル情報が設定されます。たとえば、ユーザ X がデスクに向かって電話機にログインした場合は、そのユーザのディレクトリ番号、スピード ダイヤル、およびその他のプロパティがその電話機に表示されますが、ユーザ Y が別のときに同じデスクを使用した場合は、ユーザ Y の情報が表示されます。EM 機能では、認証されたユーザのデバイス プロファイルに従って電話機が動的に設定されます。このアプリケーションの利点は、電話機が EM をサポートしている限り、物理的な場所に関係なく、ユーザが Cisco Unified CM クラスタ内の任意の電話機で自分の内線番号に接続できることです。

ここでは、エクステンション モビリティ機能の設計について次の項目を説明します。

エクステンション モビリティ対応 Unified CM サービス

EM アプリケーションは、Cisco エクステンション モビリティ サービスに依存します。このサービスは機能サービスであり、[サービスアビリティ（Serviceability）] ページから手動でアクティブにする必要があります。

EM は、インストール時にすべての Unified CM ノードで自動的にアクティブになる Cisco エクステンション モビリティ アプリケーション ネットワーク サービスにも依存します。

Cisco エクステンション モビリティ アプリケーション サービスは、EM ユーザ電話機と Cisco エクステンション モビリティ サービスとの間のインターフェイスを提供するネットワーク サービスです。また、Cisco エクステンション モビリティ アプリケーション サービスは、クラスタ内の変更通知インジケータにサブスクライブして、アクティブな Cisco エクステンション モビリティ サービスがあるクラスタ内のノードのリストを維持します。

エクステンション モビリティのアーキテクチャ

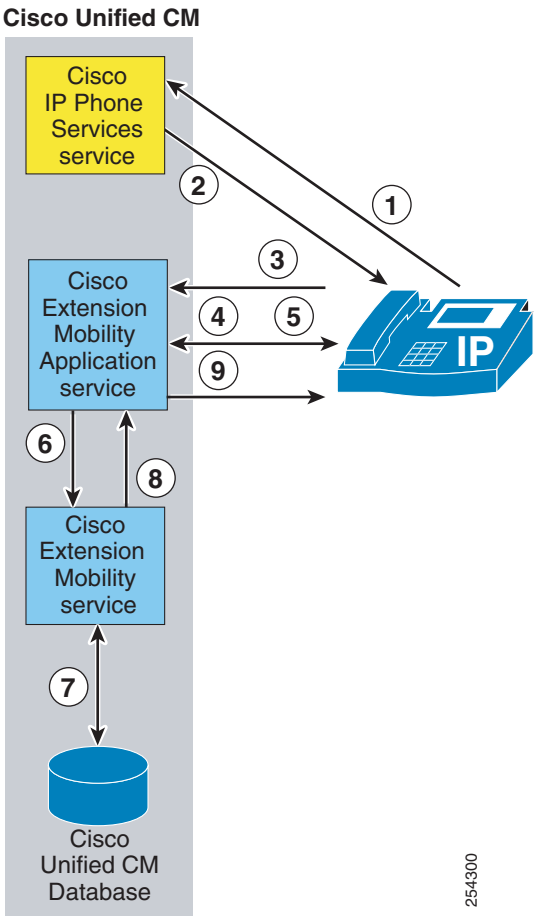
図 18-4 は、EM アプリケーションのメッセージ フローとアーキテクチャを示しています。電話機のユーザが EM アプリケーションにアクセスする場合、次の一連のイベントが発生します。

1. ユーザが電話機の [サービス（Services）] または [アプリケーション（Applications）] ボタンを押すと、[エンタープライズパラメータ設定（Enterprise Parameter configuration）] ページの [URL サービス（URL Services）] パラメータで指定された URL に発信されます（図 18-4 のステップ 1 を参照）。
2. HTTP/XML コールが IP Phone Service に対して生成され、このコールはユーザの電話機が加入しているすべてのサービスのリストを返します（図 18-4 のステップ 2 を参照）。

(注)　Services Provisioning エンタープライズ パラメータが内部に設定されている場合、ステップ 1 および 2 はバイパスされます。一方、[サービスのプロビジョニング(Services Provisioning)] が [外部 URL(External URL)] または [両方(Both)] に設定されている場合、ユーザが回線ボタンまたはスピード ダイヤル ボタンを押して、Cisco エクステンション モビリティ アプリケーション サービスへの直接コールを生成できるように、[サービス URL(Service URL)] ボタンをユーザの電話機の EM に対して設定できます。ステップ 1 およびステップ 2 もバイパスされます。

3. 次に、ユーザはエクステンション モビリティ電話サービスのリストを選択します。この選択によって、電話機と Cisco エクステンション モビリティ サービス間のインターフェイスの役割を果たす Cisco エクステンション モビリティ アプリケーション サービスに対して HTTP コールが生成されます(図 18-4 のステップ 3 を参照)。
4. 次に、Cisco エクステンション モビリティ アプリケーション サービスは、ユーザ ログイン クレデンシャル(ユーザ ID および PIN)を要求している電話機に XML 応答を返すか、またはユーザがすでにログインしている場合は、ユーザに電話機からログオフするかどうかを尋ねる応答を返します(図 18-4 のステップ 4 を参照)。
5. ユーザがログインしようとしている場合、そのユーザは電話機のキーパッドを使用して有効なユーザ ID および PIN を入力する必要があります。ユーザが [送信(Submit)] ソフトキーを押した後に、入力したユーザ ID および PIN を含む応答が、Cisco エクステンション モビリティ アプリケーション サービスに返されます(図 18-4 のステップ 5 を参照)。
6. 次に、Cisco エクステンション モビリティ アプリケーション サービスは、このログイン情報を Cisco エクステンション モビリティ サービスに転送します。このサービスは、Unified CM データベースと対話して、ユーザのクレデンシャルを検証します(図 18-4 のステップ 6 を参照)。Cisco エクステンション モビリティ アプリケーション サービスはクラスタの変更通知にサブスクライブして、Cisco エクステンション モビリティ サービスがアクティブになっているクラスタ内の全ノードのリストを維持します。その結果、同じ Unified CM ノードで Cisco エクステンション モビリティ サービスが実行されていない場合、Cisco エクステンション モビリティ アプリケーション サービスは、Cisco エクステンション モビリティ サービスが実行されている他の Unified CM ノードにログイン情報を転送します。
7. ユーザのクレデンシャルの検証に成功したときに、Cisco エクステンション モビリティ サービスも Unified CM データベースと対話して、適切なユーザ デバイス プロファイルを読み取って選択し、デバイスのプロファイルに基づいて電話機の設定に必要な変更を書き込みます(図 18-4 のステップ 7 を参照)。
8. これらの変更が加えられると、Cisco エクステンション モビリティ サービスは、Cisco エクステンション モビリティ アプリケーション サービスに成功応答を返します(図 18-4 のステップ 8 を参照)。
9. 次に Cisco エクステンション モビリティ アプリケーション サービスは電話機にリセット メッセージを送信し、電話機はリセットされ、新しい電話設定を受け入れます(図 18-4 のステップ 9 を参照)。

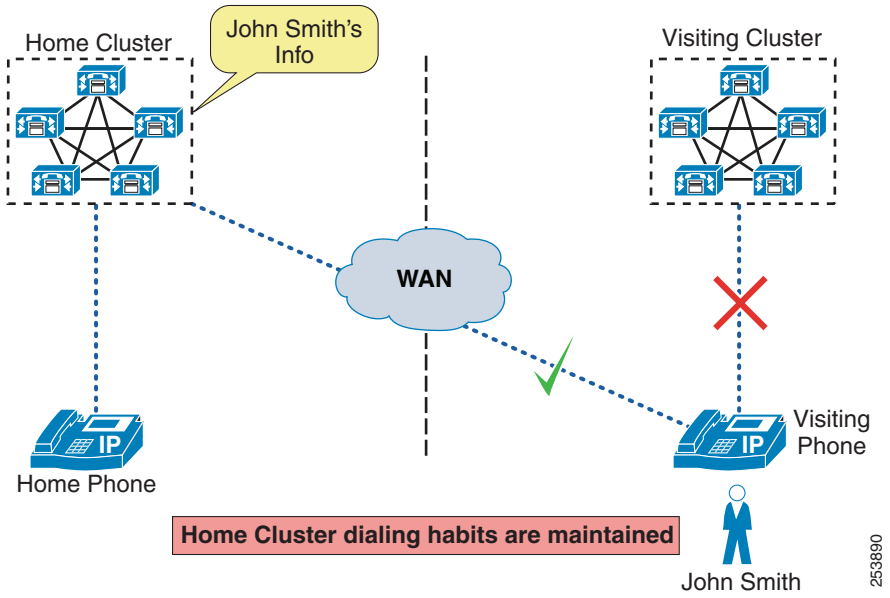
図 18-4　EM アプリケーションのアーキテクチャとメッセージ フロー



クラスタ間のエクステンション モビリティ（EMCC）

Unified CM は、クラスタ間のエクステンション モビリティ（EMCC）という新機能によって、企業内のクラスタ間でエクステンション モビリティ ログインを実行する機能を提供します。EMCC のアーキテクチャの概要を理解することが重要です。EMCC 機能はホーム クラスタおよび Visiting クラスタという概念を使用します。これらの用語は、ログインを実行するユーザの観点から定義されています。ユーザがオフィスに移動して電話機にログインしようとしたときに、この電話機が登録されているクラスタのデータベースにユーザの情報がない場合、このクラスタは Visiting クラスタと見なされ、この電話機は以降は Visiting 電話機と呼ばれます。図 18-5 に、ホーム クラスタと Visiting クラスタの概念を示します。

図 18-5　EMCC のホーム クラスタと Visiting クラスタ



Visiting クラスタ内の EM サービスは、Unified CM 内で構成されている各 EMCC リモート クラスタに照会を送信して、ユーザのホーム クラスタを見つけようとします。ユーザのホーム クラスタが肯定応答を返した場合、両方のクラスタの EM サービス間で通信が開始され、情報が交換されます。基本的にはデバイス情報がホーム クラスタのデータベースに取り込まれ、ホーム クラスタはこの Visiting 電話機の設定ファイルを作成できます。この設定ファイルには、Visiting クラスタからデバイス設定、ホーム クラスタから設定パラメータ、およびホーム クラスタ内のユーザのデバイス プロファイルが組み込まれます。ホーム クラスタの TFTP サーバにこの Visiting 電話機の設定ファイルができると、Visiting クラスタによって発行されたリセットによって、Visiting 電話機は Visiting クラスタから小さな設定をダウンロードし、これによってさらにホーム クラスタから証明書と完全な設定をダウンロードするよう指示されます。最終的には、Visiting 電話機はホーム クラスタにクロス登録されます。つまり、すべての呼制御シグナリングはホーム クラスタの Unified CM サブスクライバと Visiting 電話機の間で発生し、ユーザのホーム クラスタのダイヤリング手順が維持されます。

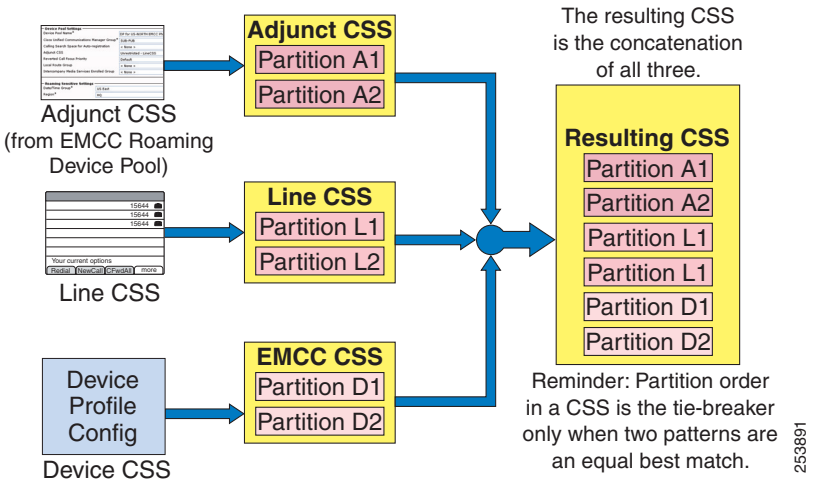
EMCC ログイン プロセスの段階的な説明については、次の Web サイトで入手可能な最新バージョンの『*Feature Configuration Guide for Cisco Unified Communications Manager*』で、クラスタ間のエクステンション モビリティの情報を参照してください。

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

呼処理

EMCC 呼処理動作はダイヤル プランの設計に影響するため、これを理解することも重要です。ユーザが Visiting クラスタの電話機にログインすると、ユーザがダイヤルした数字はホーム クラスタによって、Visiting 電話機の集合 Call Search Space（CSS）に従って分析されます。これは、Visiting 電話機用のホーム クラスタのデバイス プール（EMCC ローミング デバイス プールと呼ばれる）内の付属 CSS、ユーザのデバイス プロファイルに関連付けられたディレクトリ番号に設定された回線 CSS、およびユーザのデバイス プロファイルに設定された EMCC CSS を連結したものです。図 18-6 に、EMCC 電話機の結果の CSS を示します。

図 18-6　EMCC 電話機の結果の CSS



付加コーリング サーチ スペースは、新規のコール ルーティング設定パラメータです。このパラメータは、EMCC により使用され、Visiting クラスタからユーザに対して緊急番号のインターセプトおよびルーティングを行います。付加 CSS には、911、112、または 999 などのディレクトリ番号の付いたパーティションがあります。このパーティションは、Visiting クラスタにコールをルーティングして、そのコールが電話機の物理的な場所に対してローカルな緊急サービスに連絡できるようにします。付加コーリング サーチ スペースと EMCC ローミング デバイス プールの詳細、および Visiting 電話機に関連付ける方法については、次の Web サイトで入手可能な最新バージョンの『*Feature Configuration Guide for Cisco Unified Communications Manager*』で、クラスタ間のエクステンション モビリティの情報を参照してください。

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

(注)　EMCC 機能に関連付けられた EMCC ローミング デバイス プールは、デバイス モビリティ機能に関連付けられたローミング デバイス プールとは関係ありません。

EMCC ユーザは、コールを発信する際に、ホームの Unified CM のルートおよび番号計画が利用されることを承知しておく必要があります。たとえば、クラスタ Aからのユーザがクラスタ Bから電話機へログインするときに、そのすぐ隣にあるクラスタ B の電話機のディレクトリ番号に発信する場合、ユーザはクラスタ A からクラスタ B の電話機に発信する場合と同様に適切なパターンをダイヤルする必要があります。これは、ホーム クラスタがクラスタ A からクラスタ B へのクラスタ間トランク コールを開始する可能性があることを意味しますが、メディアは Visiting 電話機とリモート電話機の間でローカルに流れます。

EMCC クラスタを +E.164 の番号指定を使用して配置する場合、ユーザはすでに相手の電話番号の完全な番号をダイヤルすることに慣れているので、ダイヤリング手順を変更する必要はありません。

ルーティングされた PSTN コールでは、呼処理動作に影響する次の 2 つの異なる設定があります。

- ローカル ルート グループ(LRG)機能を使用しないルート パターン
- LRG 機能を使用するルート パターン

EMCC ログイン ユーザが PSTN コールをダイヤルすると、番号分析が（ルート リストおよびルート グループ コンストラクトを通じて、または音声ゲートウェイ宛に直接設定されて）最終的に音声ゲートウェイにつながるルート パターンと一致した場合、コールはゲートウェイに送信されます。標準ローカル ルート グループ（LRG）機能が使用されていない場合、コールはホーム クラスタに関連付けられた音声ゲートウェイを介します。したがって、メディアは Visiting 電話機から（通常は WAN を介して）音声ゲートウェイへ流れます。ルート パターンが、標準 LRG を使用するように設定されたルート リストにつながる場合、動作は変わります（LRG の詳細については、ローカル ルート グループ（14-32 ページ）を参照してください）。Unified CM のロジックは、EMCC ログイン デバイスについて標準 LRG を呼び出す必要がある場合、エンドポイントを EMCC デバイスとして認識し、PSTN コールを、指定された EMCC 固有の SIP トランクを介して、この Visiting 電話機が通常登録される Visiting クラスタに送信します。

（注）　EMCC トランク サービス タイプの SIP トランクは、クラスタごとに 1 つだけ必要です。このトランクには宛先情報は設定されていません。その情報は、EMCC リモート クラスタの追加および更新時に動的に収集されます。

Visiting クラスタ内の EMCC SIP トランクでコール Invite が受信されると、Visiting クラスタは再度、トランクの CSS に従って（または、Visiting 電話機の元のデバイス設定の CSS に従って）着信番号に対して番号分析を使用し、それに応じてコールをルーティングします。EMCC SIP トランク上の SIP Invite には追加情報が含まれています。つまり、Visiting 電話機のデバイス名です。これにより、Visiting クラスタはデータベース内にある Visiting 電話機の設定済みデバイス CSS を判別できます（必要な場合）。番号分析の結果が、最終的に標準 LRG を指すルート パターンとの一致である場合、Visiting クラスタはこの Visiting 電話機の設定済み標準 LRG を判別できます。Visiting クラスタ内の標準 LRG には一般に、Visiting クラスタに関連付けられた音声ゲートウェイが含まれているため、PSTN コールは、Visiting 電話機に対してローカルな音声ゲートウェイに送信されます。

緊急番号へのコールを考慮すると、LRG と LRG 以外の呼処理動作の違いは重要です。ローカル ルート グループ（LRG）の使用は、EMCC 配置の場合、クラスタ全体には必要ありませんが、EMCC ログイン電話機は、緊急コールを正しくルーティングするために LRG にアクセスする必要があります。Visiting 電話機に対して、ローカルである適切な音声ゲートウェイ経由でコールを発信できるように、緊急コールを Visiting クラスタに正しくルーティングするには LRG が必要です。EMCC デバイス用ローミング デバイス プール設定内の付加コーリング サーチ スペースにより、管理者は緊急ルート パターンを追加できます。緊急ルート パターンは、EMCC ログイン デバイスの LRG を使用しますが、ホーム クラスタ内の他のデバイスの緊急ダイヤリングに影響しません。前述したように、EMCC ログイン電話機は、（ジオロケーションにより）別のクラスタのすべての電話デバイスを示すデバイス プールに関連付けられます。デバイス プールの付加コーリング サーチ スペースでは、EMCC ログイン電話機の緊急コールだけを LRG 経由で送信するように、Visiting クラスタの緊急ルート パターンを設定できます。したがって、ホーム クラスタおよび Visiting クラスタが同じ緊急ルート パターンを使用している場合でも、EMCC ログイン電話機の緊急コールは、LRG 経由で Visiting クラスタにルーティングします。EMCC SIP トランク経由で Visiting クラスタでコールが受信されると、Visiting クラスタのダイヤル プランがコールのその後の処理を行います。

（注）　EMCC をサポートするクラスタが緊急呼処理に Cisco Emergency Responder も使用している場合、その導入をサポートするダイヤル プランの設定方法の詳細については、次の Web サイトで入手可能な最新バージョンの『*Cisco Emergency Responder Administration Guide*』を参照してください。
https://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-maintenance-guides-list.html。

（注）　標準 LRG が緊急ルート パターン用にすでに配置されており、ホーム クラスタと Visiting クラスタが同じ緊急ダイヤル ストリングを使用する場合、付加 CSS を使用する必要はありません。

詳細な EMCC 呼処理の例と設定については、次の Web サイトで入手可能な最新バージョンの『*Feature Configuration Guide for Cisco Unified Communications Manager*』で、クラスタ間のエクステンション モビリティの情報を参照してください。

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

メディア リソース

RSVP Agent を除くすべてのメディア リソースは、Visiting 電話機に割り当てられたデバイス プールのメディア リソース グループ リストに従って、ホーム クラスタから割り当てられます。会議、トランスコーディング、および保留音は、すべて通常どおり機能します。違いは、メディアは Visiting 電話機とメディア リソースの間を、（通常は）ホーム クラスタと Visiting クラスタを隔てる WAN を介してストリーミングされることです。EMCC ログイン ユーザが、RSVP Agent を使用する必要があるコールを行うと、Unified CM EMCC ロジックはそれが Visiting 電話機であることを判別でき、EMCC SIP トランクを介してリソース要求を Visiting 電話機が属するリモート クラスタに送信します。Visiting 電話機のデバイス名はこの要求に含まれています。これにより、Visiting クラスタは、通常この Visiting 電話機に割り当てられる RSVP Agent メディア リソースを確認でき、コールでの使用を割り当てることができます。

エクステンション モビリティのセキュリティ

Unified CM では、HTTPS を使用するエクステンション モビリティ セキュア サービス URL を作成できます。これにより、EM のログイン/ログアウトの交換全体が暗号化されます。エクステンション モビリティではセキュア サービス URL を設定することを推奨します。HTTPS をサポートしない電話機が EM 用に配置されている場合は、非セキュア サービス URL も設定する必要があります。セキュア サービス URL と非セキュア サービス URL がサービスに対して存在する場合、HTTPS をサポートする電話機は、デフォルトでセキュア サービス URL を使用します。HTTPS をサポートする電話機の全リストについては、次の Web サイトで入手可能な最新バージョンの『*Security Guide for Cisco Unified Communications Manager*』で、HTTPS の情報を参照してください。

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

EM 機能は、要求のソース IP アドレスを検証することによって、EM ログインおよびログアウト要求にオプション レベルのセキュリティを提供します。デフォルトでは、EM はこの要求の検証を実行しません。したがって、EM セキュリティを有効にするには、管理者はクラスタ全体のサービス パラメータ Validate IP Address を true に設定する必要があります。

EM ログインおよびログアウト HTTP 要求を処理する Web プロキシを実装する組織は、Allow Proxy サービス パラメータを true に設定する必要があります。プロキシ サーバは、HTTP 要求を転送している間に、そのホスト名とともに HTTP ヘッダーの via-field をセットします。デバイスと Unified CM の間に複数のプロキシ サーバがある場合で、すべてのサーバで要求が転送される場合は、次に HTTP ヘッダーの via-field にはフォワーディング パスで各プロキシ サーバのホスト名のカンマ区切りリストが必要になります。Allow Proxy サービス パラメータは、true に設定されている場合、Web プロキシを介して受信した EM ログインおよびログアウトが可能です。また、プロキシされた EM 要求はプロキシ サーバのソース IP アドレスを使用する場合、その IP アドレスは IP サービス パラメータの信頼できるリストにも設定する必要があります。

Unified CM 8.*x* から HTTPS および Security By Default がサポートされ、Unified CM 9.*x* ではセキュアな電話機が導入されたことで、EMCC のクラスタ間の連携には、クラスタ相互の通信をセキュアな方法で行うためにいくつかの段階が必要になりました。特に、EMCC に参加するすべてのクラスタで、Tomcat（Web）および TFTP 証明書を中央の sFTP サーバにエクスポートする必要があります。EMCC に使用する電話がセキュア モードになる場合は、CAPF 証明書もエクスポートする必要があります。これらのセキュリティ証明書はすべて結合され、各クラスタは結合済み証明書をインポートする必要があります。EMCC に参加する可能性がある新しいノードがクラスタに追加されるたびに、または既存のノードで証明書が更新された場合は、エクスポート、結合、およびインポートというプロセスを繰り返す必要があることに留意することが重要です。これらの手順はすべて、Unified CM Serviceability の管理によって簡素化されています。EMCC の設定の詳細については、次の Web サイトで入手可能な最新バージョンの『*Feature Configuration Guide for Cisco Unified Communications Manager*』で、クラスタ間のエクステンション モビリティの情報を参照してください。

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

セキュア モードの電話機のサポート

Cisco Unified CM 9.*x* から、ユーザはセキュア モードの電話機、つまり認証済みまたは暗号化済みのデバイス セキュリティ プロファイルを持つ電話機を使用して EMCC によりログインできるようになりました。ユーザがセキュア モードの電話機でログインする場合、デバイス セキュリティ プロファイル内のコンフィギュレーション（デバイス セキュリティ モード、TFTP 暗号化オプション、伝送プロトコルなど）がホーム クラスタに転送され、電話機は Visiting クラスタ内で本来使用されていたのと同じセキュア モードで動作することが可能になります。たとえば、電話機が Visiting クラスタ内の暗号化されたデバイス セキュリティ モードに設定され、ユーザが EMCC 経由でログインする場合、電話機は依然としてシグナリング用のセキュア TLS チャネルとメディア用 sRTP を持つ暗号化されたデバイス セキュリティ モードで動作します。ただし、1 つの条件として、ホーム クラスタのセキュリティ モードが混合モードに設定されていることが必要です。ホーム クラスタがノンセキュアに設定されている場合は、EMCC ログインに失敗します。電話機がセキュア モードでない場合、電話機は Visiting クラスタが混合モードまたはノンセキュア モードにあるかどうかに関係なく、EMCC ログイン後、ノンセキュア モードで動作し続けます。表 18-2 にこの動作を示します。

Unified CM 8.*x* は、EMCC をサポートしていますが、セキュア モードの電話機についてはサポートしていません。したがって、セキュア モード登録された電話機から Unified CM 8.*x* を実行中の Visiting クラスタへの EMCC ログイン試行は、ホーム クラスタで Unified CM 8.*x* 以降とそれ以降のリリースのどちらが実行されているかにかかわりなく、失敗します。同様に、セキュア モードの電話機から Unified CM 8.*x* を実行中のホーム クラスタへの EMCC ログイン試行は、Visiting クラスタで Unified CM 8.*x* とそれ以降のリリースのどちらが実行されているかにかかわりなく、失敗します。表 18-2 にこの動作を示します。

表 18-2　EMCC ログイン後の電話機のセキュリティ モード

Visiting クラスタ	Unified CM 8.*x* を実行中のホーム クラスタ	Unified CM 9.*x* 以降のリリースを実行中のホーム クラスタ	
	混合モードまたはノンセキュア モード	混合モード	ノンセキュア モード
セキュア モードの電話機。Visiting クラスタは Unified CM 8.*x* を実行中	EMCC ログインに失敗	EMCC ログインに失敗	EMCC ログインに失敗
セキュア モードの電話機。Visiting クラスタは Unified CM 9.*x* 以降のリリースを実行中	EMCC ログインに失敗	セキュア モード	EMCC ログインに失敗
ノンセキュア モードの電話機。Visiting クラスタは Unified CM 8.*x* 以降のリリースを実行中（混合モードまたはノンセキュア モードの Visiting クラスタ）	ノンセキュア モード	ノンセキュア モード	ノンセキュア モード

（注）　Cisco Unified CM 9.0 では、EMCC SIP トランクをセキュア プロファイルで設定できません。したがって、ローカル PSTN へのコールは、シグナリングにセキュア チャネルを使用しません。ただし、電話と PSTN ゲートウェイがセキュア モードで設定されている場合、メディアは暗号化されます。

エクステンション モビリティのハイ アベイラビリティ

図 18-4 に示す EM アーキテクチャに従って、Unified CM データベースの読み取りおよび書き込みが要求されます。EM はユーザに面した機能であって、データベースの書き込みは、EM がサブスクライバ ノードで実行できるかどうかに関係します。したがって、Unified CM パブリッシャが利用できない場合、その場合でも EM ログインおよびログアウトはできます。

冗長性の見地から、次のコンポーネント レベルの冗長性については、全面的な EM の復元性を得るよう検討する必要があります。

- Cisco CallManager Cisco IP Phone サービス

  CallManager Cisco IP Phone サービスのハイ アベイラビリティは、Services Provisioning サービス パラメータの使用、または Cisco CallManager Cisco IP Phone サービスを実行する複数の Unified CM ノードを指すロード バランサ デバイスの使用により実現されます。詳細については、IP Phone サービスのハイ アベイラビリティ（18-6 ページ）を参照してください。

- Cisco エクステンション モビリティ サービス

  Cisco エクステンション モビリティ サービスのハイ アベイラビリティは、Cisco エクステンション モビリティ サービスを複数の Unified CM ノードでアクティブにすることにより実現されます。

(注)　Cisco エクステンション モビリティ サービスは、3 つ以上のノードでアクティブにできますが、最大 2 つのノードが、ログイン/ログアウト要求を常にアクティブに処理します。ロード バランサを使用する場合は、2 つの Unified CM ノードのみにエクステンション モビリティ要求を送信するようにロード バランサを設定します。ロード バランサは、障害時のみ、Cisco エクステンション モビリティ サービスを実行するその他のノードに対してログイン/ログアウト リクエストの送信を開始します。

2 つの Unified CM ノード間の要求をロード バランシングしたり、冗長性を提供したりするため、サーバ ロード バランサ デバイスの導入を推奨します。サーバ ロード バランサがない場合、ロード バランシングは均等でなく、冗長性には手動で対応します。たとえば、2 つの EM IP Phone サービスをそれぞれの電話機で設定できます。1 つの Unified CM ノードが到達不能の場合、エンド ユーザはもう一方のノードに到達するために、もう一方の EM IP Phone サービスを手動で選択する必要があります。

(注)　EM IP Phone サービスに冗長性を提供することは、EM IP Phone サービスのリストからサービスを手動で選択する作業をエンド ユーザに任せることで可能になりますが、この方法の場合、ハイアベイラビリティの実現が困難になる可能性があります。ユーザが電話サービス メニュー(または割り当てられた機能キー)から選択可能になる EM IP Phone サービスを制御できないため、EM ログイン/ログアウト要求を処理する Unified CM ノード間で、EM ログイン/ログアウトのロード バランシングを確実にする方法はありません。さらに、EM サービスの応答に遅延が発生した場合のエンド ユーザの行動は、障害シナリオではよくある行動ですが、EM サービス コールをキャンセルして代替 EM IP Phone サービスを選択するというもので、たいていの場合は状況を悪化させます。これは、ネットワークのみならず、EM ログイン/ログアウト要求を処理する残りの Unified CM ノードでの輻輳および負荷の増大につながる場合があります。

Cisco エクステンション モビリティ サービスを実行する 2 つの Unified CM ノードを使用した配置は、1 分あたりのログイン/ログアウト要求の数に関して最高のキャパシティを提供します(詳細については、エクステンション モビリティのキャパシティ プランニング(18-20 ページ)を参照してください)。冗長性も提供します。ただし、障害が発生した場合は、1 つのノードしか残っていないので、ログイン/ログアウト要求のキャパシティは減少します。したがって、最高のログイン/ログアウトのキャパシティを実現して、このキャパシティを障害発生時にも維持するには、Cisco エクステンション モビリティ サービスを追加の Unified CM ノードでアクティブにする必要があります。ロード バランサは、任意の時点で 2 つの Unified CM ノードのみにエクステンション モビリティ要求を送信するように配置および設定する必要があります。1 つの Unified CM ノードで障害が発生すると、ロード バランサは 2 つの Unified CM ノードがエクステンション モビリティ要求を処理し続けるように、別の Unified CM ノードに対してエクステンション モビリティ ログイン/ログアウト要求の送信を開始できます。このため、エクステンション モビリティ キャパシティが維持されます。

(注)　複数の IP リストを持つ DNS A レコードまたは SRV レコードを使用した冗長な設計は推奨できません。DNS 要求に対して複数の IP アドレスが戻ると、電話はタイムアウトを待ってから次にリストされた IP アドレスを試します。ほとんどの場合は、この動作よりエンド ユーザにとって許容できない遅延が発生します。また、このために Cisco エクステンション モビリティ アプリケーション サービスが有効である 3 つ以上のサブスクライバ ノードによってログイン/ログアウト要求が処理される場合がありますが、そのような処理はサポートされていません。

EMCC では、管理者により、リモート クラスタで EM サービスを実行している Unified CM サブスクライバ ノードの 1 つの FQDN または IP アドレスを指定し、Unified CM Web 管理画面を経由してリモート クラスタが追加されます。2 つのクラスタ間の EM サービスは、Unified CM バージョンに関する情報、EMCC EM サービス通信の EM サービス ノードの順序付きのリスト、リモート クラスタで使用可能な EMCC SIP トランク サービス（PSTN アクセスまたは RSVP Agent、あるいはその両方）、および各 EMCC サービスの EMCC SIP トランク操作を処理する最大 3 つのリモート Unified CM ノードの順序付きのリストを提供します。HTTPS 経由の EMCC EM サービス通信には、ユーザのホーム クラスタの検索、EMCC ログイン時の情報交換、およびリモート クラスタ更新が含まれます。最初の更新で、リモート クラスタのエクステンション モビリティ アプリケーション サービスが照会され、そのリスト内の最初の 3 つの EM サービス ノードが返されます。この順序付きのリストによって、EMCC 通信に使用されるリモート クラスタ EM サービス ノードが決まります。

リモート クラスタは、EMCC の PSTN アクセス サービスおよび RSVP Agent サービスのプライマリ、セカンダリ、および 3 次オプションに関する情報を、それらのサービスの割り当て済み EMCC SIP トランクのデバイス プールに関連付けられた Unified CM Group から取得します。これにより、EMCC SIP トランクを処理するプライマリ Unified CM サブスクライバがオフラインの場合、EMCC SIP トランク コールはセカンダリ Unified CM サブスクライバなどによって処理されます。

電話機に EMCC 経由でログインすると、割り当て済み EMCC デバイス プール内に設定された Unified CM Group の形式で、電話機に冗長性が提供されます。Visiting 電話機がリモート サイトに設置されており、Visiting クラスタおよびホーム クラスタの両方が到達不能になる WAN 障害があった場合、Visiting クラスタの SRST リファレンスは、EMCC 電話機により維持されます。そのため、EMCC ログイン電話機は、設置されたサイト内の適切な SRST ルータに登録可能になっています。EMCC ログイン ユーザの DID は、この SRST サイトにあるローカル ゲートウェイに関連付けられることはほとんどないため、着信コールはユーザのホーム クラスタ上のコール転送ルールに基づいてルーティングされることになります。SRST モードの間、そのユーザは SRST フェールオーバー登録中に Visiting SRST サイトで設定されたダイヤル手順に適応する必要もあります。ネットワーク障害発生中の EMCC ログイン電話機の動作のさらなる例は、次の Web サイトで入手可能な最新バージョンの『*Feature Configuration Guide for Cisco Unified Communications Manager*』で、「Cisco Extension Mobility Cross Cluster」セクションを参照してください。

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

ホーム クラスタへの登録を可能にする EMCC 設定ファイルをダウンロードするために Visiting 電話機が使用する、デフォルトおよびバックアップの Unified CM TFTP サーバを設定することも推奨します。これは、[EMCC Feature Configuration] で設定します。

エクステンション モビリティのキャパシティ プランニング

Cisco エクステンション モビリティ アプリケーションを実行している単一の Unified CM の場合、Unified CM ノードが 7,500 人のユーザまたは 10,000 人のユーザ用の VM 構成で展開されているときのクラスタ全体の最大キャパシティは、1 分あたり 250 回のログインまたはログアウトです。Cisco エクステンション モビリティ ログインおよびログアウト機能は、ログイン/ログアウトのクラスタ キャパシティを増加するためにサブスクライバ ノードのペアに分散できます。ロード バランサ デバイスを使用できますが、手動で EM 負荷を 2 つのサブスクライバ ノード間で均等に分散するには、サブスクライバ ノードの 1 つを指している EM 電話サービスに加入している 1 つの電話機グループと、2 番めのサブスクライバ ノードを指している別の EM 電話サービスに加入している別の電話機グループの、2 つのグループに電話機を分割する必要があります。EM 負荷がこの方法で分散され、7,500 人のユーザまたは 10,000 人のユーザ用の VM 構成を使用した Unified CM ノード間で均等な場合、1 分あたりのクラスタ全体のキャパシティは最大で 375 回の順次ログインまたはログアウト（あるいはその両方）になります。

（注）　Cisco エクステンション モビリティ サービスは、冗長性を目的として 3 つ以上のノードでアクティブにできますが、最大 2 つのサブスクライバ ノードまでが同時にアクティブにログイン/ログアウト処理することをサポートしています。

（注）　EM セキュリティの有効化はパフォーマンスを低下しません。

EMCC ログイン/ログアウト処理は、クラスタ内 EM ログイン/ログアウトよりも多くの処理リソースを必要とします。したがって、サポートされるログイン/ログアウトの最大レートは低くなります。クラスタ内 EM ログイン/ログアウトがない場合、Unified CM は 7,500 人のユーザまたは 10,000 人のユーザ用の VM 構成を使用して、1 分あたり 75 回の EMCC ログイン/ログアウトの最大レートをサポートします。ほとんどの配置では、クラスタ内ログイン/ログアウトとクラスタ間ログイン/ログアウトの組み合わせが発生します。より一般的なこのシナリオでは、EMCC ログイン/ログアウトの混合（ホーム クラスタまたは Visiting クラスタのどちらとして機能する場合でも）は、1 分あたり 40 回のモデルにする必要があります。同時にクラスタ内 EM ログインは、シングル EM ログイン サーバを使用する場合、185 回のログイン/ログアウトのモデルにする必要があります。2 つの Unified CM ノードをデュアル EM サービス構成で展開し、7,500 人のユーザまたは 10,000 人のユーザ用の VM 構成を使用する場合、クラスタ内 EM ログインのレートは 1 分あたり 280 回のログイン/ログアウトにまで増加できます。

キャパシティ制限の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

EMCC ログイン デバイス（Visiting 電話機）は、クラスタ内の他のエンドポイントの 2 倍のリソースを消費します。EMCC ログイン デバイスの最大サポート数はクラスタあたり 2,500 台ですが、これによっても、クラスタあたりの他のデバイスの理論的な最大数は 30,000 から 25,000 に減少します。クラスタ内の他の登録デバイス数を削減しても、EMCC ログイン デバイスの最大サポート数は 2,500 台のままです。

クラスタに追加できる EMCC リモート クラスタ数に技術的な制限はありません。ただし、リモート クラスタ数が増えると、フルメッシュ要件によって EM サービスの負荷は増大します。サイト数が多い（10 を超える）場合、Cisco Real Time Monitoring Tool（RTMT）を使用して EM の CPU をモニタする必要があります。

エクステンション モビリティの設計上の考慮事項

次のガイドラインと制限は、Unified CM 環境内の EM の配置と動作に関連して適用されます。

- EM ユーザは、自動代替ルーティング（AAR）または Voice over PSTN（VoPSTN）、あるいはその両方の配置モデルが使用されている場合、クラスタ内のロケーションまたはサイト間で移動できません。

  EM 機能は、コール ルーティングを IP ネットワークの使用に依存します。E.164 PSTN 番号は静的で、PSTN はホーム サイトからの EM ユーザのディレクトリ番号（DN）の移動を考慮に入れられないため、PSTN を通じたコール ルーティングにはより多くの問題が伴います。AAR は、VoPSTN 配置モデルと同様に、コール ルーティングを PSTN に依存します。いずれの場合も、ロケーションおよびサイト間の EM ユーザの移動は、ユーザの移動するすべてのサイトが同じ AAR グループに属する場合にだけサポートされます。詳細については、エクステンション モビリティ（14-90 ページ）を参照してください。

- Cisco エクステンション モビリティ サービスまたはこのサービスを実行中のノードの再起動は、自動ログアウト設定に影響を与えます。

  Cisco エクステンション モビリティ サービスを停止するまたは再起動する場合、システムは最大ログイン間隔が経過後のすでにログインしているユーザを自動ログアウトしません。これらの電話機は、手動でログアウトするか、毎日のデータベース クリーンアップ処理が実行されるのを待つ必要があります（通常は深夜）。

Cisco TelePresence エンドポイントなどの一部のシスコのエンドポイントはエクステンション モビリティをサポートしない場合があります。

WebDialer では、エクステンション モビリティを使用してログインされた電話機だけを使用できます。詳細については、WebDialer（18-38 ページ）を参照してください。

クラスタ間のエクステンション モビリティ（EMCC）の設計上の考慮事項

EMCC を配置する場合、次の設計上の考慮事項が適用されます。

一般的な設計上の考慮事項

- Unified CM 9.1(1) 以前のリリースでは、EMCC ではすべてのユーザが企業内のすべてのクラスタにわたって一意である必要があります。LDAP 同期によって複数のクラスタの共通ユーザが保守されている場合は、ある種のフィルタリングを適用する必要があります。
- Unified CM 9.1(1) リリース以降、同じユーザ ID は複数のクラスタに存在できます。ただし、1 つのクラスタのみをユーザの**ホーム クラスタ**として定義する必要があります。ユーザがそのユーザ用に選択された**ホーム クラスタ**のオプションを含むクラスタにログインしようとすると、クラスタはローカル EM ログインを実行し、リモート クラスタによる EMCC ログインは実行しません。
- 使用を計画している機能との組み合わせで、クラスタ間のネットワーク遅延を考慮します。Visiting 電話機がホーム クラスタに登録されると、機能は動作します。ただし、特定の配置のネットワーク遅延によっては、すべてのアプリケーションおよび機能がユーザ要件を満たすとはかぎりません。特定のネットワークに対して機能の操作性を判断するためにテストが必要な場合があります。

  たとえば、EMCC は Visiting 電話機の動的 CTI 制御をサポートします。ただし、アプリケーションを介してオフフックが発行され、電話機がオフフックになるまでに 1 秒かかる場合、内勤者はこれを許容できてもコール センター エージェントは許容できない場合があります。

- ログイン プロセス中に電話機ロード ファームウェアは強制されません。代わりに、クロス登録によって新しい電話機ファームウェアがダウンロードされないように、Visiting クラスタの電話機ロード情報が保守されます。
- ホーム クラスタのロケールが Visiting クラスタのロケールと異なる場合、電話機は Visiting クラスタの TFTP サーバから新しいロケールをダウンロードします。そのロケールを使用できない場合、電話機はロケールを変更せず、Visiting クラスタのロケールを保守します。
- EMCC ログインの合計数は、Bulk Administration Tool（BAT）の EMCC 挿入デバイスの合計数によって制御されます。
- EMCC は、RSVP ベースおよび Unified CM のロケーション ベースのコール アドミッション制御をサポートします。
- RSVP Agent を除き、その他のすべてのメディア リソースは、EMCC ローミング デバイス プールに関連付けられたメディア リソース グループ リストに従って、ホーム クラスタから割り当てられます。
- オーディオおよびビデオ コーデックは、EMCC リージョン設定によって決まります。これらの設定は、EMCC 登録電話機の通常のリージョン設定よりも優先されます。すべての EMCC リージョン パラメータは、すべてのクラスタで同じ値を使用して設定する必要があります。異なる場合、そのクラスタの RSVP Agent は、リモート クラスタ更新操作によって使用不可になります。
- EMCC ローミング デバイス プールを正しく割り当てるには、EMCC 対応電話機に、デバイス設定またはデバイス プール経由で設定されたジオロケーションが必要です。

呼処理の設計上の考慮事項

- ユーザのディレクトリ番号の着信コールは常にホーム クラスタの音声ゲートウェイで受信されるため、着信コールでは RTP メディアは Visiting 電話機とホーム ゲートウェイ間を流れます。
- EMCC SIP トランクを介して送信されるコールは、ホーム クラスタの番号操作を通過します。コールされる番号には、Visiting クラスタのルート パターンと一致するために操作が必要な場合があります。
- ホーム クラスタの H.323 および SIP ゲートウェイの設定済みコーデック能力を確認します。たとえば、ホーム クラスタのゲートウェイが G.711 コールだけを受け入れるように設定されており、EMCC リージョンの帯域幅が 8 kbps（G.729）に設定されている場合、コールを完了するにはトランスコーダが必要です。あるいは、G.711 以外に G.729 を許可するように、H.323 または SIP ゲートウェイ ダイヤル ピアを設定できます。
- EMCC 緊急コールの発信者について、設計上の考慮事項を作成する必要があります。ダイヤル プラン設定によっては、Visiting クラスタのゲートウェイからの発呼側番号は、通常はホーム クラスタに関連付けられる、ユーザの DID である場合があります。このことにより、EMCC SIP トランクまたはルート パターンで着信する、または Visiting ゲートウェイで発信する発呼側番号を変換する必要があります。
- EMCC が Cisco Emergency Responder とともに配置される場合、Emergency Responder は、1 つの Emergency Responder クラスタによって処理されるすべてのクラスタに配置される必要があります。Visiting クラスタが Emergency Responder とともに配置され、ホーム クラスタは Emergency Responder とともに配置されない場合、コールが Visiting クラスタに戻ったときに Emergency Responder は Visiting 電話機を識別できません。

Unified CM Assistant

Cisco Unified CM Assistant は、Unified CM に統合されたアプリケーションです。これを使用すると、1 人または複数のマネージャに代わってアシスタントが着信コールを処理できます。Unified CM Assistant Console デスクトップ アプリケーションまたは Unified CM Assistant Console 電話サービスをアシスタントの電話機で使用すると、アシスタントが手早くマネージャの状態を確認し、コールをどうするかを決定できます。自分の電話機のソフトキーおよびサービス メニューを使用するか、または PC インターフェイスを介してキーボード ショートカット、ドロップダウン メニューを使用するか、あるいはマネージャのプロキシ回線へのコールのドラッグ アンド ドロップすることによって、アシスタントはコールを処理できます。

ここでは、Unified CM Assistant 機能の設計について次の項目を説明します。

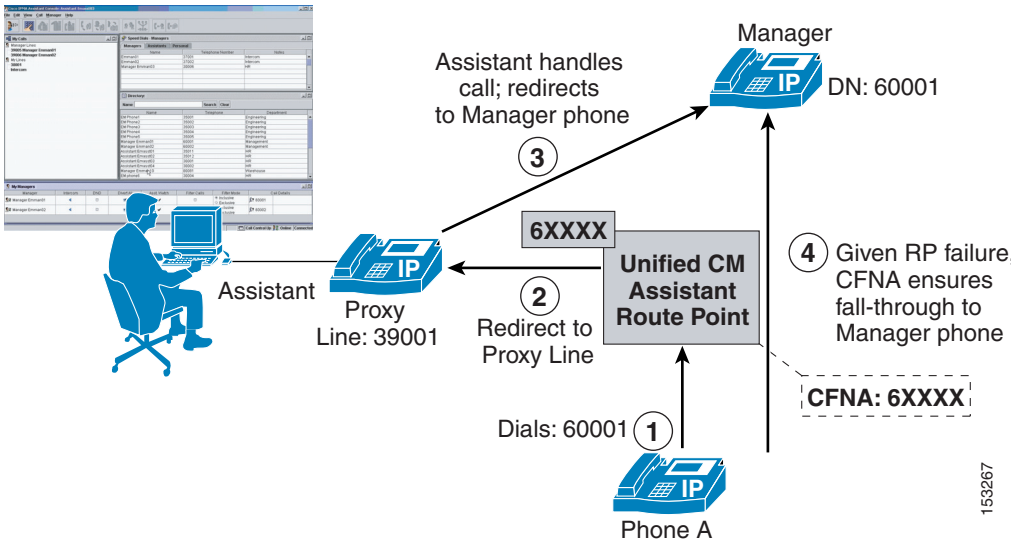
Unified CM Assistant のアーキテクチャ

Unified CM Assistant アプリケーションは、プロキシ回線モードとシェアド ライン モードの 2 つのモードで動作できます。各モードの動作と機能は異なり、それぞれに長所と短所があります。どちらのモードも、1 つのクラスタ内で設定できます。ただし、同一のアシスタントでモードを混合させることはできません。1 人以上のマネージャにサポートを提供している 1 人のアシスタントは、シェアド ライン モードまたはプロキシ回線モードのいずれかでこれらのマネージャをサポートできます。

Unified CM Assistant のプロキシ回線モード

図 18-7 は、プロキシ回線モードでの Unified CM Assistant の単純なコール フローを示しています。この例で、電話機 A は、ディレクトリ番号（DN）60001 でマネージャの電話機をコールします（ステップ 1）。CTI/Unified CM Assistant Route Point（RP）は、6XXXX に設定された DN に基づいてこのコールを代行受信します。次に、マネージャの DN に基づいて、コールはルート ポイントにより、アシスタントの電話機上のマネージャのプロキシ回線（DN:39001）に転送されます（ステップ 2）。次に、アシスタントはコールに応答または処理し、必要に応じてマネージャの電話機にコールを転送します（ステップ 3）。Unified CM Assistant アプリケーションの障害、または Unified CM Assistant RP の障害が発生した場合に、マネージャの DN へのコールがマネージャの電話機を直接呼び出すよう、RP の Call Forward No Answer（CFNA）の 6XXXX 設定による呼び出しメカニズムが存在します（ステップ 4）。

図 18-7　Unified CM Assistant のプロキシ回線モード

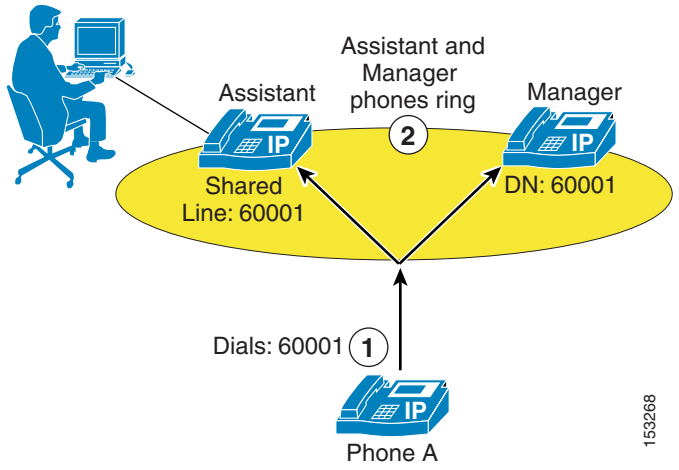


(注)　図 18-7 に示す CFNA による呼び出しメカニズムでは、Unified CM Assistant RP のディレクトリ番号設定ページの [Forward No Answer Internal] フィールドと [Forward No Answer External] フィールドの両方で、Unified CM Assistant RP ディレクトリ番号と同じ集約番号桁の設定が必要です。また、これらの各コール転送パラメータのコーリング サーチ スペース（CSS）フィールドは、Unified CM Assistant RP または Unified CM Assistant アプリケーションに障害が発生した場合にマネージャの電話機の DN に到達できるように、マネージャの電話機の DN が設定されたパーティションを含むコーリング サーチ スペースで設定する必要があります。

Unified CM Assistant のシェアド ライン モード

図 18-8 は、シェアド ライン モードでの Unified CM Assistant の単純なコール フローを示しています。この例で、電話機 A は、アシスタントの電話機のシェアド ラインであるディレクトリ番号（DN）60001 でマネージャの電話機をコールします（ステップ 1）。このコールは、アシスタントとマネージャの電話機の両方で着信音を鳴らします。ただし、マネージャが Do Not Disturb（DND）機能を呼び出した場合、着信音が鳴るのはアシスタントの電話機だけになります（ステップ 2）。

図 18-8　Unified CM Assistant のシェアド ライン モード



Unified CM Assistant のシェアド ライン モードでは、マネージャの電話機へのコールを代行受信するために Unified CM Assistant RP は必要ありません。ただし、マネージャの電話機および Unified CM Assistant Console デスクトップ アプリケーションの Do Not Disturb（DND）機能は、Cisco IP Manager Assistant（IPMA）および Cisco CTIManager サービスに依存します。さらに、Unified CM Assistant シェアド ライン モードでは、コール フィルタリング、コール代行受信、アシスタント選択、Assistant Watch などの機能は使用できません。

Unified CM Assistant のアーキテクチャ

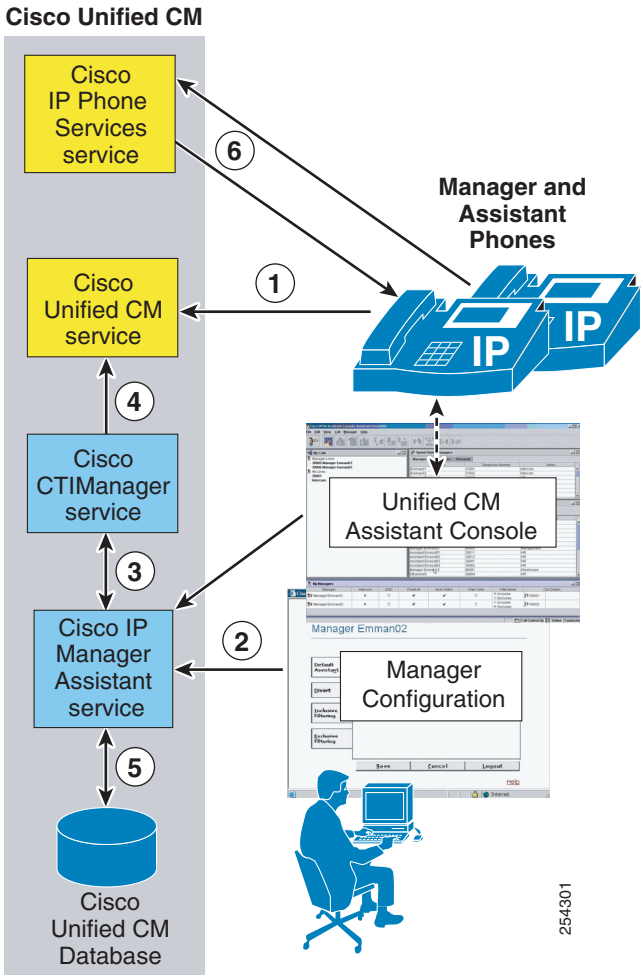
Unified CM Assistant アプリケーションのアーキテクチャは、その機能と同様に、そのアーキテクチャについても理解することが重要です。図 18-9 は、Unified CM Assistant のメッセージ フローとアーキテクチャを示しています。Unified CM Assistant のマネージャおよびアシスタント ユーザに対して Unified CM Assistant を設定すると、次の一連の対話とイベントが発生します。

1. マネージャとアシスタントの電話機は Cisco CallManager サービスに登録され、コール フロー処理にキーパッドとソフトキーが使用されます（図 18-9 のステップ 1 を参照）。
2. Unified CM Assistant Console デスクトップ アプリケーションと Manager Configuration Web ベース アプリケーションは、どちらも Cisco IP Manager Assistant サービスと通信およびインターフェイスします（図 18-9 のステップ 2 を参照）。
3. 次に、Cisco IP Manager Assistant サービスは、回線モニタリング情報および電話制御情報を交換するために、CTIManager サービスと対話します（図 18-9 のステップ 3 を参照）。
4. CTIManager サービスは、Unified CM Assistant 電話制御情報を Cisco CallManager Service に渡し、さらに Unified CM Assistant RP をも制御します（図 18-9 のステップ 4 を参照）。
5. それと並行して、Cisco IP Manager Assistant サービスは、Unified CM データベースとの間で、Unified CM Assistant アプリケーション情報の読み取りと書き込みを行います（図 18-9 のステップ 5 を参照）。
6. マネージャは、Services または Applications ボタンを押すことにより、Unified CM Assistant 電話サービスを呼び出して、その電話機が加入している（Unified CM Assistant 電話サービスを含む）すべてのサービスのリストを返す IP Phone サービス サービスへのコールを生成できます（図 18-9 のステップ 6 を参照）。

Unified CM Assistant 電話サービスは Cisco IP Manager Assistant サービスで制御され、電話機を使用してマネージャによって加えられた設定の変更は、Cisco IP Manager Assistant サービスを通じて処理および伝達されます。

（注）　Services Provisioning エンタープライズ パラメータが内部に設定されている場合、ステップ 1 および 2 はバイパスされます。一方、Services Provisioning が外部 URL または両方に設定されている場合、ユーザが回線ボタンまたはスピード ダイヤル ボタンを押して、Cisco IP Manager Assistant サービスへの直接コールを生成できるように、Service URL ボタンはユーザの電話機で Unified CM Assistant 電話サービスの設定ができます。ステップ 1 および 2 もバイパスされます。

図 18-9　Unified CM Assistant のアーキテクチャ



（注）　図 18-9 は、同じノードですべてが実行されている IP Phone Service、Cisco CallManager、CTIManager、および Cisco IP Manager Assistant サービスを示していますが、この設定は必須ではありません。これらのサービスではクラスタ内の複数のノードに分散できますが、説明を簡単にするためにここでは同じノードにあるものとしています。

Unified CM Assistant のハイ アベイラビリティ

Unified CM Assistant アプリケーションの冗長性は、次の 2 つのレベルで実現できます。

- コンポーネント レベルとサービス レベルでの冗長性

  このレベルでの冗長性については、Unified CM Assistant サービスまたはサーバの冗長性、および CTIManager サービスの冗長性に関して検討する必要があります。同様に、パブリッシャの冗長性の欠如、およびこのコンポーネントの障害の影響も検討する必要があります。

- デバイス レベルと到達可能性レベルでの冗長性

  このレベルでの冗長性については、アシスタントとマネージャの電話機、Unified CM Assistant ルート ポイント、Unified CM Assistant Console デスクトップ アプリケーション、および電話サービスに関連して検討し、さらにアシスタントとマネージャの到達可能性に関する冗長性として検討する必要があります。

サービスとコンポーネントの冗長性

図 18-9 に示すように、Unified CM Assistant 機能は、主に Cisco IP Manager Assistant サービスおよび Cisco CTIManager サービスに依存します。いずれの場合も、冗長性はプライマリおよびバックアップのメカニズムを使用して自動的に組み込まれます。Unified CM Assistant サーバ（Cisco IP Manager サービスを実行しているノード）のアクティブおよびバックアップのペアは最大で 3 個まで定義できます。つまり、単一クラスタ内で合計 6 つの Unified CM Assistant サーバになります。アクティブおよびバックアップ Unified CM Assistant サーバ ペアは Cisco IPMA Server IP Address、Pool 2、Cisco IPMA Server IP Address、および Pool 3 Cisco IPMA Server IP Address サービス パラメータを使用して設定されます。これらのパラメータを設定することで、必要な Unified IP Assistant サービスに冗長性が与えられます。いずれかのプライマリ Unified CM Assistant に障害が発生した場合、バックアップまたはスタンバイ Unified CM Assistant サーバが Unified CM Assistant サービス要求を処理できます。Unified CM Assistant サーバの各ペアでは、任意の時点でアクティブになり、要求を処理する Unified CM Assistant サーバは 1 つだけです。その別の Unified CM Assistant サーバはスタンバイ状態になり、アクティブなサーバに障害が発生しない限り、要求を処理しません。

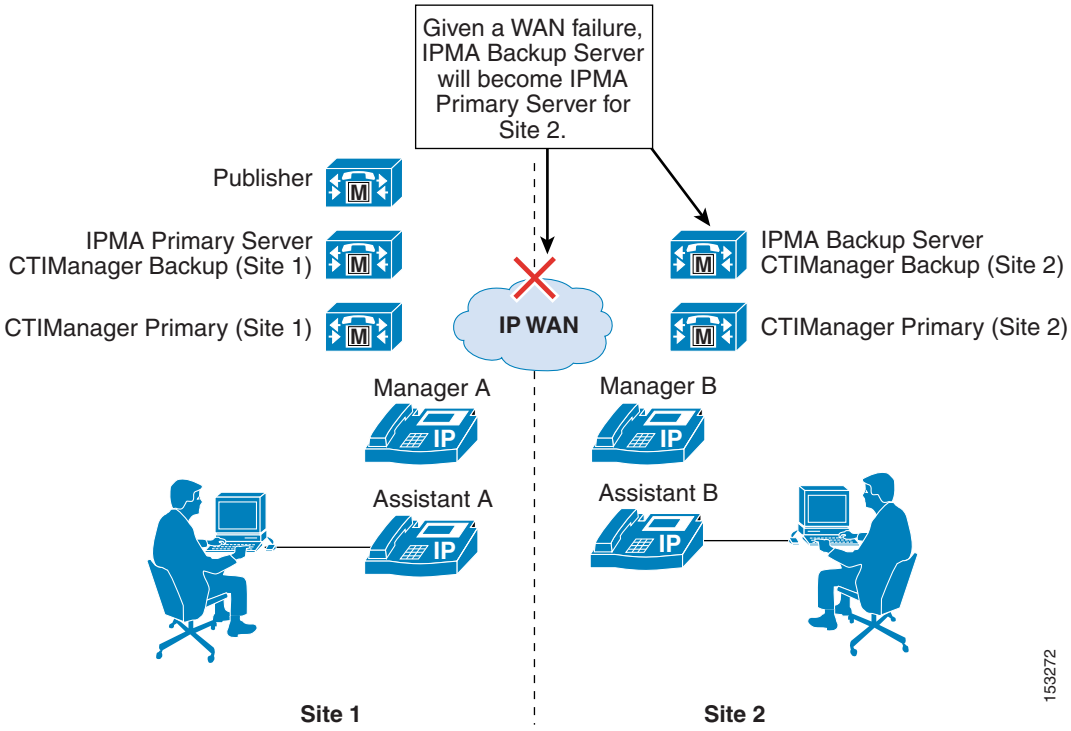
また、CTIManager (Primary) IP Address および CTIManager (Backup) IP Address サービス パラメータを使用して、2 つの CTIManager サーバまたはサービスを各 Unified CM Assistant サーバ用に定義できます。これらのパラメータを設定すると、CTIManager サービスに冗長性を与えることができます。このため、プライマリ CTIManager に障害が発生した場合でも、CTIManager サービスはバックアップ CTIManager から提供できます。クラスタ ノードのすべての Unified IP Assistant および CTIManager サービスに障害が発生した場合は、Unified CM Assistant ルート ポイントおよび Unified CM Assistant Console デスクトップ アプリケーションがダウンし、その結果 Unified CM Assistant アプリケーション全体がダウンします。ただし、前にも説明したように、Unified CM Assistant に障害が発生した場合、CFNA による呼び出しメカニズムは引き続き動作し、マネージャへのコールは直接マネージャの電話にルーティングできます。

（注）　Unified IP Assistant シェアド ライン モードで設定した場合、Unified CM Assistant および CTIManager サービスが障害によって完全に停止しても、電話機は 1 本の回線を共有し続けるため、アシスタントは引き続きマネージャの代わりにコールを処理できます。ただし、Unified CM Assistant Console デスクトップ アプリケーションと DND の機能は、使用できなくなります。

図 18-10 は、WAN を通じたクラスタリングで、2 サイトの配置による Unified CM Assistant および CTIManager のプライマリ サーバとバックアップ サーバの冗長設定を示しています。最大限の冗長性を実現するため、サイト 1 のノードはプライマリ Unified CM Assistant サーバとして設定し、サイト 2 のノードはバックアップ Unified CM Assistant サーバとして設定します。WAN に障害が発生した場合、既存のプライマリ Unified CM Assistant サーバはサイト 2 から到達できなくなるため、サイト 2 のバックアップ Unified CM Assistant サーバがプライマリ Unified CM Assistant サーバになります。このようにすることで、クラスタオーバー WAN 環境で、Unified CM Assistant サーバは WAN の障害に対して冗長性を持つことができます。さらに、サイト 1 とサイト 2 の両方でプライマリおよびバックアップ CTIManager を設定すると、CTIManager は WAN の障害に対する冗長性を持ち、各サイトで CTIManager の障害に対して追加の冗長性が提供されます。

（注）　図 18-10 で説明するシナリオは、特別な状況を示しています。通常の動作時に、Unified CM Assistant サーバの任意ペアを同時にアクティブにすることはできません。Unified CM Assistant サーバのアクティブおよびバックアップ ペアがネットワークを通じて通信できる場合、一方のサーバはバックアップ モードとなり、要求を処理できません。

図 18-10　WAN を通じた 2 サイト クラスタリングによる Unified CM Assistant の冗長性



前に説明したように、パブリッシャは、Unified CM Assistant 情報を Unified CM データベースへ書き込みする時に単一の障害点となります。パブリッシャに障害が発生しても、Unified CM Assistant アプリケーションのすべての部分が引き続き動作します。ただし、Unified CM Assistant アプリケーション設定を変更できなくなります。パブリッシャが回復するまで、Unified CM Assistant Console デスクトップ アプリケーション、Manager Configuration Web ベース アプリケーション、電話機のソフトキー、または Unified CM Assistant 電話サービスを通じて設定を変更できません。この条件には、Do Not Disturb、DivertAll、Assistant Watch、コール フィルタリングなどの機能の有効化や無効化、およびコール フィルタとアシスタント選択設定の変更が含まれます。

デバイスと到達可能性の冗長性

デバイス レベルでの Unified CM Assistant の冗長性は、いくつかのメカニズムに依存しています。まず第 1 に、マネージャおよびアシスタントの電話機と Unified CM Assistant RP は、デバイス登録用のデバイス プールと Unified CM グループ設定の組み合わせによって提供される組み込み冗長性に依存します。

また、一部のデバイスは、追加の冗長性および機能のためにコンポーネント サービスに依存します。たとえば、Unified CM Assistant RP は呼制御機能に関して CTIManager にも依存するため、前の項で説明したプライマリおよびバックアップ CTIManager に依存する必要があります。Unified CM Assistant Console デスクトップ アプリケーションも、冗長性と機能がコンポーネント サービスに依存します。Assistant Console デスクトップ アプリケーションは、マネージャの着信コールの処理を持続できるように、プライマリ Unified CM Assistant サーバからバックアップ サーバ（およびその反対）への自動フェールオーバーをサポートしています。この自動フェールオーバーに要する時間は、Cisco Unified IPMA Assistant Console Heartbeat Interval および Cisco Unified IPMA Assistant Console Request Timeout のサービス パラメータを使用して制御できます。ハートビートまたはキープアライブの頻度は、Unified CM Assistant サーバの障害がデスクトップ アプリケーションですばやく検出されるように設定しますが、キープアライブをあまり頻繁に送信することで、ネットワークに悪影響を与えないように注意してください。多数の Assistant Console アプリケーションが使用されている場合、この考慮事項は特に重要です。

Unified CM Assistant Console 電話サービスは、Unified CM Assistant Console デスクトップ アプリケーションとは異なり、プライマリ Unified CM Assistant サーバに障害が発生した場合の冗長性には手動で調整する必要があります。プライマリ Unified CM Assistant サーバがダウンした場合、電話コンソールを使用しているアシスタントにはこの状態の表示が見えません。ただし、アシスタント電話では、ソフトキーを使用するときにメッセージ「Host not found Exception」を受信します。バックアップ Unified CM Assistant サーバで電話コンソールを引き続き使用するには、ユーザは IP Services メニューから再びログインして、セカンダリ Unified CM Assistant 電話サービスを手動で選択する必要があります。

マネージャおよびアシスタントの到達可能性に確実に冗長性を与えるフェールオーバー メカニズムは、他にもいくつかあります。第 1 に、（プロキシ回線モードで）Unified CM Assistant アプリケーションを通じてマネージャのアシスタントに送信されるコールは、設定した時間の経過後にそのコールへの応答がない場合、次の応答可能なマネージャのアシスタントに転送します。設定した時間の経過後に次のアシスタントがコールに応答しない場合、そのコールは次の応答可能なマネージャのアシスタントに再び転送され、それ以降も同様に転送が続けられます。このメカニズムは、Cisco IPMA RNA Forward Calls および Cisco IPMA RNA Timeout のサービス パラメータを使用して設定します。第 2 に、前述したように、クラスタ ノードのすべての Unified IP Assistant と CTI サービスに障害が発生した場合、Unified CM Assistant RP は使用できなくなります。ただし、Unified CM Assistant RP の CFNA 設定に基づいて、すべてのマネージャの DN に対するコールはマネージャの電話機に直接呼び出され、マネージャの到達可能性に十分な冗長性が与えられます。

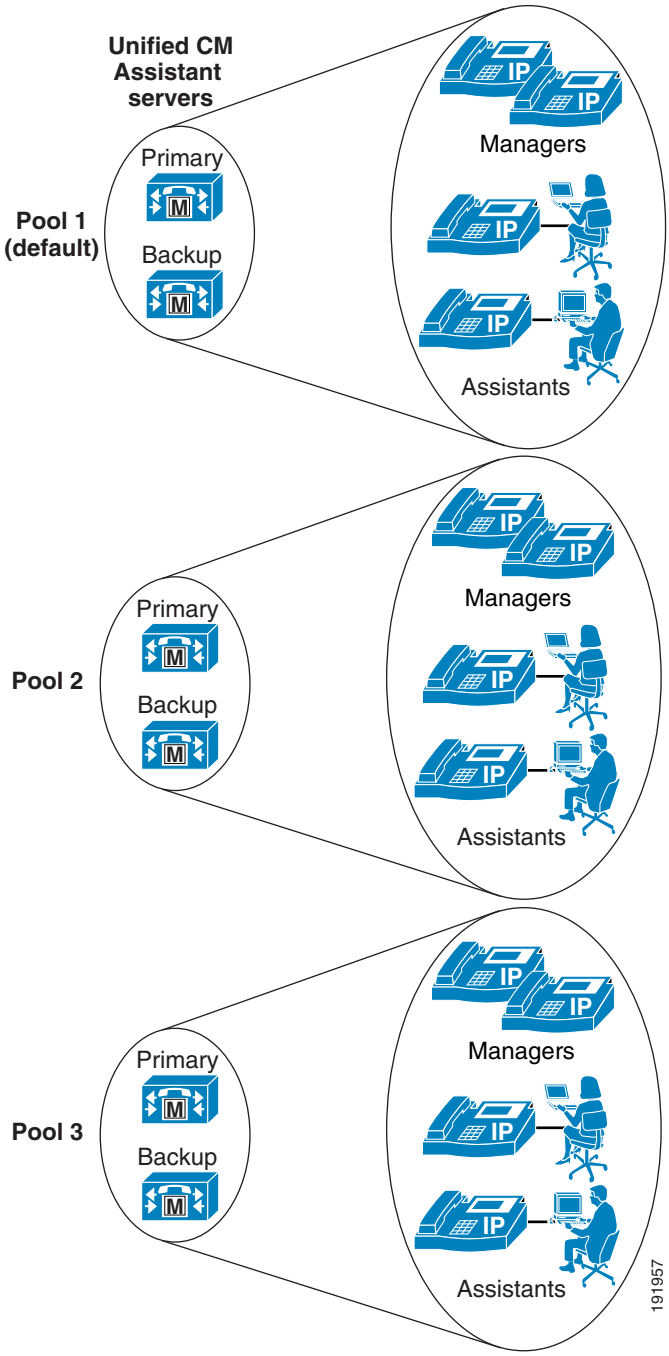
Unified CM Assistant のキャパシティ プランニング

Cisco Unified CM Assistant アプリケーションは、次のキャパシティをサポートしています。

- マネージャあたり最大 10 人のアシスタントを設定できる。
- 1 人のアシスタントに対して最大 33 人のマネージャを設定できる（マネージャ毎に 1 つの Unified CM Assistant 制御回線がある場合）。
- クラスタあたり最大 3500 人のアシスタントと 3500 人のマネージャを、7,500 人のユーザまたは 10,000 人のユーザ用の VM 構成を使用して設定できる（合計 7000 人）。
- プライマリおよびバックアップ Unified CM Assistant サーバのペアをクラスタあたり最大 3 組配置できる。ただし、Enable Multiple Active Mode アドバンスト サービス パラメータが True に設定され、Unified CM Assistant サーバの 2 番めおよび 3 番めのプールが設定されている場合。

Unified CM Assistant 最大でアシスタント 3500 人とマネージャ 3500 人（合計 7000 人）のキャパシティを実現するには、マルチの Unified CM Assistant サーバ プールを定義する必要があります。図 18-11 に示しているように、最大 3 個のプールを設定できます。各プールはプライマリおよびバックアップ Unified CM Assistant サーバおよびマネージャとアシスタントのグループで構成されています。Pool 1 の Unified CM Assistant サーバは Cisco IPMA Server（Primary/Backup）の IP Address サービス パラメータで設定し、Pool 2 のサーバは Pool2 で Cisco IPMA Server（Primary/Backup）の IP Address アドバンスト サービス パラメータで設定し、Pool 3 のサーバは Pool3 で Cisco IPMA Server（Primary/Backup）の IP Address アドバンスト サービス パラメータで設定します。

図 18-11　Unified CM Assistant Server Pools 環境下のマルチ アクティブ モード



Cisco Unified CM Assistant アプリケーションは、回線モニタリングおよび電話制御のために CTIManager と対話します。Unified CM Assistant 用のまたはマネージャ電話用の各回線（インターコム回線を含む）が CTI 回線を CTIManager と共に必要になります。また、各 Unified CM Assistant ルート ポイントは、CTI 回線インスタンスが CTIManager と共に必要になります。Unified CM Assistant を設定する場合、必要な CTI 回線または接続の数について、CTI 回線または接続に対する全体的なクラスタ制限と合わせて考慮する必要があります（クラスタごとの CTI 接続制限の詳細については、CTI のキャパシティ プランニング (9-32 ページ) を参照してください）。他のアプリケーションの CTI 回線を追加する必要がある場合は、Unified CM Assistant のキャパシティが制限される可能性があります。

Unified CM Assistant の設計上の考慮事項

Unified CM Assistant には、重複および共有内線番号に関して次の制限があり、ディレクトリ番号のプロビジョニングを計画する場合に注意する必要があります。

- プロキシ回線モードの Unified CM Assistant では、アシスタントの電話機のプロキシ回線番号は、異なるパーティション間でも一意にする必要があります。
- プロキシ回線モードの Unified CM Assistant では、2 人のマネージャは異なるパーティション間でも、同じ Unified CM Assistant 制御回線番号（DN）を持つことができません。

Multiple Active Mode を有効にして複数の Unified CM Assistant サーバ プールを使用する場合は、Unified CM Assistant サーバ プールの間でマネージャおよびアシスタントが均等に分散されるようにして、適切なサーバ プール（1 から 3）がエンド ユーザの [Manager Configuration] ページの [Assistant Pool] フィールドで選択されることを確認します。マネージャに連携したアシスタントは、そのマネージャが設定されたプールに自動的に割り当てられます。

Unified CM Assistant は、CTI Manager に対する安全でない接続と安全な接続（トランスポート層セキュリティ）の両方をサポートします。

Cisco TelePresence System EX90 などの一部のシスコのエンドポイントは Cisco Unified CM Assistant をサポートしない場合があります。詳細については、次の Web サイトで入手可能な『*Feature Configuration Guide for Cisco Unified Communications Manager*』の最新バージョンを参照してください。

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

Unified CM Assistant のエクステンション モビリティの考慮事項

Unified CM Assistant のマネージャは、エクステンション モビリティ（EM）を使用して、プロキシ回線モードとシェアド ライン モードの両方でそれぞれの電話機にログインできます。ただし、そのマネージャは、エンド ユーザ ディレクトリの [Cisco Unified CM Assistant Manager] 設定ページで、Mobile Manager として設定する必要があります。Unified CM Assistant と組み合わせて EM を使用する場合、ユーザが EM を使用して複数の電話機にログインできないようにする必要があります。この動作は、EM サービス パラメータの Multiple Login Behavior を使用して有効または無効にできます。クラスタ内で同じユーザによる複数の EM ログインが必要な場合、EM を使用する Unified CM Assistant のマネージャに、複数の電話機にログインしないよう指示する必要があります。マネージャが EM で 2 つの異なる電話機にログインすることを許可すると、2 人のマネージャは異なるパーティション間でも同じ Unified CM Assistant 制御回線番号（DN）を持つことができないという、前述の制限に違反することになります。

（注）　Unified CM のアシスタントは、Mobile Assistant の概念がないため、EM を使用してそれぞれの電話機にログインできません。

Unified CM Assistant のダイヤル プランの考慮事項

ダイヤル プラン設定は、プロキシ回線モードで設定される Unified CM Assistant では非常に重要です。マネージャの DN に対するコールが Unified CM Assistant RP で代行受信され、アシスタントの電話機に転送されることを保証するには、Unified CM Assistant RP およびアシスタントの電話機上のマネージャのプロキシ回線を除いて、すべてのデバイスからマネージャの DN に到達できないように、コーリング サーチ スペースおよびパーティションを設定する必要があります。

図 18-12 は、ダイヤル プラン コンポーネント内の各種デバイスのコーリング サーチ スペース、パーティション、および設定に対する最小要件を持つ、プロキシ回線モードの Unified CM Assistant ダイヤル プランの例を示しています。プロキシ回線モードでは 3 個のパーティションが必要です。図 18-12 の例では、次のパーティションになります。

- すべての Unified CM Assistant RP DN を含む Assistant_Route_Point パーティション
- すべてのアシスタントとその他のユーザの電話機 DN を含む Assistant_Everyone パーティション
- すべてのマネージャの電話機の DN を含む Assistant_Manager パーティション

また、2 つのコーリング サーチ スペースが必要です。図 18-12 の例では、次のコーリング サーチ スペースになります。

- Assistant_Route_Point パーティションおよび Assistant_Everyone パーティションを含む ASSISTANT_EVERYONE_CSS コーリング サーチ スペース
- Assistant_Manager パーティションおよび Assistant_Everyone パーティションを含む MANAGER_EVERYONE_CSS コーリング サーチ スペース

これは、この例でのダイヤル プランの範囲です。ただし、コール ルーティングが必要に応じて動作するように、適切なコーリング サーチ スペースでさまざまな電話機および Unified CM Assistant RP DN または回線を適切に設定することも重要です。この場合、すべてのユーザの回線、アシスタントのプライマリ（またはパーソナル）回線、およびマネージャの電話回線は、これらの回線すべてが Assistant_Everyone パーティションおよび Assistant_Route_Point パーティションのすべての DN に到達できるように、ASSISTANT_EVERYONE_CSS コーリング サーチ スペースで設定します。テレフォニー ネットワーク内のデバイスで設定されるインターコムなどの回線は、この同じコーリング サーチ スペースで設定します。すべてのマネージャのプロキシ回線およびすべての Assistant_RP 回線は、これらの回線すべてが Assistant_Manager パーティションのマネージャ DN および Assistant_Everyone パーティションに属するすべての DN に到達できるように、MANAGER_EVERYONE_CSS コーリング サーチ スペースで設定します。この方法により、ダイヤル プランでは、アシスタントの電話機の Assistant_RP 回線およびマネージャのプロキシ回線だけが、マネージャの電話機 DN に直接到達できるように確保します。

図 18-12　Unified CM Assistant のプロキシ回線モードのダイヤル プランの例

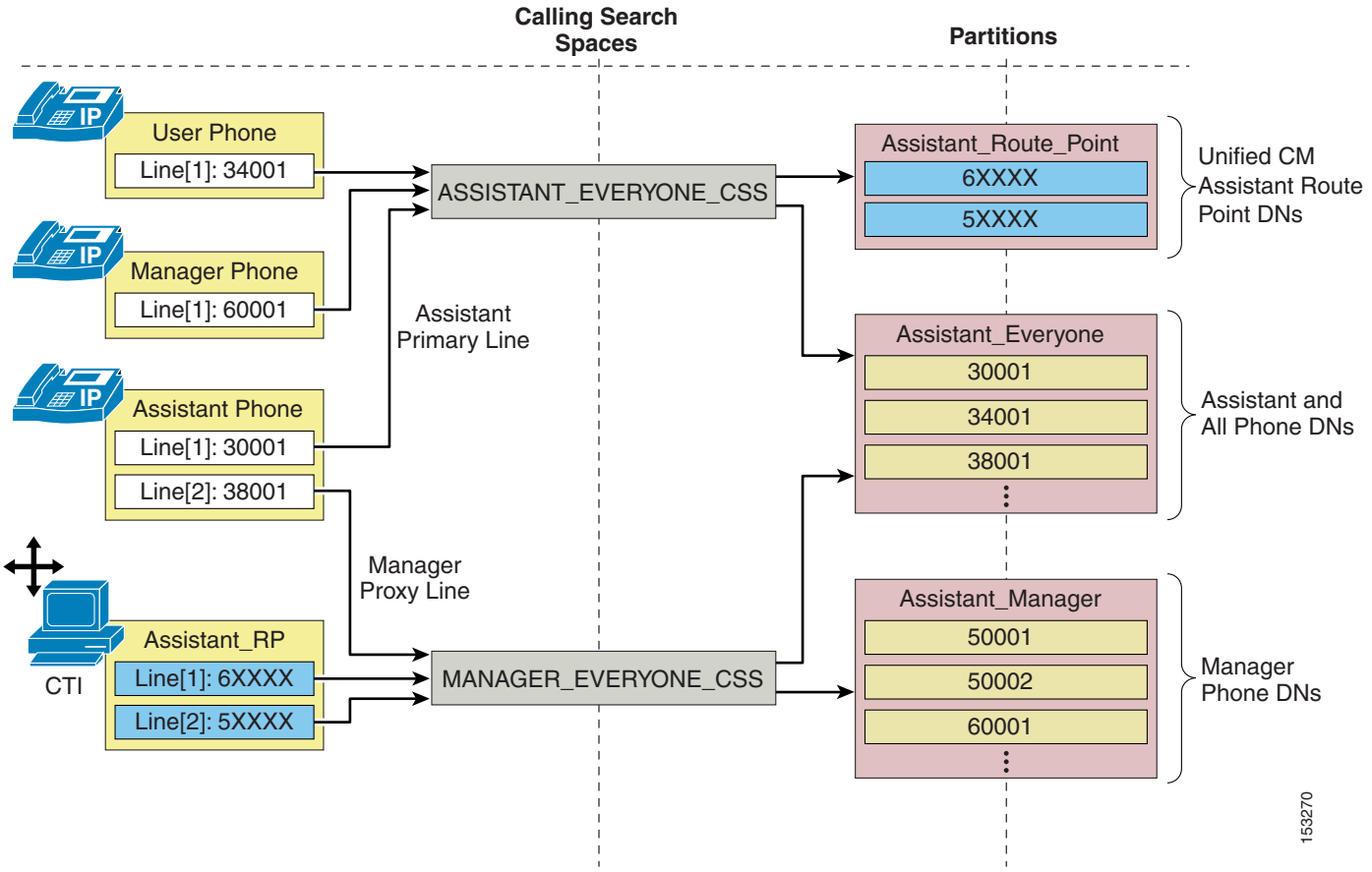


図 18-12 の例では、プロキシ回線モードでの Unified CM Assistant に関するダイヤル プランの最小要件を示しています。ただし、実際のテレフォニー ネットワークには、ほとんどの場合、Unified CM Assistant のコーリング サーチ スペースおよびパーティションとの統合が必要な追加または既存のダイヤル プラン要件があります。図 18-13 は、このような統合ダイヤル プランを示しています。この例では、前述したダイヤル プランは、2 つの追加のパーティションと 1 つの追加のコーリング サーチ スペースを処理する必要があります。図 18-13 では On Cluster パーティションが追加され、追加の電話機 DN もいくつか含まれています。On Cluster パーティションは、既存のデバイスがこれらの追加 DN に到達できるように、既存の Unified CM Assistant コーリング サーチ スペースの両方（ASSISTANT_EVERYONE_CSS および MANAGER_EVERYONE_CSS）に追加されています。UNRESTRICTED_CSS コーリング サーチ スペースも、既存のダイヤル プランに追加されています。このコーリング サーチ スペースは Assistant_Route_Point、Assistant_Everyone、および新たに追加した On Cluster パーティションで設定します。また、PSTN という別の新しいパーティションが追加されています。これには、共通ルート リスト（RL）、ルート グループ（RG）、およびボイス ゲートウェイ メカニズムを通じて、PSTN にコールをルーティングするために使用されるルート パターンのセットが含まれています。この PSTN パーティションは、UNRESTRICTED_CSS コーリング サーチ スペースの一部として設定します。

電話機およびデバイス回線のコーリング サーチ スペースの設定は、新しく追加したパーティションおよびコーリング サーチ スペースを組み込むために調整できます。ただし、Assistant_RP およびアシスタントの電話機のマネージャ プロキシ回線は、MANAGER_EVERYONE_CSS コーリング サーチ スペースに割り当てたままにする必要があります。この例で、マネージャには PSTN への無制限アクセスが与えられる可能性があるため、マネージャの電話回線は、最初に設定された ASSISTANT_EVERYONE_CSS コーリング サーチ スペースから、新しい UNRESTRICTED_CSS に移動されています。

図 18-13　Unified CM Assistant のプロキシ回線モードのダイヤル プラン統合の例

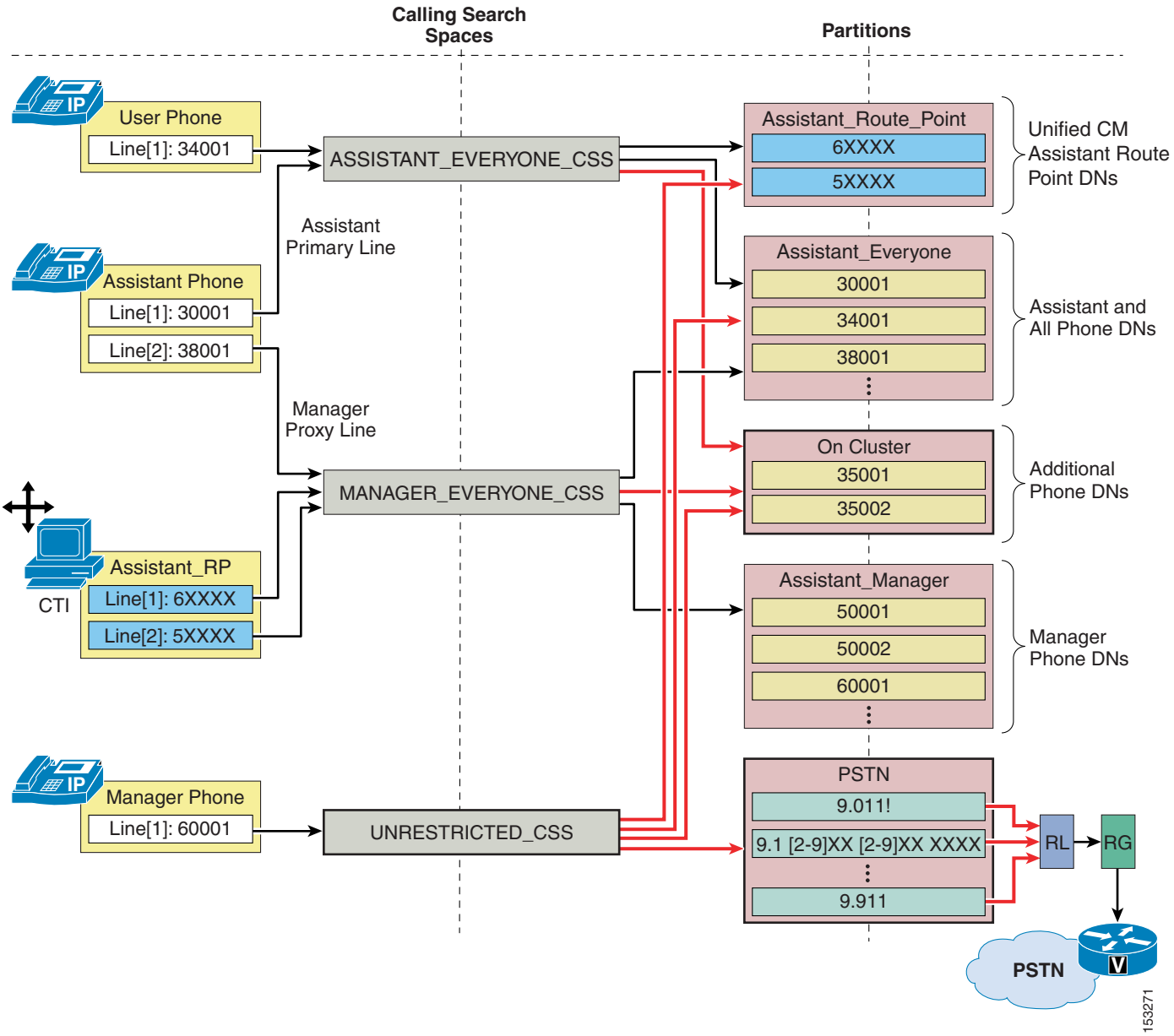


図 18-13 に示すように、追加のパーティションとコーリング サーチ スペースを新規または既存の Unified CM Assistant ダイヤル プランに統合することはできますが、基になるプロキシ回線モードのメカニズムが影響を受けないように注意する必要があります。

Unified CM Assistant シェアド ライン モードでは、特別なダイヤル プランのプロビジョニングは必要ありません。注意の必要な Unified CM Assistant RP またはプロキシ回線が存在しないため、マネージャとアシスタントの電話機は、ネットワーク内の他の電話機と同様にコーリング サーチ スペースおよびパーティションで設定できます。シェアド ライン モードに関する唯一の要件は、シェアド ラインの機能を実現できるように、マネージャとアシスタントの DN が同じパーティションに属する必要があることです。

Unified CM Assistant Console

Unified CM Assistant Console デスクトップ アプリケーションまたは Unified CM Assistant Console 電話サービスは、アシスタントがマネージャの代わりにコールを処理するために必要です。このデスクトップ アプリケーションは、コールを処理するためのグラフィカル インターフェイスをアシスタントに提供しますが、電話サービスはコールを処理するためのメニュー方式インターフェイスを提供します。デスクトップ アプリケーションと IP フォン サービスの両方では、アシスタントがマネージャの電話機の設定および環境の設定ができて、回線ステータスおよび可用性をモニタできます。また、このデスクトップ アプリケーションは、クリックコール スピード ダイヤルおよびディレクトリ エントリなど別の機能を備えています。この別の機能も従来のソフトキーおよびメニュー アプローチを使用してアシスタントの電話機で行うことができます。

Unified CM Assistant Console のインストール

Unified CM Assistant Console デスクトップ アプリケーションは、次の URL からインストールできます。

https://<*Server_IP-Address*>:8443/plugins/CiscoUnifiedCallManagerAssistantConsole.exe

（ここで、<*Server_IP-Address*> は、クラスタ内のいずれかのノードの IP アドレスです）

Unified CM Assistant Console 電話サービスは、いかなるインストールも必要がありません。アシスタントの電話機をコンソールとして使用可能にするには、アシスタントの電話機を Unified CM Assistant 電話サービスにサブスクライブします（これは、マネージャの電話機もサブスクライブする必要があることと同じサービスです）。

Unified CM Assistant Console の QoS

インストール後に、マネージャに代わってコールを処理するには、アシスタントがユーザ ID とパスワード（Cisco Unified CM の End-user ディレクトリで設定されている）を入力してアプリケーションにログインし、[Go Online] アイコンまたはメニュー項目をクリックして、ステータスを「online」に切り替える必要があります。ユーザがログインし、オンライン状態になると、デスクトップ アプリケーションは TCP ポート 2912 で Unified CM Assistant サーバと通信します。このアプリケーションは、トラフィックを受信する場合に一時的な TCP ポートを選択します。Cisco Unified CM 上の Unified CM Assistant サーバは、呼制御（コール フローの生成と処理）のためにデスクトップ アプリケーションとインターフェイスするので、TCP ポート 2912 で Cisco Unified CM から受信されたトラフィックは、Cisco Unified CM によって 24 の Diffserv コード ポイント（DSCP）または CS3 の Per Hop Behavior（PHB）として、QoS マーキングされます。この方法により、Unified CM Assistant 電話制御トラフィックは、その他のすべてのコール シグナリング トラフィックと同様に、ネットワークを通じてキューに入れることができます。

対称的なマーキングとキューを保証するため、Cisco Unified CM の TCP ポート 2912 を宛先とする Unified CM Assistant Console アプリケーション トラフィックも、DSCP 24（PHB CS3）としてマーキングする必要があります。これにより、このトラフィックが、Cisco Unified CM および Unified CM Assistant サーバに向かうネットワーク パスに沿って適切なコール シグナリング キューに配置されます。Unified CM Assistant Console アプリケーションは、すべてのトラフィックをベストエフォートとしてマーキングします。つまり、スイッチ ポート レベル（または、可能な限りコンソール PC に近いネットワーク パスに沿った場所で）アクセス コントロール リスト（ACL）を適用することで、アプリケーション PC から送信され、TCP ポート 2912 の Cisco Unified CM を宛先とするトラフィックを、DSCP 0（PHB Best Effort）から DSCP 24（PHB CS3）に再マーキングする必要があります。

Unified CM Assistant Console のディレクトリ ウィンドウ

Assistant Console デスクトップ アプリケーションのディレクトリ ウィンドウを使用すると、アシスタントは Cisco Unified CM Directory エンド ユーザを検索できます。ディレクトリ ウィンドウの [Name] フィールドに入力する検索文字列は、Unified CM Assistant サーバに送信され、Cisco Unified CM データベースに対して検索が直接実行されます。次に、Unified CM Assistant サーバによって、検索照会への応答がデスクトップ アプリケーションに返されます。

デスクトップ アプリケーションのディレクトリ検索によって生じる追加のトラフィックはわずかですが、1 つ以上の Unified CM Assistant コンソール アプリケーションがリモート サイトで実行されている集中型の呼処理配置では、このトラフィックが問題になることがあります。1 つのエントリが得られるディレクトリ検索では、Unified CM Assistant サーバからデスクトップ アプリケーションへの約 1 キロビットのトラフィックが発生します。1 回の検索あたり最大 25 のエントリを取得できるため、デスクトップ アプリケーションで実行される検索ごとに最大約 25 キロビットのトラフィックが生成されることがあります。ただし、Unified CM Assistant サーバからの低速 WAN リンクを通じて、複数の Unified CM Assistant Console デスクトップ アプリケーションでディレクトリ検索が実行されると、輻輳、遅延、およびキューの発生する可能性が高くなります。また、ディレクトリ検索トラフィックは、デスクトップに対するその他すべての Unified CM Assistant トラフィックと同様に、TCP ポート 2912 の Cisco Unified CM から発生します。つまり、ディレクトリ検索トラフィックも DSCP 24（PHB CS3）としてマーキングされるため、コール シグナリング トラフィックと同様にキューに入れられます。このため、ディレクトリ検索によって、呼制御トラフィックの輻輳、オーバーラン、または遅延が生じる可能性があります。

（注） ディレクトリ検索で 25 を超えるエントリが生成される場合、アシスタントには、ダイアログ ボックスを介して警告メッセージ「検索結果が 26 項目以上あります。（Your search returned more than 25 entries.）検索条件を設定し直してください。（Please refine your search.）」が表示されます。

ネットワーク輻輳の可能性を考慮に入れて、管理者は Unified CM Assistant Console ユーザに次の操作の実行を推奨することを推奨します。

- ディレクトリ ウィンドウ検索機能の使用を制限する。
- 返されるエントリの数を減らすため、この機能を使用するときは、[Name] フィールドにできる限り多くの情報を入力し、ワイルドカードやブランクでの検索は実行しない。

これらの推奨事項は、次のいずれかの条件が該当する場合は特に重要です。

- クラスタ内に多数の Unified CM Assistant Assistants が存在する。
- Cisco Unified CM または Unified CM Assistant サーバ（あるいはその両方）から低速 WAN リンクによって分離されている多数のアシスタントが存在する。

Unified CM Assistant Phone Console の QoS

Unified CM Assistant Phone Console 電話サービスを使用してマネージャに代わってコールを処理するには、アシスタントがユーザ ID と PIN（Unified CM の End-user ディレクトリで設定されている）を入力してアプリケーションにログインする必要があります。ユーザがログインしている状態になると、電話コンソール サービスは HTTPS および SCCP を使用して Unified CM と通信します。Unified CM Assistant コール生成および呼処理の呼制御トラフィックは、SCCP を使用して電話と Unified CM の間で送信されます。デフォルトでは、このトラフィックは 24 の Diffserv コード ポイント（DSCP）または CS3 の Per Hop Behavior（PHB）として、QoS マーキングされます。こうして、コール シグナリング トラフィックと同様にネットワークを通じてキューに入れられ確保します。したがって、追加の QoS の設定またはマーキングの必要はありません。

WebDialer

WebDialer は Cisco Unified CM のクリックコール アプリケーションで、ユーザはサポートされる任意の電話デバイスを使用して自分の PC から簡単にコールを発信できます。管理者が CTI リンクを管理したり、JTAPI または TAPI アプリケーションを作成したりするために必要なものはありません。Cisco WebDialer には、独自のユーザ インターフェイスと認証メカニズムを提供するための、簡単な Web アプリケーションと HTTP または Simple Objects Access Protocol（SOAP）が用意されているからです。

ここでは、WebDialer 機能の設計について次の項目を説明します。

- WebDialer のアーキテクチャ（18-38 ページ）
- WebDialer のハイ アベイラビリティ（18-44 ページ）
- WebDialer のキャパシティ プランニング（18-45 ページ）
- WebDialer の設計上の考慮事項（18-47 ページ）

WebDialer のアーキテクチャ

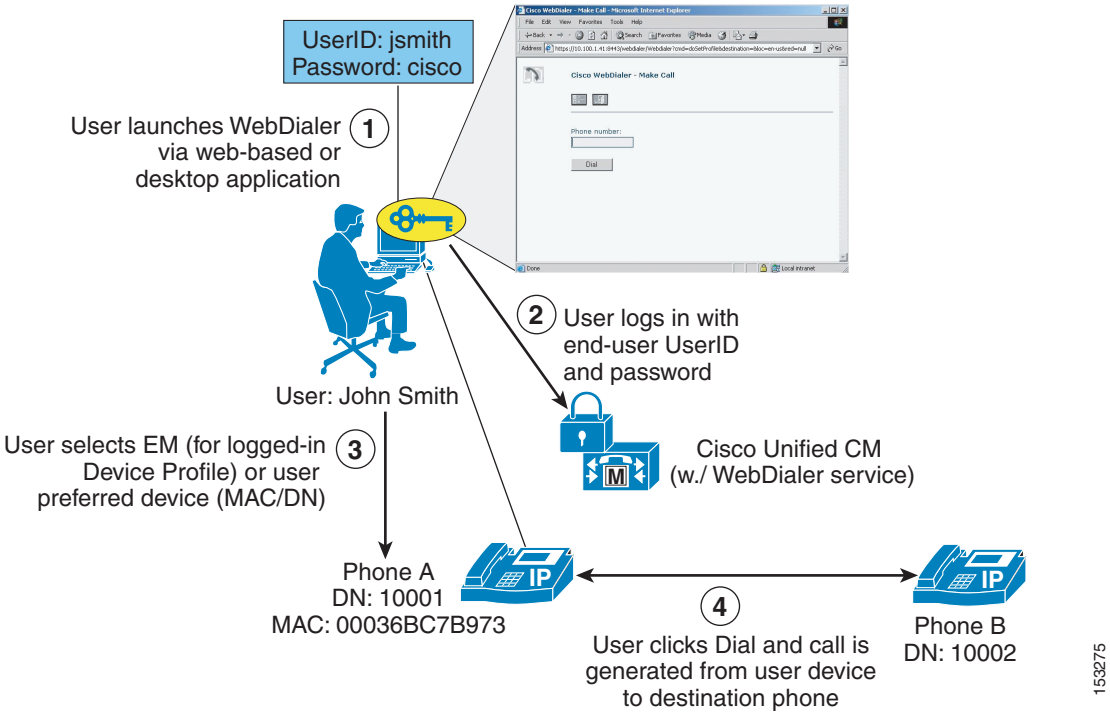
WebDialer アプリケーションには、WebDialer サーブレットと Redirector サーブレットの 2 つのサーブレットが含まれています。サブスクライバ サーバで Cisco WebDialer Web サービスがアクティブである場合、両方のサーブレットが有効になります。これらのサーブレットは関連していますが、それぞれ異なる機能を提供し、同時に実行するように設定できます。

WebDialer サーブレット

図 18-14 は、単純な WebDialer の例を示しています。この例では、ユーザ John Smith は Web ベースまたはデスクトップ アプリケーションから WebDialer を起動します（ステップ 1）。WebDialer は、ログイン クレデンシャル要求で応答します。ユーザは、Unified CM エンド ユーザ ディレクトリで設定される有効なユーザ ID とパスワードで応答する必要があります。この場合、John Smith は userID = jsmith および password = cisco を送信します（ステップ 2）。次に、このログインに基づいて、WebDialer は [Cisco WebDialer の初期設定（Cisco WebDialer Preferences）] 設定ページで応答し、ユーザは、[ユーザ指定デバイス（User preferred device）] または [エクステンション モビリティを使用する（Use Extension Mobility）] のいずれかを示す必要があります（ユーザが EM デバイス プロファイルを持つと想定して）。この場合、ユーザ John Smith は、[ユーザ指定デバイス（User preferred device）] を選択し、設定ページのドロップダウン メニューからその電話機に対して適切な MAC アドレス（SEP00036BC7B973）とディレクトリ番号（10001）を選択します（ステップ 3）。最後に、コールする電話番号を要求する画面が表示され（この値はすでに表示されていることがあります）、ユーザは [Dial] をクリックする必要があります。この場合、John Smith が 10002 と入力し、[Dial] をクリックすると、その電話機から番号 10002 の電話機 B へのコールが自動的に生成されます（ステップ 4）。

（注）　ユーザが以前に WebDialer アプリケーションにログインし、Web ブラウザおよびサーバの Cookie がまだアクティブになっている場合、次の要求時に再ログインは求められません。Cookie がブラウザでクリアされるか、または WebDialer サーバの再起動によってクリアされた場合は、再ログインが要求されます。一方、ユーザ Web ブラウザ クッキーは期限を WebDialer サービス パラメータで設定できます。これは、WebDialer サービス パラメータで設定された通り所定の時間が経過した後、自動的に期限切れになります。

図 18-14　WebDialer サーブレットの動作



Redirector サーブレット

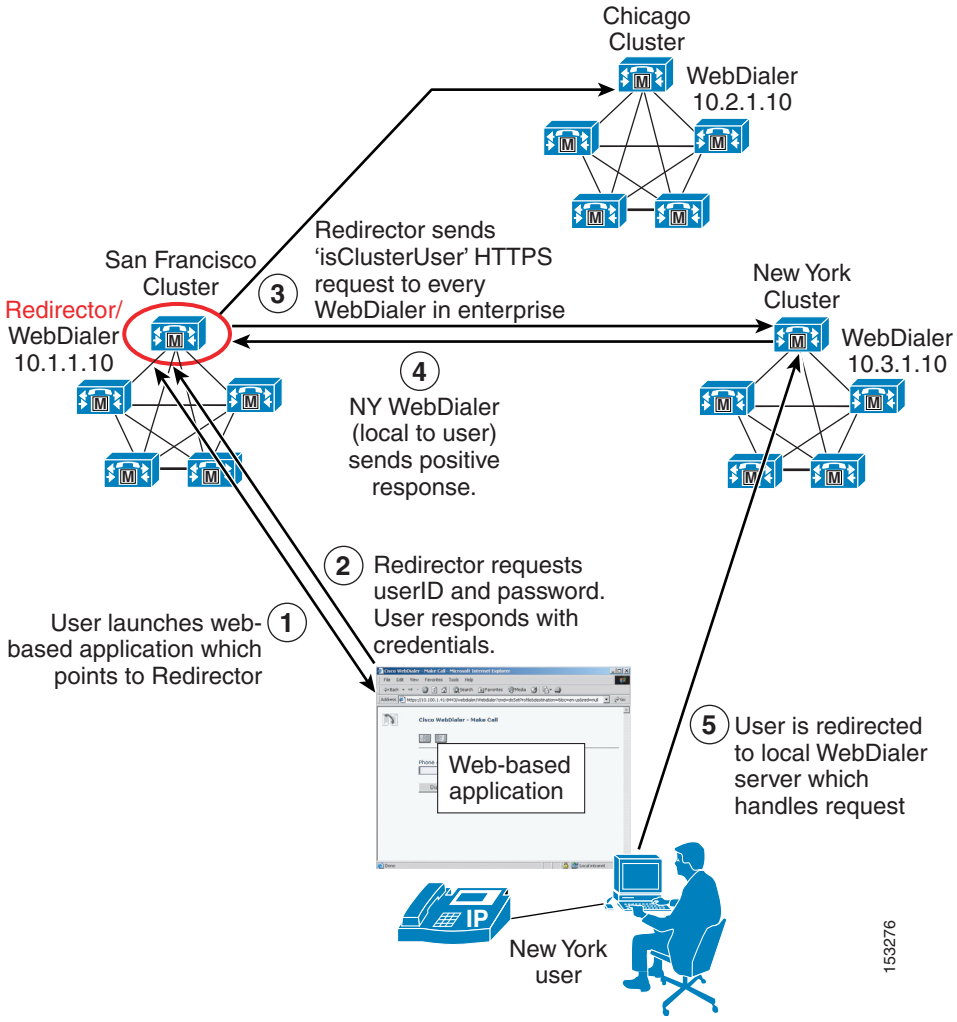
Redirector サーブレットは、マルチクラスタまたは分散型の呼処理環境において、WebDialer 機能を提供します。この機能を使用すると、すべての Unified CM クラスタ間で単一の企業全体の Web ベース WebDialer アプリケーションを使用できます。図 18-15 は、WebDialer アプリケーションの一部として Redirector サーブレットの基本的な動作を示しています。この例で、この企業には 3 個の Unified CM クラスタとして、New York、Chicago、および San Francisco があります。3 個のクラスタはすべて、単一の WebDialer アプリケーションで設定されます。San Francisco クラスタは、Redirector として指定されます。

企業全体の Web ベース アプリケーションは San Francisco の Redirector を指し、New York のユーザから起動されます（図 18-15 のステップ 1 を参照）。次に、Redirector はユーザのログインを要求し、New York ユーザは自分のユーザ ID とパスワードで応答します（図 18-15 のステップ 2 を参照）。

（注）　ユーザが以前に WebDialer アプリケーションにログインし、Web ブラウザおよびサーバの Cookie がまだアクティブになっている場合、次の要求時に再ログインは求められません。一方、ユーザ Web ブラウザ クッキーは期限を WebDialer サービス パラメータで設定できます。これは、WebDialer サービス パラメータで設定された通り所定の時間が経過した後、自動的に期限切れになります。

次に、Redirector は、（List of WebDialers サービス パラメータの設定に従って）企業内のすべての WebDialer に isClusterUser HTTPS 要求を同時に送信します。この例で、要求は Chicago および New York の WebDialer サーバに送信されます（図 18-15 のステップ 3 を参照）。New York ユーザは New York クラスタに対してローカルであるため、New York の WebDialer は肯定応答を返します（図 18-15 のステップ 4 を参照）。最後に、New York ユーザはアプリケーション要求を処理するローカル WebDialer サーバに転送されます（図 18-15 のステップ 5 を参照）。この転送はユーザに通知されません。ただし、ブラウザのアドレス バーの URL は、ユーザが Redirector から WebDialer サーバに転送されたときに変更されます。この例では、1 個の Redirector のみ配置されます。ただし、Redirector に冗長性を提供するには、サービスとコンポーネントの冗長性（18-45 ページ）に説明されているように複数のクラスタに Redirector を設定します。

図 18-15　IRedirector サーブレットの動作



（注）　Redirector アプリケーションは、Unified CM データベースでのユーザ認証の必要な企業全体のアプリケーションであるため、すべての Unified CM クラスタですべてのエンド ユーザのユーザ ID を一意にすることを強く推奨します。一意でない場合、Redirector アプリケーションが isClusterUser 要求に対する複数の肯定応答を受信する可能性があります。この場合、Redirector アプリケーションによって、ユーザは自分のローカル WebDialer サーバを手動で選択するように求められます。このため、ユーザは自分のローカル サーバを知っている必要があります。正しくないサーバを選択した場合、WebDialer 要求は失敗します。

WebDialer のアーキテクチャ

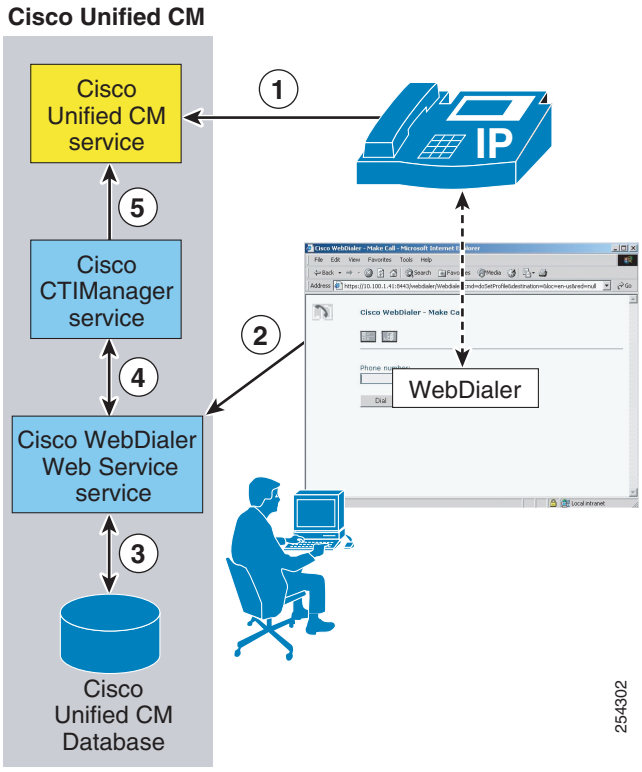
WebDialer アプリケーションのアーキテクチャは、その機能と同様に、そのアーキテクチャについても理解することが重要です。図 18-16 は、WebDialer のメッセージ フローとアーキテクチャを示しています。次の一連の対話とイベントが発生します。

1. WebDialer ユーザの電話機は、Cisco CallManager サービスを通じて登録し、コールの発信と受信を行います（図 18-16 のステップ 1 を参照）。
2. ユーザの PC 上の WebDialer アプリケーションは、次のいずれかのインターフェイスを通じて Cisco WebDialer Web Service と通信します（図 18-16 のステップ 2 を参照）。
   - HTML over HTTPS

     このインターフェイスは、HTTPS プロトコルに基づいて Web ベースのアプリケーションで使用されます。これは、Redirector サーブレットへのアクセスを提供する唯一のインターフェイスです。
   - Simple Object Access Protocol（SOAP）over HTTPS

     このインターフェイスは、SOAP インターフェイスに基づいてデスクトップ アプリケーションで使用されます。
3. WebDialer Web サービスは、Unified CM データベースからユーザおよび電話の情報を読み取ります（図 18-16 のステップ 3 を参照）。
4. 次に、WebDialer Web サービスは、回線と電話の制御情報を交換するために、CTIManager サービスと対話します（図 18-16 のステップ 4 を参照）。
5. CTIManager サービスは、WebDialer 電話制御情報を Cisco CallManager サービスに渡します（図 18-16 のステップ 5 を参照）。

図 18-16　WebDialer のアーキテクチャ



（注）　図 18-16 は、すべて同じノードで実行されている Cisco Unified CallManager、CTIManager、および WebDialer Web Service サービスを示していますが、この設定は必須ではありません。これらのサービスはクラスタ内の複数のノードに分散できますが、説明を簡単にするためにここでは同じノードにあるものとしています。

WebDialer の URL

Web ベースのアプリケーションから HTML-over-HTTPS インターフェイスを通じて WebDialer アプリケーションにアクセスするには、次の URL を使用します。

- WebDialer サーブレット

  https://<*Server-IP_Addr*>:8443/webdialer/Webdialer?destination=<*Number_to_dial*>

  （ここで、<*Server_IP-Address*> は、Cisco WebDialer Web Service サービスを実行しているクラスタ内のノードの IP アドレスで、<*Number_to_dial*> は WebDialer ユーザがダイヤルする番号です）

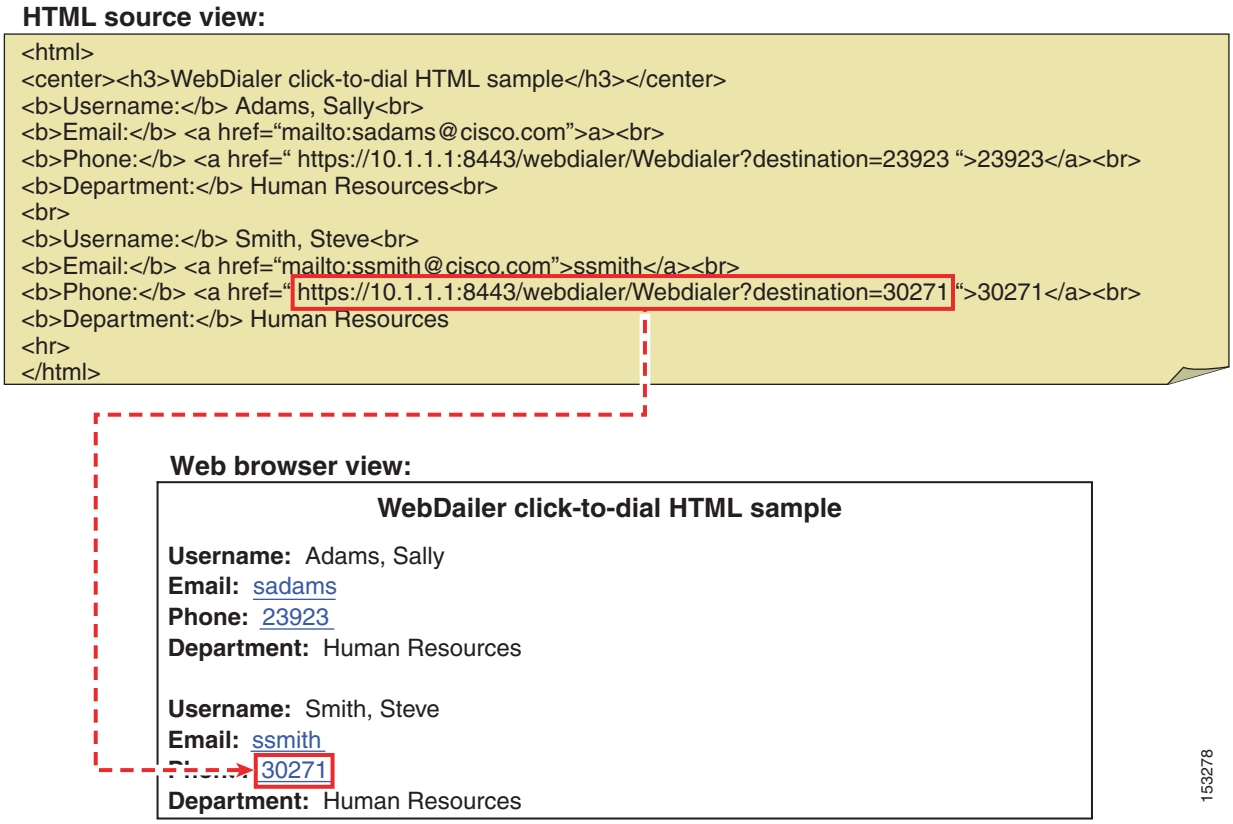
- Redirector Servlet

  https://<*Server-IP_Addr*>:8443/webdialer/Redirector?destination=<*Number_to_dial*>

  （ここで、<*Server_IP-Address*> は、Cisco WebDialer Web Service サービスを実行している企業内のノードの IP アドレスで、<*Number_to_dial*> は WebDialer ユーザがダイヤルする番号です）

図 18-17 は、Cisco WebDialer アプリケーションをコールするクリックコール Web ベース アプリケーションで使用される、HTML ソース コードの例を示しています。この例で、HTML ソース ビューの URL https://10.1.1.1:8443/webdialer/Webdialer?destination=30271 は、Web ブラウザ ビュー内のユーザ Steve Smith 用の「Phone: 30721」リンクに対応しています。ユーザがこのリンクをクリックすると、WebDialer アプリケーションが起動し、ログイン後に Dial をクリックすると、そのユーザの電話機から Steve Smith の電話機へのコールが生成されます。URL を https://10.1.1.1:8443/webdialer/Redirector?destination=30271 に変更すると、Redirector を使用するクリックコール アプリケーションで同じコードを使用できます。

図 18-17　WebDialer URL の HTML の例



デスクトップ アプリケーションのクリックコールで使用される SOAP-over-HTTPS ソース コードの情報および例については、次の Web サイトで入手可能な『*Cisco WebDialer Developer Guide*』の WebDialer API Programming 資料を参照してください。

https://developer.cisco.com/site/webdialer/discover/getting-started/

WebDialer のハイ アベイラビリティ

WebDialer アプリケーションの冗長性は、次の 2 つのレベルで実現できます。

- コンポーネント レベルとサービス レベルでの冗長性

  このレベルでの冗長性については、冗長性を、WebDialer サービスおよび CTIManager サービスの冗長性に関して検討する必要があります。同様に、パブリッシャの冗長性の欠如、およびこのコンポーネントの障害の影響も検討する必要があります。

- デバイス レベルと到達可能性レベルでの冗長性

  このレベルでの冗長性については、ユーザの電話機および WebDialer ユーザ インターフェイスに関連して検討する必要があります。

サービスとコンポーネントの冗長性

図 18-16 に示すように、WebDialer 機能は、主に Cisco WebDialer Web Service および Cisco CTIManager サービスに依存します。WebDialer サービスはクラスタ内の複数のノードで有効にできます。これらの複数ノードへの到達可能性はデバイスと到達可能性の冗長性（18-45 ページ）の項で説明されています。CTIManager の場合、冗長性は、プライマリおよびバックアップのメカニズムを使用して自動的に組み込まれます。Primary Cisco CTIManager および Backup Cisco CTIManager のサービス パラメータを使用すると、クラスタ内に 2 つの CTIManager サーバまたはサービスを定義できます。これらのパラメータを設定すると、CTIManager サービスに冗長性を与えることができます。このため、プライマリ CTIManager に障害が発生した場合でも、CTIManager サービスはバックアップ CTIManager から提供できます。Web ベース（またはデスクトップ）アプリケーションが指している WebDialer サーバに障害が発生し、クラスタ ノード上のプライマリおよびバックアップ CTIManager サービスにも障害が発生した場合、WebDialer アプリケーションはダウンします。WebDialer サービスは Unified CM パブリッシャに依存しません。

デバイスと到達可能性の冗長性

デバイス レベルでの WebDialer の冗長性は、いくつかのメカニズムに依存しています。まず第 1 に、ユーザの電話機は、デバイス登録用のデバイス プールと Unified CM グループ設定の組み合わせによって提供される組み込み冗長性に依存します。

複数の WebDialer サービスは冗長性を提供するために同じクラスタで複数の Unified CM サブスクライバを実行できます。しかしながら、多くのアプリケーションは複数の IP アドレスを処理するようには備わっていません。企業では、複数の WebDialer サーバのプレゼンスをマスクしてサーバ ロード バランサ（SLB）使用することを推奨します。SLB 機能は、仮想 IP アドレスまたは DNS-resolvable hostname を実現します。この DNS-resolvable hostname は、WebDialer サーバの実 IP アドレスのフロントエンドになるものです。Cisco IOS SLB 機能を実行するシスコ デバイスなど多くの SLB デバイスは、複数の WebDialer サーバおよび障害イベント発生時に自動的な転送要求のステータスをモニタする設定ができます。SLB 機能は、追加のクリックコール キャパシティを必要とする場合、ロード バランサ WebDialer 要求も設定できます。代替えとして、DNS Service（SRV）レコードも冗長性の提供に使用できます。

マルチ クラスタ環境と同様に、単一の Redirector サーブレットが複数の WebDialer をサポートする場合は、単一障害点になる可能性があります。この単一障害点を回避するために、各クラスタの Redirector サーブレットを設定し、Redirector サーバの実際の IP アドレスをフロントエンドにする仮想 IP アドレスまたは DNS-resolvable hostname を実現するためにサーバ ロード バランサ（SLB）を使用します。

WebDialer のキャパシティ プランニング

WebDialer および Redirector サービスは Unified CM クラスタ内で複数のサブスクライバ ノードを実行でき、次のキャパシティがサポートされています。

- 各 WebDialer サービスは、ノードごとに 1 秒あたり最大 4 コール要求まで処理できます。
- 各 Redirector サービスは、1 秒あたり最大 8 コール要求まで処理できます。

次の一般式が WebDialer の 1 秒あたりのコール数の決定に使用できます。

（WebDialer のユーザ数）*（（平均 BHCA）/（3600 秒/時間））

この計算を行う場合、特に WebDialer サービスを使用した発信の、ユーザあたりの BHCA を適切に推定することが重要です。以下の例で、サンプルの組織に対して WebDialer デザイン計算式をどのように使用するかを示します。

例 18-1　WebDialer のコール数 1 秒あたりの計算

会社 XYZ は、WebDialer サービスを使用してクリックコール アプリケーションを稼働させることを考えています。その事前のトラフィック分析結果は次の資料の通りです。

- 10,000 人をクリックコール機能で有効にする。
- 各ユーザの平均 6 BHCA
- すべてのコールの 50 % が発信で、50 % が着信
- 計画では、すべての発信のうち、WebDialer サーバを使用して開始する発信を 30 % と見積もる。

(注)　これらの値は、WebDialer 配置のサイジングの演習を示すために使用した例です。ユーザのダイヤル特性は、組織によって大きく異なります。

10,000 ユーザで各 6 BHCA ならば、合計 60,000 BHCA です。ただし、WebDialer 配置のサイジングの計算は、発信コールのみ考慮します。このサイジングの例で最初の情報では、合計 BHCA の 50 %が発信です。これは、WebDialer を用いたクリックコールが利用可能なすべてのユーザで、合計 30,000 発信 BHCA という結果になります。

この発信数のうち、WebDialer サービスを使用して発信される割合は、組織によって変化します。この例の組織では、ユーザはいくつかのクリックコール アプリケーションを利用可能で、発信の 30 % が WebDialer を使用すると見積もられています。

（30,000 発信 BHCA）* 0.30 = 9,000 発信 BHCA が WebDialer を使用

9,000 BHCA の負荷をサポートするのに必要な WebDialer サーバの数を判別するには、この値を最繁時に維持する必要のある平均の Busy Hour Call Attempt（BHCA）1 秒あたりに変換します。

（9,000 call attempts / 時間）*（時間/3600 秒）= 2.5 cps

各 WebDialer サービスは最大で 4 cps をサポートできます。したがって、この例では、WebDialer サービスを実行するため 1 つのノードを設定できます。これは、将来の WebDialer 拡張使用に利用できます。障害の発生時に WebDialer キャパシティを維持するため、冗長性を提供する追加のバックアップ WebDialer サーバを設置する必要があります。

Cisco WebDialer アプリケーションは、電話制御のために CTIManager と対話することに留意してください。有効にすると、各 WebDialer サービスは単一持続性 CTI 接続を CTIManager に開きます。また、各 WebDialer の個々の MakeCall（または EndCall）要求は一時的な CTI 接続を生成します。WebDialer コール レートの処理に必要な CTI 接続の数も、クラスタごとの CTI 接続制限に対して適用されます（クラスタごとの CTI 接続制限の詳細については、CTI のキャパシティ プランニング（9-32 ページ）を参照してください）。

WebDialer の設計上の考慮事項

次のガイドラインと制限は、Unified CM 環境内の WebDialer の配置と動作に関連して適用されます。

- 管理者は、すべての WebDialer ユーザが Unified CM エンド ユーザ ディレクトリの電話機またはデバイス プロファイルに関連付けられることを確認します。
  - 電話機が関連付けられていない状態でユーザが [Cisco WebDialer Preferences] 画面の [Use permanent device] を選択すると、Dial ボタンを押したときに次のメッセージが表示されます。

    「ユーザ用に設定されているサポート済みデバイスはありません（No supported device configured for user）」
  - デバイス プロファイルが関連付けられていない状態で（またはプロファイルを使用してログインしないで）ユーザが [Cisco WebDialer Preferences] 画面の [Use Extension Mobility] を選択すると、Dial ボタンを押したときに次のメッセージが表示されます。

    「*<dialed_ number>* へのコールに失敗しました：ユーザがログインしているデバイスがありません（Call to <dialed_ number> failed: User not logged in on any device）」
- HTTPS 経由の WebDialer および Redirector サーブレットのアプリケーションとのインターフェイス。
- クライアント識別コード（CMC）または強制承認コード（FAC）を使用している場合、WebDialer ユーザはトーンが聞こえたときに、電話機のキーパッドを使用して適切なコードを入力する必要があります。トーンが聞こえたときに適切なコードを入力しないと、コールの失敗を示すリオーダー トーンが聞こえます。
- Cisco WebDialer は、Cisco Computer Telephony Integration（CTI）をサポートする、すべてのシスコのエンドポイントで使用可能です。

Cisco Computer Telephony Integration（CTI）をサポートするシスコのエンドポイントの一覧については、次の URL にある『*CTI (TAPI/JTAPI) Supported Device Matrix*』を参照してください。

https://developer.cisco.com/site/jtapi/wiki/cti-tapi-jtapi-supported-device-matrix/

Cisco Unified Attendant Consoles

アテンダント コンソールの統合によって、受付係は、組織内でその目的のために特別に設計された Microsoft Windows デスクトップ アプリケーションからコールに応答したり、コールを転送または送信したりできます。Cisco Unified Attendant Consoles はローカルおよび企業のディレクトリへのアクセスを提供し、ユーザはユーザ回線の状態、Jabber のステータス、Skype for Business のステータス（Cisco Unified Attendant Console Advanced のみ）を見ることができます。

Cisco Unified Communications ポートフォリオには、次の 2 つのエディションの Cisco Unified Attendant Console が用意されています。

- Cisco Unified Attendant Console Standard

  このコンソールはユーザの電話機のモニタと制御を行うために Unified CM に直接統合されるローカル インストールです（「サーバレス」ソリューション）。コンソール アプリケーション経由で実行されるコール ルーティングと制御はソフトウェアへのログインに使用されるデバイスを模倣します。

- Cisco Unified Attendant Console Advanced

  このローカル アテンダント コンソール アプリケーションは中央の Cisco Unified Attendant Console Advanced Windows サーバ アプリケーションに接続します（Unified CM とは分離）。Cisco Unified Attendant Console Advanced サーバは Secure Socket Layer（SSL）を利用し、CTI および AXL 経由で Unified CM と通信します。すべてのコール ルーティングと制御は中央のサーバ アプリケーションによって実行されます。

ここでは、アテンダント コンソールの設計について次の項目を説明します。

- Cisco Unified Attendant Console Standard の設計上の考慮事項（18-48 ページ）
- Cisco Unified Attendant Console Advanced のアーキテクチャ（18-48 ページ）
- Cisco Unified Attendant Console Advanced の設計上の考慮事項（18-51 ページ）
- Cisco Unified Attendant Console のキャパシティ プランニング（18-53 ページ）

Cisco Unified Attendant Console Standard の設計上の考慮事項

次の設計上のガイドラインと制限は、Unified CM テレフォニー環境内の Cisco Unified Attendant Console Standard の導入および動作に適用されます。

- Cisco Unified Attendant Console Standard の各インストールには Unified CM との CTI および AXL 接続が必要です。
- コンソール ユーザ デバイスと連絡先に属するすべてのデバイス（Attendant Console ディレクトリ内に回線状態（話中ランプ フィールド）が必要）は定義済み Unified CM アプリケーション ユーザに割り当てる必要があります。
- 回線の総数（デバイスとそれぞれの回線の総数）は 5,000 を超えることができません。これはハードコードされた制限ではありませんが、この制限を超過すると Attendant Console および Unified CM 環境のパフォーマンスと安定性が低下する可能性があります。

共有回線およびコール ルーティングに関する設計上の考慮事項については、次の Web サイトで入手可能な最新バージョンの『*Cisco Unified Attendant Console Standard Installation and Configuration Guide*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-attendant-console-standard/model.html

Cisco Unified Attendant Console Advanced のアーキテクチャ

図 18-18 に、サーバ ベースの Cisco Unified Attendant Console Advanced 統合の上位レベル アーキテクチャの概要を示しますソリューションの機能と動作を理解することにより、アーキテクチャ自体の理解も深まります。次の一連の手順（図 18-18 を参照）は、アテンダント コンソールへの一般的なコールに関係するイベントを示しています。

1. コールが Unified CM に入ります。着信番号は CTI ルート ポイントに設定されたディレクトリ番号と一致します。
2. CTI ルート ポイントは、アテンダント コンソール サーバ アプリケーションによって CTI が制御され、サーバに設定されているキュー Direct Dial In（DDI）に関連付けられます。
3. アテンダント コンソール サーバ アプリケーションは、コールを直接 Computer Telephony（CT）ゲートウェイ デバイスのいずれかに内部的にリダイレクトします。このプロセスの一環として、アテンダント コンソール サーバ アプリケーションは、コールを CTI ポートにリダイレクトする CTI リダイレクト メッセージを CTI Manager サービスに送信します。

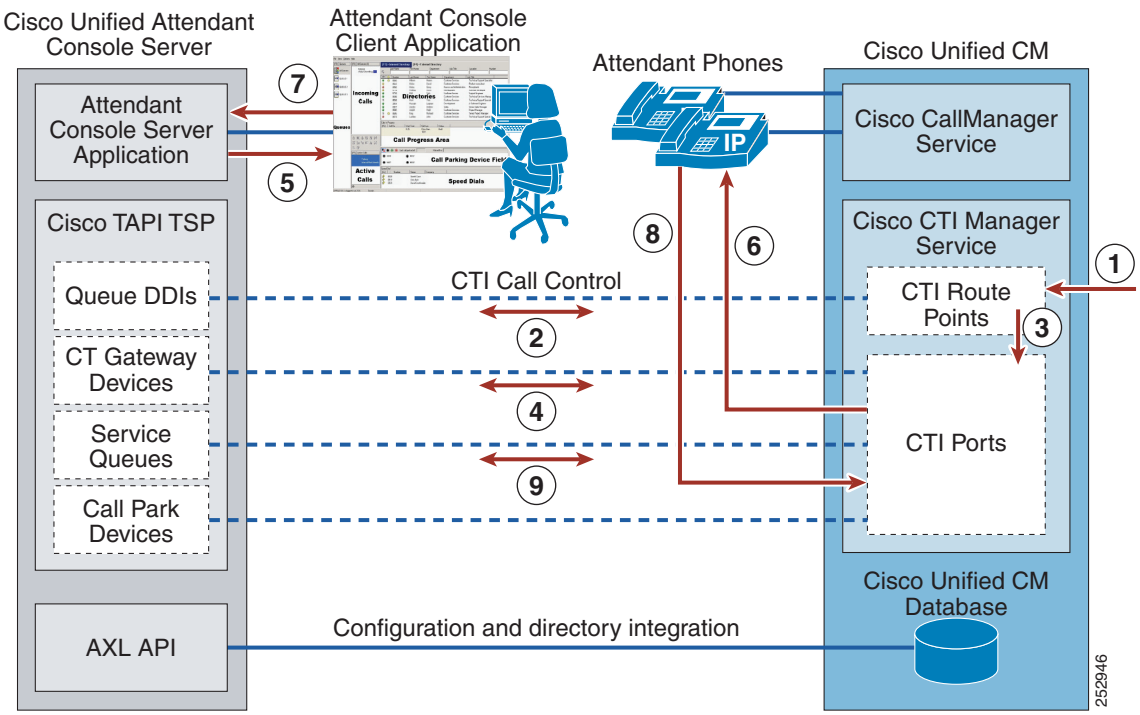
（注）　CTI リダイレクト メッセージでは、コールは接続されません。コールへの応答はなく、メディア接続もありません。

4. アテンダント コンソール サーバ アプリケーションはここで、コールを CT ゲートウェイ デバイスに関連付け、CTI ポートでそのコールを制御します。
5. この時点で、コールは、キュー DDI に関連付けられたシステム内のアテンダント コンソール クライアント アプリケーションに送信されます。
6. コンソール担当者がアテンダント コンソール クライアント アプリケーションを介してコールに応答することを選択すると、別の CTI リダイレクト メッセージが CTI Manager サービスに送信され、それによってコールが CTI ポートから応答するコンソール担当者の電話機に転送されます。コールは、コンソール担当者の電話機の設定に応じて、その電話機のハンドセットまたはヘッドセットに自動的に接続します。コンソール担当者の電話機および発信側のゲートウェイまたは電話機のリージョンとロケーションの設定によって、メディアに使用されるコーデックが決定します。
7. 別の内線番号への転送が必要である場合、コンソール担当者はアテンダント コンソール クライアント アプリケーションを介して転送を開始し、アテンダント コンソール サーバ アプリケーションに転送を伝達します。
8. アテンダント コンソール サーバ アプリケーションはそのコールを内部的にサービス キューに関連付け、CTI リダイレクト メッセージを CTI Manager サービスに送信します。これによって、コールはコンソール担当者の電話機からアテンダント コンソール サーバ アプリケーションによって制御される CTI ポートにリダイレクトされます。

（注）　コール転送はコンソール担当者の電話機から発信される場合もありますが、その場合はアテンダント コンソール サーバ アプリケーションがコール フローから外れ、拡張機能（転送再コール機能など）は利用できなくなります。

9. この段階で、サービス キューは転送を実行する前にコールに実際に応答するので（短い接続があります）、アテンダント コンソール サーバ アプリケーションにインストールされた Cisco Media ドライバが起動します。この CTI ポートおよびコール開始ゲートウェイまたは電話機のリージョンとロケーションの設定によって、メディアに使用されるコーデックが決定します。設定されている CTI ポートの保留音（MoH）オーディオ ソースも、発信者に聞こえる MoH に影響します。転送はこのように実行されるので、応答がない場合、アテンダント コンソール クライアント アプリケーションが引き続きコールを制御します。最終的な相手がコールを受信すると、アテンダント コンソール サーバ アプリケーションはコール フローから外れます。

図 18-18　サーバ ベースの Cisco Unified Attendant Consoles のアーキテクチャ



アテンダント コンソール サーバ アプリケーションのコール パーク機能では、Unified CM の固有のコール パーク機能は使用されません。代わりに、コール パーク デバイスを使用する独自のコール パーク機能が使用されます。コール パーク デバイスは、図 18-18 のステップ 7 ～ 9 にあるように、サービス キューとほとんど同様に機能します。転送と同様に、コール パーク デバイスを利用することで、コールのパーク中にアテンダント コンソール サーバ アプリケーションがコールを制御できるようになります。

Cisco Unified Attendant Console Advanced のハイ アベイラビリティ

Cisco Unified Attendant Console Advanced は、2 台の Cisco Unified Attendant Console サーバを持つ復元性の高い構成にインストールできます。

- パブリッシャ：クライアントによって使用されるプライマリ サーバ。このサーバに失敗した場合、すべてのアテンダントのオペレータはサブスクライバ サーバに切り替えられます。パブリッシャが再度実行されると、オペレータはパブリッシャに再接続するよう求められます（または設定により自動的に再接続されます）。
- サブスクライバ：パブリッシャが何らかの理由で停止した場合に使用されます。

CTI と AXL 通信の両方について、統合の両側に冗長性を備えることを検討する必要があります。

CTI に関しては、アテンダント コンソール サーバ アプリケーションは Cisco TAPI Telephony Service Provider（TSP）プラグイン（Unified CM からダウンロード）を使用して、CTI Manager サービスと通信します。Cisco TSP では、プライマリとバックアップの CTI Manager サービスを設定できます。プライマリの CTI Manager サービスがオフラインになった場合の復元性を高めるため、クラスタ内の少なくとも 2 つの Unified CM サブスクライバ ノードで CTI Manager サービスを有効にすることを推奨します。アテンダント コンソール サーバに障害が発生した場合の復元性を達成するには、キュー DDI に関連付けられた CTI ルート ポイントに対して設定された Call Forward Unregistered（CFU）および Call Forward CTI の障害接続先を利用します。アテンダント コンソール サーバ アプリケーションがオフラインになると、コールは自動的に Call Forward の設定に従います。たとえば、冗長アテンダント コンソールが配置されている場合、パブリッシャがオフラインになると、コールは Cisco Unified Attendant Console サブスクライバ サーバに転送されます。単一のアテンダント コンソール サーバでは、宛先として 1 台の IP Phone に関連付けられたハント パイロット番号またはディレクトリ番号（DN）を使用できます。

AXL 通信を有効にするには、Unified CM ノードで Cisco AXL Web Service をアクティブにします。複数の Unified CM ノードで Cisco AXL Web Service を有効にできますが、アテンダント コンソール サーバ アプリケーションには Unified CM 接続用に 1 つのエントリしか設定できません。障害が発生した場合、管理者は Cisco AXL Web Service を実行するバックアップ用の Unified CM ノードにこのエントリをアップデートできます。冗長 Cisco Unified Attendant Consoles が配置されている場合、アテンダント コンソール サーバは AXL Web Service の異なる Unified CM ノードで設定できます。

Unified CM には、Cisco Unified Attendant Console に属する一連の CTI ルート ポイントおよび CTI ポートが準備されています。関連付けられたデバイス プールにより、登録の維持を担当する Unified CM 呼処理ノードの優先順位付けされたリストを含む Unified CM グループが決定します。Unified CM グループ内のプライマリの Unified CM がオフラインである場合、CTI ルート ポイントと CTI ポートはセカンダリの Unified CM ノードを登録できるので、CTI ルート ポイントおよびポート自体のハイ アベイラビリティが実現します。

Cisco Unified Attendant Console Advanced の設計上の考慮事項

次の設計上のガイドラインと制限は、Unified CM テレフォニー環境内の Cisco Unified Attendant Console Advanced の導入および動作に適用されます。

- 次の一般的な設計指針は、アテンダント コンソール サーバ アプリケーション コンポーネントに適用します。
  - キュー DDI

    1 つの一意なキュー DDI が、特にアテンダント コンソールにルーティングされる、システム内の一意の着信ディレクトリ番号ごとに必要です。
  - CT ゲートウェイ デバイス

    キュー DDI に入るすべての着信コールは、直接 CT ゲートウェイ デバイスにリダイレクトされます。CT ゲートウェイ デバイスが所定の時間に予想される最大着信コール数を処理するのに十分な台数になるよう、システムを設計してください。
  - サービス キュー（Service Queue）

    コンソール担当者がコールを転送するか、コールを保留にするたびに、サービス キューが必要になります。システム内のすべてのコンソール担当者が所定の時間に転送する、または保留にするコールの最大数を維持できるだけの十分なサービス キューが用意されるように、システムを設計する必要があります。コンソール担当者ごとに 3 つか 4 つのサービス キューを用意することが一般的なガイドラインですが、シナリオによってはさらに多くのキューが必要になる場合もあります。

- コール パーク デバイス

  コンソール担当者がアテンダント コンソール クライアント アプリケーションを介してコール パーク機能を起動するたびに、コール パーク デバイスが必要になります。この機能では、Unified CM の固有のコール パーク機能は使用されません。所定の時間にシステム内のすべてのコンソール担当者がパークするコールの最大数を処理できるだけの十分なコール パーク デバイスが用意されるように、システムを設計してください。

- アテンダント コンソール サーバ アプリケーションに設定されたすべてのキュー DDI、CT ゲートウェイ デバイス、サービス キュー、およびコール パーク デバイスによって、Unified CM 内の CTI ルート ポイントまたは CTI ポートが作成されます。また、Cisco Unified Attendant Console Advanced の統合を処理するために必要な CTI 接続の数も、クラスタごとの CTI 接続制限までカウントされます（クラスタごとの CTI 接続制限の詳細については、CTI のキャパシティ プランニング（9-32 ページ）を参照してください）。
- アテンダント コンソール サーバ アプリケーションは、エンド ユーザ デバイスのビジー ランプ フィールド（BLF）モニタリングを可能にしますが、このアプリケーションでは、BLF スピード ダイヤル機能を実現する Unified CM 内の同一機能は使用されないことに注意してください。代わりに、アテンダント コンソール サーバ アプリケーションは、CTI を介して Unified CM と通信することで、モニタ対象デバイスの回線状態情報を取得します。アテンダント コンソール サーバ アプリケーションがエンド ユーザ デバイスをモニタする場合は、BLF のモニタ対象デバイスの台数が 2,000 に到達するまで、CTI 経由でモニタが継続されます。この上限に到達すると、BLF プラグインが、新しく要求されたデバイスをモニタするためにモニタ対象デバイスのリストからデバイスを削除し始めます。このため、アテンダント コンソール サーバから CTI 経由で開始されるデバイスの台数が上限（2,000）を超えることはありません。CTI 経由でモニタされるこれらのデバイスは、Unified CM 上の CTI 上限も考慮されます。
- Quality of Service（QoS）に関しては、アテンダント コンソール サーバ アプリケーション、アテンダント コンソール クライアント アプリケーション、および Cisco TSP はすべて Best Effort としてマークされたトラフィック（DSCP=0）を送信します。このトラフィックが WAN または通常輻輳するリンクを経由する場合は、ネットワークを介して優先的に処理されるようにパケットにマーキングする必要があります。これらのアプリケーションに関連付けられた TCP ポート番号の完全な一覧については、次の Web サイトで入手可能な最新バージョンの『*Cisco Unified Attendant Console Advanced Administration and Installation Guide*』を参照してください。

  https://www.cisco.com/c/en/us/support/unified-communications/unified-attendant-consoles/products-maintenance-guides-list.html

- Cisco TSP はパーティションを認識しません。したがって、Cisco Unified Attendant Console Advanced は重複するダイヤル プランをサポートしていません（この中には Attendant Console システム番号、コンソール ユーザ番号、連絡先番号が含まれます）。

Cisco Unified Attendant Consoles Advanced に関する追加の設計ガイダンスについては、次の Web サイトで入手可能なマニュアルを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-attendant-consoles/products-implementation-design-guides-list.html

Cisco Unified Attendant Console のキャパシティ プランニング

Cisco Unified Attendant Console のエディションの比較とそれぞれの機能については、Cisco Unified Attendant Console の製品ドキュメンテーションを参照してください。次の Web サイトで入手できます。

https://www.cisco.com/c/en/us/support/unified-communications/unified-attendant-consoles/tsd-products-support-series-home.html

Unified CM クラスタを正しくサイジングするには、Unified CM クラスタのスケーラビリティに影響する可能性がある相互依存変数が多数存在するため、シスコ代理店またはシスコのシステム エンジニアが Cisco Collaboration Sizing Tool（https://www.cisco.com/go/cst）を使用して、多数の CTI リソースと大量のコールを包含するすべての設計を検証する必要があります。サイジング ツールを使用すると、Attendant Console 設計基準を満たすために必要なサーバまたはクラスタの正確な台数を決定できます。

Cisco Paging Server

Cisco Paging Server は、ユーザが音声のみのメッセージを組織内の最大 50 の IP Phone のグループに送信できるようにします。Cisco Paging Server は基本的なページング モードの Singlewire InformaCast です。より大きい電話または他のエンドポイントのグループに通知、またはブロードキャストをスケジュールするユーザは、Advanced Notification モードへのアップグレードを検討する必要があります。

Cisco Paging Server はオープン仮想アプライアンス（OVA）として配布され、VMware 内で仮想マシンとして実行されます。この仮想マシンは Unified CM 仮想マシンと共存して実行する場合があります。Cisco Paging Server は、SIP、SNMP、AXL と CTI を使用して Unified CM と通信します。単一の Cisco Paging Server は Unified CM クラスタごとにサポートされます。

Cisco Paging Server は HTTP を使用して IP Phone と通信します。Cisco Paging Server 9.0.1 以降では、HTTP または CTI は電話機との通信に使用できます。HTTP モードでは、Cisco Paging Server はコマンドおよびクレデンシャルを IP Phone HTTP サーバに送信します。IP Phone は、クレデンシャルを検証し、次のコマンドを実行します。CTI モードでは、Unified CM 経由で各電話機にコマンドを送信します。CTI モードでは、Cisco Paging Server が各リクエストに対してクレデンシャルを送信する必要がないため、各電話機は Web サーバを有効化する必要がなく、コマンドがすばやく実行されます。また、CTI モードでは、話中電話機を迅速にチェックできます。

Cisco Paging Server が開始した後は、SNMP を使用して設定可能な間隔で Unified CM に接続します。Cisco Paging Server サーバは SNMP を使用して、他の Unified CM クラスタ メンバの IP アドレスと各クラスタ メンバに登録された電話機の一覧を検索します。SNMP 通信が完了すると、Cisco Paging Server は AXL を使用してデバイス名、説明、デバイス プール、コーリング サーチ スペース、電話番号やロケーションなどの各登録済みの電話に関する詳細情報を特定します。この情報は、*受信者グループ*と呼ばれる論理電話機グループを作成するのに使用できます。Cisco Paging Server では、受信者グループには最大 50 の電話機を含めることができます。

ブロードキャストは常に Cisco Paging Server へのボイスコールとして開始されます。Cisco Paging Server でのこれらのコールに応答するサービスは DialCast と呼ばれます。DialCast は CTI や SIP 経由でコールを受信できます。CTI の場合、コールは CTI ルート ポイントに着信し、処理されます（Cisco Paging Server では CTI ポートは着信コールに応答する必要はありません）。SIP の場合、コールは SIP トランクの Unified CM から発信します。CTI と SIP の両方が有効でサポートされます。ただし、SIP のトラブルシューティングは CTI のトラブルシューティングよりもはるかに容易なため、CTI 経由の SIP コール フローを推奨します。

Cisco Paging Server はマルチキャストを使用して IP Phone に音声を送信します。マルチキャスト ストリームは Cisco Paging Server から発信され、IP Phone で受信されます（図 18-19 を参照）。

図 18-19　複数の電話機グループにメッセージを送信する Cisco Paging Server

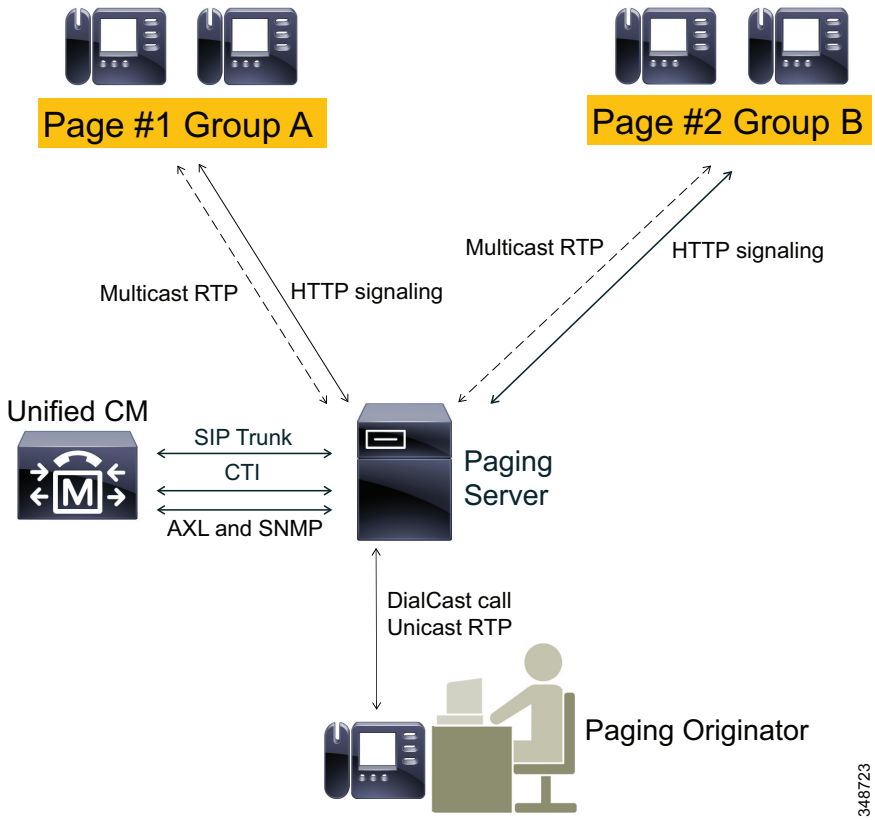


図 18-19 に示すように、このシーケンスは Cisco Paging Server が 1 台以上の IP Phone に対してブロードキャストを開始する方法を説明します。

1. 発信者は、Unified CM で定義された番号にダイヤルします。この番号は、SIP トランクまたは CTI ルート ポイント経由で Cisco Paging Server にコールをルーティングします。
2. Cisco Paging Server は、このコールに DialCast コールとして応答します。
3. 発信者には低く小さいトーンが聞こえます。Cisco Paging Server はこのトーンを再生しますが、受信者グループ内の各電話機に HTTP 経由でコマンドを送信します。このコマンドは、各電話機にマルチキャスト グループに参加するよう要求します。
4. すべての電話機がマルチキャスト グループに参加すると、Cisco Paging Server はゴーサインを示す高いトーンを再生します。発信者にこのトーンが聞こえる場合、Cisco Paging Server が RTP ストリームを発呼側 IP Phone から受信側の電話機にマルチキャスト RTP ストリームとして送信していることを示します。発信者が話すと、その音声は受信側の電話に送信されます。
5. 発信者が切断すると Cisco Paging Server は各 IP Phone に別の要求を送信します。このとき、マルチキャスト グループから抜けてブロードキャストは終了します。

Cisco Paging Server の設計上の考慮事項

電話機の選択および Unified CM 機能の相互作用

- すべての Cisco IP Phone が Cisco Paging Server と互換性があるわけではありません。最新のリストについては、次の URL で入手可能な互換性情報を参照してください。

  https://www.singlewire.com/compatibility-matrix

- ブロードキャストを受信するには、IP Phone でスピーカーフォンが有効になっていなければなりません。
- Cisco Paging Server は応答不可（DND）を認識せず、DND 対応の電話機に送信します。

マルチキャストの考慮事項

- Cisco Paging Server と IP Phone が別々の IP サブネットにある場合、これら 2 つのサブネット間のルータをマルチキャスト ルーティング用に設定する必要があります。
- Cisco Paging Server はマルチキャスト ルーティングに特別な方法（SM、DM、S-DM、SSM など）を必要としません。
- ワイドエリア ネットワークによってはマルチキャスト ルーティングをサポートしないものもあります。これらの環境においては、サイト間で GRE トンネルが構築され、マルチキャスト転送に使用される場合があります。
- マルチキャスト メディア ストリームは常に G.711 mu-law コーデックを使用します。その他のコーデックは許可もサポートもされません。
- RTP フローは常に、開始側から Cisco Paging Server からのユニキャストであり、Cisco Paging Server から受信側の電話へのマルチキャストです。Cisco Paging Server が中央に展開する場合、ページは WAN の境界を通過する場合があります。
- Cisco Paging Server のマルチキャスト メディア ストリームはコールではありません。これらは、RSVP にも、ロケーション ベースのコール アドミッション制御にも、適用されません。WAN エンジニアは企業ネットワーク上の他の音声ストリーミングに加えて、これらのマルチキャスト メディア ストリームにもバジェットを割り当てる必要があります。ただし、開始側と Cisco Paging Server の間のコールは通常のボイスコールです。このコールは通常のコール アドミッション制御の制限があります。
- マルチ サイト配置がある場合は、単一のデフォルト アドレスよりも、マルチキャスト アドレス範囲を使用するページング サーバを設定することを推奨します。これは、Internet Group Management Protocol（IGMP）のマルチキャストの join が、アドレスおよびポートではなく、マルチキャスト アドレスのみで有効になるためです。2 つのブロードキャストが異なる 2 つのサイトで同時に行われる場合、いずれかのサイトの電話機はマルチキャスト アドレスだけに IGMP Join を送信します。両方のサイトが 1 つの同じアドレスを使用する場合、両方でブロードキャストの RTP ストリームは両方のサイトに送信されます。
- マルチキャスト ストリームは IPSec トンネルを通過する場合を除き、暗号化できません。
- 異なる電話機モデルとファームウェア バージョンはスイッチの設定に影響を与える可能性があるさまざまな IGMP バージョンを使用している可能性があります。

その他の考慮事項

- DialCast への着信コールは、G.711 mu-law コールである必要があります。他のコードを使用して DialCast に着信するコールはトランスコーディングされる必要があります。
- Cisco Paging Server は Unified CM への CTI 接続を維持しますが、この CTI 接続が Unified CM に配置する負荷は非常に低くします。この接続が必要とするリソースは、クラスタのサイズに関係なく一定に保たれます。
- Cisco Paging Server は、サーバと電話機との間のファイアウォールが Network Address Translation（NAT）を使用するように構成されないことを要求します。
- Cisco Paging Server 8.4 以降は、QoS 値は Unified CM デフォルト値（シグナリング用の DSCP CS3 とメディア用の DSCP EF）に設定されます。シグナリング（DSCP CS3）は CTI および SIP トラフィックに適用され、メディア（メディア（DSCP EF）は SIP および CTI 側開始 RTP ストリームと発信マルチキャスト RTP ストリームに適用されます。Paging Server DSCP 値はフィールドでは変更できません。これらとは異なる DSCP 値を使用するユーザは、ネットワークのページング サーバ トラフィックを再マークする必要があります。

詳細については、次の URL から入手可能な『*InformaCast Virtual Appliance Basic Paging Installation and User Guide*』の最新バージョンを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/paging-server/products-maintenance-guides-list.html

シスコのボイス メッセージング

改訂日：2018 年 3 月 1 日

この章では、Cisco Unified Communications システムで利用可能なボイス メッセージング ソリューションについて説明します。この章では、シスコのボイス メッセージング製品である Cisco Unity Connection、および Cisco Unity Express を取り上げ、これらの製品を Cisco Unified Communications Manager（Unified CM）とともに配置するための設計ガイドラインとベスト プラクティスを説明します。また、この章では、業界標準プロトコルを使用した、サードパーティ製ボイスメール システムとの統合についても説明します。

このガイドでは、Unified CM に関するメッセージング配置のシナリオが中心ですが、特に、集中型 Unified CM 配置の Survivable Remote Site Telephony（SRST）フォールバック サポートで使用される場合には、適宜、Cisco Unified Communications Manager Express（Unified CME）についても説明します。

この章では、次のトピックについて取り上げます。

この章ではまず、Cisco メッセージング ソリューションのポートフォリオの各製品について簡単に説明した後、企業向け Unified Communications ソリューションにおける各製品の位置付けに関する簡単な概要を示します。次に、メッセージング配置モデルを基盤として、ボイスメール統合を説明します。ここではまず、さまざまなメッセージング配置モデルを定義した後、さまざまな Unified CM 呼処理配置モデルにおける各メッセージング配置モデルの位置付けを説明します。この項では、Cisco Unity Connection について説明します。Cisco Unity Express については、別に専用の項を設けて、サポートされる配置モデルを説明します。シスコのボイス メッセージング製品ポート フォリオ内で利用可能な相互運用性のための主要な設計ガイドラインについて説明します。仮想化では、仮想システム設計時に考慮する必要がある重要な設計上の要素についても説明します。この項では、トランスコーディングや Unified CM とのさまざまな統合を含む、多くのシステムレベルの設計上の考慮事項およびベスト プラクティスについて説明します。さらに、この章では、サポートされている業界標準プロトコルを使用したサードパーティ製ボイスメール統合の詳細について説明します。

この章では、基本設計に関する説明を行います。また、Unified CM を使用してコラボレーション システムにボイス メッセージング製品をどのように組み込むかに重点を置いて説明します。各製品の詳細な設計ガイドラインおよびサードパーティ製のメッセージングとテレフォニー システムの相互運用性に関する情報については、次に示す Cisco Unity Connection の設計ガイドを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

ボイス メッセージング ポートフォリオ

Cisco Unified Communications のメッセージング ポートフォリオは、Cisco Unity Connection と Cisco Unity Express の 2 つの主なメッセージング製品で構成されます。それぞれの製品が対応する要件は異なりますが、互いに他の製品と重なり合う機能とスケーラビリティを備えています。また、ボイス メール ネットワーキングを使用して互いに連携する機能により、この章で後ほど説明するとおり、より高いスケーラビリティに加えてボイスメールの相互運用性を実現します。

これらの製品を検討する場合、それらに搭載されたメッセージング オプションを理解し、特定の配置要件に適したオプションを判断するためには、製品が該当するメッセージング タイプを考慮することが役立ちます。次の定義は、このようなメッセージング タイプの説明に役立ちます。

- *ボイスメール専用*とは、いずれのメッセージング クライアント経由でもボイスメールにアクセスできないテレフォニー ボイスメール統合を指します。
- *ユニファイド メッセージング*とは、テレフォニー アクセス、およびメッセージ クライアントを介したボイスメールへのアクセスを備えたボイスメールを指します。
- *ユニファイド メッセージング*とは、テレフォニー アクセス、およびメッセージング クライアントを介したボイスメール、電子メール、FAX へのアクセスを備えたボイスメールを指します。

表 19-1 は、これらのタイプのメッセージングをサポートするシスコ製品を示します。

表 19-1　各製品でサポートされるメッセージング環境

メッセージング タイプ	Cisco Unity Connection	Cisco Unity Express
ボイスメール専用	○	○
ユニファイド メッセージング	○	○
ユニファイド メッセージング	○	X

（注）　Cisco Unity Connection を使用したユニファイド メッセージングの詳細については、Cisco Unity Connection による単一受信トレイ（19-45 ページ）を参照してください。

上のメッセージング タイプと定義に基づき、次の 2 つのメッセージング製品のオプションが用意されています。

- Cisco Unity Connection

  このオプションは、20,000 ユーザ以下の中規模企業用に、ユニファイド/統合メッセージング、音声認識、およびコール転送ルールを 1 つのシステムに組み合わせて管理しやすくしたものです。また、デジタルまたは HTTP ネットワーク システムを使用して、複数の Cisco Unity Connection クラスタを組み合わせることができます。（必要であれば、さらに Voice Profile for Internet Mail（VPIM）ネットワーキングを使用して、100,000 人を超えるユーザをサポートするために 2 つの HTTP またはデジタル ネットワーク システムを結合することができます）。Cisco Unity Connection は、1 つのデジタル ネットワークまたは HTTPS ネットワーク上で最大 100,000 人のユーザをサポートできます。Cisco Unity Connection は、Cisco Business Edition でも利用できます。Cisco Business Edition 6000 は、最大 1,000 人のユーザまでサポートします。Cisco Business Edition 7000 では、通常の Cisco Unity Connection のキャパシティ プランニング ルールが適用されます。Cisco Business Edition の詳細については、呼処理の設計上の考慮事項（9-26 ページ）を参照してください。

- Cisco Unity Express

  このオプションは、中小規模企業および 500 ユーザ以下の支社用に、特定の Cisco サービス統合型ルータ（ISR）で、コスト効率の良いボイス メッセージングおよび統合メッセージング、自動応答、および自動音声応答（IVR）の各機能を提供します。Cisco Business Edition 4000 の一部として、Cisco ISR 4321 上のコンテナとして展開された Unity Express は最大で 200 人のユーザをサポートします。

製品機能の比較については、次の場所にある機能比較資料を参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/unity-connection/datasheet-listing.html

ボイス メッセージング製品のスケーラビリティの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章のボイス メッセージング（25-45 ページ）の項を参照してください。

この章では、Cisco Unity Connection および Cisco Unity Express と Cisco Unified Communications Manager（Unified CM）の統合について、設計上の側面を中心に説明します。Cisco Unified CM には、Session Initiation Protocol（SIP）トランクの機能が搭載されているため、SIP プロキシ サーバを配置することなく、直接 Cisco Unity Connection と統合できます。

上で説明したように、この章で扱う設計に関するトピックは、ボイスメールのみの設定、ユニファイド メッセージング設定、およびユニファイド メッセージング設定に適用されます。さらに、この章では、Microsoft Exchange（2003、2007、または 2010）と Cisco Unity Connection の配置の設計面について説明します。Cisco Unity Connection および Unity Express は外部メッセージ ストアに依存しません。

Cisco Unity Connection に関するその他の設計情報（他のシスコ以外のメッセージング システムとの統合など）については、次の場所にある『*Design Guide for Cisco Unity Connection*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

Cisco Unity Express に関するその他の設計情報（他のシスコ以外のメッセージング システムとの統合など）については、次の Web サイトで入手可能な適当な製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/unity-express/index.html

メッセージング配置モデル

この章では、Cisco Unity Connection および Cisco Unity Express について、さまざまなメッセージング配置モデルの概要を示します。Cisco Unity Connection に固有の配置モデルや設計に関する考慮事項とさまざまなメッセージング コンポーネントの詳細については、次の場所にある『*Design Guide for Cisco Unity Connection*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

Cisco Unity Express については、次の Web サイトで入手可能な適当な製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/unity-express/index.html

Cisco Unity Connection は、次の 3 つの主なメッセージング配置モデルをサポートしています。

- 単一サイト メッセージング
- 集中型メッセージングを使用するマルチサイト配置
- 分散型メッセージングを使用するマルチサイト配置

Cisco Unity Express もまた、次の 3 つの主なメッセージング配置モデルをサポートしています。

- 単一サイト メッセージング
- 分散型メッセージングを使用するマルチサイト配置
- Cisco Unified CME により分散型メッセージングを使用するマルチサイト配置

（注） Cisco Unity Express は、最大 10 の Unified CME を持つ集中型ボイス メッセージングをサポートします。詳細については、https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-express/index.html にある Cisco Unified Communications Manager Express のマニュアルを参照してください。

Cisco Unified CM と Unified CME の呼処理配置モデルは、Cisco Unity Connection および Unity Express のメッセージング配置モデルに依存しませんが、互いに対して考慮が必要な暗黙的要件があります。

アクティブ/アクティブ設定では、Cisco Unity Connection のメッセージング冗長性を利用できます。詳細については、次の場所にある『*Design Guide for Cisco Unity Connection*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

すべてのメッセージング配置モデルが、ボイスメール、ユニファイド メッセージング、およびユニファイド メッセージングのインストールをサポートしています。

単一サイト メッセージング

このモデルでは、メッセージング システムとメッセージング インフラストラクチャ コンポーネントがすべて、同じサイトのアベイラビリティの高い同じ LAN 上に置かれます。サイトは、単一サイトである場合も、高速メトロポリタン エリア ネットワーク（MAN）を介して相互接続されたキャンパス サイトである場合もあります。メッセージング システムのクライアントもすべて、単一（またはキャンパス）サイトに置かれます。このモデルの際立った特徴は、リモート クライアントが存在しないことです。

集中型メッセージング

このモデルでは、単一サイト モデルと同様に、メッセージング システムとメッセージング インフラストラクチャ コンポーネントがすべて、同じサイトに置かれます。サイトは、1 つの物理的なサイトである場合も、高速 MAN を介して相互接続されたキャンパス サイトである場合もあります。ただし、単一サイト モデルとは異なり、メッセージング クライアントをローカルとリモートの両方に置くことができます。

分散型メッセージング

分散型メッセージング モデルは、共通のメッセージング バックボーンを持つ複数の単一サイト メッセージング システムで構成されます。複数のロケーションを持つことができ、各ロケーションに独自のメッセージング システムとメッセージング インフラストラクチャ コンポーネントが置かれます。すべてのクライアント アクセスが各メッセージング システムに対してローカルであり、メッセージング システムは、すべてのロケーションにまたがるメッセージング バックボーンを共有します。分散型メッセージング システムからのメッセージ送信は、フルメッシュ タイプまたはハブアンドスポーク タイプのメッセージ ルーティング インフラストラクチャによって、メッセージング バックボーンを介して行われます。

分散型メッセージングは、基本的に、共通のメッセージング バックボーンを持つ複数の単一サイト メッセージング モデルです。このルールの例外は、PBX-IP Media Gateway（PIMG）統合と T1-IP Media Gateway（TIMG）統合です。PIMG 統合と TIMG 統合は、設計に関するこのドキュメントでは説明しません。PIMG または TIMG の詳細については、次の場所にある最新の Cisco Unity Connection の統合ガイドを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html

分散型メッセージング モデルは、ローカルおよびリモートの GUI クライアント、TRaP、およびメッセージのダウンロードに関して、集中型メッセージングと同じ設計基準を持っています。

メッセージングと Unified CM 配置モデルの組み合わせ

ここでは、さまざまなメッセージング配置モデルを Unified CM 呼処理配置モデルに統合する場合の設計上の考慮事項について説明します。表 19-2 では、Cisco Unity Connection および Unity Express によってサポートされるメッセージング配置モデルと呼処理配置モデルのさまざまな組み合わせを示します。

表 19-2　サポートされているメッセージングと Unified CM 呼処理配置モデルの組み合わせ

モデル タイプ	Cisco Unity Connection	Cisco Unity Express
単一サイト メッセージングと単一サイト呼処理	○	○
集中型メッセージングと集中型呼処理	○	X[1]
分散型メッセージングと集中型呼処理	○	○
集中型メッセージングと分散型呼処理	○	なし[1]
分散型メッセージングと分散型呼処理	○	○
集中型メッセージングと WAN を介したクラスタリング	○	X
分散型メッセージングと WAN を介したクラスタリング	○	○

1. Unified CME による集中型ボイスメール メッセージングが Cisco Unity Express でサポートされていますが、これは Unified CM 呼処理配置モデルには適用されません。

この項では、次の項目について説明します。

- Cisco Unity Connection メッセージングおよび Unified CM の配置モデル
- Cisco Unity Express の配置モデル

各トピックではメッセージングと Unified CM の配置モデルの組み合わせを定義した後、そのモデルに適用可能なシスコのボイスメール メッセージング製品と、そのモデルの組み合わせに関する設計上の考慮事項について説明します。ここでは、各製品のすべての組み合わせを取り上げるわけではありません。いくつかの例を示し、各製品のベスト プラクティスと設計上の考慮事項を説明します。ここでの説明は、基本となるメッセージング配置モデルと Unified CM とのインタラクションの理解を促すためのものであり、すべての可能性を詳細に説明することは意図していません。

サイト分類の詳細と、サポートされているメッセージング配置モデルと呼処理配置モデルの組み合わせの詳細な分析については、次の場所にある『*Design Guide for Cisco Unity Connection*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

Cisco Unity Connection メッセージングおよび Unified CM の配置モデル

ここでは、Cisco Connection によってサポートされるメッセージング配置モデルと呼処理配置モデルのさまざまな組み合わせを示します。

集中型メッセージングと集中型呼処理

集中型メッセージングでは、ボイス メッセージング サーバは Unified CM クラスタと同じサイトに配置されます。集中型呼処理では、サブスクライバがクラスタおよびメッセージング サーバに対して、リモートとローカルのどちらにも存在できます（図 19-1 を参照）。リモート ユーザが中央のサイトのリソース（音声ポート、IP Phone、テールエンド ホップオフ（TEHO）の場合の PSTN ゲートウェイなど）にアクセスする場合、そのコールはゲートキーパー コール アドミッション制御にとって透過的になります。したがって、Unified CM でリージョンとロケーションを設定して、コール アドミッション制御を提供する必要があります。（帯域幅の管理（19-33 ページ）を参照）。IP フォンまたは MGCP ゲートウェイにリージョン間コールを発信する場合、IP フォンは設定済みのリージョン間コーデックを自動的に選択します。

図 19-1　集中型メッセージングと集中型呼処理

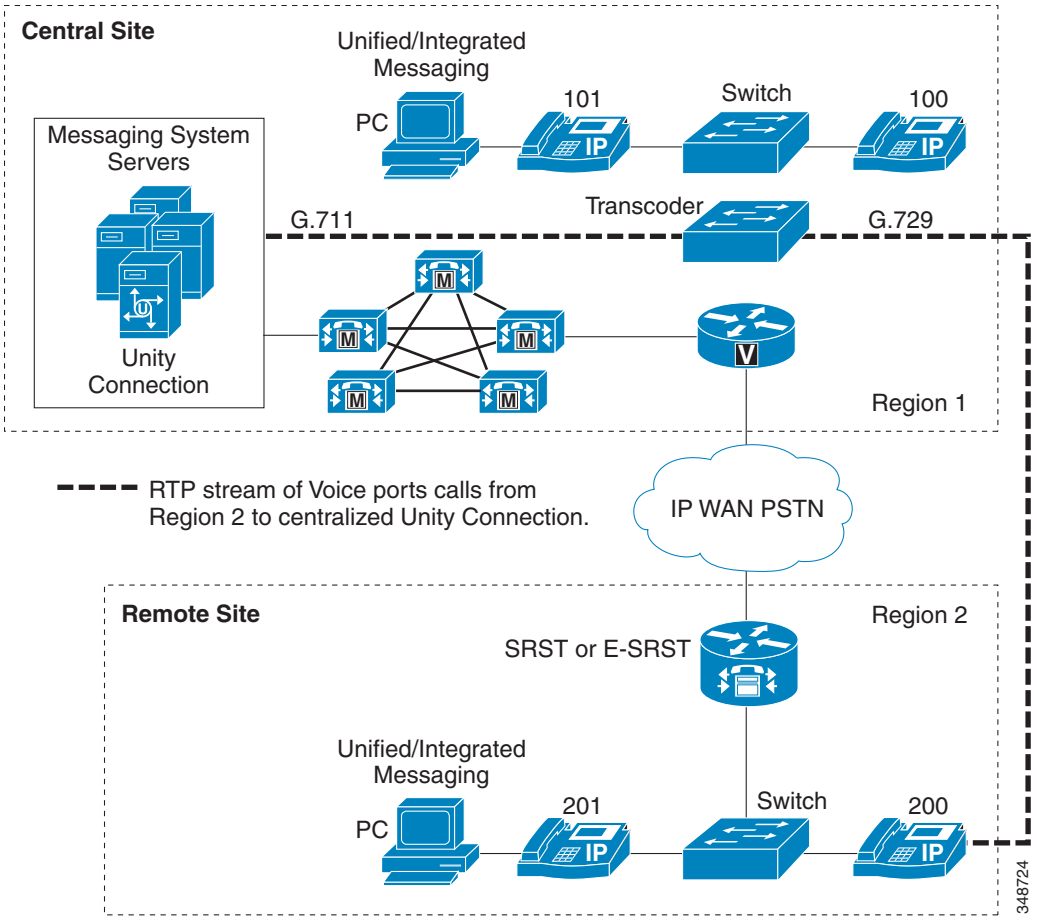


図 19-1 では、リージョン 1 と 2 が、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。

図 19-1 で示しているように、内線番号 200 からリージョン 1 のボイスメール ポートにコールが発信されると、エンドポイントではリージョン間の G.729 コーデックが使用されますが、RTP ストリームがトランスコードされ、音声ポート上では G.711 が使用されます。Unified CM トランスコーディング リソースは、ボイスメール システムと同じサイトに置く必要があります。

AAR によってルーティングされるボイスメール コールで RDNIS が送信されないことによる影響

集中メッセージング環境では、WAN がオーバーサブスクリプションの状態になった場合に、Unified CM の機能である Automated Alternate Routing（AAR; 自動代替ルーティング）が、PSTN を介してコールを中央サイトのメッセージング ストアにルーティングできます。ただし、PSTN を介してコールが再ルーティングされる場合、Redirected Dialed Number Information Service（RDNIS）が損なわれることがあります。Cisco Unity Connection がメッセージング クライアントに対してリモートである場合は、正しくない RDNIS 情報によって、AAR が PSTN を介して再ルーティングするボイスメール コールに影響が及ぶことがあります。RDNIS 情報が正しくない場合、コールはダイヤル先のユーザのボイスメール ボックスに到達せず、自動アテンダント プロンプトを受信します。発信者は、到達を試みているユーザの内線番号を再入力するように要求されることがあります。この動作は主に、電話通信事業者がネットワークを介した RDNIS を保証できない場合の問題です。通信事業者が RDNIS の正常な送信を保証できない理由は数多くあります。通信事業者に問い合わせて、回線のエンドツーエンドで RDNIS の送信を保証しているかどうかを確認してください。オーバーサブスクリプションの状態になった WAN に対して AAR を使用する代わりの方法は、単に、オーバーサブスクリプションの状況で発信者にリオーダー トーンが聞こえるようにすることです。

Cisco Unity Connection Survivable Remote Site Voicemail

Cisco Unity Connection Survivable Remote Site Voicemail（SRSV）は、WAN の障害時に支社サイト ユーザにボイスメール サービスのサバイバビリティを提供する、集中型 Cisco Unified Communications Manager および Cisco Unity Connection 展開モデルで使用されます。現在、Cisco Unity Connection は、Cisco Unified Messaging Gateway を使用せずに、中央サイトで SRSV 機能をネイティブでサポートしています。Cisco Unity Connection SRSV は、Cisco Unity Express SRSV の代替オプションです。Cisco Unity Connection は、通常の動作中に、電話機とユーザ メールボックスに関する情報を支社サイト SRSV サーバに更新します。WAN の障害時に Unity Connection SRSV ブランチ サーバは、バックアップ自動応答およびボイスメール ストレージとして機能します。すべての着信中の無応答コールおよびビジー コールは、外部発信者または内部発信者がボイス メッセージを残す可能性がある Unity Connection SRSV ブランチ サーバに転送されます。

WAN が回復すると、すべてのボイスメールが支社サイト SRSV から削除され、中央 Cisco Unity Connection サーバにアップロードされます。アップロードが完了すると、支社サイト SRSV がアイドル状態に移行します。すべての着信中の無応答コールおよびビジー コールが、中央 Cisco Unity Connection サーバに再度転送されます。

SRSV 配置モデル

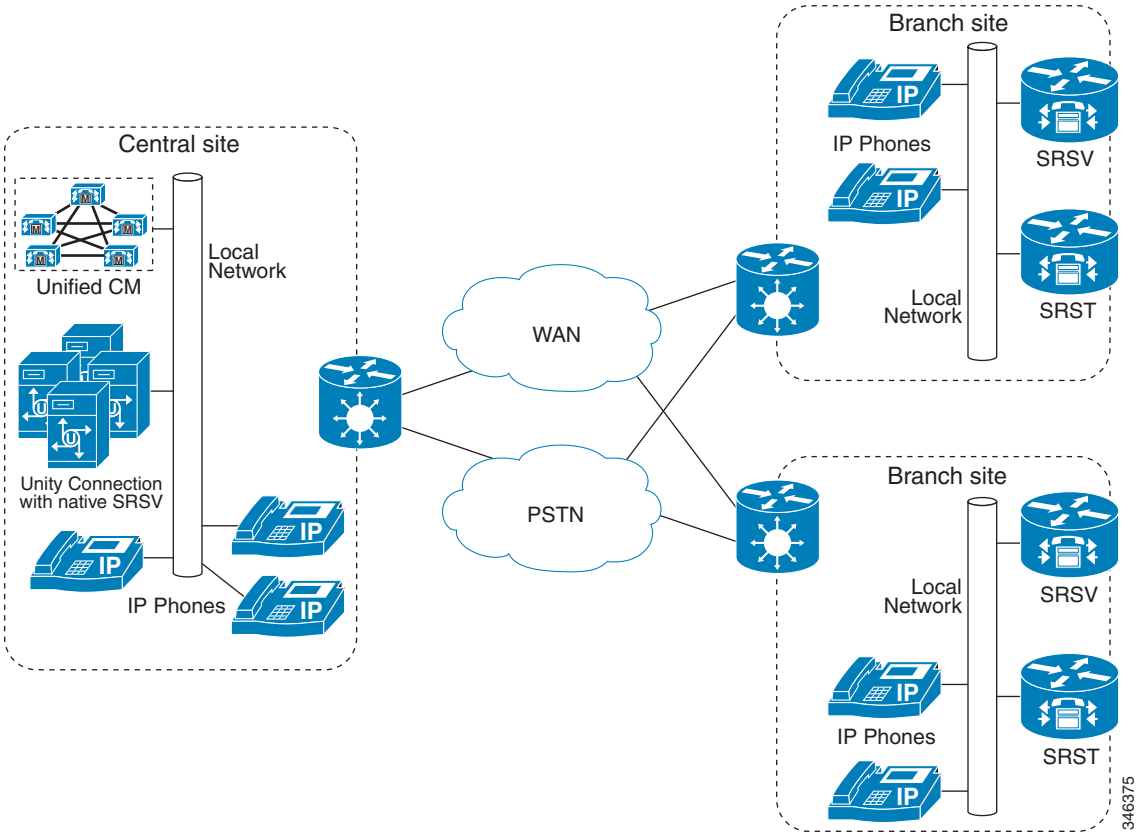
次の配置モデルが Survivable Remote Site Voicemail（SRSV）をサポートしています。

- 集中型 Unfied CM および Unity Connection がある支社サイトの SRST または E-SRST（19-9 ページ）
- 集中型 Unified CM/Unity Connection がある支社サイトの複数の E-SRST または SRST サーバ（19-10 ページ）

集中型 Unfied CM および Unity Connection がある支社サイトの SRST または E-SRST

図 19-2 に示すように、中央サイトには、正常な状態でプライマリ呼処理およびボイス メッセージ サービスを提供するための Cisco Unified CM および Unity Connection が含まれています。支社サイトでは、Cisco Unified Enhanced Survivable Remote Site Telephony（E-SRST）および Cisco Unity Connection SRSV ブランチ サーバが、WAN 障害時のバックアップ コール エージェントとボイス メッセージング サーバとしてインストールされています。中央サイトにインストールされている Cisco Unity Connection は、すべての電話機とボイス メールボックスの情報を支社サイト SRSV サーバにアップロードします。中央サイトへの接続が失われるまで、SRST または E-SRST はアイドル状態のままです。支社サイトが中央サイトから分離され、電話機と Unified CM 間のキープアライブ タイマーの期限が切れると、未応答のコールとビジー コールを Unity Connection SRSV ブランチ サーバに送信するように事前設定された E-SRST または SRST ルータに支社の電話機が復帰します。サブスクライバは、ボイスメールにアクセスして WAN の障害時に残されたボイス メッセージを聞くことができます。WAN が回復すると、すべてのボイス メッセージは、中央 Cisco Unity Connection のサブスクライバ メールボックスにアップロードされます。

図 19-2　集中型 Unfied CM および Unity Connection がある支社サイトの SRST または E-SRST

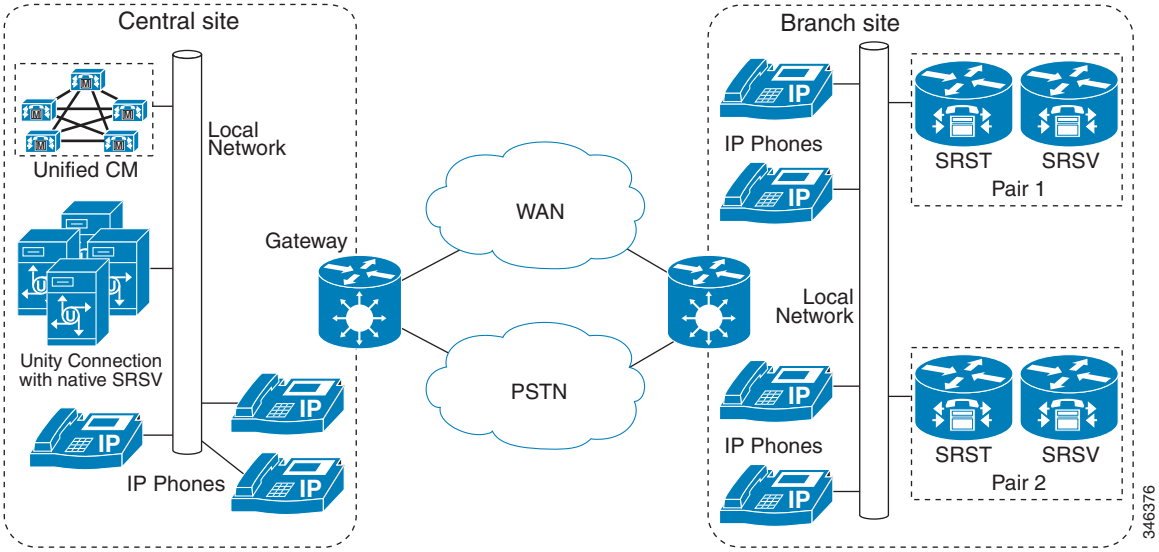


集中型 Unified CM/Unity Connection がある支社サイトの複数の E-SRST または SRST サーバ

この配置モデルは、最初のシナリオに似ていますが、複数の E-SRST と Cisco Unity Connection SRSV ブランチ サーバがロード バランシングのために支社サイトでペアになっています（図 19-3 を参照）。管理者は、Unified CM の 2 つの異なる SRST 参照を使用して 2 つの E-SRST サーバにわたって支社サイト ユーザを手動で分割し、ロード バランシングを実現する必要があります。Cisco Unity Connection は、メールボックス情報をペア化されている適切な Cisco Unity Connection SRSV ブランチ サーバにプッシュします。この設定では、各 Cisco Unity Connection SRSV ブランチ サーバに 1 つの支社 E-SRST のユーザのメールボックスが含まれます。

各 Cisco Unity Connection SRSV ブランチ サーバは、WAN 障害時にペア化された E-SRST ルータから転送されたコールを処理します。最初のシナリオと同様に、Cisco Unity Connection SRSV ブランチ サーバは、WAN の回復時に中央 Cisco Unity Connection のサブスクライバ メールボックスにすべてのボイスメールをアップロードします。

図 19-3　集中型 Unified CM/Unity Connection がある支社サイトの複数の E-SRST または SRST サーバ



（注）　支社サイトで、複数の E-SRST サーバと単一の Cisco Unity Connection SRSV ブランチ サーバのペア化はサポートされていません。

Survivable Remote Site Voicemail の配置ガイドライン

- サポートされるリモート サイトの最大数は、中央 Cisco Unity Connection ごとに 35 個です。各仮想プラットフォーム オーバーレイでサポートされるリモート サイトの詳細については、次の URL で入手可能な最新バージョンの『*Cisco Unity Connection Supported Platforms List*』を参照してください。

  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-guides-list.html

- このソリューションでは、SRST および拡張 SRST（E-SRST）の両方のフォールバック方式をサポートしています。Cisco Unity Connection SRSV ブランチ サーバは、Cisco Services-Ready Engine（SRE）900 と 910 ブレード サーバ、および Cisco Unified Computing System（UCS）または UCS E-Series などのサポートされている Cisco Unity Connection プラットフォームで動作します。Cisco Unity Connection SRSV ブランチ サーバと SRST または E-SRST ルータの両方が、単一の論理ユニットとして表示されます。ここで SRST ルータは、WAN の障害時にすべての制御シグナリングを処理します。
- Cisco Unity Connection SRSV ブランチ サーバは、WAN リンクがダウンし、SRST がアクティブ状態の場合にアクティブになります。それ以外の場合は、アイドル状態のままです。
- Cisco Unity Connection と Cisco Unity Connection SRSV との間で接続をセキュアに保つには、HTTP over Secure Socket Layer（SSL）プロトコルを使用します。

SRSV では、次のアクティビティを行う場合に WAN リンクの帯域幅が使用されます。

- Cisco Unity Connection から Cisco Unity Connection SRSV への設定のアップロード
- WAN リンクが復元された場合に、支社 Cisco Unity Connection SRSV サーバから中央 Cisco Unity Connection に音声メッセージをアップロード

分散型メッセージングと集中型呼処理

分散型メッセージングは、テレフォニー環境内に複数のメッセージング システムが分散されており、各メッセージング システムがローカル メッセージング クライアントだけにサービスを提供することを意味します。このモデルは集中型メッセージングとは異なります。集中型メッセージングでは、メッセージング システムに対してローカルなクライアントとリモートのクライアントの両方が存在します。

図 19-4 では、集中型呼処理を使用する分散型メッセージング モデルを示しています。他のマルチサイト呼処理モデルと同様に、WAN 帯域幅を管理するためにリージョンとロケーションを使用する必要があります。

E-SRST モードの Cisco Unified Communications Manager Express は、IP フォンおよび Cisco Unity Connection ボイスメール ポートの両方の呼処理バックアップに使用されます。このフォールバック サポートは、リモート サイト（たとえば、図 19-4 のリージョン 2）に配置され、WAN 障害などのために電話機と Unified CM との接続が失われた場合に、バックアップの呼処理を提供します。またリモート サイトのユーザに対し、WAN 障害時に、ローカルの Cisco Unity Connection サーバへのアクセスと MWI のサポートを提供します。E-SRST モードの詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/unified-survivable-remote-site-telephony/index.html

図 19-4　　分散型メッセージングと集中型呼処理

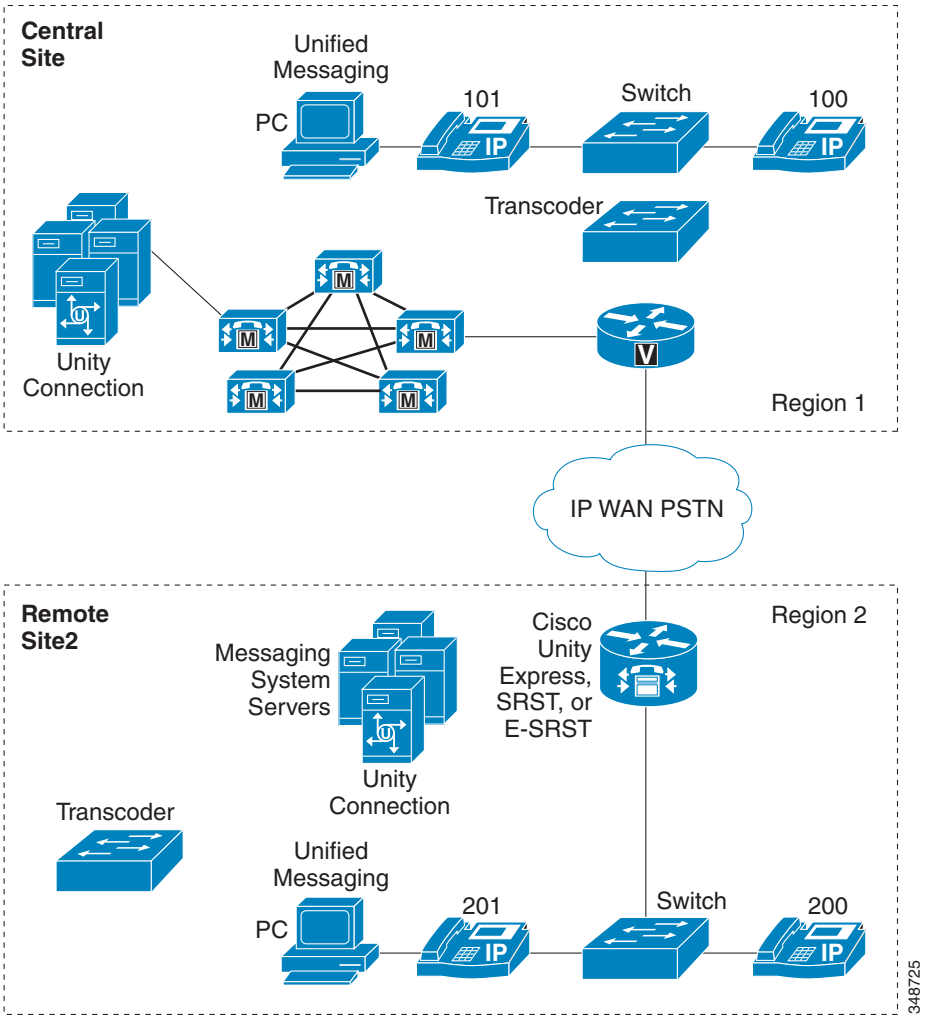


図 19-4 の構成では、トランスコーダ リソースが各 Cisco Unity Connection メッセージ システム サイトに対してローカルである必要があります。リージョン 1 と 2 は、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。

Unified CM サーバに設定されているコーリング サーチ スペースとデバイス プールによって、両方の Cisco Unity Connection サーバのボイス メッセージング ポートに、適切なリージョンとロケーションが割り当てられる必要があります。さらに、テレフォニー ユーザをボイスメール ポートの特定のグループに関連付けるために、Unified CM ボイスメール プロファイルを設定する必要があります。コーリング サーチ スペース、デバイス プール、およびボイスメール プロファイルの設定方法の詳細については、次の場所にある『*Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*』の該当する版を参照してください。

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

Cisco Unity Connection は、相互に通信するために WAN にある複数の Unity Connection クラスタをイネーブルにするデジタルおよび HTTPS ネットワーキングをサポートしています。デジタルまたは HTTPS ネットワーキングを使用して、複数の Unity Connection クラスタでは、共通のディレクトリ情報を共有できます。これにより、複数のクラスタ上のユーザはボイスメールを相互に残しておくことができます。Cisco Unity Connection クラスタは、Microsoft Active Directory などの企業ディレクトリと統合してユーザ情報を同期し、デジタルまたは HTTPS ネットワーキングを使用してディレクトリ情報を同時に共有できます。

E-SRST による Cisco Unity Connection

E-SRST を使用すると、Cisco Unity Connection サーバをリモート サイトに置き、中央サイトの Unified CM に登録して、リモート ロケーションにある E-SRST にフォールバックできます。WAN リンクがダウンし、電話機が E-SRST ルータにフェールオーバーすると、Cisco Unity Connection のボイスメール ポートも E-SRST モードにフェールオーバーします。これにより、リモート サイトのユーザが、WAN の障害時に、MWI 機能も含めてボイスメールにアクセスできるようになります。

（注）　Unified CM から E-SRST モード、またはその逆方向にフェールオーバーが発生した場合、Cisco Unity Connection サーバから MWI を再同期する必要があります。

メッセージング配置モデルの組み合わせ

複数のメッセージング モデルを同じ配置で組み合わせることができます。ただし、その配置は、上記の項で示したすべてのガイドラインに従う必要があります。図 19-5 では、集中型メッセージングと分散型メッセージングの両方が同時に採用されるユーザ環境を示しています。

図 19-5　結合された配置モデル

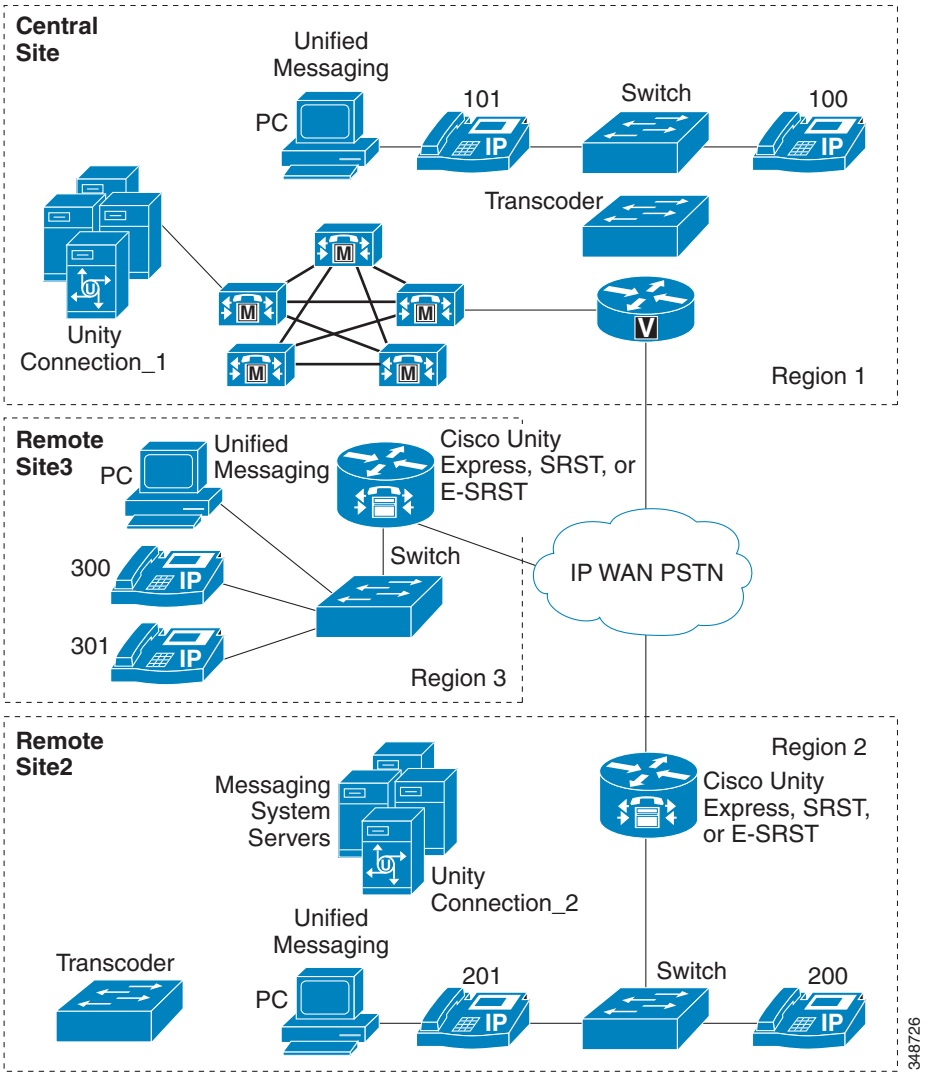


図 19-5 では、2 つのメッセージング モデルの組み合わせを示しています。リージョン 1 と 3 は集中型メッセージングと集中型呼処理を使用し、リージョン 2 は分散型メッセージングと集中型呼処理を使用しています。すべてのリージョンが、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。

図 19-5 では、中央サイトとサイト 3 の間で、集中型メッセージングと集中型コール シグナリングが使用されています。中央サイトのメッセージング システムは、中央サイトとサイト 3 の両方のクライアントにメッセージング サービスを提供します。サイト 2 は、集中型呼処理を使用する分散型メッセージング モデルを使用しています。サイト 2 に置かれているメッセージング システム（Unity Connection 2）は、サイト 2 の中にいるユーザだけにメッセージング サービスを提供します。この配置では、両方のモデルが、この章に記載されているそれぞれの設計上のガイドラインに従っています。トランスコーディング リソースは各メッセージング システム サイトに対してローカルに置かれ、サイト 2 のユーザが中央サイトのユーザにメッセージを残す場合のように、（メッセージング システムに対して）リモートのサイトからメッセージング サービスにアクセスするクライアントをサポートします。

さらに、E-SRST モードは、IP フォンおよび Cisco Unity Connection ボイスメール ポートの両方のコール処理バックアップに使用されます。このフォールバック サポートは、リモート サイト（たとえば、図 19-5 のリージョン 2）に配置され、WAN 障害などのために電話機と Unified CM との接続が失われた場合に、バックアップの呼処理を提供します。またリモート サイトのユーザに対し、WAN 障害時に、ローカルの Cisco Unity Connection サーバへのアクセスと MWI のサポートを提供します。E-SRST の詳細については、次の Web サイトで入手可能な製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/unified-survivable-remote-site-telephony/index.html

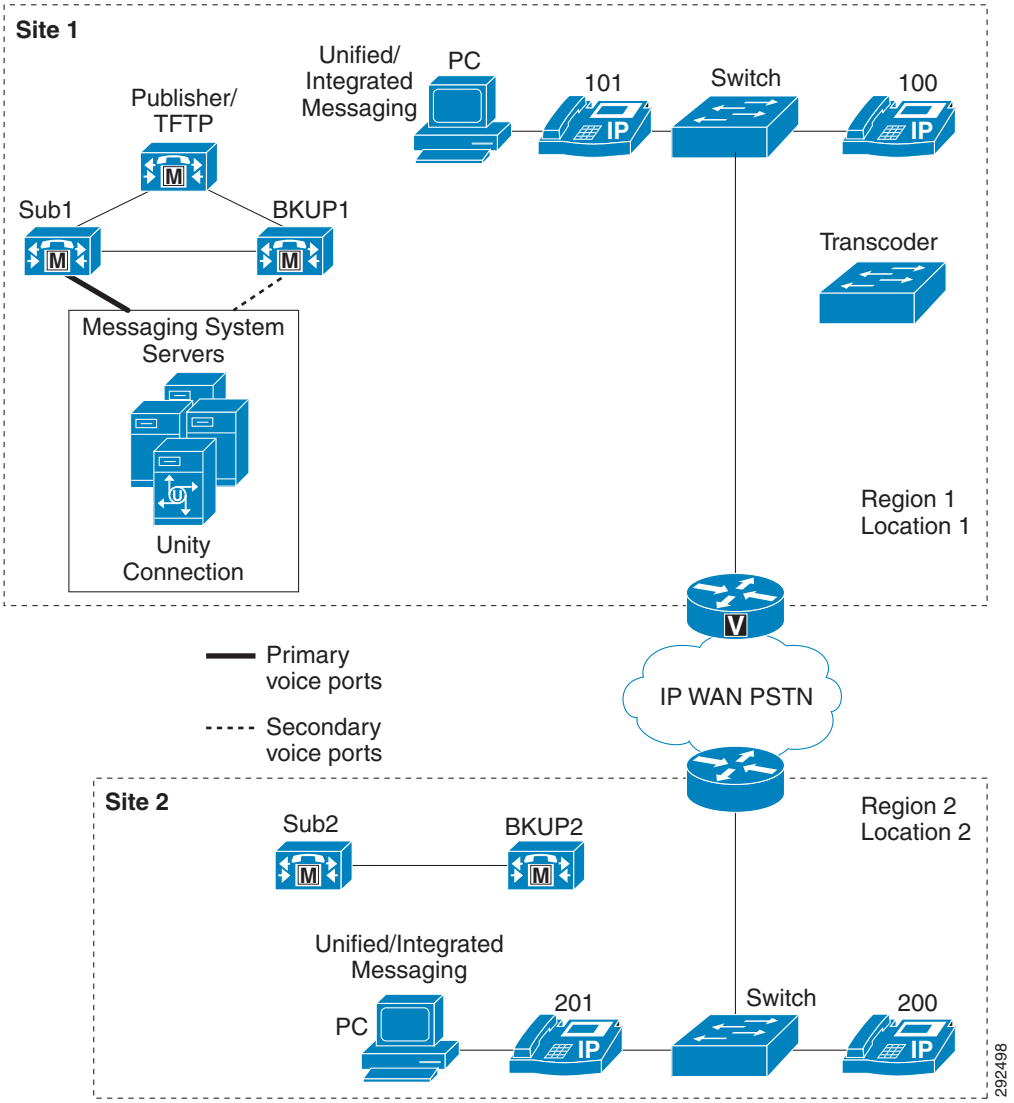
集中型メッセージングと WAN を介したクラスタリング

ここでは、集中型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介した Unified CM クラスタリングを一緒に配置する場合の Cisco Unity Connection の設計上の問題について説明します。このモデルで WAN に障害が発生した場合は、WAN が復元されるまで、すべてのリモート メッセージング サイトがボイスメール機能を失います（図 19-6 を参照）。

WAN を介したクラスタリングは、ローカル フェールオーバーをサポートしています。ローカル フェールオーバーでは、各サイトが、物理的にそのサイトに置かれているバックアップ サブスクライバ サーバを持ちます。ここでは、Cisco Unity Connection 集中型メッセージングと、WAN を介したクラスタリングのローカル フェールオーバーを一緒に配置する方法を中心に説明します。

詳細については、IP WAN を介したクラスタリング（10-46 ページ）の項を参照してください。

図 19-6　Cisco Unity Connection 集中型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介したクラスタリング



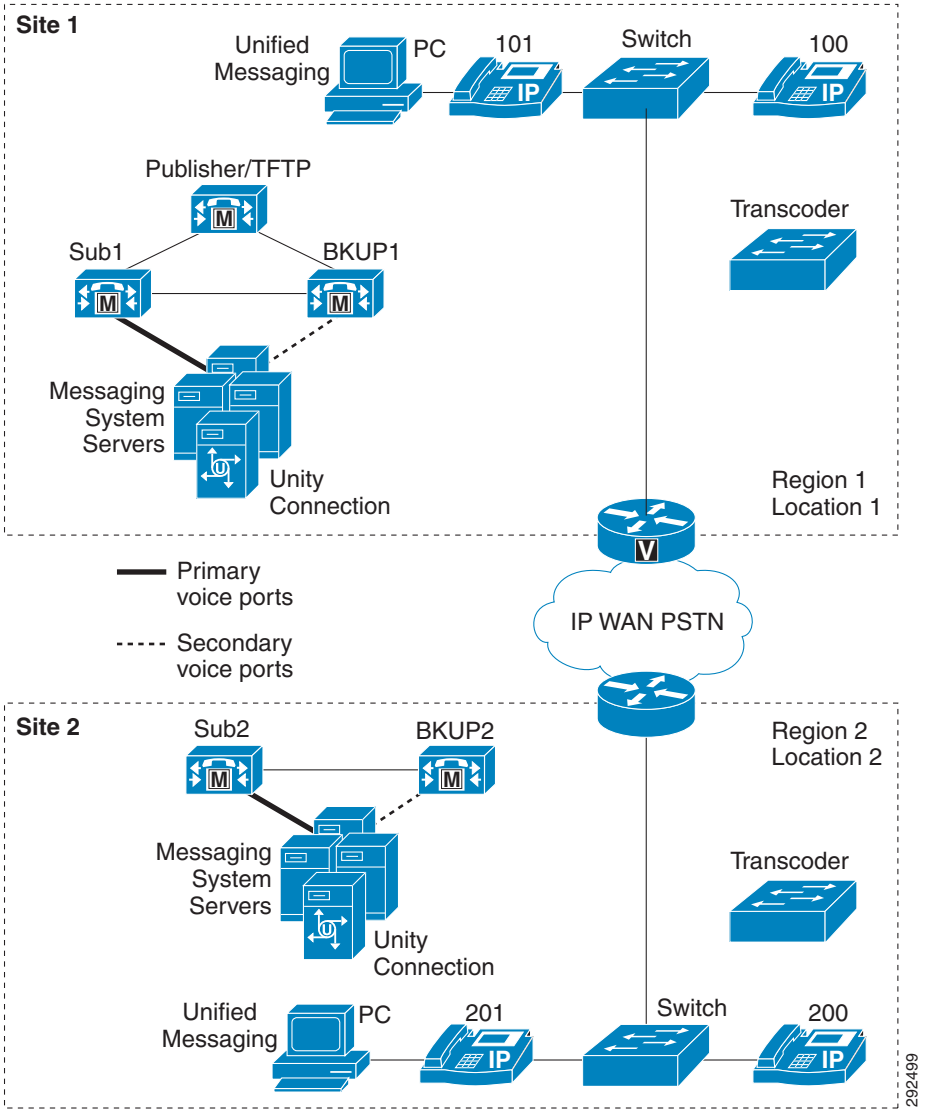
クラスタリングされたサーバ間の最小帯域幅の要求については、ローカル フェールオーバー配置モデル（10-50 ページ）の項を参照してください。

Unified CM による WAN を介したクラスタリングでは、Cisco Unity Connection と同様、最大 8 サイトがサポートされます。ボイスメール ポートは、Cisco Unity Connection メッセージング システムが置かれているサイトだけに設定されます（図 19-6 を参照）。ボイスメール ポートは、WAN を介してリモート サイトに登録されません。他のサイトのメッセージング クライアントは、プライマリ サイトのすべてのボイスメール リソースにアクセスします。WAN に障害が発生すると、リモート サイトは集中型メッセージング システムにアクセスできなくなるため、WAN を介してリモート サイトに音声ポートを設定してもメリットがありません。ユニファイド メッセージングの場合、帯域幅を考慮して、ボイスメール ポートで TRaP を無効にし、すべてのメッセージング クライアントがそのローカル PC にボイスメール メッセージをダウンロードするようにする必要があります。

分散型メッセージングと WAN を介したクラスタリング

Cisco Unity Connection メッセージング サーバも配置されたローカル フェールオーバー サイトでは、集中型メッセージング モデルと同様に、音声ポートがローカル Unified CM サブスクライバ サーバに登録されます。音声ポートの設定については、Unified CM クラスタとの音声ポート統合（19-41 ページ）および専用 Unified CM バックアップ サーバを使用する音声ポート統合（19-43 ページ）を参照してください。

図 19-7　WAN を介した Cisco Unity Connection 分散型メッセージングおよびクラスタリング



WAN を介したクラスタリングを含む単純分散型メッセージング実装では、クラスタ内の各サイトに、独自の Cisco Unity Connection メッセージング サーバとメッセージング インフラストラクチャ コンポーネントが置かれます。すべてのサイトにローカル Cisco Unity Connection メッセージング システムが置かれるわけではなく、一部のサイトで、ローカル メッセージング クライアントがリモート メッセージング サーバを使用する場合、その配置は分散型メッセージングと集中型メッセージングの組み合わせモデルとなります。(メッセージング配置モデルの組み合わせ (19-13 ページ)を参照)。このモデルで WAN に障害が発生した場合は、WAN が復元されるまで、集中型メッセージングを使用するすべてのリモート サイトがボイスメール機能を失います。

ローカル メッセージング サーバを持たない各サイトは、そのすべてのメッセージング クライアントに対して単一のメッセージング サーバを使用する必要がありますが、そのようなサイトのすべてが同じメッセージング サーバを使用する必要はありません。たとえば、サイト 1 とサイト 2 のそれぞれがローカル メッセージング サーバを持っているとします。その場合、サイト 3 のすべてのクライアントがサイト 2 のメッセージング サーバを使用し(そのメッセージング サーバに登録し)、サイト 4 のすべてのクライアントがサイト 1 のメッセージング サーバを使用するようにできます。ローカル Cisco Unity Connection メッセージング サーバを持つサイトには、トランスコーダ リソースが必要です。

他の分散型呼処理配置と同様に、これらのサイト間のコールはゲートキーパー コール アドミッション制御にとって透過的です。したがって、Unified CM でリージョンとロケーションを設定してコール アドミッション制御を提供する必要があります(帯域幅の管理 (19-33 ページ)を参照)。

分散配置された Cisco Unity Connection サーバは、デジタルまたは HTTPS でネットワーク接続することもできます。

メッセージングの冗長性

ここでは、Cisco Unity Connection に関するメッセージングの冗長性について説明します。Cisco Unity Express は、メッセージングの冗長性をサポートしていません。

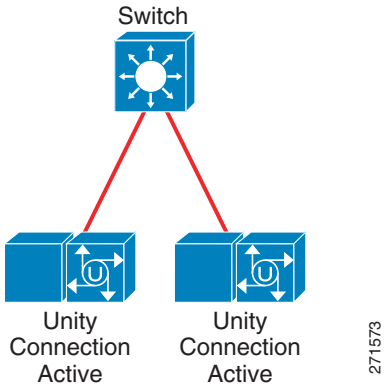
Cisco Unity Connection

Cisco Unity Connection は、プライマリとセカンダリの 2 台のサーバをアクティブ/アクティブのサーバ ペアに設定したアクティブ/アクティブ冗長モデルで、メッセージング冗長性とロードバランシングをサポートします。アクティブ/アクティブ冗長モデルでは、プライマリとセカンダリの両方のサーバが、コールおよび HTTP 要求と IMAP 要求をアクティブに受け付けます。詳細については、次の場所にある『*Design Guide for Cisco Unity Connection*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

図 19-8 は、Cisco Unity Connection のアクティブ/アクティブ メッセージング冗長性を示します。

図 19-8　Cisco Unity Connection メッセージングの冗長性



Cisco Unity Connection の SIP トランクの実装には、メッセージングの冗長性の機能にコールの分岐（転送）が必要です。Cisco Unified Communications Manager は、複数の宛先 SIP トランク機能をサポートします。この複数の宛先 SIP トランク機能により、管理者は、Cisco Unified CM と Cisco Unity Connection 間のフルメッシュ トランキングを定義し、冗長性を実現できます。また、ペアのそれぞれのサーバに対する 2 つの個別の SIP トランクを設定し、同じルート リストに関連付けられている同じルート グループに追加できます。このルート グループは、トップダウンの順で設定して、コールがプライマリ Unity Connection サーバに送信され、オーバーフロー コールがセカンダリ Unity Connection サーバに送信されるようにする必要があります。

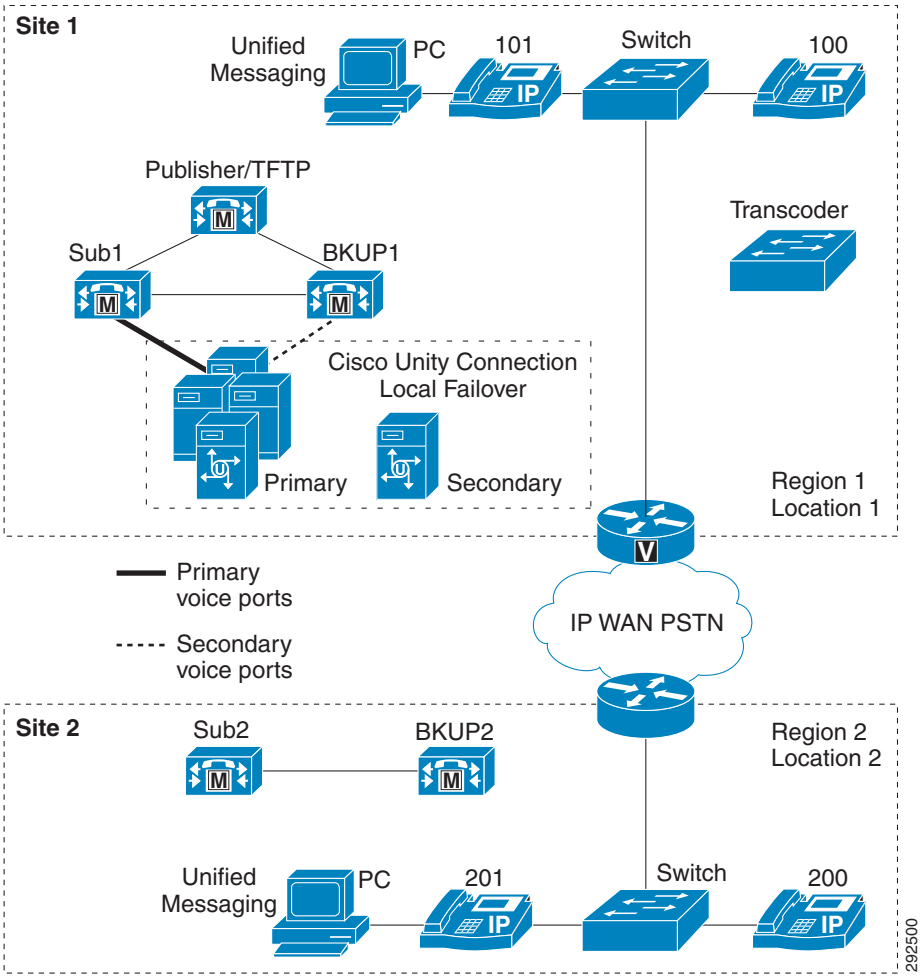
（注）　正しく機能するには、SIP OPTIONS ping を Cisco Unity Connection フェールオーバーの Cisco Unified CM SIP トランクで有効にする必要があります。

Cisco Unity Connection のフェールオーバーと WAN を介したクラスタリング

Cisco Unity Connection のローカル フェールオーバーと WAN を介したクラスタリングを配置する場合は、集中型メッセージングと WAN を介したクラスタリング（19-15 ページ）および分散型メッセージングと WAN を介したクラスタリング（19-17 ページ）で説明している設計プラクティスを適用します。正常な動作時、プライマリ Cisco Unity Connection サーバからの音声ポートは WAN を通過しません。

図 19-9 は、Cisco Unity Connection ローカル フェールオーバーを示しています。プライマリとセカンダリ両方の Cisco Unity Connection サーバが物理的に同じサイトに置かれていることに注意してください。Cisco Unity Connection フェールオーバーは、Unified CM の WAN を介したクラスタリングで使用可能な最大数までリモート サイトをサポートします。

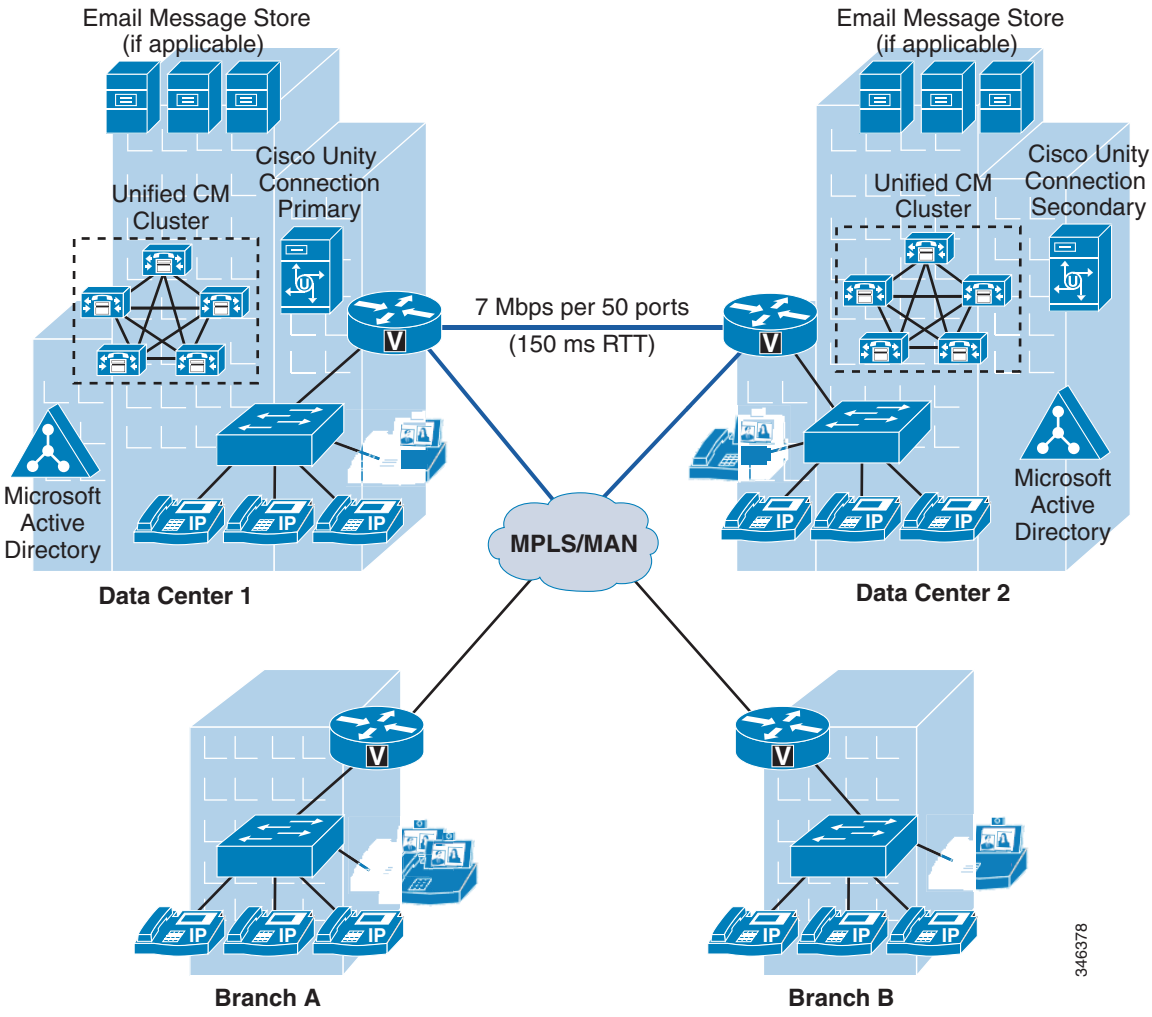
図 19-9　Cisco Unity Connection のローカル フェールオーバーと WAN を介したクラスタリング



Cisco Unity Connection の冗長性と WAN を介したクラスタリング

Cisco Unity Connection は、冗長性のためにアクティブ/アクティブとアクティブ/スタンバイの両方のクラスタリングをサポートし、WAN に配置できます。アクティブ/アクティブ設定、つまり「ハイ アベイラビリティ」設定では、ハイ アベイラビリティと冗長性の両方が提供されます。アクティブ/アクティブ ペアの両方のサーバでは Cisco Unity Connection アプリケーションが実行され、コールおよびクライアントからの HTTP 要求や IMAP 要求を受け付けます。Cisco Unity Connection プライマリ サーバはアクティブ/スタンバイ展開のすべての着信コールや管理上の変更を処理します。セカンダリ サーバがこのシナリオのコールを処理するのは、プライマリ サーバが障害状態にあるか、または使用できない場合だけです。クラスタの各サーバは、WAN 経由で異なるサイトに配置できます。その場合、以降に示す設計上の考慮事項に従う必要があります。図 19-10 は、地理的に分離されたデータセンター向けの WAN 経由のクラスタリングの Cisco Unity Connection の配置を示します。

図 19-10　2 つのサイト間でハイ アベイラビリティが確保された Cisco Unity Connection



異なるサイトに Cisco Unity Connection サーバを配置する場合は、次の遅延および帯域幅要件を考慮してください。

- 異なるサイトにあるアクティブ/アクティブ ペア間の最大 RTT は 100 ms
- 異なるサイトにあるアクティブ/スタンドバイ ペア間の最大 RTT は 150 ms
- 50 ポートごとに最低 7 Mbps の帯域幅が必要（たとえば、250 ポートでは 35 Mbps が必要）

(注)　帯域幅および遅延の要件は、Cisco Unity Connection のバージョンによって異なることがあります。

すべての要件の詳細については、次の Web サイトで入手可能な最新バージョンの『*System Requirements for Cisco Unity Connection*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-guides-list.html

（注）　Cisco Unity Connection クラスタ機能も Cisco Business Edition 6000 でサポートされます。

集中型メッセージングと分散型 Unified CM クラスタ

Cisco Unity Connection は、複数の Unified CM クラスタによる集中型メッセージング設定に配置することもできます（図 19-11 を参照）。複数統合および複数の Unified CM クラスタに伴う MWI の考慮事項の詳細については、Cisco Unified CM との統合（19-36 ページ）の項を参照してください。

図 19-11　Cisco Unity Connection と複数の Unified CM クラスタの統合

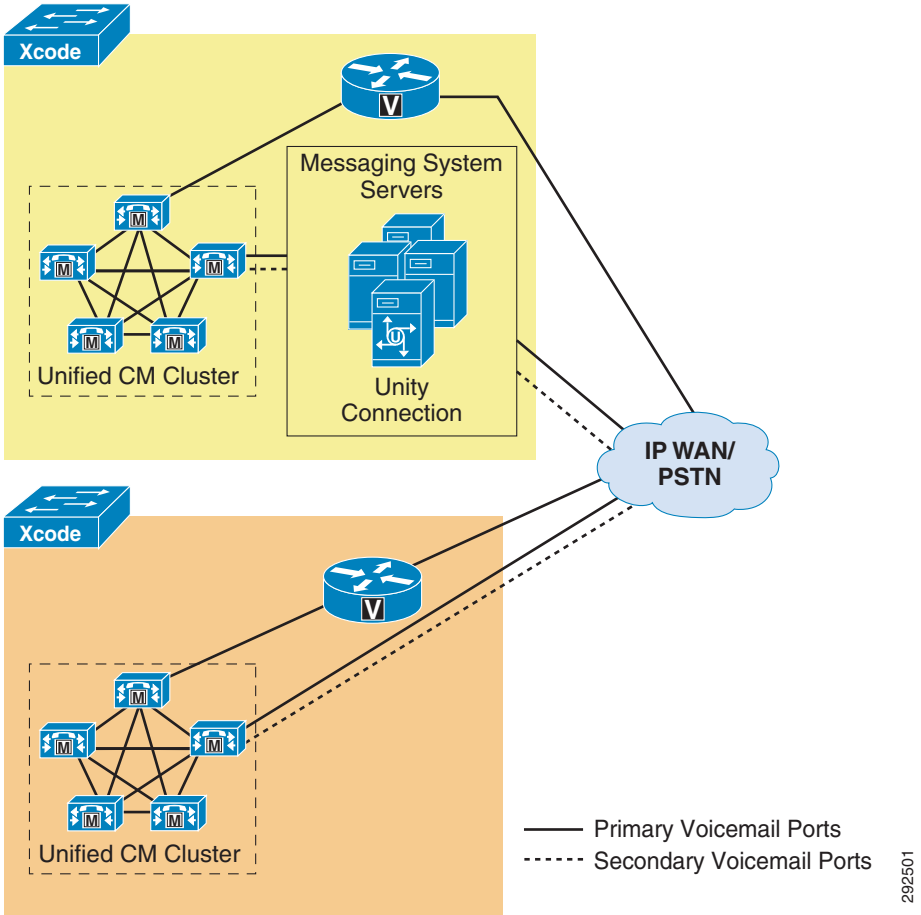


図 19-11 の設定では、クラスタ 1 とクラスタ 2 の両方のサイトのメッセージング クライアントが、物理的にクラスタ 1 に置かれている Cisco Unity Connection メッセージング インフラストラクチャを使用します。

Cisco Unity Express の配置モデル

ここではまず、Cisco Unity Express を概観し、製品に関する情報を提供します。次に、配置モデルについての項では、集中型と分散型の両方の呼処理における分散型ボイス メッセージングを中心に、Cisco Unity Express に関してサポートされている 3 つの配置モデルを紹介し、次いで配置の特徴と設計ガイドラインを示します。最後に、Cisco Unity Express と Unified CM、さらには Cisco Unity Express と Unified SRST または E-SRST モードの間で使用されるシグナリング コール フローとさまざまなプロトコルについて説明します。

Cisco Unity Express の概要

Cisco Unity Express は、Cisco Integrated Services Router（ISR）の Cisco ネットワーク モジュール上で実行される Linux ベースのソフトウェアです。Cisco Unified Communications Manager（Unified CM）、Cisco Unified SRST、または Cisco Unified Communications Manager Express（Unified CME）とともに配置できる、エントリレベルの自動応答（AA）およびボイスメール ソリューションです。以前のリリースでは、Cisco Unity Express は Unified CME または Survivable Remote Site Telephony（SRST）ルータとの共存配置に限定されていました。ただし、Cisco IOS Release 12.3(11)T で H.323-to-SIP コール ルーティング機能が導入されたため、Unified CM または Unified CME とともに配置する場合に、Cisco Unity Express と SRST または Unified CME を 2 つの異なるルータに配置できるようになりました。Cisco Unity Express は、SIP を使用して Cisco Unified Communications Manager Express（Unified CME）と通信し、JTAPI を使用して Cisco Unified Communications Manager（Unified CM）に接続します。

Cisco Unity Express のサポートされているハードウェア プラットフォームおよび容量の詳細については、次の Web サイトで入手可能な製品リリース ノートを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-express/products-release-notes-list.html

Unified CM と Unified CME の相互運用性の詳細については、複数の呼処理エージェントの統合（9-36 ページ）を参照してください。

Unified CME でサポートされている配置モデルの詳細については、次の Web サイトで入手可能な適当な Cisco Unified Communications Manager Express の設計に関する資料を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/products-implementation-design-guides-list.html

配置モデル

Cisco Unity Express は、単一のサイトとして配置することも、Cisco Unified Communications Manager（Unified CM）または Unified Communications Manager Express（Unified CME）の分散型ボイスメールおよび自動応答（AA）ソリューションとして配置することもできます。ただし、Cisco Unity Express は、次のようなすべての Cisco Unified CM 配置モデルでサポートされます。

- 単一サイト配置
- 集中型呼処理を使用するマルチサイト配置
- 分散型呼処理を使用するマルチサイト配置

図 19-12 は、Cisco Unity Express を統合した集中型呼処理配置を、図 19-13 は、分散型呼処理配置を示しています。

Unified CME によって制御される Cisco Unity Express サイト、および Unified CM によって制御されるその他のサイトは、SIP トランキング プロトコルを使用して相互接続できます。Cisco Unity Express は Unified CM または Unified CME のいずれかと統合できますが、両方と同時に統合はできません。

（注）　Cisco Unity Express は、最大 10 の Unified CME を持つ集中型配置モデルをサポートします。

図 19-12　集中型呼処理配置における Cisco Unity Express

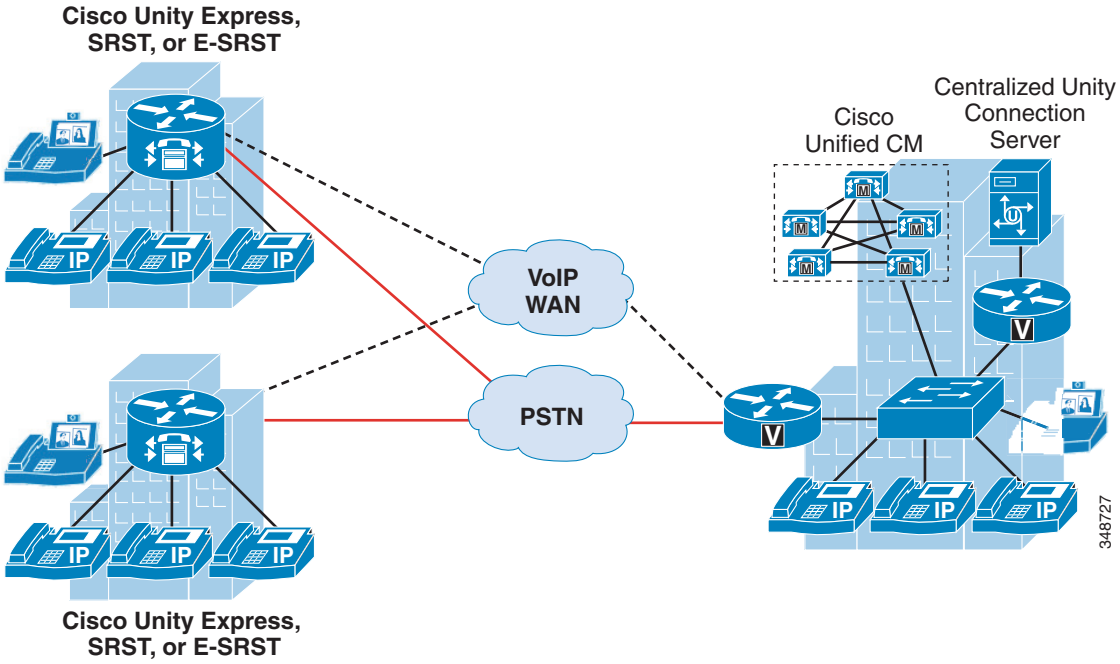
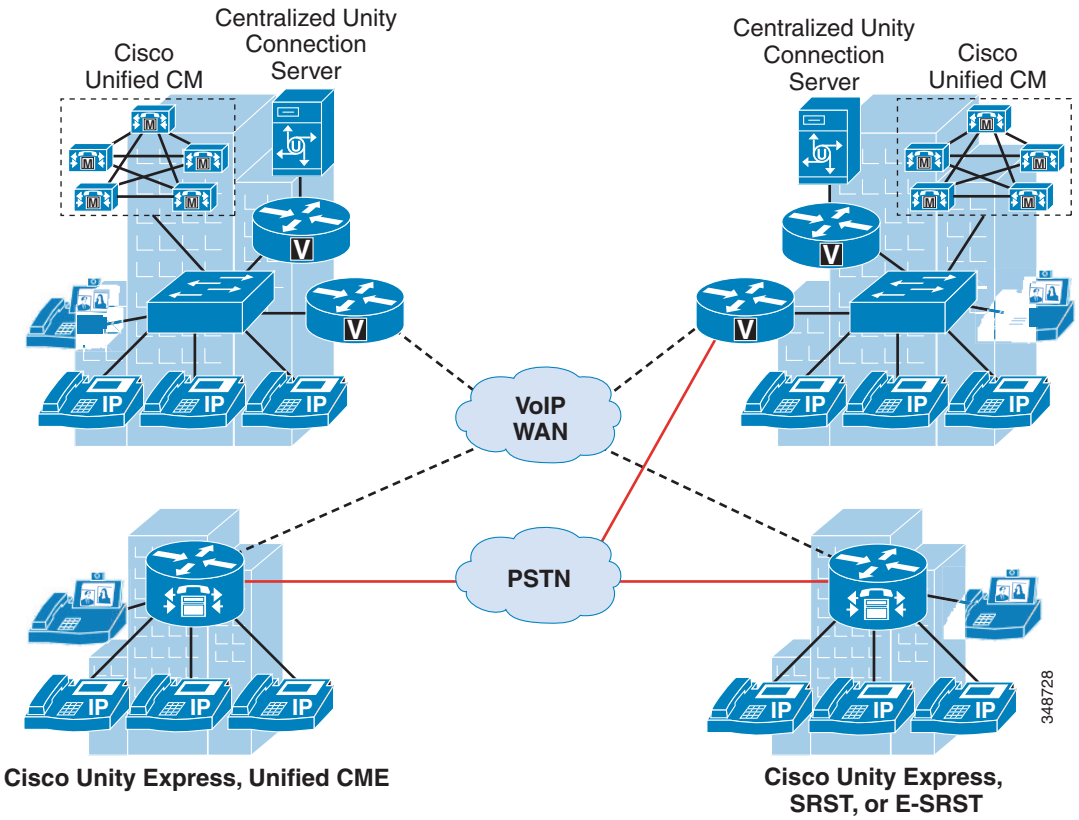


図 19-13　分散型呼処理配置における Cisco Unity Express



Cisco Unity Express を使用した最も一般的な配置モデルは、集中型呼処理を使用したマルチサイト WAN モデルです。このモデルでは、Cisco Unity Express が、小規模なリモート オフィスで分散型ボイスメール機能を提供し、中央の Cisco Unity Connection システムが本社および大規模なリモート サイトにボイスメール機能を提供します。

Unified CM ネットワーク配置に次の条件のいずれかが該当する場合は、分散型ボイスメール ソリューションとして Cisco Unity Express を使用してください。

- WAN の可用性にかかわらず、ボイスメールと AA アクセスのサバイバビリティを確保する必要がある。
- 利用可能な WAN の帯域幅が不十分なために、WAN を介して中央のボイスメール サーバにアクセスするボイスメール コールがサポートできない。
- ローカル コミュニティに対して割り当てられている AA または支店サイトの PSTN の電話番号のカバレッジが地域的に制限されているため、市外通話料金を支払わずにこれらの番号をダイヤルして中央の AA サーバに接続できない。
- PSTN を使用して支店にかけた場合、コールが支店の AA から同じ支店内の内線番号に転送される可能性が高い。
- 経営理念上、リモート オフィスが、独自のボイスメールや AA テクノロジーを選択することを許可されている。

集中型または分散型の Unified CM 配置では、Cisco Unity Express に対して次の特徴とガイドラインが適用されます。

- 単一の Cisco Unity Express は、単一の Unified CM クラスタに統合できます。
- Cisco Unity Express は、JTAPI アプリケーションとコンピュータ テレフォニー インテグレーション（CTI）Quick Buffer Encoding（QBE）プロトコルを使用して、Unified CM に統合できます。CTI ポートと CTI ルート ポイントは、Cisco Unity Express ボイスメールと自動応答（AA）アプリケーションを制御します。
- Cisco Unity Express 対応の Unified CM には、次の CTI ポートが定義されています。
  - 自動応答機能エントリ ポイント（Cisco Unity Express は、最大 5 つの異なる AA を設定できるので、ルート ポイントも最大 5 つまで必要になることがあります）
  - ボイスメールのパイロット番号
  - グリーティング管理システム（GMS）パイロット番号（オプション。GMS を使用しない場合は、このルート ポイントを定義する必要はありません）
- Unified CM 上で Cisco Unity Express にサポートされる CTI ポートとメールボックスの数は、ハードウェア プラットフォームによって異なります。詳細については、次の URL から入手できる Cisco Unity Express のデータ シートを参照してください。

  https://www.cisco.com/c/en/us/products/unified-communications/unity-express/datasheet-listing.html
- サポートされている最大数より多くのメールボックスが必要な Cisco Unity Express 配置では、Cisco Unity Connection を使用することを検討してください。
- 各 Cisco Unity Express メールボックスは、必要に応じて最大 2 つの異なる内線に関連付けることができます。
- Cisco Unity Express とともに配置されたオフィスでは、自動応答機能をそのオフィスに置くことも（Cisco Unity Express の AA アプリケーションを使用）、中央サイトに置くことも（ボイスメールのみに Cisco Unity Express を使用）できます。
- Cisco Unity Express は、Voice Profile for Internet Mail (VPIM) version 2 経由で、他の Cisco Unity Express または Cisco Unity Connection とネットワーク接続できます。これにより、Cisco Unity Express サブスクライバは、別のリモート Cisco Unity Express または Cisco Unity Connection サブスクライバとの間で、メッセージの送受信や転送を行うことができます。
- Cisco Unity Express では、フェールオーバー用の Unified CM を最大 3 つまで指定できます。3 つの Unified CM のいずれにも IP 接続できなくなった場合、Cisco Unity Express は、Survivable Remote Site Telephony（SRST）コール シグナリングに切り替えて、AA 応答サービス、IP 電話へのメールボックス アクセス、および支店に着信する PSTN コールを提供します。
- Cisco Unity Express の自動応答機能は、内線によるダイヤルと名前によるダイヤルの機能をサポートしています。内線によるダイヤルの操作では、発信側が、ネットワーク内の任意のユーザ エンドポイントにコールを転送できます。名前によるダイヤル操作では、Cisco Unity Express 内部のディレクトリ データベースを使用し、外部の LDAP や Active Directory データベースとのインタラクションを行いません。
- Unified CM を使用した集中型 Cisco Unity Express はサポートされていません。
- Cisco Unity Express は、SIP 電話を制御する Cisco Unified CM や Unified CME がない純粋な SIP ネットワークではサポートされません。
- Cisco Unity Express は、Unified CME または SRST ルータ、あるいは PSTN ゲートウェイと別のルータ上に配置できます。
- Unified CME または SRST 以外のルータ上に Cisco Unity Express を配置する場合、コマンド、**allow-connections h323 to sip** を使用して H.323 から SIP へのルーティングを行います。

図 19-14 は、Unified CM と Cisco Unity Express の間のコール フローに関係するプロトコルを示します。

図 19-14　Cisco Unity Express と Unified CM の間で使用されるプロトコル

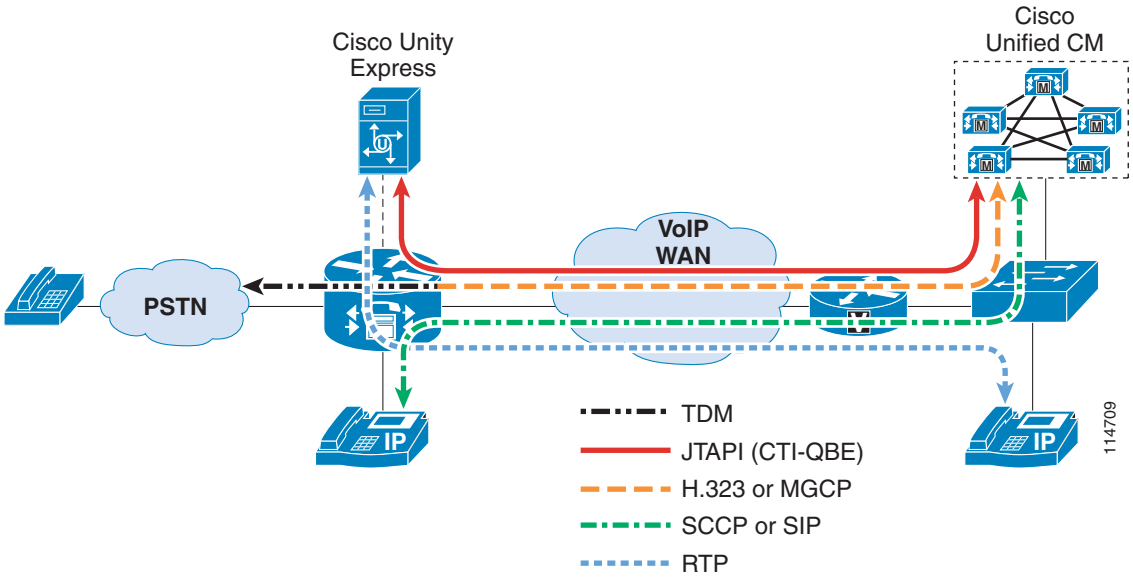


図 19-14 は、次のシグナリングとメディア フローを示しています。

- 電話機は、Unified CM から SCCP または SIP を介して制御されます。
- Cisco Unity Express は、Unified CM から JTAPI（CTI-QBE）を介して制御されます。
- 電話機のメッセージ待機インジケータ（MWI）は、メールボックスの内容の変化を CTI-QBE 経由で Unified CM に伝達する Cisco Unity Express と、それに対してランプの状態変更の MWI メッセージを電話機に送信する Unified CM によって制御されます。
- 音声ゲートウェイは、H.323、SIP、または MGCP 経由で Unified CM と通信します。
- Real-Time Transport Protocol（RTP）ストリーム フローは、エンドポイント間の音声トラフィックを搬送します。

図 19-15 は、WAN リンクがダウンした場合に、SRST または E-SRST モードのルータと Cisco Unity Express の間のコール フローに関係するプロトコルを示しています。

図 19-15　Cisco Unity Express と SRST または E-SRST のルータの間で使用されるプロトコル

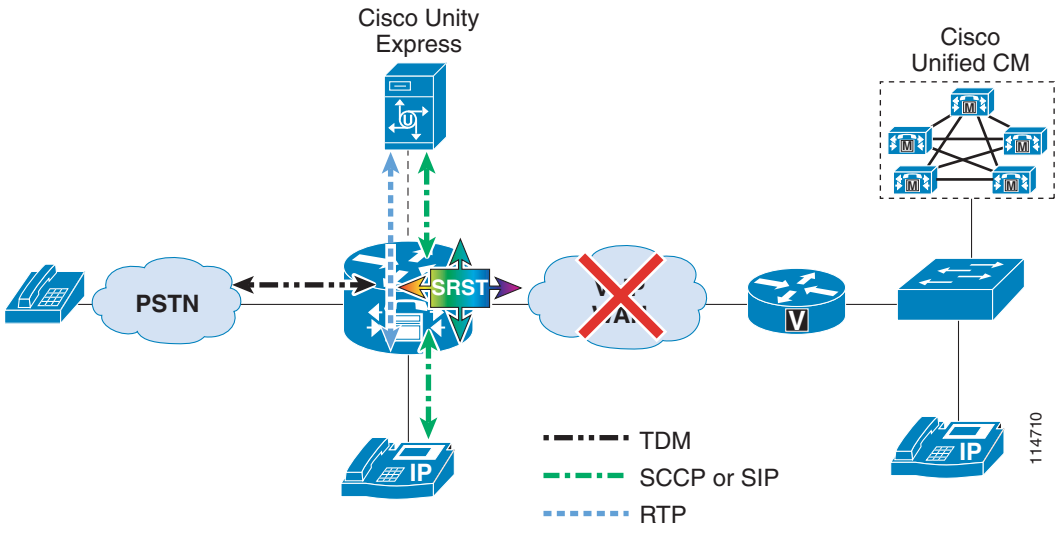


図 19-15 は、次のシグナリングとメディア フローを示しています。

- 電話機は、SRST または E-SRST モードのルータから SCCP または SIP 経由で制御されます。
- Cisco Unity Express は、内部 SIP インターフェイス経由で SRST ルータと通信します。
- 以前のリリースの Cisco Unity Express では、SRST モードでの MWI の変更はサポートされていませんが、通常動作でボイス メッセージを送信および検索できます。しかし、Unified CM に電話機を再登録するまで、電話機の MWI ランプはそのままです。その時点で、すべての MWI ランプの状態が、ユーザの Cisco Unity Express ボイスメール ボックスの現在の状態に自動的に再同期されます。Cisco Unity Express も、SRST モードで MWI をサポートします。
- Cisco Unity Express では、SIP Subscriber/Notify および Unsolicited Notify がサポートされており、MWI 通知を Unified CME モードと SRST モードの両方で生成できます。
- RTP ストリーム フローは、エンドポイント間の音声トラフィックを搬送します。
- SRST は、MWI 通知を受信するように登録された各 ephone-dns の MWI について、Cisco Unity Express にサブスクライブします。

（注） Unified CM MWI（JTAPI）は、SIP MWI 方式に依存しません。

ボイスメール ネットワーキング

この項では、Cisco Unity Connection および Cisco Unity Express を含むボイスメール ネットワーキングに関する留意点について説明します。

ボイスメール ネットワーキングでは、Cisco Unity Connection、Cisco Unity Express などのシステム間で、組み込みのシンプル メール転送プロトコル（SMTP）サーバおよび Voice Profile for Internet Mail（VPIM）バージョン 2 プロトコルのサブセットを使用して、ボイスメール メッセージの送受信、返信、転送を行えます。いずれのボイスメール メッセージング製品も、VPIM メッセージングにより、製品間の相互運用性をサポートしています。

Cisco Unity Express のボイスメール ネットワーキング

Cisco Unity Express は、メッセージのルーティングでは VPIM を、メッセージ配信では SMTP を使用して、Cisco Unity Connection と通信します。Cisco Unity Express ボイスメール ネットワーキングは、次の機能を提供します。

- サブスクライバは、発信側のシステム上でロケーション設定されたリモート Cisco Unity Express または Cisco Unity Connection との間で、メッセージの送受信や転送を行うことができます。
- サブスクライバはまた、リモート システムから受信したメッセージに対して返信できます。
- サブスクライバは、配布リストの受信者にも、Cisco Unity Connection から発信される個別のメッセージの受信者にもなることができます。

特定の製品におけるボイスメール ネットワーキングの詳細については、次の Web サイトで入手可能な該当するボイスメール製品のマニュアルを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

複数の Cisco Unity Connection クラスタ間またはネットワーク間の相互運用性

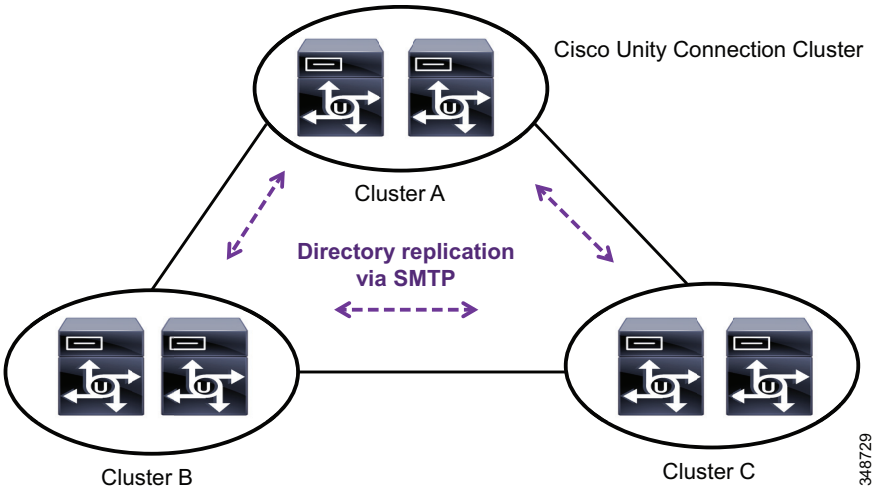
Cisco Unity Connection（デジタル ネットワーク、HTTPS ネットワーク、スタンドアロン サーバ、またはクラスタ）は、他の Cisco Unity Connection（デジタル ネットワークまたは HTTPS ネットワーク）と相互運用できます。これにより、ユーザは、ディレクトリを共有したり、簡単に管理を行ったり、その他の機能を使用したりできます。また、ノード（クラスタまたはスタンドアロン サーバ）の合計数を最大 25 まで拡張できます。

デジタル ネットワーキング

デジタル ネットワーク システムは、ディレクトリ レプリケーションおよびメッセージ転送の両方で Simple Mail Transfer Protocol（SMTP）を使用します。図 19-16 に示すように、複数の Unity Connection ノードはディレクトリ情報を共有するために完全メッシュ トポロジで結合されます。完全メッシュ トポロジだけが Cisco Unity Connection デジタル ネットワーキングでサポートされます。

ネットワーキングに完全メッシュ トポロジを使用するのに必要なのは、ノード間の情報の転送用のシングル ホップだけですが、ノード数と共にリンクの数も増えます。

図 19-16　デジタル ネットワーキング



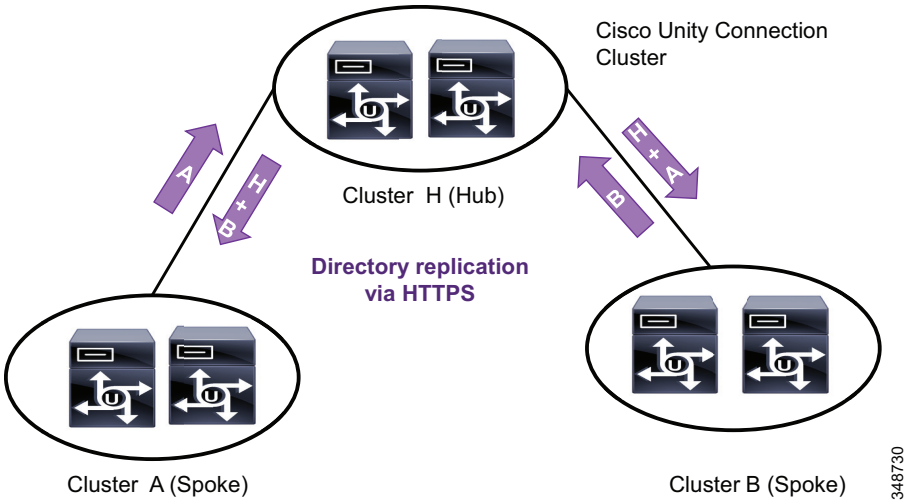
Cisco Unity Connection デジタル ネットワーキングを配置する際には、次のガイドラインを考慮してください。

- 各 Cisco Unity Connection デジタル ネットワークでは、最大で 10 のサーバをサポートできます。
- 単一の Cisco Unity Connection デジタル ネットワークは、最大 100,000 人のユーザをサポートしますが、より多くのユーザをサポートするために Voice Profile for Internet Mail（VPIM）ネットワーキングを使用して複数のデジタル ネットワークを組み合わせることができます。デジタル ネットワーク システム内のいずれかの Cisco Unity Connection ノードで Cisco Unity Connection 7.0 が実行されている場合、サポートされる最大ユーザ数は 50,000 です。
- 1 つの Cisco Unity Connection は、1 つの Cisco Unity Connection デジタル ネットワークだけに属することができます。
- 複数の Cisco Unity Connection デジタル ネットワークは VPIM を使用して組み合わせることができます。各 Cisco Unity Connection デジタル ネットワークには、ブリッジヘッドまたはサイト ゲートウェイとして定義されたサーバが 1 台必要です。ブリッジヘッドまたはサイト ゲートウェイは他のデジタル ネットワークと通信するために使用されます。

HTTPS ネットワーキング

HTTPS ネットワーキングは、ツリー構造のデータ レプリケーションをイネーブルにするハブ アンド スポーク トポロジを使用します。ハブはすべてのリーフ スポークの通信のシングル ポイントです。すべてのディレクトリ レプリケーションは HTTPS プロトコルを使用して、ハブ経由で行われます。各スポークはハブからディレクトリ情報を収集するリーフ ノードです。1 つのスポークは、1 つのハブにのみ接続できます。図 19-17 に示すように、スポーク クラスタ A および B はハブ クラスタ H に接続されます。クラスタ A はディレクトリ情報を取得する必要がある場合、ノード H にクエリを送信します。ハブ ノード H は、自身のディレクトリ情報とノード B のディレクトリ情報を ノード A に複製します。

図 19-17　HTTPS ネットワーキング



Cisco Unity Connection HTTPS ネットワーキングを配置する際には、次のガイドラインを考慮してください。

- 単一の Unity Connection ノードまたはクラスタを 1 つの HTTP ネットワークのみのメンバーにすることができます。
- 単一の HTTPS ネットワークは、最大 100,000 人のユーザと 150,000 の接続をサポートしますが、100,000 人以上のユーザや接続をサポートするために Voice Profile for Internet Mail（VPIM）ネットワーキングを使用して複数のデジタルまたは HTTPS ネットワークを組み合わせることができます。
- 単一の HTTPS ネットワーク システムは 1 つのサイトをサポートし、各サイトに最大 25 ノードを持つことができますが、VPIM を使用して複数の HTTPS ネットワーク システムを組み合わせることができます。
- すべての Cisco Unity Connection サーバは HTTPS ネットワーキングをサポートするバージョン 10.0 以上である必要があります。
- HTTPS のネットワークでは、Cisco Unity Connection ロケーションはハブ アンド スポーク トポロジを使用して結合されます。どのロケーションに対しても、HTTPS の直接リンクの数は 5 以下である必要があります。
- HTTPS ネットワーキングを同じサイトでデジタル ネットワーキングと使用することはできません。ただし、単一の HTTPS ネットワークは VPIM を使用してデジタル ネットワークと通信できます。各 Cisco Unity Connection デジタルまたは HTTPS ネットワークには、ブリッジヘッドまたはサイト ゲートウェイとして定義されたサーバが 1 台必要です。ブリッジヘッドまたはサイト ゲートウェイは他のデジタルまたは HTTP(S) ネットワークと通信するために使用されます。
- 完全同期はノードまたはクラスタが HTTPS ネットワークに追加された後に実行されます。ディレクトリ データに不一致がある場合、再同期が行われます。HTTPS ネットワーキングは、手動および自動の両方による完全同期と再同期をサポートしています。自動同期の定期的な間隔は設定可能です。
- ディレクトリ レプリケーションは Unity Connection のパブリッシャ ノードを介して行われます。パブリッシャがダウンすると、このパブリッシャ ノードを介したディレクトリ レプリケーションが停止し、サブスクライバ ノードがディレクトリ レプリケーションを提供します。

これらの相互運用性オプションの詳細については、次の Web サイトで入手可能な『*Networking Guide for Cisco Unity Connection*』の最新バージョンを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

Cisco Unity Connection の仮想化

Cisco Unified Computing System（UCS）は、総所有コスト（TCO）を削減してビジネスの機動性を向上させることを目的として設計された統合システムに、コンピューティング、ネットワーキング、ストレージ アクセス、および仮想化を一体化した、次世代のデータセンター プラットフォームです。Cisco Unity Connection は、Cisco Unified Computing System の VMware による仮想化をサポートします。

Cisco Unity Connection の仮想化には、次の主な設計上の考慮事項が適用されます。

- 最大 20,000 人のユーザがサポートされます。
- テスト済みリファレンス構成には、選択された Cisco Unified Computing System（UCS）プラットフォームが含まれます。その他のプラットフォームは、仕様ベースのハードウェアのサポート ポリシーによりサポートされる場合があります。
- 仮想化には、VMware ESXi が必要です。
- アクティブ/アクティブ クラスタのサーバは異なるブレードに配置する必要があります。可能であれば異なるシャーシに配置します。

（注）　VMware vSphere ESXi 5.1 以前の場合は、1 つ以上のプロセッサ コアを VMware ESXi ハイパーバイザ/スケジューラのために予約する必要があります。VMware vSphere ESXi 5.5 以降では、仮想マシンの遅延を軽減するために、遅延感度機能が搭載されています。遅延感度の値を高く設定した場合は、ESXi ハイパーバイザやスケジューラ用に未使用のプロセッサ コアを予約する必要はありません。

仮想システムでの Cisco Unified Communications および Cisco Unity Connection の配置の詳細については、次の Web サイトで入手可能な資料を参照してください。

http://www.cisco.com/go/virtualized-collaboration

仮想サーバ上での Unified Communications の配置の全般的な情報については、仮想サーバでの Unified Communications の配置（10-58 ページ）の項でも確認できます。

Cisco Unity Connection の仮想化については、次の Web サイトで入手可能な最新バージョンの『*Design Guide for Cisco Unity Connection*』も参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

ボイス メッセージングのベスト プラクティス

ここでは、これまでに言及されていないが、ソリューションの中で、製品の重要な側面として考慮すべき一般的なベスト プラクティスとガイドラインを説明します。Cisco Unity Connection のグループと、Cisco Unity Express の 2 つのグループにわかれています。

Unified CM を使用した Cisco Unity Connection のベストプラクティス

この項の説明は、Cisco Unity Connection に適用されます。Cisco Unity Express については、Cisco Unity Express の配置に関するベスト プラクティス（19-46 ページ）を参照してください。

帯域幅の管理

Unified CM は、帯域幅を管理するためのさまざまな機能を備えています。リージョン、ロケーション、およびゲートキーパーさえも使用して、Unified CM は、WAN リンクを介して伝送される音声コールの数によって既存の帯域幅がオーバーサブスクリプションの状態になることがなく、音声品質が低下しないことを保証できます。Cisco Unity Connection は、帯域幅の管理とコールのルーティングを Unified CM に依存しています。コールまたは音声ポートが WAN リンクを通過することのある環境に Cisco Unity Connection を配置する場合、このようなコールはゲートキーパーベースのコール アドミッション制御にとって透過的になります。このような状況は、Cisco Unity Connection サーバが分散クライアントにサービスを提供している場合（分散型メッセージングまたは分散型呼処理）、または Unified CM がリモートに置かれている場合（分散型メッセージングまたは集中型呼処理）、いつでも発生します。Unified CM は、コール アドミッション制御用のリージョンとロケーションを提供します。

図 19-18 では、集中型メッセージングと集中型呼処理を使用する小規模なサイトで、リージョンとロケーションを連携させて使用可能な帯域幅を管理する方法を示しています。リージョンとロケーションの詳細については、帯域幅管理（13-1 ページ）の章を参照してください。

図 19-18　　ロケーションとリージョン

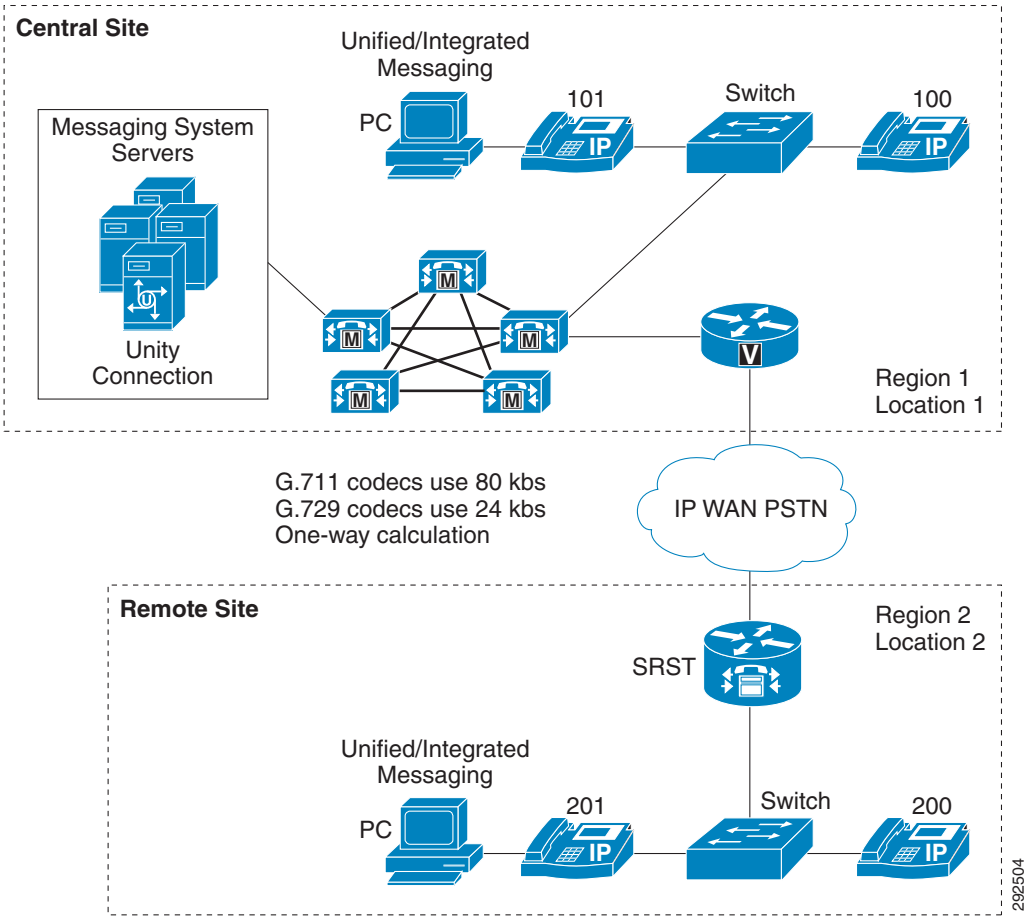


図 19-18 では、リージョン 1 と 2 が、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。ロケーション 1 と 2 は、両方 24 kbps に設定されています。ロケーションの帯域幅は、ロケーション間コールの場合にだけ配分されます。

リージョン内（G.711）コールは、ロケーションの使用可能な帯域幅に対して配分されません。たとえば、内線番号 100 が内線番号 101 をコールする場合、このコールはロケーション 1 の使用可能帯域幅 24 kbps に対して配分されません。ただし、G.729 を使用するリージョン間コールは、ロケーション 1 とロケーション 2 の両方の帯域幅割り当て 24 kbps に対して配分されます。たとえば、内線番号 100 が内線番号 200 をコールすると、このコールは接続されますが、追加の（同時）リージョン間コールでは、リオーダー（ビジー）トーンが聞こえます。

ネイティブ トランスコーディング動作

Cisco Unity Connection では、IP エンドポイントと Cisco Unity Connection サーバとの間でコールがネゴシエートされたコーデックと、録音または再生のコーデック形式が異なる場合、ネイティブ トランスコーディングが行われます。コールが G.729 でネゴシエートされ、システム全体の録音形式が G.711 で行われる場合、サーバはそのコールをネイティブにトランスコードする必要があります。Cisco Unity Connection のネイティブ トランスコーディングは、外部ハードウェア トランスコーダを使用せず、サーバのメイン CPU を使用します。ネイティブ トランスコーディングという名称はここから来ています。

Cisco Unity Connection の動作

Cisco Unity Connection では、Cisco Unity Connection SCCP または SIP シグナリングによってサポートされているすべてのコーデック形式（G.711 mu-law、G.711 a-law、G.729、iLBC、および G.722）のコールは、常にリニア PCM にトランスコードされます。リニア PCM の録音は、General Configuration の設定でシステムワイドに指定されたシステムレベルの録音形式（リニア PCM、G.711 mu-law/a-law、G.729a、または G.726）にエンコードされます（G.711 mu-law がデフォルト）。この章ではこれ以降、発信側デバイスと Unity Connection の間でネゴシエートされるコーデックを「ライン コーデック」、システムレベルの録音形式として設定されたコーデックを「録音コーデック」と呼びます。

トランスコーディングは、本来すべての接続で発生するので、ライン コーデックと録音コーデックが違っても、システムへの影響にほとんど違いはありません。ただし、iLBC または G.722 を使用する場合は例外です。G.722 と iLBC は、トランスコードに要する処理能力が大きいので、システムに対する影響も大きくなります。G.722 と iLBC は、G.711 mu-law の約 2 倍のリソースを必要とします。そのため、G.722 または iLBC 接続の場合、システムは G.711 mu-law 接続の半分しかサポートできません。

原則として、デフォルトのコーデックは G.711 のままにしておくことを推奨します。設定がディスク容量に制約される場合は、G.729a や G.726 などの低ビット レート コーデックを録音形式として設定できますが、オーディオ品質は G.711 オーディオの忠実度とは異なることに留意してください。また、G.722 がライン上のデバイスで使用されている場合は、リニア パルス符号変調（PCM）が、録音のオーディオ品質を高めるオプションです。ただし、この場合はディスク使用量が増加し、ディスク容量に影響を及ぼします。

また録音コーデックを変更したり、特定のライン コーデックのみをアドバタイズしたりする理由がいくつかあります。SCCP 統合または SIP 統合の際に、システムレベルの録音形式やアドバタイズされるコーデックについて決定する場合は、次の要因を検討してください。

- 大部分のエンドポイントと Cisco Unity Connection の間で、どのコーデックがネゴシエートされるか。これは、Cisco Unity Connection によるアドバタイズメントが必要なコーデックとそうでないコーデックの判断に役立ちます。次に、たとえば多くのクライアントを G.722 や iLBC によって Cisco Unity Connection に接続する必要がある場合など、大きな処理能力を必要とする Cisco Unity Connection のネイティブ トランスコーディングの代わりに、Unified CM が、ハードウェア トランスコーディング リソースを提供する必要がある場合を決定できます。
- どのタイプのグラフィカル ユーザ インターフェイス（GUI）クライアント（Web ブラウザ、電子メール クライアント、メディア プレーヤーなど）で録音を取得するか、またその GUI クライアントはどのコーデックをサポートするか。
- 選択したコーデックは、どの程度の品質のサウンドを生成するか。コーデックの中には、他のコーデックより高品質なものがあります。たとえば、G.711 は G.729a より品質が高く、高い音質が求められる場合に適切です。
- 1 秒間の録音にどの程度のディスク容量が必要か。

表 19-3 では、Cisco Unity Connection がサポートするコーデック形式の特徴を概観します。

表 19-3　コーデックの特徴

録音形式（コーデック）	音質	サポート状況	使用ディスク領域
リニア PCM	高品質	広範なサポート	16 KBps
G.711 mu-law および a-law	中間	広範なサポート	8 KBps
G.729a	低品質	限定的なサポート	1 KBps
G.726	中間	中程度のサポート	3 KBps
GSM 6.10	中間	中程度のサポート	1.6 KBps

Cisco Unity Connection がコーデックをアドバタイズする方法の変更の詳細については、『*System Administration Guide for Cisco Unity Connection*』を参照してください。アドバタイズするコーデックとして選択できるのは、G.711 mu-law、G.711 a-law、G.729、iLBC、および G.722 です。また優先順位の高い順にコーデックを記載したリストもあります。SCCP 統合では、コーデックがアドバタイズされ、ネゴシエートされるコールのポートとデバイスのロケーションに基づいて Unified CM がコーデックをネゴシエートするので、コーデックの順序は意味を持ちません。しかし SIP 統合では、順位のリストが意味を持ちます。コーデックに優先順位を設定すると、Cisco Unity Connection は両方のプロトコルをサポートするものの、指定された一方のみの使用が適していることをアドバタイズします。

Cisco Unity Connection Administration でシステムレベルの録音形式を変更する方法の詳細については、『*System Administration Guide for Cisco Unity Connection*』をそれぞれ参照してください。

Cisco Unified CM との統合

Cisco Unified CM は、Cisco Unity Connection と SCCP または SIP で統合できます。ここでは、電話機、SIP トランク、および音声ポートに関して、その統合の詳細を説明します。

Cisco Unity Connection では、ユーザは 1 つ以上のポート グループを含む電話機システムに関連付けられます。ポート グループは、MWI ポートに関連付けられているので、MWI 要求は、その特定のポート グループに関連付けられたポートを通じて行われます。Cisco Unity Connection の電話システムとポート グループは、System Administrator に設定されます。

Cisco Unity Connection は、同時に最大 90 個の同時電話システムおよびポート グループをサポートします。Unity Connection のタッチトーン カンバセーション（電話ユーザ インターフェイス（TUI））および音声認識（Voice User Interface（VUI））機能だけを使用している場合は、シスコは最大 90 個のポート グループを使用することを推奨しています。カレンダーや音声合成（TTS）などのその他すべての機能を使用している場合、Unity Connection は最大 60 個の同時電話システムをサポートします。この機能は、SCCP 統合と SIP 統合のいずれでも同じ方法で動作します。詳細については、次の Web サイトで入手可能な該当する Cisco Unity Connection のアドミニストレーション ガイドを参照してください。

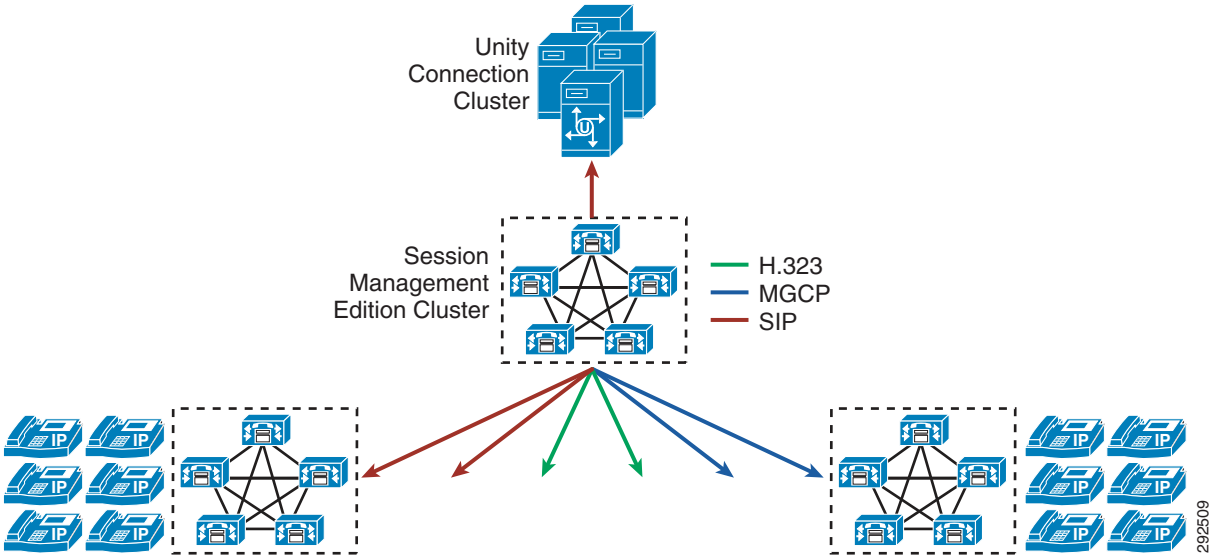
https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

複数クラスタを接続するオプションとして、Cisco Unity Connection で新しい Unified CM クラスタごとに統合を追加するという方法と別に、Unified CM は Annex M.1（QSIG のメッセージ トンネリング）をサポートしています。これにより、管理者は、Unified CM クラスタの間にあるクラスタ間トランク（ICT）で QSIG を有効にできます。ICT で QSIG を有効にすると、複数のクラスタがサポートされている場合でも、Cisco Unity Connection は 1 つの Unified CM クラスタのみに統合され、この 1 つのクラスタでのみ、MWI をオン/オフするポートを指定する必要があります。Unified CM の Annex M.1 機能によって、MWI 要求をそれらの ICT 経由で伝搬し、適切な Unified CM クラスタとそのクラスタ内の電話機に伝達できます。他のクラスタから発信されたすべてのコールは、その 1 つのクラスタに統合された Cisco Unity Connection サーバに転送できます。ICT で Annex M.1 が有効になっていれば、他のクラスタで MWI ポートを指定する必要はありません。

Cisco Unified CM Session Management Edition との統合

Cisco Unity Connection は、Cisco Unified CM Session Management Edition と統合して、すべてのリーフ Unified Communications クラスタに関連付けられたユーザにボイス メッセージング サービスを提供できます。（図 19-19 を参照）。

図 19-19　Unified CM Session Management Edition を使用した Cisco Unity Connection 配置



次の情報が、Unified Communications リーフ クラスタと Unified CM Session Management Edition との間のクラスタ間トランク、および Cisco Unity Connection への SIP トランクで送信される必要があります。

- 元の着信側番号またはリダイレクト番号
- Calling Party Number; 発番号
- コール転送の理由

非 Q.SIG トランク

非 Q.SIG トランクの場合、元の着信側番号またはリダイレクト番号を提供するため、次の設定をイネーブルにする必要があります。

- MGCP と H.323 ゲートウェイおよび H.323 トランクの着発信番号情報要素（IE）配信リダイレクト
- SIP トランク上の着発信の Diversion ヘッダー配信のリダイレクト

非 Q.SIG MGCP、H.323 または SIP トランクで送信される転送情報は、リダイレクト DN に割り当てられたボイスメール プロファイルのボイス メールボックス マスクで定義された発信側変換だけをピックアップします。ルート パターンまたはルート リスト、または発信の発呼側変換コーリング サーチ スペース（CSS）で定義された発信側変換は、転送情報に適用されません。

Q.SIG 対応トランク

Q.SIG 対応の SIP、MGCP および H.323 トランクの場合、元の着信側番号は Q.SIG 転送レッグ情報のアプリケーション プロトコル データ ユニット（APDU）で送信されます。

Q.SIG 対応の H.323、MGCP および SIP トランクでは、発信番号、着信番号、リダイレクト番号の情報はすべてカプセル化された Q.SIG メッセージで送信され、外部 H.323 メッセージや SIP ヘッダーでは送信されません。送信される転送情報は、発信側変換を使用せず、ボイス メール マスク設定を反映しません。Q.SIG トンネリング対応トランクは、Q.SIG APDU での「+」文字の転送をサポートしません。このような制限のため、ユーザのボイス メール ボックス番号は、リーフ Unified Communications システムで使用されるディレクトリ番号と同じ形式である必要があります。次に例を示します。

- 4YYYY 形式の電話番号を持つユーザには、同じ 4YYYY 形式を使用した、対応するボイスメールボックス番号を設定する必要があります。
- E.164 +XX4YYYY 形式の電話番号を持つユーザには、同じ E.164 +XX4YYYY 形式を使用した、対応するボイス メールボックス番号を設定する必要があります。

Cisco Unity Connection では、ユーザのボイス メールボックスに代替内線番号を関連付けることができます。次に例を示します。

- プライマリ VM ボックス番号：4YYYY
- +E.164 の代替 VM ボックス番号：+XX4YYY

Redirected Dialed Number Information Service（RDNIS）は、Q.SIG 対応 H.323 または SIP トランクではサポートされません。元の着信側番号またはリダイレクト番号は、RDNIS 経由ではなく、Q.SIG DivertingLegInformation2 APDU で送信されます。

Cisco Unity Connection による E.164 番号サポート

Cisco Unity Connection は次のフィールドの E.164 番号形式をサポートします。

- エンド ユーザのプライマリ内線番号
- エンド ユーザに対する転送ルールの内線番号
- システム コール ハンドラの内線番号
- ディレクトリ ハンドラの内線番号
- インタビュー ハンドラの内線番号
- エンド ユーザに対する通知デバイスの電話番号
- エンド ユーザの個人的な連絡先電話番号
- Cisco Unity Connection System に関するシステムの連絡先電話番号

- Cisco Unity Connection System のパーソナル着信転送ルール（PCTR）電話番号
- エンドユーザの代行内線番号
- Cisco Unity Connection System の規制パターン
- Cisco Unity Connection System のメッセージ待機インジケータ（MWI）内線番号

ユーザを E.164 形式のプライマリ電話番号を持つ LDAP からインポートする場合、電話番号を内線番号に変換する正規表現と置換パターンを使用します。このタスクの詳細については、次の場所にある『*System Administration Guide for Cisco Unity Connection*』の最新版で、電話番号から内線番号への変換に関するセクションを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

Cisco Unified Communications Manager（Unified CM）から、AXL 統合を経由して、E.164 形式の内線番号とともにユーザをインポートする場合、E.164 内線番号を Unified CM から、カンマ区切り値（CSV）ファイルにエクスポートする必要があり、Bulk Administration Tool（BAT）を使用して、それらの番号を Unity Connection にインポートする前に、代行内線番号で必要な変換（たとえば、Excel 形式）を実行しなければなりません。

Cisco Unity Connection による SIP URI ダイヤルのサポート

Cisco Unity Connection は、代行内線番号への SIP URI ダイヤルをサポートしています。SIP URI ダイヤルによって、ユーザは、Unity Connection を呼び出している間に、SIP URI 電話機から自動的にボイスメールにアクセスできます。英数字のアドレスに広く使用されている方式は、*ユーザ@ホスト* という簡略化された SIP URI で、左側（LHS、ユーザ部分）は英数字、右側（RHS、ホスト部分）はドメイン名です。SIP URI は、Unity Connection でユーザの代行内線番号として設定されます。

HTTPS およびデジタル ネットワーキングでは、代行内線番号用の SIP URI は SIP URI をサポートするノードでのみ複製されます。

Cisco Unity Connection の SIP URI は次の機能をサポートしています。

- サインイン試行
- 無応答（RNA）
- ボイスメール通知デバイス（勤務先電話、携帯電話、自宅電話）

管理者は、LDAP ディレクトリまたは Cisco Unified CM との AXL 統合から URI を Unity Connection にインポートできます。

（注） 管理者は、電話タイプがディレクトリ URI の代行内線番号を削除または編集できません。この代行内線番号は、元の送信元（LDAP ディレクトリまたはユーザのインポート元の Cisco Unified Communications Manager）からのみ編集または削除できます。

拡張メッセージ待機インジケータ（eMWI）

拡張メッセージ待機インジケータ（eMWI）は、従来の MWI を拡張したものであり、ボイス メッセージの数が視覚的に表示されます。従来の MWI は、新しいボイス メッセージが到着したときに電話機のメッセージ ランプをオンにし、ユーザのボイスメール ボックスから新しいボイス メッセージが削除されたときにオフにするという 2 値形式の表示です。eMWI は、Cisco Unity Connection を使用し、Cisco Unified IP Phone 8900 および 9900 シリーズの SIP 電話機でサポートされます。

eMWI では、ユーザのボイスメール ボックス内の未再生メッセージが視覚的に表示され、メッセージのステータスが色付きで表示されます。未再生メッセージは電話機の画面に赤色で表示されます。eMWI は、SIP および SCCP の統合を通じて Cisco Unity Connection の Unified CM でサポートされます。eMWI は、システムが SRST モードで動作している場合は機能しません。Cisco Unity Connection との統合においては、Cisco Unity Connection サーバ上に保管されているメッセージだけが eMWI で通知され、外部の IMAP サーバに保管されているメッセージについては通知されません。

eMWI は、Unified CM を使用した分散型呼処理環境で動作します。1 つのクラスタがクラスタ間トランク（H.323 または SIP）経由でボイス メッセージング サーバへの接続を提供する、分散型呼処理と集中型ボイス メッセージング統合のシステムでは、クラスタ間トランク経由での eMWI 更新がサポートされており、エンド デバイスに表示されます（図 19-20 を参照）。

（注）　eMWI は、クラスタ間トランク（H.323 または SIP）経由の、集中型メッセージングと分散型呼処理の環境でも動作します。

図 19-20　拡張メッセージ待機インジケータ（eMWI）

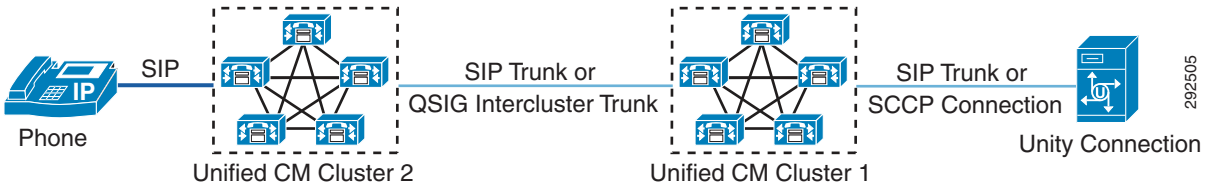


図 19-21 に、クラスタ間トランク（H.323 または SIP）経由の、分散型呼処理と集中型ボイス メッセージングの環境における eMWI を示します。

図 19-21　分散型呼処理と集中型ボイス メッセージングの eMWI

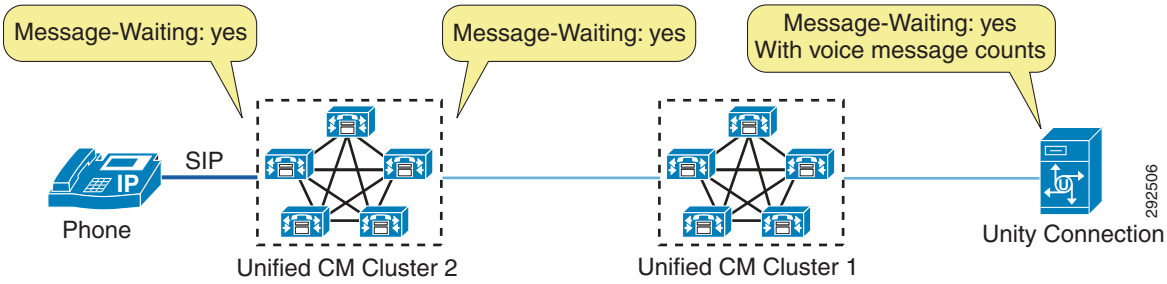


図 19-21 に示すように、クラスタ 2 およびそのボイス メッセージング ソリューションでは eMWI がサポートされますが、クラスタ 1 ではサポートされません。ボイス メッセージ数が含まれた eMWI 更新がボイス メッセージ ソリューションからクラスタ 2 の電話機に送信された場合、クラスタ 1 では、ボイス メッセージ数なしの標準 MWI だけがクラスタ 2 に転送されます。

eMWI には、次のガイドラインが適用されます。

- すべてのクラスタで eMWI がサポートされている必要があります。中間クラスタで eMWI がサポートされていない場合、終端のクラスタでは、ボイス メッセージ数なしの標準 MWI だけが受信されます。
- 標準の MWI では、ランプ状態の変更（オンまたはオフ）だけが送信されるため、多くのトラフィックは生成されません。ただし、eMWI を有効にすると、メッセージング システムからメッセージ数も送信されるため、トラフィック量が増える可能性があります。トラフィック量は、メッセージ数と変更通知数に依存します。

Unified CM クラスタとの音声ポート統合

単一サイト メッセージング環境に Cisco Unity Connection を配置する場合、Unified CM クラスタとの統合は SCCP 音声ポートまたは SIP トランクを介して行われます。Unified CM サブスクライバに障害が発生した場合でも（Unified CM フェールオーバー）、ユーザおよび外部コールが引き続きボイス メッセージングにアクセスできるように、設計上の考慮事項には、Cisco Unified CM サブスクライバ間の音声ポートの適切な配置についても考慮する必要があります（図 19-22 を参照）。

図 19-22　Unified CM クラスタと統合された Cisco Unity Connection サーバ（専用バックアップ サーバなし）

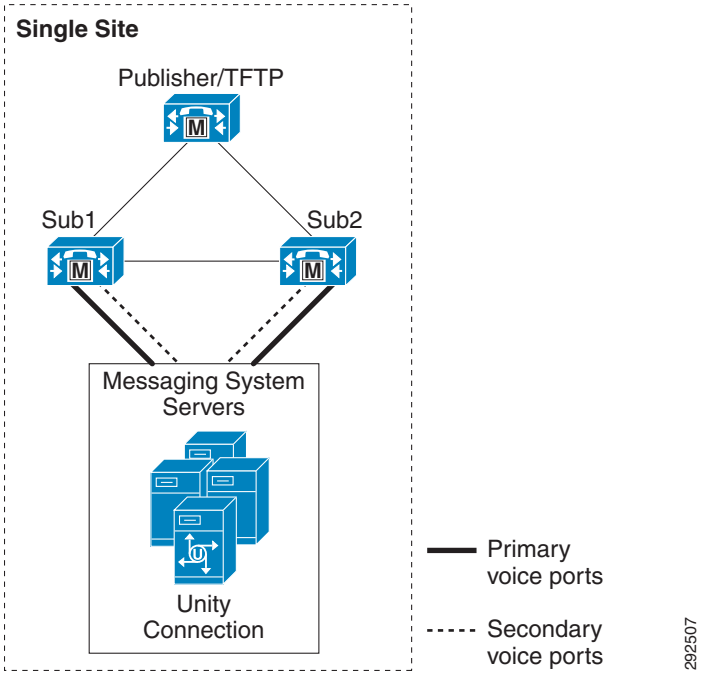


図 19-22 の Unified CM クラスタは、1 対 1 のサーバ冗長性および 50/50 のロード バランシングを採用しています。正常な動作時には、各サブスクライバ サーバがアクティブで、サーバの全呼処理負荷の最大 50 % を処理します。1 台のサブスクライバ サーバに障害が発生すると、残りのサブスクライバ サーバが、障害の発生したサーバの負荷を担います。

この設定では、ボイスメール ポートのグループが 2 つ使用され、各グループに、ライセンスのある音声ポートの合計数の半分が含まれています。1 つのグループは、プライマリ サーバがサブ 1 で、セカンダリ（バックアップ）サーバがサブ 2 になるように設定されています。もう 1 つのグループは、サブ 2 がプライマリ サーバで、サブ 1 がバックアップになるように設定されています。

MWI 専用ポートや他の特殊なポートが、2 つのグループ間で等しく分散されていることを確認してください。音声ポートの設定中は、命名規則に特に注意してください。Cisco Unity Connection でポートの 2 つのグループを設定する場合は、必ずデバイス名プレフィックスがグループごとに一意となるようにし、Unified CM Administration でボイスメール ポートを設定するときと同じデバイス名を使用します。この例では、デバイス名プレフィックスがポートのグループごとに一意になっています。グループ サブ 1 ではデバイス名プレフィックスとして CiscoUM1 が使用され、サブ 2 では CiscoUM2 が使用されています。

着信ボイスメール ポートと発信ボイスメール ポート（MWI、メッセージ通知、および TRaP 用）の比率に関する設計上の詳細情報については、次の場所にある『*Cisco Unity Connection System Administration Guide*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

（注）　デバイス名プレフィックスは、ポートのグループごとに一意で、Unified CM Administration に設定されているボイスメール ポートの命名規則と一致する必要があります。

Unified CM Administration では、この例のポートの半分が一意なデバイス名プレフィックス CiscoUM1 を使用して登録されるように設定され、残りの半分が一意のデバイス プレフィックス（CiscoUM2）を使用して登録されるように設定されています（表 19-4 を参照）。表 19-4 に示すように、ポートが Unified CM に登録される場合、半分がサブスクライバ サーバ サブ 1 に登録され、残りの半分がサブ 2 に登録されます。

表 19-4　Unified CM Administration でのボイスメール ポート設定

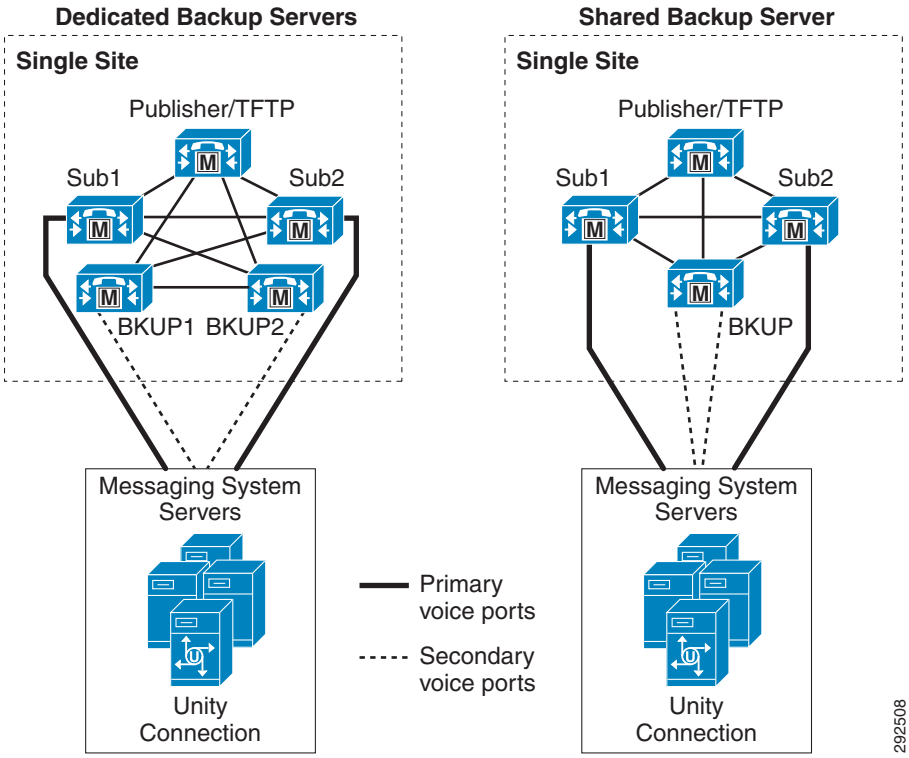
デバイス名（Device Name）	説明	[デバイス プール（Device Pool）]	SCCP セキュリティ プロファイル	ステータス	[IP アドレス（IP Address）]
CiscoUM1-VI1	Unity Connection 1	デフォルト	Standard Profile	サブ 1 に登録	1.1.2.9
CiscoUM1-VI2	Unity Connection 1	デフォルト	Standard Profile	サブ 1 に登録	1.1.2.9
CiscoUM1-VI3	Unity Connection 1	デフォルト	Standard Profile	サブ 1 に登録	1.1.2.9
CiscoUM1-VI4	Unity Connection 1	デフォルト	Standard Profile	サブ 1 に登録	1.1.2.9
CiscoUM2-VI1	Unity Connection 1	デフォルト	Standard Profile	サブ 2 に登録	1.1.2.9
CiscoUM2-VI2	Unity Connection 1	デフォルト	Standard Profile	サブ 2 に登録	1.1.2.9
CiscoUM2-VI3	Unity Connection 1	デフォルト	Standard Profile	サブ 2 に登録	1.1.2.9
CiscoUM2-VI4	Unity Connection 1	デフォルト	Standard Profile	サブ 2 に登録	1.1.2.9

（注）　Unified CM Administration でボイスメール ポートに使用される命名規則は、Cisco UTIM で使用されるデバイス名プレフィックスと一致する必要があります。一致しないと、ポートの登録に失敗します。

専用 Unified CM バックアップ サーバを使用する音声ポート統合

この Unified CM クラスタ構成では、各サブスクライバ サーバが 50 % を超える呼処理負荷で動作できます。各プライマリ サブスクライバ サーバは、専用バックアップ サーバまたは共有バックアップ サーバを持ちます（図 19-23 を参照）。正常な動作時、バックアップ サーバはコールを処理しませんが、サブスクライバ サーバの障害時またはメンテナンス時に、バックアップ サーバはそのサブスクライバ サーバのすべての負荷を担います。

図 19-23　単一の Unified CM クラスタと統合された Cisco Unity Connection サーバ（バックアップ サブスクライバ サーバを使用）



この場合のボイスメール ポートの設定は、50/50 のロード バランシング クラスタに似ています。ただし、もう 1 台のサブスクライバ サーバをセカンダリ サーバとして使用するように音声ポートを設定せず、個別の共有バックアップ サーバまたは専用バックアップ サーバを使用します。共有バックアップ サーバと共にクラスタリングされた Unified CM では、両方のサブスクライバ サーバのセカンダリ ポートが、単一のバックアップ サーバを使用するように設定されます。

音声ポート名（デバイス名プレフィックス）は、Cisco UTIM グループごとに一意で、Unified CM サーバ上で使用されるデバイス名と同じである必要があります。

Cisco Unity Connection のボイスメール ポートを設定するには、Unity Connection Administration コンソールの [テレフォニー統合（Telephony Integration）] セクションを使用します。詳細については、次の Web サイトで入手可能な Cisco Unity Connection のアドミニストレーション ガイドを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

Cisco Unity Connection による IPv6 サポート

現行の IP アドレッシングに対する要件は、現行バージョンの IP アドレッシングである IPv4 で使用可能な IP アドレスのセットを上回っています。そのため、ほとんどの IP ベースのソリューションが、IPv4 より多くの IP アドレスが使用可能な IPv6 のサポートを取り込む方向に進んでいます。Cisco Unity Connection は、SCCP または SIP 経由の Cisco Unified Communications Manager システム統合を使用して IPv6 アドレッシングをサポートします。コンポーネント レベルでは、呼制御とメディア経由でのみ、デュアル スタック アドレッシング（IPv4 と IPv6 の両方）がサポートされます。

Cisco Unity Connection は、次の IPv6 アドレス タイプをサポートします。

- 一意のローカル アドレス
- グローバル アドレス

（注）　ボイス メッセージは .wav ファイルとして保存されるため、IPv6 や IPv4 とは無関係です。

IPv6 サポートはデフォルトで無効になっていますが、システム管理者は Cisco Unified Operating System Administration とコマンドライン インターフェイス（CLI）のどちらかで IPv6 を有効にして、IPv6 アドレス設定値を構成できます。Cisco Unity Connection は、ルータ アドバタイズメントと DHCP のどちらかを経由して、または、Cisco Unified Operating System Administration と CLI のどちらかで手動で設定されたアドレスから、IPv6 アドレスを取得できます。Cisco Unity Connection Administration、Cisco Personal Communications Assistant は IPv6 アドレスを使用してアクセスできます。

（注）　IPv6 アドレッシングは、Cisco Unity Connection のインストールまたはアップグレード時にイネーブルにできません。Cisco Unity Connection は、「IPv6 のみ」のサーバ設定をサポートしていません。また、Cisco Unity Connection は、IPv6 専用のユニキャストをサポートしています。

IPv6 を介した Cisco Unity Connection は、次の機能をサポートします。

- Cisco Unity Connection は、IPv6 を介した自動検出機能を備え、Unity Connection が通信相手の Microsoft Exchange Server を検索できるようにします。
- Cisco Unity Connection は、IPv6 Microsoft Exchange 2007 または 2010 サーバと統合してシングル インボックス機能をイネーブルにできます。
- Cisco ViewMail for Outlook（VMO）は、IPv6 を介した Outlook と Cisco Unity Connection との通信をサポートします。
- Cisco Unity Connection で受信されたボイス メッセージは、IPv6 上の Outlook などの IMAP クライアントを使用してアクセスできます。
- Cisco Unity Connection は、IPv6 を介して LDAP と統合し、ユーザ情報をインポートできます。
- Cisco Unity Connection はまた、IPv6 を介した Telephone Record and Playback（TRaP）機能を提供し、これによりユーザは IPv6 対応電話機を介してメッセージの録音や再生が実行でき、IPv6 を介したシグナリングが発生します。

Cisco Unity Connection による単一受信トレイ

Cisco Unity Connection は、Microsoft Exchange 2003、2007、2010（クラスタ版または非クラスタ版）とのシングル インボックス機能をサポートし、ボイスメールに Unified Messaging を提供します。Cisco Unity Connection は、この 3 つすべての Microsoft Exchange バージョンを同時にサポートすることも、いずれかを個別にサポートすることもできます。Unity Connection では、Microsoft Business Productivity Online Suite（BPOS）専用サービスおよび Microsoft Office 365 クラウドベース Exchange サーバとの相互運用性もサポートされています。Unity Connection は、Microsoft Exchange Online を使用してシングル インボックス機能をイネーブルにします。詳細については、次の Web サイトで入手可能な最新バージョンの『*Unified Messaging Guide for Cisco Unity Connection*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

Cisco Unity Connection ViewMail for Microsoft Outlook から送られてくるものも含め、すべてのボイス メッセージが Cisco Unity Connection に保存されてから、すぐに受信者の Microsoft Exchange メールボックスに複製されますが、複製はオプションです。また、この機能はユーザ単位で設定可能です。

Cisco Unity Connection でボイスメール用のユニファイド メッセージングをサポートするには、いくつかの設計上の留意点があります。ユーザの電子メールは、電子メールとボイスメールを含むすべてのメッセージに対する単一のコンテナになります。メッセージが受信トレイ下の別のフォルダに移動されても、Cisco Unity Connection から削除されることはありません。ただし、ユーザがボイス メッセージを受信トレイ フォルダ下ではない Outlook フォルダに移動した場合は、Cisco Unity Connection からそのメッセージが削除されますが、コピーが Outlook 内に残っているため、ViewMail for Outlook で再生できます。ユーザがメッセージを受信トレイ フォルダまたは受信トレイ フォルダ下のフォルダに移動すると、そのメッセージがユーザの Cisco Unity Connection メールボックスに表示されます。また、ユーザが Cisco Unity Connection からボイス メッセージを削除した場合、または、メッセージの有効期限が切れたために Cisco Unity Connection から自動的に削除された場合は、そのメッセージが Microsoft Exchange からも削除されます。同様に、Microsoft Exchange からボイス メッセージが削除された場合は、Cisco Unity Connection からも削除されます。

メッセージが保護対象かつプライベートとしてマークされている場合は、実メッセージが Microsoft Exchange に複製されません。代わりに、そのメッセージに関する簡単な説明付きのプレースホルダーが作成されます。実メッセージの唯一のコピーが Cisco Unity Connection 上に保存され、ユーザがそのメッセージを取り出すと、通常のメッセージの場合と違って、ローカル ソースではなく、Cisco Unity Connection から直接再生されます。これは、オーディオ ファイルが Outlook からボイスメール経由でアクセスされた場合は、ローカル アクセスできないことも意味します。保護対象でプライベートのメッセージを受信トレイおよび受信トレイ下のフォルダ以外のフォルダに移動した場合は、そのメッセージが完全に削除されるため、取り出せなくなります。

（注） メッセージング展開の種類に関係なく、すべての音声メッセージが Cisco Unity Connection サーバ上に保存されます。Cisco Unity Connection は、ボイス メッセージング トラフィック、通知、および同期化の信頼できるソースです。

1 つのボイスメール メッセージに割り当て可能なスペース容量は、メッセージの有効期限と同様に、Cisco Unity Connection サーバ上で設定されます。ボイスメール メッセージの最大サイズは Microsoft Exchange サーバ上で設定されます。一般的に、Microsoft Exchange サーバには、メールボックスに同期される Cisco Unity Connection よりも大きなサイズが保存されます。そのため、Microsoft Exchange 上のメッセージの最大サイズは、Cisco Unity Connection 上の最大サイズよりも大きくする必要があります。

Cisco Unity Connection と Microsoft Exchange 間の通信のセキュリティ面から、デフォルト オプションとして HTTPS が選択されます。HTTP もサポートされていますが、セキュリティが低下するうえ、Microsoft Exchange 上で余分な設定が必要になる場合があるため、推奨できません。その一方で、証明書サーバへのアクセスが可能な場合に、Microsoft Exchange 証明書を確認するためのオプションが用意されています。

Cisco Unity Express の配置に関するベスト プラクティス

Cisco Unity Express を配置する場合は、次のガイドラインとベスト プラクティスを使用してください。

- ボイスメールの宛先として Cisco Unity Express を持つ IP 電話が、Cisco Unity Express をホストするルータと同じ LAN セグメントに置かれていることを確認します。
- Cisco Unity Express を使用して配置するサイトで無中断の自動応答機能（AA）と電子メール アクセスが必要な場合は、Cisco Unity Express、SRST、および PSTN の音声ゲートウェイがすべて同じ物理サイトに置かれていることを確認します。ホットスタンバイ ルータ プロトコル（HSRP）やその他の冗長性ルータ設定は、現在、Cisco Unity Express ではサポートされていません。
- 各メールボックスは、プライマリ内線番号とプライマリ E.164 番号に関連付けることができます。通常、この番号は、PSTN の発信者が使用する Direct-Inward-Dial（DID）番号です。プライマリ E.164 番号が他の番号に設定されている場合、SRST モード時に正しいメールボックスに到達するように、Cisco IOS トランスレーション パターンを使用して、プライマリ内線番号かプライマリ E.164 番号に一致させます。

Unified CM とのボイスメール統合

- 各 Cisco Unity Express サイトは、ボイスメール用と AA 用（ライセンスされ、購入している場合）に CTI ルート ポイントを 1 つずつ関連付ける必要があります。またライセンスされた Cisco Unity Express ポートと同じ数の CTI ポートを設定する必要があります。Cisco Unity Express の数が、呼処理（9-1 ページ）の章に示すスケーラビリティ ガイドラインを超えないことを確認します。
- Cisco Unity Express は、Unified CM 上の JTAPI ユーザに関連付けられます。単一の JTAPI ユーザをシステム内の Cisco Unity Express の複数のインスタンスに関連付けることは可能ですが、Unified CM 内の専用の JTAPI ユーザをそれぞれ単一の Cisco Unity Express に関連付けることを推奨します。
- Unified CM を以前のバージョンからアップグレードした場合、JTAPI ユーザのパスワードは、Unified CM で自動的にリセットされます。したがって、管理者は、アップグレードの後、JTAPI パスワードが Cisco Unity Express と Unified CM の間で同期化され、Cisco Unity Express を Unified CM に登録できることを確認する必要があります。
- CTI ポートと CTI ルート ポイントは、特定の場所で定義できます。Unified CM と Cisco Unity Express の間で、ロケーションベースのコール アドミッション制御を使用することを推奨します。RSVP を使用することもできます。
- Cisco Unity Express と Unified CM の間を通過する WAN のシグナリング トラフィックのための、適切な Quality of Service（QoS）と帯域幅を確保します。各 Cisco Unity Express サイトの CTI-QBE シグナリングのために、20kbps の帯域幅をプロビジョニングします。詳細については、ネットワーク インフラストラクチャ（3-1 ページ）の章を参照してください。

- Unified CM から Cisco Unity Express への CTI-QBE シグナリング パケットは、AF31（0x68）という DSCP 値でマーキングされています。Unified CM は、CTI-QBE シグナリングに TCP ポート 2748 を使用します。
- Unified CM JTAPI ライブラリは、すべての発信 QBE シグナリング パケットに、適正な IP Precedence ビットを設定します。その結果、Cisco Unity Express と Unified CM の間のすべてのシグナリングに、適正な QoS ビットが設定されます。

Cisco Unity Express コーデックと DTMF のサポート

Cisco Unity Express へのコールは、G.711 のみを使用します。ローカルのトランスコーダを使用して、WAN を通過する G.729 コールを G.711 コールに変換することを推奨します。Unified CM リージョンは、リージョン内コールに G.711 音声コーデックを、リージョン間コールに G.729 音声コーデックを使用するように設定できます。

Cisco Unity Express サイトにトランスコーディング機能がない場合、必要な数の G.711 ボイス メールに対応する十分な帯域幅を WAN 上にプロビジョニングします。IP フォンと Cisco Unity Express デバイス（CTI ポートと CTI ルート ポイント）の間のコールに G.711 音声コーデックを使用するように、Unified CM リージョンを設定します。

Cisco Unity Express は、DTMF リレーのみをサポートし、インバンド DTMF トーンはサポートしていません。Cisco Unity Express では、DTMF は、SIP または JTAPI のいずれかの呼制御チャネルを介してアウトオブバンドで搬送されます。Cisco Unity Express 2.3 は、RFC 2833 を使用した、Cisco Unity Express への G.711 SIP コールをサポートします。

JTAPI、SIP トランクおよび SIP 電話機のサポート

Cisco Unified CM は SIP トランク プロトコルをサポートしますが、Cisco Unity Express は Unified CM との通信に JTAPI を使用します。Cisco Unity Express は、SCCP 電話機と SIP 電話機の両方をサポートします。

- SRST を使用できるように SIP トランクを設定し、（JTAPI によって）SIP 電話機をサポートするように Unified CM を設定します。
- Cisco Unity Express は、トランスコーダ経由で G.729 SIP コールをサポートします。また Cisco IOS Release 12.3(11)XW で RFC 2833 がトランスコーダをパススルーする能力が追加されています。
- Cisco Unity Express は、Unified CM からのスロースタート コールの場合、コール設定のためのディレイド メディア（delayed media、INVITE メッセージ内に SDP なし）をサポートします。
- Cisco Unity Express は、ブラインド転送と打診転送の両方をサポートしますが、デフォルトの転送モードは、SIP コールで REFER を使用した打診転送（半自動）です。転送モードを、REFER を使用する打診転送または BYE/ALSO を使用するブラインド転送に明示的に変更するには、Cisco Unity Express コマンドライン インターフェイスを使用します。リモート エンドで REFER がサポートされていない場合は、BYE/ALSO が使用されます。
- Cisco Unity Express は、ボイス メッセージ通知のためのアウトコールをサポートしています。また、打診転送もサポートしています。これらのいずれのコール設定時でも、Cisco Unity Express は INVITE に対する 3*xx* 応答を受信できます。Cisco Unity Express は、INVITE に対する 301（Moved Permanently）と 302（Moved Temporarily）応答のみを処理します。これには、3*xx* 応答の Contact ヘッダーに含まれ、新しい INVITE の送信に使用する URL が必要です。305（Use Proxy）応答は、サポートされていません。

(注)　Cisco Unified CM と Cisco Unity Express 間の互換性については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/unity_exp/compatibility/cuecomp.html にある『*Cisco Unity Express Compatibility Matrix*』を参照してください。

Cisco Unity Express の詳細については、次の Web サイトで入手可能な製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/unity-express/index.html

サードパーティ製ボイスメールの設計

この項では、サードパーティ製ボイスメール システムを Cisco Unified Communications とともに配置する場合のさまざまなオプションについて説明します。統合とメッセージングの両方について説明します。

(注)　この項では、ポートやストレージに関するサードパーティ製ボイスメール システムのサイジング方法については説明しません。この情報については、ボイスメール ベンダーに連絡してください。ボイスメール ベンダーは、具体的なトラフィック パターンに基づいて、各ベンダーのシステムにおける個別の要件をより適切に判断できます。

統合

*統合*は、ボイスメール システムとその関連する PBX または呼処理エージェントとの間の物理的な接続として定義されます。統合によって、これらの間にフィーチャ セットも提供されます。ボイスメール ベンダーは数多くあり、Cisco Unified CM を配置する場合に既存のボイスメール システムを引き続き使用することも一般的です。

(注)　シスコでは、サードパーティ製ボイスメール システムのテストや認証は行っていません。通常、この業界では、さまざまな PBX システムに対して自社の製品をテストまたは認証することはボイスメール ベンダーの責任であるとされています。シスコでは、そのような機器とのシスコのインターフェイスをテストし、どのようなサードパーティ製ボイスメール システムが接続されるかにかかわらずこれらのインターフェイスをサポートします。

Cisco Unified CM は QSIG を使用してサードパーティの PBX と統合でき、これにより、サードパーティの PBX を 一次群速度インターフェイス（PRI）T1/E1 トランクを介して Unified CM に接続できます。各方式にはそれぞれの利点と欠点があり、使用する方式はボイスメール システムと現在の PBX との統合方法に大きく依存します。

現在、ボイスメール統合に使用できる他の方法には、H.323 や SIP があります。ただし、ベンダーにおけるさまざまな実装方式、サポートされる機能、およびその他の要因によって、これらのサードパーティ製ボイスメール統合は、お客様が評価する必要があります。これらのオプションの詳細については、シスコのアカウント チームまたはシスコ代理店に連絡してください。

メッセージ

*メッセージング*は、ボイスメール システム間でのメッセージの交換として定義されます。メッセージングの目的で使用できるいくつかのオープンな標準があります。

異なるシステム間でのメッセージングを可能にするために配置される最も一般的なプロトコルは、Voice Profile for Internet Mail（VPIM）です。VPIM の仕様は何度か更新されており、最新ではないバージョン 2 が現在でも最も広く採用されているようです。VPIM よりも前から存在するメッセージング プロトコルに Audio Messaging Interchange Specification - Analog（AMIS-A）がありますが、ユーザ インターフェイスが使いにくく、アナログ テクノロジーが使用されており、機能も少ないことから、ほとんど使用されていません。

コラボレーションのインスタント メッセージングとプレゼンス

改訂日：2018 年 3 月 1 日

Cisco Unified Communications Manager IM and Presence サービスは、ネイティブな標準ベースのデュアルプロトコル企業インスタント メッセージング（IM）、および Cisco Unified Communications の一部としてのネットワークベースのプレゼンスを提供します。Cisco Unified Communications Manager のこのセキュアかつスケーラブルで管理の容易なサービスでは、ユーザに企業内外への機能豊富な通信機能が提供されます。

Cisco Unified Communications Manager IM and Presence サービスは IM and Presence のオプションの 1 つであり、Cisco Unified Communications および Collaboration システムの価値を高めます。このソリューションの主要なプレゼンス コンポーネントは、すべてのオンプレミス配置で必要な Cisco IM and Presence サービスです。このサービスは Extensible Communications Platform（XCP）を備え、ユーザの在籍ステータスと通信機能に関する情報を収集する SIP/SIMPLE および Extensible Messaging and Presence Protocol（XMPP）をサポートしています。ユーザの在籍ステータスは、ユーザが電話機などの通信デバイスをアクティブに使用しているかどうかを示します。ユーザの通信能力は、ビデオ会議、Web コラボレーション、インスタント メッセージング、基本オーディオなど、ユーザが使用できる通信の種類を示します。

IM and Presence サービスは、シスコやサードパーティの互換性のあるデスクトップとモバイル プレゼンス、およびインスタント メッセージング クライアントと緊密に統合されており、Cisco Jabber SDK も含まれています。これにより、クライアントはインスタント メッセージング、プレゼンス、クリックツーコール、電話制御、音声、ビデオ、ビジュアル ボイスメール、Web コラボレーションなど多数の機能を実行できます。IM and Presence サービスが提供するリッチなオープン インターフェイスによる柔軟性が、IM およびシスコのネットワークベース プレゼンスの実装に加え、さまざまなビジネス アプリケーションの IM and Presence フェデレーションを可能にします。

Cisco IM and Presence サービスによって取得された集約ユーザ情報により、Cisco Jabber、Cisco Unified Communications Manager アプリケーション、およびサードパーティ製のアプリケーションはユーザの生産性を高めることができます。これらのアプリケーションは、最も効果的な通信形態を判断することにより、ユーザ間のコミュニケーションの効率性を高めます。

（注） Cisco IM and Presence サービスは、Cisco Unified Computing System（UCS）上の仮想サーバでシスコが提供する VM 設定オプション ユーザ設定テンプレートを使用して、Cisco Unified Communications Manager（Unified CM）の同等のバージョンとともに配置する必要があります。シスコは仮想サーバ間での VM リソースのオーバーサブスクリプションをサポートしていないため、配置される仮想サーバごとに専用のシステム リソースを使用する必要があります。

この章では、オンプレミス、クラウド、およびハイブリッド オプション用の Cisco Unified Communications システムにおけるプレゼンスとインスタント メッセージングの基本概念を説明し、プレゼンスおよびインスタント メッセージング ソリューションのさまざまなコンポーネントを最適に配置するためのガイドラインを示します。

この章の変更点

表 20-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 20-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
永続的なチャット	永続的なチャットとコンプライアンス ロギングに関する考慮事項（20-34 ページ）	2018 年 3 月 1 日
集中型 IM and Presence の導入	集中型 IM and Presence の導入（20-35 ページ）	2018 年 3 月 1 日

プレゼンス

*プレゼンス*とは、ユーザが特定のデバイス セットで通信する能力とその意志を意味します。プレゼンスでは、次の段階またはアクティビティが実行されます。

- ユーザ ステータスのパブリッシュ

  ユーザ ステータスの変更は、ユーザによるキーボード操作、電話機の使用、WebEx Meeting ステータス、ネットワークへのデバイス接続、Microsoft Exchange のカレンダー ステータスを認識することにより、自動的にパブリッシュできます。

- ステータスの収集

  パブリッシュされた情報は、すべての利用可能なソースから収集され、プライバシー ポリシーが適用され、現在のステータスが集約および同期されてから、保存されたうえで消費されます。

- 情報の消費

  デスクトップ アプリケーション、カレンダー アプリケーション、およびデバイスが、ユーザ ステータス情報を使用して、エンド ユーザにリアルタイムの更新情報を提供します。これにより、エンド ユーザは、適切な通信方法を判断できるようになります。

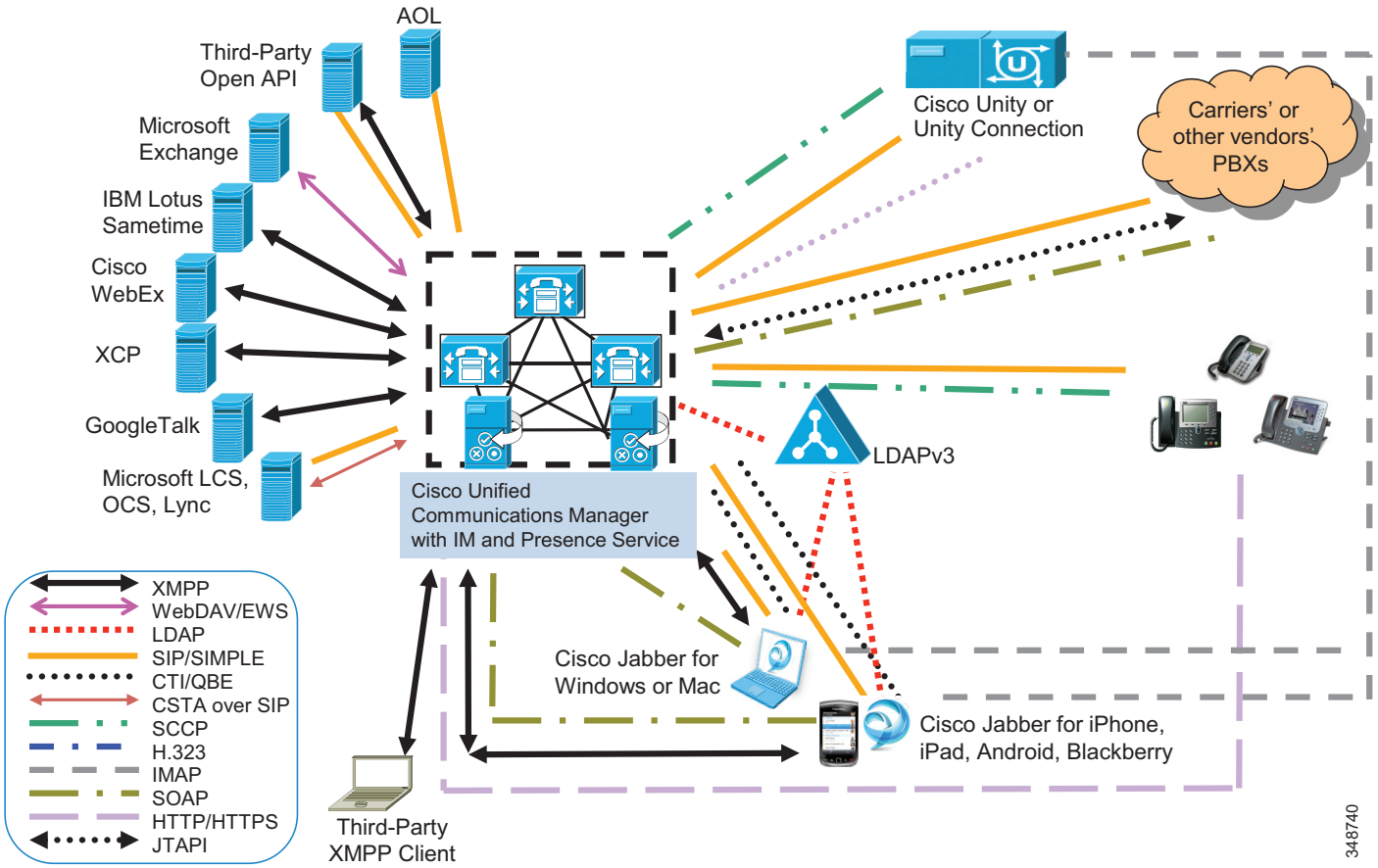
ステータス情報は、デバイスやユーザが実行可能な機能（音声、ビデオ、インスタント メッセージング、Web コラボレーションなど）と、デバイスやユーザの状態（連絡可能、ビジー、通信中など）の両方を示します。プレゼンス ステータスは、クライアントへのログインや電話機のオフフックなどの自動イベントによって決定されるか、またはユーザがステータス変更ピックリストから [Do Not Disturb] を選択したなどのユーザによるステータス変更の明示的な通知イベントによって決定されます。

プレゼンスに関する用語として、ウォッチャ、プレゼンス エンティティ（*presentity*）、およびプレゼンス サーバがあります。プレゼンス エンティティは、SIP/SIMPLE クライアントの場合は PUBLISH または REGISTER メッセージを、XMPP クライアントの場合は XML プレゼンス スタンザを使用して、自身の現在のステータスをプレゼンス サーバにパブリッシュします。プレゼンス エンティティは、通信クラスタ内外のディレクトリ番号（DN）または SIP のユニフォーム リソース識別子（URI）です。ウォッチャ（デバイスまたはユーザ）は、プレゼンス サーバにメッセージを送信することにより、プレゼンス エンティティに関するプレゼンス ステータスを要求します。これに対しプレゼンス サーバは、要求されたプレゼンス エンティティの現在のステータスが含まれたメッセージをウォッチャに返します。

オンプレミスの Cisco IM and Presence サービスのコンポーネント

Cisco IM and Presence サービスでは、図 20-1 に示すコンポーネントが対象になります。

図 20-1　Cisco IM and Presence サービスのインターフェイス



オンプレミスの Cisco IM and Presence サービス ユーザ

ユーザのプレゼンスは通常、ユーザのプレゼンス ステータス、システム上のユーザ数、またはユーザのプレゼンス機能で示されます。

Unified CM でエンドユーザとして指定されたユーザには、ライン アピアランスを関連付ける必要があります。Unified CM で IMP PUBLISH Trunk サービス パラメータを使用する場合は、ユーザをライン アピアランスと関連付ける必要があります。ライン アピアランスに関連付けることによって、ユーザは実質的にライン アピアランス（特定のデバイスのディレクトリ番号または URI）に結合されるので、より詳細できめ細かいプレゼンス情報を集約できます。ユーザを複数のライン アピアランスにマップすることも、各ライン アピアランスに複数のユーザ（最大 5 人）を割り当てることも可能です。

（注）　音声専用、ビデオ専用、または IM 専用の導入の場合、シスコ コラボレーション システム リリース（CSR）12.*x* の IM and Presence サービスの、フル UC モードでのクラスタ容量の制限は 75,000 ユーザです。

この章では、*プレゼンス ユーザ*という概念が随所で使用されます。Cisco IM and Presence で定義されるユーザの意味を常に念頭に置いてください。デフォルトで、Unified Communications 配置では IM and Presence サービス ユーザは *user@default_domain*（Jabber ID（JID）の基本）として定義されます。ここで、*user* は手動または Unified CM LDAP 同期アグリーメント（sAMAccountName、電子メール、employeenumber、telephonenumber、または UserPrincipalName）で設定されている値、*default_domain* は IM and Presence サービス管理で設定されているドメインです。

拡張 IM アドレッシングおよび IM アドレス スキーム

拡張 IM アドレッシング機能では、Unified CM IM and Presence で追加の IM アドレス（JID）設定オプションを使用でき、マルチドメイン サポートが提供されます。

IM アドレッシング方式：

- *UserID@Default_Domain* は、IM and Presence サービスをインストールした場合の、デフォルトの IM アドレッシング方式です。
- DirectoryURI IM アドレッシング方式は、複数のドメイン、ユーザのメール アドレスの調整、および Microsoft SIP URI の調整をサポートしています。

user@default_domain のデフォルト設定では 1 つのドメインだけが許可されますが、DirectoryURI では複数のドメインや電子メール アドレスを連絡先識別子としてより柔軟に処理することができます。ユーザは各自の sAMAccountName 属性を使用して Jabber にログインでき、Jabber ID が DirectoryURI フィールドにマッピングされます。Fleixble JID 構造により認証用の UID とは独立しています。

（注）　DirectoryURI は Unified CM のグローバル管理設定です。IM and Presence サービス アドレッシングに DirectoryURI を選択する場合、配置内のすべてのクライアントは DirectoryURI オプションを処理およびサポートできる必要があります。

ユーザ ID は電子メール アドレスにマッピングできますが、それが IM URI が電子メール アドレスに等しいという意味ではありません。代わりに、*<email-address>@Default_Domain* となります。たとえば、amckenzie@example.com @sales-example.com です。選択した設定をマッピングする Active Directory（AD）は、IM and Presence サービス クラスタ内のすべてのユーザに対してグローバルに適用されます。個々のユーザに対して異なるマッピングを設定することはできません。

単一 IM ドメインに限定される UserID@Default_Domain IM アドレッシング方式とは異なり、DirectoryURI IM アドレッシング方式は複数の IM ドメインをサポートします。DirectoryURI に指定されたドメインは IM and Presence サービスによってホストされているものとして処理されます。ユーザの IM アドレスを使用して、Cisco Unified Communications Manager で設定されているとおりにそれらのユーザの DirectoryURI に合わせます。

シングル サインオン（SSO）ソリューション

シスコではシングル サインオン ソリューション（SSO）として SAML SSO（リリース 10.0(1) 以降）の使用を推奨しています。

SAML は、すべてのオペレーティング システムでフェデレーテッド認証を有効にするオープン スタンダードです。SAML 標準により、クライアントは自身のプラットフォームのオペレーティング システム（OS）に関係なく、SAML 対応の Collaboration サービスに対して認証を行うことができます。SAML とは、ユーザおよびユーザの属性に関する情報を共有するために定義された標準セットであり、認証の要求方法、およびアクセスを許可または拒否する方法を提供します。たとえば SAML を使用すると、2 つの組織がパスワードを交換せずに信頼関係を確立することができます。

SAML は次のエンドユーザ アプリケーションをサポートします。

- Cisco Unified CM
- Cisco IM and Presence サービス
- Cisco Unity Connection
- Cisco WebEx Connect および Messenger Cloud

SAML SSO は次のエンドユーザ クライアントもサポートします。

- WebEx iOS
- WebEx Android
- WebEx Connect
- WebEx Messenger
- Jabber for Windows
- Jabber iOS
- Jabber for Android
- Jabber for Mac

SAML SSO の詳細については、オンプレミスの Cisco IM and Presence サービスの Jabber 用 SAML SSO（20-44 ページ）の項、または次の Web サイトで入手可能な『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』の最新バージョンを参照してください。

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

IM and Presence のコラボレーション クライアント

Jabber クライアントの Cisco Collaboration ソフトウェア ファミリを使用すると、ユーザは音声およびビデオ コールに簡単にアクセスでき、同僚のプレゼンス情報を含む連絡先ディレクトリや、インスタント メッセージング（IM）、ボイス メッセージング、デスクトップ共有、および会議のツールを利用できます。

Cisco Jabber クライアントではさまざまなオプションから選択でき、サードパーティ製 XMPP クライアントとアプリケーションも使用できます。Cisco Jabber クライアントは、インターフェイスの共通セットにより、基礎となる Cisco Unified Communication サービスと統合されます。一般に、各クライアントでは特定のオペレーティング システム、およびデスクトップとモバイルの両方のアプリケーションがサポートされます。

この章のクライアント固有の項では、Cisco Unified Communications システムへの統合に関して、関連する配置上の考慮事項、プランニング、および設計ガイドラインも提供しています。

次のコラボレーション クライアントが、Cisco Unified Communications システムでサポートされます。

- デスクトップ クライアント：
  - Cisco Jabber for Windows
  - Virtualization Experience Media Engine（VXME）for Windows
  - Cisco Jabber for Mac
- Web プラットフォーム：
  - Cisco Jabber Guest
  - Cisco Jabber Web SDK
- モバイル クライアント：
  - Cisco Jabber for iPhone
  - Cisco Jabber for iPad
  - Cisco Jabber for Blackberry
  - Cisco Jabber for Android
  - モバイルおよびタブレット

Macintosh と Windows の両方で使用できる Cisco Jabber デスクトップ クライアントは、基本的な IM and Presence、音声とビデオ、ビジュアル ボイスメール、デスクトップ共有、デスクフォン制御、Microsoft Office との統合、およびコンタクト管理など、堅牢で機能豊富なコラボレーション機能を提供します。

Cisco Jabber デスクトップ クライアントを配置して、Cisco IM and Presence および Cisco Unified Communications Manager がクライアント設定、インスタント メッセージングとプレゼンス、およびユーザとデバイスの管理を提供するオンプレミス サービスを利用できます。Cisco Jabber for Windows と Cisco Jabber for Mac は、Cisco WebEx Messenger サービスと統合することで、クラウドベースの環境でも使用できます。

マルチ デバイス メッセージング（MDM）とログイン

ユーザが Jabber デスクトップまたはモバイル クライアントにログインすると、すべての Cisco Jabber クライアントが IM and Presence サービス ノードに関連付けられます。ユーザが関連付けられた IM and Presence ノードは、在席状況、連絡先リスト、および機能ベースのタスクなど、そのユーザに対するすべての変更をモニタします。

IM and Presence サービス ノードは、それぞれのプレゼンス対応ユーザの登録済みクライアントをすべて追跡します。これは、ユーザが Cisco Jabber for iOS、Android、Windows、または Mac など、各種 Jabber クライアントの 1 つでログインしていても、すべてでログインしていても変わりません。

複数のクライアントにログインしているユーザ間で新しい IM セッションが開始されると、最初の着信メッセージが受信ユーザのすべての登録済みクライアントにブロードキャストされます。その後で、IM and Presence サービス ノードが登録済みクライアントのいずれかからの最初の応答を待機します。最初に応答したクライアントは、ユーザが別の登録済みクライアントから応答を開始するまで、引き続き着信メッセージを受け取ります。その後で、ノードが以降のメッセージをこの新しいクライアントに再ルーティングします。

次に例を示します。

> Johnny は Betty と IM カンバセーションを始めようと思っています。Johnny は、Cisco Jabber for Windows と Cisco Jabber for Android にすでにログインしています。また、Betty は、2 つのクライアントを中央の IM and Presence サービス ノードに登録しています。Johnny は次のようなメッセージを送信して会話を開始します。「こんにちは、Betty。今時間がありますか?」
>
> IM and Presence サービス ノードは、Betty に 2 つの登録済みクライアントがあることを識別し、両方に Johnny のメッセージをブロードキャストします。Betty は自分のデスクで、ノートパソコンと電話の両方に表示される Johnny のメッセージを見ます。Anita はノートパソコンを使用して応答することを選択し、次のようなメッセージを返信します。「数分後に会議がありますが、短時間ならチャットできます。」
>
> IM and Presence サービス ノードは、Betty が Cisco Jabber for Windows を使用して応答したことを特定して、これを会話で以降のすべてのメッセージをルーティングするクライアントとしてマーキングします。Johnny が「すぐに済みます」と返信すると、この返信は Cisco Jabber for Windows に直接ルーティングされます。会話のある時点から Betty が電話を使用して Johnny に応答し始めると、IM and Presence サービス ノードは以降のメッセージを Cisco Jabber for Windows ではなく、電話にルーティングします。

（注）　ユーザがログインするすべてのクライアントが、IM and Presence および Unified CM クラスタ上のユーザとデバイスの合計キャパシティの制限に影響します。たとえば 15,000 ユーザ VM 設定のクラスタでは、すべてのユーザが各自の iPhone およびデスクトップ Jabber クライアントにログインする場合、最大キャパシティは 15,000 ではなく 7,500 プレゼンス ユーザになります。

Jabber デスクトップ クライアント モード

Cisco Jabber デスクトップ クライアントは、次の 2 つのモードのいずれかで、呼制御に対して動作できます。

- ソフトフォン モード: コンピュータ上で音声とビデオを使用

  ソフトフォン モードの Jabber デスクトップ クライアントは、音声およびビデオ コール制御機能の SIP エンドポイントとして Unified CM に直接登録され、デバイス タイプ **Client Services Framework** として Unified CM で設定されます。

- デスクフォン制御モード: 音声（サポートされる場合はビデオも）に Cisco IP Phone を使用

  デスクフォン制御モードの Jabber デスクトップ クライアントは、SIP を使用して Unified CM に登録されることはありませんが、代わりに Cisco IP Phone を制御しながら、CTI/JTAPI を使用してコールの開始、モニタ、終了、回線状態のモニタを実行し、コール履歴を提供します。

モバイル クライアント用 Cisco Jabber

シスコは、Android、BlackBerry、Apple iOS デバイス（iPhone や iPad）向けにコラボレーション クライアントを提供しています。モバイル デバイス用 Cisco Jabber の詳細については、モバイル コラボレーション（21-1 ページ）の章を参照してください。

Cisco UC Integration™ for Microsoft Lync

Cisco UC Integration™ for Microsoft Lync は、一貫したユーザ エクスペリエンスを保ちつつ、Cisco Unified Communications サービスと Microsoft Lync および Microsoft Office Communications Server（OCS）R2 との統合を可能にします。このソリューションは、標準ベースの音声とビデオ、ユニファイド メッセージング、Web 会議、デスクフォン制御、テレフォニー プレゼンスなどの幅広い一連の Cisco Unified Communications サービスへのアクセスを提供することにより、Microsoft Lync のプレゼンスとインスタント メッセージングの機能を拡張します。

サードパーティ製 XMPP クライアントとアプリケーション

Cisco IM and Presence では SIP/SIMPLE および Extensible Messaging and Presence Protocol（XMPP）がサポートされているため、サードパーティ製のクライアントおよびアプリケーションで、プレゼンスおよびインスタント メッセージングの更新を複数のクライアント間で通信することがサポートされています。サードパーティ製 XMPP クライアントで、さまざまなデスクトップ オペレーティング システム間での拡張された相互運用性が実現します。また、Web ベースのアプリケーションは、SOAP、REST、または BOSH（Cisco AJAX XMPP Library API に基づく）を使用する HTTP インターフェイスを使用して、プレゼンスの更新、インスタント メッセージング、および参加者リストの更新を取得できます。サードパーティ製のオープン インターフェイスの詳細については、サードパーティ製プレゼンス サーバ統合（20-66 ページ）の項を参照してください。

SAML のシングル サインオン

シングル サインオンを利用すると、Cisco Jabber ユーザはすべての Jabber サービスに安全にアクセスできます。それぞれに個別にログインするよう要求されることはありません。Cisco Jabber アプリケーションでは、企業のアイデンティティ プロバイダーが実行する認証を使用します。アイデンティティ プロバイダーは、Cisco Jabber ユーザの認証エクスペリエンスを制御できます。たとえば、Cisco Jabber アプリケーションの初回実行時にユーザに社内ユーザ名とパスワードを一度要求し、ユーザに Cisco Jabber サービスの使用を許可する時間を指定することで制御します。

Cisco Jabber アプリケーションは Security Assertion Markup Language（SAML）を使用します。SAML は XML ベースのオープン スタンダードのデータ形式で、アイデンティティ プロバイダーによるクレデンシャルの確認後に定義済みの一連のシスコ サービスに対する透過的なアクセスを可能にします。SAML シングル サインオンは、Cisco WebEx Messenger サービス、Cisco Unified Communications Manager、および Cisco Unity Connection に対して有効にすることができます。SSO は、サービス ディスカバリを使用する Cisco Jabber クライアントで使用するために導入します。

SAMLv2 SSO は次の配置モデルをサポートします。

- オンプレミス配置モデル
  - IM and Presence および Unified CM
  - IM and Presence、Unified CM、および Unity Connection（SSO）
  - IM and Presence、Unified CM、Unity Connection（SSO）、および Cisco Mobile ワークスペース ソリューション（SSO、または SSO なし）
- ハイブリッド配置モデル
  - WebEx Messenger（SSO）および Unified CM
  - WebEx Messenger（SSO）、Unified CM、および Unity Connection
  - WebEx Messenger（SSO）、Unified CM、Unity Connection、および WebEx Meeting Center

Cisco Unified CM ユーザ データ サービス（UDS）

UDS は、Unified CM によって提供される包括的なサービス API です。UDS は、連絡先ソースに対する Cisco Expressway モバイルおよびリモート アクセスを介して Jabber が使用できる連絡先ソース API を提供します。UDS 連絡先ソースは、Unified CM のエンド ユーザ テーブルの情報を使用して連絡先検索サービスを提供します。

Cisco Unified CM 11.5 以降は、連絡先の検索に UDS-to-LDAP プロキシ機能を使用することもできます。この機能を有効にしても、連絡先の検索は引き続き UDS によって処理されますが、UDS が Jabber クライアントに結果をリレーすることで社内 LDAP ディレクトリにプロキシ処理されます。これにより Jabber クライアントは、Unified CM 内でサポートされる最大ユーザ数を超える社内ディレクトリを検索することができます。

UDS コンタクト サービスは、Expressway モバイルおよびリモート アクセスを介して接続されたリモート Jabber クライアントに対して常に使用され、社内ネットワーク上のクライアントに対してはオプションのコンタクト サービスとして使用されます。UDS 連絡先ソース データを入力するには、Unified CM の Web インターフェイス（エンドユーザが作成）、Active Directory またはサポートされている他の LDAP ソースに対する LDAP 同期機能、または UDS-to-LDAP プロキシ機能を使用します。

UDS では LDAP 連絡先ソースと同じ属性リストはサポートされません。代わりに、UDS は次の属性をサポートしています。

[username、firstname、lastname、middlename、nickname、phone number、homenumber、mobilenumber、email、directory URI、msURI、title、department、manager]

UDS では、LDAP 連絡先ソースと同レベルの予測検索または Ambiguous Name Resolution（ANR）は提供されません。UDS は firstname、lastname、および email address に対して検索を行います。

（注）　Ambiguous Name Resolution（ANR）は Lightweight Directory Access Protocol（LDAP）クライアントに関連付けられた検索アルゴリズムであり、複雑な検索フィルタなしでオブジェクトをバインドすることができます。ANR は、クライアントが認識していない可能性があるオブジェクトおよび属性を見つけるときに役立ちます。

オンプレミス配置での UDS の使用に関する考慮事項は次のとおりです。

- Jabber オンプレミス（オンネット）では連絡先ソースとして LDAP または UDS を使用できます。
- UDS は Unified CM が提供する一連の HTTP ベースのサービスです。UDS 連絡先ソースは、連絡先と番号の解決を提供する UDS サービスです。
- Expressway モバイルおよびリモート アクセスを介してリモート接続された Jabber は、連絡先ソースとして常に UDS を使用します。上記のとおり、設計がクラスタ サイジングに関する推奨事項に準拠している必要があります。

UDS はクラスタ内のすべての Unified CM サーバ上で実行される統合ネットワーク サービスであり、サーバ検出に不可欠です。IM 専用の配置の場合、音声とビデオは配置に含まれませんが、UDS サービスの負荷を処理および分散するために、Unified CM の呼処理サブスクライバ ペアが必要です。必要な Unified CM サブスクライバ ペアの数は IM 専用ユーザ数によって決まります。たとえば標準の Unified CM クラスタでユーザ数またはエンドポイント数が 40,000 である場合、40,000 人の IM 専用ユーザをサポートするには 4 つのサブスクライバ ペアが必要です。

LDAP ディレクトリ

次のような多くの異なる要件を満たすように、社内 LDAP ディレクトリを設定できます。

- ユーザ プロビジョニング：ディレクトリ統合を使用して、Cisco Unified Communications Manager データベースに LDAP ディレクトリからユーザを自動的にプロビジョニングできます。Cisco Unified CM は LDAP ディレクトリの内容と同期されるため、LDAP ディレクトリに変更が発生するたびに手動でユーザ情報の追加、削除、変更を行う必要はありません。
- ユーザ認証：LDAP ディレクトリのクレデンシャルを使用してユーザを認証できます。Cisco IM and Presence は、Cisco Unified Communications Manager からすべてのユーザ情報を同期してクライアント ユーザを認証します。
- ユーザ ルックアップ：LDAP ディレクトリの参照を有効にして、シスコのクライアントまたはサードパーティ製 XMPP クライアントが LDAP ディレクトリで連絡先を検索できるようにします。

AD グループおよびエンタープライズ グループ

Cisco Jabber ユーザは Microsoft Active Directory のグループを検索して、自分の連絡先リストに追加できます。

Cisco Unified CM は、指定された間隔（LDAP ディレクトリ設定の [LDAP ディレクトリ同期スケジュール（LDAP Directory Synchronization Schedule）] パラメータで指定）でデータベースを Microsoft Active Directory グループと同期し、同期時に Jabber エンドユーザの連絡先リストも更新します。

AD グループ同期機能が有効な状態で、Cisco Jabber ユーザがグループを連絡先リストに追加する場合、Cisco Jabber クライアントは IM and Presence サービス ノードにグループ要求を送信します。IM and Presence サービス ノードは各グループ メンバーに関する次の情報を提供します。

- 表示名（Display Name）
- ユーザ ID と役職（User ID and Title）
- 電話番号（Phone number）
- メール ID（Mail ID）

グループおよびユーザ フィルタに関する AD グループの考慮事項

- グループ フィルタは、Cisco CallManager アプリケーションの管理者が設定および検証する必要があります。
- 管理者は、ユーザ フィルタとグループ フィルタが適切に指定され、ユーザおよびグループ フィルタ用の適切なフィルタ フィールドに割り当てられていることを確認する必要があります。
- DirSync サービスではフィルタ文字列形式の構文または論理の正確さが検証されないため、管理者がフィルタの精度を確認する必要があります。
- 各フィルタ文字列に対して、同期の実行時にセキュリティ グループを無視するための文字列を 1 つ追加する必要があります。

WebEx ディレクトリ統合

WebEx ディレクトリの統合は WebEx 管理ツールの使用により実現します。WebEx は WebEx Messenger サービスに企業ディレクトリ情報のカンマ区切り形式（CSV）ファイルをインポートします。詳細については、次の Web サイトにあるマニュアルを参照してください。

https://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?17444.htm

ディレクトリ検索

ローカル Jabber デスクトップ クライアント キャッシュまたは連絡先リストで連絡先が見つからない場合、連絡先の検索を実行できます。WebEx Messenger ユーザは、連絡先名が入力されるとキャッシュ、連絡先リスト、およびローカル Outlook の連絡先リストを照会する予測検索を使用できます。一致が見つからない場合、検索は社内ディレクトリ（WebEx Messenger データベース）への照会を続けます。

Jabber クライアントの一般的な配置モデル

Cisco Jabber デスクトップ クライアントは、次の配置モデルをサポートします。

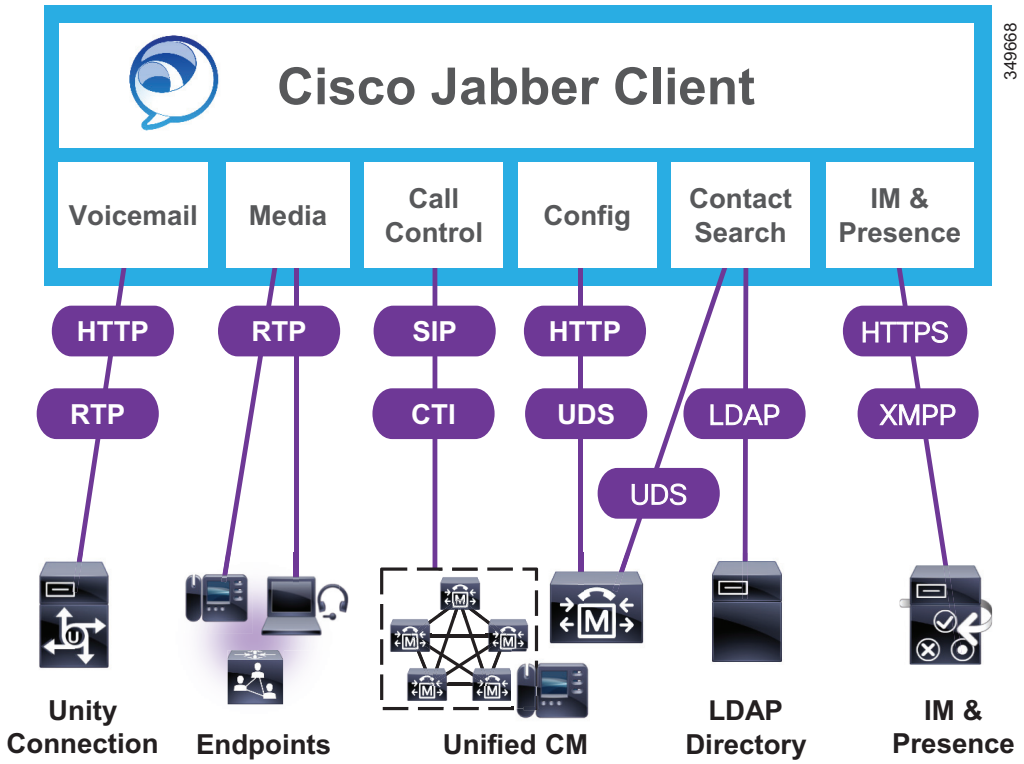
- オンプレミス配置モデル（20-12 ページ）
- クラウドベース配置モデル（20-13 ページ）
- クラウドベース/オンプレミス ハイブリッド配置モデル（20-14 ページ）
- 集中型 IM and Presence の導入（20-35 ページ）

配置モデルの選択は、主に IM and Presence の製品選択、および音声やビデオ、ボイスメール、デスクフォン制御といった追加サービスの要件に依存します。

オンプレミス配置モデル

オンプレミス配置モデルでは、運用や保守管理を自社で行う企業ネットワーク上ですべてのサービスがセットアップおよび設定されます（図 20-2 を参照）。

図 20-2　Jabber オンプレミス配置モデル



Cisco Jabber for Windows のオンプレミス配置モデルには、次のコンポーネントが必要です。

- Cisco Unified Communications Manager は、すべてのユーザおよびデバイスの設定機能を提供します。
- Cisco Unified Communications Manager およびシスコの会議デバイスは、音声およびビデオ会議機能を提供します。
- Cisco Unity Connection はボイスメール機能を提供します。
- Cisco IM and Presence はインスタント メッセージングおよびプレゼンス サービスを提供します。
- Microsoft Active Directory またはサポートされている他の LDAP ディレクトリは連絡先ソースを提供します。

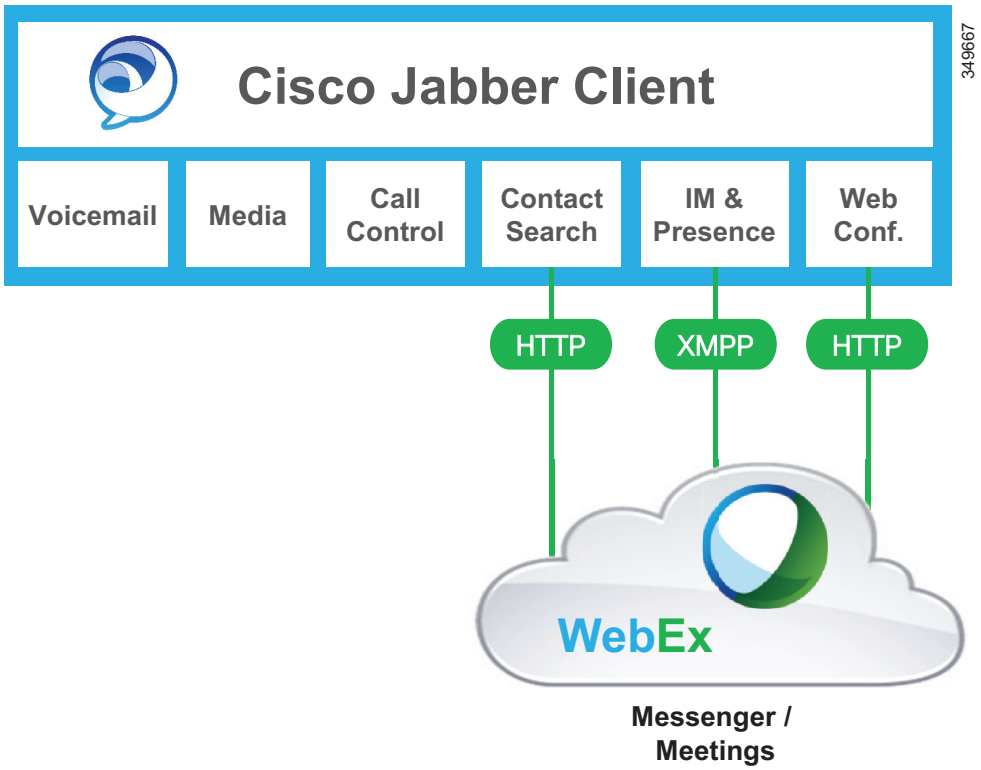
これらのコンポーネントは、Cisco Jabber クライアントの基本配置を実現する重要な要件です。基本配置をセットアップおよび設定した後は、次のような追加の配置オプションを設定できます。

- 音声：音声コール機能を提供します。
- ビデオ：ビデオ コールの送受信を可能にする機能を提供します。
- ボイスメール：ユーザが Cisco Jabber クライアントのユーザ インターフェイスで直接利用するか、ボイスメール番号のダイヤル時に取得できるボイスメール機能を提供します。
- デスクトップ共有：Binary Flow Control Protocol（BFCP）によりデスクトップを共有できるようにします。
- Microsoft Office 統合：Microsoft Outlook などの Microsoft Office アプリケーションのユーザ インターフェイスで、ユーザの在籍ステータスおよびメッセージング機能を直接提供します。

クラウドベース配置モデル

クラウドベース配置モデルでは、すべて（またはほとんど）のサービスが Cisco WebEx を使用してクラウドでホストされます。Cisco WebEx を使用してクラウドベース配置モデルを実装する場合は、Cisco WebEx 管理ツールでクラウドベース配置を管理およびモニタします（図 20-3 を参照）。

図 20-3　Jabber クラウドベース配置モデル（WebEx）



Cisco Jabber for Windows のクラウドベース配置モデルでは、次のサービスに Cisco WebEx Messenger サービスを使用します。

- インスタント メッセージングおよびチャット機能
- ユーザのプレゼンス機能
- ネイティブ デスクトップ共有
- ユーザ設定および連絡先ソース

これらのサービスは、Cisco Jabber for Windows の基本配置を実現するために必要な基本コンポーネントです。基本配置をセットアップおよび設定した後は、次のような追加の配置オプションを設定できます。

- Cisco WebEx Meeting Center：オンライン会議やイベントなどのホステッド コラボレーション機能を提供します。
- Microsoft Office 統合：Microsoft Outlook などの Microsoft Office アプリケーションのユーザ インターフェイスで、ユーザの在籍ステータスおよびメッセージング機能を直接提供します。この統合はデフォルトで設定されます。
- カレンダー統合：WebEx Meeting Center、Outlook、および IBM Lotus Notes とのカレンダー統合もサポートされます。

WebEx Messenger サービスの Jabber クライアント向け設定については、次の Web サイトで入手可能な『*Cisco WebEx Messenger Administrator's Guide*』を参照してください。

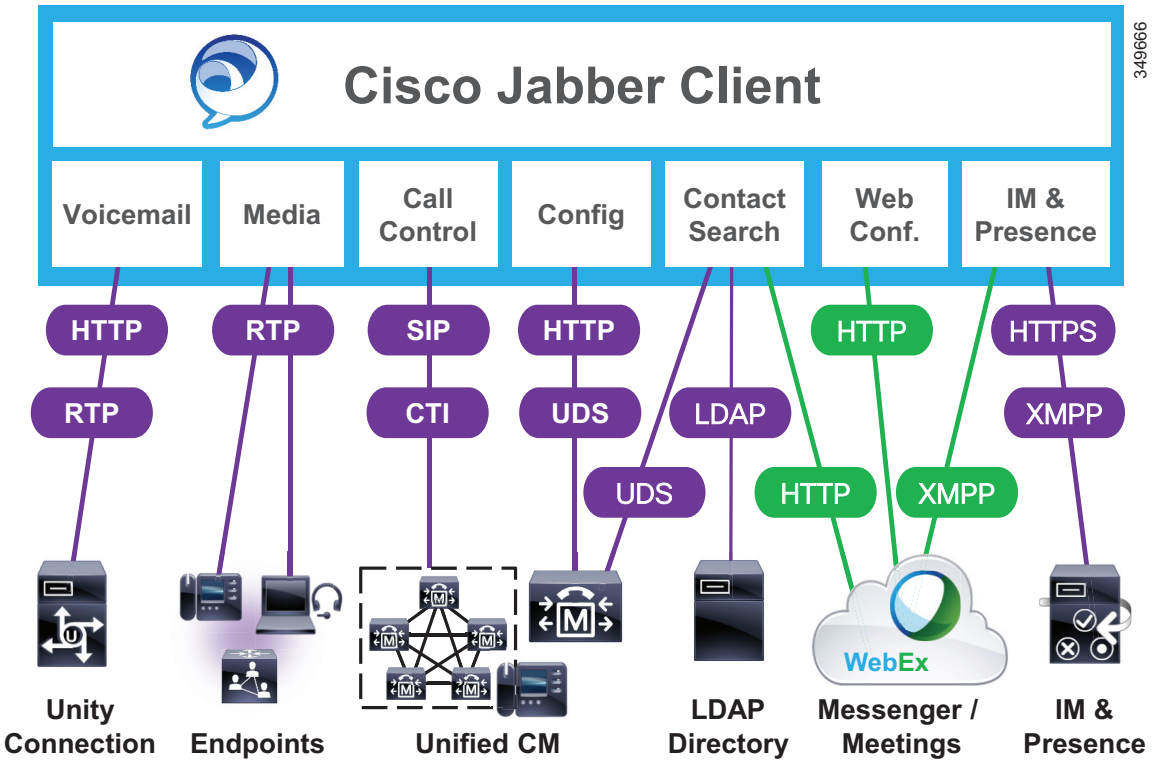
https://www.webex.com/webexconnect/orgadmin/help/index.htm

クラウドベース/オンプレミス ハイブリッド配置モデル

ハイブリッド配置では、Cisco WebEx Messenger サービスでホストされるクラウドベース サービスが、オンプレミス配置の次のコンポーネントと組み合わされます（図 20-4 を参照）。

- Cisco Unified Communications Manager は、ユーザおよびデバイス サービスを提供します。
- Cisco Unity Connection はボイスメール サービスを提供します。

図 20-4　Jabber クラウドベース/オンプレミス ハイブリッド配置モデル



クライアント固有の設計の考慮事項

ここでは、Mac および Windows 用の Cisco Collaboration デスクトップ クライアントに固有の設計に関する考慮事項について説明します。これらのクライアント タイプの一般的な設計の考慮事項については、Cisco Jabber デスクトップ クライアントのアーキテクチャ (8-25 ページ) の項にある設計ガイドラインを参照してください。

電話機固有のプレゼンスおよびビジー ランプ フィールド

Unified CM に接続するエンドポイントは、他の 1 つ以上のエンドポイントの回線ステータスをアイドル、ビジー、不明として受信できます。ステータスは、コール履歴、ディレクトリ、およびビジー ランプ フィールド (BLF) 機能を使用して表示されます。ユーザが参照を実行した後でのみコール履歴とディレクトリのプレゼンスが受信されている間は、BLF は継続的に電話機またはビデオ電話の回線ステータスをモニタし、そのステータスをモニタリング デバイスに設定されている特定のプレゼンス対応のスピード ダイヤルに表示します。

ユーザのテレフォニー プレゼンス要求は、クラスタ内かクラスタ外かに関係なく、すべて Cisco Unified CM で処理されます。

ウォッチャとプレゼンス エンティティが同じ Unified CM クラスタ内にある場合、プレゼンス要求を送信した Unified CM ウォッチャは、プレゼンス ステータスなどの応答を直接受信します。

プレゼンス エンティティがクラスタ外にある場合、Unified CM は、SIP トランク経由で外部のプレゼンス エンティティに照会します。ウォッチャが、SUBSCRIBE コーリング サーチ スペースとプレゼンス グループ（いずれもUnified CM のプレゼンス ポリシー（20-18 ページ）の章を参照）に基づいて外部プレゼンスをモニタする権限を持つ場合、SIP トランクはプレゼンス要求を外部プレゼンス エンティティに転送し、外部プレゼンス エンティティからの応答を待って、現在のプレゼンス ステータスをウォッチャに返します。

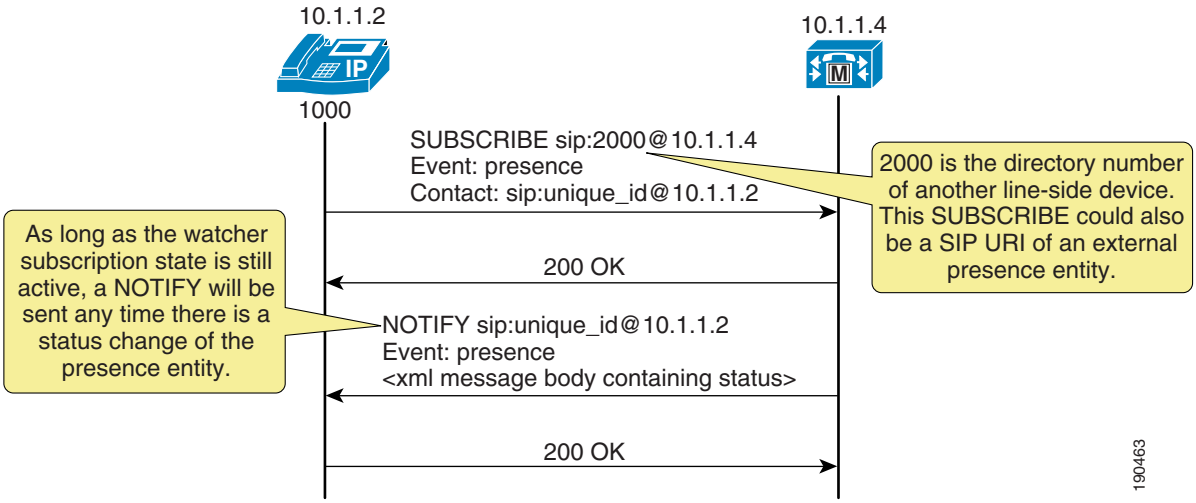
Unified CM クラスタ外のウォッチャは、プレゼンス要求を SIP トランクに送信します。Unified CM がそのプレゼンス エンティティをサポートしている場合、現在のプレゼンス ステータスを応答として返します。Unified CM がそのプレゼンス エンティティをサポートしていない場合、SIP エラー応答によってプレゼンス要求を拒否します。

SIP を使用した Unified CM のプレゼンス

Unified CM で、*SIP 回線*という用語は、Unified CM に直接接続され、登録されている SIP 対応のエンドポイントを表し、*SIP トランク*という用語は、SIP をサポートするトランクを表します。プレゼンス ウォッチャとして動作する SIP 回線側エンドポイントは、指定されたプレゼンス エンティティのプレゼンス ステータスを要求する SIP SUBSCRIBE メッセージを Unified CM に送信します。

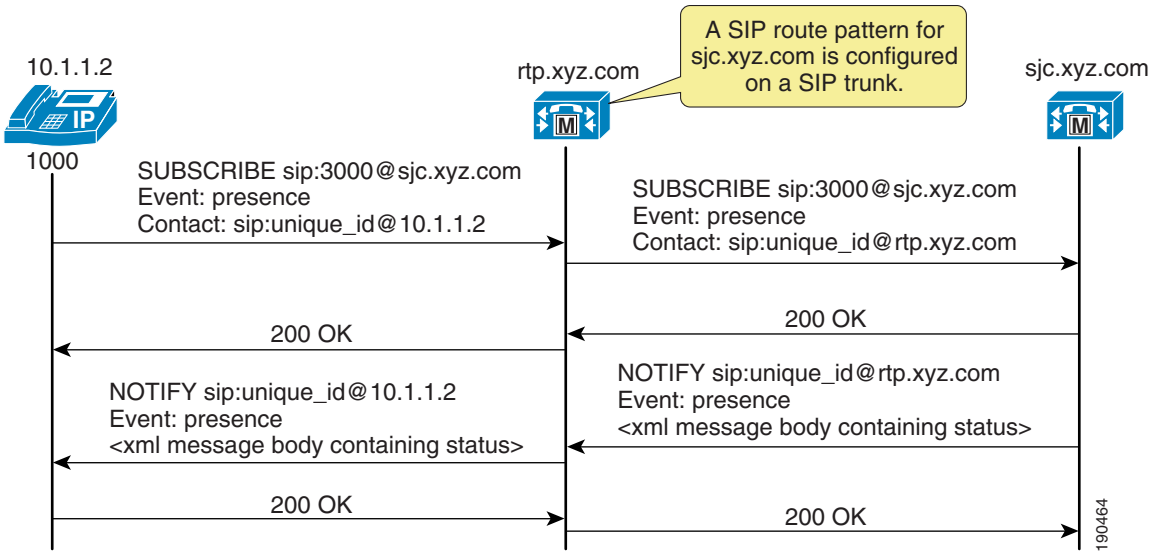
そのプレゼンス エンティティが Unified CM クラスタ内にある場合、Unified CM は、SIP 回線側プレゼンス要求に対し、プレゼンス エンティティの現在のステータスを示す SIP NOTIFY メッセージをプレゼンス ウォッチャに応答として送信します（図 20-5 を参照）。

図 20-5　　SIP 回線の SUBSCRIBE/NOTIFY の交換



そのプレゼンス エンティティが Unified CM クラスタ外にある場合、Unified CM は、SUBSCRIBE コーリング サーチ スペース、プレゼンス グループ、および SIP ルート パターンに基づいて、SUBSCRIBE 要求を外部の適切な SIP トランクにルーティングします。Unified CM は、プレゼンス エンティティのステータスを示す SIP NOTIFY 応答をトランクで受信すると、SIP 回線側プレゼンス要求に対し、プレゼンス エンティティの現在のステータスを示す SIP NOTIFY メッセージをプレゼンス ウォッチャに送信して応答します（図 20-6 を参照）。

図 20-6　　SIP トランクの SUBSCRIBE/NOTIFY の交換



Unified CM クラスタの外側にあるディレクトリ番号または SIP URI に対する SUBSCRIBE メッセージは、Unified CM 内の SIP トランク上で送受信されます。SIP トランクは、別の Unified CM とのインターフェイスとして動作するか、Cisco IM and Presence サービスとのインターフェイスとして動作できます。

Unified CM のスピード ダイヤルのプレゼンス

Unified CM は、ビジー ランプ フィールド（BLF）スピード ダイヤルを使用しスピード ダイヤルのプレゼンス機能をサポートしています。BLF スピード ダイヤルは、スピード ダイヤルとプレゼンス インジケータの両方の機能を備えています。ただし、BLF スピード ダイヤルを設定できるのは管理者のみで、システム ユーザは BLF スピード ダイヤルを設定できません。

管理者は、対象のディレクトリ番号または URI に対し、宛先の Unified CM クラスタまたは SIP トランク内のディレクトリ番号または URI に解決可能な BLF スピード ダイヤルを設定する必要があります。SIP URI に対して、BLF スピード ダイヤル用に、BLF SIP 回線側エンドポイントを設定することもできますが、SCCP 回線側エンドポイントの設定はできません。BLF スピード ダイヤルのインジケータは、回線レベルのインジケータであり、デバイス レベルのインジケータではありません。

（注） クラスタあたり最大 30,000 BLF スピード ダイヤルを設定できます。

BLF スピード ダイヤルをサポートしている電話機モデルのリストについては、https://www.cisco.com/ で入手可能な Cisco Unified IP Phone のアドミニストレーション ガイドを参照してください。

図 20-7 では、電話機のさまざまなタイプの BLF スピード ダイヤルのインジケータを示しています。

図 20-7　Cisco Unified IP Phone 7900 シリーズのスピード ダイヤルのプレゼンスのインジケータ

State	Icon	LED
Idle		
Busy		
Unknown		

190465

Unified CM のコール履歴のプレゼンス

Unified CM は、コール履歴リストに関するプレゼンス機能をサポートしています（電話機の Directories ボタン）。コール履歴リストのプレゼンス機能は、Unified CM Administration 内の **BLF for Call Lists** エンタープライズ パラメータによって制御されます。**BLF for Call Lists** エンタープライズ パラメータは、電話機の Directories ボタンを使用するすべてのページ（不在着信、着信履歴、発信履歴、個人ディレクトリ、社内ディレクトリ）に影響を及ぼし、グローバルに設定されます。

通話履歴リストのプレゼンス機能をサポートしている電話機モデルのリストについては、https://www.cisco.com/ で入手可能な Cisco Unified IP Phone のアドミニストレーション ガイドを参照してください。

コール履歴リストのプレゼンス インジケータには、図 20-7 のアイコン列と同じインジケータが使用されます。LED インジケータはありません。

Unified CM のプレゼンス ポリシー

Unified CM には、プレゼンス ステータスを要求するユーザに対して、ポリシーを設定する機能があります。このポリシーを設定するには、まずプレゼンス ステータスに関する SIP SUBSCRIBE メッセージを特にルーティングするコーリング サーチ スペースを設定します。次に、ユーザを関連付けることのできるプレゼンス グループを設定し、そのグループに対し、他のグループのユーザのプレゼンス ステータスを表示するためのルールを指定します。

Unified CM の SUBSCRIBE コーリング サーチ スペース

Unified CM のプレゼンス ポリシーの第 1 の側面は、SUBSCRIBE コーリング サーチ スペースです。Unified CM は、SUBSCRIBE コーリング サーチ スペースを使用して、ウォッチャ（電話機またはトランク）から送信されるプレゼンス要求（Event フィールドが Presence に設定された SUBSCRIBE メッセージ）のルーティング方法を決定します。SUBSCRIBE コーリング サーチ スペースは、ウォッチャに関連付けられ、ウォッチャが「確認」できるパーティションをリストします。このメカニズムによって、プレゼンス SUBSCRIBE 要求を通常の呼処理コーリング サーチ スペースから独立してルーティングするという詳細な制御が可能になります。

SUBSCRIBE コーリング サーチ スペースは、デバイス別またはユーザ別に割り当てることができます。ユーザがエクステンション モビリティを使用してデバイスにログインするか、管理によってデバイスに割り当てられると、開始されるサブスクリプションにユーザ設定が適用されます。

SUBSCRIBE コーリング サーチ スペースを [<なし>(<None>)] に設定すると、BLF スピード ダイヤルとコール履歴リストのプレゼンス ステータスが機能しなくなり、サブスクリプション メッセージが「ユーザ不明(user unknown)」として拒否されます。有効な SUBSCRIBE コーリング サーチ スペースを指定すると、インジケータが動作し、SUBSCRIBE メッセージが受け入れられて、適切にルーティングされます。

(注)　<None> と定義されたままのコーリング サーチ スペースを残さないでください。コーリング サーチ スペースを<None> に設定したままにすると、プレゼンス ステータスやダイヤル プランの動作が予測困難になる可能性があります。

Unified CM のプレゼンス グループ

Unified CM のプレゼンス ポリシーの第 2 の側面は、プレゼンス グループです。プレゼンス グループには、デバイス、ディレクトリ番号、およびユーザを割り当てることができます。すべてのユーザは、デフォルトで Standard Presence Group に割り当てられています。プレゼンス グループは、定義済みのプレゼンス グループとのユーザのアソシエーションに基づいて、ウォッチャがモニタできる対象を制御します(たとえば、Contractors(派遣社員)から Executives(エグゼクティブ)のモニタは禁止するが、逆は許可するなど)。ユーザがエクステンション モビリティ経由でデバイスにログインするか、管理によってデバイスに割り当てられると、開始されるサブスクリプションにプレゼンス グループのユーザ設定が適用されます。

複数のプレゼンス グループが定義されている場合は、Inter-Presence Group Subscribe Policy サービス パラメータが使用されます。1 つのグループと別のグループとの関係が、許可や禁止ではなく Use System Default 設定による場合、このサービス パラメータの値が有効になります。Inter-Presence Group Subscribe Policy サービス パラメータが **Disallowed** に設定されている場合、SUBSCRIBE コーリング サーチ スペースが許可していても、Unified CM は要求をブロックします。Inter-Presence Group Subscribe Policy サービス パラメータは、コール履歴リストがあるプレゼンス ステータスにのみ適用され、BLF スピード ダイヤルには使用されません。

依存関係レコードを有効にすると、プレゼンス グループは、関連付けられたすべてのディレクトリ番号、ユーザ、およびデバイスをリストできます。依存関係レコードを使用することで、管理者はグループレベルの設定に関する特定の情報を検索できます。ただし、Dependency Record Enterprise パラメータを有効にすると、CPU の使用量が大きくなるので注意してください。

Unified CM のプレゼンス ガイドライン

システム管理者は、Unified CM で Unified CM Administration の中から、ユーザの電話機の状態のプレゼンス機能の設定と制御が可能です。Unified CM 内でプレゼンスを設定する場合は、次のガイドラインに従ってください。

- ユーザの電話機の状態のプレゼンス ステータスを表示できる適切なモデルの Cisco Unified IP Phone を選択します。
- プレゼンス ユーザのプレゼンス ポリシーを定義します。
  - SUBSCRIBE コーリング サーチ スペースを使用して、ウォッチャ プレゼンスベースの SIP SUBSCRIBE メッセージが正しい宛先にルーティングされるように制御します。
  - プレゼンス グループを使用して同類のユーザのセットを定義し、他のユーザ グループのプレゼンス ステータスの更新を許可するか禁止するかを定義します。

- コール履歴リストのプレゼンス機能はグローバルに有効になりますが、プレゼンス ポリシーを使用してユーザ ステータスをセキュリティ保護できます。
- BLF スピード ダイヤルは管理制御され、プレゼンス ポリシー設定の影響を受けません。

（注）　Cisco Business Edition は、Unified CM によってユーザ プレゼンス機能を設定および制御する場合とほぼ同じ方法で使用できます。詳細については、呼処理（9-1 ページ）の章を参照してください。

ユーザ プレゼンス：Cisco IM and Presence アーキテクチャ

Cisco IM and Presence サービスは、インスタント メッセージングとプレゼンスに標準ベースの XMPP を使用します。Cisco IM and Presence サービスは、SIP IM プロバイダーとの相互運用のために SIP もサポートしています。また、Cisco IM and Presence は、Simple Object Access Protocol（SOAP）経由の設定インターフェイス、Representational State Transfer（REST）経由のプレゼンス インターフェイス、および Cisco AJAX XMPP Library（CAXL）経由のプレゼンス、インスタント メッセージング、および Bidirectional-streams Over Synchronous HTTP（BOSH）インターフェイスを備えた HTTP インターフェイスを提供します。Cisco AJAX XMPP Library Web ツール キットは、Cisco IM and Presence 内の Extensible Communications Platform 上の BOSH インターフェイスと通信します。Cisco IM and Presence サービスは、これらの標準ベースの SIP、SIMPLE、XMPP、および HTTP インターフェイスを使用して、ユーザ機能および属性を収集、集約、および配布します。

シスコ製またはサードパーティ製のアプリケーションは、プレゼンスとの統合によって、エンドユーザ エクスペリエンスおよび効率性を向上させるサービスを提供できます。Cisco IM and Presence サービスの中心となるコンポーネントは、プレゼンス、インスタント メッセージング、参加者、ルーティング、ポリシー、およびフェデレーション管理を処理する Extensible Communications Platform（XCP）、プレゼンス ステータス収集、ネットワークベースの高度なプレゼンス構成、およびプレゼンス対応ルーティング機能を処理する高度なプレゼンス サービス、および永続的なチャットとメッセージ アーカイブが外部データベースに対して処理されるアドホック グループ チャット ストレージのサポートです。永続的なチャットが有効になっていると、アドホック チャットの期間中、アドホック ルームが外部の PostgreSQL、Microsoft SQL、または Oracle データベースに保存されます。永続的なチャットが無効の場合、アドホック チャットは、チャットの期間中揮発性メモリに保管されます。

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

Cisco IM and Presence サービスは、Microsoft Lync Server 2010 および 2013、および Unified CM に接続された Cisco Unified IP Phone 用の Microsoft Lync クライアントとの相互運用性もサポートしています。Microsoft Lync クライアントの相互運用性には、クリックツーダイヤル機能、リモート呼制御（RCC）経由の電話制御機能、および Cisco Unified IP Phone のプレゼンス ステータスが含まれます。

オンプレミスの Cisco IM and Presence サービス クラスタ

Cisco IM and Presence サービスで使用される基礎となるアプライアンス モデルおよびハードウェアは、Unified CM や Cisco Unified Computing System（UCS）プラットフォーム上の Unified CM で使用されるものと同じです（同様の管理インターフェイスなど）。サポートされるプラットフォームの詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Compatibility Matrix*』の最新バージョンを参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

Cisco IM and Presence サービス クラスタは、最大 6 台のサーバで構成され、そのうち 1 つはパブリッシャに指定されています。これは、Unified CM のパブリッシャおよびサブスクライバと同じアーキテクチャ概念を採用しています。Cisco IM and Presence サービス クラスタ内の各サーバをグループ化して、サブクラスタを構成できます。サブクラスタには、最大で 2 台のサーバを関連付けることができます。図 20-8 は Cisco IM and Presence サービス クラスタの基本的なトポロジを示し、図 20-9 は可用性の高いトポロジを示しています。また、Cisco IM and Presence サービス クラスタには、2 台のサーバが設定されたサブクラスタと、1 台のサーバが設定されたサブクラスタを混合して配置することもできます（図 20-10 を参照）。

図 20-8　　オンプレミスの Cisco IM and Presence サービスの基本的な配置

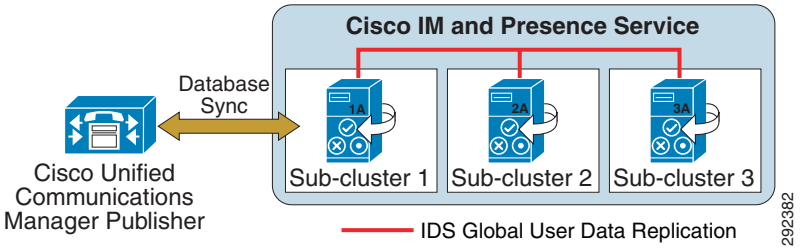


図 20-9　　オンプレミスの Cisco IM and Presence サービスのハイ アベイラビリティ配置

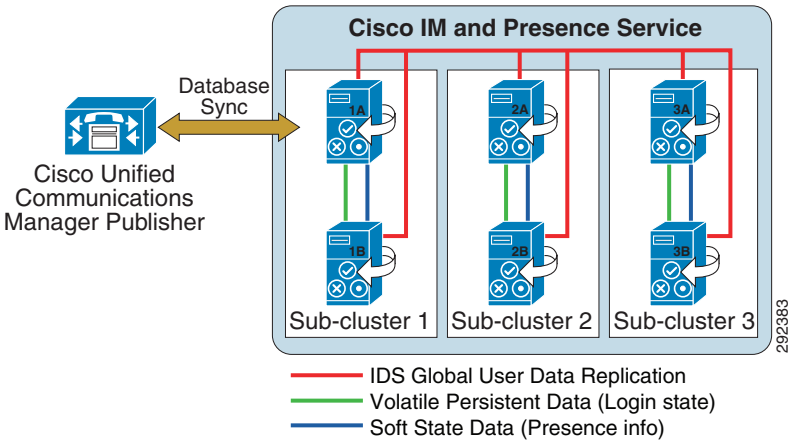
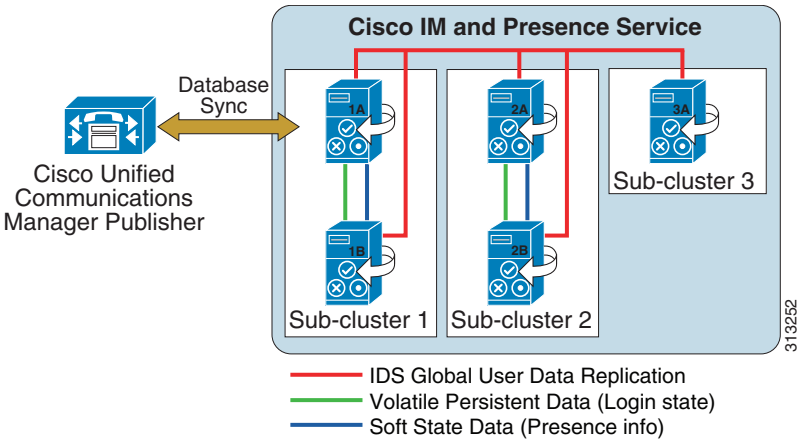


図 20-10　　オンプレミスの Cisco IM and Presence サービスの混合配置



オンプレミスの Cisco IM and Presence サービスは、ユーザ情報とデバイス情報を共有することによって、Unified CM パブリッシャが使用するデータベースを利用し、それを拡張します。

Cisco Unified CM とのアベイラビリティ統合をサポートするには、CUCM ドメインの SIP Proxy サービス パラメータが Unified CM クラスタの DNS ドメインと一致する必要があります。デフォルトでは、CUCM ドメインの SIP Proxy サービス パラメータは IM and Presence データベース パブリッシャ ノードの DNS ドメインに設定されます。したがって、IM and Presence データベース パブリッシャ ノードの DNS ドメインが Unified CM クラスタの DNS ドメインと異なる場合、IM and Presence データベース パブリッシャ ノードで Cisco Unified CM IM and Presence の管理ユーザ インターフェイスを使用してこのサービス パラメータを更新する必要があります。Cisco Unified Communications Manager クラスタに関連付けられた DNS ドメインの指定の詳細については、次の Web サイトで入手可能な『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』の最新バージョンを参照してください。

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

IM and Presence はすべての Unified CM ノードのアクセス コントロール リスト（ACL）エントリを維持することに注意してください。これらのエントリは FQDN ベースで、Unified CM のホスト名を IM and Presence パブリッシャの DNS ドメインに付加することによって生成されます。そのため、IM and Presence パブリッシャ（データベース）の DNS ドメインが Unified CM クラスタの DNS ドメインと異なる場合、無効な ACL エントリが生成されることで問題が発生する可能性があります。

（注）　単一の Unified CM クラスタがサポートするのは、1 つの IM and Presence サービス クラスタのみであるため、Unified CM クラスタごとに、別々の IM and Presence サービス クラスタが必要です。

クラスタ内トラフィックは、Cisco IM and Presence サービスと Unified CM の間、および Cisco IM and Presence サービス パブリッシャとサブスクライバ サーバの間に非常に低いレベルで加わります。両方のクラスタは、共通のホスト ファイルを共有し、IPTables を使用した強力な信頼関係を備えています。データベースとサービスのレベルでは別個の異なるクラスタですが、設定と管理は主に Unified CM クラスタで行われ、制限付きの設定と管理は IM and Presence サービス クラスタで行われます。現在、クラスタ内トラフィックには、トランスポート層セキュリティ（TLS）や IPSec は使用されていません。

Cisco IM and Presence サービス パブリッシャは、Simple Object Access Protocol（SOAP）インターフェイスを使用して、AVVID XML Layer Application Program Interface（AXL API）経由で Unified CM パブリッシャと直接通信します。最初の設定時に、Cisco IM and Presence サービス パブリッシャは、Unified CM ユーザおよびデバイス データベース全体の初期同期を実行します。すべての Cisco IM and Presence サービス ユーザは、Unified CM エンド ユーザ設定で設定されます。同期の際、Cisco IM and Presence サービスは、Unified CM データベースからこれらのユーザをそれ自体のデータベースに入力しますが、その管理インターフェイスからエンドユーザ設定を提供することはありません。同期後、Cisco IM and Presence サービスでユーザを管理するには、Cisco Unified Communications Manager の管理者インターフェイスを介して IM and Presence サービスに対してユーザを有効にする必要があります。

（注）　Cisco IM and Presence サービスは、最大 160,000 ユーザの同期をサポートします（Unified CM と同等）。ただし、Cisco IM and Presence サービス クラスタに対してライセンスされたプレゼンス ユーザの最大数は、メガクラスタ配置で 3 つのサブクラスタ ペアに 25,000 ユーザ IM and Presence VM テンプレートを使用した場合は 75,000 です。

Unified CM から最初に Cisco IM and Presence サービス データベースを同期する場合、少し時間がかかることがあります。所要時間は、データベース内の情報量と現在システムにかかっている負荷によって異なります。それ以降は、新しいユーザ情報やデバイス情報が Unified CM に追加されたときに、Unified CM から Cisco IM and Presence サービスへのデータベースの同期がリアルタイムで実行されます。

（注）　Cisco IM and Presence サービスによる Unified CM からの初期データベース同期の際、同期エージェントがアクティブな間は、管理作業を一切行わないでください。

オンプレミスの Cisco IM and Presence サービスのハイ アベイラビリティ

Cisco IM and Presence サービス クラスタは、最大 6 台のサーバで構成されていますが、これを複数のサブクラスタ（最大 3 つのサブクラスタ）に構成してハイ アベイラビリティを実現できます。サブクラスタには最大 2 台のサーバが含まれ、フェールオーバー イベントの発生時には、サブクラスタの片方のサーバに関連付けられたユーザが、自動的にサブクラスタの他方のサーバを使用できるようになります。Cisco IM and Presence サービスはサブクラスタ間のフェールオーバー機能を提供しません。

Cisco IM and Presence サービス クラスタをハイ アベイラビリティを確保して配置する場合、フェールオーバーの発生時にサブクラスタ内の 1 台のサーバに対してオーバーサブスクリプションにならないよう、サーバあたりの最大ユーザ数を考慮する必要があります。

アクティブ/アクティブとアクティブ/スタンバイの 2 種類の異なる設定を使用することで、ハイ アベイラビリティを実現できます。平衡型モードでは、連動するようにプレゼンス冗長グループ内のノードを設定できます。コンポーネントの障害や停電により、いずれかのノードが停止すると、ユーザのロード バランシングとユーザのフェールオーバーが自動的に有効になり、冗長ハイ アベイラビリティが提供されます。アクティブ/スタンバイの設定では、アクティブ ノードが停止すると、スタンバイ ノードはアクティブ ノードを自動的に引き継ぎます。

配置上の考慮事項

IM and Presence サービス クラスタは、25,000 ユーザ VM 設定テンプレートで 3 つの IM and Presence ノードを配置した場合、フル UC モードで最大 75,000 ユーザをサポートします。ただしハイ アベイラビリティは確保されません。

75,000 ユーザのハイ アベイラビリティ配置では、3 つの IM and Presence サブクラスタ ペアを 25,000 ユーザ VM 設定テンプレート オプションで配置する必要があります。

（注）　25,000 ユーザ VM 設定は、事前にシスコによって確認および承認されたメガクラスタ配置に使用する必要があります。メガクラスタ配置以外の場合は、15,000 ユーザまたは 5,000 ユーザ VM 設定テンプレートなど、キャパシティの少ない VM 設定テンプレートを使用してください。ただし、メガクラスタ以外の配置でも 25,000 ユーザ IM and Presence VM 設定の使用が望ましい場合は、25,000 ユーザ VM 設定を配置する前に、シスコに設計トポロジを伝えて承認を要求してください。25,000 ユーザ VM テンプレートを使用した IM and Presence 設定の設計を確認した上で、例外が提供される場合があります。

オンプレミスの Cisco IM and Presence サービス配置モデル

Unified CM では、次の配置モデルを選択できます。

- 単一サイト
- 集中型呼処理を使用するマルチサイト WAN
- 分散型呼処理を使用するマルチサイト WAN
- WAN を介したクラスタリング
- 集中型 IM and Presence

Cisco IM and Presence サービスは、すべての Unified CM 配置モデルでサポートされます。ただし、初期ユーザ データベース同期のために、Cisco IM and Presence サービス パブリッシャを Unified CM パブリッシャと同じ物理データセンターに共存させることを推奨します。すべてのオンプレミスの Cisco IM and Presence サーバは、地理的なデータセンターの冗長性および WAN を介したクラスタリングを除き、物理的に Cisco IM and Presence サービス クラスタ内の同じデータセンターに配置する必要があります（詳細については、WAN を介したクラスタリング（20-32 ページ）を参照してください）。

Unified CM の配置モデルの詳細については、コラボレーションの配置モデル（10-1 ページ）の章を参照してください。

Cisco IM and Presence サービスの配置は、ハイ アベイラビリティの要件、合計ユーザ数、および使用するサーバに依存します。詳細な設定および配置の手順については、次の Web サイトで入手可能な『*Deployment Guide for Cisco IM and Presence*』を参照してください。

https://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

可用性が高い Cisco IM and Presence サービス クラスタには、サブクラスタごとに 2 台のサーバが必要です。これにより、ユーザはサブクラスタ内のサーバ間でフェールオーバーを実行できますが、サポートされる合計ユーザ数とフェールオーバー時間は、有効にする機能、連絡先リストの平均サイズ、サーバ上のトラフィック レート、およびサーバの配置（WAN を介した配置の場合）によって異なります。Cisco IM and Presence サービスのサブクラスタに 2 台のサーバを設定すると、Unified CM 管理の [システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Group）] で [ハイアベイラビリティ（High Availability）] が設定されている場合、常にハイ アベイラビリティとして動作します。ハイ アベイラビリティは、アクティブ/スタンバイ モデルまたはアクティブ/アクティブ モデルを使用して配置できます。これらのモードは、エンタープライズ パラメータの [プレゼンスサーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] によって制御されます。デフォルトで、すべてのユーザはクラスタ内のすべてのサーバに均等に割り当てられます。このパラメータはデフォルト値のままにすることを推奨します。

（注）　各サブクラスタはプレゼンス冗長グループです。

Cisco IM and Presence アクティブ/スタンバイ モード（[プレゼンスサーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] を [なし（None）] に設定）は、手動でユーザをサブクラスタの最初のサーバに割り当て、2 番目のサーバにユーザを 1 人も割り当てずにすべての処理を同期させ、サブクラスタの最初のサーバに障害が発生した場合のフェールオーバーに備えることで実現されます。たとえば、図 20-9 では、最初のユーザをサーバ 1A、2 番めのユーザをサーバ 2A、3 番めのユーザをサーバ 3A、4 番めのユーザをサーバ 1A、5 番めのユーザをサーバ 2A、6 番めのユーザをサーバ 3A、というように割り当てています。これにより、ユーザは、クラスタのすべての「A」サーバに均等に割り当てられます。

Cisco IM and Presence アクティブ/アクティブ モード（[プレゼンスサーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] を [平衡化（balanced）] に設定）は、デフォルト設定であり、負荷分散の目的で推奨されます。このモードでは自動的にユーザがサブクラスタ内のすべてのサーバに均等に割り当てられます。各サーバは同期され、サブクラスタ内の他のサーバの障害時には、フェールオーバーが可能です。たとえば、図 20-9 では、最初のユーザをサーバ 1A、2 番目のユーザをサーバ 2A、3 番目のユーザをサーバ 3A、4 番目のユーザをサーバ 1B、5 番目のユーザをサーバ 2B、6 番目のユーザをサーバ 3B、というように割り当てます。ユーザは、クラスタ内のすべてのサーバに均等に割り当てられます。

[プレゼンスサーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] を [平衡化（balanced）] に設定した *Cisco IM and Presence アクティブ/アクティブ*配置では、使用する機能、ユーザの連絡先リストのサイズ、および生成されるトラフィック（ユーザ データ プロファイル）に応じた柔軟な冗長構成が可能です。完全な冗長性モードの Cisco IM and Presence アクティブ/アクティブ配置では、機能に関係なく、サポートされる合計ユーザ数を半分にする必要があります（たとえば、15,000 ユーザ OVA をバランス型のハイ アベイラビリティ冗長構成で配置する場合、1 つのサブクラスタでサポートされるユーザ数は、最大 15,000 人になります）。非冗長モードの Cisco IM and Presence アクティブ/アクティブ配置では、使用する Cisco IM and Presence サービスの機能、ユーザの連絡先リストの平均サイズ、および生成されるトラフィックをさらに詳細に検討する必要があります。たとえば、プレゼンスとインスタント メッセージングを有効にし、カレンダーとモビリティ統合を無効にした配置で、連絡先リストが平均 30 ユーザ、ユーザ データ プロファイルが少数のプレゼンスとインスタント メッセージングの更新の場合、サブクラスタあたり 15,000 人を超えるユーザをサポートできます。

ハイ アベイラビリティ構成でない Cisco IM and Presence サービス クラスタ配置の場合、サブクラスタの各サーバは、そのサーバの最大ユーザ数までサポートできます。また、クラスタ内のすべてのサーバに対してサポートされる合計ユーザ数は、IM and Presence サービス クラスタの最大ユーザ数まで許容されます。サブクラスタに 2 台目のサーバを追加した後でも、サブクラスタはハイ アベイラビリティ配置と同様に動作しますが、オンライン サーバがキャパシティの上限（有効な Cisco IM and Presence サービス機能、ユーザの連絡先リストの平均サイズ、およびユーザによって生成されるトラフィック量に基づく）に達すると、サーバに障害が発生した場合にフェールオーバーが成功しないことがあります。

オンプレミスの Cisco IM and Presence サービスの配置例

例 20-1　単一の Unified CM クラスタで Cisco IM and Presence サービスを配置

配置要件：

- 4,000 ユーザを最大 13,000 ユーザまで拡張可能
- 単一の Cisco Unified Communications Manager クラスタ
- インスタント メッセージのロギングおよびコンプライアンスへの準拠が不要
- ハイ アベイラビリティが不要

ハードウェアおよびソフトウェア プラットフォーム：

- 15,000 ユーザ VM 設定フル UC テンプレート対応の Cisco UCS 仮想マシン

配置：

- 1 つのシングルサーバのサブクラスタ（[平衡化（balanced）] に設定した [プレゼンスサーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] を使用）

例 20-2　2 つの Unified CM クラスタで Cisco IM and Presence サービスを配置

配置要件：

- 11,000 ユーザを最大 24,000 ユーザまで拡張可能
- 2 つの Cisco Unified Communications Manager クラスタ
- インスタント メッセージのロギングおよびコンプライアンスへの準拠が不要
- ハイ アベイラビリティが不要

ハードウェアおよびソフトウェア プラットフォーム：

- 2 つの 15,000 ユーザ VM 設定フル UC テンプレート対応の Cisco UCS 仮想マシン

配置：

- 2 つの Cisco IM and Presence サービス クラスタ（Cisco Unified Communications Manager クラスタごとに 1 つ）で各クラスタに 1 つのサーバ（[平衡化（balanced）] に設定した [プレゼンスサーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] を使用）

例 20-3　単一の Unified CM クラスタで Cisco IM and Presence サービスを配置

配置要件：

- 500 ユーザを最大 2500 ユーザまで拡張可能
- 単一の Cisco Unified Communications Manager クラスタ
- インスタント メッセージのアーカイブが必要
- ハイ アベイラビリティが必要

ハードウェア：

- 2 つの 5,000 ユーザ VM 設定フル UC テンプレート対応の Cisco UCS 仮想マシン

配置：

- 2 台のサーバから構成される 1 つのサブクラスタ（[平衡化（balanced）] に設定した [プレゼンス サーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] を使用）、およびクラスタ用の PostgreSQL、Microsoft SQL、または Oracle データベース インスタンス

例 20-4　単一の Cisco Business Edition クラスタで Cisco IM and Presence サービスを配置

配置要件：

- 150 ユーザを最大 1,000 ユーザまで拡張可能
- 単一の Cisco Business Edition
- インスタント メッセージのアーカイブと永続的なチャットが必要
- ハイ アベイラビリティが必要

ハードウェア：

- 1,000 ユーザ VM 設定フル UC テンプレートを使用する Cisco Business Edition 6000H

配置：

- 2 台のサーバから構成される 1 つのサブクラスタ（[平衡化（balanced）] に設定した [プレゼンス サーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] を使用）、およびクラスタ内のサーバごとに固有の PostgreSQL、Microsoft SQL、または Oracle データベース インスタンス（永続的なチャット機能用）

例 20-5　メガクラスタで Cisco IM and Presence サービスを配置

これは、40,000 を超えるユーザやデバイスの配置が必要な場合のメガクラスタ配置の構成例です。

（注）　Unified CM サブスクライバ ペアが 5 つ以上必要なすべての配置は、配置前にシスコのメガクラスタ チームによって確認および承認される必要があります。メガクラスタの承認および確認プロセスの詳細については、https://wiki.cisco.com/display/CCM/Megacluster にある情報を参照してください。

IM and Presence の配置要件：

- 25,000 ユーザ IM and Presence VM 設定テンプレートを使用する 6 個のノード
- ハイ アベイラビリティ モードで 3 つのサブクラスタ サブスクライバ ペアとして分散されるノード

Unified CM の配置要件：

- 10,000 ユーザ Unified CM VM 設定テンプレートを使用する 19 個のノード
- 専用パブリッシャで配置される Unified CM
- 専用 TFTP1 サーバおよびバックアップ TFTP2 サーバ
- 8 個のサブスクライバ ペア仮想ノード
- インスタント メッセージのコンプライアンス準拠が必要
- ハイ アベイラビリティが必要

ハードウェア プラットフォーム：

- Unified CM 10,000 ユーザ VM 設定テンプレートおよび 25,000 ユーザ IM and Presence VM 設定テンプレート付きの Cisco UCS B シリーズ

例 20-6　単一の UCS B シリーズ サーバ上で複数の Unified CM クラスタに Cisco IM and Presence サービスを配置

配置要件

- 5 つの異なる Unified CM クラスタに属する 75,000 ユーザ
- インスタント メッセージのコンプライアンス準拠が必要
- ハイ アベイラビリティが必要

ハードウェアおよびソフトウェア プラットフォーム：

- 10 個の 15,000 ユーザ VM 設定フル UC テンプレート付きの Cisco UCS B シリーズ

展開

- 単一プラットフォーム UCS B シリーズに 5 つの Cisco IM and Presence サービス クラスタ（5 つの Unified CM クラスタそれぞれに 15,000 ユーザが付属）

オンプレミスの Cisco IM and Presence サービスのパフォーマンス

Cisco IM and Presence サービス クラスタは、シングルサーバとマルチサーバの両方の構成をサポートします。Cisco IM and Presence サービス クラスタによってサポートされる最大ユーザ数は、配置で使用されるプラットフォームによって異なります。たとえば、それぞれが独自のサブクラスタを構成する 3 つの 2,000 ユーザ VM 設定テンプレートで Cisco IM and Presence サービス クラスタを配置すると、合計 6,000 ユーザがサポートされます。Cisco IM and Presence サービス クラスタでサポートされるフル UC ユーザの最大数は 75,000 であり、クラスタ配置でサポートされるデバイスの最大数を超えることはありません。サポートされる IM 専用ユーザの最大数は 75,000 です。Cisco IM and Presence サービスのプラットフォーム要件、およびプラットフォームごとにサポートされる最大ユーザ数の詳細リストについては、次の Web サイトで入手可能なマニュアルを参照してください。

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html

Cisco IM and Presence サービスは仮想サーバ上で VM 設定テンプレートのみを使用した配置をサポートします。Cisco IM and Presence サービスでは物理サーバはサポートされません。

クラスタ内のすべての IM and Presence ノードに同一の VM 設定を使用することを推奨します。ただし、IM and Presence パブリッシャ ノードに使用される VM 設定が、同じクラスタ内のいずれかのサブスクライバ ノードに使用される VM 設定のキャパシティ以上であれば、キャパシティが異なる VM 設定をクラスタ内に混在させることができます。

同様のガイドラインが冗長性およびハイ アベイラビリティ モデルにも適用されます。クラスタ内の IM and Presence のスタンバイ/バックアップ仮想サブスクライバ ノードで使用する VM 設定は、IM and Presence パブリッシャまたはそれぞれのアクティブ/プライマリ サブスクライバの VM 設定以下である必要があります。

同じ IM and Presence クラスタ内に VM 設定を混在させる場合は、使用される各種 VM 設定によってパフォーマンスとキャパシティに影響が出る可能性があることを考慮してください。クラスタ全体のキャパシティは、最終的にクラスタ内の最小 VM 設定のキャパシティによって決まる場合があります。

（注）　IM and Presence と Unified CM を統合してもこれらが同じクラスタに属することはなく、2 つの別のクラスタに属します。

オンプレミスの Cisco IM and Presence サービス配置

Cisco IM and Presence サービスは、次のいずれかの構成で配置できます。

- シングルクラスタ配置（20-29 ページ）
- クラスタ間展開（20-31 ページ）
- WAN を介したクラスタリング（20-32 ページ）
- フェデレーション配置（20-39 ページ）

シングルクラスタ配置

図 20-11 に、Cisco IM and Presence サービス、LDAP サーバ、および Cisco Unified Communications Manager 間で基本的な機能に使用される通信プロトコルを示します。Cisco IM and Presence サービスの管理と設定の詳細については、次の Web サイトで入手可能な Cisco IM and Presence のインストール、管理、および設定に関するマニュアルを参照してください。

https://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

図 20-11　Cisco IM and Presence サービス コンポーネント間の相互作用

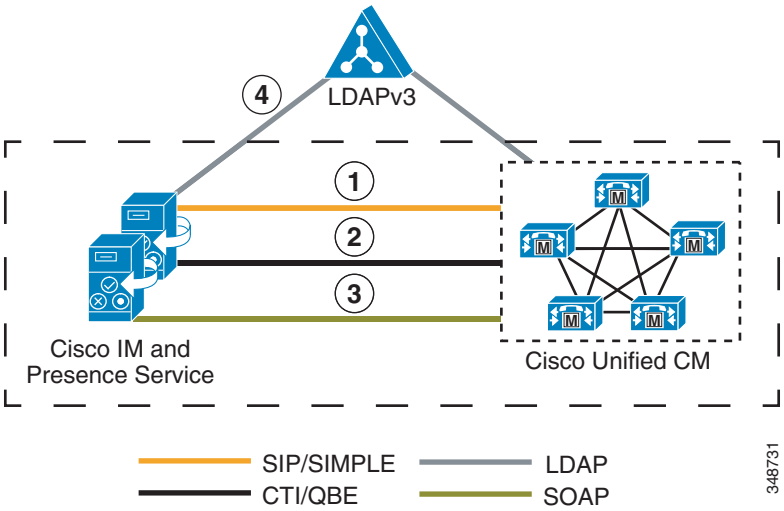


図 20-11 に、Cisco IM and Presence サービス コンポーネント間の次の相互作用を示します。

1. Cisco IM and Presence サービスと Unified CM 間の SIP 接続は、すべての電話機の状態のプレゼンス情報交換を処理します。

   Unified CM の設定では、Cisco IM and Presence サービスをアプリケーション サーバとして Unified CM に追加する必要があります。また Cisco IM and Presence サービスを指す SIP トランクが必要です。SIP トランクに設定するアドレスは、Cisco IM and Presence サービスに対して解決されるドメイン ネーム システム（DNS）サーバ（SRV）の完全修飾ドメイン名（FQDN）、または個別の Cisco IM and Presence サービスの IP アドレスです。Cisco IM and Presence サービスは、管理者が Cisco IM and Presence サービスの管理によってシステム トポロジ ページでノードを追加すると、Cisco Unified Communications Manager アプリケーション サーバ エントリの設定を AXL/SOAP で自動的に処理します。

   ネットワーク内の DNS の可用性が非常に高く、DNS SRV の利用が可能な場合、Cisco IM and Presence サービス パブリッシャとサブスクライバの DNS SRV FQDN を使用して、Unified CM 上に SIP トランクを設定します。また、Unified CM サブスクライバの DNS SRV FQDN を同等の重み付けで使用し、Cisco IM and Presence サービス上にプレゼンス ゲートウェイを設定します。この設定により、プレゼンス情報の交換に使用するすべてのサーバ間でプレゼンス メッセージングが均等に振り分けられます。

   DNS がハイ アベイラビリティでない場合、またはネットワーク内で信頼できるオプションでない場合は、IP アドレスを使用する。IP アドレスを使用すると、単一のサブスクライバが指されるので、プレゼンス メッセージング トラフィックを複数の Unified CM サブスクライバ間で均等に振り分けることはできません。

   Unified CM では、PUBLISH メソッド（SUBSCRIBE/NOTIFY ではなく）を設定し、Cisco IM and Presence サービスへの SIP トランク インターフェイス上で使用できるようにする IMP PUBLISH Trunk というサービス パラメータによって、通信をさらに簡素化し、使用帯域幅を削減します。IMP PUBLISH Trunk サービス パラメータを有効にした場合、ユーザをプライマリ内線だけでなく、ライン アピアランスと関連付ける必要があります。

2. Cisco IM and Presence サービスと Unified CM との間のコンピュータ テレフォニー インテグレーション Quick Buffer Encoding（CTI-QBE）接続は、Cisco IM and Presence サービスのプレゼンス対応ユーザが、Unified CM に登録済みの各自に関連付けられた電話機を制御するために使用するプロトコルです。この CTI 通信は、Cisco Jabber が Desk Phone モードで Click to Call を行う場合、または Microsoft Office Communicator が Microsoft Office Communications Server 2007 または Microsoft Lync によって Click to Call を行う場合に実行されます。

   a. Unified CM の設定では、ユーザを CTI Enabled グループに関連付け、そのユーザに割り当てられたプライマリ内線で CTI 制御を有効にする必要があります（[Directory Number] ページのチェックボックス）。また CTI Manager サービスも、Cisco IM and Presence サービス パブリッシャおよびサブスクライバとの通信に使用される各 Unified CM サブスクライバ上でアクティブにする必要があります。Microsoft Office Communications Server 2007 または Microsoft Lync との統合では、Unified CM で、CTI Enabled グループと役割を使用して、アプリケーション ユーザを設定する必要があります。

   b. Cisco Jabber と連携して使用するための Cisco IM and Presence サービスの CTI 設定（CTI サーバおよびプロファイル）は、Unified CM とのデータベースの同期時に自動的に作成されます。すべての Cisco Jabber CTI 通信は、Cisco IM and Presence サービスを介さずに、直接 Unified CM と実行されます。

Microsoft Office Communications Server 2007 または Microsoft Lync と連携して使用するための Cisco IM and Presence サービスの CTI 設定（Desktop Control Gateway）では、Desktop Control Gateway のアドレス（Cisco Unified Communications Manager のアドレス）とプロバイダー（Unified CM で以前に設定されたアプリケーション ユーザ）を設定する必要があります。スケーラビリティを拡大させるため、最大 8 個の Cisco Unified Communications Manager アドレスをプロビジョンできます。Cisco IM and Presence サービスの Desktop Control Gateway の設定で使用できるのは、IP アドレスのみです。管理者は、Cisco Unified Communications Manager アドレスの設定および割り当てが、ロード バランシングのために均等に分散されるようにする必要があります。

3. AXL/SOAP インターフェイスは、Unified CM からのデータベースの同期を処理して、Cisco IM and Presence サービス データベースにデータを入力します。
   a. Unified CM では、その他の設定は必要ありません。
   b. Cisco IM and Presence サービスのセキュリティ設定では、AXL 設定内の Unified CM AXL アカウントのユーザとパスワードを設定する必要があります。

      Sync Agent サービス パラメータである [ユーザ割り当て（User Assignment）] は、デフォルトで [平衡化（balanced）] に設定され、すべてのユーザが Cisco IM and Presence サービス クラスタ内のすべてのサーバに均等にロードバランスされます。管理者は、[ユーザ割り当て（User Assignment）] サービス パラメータを [なし（None）] に変更して、Cisco IM and Presence サービス クラスタ内の特定のサーバに手動でユーザを割り当てることができます。

4. LDAP インターフェイスは、ユーザの LDAP 認証に使用されます。LDAP 同期と認証の詳細については、ディレクトリ統合とアイデンティティ管理（16-1 ページ）の章を参照してください。

   Unified CM は、手動設定または LDAP からの直接同期によるすべてのユーザ エントリを処理し、Cisco IM and Presence サービスは Unified CM からすべてのユーザ情報を同期します。ユーザが Cisco IM and Presence サービスにログインし、LDAP 認証が Unified CM で有効になっている場合、Cisco IM and Presence サービスは LDAP に直接アクセスし、Bind 操作を使用してユーザを認証します。

   Microsoft Active Directory を使用する場合は、パラメータの選択を慎重に考慮してください。大規模な Active Directory 実装が存在し、設定でドメイン コントローラが使用されている場合、Cisco IM and Presence サービスで十分なパフォーマンスが得られないことがあります。Active Directory の応答時間を改善するために、場合によっては、ドメイン コントローラをグローバル カタログに追加し、LDAP ポートを 3268 に設定する必要があります。

クラスタ間展開

前の項までは、単一の Cisco IM and Presence サービス クラスタが、単一の Unified CM クラスタと通信する配置トポロジについて説明しました。しかし単一のクラスタ内だけの通信では、プレゼンスやインスタント メッセージングの機能には限りがあります。そこで、プレゼンスとインスタント メッセージングの能力と機能を拡張できるよう、これらのスタンドアロンのクラスタにピア関係を設定することで、同じドメイン内の複数のクラスタ間で通信できるようになります。この機能により、1 つのクラスタ内のユーザが、同じドメイン内の異なるクラスタにいるユーザと通信したり、プレゼンスをサブスクライブしたりできます。

フルメッシュのプレゼンス トポロジを作成するには、それぞれの Cisco IM and Presence サービス クラスタと、同じドメイン内の他のそれぞれの Cisco IM and Presence サービス クラスタとの間に、個別のピア関係が設定されている必要があります。このクラスタ間ピアに設定されているアドレスは、リモートの Cisco IM and Presence サービス クラスタ サーバに対して解決される DNS FQDN、または単純に Cisco IM and Presence サービス クラスタ サーバの IP アドレスです。

各 Cisco IM and Presence サービス クラスタ間のインターフェイスには、AXL/SOAP インターフェイスとシグナリング プロトコル インターフェイス（SIP または XMPP）の 2 つが使用されます。IM and Presence サービス クラスタのパブリッシャ専用サーバ間の AXL/SOAP インターフェイスはホーム クラスタ アソシエーション用にユーザ情報の同期を処理しますが、これは完全なユーザ同期ではありません。シグナリング プロトコル インターフェイス（SIP または XMPP）は、配置内のすべてのサーバ間でフルメッシュです。これは、サブスクリプション トラフィックと通知トラフィックを処理し、同じドメイン内のリモートの Cisco IM and Presence サービス クラスタでユーザが検出されると、URI のホスト部分を書き換えてから転送します。

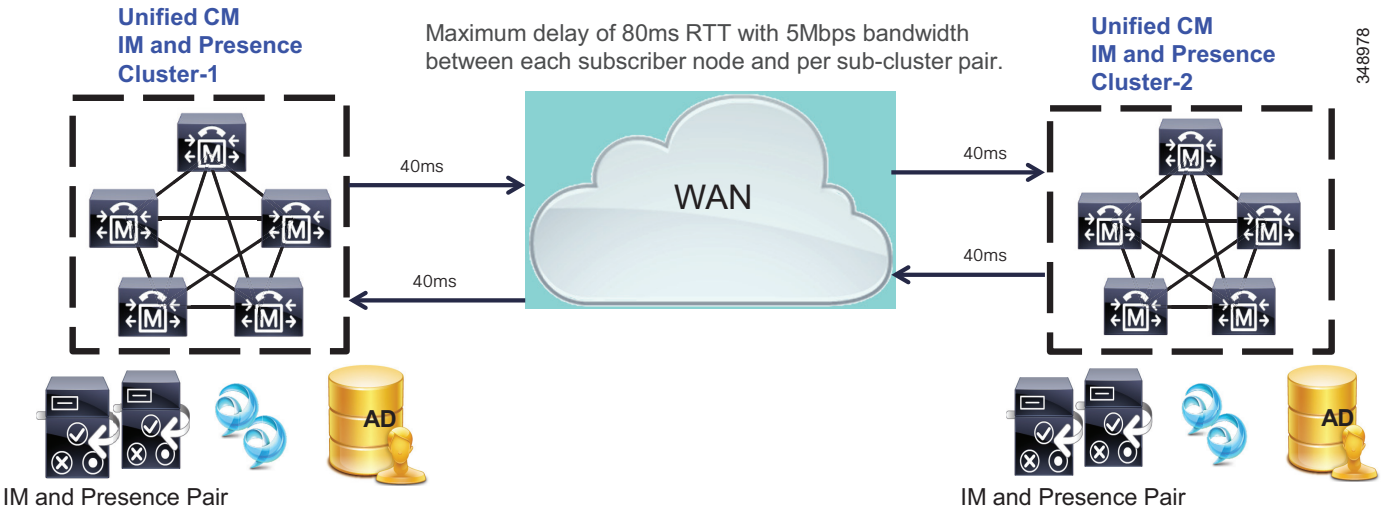
WAN を介したクラスタリング

Cisco IM and Presence サービス クラスタは、ワイド エリア ネットワーク（WAN）を介して配置されたサブクラスタのノードの 1 つを使用して配置できます。これにより、サイトをまたがるノード間でサブクラスタの地理的冗長性とユーザのハイ アベイラビリティが実現します。次のガイドラインは、Cisco IM and Presence サービスの配置と WAN を介したクラスタリングの計画時に使用する必要があります。

データセンターの地理的冗長性とリモート フェールオーバー

Cisco IM and Presence サービス クラスタは、単一サブクラスタ トポロジで 2 つのサイト間に配置できます。このトポロジでは、サブクラスタの一方のサーバが 1 つの地理的サイトに置かれ、サブクラスタの他方のサーバが別のサイトに置かれます。この配置では、5 Mbps 以上の帯域幅を確保し、遅延を 80 ms ラウンド トリップ時間（RTT）以下に抑え、TCP によるメソッド イベント ルーティングを行う必要があります（図 20-12 を参照）。

図 20-12　クラスタ内帯域幅と遅延



ハイ アベイラビリティと規模

Cisco IM and Presence サービスのハイ アベイラビリティにより、サブクラスタ内の 1 つのノードのユーザは、サブクラスタ内の別のノードに自動的にフェールオーバーされます。最大 2 つのノードで構成される Cisco IM and Presence サービス サブクラスタでは、リモート フェールオーバーは基本的に 2 つのサイト間（各ノードに 1 つのサイト）で行われます。スケーラブルなハイ アベイラビリティの Cisco IM and Presence サービス クラスタでは、最大 3 つのサブクラスタを構成できます。したがって、スケーラブルなハイ アベイラビリティのリモート フェールオーバー トポロジは、次のような 2 つのサイトで構成されます。

- サイト A：サブクラスタ 1 ノード A、サブクラスタ 2 ノード A、およびサブクラスタ 3 ノード A
- サイト B：サブクラスタ 1 ノード B、サブクラスタ 2 ノード B、およびサブクラスタ 3 ノード B

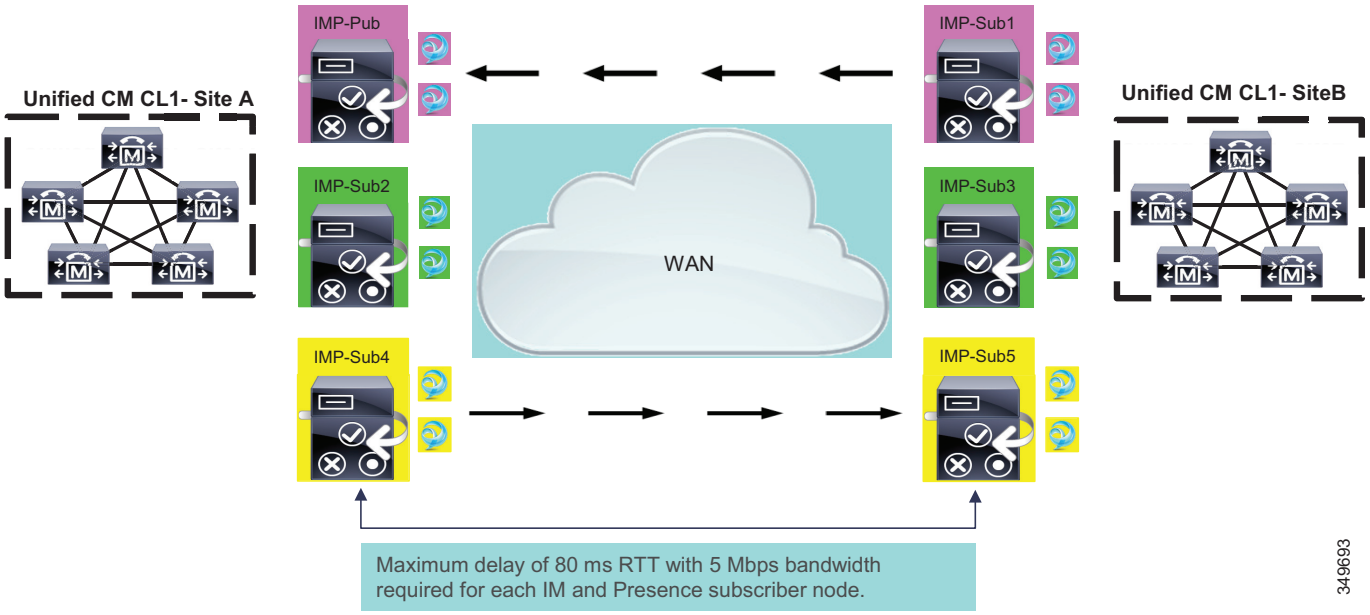
この配置では、1 つのサブクラスタごとに 5 Mbps 以上の帯域幅を確保し、遅延を 80 ms ラウンドトリップ時間（RTT）以下に抑え、TCP によるメソッド イベント ルーティングを行う必要があります。この配置に追加される新しい各サブクラスタには、データベースと状態の複製を処理するために、さらに 5 Mbps の専用帯域幅が必要です。

スプリット サブクラスタ モデルでは、サブクラスタ ペアが WAN を介して分割され、2 つの別々の場所に配置されます。スプリット サブクラスタ モデルは、6 箇所に別々に配置された最大 6 つのノードをサポートします。これは、帯域幅と遅延の要件が満たされ、最大ラウンドトリップ時間（RTT）が 80 ms で 6 つの各ノードの帯域幅が 5 Mbps であると想定した場合です。

スプリット サブクラスタ配置には、次の要件があります。

- Unified CM パブリッシャおよび IM and Presence パブリッシャは、同じ WAN 側に存在する必要があります。この要件が満たされないと、アップグレード（特に更新（デュアル）アップグレード）で問題が発生する可能性があります。
- すべての IM and Presence ノードには 5 Mbps 以上の帯域幅が必要であり、データベースの同期用にクラスタにはさらに 5 Mbps が必要です。
- 各 IM and Presence ノードの RTT 遅延は 80 ms 以下である必要があります。
- すべてのユーザをすべてのスプリット クラスタ ノードに均等に分散する必要があります（図 20-13 を参照）。たとえば、サブクラスタが 15,000 ユーザをサポートすると想定した場合、スプリット サブクラスタの各ノードは 15,000 ユーザ VM 設定テンプレートで 7,500 をサポートします。

図 20-13　　WAN を介して分割された IM and Presence サブクラスタ



ローカル フェールオーバー

2 つのサイト間の Cisco IM and Presence サービス クラスタ配置では、1 つのサイトごとに 1 つのサブクラスタ トポロジ（単一ノードまたはハイ アベイラビリティ構成のデュアル ノード）を構成することもできます。この場合、一方のサブクラスタを 1 つの地理的サイトに置き、他方のサブクラスタを別の地理的サイトに置きます。このトポロジにより、ユーザは、異なるサイトまたは場所にフェールオーバーせずに、（ハイ アベイラビリティまたはハイ アベイラビリティでない）ローカル サイトに残ることができます。この配置では、それぞれのサイトの各サブクラスタ間に 5 Mbps 以上の専用帯域幅を確保し、遅延を 80 ms ラウンドトリップ時間（RTT）以下に抑え、TCP によるメソッド イベント ルーティングを行う必要があります。

帯域幅と遅延に関する考慮事項

WAN を介してノードが分割されたトポロジを持つ Cisco IM and Presence サービス クラスタでは、ユーザのクライアント内の連絡先数が、帯域幅の要件や配置の基準に影響を及ぼす可能性があります。Cisco IM and Presence サービスのクラスタ内およびクラスタ間で生成されるトラフィックは、プレゼンス ユーザ プロファイルの特性や配置に必要な帯域幅に直接関係します。帯域幅が小さい（10 Mbps 以下）環境のクライアントでは、リモート連絡先を 25 % 以下にすることを推奨します。最大ラウンドトリップ遅延は、常に 80 ms 以下にする必要があります。

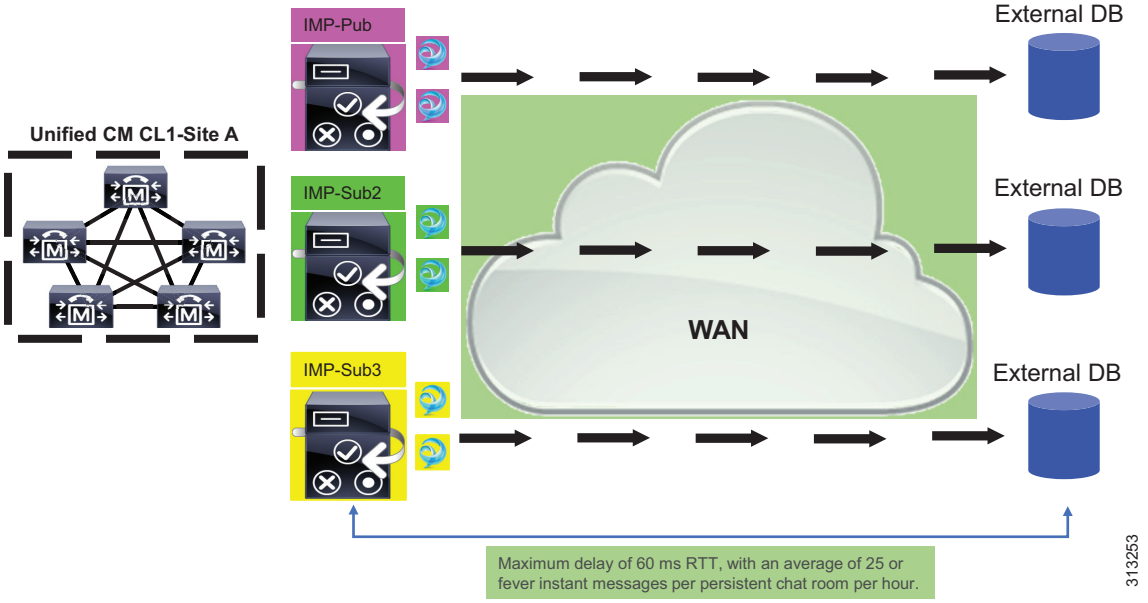
永続的なチャットとコンプライアンス ロギングに関する考慮事項

Cisco IM and Presence サービスが永続的なチャット、メッセージ アーカイブ、またはコンプライアンス ロギングに対して有効になっており、サブクラスタが WAN を介して分割されている場合は、外部データベース サーバをそれが関連付けられた Cisco IM and Presence サービス サブスクライバ ノードと同じ WAN 側に配置することをお勧めします。

単一サーバで複数のデータベース インスタンスをサポートできる能力と外部データベース サーバを関連する IM and Presence ノードと同じ WAN 側に配置するという推奨事項を考慮して、Cisco IM and Presence サービス クラスタが WAN を介して分割されている場合は、ベスト プラクティスとして 2 つの外部データベース サーバの展開をお勧めします。

(注)　これは、同じデータセンター内に配置する外部データベース サーバと関連する IM and Presence ノードに対する要件ではありません。ただし、外部データベース サーバと IM and Presence サブスクライバ ノード間の最大サポート遅延は 60 ms ラウンド トリップ時間（各方向に 30 ms）を超えないようにする必要があり、最小帯域幅割り当ては Cisco IM and Presence サービスに関する WAN 経由のクラスタリング要件を満たしている必要があります。また、常設チャット ルームあたりのインスタント メッセージの平均数は 1 時間あたり 25 件を超えないようにする必要があります。（図 20-14 を参照）。

図 20-14　WAN 経由の外部データベースを使用した永続的なチャット



(注)　WAN 経由で外部データベースを展開する場合や高可用性が必要な場合は Oracle Database 12c を使用することをお勧めします。

集中型 IM and Presence の導入

集中型 IM and Presence は、複数のリモート Cisco Unified CM の音声クラスタとビデオ クラスタにプレゼンス サービスを提供できます。集中型導入では、IM and Presence サービスがリモート Unified CM クラスタ上のすべてのユーザに対するすべてのプレゼンス関連サービスを管理し、各リモート Unified CM クラスタが個別のユーザの音声とビデオのニーズを処理します。

集中型 IM and Presence モデルは、複数の場所に Unified CM クラスタを分散させるため、すべての場所に IM and Presence クラスタを展開する必要のない大企業向けのオプションを提供します。つまり、1 つの集中型 IM and Presence クラスタがあれば、複数のリモート Unified CM クラスタに対するプレゼンス サービスを賄うことができます。

場所の数は多いものの、それぞれの場所のユーザ数は非常に少ない導入では、このモデルから多くの恩恵を受けることができます。たとえば、ある病院が 50 か所にいる 100 人ずつのユーザに音声、ビデオ、プレゼンス サービスを提供しているとします。この場合は、Unified CM の 50 クラスタと IM and Presence の 50 クラスタを展開するのは現実的ではありません。それよりも、1 つの集中型 IM and Presence クラスタで 50 台のリモート Unified CM クラスタを制御する方が効率的で簡単ですし、仮想サーバを減らすことでコストを大幅に削減できます。

集中型 IM and Presence クラスタは、15k/25k ユーザ IM and Presence VM テンプレートを使用して展開する必要があります。集中型クラスタ用の Unified CM パブリッシャは、10k ユーザ Unified CM VM テンプレートを使用して展開する必要があります。（図 20-15 を参照）。

（注）　40,000 台を超えるクライアントまたはデバイスを展開する場合の集中型導入設計は、シスコのメガクラスタ レビュー プロセスを通して審査および承認される必要があります。

集中型 IM and Presence 導入の詳細については、次の場所にある『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』に関するガイドの最新版を参照してください。

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

図 20-15　　集中型 IM and Presence の導入

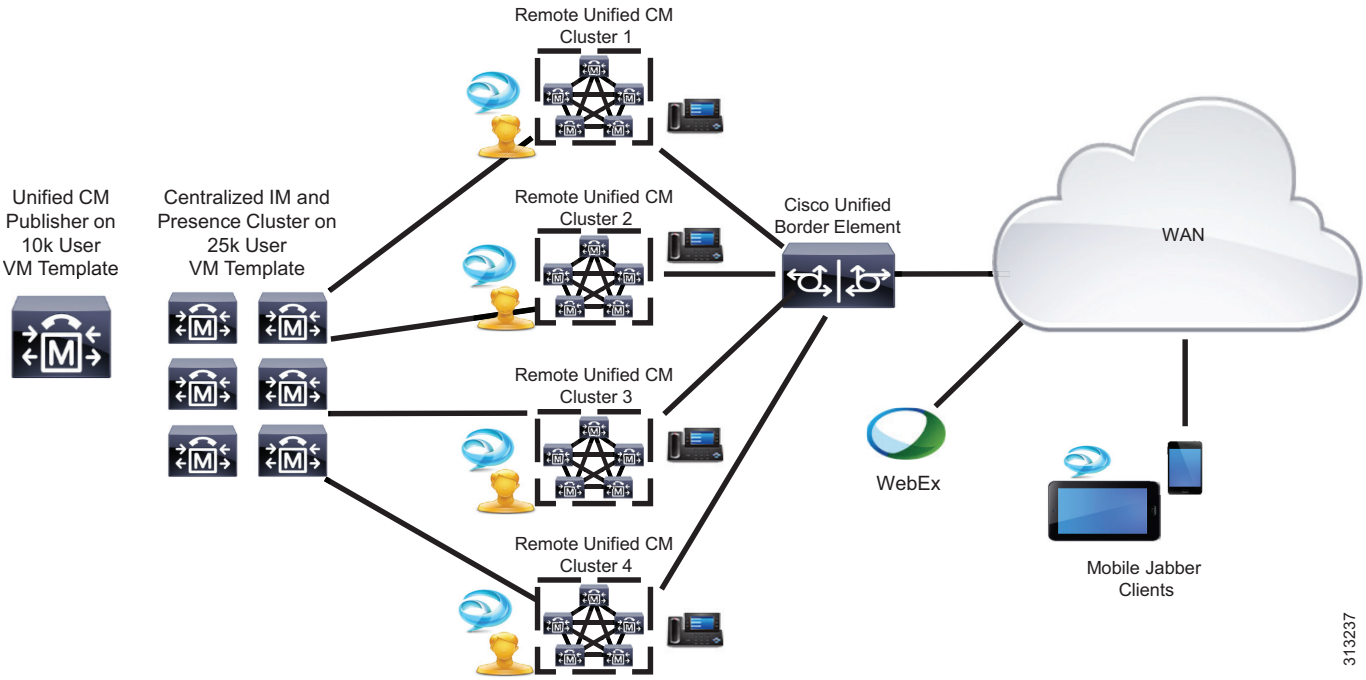


図 20-16 に、シングル サインオン（SSO）を使用しない場合の集中型 IM and Presence の次のログイン フロー ステップを示します。

- ステップ 1 ～ 2：DNS に問い合わせて、SRV レコードを取得します。
- ステップ 3 ～ 4：UDS に問い合わせて、ホーム Unified CM クラスタを取得します。
- ステップ 5 ～ 8：LDAP 認証を介して Unified CM クラスタからアクセス トークンとリフレッシュ トークンを取得します。
- ステップ 9：[UC サービス プロファイル（UC Service Profile）] -> [IM and Presence プロファイル（IM & Presence Profile）] を読んで、IM and Presence ノード情報を入手します。
- ステップ 10：Jabber クライアントが SOAP インターフェイスと XMPP インターフェイスを介して同じアクセス トークンを使用して IM and Presence クラスタに登録します。
- ステップ 11：IP Multimedia Subsystem（IMS）API が AuthZ サービスを呼び出してトークンを検証し、その応答が Jabber クライアントに送り返されます。

（注）　リモート Cisco Unified CM クラスタ上のサービス パラメータ [Unified CM IM and Presence でのユーザの有効化（Enable User for Unified CM IM and Presence）] は無効（オフ）にする必要があります。

図 20-16　シングル サインオン（SSO）を使用しない集中型 IM and Presence ログイン フロー

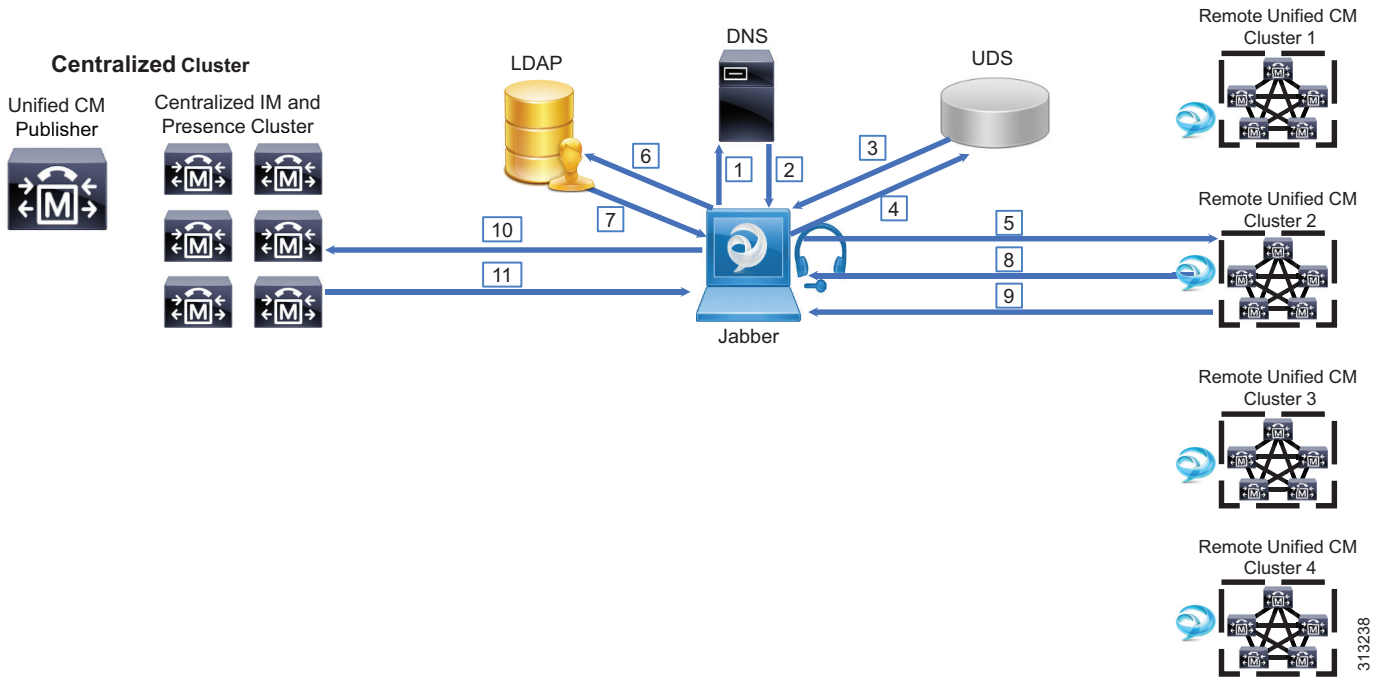


図 20-17 に、シングル サインオン（SSO）を使用する場合の集中型 IM and Presence の次のログイン フロー ステップを示します。

- ステップ 1 ～ 2：DNS に問い合わせて、SRV レコードを取得します。
- ステップ 3 ～ 4：UDS に問い合わせて、ホーム Unified CM クラスタを取得します。
- ステップ 5 ～ 8：ID プロバイダー（IDP）認証を介して Unified CM クラスタからアクセス トークンとリフレッシュ トークンを取得します。
- ステップ 9：[UC サービス プロファイル（UC Service Profile）] -> [IM and Presence プロファイル（IM & Presence Profile）] を読んで、IM and Presence ノード情報を入手します。
- ステップ 10：Jabber クライアントが SOAP インターフェイスと XMPP インターフェイスを介して同じアクセス トークンを使用して IM and Presence クラスタに登録します。
- ステップ 11：IP Multimedia Subsystem（IMS）API が AuthZ サービスを呼び出してトークンを検証し、その応答が Jabber クライアントに送り返されます。

（注）　リモート Cisco Unified CM クラスタ上のサービス パラメータ [Unified CM IM and Presence でのユーザの有効化（Enable User for Unified CM IM and Presence）] は無効（オフ）にする必要があります。

図 20-17　シングル サインオン（SSO）を使用した集中型 IM and Presence ログイン フロー

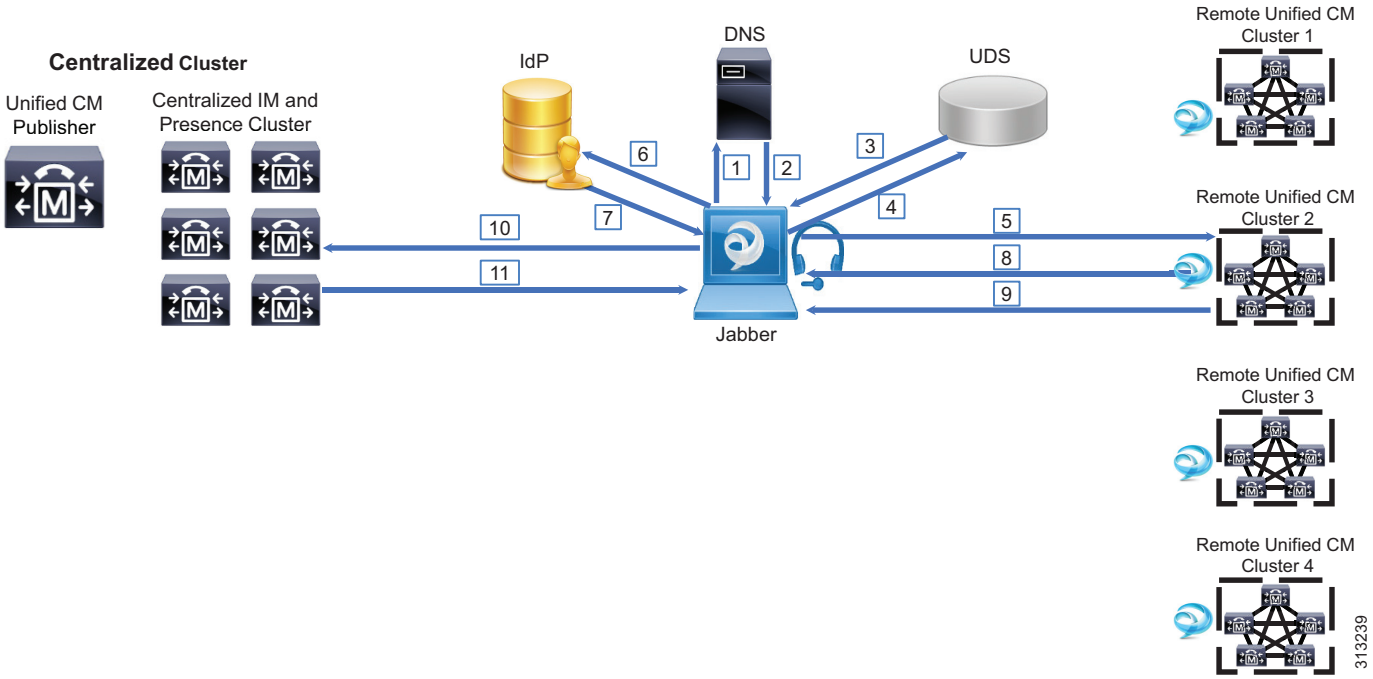
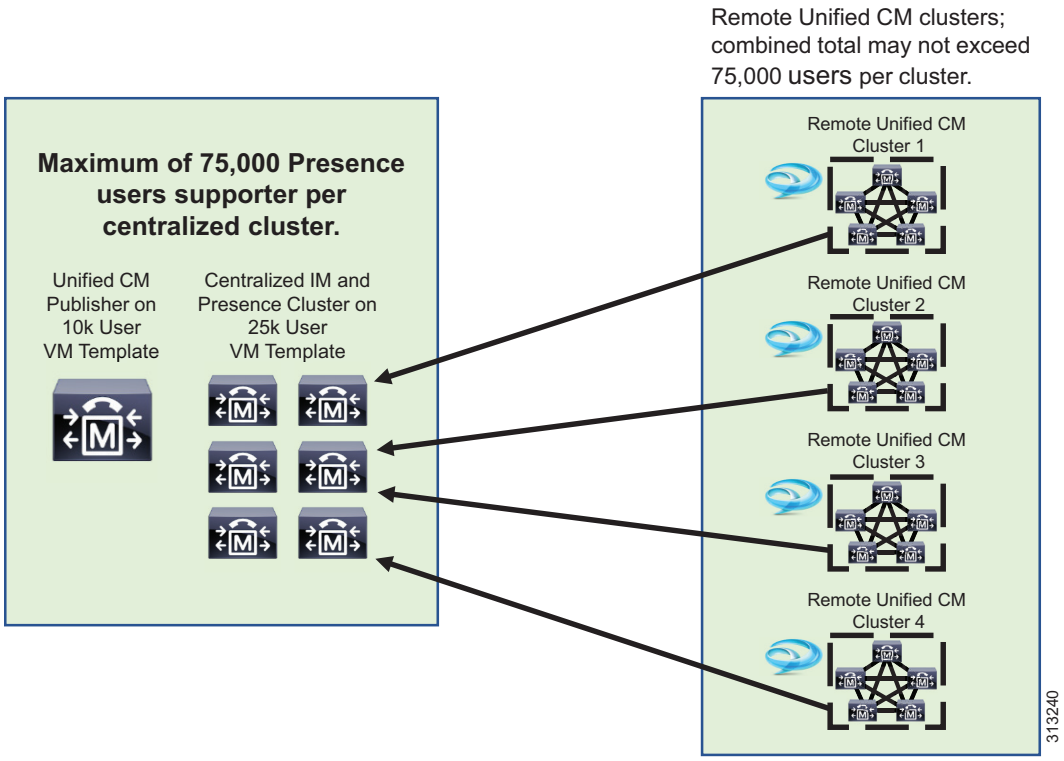


図 20-18　集中型 IM and Presence のサポート ユーザの最大数



フェデレーション配置

Cisco IM and Presence サービスは企業間通信に対応するため、異なるドメイン間でプレゼンス情報やインスタント メッセージング通信を共有できるドメイン間フェデレーションを搭載しています。ドメイン間フェデレーションの構築には、明示的な DNS ドメインを設定し、さらに DMZ にセキュリティ アプライアンス（Cisco Adaptive Security Appliance）を置いて、フェデレーション接続を企業で終端させる必要があります。

マルチドメイン サポート

IM and Presence サービスでは、フェデレーションに複数のドメインを設定することができます。DirectoryURI を使用している場合、ドメインはシステムによって自動的に検出されます。または、管理者が手動でドメインを追加することもできます。フェデレーション配置に複数のドメインが含まれる場合、DNS SRV レコードを各電子メール ドメインに対してパブリッシュする必要があります。各 DNS SRV レコードは、XMPP フェデレーションがすべての XMPP フェデレーション ノードのリストで、SIP フェデレーションがルーティング IM and Presence ノードの Public FQDN である一連の結果と同一に解決される必要があります。

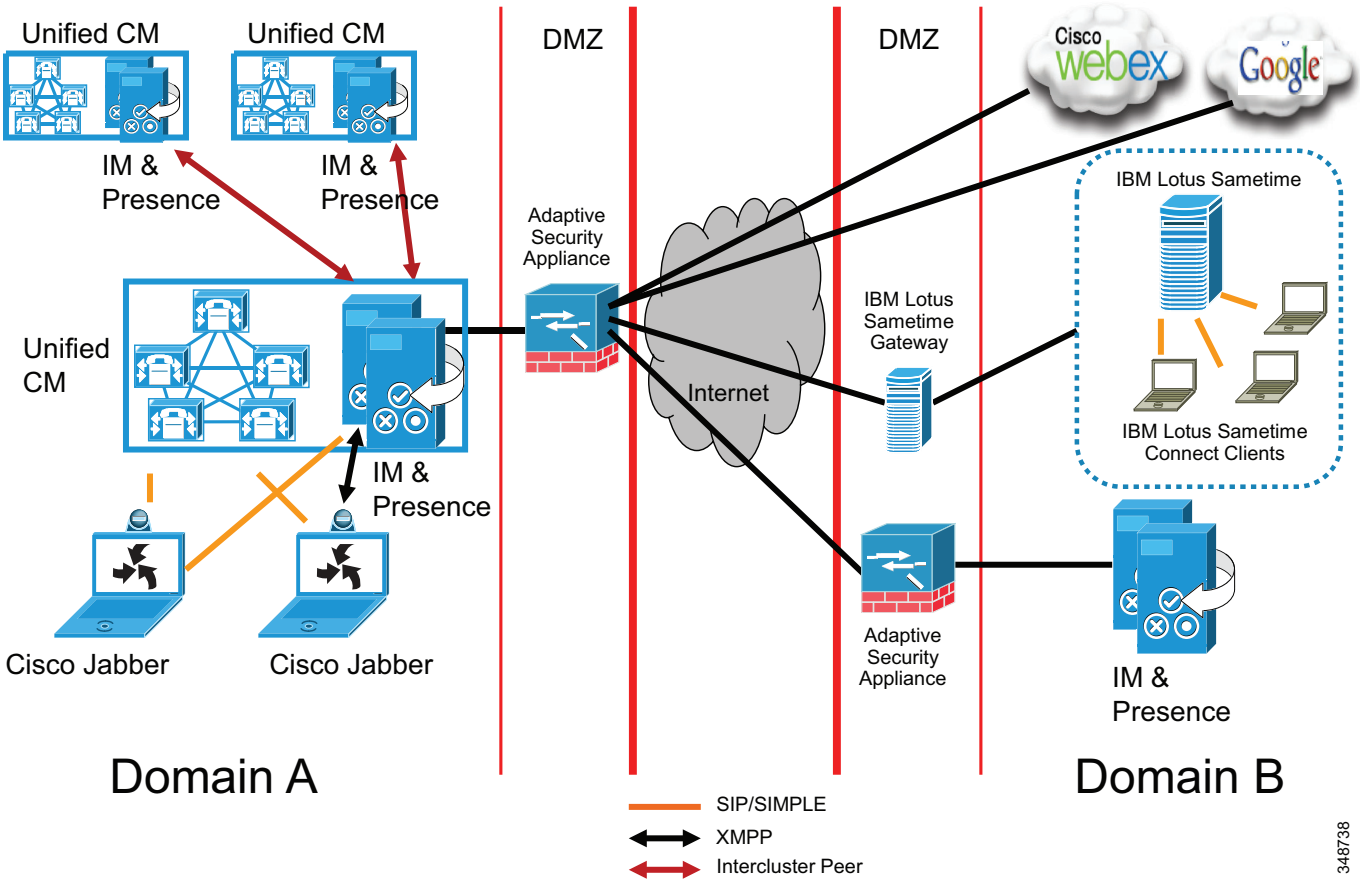
また、複数の電子メール ドメインを設定したフェデレーションでは、セキュリティ証明書 cup-xmpp（XMPP クライアントに提示される証明書）および cup-xmpp-s2s（フェデレーション システムに提示される証明書）の再生成が必要です。両方の証明書で、すべてのドメインを Subject Alt Name（SAN）のエントリとして含める必要があります。手動管理設定で、管理者はドメインを事前入力するオプションを使用できるため、新しいドメインが自動的に検出されるたびに証明書を再生成する必要はありません。

フェデレーション ドメインがすべて同じ信頼性境界内に存在する場合（配置では単一データセンター内にすべてのコンポーネントが含まれます）は、Adaptive Security Appliance を使用する必要がありません。ドメイン間フェデレーションの詳細については、次の Web サイトで入手可能な『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』の最新バージョンを参照してください。

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

図 20-19 に、ドメイン A とドメイン B という 2 つの異なるドメイン間の基本的なドメイン間フェデレーション配置を示します。DMZ の Adaptive Security Appliance（ASA）は社内への境界として使用されます。XMPP トラフィックはそのまま通過しますが、SIP トラフィックは検査されます。フェデレーションのすべての着信トラフィックは、フェデレーション ノードとして有効化された Cisco IM and Presence サービス経由でルーティングされ、内部ではユーザがいるクラスタの適切なサーバにルーティングされます。クラスタ間配置では、クラスタ間ピアはトラフィックをドメイン内の適切なホーム クラスタに伝達します。フェデレーションのすべての発信トラフィックは、XMPP フェデレーションが有効化された IM and Presence サービス クラスタ内の任意のノードを経由して外部に誘導されます。大企業での配置においては、複数のノードをフェデレーション ノードとして有効化できます。その場合、各要求は、DNS SRV ルックアップから返されるデータのラウンドロビン実装に基づいてルーティングされます。

図 20-19　IM and Presence サービス XMPP フェデレーション（ドメイン間）



また、Cisco IM and Presence サービスでは、Microsoft と AOL とのドメイン間フェデレーションを行えるように SIP からの設定も提供されます（図 20-20 を参照）。Cisco IM and Presence サービスは、Microsoft Lync Server とのドメイン間フェデレーションによって、基本プレゼンス（応対可能、不在、ビジー、オフライン）とポイントツーポイントのインスタント メッセージングを提供します。高度なプレゼンス機能（通話中、会議中、休暇中など）や高度なインスタント メッセージング機能はサポートされていません。Cisco IM and Presence サービスによる AOL とのドメイン間フェデレーションにより、AOL パブリック コミュニティ（aim.com、aol.com）のユーザ、AOL によりホストされたドメインのユーザ、および AOL とのフェデレーションを行う遠端企業のユーザ（つまり、AOL はクリアリング ハウスとして使用されます）とのフェデレーションが可能になります。

（注）　Cisco IM and Presence サービスでは、AOL ネットワーク（ホストされたネットワークとパブリック コミュニティの両方から構成されます）の各ドメインに対して SIP フェデレーション（ドメイン間と AOL）を設定する必要があります。ホストされた一意のドメインをそれぞれ設定する必要がありますが、AOL ネットワークではユーザを user@aol.com または user@aim.com と指定できるため、単一の aol.com パブリック コミュニティだけを指定する必要があります。

図 20-20　IM and Presence サービス SIP フェデレーション（ドメイン間）

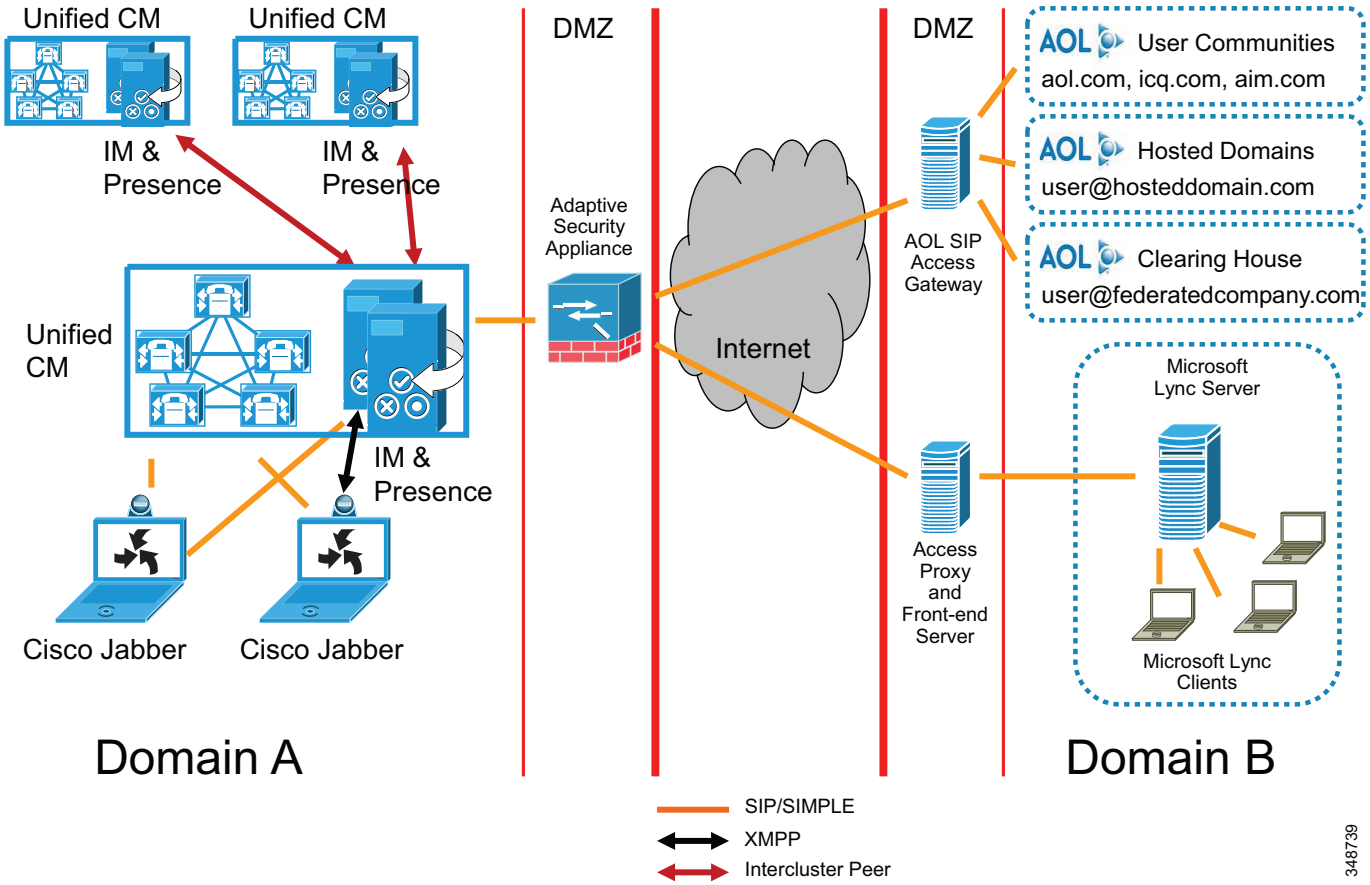


表 20-2 に、Cisco IM and Presence サービスと Microsoft Lync Server との間のステータスのマッピングを示します。

表 20-2　プレゼンス ステータスのマッピング

シスコでのステータス	シスコのランプの色	Microsoft Lync Server に対するステータス	AOL に対するステータス
サイレント	赤	ビジー	退席中
ビジー	黄	ビジー	退席中
電話中	黄	ビジー	退席中
会議中	黄	ビジー	退席中
退席中	黄	退席中	退席中
応対可	グリーン	応対可	応対可
応対不可/オフライン	グレー	オフライン	オフライン

（注） Cisco IM and Presence サービスは、他のドメインが、DNS SRV によって Cisco IM and Presence サービスを検出できるように、ドメインに関する DNS SRV レコードをパブリッシュする必要があります（SIP、XMPP、および各テキスト会議ノード）。Microsoft Lync Server 配置では、Cisco IM and Presence サービスが Access Edge サーバ上の Public IM Provider として設定されているので、このようなパブリッシュが必要です。Cisco IM and Presence サービスが DNS SRV を使用している Microsoft ドメインを検出できない場合、Cisco IM and Presence サービスで外部ドメインのスタティック ルートを設定する必要があります。

Cisco IM and Presence サービスの SIP フェデレーション配置は、Adaptive Security Appliance と Cisco IM and Presence サービス間にロード バランサを使用することで、冗長性のある構成にできます。または、冗長構成の Adaptive Security Appliance によって冗長性を実現することもできます。XMPP フェデレーションの場合は、DNS SRV レコードを使用して冗長性を実現できます。

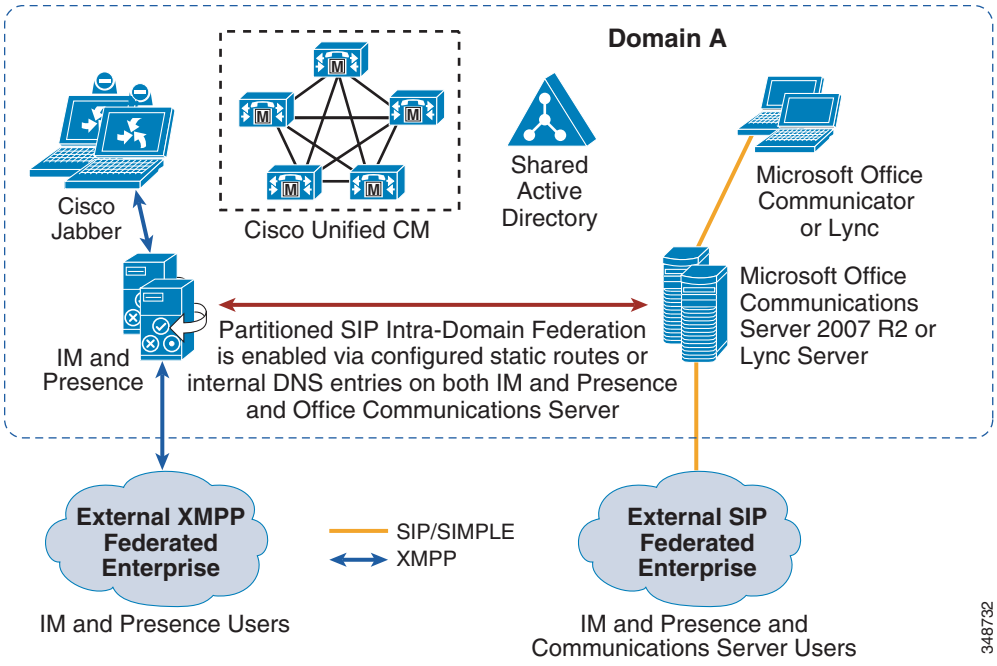
フェデレーション配置に関するその他の設定および配置上の考慮事項については、次の Web サイトで入手可能な『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』の最新バージョンを参照してください。

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

図 20-21 に示すパーティション化されたドメイン内フェデレーション配置はセカンダリ オプションであり、これにより、Cisco IM and Presence サービスと Microsoft Lync Server は、同じプレゼンス ドメイン内でプレゼンスおよびインスタント メッセージングをフェデレーションできます。ユーザは、単一プレゼンス ドメイン内の両方の配置にわたってパーティション化され、Cisco IM and Presence サービスまたは Microsoft Lync Server のいずれかでライセンス供与されます。

（注） シスコ プラットフォームと Microsoft プラットフォームの両方で同時に特定のユーザへのライセンス供与を行うことはできません。

図 20-21　Cisco IM and Presence サービス ドメイン内フェデレーション



シスコ プラットフォームと Microsoft プラットフォーム間のパーティション化されたドメイン内フェデレーションは、SIP/SIMPLE プロトコルに基づいており、Microsoft の Cisco IM and Presence サービス ドメイン間フェデレーション サポートでサポートされているため、基本プレゼンスおよびインスタント メッセージング交換が可能になります。高度なプレゼンスおよびグループ チャット機能は、パーティション化されたドメイン内プレゼンス フェデレーションではサポートされていません。

ドメイン間フェデレーションおよびパーティション化されたドメイン内フェデレーションは、次の条件で同時にサポートされます。

- XMPP フェデレーションは Cisco IM and Presence サービス配置で有効化できますが、Cisco IM and Presence サービスのライセンスされたユーザのみが使用できます。
- SIP フェデレーションは Cisco IM and Presence サービス、Microsoft Office Communications Server 2007 R2、または Lync Server のいずれかで有効化することができます。ただし、シスコと Microsoft の両方のユーザが使用できる SIP フェデレーションの場合は、Microsoft Office Communications Server 2007 R2 または Lync Server で有効にする必要があります。
- Microsoft Lync または Office Communications Server との SIP/SIMPLE のドメイン間フェデレーションが、パーティション化されたドメイン内フェデレーションと並行して必要な場合は、外部フェデレーションを管理するように Microsoft Office Communications Server または Lync Server を設定することができます。Cisco IM and Presence サービス管理は、外部ドメインの Microsoft 環境へのスタティック ルートを使用して設定する必要があります。また、Cisco IM and Presence サービスは SIP フェデレーションを管理することができ、Microsoft Lync または Office Communications Server は XMPP フェデレーションを管理することができます。

オンプレミスの Cisco IM and Presence サービスの Jabber 用 SAML SSO

（注）　SAML SSO 配置でサポートされるエンドポイントは Cisco Jabber です。

Security Assertion Markup Language シングル サインオン（SAML SSO）機能は、コラボレーション ソリューション内の複数のアプリケーションに何度もログインする必要をなくすことで、エンド ユーザ エクスペリエンスを向上させます。

SAML SSO は、Unified CM、Cisco Unity Connection、IM and Presence、Jabber クライアントなどの複数の Unified Communications アプリケーション間でエンド ユーザのクレデンシャルと関連情報を使用するセキュアなメカニズムを提供します。

SAML SSO 機能が正常に動作するよう、認証および各ユーザに関連する 2 台以上のデバイスを必要とする 5 つ以上のサービスを各ユーザが所有すると仮定して、各クラスタのユーザ数に合わせてネットワーク アーキテクチャが拡張されていることを確認します。複数の Unified Communications アプリケーション間の配置で、Cisco Jabber クライアントが正常にログインするには、すべての SAML 要求が IdP によって認証される必要があります。

（注）　SSO は、SAML および OAuth のみを使用する Unified Communications サービスでサポートされます。

SAML SSO を使用する Cisco Jabber は、ログイン時にパフォーマンスに影響を及ぼします。5,000 ユーザの現在の最大ログイン レートは 30 分以内です。これは、デバイスとユーザがすべてのノードに均等に分散されていて、Cisco Jabber がソフトフォン モードである場合です。

Cisco Jabber は、SAML SSO をサポートする IM and Presence 配置で唯一サポートされているクライアント/エンドポイントです。

サイジング情報と例については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章の SAML SSO Cisco Jabber クライアント（25-21 ページ）の項を参照してください。

オンプレミスの Cisco IM and Presence サービスの企業インスタント メッセージング

Cisco IM and Presence サービスには、Extensible Communications Platform（XCP）でサポートされている企業インスタント メッセージング機能が組み込まれています。また、マルチデバイス ユーザ エクスペリエンスのサポートを向上させるためにいくつかの変更を行うことができます。Cisco IM and Presence サービスでは、XCP インスタント メッセージング ルーティング アーキテクチャが変更され、最初のインスタント メッセージが、既存の XCP インストールで行われるように最も優先順位の高いデバイスにルーティングされるのではなく、ユーザの負ではない優先順位のすべてのログイン済みデバイスにルーティングされます。Cisco IM and Presence サービス SIP クライアントおよび XMPP クライアント間のポイントツーポイントのインスタント メッセージングの下位互換性サポートは、IM 内部ゲートウェイ機能によって提供されます。

IM and Presence サービスは、アドホック チャット ルームと永続的なチャット ルームの両方の IM 交換をサポートします。デフォルトで、IM and Presence サービスの Text Conference（TC）コンポーネントは、アドホック チャット ルームの IM 交換を処理するように設定されています。

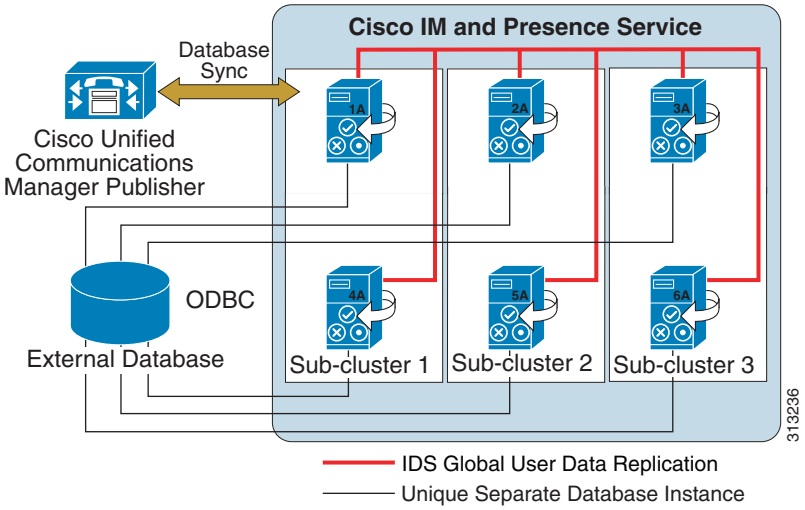
アドホック チャット ルームは、1 人のユーザがチャット ルームに接続されている限り存続する IM セッションで、最後のユーザがルームを離れるとシステムから削除されます。IM 会話のレコードは永続的に維持されません。

永続的なチャット ルームは、すべてのユーザがルームを離れても存続するグループ チャット セッションで、アドホック グループ チャット セッションのように終了することはありません。その目的は、ユーザが後で永続的なチャット ルームに戻って、協力し特定のトピックに関する知識を共有したり、そのトピックに関する発言のアーカイブを検索したり、そのトピックのディスカッションに参加したりできるようにすることです。

永続的なチャットの場合、クラスタの各ノードに対する外部データベース インスタンスの 1:1 のマッピングが必要です。データベースのサイズを考慮する必要があります。メッセージのアーカイブはオプションであり、実行すると外部データベース インスタンスが接続されているノード上のトラフィックが増加します。大規模な配置では、ディスク領域がすぐにいっぱいになる可能性があるため、記録される情報量の処理に対してデータベースの大きさが十分であることを確認する必要があります。

Cisco IM and Presence サービスでは、外部データベースの基本的なインターフェイスが使用され、データベースの管理、インターフェイス フック、または設定は提供されません。Cisco IM and Presence サービスを永続的なグループ チャットとともに配置する場合は、クラスタ内の各サーバに個別のデータベース インスタンスが必要です（図 20-22 を参照）。データベース インスタンス間で同じハードウェアを共有することはできますが、必ずしも共有する必要はありません。

図 20-22　Cisco IM and Presence サービスの永続的なチャット

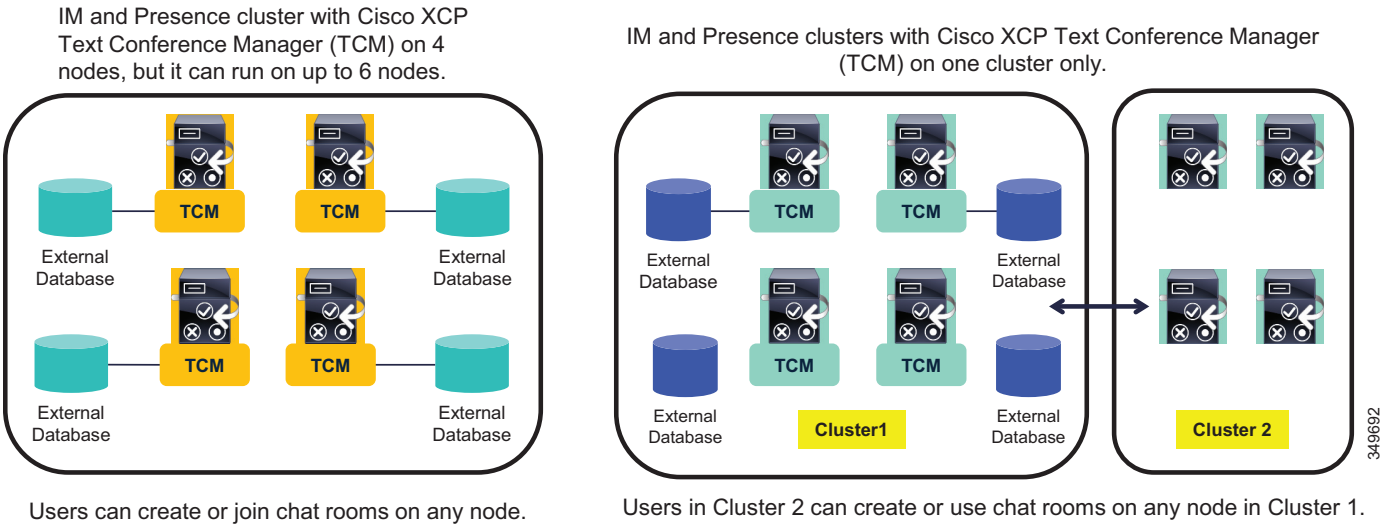


永続的なチャットが有効な場合は、外部データベースを Cisco XCP Text Conference Manager サービスに関連付ける必要があり、また、データベースがアクティブで到達可能である必要があります。そうでない場合は、Text Conference Manager は起動しません。Text Conference Manager サービスが起動した後で外部データベースとの接続が失敗した場合、Text Conference Manager サービスはアクティブなままで動作を継続します。ただし、メッセージはデータベースに書き込まれなくなり、接続が回復するまで新しい永続的なチャット ルームを作成できません。

永続的なチャットの配置に関する考慮事項

- 永続的なチャットはクラスタ内の 1 つ以上のノードに配置できます（図 20-23 を参照）。
- 永続的なチャットをサポートする各ノードは、専用のデータベース インスタンスに割り当てる必要があります。
- 外部データベース サーバは複数のインスタンスをサポートできます。
- 永続的なチャットはクラスタ全体の設定です。
- クラスタ内の少なくとも 1 つのノードを外部データベースに割り当てる必要があります。
- Cisco XCP Text Conference Manager サービスは、外部データベースに割り当てられていないノードでは動作しません。
- 純粋なインスタント（アドホック）会議には、外部データベースは必要ありません。

図 20-23　永続的なチャット配置



IM and Presence Service のチャット ルームの制限

IM and Presence サービスは、XMPP クライアント間のポイントツーポイント ファイル転送をサポートします。表 20-3 に、IM and Presence サービスのチャット ルームの制限を示します。

表 20-3　IM and Presence サービスのチャット ルームの制限

項目	最大数
ノードごとの永続的なチャット ルーム	1,500 ルーム
ノードあたりのルームの合計（アドホックおよび永続的）	16,500 ルーム
ルームごとの利用者	1,000 利用者
アーカイブから取得されたメッセージこれは、ユーザがルーム履歴を問い合わせたときに返されるメッセージの最大数です。	100 メッセージ
デフォルトで表示されるチャット履歴のメッセージこれは、ユーザがチャット ルームに入室したときに表示されるメッセージの数です。	15 メッセージ

マルチユーザ チャットとも呼ばれるテキスト会議は、アドホック グループ チャットおよび永続的なグループ チャットとして定義され、XCP フィーチャ セットの一部としてサポートされます。また、オフライン インスタント メッセージング（現在オフラインであるユーザのためにインスタント メッセージを保存する機能）も XCP フィーチャ セットの一部としてサポートされます。Cisco IM and Presence サービスでは、これらの各インスタント メッセージング機能における保存は、異なる場所で処理されます。オフライン インスタント メッセージングは、Cisco IM and Presence サービス IDS データベースにローカルに保存されます。

アドホック グループ チャットは、Cisco IM and Presence サービスでメモリ内にローカルに保存されます。永続的なグループ チャットには、チャット ルームおよび会話を保存するための外部データベースが必要です。サポートされている外部データベースは、PostgreSQL（https://www.postgresql.org/ を参照）、Microsoft SQL、および Oracle（https://www.oracle.com を参照）です。

（注） シスコでは、データベースのベスト プラクティスおよびデータ抽出ツールを提供していません。これらのタスクとツールはデータベース管理者によって提供されることが予想されます。

（注） Oracle を外部データベースとして使用する場合は、テーブルスペースの情報を設定する必要があります。

マネージド ファイル転送

マネージド ファイル転送（MFT）を使用すると、Cisco Jabber などの IM and Presence サービス クライアントは他のユーザ、アドホック グループ チャット ルーム、および永続的なチャット ルームにファイルを転送できます。ファイルは外部ファイル サーバのリポジトリに保存され、トランザクションが外部データベースのログに記録されます。

この設定はファイル転送に固有な設定であり、法規制コンプライアンスのためのメッセージ アーカイバ機能には影響しません。

（注） IM and Presence ノードから外部の各サードパーティ データベースへの接続は 1 つしか存在しないため、MFT または永続的なチャットのハイ アベイラビリティ ソリューションはありません。

ソフトウェア

- Cisco IM and Presence サービス リリース 10.5(2) 以降
- PostgreSQL または Microsoft SQL
- Oracle バージョン 9i、10g、または 11g
- ファイル サーバ バージョン CentOS 6.5 以降

（注） Oracle Data Guard は、外部データベースとして使用できますが、シスコではテストされていません。

（注） 外部データベースとの暗号化接続が必要な場合は、Oracle 11g を使用してください。サポートされている他のデータベース バージョンでは、暗号化接続を確立できません。

Linux または Windows オペレーティング システムにデータベースをインストールできます。サポートされているオペレーティング システムとプラットフォーム要件の詳細については、PostgreSQL、Microsoft SQL、および Oracle のマニュアルを参照してください。

IPv4 と IPv6 はデュアルスタック モードのままでサポートされます。

転送プロセス

1 人の受信者にファイルを転送するためのフローには、次の手順が含まれます。

1. 送信者のクライアントは HTTP 経由でファイルをアップロードし、サーバはファイルの URI を応答として返します。
2. ファイルは、ファイル サーバのリポジトリに格納されます。
3. 外部データベース ログ テーブルに、アップロードを記録する項目が書き込まれます。
4. 送信者のクライアントが受信者に IM を送信します。IM にはファイルの URI が含まれます。
5. 受信者のクライアントが HTTP 経由でファイルを要求します。
6. ファイルがリポジトリから読み取られます（取得されます）。
7. ダウンロード要求がログ テーブルに記録されます。
8. ファイルが受信者にダウンロードされます。

グループ チャットや永続的なチャット ルームにファイルを転送するためのフローもこれと類似していますが、異なる点として送信者はチャット ルームに IM を送信し、チャット ルームの各参加者は個別にファイル ダウンロード要求を送信します。

IM and Presence サービスでのマネージド ファイル転送

IM and Presence サービス ノードでマネージド ファイル転送を有効にする場合は、次の情報を考慮してください。

- IM and Presence サービス ノードに、永続的なグループ チャット機能、メッセージ アーカイバ機能、またはマネージド ファイル転送機能を組み合わせて配置する場合は、これらの機能すべてに、同一の物理外部データベース インストールとファイル サーバを割り当てることができます。ただし、サーバの容量を判断する際には、見込まれる IM トラフィックおよびファイル転送（サイズと数）を考慮する必要があります。
- ノードの公開キーはノードの割り当てが解除されると無効になります。後日ノードが再割り当てされると、新しいノード公開キーが自動的に再生成されます。外部ファイル サーバも再設定する必要があります。
- マネージド ファイル転送が必要な各ノードで、Cisco XCP File Transfer Manager サービスがアクティブである必要があります。

マネージド ファイル転送のキャパシティ

すべての Jabber ユーザが自由にファイル転送を使用できるため、ファイル転送の使用状況によってはシステムに影響する可能性があります。必要なキャパシティを効果的に計算するには、表 20-4 を参照してください。

表 20-4 の値は、500 キロバイト（KB）の転送ファイル サイズに厳密に基づいています。これらの値を調整して異なるキャパシティを計算することができます。たとえば、次のシナリオはどれも 1 時間あたり 1,500 の転送に相当します。

- 1 時間に 1,500 人の各ユーザが 500 KB のファイル 1 個をダウンロードまたはアップロードする。
- 3,000 人の各ユーザが 1 時間に 250 KB のファイル 1 個を転送する。
- 750 人の Jabber ユーザが他の 750 人の Jabber ユーザに 500 KB のファイル 1 個を送信する。

サポートされる最大転送数は 500 KB のファイルで 12,000 です。

表 20-4　Jabber ファイル転送のキャパシティ

使用レベル	1 時間あたりの転送数	CPU %（合計）	CPU %（AFT）	AFT_LOG テーブル	AFT_LOG サイズ	JM テーブルの追加サイズ
低レベル	1,500	35 %	25 %	3,000	0.6 MB	1.5 MB
中レベル	4,500	50 %	40 %	9,000	2.8 MB	4.5 MB
最大レベル	12,000	65 %+	55 %	24,000	7.8 MB	12.0 MB

[ファイル転送（File Transfer）] ウィンドウの [ファイル転送タイプ（File Transfer Type）] には次のコントロールがあります。

- [無効（Disabled）]：ファイル転送はクラスタに対して無効です。
- [ピアツーピア（Peer-to-Peer）]：1 対 1 のファイル転送は許可されますが、サーバではファイルのアーカイブや保存が行われません。グループ チャットのファイル転送はサポートされません。

マネージド ファイル転送と永続的なグループ チャットの両方で、IM and Presence クラスタ内の IM and Presence ノードごとに外部データベース インスタンスが必要です。

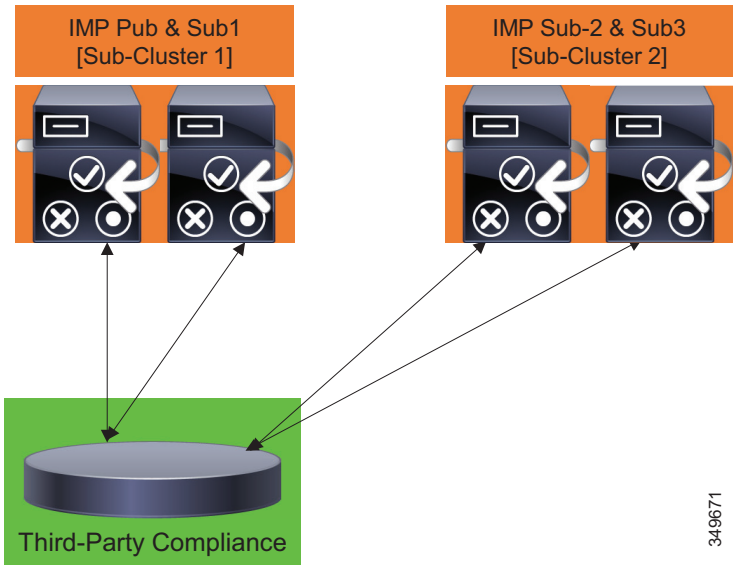
（注） マネージド ファイル転送が有効になっているノードを、ピアツーピアが有効になっているノードを含むクラスタに配置しないでください。推奨される移行パスは、ピアツーピア ノードをマネージドおよびピアツーピア ファイル転送ノードとして設定した後、それらのノードをマネージド ファイル転送ノードに変更することです。

オンプレミスの Cisco IM and Presence サービスのメッセージ アーカイブおよびコンプライアンス

アーキテクチャの一部として、Cisco IM and Presence サービスにはメッセージ アーカイバ コンポーネントが含まれています。このコンポーネントによって、非ブロッキング コンプライアンスの一部として、ポイントツーポイント メッセージ、テキスト会議メッセージ、フェデレーション メッセージ、およびクラスタ間メッセージを外部データベースにロギングできます。Cisco IM and Presence サービスのメッセージ アーカイブには、クラスタごとに外部データベース（PostgreSQL、Microsoft SQL、または Oracle）インスタンスが必要です。同じデータベースを複数のクラスタで共有できますが、クラスタ間ピア導入のユーザ数が多い場合は、容量の需要と大量のデータ挿入のためにさらに多くのデータベース インスタンスが必要になります。IM and Presence クラスタあたり 1 つの外部データベース インスタンスがサポートされますが、最低でもサブクラスタ ペアごとに 1 つの外部データベース インスタンスを配置することが推奨されます。

図 20-24 に示すように、メッセージのロギングだけでなく、メッセージ配信とメッセージ内容に対するポリシー適用も可能にする、ブロッキング サードパーティ コンプライアンス ソリューションは、サードパーティ コンプライアンス サーバ ソリューションを通して提供されます。Cisco IM and Presence サービスのサードパーティ製コンプライアンスは、クラスタ内の各サーバに複数のコンプライアンス サーバ、各コンプライアンス サーバに複数のサーバ、またはその他の組み合わせで展開できます。サードパーティ コンプライアンス ソリューションの使用は、メッセージ アーカイバ機能の使用と相互排他的です。

図 20-24　　オンプレミス Cisco IM and Presence サービス：サードパーティ コンプライアンス



クラスタ内のすべての Cisco IM and Presence サービス サーバが、コンプライアンスの対象となります。図 20-25 は IM and Presence サービス クラスタ内の各サーバに対するコンプライアンス サーバの配置を示し、図 20-26 は、複数の IM and Presence サービス サーバへの単一のコンプライアンス サーバのマッピング、または単一の IM and Presence サービス サーバへの複数のコンプライアンス サーバのマッピングを示しています。さまざまな配置オプションによって、コンプライアンス ポリシー ルーティングとクラスタ配置の柔軟性が向上します。

図 20-25　Cisco IM and Presence サービスのサードパーティ コンプライアンス

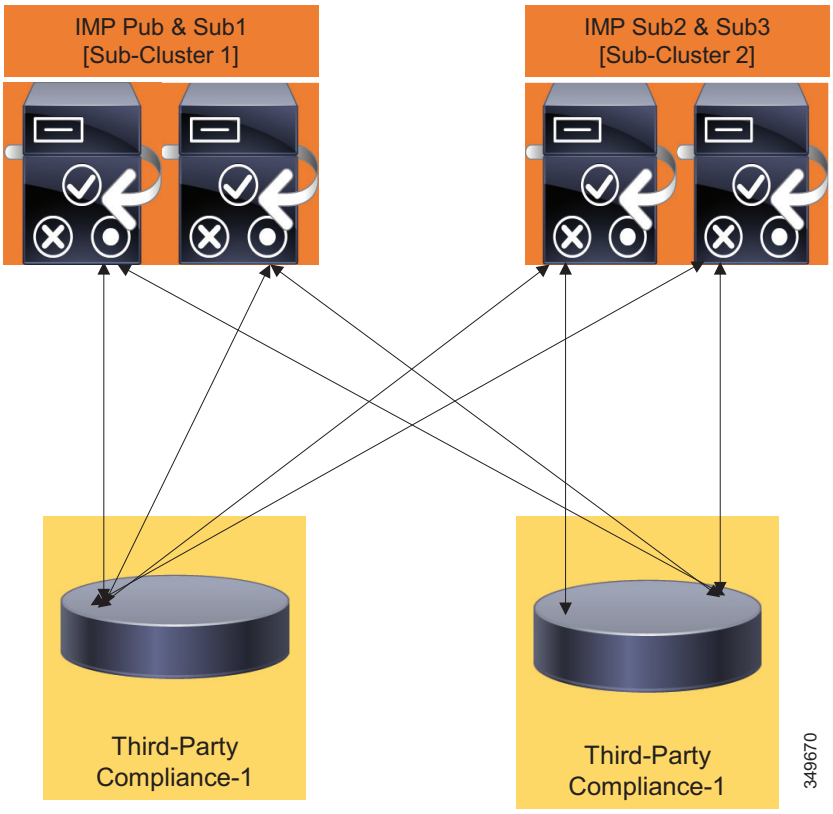
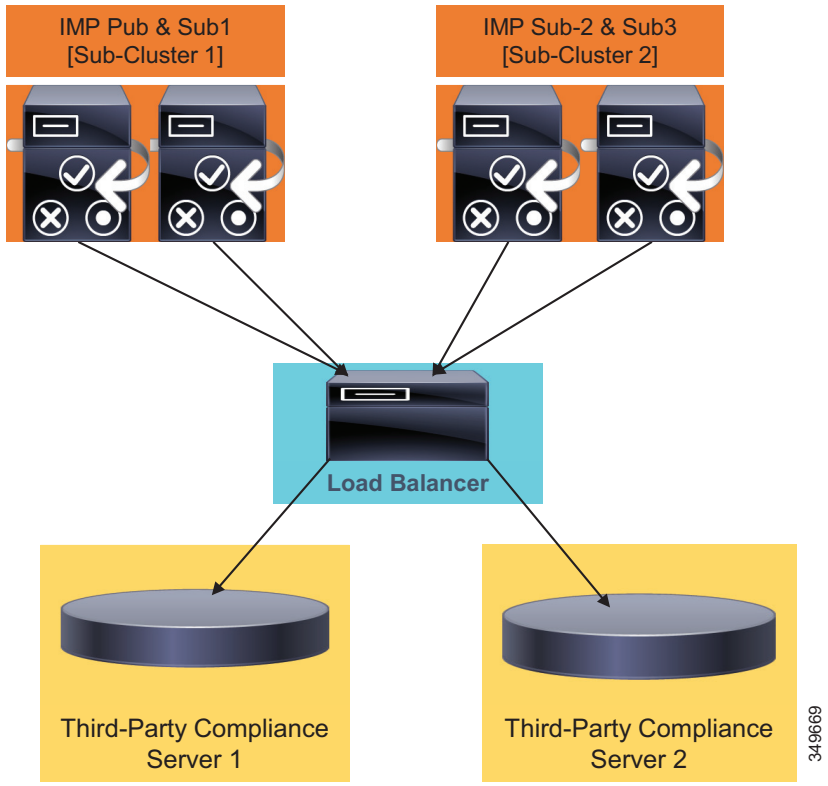


図 20-26　完全なハイ アベイラビリティ クラスタ全体のコンプライアンス



クラスタ全体のコンプライアンスによって、特定のイベントに基づいてコンプライアンス プロファイルを設定でき、コンプライアンス プロファイルでイベントが重複した場合、これらのイベントを順位付けして適切なコンプライアンス サーバにルーティングできます。すべてのコンプライアンス サーバにコンプライアンス プロファイルを割り当てる必要があり、複数のコンプライアンス サーバで同じコンプライアンス プロファイルを共有できます。

IM and Presence サービスの外部データベース要件は、使用する機能によって異なります。たとえば、永続的なグループ チャット機能を有効にするには、IM and Presence サブクラスタ ペアごとに外部データベースが必要です。この場合、クラスタ内のすべての IM and Presence サブクラスタ ペアが固有のデータベース インスタンスを指しますが、同じ物理データベース インストールを共有することができます。

メッセージ アーカイバ（コンプライアンス）機能では、IM and Presence クラスタごとに 1 つ以上の外部データベース インスタンスが必要です。ただし、各サブクラスタ ペアを 2 つの外部データベース インスタンスと 1:1 でマッピングし、それぞれのコンプライアンス サーバに割り当てられたコンプライアンス プロファイルで IM and Presence ノードをそれぞれ定義することが推奨されます。

マネージド ファイル転送機能には、Cisco XCP File Transfer Manager サービスがアクティブになっている IM and Presence サービス クラスタ内の IM and Presence サービス ノードごとに固有の論理外部データベース インスタンスが 1 つ必要です。

（注）　IM and Presence サービス ノード上に永続的なグループ チャット、メッセージ アーカイバ（コンプライアンス）、およびマネージド ファイル転送機能を組み合わせて配置する場合は、各機能に同じ外部データベースを割り当てることができます。

コラボレーション クライアントのメッセージ ロギング ストレージ要件

メッセージ アーカイブと永続的なチャット機能は、外部データベースを使用してメッセージをオフラインで保存します。配置のストレージ要件には、カスタマー トポロジ、データベースの調整方法、組織内でのメッセージングの使用方法などの複数の考慮事項が存在します。次の計算は、外部データベース ストレージ配置のロー データベース ストレージ要件を見積もるために使用する入力値のガイドラインを提供します。

Cisco IM and Presence サービスは SIP クライアントと XMPP クライアントの両方をサポートし、メッセージあたりのオーバーヘッドのサイズはプロトコルによって若干異なります。メッセージ アーカイブの 1 つのメッセージあたりのオーバーヘッドは、実際には配置、Jabber ID/UserID サイズ、クライアント タイプ、およびスレッド ID に応じて大きくなったり、小さくなったりすることがあります。したがって、平均のオーバーヘッド サイズが使用されます。SIP ベースのメッセージの場合、平均オーバーヘッドは 800 バイトになり、XMPP メッセージの場合、平均オーバーヘッドは 600 バイトになります。

Cisco Jabber ユーザに対する 1 ヵ月あたりのメッセージ アーカイブの最低ストレージ要件（バイト単位）は、次のように計算できます。

（ユーザ数）*（1 時間あたりのメッセージ数）*（1 ヵ月あたりのビジー時間数）*（600 +（3 * メッセージあたりの文字数））

Cisco IM and Presence サービスのコンプライアンス設定で [発信メッセージのロギングの有効化（Enable Outbound Message Logging）] が有効になっている場合は、上記のメッセージ アーカイブ要件を 2 倍にする必要があります。

Cisco Jabber ユーザに対する 1 ヵ月あたりの永続的なチャットの最低ストレージ要件（バイト単位）は、次のように計算できます。

（ユーザ数）*（1 時間あたりの永続的なチャット メッセージ数）*（1 ヵ月あたりのビジー時間数）*（700 +（3 * メッセージあたりの文字数））

（注） 永続的なチャットは XMPP クライアントでのみサポートされ、700 バイトの平均オーバーヘッドを使用します。

表 20-5 に、データベース容量に関する要件の特定を支援するスプレッドシートの例を示します。これらの計算は、非常に簡略化された形で示されています。この例では、データベース タイプ間の違いやストレージの使用方法は提供されません。

表 20-5　データベース ストレージ要件を見積もるためのスプレッドシートの例

	A	B	C	D	E
1	**説明**	**メッセージ アーカイバ**	**永続的なチャット**	**マネージド ファイル転送**	**合計**
2	機能が有効	○	○	○	
3	メッセージ アーカイバのアウトバウンド メッセージ ロギングが有効	なし			
4	ユーザ数	2500	2500	2500	
5	ユーザごとの 1 時間あたりのメッセージの推定件数	15	15	2	
6	1 ヵ月あたりのビジー時間数	200	200	200	

表 20-5　データベース ストレージ要件を見積もるためのスプレッドシートの例(続き)

	A	B	C	D	E
7	メッセージあたりの平均文字数	250	250	250	
8	メッセージあたりの XMPP メッセージ オーバーヘッド バイト数	600	700	600	
9	データベース テキスト メッセージ エンコーディング係数	3	3	3	
10	バッファ量乗数(パーセント)	150.00%	150.00 %	150.00 %	
11	**計算**				
12	1 ヵ月あたりのメッセージ件数	7,500,000	7,500,000	1,000,000	16,000,000
13	上記の計算式	IF(B2="Yes", IF(B3="Yes", 2,1)* ROUNDUP(B4*B5*B6,0),0)	IF(C2="Yes", ROUNDUP(C4*C5*C6, 0),0)	IF(D2="Yes", ROUNDUP(D4*D5*D6, 0),0)	
14	1 ヵ月間に使用される推定総 GB ストレージ	9.9	10.7	1.4	22.0
15	上記の計算式	ROUNDUP((B12* ((B7*B9)+B8))/ 1024000000,1)	ROUNDUP((C12* ((C7*C9)+C8)) / 1024000000,1)	ROUNDUP((D12* ((D7*D9)+D8)) / 1024000000,1)	
16	1 ヵ月間にプロビジョニングする推定総データベース GB	14.9	16.1	2.1	33.1

これらのメッセージ アーカイブ数と永続的なチャット数は、長期の平均値に基づいた最小ストレージ要件です。したがって、非常に大きい UserID、予想よりも大きいインスタント メッセージ長、およびストレージ要件を増加させる可能性がある他の要因に対応するために、1.5(150 %)のバッファ係数を使用する必要があります。表 20-6 に、Cisco Collaboration クライアントのストレージ要件の例を示します。

表 20-6　Cisco Collaboration クライアントのメッセージ ロギング ストレージ要件の例

プロファイル	ユーザ数	1 時間あたりのメッセージ数	1 ヵ月あたりのビジー時間数	メッセージの平均サイズ	メッセージ アーカイブ ストレージの要件	永続的なチャット ストレージの要件
低	1,500	10	200	100	2.7 GB	3.0 GB
中	2,500	15	200	250	9.9 GB	10.7 GB
高	2,500	25	200	500	25.7 GB	26.9 GB

オンプレミスの Cisco IM and Presence サービスのカレンダー統合

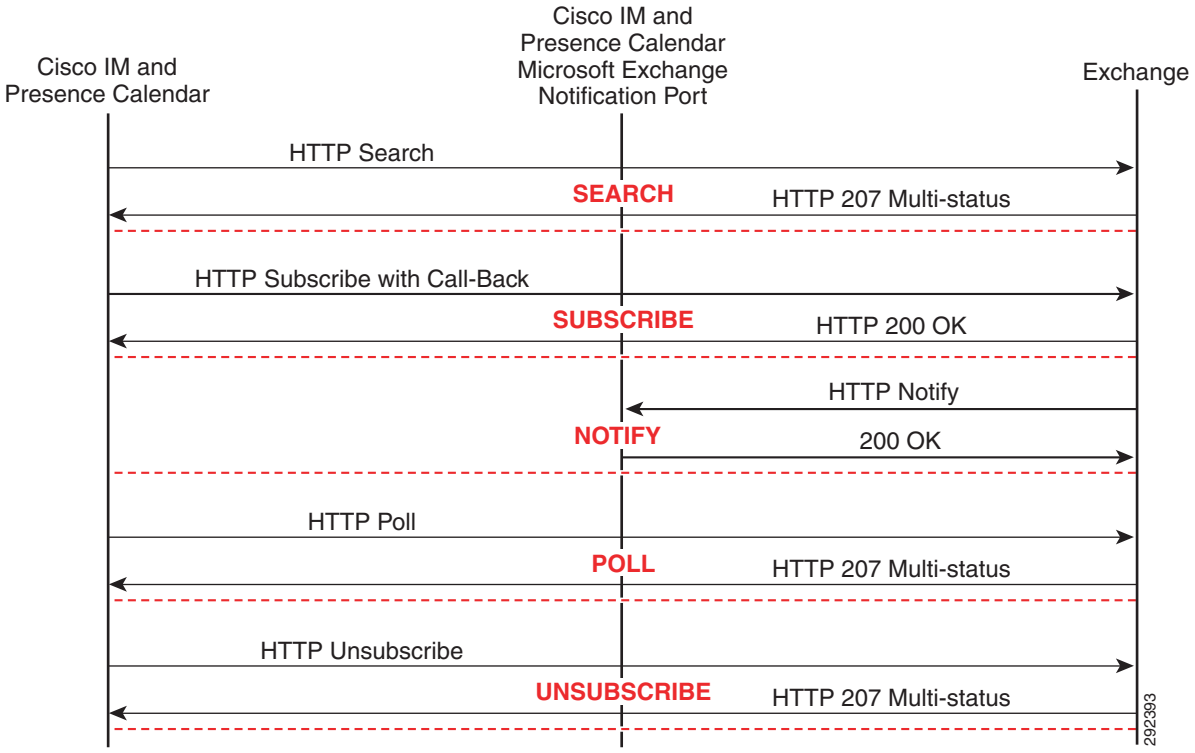
Cisco IM and Presence サービスは、Microsoft Exchange 2010 または 2013 サーバ側の統合でカレンダー モジュール インターフェイスを使用してカレンダー ステータスを取得し、それをプレゼンス ステータスに集約できます。シスコは、Microsoft Exchange の設定、配置、またはベスト プラクティス手順は提供していませんが、Cisco IM and Presence サービスと Microsoft Exchange 2010 または 2013 のカレンダー モジュール インターフェイスとの統合に関するガイドラインをこの項で提供しています。

Microsoft Exchange の統合は、Microsoft Active Directory 2008 および Active Directory 2012 と Windows Server 2008 および Windows Server 2012 でサポートされます。Microsoft Exchange 2010 または 2013 では、Microsoft Exchange からの要求の送信や通知の受信を可能にする Exchange Web サービス（EWS）経由で、サーバからカレンダー データを取得できます。Microsoft Exchange との統合は、カレンダー アプリケーション用の別のプレゼンス ゲートウェイによって実現されます。管理者が Outlook 対応のプレゼンス ゲートウェイを設定すると、ユーザは自分のプレゼンス ステータスにカレンダー情報を集約するかどうかを切り替えられるようになります。

カレンダー情報の取得に使用される交換 ID は、そのユーザの LDAP 構造の電子メール ID から取得されます。電子メール ID が存在しない場合、または LDAP が使用されていない場合は、Cisco IM and Presence サービスのユーザ ID が交換 ID としてマッピングされます。

Cisco IM and Presence サービスから Microsoft Exchange Server へのカレンダー ステータスに関するサブスクリプションによって、情報が収集されます。図 20-27 は、このやり取りを示します。

図 20-27　Cisco IM and Presence サービスと Microsoft Exchange 間の Outlook Web Access 通信



Microsoft Outlook カレンダー統合

IM and Presence サービスでは、ユーザの応答可能性をパブリッシュするときに、Microsoft Outlook カレンダーの空きおよびビジーのデータを組み込むことができます。この機能により、ユーザの応答可能性とステータスが自動的に維持されます。これはサーバ間の統合に基づいているため、発信元ユーザのログイン状況が別のユーザに表示されます。Microsoft Outlook カレンダー機能では、Microsoft Exchange Server へのゲートウェイ接続を確立する必要があり、Microsoft Exchange Server 2003、2007、および 2010 と互換性があります。

（注）　Cisco IM and Presence サービスは、単一または複数の Microsoft Exchange Server とともに単一のフォレスト内にのみ配置できます。Microsoft Exchange 配置では、複数の Exchange Server で構成されるクラスタを使用できるので、Cisco IM and Presence サービスは、Cisco IM and Presence サービスがステータスを要求する対象ユーザをホストしている Exchange Server への REDIRECT メッセージを受け入れます。

多言語カレンダーのサポート

カレンダー統合配置の要件で複数の言語を指定する場合は、次の設計ガイドラインに従ってください。

- Cisco IM and Presence サービスには、Cisco Unified Communications Manager と同様に、ユーザが必要なロケールを選択できるように適切なロケールがインストールされている必要があります。
- Cisco IM and Presence サービスは、カレンダー統合用に Unified Communications の標準ロケールをすべてサポートしています。
- エンド ユーザ用ページ、または管理用の Bulk Administration Tool によって、ユーザに目的のロケールが設定される必要があります。
- Cisco IM and Presence サービスは、最初の照会とともに適切なロケール フォルダを送信します。照会は必要に応じて、フロントエンドまたはクライアント アクセス用 Microsoft Exchange Server の最初の応答によってリダイレクトされます。

Exchange Web サービス カレンダー統合

Cisco IM and Presence サービスでは、ユーザの全体のプレゼンス ビューに集約されるカレンダー ステータス情報を Microsoft Exchange Web サービスが収集することを許可するよう設定できます。ユーザ メールボックスが設定された Exchange Server に存在する場合、Cisco IM and Presence サービスは Exchange Server と直接通信します。その一方で、ユーザ メールボックスが設定された Exchange Server 以外のサーバに存在する場合、Cisco IM and Presence サービスは Exchange Server のリダイレクションに従ってユーザ メールボックスが存在するサーバを見つけます。サーバ ファームの Exchange Server だけが、設定された Exchange Server として機能できます。サーバ ファームのサーバを 1 つのみ指定する必要があります。

Microsoft Exchange Web サービスは、エンドユーザが使用する言語に関係なく、Exchange クライアント アクセス サーバと連携するために使用されるプロトコルを指定します。したがって、エンドユーザの言語を決定するためにロケールを使用する必要はありません。Cisco IM and Presence サービス カレンダー統合は、単一の Microsoft Exchange フォレストでのみサポートされます。

Cisco IM and Presence Exchange Web サービス カレンダー統合は、カレンダー情報のポーリング（図 20-28 を参照）とカレンダー情報のサブスクリプション/通知（図 20-29 を参照）の両方をサポートします。さまざま設定パラメータを使用して、ポーリング間隔のレート、サブスクリプション頻度、およびタイマーの耐障害性を制御します。その他の設定の詳細については、次の Web サイトで入手可能な『*Integration Note for Configuring Cisco IM and Presence with Microsoft Exchange*』を参照してください。

https://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

図 20-28　Cisco IM and Presence サービス カレンダーを使用した Exchange Web サービスのポーリング

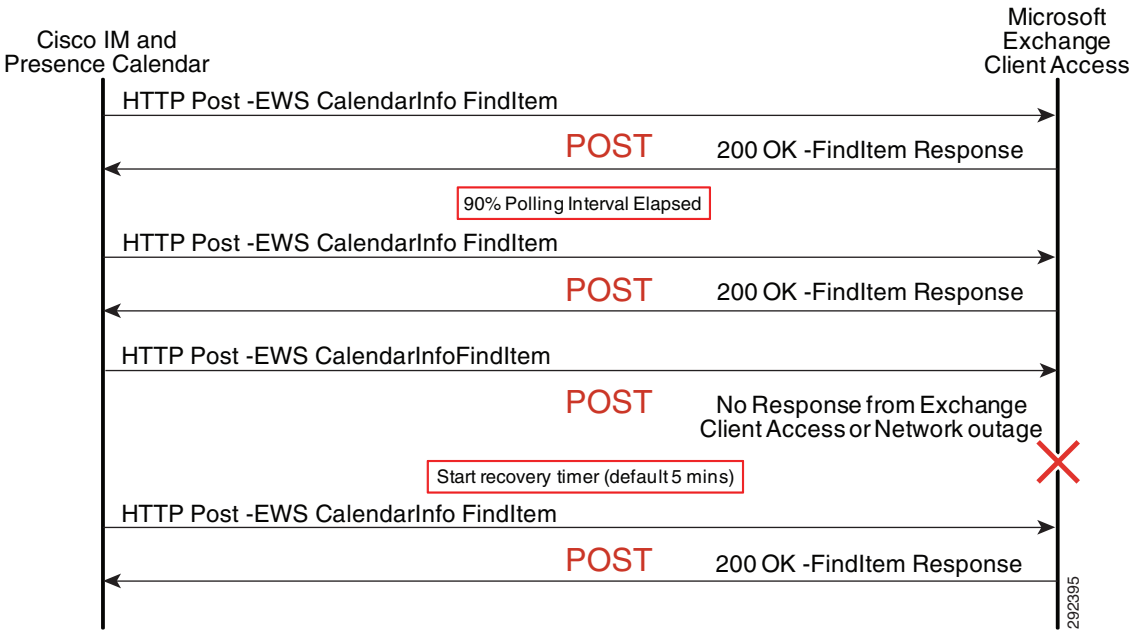
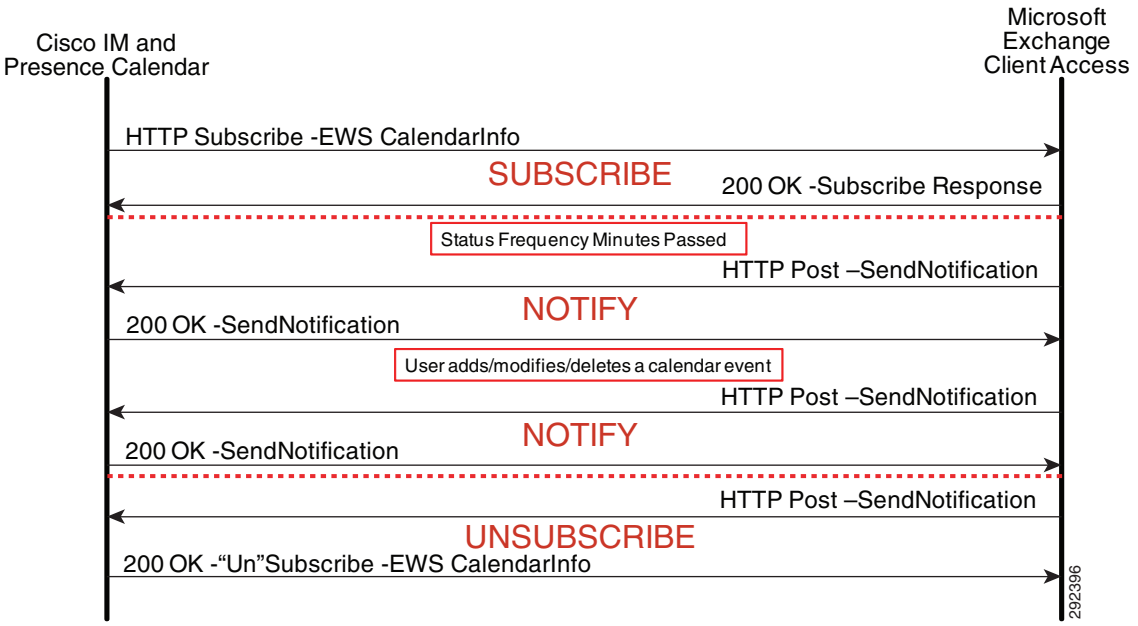


図 20-29　Cisco IM and Presence サービス カレンダーを使用した Exchange Web サービスのサブスクリプション/通知



クライアント アクセス サーバ（CAS）ロールがインストールされた各サーバに対して Service Connection Point（SCP）Active Directory オブジェクトが作成されている場合は、Cisco IM and Presence サービスで Exchange Web サービスの Auto Discover もサポートされます。Auto Discover では、ドメインと、ホストおよびポートの代わりにサイト（任意）を使用してカレンダー ゲートウェイが設定されます。Cisco IM and Presence サービスは、自動検出アルゴリズムを使用して適切なクライアント アクセス サーバである Exchange Server との接続に使用する Exchange Web サービスの URL を特定します。

オンプレミスの Cisco IM and Presence サービス モビリティ統合

Cisco IM and Presence サービスでは、連絡先リストとプレゼンス ステータスを Cisco Jabber Mobile IM と統合できます。Jabber Mobile IM は引き続き Cisco Unified CM と直接通信しますが、Cisco Unified CM は、AXL/SOAP および SIP 経由で Cisco IM and Presence サービスと通信します。

Cisco Unified CM が Cisco IM and Presence サービスとの間で管理セッションを確立するには、その前に Cisco IM and Presence サービスと Cisco Unified CM 上でアプリケーション ユーザを設定する必要があります。Cisco Jabber Mobile IM のエンドユーザ ログインにより、Cisco IM and Presence サービスに対してシステム設定、ユーザ設定、連絡先リスト、プレゼンス ルール、およびアプリケーション ダイヤル ルールを求める Cisco Unified CM SOAP 要求が生成されます。その後、Unified Communicator Change Notifier（UCCN）設定と Presence SIP サブスクリプションが実行されます。

オンプレミスの Cisco IM and Presence サービス サードパーティ製 Open API

Cisco IM and Presence サービスでは、SIP/SIMPLE と XMPP に加え、HTTP を介してサードパーティ製アプリケーションと統合できます。HTTP インターフェイスは、設定インターフェイスのほか、Representational State Transfer（REST）経由のプレゼンス インターフェイスを備えています。サードパーティ製の Open API は、プレゼンスへのアクセス メカニズムとして、リアルタイム イベンティング モデルとポーリング モデルの 2 つのメカニズムを持っています。

サードパーティ製 Open API の詳細については、次の Web サイトの Cisco Developer Community を参照してください。

https://developer.cisco.com/web/cdc

リアルタイム イベンティング モデル

リアルタイム イベンティング モデルでは、Cisco IM and Presence サービス上でアプリケーション ユーザを使用して管理セッションを確立することにより、エンド ユーザがそのセッション キーを使用してログインできるようになります。ユーザはログインすると、Representational State Transfer（REST）を使用してプレゼンスの更新について登録とサブスクリプションを行います。図 20-30 に、サードパーティ製 Open API リアルタイム イベンティング モデルでの Cisco IM and Presence サービスとの対話を示します。

図 20-30　サードパーティ製 Open API リアルタイム イベンティング モデル

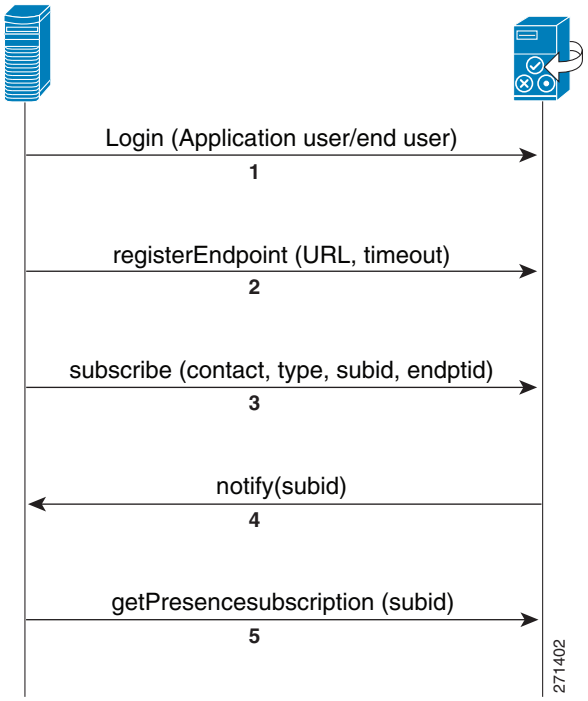


図 20-30 のコールフローは、次の一連のイベントを示しています。

1. アプリケーションが、スーパーユーザ アプリケーション ユーザ（APIUser）経由で Cisco IM and Presence サービスに対して SOAP ログイン要求を開始し、Cisco IM and Presence サービスがセッション キーを返します。これにより、アプリケーションはセッションキーを使用してエンド ユーザをログインさせられるようになります（実質的には、エンド ユーザがアプリケーション経由でログインします）。
2. エンド ユーザが、アプリケーションユーザ セッション キーを使用してエンドポイントを登録します。
3. アプリケーションが、ユーザの代わりに（セッション キーを使用して）サブスクライブ要求を開始し、ユーザ情報、連絡先リスト、およびプレゼンス ルールを取得します。
4. Cisco IM and Presence サービスが、非保護の通知を送信します。
5. アプリケーションが、ユーザのプレゼンス ステータスを要求します。

ポーリング モデル

ポーリング モデルでは、Cisco IM and Presence サービス上でアプリケーション ユーザを使用して管理セッションを確立することにより、エンド ユーザがそのセッション キーを使用してログインできるようになります。ユーザがログインすると、アプリケーションは、ここでも Representational State Transfer（REST）を使用して、定期的にプレゼンスの更新を要求します。図 20-31 に、サードパーティ製 Open API ポーリング モデルでの Cisco IM and Presence サービスとの対話を示します。

図 20-31　サードパーティ製オープン API ポーリング モデル

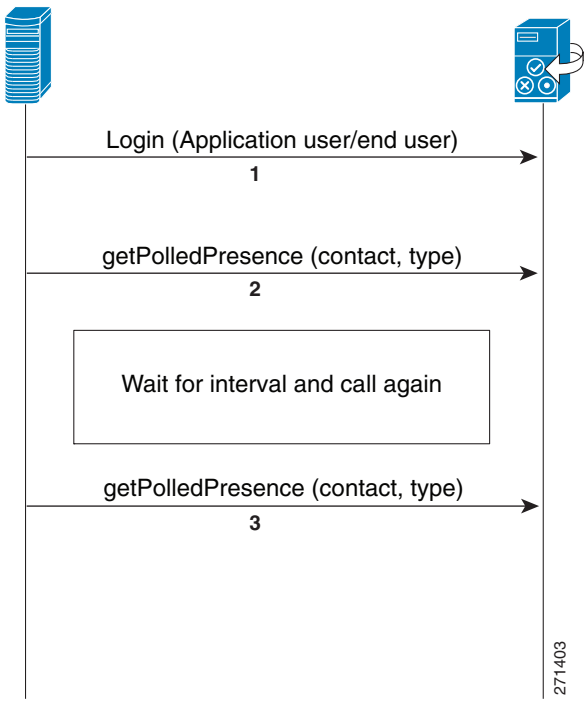


図 20-31 のコールフローは、次の一連のイベントを示しています。

1. アプリケーションが、スーパーユーザ アプリケーション ユーザ（APIUser）経由で Cisco IM and Presence サービスに対して SOAP ログイン要求を開始し、Cisco IM and Presence サービスがセッション キーを返します。これにより、アプリケーションはセッションキーを使用してエンド ユーザをログインさせられるようになります（実質的には、エンド ユーザがアプリケーション経由でログインします）。
2. アプリケーションがプレゼンス ステータスを要求します。イベンティング モデルは省略されます。
3. アプリケーションがプレゼンス ステータスを要求します。イベンティング モデルは省略されます。

（注）　ポーリング モデルでは、基本プレゼンスと高度なプレゼンスの両方が取得できますが、Presence サーバの負荷が大きくなります。

Extensible Messaging and Presence Protocol インターフェイス

XCP アーキテクチャでは、プレゼンス、インスタント メッセージング、および参加者管理に、クライアント XMPP インターフェイスおよび Cisco AJAX XMPP Library インターフェイスという 2 つのオープンなインターフェイスを追加で使用できます。クライアント XMPP の機能によって、サードパーティ製 XMPP クライアントにプレゼンス、インスタント メッセージング、および参加者管理を統合できます。これは、Cisco IM and Presence サービスにおける SIP/SIMPLE インターフェイスを補完するインターフェイスです。クライアント XMPP インターフェイスは、Cisco IM and Presence サービス内では通常の XMPP クライアントとして処理されます。そのため、インターフェイスのサイジングは、通常の XMPP クライアントとして処理する必要があります。

Cisco AJAX XMPP Library API は、XCP 機能を Web アプリケーションおよびウィジェットに統合するための Web 2.0 スタイルのインターフェイスを提供し、Cisco IM and Presence サービスから直接利用できます。Cisco AJAX XMPP Library API は Bidirectional-streams Over Synchronous HTTP（BOSH）インターフェイスと通信するクライアント側専用の JavaScript ライブラリです。BOSH は、基本的にロングポーリング手法を使用してサーバから Web ブラウザにデータをプッシュできる XMPP over HTTP インターフェイスです。

いずれかのモデルのサードパーティ製 Open API を Cisco IM and Presence サービスと統合する場合は、次の要件に従ってください。

- プレゼンス インターフェイスに対する証明書（sipproxy.der）と設定インターフェイスに対する証明書（tomcat_cert.der）が必要です。
- 1 つの Cisco IM and Presence サービス配置で、1000 人を超えるサードパーティ製 Open API ユーザの統合はできません。
- パフォーマンスの向上を図るには、サードパーティ製 Open API ユーザを Cisco IM and Presence サービス クラスタにあるすべてのサーバに均等に振り分けてください。

Cisco IM and Presence サービスのサードパーティ製 Open API の使用に関する詳細とサポートについては、次の Web サイトの Cisco Developer Services を参照してください。

https://developer.cisco.com/web/cupapi

開発者向けの情報は、Cisco Developer Community にも用意されています。次の Web サイトからログインしてアクセスしてください。

https://developer.cisco.com/

オンプレミスの Cisco IM and Presence サービスの設計に関する考慮事項

- LDAP 統合が可能な場合、すべてのユーザ情報（番号、ID など）は、単一のソースから Unified CM との LDAP 同期を使用してプルする必要があります。ただし、LDAP server および LDAP 同期が有効でない Unified CM の両方を含む配置の場合、管理者は、ユーザのディレクトリ番号のアソシエーションの設定にあたって、Unified CM と LDAP の両方に一貫した設定を行う必要があります。
- Cisco IM and Presence サービスは、Diffserv コード ポイント（DSCP）により、レイヤ 3 IP パケットをマーキングします。Cisco IM and Presence サービスは、SIP プロキシの下の Differential Service Value サービス パラメータ（デフォルトは DSCP 24（PHB CS3））に基づいて、すべての IM and Presence トラフィックをマーキングします。
- Cisco IM and Presence サービスのプレゼンス ポリシーは、ユーザが作成した定義済みのルール セットによって、厳格に制御されます。
- サービス パラメータ IMP PUBLISH Trunk を使用して、Cisco IM and Presence サービスとの SIP 通信トラフィックを簡素化します。
- Unified CM のプレゼンス ユーザは、プライマリ内線だけでなく、ライン アピアランスと関連付けます。これにより、デバイスとユーザのプレゼンス ステータスの詳細度が向上します。サービス パラメータ IMP PUBLISH Trunk を使用している場合は、Unified CM 内のプレゼンス ユーザをライン アピアランスと関連付けてください。
- サーバ ハードウェアとクラスタ トポロジの特性を決定する際は、プレゼンス ユーザ プロファイル（ユーザ アクティビティおよび連絡先リストの連絡先とサイズ）を考慮する必要があります。Cisco IM and Presence のシステム アーキテクチャは、フル装備のシステムでユーザ 1 人あたり 75 件という連絡先リストの平均サイズに基づいています。システム全体ではユーザごとの連絡先リストのサイズが異なりますが、システムのユーザの多くが 75 件の連絡先という平均リスト サイズを超える場合はシステム パフォーマンスに影響します。デフォルトでは、連絡先リストの最大サイズは 200 です。一部のユーザの連絡先が 200 件を超えている場合は、IM and Presence クラスタの [プレゼンスの設定（Presence Settings）] を修正することで、この最大連絡先リスト サイズを変更できます。サイジングの追加情報については、Cisco IM and Presence（25-35 ページ）と名簿管理（25-36 ページ）のセクションを参照してください。
- クラスタ全体として最高のパフォーマンスを得るには、[プレゼンスサーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] エンタープライズ パラメータに、デフォルトの [平衡化（balanced）] を使用します。
- Cisco IM and Presence サービスでは、永続的なチャットを行う場合、クラスタ内の各サーバに外部データベース インスタンスが必要です。また、メッセージ アーカイブについては、クラスタごとに 1 つのデータベース インスタンスが必要です。サードパーティ製コンプライアンスは、1 つの外部コンプライアンス データベースに対する IM and Presence サービス クラスタ内のすべてのサーバまたはサーバのサブセットのマッピングをサポートします。IM and Presence サーバごとに複数のコンプライアンス サーバ、コンプライアンス サーバごとに複数の IM and Presence サーバ、またはその組み合わせといった、3 つの外部データベース オプションが柔軟な配置を実現します。
- コンプライアンス サーバは専用にすることも、同じクラスタ内の IM and Presence ノードと共有することもできます。コンプライアンス プロファイルで定義されている両方の IM and Presence ノードで、サブクラスタ ペアごとに 2 台のコンプライアンス サーバを配置することを推奨します。クラスタ全体で 1 台のコンプライアンス サーバであってもサポートされますが、お勧めしません。

- Linux または Windows オペレーティング システムにデータベースをインストールできます。サポートされるオペレーティング システムとプラットフォームの要件の詳細については、次の該当するデータベースのマニュアルを参照してください。
  - https://www.postgresql.org/docs/manuals/ で入手可能な PostgreSQL のマニュアル
  - https://docs.oracle.com/en/database/database.html で入手可能な Oracle のマニュアル
- Cisco IM and Presence サービスは、フル Unified Communications モードでクラスタあたり合計 75,000 ユーザをサポートします。ユーザのサイジングにおいては、SIP/SIMPLE ユーザの数および XMPP ユーザの数を考慮する必要があります。SIP/SIMPLE ユーザは XCP アーキテクチャへの IM ゲートウェイ機能を利用するため、XMPP ユーザの方が若干パフォーマンスがよくなります。
- すべての eXtensible Communications Platform（XCP）通信およびロギングは GMT で実行および保管され、インストールされたロケーションに合せてローカライズされません。
- ユーザおよび連絡先リストを簡単に移行できるように、Cisco IM and Presence Bulk Administration Tool では、一括インポートの入力としてカンマ区切り値（csv）ファイルを使用した一括連絡先リスト インポートをサポートしています。

Cisco IM and Presence サービスによって使用されるポートの完全なリストについては、次の Web サイトで入手可能な『*Port Usage Information for Cisco IM and Presence*』を参照してください。

https://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html

連絡先リストとウォッチャ リストの推奨事項

（注）　このセクションで提示するガイドラインは、特定のテスト条件下で Cisco によって検証された事実に厳密に基づいています。この推奨事項の目的は、クラスタ内の連絡先リストとウォッチャ リストの管理に関して、IM and Presence 導入におけるプレゼンス ユーザの導入と分散を支援することです。

IM and Presence クラスタ

IM and Presence の標準導入は、3 つの IM and Presence サブクラスタ ペア（6 ノード）の 1 つのフル稼働しているクラスタで 45,000 人のプレゼンス対応ユーザをサポートするように設計されており、15k ユーザ IM and Presence VM テンプレートを使用して展開されます。

連絡先リストとウォッチャ リストに関する推奨事項は、クラスタ平均が、クラスタ内のユーザあたり 75 人のプレゼンス対応連絡先を超えないことです。この値は、ユーザあたり平均 100 人の総連絡先（それぞれのバディ リストで 75 人のプレゼンス対応ユーザと 25 人の非プレゼンス対応ユーザに分けられている）の検証テストから抽出されたものです。このセクションの後半では、75 人のプレゼンス対応ユーザを中心に説明します。これは、システムのパフォーマンスと拡張性に最も影響する要素だからです。

IM and Presence システムのパフォーマンスと安定性の管理を支援するには、IM and Presence 名簿テーブルを適切に維持、管理、監視することが重要です。このテーブルは、基本的にすべてのプレゼンス ユーザのエンドユーザ連絡先リストとウォッチャ リストで構成されています。

（注）　ユーザあたり 75 人のプレゼンス対応連絡先というクラスタ平均は、[連絡先リストの最大サイズ（ユーザごと）（Maximum Contact List Size (per user)）] と [ウォッチャの最大数（ユーザごと）（Maximum Watchers (per user)）] のサービス パラメータと同じではありません。これらのデフォルト値は、Cisco IM and Presence のリリース バージョンに応じて、それぞれ、150 と 200 です。

プレゼンス状態変更の影響

状態変更がシステムに与える影響を理解するために、標準的な作業日の 1 人のユーザの視点からイベントを検討してみます。Bob という名前のユーザがバディ リスト内に 75 人の連絡先を登録しており、その 75 人の連絡先もバディ リスト内に Bob を 1 人の連絡先として登録しているとします（ただし、ほとんどの導入で必ずしもあてはまるとは限りません）。

Bob が初めてデスクトップ Jabber クライアントにログインすると、75 件の通知が生成され、彼のバディ リスト内のすべての連絡先に送信されます。その後で、Bob が卓上電話機を使用して電話を掛けると、彼の状態を「電話中」に更新する、別の 75 件の通知が彼の連絡先に送信されます。Bob の状態変更ごとに、彼のバディ リスト内の連絡先あたり 1 件の通知が発行されます。ただし、Bob もその連絡先のバディ リストに登録されている場合です。

すべてのプレゼンス対応ユーザが、バディ リスト内のすべてのプレゼンス対応連絡先にステータス変更更新を発行します。ステータス変更には、電話機のハンドセットの持ち上げ、コールの発信、電話の切断、会議への参加などのアクションが含まれます。そのため、75 人のプレゼンス対応連絡先を持つすべてのユーザのすべてのアクションによって、最低 75 件の通知が生成されます。

たとえば、それぞれのバディ リストに 75 人の連絡先が登録されている、3,000 人のプレゼンス対応ユーザの導入を考えてみます。3,000 人すべてのユーザが同時に会議またはオールハンズ ミーティングに参加すると、225,000 件のプレゼンス更新通知が生成されます。同様に、9,000 人のプレゼンス ユーザの導入では、すべてのユーザが同時にプレゼンス ステータスの変化を引き起こすアクションを実行すると、675,000 件のプレゼンス更新通知が生成されます。これらの通知によって、システム リソースが使用され、特に、ピーク使用時間中のシステム パフォーマンスに影響が出ます。これが、ユーザをクラスタ全体に均等に分散させ、ユーザあたり 75 人の連絡先という推奨平均値を超えないようにすることが不可欠な理由です。

プレゼンス ユーザの分散

IM and Presence データベースの予算、つまり、最大許容連絡先エントリ数は、設定済みのプレゼンス ユーザの総数に、各ユーザがバディ リストに登録可能なプレゼンス連絡先の推奨平均数（75）を掛けて求めることができます。たとえば、45,000 人のユーザがフル稼働しているクラスタの推奨予算（IM and Presence 連絡先の最大数）は、次のようになります。

（45,000 人のユーザ）＊（ユーザあたり 75 人の連絡先）= クラスタの 3,375,000 人の IM and Presence 連絡先

それぞれのサブクラスタ内に 15,000 人のユーザが配置された 3 つのサブクラスタ ペア（6 ノード）が導入に存在する場合は、平均で次のようになります。

15,000 人のユーザ＊ユーザあたり 75 人の連絡先 = サブクラスタ ペアあたり 1,125,000 人の連絡先

すべての IM and Presence ユーザがバディ リストに 75 人以下の連絡先を登録している場合は、上記の計算で示したように、ユーザをサブクラスタ間で均等に分散することができます。ただし、一部のユーザがバディ リストに 75 人を超える連絡先を登録する必要がある場合は、次のセクションで説明する、カスタム分散が必要です。

ヒント　大量の連絡先（75 人を超える）を持つユーザは、そのすべてが同じ IM and Presence ノードに存在するのではなく、ノード全体に均等に分散されるようにしてください。

カスタム分散

ここでも、3 つのサブクラスタに 45,000 人のユーザが分散された、フル稼働の IM and Presence クラスタを考えてみます。たとえば、クラスタ内の 1,000 人のユーザがバディ リストに 500 人のプレゼンス対応連絡先を登録する必要があるとします。このケースでは、これらの 1,000 人のユーザで以下のことが必要です。

（1,000 人のユーザ）*（ユーザあたり 500 人の連絡先）= 500,000 個の IM and Presence データベース エントリ

クラスタ全体で許容される IM and Presence データベース エントリの最大数は 3,375,000 です。それぞれが 500 人の連絡先を持つ 1,000 人のユーザの場合を見積ったら、残りの使用可能な連絡先エントリは次のようになります。

3,375,000 - 500,000 = 2,875,000 の連絡先エントリがクラスタ内の残りの 44,000 人のプレゼンス ユーザで使用可能。

使用可能な連絡先エントリがクラスタ内の残りの 44,000 人のユーザの間で均等に分散されている場合は、次のようになります。

2,875,000/44,000 = ユーザあたり 65 人の連絡先の最大値

（注） 上の例では、500 人の連絡先を持つユーザを 3 つのサブクラスタ ペア間で均等に分散する必要があります。使用状況やリソース要件の変化に合わせて、IM and Presence ユーザの分散を頻繁に監視および調整することによってシステムの安定性を確保することも重要です。加えて、クラスタ内のいずれかのユーザに必要な連絡先の数がサービス パラメータ [連絡先リストの最大サイズ（ユーザごと）（Maximum Contact List Size (per user)）] のデフォルト値より高い場合は、そのパラメータの設定と [ウォッチャの最大数（ユーザごと）（Maximum Watchers (per user)）] の設定の両方をより高い値に変更する必要があります。

ステータス変更通知の影響

上の例では、ユーザあたり 500 人の連絡先があるカスタム分散では、均等に分散されたオプションのステータス変更あたり 75 件の通知と比較して、ステータス変更あたり 500 件の通知が生成されることになります。以降の例では、75 人の連絡先を持つ 1,000 人のユーザと 500 人の連絡先を持つ 1,000 人のユーザの影響の比較を示します。

- 1000 * 75 =（75,000 件の通知）/（3,600 秒、つまり、1 時間）= クラスタあたり 21 件の通知/秒またはサブクラスタ ペアあたり 7 件の通知/秒。
- 1000 * 500 =（500,000 件の通知）/（3,600 秒、つまり、1 時間）= クラスタあたり 139 件の通知/秒またはサブクラスタ ペアあたり 47 件の通知/秒。

モバイル & リモート アクセス

ユーザは VPN クライアントを使用せずに、企業のファイアウォールの外からコラボレーション ツールにアクセスできます。シスコのコラボレーション ゲートウェイを使用して、クライアントは公衆 Wi-Fi ネットワークやモバイル データ ネットワークなどのリモート ロケーションから社内ネットワークに安全に接続できます。

Cisco Unified Communications のモバイルおよびリモート アクセスは Cisco Collaboration Edge アーキテクチャの中核を成します。Cisco Jabber などのエンドポイントが企業ネットワーク外にある場合に、Cisco Unified Communications Manager（Unified CM）への登録、呼制御、プロビジョニング、メッセージング、およびプレゼンスの機能を使用することができるようになります。Cisco Expressway は、Unified CM 登録にセキュアなファイアウォール トラバーサルと回線側サポートを提供します。

サードパーティ製 SIP または H.323 デバイスは、ネイバー ゾーンで Cisco Expressway に接続されている Cisco VCS に登録でき、必要に応じて SIP トランクを介して Unified CM に登録されたデバイスと相互運用できます。

Cisco Expressway サーバのセットアップ方法については、次の Web サイトで入手可能な『*Cisco Expressway Basic Configuration Deployment Guide*』および『*Mobile and Remote Access via Cisco Expressway Deployment Guide*』の最新バージョンを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

モバイルおよびリモート アクセスを使用する場合、次の Jabber 機能はサポートされません。

- UDS の以外のディレクトリ アクセス機能
- リモート エンドポイントに対する証明書のプロビジョニング
- ファイル転送
- デスクフォン制御モード

サードパーティ製プレゼンス サーバ統合

Cisco IM and Presence サービスでは、SIP アプリケーションと SIMPLE アプリケーションを Cisco Unified Communications ソリューションに統合できるよう、SIP と SIP for Instant Messaging and Presence Leveraging Extensions（SIMPLE）に基づくインターフェイスを提供しています。これにより、サードパーティ製のプレゼンス サーバやアプリケーションをこの SIP/SIMPLE と連携して設定し、統合して、プレゼンス集約やフェデレーションを提供できます。

リモート呼制御（RCC）用 Microsoft Communications Server

Microsoft 製品のセットアップ、設定、および配置に関するすべての情報は、次の Web サイトにあるマニュアルを参照してください。

https://www.microsoft.com/

シスコは、Microsoft Communications 製品の設定、配置、またはベスト プラクティス手順は提供していませんが、Cisco IM and Presence サービスと Microsoft Lync との統合に関する次のガイドラインを提供しています。

シスコは、機能の相互運用性と、Cisco IM and Presence サービスを Microsoft Lync と統合するための設定手順を示すマニュアルを作成しました。このマニュアルには次の URL でアクセスできます。

https://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

Cisco IM and Presence サービスと Microsoft Lync の統合に関するガイドライン

次のガイドラインは、Cisco IM and Presence サービスと Microsoft Lync を統合するときに適用されます。

- Cisco IM and Presence サービスと Microsoft Lync との通信には、SIP/SIMPLE インターフェイスが使用されます。ただし、Microsoft Lync は SIP 経由の Computer-Supported Telecommunications Applications（CSTA）トラフィックをトンネルします。したがって、Cisco IM and Presence サービス上の CTI ゲートウェイは、Click to Call の電話制御のために CSTA-CTI 変換を処理するように設定する必要があります。
- リモート呼制御用の Microsoft Lync とともに Cisco IM and Presence サービスを配置する場合は、Cisco IM and Presence サービス クラスタを形成するサーバの単一サブクラスタ ペアで構成する必要があります。
- 次の表では、プラットフォームごとのサポートされるユーザ数を示します。ユーザ数は、IM and Presence サービス プラットフォームに関係なく、Unified CM プラットフォームの相当数にのみ基づきます。

Cisco Unified Communications Manager VM 設定テンプレート	サーバごとのサポートされる Microsoft Office Communicator または Lync ユーザ数	クラスタごとのサポートされる Microsoft Office Communicator または Lync ユーザ数
1,000 ユーザ	1,000	4,000
2,500 ユーザ	2,500	10,000
7,500 ユーザ	7,500	30,000
10,000 ユーザ	10,000	40,000

- LDAP、Unified CM、および Microsoft Lync で、同じエンドユーザ ID を設定する必要があります。これにより、Active Directory（AD）による Microsoft Lync 認証と Unified CM のエンドユーザ設定との競合、さらには Unified CM 上でのユーザの電話制御との競合を防止できます。

  Active Directory については、General、Account、および Communications のユーザのプロパティですべて同一の ID を使用することを推奨します。Cisco IM and Presence サービス ユーザの一貫性を維持するために、Unified CM で LDAP 同期と LDAP 認証を有効にする必要があります。
- Microsoft Lync のホスト認証に Cisco IM and Presence サービス パブリッシャとサブスクライバを含めるように設定する必要があります。
- Microsoft Lync プロパティのスタティック ルートによって SIP メッセージが Cisco IM and Presence サービスにルーティングされるように設定する必要があります。
- Cisco IM and Presence サービスで発着信のアクセス コントロール リスト（ACL）を設定して、Microsoft Lync との通信を許可する必要があります。
- Unified CM で各ユーザのプレゼンスを有効にするだけでなく、Cisco IM and Presence サービス設定で、各ユーザに Microsoft Lync の使用を許可する必要があります。
- Microsoft Lync のログイン時に、Microsoft Lync と Microsoft Communications Server 間での設定情報の交換や、Cisco IM and Presence サービス CTI ゲートウェイとの初期通信のために必要となる帯域幅を考慮に入れる必要があります。
- ディレクトリ番号からそれに対応するユーザを検索するリバース ルックアップの問題に対処するには、次の Web サイトで入手可能な『*Release Notes for Cisco IM and Presence*』に記載されているガイドラインを使用してください。

  https://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html

クラウド内サービスとアーキテクチャ

ここでは、Cisco IM and Presence サービスのクラウド内サービスとアーキテクチャについて説明します。このホステッド サービスは、オンプレミス ソリューションと同じユーザ エクスペリエンスを提供します。

Cisco WebEx Messenger

Cisco WebEx Messenger は、同期および非同期コラボレーションに対応したマルチテナント型 Software-as-a-Service（SaaS）プラットフォームです。WebEx Messenger プラットフォームは、Cisco WebEx Collaboration Cloud 内でホストされ、コラボレーション アプリケーションと統合を可能にします。これにより、会社およびエンド ユーザが自分の作業環境をカスタマイズすることが可能になります。Cisco WebEx Messenger サービスの詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

https://developer.cisco.com/web/webex-developer

Cisco Collaboration Cloud の詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

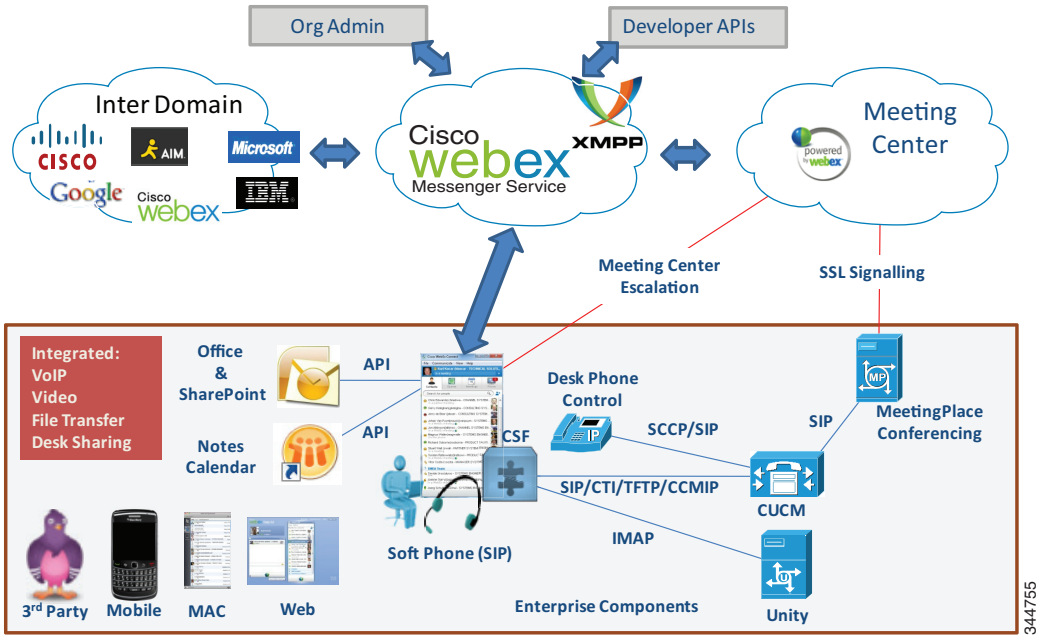
https://www.cisco.com/en/US/solutions/ns1007/collaboration_cloud.html

Cisco WebEx Messenger サービスの配置

Cisco WebEx Messenger ソリューションの配置は、図 20-32 に示すように、次のコンポーネントで構成されています。

- プレゼンス、インスタント メッセージング、VoIP、PC 間ビデオ、メディア転送（スクリーン キャプチャとファイル転送）、およびデスクトップ共有のための、Cisco WebEx Messenger XMPP クラウド プラットフォームへのセキュア接続（SSL と AES）
- Cisco WebEx Meetings
- 他の WebEx Messenger 組織との XMPP フェデレーション、サードパーティ製 XMPP クライアント、および XMPP インスタント メッセージング（IM）ネットワーク
- 呼制御、ボイス メッセージング、およびコール履歴のための、Cisco Unified Communications 統合
- Microsoft Outlook および IBM Lotus Notes カレンダー統合
- プレゼンス、Click-to-Communicate 機能のための、Microsoft Outlook への統合

図 20-32　Cisco WebEx Messenger サービスの配置



中央集中型の管理

Cisco WebEx Messenger サービスでは、組織全体にわたるソリューションを管理するための Web ベースの管理ツールを提供しています。Cisco WebEx Messenger サービス ユーザは、Cisco WebEx 管理ツールを介して設定および管理されます。これにより、管理者は機能およびサービスに対してセキュリティとポリシーの基本制御を設定できます。これらのポリシーは、企業全体、グループごと、または個別に適用できます。ユーザ データベースをプロビジョニングにするためのさまざまな方法があります。これらの方法については、次の Web サイトで入手可能な『Cisco WebEx Administrator's Guide』を参照してください。

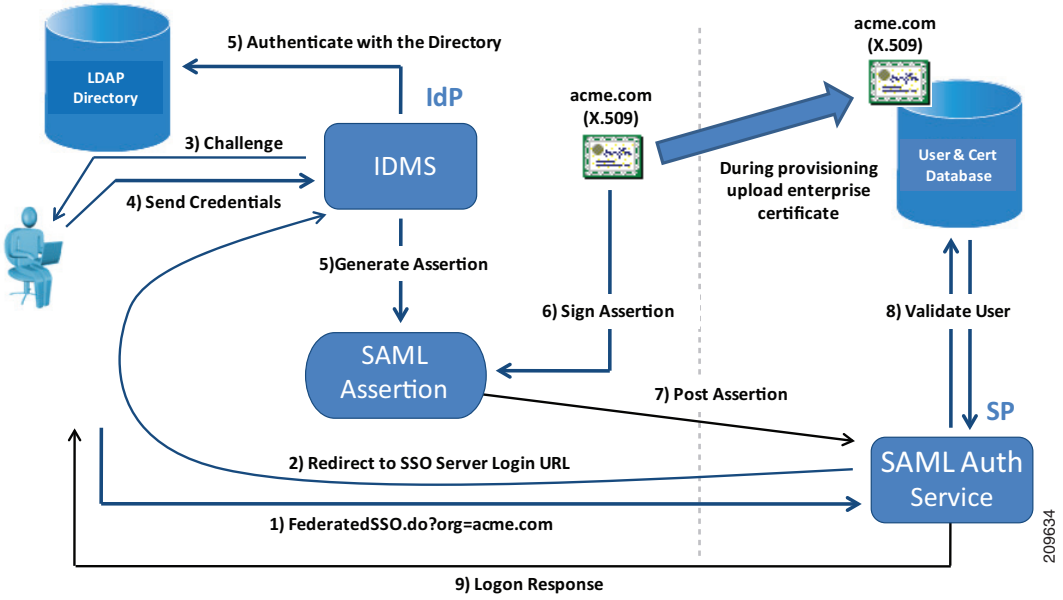
https://www.webex.com/webexconnect/orgadmin/help/index.htm

シングル サインオン

シングル サインオン（SSO）を使用すると、会社は Security Assertion Markup Language（SAML）サポートなどのオンプレミス SSO システムを使用でき、ユーザが会社のログイン クレデンシャルを使用してソリューション内の Unified Communications アプリケーションに安全にログインできるようにすることで、Cisco WebEx Messenger または IM and Presence サービスの管理を簡素化できます。ユーザのログイン クレデンシャルはシスコに送信されないため、ユーザの会社のログイン情報は保護されます。図 20-33 に、Cisco WebEx Messenger および Unified CM へのユーザ ログイン時に発生するクレデンシャル ハンドシェイクを示します。

（注）　Cisco Jabber を Cisco WebEx Meeting Server とともに配置する場合、Cisco Unified CM と WebEx Meeting Server が同じドメインに存在する必要があります。

図 20-33　Cisco WebEx Messenger サービスでのユーザ ログイン認証プロセス



ユーザ アカウントは、ユーザが初めて Cisco IM クライアントにログインしたときに自動的に作成されるように設定できます。ユーザの会社のログイン アカウントが非アクティブになると、そのユーザは Cisco WebEx Messenger サービスにアクセスできなくなります。

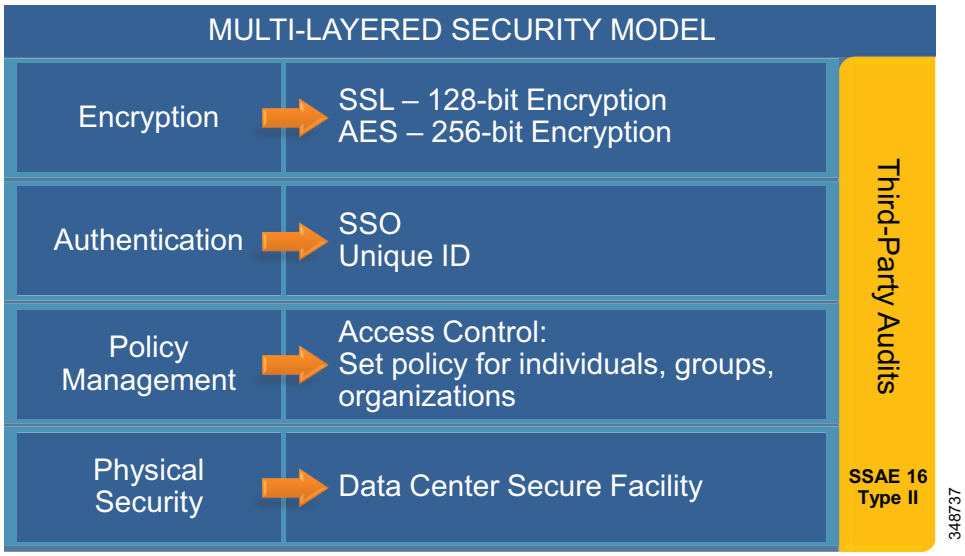
WebEx Messenger サービスを使用したシングル サイン オンの詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

https://developer.cisco.com/web/webex-developer/sso-reference

セキュリティ

Cisco WebEx セキュリティ モデルは、セキュリティの機能レイヤで構成されています。図 20-34 に、各レイヤを構成する、独立しているが相互に関連する要素を示します。

図 20-34　WebEx セキュリティ モデル



最下位層は、Cisco WebEx データセンターの物理セキュリティを示しています。すべての従業員は、広範なバックグラウンド チェックを通過し、データセンターに入るためのデュアルファクタ認証を実行する必要があります。

次のレベルのポリシー管理では、WebEx Messenger 組織管理者が、個々のユーザ、グループ、または Cisco WebEx Messenger 組織全体に異なるポリシーを設定することによってアクセス コントロール レベルを設定し、管理できます。外部ユーザまたはドメインに固有のホワイトリスト ポリシーを作成して、インスタント メッセージング交換を許可できます。Cisco WebEx Messenger 組織モデルでは、ユーザ ベース全体に固有の役割やグループを作成することもでき、管理者は特定の権限を役割やグループに割り当てたり、組織全体に対してアクセス コントロールなどのポリシーを設定したりできます。

Cisco WebEx Messenger サービスへのアクセスは、認証レイヤで制御されます。いずれのユーザも一意のログインとパスワードを所有します。パスワードが保存されたり、クリア テキストの E メールで送信されたりすることはありません。パスワードを変更できるのは、エンド ユーザ自身だけです。管理者は、次のログイン時にエンド ユーザがパスワードを変更するように、パスワードのリセットを選択できます。また、管理者は、Cisco WebEx Messenger サービスと企業のディレクトリとの間のシングル サイン オン（SSO）統合を使用して、エンドユーザのアクセス管理を簡略化することもできます。シングル サイン オン統合は、Identity Management System（IDMS）を使用して実現されます。

暗号化レイヤでは、Cisco WebEx Messenger ユーザ間のすべてのインスタント メッセージング通信が暗号化されます。Cisco WebEx Messenger ユーザと Messenger Collaboration クラウドのサーバとの間のすべてのインスタント メッセージング通信は、SSL 暗号化を使用してデフォルトで暗号化されます。256 ビットの AES レベル暗号化を使用して IM 通信をエンドツーエンドで暗号化できる追加のセキュリティ レベルを使用できます。

Cisco WebEx Messenger プラットフォームでは、SSAE 16 Type II 監査などのサードパーティによる監査を使用して、カスタマーに半年ごとに別個のセキュリティ レポートを提供します。カスタマーは、シスコのセキュリティ組織に要求すればいつでもこのレポートを確認できます。その他の Cisco WebEx Messenger サービスのセキュリティについては、次の Web サイトで入手可能な『*Cisco WebEx Connect Security White Paper*』を参照してください。

https://www.cisco.com/en/US/products/ps10528/prod_white_papers_list.html

ファイアウォール ドメインのホワイト リスト

アクセス コントロール リストは、webex.com ドメインおよび webexconnect.com ドメインと、この両ドメインのすべてのサブドメインからのすべての通信を許可するように明確に設定する必要があります。WebEx Messenger プラットフォームからエンドユーザにユーザ名とパスワードを通知する電子メールが送信されます。これらの電子メール メッセージは mda.webex.com ドメインから発信されます。

インスタント メッセージのロギング

Cisco WebEx Messenger サービスのインスタント メッセージング通信は、ユーザがログインしているパーソナル コンピュータのローカル ハード ドライブに記録されます。インスタント メッセージのロギングは Cisco WebEx Messenger サービスの機能です。この機能は Org Admin ツールでポリシーを使用して有効にすることができます。

エンド ユーザは、ロギングの詳細、ロギングの有効化または無効化、およびログの保存期間を設定できます。これらのメッセージ履歴設定は、IM クライアント プリファレンスの [全般（General）] にあります。

詳細な監査機能や e-Discovery（電子情報の開示）機能を必要とする場合は、サードパーティ製のソリューションを利用することも検討してください。現在シスコでは、インスタント メッセージング通信の詳細な監査をサポートしていません。ただし、Cisco WebEx Messenger サービスでは、ユーザ間で交換されるインスタント メッセージのロギングとアーカイブを実行できます。ログのアーカイブは、サードパーティの SaaS アーカイブ サービスを使用して実行できます。または、ログをオンプレミス SMTP サーバにセキュアに配信できます。

インスタント メッセージのアーカイブの詳細については、次の Web サイトで入手可能な『Cisco WebEx Administrator's Guide』を参照してください。

https://www.webex.com/webexconnect/orgadmin/help/index.htm

Cisco WebEx Messenger サービスのキャパシティ プランニング

エンドユーザが WebEx Messenger サービスにログインして、プレゼンス、インスタント メッセージング、および Voice over IP（VoIP）コーリングなどの基本機能を利用するために必要なものは、56 kbps ダイヤルアップ インターネット接続だけです。ただし小規模のオフィスや支店で、ファイル転送、スクリーン キャプチャ、および PC 間ビデオ コールなどの高度な機能を利用するには、512 kbps 以上のブロードバンド接続が必要です。高品位 720p などの高い品質のビデオの場合、推奨される最小の帯域幅接続は 2 Mbps です。

ネットワークおよびデスクトップの要件の詳細については、次の Web サイトで入手可能な『Cisco WebEx Administrator's Guide』を参照してください。

https://www.webex.com/webexconnect/orgadmin/help/index.htm

Cisco Webex Messenger 配置でのネットワーク要件については、次の Web サイトで入手可能です。

https://www.webex.com/webexconnect/orgadmin/help/17161.htm

Cisco WebEx Messenger サービスのハイ アベイラビリティ

WebEx Messenger は、Software as a Service（SaaS）アプリケーションです。エンドユーザが IM クライアントにログインするには、エンドユーザ デバイスをインターネットに接続する必要があります。標準のインターネット接続があれば、利用できます。エンド ユーザがリモートの場合は、WebEx Messenger サービスにログインするために、そのユーザが会社の VPN を介して接続する必要はありません。Cisco WebEx Messenger サービスの IM クライアントは、可用性の高い冗長なトポロジに配置できます。Cisco WebEx Messenger Software-as-a-Service アーキテクチャの配置は、この項で説明する各種のネットワークおよびデスクトップ要件で構成されます。

高可用性

マルチテナント型 Software-as-a-Service アーキテクチャを使用していて、グループ内のいずれかの個別サーバが何らかの理由で停止した場合、要求を Cisco WebEx Messenger プラットフォーム内の利用可能な他のサーバにルーティングできます。

Cisco WebEx Network Operations Team は、Cisco WebEx Network Operations Center（NOC）から Cisco WebEx Collaboration Cloud を毎日 24 時間アクティブにモニタします。Cisco WebEx テクノロジーの概要については、次の Web サイトを参照してください。

https://www.cisco.com/en/US/solutions/ns1007/collaboration_cloud.html

冗長性、フェールオーバー、およびディザスタ リカバリ

Cisco WebEx のグローバル サイト バックアップ アーキテクチャは、電源異常、自然災害による停電、放電過多、ネットワーク容量過多、その他のタイプのサービス中断を処理します。グローバル サイト バックアップでは、手動と自動の両方のフェールオーバーをサポートします。手動フェールオーバー モードは通常、メンテナンス時間枠で使用されます。自動フェールオーバー モードは、サービス中断によるリアルタイム フェールオーバーの場合に使用されます。

グローバル サイト バックアップは、エンド ユーザに対して自動的かつ透過的であり、すべてのユーザが利用できます。フェールオーバー可能なユーザ数に制限はありません。

グローバル サイト バックアップは、次の主要コンポーネントで構成されます。

- グローバル サイト サービス：ネットワーク レベルでトラフィックのモニタリングとスイッチングを行います。
- データベース複製：プライマリ サイトでのデータ トランザクションをバックアップ サイトに確実に転送します。
- ファイル複製：ファイル変更が、プライマリ サイトとバックアップ サイト間で同期されるようにします。

Cisco WebEx Messenger サービスの設計に関する考慮事項

Cisco WebEx Messenger は、Software as a Service モデルとして配置されるため、設計と配置の考慮事項は最小限で済みます。Cisco WebEx Messenger ソリューションには、Windows と Mac デスクトップ、および一般的なモバイル デバイスで使用可能なクライアント オプションがあります。

サードパーティ製 XMPP クライアントから Cisco WebEx Messenger サービスへの接続

シスコでは、他の XMPP クライアントによる Cisco WebEx Messenger サービスへの接続を公式にサポートしていませんが、XMPP プロトコルの性質上、エンド ユーザはさまざまな XMPP クライアントで WebEx Messenger サービスのクレデンシャルを使用してプレゼンス クラウドに接続できます。XMPP ソフトウェア クライアントのリストは、次の Web サイトで入手できます。

https://xmpp.org/software/clients.shtml

組織のポリシーは、サードパーティ製の XMPP クライアントに適用できません。また、エンドツーエンド暗号化、デスクトップ共有、ビデオ コール、PC 間コール、および電話会議などの機能は、サードパーティ製のクライアントではサポートされていません。WebEx Messenger サービス以外の XMPP IM クライアントが WebEx Messenger サービス ドメインに対して認証できるようにするには、DNS SRV レコードを更新する必要があります。特定の DNS SRV エントリは、Cisco WebEx 管理の [設定と IM フェデレーション（Configuration and IM Federation）] で見つけることができます。

Cisco WebEx 管理の [設定と XMPP IM クライアント（Configuration and XMPP IM Clients）] で、Messenger サービス以外の XMPP クライアントの使用を明示的に許可する必要があります。

サードパーティ製 XMPP クライアントが WebEx Messenger プラットフォームに接続できるようにする方法の詳細については、次の Web サイトで入手可能な『Cisco WebEx Administrator's Guide』を参照してください。

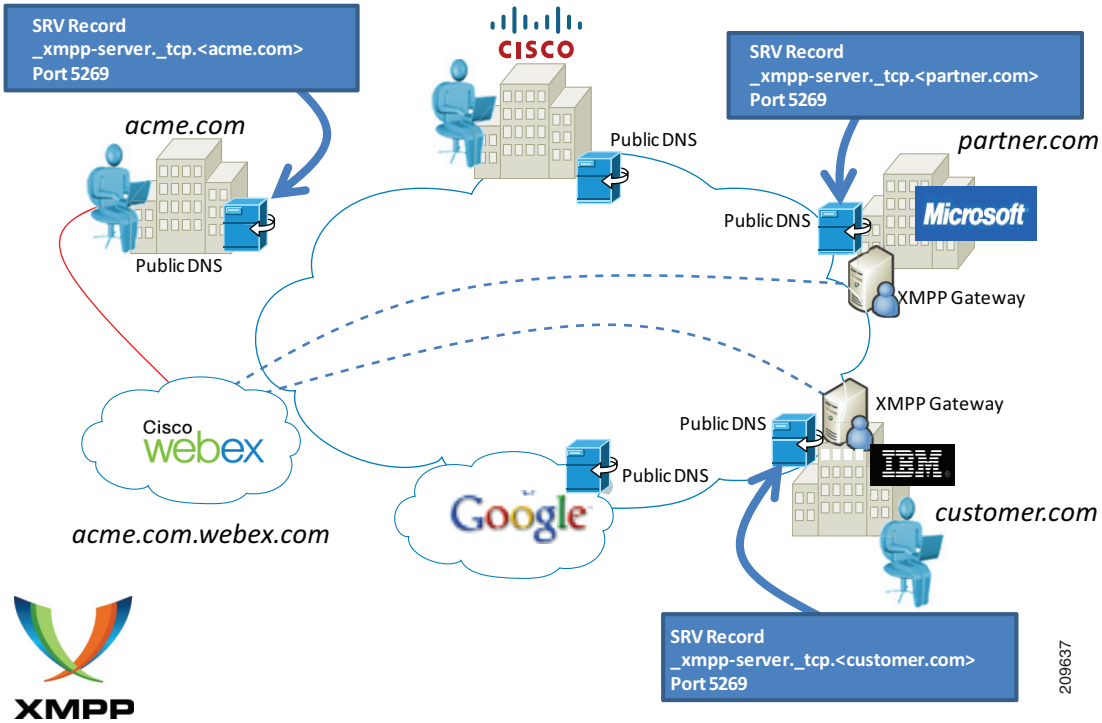
https://www.webex.com/webexconnect/orgadmin/help/index.htm

サードパーティ製 XMPP クライアントを使用したインスタント メッセージングおよびプレゼンス フェデレーション

Cisco WebEx Messenger サービス ネットワークは、GoogleTalk および Jabber.org などの XMPP ベースのインスタント メッセージング ネットワークとフェデレーションできます（図 20-35 を参照）。XMPP に基づいた公衆インスタント メッセージング ネットワークのリストは、次の Web サイトで入手できます。

https://xmpp.org/

図 20-35　ドメイン間フェデレーション



現在、WebEx Messenger サービスには Yahoo! Messenger および Windows Live Messenger との相互運用性はありませんが、フェデレーション ゲートウェイ経由で AIM とフェデレーションすることはできます。

その他のリソースおよびドキュメンテーション

『Cisco WebEx Administrator's Guide』は、次の Web サイトで入手できます。

https://www.webex.com/webexconnect/orgadmin/help/index.htm

モバイル コラボレーション

改訂日：2018 年 3 月 1 日

モバイル コラボレーション ソリューションおよびアプリケーションを使用すれば、モバイル ワーカーはどこからでも会社の IP コミュニケーション環境の機能を利用できます。モバイル コラボレーション ソリューションを使用すると、モバイル ユーザは業務上の電話をさまざまなデバイスで扱うことができ、オフィスビル内の移動中やオフィス間の移動中、地理的に会社外のロケーション間の移動中に企業アプリケーションにアクセスできます。モバイル コラボレーション ソリューションでは、モバイル ワーカーは持続的に到達可能性を得ることができ、さまざまな場所での移動中や作業中の生産性を向上させることができます。

モバイル コラボレーション ソリューションは、主に次の 2 つのカテゴリに分けられます。

- 社内型モビリティ

  このタイプのモビリティは、企業の敷地内での移動に限られます。

- 社外型モビリティ

  このタイプのモビリティは、企業インフラストラクチャの外部にまで至るモビリティを指し、一般には何らかの形のインターネット、モバイル ボイス ネットワーク、およびモバイル データ ネットワーク通過が含まれます。

社内型モビリティは、企業のネットワーク境界内に使用が制限されます。この境界は単一の物理的な建物のみを範囲としても、近くの、あるいは離れた複数の物理的な建物を範囲としても、またはホーム オフィスまで広がったネットワーク インフラストラクチャの場合、企業により制御され管理されるホーム オフィスを範囲としてもかまいません。

一方、社外型モビリティには、企業インフラストラクチャによるインターネットまたはモバイル プロバイダー インフラストラクチャへのブリッジングが含まれ、ユーザは公共およびプライベート ネットワークを使用して企業サービスに接続できます。これらの 2 つのタイプのモビリティ間の線引きはあいまいな場合もあり、特にモバイル デバイスが、インターネットまたはモバイル データおよびモバイル音声ネットワークを介したコラボレーション サービスで企業に接続するようなシナリオの場合に顕著です。

社内型モビリティは、フィーチャ セットおよびソリューションに基づき、次の 3 つの主要な領域に分けられます。

- キャンパス/単一サイト モビリティ

  このタイプの企業モビリティでは、ユーザは、一般に単一の IP アドレス空間および PSTN 入出力境界により区切られた単一の物理的な場所内を動き回ります。このタイプのモビリティには、1 つの物理ネットワーク ポートから他のポートへの電話の移動や、無線インフラストラクチャ アクセス ポイント間でのワイヤレス LAN デバイスのローミング、ユーザが一時的に異なる領域への特定の電話機に企業電話番号などのデバイス プロファイルを適用する Cisco エクステンション モビリティ（EM）などの操作や機能が含まれます。

- マルチサイト モビリティ

  このタイプのモビリティでは、ユーザは社内の物理的な場所の間を移動します。この移動には、一般的に IP アドレス空間や PSTN 入出力境界を越えることも含まれます。このタイプのモビリティには、キャンパス モビリティと同じタイプの操作や機能（物理的なハードウェアの移動、WLAN ローミング、Cisco エクステンション モビリティ）が含まれますが、それらは企業内のそれぞれのサイトに複製されます。さらに、デバイス モビリティ機能を利用して、ユーザがサイト間でデバイスを移動させると、電話のコールがローカル サイトのイーグレス ゲートウェイを介してルーティングされ、メディア コーデックが適切にネゴシエートされ、コール アドミッション制御メカニズムでデバイスの場所が認識されるようにできます。

- リモート サイト モビリティ

  このタイプのモビリティでは、ユーザは社外のロケーションに移動しても、仮想的に企業ネットワークをリモート ロケーションまで拡張して、何らかの安全な形式で会社に接続できます。このタイプのモビリティには、VPN ベースのリモート企業接続または VPN なしのリモート企業接続が含まれます。VPN リモート企業接続は、Cisco Virtual Office などのリモート テレワーカー ソリューションや、VPN 対応電話機、クライアント、Office Extend Access Point 機能などのその他のリモート接続方法が含まれます。VPN なしのリモート企業接続は、リバース プロキシ ファイアウォール セッション ベースの接続を有効にし、VPN トンネルを必要とせずにリモート エンドポイントとクライアントが企業に接続できるようにします。VPN なしのリモート接続は、Cisco Expressway モバイル & リモート アクセス機能によりサポートされます。

- クラウドおよびハイブリッド サービス モビリティ

  このモビリティ タイプには、クラウド コラボレーション サービスや、クラウドおよびオンプレミス コラボレーション サービスの統合などがあります。これにはクラウドからのサービスの提供が関係するため、これらのサービスを利用するのに、インターネットに接続可能などのデバイスでも使用できます。ユーザが社内外のいずれにいるかどうか、企業ネットワークまたは別のネットワークに接続しているかどうか、移動中であるかどうかなどに関係なく、ユーザはこれらのクラウド サービスを利用できます。

社外型モビリティは、大まかに次の 2 つの Cisco ソリューション セットに分けられます。

- Cisco Unified Mobility

  Cisco Unified Communications Manager（Unified CM）の一部である Cisco Unified Mobility 機能スイートにより、モバイル ユーザのエンタープライズ番号をユーザのモバイルまたはリモート デバイスに関連付け、エンタープライズ ネットワーク上のユーザの固定の会社のデスクフォンと、モバイル ボイス プロバイダー ネットワーク上のユーザのモバイル デバイスとを接続できます。このタイプの機能は、固定モバイル コンバージェンスと呼ばれることがあります。

- Cisco Mobile クライアント ソリューション

  Cisco Mobile クライアント アプリケーションは、デュアル モード スマート フォンおよび他のモバイル デバイスで実行され、企業のコラボレーション アプリケーションとサービスへのアクセスを提供します。デュアルモード電話には、802.11 ワイヤレス LAN ネットワークと携帯電話音声およびデータ ネットワークの両方に接続できる二重無線アンテナが装備されています。モバイル デバイスに配置された Cisco Mobile クライアントにより、モバイル デバイスは、エンタープライズ ワイヤレス LAN 経由またはパブリックまたはプライベートの Wi-Fi ホット スポットまたはモバイル データ ネットワークを介してインターネット経由で Cisco Unified CM に登録し、次いで IP を介した音声コールとビデオ コールの送受信用のエンタープライズ IP テレフォニー インフラストラクチャを利用できます。デュアル モード電話では、モバイル ユーザが企業の WLAN に関連付けされていない場合、またはこれらのデバイスでエンタープライズ ネットワークに安全に接続されていない場合、電話のコールはモバイル音声プロバイダー ネットワークを使用して行われます。モバイル デバイスの音声サービスとビデオ サービスを有効にするだけでなく、Cisco Mobile クライアントでは、音声とインスタント メッセージング、プレゼンス、エンタープライズ ディレクトリへのアクセスなどの他のコラボレーション サービスへもアクセスできます。

特に断りがない限り、この章で説明するさまざまなアプリケーションと機能は、すべての Cisco Unified Communications 配置モデルに適用されます。

この章ではまず、モビリティ機能と企業インフラストラクチャ内で利用可能なソリューションについて説明します。これには、キャンパス/単一サイトの配置、マルチサイトの配置、さらにはリモート サイトの配置での、機能検証や設計上の考慮事項が含まれます。この一連の包括ソリューションは、企業クラスのコミュニケーションや物理ロケーションに関係しない生産性の改善などを含め、社内のモバイル ワーカーに多くの利点をもたらします。この社内型モビリティに関する説明を踏まえて、モバイル プロバイダーおよびインターネット プロバイダーのインフラストラクチャおよび機能を活用した、社外型モビリティ ソリューションを検証します。これらのソリューションにより、安定した企業モビリティ インフラストラクチャの上に構築できる高度なモバイル機能とコミュニケーション フローを活用するための企業ネットワーク インフラストラクチャとプロバイダー ネットワーク インフラストラクチャのモバイル機能のブリッジングが可能になります。

この章では、企業のコラボレーション モビリティ ソリューションのモビリティ アーキテクチャ、機能性、および設計と配置の示す意味について包括的に検証します。この章の分析と説明は、大まかに次のような構成になっています。

- 社内型モビリティ
  - キャンパス企業モビリティ（21-4 ページ）
  - マルチサイト企業モビリティ（21-12 ページ）
  - リモート企業モビリティ（21-27 ページ）
  - クラウド サービスとハイブリッド サービスのモビリティ（21-36 ページ）
- 社外型モビリティ
  - Cisco Unified Mobility（21-51 ページ）
  - シスコのモバイル クライアントおよびデバイス（21-81 ページ）

この章の変更点

表 21-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 21-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Jabber 対応の Apple プッシュ通知サービス（APNs）	Cisco Jabber for iPhone and iPad 対応の Apple プッシュ通知サービス（APNs）（21-108 ページ）	2018 年 3 月 1 日
Cisco Jabber でのリフレッシュ トークンを使用した OAuth 2.0	Cisco Jabber とリフレッシュ トークンを使用した OAuth でのログイン フロー（21-109 ページ）	2018 年 3 月 1 日

社内型モビリティ

この項では、社内で使用可能なモビリティ機能およびソリューションについて検証します。この検証には、次のタイプの企業モビリティのアーキテクチャ、機能性、および設計と配置の意味に関する説明が含まれます。

- キャンパス企業モビリティ（21-4 ページ）
- マルチサイト企業モビリティ（21-12 ページ）
- リモート企業モビリティ（21-27 ページ）
- クラウド サービスとハイブリッド サービスのモビリティ（21-36 ページ）

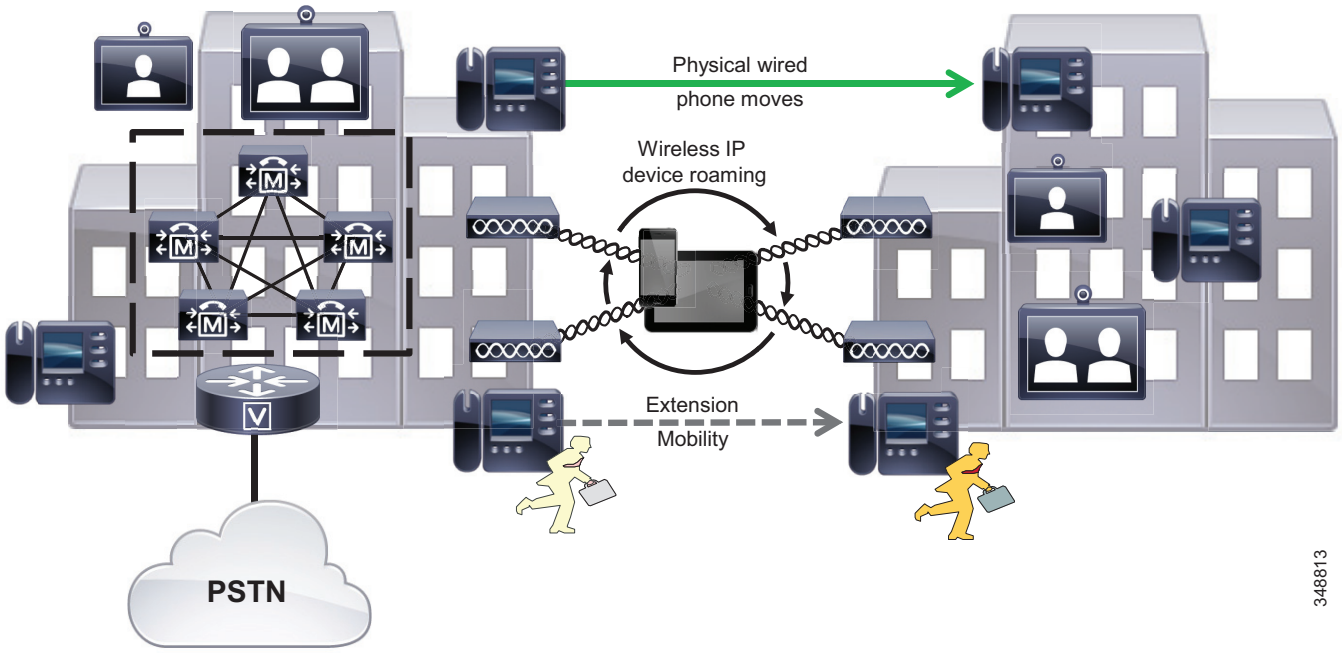
キャンパス企業モビリティ

キャンパスまたは単一サイトの企業モビリティは、一般に単一の IP アドレス空間および PSTN 入出力境界により区切られた単一の物理的な場所内のモビリティを指します。ここでのモビリティには、この物理ロケーション内でのユーザの移動だけではなく、エンドポイント デバイスの移動も含まれます。

キャンパス企業モビリティのアーキテクチャ

図 21-1 に示すように、キャンパス企業モビリティのアーキテクチャは、（図のように）近接する単一の建物または複数の建物を含む単一の物理的な場所に基づいており、ユーザはキャンパス内を自由に移動でき、IP および PSTN 接続を維持できます。一般にキャンパス配置には、単一 IP アドレス空間および PSTN 入出力境界によって区切られた PSTN およびインターネット プロバイダー ネットワークへの、共有一般接続または接続セットが含まれます。この企業キャンパス内のすべてのユーザは、一般ネットワーク インフラストラクチャに接続され、一般ネットワーク インフラストラクチャから到達可能です。

図 21-1　　キャンパス企業モビリティのアーキテクチャ



キャンパス モビリティのタイプ

企業キャンパス内のモビリティには一般的に、デバイス、ユーザ、またはその両方のキャンパス インフラストラクチャ全体の移動が含まれます。シスコ コラボレーション展開内のキャンパス企業モビリティは主に、有線電話機の物理的な移動、ワイヤレス デバイスの移動、電話機や通話ソフトウェアを持たないユーザの移動の 3 つに分けられます。移動のタイプについては後で説明します。

物理的な有線デバイスの移動

図 21-1 に示すように、物理的な有線電話機の移動は、キャンパス インフラストラクチャ内で簡単に行えます。このタイプの電話機の移動は、建物の単一階内、建物の複数階にわたって、またはキャンパス内の建物間で発生することが考えられます。従来の、物理的な電話機のポートが特定のオフィス、パーティション、または建物内のその他の空間に固定されている PBX 配置とは異なり、IP テレフォニーの配置では、電話はネットワーク インフラストラクチャの任意の IP ポートにつないで IP PBX に接続できます。

Cisco 環境では、これは単に Cisco Unified IP Phone または Cisco TelePresence System エンドポイントをネットワークから取り外し、キャンパス内の他の場所に運んで他の有線ネットワーク ポートに接続するだけのことです。新しいネットワーク ロケーションに接続すると、この電話が Unified CM に再登録され、前のロケーションと同じように発信や着信ができます。

物理デバイスのこれと同じ移動は、有線 PC で実行するソフトウェアベースの電話にも適用されます。たとえば、Cisco IP Communicator または Cisco Jabber を実行しているラップトップ コンピュータを、キャンパス内のあるロケーションから別のロケーションへ移動でき、ラップトップを新しいロケーションのネットワーク ポートに接続すると、ソフトウェアベースの電話を Cisco Call Control に再登録して、電話の呼処理を再開できます。

キャンパス内の物理的なデバイス モビリティに対応するには、電話デバイスやソフトウェアベースの電話を実行しているコンピュータを物理的に移動する際は、新しいロケーションで使用されるネットワーク接続の IP 接続、接続速度、Quality of Service、セキュリティ、およびインライン パワーや動的ホスト制御プロトコル（DHCP）などのネットワーク サービスが前の場所のものと同じであるよう注意してください。これらの接続パラメータ、サービス、および機能が同じでないと、機能が低下し、場合によっては、機能が完全に失われます。

ワイヤレス デバイス ローミング

キャンパス エッジで無線ネットワークに接続できるよう無線 LAN ネットワークが配置されている場合、ワイヤレス デバイスは、図 21-1 で示すように、企業キャンパス全体を移動またはローミングできます。

ワイヤレス デバイスの例には、Cisco Unified Wireless IP Phone 7925G および 8821 などのワイヤレス デバイス、無線で接続した Cisco DX80、および Cisco Jabber などの Cisco Mobile クライアントなどが含まれます（シスコのモバイル クライアントおよびデバイス（21-81 ページ）を参照）。

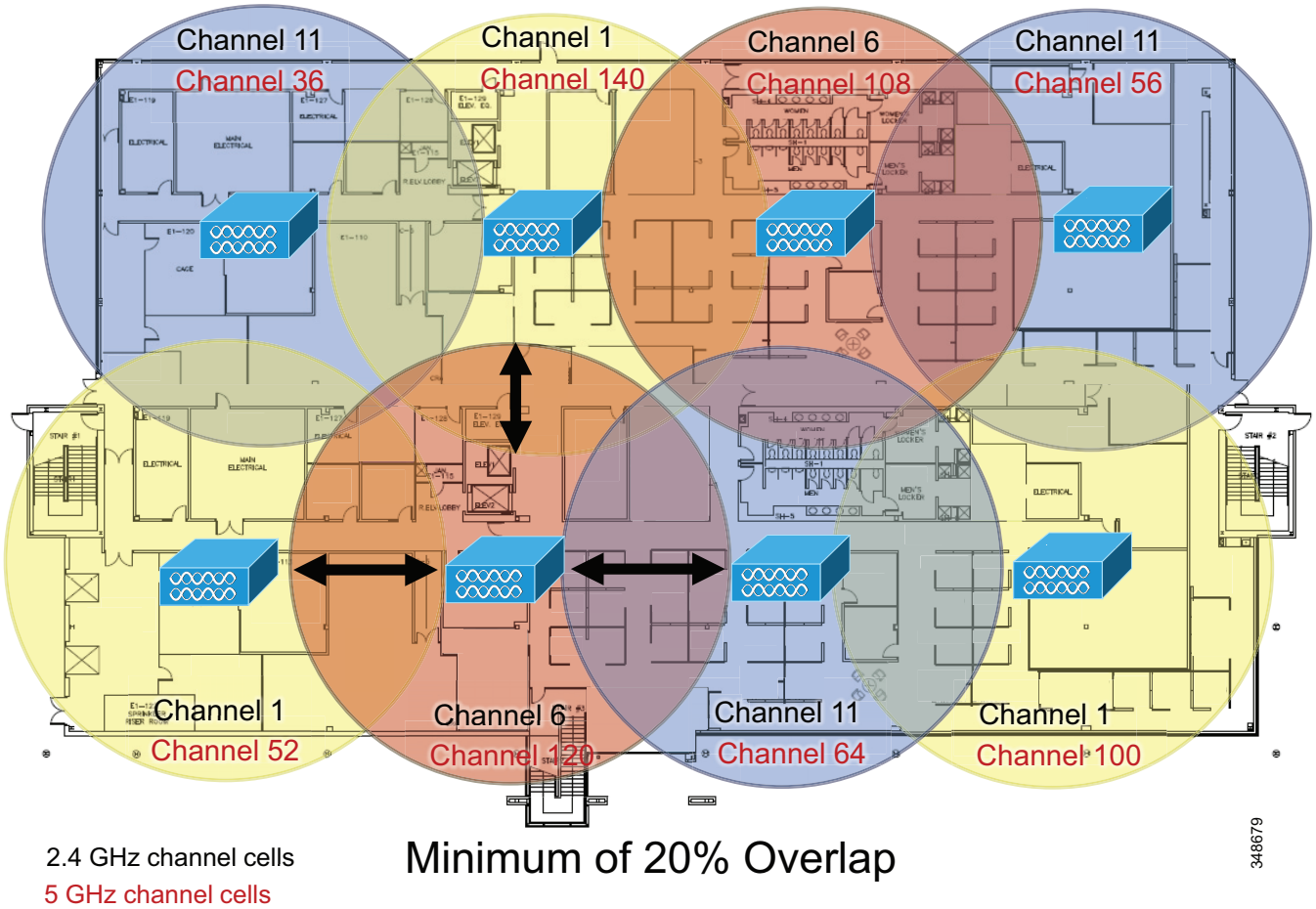
WLAN ネットワークは、1 箇所以上のワイヤレス アクセス ポイント（AP）から構成されます。ワイヤレス AP は、ワイヤレス デバイスに対してワイヤレス ネットワーク接続を提供します。ワイヤレス AP は、ワイヤレス ネットワークと有線ネットワークとの間の境界ポイントとなります。ネットワークのカバー領域および容量を拡張するために、物理的なネットワーク敷設領域に複数の AP が分散して配置されます。

ワイヤレス デバイスおよびワイヤレス クライアントは、基礎となる WLAN インフラストラクチャに依存して重要なシグナリングとリアルタイムの音声とビデオのメディア トラフィックの両方を伝送するため、データ トラフィックとリアルタイム音声トラフィックの両方に最適化された WLAN ネットワークの配置が必要になります。WLAN ネットワークの配置が適切でないと、多くの干渉が発生し、容量が低下するため、音声とビデオの品質が低下するだけでなく、コールがドロップされたり、つながらなかったりする可能性もあります。このように配置された WLAN は、音声コールの発信および受信に使用できなくなります。したがって、ワイヤレス フォンとクライアントを配置する場合は、Voice and Video over WLAN（VVoWLAN）の配置が正常に行われるように、配置前、配置中、配置後に WLAN 無線周波数（RF）事前現地調査を実施して、適切なセル境界、設定、機能設定、容量、および冗長性を判断する必要があります。

AP は、ネットワーク内に自律的に配置して、各 AP が他のすべての AP とは独立して設定、管理、および運用されるようにすることも、WLAN コントローラによってすべての AP が設定、管理、および制御されるように管理モードで配置することもできます。後者のモードでは、WLAN コントローラは、AP の管理、および AP 設定と AP 間ローミングの処理を担当します。いずれの場合も、VVoWLAN を正常に配置するには、次の一般的なガイドラインに従って AP を配置する必要があります。

- 図 21-2 に示すように、隣接していない WLAN AP チャネル セルは、20 % 以上オーバーラップする必要があります。このようにオーバーラップさせることによって、ワイヤレス デバイスがキャンパス ロケーション内で移動した場合に AP 間で正常にローミングして、ボイス ネットワーク接続およびデータ ネットワーク接続を維持できます。2 つの AP 間で正常にローミングしたデバイスは、音声品質や音声パスに目立った変更なしにアクティブな音声コールを維持できます。

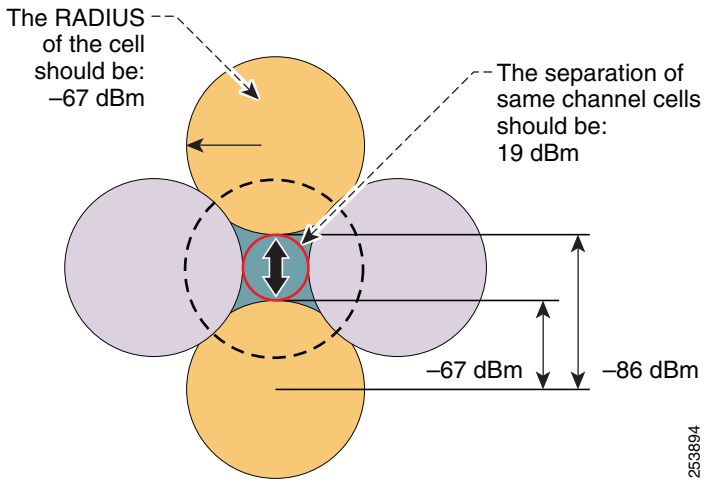
図 21-2　　WLAN チャネル セル オーバーラップ



- 図 21-3 に示すように、WLAN AP チャネル セルは、-67 デシベル/ミリワット（dBm）のセル パワーレベル境界（またはチャネル セル半径）で配置する必要があります。また、同一チャネルのセル境界の分離は、約 19 dBm にする必要があります。

  約 -67 dBm（またはそれ未満）のセル半径にすることで、リアルタイムの音声とビデオのトラフィックで問題となるパケット損失を最小限に抑えることができます。19 dBm の同一チャネル セル分離は、AP またはクライアントにおいて、同じチャネルに関連付けられている他のデバイスとの同一チャネル干渉が発生しないようにするために重要です。同一チャネル干渉が発生すると、音声品質が低下するためです。セル半径についての -67 dBm のガイドラインは、2.4 GHz（802.11b/g/n）と 5 GHz（802.11a/n/ac）の両方の配置に該当します。

図 21-3　　WLAN セル半径および同一チャネル セル分離



(注)　19 dBm の同一チャネル セル分離は、単純化されたものであり、理想的な状態を示しています。ほとんどの配置においては、このような 19 dBm の分離を実現することができません。最も重要な RF 設計基準は、-67 dBm のセル半径と、セル間の 20 % 以上の推奨オーバーラップです。これらの制約を遵守して設計することによって、チャネルの分離が最適化されます。

無線ローミングは無線電話だけではなく、PC で実行するソフトウェアベースの電話にも適用されます。たとえば、ユーザは Cisco IP Communicator または Cisco Jabber を実行しているラップトップ コンピュータを使用して、キャンパス中を無線でローミングできます。

ほとんどのワイヤレス AP、無線電話、およびワイヤレス PC クライアントでは、企業の WLAN に安全にアクセスできるように、さまざまなセキュリティ オプションが用意されていますWLAN インフラストラクチャとワイヤレスデバイスの両方でサポートされており、企業のセキュリティ ポリシーおよびセキュリティ要件に一致するセキュリティの方法を必ず選択してください。

Cisco Unified Wireless Network のインフラストラクチャの詳細については、ワイヤレス LAN インフラストラクチャ (3-66 ページ)を参照してください。WLAN 経由の音声およびビデオなど WLAN 設計上のリアルタイム トラフィックの詳細については、次の Web サイトから入手可能な『*Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide*』を参照してください

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd.html

エクステンション モビリティ (EM)

図 21-1 に示すように、有線およびワイヤレス電話機の物理的な移動に加え、ユーザ自身も電話機または PC ハードウェアを持たずにキャンパス インフラストラクチャ内を移動できます。これらの場合、ユーザの会社の電話番号および他の設定を含むプロファイルを適用することにより、ユーザは 1 つのデバイスから別のデバイスに、会社の内線番号または会社の番号を移動できます。

EM 機能により、ユーザはセキュリティ クレデンシャル (ユーザ ID および PIN 番号) のセットを使用して、キャンパス内にある IP フォンにログインできます。ログインすると、会社の電話番号やコール特権から、設定したスピード ダイヤルまでを含めたユーザ個人のデバイス プロファイルが、ユーザがデバイスをログアウトするまで、またはログインのタイムアウトまで、一時的にこの電話に適用されます。EM 機能は、Unified CM の一部として使用できます。

この機能は、会社の外でほとんどの時間を費やし、物理的に、オフィスには時々しかいないモバイル企業ユーザに特に役に立ちます。ホット シーティングまたはフリー シーティングと呼ばれることもあるこれらのタイプのモバイル ユーザに、一時的にオフィスのスペースを提供することで、システム管理者は頻度が低く一時的にしか IP フォンハードウェアを使用する必要がない多数のモバイル ユーザに対応できます。

キャンパス内で EM を利用するには、Unified CM 管理者がユーザ デバイス プロファイルおよびユーザ クレデンシャルを設定し、EM 電話サービスへ IP フォンを登録する必要があります。

（注）　EM は Unified CM コール制御によってのみ、EM 対応エンドポイント デバイスだけでサポートされます。

EM の詳細については、エクステンション モビリティ（18-9 ページ）を参照してください。

キャンパス企業モビリティのハイ アベイラビリティ

キャンパス企業モビリティ機能およびソリューションは、モビリティ機能のハイ アベイラビリティを保証するよう、冗長な方式で設定し配置する必要があります。

たとえば、有線の IP 電話およびソフトウェアベースの IP 電話を実行しているコンピュータを効率的にサポートするため、冗長で普及しているネットワーク接続またはポートが使用可能である必要があります。さらに、これらの冗長なネットワーク接続は、適切なセキュリティ、Quality of Service、およびその他のネットワークベースの機能などの、有線デバイスのロケーションを移動しても最適な操作とボイス品質を確保できる適切な特性を備えたまま配置される必要があります。最終的には、正常なキャンパス モビリティの配置は、ネットワーク接続、PSTN 接続、およびその他のアプリケーションやサービスが、ハイ アベイラビリティのある方式で配置されている場合にのみ可能です。

同様に、ワイヤレス デバイスを接続およびローミングするための WLAN ネットワークの配置や調整では、ワイヤレス サービスに対するハイ アベイラビリティを考慮することも重要です。配置するデバイス数に対する弾力性と十分なカバレッジを確保するために、WAN ネットワークは、同一チャネル セルがオーバーラップすることなく、適切で冗長なセルによるカバレッジが保証されるように配置する必要があります。同一チャネル セルがオーバーラップしない十分なセル カバレッジ、および AP 間のローミングを容易に実行可能にするための異なるチャネル セルの十分なオーバーラップを提供することによって、ワイヤレス デバイスおよびクライアントに対するネットワーク接続でハイ アベイラビリティを確保できます。

最後に、EM をキャンパス内のユーザ モビリティに利用する場合、Unified CM クラスタ内の単一ノードの障害が Extension Mobility 機能の動作を妨げないよう、この機能を冗長な方式で配置する必要があります。可用性が高くなるような Cisco Extension Mobility の詳細については、エクステンション モビリティのハイ アベイラビリティ（18-17 ページ）を参照してください。

キャンパス企業モビリティのキャパシティ プランニング

キャンパス企業モビリティを正常に配置するには、これらのモビリティ機能とソリューションを使用するすべてのモバイル ユーザに対応できる十分なキャパシティを用意する必要があります。

有線デバイスおよびコンピュータの物理的な移動に対するキャパシティの考慮は、キャンパス ネットワーク インフラストラクチャ内で使用できるネットワーク ポート数に完全に依存しています。キャンパス内でデバイスを移動するユーザのため、それぞれのロケーションに、モバイル ユーザのデバイスの接続に使用できるある程度の数の使用可能なネットワークポートがある必要があります。ネットワークポートが不足してこの有線デバイスの移動に対応できないと、1 つのロケーションから別のロケーションへ物理的にデバイスを移動できないことになる可能性があります。

企業 WLAN 内にワイヤレス デバイスを配置し、ワイヤレス デバイス ローミングを利用する場合、WLAN インフラストラクチャのデバイスの接続性とコール キャパシティを考慮することも重要です。デバイス数またはアクティブ コール数の面でのキャンパス WLAN インフラストラクチャのオーバーサブスクリプションは、ワイヤレス接続のドロップ、音声とビデオの品質の低下、またはコール セットアップの遅延や失敗の原因となります。Voice and Video over WLAN（VVoWLAN）の配置をオーバーサブスクライブする可能性は、必要なコール キャパシティを処理するために十分な数の AP を配置することで、著しく最小限に抑えられます。AP のコール キャパシティは、単一チャネル セル領域内でサポートできる音声またはビデオの同時双方向ストリームの数に基づきます。VVoWLAN のコール キャパシティの一般的なルールは次のとおりです。

- データ レート 24 Mbps 以上の Bluetooth を無効にした 802.11g/n（2.4 GHz）チャネル セルあたり最大 27 個の同時 Voice over WLAN（VoWLAN）双方向ストリーム。
- データ レート 24 Mbps 以上の 802.11a/n（5 GHz）チャネル セルあたり最大 27 個の同時 VoWLAN 双方向ストリーム。
- 720p のビデオ解像度（高解像度）および最大 1 Mbps のビデオ ビット レート、Bluetooth が無効の 802.11 g/n（2.4 GHz）あたり、または 802.11 a/n（5 GHz）チャネル セルあたり最大 8 の VVoWLAN 同時双方向のストリームを前提としています。

これらの音声およびビデオ コール キャパシティ値は、RF 環境、設定またはサポートされているビデオ解像度とビット レート、ワイヤレス エンドポイントとその固有の機能、および基礎となる WLAN システム機能に大きく依存します。一部の配置では、実際のキャパシティはこれよりも小さくなることもあります。

（注）　同じ AP に関連付けられている 2 台のワイヤレス エンドポイント間の単一のコールは、2 つの同時双方向ストリームであると見なされます。

EM のスケーラビリティは、Unified CM 内のログイン率およびログアウト率にほぼ依存します。十分な EM ログイン/ログアウト キャパシティがモバイル ユーザに提供できるよう、Unified CM クラスタ内で有効なエクステンション モビリティ ユーザ数と、キャンパス内を移動するユーザ数、任意の時間にこの機能を使用しているユーザ数を把握することが重要です。EM キャパシティ プランニングの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

いずれの場合も、キャンパス内の Unified CM クラスタには、有線デバイスかワイヤレス デバイスにかかわらず、移動されたデバイスに対するデバイス登録を処理する十分なデバイス登録キャパシティが必要です。もちろん、キャンパス内を移動しているすべてのデバイスが、すでにキャンパス ネットワーク内に配置されている場合、コール制御プラットフォーム内の十分なキャパシティが、デバイスの移動の前にすでに配置されている必要があります。ただし、新しいデバイスをモビリティを目的として配置に追加する場合は、デバイス登録キャパシティを考慮する必要があり、必要に応じてさらにキャパシティを追加する必要があります。

最後に、Unified CM によって提供される多くの機能により、これらのモビリティ ソリューションの設定および配置はシステム全体のサイジングと関わっています。実際のシステム キャパシティの決定は、エンドポイント デバイスや EM ユーザの数、配置されている CTI アプリケーションの数に対する最繁時呼数（BHCA）レートなどの考慮事項に基づきます。一般的なシステム サイジング、キャパシティ プランニング、および配置上の考慮事項の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

キャンパス企業モビリティの設計上の考慮事項

キャンパス企業モビリティ機能を配置する際は、次の設計上の考慮事項に従ってください。

- キャンパス内の物理的なデバイス モビリティに対応するには、新しいロケーションで使用されるネットワーク接続の IP 接続（VLAN や VLAN 間ルーティングなど）、接続速度、Quality of Service、セキュリティ、およびネットワーク サービス（インライン パワー、動的ホスト制御プロトコル（DHCP）など）が前のネットワーク接続と同じタイプであることを確認してください。これらの接続パラメータ、サービス、および機能が同じでないと、機能が低下するか、場合によっては機能が完全に失われます。
- ワイヤレス IP デバイスやソフトウェアベース クライアントを展開する場合は、Voice and Video over WLAN（VVoWLAN）の展開が正常に行われるように、展開前、展開中、定期的に展開後に WLAN 無線周波数（RF）事前現地調査を実施して、適切なセル境界、設定、機能設定、容量、および冗長性を判断する必要があります。
- AP は、20 % 以上のセル オーバーラップを確保して配置する必要があります。このようにオーバーラップさせることによって、デュアルモード デバイスがロケーション内で移動した場合に AP 間で正常にローミングして、ボイス ネットワーク接続およびデータ ネットワーク接続を維持できます。
- パケット損失を最小限に抑えるために、AP は -67 dBm のセル パワー レベル境界（またはチャネル セル半径）で配置する必要があります。また、同一チャネルのセル境界の分離は、約 19 dBm にする必要があります。19 dBm の同一チャネル セル分離は、AP またはクライアントにおいて、同じチャネルに関連付けられている他のデバイスとの同一チャネル干渉が発生しないようにするために重要です。同一チャネル干渉が発生すると、音声とビデオの品質が低下するためです。
- 単一の Unified CM ノードが失われた場合に機能の実行に悪影響が及ばないように、EM サービスは冗長性の高い方式で配置してください。EM サービスが重要な場合、Unified CM ノード障害を回避し可用性が高い機能を提供するためのサーバ ロード バランシング ソリューションを考えます。EM のハイ アベイラビリティの詳細については、エクステンション モビリティのハイ アベイラビリティ（18-17 ページ）を参照してください。
- キャンパス ネットワークのワイヤレスの音声とビデオコールのキャパシティは十分に用意してください。そのためには、無線ユーザの BHCA レートに基づき、目的のコール キャパシティの処理に適した数のワイヤレス AP を展開します。各 802.11g/n（2.4 GHz）または 802.11a/n/ac（5 GHz）チャネル セルは、24 Mbps 以上のデータ レートで最大 27 の同時音声のみのコールをサポートできます。各 802.11g/n（2.4 GHz）または 802.11a/n/ac（5 GHz）チャネル セルは、最大 1 Mbps ビット レートでビデオ解像度 720p の場合、最大 8 の同時ビデオ コールをサポートできます。2.4 GHz WLAN 配置では、このキャパシティを実現するには Bluetooth を無効にする必要があります。実際のコール キャパシティは、RF 環境、ワイヤレス エンドポイント タイプおよび WLAN インフラストラクチャによって、さらに小さくなることがあります。

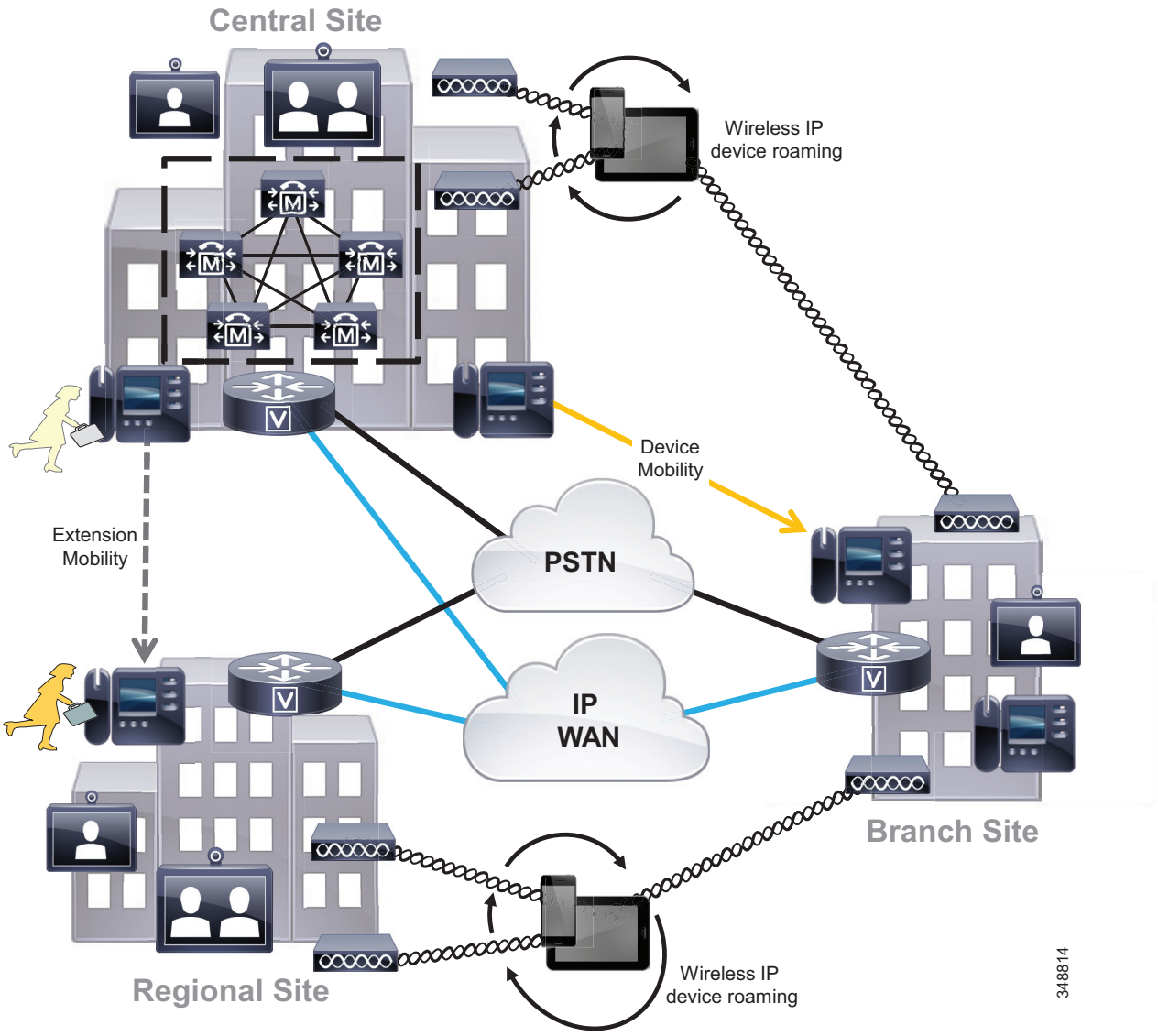
マルチサイト企業モビリティ

マルチサイト企業モビリティとは、複数の物理的な場所があり、それぞれが一意の IP アドレス空間および PSTN 入出力境界を持つ社内でのモビリティを指します。この場合のモビリティには、ユーザやエンドポイント デバイスの各物理ロケーション内の移動だけではなく、サイトおよびロケーション間のユーザやエンドポイント デバイスの移動も含まれます。

マルチサイト企業モビリティのアーキテクチャ

図 21-4 に示すように、マルチサイト企業モビリティのアーキテクチャは、地理的に離れた 2 つ以上のロケーションまたはサイトに基づいています。ユーザとデバイスの数が多い中央またはキャンパス サイトから、ユーザとデバイスの数が少なめの中規模の地域サイト、それよりも小規模な支社サイトまで、サイトの規模は異なってもかまいません。一般にマルチサイト企業配置は、サイトを相互接続する IP WAN リンクや、各ロケーションでのローカル PSTN 入出力で構成されています。さらに多くの場合、サイト間のネットワーク障害中でも機能を維持するため、重要なサービスはそれぞれの物理サイトに複製されています。モビリティの観点からは、ユーザとそのデバイスはサイト内またはサイト間で移動できます。

図 21-4　　マルチサイト企業モビリティのアーキテクチャ



(注)　図 21-4 では、集中呼処理を使用するマルチサイト配置（セントラル サイト内にある単一 Unified CM または VCS クラスタから明らか）を示していますが、マルチサイト企業モビリティの配置と同じ設計および配置の考慮事項が、分散型呼処理環境に適用されます。分散型呼処理環境に配置された場合のモビリティ機能の動作の違いについて、以降で説明します。

マルチサイト企業モビリティのタイプ

マルチサイト企業モビリティ配置には、デバイス、ユーザ、またはその両方の単一サイト内での移動だけではなく、サイト間のユーザおよびデバイスの移動も含まれます。

キャンパス/単一サイト企業配置でサポートされているタイプと同じモビリティ機能とソリューションが、マルチサイト配置の単一サイト内でのユーザやデバイスのサイト内移動に適用されます。これらには、有線電話機の物理的な移動、無線電話ローミング、およびエクステンション モビリティが含まれます。これらのタイプのモビリティソリューションおよび機能の詳細については、キャンパス企業モビリティ (21-4 ページ)を参照してください。

マルチサイト配置でのサイト内モビリティでも、これらのモビリティ機能が同じようにサポートされます。ただし、2 つ以上のサイト間に適用される場合の機能との主な違いとして、これらの機能はデバイス モビリティ機能により拡張されます。デバイス モビリティ機能では、企業ネットワークに接続するときにデバイスが使用する IP アドレスを基にしたダイナミックなロケーション認識メカニズムが提供されます。

物理的な有線デバイスの移動

物理的な有線電話機の移動は、マルチサイト配置の各サイト内でも、サイト間でも簡単に対応できます。キャンパス/単一サイト配置と同様、マルチサイト配置の単一サイトに制限された有線デバイスの移動は、Cisco エンドポイントをネットワークから外し、サイト内の別のロケーションに移動して、別の有線ネットワーク ポートに接続するだけです。新しいネットワークの場所に接続すると、この電話がコール制御プラットフォームに再登録され、前のロケーションと同じように発信や着信ができます。

マルチサイト配置でのサイト間またはロケーション間の有線デバイスの移動も、基本的には同じ形です。ただし、このタイプのモビリティと組み合わせた場合、デバイス モビリティ機能により、デバイスが移動先の新しいロケーションで再登録されると、適切にコール アドミッション制御が動作し、ゲートウェイおよびコーデックが選択されます。この機能の詳細については、デバイス モビリティ (21-15 ページ)を参照してください。

ワイヤレス デバイス ローミング

各サイトで使用できる、無線ネットワークに接続するための無線 LAN ネットワーク インフラストラクチャが使用可能な場合、単一サイトのキャンパス配置と同様、ワイヤレス デバイスは、図 21-4 に示すように、マルチサイト企業配置全体を移動またはローミングできます。しかし、サイト間の有線電話機の移動と同様ワイヤレス デバイスでも、コールの発着信の際に正しいゲートウェイおよびコーデックが確実に使用されるよう、またコール アドミッション制御が帯域幅を適切に管理するよう、デバイス モビリティ機能が配置されなければなりません。この機能の詳細については、デバイス モビリティ (21-15 ページ)を参照してください。

分散型呼処理環境では、有線電話機と同様に、コール ルーティングにより発生する可能性のある問題を回避するため、単一の呼処理プラットフォームまたはクラスタだけにワイヤレス デバイスを登録するように設定する必要があります。

エクステンション モビリティ（EM）

単一サイト内での EM のサポートに加え、図 21-4 に示すように、この機能はサイト間でもサポートされ、ユーザが企業内のサイト間を移動して、各場所で電話機にログオンできます。

また、ユーザが異なる Unified CM クラスタのサイト間や電話間を移動する場合、EM も分散型呼処理の配置でサポートされます。分散型呼処理環境でエクステンション モビリティをサポートするには、Cisco Extension Mobility Cross Cluster（EMCC）機能を設定する必要があります。この機能の詳細については、クラスタ間のエクステンション モビリティ（EMCC）（18-11 ページ）を参照してください。

（注）　EM と EMCC は、Unified CM コール制御によってのみ、EM 対応エンドポイント デバイスだけでサポートされます。

デバイス モビリティ

Cisco Unified CM では、場所、地域、通話サーチ スペース、メディア リソースなど、さまざまな設定を使用して、サイト、つまり物理的な場所が識別されます。特定のサイトにある Cisco Unified IP Phone は、これらの設定により静的に設定されます。Unified CM では、適切なコールの確立、コール ルーティング、メディア リソースの選択などのためにこれらの設定を使用します。一方、Cisco Unified Wireless IP Phone などのデュアルモード電話機やその他のモバイル クライアント デバイスは、各自のホーム サイトからリモート サイトに移動される場合、電話機に静的に設定されているホーム設定を保持しています。この結果 Unified CM では、リモート サイトの電話機にあるこれらのホーム設定を使用します。この状況は、コール ルーティング、コーデックの選択、メディア リソースの選択、およびその他の呼処理機能における問題の原因となる場合があるため望ましくありません。

Cisco Unified CM では、デバイス モビリティという機能を使用します。この機能により、Unified CM では、IP フォンがホーム ロケーションにあるのか、ローミング ロケーションにあるのかを判別できます。Unified CM では、デバイスの IP サブネットを使用して、その IP フォンの正確な場所を判別します。クラスタ内でのデバイス モビリティを使用できるようにすることで、モバイル ユーザは 1 つのサイトから別のサイトにローミングでき、このときサイト固有の設定を取得します。次に、Unified CM では、これらの動的に割り当てられた設定を使用して、コール ルーティング、コーデックの選択、メディア リソースの選択などを行います。

この項では、最初にデバイス モビリティ機能の主要な目的について説明し、続いてデバイス モビリティ機能そのものについて詳細に説明します。ここでは、デバイス モビリティ機能のさまざまなコンポーネントおよび構成要素について取り上げます。この項では、デバイス モビリティ機能が企業ダイヤル プランに与える影響を、さまざまなダイヤル プラン モデルへの影響も含めて詳細に説明します。

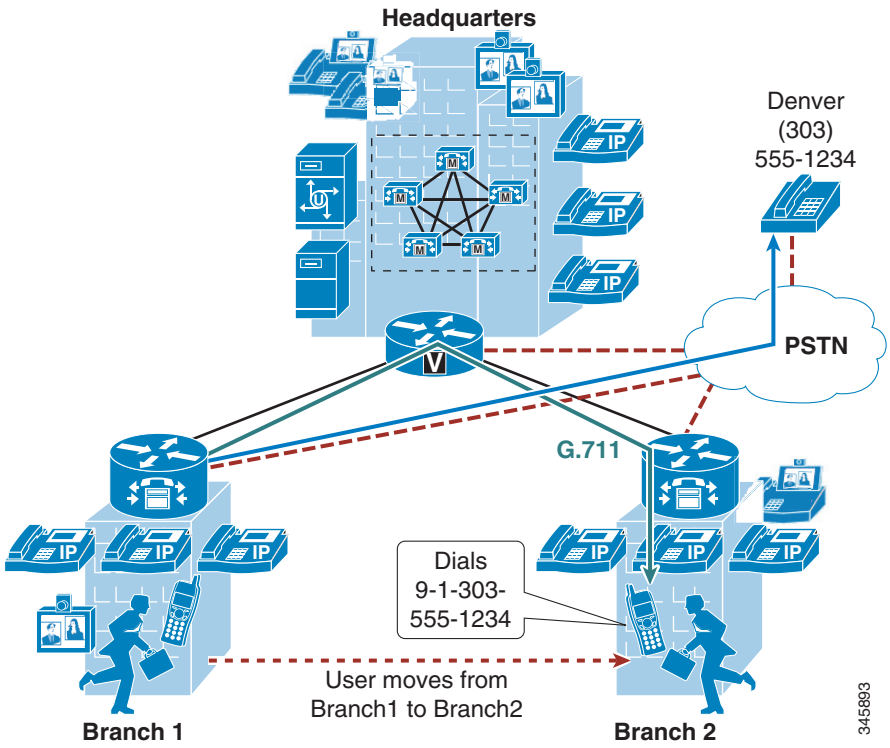
（注）　デバイス モビリティは Unified CM コール制御だけでサポートされます。

デバイス モビリティの必要性

この項では、Unified CM クラスタに多くのモバイル ユーザが含まれている場合のデバイス モビリティの必要性について説明します。

図 21-5 は、本社サイト（HQ）にあり、デバイス モビリティ機能を備えない Unified CM クラスタを含んでいる架空のネットワークを示しています。このクラスタには、支店 1 と支店 2 の 2 つのリモート サイトがあります。サイト内コールでは、いずれも G.711 音声コーデックが使用されます。一方サイト間コール（IP WAN を経由するコール）では、いずれも G.729 音声コーデックが使用されます。各サイトには、外部コールのための PSTN ゲートウェイがあります。

図 21-5　　リモート サイトを 2 つ持つネットワークの例



支社 1 のユーザが支社 2 に移動し、Denver にいる PSTN ユーザに通話すると、次のような動作が発生します。

- Unified CM では、そのユーザが支社 1 から支社 2 に移動したことを認識していません。PSTN への外部コールが WAN を経由して支社 1 のゲートウェイに送られ、そこから PSTN に出ます。これにより、モバイル ユーザの PSTN コールすべてに、引き続きそのユーザのホーム ゲートウェイが使用されます。
- このモバイル ユーザと支社 1 ゲートウェイは、同じ Unified CM リージョンおよびロケーションに存在しています。ロケーション ベースのコール アドミッション制御は、異なるロケーションに存在しているデバイスおよび G.711 音声コーデックを使用するリージョン内コールにだけ適用可能です。したがって、IP WAN を経由する支社 1 ゲートウェイへのコールでは G.711 コーデックが使用され、コール アドミッション制御のための Unified CM によるトラッキングは行われません。この動作の結果、リモート リンクすべてが低速リンクである場合に、IP WAN 帯域幅のオーバー サブスクリプションが発生する場合があります。
- モバイル ユーザが、複数の支社 2 ユーザを Denver にいる PSTN ユーザとの既存のコールに追加することで、会議を作成します。モバイル ユーザは支社 1 ゲートウェイの会議リソースを使用します。したがって、すべての会議ストリームが IP WAN 経由で流れます。

（注） デバイス モビリティは、クラスタ内機能で、複数の Unified CM クラスタには拡張されません。分散型呼処理環境では、配置内の各 Unified CM クラスタでデバイス モビリティを有効にし、設定する必要があります。

(注)　デバイス モビリティが設定されていない環境では、管理者はサイト ロケーション間に WAN 帯域幅を多めにプロビジョニングし、WAN 経由とサイト間のデバイスの物理的な移動で、WAN を多めにサブスクライブしないようにします。各 WAN リンクについて余分にプロビジョニングする帯域幅の量は、ユーザが 2 か所の場所の間でデバイスを移動する際の予測レートによって異なります。

デバイス モビリティ アーキテクチャ

Unified CM デバイス モビリティ機能は、上記の問題を解決するために有用です。この項では、この機能の動作方法を簡単に説明します。この機能の詳細については、次の Web サイトで入手可能な最新バージョンの『*Feature Configuration Guide for Cisco Unified Communications Manager*』で、デバイス モビリティに関する情報を参照してください。

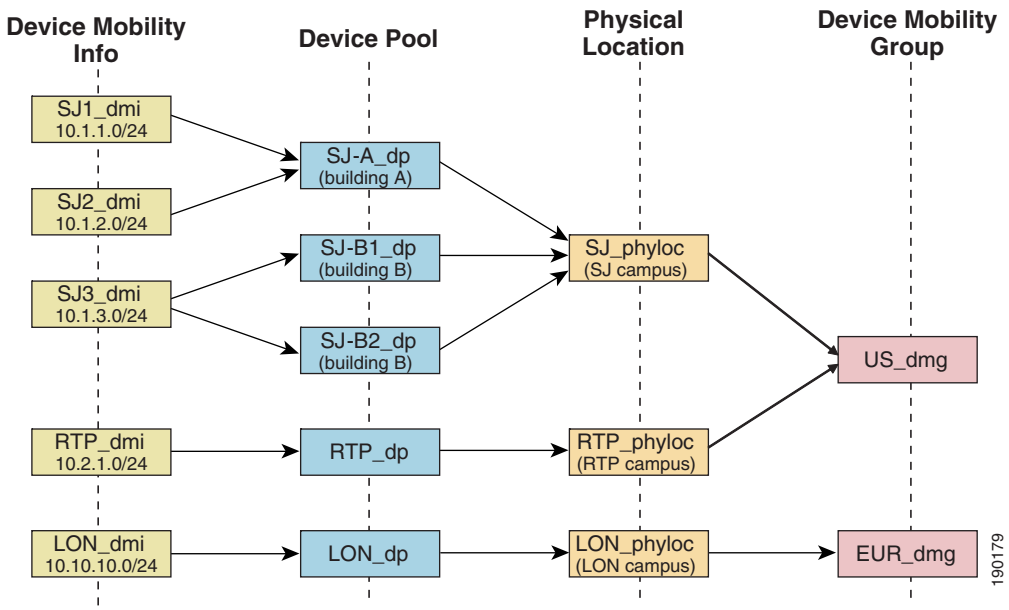
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

デバイス モビリティには次のような要素が含まれます。

- デバイス モビリティ情報:IP サブネットを設定し、デバイス プールを IP サブネットに関連付けます。
- デバイス モビリティ グループ:ダイヤリング パターンが類似しているサイトの論理グループを定義します(たとえば、図 21-6 の US_dmg および EUR_dmg)。
- 物理ロケーション:デバイス プールの物理ロケーションを定義します。言い換えると、この要素では、IP 電話およびデバイス プールに関連付けられているその他のデバイスの地理的なロケーションを定義します(たとえば、図 21-6 に示されている San Jose の IP 電話は、すべて物理ロケーション SJ_phyloc を使用して定義されています)。

図 21-6 は、この 3 つの用語すべての関係を示します。

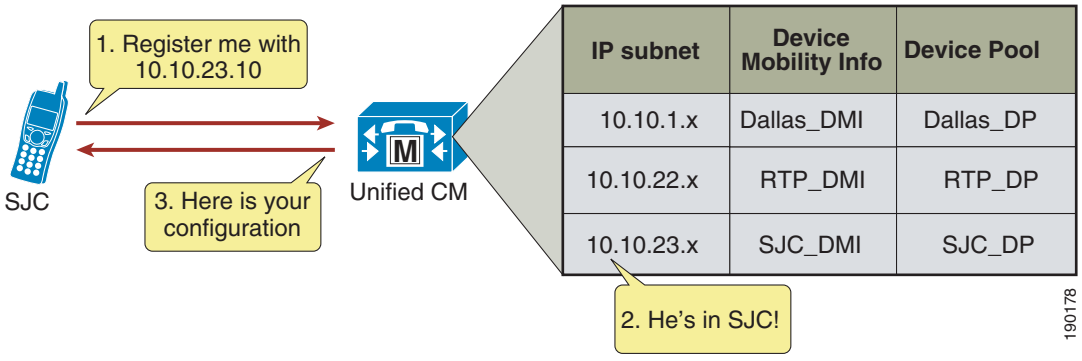
図 21-6　デバイス モビリティ コンポーネントの関係



Unified CM では、デバイスの IP サブネットに基づいてデバイス プールを IP フォンに割り当てます。次の手順は、図 21-7 に図示がありますが、この動作を説明したものです。

1. IP フォンでは、その電話の IP アドレスを Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）登録メッセージに含めて送信することにより、Unified CM への登録を試行します。
2. Unified CM では、デバイスの IP サブネットを抽出し、デバイス モビリティ情報に設定されているサブネットと照合します。
3. サブネットが一致すると、Unified CM では、デバイス プール設定に基づいて、デバイスに新規設定を提供します。

図 21-7　　電話登録プロセス



Unified CM では、デバイス プール設定にあるパラメータ一式を使用して、デバイス モビリティに対応します。これらのパラメータは、次の 2 つの主要なタイプについてのパラメータです。

- ローミングに依存する設定（21-18 ページ）
- デバイス モビリティ関連の設定（21-19 ページ）

ローミングに依存する設定

これらの設定にあるパラメータは、デバイスがデバイス モビリティ グループの内部または外部をローミングしているときに、デバイス レベルの設定より優先されます。この設定には、次のパラメータが含まれます。

- 日付/時刻グループ
- 地域
- メディア リソース グループ リスト
- 参照先
- ネットワーク ロケール
- SRST リファレンス
- 物理ロケーション
- デバイス モビリティ グループ

ローミングに依存する設定は、主に、適切なコール アドミッション制御および音声コーデックの選択を実施するために有用です。これは、ロケーションおよびリージョンの設定は、デバイスのローミング デバイス プールに基づいて使用されるためです。

さまざまなコール アドミッション制御手法については、帯域幅管理（13-1 ページ）の章を参照してください。

ローミングに依存する設定により、メディア リソース グループ リスト（MRGL）も更新されて、保留音、会議、トランスコーディングなどで適切なリモート メディア リソースが使用されるようになり、これによりネットワークが効率的に使用されます。

ローミングに依存する設定により、Survivable Remote Site Telephony（SRST）ゲートウェイも更新されます。モバイル ユーザは、ローミング中に別の SRST ゲートウェイに登録します。この登録が、ローミング電話機が SRST モードであるときのダイヤリング動作に影響することがあります。

たとえば、ユーザが Unified CM への接続を失う新しいロケーションに電話機を移動した場合、ローミングに依存するデバイス モビリティ設定に基づいて、移動された電話機に対して新しい SRST リファレンスが設定されます。また、移動された電話機はローカルなローミング ロケーション SRST ルータの制御下に入ります。この場合、デバイスの DID が変更されず、ホーム ロケーションに固定されたままになるため、ユーザの電話機は PSTN や他のサイトから到達不能になるだけでなく、SRST 内で実装されている短縮ダイヤルを使用しなければ、ローカルな障害発生サイト内のデバイスから到達することも困難になる可能性があります。

たとえば、ユーザが電話機を San Jose のホーム ロケーション（ディレクトリ番号が 51234 で、関連付けられた DID が 408 555 1234）から New York のリモート ロケーションに移動したとします。また、ユーザが New York ロケーションにローミングして間もなく、New York のサイトと San Jose の間のリンクに障害が発生したとします。このシナリオでは、New York サイトにある電話機はすべて、そのサイト内の SRST ルータにフェールオーバーされます。また、ローミング電話機または移動された電話機は、その SRST リファレンスがデバイス モビリティのローミング依存設定に基づいて更新されたために、New York の SRST ルータに登録されます。このシナリオでは、New York のローカルなデバイスが Unified CM に登録するのと同じように、5 桁の内線番号とともに SRST ルータに登録されます。その結果、ローミング電話機のディレクトリ番号は 51234 のまま変わりません。他のすべてのサイトから、および PSTN からローミング電話機に到達するために、番号 408 555 1234 が、この特定の DID が固定されている San Jose の PSTN ゲートウェイにルーティングされます。New York サイトは San Jose サイトから切断されているため、このようなコールはいずれもユーザのデスクフォンには到達不能です。したがって、コールはユーザのボイスメール ボックスにルーティングされます。同様に、ローカルの障害発生サイト内のコールは、5 桁の短縮ダイヤルを使用して、または SRST ルータ内の **dialplan-pattern** および **extension-length** コマンドで定義されているように設定済みの番号をプレフィックスとして付加して、ダイヤルする必要があります。いずれの場合も、ローカル発信者が、短縮ダイヤルによりローカル ローミング デバイスに到達するために必要なダイヤリング動作を理解している必要があります。ローカル ローミング電話機に到達するために、5 桁をダイヤルするだけでよいこともあれば、ユーザが特別な番号プレフィックスをダイヤルする必要があることもあります。同じロジックが、New York の移動された電話機またはローミング電話機からの発信ダイヤリングにも適用されます。短縮ダイヤルを使用してローカル内線番号に到達するためには、そのダイヤリング動作を変更する必要があるためです。ただし、ローカルなローミング デバイスから PSTN への発信ダイヤリングは、常に同じである必要があります。

デバイス モビリティ関連の設定

これらの設定にあるパラメータは、デバイスがデバイス モビリティ グループの内部をローミングしているときにだけ、デバイス レベルの設定より優先されます。この設定には、次のパラメータが含まれます。

- [デバイス モビリティ コーリング サーチ スペース（Device Mobility Calling Search Space）]
- [AAR コーリングサーチスペース（AAR Calling Search Space）]
- [AAR グループ（AAR Group）]
- [発呼側トランスフォーメーション CSS（Calling Party Transformation CSS）]

コーリング サーチ スペースは、ダイヤルできるパターンまたは到達できるデバイスを指示するため、デバイス モビリティ関連の設定は、ダイヤル プランに影響します。

デバイス モビリティ グループ

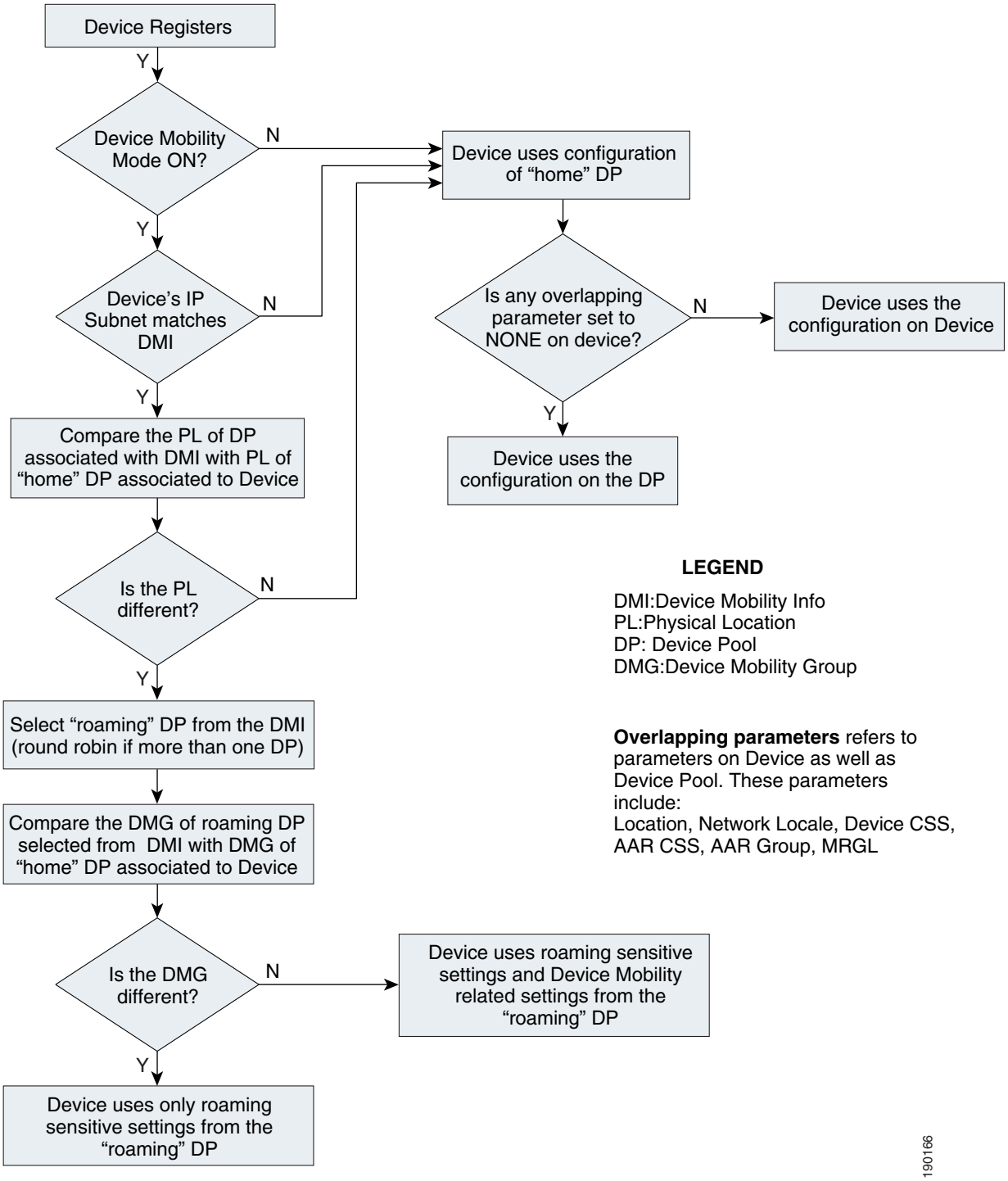
前述したように、デバイス モビリティ グループは、ダイヤリング パターンが類似したサイト（たとえば、同じ PSTN アクセス コードを持つサイトなど）の論理グループを定義します。このガイドラインを使用すると、すべてのサイトがサイト固有のコーリング サーチ スペースに類似したダイヤリング パターンを持ちます。ダイヤリング動作が異なるサイトは、異なるデバイス モビリティ グループに属します。図 21-6 に示すように、San Jose サイトと RTP サイトのデバイス モビリティ情報、デバイス プール、および物理ロケーションは異なります。ただし、必要なダイヤリング パターンと PSTN アクセス コードは 2 つのロケーション間で同じであるため、これらはすべて同じデバイス モビリティ グループ US_dmg に割り当てられています。一方、London サイトは別のデバイス モビリティ グループ EUR_dmg に割り当てられています。これは、必要なダイヤリング パターンと PSTN アクセス コードが US サイトのものとは異なるためです。デバイス モビリティ グループ内をローミングするユーザは、新規コーリング サーチ スペースを受け取った後であっても、ダイヤリング動作をリモート ロケーションで維持できます。デバイス モビリティ グループの外部をローミングするユーザは、自身のホーム コーリング サーチ スペースを使用するため、やはり、ダイヤリング動作をリモート ロケーションで維持できます。

ただし、デバイス モビリティ グループが、異なるダイヤリング パターンを持つ複数のサイトとともに定義されている場合（たとえば、あるサイトではユーザが外線使用時に 9 をダイヤルする必要があるが、別のサイトではユーザが外線使用時に 8 をダイヤルする必要がある場合）、そのデバイス モビリティ グループ内のユーザ ローミングにより、すべてのロケーションで同じダイヤリング動作を維持できいないことがあります。ユーザは、各ロケーションで新規コーリング サーチ スペースを受け取った後で、異なるロケーションにおいて異なる番号をダイヤルする必要がある場合があります。この動作はユーザの混乱を招く可能性があるため、異なるダイヤリング パターンを持つサイトを同じデバイス モビリティ グループに割り当てることは推奨しません。

デバイス モビリティの動作

デバイス モビリティ機能の動作を図 21-8 のフローチャートに示します。

図 21-8　デバイス モビリティ機能の動作



デバイス モビリティ機能には、次のガイドラインが適用されます。

- 図 21-8 にリストされている重複するパラメータがデバイスおよびデバイス プールで同じ設定を持つ場合は、デバイスではこれらのパラメータに NONE を設定できます。次にこれらのパラメータをデバイス プールに設定する必要があります。この方法を実施すると、デバイスにすべてのパラメータを個別に設定する必要がないため、設定の量を大幅に削減できます。
- サイトごとに物理ロケーション 1 つを定義してください。1 つのサイトが複数のデバイス プールを持つことができます。
- PSTN または外部/オフネット アクセスのダイヤリング パターンが類似したサイトを、同じデバイス モビリティ グループを使用して定義してください。
- 企業のポリシーに応じて、未定義のサブネットすべてに対応する、IP サブネット 0.0.0.0 の「catch-all」デバイス モビリティ情報を定義できます。このデバイス モビリティ情報は、ネットワーク リソースのアクセスまたは使用を制限できるデバイス プールを割り当てるために使用できます（たとえば、ローミング中にこのデバイス プールに関連付けられているデバイスからの通話すべてをブロックする通話サーチ スペース NONE を使用してデバイス プールを設定できます）。ただし、これを行う場合、管理者は、911 およびその他の緊急通話であってもブロックされるという事実を承知する必要があります。コーリング サーチ スペースは、911 またはその他の緊急コールだけにアクセスを許すパーティションを含めて設定できます。

ダイヤル プランの設計上の考慮事項

デバイス モビリティ機能は、選択されたローミング デバイス プールの設定、またはエンドポイントが登録されている IP アドレスに基づいて、複数のデバイスおよびデバイス プール設定を使用します。サブネットのデバイス プールの設定により更新される設定の詳細については、次の Web サイトで入手可能な最新バージョンの『*Feature Configuration Guide for Cisco Unified Communications Manager*』で、デバイス モビリティに関する情報を参照してください。

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

ダイヤル プランから見ると、主に AAR グループ、AAR CSS、デバイス CSS、ローカル ルート グループ、および発信コールの発呼側変換 CSS 設定が関連しています。

ローミング デバイスのイーグレス ゲートウェイの選択

通常、ローミング デバイスの目的のイーグレス ゲートウェイの選択動作は、訪問したサイトに対してローカルなゲートウェイを使用することです。発信側デバイスに固有のイーグレス ゲートウェイの選択を実装するための推奨される方法は、標準ローカル ルート グループを使用するルート リストを指す PSTN ルート パターンを使用することです。ルート リストの標準ローカル ルート グループを効果的に使用することは、実際のコールをルーティングする際に標準ローカル ルート グループが発信側エンドポイントのデバイス プール内で設定されたローカル ルート グループと置き換えられることを意味します。このスキーマは、サイトが不特定のルート パターンとルート リストが使用できるようになります。サイト固有のイーグレス ゲートウェイ接続は、デバイス プール レベルでローカル ルート グループの設定に完全に依存します。

ローミング デバイスでは（デバイス モビリティ グループ内またはデバイス モビリティ グループ間のローミング）、デバイス モビリティ機能により、ローミング デバイス プールのローカル ルート グループが標準ローカル ルート グループとして常に使用されるようになります。これにより、ローカル ルート グループのイーグレス ゲートウェイの選択で、訪問したサイトに固有のルート グループ（つまり、訪問したサイトに対してローカルなゲートウェイ）が通常使用されることが保証されます。この動作は、たとえば、標準ローカル ルート グループのルート リストを使用するルート パターンによってルーティングされる緊急通話が、訪問したサイトに対してローカルなイーグレス ゲートウェイを常に使用するようになります。

ローカル ルート グループのイーグレス ゲートウェイの選択は、ダイヤル プラン（14-1 ページ）の章で説明されているすべてのダイヤル プラン アプローチで使用できます。

ローミングしたエンドポイントが、特定のコールをホーム サイトのゲートウェイにルーティングする必要がある場合は、標準ローカル グループの代わりに固定されたサイト固有のルート グループを使用するルート リストを指すルート パターンを使用して、このようなコールのルーティングを実装する必要があります。

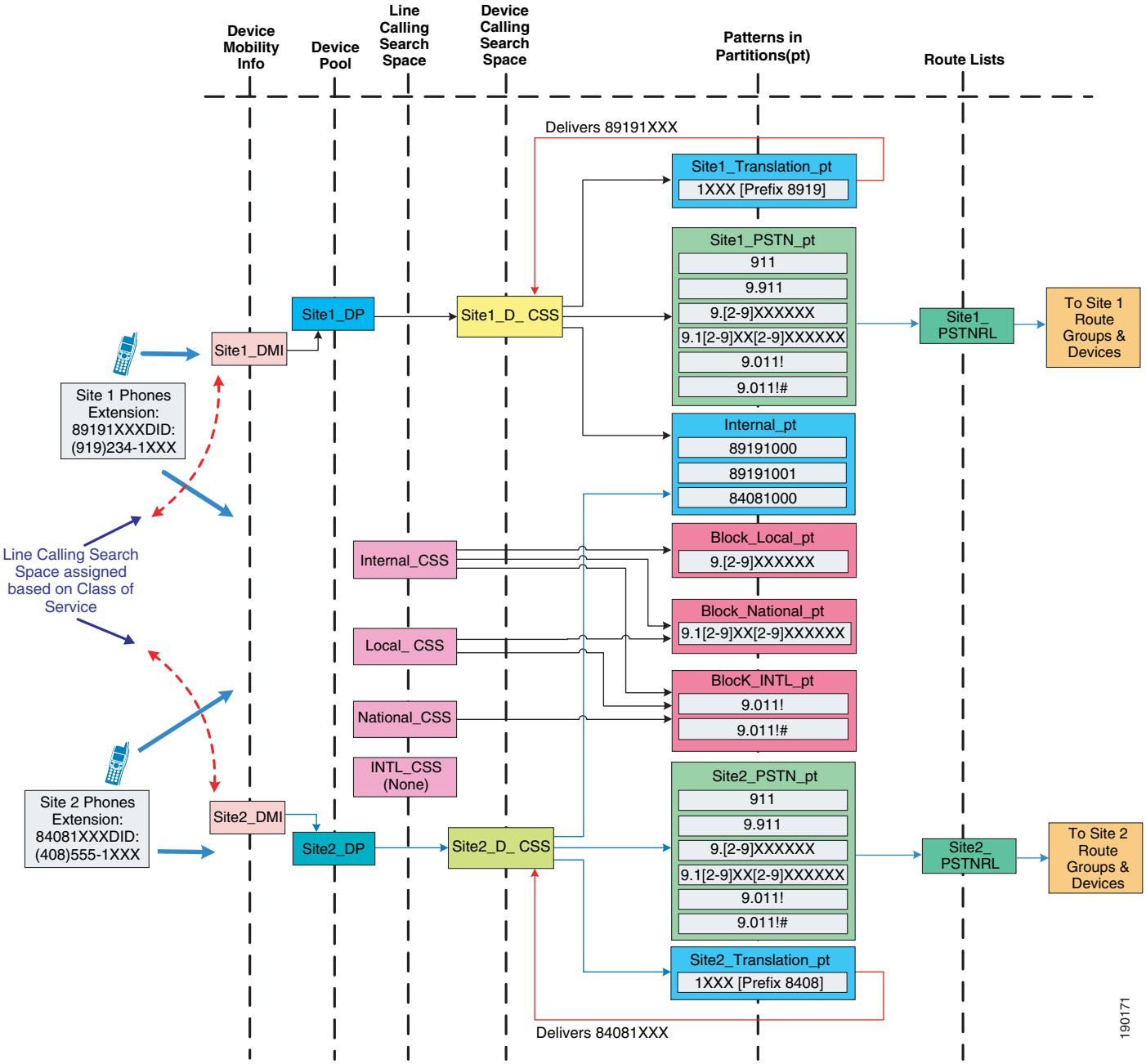
回線/デバイスのダイヤル プラン アプローチでは、これらのルート パターンはエンドポイントで設定されたデバイス CSS によってアドレス指定されます。ローミングし、かつ同一モビリティ グループを使用している場合には、発信側エンドポイントのデバイス CSS は、ローミング デバイス プールで設定されたデバイス モビリティ CSS に置き換えられます。固定されたイーグレス ゲートウェイの選択がいくつかのコールにおいて必要であり、これらのコールのルート パターンがデバイス CSS によってアドレス指定される場合、ローミング デバイスが常にデバイス モビリティ グループをまたがってローミングを行う必要があります。これは、ローミング エンドポイントが、エンドポイントで設定されたデバイス CSS を常に使用することを保証します。

ダイヤル プラン（14-1 ページ）の章で説明されている +E.164 ダイヤル プラン アプローチを使用する場合、すべての PSTN ルート パターンは、ローミング デバイスに対して変更されてないか、更新されていない回線 CSS によってアクセスされます。このダイヤル プランでは、固定ゲートウェイ（たとえば、ローミング デバイスのホーム ロケーション）に特定の PSTN にある宛先を接続しているサイト固有のルート パターンは、デバイス モビリティ動作から影響を受けません。

ローカル ルート グループを持たない回線/デバイス アプローチを使用する、フラット アドレッシングの可変長のオンネット ダイヤリング

図 21-9 は、デバイス モビリティのためのフラット アドレッシングによる可変長オンネット ダイヤリング プランを示します。

図 21-9　デバイス モビリティのためのフラット アドレッシングによる可変長オンネット ダイヤリング プラン



次の設計上の考慮事項が、図 21-9 のダイヤル プラン モデルに適用されます。

- このダイヤル プランで 4 桁のサイト内ダイヤリングを実装するトランスレーション パターンは、デバイス CSS によって参照されます。これは、サイト固有の回線 CSS を持つ要件を回避するために行われます。(ユーザがデバイス モビリティ グループ内でローミングしているとすると)デバイス CSS がローミング デバイス プールのデバイス モビリティ CSS で更新されるため、モバイル ユーザは訪問したサイトのサイト内ダイヤリングを継承します。この動作が望ましくない場合は、各サイトをデバイス モビリティ グループとして定義することを検討してください。ただし、ユーザは、外部 PSTN コールすべてで、モバイル電話では引き続きホーム ゲートウェイが使用され、したがって WAN 帯域幅が消費されることを承知しておく必要があります。これは、標準ローカル ルート グループを使用して回避できます(ローミング デバイスのイーグレス ゲートウェイの選択(21-22 ページ)を参照)。
- PSTN および内部電話機パーティションへのアクセスだけを持つローミング ユーザのために追加のデバイス コーリング サーチ スペースを設定できます。この設定には、サイトごとに 1 つ以上の追加のデバイス プールとコーリング サーチ スペースが必要です。したがって、*N* 個のサイトには、*N* 個のデバイス プールおよび *N* 個のコーリング サーチ スペースが必要です。ただし、この設定では、各サイトをデバイス モビリティ グループとして定義する必要がありません。この設定を適用しているモバイル ユーザは、ローミング時にデバイス CSS からトランスレーション パターンを参照しません。
- リモート SRST ゲートウェイに登録されているモバイル ユーザは、一意な内線番号を持ちます。ただし、モバイル ユーザは、リモート SRST ゲートウェイに登録されているときは、PSTN ユーザがモバイル ユーザと通話できないことを承知しておく必要があります。

従来のアプローチとローカル ルート グループを使用した +E.164 ダイヤル プラン

ダイヤル プラン(14-1 ページ)の章で説明したように、回線/デバイス アプローチにはいくつかの特定の問題があり、回線/デバイス アプローチに基づいて +E-164 ダイヤル プランを作成することは推奨されません。+E.164 ダイヤル プランの推奨されるアプローチは、回線 CSS でサービス クラスの選択とダイヤリングの正規化を組み合わせて、ローカル ルート グループ機能を使用してサイト固有のイーグレス ゲートウェイ選択の要件に対応することです。このアプローチでは、電話機のデバイス CSS はまったく使用されません。デバイス モビリティとこのアプローチを併用する場合、設計のローミングを受けやすい唯一のコンポーネントは、デバイス プールのローカル ルート グループです。ローミング電話機では(デバイス モビリティ グループ内またはデバイス モビリティ グループ間のローミング)、電話のホーム デバイス プールで定義されたローカル ルート グループは、ローミング デバイス プールで定義されたローカル ルート グループによって常に更新されます。これは、すべてのコールが、訪問したサイトに対してローカルなゲートウェイを介して出力されることを保証されます。

マルチサイト企業モビリティのハイ アベイラビリティ

マルチサイト企業モビリティ機能およびソリューションは、モビリティ機能のハイ アベイラビリティを保証するため、冗長性を備えた方法で設定、配置する必要があります。有線電話機の移動、無線ローミング、およびマルチサイト モビリティ配置での EM のハイ アベイラビリティの考慮事項は、キャンパス モビリティ配置での考慮事項と同様です。キャンパス環境と同じく、冗長ネットワーク ポート、無線セル カバレッジ、およびエクステンション モビリティのログインおよびログアウトを処理する Unified CM ノードが、高可用なサービスを確保するために必要です。

また、デバイス モビリティ機能のハイ アベイラビリティを考慮することも重要です。デバイス モビリティ機能はネイティブで Unified CM コール制御内に統合されているため、デバイス モビリティの機能がクラスタ ノードの障害による影響を受けることはありません。パブリッシャ ノードまたは呼処理（サブスクライバ）ノードに障害が発生した場合、デバイス プール、デバイス モビリティ情報、デバイス モビリティ グループ、およびデバイス モビリティに関連する他のすべての設定は保持されます。また、呼処理ノードに障害が発生した場合、影響を受ける電話機は、Unified CM Group の構成要素に基づいて、通常どおりセカンダリ呼処理ノードまたは Survivable Remote Site Telephony（SRST）リファレンス ルータにフェールオーバーします。

（注）　Cisco TelePresence System エンドポイントは Cisco IOS SRST での登録の冗長性をサポートしていません。

マルチサイト企業モビリティのキャパシティ プランニング

デバイス モビリティのスケーラビリティの考慮事項と同様、この機能および各種の構成要素（デバイス プールやデバイス モビリティ グループなど）に関連する特定のキャパシティ制限または強制的なキャパシティ制限はありません。一般的なシステム サイジング、キャパシティ プランニング、および配置上の考慮事項の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

マルチサイト企業モビリティの設計上の考慮事項

企業モビリティの設計上の考慮事項はすべて、マルチサイト企業モビリティ配置にも適用されます（キャンパス企業モビリティの設計上の考慮事項（21-11 ページ）を参照）。さらに、次の設計に関する推奨事項が、特にマルチサイト モビリティ環境に適用されます。

- サイト間の接続や、他のサイトの接続の障害が重要な動作を妨害しないよう、すべての重要なサービス（デバイス登録、PSTN 接続、DNS、DHCP など）をマルチサイト配置内の各サイトで確実に配置してください。加えて、デバイスや必要なコール キャパシティをサポートするため、十分な数の物理ネットワーク ポートおよびワイヤレス LAN AP が各サイトで使用できるようにしてください。
- 異なるダイヤリング パターンを持つ複数のサイト（たとえば、異なる PSTN アクセス コードを持つ複数のサイト）が同じデバイス モビリティ グループ内に設定されている場合、ローミング ユーザが各自のロケーションに基づいて異なる方法で番号をダイヤルする必要があるため、混乱を招く可能性があります。このため、類似のダイヤリング パターンを持つサイト（たとえば、同じ PSTN アクセス コードを持つサイト）を同じデバイス モビリティ グループに割り当てることを推奨します。これにより、ローミング ユーザは、デバイス モビリティ グループ内のすべてのサイトで同じ方法で番号をダイヤルできます。
- 「ローミング」デバイス プールからのデバイス モビリティ設定が適用されるのは、同じデバイス モビリティ グループ内でローミングするときだけです。移動された電話機からの元のコールが「ホーム」またはデバイスで設定されているコーリング サーチ スペースを使用し、結果的にコール ルーティング動作が引き起こされるため、異なるデバイス モビリティ グループ間でのローミングを避けてください。これにより、ローカルな「ローミング」ゲートウェイではなく別のサイトのゲートウェイを経由してコールがルーティングされる可能性があります。その結果、不必要に WAN 帯域幅が消費されることがあります。

- 物理ロケーションは各サイトに 1 つだけ定義してください。そうすることで、ユーザがサイト間でローミングを行う場合にだけ、デバイス モビリティが適用されます。同じサイト内でローミングを行う場合は、デバイス モビリティに影響する要素（たとえば、WAN 帯域幅消費、コーデック選択、コール アドミッション制御など）を考慮する必要はありません。単一のサイト内では通常、低速のリンクは配置されないためです。
- フェールオーバーのシナリオでは、「ローミング」電話機は、「ローミング」デバイス プールのローミング依存設定に従って、SRST リファレンス/ゲートウェイを利用します。したがって、これらの状況においては、「ローミング」電話機の DID は別のロケーションの PSTN ゲートウェイに固定されているために、PSTN からこの電話機に到達することはできません。さらに、「ローミング」電話機からコールを発信する場合は、PSTN アクセス コードなどの要素に対してダイヤリング動作を変更する必要があることがあります。また、電話機で設定されているスピード ダイヤルが使用できなくなることもあります。
- システムで、短縮ダイヤルを使用できることや、短縮ダイヤルに依存するスピード ダイヤルを使用できることが要求されている場合は、固定オンネット ダイヤル プラン モデルを使用することを推奨します。このモデルを使用すると、（直接またはスピード ダイヤルによる）短縮ダイヤルは、モバイル ユーザの電話機がローミングを行う場所にあっても、動作を継続するためです。すべての内線番号またはディレクトリ番号は全サイトにわたって一意であるため、短縮ダイヤルを使用し続けることができます。また、重複する内線番号がないため、短縮ダイヤルを普遍的に使用できます。
- システムが可変長オンネット ダイヤル プラン モデルを使用する場合（回線/デバイスまたは回線 CSS だけの +E.164 ダイヤル プラン アプローチを使用）、コールされたときに単一の一意の内線番号に到達されるように不変的な方法でスピード ダイヤルを設定することを推奨します。完全な +E.164 番号を使用するか、サイトまたはアクセス コードを使用してスピード ダイヤルを設定することにより、ローミング ユーザはすべてのロケーションで同じスピード ダイヤルを使用できます。
- VPN 接続を介して企業ネットワークにアクセスすることがあるユーザに対してデバイス モビリティを有効にした場合は、VPN ロケーションへの「ローミング」により確実に動的デバイス モビリティ設定変更が行われるように、VPN が接続された電話機のデバイス モビリティ情報（DMI）に、VPN コンセントレータにより配信または所有された IP サブネットが含まれている必要があります。DMI は、VPN コンセントレータと同じ場所にあるデバイスに使用されているデバイス プールに関連付ける必要があります。
- Cisco Expressway モバイル & リモート アクセスを介してエンタープライズ ネットワークにアクセスすることがあるユーザに対してデバイス モビリティを有効にした場合は、Expressway ロケーションへの「ローミング」により確実に動的デバイス モビリティ設定変更が行われるように、Expressway に接続しているデバイスのデバイス モビリティ情報（DMI）に、Expressway-C ノードにより使用された IP サブネットが含まれている必要があります。DMI は、Expressway-C ノードと同じ場所に配置されているデバイスに使用されているデバイス プールに関連付ける必要があります。

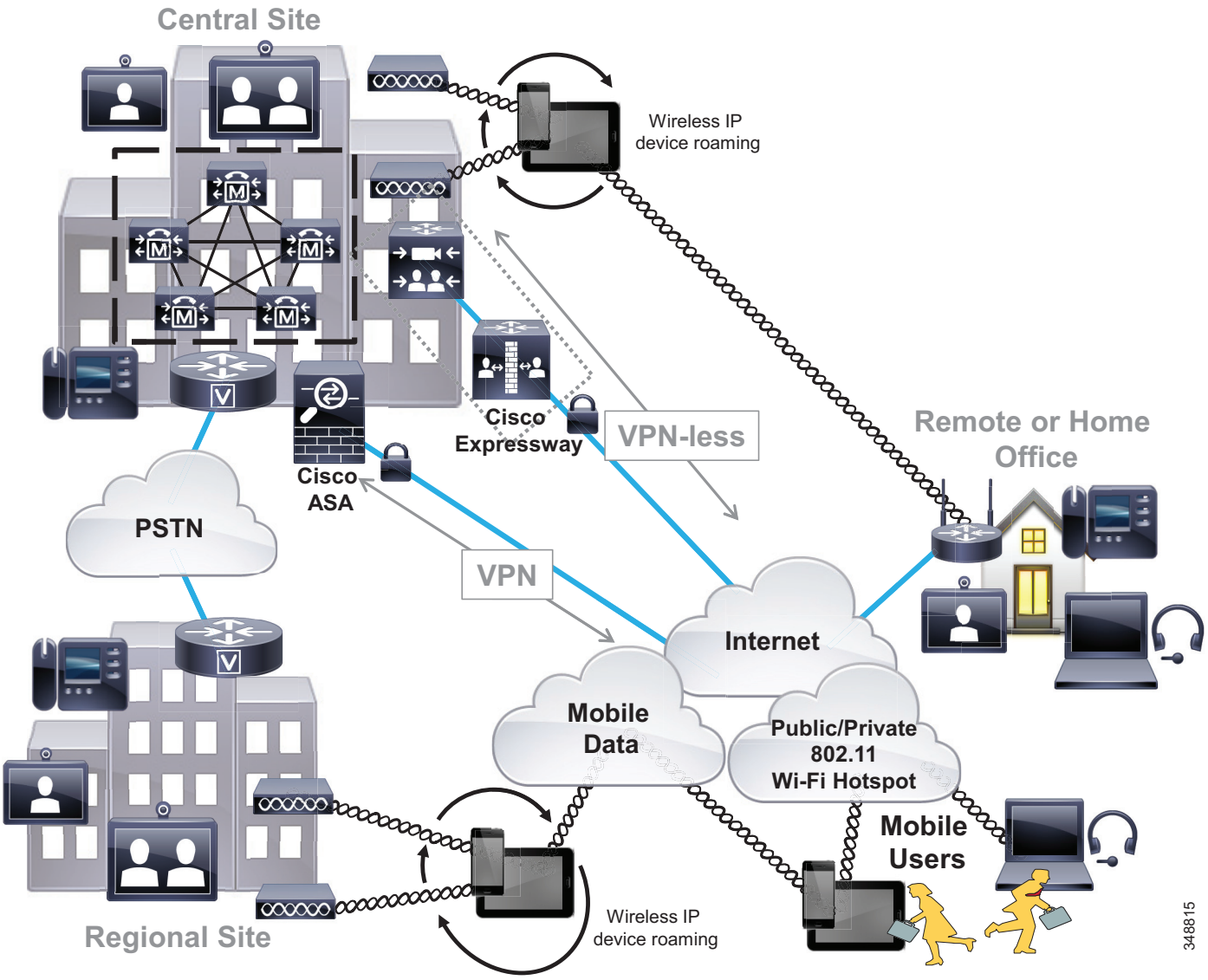
リモート企業モビリティ

リモート企業モビリティは、企業から離れたロケーションにいて、公共のインターネットを介した安全な接続により企業ネットワーク インフラストラクチャに接続しているモバイル ユーザを指します。ここでモビリティは、これらのリモート ロケーションでのエンドポイント デバイスの配置や、企業と各自のロケーション間での頻度に関わらないユーザの移動や、場合によってはユーザが使用するモバイル デバイスを処理します。

リモート企業モビリティのアーキテクチャ

図 21-10 に示すように、リモート企業モビリティのアーキテクチャは、リモート物理ロケーション（一般に、従業員のホーム オフィスや、それ以外の、インターネット経由で会社に安全に接続できるあらゆるリモート ロケーション）に基づいています。これらのリモート サイトは、一般にユーザのコンピュータ、電話機、およびその他の機器またはエンドポイントへ接続できる IP ネットワークで構成されます。場合によっては、この IP ネットワークを企業の制御下に置き、リモート ロケーションとエンタープライズ ネットワーク間に安全なトンネルまたは接続を備えた VPN ルータまたはエッジ セキュリティ プラットフォームを構成できます。また、リモート サイト IP ネットワークはインターネットへの接続を提供し、ユーザのコンピュータまたはエンドポイント デバイスでソフトウェアベースのクライアント機能を使用してエンタープライズ ネットワークへの安全な接続を作成する必要があります。無線接続をリモート ロケーションで使用して、ユーザのコンピュータまたはエンドポイントを無線接続できるようにすることもできます。無線接続をリモート ロケーションで使用する場合、ワイヤレス フォンおよびモバイル デバイスをエンタープライズ ネットワークからホーム オフィスへ移動することもでき、ワイヤレス企業デバイスまたはモバイル電話機をリモート ロケーション内で利用して発信および受信することもできます。

図 21-10　　リモート企業モビリティのアーキテクチャ



リモート企業モビリティのタイプ

リモート企業モビリティ配置は、デバイス モビリティをサポートすることではなく、主にリモート ユーザをサポートすることに重点を置いています。確かにユーザは、エンドポイント デバイスを持っても持たなくても定期的に企業ロケーション間またはロケーションとリモート サイト間を移動できます。ただし、これらの配置の主な目的は、固定したロケーションでも、アクティブに移動している場合でも、企業ユーザのリモート接続をサポートすることです。図 21-10 に示すように、リモート サイト モビリティには、主に 2 つのタイプのセキュア リモート接続があります。

- VPN セキュア リモート接続
- VPN なしのセキュア リモート接続

VPN セキュア リモート接続

VPN セキュア リモート接続は、企業およびリモート ネットワークまたはデバイス間のレイヤ 3 のセキュア トンネルを実現します。安全なリモート企業接続用の VPN 使用して、エンタープライズ ネットワークの境界を実質的に VPN 終端の場所まで拡張します。VPN 終端デバイスまたはネットワークの場所からの VPN 接続は、デバイスやネットワークが物理的に企業の境界内にある場合と同様のネットワークの接続性を提供します。Cisco 適応型セキュリティ アプライアンス（ASA）ヘッドエンド コンセントレータと Cisco AnyConnect クライアントは、安全なコラボレーションとその他の企業ワークフローの両方に VPN 接続を提供します。ルータ ベースの VPN 接続とクライアント ベースの VPN は、2 つの一般的な VPN 展開タイプです。どちらのタイプもリモート サイトへのセキュアな接続をサポートしており、固定された場所に残るものやリモート サイトと企業間で移動可能なものなど、さまざまなエンドポイント デバイスに対応できます。固定された場所のデバイスには、有線ビデオ エンドポイント、IP フォン、デスクトップ コンピュータなどがあります。デュアル モードの携帯電話、ワイヤレス IP フォン、ラップトップ コンピュータ、タブレットは、リモート サイトと企業間で定期的に移動するエンドポイントの例です。

ルータ ベースのリモート VPN 接続

ルータ ベースの VPN トンネルによりセキュアな接続が実現します。図 21-10 に示すように、これらのタイプのシナリオでは、配置したリモート サイト ルータ（たとえば、Cisco Virtual Office ソリューションのルータ）は、エンタープライズ ネットワークへの安全なレイヤ 3 VPN トンネルを設定する必要があります。これにより実質的に、企業ネットワークの境界をリモート サイト ロケーションまで広げます。このタイプの接続のメリットは、より幅広い種類のデバイスとエンドポイントをリモート サイトに配置できることです。これらのデバイスで接続の安全性を確保する必要がなく、特別なソフトウェアや設定の必要がないためです。代わりに、これらのデバイスはリモート サイト ネットワークに接続するだけで、リモート サイト ルータから企業 VPN ヘッドエンドまでの安全な VPN IP パスを利用できます。図 21-10 に示すように、リモート サイト ルータはワイヤレス ネットワーク接続も提供できます。

クライアントベースの安全なリモート接続

ワイヤレスおよび有線 IP フォンと、ソフトウェアベースの PC、スマート フォン、タブレットのテレフォニー クライアントは、図 21-10 に示すように、自宅、モバイル プロバイダー、Wi-Fi ホット スポット ネットワークなどのリモート ネットワークの場所からインターネット経由で接続できます。クライアント ベースの VPN シナリオの VPN 接続は、エンドポイント デバイスで実行しているソフトウェア クライアントによって確立されます。したがって、エンドポイントとソフトウェア クライアントは、企業の VPN ヘッドエンド ターミネーション コンセントレータに安全に VPN 接続する必要があります。これにより実質的に、エンタープライズ ネットワークの境界をリモート デバイスまで広げます。このタイプの接続のメリットは、ルータ ベースの VPN 接続が現実的ではないパブリック ネットワークを含め、より幅広いネットワークの場所に対応できることです。このようなさまざまなネットワーク間の接続によって、クライアント デバイスが移動中であっても安全な接続を実現できます。エンドポイント デバイスのタイプによっては、音声およびビデオ通話などのコラボレーションのワークフローが VPN 接続を利用する唯一の機能である場合があります。PC、スマート フォン、タブレットなどの多目的デバイスの場合、VPN 接続を介した完全な企業ワークフローが可能です。

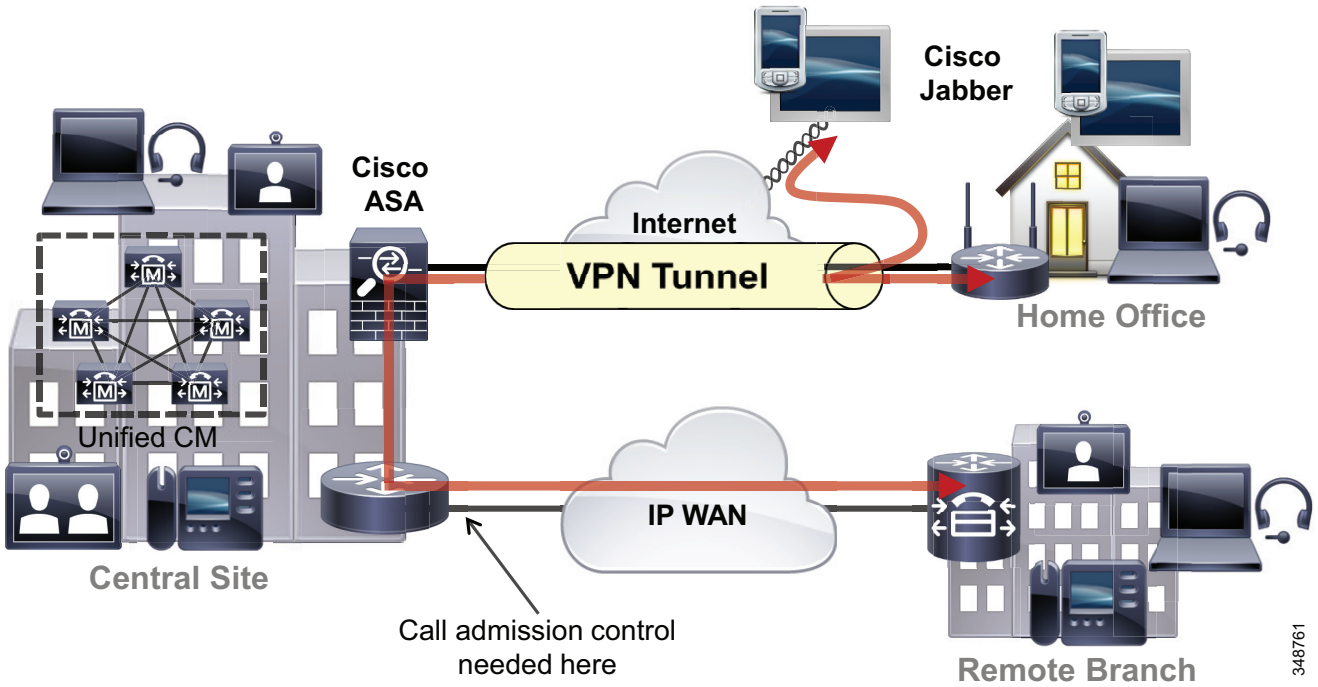
これらのタイプのデバイスの例には、有線またはワイヤレス接続の PC または Cisco AnyConnect などのソフトウェアベースの VPN を使用したワイヤレス接続のモバイル クライアント デバイスや、組み込み VPN クライアントを使用する Cisco Unified IP Phone 7965 などの有線の Cisco Unified IP Phone が含まれます。

デバイス モビリティと VPN のリモート企業接続

クライアントベースまたはルータベースの VPN リモート接続のどちらを配置するかにかかわらず、コール アドミッション制御およびコーデックがエンドポイント デバイスに正しくネゴシエートされ、適切な企業サイトの PSTN ゲートウェイおよびメディア リソースが使用されるようにするため、デバイス モビリティ機能を使用できます。VPN 接続経由で受信したエンドポイント デバイスの IP アドレスに基づいて、Unified CM はデバイスのロケーションを動的に決定します。

図 21-11 は、Cisco Jabber コラボレーション クライアントがリモート サイトのコンピュータまたはモバイル デバイスで実行されている、クライアントベースの安全なリモート接続の例です。このソフトウェアベースのコラボレーション アプリケーションは、クライアントベースの VPN を介して企業に接続され、Unified CM に登録されています。

図 21-11　　リモート サイトの Cisco Jabber 向けのクライアントベースの VPN 接続



次は、クライエントベースまたはルータベースの VPN 接続経由で企業に接続しているリモート サイトにおける、ユーザ デバイスのデバイス モビリティ機能の有効化に関する設計ガイドラインです。

- VPN コンセントレータによって配布または所有されている IP サブネットを指定してデバイス モビリティ情報（DMI）を設定します。
- VPN コンセントレータと同じ場所にあるデバイスに使用されるデバイス プールと同じデバイス プールに DMI を関連付けます。ただし、コール特権、ネットワーク ロケールなどのパラメータを考慮する必要があります。
- リモート サイトのユーザに、クライアントベースまたはルータベースの VPN 接続を行う場合は、地理的に最も近い企業 VPN コンセントレータを指定するよう指導します。

これらのガイドラインにより、確実に、企業 WAN 上でおよびリモート サイトへの接続を介して、コール アドミッション制御が正しく適用されます。

VPN の配置の詳細については、次のサイトの Design Zone for Security の *Security in WAN* で入手可能な各種の VPN 設計ガイドを参照してください。

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_wan_security.html

VPN なしのセキュア リモート接続

VPN なしのセキュア リモート接続により、企業とリモート接続デバイス間のリバース プロキシ TLS のセキュアな接続が可能になります。このタイプの接続では、完全なレイヤ 3 VPN トンネルに必要なオーバーヘッドを最小限に抑えながら、セキュアなファイアウォール トラバーサルが許可されます。VPN なしのリバース プロキシを使用して、セキュアな接続はデバイスまたはクライアント アプリケーションまでエンタープライズ ネットワークの境界を拡張します。Cisco Collaboration Edge アーキテクチャには Cisco Expressway が採用されています。

Cisco Expressway により、トラフィックが企業の物理境界内で生成される場合のように、特定のエンドポイントまたはクライアント アプリケーションのトラフィック フローにセキュアなトラバーサルを提供します。ただし、すべてのトラフィック フローがこの接続タイプでサポートされるわけではありません。ここで説明した Cisco Collaboration Edge Architecture ソリューションは、音声およびビデオ通話、IM およびプレゼンス、ビジュアル ボイスメール、および社内ディレクトリ アクセスなどのコラボレーション ワークフローを保護します。非コラボレーション アプリケーションやサービスへのアクセスを含む完全な企業ワークフローは、次の接続のタイプではサポートされません。

Cisco Collaboration Edge Architecture の詳細については、次のサイトで入手可能なマニュアルを参照してください。

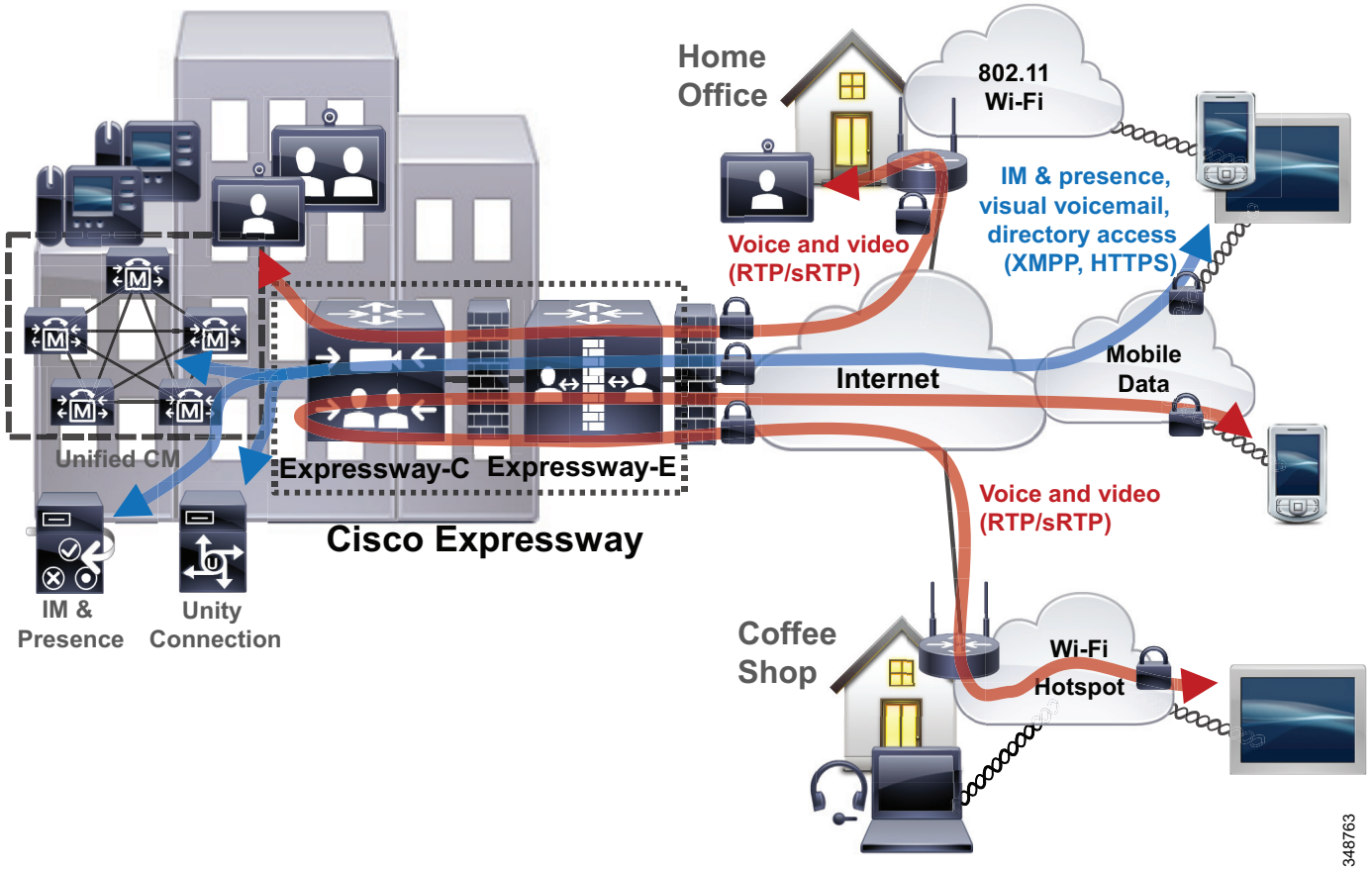
https://www.cisco.com/c/en/us/solutions/collaboration/collaboration-edge-architecture/index.html

Cisco Expressway

Cisco Expressway ソリューションのモバイル & リモート アクセス機能は、逆プロキシ ファイアウォール トラバーサル接続を提供します。これにより、リモート ユーザとそのデバイスが企業のコラボレーション アプリケーションおよびサービスにアクセスして利用できます。

図 21-12 に示すように、Cisco Expressway ソリューションには、2 つの主なコンポーネント（Expressway-E ノードと Expressway-C ノード）が含まれています。これら 2 つのコンポーネントは Unified CM と組み合わせて動作し、安全なモバイル & リモート アクセスを実現します。Expressway-E ノードは、モバイル & リモート デバイスにセキュアなエッジ インターフェイスを提供します。通常、このノードはエンタープライズ ネットワークの DMZ 領域内にあります。Expressway-C ノードは、Unified CM へのプロキシ登録を提供し、リモート セキュア エンドポイント登録を可能にします。内部エンタープライズ ネットワークにある Expressway-C ノードは、Expressway-E ノードとのセキュアな TLS アウトバウンド接続を確立します。この接続がセキュアなメディア トラバーサルに使用されます。

図 21-12　Cisco Expressway モバイル & リモート アクセスの安全なリモート コラボレーション



Unified CM に登録されると、リモート デバイスは SIP シグナリングと RTP メディアを使用して IP 経由で音声およびビデオ通話の発信および受信ができるようになります。安全な Cisco Expressway モバイル & リモート接続は、デバイス登録および音声とビデオ通話だけでなく、IM およびプレゼンス、ビジュアル ボイスメール、社内ディレクトリ アクセスなどのコラボレーションのワークフローが追加で可能になります。完全なコラボレーション機能は、VPN トンネルを必要とせずに企業から入手できます。音声およびビデオ メディア、シグナリング、およびその他のコラボレーション トラフィックは Expressway C ノードでエンタープライズ ネットワークを通過します。図 21-12 に示すように、社外の 2 台のリモート デバイス間のコールが社内 Expressway C のノードでヘアピンされます。

セキュアなエンドポイントからすべてのトラフィックが VPN トンネルを通過して企業に戻る VPN セキュア接続とは異なり、Cisco Expressway モバイル & リモート アクセスは、コラボレーション トラフィックのみで企業への安全な接続を実現します。非コラボレーション ワークフローおよびトラフィックはセキュア Cisco Expressway 接続を通過しません。代わりに、他のすべてのトラフィックはローカル ネットワークまたはインターネットに直接送信され、エンタープライズ ネットワークを通過しません。

Cisco Expressway モバイル & リモート アクセス機能は、Cisco ハードウェアのエンドポイントおよび Cisco Jabber ソフトウェア ベースのクライアント エンドポイントの両方をサポートします。サポートされている Cisco ハードウェア エンドポイントには Cisco TelePresence EX、MX、および SX シリーズのビデオ エンドポイント、Cisco DX、7800、および 8800 シリーズのデスクフォンがあります。Cisco Jabber デスクトップおよびモバイル クライアントも、Cisco Expressway モバイル & リモート アクセスをサポートします。特に、Cisco Jabber モバイル クライアントは Cisco Expressway モバイル & リモート アクセス接続を移動中もサポートするため、モバイル ユーザの場所やネットワーク接続のタイプに関係なく、安全なリアルタイム コラボレーションが可能になります。

リモート セキュア接続の実現に VPN を使用する場合と同様、Expressway モバイル & リモート アクセスを使用したデバイス モビリティ設定は、低速リンクのコール量の監視、適切なコーデックのネゴシエーション、およびローカル ゲートウェイ リソースを使用したコールのルーティングのために Unified CM がエンドポイントの場所を追跡できるようにする上で重要です。Expressway モバイル & リモート アクセスを使用している環境でデバイス モビリティを設定するときには、次の作業を必ず行ってください。

- Expressway-C ノードが使用する IP サブネットを使用してデバイス モビリティ情報（DMI）を設定します。
- Expressway-C ノードと同じ場所に配置されているデバイスに使用されているデバイス プールに、DMI を関連付けます。

Cisco Expressway モバイル & リモート アクセス機能では、Expressway-C と Expressway-E クラスタのペアあたり最大 10,000 件の Unified CM へのリモート エンドポイント登録がサポートされています。また Expressway クラスタ ペアでは最大 2,000 の同時ビデオ コールまたは 4,000 の同時音声のみのコールがサポートされています。Expressway ノードあたりのキャパシティを含む Cisco Expressway のキャパシティの詳細については、Cisco Expressway（25-39 ページ）の項を参照してください。

規模拡大または複数の地理的な場所を対象とした設計に対応するため、複数の Expressway クラスタを展開します。複数サイトを導入する場合、場所に関係なくユーザとユーザのデバイスに対してリモート企業接続を提供するため、Expressway クラスタを複数の地域にわたって分散する必要があります。Expressway モバイル & リモート アクセス接続を効果的に分散し、デバイスが最も近い位置の Expressway サービス ノードまたはクラスタに接続できるようにするには、GeoDNS サービスが推奨されます。GeoDNS サービスにより、Expressway DNS サービス レコードに対する DNS クエリの送信元 IP アドレスにより決定される場所、またはデバイスの場所と使用可能な Expressway サービス ノードの間での最も短い平均遅延に基づき、モバイル デバイスは最も近い Expressway サービス ポイントに振り分けられます。

Cisco Expressway ソリューションの詳細については、次の Web サイトで入手可能なデータ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html

リモート企業モビリティのハイ アベイラビリティ

リモート サイト モビリティ環境では、企業 VPN または VPN なしのセキュリティ サービスが、冗長性を備えた方法で企業内に設定され配置されている必要があります。これにより、VPN とリバース プロキシ ファイアウォール トラバーサルによる安全な接続の可用性が高いことが保証されます。企業内または企業エッジの VPN コンセントレータまたは Cisco Expressway ノードで障害が発生した場合、他の VPN または VPN なしのリモート エッジ ノードを備えたクライアントまたはエンドポイントで、新しい安全な接続を設定できます。Unified CM クラスタまたはその他のアプリケーション サーバ ノードの冗長性に基づき、デバイス登録、音声およびビデオ サービス、IM およびプレゼンス、およびその他のコラボレーション サービスの可用性が高くなります。このレベルのコラボレーション サービスの冗長性は、オンプレミスと同様に、エンドポイントとクライアントが VPN 経由で企業に接続される場合にも適用されます。

エンドポイントとクライアントが Cisco Expressway モバイル & リモート アクセスを使用して接続している場合は、コラボレーション アプリケーションとサービスの冗長性が限定されます。Cisco Expressway ソリューションの場合、モバイル & リモート アクセスのハイ アベイラビリティは各ノード タイプのクラスタを配置することによって実現されます。Unified CM ノードのクラスタ、Expressway E のノードのクラスタ、および Expressway C のノードのクラスタの配置では、1 つまたは複数のプライマリ ノードに障害が発生した場合に、バックアップ ノードがモバイル & リモート アクセスおよびデバイス登録を提供できます。

リモート企業モビリティのキャパシティ プランニング

リモート企業モビリティ環境のスケーラビリティの考慮事項で最も重要なのは、企業のヘッドエンド セッション終端装置です。管理者は、すべてのリモート セキュア接続要件に対応する十分な VPN セッションおよび VPN なしの接続キャパシティを配置する必要があります。Cisco Expressway 経由のクライアントまたはルータ ベースの VPN または VPN なしのリモート エッジ セキュア接続の場合も、デバイス登録の負荷およびセキュア接続で利用可能なさまざまなコラボレーションのワークフローを処理できる十分なプラットフォームまたはノードの容量を提供する必要があります。適切なキャパシティを用意しないと、一部のリモート サイトとデバイスが会社に接続できなくなり、基本的なテレフォニー サービスでもアクセスできなくなります。さらに、キャンパスまたはマルチサイト企業モビリティの配置と同様、すべてのリモート ユーザのデバイスを処理できるよう、企業内に十分なデバイス登録キャパシティを用意することが重要です。

Cisco Call Control およびゲートウェイ エッジでのキャパシティ（プラットフォーム固有のエンドポイント設定や登録キャパシティなど）の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

リモート企業モビリティの設計上の考慮事項

モバイル ユーザがリモート サイト接続できるようにする場合、次の設計上の推奨事項を考慮してください。

- デバイス モビリティを使用する場合は、VPN コンセントレータが配布または所有する IP サブネットを含むデバイス モビリティ情報（DMI）、または、Expressway の場合は、Expressway-C ノードで使用されるサブネットを含むデバイス モビリティ情報を、忘れずに設定してください。VPN コンセントレータや Expressway-C ノードと同じ場所に設置されたデバイス用に設定されるデバイス プールに、DMI を割り当てます。
- リモート サイト ユーザに、VPN を接続する場合は最も近い VPN コンセントレータを選択するよう指導します。

- VPN を使用したすべてのリモート サイトの場所およびデバイスへの接続を用意するため、適切な VPN セッション キャパシティが確実に使用できるようにしてください。
- すべてのリモート デバイスへの VPN なしのセキュアな接続を用意するため、適切なリバース プロキシ ファイアウォール通過セッション キャパシティが確実に使用できるようにしてください。十分な Expressway-E と Expressway-C ノードおよびセッション キャパシティが確実に使用できるようにしてください。いずれの場合も、十分な Unified CM 登録キャパシティが必要です。

クラウド サービスとハイブリッド サービスのモビリティ

クラウド サービスとハイブリッド サービスのモビリティとは、Cisco Collaboration Cloud から配信されるコラボレーション アプリケーションとコラボレーション サービスを利用するモバイル ユーザのことです。このようなタイプのモビリティには、クラウド コラボレーション サービスのみを利用する純粋なクラウド展開と、クラウドと企業オンプレミスの両方のコラボレーション アプリケーションやサービスを活用するハイブリッド展開が含まれます。

モバイル デバイスとクライアントは、インターネットを介して Cisco Collaboration Cloud および他のクラウドのコラボレーション アプリケーションとサービスに接続します。クライアントとデバイスは、企業オンプレミスでもリモートのどちらにいてもかまいません。インターネットへのアクセスにより、各デバイスは（移動中でも移動していなくても）エンタープライズ ネットワークや公共ネットワーク、またはプライベート ネットワークを介して接続されるこれらのサービスを利用できます。

企業はクラウドからのコラボレーション サービスを有効にし、状況によっては、さまざまな理由からこれらのサービスを企業のコラボレーション インフラストラクチャに統合します。企業において、ソフトウェア サービスとアプリケーションの配信で、クラウドへの注目度が高まっている主な理由には次のようなものがあります。

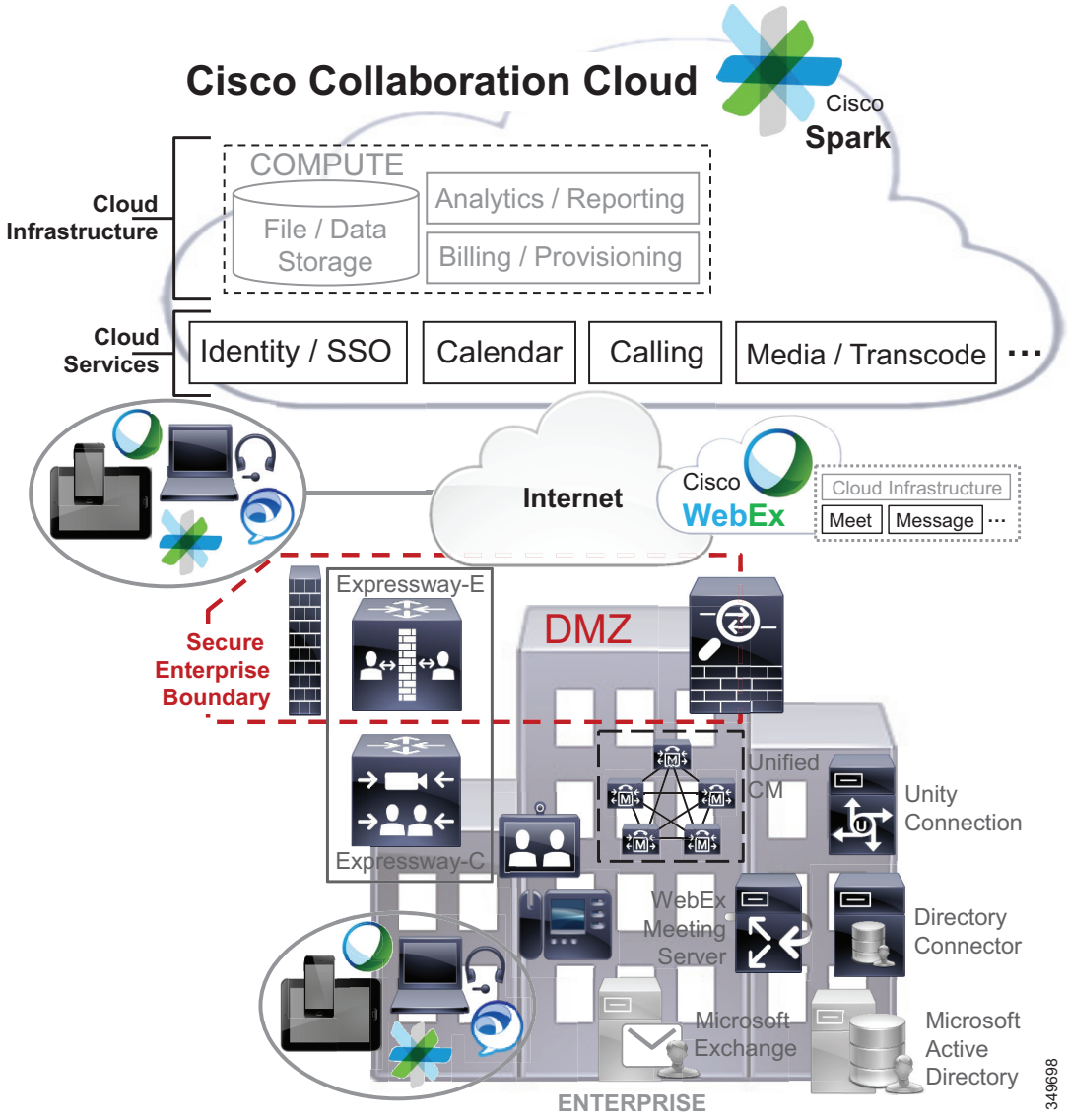
- クラウド サービス更新プログラムは継続的かつ自動的に配信されるため、新しい機能と報告されている問題の解決が迅速に提供される
- コンピューティング リソースが柔軟に運用されるので、オンデマンドのユーザ キャパシティとサービス パフォーマンスが実現
- クラウド アプリケーションおよびサービス機能の一元化されたオンライン管理が可能
- 可用性の高いクラウド アーキテクチャにより、広い地域をカバーすると同時にサービスの復元力を提供
- インフラストラクチャの資本コストと管理は、クラウド ベンダーが負担ベンダーはインフラストラクチャを管理し、そのセキュリティにも責任を持ちます。これには、コンピューティング、ストレージ、電源、ネットワーク、および基本的なサービスとアプリケーションが含まれます。

クラウドおよびハイブリッド サービスのモビリティ アーキテクチャ

図 21-13 に示すように、クラウドおよびハイブリッド サービスのモビリティ アーキテクチャはインターネットに接続された Cisco Collaboration Cloud および Cisco WebEx Collaboration Cloud サービスに基づいています。Collaboration Cloud と WebEx Collaboration Cloud サービスは、セキュアで復元力のあるクラウド コンピューティング インフラストラクチャで実現されます。このアーキテクチャで配信されるクラウド コラボレーション サービスには、Cisco Spark メッセージ、会議、コールと、WebEx ミーティングとメッセージングがあります。これらのサービスは純粋なクラウド導入に加えて、企業のオンプレミス サービスとともに導入することもできます。たとえば、企業は WebEx Meeting Center の会議および WebEx Messenger IM and Presence（クラウドからのサービス）を、Unified CM の音声およびビデオ通話および Unity Connection のボイス メッセージング（オンプレミスで提供されるサービス）と並行して有効にできます。Cisco Spark のメッセージ、会議、通話は、企業アイデンティティ、シングル サインオン（SSO）、予定表、通話などのクラウド ハイブリッド サービスの企業統合で強化できます。

クラウド サービスの企業統合は一般に、サービス関連のトラフィックを企業が送受信するための、クラウドと企業間のセキュアな接続に依存します。このトラフィックは図 21-13 に示すように、セキュアな企業境界 DMZ を通過する必要があります。

図 21-13　クラウドおよびハイブリッド サービスのモビリティ アーキテクチャ



Cisco Jabber、Cisco Spark、Cisco WebEx などのシスコのデスクトップ、Web ブラウザ、モバイル デバイスのコラボレーション アプリケーションやクライアントは、企業外からのインターネットを介したリモート接続または社内接続のどちらでも、シスコ コラボレーション クラウドおよび WebEx Collaboration Cloud からのサービスを利用します。

クラウドベースのサービスを利用できる Cisco クライアントについての詳細は、シスコのモバイル クライアントおよびデバイス（21-81 ページ）を参照してください。

クラウド ハイブリッド サービス統合のタイプ

クラウド ハイブリッド コラボレーション サービスの統合には主に 2 つのタイプがあります。

- Cisco WebEx Collaboration Cloud のハイブリッド統合（21-39 ページ）
- Cisco Spark Hybrid Services（21-39 ページ）

Cisco WebEx Collaboration Cloud のハイブリッド統合

Cisco WebEx Collaboration Cloud の機能はスタンドアロン サービスとして利用可能である一方、ハイブリッド統合により、既存の企業のオンプレミス コラボレーション サービスを強化して、以下も実現できます。

- Cisco WebEx Messenger サービスを使用したインスタント メッセージング（IM）とプレゼンス
- Cisco WebEx Meetings サービスを使用した、デスクトップ共有による音声およびビデオ会議

Cisco WebEx のハイブリッド統合はこの章ではとりあげません。

Cisco WebEx Collaboration Cloud およびハイブリッドの企業のコラボレーションの統合の詳細については、Cisco WebEx Software as a Service（11-28 ページ）のセクションを参照してください。

Cisco WebEx Messenger とハイブリッドの企業の統合の詳細については、Cisco WebEx Messenger（20-68 ページ）のセクションを参照してください。

Cisco Spark Hybrid Services

Cisco Collaboration Cloud で実現される Cisco Spark のハイブリッド コラボレーション サービス統合は次のとおりです。

- Cisco Spark アイデンティティ サービス（21-39 ページ）
- Cisco Spark カレンダー サービス（21-41 ページ）
- Cisco Spark コール サービス（21-44 ページ）

Cisco Spark Hybrid Services に関する一般的な情報については、https://collaborationhelp.cisco.com/article/en-us/DOC-6433 に掲載されている基本情報を参照してください。

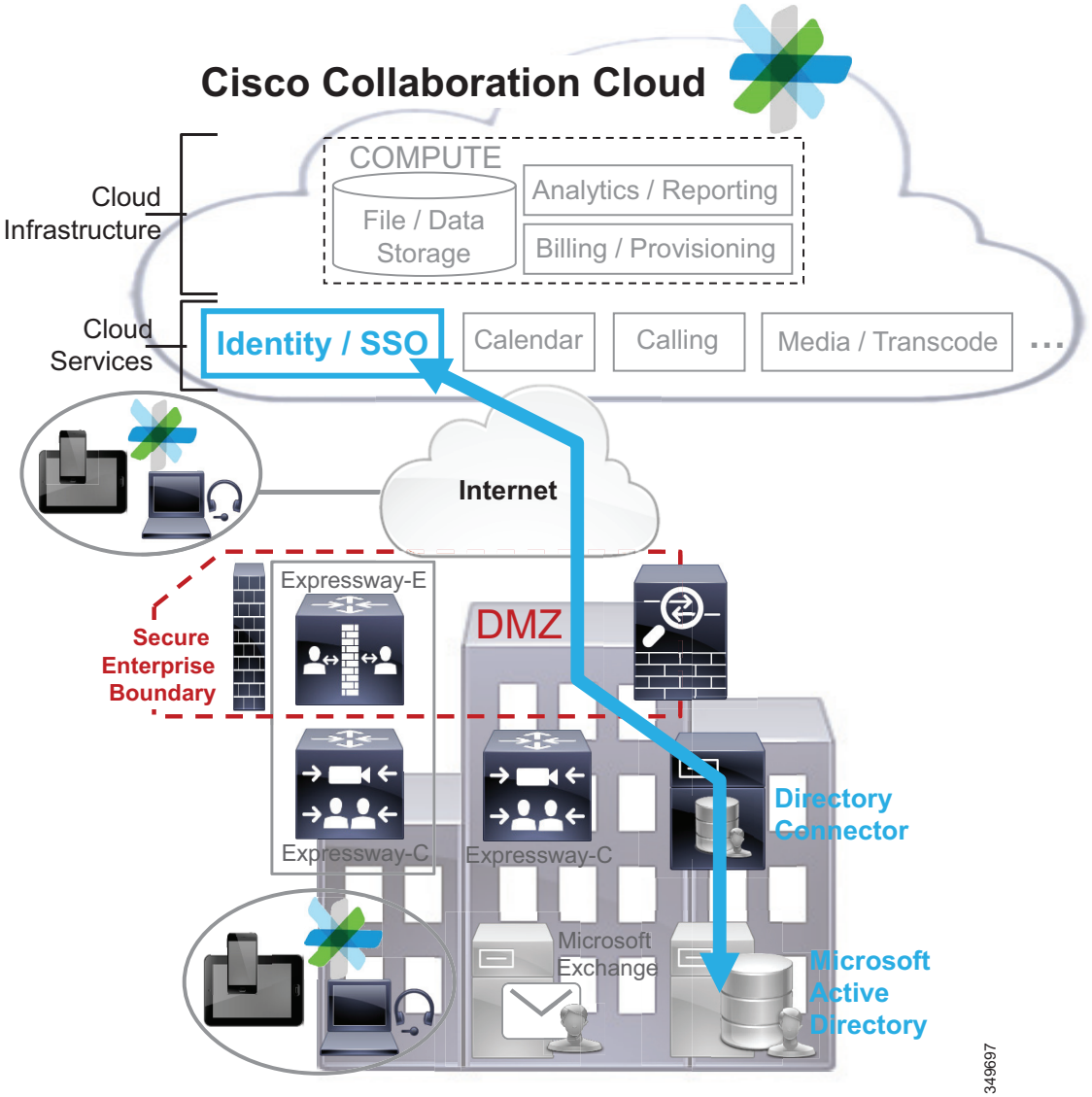
Cisco Spark アイデンティティ サービス

Cisco Spark Hybrid Services は、企業のオンプレミス Microsoft Active Directory を Cisco Collaboration Cloud Common Identity Services（CIS）と統合するためのメカニズムを提供します。エンタープライズ ディレクトリ情報をクラウドの CIS と同期することで、組織はシスコ クラウドための企業ユーザの設定とプロビジョニングを迅速に実現できます。企業が Cisco Spark Hybrid Services のシングル サインオン（SSO）を実装または統合する場合には、クラウドのアイデンティティ サービスに SSO 機能も含まれることに注意してください。

図 21-14 に示すように、オンプレミスの Cisco Directory Connector は、Microsoft Active Directory とエンタープライズ ネットワークを介して通信し、同期します。次に、Directory Connector はディレクトリ データをプッシュし、セキュアな企業境界および企業のファイアウォールを通って、インターネットを介しクラウド アイデンティティ（CIS）および SSO サービスと通信します。クラウドへのこの接続は企業内から開始され、企業のファイアウォールでポートを開く必要はありません。これは、インターネット上の Web サーバへのアウトバウンド接続を開始し、同じ接続で応答を受信する HTTPS Web クライアントに似ています。

クラウドの CIS とオンプレミスの Cisco Directory Connector との間の通信には HTTPS が使用されます。Cisco Directory Connector と Microsoft Active Directory 間の同期には、Microsoft Active Directory API が使用されます。

図 21-14　Cisco Spark Hybrid Services：クラウド アイデンティティ サービスとエンタープライズ ディレクトリの統合



ユーザの同期に使用される CIS と Directory Connector 間の接続は、Directory Connector ソフトウェアのインストール中に自動的にセットアップされます。Directory Connector ソフトウェアは Cisco Spark Control Hub からダウンロードされます。ユーザ情報を同期するために使用される Directory Connector と Microsoft AD 間の接続は、Directory Connector 上の設定で制御されます。Directory Connector 管理ページのグラフィカル ユーザ インターフェイスを使用して、オブジェクト タイプ、LDAP フィールドのマッピング、ベース DN を設定し、どのユーザ アカウントでどのアカウント情報を同期するかを制御します。

Cisco Directory Connector ソフトウェアは Microsoft Windows Server オペレーティング システムが動作するサーバまたは仮想マシンにインストールして実行します。Cisco Directory Connector の導入には次の要件と推奨が適用されます。

- Microsoft Windows サーバまたは仮想マシンは、企業の Microsoft Active Directory ドメインのメンバーである必要があります。
- Directory Connector ソフトウェアはドメインの管理者権限を持つアカウントを使用して Windows サーバまたは仮想マシンにインストールする必要があります。
- Active Directory の電子メール アドレス属性は、Cisco CIS と同期するすべてのユーザ アカウントに設定される必要があります。電子メール アドレスのない Active Directory のユーザ アカウントは、CIS と同期されません。
- Directory Connector は、Active Directory Domain Service（AD DS）および Active Directory Lightweight Directory Service（AD LDS）とは別のサーバまたは仮想マシンにインストールすることを推奨します。

導入の要件、インストール、設定を含め、Cisco Directory Connector の詳細については、以下のリンク先から入手できる最新バージョンの『*Deployment Guide for Cisco Directory Connector*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html

企業ユーザがオンプレミス Microsoft Active Directory と Cisco Collaboration Cloud CIS の間で同期された後は、組織の管理者が Cisco Spark Control Hub を使用してユーザ アカウントを簡単に管理できます。管理者はこのハブからユーザ ロールを割り当て、ユーザ機能を管理し、Cisco Spark Hybrid Services などの特定のクラウド サービスに対してユーザに権限を付与したりユーザを有効にしたりします。

Cisco Spark カレンダー サービス

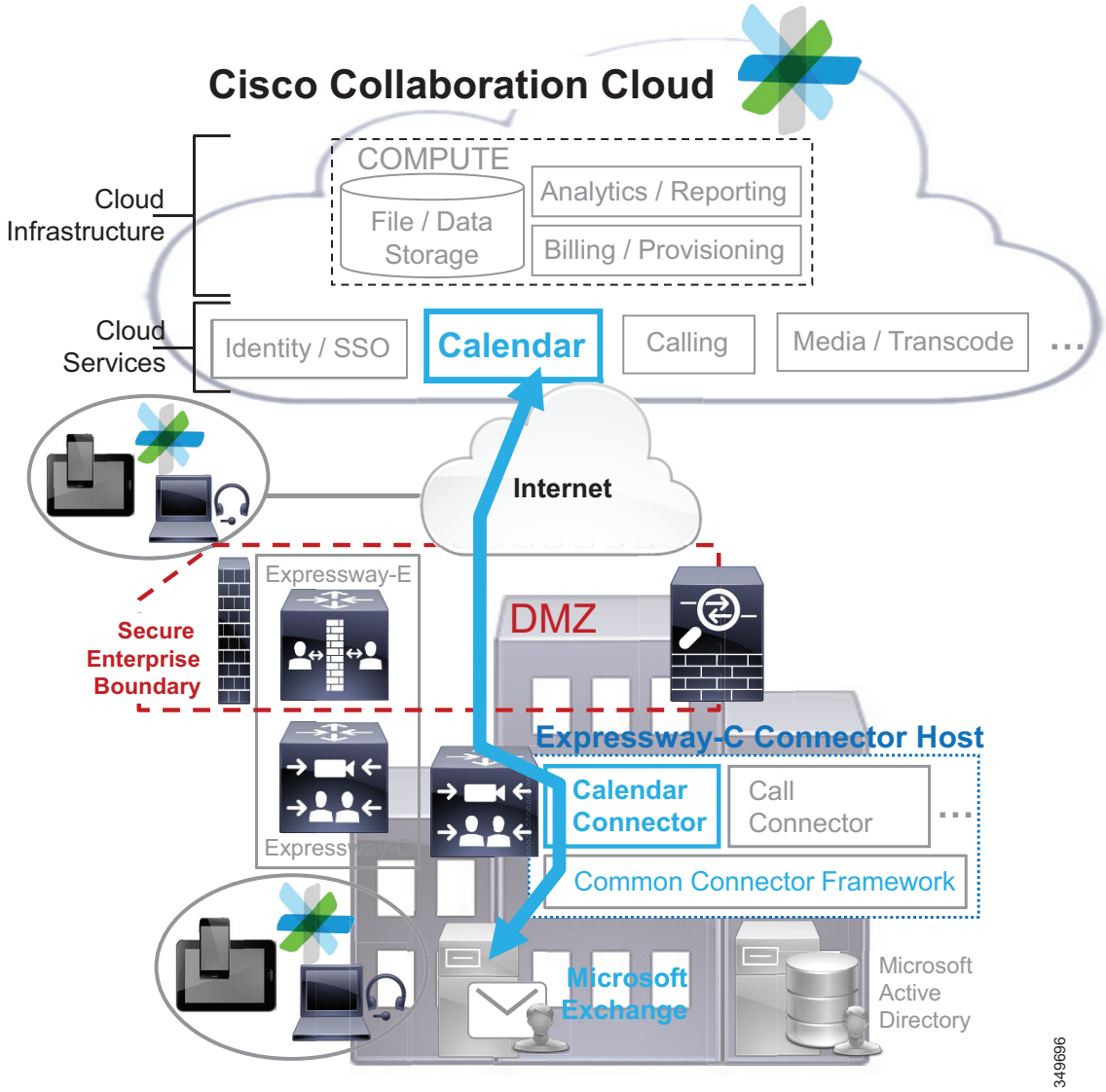
Cisco Spark Hybrid Services は、企業のオンプレミスの Microsoft Exchange の予定表機能を Cisco Collaboration Cloud のカレンダー サービスと統合するためのメカニズムを提供します。企業のカレンダー サービスを Cisco Collaboration Cloud に統合すると、組織は、会議の出席依頼の [ロケーション（location）] フィールドに @spark や @webex を含めるだけで、Outlook の会議の招待に Cisco Spark および Cisco WebEx の豊富なコラボレーション機能を自動的に組み込むことができます。

カレンダー コネクタは、クラウドのカレンダー サービスと企業の Exchange 環境間の統合とコミュニケーションの仲介を担当します。図 21-15 に示すように、基盤となる一般的なコネクタ フレームワークに依存するオンプレミス Cisco Expressway-C コネクタのホスト カレンダー コネクタは、エンタープライズ ネットワークで Microsoft Exchange と通信します。次に、カレンダー コネクタは予定表データをプッシュし、セキュアな企業の境界および企業のファイアウォールを通って、インターネットを介しクラウドのカレンダー サービスと通信します。クラウドへのこの接続は企業内から開始され、企業のファイアウォールでポートを開く必要はありません。これは、インターネット上の Web サーバへのアウトバウンド接続を開始し、同じ接続で応答を受信する HTTPS Web クライアントに似ています。

クラウドのカレンダー サービスとオンプレミスのカレンダー コネクタとの間の通信には HTTPS が使用されます。Expressway-C のカレンダー コネクタ コンポーネントと Microsoft Exchange 環境間の通信には Microsoft Exchange Web サービス（EWS）が使用されます。

カレンダー コネクタは Exchange 環境と通信を行い、通知をモニタしてユーザの予定表からの情報を取得し、Cisco Spark のルーム情報と WebEx ミーティング情報を会議の招待に追加します。

図 21-15　Cisco Spark Hybrid Services：企業予定表の統合



Expressway-C コネクタ ホストと Cisco Collaboration Cloud 間の接続と、クラウドのカレンダー サービスとカレンダー コネクタ間の接続は、Expressway-C のハイブリッド サービス コネクタの設定時に自動的に確立されます。Calendar Connector ソフトウェアは、Expressway-C を正常に登録した後（すでに登録されている場合は、カレンダー コネクタ サービスが Cisco Spark Control Hub から有効にされた時点で）、Cisco Collaboration Cloud から Expressway-C に自動的にダウンロードされ、インストールされます。

Expressway-C のグラフィカル ユーザ インターフェイスでのカレンダー コネクタの設定中に、Microsoft Exchange の接続情報を管理者が提供します（または、企業の Active Directory から取得されることもあります）。さらに管理者は、@webex が招待ロケーション フィールドに指定されたときに WebEx ミーティング ルームの詳細が会議の招待に追加されるよう、組織の WebEx Meeting Center と Collaboration Meeting Room のサイト情報を指定します。

Expressway-C および共通コネクタ フレームワークを利用する Cisco Spark Hybrid Services では Cisco Collaboration Cloud とオンプレミス Expressway-C との間のセキュアな接続が必要です。Expressway-C のカレンダー コネクタを動作させるために、コネクタ管理とカレンダー サービスのために Cisco Collaboration Cloud が提供する CA 署名付き証明書を Expressway-C の証明書信頼リストと照合します。これにより、Expressway-C と Collaboration Cloud 間のセキュアな接続が提供されます。Expressway-C は、Calendar Connector ソフトウェアをダウンロードしてカレンダー コネクタ サービスを開始する前に、クラウドの証明書を確認します。カレンダー コネクタ サービスはクラウドの証明書 CA が信頼リストにない場合、開始されません。クラウドは最初の設定時に、必要なクラウドのパブリック CA 証明書を Expressway-C の信頼リストに自動的に追加します。または、組織がクラウドの証明書を手動で管理することを選択する場合もあります。その場合は、Expressway の管理者がクラウドの CA 証明書を Expressway の信頼リストに追加して、正しい操作を確保します。任意で、Expressway-C のカレンダー コネクタと企業の Exchange サーバ間で CA 証明書を交換し、各サーバの信頼リストに追加すれば、セキュア接続が両者の間の接続にまで拡張されます。

カレンダー コネクタと Microsoft Exchange 間の適切な統合と通信を行うためには、偽装アカウントを使用する必要があります。このアカウントは、個々の予定表の会議情報を照会するために、ユーザに代わってカレンダー コネクタにより使用されます。カレンダー コネクタはユーザの電子メールや連絡先リストにアクセスするためにこのアカウントを使用しません。それで、Cisco Collaboration Cloud はコネクタから Exchange 環境の偽装アカウントの認証情報にアクセスしたりその情報を取得することはできません。さらに、Collaboration Cloud は企業の Exchange 環境に、直接的にもカレンダー コネクタを介してもアクセスできません。

カレンダー コネクタの導入には次の要件と推奨が適用されます。

- ハイブリッド サービスのユーザは Collaboration Cloud Common Identity Service（CIS）に対して認証されるため、Cisco Directory Connector および企業の Active Directory への統合が推奨されます。
- Cisco Spark Hybrid Services には、Cisco Expressway X8.7.1 以降のバージョンが必要です。
- カレンダー サービスの利用が許可されるユーザ数、個々のユーザの Exchange 予定表のサイズ、および @spark と @webex が使用されるレートにより、このサービスを有効にするときに Exchange サーバにかかる追加の負荷の量が決まります。Exchange の偽装アカウントにスロットリング ポリシーを作成して適用すると、企業の Exchange 環境へのカレンダー コネクタおよびカレンダー サービスの影響を低減できます。

導入の要件、インストール、設定を含め、カレンダー コネクタの詳細については、以下のリンク先から入手できる最新バージョンの『*Deployment Guide for Cisco Spark Hybrid Calendar Service*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html

カレンダー コネクタが実行され、ユーザが有効になると、有効になったユーザは Cisco Spark のコラボレーションを組み込み、WebEx ミーティング情報を Outlook 予定表の招待に追加できます。そのためには、次の手順を実行します。

- @spark

  @spark が Outlook 予定表の出席依頼の [ロケーション（location）] フィールドに追加されると、カレンダー コネクタとクラウドのカレンダー サービスは、その出席依頼の件名と一致する名前の付いた新しい Cisco Spark コラボレーション ルームを作成します。予定表の出席依頼にあるすべてのユーザは、この Cisco Spark のルームに追加されます。これによりコラボレーションが促進され、会議の主催者と出席者は会議前、会議中、そして会議後でも、やりとりを行ったり、資料を共有することができるようになります。予定表の出席依頼に配布リストが含まれている場合は、配布リストに掲載されたユーザは自動的に Cisco Spark ルームに追加されませんが、会議の招待は受け取ります。

- @webex：これを指定すると、WebEx ミーティング招待情報が Cisco Spark ルームに追加されます。

  @webex（複数の WebEx サイトを持つ組織の場合は @webex:<*サイト*>）を、Outlook 予定表の出席依頼の [ロケーション（location）] フィールドに追加すると、カレンダー コネクタにより、ユーザの WebEx コラボレーション会議室情報が招待に自動的に追加されます。WebEx ミーティング参加リンク（手動または WebEx の生産性向上ツールで追加されます）が、すでに予定表の招待に存在する場合、カレンダー コネクタは WebEx ミーティング情報を追加しません。

@webex を @spark と組み合わせて使用すると、WebEx ミーティング情報は予定表の会議の招待だけではなく、Cisco Spark ルームにも追加されます。

Cisco Spark コール サービス

Cisco Spark Hybrid Services により、Cisco Collaboration Cloud の通話サービスと企業のオンプレミス コール制御との統合が可能になりました。企業のコール サービスをクラウドに統合することにより、組織は既存のオンプレミス電話、コラボレーション クライアント、および Cisco Spark クライアント間でのデスクトップ共有と、音声通話、ビデオ通話を有効にできます。

図 21-16 に示すように、Cisco Spark のハイブリッド コール サービスには次の 3 つのエンタープライズ コンポーネントが必要です。

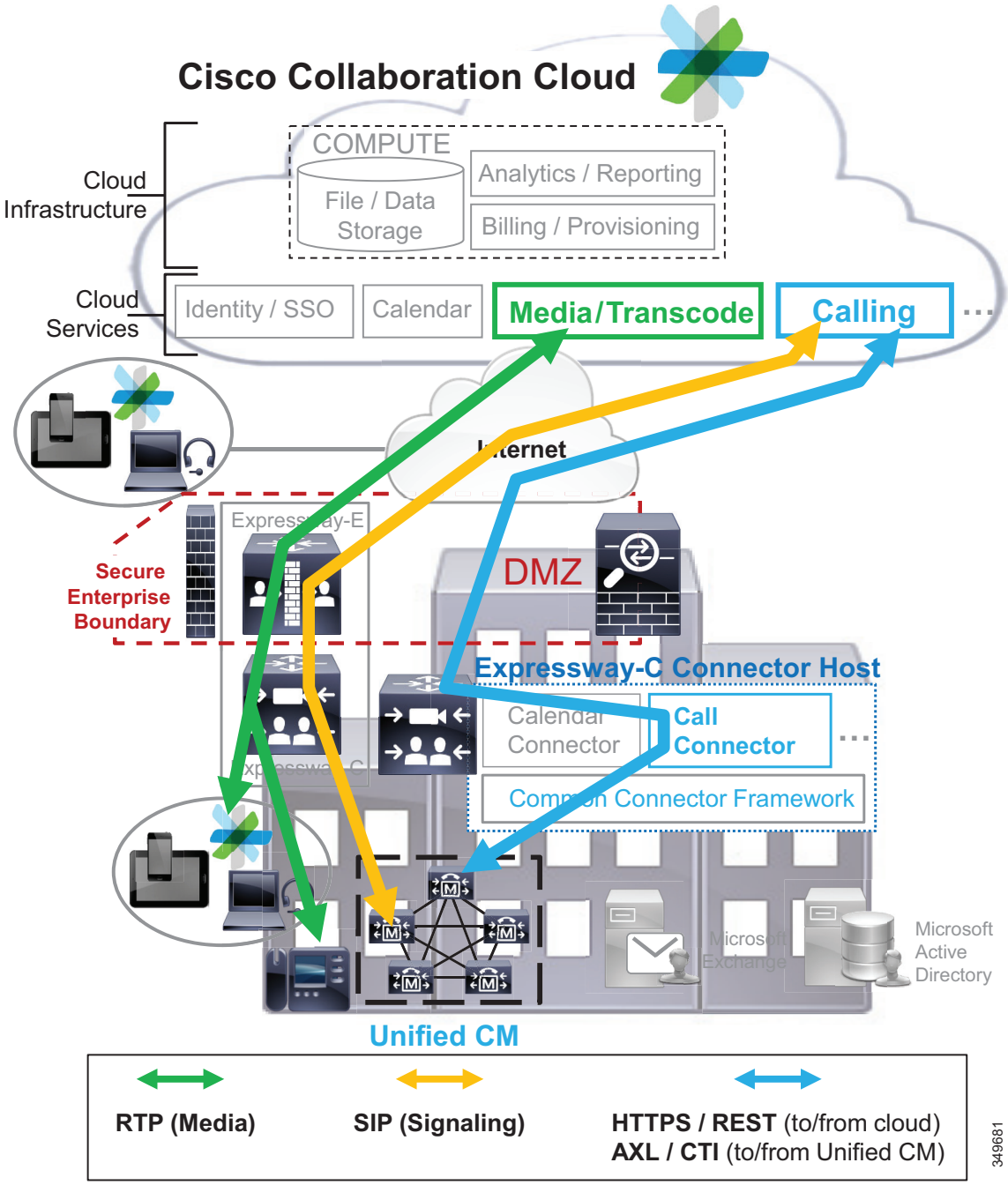
- Cisco Call Connector：このソフトウェアは Cisco Expressway-C コネクタ ホストで動作し、Cisco Collaboration Cloud の通話サービスと企業の Unified CM 展開との間の統合とコミュニケーションを調整します。
- Cisco Unified CM：これは企業のコール制御を担い、企業のエンドポイントとクライアント、および企業が接続しているクラウド クライアントの音声およびビデオ通話サービスと、PSTN 接続を提供します。企業のコール制御は、Cisco Business Edition 6000 または Cisco Hosted Collaboration System（HCS）で行うこともできます。
- Cisco Expressway-E と Expressway-C：このサーバ ペアはコール メディアおよびシグナリングにセキュアなエンタープライズ エッジ ファイアウォール トラバーサルを提供します。Expressway のモバイルおよびリモート アクセスや Business-to-Business（B2B）に使用される既存のサーバ ペアは、十分なコール キャパシティがあれば、利用できます。

Cisco Expressway-C コネクタ ホストにあるコール コネクタは、基本となる共通コネクタ フレームワークを使用して、エンタープライズ ネットワーク経由で Unified CM と通信します。他の企業のクラウド コネクタと同様に、コール コネクタはセキュアな企業の境界および企業のファイアウォールを通って、インターネットを介しクラウドと通信します。クラウドへのこの接続は企業内から開始され、企業のファイアウォールでポートを開く必要はありません。前述したように、これはインターネット上の Web サーバへのアウトバウンド接続を開始する HTTPS Web クライアントに似ています。

コール コネクタは REST ベースの HTTPS を使用して Cisco Collaboration Cloud の通話サービスと通信します。また、Administrative XML Layer（AXL）を使用して Unified CM と通信し、ユーザの企業デバイスの情報を取得するのに加えて、コンピュータ テレフォニー インテグレーション（CTI）を使用して、ユーザの企業回線をモニタします。

カレンダー コネクタと同様、Expressway-C コネクタ ホスト、コール コネクタ、Cisco Collaboration Cloud、およびクラウド通話サービスの間の接続は、Expressway-C でハイブリッド サービス コネクタを設定する際に自動的に確立されます。コール コネクタ ソフトウェアは、Expressway-C コネクタ ホストを正常に登録した後（すでに登録されている場合は、コール コネクタ サービスが Cisco Spark Control Hub と Expressway-C コネクタ ホストの両方から有効にされた時点で）、Cisco Collaboration Cloud から自動的にダウンロードされ、コネクタ ホストにインストールされます。

図 21-16　Cisco Spark Hybrid Services：企業の通話の統合



Cisco Spark Hybrid Services の通話は 2 つの機能を可能にします。

- コール サービス認識

  この機能は、Unified CM に登録済みのエンドポイントで、2 人の Cisco Spark が有効になっているユーザ間の通話に「ワンクリックで共有（one-click-to-share）」機能を提供します。2 人のユーザが企業の回線を使用して 1 対 1 で通話中に、クラウド通話サービスはハイブリッド サービスのコール コネクタから受信した情報に基づいてアクティブ コールを認識し、2 人のユーザ間の Cisco Spark ルームをリストの先頭に移動します（または、その 2 人の間に Cisco Spark ルールが作成されていなかった場合は、1 対 1 のルームを作成します）。そして、両方のユーザの Cisco Spark デスクトップ（または Web）クライアントのルーム内にあるデスクトップ共有ボタンを有効にします。どちらのユーザもこのボタンをクリックして、デスクトップを共有することができます。コール サービス認識を使用すると、Cisco Collaboration Cloud が Cisco Spark のコラボレーション ルームとデスクトップ共有を利用している間、1 対 1 通話のコール メディアとシグナリングは Unified CM と 2 つの企業デバイスでのみ処理されます。デスクトップの共有を可能にするだけでなく、コール サービス認識は統一されたコール履歴リストを Cisco Spark クライアントに提供します。

- コール サービス接続

  この機能により、Cisco Spark ユーザは企業のオンプレミス コール制御（Cisco Unified CM）を使用してコールを発信および受信できるようになります。この機能を設定すると、ユーザのエンタープライズ番号への着信コールは、Unified CM に登録されている電話機とクライアントだけでなく、Cisco Collaboration Cloud にも拡張されてユーザの Cisco Spark クライアントにルーティングされるため、ユーザは一番早く応答できるデバイス（企業の登録されたデスクフォンや、ユーザの携帯電話上で動作する Cisco Spark クライアントなど）を使用して、コールに応答することができます。同様に、Cisco Spark から発信された着信コールは、ユーザの Cisco Spark クライアントだけではなく、Cisco Collaboration Cloud によって企業の Unified CM にまで拡張され、Unified CM に登録されたユーザの各エンドポイントで呼び出し音が鳴ります。

  ユーザが Cisco Spark クライアントの通話タブ内で番号または URI を入力してコールを発信すると、そのコールは企業の Unified CM および必要に応じて企業の PSTN 接続を使用してルーティングされます。コール サービス接続は、コール サービス認識機能が同時に有効になっていないユーザに対しては、有効にすることはできません。

  コール サービス接続機能を有効にするには、各ユーザの Cisco Spark リモート デバイス（Spark RD）が Unified CM 内で設定されていなければなりません。このデバイスは、Cisco Collaboration Cloud のユーザを、リモート接続先として設定された企業 DN および Cisco Spark の通話 SIP URI と関連付けます。このデバイスの関連付けと、設定されたリモート接続先により、コールの発信元に応じてコールが Unified CM とコラボレーション クラウドの両方に分岐されます。Cisco Collaboration Cloud は SIP の連絡先ヘッダーとコール ルーティング ロジックを使用して、クラウドと企業コール制御間のコール分岐ループを防ぎます。

  （注）　Cisco Spark コール サービス接続の以前の導入では CTI リモート デバイスが使用されていましたが、現在の導入に適切な Unified CM デバイス タイプは Cisco Spark リモート デバイス（Spark RD）です。

  コール コネクタは Unified CM に Spark RD を登録します。この登録はコール コネクタが Cisco Collaboration Cloud に接続している限り、アクティブです。

コール サービス接続が有効になっていると、RTP コール メディアおよび SIP コール シグナリングは Expressway-E と Expressway-C サーバ ペアを使用して Cisco Collaboration Cloud との間でルーティングされます（図 21-16 を参照）。コール メディアは企業に接続されたエンドポイント（またはゲートウェイ）と Cisco Collaboration Cloud のメディアおよびトランスコーディング サービス間の Expressway-E および Expressway-C サーバを通過します。クラウド通話サービスと Unified CM 間の SIP シグナリングも、Expressway-E と Expressway-C サーバを通過します。コール サービス接続の RTP メディアと SIP シグナリングは既存のモバイルおよびリモート アクセス、または B2B Expressway-E と Expressway-C サーバを通過できます。または、専用のハイブリッド サービスの Expressway-E および Expressway-C サーバのセットを導入することもあります。

Cisco Spark のカレンダー サービスと全く同じように、Cisco Spark 通話サービスも Expressway-C コネクタ ホストと共通コネクタ フレームワーク間のセキュアな接続に依存します。そしてカレンダー コネクタ同様、コール コネクタを動作させるために、コネクタ管理とコール サービス用に Cisco Collaboration Cloud により提供された CA 署名付き証明書が、Expressway-C コネクタ ホストの証明書信頼リストと照合されます。Expressway-C コネクタ ホストは Call Connector ソフトウェアをダウンロードしてコネクタ サービスを開始する前に、クラウドの証明書を確認します。コール コネクタ サービスはクラウドの証明書 CA が信頼リストにない場合、開始されません。クラウドは最初の設定時に、必要なクラウドのパブリック CA 証明書を Expressway-C コネクタ ホストの信頼リストに自動的に追加します。または、クラウドの証明書を手動で管理することもできます。その場合は、管理者がクラウドの CA 証明書を Expressway-C コネクタ ホストの証明書信頼リストに追加する必要があります。

コール コネクタの導入には次の要件と推奨が適用されます。

- ハイブリッド サービスのユーザは Collaboration Cloud Common Identity Service（CIS）に対して認証されるため、Cisco Directory Connector および企業の Active Directory への統合が必要です。
- Cisco Spark Hybrid Services には、Cisco Expressway X8.7.1 以降のバージョンが必要です。
- コール サービス認識は、コール サービス接続機能の前提条件です。
- 高可用性を実現するためには、Cisco Spark コール サービスに必要な AXL Web サービスと CTIManager サービスが、少なくとも 2 つの Unified CM ノードで有効になっている必要があります。

導入の要件、インストール、設定を含め、コール コネクタの詳細については、以下のリンク先から入手できる最新バージョンの『*Deployment Guide for Cisco Spark Hybrid Call Services*』に記載されているコール サービス対応のセットアップに関する情報を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

クラウドおよびハイブリッド サービス モビリティのハイ アベイラビリティ

他の企業モビリティの機能とソリューション同様、クラウド サービスのハイ アベイラビリティを提供するためには、クラウドおよびハイブリッド サービスを冗長構成で設定および展開する必要があります。もともと、クラウドのインフラストラクチャとプラットフォームには復元力があります。ほとんどの管理型クラウド インフラストラクチャと同様、Cisco Collaboration Cloud と WebEx Cloud は、高度な RAID ストレージ アレイや電力網、持続的なデータのバックアップ、データ センター分散によるオンデマンド コンピューティング、および移行機能を使用して、可用性の高いクラウド サービスを確保しています。

ハイブリッド サービスを展開する場合、クラウドの復元力に加えて、オンプレミスのインフラストラクチャの冗長性も考慮する必要があります。エンタープライズ ネットワークやセキュアな企業の境界など、オンプレミスのエンタープライズ ネットワーク インフラストラクチャのコンポーネントを、可用性の高い形で配置することが重要です。WebEx Meeting Server、Expressway-C コネクタ ホスト、企業アプリケーション（Microsoft Exchange や Active Directory など）を含むコラボレーション コンポーネントは、冗長構成で配置する必要があります。

従来の Microsoft Exchange および Active Directory のハイ アベイラビリティ導入手法は、これらのアプリケーションが企業運用にとって重要であることを前提とすると、ほぼ間違いなく用意されています。用意されていない場合は、これらのアプリケーションの高可用性を実装することを検討してください。オンプレミスの Microsoft アプリケーションの高可用性は、ハイブリッド サービス統合にも適用されます。

クラウドおよびハイブリッド サービス モビリティのキャパシティ プランニング

クラウドおよびハイブリッド サービスの導入を成功させるには、クラウド サービスを使用するすべてのユーザに対して十分なキャパシティを用意することが必要です。クラウドのキャパシティはオンデマンドであり、クラウド コンピューティングとストレージの柔軟性を考えると事実上無限である一方で、権限付与のコストを検討する必要があります。

ハイブリッド統合に伴い、企業のオンプレミス インフラストラクチャを前提として、拡張性に関する新たな考慮事項が生じます。Microsoft アプリケーション（Exchange と Active Directory）の場合は、容量に関連する Microsoft のガイダンスに従い、既存のオンプレミス使用量を超えるハイブリッド サービスの追加オーバーヘッドに対して適切なキャパシティが提供されるようにします。特に、サーバ リソースのオーバーサブスクリプションを回避するために、Exchange サーバのスロットリング ポリシーを実装することが重要です。

Expressway-C ノード（大規模な OVA または大規模アプライアンス）は最大 5,000 人のクラウド ハイブリッド サービス ユーザをサポートします。

また、Directory Connector の場合、多数のユーザをコラボレーション クラウド CIS と同期しようとしている企業は、他のアプリケーションやサービスを企業に提供するために使用されてるのではない大容量の Windows サーバ（仮想マシンまたはハードウェア）に、Directory Connector を導入する必要があります。

いずれの状況でも、重要なオンプレミス コラボレーション インフラストラクチャのコンポーネント（Exchange、Active Directory、Directory Connector、Expressway-C、および WebEx Meeting Server）をモニタすることが重要です。また、サーバや仮想マシンの故障時や、CPU やメモリ使用量が定期的にクリティカル レベルになる際には、より多くのリソースを追加し、負荷を分散することを検討してください。

クラウドおよびハイブリッド サービス モビリティの設計に関する考慮事項

クラウド サービスとハイブリッド サービスを実現し、導入する際には、次の設計要件と推奨事項を考慮してください。

- Cisco Directory Connector ソフトウェアは、企業の Active Directory ドメインのメンバーである Microsoft Windows サーバに、ドメインの管理者権限のあるアカウントを使用してインストールする必要があります。
- Cisco Directory Connector は Active Directory Domain Service（AD DS）または Active Directory Lightweight Directory Services（AD LDS）が有効な Windows サーバにインストールしてはなりません。
- Cisco Spark Hybrid Services の認証には、Cisco Directory Connector と企業の Active Directory を統合することをお勧めします。
- Cisco Spark Hybrid Services には、Cisco Expressway X8.7.1 以降のバージョンが必要です。
- カレンダー サービスが有効なユーザ数、個々のユーザの Exchange 予定表のサイズ、および @spark と @webex が使用されるレートにより、Cisco Spark カレンダー サービスを有効にするときに Exchange サーバにかかる追加の負荷の量が決まります。Exchange の偽装アカウントにスロットリング ポリシーを作成して適用すると、企業の Exchange 環境へのカレンダー コネクタおよびカレンダー サービスの影響を低減できます。
- ユーザに対してコール サービス接続機能を有効にするには、コール サービス認識を有効にする必要があります。
- Cisco Spark コール サービスには Unified CM AXL Web サービスと CTIManager サービスが必要であり、これらのサービスの高可用性を実現するためには、少なくとも 2 つの Unified CM ノードで有効になっている必要があります。

Cisco Collaboration Cloud および Cisco Spark Hybrid Services の詳細については、https://collaborationhelp.cisco.com/article/en-us/nkg4mud に掲載されている Cisco Spark の情報を参照してください。

Cisco Spark Hybrid Services のデプロイに関する詳細は、https://www.cisco.com/go/pa から入手できる最新バージョンの『*Preferred Architecture for Cisco Spark Hybrid Services, CVD*』を参照してください。

社外型モビリティ

Cisco のモバイル コラボレーション ソリューションを使用すると、モバイル ユーザは、デスクフォンだけでなく、1 台以上のリモート電話機でも会社の電話番号へのコールを処理できます。また、モビリティ ユーザは、まるで社内から電話をかけているかのようにリモート電話機から電話をかけることもできます。さらに、モビリティ ユーザは、保留、転送、会議などのエンタープライズ機能だけでなく、携帯電話上でのボイスメール、会議、プレゼンスなどのエンタープライズ アプリケーションも利用できます。これによって、ユーザは外出先でも生産性を持続させることができます。

さらに、モバイル音声ネットワークやモバイル データ ネットワークおよび 802.11 WLAN への接続を提供するデュアルモード電話を使用すると、ユーザは社外で企業アプリケーションを利用できるだけでなく、社内にいるとき、またはエンタープライズ ネットワークにリモート接続されているときにエンタープライズ テレフォニー インフラストラクチャを利用して、モバイル音声ネットワークの分単位の料金を支払わずにコールの発信と受信を行うことができます。

Cisco Unified Mobility ソリューション内に配布される Fixed Mobile Convergence（FMC）モビリティ機能は、Cisco Unified CM によって提供され、Cisco Jabber などの Cisco Mobile クライアントと併用できます。

Cisco Unified Mobility では、次のモビリティ アプリケーション機能が提供されます。

- シングル ナンバー リーチ（SNR）

  シングル ナンバー リーチを使用すれば、1 つの会社の電話番号でユーザの IP デスクフォンと携帯電話の両方を同時に呼び出すことができます。SNR ユーザは、着信コールをデスクフォンでも携帯電話でも受けることができ、通話中のコールを妨げることなく別の電話に転送できます。

- 通話切替機能

  通話切替機能により、モビリティ コールの通話中に、携帯電話の保留、保留解除、転送、会議、およびリダイレクト コール パーク機能を呼び出すことができます。これらの機能は、携帯電話のキーによって呼び出され、保留音やカンファレンス ブリッジといった企業のメディア リソースを活用します。

- シングル企業ボイスメール ボックス

  シングル企業ボイスメール ボックスは、モバイル ボイスメール回避機能を提供し、ユーザの会社の電話番号に着信し、さらに携帯電話に転送されたコールに応答がなかった場合に、携帯電話のボイスメール システムではなく、会社のボイスメール システムにコールを蓄積します。これにより、ボイスメール ボックスが 1 箇所に統合され、ユーザは複数のボイスメール システムでメッセージを確認する必要がなくなります。

- モバイル音声アクセスとエンタープライズ機能アクセスの 2 段階ダイヤリング

  モバイル音声アクセスとエンタープライズ機能アクセスの 2 段階ダイヤリングによって、まるで会社の IP デスクフォンからかけているかのように、携帯電話から発信できます。長距離電話や国際電話、または通常は企業外部から到達不能なシステム上の内部の DID 以外の内線番号へのコールにおいてこれらの機能を使用すると、通話料金を節約できます。また、企業でこれらの 2 ステージ ダイヤリング機能を使用すると、中央で一括管理されたコール詳細レコードによって、ユーザのコール発信を容易に追跡管理できるようになります。さらに、これらの機能によって、発信者 ID を送信する際にユーザの携帯電話番号を隠すことができます。代わりに、発信者 ID として、ユーザの会社の電話番号が送信されます。これによって、ユーザへの返信コールは会社の電話番号にかけられるため、コールを会社で一括管理できます。

Cisco Mobile クライアントおよびデバイスは、音声とデータ接続用のモバイル プロバイダー ネットワークおよび 802.11 のワイヤレス ネットワークの両方に接続できる機能を提供します。これは、ユーザが 1 つのデバイスから両方のエンタープライズ コール制御、場合によってはモバイル ネットワークのコール制御を利用できるようにします。可能であれば、コールを送受信するための企業のテレフォニー インフラストラクチャを利用することによって、また、デュアル モード電話機の場合は企業接続が利用できないときだけにモバイル音声ネットワークに戻ることによって、モバイル クライアントおよびデバイスは、テレフォニーのコストの削減を支援できます。また、デュアルモード電話、およびそこで実行されるクライアントには、ハンドオフ メカニズムが備えられているため、ユーザが社外に移動した場合に、通話中のボイスコールにおいて、WLAN インターフェイスとモバイル音声インターフェイスを簡単に切り替えることができます。

Cisco Mobile クライアントでは、モバイル デバイスを有効にして、802.11 WLAN の IP 経由またはモバイル データ ネットワーク経由で音声またはビデオ コールを発信できるようにすることに加え、Dial via Office 機能を使用した企業の自動化ダイヤリングも有効にしました。Dial via Office コールは、IP ネットワーク経由の SIP シグナリングを使用して設定され、一方メディア パスは、モバイル音声ネットワークおよび PSTN 経由で設定されます。シスコのモバイル クライアントとデバイスは、社内ディレクトリ アクセス、プレゼンスおよびインスタント メッセージング（IM）などの他の Unified Communications サービスも提供します。これらのデバイスとクライアントでは、モバイル ユーザは、コラボレーション アプリケーションへのアクセスを提供することによって社内、社外にかかわらず生産性を維持できると同時に、ユーザは、パブリックまたはプライベートの WiFi モバイル ホット スポットやモバイル データ ネットワーク、社内で WLAN 経由にかかわらず、モバイル デバイスからエンタープライズ コールを送受信できます。

この項では、まず、Unified Mobility の特徴、機能、および設計と配置に関する考慮事項について説明します。Unified Mobility のさまざまなメリットおよびモバイル クライアントとデバイスを統合することによってその機能が利用できるという事実を前提として、Cisco Jabber などのモバイル クライアント アプリケーションを検証します。この項には、次のモビリティ アプリケーションおよび機能のアーキテクチャ、機能性、および設計と配置の意味に関する説明も含まれます。

- Cisco Unified Mobility（21-51 ページ）
- シスコのモバイル クライアントおよびデバイス（21-81 ページ）

Cisco Unified Mobility

Cisco Unified Mobility は、Cisco Unified CM に組み込まれたネイティブなモビリティ機能を意味し、シングル ナンバー リーチ、モバイル音声アクセス、およびエンタープライズ機能アクセスの各機能が含まれます。

Unified Mobility の機能は、Unified CM の設定によって異なります。したがって、この設定だけでなく、論理コンポーネントの特性も理解することが重要です。

図 21-17 に、Unified Mobility に関する設定要件を示します。まず、ユーザに関しては、モビリティ ユーザの会社の電話機は、電話番号、パーティション、通話サーチ スペースなどの該当する回線レベル設定値を使用して設定されます。この他に、会社の電話機のデバイス レベルの設定には、デバイス プール、共通デバイス設定、コーリング サーチ スペース、メディア リソース グループ リスト、ユーザとネットワークの保留音源などのパラメータが含まれます。ユーザの会社の電話機に関するこれらの回線およびデバイス設定のすべてが、着信コールと発信コールのコール ルーティングや保留音（MoH）の動作に影響を与えます。

次に、Unified Mobility 機能が利用できるように、モビリティ ユーザごとのリモート接続先プロファイルを設定する必要があります。リモート接続先プロファイルは、ユーザの会社の電話回線と同じ電話番号、パーティション、および通話サーチ スペースを使用して回線レベルで設定します。これによって、リモート接続先プロファイルと会社の電話機の間で回線が共有されます。リモート接続先プロファイル設定には、デバイス プール、コーリング サーチ スペース、コーリング サーチ スペースの再ルーティング、およびユーザとネットワークの保留音源に関するパラメータが含まれます。リモート接続先プロファイルは、その設定にユーザの回線レベルの会社の電話機の設定が反映されますが、回線レベルの設定とプロファイル レベルの設定を組み合わせることによって、ユーザのリモート接続先電話機に継承されるコール ルーティングおよび MoH 動作が決定される仮想電話機と見なす必要があります。リモート接続先プロファイルと会社の電話機の間で共有されるユーザの会社の電話番号を使用すれば、その番号に電話することによってユーザのリモート接続先に転送できます。

図 21-17　Cisco Unified Mobility の設定アーキテクチャ

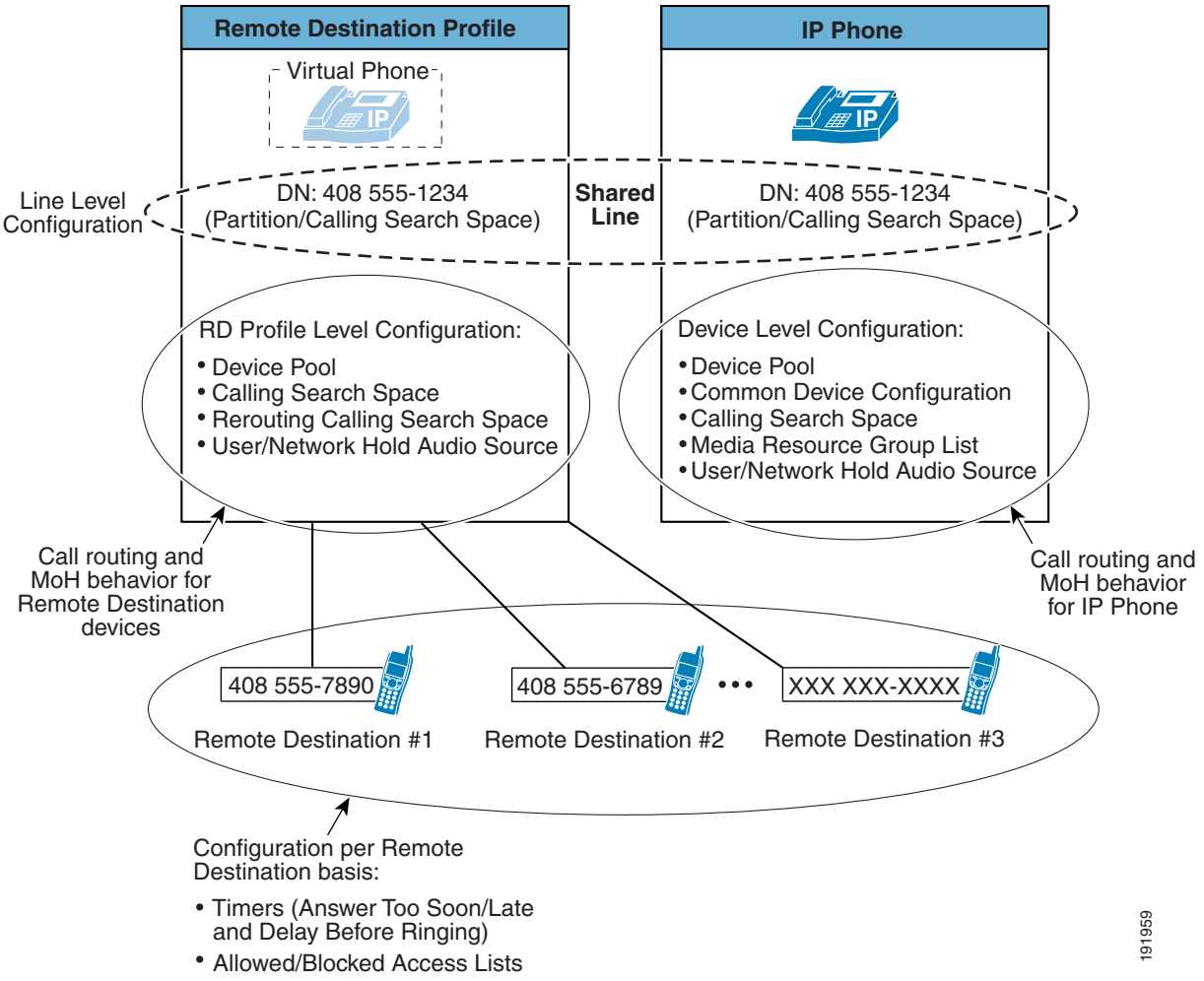


図 21-17 に示すように、モビリティ ユーザは、1 つまたは複数のリモート接続先をリモート接続先プロファイルに関連付けることができます。リモート接続先は、ユーザを呼び出すための単一の PSTN 電話番号を表しています。ユーザは、最大で 10 個のリモート接続先を定義できます。リモート接続先ごとにコール ルーティング タイマーを設定して、コールを特定のリモート電話に転送する時間だけでなく、コールを転送する前に待機する時間とリモート電話でコールを受ける準備ができるまでの時間を調整できます。また、モビリティ ユーザは、リモート接続先ごとに、リモート電話に転送する特定の電話番号からのコールを許可または拒否するフィルタを設定できます。

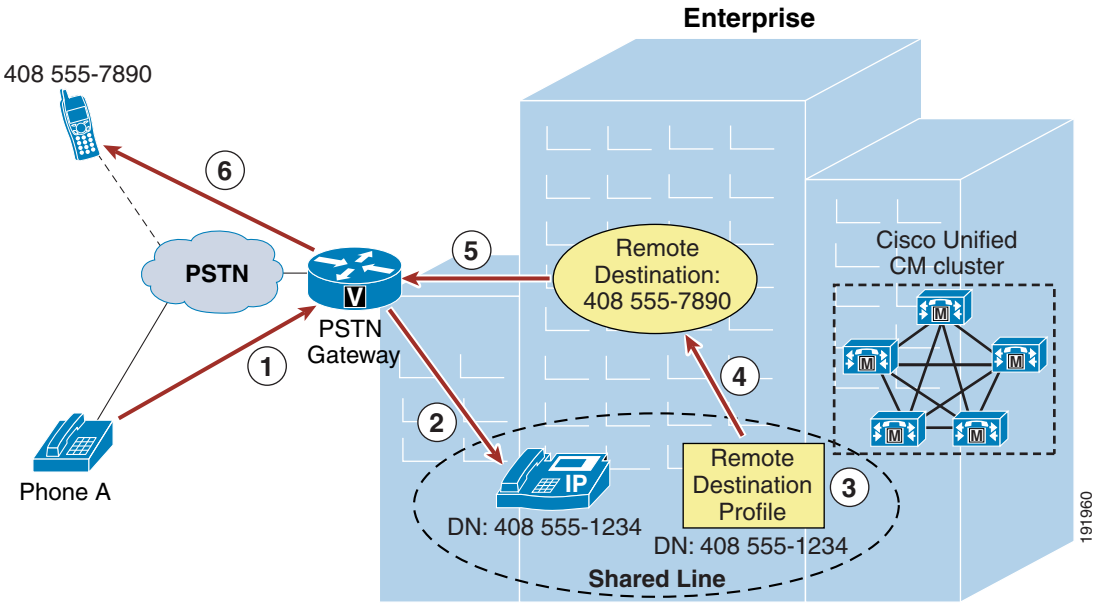
シングル ナンバー リーチ

シングル ナンバー リーチ（SNR）機能を使用すれば、企業ユーザへの着信コールをそのユーザの IP デスク フォンのほかに、最大 10 個の設定可能なリモート接続先に転送できます。一般的に、ユーザのリモート接続先は携帯電話です。コールがデスクトップフォンとリモート接続先電話機の両方に転送されれば、ユーザはどちらかの電話機で応答できます。ユーザは、リモート接続先電話機のいずれかまたは IP デスクトップフォンでコールに応答したときに、そのコールを別の電話機でハンドオフするか、ピックアップするかを選択できます。

シングル ナンバー リーチ機能

図 21-18 に、シングル ナンバー リーチの基本的なコール フローを示します。この例では、PSTN 上の電話機 A から SNR ユーザの会社の電話番号（DN）408-555-1234 に電話をかけます（ステップ 1）。コールが会社の PSTN ゲートウェイから Unified CM を経由して DN 408-555-1234 の IP フォンに転送され（ステップ 2）、この電話が鳴り出します。コールは、同じ DN を共有するユーザのリモート接続先プロファイルにも転送されます（ステップ 3）。次に、コールがユーザのリモート接続先プロファイルに関連付けられたリモート接続先（この場合は 408-555-7890）に発信されます（ステップ 4）。リモート接続先への発信コールが PSTN ゲートウェイを介してルーティングされます（ステップ 5）。最後に、番号が 408 555-7890 のリモート接続先 PSTN 電話機で呼出音が鳴ります（ステップ 6）。どちらの電話機でも応答できます。

図 21-18　　シングル ナンバー リーチ



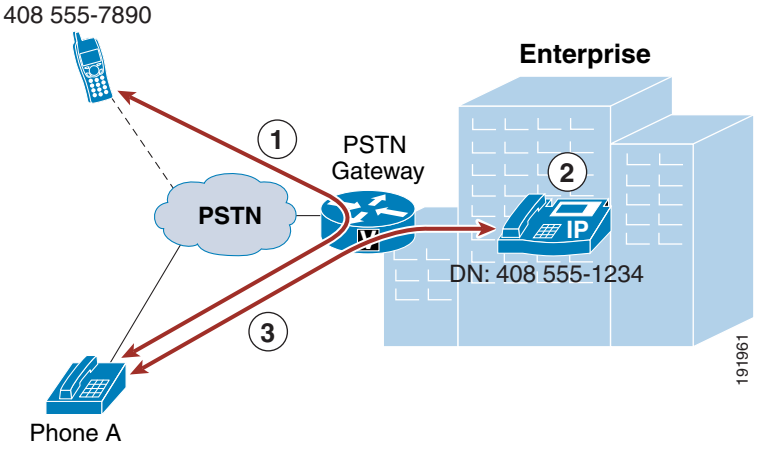
通常、シングル ナンバー リーチ ユーザの設定済みリモート接続先は、モバイル ボイス ネットワークまたはセルラー プロバイダー ネットワーク上の携帯電話です。ただし、PSTN により到達可能な任意の接続先をユーザのリモート接続先として設定できます。さらに、SNR ユーザは 10 件までリモート接続先を設定できるため、着信コールは最大で 10 台の PSTN 電話機とユーザのデスク フォンを呼び出すことができます。デスクトップフォンまたはリモート接続先電話機のいずれかでコールに応答すると、他のリモート接続先またはデスクトップフォン（デスクトップフォンで応答しなかった場合）に転送されたすべてのコール レッグがクリアされます。リモート接続先で着信コールに応答した場合は、2 つのゲートウェイ ポートを使用している会社の PSTN ゲートウェイ内で音声メディア パスがヘアピンされます。SNR 機能を配置する場合はこの利用を考慮する必要があります。

（注）　図 21-18 に示すようにシングル ナンバー リーチを動作させるには、[エンドユーザ（End User）] 設定ページでユーザ レベルの [モビリティの有効化（Enable Mobility）] チェックボックスがオンになっており、少なくとも 1 つのユーザの設定済みリモート接続先で [シングルナンバーリーチを有効にする（Enable Single Number Reach）] チェックボックスがオンになっていることを確認します。

デスク フォンのピックアップ

図 21-19 に示すように、ユーザがリモート接続先デバイスでシングル ナンバー リーチに応答した場合（ステップ 1：この場合は 408 555-7890）は、ユーザはデスク フォンの [再開（Resume）] ソフトキーを押すだけで、いつでもリモート接続先でコールをいったん切ってから、デスク フォンでピックアップできます（ステップ 2：この場合は DN 408 555-1234）。電話機 A を使用している元の発信者とデスクトップフォンとの間でコールが再開されます（ステップ 3）。

図 21-19　デスクトップフォンのピックアップ



デスクトップフォンのピックアップは、設定済みのリモート接続先電話機で会社の固定コールの通話が行われた後、その電話が切られた場合にいつでも実行できます。

（注）　会社の固定コールとは、会社の PSTN ゲートウェイ経由で接続された少なくとも 1 つのコール レッグがあり、リモート接続先から会社の DID に発信された、あるいはシングル ナンバー リーチ、モバイル ボイス アクセス、エンタープライズ機能アクセス、または Intelligent Session Control によって発信されたすべてのコールを指します。

デスクトップフォンでコールをピックアップまたは保留解除するためのオプションは、一定時間しか使用できません。そのため、シングル ナンバー リーチ ユーザは、必ず、着信電話機が切れていることを確認してから、リモート接続先電話機を切るようにしてください。これによって、他の誰かがデスクトップフォンでコールを保留解除できないことが保証されます。デフォルトで、リモート接続先電話機が切られてから 10 秒間はコールをデスクトップフォンでピックアップできます。ただし、この時間は設定可能であり、[End User] 設定ページで Maximum Wait Time for Desk Pickup パラメータを変更することによって、ユーザごとに 0 ～ 30,000 ミリ秒に設定できます。デスクトップフォンのピックアップは、リモート接続先電話機で通話切替保留機能を呼び出した後でも実行できます。ただし、このような場合は、Maximum Wait Time for Desk Pickup パラメータの設定が、ピックアップに使用できる時間に影響しません。通話切替保留されたコールは、リモート電話機とデスクトップフォンのどちらかで手動で保留解除されるまで、保留のままで、デスクトップフォンでピックアップできます。

デスクトップフォンのピックアップを実行するもう 1 つの方法に、通話切替セッション ハンドオフ機能を使用する方法があります。この通話切替機能は、セッション ハンドオフのデフォルトのエンタープライズ機能アクセス コードである *74 を手動で入力することによって呼び出します。これにより、Unified CM への DTMF シーケンスが生成されます。この機能が呼び出されると、Unified CM からユーザの会社のデスクトップフォンに新しいコールが送信されます。ユーザは、セッション ハンドオフを完了させるために、この新しいコールがデスクトップフォンの点滅表示または呼出音によって通知されたらこのコールに応答する必要があります。

デスクトップフォンのピックアップを行う場合にこの方法を使用すると、他の方法（携帯電話でコールを切断する方法や通話切替保留機能を使用する方法など）と比較して、ユーザと遠端の電話機との間の会話がハンドオフ プロセス中にも維持されるという利点があります。*74 シーケンスを入力すると、ハンドオフ コールがユーザのデスクトップフォンに送信されるため、ユーザは会話を継続できます。ユーザがデスクトップフォンでコールに応答すると、コール レッグが切り替えられて、遠端へのコール レッグが、デスクトップフォンに作成された新しいコール レッグに接続されます。これにより、音声パスが切断されずに、またはほぼ瞬間的にカットスルーされます。モバイル デバイスの元のコール レッグは、後でクリアされます。

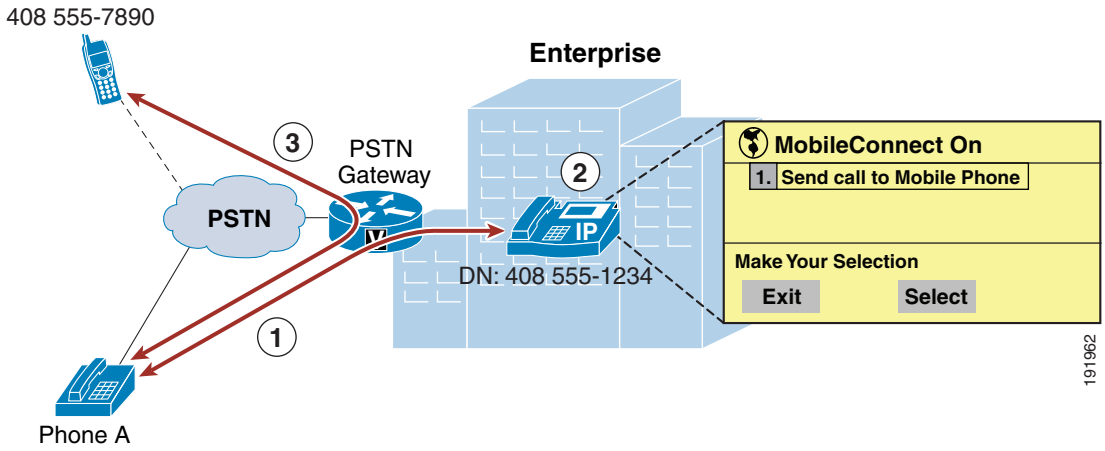
コールを切断してデスク フォンのピックアップを呼び出す方法では、エンド ユーザの [デスクフォンピックアップの最大待機時間（Maximum Wait Time for Desk Pickup）] の設定によってデスク フォンでコールをピックアップできる時間が決定されます。一方、セッション ハンドオフでは、[セッションハンドオフアラートタイマー（Session Handoff Alerting Timer）] サービス パラメータによって、デスク フォンでどの程度の時間呼出音または点滅表示によってコールが通知された後にハンドオフ コールがクリアされるかが決定されます。デフォルトのハンドオフ アラート時間は 10 秒です。また、セッション ハンドオフでは、デスクトップフォンに設定されたどの自動転送設定も関与しません。その結果、ハンドオフ機能では、ボイスメールやその他の自動転送宛先への転送は行われません。Session Handoff Alerting Timer 期間を経過してもコールに応答しないと、コールはクリアされて、ユーザのデスクフォン回線から Remote In Use 状態が削除されます。ただし、このシナリオでは、携帯電話の元のコールは維持されます。

セッション ハンドオフおよびその他の通話切替機能の詳細については、通話切替機能（21-56 ページ）を参照してください。

リモート接続先電話のピックアップ

図 21-20 に、シングル ナンバー リーチのリモート接続先電話のピックアップ機能を示します。電話機 A から SNR ユーザの会社の DN 408 555-1234 にコールを発信し、そのユーザがデスク フォンで応答してコールが通話中になっている場合（ステップ 1）は、ユーザは [モビリティ（Mobility）] ソフトキーを押す必要があります。この電話機で SNR 機能が有効になっており、リモート接続先ピックアップが使用できる場合、ユーザは [選択（Select）] ソフトキーを押します（ステップ 2）。ユーザのリモート接続先電話機に対するコール（この場合は 408 555-7890）が実行され、リモート電話機が鳴り出します。リモート電話機でコールが応答されると、電話機 A と、番号が 408 555-7890 の SNR ユーザのリモート電話機との間でコールが再開されます（ステップ 3）。

図 21-20　　リモート接続先電話のピックアップ



シングル ナンバー リーチ ユーザに対して複数のリモート接続先が設定されている場合は、[選択(Select)] ソフトキーを押したときに各リモート接続先が呼び出され、ユーザは好きな電話機をピックアップできます。

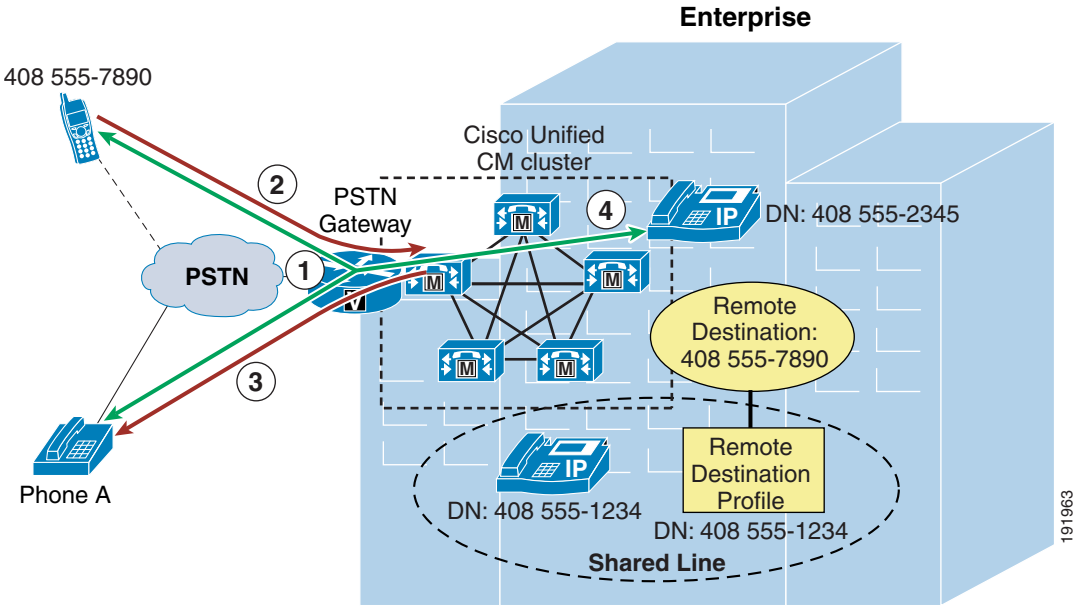
(注)　図 21-20 に示すように、リモート接続先電話機のピックアップを動作させるには、1 つ以上のユーザの設定済みリモート接続先で [Mobile Phone] チェックボックスがオンになっていることを確認してください。加えて、[Mobility] ソフトキーをすべてのモビリティ ユーザの関連するデスクトップフォン ソフトキー テンプレートに追加する必要があります。[Mobile Phone] チェックボックスをオンにして、Mobility ユーザが [Mobility] ソフトキーを使用できるようにしなければ、リモート接続先電話機のピックアップ機能が使用できません。

(注)　Cisco TelePresence System の C、EX、MX、SX、TX の各シリーズのビデオ エンドポイントは、上述のリモート接続先のピックアップをサポートしていません。これらのエンドポイントでは、モビリティ ソフトキーまたは [Send call to Mobile Phone] オプションはユーザから見えないようになっています。したがって、これらのエンドポイントは、リモート接続先のピック アップを使用してモバイル デバイスに進行中のコールを送信できません。

通話切替機能

図 21-21 に示すように、ユーザがリモート接続先デバイスでシングル ナンバー リーチ コールに応答(ステップ 1:この場合は 408 555-7890)したら、会社の PSTN ゲートウェイ経由でリモート接続先電話機から Unified CM に DTMF 番号を送信することによって、保留、保留解除、転送、会議、ダイレクト コール パーク、セッション ハンドオフなどの通話切替機能を呼び出すことができます(ステップ 2)。通話切替機能の保留、転送、会議、またはダイレクト コール パークが呼び出されると、Unified CM から電話の相手に MoH が送信されます(ステップ 3:この場合は電話機 A)。通話中のコールを別の電話機やダイレクト コール パーク番号に転送したり、会社の会議リソースを使用して新しい電話機で会議に参加できます(ステップ 4)。

図 21-21　　モビリティ通話切替機能



Unified CM に転送された一連の DTMF 番号によって、リモート接続先電話機で通話切替機能が呼び出されます。Unified CM で受信されるこれらの番号シーケンスが、設定済みの保留、独占保留、保留解除、転送、会議、およびセッション ハンドオフ用のエンタープライズ機能アクセス コードと照合され、該当する機能が実行されます。

(注)　ダイレクト コール パークの通話切替機能を有効にするには、ダイレクト コール パーク番号とコール パーク取得プレフィックスを使用して Cisco Unified CM を設定する必要があります。

(注)　転送、会議、およびダイレクト コール パークの通話切替機能を実行するために、コールに応答して、ユーザ入力（PIN 番号、通話切替機能アクセス コード、およびターゲット番号を含む）を取得し、必要なコール レッグを作成して転送、会議、またはダイレクト コール パークの処理を完了させる、システム設定のエンタープライズ機能アクセス DID への別のコール レッグがリモート接続先電話機で生成されます。

通話切替セッション ハンドオフ機能では、遠端は保留にならないため、MoH は遠端に転送されません。モバイル ユーザがデスクトップフォンでハンドオフ コールに応答するまでの間、元の音声パスが維持されます。ユーザがコールに応答すると、コール レッグが会社のゲートウェイで切り替えられ、音声パスが引き続き維持されます。

通話切替機能は、手動で機能アクセス コードを入力し、適切なキー シーケンスを入力することによって呼び出されます。表 21-2 に、通話切替機能を呼び出すためのキー シーケンスを示します。

表 21-2　手動通話切替機能のキー シーケンス

通話切替機能	エンタープライズ機能アクセス コード（デフォルト）	手動キー シーケンス
保留	*81	入力：*81
独占保留	*82	入力：*82
復帰	*83	入力：*83
転送	*84	1. 入力：*82（独占保留） 2. エンタープライズ機能アクセス DID への新しいコールの発信 3. 接続時の入力： <*PIN_number*> # *84 # <*Transfer_Target/DN*> # 4. 転送ターゲットでの応答時（打診転送の場合）またはリングバック時（初期在席転送の場合）の入力：*84
ダイレクト コール パーク	該当なし	1. 入力：*82（独占保留） 2. エンタープライズ機能アクセス DID への新しいコールの発信 3. 接続時の入力： <*PIN_number*> # *84 # <*Directed_Call_Park_Number*> # *84 # （注）　パークされたコールを取得するには、モバイル ボイス アクセスまたはエンタープライズ機能アクセス 2 ステージ ダイヤリングを使用してコールをダイレクト コール パーク番号に発信する必要があります。ダイヤルするダイレクト コール パーク番号が入力する際、適切なコール パーク取得プレフィックスを付加する必要があります。
会議	*85	1. 入力：*82（独占保留） 2. エンタープライズ機能アクセス DID への新しいコールの発信 3. 接続時の入力： <*PIN_number*> # *85 # <*Conference_Target/DN*> # 4. 会議ターゲットによる応答時の入力：*85
セッション ハンドオフ	*74	1. 入力：*74 2. デスクトップフォンに呼出音または点滅表示で通知されたら応答

(注)　保留や会議などの通話切替機能のためのメディア リソース割り当ては、リモート接続先プロファイル設定、またはデュアルモード電話機および Unified Mobile Communicator の場合にはデバイス設定で決定されます。リモート接続先プロファイルまたはモバイル クライアント デバイスに設定されたデバイス プールのメディア リソース グループ リスト（MRGL）が、会議通話切替機能のための会議ブリッジの割り当てに使用されます。リモート接続先プロファイルまたはモバイル クライアント デバイスのユーザ保留オーディオ ソースとネットワーク保留 MoH オーディオ ソースの設定、およびデバイス プールのメディア リソース グループ リスト（MRGL）が、保留デバイスに送信する MoH ストリームの決定に使用されます。

シングル企業ボイスメール ボックスによるモバイル ボイスメール回避

Cisco Unified Mobility シングル ナンバー リーチに関する追加の考慮事項は、モバイル ボイスメール回避です。シングル企業ボイスメール ボックス機能では、応答がないすべての企業ビジネス コールは最終的に企業ボイスメール システムに転送されます。これによって、ユーザは、応答がない会社の電話番号へのコール用に用意された複数のメールボックス（会社、携帯電話、自宅など）をチェックする必要がなくなります。この機能は、モバイルまたは非企業のボイス メールを避けるために、2 種類の方式を提供します。

- タイマー制御方式: この方法によってシステムは、自動転送タイマーと組み合わせた 1 組のタイマー（リモート接続先ごとに 1 つ）に依存し、無応答時にコールがボイスメール システムに転送されると企業ボイスメール システムがコールを受信するようになります。
- ユーザ制御方式: この方法によってシステムは、コールが応答されてコールがユーザまたは非企業ボイス メールに受信されたかを判断する場合はリモート接続先からの DTMF トーンの確認に依存します。

システム設定は、タイマー制御方式またはユーザ制御方式が使用されているかどうかを判断します。使用される方式は、Voicemail Selection Policy サービス パラメータによってグローバルに設定でき、また、Single Number Reach Voicemail Policy によって個々のリモート接続先ごとに設定できます。デフォルトでは、システムおよびすべてのリモート宛先はタイマー制御メソッド方式を使用します

タイマー コントロールのモバイル ボイスメールの回避

この方式では、システムは [Remote Destination] 設定ページのタイマーのセットに依存します。これらのタイマーの目的は、コールが無応答呼び出しでボイスメール システムに転送されたときに、そのコールがリモート接続先のボイスメール システムではなく、会社のボイスメール システムに転送されることを保証することです。これらのタイマーは、他のシステム無応答転送タイマーとともに、次のように非企業ボイスメール システムを回避するように設定する必要があります。

- デスクフォンの無応答転送時間をリモート接続先電話機よりも短くします。

  これを実現するために、Unified CM のグローバルな無応答転送タイマー フィールドまたは個々の電話回線の無応答呼び出し期間フィールドを、リモート接続先電話機のモバイル ボイスメール システムに転送されるまでの呼び出し期間より短い値に設定します。加えて、[Remote Destination] 設定ページの [Delay Before Ringing Timer] パラメータを使用して、リモート接続先電話機の呼び出しを遅らせることによって、リモート接続先電話機からそのモバイル ボイスメール ボックスに転送されるまでの時間を延ばすことができます。ただし、[Delay Before Ringing Timer] パラメータを調整する場合は、グローバルな Unified CM 無応答転送タイマー（または回線レベルの無応答呼び出し期間フィールド）が、モビリティ ユーザが余裕を持ってリモート接続先電話機の呼び出しに応答できる値に設定されていることを確認する必要があります。[呼び出し前の遅延タイマー（Delay Before Ringing Timer）] パラメータは、リモート接続先ごとに設定することが可能で、デフォルト値は 4,000 ミリ秒です。

- 着信コールがモバイル ボイスメール システムに転送されるまでリモート接続先デバイスで呼び出しを停止します。

  これを実現するには、各リモート接続先に Answer Too Soon Timer および Answer Too Late Timer を使用します。まず、[Remote Destination] 設定ページの [Answer Too Soon Timer] パラメータに、電源オフまたは圏外の携帯電話へのコールがモバイル ボイスメール システムに転送されるまでにかかる時間より長い値を設定する必要があります。デフォルトでは、このタイマーは 1,500 ミリ秒（つまり 1.5 秒）に設定されます。Answer Too Soon Timer が切れる前にコールが応答された場合、リモート接続先へのコール レッグが切断されます。これにより、モバイル ボイスメール システムにすぐに転送されたコールは接続されませんが、呼び出し後にユーザが応答したコールは接続されます。

  次に、[Remote Destination] 設定ページの [Answer Too Late Timer] パラメータを、リモート接続先電話機が呼び出されてからボイスメール ボックスに転送されるまでの時間より短い値に設定します。デフォルトでは、このタイマーは 19,00 ミリ秒（つまり 19 秒）に設定されます。このタイマーが切れる前にコールに応答がなかった場合、リモート接続先へのコール レッグが切断されます。これにより、コールがモバイル ボイスメール システムに転送されるまでリモート接続先電話機で呼び出しが停止されます。

（注） モビリティ ユーザが、[呼び出し開始タイマー（Answer Too Soon Timer）] が切れてから、手動でリモート接続先に宛先変更した着信コールは、最終的にモバイル ボイスメール ボックスに転送される可能性があります。この発生を回避するには、モビリティ ユーザがユーザ制御方式を設定するか、またはボイス メールに宛先変更する着信コールの呼出音を無視または停止するように指示される必要があります。これによって、無応答コールは必ず、企業ボイスメール ボックスに転送されることが保証されます。

（注） ほとんどの配置シナリオでは、[Delay Before Ringing Timer]、[Answer Too Late Timer]、および [Answer Too Soon Timer] のデフォルト値で十分であり、変更する必要はありません。

ユーザ制御のモバイル ボイスメールの回避

この方式では、システムは、コールが応答されたときのリモート宛先からの DTMF 確認トーンにコールに依存します。DTMF トーンがシステムによって受信された場合、システムはユーザがコールに応答し、DTMF トーンを生成するキーを押したことを認識します。一方、DTMF トーンがシステムで受信されない場合、システムは、コール レッグが非企業ボイス メール システムで応答されてコール レッグが切断されると見なします。

ユーザ制御方式が有効な場合、エンド ユーザの応答時に、DTMF トーンを生成するキー パッド ボタンを押すように求める音声プロンプトが再生されます。デフォルトでは、音声プロンプトは、ユーザがコールに応答してから 1 秒後に再生されます。ユーザが応答直後に DTMF トーンを生成するキー パッドを押すと、音声プロンプトが聞こえない場合があります。音声プロンプトは、リモート接続先のコール レッグでだけ再生されるため、遠端側にはプロンプトが聞こえません。音声プロンプトがユーザに再生されたら、デフォルトでシステムは、DTMF トーンを受信するために 5 秒間待機します。トーンが受信されない場合、システムはコール レッグを切断しますが、通話がユーザによって応答されるまで、または企業ボイス メール システムに転送されるまで、ユーザの設定した他のデバイスを鳴らし続けます。

(注)　ユーザ制御のモバイル ボイス メールの回避方式は、モバイル ボイス ネットワークまたは PSTN のリモート宛先から Unified CM まで DTMF トーンのリレーが成功することに完全に依存しています。DTMF トーンは Unified CM にアウトオブバンドで送信されます。DTMF リレーがネットワークおよびシステムで正しく設定されていない場合、DTMF は受信されず、ユーザ制御方式に依存するリモート宛先へのすべてのコール レッグは切断されます。システム管理者は、ユーザ制御方式を有効にする前に、企業のテレフォニー ネットワークで適切な DTMF の相互運用およびリレーを確認する必要があります。DTMF が PSTN から Unified CM に効果的にリレーできない場合、代わりにタイマー コントロールのモバイル ボイス メールの無効化方式を使用する必要があります。

シングル ナンバー リーチの有効化および無効化

シングル ナンバー リーチ（SNR）機能は、次の方法のいずれかを使用して有効または無効にできます。

- エンド ユーザのための Cisco Unified CM Administration または Cisco Unified CM Self Care Portal

  管理者またはユーザが、[シングルナンバーリーチを有効にする（Enable Single Number Reach）] チェックボックスをオフにしてその機能を無効にするか、[シングルナンバーリーチを有効にする（Enable Single Number Reach）] チェックボックスをオンにしてその機能を有効にします。これをリモート接続先ごとに実行します。

- モバイル ボイス アクセスまたはエンタープライズ機能アクセス

  モビリティ対応ユーザが、モバイル ボイス アクセスまたはエンタープライズ機能アクセスにダイヤルインして、適切なクレデンシャルを入力後に、数字の 2 を入力して有効にするか、数字の 3 を入力して無効にします。モバイル ボイス アクセスでは、単一のリモート接続先またはすべてのリモート接続先の SNR を有効/無効にするように促されます。エンタープライズ機能アクセスでは、呼び出しているリモート接続先の SNR しか有効/無効にできません。

- デスク フォンの [モビリティ（Mobility）] ソフトキーまたはアイコン

  ユーザは、電話がオンフック状態のときに [Mobility] ソフトキーを押して、モバイル コネクトを有効にするか、無効にするかを選択します。一部の電話機のモデルでは、ユーザはモビリティ アイコンにタッチしてから、[オフ（Off）] を選択して、シングル ナンバー リーチを無効にします。または、[この電話だけ呼び出す（Ring only this phone）] を選択することもできます。シングル ナンバー リーチを再度有効にするには、[すべてのデバイスを呼び出す（Ring all devices）] を選択します。この方法では、ユーザのリモート接続先すべてでシングル ナンバー リーチが有効または無効にされます。

(注)　前述の [モビリティ（Mobility）] ソフトキーを押すと表示されるダイアログ ボックスでは、新しい機能名である「シングル ナンバー リーチ」ではなく、古い機能名「モバイル コネクト」が使用されています。機能および有効化と無効化の手順は同じです。

シングル ナンバー リーチ コールの許可または拒否用のアクセス リスト

アクセス リストは、Cisco Unified CM 内で設定して、リモート接続先に関連付けることができます。アクセス リストは、モビリティ対応ユーザのリモート接続先に転送される着信コールを許可または拒否（着信コールの発信者 ID に基づく）するために使用されます。さらに、これらのアクセス リストは時刻に基づいて呼び出されます。

アクセス リストは、拒否または許可するモビリティ対応ユーザごとに設定されます。アクセス リストには、特定の番号または番号マスクで構成された 1 つ以上のメンバーまたはフィルタが含まれており、このフィルタが発信側の着信コールの発信者 ID と比較されます。発信者 ID と照合するための特定の番号文字列または番号マスクが含まれることに加えて、アクセス リストには、発信者 ID が使用できない、または、発信者 ID がプライベートに設定されている着信コール用のフィルタも含めることができます。拒否対象のアクセス リストには、アクセス リストに入力された番号からのコールは拒否されるが、その他の番号からのコールは許可されるように、リストの最後に暗黙の「すべて許可」が含まれています。許可対象のアクセス リストには、アクセス リストに入力された番号からのコールは許可されるが、その他の番号からのコールは拒否されるように、リストの最後に暗黙の「すべて拒否」が含まれています。

設定したアクセス リストを [リモート接続先（Remote Destination）] 設定画面で設定した [呼び出しスケジュール（Ring Schedule）] に関連付けると、設定した [呼び出しスケジュール（Ring Schedule）] と選択したアクセス リストの組み合わせによって、リモート接続先ごとのシングル ナンバー リーチ コールの時刻コール フィルタリングが提供されます。Cisco Unified CM Administration インターフェイスを使用している管理者または Cisco Unified CM Self Care Portal を使用しているエンド ユーザは、アクセス リストと Ring Schedule を設定してリモート接続先に関連付けることができます。

シングル ナンバー リーチのアーキテクチャ

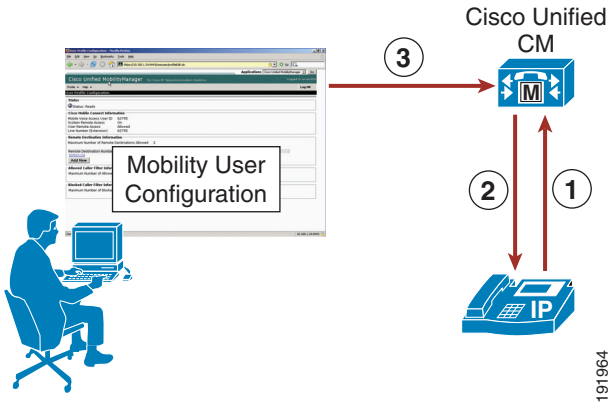
シングル ナンバー リーチ（SNR）機能のアーキテクチャを理解することは、その機能を理解することと同様に重要です。図 21-22 に、SNR に必要なメッセージ フローとアーキテクチャを示します。次の相互作用とイベントのシーケンスが、Unified CM、SNR ユーザ、および SNR ユーザのデスク フォンの間で発生する可能性があります。

1. SNR 機能の有効化または無効化、あるいはリモート接続先電話機の通話中コールのピックアップを希望している SNR 電話機のユーザが、デスク フォンの [モビリティ（Mobility）] ソフトキーを押します（図 21-22 のステップ 1 を参照）。
2. Unified CM から SNR のステータス（オンまたはオフ）が返されます。ユーザは、電話が接続状態であれば携帯電話にコールを転送するオプションを選択することも、電話がオン フック状態であれば SNR のステータスを有効/無効にすることもできます（図 21-22 のステップ 2 を参照）。
3. シングル ナンバー リーチ ユーザは、Unified CM Self Care Portal を使用して、次の URL にある Web ベースの設定ページ経由で独自のモビリティ設定を構成できます。

   https://<*Unified-CM_Server_IP_Address*>/ucmuser/

   ここで、<*Unified-CM_Server_IP_Address*> は、Unified CM パブリッシャ サーバの IP アドレスです（図 21-22 のステップ 3 を参照）。

図 21-22　　シングル ナンバー リーチのアーキテクチャ



シングル ナンバー リーチのハイ アベイラビリティ

シングル ナンバー リーチ機能には、次のコンポーネントが必要です。

- Unified CM サーバ
- PSTN ゲートウェイ

各コンポーネントの冗長性または弾力性を向上させて、さまざまな障害シナリオでシングル ナンバー リーチの機能が失われないようにする必要があります。

Unified CM サーバの冗長性

シングル ナンバー リーチ機能には、Unified CM サーバが不可欠です。Unified CM Group による電話機とゲートウェイの登録が冗長になっていれば、Unified CM サーバが故障しても SNR 機能は影響を受けません。

SNR ユーザが Unified CM Self Care Portal Web インターフェイスを使用してモビリティ設定（リモート接続先とアクセス リスト）を構成できるようにするには、Unified CM パブリッシャ サーバが使用可能である必要があります。パブリッシャがダウンすると、ユーザはモビリティ設定を変更できなくなります。同様に、管理者も Unified CM でモビリティ設定を変更できなくなります。ただし、既存のモビリティ設定と機能は維持されます。最後に、システムで SNR のステータスに対する変更を Unified CM パブリッシャ サーバ上に記録する必要があります。Unified CM パブリッシャが使用できない場合は、SNR を有効化または無効化できなくなります。

PSTN ゲートウェイの冗長性

シングル ナンバー リーチ機能は、新しいコール レッグを PSTN に拡張して SNR ユーザのリモート接続先電話機に到達する機能に依存しているため、PSTN ゲートウェイの冗長性は重要です。PSTN ゲートウェイが故障したり、容量不足の場合は、SNR コールを完了できません。通常は、会社の IP テレフォニー ダイヤル プランを通して、物理的なゲートウェイの冗長性とコールの再ルーティング機能だけでなく、予想されるコール アクティビティを処理する十分な容量が提供されることによって、PSTN アクセスに冗長性が提供されます。Unified CM が、コール ルーティングの弾力性を確保するための十分な容量、複数のゲートウェイ、およびルート グループとルート リストの構造で構成されていれば、この冗長性によって SNR 機能の持続性が保証されます。

モバイル ボイス アクセスとエンタープライズ機能アクセス

モバイル ボイス アクセス（システム リモート アクセスとも呼ばれる）とエンタープライズ機能アクセス 2 段階ダイヤリングは、シングル ナンバー リーチ アプリケーションに組み込まれている機能です。両方の機能を使用すれば、モビリティ対応ユーザは、外出先でも、Unified CM に直接接続されているかのように電話をかけることができます。この機能は、従来のテレフォニー環境では、一般的に、Direct Inward System Access（DISA）と呼ばれています。これらの機能を通して、通話料金を抑えたり、モバイル ユーザごとに通話料を請求するのではなく、直接会社に請求するように配慮することによって、会社にメリットがもたらされます。加えて、これらの機能を使用すれば、ユーザは、発信者 ID を外部に送信するときに、携帯電話やリモート接続先の番号を隠すことができます。代わりに、発信者 ID として、ユーザの会社の電話番号が送信されます。これによって、ユーザへの返信コールは会社の電話番号にかけられるため、コールを会社で一括管理できます。また、モバイル ユーザは、これらの機能を使用して、通常は企業外部から到達不能な内部の内線番号や DID 以外の会社の電話番号にダイヤルできます。

モバイル ボイス アクセスには、H.323 または SIP VoiceXML（VXML）ゲートウェイで応答および処理されるシステム設定の DID 番号を呼び出すことによってアクセスします。VoiceXML ゲートウェイによって、モバイル ボイス アクセス ユーザに対する双方向音声応答（IVR）プロンプトが再生され、ユーザ認証と電話機のキーパッド経由でダイヤルされる番号入力が要求されます。

エンタープライズ機能アクセス機能には、前述した通話切替機能や会議機能だけでなく、2 ステージ ダイヤリング機能が含まれています。2 ステージ ダイヤリングは、IVR プロンプトを除いて、モバイル ボイス アクセスと同様の方法で動作します。システム設定のエンタープライズ機能アクセス DID が Unified CM によって応答されます。ユーザは、電話機のキーパッドまたはスマート フォン ソフトキーを使用して、認証とダイヤルする番号を入力します。これらの入力はプロンプトなしで受信されます。

モバイル ボイス アクセスとエンタープライズ機能アクセス 2 段階ダイヤリングの両方の機能を使用すれば、ユーザは、入力番号に対するコールが接続されたときに、通話切替機能を呼び出したり、シングル ナンバー リーチと同様にデスク フォンでコールをピックアップしたりできます。この動作は、コールが会社のゲートウェイに固定されることによって可能になります。

モバイル ボイス アクセス IVR VoiceXML ゲートウェイ URL

モバイル ボイス アクセス機能を使用するには、Unified CM VoiceXML アプリケーションを H.323 または SIP ゲートウェイ上にインストールする必要があります。このアプリケーションをロードするための URL は次のとおりです。

http://<*Unified-CM-Publisher_IP-Address*>:8080/ccmivr/pages/IVRMainpage.vxml

ここで、<*Unified-CM-Publisher_IP-Address*> は、Unified CM パブリッシャ ノードの IP アドレスです。

モバイル ボイス アクセス機能

図 21-23 に、モバイル ボイス アクセスのコール フローを示します。この例では、モバイル ボイス アクセス ユーザが PSTN 電話機（408 555-7890）からモバイル ボイス アクセス会社の DID DN 408-555-2345 にダイヤルします（ステップ 1）。

このコールは、VoiceXML ゲートウェイとしても機能する会社の PSTN H.323 または SIP ゲートウェイに到達します（ステップ 2）。

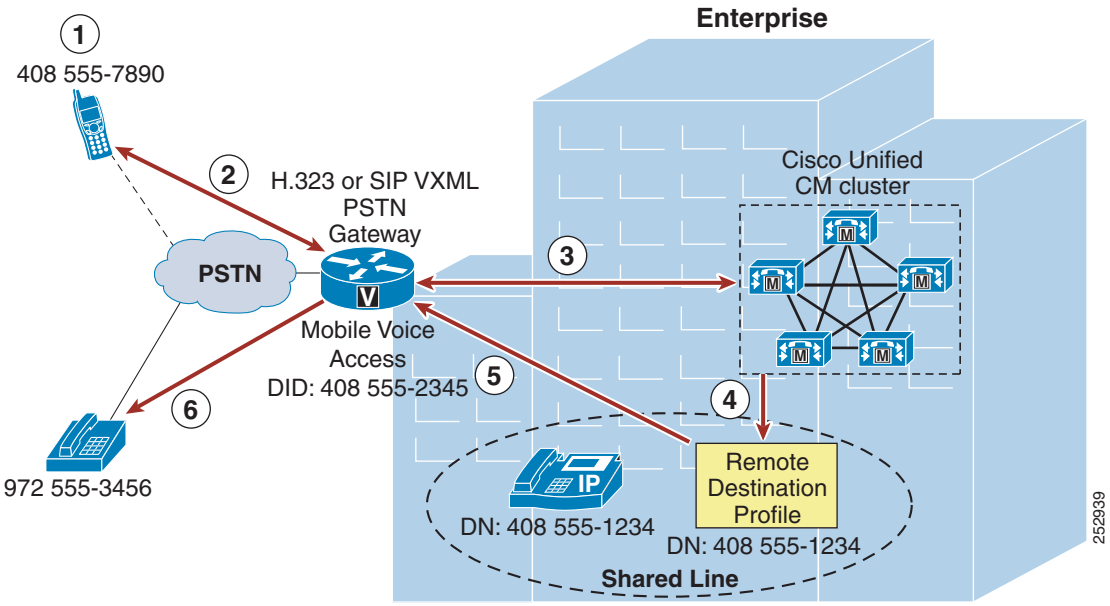
(注)　ネイティブ VoiceXML のサポートは Cisco IOS XE では利用できないため、Cisco 4000 シリーズ Integrated Services Router（ISR）をモバイル ボイス アクセスの VoiceXML ゲートウェイとして導入することはできません。代わりにネイティブ VXML をサポートする Cisco IOS ゲートウェイを使用する必要があります。

ユーザは、IVR 経由で、数字のユーザ ID（後ろに # 記号が続く）、PIN 番号（後ろに # 記号が続く）、および 1 の入力と、相手の電話番号が続くモバイル ボイス アクセス コールの発信を要求されます。この場合は、ユーザが相手の番号として 9 1 972 555 3456（後ろに # 記号が続く）を入力します。

(注)　モバイル ボイス アクセス ユーザがかけている PSTN 電話機が、そのユーザのシングル ナンバー リーチ リモート接続先として設定されており、Unified CM で着信コールの発信者 ID とこのリモート接続先を照合可能な場合は、数字のユーザ ID を入力する必要がありません。代わりに、PIN 番号の入力だけが要求されます。

その一方で、IVR プロンプトが Unified CM からゲートウェイに転送され、ゲートウェイでユーザに対してプロンプトが再生され、ゲートウェイでユーザの数字の ID と PIN 番号を含む入力が収集されます。この情報は、認証と 9 1 972 555 3456 へのコールを発信するために Unified CM に転送されます（ステップ 3）。ユーザの認証とダイヤルする番号の受信後に、Unified CM でユーザのリモート接続先プロファイル経由のコールが発信されます（ステップ 4）。972 555-3456 への発信コールが、PSTN ゲートウェイ経由で経路設定されます（ステップ 5）。最後に、番号が 972 555-3456 の PSTN 接続先電話機で呼出音が鳴ります（ステップ 6）。

図 21-23　モバイル ボイス アクセス



(注)　モバイル ボイス アクセスを図 21-23 のように動作させるには、システム全体の Enable Mobile Voice Access サービス パラメータが True に設定され、[End User] 設定ページでユーザごとに [Enable Mobile Voice Access] チェックボックスがオンになっていることを確認してください。

(注)　モバイル ボイス アクセス機能を使用するには、Unified CM Serviceability の設定ページで [Cisco Unified Mobile Voice Access Service] を手動でアクティブにする必要があります。このサービスは、パブリッシャ ノードでのみアクティブにできます。

(注)　ネイティブ VoiceXML をサポートしない Cisco 4000 シリーズ ISR を PSTN ゲートウェイとして使用する場合、モバイル ボイス アクセスに必要な VoiceVXML 機能を H.323 Cisco IOS ゲートウェイで提供するようにしてください。次のセクションで説明するように、H.323 Cisco IOS ゲートウェイでは、ヘアピニングという導入方法を使用してネイティブ VoiceXML をサポートします。

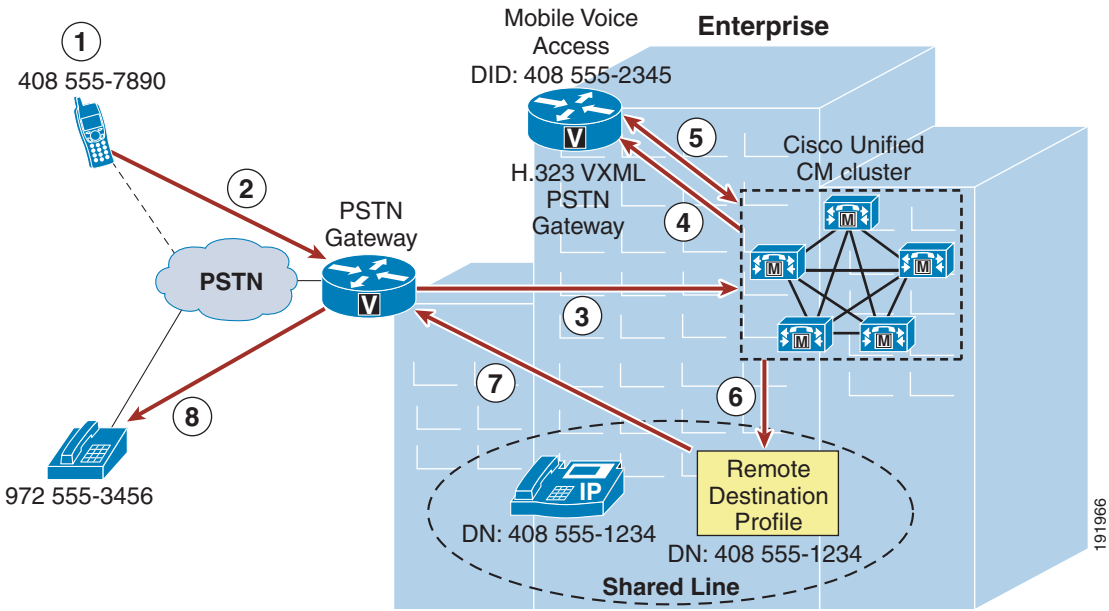
ヘアピニングを使用したモバイル ボイス アクセス

会社の PSTN ゲートウェイで H.323 または SIP が使用されていない配置では、H.323 を実行している別のゲートウェイ上のヘアピニングを使用することによってモバイル ボイス アクセス機能を提供することもできます。ヘアピニングを使用したモバイル ボイス アクセスの場合は、VoiceXML 機能を別の H.323 ゲートウェイに持たせる必要があります。図 21-24 に、ヘアピニングを使用したモバイル ボイス アクセスのコール フローを示します。この例では、前の例と同じく、モバイル ボイス アクセス ユーザが PSTN 電話機（408 555-7890）からモバイル ボイス アクセス会社の DID DN 408-555-2345 にダイヤルします（ステップ 1）。コールが、会社の PSTN ゲートウェイに入ってきて（ステップ 2）、呼処理のために Unified CM に転送されます（ステップ 3）。Unified CM が着信コールを H.323 VoiceXML ゲートウェイにルーティングします（ステップ 4）。IVR がユーザに、自分の数字のユーザ ID と PIN、およびモバイル ボイス アクセス コールを作成するための 1 を入力し、続けて接続先の電話番号を入力するように求めます。この場合も、ユーザが相手の番号として 9 1 972 555 3456（後ろに # 記号が続く）を入力します。

(注)　ヘアピニングを使用したモバイル ボイス アクセスでは、システムを呼び出しているユーザが発信者 ID によって自動的に特定されません。代わりに、PIN を入力する前に、手動でリモート接続先の番号を入力する必要があります。ユーザが自動的に特定されない理由は、ヘアピニングを使用する配置では、公衆網ゲートウェイにおいて最初にコールを Unified CM にルーティングして、ヘアピンされるモバイル ボイス アクセス ゲートウェイに到達する必要があるためです。コールが最初に Unified CM にルーティングされるため、発信番号が携帯の番号から会社の電話番号に変換されてから、コールがモバイル ボイス アクセス ゲートウェイによって処理されます。このため、モバイル ボイス アクセス ゲートウェイでは、発信番号と設定されているリモート接続先の照合を行うことができず、ユーザはリモート接続先番号の入力を求められます。これは、ヘアピニングを使用する配置に特有の現象です。通常のモバイル ボイス アクセスのフローにおいては、モバイル ボイス アクセス機能はローカル ゲートウェイで利用できるため、PSTN ゲートウェイで最初にコールを Unified CM にルーティングしてからモバイル ボイス アクセスにアクセスする必要がありません。

その間に、H.323 VoiceXML ゲートウェイは、ユーザ入力を収集して Unified CM に転送し、転送された IVR プロンプトを PSTN ゲートウェイおよびモバイル ボイス アクセス ユーザに対して再生します。これを受けて Unified CM がユーザ入力を受信し、ユーザを認証し、ユーザ入力に基づいて適切な IVR プロンプトを H.323 VoiceXML ゲートウェイに転送します（ステップ 5）。ダイヤルする番号の受信後に、Unified CM でユーザのリモート接続先プロファイルを使用したコールが発信されます（ステップ 6）。972 555-3456 への発信コールが、PSTN ゲートウェイ経由で経路設定されます（ステップ 7）。最後に、番号が 972 555-3456 の PSTN 接続先電話機で呼出音が鳴ります（ステップ 8）。

図 21-24　　ヘアピニングを使用したモバイル ボイス アクセス



(注)　モバイル ボイス アクセスをヘアピニング モードで配置する場合は、PSTN ゲートウェイでのモバイル ボイス アクセス DID と Cisco Unified CM 内のモバイル ボイス アクセス電話番号（**Media Resources - Mobile Voice Access**）を別々の番号として設定することを推奨します。そうすれば、Unified CM 内のトランスレーション パターンを使用して、モバイル ボイス アクセス DID の着信番号を設定済みのモバイル ボイス アクセス電話番号に変換できます。Unified CM 内で設定されたモバイル ボイス アクセス電話番号は管理者にしか表示されないため、DID と電話番号間の変換をエンド ユーザが意識する必要はなく、エンド ユーザのダイヤリング動作に変更は生じません。この方法は、マルチクラスタ環境でのモビリティ コール ルーティング問題を回避するために推奨されています。この推奨事項は、非ヘアピニング モードのモバイル ボイス アクセスには当てはまりません。

(注)　ヘアピニング モードのモバイル ボイス アクセスは、H.323 VXML ゲートウェイだけでサポートされています。

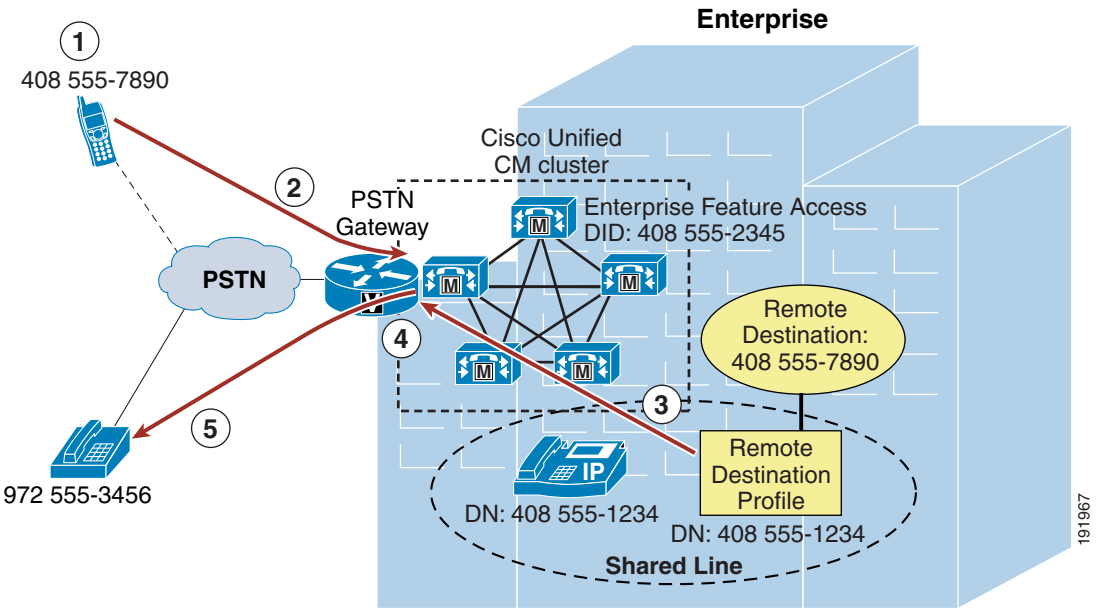
2 段階ダイヤリングを伴うエンタープライズ機能アクセス

図 21-25 に、エンタープライズ機能アクセス 2 ステージ ダイヤリングを示します。この例では、モビリティ ユーザがリモート接続先電話機（408 555-7890）からエンタープライズ機能アクセス DID 408 555-2345 にダイヤルします（ステップ 1）。コールが接続されると、Unified CM で認証されるユーザの PIN（後ろに # 記号が続く）で始まる DTMF 番号を PSTN ゲートウェイ経由で Unified CM に送信するためにリモート接続先電話機が使用されます。次に、2 ステージ ダイヤリング対象コールが試みられることを示す 1（後ろに # 記号が続く）と相手の電話番号が送信されます。この場合は、ユーザが接続先番号として 9 1 972 555 3456 と入力します（ステップ 2）。

(注)　モバイル ボイス アクセスとは違って、エンタープライズ機能アクセスでは、エンド ユーザ アカウントに対して発信者 ID と PIN を照合するためにリモート接続先として設定された電話機から、すべての 2 ステージ ダイヤリング対象コールを発信する必要があります。エンタープライズ機能アクセスにおいては、モビリティ ユーザが自身を識別するためのリモート接続先番号または ID をシステムに入力するための仕組みは用意されていません。同一性は、着信コールの発信者 ID と入力された PIN の組み合わせを通してのみ確立できます。

次に、発信コールがユーザのリモート接続先プロファイル経由で開始され（ステップ 3）、PSTN 番号 972 555-3456 へのコールが会社の PSTN ゲートウェイ経由で経路設定されます（ステップ 4）。最後に、PSTN 電話機が呼び出されます（ステップ 5: この場合は 972 555-3456）。モバイル ボイス アクセスと同様に、各エンタープライズ機能アクセス 2 ステージ ダイヤリング対象コールの音声メディア パスは、2 つのゲートウェイ ポートを使用している PSTN ゲートウェイ内でヘアピンされます。

図 21-25　エンタープライズ機能アクセス 2 ステージ ダイヤリング機能



(注)　エンタープライズ機能アクセス 2 ステージ ダイヤリングを図 21-25 のように動作させるには、システム全体の Enable Enterprise Feature Access サービス パラメータが True に設定されていることを確認してください。

デスク フォンとリモート接続先電話機のピックアップ

モバイル ボイス アクセス機能とエンタープライズ機能アクセス機能はシングル ナンバー リーチと緊密に統合されているため、モバイル ボイス アクセスまたはエンタープライズ機能アクセス 2 段階ダイヤリング対象コールが確立されていれば、ユーザはシングル ナンバー リーチ機能を利用して、最初に着信した電話機をオン フックしてデスク フォンの [再開（Resume）] ソフトキーを押すだけで、または、通話切替保留機能を使用して、通話中のコールをデスク フォンでピックアップできます。さらに、その後で、ユーザの設定済みリモート接続先電話機で Mobility ソフトキーを押して Send Call to Mobile Phone を選択することによって、そのコールをピックアップできます。

シングル ナンバー リーチの有効化および無効化

モバイル ボイス アクセスとエンタープライズ機能アクセスのユーザはまるで社内にいるかのように PSTN から電話がかけられるだけでなく、H.323 または SIP VoiceXML ゲートウェイ上のモバイル ボイス アクセスで提供される機能とエンタープライズ機能アクセスで提供される機能によって、ユーザは電話機のキーパッドを使用して、リモート接続先ごとのシングル ナンバー リーチ機能をリモートで有効または無効にすることもできます。1 を入力して電話をかけるのではなく、ユーザは、2 を入力してシングル ナンバー リーチ機能を有効にし、3 を入力してシングル ナンバー リーチ機能を無効にします。

モバイル ボイス アクセスを使用するにあたって、複数のリモート接続先を設定する場合は、シングル ナンバー リーチ機能を有効または無効にするリモート接続先の電話番号を入力するように要求されます。エンタープライズ機能アクセスでは、呼び出しているリモート接続先電話機のシングル ナンバー リーチしか有効/無効にできません。

（注）　[モバイルボイスアクセスの有効化（Enable Mobile Voice Access）] サービス パラメータが [False（False）] に設定されており、2 段階ダイヤリング対象コールを行うことができない場合でも、モバイル ボイス アクセスでは、リモートからシングル ナンバー リーチを有効または無効にする機能が提供されます。システムにモバイル ボイス アクセス電話番号が設定され、ユーザのアカウントでモバイル ボイス アクセスが有効にされ、Cisco Unified Mobile Voice Access サービスがパブリッシャ上で実行されている限り、認証済み発信側のユーザはシングル ナンバー リーチを有効または無効にできます。

モバイル ボイス アクセスとエンタープライズ機能アクセスの番号拒否

管理者は、モバイル ボイス アクセスとエンタープライズ機能アクセスの 2 ステージ ダイヤリングのユーザが、それらの機能の使用中は特定の番号にダイヤルできないようにできます。オフネット コールに対してこれらの機能を使用している場合に特定の番号へのコールを制限または拒否するには、[System Remote Access Blocked Numbers] サービス パラメータ フィールドでそのような番号のカンマ区切りのリストを設定できます。このパラメータに拒否する番号を設定したら、モバイル ボイス アクセスまたはエンタープライズ機能アクセスが使用されている場合は、ユーザのリモート接続先電話機からそれらの番号にダイヤルできなくなります。管理者が拒否したい番号には、911 などの緊急電話番号を含めることができます。拒否する番号を設定する場合は、会社のユーザが該当するプレフィックスまたは振り分け用の数字を付けてダイヤルするようにそれらの番号が設定されていることを確認してください。たとえば、緊急電話番号を拒否対象とし、システム ユーザが緊急電話番号をダイヤルするときは 9911 を使用しなければならない場合は、[System Remote Access Blocked Numbers] フィールドに設定する番号を 9911 にする必要があります。

モバイル ボイス アクセスのアクセス番号

Unified CM システムでは、1 つのモバイル ボイス アクセス電話番号だけを設定することもできますが、これらの内部で設定された番号にアクセス可能な外部番号を複数使用できます。たとえば、米国の New York に配置されたシステム、San Jose のリモート サイト、および London の海外サイトがある場合を考えます。システムのモバイル ボイス アクセス電話番号が 555-1234 に設定されている場合でも、各ロケーションのゲートウェイを設定して、ローカル DID 番号またはフリーダイヤル DID 番号をこのモバイル ボイス アクセス電話番号にマッピングできます。たとえば、New York のゲートウェイの DID である +1 212 555 1234 と +1 800 555 1234 の両方をモバイル ボイス アクセス番号にマッピングし、さらに San Jose のゲートウェイの DID +1 408 666 5678 および London のゲートウェイの DID +44 208 777 0987 もシステムのモバイル ボイス アクセス番号にマッピングできます。

システム管理者は、複数のローカル DID 番号またはフリーダイヤル DID 番号を用意することによって、モバイル ボイス アクセスの 2 段階ダイヤリング対象コールが常にローカルまたはフリーダイヤルのコールとしてシステムに発信されるようにでき、さらにテレフォニー関連コストを削減できます。

リモート接続先の設定と発信者 ID の照合

モバイル ボイス アクセス機能およびエンタープライズ機能アクセス 2 段階ダイヤリング機能に加えて、DTMF ベースの通話切替機能の転送と会議のユーザを認証するときに、発信元のリモート接続先電話機の発信者 ID がシステム内で設定されたすべてのリモート接続先に対して照合されます。この発信者 ID の照合は、リモート接続先番号の設定方法、システムで PSTN 振り分け用数字を含めるために番号プレフィックスが必要かどうか、[Matching Caller ID with Remote Destination] パラメータが [Partial Match] と [Complete Match] のどちらに設定されているかなどの複数の要因に左右されます。いずれの場合も、要件は、1 つまたは複数のリモート接続先番号に基づいて各モビリティ ユーザを識別できることです。したがって、リモート宛先番号がシステム内で一意に設定されるだけでなく、着信コールの発信者 ID の一致（完全照合を使用するか、一部照合を使用するか）が 1 つのリモート宛先に常に一意に対応しなければならないことも重要です。単一または一意の一致が見つからない場合、発信者 ID 照合は失敗します。

この照合の特性を制御するために、次の 2 つのアプローチを検討してください。

完全発信者 ID 照合の使用

このアプローチでは、発信者 ID が PSTN から供給されているかのようにリモート接続先を設定します。たとえば、リモート接続先電話機の発信者 ID を PSTN からシステムに 4085557890 として供給する場合は、[Remote Destination] 設定ページでこの番号を設定する必要があります。

このリモート接続先にシングル ナンバー リーチ コールを適切にルーティングするには、+E.164 ダイヤル方式または番号プレフィックス メカニズムを使用して必要な PSTN アクセス コードおよび他の必要な数字にプレフィックスを付けるようにダイヤル プランを設定する必要があります。たとえば、グローバル +E.164 ダイヤル プランを使用しないで、企業からのコールをダイヤルするときに 9 個のまたは他の PSTN 振り分け用数字または国番号が PSTN に到達するために必要であることが想定される場合、設定済みのリモート接続先番号の先頭に適切な PSTN 振り分け用数字と国番号を追加するように番号プレフィックスを設定する必要があります。番号プレフィックスは、Unified CM システム内でトランスレーション パターン、ルート パターン、またはルート リスト コンストラクトを使用して実施する必要があります。この完全照合アプローチおよび番号プレフィックス方式を使用する場合、Matching Caller ID with Complete Match パラメータをデフォルト設定の [Complete Match] のままにする必要があります。

アプリケーション ダイヤル ルールは、これらのシナリオで番号プレフィックスを提供するためにも使用されることがあります。ただし、アプリケーション ダイヤル ルールが着信ディジット ストリングの長さに基づくため分割できないことも注目すべきことであり、それは、システム全体でグローバルに適用されることを意味します。これは特に、複数のダイヤル ドメイン（たとえば、異なる国）が単一の Unified CM クラスタでサポートされる必要があるシナリオにおけるアプリケーション ダイヤル ルールの使用を厳しく制限します。

(注)　アプリケーション ダイヤル ルールはシングル ナンバー リーチ、モバイル ボイス アクセス、およびエンタープライズ機能アクセスのコールに適用されるだけでなく、Cisco WebDialer、Cisco Unified CM Assistant、および Cisco Jabber アプリケーションから発信されたコールにも適用されます。したがって、すべてのアプリケーションを通してダイヤリング動作が期待どおりに機能するように、これらの規則を慎重に設定する必要があります。

推奨されるダイヤル プラン アプローチは、発信者 ID を PSTN からの入力の +E.164 に常にグローバル化し、リモート接続先を +E.164 として常に設定することです。これによって、すべての設定済みリモート接続先と比較すると、PSTN からの発信者 ID（正規化後）が一意の一致を常に提供することが保証されます。+E.164 ダイヤリングをサポートするダイヤル プランと組み合わせると、これは複数の国際番号計画をサポートしている場合でも、番号プレフィックスを不要にし、リモート接続先のユーザおよび番号の一意の ID を確認します。推奨されるダイヤル プラン アプローチがトランクの要件やユーザの希望に従って入力の発信者 ID をグローバル化し、出力でローカライズするため、PSTN から供給される発信者 ID を使用することはこのアプローチと互換性がありません。

部分発信者 ID 照合の使用

このアプローチでは、リモート接続先が、システムから PSTN にダイヤルされたかのように設定されます。たとえば、リモート接続先の番号が 14085557890 で、システムから PSTN にアクセスするために 9 を入力する必要がある場合は、[Remote Destination] 設定ページでこの番号を 914085557890 に設定する必要があります。このアプローチでは、システムにおける番号プレフィックス メカニズムの設定を必要としませんが、[Matching Caller ID with Remote Destination] サービス パラメータを [Partial Match] に設定し、[Number of Digits for Caller ID Partial Match] をリモート接続先発信者 ID に対して照合すべき連続桁数を表す適切な数字に設定する必要があります。たとえば、リモート接続先の発信者 ID が 14085557890 で、リモート接続先が 914085557890 に設定されている場合は、[Number of Digits for Caller ID Partial Match] を 10 または 11 に設定するのが理想的です。この例では、このパラメータをさらに少ない桁数に設定できます。ただし、システム内のすべての設定済みリモート接続先を一意的に識別できるように十分な連続桁数が照合されることを保証するように注意してください。部分発信者 ID 照合を使用したときに完全な一致が見つからない場合、または複数の設定済みリモート接続先が一致した場合は、システムで一致するリモート接続先番号が存在しないものとして処理されます。したがって、モバイル ボイス アクセスの場合は、PIN を入力する前にリモート接続先番号/ID を手動で入力する必要があります。エンタープライズ機能アクセスには、ユーザがリモート接続先番号を入力するメカニズムがありません。そのため、この機能を使用する場合は、一致が一意的にしか発生しないことを確認してください。

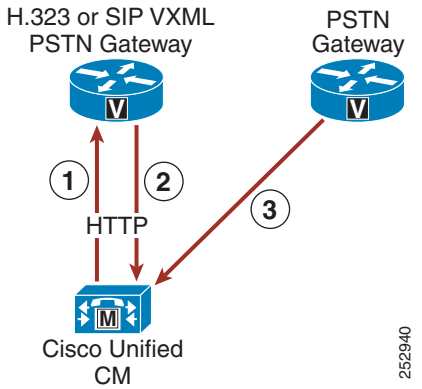
(注)　PSTN サービス プロバイダーが可変長の発信者 ID を送信する場合は、着信コールごとの一意的な発信者 ID の一致が保証できない可能性があるため、部分発信者 ID 照合の使用は推奨できません。これらのシナリオでは、完全発信者 ID 照合または +E.164 ダイヤル プランは望ましい方法です。

モバイル ボイス アクセスとエンタープライズ機能アクセスのアーキテクチャ

モバイル ボイス アクセスとエンタープライズ機能アクセスのアーキテクチャを理解することは、それらの機能性を理解することと同じくらい重要です。図 21-26 は、モバイル ボイス アクセスとエンタープライズ機能アクセスに必要なメッセージ フローとアーキテクチャを示しています。Unified CM、PSTN ゲートウェイ、および H.323 または SIP VXML ゲートウェイの間には、次の一連の対話とイベントが発生します。

1. Unified CM から HTTP 経由で IVR プロンプトとインストラクションが H.323 または SIP VXML ゲートウェイに転送されます（図 21-26 のステップ 1 を参照）。これによって、VXML ゲートウェイで着信モバイル ボイス アクセス発信者に対してこれらのプロンプトを再生できます。
2. H.323 または SIP VXML ゲートウェイでは、HTTP を使用してモバイル ボイス アクセス ユーザの入力が Unified CM に戻されます（図 21-26 のステップ 2 を参照）。
3. PSTN ゲートウェイでは、リモート接続先電話機からのエンタープライズ機能アクセス 2 ステージ ダイヤリングおよび通話切替機能に関するユーザまたはスマート フォンのキー シーケンスに応答して DTMF 番号が転送されます（図 21-26 のステップ 3 を参照）。

図 21-26　モバイル ボイス アクセスとエンタープライズ機能アクセスのアーキテクチャ



（注）　図 21-26 では PSTN ゲートウェイとは別のボックスとして H.323 または SIP VoiceXML ゲートウェイが描かれていますが、これはアーキテクチャ上の要件ではありません。PSTN ゲートウェイで H.323 または SIP 以外のプロトコルを実行する必要がなければ、VoiceXML 機能と PSTN ゲートウェイ機能を同じボックスで処理できます。H.323 または SIP ゲートウェイは、モバイル ボイス アクセス VoiceXML 機能に不可欠です。

（注）　Cisco IOS XE ではネイティブ VoiceXML のサポートを提供していないため、Cisco 4000 シリーズ ISR をモバイル ボイス アクセスの VoiceXML ゲートウェイとして使用することはできません。Cisco 4000 シリーズ ISR を PSTN ゲートウェイとして使用する場合は、VoiceXML 機能のほとんどを、ネイティブ VoiceXML をサポートする Cisco IOS ゲートウェイで提供する必要があります。

モバイル ボイス アクセスおよびエンタープライズ機能アクセスのハイ アベイラビリティ

モバイル ボイス アクセス機能とエンタープライズ機能アクセス機能には、シングル ナンバー リーチ機能と同じコンポーネントと冗長性メカニズムが必要です（シングル ナンバー リーチのハイ アベイラビリティ（21-63 ページ）を参照）。Unified CM Group は、PSTN ゲートウェイ登録の冗長性に欠かせません。同様に、PSTN の物理ゲートウェイとゲートウェイ接続の冗長性を提供する必要があります。PSTN と会社間の冗長なアクセスは、ゲートウェイが故障した場合に、リモート接続先電話機からモバイル ボイス アクセス機能とエンタープライズ機能アクセス機能にアクセスするために必要です。ただし、必要に応じて、H.323 または SIP VoiceXML ゲートウェイに対して物理的な冗長性を提供できますが、Unified CM 上には、Cisco Unified Mobile Voice Access サービス用の冗長性メカニズムがありません。このサービスは、パブリッシャ ノードでしか有効にして実行することができません。そのため、パブリッシャ ノードが無効な場合は、モバイル ボイス アクセス機能が使用できません。エンタープライズ機能アクセスと 2 ステージ ダイヤリング機能には、このようなパブリッシャとの依存関係がないため、モビリティ ユーザに同等の機能性（IVR プロンプトが再生されない）を提供できます。

Cisco Unified Mobility の配置の設計

Cisco Unified Mobility ソリューションでは、Cisco Unified CM を介してモビリティ機能が提供されます。機能には、シングル ナンバー リーチ、モバイル ボイス アクセス、およびエンタープライズ機能アクセスが含まれます。この機能を配置する場合は、ダイヤル プランの意味、ガイドラインと制約事項、および性能と容量に関する考慮事項を理解しておくことが重要です。

Cisco Unified Mobility のダイヤル プランに関する考慮事項

Unified Mobility を適切に設定してプロビジョニングするには、リモート接続先プロファイル設定のコール ルーティング動作とダイヤル プランの意味を理解しておくことが重要です。

リモート接続先プロファイルの設定

Unified Mobility を設定する場合は、[Remote Destination Profile] 設定ページにある次の 2 つの設定を考慮する必要があります。

- [コーリングサーチスペース（Calling Search Space）]

  この設定と電話番号または回線レベルのコーリング サーチ スペース（CSS）を組み合わせて、モビリティ ダイヤル対象コール用にアクセス可能なパーティションが決定されます。この設定は、モバイル ボイス アクセスとエンタープライズ機能アクセス 2 ステージ ダイヤリングを含む、リモート接続先電話機からのモビリティ ユーザによるコールだけでなく、通話切替の転送機能と会議機能の組み合わせによるコールにも影響します。この CSS と回線レベルの CSS の組み合わせの中に、ユーザのリモート接続先電話機から発信されたビジネス コールのためにアクセスする必要のあるすべてのパーティションが含まれていることを確認してください。ローカル ルート グループを持つ回線だけの従来のアプローチを使用する +E.164 ダイヤル プランでは、この CSS は必要なく、**<None>** に設定できます。

- [再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）]

  この設定によって、ユーザのリモート接続先電話機にコールが送信されたときにアクセスするパーティションが決定されます。これは、すべてのシングル ナンバー リーチ コールに適用されます。ユーザの会社の電話番号へのコールもシングル ナンバー リーチ経由でユーザのリモート接続先に送信される場合は、この CSS によってシステムからリモート接続先電話機に到達する方法が決定されます。したがって、CSS を通して、PSTN またはモバイル ボイス ネットワークに到達するために、適切なルート パターンとゲートウェイを含むパーティションにアクセスできる必要があります。

リモート接続先プロファイル ルーティング CSS を設定する場合は、この CSS 内のルート パターンが、ユーザのデスクトップフォンへの着信コールを経路設定するゲートウェイと同じコール アドミッション制御ロケーションにあるゲートウェイを指すようにすることを推奨します。これによって、コールをリモート接続先に経路設定するときに、2 地点間の帯域幅不足によるコール アドミッション制御拒否が発生しなくなります。さらに、WAN 帯域幅が不十分な場合は、初期シングル ナンバー リーチ コールの経路設定後のコール アドミッション制御チェックで拒否されないため、同じコール アドミッション制御ロケーション内のゲートウェイに着信コール レッグと発信コール レッグを経路設定することによって、このコール中の以降のデスク フォンまたはリモート接続先のピックアップ動作で WAN 帯域幅のオーバーサブスクリプションが発生する可能性のあるコール アドミッション制御の必要がなくなることが保証されます。

標準ローカル ルート グループを使用するルート リストを指すルート パターンを使用する場合は、発信者のデバイス プールで設定されたローカル ルート グループが使用されます。この場合リモート接続先へのコール レッグの出力ゲートウェイは、元の発信側デバイスに対してローカルです。PSTN からのコールの場合、これは、元の発信者（この場合、着信ゲートウェイ）と同じコール アドミッション制御ロケーションで出力ゲートウェイを使用する上記の要件を満たすのに役立ちます。

2 段階ダイヤリング対象コールを送信したときのコール アドミッション制御拒否が最小化されるようにすることも同様に重要です。2 段階ダイヤリング対象コールのコール アドミッション制御拒否は、発信コール レッグをルーティングするために使用される出力ゲートウェイが着信コール レッグの入力ゲートウェイによって選択されるようにローカル ルート グループ コンストラクトを使用することによって最小化、または回避できます。この方法で、使用される入力ゲートウェイおよび出力ゲートウェイは、同じコール アドミッション制御ロケーションにあるようになります。また、リモート接続先プロファイルのデバイス レベルの CCS 内のルート パターンは、モバイル ボイス アクセス システムまたはエンタープライズ機能アクセス システムのアクセス番号への着信コール レッグを処理した入力ゲートウェイと同じコール アドミッション制御ロケーションにある出力ゲートウェイを指す必要があります。ただし、デスクトップフォンがモバイル ボイス アクセスまたはエンタープライズ機能アクセス システムのアクセス番号が転送されるゲートウェイとは異なるコール アドミッション制御ロケーション内に存在する場合は、以降のデスクトップフォンのピックアップによって、WAN 帯域幅のオーバーサブスクリプションが発生する可能性があることに注意してください。

自動発信者 ID 照合とエンタープライズ コール アンカリング

理解しておく必要のある Unified Mobility ダイヤル プランのもう一つの側面は、設定済みのリモート接続先電話機からの着信コールに対する自動発信者 ID 識別に関するシステム動作です。着信コールがシステムに入ると、そのコールに対して提供された発信者 ID が設定済みのすべてのリモート接続先電話機と比較されます。一致するものが見つかった場合は、そのコールが自動的にその会社のものと固定されるため、ユーザは通話切替機能を呼び出したり、通話中のコールをデスクトップフォンでピックアップできます。この動作は、着信コールがモバイル ボイス アクセスまたはエンタープライズ機能アクセスを使用したモビリティ コールとして開始されていない場合でも、モビリティ ユーザのリモート接続先電話機からの着信コールすべてに対して行われます。

(注)　設定済みのリモート接続先番号に対する自動着信コール発信者 ID 照合は、Matching Caller ID with Remote Destination サービス パラメータが Partial Match と Complete Match のどちらに設定されているかの影響を受けます。この設定に関する詳細については、リモート接続先の設定と発信者 ID の照合（21-70 ページ）を参照してください。

自動エンタープライズ コール アンカリングに加えて、設定済みのリモート接続先電話機から会社に電話がかかった場合の着信コール ルーティングと発信コール ルーティングも考慮する必要があります。設定済みのリモート接続先からのコールに対する着信コール ルーティングは、Inbound Calling Search Space for Remote Destination サービス パラメータの設定によって次の 2 つの方法のどちらかで発生します。デフォルトで、このサービス パラメータは、**Trunk or Gateway Inbound Calling Search Space** に設定されます。このサービス パラメータがデフォルト値に設定されている場合、設定済みのリモート接続先からの着信コールは、コールが着信する PSTN ゲートウェイまたはトランクの着信通話サーチ スペース（CSS）を使用してルーティングされます。一方、[リモート接続先の着信通話サーチ（Inbound Calling Search Space for Remote Destination）] パラメータが [リモート接続先プロファイル+回線通話サーチスペース（Remote Destination Profile + Line Calling Search Space）] に設定されている場合は、リモート接続先からの着信コールが、PSTN ゲートウェイまたはトランクの着信 CSS をバイパスして、代わりに、関連するリモート接続先プロファイル CSS（と回線レベル CSS の組み合わせ）を使用してルーティングされます。

リモート接続先電話機からの着信コールの特性を考えると、このような着信コールへのアクセスを社内の電話機に到達させるために必要なすべてのパーティションに提供するためには、コーリング サーチ スペースが適切に設定されていることを確認する必要があります。これによって、リモート接続先電話機からの適切なコール ルーティングが保証されます。

(注)　設定済みのリモート接続先電話機からではない着信コールでは、必ず、トランクまたはゲートウェイ着信 CSS が使用されるため、Inbound Calling Search Space for Remote Destination サービス パラメータの影響を受けません。

モバイル ボイス アクセスまたはエンタープライズ機能アクセス コールの発信コール ルーティングでは、必ず、リモート接続先プロファイル回線 CSS とデバイス レベル CSS を連結したものが使用されるため、オフネットまたは PSTN アクセスに必要なすべてのルート パーティションへのアクセスを提供するためには、これらのコーリング サーチ スペースが適切に設定されていることを確認する必要があります。これによって、リモート接続先電話機からの適切な発信コール ルーティングが保証されます。

Intelligent Session Control およびすべてのシェアド ライン呼び出し

Intelligent Session Control 機能を使用すると、設定されたリモート接続先番号への社内からの直接コールを、自動的にコール アンカリングできます。通常、モビリティ コール アンカリングは、ユーザの会社の電話番号にかけられたコール、またはユーザの会社の電話番号からかけられたコールでだけ行われます。エンタープライズ 2 段階ダイヤリングによって外部から発信されたコールは、内部コールとしてルーティングされるため、システムはアンカリングを行います。Intelligent Session Control 機能を有効にすると、社内から設定済みリモート接続先への直接コールもアンカリングが行われます。

この機能は、Reroute Remote Destination Calls to Enterprise Number サービス パラメータを True に設定することによって有効にします。デフォルトで、このサービス パラメータは False に設定されており、この機能は無効になっています。この機能を有効にすると、ダイヤルされたリモート接続先へのコールが PSTN 経由でルーティングされるだけでなく、コールが自動的に会社のゲートウェイ内部で固定されます。このタイプのコールを固定することによって、着信側モバイル ユーザが通話切替機能およびデスクトップフォンのピックアップまたはセッション ハンドオフを呼び出すことができるようになります。

たとえば、Intelligent Session Control 機能が有効にされており、モビリティ対応ユーザのリモート接続先番号が携帯の番号に対応する 408 555 1234 として設定されているとします。別のユーザがデスクトップフォンからそのモビリティ対応ユーザのリモート接続先番号（408 555 1234）にダイヤルすると、そのコールは PSTN 経由でリモート接続先にルーティングされ、同時に会社のゲートウェイでアンカリングされます。コールがセットアップされて固定されると、着信側モビリティ対応ユーザは、保留、転送、会議などの通話切替機能を呼び出したり、デスクトップフォンのピックアップまたはセッション ハンドオフを実行したりできるようになります。

この同じ例で、Intelligent Session Control 機能が無効であるとすると、システム ユーザがこのモビリティ対応ユーザのリモート接続先に社内のデスク フォンから直接ダイヤルした場合、そのコールは PSTN 経由で着信側リモート接続先にルーティングされますが、アンカリングはされません。その結果、モバイル ユーザは、保留や転送などの通話切替機能を呼び出したり、デスクトップフォンのピックアップまたはセッション ハンドオフを実行したりできません。

この機能を有効にする場合は、ダイヤル プランの設定およびコール ルーティングへの影響を理解することが重要となります。この機能を呼び出すには、内部ユーザが PSTN のリモート接続先番号に到達するためにダイヤルする番号（必要なすべての PSTN 振り分け用数字を含む）は、システムに設定されているリモート接続先（またはモビリティ ID）番号と一致する必要があります。たとえば、リモート接続先番号がシステムに 408 555 1234 と設定されており、通常、発信する番号に加えて PSTN 振り分け用数字 91 を内部ユーザがダイヤルする必要がある場合は、再ルーティングおよびそれによるエンタープライズ コール アンカリングは実行されません。これは、ユーザが PSTN のリモート接続先に到達するために 91 408 555 1234 をダイヤルした一方、リモート接続先は 408 555 1234 と設定されており、これらの番号が一致しないためです。

この機能が適切に機能するには、設定されたリモート接続先と、PSTN のこのリモート接続先に到達するためにダイヤルする必要がある番号とが一致する必要があります。これらの番号が一致するようにするには、Matching Caller ID with Remote Destination サービス パラメータを **Partial Match** に設定します。このパラメータを Partial Match に設定し、Number of Digits for Caller ID Partial Match サービス パラメータを使用して部分一致対象桁数を指定することによって、ダイヤルされた番号に PSTN 振り分け用数字が含まれていても、設定されたリモート接続先番号とダイヤルされた番号が一致します。

前の例を使用し、システムが 10 桁の部分一致を使用するように設定されているとすると、ダイヤルされた番号 9 1 408 555 1234 は、設定されたリモート接続先 408 555 1234 に一致します。これは、部分一致では、Number of Digits for Caller ID Partial Match に指定された桁数（この場合は 10 桁）が照合されるためです。2 つの番号は、右から左に向かって照合されます。ダイヤルされた番号 9 1 408 555 1234 の最後の 10 桁は 408 555 1234 であり、この 10 桁が、10 桁の設定されたリモート接続先（408 555 1234）に一致します。この例では、発信コールは社内で固定され、着信側モバイル ユーザは通話切替機能を呼び出したり、デスクトップフォンのピックアップまたはセッション ハンドオフを実行したりできます。

この機能を使用する場合、一見すると、必要なすべての PSTN 振り分け用数字を含むリモート接続先番号またはモビリティ ID 番号を設定する方が簡単に見えます。しかし、必要な PSTN 振り分け用数字を含む番号を設定し、発信者 ID の部分一致を設定していない場合、設定されたリモート接続先またはモビリティ ID からの着信コールに対して発信者 ID の自動照合およびエンタープライズ アンカリングを実行できません。前の例では、リモート接続先番号が 9 1 408 555 1234 と設定されており、発信者 ID の完全一致が使用されている場合、リモート接続先からの着信コールの発信者 ID は 408 555 1234 となり、これらの番号が一致せず、リモート接続先からの着信コールが想定どおりに固定されません。

このように発信コールでダイヤルされる Intelligent Session Control 機能を使用する場合には、番号と、着信コールの設定されたリモート接続先番号が異なる可能性があるため、PSTN に到達するために 1 つ以上の振り分け用数字が必要なすべての配置において、発信者 ID の（完全一致ではなく）部分一致を有効にすることを推奨します。これにより、PSTN 振り分け用数字を使用してリモート接続先番号に直接発信されたコールが一致し、アンカーされるようになります。一方で、PSTN に到達するために振り分け用数字が必要なく、ユーザが完全な E.164 番号をダイヤルして PSTN にコールをルーティングできる場合には、発信者 ID と照合されるリモート接続先の番号が、PSTN のリモート接続先またはモビリティ ID に到達するために内部ユーザがダイヤルする番号と同じであるため、発信者 ID の完全一致設定を使用することを推奨します。

Intelligent Session Control 機能を有効にする場合は、再ルーティング機能の実行時の、会社の回線およびリモート接続先回線の動作を理解することも重要です。コールの再ルーティングでは、Do Not Disturb（DND）、Access Lists と Time of Day コール フィルタリング、および Delay Before Ringing Timer の各リモート接続先回線設定は無視されます。再ルーティングされるすべてのコールは、フィルタリングされずにすぐにルーティングされます。会社のデスクトップフォン回線設定も、デフォルトで無視されるか、またはバイパスされます。ただし、Ignore Call Forward All on Enterprise DN サービス パラメータを False に設定することによって、再ルーティング機能の実行時に会社のデスクトップフォン回線の Call Forward All 設定を有効にできます。このパラメータが False に設定されている場合、会社のデスクトップフォン回線に Call Forward All の接続先が設定されていると、再ルーティングの実行時にコールはリモート接続先にルーティングされません。代わりに、コールは Call Forward All の接続先にルーティングされます。デフォルトで、このサービス パラメータは True に設定されており、会社のデスクトップフォン回線の Call Forward All 設定は無視されます。

Intelligent Session Control 機能は、すべてのシェアド ライン呼び出し機能を使用することによって、さらに強化できます。この機能は、すべてのシェアド ライン呼び出しサービス パラメータを True に設定することによって有効になります。デフォルトで、このサービス パラメータは True に設定されており、この機能は有効になっています。ただし、すべてのシェアド ライン呼び出し機能は Intelligent Session Control 機能に依存しており、この機能も、すべてのシェアド ライン呼び出し機能を使用するときに順番に有効にする必要があります。すべてのシェアド ライン呼び出し機能、Intelligent Session Control 機能の両方を有効にすると、システムが内部で発信されたコールをダイヤル対象リモート接続先に PSTN でルーティングさせるだけでなく、ユーザの他のシェアド ライン デバイスもすべて、コールを受信します。これには、ユーザの会社のデスクフォンおよび他の設定済みリモート接続先が含まれます。呼び出されたユーザは、デバイス上で着信コールに応答でき、コールは会社にアンカーされます。

（注）　すべてのシェアド ライン呼び出しが有効であるときに、モバイル クライアント デバイスは、デバイスが Unified CM に登録されている場合にはデバイスの携帯電話音声インターフェイスでコールを受信しません。

発信者 ID 変換

設定済みのリモート接続先番号によってクラスタに発信されたコールは、自動的に、発信者 ID または発番号が、発信元のリモート接続先電話機の番号から関連する会社のデスクトップフォンの番号に変更されます。たとえば、408 555-7890 という番号のリモート接続先電話機が設定され、555-1234 という番号の会社のデスクトップフォンに関連付けられている場合は、クラスタ内の任意の電話番号に向けられたユーザのリモート接続先電話機からのコールがすべて、自動的に、発信者 ID が 408 555-7890 のリモート接続先電話番号から 555-1234 の会社の電話番号に変更されます。これによって、アクティブ コールの発信者 ID 表示とコール履歴ログの発信者 ID に、ユーザの携帯電話の番号ではなく、会社の卓上電話の番号が反映され、すべての返信コールがユーザの会社の電話番号に対して発信され、このようなコールが会社に固定されることが保証されます。

同様に、リモート接続先電話機から外部の PSTN 接続先へのコールと、モバイル ボイス アクセスやエンタープライズ機能アクセス 2 段階ダイヤリング経由で会社にアンカーされたコール、つまり、シングル ナンバー リーチの結果として PSTN に分岐されたコールも、発信者 ID が発信元のリモート接続先電話機の番号から関連する会社の電話番号に変更されます。

最後に、発番号を会社の電話番号ではなく、会社の DID 番号として外部の PSTN 電話機に供給する場合は、発信側のトランスフォーメーション パターンを使用できます。発信側のトランスフォーメーション パターンを使用して発信者 ID を会社の電話番号から会社の DID に変換することによって、外部の接続先からの返信コールは、完全な会社の DID 番号でダイヤルされていることから、その会社に固定されます。このような変換とダイヤル プランの意味については、Cisco Unified Mobility 固有の考慮事項（14-92 ページ）を参照してください。

モバイル ボイスと Unified Mobility の間の相互作用のインテリジェント プロキシミティ

Cisco DX シリーズ エンドポイントと Cisco IP Phone 8851 および 8861 でのモバイル ボイス機能のインテリジェント プロキシミティには、Unified Mobility 機能セット（シングル ナンバー リーチ（SNR）、リモート接続先およびデスク フォンのピックアップ、エンタープライズ 2 段階ダイヤリング、およびモバイル ボイスメールの回避を含む）との互換性があります。DX シリーズ エンドポイントと IP Phones 8851 および 8861 でのモバイル ボイスと Bluetooth ペアリングのインテリジェント プロキシミティの詳細については、インテリジェント プロキシミティ（8-15 ページ）を参照してください。

Unified Mobility に関するガイドラインと制約事項

（注）　Cisco Unified Mobility ソリューションは、シスコ機器でのみ検証されています。このソリューションは他のサードパーティ製 PSTN ゲートウェイおよびセッション ボーダー コントローラ（SBC）でも機能しますが、Cisco Mobility のそれぞれの機能が期待通りに機能する保証はありません。サードパーティ製 PSTN ゲートウェイまたは SBC でこのソリューションを使用している場合、シスコ テクニカル サポートが発生した問題を解決できない可能性があります。

次のガイドラインと制約事項は、Unified CM テレフォニー環境内のシングル ナンバー リーチの配置と動作に関連して適用されます。

- シングル ナンバー リーチは、PRI TDM PSTN 接続だけでサポートされます。T1 接続または E1-CAS、FXO、FXS、および BRI PSTN 接続はサポートされません。この PRI 要件は、完全な機能サポートを保証するためには、Cisco Unified CM で PSTN からの迅速な応答と切断の指示を受信する必要があることに基づいています。応答指示は、シングル ナンバー リーチ コールが特定のリモート接続先で応答されたときに、Cisco Unified CM でデスク フォンとその他のリモート接続先の呼び出しを停止するために必要です。加えて、応答指示は、シングル企業ボイスメール ボックス機能をサポートするために必要です。最後に、切断指示はデスクトップフォンピックアップのために必要です。PRI PSTN 接続では、必ず、応答指示または切断指示が提供されます。
- シングル ナンバー リーチは、SIP トランク VoIP PSTN 接続でもサポートされます。Unified CM SIP トランクとサービス プロバイダー トランクの間の責任分界点として、Cisco IOS Unified Border Element の使用が推奨されます。VoIP ベースの PSTN 接続では、VoIP ベースの PSTN 接続によって提供されるエンドツーエンドのシグナリング パスによって、Unified CM に迅速な応答と切断の指示を提供できます。
- シングル ナンバー リーチでは、ユーザあたり最大 2 つの同時コールをサポートできます。それ以上の着信コールは、自動的に、ユーザのボイスメールに転送されます。

- シングル ナンバー リーチは、Multilevel Precedence and Preemption（MLPP）と連動しません。コールが MLPP によって割り込まれた場合は、そのコールに対するシングル ナンバー リーチ機能が無効になります。
- シングル ナンバー リーチ サービスでは、ビデオ コールに応答できません。デスクトップ フォンで受信されたビデオ コールは携帯電話でピックアップできません。
- リモート接続先は、別のクラスタまたはシステム上の時分割多重（TDM）装置またはオフシステム IP 電話にする必要があります。IP 電話は、リモート接続先と同じ Unified CM クラスタ内に設定できません。
- モバイル ボイス アクセスの VoiceXML 機能は、Cisco IOS XE ソフトウェアではサポートされていません。Cisco IOS XE はネイティブ VoiceXML をサポートしていないため、Cisco 4000 シリーズ ISR をモバイル ボイス アクセスの VoiceXML ゲートウェイとして使用することはできません。代わりに、VoiceXML 機能を提供するために別個の H.323 Cisco IOS ゲートウェイを導入し、ヘアピニング対応のモバイル ボイス アクセスを設定してください。

ガイドラインと制約事項の詳細については、次の Web サイトで入手可能な『*Feature Configuration Guide for Cisco Unified Communications Manager*』の最新版で Cisco Unified Mobility に関する情報を参照してください。

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

Cisco Unified Mobility のキャパシティ プランニング

Cisco Unified Mobility は、Unified CM クラスタあたり最大 40,000 のリモート接続先またはモビリティ ID をサポートします。モビリティ対応ユーザの最大数は、ユーザあたり 1 つのリモート接続先またはモビリティ ID を想定すると、40,000 人のユーザになります。ユーザあたりのリモート接続先数またはモビリティ ID 数が増加するほど、サポートされるモビリティ対応ユーザ数が減少します。

（注）　モビリティ対応ユーザは、リモート接続先プロファイルを持ち、1 つ以上のリモート接続先またはモバイル クライアント デバイスおよびモビリティ ID が設定されているユーザとして定義されます。

（注）　モビリティ ID は、システム内でリモート接続先と同様に設定され、リモート接続先と同じ容量になります。ただし、リモート接続先と違って、モビリティ ID は、リモート接続先プロファイルではなく、直接電話機に関連付けられます。モビリティ ID は、Cisco Jabber を実行するデュアル モード モバイル クライアント デバイスだけに適用されます。

Cisco Unified Mobility の拡張性と性能は、モビリティ ユーザ数、ユーザごとのリモート接続先数またはモビリティ ID 数、およびそれらのユーザの最繁時呼数（BHCA）レートに依存します。ユーザあたりの複数のリモート接続先またはユーザあたりの高い BHCA によって、Cisco Unified Mobility の容量が減少することがあります。Unified CM サーバ ノードのキャパシティ、およびハードウェア固有のノードあたりとクラスタあたりのキャパシティを含む Cisco Unified Mobility のサイジングの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

Cisco Unified Mobility の設計上の考慮事項

Unified Mobility を配置する場合は、次の設計上の推奨事項に従ってください。

- PSTN ゲートウェイ プロトコルで、アウトオブバンド DTMF リレーが使用できる、または、インバンド DTMF をアウトオブバンド DTMF に変換するためのメディア ターミネーション ポイント（MTP）が割り当てられていることを確認します。PSTN 接続用の Cisco IOS ゲートウェイを使用している場合は、アウトオブバンド DTMF リレーがサポートされます。ただし、サードパーティ製ゲートウェイでは、一般的なアウトオブバンド DTMF 方式がサポートされない可能性があるため、結果として、MTP が必要になる場合があります。エンタープライズ機能アクセス 2 ステージ ダイヤリング機能と通話切替機能を使用するには、Cisco Unified CM で DTMF 番号をアウトオブバンドで受信する必要があります。

  （注）　インバンド DTMF をアウトオブバンド DTMF に変換するために MTP 上でリレーする場合は、十分な MTP 容量が提供されることを確認してください。エンタープライズ機能アクセス 2 ステージ ダイヤリングまたは通話切替機能の高い使用頻度が予想される場合は、ハードウェア ベースの MTP または Cisco IOS ソフトウェア ベースの MTP を推奨します。

- Unified Mobility を配置する前に、PSTN プロバイダーと連携して次のことを保証する必要があります。
  - 会社へのすべての着信コールに関する発信者 ID が、サービス プロバイダーから供給される。これは、エンタープライズ機能アクセス 2 ステージ ダイヤリングまたは通話切替転送、会議、およびダイレクト コール パーク機能が必要な場合の要件です。
  - 発信コールの発信者 ID は、サービス プロバイダーに制限されない。これは、モビリティ対応ユーザが、一般的な会社のシステム番号やその他の意味のない発信者 ID ではなく、リモート接続先にいる元の発信者の発信者 ID を受信することが期待される場合の要件です。

    （注）　プロバイダーによっては、トランク上の発信コールの発信者 ID が、そのトランクで処理される DID に制限される場合があります。そのため、発信者 ID が制限されない別の PRI トランクをプロバイダーから入手する必要があります。無制限の PRI トランクを要求すると、プロバイダーによっては、このトランク経由で緊急電話番号にコールを送信または発信しないことが記された署名付きの同意書を要求される場合があります。

    （注）　プロバイダーによっては、[Redirected Dialed Number Identification Service (RDNIS)] フィールドまたは SIP の Diversion ヘッダーにトランクで処理される DID が含まれている限り、そのトランクには発信コールの発信者 ID を無制限で許可します。ゲートウェイまたはトランクの設定ページで [Redirecting Number IE Delivery] > [Outbound] チェックボックスをオンにすることによって、リモート接続先に分岐されたコールの RDNIS または SIP の Diversion ヘッダーにユーザの企業番号を取り入れることができます。RDNIS または SIP の Diversion ヘッダーに対応し、発信コールの発信者 ID を無制限で許可しているかどうかは、サービス プロバイダーに問い合わせてください。

- 一般に、モビリティ コール フローには複数の PSTN コール レッグが含まれるため、Unified Mobility にとって PSTN ゲートウェイ リソースの計画と配置が極めて重要です。モビリティ対応ユーザ数が多い場合は、PSTN ゲートウェイ リソースを増やす必要があります。PSTN 利用を制限または削減するために、次の方法が推奨されています。
  - モビリティ対応ユーザあたりのリモート接続先数を 1 つに制限します。これによって、着信コールをユーザのリモート接続先に転送するために必要な DS0 数が削減されます。コールがユーザの会社の電話番号に送られると、そのコールがリモート接続先のいずれかで応答されなくても、設定済みのリモート接続先ごとに 1 つずつの DS0 が消費されます。コールがリモート接続先で応答されなくても、リモート接続先あたり 1 つの DS0 が 10 秒間も使用される可能性があります。
  - アクセス リストを使用して、着信コールの発信者 ID に基づいて、特定のリモート接続先へのコールの拡張を拒否または制限します。時刻に基づいてアクセス リストを呼び出すことができるため、エンド ユーザまたは管理者がアクセス リストを頻繁に更新する必要がありません。
  - 会社の番号に電話がかかってきたときに DS0 が使用されないよう、不要になったシングル ナンバー リーチを無効にするようエンド ユーザに伝えてください。シングル ナンバー リーチが無効になっている場合は、着信コールでデスク フォンの呼出音が鳴りますが、誰も電話に出なければ、そのコールが会社のボイスメールに転送されます。
- ロケーション間の WAN 帯域幅の不足によってコール アドミッション制御が拒否される可能性と、デスク フォンのピックアップまたはリモート接続先のピックアップによって WAN 帯域幅のオーバーサブスクリプションが発生する可能性があるため、リモート接続先プロファイル CSS と CSS の再ルーティングを設定して、CSS 内のルート パターンが、着信コール レッグが到達するゲートウェイと同じコール アドミッション制御ロケーション内に配置されたゲートウェイを指すようにすることを推奨します。詳細については、リモート接続先プロファイルの設定（21-73 ページ）を参照してください。
- 公衆網にアクセスするために公衆網振り分け用数字をダイヤルする必要がある配置において Intelligent Session Control 機能を有効にする場合は、[リモート接続先との発信者 ID の一致（Matching Caller ID with Remote Destination）] サービス パラメータを [部分一致（Partial Match）] に設定し、適切な桁数（[発信者 ID の部分一致の桁数（Number of Digits for Caller ID Partial Match）] サービス パラメータ）を設定して、設定されたリモート接続先またはモビリティ ID の部分一致が実行されるようにすることを推奨します。これにより、Intelligent Session Control 機能、およびモビリティの発信者 ID の自動照合機能とアンカリング機能が適切に機能するようになります。

シスコのモバイル クライアントおよびデバイス

モバイル ユーザ、携帯電話、携帯通信事業者サービスが普及するにつれて、単一のデバイスを使用して社内および社外の両方で音声、ビデオ、およびデータ サービスを使用できることがますます魅力的なソリューションとなっています。デュアル モード スマート フォン、およびそのスマート フォンで実行されるクライアントなどのモバイル デバイスは、企業に対して、カスタマイズされた音声、ビデオ、およびデータ サービスを社内にいながらユーザに提供する機能、および一般的な音声およびデータ サービスの代替の接続方法としてモバイル通信事業者ネットワークを利用する機能を利用可能にします。社内で音声、ビデオ、およびデータ サービスを利用可能にし、モバイル クライアント サービスに対してネットワーク接続を提供することによって、企業はこれらのサービスをローカルまたはリモートでより安価な接続コストで提供できます。たとえば、企業ネットワーク上で発信される Voice over IP（VoIP）コールは、通常、モバイル ボイス ネットワーク上で発信される同じコールよりもコストが少なく済みます。

Voice and Video over IP（VVoIP）機能に加えて、これらのモバイル クライアントとデバイスによって、モバイル ユーザは他のバック エンドのコラボレーション アプリケーションとサービスにアクセスできます。シスコのモバイル クライアントとサービスを通じて利用可能なサービスおよびアプリケーションには、会社のディレクトリ、会社のボイス メール、および XMPP ベースの IM（インスタント メッセージング）とプレゼンスが含まれます。さらに、ユーザがシングル ナンバー リーチ、モバイル ボイス アクセスまたはエンタープライズ機能アクセスを介したエンタープライズ 2 段階ダイヤリング、および 1 つの企業ボイスメール ボックスなどのモバイル デバイスで追加機能を利用できるように、これらのクライアントおよびデバイスは Cisco Unified Mobility とともに配置できます。

この項では、モバイル クライアントのアーキテクチャについて説明します。また、企業の WLAN ネットワークとモバイル ボイス ネットワークとの間でアクティブなボイスコールを移動する場合のリモート セキュア接続およびハンドオフに関する考慮事項を含む、シスコのモバイル クライアントとデバイスによって提供される共通の機能について説明します。一般的なモバイル クライアント ソリューション アーキテクチャおよび機能について説明した後、ここでは、次の特定のモバイル クライアントとデバイスのさまざまな機能および統合に関する考慮事項について説明します。

- Cisco Jabber：Android および iPhone や iPad などの Apple iOS モバイル デバイスに使用できるモバイル クライアントです。企業の WLAN ネットワークの IP 経由、またはモバイル データ ネットワーク経由で音声またはビデオ コールを発信する機能、ならびに社内ディレクトリと企業ボイスメール サービス、および XMPP ベースの企業向け IM およびプレゼンスにアクセスする機能を提供します。
- Cisco Spark：Android および iPhone や iPad などの Apple iOS デバイスに使用できるモバイル クライアントです。IP 経由の音声コールやビデオ コール、セキュアなパーシステント メッセージング、およびファイル共有を可能にする、1 対 1 および 1 対多のクラウド ベースのコラボレーション ルームを提供します。
- Cisco WebEx Meetings：Android、BlackBerry、Windows Mobile、および iPhone や iPad などの Apple iOS デバイスに使用できるモバイル クライアントです。ユーザが移動中に Cisco WebEx 会議に出席、参加する機能を提供します。
- Cisco AnyConnect Mobile：Android および Apple iOS デバイスで使用可能なモバイル クライアントであり、ユーザが企業外にいる場合でも、オンプレミス コラボレーション アプリケーションおよびサービスへのアクセスに対して、企業が安全にリモート VPN から接続できるようにします。

また、シスコのモバイル クライアントとデバイスのハイ アベイラビリティおよびキャパシティ プランニングの考慮事項についても説明します。

シスコのモバイル クライアントおよびデバイスのアーキテクチャ

シスコのモバイル クライアントは、IP ベースのネットワーク接続機能（IEEE 802.11 無線ローカル エリア ネットワークまたはモバイル プロバイダーのデータ ネットワーク）およびデュアル モード電話機だけを備えたタブレットおよびハンドヘルド デバイスなどのさまざまなモバイル デバイスで配置されます。デバイスが従来のセルラーまたはモバイル ネットワーク テクノロジーによってモバイル ボイス ネットワークとデータ キャリア ネットワークの両方に接続でき、また、802.11 を使用してワイヤレス ローカルエリア ネットワーク（WLAN）に接続できる 2 つの物理インターフェイスが含まれます。シスコのモバイル クライアントとデバイスは、802.11 WLAN 経由でのオンプレミス データおよびリアルタイム トラフィック（音声およびビデオ）接続を可能にします。また、これらのクライアントおよびデバイスは、パブリックまたはプライベートの WLAN 経由、またはモバイル データ ネットワーク経由で企業へのリモート データおよびリアルタイム トラフィック（音声およびビデオ）接続を提供します。プロバイダーの携帯電話音声の無線を備えたデバイスでは、音声接続がモバイル ボイス ネットワークおよび PSTN 経由で有効にされることもあります。

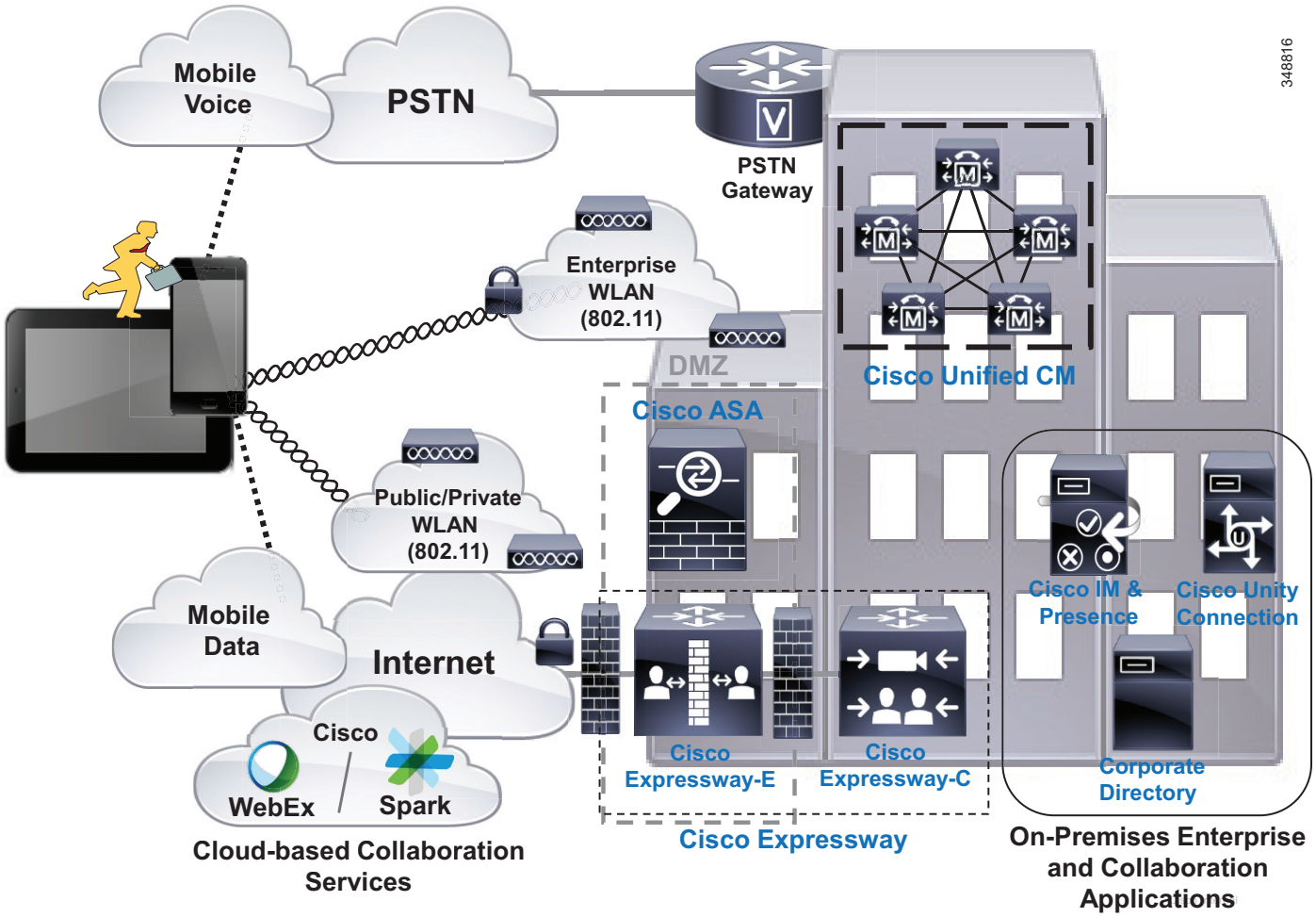
(注)　この項で*デュアルモード電話機*という用語を使用する場合、802.11 に準拠した無線機、および音声とデータの通信事業者ネットワークへの接続用の携帯電話無線機を備えたデバイスを指します。Digital Enhanced Cordless Telecommunications（DECT）やその他の規格に準拠した無線機、または複数の携帯電話無線機を備えたデュアルモード デバイスは、この項のデュアルモード電話機には含まれません。

図 21-27 は、Cisco Collaboration 展開にモバイル クライアント デバイスを接続して有効にするための、基本的なシスコのモバイル クライアントおよびデバイスのソリューション アーキテクチャを示します。音声サービスとビデオ サービスの場合は、モバイル クライアント デバイスが企業の WLAN に関連付けられるか、インターネットに（パブリックまたはプライベートから WLAN ホット スポットまたはモバイル データ ネットワークから）接続され、シスコのモバイル クライアントは、Session Initiation Protocol（SIP）を使用して会社の電話機として Cisco Unified CM に登録されます。登録されると、クライアント デバイスは、基礎となる企業の Cisco IP テレフォニー ネットワークを利用して、コールを発信および受信します。モバイル デバイスが企業ネットワークに接続されており、かつクライアントが Unified CM に登録されている場合、そのデバイスはユーザが持つ会社の電話番号を使用して発着することができます。ユーザの会社の電話番号に着信コールがあると、モバイル クライアント デバイスの呼出音が鳴ります。ユーザが Cisco IP デスク フォンを持っている場合は、モバイル クライアントを登録すると、ユーザの会社の番号でシェア ド回線インスタンスが使用可能になり、コールが着信すると、ユーザのデスク フォンとモバイル デバイスの両方の呼出音が鳴ります。モバイル クライアント デバイスが登録されておらず、かつ条件を満たしていない場合（携帯電話網へ接続している、ユーザに対して Cisco Unified Mobility が有効になっている、ユーザの携帯電話番号に対してシングル ナンバー リーチが有効になっている）、そのモバイル クライアント デバイスは会社の番号への着信コールを受け取りません。このようなシナリオではモバイル ボイス ネットワークおよび PSTN は音声のみのコールの発信および受信に使用されます。

シングル ナンバー リーチなどの Unified Mobility 機能は、携帯電話音声の無線を持たないタブレットや他のモバイル クライアント デバイスと互換性がありません。その理由は、これらの非デュアル モードのデバイスはネイティブ PSTN の到達可能番号を持たないためです。非デュアル モードのデバイスは、企業に接続してエンタープライズ呼制御システムに登録される場合だけ、エンタープライズ コールを発信および受信できます。

図 21-27 に示すように、シスコのモバイル クライアントとデバイスは、企業に接続されると、社内ディレクトリ、Cisco Unity Connection 企業ボイス メール システム、およびメッセージングやプレゼンスなどの追加エンタープライズ コラボレーション サービスにアクセスするための Cisco IM and Presence サービスなどの他のバック エンド アプリケーション サーバと直接通信することもできます。シスコのモバイル クライアントとデバイスは、IM and Presence と Web Conferencing サービスを提供する Cisco WebEx などのクラウドベースのコラボレーション サービスとも統合します。

図 21-27　シスコのモバイル クライアントおよびデバイスのアーキテクチャ



(注)　コールの音声とビデオの品質は、Wi-Fi またはモバイル データ ネットワーク接続によって異なります。Cisco Technical Assistance Center（TAC）は、3G/4G モバイル データ ネットワークまたは非社内 Wi-Fi ネットワーク経由で接続または音声およびビデオ品質の問題を解決できません。

モバイル ボイス ネットワークとモバイル データ ネットワーク、および WLAN ネットワークの両方に同時に接続するために、デュアルモードのモバイル クライアント デバイスでは、デュアル転送モード（DTM）がサポートされている必要があります。デバイスで DTM がサポートされていると、デバイスの携帯電話無線機と WLAN インターフェイスの両方からデバイスに到達可能になり、両方のインターフェイスでコールを発信および受信できます。モバイル ボイス ネットワークおよびモバイル データ ネットワークでデュアル接続デバイスがサポートされていない場合には、適切なモバイル クライアント操作が実行できない場合があります。

ワイヤレス LAN ネットワーク インフラストラクチャを介した音声およびビデオ

さまざまなモバイル クライアント デバイス機能、およびこれらの機能がエンタープライズ テレフォニー インフラストラクチャに与える影響について考慮する前に、適切に調整され、QoS に対応し、ハイ アベイラビリティを備えた WLAN ネットワークを計画して配置することが重要です。デュアルモード電話機および他のモバイル デバイスは、重要なシグナリング トラフィック、コールのセットアップやさまざまなアプリケーションへのアクセスのためのその他のトラフィック、およびリアルタイムの音声とビデオのメディア トラフィックにおいて、基礎となる WLAN インフラストラクチャを利用するため、データ トラフィックおよびリアルタイムのメディア トラフィックの両方に最適化された WLAN ネットワークの配置が必要になります。WLAN ネットワークの配置が適切でないと、多くの干渉が発生し、容量が低下するため、音声とビデオの品質が低下するだけでなく、コールがドロップされたり、つながらなかったりする可能性もあります。このように展開された WLAN は、コールの発信および受信に使用できなくなります。したがって、デュアル モード フォンと他のモバイル デバイスを配置する場合は、Voice and Video over WLAN の配置が正常に行われるように、配置前、配置中、配置後に WLAN 無線周波数（RF）サイト サーベイを実施して、適切なセル境界、設定、機能設定、容量、および冗長性を判断する必要があります。実稼働環境への配置の前に、WLAN の配置に対してモバイル デバイスのデバイス タイプまたはクライアントごとにテストを実施して、統合および動作が適切に行われるようにする必要があります。Quality of Service を含む WLAN サービス（Cisco Unified Wireless Network など）経由の最適なリアルタイム トラフィックが提供されるように配置および設定された WLAN を使用することによって、モバイル クライアント デバイスを正常に展開できます。

シスコでは、可能な場合は、音声およびビデオ トラフィックを生成できるモバイル クライアントとデバイスを接続するための 5 GHz 帯域 WLAN を利用することを推奨します（802.11a/n/ac）。5 GHz WLAN は、音声コールとビデオ コールに対し、スループットを改善して干渉を低減します。

Voice and Video over WLAN の配置およびワイヤレス デバイス ローミングの詳細については、ワイヤレス デバイス ローミング（21-6 ページ）を参照してください。

（注）　デュアルモード電話と他のモバイル クライアント デバイスは、インターネットを経由して会社に接続して呼制御やその他の Unified Communications サービスを利用できますが、シスコでは、このように接続した場合の音声とビデオの品質を保証できず、接続または音声とビデオの品質上の問題を解決できません。このような接続には、パブリックまたはプライベートの WLAN アクセス ポイント（AP）やホット スポット経由、あるいはモバイル データ ネットワーク経由の企業へのリモート接続があります。シスコでは、デュアル モード電話機およびその他のモバイル クライアント デバイスを接続するためのエンタープライズ クラスの音声およびビデオが最適化された WLAN ネットワークを推奨します。ほとんどのパブリックまたはプライベートの WLAN AP およびホット スポットは、データ アプリケーションおよびデバイスに合せて調整されています。この場合、AP 無線が最大電力に合わせて調整され、ダイナミック パワー コントロールにより、ネットワーク接続時にデバイスで最大電力が有効になり、クライアントの容量が大きくなります。このような調整方法は、パケットのドロップや損失時に再送信ができるデータ アプリケーションにとっては理想的ですが、パケットのドロップが大量に発生する可能性があるため、リアルタイム トラフィック アプリケーションでは音声とビデオの品質が非常に悪くなる可能性があります。同様に、モバイル プロバイダーのデータ ネットワークは、輻輳や接続のドロップの影響を受けやすいため、コール品質が低下したり、コールがドロップされる可能性があります。

クラウドまたはオフプレミスのコラボレーション インフラストラクチャ

シスコが提供する Cisco WebEx および Cisco Spark クラウド サービスは、企業構内にハードウェアを配置せずに利用することができます。すべてのサービス（音声、ビデオ、メッセージング、ファイルおよびコンテンツ共有、ミーティングおよびコラボレーション ルーム情報）は、インターネットまたはクラウドで安全にホストされます。これは、クライアントからのすべてのコンテンツ、音声とビデオのトラフィックがインターネットを通過し、Cisco Collaboration Cloud 内で混合され管理されていることを意味します。

Cisco Collaboration Cloud インフラストラクチャは、モバイル クライアントとデバイスに WebEx および Cisco Spark の以下の機能を提供します。

- WebEx ミーティング。コンテンツ共有機能を備えた Web 対応の音声およびビデオ会議を提供します。
- WebEx Messenger。XMPP IM and Presence、ポイントツーポイントの音声およびビデオ通話を提供します。
- Cisco Spark。ビデオ通話、メッセージング、ファイル共有機能を備えた 1 対 1 および 1 対多のコラボレーション ルームを提供します。

モバイル クライアントとデバイスの Quality of Service

シスコのモバイル クライアントのアプリケーションおよびデバイスは、シスコのコラボレーション QoS マーキング推奨事項に従って、一般にレイヤ 3 QoS パケット値をマークします。表 21-3 に、これらのマーキングを要約します。

表 21-3　シスコのモバイル クライアントのレイヤ 3 QoS マーキング

トラフィックのタイプ	レイヤ 3 マーキング	
	DSCP[1]	PHB[2]
音声メディア（音声のみ）	DSCP 46	PHB EF
ビデオ メディア（音声およびビデオ）	DSCP 34	PHB AF41
コール シグナリング	DSCP 24	PHB CS3

1. DiffServ コード ポイント
2. Per-hop behavior

シスコのモバイル クライアントのレイヤ 2 802.11 WLAN パケット マーキング（ユーザ プライオリティ、または UP）には、さまざまなモバイル プラットフォームおよびファームウェアの制約による課題があります。シスコのモバイル クライアントがさまざまなモバイル デバイスで実行されるため、レイヤ 2 ワイヤレス QoS が矛盾する場合があります。したがって、レイヤ 2 ワイヤレス QoS のマーキングを、WLAN のトラフィックを適切に処理するためには使用できません。

適切なモバイル クライアントのアプリケーション レイヤ 3 またはレイヤ 2 パケット マーキングにかかわらず、モバイル デバイスは、データおよびリアルタイム トラフィックの両方を含むさまざまなタイプのトラフィックの生成において、デスクトップ PC と同じさまざまな課題を示します。これを考えると、一般にモバイル デバイスはコラボレーション エンドポイントの信頼できないカテゴリに分類されます。モバイル クライアント デバイスが信頼されているエンドポイントとして見なされない配置では、ネットワークのプライオリティ キューイングと専用帯域幅が適切なトラフィックに適用されるようにするために、トラフィック タイプとポート番号に基づいてパケット マーキングまたは再マーキングすることが必要です。モバイル デバイスのトラフィックを再マーキングするだけでなく、ネットワーク ベースのポリシングとレート制限を使用してモバイル クライアント デバイスが大量のネットワーク帯域幅を消費しないようにすることを推奨します。

また、シスコのモバイル クライアントのレイヤ 3 マーキングが適切で、モバイル クライアント デバイスが信頼されているとすると、シスコのモバイル クライアントのトラフィックは、プライオリティの音声キューイングおよび専用ビデオ メディアとコール シグナリング帯域幅キューを使用して企業ネットワークを通過すると、適切にキューに入ります。

シスコのモバイル クライアントおよびデバイスの性能と機能

シスコのモバイル クライアントおよびデバイスは、さまざまな性能と機能が用意されます。機能や動作はデバイスによって異なりますが、この項に説明する共通の動作はすべての非クラウドベースのシスコ モバイル クライアントに適用されます。

エンタープライズ コール ルーティング

シスコのモバイル クライアントとデバイスが企業のテレフォニー インフラストラクチャおよび呼制御サービスを使用してコールを発信および受信できるため、モバイル クライアント デバイスに関係するコール ルーティングの性質と動作を理解することが重要です。

着信コール ルーティング

モバイル クライアントとデバイスが会社の電話番号を持つエンタープライズ デバイスとして Unified CM に登録すると、モバイル デバイスは、システムへの着信コールがユーザの会社の電話番号宛てである場合に呼出音が鳴ります。これは、PSTN または他の Unified CM クラスタや企業 IP テレフォニー システムから発信された着信コール、および同じ Unified CM 内の他のユーザから発信された着信コールにおける動作です。モバイル クライアント デバイスのユーザは、会社の電話番号に関連付けられている他のデバイスまたはクライアントを持っている場合には、これらのデバイスもシェアド ラインとして呼び出されます。コールがいずれかのデバイスまたはクライアントで応答されると、他のすべてのデバイスおよびクライアントの呼出音は停止します。

ユーザに対して Cisco Unified Mobility が有効になっており、ユーザのデュアルモード携帯電話の番号でシングル ナンバー リーチが有効になっているシナリオにおいては、着信コールはユーザの携帯電話の番号に対応するモビリティ ID に転送される場合があります。ただし、これは、モバイル デバイスが企業の WLAN ネットワークに接続されているか、セキュアな接続で企業ネットワークに接続され、Unified CM に登録されているかによって異なります。デバイスが企業ネットワークに直接接続されているか、セキュア リモート接続を介して接続されている場合には、携帯の番号でシングル ナンバー リーチが有効になっていても、ユーザの会社の電話番号への着信コールは、シングル ナンバー リーチによってモバイル デバイスのモビリティ ID に転送されません。Unified CM に登録されている場合にデュアルモード モバイル デバイスのモビリティ ID に会社の電話番号への着信コールが転送されない理由は、デバイスが企業ネットワークに接続され、利用可能であるということがシステムによって認識されるためです。したがって、企業の PSTN リソースの利用を少なくするために、Unified CM では、PSTN を経由してデュアルモード携帯電話のモバイル ボイス ネットワーク インターフェイスにコールを転送する処理は行われません。代わりに、会社の電話番号に対応する WLAN またはモバイル データ ネットワーク インターフェイスだけがコールを受信します。

（注） Dial Via Office が有効になっている場合（Dial Via Office（21-93 ページ）を参照してください）で、クライアントが登録されていても、Unified CM は着信コールを VoIP 経由で会社の電話番号に転送せず、シングル ナンバー リーチを使用してユーザの携帯電話番号に転送します。

モバイル デバイスが企業ネットワークに直接またはセキュア リモート接続を介して接続されていないか、Unified CM に登録されていない状況では、ユーザに対して Unified Mobility が有効になっており、そのモビリティ ID に対してシングル ナンバー リーチが有効である場合、会社の番号への着信コールが、設定済みのモビリティ ID ごとのデュアル モード携帯電話番号に転送されます。Unified Mobility でのモバイル クライアントおよびデバイスの統合の詳細については、Cisco Jabber と Cisco Unified Mobility との間の相互作用（21-116 ページ）を参照してください。

上記と同じ動作とロジックが、すべてのシェアド ライン呼び出し機能に当てはまります。この機能が有効である場合、デュアル モード モバイル クライアント デバイスが Unified CM に*登録されていない*場合に限り、コールはモビリティ ID または携帯電話番号に転送されます。すべてのシェアド ライン呼び出し機能の詳細については、Intelligent Session Control およびすべてのシェアド ライン呼び出し（21-75 ページ）を参照してください。

いずれの場合も、デュアル モード デバイスのモバイル ネットワーク電話番号に直接発信された着信コールは、プロバイダー ネットワークまたはデバイス設定がモバイル ネットワークによってデバイスに転送されないように設定されていないかぎり、常にモバイル ネットワークのデュアル モード デバイスのモバイル ボイス インターフェイスに直接ルーティングされます。このようなコールは、ユーザの会社の電話番号に対して発信されたコールではないため、適切な動作です。これらのコールは個人的なコールであると見なされるため、会社経由でルーティングされません。

（注） タブレット デバイスなどの携帯電話音声の無線のないモバイル クライアント デバイスは、デュアルモード デバイスではなく、モバイル ボイス ネットワーク インターフェイスでは到達できません。これらのデバイスは、Voice over IP によって会社の電話番号でのみ到達できます。

発信コール ルーティング

デュアルモード モバイル デバイスからの発信コールで使用されるインターフェイスは、ロケーション、およびその特定の時刻におけるデバイスの接続状況に応じて異なります。デュアルモード デバイスが企業に接続されず、Unified CM に登録されていない場合、コールは、通常どおりセルラー音声無線インターフェイスによってモバイル ボイス ネットワークにルーティングされます。ただし、企業に接続され、Unified CM に登録されている場合、モバイル デバイスはすべてのコールをエンタープライズ テレフォニー インフラストラクチャ経由で発信する必要があります。企業接続が使用できない場合、またはモバイル クライアントが登録されていない場合は、会社の番号からコールを発信することはできず、代わりにモバイル クライアント デバイスの携帯の番号を使用してモバイル ボイス ネットワーク経由でコールを発信する必要があります。または、Cisco Unified Mobility に装備されている 2 段階ダイヤリング機能を利用することもできます（モバイル ボイス アクセスとエンタープライズ機能アクセス（21-64 ページ）を参照）。

ダイヤル プラン

企業のダイヤル プランによって、モバイル クライアント デバイスが企業に接続され、Unified CM に登録されている場合のダイヤリング動作が決定されます。たとえば、企業のダイヤル プランの設定で、内部の内線番号に到達するために短縮ダイヤルの使用が許可されている場合、Unified CM に登録されているモバイル デバイスではこの短縮ダイヤルを利用できます。デュアルモードの携帯電話ユーザが発信コールにおいて社内で企業のダイヤリング手順、短縮ダイヤル、およびサイト ベースの番号または PSTN 振り分け用数字を使用してダイヤルできることは確かに便利ですが、携帯電話ユーザは、通常、携帯電話において、モバイル ボイス ネットワークで発信コールに対して要求される完全な E.164 ダイヤル ストリングを使用して発信コールの番号をダイヤルするため、これは若干不自然なダイヤリング方式となります。

企業におけるエンド ユーザ ダイヤリング エクスペリエンスは、最終的には企業のポリシーおよび企業のテレフォニー配置の管理者によって決定されます。ただし、デュアルモード モバイル デバイスでは、デバイスが企業ネットワークに接続されて Unified CM に登録されているかどうかにかかわらず、デュアルモード クライアント デバイスのダイヤリング手順が維持されるように、必要なダイヤル ストリングを正規化することを推奨します。モバイル ボイス ネットワークにおけるダイヤリングは、通常完全な +E.164（先頭に「+」が付きます）を使用して行われ、携帯電話の連絡先は通常完全な +E.164 番号で保存されるため、デュアルモード モバイル デバイスにおいては、企業のダイヤル プランは先頭に「+」を付けた完全な +E.164 番号を使用できるように設定することを推奨します。Unified CM 内で、デュアルモード電話のこのような発信ダイヤリングを処理するようにダイヤル プランが設定されている場合、ユーザは連絡先を +E.164 形式で 1 セットだけ電話機に保存するだけで済みます。これらの連絡先からダイヤルする場合や、完全な +E.164 番号を使用して手動でダイヤルする場合、デバイスが企業ネットワークに直接接続されているか、セキュア リモート接続を介して接続され Unified CM に登録されているか、またはモバイル ボイス ネットワークにだけ接続されているかにかかわらず、コールは常に適切な接続先にルーティングされます。このように企業のダイヤル プランを設定すると、ユーザのモバイル デバイスのダイヤリング手順が維持され、デバイスが企業に接続され Unified CM に登録されているかどうかを気にする必要がなくなるため、最善のエンド ユーザ ダイヤリング エクスペリエンスが提供されます。

デュアルモード電話から正規化されたダイヤリングを行うには、企業に接続されているか、またはモバイル ボイス ネットワークだけに接続されているかにかかわらず、次の点を考慮して Unified CM 内のダイヤル プランを設定します。

- 企業のダイヤル プランで、デュアルモード電話機からの、通常モバイル ボイス ネットワークで使用されるダイヤル ストリングを処理できるようにします。たとえば、ダイヤル プランでは、携帯電話からモバイル ボイス ネットワークを経由して特定の電話機に到達するためにダイヤルされる +1 408 555 1234 や 408 555 1234 などのストリングを処理できるように設定する必要があります。後者の 10 桁のダイヤル方式（たとえば、408 555 1234）をサポートすると、サイト内の短縮ダイヤルなどの他のダイヤリング手順と潜在的にオーバーラップする可能性があります。この場合、管理者は、どのオーバーラップしているダイヤリング手順（10 桁のダイヤルまたはサイト内の短縮ダイヤル）が企業ネットワークに登録されているデュアル モード電話機で使用できるようにする必要があるかを決定する必要があります。デュアル モード電話機でサポートされているダイヤリング手順のセットは、標準のエンドポイントでサポートされるダイヤリング手順のセットと異なることがよくあります。
- 会社の他の電話番号へのコールにおいては、短縮ダイヤルが設定されているシステムでは、ダイヤル ストリングを変更して、必要に応じて会社の内線番号に再ルーティングできる必要があります。たとえば、企業のダイヤル プランが 5 桁の内部ダイヤルに基づいているとすると、会社の内線番号へのコール ルーティングが処理されるようにシステムを設定して、デュアルモード デバイスが Unified CM に登録されているときにコールが発信された場合、+1 408 555 1234 や 408 555 1234 に発信されたコールが変更されて、51234 に再ルーティングされるようにする必要があります。
- 会社のデュアルモード デバイスへのすべての着信コールの発信番号または発信者 ID プレフィックスの先頭に適切な数字を付加して、不在コール、発信コール、および着信コールのコール履歴リストが完全な +E.164 形式となるようにします。これにより、デュアルモード デバイスのユーザは、ダイヤル ストリングを編集することなくコール履歴リストからダイヤルできます。ユーザは、企業に接続されているかどうかにかかわらず、コール履歴リストから番号を選択してリダイヤルできます。たとえば、社内の 51234 からデュアルモード ユーザの会社の電話番号にコールが発信され、そのコールに応答がない場合、発信番号を操作して、デュアルモード デバイスの履歴リストに 408 555 1234 または +1 408 555 1234 という形式のエントリが残るように Unified CM を設定する必要があります。この番号は、デュアル モード デバイスが、これ以上の処理の必要とすることなく、企業または単にモバイル ボイス ネットワークに接続されているかどうかダイヤルできます。

デュアルモード デバイスの正規化されたダイヤリングの例外の 1 つに、会社の内線番号または電話に内部からだけ到達可能なシナリオがあります(つまり、対応する外部から到達可能な DID 番号がない場合)。このような場合は、短縮形式を使用して、外部から到達できない番号をダイヤルできます(手動でダイヤルするか、または連絡先からダイヤルします)。これらの番号は外部では利用できず、社内からだけダイヤルできるため、連絡先リストにこれらの番号を保存する場合には、社内だけで使用できるという何らかのマークが必要となります。さらに、これらの内部専用番号からの着信コールの発信番号をコール履歴リストに保存する場合は、番号が変更されないようにする必要があります。これらの番号には、社内からだけ発信できるためです。すべてのコール履歴リストにおいて、これらの内線番号からのコールは番号を変更しないで保存する必要があります。このように変更しないで保存された番号、つまり短縮ダイヤル ストリングは、デバイスが企業に接続され Unified CM に登録されているときにだけ正常にダイヤルできます。

タブレットなどの携帯電話音声の無線がないモバイル クライアント デバイスは、企業接続および企業の音声とビデオ テレフォニーまたはクラウドベースのコラボレーション サービスだけに依存します。

緊急サービスおよびダイヤリングの考慮事項

モバイル クライアント デバイスから 911、999、112 などの緊急サービス番号に対してコールを発信する場合、事態は少々複雑になります。モバイル クライアント デバイスは社内または社外に位置する可能性があるため、緊急時におけるデバイスおよびユーザの位置の通知について考慮する必要があります。セルラー音声無線を備えたデュアルモード モバイル デバイスはプロバイダー ネットワークの位置サービスを利用しています。デバイスが接続され、通常は企業ワイヤレス ネットワークよりもはるかに正確に位置を特定できる場合は、これらの位置サービスは常に利用可能できます。そのため、デュアルモード デバイス ユーザは緊急コールを発信し、デバイスおよびユーザの位置を特定する場合には、モバイル ボイス ネットワークを利用することを推奨します。シスコのデュアルモード クライアント デバイスが緊急サービスおよび位置サービスにモバイル プロバイダーのボイス ネットワークのみを利用するよう、これらのクライアントは、モバイル クライアント デバイス設定ページの [緊急電話番号(Emergency Numbers)] フィールドに設定された番号に対するすべてのコールを強制的にモバイル ボイス ネットワーク経由でルーティングします。さらに、デュアルモード電話機のユーザに対して、すべての緊急コールを企業ネットワークではなくモバイル ボイス ネットワーク経由で発信するように指示します。

WLAN またはモバイル データ ネットワークを介した緊急コールを発信することは推奨されませんが、携帯電話音声の無線がないモバイル デバイスは、これらのデータ インターフェイスだけを経由して発信できます。携帯電話音声の無線がないモバイル デバイスは、緊急コール発信用に利用すべきではありません。

会社の発信者 ID

モバイル クライアント デバイスが企業に接続され、Unified CM に(モバイル データ ネットワークまたは WLAN 経由で)登録された場合、WLAN またはモバイル データ ネットワーク経由の企業回線で行われたすべてのコールは、発信者 ID としてユーザの会社の電話番号でルーティングされます。これにより、遠端でコール履歴リストから発信される返信コールはユーザの会社の電話番号に対して発信されることになり、常に会社経由でルーティングされます。デュアルモード モバイル デバイス ユーザに対して Cisco Unified Mobility が有効になっており、携帯電話の番号でシングル ナンバー リーチがオンになっている場合、デュアルモード デバイスが企業に接続されていないときには、会社の電話番号への返信コールも PSTN 経由でデュアルモード デバイスに転送されます。

通話切替機能

モバイル クライアント デバイスが企業に接続され、企業エンドポイントとして Unified CM に登録されている場合、Unified CM でサポートされている SIP コール シグナリング方式を使用して、保留、保留解除、転送、会議などの呼処理付加サービスを呼び出すことができます。Unified CM に登録された IP Phone やクライアントと同様に、これらのデバイスでは、保留音（MoH）、カンファレンス ブリッジ、メディア ターミネーション ポイント、トランスコーダなどの企業のメディア リソースを利用できます。

外部コール ルーティング

デュアル モード モバイル クライアント デバイスが企業に接続されている場合、または Unified CM に登録されていない場合は、モバイル ボイス ネットワーク経由だけでコールを発信および受信できます。このため、デュアルモード モバイル デバイスが登録されていない場合に発信または受信されるすべてのコールにおいて、Unified CM は関与しません。企業に接続されていないデュアルモード電話からコールが発信された場合、ネットワークに送信される発信者 ID は携帯の番号です。このため、応答されなかったコールへの返信コールは、会社経由でルーティングされるのではなく、デュアルモード デバイスの携帯の番号に直接発信されることになります。

デュアルモード モバイル クライアント デバイスが Cisco Unified Mobility と統合されている場合は、デュアルモード デバイスが社外にあり Unified CM に登録されていない場合でも、エンタープライズ 2 段階ダイヤリング サービスを利用して会社経由でコールを発信できます。Unified Mobility の 2 段階ダイヤリングは、モバイル ボイス アクセスまたはエンタープライズ機能アクセスを使用して実行され、ユーザはエンタープライズ システム アクセスの DID 番号をダイヤルし、クレデンシャルを入力してから発信番号をダイヤルする必要があります。Unified Mobility の 2 ステージ ダイヤリング機能の詳細については、モバイル ボイス アクセスとエンタープライズ機能アクセス（21-64 ページ）を参照してください。

同様に、デュアルモード電話機が Unified Mobility と統合されている場合、ユーザは、会社の電話番号への着信コールをシングル ナンバー リーチ経由で携帯の番号で受信したり、DTMF キー シーケンスを使用して保留、保留解除、転送、会議などの通話切替機能を呼び出したり、デスク フォンのピックアップを実行してアクティブなコールを携帯電話から会社のデスク フォンに移動したりできます。

リモート セキュア企業接続

モバイル クライアント デバイスは、Unified CM に対してクライアントを登録し、その他のコラボレーション アプリケーションやサービスにアクセスするために企業に安全な接続があるとすれば、企業に接続されていない場合でも IP コールや他のコラボレーション サービス経由でエンタープライズ音声およびビデオ用の IP テレフォニーのインフラストラクチャを利用できます。これらのデバイスに対するリモート セキュア接続は、インターネット経由のクライアント接続を保護するために Cisco AnyConnect モバイル クライアント VPN ソリューションまたは VPN なしの Cisco Expressway モバイルおよびリモート アクセス機能の使用が必要です。

リモート接続されたモバイル クライアント デバイスの音声およびビデオの品質とユーザ エクスペリエンスは、インターネット ベースのネットワーク接続の特性によって異なります。このようなクライアント接続タイプでは、シスコは音声とビデオの品質も正常接続も保証しません。このような接続を業務上重要な通信に使用する場合は、注意が必要です。信頼できない、または低帯域幅のインターネット接続を備えたデュアルモード デバイスの場合、デュアルモード デバイスのユーザは、接続が使用可能である場合、リモート企業テレフォニー インフラストラクチャに依存するのでなく、モバイル ボイス ネットワーク経由でコールを発信することが推奨されます。

追加のサービスおよび機能

呼処理サービスや呼制御サービスに加えて、シスコのモバイル クライアントとデバイスは、この項で説明する追加の機能およびサービスを提供できます。

デュアルモード コール ハンドオフ

デュアル モード デバイス配置の、1 つの非常に重要な側面は、ユーザが社内と社外の間を移動する、またはデバイスが企業ネットワークとの間で接続、切断するときに、ネットワーク接続が携帯電話音声の無線から WLAN 無線に切り替わり、また、その逆のことが起こるコール プリザベーションです。デュアルモード電話のユーザは多くの場合移動するため、デュアルモード ユーザが社内と社外の間を移動するときにアクティブなコールが維持されることが重要です。このため、デュアルモード クライアント デバイスおよび基礎となる企業のテレフォニー ネットワークでは、何らかの形式のコール ハンドオフが可能である必要があります。

デュアルモード クライアント、および基礎となる IP テレフォニー インフラストラクチャの両方でサポートされる必要がある 2 種類のコール ハンドオフがあります。

- ハンドアウト

  コール ハンドアウトとは、アクティブ コールをデュアルモード電話の WLAN またはモバイル データ ネットワーク インターフェイスからデュアルモード電話のセルラー音声インターフェイスに移動することを指します。このためには、コールが、会社の PSTN ゲートウェイ経由で、企業の IP ネットワークからモバイル ボイス ネットワークにハンドアウトされることが必要です。

- ハンドイン

  コール ハンドインとは、アクティブ コールをデュアルモード電話のセルラー音声インターフェイスからデュアルモード電話の WLAN またはモバイル データ ネットワーク インターフェイスに移動することを指します。このためには、コールが、会社の PSTN ゲートウェイ経由で、モバイル ボイス ネットワークから企業の IP ネットワークにハンドインされることが必要です。

デュアルモード電話機のハンドオフ動作は、デュアルモード クライアントの特性およびその特定の機能に依存しています。デュアル モード クライアントのハンドオフは、ユーザによって手動で呼び出したり、またはネットワーク条件に基づいて自動的に呼び出したりできます。手動ハンドオフのシナリオにおいては、デュアルモード ユーザは、各自のロケーションおよび必要性に基づいてハンドオフ動作を行い、完了する必要があります。自動ハンドオフにより、モバイル クライアントは WLAN 信号をモニタし、クライアントの WLAN 信号の強弱に基づいてハンドオフの決定を行います。弱い WLAN 信号の場合はハンドアウトが行われ、強い WLAN 信号の場合はハンドインが行われます。自動ハンドオフは、WLAN 信号の強度をモニタする機能を提供するモバイル デバイスに依存します。

ハンドオフ動作は、電話のコールにおいてエンタープライズ IP テレフォニー インフラストラクチャを最大限に活用するために重要となります。また、これらの動作は、音声の継続性と良好なユーザ エクスペリエンスを提供し、ユーザが元のコールをいったん切ってから再度コールを発信し直す必要がないようにするためにも必要です。

XMPP ベースの IM およびプレゼンス

一部のモバイル クライアントは、オンプレミスまたはオフプレミスのアプリケーション サーバまたはサービスとの統合によって、Extensible Messaging and Presence Protocol（XMPP）に基づいて企業インスタント メッセージング（IM）およびプレゼンス サービスを提供できます。いずれの場合も、これらのモバイル クライアントの IM およびプレゼンス機能は、次を有効化します。

- ユーザを連絡先リストまたはバディ リストに追加する。
- ユーザのプレゼンスおよび応答可能性のステータスを設定および伝達する。
- バディまたは連絡先のプレゼンス ステータスを受信する。
- インスタント メッセージング（IM）またはテキスト メッセージを作成し、送信する。
- IM またはテキスト メッセージを受信する。

IM and Presence はモバイル クライアントの必須機能ではありませんが、これによって、ユーザは自分のプレゼンス ステータスを連絡先に表示したり、連絡先のプレゼンス ステータスを表示したりできるため、生産性が向上します。また、ユーザは、モバイル ショート メッセージ サービス（SMS）メッセージのコストをかけずに、企業ベースの IM メッセージを送信できます。

社内ディレクトリ アクセス

モバイル クライアントとデバイスは、連絡先を検索するために企業ディレクトリにアクセスできます。次のいずれかを使用して、企業ディレクトリへのアクセスを有効にします。

- クライアントと互換性のある LDAP ディレクトリの間の通信用の Lightweight Directory Access Protocol（LDAP）
- クライアントと User Data Services（UDS）API 間の REST ベース（HTTPS）通信。この通信では、Unified CM クラスタのエンドユーザ データベース内に格納されるユーザの連絡先情報への認証済みアクセスを有効にする一連の操作が提供されます。

  連絡先の検索には、UDS-to-LDAP プロキシを使用することもできます。有効にしても、連絡先の検索は UDS によって処理されますが、モバイル クライアントに結果をリレーする UDS を使用して、社内 LDAP ディレクトリにプロキシされます。これにより、モバイル クライアントでは Unified CM 内でサポートされるユーザの数を上回る社内ディレクトリを検索することができます。

社内ディレクトリ アクセスはモバイル デバイスおよびクライアントに必須の機能ではありませんが、モバイル デバイスから社内ディレクトリ情報にアクセスできると、モバイル ユーザのユーザ エクスペリエンスが向上します。

企業ボイスメール サービス

多くのモバイル クライアントとデバイスも、企業ボイス メール サービスにアクセスできます。シスコのモバイル クライアントでは、ユーザの企業ボイスメール ボックスに未読のボイスメールが存在し、モバイル デバイスが企業ネットワークに接続されている場合に、企業のメッセージ待機インジケータを受信できます。さらに、モバイル クライアントを使用して、企業ボイスメール メッセージを取得することもできます。通常、企業ボイスメール メッセージは、ユーザがボイスメール システム番号にダイヤルし、必要なクレデンシャルを入力してから各自のボイスメール ボックスに移動して取得します。ただし、Cisco Jabber モバイル クライアントは、ボイスメール ボックス内のすべてのメッセージのリストをダウンロードおよび表示し、モバイル デバイスにダウンロードして再生する個別のメッセージを選択することによって、ボイスメール ボックスからボイスメール メッセージを取得する機能を備えています。この機能は、ビジュアル ボイスメールと呼ばれることもあります。モバイル クライアントおよび企業ボイスメール システムの両方において、ネットワーク経由でのメッセージ待機インジケータ（MWI）、ボイスメール メッセージ情報、およびメッセージのダウンロードの提供と受信が可能である必要があります。Cisco Unity Connection は、REST（HTTPS）を使用したビジュアル ボイスメールをサポートし、MWI、ボイス メール リスト、およびメッセージのダウンロードを提供します。

Dial Via Office

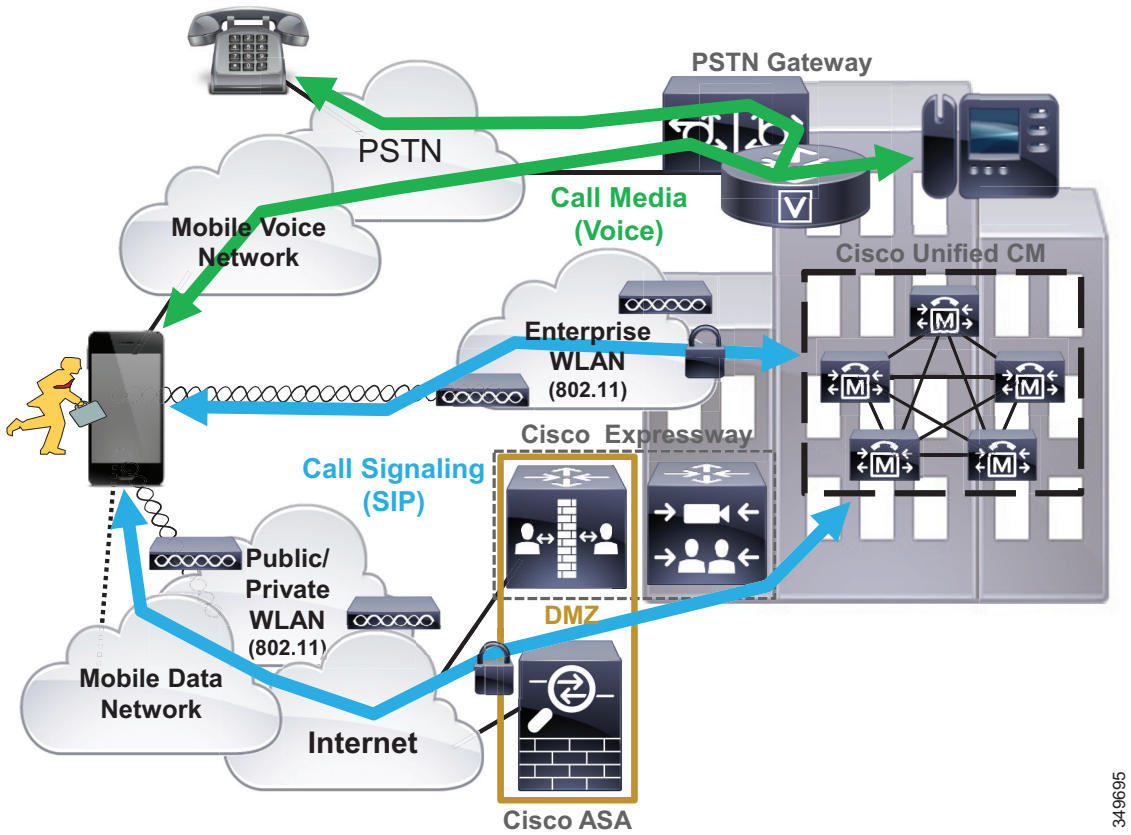
Dial Via Office（DVO）機能によって企業のダイヤリング機能が自動化され、デュアル モードのモバイル デバイスが企業テレフォニー インフラストラクチャ経由でコールを開始できるようになりました。DVO 通話を導入すると、企業に次の利点がもたらされます。

- 直接ダイヤルされた携帯電話コールと比較して、国際電話（おそらくは）長距離電話のコストを削減します。モバイル データ通過の場合は、モバイル データのコストも考慮する必要があることに注意してください。
- 社内番号に電話をかけることができます。DVO コールは会社の内線番号を使用して発信されるため、DID 以外または内部専用の会社の内線番号にも到達できます。

- 携帯電話番号のマスキング。DVO コールでは、システムは携帯電話番号ではなくユーザの社内番号を発信者 ID として送信します。
- 一元化された会社のコール詳細レコード（CDR）とコール ログ。DVO コールは企業テレフォニー インフラストラクチャから発信されるため、コールが PSTN およびモバイル ボイス ネットワークを通過する場合も、管理者はこれらのコールを完全に認識しています。
- 社内コール アンカリング。DVO コールは社内でアンカーされるため、ユーザは Cisco Unified Mobility DTMF ベースの通話切替機能、およびデスクトップフォンのピック アップを利用することができます。

Cisco Jabber クライアントを実行するデュアル モードのモバイル デバイスは、会社の内線番号を使用して電話をかける Unified CM テレフォニー インフラストラクチャと会社の PSTN ゲートウェイを使用して DVO コールを発信することができます。ただし、音声メディアが IP ネットワークを通過する Voice over IP（VoIP）とは異なり、この機能は、図 21-28 に示すように、クライアントと IP 接続（WLAN またはモバイル データ）経由の Unified CM 間の SIP シグナリングと、モバイル デバイス、モバイル ボイス ネットワーク、PSTN 間の音声メディアによって実現されます。

図 21-28　Cisco Dial Via Office のアーキテクチャ



（注）　DVO コールの場合、ユーザの携帯電話からのすべての音声またはメディアは、モバイル ボイス ネットワーク、PSTN、および会社の PSTN ゲートウェイを経由して常に移動します。メディアが会社へのデータ接続を通過することはありません。モバイル データ ネットワーク接続は、コール シグナリング トラフィックとその他のアプリケーションの相互作用以外には使用されません。

Cisco Jabber クライアント向け Dial via Office の詳細については、デュアルモード デバイス向けの Cisco Jabber Dial Via Office（21-104 ページ）を参照してください。

モバイル クライアント ユーザ用の設定の簡素化

シスコのモバイル クライアントは、モバイル クライアント デバイスで初回エンドユーザ クライアントの設定を単純化するための簡素化された設定方式を提供します。この設定方式は、社内 DNS サーバ内の RFC 2782 標準 Domain Name Service（DNS SRV レコード）に依存し、自動的にネットワークのコラボレーション サービスを検出します。DNS SRV レコードは、呼制御や IM およびプレゼンス サービス用の適切なアプリケーション サーバにモバイル クライアントを転送します。この設定とプロビジョニング方式は、ユーザが XMPP IM およびプレゼンス サーバや音声とビデオ呼制御サーバまたは TFTP サーバ ホスト名または IP アドレスを手動で設定する必要性を緩和します。代わりにユーザは単にユーザ ID とドメイン名を入力し、クライアント アプリケーションは自動的に利用可能なコラボレーション サービスを検出し、適切なクレデンシャルをユーザに要求するアプリケーションを使用してこれらのバック エンド サーバに接続します。サービスが検出されない場合、またはサービスの検出操作が失敗した場合、モバイル クライアント アプリケーションは、コラボレーション アプリケーション サーバのホスト名または IP アドレスおよびクレデンシャルを要求する手動の設定モードに戻ります。プライオリティおよび重み付けが表示された複数の DNS SRV レコードは、これらのサービスを提供する複数のサーバにバック エンドのコラボレーション アプリケーション サービスとモバイル クライアント分散のハイ アベイラビリティを確保します。

（注）　モバイル クライアント ユーザの簡素化された設定は、バック エンド アプリケーション サーバのクライアントとサービス設定とプロビジョニング関連する管理タスクを簡素化しません。社内 DNS サーバに DNS SRV レコードを作成することに加え、ユーザ アカウント、モバイル クライアント デバイス、およびサービス設定を追加するすべての管理作業が必要になります。

Cisco Bring Your Own Device（BYOD）インフラストラクチャ

Cisco Jabber などのシスコのモバイル クライアント アプリケーションは、Android や Apple iOS のスマートフォンやタブレットなどのモバイル デバイスのユーザへの、音声、ビデオ、およびインスタント メッセージングを含むコアの Unified Communications およびコラボレーション機能を提供します。シスコのモバイル クライアント デバイスが企業ワイヤレス LAN に接続されている場合、クライアントは Cisco Bring Your Own Device（BYOD）インフラストラクチャ内に配置できます。

シスコのモバイル クライアントとデバイスは、企業ワイヤレス LAN 接続、または VPN 経由のリモート セキュア接続または VPN なしの接続に依存しているため、Cisco Unified アクセス ネットワーク内に配置し、BYOD インフラストラクチャで配信される ID、セキュリティ、およびポリシー機能を利用することができます。

Cisco BYOD インフラストラクチャは、さまざまなデバイスの所有権とアクセス要件に対応するために、種々のアクセス使用例またはシナリオが用意されています。次のハイ レベルなアクセス使用例モデルを考慮する必要があります。

- 基本的なアクセス：この使用例は、ゲストのデバイスの基本的なインターネット アクセスだけを有効にします。この使用例では、企業リソースへのアクセスを提供せずに、従業員所有の個人用デバイスのネットワーク接続を可能にする機能を提供します。
- 制限付きアクセス：この使用例は、社内ネットワーク リソースへのフル アクセスを有効にしますが、企業所有デバイスだけに適用されます。
- 拡張アクセス：この使用例は、社内ポリシーに基づいて、企業所有デバイスと従業員所有の個人用デバイスの両方が社内ネットワーク リソースに対して高精度なアクセスを実現します。

シスコのコラボレーション モバイル クライアントは、企業のデバイスまたは個人のデバイスのいずれで動作しているかにかかわらず、通常は多数のバック エンドのオンプレミスの企業アプリケーション コンポーネントへのフル機能でのアクセスが必要です。このため、制限付きアクセスまたは拡張アクセスの使用例のシナリオは一般に、Cisco Jabber for Android or iPhone などのアプリケーションに適用されます。この 2 つのアクセス モデルの主な違いは、制限付きアクセスでは、企業所有デバイスに社内ネットワーク リソースへのフル アクセスが与えられている点です。拡張アクセスの場合は、従業員所有のデバイスにもフル アクセスが与えられるだけでなく、社内ネットワーク リソースへのアクセスが高精度で行われるため、このアクセス状態で実行されるデバイスとアプリ ケーションは、企業のセキュリティ ポリシーに基づいて特定のリソースだけにアクセスすることができます。

クラウドベースのコラボレーション サービスの場合は、シスコのモバイル クライアントおよびデバイスは、企業ネットワーク接続は不要で、インターネットを介してクラウドに直接接続します。これらの使用例がインターネット アクセスだけを必要とするため、これらのシナリオでは、ユーザおよびモバイル デバイスは、基本的なアクセス モデルを使用して配置できます。

Cisco BYOD インフラストラクチャの詳細と BYOD アクセスの使用例については、以下のリンク先に掲載されている BYOD 情報を参照してください。

https://www.cisco.com/c/en/us/solutions/byod-smart-solution/overview.html

Cisco BYOD インフラストラクチャ内にシスコのモバイル クライアントおよびデバイスを配置する場合は、次のハイレベルな設計と配置のガイドラインを考慮してください。

- ネットワーク管理者は、企業のテレフォニー インフラストラクチャの最大使用を保証するために、音声およびビデオ対応クライアントがバックグラウンドで企業ネットワークに（初期のプロビジョニングの後）、ユーザの介入なしで接続することを許可することを検討する必要があります。具体的には、証明書ベースの ID および認証を使用すると、ネットワーク接続および認証の遅延を最小化することによって優れたユーザ エクスペリエンスを容易にします。
- シスコのモバイル クライアントとデバイスがセキュア VPN または VPN なしの接続を介して企業ネットワークにリモート接続できるシナリオの場合：
  - ネットワーク管理者は、企業テレフォニー インフラストラクチャを最大限に活用するために、企業のセキュリティ ポリシーをユーザの介入のないシームレス セキュア接続の必要性に対して評価する必要があります。証明書ベースの認証を利用し、デバイスのピン ロック ポリシーを適用すると、エンド ユーザがデバイスを所有し、ネットワークにアクセスするためのピン ロックを知っている必要があるため、ユーザの介入および二要素認証のような機能なしでシームレスに接続することができます。二要素認証が必要な場合、デバイスを企業にリモート接続するには、ユーザの介入が必要となります。
  - インフラストラクチャのファイアウォール設定によって、必要なすべてのクライアント アプリケーションのネットワーク トラフィックが企業ネットワークにアクセスできることが重要です。適切なアクセス ソリューションを提供すること、または企業のファイアウォールで適切なポートやプロトコルへのアクセスを開くことに失敗すると、シスコのモバイル クライアントやデバイスを音声およびビデオ テレフォニー サービス用のオンプレミスの Cisco Call Control に登録できなくなったり、企業ディレクトリ アクセスや企業ビジュアル ボイスメールなどの他のクライアント機能を失ったりする可能性があります。

- Cisco Jabber などの企業のコラボレーション アプリケーションが従業員所有のモバイル デバイスにインストールされている場合は、特定の状況下においてデバイスをワイプするか、工場出荷時の設定にリセットすることが企業のセキュリティ ポリシーで定められている場合、デバイスの所有者にそのポリシーについて知らせ、デバイスから個人データを定期的にバックアップすることを奨励する必要があります。
- シスコのコラボレーション モバイル クライアントおよびデバイスを導入する場合、クライアント アプリケーションの音声とビデオ コールの品質、およびすべての機能の適切な動作を保証するために、エンドツーエンドの基盤となるネットワーク インフラストラクチャが、音声メディアと専用ビデオのプライオリティ キューイングやシグナリング帯域幅など必要な QoS クラスのサービスをサポートすることが重要です。

シスコのモバイル クライアントおよびデバイスの設計上の考慮事項

ここでは、次のシスコ モバイル クライアントおよびデバイスの設計上の考慮事項について説明します。

- Cisco Jabber for Android および Apple iOS（21-97 ページ）
- Cisco Spark（21-117 ページ）
- Cisco WebEx Meetings（21-118 ページ）
- Cisco AnyConnect モバイル クライアント（21-118 ページ）

Cisco Jabber for Android および Apple iOS

ここでは、Cisco Jabber の特性および配置上の考慮事項について説明します。

Cisco Jabber モバイル クライアントは、Android および iPad や iPhone などの Apple iOS に使用できます。適切なストアやマーケット（Apple の App Store や Google Play）からクライアント アプリケーションをダウンロードし、Apple iOS または Android デバイスにインストールすると、企業ネットワークに接続して SIP 対応の会社の電話機として Unified CM に登録できます。

Cisco Jabber モバイル クライアントに登録および呼制御サービスを提供するには、Unified CM 内でデバイスが **Cisco Dual Mode for Android** または **iPhone**、あるいは **Cisco Jabber for Tablet** デバイス タイプとして設定される必要があります。次に、企業の WLAN にアクセスして企業の WLAN インフラストラクチャおよびセキュリティ ポリシーに基づいて接続するよう、モバイル デバイスを設定する必要があります。または、モバイル データ ネットワークや非企業 WLAN 経由でモバイル デバイスを企業ネットワークに接続できます。企業ネットワークにアクセスするようにモバイル デバイスを設定すると、Cisco Jabber クライアントが起動したときに、デバイスが Unified CM に登録されます。Unified Mobility と統合し、ハンドオフ機能を利用するには、Android または iPhone スマートフォンの携帯番号を、Unified CM 内で Cisco Dual-Mode for Android または iPhone デバイスに関連付けられたモビリティ ID として設定する必要があります。

Cisco Jabber クライアントは、次のデバイスでサポートされます。

- Android

  Android フォンおよびタブレットのさまざまなモデル。（特定のデバイスおよびファームウェアのサポート情報については、次に参照されているリリース ノートを参照してください。）これらのデバイスで実行するファームウェア バージョンの最小要件は 4.1(2) となっていますが、最新バージョンの Android ファームウェアが必要になる場合もあります。ほとんどの Android デバイスの WLAN インターフェイスで、802.11a、802.11b、802.11g、802.11n および 802.11ac ネットワーク接続がサポートされています。

- Apple iOS

  iPhone、iPad などのさまざまな Apple iOS デバイス。(特定のデバイスおよびファームウェアのサポート情報については、次に参照されているリリース ノートを参照してください。)これらのデバイスでは、iOS バージョン 10.3 以降が実行されている必要があります。ほとんどの Apple iOS デバイスの WLAN インターフェイスでは、802.11a、802.11b、802.11g、および 802.11n ネットワーク接続がサポートされています。新しい一部の Apple デバイスでは、802.11ac がサポートされています。

最新の特定のデバイスおよびファームウェア バージョンの詳細については、次の製品リリース ノートを参照してください。

- Android

  https://www.cisco.com/c/en/us/support/unified-communications/jabber-android/products-release-notes-list.html

- iPhone および iPad

  https://www.cisco.com/c/en/us/support/customer-collaboration/jabber-iphone-ipad/products-release-notes-list.html

Cisco Jabber for Android、iPad、および iPhone クライアントは、音声および Voice-over-IP フォン サービスだけでなく、XMPP ベースの企業インスタント メッセージング(IM)およびプレセンスを提供し、さらに企業のコンタクト ソースにアクセスするよう設定された場合は企業の連絡先およびディレクトリ サービス、Cisco Unity Connection に統合された場合は企業ボイスメール メッセージ待機インジケータ(MWI)およびビジュアル ボイスメールも提供します。

スマートフォン(Android および iPhone)上の Cisco Jabber クライアントでは、Cisco Jabber デュアルモード ハンドオフ(21-101 ページ)の項に説明されているように、手動によるハンドアウトだけを実行できます。

Cisco Jabber Android および Apple iOS クライアント、追加の機能、およびサポートされているハードウェアとソフトウェアのバージョンの詳細については、次の Cisco Jabber マニュアルを参照してください。

- Android

  https://www.cisco.com/c/en/us/support/unified-communications/jabber-android/tsd-products-support-series-home.html

- iPhone および iPad

  https://www.cisco.com/c/en/us/support/customer-collaboration/jabber-iphone-ipad/tsd-products-support-series-home.html

Cisco Jabber サービス ディスカバリ

前述のように、Jabber などのシスコ モバイル クライアントは、DNS ルックアップや DNS SRV DNS サービス レコード解決に基づいて、使用可能なコラボレーション サービスを検出できます。サービス ディスカバリが適切に設定されている場合、ユーザがユーザ名とドメインだけを入力すると、使用可能なコラボレーション サービスをクライアントが自動的に検出して接続します。

図 21-29 に示されているように、クライアントの初期設定時、またはネットワーク接続の変更時に、Jabber は次の SRV レコードに関して DNS に照会することにより、コラボレーション サービスを検出します。

- _cisco_uds._tcp.<*domain*>

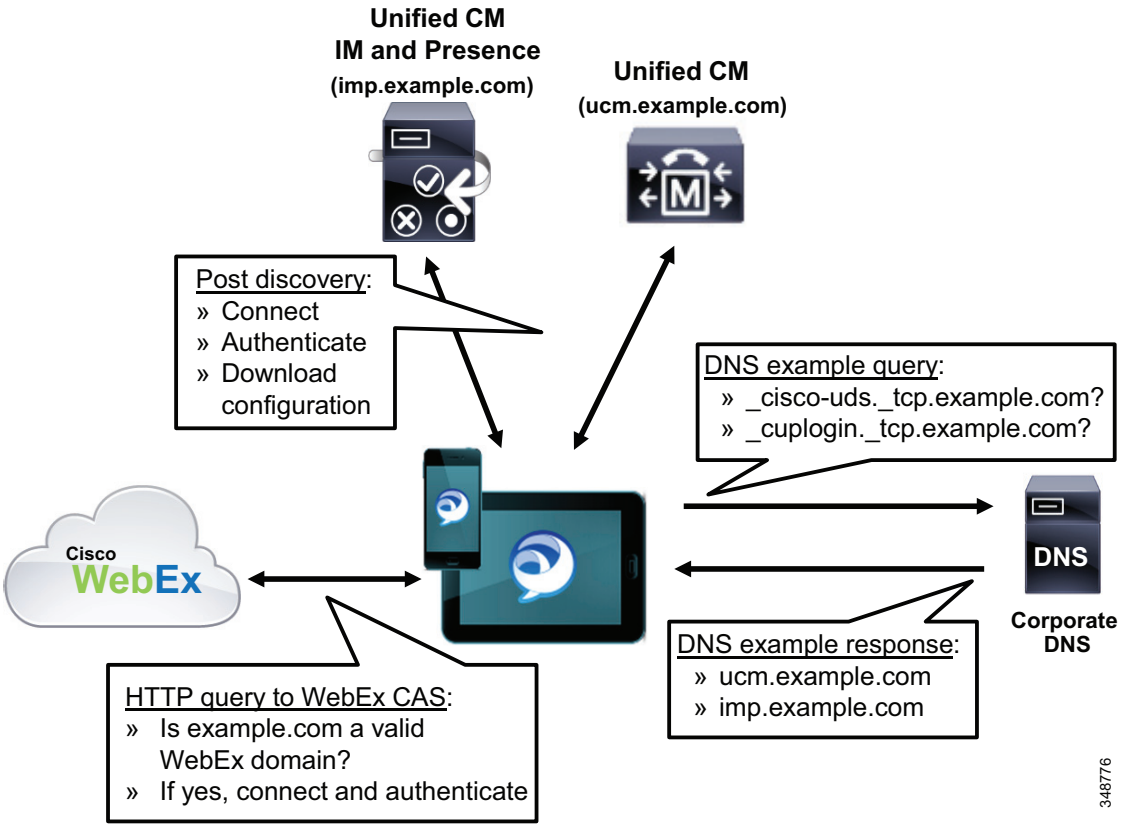
  Voice and Video over IP（VVoIP）通話を有効にする電話専用モード、または音声とビデオ通話および IM とプレゼンスを有効にするフル UC モードで Jabber が配置されると、このタイプの SRV レコードが企業 DNS サーバに追加されます。このレコードのクエリが DNS によって解決されると、Cisco Jabber は Unified CM に接続し、オーセンティケータを決定し、利用可能なサービスを特定します。

- _cuplogin._tcp.<*domain*>

  XMPP ベースの IM とプレゼンスを有効にする IM 専用モードで Jabber が配置されると、このタイプの SRV レコードが企業 DNS サーバに追加されます。このレコードのクエリが DNS によって解決されると、Cisco Jabber は Unified CM IM and Presence に接続し、認証します。

Cisco WebEx Messenger を使用したハイブリッド展開の場合、初期設定時およびネットワーク接続の変更時に、ドメインが有効な WebEx ドメインであるかどうかを判別するために、クライアントは Cisco WebEx Messenger サービスに関して Central Authentication Service（CAS）URL に向けて HTTP クエリも発行します。有効な WebEx ドメインが入力された HTTP クエリに対する肯定の確認をクライアントが受け取ると、クライアントは WebEx Messenger サービスに接続して認証し、Cisco WebEx Org Admin で設定された使用可能な UC サービスとクライアント設定に関する情報を取得します。

図 21-29　　Cisco Jabber サービス ディスカバリ



UDS サービスは Unified CM クラスタのすべてのノードで動作しますが、Unified CM UDS サービスの DNS SRV レコードを設定するとき、管理者は Unified CM サブスクライバ ノードにのみ解決するようレコードを設定する必要があります。これにより、UDS サービスとのクライアント対話でパブリッシャ ノードが回避され、代わりにクラスタ内の呼処理ノードに負荷が分散されます。

サービス ディスカバリが設定されていない展開、または DNS を信頼できない展開では、Jabber クライアントは手動設定に戻ります。その場合、ユーザはオーセンティケータとサービス ノードの IP アドレスを入力する必要があります。手動で設定された IP アドレスは、後続の接続で使用するために Jabber クライアントによってキャッシュされます。

サービス ディスカバリまたは手動設定が完了すると、Jabber は認証を行い、サービス プロファイルや jabber-config.xml ファイル（入手可能な場合）をダウンロードする必要があります。このファイルは、ボイスメールやディレクトリなどの追加のバックエンド アプリケーション サービスにクライアントを誘導し、適切な設定を有効にします。

Cisco Jabber 社内ディレクトリ アクセス

Cisco Jabber モバイル クライアントは、企業の連絡先情報にアクセスするためにさまざまな方法に依存します。ローカル デバイスの連絡先や、以前に Jabber バディ リストに追加された連絡先に加えて、Jabber モバイル クライアントは次の方法を使用して、社内ディレクトリ サービスにアクセスできます。

- Cisco ディレクトリ統合（CDI）

  CDI 方式の社内ディレクトリ アクセスは、Jabber クライアントとサポート対象の LDAP 対応ディレクトリ（Microsoft Active Directory、OpenLDAP など）の間の LDAP 通信に依存します。オンプレミス Jabber クライアントでは、CDI がディレクトリ統合のデフォルト方式となっています。

- Unified CM ユーザ データ サービス（UDS）

  社内ディレクトリ アクセスの UDS 方式は、Unified CM の各ノードで実行される Unified CM UDS サービスと Jabber クライアントとの間の HTTP 通信に依存します。

- Unified CM UDS-to-LDAP プロキシ

  社内ディレクトリ アクセスのこの方式は、ローカル ユーザ ディレクトリを使用する代わりに、社内 LDAP ディレクトリに対してディレクトリ検索を解決またはプロキシする Unified CM UDS サービスに依存します。UDS-to-LDAP プロキシにより、Jabber ユーザはローカル Unified CM クラスタ エンドユーザ データベースに制限されることなく、社内ディレクトリ全体に対して検索を実行できます。

Jabber クライアントのディレクトリ統合方法を設定するため、また Jabber クライアントのいくつかのディレクトリ関連設定を行うために、jabber-config.xml ファイルが使用されます。

オンプレミス クライアントには、CDI 方式のディレクトリ アクセスを使用することをお勧めします。

Expressway モバイルとリモート接続を使用してリモートで Jabber クライアントを接続する場合は、UDS 方式のディレクトリ アクセス（ローカル Unified CM データベースまたは UDS-to-LDAP プロキシ）のみがサポートされます。社内ディレクトリのサイズがローカル Unified CM ディレクトリのサイズを超過する場合（ユーザ数が 160,000 を超える場合）、モバイル クライアント ユーザがディレクトリ全体を検索できるよう、UDS-to-LDAP プロキシを有効にすることを検討してください。

Cisco Jabber デュアルモード ハンドオフ

Cisco Jabber などの Cisco デュアルモード クライアントを適切に配置するには、クライアント内部のハンドオフ動作の特性について理解することが重要です。Cisco Jabber デュアルモード クライアントによって使用されるハンドオフ方式は、Cisco Dual-Mode for iPhone または Cisco Dual-Mode for Android デバイスの設定ページの [モバイル ネットワークへ転送（Transfer to Mobile Network）] 設定に基づきます。

[Transfer to Mobile Network] の設定に応じて、ハンドオフには次の 2 つの方式があります。

- ハンドオフのモバイル ソフトキー方式（21-101 ページ）

  この方式では、[Transfer to Mobile Network] の設定を [Use Mobility Softkey (user receives call)] に設定する必要があります。このタイプのハンドオフでは、Unified CM システムは、PSTN を介してユーザのモバイル番号へのコールを発信します。

- ハンドオフ番号方式のハンドオフ（21-102 ページ）

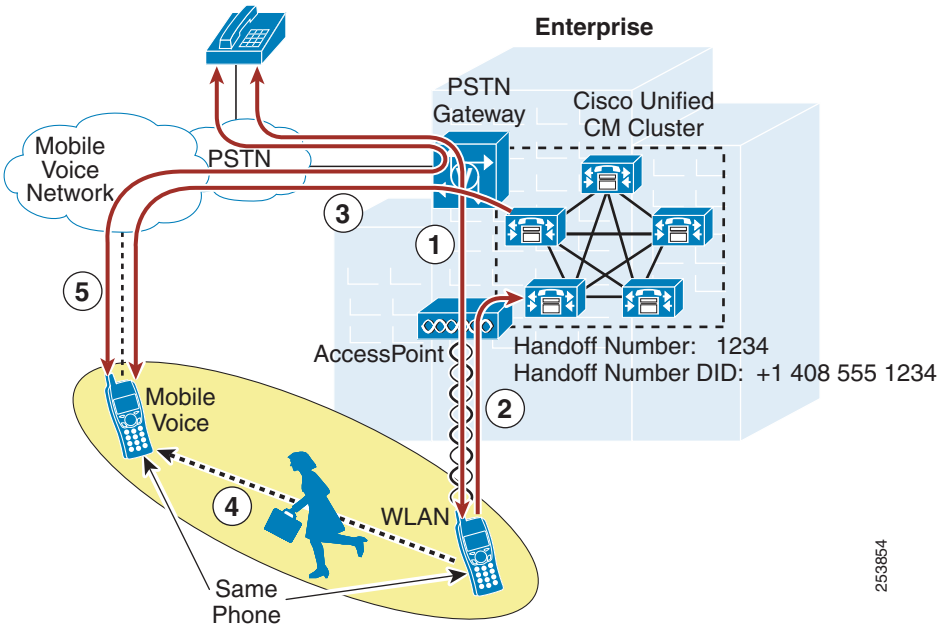
  この方式では、[モバイル ネットワークへ転送（Transfer to Mobile Network）] の設定を [HandoffDN 機能の使用（ユーザが発信）（Use HandoffDN Feature (user places call)）] に設定する必要があります。このタイプのハンドオフでは、モバイル クライアントが、モバイル ボイス ネットワークを介して、Unified CM システム内で設定されているハンドオフ番号に対してコールを発信します。

（注）　ハンドオフ機能は、デュアルモード スマートフォンにのみ適用されます。この機能は、Samsung Galaxy Note Pro など、セルラー音声無線を使用しないデバイスではサポートされません。

ハンドオフのモバイル ソフトキー方式

図 21-30 に示す動作は、社内の iPhone または Android デュアルモード デバイスにおけるアクティブなコールが、手動で WLAN インターフェイスから会社の PSTN ゲートウェイ経由でモバイル ボイス ネットワーク（デバイスの携帯電話インターフェイス）に移動される様子を示しています。図に示すように、企業の WLAN に関連付けられ、Unified CM に登録されたモバイル クライアント デバイスと、PSTN ネットワーク上の電話機との間に既存のコールがあります（ステップ 1）。これは手動のプロセスであるため、ユーザが Cisco Jabber クライアント内のコール中メニューから [モバイル ネットワークの使用（Use Mobile Network）] ボタンを選択して、コールをハンドアウトする意図があることを Unified CM に通知する必要があります（ステップ 2）。次に、Unified CM から、このモバイル デバイスに対応する設定済みのモビリティ ID 番号に対して、会社の PSTN ゲートウェイを経由してコールが発信されます（ステップ 3）。このモビリティ ID へのコールは、モバイル ボイス ネットワーク（iPhone または Android デバイスの携帯電話インターフェイス）に対して発信されます。これで、ユーザは、社外に移動して、WLAN ネットワークのカバー領域から離れることができます（ステップ 4）。一方、Unified CM からの着信コールがモバイル ボイス ネットワーク インターフェイスで受信され、ユーザは手動でこのコールに応答し、ハンドアウトを完了する必要があります。携帯電話インターフェイスで着信コールが応答されると、WLAN を通過していた RTP ストリームが PSTN ゲートウェイにリダイレクトされ、モバイル クライアント デバイスと元の PSTN 電話機との間のコールは会社のゲートウェイでアンカーされて、中断されずに継続します（ステップ 5）。

図 21-30　Cisco Jabber デュアルモード ハンドアウト（WLAN からモバイル ボイス ネットワークへ）：モバイル ソフトキー方式

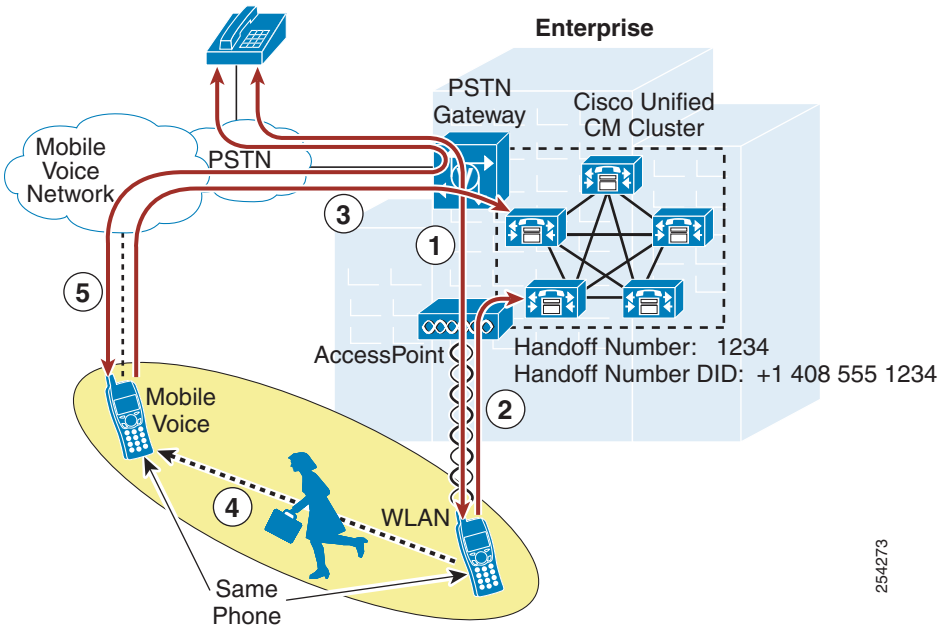


ハンドオフ番号方式のハンドオフ

図 21-31 に、社内の iPhone デュアルモード電話機におけるアクティブなコールが、手動で WLAN インターフェイスから会社の PSTN ゲートウェイ経由でモバイル ボイス ネットワークまたは携帯電話インターフェイスに移動される図 21-30 と同じハンドオフ動作を示します。ただし、このケースでは、ハンドオフ番号方式のハンドアウトが使用されます。

図 21-31 に示すように、企業の WLAN に関連付けられ、Unified CM に登録されたデュアルモード デバイスと、PSTN ネットワーク上の電話機との間に既存のコールがあります（ステップ 1）。これは手動のプロセスであるため、ユーザが Cisco Jabber デュアルモード クライアント内のコール中メニューから [モバイル ネットワークの使用（Use Mobile Network）] ボタンを選択して、コールをハンドアウトすることを Unified CM に通知する必要があります（ステップ 2）。次に、Cisco Jabber クライアントが、Unified CM システム内で設定されているハンドオフ番号に向けて、モバイル ボイス ネットワークを介して携帯電話インターフェイスからコールを自動発信します（ステップ 3）。これで、ユーザは、社外に移動して、WLAN ネットワークのカバー領域から離れることができます（ステップ 4）。その間に、Cisco Jabber クライアントからの着信コールが Unified CM によって受信されます。着信したコールの発信番号がユーザに設定されているモビリティ ID と一致したと仮定すると、WLAN を通過した RTP ストリームが PSTN ゲートウェイにリダイレクトされ、Cisco Jabber モバイル クライアントと元の PSTN 電話との間のコールは、会社のゲートウェイでアンカーされて、中断されることなく継続します（ステップ 5）。

図 21-31　Cisco Jabber デュアルモード ハンドアウト：ハンドオフ番号方式



（注） ハンドオフ番号方式のハンドアウトでは、Unified CM が、着信したコールの発信番号として、ハンドオフを試みている Cisco Dual Mode デバイスの下で設定されているモビリティ ID 番号と一致する番号を PSTN ネットワークから受け取る必要があります。発信者 ID がデュアルモード デバイスから送信されない場合、PSTN プロバイダーが着信したコールの発信者 ID を会社に送信しなかったり、着信したコールの発信者 ID が設定されているモビリティ ID と一致しなかった場合は、ハンドアウト動作は失敗します。

（注） Cisco Jabber デュアルモード クライアントはハンドインをサポートしません。デュアルモード モバイル ボイス ネットワーク（セルラー インターフェイス）と会社の電話（または会社のゲートウェイでコールがアンカーされた PSTN 電話機）との間で通話中のコールがアクティブである場合、コールをデュアルモード デバイスの WLAN インターフェイスに移動するには、コールをいったん切断し、デュアルモード クライアントが企業ネットワークに接続されて Unified CM に登録されてからリダイヤルするのが唯一の方法です。

Cisco Jabber モバイル クライアントの WLAN 設計上の考慮事項

Cisco Jabber モバイル クライアントを配置する際には、次の WLAN ガイドラインを考慮してください。

- 可能な場合は、デバイスの WLAN インターフェイス上で同じ IP アドレスを使用できるように、Cisco Jabber モバイル クライアントが必ず WLAN のレイヤ 2 でだけローミングするようにしてください。デバイスの IP アドレス変更のために、サブネットの境界を越えるレイヤ 3 ローミングのシナリオでは、コールがドロップされます。
- 同じ SSID が AP 全体で使用される WLAN ネットワークに Cisco Jabber モバイル クライアントを配置します。SSID が異なると、AP 間のローミングがはるかに低速になります。

- WLAN 上のすべての AP が、その SSID をブロードキャストするようにしてください。SSID が AP によってブロードキャストされないと、他の Wi-Fi ネットワークに参加するようユーザがデバイスから要求される場合や、デバイスが自動的に他の Wi-Fi ネットワークに参加する場合があります。この場合、コールは中断されます。
- 可能な場合は、5 GHz 帯域 WLAN（802.11a/n/ac）に Cisco Jabber モバイル クライアントを配置します。5 GHz WLAN は、音声コールとビデオ コールに関してスループットを改善し、干渉を低減します。

デュアルモード デバイス向けの Cisco Jabber Dial Via Office

Unified CM の管理者は、Cisco Dual Mode for iPhone または Android デバイス設定ページの [製品固有の設定レイアウト（Product Specific Configuration Layout）] セクションを使用して各デュアルモード デバイスに対する Dial Via Office（DVO）コールを有効または無効にできます。DVO が有効な場合、ユーザは Cisco Jabber アプリケーション内の [コール オプション（Calling Option）] 設定を使用して DVO をオンにできます。DVO のコール オプションは、Jabber クライアントによって使用される発信コール方式だけでなく、着信コール方式も定めることに注目してください。表 21-4 は、ネットワーク接続の種類に基づくさまざまなコール オプションと、対応する発信コール方式と着信コール方式を示しています。

表 21-4　Cisco Jabber Dial Via Office コール オプションを使用した着信コール方式と発信コール方式

デバイス IP 接続	Cisco Jabber DVO コール オプション					
	自動選択		モバイル ボイス ネットワーク		Voice over IP	
	発信コール	着信コール	発信コール	着信コール	発信コール	着信コール
802.11 WLAN（社内/企業）	Voice over IP	Voice over IP	Dial via Office	シングル ナンバー リーチ（Single Number Reach）	Voice over IP	Voice over IP
802.11 WLAN（非社内/企業）						
モバイル データ	Dial via Office	シングル ナンバー リーチ（Single Number Reach）				
IP なし	発信コール：ネイティブ携帯電話 着信コール：シングル ナンバー リーチ					

DVO が最初に有効になったときのデフォルトのコール オプションは [自動選択（Autoselect）] です。これにより、デバイスが 802.11 WAN 経由で接続している場合は Cisco Jabber の着信コールと発信コールの両方で Voice over IP（VoIP）が発生します。デバイスがモバイル データ ネットワークに接続している場合は、発信コールに DVO が使用され、着信コールにシングル ナンバー リーチが使用されます。

いずれの場合も、Unified CM 内のモバイル クライアント デバイス設定で [緊急番号（Emergency Numbers）] フィールドに設定された緊急番号に発信されるコールは、選択されているコール オプションに関係なく、携帯電話ネットワーク経由で直接ダイヤルされます。

（注）　Dial via Office コール機能は、デュアルモードのスマートフォンにのみ適用されます。この機能は Apple iPad などのタブレットではサポートされません。これらのデバイスにセルラー音声無線がないためです。

シングル ナンバー リーチの場合と同様に、Dial Via Office が Cisco Jabber クライアントで有効になっている場合は、Cisco Unified Mobility のモバイル ボイス メール回避またはシングル企業ボイスメール ボックス機能が実行されます。Dial Via Office の場合、このボイス メール回避機能により、DVO コールのセットアップ中にネットワーク パス障害やその他の通信エラーが発生した場合、呼び出されたユーザが発信側ユーザのボイス メール ボックスに転送されないことが保証されます。通常は、ボイスメール回避によるユーザ制御方式が、全体的に最も優れたユーザ エクスペリエンスを実現します。これは、DVO コール レッグが誤ってボイスメール システムによって応答された場合、DTMF トーンが Unified CM によって受信されないとコール レッグが切断され、DVO コールが消去されるためです。Cisco Jabber ユーザでモバイル ボイス メール回避方式によるユーザ制御が有効になっている場合、クライアント デバイスでモビリティ コールを受信したときに、モバイル デバイスのキー パッドにあるボタンを押す必要があることをユーザに通知する必要があります。ボタンを押さないと、コール セットアップで障害が発生します。

(注)　モバイル ボイス メール回避によるユーザ制御方式は、PTSN 接続と PTSN ゲートウェイおよびアウトオブバンド経由でモバイル デバイスから Unified CM まで DTMF トーンが正常に伝達されることに完全に依存しているため、PSTN から Unified CM に着信 DTMF を伝達できない場合、モバイル デバイスから発信した（Dial Via Office Reverse）、またはモバイル デバイスが受信（シングル ナンバー リーチ）した社内コールがすべて切断されます。DTMF が PSTN から Unified CM に効果的にリレーできない場合、代わりにタイマー コントロールのモバイル ボイス メールの無効化方式を使用する必要があります。

シングル企業ボイス メール ボックスのボイス メールの回避機能に関する詳細情報については、シングル企業ボイスメール ボックスによるモバイル ボイスメール回避（21-59 ページ）を参照してください。

Dial Via Office コール オプションの使用例

Dial Via Office を配置するときには、次の Cisco Jabber クライアントのコール オプションのユーザ プロファイルを考慮してください。

- 自動選択

  [自動選択（Autoselect）] の一般的なユーザ プロファイルは、オフィス内とオフィス外の両方で移動するユーザです。このユーザ プロファイルの [自動選択（Autoselect）] は、802.11 WLAN 接続が使用可能な場合、VoIP を利用することでコストをできるだけ抑え、WLAN 接続が使用できない場合は、モバイル ボイスおよびデータ ネットワーク（DVO およびシングル ナンバー リーチ）に戻ります。

- モバイル音声ネットワーク

  [モバイル音声ネットワーク（Mobile Voice Network）] コール オプションの一般的なユーザ プロファイルは、WLAN カバレッジがほとんどなく、IP 接続で高品質かつ信頼性の高い通話を実現するためにモバイル データ接続では満足なスループットと信頼性が得られない高度なモバイル ユーザです。

- Voice over IP

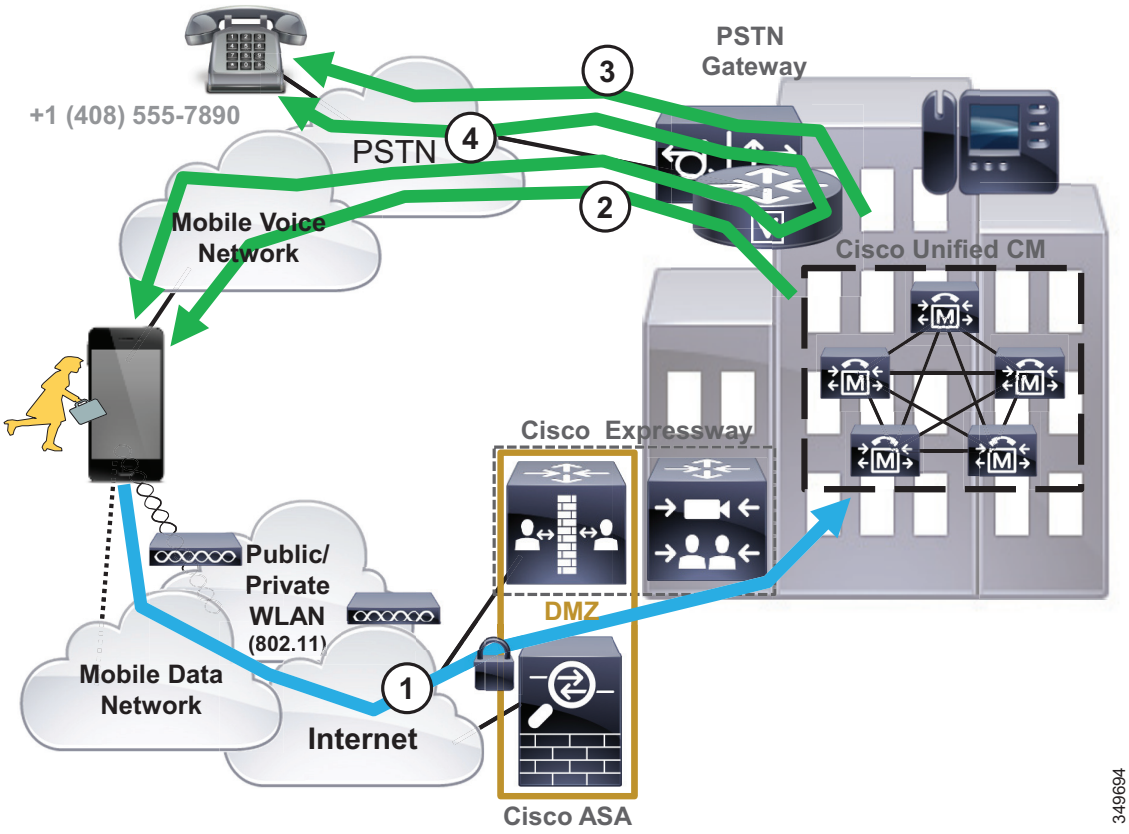
  [Voice over IP] コール オプションの一般的なユーザ プロファイルは、オフィス（自宅または会社）内で移動する、社内コールで社外への発信を通常必要としないユーザです。また、このユーザ プロファイルを使用する場合、企業負担および従業員負担のモバイル ボイス/データ サービスの点で、モバイル ボイスとデータのコストが重要な考慮事項になります。

Dial Via Office Reverse

Cisco Jabber クライアントは Dial Via Office Reverse（DVO-R）をサポートします。DVO のこの方式では、Unified CM システムからユーザ設定されたモビリティ ID または携帯電話番号への着信コールによってコール セットアップが実施されます。

図 21-32 は、DVO-R のコール フローを示しています。この例では、Cisco Jabber ユーザが PSTN 電話機（+1 408 555-7890 ）に電話をかけようとしています。ユーザは番号をダイヤルするか、Cisco Jabber クライアント内の連絡先リストから番号を選択し、企業および Unified CM に IP 接続経由で SIP コール セットアップ要求を生成します（ステップ 1）。コール セットアップ要求に基づいて、Unified CM は社内 PSTN ゲートウェイを使用して、ユーザの設定したモビリティ ID（携帯電話番号）にリバース コールを発信します（ステップ 2）。Unified CM からの着信コールがモバイル デバイスで応答されると、ユーザが呼び出した番号または選択した番号にコールが転送されます（ステップ 3：この場合は +1 408-555-7890）。一度コールが遠端で応答されると、メディア パスが接続され、会社の PSTN ゲートウェイ（ステップ 4）経由で固定されます。コールが会社のゲートウェイに固定されたため、ユーザはこのコール中の任意の時点で Unified Mobility のデスクトップフォン ピックアップ機能を使用したり、Unified Mobility DTMF ベースの通話切替機能を呼び出したりすることができます。

図 21-32　Cisco Jabber Dial Via Office Reverse



(注)　図 21-32 に示すコール フローでは、Cisco Jabber が Unified CM に登録されていると想定し、DVO がユーザに対して有効で、クライアントのコール オプション設定が [モバイル音声ネットワーク(Mobile Voice Network)] または [自動選択(Autoselect)] であると想定しています。クライアント設定が [自動選択(Autoselect)] の場合、Cisco Jabber を実行しているデュアル モード デバイスはモバイル データ ネットワーク経由で IP 接続される必要があります。802.11 WLAN 経由で接続されている場合、クライアントは DVO ではなく Voice over IP を使用します。

デフォルトで、DVO-R コールバックのコール レッグが(図 21-32 に示すように)ユーザのモバイル デバイスに転送されますが、ユーザが Cisco Jabber クライアント内の [DVO コールバック番号(DVO Callback Number)] フィールドで代替コールバック番号を指定することがあります。デフォルトで [DVO コールバック番号(DVO Callback Number)] フィールドには、ユーザ設定のモビリティ ID が入ります。ユーザがこのフィールドに異なる番号を設定すると、DVO-R コールバックのコール レッグがその番号に転送されます。たとえば、ユーザはコールバックを携帯電話で受信するよりも、自宅の電話に転送するよう希望することがあります。

(注)　代替コールバック番号を使用して DVO-R を呼び出す場合、Unified CM からのコールバックのコール レッグがユーザ指定の代替番号へ転送されると、そのコールは会社に固定されません。このような場合、ユーザはデスクトップフォンのピック アップを実行したり、代替コールバック番号を使用した DVO-R コールでの DTMF ベースの通話切替機能を呼び出したりすることができません。また、DVO-R 代替番号へのコールに対してボイス メール回避が適用されません。

(注)　DVO-R コールでは En-bloc ダイヤル方式が利用されるため、[オーバーラップ送信を許可(Allow Overlap Sending)] が有効にされるパターンでも、重複送信は適用されません。

モバイル プロファイルおよび Dial Via Office Reverse

モバイル クライアント デバイス向けモビリティ ID に Cisco Unified CM モビリティ プロファイルが割り当てられることがあります。必須ではありませんが、モビリティ プロファイルは、モビリティ ID または代替コールバック番号に DVO-R コールバックのコール レッグのセットアップ時にシステムによって送信される発信者 ID を指定します。モビリティ プロファイル設定ページの [Dial-via-Office Reverse Callback Configuration] セクションの [Callback Caller ID] フィールドに設定された番号は、発信者 ID として送信される番号ですモビリティ ID にモビリティ プロファイルが割り当てられていない場合、または [コールバック発信者 ID(Callback Caller ID)] フィールドが空白のままである場合、システムは、設定されたデフォルトのエンタープライズ機能アクセス番号を送信します。

(注)　モビリティ プロファイルの [モバイル クライアント コール オプション(Mobile Client Calling Option)] フィールドは DVO 操作に影響しません。この設定に関係なく、DVO コールが有効である場合は Cisco Jabber クライアントが DVO-R コールを発信します。Dial via Office Forward (DVO-F) コール オプションは、現在使用できません。

Cisco Jabber ポイントツーポイント コール

Cisco Jabber モバイル クライアントは、Unified CM の登録を必要としないポイントツーポイントの Voice and Video over IP(VVoIP)通話を提供できます。代わりに、Jabber クライアントは REST/HTTPS コール シグナリング用の Cisco WebEx Messenger クラウド サービスを活用します。ポイントツーポイント コール メディアでは、音声通話に G.722 コーデック、ビデオ通話に H.264 コーデックで RTP プロトコルを利用します。REST ポイントツーポイント コールでは、Jabber モバイル クライアントごとに 1 つのコールだけがサポートされ、保留、保留解除、転送、会議などの通話中の補足機能はサポートされません。

Cisco Jabber for iPhone and iPad 対応の Apple プッシュ通知サービス（APNs）

これまでの Cisco Jabber for iPhone and iPad クライアントでは、デバイス上でバックグラウンドで実行されている間、定期的なダイレクト IP ソケット キープアライブ メッセージを使用して、クライアントがバックグラウンドに移るときに、Voice and Video over IP（VVoIP）サービスや IM およびプレゼンス サービス用の接続を維持していました。このような定期的なメッセージにより、ユーザへの通知とクライアントでの着信コールおよびメッセージの受信が確実になります。Cisco Jabber for iPhone and iPad 11.9 以降、および Cisco Unified CM and IM and Presence Service リリース 11.5 SU3 以降（ならびに最新バージョンの WebEx Messenger）では、Apple iOS デバイス上でクライアントがバックグラウンドで実行中も、クライアントは Apple プッシュ通知サービス（APNs）を介して着信コールおよびメッセージを受信できるようになっています。

図 21-33 に、APNs のアーキテクチャを示します。緑色の矢印で示されているように、Unified CM や Unified CM IM and Presence Service（または WebEx Messenger）でクライアントへの通知が必要になると、Unified CM と Unified CM IM and Presence Service（または WebEx Messenger サービス）は、エンタープライズ ネットワークからインターネット上の Cisco Collaboration Cloud にアウトバウンド HTTPS 通知を送信します（ステップ 1）。Cisco Collaboration Cloud はインターネット上の Apple プッシュ通知サービス（APNs）へのセキュアな接続を確立して、Jabber クライアントへの通知を APNs に転送します（ステップ 2）。APNs は受信した通知を Jabber iOS クライアント デバイスに転送します（ステップ 3）。転送先のデバイスは、キャリア ネットワーク上の Apple デバイスの初期プロビジョニングであらかじめ APNs に登録されます。APNs によるこの通知により、ユーザに対するアラートがトリガーされます。この通知アーキテクチャは、Jabber for Apple iOS クライアントがオンプレミスで接続されているか、あるいは VPN または Expressway モバイルおよびリモート アクセスを介して接続されているかに関係なく適用されます。

図 21-33　Cisco Jabber for Apple iOS と APNs アーキテクチャの概要

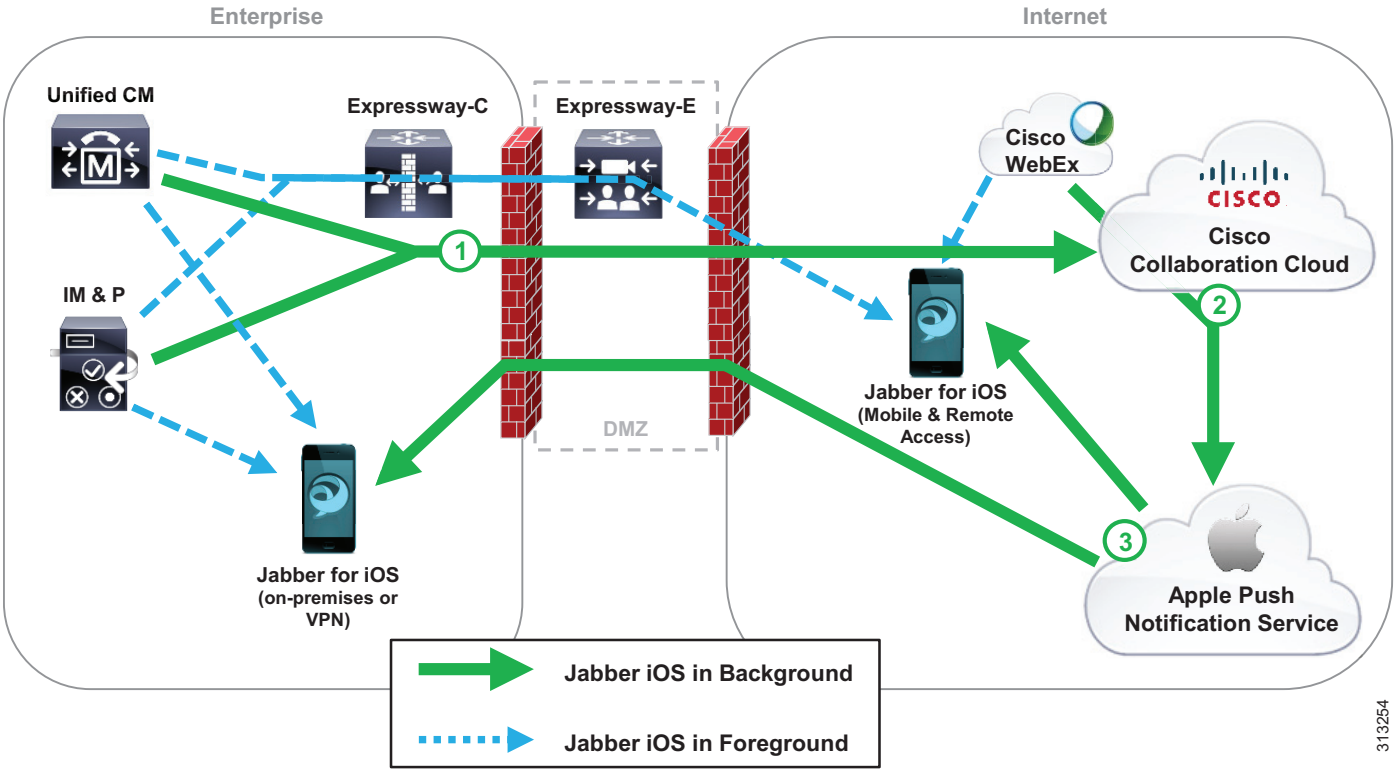


図 21-33 の青色の矢印で示されているように、Jabber for Apple iOS クライアントがフォアグラウンドで実行されているときは、Unified CM や Unified CM IM and Presence Service は SIP および XMPP を使用してクライアントに直接通知を送信します。

オンプレミスの Unified CM および Unified CM IM and Presence 導入環境では、管理者がクラウド オンボーディング プロセスによって、Cisco Jabber for iPhone and iPad クライアントの APNs を Unified CM 上で有効にします。APNs が有効にされると、バックグラウンドで実行中の Cisco Jabber for iPhone and iPad クライアントは、APNs を介してコールやメッセージの通知を受信するようになります。

(注)　最新バージョンの Apple iOS（iOS 10 と iOS 11 を含む）では引き続き、バックグラウンドで実行中の Cisco Jabber for iPhone and iPad クライアントが接続を維持するためのキープアライブ メッセージをサポートしています。したがって、Unified CM 上で APNs を有効化することは、まだ要件ではありません。ただし、Apple ではダイレクト IP ソケット方式の通知のサポートを終了していることから、Apple iOS デバイス上でバックグラウンドで実行中の Jabber for Apple iOS クライアントに通知を送信するには、APNs が間もなく要件となるはずです。現行のダイレクト IP ソケット方式が今後の Apple iOS リリースで除去された時点で、Cisco Jabber for iPhone and iPad クライアントがバックグラウンドで実行されている間、ユーザに着信コールやメッセージを通知する手段は APNs のみとなります。

WebEx Messenger を使用するクラウドまたはハイブリッド導入環境では、APNs は WebEx クラウド内でデフォルトによって有効にされています。したがって、バックグラウンドで実行中の Cisco Jabber for iPhone and iPad 11.9 以降のクライアントは APNs を介して IM 通知を受信します。

WebEx Messenger での Jabber 間コールは APNs でサポートされていません。WebEx Messenger で Jabber 間コール機能を使用する予定の場合は、jabber-config.xml ファイルの **< Policies >** **< Push_Notification_Enabled >** パラメータを使用して手動で APNs を無効にする必要があります。jabber-config.xml のパラメータについて詳しくは、以下のリンク先から入手できる最新バージョンの『*Parameters Reference Guide for Cisco Jabber*』を参照してください。

https://www.cisco.com/c/en/us/support/customer-collaboration/jabber-iphone-ipad/products-installation-guides-list.html

WebEx Messenger でエンドツーエンドの暗号化（AES）ポリシーを [強制（enforced）] または [オプション（optional）] に設定すると、APNs が自動的に無効にされて、バックグラウンドで実行中のクライアントは通常の方法で IM 通知を受信することになります。

(注)　バックグラウンドで実行中の Jabber に対する APNs の使用は、Cisco Jabber for iPhone and iPad クライアントにのみ適用されます。Windows、Mac、および Android Jabber クライアントには適用されないため、これらのクライアントはバックグラウンドで実行されている間、引き続き通常の方法で IM 通知を受信します。

Cisco Jabber とリフレッシュ トークンを使用した OAuth でのログイン フロー

Cisco Jabber 11.9 以降、OAuth 2.0 承認フレームワークを使用して、クライアント承認と認証を容易に行えるようになっています。これにより、ログインが迅速化されるとともに、起動時やネットワーク遷移時の再認証も迅速化されます。Cisco Unified CM 12.0 および Unified CM 11.5(1) SU3 の前までは、導入環境内でシングル サインオン（SSO）が有効にされている場合、Cisco Jabber は OAuth のみを使用していました。OAuth 実装は、認証を行い承認トークンをクライアントに発行する承認サーバとしての役割を果たす Unified CM パブリッシャに依存します。このトークンとリフレッシュ トークンにより、クライアントがコラボレーション サービスに要求を行い承認を取得することが可能になります。また、リフレッシュ トークンを使用して、期限切れの承認トークンを素早く更新できます。OAuth 2.0 フレームワークの詳細については、承認フレームワーク（16-46 ページ）の項を参照してください。

OAuth を Jabber クライアントの承認と認証に使用するには、Cisco Unified CM、Unified CM IM and Presence、Unity Connection で、**OAuth with Refresh Login Flow** サービス パラメータを有効にする必要があります。同様に、Jabber クライアントが Expressway モバイルおよびリモート アクセスで OAuth を使用するには、**Authorize by OAuth token with refresh** 設定を Expressway-C で有効にする必要があります。

Cisco Jabber での OAuth 展開の詳細については、次の URL で入手可能な最新バージョンのホワイト ペーパー『*Deploying OAuth with Cisco Collaboration Solution Release 12.0*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

Cisco Jabber および Expressway モバイルとリモート アクセス

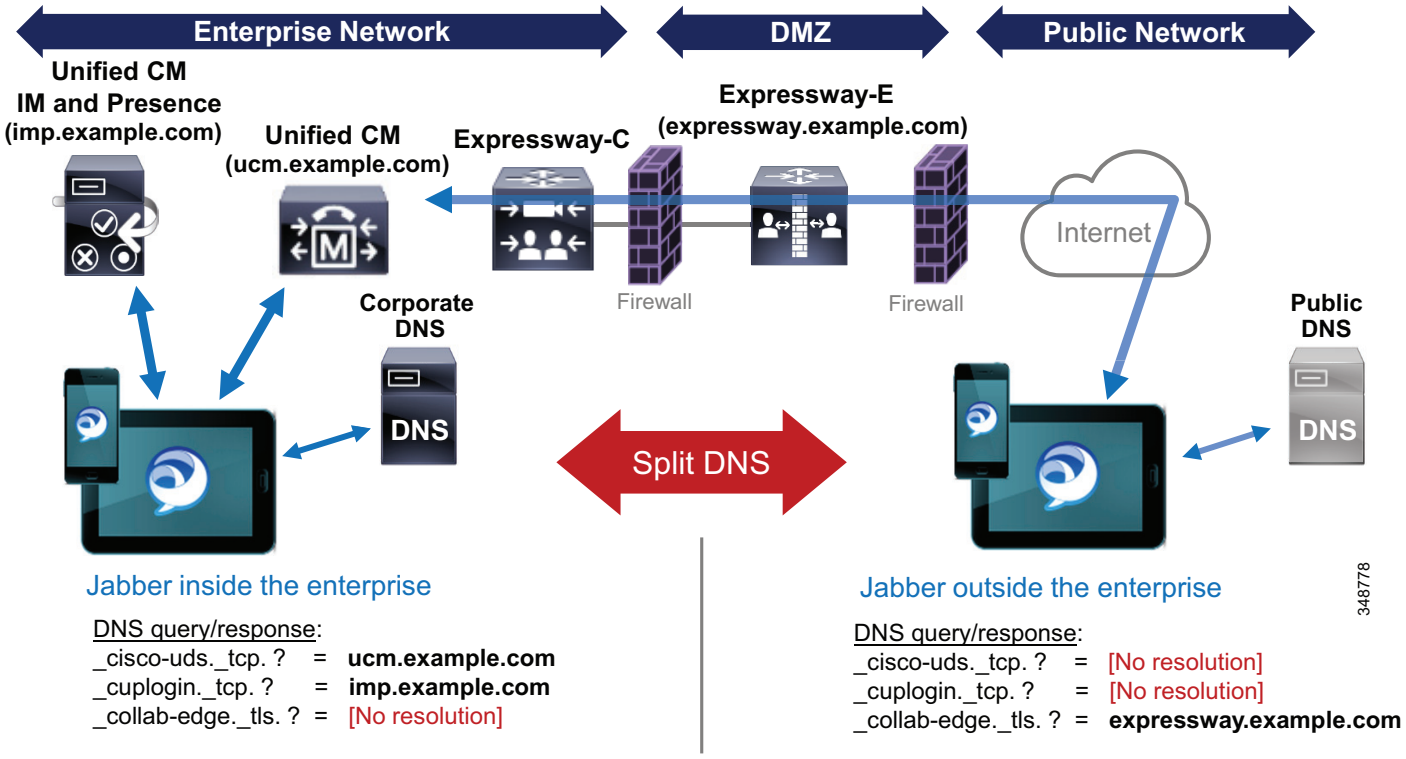
Cisco Expressway ソリューションのモバイルおよびリモート アクセス機能は、Cisco Jabber 用のセキュアなファイアウォール トラバーサルを提供します。これにより、リモート Jabber ユーザが企業の外にいるときに、モバイル デバイスから企業のコラボレーション アプリケーションやサービスにアクセスできます。

Expressway モバイルおよびリモート アクセス接続を通過するすべてのコラボレーション トラフィック（コール メディアやシグナリングを含む）は暗号化されます。暗号化された接続は、企業内の Expressway C ノードと Jabber エンドポイントの間で行われます。Expressway C と企業内のエンドポイントおよびアプリケーションの間のトラフィックは、デフォルトでは暗号化されません。Unified CM Cisco 証明書信頼リスト（CTL）プロバイダーおよび認証局プロキシ関数（CAPF）サービスに基づくセキュリティ設定によって促進されるデバイス認証、SRTP メディア、および TLS SIP シグナリング暗号化の混合モードとして Unified CM クラスタが設定されている場合にのみ、企業内のメディアとシグナリング トラフィックが暗号化されます。

DNS クエリ解決およびスプリット DNS 解決設計に基づいて、Jabber は企業との相対的なロケーション（内部または外部）を判別します。この場合、Unified CM のサービス レコード（_cisco-uds._tcp）および Unified CM IM and Presence のサービス レコード（_cuplogin._tcp）が社内 DNS でのみ設定され、Expressway のサービス レコード（_collab-edge._tls）がパブリック DNS でのみ設定されます。この分けられた設計により、企業内の場合は社内 DNS 解決で Jabber がコラボレーション サービスに直接誘導され、パブリック DNS 解決では Expressway 経由で接続するように Jabber に指示します。モバイル デバイスのネットワーク接続が変更されるたびに DNS クエリが Jabber によって送信されます。

図 21-34 に示すように、Jabber は _cisco-uds._tcp、_cuplog._tcp、および _collab-edge._tls の 3 つの SRV サービス レコードに関して DNS に照会します。企業内に位置している場合、Jabber クライアントは Unified CM または Unified CM IM and Presence を指し示す解決を社内 DNS から受け取ります。この場合、Jabber は解決されたコラボレーション アプリケーション サービス ノードに直接接続します。企業の外に位置している場合、Jabber はパブリック DNS から Unified CM または Unified CM IM and Presence の解決を受け取らず、代わりに Expressway を介して企業に接続するようクライアントに指示する Expressway 解決を受け取ります。

図 21-34　Cisco Jabber：企業内外のスプリット DNS 解決



（注）　Cisco AnyConnect VPN がリモート エンタープライズ接続に使用される場合、Jabber は VPN トンネル経由で社内 DNS から DNS クエリ解決を受け取り、コラボレーション サービス ノードに直接接続します。

Cisco Jabber モバイル クライアント用の Expressway モバイルおよびリモート アクセスを配置するときには、以下のサポートされない機能について考慮してください。

- デュアルモード ハンドオフ

  Jabber デバイスの WLAN インターフェイスからセルラー音声インターフェイスへのアクティブ コールの移動は、Expressway 接続ではサポートされません。

- エンドポイント認証およびメディアとシグナリングの暗号化のための CAPF 登録

  安全なメディアおよびシグナリングが企業ネットワークで必要とされる場合、Jabber デバイスはオンプレミスで、Expressway 経由の接続の前に、CAPF 登録を完了する必要があります。

- ユーザ単位またはデバイス単位のアクセス制限

  Expressway モバイルおよびリモート アクセスを介して接続しないよう特定のユーザやデバイスを制限するメカニズムはありません。コラボレーション インフラストラクチャ（Unified CM および Unified CM IM and Presence）で Expressway モバイルおよびリモート アクセスが展開されて Jabber 用にユーザがすでにプロビジョニングされている場合、ユーザは Expressway を介して接続できます。

- セッションの永続性

  Expressway モバイルおよびリモート アクセス経由のすべてのコールおよび他のコラボレーション アプリケーション接続は、ネットワーク パスが変更されるか失われると、必ず消去されます。

- LDAP ディレクトリ アクセス

  Expressway モバイルおよびリモート アクセス接続では LDAP トラフィックが無効です。このため、ディレクトリ アクセス方式として CDI が設定されていても、Expressway 経由で接続する際にすべての Jabber クライアントは社内ディレクトリ アクセスに UDS 方式だけを使用できます。

上記のいずれかの機能を配置する必要がある場合、安全な企業リモート アクセス用に Expressway の代わりに AnyConnect VPN を使用することを考慮してください。

Cisco AnyConnect VPNス プリット トンネルを使用した Cisco Jabber と Expressway モバイルおよびリモート アクセス

Jabber ユーザが VPN または Expressway のいずれかを介して接続できるようにするために、VPN および Expressway を並行して展開する必要が生じることがあります。このような状況では、2 つの方式を使用できます。Jabber ユーザはコラボレーション ワークロード用に Expressway モバイルおよびリモート アクセス機能を使用できます。また、企業への接続でコラボレーション外部のワークロードが必要な場合は、すべてのデバイス トラフィック用に VPN を使用できます。これらのシナリオでは、Cisco AnyConnect VPN クライアントによって企業への接続が確立されると、VPN オンデマンド トリガーまたはユーザによる手動起動のためにアクティブな接続がドロップされます。ユーザが使用を再開するには、VPN を介してプロビジョニングされたコラボレーション サービスに Jabber クライアントが再接続するのを待つ必要があります。これは、ユーザ エクスペリエンスを低下させます。

別の方法として、スプリット トンネリングを使って AnyConnect VPN と Expressway を同時に使用することもできます。この場合、コラボレーション フローは Expressway モバイルおよびリモート アクセス接続を必ず経由し、他すべてのトラフィックは VPN トンネルを経由します。この代替的な方法では、VPN トンネルが確立されると Jabber クライアントは Expressway から切断して VPN で再接続するのを回避できるため、通常はユーザ エクスペリエンスが向上します。

図 21-35 に示すように、この展開方法によって実現するスプリット トンネリングは、2 つの基本原則に依存しています。

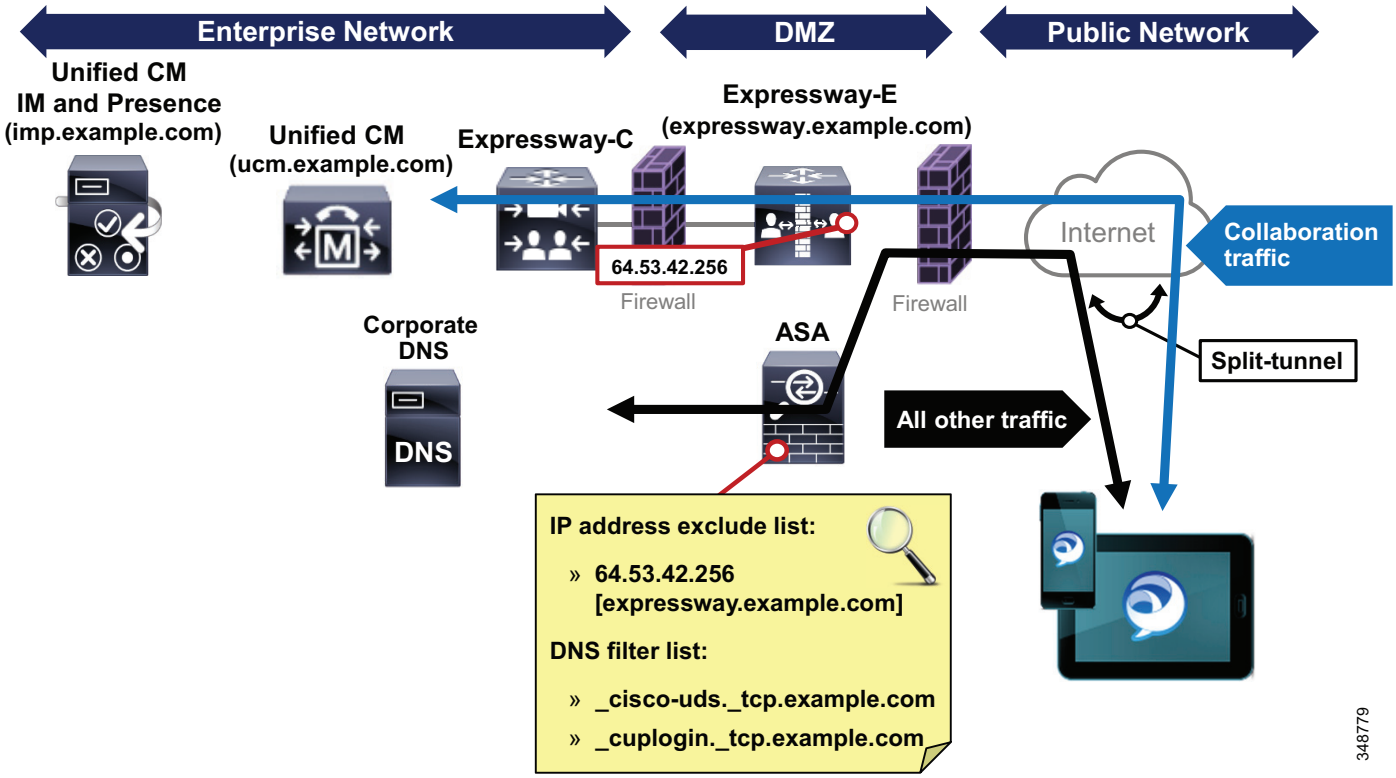
- Cisco 適応型セキュリティ アプライアンス（ASA）VPN ヘッドエンドでの DNS フィルタリング

  _cisco-uds._tcp.<*domain*> および _cuplogin._tcp.<*domain*> に関する Jabber クライアントからの DNS クエリをフィルタリングするために ASA でのトラフィック フィルタリングが使用されます。これらの DNS クエリがフィルタリングされるため、Jabber クライアントはコラボレーション サービスに直接接続するための Unified CM および IM and Presence サービス レコード要求を解決できません。したがって _collab-edge._tcp.<*domain*> に関する DNS 解決のみが得られ、結果として Expressway 接続とトラバーサルが常に使用されます。

- VPN トンネルでの Expressway アクセスの除外

  パブリックにインターフェイスに面している Expressway-E に Jabber クライアントが接続するのを防ぐために、ASA での IP アドレス フィルタリングが使用されます。Expressway-E ノードのパブリック インターフェイス IP アドレスをフィルタリングするとき、スプリット トンネル VPN 接続が作成され、結果として VPN トンネルから Jabber トラフィックが除外されます。こうして、このトラフィックが Expressway を通過し、その他すべてのトラフィックは VPN トンネルを通過します。

図 21-35　Cisco Jabber：Expressway モバイルおよびリモート アクセスと Cisco AnyConnect VPN



Expressway モバイルおよびリモート アクセスを使用する AnyConnect VPN スプリット トンネリングの場合、パブリック DNS で設定された同じ Expressway DNS SRV レコード（_collab-edge._tls）が社内 DNS に追加されます。これにより、VPN トンネル経由でパブリック DNS へのアクセスを提供したり DNS クエリを転送したりする必要がなくなります。

同じ _collab-edge._tls SRV レコードを社内 DNS で設定することは、Jabber と Expressway モバイルおよびリモート アクセスの配置で期待される基本的なスプリット DNS 設計にそぐわないように思われるかもしれませんが、実際には Jabber での SRV 解決設定順序によって適切な動作が保証されます。Jabber での SRV 解決設定順序によると、最初は Unified CM（_cisco-uds._tcp）、次に IM and Presence（_cuplogin._tcp）、そして最後に Expressway（_collab-edge._tls）です。したがって、_collab-edge._tls クエリが社内 DNS で解決できる場合でも、社内 DNS が _cisco-uds._tcp または _cuplogin._tcp サービスのクエリを最初に解決するため、クライアントはコラボレーション サービスに直接接続します。

AnyConnect VPN を使用する Jabber と Expressway モバイルおよびリモート アクセスの詳細については、次の URL で入手できる『*Cisco Unified Access (UA) and Bring Your Own Device (BYOD) CVD*』の Cisco Expressway シリーズとモバイルおよびリモート アクセスのコラボレーションに関する情報を参照してください。

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.html

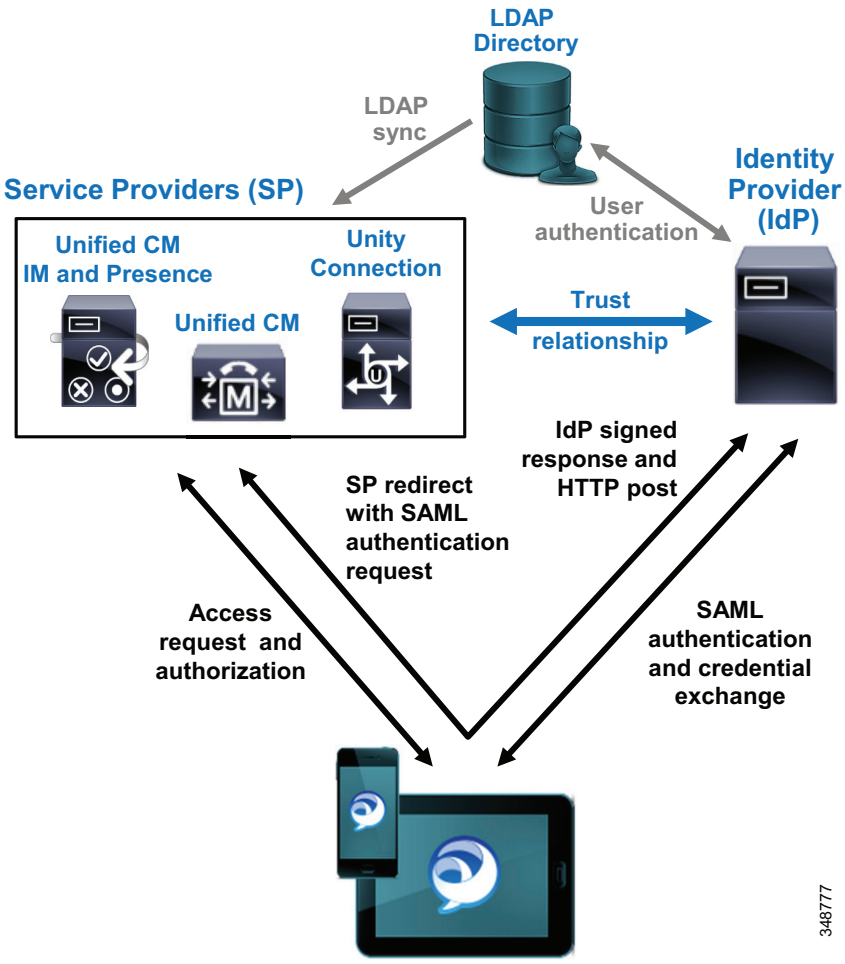
Cisco Jabber と SAML シングル サインオン

Cisco Jabber モバイル クライアントは、Security Assertion Markup Language（SAML）バージョン 2 を使用してシングル サインオン（SSO）を活用できます。Jabber とシスコ コラボレーション インフラストラクチャ（Unified CM、Unified CM IM and Presence など）、および Unity Connection は、ユーザ接続を識別して認証するために Web ベースの SSO SAML v2 を使用します。これにより、Jabber ユーザ クレデンシャルの単一セットを使ってすべてのコラボレーション サービスにアクセスできます。

図 21-36 に示すように、Cisco Jabber SSO は、Unified CM などのコラボレーション アプリケーション（サービス プロバイダーとも呼ばれます）と ID プロバイダー（IdP）の間の事前に確立された信頼関係に依存します。Unified CM および Unity Connection サービス プロバイダーは、ユーザを特定するために、社内 LDAP ディレクトリとの LDAP 同期および統合を使用します。同様に、IdP はユーザを認証するために LDAP 社内ディレクトリを使用します。Cisco Jabber およびコラボレーション サービスでサポートされる IdP には、Ping Federate、Microsoft Active Directory フェデレーション サービス（ADFS）、および Open Access Manager（OpenAM）が含まれます。

図 21-36 には、基本的な Jabber SSO のフローが示されています。SSO フローは、コラボレーション サービス プロバイダーへのアクセス（たとえば、呼制御サービス用の Unified CM へのアクセス）を要求する Jabber クライアントで始まります。サービス プロバイダーは、コラボレーション サービス プロバイダーに直接ログインしてアクセスする代わりに、SAML 認証要求を使って Jabber クライアントを IdP にリダイレクトします。IdP は Jabber ユーザに認証クレデンシャルを要求し、社内 LDAP ディレクトリに対してユーザを認証します。ユーザが正常に認証された場合、IdP は署名付きアサーションを返します。Jabber は HTTP POST を使用してこれをコラボレーション サービス プロバイダーに転送します。次にコラボレーション サービス プロバイダーは、署名付きアサーションを検証し、Jabber クライアントに許可を与えます。たとえば、Jabber は Unified CM に正常に登録されます。

図 21-36　SAML SSO を使用する Cisco Jabber



署名付きアサーションを Jabber クライアントに転送することに加えて、IdP は認証済み Jabber クライアントのセキュリティ コンテキストを保存します。クライアントが他のコラボレーション サービス プロバイダーへのアクセスを要求した場合、IdP は改めてクレデンシャルを交換する必要がなく、後続の署名付きアサーションを提供できます。こうして SSO により、Jabber ユーザまたはクライアントは、クレデンシャルを一度だけ入力して、複数のコラボレーション サービスにアクセスすることができます。

ユーザ認証時にコラボレーション サービス プロバイダーが IdP とは直接通信しない点に注意してください。

SSO の詳細については、アイデンティティ管理アーキテクチャの概要（16-35 ページ）および最新バージョンの『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』を参照してください（次の URL から入手できます）。

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

SSO でユーザを識別し、オンプレミス コラボレーション アプリケーション/サービスに対して認証することに加えて、Expressway モバイルおよびリモート アクセス接続でのユーザ認証のために SAML SSO を有効にすることもできます。これらのシナリオでは、インバウンド リモート アクセス接続用の認証を仲介させるために、HTTPS リバース プロキシを企業の DMZ に配置します。HTTPS リバース プロキシは社内 IdP と通信し、リモート クライアントと社内 IdP の間の SAML 要求/認証交換を仲介します。DMZ の HTTPS リバース プロキシとして任意の汎用 HTTPS リバース プロキシを使用できますが、SSO SAML 要求の仲介やプロキシのために IdP プロキシの役割を果たす IdP インスタンスを DMZ にインストールするオプションが、一部の IdP ベンダーで提供されています。

Cisco Jabber と Cisco Unified Mobility との間の相互作用

Cisco Jabber モバイル クライアントを Cisco Unified Mobility に統合することで、Cisco シングル ナンバー リーチ、通話切替 DTMF 機能、2 段階ダイヤリング、シングル企業ボイスメール ボックスのモバイル ボイスメール回避を利用できます。

Unified Mobility と統合するには、iPhone または Android デュアルモード携帯電話番号を、Cisco Dual Mode for iPhone または Cisco Dual Mode for Android デバイスに関連付けられたモビリティ ID として Unified CM 内で設定する必要があります。システム内で携帯の番号をモビリティ ID として設定した後は、iPhone または Android デュアルモード デバイスが企業に接続されず Unified CM に登録されていない場合に、シングル ナンバー リーチを利用して、ユーザの会社の電話番号への着信コールをモバイル ボイス ネットワーク経由で iPhone または Android デュアルモード デバイスに転送できます。デュアル モード デバイスが会社に接続され、Unified CM に登録されている場合、着信 Voice-over-IP コールが有効になるようにクライアント コール オプションが設定されると（デバイスが WLAN に接続しているときの [Voice over IP] または [自動選択（Autoselect）]）、会社の電話番号に対する着信 IP コールはデバイスのモバイル ボイス ネットワーク インターフェイスに転送されません。iPhone または Android デュアルモード デバイスが企業に接続されている場合は、デバイスの WLAN またはモバイル データ インターフェイスだけが着信コールを受信します。これにより、会社の PSTN ゲートウェイ リソースの必要以上の消費を回避できます。

携帯電話音声ネットワークを介して社内コールを処理する場合、iPhone または Android デュアルモード デバイスは、DTMF を使用して通話切替機能を呼び出したり、会社の任意の固定コールに対するデスクトップフォンのピック アップを実行したりできます。また、デュアルモード デバイスでは、コールを発信する場合にモバイル ボイス アクセスとエンタープライズ機能アクセスの 2 ステージ ダイヤリング機能を利用して、これらのコールを会社経由でルーティングし、会社の PSTN ゲートウェイにアンカリングできます。

iPhone または Android デュアルモード デバイスにモビリティ ID を設定することに加えて、リモート接続先として追加の携帯電話番号またはオフシステム電話番号を設定して、それらの番号を Unified CM 内で Cisco Dual Mode for iPhone または Cisco Dual Mode for Android デバイスに関連付けることができます。モビリティ ID および追加のリモート接続先をデュアルモード デバイスに関連付けるときに、リモート接続先プロファイルを設定する必要はありません。

（たとえば Android スマートフォンで Cisco Jabber for Android を実行し、Apple iPad で Cisco Jabber for iPhone and iPad を実行しているユーザなど）モバイル ユーザが複数のモバイル デバイスにまたがる複数のシスコ モバイル クライアントをプロビジョニングする場合、モビリティ ID をタブレット デバイス（Cisco Jabber for Tablet）ではなく、デュアルモード デバイス（Cisco Dual Mode for Android など）に関連付けます。デュアルモード デバイスは、デュアルモード ハンドオフや Dial Via Office などのモビリティ ID 固有の機能を利用するため、モビリティ ID をこのデバイスに関連付ける必要があります。モビリティ ID と同じデバイスに他のリモート接続先をすべて関連付けます。同じユーザに対して異なるモバイル クライアント デバイスの異なるリモート宛先を関連付けると、設定がより複雑になり、問題の修復が難しくなります。

Cisco Unified Mobility のフィーチャ セット、および設計と配置の考慮事項の詳細については、Cisco Unified Mobility（21-51 ページ）を参照してください。

Cisco Jabber とモバイル音声用 Cisco Intelligent Proximity の間の相互作用

モバイル音声用のインテリジェント プロキシミティ機能は、携帯電話またはデュアルモード デバイスのモバイル回線でハンズフリー音声を可能にするために設計されています。このため通常は、Jabber クライアント デバイスの携帯電話回線の通話でのみ、インテリジェント プロキシミティ可能な IP エンドポイントでハンズフリー音声再生を行えます。Cisco Jabber での Voice and Video over IP コールの場合、モバイル音声のインテリジェント プロキシミティは起動されません。これに関する唯一の例外は、Cisco IP Phone 8851 および 8861 エンドポイントです。これらの IP フォンは音声専用であるため、モバイル音声のインテリジェント プロキシミティを使用すると、Jabber IP ベース コールの音声が 8851 フォンまたは 8861 フォンを経由してストリーミングされ、このコールのビデオ部分は Jabber クライアント デバイスに残ります。モバイル音声のインテリジェント プロキシミティが可能なその他のハードウェア エンドポイントの場合、Jabber IP ベースのコールの音声は IP エンドポイントで再生されません。

Cisco Spark

Cisco Spark モバイル クライアントは、Android および iPad や iPhone などの Apple iOS で使用できます。適切なアプリケーション ストア（Apple の App Store や Google Play）からクライアント アプリケーションをダウンロードし、Apple iOS または Android デバイスにインストールした後、ユーザは自分の電子メール アドレスを入力し、結果として送られてくるプロビジョニング電子メールでアカウントをアクティブにする必要があります。ユーザがアカウントをアクティブにすると、クライアントは Cisco Collaboration Cloud に接続します。ユーザは、暗号化されたインスタント メッセージ（IM）を使って 1 人以上の他のユーザと通信するための安全なコラボレーション ルームを作成できます。ユーザは、自分のアカウントのパスワードを設定するために、Web ブラウザを使用して少なくとも一度 Cisco Spark（https://web.ciscospark.com/）にアクセスする必要があります。あるいは、ユーザは https://download.ciscospark.com/ からダウンロードして入手できるデスクトップ用の Cisco Spark クライアントを使用することもできます。これを行わないと、ユーザがモバイル クライアントで接続するたびに、電子メールを介してアカウントを有効にする必要が生じます。

Cisco Spark for Android、iPad、および iPhone クライアントは、セキュアで持続的な IM コラボレーション ルームを提供するだけでなく、暗号化された Voice and Video over IP やファイル共有機能も提供します。

Cisco Spark クライアントが正常に動作するには、モバイル デバイスがワイヤレス ネットワーク（企業またはパブリック/プライベート 802.11 WLAN、あるいはモバイル プロバイダー データ ネットワーク）に接続することで、インターネットにアクセスできる必要があります。

（注）　Cisco Jabber と同じく、Apple iOS デバイス上で稼働する, Cisco Spark モバイル クライアント（iPhone と iPad）も、バックグラウンドでの実行中に Apple プッシュ通知サービス（APNs）を使用します（Cisco Jabber for iPhone and iPad 対応の Apple プッシュ通知サービス（APNs）（21-108 ページ）を参照）。

Cisco Spark モバイル クライアント、追加の機能、およびサポートされているハードウェアとソフトウェアのバージョンの詳細については、次の Cisco Spark のドキュメントを参照してください。

https://support.ciscospark.com/

Cisco WebEx Meetings

Cisco WebEx Meetings モバイル クライアントは、特定の Android、Apple iOS、BlackBerry、および Windows Phone モバイル デバイスで稼働します。このクライアントを使用すると、モバイル エンドポイントはデスクトップ ブラウザ ベースの Cisco WebEx Meetings と同様の機能を持つ Cisco WebEx Meetings に参加できます。このクライアントによって、Cisco WebEx 音声およびビデオ会議へのアクティブな参加（参加者リストや共有コンテンツを表示する機能を含む）が可能になります。

Cisco WebEx モバイル クライアントに関する詳細情報については、次の URL にある製品情報を参照してください。

https://www.cisco.com/c/en/us/products/conferencing/webex-meetings/index.html

シスコのクラウド コラボレーション サービス：Cisco Spark および Cisco WebEx 用の SAML SSO

前述のオンプレミス エンタープライズおよびコラボレーション エッジと同様に、Cisco Spark や Cisco WebEx などのクラウド コラボレーション サービスに安全にログインにするためにエンタープライズ SSO を使用することもできます。このタイプの配置では、企業 IdP と、企業 DMZ に配置された HTTPS リバース プロキシを併用することで、企業クレデンシャルを活用してユーザを識別し、Cisco Spark や Cisco WebEx へのアクセスを認証します。

Cisco AnyConnect モバイル クライアント

Cisco AnyConnect モバイル クライアントは、Cisco Jabber モバイル デバイス クライアント用の安全なリモート接続機能を提供し、モバイル データ ネットワークと非企業 WLAN 経由の接続を有効にします。Cisco AnyConnect モバイル クライアントは、Apple の App Store または Google Play（以前の Android Market）からダウンロードできます。このクライアント アプリケーションは、Cisco Adaptive Security Appliance（ASA）ヘッドエンドで利用可能な Cisco AnyConnect VPN ソリューションを使用して、Apple iOS および Android モバイル デバイスに SSL VPN 接続を提供します。

モバイル データ ネットワークあるいはパブリック/プライベート Wi-Fi ホット スポットを介した接続に VPN ネットワーク接続を利用する場合は、企業のセキュリティ要件およびポリシーに沿った広帯域かつセキュアな VPN インフラストラクチャを配置することが重要です。この接続を利用するユーザおよびデバイスの数に基づき、広帯域幅、信頼性の高い接続、および適切なセッションまたは接続キャパシティをこの VPN インフラストラクチャで提供できるよう、慎重に計画することが必要です。

Cisco AnyConnect を使用したセキュアなリモート VPN 接続の詳細については、次の Web サイトで入手可能な Cisco AnyConnect Secure Mobile Client マニュアルを参照してください。

https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html

シスコのモバイル クライアントおよびデバイスのハイ アベイラビリティ

モバイル デバイス、特にデュアルモード電話機はその特性上、ネットワーク接続に関して高い可用性を備えています（WLAN ネットワークが利用できない場合には、モバイル ボイスおよびデータ ネットワークを音声およびデータ サービスに使用できます）。しかし企業の WLAN および IP テレフォニー インフラストラクチャのハイ アベイラビリティについては、まだ考慮すべき点があります。

まず、企業の WLAN は、冗長な WLAN アクセスが可能になるように配置する必要があります。たとえば、AP およびその他の WLAN インフラストラクチャ コンポーネントは、ワイヤレス AP の 1 つに障害が発生しても、モバイル デバイスのネットワーク接続には影響がないように配置する必要があります。同様に、モバイル デバイスが常にネットワークに安全に接続できるように、WLAN の管理およびセキュリティ インフラストラクチャも高い冗長性を備えた配置にする必要があります。コントローラベースのワイヤレス LAN インフラストラクチャが推奨されます。その理由は、企業内 AP の集中型設定および管理が可能であり、ネットワーク アクティビティや AP の障害に基づいて WLAN を動的に調整できるためです。

次に、Cisco ASA ヘッドエンド VPN ターミネータや Cisco Expressway E および Expressway C ノードを含むリモート セキュア接続ソリューションのコンポーネントは、高い冗長性を備えた配置にする必要があります。こうすると Cisco ASA や Cisco Expressway ノードの損失がモバイル クライアントの安全なモバイルやリモート アクセスの接続に影響したり、妨げになったりしません。

次に、Unified CM の呼処理サービスおよび登録サービスのハイ アベイラビリティについて考慮する必要があります。Unified CM の呼処理サービスを利用する企業内の他のデバイスの場合と同様に、モバイル クライアント デバイスを Unified CM に登録する必要があります。Unified CM クラスタのアーキテクチャにはプライマリとバックアップの呼処理サービスおよびデバイス登録サービスが用意されており、冗長な特性を持っているため、1 つの Unified CM サーバ ノードで障害が発生しても、モバイル デバイスの登録やコール ルーティングは引き続き利用可能です。

PSTN アクセスについても同様の事項を考慮する必要があります。IP テレフォニー配置と同様、複数の PSTN ゲートウェイおよびコール ルーティング パスを配置して、PSTN への可用性の高いアクセスを確保する必要があります。このことは、モバイル クライアント デバイスの配置に固有の考慮事項ではありませんが、それでも重要な考慮事項です。

Cisco Collaboration Cloud の場合、クラウド データセンターにおける冗長性の高いコンポーネントおよびリソース設計（コンピューティングとネットワーク アクセスの両方のプラットフォームを含む）のために、WebEx および Cisco Spark サービスは高い可用性を備えています。この耐障害性に優れたインフラストラクチャ設計は、Cisco Collaboration Cloud サービスに依存するシスコ モバイル クライアントに信頼性の高いアクセスを提供します。

シスコのモバイル クライアントおよびデバイスのキャパシティ プランニング

シスコのモバイル クライアントおよびデバイス（デュアルモード電話機を含む）におけるキャパシティ プランニングに関する考慮事項は、登録、呼処理、PSTN アクセス サービスのために IP テレフォニー インフラストラクチャやアプリケーションを利用している他の IP テレフォニー エンドポイントまたはデバイスの場合と同じです。

Unified CM を使用してシスコのモバイル クライアントとデバイスを配置するときには、Unified CM での登録負荷および Unified Mobility の制限事項を考慮することが重要です。1 つの Unified CM サーバは、最大 40,000 台のデバイスの設定と登録を処理できます。モバイル クライアントとデバイスを配置するときには、クラスタあたりサポートされる最大デバイス数を考慮する必要があり、場合によっては追加的な負荷を処理するために呼処理クラスタをさらに配置する必要が生じることもあります。

また、前に説明したように、1 つの Unified CM クラスタ内のリモート接続先およびモビリティ ID の最大数は 40,000 です。ほとんどのデュアルモード モバイル クライアント デバイスは、シングル ナンバー リーチ、シングル企業ボイスメール ボックス、モバイル ボイスメール、モバイル ボイスメール回避、デスクトップフォンのピックアップ、2 段階ダイヤリングなどの機能を利用するために Unified Mobility と統合されることが多いため、これらの各デュアルモード モバイル デバイスの携帯電話番号を Unified CM クラスタ内のモビリティ ID として設定する必要があります。これは、Unified Mobility との統合を容易にするため、またハンドオフ番号方式のハンドアウトを容易にするために必要です。したがって、これらのデュアルモード デバイスを Unified Mobility と統合するときには、Unified CM クラスタにおけるリモート接続先およびモビリティ ID の全体的な容量を考慮して、十分な容量を確保することが重要です。追加のユーザまたはデバイスがシステム内の Unified Mobility にすでに統合されている場合は、これらのユーザまたはデバイスによって、デュアルモード デバイスで利用可能なリモート接続先およびモビリティ ID の空き容量が制限される可能性があります。

シスコのモバイル クライアントの拡張性に関するもう 1 つの考慮事項は、Expressway C と Expressway E での Cisco Expressway モバイル/リモート アクセス コールおよびプロキシ登録キャパシティです。Expressway C および Expressway E クラスタは、最大 10,000 件のプロキシ登録と最大 2,000 のビデオまたは 4,000 の音声コールをサポートします。シスコのモバイル クライアントに使用できるキャパシティを決定する際、その他の Expressway 接続デバイス（たとえば Cisco TelePresence MX/SX シリーズのデバイスのような Jabber デスクトップ クライアントや固定エンドポイント、および 7800 や 8800 シリーズのデバイスのようなシスコ デスク フォン）を計算に含めるのを忘れないでください。同様に、Expressway モバイルおよびリモート アクセスを介して企業に接続するシスコのモバイル クライアント デバイスに関して、Unified CM クラスタ ノードの登録負荷を考慮する必要もあります。Cisco Expressway モバイルおよびリモート アクセスのサイジングについては、Cisco Expressway（25-39 ページ）を参照してください。

モバイル クライアント デバイスを展開するときには、Unified CM システムおよび PSTN ゲートウェイの全体的な呼処理能力を考慮する必要もあります。モバイル デバイスの実際の設定および登録を処理する以外に、こうしたシステムでは、これらのモバイル デバイスとユーザによって増加する BHCA の影響に対処するための十分な能力も必要です。同様に、モバイル デバイスを処理するのに十分な PSTN ゲートウェイ能力を確保することも重要です。通常、デュアルモード モバイル デバイスを持つユーザは頻繁に移動することが多いため、Unified Mobility に統合されているデュアルモード デバイスではこれが特に当てはまります。通常、頻繁に移動するユーザは、モバイル ユーザの会社の電話番号への着信コールによって PSTN への 1 つ以上のコールが発信されるシングル ナンバー リーチなどのモビリティ機能や、会社の PSTN ゲートウェイを利用してユーザが会社経由でコールを発信する 2 ステージ（段階）ダイヤリングなどを使用することで、会社の PSTN ゲートウェイの負荷を高める傾向にあります。

最後に、シスコのモバイル クライアントとデバイスを配置する場合、企業モビリティ配置と同様に、802.11 WLAN コール キャパシティを考慮する必要があります。前述のとおり、802.11 チャネル セルあたり、最大 27 件の VoWLAN コールまたは最大 8 件の VVoWLAN コールが可能です。ここでは、デバイスが 2.4 GHz 帯域に配置される場合の Bluetooth なし、VoWLAN コール用に 24 Mbps 以上のデータ レート、および VVoWLAN コール用に最大 1 Mbps ビット レートで 720p のビデオ解像度を想定しています。実際のコール キャパシティは、RF 環境、ワイヤレス エンドポイント タイプおよび WLAN インフラストラクチャに応じてさらに小さくなることがあります。802.11 WLAN コール キャパシティの詳細については、キャンパス企業モビリティのキャパシティ プランニング（21-9 ページ）を参照してください。

上記のすべての考慮事項が、モバイル クライアントやデバイスに固有であるわけではありません。これらの考慮事項は、デバイスやユーザが Unified CM に追加されてシステム全体の負荷が高まるすべての状況に当てはまります。

一般的なシステム サイジング、キャパシティ プランニング、および配置上の考慮事項の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

シスコのモバイル クライアントおよびデバイスの設計上の考慮事項

シスコのモバイル クライアントとデバイスを配置する際は、次の設計上の推奨事項に従ってください。

- モバイル ボイス ネットワークとモバイル データ ネットワーク、および WLAN ネットワークの両方に同時に接続するために、デュアルモード モバイル デバイスでは、デュアル転送モード（DTM）がサポートされている必要があります。これにより、デバイスのセルラー無線と WLAN インターフェイスの両方からデバイスに到達可能になり、両方のインターフェイスでコールを発信および受信できます。モバイル ボイス ネットワークおよびモバイル データ ネットワークでデュアル接続デバイスがサポートされていない場合には、適切なデュアルモード クライアント操作が実行できない場合があります。
- WLAN AP は、20 % 以上のセル オーバーラップを確保して配置される必要があります。このようにオーバーラップさせることによって、モバイル デバイスがロケーション内で移動した場合に AP 間で正常にローミングして、ボイス ネットワーク接続およびデータ ネットワーク接続を維持できます。
- パケット損失を最小限に抑えるために、WLAN AP は -67 dBm のセル パワー レベル境界（またはチャネル セル半径）で配置される必要があります。また、同一チャネルのセル境界の分離は、約 19 dBm にする必要があります。AP またはクライアントにおいて、同じチャネルに関連付けられている他のデバイスとの同一チャネル干渉を発生させないようにするには、19 dBm の同一チャネル セル分離が重要です。このような干渉が発生すると、音声とビデオの品質が低下する場合があります。
- 可能であれば、音声およびビデオ トラフィックを生成できるモバイル クライアントおよびデバイス接続用の 5 GHz WLAN 帯域（802.11a/n/ac）を利用してください。5 GHz WLAN は、音声コールとビデオ コールに関してスループットを改善し、干渉を低減します。
- クライアント アプリケーションの音声とビデオ コールの品質、およびすべての機能の適切な動作を保証するために、音声メディアと専用ビデオおよびシグナリング帯域幅に対するプライオリティ キューイングを含む必要なエンドツーエンド QoS サービス クラスをサポートするように、企業の有線および無線 LAN を配置して設定する必要があります。ほとんどのクライアントがシスコの QoS の推奨事項に基づいてレイヤ 3 でトラフィックを適切にマークしますが、適切なレイヤ 2 WLAN UP マーキングはクライアント デバイスとベンダー実装に依存します。このため、レイヤ 2 マーキングはプラットフォーム間で一貫しておらず、信頼度は低くなります。
- モバイル デバイスがデスクトップ コンピュータと同様に、多種多様なデータおよびリアルタイム トラフィックを生成する可能性があるため、これらのデバイスは通常、信頼できないと見なされます。したがって、ポート番号やプロトコルに基づいてこれらのクライアント デバイスからのすべてのトラフィックを再マーキングするよう、ネットワークを設定する必要があります。同様に、ネットワークへの入口のレート制限およびポリシングが推奨されます。
- シスコでは、モバイル デバイスやクライアントに接続するために、エンタープライズ クラスの音声/ビデオ最適化された WLAN ネットワークだけを使用することを推奨します。ほとんどのモバイル クライアント デバイスは、パブリック/プライベート WLAN アクセス ポイントやホット スポットに接続し、インターネット経由で会社に接続して呼制御やその他のコラボレーション サービスを利用できますが、このようなタイプの接続の場合、音声とビデオの品質は保証されません。
- シスコのコラボレーション モバイル クライアントおよびデバイスを Bring Your Own Device（BYOD）インフラストラクチャに配置する場合、管理者は、ユーザの介入を必要とせず、IP テレフォニー インフラストラクチャを最大限に活用できるネットワーク接続方式を考慮する必要があります。さらに、リモート接続シナリオでは、シスコ モバイル クライアントとデバイスがコラボレーション サービスにアクセスできるように、すべての関連するポートを企業ファイアウォールでオープンにする必要があります。

- BYOD インフラストラクチャにおいて、紛失または盗難されたモバイル デバイスをリモートで消去、あるいは工場出荷時の状態にリセットすることが企業のポリシーにより定められている場合、個人のモバイル デバイスを使用している従業員はポリシーを認識し、定期的に個人データをバック アップする必要があります。
- デュアルモード デバイスが社内にあり、Unified CM に登録されている場合、Unified Mobility シングル ナンバー リーチ機能は、デュアルモード デバイスの設定済みモビリティ ID に着信コールを転送しません。これは、企業の PSTN リソースの利用を削減するための仕様です。デュアルモード デバイスは Unified CM に登録されるため、システムでは、デバイスが社内で到達可能であるかどうかを把握できます。社内で到達可能である場合は、コールを PSTN に転送してデュアルモード デバイスのセルラー音声無線を呼び出す必要性がありません。シングル ナンバー リーチでは、デュアルモード デバイスが登録されていない場合にのみ、ユーザの会社の電話番号への着信コールが公衆網のモビリティ ID 番号に転送されます。
- モバイル デバイスを配置するときには、モバイル デバイスが企業に接続されているかどうかにかかわらずユーザがダイヤリング手順を維持できるように、必要なダイヤル ストリングを正規化することを推奨します。モバイル ネットワークにおけるダイヤリングは通常、完全な E.164（先頭に「+」が付く場合と付かない場合がある）を使って行われ、携帯電話の連絡先は通常、完全な E.164 番号で保存されるため、完全な E.164 番号と、先頭に「+」を付けた完全な E.164 番号をモバイル クライアント デバイス用に使用できるよう企業のダイヤル プランを設定することを推奨します。このように企業のダイヤル プランを設定すると、ユーザはデバイスが Unified CM に登録されているかどうかを気にする必要がなくなるため、最善のエンド ユーザ ダイヤリング エクスペリエンスを提供できます。
- デュアルモード電話機のユーザが緊急コールを発信してデバイスやユーザの位置を特定するときには、モバイル ボイス ネットワークのみを使用させることを推奨します。その理由は、モバイル プロバイダー ネットワークが通常、WLAN ネットワークよりもはるかに信頼性の高い位置情報を提供するためです。デュアルモード電話機から緊急コールや位置サービスを利用するときにモバイル ボイス ネットワークだけが使用されるようにするには、Unified CM 内のデュアルモード デバイスの [緊急番号（Emergency Numbers）] フィールドを、911、999、112 などの緊急番号に設定し、これらのコールが強制的にモバイル ボイス ネットワーク経由で送信されるようにします。デュアルモード電話機のユーザに対して、すべての緊急コールを企業ネットワークではなくモバイル ボイス ネットワーク経由で発信するように指示します。企業の WLAN またはモバイル データ ネットワークを介して緊急コールを発信することは推奨されませんが、セルラー音声無線がないモバイル デバイスは、これらのデータ インターフェイスを介してのみ発信できます。セルラー音声無線がないモバイル デバイスを、緊急コールの発信用に使用すべきではありません。
- モバイル デバイス上に Cisco Jabber を配置するときには、次の配置ガイドラインを満たすよう WLAN ネットワークを設定してください。
  - WLAN のレイヤ 3 で Cisco Jabber モバイル クライアント デバイスのローミングを最小限に抑えます。デバイスの IP アドレスが変わるレイヤ 3 のローミングでは、ローミング時間が長くなり、音声パケットがドロップされ、コールがドロップされる場合もあります。
  - 最も高速な AP 間ローミングを確保するために、WLAN 内の Cisco Jabber モバイル クライアント デバイスで使用されるすべての AP に対して同一の SSID を設定します。
  - コール中に WLAN インフラストラクチャ内の他の AP に参加するように求められるとコールが中断されるおそれがあるので、これを防ぐために、会社のすべての WLAN AP が自身の SSID をブロードキャストするように設定します。

- モビリティ対応ユーザの BHCA レートに基づき、適切なコール キャパシティを処理できる適切な数のワイヤレス AP を配置することにより、シスコのモバイル クライアントおよびデバイス用に企業ワイヤレス ネットワークで十分なワイヤレス音声およびビデオ コール キャパシティを提供します。各 802.11g/n（2.4 GHz）または 802.11a/n/ac（5 GHz）チャネル セルは、24 Mbps 以上のデータ レートで最大 27 件の音声専用コールを同時にサポートできます。各 802.11g/n（2.4 GHz）または 802.11a/n/ac（5 GHz）チャネル セルは、最大 1 Mbps ビット レートでビデオ解像度 720p の場合、最大 8 件のビデオ コールを同時にサポートできます。2.4 GHz WLAN 配置では、このキャパシティを実現するには Bluetooth を無効にする必要があります。実際のコール キャパシティは、RF 環境、ワイヤレス エンドポイント タイプおよび WLAN インフラストラクチャに応じてさらに小さくなることがあります。
- Dial via Office Reverse（DVO-R）を配置するとき、ユーザ制御によるボイス メール回避方式を使用すると、受信側ユーザが発信側ユーザのボイス メールボックスに転送されなくなります。このボイス メール回避方式では、DVO-R コールを接続するために、発信側ユーザがモバイル デバイス キー パッドで番号を押す必要があります。モバイル デバイスのキーを押さない場合、DVO コールが消去されます。
- 代替コールバック番号を使用する DVO-R コールは会社に固定されていないため、デスクトップフォン ピック アップと DTMF ベースの通話切替機能をこれらのコールに使用することはできません。また、代替コールバック番号へのコールにはボイス メール回避が適用されません。
- WLAN からのセルラー デュアルモード ハンドオフ、LDAP ディレクトリ アクセス、ユーザ単位またはデバイス単位のアクセス制限、ネットワーク パス変更時のセッション永続性といった機能は、Expressway モバイルおよびリモート アクセス接続ではサポートされません。これらの機能のいずれかが必要な場合、Jabber モバイル クライアント用の Cisco AnyConnect VPN ソリューションの導入を検討してください。
- さまざまなモバイル デバイスのさまざまなシスコ モバイル クライアントがモバイル ユーザに提供される場合、モビリティ ID および追加的なリモート接続先が常に Cisco Jabber デュアル モード デバイス タイプに関連付けられる必要があります。
- モバイル デバイスを介して Cisco Spark アカウントを最初にダウンロード、インストールし、アクティブ化した後、ユーザは自分のアカウントのパスワードを作成するために Web ブラウザまたはデスクトップ クライアントを使って Cisco Spark にアクセスする必要があります。これが完了すると、ユーザは任意のクライアント（モバイル、デスクトップ、または Web ブラウザ）を使用して Cisco Spark にアクセスできるようになります。パスワードを設定しないと、サインアウトした後に毎回、ユーザは電子メールでアカウントを再アクティブ化しなければなりません。

Cisco Unified Contact Center

改訂日：2018 年 3 月 1 日

この章では、Cisco Unified Communications システムで使用可能な Cisco Unified Contact Center ソリューションについて説明します。Cisco Unified Contact Center Express、Cisco Unified Contact Center Enterprise、Cisco Unified Customer Voice Portal などのシスコ製品に関する情報を示します。また、Cisco Unified Communications Manager やその他の Unified Communications コンポーネントを使用してこれらの Cisco Unified Contact Center 製品を配置する際の設計上の考慮事項についても取り上げます。

この章では、次のトピックについて取り上げます。

この章では最初に、メインの Cisco Unified Contact Center ポートフォリオの概要を示します。続いて、コンタクト センターのさまざまな Unified Communications 配置モデルについて取り上げます。最後に、帯域幅、遅延、Cisco Unified Communications Manager との統合、サイジングなどのトピックに関する設計上の考慮事項について説明します。

この章の目的は、各コンタクト センター製品とその各種コンポーネントの詳細を説明することではなく、各製品を Cisco Unified Communications システムと統合する際の設計上の考慮事項について説明することです。Unified Contact Center の各製品の詳細な設計ガイドラインは、Cisco Unified Contact Center Express、Cisco Unified Contact Center Enterprise、および Cisco Unified Customer Voice Portal 製品向けの設計ガイドを参照してください。製品別の設計ガイドへのリンクは、次の Web サイトを参照してください。

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

この章の変更点

表 22-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 22-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
以下の製品は販売終了（EoS）となったため、このドキュメントから削除されました。 • Cisco MediaSense • Cisco Connected Analytics for Contact Center • Cisco Prime Collaboration Contact Center Assurance	これらの製品については、https://www.cisco.com/go/srnd から入手できる SRND の以前のバージョンを参照してください。	2018 年 3 月 1 日

Cisco Contact Center アーキテクチャ

この章では、次の主要な Cisco Contact Center 製品および関連機能について説明します。

- Cisco Unified Communications Manager（Unified CM）のコール キューイング機能
- Cisco Unified Contact Center Enterprise（Unified CCE）
- Cisco Unified Customer Voice Portal（Unified CVP）
- Cisco Unified Contact Center Express（Unified CCX）

Cisco Unified CM コール キューイング

Cisco Unified CM コール キューイング機能は、ハント パイロット番号に発信者をキューイングする機能を提供します。このオプションをイネーブルにすると、ハント パイロットへの発信者はコールに応答するハント メンバーして設定された利用可能なエージェント待ちのキューに置くことができます。発信者が最初にキューに入ると最初のグリーティング アナウンスを受信し、キューにある間は定期アナウンスが再生されます。エージェントが使用可能になると、キューからコールが取得され、エージェントによって応答されます。非常に限定された機能だけの基本的なコンタクト センターを必要とするお客様に対して、Cisco Unified CM コール キューイングは任意で設定できます。ただし、フル機能の Cisco Contact Center 製品とは異なり、Unified CM コール キューイング オプションには、エージェント デスクトップ、スーパーバイザ、およびレポート機能などのコンタクト センターの機能の多くがありません。フル機能のコンタクト センターが必要な場合、Cisco Unified Contact Center Enterprise または Cisco Unified Contact Center Express を使用する必要があります。

ハント パイロット行のメンバーはフォン画面からこれらの関連のハント パイロットに関するキューの状態を表示します。キューの状態には、次の情報が含まれます。

- ハント パイロット番号
- キューで待機しているコールの数
- コールの最長待機時間

また、Unified CM コール キューイングはハント パイロット番号に基づくサービスアビリティ カウンタを介して、他の統計情報とともに、現在キューで待機しているコール数およびコールの最長待機時間に関する統計情報を提供します。これにより、スーパーバイザは、Real Time Monitoring Tool（RTMT）を使用してキューの状態をモニタすることができます。

次のいずれかの状況が発生した場合、各ハント パイロットに対して、発信者はボイスメールまたは別のハント パイロットなどの設定可能な代替の宛先にルーティングできます。

- [キューで許可されている最大発信者数（Maximum Number of Callers Allowed in Queue）] パラメータで設定したキュー内の発信者数が最大に達した。
- キュー内の発信者の待機時間が [キュー内の最大待機時間（Maximum Wait Time in Queue）] パラメータで設定したしきい値を超過した。
- ハント メンバーが記録されていないか、登録されていない。

（注）　SIP トランクを使用してキューに対応したハント パイロット番号にルーティングされる発信者は、その SIP トランクに関連付けられた SIP プロファイルの [1xx に SDP が含まれている場合に PRACK を送信（Send PRACK if 1XX contains SDP）] に [SIP Rel1XX オプション（SIP Rel1XX Options）] を設定する必要があります。

Unified CM コール キューイング オプションの詳細については、次の Web サイトで入手可能な『*System Configuration Guide for Cisco Unified Communications Manager*』の最新バージョンを参照してください。

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

Cisco Unified Contact Center Enterprise

Cisco Unified Contact Center Enterprise（Unified CCE）は、コンタクト センター ソリューションを提供します。これにより、インバウンドおよびアウトバウンドの音声アプリケーションを、リアルタイム チャット、Web コラボレーション、電子メールなどのインターネット アプリケーションと統合できます。この統合により、顧客がどの通信チャネルを選択したかに関係なく、各エージェントが同時に複数のインタラクションに対応することを支援する統合的な機能が提供されます。各インタラクションは一意であり、個別的なサービスを必要とすることがあるため、シスコは、ほぼすべてのコンタクト属性に基づいて各インタラクションを管理するためのコンタクト センター ソリューションを提供しています。Unified CCE 配置は通常、大規模なコンタクト センターに対して使用され、何千ものエージェントをサポートできます。

また、事前設計され、バインドされている Unified CCE である Cisco Packaged Contact Center Enterprise（Packaged CCE）の配置モデルもあります。コンタクト センターの要件がソリューションの境界に該当するカスタマーは、簡素化された管理インターフェイス、より小規模なハードウェア フットプリント、およびより高速なインストールの利点を活用できます。また、Cisco Unified Contact Center Enterprise および Cisco Unified Customer Voice Portal の包括的な機能セットも利用できます。ソリューションには、包括的なレポーティングを提供するための Cisco Unified Intelligence Center および強化された次世代デスクトップ エクスペリエンスを提供するための Cisco Finesse デスクトップ ソフトウェアが同梱されています。Packaged CCE の詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

- https://www.cisco.com/en/US/products/ps12586/index.html
- https://www.cisco.com/en/US/products/ps12586/tsd_products_support_series_home.html
- https://docwiki.cisco.com/wiki/Packaged_CCE

Unified CCE は、次の主要なソフトウェア コンポーネントを採用しています。

- Call Router

  Call Router は、コールまたはカスタマー コンタクトのルーティング方法に関するすべての決定を行います。

- Logger

  Logger は、コンタクト センターの設定情報とデータサーバへ配信する履歴レポートデータを一時的に格納するデータベースを保持します。Call Router および Logger の組み合わせは、*Central Controller* と呼ばれます。

- ペリフェラル ゲートウェイ

  Peripheral Gateway（PG）は、各種の「周辺」機器（Cisco Unified CM、Cisco Unified IP Interactive Voice Response（Unified IP IVR）、Cisco Unified CVP、または Cisco Unified Web Interaction Manager（Unified WIM）や Cisco Unified E-Mail Interaction Manager（Unified EIM）などのマルチチャネル製品）を接続します。Unified CM と連携するペリフェラル ゲートウェイは、*Agent PG* とも呼ばれます。

- CTI サーバおよび CTI Object Server（CTI OS）

  CTI サーバおよび CTI Object Server は、エージェント デスクトップと連携します。エージェント デスクトップは、Cisco Finesse エージェントとスーパーバイザのデスクトップ、Finesse IP Phone Agent、またはサードパーティ製 CRM アプリケーション向けのカスタマー リレーションシップ マネージメント（CRM）コネクタに基づいて設定できます。

- Administration & Data Server

  Administration & Data Server は、設定インターフェイスと、リアルタイム データ ストレージと履歴データ ストレージを提供します。

Cisco Unified CCE ソリューションは、エージェントの電話機を制御する Cisco Unified Communications Manager（Unified CM）との統合に基づいています。Unified CM を使用せず従来の ACD を使用する配置では、Unified CCE ではなく Cisco Unified Intelligent Contact Management Enterprise（Unified ICME）を使用します。

キューイングおよびセルフサービスの機能は、Cisco Unified IP Interactive Voice Response（Unified IP IVR）または Cisco Unified Customer Voice Portal（Unified CVP）によって提供され、Unified CCE Call Router によって制御されます。

ほとんどの Unified CCE コンポーネントは冗長構成にする必要があります。冗長インスタンスは、サイド A インスタンスおよびサイド B インスタンスと呼ばれます。たとえば、Call Router A および Call Router B は、2 つの異なる仮想マシン上で稼働する Call Router コンポーネントの冗長インスタンスです。

エージェントは、いくつかのビデオ エンドポイント、および Cisco DX70 や DX80 などの Cisco TelePresence エンドポイントを含めて、多種多様のエンドポイントを使用できます。サポートされるエンドポイントの一覧については、以下のリンク先から入手できる『*Unified CCE Solution Compatibility Matrix*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html

Cisco Unified Customer Voice Portal

Cisco Unified Customer Voice Portal（Unified CVP）は、Voice over IP（VoIP）ネットワークでの通信事業者クラスの音声およびビデオ IVR サービスを提供します。CRM データベース統合と、自動音声認識（ASR）とテキストツースピーチ（TTS）の統合により、Unified CVP は、基本的な入力要求と情報収集のアプリケーションや高度なセルフサービス アプリケーションを実行できます。また、Unified CVP は、音声ゲートウェイと IP エンドポイント間でコールをルーティングおよび転送することにより、IP ベースのコール スイッチング サービスを提供します。

Unified CVP は、Voice Extension Markup Language（VXML）をベースにしています。これは HTML に似た業界標準のマークアップ言語であり、Web 開発とコンテンツ配信の力を利用する IVR サービスを開発する目的で使用されます。

Unified CVP ソリューションは、次の主要なコンポーネントを採用しています。

- Unified CVP コール サーバ

  Unified CVP コール サーバは、SIP サービスに呼制御機能を提供します。また、Unified CVP コール サーバは、Intelligent Contact Management（ICM）サービスを介して Unified CCE Call Router と統合できます。IVR サービスは、VXML Micro アプリケーションを実行したり、VoiceXML ページを作成するためのプラットフォームを提供します。

- Unified CVP VXML Server

  このコンポーネントは、VoiceXML ゲートウェイに組み込まれた音声ブラウザと VoiceXML ページをやりとりすることによって、複雑な IVR アプリケーションを実行します。Unified CVP VXML アプリケーションは、Cisco Unified Call Studio を使用して記述され、実行のために Unified CVP VXML Server に配置されます。Unified CVP コール サーバまたは Unified CVP VXML Server を経由する RTP トラフィックはないことに注意してください。

- Cisco Voice Gateway

  Cisco Voice Gateway は、コールが Unified CVP システムに出入りするポイントです。Cisco Voice Gateway には、PSTN への TDM インターフェイスを含めることができます。あるいは、PSTN へのインターフェイスが IP 音声トランクである場合は、Cisco Unified Border Element を使用することもできます。

- Cisco VoiceXML Gateway

  VoiceXML Gateway は、Cisco IOS Voice Browser をホストします。このコンポーネントは、Unified CVP Server IVR Service または Unified CVP VXML Server からの VoiceXML ページを解釈します。VoiceXML Gateway では、.wav ファイルをベースにしたプロンプトを発信者に再生できます。また、DTMF 入力または音声を介して発信者からの入力を受け入れることができます（自動音声認識と統合されている場合）。続いて VoiceXML Gateway は、制御側アプリケーションに結果を返し、次の指示を待機します。

  Cisco VoiceXML Gateway は、Cisco 音声ゲートウェイと同じルータ上に配置できます。このモデルは、小規模な拠点オフィスに配置する場合に適していますが、しかし、VoiceXML Gateway を個別のルータ プラットフォーム上で実行することもできます。このモデルは、複数の音声ゲートウェイが含まれる大規模な集中型配置での使用に適しています。

- Video Media Server

  Unified CVP の包括展開のビデオ メディア サーバは、Video in Queue 機能のビデオ ストリーミングを有効にします。Cisco TelePresence Content Server は、ビデオ メディア サーバとして使用できます。

Unified CVP は、スタンドアロンで配置することも、音声およびビデオ セルフサービスおよびキューイングの機能を利用するために Unified CCE と統合することもできます。Unified CVP ソリューションは現在、G.711 a-law コーデックのエンドツーエンドをサポートします。

Unified CVP の Basic Video Service は、Unified CVP が包括展開モデルの Cisco Contact Center Enterprise（Unified CCE）とともに配置されている場合に使用できます。このサービスでは、ビデオ発信者が音声専用 IVR と対話し、その後、ビデオ エージェントに接続することができます。カスタマーとエージェント エンドポイントとして Cisco DX70 や DX80 などの Cisco TelePresence エンドポイントをサポートします。また、ビデオ エージェントは、電話機から直接内線をダイヤルして、2 番目の音声専用エージェントで会議を行うこともできます。

Video in Queue（VIQ）Basic Video は、Unified CVP のオプション機能であり、ビデオ対応のエージェントまたはエキスパートを待機しているときに発信者に対してビデオ再生を有効にできます。Cisco TelePresence Content Server は、ビデオ ストリーミングを有効にします。発信者はその後、ビデオ エージェントに接続できます。

Unified CVP システム設計と詳細なコール フローの詳細については、次の Web サイトで入手可能な『*Cisco Unified Customer Voice Portal Design Guide*』を参照してください。

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-implementation-design-guides-list.html

Cisco Unified Contact Center Express

Cisco Unified Contact Center Express（Unified CCX）は、400 までのエージェントに対して、使いやすく可用性の高い高度なカスタマー インタラクションを提供する必要のある、部門、企業の支店、または中小規模の会社のニーズに対応するものです。Unified CCX は、複数のサイトにわたる統合セルフサービス アプリケーションを使用して可用性の高い仮想コンタクト センターをサポートすることにより、カスタマー コンタクト インタラクションの効率、可用性、およびセキュリティを高めるような設計になっています。導入をシンプルにするため、Unified CCX は Cisco Business Edition 6000 または 7000 システムに事前ロードすることができます。

Unified CCX は、呼制御のために JTAPI を使用して Unified CM と統合します。Unified CCX のすべてのコンポーネント（Unified CCX エンジン、Unified CCX データベース、Finesse Server、Unified CCX Outbound Dialer、Cisco Unified Intelligence Center、および Express E-mail Manager を含む）が、単一の仮想マシン上にインストールされます。システムの冗長性のために、2 番目に同一の Unified CCX インスタンスを展開に追加できます。

Unified CCX には着信音声/ビデオ通話、サイレント モニタリング、および Cisco Unified Intelligence Center レポート機能が組み込まれています。追加ライセンスとコンポーネントを利用すると、発信ダイヤリング、通話録音、電子メール、チャット、ソーシャル ネットワーク モニタリング、およびワークフォース最適化をサポートするソリューションを強化できます。

Unified CCX は、自動音声認識（ASR）と音声合成（TTS）、HTTP、VXML などの高度な機能をサポートします。また、コンタクト センターのパフォーマンスと品質を最適化するために、Cisco Unified Workforce Optimization などの製品もサポートしています。エージェントは、カメラを搭載した Cisco Unified IP Phone 9900 シリーズなどの多様なビデオ エンドポイントを使用できます。サポートされるエンドポイントの一覧については、次の Web サイトで入手可能な『*Unified CCX Software Compatibility Matrix*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html

Cisco Unified CCX には、顧客の着信コールのプロンプト、コレクト、キューイングの IP IVR 機能が含まれています。

Cisco SocialMiner

Cisco SocialMiner は、Twitter、Facebook、またはパブリック フォーラムやブログのサイトなどを通して通信することによって、顧客および見込み客に対するプロアクティブな応答を支援できる、ソーシャル メディア カスタマー ケア ソリューションです。ソーシャル メディア モニタリング、キューイング、およびワークフローを提供してソーシャル メディア ネットワークでの顧客の投稿を整理し、顧客にソーシャル メディア カスタマー ケア チームを提供することにより、企業は、顧客が使用しているソーシャル ネットワークと同じソーシャル ネットワークを使用して、リアルタイムで顧客に応答できます。詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

https://www.cisco.com/en/US/products/ps11349/index.html

サードパーティのマルチチャネルアプリケーション用のユニバーサル キュー

ユニバーサル キューは、さまざまなメディア チャネルからコンタクト センターのエージェントに要求をルーティングするシステムの機能です。

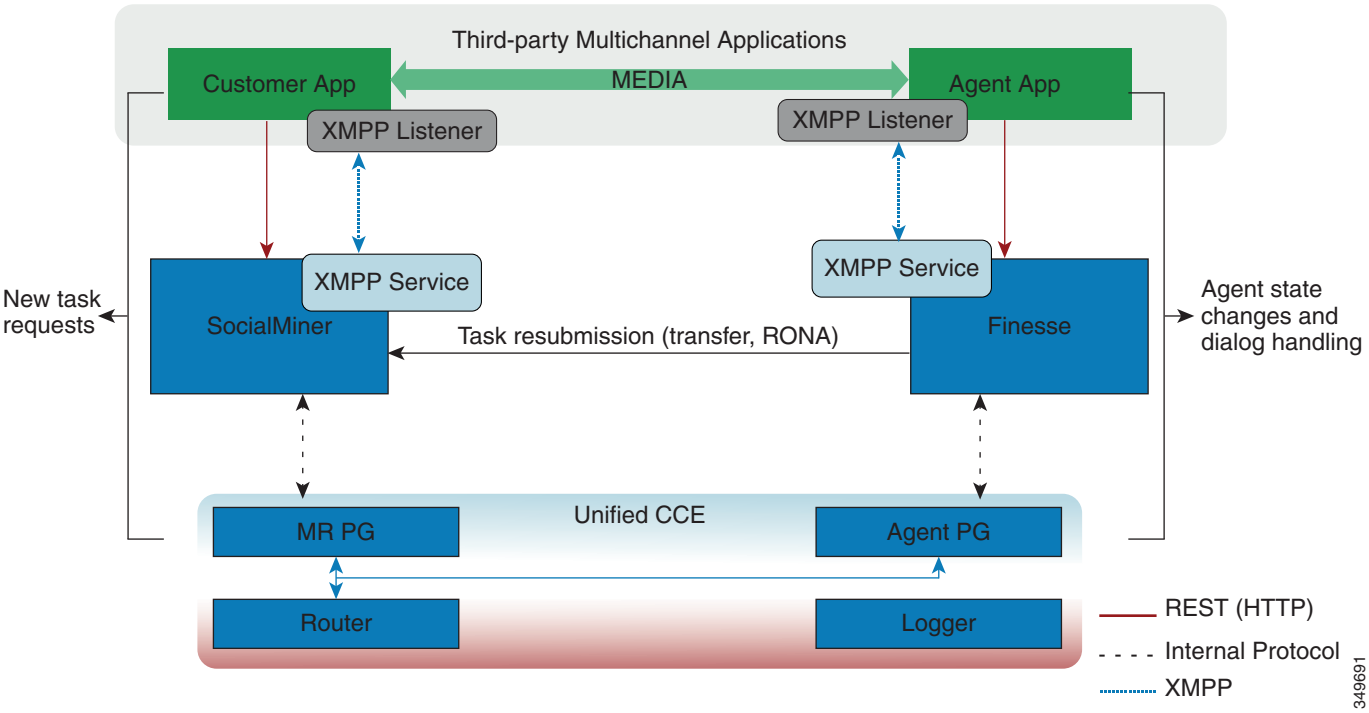
音声通話、電子メール、チャットなどの組み合わせを処理するようにエージェントを設定できます。たとえば、エージェントが音声、電子メール、およびチャットを処理する場合、3 種類のメディア ルーティング ドメイン（MRD）でスキル グループまたはプレシジョン キューのメンバーとしてエージェントを設定できます。メディアを問わず、ビジネス ルールに基づいてこれらのエージェントに要求を送信するようにルーティング スクリプトを設計できます。複数の MRD にサインインしたエージェントは、タスク単位でメディアを切り替えることができます。

ユニバーサル キューイング API は、Unified CCE でサードパーティのマルチチャネル タスクを要求、キューイング、ルーティング、および処理する標準的な方法を提供します（図 22-1 を参照）。

コンタクト センターの顧客またはパートナーは、ユニバーサル キューを使用するために、Cisco SocialMiner および Cisco Finesse API を使用したアプリケーションを開発できます。SocialMiner Task API は、アプリケーションが音声以外のタスク要求を Unified CCE に送信できるようにします。Finesse API は、エージェントがさまざまなタイプのメディアにサインインし、タスクを処理できるようにします。エージェントは各メディアにサインインし、独立してそれぞれの状態を管理できます。

シスコ パートナーは、Cisco DevNet（https://developer.cisco.com/site/devnet/home/index.gsp）で入手できるサンプル コードをこれらのアプリケーションを構築するためのガイドとして使用できます。

図 22-1　サードパーティのマルチチャネル アプリケーション ソリューション コンポーネント用のユニバーサル キュー



SocialMiner とユニバーサル キュー

サードパーティのマルチチャネル アプリケーションは、SocialMiner の Task API を使用して、音声以外のタスクを Unified CCE に送信します。この API は、SocialMiner タスク フィード、キャンペーン、および通知と連携し、コンタクト センターにタスクの要求を渡してルーティングさせます。

Task API は、タスクの要求にコール変数と拡張コール コンテキスト（ECC）変数の使用をサポートします。これらの変数は、チャット ルームの URL や電子メールの処理といったメディアの属性など、顧客固有の情報を要求で送信するために使用されます。

Unified CCE とユニバーサル キュー

Cisco Unified CCE は、ユニバーサル キューの一部として以下の機能を提供します。

- タスクの要求を処理します。
- タスクの要求の待機時間を予測します。
- エージェントが選択されたときに SocialMiner に通知します。
- スキル グループまたはプレシジョン キューのルーティングを使用して、エージェントにタスクの要求をルーティングします。
- メディア全体のコンタクト センター アクティビティについて報告します。

Finesse とユニバーサル キュー

Cisco Finesse は、Media API および Dialog API 経由でユニバーサル キュー機能を提供します。Media API の場合、サードパーティのマルチチャネル アプリケーションを使用するエージェントは、以下の処理が可能です。

- 複数の MRD にサインインします。
- 複数の MRD で状態を変更します。

Dialog API の場合、サードパーティのマルチチャネル アプリケーションを使用するエージェントは、複数の MRD からのタスクを処理できます。

管理

Cisco Contact Center 製品には、管理の機能が組み込まれています。たとえば、Unified CCE は、Unified CCE とともにインストールされる Configuration Manager ツール、または Contact Center Enterprise 環境の主な管理タスクを簡単に実行できる Web ベースの管理ツールを使用して管理できます。また、REST API では、サードパーティの開発者が管理およびサポート タスクの多くを管理できるアプリケーションを作成できます。

Unified CVP は、Operations, Administration, Maintenance, and Provisioning（OAMP）と呼ばれる Unified CVP Operations Console を使用して管理できます。

さらに、エージェントや機器の管理などの基本的な管理機能を実行するための操作および手順を簡素化するために、Cisco Unified Contact Center Management Portal（Unified CCMP）を配置できます。Unified CCMP は、コンタクト センターのシステム管理者、ビジネス ユーザ、およびスーパーバイザ向けに設計されたブラウザベースの管理アプリケーションです。Cisco Unified Contact Center Enterprise（Unified CCE）、Unified Communications Manager（Unified CM）、および Unified Customer Voice Portal（Unified CVP）機器を重ね合わせた緻密なマルチテナントのプロビジョニング プラットフォームです。

レポート

Cisco Unified Intelligence Center は、Cisco Contact Center ソリューション用の主要なレポーティング ツールです。Unified CCE、Unified CCX、および Unified CVP でサポートされています。このプラットフォームは Web ベースのアプリケーションであり、多数の Web 2.0 機能、高いスケーラビリティ、優れたパフォーマンス、および高度な各機能（他の Cisco Unified Communications 製品やサードパーティ製データ ソースからのデータを統合する機能など）を提供します。

Cisco Unified Intelligence Center は、データベース（Unified CCE Administration & Data Server データベースや Unified CVP Reporting Informix データベースなど）からソース データを取得します。次にレポートが生成されて、レポーティング クライアントに提供されます。

マルチチャネル サポート

Cisco Unified Enterprise ソリューションでは、マルチチャネル サポートのための Web インタラクションおよび電子メール インタラクションをサポートしています。Cisco Unified Web Interaction Manager（Unified WIM）テクノロジーにより、ほとんどすべての Web ブラウザから通信を確立できます。Cisco Unified E-Mail Interaction Manager（Unified EIM）は、着信電子メール ルーティング、自動電子メール応答またはエージェント介入による電子メール応答、リアルタイム レポーティングと履歴レポーティングを提供し、エージェント、スーパーバイザ、管理者、ナレッジ ベース管理者向けのロールベースの階層権限を提供します。

これらの製品の設計情報については、次の URL で入手可能な『*Cisco Unified E-Mail and Web Interaction Manager Solution Reference Network Design Guide*』を参照してください。

https://www.cisco.com/en/US/products/ps7236/products_implementation_design_guides_list.html

録音とサイレント モニタリング

Cisco Unified Contact Center ソリューションでは、次の各メカニズムに基づいて、録音とサイレント モニタリングの機能が提供されます。

- Cisco スイッチの SPAN 機能

  この機能により、ネットワーク トラフィックは、Cisco コンタクト センター サーバが接続されている宛先ポートに複製されます。

- Cisco IP Phone のビルトイン ブリッジ（BIB）による Unified CM およびメディア複製

  このオプションを使用した場合は、録音フローのセットアップ中に Unified CM が呼び出され、それらのフローに対するコール アドミッション制御を実行できるようになります。

- Cisco Unified Border Element ゲートウェイによるメディア フォーキング

録音中およびモニタ中のコールの詳細については、コール録音とモニタリング（23-1 ページ）の章を参照してください。

Contact Sharing

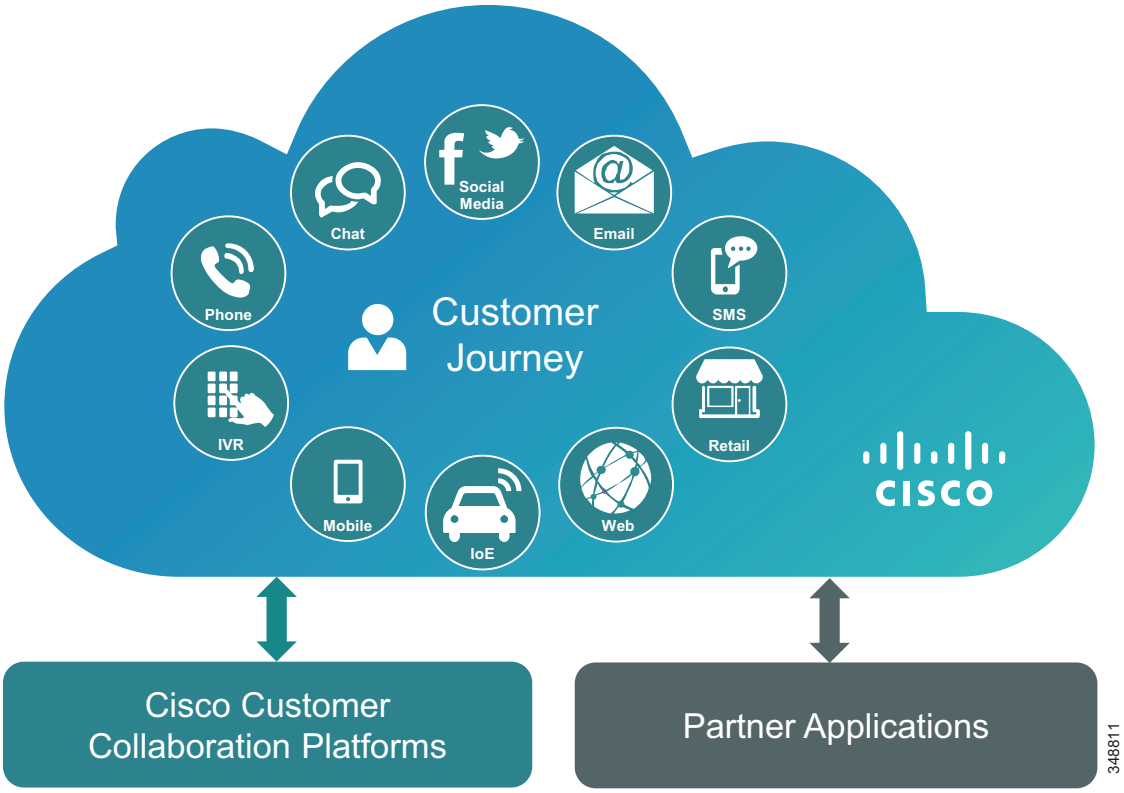
Contact Sharing を使用すると、大規模なコンタクトセンターの規模をさらに拡大できます。一元化されたセルフサービス（IVR ICM 配置モデル）は、Contact Sharing ルーティング ノードを使用してコールを 2 つの Unified CCE インスタンスに分散し、水平拡大を実現します。ライブ データは、Contact Sharing の条件であり、Contact Sharing を使用する前にインストールおよび設定する必要があります。また、Contact Sharing は、IVR Cisco Intelligent Contact Management（ICM）配置モデルを導入で有効にする必要があります。Contact Sharing の詳細については、次の Web サイトで入手可能な『*Cisco Unified Contact Center Enterprise Features Guide*』の最新バージョンを参照してください。

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html

コンテキスト サービス

コンテキスト サービスは、カスタマー ジャーニー データのリポジトリを提供するクラウドベースのストレージ サービスです。Cisco Contact Center の顧客は、その他の Cisco Customer Collaboration 製品との統合や、サードパーティ統合用の API を利用して、シームレスなオムニチャネル エクスペリエンスを実現できます（図 22-2 を参照）。

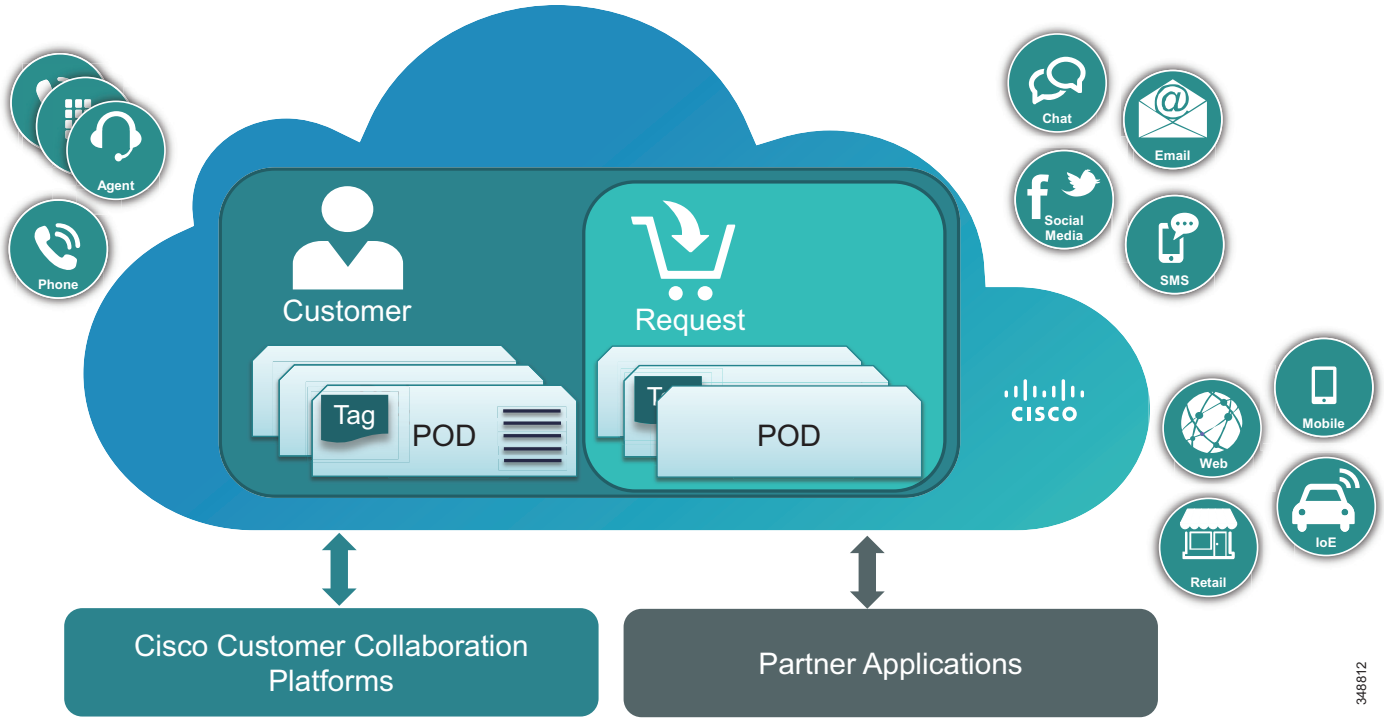
図 22-2　　コンテキスト サービスの統合



コンテキスト サービスにより、アプリケーションは、カスタマー ジャーニー アクティビティを読み書きできます。Cisco Contact Center の顧客（このセクションでは「*ビジネス*」と呼びます）は、Cisco Contact Center プラットフォーム内からコンテキスト サービスにアクセスできます。Cisco Contact Center プラットフォームでは、コンタクト センターのインタラクションに関するコンテキスト データのポストに対応しており、オプションでそのように設定できます。

コンテキスト サービスは、このデータを Piece of Data（POD）と呼ばれる要素に保存します。POD は、メディア（音声録音など）を除き、コンシューマ インタラクションに関するあらゆるメタデータを保存できます。ビジネスは、POD に保存するフィールド（メタデータ）および各フィールドのデータ プライバシー レベルを選択します。POD は、顧客が編成でき、要求と呼ばれるインタラクションのコレクションの一部としてグループ化することができます（図 22-3 を参照）。コンテキスト サービスは、関連付け、傾向分析、分析を実施するために POD をグループ化するタギング機能もあります。

図 22-3　　Piece of Data (POD) と要求



コンテキスト サービスは、Cisco Intercloud にホストされます。Cisco Intercloud は、シスコとパートナーのデータセンターのエコシステムであり、シスコ データ センター チームがグローバルに管理および運用しています。コンテキスト サービスが従うデータ プライバシー モデルは、各ビジネスによるデータへのアクセスを制御する Cisco Spark に非常に近いものになっています。データは、クライアントでオンプレミスに暗号化/復号化され、シスコ データセンターに暗号化された BLOB として保存されます。ビジネスは、暗号キー（キーストア）を自身の宅内にホストすることもできます。これは貴重品を銀行の貸金庫（ロッカー）に預けることに似ています。貴重品が銀行内にあっても、顧客が貸金庫の鍵を持ち、貸金庫へのアクセスを管理します。これはデータ プライバシーに対する新しいアプローチであり、プライベート クラウドをホスティングする際のオーバーヘッドなしで管理できます。コンテキスト サービスは、データ プライバシーの分類レベルを提供するため、ビジネスは顧客の個人識別情報（PII）をその他の暗号化されたデータとは分離して保存できます。それによって、ビジネスはサードパーティの分析ベンダーに対して顧客の PII データへのアクセスを提供しなくても、自身の暗号化されたデータへの管理されたアクセスを提供できます。

コンテキスト サービスは、ユニバーサル キュー タスクの連絡先データを保存できます。コンテキスト サービスが有効な場合、SocialMiner は受信したタスクの要求からデータを選択してクラウドの POD に保存します。POD のメディア タイプはタスクの要求で指定できます。メディア タイプを指定しない場合は、メディア タイプ **event** が POD に設定されます。

コンテキスト サービスは、Cisco Collaboration Management（Atlas）によって管理されます。Atlas は、Cisco Spark を含むすべてのシスコ クラウド コラボレーション製品のための管理ポータルです。シスコ パートナーおよびビジネスは、Collaboration Management を使用してオンプレミス クライアントに接続したり、POD データ モデル（フィールド）を管理したり、POD の使用状況をモニタしたりします。

コンテキスト サービスは、オープンな API と Java/JS SDK を提供して、技術パートナーが自分のアプリケーションとコンテキスト サービスを統合しやすくします。

シスコのコンテキスト サービスの詳細については、https://www.cisco.com/go/srnd から入手できるシスコ ユニファイド コンタクト センターの設計ガイドを参照してください。

Cisco Virtualized Voice Browser

Cisco Virtualized Voice Browser（Cisco VVB）は、VoiceXML ドキュメントを解釈するためのプラットフォームを提供します。新しいコールがコンタクト センターに到着すると、VVB は VoIP エンドポイントを表す VXML ポートを割り当てます。Cisco VVB は Cisco Unified Customer Voice Portal（Unified CVP）VXML サーバに HTTP 要求を送信します。Unified CVP VXML サーバは HTTP 要求に対応して要求を実行し、動的に生成された VXML ドキュメントを送信します。Cisco VVB の詳細については、次の Web サイトにある『*Installing and Configuring Guide for Cisco HCS*』の最新版で、Cisco Virtualized Voice Browser の設計上の考慮事項と設定オプションについて参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html

コンタクト センター配置モデル

この項では、Cisco Unified Contact Center ソリューションの配置に使用されるさまざまな設計モデルについて説明します。これらの配置モデルの詳細については、https://www.cisco.com/go/srnd から入手できるシスコ ユニファイド コンタクト センターの設計ガイドを参照してください。

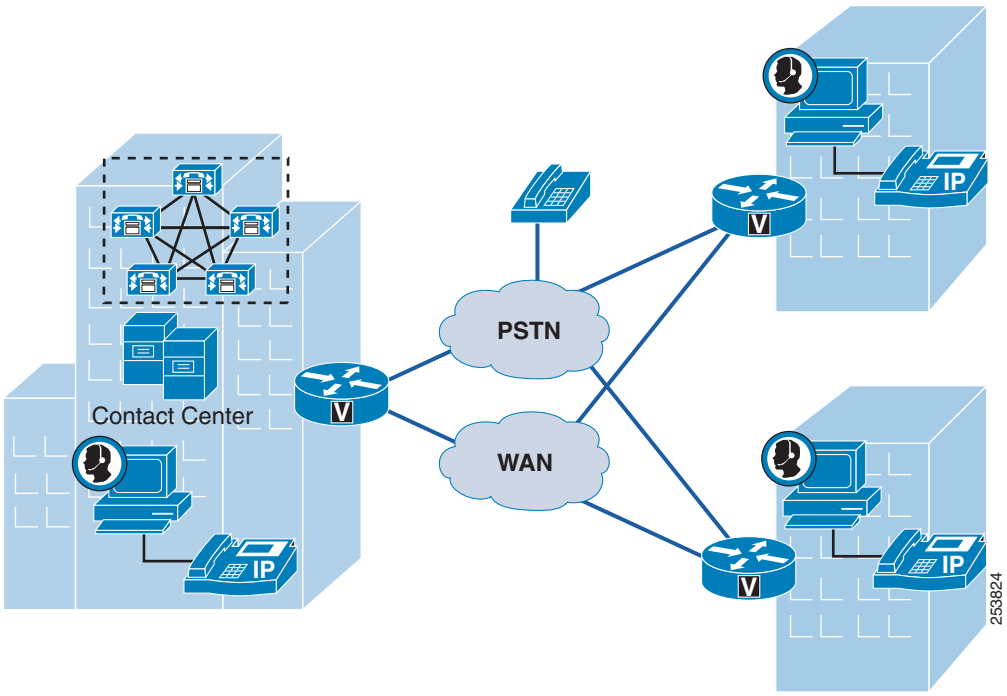
単一サイト コンタクト センター

この配置では、呼処理エージェント、音声ゲートウェイ、コンタクト センター アプリケーションなどのすべてのコンポーネントが同じサイトに存在します。エージェントとスーパーバイザも、そのサイトに配置されます。単一サイト配置モデルの主要なメリットは、WAN 接続が不要なので、低帯域幅のコーデック（G.729、トランスコーダ、RTP ヘッダー圧縮（cRTP）、コール アドミッション制御など）を使用する必要がないことです。

集中型呼処理を使用するマルチサイト コンタクト センター

集中型呼処理を使用するマルチサイト配置は、単一の呼処理クラスタで構成されます。このクラスタは、多数のリモート サイトにサービスを提供し、IP WAN を使用します。また、Cisco Contact Center アプリケーション（Unified CCE、Unified CCX、Unified CVP）は通常、管理の全体的なコストを削減するために集中化されます。図 22-4 はこのタイプの展開を示しています。

図 22-4　　集中型呼処理を使用するマルチサイト コンタクト センター



このタイプの配置では、エージェントまたは音声ゲートウェイがリモート サイトに存在しているため、サイト間の帯域幅の要件を考慮することが重要です。また、コール アドミッション制御や Quality of Service（QoS）などを慎重に設定することも重要です。Unified Communications ソリューションの全般的な設計上の考慮事項の詳細については、コラボレーションの配置モデル（10-1 ページ）の章を参照してください。

Unified Communications システムでのコンタクト センター配置には、通常、さらに次のような帯域幅の要件があります。

- エージェントが処理するトラフィック量のほうが、標準的なユーザが処理するトラフィック量よりも多いこと、その結果、音声およびシグナリング トラフィックもエージェントのほうが多いこと。
- エージェントとスーパーバイザが、画面ポップアップ、レポート、統計などの機能が搭載されたデスクトップを使用していること。この場合、エージェントまたはスーパーバイザのデスクトップとコンタクト センター サーバの間のデータ トラフィックが発生します。また、たとえばエージェントまたはスーパーバイザがリモートにあり、中央にあるサーバからデータをプルする場合は、帯域幅の計算でレポーティング情報を考慮する必要があります。詳細およびガイダンスについては、https://www.cisco.com/go/srnd から入手できる、該当する Cisco コンタクト センター製品の設計ガイドを参照してください。
- IVR ソリューションのタイプによっては、音声ゲートウェイと IVR システムの間にトラフィックが発生することがあります。たとえば、音声ゲートウェイが分散されており、Unified IP IVR を使用するリモート サイトに配置された音声ゲートウェイにコールが到着した場合、音声ゲートウェイと Unified IP IVR の間に WAN 経由の音声トラフィックが発生します。Unified CVP を使用すると、コールをリモート サイトでキューイングできます。この場合、VXML ゲートウェイがコール トリートメントとキューイングを提供し、それにより WAN 経由の IVR の音声トラフィックを回避して、全体的な WAN 帯域幅要件を低減します。

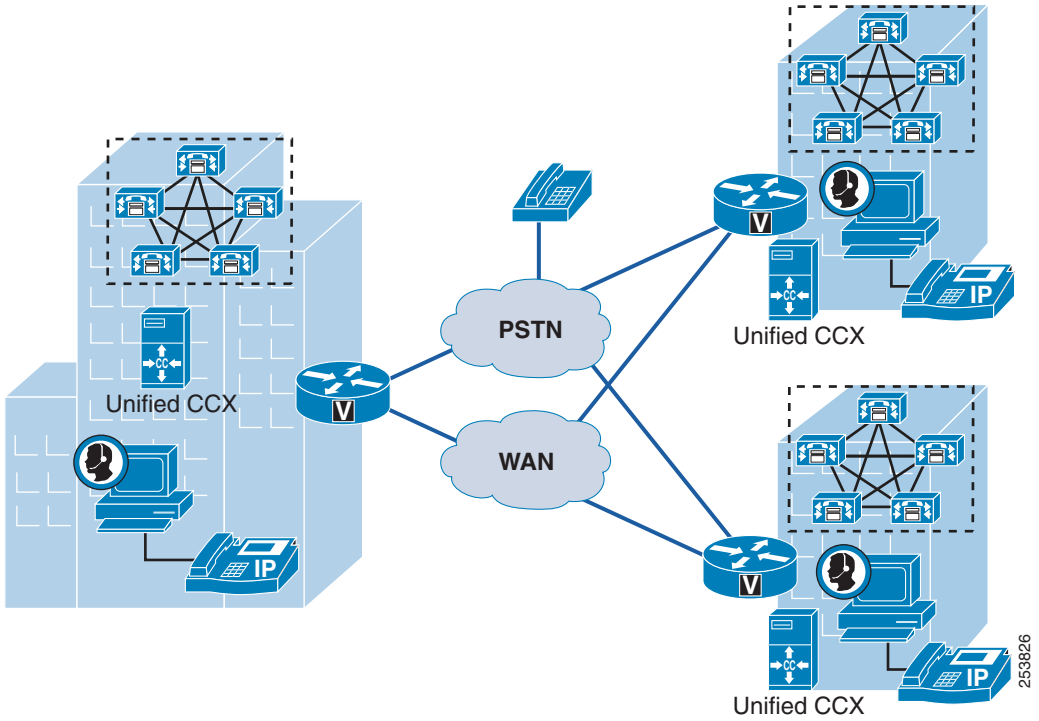
リモート エージェント（たとえば、自宅勤務のエージェントなど）も、Cisco Unified Contact Center でサポートされます。主に 2 つのソリューションがあります。1 つめのソリューションでは、エージェントは、ブロードバンド インターネット接続により中央サイトに接続された IP Phone を使用する必要があります。このソリューションでは、電話機は Cisco Unified Contact Center アプリケーションにより CTI 制御されます。2 つめのソリューションは、Cisco Unified Mobile Agent に基づいています。これにより、エージェントは、携帯電話などの任意の PSTN 電話機を使用してコール センターに参加できます。

分散型呼処理を使用するマルチサイト コンタクト センター

分散型呼処理を使用するマルチサイト配置は、複数のサイトで構成されます。それぞれのサイトに、IP WAN に接続された独自の呼処理クラスタがあります。この項では、各 Unified CM クラスタにエージェントが登録されていることを前提としています。

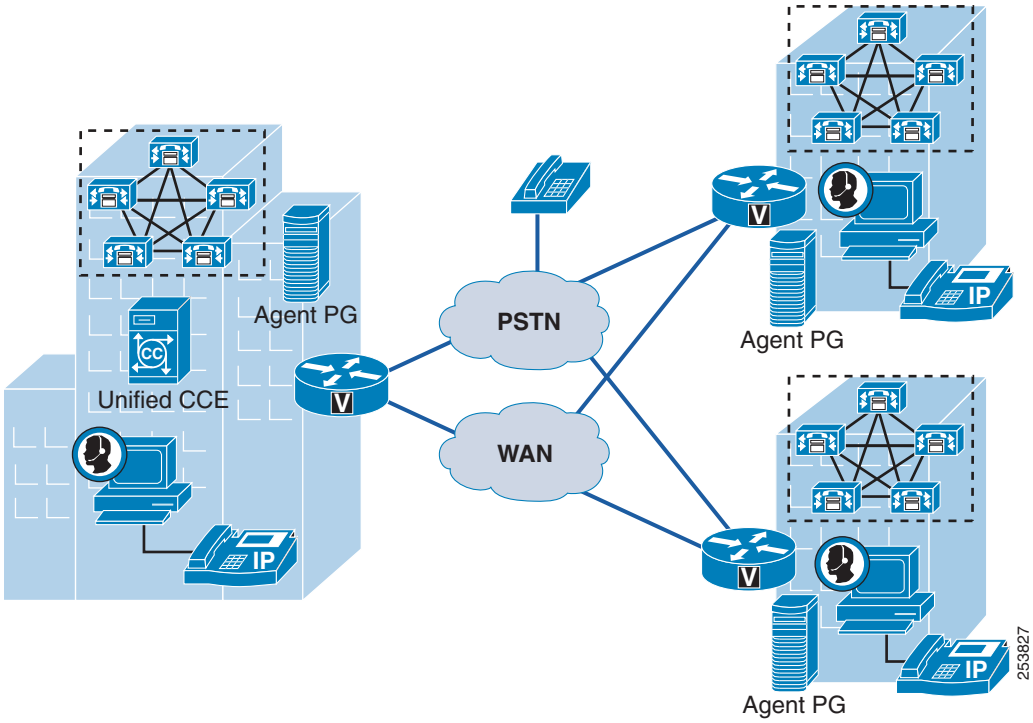
1 つの Unified CCX 配置を複数の Unified CM クラスタ間で共有することはできません。図 22-5 に示すように、各 Unified CM クラスタにそれぞれの Unified CCX 配置が必要です。

図 22-5　　分散型呼処理を使用するマルチサイト Unified CCX 配置



Unified CCE の要件は、Unified CCX の要件とは異なります。1 つの Unified CCE システムは、複数の地理的なロケーションに分散された複数の Unified CM クラスタにまたがることができます。Unified CCE Agent PG は、それぞれの Unified CM クラスタ ロケーションにインストールする必要があります。Unified CCE Central Controller（Call Router + Logger）から物理的にリモートにすることもできます。図 22-6 に、このタイプの配置を示し、Agent PG の位置を示します。

図 22-6　　分散型呼処理を使用するマルチサイト Unified CCE 配置



複数のコンタクト センター配置が必要な場合は、Unified ICM を介してこれらの配置を接続します。このためには、親子配置モデルを使用して、単一の仮想コンタクト センターを構成します。親子モデルを使用すると、すべてのコンタクト センター配置にわたってエンタープライズ キューイングとエンタープライズ レポーティングを実行できるなど、複数のメリットがあります。また、サイトが完全な冗長構成となるため、スケーラビリティが向上します。親子モデルの詳細については、次の各マニュアルを参照してください。

- 次の URL で入手可能な『*Cisco Unified Contact Center Enterprise Design Guide*』

  https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html

- 次の URL で入手可能な『*Cisco Contact Center Gateway Deployment Guide for Cisco Unified ICME/CCE*』

  https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html

分散型呼処理を使用するマルチサイト配置でも、集中型呼処理を使用するマルチサイト モデルの場合と同様に、QoS、コール アドミッション制御、コーデックなどを慎重に設定する必要があります。

IP WAN を介したクラスタリング

この配置モデルでは、単一の Unified CM クラスタが、QoS 機能が有効になっている IP WAN により接続された複数のサイトにわたって配置されます。このモデルを使用すると、Cisco Unified Contact Center ソリューションを配置できます。実際には、Cisco Unified Contact Center コンポーネント自体を WAN 経由でクラスタ化することもできます。

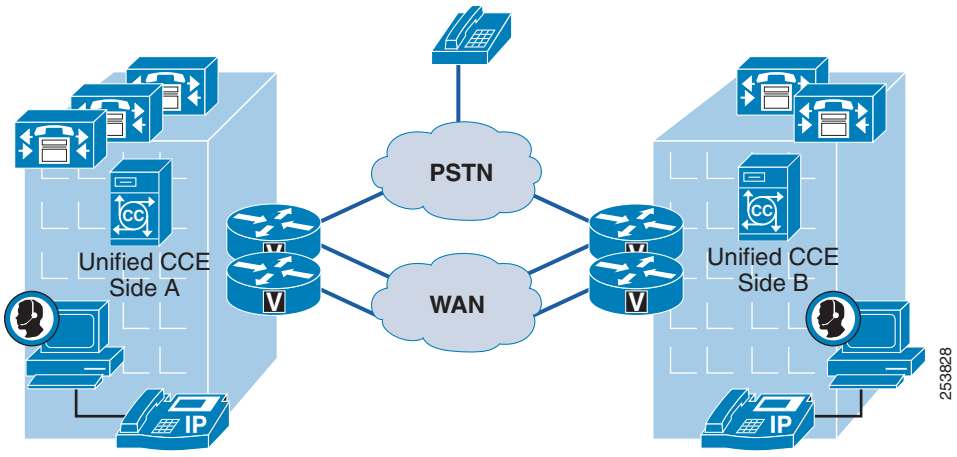
たとえば、Unified CCE を使用すると、サイト A コンポーネントを Unified CCE のサイド B コンポーネントからリモートにし、IP WAN 接続によってサイド B コンポーネントから分離できます（Unified CCE のハイ アベイラビリティの詳細については、コンタクト センターのハイ アベイラビリティ（22-19 ページ）を参照してください）。このタイプの配置には、次の設計上の考慮事項が適用されます。

- 2 つのサイト間の IP WAN は、単一障害点のないハイ アベイラビリティ構成にする必要があります。たとえば、IP WAN リンク、ルータ、およびスイッチは冗長構成にする必要があります。WAN リンク冗長性は、複数の WAN リンクを使用して、または柔軟性に優れていて冗長性を備えている SONET リングを使用して実現できます。
- Agent Peripheral Gateway（PG）および接続先の CTI Manager はデータセンターと同じ場所に設置する必要があります。Unified CCE を配置する際は、大量のリダイレクト トラフィックと転送トラフィック、および追加の CTI トラフィックがあるため、Unified CM ノード間の Intra-Cluster Communication Signaling（ICCS）帯域幅の要件が高くなります。
- 1 つのサイトに Unified CCE プライマリ ノードと Unified CM プライマリ ノードを配置して、別のサイトに Unified CCE セカンダリ ノードと Unified CM セカンダリ ノードを配置した場合、2 つのサイト間の最大遅延は、Unified CM の遅延要件（ラウンド トリップ時間 [RTT]）が 80 ms）によって決まります。ただし、Unified CCE ノードが Unified CM ノードと異なる場所にある場合は、Unified CCE 冗長ノード間の遅延がさらに大きくなる可能性があります。

図 22-7 は、WAN 経由のクラスタリングを使用する Unified CCE の配置を示しています。詳細については、次の Web サイトで入手可能な『*Cisco Unified Contact Center Enterprise Design Guide*』を参照してください。

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html

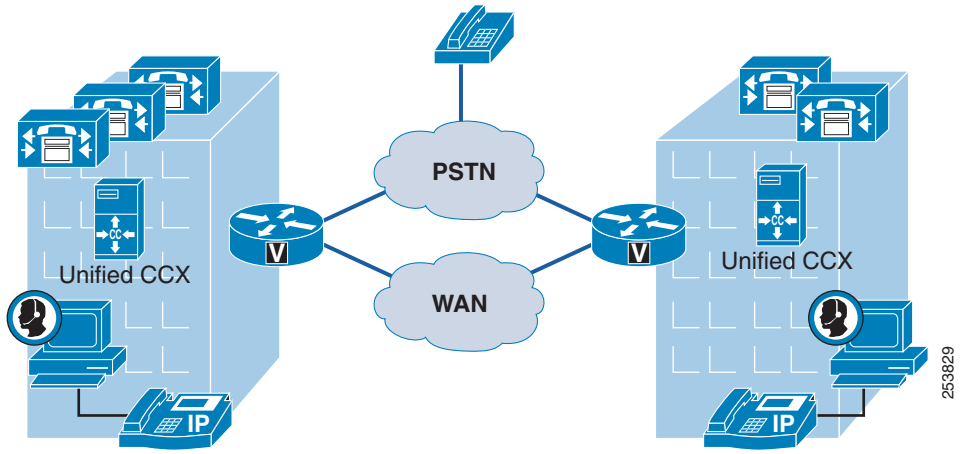
図 22-7　　WAN 経由のクラスタリングを使用する Unified CCE 配置



Unified CCX ソリューションおよび Unified IP IVR ソリューションを使用すると、Unified CCX プライマリ ノードまたは Unified IP IVR プライマリ ノードをバックアップ ノードからリモートにすることもできます。Unified CCX 配置の要件は、Unified CCE 配置の要件とは異なります。たとえば、Unified CCX では冗長な WAN リンクは必要ありません。また、Unified CCX のプライマリ ノードとバックアップ ノードの間の最大遅延は、80 ms RTT です。図 22-8 はこのタイプの展開を示しています。詳細については、次の Web サイトで入手可能な『*Cisco Unified Contact Center Express Design Guide*』を参照してください。

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-implementation-design-guides-list.html

図 22-8　　WAN 経由のクラスタリングを使用する Unified CCX 配置



コンタクト センターを配置する際の設計上の考慮事項

この項では、コンタクト センターを配置する際の次の主要な設計上の考慮事項について簡単に説明します。

- コンタクト センターのハイ アベイラビリティ（22-19 ページ）
- 帯域幅、遅延、および QoS に関する考慮事項（22-19 ページ）
- コール アドミッション制御（22-21 ページ）
- Unified CM との統合（22-21 ページ）
- コンタクト センターのその他の設計上の考慮事項（22-22 ページ）

コンタクト センターのハイ アベイラビリティ

すべての Cisco Unified Contact Center 製品は、ハイ アベイラビリティを提供します。たとえば、Unified CCX または Unified IP IVR の場合、2 番目に同一の Unified CCX または Unified IP IVR ノードを追加することで、ハイ アベイラビリティが実現されます。第 2 ノードはプライマリ ノードと同じデータセンターに配置でき、地理的冗長性が必要な場合は、プライマリ ノードから WAN を介してプライマリ ノードとは異なるデータセンターに第 2 ノードを配置できます（IP WAN を介したクラスタリング（22-17 ページ）を参照）。1 つのノードがアクティブ ノードとなり、すべての呼処理を取り扱います。他のノードはスタンバイ モードとなり、プライマリ ノードに障害が発生したときだけアクティブになります。また、Unified CVP は、複数の Unified CVP ノード、音声ゲートウェイ、VXML ゲートウェイ、SIP プロキシなどを使用するハイ アベイラビリティ配置をサポートしています。

Unified CCE では、ほとんどのコンポーネントは冗長構成にする必要があります。冗長インスタンスは、サイド A インスタンスおよびサイド B インスタンスと呼ばれます。たとえば、Call Router A および Call Router B は、2 つの異なる仮想マシン上で稼働する Call Router モジュール（プロセス）の冗長インスタンスです。この冗長構成は、*デュプレックス モード*とも呼ばれます。Call Router は 2 つのインスタンスで同期して実行されます。つまり、すべてのコールは、デュプレックス インスタンスの両サイドで処理されています。他のコンポーネント（ペリフェラル ゲートウェイなど）は、ホットスタンバイ モードで稼働します。つまり、常にペリフェラル ゲートウェイのうち 1 つだけがアクティブな状態となります。

Unified Contact Center コンポーネントそのものを冗長構成にするだけでなく、Unified Contact Center コンポーネントと Unified CM との統合を冗長構成にすることもできます。たとえば、Unified CCX ノードまたは Unified IP IVR ノードそれぞれをプライマリ CTI Manager に接続し、さらにプライマリ CTI Manager の障害発生時に備えてバックアップ CTI Manager にも接続できます。Unified CCE を使用して、PG サイド A をプライマリ CTI Manager に接続し、冗長な PG サイド B をセカンダリ CTI Manager に接続することで、1 つの CTI Manager に障害が発生した場合のハイ アベイラビリティが実現されます。

詳細については、https://www.cisco.com/go/srnd から入手できるシスコ ユニファイド コンタクト センターの設計ガイドを参照してください。

帯域幅、遅延、および QoS に関する考慮事項

この項では、マルチサイト コンタクト センター配置における WAN 帯域幅のプロビジョニング方法を、さまざまなタイプの呼制御トラフィックおよびリアルタイム音声トラフィックを考慮に入れて説明します。適切に帯域幅プロビジョニングおよび QoS を実装することは、コンタクト センター配置の成否を決める重要な要素であるため、遅延および QoS パラメータについて理解しておくことが重要です。

帯域幅のプロビジョニング

コンタクト センター ソリューションは、次の主要なタイプのトラフィックに対応できる十分な WAN 帯域幅を必要とします。

- 着信ゲートウェイと IVR システムの間の音声トラフィック。Unified IP IVR を使用する場合、Unified IP IVR クラスタが中央に配置され、PSTN ゲートウェイがリモートに配置されていると、WAN 経由の音声トラフィックが発生します。Unified CVP を使用する場合、エッジでコールをキューイングできます。このため、音声トラフィックをリモート サイトに対してローカルに保ち、WAN リンクを介する音声トラフィックを回避できます。ビデオ キューイングは Unified CVP Video in Queue（ViQ）機能でもサポートされ、その発信者とビデオ メディア サーバ間のビデオ トラフィックを考慮します。
- 着信ゲートウェイとエージェントの間の音声トラフィック。または内線コールの発信者とエージェントの間の音声トラフィック。コンタクト センター配置がビデオをサポートしていれば、発信者とエージェントの間にビデオ トラフィックが発生することがあります。
- 音声およびビデオ シグナリング トラフィック。これは通常、着信ゲートウェイまたは発信者エンドポイントと Unified CM の間、およびエージェント電話機と Unified CM の間のシグナリング トラフィックに対応します。
- Unified CVP が配置されている場合の VXML ゲートウェイ トラフィック。このトラフィックには、メディア サーバからのメディア ファイル取得や、VXML サーバとの間で交換される VXML ドキュメントが含まれます。
- Finesse エージェントまたはスーパーバイザ デスクトップと Finesse ガジェットをホストするアプリケーション サーバ間のデータ トラフィック。
- レポーティング ユーザと Unified Contact Center Reporting サーバの間のレポーティング トラフィック。
- Unified Contact Center サーバ間のトラフィック（サーバどうしがリモートに配置されている場合）。たとえば、このタイプのトラフィックは、IP WAN 経由またはマルチサイトでのクラスタリングや、Unified CCE Central Controller からリモートの PG を使用して分散呼処理を行う場合に発生します。
- 大量のリダイレクト トラフィックと転送トラフィック、および追加の CTI トラフィックによって Unified CM サブスクライバ間に発生する、追加の Intra-Cluster Communication Signaling（ICCS）トラフィック。
- 録音とサイレント モニタリングによる音声トラフィック。ソリューションによっては、エージェントとの会話をサイレントにモニタリングまたは録音する目的で、1 つまたは 2 つの RTP ストリームを送信できます。

帯域幅の計算とガイドラインについては、https://www.cisco.com/go/srnd から入手できるシスコ ユニファイド コンタクト センターの設計ガイドを参照してください。

遅延

エージェントおよびスーパーバイザは、呼処理コンポーネントおよびコンタクト センターからリモートな場所に配置できます。技術的には、Finesse サーバと Finesse デスクトップの間の遅延は、タイムアウト値が高くなるため、非常に大きくなる可能性があります。遅延時間が長いと、ユーザ エクスペリエンスに影響し、混乱が発生したり、ユーザに許容されない状態となることがあります。たとえば、電話が鳴り出していても、デスクトップが更新されるのはあとになってからということがあります。

コンタクト センターのコンポーネントと呼処理コンポーネントの間、およびコンタクト センターのコンポーネント間の遅延の要件は、コンタクト センターのソリューションによって異なります。たとえば、Unified CCX 冗長ノードは互いにリモートの場所に配置でき、最大遅延は 80 ms RTT です。Unified CCE を使用する場合、Unified CCE コンポーネントと Unified CM の間、または Unified CCE 各コンポーネント間の最大遅延は、80 ms RTT より大きくなります。

詳細については、https://www.cisco.com/go/srnd から入手できるシスコ ユニファイド コンタクト センターの設計ガイドを参照してください。

QoS

他の Unified Communications コンポーネントを使用する配置と同様に、コンタクト センター配置でも、時間に依存するトラフィックや重要なトラフィックを優先させるために、Quality of Service（QoS）の設定が必要となります。コンタクト センター環境における音声および音声シグナリング用の QoS マーキングは、他の Unified Communications 配置の場合と同じです。コンタクト センターに固有のトラフィックは、特定の QoS マーキングを使用してマークする必要があります。たとえば、Unified CCE プライベート ネットワークのトラフィックには、AF31 としてマークする必要のあるものや、AF11 としてマークする必要のあるものがあります。ユニファイド コンタクト センター ソリューションごとの QoS マーキングの推奨値および QoS 設計ガイドラインについては、https://www.cisco.com/go/srnd から入手できる、該当するシスコ ユニファイド コンタクト センター設計ガイドを参照してください。

コール アドミッション制御

他の Unified Communications コンポーネントを使用する配置と同様に、コンタクト センター配置でも、コール アドミッション制御を慎重にプロビジョニングする必要があります。帯域幅管理（13-1 ページ）の章に記載されているメカニズムが、コンタクト センター環境にも適用されます。

コール アドミッション制御の計算では、サイレント モニタリングと録音に関連する音声トラフィックが考慮されないことがあります。たとえば、Unified CM によるサイレント モニタリングと録音で発生する音声トラフィック（電話機で分岐（転送）される音声トラフィック）は、コール アドミッション制御の計算で適切に考慮されますが、デスクトップベース（エージェント IP Phone の背面に接続されているデスクトップ）のサイレント モニタリングで発生する音声トラフィックは考慮されません。

Mobile Agent および Unified CVP のコール アドミッション制御には、特別の考慮事項が適用されます。詳細については、https://www.cisco.com/go/srnd から入手できるシスコ ユニファイド コンタクト センターの設計ガイドを参照してください。

Unified CM との統合

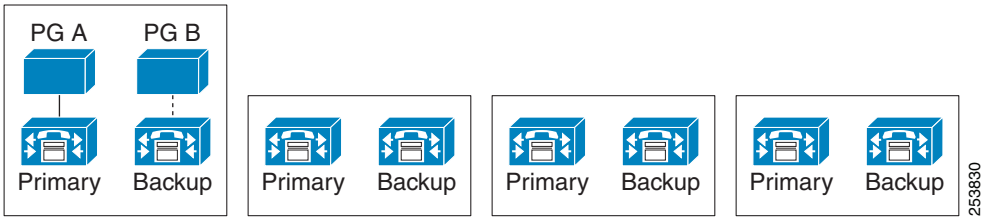
Cisco Unified Contact Center コンポーネントを Unified CM と統合する際は、次の設計上の考慮事項が適用されます。

- 管理およびアップグレードの目的で、コンタクト センター配置とコンタクト センター以外の配置に対しては、別々の Unified CM クラスタを使用することを推奨します。別々のクラスタを使用できない場合は、コンタクト センターのアプリケーションとコンタクト センター以外のアプリケーションに別々の Unified CM サブスクライバ ノードを使用することを推奨します。
- コンタクト センター配置で Unified CM に対して 2:1 冗長スキームを使用することは推奨しません。高い復元性と高速なアップグレードを実現するために、1:1 の冗長構成を使用してください。

- Unified CM と Unified CCX、Unified IP IVR、または Unified CCE の間の統合は、JTAPI を介して行います。Unified CCX クラスタはプライマリ CTI Manager に接続します。また、セカンダリ CTI Manager へのバックアップ接続もあります。Unified CCE を使用する場合、Agent PG は 1 つだけの CTI Manager に接続します。冗長な Agent PG は、バックアップ CTI Manager だけに接続します。プライマリ CTI Manager に障害が発生すると、プライマリ Agent PG にも障害が発生し、フェールオーバーがトリガーされます。
- 1 つの PG で、集中型配置におけるすべての Unified CM サブスクライバ ペアにおけるエージェント電話機を制御およびモニタできます（図 22-9 を参照）。
- 複数の Unified CCX を単一の Unified CM クラスタと統合することは可能です。

Unified CM 統合の詳細については、https://www.cisco.com/go/srnd から入手できるシスコ ユニファイド コンタクト センターの設計ガイドを参照してください。

図 22-9　　1 つの Agent PG と 4 つの Unified CM サブスクライバ ペアを使用する配置



コンタクト センターのその他の設計上の考慮事項

下記で示す状況においては、それぞれ設計上の考慮事項が追加で適用されます。

- Unified CVP ではエッジでのキューイングが可能であるため、Unified IP IVR ではなく Unified CVP を配置すれば、マルチサイト配置の帯域幅の要件を小さくできます。
- Cisco Unified Contact Center 製品およびコンポーネントのほとんどは、VMware をベースにした仮想化環境にインストールできます。
- シナリオによっては、メディア ターミネーション ポイント（MTP）リソースが必要となることもあります。たとえば、Mobile Agent と SIP トランク経由の着信コールを使用する場合、RFC 2833 がネゴシエートされるときに、関連付けられた CTI ポートに対して MTP が必要となります。また、Unified CVP を使用するシナリオでも、MTP が必要となることがあります。Unified CCX Extend and Connect で RFC 2833 がネゴシエートされるときに、関連付けられた CTI Remote Device に対して MTP が必要となります。
- トランスコーダが必要になる場合があります。たとえば、WAN で接続された場所にある電話機が G.729 コーデックだけをサポートしているが、Unified CVP は G.711 対応に設定されている場合、Unified CM はトランスコーダに対応します。ただし、ゲートウェイまたは Cisco Unified Border Element から到着する着信コールは、Unified CVP で G.711 から開始し、トランスコーダを必要とせずにエージェントを使用して、後で G.729 に再ネゴシエートできます。
- Unified CM では、一部のサードパーティ製コンタクト センター製品もサポートされています。Unified CM との統合は JTAPI に基づいて行うことができます。また、コール トリートメントとキューイングおよび CTI ルート ポイントに対して CTI ポートを使用できます。Unified CM のサイズを適切に設定するには、コール フローとそれが Unified CM に与える影響をよく理解することが重要です。また、冗長構成の実装方法と、それが Unified CM または CTI のスケーラビリティに影響するかどうかも理解しておくことが重要です。

設計上の考慮事項の詳細については、https://www.cisco.com/go/srnd から入手できるシスコ ユニファイド コンタクト センターの設計ガイドを参照してください。

コンタクト センターのキャパシティ プランニング

すべての導入は、Cisco Collaboration Sizing Tool を使用してサイジングする必要があります。このツールは、コンタクト センター製品（Unified CCE、Unified IP IVR、Unified CVP、Unified CCX など）のサイジングを実行します。このツールによって、配置に必要なコンタクト センター リソース（エージェント数、IVR ポート数、ゲートウェイ ポート数など）が決定されます。コンタクト センター コンポーネントそのもののサイジングだけでなく、Unified CM や音声ゲートウェイを含む Unified Communications の残りの要素のサイズも決定されます。このツールは、シスコの従業員およびパートナーだけが（適切なログイン認証を使用して）、https://cucst.cloudapps.cisco.com/landing から入手できます。

一般に、コンタクト センターのサイジングには、コンタクト センターへの着信コールの最繁時呼数（BHCA）が大きく影響します。また、[Service Level Goal] や [Target Answer Time] などの他のパラメータも影響を与えます。たとえば、コールの 90 % を 30 秒以内に応答処理する必要のある配置では、コールの 80 % を 2 分以内に応答処理する必要のある配置よりも多くのコンタクト センター リソースが必要となります。サイジングに影響を与えるもう 1 つのパラメータは、Finesse または Finesse IP Phone Agent が使用されているかどうかです。サイジングには Unified CST を使用して、https://www.cisco.com/go/srnd から入手できる、該当するシスコ ユニファイド コンタクト センター設計ガイドで詳細情報を参照してください。

また、コンタクト センターの設計も、Unified CM サイジングに影響を与えます。コンタクト センター ソリューション内に配置される Unified CM のサイジングには、次の考慮事項が適用されます。

- 単一の Unified CM クラスタ内の Unified CCE エージェントの最大数は、IVR ソリューションによって異なります。Unified IP IVR を使用する場合、コール トリートメントとキューイング中に CTI ルート ポイントおよび CTI ポートが使用されます。これにより、Unified CM リソースが消費されます。Unified CVP を使用する場合、コール トリートメントとキューイングは通常、VXML ゲートウェイ、Unified CVP VXML サーバ、および Unified CVP Call Server によって処理されます。これによる Unified CM への影響はありません。したがって、Unified IP IVR よりも Unified CVP を使用したほうが、単一の Unified CM クラスタでサポートできるエージェント数が多くなります。
- Unified CCE Mobile Agent 機能は CTI ポートに依存しているため、Unified CM サブスクライバからの追加のリソースが必要となります。したがって、Mobile Agent を配置した場合は、Unified CM のスケーラビリティが低下します。
- Unified CCE の展開では、SIP ダイヤリングがサポートされます。SIP ダイヤラを使用する場合、各発信コールは SIP ダイヤラ ポートから直接、発信音声ゲートウェイに送信されます。コールはエージェントに転送されて初めて、Unified CM に到達します。したがって、SIP ダイヤラを使用すると、Unified CM のキャパシティははるかに大きくなります。
- Unified CM のサイジングを行う際には、追加の CTI アプリケーションを考慮に入れることも重要です。たとえば、一部の PC クライアントは、CTI を介してリモートから電話機を制御できます。また、一部のコール録音アプリケーションは、CTI Manager を使用して直接 Unified CM と統合できます。さらに、エージェント電話機をモニタできるものもあります。これには、Unified CM からの追加のリソースが必要となることがあります。詳細については、コンピュータ テレフォニー インテグレーション（CTI）（9-29 ページ）、および https://www.cisco.com/go/srnd から入手できるシスコ ユニファイド コンタクト センターの設計ガイドを参照してください。

- Unified CM からのリソースを消費するサイレント モニタリングと録音ソリューションもあれば（Unified CM をベースにしたサイレント モニタリングや録音機能など）、消費しないソリューションもあります（SPAN またはデスクトップ サイレント モニタリングと録音など）。
- 繰り返しますが、サイジングは複雑であるため、すべての導入は Cisco Collaboration Sizing Tool を使用してサイジングする必要があります。このツールは、シスコの従業員とパートナーだけが（適切なログイン認証を使用して）、https://cucst.cloudapps.cisco.com/landing から入手できます。

詳細については、https://www.cisco.com/go/srnd から入手できるシスコ ユニファイド コンタクト センターの設計ガイドを参照してください。

ビデオによるカスタマー ケア

人と人のふれ合いを大切にしたカスタマー エンゲージメントのため、ビデオ対応のカスタマー エクスペリエンスを含めるようにカスタマー ケアを拡大することにより、顧客とエージェントの両者にとってインタラクションを大幅に向上させることができます。

Cisco Remote Expert ソリューション

Cisco Remote Expert ソリューションにより、顧客と社内従業員は複数のチャネルを通じてエキスパートに接続できます。また、収益の最適化、エキスパートの生産性向上、顧客ロイヤルティの構築に役立つ一貫したインタラクティブ エクスペリエンスを提供します。Cisco Remote Expert は、スペシャリストの仮想プールを作成し、スペシャリストの可用性を管理し、複数のチャネルやデバイスを通じて高品質の音声とビデオを使用して顧客をエキスパートに迅速に接続します。

複数のタッチ ポイントやデバイスを通じて一貫した顧客および従業員のエクスペリエンスを提供するよう設計されている Cisco Remote Expert ソリューションは、カスタマー ケア用の新しい業界ベンチマークを確立し、次の利点を提供するエンドツーエンドのマルチチャネル コラボレーション プラットフォームです。

- 応答時間の改善

  顧客は、パーソナル デバイスやキオスクから、または店舗、支店、クリニックなどにある顧客のワークステーションから、ボタン 1 つでビデオを介してエキスパートにアクセスできます。

- 成約率の向上

  Cisco Remote Expert は、製品とサービスに関する問い合わせに十分答えるために必要となる適切なリソースへインテリジェントに顧客をルーティングできます。

- クロスセルおよびアップセルの機会の改善

  顧客は、顧客のニーズに対処して関連する製品やサービスを提案できる熟練したエキスパートと連携できます。

- 生産性の向上

  各分野の専門家は、デバイスや場所に関係なく顧客にアクセスできる単一のプラットフォームを使用できます。

Cisco Remote Expert ソリューションは、Cisco Validated Design リファレンス アーキテクチャとパートナー エコシステムでサポートされる業界トップクラスの高品質コラボレーション製品およびサービスを採用します。

Remote Expert の詳細については、次の URL にある『*Cisco Remote Expert Solution Design Guide*』を参照してください。

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone/remote_expert.html

ネットワーク管理ツール

Unified CCE は、簡易ネットワーク管理プロトコル（SNMP）を使用して管理します。Unified CCE デバイスは、SNMP v1、v2c、および v3 をサポートする組み込み型の SNMP エージェント インフラストラクチャを持ち、CISCO-CONTACT-CENTER-APPS-MIB により定義された計測手段を公開します。この MIB により、標準の SNMP 管理ステーションでモニタ可能な構成、検出、および状態の計測手段が提供されます。さらに、Unified CCE は、管理者にシステムの障害があれば警告する豊富な SNMP 通知セットを提供します。また、Unified CCE は、より詳細なイベント セットを必要とする管理者に対して、（RFC 3164 に準拠する）標準的な syslog イベント フィードも提供します。

Unified CCE SNMP エージェント インフラストラクチャおよび syslog フィードの設定の詳細については、次のサイトで入手可能な『*SNMP Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*』を参照してください。

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

Unified CVP の状態モニタリングは、任意の SNMP 標準モニタリング ツールを使用して実行できます。これにより、ソリューション ネットワークの状態の詳細が表形式で視覚的に示されます。すべての Unified CVP 製品コンポーネントおよびほとんどの Unified CVP ソリューション コンポーネントは、標準的な SNMP 管理ステーションまたはモニタリング ツールに配信できる SNMP トラップおよび統計も発行します。

Unified CCX は、SNMP および syslog インターフェイスを使用して管理することもできます。

Cisco Prime Collaboration は、コンタクト センター配置の管理にも役立ちます。たとえば、Cisco Prime Collaboration Assurance を使用して、アクティブ コール数、着信コール数/秒、またはログインしているエージェント数をモニタできます。

また、Prime Collaboration Assurance Advanced がすでに実装されている場合は、Prime Contact Center Assurance モジュールを追加できます。Prime Contact Center Assurance モジュールは、カスタマー ケア環境のトポロジ、およびコンポーネント間の関係を図示します。また、エラーの根本原因の分析を迅速化するイベント相関、パフォーマンスの問題の検出と解決に役立つパフォーマンス ダッシュボード、コール フローを中断するデバイスの特定に役立つコール トレース分析を提供します。

コール録音とモニタリング

改訂日：2018 年 3 月 1 日

コール モニタリングおよび録音ソリューションは、Cisco IP Phone、Cisco Unified Border Element デバイス、Cisco スイッチなどの Unified Communications および Collaboration ソリューションのさまざまなコンポーネントにわたって適用される音声コールおよびビデオ コールを自動的にモニタし、録音する方法を提供します。こうした録音は、コンプライアンス、音声テキスト変換、音声分析、ポッドキャスティング、ブログなどのさまざまな目的に、コール センターと他のエンタープライズ機能で使用できます。この章では、音声コールとビデオ コールの両方に Cisco Unified Communications および Collaboration ソリューションで利用できるさまざまなコール録音ソリューションの概要を示します。また、Cisco Unified Communications および Collaboration ソリューションに組み込まれたコール録音ソリューションに関する基本的な設計の考慮事項の概要についても示します。

この章の変更点

表 23-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 23-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco MediaSense は販売終了（EoS）となり、この章から削除されました。	Cisco MediaSense については、https://www.cisco.com/go/srnd で入手可能な SRND の過去のバージョンを参照してください。	2018 年 3 月 1 日
Cisco TelePresence Content Server（TCS）は販売終了（EoS）となり、この章から削除されました。	Cisco TCS については、https://www.cisco.com/go/srnd で入手可能な SRND の過去のバージョンを参照してください。	2018 年 3 月 1 日

モニタリング ソリューションと録音ソリューションの種類

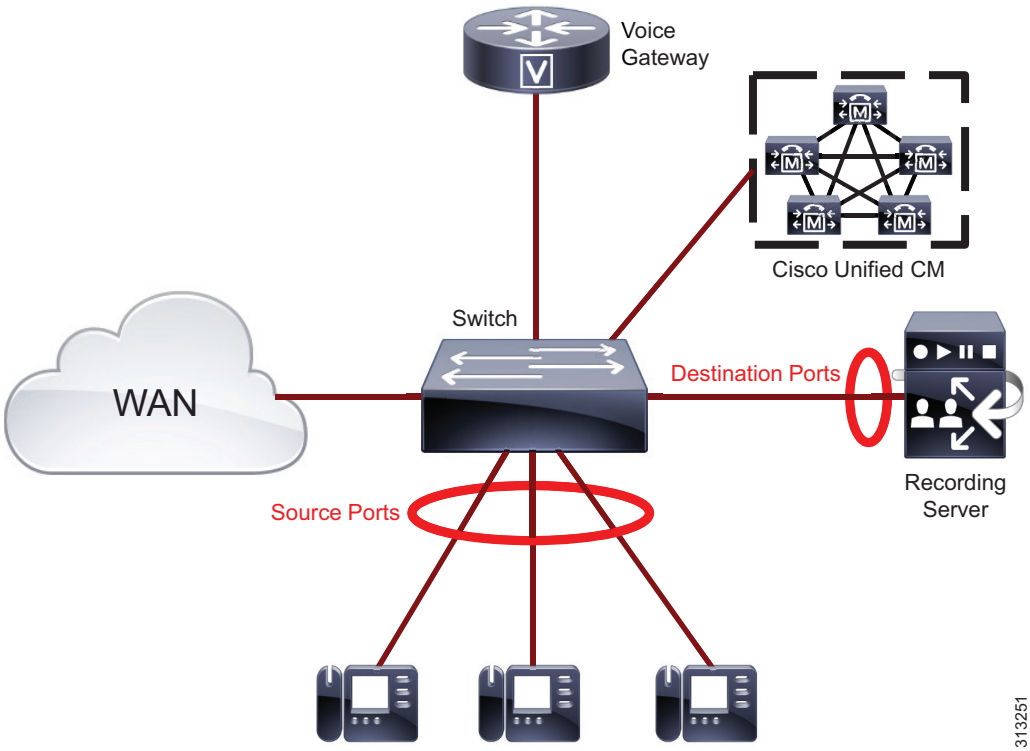
ここでは、次の種類のコール録音ソリューションおよびモニタリング ソリューションについて説明します。

SPAN ベース ソリューション

スイッチド ポート アナライザ（SPAN）に基づく録音ソリューションは、コールの録音にパケット スニッフィング テクノロジーを使用します。SPAN は、ネットワーク トラフィックのモニタリングの方法です。SPAN がスイッチ ポートまたは VLAN で有効になっている場合、スイッチは、そのポートまたは VLAN を通過するすべてのネットワーク パケットのコピーを、録音サーバまたはモニタリング サーバ（Cisco Unified Workforce Optimization Quality Managementまたはサードパーティ製録音サーバなど）がそれらのパケットを分析する別のポートに送信します。ネットワーク トラフィックに組み込まれている VoIP RTP パケットを検出して解読し、オーディオとしてストレージに格納します。SPAN は、必要に応じて Cisco 音声ゲートウェイまたは Cisco IP Phone に接続されたポートで有効にできます。たとえば、IP Phone 間の内部コールを録音する場合、SPAN は、IP Phone に接続するスイッチ ポートで有効になっている必要があります。

図 23-1 に、内部コールの録音用の SPAN ベースの録音ソリューションの展開を示しています。送信元ポートとしてマークされた IP Phone に接続するポートは、録音サーバに接続した宛先ポートにミラーリングされます。

図 23-1　　内部コール用の SPAN ベースのコール録音フロー



一部のシスコ パートナーは、Cisco Unified Communications および Collaboration ソリューションに SPAN ベースの録音サーバとアプリケーションを提供します。技術的な詳細については、次の Web サイトで入手可能な『*Cisco Developer Network Marketplace Solutions Catalog*』の特定のパートナー製品の情報を参照してください。

https://marketplace.cisco.com/catalog/search?utf8=%E2%9C%93&x=48&y=6&search%5Btechnology_category_ids%5D=1900

さらに、ポートのミラーリングが有効な場合、ネットワーク トラフィック フローは、適切な帯域幅のプロビジョニングについて考慮する必要があります。

SPAN ベースの録音および仮想化

ここでは、仮想化が有効になっている一般的な SPAN ベースの導入の一部と、制限事項の一部について確認します。VMware は、vSphere 5.0 を開始する VMware vSphere 分散スイッチ（VDS）で SPAN 機能をサポートします。

仮想化されたセットアップでは、Unified Communications アプリケーション、コンタクト センター アプリケーション、およびポート アナライザ アプリケーションの一部が同じホストまたは異なるホストの仮想マシン上に導入される場合があります。仮想化されたセットアップでは、SPAN ベースの録音ソリューションにいくつかの制限があります。たとえば、次の機能は仮想化による Cisco Unified Contact Center Enterprise（Unified CCE）の導入ではサポートされていません。

- リモート サイレント モニタリング
- Cisco Unified Computing System（UCS）B シリーズ シャーシでの SPAN ベースのサイレント モニタリングおよび録音

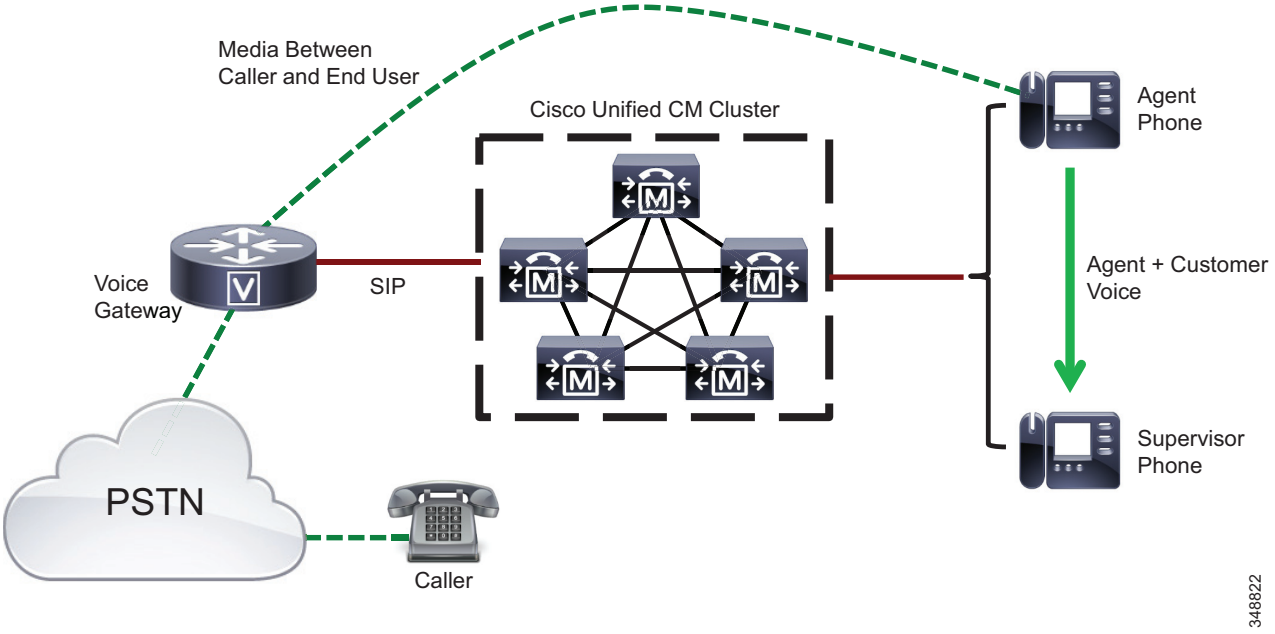
（注）　SPAN ベースのサイレント モニタリングおよび録音は UCS B シリーズ シャーシではサポートされません。

Unified CM のサイレント モニタリング

Unified CM のサイレント コール モニタリング機能では、エージェントと顧客の両者がスーパーバイザのコールへの参加を認識せずに、スーパーバイザは両者の会話を聞くことができます。コール モニタリング中、エージェントの電話機は、電話機の 2 つの音声 RTP ストリームを組み合わせ（エージェント用と顧客用）、スーパーバイザの電話機に生成されるストリームを送信します。さらに、ウィスパー コーチングでは、コール モニタリング セッション中でもスーパーバイザはエージェントと話ができます。コール モニタリングおよびウィスパー コーチングは Unified CM の JTAPI インターフェイスまたは TAPI インターフェイスを介したコール センター アプリケーションによって呼び出すことができます。

図 23-2 に、Cisco Unified CM のサイレント モニタリングの基本的な設定を示します。

図 23-2　Unified CM のサイレント モニタリングのアーキテクチャ



Unified CM のネットワーク ベースの録音

Unified CM のネットワークベースの録音機能では、システム管理者が発信側と着信側との間の会話を録音することができます。ネットワークベースの録音を使用して、サポート対象の IP フォン モデルのビルトイン ブリッジ（BIB）かサポート対象のバージョンおよび設定の SIP ゲートウェイのいずれかを使用してメディアをフォーキングできます。管理者はどちらか一方のフォーキング デバイス タイプに設定できます。ただし、優先するフォーキング デバイスが使用できない場合は、Unified CM がもう一方の方法に自動的にフェールオーバーします。たとえば、IP フォンに [電話を優先（Phone Preferred）] で有効にされた録音があっても利用可能な録音リソースがない（電話機にビルトイン ブリッジがない）場合、ゲートウェイがコールの録音に使用されます。

コール録音用に Unified CM で使用されるメディア フォーキング デバイスに関係なく、Unified CM は録音サーバに対して、録音されたコールの近端および遠端側に関するメタデータを常に提供します。メタデータは、SIP Invite の FROM ヘッダーと Unified CM と録音サーバの間で送信される他の SIP メッセージにあります。

Unified CM サイレント コール モニタリングおよびコール録音機能の詳細については、次の Web サイトで入手可能な『*Feature Configuration Guide for Cisco Unified Communications Manager*』の最新バージョンを参照してください。

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

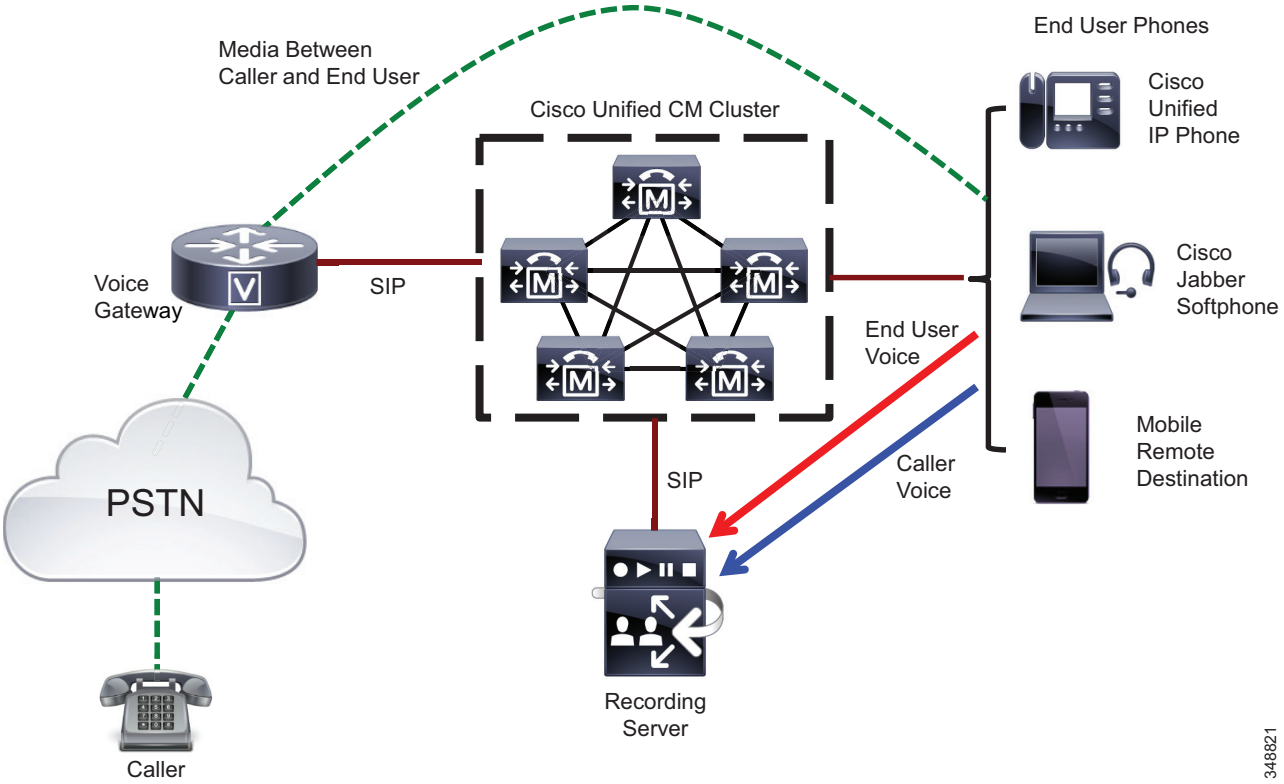
Cisco Unified CM のネットワークベースの録音は、個々の回線インスタンスごとに自動録音と選択的録音をサポートします。これは、録音が必要な回線の各インスタンスに録音プロファイルを割り当てることによって実行されます。複数回線デバイスの単一回線または共有回線の単インスタンスの録音が可能です。自動録音では、Unified CM はエンドポイントに接続されるすべてのコールを自動的に録音します。選択的録音では、エンドポイントのコールの録音を開始するようにユーザまたは JTAPI/CTI を介して外部アプリケーションが明示的に Unified CM に要求する必要があります。ユーザは、エンドポイントの [録音開始（Start Recording）] ボタンを押すか、JTAPI または TAPI アプリケーションから録音要求を送信することによって、録音を要求できます。録音を開始するために、Unified CM は要求をフォーキング デバイスに送信します。フォーキング デバイスは、メディアが録音される録音サーバに会話のメディアを分岐します。

（注）　通話録音と Multilevel Precedence and Preemption（MLPP）の両方を有効にした場合は、両方の機能を使用する回線が 2 つの追加のコール レッグを生成します。そのため、このような回線のビジートリガーを 3 に設定する必要があります。

ビルトイン ブリッジを使用した Unified CM のネットワークベースの録音

BIB を使用した Cisco Unified CM のネットワークベースの録音では IP フォンのビルトイン ブリッジを使用してコール録音を有効にします（図 23-3 を参照）。コールの録音中にエージェントの電話機が 2 つのストリームを録音サーバに分岐します。2 つのストリームのうち 1 つは着信側の音声用、もう 1 つは発信側の音声用で、別々に録音されます。1 つのストリームが必要な場合、顧客は録音されたストリームを混合して、サードパーティ製のアプリケーションから会話を生成することができます。

*図 23-3　　電話機のビルトイン ブリッジを使用した **Unified CM** のネットワークベースの録音*



Unified CM でのコール モニタリングおよびコール録音をサポートする Cisco Unified IP Phone の一覧は、次の Web サイトで入手可能な『*Unified CM Silent Monitoring/Recording Supported Device Matrix*』を参照してください。

https://developer.cisco.com/site/uc-manager-sip/documents/supported/

ゲートウェイを使用した Cisco Unified CM のネットワークベースの録音

コールが録音ゲートウェイを通過すると、Cisco Unified CM のネットワークベースの録音ではゲートウェイのメディア フォーキング機能を使用してコールを録音します。外部コールを電話機のエンド ユーザに接続すると、Unified CM はゲートウェイで実行している UC ゲートウェイ サービス API を介して録音サーバに会話のメディアを分岐するようにゲートウェイに要求します。分岐されたメディアは、2 つの RTP ストリーム（エンドユーザの音声用と発信者の音声用）で構成され、録音サーバはストリームを別々にキャプチャします。録音対応ゲートウェイがコールに含まれている場合は、Cisco Unified IP Phone のエンド ユーザに接続された外部コール、PC で実行中の Cisco Softphone（Cisco Jabber など）、リモート接続先としてのモバイル フォン、CTI ポート、Extend and Connect の接続先など、複数の録音シナリオが考えられます。基本的に、Unified CM が登録された音声ゲートウェイで外線コールが終了すると、発信者側からのコールの会話はすべて、コールが企業内のどこに着信する場合でも録音できます。

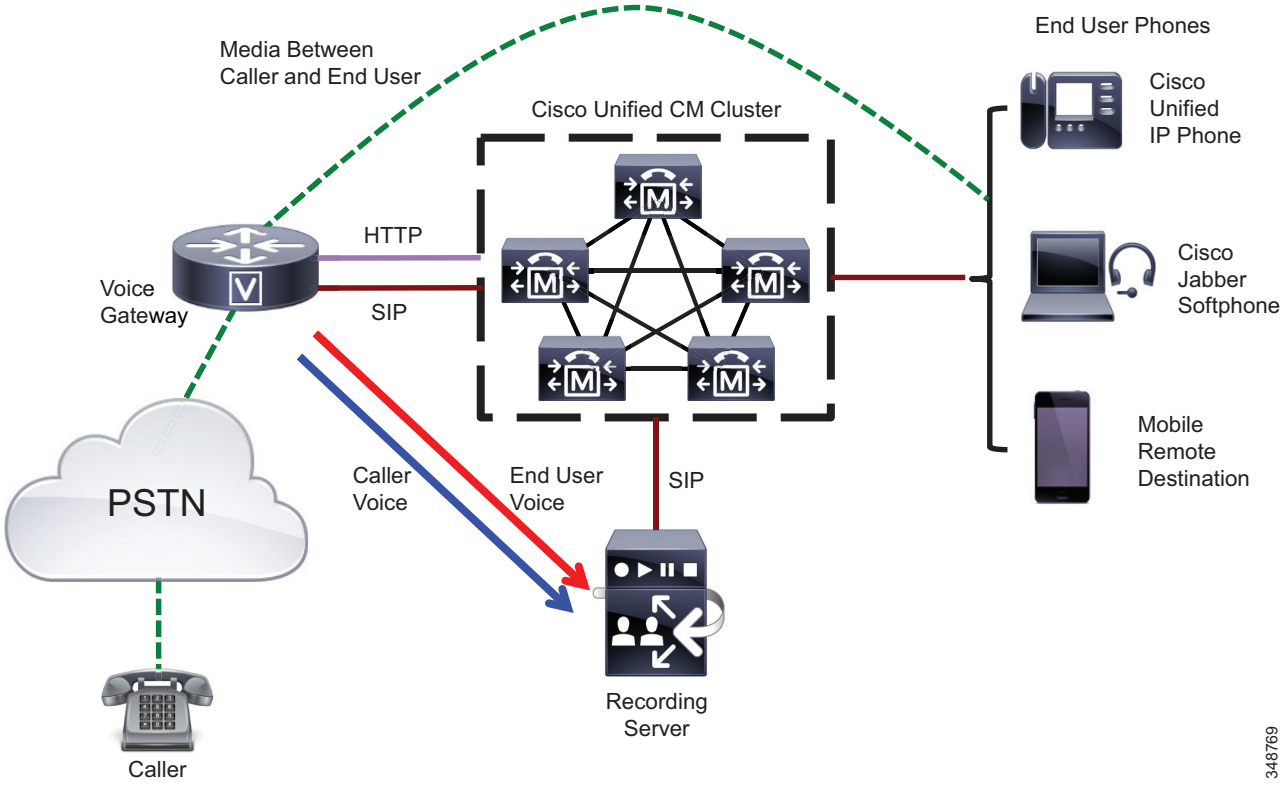
Cisco Unified CM のネットワークベースの録音は、上記以外のコール タイプもサポートします。詳細については、次の Web サイトで入手可能な『*Feature Configuration Guide for Cisco Unified Communications Manager*』の最新バージョンを参照してください。

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

（注）　音声ゲートウェイからメディア フォーキングを呼び出すと 2 つの RTP ストリームが生成されて、サイレント モニタリングが必要な場合は、アプリケーションはストリームの混合を管理します。

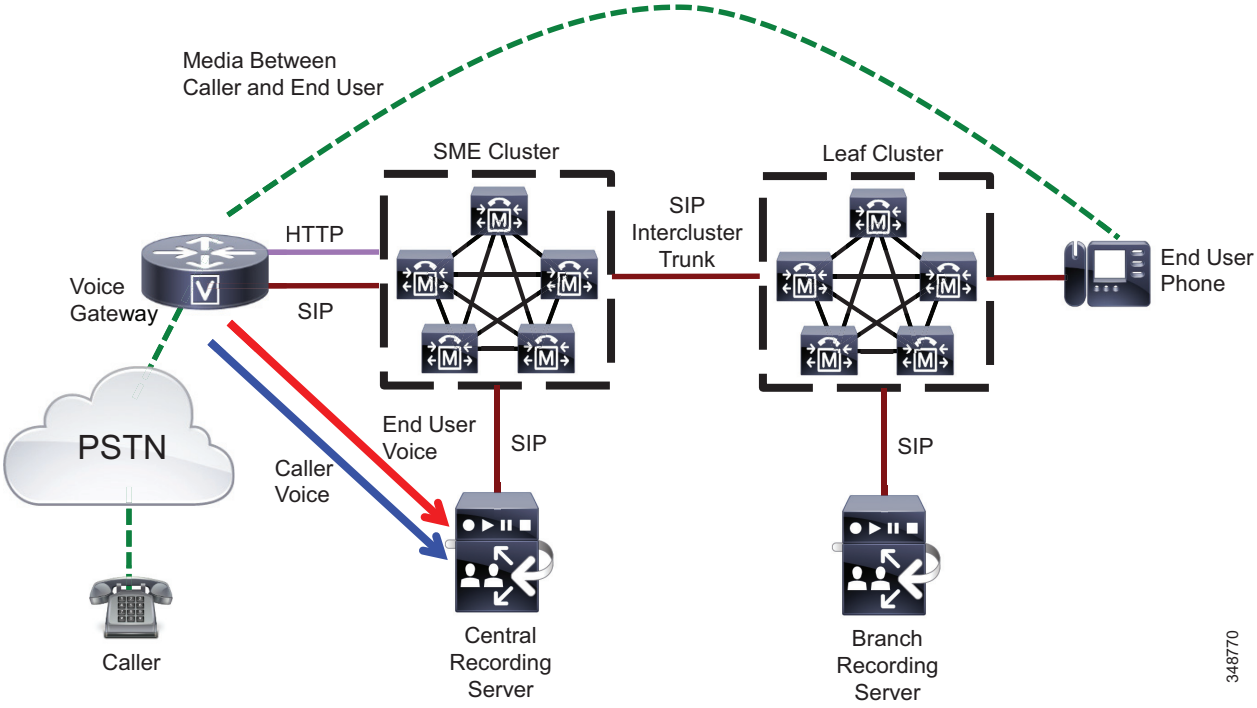
図 23-4 ゲートウェイを使用した Cisco Unified CM のネットワークベースの録音の基本的な設定を示します。Cisco Unified CM および音声ゲートウェイは録音対応の SIP トランクを介して接続されます。Unified CM は HTTP インターフェイスを介してゲートウェイで UC ゲートウェイ サービス API に登録されます。これによって、Unified CM はゲートウェイを通過するすべてのコールのコール イベントの通知を受信し、録音の開始または停止を決定できるようにします。ゲートウェイ コールが電話機のエンド ユーザに接続されると、設定された録音オプションに従って、Unified CM はメディアを分岐するようゲートウェイにすぐに通知するか、ゲートウェイに通知する前に録音開始のユーザ指示を待機する場合があります。Unified CM はゲートウェイに、録音停止のユーザ指示により分岐を停止するよう通知するか、ゲートウェイはコール終了時に自動的に録音を停止します。録音を開始または停止する要求は、Extended Media Forking（XMF）API を使用して HTTP インターフェイスを介して送信されます。

図 23-4　　ゲートウェイを使用したネットワークベースの録音



ゲートウェイを使用した Unified CM のネットワークベースの録音で、エンド ユーザの電話機とメディア フォーキング デバイス（音声ゲートウェイ）が分離されます。これらは同じ Unified CM クラスタ（図 23-4 を参照）または別の Unified CM クラスタに登録できます。したがって、このソリューションは、Cisco Unified CM Session Management Edition（SME）などの複数のクラスタ環境に導入できます。図 23-5 に、SME を使用して Unified CM のネットワークベースの録音を導入する例を示します。ここでは、音声ゲートウェイは SME クラスタに登録され、エンド ユーザの電話機はリーフ クラスタに登録されます。SME クラスタとリーフ クラスタは、ゲートウェイの録音オプションが両側でイネーブルにされた状態で、SIP クラスタ間トランク（ICT）で接続されます。したがって、録音呼び出し要求および応答は SME とリーフ クラスタの間で送信できます。また、顧客は、録音サーバを音声ゲートウェイのある SME クラスタの中央に導入するか、またはすべてのリーフ クラスタに録音サーバを分布するオプションがあります。

図 23-5　SME を使用した Cisco Unified CM のネットワークベースの録音の導入



Unified CM のネットワークベースの録音を導入する場合は、次のガイドラインに従ってください。

- ゲートウェイを使用したネットワークベースの録音は、Cisco サービス統合型ルータ（ISR）（ISR 4K など）や Cisco アグリゲーション サービス ルータ（ASR）など、さまざまなプラットフォームでサポートされます。詳細な要件については、次の Web サイトで入手可能な『*Feature Configuration Guide for Cisco Unified Communications Manager*』の最新バージョンを参照してください。

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

- SIP のみが音声ゲートウェイと Cisco Unified CM の間でサポートされ、SIP プロキシ サーバはサポートされません。
- クラスタ間録音では、クラスタを相互接続するために SIP トランクがサポートされます。
- 安全な録音はサポートされていません。
- IPv6 はサポートされていません。

エージェント デスクトップ

エージェント デスクトップのモニタリング ソリューションと録音ソリューションは、スーパーバイザがサイレント モニタリングを実行し、必要に応じてコール録音を開始できるコンタクト センター導入固有の機能です。次のエージェント デスクトップのモニタリング ソリューションと録音ソリューションが使用できます。

- Cisco Agent Desktop（CAD）サイレント モニタリングおよび録音
- Cisco リモート サイレント モニタリング（RSM）

これらのソリューションについては、次のドキュメントの最新版に詳しく記載されています。

- 次の場所にある『*Solution Design Guide for Cisco Unified Contact Center Enterprise*』

  https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html

- 次の場所にある『*Solution Design Guide for Cisco Unified Contact Center Express*』

  https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-implementation-design-guides-list.html

モニタリングおよび録音のキャパシティ プランニング

すべてのタイプのモニタリングおよびコール録音、またはこのいずれかを有効にすると、Unified Communications システム全体の容量に影響を及ぼします。Unified CM からのリソースを消費するサイレント モニタリングと録音ソリューションもあれば（Unified CM をベースにしたサイレント モニタリングや録音機能など）、消費しないソリューションもあります（SPAN またはデスクトップ サイレント モニタリングと録音など）。コール録音を有効にした Unified Communications システムのキャパシティ プランニングを実行する場合は、次の事項を考慮してください。

- Unified CM のコール録音では、録音された各コールはコール処理コンポーネント BHCA キャパシティに 2 件のコールを追加します。IP フォンまたは音声ゲートウェイからのメディアのフォーキングは Unified CM または音声ゲートウェイそれぞれからリソースを消費します。
- 帯域幅の要件は、録音サーバに分岐されたメディアを送信するため、メディア フォーキングが IP Phone または Cisco Unified Border Element デバイスで有効になると増加します。エージェント デスクトップのモニタリングおよび録音の場合、所定の時間にモニタまたは録音されるコールの数によって、帯域幅の使用率が不安定になる場合があります。
- Cisco Unified Border Element を使用したコールの録音は、コールの重みを 2 倍にします。したがって、Cisco Unified Border Element を通過するすべてのコールを録音した場合、コールのキャパシティは半分になります。
- Cisco Unified Border Element のメモリ使用率は、録音されるコールごとに増加します。
- 録音とモニタリングを呼び出すため、CTI アプリケーションが Cisco Unified CM と相互作用している場合は、Unified CM クラスタの導入モデルを考慮し、クラスタ全体に CTI アプリケーションのロードバランスを実行する必要があります。

サイジングは複雑であるため、次の Web サイトからシスコの従業員とパートナーだけが（適切なログイン認証を使用して）入手できる Cisco Collaboration Sizing Tool を使用してサイジングする必要があります。

https://cucst.cloudapps.cisco.com/landing

PART 4

コラボレーション システムのプロビジョニングと管理

このパートの内容

マニュアルのこのパートに含まれる章は、次のとおりです。

コラボレーション システムのプロビジョニングと管理の概要

改訂日:2015 年 6 月 15 日

ネットワーク、コール ルーティング、呼制御インフラストラクチャ、およびアプリケーションとサービスを Cisco Unified Communications および Collaboration システムに配置した後は、ネットワークとアプリケーションの管理コンポーネントをそのインフラストラクチャの最上位に追加または階層化できます。既存の Cisco Unified Communications および Collaboration インフラストラクチャに配置して、システムの動作をモニタおよび管理できるアプリケーションおよびサービスが多数存在します。これらのアプリケーションとサービスは、次の 4 つの基本領域に分類できます。

- ユーザとデバイスのプロビジョニング サービス:ユーザとデバイスを一元的にプロビジョニングして設定する能力を Unified Communications および Collaboration アプリケーションおよびサービスに提供します。
- 音声品質のモニタリングおよびアラート:システム内で発生するさまざまなコール フローを継続的にモニタして、音声およびビデオ品質が許容できるかどうかを判別し、品質が許容できない場合は、管理者に警告します。
- 運用と障害のモニタリング:アプリケーションとサービスのすべての処理を一元的にモニタし、ネットワークおよびアプリケーションの障害に関するアラートを管理者に発行します。
- ネットワークとアプリケーションのプローブ:導入全体のさまざまなロケーションでネットワークとアプリケーションのトラフィック情報をプローブおよび収集し、管理者が中央ロケーションでこの情報にアクセスし、取得できるようにします。

本 SRND のこのパートでは、上記で説明しているアプリケーションとサービスについて説明します。さまざまなネットワーク管理アプリケーションとサービスの概要を示したあと、アーキテクチャ、ハイ アベイラビリティ、キャパシティ プランニング、および設計上の考慮事項について説明します。ここでは、アプリケーションおよびサービスの設計関連の側面を中心に説明します。製品固有のサポートおよび設定情報については、関連する製品マニュアルを参照してください。

SRND のこのパートには、Cisco Unified Communications および Collaboration 配置のサイジング方法と、サードパーティおよび従来のコミュニケーション システムから Cisco Unified Communications および Collaboration システムに移行するための推奨方法に関する詳細情報も含まれます。

SRND のこの部分に含まれる章は、次のとおりです。

- コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）

  この章では、個々の Unified Communications および Collaboration コンポーネント、および相互通信する複数のコンポーネントで構成されたシステムのサイジングについて説明します。各種 Unified Communications および Collaboration 製品がサポートするさまざまな機能がパフォーマンスに及ぼす影響、および複雑な Unified Communications および Collaboration ネットワークを配置する方法として「データシートによる設計」が適していない理由についても説明します。加えて、利用できるさまざまなサイジング ツール、特に Cisco Collaboration Sizing Tool の使用方法について詳しく説明します。

- Cisco Collaboration システムの移行（26-1 ページ）

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

- ネットワーク管理（27-1 ページ）

  この章では、Unified Communications および Collaboration ネットワークとアプリケーションの管理サービスについて説明します。これは、ほとんどの Unified Communications および Collaboration 導入で一般的に普及しているサービス セットです。これらの管理サービスにより、管理者はユーザとデバイスをプロビジョニングおよび設定し、ネットワークとアプリケーションの動作や音声およびビデオ品質をモニタし、問題が発生したときにアラートとアラームを受信できます。また、この章では、配置モデルに対するこれらの管理アプリケーションとサービスの影響についても説明し、ネットワークとアプリケーションの管理サービスおよびアプリケーションに関する設計と導入のベスト プラクティスを示します。

アーキテクチャ

他のネットワークおよびアプリケーション テクノロジー システムの場合と同様、運用とサービスアビリティのアプリケーションおよびサービスは、基盤となるネットワーク インフラストラクチャ、システム インフラストラクチャ、およびアプリケーション インフラストラクチャの最上位で階層化して、これらのインフラストラクチャをモニタおよび制御できるようにする必要があります。Unified Communications および Collaboration の運用とサービスアビリティ サービス（ユーザとデバイスのプロビジョニング、音声およびビデオ品質のモニタリングおよびアラート、運用と障害のモニタリング、ネットワークとアプリケーションのプローブなど）はすべて、運用とサービスアビリティのさまざまなアプリケーションおよびプローブにネットワーク接続するために、基盤のネットワーク インフラストラクチャを使用します。Unified Communications および Collaboration のコール ルーティングと呼制御のインフラストラクチャ、または Unified Communications および Collaboration のクライアントとサービスとの直接の依存関係はありませんが、これらのインフラストラクチャおよびアプリケーションは、さまざまな運用サービスや管理サービスが実際に管理および設定する対象となります。たとえば、ユーザとデバイスのプロビジョニング サービスと、モニタリングおよびアラートの各種サービスでは、さまざまな Unified Communications および Collaboration のアプリケーションとサービス ノードに接続するためにネットワーク インフラストラクチャを利用して、さまざまなコンポーネントおよび動作を設定およびモニタします。また、これらのサービスは、コンポーネント（呼処理エージェント、PSTN ゲートウェイと IP ゲートウェイ、メディア リソース、エンドポイントなど）および（メッセージング、リッチ メディア会議、およびコラボレーション クライアント用の）各種 Unified Communications および Collaboration アプリケーションと直接通信し、場合によっては設定の変更やアラートの受信を行います。これらのインフラストラクチャ レイヤおよび基本的な Unified Communications および Collaboration サービスとアプリケーションに依存する以外に、運用とサービスアビリティに関連するそれぞれのサービスは、多くの場合、完全に機能するために相互に依存します。

ハイ アベイラビリティ

ネットワーク、コール ルーティング、呼制御の各インフラストラクチャ、および重要な Unified Communications および Collaboration アプリケーションとサービスの場合と同様に、運用とサービスアビリティ サービスは、ネットワークやアプリケーションに障害が発生した場合でも必要なプロビジョニング、モニタリング、およびアラートが引き続き実行されるように、ハイ アベイラビリティを実現する必要があります。発生する可能性のあるさまざまなタイプの障害、およびこれらの障害に関する設計上の考慮事項を理解することが重要となります。Unified Communications および Collaboration の運用とサービスアビリティ コンポーネントは、他のコンポーネントやサービスに依存していることから、場合によっては、1 つの運用および管理アプリケーションまたはサービスの障害が、複数のサービスに影響を及ぼすことがあります。たとえば、ネットワーク管理導入のさまざまなアプリケーション サービス コンポーネントが適切に機能していても、ネットワーク接続の切断または障害が発生すると、冗長ネットワーク プローブが別の接続パスとともに展開されていない限り、ネットワーク プローブはネットワークの正常性または音声およびビデオ品質をモニタできなくなります。

ユーザとデバイスのプロビジョニングなどの運用とサービスアビリティ機能の場合、ハイ アベイラビリティに関する考慮事項には、ネットワーク接続またはアプリケーション サーバの障害による一時的な機能の喪失によって、管理者がユーザとデバイスをプロビジョニングできなくなったり、ユーザ アカウントまたはデバイス設定を変更できなくなったりすることが含まれます。また、これらのタイプの運用のフェールオーバーに関する考慮事項には、特定の障害が発生した場合に、管理者が一部の設定変更を引き続き実行できるように、冗長な運用または管理のアプリケーションによって一部の機能を処理できるようにするというシナリオが含まれます。

ハイ アベイラビリティに関する考慮事項は、音声およびビデオ品質のモニタや、アプリケーションおよび動作障害のモニタなどのサービスを提供する運用とサービスアビリティのアプリケーションに対しても考慮する必要があります。ネットワークの接続性が妨げられたり、サーバやアプリケーションで障害が発生した場合は、モニタやアラートに関する機能が縮退したり、場合によっては、これらの機能が完全に失われます。これは、音声およびビデオ品質のモニタリングにおいては、コール フローやデバイスに関する品質の測定ができなくなる場合があることを意味します。運用と障害モニタリング サービスにおいては、設定変更された内容を追跡するためのデータや、障害の発生を示すのアラートやインジケータが損失してしまう可能性も考慮して冗長化を行う必要があります。

キャパシティ プランニング

ネットワーク、コール ルーティング、および呼制御の各インフラストラクチャ、および Unified Communications および Collaboration アプリケーションとサービスは、個々のコンポーネントおよびシステム全体のキャパシティとスケーラビリティを理解して設計および配置する必要があります。同様に、運用とサービスアビリティのコンポーネントとサービスの導入についても、キャパシティとスケーラビリティの考慮事項に注意して設計する必要があります。運用とサービスアビリティの各種アプリケーションとコンポーネントを配置する場合は、アプリケーション自体のスケーラビリティの考慮が重要となるだけでなく、基盤となるインフラストラクチャのスケーラビリティについても考慮する必要があります。ネットワーク インフラストラクチャは、利用可能な帯域幅を有し、運用によって発生する追加のトラフィック負荷を処理できる必要があります。同様に、コール ルーティングと呼制御インフラストラクチャでは、使用中のさまざまな運用とサービスアビリティ コンポーネントによって実施される、必要な入力と出力を処理できる必要があります。たとえば、音声品質のモニタリングやアラート、運用と障害のモニタリングなどの運用アプリケーションとサービスでは、所定の時間にモニタできるデバイスやコール フローの数に関して、これらの個々のアプリケーションやサービスに対するキャパシティの暗黙的要件がありますが、モニタとアラートの実行に必要となる、追加のネットワーク トラフィックおよび接続を処理するための、基盤となるインフラストラクチャおよびモニタ対象アプリケーションのスケーラビリティも、同様に重要となります。モニタおよびアラートのアプリケーションやサービス自体が多数のネットワーク デバイスやコール フローをサポートできる場合でも、基盤となるネットワークやデバイスが、接続のプローブ、またはモニタリングおよびアラート サービスによって生成されたアラーム メッセージング負荷を処理できるキャパシティを持っていない場合があります。

ユーザまたはデバイスのプロビジョニング機能を提供する運用アプリケーションまたはサービスの場合、キャパシティ プランニングの考慮事項には、プロビジョニング アプリケーションが要求された負荷を処理できること、およびユーザまたはデバイスのプロビジョニング処理が、特定の基礎となる Unified Communications のアプリケーションとサービスでサポートされているデバイスまたはユーザの数を超えないことを保証するだけでなく、プロビジョニングまたは設定変更のトランザクションが、基礎となるネットワークのキャパシティ、または特定のアプリケーションでトランザクションを処理できる割合のいずれも超えないことを保証することが含まれます。基盤となるネットワーク インフラストラクチャ、およびコール ルーティングと呼制御のインフラストラクチャが追加の負荷を処理できると想定すると、ほとんどの場合、運用プロビジョニング アプリケーション サーバを増やしたり、基になる Unified Communications および Collaboration のアプリケーション インスタンスやサービス インスタンスを増やしたりすることで、キャパシティを追加できます。

システム サイジング、キャパシティ プランニング、およびサイジングに関連する配置上の考慮事項の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

コラボレーション ソリューション サイジング ガイダンス

改訂日：2018 年 3 月 1 日

この章では、シスコ コラボレーション製品およびシステムのシステム サイジングについて説明します。サイジングは、システムが提供するユーザの数、トラフィックの構成、トラフィックの負荷、および機能に基づいてシステムに必要なハードウェア プラットフォームを正確に見積もります。

正確なサイジングは、導入されたシステムがコール量とスループットに関して予期されたサービス品質を満たすために重要です。スタンドアロン製品の場合、システム サイズの手動計算が実行できる場合があります（スタンドアロン製品のサイジング（25-52 ページ）の項で詳しく説明）。ただし、複雑なシステム導入では、多くのサイジングの考慮事項があります。たとえば、複数の製品がさまざまな場所に分散しており、ビデオ エンドポイント、コール センター、および音声/ビデオ会議が含まれている場合があります。シスコは、その複雑さを扱うための一連のサイジング ルールを提供します。

この章では、システム サイジングの方法およびサイジングに影響を与える要因に関する概要、およびサイジング ツールの使用方法について説明します。

（注） この章は、このマニュアルの他の章で説明する製品の説明、および設計と導入についての考慮事項とあわせて読む必要があります。導入を成功させるには、これら両面をよく理解する必要があります。

この章の主な内容は、次のとおりです。

(注)　コラボレーション サイジング ツールを使用しない簡単なサイジングのガイダンスについては、https://www.cisco.com/go/pa で入手可能な『*Cisco Preferred Architecture for Enterprise Collaboration CVD*』の最新版を参照してください。

この章の変更点

表 25-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 25-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Jabber クライアントのサイジング	Cisco Jabber クライアント（25-19 ページ）	2018 年 3 月 1 日
集中型 IM and Presence クラスタのサイジング	集中型 IM and Presence（25-38 ページ）	2018 年 3 月 1 日

システム サイジングに関する方法論

正確なシステム サイジングを実行するため、シスコは、通常の動作条件でシステムが処理する必要がある予想される最大のトラフィックを見積もるため、実際のパフォーマンス テストの結果によってサポートされ、業界標準のトラフィック エンジニアリング モデルが組み込まれている方法論に従います。

次の各項では、サイジングの方法論について説明します。

- パフォーマンス テスト（25-2 ページ）
- システム モデリング（25-3 ページ）
- トラフィック エンジニアリング（25-5 ページ）

パフォーマンス テスト

それぞれの製品は一連の機能を実行し、それぞれの機能はさまざまなリソース（CPU やメモリなど）を利用します。シスコは、さまざまな使用レベルで各機能に対するリソースの使用率を正確に測定できるパフォーマンス テストを定義および実行します。

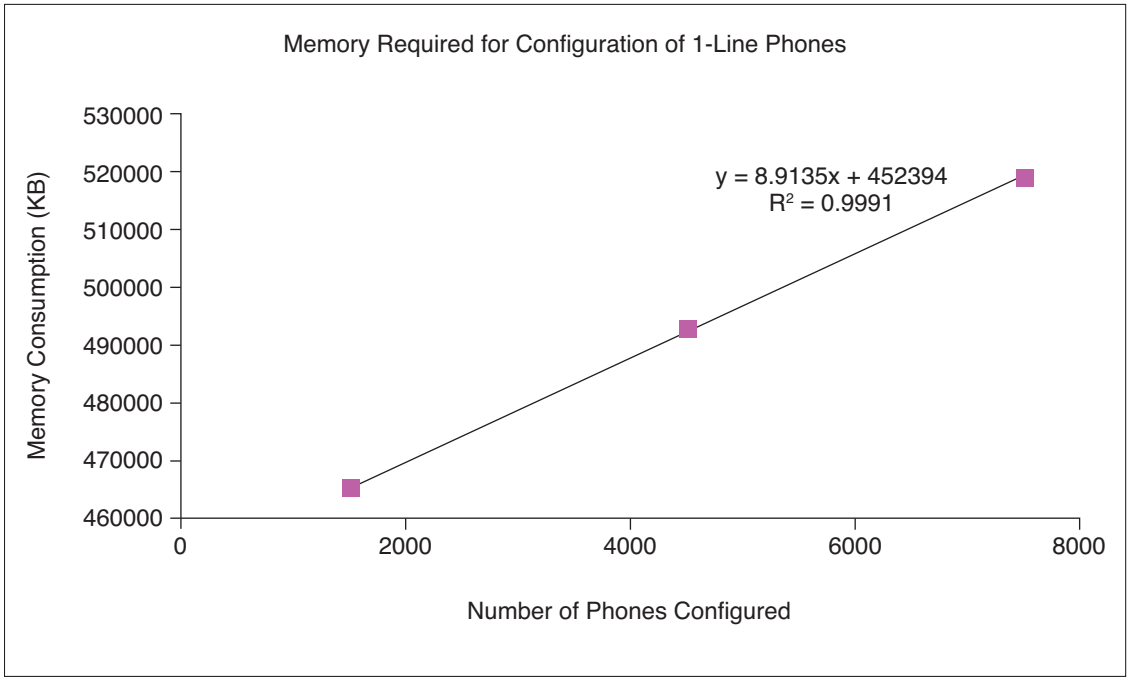
ほとんどのシステムは、特定の範囲内で線形性を示し、その範囲を超えるとシステムのパフォーマンスが予測不能になります。シスコは、各機能のリソース使用率の線形範囲を識別し、確定するため、各パフォーマンス テストに使用レベルを設定します。各テストの結果は、最小限のデータ ポイントを使用してグラフ化できます。必要に応じて、追加のデータ ポイント（中間負荷レベルで）実際のシステム動作を定義するために取得されます。

グラフの線形セクションの傾斜は、追加作業の各差分のリソース使用状況やコストを定義します。R^2 値を使用して、一致精度を予測します。R^2 値が 1 に近い場合、式はデータとほぼ一致しています。

たとえば、図 25-1 に、単一回線の IP Phone を設定するために必要なメモリを判断するために実行されたテストの結果を示します。Unified CM で 1,500 台、4,500 台、および 7,500 台の単一回線の IP Phone を設定することで消費されるメモリを示しています。グラフは、傾向線の式が線形であり、制御変数（電話機の数）に基づく従属変数（この場合はメモリ）の予測に使用できることを示しています。

この特定の試験では、R^2 値はきわめて 1 に近くなっています。式から、7,500 台の単一回線電話の設定で使用されるメモリは約 519,000 キロバイトであり、システム内のエンドポイント用に設定された追加の回線それぞれがさらに 8.91 キロバイトを使用すると計算できます。

図 25-1　　単一回線の電話機の設定に必要なメモリ



システム モデリング

シスコは、パフォーマンス テストの結果を使用してシステム モデルを作成します。システム モデルは、指定された機能、エンドポイント、およびモデルへの入力として提供されるトラフィックの構成のセットに対する最大リソース使用率を計算する数学的モデルです。

特定の製品に対するシステム モデルを作成するには、次の手順を実行します。

1. 製品が実行するすべての機能を列挙します。テストする必要がある機能の種類を識別します。たとえば、各コール タイプが使用する測定されたリソースの量は異なります。
2. 対象のリソースを決定します。通常、メモリおよび CPU が含まれます。特定の製品には、システム サイジングに影響を与える追加のリソースが含まれている可能性があります。
3. パフォーマンス テスト（前述の項で説明）を実行し、各機能のリソース使用率を判別します。
4. 機能ごとに、線形範囲を使用してリソース使用率を定義します。

他の要因（ソフトウェア リリース、コールの構成、エンドポイントのタイプなど）がリソース使用率に影響を与える可能性があるため、これらの手順を何度も実行する必要があります。

製品のシステム モデルは、製品によってサポートされている各機能に関する式の集約で構成されます。一部の製品のモデルはかなりシンプルですが、複数の機能、複数のエンドポイント タイプ、および複数のコール タイプをサポートする製品のモデルは非常に複雑になることがあります。

メモリおよび CPU のリソース タイプに関する特定の考慮事項については、次の項で説明します。

メモリ使用率の分析

システム モデルは、異なる使用特性を持つスタティック メモリとダイナミック メモリを区別します。また、オペレーティング システムとその他のプロセス用に予約されているシステム メモリもあります。これらの 3 つのメモリ タイプについては、次の項で説明します。

スタティック メモリ

スタティック メモリはシステムにトラフィックがない場合でも消費されます。スタティック メモリ使用率には、システム設定のデータおよび登録済みエンドポイントのデータが含まれます。スタティック メモリには、ダイヤル プラン（パーティション、トランスレーション パターン、ルート リスト、およびグループなどの項目を含む）の設定も含まれます。また、スタティック メモリには CTI および他のアプリケーションに割り当てられたメモリも含まれます。大規模なシステムでは、スタティック メモリは、主に設定済みエンドポイント数およびダイヤル プランのサイズの関数です。

消費されるメモリの量は、エンドポイントのタイプごとに異なることに注意してください。メモリ使用率は、デバイス プロトコル（SIP または SCCP）、ライン アピアランスの数、セキュリティ機能、およびその他の要因によって異なる場合もあります。これらの要因をそれぞれ測定し、モデルに組み込む必要があります。

ダイナミック メモリ

ダイナミック メモリは、各アクティブ コールのコンテキストの保存などの一時的なアクティビティに使用されます。大規模なシステムでは、ダイナミック メモリは、主に同時発生コール数の関数です。

同時発生コール数は、平均コール保留時間（ACHT）によって決定されます。ACHT が長くなると同時発生アクティブ コール数が大きくなるため、より多くのダイナミック メモリが使用されます。

メモリ使用率は、コールのタイプおよびプロトコル（SCCP および SIP など）によって大きく異なる場合があります。

システム メモリ

システム メモリは、オペレーティング システム（OS）およびその他のプロセスとサービスによって必要とされます。また、一部のメモリは、一時的な使用率の急激な増加のために予約されている場合があります。システム メモリにより、プラットフォームで動作するアプリケーションで使用可能なメモリ量が減少します。

CPU 使用率の分析

非アクティブなシステムで多少の CPU アクティビティが表示されますが、ほとんどの CPU の使用は、コールのセットアップまたは終了時に発生します。したがって、CPU 使用率の主な決定要因の 1 つは提供されるコール レートです。

CPU 使用率は、コールのタイプによって大きく異なる場合があります。コールは同じサーバ内で発信または終端するか、2 つの異なるサーバまたはクラスタ間で発信または終端できます。また、Unified CM クラスタから発信され、PSTN ゲートウェイまたはトランクで終端することもできます。

CPU 使用率の分析は、Unified CM でのコールの発信と終了のコストの違い、使用中のプロトコル、およびセキュリティ機能が有効かどうかを考慮する必要があります。CPU 使用率は、コンフィギュレーション データベースの複雑さ、および CDR または CMR のどちらが生成されているかなどの要因によっても異なります。

CPU 使用率は、実際のハードウェア プラットフォームによって大幅に異なります。したがって、同じパフォーマンス テストを各製品がサポートされているすべてのサーバに対して繰り返す必要があります。

また、CPU 使用率は、コール転送、会議、およびメディア リソース機能（MTP や保留音）など、CPU 消費が激しいコール操作の影響も受けます。シェアド ラインは、シェアド ラインへの各コールが回線を共有するすべての電話機に提供されるため、追加の CPU リソースを消費します。

トラフィック エンジニアリング

シスコは、業界標準のトラフィック エンジニアリング モデルを使用してシステムの動的な負荷を見積もります。

トラフィック エンジニアリングは、一連のユーザに対して予測される最大トラフィック レベルを計算する数学的モデルを提供します。特定のトラフィック負荷をサポートするのに必要な共有リソース（PSTN トランクなど）の量がモデルによって決まります。

次の項では、異なるタイプのトラフィックに関して、トラフィック エンジニアリングの考慮事項を説明します。

定義

トラフィック エンジニアリングでは、次の用語を定義します。

最大同時コール

システムで一度に処理可能な、同時アクティブ コールの最大数。

コール数/秒

1 秒間にシステムに着信した新しいコールの試行数および同じ 1 秒間に切断した既存のコール数。この単位は、システムが最繁時に受信することが予測される 1 秒間の平均コール数を定義するために使用できます（この数は 60 で割ることによって求められる最繁時のコール数に相当します）。

また、システムが処理する必要があるトラフィックの最大バーストを定義するためにも使用できます。

最繁時

24 時間の中でトラフィックが最大となる 1 時間。この時間は、組織とトラフィックのタイプによって異なります。ビジネス音声トラフィックの場合、従来、最繁時は午前中（たとえば、午前 10 時～午前 11）と見なされています。

最繁時呼数（BHCA）

ユーザ BHCA は、ユーザが最繁時にコールを開始または受信する平均数を表します。通常、BHCA は、1 年間の最も通話の多い 30 日間の最繁時呼数の平均で計算されます。システム BHCA は、ユーザ BHCA にユーザ数を掛け合わせたものです。

ブロック係数

リソース不足によって最繁時にコールがブロックされる確率で表されるサービス グレードを示します。たとえば、1 % のブロック係数は、処理に必要なリソースの不足が原因で 100 コールごとに 1 コールがブロックされる可能性があることを示しています。

平均コール保留時間

リソースがビジーである平均期間です。たとえば、音声コールの場合、ACHT は、2 者間に開いている通話路がある場合のコール設定とコール終了間の期間です。音声システムのトラフィック エンジニアリングで使用する保留時間の業界平均値は 3 分（180 秒）です。

アーラン

アーランはシステムのトラフィック負荷の測定単位です。アーランを計算するには、1 時間あたりのコール数に平均保留時間（1 時間単位）を掛け合わせます。リソース要件は、適切なアーラン モデルを使用してアーランから取得できます。

リソース（トランク グループなど）によって処理されるアーランの数は、同時コール数と等しくなります。アーラン値は通常、1 時間の期間で平均化されます。

アーラン B モデル

アーラン B モデルにより、指定されたブロック係数でトラフィック負荷（アーラン単位）を処理するために必要なトランク数を判断できます。拡張アーラン B モデルには、再試行（ブロックされたコールのため）のモデルが含まれます。再試行の割合は、拡張アーラン B モデルへの追加入力です。

アーラン C モデル

アーラン C モデルは着信コールのキューイングを備えているため、コール センター トラフィックをモデル化するのに非常に役立ちます。

バースト トラフィック

トラフィック モデルは、コール試行の着呼率がかなり安定していることを前提としています。これは、独立して動作する多数のサブスクライバに対して有効な前提です。ただし、実際のシステムでは、多数のコールが非常に短時間に到着する可能性があります。このようなトラフィック バーストはシステム リソースを急速に消費し、多数のコールがブロックされることがあります。製品によっては、処理できるトラフィック バーストのサイズと期間が指定されている可能性があります。

音声トラフィック

標準音声トラフィックは、最繁時呼数（BHCA）および平均コール保留時間（ACHT）の指定によって特徴付けられます。たとえば、システム BHCA が 200 で平均コール期間が 3 分の場合、システムは合計 600 分間（10 アーラン）使用されます。

共有リソース（PSTN トランク グループなど）の使用率を計算するには、ブロック係数も指定する必要があります。たとえば、アーラン値とブロック係数が指定されている場合、アーラン カルキュレータまたはルックアップ テーブルを使用して PSTN ゲートウェイで必要な音声回線を計算できます。

表 25-2 に、トランクの数、ブロック確率、およびトラフィックのアーランの関係を示します。

表 25-2　アーラン B トラフィック テーブル（必要な回線の数）

	ブロック確率					
アーラン数	0.05 %	1 %	2 %	3 %	4 %	5 %
10	19	18	17	16	15	15
20	32	30	36	27	26	26
30	44	54	39	38	37	36

表 25-2 より、次の情報を確認できます。

- アーラン要件が 20 でブロック係数が 1 % の場合、システムには 30 回線が必要です。
- より大きいブロック係数（5 % など）を指定するのではなく、より小さいブロック係数（1 % など）をするには、回線を追加する必要があります。

コンタクト センター トラフィック

コンタクト センターでは、通常これらのシステムが少数のエージェントまたは自動音声応答（IVR）システムによって処理される大量のコールを処理するため、独特のトラフィック パターンが見られます。コンタクト センターは、高いリソース使用率を実現するように設計されているため、エージェント、トランク、および IVR システムは業務時間中（通常は 1 日 24 時間）ずっと稼働した状態が続きます。コール キューイングの使用が一般的で（着信コール トラフィックがオペレータの処理能力を超えると、次のオペレータが空くまでコールはキュー内で待機します）、オペレータは通常、自分の勤務時間の間、コンタクト センターに寄せられた電話の応対に専念します。

コンタクト センターでのコールの平均保留時間は、多くの場合、通常のビジネス コールよりも短くなります。IVR システムの段階で用件が済み、オペレータと通話しない場合が多くなります。これらのコールは、セルフサービス コールと呼ばれます。エージェントの平均保留時間は 3 分（一般業務トラフィックと同じ）であるのに対して、セルフサービス コールの平均保留時間は約 30 秒であることから、コンタクト センター全体での平均保留時間は一般業務トラフィックよりも短くなります。

コンタクト センター管理の目標は、リソース（IVR ポート、PSTN トランク、オペレータなど）の使用を最適化するためです。そのため、リソース使用率が高くなります。

コンタクト センターでは通常、一般的な業務環境よりも着呼率が高くなります。これらの着呼率は、一般業務トラフィックとは異なる時間帯（通常の最繁時ではない時間帯）に異なる理由で最大になります。たとえば、特別な休日パックのテレビ CM を流して申し込み用のフリー ダイヤルを知らせた場合、システムの着呼率は、CM 放送後の約 15 分間にトラフィックのピークを迎えます。この着呼率は、コンタクト センターの平均着呼率を 1 桁上回ることもあります。

前述したように、コンタクト センターのサイジングは、アーラン C モデルを使用してキューで待機中のコールを考慮します。コンタクト センターには、自動音声応答（IVR）ポートなどの追加のリソースが必要です。PSTN ゲートウェイをサイジングする場合は、キューでコールが待機する時間を考慮する必要があります（コンタクト センター トラフィックに対するゲートウェイのサイジング（25-42 ページ）を参照）。

(注)　シスコ ユニファイド コンタクト センターの導入に関する追加情報については、次の場所にある『*Solution Design Guide for Cisco Unified Contact Center Enterprise*』の最新版を参照してください。https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html。

ビデオ トラフィック

ポイントツーポイント ビデオ トラフィックは、着呼率、ピーク時の使用時間、および通話時間が同等の音声トラフィックと類似した特徴を示します。また、コール セットアップおよび終了のシグナリングは、音声コールに類似しています。

ビデオ パケットのペイロードは音声パケットよりもはるかに大きいため、ビデオ トラフィックには、音声をはるかに上回るネットワーク帯域幅が必要です。また、ビデオ トラフィックは、音声よりもバーストが大きくなります。音声パケット サイズは、通常はほぼ一定（使用中のエンコーディング アルゴリズムによって固有）ですが、ビデオ フレームのサイズは、以前のフレームからどれほどの変更があったかに応じて大幅に異なります。その結果、RTP パケット ストリームはトラフィックのバーストを示すことがあります。

ビデオ会議への影響については、次の項で説明します。

会議およびコラボレーション トラフィック

会議トラフィックには、ポイントツーポイントの音声/ビデオ コールとは大きく異なる特性があります。会議トラフィックのトラフィック モデルでは、次の違いを考慮する必要があります。

- コール到達

  従来のトラフィック モデルは、最繁時の着信が最繁時全体に渡ってポアソン分布することを前提としています。ただし、ほとんどの参加者は、開始時間の 5 ～ 10 分以内に会議コールに参加し、ほとんどの会議コールは正時に開始されるようにスケジューリングされています。したがって、着呼率は、時間全体でのポアソン分布ではなく、開始後 0 分の単一のバーストで表されます。

- ピーク

  ビジネス音声トラフィックには通常、午前中（10:00 ～ 11:00 AM）と午後（1:00 ～ 2:00 PM）の個別のピークがあります。ただし、会議機能は通常は限られたリソースであるため、会議は、営業日全体により均等に配布され、ピーク時にピークが緩和されます。

- 通話時間

  平均ビジネス音声コール期間は 3 分です。平均会議コール時間はほぼ 50 分です（30 分、60 分、さらに長い会議の組み合わせによって異なります）。

- ビデオ会議

  ビデオ ストリームの切り替えまたは組み合わせを提供するには、専用装置が必要です。そのため、ビデオ エンドポイントの予期される使用率は、モデルにおける重要な要素です。

会議用の導入のサイジングでは、主に必要な同時接続数を特定します。たとえば、TelePresence Server のサイジングでは次の事項を考慮する必要があります。

- 地理的なロケーション：Unified CM のサービスを提供する地域ごとに、会議専用のリソースを確保する必要があります。
- TelePresence Server プラットフォームの選択：ハードウェアかソフトウェアか
- TelePresence Server プラットフォームの容量
- TelePresence Conductor プラットフォームの容量
- 会議のタイプ：音声またはビデオ（あるいはその両方）。スケジュールされた会議またはスケジュールされていない会議（あるいはその両方）
- 会議のビデオ解像度：高品質の会議ほど多くのリソースを消費します。
- 大規模な会議の要件：オールハンズ ミーティングなど

地域ネットワークの会議メディアをできるだけ多く維持するため、会議リソースは一般に 1 つの地域でのみ使用されます。したがって、サイジングは地域単位で検討することができます。

システム サイジングの考慮事項

大規模で複雑な導入の場合、システム設計者は、システム サイジングに影響する多くの設計と導入の要因を考慮する必要があります。次の項では、これらの要因について説明します。

- ネットワーク設計の要因（25-9 ページ）
- その他のサイジングの要因（25-10 ページ）

ネットワーク設計の要因

ソリューション サイジングは、次のネットワーク設計の要素の影響を受けます。

- クラスタ サイズ

  主要な設計上の決定項目として、大規模な集中型の Cisco Unified CM クラスタを作成するか、それぞれの主要な場所でクラスタを作成するかどうかがあります。中央クラスタの使用率は高くなる可能性がありますが、クラスタの制限を超えた場合は、2 つめのクラスタを使用せざるを得なくなる可能性があります。

  一部のシステムの制限は絶対ではなく、システムで設定された他のサービスのサイズに基づいて動的に変更できます。

- 個々の製品間の相互作用

  Unified CM は、ほとんどの Cisco Collaboration 配置において中心的な役割を果たしており、システムの他のコンポーネントによって影響を受けます。たとえば、Cisco WebEx Meetings Server の追加は、短時間（会議セッションの開始時）に多数のコール セットアップを集中させる傾向があります。Unified CM によって網羅された他の機能に応じて、追加の Unified CM サーバ ノードが必要になる場合があります。

- サーバ機能

  それぞれのタイプのサーバまたはルータは、異なる機能をサポートします。たとえば、より強力なサーバには Cisco Business Edition 6000 プラットフォームまたは Cisco Integrated Services Router（ISR）よりも多くのネットワーク ポートがある場合があります。

  別の例として、Cisco Integrated Service Router（ISR）の各種モデルでは、ホストできるネットワーク モジュールまたは Cisco Unified Computing System（UCS）E シリーズ ブレード サーバのモジュールの数とタイプに制限があります。

- オプションの機能

  システム サイジングは、コール詳細レコード（CDR）またはコール管理レコード（CMR）の生成などのオプションを有効にしている場合に影響を受ける可能性があります。

その他のサイジングの要因

次の追加の要因もシステム サイジングに影響します。

- コール タイプの混合

  各コール タイプ（同じサブスクライバ ノード内の電話機間のコール、同じクラスタ内の 2 つのサブスクライバ ノード間のコール、2 つのクラスタ間のコール、および PSTN に出入りするコール）によって消費されるリソースには違いがあります。異なるタイプの電話機やゲートウェイからのコールも、プロトコルやビデオなどのサービスによって異なります。

- エンドポイント タイプの混合

  サイジングに影響する別の明確な要因の例として、期待される電話機とユーザの数があります。この場合も、電話機のタイプ、電話機に設定されている回線の数、電話機がセキュア モードであるかどうかなどがシステム サイジングに影響します。

- システム リリース

  システム リソースの使用率は、システム リリースに応じて異なることがあります。場合によっては、リリースの新機能によってリソース使用率が増加する原因となる可能性があります。また、ソフトウェアの向上によってリソース使用率が低下する可能性があります。

- 外部アプリケーションの使用

  外部アプリケーションは、CTI などのインターフェイスを使用してコール処理エージェントと通信できます。システム サイジングでは、この負荷の影響を考慮する必要があります。

- 予想されるシステムの拡張

  システム使用率が来年または再来年に増加することが予測されている場合は、近い将来に破壊的とも言える可能性のあるアップグレードに直面する代わりに、その成長を元のシステムに組み込むことを推奨します。

- 平均およびピーク時使用率

  システム サイジングが、現実的なピーク時使用率の観点に基づいていることを確認します。ピークが過小評価されていると、実際にピーク トラフィックに遭遇した場合に、システムでサービスの低下または機器の障害が発生する可能性があります。

すべての要因およびその変動の可能性により、大規模システム配置の正確なサイジングは複雑な作業です。このため、シスコは次の項で説明するシステム サイジング ツールを使用することを強く推奨します。

サイジング ツールの概要

シスコでは、正確なソリューション サイジングを支援する複数のサイジング ツールを提供しています。サイジング ツールは、次のサイトで入手できます（シスコの従業員および認定パートナーだけがこのサイトにアクセスできます）。

https://cucst.cloudapps.cisco.com/landing

シスコは、サイジング ツールを使用してシステム サイジングを実行することを推奨します。これらのツールでは、パフォーマンス テストに基づくデータ、個々の製品制限とパフォーマンス レーティング、製品リリースにおける拡張機能と新規機能、この SRND の設計上の推奨事項、およびその他の要因が考慮されています。システム設計者によって提供される入力に基づいて、ツールは、サイジング アルゴリズムを提供されたデータに適用して、一連のハードウェア リソースを推奨します。

サイジング ツールにアクセスできない場合は、シスコ アカウント担当者またはシスコ パートナー インテグレータに問い合わせて、システムのサイジング情報を取得してください。

次のツール固有の項には、ツールに必要な入力に関する説明、および最適な入力内容を既存のシステムから収集する方法、また設計段階のシステムに対して見積もる方法が記載されています。言うまでもなく、ツールによって生成されるサイジングの推奨内容は、ユーザが提供する入力データの正確性と同程度の正確性しかありません。

シスコは、次のサイジング ツールを提供しています。

- Cisco Collaboration Sizing Tool

  このツールは、システムの導入全体を通してユーザをガイドします。このツールは、次の製品およびコンポーネントに対応しています。

  - Cisco Unified Communications Manager（Unified CM）
  - IM and Presence サービス
  - ボイス メッセージング
  - [会議（Conferencing）]
  - ゲートウェイ
  - Cisco Unified Communications Management Suite
  - Cisco Unified Contact Center コンポーネント

- Cisco Unified Communications Manager Session Management Edition（SME）Sizing Tool

  これは、Unified CM Session Management Edition の導入の特定の機能に重点を置いた専用ツールです。

- Cisco VXI Sizing and Configuration Tool

  これは、Cisco Virtual Experience Infrastructure（VXI）のサイジング専用ツールです。

これらのツールおよびアクセス権限の詳細については、次の場所にある『*Collaboration Sizing Tool Frequently Asked Questions*』を参照してください。

https://cucst.cloudapps.cisco.com/help/UC_Sizing_Tools_FAQ.pdf

注意　システム設計のいずれかのパラメータが、前述のサイジング ツールが入力を許容する値の範囲を超える場合、作業を進める前に設計についてシスコのアカウント チームまたはシスコのシステム エンジニア（SE）に相談する必要があります。

これらのサイジング ツールに加えて、有効なログイン アカウントを持つシスコのパートナーとお客様は Virtual Machine Placement Tool を Virtual Machine Placement Tool 利用できます。Virtual Machine Placement Tool は、Tested Reference Configurations（TRC）または仕様ベースのハードウェアを選択し、これらのサーバ上のさまざまな Cisco Collaboration アプリケーションの仮想マシンをドラッグ アンド ドロップするグラフィカル ツールです。サードパーティ製アプリケーションの仮想マシンを表すプレースホルダは、Cisco Collaboration アプリケーションをサードパーティ製アプリケーションと共存させて配置する際にも使用できます。サイジング ツールは、必要なサーバの規模と仮想マシンの台数を決定します。さまざまな仮想マシンの配置方法や配置する必要のあるサーバ数を決定するために、この情報を Virtual Machine Placement Tool に入力できます。共存ルールの一部はツールに実装されていますが、次の Web サイトで入手可能なガイドラインを確認することを推奨します。

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html

Virtual Machine Placement Tool は次の Web サイトから入手可能です（正しいログイン認証がある場合）。

https://www.cisco.com/go/vmpt

SME サイジング ツールの使用

Session Management Edition（SME）は、特定の導入モードで動作する Unified CM です。純粋な SME の導入では、コール トラフィックがトランク インターフェイスでのみ動作し、SME はライン インターフェイスをホストしません。

SME クラスタは、通常の Unified CM クラスタと同じトポロジに従います。パブリッシャ ノードにマスター設定リポジトリが用意されています。クラスタ内の電話機や MGCP ゲートウェイの数が比較的少ない場合、TFTP サービスをパブリッシャ ノードで実行できます。呼処理サブスクライバについては、冗長性の比率を 1:1 にすることを推奨します。

SME クラスタをサイジングするには、期待される機能を考慮する必要があります。基本構成では、SME は、多くのリーフ クラスタのルーティング集約ポイントとして機能します。接続されているすべてのリーフ クラスタに集中型 PSTN アクセスを提供します。高度な構成では、SME は集中型ボイス メッセージング、モビリティ、および会議サービスもホストできます。SME のパフォーマンスは、リーフ クラスタが SME への接続に使用するトランク プロトコルのタイプおよびこれらのトランクの BHCA の影響を受けます。

SME のサイジング ツールには、次の入力パラメータが必要です。

- クラスタが処理するトランク インターフェイスの各種タイプ。SME では次のトランク プロトコルがサポートされます。ただし、優先プロトコルとしては SIP トランクを推奨します。
  - SIP
  - H.323
  - MGCP（Q.931）
  - SIP（Q.SIG）
  - H.323 Annex M1
  - MGCP（Q.SIG）
- トランク インターフェイスの各タイプを経由して SME クラスタ サービスにアクセスするユーザの数。
- クラスタ間コールのためにリーフ クラスタへの各トランク インターフェイスにアクセスするユーザあたりの BHCA

- オフネット（PSTN）コールのためにリーフ クラスタへの各トランク インターフェイスにアクセスするユーザあたりの BHCA
- SME クラスタによって PSTN への接続に使用されるトランク インターフェイスのタイプ
- コールの平均保留時間
- ルートおよびトランスレーション パターンの数

SME がサービス集約ポイントとして機能する場合は、次の追加のサイジング パラメータを考慮する必要があります。

- 集中型ボイス メッセージングの場合、ボイスメールに送信されるコールの割合
- モビリティの場合、ユーザの数およびユーザあたりのリモート接続先の数
- 会議の場合、会議ダイヤルイン間隔

SME のパフォーマンスは、プロトコルの各ペアの 1 秒あたりのコール数で測定されます。ハードウェア プラットフォームやソフトウェア バージョン間で違いがあります。

VXI サイジング ツールの使用

Cisco Virtualization Experience Infrastructure（VXI）はシステム アプローチの 1 つであり、仮想デスクトップ、音声、およびビデオを統合することで、優れた仮想ワークスペース エクスペリエンスを提供します。Cisco VXI Sizing Tool は、Virtualization Experience Infrastructure ソリューションのサイジング コンポーネントのタスクを支援します。

Cisco Collaboration Sizing Tool の使用

Cisco Collaboration Sizing Tool は、さまざまな製品やコンポーネントのサイジングに対応しています。ツールによってサポートされているコンポーネントとバージョンの完全なリストについては、サイジング ツールのインストール パッケージに含まれているリリース ノートを参照してください。

次の項では、各製品のサイジングに影響する重要な要因、およびこれらの各製品がシステム導入内の他の製品のサイジングに関する考慮事項に及ぼす影響について説明します。

- Cisco Unified Communications Manager（25-14 ページ）
- メディア リソース（25-30 ページ）
- Cisco Unified CM メガクラスタの導入（25-34 ページ）
- Cisco IM and Presence（25-35 ページ）
- 緊急サービス（25-38 ページ）
- ゲートウェイ（25-41 ページ）
- ボイス メッセージング（25-45 ページ）
- コラボレーティブ会議（25-47 ページ）
- Cisco Prime Collaboration 管理ツール（25-51 ページ）
- Cisco Unified Communications Manager Express（25-52 ページ）
- Cisco Business Edition（25-53 ページ）

Cisco Unified Communications Manager

Cisco Unified Communications Manager（Unified CM）は、Unified Communications 導入のハブです。これは、エンドポイントの制御、コールのルーティング、ポリシーの施行、およびアプリケーションのホストなどの主要な機能を実行します。Unified CM は、PSTN ゲートウェイ、Cisco Unity Connection、Cisco Unified MeetingPlace、Cisco Unified Communications Manager IM and Presence Service、および Cisco Unified Contact Center などの他の Unified Communications 製品に対する連携を提供します。連携機能は、Unified CM のパフォーマンスに影響を与えるため、Unified CM サイジングで考慮する必要があります。

多くの要因が Unified CM のパフォーマンスに影響するため、Unified CM 導入のサイジングで考慮する必要があります。次の項では、これらの要因について説明します。

仮想ノードとクラスタの最大数

サイジング ツールには、次のサーバ ノードとクラスタの最大数が適用されます。これらの値は、Unified CM ソフトウェアのバージョンに応じて異なることがあります。

- 各クラスタは、最大 40,000 台のセキュアまたは非セキュア SCCP または SIP 電話機の設定および登録をサポートできます。
- クラスタ内のエンドポイント数が 1,250 を超えた場合は、専用パブリッシャに加えて 2 つの TFTP サーバ ノードが必要です。
- CTI 接続のサポートが最新のいくつかのリリースで向上し、各クラスタは最大 40,000 の CTI 接続をサポートできます。
- クラスタ内の呼処理サブスクライバの数は、4 つおよびスタンバイ 4 つの合計 8 つの呼処理サブスクライバ ノードを超えることはできません。また、パブリッシャ、TFTP、メディア サーバなどのクラスタ内のサーバ ノードの合計数がクラスタで許可されるサーバの最大数である 21 を超えることはできません。
- Unified CM の仮想マシン（VM）設定の名前は、平均で各ユーザに電話機 1 台と想定した場合の最大ユーザ数に相当します。そうでない場合は、VM 設定は、Unified CM ノードに登録されているエンドポイントの最大数を示します。たとえば、10k ユーザの VM 設定では、ユーザ 1 人あたり 1 台のデバイスと想定し、最大 10,000 人のユーザをサポートします。ただし、ユーザ 1 人あたりに複数のデバイスを導入する場合、サポートされるユーザの最大数は減少します。たとえば、ユーザ 1 人あたりのデバイスが 2 台の場合は、10k ユーザの VM 設定でサポートするユーザ数は最大 5,000 人、デバイスは最大 10,000 台になります。この原則は、小規模な Unified CM VM 設定にも適用されます。

展開オプション

次の導入オプションは、システム内のすべての動作に影響する全体的な設定であり、登録されているエンドポイントの数や進行中のコールの数とは無関係です。

データベースの複雑さ

Unified CM のコンフィギュレーション データベースが複雑であると見なされる場合、CPU 使用率はかなり高くなります。データベースが単純か複雑かを判断するメトリックはありません。一般に、数千を超えるエンドポイントと数百を超えるダイヤル プラン要素（トランスレーションおよびルート パターン、ハント パイロット、シェアド ラインなど）がある場合、データベースは複雑になります。

リージョンおよびロケーションの数

Unified CM クラスタ内のリージョンとロケーションの設定には、データベースとスタティック メモリの両方が必要です。クラスタに定義できるゲートウェイの数は、定義できるロケーションの数にも関係します。表 25-3 に、一部の Unified CM の VM 設定におけるこれらの制限を示します。

表 25-3　リージョン、ロケーション、ゲートウェイ、およびトランクの最大数

VM 設定	リージョンの最大数	ロケーションの最大数	トランクとゲートウェイの最大数
1,000 人または 2,500 人のユーザ	1,000	1,000	1,100
7,500 人または 10,000 人のユーザ	2,000	2,000	2,100

クラスタに最大数のロケーションとリージョンを実際に定義できるかどうかは、コーデック マトリクスがどの程度「疎」であるかによって異なります。リージョン間コーデック設定にデフォルト以外の値が多すぎる場合は、リージョンまたはロケーションのためにシステムをフル キャパシティに拡張できません。一般に、デフォルトからの変更は最大数の 10% を超えないようにします。

コール詳細レコードおよびコール管理レコード

コール詳細レコード（CDR）とコール管理レコード（CMR）の生成により、CPU に大きな負荷がかかります。

高可用性

指定した導入に必要なノードの最小数を特定した後、冗長性を提供するために目的の数の追加のサブスクライバ ノードを追加します。冗長性オプションについては、呼処理（9-1 ページ）の章を参照してください。

クラスタあたりの仮想サーバ ノードの数

通常のクラスタに最大 4 つのサブスクライバ ペアを設定できます。分散型トポロジでは、クラスタが最大数に達していない場合でも複数のクラスタがある場合があります。

集中型トポロジの場合、キャパシティの制限に到達しない限りは通常は 1 つのクラスタがあります。他のシステム制限によって、ノードごとの使用率が制限に達していない場合でも、新しいクラスタを使用せざるを得ない可能性があることに注意してください。

VM 設定およびハードウェア プラットフォームの選択

シスコはハイパーバイザにロードできる Open Virtualization Archive（OVA）の VM 設定を提供します。指定する機能はテンプレートごとに異なります。たとえば、10,000 人のユーザ用テンプレートでは、10,000 個のエンドポイントの最大キャパシティを持つ仮想マシンを定義します。また、最大 1,000、2,500、および 7,500 個のエンドポイントをサポートするように定義されたテンプレートもあります。

Unified CM およびその他の Unified Communications 製品用に正式に定義された VM 設定は、次の Web サイトから入手できます。

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html

Unified CM の特定の情報については、次の Web サイトから入手できます。

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-communications-manager.html

Unified CM では、VM 設定の一部はローエンド ハードウェア プラットフォームではサポートされていません。どの VM 設定がハードウェア プラットフォームでサポートされているかを確認するには、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/go/virtualized-collaboration

ハードウェアおよび仮想化ソフトウェアの要件

次の要件は、すべてのアプリケーションに共通です。追加の要件および制限事項については、各アプリケーションの製品マニュアルを参照してください。

- サポートされている必要な仮想化ハードウェアの詳細については、次の Web サイトを参照してください。

  https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-hardware.html

- サポートされている必要な仮想化ソフトウェアの詳細については、次の Web サイトを参照してください。

  https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html

（注）　Unified CM およびその他の Unified Communications 製品を実行する仮想マシンの配置の選択は、パフォーマンスと可用性に影響することがあります。これらの詳細および UCS の導入における Unified Communications のその他の考慮事項については、次の Web サイトのマニュアルを参照してください。
http://www.cisco.com/go/virtualized-collaboration。

エンドポイント

エンドポイントの数は、システムでサポートする必要がある全体の負荷の重要な部分です。さまざまなタイプのエンドポイントがあり、タイプごとに Unified CM にかかる負荷は異なります。エンドポイントは次の要素で区別できます。

- デジタル（IP）またはアナログ（アダプタを使用）
- ソフトウェアベースまたはハードウェア
- サポートされるプロトコル（SIP または SCCP）
- エンドポイントでセキュリティが設定されているかどうか
- ダイヤル モード（一括またはオーバーラップ）
- 音声のみ、または音声とビデオ
- ゲートウェイなどの他のデバイス（H.323 または MGCP）

システムで設定されている各エンドポイントは、定義され登録されているだけのシステム リソース（スタティック メモリなど）を使用します。エンドポイントは、コール レートに基づいて CPU とダイナミック メモリを消費します。

エンドポイントは、Unified CM 内で実行されるサービスと対話するアプリケーション（CTI など）を実行することによって、Unified CM にさらに負荷をかけます。

表 25-4 に、異なるタイプの VM 設定でサポートされているエンドポイントの最大数を示します。これらはガイドラインとしての値であることに注意してください。導入に他のアプリケーションが含まれているために、システムによってはこれらの最大容量をサポートしない場合があります。

表 25-4　VM 設定ごとにサポートされるエンドポイントの最大数

VM 設定	OVA テンプレートごとの最大エンドポイント数[1]
10,000 人のユーザ	10,000
7,500 人のユーザ	7,500
2,500 人のユーザ	2,500
1,000 人のユーザ	1,000

1. これらの制限は、データベースで設定され、仮想サブスクライバ ノードごとに登録可能なエンドポイントの最大数を表します。メディア ターミネーション ポイント（ソフトウェアのハードウェア）または SIP トランクなどの他のすべての登録済みデバイスは、これらの制限に対してカウントされません。

Cisco Collaboration System Release（CSR）12.*x* では、次の VM 設定テンプレートの場合、Unified CM を導入するのに、すべての仮想ノードで vRAM のメモリを 2 GB 増やす必要があります。

- 1,000 ユーザ
  - 2 vCPU
  - 6 GB の vRAM
  - 80 GB の vDisk
- 2,500 ユーザ
  - 4 vCPU
  - 6 GB の vRAM
  - 80 GB の vDisk

- 7,500 ユーザ
  - 2 vCPU
  - 8 GB の vRAM
  - 110 GB の vDisk
- 10,000 ユーザ
  - 4 vCPU
  - 8 GB の vRAM
  - 110 GB の vDisk

詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/go/virtualized-collaboration

Cisco Collaboration クライアントおよびアプリケーション

Cisco Collaboration クライアントには、ユーザのデスクトップや他のアクセス デバイスで実行される、次のソフトウェア アプリケーションが含まれます。

- Cisco Jabber クライアント（25-19 ページ）
- Cisco WebEx Connect（25-21 ページ）
- Cisco UC Integration™ for Microsoft Lync（25-22 ページ）
- サードパーティ製 XMPP クライアントとアプリケーション（25-22 ページ）

Cisco Jabber デスクトップ クライアント

Cisco Jabber は、Windows 用と Mac 用の Cisco Jabber クライアントおよび Microsoft Lync 用の Cisco UC Integration™ を含めて、これらのクライアントの基本となるサービス レイヤを提供します。

Jabber デスクトップ クライアントは、Unified CM でそれぞれが異なるリソースを使用する 2 つのオペレーション モードを提供します。Jabber クライアントは、ソフトフォン モードで動作する場合、SIP 登録されたエンドポイントとして機能し、システム内のエンドポイントの総数としてカウントされます。Jabber クライアントは、デスクフォン モードで動作する場合、CTI エージェントとして機能するため、Unified CM で CTI リソースを使用します。

ユーザは、いずれかのモードで動作するように Jabber ベースのクライアントを切り替えることができます。したがって、予想される使用方法に必要なシステム リソースを正しく把握する必要があります。

Jabber デスクトップ クライアントの導入では、さらに次の項目についても考慮する必要があります。

- デバイス設定

  ソフトフォン モードで設定した場合は、Unified CM 呼制御の設定情報のために、Jabber デスクトップ クライアントのコンフィギュレーション ファイルが TFTP または HTTP 経由でクライアントにダウンロードされます。さらに、アプリケーション ダイヤル規則やディレクトリ ルックアップ規則があれば、それらも TFTP または HTTP を介して Jabber デスクトップ クライアントのデバイスにダウンロードされます。

  Jabber デスクトップ クライアントは Cisco Unified CM Cisco IP Phone（CCMCIP）または UDS サービスを使用してユーザに関連付けられたデバイスについての情報を集め、この情報を使用してデスクフォン制御モードにあるクライアントが制御可能な IP Phone のリストを提供します。ソフトフォン モードの Jabber デスクトップ クライアントは、Unified CM への登録のデバイス名を検出するために CCMCIP または UDS サービスを使用します。

- デスクフォン モード

  デスクフォン モードで設定した場合は、IP Phone の制御を可能にするために、ログインと登録の際に Jabber デスクトップ クライアントが Unified CM への CTI 接続を確立します。Unified CM は、最大 40,000 個の CTI 接続をサポートします。デスク フォン モードで動作する多数のクライアントがある場合は、CTI 接続を CTIManager サービスを実行中の Unified CM サブスクライバ全体に均等に分散させるようにします。このことは、それぞれ異なる CTIManager アドレスのペアを持つ複数の CTI ゲートウェイ プロファイルを作成し、CTI ゲートウェイ プロファイルの割り当てをデスクフォン モードを使用するすべてのクライアントに配分することで実現できます。

- [ボイスメール（Voicemail）]

  ボイスメール用に設定されている場合、Jabber デスクトップ クライアントは、メールストアとの IMAP または REST 接続を通じてボイスメールを更新および取得します。

- 認証

  クライアントのログインと認証、コンタクト プロファイル情報、および着信したコールの発信者 ID のすべてが、ローカル Jabber デスクトップ クライアント キャッシュに保存されていない限り、LDAP ディレクトリへの照会を通じて処理されます。

- 連絡先の検索

  Jabber デスクトップ クライアントで使用できる複数のコンタクト ソースがあります。たとえば、UDS サービスは、クライアントが Unified CM ユーザ データベース内のコンタクトを検索するために使用できます。また、LDAP 統合を使用できます。要求されたコンタクトがローカル Jabber デスクトップ クライアント キャッシュで見つからない場合は、UDS または LDAP のコンタクト検索が実行されます。

Cisco Jabber クライアント

Cisco Jabber クライアントのためのソリューションの設計とサイジングを検討する際は、すべてのコンポーネントについて、スケーラビリティに関する次のインパクトを考慮する必要があります。

- クライアントのスケーラビリティ

  Cisco IM and Presence サービス VM 設定テンプレートによって、クラスタでサポートできるユーザの数が決定されます。Cisco Jabber クライアントの導入は、クラスタ内の全ノードで、全ユーザに均等にする必要があります。これは、User Assignment Mode Sync Agent サービス パラメータを [balanced] に設定すれば、自動的に処理されます。

- IMAP のスケーラビリティ

  IMAP または IMAP-Idle の接続数は、メッセージング統合プラットフォームが決定します。

- 音声、ビデオ、および Web 会議

  クライアントは、ネットワークで提供される会議サービスにアクセスできます。これらのサービスの同時参加者の数をサイジングする場合、これらのユーザを考慮する必要があります。詳細については、Cisco Rich Media Conferencing（11-1 ページ）の章を参照してください。

Cisco Jabber クライアントは、iPhone、iPad、Android ではモバイル クライアントとして、Windows と Mac ではデスクトップ クライアントとしてサポートされます。Jabber クライアントを使用した導入のサイジングでは、ユーザがデスクトップ クライアントとモバイル クライアントの任意の組み合わせを使用している可能性があることに注意してください。ユーザに対してマルチ デバイス メッセージング（MDM）機能が有効になっている場合は、ユーザに関連付けられた各クライアントがデバイスと見なされるため、Unified CM テンプレートと IM and Presence VM テンプレートの両方で、サポートされるユーザの総数にカウントされます。

(注)　ユーザがデスクトップ制御モードで 1 つの Jabber デスクトップ クライアントだけを使用している場合は、単一のデバイスと見なされます。これは、デスク フォン制御が CTI リソースと回線を利用するという事実によります。

Cisco Jabber クライアントは、Unified CM と連携します。そのため、Cisco Jabber クライアントの音声またはビデオ コールを開始した場合、Unified CM の現在の機能に関する次のガイドラインが適用されます。

- CTI のスケーラビリティ

  デスクフォン モードでは、Cisco Jabber クライアントからのコールは Unified CM の CTI インターフェイスを使用します。したがって、呼処理 (9-1 ページ) の章に明記された CTI の制限を遵守してください。Unified CM クラスタのサイジングを行う際は、これらの CTI デバイスを含める必要があります。

- コール アドミッション制御

  Cisco Jabber クライアントは、Unified CM ロケーションまたは RSVP 経由で、音声またはビデオ コールに対してコール アドミッション制御を適用します。

- コーデックの選択

  Cisco Jabber クライアントの音声およびビデオ コールは、Unified CM リージョン設定によるコーデックの選択を利用します。

- Cisco Unity Connection

  このマニュアルのシスコのボイス メッセージング (19-1 ページ) の章の帯域幅の管理 (19-33 ページ) の項を参照してください。

- Cisco Jabber クライアントは、iPhone、iPad、Droid ではモバイル クライアントとして、Windows PC と Mac ではデスクトップ クライアントとしてサポートされます。

  Jabber クライアントを使用した導入のサイジングでは、ユーザがデスクトップ クライアントとモバイル クライアントを使用している場合や複数のモバイル クライアントまたはデスクトップ クライアントを使用している場合があることに注意してください。マルチ デバイス メッセージング (MDM) のユーザの方がこの機能を要求する可能性が高くなります。有効になっている場合は、ユーザに関連付けられた各クライアントがデバイスと見なされるため、Unified CM テンプレートと IM and Presence VM テンプレートの両方で、サポートされるユーザの総数にカウントされます。ユーザがデスクトップ制御モードで 1 つの Jabber デスクトップ クライアントだけを使用している場合は、単一のデバイスと見なされます。これは、デスク フォン制御が CTI リソースを利用するという事実によります。

- Cisco WebEx Meetings Server

  Cisco WebEx Meetings Server は、仮想化環境内の音声、ビデオ、コラボレーションのセッションで WebEx 会議サービスを提供します。Cisco WebEx Meetings Server の詳細については、次の Web サイトで入手可能な『*Cisco WebEx Meetings Server Planning Guide and System Requirements*』を参照してください。

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

- Cisco Unified CM ユーザ データ サービス (UDS)

  UDS は、Unified CM によって提供される包括的なサービス API です。UDS は、Jabber over Cisco Edge シリーズのデバイスが連絡先ソースの検索に使用できる連絡先ソース API を提供します。UDS の連絡先ソースを連絡先の解決に使用すると、システムにさらに負荷がかかります。

SAML SSO Cisco Jabber クライアント

Cisco Unified CM 10.*x* は、Security Assertion Markup Language シングル サインオン（SAML SSO）機能を提供します。この機能を使用すると、ユーザが 1 度のログインで Cisco Collaboration ソリューション内のすべてのアプリケーションにアクセスできるため、エンド ユーザのエクスペリエンスが向上します。

SAML SSO はエンド ユーザのクレデンシャルや関連情報を使用して複数の Unified Communications のアプリケーション（Unified CM、Cisco Unity Connection、IM and Presence など）に利用するセキュアなメカニズムを提供します。SAML シングル サインオン機能が予想どおりに機能するように、ネットワーク アーキテクチャは各クラスタのユーザ数をサポートするように拡張する必要があります。

複数のアプリケーション（Unified CM、Cisco Unity Connection、IM and Presence など）への Unified Communications の導入の場合、すべての SAML 要求は ID プロバイダー（IdP）で認証して Cisco Jabber クライアントが正常にログインするようにする必要があります。

（注）　SSO は SAML を使用して Unified Communications サービスでサポートされます。

普段の日の同じ時刻にシステムにログインするユーザの数がユーザがログインするための所要時間に影響する可能性があるため、システム サイジングでは SAML SSO ログインによる Cisco Jabber も考慮する必要があります。システムが 1 回につき処理できる要求の数の制限要因により、これが予期されます。Jabber ユーザの現在の最大ログイン レートは 1 秒あたり 2.7 ログイン（1 分あたり約 166 ログイン）または 1 時間内で 10,000 ログインです。これは、すべてのユーザとデバイスがすべてのノードに均一に分散されており、Cosco Jabber がソフトフォン モードにあることを想定しています。

Unified CM クラスタの安定性に影響する可能性がある相互依存変数（リージョン、ロケーション、ゲートウェイ、メディア リソースなど）が多数存在しています。したがって、必要な負荷の処理にリソースを使用できるように効果的に導入するには、ユーザの数、エンドポイント、1 時間あたりの 1 ユーザごとのコール数を特定することが重要です。

たとえば、5,000 人のユーザをサポートする冗長サブスクライバ ペアで、それぞれが 2 つのデバイス（デスク フォンとソフトフォン）に関連付けられている導入を検討します。この導入では、次の数の仮想マシンと VM 設定が必要です（高可用性と冗長性を想定）。

- 10k ユーザの VM 設定の Unified CM サブスクライバを 1 ペア
- IM and Presence の 5k ユーザの VM 設定を 1 ペア

IM and Presence の 5k の VM 設定ペアは 5,000 人のユーザをサポートし、Unified CM の 10k の VM 設定のペアは 10,000 個のデバイスをサポートします。

Cisco WebEx Connect

エンド ユーザが Cisco WebEx Messenger サービスにログインして、プレゼンス、インスタント メッセージング、および Voice over IP（VoIP）コーリングなどの基本機能を利用するために必要なものは、56 kbps ダイヤルアップ インターネット接続だけです。ただし、小規模のオフィスやブランチ オフィスでファイル転送やスクリーン キャプチャなどの高度な機能を利用するには、512 kbps 以上のブロードバンド接続が必要です。

ネットワークとデスクトップの要件の詳細については、次の場所にある『*Cisco WebEx Messenger Administration Guide*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/webex-messenger/products-installation-guides-list.html

Cisco Unified Communications 統合は、クリックコール アプリケーションおよび Cisco Unified Client Services Framework でのデスクフォン制御モードに Unified CM CTI Manager を使用します。したがって、アプリケーションと CTI（25-24 ページ）の項に明記された CTI の制限を遵守してください。Cisco UC Integration™ for Connect がソフトフォン（コンピュータ上の音声）モードで動作している場合、Cisco Jabber Desktop Client は Cisco Unified CM に SIP 登録されたエンドポイントです。Cisco Unified Communications を含むソリューションのサイジングを行う際には、Unified CM クラスタ上のリソースを使用する CTI デバイスと SIP エンドポイント デバイスを含める必要があります。

Cisco UC Integration™ for Microsoft Lync

Cisco UC Integration™ for Microsoft Lync は、クリックツーダイヤル アプリケーションとデスクフォン制御モードに Unified CM CTI Manager を使用します。したがって、呼処理（9-1 ページ）の章に明記された CTI の制限を遵守してください。Cisco UC Integration™ for Microsoft Lync がソフトフォン（コンピュータ上の音声）モードで動作している場合、クライアントは Cisco Unified CM に SIP 登録されたエンドポイントです。Cisco Unified Communications を含むソリューションのサイジングを行う際には、Unified CM クラスタ上のリソースを使用する CTI デバイスと SIP エンドポイント デバイスを含める必要があります。

サードパーティ製 XMPP クライアントとアプリケーション

サードパーティ製の Extensible Messaging and Presence Protocol（XMPP）クライアントは、WebEx Messenger サービスのプラットフォームと Cisco IM and Presence サービスの両方で使用される場合があります。これらのクライアントでは、音声、ビデオ、およびその他のコラボレーション機能は（インスタント メッセージングおよびチャットを除く）これらのクライアントでは、通常サポートされません。機能によっては、これらのクライアントが前述のサーバ上でサポートされるデバイス容量にカウントされる場合があります。

Mobile Unified Communications

ユニファイド コミュニケーションのモビリティは多面的です。モバイル通信のさまざまな側面がそれぞれ Unified CM リソースを消費し、個別的にもシステム全体の一部としても考慮する必要があります。次のサイジングの考慮事項は、モビリティに適用されますが、Unified CM に影響を与えないモビリティの側面はここでは説明していないことに注意してください。

Cisco Unified Mobility

シングル ナンバー リーチ（以前の Mobile Connect）とエンタープライズの 2 ステージ ダイヤリング機能（Mobile Voice Access および Enterprise Feature Access）をサポートするための Unified CM のキャパシティにとって重要な、2 種類のパラメータがあります。これらの機能が適切に動作するには、モビリティを有効にし、シェアド ラインを使用したリモート接続先がユーザ用に定義されている必要があります。表 25-5 に、各クラスの Unified CM のMV 設定で構成されるクラスタ内のユーザ、リモート接続先、モビリティ ID の各制限を示します。

表 25-5　クラスタごとのモビリティ ユーザ、リモート接続先、モビリティ ID の最大数

クラスタ ノード	クラスタごとのモビリティ対応ユーザの最大数	クラスタごとのリモート接続先とモビリティ ID の最大数
10,000 人のユーザの VM 設定	40,000	40,000（またはノードあたり 10,000）
7,500 人のユーザの VM 設定	30,000	30,000（またはノードあたり 7,500）
2,500 人のユーザの VM 設定	10,000	10,000（またはノードあたり 2,500）
1,000 人のユーザの VM 設定	4,000	4,000（またはノードあたり 1,000）

(注)　モビリティ対応ユーザは、リモート接続先プロファイルを持ち、1 つ以上のリモート接続先またはデュアルモード デバイスおよびモビリティ ID が設定されているユーザとして定義されます。

システムに定義されているそれぞれのリモート接続先およびモビリティ ID は、いくつかの方法で Unified CM に影響します。

- リモート接続先またはモビリティ ID はデータベースのスタティック メモリおよび設定領域を占有します。
- 各オカレンスでは、ユーザのプライマリ デバイスとのシェアド ラインを使用し、そのためその回線へのコールはより多くの CPU リソースを使用します。
- リモート接続先またはモビリティ ID が外線番号（ユーザの携帯電話またはホームなど）の場合、コールを拡張するために、ゲートウェイのリソースが使用されます。

コール トラフィック

コール トラフィックの量と質は、Unified CM のサイジングにおいて非常に重要な要素です。

ハーフコール モデルでは、コールの発信と終端は異なるイベントと見なされるため、コールの種類を区別することが重要です。同じサブスクライバ ノードに登録されているエンドポイントの場合、これらのエンドポイント間のコールについてはその両半分をそのサブスクライバが処理します。同じクラスタ内の 2 つのサブスクライバ ノード間で発信されたコールについては、参加している各サブスクライバは、コールの発信または終端のいずれかを処理します。異なるクラスタに登録されているエンドポイント間で発信されたコールについては、各クラスタは各コールの片半分のみを処理します。クラスタに登録されているエンドポイントと PSTN 間で発信されたコールについては、PSTN ゲートウェイはコールの片半分を処理し、これらのコール タイプに基づいてゲートウェイをサイジングします。

コール トラフィックの正確なサイジングについては、次の要素を考慮する必要があります。

- ユーザあたりの総最繁時呼数（BHCA）
- コールあたりの平均コール保留時間（ACHT）
- MGCP、H.323、および SIP プロトコルを使用した PSTN との間の BHCA
- H.323 クラスタ間トランクまたは SIP プロトコルを使用した他のクラスタとの間の BHCA
- クラスタ内の BHCA

コールのタイプごとに、呼設定にかかる CPU リソースの量は異なります。最繁時呼数により、CPU 使用率が決まります。CPU 要件は、コール発信レートによって直接影響を受けます。ACHT によって、コールを持続時間中保持するためのダイナミック メモリ要件が決まります。ACHT が長くなるほど、割り当てたままにする必要があるダイナミック メモリが多くなるため、メモリ要件が大きくなります。

コール トラフィックは、他のソースで発生する可能性もあります。コールが転送でリダイレクトされるか、ボイスメールにリダイレクトされるたびに、CPU による処理が必要になります。1 つの電話番号が複数の電話機に設定されている場合は、その番号への着信コールをそれらすべての電話機に表示する必要があるため、コール セットアップ時に CPU 使用率が高くなります。高度な機能を使用する場合は、このテクノロジーを使用して発信されたコール数と、これらのコールのうちでコール品質のために PSTN にリダイレクトする必要があるコールの割合も考慮する必要があります。

ダイヤル プラン

Unified CM のダイヤル プランは、コール ルーティングおよび関連付けられるポリシーを決定する設定要素で構成されます。一般に、ダイヤル プラン要素は、Unified CM のスタティック メモリ領域を占有します。次のダイヤル プラン要素が、必要なメモリ量に影響を与えます。

- 電話番号
- 共有電話番号、および同じ DN を共有するエンドポイントの平均数
- パーティション、コーリング サーチ スペース、トランスレーション、およびトランスフォーメーション パターン
- ルート パターン、ルート リスト、およびルート グループ
- アドバタイズされ、学習された DN パターン
- ハント パイロットおよびハント リスト
- 循環、シーケンシャル、およびブロードキャスト回線グループとそのメンバーシップ

Unified CM によってダイヤル プラン要素に適用される絶対的な制限はありませんが、使用可能な共有システム メモリの量が固定されています。

ほとんどのダイヤル プラン要素は、CPU 使用率に直接影響を与えません。ハント リストや回線グループなどのシェアド ラインは例外です。特定の電話番号を共有するすべてのエンドポイントにコールを表示する必要があるため、シェアド ラインごとにコール セットアップの CPU コストが増えます。

アプリケーションと CTI

Unified CM のコンテキストでは、アプリケーションは、Unified CM によって提供される単純な呼処理を超える「追加」機能です。一般に、これらのアプリケーションでは、Computer Telephone Integration（CTI）が利用され、ユーザはコールの発信、終端、再ルーティング、モニタ、および処理を行うことができます。Cisco Unified CM Assistant、アテンダント コンソール、コンタクト センターなどの機能は、CTI を利用して動作します。

大規模な Unified CM の VM 設定は登録されているすべてのデバイスに対する CTI をサポートできますが、より小規模な VM 設定ではそこまで大きく拡張しません。表 25-6 に、各 Unified CM の VM 設定でサポートされる CTI リソースの最大数を示します。これらの最大値は、次のタイプの CTI リソースに適用されます。

- CTI で制御またはモニタされ、Unified CM サブスクライバ ノードに登録できるエンドポイントの最大数。
- CTI Manager サービスを実行している Unified CM サブスクライバ ノードでモニタまたは制御できるエンドポイントの最大数。
- CTI Manager サービスを実行している Unified CM サブスクライバ ノードに接続できる TAPI/JTAPI アプリケーション インスタンスの最大数。CTI Manager サービスを実行している Unified CM サブスクライバ ノードに接続できる TAPI/JTAPI アプリケーション インスタンスは、CTI 接続と呼ばれることもあります。

VM 設定用の CTI リソースの最大数がその VM 設定のエンドポイント キャパシティに対応することに注意してください。

Unified CM によって提供されるネイティブ アプリケーション以外に、Unified CM CTI リソースを使用するサード パーティ製アプリケーションも導入できます。CTI ポートとルート ポイントを数える場合は、サードパーティ アプリケーションも考慮してください。

表 25-6　Unified CM における CTI リソースの制限

VM 設定	仮想マシンあたりの最大 CTI リソース
1,000 人のユーザ	1,000
2,500 人のユーザ	2,500
7,500 人のユーザ	5,000 または 7,500[1]
10,000 人のユーザ	10,000

1. Unified CM 10.5 以降のリリースでサポートされる CTI リソースは 7,500 個で、リリース 10.5 より前の Unified CM でサポートされる CTI リソースは 5,000 個です。

接続とデバイスの最大数以外に、CTI 制限は次の影響も受けます。

- 各制御対象デバイスの回線数（制御対象デバイスあたり最大 5 回線）
- CTI によって制御される回線の共有接続数（回線あたり最大 5）
- アクティブな CTI アプリケーションの数（デバイスあたり最大 5）
- 制御対象デバイスあたり最大 6 BHCA

Unified CM で利用できる CTI リソースは、これらのいずれかの値を超えた場合に減少します。

Unified CM クラスタに必要な CTI リソースの決定

次の手順に従って、Unified CM クラスタに必要な CTI リソースの数を決定します。

手順 1　総 CTI デバイス数を調べます。

クラスタ上で使用される予定の CTI デバイスの数を数えます。

手順 2　CTI 回線係数を調べます。

表 25-7 に従って、クラスタ内のすべてのデバイスの CTI 回線係数を決定してください。

表 25-7　CTI 回線係数

CTI デバイスごとの回線数	CTI 回線係数
1 ～ 5 回線	1.0
6 回線	1.2
7 回線	1.4
8 回線	1.6
9 回線	1.8
10 回線	2.0

(注)　クラスタ内のデバイスの回線係数がばらついている場合は、システム内のすべての CTI デバイスでの平均回線係数を求めます。

手順 3　アプリケーション係数を調べます。

表 25-8 に従って、クラスタ内のすべてのデバイスのアプリケーション係数を決定してください。

表 25-8　CTI アプリケーション係数

CTI デバイスごとのアプリケーション数	CTI アプリケーション係数
1 ～ 5 個のアプリケーション	1.0
6 個のアプリケーション	1.2
7 個のアプリケーション	1.4
8 個のアプリケーション	1.6
9 個のアプリケーション	1.8
10 個のアプリケーション	2.0

手順 4　次の公式に従って、CTI リソースの必要な数を計算します。

CTI リソースの必要な数 =（CTI デバイスの合計数）*（CTI 回線係数または CTI アプリケーション係数の大きい方）

次の例は、このプロセスを示しています。

例 1: デバイスごとの平均回線数が 9、平均アプリケーション数が 4 で、500 台の CTI デバイスが配置されています。表 25-7 と表 25-8 にリストされている係数に従うと、デバイスごとの回線数が 9 の場合の回線係数は 1.8、デバイスごとのアプリケーション数が 4 の場合のアプリケーション係数は 1.0 になります。これらの値を手順 4 の式に代入すると、次の値が得られます。

（500 CTI デバイス）*（{回線係数 1.8 またはアプリケーション係数 1.0} の大きい方）

（500 CTI デバイス）*（回線係数 1.8）= 900 の総 CTI リソースが必要

例 2: デバイスごとの平均回線数が 5、平均アプリケーション数が 9 で、2,000 台の CTI デバイスが配置されています。表 25-7 と表 25-8 にリストされている係数に従うと、デバイスごとの回線数が 5 の場合の回線係数は 1.0、デバイスごとのアプリケーション数が 9 の場合のアプリケーション係数は 1.8 になります。これらの値を手順 4 の式に代入すると、次の値が得られます。

(2000 CTI デバイス)*({回線係数 1.0 またはアプリケーション係数 1.8} の大きい方)

(2000 CTI デバイス)*(アプリケーション係数 1.8)= 3,600 の総 CTI リソースが必要

例 3: デバイスごとの平均回線数が 2、平均アプリケーション数が 3 で、5,000 台の CTI デバイスが配置されています。表 25-7 と表 25-8 にリストされている係数に従うと、デバイスごとの回線数が 2 の場合の回線係数は 1、デバイスごとのアプリケーション数が 3 の場合のアプリケーション係数は 1 になります。これらの値を手順 4 の式に代入すると、次の値が得られます。

(5,000 CTI デバイス)*({回線係数 1 またはアプリケーション係数 1} の大きい方)

(5,000 CTI デバイス)*(回線係数またはアプリケーション係数 1)= 5,000 の総 CTI リソースが必要

IP Phone サービス

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

Cisco Unified IP Phone サービスの大部分は、HTTP クライアントとして機能します。ほとんどの場合、加入サービスのロケーションへの転送サーバとしてだけ Unified CM が使用されます。Unified CM はリダイレクト サーバとしてのみ機能するため、多数の要求(1 分あたり数百以上の要求)がない限り、Unified CM へ与えるパフォーマンスの影響は通常最小限になります。

統合された Extension Mobility と Unified CM Assistant アプリケーションの IP Phone サービスを除き、IP Phone サービスは独立した Web サーバに存在する必要があります。Unified CM ノードで、Extension Mobility および Unified CM Assistant 以外の電話サービスを実行することはサポートされていません。

Cisco Extension Mobility および Extension Mobility Cross Cluster

Extension Mobility(EM)は、次のようにシステム パフォーマンスに影響します。

- EM プロファイルを作成するには、ディスク データベース領域とスタティック メモリの両方が必要になります。
- ユーザが EM アカウントにログインする頻度は、CPU 使用率とメモリ使用率の両方に影響します。Unified CM ノードがサポートできる 1 分あたりの最大ログイン数には制限があります。
- Extension Mobility Cross Cluster(EMCC)の方がリソースに大きな影響を及ぼします。Unified CM ノードがサポートできる EMCC ユーザの数には制限があります。サポートされる最大 EMCC ログイン レートは、EM に対してサポートされるレートよりも低くなります。さらに、EM と EMCC のログイン レートにトレードオフがあります。両方が同時に発生した場合、それぞれの最大キャパシティが減ります。
- クラスタあたりの EM と EMCC のログイン レートは、共有データベース内のプロファイルにアクセスする必要があるため、各ノードのログイン レートとクラスタ内のノード数を単純に掛け合わせたものではありません。複数の呼処理サブスクライバで構成されるクラスタ内の最大ログイン レートは、単一サーバ ノードの 1.5 倍に制限する必要があります。

表 25-9 に、VM 設定のタイプごとの 1 分あたりの EM と EMCC の最大ログイン数を示します。

表 25-9　VM 設定ごとの EM と EMCC のレート

VM 設定	最大 EM ログイン レート（ノードあたり）	最大 EM ログイン レート（デュアル ノード）	最大 EMCC ログイン レート（ノードあたり）	最大 EMCC ログイン レート（デュアル ノード）	最大同時 EMCC デバイス
1,000 人のユーザ	200	300	60	70	333
2,500 人のユーザ	235	352	71	80	833
7,500 人または 10,000 人のユーザ	250	375	75	90	2,500

Cisco エクステンション モビリティ ログインおよびログアウト機能は、ログイン/ログアウトのクラスタ キャパシティを増加するためにサブスクライバ ノードのペアに分散できます。たとえば、EM 負荷が 7,500 人のユーザの VM 設定を持つ 2 つの仮想マシンの間で均等に分散される場合、1 分あたりのクラスタ全体のキャパシティは最大で 375 回の順次ログインまたはログアウト（あるいはその両方）になります。

（注）　Cisco Extension Mobility サービスは、冗長性を目的として 3 つ以上のノードでアクティブにできますが、最大 2 つのサブスクライバー ノードまでが同時にアクティブにログイン/ログアウト処理することをサポートしています。

（注）　EM セキュリティの有効化はパフォーマンスを低下しません。

EMCC ログイン/ログアウト処理は、クラスタ内 EM ログイン/ログアウトよりも多くの処理リソースを必要とします。したがって、サポートされるログイン/ログアウトの最大レートは EMCC では低くなります。クラスタ内 EM ログイン/ログアウトがない場合、Unified CM は 7,500 人のユーザまたは 10,000 人のユーザ用の VM 設定を使用して、仮想マシンごとに 1 分あたり 75 回の EMCC ログイン/ログアウトの最大レートをサポートします。ほとんどの導入では、クラスタ内ログイン/ログアウトとクラスタ間ログイン/ログアウトの組み合わせが発生します。より一般的なこのシナリオでは、EMCC ログイン/ログアウトの混合（ホーム クラスタまたは Visiting クラスタのどちらとして機能する場合でも）は、1 分あたり 40 回のモデルにする必要があります。同時にクラスタ内 EM ログインは、シングル EM サーバ ノードを使用する場合、185 回のログイン/ログアウトのモデルにする必要があります。クラスタ内 EM ログイン レートは、デュアル EM ノード構成で 7,500 人のユーザまたは 10,000 人のユーザ用のVM 設定を使用する場合、1 分あたり 280 回のログイン/ログアウトに増やすことができます。（表 25-9 を参照）。

EMCC ログイン デバイス（Visiting 電話機）は、クラスタ内の他のエンドポイントの 2 倍のリソースを消費します。EMCC ログイン デバイスの最大サポート数はクラスタあたり 2,500 台ですが、これによっても、クラスタあたりの他のデバイスの理論的な最大数は 30,000 から 25,000 に減少します。クラスタ内の他の登録デバイス数を削減しても、EMCC ログイン デバイスの最大サポート数は 2,500 台のままです。

Cisco Unified CM Assistant

Cisco Unified CM Assistant アプリケーションは、回線モニタリングおよび電話制御のために Unified CM で CTI リソースを使用します。Unified CM Assistant 用のまたはマネージャ電話機用の各回線（インターコム回線を含む）が CTIManager 経由で CTI 制御されている必要があります。加えて、CTIManager 経由で CTI 制御された Unified CM Assistant ルート ポイントも必要になります。Unified CM Assistant を設定する場合、必要な CTI 回線または CTI 接続の数について、クラスタ全体での CTI 回線または CTI 接続に対する制限も合わせて考慮する必要があります。

Unified CM Assistant には、次の制限が適用されます。

- マネージャあたり最大 10 人のアシスタントを設定できる。
- 1 人のアシスタントに対して最大 33 人のマネージャを設定できる（マネージャ毎に 1 つの Unified CM Assistant 制御回線がある場合）。
- クラスタあたり最大 3500 人のアシスタントと 3500 人のマネージャを、7,500 人のユーザまたは 10,000 人のユーザ用の仮想マシンを使用して設定できる（合計 7000 人）。
- プライマリおよびバックアップ Unified CM Assistant ノードのペアをクラスタあたり最大 3 組導入できる。ただし、[複数のアクティブモードを有効化（Enable Multiple Active Mode）] の拡張サービスパラメータが [はい（True）] に設定され、Unified CM Assistant サーバの 2 番めおよび 3 番めのプールが設定されている場合。

Unified CM Assistant 最大でアシスタント 3,500 人とマネージャ 3,500 人（合計 7,000 人）のキャパシティを実現するには、複数の Unified CM Assistant サーバ プールを定義する必要があります（詳細については、Unified CM Assistant（18-23 ページ）を参照してください）。

Cisco WebDialer

Cisco WebDialer を使用すると、ユーザは簡単にコールを開始できます。追加リソースが必要になるのはコールの開始時のみで、コール中は不要であるため、Unified CM に対する Cisco WebDialer の影響はかなり限定されます。コールが確立されると、Unified CM に対する影響は他のコールと同様になります。

WebDialer および Redirector サービスは Unified CM クラスタ内で複数のサブスクライバ ノードを実行でき、次のキャパシティがサポートされています。

- 各 WebDialer サービスは、ノードごとに 1 秒あたり最大 4 コール要求まで処理できます。
- 各 Redirector サービスは、1 秒あたり最大 8 コール要求まで処理できます。

次の一般式が WebDialer の 1 秒あたりのコール数の決定に使用できます。

（WebDialer のユーザ数）*（（平均 BHCA）/（3600 秒/時間））

この計算を行う場合、特に WebDialer サービスを使用した発信の、ユーザあたりの BHCA を適切に推定することが重要です。以下の例で、サンプルの組織に対して WebDialer デザイン計算式をどのように使用するかを示します。

例：1 秒あたりの WebDialer コール数の計算

会社 XYZ は、WebDialer サービスを使用してクリックコール アプリケーションを稼働させることを考えています。その事前のトラフィック分析結果は次の資料の通りです。

- 10,000 人をクリックコール機能で有効にする。
- 各ユーザの平均 6 BHCA
- すべてのコールの 50 % が発信で、50 % が着信
- 計画では、すべての発信のうち、WebDialer サーバを使用して開始する発信を 30 % と見積もる。

（注）　これらの値は、WebDialer 配置のサイジングの演習を示すために使用した例です。ユーザのダイヤル特性は、組織によって大きく異なります。

10,000 ユーザで各 6 BHCA ならば、合計 60,000 BHCA です。ただし、WebDialer 配置のサイジングの計算は、発信コールのみ考慮します。このサイジングの例で最初の情報では、合計 BHCA の 50 % が発信です。これは、WebDialer を用いたクリックツーコールが利用可能なすべてのユーザで、合計 30,000 発信 BHCA という結果になります。

この発信数のうち、WebDialer サービスを使用して発信される割合は、組織によって変化します。この例の組織では、ユーザはいくつかのクリックコール アプリケーションを利用可能で、発信の 30 % が WebDialer を使用すると見積もられています。

(30,000 発信 BHCA)* 0.30 = 9,000 発信 BHCA が WebDialer を使用

9,000 BHCA の負荷をサポートするのに必要な WebDialer サーバ ノードの数を判別するには、この値を最繁時に維持する必要のある 1 秒あたりの Busy Hour Call Attempt（BHCA）に変換します。

（9,000 call attempts / 時間）*（時間/3,600 秒）= 2.5 cps

各 WebDialer サービスは最大で 4 cps をサポートできます。したがって、この例では、WebDialer サービスを実行するため 1 つのノードを設定できます。これは、将来の WebDialer 拡張使用に利用できます。サーバ ノードの障害発生時に WebDialer キャパシティを維持するには、冗長性を提供する追加のバックアップ WebDialer サーバ ノードを配置する必要があります。

Attendant Console

Attendant Console を使用した Cisco Unified CM の統合は CTI リソースを利用します。サーバベースのアテンダント コンソールはアテンダントがコールを送信した最後の 2,000 人のユーザをモニタするため、CTI リソースの使用率が増加します。さらに、各コールでは、グリーティングやキューイングなどに多数の CTI ルート ポイントとポートが使用されます。

メディア リソース

Unified CM は、Cisco IP Voice Media Streaming Application（IPVMS）を提供します。これは、ソフトウェアだけで実行可能で、ハードウェア リソースを必要としない特定のメディア機能を提供します。Unified CM は、メディア ターミネーション ポイント（MTP）、会議ブリッジ、アナンシエータ（アナウンスの再生用）、または保留音ストリームのソースとして動作できます。Unified CM の機能は、Cisco Integrated Service Router（ISR）によって提供される同様の機能と比べて限定されますが、一般的には保留音ストリーム（ユニキャストとマルチキャストの両方）の主要なソースです。

Cisco IP Voice Media Streaming Application は、次の 2 つの方法のいずれかで導入できます。

- 共存配置

  共存導入では、Streaming Application は Unified CM ソフトウェアも実行している、クラスタ内の任意のサーバ ノード（パブリッシャまたはサブスクライバ）で実行されます。

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

- スタンドアロン配置

  スタンドアロン導入では、Streaming Application は Unified CM クラスタ内の専用サーバ ノードで実行されます。Cisco IP Voice Media Streaming Application サービスは、サーバ ノードで使用できる唯一のサービスであり、サーバ ノードには、ネットワーク内のデバイスにメディア リソースを提供する機能だけがあります。

Cisco IP Voice Media Streaming Application は MTP、アナンシエータ、および会議機能を提供しますが、これらの機能を Cisco Integrated Service Router（ISR）に配置した方が拡張性が向上します。ただし、このアプリケーションの保留音機能は、簡単には外部ソースに配置できません。表 25-10 に、これらの各サービスに設定できる最大値を示します。

表 25-10　Cisco IP Voice Media Streaming Application のキャパシティ制限

メディア デバイス タイプ	デフォルトの数量	ストリームまたはデバイスの最大数	サポートされるコーデック
アナンシエータ	48	750	G.711、G.729、L16WB
ソフトウェア会議ブリッジ	48	256	G.711、L16WB
保留音	250	1,000	G.711、G.729、L16WB
ソフトウェアのメディア ターミネーション ポイント（MTP）	48	512	G.711、L16WB、パススルー

ここでは、表 25-10 について説明します。

- すべての値は、メディア デバイスごとにサポートされる発信者の数を表します。たとえば、48 のソフトウェア会議ブリッジは 16 の三者会議をサポートできます。
- これらのデバイスは、デフォルト設定またはデフォルトに近い設定を使用すると呼処理ノードと共存できます。
- キャパシティを最大値まで引き上げる場合は、メディア デバイスを（呼処理と一緒ではなく）スタンドアロン ノードに導入することを推奨します。
- MoH オーディオ ソースを最初の（グリーティング）アナウンスに使用する場合は、その最初のアナウンスを 15 秒未満に保持することを推奨します。そうしないと、MoH サーバ ノードあたりの MoH ストリームの最大値を余分なファイル I/Oのために 500 ～ 700 の間に引き下げる必要がある場合があります。
- 各メディア デバイスは、IPVMS サービス パラメータで無効または有効にすることができます（MoH は [MoH デバイス設定（MoH device configuration）] ページにあります）。MoH 専用の Unified CM ノードなどを設定することができます。

（注）　個別の ISR でサポートされている DSP の各メディア機能のキャパシティを計算するには、Cisco ISR の製品データ シートまたはメディア リソース（7-1 ページ）の章を参照してください。

保留音

表 25-11 11 に、VM 設定と、各ノードがサポートできる同時保留音（MoH）ストリームの最大数を示します。実際の使用率がこれらの制限値を超えないようにしてください。MoH の最大ストリーム キャパシティに到達してさらに負荷が増えると、MoH の品質低下、MoH 動作の不安定化、または MoH 機能の損失を引き起こす可能性があります。さらに MoH ノード（共存および専用）が増えると、Unified CM のクラスタ MoH ストリームのキャパシティが増大します。

表 25-11　保留音のノード当たりの最大ストリーム キャパシティ

Unified CM OVA テンプレート	Unified CM 10.5(2) 以降		Unified CM 10.5(1) 以前	
	共存 MoH ストリーム（非 sRTP）[1]	スタンドアロン MoH ストリーム	共存 MoH ストリーム	スタンドアロン MoH ストリーム
1,000 人のユーザ	500	750	500	500
2,500 人のユーザ			1,000	1,000
7,500 人のユーザ	750	1,000	1,000	1,000
10,000 人のユーザ				

1. 非 sRTP ストリームに基づくすべてのキャパシティ。

表 25-12 に示すように、Unified CM 10.5(2) 以降、Unified CM クラスタでの保留音の最大 500 個の一意のオーディオ ソースを定義できるようになりました。表 25-12 に示す最大オーディオ ソース キャパシティは、クラスタ内で使用される VM 設定のサイズと MoH サーバ タイプに基づいたクラスタ単位のものです。Unified CM クラスタに MoH ノードを追加すると、MoH ストリームのキャパシティのみが増加し、オーディオ ソースのキャパシティは増加しません。オーディオ ソースのキャパシティは、共存 MoH ノードからスタンドアロンの MoH ノードに移動することによってのみ増加させることができ、クラスタ全体のノード VM 設定サイズを大きくしたり、追加 Unified CM クラスタを増やしたりできます。

表 25-12　保留音のクラスタあたりの最大オーディオ ソース キャパシティ

Unified CM OVA テンプレート	Unified CM 10.5(2) 以降		Unified CM 10.5(1) 以前	
	共存 MoH ソース	スタンドアロン MoH ソース	共存 MoH ソース	スタンドアロン MoH ソース
1,000 人のユーザ 2,500 人のユーザ	100	250	50	
7,500 人のユーザ 10,000 人のユーザ	250	500		

表 25-11 および表 25-12 に示したキャパシティの制限は、ユニキャスト、マルチキャスト、またはユニキャストとマルチキャストの同時ストリームに適用されます。

パフォーマンスに関する考慮事項

MoH オーディオ ソースとストリームの数を最大にするには、ソフトウェア MTP やソフトウェア会議ブリッジを無効にするなど、他の一部のメディア デバイスの数を減らす必要があります。Cisco IP Voice Media Streaming Application サービスは、すべてのメディア デバイスの最大設定を同時にサポートしません。システム リソース（CPU 使用率やディスク I/O など）をメディア デバイスでオーバーサブスクライブすると、システム全体のパフォーマンスに影響を及ぼします。IPVMS アラームは、メディア デバイスがプロビジョニングされたキャパシティを満たすことができない場合に発行されます。

ローエンド設定（1,000 ユーザまたは 2,500 ユーザの VM 設定）と中程度の呼処理と MoH の共存では、MoH は最大 500 のストリーム、100 の MoH オーディオ ソース、MTP での 48 ～ 64 のアナンシエータ ストリーム、デフォルト値に設定されるか無効になっている会議ブリッジに制限されます。

250 のオーディオ ソースの 750 MoH ストリームと 250 のアナンシエータ ストリームをサポートするには、1,000 人のユーザまたは 2,500 人のユーザ用の VM 設定の専用 MoH ノードが必要です。

最大 1,000 の MoH ストリーム、500 の MoH オーディオ ソース、および 750 のアナンシエータをサポートするには、最低でも 7,500 人のユーザ用の OVA 専用スタンドアロン MoH サーバが必要です。

MoH 用またはアナンシエータあるいはその両方の sRTP を使用すると、MoH 発信者の最大数が 25 % 減少します。この場合には、MoH およびアナンシエータ専用の IPVMS を推奨します。

Unified CM MoH サーバは 4 つのコーデック（G.711 ulaw、G.711 mulaw、G729a、および高帯域オーディオ）をサポートします。ユニキャスト MoH を使用すると、コール セットアップ時にコーデックがネゴシエートされるため、MoH ストリームの数は有効になっている MoH コーデックの数ではなく、ユニキャスト MoH で保留になっているエンドポイントの数によって異なります。マルチキャスト MoH の場合、各マルチキャスト対応オーディオ ソースが、有効になっている MoH コーデックごとに 1 つの MoH ストリームを生成します。たとえば、2 つのコーデックが有効になっていて、500 すべての MoH ソースがマルチキャスト対応である場合、エンドポイントが保留になっていなくても、1,000 のマルチキャスト MoH ストリームがアクティブになります。このシナリオでは、エンドポイントがユニキャスト MoH に配置されている場合は、MoH ストリームのキャパシティを増やす必要があります。

Unified CM に対する影響

共存モードまたはスタンドアロン モードのどちらで導入したかにかかわらず、Cisco IP Voice Media Streaming Application は CPU とメモリ リソースを消費します。Unified CM の全体のサイジングでは、この影響を考慮する必要があります。

一般に、メディア リソースの使用率は、Unified CM で処理する必要がある BHCA に加算されると見なされます。

コール キューイング（ハント パイロットのキューイング）

コール キューイングに送信できるメディア ストリームの最大数は、保留音ストリームと同じです。詳細については、保留音（25-31 ページ）を参照してください。

有効なコール キューイングのハント パイロットの最大数は、Unified CM サブスクライバ ノードごとに 100 です。各ハント パイロットのキューの同時発信者の最大数は 100 です。すべてのハント リストに含まれるメンバの最大数は、コール キューイングがイネーブルのときには変更されません。

LDAP ディレクトリ統合

Unified CM データベース同期機能には、LDAP ストアから Unified CM パブリッシャ データベースへユーザ設定データ（属性）のサブセットをインポートするメカニズムがあります。ユーザ アカウントの同期が発生すると、各ユーザの LDAP アカウント情報が、そのユーザの特定の Unified Communications 機能を有効にするために必要な追加データと関連付けられることがあります。認証も有効な場合、パスワード確認のための LDAP ストアへのバインドに、ユーザのクレデンシャルを使用します。同期や認証が有効な場合に、エンド ユーザのパスワードは Unified CM データベースには格納されません。

ユーザ アカウント情報はクラスタ固有です。各 Unified CM パブリッシャ ノードは、このクラスタから Unified Communications サービスを受けているユーザの一意のリストを保持しています。同期アグリーメントはクラスタ固有で、各パブリッシャにはユーザ アカウント情報の独自コピーがあります。

Unified CM クラスタの最大ユーザ数は、クラスタのメンバー間で複製される内部コンフィギュレーション データベースの最大サイズによって制限されます。現在、設定または同期可能なユーザの最大数は 160,000 です。ディレクトリ同期のパフォーマンスを最適化するには、次の点を考慮してください。

- 電話機や Web ページからのディレクトリ ルックアップには、Unified CM データベースまたは IP Phone Service SDK を使用できる。ディレクトリ ルックアップ機能に Unified CM データベースを使用する場合、LDAP ストアから設定された、または同期されたユーザだけがディレクトリに表示されます。ユーザのサブセットを同期すると、ユーザのそのサブセットだけがディレクトリ ルックアップに表示されます。
- ディレクトリ ルックアップに IP Phone Services SDK を使用する場合に、LDAP に対する Unified CM ユーザの認証が不要であれば、Unified CM クラスタにログインするユーザのサブセットだけに同期を制限できます。
- クラスタが 1 つしか存在せず、LDAP ストア内のユーザ数が Unified CM クラスタでサポートされている最大ユーザ数よりも少なく、ディレクトリ ルックアップが Unified CM データベースに実装されている場合、LDAP ディレクトリ全体をインポートできます。
- 複数のクラスタが存在し、LDAP 内のユーザ数が Unified CM クラスタでサポートされている最大ユーザ数よりも少ない場合、すべてのユーザを各クラスタにインポートし、ディレクトリ ルックアップにすべてのエントリを確実に含めることができます。
- LDAP のユーザ アカウントの数が Unified CM クラスタでサポートされている最大ユーザ数を超え、ユーザ セット全体をすべてのユーザに表示する必要がある場合は、Unified IP Phone Services SDK を使用して Unified CM からディレクトリ ルックアップをオフロードする必要があります。
- 同期と認証の両方を有効にすると、Unified CM データベースに設定または同期されたユーザ アカウントはそのクラスタにログインできるようになる。同期するユーザの決定は、ディレクトリ ルックアップ サポートの決定に影響します。

(注)　シスコは、上記で説明している制限までユーザ アカウントの同期をサポートしていますが、この制限を強制しているわけではありません。多くのユーザ アカウントを同期化すると、ディスク容量のスターベーション、データベース パフォーマンスの低速化、およびアップグレードの長時間化を招くことがあります。

Cisco Unified CM メガクラスタの導入

呼処理サブスクライバの数が通常クラスタの最大値 4 ペアを超える場合、Unified CM クラスタはメガクラスタと見なされます。メガクラスタには、最大 8 ペアの呼処理サブスクライバと 1 つのメガクラスタに 21 未満のサーバ ノードを含めることができます。

たとえば、サーバの上限値の 21 を考慮して、パブリッシャ、TFTP、TFTP バックアップ、MoH、MoH バックアップ、8 個のプライマリ サーバおよび 8 個の バックアップサーバを含めることができます。

(注)　IM and Presence はメガクラスタの導入の場合、サーバ上限値の 21 を考慮しません。

Cisco IM and Presence では VM 設定テンプレートを導入し、25,000 ユーザの VM 設定を使用してメガクラスタの導入と一致するようにしています。

Unified Communications の導入は、Unified CM メガクラスタで簡素化できる場合があります。このような導入では、次の上限が拡大されます。

- サポートされるエンドポイントの最大数が通常のクラスタの数（8 ペアの呼処理サブスクライバ）の 2 倍になります。
- CTI デバイスと接続の最大数も 2 倍になります。

ただし、クラスタ全体の定数は増えません。これらの中で重要なものは次のとおりです。

- コンフィギュレーション データベースのサイズ
- ロケーションとリージョンの数
- 同期済みまたはプロビジョニング済みの LDAP エンド ユーザの最大数（1 クラスタあたり 160,000）

（注）　メガクラスタの導入に関しては複雑な考慮事項が多数あるので、このような導入の実現を望むお客様は、シスコのアカウント チーム、シスコ アドバンスド サービス、または認定された Cisco Unified Communications パートナーに関与してもらう必要があります。

Cisco IM and Presence

他のすべてのアプリケーションと同様、Cisco IM and Presence のサイジングは、次の方法で実行されます。

- システムを最も基本的なサービスに分解する。
- これらの各サービスのユニット コストを求める。
- 特定のシステム記述を識別されたサービスの集約として分析し、正味システム コストを求める。
- システム コストと導入オプションに基づいて必要なサーバの数を決定する。

IM and Presence については、分析対象システムの次のシステム変数が関連し、正確なサイジングのために考慮する必要があります。

- ユーザの数とタイプ
  - ユーザがプレゼンス サービスを取得するために使用するクライアント
  - ユーザの動作モード（インスタント メッセージ専用、または完全な Unified Communications ファシリティ）
- 標準ユーザが実行するプレゼンス関連のアクティビティ
  - 連絡先リストのサイズと構成（クラスタ内、クラスタ間、およびフェデレーション）。Cisco IM and Presence のシステム アーキテクチャは、フル装備のシステムでユーザ 1 人あたり 75 件という連絡先リストの平均サイズに基づいています。システム全体ではユーザごとの連絡先リストのサイズが異なりますが、システムのユーザの多くが 75 件の連絡先という平均リスト サイズを超える場合はシステム パフォーマンスに影響します。デフォルトでは、連絡先リストの最大サイズは 200 です。一部のユーザの連絡先が 200 件を超えている場合は、IM and Presence クラスタの [プレゼンスの設定（Presence Settings）] を修正することで、この最大連絡先リスト サイズを変更できます。
  - 最繁時におけるユーザごとのインスタント メッセージ（2 人のユーザ間で直接やり取り）の数
  - チャット ルームの数、各チャット ルームのユーザ数、および各チャット ルームのユーザあたりのインスタント メッセージ数によるチャット サポート
  - 各ユーザの状態変更（コール関連とユーザ開始の両方）

- 導入モデル
  - クラスタ間プレゼンスがサポートされるかどうか
  - フェデレーションがサポートされるかどうか
  - ハイ アベイラビリティが必要かどうか
- サーバ設定
  - 目的の VM 設定のサイズ
- システム オプション
  - コンプライアンス レコーディングが必要かどうか

システム要件を定量化したら、表 25-13 のデータから必要な仮想マシンの数を特定できます。

表 25-13　IM and Presence クラスタごとにサポートされる最大ユーザ数[1]

VM 設定	完全な Unified Communications モードでサポートされる最大ユーザ数
500 人のユーザ	1,500
1,000 人のユーザ	1,000
2,000 人のユーザ	6,000
5,000 人のユーザ	15,000
15,000 人のユーザ	45,000
25,000 人のユーザ	75,000

1. サポートされる最大サブクラスタ数は 3 です。

名簿管理

ユーザの連絡先とウォッチャの数はシステム パフォーマンスに影響します。重大な影響の可能性があるため、システム管理者は使用率を監視して、ユーザごとのクラスタ平均が 75 件の連絡先またはウォッチャ、あるいはその両方を超えないように確認する必要があります。

デフォルトでは、サービス パラメータは、ユーザごとに最大連絡先数は 200、ウォッチャ数は 200 に設定されます。このデフォルトのパラメータ設定は、多数の連絡先を必要とするユーザにオプションを提供するためのものです。IM and Presence ノードの 15,000 プレゼンスのユーザ全員が 200 件の連絡先とウォッチャをそれぞれに設定できるという意味ではありません。

IM and Presence のすべての導入で、ユーザごとの連絡先かウォッチャまたはその両方のサービス パラメータを 200 に設定している場合でも、そのクラスタ平均 75 を超えないようにすることを推奨します。

たとえば、15,000 のユーザ VM 設定テンプレートが 3 つのサブクラスタと 45,000 人のプレゼンス対応ユーザが含まれているフル装備のクラスタ内にあるとします。クラスタのすべてのユーザの連絡先の平均を 75 件に維持したい場合は、クラスタ全体で許容する連絡先の最大数は次のようになります。

(45,000 人のユーザ)*(ユーザごとに 75 件の連絡先) = 3,375,000 件の連絡先が IM and Presence で許可

クラスタ内のすべてのユーザの連絡先の総数が 3,375,000 を超えない範囲で、クラスタ内の一部のユーザは最大 200 件の連絡先を設定すると同時に他のユーザの連絡先の件数は少なくなります。

また、5,000 人の IM and Presence ユーザを含む導入で、これらのユーザのうちの 50 人それぞれが 1,000 件の連絡先を必要としているものとします。この導入で許可された連絡先の最大数は次のようになります。

（5,000 人のユーザ）*（ユーザごとに 75 件の連絡先）= 375,000 件の連絡先が導入全体で許可

50 人のヘビー ユーザには、（50 人のユーザ）*（ユーザごとに 1,000 件の連絡先）= 50,000 件の連絡先。この場合は、（375,000 - 50,000）= 325,000 件の連絡先が残りの 4,950 人のユーザに使用できます。つまり、

325,000/4,950 = 残りの 4,950 人の各ユーザが使用できるのは平均で約 65 件の連絡先

Cisco IM and Presence の追加情報については、次の場所にある『*Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-device-support-tables-list.html

Cisco IM and Presence 用に正式に定義された VM 設定は、次の Web サイトから入手できます。

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html

Unified CM に対する影響

Cisco IM and Presence サービスは、Unified CM のパフォーマンスに次のように影響します。

- AXL/SOAP インターフェイスを介したユーザ同期
- SIP トランクを介したプレゼンス情報
- 電話制御を有効にする CTI トラフィック

一般に、ユーザ同期（ワンタイム ヒットを除く）の影響および SIP トランクを介したプレゼンス情報の影響はごくわずかです。ただし、電話機の CTI 制御の影響は、CTI の制限で考慮する必要があります。

IM and Presence の VM 設定は、Unified CM の VM 設定とは異なります。IM and Presence のテンプレートはユーザ ベースですが、Unified CM のテンプレートはデバイス ベースです。たとえば、Unified CM の 10k ユーザの VM 設定で使用する 5k ユーザの IM and Presence の VM 設定では、5,000 人のユーザとそれぞれ 2 台のデバイスをサポートします。同じクラスタ内の IM and Presence ノードは、同じタイプの VM 設定を使用する必要があります。

（注）　IM and Presence リリース 11.5 より前は、同時ユーザ ログイン数が最大で IM and Presence VM テンプレート容量の 80 % に制限されていました。IM and Presence 11.5 以降のリリースでは、プレゼンス ユーザの 100 % が同時に Jabber を介してログインできます。たとえば、45,000 人のプレゼンス対応ユーザの導入では、IM and Presence 11.5 より前のリリースが 36,000（45,000 の 80 %）件の同時ログインしかサポートしないのに対して、IM and Presence 11.5 以降のリリースは 45,000 人すべてのユーザの同時ログインをサポートします（ユーザ ログインあたり 1 つの Jabber クライアントのみとする）。また、この拡張機能は、許容される同時 Jabber ユーザ数を 20 % 増加させます。

集中型 IM and Presence

Cisco IM and Presence は、集中型導入オプションをサポートしています。集中型 IM and Presence クラスタは、複数のリモート Unified CM クラスタ上でユーザにプレゼンス サービスを提供できます。ただし、すべてのリモート Unified CM クラスタ全体のユーザの総数が 75,000 人を超えないようにする必要があります（各ユーザが 1 つずつのクライアントを使用するものとする）。1 人のユーザが複数のクライアントを使用する場合は、この制限が下がります。

（注）　集中型 IM and Presence クラスタには、クラスタ内の全部で 7 つのサーバ（3 つの IM and Presence サブクラスタ ペア（6 サーバ）+ Unified CM パブリッシャ ノード）用の Unified CM パブリッシャー ノードが必要です。

集中型 IM and Presence クラスタの展開では、クラスタ内のすべての IM and Presence ノードに対して 25k ユーザ IM and Presence VM テンプレートを使用し、その集中型クラスタの Unified CM パブリッシャ ノードに対して 10k ユーザ Unified CM VM テンプレートを使用することをお勧めします。

集中型 IM and Presence の導入は WAN 経由でクラスタ化できますが、次のような制限があります。

- すべてのリモート Unified CM クラスタが、集中型 IM and Presence クラスタの 80 ms のラウンドトリップ時間（RTT）内に収まる必要があります。
- 集中型 IM and Presence クラスタは、最大遅延が 300 ms RTT のクラスタ間トランクを介して別の集中型 IM and Presence クラスタに接続することができます。

緊急サービス

Cisco Emergency Responder は、電話機のロケーションと電話機の接続先のアクセス スイッチ ポートを追跡します。電話機は、自動的に検出するか、手動で Emergency Responder に入力できます。表 25-14 に、Emergency Responder をサポートする VM 設定とその最大キャパシティを示します。

（注）　これらの制限は、スタンドアロンの Emergency Responder の導入に適用され、また、ネイティブ緊急サービスが使用されていないものと想定しています。

表 25-14　Cisco Emergency Responder の VM 設定とキャパシティ

VM 設定	自動的に追跡される電話機の最大数	手動で設定される電話機の最大数	ローミング電話機の最大数	スイッチの最大数	スイッチ ポートの最大数	緊急応答ロケーションの最大数
12,000 人のユーザ	12,000	2,500	1,200	500	30,000	3,000
20,000 人のユーザ	20,000	5,000	2,000	1,000	60,000	7,500
30,000 人のユーザ	30,000	10,000	3,000	2,000	120,000	10,000
40,000 人のユーザ	40,000	12,500	4,000	2,500	150,000	12,500

Cisco Emergency Responder およびその他の Unified Communication 製品用に正式に定義された VM 設定は、次の Web サイトで入手できます。

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-emergency-responder.html

Unified CM クラスタごとにアクティブにできる Emergency Responder は 1 つのみです。したがって、クラスタ内のすべての電話機に緊急対応できる十分なリソースがある OVA テンプレートを選択してください。

Emergency Responder のネットワークのハードウェアおよびソフトウェア要件の詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』を参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

Cisco Expressway

Cisco Expressway の導入は、リモート エンドポイントの登録を含むコール制御のコンポーネントとしての Cisco Unified CM に依存します。このようなシステムのサイジングでは、実行する機能と Unified CM への影響を考慮する必要があります。

Cisco Expressway をサイジングする場合、通常は Cisco Expressway-C と Expressway-E のノードペアの必要数を決定する次のパラメータを検討する必要があります。

- ピーク使用時における Expressway-C ノードと Expressway-E の各ノード ペアによるエンドポイント登録の数
- Expressway-C ノードと Expressway-E の各ノードペアを通過する同時音声専用コールとビデオ コールの予測数

Expressway-C クラスタと Expressway-E クラスタは最大 6 つのノードをサポートします。

モバイルおよびリモート アクセスにはライセンスは特に必要ありませんが、Business-to-Business（B2B）コミュニケーションにはリッチ メディアのライセンスが必要です。リッチ メディア セッション形式のライセンスは、Expressway クラスタ全体で共有されます。クラスタ内の各 Expressway ノードに割り当てられたリッチ メディア セッションは、クラスタ内のすべてのノードで共有されるクラスタ データベースに供与されます。このモデルでは、いずれか 1 つの Expressway ノードが物理的なキャパシティよりも多くのライセンスを保持できます。

Cisco Expressway のキャパシティ プランニング

表 25-15 に、Cisco Expressway のプロキシ登録数と Cisco Expressway-C ノードと Expressway-E ノードのペアおよびクラスタのコール キャパシティを示します。

表 25-15　Cisco Expressway-C ノードと Expressway-E ノードおよびクラスタのキャパシティ

プラットフォーム	プロキシ登録数[1]	ビデオ コール	音声専用コール
大規模な OVA（または Expressway アプライアンス）	ノードごとに 2,500 クラスタごとに 10,000	ノードごとに 500 クラスタごとに 2,000	ノードごとに 1,000 クラスタごとに 4,000
中規模な OVA（または Expressway アプライアンス）	ノードごとに 2,500 クラスタごとに 10,000	ノードごとに 100 クラスタごとに 400	ノードごとに 200 クラスタごとに 800
小規模な OVA（Business Edition 6000）	ノードごとに 2,500 クラスタごとに 2,500[2]	ノードごとに 100 クラスタごとに 100[2]	ノードごとに 200 クラスタごとに 200[2]

1. プロキシ登録は、モバイルおよびリモート アクセス接続にのみ適用され、Business-to-Business（B2B）コミュニケーションには適用されません。
2. Cisco Expressway-C と Expressway-E を複数の Business Edition 6000 ノードにわたってクラスタ化して冗長性を持たせることができます。ただし、Business Edition 6000 でクラスタ化する場合は、キャパシティは増えません。

（注）　大規模 OVA テンプレートは、限られたハードウェアでのみサポートされます。詳細については、https://www.cisco.com/go/virtualized-collaboration にあるドキュメントを参照してください。

Cisco Expressway をクラスタ化する場合は、次のガイドラインが適用されます。

- Expressway クラスタは最大 6 ノードをサポートします（クラスタ容量はノード容量の最大 4 倍）。
- Expressway-E クラスタと Expressway-C クラスタの各ペア間およびペア内のすべてのノードの容量は、同じである必要があります。たとえば、Expressway-E クラスタ内または対応する Expressway-C クラスタ内の他のノードが最小サイズの VM 設定を使用している場合は、大規模な VM 設定を使用している Expressway-E を導入しないでください。
- Expressway のピアは、Expressway-E クラスタと Expressway-C クラスタで同じ数だけ展開する必要があります。たとえば、3 ノードの Expressway-E クラスタは、3 ノードの Expressway-C クラスタとともに展開する必要があります。
- Expressway-E クラスタと Expressway-C クラスタのペアは、ノード容量がすべてのノードで同じであるかぎり、アプライアンスで実行されるノードまたは仮想マシンとして実行されるノードを組み合わせて構成できます。
- Expressway ノードの VM 設定または Expressway アプライアンスは、Expressway シリーズのクラスタ ペア間およびそれらのクラスタ ペア内で一致する必要があります。
- 複数の Expressway シリーズ クラスタのペアを導入してキャパシティを増やすことができます。

（注）　Cisco Expressway クラスタと Cisco Unified CM クラスタ間には依存関係があります。また、Expressway のキャパシティ プランニングでも、関連または依存する Unified CM クラスタのキャパシティも考慮する必要があります。

サイジングの制限、キャパシティ プランニング、および導入に関する考慮事項など、Cisco Expressway のキャパシティ プランニングに関する考慮事項の詳細については、次の Web サイトで入手可能な Cisco Expressway の製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html

ゲートウェイ

PSTN ゲートウェイは、Unified Communications システムと PSTN 間のトラフィックを処理します。トラフィック量は、リソース使用率（CPU とメモリ）およびゲートウェイに必要な PSTN DS0 回線を決定します。

PSTN トラフィックは Unified CM に登録されているエンドポイントによって生成されますが、音声自動応答装置（IVR）アプリケーションやコンタクト センター配置の一部などの他のソースがある場合もあります。

ゲートウェイは、リソース（CPU、メモリ、DSP など）を必要とする他の機能も実行できます。これらの機能には、メディア ターミネーション ポイント（MTP）、トランスコーディング、会議ブリッジ、RSVP Agent などのメディア処理が含まれます。

特に Cisco Integrated Service Router（ISR）に基づくゲートウェイは、VXML 処理エンジンとしての動作、境界要素としての機能、Cisco Unified Communications Manager Express または Survivable Remote Site Telephony（SRST）としての役割、または WAN エッジ機能の実行などのその他の機能を提供できます。ゲートウェイの負荷を計算するときは、これらのすべてのアクティビティを考慮する必要があります。

ゲートウェイ グループ

ゲートウェイの数を考慮するときは、物理ゲートウェイ サーバの地理的な配置も考慮する必要があります。PSTN アクセスが分散される配置モデルでは、ゲートウェイをグループとしてサイジングし、適切な負荷を各グループに割り当てる必要があります。

共通の特性を持つゲートウェイ群の、特定のゲートウェイを特定の機能専用にする場合にも、グループ化が適切なことがあります。

したがって、必要なゲートウェイの数を正確に見積もるには、次の情報が必要です。

- 共通のグループ プロファイルを共有するゲートウェイのグループ。共通のプロファイルは、導入の複雑さに依存します。
- 各グループのプロファイルを構成するトラフィック パターン、プラットフォーム、ブロック確率など。
- グループを構成する個々のゲートウェイ プラットフォーム。特定のゲートウェイ モデルを決定するときは、期待される機能とキャパシティをそのモデルでサポートできることを確認します。パフォーマンス要件を満たすために選択したプラットフォームの機能に応じて、ゲートウェイ グループに複数のゲートウェイが必要になることがあります。

PSTN トラフィック

PSTN 回線は、システム内のすべてのユーザによって共有され、通常は PSTN 回線よりも多くのユーザが存在します。必要な回線の数は、コール トラフィックの項で説明されているトラフィック管理の原理を使用して予測されます（コール トラフィック (25-23 ページ)）。

必要な PSTN 回線の数は、企業で受信および発信される外部トラフィックの量によって決まります。TDM ベースのシステムから変換する場合、お客様の多くは、IP ベースのコミュニケーション システムにおいても、それまでのシステムで使用していたのと同じ数の回線を使用し続けます。しかし、新たにトラフィック分析を行うことで、現在のトラフィックのレベルに対してシステムのプロビジョニングが過剰である（その結果、不要な回線にコストを費やしている）かどうかを明らかにすることができます。システムのプロビジョニングが不足している場合、許容できない数のコールのブロックや損失が発生します。この場合は回線数を増やすと状況が改善します。

ゲートウェイの DSP 要件は、PSTN 回線の数によって決まります。IP と TDM 音声間の変換を実行するには、DSP リソースが必要です（PSTN 回線は TDM エンコーディングを使用します）。

重要な入力の 1 つにブロック係数があり、ピーク トラフィック レベルで処理できない可能性があるコール試行の比率が決まります。ブロック係数を小さくとると、より多くのコール試行が成功しますが、システムはブロック係数が高い場合よりもより多くの回線を必要とします。

コンタクト センター トラフィックに対するゲートウェイのサイジング

短い通話時間とバースト性のある着呼率は、PSTN ゲートウェイのトラフィック処理能力に影響を与えます。このような状況では、通話時間の長いコールを一定期間にわたって均等に受けるような場合に比べて、すべてのコールをタイムリーに処理するためにゲートウェイでより多くのリソースが必要となります。ゲートウェイにはこのようなトラフィック パターンを処理するさまざまな機能が装備されているため、ゲートウェイを選定する際は使用する環境を考慮して入念に検討する必要があります。ゲートウェイの中には、サポートする T1/E1 ポートの数が多い機種や、同時に着信した複数コールの処理能力が高い機種などがあります。

複数のコールがほぼ同時に着信する（つまり、着呼率が高い、またはバースト性がある）トラフィック パターンでは、適切なコール数/秒（cps）性能を持つゲートウェイが最も適しています。このような状況で、たとえば、Cisco 3945 ntegrated Services Router では 28 cps（一度にアクティブにできるコール数は 420 ）を維持できます。

着呼率が安定したトラフィック パターンでは、通常、ゲートウェイが処理可能なアクティブ コールの最大数がより重要になります。このような状況で、たとえば保留時間が 180 秒のコールを使用すると、Cisco 3945 Integrated Services Router では 720 の同時アクティブ コール（着呼率は最大 4 cps）を維持できます。

これらの数値は、次の条件がすべて該当する場合を前提とします。

- CPU 使用率が 75% を超えない。
- PSTN ゲートウェイ コールは、ISDN PRI トランクで H.323 を使用して行われる。
- Real Time Control Protocol（RTCP）タイマーがデフォルト値の 5 秒に設定されている。
- 音声アクティビティ検出（VAD）がオフになっている。
- G.711 のパケット化の周期は 20 ms である。
- Cisco IOS Release 15.0.1M が使用されている。
- 専用の音声ゲートウェイ設定を使用し、イーサネット（またはギガビット イーサネット）出力を有効に、QoS 機能を無効にしている（QoS 対応の出力インターフェイスまたはイーサネット以外の出力インターフェイス、あるいはその両方を使用すると、CPU リソースの消費量が増えます）。
- 付加コール機能や付加サービス、たとえばセキュリティ全般（アクセス コントロール リストやファイアウォールなど）、音声固有のセキュリティ（TLS、IPSec、SRTP）、AAA ルックアップ、ゲートキーパーを介したコール セットアップ、VoiceXML または TCL によるコール フロー、コール アドミッション制御（RSVP）、SNMP ポーリング/ロギングなどを有効にしていない。このような追加のコール機能を有効にすると、CPU リソースの消費量が増えます。

音声アクティビティ検出（VAD）

音声アクティビティ検出（VAD）は、コールの特定の方向の通話路が無音と認識されている間、IP パケットがほとんど生成されないようにするデジタル信号処理機能です。通常は、ある時点で発話しているのは一方の通話者だけなので、パケットは一方向だけに流れればよく、逆方向（無音方向）では不定期のキープアライブを除き、パケットを送信する必要はありません。そのため、VAD を使用すると、VoIP コールで送信される IP パケットの数が大幅に減少し、それに伴ってゲートウェイ プラットフォームの CPU サイクルも大幅に低下します。VAD によってパケットが実際にどの程度減少するかは、コール フロー、アプリケーション、および会話の状況によって異なりますが、VAD 設定を無効にした場合と比べて、パケットが 10 ～ 30 % 少なくなる傾向があります。

VAD は、エンドポイントや Unified CM ネットワークに配置された音声ゲートウェイではほとんどの場合無効にされており、その他の種類のネットワークに配置された音声ゲートウェイでは、ほとんどの場合、有効にされています。

コーデック

G.711 と G.729A のサンプリング時間はどちらもデフォルトで 20 ms に設定されているため、VoIP コールの一方向のパケット レートは 50 パケット/秒（pps）になります。G.711 の IP パケット（200 バイト）は G.729A のパケット（60 バイト）よりも大きいですが、この差が音声ゲートウェイの CPU パフォーマンスに大きな影響を与えるとは実証されていません。G.711 と G.729 のパケットはどちらもルータには「小さい」IP パケットと見なされます。そのため、パケット レートが CPU パフォーマンスに影響を与える重要なコーデック パラメータです。

パフォーマンスの過負荷

Cisco IOS は、割り込みレベルのイベントを処理するために、ピーク処理中にも CPU の使用率が 100 % にならないように設計されています。この項に示すパフォーマンスの数値は、約 75 % の平均的な負荷を実行しているプロセッサで測定されたものです。特定の Cisco IOS ゲートウェイの負荷がこのしきい値を継続的に超えると、次のようになります。

- Cisco Technical Assistance Center（TAC）でその配置がサポートされなくなります。
- Cisco IOS ゲートウェイで、Q.921 タイムアウト、ダイヤル後遅延の増大、インターフェイス フラップなどの異常な動作が起こります。

Cisco IOS ゲートウェイは短時間のコールのバーストであれば処理できるようになっていますが、推奨される着呼率（コール数/秒）が継続的に超過するような状況はサポートされていません。

（注） ゲートウェイに未使用のハードウェア ポートがある場合は、そのポートを他のタスクに割り当てたくなるものです（たとえば、Cisco Communication Media Module（CMM）ゲートウェイで、トラフィック計算によって PSTN トラフィックに一部のポートしか使えないことがわかっている場合など）。しかし、残りのポートは必ず未使用のままにしておく必要があります。そうしないと、CPU がサポートされるレベルを超えて過負荷状態に陥ります。

パフォーマンスの調整

Cisco IOS 音声ゲートウェイの CPU 使用率は、シャーシで有効にされているすべてのプロセスの影響を受けます。最も低レベルのプロセスの一部（IP ルーティングやメモリのデフラグなど）は、シャーシにライブ トラフィックがないときにも実行されます。

CPU 使用率が下がると、リアルタイムの音声パケットやコール セットアップ命令の処理に十分な CPU リソースを使用できるようになり、Cisco IOS 音声ゲートウェイのパフォーマンスが向上します。CPU 使用率を削減する手法のいくつかを表 25-16 に示します。

表 25-16　ゲートウェイの CPU 使用率を削減する手法

手法	CPU 使用率の削減量	説明
VAD を有効にする	最大 20 %	VAD を有効にすると、標準的な会話において音声パケットの量が最大 45 % 減少します。問題は、音声認識を使用している場合や遅延が長い場合に音声品質が低下する可能性があることです。音声は発話の開始時に突然生じ、終了時に唐突に消失するように感じられます。
RTCP を無効にする	最大 5 %	RTCP を無効にすると、発信側と着信側のゲートウェイ間で送信されるアウトオブバンド情報が減少します。その結果、相手側のゲートウェイに表示される統計情報の品質が低下します。また、コールがすでにアクティブでないかどうかを判断するために RTCP パケットが使用されている場合は、着信側ゲートウェイでコールの「未完結状態」が長くなる可能性があります。
その他の重要でない機能（認証、許可、アカウンティング（AAA）、簡易ネットワーク管理プロトコル（SNMP）、ロギングなど）を無効にする	最大 2 %	これらのプロセスは、必要でない場合は無効にできます。これらのプロセスを無効にすると、CPU がその分解放されて CPU 使用率が低下し、リアルタイム トラフィックの処理が高速になります。
コール パターンを変更してコールの長さを長くする（これにより、1 秒あたりのコール数を削減する）	可変	これはさまざまな手法で実現できます。たとえば、コールの最初に長い導入プロンプトを再生する（または既存の導入プロンプトを長くする）、コール スクリプトをコール センターで調整する、といった手法があります。

その他の情報

この章では、すべてのゲートウェイ、その機能、および呼処理キャパシティの詳細については説明していません。Cisco 音声ゲートウェイの詳細については、次のマニュアルを参照してください。

- Cisco Voice Gateway ソリューション：

  https://www.cisco.com/c/en/us/products/unified-communications/communications-gateways/index.html

- 次の Cisco Voice Gateway でサポートされるインターフェイスおよびシグナリング タイプ：
  - Cisco 3900 シリーズ サービス統合型ルータ

    https://www.cisco.com/c/en/us/products/routers/3900-series-integrated-services-routers-isr/relevant-interfaces-and-modules.html
  - Cisco 2900 シリーズ サービス統合型ルータ

    https://www.cisco.com/c/en/us/products/routers/2900-series-integrated-services-routers-isr/relevant-interfaces-and-modules.html

- MGCP、SIP、および H.323 でサポートされるゲートウェイ機能：

  https://www.cisco.com/c/dam/en/us/products/collateral/routers/2800-series-integrated-services-routers-isr/product_data_sheet0900aecd8057f2e0.pdf

- SIP ゲートウェイ RFC 準拠：

  https://www.cisco.com/c/en/us/products/collateral/unified-communications/ios-gateways-session-initiation-protocol-sip/product_data_sheet0900aecd804110a2.html

- FXS ゲートウェイでサポートされる Skinny Client Control Protocol（SCCP）機能：

  https://www.cisco.com/c/en/us/products/collateral/unified-communications/vg-series-gateways/product_data_sheet09186a00801d87f6.html

- ゲートウェイの容量、および会議、トランスコーディング、メディア ターミネーション ポイント（MTP）、MGCP、SIP、H.323 ゲートウェイ機能に必要な Cisco IOS および Unified CM の最小リリース：

  https://www.cisco.com/c/dam/en/us/products/collateral/routers/2800-series-integrated-services-routers-isr/product_data_sheet0900aecd8057f2e0.pdf

ボイス メッセージング

ボイス メッセージングは、単独でサイジングするだけでなく、他の Unified Communications コンポーネント（主に Unified CM）に対する影響も考慮してサイジングする必要があるアプリケーションです。

合計ユーザ数は、ボイス メッセージング システムをサイジングする主な要因です。ボイス メッセージングのサイジングに影響を与えるその他の要因は次のとおりです。

- アプリケーションで処理する必要がある最繁時のコール数
- サーバに残されるメッセージの平均的な長さ
- 最繁時にメッセージを確認するユーザの数
- ユーザ セッションの平均的な長さ
- 音声認識や音声合成セッションなどの高度な操作
- メディア トランスコーディング
- ボイス メッセージング システム上のポートは、ゲートウェイ上の DS0 に似ており、最適化する必要がある共有リソースです。確率的着呼に関する同じ考慮事項とブロックの必要性が両方のリソース タイプに適用されます。

表 25-17 に、各種ボイス メッセージング ソリューションが配置の拡張性要件に適合可能かどうかを示します。

表 25-17　ボイス メッセージング ソリューションの拡張

対処方法	単一ノードでサポートされる最大ユーザ数（またはフェールオーバーまたはクラスタの導入）				デジタル ネットワーキング ソリューションでサポートされる最大ユーザ数	HTTPS ネットワーキング ソリューションでサポートされる最大ユーザ数
	500	1,000	15,000	20,000	100,000	100,000
Cisco Unity Express	○	X	X	X	○	X
Cisco Business Edition	○	○	X	X	X	X
Cisco Unity Connection（Unified/Integrated Messaging and Cisco Business Edition 7000）	○	○	○	○	○	○

表 25-18 に、Cisco Unity Connection を実行している各種 VM 設定のさまざまな機能の上限を示します。

表 25-18　Cisco Unity Connection 用の VM 設定とキャパシティ

VM 設定	ポートの最大数	最大音声認識セッション数	最大音声合成セッション数	ボイスメール ユーザの最大数
100 人のユーザ	8	8	8	100
500 人のユーザ	16	16	16	500
1,000 人のユーザ	24	24	24	1,000
5,000 人のユーザ	100	100	100	5,000
10,000 人のユーザ	150	150	150	10,000
20,000 人のユーザ	250	250	250	20,000

Cisco Unity Connection 用の正式の VM 設定の定義は、次の Web サイトから入手できます。

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unity-connection.html

Unified CM に対する影響

Unified CM に対するボイス メッセージング システムの影響は、Unified CM で実行する必要がある追加処理を考慮して測定できます。これらの追加処理によるコール フローは、Unified CM のサイジング負荷を次のように増やします。

- ユーザがいないとき、あるいはユーザが応答不可（DND）または他の機能を使用してコールを故意に転送するときに、ボイス メッセージング システムに転送する必要があるコール。
- ボイス メッセージングのパイロット番号をダイヤルしてボイス メッセージにアクセスするユーザからのコール。これらのコールは、Unified CM を通過し、コールの数と期間など、Unified CM が処理するコールに追加する必要があります。

コラボレーティブ会議

Cisco コラボレーティブ会議システムには、呼制御のためのコンポーネントとして Cisco Unified CM が含まれます。このようなシステムのサイジングでは、実行する機能と Unified CM への影響とを考慮に入れる必要があります。

そのような会議システムをサイジングする場合は、一般に次のパラメータを考慮してノードのタイプと数を決定する必要があります。

- システムを一度に使用できるユーザの数
- ピーク使用時におけるシステム上の音声、ビデオ、および Web ユーザの数
- 必要なダイヤルイン期間
- ビデオ解像度とオーディオ コーデックの要件

音声会議のサイジングに関するガイドライン

音声会議容量を計算するために次の方法を推奨します。

- 平均月間使用時間に基づく計算

  音声会議の平均使用時間（1 ヵ月あたりの平均時間（分））がわかっている場合は、表 25-19 を使用して音声会議容量を計算します。

表 25-19　平均月間使用時間に基づく音声会議容量

平均月間使用時間（分）	ベースライン使用時間（1 ヵ月間のポートあたりの分数）	予想ポート数
20,000 ～ 50,000	1,500	15 ～ 35
50,000 ～ 500,000	2,000	25 ～ 250
500,000 ～ 1,000,000	3,000	165 ～ 335
1,000,000 ～ 2,000,000	3,500	285 ～ 570
2,000,000 ～ 8,000,000	4,000	500 ～ 2,000

- ユーザ数に基づく計算

  平均的使用率の 20 ユーザごとに 1 ポートを割り当てるように検討する必要があります。使用頻度の高い会議ユーザの場合は、15 ユーザごとに 1 ポートを用意します。たとえば、6000 ユーザのシステムでは、300 音声ポートを用意する必要があります。ただし、ユーザの会議使用頻度が高い場合は、400 音声ポートを検討します。

- ピーク時の使用時間に基づく計算

  一般的に、音声会議のピーク時の使用時間は、既存の音声会議システムのログまたはサービス プロバイダーの請求書から得られます。余裕をもった会議容量を確保するために、実際のピーク時使用時間よりも 30 % 多い容量を用意することを推奨します。

システム サイジングに影響する要素

システム ベースライン ポートの要件について前述した方法による見積もり以外に、次の要素もシステム サイジングに影響します。

- 「オペレータ スケジュール」モデルからユーザ スケジュール モデルに移行する場合は、ベースラインに 20 % 上積みしなければならない可能性があります。
- デフォルトの平均会議サイズは、会議あたり 4.5 発信者です。デフォルトと異なる場合は、自分のケースに応じた値を使用してください。
- 次の条件が当てはまる場合は、それに応じてベースライン見積もりを増やします。

  (1 日あたりの予想会議数)*(予想ユーザ数)> ベースラインの 80 %
- 最大規模の会議が予想容量の 20 % を超えている場合は、それに応じて見積もりを増やします。
- 専用ポートを使用して会議を連続して行う場合は、追加のポート((会議数)*(専任発信者数))をベースラインに加算する必要があります。

総ポート数には、上記要素のすべてとベースラインが含まれます。見積もったポート容量の合計がサポートされる最大ポート数の 80 % を超える場合、会議システムの容量拡張を検討してください。

ビデオ会議のサイジングに関するガイドライン

ビデオ会議のキャパシティを計算するために次の 3 つの方法を推奨します。

- ナレッジ ワーカの数に基づく計算

  40 人のナレッジ ワーカごとに 1 つのビデオ ユーザ ライセンスを用意することを推奨します。
- 音声会議ユーザ ライセンス数に基づく計算

  既存の音声ユーザ ライセンス数の 17 ～ 25 % の範囲のビデオ会議容量を用意することを推奨します。この割合は、ビデオ会議に関するビジネス要件と会議システムの規模によって異なります。
- 既存のビデオ マルチポイント コントロール ユニット(MCU)に基づく計算

  既存のビデオ会議システムをそのまま置き換えることを推奨します。

Unified CM に対する影響

Unified CM に対する影響は、会議システムによって生成される追加分のコール トラフィックに基づいて分析できます。最大の影響は、会議ユーザが通常 0 分または 30 分にスケジュールされる会議にダイヤルインしたときに発生します。会議の開始後数分以内に大量のコール トラフィックが発生し、その数分間の Unified CM 上の負荷が増大するため、適切に設計する必要があります。さらに、会議ユーザに PSTN または他のクラスタからの発信者が含まれている場合、それらのパラメータも考慮してゲートウェイに対するその影響を測定する必要があります。

Cisco WebEx Meetings Server

Cisco WebEx Meetings Server は、企業によって提供されたサーバ（企業データセンター内の Cisco UCS サーバ クラスタ）を使用して WebEx 会議サービスを提供します。

Cisco WebEx Meetings Server は、異なる構成で提供されます。この場合、サイジング ツールで、主に会議サービスにアクセスできるナレッジ ワーカーの数に基づいて選択されます。

各構成について、シスコは、ハードウェアと VMware 製品の特定の構成がある標準 Cisco UCS サーバ タイプを推奨しています。ただし、Cisco WebEx Meetings Server は、これらの仕様を満たしているか、またはそれらを上回る、同等またはより優れた Cisco UCS Server で機能するように設計されています。

この製品は、DVD 上のソフトウェア パッケージの集まりではなく、VMware vSphere 対応の OVA 仮想アプライアンスとしてパッケージ化されています。Cisco WebEx Meeting Server は、OVA を導入し Cisco WebEx Meeting Server 製品をインストールするのに vCenter 製品を必要とします。

現在、Cisco WebEx Meetings Server は、Cisco UCS サーバの共存モードでは動作しません。Cisco WebEx Meetings Server には、専用 UCS サーバが必要です。

Cisco WebEx Meetings Server の詳細については、次の場所にある『*Cisco WebEx Meetings Server Planning Guide and System Requirements*』の最新版を参照してください。

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

サイジングの要因

サイジング ツールは、次の入力を使用してシステム容量を計算します。

- ナレッジ ユーザの数

  ナレッジ ユーザの数は、会議システムにアクセス（会議を開始または会議に参加するため）できる従業員の集合として定義されます。

  多くのナレッジ ユーザは、使用可能な会議ポートを共有します。任意の時点で、一部のユーザのみ会議コールでアクティブであることが前提とされています。この割合に基づいて、これらのユーザをサポートするのに必要な会議ポートの数を見積もることができます。

  サイジング ツールは、低い使用率（一度に 3.3 % のユーザがアクティブ）、平均的な使用率（5 % がアクティブ）、および高い使用率（10 % がアクティブ）を定義します。そのため、平均的な使用率で動作するシステムは、高い使用率のシステムに比べて 2 倍のユーザをサポートします。

- 1 ヵ月あたりのユーザ時間（分）

  1 ヵ月あたりのユーザ時間（分）は、すべてのポートにおける月のアクティブ会議の合計時間（分）です。この値は、数千分で表されます。この要因は、記録サーバのサイズを計算する際に重要となります。

- 実際のピーク使用率

  実際のピーク使用率は、システムの同時ユーザの最大数として定義されます。この数は、必要な会議ポート数を決定する際に重要となります。シスコは、ピーク使用時に十分な会議ポートが使用可能であることを保証するため、実際のピーク使用率よりも 30 % 多くのユーザを処理するのに十分な容量のプロビジョニングを推奨しています。

- [ビデオ（Video）]

  ビデオおよび高画質ビデオでの会議の割合は、システムによって要求されるネットワーク帯域幅に影響を与えます。最大 50 % のユーザが高画質ビデオを使用できます。

- トラフィックの構成

  異なるコール タイプには、異なる Unified CM リソースが必要です。Unified CM の影響を正確に評価するため、ツールは次のコール タイプの評価を要求します。

  - エンタープライズ IP Phone を介して着信する会議コールの割合。このコール レッグは Unified CM によって処理されるため、Unified CM キャパシティに影響を与えます。
  - PSTN ゲートウェイのサイジングに影響を与える外部コール レッグの割合。

- 外部ユーザによるアクセス

  外部ユーザがシステムにアクセスする必要がある場合は、追加の仮想マシンを設定してリバース プロキシ機能を提供します。システムが内部ユーザだけを対象としている場合は、これらの追加の仮想マシンは必要ありません。

- ディザスタ リカバリ

  ディザスタ リカバリでは、セカンダリ データセンターにコールドスタンバイ システムを設定できます。プライマリ システムがハイ アベイラビリティで設定されている場合、ディザスタ リカバリ システムに対してハイ アベイラビリティを設定するように選択することもできます。

- ハイ アベイラビリティ

  システムは、非冗長モードまたはハイ アベイラビリティ（HA）モードで設定できます。HA モードでは、クラスタは 1 つ以上のバックアップ サーバでプロビジョニングされます（システム サイズに応じて特定の設定）。

システムのキャパシティ

Cisco WebEx Meetings Server は、表 25-20 に示すよう、4 つのシステム サイズで提供されます。システム サイズは、システムの同時ユーザの最大数で表されます。最大同時ユーザは、所定の時間に会議コールに参加できるユーザの最大数を定義します。

表 25-20　Cisco WebEx 会議サーバ用の VM 設定とキャパシティ

最大数	50 人の同時ユーザ	250 人の同時ユーザ	800 人の同時ユーザ	2,000 人の同時ユーザ
音声と Web ユーザ（組み合わせ）	50	250	800	2,000
ビデオおよびビデオ共有（組み合わせ）	25	125	400	1,000
1 つの会議の参加者	50	100	100	100
終了した会議の録画の再生	12	63	200	500
進行中の会議の録画	3	13	40	100
会議数（会議あたり平均 2 人の参加者）	25	125	400	1,000
コール数/秒	1	3	8	20

次のオプションの機能がシステム容量に影響を与えることなく使用できることに注意してください。

- 暗号化された音声（sRTP）
- セキュアな Web 会議センター（SSL）
- 異なる音声コーデック
- 低解像度のビデオ

録音（Recordings）

最大 5 % のポート（または 10 % の会議）を録画できます。録画された会議を保存するには、十分なサイズの NFS 搭載ハード ドライブをプロビジョニングする必要があります。50 ～ 100 MB のサイズのファイルが 1 つの会議で生成されます。

ネットワーク帯域幅

LAN および WAN で必要な帯域幅を見積もるため、サイジング ツールは次の前提を行います。

- 各ポートは、1 Mbps のネットワーク帯域幅を使用する。
- ユーザの構成は、80 % が企業内部であり、20 % が外部である。

そのため、LAN の必要な帯域幅（Mbps）は 0.8 *（ポート数）であり、WAN は 0.2 *（ポート数）です。

Cisco Prime Collaboration 管理ツール

Cisco Prime Collaboration は、Cisco Unified Communication と TelePresence システムを試験、導入、およびモニタリングする統合ツール セットを提供します。Cisco Prime Collaboration には、Prime Collaboration Provisioning、Prime Collaboration Assurance、Prime Collaboration Analytics が含まれます。

これらのアプリケーションは仮想マシン上で実行されます。Cisco Prime Collaboration Provisioning は独自の仮想マシン上で実行され、Cisco Prime Collaboration Assurance と Cisco Prime Analytics は同じ仮想マシン上で実行されます。これらのアプリケーションの仮想マシン サイジングは比較的単純で、管理するエンドポイントまたはネットワーク デバイスの数に直接依存します。

Cisco Prime Collaboration Provisioning

Cisco Prime Collaboration Provisioning は最大 150,000 のエンドポイントをサポートし、単一のマシン（最大 10,000 のエンドポイントの場合）または 2 台のマシン（10,000 以上エンドポイントの場合）のいずれかに実装されます。

さまざまなレベルのパフォーマンスに必要な仮想マシン リソースについては、次の場所にある『Cisco Prime Collaboration のインストール ガイドとアップグレード ガイド』の最新版に記載されています。

https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.html

Cisco Prime Collaboration Assurance

Cisco Prime Collaboration Assurance は、ルータやスイッチなどの電話やその他のネットワーク デバイスを管理できます。これは単一マシン構成で動作し、最大 150,000 台の電話機をサポートします。

さまざまなレベルのパフォーマンスに必要な仮想マシンのリソースについては、次の Web サイトから入手可能な『*Cisco Prime Collaboration Quick Start Guide*』の最新バージョンを参照してください。

https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.html

Cisco Prime Collaboration Analytics

Cisco Prime Collaboration Analytics は、Cisco Prime Collaboration Assurance と同じ仮想マシン上で実行し、音声品質を測定するために Cisco Network Analysis Module（NAM）と連携して動作します。

さまざまなレベルのパフォーマンスに必要なハードウェア リソースについては、次の Web サイトから入手可能な『*Cisco Prime Collaboration Data Sheet*』の最新バージョンを参照してください。

https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/datasheet-listing.html

スタンドアロン製品のサイジング

次の製品はサイジング ツールに含まれていませんが、次の項でこれらの製品をサイジングする方法について説明します。

- Cisco Unified Communications Manager Express（25-52 ページ）
- Cisco Business Edition（25-53 ページ）

Cisco Unified Communications Manager Express

Cisco Unified Communications Manager Express（Unified CME）は、Cisco IOS サービス統合型ルータ（ISR）プラットフォーム（ローエンドの Cisco 881 ISR からハイエンドの Cisco 3945E ISR 2 まで）のいずれかで実行されます。これらの各ルータでは、サポートできる電話機の数に上限があります。これらのプラットフォームが呼処理を実行するための実際のキャパシティは、IP ルーティング、ドメイン ネーム システム（DNS）、Dynamic Host Control Protocol（DHCP）などのほかに他に実行する機能によって制限されることがあります。

Unified CME は、単一の Cisco IOS プラットフォーム上で最大 450 エンドポイントをサポートできます。ただし、各ルータ プラットフォームのエンドポイントのキャパシティは、システムのサイズによって異なります。Unified CME は Cisco Collaboration Sizing Tool ではサポートされないため、次の場所にある Unified CME の製品データ シートに記載されているキャパシティ情報に従う必要があります。

https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-express/datasheet-listing.html

Cisco Business Edition

Cisco Business Edition は、音声、ビデオ、モビリティ、メッセージング、会議、インスタント メッセージとプレゼンス、コンタクト センター アプリケーション用のプレミアム サービスがプリロードされ、パッケージ化されたコラボレーション ソリューションです。

Cisco Business Edition 4000（BE4000）は、Business Edition ファミリに新しく加えられたものです。BE4000 は、Cisco Unified Communication Manager Express が組み込まれており、中小の単一サイト導入と、リモート サイトでのローカル呼処理が必要な導入に呼処理サービスを提供します。

BE4000 は、それぞれのデバイスにテレフォニーとボイスメール ポートがライセンスされている最大 200 台の音声テレフォニー デバイスに音声テレフォニーおよびボイスメール サービスを提供する、専用のクラウドマネージ型プラットフォームです。

BE4000 は、次の最大 200 ユーザをサポートします。

- Cisco IP Phone 7800 シリーズと 8800 シリーズ SIP エンドポイント
- Cisco Unity Express Virtual ボイスメール
- 最大で 5 の最繁時呼数（BHCA）

Cisco Unified Business Edition 6000 と 7000 の両方に、形式を選択するためのプラットフォーム モデル オプションが備わっています。

Cisco Business Edition 6000 は、次の 3 つのハードウェア プラットフォーム オプションで入手できます。

- BE6000H：最大キャパシティは 1,000 ユーザ、2,500 デバイス、および 100 コンタクト センター エージェントです。9 つのコラボレーション アプリケーション オプションを単一の仮想化サーバ プラットフォームでサポートします。最大 BHCA は 5,000 です。
- BE6000M：最大キャパシティは 1,000 ユーザ、1,200 デバイス、および 100 コンタクト センター エージェントです。5 つのコラボレーション アプリケーション オプションを単一の仮想化サーバ プラットフォームでサポートします。最大 BHCA は 5,000 です。
- BE6000S：最大キャパシティは 150 ユーザ、300 デバイスです。単一の統合ルータ/ゲートウェイ/仮想化ブレード サーバ プラットフォームで 5 つの固定コラボレーション アプリケーションをサポートします。最大 BHCA は 750 です。

Cisco Business Edition 6000 ソリューションの詳細については、https://www.cisco.com/go/be6000 を参照してください。

Cisco Business Edition 7000 は、次の 2 つのハードウェア プラットフォーム オプションで入手できます。

- BE7000H：通常、この高密度モデルは、3,000 ～ 15,000 台のデバイスと複数サイトを持つ 1,000 ～ 5,000 人のユーザ用にサイジングされた導入で 5 ～ 10 のコラボレーション アプリケーションをサポートします。
- BE7000M ：通常、この中密度モデルは、3,000 ～ 15,000 台のデバイスと複数サイトを持つ 1,000 ～ 5,000 人のユーザ用にサイジングされた導入で 4 ～ 6 のコラボレーション アプリケーションをサポートします。

Cisco Business Edition 7000 ソリューションの詳細については、https://www.cisco.com/go/be7000 を参照してください。

Cisco Business Edition の最繁時呼数（BHCA）

この項では、Cisco Business Edition 6000H を例として使用してキャパシティを計算します。ただし、この項の情報は BE6000M とキャパシティが小さい 750 BHCA の BE6000S にも適用されます。

前述のとおり、Business Edition 6000H は、最大 5,000 BHCA をサポートします。システム使用の計算では、Cisco Business Edition 6000 のオーバーサブスクリプションを避けるため、この BHCA 最大数を超えないようにします。任意の電話機の BHCA が 4 BHCA を超えたときに、BHCA に対する配慮が必要になります。真の BHCA 値は、最繁時における電話機の使用状況の基準測定を実施することによってのみ、決定されます。この使用状況を基準なしで見積もった場合は特に注意が必要です。

Cisco Business Edition 6000H のデバイスの計算

デバイスは、この見積もりの目的に沿って 2 つの主なカテゴリーに分けられます。すなわち、電話デバイスとトランク デバイスです。

電話デバイスは、単一のコール可能なエンドポイントです。これには、Cisco Unified IP Phone 8800 シリーズ、またはその他のコラボレーション音声およびビデオ エンドポイントなどの単体のクライアント デバイス、Cisco Jabber などのソフトウェア クライアント、アナログ電話機ポートや H.323 クライアントなどが含まれます。Cisco Business Edition 6000 は BE6000S の最大 300 のエンドポイント、中密度のサーバでは最大 1,200 のエンドポイント、高密度サーバでは最大 2,500 のエンドポイントをサポートしますが、上記で説明するように、実際のエンドポイント キャパシティはシステムの合計 BHCA によって異なります。

トランク デバイスは、複数のコールを複数のエンドポイントまで伝送します。これには、SIP トランクまたはゲートキーパー制御 H.323 トランクなどのトランクまたはゲートウェイ デバイスを使用できます。Business Edition 6000 は、H.323 トランク、SIP トランク、および MGCP トランクやゲートウェイならびにアナログ ゲートウェイのようなクラスタ間トランキングをサポートします。他のプロトコルではなく、SIP トランクの使用を推奨します。

BHCA を見積もる方法は、両方のタイプのデバイスでほとんど同じですが、一般に、トランク デバイスは、外部のユーザ グループ（PSTN または他の PBX 内線）にアクセスするためにより大きなエンドポイントのグループで使用されるため、BHCA が高くなります。

BHCA に基づく使用状況の特性を参照してデバイス グループ（電話デバイスまたはトランク デバイス）を定義してから、各デバイス グループの BHCA を加算して、システムの総 BHCA を求めることができます。これによって、サポートされる最大数の 5,000 BHCA を超えないことを常に確認します。

たとえば、4 BHCA の 100 台の電話機と 12 BHCA の 80 台の電話機の総 BHCA は、次のように計算できます。

4 BHCA の 100 台の電話機：100 * 4 = 400

12 BHCA の 80 台の電話機：80 * 12 = 960

すべての電話機の総 BHCA = (100 * 4) + (80 * 12) = 1,360 BHCA

トランク デバイスの場合は、デバイスで処理されるコールのうち PSTN との間で発着信する割合がわかっていれば、BHCA を計算できます。この例では、すべてのデバイス コールの半分が PSTN との間で発着信している場合、デバイス BHCA（この場合は 1360）のゲートウェイに対する実効値は、1360 の半分、つまり、680 BHCA になります。したがって、この例での電話デバイスとトランク デバイスに関する総システム BHCA は次のようになります。

総システム BHCA = 1,360 + 680 = 2,040 BHCA

複数の電話機でシェアド ラインにしている場合は、シェアド ラインを設定している電話機ごとに 1 つずつのコール レッグ（コールごとに 2 コール レッグ）を BHCA に含める必要があります。複数のデバイス グループにまたがるシェアド ラインは、そのグループの BHCA に影響します。つまり、シェアド ラインに対する 1 つのコールが、回線インスタンスあたり 1 つのコール レッグ、つまり、1 コールの半分として計算されます。BHCA が異なる複数の電話機グループがある場合は、次の方法で BHCA 値を計算します。

シェアド ライン BHCA = 0.5 *（シェアド ライン数）*（1 回線あたりの BHCA）

たとえば、次の特徴を持つ 2 つのユーザ クラスがあるとします。

8 BHCA の 100 台の電話機 = 800 BHCA

4 BHCA の 150 台の電話機 = 600 BHCA

また、1 グループあたり 10 本のシェアド ラインがあるとして、次の BHCA 値に加算します。

8 BHCA のグループ内の 10 本のシェアド ライン = 0.5 * 10 * 8 = 40 BHCA

4 BHCA のグループ内の 10 本のシェアド ライン = 0.5 * 10 * 4 = 20 BHCA

この場合のすべての電話デバイスに関する総 BHCA は、シェアド ラインの BHCA の合計に加算された電話機グループごとの BHCA の合計になります。

800 + 600 + 40 + 20 = 1,460 総 BHCA

上記の各例の総 BHCA は、システムの最大数である 5,000 BHCA を下回っているため、許容範囲に含まれることに注意してください。

Business Edition 6000 でシングル ナンバー リーチ（SNR）用に Cisco Unified Mobility を使用している場合、リモート接続先およびモビリティ ID に転送されたコールまたはオフシステム電話番号が BHCA に影響することに留意してください。アプライアンスがオーバーサブスクライブするのを防ぐには、この SNR リモート接続先またはオフシステム電話の BHCA を考慮する必要があります。これらの SNR 機能の BHCA を計算するには、Cisco Unified Mobility のキャパシティ プランニング（21-79 ページ）を参照して、その値を総 BHCA 値に加算します。

（注）　Secure RTP（SRTP）を使用したメディア認証と暗号化は、システム リソースとシステム性能に影響を与えます。メディア認証または暗号化の使用を検討している場合は、この事実に留意して適切な調整を行ってください。通常、セキュリティに対応していない 100 台の IP Phone は、セキュリティに対応した 90 台の IP Phone と同じ影響をシステム リソースに与えます（10 対 9 の割合）。

Cisco Business Edition 6000 について考慮するキャパシティ プランニングのもう 1 つの側面は、コール カバレッジです。特殊なデバイス グループを作成し、特定のサービスの着信コールを複数のルール（トップダウン、循環ハント、最長アイドル時間、またはブロードキャスト）に従って処理できます。これは、Cisco Business Edition 6000 のハント グループまたは回線グループの設定で実現されます。回線グループの分配アルゴリズムにブロードキャスト（全メンバーを呼び出す）を用いる場合には、この要素によっても BHCA が影響を受けます。Cisco Business Edition 6000 でブロードキャスト分配アルゴリズムが必要な場合は、1 つのハント グループまたは回線グループのメンバー数を 3 以下にすることを推奨します。システムの負荷によっては、この実施によってシステムの BHCA が大きく影響され、プラットフォームのリソースがオーバーサブスクライブする可能性があります。ブロードキャストの分配アルゴリズムを使用するハント グループまたは回線グループの数も 3 以下に制限する必要があります。これらはシステム BHCA のオーバーサブスクリプションを回避するために開発されたベスト プラクティスの推奨事項です。システム全体の BHCA キャパシティを超えない限り、配置内でのこれらの推奨事項の超過はサポートされます。

Unified CM クラスタ内に異なる種類のハードウェア プラットフォームを混在させることも可能です。ただし、すべての VM 設定がすべてのサーバ プラットフォームでサポートされているわけではないため、ハードウェア プラットフォームおよび Business Edition プラットフォームの混在（9-9 ページ）の項で説明するように、VM 設定の混在がクラスタ全体のキャパシティに影響します。

Cisco Business Edition 6000 用の Cisco Unified Mobility

Cisco Business Edition 6000 システムでの Cisco Unified Mobility ユーザの容量は、サーバのハードウェアではなく、ユーザあたりのリモート接続先数および Unified Monbility を有効にしているユーザの BHCA にのみ依存します。したがって、Cisco Business Edition 6000 でサポートされるリモート接続先数は、これらのユーザの BHCA に直接依存します。

設定された各リモート接続先またはモビリティ ID は、BHCA に影響を与える可能性があります。ユーザに設定されているリモート接続先またはモビリティ ID ごとに、追加のコール レッグが 1 つずつ使用されます。各コールは 2 つのコール レッグで構成されているため、1 つのリモート接続先の呼び出しが 1 つのコールの半分に相当します。そのため、リモート接続先の合計 BHCA は次の式で計算できます。

リモート接続先およびモビリティ ID の合計 BHCA = 0.5 *（ユーザ数）*（ユーザごとのリモート接続先数およびモビリティ ID）*（ユーザ BHCA）

次に例を示します。

5 BHCA ごとに 300 人のユーザがいて、それぞれのユーザに 1 つずつのリモート接続先またはモビリティ ID（全部で 300 のリモート接続先およびモビリティ ID）が割り当てられたシステムがあるとすると、リモート接続先およびモビリティ ID の合計 BHCA の計算は次のようになります。

リモート接続先およびモビリティ ID の合計 BHCA =
0.5 *（300 ユーザ）*（ユーザあたり 1 リモート接続先またはモビリティ ID）*（ユーザあたり 5 BHCA）=
750 BHCA

この例でユーザの合計 BHCA は（300 ユーザ）*（ユーザあたり 5 BHCA）、つまり 1,500 です。この値にリモート接続先の合計 BHCA である 750 を加算すると、システムの合計 BHCA 2,250（ユーザの合計 BHCA 1,500 + リモート接続先およびモビリティ ID BHCA の合計 750）が得られます。

上記の例のシステムで他のアプリケーションや追加の BHCA 変数が使用されている場合は、容量はさらに制限される可能性があります（詳細については、前項を参照してください）。

Cisco Business Edition 6000 キャパシティ プランニングの詳細については、他の製品情報と同様に、Cisco Business Edition 6000 に関する次の製品マニュアルを参照してください。

- https://www.cisco.com/go/be6000
- https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html

Cisco Collaboration システムの移行

改訂日：2018 年 3 月 1 日

この章では、管理者が従来の PBX システムから IP テレフォニー、および以前の Cisco Collaboration System リリース（9.*x*、10.*x*、11.*x*）から最新の Cisco Collaboration システム リリース（CSR）12.*x* に移行する際の管理上の推奨事項について説明します。

Open Virtualization Archive（OVA）テンプレート、VMware、ESXi Hypervisor、および Collaboration アプリケーションのハードウェアおよびソフトウェアの最小要件については、次のマニュアルを参照してください。

- *Virtualization Software Requirements*

  https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html

- *VMware Compatibility Guide*

  https://www.vmware.com/resources/compatibility

Cisco Collaboration システム リリース 12.*x* 以降のリリースでは、ほとんどの Cisco Collaboration アプリケーションには仮想化の導入が必要であり、ハイパーバイザなしではサーバに直接インストールされない可能性があります。VMware vSphere ESXi は現在サポートされる唯一のハイパーバイザであり、Cisco Collaboration システム内のすべての仮想化展開で必須です。Cisco Collaboration システム リリースのいずれのリリースも、VMware vSphere ESX を含めて、ESXi 以外のどの VMware のサーバ仮想化製品もサポートしていません。

この章では、次の種類の移行について説明します。

- Cisco 7800 Series MCS サーバから Cisco Unified Computing System（UCS）サーバ上の Cisco Unified Communications Manager（Unified CM）
- Cisco Video Communication Server（VCS）のエンド ポイント登録から Unified CM 登録
- H.323 ゲートウェイおよびトランクから SIP ゲートウェイおよびトランク
- SCCP エンドポイントから SIP エンドポイント
- 番号ダイヤルから URI ダイヤル
- シスコ スマート ソフトウェア ライセンシングおよび Cisco Smart Software Manager（Cisco SSM）によるライセンス管理への移行

移行が正常に行われるように、次のリソースを使用してすべての要件が満たされているかどうかを移行前に検証することを推奨します。

- *Cisco Collaboration Systems Release Compatibility Matrix*

  https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/CSR-Compatibility-Matrix.html

- *Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service*

  https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-device-support-tables-list.html

この検証は、サポートされるアップグレード パスを使用して移行が正常に行われるようにします。たとえば、アプリケーションの以前のソフトウェア バージョンの中には、正常に移行するために複数のアップグレードが必要になるものもあります。同様に、サーバ ハードウェアとソフトウェアの互換性を実現するために、複数ステップのハードウェアおよびソフトウェアのアップグレードを組み合わせる必要がある場合があります。

Cisco Collaboration システム製品の詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

https://www.cisco.com/c/en/us/solutions/collaboration/collaboration-systems-release/index.html

サポートされているすべてのシステム ハードウェアの一覧については、次の URL で入手可能なユニファイド コンピューティング製品のマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/servers-unified-computing/product-listing.html

この章の変更点

表 26-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 26-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Prime License Manager がシスコ スマート ソフトウェア ライセンシングで置き換えられました。	Cisco Smart Software Manager（26-9 ページ）	2018 年 3 月 1 日
Cisco Collaboration System Release（CSR）12.*x* のその他のマイナー アップデート。	この章の各項で説明	2018 年 3 月 1 日

ソリューションの共存または移行

これは重要な選択です。共存とは、通常、2 つ以上のシステムが長期間（たとえば 6 ヵ月を超える任意の期間）にわたって共存することを意味します。このシナリオでは、PBX やボイスメールなどの機能の透過性が重要な考慮事項になります。必要な機能の透過性レベルを実現するために、既存のシステムへの投資やアップグレードが必要となる場合があります。移行は、通常、短期間（6 ヵ月未満の任意の期間）で実施します。このシナリオでは、ユーザは、移行が「短い」期間で完了することを認識しているため、既存の機能の一部しか提供されないことを許容しやすくなります。この「短い」期間については、多くの場合、既存のシステム機能で十分であるため、一般的に、移行は共存よりもコストが少なくなります。

移行の前提条件

すべての管理者は、いずれのコラボレーション移行手順も実行する前に、IP インフラストラクチャが「コラボレーション対応」（冗長性、ハイ アベイラビリティ、電力消費、Quality of Service（QoS）、インライン パワー、イーサネット ポートなど）となっていることを確認する必要があります。詳細については、ネットワーク インフラストラクチャ（3-1 ページ）の章を参照してください。

Cisco Unified Computing System（UCS）に Cisco Unified Communications を初めて導入する場合、次の Web サイトから入手可能な『*Cisco UCS Site Preparation Guide*』に記載されているガイドラインに従ってください。

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/site-prep-guide/ucs_site_prep.html

特長や機能が移行時に保持または変換されて同等の動作が保証されるよう、主要なシステム要件を判断する上で、ユーザのビジネス ニーズは重要となります。サポートされる機能を理解するには、さまざまなデバイスとソフトウェアの機能とバージョンのリストが役に立ちます。通常、すべての要件（FAX/モデム、環境制御システムなど）が適切に特定および考慮されるように、何らかのサイト サーベイまたはユーザ サーベイを実施する必要があります。

Cisco Collaboration システムの移行

仮想化された Cisco Collaboration システムの移行方法としては、段階的な移行と並行カットオーバーの 2 種類が主となっています。Cisco Prime Collaboration Deployment を使うことで、移行プロセスを管理し、簡略化できます。

段階的な移行

この方法は通常、Cisco Unified Communications Manager（Unified CM）を中心とした、小規模なトライアルから始めます。カスタマーが Unified CM に慣れてきたら、管理者はユーザを新しい Unified CM リリースの実稼働システムへとグループ単位で移行、移動します。

並行カットオーバー

この方法の始め方は段階的な移行と同様ですが、カスタマーがトライアルの進行状況に納得した時点でカットオーバーする日時を決め、すべてのユーザを一度に新しい Cisco Collaboration システムに移行します。

並行カットオーバーには、段階的な移行に比べて次の利点があります。

- 並行カットオーバーを採用した場合、予期しない事態が発生したとき、最小限の労力で、基本的に以前の状態のままのシステムに戻すことができる、バックアウト計画を使用できます。たとえば、PBX からの段階的な移行の場合、着信 PSTN トランクを Cisco Collaboration システムから PBX に転送して戻すだけで、ユーザに対してサービスを復元できます。
- 並行カットオーバーの場合、システムがライブ トラフィックを伝送する前に、コラボレーション サービスの設定を確認できます。このシナリオは、コラボレーション サービスのカットオーバー前に任意の期間実行できるため、すべてのユーザ情報（電話機、ゲートウェイ、ダイヤル プラン、メールボックスなど）が正しく設定されていることを確認できます。

- 並行カットオーバーの場合、システムがライブ トラフィックを伝送する前に、Unified Communications サービスの設定を確認できます。このシナリオでは、Unified Communications サービスのカットオーバー前に任意の期間実行できるため、すべてのユーザ情報（電話機、ゲートウェイ、ダイヤル プラン、メールボックスなど）を適切に設定できます。
- 加入者がカットオーバー前に、自分の都合に合わせてコラボレーション サービスを試したり使用したりできるため、ゆとりを持ってトレーニングを実行できます。
- システム管理者は、「利害共同体」のために特別なプロビジョニングを行う必要はありません。段階的な移行では、コール ピックアップ グループ、ハント グループ、シェアド ラインなどの機能の完全性の維持を考慮する必要があります。こうした関連性は、並行カットオーバーでサービス全体を移行する場合は、簡単に調べることができます。

並行カットオーバーでは、サービスを提供する前にサービス全体を導入しなくてはならないため、最初の時点からコラボレーション サービス（サポートするインフラストラクチャを含む）に対する全額投資が必要であるという短所があります。一方、段階的な移行では、必要となったときにシステムの個々のコンポーネントを購入できます。このアプローチでは、完全に配置する前に、小規模な試用システムから開始できます。いずれかの方法が正しいというわけではなく、それぞれのカスタマーの環境と優先事項に応じて、最適なオプションが決まります。

Cisco Collaboration システムの移行例

PBX システムから Cisco Collaboration システムに移行する場合の、段階的な移行と並行カットオーバーの例を以下に 示します。

例 26-1　Cisco Collaboration システムへの段階的な移行

このアプローチは通常、主要な企業 PBX に接続された Cisco Collaboration システムの小規模なトライアルを伴います。使用するシグナリング プロトコルの選択は、必要な機能および実装コストによって決まります。Cisco Unified Communications Manager（Unified CM）では、通常の PSTN タイプ PRI や QSIG PRI、および H.323 と SIP をサポートしています。これらのオプションのうち、QSIG PRI は、通常、任意の 2 つのシステム間に最高レベルの機能透過性を提供します。

PSTN タイプ PRI は、基本的なコール接続および自動番号識別（ANI）を提供します。このプロトコルで発信者名情報がサポートされる場合もあります。このレベルの接続は、すべての PBX で使用できるため、最もコストがかからないオプションとされています。PBX が PRI を介してパブリック ネットワークに接続できれば、Unified CM を接続の「ネットワーク」側として設定することで、Unified CM にも接続できるからです。

PSTN タイプ PRI または QSIG では、段階的な移行のプロセスが似ています。ユーザをグループ単位で PBX から Unified CM に移動しますが、一度にグループを 1 つずつ移動して、移行を完了します。

23,000 人ほどのユーザが約 60 のビルに分散した Cisco San Jose キャンパスでは、この方法で Cisco Collaboration システムへの移行が行われました。週末ごとに 1 つのビルというペースで、開始から完了までかかった期間はわずか 1 年余りです。選択されたビル内のすべてのユーザが特定され、金曜日の夜に、それらのユーザの内線番号が PBX から削除されました。同時に、PBX ルーティング テーブルへの追加が行われ、これらの内線番号にダイヤルしたすべての人が正しい PRI トランクを通じてルーティングされ、Unified CM に配信されるようにしました。週末の間に、ユーザの新しい内線番号が Unified CM に作成され、新しい IP Phone が該当するオフィス ロケーションに届けられ、月曜日の朝には使用できる準備が整っていました。このプロセスは、すべてのユーザが移行されるまで、各ビルに対して繰り返されました。

例 26-2　Cisco Collaboration システムへの並行カットオーバー

このアプローチでは、すべての IP Phone およびゲートウェイが完全に設定および導入され、ユーザのデスク上には IP Phone と PBX 電話機の両方が同時に置かれます。このアプローチでは、システムをテストする機会だけでなく、新しい IP Phone にユーザが慣れる機会を提供します。発信専用のトランクも Cisco Collaboration システムに接続できるため、ユーザは新しい IP Phone を使用して外線電話と内線電話のいずれも発信することができます。

Cisco Collaboration テレフォニー システムが完全に導入された時点で、着信 PSTN トランクを PBX から IP テレフォニー ゲートウェイに移動して新しいシステムを完全なサービスに移行する日時を選択できます。Cisco Collaboration システムの運用に確信が持てるまで PBX をそのまま残しておき、確信できた時点で PBX の使用を停止することもできます。

Cisco San Jose キャンパスのボイスメール サービスは、4 つの Octel 350 システムによって 23,000 人ものユーザに提供されていました。Cisco Unity サーバがインストールされ、ユーザのメールボックスが設定されました。ユーザは、新しいアクセス番号をダイヤルして自分の Cisco Unity メールボックスにアクセスできます。これにより、自分の名前とグリーティングを録音し、また新しいテレフォニー ユーザ インターフェイス（TUI）に慣れることができます。約 2 週間後の金曜日の夜、Unified CM 一括管理ツール（BAT）による更新が実行され、話中転送番号と無応答転送番号（CFB/CFNA）、および Unity システムへのすべてのユーザの Messages ボタンの宛先番号が変更されました。月曜日の朝には、Cisco Unity によるサービスがユーザに提供されていました。Octel 350 システムは 1 ヵ月間そのまま残されたので、ユーザは使用停止までに同システムに残っていたすべてのメッセージに対応することができました。

Cisco Collaboration システムの移行の概要

Cisco Collaboration システムの移行は 2 つの方法いずれでも可能であり、どちらか一方の方法が正しいということはありません。しかし、並行カットオーバーの方法が最適である場合がほとんどです。シスコは、Unified CM システムと PBX システム間の相互運用性テスト専用の実験施設を持っています。現在お使いのシステム アーキテクチャやアプリケーションは、その対象である場合とそうでない場合があります。シスコはこれらのテスト システムとその相互運用性およびエンドユーザ機能について文書化しています。こうしたドキュメントはインストールや移行プロセスに大いに役立ちます。このテストの結果は、次の Web サイトに公開されているアプリケーション ノートとして入手できます。

https://www.cisco.com/c/en/us/solutions/enterprise/interoperability-portal/index.html

アプリケーション ノートは頻繁に更新され、この Web サイトには新しいドキュメントが継続的に追加されています。この Web サイトを頻繁に確認して、最新情報を入手してください。

Cisco Prime Collaboration Deployment は、MCS サーバ上で稼働する Cisco Collaboration システムから仮想化環境で稼働する同システム、あるいは以前のバージョンから Cisco Collaboration システム リリース 12.*x* へ移行する際に使用される主要なツールです。

中央集中型の導入

Cisco Collaboration システムの集中型導入を選択した企業は、次の 2 つのオプションから選択できます。

- 外側から開始し、中央サイトに向かって内側に進める（つまり、最も小さいサイトから最も大きいサイトへ）。
- 中央サイトから開始し、エッジに向かって外側に進める。

ほとんどのカスタマーは、次の利点があるため、最初のオプションを選択します。

- すべての Cisco Collaboration サービスの導入が完了した後、サービスをリモート拠点に導入する前に小規模なトライアルが実施できる。
- Cisco Collaboration サービスを 1 拠点ずつ導入し、以降の拠点は適宜移行できる。
- Cisco Collaboration のコア サービスが中央サイトに配置された後の実施コストはこのオプションが最も低い。
- IT スタッフは、中央サイトに移行する前に、小規模サイトの移行時に貴重な経験を積むことができる。

リモート サイトは、並行カットオーバーの方法で移行するべきですが、中央サイトの移行は、並行または段階的のいずれの方法でも可能です。

どの Cisco Collaboration サービスを最初に移行するか

この選択は、カスタマーの個別のビジネス ニーズに大きく依存します。Cisco Collaboration ソリューションでは、個々のサービスのほとんどを他のサービスとは独立して導入できます。たとえば、IP テレフォニーとボイス メッセージングは互いに独立して導入できます。

この機能により、大幅な柔軟性がカスタマーにもたらされます。あるカスタマーが、ボイスメール システムのサポートが終了したことによって、顧客満足度の低下につながるさまざまな問題を抱えているとします。多くの場合、Cisco Unity Connection は現在使用している PBX と併用して導入、または統合できるため、この問題は解決できます。新しいボイスメール システムが適切に運用できるようになった後、次のコラボレーション サービス、つまり IP テレフォニーに取りかかることができます。

Unified CM へのビデオ デバイスの移行

Cisco Unified Communications Manager（Unified CM）によって制御されているビデオ エンドポイントは、ビデオ中心の Cisco Video Communications Server（VCS）で使用できる機能の一部のみをサポートします。一方で、Cisco Unified CM に移行することで、単一の呼制御エージェントのもと、統合ダイヤル プランなど、さまざまな機能が統一されるという利点もあります。以下に、Unified CM へのビデオ エンドポイントの移行についてのガイドラインを示します。

- 技術的機能（コーデックやコンテンツ共有機能など）が完全にサポートされ、移行によって何らかの機能が失われることがないことを確認します。
  - 段階的な移行ではしばらくの間、既存の電話機はバックアップとして残したまま、新しいデバイスに慣れることができます。このため、この目的を達成するにはこの移行方法が最も一般的です。
  - ユーザが優れたエクスペリエンスを得られるように、十分なネットワーク キャパシティを提供します。ビデオ解像度の向上に伴い、音声のみのコールと比較して高い帯域幅が必要になります。
  - ダイヤル プランと関連するゲートウェイ（ISDN H.320 ゲートウェイなど）、およびアプリケーション サーバ（会議サーバおよびブリッジなど）を移行します。
- エンドポイントについては、エンドポイントのバージョンのアップグレードを伴う場合や、一部のデバイスで異なるライセンスが必要な場合は、必要な追加ライセンスを検討します。
  - システム管理ツールは、多数のエンドポイントがある場合や、エンドポイントにより多くのバックエンド管理やサポートが必要な場合に非常に役立ちます。

組織はデバイスの種類、実行可能性、および必要なタスクの範囲を評価して、Unified CM へのビデオ デバイスの移行が可能な限り効率的かつ効果的に行われるようにできます。

Cisco Collaboration システム リリース 12.*x* へのライセンス移行

Cisco Collaboration システム リリース 12.*x* では、シスコ スマート ソフトウェア ライセンシングにより、ライセンスを一元管理できるようになっています。12.*x* リリースのライセンス モデルは、以前のシステム リリースで使用されていた Prime License Manager ではなく、Cisco Smart Software Manager（SSM）で管理されます。

Cisco Unified Communications またはコラボレーション ソリューションを導入済みのお客様は Cisco Global Licensing Operations（GLO）プロセスを使用して既存のライセンスをシスコ スマート ソフトウェア ライセンシングに移行できます。

Cisco Global Licensing Operations（GLO）によるライセンスの移行

Cisco ソフトウェア ライセンシング プロセスおよび機能に熟練したユーザ向けのセルフサービス オプションが用意されています。このセルフサービス オプションは Product License Registration ツールより利用できます。

https://tools.cisco.com/SWIFT/LicensingUI/migrateDisplayProducts

（注）　上記のリンクで Product License Registration ツールにアクセスするには、有効な Cisco.com のログイン ID とパスワードが必要です。

また、Support Case Manager https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case を使用してケースを開くことで、Cisco Global Licensing Operation（GLO）チームのサポートを受けることもできます。

ライセンスを移行する場合は必ずこのセクションで示すガイドラインに従ってください。

ライセンス移行プロセスが簡素化されて、Cisco Smart Software License Manager への移行が大幅に容易になりました。Cisco Collaboration システム リリース 12.*x* へのアップグレードを希望するカスタマーは、移行に関するあらゆるニーズに関して、Cisco Global Licensing Operations（GLO）チームに直接問い合わせることできます。GLO がリクエストを処理して、組織の Cisco スマート アカウントにライセンスを転送します。シスコはライセンスの付与対象となるリリース 12.*x* ユーザの数を反映するべく、現行のソフトウェア サービス契約書の製品記録を調整します。

移行するシステムに未使用の製品アクティベーション キー（PAK）がある場合は必ず登録してください。以前のライセンス モデルで拡張を考慮していた場合は、今回の移行でも考慮してください。たとえば、12.*x* よりも前のリリースのクラスタを保持しつつ、残りを 12.*x* にアップグレードする必要がある場合、GLO チームへのライセンス移行リクエストに、移行する必要があるユーザの正確な数と、現状のままにするユーザの正確な数を明記してください。

必ずすべてのライセンスのニーズを詳しく分析して、リクエストでニーズを明確に伝えるようにしてください。DLU を含む 9.*x* よりも前のリリースからの移行の場合、DLU は移行後は「失効」状態となるため、古いスキーマに戻すことはできません。

(注)　ライセンス プロセスは新しいリリースごとに変更される可能性があります。必ずシスコの GLO チームにプロセスを確認してから license@cisco.com にライセンス リクエストを送信してください。

ライセンス移行に関する GLO への問い合わせは、以下の段階で行うことができます。

アップグレード前

GLO に次の情報を提供する必要があります。

- 9.*x* よりも前のシステムからアップグレードする場合、Cisco Unified Communications Manager パブリッシャ ノードに対して実行した License Count Utility（LCU）の出力を使用します。
- Cisco Unified Communications Manager パブリッシャ ノードの MAC アドレスを提供します。可能であれば、以前のパブリッシャまたはライセンスの MAC アドレスも提供します。

アップグレード後

GLO に次の情報を提供する必要があります。

- 9.*x* よりも前のシステムからアップグレードする場合、Cisco Unified Communications Manager パブリッシャ ノードに対して実行した License Count Utility（LCU）の出力を使用します。
- Cisco Unified Communications Manager パブリッシャ ノードの MAC アドレスを提供します。可能であれば、以前のパブリッシャまたはライセンスの MAC アドレスも提供します。
- 契約書を更新するためのサイト情報（名前の置換情報、市、州、国）。
- （オプション）ライセンスおよびソフトウェアサポート契約更新の送信先となる電子メール アドレス。
- （オプション）User Connect License（UCL）利用のカスタマーの場合、カスタマーが希望する未使用の DLU の割り当て方法。

(注)　9.*x* よりも前のシステムを Collaboration システム リリース 12.*x* に移動する場合、カスタマーは未使用の DLU を使用するか、移行時に破棄するかを決定する必要があります。DLU を破棄した場合、払い戻しはありませんが、その後のサービス料金に対して割引を受けられます。現行の契約書上の Cisco Unified Communications Software Subscription（UCSS）ユーザとの違いを確認し、更新時に UCSS および Essential Operate サービス（ESW）の料金に変更がある場合はその金額を見積もります。

移行時にカスタマーは既存のライセンスの使用方法を選択できます。次のオプションがあります。

- ライセンスの数量とタイプを保持する。
- ライセンス数を減らし、タイプを変更する（払い戻しなし）。
- DLU を変換することでライセンス数を増やす。

アップグレード プロセスが完了すると、情報がロックされ、今後のカスタマーの権利として記録されます。これ以降、ライセンス移行情報が変更されることはありません。

詳細については、次のマニュアルを参照してください。

- 『*Cisco Smart Software Licensing Overview*』（以下のリンク先から入手可能）

  https://www.cisco.com/go/smartlicensing

- 最新バージョンの『*System Configuration Guide for Cisco Unified Communications Manager*』（以下のリンク先から入手可能）に記載されているシスコ スマート ソフトウェア ライセンシングに関する情報

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

Cisco Smart Software Manager

Cisco Smart Software Manager（Cisco SSM）では現在、以下のシスコ コラボレーション アプリケーションをサポートしています。

- Cisco Unified CM
- Cisco IM and Presence サービス
- Cisco Unity Connection
- Cisco Emergency Responder

Cisco Smart Software Manager の詳細については、以下のリンク先から入手可能なマニュアルを参照してください。

https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html

Cisco Prime Collaboration Deployment を使用した物理サーバから仮想マシンへの移行

Cisco Prime Collaboration Deployment は、管理者がレガシーの Cisco Unified CM および Cisco IM and Presence サービスから Cisco Collaboration システム リリース 12.*x* の仮想化環境への移行を実行できるようにする管理アプリケーションです。Cisco Prime Collaboration Deployment はクラスタを移行してデータ移行を処理し、実稼働（ソース）クラスタにほとんど影響を与えずにすべての新しい VMware ESXi ホストに 12.*x* リリースをインストールできます。以前の移行方法は、「サーバ リカバリ」を行う Disaster Recovery System を使って、アップグレードを行った後にバックアップから復元するという、多くの手順を要するものでした。Cisco Prime Collaboration Deployment では、直接移行することができます。

Cisco Prime Collaboration Deployment を使って、以下を行うことも可能です。

- Unified Communications ソフトウェア（8.6.1 以降のリリース）のアップグレード
- クラスタ（8.6.1 以降のリリース）への Cisco Option Package（COP）ファイル（ロケールまたはデバイス パック）のインストール
- スイッチのバージョン
- Reboot
- 既存のクラスタ上の IP アドレスまたはホスト名の変更
- 新しい Unified CM または IM and Presence クラスタのインストール

Cisco Prime Collaboration Deployment 移行の種類

Cisco Prime Collaboration Deployment は 2 種類の移行をサポートします。

- 単純な移行（26-10 ページ）

  単純な移行では、クラスタ内の各ノードは元のホスト名、IP アドレスなどのネットワーク設定をすべて保持します。

- ネットワークによる移行（26-11 ページ）

  ネットワーク移行では、クラスタ内の 1 つ以上のノードでホスト名や IP アドレスなど、Collaboration Applications に必要なネットワーク設定が変更されます。

Cisco Prime Collaboration Deployment 移行の前提条件

- VMware ESXi Hypervisor をインストールしていること。
- Cisco Prime Collaboration Deployment 仮想マシン（仮想アプライアンスとして提供）を導入していること。
- Cisco Collaboration アプリケーション用の Open Virtualization Archive（OVA）ファイルをダウンロードし、OVA を使ってインストール先となる仮想マシンを作成していること。
- ターゲット リリース用の Cisco ISO イメージをダウンロードし、Cisco Prime Collaboration Deployment にアップロードしていること。
- 仮想マシンに Cisco Collaboration システム リリース 12.*x* ノードをインストールしていること。

単純な移行

この移行方法では、移行中に IP アドレスやホスト名が変更されません。以下に Cisco Prime Collaboration Deployment における移行タスク設定で推奨される手順を示します。この手順に従うことで、高い可用性を提供しながら移行を実現できます。

Cisco Prime Collaboration Deployment はまずすべての既存ノードのデータをエクスポートします。次に既存のパブリッシャを停止し、仮想マシンとして稼働する新しいパブリッシャをインストールして、パブリッシャのデータをインポートします。

パブリッシャの移行が完了したら、Cisco Prime Collaboration Deployment はクラスタの TFTP ノードとバックアップ コール処理ノードを移行します。まず、既存の TFTP ノードとバックアップ コール処理ノードを停止します。次に、Prime Collaboration Deployment は新しい TFTP ノードとバックアップ コール処理ノードをインストールし、バックアップ データをインポートします。

バックアップ コール処理ノードの移行が完了すると、Cisco Prime Collaboration Deployment の移行タスクが一時停止します。ここで管理者は、Unified Communications Manager グループ内の順序を変更して、またはデバイス プールを使用して、すべての電話機がバックアップ コール処理ノードに再登録されるよう設定します。

最後に、Cisco Prime Collaboration Deployment はプライマリ呼処理ノードを移行します。これが完了すると、電話機をプライマリ呼処理サーバに再登録できます。

詳細については、以下のリンク先から入手可能な最新バージョンの『*Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service*』を参照してください。

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

ネットワークによる移行

Cisco Prime Collaboration Deployment は、ネットワーク設定の、サーバの IP アドレスやホスト名などのパラメータの変更が必要な移行でも使用できます。移行元となる Unified CM クラスタがリリース 8.*x* 以降を搭載している場合、Bulk Certificate Management のエクスポート、統合、インポートの各機能を使って、個々の電話機の ITL を手動で削除することなく電話機の初期信頼リスト（ITL）を移行中に更新できます。

詳細については、次のサイトで入手可能な『*Cisco Prime Collaboration Deployment Administration Guide*』の最新版を参照してください。

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

Cisco VCS から Unified CM へのビデオ エンドポイントの移行

Cisco TelePresence Video Communication Server（VCS）から Cisco Unified CM に移行したビデオ エンドポイントでは、ビデオ中心の VCS 環境で使用できる機能の一部しかサポートされない場合があります。一方で、Cisco Unified CM に移行することで、単一の呼制御エージェントのもと、統合ダイヤル プランなど、さまざまな機能が統一されるという利点もあります。Cisco Unified CM へのビデオ エンドポイントの移行は、SIP および SCCP エンドポイントの両方をサポートしますが、シスコはすべてのカスタマーに、SIP エンドポイントに移行することを推奨します。SCCP はサポートされてはいますが、Unified Communications ベンダーとカスタマーの両方で SIP の人気が高まり、SIP の機能も拡張されています。このため、SIP は Unified Communications の新しい標準、そして推奨される選択肢となっています。

ビデオ エンドポイントを SIP エンドポイントとして Unified CM に移行する際は、次の推奨事項を考慮してください。

- 技術的機能（コーデックやコンテンツ共有機能など）が完全にサポートされ、移行によって何らかの機能が失われることがないことを確認します。
- ユーザが優れたエクスペリエンスを得られるように、十分なネットワーク キャパシティを提供します。ビデオ解像度の向上に伴い、音声のみのコールと比較して高い帯域幅が必要になります。
- ダイヤル プランと関連するゲートウェイまたはトランク（ISDN H.320 ゲートウェイなど）、およびアプリケーション サーバ（会議サーバおよびブリッジなど）を移行します。
- エンドポイントについては、エンドポイントのバージョンのアップグレードを伴う場合や、一部のデバイスで異なるライセンスが必要な場合は、必要な追加ライセンスを検討します。
- システム管理ツールは、多数のエンドポイントがある場合や、エンドポイントにより多くのバックエンド管理やサポートが必要な場合に非常に役立ちます。
- カスタマーは、Unified CM へのビデオ デバイスの移行が可能な限り効率的かつ効果的に行われるようにするため、デバイスの種類、実行可能性、および必要なタスクの範囲を評価する必要があります。

H.323 から SIP への移行

H.323 は、音声、ビデオ、およびデータ会議など、IP ネットワーク上でのマルチメディア通信の要件を十分に理解した上で設計されています。また、これらの機能を実行するための統合システム全体を定義しています。SIP の導入は増加しているものの、H.323 はビデオ会議分野での歴史が長いため、今でもビデオ会議のエンドポイントに最も広く導入されているプロトコルです。多くの組織が、H.323 の導入に多大な労力とコストを費やし、その結果使用環境への適合方法を理解しています。

SIP は実装しやすく、ビデオ市場での人気が高まりつつあります。多くの組織がシグナリング プロトコルの変更に苦慮する中、業界は進化を続け、SIP はその使いやすさと他のベンダー製品と統合可能なことから人気を博しています。Cisco Collaboration システムは H.323 と SIP の両方をサポートしていますが、シスコは SIP を推奨しています。H.323 に類似した一連のサービスを提供し、かつ H.323 よりもはるかにシンプルで柔軟性に富み、拡張性にも優れているためです。

H.323 から SIP へのトランクの移行

Cisco Unified CM は SIP と H.323 の両方のクラスタ間トランクをサポートしています。多くの場合、SIP と H.323 のどちらを使用するかは、それぞれのプロトコルが提供する独自の機能によって決定されます。エクスペリエンス、相互運用性の容易さ、特長、他のさまざまな製品との機能性など、多くの要因がカスタマーの選択に影響します。Cisco Collaboration システムは H.323 トランクと SIP トランクの両方をサポートしますが、シスコはすべての導入において SIP トランクを使用することを推奨します。SIP トランクは相互運用がしやすく、他にも H.323 トランクでは利用できない特長や機能を提供しているためです。

H.323 および SIP トランクの機能と操作の詳細については、Cisco Unified CM トランク（6-1 ページ）の章を参照してください。

H.323 から SIP へのゲートウェイの移行

Cisco Unified Communications Manager（Unified CM）は、ゲートウェイで SIP と H.323 の両方のプロトコルをサポートします。シスコのゲートウェイは、Cisco Collaboration システムを公衆電話交換網（PSTN）、従来型の PBX、またはサードパーティ製の外部導入ソリューションに接続するための複数の方法を提供します。シスコは音声とビデオ両方のゲートウェイを、エントリレベルからハイエンドまで、両方のプロトコルを完全にサポートする形で提供していますが、すべてのコール シグナリングにおいて SIP を選択することを強く推奨します。SIP は Cisco Collaboration の音声およびビデオ製品のポートフォリオ全体との相互運用性に優れているためです。

H.323 および SIP ゲートウェイの機能と操作の詳細については、ゲートウェイ（5-1 ページ）の章を参照してください。

SCCP から SIP へのエンドポイントの移行

Session Initiation Protocol（SIP）の標準シグナリングに関する一般的な推奨事項を考慮すると、同等の機能と規格適合の実現に向けて、管理者は既存の SCCP IP エンドポイントを SIP IP エンドポイントに移行することを検討する必要があります。既存の SCCP IP Phone モデルが SIP ロードをサポートする場合、管理者は Cisco Unified CM Bulk Administration Tool（BAT）を使用して移行できます。

Unified CM BAT は、SCCP 電話機から SIP 電話機への移行における推奨ツールです。SIP は、業界の普遍的なプロトコル標準です。Unified CM BAT には、電話機を SCCP から SIP に移行するワークフローがオプションとして提供されています（[一括管理（Bulk Administration）] > [電話（Phones）] > [電話機の移行（Migrate Phones）] > [SCCP から IP（SCCP to SIP）]）。このワークフローを使って既存の SCCP 電話機についてのレポートを作成できます。移行する SCCP 電話機を選択した後、SIP に移行するジョブは、すぐに実行するか、後で実行するようスケジュールできます。SCCP から SIP への移行では電話機レポート内の SIP 固有のデフォルト値のみが移行され、テンプレート内の他の値は移行されません。SCCP から SIP への電話機の移行は、移行自体が電話機をリセットするため、手動でリセットする必要はありません。

移行詳細と具体的な手順については、以下のリンク先から入手可能な最新バージョンの『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

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

SIP URI ダイヤルおよび電話番号

SIP Uniform Resource Identifier（URI）は、ユーザにコールを転送する際のアドレッシング スキーマです。URI とは、本質的にはユーザに割り当てられた電話番号のエイリアスです。SIP URI は電子メール アドレスに似ており、次の形式で記述されます。

sip:*x*@*y*:*Port*

ここで、*x* はユーザ名、*y* はホスト（ドメインまたは IP）です。

次に例を示します。

username@cisco.com または users-directorynumber@cisco.com

URI は、@ 記号で区切られたユーザ名とホスト アドレスで構成される英数字の文字列です。Cisco Unified CM は次のディレクトリ URI の形式をサポートしています。

- *ユーザ名@ ドメイン名*（joe@cisco.com など）
- *ユーザの電話番号@ ドメイン名*（9728135555@cisco.com など）

SIP 要求に user=phone タグがある場合、SIP URI は数値型の SIP URI として解釈され、Unified CM は SIP URI のユーザ部分を電話番号と見なします。user=phone がない場合は、発信側デバイス（エンドポイントまたはトランク）の SIP プロファイルのダイヤル ストリング解釈の設定に従います。この設定では、Unified CM が数値型 SIP URI として許容する文字セット（0 ～ 9、*、#、+ およびオプションとして A ～ D）を定義するか、またはディレクトリ URI としての解釈を強制します。

（注） ポートを指定しない場合、デフォルトの SIP ポート（5060）が使用されます。SIP ポートをデフォルトから変更した場合は、SIP URI で指定する必要があります。

以下に Unified CM およびサポートされるエンドポイントについての、URI および電話番号（DN）の考慮事項を示します。

- DN は、エンドポイント デバイスのプライマリ ID です。
- DN には URI が割り当てられます。各 DN は最大 5 つの URI をサポートできます。
- デバイスは常に DN と共に登録されます。

- URI を使って、Cisco Unified IP Phone 9900 シリーズ、Cisco Unified IP Phone 8961、Cisco Jabber、Cisco DX シリーズ、およびサードパーティのエンドポイントから電話をかけることができます。
- プライマリ URI は、Unified CM の LDAP から直接同期できます。

詳細については、エンドポイント SIP URI の実装（14-83 ページ）の項を参照してください。

仮想 Unified CM と USB 対応

オーディオ ソース ファイルからの保留音（MoH、ユニキャストまたはマルチキャストを使用）はサポートされますが、仮想サーバで USB オーディオがサポートされていないため、Unified CM への固定またはライブのオーディオ ソースの接続はサポートされていません。以下に、仮想 Unified CM サーバ ノードによるライブ オーディオ ソース MoH についてのガイドラインを示します。

- Unified CM では USB オーディオ デバイスからのライブまたは固定オーディオ ソース フィードはサポートされません。
- 代替手段として、Cisco IOS ルータを使ってマルチキャスト MoH フィードを固定またはライブのオーディオ ソースから提供することはできます。これを行うには、Survivable Remote Site Telephony（SRST）または Enhanced SRST を使って Cisco IOS ルータにマルチキャスト MoH を設定する必要があります。
- Cisco IOS ルータがエンドポイントやゲートウェイに音声をストリーミングするには、ネットワークでマルチキャストが有効になっている必要があります。

Cisco UCS B シリーズ ブレード サーバおよび C シリーズ ラックマウント サーバは、シリアル ポート、Video Graphics Array（VGA）モニタ ポート、および 2 つの Universal Serial Bus（USB）ポートを提供するローカル キーボード、ビデオ、およびマウス（KVM）ケーブル接続をサポートしますが、Unified CM VMware 仮想アプリケーションはこれらの USB ポートおよびシリアル ポートにアクセスできません。よって、Unified CM では Simplified Message Desk Interface（SMDI）連携を可能にする Cisco Messaging Interface（CMI）サービスや、オーディオ カードやフラッシュ ドライブを使用したこれらのサーバへのライブ MoH オーディオ フィードを可能にする固定 MoH オーディオ ソース連携がサポートされなくなっています。

オンプレミスの Cisco IM and Presence Service の移行

Cisco MCS 物理サーバ上で稼働する既存の Cisco IM and Presence 導入をリリース 12.*x* にアップグレードするには、仮想化環境への移行が必要です。この移行を促進するには Cisco Prime Collaboration Deployment を使用します。

ネットワーク管理

改訂日：2018 年 3 月 1 日

ネットワーク管理は、さまざまなツール、アプリケーション、および製品によって構成され、ネットワーク システム管理者による新規および既存ネットワーク配置のプロビジョニング、運営、モニタリング、および保守を支援します。ネットワーク管理者は、ネットワーク デバイスを配置および設定する場合、また、ネットワーク インフラストラクチャやルータ、サーバ、スイッチなどのコンポーネントの正常性を運用、モニタリング、および報告する場合に、さまざまな課題に直面します。ネットワーク管理は、システム管理者による各ネットワーク デバイスとネットワーク アクティビティのモニタを支援し、問題をタイムリーに特定および調査することで、性能と生産性を高めるのに役立ちます。

リッチ メディアとデータのコンバージェンスにより、統合管理の必要性は以前よりもさらに強まっています。Cisco Prime Collaboration（Prime Collaboration）は、Cisco Unified Communications と TelePresence システムの試験、展開、およびモニタリングを支援する統合ツール セットを提供します。Prime Collaboration は、さまざまな管理段階を実装して、音声、ビデオ、コンタクト センター、リッチ メディア アプリケーションなどの Cisco Unified Communications アプリケーションの性能と可用性を戦略的に管理します。ネットワーク管理は一般的に、計画（Plan）、設計（Design）、実装（Implement）、および運用（Operate）（PDIO）の各段階からなります。表 27-1 に、PDIO 段階と各段階に含まれる主なタスクを示します。

表 27-1　ネットワーク管理の段階およびタスク

計画および設計	実装	運用
Cisco Unified Communications 機能のネットワーク インフラストラクチャの能力を査定します。たとえば、全体的なコール品質を予測します。 Cisco Unified Communications をサポートするようにネットワークを準備します。 ネットワーク管理のベスト プラクティスを分析します。	Cisco Unified Communications を配置およびプロビジョニングします。たとえば、ダイヤル プラン、パーティション、ユーザ機能などを設定します。 既存インフラストラクチャの機能で Cisco Unified Communications をサポートできるようにします。	ユーザ、サービス、IP Phone などの変更を管理します。 運用、キャパシティ プランニング、エグゼクティブ サマリーなどのレポートを生成します。 ユーザ エクスペリエンスを監視および報告します。たとえば、音声品質をモニタするセンサーを使用します。 ネットワーク障害、デバイス障害、コール ルーティング問題などの問題をモニタおよび診断します。

この章では、Cisco Unified Communications Management の実装段階と運用段階に適用される次の管理ツールおよび製品の設計ガイドラインについて説明します。

- Cisco Prime Collaboration は、Unified Communications と TelePresence サービスの初期展開、進行中の運用アクティベーションのプロビジョニングを管理します。Cisco Prime Collaboration は、Cisco Unified Communications システム全体の予防的および反応的な診断を備えた包括的なモニタリング機能を提供します。また、Cisco Unified Communications システムのモニタリング、評価の音声品質の信頼性が高い方式を提供します。詳細については、次の URL から入手可能な関連製品のマニュアルを参照してください。

  https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html

- Cisco TelePresence Management Suite（TMS）は、リモート システムを含む、Telepresence ビデオ会議ネットワークの可視性と集中制御を提供します。詳細については、次の URL から入手可能な関連製品のマニュアルを参照してください。

  https://www.cisco.com/c/en/us/products/conferencing/telepresence-management-suite-tms/index.html

Cisco Unified Communications Manager（Unified CM）でサポートされているソフトウェア バージョンについては、以下のリンク先から入手できる最新バージョンの『*Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-device-support-tables-list.html

この章の変更点

表 27-2 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 27-2　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Prime License Manager がシスコ スマート ソフトウェア ライセンシングで置き換えられました。	シスコ スマート ソフトウェア ライセンシング（27-23 ページ）	2018 年 3 月 1 日
その他の小さな修正および更新	この章の各項で説明	2018 年 3 月 1 日

Cisco Prime Collaboration

Cisco Prime collaboration は、基礎となるトランスポート インフラストラクチャを含めた Cisco Collaboration システムのための、音声およびビデオ ネットワークの包括的な監視と診断機能を提供します。Prime Collaboration は統合アプリケーションであり、ビデオの導入を音声と分けて管理する手間を省きます。Prime Collaboration Assurance と Prime Collaboration Provisioning の 2 つの個別のアプリケーションとして提供され、個別の仮想マシンにインストールされます。Prime Collaboration は Standard モードと Advanced モードの 2 つのモードで使用可能です。

Prime Collaboration Assurance アプリケーションでは次のことが可能です。

- Cisco Collaboration アプリケーションのエンドツーエンドのサービス モニタリング。
- Cisco TelePresence システムと電話機に対するリアルタイムのサービス トラブルシューティングおよび診断。
- ビデオ サービス準備状況の評価
- Cisco IP サービス レベル契約（IP SLA）と Video SLA Assessment Agent（VSAA）を使用した診断テスト。
- 音声およびビデオ システムのサービス レベル レポートおよびインベントリ レポート。

（注）　Prime Collaboration Assurance Advanced には Prime Collaboration Analytics も含まれます。Prime Collaboration Analytics ライセンスを購入した場合、Prime Collaboration Analytics ダッシュボードにアクセスできます。Prime Collaboration Analytics では、ネットワーク内のトラフィックのトレンド、テクノロジー導入のトレンド、過剰に利用されているリソースまたは十分に利用されていないリソースを確認できます。また、断続的および繰り返し発生するネットワークの問題を追跡し、サービス品質の問題に対処できます。

Prime Collaboration Provisioning アプリケーションでは次のことが可能です。

- サブスクライバ（個々の電話、ボイスメール、またはその他のサービスの所有者）向けに注文する標準サービス（電話機、回線、ボイスメールなど）。
- 一貫した方法で Cisco Unified Communications の音声インフラストラクチャを自動設定する、設定テンプレート。
- 既存の Cisco Unified Communications ネットワークへのプロビジョニング アプリケーションの簡単な追加。
- 電話機のユーザを移動、追加、削除、変更するための簡略化したポリシードリブンの Day 2 プロビジョニング インターフェイス
- エンド ユーザが個人のオプションをすばやく簡単に変更できる、セルフケア機能

Prime Collaboration の利点と主な機能、配置のガイドライン（ホワイト ペーパー）の詳細については、次の URL から入手可能な Cisco Prime Collaboration のマニュアルを参照してください。

https://www.cisco.com/go/primecollaboration

フェールオーバーおよび冗長性

Prime Collaboration は現在フェールオーバーをサポートしていません。ただし、NIC チーミング対応のデュアル イーサネット ネットワーク インターフェイス カード（NIC）を搭載したサーバ プラットフォームに配置した場合は、ネットワーク耐障害性をサポート可能です。この機能は、サーバを 2 枚の NIC、つまり 2 本のケーブルでイーサネットに接続できるようにするものです。NIC チーミングは、障害の発生したポートから正常なポートに作業負荷を転送することによって、ネットワークのダウンタイムを防止します。NIC チーミングは、ロード バランシングやインターフェイス速度向上のためには使用できません。

Prime Collaboration Assurance は VMware vSphere レプリケーションによって地理的な冗長性を提供します。リモート サイトでのみ VMware アクティベーションが必要です。

Cisco Prime Collaboration サーバのパフォーマンス

Prime Collaboration は仮想環境でのみ動作し、コンポーネントごとに最低 1 台の仮想マシンが必要です。Assurance と Provisioning が必要な場合は、2 台の仮想マシン（それぞれに各 1 台）が必要です。特定のシステムの要件およびキャパシティ情報については、以下のリンク先から入手できる最新バージョンの『*Cisco Prime Collaboration Provisioning Install and Upgrade Guide*』を参照してください。

https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.html

シスコ コラボレーションおよびネットワーク管理アプリケーションのネットワーク インフラストラクチャ要件

ネットワーク内のドメイン ネーム サービス（DNS）でデバイスの IP アドレスに対してリバース ルックアップを実行して、デバイスのホスト名を取得できるようにすることを強く推奨します。DNS を使用しない場合は、IP アドレスからホスト名への解決にホスト ファイルを使用することもできます。

ネットワーク タイム プロトコル（NTP）を実装して、ネットワーク デバイスのクロックをネットワーク タイム サーバまたはネットワーク対応クロックに同期できるようにする必要があります。NTP によって、ネットワーク中のデバイスのすべてのログ、トラップ、ポーリング、およびレポートのタイムスタンプが正確であることが保証されるため、NTP はネットワークの運用および管理に不可欠なネットワーク サービスです。

ネットワーク内の Cisco Discovery Protocol（CDP）で適切なモニタリングを確実にできるようにする必要があります。Prime Collaboration の自動デバイス検出は、CDP テーブルに基づきます。CDP の代わりに ping スイープを使用することもできますが、ping スイープを使用して検出された IP Phone は「管理対象外」として報告されます。また、簡易ネットワーク管理プロトコル（SNMP）もネットワーク デバイス上で有効にして、Prime Collaboration が設定済みのポーリング間隔でネットワーク デバイスの情報を取得したり、管理対象デバイスによって送信されたトラップ通知で警告および障害を受信できるようにする必要があります。

Cisco Unified Communications ネットワークの詳細については、ネットワーク インフラストラクチャ（3-1 ページ）の章を参照してください。

Assurance

Cisco Prime Collaboration Assurance は、一貫性のある高画質ビデオと音声のコラボレーション体験を確実にユーザに提供するために役立つ、一連のモニタリング、トラブルシューティング、レポートの機能を備えた、包括的なビデオおよび音声サービス保証管理システムです。Prime Collaboration Assurance は Standard と Advanced の 2 つのモードで使用可能です。

Prime Collaboration Assurance は、アプリケーションと基盤となるトランスポート インフラストラクチャの統合保証管理を可能にするすべての機能を備えています。これには、Cisco TelePresence ソリューションと Unified Communications システム全体のリアルタイム モニタリングやトラブルシューティングが含まれます。

Prime Collaboration Standard は、Unified Communications と TelePresence コンポーネントの管理に役立つ基本的な保証機能を提供します。機能は次のとおりです。

- ボイスメールと IM and Presence を含む Unified Communications コンポーネントのサポート
- Unified Communications のコア コンポーネントの障害モニタリング（Cisco Unified CM および Cisco Unity Connection）
- Unified Communications のコア コンポーネントの期間トレンドを表示する、設定済みのカスタマイズ可能なパフォーマンス メトリックス ダッシュボード
- Cisco TelePresence Video Communication Server（VCS）を含む、TelePresence コンポーネントのサポート
- Unified Communications コンポーネントのサービスアビリティ ページのコンテキスト相互起動
- シングルレベルのロールベース アクセス コントロール（RBAC）

Prime Collaboration Standard には、Unified Communications および TelePresence コンポーネントの管理に役立つ次の機能が含まれています。

- デバイス インベントリ管理

  Cisco Unified Communications Manager（電話機および TelePresence エンドポイント）、Cisco TelePresence VCS、Cisco TelePresence Management Suite（TMS）に登録されているエンドポイントを検出して管理できます。検出の一部として、デバイスの詳細も取得され、Prime Collaboration データベースに保存されます。検出が完了したら、次のデバイス管理タスクを実行できます。

  - デバイスの追加または削除
  - デバイス クレデンシャルの管理
  - デバイスの検出

- モニタリングおよび障害管理

  サービス オペレータは、企業のすべての音声およびビデオ セッションについて、ネットワークにおけるサービス低下の原因を迅速に特定する必要があります。Prime Collaboration では、サービス インフラストラクチャとネットワーク関連の問題の詳細な分析を行えます。

  Prime Collaboration は、設定されたポーリングパラメータに基づいて管理対象デバイスから定期的に情報をインポートします。

  ホーム ページには、システム パフォーマンス、デバイス ステータス、デバイス検出、CTI アプリケーション、音声メッセージング ポートをモニタするのに役立つ複数の構成済みダッシュレットが含まれています。これらのダッシュレットにより、システムの健全性を監視するための事前定義済みの一連の管理オブジェクトを監視することができます。ダッシュレットから状況に応じたサービスアビリティ ページを起動できます。

  Prime Collaboration は、ほぼリアルタイムで、迅速かつ正確な障害検出を実現します。Prime Collaboration では、ユーザにとって重要なイベントをモニタできます。アラームの通知を送信するように Prime Collaboration を設定できます。

  Cisco TelePresence Management System や Unified Communications アプリケーションにおける障害以外にも、Cisco TMS で発生したカスタム チケットを表示します。

  アラーム ブラウザを使用して、アラームやシステムのイベントを表示し、トラブルシューティングを開始できます。また、障害通知を送信するように Prime Collaboration を設定し、Call Events UI の Cisco TMS アプリケーションに関連するコールの接続または切断の詳細を表示できます。

Cisco Prime Collaboration Assurance は、Cisco Unified Communications インフラストラクチャ全体の統合ビューを提供し、Cisco Unified Communications ネットワークの各要素の現在の動作ステータスを示します。また、Prime Collaboration は、問題を迅速に切り分けて解決するための診断機能も備えています。Cisco ゲートウェイ、ルータ、スイッチに加えて、Prime Collaboration は、次のようなさまざまな Cisco Unified Communications 要素の運用ステータスも継続的にモニタリングします。

- Cisco Unified Communications Manager（Unified CM）
- Cisco Unified Communications Manager Express（Unified CME）
- Cisco Unified Communications Manager Session Management Edition
- Cisco Unity Connection
- Cisco Unity Express
- Cisco Unified Contact Center Enterprise（Unified CCE）、Unified Contact Center Express（Unified CCX）、および Unified Customer Voice Portal（Unified CVP）

  （注）　Cisco Prime Collaboration のサービス レベル ビューは、複数の Cisco Unified Contact Center Enterprise（Unified CCE）の配置はサポートしていません。

- Cisco IM and Presence
- Cisco Emergency Responder
- Cisco Unified Border Element
- Cisco Unified Endpoint

（注）　Cisco Prime Collaboration は仮想環境で動作する Unified Communications および TelePresence アプリケーションに対応していますが、VMware やハードウェアをモニタすることはできません。VMware ホストの管理には vCenter を使用してください。Unified Computing System（UCS）B シリーズ ブレード サーバの場合、UCS Manager には Cisco UCS 内のすべてのソフトウェアとハードウェア コンポーネントを統合管理する機能が組み込まれています。これにより、複数のシャーシを制御し、何千もの仮想マシンのリソースを管理します。UCS C シリーズ サーバの場合、Cisco Integrated Management Controller は管理サービスを備えています。

サポートされている製品（特に Cisco エンドポイント）および Prime Collaboration でサポートされているバージョンの詳細については、次の URL から入手可能な Cisco Prime Collaboration のデータ シートを参照してください。

https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html

Unified Communications の構成要素をモニタするプロトコルの 1 つとして、Prime Collaboration では簡易ネットワーク管理プロトコル（SNMP）が使用されます。SNMP は、トランスポート層プロトコルとして UDP を使用するアプリケーション層プロトコルです。SNMP で管理されるネットワークには、次の 3 つのキーとなる要素があります。

- 管理対象デバイス：SNMP エージェントを持つネットワーク デバイス（Unified CM、ルータ、スイッチなど）。
- エージェント：管理対象デバイスに存在するネットワーク管理ソフトウェア モジュール。このエージェントは、デバイスのローカル管理情報を SNMP メッセージに変換します。
- マネージャ：管理ステーションで実行され、ネットワーク内の別のエージェントに接続して管理情報を取得するソフトウェア（Prime Collaboration など）。

SNMP の実装では、SNMP v1、SNMP v2c、および SNMP v3 の 3 つのバージョンがサポートされています。SNMP v3 は、認証、暗号化、およびメッセージの完全性をサポートしています。管理トラフィックにセキュリティが必要な場合は、SNMP v3 を使用できます。Prime Collaboration は、SNNP の 3 種類のバージョンをすべてサポートしています。エージェントとマネージャが正常に通信するには、各デバイスに SNMP v1 および v2c のリード/ライト（read/write）コミュニティ ストリングまたは SNMP v3 のクレデンシャルを設定する必要があります。Prime Collaboration では、ネットワーク デバイス情報を収集するために SNMP 読み取りアクセスだけが必要です。

SNMP の詳細については、次の URL から入手可能な Cisco Prime Collaboration のマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html

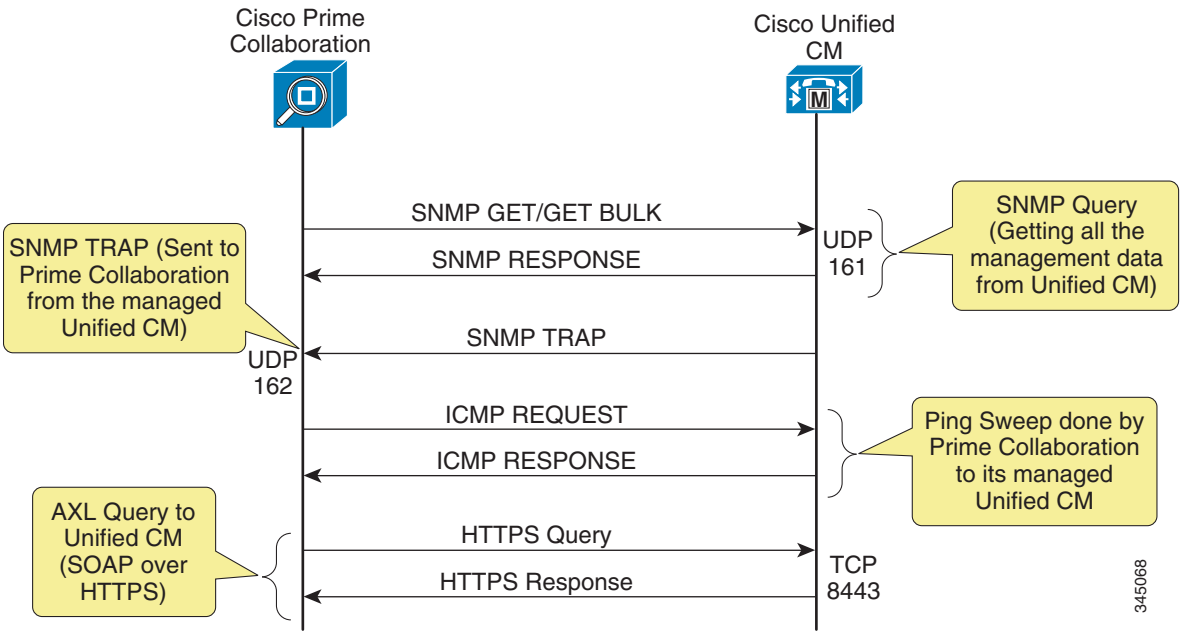
Assurance の設計上の考慮事項

Cisco Prime Collaboration は、次のような方法でネットワーク内の他のデバイスとインターフェイスを取ります。

- 簡易ネットワーク管理プロトコル（SNMP）を使用して、すべての Cisco Unified Communications サーバ、ゲートウェイ、スイッチを管理します。
- Administrative XML Layer（AXL）を使用して、Unified CM を管理します。AXL は、Simple Object Access Protocol（SOAP）over HTTPS Web サービスとして実装されます。
- HTTP を使用して IP Phone に接続し、シリアル番号とスイッチ情報を収集します。IP Phone で HTTP が有効になっている必要があります。
- 拡張イベント処理と Cisco Unified CM のリモート syslog を統合し、Cisco Real-Time Monitoring Tool（RTMT）インターフェイスを利用して、事前に収集された Unified CM クラスタ全体のデータにアクセスします。
- Skinny Client Control Protocol（SCCP）および Session Initiation Protocol（SIP）を使用して、統合テストのために Cisco Unified IP Phone と通信します。
- インターネット制御メッセージ プロトコル（ICMP）または ping スイープを使用して、Cisco IOS ルータやスイッチ、および他の音声デバイスや非音声デバイスとインターフェイスします。

図 27-1 は、パフォーマンス カウンタとアラームを収集するために Prime Collaboration が Unified CM との複数のインターフェイスを利用するしくみシステム レベルの概要を示しています。

図 27-1　Prime Collaboration と Unified CM のシステム レベルの統合



通話品質のモニタリング（サービス エクスペリエンス）

Cisco Prime Collaboration Assurance Advanced は Cisco Unified Communications ネットワークでのコールの音声品質をモニタします。また、Unified CM とネットワーク解析モジュール（NAM）を利用して、ネットワーク内の疑似コールではなく、実際のコールに関する音声品質統計情報をモニタリングして収集します。次に、収集した品質統計情報を事前定義されたしきい値と比較します。

また、Prime Collaboration Assurance Advanced は、Cisco Prime Analytics（Prime Collaboration Advanced でのみ利用可能）にも音声品質情報を送信して、Analytics がコール データ分析を実行してレポートを生成できるようにします。

（注）　一連のグローバルなコール品質しきい値は、サポートされているコーデック タイプごとに 1 つずつ定義できます。モニタ対象の Unified CM クラスタに基づいて、異なるしきい値をグループ化できます。

音声品質の測定

音声品質とは、IP Phone コールの音声および会話の品質を測る質的および量的な基準です。音声品質の測定は、音声会話の明確度および明瞭度を表して、評価します。Prime Collaboration は、ネットワーク解析モジュール（NAM）と Unified CM を使用して音声品質情報をモニタし、レポートします。

Unified CM の音声品質のモニタリング

Unified CM は、コール終了時に音声およびビデオ情報とメトリックをコール詳細レコード（CDR）とコール管理レコード（CMR）に保存します。CMR と CDR は、セキュア ファイル転送プロトコル（SFTP）を介して、60 秒ごとに Prime Collaboration に転送されます。Unified CM と統合するには、Unified CM の Unified Serviceability の設定 Web ページで、Prime Collaboration を課金アプリケーション サーバとして設定する必要があります。Unified CM クラスタごとに最大 3 つの課金アプリケーション サーバを設定できます。次の設定を課金アプリケーション サーバに指定します。

- Prime Collaboration Assurance 仮想マシンのホスト名または IP アドレス
- SFTP ファイル転送のユーザ名およびパスワード
- プロトコル：SFTP
- CDR と CMR ファイルを転送する Prime Collaboration 仮想マシンのディレクトリ パス

（注）　Cisco CE または TE ソフトウェアを実行している Cisco Jabber およびエンドポイントは、コール終了時の音声およびビデオ情報を生成しません。したがって、これらのエンドポイントの CMR はありません。

これまでは、音声品質をモニタする 1 つの方法として、Cisco Voice Transmission Quality（CVTQ）アルゴリズムを使用することに重点が置かれていました。CVTQ は Klirrfaktor（K ファクタ）方式に基づいて、音声コールの MOS 値を見積もります。Cisco CSR 12.*x* では、重要な統計情報はパケット カウント、隠蔽率、隠蔽秒数カウンタです。これらはネットワーク障害が耳に聞こえるレベルになる前や、MOS によって視覚化される前にネットワーク オペレータに警告を発します。表 27-3 は、これらのカウンタとカウンタから計算されるメトリックを示しています。

表 27-3　通話品質を測定するカウンタとメトリック

カウンタまたはメトリック	説明
Concealment（隠蔽）	障害が発生したネットワークでのパケット（フレーム）損失および音声品質への影響を測定します。
CS：隠蔽秒数	隠蔽が生じた秒数（聞こえない可能性がある）
SCS：重大な隠蔽発生秒数	損失が 5 % を超えた秒数（音声）
SCSR（SCS 比率）：SCS/継続時間	音声品質を測定するメトリック
CSR（CS 比率）：CS/継続時間	ネットワーク品質を測定するメトリック

表 27-3 に示すように、SCSR は音声品質の測定基準であり、Prime Assurance によってコールの評価に使用されます。継続時間が 20 秒未満のコールの場合は、通話品質の評価に次の SCSR 値が使用されます。

グレード	SCSR 値
良好（Good）	0.20 未満
可（Acceptable）	0.20 <= SCSR <= 0.30
不良（Poor）	0.30 より多い

継続時間が 20 秒以上のコールの場合は、通話品質の評価に次の SCSR 値が使用されます。

グレード	SCSR 値
良好（Good）	0.03 未満
可（Acceptable）	0.03 <= SCSR <= 0.07
不良（Poor）	0.07 より多い

Cisco Network Analysis Module（NAM）

Cisco NAM は、リモート モニタリング（RMON）および一部の SNMP 管理情報ベース（MIB）を利用して、ネットワーク管理者が Unified Communications インフラストラクチャのすべてのレイヤを表示し、アプリケーションや、音声とビデオのアプリケーションの QoS などのネットワーク サービスをモニタ、分析、トラブルシューティングできるようにするトラフィック分析モジュールです。Cisco NAM 4.0 で追加された音声計測方法では、NAM を Prime Collaboration と統合し、NAM に組み込まれているデータ収集とパフォーマンス分析を介してコール メトリクスを利用できます。

Cisco NAM は、Prime Collaboration を補完して企業全体の音声管理ソリューションを提供します。NAM アプライアンスは、トラブルシューティングおよび分析のためのグラフィカル ユーザ インターフェイスを備えており、RTP を使用した音声品質分析、音声制御、およびシグナリング モニタリングのための豊富なフィーチャ セットを提供します。

Cisco Prime Collaboration は、音声品質メトリックのために 60 秒ごとに NAM をポーリングをします。次に、そのデータの MOS を計算します。これにより、Prime Collaboration は、CDR と NAM からのコール ストリーム レポートを相互に関連させてさらに高度な分析を行うことができます。

Cisco NAM の詳細については、次のサイトを参照してください。

https://www.cisco.com/go/nam

音声品質モニタリング方法の比較

Unified CM の通話品質（CDR および CMR）と NAM は相互に補完して、音声品質測定のトータル ソリューションを実現します。Unified CM と Cisco NAM による音声品質モニタリングの主な違いは、次のとおりです。

- Cisco NAM は 60 秒ごとに音声品質統計情報を生成します。Unified CM は、コールが完了（終了）した後に音声品質の統計情報を生成します。
- Unified CM は、自身のクラスタ内のコール セグメントだけをモニタします。
- ネットワーク内の全体的な音声コール品質を測定するには、Unified CM の音声品質モニタリングを使用するのが最適です。

Unified CM の通話品質メトリックが使用されていない場合でも、Prime Collaboration は Unified CM の CDR 情報を使用して NAM レポートと相互に関連させ、次のメトリクスを取得します。

- 発信元か宛先、またはその両方の内線番号
- デバイス タイプ
- ゲートウェイを介したコールの場合に、コールが送信されるインターフェイス
- コールの切断理由（可能な場合）
- 電話機が接続される（Unified CM クラスだけでなく）正確な Unified CM サーバ

トランク使用率

Cisco Prime Collaboration はリアルタイムの Unified CM トランク使用率のパフォーマンス グラフを表示します。また、Cisco Prime Analytics と緊密に統合されており、長期間にわたるトレンド分析とレポート処理を行えるように、収集したコール情報を Analytics に提供します。コール情報は、Prime Collaboration が Unified CM から収集した CDR および CMR レコードから提供されます。

フェールオーバーおよび冗長性

Unified CM パブリッシャ サーバは、SFTP 経由で CDR および CMR ファイルを Prime Collaboration に転送します。パブリッシャ サーバを使用できない場合はフェールオーバー メカニズムがないため、Prime Collaboration は Unified CM クラスタ内のコールの MOS 値を含む新しい CDR や CMR ファイルを取得できません。

音声モニタリング機能

Cisco Prime Collaboration は、次の音声品質モニタリング機能をサポートしています。

- 次のいずれかのシナリオ。
  - 1 分あたり 5,000 本のセンサーベースの RTP ストリーム（NAM モジュール）
  - 1 分あたり 1,600 本の Unified CM コール
  - 1 分あたり 1,500 本の RTP ストリームと 666 本の Unified CM コール
- Prime Collaboration は、特定の Unified CM クラスタに設定されているすべての Cisco Unified IP Phone について、音声品質情報を（CDR と CMR ファイルを通じて）自動的に選択して収集します。クラスタ内の特定の IP Phone だけをモニタする設定オプションはありません。

（注）　Prime Collaboration がフル キャパシティで動作している場合、予想されるデータベース増加（Syslog、CDR、および CMR のファイル）は 1 日あたり約 2.4 GB になると推定されます。

Assurance のポートおよびプロトコル

表 27-4 は、Cisco Prime Collaboration のさまざまなプロトコル インターフェイスで Assurance に対して使用されるポートを示しています。これらのポートを社内ファイアウォール（該当する場合）で許可して、Prime Collaboration とネットワーク内の他のデバイス間の通信を可能にすることを推奨します。

表 27-4　Assurance に対する Cisco Prime Collaboration のポートの使用

プロトコル	ポート	サービス
UDP	161	SNMP ポーリング
UDP	162	SNMP トラップ
TCP	80	HTTP
TCP	443	HTTPS
TCP	1741	CiscoWorks HTTP サーバ
UDP	22	SFTP
TCP	43459	データベース
UDP	514	Syslog
TCP	8080	Unified CM のステータス確認 Web サービス
TCP	8443	Unified CM と Prime Collaboration 間の SSL ポート

（注）　Cisco NAM は、デフォルト以外のポートを使用して、HTTPS でリモートにアクセスされます。Prime Collaboration は各 Cisco NAM と使用して認証を行い、HTTP/S セッションを維持します。

Prime Collaboration または管理対象デバイスから発信されるすべての管理トラフィック（SNMP）には、デフォルトのマーキングとして DSCP 0x00（PHB 0）が付けられます。ネットワーク管理システムの目標は、ネットワーク内のすべての問題または誤動作に対応することです。正確かつ信頼性の高いモニタリングを保証するために、ネットワーク管理データを優先順位付けする必要があります。QoS メカニズムを実装すると、パケット遅延、パケット損失、およびジッタが確実に減少します。ネットワーク管理トラフィックに IP Precedence 2、つまり DSCP 0x16（PHB CS2）を付けて、最小帯域幅保証を提供することを推奨します。Windows オペレーティング システムでは、DSCP 値を設定する必要があります。

管理対象デバイスがファイアウォールの背後にある場合、管理トラフィックを許可するようにファイアウォールを設定する必要があります。ネットワーク アドレス変換（NAT）を使用するネットワークでは、Prime Collaboration のサポートに制限があります。Prime Collaboration サーバから NAT の背後にあるデバイスの NAT IP アドレスへの IP 接続と SNMP 接続が必要です。Prime Collaboration ではスタティック NAT がサポートされます。

帯域幅の要件

Prime Collaboration は、設定された間隔で管理対象デバイスをポーリングして運用ステータス情報を取得します。この情報には、重要な管理データが大量に含まれている可能性があります。特に低速 WAN 上に多数の管理対象デバイスがある場合は、帯域幅を管理データ用にプロビジョニングする必要があります。トラフィック量は、管理対象デバイスのタイプによってそれぞれ異なります。たとえば、Cisco 音声ゲートウェイのモニタリングと比較した場合、Unified CM のモニタリングのほうがより多くの管理メッセージを含んでいることがあります。また、管理トラフィックの量は、管理対象デバイスが完全モニタリング状態にあるのか部分モニタリング状態にあるのか、および統合テストが実行されているのかどうかによって変わります。

Analytics

Cisco Prime Collaboration Analytics は、Prime Assurance にさらに多くの利点をもたらします。Analytics は、長期間にわたって低下を識別するトレンド分析機能を備えています。また、トレンド分析を利用して、キャパシティ プランニングと Quality of Service（QoS）情報を提供することもできます。キャパシティ プランニング機能により、管理者は拡張を計画したり、ネットワーク内の過剰に利用されているリソースや十分に利用されていないリソース（TelePresence エンドポイントなど）を特定したりできます。Analytics は、CIO プランナーや IT プランナーに実践的な情報を提供するレポートを自動生成できます。レポートは固有のビジネス ニーズに合わせてカスタマイズ可能です。

Analytics は次の事前定義されたダッシュボードをサポートしています。

- テクノロジー導入（Technology Adoption）
- 資産使用状況（Asset Usage）
- トラフィック分析（Traffic Analysis）
- キャパシティ分析（Capacity Analysis）
- サービス エクスペリエンス（Service Experience）

必要に応じて、カスタムのダッシュボードとダッシュレットも作成できます。

[テクノロジー導入（Technology Adoption）] ダッシュボードを使用すると、配置されたデバイスと使用された時間（分）を表示して、音声およびビデオの配置の進捗状況を表示できます。この情報によって、現在の導入分析に基づいた、よりインテリジェントなテクノロジー投資の決定が可能になります。

[資産使用状況（Asset Usage）] ダッシュボードには、長期にわたるコラボレーション ネットワーク リソースの使用率分析が表示されます。また、使用頻度が最も低いリソースと最も高いリソース（エンドポイント）などの情報も示されます。

[トラフィック分析（Traffic Analysis）] ダッシュボードを使用すると、長期的なサービス品質の問題を分析したり、音声およびビデオ トラフィックのパターンを特定することができます。上位 *N* 件の発信者、上位 *N* 件のダイヤル番号、上位 *N* 件のオフネット トラフィックの場所、上位 *N* 件のコール トラフィックの場所を示すオプションもあります。

[キャパシティ分析（Capacity Analysis）] ダッシュボードには、会議デバイス、コール アドミッション制御の帯域幅、トランクなど、未使用または十分に利用されていない音声およびビデオ資産を追跡できるオプションがあります。提供される情報は、機器とネットワーク コストの最適化に役立ちます。

[サービス エクスペリエンス（Service Experience）] ダッシュボードを使用すると、コラボレーションの配置におけるコール品質の問題を特定できます。品質に問題がある上位 *N* 件のエンドポイントを表示したり、品質レベルに基づいてフィルタリングすることができます。また、通話障害の分析、ユーザ グループやエンドポイント グループによるサービス使用状況の識別、IT 費用を効率的な割り当てを行うことができます。

機能のサポートや機能の詳細については、https://www.cisco.com から入手可能な Cisco Prime Collaboration Analytics 製品のマニュアルを参照してください。

（注） 現在、Analytics による冗長性およびフェールオーバーのサポートはありません。

Analytics サーバのパフォーマンス

Analytics は Prime Assurance の OVA 含まれており、同じ仮想マシン上で動作します。Analytics には別途ライセンスが必要なので注意してください。

プロビジョニング

Prime Collaboration Provisioning は、次の形式で使用可能です。

- Prime Collaboration Provisioning Standard
- Prime Collaboration Provisioning Advanced

Prime Collaboration Provisioning Standard は、Cisco Prime Collaboration Provisioning の簡素化されたバージョンです。すべてのコラボレーション サービスで、簡素化されたプロビジョニングを提供します。電話、ボイスメール クライアント、ビデオ エンドポイントを含めたすべてのサービスをプロビジョニングできます。Provisioning のサポートは、制限された承認権限を持つ 1 台の Unified Communications クラスタで利用できます。

Provisioning Advanced は、個別ドメインへの委任、インフラストラクチャ インスタンスの設定用テンプレートのサポート、詳細バッチ プロビジョニングなど、より高度な機能を提供します。表 27-5 は、Prime Collaboration Provisioning Standard と Prime Collaboration Provisioning Advanced で使用できる機能を示しています。

表 27-5　Prime Collaboration Provisioning Standard および Advanced の機能

機能	標準	詳細設定
ロールまたは Role Based Access Control（RBAC）の委任	単一のユーザ ロールをすべてのドメインに適用できます。異なるドメインにユーザ ロールを委任することはできません。	リージョンやグループに基づいて、任意のユーザ ロールを特定の論理ドメインに割り当てることができます。
オーダー ワークフロー権限	オーダー ワークフロー アクティビティ（オーダーの承認、MAC アドレスの割り当て、出荷エンドポイント、エンド ユーザのエンドポイントの受領など）は使用できません。	オーダー ワークフロー アクティビティは、エンド ユーザの要件に基づいて大幅にカスタマイズできます。アクティビティ権限を有効または無効にしたり、異なるユーザに割り当てたりして、オーダー ワークフローの効率を向上させることができます。
バッチ プロビジョニング	これらを 1 つのバッチに組み合わせることで、多数のサービスを展開できます。 **注:** バッチ プロビジョニングは 1 つのクラスタでのみ利用できます。	複数のクラスタにわたって高度なバッチ オプション（ユーザやサービスのインポート、ユーザやサービスの追加または変更など）を提供します。複数のクラスタにわたってバッチ インポートのインフラストラクチャを設定することもできます。

表 27-5　Prime Collaboration Provisioning Standard および Advanced の機能（続き）

機能	標準	詳細設定
インフラストラクチャ テンプレート	Infrastructure Configuration テンプレートはカスタマイズできません。	Cisco Unified Communications Manager、Cisco Unified Communications Manager Express、および Cisco Unity Express の初期設定や再設定に使用するテンプレートを作成できます。キーワードの追加や更新、テンプレート プロビジョニングのスケジュール設定など、設定を追加、編集、削除することができます。
Unified CM クラスタのサポート	1 つのクラスタだけを設定できます。	複数のクラスタを設定できます。
API	North Bound Interface（NBI）のサポートは使用できません。	North Bound Interface（NBI）のサポートを使用できます。

Cisco Prime Collaboration は、Cisco Unified Communications Manager（Unified CM）、Cisco Unified Communications Manager Express（Unified CME）、Cisco Unity Connection、および Cisco Unity Express の新規と既存の両方の配置について、簡素化された Web ベースのプロビジョニング インターフェイスを提供します。Prime Collaboration は、インフラストラクチャとサブスクライバの両方に対して、導入時（Day 1）および導入後（Day 2）のニーズに応じたプロビジョニングを提供します。1 日目に必要なものには、新規配置の設定およびサイトまたはロケーションの追加が含まれ、2 日目に必要なものには、Cisco Unified Communications ソリューションのさまざまなコンポーネントにおける継続的な移動、追加、および変更のためのサービスが含まれます。

また、Cisco Prime Collaboration では Northbound API を公開しているので、シスコ製品やサードパーティ製品を外部アプリケーション（HR システム、カスタムまたはブランド製のユーザ ポータル、他のプロビジョニング システム、ディレクトリ サーバなど）と統合できます。

Prime Collaboration のシステム要件とインストール手順、プロビジョニング ユーザとサポートされるコンポーネントのインフラストラクチャ、およびキャパシティ情報については、次の URL から入手可能な Cisco Prime Collaboration のマニュアルを参照してください。

https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html

Prime Collaboration をネットワーク管理ソリューションとして使用する方法をより深く理解して、さまざまな Cisco Unified Communications コンポーネントをプロビジョニングできるように、次の項では Prime Collaboration の基本概念について説明します。

プロビジョニングの概念

Cisco Prime Collaboration は、Cisco Unified Communications システムの次のコンポーネントのプロビジョニング インターフェイスとして動作します。

- コール プロセッサ
  - Cisco Unified Communications Manager（Unified CM）
  - Cisco Unified Communications Manager Express（Unified CME）
- メッセージ プロセッサ
  - Cisco Unity Connection
  - Cisco Unity Express

- プレゼンス プロセッサ
  - Cisco IM and Presence
  - Cisco 音声ゲートウェイ
  - Cisco VG224、VG204、VG202 アナログ音声ゲートウェイ

(注) コンポーネントのバージョンの互換性については、https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html で Prime Collaboration の情報を参照してください。

次の項では、これらのコンポーネントの設定に関連する Prime Collaboration の概念について説明します。

ドメイン

ドメインは、システム内に複数の論理グループを作成するという管理上の目的で使用されます。ドメインには次の特性があります。

- ドメインは、地理的なロケーションまたは組織ユニットにマッピングできます。
- 1 つのドメインには、複数のコール プロセッサおよび複数のオプションのメッセージ プロセッサを含めることができます。
- 1 つの特定のコール プロセッサまたはメッセージ プロセッサを、複数のドメインのメンバーに設定できます。
- ドメインでサブスクライバを分割して、サブスクライバを別々に管理できます。

サービス エリア

サービス エリアはオフィスを示します。サービス エリアによって、ドメイン内のダイヤル プランおよび他の音声関連の設定が決まります。現実には、各オフィスに複数のサービス エリアが存在することがあります。サービス エリアによって、Unified CM 内で使用されるデバイス グループ、ルート パーティション、コーリング サーチ スペースなどの属性が決まります。サービス エリアには次の特性があります。

- 各サービス エリアは、単一のコール プロセッサおよびオプションの 1 つのメッセージ プロセッサに割り当てられます。
- 各サービス エリアは 1 つのダイヤル プランと関連付けられる必要があります。

ワークフローおよびオーダーの管理

新規サイトを展開する場合、または既存のサイトに対して移動、追加、および変更を行う場合、ユーザは、オーダーの作成とそのオーダーの処理という 2 段階のプロセスで基盤となるシステムを変更します。これらの段階の両方にポリシーを設定できます。たとえば、1 つのユーザ グループはオーダーの作成と送信だけができ、別のユーザ グループは処理関連のアクティビティの表示および実行ができるようにシステムを設定できます。Prime Collaboration には、Prime Collaboration の設定方法に基づいて、サービス アクティベーションやビジネス フローなどのオーダー処理を実行するオートメーション エンジンが含まれています。

ワークフローは、オーダー プロセスのアクティビティ（承認、電話機割り当て、出荷、および受領）を連係させます。

設定テンプレート

Prime Collaboration では、設定テンプレートを使用することにより、一貫した方法で Unified CM、Unified CME、Cisco Unity Express、Cisco Unity Connection を設定できます。テンプレートを使用して、これらの製品を設定したり、既存の製品で増分ロールアウトを実施したり、既存の顧客全員に新しいサービスを展開したりできます。

バッチ プロビジョニング

ユーザの作成およびそのサービスのプロビジョニングは、新規支店のロール アウトまたはレガシー システムからの移行用のバッチ プロビジョニングで自動的に実行することもできます。

ベスト プラクティス

次のベスト プラクティスとガイドラインは、Prime Collaboration を使用して、新規または既存の配置用に Cisco Unified Communications コンポーネントをプロビジョニングする場合に該当します。

- その他の導入時（Day 1）アクティビティ（新規サイトのロール アウトなど）や、導入後（Day 2）のアクティビティ（移動、追加、変更など）に Prime Collaboration を使用するには、事前に管理対象デバイスを起動しておく必要があります。
- Cisco Unified CM、Cisco Unity Connection、Unified CME、Survivable Remote Site Telephony（SRST）、Cisco Unity Express、Cisco IM and Presence サービスには、事前設定が必要です。
- 正しいドメイン、サービス エリア、およびプロビジョニング属性を定義します。
- 必要に応じて、ワークフロー規則だけを変更します。
- サブスクライバ タイプ、拡張規則の設定、および他の設定パラメータの使用を検討します。

これらのベスト プラクティスは、次のような基本タスクによってサポートされています。

- Unified CM、Unified CME などのコール プロセッサおよび Cisco Unity、Unity Connection、Unity Express などのメッセージ プロセッサの追加
- ドメインの作成、およびコール プロセッサとメッセージ プロセッサの作成済みドメインへの割り当て
- Unified CM または Unified CME 用の設定テンプレートを作成および使用した音声ネットワークのプロビジョニング、または既存の配置からの現在の音声インフラストラクチャ設定のインポート
- Prime Collaboration に対する LDAP ユーザの一括同期の実行（該当する場合）。
- 各ドメインのサービス エリアの作成（一般的に、ダイヤル プランごとに 1 つのサービス エリア）および各サービス エリアへのサブスクライバ（ユーザ）タイプの割り当てによる配置の設定
- 各ドメインの管理ユーザの作成
- サブスクライバまたはユーザのサービスのオーダー、更新、または変更

Prime Collaboration の設計上の考慮事項

次の設計上の考慮事項は、Prime Collaboration を使用してプロビジョニングする場合に該当します。

- 次のいずれかの方法でドメインを設定します。
  - 複数のサイトに対して、複数のコール プロセッサと複数のメッセージ プロセッサを持つ単一のドメインを作成します。
  - サイトごとに 1 つのコール プロセッサと 0 個以上のオプションのメッセージ プロセッサで構成されるドメインを作成します。
  - サブスクライバのサブセットを管理するために個別の管理者が必要な場合は、複数のドメインを作成します。
- 複数のダイヤル プランに対して複数のサービス エリアを作成します。
- Prime Collaboration のコール プロセッサとして Unified CM パブリッシャだけを追加します。Prime Collaboration を使用して行った Unified CM パブリッシャの変更はすべて、全 Unified CM サブスクライバ サーバと同期されます。
- Unified CM、Unified CME、または Cisco Unity Express の設定テンプレートを使用します。
- Unified CME および Cisco Unity Express の設定テンプレートには、Cisco IOS コマンドを使用します。
- Unified CM 設定テンプレート用の Cisco Unified CM インフラストラクチャ データ オブジェクトを追加します。
- 大量の電話機および回線（DN）がある場合は、既存のバッチ プロビジョニング用の設定テンプレートを変更します。
- 2 日目のサービス（電話機、回線、ボイスメールなど）の移動、追加、および変更のために、個々のドメイン管理者でそれぞれのサブスクライバ セットを管理する場合は、単一サイトの配置であっても、複数のドメインを作成します。
- 1 つのダイヤル プランに 1 つのサービス エリアを作成します。
- デバイス プール、ロケーション、コーリング サーチ スペース、および電話機に複数のダイヤル プランが必要な場合は、複数のサービス エリアを作成します。
- Prime Collaboration は、次の特性を備えた IPv6 対応アプリケーションです。
  - Prime Collaboration は IPv4 リンクを介して Unified CM と通信します。Unified CM には IPv4 の SOAP AXL インターフェイスしかないため、Prime Collaboration のユーザ設定インターフェイスでは IPv4 IP アドレスしか入力できません。したがって、Prime Collaboration は IPv4 アドレスを使用して Unified CM の AXL インターフェイスと通信する必要があります。
  - Prime Collaboration は、SIP トランクの AXL 応答メッセージに含まれている IPv6 アドレスを処理します。
  - IPv6 対応機能のサポートは、現在の Cisco Unified Communications Manager Express、Cisco Unity Express、および Cisco Unity Connection のデバイスのサポートには影響を与えません。

冗長性およびフェールオーバー

Prime Collaboration が設定プロセスの途中で失敗した場合は、Prime Collaboration GUI から設定済みデバイスに対して行われた変更が保存されていない可能性があり、復元できません。管理者は、Prime Collaboration が復旧されるまで、telnet などの他のツールを使用するか、管理対象デバイスにログイン（HTTP）して、手動手順により設定プロセスを続行する必要があります。コール プロセッサ（Unified CM または Unified CME）、メッセージ プロセッサ（Unity Connection、または Unity Express）、およびドメインに対して Prime Collaboration から同期化を実行しない場合、管理対象デバイスに手動で追加された設定変更は Prime Collaboration のダッシュボードやデータベースに自動的に表示されません。

プロビジョニングのポートとプロトコル

表 27-6 は、Prime Collaboration のさまざまなプロトコル インターフェイスで使用されるポートを示しています。これらのポートを社内ファイアウォール（該当する場合）で許可して、Prime Collaboration とネットワーク内の他のデバイス間の通信を可能にすることを推奨します。

表 27-6　プロビジョニングのために Prime Collaboration で使用されるポート

プロトコル	ポート	サービス
TCP	80	HTTP[1] [2]
TCP	8443	HTTPS[2]
TCP	22	SSH[3]
SSH	23	Telnet[3]
TCP	1433	データベース[4]

1. Prime Collaboration Administration の Web ページにアクセスします。
2. Prime Collaboration は、Administrative XML Layer（AXL）Simple Object Access Protocol（SOAP）を介して Unified CM をプロビジョニングします。
3. Prime Collaboration が Unified CME や Cisco Unity Express と通信する場合。
4. Prime Collaboration が Cisco Unity Connection のデータベースに接続する場合。

Cisco TelePresence Management Suite（TMS）

Cisco TelePresence Management Suite（TMS）は、ビデオ エンドポイントのスケジューリングと会議デバイスをサポートします。スケジューリングによって、エンドポイントとポート リソースの可用性が確保され、TelePresence 会議への接続が簡便になります。大部分の企業は、カレンダー アプリケーションを使用して会議のスケジュール作成しています。そのような場合は、カレンダー統合を行うと、ユーザが既存のカレンダー クライアントを使用して会議をスケジュールできるようになります。

カレンダー オプション

カレンダーを統合すると、会議が作成される場所に関係なく、リソースの可用性情報を検討しながら、カレンダー アプリケーションから直接ビデオ会議をスケジュールして参加者を招待できます。カレンダー オプションには次のものがあります。

- Cisco TelePresence Management Suite Extension for Microsoft Exchange（TMSXE）

  会議の主催者は、Microsoft Outlook クライアントを使用して会議をスケジュールすることができます。

- Cisco TelePresence Management Suite Extension for IBM Lotus Notes（TMSXN）

  会議の主催者は、IBM Lotus Notes クライアントを使用して会議をスケジュールすることができます。

- Cisco TelePresence Management Suite Extension Booking API（TMSBA）

  会議の主催者は、API の統合により、追加グループウェア カレンダー システムを使用して会議をスケジュールすることができます。

- Cisco TMS Web ベースのユーザ インターフェイス

  ユーザまたは管理者は、Web ベースのインターフェイスを使用して会議をスケジュールすることができます。これは Cisco TMS コア アプリケーションの一部なので、別途インストールしたり統合する必要はありません。

Cisco TMS の拡張機能と API の詳細については、次の URL から入手可能な製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/tsd-products-support-series-home.html

Cisco TMS では、ユーザと管理者が Web ベースのインターフェイスを使用して会議をスケジュールすることもできます。これは Cisco TMS コア アプリケーションの一部なので、別途インストールしたり統合したりする必要はありません。

組織で選択したスケジュールおよび管理プラットフォームを社内のカレンダー アプリケーションに統合することを強く推奨します。ただし、TMS Web インターフェイスを使用して会議をスケジュールすることもできます。

Cisco TMS カレンダー統合を社内のカレンダー アプリケーションとして展開する場合は、環境に応じた適切な拡張機能を選択してください。たとえば、既存のカレンダー アプリケーションが Microsoft Exchange の場合は TMSXE を使用します。TMSXE はスタンドアロン サーバにインストールされ、TMSXN は Lotus Domino サーバにインストールされます。統合ソフトウェアは Cisco TMS とは別にインストールされ、HTTP または HTTPS を使用してカレンダー サーバと通信します。

シスコでは、ビデオ会議リソース（Cisco TelePresence Video Communication Server または Cisco MCU）をスケジュール済み会議または永続的/臨時会議専用に設定することを推奨します。永続的会議や臨時会議は計画されているリソースを消費する可能性があるからです。これによってサーバのリソースが不足し、予定のビデオ参加者が会議に参加できなかったり、音声のみでの参加となったりするなど、スケジュールされている会議に悪影響が及ぶことになります。

レポート

Cisco TMS は、以下のような各種のレポートおよび分析機能を備えています。

- 資産管理レポート：チケット ログ、デバイス イベント、デバイス アラーム、接続
- 管理対象のエンドポイントとインフラストラクチャに関する詳細なコール履歴レポート
- スケジューリング アクティビティ レポート（使用されたユーザ ベースのスケジューリング インターフェイスなど）、イベント ログ、会議レポート

ただし、これらの機能の一部は特定の展開でのみ機能します。たとえば、Cisco TelePresence TX9000 や Cisco TelePresence System EX90 などのエンドポイントが Cisco Unified Communications Manager（Unified CM）に登録されている場合、Cisco TMS はそのエンドポイントに対してレポートを生成できません。Cisco TMS は、Cisco TelePresence Video Communication Server（VCS）に登録されているエンドポイントに対してのみコール詳細レコード（CDR）レポートを生成できます。Unified CM に登録されているエンドポイントの場合は、CDR を Unified CM からダウンロードできます。

さらにカスタマイズしたレポート、ビジネス知識、ビジネス インテリジェンス アプリケーションとの統合を必要とする組織では、Cisco TelePresence Management Suite Analytics Extension（TMSAE）を使用できます。これは、ビデオ ネットワークに高度なレポート機能を提供する Cisco TMS 用のオンライン分析処理システムです。Cisco TMSAE の詳細については、次の URL から入手可能な製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/tsd-products-support-series-home.html

管理

TelePresence 環境における管理の主な役割は、プロビジョニング、モニタリング、メンテナンス、リソース管理などです。Cisco TelePresence Management Suite（Cisco TMS）を使用すると、TelePresence 環境ともに TelePresence 環境でサポートされるスケジューリング インターフェイスを管理できます。

エンドポイントとインフラストラクチャの管理

Cisco TMS は、Cisco VCS と Cisco Unified CM の両方に登録されているエンドポイントを管理できます。デバイスの管理方式には、直接管理とプロビジョニングの 2 種類があります。

直接管理対象のデバイスは、Cisco TMS システム ナビゲータに手動で追加します。Cisco TMS は 5,000 台の直接管理対象デバイスをサポートします。Cisco TMS は、HTTP または SNMP プロトコル経由でエンドポイントと直接通信します。直接管理対象のエンドポイントが Unified CM に登録されている場合は、Unified CM が、ソフトウェアのアップグレードなど、大部分の管理機能に対処します。直接管理対象のエンドポイントが Cisco VCS に登録されている場合は、Cisco TMS が、ソフトウェアのアップグレードなどの機能を含めて、エンドポイントの管理やプロビジョニングに対処します。

Cisco TMS も Cisco VCS、Cisco MCU などのインフラストラクチャ デバイスを直接管理できます。現在、Cisco TMS は、Cisco VCS に登録されている会議デバイスに対してのみスケジューリングと管理をサポートしています。

プロビジョニング対象のエンドポイントは TMS システム ナビゲータにはありませんが、Cisco TMS Provisioning Extension（TMSPE）を介して Cisco TMS でプロビジョニングされます。Cisco TMS は 100,000 台のプロビジョニング対象デバイスをサポートします。プロビジョニング方式を使用すると、Cisco TMS のサポート可能範囲が大幅に拡大します。また、システムを手動で追加する必要がないため、一括配置の手順もシンプル化されます。ただし、直接管理対象エンドポイントと比べて、プロビジョニング対象エンドポイントに対する Cisco TMS の制御性は低下します。さらに、プロビジョニング対象のエンドポイントではスケジューリングはサポートされません。

Cisco TMS は、プロビジョニング対象エンドポイントに加えて、Cisco VCS に登録されている直接管理対象エンドポイントの電話帳機能も備えています。電話帳を使用すると、ユーザの検索やダイヤル アウトの操作性が向上します。

Cisco TMS には、スケジュールされたビデオ会議と臨時ビデオ会議の両方をモニタするインターフェイスもあります。

詳細については、『*Cisco TelePresence Management Suite Administrator Guide*』の最新バージョンを参照してください。このマニュアルは次の URL から入手できます。

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html

プロビジョニング

Cisco TMS Provisioning Extension（TMSPE）は、Cisco TMS および Cisco VCS 用のプロビジョニング アプリケーションです。Cisco TMSPE を使用することで、ビデオ会議ネットワーク管理者は、大規模展開が可能なビデオ会議ソリューションを作成して管理できます。Cisco TMSPE は、Cisco TMS サーバの TMS エージェントに代わるアドオンであり、次の主要機能を備えています。

- Microsoft および汎用 LDAP ソース（LDAP、LDAPS、AD）からユーザをインポートする機能
- Cisco TMS Provisioning Extension（Jabber ビデオ、Cisco IP Video Phone E20、Cisco TelePresence System EX シリーズおよび MX シリーズなど）でサポートされるデバイスに対するユーザのパーソナライズおよび管理デバイス設定の制御
- Cisco TMSPE でサポートされるデバイスの多層型電話帳
- Cisco VCS Web ユーザ インターフェイスの代わりに、Microsoft Active Directory（AD）ログインを使用する Cisco TMS 上のエンド ユーザ FindMe ポータル
- 最大 100,0000 人のユーザとデバイスをサポート

詳細については、『*Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*』の最新バージョンを参照してください。このマニュアルは次の URL から入手できます。

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-and-configuration-guides-list.html

電話帳

電話帳を使用すると、連絡先の保守性やダイヤルの操作性が向上します。Cisco TMS 電話帳は Microsoft Active Directory（AD）、Cisco Unified CM、H.350 サーバ、ゲートキーパーなど、さまざまなソースから作成して設定できます。

電話帳にはローカル電話帳とグローバル電話帳の 2 種類があります。ローカル電話帳（別称「*お気に入り*」）は、エンド ユーザ固有のエンドポイントに格納されるファイルです。連絡先は、必要に応じて、ユーザが追加、変更、削除できます。

グローバルまたは社内電話帳は Cisco TMS からエンドポイントに送信されます。これらの電話帳は AD、H.350 サーバ、またはローカル Cisco TMS データベースから自動的に入力されるため、エンドポイントからは変更できません。管理者は、特定のユーザの電話帳を選択して適切なエンドポイントに送信できます。

メンテナンスとモニタリング

Cisco TMS には、エンドポイントやインフラストラクチャのデバイスのソフトウェア イメージを追加できるソフトウェア マネージャ リポジトリがあります。それらのイメージを使用して、Cisco VCS に登録済みの一致するエンドポイントやインフラストラクチャのデバイスをアップグレードすることができます。管理者は、複数のデバイスを選択して Cisco TMS から一度にアップグレードできます。Cisco TMS ではアップグレードの状態が示されます。Cisco TMS を使用してアップグレードするほうが、エンドポイントやインフラストラクチャのデバイスを手動でアップグレードよりも簡便です。

Cisco TMS は会議のモニタ機能も備えています。Cisco TMS ではすべてのスケジュールされた会議が一覧表示され、会議のステータス（[アクティブ（Active）] など）とともに、アクティブな会議の参加者ごとのパケット損失の詳細が TMS の Conference Control Center に表示されます。エラーは TMS のチケット サービスに表示されます。たとえば、設定エラーがある場合、Cisco TMS はそれを検出して、該当するデバイスに関連付けられているチケットをオープンします。各チケットには ID と重大度が含まれています。

シスコ スマート ソフトウェア ライセンシング

Cisco Collaboration System Release（CSR）12.0 以降には、シスコ スマート ソフトウェア ライセンシングと、組織のコラボレーション ライセンスを管理するための Cisco Smart Software Manager（SSM）が同梱されています。Cisco SSM は、Cisco Unified CM、Cisco Unity Connection、Cisco Emergency Responder ならびに他のシスコ製品のラインセンスの適用、追跡、管理を一元化する手段となります。Cisco Smart Software Manager では管理者を支援するために、ユーザにアプリケーション サーバに対するライセンスを適用するために必要なステップの多くを自動化しています。

シスコ スマート ソフトウェア ライセンシングを構成する、シスコでホストされた Cisco Smart Software Manager Web ポータルでは、組織のコラボレーション アプリケーションの権限付与とライセンスが追跡されてコラボレーション コンポーネントと同期されます。

お客様がライセンスを購入すると、それらのライセンスが自動的にお客様の Cisco スマート アカウントに適用されて、Cisco SSM を介してオンプレミス アプリケーションと同期されます。Cisco Smart Software Manager はオンプレミスのコラボレーション アプリケーション インスタンスをシスコ ライセンシング サービスに登録し、それらのアプリケーションに対して組織のラインセンスを同期させます。

次の Unified Communications アプリケーションでは、シスコ スマート ソフトウェア ライセンシングを使用します。

- Cisco Unified Communications Manager（Cisco Unified CM）：Cisco IM and Presence（Unified CM を介してライセンス付与）および Cisco Unified Communications Manager Session Management Edition（SME）が含まれています。
- Cisco Unity Connection
- Cisco Emergency Responder

Cisco Smart Software Manager ポータルを使用してソフトウェアおよび権限付与を管理するには、最初に適切なライセンスを購入して Cisco スマート アカウントに適用する必要があります。その上で、組織の管理者が Cisco Smart Software Manager ポータル（https://software.cisco.com）で製品インスタンス登録トークンを生成します。その後、管理者は Cisco Smart Software Manager ポータルからコピーした登録トークンを使用して、コラボレーション アプリケーション製品インスタンスを登録します。登録後は、アプリケーションが Cisco Smart Software Manager と同期されて、ユーザおよび機能のライセンス資格情報を受信するようになります。

アプリケーションの非準拠状態は 90 日まで許容されます。この期間内はシステムが正常に機能し、ライセンスが不足している場合や、システムと Cisco SSM の間の通信が失われた場合は、管理者が変更を行うことができます。システムの非準拠状態が 90 日間続くと（つまり、不足しているライセンスが購入されない場合、または Cisco SSM との通信が復旧されない場合）、コラボレーション アプリケーションの機能は次のように制限されることになります。

- Cisco Unified Communications Manager（Unified CM）：コール制御

  システムの非準拠状態が 90 日間続いた場合、Unified CM は引き続きコールの処理を行いますが、ユーザまたはデバイスの移動、追加、変更、削除（MACD）は許可されなくなります。

- Cisco Unity Connection：ボイス メッセージング

  システムが非準拠状態の場合、引き続きシステムを使用して管理上の変更を行うことはできますが、システムはボイス メッセージング サービスを提供しなくなります。つまり、システムがコールに応答しなくなるため、発信者がメッセージを残したり、ユーザがボイス メッセージを取得したりすることはできません。

- Cisco Emergency Responder

  システムが非準拠状態の場合、Cisco Phone Tracking Engine サービスは停止されて、システムは電話機を追跡してロケーションを更新することをしなくなります。

シスコ スマート ソフトウェア ライセンシングおよび Cisco Smart Software Manager を使用したライセンス管理の詳細については、以下のリンク先から入手できる情報を参照してください。

https://www.cisco.com/go/smartlicensing

導入シナリオ

サポートされているすべてのアプリケーションのパブリッシャ ノードでは、シスコ スマート ソフトウェア ライセンシングが自動的に有効にされます。各クラスタ内のパブリッシャ ノードでは、Cisco Smart Licensing Manager サービスが自動的にアクティベートされて起動され、このサービスによってライセンスが管理されるようになります。パブリッシャ ノードは、クラスター内の他のすべてのノードのライセンスを管理します。

コラボレーション アプリケーションを登録して Cisco Smart Software Manager（SSM）とライセンス情報を同期させるには、各クラスタのパブリッシャ ノード上で実行中の Cisco Smart Licensing Manager サービスがインターネットを介して Cisco SSM サービスと通信する必要があります。この通信は直接行われることも、仲介されることもあります。

コラボレーション アプリケーションはインターネットで HTTPS を使用して直接 Cisco SSM サービスと通信しようとします。組織でアウトバウンド HTTPS トラフィックが許可されている場合、アウトバウンド HTTPS トラフィックはオンラインの Cisco SSM サービスに問題なく渡されます。組織のデータ センター アプリケーションから直接インターネットにアウトバウンド HTTPS トラフィックを渡すことが許可されていない場合は、シスコ スマート ソフトウェア ライセンシングとの通信を HTTP プロキシによってインターネットにリダイレクトできます。HTTP プロキシを使うか使わないかに関わらず、いずれの場合もアプリケーションと Cisco SSM オンライン サービスとの通信はインターネットを介して直接行われます。

別の方法として、コラボレーション アプリケーション パブリッシャ ノード間の通信をオンプレミスの Cisco Smart Software Manager サテライト システムに転送することもできます。これは、スマート ライセンシングとの通信を仲介するという方法です。Cisco SSM サテライト システムは、オンプレミスのデータ センター内の仮想マシン（VM）に配備されます。SSM サテライト システムが仲介者として、オンプレミスのコラボレーション アプリケーションとインターネットでホストされたオンラインの Cisco SSM サービスとの間で通信を中継します。SSM サテライトでは、定期的に Cisco SSM オンライン サービスに接続して同期する必要があります。この定期的な同期は、Cisco SSM サテライト システムと Cisco SSM オンライン サービス間の直接 HTTPS 通信を使用して行います。これが、Cisco SSM サテライト接続モードです。前述のとおり、組織がインターネットへのアウトバウンド HTTPS トラフィックに対して制限を課している場合は、HTTP プロキシを使用するか、あるいは SSM サテライト システムからのレポート ファイルを定期的に手動でオンライン サービスにアップロードするかのどちらかで、登録と承認を保守することになります。

Cisco SSM の直接導入または仲介による導入のいずれかを選択する際に主な考慮事項となるのは、インターネットとオンライン サービスのアクセスに関する組織のネットワークおよびセキュリティ ポリシーです。組織がインターネットへのアウトバウンド アクセスを制限している場合は、Cisco SSM サテライトの仲介による導入を検討してください。その際、オンプレミスのデータセンター内の独立した Cisco Smart Software Manager サテライト VM に関する要件に留意する必要があります。

展開の推奨事項

一般的に言えば、オンプレミスのコラボレーション アプリケーション（Unified CM、Unity Connection、Emergency Responder）クラスタのパブリッシャ ノードと Web でホストされた Cisco Smart Software Manager サービスとの間では、直接通信またはプロキシ通信が推奨されます。この場合、アプリケーション パブリッシャ ノードから Cisco Smart Software Manager サービスへのアウトバウンド HTTPS 通信は、組織のファイアウォールを通過しなければなりません。組織のポリシーで Web へのアウトバウンドの直接通信が許可されていなければ、クラスタのパブリッシャ ノードで組織内の新しいまたは既存の標準的な HTTP/HTTPS プロキシ サーバを使用することで、ファイアウォール トラバーサルおよび Web でホストされた Cisco Smart Software Manager サービスへのアクセスを可能にすることができます。

管理者が Cisco SSM 内で製品登録トークンを生成したりコラボレーション アプリケーション パブリッシャ インスタンスを登録したりする際は、ライセンスを管理しやすくするために、同じスマート アカウントの下で複数の仮想アカウントや登録トークンを使用して、特定の製品タイプや特定のロケーションにある製品をグループ化することができます。

複数の仮想アカウントを作成することをお勧めします。そうすれば、プールしたライセンスを組織全体の複数の製品や仮想ライセンスで共有できるため、ライセンスの管理が容易になります。さらに、仮想アカウントごとに製品インスタンスとトークンを区分すれば、組織は一層簡単にライセンスのコストを追跡して説明できるようになり、運用コストやその他の経費をさらに効果的に管理するために会計処理の項目を細分化することが可能になります。

（注）　複数の Cisco スマート アカウントのライセンスをプール、移動、管理することはできないため、組織が確立するスマート アカウントは 1 つに制限することを推奨します（そのスマート アカウントで必要な数だけ仮想アカウントを作成します）。ただし、この制限を緩めなければならない組織固有のポリシーや要件（法規制やその他の制約）がある場合は、その限りではありません。

冗長性

オンラインの Cisco SSM サービスは可用性に極めて優れています。ただし、インターネット接続に問題が発生して、コラボレーション アプリケーション システムが非準拠状態になった場合、システムが正常な動作を続けるのは 90 日間となります。システムが完全に非準拠状態になると、ユーザとデバイスをプロビジョニングできなくなります。正常なシステム運用を維持するためには、オンラインの Cisco SSM に常に到達可能でなければなりません。

Cisco SSM サテライト システムを使用してシスコ スマート ソフトウェア ライセンシングを仲介モードで導入する場合、高可用性を確保するために、少なくとも 2 つの SSM サテライト VM をインストールして設定してください。Cisco SSM サテライト システムはアクティブ/スタンバイの冗長性方式に依存します。つまり、アクティブ（プライマリ）システムで障害が発生した場合やコラボレーション アプリケーションあるいは Cisco SSM オンライン サービスに接続できなくなった場合は、スタンバイ（バックアップ）システムが SSM 運用を引き継ぎます。

Cisco Smart Software Manager のキャパシティ プランニング

サービス データ センター内の計算リソースに柔軟性が備わっていれば、オンラインの Cisco SSM サービスはほぼ無限にスケーリングします。つまり、組織は Cisco SSM を使用してライセンス付与するコラボレーション アプリケーションは、事実上、無限の数になるということです。

一方、仲介モードで稼働する場合、Cisco SSM サテライト VM にはキャパシティの制限があります。Cisco SSM サテライト VM ごとに、最大 4,000 件の製品インスタンス登録を処理できます。Cisco SSM を仲介モードで導入する場合は必ず、導入にライセンスが必要となるすべての製品インスタンスを処理するのに十分な数の VM を導入してください。

その他のツール

上記のネットワーク管理ツール以外に、次のツールにも Cisco Unified Communications システムのトラブルシューティングおよびレポート機能が備えられています。

- Cisco Unified Analysis Manager（27-26 ページ）
- Cisco Unified Reporting（27-27 ページ）

Cisco Unified Analysis Manager

Cisco Unified Analysis Manager は Cisco Unified Communications Manager Real-Time Monitoring Tool（RTMT）に含まれています。RTMT はクライアント側アプリケーションとして動作し、HTTPS と TCP を使用して、システム パフォーマンス、デバイス ステータス、デバイス検出、Unified CM 用 CTI アプリケーションをモニタします。RTMT は、HTTPS を使用して直接デバイスに接続し、システムの問題をトラブルシューティングできます。

他の RTMT 機能とは異なり、Unified Analysis Manager は 1 つだけではなく複数の Unified Communications の構成要素をサポートするという点で独特です。Unified Analysis Manager は、起動されると Unified Communications システムからトラブルシューティング情報を収集して、その情報の分析を提供します。この情報を使用して独自のトラブルシューティング操作を実行したり、分析のために Cisco Technical Assistance Center（TAC）に情報を送信したりできます。

Unified Analysis Manager では、以下のユニファイド コミュニケーション要素をサポートしています。

- Cisco Unified Communications Manager
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- Cisco IOS Voice Gateway
- Cisco Unity Connection
- Cisco IM and Presence

Unified Analysis Manager は、次のような主要機能を提供します。

- Unified Communications 要素からの Unified Communications アプリケーションのハードウェア、ソフトウェア、およびライセンス情報の収集をサポートします。
- Unified Communications 要素全体のトレース レベルの設定およびリセットをサポートします。
- Unified Communications 要素からのログおよびトレース ファイルの収集および定義済み FTP サーバへのエクスポートをサポートします。
- Unified Communications 要素全体のコール パスの分析（コール トレース機能）をサポートします。

レポート オプションの詳細については、最新バージョンの『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』に記載されている Cisco Unified Analysis Manager に関する情報を参照してください。このマニュアルは次の URL から入手できます。

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

Cisco Unified Reporting

Cisco Unified Reporting Web アプリケーションは、Cisco Unified Communications Manager クラスタ データをトラブルシューティングまたは調査するためのレポートを生成します。Unified Communications Manager コンソールからアクセスできる便利なツールです。このツールにより、既存のソースからのデータの収集、データの比較、および異常の報告が容易になります。たとえば、クラスタ内の全サーバのホスト ファイルを表示するレポートを参照できます。このアプリケーションは、パブリッシャ サーバおよび各サブスクライバ サーバから情報を収集します。各レポートは、レポートの生成時にアクセス可能なすべてのアクティブ クラスタ ノードのデータを提供します。

たとえば、Unified CM クラスタの一般的な管理には、次のレポートを使用できます。

- Unified CM Cluster Overview：全サーバの Unified CM バージョン、ホスト名、IP アドレス、ハードウェア詳細の要約など、クラスタの概要を示します。
- Unified CM Device Counts Summary：Cisco Unified Communications Manager データベースに存在するデバイスの数を、モデルおよびプロトコル別に示します。

Unified CM クラスタのデバッグには、次のレポートを使用できます。

- Unified CM Database Replication Debug：データベース複製のデバッグ情報を提供します。

Unified CM クラスタのメンテナンスには、次のレポートを使用できます。

- Unified CM Database Status：Unified CM データベースの正常性のスナップショットを提供します。アップグレードの前には、このレポートを生成して、データベースが正常であることを保証する必要があります。

レポート オプションの詳細については、次の URL で入手可能な『*Cisco Unified Reporting Administration Guide*』の最新バージョンを参照してください。

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

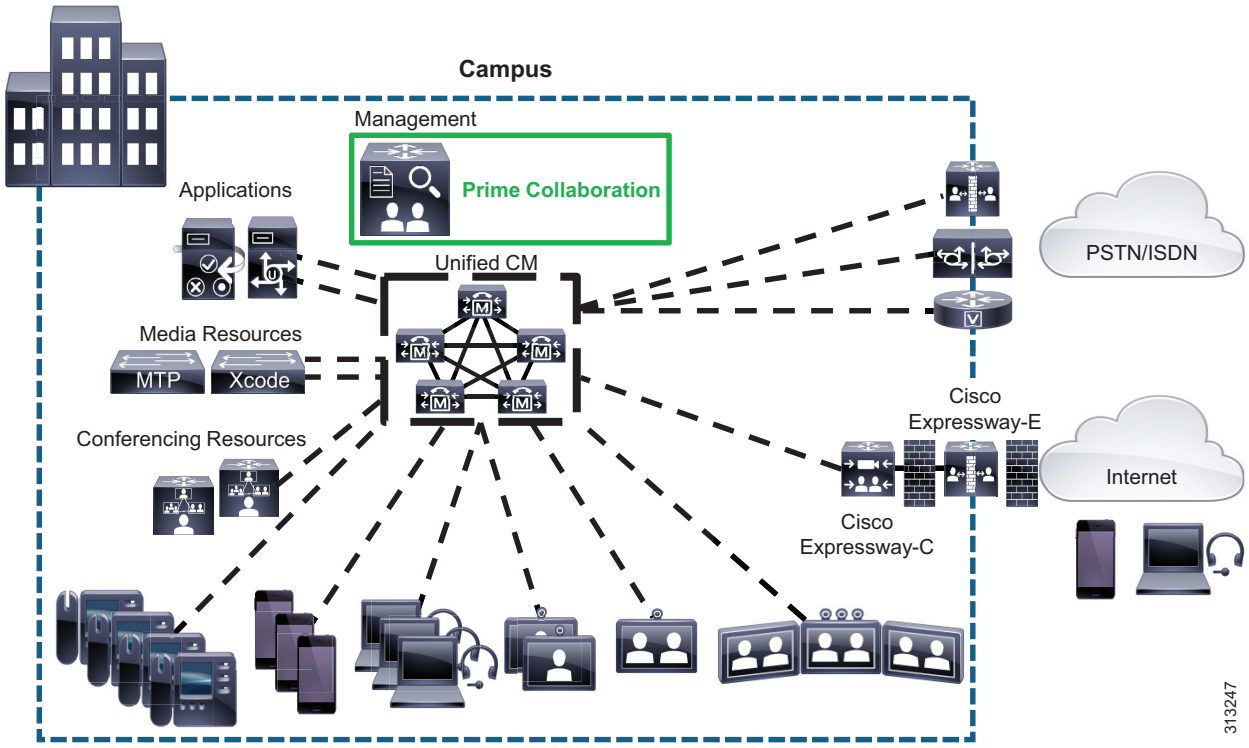
Cisco Unified Communication 配置モデルとの統合

この項では、さまざまな配置モデルに、シスコ コラボレーションおよびネットワーク管理アプリケーションを配置する方法について説明します。配置モデルの詳細については、コラボレーションの配置モデル（10-1 ページ）の章を参照してください。

キャンパス

キャンパス モデルでは、シスコ ネットワーク管理アプリケーションは呼処理エージェントとともに単一サイト（またはキャンパス）に配置され、IP WAN 上で提供されるテレフォニー サービスを使用しません。企業は、一般的に、LAN またはメトロポリタン エリア ネットワーク（MAN）上に単一サイト モデルを配置します。図 27-2 に、シスコ ネットワーク管理アプリケーションの単一サイト モデルの配置図を示します。

図 27-2　　キャンパスの展開



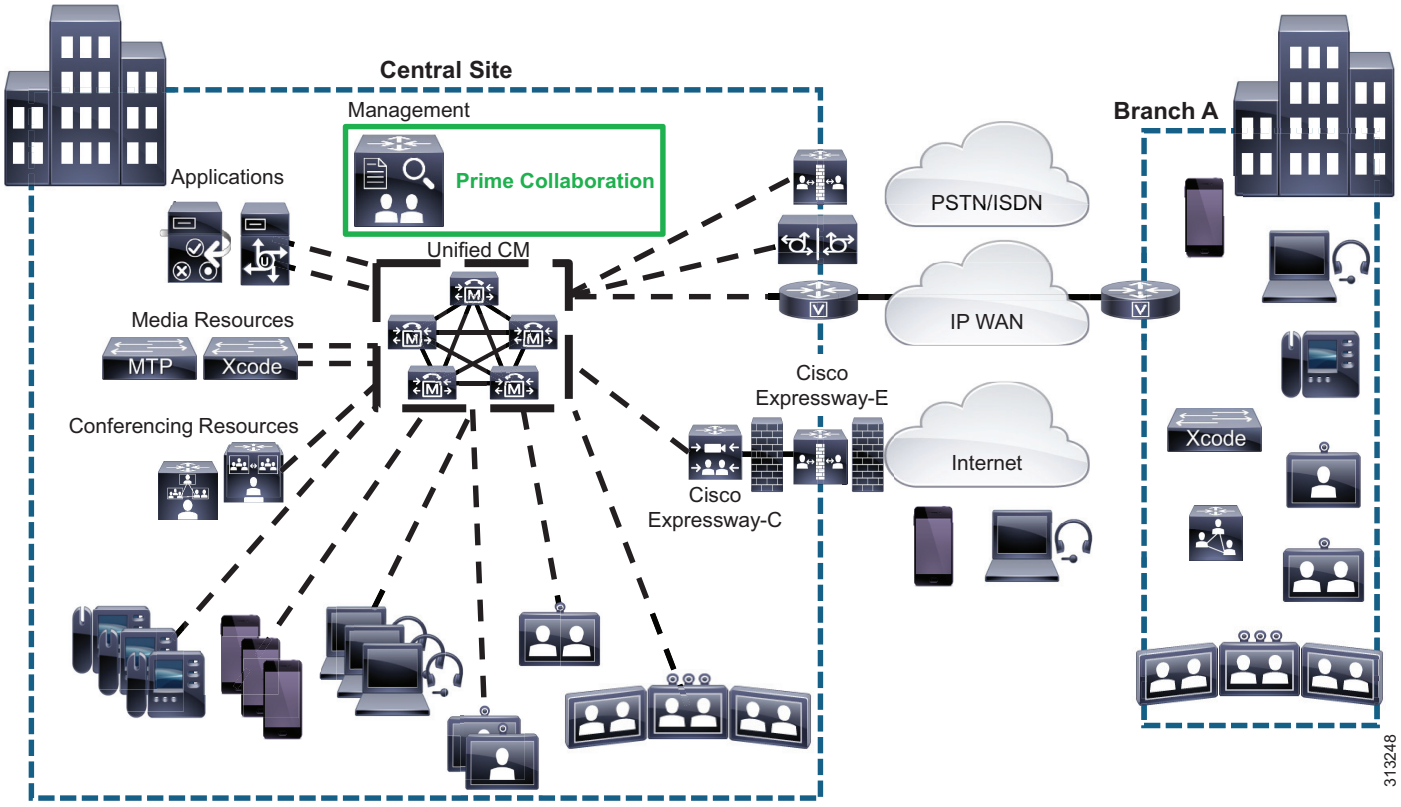
単一サイト モデルで Prime Collaboration を展開する場合には、次の設計特性と推奨事項が該当します。

- Unified CM 音声品質モニタリングを展開して、ネットワーク内の全体的な音声品質をモニタすることを推奨します。
- Cisco NAM を展開して、ネットワーク内の重要な IP Phone デバイス、ゲートウェイ デバイス、アプリケーション サーバをモニタし、音声品質の問題を調査およびトラブルシューティングすることを推奨します。

集中型呼処理を使用するマルチサイト WAN

集中型呼処理を使用するマルチサイト WAN モデルは、実際には単一サイト モデルの拡張であり、中央サイトとリモート サイト間で IP WAN を使用します。IP WAN は、サイト間の音声トラフィックと、中央サイトとリモート サイト間の呼制御シグナリングの転送に使用されます。図 27-3 に、シスコ ネットワーク管理アプリケーションの、集中型呼処理を使用するマルチサイト WAN モデルの配置図を示します。

図 27-3　集中型呼処理を使用するマルチサイト WAN 配置



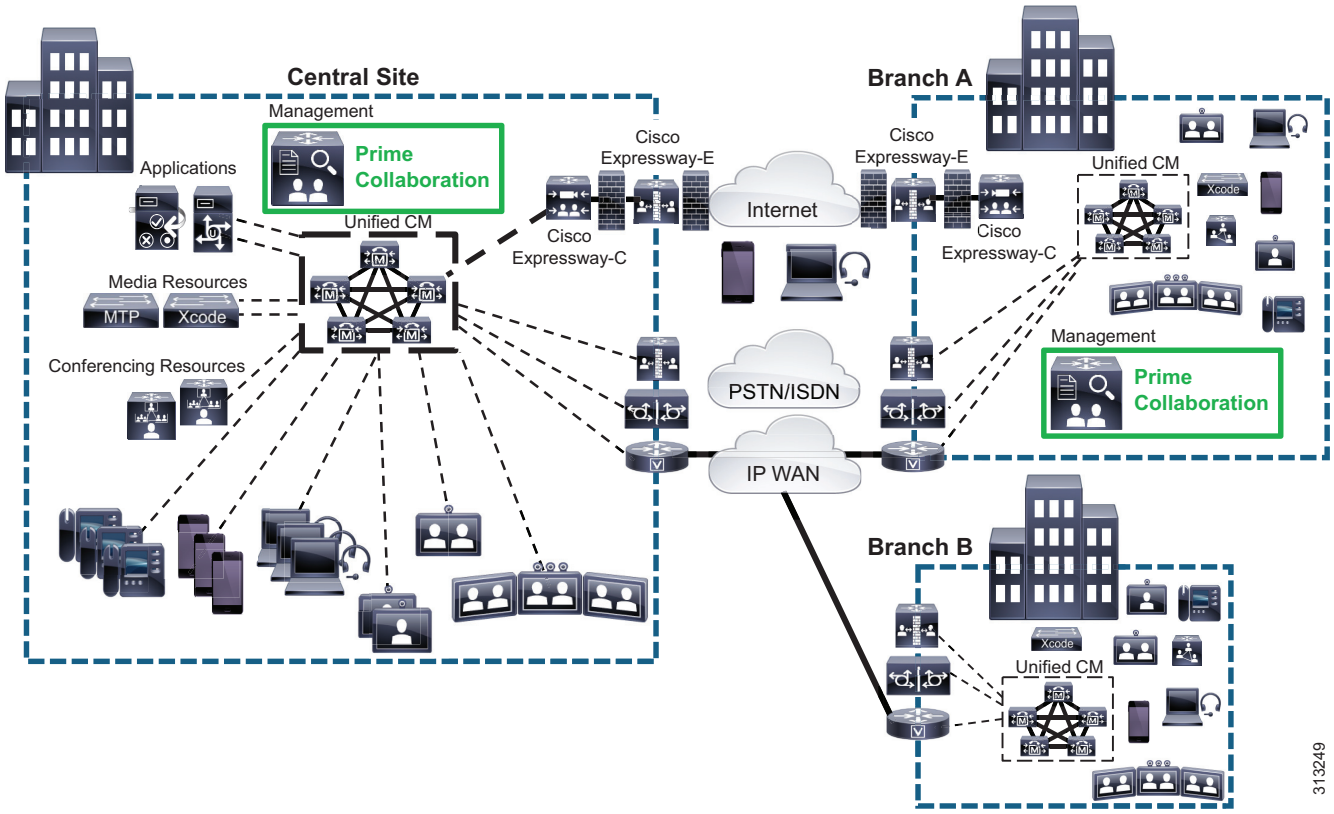
集中型呼処理を使用するマルチ サイト モデルで Prime Collaboration を展開する場合には、次の設計特性と推奨事項が該当します。

- すべてのネットワーク管理アプリケーション（Prime Collaboration など）を中央サイトに配置して、呼処理エージェントでそれらを検索することを推奨します。このような実装のメリットは、呼処理エージェントとネットワーク管理アプリケーション間のネットワーク管理トラフィックを、WAN 回線で送信するのではなく LAN 内で保持できることにあります。
- 複数の Prime Collaboration を配置して、各インスタンスでマルチサイトとマルチクラスタの Unified Communications 環境を管理できます。この配置シナリオでは、Manager of Managers（MoM）を配置することを推奨します。各 Prime Collaboration では、SNMP トラップ、syslog 通知、電子メールを使用して上位レベルの MoM にリアルタイム通知を送り、モニタ対象のネットワークのステータスを報告できます。
- Unified CM 音声品質モニタリングを展開して、ネットワーク内の全体的な音声品質をモニタすることを推奨します。
- サービス レベル契約（SLA）機能と模擬テスト機能を使用して、ネットワーク インフラストラクチャの状態をチェックすることを推奨します。
- Cisco NAM を展開して、ネットワーク内の重要な IP Phone デバイス、ゲートウェイ デバイス、アプリケーション サーバをモニタし、音声品質の問題を調査およびトラブルシューティングすることを推奨します。

分散型呼処理を使用するマルチサイト WAN

分散型呼処理を使用するマルチサイト WAN モデルは、複数の独立したサイトで構成されており、各サイト専用の呼処理エージェントが、IP WAN に接続されています。図 27-4 に、シスコ ネットワーク管理アプリケーションの、分散型呼処理を使用するマルチサイト WAN モデルの配置図を示します。

図 27-4　　分散型呼処理を使用したマルチサイト WAN 配置



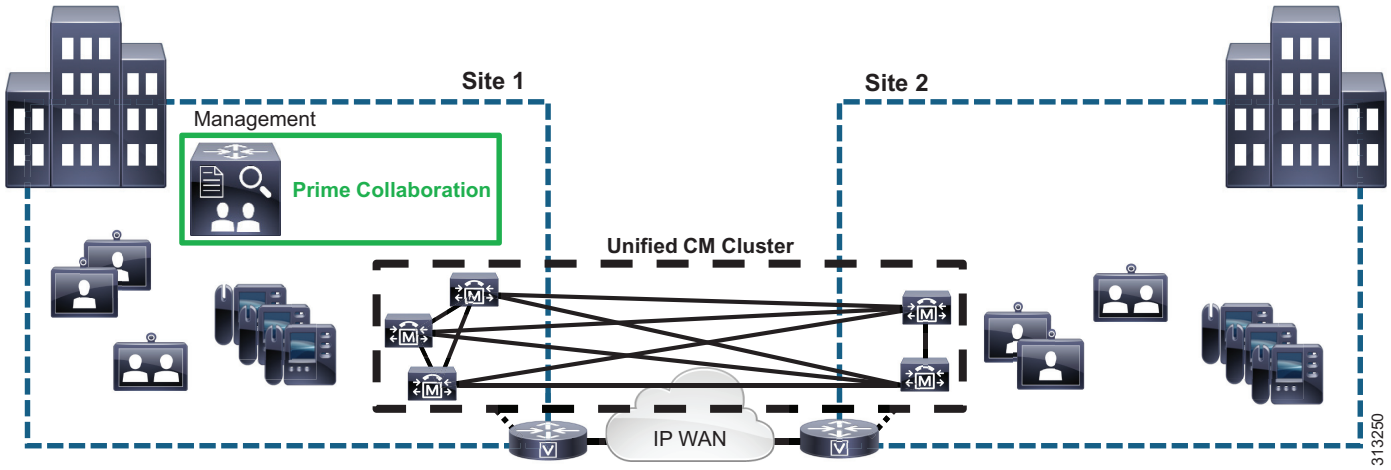
分散型呼処理を使用するマルチ サイト WAN 展開には、Prime Collaboration の配置に関して、単一サイト展開や集中型呼処理を使用するマルチ サイト WAN 展開と同じ要件が多数あります。分散型呼処理モデルについては、ここでリストされているベスト プラクティスおよび推奨事項に加えて、このような他のモデルのベスト プラクティスおよび推奨事項にも従ってください。

- Cisco Prime Collaboration Deployment を 1 つだけ使用して複数の Unified CM クラスタを管理する場合は、コール量とエンドポイント数が最も多い Unified CM クラスタとともに Prime Collaboration を配置することを推奨します。
- 複数の Prime Collaboration を配置して、各インスタンスでマルチサイトとマルチクラスタの Unified Communications 環境を管理できます。この配置シナリオでは、Manager of Managers（MoM）を配置することを推奨します。各 Prime Collaboration では、SNMP トラップ、syslog 通知、電子メールを使用して上位レベルの MoM にリアルタイム通知を送り、モニタ対象のネットワークのステータスを報告できます。
- Unified CM 音声品質モニタリングを展開して、ネットワーク内の全体的な音声品質をモニタすることを推奨します。
- Cisco NAM を展開して、ネットワーク内の重要な IP Phone デバイス、ゲートウェイ デバイス、アプリケーション サーバをモニタし、音声品質の問題を調査およびトラブルシューティングすることを推奨します。

WAN を介したクラスタリング

WAN を介したクラスタリングとは、QoS 機能対応の IP WAN で相互接続された複数のサイトに、単一の Unified CM クラスタを配置することをいいます。この配置モデルは、IP WAN リンクで障害が発生した場合に呼処理復元性を提供することを目的としています。図 27-5 に、シスコ ネットワーク管理アプリケーションの、WAN を介したクラスタリングの配置図を示します。

図 27-5　　WAN を介したクラスタリング



（注）　このモデルによる Prime Collaboration の展開では、ネイティブ ハイ アベイラビリティや冗長性のサポートはありません。

WAN を介したクラスタリングを使用する Prime Collaboration を展開する場合には、次の設計特性と推奨事項が該当します。

- Prime Collaboration を Unified CM パブリッシャが設置されている本社サイトに配置することを推奨します。
- 複数の Prime Collaboration を配置して、各インスタンスでマルチサイトとマルチクラスタの Unified Communications 環境を管理できます。この配置シナリオでは、Manager of Managers（MoM）を配置することを推奨します。各 Prime Collaboration では、SNMP トラップ、syslog 通知、電子メールを使用して上位レベルの MoM にリアルタイム通知を送り、モニタ対象のネットワークのステータスを報告できます。
- Unified CM 音声品質モニタリングを展開して、ネットワーク内の全体的な音声品質をモニタすることを推奨します。
- Cisco NAM を展開して、ネットワーク内の重要な IP Phone デバイス、ゲートウェイ デバイス、アプリケーション サーバをモニタし、音声品質の問題を調査およびトラブルシューティングすることを推奨します。

改訂日：2018 年 3 月 1 日

A

AA	Automated Attendant; 自動応答機能
AAD	Alerts and Activities Display; 警告とアクティビティの表示
AAR	Automated Alternate Routing（自動代替ルーティング）
AC	Cisco Attendant Console
ACD	Automatic Call Distribution; 自動着呼分配
ACE	Cisco Application Control Engine
ACF	Admission Confirm; アドミッション確認
ACL	Access Control List; アクセス コントロール リスト
ACS	Access Control Server
AD	Microsoft Active Directory
ADAM	Active Directory Application Mode; Active Directory アプリケーション モード
ADFS	Microsoft Active Directory Federated Services; Microsoft Active Directory フェデレーション サービス
ADPCM	Adaptive Differential Pulse Code Modulation; 適応的差分パルス符号変調
ADUC	Active Directory Users and Computers; Active Directory ユーザとコンピュータ
AES	Advanced Encryption Standard; 高度暗号化規格
AFT	ALI Formatting Tool
AGM	Cisco Access Gateway Module; Cisco アクセス ゲートウェイ モジュール
ALG	Application Layer Gateway; アプリケーション層ゲートウェイ
ALI	Automatic Location Identification; 自動ロケーション識別
AMI	Alternate Mark Inversion; 交互マーク反転
AMIS	Audio Messaging Interchange Specification

AMWI	Audible Message Waiting Indication; 音声メッセージ待機インジケータ
ANI	自動番号識別
AP	Access Point; アクセス ポイント
APDU	Application protocol data unit; アプリケーション プロトコル データ ユニット
API	Application Program Interface; アプリケーション プログラミング インターフェイス
APNs	Apple Push Notification service; Apple プッシュ通知サービス
ARJ	Admission Reject; アドミッション拒否
ARP	Address Resolution Protocol; アドレス解決プロトコル
ARQ	Admission Request; アドミッション要求
ASA	Cisco Adaptive Security Appliance
ASP	Active Server Page
ASR	Automatic Speech Recognition; 自動音声認識
ATA	Cisco アナログ電話アダプタ; ATA
ATM	Asynchronous Transfer Mode; 非同期転送モード
AVC	Advanced Video Coding
AXL	Administrative XML Layer

B

BAT	Cisco Bulk Administration Tool
BBWC	Battery-Backed Write Cache; バッテリ バックアップ式ライト キャッシュ
BES	Blackberry Enterprise Server
BFCP	Binary Floor Control Protocol（BFCP; バイナリ フロア制御プロトコル）
BFD	Bidirectional Forwarding Detection; 双方向フォワーディング検出
BGP	Border Gateway Protocol; ボーダー ゲートウェイ プロトコル
BHCA	Busy Hour Call Attempts; 最繁時呼数
BHCC	Busy Hour Call Completions; 最繁時発呼完了
BIB	Built In Bridge; ビルトイン ブリッジ
BLF	Busy Lamp Field; ビジー ランプ フィールド

BOSH	Bidirectional-streams Over Synchronous HTTP
BPDU	Bridge Protocol Data Unit; ブリッジ プロトコル データ ユニット
bps	ビット/秒
BRI	Basic Rate Interface; 基本速度インターフェイス
BTN	Bill-To Number; 請求先番号

C

CA	Certificate Authority
CAC	コール アドミッション制御
CAM	Content-Addressable Memory; 連想メモリ
CAMA	Centralized Automatic Message Accounting
CAPF	Certificate Authority Proxy Function
CAPWAP	Control and Provisioning of Wireless Access Points
CAR	Cisco CDR Analysis and Reporting; Cisco CDR 分析とレポート
CAS	Channel Associated Signaling; 個別線信号方式
CBWFQ	クラスベースの重み付け均等化キューイング
CCA	Clear Channel Assessment
CCD	Call Control Discovery（呼制御ディスカバリ）
CCS	Common Channel Signaling; 共通線信号方式
CDI	Cisco AMP の統合
CDP	Cisco Discovery Protocol
CDR	Call Detail Record; コール詳細レコード
CER	Cisco Emergency Responder
CGI	Common Gateway Interface
CIF	Common Intermediate Format
CIR	Committed Information Rate; 認定情報レート
CKM	Cisco Centralized Key Management
CLEC	Competitive Local Exchange Carrier; 競争的地域通信事業者

CLID	Calling Line Identifier; 発呼回線 ID
CM	Cisco Unified Communications Manager（Unified CM）
CMC	Client Matter Code（クライアント識別コード）
CME	Cisco Unified Communications Manager Express（Unified CME）
CMI	Cisco Messaging Interface
CMM	Cisco Communication Media Module; Cisco コミュニケーション メディア モジュール
CMR	Call Management Record; 呼管理レコード
CMR	Collaboration Meeting Room
CO	Central Office; セントラル オフィス
COM	Component Object Model; コンポーネント オブジェクト モデル
COP	Cisco Option Package
COR	Class Of Restriction; 制限クラス
CoS	サービス クラス
CPCA	Cisco Unity Personal Assistant
CPI	Cisco Product Identification tool; シスコ製品識別ツール
CPL	Call Processing Language; 呼処理言語
CPN	Calling Party Number; 発番号
CRM	Customer relationship management; カスタマー リレーションシップ マネージメント
CRS	Cisco Customer Response Solution; シスコ カスタマー応答ソリューション
cRTP	Compressed Real-Time Transport Protocol; RTP ヘッダー圧縮
CSF	Client Services Framework
CSTA	Computer-Supported Telecommunications Applications
CSUF	Cross-Stack UplinkFast
CSV	Comma-Separated Value; カンマ区切り値
[CTI]	Computer Telephony Integration; コンピュータ テレフォニー インテグレーション
CTL	証明書信頼リスト
CUBE	Cisco Unified Border Element（以前の Cisco Multiservice IP-to-IP Gateway（IP-IP ゲートウェイ））
CUE	Cisco Unity Express
CUMI	Cisco Unity Connection Messaging Interface

CUPI	Cisco Unity Connection Provisioning Interface; Cisco Unity Connection プロビジョニング インターフェイス
CUSP	Cisco Unified SIP Proxy
CVTQ	Cisco Voice Transmission Quality
CWA	Microsoft Office Communicator Web Access

D

DC	Domain Controller; ドメイン コントローラ
DDNS	Dynamic Domain Name Server; ダイナミック ドメイン ネーム サーバ
DDR	Delayed Delivery Record
DECT	Digital Equipment Cordless Telephony
DFS	Dynamic Frequency Selection; 動的周波数選択
DHCP	ダイナミック ホスト コンフィギュレーション プロトコル
DID	Direct Inward Dial; 直通社内通話
DIT	Directory Information Tree; ディレクトリ インフォメーション ツリー
DMVPN	Dynamic Multipoint Virtual Private Network; Dynamic Multipoint バーチャル プライベート ネットワーク
DMZ	非武装地帯
[DN]	ディレクトリ番号
DNIS	Dialed Number Identification Service; 着信番号識別サービス
DNS	ドメイン ネーム システム
DoS	Denial of Service; サービス拒否
DPA	Digital PBX Adapter
DRS	Disaster Recovery System
DSCP	DiffServ コード ポイント
DSE	Digital Set Emulation
DSP	デジタル シグナル プロセッサ
DTIM	Delivery Traffic Indicator Message
DTLS	Datagram Transport Layer Security プロトコル

DTMF Dual Tone MultiFrequency

DTPC Dynamic Transmit Power Control; ダイナミック伝送パワー コントロール

DUC Domino Unified Communications サービス

E

E-SRST Enhanced Survivable Remote Site Telephony

E&M 受信（recEive）と送信（transMit）、または Ear and Mouth

EAP Extensible Authentication Protocol

EAPOL Extensible Authentication Protocol over LAN

EC Echo Cancellation; エコー キャンセレーション

ECC Extended Call Context; 拡張コール コンテキスト

ECDSA Elliptical Curve Digital Signature Algorithm; 楕円曲線デジタル署名アルゴリズム

ECM Error Correction Mode; エラー訂正モード

ECS Empty Capabilities Set

EI Enhanced Image

EIGRP Enhanced Interior Gateway Routing Protocol

ELCAC 拡張位置のコール アドミッション制御

ELIN Emergency Location Identification Number; 緊急ロケーション識別番号

EM エクステンション モビリティ（Extension Mobility）

EMCC クラスタ間のエクステンション モビリティ（Extension Mobility Cross Cluster）

ER Cisco Emergency Responder

ERL Emergency Response Location; 緊急応答ロケーション

ESF Extended Super Frame; 拡張スーパー フレーム

F

FAC 強制承認コード

FCC Federal Communications Commission; 米国連邦通信委員会

FCoE Fibre Channel over Ethernet; ファイバ チャネル オーバー イーサネット

FECC	遠端カメラ制御
FIFO	First-In, First-Out; ファーストイン ファーストアウト
[FQDN]	完全修飾ドメイン名
FR	フレーム リレー
FTP	File Transfer Protocol
FWSM	Firewall Services Module
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station

G

GARP	Gratuitous Address Resolution Protocol
GC	Global Catalog; グローバル カタログ
GDPR	Global Dial Plan Replication; グローバル ダイヤル プラン レプリケーション
GKTMP	Gatekeeper Transaction Message Protocol
GLBP	Gateway Load Balancing Protocol
GMS	Greeting Management System; グリーティング管理システム
GPO	Group Policy Object; グループ ポリシー オブジェクト
GPRS	General Packet Radio Service
GSB	Global Site Backup; グローバル サイト バックアップ
GSM	Global System for Mobile Communication
GSS	Global Site Selector
GUI	Graphical User Interface（グラフィカル ユーザ インターフェイス）
GUP	Gatekeeper Update Protocol

H

H.225D	H.225 Daemon; H.225 デーモン
HDLC	High-Level Data Link Control; ハイレベル データリンク コントロール
HMS	Hardware Media Server

HP	Hewlett-Packard
HSRP	Hot Standby Router Protocol; ホットスタンバイ ルータ プロトコル
HTTP	ハイパーテキスト転送プロトコル
HTTPS	HTTP Secure
HVD	Hosted virtual desktop; ホストされた仮想デスクトップ
Hz	Hertz; ヘルツ

I

IANA	Internet Assigned Numbers Authority
IAPP	Inter-Access Point Protocol; アクセス ポイント間プロトコル
ICA	Independent Computing Architecture
ICCS	Intra-Cluster Communication Signaling; イントラクラスタ コミュニケーション シグナリング
ICE	Interactive Connectivity Establishment
ICMP	Internet Control Message Protocol; インターネット制御メッセージ プロトコル
ICS	IBM Cabling System; IBM 配線システム
[ICT]	InterCluster Trunk; クラスタ間トランク
IdP	アイデンティティ プロバイダー
IE	Information Element; 情報要素
IETF	インターネット技術タスク フォース
IGMP	Internet Group Management Protocol; インターネット グループ管理プロトコル
IIS	Microsoft Internet Information Server
ILS	Intercluster Lookup Service; クラスタ間検索サービス
IM	インスタント メッセージ
IMAP	Internet Message Access Protocol
IMS	IP Multimedia Subsystem; IP マルチメディア サブシステム
IntServ	Integrated Service; 統合サービス
IntServ/DiffServ	Integrated Service/Differentiated Service; 統合サービス/ディファレンシエーテッド サービス
IOPS	Input/output operations per second; 1 秒当たりの入出力処理

IP	インターネット プロトコル
IPCC	Cisco IP Contact Center; シスコ IP コンタクト センター
IPMA	Cisco IP Manager Assistant
IPPM	Cisco IP Phone Messenger
IPSec	IP Security
IP SLA VO	IP Service Level Agreement Video Operation; IP サービス レベル契約ビデオ操作
IPVMS	Cisco IP Voice Media Streaming Application
ISO	International Standards Organization; 国際標準化機構
ISR	Integrated Services Router; サービス統合型ルータ
ITEM	CiscoWorks IP Telephony Environment Monitor
ITL	初期信頼リスト
ITU	国際電気通信連合
IVR	Interactive voice response（音声自動応答装置）

J

JCF	Jabber Client Framework; Jabber クライアント フレームワーク
JID	Jabber ID
JTAPI	Java Telephony Application Programming Interface; Java テレフォニー API

K

kbps	Kilobits per second; キロビット/秒
KEM	Key Expansion Module; キー拡張モジュール
KPML	Key Press Markup Language

L

LAN	Local Area Network; ローカル エリア ネットワーク
LBM	Location Bandwidth Manager; ロケーション帯域幅マネージャ
LBR	Low Bit-Rate; 低ビット レート

LCD Liquid Crystal Display; 液晶ディスプレイ

LCF Location Confirm; ロケーション確認

LCS Live Communications Server

LDAP Lightweight Directory Access Protocol

LDAPS LDAP over SSL

LDIF LDAP Data Interchange Format

LDN Listed Directory Number

LEAP Lightweight Extensible Authentication Protocol

LEC Local Exchange Carrier; 地域通信事業者

LFI Link Fragmentation and Interleaving; リンク フラグメンテーション/インターリーブ

LHS Left-hand side; 左側

LLDP Link Layer Discovery Protocol

LLDP-MED Link Layer Discovery Protocol for Media Endpoint Devices

LLQ Low-Latency Queuing; 低遅延キューイング

LRG ローカル ルート グループ

LRJ Location Reject; ロケーション拒否

LRQ Location Request; ロケーション要求

LSC Locally Significant Certificate; ローカルで有効な証明書

LUN Logical unit number; 論理ユニット番号

LWAP Light Weight Access Point; Lightweight アクセスポイント

LWAPP Light Weight Access Point Protocol; Lightweight アクセス ポイント プロトコル

M

MAC Media Access Control; メディア アクセス コントロール

MAN Metropolitan Area Network; メトロポリタン エリア ネットワーク

Mbps Megabits per second; メガビット/秒

MCM Multimedia Conference Manager

MCS Media Convergence Server

MCU	マルチポイント コントロール ユニット
MDN	Mobile Data Network; モバイル データ ネットワーク
MDS	Mobile Data Services
MFT	MultiFlex Trunk; マルチフレックス トランク
MGCP	Media Gateway Control Protocol
MIB	管理情報ベース
MIC	製造元でインストールされる証明書
MIME	Multipurpose Internet Mail Extension
MIPS	Millions of Instructions Per Second
MISTP	Multiple Instance Spanning Tree Protocol
MITM	Man-In-The-Middle; 中間者
MLA	Cisco Multi-Level Administration; Cisco マルチレベル管理
MLP	Multilink Point-to-Point Protocol; マルチリンク ポイントツーポイント プロトコル
MLPP	Multilevel Precedence and Preemption
MLPPP	Multilink Point-to-Point Protocol; マルチリンク ポイントツーポイント プロトコル
MLTS	Multi-Line Telephone System
MMoIP	Multimedia Mail over IP; マルチメディア メール オーバー IP
MMP	Mobile Multiplexing Protocol
MOC	Microsoft Office Communicator
MoH	保留音
MOS	Mean Opinion Score; 平均オピニオン評点
MPLS	マルチプロトコル ラベル スイッチング
MRD	メディア ルーティング ドメイン（Media Routing Domain）
MRG	Media Resource Group; メディア リソース グループ
MRGL	Media Resource Group List; メディア リソース グループ リスト
ms	Millisecond; ミリ秒
MSI	Media Services Interface; メディア サービス インターフェイス
MSP	Managed Service Provider; 管理対象サービス プロバイダー
MSP	Media Services Proxy; メディア サービス プロキシ

MTLS Mutual Transport Layer Security

MTP Media Termination Point; メディア ターミネーション ポイント

mW milli-Watt; ミリワット

MWI メッセージ受信インジケータ

MXE メディア エクスペリエンス エンジン

N

NAS Network Attached Storage

NAT ネットワーク アドレス変換

NDR Non-Delivery Receipt

NENA National Emergency Number Association

NFAS Non-Facility Associated Signaling

NIC Network Interface Card; ネットワーク インターフェイス カード

NOC Network Operations Center

NPA Numbering Plan Area; 番号計画エリア

NSE Named Service Event

NSF Network Specific Facilities

NTE Named Telephony Event

NTLP Network Transmission Loss Plan

NTP ネットワーク タイム プロトコル

O

OBTP One Button To Push

OCS Microsoft Office Communicator Server

ORA Open Recording Architecture

OSPF Open Shortest Path First

OU Organizational Unit; 組織単位

OVA	Open Virtualization Archive
OWA	Outlook Web Access

P

PAC	Protected Access Credential
PAK	製品アクティベーション キー
PBX	Private Branch eXchange; 構内交換機
PC	Personal Computer; パーソナル コンピュータ
PCAP	Phone Control and Presence
PCI	Peripheral Component Interconnect
PCM	Pulse Code Modulation; パルス符号変調
PCoIP	PC over IP
PCTR	Personal Call Transfer Rule; パーソナル着信転送ルール
PD	Powered Device; 受電デバイス
PHB	Per-Hop Behavior; ホップごとのふるまい
pii	個人情報
[PIN]	Personal Identification Number; 個人識別番号
PINX	Private Integrated services Network eXchange
PIX	Private Internet eXchange
PKI	Public Key Infrastructure; 公開キー インフラストラクチャ
PLAR	Private Line Automatic Ringdown
POD	Piece of Data; データの一部分
PoE	Power over Ethernet
POTS	Plain Old Telephone Service（一般電話サービス）
PPP	Point-to-Point Protocol; ポイントツーポイント プロトコル
pps	Packets per second; 1 秒あたりのパケット数
PQ	プライオリティ キュー
PRACK	Provisional Reliable Acknowledgements

PRI	Primary Rate Interface（一次群速度インターフェイス）
PSAP	Public Safety Answering Point
PSE	Power Source Equipment
PSK	Pre-Shared Key; 事前共有キー
PSTN	Public Switched Telephone Network; 公衆電話交換網
PVC	Permanent Virtual Circuit; 相手先固定接続

Q

QBE	Quick Buffer Encoding
QBSS	QoS Basic Service Set
QoS	Quality of Service
QSIG	Q signaling

R

RADIUS	Remote Authentication Dial-In User Service
RAS	Registration Admission Status
RBAC	ロールベース アクセス コントロール
RCC	Remote Call Control; リモート呼制御
RCP	Remote Copy Protocol; リモート コピー プロトコル
RDNIS	Redirected Dialed Number Information Service
REST	Representational State Transfer
RF	Radio Frequency; 無線周波数
RFC	コメント要求
RHS	Right-hand side; 右側
RIM	Research In Motion
RIP	Routing Information Protocol
RIS	Real-time Information Server

RMA	リモートからのモバイル アクセス
RMTP	Reliable Multicast Transport Protocol
RoST	RSVP over SIP Trunks
RSA	Rivest, Shamir, and Adelman
RSNA	Reservationless Single Number Access
RSP	Route/Switch Processor; ルート スイッチ プロセッサ
RSSI	Relative Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
RSVP	リソース予約プロトコル
RTCP	Real-Time Transport Control Protocol
RTMP	Real-Time Messaging Protocol
RTMT	Cisco Real-Time Monitoring Tool
RTP	リアルタイム トランスポート プロトコル
RTSP	Real Time Streaming Protocol
RTT	Round-Trip Time; ラウンドトリップ時間

S

S1、S2、S3、および S4	Severity levels for service requests; サービス リクエストのシビラティ
SaaS	Software-as-a-Service
SAF	Service Advertisement Framework
SAML	Security Assertion Markup Language; セキュリティ アサーション マークアップ ランゲージ
SAN	Storage area networking; ストレージ エリア ネットワーキング
SBC	Session Border Controller; セッション ボーダー コントローラ
SCCP	Skinny Client Control Protocol
SCSI	Small Computer System Interface; 小型計算機システム インターフェイス
SDI	System Diagnostic Interface
SDK	Software Development Kit; ソフトウェア開発キット

SDL	Signaling Distribution Layer
SDP	Session Description Protocol
SE	Cisco Systems Engineer; シスコのシステム エンジニア
SF	Super Frame; スーパー フレーム
SFTP	セキュア ファイル転送プロトコル
SI	Standard Image
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SIS	Symbian Installation System
SIW	Service Inter-Working; サービス インターワーキング
SLA	Service level agreement; サービス レベル契約
SLA VO	IP Service Level Agreement Video Operation; IP サービス レベル契約ビデオ操作
SLB	Server Load Balancing; サーバ ロード バランシング
SLDAP	Secure LDAP
SMA	Segmented Meeting Access; セグメント化会議アクセス
SMDI	Simplified Message Desk Interface
SME	Cisco Unified Communications Manager Session Management Edition
SMS	Short Message Service; ショート メッセージ サービス
SMTP	Simple Mail Transfer Protocol
SNMP	簡易ネットワーク管理プロトコル
SOAP	Simple Object Access Protocol
SPA	Shared Port Adapter; 共有ポート アダプタ
SPAN	スイッチド ポート アナライザ
SQL	Structured Query Language; 構造化照会言語
SRE	Cisco Services-Ready Engine
SRND	Solution Reference Network Design; ソリューション リファレンス ネットワーク デザイン
SRST	Survivable Remote Site Telephony
SRSV	Survivable Remote Site Voicemail
SRTP	セキュア リアルタイム転送プロトコル

SRV	サーバ
SS7	Signaling System 7
SSID	Service Set IDentifier
SSL	Secure Sockets Layer
SSM	Cisco Smart Software Manager
SSO	シングル サインオン
STP	Spanning Tree Protocol; スパニングツリー プロトコル
STUN	Session Traversal Utilities for NAT; NAT のためのセッション トラバーサル ユーティリティ
SUP1	Cisco Supervisor Engine 1
SUP2	Cisco Supervisor Engine 2
SUP2+	Cisco Supervisor Engine 2+
SUP3	Cisco Supervisor Engine 3

T

TAC	Cisco Technical Assistance Center
TAPI	Telephony Application Programming Interface
TCD	Telephony Call Dispatcher; テレフォニー コール ディスパッチャ
TCER	Total Character Error Rate
TCL	Tool Command Language
[TCP]	伝送制御プロトコル
TCS	Terminal Capabilities Set; 端末機能セット
TDD	Telephone Device for the Deaf
TDM	Time-Division Multiplexing; 時分割多重
TEHO	Tail-End Hop-Off; テールエンド ホップオフ
TFTP	トリビアル ファイル転送プロトコル
TIP	Telepresence Ineroperability Protocol; テレプレゼンス相互運用プロトコル
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security

TMS	Cisco TelePresence Management Suite
TMSXE	Cisco TelePresence Management Suite Extension for Microsoft Exchange
ToD	時刻
ToS	Type of service; タイプ オブ サービス
TPC	Transmit Power Control; 伝送パワー コントロール
TRaP	Telephone Record and Playback; 電話での録音および再生
TRC	Tested Reference Configuration; テスト済みリファレンス構成
TRP	信頼できるリレー ポイント（Trusted Relay Point）
TSP	電話会議サービス プロバイダー
TTL	Time To Live; 存続可能時間
TTS	Text-To-Speech; テキストツースピーチ
TTY	Terminal Teletype; ターミナル テレタイプ
TUI	Telephony User Interface; テレフォニー ユーザ インターフェイス
TURN	Traversal Using Relays around NAT; NAT に関するリレーを使用したトラバーサル

U

UAC	ユーザ エージェント クライアント
UAS	ユーザ エージェント サーバ
UCCN	Unified Client Change Notifier
UCS	Cisco Unified Computing System
UDC	Universal Data Connector
UDLD	UniDirectional Link Detection; 単方向リンク検出
UDP	ユーザ データグラム プロトコル
UDPTL	Unnumbered Datagram Protocol Transport Layer
UDS	User Data Service; ユーザ データ サービス
UMTS	Universal Mobile Telecommunications System
UN	Unsolicited SIP Notify
UNC	Universal Naming Convention; 汎用命名規則

UP	ユーザ優先度
UPS	Uninterrupted Power Supply; 無停電電源
URI	ユニフォーム リソース識別子
USB	Universal Serial Bus
UTIM	Cisco Unity Telephony Integration Manager
UTP	Unshielded Twisted Pair; シールドなしツイスト ペア
UUIE	User-to-User Information Element

V

V3PN	Cisco Voice and Video Enabled Virtual Private Network; シスコ音声ビデオが利用可能なバーチャル プライベート ネットワーク
VAD	Voice Activity Detection; 音声アクティビティ検出
VAF	Voice-Adaptive Fragmentation
VATS	Voice-Adaptive Traffic Shaping
VCS	Cisco TelePresence Video Communication Server
[VDI]	Virtual Desktop Infrastructure
VDS	VMware vSphere 分散スイッチ
VIC	Voice Interface Card; 音声インターフェイス カード
VLAN	Virtual Local Area Network; バーチャル ローカルエリア ネットワーク
VMO	Cisco ViewMail for Outlook
VoIP	Voice over IP
VoPSTN	Voice over the PSTN
VoWLAN	Voice over Wireless LAN（WLAN）
VPIM	Voice Profile for Internet Mail プロトコル
VPN	Virtual Private Network; バーチャル プライベート ネットワーク
VRRP	Virtual Router Redundancy Protocol; 仮想ルータ冗長プロトコル
VUI	Voice User Interface; 音声ユーザ インターフェイス
VVB	Cisco Virtualized Voice Browser
VWIC	Voice/WAN Interface Card; 音声/WAN インターフェイス カード

VXC	Cisco Virtualization Experience Client
VXI	Cisco Virtualization Experience Infrastructure
VXME	Virtualization Experience Media Engine

W

WAN	Wide Area Network; ワイド エリア ネットワーク
WebDAV	Web-Based Distributed Authoring and Versioning
WEP	Wired Equivalent Privacy
WFQ	Weighted Fair Queuing; 重み付け均等化キューイング
WINS	Windows Internet Naming Service
WLAN	Wireless Local Area Network; ワイヤレス ローカル エリア ネットワーク
WLC	Wireless LAN controller; ワイヤレス LAN コントローラ
WLSM	Cisco Wireless LAN Services Module
WMM	Wi-Fi Multimedia
WMM TSPEC	Wi-Fi Multimedia Traffic Specification
WPA	Wi-Fi Protected Access

X

XCP	Extensible Communications Platform
XML	拡張マークアップ言語
XMPP	Extensible Messaging and Presence Protocol

き

共存	同じ物理的な場所にある複数のデバイスを指します。これらのデバイスの間に WAN または MAN 接続はありません。
共存	同じサーバまたは仮想マシン上で複数のサービスまたはアプリケーションが実行されている状態

シンボル

数値

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

に

ね

は

ひ

ふ

へ

ほ

ま

み

む

め

も

ゆ

よ

ら

り

る

れ

ろ

わ