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

Cisco Unified Communications Solution Reference Network Design (SRND)

Cisco Unified Communications Manager Release 7.*x*
2010 年 11 月 15 日

Text Part Number: OL-16394-08-J

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

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

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

このマニュアルに記載されているデザイン、仕様、表現、情報、および推奨事項（総称して「デザイン」）は、障害も含めて本マニュアル作成時点のものです。シスコシステムズおよびそのサプライヤは、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、一切の保証の責任を負わないものとします。いかなる場合においても、シスコシステムズおよびそのサプライヤは、このデザインの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはそのサプライヤに知らされていても、それらに対する責任を一切負わないものとします。

デザインは予告なしに変更されることがあります。このマニュアルに記載されているデザインの使用は、すべてユーザ側の責任になります。これらのデザインは、シスコシステムズ、そのサプライヤ、パートナーの技術的な助言や他の専門的な助言に相当するものではありません。ユーザは、デザインを実装する前に技術アドバイザーに相談してください。シスコによるテストの対象外となった要因によって、結果が異なることがあります。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco Unified Communications SRND （Cisco Unified Communications Manager 7.x）
© 2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2010–2011, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

はじめに

このマニュアルでは、Cisco Unified Communications Manager 7.*x*（7.0 およびそれ以降の 7.*x* リリースのすべて）に基づいて Cisco Unified Communications システムを展開するための、設計上の考慮事項とガイドラインについて説明しています。

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

- Cisco Unified Communications Manager（Unified CM）、旧 Cisco Unified CallManager
- Cisco Unified Communications Manager Business Edition（Unified CMBE）
- Cisco Unity、Unity Express、および Unity Connection
- Cisco Unified MeetingPlace および Unified MeetingPlace Express
- Cisco Unified Video Advantage
- Cisco Unified Presence
- Cisco Unified Mobility

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

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

新規情報、またはこのリリースからの変更情報

（注） 特に指定のない限り、このマニュアルの情報は、Cisco Unified Communications Manager 7.*x*（7.0 およびそれ以降の 7.*x* リリースのすべて）に適用されます。Cisco Unified Communications Manager のさまざまなリリースにおける違いは、具体的にマニュアルに記載されています。

次の章には、このマニュアルの現在のリリースで更新された情報、またはこのマニュアルの以前のリリースから大幅に変更された情報が記載されています。

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

マニュアルの変更履歴

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

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

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

次の表では、このマニュアルに対する改訂の履歴をリストしています。

改訂日	備考
2010/11/15	Cisco Unified MeetingPlace のキャパシティとサイジングの情報を更新しました。
2010/07/21	一部の図に細かい修正を加えました。
2010/06/04	小規模のさまざまな更新およびエラー訂正
2009/11/06	「Cisco Collaboration クライアントおよびアプリケーション」（P.23-1）への新しい章の追加、および Cisco Unified IP Phone 8900 シリーズと 9900 シリーズに関する情報の追加
2009/09/18	Cisco Unified Communications システム Release 7.1(3) に関する更新内容
2009/05/22	Cisco Unified Communications システム Release 7.1(2) に関する更新内容
2008/12/15	「新規情報、またはこのリリースからの変更情報」（P.xxxiv）に示されている更新内容
2008/08/05	Cisco Unified Communications Manager Release 7.0 を対象にしたこのマニュアルの初版です。

マニュアルの入手方法およびテクニカル サポート

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

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

シスコ製品のセキュリティ

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

米国の輸出規制の詳細については、次の URL で参照できます。

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

CHAPTER 1

概要

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

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

- IP テレフォニー

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

- カスタマー コンタクト センター

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

- ビデオ テレフォニー

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

- リッチメディア会議

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

- モビリティ

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

- TelePresence

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

- サードパーティ製アプリケーション

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

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

- Cisco Unified Communications Manager（Unified CM）、旧 Cisco Unified CallManager
- Cisco Unified Communications Manager Business Edition（Unified CMBE）
- Cisco Unified MeetingPlace および MeetingPlace Express
- Cisco Unity および Unity Express
- Cisco Unified Video Advantage
- Cisco Unified Communications エンドポイント
- Cisco Unified Presence
- Cisco Unified Communications アプリケーション

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

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

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

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

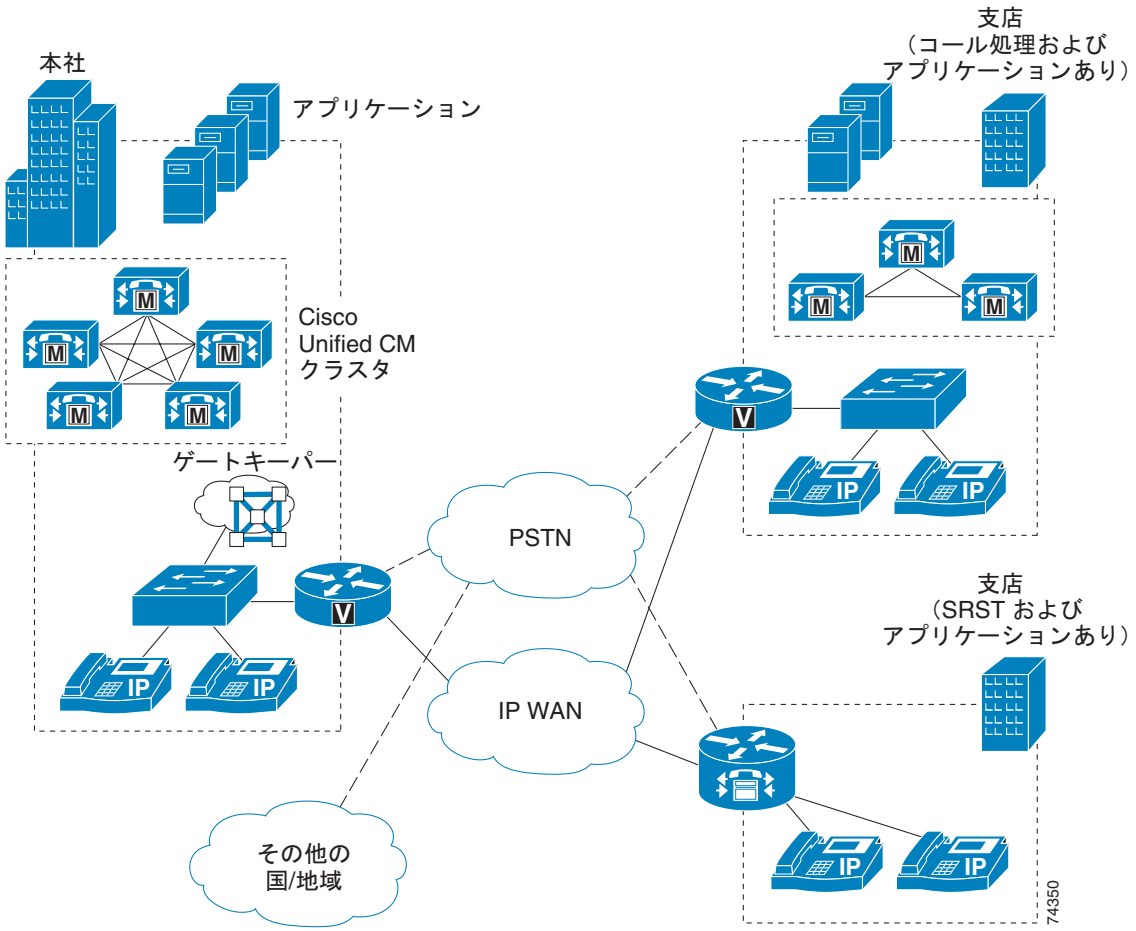
http://www.cisco.com

Cisco Unified Communications の概要

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

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

図 1-1　一般的な Unified Communications の配置



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

- 「Cisco IP ネットワーク インフラストラクチャ」（P.1-4）
- 「QoS」（P.1-4）
- 「コール処理エージェント」（P.1-4）
- 「通信エンドポイント」（P.1-5）
- 「プレゼンス」（P.1-6）
- 「会議、メッセージング、およびコラボレーション機能」（P.1-7）
- 「アプリケーション」（P.1-8）
- 「セキュリティ」（P.1-10）
- 「ネットワーク管理」（P.1-10）

Cisco IP ネットワーク インフラストラクチャ

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

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

QoS

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

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

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

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

コール処理エージェント

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

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

- 単一サイト コール処理モデル

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

- 集中型コール処理を使用するマルチサイト WAN モデル

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

- 分散型コール処理を使用するマルチサイト WAN モデル

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

- IP WAN を介したクラスタ化

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

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

通信エンドポイント

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

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

- ソフトウェアベースのエンドポイント

  Cisco IP Communicator および Cisco Unified Personal Communicator は、ご使用のコンピュータをフル機能の IP Phone に変えるデスクトップ アプリケーションです。これらのアプリケーションには、コール トラッキング、デスクトップ コラボレーション、およびオンライン電話帳からのワンクリック ダイヤルといった機能が追加されています。Cisco IP Communicator は、拡張されたテレフォニー機能を PC から提供するソフトウェアベースのアプリケーションです。旅行時の補助的な電話機、在宅勤務用のデバイス、メインのデスクトップ電話機などとして機能することで、さまざまなお客様のニーズに適合するよう設計されています。Cisco Unified Personal Communicator

では、幅広い通信アプリケーションとサービスが 1 つのデスクトップ コンピュータ アプリケーションとして統合され、音声、ビデオ、Web 会議、コール管理、電話帳、在席情報に対する強力なコミュニケーション ツールに迅速かつ簡単にアクセスできます。

- ビデオ テレフォニー エンドポイント

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

- ワイヤレス（モビリティ）エンドポイント

  Cisco Wireless IP Phones 7920 および 7921G は、シスコの IP Phone ファミリを 10/100 イーサネットから Wireless LAN（WLAN; 無線 LAN）へと広げます。どちらも、組み込み型の無線アンテナを備えた、ハードウェアベースの電話機です。Cisco Unified Wireless IP Phone 7920 はネットワークへの 802.11b 無線 LAN 接続を可能にし、Cisco Unified Wireless IP Phone 7921G はネットワークへの 802.11b、802.11g、または 802.11a 無線 LAN 接続を可能にします。これらの電話機は、他の Cisco Unified IP Phone と同様の機能を提供します。

各種のエンドポイントの詳細については、「Unified Communications エンドポイント」（P.20-1）を参照してください。

プレゼンス

*プレゼンス*とは、ユーザが特定のデバイス セットで通信する能力とその意志を意味します。Cisco Unified Presence は、Cisco Unified Communications システムの価値を高める多くのコンポーネントから構成されており、ユーザの可用性ステータスおよびコミュニケーションに関する情報を提供します。ユーザの可用性ステータスは、ユーザが電話機などの通信デバイスをアクティブに使用しているかどうかを示します。ユーザの通信能力は、ビデオ会議、Web コラボレーション、インスタント メッセージング、基本オーディオなど、ユーザが使用できる通信の種類を示します。

ユーザ ステータスの変更は、ユーザによるキーボード操作、電話機の使用、またはネットワークへのデバイス接続などを認識することによって自動的に判断されます。このステータス情報は、すべての利用可能なソースから収集され、プライバシー ポリシーが適用され、現在のステータスが集約、同期されてから、サーバに保存されます。デスクトップ アプリケーション、カレンダー アプリケーション、およびデバイスは、ユーザ ステータス情報にアクセスし、より適切な通信の判断に役立つように、エンド ユーザにリアルタイムの更新を提供します。

ステータス情報は、デバイスやユーザが実行可能な機能（音声、ビデオ、Web コラボレーションなど）と、デバイスやユーザの状態（利用可能、ビジー、通信中など）の両方を示します。Presence ステータスは、コンピュータへのログインや電話機のオフフックなどの自動イベントによって決定されるか、またはユーザがステータス変更ピックリストから Do Not Disturb を選択したなど、ユーザによるステータス変更の明確な通知イベントによって決定されます。

Cisco Unified Communications システムの Presence 機能の詳細については、「Cisco Unified Presence」（P.22-1）を参照してください。

会議、メッセージング、およびコラボレーション機能

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

- 会議

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

- ユニファイド メッセージング

  時分割多重（TDM）ベースの専用メッセージング ソリューションとは異なり、Cisco Unified Communications プラットフォームは、シスコの標準ベースの音声およびデータ通信用オープンプロトコル アーキテクチャを基盤としています。この標準ベース サービス プラットフォームは、Voice over IP（VoIP）、インターネット FAX、Store-and-Forward ボイスメール、電子メールなどの同期および非同期メッセージ タイプを、共通メッセージ ストアおよびディレクトリで組み合わせています。この方式により、異なるボイスメールや電子メール システムなど、異なるメッセージ ストアやディレクトリを同期させる必要がなくなるため、運用およびメンテナンスのコストを大幅に削減できます。サードパーティ製ボイスメール システムと Unified CM との統合の詳細については、「Third-Party Voicemail Design」（P.12-1）を参照してください。Cisco Unity、Unity Express、および Unity Connection と Unified CM との統合の詳細については、「シスコの音声メッセージング」（P.13-1）を参照してください。

- ビデオ テレフォニー

  ビデオ テレフォニー機能が Cisco Unified CM に完全に統合され、シスコおよびシスコの戦略的パートナーから新しいビデオ エンドポイントも入手できるようになりました。ビデオ コールおよび会議は、IP Phone で音声コールを発信するのと同じくらい簡単になりました。Unified CM でのビデオ機能の詳細については、「IP ビデオ テレフォニー」（P.16-1）を参照してください。

- マルチメディア コラボレーション

  Cisco Unified MeetingPlace および Cisco Unified MeetingPlace Express は、音声、ビデオ、および Web 会議機能を統合した完全なリッチメディア会議アプリケーションであり、リモート会議を対面式の会議と同じくらい自然なものにします。MeetingPlace と Unified CM の統合の詳細については、「Cisco Unified MeetingPlace」（P.14-1）、および 「Cisco Unified MeetingPlace Express」（P.15-1）を参照してください。

- TelePresence

  Cisco TelePresence は、高度なビジュアル、オーディオ、およびコラボレーション テクノロジーを利用して、統合ネットワーク上で「生の」会議の臨場感を創り出す革新的なソリューションです。Cisco TelePresence は、現在の企業で採用されている標準 IP テクノロジーを利用して、統合音声、ビデオ、およびデータ ネットワーク上で動作します。このシステムは、ブロードバンド接続を使用して、支店との間で高品質のリアルタイム音声およびビデオ通信をサポートします。また、高品位ビデオなどの広帯域アプリケーションの Quality of Service（QoS）、セキュリティ、信頼性、および高可用性を保証する機能を提供します。Cisco TelePresence については本マニュアルでは解説しませんが、次の Web サイトから詳しい情報を入手できます。

  http://www.cisco.com/en/US/products/ps7060/index.html

アプリケーション

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

- IP Phone サービス

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

- エクステンション モビリティ

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

- Cisco Unified Communications Manager Assistant

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

- Attendant Console

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

- WebDialer

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

これらのアプリケーションの詳細については、「Cisco Unified CM アプリケーション」（P.24-1）を参照してください。

上記の企業テレフォニー ユーザ用アプリケーションに加えて、Cisco のモビリティ アプリケーションは、Cisco Unified Communications 環境の機能をあらゆる場所の外勤職員に提供します。Cisco Unified Communications ソリューションのモビリティ機能は、Cisco Unified Mobility アプリケーショ

ン サーバから提供されます。Unified Mobility サーバは、Java Telephony Application Programming Interface（JTAPI）および AVVID XML Layer（AXL）を介して Cisco Unified CM と通信し、次のモビリティ アプリケーション機能を提供します。

- モバイル コネクト

  シングル ナンバー リーチとも呼ばれる Cisco Unified Mobility は、1 つの会社の電話番号への着信コールを、Cisco Unified Communications ユーザの IP デスクトップフォンおよび携帯電話に同時に転送します。モバイル コネクト ユーザは、着信コールをデスクトップフォンでも携帯電話でも受けることができ、通話中のコールを妨げることなく別の電話に転送することができます。

- 通話切替機能

  通話切替機能により、モビリティ コールの通話中に、携帯電話の保留、保留解除、転送、会議、およびリダイレクト コール パーク機能を呼び出すことができます。これらの機能は、携帯電話のキーによって呼び出され、保留音やカンファレンス ブリッジといった企業のメディア リソースを活用します。

- シングル企業ボイスメール ボックス

  シングル企業ボイスメール ボックスは、ユーザの会社の電話番号に着信し、さらに携帯電話に転送されたコールに応答がなかった場合に、携帯電話のボイスメール システムではなく、会社のボイスメール システムにコールを蓄積します。これにより、ボイスメール ボックスが 1 箇所に統合され、ユーザは複数のボイスメール システムでメッセージを確認する必要がなくなります。

- 2 ステージ ダイヤリング機能付きモバイル ボイス アクセスとエンタープライズ機能アクセス

  2 ステージ ダイヤリング機能付きモバイル ボイス アクセスとエンタープライズ機能アクセスによって、まるで会社の IP 卓上電話からかけているかのように、携帯電話から発信することができます。これらの機能により、企業は長距離電話や国際電話の料金を節約することができるうえ、中央で一括管理される詳細コールレコードによってユーザのコール発信を容易に追跡管理できるようになります。さらに、これらの機能によって、発信者 ID を送信する際にユーザの携帯電話番号を隠すことができます。代わりに、発信者 ID として、ユーザの会社の電話番号が送信されます。これによって、ユーザへの返信コールは会社の電話番号にかけられるため、コールを会社で一括管理できます。

Cisco Unified Mobile Communicator は、携帯電話の機能にアクセスし、これらの機能を制御するためのリッチ ユーザ インターフェイスとして、Cisco Unified Mobility Advantage ソフトウェアが稼動しているサーバと連携して動作するグラフィカル クライアントを提供します。このシステムは既存の社内 LDAP ディレクトリに統合されるため、ユーザはすべてのデバイス上で単一のクレデンシャル セットを使用できます。また、Cisco Unified Mobile Communicator と Unified Mobility Advantage の間のすべてのトラフィックは、Secure Socket Layer（SSL）プロトコルによって保護されます。Cisco Unified Mobile Communicator は、携帯電話ユーザに次の機能を提供します。

- 社内および個人ディレクトリへのアクセス
- プレゼンスとバディの会社との同期化
- 社内ボイスメールへのビジュアル アクセス
- デスクトップフォンの不在コール、発信コール、および受信コールの履歴確認
- セキュア Store-and-Forward テキスト メッセージング
- 会議通知の受信
- Cisco Unified CM を使用した Dial-via-office

Cisco Unified Mobility および関連アプリケーションの詳細については、「シスコ モビリティ アプリケーション」（P.25-1）を参照してください。

セキュリティ

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

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

Cisco Unified Communications ネットワークの詳細については、「音声セキュリティ」（P.19-1）を参照してください。

ネットワーク管理

ネットワーク管理は、さまざまなツール、アプリケーション、および製品によって構成され、ネットワーク システム管理者による新規および既存ネットワーク配置のプロビジョニング、運営、監視、および保守を支援します。ネットワーク管理は、システム管理者による各ネットワーク デバイスとネットワーク アクティビティの監視を支援し、問題をタイムリーに特定および調査することで、性能と生産性を高めるのに役立ちます。ネットワーク管理の標準的な段階は、計画（Planning）、設計（Design）、実装（Implementation）、および運用（Operation）です（PDIO）。ネットワーク管理者は、さまざまな管理段階を実装することで、音声、ビデオ、コンタクト センター、およびリッチメディア アプリケーションなどの Cisco Unified Communications アプリケーションの性能と可用性を戦略的に管理します。

Cisco Unified Communications Management Suite は、次の統合ツールを提供し、Cisco Unified Communications システムのテスト、配置、および監視を支援します。

- Cisco Unified Provisioning Manager（Unified PM）：IP コミュニケーション サービスの初期配置と運用開始のプロビジョニングを管理します。
- Cisco Unified Operations Manager（Unified OM）：Cisco Unified Communications システム全体の予防的および反応的な診断を備えた包括的な監視機能を提供します。
- Cisco Unified Service Monitor（Unified SM）：Cisco Unified Communications システムの音声品質を監視および評価するための信頼性の高い手段を提供します。
- Cisco Unified Service Statistics Manager（Unified SSM）：Cisco Unified Communications の配置用の高度な統計分析およびレポート機能を提供します。
- Cisco Monitor Manager（MM）：ユーザ数が 5 ～ 250 程度の中小企業（SMB）に配置でき、システムの主要デバイス パラメータをアクティブに監視します。
- Cisco Monitor Director（MD）：Cisco Monitor Manager（MM）と連携して動作し、管理対象となるサービス プロバイダ ロケーションにおける SMB サイトのアクティブ音声およびデータ ネットワーク管理をサポートします。
- Cisco netManager：SMB 環境に配置された Cisco Unified Communication システムに、管理、監視、および診断機能を提供します。

Cisco Unified Communications Management Suite の詳細については、「Network Management」（P.26-1）を参照してください。

CHAPTER 2

Unified Communications の配置モデル

この章では、Cisco Unified Communications Manager（Unified CM）の配置モデルについて説明します。以前のリリースの Cisco Unified CM での設計ガイドについては、次の Web サイトで入手可能な Unified Communications ソリューション リファレンス ネットワーク デザイン（SRND）のマニュアルを参照してください。

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

各 Cisco Unified Communications ソリューションは、Unified CM の配置モデルに基づいています。また、配置モデルのタイプは、次の 1 つ以上の要素に基づいています。

- コール処理エージェント クラスタの数
- IP Phone の数
- コール処理エージェント クラスタおよび IP Phone のロケーション

次の各項では、さまざまなタイプの配置モデルについて説明します。

この章の新規情報

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

表 2-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
Cisco Unified CM Session Management Edition	「Unified CM Session Management Edition」（P.2-19）
SRST モードの Cisco Unified Communications Manager Express（Unified CME）は、現在 Cisco Unity Express をサポート	「SRST モードの Unified CME のベスト プラクティス」（P.2-10）

表 2-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報 （続き）

新規トピックまたは改訂されたトピック	説明箇所
WAN を介した CTI Manager	「ローカル フェールオーバー配置モデル」（P.2-26）
サポートされているゲートウェイおよびリージョンの数の増加	「単一サイト」（P.2-2） 「集中型コール処理を使用するマルチサイト」（P.2-4） 「分散型コール処理を使用するマルチサイト」（P.2-15）

単一サイト

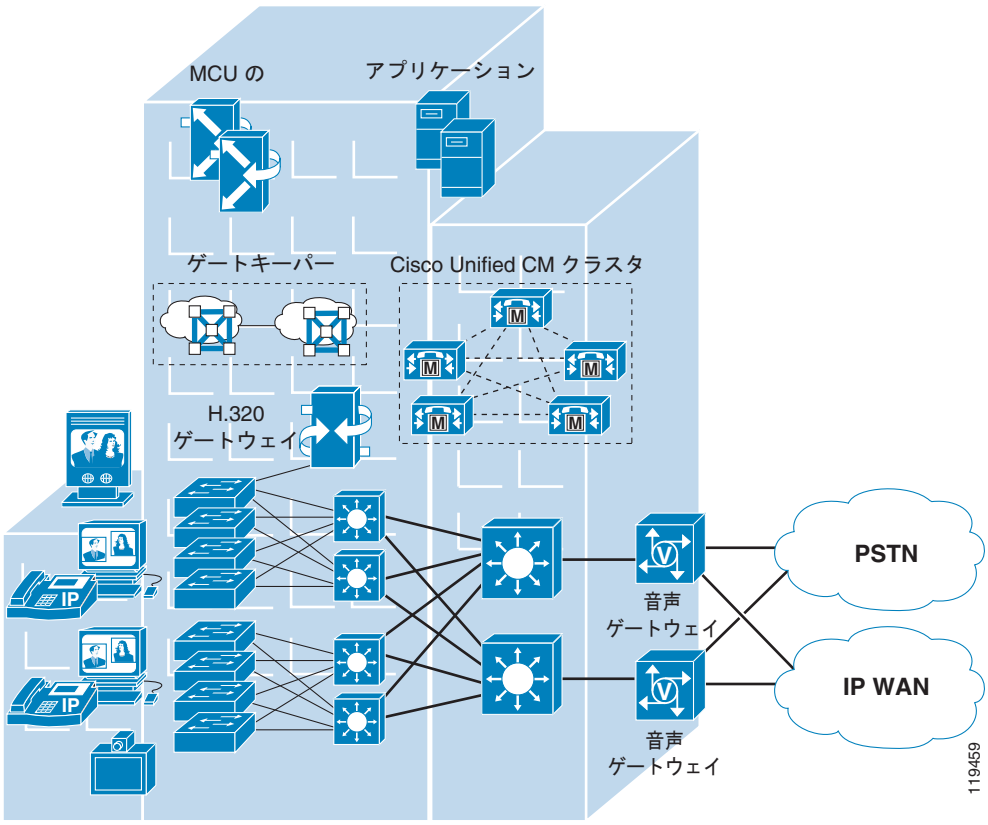
単一サイトで Cisco Unified Communications を実現する場合のモデルは、その単一サイト（キャンパス）に配置される 1 つのコール処理エージェント クラスタから構成されています。テレフォニー サービスは、IP WAN を使用して行われることは*ありません*。企業は、一般的に、LAN または MAN に対しては単一サイト モデルを配置して、サイト内の音声トラフィックを伝送しています。このモデルでは、コールが LAN または MAN を越えて発信される場合は、PSTN（公衆電話交換網）が使用されます。

単一サイト モデルの設計上の特長は、次のとおりです。

- 単一の Cisco Unified CM クラスタ。
- クラスタあたり最大 30,000 の設定済みおよび登録済み Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone または SCCP ビデオ エンドポイント。
- Unified CM クラスタあたり最大 2,100 のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H.323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）。
- すべてのサイト外部のコールに対して公衆網で対応。
- 会議、トランスコーディング、および Media Termination Point（MTP; メディア ターミネーション ポイント）に対してデジタル シグナル プロセッサ（DSP）リソースで対応。
- ボイスメール、ユニファイド メッセージング、Cisco Unified Presence、音声とビデオの各コンポーネント。
- レガシー Private Branch Exchange（PBX; 構内交換機）システムおよびボイスメール システムとの統合機能。
- コールを発信するためにゲートキーパーを必要とする H.323 クライアント、MCU、および H.323/H.320 ゲートウェイを、Cisco IOS ゲートキーパー（Cisco IOS Release 12.3(8)T 以降）に登録することが必要。Unified CM は H.323 トランクを使用してゲートキーパーと統合し、そこに登録された H.323 デバイスのコール ルーティングと帯域幅管理サービスを提供します。複数の Cisco IOS ゲートキーパーを使用して、冗長性を提供することもできます。
- マルチポイント ビデオ会議には MCU リソースが必要です。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。
- 公衆 ISDN 網上で H.320 ビデオ会議デバイスと通信するために H.323/H.320 ビデオ ゲートウェイが必要です。
- サイト内のデバイス間の広帯域オーディオ（G.711、G.722、Cisco Wideband Audio など）。
- サイト内のデバイス間の広帯域ビデオ（384 kbps 以上など）。7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec もサポートされます。

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

図 2-1　単一サイトの配置



単一サイト モデルのベスト プラクティス

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

- 一般的なインフラストラクチャ 構想に基づいて可用性および耐障害性を高めます。Cisco Unified Communications への迅速な移行、アプリケーションにビデオ ストリーミングやビデオ会議などを容易に統合、および Cisco Unified Communications の配置を拡張し、WAN または複数の Unified CM クラスタへのアクセスを可能にするには、インフラストラクチャを適切に構築する必要があります。
- 自社内のコール パターンを知っておく必要があります。単一サイト モデルは、大部分のコールが社内の同一サイトから発信されている場合、または社外の公衆網ユーザ宛てに発信されている場合に適用します。
- すべてのエンドポイントに G.711 コーデックを使用します。この方式を実施すると、トランスコーディングに対してデジタル シグナル プロセッサ（DSP）リソースを消費する必要がなくなり、その分のリソースは、会議やメディア ターミネーション ポイント（MTP）などの他の機能に割り当てることができます。
- H.323 機能を必要と*しない*場合は、公衆網に Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）ゲートウェイを使用します。この方式を実施すると、ダイヤル プランの設定が容易になります。H.323 は、特定の機能（たとえば、Signaling System 7（SS7）や Non-Facility Associated Signaling（NFAS））をサポートするために必要な場合があります。

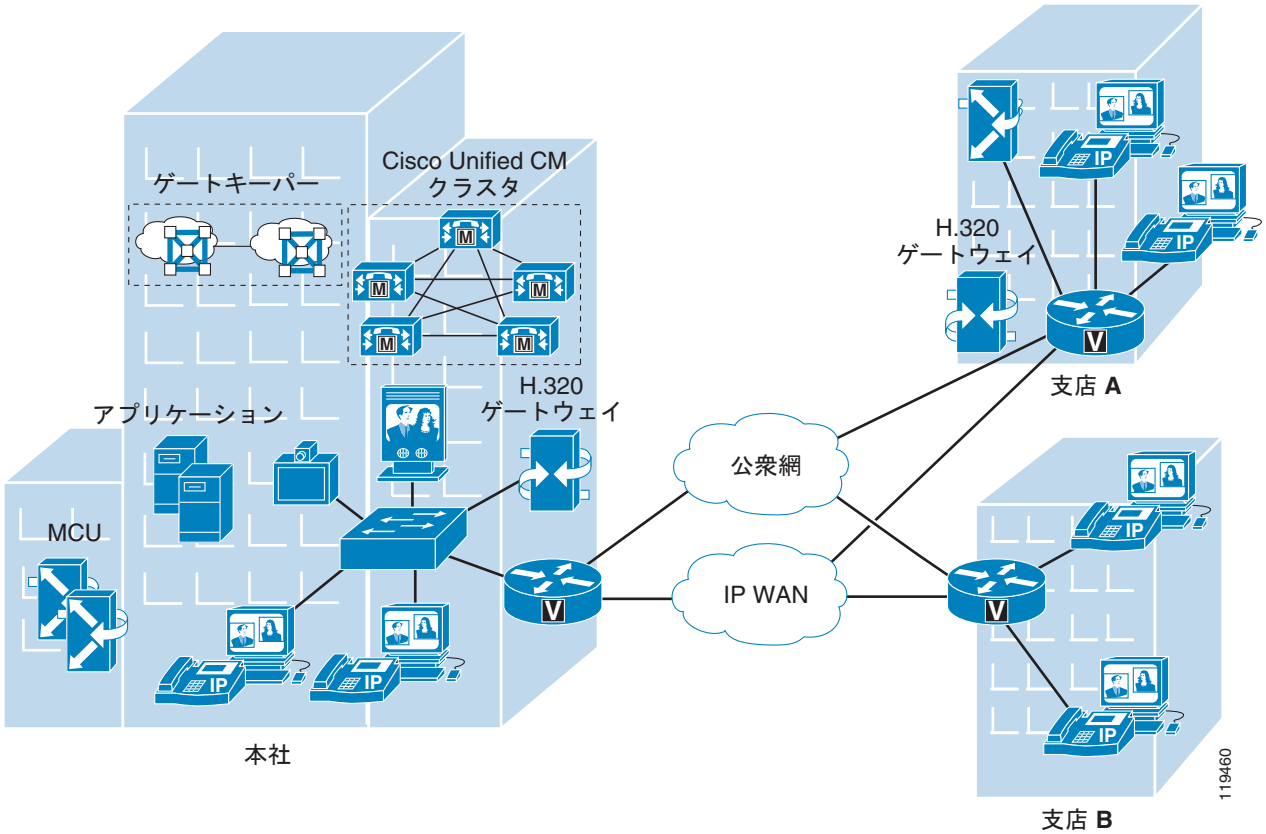
- 高可用性、電話機用の接続オプション（インライン パワー）、Quality of Service（QoS）メカニズム、およびセキュリティ用の推奨ネットワーク インフラストラクチャを実装しています（「ネットワーク インフラストラクチャ」（P.3-1）を参照）。
- 「コール処理」（P.8-1）の章にリストされているプロビジョニングの推奨事項を実行します。

集中型コール処理を使用するマルチサイト

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

（注）　このマニュアルで説明する集中型コール処理モデル用のソリューションでは、さまざまなサイトが QoS に対応した IP WAN に接続されます。

図 2-2　集中型コール処理を使用するマルチサイト配置



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

- 単一の Unified CM クラスタ。
- クラスタあたり最大 30,000 の設定済みおよび登録済み Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone または SCCP ビデオ エンドポイント。
- Unified CM クラスタあたり最大 2000 のロケーションまたは支店サイト。
- Unified CM クラスタあたり最大 2,100 のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H.323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）。
- すべての外部コールに対して公衆網で対応。
- 会議、トランスコーディング、および Media Termination Point（MTP; メディア ターミネーション ポイント）に対してデジタル シグナル プロセッサ（DSP）リソースで対応。
- ボイスメール、ユニファイド メッセージング、Cisco Unified Presence、音声とビデオの各コンポーネント。
- レガシー Private Branch Exchange（PBX; 構内交換機）システムおよびボイスメール システムとの統合機能。
- コールを発信するためにゲートキーパーを必要とする H.323 クライアント、MCU、および H.323/H.320 ゲートウェイを、Cisco IOS ゲートキーパー（Cisco IOS Release 12.3(8)T 以降）に登録することが必要。Unified CM は H.323 トランクを使用してゲートキーパーと統合し、そこに登録された H.323 デバイスのコール ルーティングと帯域幅管理サービスを提供します。複数の Cisco IOS ゲートキーパーを使用して、冗長性を提供することもできます。
- マルチポイント ビデオ会議には MCU リソースが必要です。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。すべてのリソースが中央サイトに存在していても、ローカル会議リソースが必要な場合はリモート サイトに分散していてもかまいません。
- 公衆 ISDN 網上で H.320 ビデオ会議デバイスと通信するために H.323/H.320 ビデオ ゲートウェイが必要です。これらのゲートウェイは中央サイトにあっても、ローカル ISDN アクセスが必要な場合はリモート サイトに分散していてもかまいません。
- 同じサイト内のデバイス間の広帯域オーディオ（G.711、G.722、Cisco Wideband Audio など）、および異なるサイトのデバイス間の狭帯域オーディオ（G.729、G.728 など）。
- 同じサイト内のデバイス間の広帯域ビデオ（384 kbps 以上など）、および異なるサイトのデバイス間の狭帯域ビデオ（128 kbps など）。同じサイト内のデバイス間のコールに限っては、7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec を推奨します。
- 最大 768 kbps 以上の WAN リンク速度。速度が 768 kbps 未満の WAN 接続ではビデオを*推奨しません*。
- Unified CM のロケーション（静的または Resource Reservation Protocol[RSVP] 対応）でコール アドミッション制御を提供し、ビデオ コールでは Automated Alternate Routing（AAR; 自動代替ルーティング）もサポート。
- Survivable Remote Site Telephony（SRST）バージョン 4.0 以降ではビデオをサポート。ただし、バージョン 4.0 よりも前の SRST ではビデオをサポートしていないため、リモート サイトの SCCP ビデオ エンドポイントは、WAN 接続がダウンすると、音声のみのデバイスになります。
- SRST ルータの代わりに Cisco Unified Communications Manager Express（Unified CME）バージョン 4.0 以降を使用して、リモート サイトのサバイバビリティ（呼処理の継続）を確保。Unified CME では、WAN の障害時に、SRST よりも多くの機能が提供されます。
- Cisco Unified Communications Manager Express（Unified CME）は、支店またはリモート サイトで Cisco Unity サーバと統合可能。Cisco Unity サーバは、中央サイトの Unified CM に通常モードで登録され、Unified CM が到達不能の場合や WAN の障害時は、Unified CME に SRST モードでフォール バックできます。これにより支店のユーザは、MWI を使用してボイスメールにアクセスできます。

IP WAN の接続オプションは、次のとおりです。

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

WAN エッジに置かれているルータには、プライオリティ キューイングやトラフィック シェーピングなどの QoS メカニズムが装備されていて、WAN の帯域幅が恒常的に不足している場合に、データ トラフィックから音声トラフィックを保護しています。加えて、音声トラフィックによる WAN リンクのオーバーサブスクリプションや確立されたコールの品質低下を防止するために、コール アドミッション制御方式が必要です。集中型コール処理配置の場合は、Unified CM 内に設定された*ロケーション*（静的または RSVP 対応）でコール アドミッション制御が行われます（ロケーションの詳細については、「コール アドミッション制御」（P.9-1）の章を参照してください）。

リモート サイトでは、さまざまな Cisco ゲートウェイにより、公衆網を介したアクセスが可能です。IP WAN に障害が起きた場合、または IP WAN 上で使用可能な帯域幅がすべて消費されてしまった場合でも、リモート サイトのユーザは、公衆網アクセス コードをダイヤルして、公衆網を利用してコールを発信できます。Cisco Unified Survivable Remote Site Telephony（SRST）機能は、SCCP および SIP 電話機の両方で使用可能です。Cisco Unified IP Phone が、リモートの 1 次、2 次、および 3 次 Unified CM への接続を失った場合、または WAN 接続がダウンした場合に、支店でのコール処理を提供します。Cisco Unified SRST 機能は、SRST 機能を実行する Cisco IOS ゲートウェイ、または SRST モードで動作する Cisco Unified CME Release 4.0 以降で使用できます。SRST モードで動作する Unified CME では、Cisco IOS ゲートウェイの SRST よりも多くの機能が電話機に提供されます。

集中型コール処理モデルのベスト プラクティス

マルチサイトの集中型コール処理配置を実装する際は、次のガイドラインおよびベスト プラクティスに従ってください。

- 音声のカットスルー遅延（クリッピングとも呼ばれます）を減らすために、Unified CM とリモート ロケーション間の遅延を最小限に抑えます。
- Unified CM 内のロケーション（静的または RSVP 対応）でリモート支店との間のコール アドミッション制御が行われるように設定する。このメカニズムをさまざまな WAN トポロジに適用する方法については、「コール アドミッション制御」（P.9-1）の章を参照してください。
- 各リモート サイトでの Survivable Remote Site Telephony（SRST）モードでサポートされている IP Phone およびライン アピアランスの数は、その支店内にあるルータのプラットフォーム、取り付け済みメモリ容量、および Cisco IOS リリースにより異なります。Cisco IOS ゲートウェイの SRST では最大 720 台の電話機がサポートされますが、SRST モードで動作する Unified CME の場合は、最大 240 台です（SRST または Unified CME プラットフォームおよびコード仕様に関する詳細は、http://www.cisco.com から入手できる SRST および Unified CME の文書を参照してください）。一般的には、特定サイトに対して集中型コール処理か、分散コール処理かを決定するには、次に示す種々の要素によります。
  - IP WAN 帯域幅、または遅延制限
  - 音声ネットワークに関する臨界状況
  - 機能セットの必要性
  - スケーラビリティ

  - 管理の容易性
  - コスト

  お客様のビジネス ニーズに分散型コール処理モデルがふさわしいと判断する場合は、2 つの選択肢があります。各サイトに Unified CM クラスタをインストールする方法と、リモート サイトで Unified CME を稼動する方法です。

- リモート サイトでは、次の機能を使用して、WAN 障害が発生した場合のコール処理のサバイバビリティを確保します。
  - SCCP 電話機の場合は、Cisco IOS ゲートウェイの SRST を使用するか、SRST モードで動作する Unified CME を使用します。
  - SIP 電話機の場合は、SIP SRST を使用します。
  - MGCP 電話機の場合は、MGCP ゲートウェイ フォールバックを使用します。

  SRST または SRST モードの Unified CME、SIP SRST、および MGCP ゲートウェイ フォールバックは、同一の Cisco IOS ゲートウェイに相互に存在することができます。

リモート サイトのサバイバビリティ（呼処理の継続）

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

表 2-2　リモート サイトの高可用性を提供する方法

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

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

表 2-2 の 3 番目と 4 番目のソリューションでは、ISDN バックアップ リンクを使用して、WAN 障害時の存続可能性を提供します。ISDN バックアップ用には、次の 2 つの配置オプションがあります。

- データのみの ISDN バックアップ

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

- データと音声の ISDN バックアップ

  このオプションでは、ISDN はデータと音声の両方の存続性を確保するのに使用されます。この場合、IP Phone は常に Unified CM クラスタとの IP 接続を保持するので、SRST または SRST モードの Unified CME は使用されません。しかし、データと音声のトラフィックの転送に ISDN を使用するのは、次の条件がすべて満たされる場合だけにすることをシスコはお勧めします。

  - ISDN リンク上で音声トラフィックに割り当てられた帯域幅が、IP WAN リンク上で音声トラフィックに割り当てられた帯域幅と同じである。
  - ISDN リンクの帯域幅が固定されている。
  - 必要なすべての QoS 機能が、ルータの ISDN インターフェイスに配置されている。QoS の詳細については、「ネットワーク インフラストラクチャ」（P.3-1）の章を参照してください。

表 2-2 にリストされている 5 番目のソリューションでは、WAN 障害が検出された場合、Survivable Remote Site Telephony（SRST）または SRST モードの Unified CME が、リモート オフィスのルータ内でコール処理機能のサブセットを提供し、IP Phone を拡張して、ローカル ルータ内のコール処理機能に「re-home」機能を提供することによって、音声サービスのみの高い可能性を提供します。図 2-3 では、SRST または SRST モードの Unified CME を使用した典型的なコールのシナリオを示しています。

図 2-3　Survivable Remote Site Telephony（SRST）または SRST モードの Unified CME

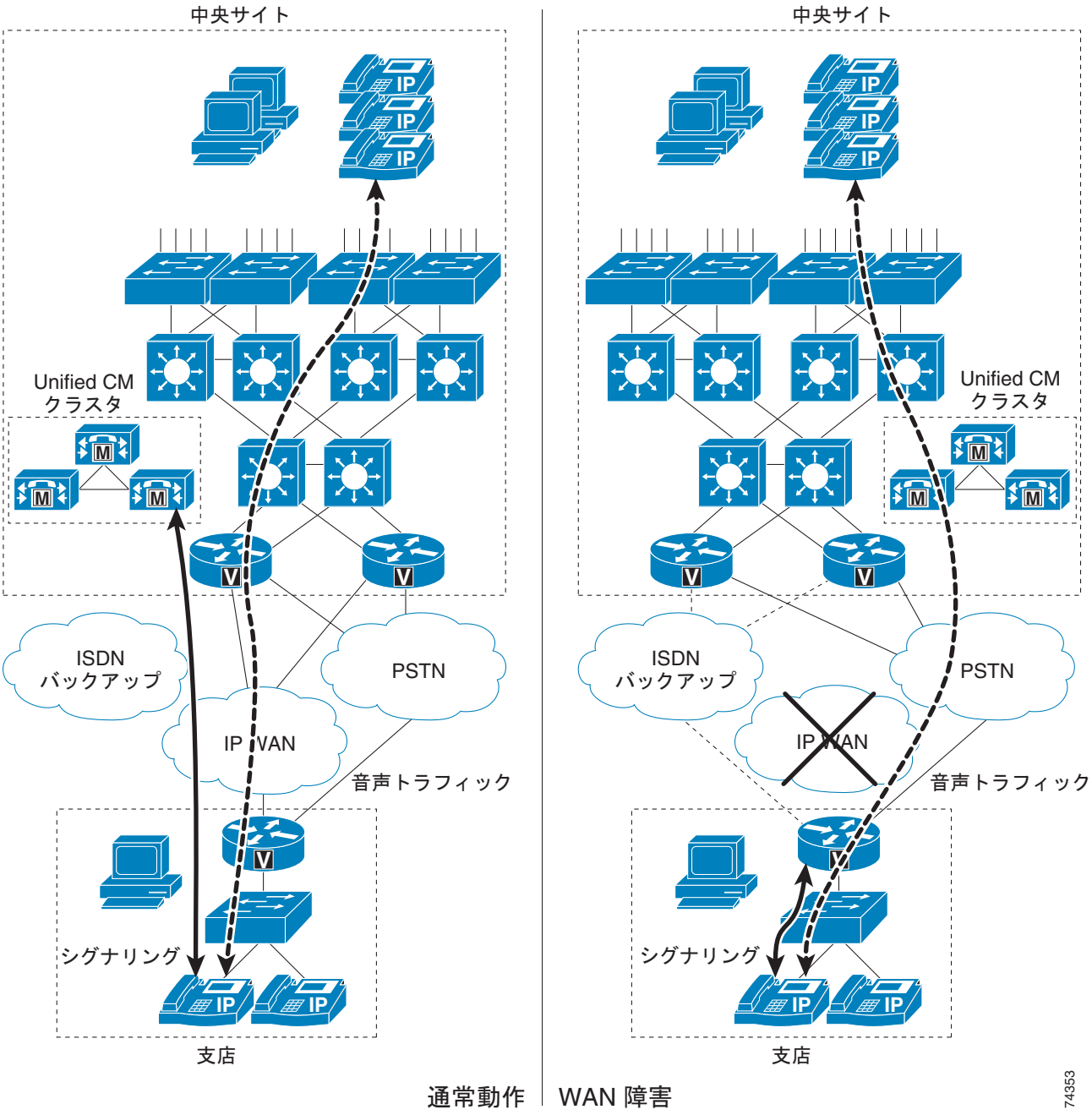


図 2-3 の左側に表示されている通常の動作では、支店は、データ トラフィック、音声トラフィック、およびコール シグナリングを伝送する IP WAN を経由して、中央サイトに接続されます。支店の IP Phone は、中央サイトの Unified CM クラスタとコール シグナリング情報を交換し、IP WAN を介してコールを発信します。支店のルータまたはゲートウェイは、両方のタイプのトラフィック（コール シグナリングと音声）を透過的に転送し、IP Phone を認識しません。

支店との WAN リンクに障害が起きた場合、またはその他のなんらかのイベントにより、Unified CM クラスタとの接続が失われた場合、支店の IP Phone は支店のルータに SRST モードで再登録されます。支店のルータ、SRST、または SRST モードで動作する Unified CME は、設定について IP Phone に照

会し、この情報を使用して独自の設定を自動的に作成します。支店の IP Phone は、内部で、または公衆網を介してコールの発信と受信を行うことができます。電話機は「Unified CM fallback mode」というメッセージを表示し、Unified CM の一部の拡張機能が利用不能になり、電話機のディスプレイでグレー表示されます。

中央サイトとの WAN 接続が再度確立されると、支店の IP Phone は、Unified CM クラスタに自動的に再登録され、正常な動作に戻ります。支店の SRST ルータは、IP Phone についての情報を削除し、標準のルーティングまたはゲートウェイ設定に戻ります。SRST モードで動作する支店の Unified CME では、自動プロビジョニング オプションを使用することで、取得した電話機および回線の設定を、Unified CME ルータの実行設定に保存できます。**auto-provision none** が設定されている場合、自動でプロビジョニングされた電話機または回線の設定情報は、Unified CME ルータの実行設定に保存されません。そのため、IP Phone を交換して MAC アドレスが変更された場合でも、Unified CME での設定変更は必要ありません。

（注）　中央サイトとの WAN 接続が再度確立された場合、または Unified CM が再度到達可能になった場合でも、アクティブ コールを持つ SRST モードの電話機がただちに Unified CM に再登録されるわけではありません。再登録されるのは、そのようなアクティブ コールが終了してからです。

SRST モードの Unified CME

Unified CME が SRST モードで使用されている場合、ルータの SRST で使用できる機能よりも多くのコール処理機能が IP Phone に提供されます。コール プリザベーションや自動プロビジョニング、フェールオーバーといった SRST の機能に加え、SRST モードの Unified CME では、SCCP 電話機用に用意されている次のような Unified CME テレフォニー機能のほとんどを使用できます。

- ポケットベルによる呼び出し
- 会議
- ハント グループ
- Basic Automatic Call Distribution（B-ACD; 基本自動着信呼分配）
- コール パーク、コール ピックアップ、コール ピックアップ グループ
- オーバーレイ DN、ソフトキー テンプレート
- Cisco IP Communicator 2.0
- Cisco Unified Video Advantage 2.0
- MWI をサポートする Cisco Unity とのリモートサイトでの統合、および分散型の Microsoft Exchange または IBM Lotus Domino サーバとの統合

SRST モードの Unified CME では、WAN 障害が発生した場合に、SCCP 電話機に対するコール処理がサポートされます。ただし、SRST モードの Unified CME では、SIP 電話機、MGCP 電話機、またはエンドポイントに対するフォールバックはサポートしていません。SIP プロキシ サーバまたは Unified CM への接続が失われた場合や、WAN 接続に障害が発生した場合に、SIP 電話機および MGCP 電話機がフォールバックできるようにするために、SRST フォール バック サーバとして動作している Unified CME サーバに、SIP SRST 機能と MGCP ゲートウェイ フォールバック機能の両方を追加で設定できます。

SRST モードの Unified CME のベスト プラクティス

- Unified CM での SRST 参照の IP アドレス として、Unified CME の IP アドレスを使用します。
- Connection Monitor Duration は、SRST から Unified CM へのフォールバックを開始するまでに、電話機が WAN リンクを監視する時間を指定するタイマーです。ほとんどの場合は、デフォルト設定の 120 秒を使用します。ただし、SRST モードの電話機が、フラッピングが発生しているリンクで Unified CM にフォールバックしたり復帰したりするのを防ぐために、Unified CM の

[Connection Monitor Duration] パラメータをより長い期間に設定することができます。これにより、電話機が SRST ルータと Unified CM の間で登録と再登録を繰り返すことがなくなります。電話機が長期間にわたって SRST から Unified CM にフォールバックしなくなるため、この値を極端に長い期間に設定しないでください。

- SRST フォールバック モードの電話機は、アクティブ状態になっても Unified CM に復帰しません。
- SRST フォールバック モードの電話機は、セキュア会議から非セキュア モードに戻ります。
- **auto-provision none** を設定し、取得された ephone-dn または ephone 設定が、Unified CME ルータの実行設定に書き込まれないようにします。これにより、IP Phone が交換された場合や、MAC アドレスが変更された場合に、設定を変更する必要がなくなります。

SRST モードの Unified CME の使用に関する詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Express System Administrator Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_and_configuration_guides_list.html

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

http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html

MGCP ゲートウェイ フォールバックの詳細については、次の Web サイトで入手可能な『*Cisco CallManager and Cisco IOS Interoperability Guide*』の MGCP ゲートウェイに関する情報を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/interop/ccm_c.html

SRST ルータのベスト プラクティス

次の配置シナリオでは、SRST モードの Unified CME ではなく、Cisco Unified SRST ルータを使用します。

- 1 台の SRST ルータで、最大 720 台の電話機をサポートする場合。
- 最大 1000 台の電話機をサポートする場合は、2 台の SRST ルータを使用。各 SRST ルータ間でコールが相互にルーティングされるように、ダイヤル プランを正しく設定する必要があります。
- 基本的な SRST 機能の、単純な 1 回限りの設定を行う場合。
- Cisco Unified SRST（セキュア SRST）でのみ使用可能な SRTP メディア暗号化を使用する場合。
- Cisco VG248 音声ゲートウェイをサポートする場合。
- 到達不能または SRST ルータに登録されていない電話機のコールをルーティングする場合は、**alias** コマンドを使用。

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

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

VoPSTN は、次のいずれかの方法で実装できます。

- Automated Alternate Routing（AAR; 自動代替ルーティング）機能を使用する（AAR の詳細については、「Automated Alternate Routing」（P.10-87）の項を参照してください）。
- Unified CM と公衆網ゲートウェイの両方のダイヤル プラン構成要素を組み合せて使用する。

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

（注）　VoPSTN 配置では、Unified CM 機能セットの一部を削減した基本的な音声機能が提供されます。

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

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

- 支店のゲートウェイに着信するコールを支店サイトの外部の宛先にコール転送すると、ゲートウェイを介したヘアピンコールが発生し、2 つのトランク ポートが使用されます。この動作は、次の場合に発生します。
  - 支店の外部にあるボイスメール システムにコールが転送される場合
  - 別の支店にあるオンネットの内線番号にコールが転送される場合

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

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

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

AAR を使用する VoPSTN

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

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

VoPSTN の AAR 実装方法には、次の利点があります。

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

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

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

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

ダイヤル プランを使用する VoPSTN

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

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

VoPSTN のダイヤル プラン実装方法には、次の利点があります。

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

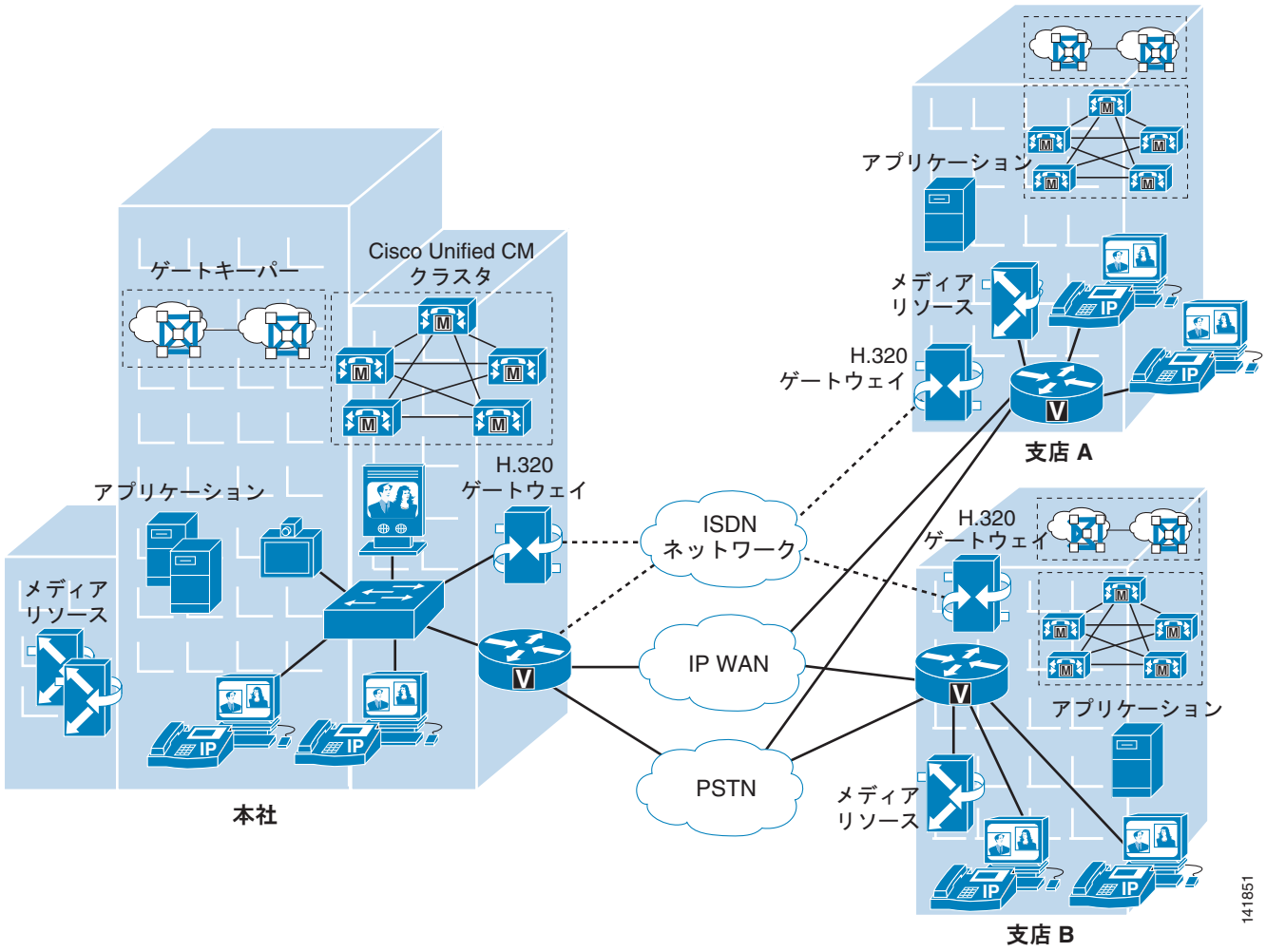
ダイヤル プラン実装方法には、VoPSTN について示した一般的な考慮事項のほかに、次の設計ガイドラインが適用されます。

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

分散型コール処理を使用するマルチサイト

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

図 2-4　分散型コール処理を使用するマルチサイト配置



分散型コール処理モデルの各サイトは、次のいずれかになります。

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

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

- クラスタあたり最大 30,000 の設定済みおよび登録済み Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone または SCCP ビデオ エンドポイント。
- Unified CM クラスタあたり最大 2,100 のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H.323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）。
- すべての外部コールに対して公衆網で対応。
- 会議、トランスコーディング、および Media Termination Point（MTP; メディア ターミネーション ポイント）に対してデジタル シグナル プロセッサ（DSP）リソースで対応。
- ボイスメール、ユニファイド メッセージング、および Cisco Unified Presence の各コンポーネント。
- レガシー Private Branch Exchange（PBX; 構内交換機）システムおよびボイスメール システムとの統合機能。
- コールを発信するためにゲートキーパーを必要とする H.323 クライアント、MCU、および H.323/H.320 ゲートウェイを、Cisco IOS ゲートキーパー（Cisco IOS Release 12.3(8)T 以降）に登録することが必要。Unified CM は H.323 トランクを使用してゲートキーパーと統合し、そこに登録された H.323 デバイスのコール ルーティングと帯域幅管理サービスを提供します。複数の Cisco IOS ゲートキーパーを使用して、冗長性を提供することもできます。Cisco IOS ゲートキーパーを使用して、分散した Unified CM クラスタ間でコール ルーティングおよび帯域幅管理を提供することもできます。多くの場合、Unified CM クラスタごとに専用のエンドポイント ゲートキーパーを持ち、それとは別のゲートキーパーを使用してクラスタ間コールを管理することを推奨します。状況によっては、ネットワークのサイズやダイヤル プランの複雑さに応じて、同じゲートキーパーを両方の機能に使用することもできます（詳細については、「ゲートキーパー」（P.16-22）を参照してください）。
- マルチポイント ビデオ会議のクラスタごとに MCU リソースが必要。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。すべてのリソースがリージョン サイトに存在していても、ローカル会議リソースが必要な場合は各クラスタのリモート サイトに分散していてもかまいません。
- 公衆 ISDN 網上で H.320 ビデオ会議デバイスと通信するために H.323/H.320 ビデオ ゲートウェイが必要です。これらのゲートウェイはリージョン サイトにあっても、ローカル ISDN アクセスが必要な場合は各クラスタのリモート サイトに分散していてもかまいません。
- 同じサイト内のデバイス間の広帯域オーディオ（G.711、G.722、Cisco Wideband Audio など）、異なるサイトのデバイス間の狭帯域オーディオ（G.729、G.728 など）。
- 同じサイト内のデバイス間の広帯域ビデオ（384 kbps 以上など）、異なるサイトのデバイス間の狭帯域ビデオ（128 kbps など）。同じサイト内のデバイス間のコールに限っては、7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec を推奨します。ただし、Cisco VT Camera Wideband Video Codec はクラスタ間トランクでサポートされていません。
- 最大 768 kbps 以上の WAN リンク速度。速度が 768 kbps 未満の WAN 接続ではビデオを*推奨しません*。

- コール アドミッション制御は、同じ Unified CM クラスタで制御されるサイト間のコールに対しては Unified CM のロケーションから提供。Unified CM クラスタ間のコールに対しては Cisco IOS ゲートキーパーから提供されます（クラスタ間トランク）。クラスタ内とクラスタ間の両方のビデオ コールに対して、自動代替ルーティング（AAR）もサポートされます。

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

IP WAN の接続オプションは、次のとおりです。

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

分散型コール処理モデルのベスト プラクティス

分散型コール処理を使用するマルチサイト配置には、単一サイトと同じ、または集中型コール処理を使用するマルチサイト配置と同じ要件が少なからずあります。分散型コール処理モデルについては、ここでリストされているベスト プラクティスに加えて、他のモデルのベスト プラクティスにも従ってください（「単一サイト」（P.2-2）および「集中型コール処理を使用するマルチサイト」（P.2-4）を参照）。

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

ゲートキーパーの使用には、次のベスト プラクティスが適用できます。

- Cisco IOS ゲートキーパーを使用して、各サイトとのコール アドミッションを制御します。
- ゲートキーパーの有効性を高めるには、HSRP（ホットスタンバイ ルータ プロトコル）ゲートキーパー ペア、ゲートキーパーのクラスタ化、および代替ゲートキーパー サポートを使用します。さらに、ネットワーク内の冗長性を確実にするために複数のゲートキーパーを使用します（「ゲートキーパーの設計上の考慮事項」（P.8-26）を参照）。
- プラットフォームの規模を適切に調整して、パフォーマンスとキャパシティの要件が満たされることを確認します。
- WAN 上のコーデックは 1 つのタイプに限定して使用します。これは、H.323 仕様では、レイヤ 2、IP、UDP（User Data Protocol）、または RTP（Real-time Transport Protocol）ヘッダーのオーバーヘッドが、帯域幅要求で許可されないからです（ヘッダーのオーバーヘッドは、パケットのペイロードまたは符号化された音声部分のみで許可されます）。WAN 上で使用するコーデックを 1 つのタイプに限定すると、最悪のシナリオに備えて IP WAN を過剰にプロビジョニングする必要がなくなるので、キャパシティ プランニングが簡単になります。
- ゲートキーパー ネットワークは、数百単位のサイトにスケーラブルです。また、設計上の制限は WAN トポロジからしか受けません。

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

- ゲートキーパーのコール アドミッション制御については、「コール アドミッション制御」（P.9-1）を参照してください。

- ゲートキーパーのスケーラビリティと冗長性については、「コール処理」（P.8-1）を参照してください。
- ゲートキーパーのダイヤル プラン解決については、「ダイヤル プラン」（P.10-1）を参照してください。

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

SIP プロキシの使用には、次のベスト プラクティスが適用できます。

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

分散型コール処理モデルのコール処理エージェント

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

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

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

表 2-3 は、推奨されるコール処理エージェントを示しています。

表 2-3　推奨されるコール処理エージェント

コール処理エージェント	推奨規模	備考
Cisco Unified Communications Manager Express（Unified CME）	最大 240 台の電話機	• 小規模なリモート サイト用 • キャパシティは Cisco IOS プラットフォームに依存する
Cisco Unified Communications Manager Business Edition（Unified CMBE）	最大 575 台の電話機	• 小規模なサイト用 • 集中型または分散型コール処理をサポートする
Cisco Unified Communications Manager（Unified CM）	50 ～ 30,000 台の電話機	• Unified CM クラスタの規模に応じて、小規模から大規模までのサイト • 集中型または分散型コール処理をサポートする
VoIP ゲートウェイを備えた従来の PBX	PBX に依存する	• IP WAN コール数と機能は、PBX と VoIP ゲートウェイを接続するプロトコルおよびゲートウェイ プラットフォームによって異なる

Unified CM Session Management Edition

Cisco Unified Communications Manager Session Management Edition を使用するユニファイド コミュニケーションの配置は、マルチサイトの分散型コール処理配置モデルのバリエーションであり、一般に、1 つのフロントエンド システム（この場合は Unified CM Session Management Edition）を介して多数のユニファイド コミュニケーション システムを相互接続するために採用されます。この項では、Unified CM Session Management Edition の配置に関する設計上の考慮事項について説明します。

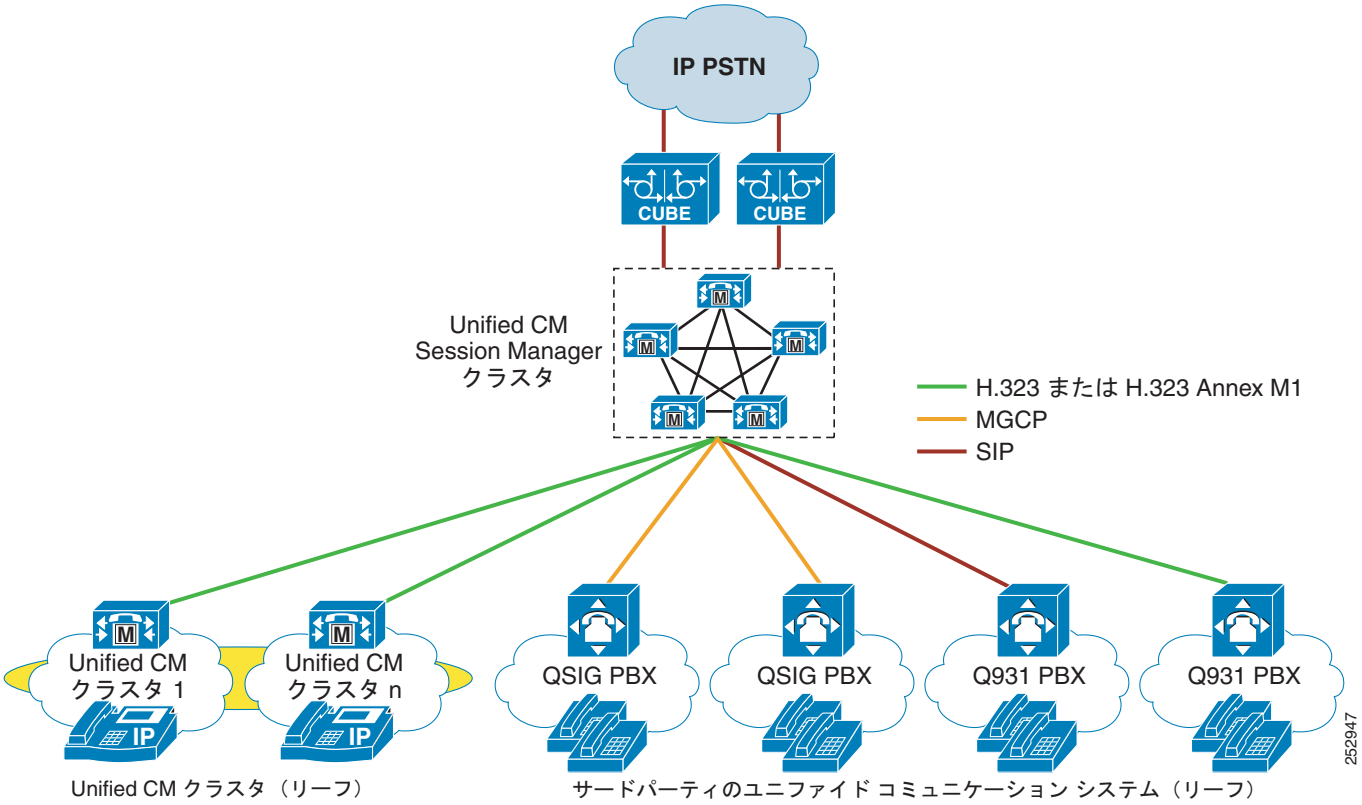
Cisco Unified CM Session Management Edition は基本的に、トランク インターフェイスだけを使用し、IP エンドポイントを使用しない Unified CM クラスタです。このクラスタには、リーフ システムと呼ばれる、複数のユニファイド コミュニケーション システムを集約することができます。

Cisco Unified CM 7.1(3) 以降のリリースでは、Unified CM Session Management Edition で次の機能がサポートされています。

- H.323 Annex M1 クラスタ間トランク
- SIP クラスタ間トランク
- SIP トランク
- H.323 トランク
- MGCP トランク
- 音声コール
- ビデオ コール
- FAX コール

また、Unified CM Session Management Edition を使用して、IP PSTN 接続、PBX、および集中型のユニファイド コミュニケーション アプリケーションなど、サードパーティのユニファイド コミュニケーション システムに接続することができます（図 2-5 を参照）。ただし、標準の Unified CM クラスタと同様に、サードパーティ デバイスからの Unified CM Session Management Edition への接続については、実稼動環境で使用する前に相互運用性をテストする必要があります。

図 2-5　Unified CM Session Management Edition を使用したマルチサイト配置



Unified CM Session Management Edition を配置する状況

次のいずれかの操作を行う場合は、Unified CM Session Management Edition を配置することをお勧めします。

- 集中型ダイヤル プランを作成および管理

  他のすべてのユニファイド コミュニケーション システムに接続するために各ユニファイド コミュニケーション システムに別個のダイヤル プランおよびトランクを設定するのではなく、Unified CM Session Management Edition を使用すると、Session Management を指す簡潔なダイヤル プランおよびトランクをリーフのユニファイド コミュニケーション システムに設定できます。Unified CM Session Management Edition には、他のすべてのユニファイド コミュニケーション システムに到達するための情報を備えた集中型ダイヤル プランが保持されます。

- 集中型公衆網アクセスを提供

  Unified CM Session Management Edition を使用すると、1 つ（または複数）の IP 公衆網トランクに公衆網アクセスを集約することができます。集中型公衆網アクセスには一般に、支店ベースの公衆網回線の削減または排除を伴います。

- アプリケーションを集中化

  Unified CM Session Management Edition の配置によって、会議やビデオ会議などの一般に使用されるアプリケーションを直接 Session Management クラスタに接続できるので、複数のトランクの管理によるリーフ システムへのオーバーヘッドが軽減されます。

- Unified Communications システムに移行するために PBX を集約

  Unified CM Session Management Edition は、レガシー PBX から Cisco Unified Communications システムへの移行の一環として、複数の PBX の集約ポイントを提供することができます。

Unified CM Session Management Edition と標準の Unified CM クラスタの相違

Unified CM Session Management Edition ソフトウェアは、Unified CM と同じです。ただし、このソフトウェアは、この新しい配置モデルの要件と制約を満たすために大幅に強化されています。Unified CM Session Management Edition は、多数のトランクツートランク接続をサポートするように設計されているため、次に示す設計上の考慮事項に従う必要があります。

- キャパシティ

  Unified CM Session Management クラスタは、リーフの Unified Communications システム間（Unified CM クラスタと PBX など）、集中型 IP 公衆網接続間、および集中型アプリケーションへの予想される BHCA トラフィック ロードに基づいて正確にサイズ設定することが重要です。Unified CM Session Management Edition クラスタを適切にサイズ設定する作業は、シスコのシステム エンジニア（SE）またはシスコ代理店と協力して行ってください。

- トランク

  可能な場合は、Unified CM トランクに静的な MTP を使用しないでください（つまり、リーフ、Session Management Unified CM SIP、または H.323 トランクに対する [MTP required] チェックボックスをオフにします）。MTP のないトランクではコーデックの選択の幅が広がり、音声、ビデオ、および暗号化がサポートされ、トランク コールが MTP リソースに固定されません。サードパーティのユニファイド コミュニケーション システムで SIP Early Offer が必要とされる場合は、Cisco Unified Border Element と一緒に Delayed Offer to Early Offer 機能を使用します。トランクでは、動的に挿入された MTP を使用できます（たとえば、インバンドからアウトオブバンドに DTMF を変換する場合など）。

- 暗号化

  暗号化されたコールは、Unified CM Session Management Edition の現在のリリースではサポートされていません。

- Unified CM バージョン

  Unified CM Session Management Edition と Unified CM リーフ クラスタの両方とも、Cisco Unified CM 7.1(2) 以降のリリースが必要です。Unified CM 7.1(2) には、トランクツートランク コールに対するいくつかの拡張機能があります。以前のバージョンの Unified CM では、クラスタを Unified CM 7.1(2) 以降のリリースにアップグレードしなければ解決できない問題が生じることがあります。

- 相互運用性

  ほとんどのベンダーが標準にある程度適合していますが、各ベンダーによるプロトコルの実装には相違があります。標準の Unified CM クラスタの場合と同様に、実稼動環境にシステムを配置する前に、サードパーティの未検証のユニファイド コミュニケーション システムとの相互運用性テストを実施することを強くお勧めします。相互運用性テストでは、Unified CM Session Management クラスタを介したシスコおよびサードパーティのリーフ システムからのコール フローと機能を検証します。シスコの相互運用性チームによってテストされたサードパーティのユニファイド コミュニケーション システムの情報を得るには、www.cisco.com/go/interoperability にアクセスして、[Cisco Unified Communications Manager - Session Management Edition] のリンクを選択してください。お使いのユニファイド コミュニケーション システムがまだシスコでテストされていない場合は、Cisco Advanced Services を利用してこのテストを実施してください。それが不可能である場合、シスコ代理店およびユーザは、実行するテストのタイプについて説明した資料をシスコの担当者から入手できます。

- 着信コールと発信コールのロード バランシング

  Session Management クラスタ内の Unified CM サーバ間に着信コールと発信コールが均等に分散されるよう、Unified CM Session Management Edition およびリーフのユニファイド コミュニケーション システムのトランクを設定します。トランク コールのロード バランシングの詳細については、「Cisco Unified CM トランク」（P.5-1）の章を参照してください。

- 設計のサポート

  Unified CM Session Management Edition の設計は、担当のシスコ SE が Cisco Unified CM Session Management チームと一緒に確認します。Unified CM Session Management Edition の設計確認プロセスの詳細について、シスコ代理店および従業員は次の Web サイトにある資料を参照できます。

  http://docwiki.cisco.com/wiki/Unified_Communications_Manager_-_Session_Manager_Edition

IP WAN を介したクラスタ化

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

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

- 「ローカル フェールオーバー配置モデル」（P.2-26）

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

- 「リモート フェールオーバー配置モデル」（P.2-32）

  リモート フェールオーバーでは、WAN を介して分割されたプライマリとバックアップのコール処理サーバを配置できます。このタイプの配置を使用すると、Unified CM サブスクライバを備えた最大 8 つのサイトを、別のサイトにある Unified CM サブスクライバでバックアップすることが可能です。

（注）　リモート フェールオーバーの配置では、サブスクライバ サーバ間で大量のクラスタ内トラフィックが流れるため、広い帯域幅が必要になる場合があります。

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

WAN を介したクラスタ化の主な利点として、次のようなものが挙げられます。

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

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

WAN の考慮事項

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

- 遅延

  任意の 2 台の Unified CM サーバ間の片方向の最大遅延は 40 msec、つまり 80 msec Round-Trip Time（RTT; ラウンドトリップ時間）以下でなければなりません。遅延の測定については、「遅延のテスト」（P.2-25）を参照してください。2 つのサイト間の伝搬遅延は、他のネットワーク遅延を考慮しない場合、1 キロメートルあたり 6 マイクロ秒になります。これは、20 ms 遅延に対して理論的な最大距離約 3000 km、つまり約 1860 マイルに相当します。この距離は、相対的なガイドラインとしてのみ記載されています。実際には、ネットワーク内の他の遅延により、これより短くなります。

- ジッタ

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

- パケット損失とエラー

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

- 帯域幅

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

- QoS

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

クラスタ内通信

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

サーバ間のクラスタ内トラフィックは、次のものから構成されます。

- 主な設定情報を提供する IBM Informix Dynamic Server（IDS）データベースからのデータベース トラフィック。IDS トラフィックは、Cisco QoS の推奨事項に沿って再優先順位付けが行われ、より高い優先順位のデータ サービスになります（たとえば、特定のビジネス ニーズによって必要な場合は IP Precedence 1）。この一例は、IDS データベース設定を使用する、エクステンション モビリティの拡張使用です。
- サブスクライバをパブリッシャに認証し、パブリッシャのデータベースにアクセスするために使用されるファイアウォール管理トラフィック。管理トラフィックは、クラスタ内のすべてのサーバ間を通過します。管理トラフィックは、Cisco QoS の推奨事項に沿って優先順位付けが行われ、より高い優先順位のデータ サービスになります（たとえば、特定のビジネス ニーズによって必要な場合は IP Precedence 1）。
- ICCS リアルタイム トラフィック。このトラフィックは、シグナリング、コール アドミッション制御、および開始と終了時のコールについてのその他の情報から構成されます。ICCS は、Cisco CallManager Service が使用可能になっているすべてのサーバ間で、伝送制御プロトコル（TCP）接続を使用します。この接続は、これらのサーバ間でフルメッシュです。クラスタには、Cisco CallManager Service が使用可能になっているサーバが 8 つしかないので、各サーバには最大 7 つの接続が可能です。このトラフィックは、優先 ICCS トラフィックであり、Cisco CallManager リリースおよびサービス パラメータ設定に応じてマークされます。
- CTI Manager リアルタイム トラフィック。このトラフィックは、コールに関係する CTI デバイスに使用されるか、Unified CM サーバ上のその他のサードパーティ製デバイスの制御または監視に使用されます。このトラフィックは、優先 ICCS トラフィックとしてマークされ、CTI Manager を備えた Unified CM サーバと、CTI デバイスを備えた Unified CM サーバとの間に存在します。

（注） Unified CM サーバ間の各種タイプのトラフィックの詳細については、http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/7_0/CCM_7.0PortList.pdf のポート使用に関する文書を参照してください。

Unified CM パブリッシャ

パブリッシャ サーバは、部分的なマスター データベースの読み取り専用コピーをクラスタ内の他のすべてのサーバに複製します。データベースのほとんどの変更は、パブリッシャで行われます。クラスタ内の別のサーバが通信不能である期間に、パブリッシャのマスター データベースに管理目的の更新などの変更が加えられた場合、パブリッシャは、通信が再確立されたときに、更新されたデータベースを複製します。ユーザ方向のコール処理機能に対するデータベースの変更は、IP Phone が登録されるサブスクライバ サーバで行われます。これらの機能には、次のものがあります。

- Call Forward All（CFA; 全コール転送）
- Message Waiting Indication（MWI; メッセージ待機インジケータ）
- プライバシーの有効 / 無効
- Do Not Disturb（DND）の有効 / 無効
- Extension Mobility（EM; エクステンション モビリティ）のログイン

- モニタ（将来的に使用、現在ユーザ レベルの更新はありません）
- ハント グループのログアウト
- デバイス モビリティ
- エンド ユーザおよびアプリケーション ユーザの CTI Certificate Authority Proxy Function（CAPF）ステータス
- クレデンシャルのハッキングと認証

各サブスクライバ サーバは、これらの変更をクラスタ内の他のすべてのサーバに複製します。パブリッシャが到達不能またはオフラインの間は、他のいかなる設定変更もデータベースに加えることはできません。パブリッシャに障害が発生している場合でも、次のものをはじめとするクラスタの通常の操作の大部分は、影響を*受けません*。

- コール処理
- フェールオーバー
- 設定済みデバイスの登録

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

コール詳細レコード（CDR）およびコール管理レコード（CMR）

コール詳細レコードとコール管理レコードが使用可能である場合、各サブスクライバによって収集され、定期的にパブリッシャにアップロードされます。パブリッシャが通信不能である間、CDR および CMR は、サブスクライバのローカル ハードディスクに保存されます。パブリッシャとの接続が再確立されると、未処理の CDR はすべて、パブリッシャにアップロードされます。パブリッシャは、レコードを CDR Analysis and Reporting（CAR; CDR 分析とレポート）データベースに格納します。

遅延のテスト

任意の 2 つのサーバ間の最大ラウンドトリップ時間（RTT）は、80 msec 以下でなければなりません。この制限には、この 2 つのサーバ間の伝送パスの遅延がすべて含まれる必要があります。Unified CM サーバで **ping** ユーティリティを使用してラウンドトリップの遅延を確認しても、正確な結果は得られません。ping は、ベストエフォート型のパケットとして送信されます。ICCS トラフィックと同じ QoS 対応パスを使用して転送されません。したがって、遅延を確認するには、Unified CM サーバに最も近いネットワーク デバイスを使用することをお勧めします。理想的には、サーバが接続されているアクセス スイッチです。Cisco IOS は、ICCS トラフィックが通過するのと同じ QoS 対応パス上で ping パケットが送信されるように、レイヤ 3 タイプ オブ サービス（ToS）ビットを設定できる拡張 ping を備えています。拡張 ping によって記録される時間は、ラウンドトリップ時間（RTT）、つまり通信パスを通過して戻るのに要する時間です。

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

```
Access_SW#ping
Protocol [ip]:
Target IP address: 10.10.10.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]: 3
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
```

```
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

エラー率

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

トラブルシューティング

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

- クラスタ内のリモート Unified CM サーバ上にある IP Phone、ゲートウェイ、またはその他のデバイスが、一時的に通信不能になることがあります。
- コールの接続が切断されたり、コールのセットアップ中に失敗する場合があります。
- ユーザにダイヤル トーンが聞こえるまでに、予想以上に長い遅延が起こる場合があります。
- Busy Hour Call Completions（BHCC）が低い場合があります。
- ICCS（SDL セッション）がリセットされたり、接続が切断されることがあります。

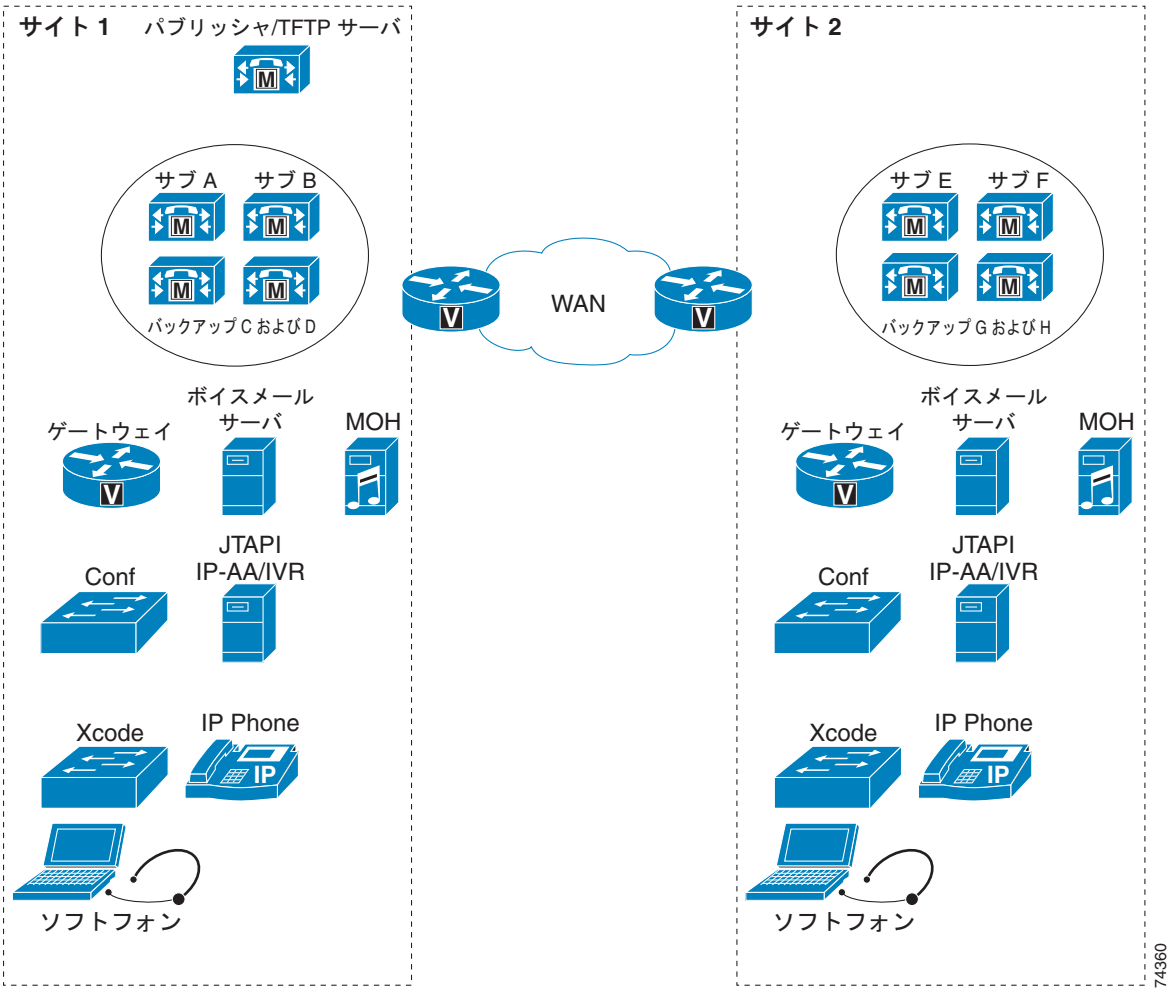
要約すると、ICCS 通信の問題のトラブルシューティングを行うには、次のタスクを実行します。

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

ローカル フェールオーバー配置モデル

ローカル フェールオーバー配置モデルは、WAN を介したクラスタ化に対する最大の復元性があります。このモデルの各サイトには、少なくとも 1 つのプライマリ Unified CM サブスクライバと 1 つのバックアップ サブスクライバがあります。この設定では、最大 4 つのサイトをサポートできます。電話機および他のデバイスの最大数は、配置されているサーバの数とタイプによって異なります。全サイトの IP Phone の最大総数は 30,000 です（図 2-6 を参照）。

図 2-6　ローカル フェールオーバー モデルの例



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

- 少なくとも 1 つのプライマリ Unified CM サブスクライバと 1 つのバックアップ サブスクライバを含むように、各サイトを設定します。
- Unified CM の *グループ*と *デバイス プール*を設定して、サイト内のデバイスが、あらゆる状況でそのサイトのサーバだけに登録されるようにします。
- 各サイトで主要なサービス（TFTP、DNS、DHCP、LDAP、および IP Phone サービス）、すべてのメディア リソース（カンファレンス ブリッジと Music On Hold）、およびゲートウェイを複製します。複製を確実に行い、最大レベルの復元性を得るよう、シスコは強くお勧めします。また、この方法を拡張して、各サイトにボイスメール システムを組み込むこともできます。
- WAN 障害が発生した場合、パブリッシャ データベースへのアクセスがないサイトでは、いくつかの機能を使用できないことがあります。たとえば、リモート サイトのシステム管理者は、設定を一切追加、変更、または削除することができません。ただし、ユーザは、「Unified CM パブリッシャ」（P.2-24）の項にリストされているユーザ方向の機能に、引き続きアクセスできます。
- WAN 障害が発生した状態では、コールを発信するサブスクライバと現在通信していない電話番号にコールを発信すると、ファースト ビジー トーンが聞こえるか、またはコール転送されます（ボイスメールまたは Call Forward Unregistered で設定された宛先に転送される可能性があります）。

- Unified CM クラスタ内の任意の 2 つのサーバ間に可能な最大ラウンドトリップ時間（RTT）は、80 msec です。

（注）　ラウンドトリップ遅延時間が長く、Busy Hour Call Attempt（BHCA; 最繁時呼数）が多い状況では、音声のカットスルー遅延が大きくなる場合があり、音声コール確立時の初期音声クリッピングの原因となる場合があります。

- WAN を介してクラスタ化されているサイト間での最繁時呼数（BHCA）が 10,000 の Intra-Cluster Communications Signaling（ICCS）トラフィックに対して、最低でも 1.544 Mbps（T1）の帯域幅が必要です。これは、呼制御トラフィックに必要な最低限の帯域幅で、WAN を介してクラスタ化されているサイト間でディレクトリ番号が共有されていない配置に適用されます。特定の遅延が発生している共有されていないディレクトリ番号間での、10,000 BHCA を超えるトラフィックの帯域幅を計算する場合は、次の計算式をガイドラインとして使用できます。

  合計帯域幅（Mbps）=（合計 BHCA/10,000）×（1 + 0.006 × 遅延）、遅延 = RTT 遅延（ms 単位）

  この呼制御トラフィックは、優先トラフィックに分類されます。優先 ICCS トラフィックには、IP Precedence 3（DSCP 24 または PHB CS3）が付けられます。

- Intra-Cluster Communication Signaling（ICCS）トラフィックに必要な帯域幅に加え、リモートからパブリッシャとなるあらゆるサブスクライバ サーバに対するデータベースおよびその他のサーバ間トラフィック用に、最低でも 1.544 Mbps（T1）の帯域幅が必要になります。

- WAN を介した CTI Manager も配置する場合は、次の公式を使用して CTI 帯域幅（Mbps）を計算できます。

  (合計 BHCA/10,000) * 1.25

例 2-1　　2 つのサイトの帯域幅の計算

Unified CM を配置した 2 つのサイト（サイト 1、サイト 2）があると仮定します。2 つのサイトは WAN を介してクラスタ化されており、ラウンドトリップ時間は 80 ms です。サイト 1 にはパブリッシャが 1 つと、TFTP および Music on Hold（MoH）を組み合わせたサーバが 1 つ、そして 2 つの Unified CM サブスクライバ サーバが配置されています。サイト 2 には TFTP/MoH サーバが 1 つと、Unified CM サブスクライバ サーバが 2 つ配置されています。サイト 1 には 5000 台の電話機があり、それぞれ 1 つの DN を持っています。サイト 2 にも 5000 台の電話機があり、それぞれ 1 つの DN を持っています。煩雑時は、サイト 1 の 2500 台の電話機がサイト 2 の 2500 台の電話機を呼び出します。それぞれのコールは、3 BHCA です。同じ煩雑時に、サイト 2 の 2500 台の電話機もサイト 1 の 2500 台の電話機を呼び出します。それぞれのコールは、3 BHCA です。この場合、次のように計算します。

煩雑時の合計 BHCA = 2500 × 3 + 2500 × 3 = 15,000

サイト間で必要な合計帯域幅 = 合計 ICCS 帯域幅 + 合計データベース帯域幅

合計 BHCA が 15,000 であり、10,000 を超えているため、合計 ICCS 帯域幅 =（15,000/10,000）×（1 + 0.006 × 80）= 2.22 Mbps という計算式を使用できます。

合計データベース帯域幅 =（パブリッシャからリモートとなるサーバの数）× 1.544 = 3 × 1.544 = 4.632 Mbps

サイト間で必要な帯域幅 = 2.22 Mbps + 4.632 Mbps = 6.852 Mbps（およそ 7 Mbps）

- WAN を介してクラスタ化されているサイト間でディレクトリ番号が共有されている場合は、さらに帯域幅を確保する必要があります。最低限必要な 1.544 Mbps の帯域幅に加え、このようなオーバーヘッドと追加帯域幅が必要になります。共有 DN 間での 10,000 BHCA のトラフィックの場合、次の計算式を使用して計算できます。

オーバーヘッド = (0.012 × 遅延 × シェアドライン) + (0.65 × シェアドライン)、各値の意味は次のとおりです。

遅延 = IP WAN を介した RTT 遅延（ms 単位）

シェアドライン = WAN 経由でディレクトリ番号が共有されている追加の電話機の平均数

特定の遅延が発生している共有されているディレクトリ番号間での、10,000 BHCA を超えるトラフィックの帯域幅を計算する場合は、次の計算式をガイドラインとして使用できます。

合計帯域幅（Mbps）=（合計 BHCA/10,000）×（1 + 0.006 × 遅延 + 0.012 × 遅延 × シェアドライン + 0.65 × シェアドライン）、各値の意味は次のとおりです。

遅延 = RTT 遅延（ms 単位）

シェアドライン = WAN 経由でディレクトリ番号が共有されている追加の電話機の平均数

例 2-2　ディレクトリ番号を共有する 2 つのサイトの帯域幅の計算

Unified CM を配置した 2 つのサイト（サイト 1、サイト 2）があると仮定します。2 つのサイトは WAN を介してクラスタ化されており、ラウンドトリップ時間は 80 ms です。サイト 1 にはパブリッシャが 1 つと、TFTP および Music on Hold（MoH）を組み合わせたサーバが 1 つ、そして 2 つの Unified CM サブスクライバ サーバが配置されています。サイト 2 には TFTP/MoH サーバが 1 つと、Unified CM サブスクライバ サーバが 2 つ配置されています。サイト 1 には 5000 台の電話機があり、それぞれ 1 つの DN を持っています。サイト 2 にも 5000 台の電話機がありますが、それぞれがサイト 1 の 5000 台の電話機と DN を共有しています。そのため、各 DN は WAN 経由で共有され、平均して 1 台の追加の電話機を持つことになります。煩雑時は、サイト 1 の 2500 台の電話機がサイト 2 の 2500 台の電話機を呼び出します。それぞれのコールは、3 BHCA です。これにより、サイト 1 の電話機も呼び出すことになります。同じ煩雑時に、サイト 2 の 2500 台の電話機がサイト 1 の 2500 台の電話機を呼び出します。それぞれのコールは、3 BHCA です。これにより、サイト 2 の電話機も呼び出すことになります。この場合、次のように計算します。

煩雑時の合計 BHCA = 2500 × 3 + 2500 × 3 = 15,000

サイト間で必要な合計帯域幅 = 合計 ICCS 帯域幅 + 合計データベース帯域幅

合計 BHCA が 15,000 であり、10,000 を超えているため、合計 ICCS 帯域幅 = (15,000/10,000) × (1 + 0.006 × 80 + 0.012 × 80 × 1 + 0.65 × 1) = 4.635 Mbps という計算式を使用できます。

合計データベース帯域幅 =（パブリッシャからリモートとなるサーバの数）× 1.544 = 3 × 1.544 = 4.632 Mbps

サイト間で必要な帯域幅 = 4.635 Mbps + 4.632 Mbps = 9.267 Mbps（およそ 10 Mbps）

（注） 上記の帯域幅は、ICCS、データベース、およびその他のサーバ間トラフィックに限定したものです。コールが IP WAN を経由する場合は、コールに使用する音声コーデックに応じて、音声またはメディア トラフィック用に追加の帯域幅をプロビジョニングする必要があります。

- クラスタ内のサブスクライバ サーバは、ローカル データベースを読み取ります。データベースの変更は、変更のタイプに応じて、ローカル データベースとパブリッシャのデータベースの両方で発生する可能性があります。クラスタ内のさまざまなサーバの同期には、Informix Dynamic Server（IDS）のデータベース複製が使用されます。そのため、長期間にわたる WAN 接続の喪失など、障害状態から回復する場合は、障害時に行われた可能性があるあらゆる変更と Unified CM データベースを同期する必要があります。このプロセスは、パブリッシャとクラスタ内のその他のサーバへのデータベース接続が復元されると、自動的に実行されます。低帯域幅のリンクや遅延が大きいリンクでは、このプロセスに時間がかかる場合があります。また、まれなケースですが、手動によるリセットやサーバ間でのデータベース複製の修復が必要になる場合もあります。この操作

は、Command Line Interface（CLI; コマンドライン インターフェイス）で **utils dbreplication repair all** や **utils dbreplication reset all** などのコマンドを使用して実行します。WAN を経由して、リモートのサブスクライバでデータベース複製の修復またはリセットを実行すると、クラスタ内のすべての Unified CM データベースが再同期されます。この場合、1.544 Mbps を超える帯域幅が必要になる場合があります。低帯域幅の場合、データベース複製の修復またはリセットが完了するまでに、時間がかかる場合があります。

（注） 同一のリモート ロケーションにある複数のサブスクライバに対して、データベース複製の修復またはリセットを実行すると、データベース複製の完了に時間がかかる場合があります。このようなリモートのサブスクライバのデータベース複製を修復またはリセットする場合は、1 つずつ実行することをお勧めします。異なるリモート ロケーションにあるサブスクライバのデータベース複製を修復またはリセットする場合は、同時に実行することができます。

- 集中型コール処理を使用するリモート支店を、WAN を介したクラスタ化を使用してメイン サイトに接続する場合は、WAN を介したクラスタ化に使用されるリンクがオーバーサブスクリプションにならないよう、慎重にコール アドミッション制御を設定します。
  - WAN を介したクラスタ化に使用されるリンク上で帯域幅が制限されていない場合（つまり、リンクへのインターフェイスが OC-3s または STM-1s で、コール アドミッション制御に関する要件がない場合）は、リモート サイトがメイン サイトのいずれかに接続される場合があります。これは、すべてのメイン サイトでロケーションを Hub_None として設定する必要があるためです。この設定が行われても、コール アドミッション制御に使用するハブアンドスポーク トポロジは保持されます。
  - Multiprotocol Label Switching（MPLS）バーチャル プライベート ネットワーク（VPN）機能を使用している場合は、Unified CM ロケーションとリモート サイトにあるすべてのサイトが、メイン サイトのいずれかに登録される場合があります。
  - メイン サイト間の帯域幅が制限されている場合は、サイト間でコール アドミッション制御を使用し、ロケーションが Hub_None として設定されているメイン サイトにすべてのリモート サイトを登録する必要があります。このメイン サイトはハブ サイトと見なされ、それ以外のリモート サイトとクラスタオーバー WAN サイトはすべて、スポーク サイトとなります。
- ソフトウェア アップグレード時は、ソフトウェア リリース ノートで説明されている標準のアップグレード手順を使用して、クラスタ内のすべてのサーバを同じ保守期間内にアップグレードする必要があります。IP WAN 経由のラウンドトリップ遅延時間が大きい場合は、ソフトウェア アップグレードにかかる時間が長くなる場合があります。また、1.544 Mbps（T1 リンク）などの低帯域幅では、ソフトウェア アップグレード プロセスの完了に時間がかかる場合があります。このような状況でアップグレード プロセスの速度を向上させるには、1.544 Mbps を超える帯域幅が必要になる場合があります。

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

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

冗長性とアップグレード時間を改善するために、2 つの Unified CM サーバで Cisco Trivial File Transfer Protocol（TFTP）サービスを使用可能にすることをお勧めします。クラスタ内に複数の TFTP サーバを配置できますが、そのような構成ではすべての TFTP サーバ上ですべての TFTP ファイルを再構築するために時間がかかります。

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

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

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

ローカル フェールオーバー用のゲートウェイ

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

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

ローカル フェールオーバー用のボイスメール

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

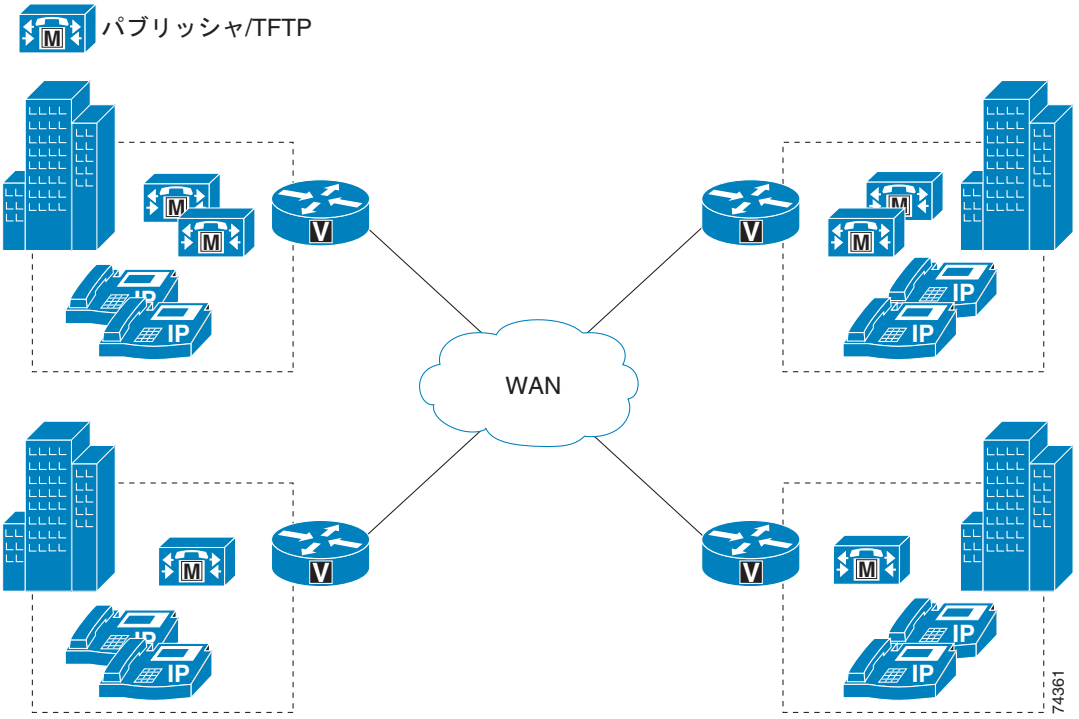
ローカル フェールオーバーに対する Music On Hold とメディア リソース

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

リモート フェールオーバー配置モデル

リモート フェールオーバー配置モデルでは、バックアップ サーバを柔軟に配置できます。各サイトには、少なくとも 1 つのプライマリ Unified CM サブスクライバを含め、バックアップ サブスクライバを必要に応じて配置します。このモデルでは、最大 8 つのサイトを配置できます。また、「コール処理」（P.8-1）の章で説明されている 1:1 冗長性と 50/50 ロードバランシング オプションを使用すると、IP Phone やその他のデバイスは、通常、ローカル サブスクライバに登録されます。バックアップ サブスクライバは、他の 1 つ以上のサイトで、WAN を介して配置されます（図 2-7 を参照）。

図 2-7　　4 サイト構成のリモート フェールオーバー モデル



リモート フェールオーバー モデルを実装する場合は、ローカル フェールオーバー モデルのガイドライン（「ローカル フェールオーバー配置モデル」（P.2-26）を参照）と、次の変更点に従ってください。

- 少なくとも 1 つのプライマリ Unified CM サブスクライバと、必要に応じてオプションのバックアップ サブスクライバを含むように、各サイトを設定します。IP WAN を経由したバックアップ サブスクライバを設定しない場合は、Survivable Remote Site Telephony（SRST）ルータをバックアップのコール処理エージェントとして使用できます。
- Unified CM の *グループ*と *デバイス プール*を設定して、WAN を介してサーバにデバイスを登録できるようにします。
- デバイスが、WAN を介して同じクラスタ内のリモート Unified CM サーバに登録される場合、シグナリング トラフィックまたは呼制御トラフィックのために帯域幅を追加する必要があります。この帯域幅は、ICCS トラフィックより大きくなる場合があります。また、シグナリングに関する帯域幅のプロビジョニング計算を使用して計算する必要があります（「帯域幅のプロビジョニング」（P.3-59）を参照）。

（注）　障害回復を目的として、これら 2 つのタイプの配置の機能を組み合わせることもできます。たとえば、Unified CM のグループでは、最大 3 つのサーバ（1 次、2 次、3 次）を設定することができます。そのため、同一のサイトに 1 次および 2 次のサーバを配置し、3 次サーバを WAN 経由でリモート サイトに配置するように Unified CM のグループを設定できます。

U. S. Section 508 準拠についての設計上の考慮事項

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

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

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

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

    IP Phone のハンドセットを TTY/TDD に接続しているカップリング機器に置きます。アコースティック カップルは、RJ-11 接続に比較すると信頼性が劣ります。カップリング方式は部屋の周囲の雑音やその他の要素で、一般的に通信エラーを起こしやすい方式です。
- stutter ダイヤルトーンをサポートする必要がある場合は、アナログ電話を Cisco VG248 または ATA 188 上に備えている FXS ポートに接続します。また、ほとんどの Cisco IP Phone では、スタッター ダイヤル トーンをサポートしています。この機能は、Audible Message Waiting Indication（AMWI; 音声メッセージ待機インジケータ）と呼ばれることもあります。この機能をサポートする具体的な Cisco IP Phone のモデルについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

CHAPTER 3

ネットワーク インフラストラクチャ

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

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

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

図 3-1　一般的なキャンパス ネットワーク インフラストラクチャ

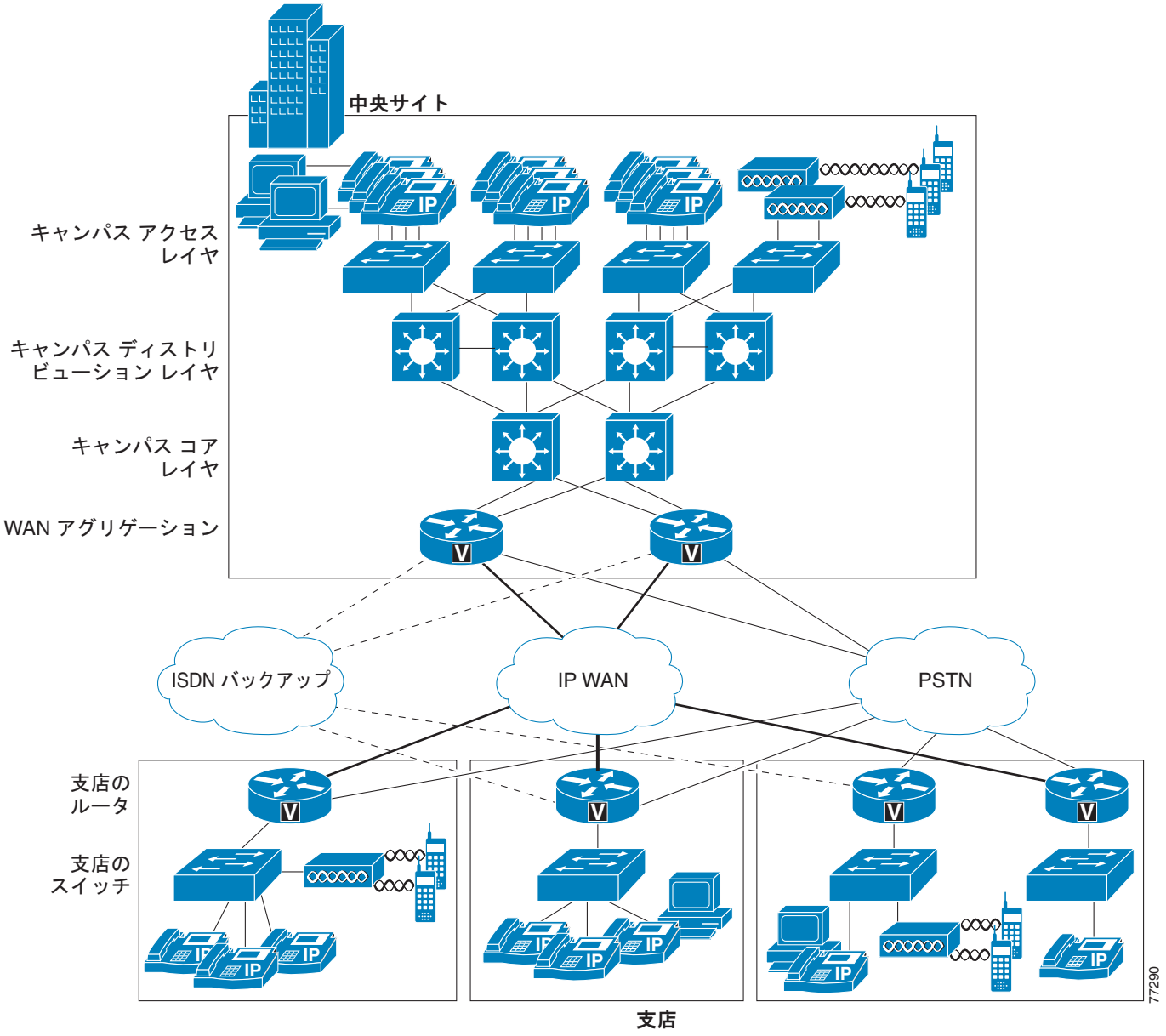


表 3-1　ネットワーク インフラストラクチャ内の役割に必要な機能

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

この章の新規情報

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

表 3-2　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
Cisco Unified Wireless IP Phone 7925G	この章の各項で説明
Dynamic Multipoint VPN	「Dynamic Multipoint VPN（DMVPN）」（P.3-39）
Bluetooth デバイスからの干渉	「無線の干渉」（P.3-76）

表 3-2　新規情報、またはこのマニュアルの以前のリリースからの変更情報 （続き）

新規トピックまたは改訂されたトピック	説明箇所
Trusted Relay Point（TRP）を使用した QoS の強制	「Trusted Relay Point（TRP）を使用した QoS の強制」（P.3-35）
ルーテッド（routed）アクセス レイヤの設計	「ルーテッド アクセス レイヤ設計」（P.3-7）
RSVP P Hop の上書き	「MPLS ネットワークにおける RSVP」（P.3-50）
無線エンドポイントのセキュリティ	「無線セキュリティ」（P.3-78）

LAN インフラストラクチャ

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

- 「高可用性のための LAN 設計」（P.3-4）
- 「LAN の QoS」（P.3-31）

高可用性のための LAN 設計

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

- 「キャンパス アクセス レイヤ」（P.3-4）
- 「キャンパス ディストリビューション レイヤ」（P.3-10）
- 「キャンパス コア レイヤ」（P.3-14）
- 「ネットワーク サービス」（P.3-15）

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

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

キャンパス アクセス レイヤ

キャンパス LAN のアクセス レイヤに含まれるネットワーク部分は、デスクトップ ポートからワイヤリング クローゼット スイッチまでです。従来、アクセス レイヤ スイッチはディストリビューション レイヤへのレイヤ 2 アップリンクを持つレイヤ 2 デバイスとして設定されてきました。レイヤ 2 およびレイヤ 2 アクセス設計に対応するスパニング ツリーの推奨事項は、十分に実証されており、以下に簡単に説明します。レイヤ 3 プロトコルをサポートする最新の Cisco Catalyst スイッチでは、新しいルー

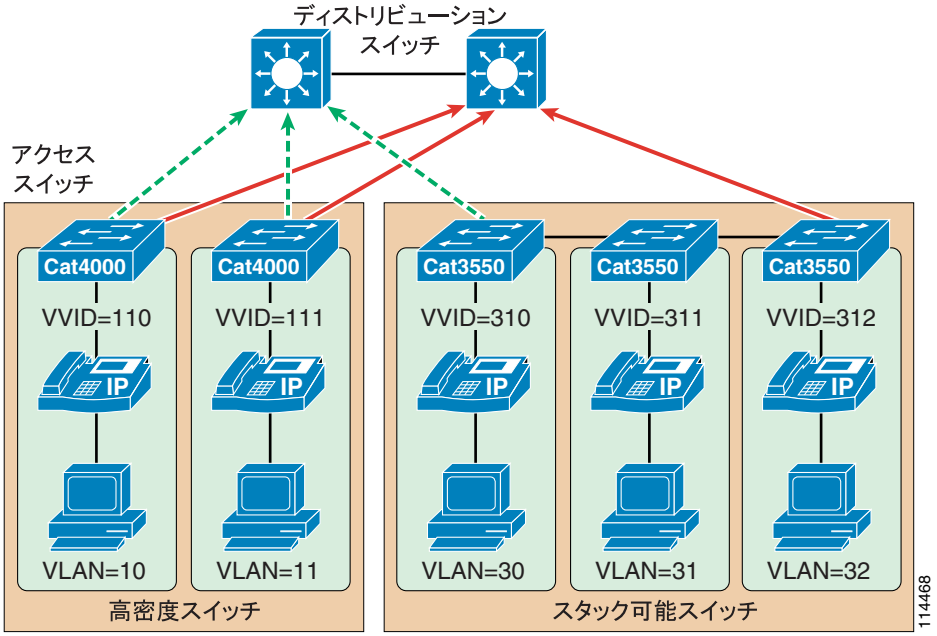
テッド アクセス設計が可能となり、コンバージェンス時間と設計の簡素化における改善が行われています。ルーテッド アクセス設計については、「ルーテッド アクセス レイヤ設計」（P.3-7）の項で詳しく説明します。

レイヤ 2 アクセス設計の推奨事項

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

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

図 3-2　音声とデータに対応するアクセス レイヤ スイッチと VLAN



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

次の理由により、音声とデータの VLAN を分離することをお勧めします。

- アドレス スペースの確保と、外部ネットワークからの音声デバイスの保護

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

- QoS 信頼性境界の音声デバイスへの拡張

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

- 悪質なネットワーク攻撃からの保護

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

- 管理および設定の容易性

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

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

- 電話機が接続されているポート上でレイヤ 2 CoS パケット マーキングを適切に処理するための 802.1Q トランキングおよび 802.1p

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

Spanning Tree Protocol（STP）

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

- PortFast

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

- ルート ガードまたは BPDU ガード

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

- UplinkFast と BackboneFast

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

- 単方向リンク検出（UDLD）

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

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

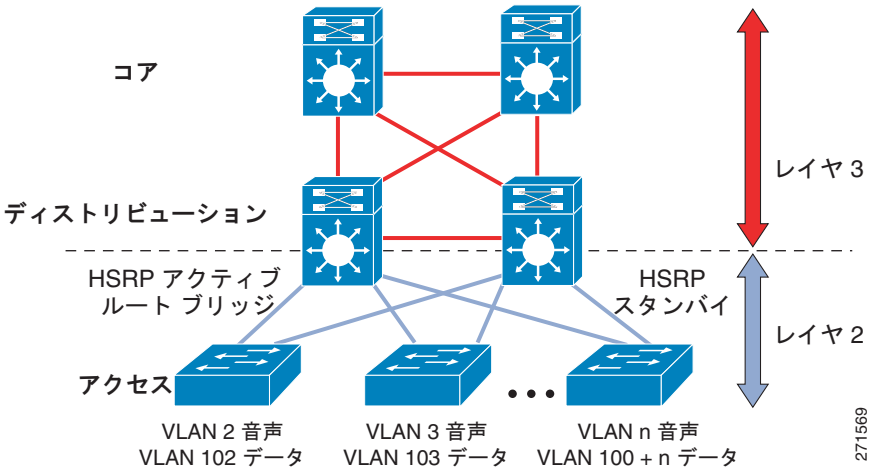
ルーテッド アクセス レイヤ設計

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

アクセス レイヤへの L2/L3 境界の移行

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

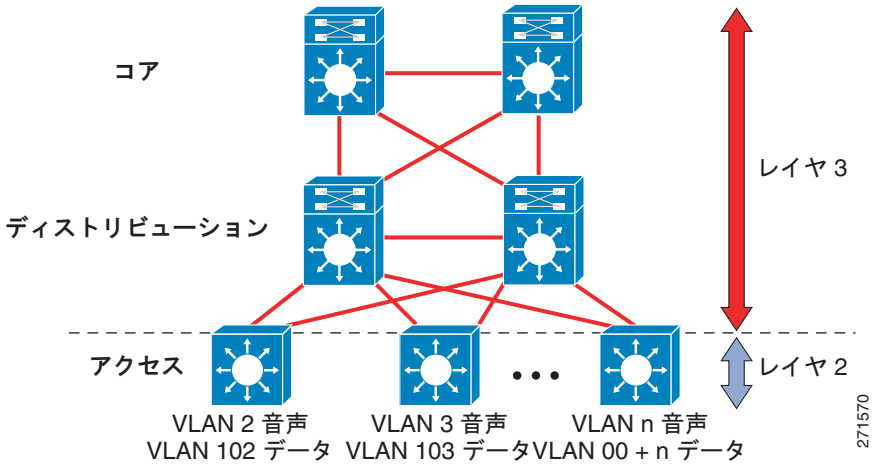
図 3-3　　従来のキャンパス設計：レイヤ 3 ディストリビューションを使用したレイヤ 2 アクセス



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

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

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



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

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

ルーテッド アクセス コンバージェンス

レイヤ 3 アクセス設計の使用には、次のような多くの潜在的利点があります。

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

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

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

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

キャンパス ディストリビューション レイヤ

キャンパス LAN のディストリビューション レイヤに含まれるネットワーク部分は、ワイヤリング クローゼットスイッチからネクストホップ スイッチまでです。ディストリビューション レイヤ スイッチには、一般に、レイヤ 3 対応の Cisco Catalyst 4000 および 6000 シリーズ スイッチと、より小規模な配置用の Cisco Catalyst 3750 があります。

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

ファーストホップ冗長プロトコル

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

ホット スタンバイ ルータ プロトコル(HSRP)と仮想ルータ冗長プロトコル(VRRP)

シスコは、必要なデフォルト ゲートウェイの冗長性に対応するために、ホットスタンバイ ルータ プロトコル（HSRP）を開発しました。その後、インターネット技術タスクフォース（IETF）は、仮想ルータ冗長プロトコル（VRRP）をデフォルト ゲートウェイの冗長性を備える標準ベースの方法として承認しました。

Cisco 機能拡張に対応する HSRP および VRRP は、両方ともデフォルト ゲートウェイをバックアップする堅固な方法を備え、適切に調整された場合、冗長なディストリビューション スイッチに 1 秒未満でフェールオーバーを提供することができます。HSRP と VRRP を選択する場合、シスコ独自の標準であり、VRRP より先に HSRP 用の機能を迅速に開発できるため、シスコは HSRP をお勧めします。ただし、シスコ製以外のデバイスとの相互運用性が必要となる場合、VRRP が正しい選択となります。

Gateway Load Balancing Protocol（GLBP）

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

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

GLPB は HSRP と同じように設定され、機能します。HSRP では、Address Resolution Protocol（ARP）を使用してデフォルト ゲートウェイの物理 MAC アドレスを取得するときに、単一の仮想 MAC アドレスがエンドポイントに指定されます。2 つの仮想 MAC アドレスが、各 GLBP ピアに 1 つずつ GLBP と共に存在します。エンドポイントが ARP を使用してデフォルト ゲートウェイを決定する

場合、仮想 MAC アドレスがラウンドロビン方式で照合されます。フェールオーバーとコンバージェンスは、HSRP と同様に動作します。バックアップ ピアは、障害が発生したデバイスの仮想 MAC アドレスを想定して、障害が発生したピアへのトラフィックの転送を開始します。

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

次の項では、HSRP 設定と操作について説明します。前述のように、GLBP は HSRP と同じように設定され、機能しますが、基本的なロード バランシング機能の追加の利点があります。

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

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

ホットスタンバイ ルータ プロトコル（HSRP）

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

- standby track

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

- standby preempt

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

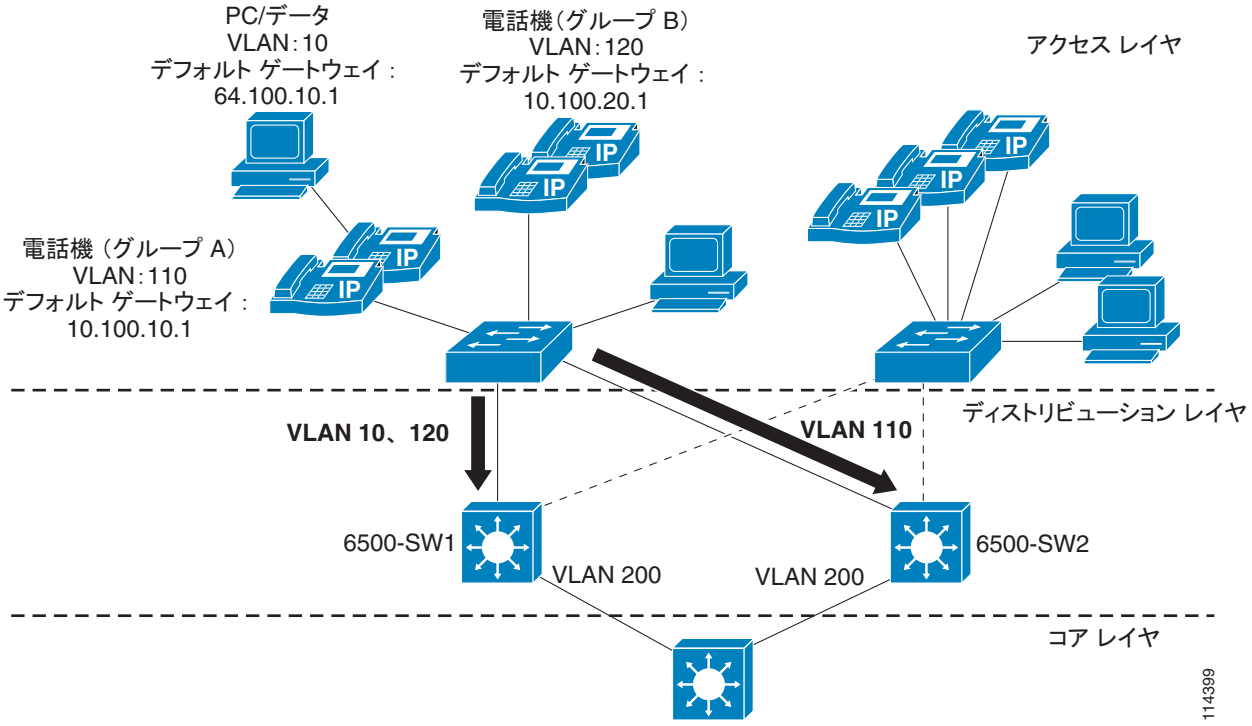
また、HSRP には、両方の HSRP ルータ間でトラフィックをロード バランシングするように設定する必要があります。ロード バランシングを行うには、アクティブ HSRP ルータである各 HSRP デバイスを 1 つの VLAN またはインターフェイス用に設定し、スタンバイ ルータを別の VLAN またはインターフェイス用に設定します。両方の HSRP デバイスにアクティブ VLAN とスタンバイ VLAN を均等に分散させると、ロード バランシングが保証されます。1 つの VLAN 上のデバイスは、アクティブ HSRP デバイスをそのデフォルト ゲートウェイとして使用し、別の VLAN 上の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

図 3-5 は、HSRP 対応のネットワークの例を示しています。この図では、2 つの Catalyst 6500 スイッチ（6500-SW1 と 6500-SW2）に複数の VLAN インターフェイスが設定されています。ネットワーク内にリンク障害がないことを前提とすると、6500-SW1 は、VLAN 110（Group A の電話機の Voice VLAN）に対応するスタンバイ HSRP ルータであり、VLAN 10（データ VLAN）および VLAN 120（Group B の電話機の Voice VLAN）に対応するアクティブ HSRP ルータになっています。6500-SW2 は、その逆に設定されています。つまり、VLAN 110 に対応するアクティブ HSRP ルータであり、VLAN 10 および VLAN 120 に対応するスタンバイ HSRP ルータになっています。両方のスイッチは、設定どおり、アクティブに使用されています。両者にすべてのレイヤ 2 VLAN を均等に分散させると、負荷を両者に分散させることができます。また、各スイッチは、そのローカル VLAN 200 インターフェイスをトラックするように設定されており、VLAN 200 にリンク障害が発生した場合は、もう一

方のスイッチがプリエンプション処理し、すべての VLAN に対応するアクティブ ルータとなります。同様に、一方のスイッチに障害が発生した場合は、もう一方のスイッチが 3 つの VLAN すべてのトラフィックを処理します。

図 3-5 のアクセス レイヤにある PC と電話機には、各 HSRP グループの HSRP アドレスに対応したデフォルト ゲートウェイが設定されています。Voice VLAN 110 および 120 のデバイスは、デフォルト ゲートウェイとして 10.100.10.1 と 10.100.20.1 をそれぞれ指しています。これらのデフォルト ゲートウェイは、両方のスイッチにある VLAN 110 および 120 インターフェイスの HSRP アドレスに対応しています。データ VLAN 10 のデバイスは、デフォルト ゲートウェイとして 64.100.10.1 を指しています。このデフォルト ゲートウェイは、両方のスイッチにある VLAN 10 インターフェイスの HSRP アドレスに対応しています。アクセス レイヤからディストリビューション レイヤに流れるトラフィックは 2 つのスイッチに分散されます（障害がない場合）が、リターン パスでの分散を保証するメカニズムはありません。コア レイヤから戻ってアクセス レイヤに向かうトラフィックは、最短および最小コストの、またはそのどちらかのルーテッド パスに沿って流れます。

図 3-5　standby preempt と standby track を使用した HSRP ネットワーク設定の例



例 3-1 および 例 3-2 は、図 3-5 に示されている 2 つの Catalyst 6500 スイッチの設定を示しています。

例 3-1　6500-SW1 の設定

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

interface Vlan110
 description Voice VLAN 110
 ip address 10.100.10.11 255.255.255.0
 standby preempt
```

```
 standby ip 10.100.10.1
 standby track Vlan 200
 standby priority 95

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

例 3-2　　6500-SW2 の設定

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

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

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

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

ルーティング プロトコル

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

ためです。アクセス レイヤ方向のすべてのインターフェイス上で **passive-interface** コマンドを使用すると、ルーティング アップデートがこれらのインターフェイスから送信されることが防止されます。したがって、ネイバールータとの隣接関係は形成されません。

キャンパス コア レイヤ

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

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

- 冗長なリンクまたはケーブル パス

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

- 冗長なデバイス

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

- 冗長なデバイス サブシステム

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

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

データ センターとサーバ ファーム

一般に、メディア リソース サーバなどの Cisco Unified CM（Unified CM）クラスタ サーバは、データ センターまたはサーバ ファーム環境に配置されます。また、カンファレンス ブリッジ、DSP またはトランスコーダ ファーム、およびメディア ターミネーション ポイントなどの、集中型ゲートウェイと集中型ハードウェア メディア リソースも、データ センターまたはサーバ ファームに配置されます。これらのサーバとリソースは音声ネットワークにおいて重要であるため、すべての Unified CM クラスタ サーバ、集中型音声ゲートウェイ、および集中型ハードウェア リソースは、複数の物理スイッチに分散させ、可能であればキャンパス内の複数の物理ロケーションにも分散させることをお勧めします。このようにリソースを分散させると、ハードウェア障害（スイッチやスイッチのライン カードの障害など）が発生しても、少なくともクラスタ内の一部のサーバを使用して、引き続きテレフォニー サービスを提供できることが保証されます。また、一部のゲートウェイとハードウェア リソースを使用して、引き続き公衆網へのアクセスと付加サービスを提供することもできます。物理的に分散させるだけでなく、これらのサーバ、ゲートウェイ、およびハードウェア リソースを別の VLAN またはサブネットに分散させる必要もあります。そのように分散させると、特定の VLAN 上でブロードキャスト ストームまたは DoS 攻撃が発生しても、一部の音声接続およびサービスは中断されずにすみます。

ネットワーク サービス

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

ドメイン ネーム システム（DNS）

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

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

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

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

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

DNS を使用した Unified CM の配置

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

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

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

Unified CM は DNS を使用して以下を実行できます。

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

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

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

表 3-3　Unified CM における DNS の使用例

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

Dynamic Host Configuration Protocol（DHCP）

DHCP は、ネットワーク上のホストが、IP アドレス、サブネット マスク、デフォルト ゲートウェイ、および TFTP サーバ アドレスなどの初期設定情報を取得するために使用します。DHCP により、各ホストに IP アドレスやその他の設定情報を手動で設定する管理負担が軽減されます。また、DHCP によ

り、デバイスをサブネット間で移動したときに、ネットワーク設定が自動的に再設定されます。設定情報はネットワーク内にある DHCP サーバから提供されます。このとき、DHCP サーバは、DHCP 対応のクライアントから送信される DHCP 要求に応答します。

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

DHCP オプション 150

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

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

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

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

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

電源復帰後の電話機による DHCP オペレーション

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

DHCP のリース期間

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

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

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

次のいずれかの方法によって、この状況を緩和できます。

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

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

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

  このアプローチは、WAN 接続の中断の影響を受けません。このアプローチを使用すると、IP アドレスの管理が分散されるため、各拠点 で設定を更新する作業が発生します（詳細については、「DHCP のネットワーク配置」（P.3-19）を参照してください）。

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

DHCP のネットワーク配置

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

- 中央の DHCP サーバ

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

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

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

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

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

```
! Activate DHCP Service on the IOS Device

service dhcp

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

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

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

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

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

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

ほとんどのネットワーク インフラストラクチャで、通常、DHCP サーバは専用のマシンで、そのネットワークで使用する DNS サービスと Windows Internet Naming Service（WINS）サービスを組み合せて実行します。場合によっては、クラスタに登録されているデバイスが 1000 以下の小規模な

Unified CM の配置では、DHCP サーバを Unified CM サーバで実行して、これらのデバイスをサポートできます。ただし、Unified CM 上で実行する他の重要なサービスとの CPU 競合などの考えられるリソースの競合を回避するために、DHCP サーバの機能を専用サーバに移動することをお勧めします。クラスタに 1000 を超えるデバイスが登録されている場合は、DHCP を Unified CM サーバでは*実行しない*で、専用のスタンドアロン サーバで実行する必要があります。

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

トリビアル ファイル転送プロトコル（TFTP）

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

TFTP ファイル システムは、次のような複数のファイル タイプを保持することができます。

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

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

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

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

（注）Cisco Unified CM 6.1 よりも前のリリースでは、TFTP サーバは、変更されたファイルを再構築するために、パブリッシャのデータベースから情報をプルしました。Unified CM 6.1 以降のリリースでは、TFTP サーバは、共存するサブスクライバ サーバ上のデータベースからローカル データベースの読み取りを実行できます。ローカル データベースの読み取りは、パブリッシャが使用できない場合にユーザ向けの機能を保持するなどの利点を提供するだけではなく、WAN を介したクラスタ化を通じて、複

数の TFTP サーバの分散を可能にします（WAN を介したクラスタ化と同じ遅延規則が、登録済み電話機を持つサーバに関して TFTP サーバに適用されます）。この設定により、TFTP サービスがエンドポイントに近くなるため、遅延が低減されるほか、サイト間で障害が分離されることが保証されます。

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

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

TFTP 動作の例

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

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

TFTP ファイル転送時間

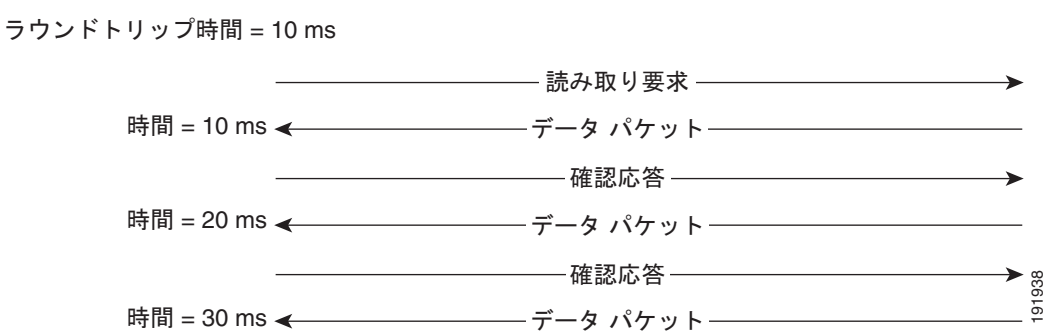
エンドポイントがファイルを要求するたびに、新しい TFTP 転送セッションが確立します。集中型コール処理配置の場合、これらの各転送が完了する時間は、エンドポイントを起動し、動作可能にするためにかかる時間と定期保守時にエンドポイントをアップグレードするためにかかる時間に影響を与えます。TFTP 転送時間は、これらの最終状態に影響を与える唯一の要因ではありませんが、重要なコンポーネントです。

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

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

TFTP はユーザ データグラム プロトコル（UDP）上で動作します。伝送制御プロトコル（TCP）とは異なり、UDP は信頼性の高いプロトコルではありません。つまり、UDP は本質的にパケット損失を検出する機能を備えていません。言うまでもなく、ファイル転送におけるパケット損失の検出は重要であるため、RFC 1350 は TFTP をロックステップ プロトコルとして定義しています。つまり、TFTP 送信側は 1 つのパケットを送信し、次のパケットを送信する前に応答を待ちます（図 3-6 を参照）。

図 3-6　TFTP パケット転送シーケンスの例

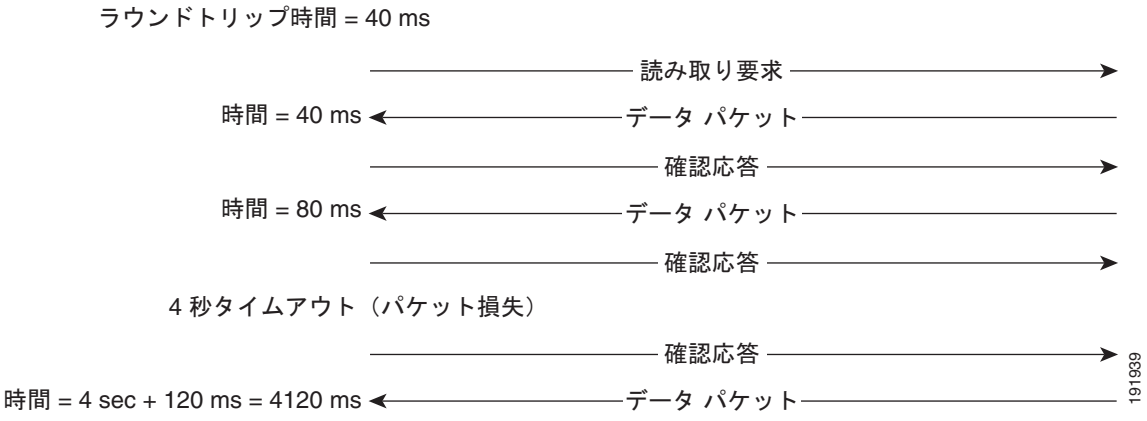


応答がタイムアウト時間（デフォルトでは 4 秒）内に受信されない場合、送信側はデータ パケットまたは確認応答を再送信します。5 回送信されても応答がない場合、TFTP セッションは失敗します。タイムアウト時間は常に同じであり、TCP タイムアウトのように適応できないので、パケット損失は、転送セッションを完了するのにかかる時間を大幅に増加させる可能性があります。

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

図 3-7 では、ラウンドトリップ時間が 40 ms に増加し、1 つのパケットが送信中に失われています。エラー率が 12% と高い率である一方、セッションを完了する時間が 30 ms（図 3-6 を参照）から 4160 ms（図 3-7 を参照）に増加しているので、TFTP の遅延とパケット損失の効果が簡単にわかります。

図 3-7　TFTP セッション完了時間におけるパケット損失の効果



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

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

定義：

FileTransferTime は秒単位です。

FileSize はバイト単位です。

RTT はラウンドトリップ時間（ミリ秒単位）です。

ERR はエラー率または失われたパケットの比率です。

Timeout はミリ秒単位です。

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

表 3-4 と 表 3-5 は、この公式を使用して、各種エンドポイント デバイス タイプ、プロトコル、およびネットワーク遅延用のソフトウェア ファイルの転送時間を計算した例を示しています。

表 3-4　SCCP デバイスの TFTP ファイル転送時間

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

表 3-5　SIP デバイスの TFTP ファイル転送時間

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

表 3-4 と 表 3-5 の値は、必要なファームウェア ファイルを電話機にダウンロードするおおよその時間です。これは、電話機を新しいファームウェアにアップグレードし、動作可能になるまでにかかる時間の推定値では*ありません*。

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

ネットワーク遅延とパケット損失は TFTP 転送時間に上記のような影響を与えるので、ローカルの TFTP サーバは便利です。このローカルの TFTP サーバは、WAN を介したクラスタを使用する配置における Unified CM サブスクライバか、または Cisco 統合サービス ルータ（ISR）などで実行する代替のローカル TFTP Load Server です。最新のエンドポイント（より大きなファームウェアファイルを必要とする）は、Load Serverアドレスを使用して設定できます。これにより、エンドポイントは、中央の TFTP から比較的小さい設定ファイルをダウンロードする一方で、ローカルの TFTP サーバ（Unified CM クラスタの一部ではない）を使用してより大きなソフトウェア ファイルをダウンロードできます。代替のローカル TFTP Load Server は、Cisco Unified IP Phones 7911、7921、7925、7937、7941、7942、7945、7961、7962、7965、7970、7971、および 7975 によってサポートされます。

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

TFTP サーバの冗長性

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

TFTP のロード シェアリング

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

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

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

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

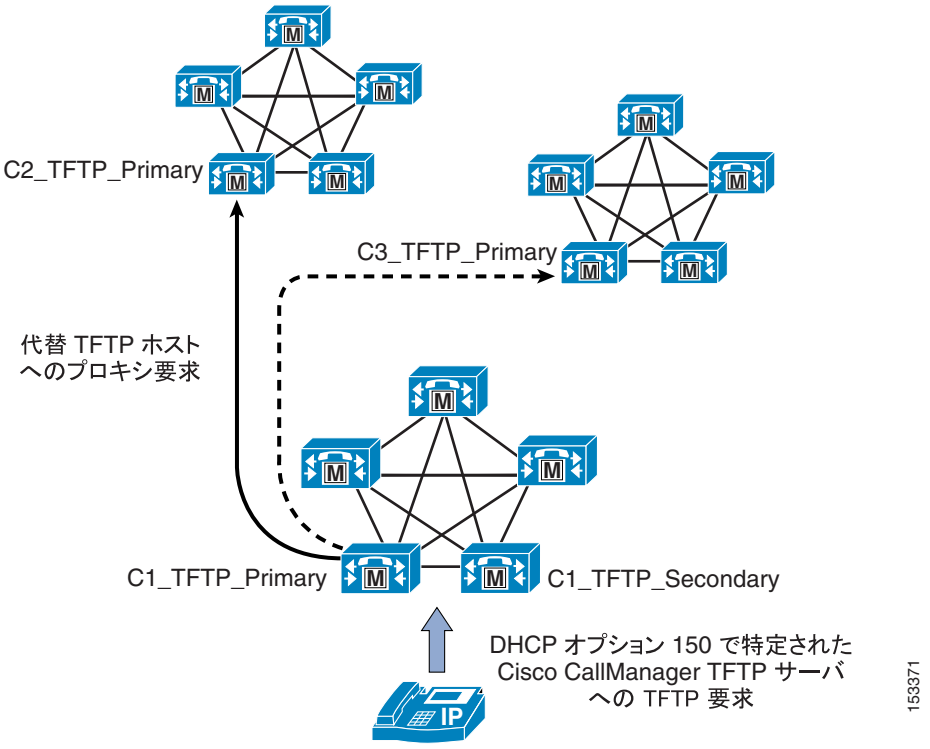
中央集中型 TFTP サービス

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

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

図 3-8 に、このプロセスの動作例を示します。Cluster 3 に登録されている電話機からの要求は、Cluster 1 で設定されている中央集中型 TFTP サーバ（C1_TFTP_Primary）に転送されます。このサーバは、次に、電話機が要求したファイルのコピーによる最初の応答があるまで、設定済みの代替 TFTP サーバのそれぞれに対して問い合せます。中央集中型セカンダリ TFTP サーバ（C1_TFTP_Secondary）への要求は、要求されたファイルが見つかるか、すべてのサーバから要求されたファイルが存在しないという応答があるまで、プロキシによって別のクラスタのセカンダリ TFTP サーバに送信されます。

図 3-8　中央集中型 TFTP サーバ



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

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

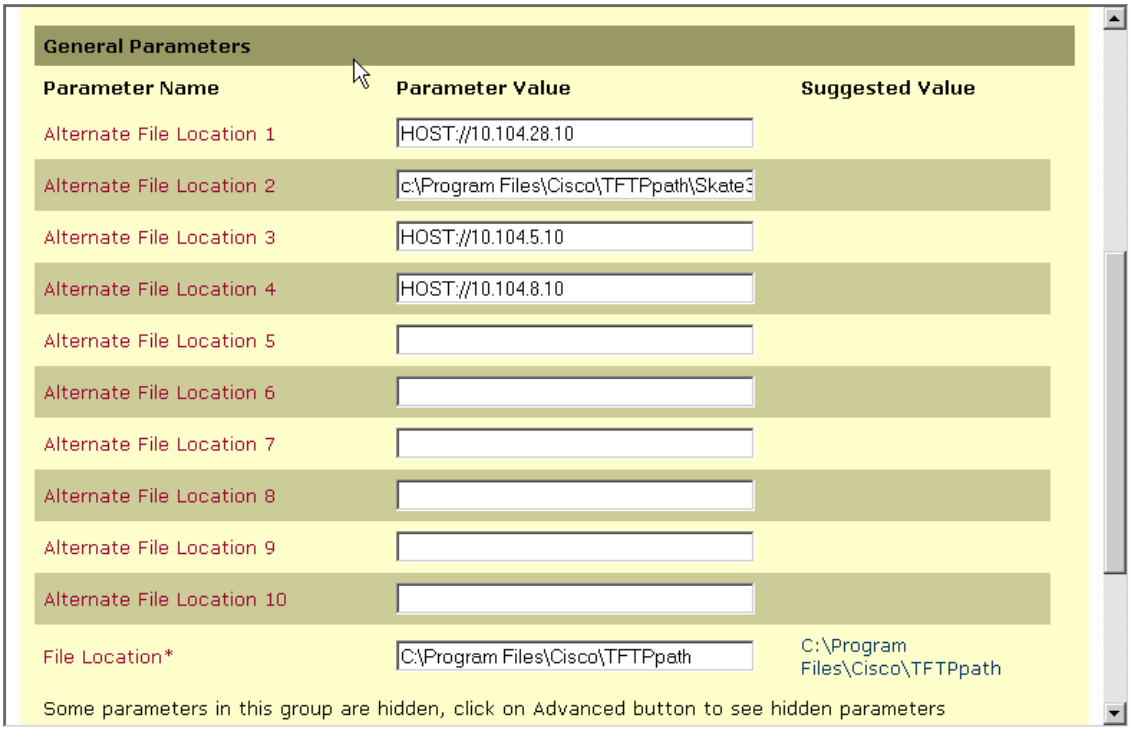
（注）　Cisco Unified CM Release 4.1(3)SR3a（およびそれ以降の Windows OS プラットフォーム対応の Unified CM リリース）には、混合モードの中央集中型 TFTP 設計をサポートする cTFTP サーバ デーモンへのアップグレードが含まれています。これらのリリースでは、中央集中型 TFTP サーバがリモート マウントとプロキシ要求の両方を、他のクラスタ内の代替 TFTP ファイル サーバに到達する方法としてサポートします。

混合モードの TFTP サーバを設定する場合、HOST プロキシ要求によって Unified CM 5.0 以降のリリースに対応するサーバを指定し、リモート マウント設定プロセスを使用して Unified CM 4.1(3)SR3a 以前の任意のサーバを指定する必要があります。図 3-9 を参照してください（リモート マウント設定の詳細については、以下を参照してください）。混合モードをサポートする任意の子クラスタは、リモート マウントとプロキシ クラスタのどちらにも設定できます。

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

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

図 3-9　　デュアル モード設定



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

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

例 3-4　　代替 TFTP ファイル ロケーション

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

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

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

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

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

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

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

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

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

（注） Cisco Unified CM Release 5.1 以降では、Enable Caching of Configuration Files サービス パラメータが使用できなくなり、設定ファイルは常にメモリにキャッシュされます（ディスクに書き込むのではなく）。

ネットワーク タイム プロトコル（NTP）

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

Unified CM の NTP 時刻同期

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

Unified CM 5.0 以降のリリースでは、クラスタのすべてのサブスクライバの NTP 時刻をパブリッシャと自動的に同期します。インストール時に、各サブスクライバは自動的に、パブリッシャで実行されている NTP サーバをポイントするように設定されます。パブリッシャはマスタ サーバと見なされ、外部サーバと同期するように設定されている場合を除き、内部ハードウェア クロックを基にクラスタに時

刻を提供します。クラスタの時刻と外部時刻源を確実に同期させるために、パブリッシャは Stratum-1、Stratum-2、または Stratum-3 NTP サーバをポイントするように設定することを強くお勧めします。

Unified CM 5.0 以降のリリースでは、Unified CM を Cisco IOS または Linux ベースの NTP サーバと同期することをお勧めします。Windows Time サービスを NTP サーバとして使用することは推奨しておらず、サポートもしていません。これは、Windows Time サービスでは、多くの場合、Simple Network Time Protocol（SNTP; 簡易ネットワーク タイム プロトコル）を使用しており、Linux ベースの Unified CM では SNTP との同期が失敗するためです。

プライマリ ノードに指定する外部 NTP サーバは、互換性、精度、およびネットワーク ジッタに関する潜在的な問題を回避するために、NTP v4（バージョン 4）とする必要があります。外部 NTP サーバは、IPv6 アドレッシングを使用する場合は NTP v4 とする*必要があります*。

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

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

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

Cisco IOS と CatOS の NTP 時刻同期

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

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

例 3-5　Cisco IOS と CatOS の NTP 設定

Cisco IOS の設定：

```
ntp server 64.100.21.254
```

CatOS の設定：

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

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

Power over Ethernet（PoE）

PoE（またはインライン パワー）は、標準的なイーサネット Unshielded Twisted-Pair（UTP; シールドなしツイストペア）ケーブルを介して供給される 48 V DC 電源です。IP Phone や、Aironet Wireless Access Points などのインライン Powered Device（PD; 受電装置）は、壁面コンセントを使用する代わ

りに、インライン パワー対応の Catalyst イーサネット スイッチや他のインライン Power Source Equipment（PSE）によって供給される電力を受信できます。デフォルトでは、インライン パワーは、すべてのインライン パワー対応 Catalyst スイッチ上で有効になっています。

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

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

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

シスコでは現在、Cisco PoE インライン パワーのほかに、IEEE 802.3af PoE 標準をサポートしています。現時点で 802.3af に準拠しているのは、一部のアクセス スイッチおよび電話機だけです。将来的には、すべての電話機とスイッチが 802.3af PoE をサポートする予定です。Catalyst 6500、4500、および 3750 は、現在、802.3af をサポートしています。802.3af PoE 標準をサポートする Cisco Unified IP Phone については、「エンドポイント機能の要約」（P.20-48）を参照してください。

カテゴリ 3 ケーブリング

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

- PC ポートを持ち、そのポートに PC が接続された IP Phone（Cisco Unified IP Phone 7975、7971、7970、7965、7962、7961、7960、7945、7942、7941、7940、7911、および 7910+SW）は、10 Mb 全二重に設定されている必要があります。

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

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

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

- PC ポートを持つが、そのポートに PC が接続されていない IP Phone（Cisco Unified IP Phone 7975、7971、7970、7965、7962、7961、7960、7945、7942、7941、7940、7912、7911、および 7910+SW）は、10Mb 半二重にネゴシエートできるようにしてもかまいません。

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

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

IBM タイプ 1A および 2A ケーブリング

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

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

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

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

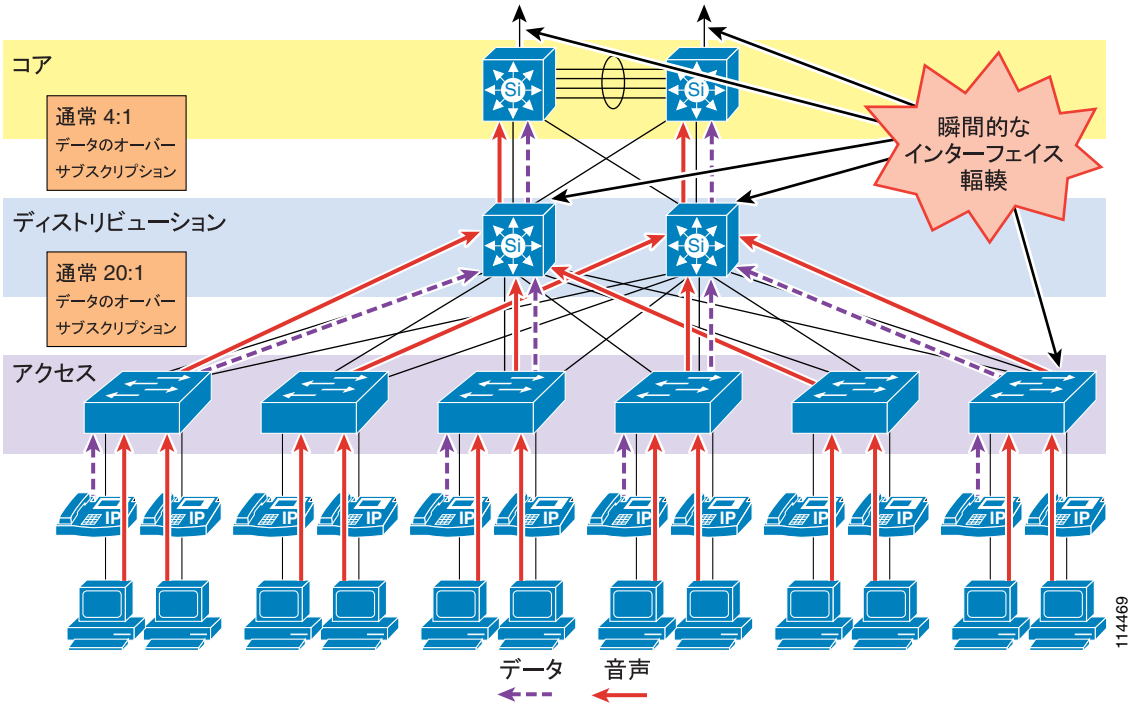
ネットワーク上でデータを伝送しても、ケーブル プラントの品質を十分にテストしたことにならない場合があります。これは、このようなテストでは、準拠に起因しない問題が判明しない場合があるためです。したがって、お客様は、タイプ 1A および 2A ケーブリングの設置がイーサネット標準に準拠していることを確認するために、ケーブル プラントの調査を実施することをお勧めします。

LAN の QoS

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

図 3-10 は、LAN インフラストラクチャで発生する一般的なオーバーサブスクリプションを示しています。

図 3-10　LAN におけるデータ トラフィックのオーバーサブスクリプション



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

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

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

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

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

- トラフィック分類

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

- キューイングまたはスケジューリング

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

- 帯域幅のプロビジョニング

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

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

- 「トラフィック分類」（P.3-33）
- 「インターフェイス キューイング」（P.3-35）
- 「帯域幅のプロビジョニング」（P.3-35）
- 「QoS が使用されない場合の IP コミュニケーションの障害」（P.3-36）

トラフィック分類

可能な限りネットワーク エッジの近くでトラフィックを分類したり、マークすることは、常に Cisco ネットワーク デザイン アーキテクチャの必要不可欠となる部分でした。トラフィック分類は、キャンパス スイッチおよび WAN インターフェイス内で使用される各種キューイング体系にアクセスするための基本的基準です。IP Phone は、その音声制御シグナリングと音声 RTP ストリームを送信元でマークします。その際は、表 3-6 に示されている値に従います。IP Phone は、このようにトラフィック フローを分類可能であり、実際に分類する必要があります。

表 3-6 は、LAN インフラストラクチャのトラフィックを分類する場合の要件をリストしています。

表 3-6　各種タイプのネットワーク トラフィックのトラフィック分類ガイドライン

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

表 3-6　各種タイプのネットワーク トラフィックのトラフィック分類ガイドライン （続き）

アプリケーション	レイヤ 3 分類			レイヤ 2 分類
	IP Precedence（IPP）	Per-Hop Behavior（PHB）	Differentiated Services Code Point（DSCP）	サービス クラス（CoS）
ネットワーク管理	2	CS2	16	2
Scavenger	1	CS1	8	1
ベストエフォート型	0	0	0	0

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

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

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

ビデオ テレフォニーのトラフィック分類

IP ビデオ テレフォニーに関係する主なクラスは、次のとおりです。

- 音声

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

- ビデオ会議

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

- コール シグナリング

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

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

ビデオ コールと音声専用コール間の QoS マーキングの相違点

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

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

シグナリング クラスは、すべての音声シグナリング プロトコル（SCCP、MGCP など）、およびビデオ シグナリング プロトコル（SCCP、H.225、RAS、CAST など）に適用されます。これらのプロトコルについては、「ソフトウェアベースのエンドポイント」（P.20-38）の項で詳しく説明します。

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

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

Trusted Relay Point（TRP）を使用した QoS の強制

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

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

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

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

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

インターフェイス キューイング

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

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

キャンパス内の送信インターフェイス バッファは、ネットワーク トラフィック自体にバースト性があるため、短い時間間隔で散発的に輻輳する傾向があります。輻輳が起きると、その送信インターフェイスを宛先とするすべてのパケットがドロップされます。音声トラフィックのドロップを防止する唯一の方法は、キャンパス スイッチ上で複数のキューを設定することです。このため、ポートごとに 2 つ以上の出力キューを持ち、レイヤ 2、レイヤ 3、またはその両方の QoS 分類に基づいてこれらのキューにパケットを送信する機能を持つスイッチを常に使用することをお勧めします。Cisco Catalyst 6000 シリーズ、4000 シリーズ、3750、3500 シリーズ、および 2950 スイッチはすべて、ポートごとに複数の出力キューをサポートします。

帯域幅のプロビジョニング

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

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

QoS が使用されない場合の IP コミュニケーションの障害

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

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

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

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

WAN インフラストラクチャ

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

- 「WAN の設計と設定」（P.3-37）
- 「WAN の QoS」（P.3-40）
- 「リソース予約プロトコル（RSVP）」（P.3-47）
- 「帯域幅のプロビジョニング」（P.3-59）

WAN の設計と設定

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

- 「配置上の考慮事項」（P.3-37）
- 「保証帯域幅」（P.3-38）
- 「ベストエフォート型の帯域幅」（P.3-39）

配置上の考慮事項

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

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

トポロジ対応コール アドミッション制御は、ハブアンドスポークと任意の WAN トポロジの両方で使用できます。このコール アドミッション制御の形式には、リソース予約プロトコル（RSVP）をサポートする WAN インフラストラクチャの部分が必要です。詳細については、「リソース予約プロトコル（RSVP）」（P.3-47）および「コール アドミッション制御」（P.9-1）を参照してください。

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

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

音声とデータは、LAN で収束される場合とまったく同じように、WAN でも収束される必要があります。QoS プロビジョニングおよびキューイング メカニズムは、一般に、WAN 環境において音声とデータを同じ WAN リンク上で相互運用できることを保証するために使用されます。音声とデータを分離して別々のリンク上で転送すると、多くの場合において問題になることがあります。これは、1 つのリンクで障害が発生すると、一般に、すべてのトラフィックが単一リンクに集中するためです。その結

果、トラフィックの各タイプでスループットが減少し、ほとんどの場合において音声品質が低下します。さらに、ネットワーク リンクまたはデバイスを別々に保守すると、最善を尽くしても、トラブルシューティングや管理が困難になります。

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

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

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

最後に、International Telecommunication Union（ITU; 国際電気通信連合）の G.114 勧告には、音声ネットワークにおける片方向の遅延は 150 ミリ秒以下でなければならないと明記されています。ネットワーク内に低速 WAN リンクを実装する場合は、この要件に留意することが重要です。片方向の遅延がこの 150 ミリ秒の勧告を超えないように、WAN リンクのトポロジ、テクノロジー、および物理的な距離を考慮する必要があります。WAN を介したクラスタ化を使用する配置では、任意の 2 台の Unified CM 6.0 サーバ間の片方向の最大遅延は 20 msec、つまり 40 msec Round-Trip Time（RTT; ラウンドトリップ時間）以下でなければなりません。Cisco Unified CM Release 6.1 以降では、2 台の Unified CM サーバ間の片方向の最大遅延は最大 40 msec、つまり 80 msec RTT にすることができます（詳細については、「IP WAN を介したクラスタ化」（P.2-22）を参照してください）。

保証帯域幅

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

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

これらのリンク テクノロジーは、専用の方式で配置されているか、またはプライベート ネットワークに配置されている場合に、保証トラフィック スループットを提供できます。これらの WAN リンク テクノロジーはいずれも、特定の速度または帯域幅サイズでプロビジョニングできます。また、これらの

リンク テクノロジーには、低リンク速度でもネットワーク トラフィックのスループットを保証できる組み込みメカニズムがあります。トラフィック シェーピング、フラグメンテーションとパケット インターリーブ、および Committed Information Rate（CIR; 認定情報レート）などの機能を使用すると、WAN においてパケットがドロップされないこと、すべてのパケットが定期的に WAN リンクにアクセスできること、およびこれらのリンクを通過しようとするすべてのネットワーク トラフィックが十分な帯域幅を使用できることを保証できます。

Dynamic Multipoint VPN（DMVPN）

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

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

ベストエフォート型の帯域幅

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

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

- インターネット
- DSL
- ケーブル
- 衛星
- 無線

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

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

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

WAN の QoS

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

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

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

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

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

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

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

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

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

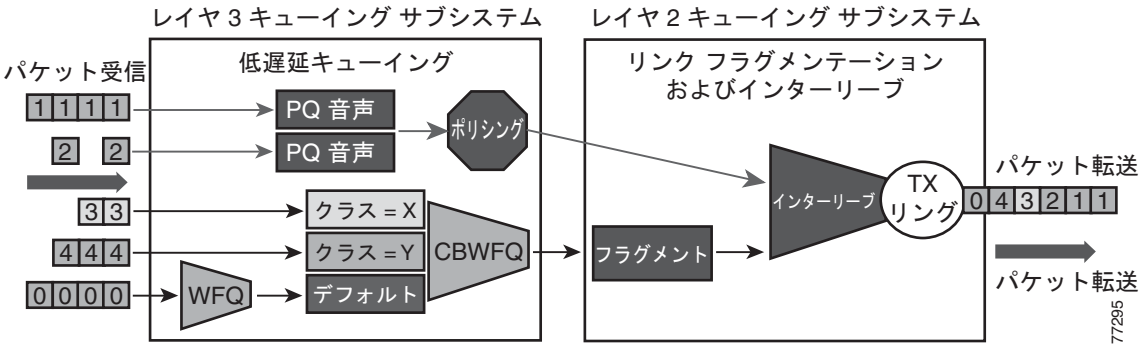
- 「トラフィックの優先順位」（P.3-41）
- 「リンク効率化手法」（P.3-43）
- 「トラフィック シェーピング」（P.3-44）

トラフィックの優先順位

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

図 3-11 は、優先付け体系の例を示しています。

図 3-11　WAN を介した VoIP 用の最適化キューイング



LLQ には、次の優先付けの基準を使用することをお勧めします。

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

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

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

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

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

リンク効率化手法

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

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

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

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

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

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

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

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

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

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

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

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

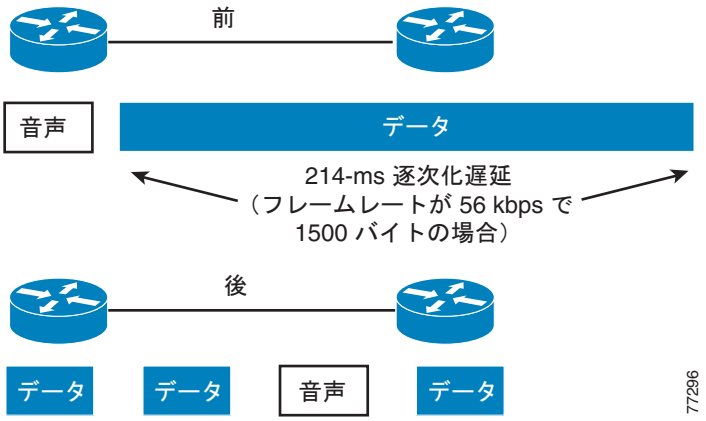
音声およびビデオに対応した IPSec VPN（V3PN）で cRTP を使用する場合の追加の推奨事項については、次の Web サイトで入手可能な V3PN 資料を参照してください。

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

LFI（Link Fragmentation and Interleaving）

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

図 3-12　LFI（Link Fragmentation and Interleaving）



Voice-Adaptive Fragmentation（VAF）

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

VAF は、一般に、Voice-Adaptive Traffic Shaping と組み合せて使用されます（「Voice-Adaptive Traffic Shaping（VATS）」（P.3-46）を参照）。VAF はオプションの LFI ツールです。VAF を有効にする場合は注意が必要です。これは、音声アクティビティが検出されるタイミングと LFI メカニズムが連動するタイミングの間に多少の遅延が生じるためです。また、最後の音声パケットが検出されてから、VAF が非アクティブになるまでの間に、設定可能な非アクティブ化タイマー（デフォルトは 30 秒）が期限切れになる必要があります。そのため、この期間は LFI が不必要に発生します。VAF は、Cisco IOS Release 12.2(15)T 以降で使用できます。

トラフィック シェーピング

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

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

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

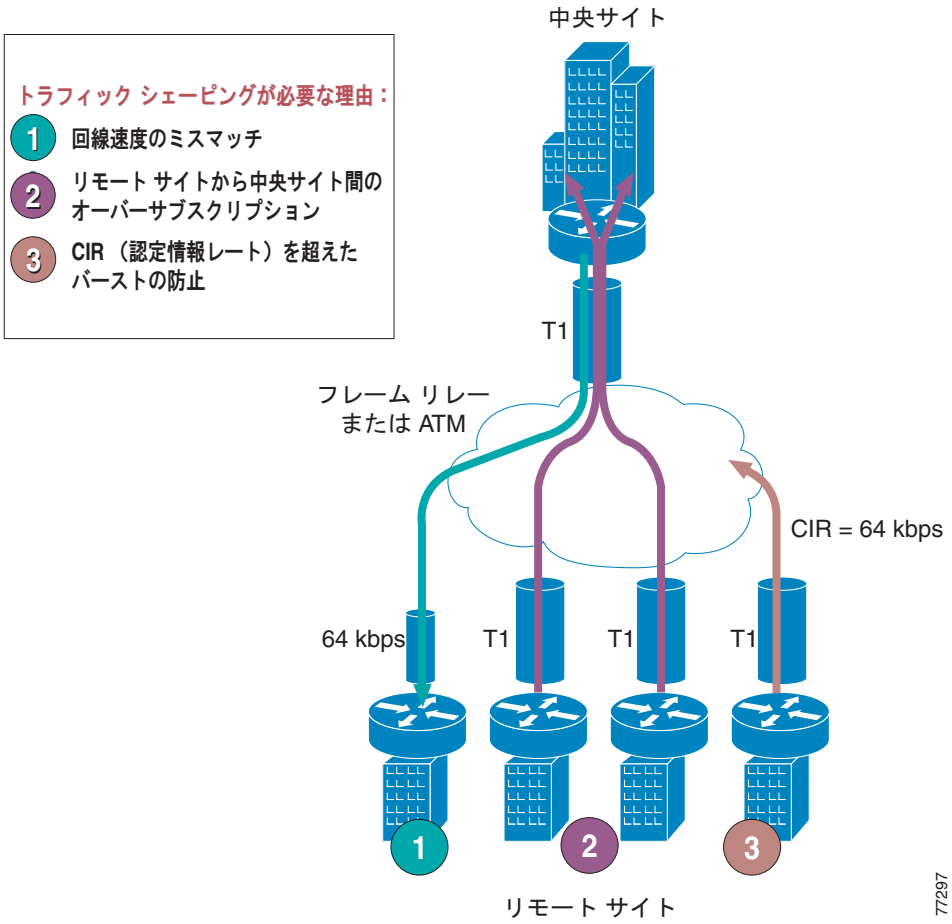


図 3-13 は、次の 3 つのシナリオを示しています。

1. 回線速度のミスマッチ

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

2. 中央サイトとリモート サイト間のリンクのオーバーサブスクリプション

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

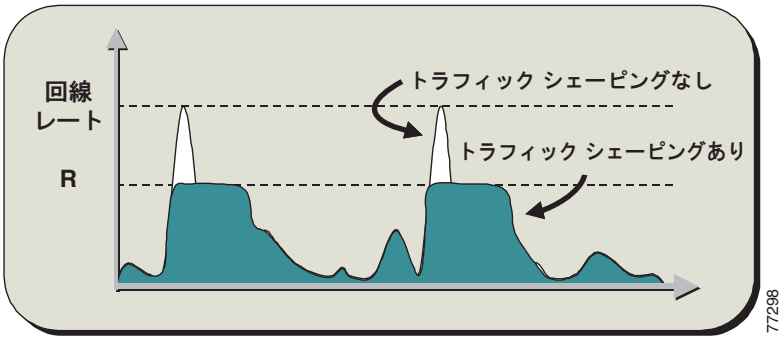
3. 認定情報レート（CIR）を超えたバースト

   もう 1 つの一般的な設定は、CIR を超えたトラフィック バーストを許可することです。CIR は、サービス プロバイダーが、損失なく、遅延の少ないネットワークを介して転送することを保証したレートです。たとえば、T1 インターフェイスを備えたリモート サイトでは、CIR が 64 Kbps に過ぎない場合があります。64 Kbps 超に相当するトラフィックが WAN を介して送信される場合、

プロバイダーは、追加トラフィックに「廃棄適性」のマークを付けます。プロバイダーのネットワークで輻輳が起きた場合、このトラフィックはトラフィック分類に関係なくドロップされるため、音声品質に悪影響を与える可能性があります。

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

図 3-14　トラフィック シェーピングのメカニズム



Voice-Adaptive Traffic Shaping（VATS）

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

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

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

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

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

リソース予約プロトコル（RSVP）

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

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

この項では、次のトピックを扱います。

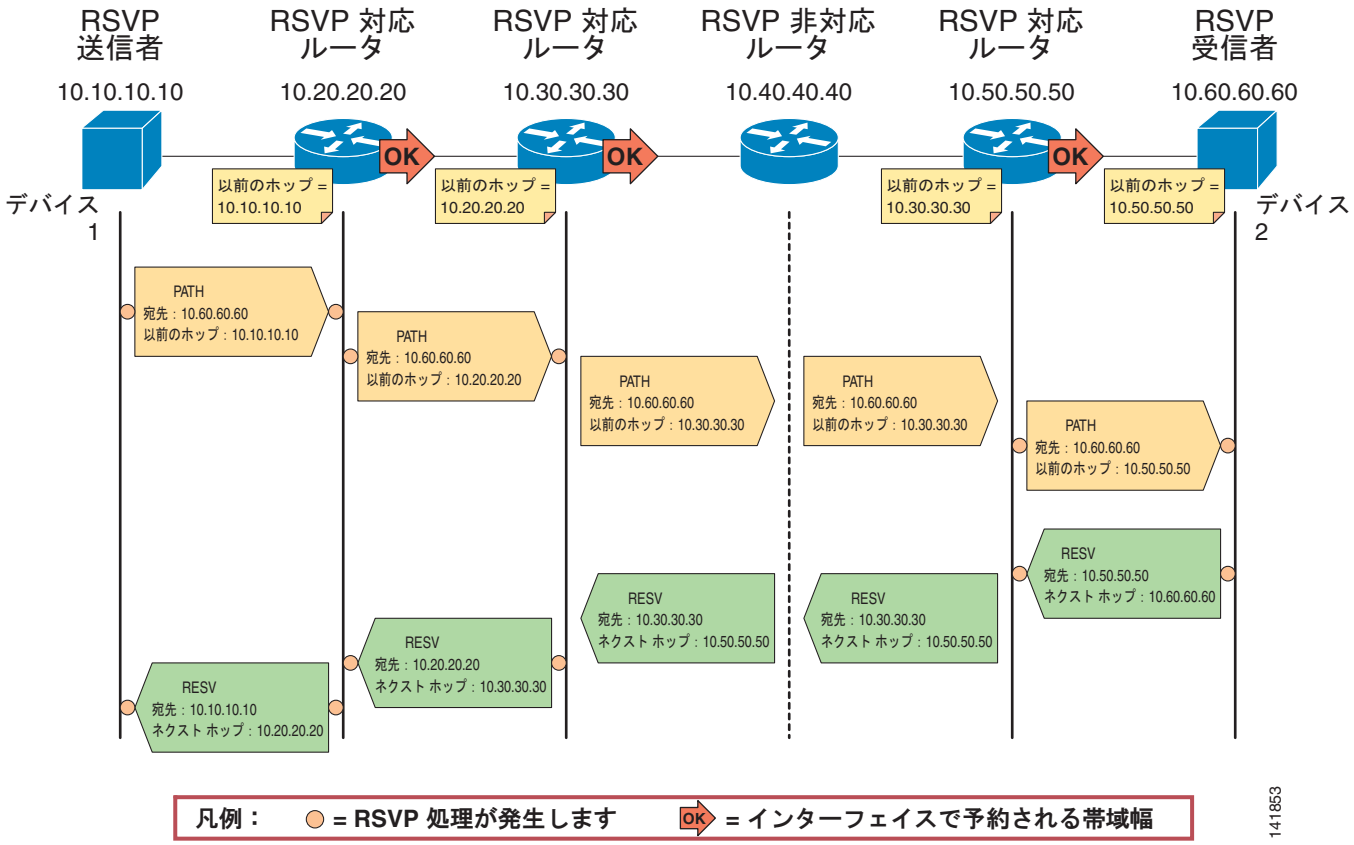
RSVP の原理

RSVP は、ネットワーク全体で、指定されたデータ フローのリソース予約を行います。RSVP 予約は単方向です。このため、2 つの RTP ストリームを含む単一の音声コールでは、各 RTP ストリームに 1 つずつの 2 つの RSVP 予約が生成されます。リソース予約は、データ フローの発信元デバイスと宛先デバイス間でシグナリング メッセージを交換することで作成され、メッセージはパスに沿って介在するルータにより処理されます。RSVP シグナリング メッセージは、IP ヘッダーのプロトコル番号が 46 に設定されている IP パケットで、既存のルーティング プロトコルに従ってネットワーク内でルーティングされます。

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

RSVP シグナリングの原理は、図 3-15 に示す例で説明できます。この図では、デバイス 1（IP アドレス 10.10.10.10）からデバイス 2（IP アドレス 10.60.60.60）に流れるデータ ストリーム用に、アプリケーションがネットワーク リソースを予約しようとします。

図 3-15　RSVP Path と Resv メッセージ フローの例



次の手順では、図 3-15 の例に示すように、単一データ フローとしての RSVP シグナリング プロセスについて説明します。

1. デバイス 1 にあるアプリケーションが Path という RSVP メッセージを発信します。このメッセージは、予約を要求するデータ フローと同じ宛先 IP アドレス（10.60.60.60）に送信され、IP ヘッダーの「router alert」オプションがオンにされて送信されます。Path メッセージには、特に次のオブジェクトが含まれています。
   - 「session」オブジェクト。宛先 IP アドレス、プロトコル番号、および UDP/TCP ポートで構成され、RSVP 対応ルータでデータ フローを識別するために使用します。
   - 「sender T-Spec」（トラフィック仕様）オブジェクト。予約が要求されたデータ フローの特性を示します。T-Spec は基本的に、特定のコーデックを使用するコール フローに必要な最大 IP 帯域幅を定義します。T-Spec は通常、データ フローの平均ビット レート、ピーク レート、およびバースト サイズの値を使用して定義されます。T-Spec については、この章の後半で詳しく説明します。
   - 「P Hop」（以前のホップ）オブジェクト。Path メッセージを最後に処理したルータ インターフェイスの IP アドレスが含まれます。この例では、P Hop は最初にデバイス 1 で 10.10.10.10 に設定されます。
2. 「router alert」オプションによって、Path メッセージは RSVP 対応ルータ（図 3-15 の 10.20.20.20）の CPU が代行受信し、RSVP プロセスに送信されます。RSVP は、このデータ フローのパス状態を作成し、Path メッセージに含まれる session オブジェクト、sender Tspec オブジェクト、および P Hop オブジェクトの値を格納します。次に、P Hop 値を発信インターフェイスの IP アドレス（この例では 10.20.20.20）で置き換えて、メッセージをダウンストリームに転送します。

3. 同様に、次の RSVP 対応ルータ（図 3-15 の 10.30.30.30）の CPU が Path メッセージを代行受信します。パス状態を作成し、P Hop 値を 10.30.30.30 に変更した後、このルータもメッセージをダウンストリームに転送します。
4. 次に、Path メッセージは、RSVP 非対応ルータ（図 3-15 の 10.40.40.40）に到達します。このルータでは RSVP が有効でないため、このメッセージは他の IP パケットと同様に、追加の処理やメッセージ オブジェクトの内容の変更は行われずに、既存のルーティング プロトコルに従ってルーティングされます。
5. その結果、Path メッセージは RSVP 対応ルータ（10.50.50.50）に転送され、ここでメッセージが処理され、対応するパス状態が作成され、メッセージがダウンストリームに転送されます。このルータで記録される P Hop には、ネットワーク パスの最後の RSVP 対応ルータの IP アドレス（この例では 10.30.30.30）がまだ含まれていることに注意してください。
6. デバイス 2 の RSVP 受信側は、P Hop 値が 10.50.50.50 の Path メッセージを受信します。ここで、Resv というメッセージを発信することによって、実際の予約が開始されます。このため、RSVP は受信側開始プロトコルと呼ばれます。Resv メッセージは、セッションのデータ フローの逆方向のパスに従って、予約要求を受信側から送信側にホップごとに伝達します。各ホップでの Resv メッセージの IP 宛先アドレスは、パス状態から取得した直前のホップ ノードの IP アドレスです。したがって、この例では、デバイス 2 は宛先 IP アドレスが 10.50.50.50 の Resv メッセージを送信します。Resv メッセージには、特に次のオブジェクトが含まれています。
   - 「session」オブジェクト。データ フローの識別に使用します。
   - 「N Hop」（次のホップ）オブジェクト。メッセージを生成したノードの IP アドレスが含まれます。この例では、N Hop は最初にデバイス 2 で 10.60.60.60 に設定されます。
7. 10.50.50.50 の RSVP 対応ルータがこのデータ フローの Resv メッセージを受信すると、受信した session オブジェクトを使用してパス状態情報と照合され、次の基準に基づいて予約要求を受け入れることができるかどうかが確認されます。
   - ポリシー制御：このユーザやアプリケーションが、この予約要求を行えるかどうか。
   - アドミッション制御：関連する発信インターフェイスに、この予約要求を満たせるだけの帯域幅リソースがあるかどうか。
8. この例では、10.50.50.50 でポリシー制御とアドミッション制御の両方が成功したとします。つまり、このセッションのパス状態の Tspec で提供される帯域幅は、発信インターフェイス（データ フローと同じ方向で、デバイス 1 からデバイス 2）で予約され、対応する「予約状態」が作成されるものとします。次に、10.50.50.50 のルータは、このセッションの P Hop に格納されている宛先 IP アドレス（10.30.30.30）にユニキャスト IP パケットとして送信することによって、Resv メッセージをアップストリームに送信できます。N Hop オブジェクトも、値 10.50.50.50 に更新されます。
9. 次に、Resv メッセージは、10.40.40.40 の RSVP 非対応ルータを通過します。ここでは、他の IP パケットと同様に、宛先 10.30.30.30 にルーティングされます。このメカニズムによって、RSVP シグナリングは、RSVP に対応していないノードが含まれる異種ネットワークで機能します。
10. 10.30.30.30 の RSVP 対応ルータは、Resv メッセージを受信し、ステップ 7 および 8 で説明したメカニズムに従って処理します。このホップでも、ポリシー制御およびアドミッション制御が成功したとします。帯域幅が発信インターフェイスで予約され、Resv メッセージが前のホップ（この例では 10.20.20.20）に送信されます。
11. 10.20.20.20 のルータで同様の処理が行われた後、Resv は最終的に RSVP 送信側のデバイス 1 に到達します。これによって、要求元のアプリケーションに対して、エンドツーエンド予約が確立され、ネットワークのすべての RSVP 対応ルータで、帯域幅がこのデータ フロー用に確保されたことが示されます。

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

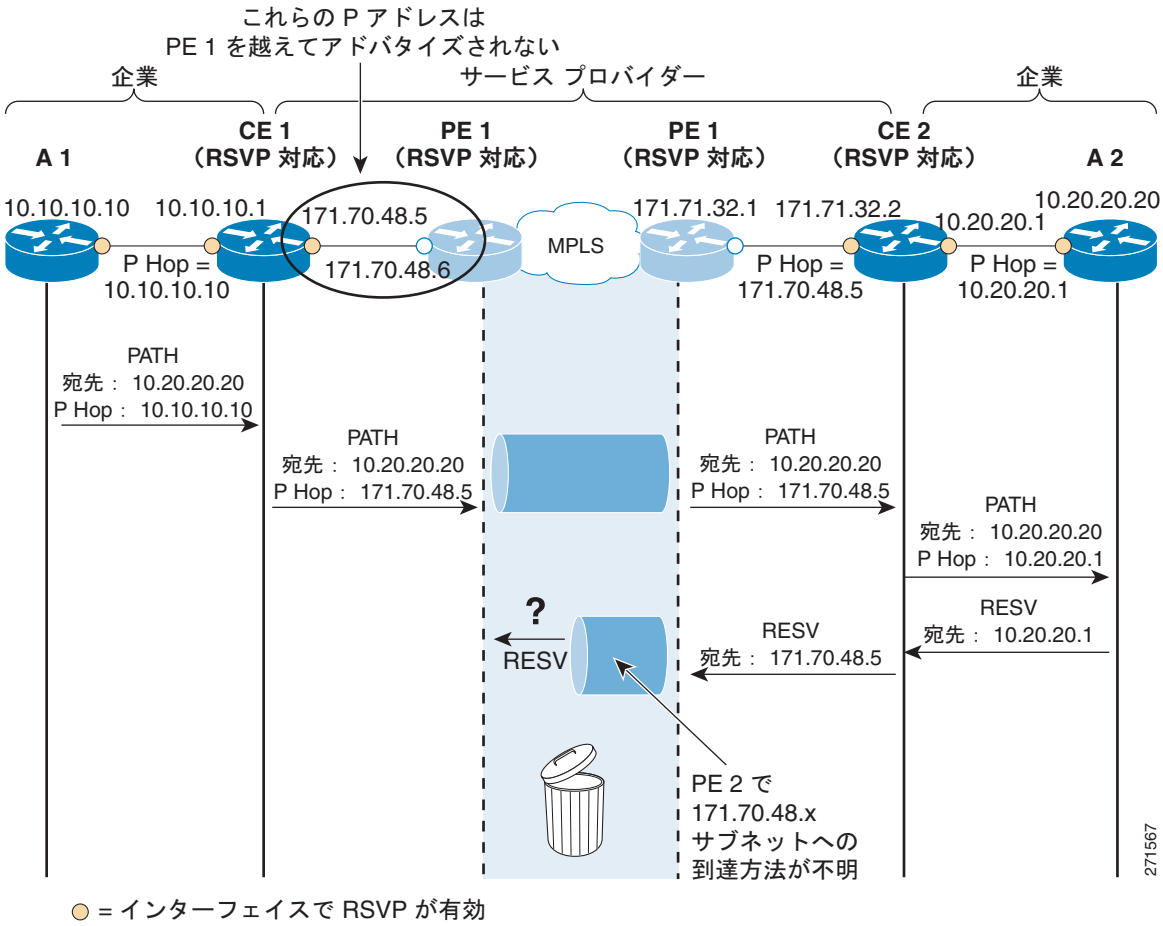
たことを示すために使用されます。たとえば、図 3-15 のノード 10.50.50.50 でアドミッション制御が失敗した場合、このノードは失敗の原因を示す ResvErr メッセージをデバイス 2 に送信して、アプリケーションがこの通知を受け取ります。

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

MPLS ネットワークにおける RSVP

一部の MPLS サービス プロバイダー ネットワークでは、カスタマー エッジ（CE）とプロバイダー エッジ（PE）間のリンクで使用する IP アドレスは、その他の MPLS ネットワークには配布されません。そのため、サブネットは PE にローカルにとどまり、PE を越えてアドバタイズされることはありません（これらが一意ではなく、他の場所でも再利用されるためです）。これにより、RSVP メッセージの P Hop（以前のホップ）値がネットワーク内で不明であるため、RSVP が RSVP メッセージを転送できない状況が発生します。図 3-16 は、このタイプの状況を示しています。

図 3-16　P Hop 上書きしない MPLS 上での RSVP



○ = インターフェイスで RSVP が有効

図 3-16 は、企業ネットワークとサービス プロバイダーの MPLS ネットワークを示しています。CE1 と CE2 は RSVP 対応、PE1 と PE2 は RSVP 非対応です。RSVP Path メッセージには P Hop オブジェクトが含まれています。このオブジェクトは、すべての RSVP ホップで書き直されます。これは、CE1 が以前の RSVP ホップ（または P Hop）であることを示すために、RSVP ルータ（たとえば、CE1）が Path メッセージを、次の RSVP ルータ（たとえば、CE2）に送信できるようにするためです。この情報は、対応する Resv メッセージをホップバイホップでアップストリームの送信側に転送するために CE2 によって使用されます。

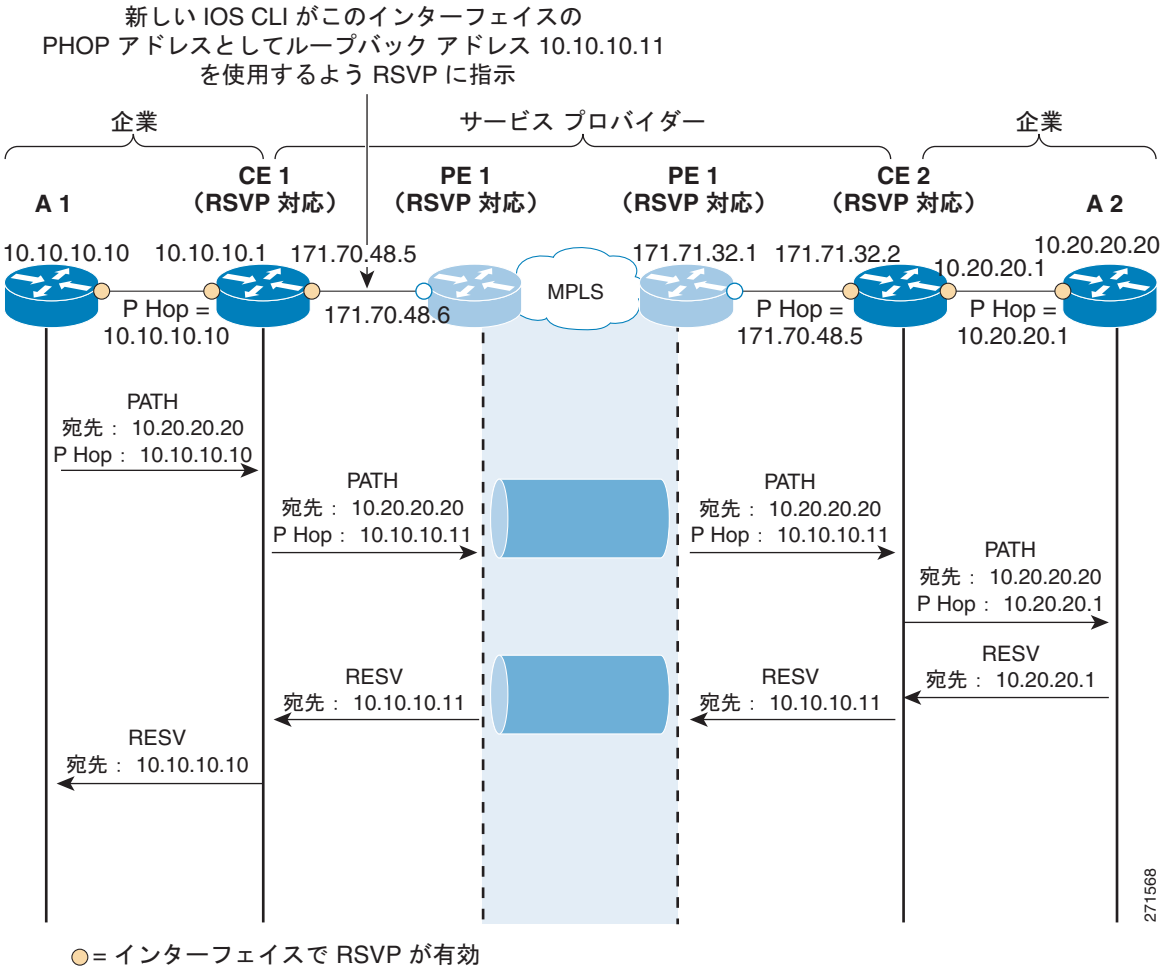
Cisco IOS では、RSVP ルータは、常に P Hop アドレスを Path メッセージを送信する出力インターフェイスの IP アドレスに設定します。一部の CE1 の IP アドレスが到達可能であるにもかかわらず、その出力インターフェイスの IP アドレスが、リモートの RSVP ルータ CE2 から到達できない場合があります。その結果、CE2 によって生成された対応する Resv メッセージが CE1 に到達しないため、予約が確立されなくなります。

コールが A1 から A2 に発信されると、A1 は RSVP セッションをセットアップしようとして、Path メッセージを CE1 に送信することで開始します。A1 は、発信インターフェイスの IP アドレス（この場合、10.10.10.10）の Path メッセージ内の P Hop オブジェクトを取り込みます。次に、CE1 は、Path メッセージを受信し、それを処理し、対応するパス状態を作成し、その出力インターフェイスの IP アドレス（171.70.48.5）を持つメッセージの P Hop フィールドを更新します。このアドレスは、ルーティング可能な IP アドレスではないため、Path メッセージをダウンストリームに転送します。この Path メッセージは、サービス プロバイダーのネットワークを通り抜け、CE2 によって処理されます。Path メッセージを受信した後、CE2 は、P Hop オブジェクトの IP アドレス（CE1 の出力インターフェイスの IP アドレス）を記録し、Path メッセージをダウンストリームの A1 に転送します。A1 は、Path

メッセージを記録および処理して、RSVP メッセージを CE2 に発信します。CE2 は、RSVP メッセージを処理し、それ自身の RSVP メッセージをアップストリームの CE1 に送信します。ただし、CE2 がこの Resv メッセージに対して応答する場合、CE2 は CE1 から受信した Path メッセージから以前に記録した IP アドレスに送信しようとします。この IP アドレス（171.70.48.5）は CE2 からルーティングできないので、Resv メッセージは失敗し、この結果予約試行は失敗します。

この動作を解決するために、Previous Hop Overwrite（以前のホップの上書き）と呼ばれる機能が Cisco IOS Release 12.4(20)T に導入されています。P Hop の上書きは、カスタマーの VPN で到達可能なルータ上の他のインターフェイスからの IP アドレスを含む Path メッセージ内の Hop オブジェクトを CE が取り込むメカニズムです。この方法で、Resv メッセージは送信側に戻る経路を見つけ、予約を確立することができます。P Hop の上書きメカニズムは、図 3-17 に示されています。

図 3-17　Cisco IOS 12.4(20)T における RSVP P Hop の上書き機能



RSVP（TSpec）におけるデータ フロー特性の説明

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

RSVP セッションのデータ フローの帯域幅の要件は、Path メッセージに含まれる TSpec（トラフィック仕様）の送信側によって特性が設定され、Resv メッセージの受信側によって送信される RSpec（予約仕様）にミラーリングされます。TSpec は、ネットワークを経由して、すべての中間ルータと宛先エンドポイントに転送されます。中間ルータはこのオブジェクトを変更せず、オブジェクトは最終受信者へ無変更のまま送信されます。

TSpec オブジェクトには、次の要素が含まれています。

- AverageBitRate（kbps）
- BurstSize（バイト）
- PeakRate（バイト）

オーディオ TSpec

オーディオ フローでは、TSpec の計算が次の測定値を指定します。

- AverageBitRate（kbps）：IP オーバーヘッドを含む
- BurstSize（バイト）：この値は、バースト内のパケットのサイズにパケット数を掛けて算出されます。オーディオ フローでは、バーストは通常 1 ～ 2 を指定します。
- PeakRate（バイト）：ピーク レート（バイト単位）は、エンドポイントが任意の時間に送信する最大バイト/秒を指します。オーディオ ストリームの場合と同様に、バーストが小さい場合、ピークレートは tokenRate の 1.1（または 1.2）倍として計算できます。

コールが応答されたときに、帯域幅予約を上方に調整するのを回避するために、Cisco Unified CM は、各リージョン コーデックに対する最大帯域幅をコール セットアップ時間で予約します。次に、Unified CM は、コールが応答されたときに、接続された当事者のメディア能力に基づく帯域幅を変更または調整します。

Unified Communications 対応 RSVP の詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager System Guide*』を参照してください。

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

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

WAN ルータでの RSVP と QoS

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

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

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

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

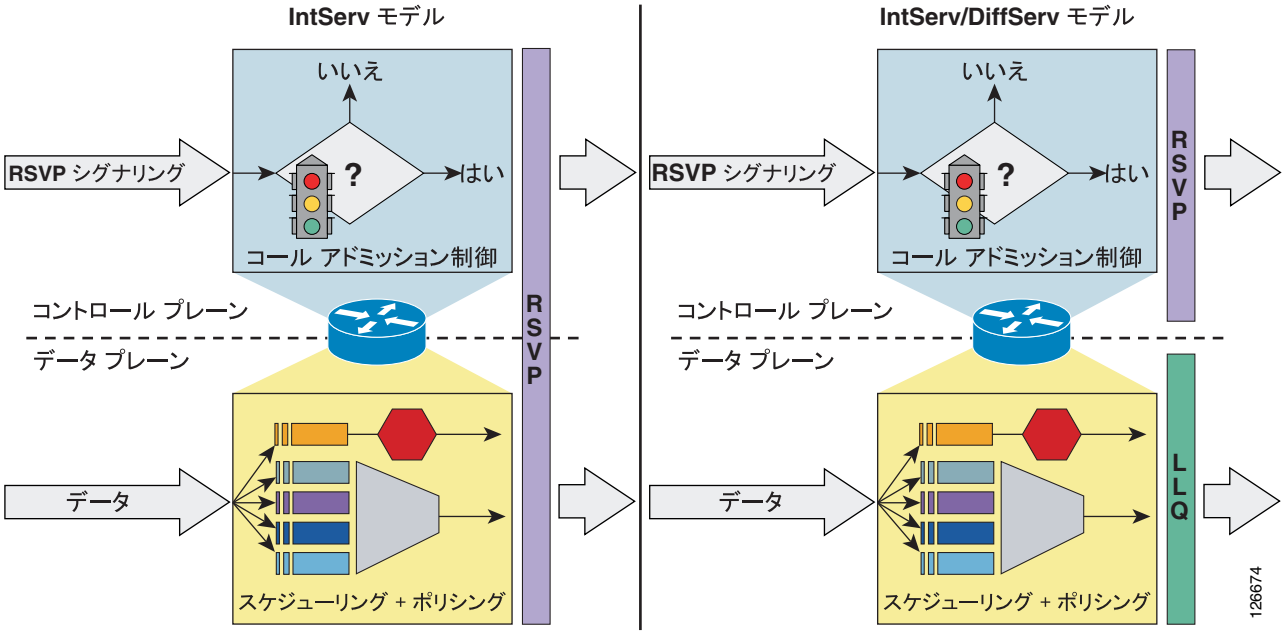
（注）　ルータ インターフェイスで RSVP を有効にすると、そのルータで RSVP に対応していないその他のすべてのインターフェイスが、RSVP メッセージをドロップします。RSVP メッセージのドロップを防ぐには、RSVP シグナリングが通過すると予想されるすべてのインターフェイスで RSVP を有効にします。インターフェイスでコール アドミッション制御を使用しない場合は、帯域幅の値をインターフェイス帯域幅の 75% に設定します。

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

http://www.ietf.org

図 3-18 に、Cisco IOS ルータから見た、これらの 2 つのアプローチの相違点を示します。

図 3-18　2 つの RSVP 運用モデル：IntServ と IntServ/DiffServ

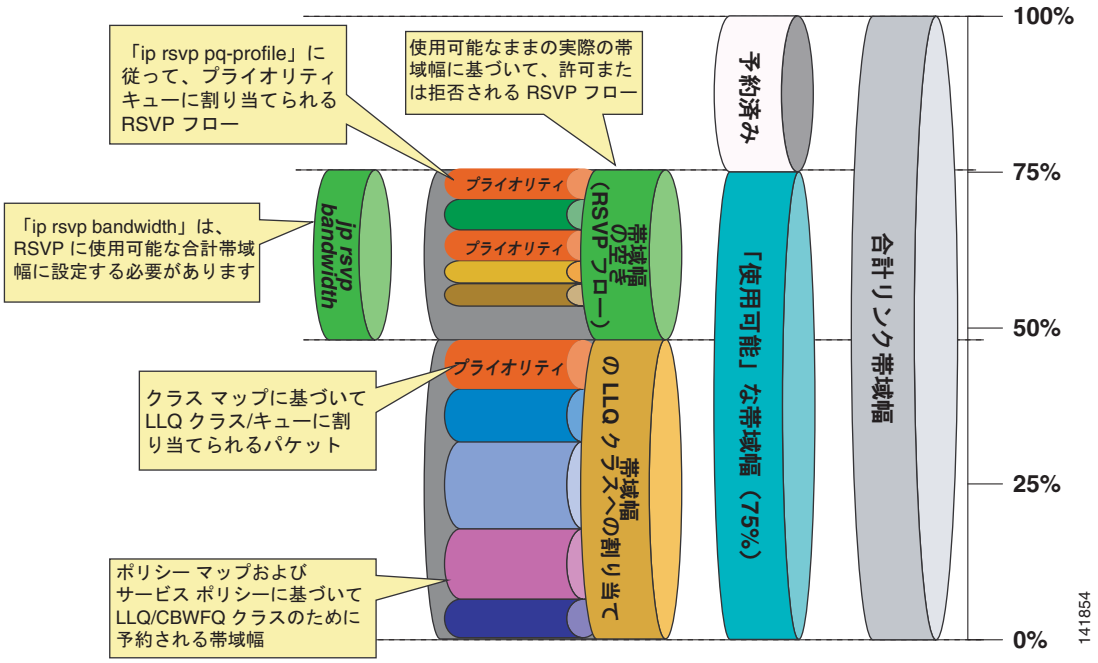


IntServ モデル

図 3-18 の左側に示すように、IntServ モデルの RSVP には、コントロール プレーンとデータ プレーンの両方が関係します。コントロール プレーンでは、RSVP が予約要求を許可または拒否します。データ プレーンでは、データ パケットを分類し、RSVP メッセージに含まれているトラフィック記述に基づいてポリシングし、適切なキューに入れます。RSVP が実行する分類は、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート、およびプロトコル番号を構成している、5 つのタプルに基づいています。このモデルでは、ルータを通過するすべてのデータ パケットを RSVP で代行受信して、RSVP でこの 5 タプルを検査し、確立済みの予約と一致するかどうかを検索できるようにする必要があります。一致が見つかった場合は、その予約のトラフィック仕様に従って、パケットが RSVP によってスケジューリングされ、ポリシングされます。

図 3-19 で示すように、IntServ モデルを Low Latency Queuing（LLQ）と組み合せる場合、使用可能な帯域幅が RSVP と事前定義済みの LLQ キューで分割されます。RSVP は、RSVP 予約された帯域幅への入力基準を制御します。ポリシー マップは、事前定義済みキューの入力基準を制御します。

図 3-19　IntServ モデルと LLQ の組み合せ



Cisco IOS ルータで IntServ 運用モデルを使用するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

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

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

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

このモデルでは、各種キューへのパケットの割り当てを RSVP が制御します。このため、次の Cisco IOS コマンドをインターフェイス コンフィギュレーション モードで使用すると、データ フロー T-Spec 値に基づくプライオリティ キュー（PQ）にフローを配置するかどうかを RSVP に通知するメカニズムを定義できます。

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

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

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

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

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

IntServ/DiffServ モデル

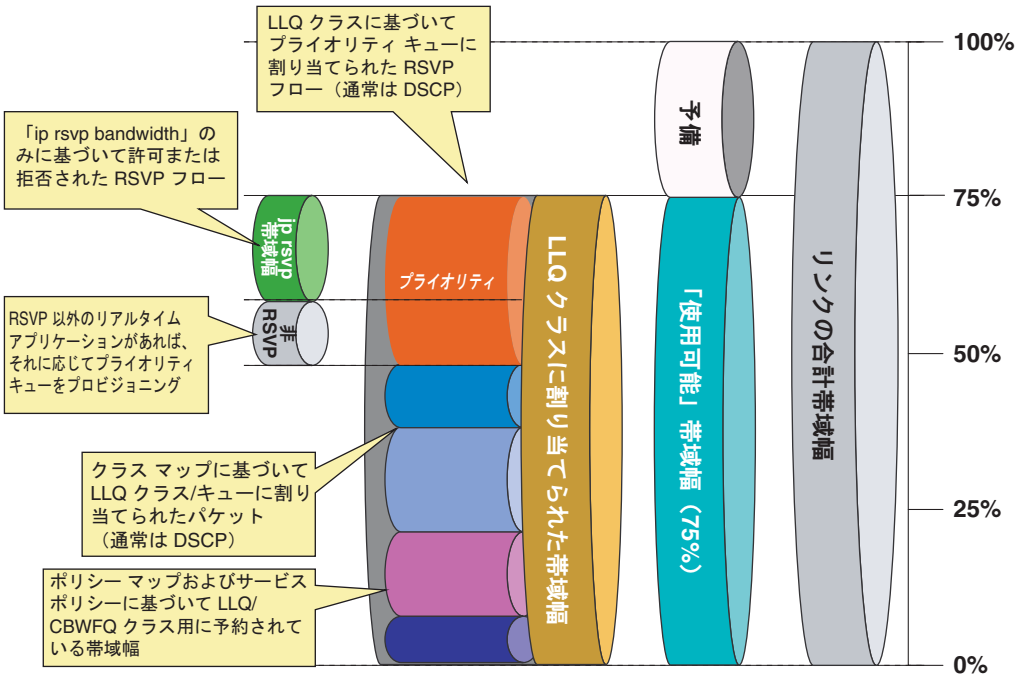
図 3-18 の右側に示すように、IntServ/DiffServ モデルの RSVP では、アドミッション制御を実行するコントロール プレーンだけが関係し、データ プレーンは関係しません。つまり、コール アドミッション制御機能は、スケジューリング機能およびポリシング機能とは独立しています。スケジューリングとポリシングは、事前定義済みのクラス マップ、ポリシー マップ、およびサービス ポリシーに従って、低遅延キュー（LLQ）アルゴリズムによって実行できます。

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

図 3-20 に示すように、使用可能な帯域幅全体（リンク速度の 75%）を LLQ クラスに割り当てることができます。これが現在、一般的に行われている割り当てです。ポリシー マップは、各キューに許可されるトラフィックを定義します。RSVP は通常、優先トラフィック用に定義されている帯域幅の量までのフローを許可するように設定されますが、このモデルでは、RSVP がスケジューリングを調整しないため、事前定義済みのプライオリティ キューを超えて RSVP で許可されるトラフィックがドロップされたり、より低い優先度のキューにマッピングし直されたりする可能性があることに注意してください。

優先トラフィックを送信するすべてのアプリケーションが RSVP 対応の場合は、RSVP 帯域幅がプライオリティ キューのサイズと一致するように設定できます。一方、図 3-20 に示すように、優先トラフィックを送信する必要がある RSVP 未使用アプリケーション（Unified CM スタティック ロケーション、ゲートキーパーなど）がある場合は、非 RSVP メカニズムで制御される優先トラフィックと RSVP で制御される優先トラフィックの間で、プライオリティ キューが分割されます。非 RSVP アドミッション制御と RSVP アドミッション制御のメカニズムを組み合せた場合は、プライオリティ キューでオーバーサブスクリプションが発生しないように、割り当てられた量を超える帯域幅を使用しないでください。

図 3-20　RSVP との LLQ 帯域幅割り当て



Cisco IOS ルータで IntServ/DiffServ 運用モデルを使用するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

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

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

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

RSVP のアプリケーション ID

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

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

app-id を使用しないと、RSVP でインターフェイスごとに設定できる帯域幅の値が 1 つだけになります。RSVP は、この帯域幅の上限に達するまで、要求を許可します。要求は区別されず、帯域幅が要求されているアプリケーション タイプも認識されません。その結果、RSVP が 1 つのタイプのアプリケーションだけに対応する要求を許可して、許可されている帯域幅を使い切ってしまい、帯域幅が使用できずに、後続のすべての要求を拒否する可能性があります。この場合、少数のビデオ コールが原因

で、すべてまたはほとんどの音声コールが許可されないことがあります。たとえば、1000 ユニットを RSVP に割り当てた場合に、RSVP が 2 つの 384 kbps ビデオ コールで帯域幅のほとんどを使い切ってしまい、音声コール用の帯域幅がほとんど残らない可能性があります。

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

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

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

次の例を参考にしてください。

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

Cisco Unified CM でのアプリケーション ID の使用方法

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

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

これらのサービス パラメータは変更可能ですが、デフォルト値のまま使用することをお勧めします。アプリケーション ID をデフォルト値のまま使用すると、同じリンク上で、複数のクラスタが予約を共有することができます。クラスタごとに異なるアプリケーション ID を使用すると、同じリンク上で、あるクラスタの予約と他のクラスタの予約を区別することができます。

音声コールにタグを付ける方法

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

ビデオ コールにタグを付ける方法

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

アプリケーション ID コール アドミッション制御モデル

「コール アドミッション制御」（P.9-1）の章で説明するように、アプリケーション ID でサポートされるコール アドミッション制御モデルは、「静的」ロケーションでサポートされるモデルとは異なります。ビデオ コールのオーディオ ストリームは、RSVP Audio Application ID でマークされるため、音

声コールの最小数を保証でき、音声およびビデオ コールのオーディオ ストリーム用に予約された、使用可能な帯域幅全体を占有することもできます。つまり、ビデオ コールは、Video Application ID（ビデオ ストリーム用）の設定済み帯域幅および Audio Application ID（音声コールおよびビデオ コールのオーディオ ストリーム用）の使用可能な設定済み帯域幅に基づいて、一定の最大帯域幅まで許可されます。先に確立されている音声コールで Audio Application ID 帯域幅全体が消費されている場合は、ビデオ コールは拒否されます。

RSVP 設計上のベスト プラクティス

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

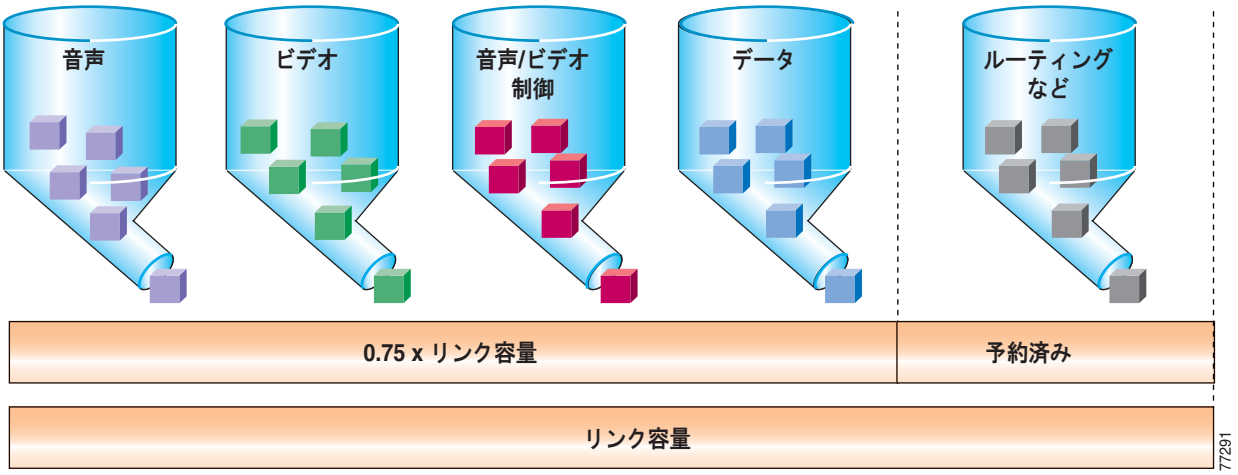
- 次のいずれかの条件に該当する場合は、IntServ/DiffServ モデルを採用することをお勧めします。
  - IP WAN インターフェイスのプライオリティ キュー（PQ）に入るトラフィックは、RSVP 対応トラフィックだけである。
  - PQ に入る RSVP 未使用トラフィックは、アウトオブバンドのコール アドミッション制御メカニズム（Unified CM ロケーションや Cisco IOS ゲートキーパーなど）によって、すべて確定的に一定量に制限される。
- プライオリティ キュー帯域幅のレイヤ 2 のオーバーヘッドを考慮すると、すべての PQ トラフィックが RSVP 対応の場合、**ip rsvp bandwidth** コマンドで指定した値と **priority** コマンドで指定した値は一致する必要があります。
- ルータの 1 つ以上のインターフェイスで RSVP を有効にする場合は、RSVP メッセージがドロップされないように、RSVP シグナリングが通過すると考えられるすべてのインターフェイスでも RSVP を有効にする必要があります。インターフェイスでコール アドミッション制御を使用しない場合は、帯域幅の値をインターフェイス帯域幅の 75% に設定します。
- 一部の PQ トラフィックが RSVP 非対応の場合は、**ip rsvp bandwidth** コマンドとアウトオブバンド コール アドミッション制御メカニズムで指定した値の合計が、**priority** コマンドで指定した帯域幅値を超えないようにする必要があります。
- ビデオ コールで使用する最大帯域幅を制限する必要がある場合は、RSVP アプリケーション ID のサポートを有効にします。アプリケーション ID のサポートは、Cisco IOS Release 12.4(6)T で導入されました。詳細については、「RSVP のアプリケーション ID」（P.3-57）を参照してください。
- WAN リンクの両側のルータの WAN インターフェイスなど、ネットワークの両端で RSVP を有効にします。
- 速度が異なる冗長リンクなど、可能性があるすべての WAN 輻輳ポイントで RSVP を有効にします。
- ロードバランスされた MPLS WAN リンクでは、対称ルーティングを確保します。
- MLPPP、ATM-IMA、および FRF.16 を含むバンドル インターフェイスでは、現在、RSVP を使用できません。
- トンネル インターフェイスでは、現在、RSVP を使用できません。
- ほとんどの Catalyst スイッチング プラットフォームでは、現在、RSVP を使用できません。

帯域幅のプロビジョニング

成功する IP ネットワークを設計する主要部分は、ネットワーク帯域幅の適切なプロビジョニングです。主要なアプリケーション（たとえば、音声、映像、およびデータ）ごとの帯域幅必要量を加算すると、必要な帯域幅を計算できます。この合計値は、任意のリンクの最小帯域幅必要量を表します。この値は、そのリンクに使用可能な合計帯域幅の約 75% 以下でなければなりません。この 75% ルールは、

ルーティングやレイヤ 2 キープアライブなどのオーバーヘッド トラフィックに、いくらかの帯域幅が必要であることを前提としています。図 3-21 は、こうした帯域幅のプロビジョニング プロセスを示しています。

図 3-21　リンクの帯域幅プロビジョニング



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

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

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

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

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

- すべてのマルチサイト WAN 配置における音声およびビデオ ベアラ トラフィック（「ベアラ トラフィック用のプロビジョニング」（P.3-61）を参照）
- 集中型コール処理を使用するマルチサイト WAN 配置における呼制御トラフィック（「集中型コール処理を使用した呼制御トラフィック用のプロビジョニング」（P.3-68）を参照）
- 分散型コール処理を使用するマルチサイト WAN 配置における呼制御トラフィック（「分散型コール処理を使用した呼制御トラフィック用のプロビジョニング」（P.3-72）を参照）

ベアラ トラフィック用のプロビジョニング

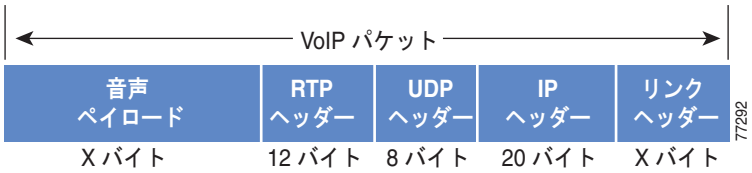
この項では、次のトラフィック タイプの帯域幅プロビジョニングについて説明します。

- 「音声ベアラ トラフィック」（P.3-61）
- 「ビデオ ベアラ トラフィック」（P.3-64）

音声ベアラ トラフィック

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

図 3-22　　一般的な VoIP パケット



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

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

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

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

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

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

表 3-9　音声ペイロードと IP ヘッダーだけの帯域幅使用量

コーデック	サンプリング レート	音声ペイロード（バイト数）	1 秒あたりのパケット数	1 会話あたりの帯域幅
G.711 および G.722-64k	20 ms	160	50.0	80.0 kbps
G.711 および G.722-64k（SRTP）	20 ms	164	50.0	81.6 kbps
G.711 および G.722-64k	30 ms	240	33.3	74.7 kbps
G.711 および G.722-64k（SRTP）	30 ms	244	33.3	75.8 kbps
iLBC	20 ms	38	50.0	31.2 kbps
iLBC（SRTP）	20 ms	42	50.0	32.8 kbps
iLBC	30 ms	50	33.3	24.0 kbps
iLBC（SRTP）	30 ms	54	33.3	25.1 kbps
G.729A	20 ms	20	50.0	24.0 kbps
G.729A（SRTP）	20 ms	24	50.0	25.6 kbps
G.729A	30 ms	30	33.3	18.7 kbps
G.729A（SRTP）	30 ms	34	33.3	19.8 kbps

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

表 3-10　レイヤ 2 ヘッダーが含まれた帯域幅使用量

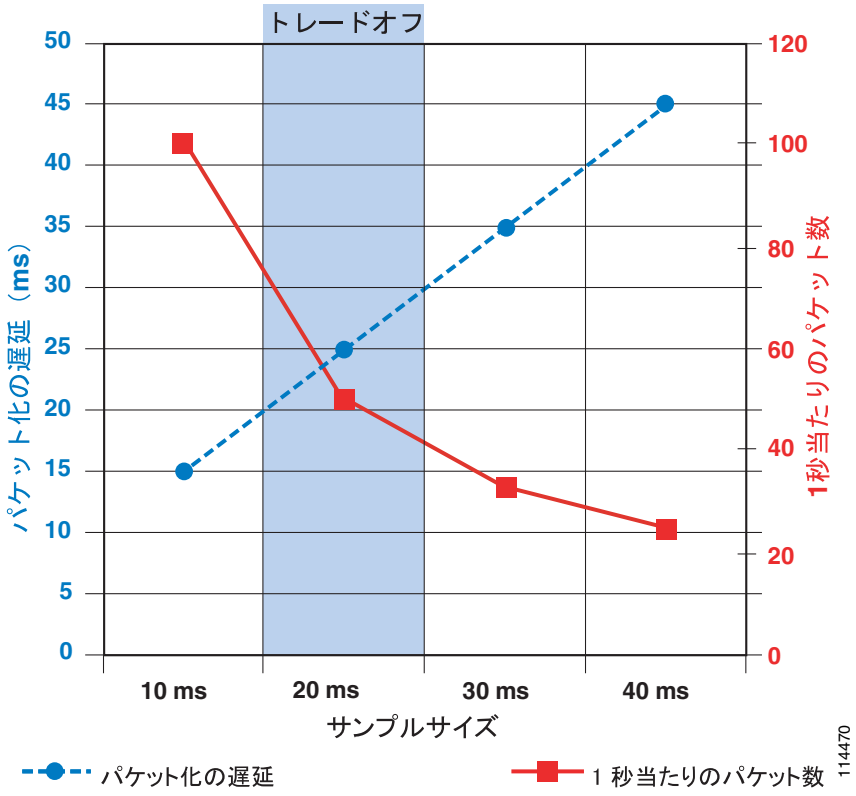
	ヘッダー タイプとサイズ						
コーデック	イーサネット 14 バイト	PPP 6 バイト	ATM 53 バイトのセルと 48 バイトのペイロード	フレーム リレー 4 バイト	MLPPP 10 バイト	MPLS 4 バイト	WLAN 24 バイト
G.711 および G.722-64k（50.0 pps）	85.6 kbps	82.4 kbps	106.0 kbps	81.6 kbps	84.0 kbps	81.6 kbps	89.6 kbps
G.711 および G.722-64k（SRTP）（50.0 pps）	87.2 kbps	84.0 kbps	106.0 kbps	83.2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

表 3-10　レイヤ 2 ヘッダーが含まれた帯域幅使用量 （続き）

コーデック	ヘッダー タイプとサイズ						
	イーサネット 14 バイト	PPP 6 バイト	ATM 53 バイトのセルと 48 バイトのペイロード	フレーム リレー 4 バイト	MLPPP 10 バイト	MPLS 4 バイト	WLAN 24 バイト
G.729A （50.0 pps）	29.6 kbps	26.4 kbps	42.4 kbps	25.6 kbps	28.0 kbps	25.6 kbps	33.6 kbps
G.729A （SRTP） （50.0 pps）	31.2 kbps	28.0 kbps	42.4 kbps	27.2 kbps	29.6 kbps	27.2 kbps	35.2 kbps
G.729A （33.3 pps）	22.4 kbps	20.3 kbps	28.3 kbps	19.7 kbps	21.3 kbps	19.8 kbps	25.1 kbps
G729A （SRTP） （33.3 pps）	23.5 kbps	21.4 kbps	28.3 kbps	20.8 kbps	22.4 kbps	20.8 kbps	26.2 kbps

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

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



ビデオ ベアラ トラフィック

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

ビデオの正確なオーバーヘッド率を計算できないという問題を解決するために、パケットが通過するレイヤ 2 メディアのタイプにかかわらず、コール速度に 20% を加算することをお勧めします。追加の 20% は、イーサネット、ATM、フレーム リレー、PPP、HDLC、およびその他の転送プロトコル間の差を吸収するための余裕となり、ビデオ トラフィックのバースト性に対するクッションにもなります（表 3-11 を参照）。

表 3-11　さまざまなビデオ コールの速度に対する推奨帯域幅

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

表 3-11 の値はコールの最大バースト速度を表し、クッションとして追加分が含まれていることに注意してください。コールの平均速度は、通常、この値を大幅に下回ります。メディア チャネルと帯域幅の使用に関する概念は、コール アドミッション制御の設定に使用する値を理解するために重要です。

Unified CM で使用する RSVP 帯域幅の値の計算

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

- Preferred G722 millisecond packet size：デフォルトは 20 ms
- Preferred G711 millisecond packet size：デフォルトは 20 ms
- Preferred G729 millisecond packet size：デフォルトは 20 ms

ただし、コーデックのサンプリング レートはコールごとにネゴシエートされ、1 つ以上のエンドポイントでサポートされないために、優先設定が使用されないことがあります。呼び出し後の失敗の原因となる、能力が完全に交換された後で予約サイズが増加することを防ぐには、この初期予約をコーデックの最悪のケース（最小パケット サイズを使用した最大コーデック ビット レート）に対応したものにします。エンドポイント間でメディア能力が交換されると、予約は正しい帯域幅割り当てに修正されます。ほとんどの場合、デフォルトのサンプリング レートが使用され、結果として予約が削減されます。

（注）　Unified CM は、RSVP 予約に SRTP オーバーヘッドまたはレイヤ 2 オーバーヘッドを含めません。RSVP T Spec 帯域幅の値と比較する場合、レイヤ 3 IP RSVP 帯域幅のステートメントは、任意の SRTP トラフィックを考慮する必要があり、SRTP トラフィックが存在する場合は、レイヤ 2 プライオリティ キューの値も余分にプロビジョニングする必要があります（表 3-10 および表 3-11 を参照）。

音声ベアラ トラフィック

音声コーデックが G729 に設定されているリージョン間コール。G.729 を使用して接続：

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

音声コーデックが G.728/iLBC の最大値に設定されているリージョン間コール。iLBC を使用して接続：

- 初期要求：48 kbps。最悪ケースのシナリオの 10 ms の G.728 を使用。
- 更新後の要求：31.2 kbps。優先サンプル サイズの 20 ms を持つ iLBC 使用。

音声コーデックが G711 に設定されているリージョン間コール。G.711 を使用して接続：

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

ビデオ ベアラ トラフィック

オーディオ ストリームと同様に、ビデオ ストリームの初期予約も、予約の時点でエンドポイントのコーデック能力が完全にはネゴシエートされていないため、リージョン設定に依存します。ビデオ コールのリージョン設定には、オーディオ ストリームの帯域幅が含まれます（詳細については、「IP ビデオ テレフォニー」（P.16-1）を参照してください）。オーディオ ストリームには独自の予約があるため、最終的なビデオ ストリームの予約は、リージョン設定から音声コーデックのビットレートを減算した値になります。ただし、これらのコーデックは完全にはネゴシエートされていないため、ビデオ ストリーム予約は、オーディオ ストリームがないという前提で、最悪のケースのシナリオで行われます。エンドポイント間でメディア能力が交換されると、予約は正しい帯域幅割り当てに修正されます。

ビデオは本質的にバースト性が高いため、ストリーム要件にオーバーヘッドを追加する必要があります（詳細については、「ビデオ ベアラ トラフィック」（P.3-64）を参照してください）。Unified CM は、次のように、ストリーム帯域幅を使用してオーバーヘッドの計算方法を決定します。

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

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

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

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

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

設定の推奨事項

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

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

次の例を参考にしてください。

- 4 つの G.729 ストリームをプロビジョニングする場合

  (3 × 24) + 40 = 112 kbps
- 4 つの G.711 ストリームをプロビジョニングする場合

  (3 × 80) + 96 = 336 kbps
- 4 つの 384 kbps ビデオ ストリーム（G.729 オーディオ）をプロビジョニングする場合

  (3 × (384 - 8) + 384) × 1.07 = 1618 kbps
- 4 つの 384 kbps ビデオ ストリーム（G.711 オーディオ）をプロビジョニングする場合

  (3 × (384 - 64) + 384) × 1.07 = 1438 kbps

アプリケーション ID をサポートする Cisco IOS 設定

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

プライオリティ キューの組み合せ

Unified CM によるアプリケーション ID サポートの実装で許可される機能（プライオリティ キューで使用可能なすべての帯域幅を音声コールで消費可能にする機能）を利用するために、音声とビデオのプライオリティ キューを分離するという以前の推奨事項を変更する必要があります（「アプリケーション ID コール アドミッション制御モデル」（P.3-58）を参照してください）。この機能を使用するには、音声とビデオの両方の一致基準を 1 つのクラスマップに組み合せる必要があります。音声トラフィックまたはビデオ トラフィックのいずれかが一致することが要件になるため、次のように、クラスマップの一致基準 **match-all** の代わりに **match-any** を使用する必要があります。

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

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

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

アプリケーション ID から RSVP ポリシー ID へのマッピング

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

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

- *Access and Communication Servers Command Reference*

  http://www.cisco.com/en/US/docs/ios/11_0/access/command/reference/arbook.html

- *Using Regular Expressions in BGP*
  http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094a92.shtml
- *Regex Engine Performance Enhancement*
  http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_rexpe.html

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

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

インターフェイスの RSVP ローカル ポリシー

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

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

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

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

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

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

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

例

次の例は、「Cisco Unified CM でのアプリケーション ID の使用方法」（P.3-58）で説明したモデルを使用する音声コールとビデオ コールの両方をサポートします。音声コールには 352 kbps の帯域幅が保証され、ビデオ コールは 154 kbps の帯域幅に制限されます。音声コールは、使用可能な RSVP 帯域幅のすべてを使用できます。

```
interface Serial0/0/1:0
 ip address 10.2.101.5 255.255.255.252
 service-policy output Voice-Policy
 ip rsvp bandwidth 506
 ip rsvp data-packet classification none
 ip rsvp resource-provider none
 ip rsvp policy local identity rsvp-voice
  maximum bandwidth group 506
  forward all
 ip rsvp policy local identity rsvp-video
```

```
 maximum bandwidth group 154
 forward all
ip rsvp policy local default
 no accept all ! Will not show in the configuration
 no forward all! Will not show in the configuration
```

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

集中型コール処理を使用した呼制御トラフィック用のプロビジョニング

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

この配置モデルには、次の考慮事項が適用されます。

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

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

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

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

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

（注）　この平均数が、特定の配置のニーズを満たさない場合、「拡張公式」（P.3-70）に記載されている拡張公式を使用して、推奨帯域幅を計算できます。

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

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

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

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

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

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

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

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

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

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

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

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

Cisco IOS ルータ上のキューに割り当てることができる最小帯域幅が 8 Kbps であるという事実を考慮すると、支店のさまざまな規模に対する最小帯域幅と推奨帯域幅の値を、表 3-12 のようにまとめることができます。

表 3-12　呼制御トラフィック用の推奨レイヤ 3 帯域幅（シグナリングの暗号化の有無別）

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

（注）　表 3-12 では、電話機あたりの毎時平均コール数を 10 と想定し、RSVP 制御トラフィックを含みません。この表の値に追加する RSVP 関連の帯域幅を判断するには、「RSVP を使用するコールに関する考慮事項」（P.3-71）を参照してください。

（注）　サイト間コールに RSVP ベースのロケーション ポリシーを使用する場合は、表 3-12 の値を増やし、Cisco RSVP Agent の制御トラフィックの分を補正する必要があります。たとえば、コールの 10% が WAN を経由する場合、表 3-12 の値に 1.1 を掛けます。

拡張公式

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

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

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

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

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

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

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

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

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

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

RSVP を使用するコールに関する考慮事項

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

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

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

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

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

シェアドライン アピアランスに関する考慮事項

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

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

  CHS = CHL ×（ライン アピアランス数）/（回線数）

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

  回線数 = 5

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

  CHL = 6

  CHS = 6 × (11 / 5) = 13.2

- 呼び出す各電話機が個別のシグナリング制御ストリームを必要とするため、Unified CM から同じ支店に送信されるパケット量は、呼び出す電話機の数に比例して増加します。Unified CM は 100 Mbps インターフェイスでネットワークに接続されるため、大量のパケットをすぐに生成でき

ますが、キューイング メカニズムがシグナリング トラフィックを処理するまで、このパケットはバッファに入れる必要があります。処理速度は、通常、100 Mbps よりも 2 桁小さい WAN インターフェイスの実効情報転送速度によって制限されます。

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

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

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

たとえば、SCCP と、同じ回線を共有する 6 台の電話機を使用する場合、トラフィックのシグナリング クラス用のキュー項目数は 78 以上に調整する必要があります。表 3-13 は、支店サイトでのシェアドライン アピアランスの量に基づいた推奨されるキュー項目数を示しています。

表 3-13　支店サイトごとの推奨されるキュー項目数

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

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

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

分散型コール処理を使用した呼制御トラフィック用のプロビジョニング

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

この配置モデルには、次の考慮事項が適用されます。

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

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

WAN を通過する制御トラフィックは、次のカテゴリのいずれかに属します。

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

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

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

公式 6：仮想タイ ライン数に基づく推奨帯域幅

推奨帯域幅（bps）= 116 ×（仮想タイ ライン数）

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

無線 LAN インフラストラクチャ

統合されたネットワークの無線 LAN（WLAN）部分に IP テレフォニーを追加する場合は、無線 LAN インフラストラクチャの設計が重要になります。Cisco Unified Wireless IP Phone 7920、7921G、および 7925G などの無線 IP テレフォニー エンドポイントが追加されている場合、音声トラフィックは WLAN 上に移動しているため、そこで既存のデータ トラフィックと合流します。有線 LAN および有線 WAN インフラストラクチャの場合と同様、WLAN に音声を追加するには、基本的な設定と設計に関するベスト プラクティスに従って、可用性の高いネットワークを配置する必要があります。また、WLAN インフラストラクチャを適切に設計するには、ネットワーク全体でエンドツーエンドの音声品質を保証するために、QoS を理解して無線ネットワーク上に配置する必要もあります。次の項では、これらの要件について説明します。

- 「WLAN の設計と設定」（P.3-74）
- 「WLAN の QoS」（P.3-80）

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

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

WLAN の設計と設定

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

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

- 「無線インフラストラクチャに関する考慮事項」（P.3-74）
- 「無線 AP の設定と設計」（P.3-77）
- 「無線セキュリティ」（P.3-78）

無線インフラストラクチャに関する考慮事項

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

- 「VLAN」（P.3-74）
- 「ローミング」（P.3-74）
- 「無線チャネル」（P.3-75）
- 「無線の干渉」（P.3-76）
- 「WLAN 上のマルチキャスト」（P.3-76）

VLAN

有線 LAN インフラストラクチャの場合と同様、無線 LAN に音声を配置する場合は、アクセス レイヤにある 2 つ以上の VLAN を有効にする必要があります。無線 LAN 環境のアクセス レイヤには、アクセス ポイント（AP）と最初のホップのアクセス スイッチが含まれます。AP とアクセス スイッチ上では、データ トラフィック用のネイティブ VLAN と、音声トラフィック用の Voice VLAN（Cisco IOS の場合）または Auxiliary VLAN（CatOS の場合）を設定する必要があります。この Voice / Auxiliary VLAN は、ネットワークにある他のすべての有線 Voice VLAN とは分離される必要があります。また、有線 LAN 上の音声エンドポイントの場合と同様、無線音声エンドポイントは、RFC 1918 プライベート サブネット アドレスを使用してアドレス指定される必要があります。無線インフラストラクチャを配置する場合は、WLAN AP の管理用に独立した管理 VLAN を設定することもお勧めします。この管理 VLAN には WLAN アピアランスを設定しないでください。つまり、関連付けられた Service Set Identifier（SSID）を設定することも、WLAN から直接アクセスできるように設定することもしないでください。

ローミング

デバイスがレイヤ 3 で移動する場合、デバイスはネイティブ VLAN の境界を越えて AP から別の AP に移動します。WLAN ネットワーク インフラストラクチャが自律分散型 AP で構成されている場合、Cisco Catalyst 6500 シリーズ Wireless Services Module（WiSM）によって、Cisco Unified Wireless IP Phone は、IP アドレスを保持し、アクティブ コールを維持しながらレイヤ 3 でローミングできます。シームレスなレイヤ 3 ローミングが行われるのは、クライアントが同じモビリティ グループ内でローミングする場合だけです。Cisco WiSM およびレイヤ 3 ローミングの詳細については、次の Web サイトで入手可能な Cisco WiSM 製品資料を参照してください。

http://www.cisco.com

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

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

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

無線チャネル

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

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

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

一部のチャネルでは、レーダー（軍事、衛星、および気象）による干渉を防止するために、802.11a 帯域が DFS（Dynamic Frequency Selection; 動的周波数選択）および TPC（Transmit Power Control; 伝送パワー コントロール）をサポートする必要があることに注意してください。規制により、チャネル 52 ～ 64、100 ～ 116、および 132 ～ 140 が DFS および TPC をサポートする必要があります。TPC は、これらのチャネル上の伝送が干渉を引き起こすほど強力にならないように制御します。DFC は、チェネルのレーダー パルスを監視し、レーダー パルスを検出した場合、DFC はチャネル上の伝送を停止して、新しいチャネルに切り替えます。

AP カバレッジは、同じチャネルで設定された AP 間でオーバーラップが発生しない（または最小になる）ように、配置する必要があります。同じチャネルのオーバーラップは、通常、19 dBm の間隔で発生します。ただし、オーバーラップのないチャネルで適切な AP 配置およびカバレッジを行うには、最

低限 20% のオーバーラップが必要です。このオーバーラップ量であれば、無線エンドポイントが AP カバレッジ セルの間を移動するときにローミングが円滑に行われることが保証されます。オーバーラップが 20% 未満の場合、ローミングに時間がかかり、音質が悪くなることがあります。

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

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

無線の干渉

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

考えられる干渉源には、次のものがあります。

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

Bluetooth 対応デバイスは、802.11 b および g デバイスと同じ 2.4 GHz 無線帯域を使用するので、Bluetooth および 802.11 b または g デバイスが相互に干渉し、その結果接続に関する問題が起きる可能性があります。Bluetooth デバイスは 802.11 b および g WLAN 音声デバイスと干渉，妨害を引き起こす潜在的な可能性があるので（その結果，音声品質の低下，登録解除，およびコールセットアップ遅延を引き起こす）、可能な場合には、すべての WLAN 音声デバイスを、5 GHz 無線帯域を使用する 802.11a に配置することをお勧めします。無線電話機を 802.11a 無線帯域に配置することで、Bluetooth デバイスによって引き起こされる干渉を回避できます。

WLAN 上のマルチキャスト

設計上、マルチキャストはユニキャストの確認応答レベルを備えていません。802.11 仕様に従って、アクセス ポイントは、次の Delivery Traffic Indicator Message（DTIM）周期に到達するまで、すべてのマルチキャスト パケットをバッファに入れる必要があります。DTIM 周期はビーコン周期の倍数です。ビーコン周期が 100 ms（通常のデフォルト）で DTIM 値が 2 の場合、アクセス ポイントは、バッ

ファに入れられた単一のマルチキャスト パケットを転送する前に、最大 200 ms 待機する必要があります。ビーコン間の周期（DTIM 設定の積としての）は、バッテリ電源式デバイスによって、一時的に省電力モードに移行するために使用されます。この省電力モードは、デバイスがバッテリ電源を節約するのに役立ちます。

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

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

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

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

無線 AP の設定と設計

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

AP の選択

無線音声を配置する場合は、次の AP を選択することをお勧めします。

- Aironet 500 シリーズ Express AP
- Aironet 1100、1130、および 1140 シリーズ AP
- Aironet 1230、1240、および 1250 シリーズ AP
- Aironet 1300 シリーズ AP
- Aironet 1510 および 1520 シリーズ AP

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

AP の配置

音声配置用に Cisco アクセス ポイント（AP）を使用するときは、いかなる場合も、15 ～ 25 を超えるデバイスを、単一の 802.11b または 802.11b/g AP に関連付けないことをお勧めします。802.11a または 802.11a/g AP では、45 ～ 50 を超えるデバイスを、単一の AP に関連付けないことをお勧めします。これらの数は、使用プロファイルおよび使用可能なデータ レートによって異なります。AP 上のデバイスの数は、各デバイスがメディアにアクセスできる期間に影響します。デバイスの数が増加すると、トラフィックの競合も増加します。上記に指定された数を越えるデバイスを関連付けると、AP のパフォーマンスが低下し、関連付けられたデバイスの応答時間が遅くなる可能性があります。

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

AP の設定

無線音声を配置する場合は、特定の AP 設定に関する次の要件に従います。

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

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

- AP 上のダイナミック伝送パワー コントロール（DTPC）を有効にする

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

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

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

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

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

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

  音声ポリシーとデータ ポリシーに各 VLAN のデフォルトの分類を設定することで、音声トラフィックがプライオリティ キューイング処理されることを保証します（詳細については、「インターフェイス キューイング」（P.3-81）を参照してください）。

無線セキュリティ

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

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

  無線クライアントと、Protected Access Credential（PAC）を使用する認証、認可、アカウンティング（AAA）サーバとの間で認証トンネルの確立を最初に要求する標準ベースのセキュリティ プロトコルです。次に、無線エンドポイントはユーザ名とパスワードを使用して、トンネルを介して認証を行い、802.1X 経由でネットワークとの認証を行います。この認証が行われると、無線デバイスとの間のトラフィックは TKIP または WEP で暗号化されます。802.1X 認証方式を使用するに

は、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、無線デバイスを認証するためのユーザ データベースにアクセスします。

- Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）

  この方法では、クライアントと公開キー インフラストラクチャ（PKI）を持つ TLS プロトコルを使用する認証サーバ間でセキュア認証トンネルが確立されると、Cisco Unified Wireless IP Phone をユーザ名とパスワードで AP に対し 802.1x で認証できます。認証時、無線デバイスとの間のトラフィックは TKIP または WEP を使用して暗号化されます。TLS は、ユーザおよびサーバ認証とダイナミック セッション キーの生成の両方で証明書を使用する機能を提供します。認証に使用される証明書は、製造元でインストールされる証明書（MIC）、またはユーザによりインストールされる証明書のいずれかになります。

- Protected Extensible Authentication Protocol（PEAP）

  この方法では、クライアントと認証サーバとの間で暗号化された SSL/TLS トンネルを通して、ユーザ名とパスワードにより、Cisco Unified Wireless IP Phone は AP に対して 802.1x で認証できます。暗号化された SSL/TLS トンネルはサーバ側の公開キー証明書を使用して作成され、Microsoft's Challenge Handshake Authentication Protocol（MS-CHAP）のバージョン 2 を使用した認証情報の交換の暗号化、およびユーザ クレデンシャルの盗難防止を確実にします。認証時、無線デバイスとの間のトラフィックは TKIP または WEP を使用して暗号化されます。

- Wi-Fi Protected Access（WPA）

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

- Wi-Fi Protected Access 2（WPA2）

  これは、WPA の 802.11i 拡張版です。これは、ネットワークに対して認証するためのユーザ名とパスワードを無線エンドポイントに要求する、標準ベースのセキュリティ プロトコルです。802.1X または事前共有キー（WPA2-PSK）を使用してこの認証が発生すると、無線デバイスとの間のトラフィックは Advanced Encryption Standards（AES）で暗号化されます。802.1X 認証方式を使用するには、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、無線デバイスを認証するためのユーザ データベースにアクセスします。

- Cisco LEAP

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

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

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

認証と ACS 配置モデル

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

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

- 集中型 ACS

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

- リモート ACS

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

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

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

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

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

WLAN の QoS

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

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

無線 QoS には、次の主要な設定領域があります。

- 「トラフィック分類」（P.3-81）
- 「インターフェイス キューイング」（P.3-81）
- 「帯域幅のプロビジョニング」（P.3-82）

トラフィック分類

有線ネットワーク インフラストラクチャの場合と同様、できるだけネットワークのエッジの近くで適切な無線トラフィックを分類またはマークすることが重要です。トラフィック マーキングは、有線および無線ネットワーク全体でキューイング方式の入力基準となるため、マーキングはできるだけ無線エンドポイントで行われる必要があります。無線ネットワーク デバイスによるマーキングまたは分類は、有線ネットワーク デバイスの場合（表 3-6 を参照）と同じである必要があります。

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

インターフェイス キューイング

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

アップストリーム キューイングでは、Wi-Fi Multimedia（WMM）をサポートするデバイスは、プライオリティ キューイングなどのキューイング メカニズムを利用できます。ただし、WMM をサポートしないデバイスは、このキューイング メカニズムを利用できません。Cisco Wireless IP Phone 7921G および 7925G は WMM をサポートしています。Cisco Wireless IP Phone 7920 は、WMM をサポートしていませんが、パケットがデバイスを通過するときにアップストリームのキューイングを行えます。ただし、無線ネットワークは共有メディアであるため、無線 LAN 上のすべてのクライアントでキューイングを行うようにするメカニズムは用意されていません。

ダウンストリーム QoS に関しては、Cisco AP は現在、無線クライアントに送信されているダウンストリーム トラフィックに対して最大 8 つのキューを割り当てることができます。これらのキューへの入力基準は、DSCP、Access Control List（ACL; アクセス コントロール リスト）、および VLAN などの要素の数に基づいて設定できます。8 つのキューが使用可能ですが、無線音声を配置する場合は 2 つのキューだけを使用することをお勧めします。音声メディアとシグナリング トラフィックはすべて、最

高レベルのプライオリティ キューに入り、他のトラフィックはすべて、ベストエフォート型キューに入る必要があります。これにより、音声トラフィックが最適にキューイング処理されることが保証されます。

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

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

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

帯域幅のプロビジョニング

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

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

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

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

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

- QoS Basic Service Set（QBSS）

  QBSS はビーコン情報要素であり、この情報要素により、AP は無線 IP 電話機にチャネル利用率情報を送信します この QBSS 値は、無線電話機が他の AP にローミングするかどうかを判別するのに役立ちます。QBSS 値が低いと、その AP がローミング先として適切な候補であることを示し、QBSS 値が高いと、デバイスがその AP にローミングするべきでないことを示しています。この QBSS 情報は便利ですが、コールが適切な QoS を保持することを保障するものではなく、またコールを処理するのに十分な帯域幅が存在することを保証するものではないため、真のコール アドミッション制御メカニズムではありません。Cisco Unified Wireless IP Phone が、高い QBSS を持つ AP に関連付けられている場合、AP は、コールのセットアップを拒否し、発信側のデバイス

に Network Busy メッセージを送信することにより、コールが開始または受信されるのを防止します。しかし、無線 IP Phone と別のエンドポイントの間でコールがセットアップされた後は、電話機が、高い QBSS を持つ AP にローミングして関連付けを行うことができ、それによりその AP で使用可能な帯域幅のオーバーサブスクリプションが発生する場合があります。

- Wi-Fi Multimedia Traffic Specification（WMM TSPEC）

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

Cisco Unified Wireless IP Phone 7920 は、QBSS だけをサポートするので、これらのデバイスでのコール アドミッション制御のために使用できる唯一のメカニズムになります。ただし、Cisco Unified Wireless IP Phone 7921G および 7925G は、QBSS と TSPEC の両方をサポートしています（TSPEC は QBSS より優先されます）。したがって、Cisco Unified Wireless IP Phone 7921G または 7925G でのコール アドミッション制御は、TSPEC を使用する場合、より正確になり、AP のコール キャパシティを超過する可能性を排除できます。

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

QBSS 情報要素が AP から送信されるのは、AP 上で **QoS Element for Wireless Phones** が有効になっている場合だけです（「無線 AP の設定と設計」（P.3-77）を参照）。

CHAPTER 4

ゲートウェイ

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

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

この章の新規情報

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

表 4-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
ベアラ機能	「音声ゲートウェイのベアラ機能」（P.4-48）
Cisco 2900 および 3900 シリーズの Integrated Services Router（ISR; サービス統合型ルータ）	「ゲートウェイの選択」（P.4-8）
Cisco VGD-1T3、VG202、および VG204 ゲートウェイ	「ゲートウェイ プロトコル」（P.4-9） 「サイト固有のゲートウェイ要件」（P.4-18）
H.320 ビデオ チャネル ボンディング	「ISDN B チャネル バインディング、ロールオーバー、およびビジーアウト」（P.4-45）
TDM ゲートウェイ	「TDM ゲートウェイと VoIP トランキング ゲートウェイ」（P.4-7）

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

新規トピックまたは改訂されたトピック	説明箇所
ビデオ会議ゲートウェイ	「ビデオ テレフォニー用のゲートウェイ」（P.4-39）
音声のゲインと減衰の設定	「ゲートウェイ ゲイン設定の調整」（P.4-8）

トラフィック パターンとゲートウェイのサイジング

この項では、さまざまなトラフィック モデルまたはトラフィック パターンの違いと、それらが音声ゲートウェイの選定にどのように影響するかについて、詳しく説明します。ここでは、トラフィック集約型配置におけるトラフィック パターンとゲートウェイのサイジングに重点を置きます。

定義と用語

この項では、次の用語と定義を使用します。

- 同時コール

  システム内ですべてが同時にアクティブになるコールの数。

- 最大同時コール

  システムで処理可能な、アクティブ（通話）状態にある同時コールの最大数。1 日の*最煩雑時間*に同時にアクティブになると予測されるコールの数がこの数を超えないようにする必要があります。

- コール数/秒（cps）

  着呼率。1 秒間に着信したコールの数（つまり、新しいコール セットアップが試行されたコールの数）として定義されます。着呼率は多くの場合 1 時間あたりのコール数で計算されますが、このメトリックでは 1 時間の最後の 5 秒間に 100 件のコールが着信した場合でも平均着呼率は 100 コール/時間となり（これは通信システムとしては非常に低い数値です）、厳密とは言えません。この例を 1 秒間あたりの着呼率に換算すると、20 コール/秒という高い率になります。20 コール/秒の着呼率が 1 時間持続すると、1 時間あたりのコール数は 72,000 件になります。したがって、コール数/時間は、着信バースト トラフィック パターンを処理するシステムの能力を把握するという目的では有効なメトリックではありません。

- Busy Hour Call Attempts（BHCA; 最繁時呼数）

  1 日の最も煩雑する時間（ピーク時間）に試行されたコールの数。これは 1 日の最も煩雑する時間のコール数/秒と同じですが、1 秒間ではなく 1 時間で表します。たとえば、10 cps は 36,000 コール/時間と同じです。Busy Hour Call Completions（BHCC; 最繁時呼完了数）というメトリックもありますが、これは一部のコールが成功しなかった場合（ブロック要因が存在する場合など）、BHCA（試行されたコールの数）より低くなる可能性があります。この章では、呼完了率が 100% である（つまり、BHCA = BHCC）と仮定しています。

- バースト トラフィック

  安定した着呼は、ある期間にわたってコール試行の間隔がほぼ均等であることを意味します。たとえば、着呼率が安定しているときには、60 コール/時間はほぼ 1 分間に 1 回コール試行があることを示します（約 0.02 cps）。着呼が集中すると、ある一定の期間（1 時間など）に到着するコールの間隔が均等でなくなり、短時間にコールが集中して 1 ～数回のスパイクが生じます。最悪のケースでは、着呼率が同じ 60 コール/時間であっても、1 時間のうちの 1 秒間にすべてのコールが集中し

ます。この場合は、その 1 時間中のほぼすべての時間の着呼率は平均 0 cps になり、1 秒間だけが 60 cps と突出します。この種のトラフィックをバースト トラフィックといい、通信システムに非常に大きな負担をかけます。

- 保持時間

  音声コールの「通話時間」。つまり、コールのセットアップから終了までの間の、2 者間に通話路が開いている時間を示します。音声システムのトラフィック エンジニアリングで使用する保持時間の業界平均値は 3 分（180 秒）です。平均コールの保持時間が短くなるほど、コールのセットアップと終了に費やされるシステム CPU 時間の割合が、通話路の維持に費やされる CPU 時間に比べて高くなります。

公衆網トラフィック パターン

音声通信システムの文脈で使用される「トラフィック」は、送受信されるコールの量を指します。特に重要となるのは、公衆網などの外部回線によって伝送されるトラフィックです。トラフィックはアーランで測定され、1 アーランは「1 つのコールが 1 時間持続すること」と定義されています。この項では、アーランについては詳しく説明しません。単に、特定のトラフィック量に対して必要な回線の数を算出する際にアーラン B とアーラン C という数表を使用する、と述べるにとどめます。

必要な外部回線のサイズは、企業で受信および生成されるトラフィックの量によって決まります。ただし、お客様の多くは一般に、IP ベースの通信システムにおいても、それまで TDM ベースのシステムで使用していたのと同じ数の回線を使用し続けます。このサイジング方法は特に問題が発生しなければ有効ですが、その一方で継続的なシステム トラフィック分析プロセスを日常的なメンテナンス業務に組み込むことも重要です。トラフィック分析を行うと、現在のトラフィック レベルに対してシステムのプロビジョニングが過剰である（その結果、不要な回線にコストを費やしている）ことが判明したり、あるいは逆にプロビジョニングが不足していてコールのブロックや損失が起こる可能性のあることが指摘されたりします（この場合は回線数を増やすと状況が改善されます）。

一般業務のトラフィック プロファイル

ほとんどのお客様のトラフィック プロファイルは一般業務パターンです。これは、*煩雑時間*が通常 1 日 2 時間（午前 10:00 ～ 11:00 と午後 2:00 ～ 3:00）あることを意味します。これらの煩雑時間パターンは、多くの場合、1 日の業務の始まりや昼休み明けなどの要因に起因します。コールそのものは保持時間が長くなる傾向があり、安定的に着信、終了する傾向も見られます。トラフィック計算に使用する保持時間の一般的な業界平均値は、3 分です。

煩雑時間のトラフィックを考慮して通信システムを設計していれば、通常は問題は起こりません。それより低いレベルでシステムを設計していると、コールのブロックや損失が発生し、業務に悪影響をもたらすおそれがあります。

コンタクト センターのトラフィック プロファイル

コンタクト センターでは、通常ある一定数のオペレータまたは Interactive Voice Response（IVR; 自動音声応答）システムを利用して大量のコールを処理するという点で、少し異なるトラフィック パターンが見られます。コンタクト センターではリソースを最大限に活用する必要があるため、オペレータ、トランク、および IVR システムは業務時間中（通常は 1 日 24 時間）ずっと煩雑した状態が続きます。コール キューイングの使用が一般的で（着信コール トラフィックがオペレータの処理能力を超えると、次のオペレータが空くまでコールはキュー内で待機します）、オペレータは通常、自分の勤務時間の間、コンタクト センターに寄せられた電話の応対に専念します。

コンタクト センターでのコールの平均保持時間は、多くの場合、一般業務の電話よりも短くなります。コールの平均保持時間が短くなる理由は、IVR システムの段階で用件が済み、オペレータと通話しない場合が多いことによります（これを「セルフサービス コール」と呼ぶことがあります）。オペレータ

と通話した場合の平均保持時間は 3 分（一般業務トラフィックと同じ）であるのに対して、セルフサービス コールの典型的な保持時間は約 30 秒であることから、コンタクト センター全体での平均保持時間は一般業務トラフィックよりも短くなります。

リソース（IVR ポート、公衆網トランク、オペレータなど）の使用を最適化するというコンタクト センターの目標と、コンタクト センターが電話応対専門の組織であることを考え合せると、コンタクト センターのシステムでは通常の業務環境よりも着呼率は高くなります。これらの着呼率は、一般業務トラフィックとは異なる時間帯（通常の煩雑時間ではない時間帯）に異なる理由で最大になります。たとえば、特別な休日パックのテレビ CM を流して申し込み用のフリー ダイヤルを知らせた場合、その電話を受け付けるシステムの着呼率は、CM 放送後の約 15 分間にトラフィックのピークを迎えます。この着呼率は、コンタクト センターの平均着呼率を 1 桁上回ることもあります。

コンタクト センター トラフィックに対するゲートウェイのサイジング

短い通話時間とバースト性のある着呼率は、公衆網ゲートウェイのトラフィック処理能力に影響を与えます。このような状況では、通話時間の長いコールを一定期間にわたって均等に受けるような場合に比べて、すべてのコールをタイムリーに処理するためにゲートウェイでより多くのリソースが必要となります。ゲートウェイにはこのようなトラフィック パターンを処理するさまざまな機能が装備されているため、ゲートウェイを選定する際は使用する環境を考慮して入念に検討する必要があります。ゲートウェイの中には、サポートする T1/E1 ポートの数が多い機種や、同時に着信した複数コールの処理能力が高い機種などがあります。

複数のコールがほぼ同時に着信する（つまり、着呼率が高い、またはバースト性がある）トラフィック パターンでは、適切なコール数/秒（cps）性能を持つゲートウェイが最も適しています。このような状況で、コールの保持時間を 15 秒と仮定した場合、Cisco AS5400XM ユニバーサル ゲートウェイでは 20 cps（一度にアクティブにできるコール数は 310）、Cisco 3845 統合サービス ルータでは 17 cps（一度にアクティブにできるコール数は 255）、Cisco Catalyst 6500 コミュニケーション メディア モジュールでは 7 cps（一度にアクティブにできるコール数は 130）を維持できます。Cisco AS5350XM ユニバーサル ゲートウェイのパフォーマンスは、コール数/秒の観点では AS5400XM と同等です。

着呼率が安定したトラフィック パターンでは、通常、ゲートウェイが処理可能なアクティブ コールの最大数がより重要になります。このような状況で、コールの保持時間を 180 秒と仮定した場合、Cisco AS5400XM ユニバーサル ゲートウェイでは 630 の同時アクティブ コール（着呼率は最大 3.5 cps）、Cisco 3845 統合サービス ルータでは 504 の同時アクティブ コール（着呼率は最大 3 cps）、Cisco Catalyst 6500 コミュニケーション メディア モジュールでは 240 の同時アクティブ コール（着呼率は最大 1.3 cps）を維持できます。

これらの数値は、次の条件がすべて該当する場合を前提とします。

- CPU 使用率が 75% を超えない。
- 公衆網ゲートウェイ コールは、ISDN PRI トランクで H.323 を使用して行われる。
- Real Time Control Protocol（RTCP）タイマーがデフォルト値の 5 秒に設定されている。
- Voice Activity Detection（VAD; 音声アクティビティ検出）がオフになっている。
- G.711 のパケット化の周期は 20 ms である。
- Cisco IOS Release 12.4.11T 以降を使用している。
- 専用の音声ゲートウェイ設定を使用し、イーサネット（GE）出力を有効に、QoS 機能を無効にしている（QoS 対応の出力インターフェイスまたはイーサネット以外の出力インターフェイス、あるいはその両方を使用すると、CPU リソースの消費量が増えます）。

- 付加コール機能や付加サービス、たとえばセキュリティ全般（アクセス コントロール リストやファイアウォールなど）、音声固有のセキュリティ（TLS、IPSec、SRTP）、AAA ルックアップ、ゲートキーパーを介したコール セットアップ、VoiceXML または TCL 対応のコール フロー、コール アドミッション制御（RSVP）、SNMP ポーリング/ロギングなどを有効にしていない。このような追加のコール機能を有効にすると、CPU リソースの消費量が増えます。

音声アクティビティ検出（VAD）

VAD は、コールの特定の方向の通話路が無音と認識されている間、IP パケットがほとんど生成されないようにするデジタル信号処理機能です。通常は、ある時点で発話しているのは一方の通話者だけなので、パケットは一方向だけに流れればよく、逆方向（無音方向）では不定期のキープアライブを除き、パケットを送信する必要はありません。そのため、VAD を使用すると、VoIP コールで送信される IP パケットの数が大幅に減少し、それに伴ってゲートウェイ プラットフォームの CPU サイクルも大幅に低下します。VAD によってパケットが実際にどの程度減少するかは、コール フロー、アプリケーション、および会話の状況によって異なりますが、VAD 設定を無効にした場合と比べて、パケットが 10 ～ 30% 少なくなる傾向があります。

VAD は、エンドポイントや Unified CM ネットワークに配置された音声ゲートウェイではほとんどの場合無効にされており、その他の種類のネットワークに配置された音声ゲートウェイでは、ほとんどの場合、有効にされています。

コーデック

G.711 と G.729A のサンプリング時間はどちらもデフォルトで 20 ms に設定されているため、VoIP コールの一方向のパケット レートは 50 パケット/秒（pps）になります。G.711 の IP パケット（200 バイト）は G.729A のパケット（60 バイト）よりも大きいですが、この差が音声ゲートウェイの CPU パフォーマンスに大きな影響を与えるとは実証されていません。G.711 と G.729 のパケットはどちらもルータには「小さい」IP パケットと見なされます。そのため、パケット レートは CPU パフォーマンスに影響を与える重要なコーデック パラメータです。

パフォーマンスの過負荷

Cisco IOS は、割り込みレベルのイベントを処理するために、ピーク処理中にも CPU の使用率が 100% にならないように設計されています。この項に示すパフォーマンスの数値は、約 75% の平均的な負荷を実行しているプロセッサを基にしています。特定の Cisco IOS ゲートウェイの負荷がこのしきい値を継続的に超えると、次のようになります。

- Cisco Technical Assistance Center（TAC）でその配置がサポートされなくなります。
- Cisco IOS ゲートウェイで、Q.921 タイムアウト、ダイヤル後遅延の増大、インターフェイス フラップなどの異常な動作が起こります。

Cisco IOS ゲートウェイは短時間のコールのバーストであれば処理できるようになっていますが、推奨される着呼率（コール数/秒）が継続的に超過するような状況はサポートされていません。

（注） ゲートウェイに未使用のハードウェア ポートがある場合は、そのポートを他のタスクに割り当てたくなるものです（たとえば、CMM ゲートウェイで、トラフィック計算によって公衆網トラフィックに一部のポートしか使えないことがわかっている場合など）。しかし、残りのポートは*必ず*未使用のままにしておく必要があります。そうしないと、CPU がサポートされるレベルを超えて過負荷状態に陥ります。

パフォーマンスの調整

Cisco IOS 音声ゲートウェイの CPU 使用率は、シャーシで有効にされているすべてのプロセスの影響を受けます。最も低レベルのプロセスの一部（IP ルーティングやメモリのデフラグなど）は、シャーシにライブ トラフィックがないときにも実行されます。

CPU 使用率が下がると、リアルタイムの音声パケットやコール セットアップ命令の処理に十分な CPU リソースを使用できるようになり、Cisco IOS 音声ゲートウェイのパフォーマンスが向上します。CPU 使用率を削減する手法のいくつかを表 4-2 に示します。

表 4-2　CPU 使用率を削減する手法

手法	CPU 使用率の削減量	説明
VAD を有効にする	最大 20%	VAD を有効にすると、標準的な会話において音声パケットの量が最大 45% 減少します。問題は、音声認識を使用している場合や遅延が長い場合に音声品質が低下する可能性があることです。音声はトーク スパートの開始時に突然生じ、終了時に唐突に消失するように感じられます。
RTCP を無効にする	最大 5%	RTCP を無効にすると、発信側と着信側のゲートウェイ間で送信されるアウトオブバンド情報が減少します。その結果、相手側のゲートウェイに表示される統計情報の品質が低下します。また、コールがすでにアクティブでないかどうかを判断するために RTCP パケットが使用されている場合は、着信側ゲートウェイでコールの「未完結状態」が長くなる可能性があります。
その他の重要でない機能（Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）、ロギングなど）を無効にする	最大 2%	これらのプロセスは、必要でない場合は無効にできます。これらのプロセスを無効にすると、CPU がその分解放されて CPU 使用率が低下し、リアルタイム トラフィックの処理が高速になります。
コール パターンを変更してコールの長さを長くする（これにより、1 秒あたりのコール数を削減する）	可変	これはさまざまな手法で実現できます。たとえば、コールの最初に長い導入プロンプトを再生する（または既存の導入プロンプトを長くする）、コール スクリプトをコール センターで調整する、といった手法があります。

追加情報

Cisco 音声ゲートウェイの機能とコール センター トラフィックの分析の詳細については、次の資料を参照してください。

- *Cisco 音声ゲートウェイ ルータと Cisco Unified CallManager の相互運用性*に関するデータ シート（*表 7*）：

  http://www.cisco.com/en/US/prod/collateral/routers/ps259/product_data_sheet0900aecd8057f2e0.pdf

- *Cisco AS5400XM ユニバーサル ゲートウェイ*のデータ シート（*表 9*）：

  http://www.cisco.com/en/US/products/hw/univgate/ps505/products_data_sheet0900aecd802efc92.html

- *Cisco AS5400XM ユニバーサル ゲートウェイの発注方法*：
  http://www.cisco.com/en/US/products/hw/univgate/ps505/prod_brochure0900aecd802f6ece.html
- 音声トラフィックに関する計算手法（アーラン計算など）：
  http://www.erlang.com/calculator/

TDM ゲートウェイと VoIP トランキング ゲートウェイ

2006 年ごろまでは、企業内部の VoIP ネットワークを外部の音声サービスに接続するには、従来の公衆網に接続された TDM ゲートウェイを経由する以外に方法はありませんでした。シスコの製品ラインナップには、公衆網をはじめ、PBX やキー システムにもアナログおよびデジタル接続できる各種 TDM ゲートウェイが揃っています。TDM 接続では、低密度アナログ（FXS、FXO）、低密度デジタル（BRI）、高密度デジタル（T1、E1、T3）など、さまざまなインターフェイスを選択できます。

2006 年ごろから、一般に「SIP トランク サービス」と呼ばれる企業向けの新しい音声サービス オプションがサービス プロバイダーから提供されるようになりました。公衆網やその他の企業外部の宛先に SIP トランクを使用して接続するには、企業の VoIP ネットワークのエッジで IP-to-IP 接続が必要です。この相互接続ポイントでは、これまで TDM ゲートウェイによって実現されていたものと同じ機能（境界の設定、コール アドミッション制御、QoS の確保、トラブルシューティングの境界の確保、セキュリティのチェックなど）が引き続き必要となります。SIP トランキング接続では、企業とサービス プロバイダー ネットワーク間の相互接続ポイントにある Cisco Unified Border Element が Session Border Controller（SBC; セッション ボーダー コントローラ）としてこれらの機能を実行します。Cisco Unified Border Element には、プロトコル変換機能により、H.323 機器と SIP 機器、または異なる種類の SIP 実装を使用した SIP 機器どうしを相互接続する機能もあります。Cisco Unified Border Element ではトランスコーディングも実行可能です。これらのいずれかの機能を利用する場合は、企業ネットワーク内部におけるプロトコル変換 またはトランスコーディング サービスなしでは相互運用できない機器間の相互接続ポイントでも Cisco Unified Border Element を使用できます。

TDM ゲートウェイ プラットフォームについては、この章の残りの部分で詳しく説明します。Cisco Unified Border Element については、「Cisco Unified CM トランク」（P.5-1）の章に詳細が記載されています。両方の機能を同一の Cisco Integrated Services Router（ISR）プラットフォームで同時に有効にすることができます。

Cisco ゲートウェイの概要

Cisco アクセス ゲートウェイを使用すると、Cisco Unified Communications Manager（Unified CM）と IP 以外の通信デバイスとの間で情報を交換できます。Cisco アクセス ゲートウェイには、アナログとデジタルの 2 種類があります。

Cisco アクセス アナログ ゲートウェイ

Cisco アクセス アナログ ゲートウェイには、トランク ゲートウェイとステーション ゲートウェイの 2 つのカテゴリがあります。

- アクセス アナログ ステーション ゲートウェイ

  アナログ ステーション ゲートウェイは、Unified CM を Plain Old Telephone Service（POTS; 一般電話サービス）のアナログ電話機、IVR システム、FAX マシン、およびボイスメール システムに接続します。ステーション ゲートウェイは、Foreign Exchange Station（FXS）ポートを備えています。

- アクセス アナログ トランク ゲートウェイ

  アナログ トランク ゲートウェイは、Unified CM を公衆網 Central Office（CO; セントラル オフィス）または PBX トランクに接続します。トランク ゲートウェイは、公衆網、PBX、またはキー システムへのアクセス用の Foreign Exchange Office（FXO）ポート、および従来型の PBX とのアナログ トランク接続用の E&M（recEive and transMit、または ear and mouth）ポートを備えています。応答と接続解除の監視の問題を最小限に抑えるために、可能な限り、デジタル ゲートウェイを使用してください。アナログ Direct Inward Dialing（DID; ダイヤルイン方式）および Centralized Automatic Message Accounting（CAMA）も、公衆網接続に使用できます。

Cisco アクセス デジタル トランク ゲートウェイ

Cisco アクセス デジタル トランク ゲートウェイは、Primary Rate Interface（PRI; 一次群速度インターフェイス）、Basic Rate Interface（BRI; 基本速度インターフェイス）、または T1 Channel Associated Signaling（CAS; 個別線信号方式）などのデジタル トランクを経由して、Unified CM を公衆網または PBX に接続します。デジタル T1 PRI トランクは、所定の従来型ボイスメール システムとの接続にも使用できます。

ゲートウェイ ゲイン設定の調整

ゲートウェイを介して Cisco Unified Communications ネットワークを公衆網に接続するには、停電、インピーダンスの不整合、および遅延などによるエコーや信号の減衰から生じる、音声品質問題に適切に対処する必要があります。このため、予期されるすべての音声パスに信号損失の状況を詳細に提供する Network Transmission Loss Plan（NTLP）を確立する必要があります。このプランを使用して、最適な声の大きさと効果的なエコー キャンセレーションを得るために信号の強さを調整する必要があるロケーションを識別できます。すべての通信事業者が同じ損失プランを使用するわけではないこと、また、セルラー ネットワークの存在が NTLP の作成をさらに複雑にすることに注意してください。このような NTLP を作成する前に、ゲートウェイで入力ゲインや出力衰退を調整することはお勧めできません。詳細については、次の Web サイトで入手可能な『*Echo Analysis for Voice Over IP*』を参照してください。

http://www.cisco.com/en/US/docs/ios/solutions_docs/voip_solutions/EA_ISD.pdf

ゲートウェイの選択

IP テレフォニー ゲートウェイを選択する場合は、次の点を考慮してください。

- 「コア機能要件」（P.4-8）
- 「ゲートウェイ プロトコル」（P.4-9）
- 「ゲートウェイ プロトコルとコア機能要件」（P.4-11）
- 「サイト固有のゲートウェイ要件」（P.4-18）

コア機能要件

IP テレフォニー アプリケーションで使用するゲートウェイは、次のコア機能要件を満たす必要があります。

- Dual Tone MultiFrequency（DTMF）リレー機能

DTMF リレー機能、特にアウトバンド DTMF は、DTMF ディジットを音声ストリームから切り離し、音声ストリームまたはベアラ トラフィックの一部としてではなく、ゲートウェイ プロトコル（H.323、SCCP、MGCP、または SIP）シグナリング チャネルを通じて、シグナリング標識として送信します。音声圧縮に低ビット レート コーデックを使用する場合、DTMF 信号の損失また歪みの可能性があるので、アウトバンド DTMF が必要です。

- 付加サービス サポート

  付加サービスは、一般に、保留、転送、および会議などの基本的なテレフォニー機能です。

- FAX/ モデム サポート

  FAX over IP により、従来のアナログ FAX マシンと IP テレフォニー ネットワークとの相互運用性が可能になります。FAX イメージは、アナログ信号から変換され、パケット ネットワークを介してデジタル データとして伝送されます。詳細については、「FAX とモデムのサポート」（P.4-27）を参照してください。

- Unified CM 冗長性サポート

  Cisco Unified Communications は、分散モデルに基づき、高いアベイラビリティを確保しています。Unified CM クラスタには、Unified CM の冗長性が用意されています。ゲートウェイは、プライマリ Unified CM に障害が発生した場合に、セカンダリ Unified CM への「re-home」機能をサポートする必要があります。冗長性は、Unified CM またはネットワークの障害時のコール存続可能性とは異なります。

企業での配置用に選択する IP テレフォニー ゲートウェイがすべて、上記のコア要件を満たしていることを確認するには、ゲートウェイ製品の資料を参照してください。さらに、どの IP テレフォニーの実装についても、各サイト特有の機能要件（たとえば、アナログまたはデジタル アクセス、DID、およびキャパシティ要件）があります（「サイト固有のゲートウェイ要件」（P.4-18）を参照してください）。

ゲートウェイ プロトコル

Cisco Unified CM（Release 3.1 およびそれ以降）では、次のゲートウェイ プロトコルがサポートされています。

- H.323
- Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）

Cisco Unified CM Release 4.0 以降では、トランク側での Session Initiation Protocol（SIP）がサポートされています。Cisco Unified CM Release 5.0 ～ 7.*x* の SIP トランクの実装は、より多くの機能をサポートするよう拡張されました。

プロトコルの選択は、サイト特有の要件と機器の設置ベースによって決まります。たとえば、リモート サイトである支店の大部分のロケーションには、Cisco 2600XM、2800、3700、または 3800 シリーズのルータが設置されます。これらのルータは、Cisco IOS Release 12.2.11(T) および Cisco Unified CM Release 3.1 以降で、SIP、H.323、および MGCP 0.1 をサポートします。ゲートウェイの設定では、MGCP は設定が単純なので H.323 または SIP よりも優先されます。一方、サポートされるインターフェイスの堅牢性により、H.323 または SIP が MGCP より優先される場合もあります。

Simplified Message Desk Interface（SMDI）は、ボイスメール システムを PBX または Centrex システムに統合するための標準です。SMDI を介してボイスメール システムに接続し、アナログ FXS またはデジタル T1 PRI を使用するには、SCCP または MGCP プロトコルが必要です。これは、H.323 または SIP デバイスは、ポートのグループから、使用される特定の回線を識別しないからです。この目的に H.323 または SIP ゲートウェイを使用すると、Cisco Message Interface は、着信コールに使用される実際のポートまたはチャネルと、SMDI 情報とを正常に相関させることができません。

また、使用される Unified CM の配置モデルも、ゲートウェイ プロトコルの選択に影響を与える場合があります（「Unified Communications の配置モデル」（P.2-1）の章を参照してください）。

表 4-3 では、どのゲートウェイが所定のプロトコルをサポートするかを示しています。これらのプロトコルはそれぞれ、コア ゲートウェイ要件をサポートするために多少異なる方法を使用します。「ゲートウェイ プロトコルとコア機能要件」（P.4-11）では、各プロトコルがこれらの機能要件をどのように満たしているかを説明します。

表 4-3　サポートされるゲートウェイ プロトコルと Cisco Unified Communications ゲートウェイ

Cisco ゲートウェイ	MGCP 0.1	H.323	SCCP	SIP
Cisco 2900	あり、Cisco IOS Release 15.0.1M 以降 サポート対象： • FXS ポート • 会議およびトランスコーディングの DSP リソース	あり、Cisco IOS Release 15.0.1M 以降 サポート対象： • FXS ポート • 会議およびトランスコーディングの DSP リソース	あり、Cisco IOS Release 15.0.1M 以降 サポート対象： • FXS ポート • 会議およびトランスコーディングの DSP リソース	あり、SIP トランク
Cisco 3900	あり、Cisco IOS Release 15.0.1M 以降 サポート対象： • FXS ポート • 会議およびトランスコーディングの DSP リソース	あり、Cisco IOS Release 15.0.1M 以降 サポート対象： • FXS ポート • 会議およびトランスコーディングの DSP リソース	あり、Cisco IOS Release 15.0.1M 以降 サポート対象： • FXS ポート • 会議およびトランスコーディングの DSP リソース	あり、SIP トランク
Cisco 3800	あり、Cisco IOS Release 12.3.11T 以降 サポート対象： • アナログ FXS/FXO • T1 CAS（E&M Wink Start; Delay Dial のみ） • T1/E1 PRI	あり、Cisco IOS Release 12.3.11T 以降	あり（DSP リソースに対して）、Cisco IOS Release 12.3.11T 以降 FXS については、Cisco IOS Release 12.4.9.T 以降を使用	あり、SIP トランク
Cisco 2800	あり、Cisco IOS Release 12.3.8T4 以降 サポート対象： • アナログ FXS/FXO • T1 CAS（E&M Wink Start; Delay Dial のみ） • T1/E1 PRI	あり、Cisco IOS Release 12.3.8T4 以降	あり（DSP リソースに対して）、Cisco IOS Release 12.3.11T 以降 FXS については、Cisco IOS Release 12.4.9.T 以降を使用	あり、SIP トランク

表 4-3　サポートされるゲートウェイ プロトコルと Cisco Unified Communications ゲートウェイ （続き）

Cisco ゲートウェイ	MGCP 0.1	H.323	SCCP	SIP
Cisco 3700	あり サポート対象： • アナログ FXS/FXO • T1 CAS（E&M Wink Start; Delay Dial のみ） • T1/E1 PRI	あり	Cisco IOS Release 12.2.13T の DSP ファーム	あり、SIP トランク
Communication Media Module（CMM; コミュニケーション メディア モジュール）	あり サポート対象： • T1 CAS FXS • T1/E1 PRI • FXS	あり	なし	あり、SIP トランク
VGD-1T3	T3 の場合、Cisco IOS Release 12.4.22T	あり	あり	あり
VG224	あり FXS、会議、およびトランスコーディング	あり、FXS のみ	あり、Cisco IOS Release 12.4(2)T 以降	あり、FXS のみ
VG248	なし	なし	あり[1]	なし
Cisco ATA 188	あり、FXS のみ	あり、FXS のみ	あり、FXS のみ	あり、サードパーティ製の SIP 電話機
Cisco AS5350XM Cisco AS5400XM	なし	あり	なし	あり、SIP トランク
VG202 および VG204	あり、FXS のみ、Cisco IOS Release 12.4(9)T 以降	あり、FXS のみ、Cisco IOS Release 12.4(9)T 以降	あり、FXS のみ、Cisco IOS Release 12.4(9)T 以降	あり、FXS のみ、Cisco IOS Release 12.4(9)T 以降

1. VG248 は、H.323、MGCP、SIP のいずれでもなく、SCCP を使用するので、真のゲートウェイではありません。

（注）　配置する前に、Cisco IOS ソフトウェアのリリース ノートを調べて、機能またはインターフェイスのサポートを確認してください。

ゲートウェイ プロトコルとコア機能要件

ここでは、各プロトコル（SCCP、H.323、MGCP、および SIP）が次のゲートウェイ機能要件をどのようにサポートするかについて説明します。

• 「DTMF リレー」（P.4-12）

- 「付加サービス」（P.4-13）
- 「Unified CM の冗長性」（P.4-15）

DTMF リレー

DTMF は、信号に音声帯域内の特定の周波数ペアを使用するシグナリング方式です。64 kbps の Pulse Code Modulation（PCM; パルス符号変調）音声チャネルは、これらの信号を容易に伝送できます。しかし、音声圧縮に低ビット レート コーデックを使用する場合、DTMF 信号の損失または歪みの可能性があります。Voice over IP（VoIP）インフラストラクチャを介して DTMF トーンを伝送するアウトバンド シグナリング方式は、コーデックにより誘発されるこれらの症状を簡単に解決します。

SCCP ゲートウェイ

Cisco VG248 は、Transmission Control Protocol（TCP; 伝送制御プロトコル）ポート 2002 を使用して、DTMF 信号をアウトバンドで伝送します。アウトバンド DTMF は、VG248 用のデフォルトのゲートウェイ コンフィギュレーション モードです。

H.323 ゲートウェイ

Cisco 3800 シリーズ製品などの H.323 ゲートウェイは、DTMF 信号をアウトバンドで交換するための拡張 H.245 機能を使用して、Unified CM と情報を交換できます。次の例は、Cisco IOS ゲートウェイ上のアウトバンド DTMF 設定例です。

```
dial-peer voice 100 voip
destination-pattern 555….
session target ipv4:10.1.1.1
CODEC g729ar8
dtmf-relay h245-alphanumeric
preference 0
```

MGCP ゲートウェイ

Cisco IOS ベースのプラットフォームでは、Unified CM 通信に MGCP を使用します（MGCP をサポートするシスコのゲートウェイ プラットフォームのリストについては、表 4-3 を参照してください）。MGCP プロトコルには、*パッケージ*の概念があります。MGCP ゲートウェイは、始動後、DTMF パッケージをロードします。MGCP ゲートウェイは、制御チャネルを介して、受信した DTMF トーンを表す*シンボル*を送信します。次に、Unified CM は、これらの信号を解釈し、アウトバンドでシグナリング エンドポイントに DTMF 信号を渡します。DTMF リレーのグローバル コンフィギュレーション コマンドは、次のとおりです。

```
mgcp dtmf-relay CODEC all mode out-of-band
```

Unified CM MGCP ゲートウェイ設定インターフェイスで、追加の設定パラメータを入力する必要があります。

デフォルトで DTMF リレーは使用可能であり、追加の設定は必要ありません。

（注）　RFC 2833 を通じて DTMF を有効にするには、**fm-package** コマンドを使用します。このコマンドは、Cisco IOS Release 12.4(6)T 以降で使用できます。

SIP ゲートウェイ

Cisco IOS ベースのプラットフォームでは、Unified CM 通信に SIP を使用できます（SIP をサポートするシスコのゲートウェイ プラットフォームのリストについては、表 4-3 を参照してください）。シスコのゲートウェイ プラットフォームでは、DTMF に関する各種の方式をサポートしていますが、Unified CM との通信には次の方式だけを使用できます。

- Named Telephony Events（NTE）、または RFC 2833
- Unsolicited SIP Notify（UN）
- Key Press Markup Language（KPML）

次の例は、NTE 用の設定を示しています。

```
dial-peer voice 100 voip
destination-pattern 555….
session target ipv4:10.1.1.1
session protocol sipv2
dtmf-relay rtp-nte
```

次の例は、UN 用の設定を示しています。

```
dial-peer voice 100 voip
destination-pattern 555….
session target ipv4:10.1.1.1
session protocol sipv2
dtmf-relay sip-notify
```

DTMF 方式の選択の詳細については、「メディア リソース」（P.6-1）の章を参照してください。

付加サービス

付加サービスは、保留、転送、および会議などのユーザ機能を提供します。これらのサービスは、音声通信の確立の基本的な要件であると見なされます。IP テレフォニー ネットワークでの使用について評価される各ゲートウェイは、ソフトウェアの Media Termination Point（MTP; メディア ターミネーション ポイント）を使用しなくても、独自に付加サービスをサポートする必要があります。

SCCP ゲートウェイ

Cisco SCCP ゲートウェイは、完全な付加サービス サポートを提供します。また、Cisco IOS Release 12.4.9T で FXS SCCP ポートもサポートしています。SCCP ゲートウェイは、ゲートウェイと Unified CM 間のシグナリング チャネル、および SCCP を使用して、コール制御パラメータを交換します（SCCP をサポートするシスコのゲートウェイ プラットフォームのリストについては、表 4-3 を参照してください）。

H.323 ゲートウェイ

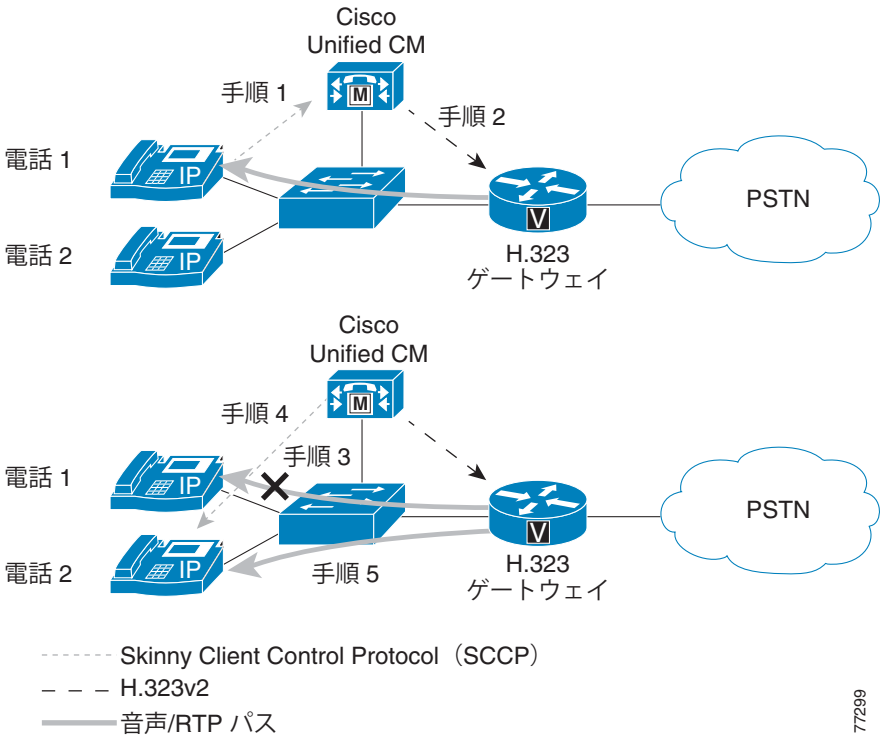
H.323v2 は、Open/Close LogicalChannel 機能と emptyCapabilitySet 機能を実行します。Cisco IOS Release 12.0(7)T および Cisco Unified CM Release 3.0 以降から始まった、H.323 ゲートウェイによる H.323v2 の使用により、MTP が付加サービスを提供する必要がなくなりました。Unified CM Release 3.1 以降では、トランスコーダが動的に割り当てられるのは、G.711 専用デバイスへのアクセスを提供すると同時に、WAN を介した G.729 ストリームを保持するために、コール中に必要な場合だけです。H.323v2 に対するフル サポートは、Cisco IOS Release 12.1.1T で利用可能です。

Unified CM を H.323 プロキシとして使用して、Cisco IOS ゲートウェイと IP Phone 間で H.323v2 コールがセットアップされた後は、その IP Phone は、ベアラ接続の変更を要求できます。Real-Time Transport Protocol（RTP）ストリームは、Cisco IOS ゲートウェイから IP Phone に直接接続されるので、サポートされる音声コーデックをネゴシエートできます。

図 4-1 と次の手順では、2 台の IP Phone 間のコール転送を示しています。

1. 電話機 1 が Cisco IOS ゲートウェイから電話機 2 にコールを転送しようとする場合、電話機 1 は、SCCP を使用して Unified CM に転送要求を出します。
2. Unified CM は、この要求を H.323v2 CloseLogicalChannel 要求に変換して、Cisco IOS ゲートウェイに送信して、適切な SessionID を求めます。
3. Cisco IOS ゲートウェイは、電話機 1 との RTP チャネルをクローズします。
4. Unified CM は、SCCP を使用して、Cisco IOS ゲートウェイとの RTP 接続をセットアップする要求を、電話機 2 に出します。同時に、Unified CM は、新しい宛先パラメータを指定して（ただし、同じ SessionID を使用）、Cisco IOS ゲートウェイに OpenLogicalChannel 要求を出します。
5. Cisco IOS ゲートウェイがこの要求を確認した後、RTP 音声ベアラ チャネルが、電話機 2 と Cisco IOS ゲートウェイとの間で確立されます。

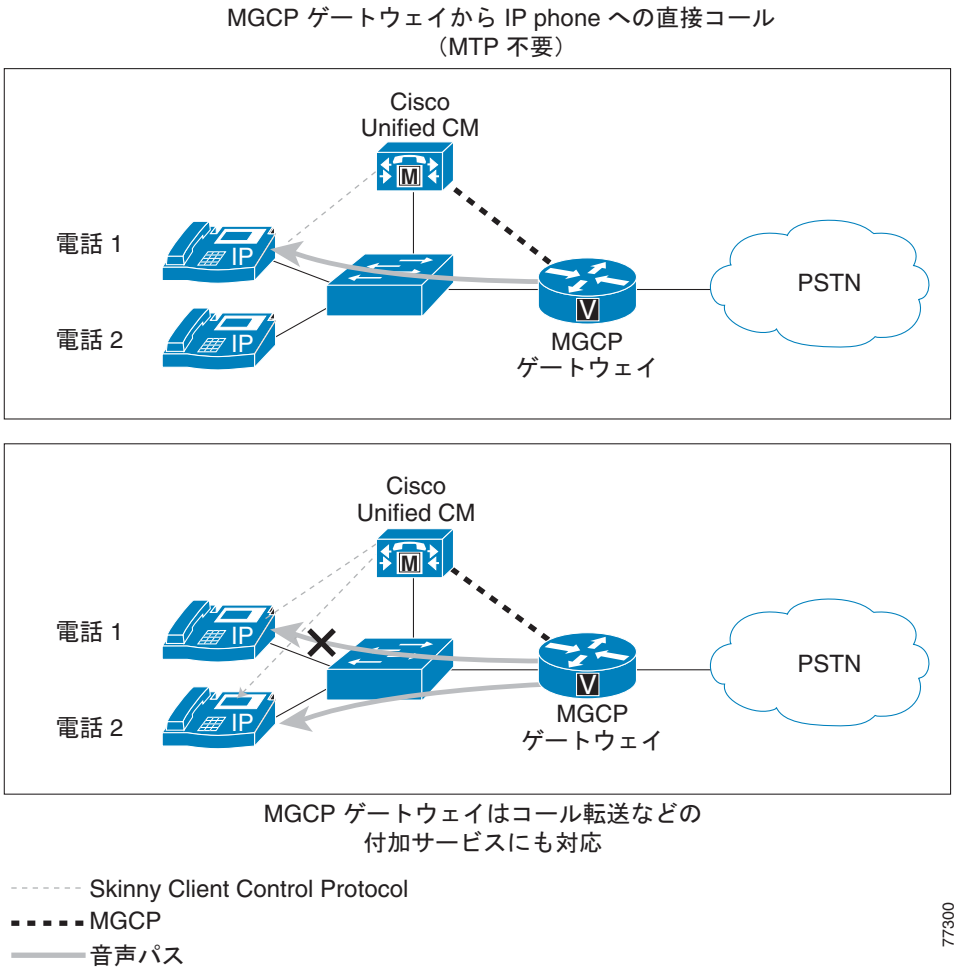
図 4-1　　H.323 ゲートウェイの付加サービス サポート



MGCP ゲートウェイ

MGCP ゲートウェイは、MGCP プロトコルを使用して、保留、転送、および会議機能を完全にサポートします。MGCP プロトコルは、すべてのセッション機能を制御する、Unified CM とのマスター / スレーブ プロトコルであるので、Unified CM は、MGCP ゲートウェイの音声接続を容易に操作できます。IP テレフォニー エンドポイント（たとえば、IP Phone）が、セッションの変更（たとえば、コールを別のエンドポイントに転送する）を必要とする場合、そのエンドポイントは、セッションの変更を SCCP を使用して Unified CM に通知します。次に、Unified CM は、Session ID に関連した現在の RTP ストリームを終了し、新しいエンドポイント情報を使用して新しいメディア セッションを開始することを、MGCP User Datagram Protocol（UDP; ユーザ データグラム プロトコル）制御接続を使用して、MGCP ゲートウェイに通知します。図 4-2 では、プロトコルが MGCP ゲートウェイ、エンドポイント、および Unified CM 間で交換される様子を示しています。

図 4-2　MGCP ゲートウェイの付加サービス サポート



SIP ゲートウェイ

Cisco IOS SIP ゲートウェイへの Unified CM SIP トランク インターフェイスは、保留、ブラインド転送、在席転送などの付加サービスをサポートしています。付加サービスのサポートは、INVITE や REFER などの SIP 方式によって実現されます。詳細については、次のマニュアルを参照してください。

- 『*Cisco Unified Communications Manager System Guide*』。次のサイトにあります。
  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- 『*Cisco IOS SIP Configuration Guide*』。次のサイトにあります。
  http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/12_4t/sip_12_4t_book.html

Unified CM の冗長性

IP テレフォニー アーキテクチャの必須部分は、高価な専有の従来型の PBX システムの代わりに、低コストの分散型 PC ベース システムを提供することです。この分散型設計は、クラスタ化された Unified CM の堅固なフォールト トレラント アーキテクチャに適しています。最も単純な形式（2 システムのクラスタ）であっても、セカンダリ Unified CM は、最初にプライマリ Unified CM によって管理されていたすべてのゲートウェイの制御権を引き受ける必要があります。

SCCP ゲートウェイ

ブート後、Cisco VG224、VG248、および ATA 188 ゲートウェイには、Unified CM サーバ情報が提供されます。これらのゲートウェイが初期設定されるときに、Unified CM のリストがゲートウェイにダウンロードされます。このリストでは、プライマリ Unified CM とセカンダリ Unified CM に優先順位が付けられています。プライマリ Unified CM が通信不能になった場合、ゲートウェイはセカンダリ Unified CM に登録されます。

WAN リンク障害用の H.323 VoIP コール プリザベーション

WAN リンク障害用の H.323 VoIP コール プリザベーション拡張機能を使用すると、他のエンドポイントとは異なるエンティティ（シグナリングをルーティングするゲートキーパーや、接続している 2 者間でシグナリングを仲介するコール エージェント（Cisco BTS 10200 Softswitch、Cisco PGW2200 Softswitch、Cisco Unified CM など）など）によってシグナリングが処理される H.323 トポロジにおいて、接続性が維持されます。コール プリザベーションが役立つのは、ゲートウェイと他のエンドポイント（通常は Cisco Unified IP Phone）は同じサイトにあるものの、コール エージェントがリモート サイトにあり、接続障害が起こりやすいような場合です。

H.323 コール プリザベーションは、次の種類の障害と接続に対応します。

障害の種類：

- WAN リンクのフラッピングや性能低下などの WAN 障害
- Cisco Unified CM ソフトウェアの障害（Unified CM サーバでの ccm.exe サービスのクラッシュなど）
- LAN 接続の障害（障害がローカル ブランチで発生した場合を除く）

接続の種類：

- Cisco Unified CM で制御された 2 つのエンドポイント間のコールで、次の条件に該当する場合
  - Unified CM がリロード中の場合
  - 一方または両方のエンドポイントと Unified CM との間で H.225.0 または H.245 メッセージのシグナリングに使用される TCP 接続が失われたか、フラッピングしている場合
  - エンドポイントがクラスタ内の異なる Unified CM に登録されていて、その 2 つの Unified CM 間の TCP 接続が失われた場合
  - IP Phone 間のコールで、公衆網が同じサイトにある場合
- ソフトスイッチによって制御されている Cisco IOS ゲートウェイとエンドポイント間のコールで、シグナリング（H.225.0、H.245、またはその両方）フローはゲートウェイとソフトスイッチ間で実行され、メディア フローはゲートウェイとエンドポイント間で実行される場合
  - ソフトスイッチがリロード中の場合
  - ゲートウェイとソフトスイッチ間の H.225.0 または H.245 TCP 接続が失われ、ソフトスイッチがエンドポイント上のコールをクリアしない場合
  - ソフトスイッチとエンドポイント間の H.225.0 または H.245 TCP 接続が失われ、ソフトスイッチがゲートウェイ上のコールをクリアしない場合
- メディア フローアラウンド モードで動作している Cisco Unified Border Element（旧称 Cisco Multiservice IP-to-IP Gateway）がコール フローに含まれていて、その Cisco Unified Border Element がリロードしているか、ネットワークの残りの部分との接続を失った場合

メディアが保持された後、一方の通話者が電話を切るか、メディアがアクティブでないことが検出されると、コールは終了します。コンピュータによって生成されたメディア ストリーム（メディア サーバからの音楽ストリーミングなど）が存在する場合は、メディア非アクティビティ検出は機能しません

が、コールは保留になる可能性があります。Cisco Unified CM はこの状況に対処するため、このようなコールは保持しないようにゲートウェイに指示しますが、サードパーティ製デバイスや Cisco Unified Border Element はそうしたことは行いません。

この機能において、フラッピングは「IP 接続の一時的な喪失が何度も繰り返されること」と定義されています。このような現象は、WAN または LAN の障害によって発生する可能性があります。Cisco IOS ゲートウェイと Cisco Unified CM 間の H.323 VoIP コールは、フラッピングが起こると終了する場合があります。Unified CM は、TCP 接続が失われたことを検出すると、コールをクリアし、TCP FIN を送信してコールで使用されていた TCP ソケットを閉じます。このとき、H.225.0 Release Complete メッセージまたは H.245 End Session メッセージは送信しません。これを *quiet clearing* と呼びます。ネットワークが短時間復帰した間に Unified CM から送信された TCP FIN がゲートウェイに到達すると、ゲートウェイはコールを終了します。TCP FIN がゲートウェイに到達しなくても、ネットワークが復帰すると、ゲートウェイから送信された TCP キープアライブが Unified CM に到達します。Unified CM はすでに TCP 接続を閉じているので、キープアライブに応答して TCP RST メッセージを送信します。ゲートウェイは RST メッセージを受け取ると、H.323 コールを終了します。

WAN リンク障害用の H.323 VoIP コール プリザベーション拡張機能の設定には、**call preserve** コマンドの設定を含める必要があります。Cisco Unified Communications Manager を使用している場合は、Service Parameters ウィンドウから Allow Peer to Preserve H.323 Calls パラメータを有効にする必要があります。

call preserve コマンドを発行すると、H.225.0 または H.245 接続でのアクティブ コールに関するソケットの終了またはソケット エラーがゲートウェイで無視されるため、これらの接続を使用しているコールを終了せずにソケットを閉じることができます。

すべてのコールに対して H.323 VoIP コール プリザベーションを有効にする例

次の設定例では、すべてのコールに対して H.323 VoIP コール プリザベーションを有効にします。

```
voice service voip
 h323
  call preserve
```

MGCP ゲートウェイ

MGCP ゲートウェイにも、プライマリ Unified CM との通信が失われた場合に、セカンダリ Unified CM にフェールオーバーする機能があります。フェールオーバーが起きても、アクティブ コールは保持されます。

MGCP ゲートウェイのコンフィギュレーション ファイル内で、プライマリ Unified CM は、**call-agent <hostname>** コマンドを使用して指定され、セカンダリ Unified CM のリストは、**ccm-manager redundant-host** コマンドを使用して追加されます。プライマリ Unified CM とのキープアライブは、MGCP アプリケーション レベルのキープアライブ メカニズムを介して行われます。このメカニズムでは、MGCP ゲートウェイは、空の MGCP notify（NTFY）メッセージを Unified CM に送信し、確認応答を待ちます。バックアップ Unified CM とのキープアライブは、TCP キープアライブ メカニズムを介して行われます。

プライマリ Unified CM が後で使用可能になると、MGCP ゲートウェイは、元の Unified CM に「re-home」（つまり復帰）できます。この復帰は、ただちに行われることもあれば、設定可能な時間が経過した後、または接続されているすべてのセッションが解除された後に行われることもあります。これは、次のグローバル コンフィギュレーション コマンドを使用して使用可能になります。

```
ccm-manager redundant-host <hostname1 | ipaddress1 > <hostname2 | ipaddress2>
[no] call-manager redundancy switchback [immediate|graceful|delay <delay_time>]
```

SIP ゲートウェイ

Cisco IOS SIP ゲートウェイでの冗長性は、H.323 と同様の方法で実現できます。SIP ゲートウェイがプライマリ Unified CM との接続を確立できない場合、高い優先順位を持ち、別の dial-peer ステートメントで指定されるセカンダリ Unified CM との接続を試行します。

デフォルトでは、Cisco IOS SIP ゲートウェイは dial-peer で設定された Unified CM の IP アドレスに SIP INVITE 要求を 6 回送信します。SIP ゲートウェイは、その Unified CM から応答を受信しなかった場合、他の dial-peer で設定された、優先順位の高い Unified CM との接続を試行します。

Cisco IOS SIP ゲートウェイは、INVITE に対する SIP 100 応答を 500 ms 待ちます。デフォルトでは、Cisco IOS SIP ゲートウェイがバックアップ Unified CM に到達するまでに最大 3 秒かかります。SIP INVITE の再試行回数は、**sip-ua** 設定で **retry invite** <*number*> コマンドを使用して変更できます。また、Cisco IOS SIP ゲートウェイが SIP INVITE 要求に対する SIP 100 応答を待つ期間は、**sip-ua** 設定で *timers trying* **<time>** コマンドを使用して変更できます。

バックアップ Unified CM へのフェールオーバーを高速化する別の方法としては、**dial-peer** 文での **monitor probe icmp-ping** コマンドの設定があります。Unified CM が Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）エコー メッセージ（ping）に応答しなかった場合、そのダイヤルピアはシャットダウンされます。このコマンドが役に立つのは、Unified CM が到達不能のときだけです。ICMP エコーメッセージは、10 秒ごとに送信されます。

次のコマンドを使用すると、Cisco IOS SIP ゲートウェイに対して Unified CM の冗長性を設定できます。

```
sip-ua
 retry invite <number>
 timers trying <time>

dial-peer voice 101 voip
 destination-pattern 2...
 session target ipv4:10.1.1.101
 preference 0
 monitor probe icmp-ping
 session protocol sipv2


dial-peer voice 102 voip
 destination-pattern 2...
 session target ipv4:10.1.1.102
 preference 1
 monitor probe icmp-ping
 session protocol sipv2
```

サイト固有のゲートウェイ要件

IP テレフォニーの実装にはそれぞれ、サイト固有の要件があります。次の質問は、IP テレフォニーゲートウェイの選択に役立ちます。

- 公衆網（または PBX）アクセスは、アナログですか、デジタルですか。
- 公衆網または PBX には、どのタイプのアナログ（FXO、FXS、E&M、DID、CAMA）インターフェイス、またはデジタル（T1、E1、CAS、CCS）インターフェイスが必要ですか。
- 公衆網アクセスがデジタルである場合、どのタイプのシグナリングが必要ですか（T1 CAS、Q.931 PRI、E1 CAS、または R2）。

- PBX は、現在どのタイプのシグナリングを使用していますか。
  - FXO または FXS: ループ スタートまたはグラウンド スタート
  - E&M: ウィンク スタート、ディレイ スタート、またはイミディエート スタート
  - E&M: タイプ I、II、III、IV、または V
  - T1: CAS、Q.931 PRI（ユーザ側またはネットワーク側）、QSIG、DPNSS、または Proprietary D チャネル（CCS）シグナリング
  - E1: CAS、R2、Q.931 PRI（ユーザ側またはネットワーク側）、QSIG、DPNSS、Proprietary D チャネル（CCS）シグナリング
- PBX は、現在どのタイプのフレーム同期（SF、ESF、または G.704）と回線エンコーディング（B8ZS、AMI、CRC-4、または HDB3）を使用していますか。
- PBX に、専有シグナリングを渡す必要がありますか。必要な場合、そのシグナリングはどのタイムスロットで渡されますか。それは HDLC フレームですか。
- ゲートウェイにどれくらいのキャパシティが必要ですか。つまり、チャネルがいくつ必要ですか（一般に、音声チャネルが 12 本以上必要な場合は、デジタルの方が、アナログ ソリューションより費用対効果が高くなります）。
- ダイヤルイン方式（DID）が必要ですか。必要な場合は、アナログか、デジタルかを指定してください（日本ではアナログ DID 未対応）。
- 発呼回線 ID（CLID）が必要ですか。
- 発信者名が必要ですか。
- どのタイプの FAX およびモデム サポートが必要ですか。
- どのタイプの音声圧縮が必要ですか。
- どのタイプの付加サービスが必要ですか。
- PBX はクロッキングをサポートしますか。または PBX は、Cisco ゲートウェイがクロッキングをサポートすることを期待しますか。
- 必要なすべてのゲートウェイ、ルータ、およびスイッチを収容するラック スペースがありますか。

（注） Direct Inward Dial（DID; ダイヤルイン方式）とは、オペレータが介在しなくても、外部コールを直接、端末回線に着信できるようにする Private Branch eXchange（PBX; 構内交換機）またはセントレック（Centrex）機能のことです。

（注） 発呼回線 ID（CLI、CLID、または ANI）とは、着呼側に対して発信番号を表示する、デジタル電話ネットワークで利用可能なサービスを指します。セントラル オフィス機器は、発信者の電話番号を識別し、発信者についての情報をコール自体と一緒に送信できるようにします。CLID は、Automatic Number Identification（ANI; 自動番号識別）と同義です。

Cisco Unified Communications ゲートウェイは、大部分の主要 PBX ベンダー製品と相互運用でき、EIA/TIA-464B に準拠しています。

可能な選択肢を絞り込むには、サイト固有およびコアのゲートウェイ要件から始めるのが適しています。必要な機能を指定した後、該当する設定ごとに、企業における規模と複雑さが異なる単一サイトの配置であるか、マルチサイトによる配置であるかに関係なく、ゲートウェイの選択を行うことができます。

次の表では、さまざまな Cisco ゲートウェイ モデルによってサポートされる機能とインターフェイス タイプをまとめています。

（注）　次の表では、Cisco IOS および Unified CM のリリース番号は、リストされている機能を特定のゲートウェイ プラットフォーム上でサポートできるようになったリリースを指しています。Cisco IOS 機能の詳細については、Cisco Feature Navigator（http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp）を参照してください。

Cisco アナログ ゲートウェイ

表 4-4 では、H.323 または SIP を使用する Cisco アナログ ゲートウェイに対してサポートされているインターフェイス タイプをリストしています。表 4-5 では、MGCP を使用する Cisco アナログ ゲートウェイに対してサポートされているインターフェイス タイプをリストしています。

表 4-4　サポートされるアナログ H.323 および SIP 機能

	インターフェイス タイプ					
Cisco ゲートウェイ	**FXS**	**FXO**	**E&M**	**FXO、バッテリ リバーサル**	**アナログ DID**	**CAMA 911**
3900 シリーズ	あり	あり	あり	あり	あり	あり
2900 シリーズ	あり	あり	あり	あり	あり	あり
VG202 および VG204	あり	なし	なし	なし	なし	なし
8800 シリーズ	あり	あり	なし	あり	なし	なし
3800 シリーズ	あり	あり	あり	あり	あり	あり
2800 シリーズ	あり	あり	あり	あり	あり	あり
3700 シリーズ[1]	あり	あり	あり	あり	あり	あり
CMM 24FXS	あり	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG224	あり	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG248	なし	なし	なし	なし	なし	なし
Analog Telephone Adapter（ATA）[1]	あり	なし	なし	なし	なし	なし
7x00 ファミリ	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外

1. これらのモデルは販売終了になりました。

表 4-5　サポートされるアナログ MGCP 機能

	インターフェイス タイプ					
Cisco ゲートウェイ	FXS	FXO	E&M	FXO、バッテリ リバーサル	アナログ DID	CAMA 911
3900 シリーズ	あり	あり	なし	あり	なし	なし
2900 シリーズ	あり	あり	なし	あり	なし	なし
VG202 および VG204	あり	なし	なし	なし	なし	なし
8800 シリーズ	あり	あり	なし	あり	なし	なし
3800 シリーズ	あり	あり	なし	あり	なし	なし
2800 シリーズ	あり	あり	なし	あり	なし	なし
3700 シリーズ[1]	あり	あり	なし	あり	なし	なし
CMM 24FXS	あり	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG224	あり	なし	なし	なし	なし	なし
VG248	なし	なし	なし	なし	なし	なし
Analog Telephone Adapter（ATA）[1]	あり	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
7x00 ファミリ	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外

1. これらのモデルは販売終了になりました。

Cisco デジタル ゲートウェイ

表 4-6 ～表 4-9 では、H.323 または SIP を使用する Cisco デジタル ゲートウェイに対してサポートされているインターフェイス タイプをリストしています。表 4-10 では、MGCP を使用する Cisco デジタル ゲートウェイに対してサポートされているインターフェイス タイプをリストしています。

表 4-6　BRI、T1 CAS、T1 FGB、T1 FGD、および T1 QSIG に対してサポートされるデジタル H.323 および SIP 機能

	インターフェイス タイプ							
Cisco ゲートウェイ	BRI（TE、ユーザ側）	BRI（NT、ネットワーク側）	BRI QSIG（Net3）	BRI 電話	T1 CAS（robbed ビット）	T1 FGB	T1 FGD	T1 QSIG
3900 シリーズ	あり	あり	あり	なし	あり	なし	あり	あり
2900 シリーズ	あり	あり	あり	なし	あり	なし	あり	あり
3800 シリーズ	あり	あり	あり	なし	あり	なし	あり	あり
2800 シリーズ	あり	あり	あり	なし	あり	なし	あり	あり
3700 シリーズ[1]	あり	あり	あり	なし	あり	なし	あり	あり
5400XM	なし	なし	なし	なし	あり	あり	あり	あり
CMM 24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	適用対象外	適用対象外	適用対象外	適用対象外	あり	なし	なし	あり
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG248	なし	なし	なし	なし	なし	なし	なし	なし
Analog Telephone Adapter（ATA）[1]	なし	なし	なし	なし	なし	なし	なし	なし
7x00 ファミリ	該当なし	該当なし	該当なし	該当なし	あり	なし	あり	あり

1. これらのモデルは販売終了になりました。

表 4-7　T1 PRI SL-1、4ESS、および 5ESS に対してサポートされるデジタル H.323 および SIP 機能

	インターフェイス タイプ					
Cisco ゲートウェイ	T1 PRI（ユーザ、DMS-100）	T1 PRI（ネットワーク、SL-1）	T1 PRI（ユーザ、4ESS）	T1 PRI（ネットワーク、4ESS）	T1 PRI（ユーザ、5ESS）	T1 PRI（ネットワーク、5ESS）
3900 シリーズ	あり	なし	あり	あり	あり	あり
2900 シリーズ	あり	なし	あり	あり	あり	あり
3800 シリーズ	あり	なし	あり	あり	あり	あり
2800 シリーズ	あり	なし	あり	あり	あり	あり
3700 シリーズ[1]	あり	なし	あり	なし	あり	なし
5400XM	あり	なし	あり	あり	あり	あり
CMM 24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	あり	あり	あり	あり	あり	あり
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG248	なし	なし	なし	なし	なし	なし
Analog Telephone Adapter（ATA）[1]	なし	なし	なし	なし	なし	なし
7x00 ファミリ	あり	なし	あり	なし	あり	なし

1. これらのモデルは販売終了になりました。

表 4-8　T1 PRI NI2、NFAS、および Network Specific Facilities（NSF）サービスに対してサポートされるデジタル H.323 および SIP 機能

	インターフェイス タイプ					
Cisco ゲートウェイ	T1 PRI（ユーザ、NI2）	T1 PRI（ネットワーク、NI2）	T1 PRI NFAS（ユーザ、DMS-100）	T1 PRI NFAS（ユーザ、4ESS）	T1 PRI NFAS（ユーザ、5ESS）	T1 PRI（Megacom または SDN、4ESS）
3900 シリーズ	あり	あり	あり	あり	あり	あり
2900 シリーズ	あり	あり	あり	あり	あり	あり
3800 シリーズ	あり	あり	あり	あり	あり	あり
2800 シリーズ	あり	あり	あり	あり	あり	あり
3700 シリーズ[1]	あり	あり	あり	あり	あり	あり
5400XM	あり	あり	あり	あり	あり	あり
CMM 24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	あり	あり	あり	あり	あり	なし
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG248	なし	なし	なし	なし	なし	なし
Analog Telephone Adapter（ATA）[1]	なし	なし	なし	なし	なし	なし
7x00 ファミリ	あり	あり	なし	なし	なし	なし

1. これらのモデルは販売終了になりました。

表 4-9　E1 および J1 に対してサポートされるデジタル H.323 および SIP 機能

	インターフェイス タイプ						
Cisco ゲートウェイ	E1 CAS	E1 MELCAS	E1 R2	E1 PRI（ユーザ側、Net5）	E1 PRI（ネットワーク側、Net5）	E1 QSIG	J1[1]
3900 シリーズ	あり	あり	あり	あり	あり	あり	なし
2900 シリーズ	あり	あり	あり	あり	あり	あり	なし
3800 シリーズ	あり	あり	あり	あり	あり	あり	あり
2800 シリーズ	あり	あり	あり	あり	あり	あり	あり
3700 シリーズ[2]	あり	あり	あり	あり	あり	あり	あり
CMM 24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	なし	なし	あり	あり	あり	あり	適用対象外
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG248	なし	なし	なし	なし	なし	なし	なし
Analog Telephone Adapter（ATA）[2]	なし	なし	なし	なし	なし	なし	なし
7x00 ファミリ	あり	なし	あり	あり	あり	あり	なし

1. このインターフェイス タイプは販売終了になりました。
2. これらのモデルは販売終了になりました。

表 4-10　サポートされるデジタル MGCP 機能

Cisco ゲートウェイ	インターフェイス タイプ							
	BRI[1]	T1 CAS（E&M）	T1 CAS フックフラッシュ	T1 PRI	T1 QSIG	E1 PRI	E1 QSIG	T3
3900 シリーズ	15.0.1M	あり[2]	あり	あり[2]	あり[2]	あり[2]	あり[2]	なし
2900 シリーズ	15.0.1M	あり[2]	あり	あり[2]	あり[2]	あり[2]	あり[2]	なし
3800 シリーズ	12.4(2)T	あり[2]	あり	あり[2]	あり[2]	あり[2]	あり[2]	なし
2800 シリーズ	12.4(2)T	あり[2]	あり（2811、2821、2851）	あり[2]	あり[2]	あり[2]	あり[2]	なし
3700 シリーズ[3]	12.4(2)T	あり[2]	あり	あり[2]	あり[2]	あり[2]	あり[2]	なし
VGD-1T3	なし	なし	なし	なし	なし	なし	なし	あり
CMM 24FXS	適用対象外	適用対象外	あり	適用対象外	適用対象外	適用対象外	適用対象外	なし
CMM-6T1/E1	適用対象外	あり	あり	あり	あり	あり	あり	なし
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	なし
VG248	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	なし
Analog Telephone Adapter（ATA）[3]	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	なし
7x00 ファミリ	適用対象外	なし	適用対象外	なし	なし	なし	なし	なし

1. Cisco IOS Release 12.4(2)T は、BRI MGCP を NM-HDV2、NM-HD-XX、オンボード H-WIC スロットの各ハードウェアでサポートします。BRI MGCP は、NM-1V/2V ハードウェアで旧リリースの Cisco IOS によってもサポートされています。
2. AIM-VOICE-30 モジュールは、MGCP のサポートに Cisco IOS Release 12.2.13T を必要とします。
3. これらのモデルは販売終了になりました。

QSIG サポート

QSIG は、企業ネットワーク内で PBX 機器を柔軟に接続するために設計された、1 組の国際標準です。その他の機能の 1 つとして、QSIG には、さまざまなベンダー製の PBX 機器を相互接続するためのオープンな標準ベースの方法が用意されています。

ECMA QSIG は、PBX-to-PBX モードの H.323 ゲートウェイでサポートされています。H.323 ゲートウェイは、QSIG 情報要素に対する QSIG 機能の完全な透過性を備えています。基本的なコールのセットアップと終了は、表 4-11 に示されているように、H.323 QSIG ゲートウェイを使用してサポートされます。

表 4-11　H.323 ゲートウェイにおける QSIG サポート

プラットフォーム	メディア	必要な Cisco IOS ソフトウェア対応リリース
Cisco 3900 シリーズ	BRI および T1/E1 QSIG	15.0.1M
Cisco 2900 シリーズ	BRI および T1/E1 QSIG	15.0.1M
Cisco 3800 シリーズ	BRI および T1/E1 QSIG	12.3.11T
Cisco 2800 シリーズ	BRI および T1/E1 QSIG	12.3.8T4
Cisco 3700[1]	T1/E1 QSIG	12.2.8T
Cisco AS5350XM Cisco AS5400XM	T1/E1	12.2.2T

1. これらのモデルは販売終了になりました。

Cisco IOS ゲートウェイにおける QSIG のサポートの詳細については、次の Web サイトにあるマニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios/12_1t/12_1t2/feature/guide/dt_qsig.html

Cisco Unified CM Release 3.3 よりも前のリリースでは、PBX が H.323 を介して QSIG を使用するゲートウェイに接続されている場合、PBX 上の電話機と、Unified CM に接続されている IP Phone との間でコールが行われるときにサポートされているのは、基本的な PRI 機能だけです。Calling Line Identifier（CLID; 発呼回線 ID）と DID 番号だけが含まれるこの基本機能は、Unified CM によってではなく、QSIG プロトコルを終端するゲートウェイによってサポートされています。

Unified CM が QSIG 機能をサポートするには、QSIG を Unified CM に直接バックホール（back-haul）する必要があります。このサポートは、すべての MGCP T1/E1 ISDN ゲートウェイと連携して、Cisco Unified CM 3.3 以降のリリースで提供されています。

FAX とモデムのサポート

ここでは、Unified CM と Cisco 音声ゲートウェイで使用可能な FAX とモデムのサポートについて説明します。まず、Cisco 音声ゲートウェイ上での FAX とモデムのサポートの概要を説明した後、サポートされるプラットフォームとコンフィギュレーション ファイル例をリストします。

ゲートウェイでの FAX パススルーと FAX リレーのサポート

FAX over IP により、従来のアナログ FAX マシンと IP テレフォニー ネットワークとの相互運用性が可能になります。FAX イメージは、アナログ信号から変換され、パケット ネットワークを介してデジタルで伝送されます。

元の形式では、FAX データはデジタルで、High-Level Data Link Control（HDLC; ハイレベル データリンク コントロール）フレームに含まれています。しかし、従来の公衆網を経由して送信するために、これらのデジタル HDLC フレームはアナログ搬送波に変調されます。このアナログ搬送波は、公衆網環境で効果的に FAX を送信するためには必要ですが、IP パケット ネットワークで使用されるデジタル転送方式にとっては最適ではありません。そのため、IP インフラストラクチャ上で FAX を送信できるように、専用の転送方法が考案されました。

IP 上で FAX を転送する主な方法には、パススルーとリレーの 2 つがあります。パススルーは最も単純な方法で、音声コーデックが人間の音声に対して行うのと同じように、アナログ FAX 信号をサンプリングしてデジタル化します。使用可能なコーデックは多数存在しますが、パススルーでは、アナログ FAX 信号の歪みが最も少ないという理由で、常に G.711 コーデックを使用して FAX 情報が伝送されます。元の音声コールで高圧縮コーデックが使用されている場合は、アップスピード機能を使用してそのコーデックが G.711 に変更されます。パススルーは一般に Voice Band Data（VBD; 音声帯域データ）とも呼ばれており、シスコではモデム パススルーと FAX パススルーの 2 種類のパススルーを提供しています。

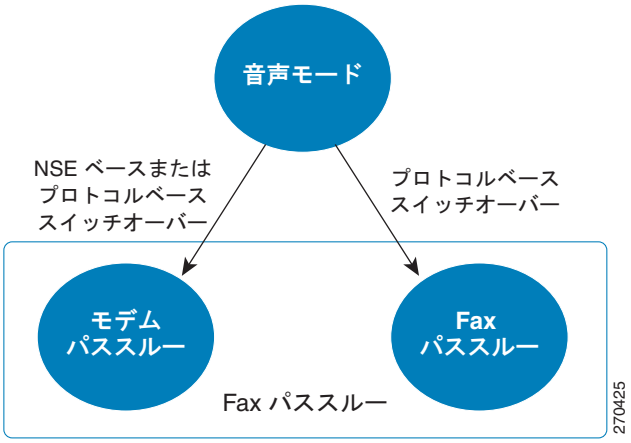
モデム パススルーは、シスコ独自の Named Signaling Event（NSE）パケットを使用して、音声モードのコールをパススルー モードに切り替えます。この音声モードからパススルーへの切り替えは、パススルーだけでなくリレーにとっても重要な概念です。Cisco 音声ゲートウェイ上のコールはすべて音声コールとして開始され、そのコールが真に FAX コールであるとゲートウェイで認識された場合にだけ、モードが適切に切り替えられます。モデム パススルーはモードの切り替えに NSE パケットを使用しますが、他の FAX およびモデム転送方法では異なるメカニズムが実装されている場合があります。

その名前にかかわらず、モデム パススルーは FAX コールにも広く使用されます。モデム パススルーは NSE ベースのパススルーとも呼ばれ、Cisco IOS Command Line Interface（CLI; コマンドライン インターフェイス）で **modem passthrough** コマンドを使用してアクティブにできます。

FAX パススルーは、基になる呼制御プロトコルに従って音声モードのコールをパススルーに切り替えるため、プロトコルベースのパススルーとも呼ばれます。FAX パススルーが対応している呼制御プロトコルは、H.323 と SIP だけです。FAX パススルーはモードの切り替えに呼制御プロトコルを利用するため、サードパーティ製デバイスを含む環境にパススルーを実装する場合は、FAX パススルーを選択する必要があります。

図 4-3 は、Cisco 音声ゲートウェイで FAX コールに使用される 2 種類のパススルー実装を示しています。

図 4-3　シスコの FAX コール用のパススルー実装

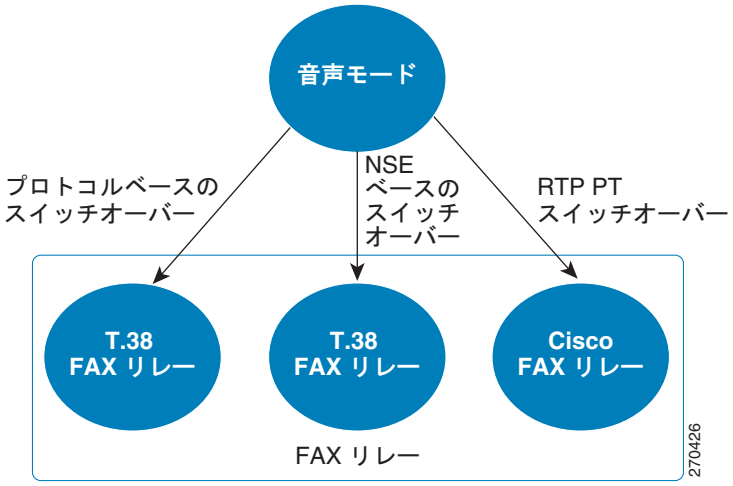


リレーは IP 上で FAX を送信するもう 1 つの主要な方法で、その実装はパススルーに比べて少し複雑です。リレーは、復調と呼ばれるプロセスによって FAX 信号からアナログ搬送波を取り除き、FAX HDLC データ フレームを復元します。続いて、これらの HDLC フレームから関連情報を取り出して FAX リレー プロトコルに効率的にパッケージ化し、相手側のゲートウェイに転送します。相手側で受信されると、FAX 情報がリレー プロトコルから取り出されて FAX HDLC フレームに再構築され、アナログ搬送波に変調されて FAX マシンに送信されます。

シスコは、T.38 と Cisco FAX リレーの 2 種類の FAX リレーをサポートしています。ITU 標準の T.38 を使用すると、T.38 仕様をサポートしているサードパーティ製デバイスと Cisco ゲートウェイを相互運用できます。ほとんどの場合、T.38 FAX リレーは呼制御プロトコルを使用して音声モードを T.38 FAX リレー モードに切り替えます（これをプロトコルベースの T.38 FAX リレーと呼びます）。ただし、シスコ独自の NSE を使用してモード切り替えを行うように T.38 FAX リレーを設定することもできます（これを NSE ベースの T.38 FAX リレーと呼びます）。サードパーティ製デバイスとの相互運用性を確保するためには、プロトコルベースの T.38 を使用する必要があります。

Cisco FAX リレーは標準化前の実装で、Cisco 音声ゲートウェイに固有の機能です。これは、ほとんどすべての Cisco 音声ゲートウェイのデフォルトの FAX 転送設定でもあります。T.38 FAX リレーおよびパススルーで使用される NSE ベースまたはプロトコルベースの方法とは異なり、Cisco FAX リレーは、特定の RTP ダイナミック Payload Types（PT; ペイロード タイプ）を利用して音声モードからリレー モードに移行します。図 4-4 に、シスコの FAX リレー方式を示します。

図 4-4　シスコの FAX コール用のリレー実装



FAX トラフィックの転送に推奨される方法は、FAX リレー モード（もっと具体的に言うと T.38）です。ただし、T.38 FAX リレーがサポートされていない場合は、代わりに Cisco FAX リレーまたはパススルーを使用できます。

ベスト プラクティス

Cisco 音声ゲートウェイで FAX サポートを最大限に実装するには、次の推奨事項とガイドラインが役立ちます。

- QoS を使用する場合は、できる限り、次のパラメータが最小になる方法を採用してください。
  - パケット損失
  - 遅延
  - 遅延変動（ジッタ）

  FAX 転送はパケット損失を非常に受けやすくなっています。パケット損失はわずかであっても FAX 障害を引き起こす可能性があります。ネットワークでパケット損失が問題となっている場合は、T.38 FAX リレーの冗長性機能を使用してください。また、ネットワーク上の恒常的なパケット遅延が 1 秒を超えないこと、および遅延変動（ジッタ）が 300 ミリ秒を超えないことを確認してください。Cisco Unified Communications ネットワークにおける QoS の実装についての詳細は、次の Web サイトにある『*Enterprise QoS Solution Reference Network Design Guide*』を参照してください。

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

- FAX コールの完全性を確保するには、次のヒントが役立ちます。
  - Call Admission Control（CAC; コール アドミッション制御）を使用して、コールが規定の合計帯域幅限界を超えると、拒否されるようにします。
  - モデムと FAX のすべての専用ポートで、コール ウェイティングを使用不可にします。
- T.38 FAX リレーは、ネットワークの考慮事項に基づいて最良の FAX パフォーマンスを実現するよう設計されており、FAX トラフィックの転送方法として最も推奨されます。

  他社の T.38 製品との相互運用性を確保する場合は、プロトコルベースの T.38 を使用します。

  特定の Cisco 音声ゲートウェイ（Cisco VG248 やいずれかの Cisco IOS SCCP ゲートウェイなど）と通信する場合は、NSE ベースの T.38 を使用する必要があります。

Unified CM のシナリオで、さまざまなコール シグナリング プロトコルを実行しているゲートウェイ間に T.38 を導入する場合は、プロトコルベースの T.38 が第一候補です。Cisco Unified CM Release 6.0 から、Unified CM は呼制御プロトコルとして H.323、SIP、および MGCP を使用したプロトコルベースの T.38 をサポートしています。インストールされている Cisco Unified CM のバージョンでプロトコルベースの T.38 がサポートされていない場合、または SCCP ゲートウェイが関係している場合は、NSE ベースの T.38 を使用します。ご使用のバージョンの Unified CM でプロトコルベースの T.38 がサポートされているかどうかを確認するには、次の Web サイトにある Cisco Unified Communications Manager のリリース ノートを参照してください。

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

- T.38 FAX リレーは、現行のほとんどの Cisco 音声ゲートウェイ（特に Cisco IOS を実行しているもの）でサポートされています。この例外として注意が必要なのは、Cisco Analog Telephone Adaptor（ATA）と、Cisco 6608、6624、DT-24/DE-30+ などのレガシー製品です。

  ほとんどの Cisco 音声ゲートウェイは Cisco FAX リレーをサポートしており、これがデフォルトの FAX 転送方法になっています。Cisco FAX リレーのサポートに関する例外として注意が必要なのは、Nextport DSP カードが装着された Cisco AS5350 および AS5400、Cisco ATA、および Cisco DT-24/DE-30+ です。もう 1 つの例外として、PVDM3 DSP 搭載の Cisco 2900 および 3900 シリーズ ゲートウェイは Cisco FAX リレーをサポートしません。

  Unnumbered Datagram Protocol Transport Layer（UDPTL）ヘッダーを使用する T.38 FAX リレーとは異なり、Cisco FAX リレーは標準の RTP ヘッダーを利用します。そのため、Cisco FAX リレーでは Secure Real-Time Transport Protocol（SRTP）を使用して FAX トランザクションのセキュリティを確保できます。

  モデム パススルーは、Cisco ATA やほとんどのレガシー音声ゲートウェイを含む現行のすべての Cisco 音声ゲートウェイでサポートされています。

  モデム パススルーはシスコ独自の NSE に基づいてモードを切り替えるため、他社の機器とは互換性がありません。ただし、パススルー ソリューションが必要な場合は、プロトコルに基づいてモード切り替えを行う FAX パススルーを使用すれば、ほとんどのサードパーティ製デバイスと相互運用できます。

  FAX パススルーは、H.323 および SIP プロトコルを使用する Cisco IOS 音声ゲートウェイだけでサポートされています。

- 大部分の FAX マシンは、現在の速度をスロー ダウンすることなく、0.4% ～ 0.6% の範囲内のパケット ドロップを受け入れるようです。しかし、0.8% ～ 1% の範囲内のパケット ドロップがあるネットワークでは、Error Correction Mode（ECM; エラー訂正モード）を無効にする必要があります。
- 複数の FAX マシンで ECM を無効にするのを検討する前に、ゲートウェイ自体で ECM を無効にすることができます。しかし、パケット ドロップが発生する場合、FAX のイメージ品質が低下する恐れがあります。したがって、ECM を無効にするときには、コールの所要時間が長くなったりコールがドロップする代わりに、イメージ品質を損なってもよいかどうかを十分に検討してください。また、パケットがドロップする原因を突き止めて、解決するために、ネットワークを監視し、評価することも必要です。

スーパー G3 FAX のサポート

Cisco IOS Release 12.4.4T が搭載された Cisco IOS ゲートウェイは、Super-Group 3（SG3; スーパー G3）FAX をサポートしています。ただし、ネゴシエートされるのは G3 速度だけです。Cisco IOS Release 15.0.1M 以降、SG3 FAX はネイティブにサポートされています。この機能の詳細については、次の Web サイトにある「*Fax Relay Support for SG3 Fax Machines at G3 Speeds*」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/sg3spoof.html

SG3 高速 FAX を本来の速度で送信する場合は、モデム パススルーを使用する必要があります。

ゲートウェイでのモデム パススルーとモデム リレーのサポート

一般に、音声ゲートウェイを使用して IP ネットワーク上のモデム セッションをサポートするには、次の 3 通りのメカニズムがあります。

- モデム パススルー
- Cisco モデム リレー
- セキュア モデム リレー（STE エンドポイント間の安全な通信）

これらの各メカニズムはいずれもモデム コールを転送できますが、リレー方式は特定のモデム変調方式だけがサポートされているという点で限定的です。それに対してモデム パススルーは、どのような変調方式でも処理できます。

IP ネットワーク経由でのモデム信号の転送を取り扱う際は、ゲートウェイで発生するモードの切り替えについて理解しておくことが重要です。Cisco ゲートウェイ上のコールはすべて、最初は音声コールとして開始されます。モデム間のコールであっても、まず音声コールとしてセットアップされます。続いて、そのコールが真にモデム コールであるとゲートウェイで認識されると、モードの切り替えが発生して、音声コール モードからモデム パススルー モードまたはモデム リレー モードに切り替わります。音声モードからモデム パススルーまたはモデム リレーへのコールの切り替え方法には、いくつかの種類があります。

「ゲートウェイでの FAX パススルーと FAX リレーのサポート」（P.4-27）の項ですでに説明したように、モデム パススルーは、シスコ独自の NSE パケットを使用して音声コールをパススルー モードに切り替えます。モデム信号が検出されると、ゲートウェイはこれらの NSE メッセージを使用して、これからモデム コールを送信することを互いに通知します。続いて、モデム信号の転送を適切に処理できるように調整を行います。たとえば、音声コーデックの G.711 へのアップスピード、VAD の無効化、エコー キャンセラの無効化などの調整が必要に応じて行われます。モデム パススルーは G.711 コーデックを使用してアナログ モデム信号を単純にサンプリングするため、どのようなモデム変調方式でも処理できますが、常に最高の速度になるとは限りません。

Cisco モデム リレーはシスコ独自の実装で、V.34 モデム コールを IP ネットワーク経由で効率的に転送します。V.90 コールもサポートされますが、V.34 の速度に強制的に減速されます。モデム パススルーと同様に、NSE パケットを使用して、音声モードから Cisco モデム リレーへの切り替えが処理されます。

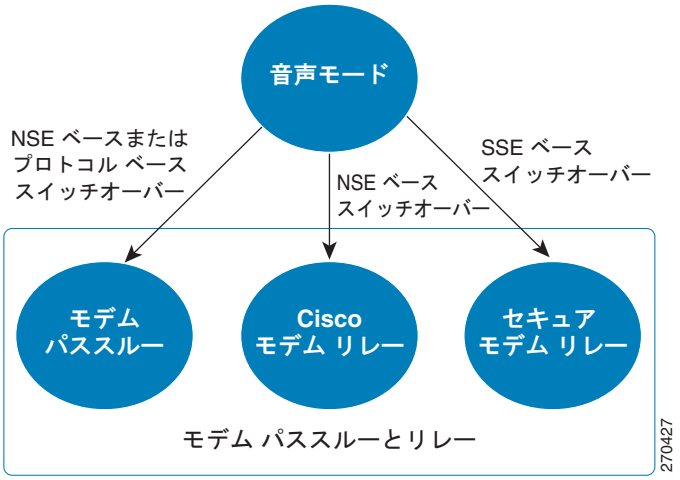
セキュア モデム リレー（「STE エンドポイント間の安全な通信」ともいいます）は、電話コールを IP インフラストラクチャ上で安全に転送できるよう設計されています。Secure Terminal Equipment（STE）と呼ばれる特殊なデバイスにより、V.32 変調を使用して暗号化された音声が伝送されます。セキュア モデム リレーは、SCCP および MGCP ゲートウェイが配置された Unified CM 環境において、STE 間の情報の転送を処理できるようになっています。セキュア モデム リレーは Cisco モデム リレーと互換性がありません。その主な理由の 1 つは、セキュア モデム リレーではモードの切り替えに NSE ではなく V.150.1 ベースの State Signaling Event（SSE）メッセージが使用されることです。

セキュア モデム リレーは STE 信号を転送するために特別に設計されたもので、政府機関または国防関連の配置以外ではほとんど使用されていません。ほとんどの場合、モデム コールの転送には Cisco モデム リレーまたはモデム パススルーを使用します。セキュア モデム リレーの詳細については、次の Web サイトにある「*Secure Communication Between IP-STE Endpoint and Line-Side STE Endpoint*」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/htv1501.html

図 4-5 に、シスコのモデム転送の実装をまとめた図を示します。モデム リレーはモデム パススルーに比べて帯域幅効率が高く、ネットワークの耐障害性にも優れているため、可能な場合は常にモデム リレーを使用してください。モデム リレーの欠点は、サポートされている変調方式がきわめて限定されていることです。それに対してモデム パススルーは、どのようなモデム変調方式でも処理できます。

図 4-5　シスコのモデム コール用のパススルー実装とリレー実装



ベスト プラクティス

IP インフラストラクチャを介して転送されるモデム トラフィックの最適なパフォーマンスを確保するには、次の推奨ベスト プラクティスを守ってください。

- IP ネットワークで Quality of Service（QoS）が使用可能になっていること、および LAN、MAN、および WAN 環境で、QoS を提供するためのすべての推奨事項に従っていることを確認します。できる限り、次のパラメータが最小になる方法を採用してください。
  - パケット損失：FAX とモデムのトラフィックには、本質的に損失のない転送が必要です。パケットが 1 つでも損失すると、再送信が行われます。
  - 遅延
  - 遅延変動（ジッタ）

  詳細については、次の Web サイトにある『*Enterprise QoS Solution Reference Network Design Guide*』を参照してください。

  http://www.cisco.com/go/designzone
- CAC を使用して、コールが規定の合計帯域幅限界を超えると、拒否されるようにします。
- 可能な場合は常に、モデム リレーを使用します。変調方式がモデム リレーでサポートされていない場合は、モデム パススルーを使用します。
- IP ネットワークにモデムを接続して、IP ネットワークの問題のトラブルシューティングや診断をしないでください。この場合、IP インフラストラクチャを構成するデバイスのトラブルシューティングに使用されるモデムは、一般電話サービス（POTS）に接続する必要があります。
- Cisco モデム リレーとモデム パススルーでは NSE に基づいてモードが切り替えられるため、異なる呼制御プロトコルを使用しているゲートウェイどうしでも簡単に通信できます。たとえば、Unified CM に接続されている MGCP ゲートウェイと H.323 ゲートウェイは、Cisco モデム リレーまたはモデム パススルーを正常にネゴシエートできます。これは、Unified CM によってすでに設定されている RTP 音声メディア ストリームの中で NSE 切り替えが行われるためです。
- モデムと FAX のすべての専用ポートで、コール ウェイティングを使用不可にします。

V.90 サポート

現在、Cisco 機器は V.34 モデムのみをサポートします。V.90 モデムは既存のハードウェアで機能し、V.34 よりも高速ですが、V.90 の完全なサポートは保証できません。

サポートされるプラットフォームと機能

FAX とモデムの機能をサポートしている Cisco プラットフォームは、次のとおりです。

- Cisco IOS ゲートウェイは次のものをサポートします。
  - モデム パススルー。
  - H.323 および SIP プロトコルに基づく FAX パススルー。
  - T.38 FAX リレー。T.38 の NSE ベースの切り替えとプロトコルベースの切り替えがどちらもサポートされます。ただし、SCCP は例外で、NSE ベースの T.38 FAX リレーだけがサポートされます。
  - Cisco FAX リレー。Nexport DSP カードを使用する Cisco AS5350、AS5400、および AS5850 では Cisco FAX リレーをサポートしていません。PVDM3 DSP を使用する Cisco 2900 および 3900 シリーズも同様です。
  - Cisco モデム リレー。
- IOS 以外の Cisco ゲートウェイは次のものをサポートします。
  - Cisco VG248 は、モデム パススルー、NSE ベースの T.38 FAX リレー、および Cisco FAX リレーをサポートします。
  - Cisco 6608 および 6624 は、モデム パススルーと Cisco FAX リレーだけをサポートします。
  - Cisco ATA は、FAX コールについてだけモデム パススルーをサポートします。ATA でモデム コールに対してモデム パススルーを使用することは、正式にはサポートされていません。

（注）　ここに示した FAX とモデムのサポート情報は、Cisco IOS ゲートウェイについては Cisco IOS Release 12.4(9)T 以降、Cisco VG248 Analog Phone Gateway については Release 1.3.1 以降で有効です。

プラットフォーム プロトコルのサポート

企業ソリューションで現在使用されている一般的な呼制御プロトコルには、H.323、SIP、MGCP、および Skinny Client Control Protocol（SCCP）があります。すべての Cisco 音声プラットフォームが、これらのプロトコル、または FAX とモデム機能をすべてサポートしているわけではないので、相互運用性の問題が発生します。また、Cisco 2800 シリーズや Cisco 3800 シリーズなどの Cisco IOS ゲートウェイを、VG248 などの IOS 以外のゲートウェイと組み合せる場合は、さらに相互運用性の問題が発生します。ここでは、FAX、モデム、およびプロトコルの機能の相互運用性をサポートしているゲートウェイの組み合せをリストしています。

ネットワークにおける一般的なプロトコルの組み合せ例としては、MGCP と H.323、SCCP と H.323、SCCP と SIP、MGCP と SIP、H.323 と SIP、SCCP と MGCP などがあります。一般的な音声ゲートウェイには、Cisco VG224、VG248、2600XM、2800、3700、3800、および Catalyst 6000 が含まれます。

表 4-12 では、FAX とモデムの相互運用性を現在サポートしている、プロトコルの組み合せをリストしています。

表 4-12　FAX とモデムの機能がサポートされる呼制御プロトコルの各種組み合せ

プロトコルの組み合せ	モデム リレー	モデム パススルー[1]	T.38 FAX リレー	Cisco FAX リレー	FAX パススルー
MGCP を使用する Unified CM と、H.323 または SIP を使用する Unified CM との組み合せ	あり	あり	あり[2]	あり	あり
MGCP を使用する Unified CM と、MGCP を使用する Unified CM との組み合せ	あり	あり	あり[2]	あり	あり
SCCP と、H.323 または SIP を使用する Unified CM との組み合せ	あり	あり	あり[3]	あり	あり
SCCP と、MGCP を使用する Unified CM との組み合せ	あり	あり	あり[3]	あり	あり
H.323 を使用する Unified CM と、H.323 または SIP との組み合せ	あり	あり	あり[2]	あり	あり
SIP を使用する Unified CM と、H.323 または SIP との組み合せ	あり	あり	あり[2]	あり	あり

1. モデム パススルーは、モデム パススルー コールと FAX パススルー コールの両方で機能します。
2. NSE ベースの T.38 FAX リレーは機能しますが、プロトコルベースの T.38 FAX リレーが機能するかどうかは Unified CM のバージョンによります。バージョン情報については、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html にある Cisco Unified Communications Manager のリリース ノートを参照してください。
3. SCCP プロトコルは、NSE ベースの T.38 FAX リレーだけで機能します。

（注）　表 4-12 は一般的な情報を示したものです。製品によっては、この表に記載されていない制限がある場合がありますので、注意してください。たとえば、Cisco ATA は H.323、SIP、および SCCP の呼制御プロトコルをサポートしていますが、どの呼制御プロトコルが使用されているかにかかわらず、モデム パススルーだけがサポートされます。

ゲートウェイ設定例

ここでは、Cisco ゲートウェイでの FAX とモデムのサポートに関する設定の概要を示します。もっと詳細な設定情報については、『Cisco IOS Fax and Modem Services over IP Application Guide』を参照してください。このマニュアルは、適切なログイン認証を持つシスコの従業員またはパートナーが次の Web サイトから入手できます。

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_configuration_guide_book09186a0080762024.html

Cisco FAX リレーは、それがサポートされているすべての音声ゲートウェイにおいて、デフォルトで有効になっています。これは明示的に無効にする必要があります。そうしなければ、音声ゲートウェイで検出されたすべての FAX コールについて転送が試行されます。Cisco IOS ゲートウェイで FAX コールの転送にモデム パススルーなどの機能を使用する場合は、dial-peer で **fax protocol none** を設定するか、**voice service voip** で同コマンドをグローバルに設定することにより、Cisco FAX リレーを無効にできます。ただし、Cisco FAX リレーを有効のままにして FAX コールを Cisco FAX リレーで処理し、高速モデム コールと SG3 FAX コールについてはモデム パススルーで処理されるように設定するのが最も良いケースもよくあります。

Cisco IOS ゲートウェイでのモデム パススルーの設定

モデム パススルーは、次の例に示すように、H.323 ゲートウェイと MGCP ゲートウェイで有効にできます。SIP ゲートウェイでは、H.323 の例と同じコマンドを使用します。また、H.323 および SIP 音声ゲートウェイでは、**voice service voip** ですべてのダイヤル ピアに対してグローバルにモデム パススルーを有効にできます。

H.323

```
!
! Cisco fax relay is ON by default
!(except for 5350/5400, where Cisco fax relay is not supported)
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
!
!
```

MGCP

```
!
ccm-manager mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
mgcp modem passthrough voip mode nse
mgcp fax t38 inhibit
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
```

Cisco VG248 でのモデム パススルーの設定

Cisco VG248 も Cisco FAX リレーとモデム パススルーをサポートしており、Cisco FAX リレーはデフォルトで有効になっています。Cisco FAX リレーは、VG248 の電話設定の Port specific parameters セクションから有効または無効にできます。

VG248 でモデム パススルーを設定するときは、2 つの重要なパラメータを設定する必要があります。1 つ目は、Port specific parameters で **Passthrough mode** を **default: automatic** に設定します。2 つ目は、Telephony Advanced settings で **Passthrough signalling** を **IOS mode** に設定します（次を参照）。

```
  ------------------------------------------------------
  |               Cisco VG248 (VGC10d8002407)          |
  ----- ------------------------------------------------
       | Advanced settings                              |
       |------------------------------------------------|
       | Allow last good configuration (enabled)        |
       | SRST policy                   (disabled)       |
       | SRST provider                 ()               |
       | Call preservation             (enabled: no timeout) |
       | Media receive timeout         (disabled)       |
       | Busy out off hook ports       (disabled)       |
       | DTMF tone dur ------------------------  100ms)  |
       | Echo cancelli| Passthrough signalling |e: use DSP)  |
       | Passthrough s|------------------------|)        |
       | Hook flash ti| legacy                 | default>)   |
```

```
      | Hook flash re| IOS mode                |             |
      | Fax relay max ------------------------  14400 bps)  |
      | Fax relay playout delay       (default: 300)        |
       ------------------------------------------------------
         ---------------------------------------------

 ------------------------------------------------------------
 |                Cisco VG248 (VGC10d8002407)               |
 ----- -------------------------------------------------------
      | Advanced settings                                    |
      |------------------------------------------------------|
      | Allow last good configuration (enabled)              |
      | SRST policy                   (disabled)             |
      | SRST provider                 ()                     |
      | Call preservation             (enabled: no timeout)  |
      | Media receive timeout         (disabled)             |
      | Busy out off hook ports       (disabled)             |
      | DTMF tone duration            (default: 100ms)       |
      | Echo cancelling policy        (alternate: use DSP)   |
      | Passthrough signalling        (IOS mode)             |
      | Hook flash timer              (<country default>)    |
      | Hook flash reject period      (none)                 |
      | Fax relay maximum speed       (default: 14400 bps)   |
      | Fax relay playout delay       (default: 300)         |
       ------------------------------------------------------
        ----------------------------------------------------
```

FAX とモデム パススルー用のクロック ソーシング

FAX とモデム パススルーを正常に送信するには、クロック信号が重要な役割を果たします。ゲートウェイのクロックは、Stratum クロッキングが提供される公衆網クロックと同期させる必要があります。このクロック同期がないと、FAX およびモデム通信は機能しません。クロックを正しく同期させるには、Cisco IOS ゲートウェイの T1 コントローラに対して次の設定を入力します（この例では、T1 コントローラは、公衆網に接続している音声ゲートウェイです）。

```
!
controller T1 0
 framing esf
 linecode b8zs
 clock source line
 channel-group 1 timeslots 1-24 speed 64
 !
```

また、公衆網に接続している他のすべてのインターフェイスでも、この設定を入力してください。

T.38 FAX リレー

T.38 FAX リレーは、Cisco ATA 188、6608、および 6624 ゲートウェイではサポートされていませんが、Cisco IOS 音声プラットフォームと VG248 ではサポートされています。

T.38 FAX リレーは、次の方法で設定できます。

- 「NSE ベースの T.38 FAX リレー」（P.4-37）
- 「プロトコルベースの T.38 FAX リレー」（P.4-38）

NSE ベースの T.38 FAX リレー

H.323 および SIP に対する NSE ベースの T.38 FAX リレーは、Cisco IOS ゲートウェイで dial-peer レベルで設定するか、**voice service voip** でグローバルに設定します。次の例は H.323 の dial-peer 設定例ですが、同じコマンド構文を SIP ダイヤル ピアにも適用できます。

H.323

```
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
 fax protocol t38 nse
!
!
```

MGCP

Cisco IOS MGCP ゲートウェイでは通常、NSE ベースの T.38 FAX リレーのことを「*ゲートウェイによって制御される* T.38 モード」と呼びます。これは、ゲートウェイが NSE メッセージを通じて T.38 の切り替えを制御するためです。ゲートウェイによって制御される T.38 FAX リレーは、コマンド **no mgcp fax t38 inhibit** を使用して有効にします。

```
!
ccm-manage mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
mgcp modem passthrough voip mode nse
no mgcp fax t38 inhibit
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
!
```

SCCP ゲートウェイ（Cisco IOS ゲートウェイまたは VG248）では、NSE ベースの T.38 FAX リレーを使用する必要があります。Cisco IOS SCCP ゲートウェイで NSE ベースの T.38 FAX リレーを有効にするには、**voice service voip** でコマンド **fax protocol t38 nse** を設定します。

ゲートウェイで使用されている呼制御プロトコルが異なる場合は、NSE 切り替えを「強制」する必要があります。同じ呼制御プロトコルを使用しているゲートウェイは、コール セットアップ中に、NSE ベースの T.38 FAX リレーがサポートされていることを互いに通知します。異なる呼制御プロトコルが使用されている場合（たとえば、一方のゲートウェイが H.323 を使用していて、他方が MGCP を使用している場合など）は、このような NSE ベースの T.38 FAX リレーの確認情報はゲートウェイ間で渡されません。そのため、NSE ベースの T.38 のサポート通知を受け取らなかった場合でも、NSE ネゴシエーションを強制的に行うようにゲートウェイをプログラムする必要があります。H.323 および SIP 音声ゲートウェイでは、これは単に既存の t38 コンフィギュレーション コマンドに **force** オプションを付ける（**fax protocol t38 nse force**）だけで済みます。MGCP では、コマンド **mgcp fax t38 gateway force** を使用します。

プロトコルベースの T.38 FAX リレー

プロトコルベースの T.38 FAX リレーでは、音声モードから T.38 への切り替えは呼制御プロトコル内で行われます。プロトコルベースの T.38 FAX リレーでサポートされている呼制御プロトコルは、H.323、SIP、および MGCP です。H.323 および SIP では、プロトコルベースの T.38 はダイヤル ピア レベルまたは **voice service voip** でグローバルに設定できます。コマンド構文は、**nse** キーワードを省略する点以外は NSE ベースの T.38 FAX リレーと同じです。

NSE ベースの T.38 FAX リレーと、H.323 および SIP 呼制御プロトコルを使用したプロトコルベースの T.38 FAX リレーでは、追加のフォールバック オプションも指定できます。このオプションを使用すると、ゲートウェイ間で初回の FAX 転送方式のネゴシエーションが失敗した場合に、別の切り替え方法、または完全に異なる転送方式を試すことができます。次の例では、H.323 ダイヤル ピアに対してプロトコルベースの T.38 FAX リレーをフォールバック オプション付きで設定しています。コマンド構文は、SIP ダイヤル ピア、および **voice service voip** によるグローバル設定の場合でも同じです。

H.323

```
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
!
! To enable T.38 fax relay and fall back to Cisco fax relay when
! T.38 fax negotiation fails. This is the default case.
 fax protocol t38 fallback cisco
!
dial-peer voice 1001 voip
 destination-pattern 2T
 session target ipv4:10.10.10.2
 modem passthrough mode nse codec g711ulaw
!
! To enable T.38 fax relay and fall back to fax passthrough when
! T.38 fax negotiation fails.
fax protocol t38 nse fallback pass-through
!
dial-peer voice 1002 voip
 destination-pattern 3T
 session target ipv4:10.10.10.3
 modem passthrough mode nse codec g711ulaw
!
! This CLI is needed when talking to MGCP endpoint where CA/GK
! doesn't support T.38 fax relay such as CCM.
 fax protocol t38 nse force fallback none
!
!
```

MGCP

MGCP 音声ゲートウェイでは、プロトコルベースの T.38 FAX リレーのことを一般に「CA によって制御される T.38 モード」と呼びます。これは、Call Agent（CA; コール エージェント）が T.38 FAX リレーの切り替えを処理するためです。次の例に示すように、MGCP に対して T.38 FAX リレーが有効になっていて、2 つの **fxr-package** コマンドも一緒に設定されていることを確認する必要があります。

```
!
ccm-manage mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
mgcp modem passthrough voip mode nse
no mgcp fax t38 inhibit
mgcp package-capability fxr-package
```

```
mgcp default-package fxr-package
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
!
```

プロトコルベースの T.38 FAX リレーには Unified CM が直接関与するため、ご使用の Unified CM のバージョンがゲートウェイの呼制御プロトコル内で T.38 FAX リレーをサポートしている必要があります。ご使用の Cisco Unified CM のバージョンが特定の呼制御プロトコルで T.38 FAX リレーをサポートしているかどうかを確認するには、次の Web サイトにある Cisco Unified Communications Manager のリリース ノートを参照してください。

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

Cisco 6608 または 6624 音声ゲートウェイと、T.38 FAX リレーをサポートするその他の Cisco 音声ゲートウェイを同時に使用するトポロジでは、次の Cisco IOS コマンドを使用してください。

```
fax protocol t38 [nse [force]] fallback [cisco | none]
modem passthrough nse codec {g711ulaw|g711alaw}
```

Cisco IOS ゲートウェイでこれら 2 つのコマンドを使用すると、Cisco 6608 および 6624 ゲートウェイとの相互運用によって Cisco FAX リレーとモデム パススルーを実行し、さらにその他の Cisco IOS ゲートウェイとの相互運用によって T.38 FAX リレーとモデム パススルーを実行できます。

ビデオ テレフォニー用のゲートウェイ

ビデオゲートウェイは、IP テレフォニーネットワークまたは公衆網へのビデオコールを終端します。音声コールおよびビデオ コールに別個のゲートウェイを配置するか、音声コールとビデオ コールの両方をルーティングする統合ゲートウェイを配置することができます。

シスコでは、音声ゲートウェイ機能を、スタンドアロン デバイス、Cisco IOS ルータに組み込むモジュール、Cisco Catalyst イーサネット スイッチに組み込むライン カードなど、さまざまな形で提供しています。これらのゲートウェイは、複数の VoIP プロトコル（H.323、MGCP、SIP、SCCP など）、複数のポート インターフェイス タイプ（FXS、FXO、E&M、T1/E1-CAS、T1/E1-PRI、ISDN BRI など）、および無数の最新 VoIP 機能をサポートしています。また、これらのゲートウェイでは、管理用およびトラブルシューティング用のインターフェイス セットを豊富に使用できます。Cisco IOS ルータは、H.320 ゲートウェイの機能もサポートしており、音声とビデオの統合ゲートウェイとして使用できます。

ビデオを追加することで既存の音声インフラストラクチャを活かした配置にするには、Cisco Unified Videoconferencing 3500 シリーズのポートフォリオからシスコのビデオ対応ゲートウェイ ファミリを使用します。

Unified Videoconferencing ゲートウェイはビデオ コール用として優れていますが、シスコ音声ゲートウェイが提供するすべての機能をサポートしているわけではありません。Unified Videoconferencing ゲートウェイには、次の特性があります。

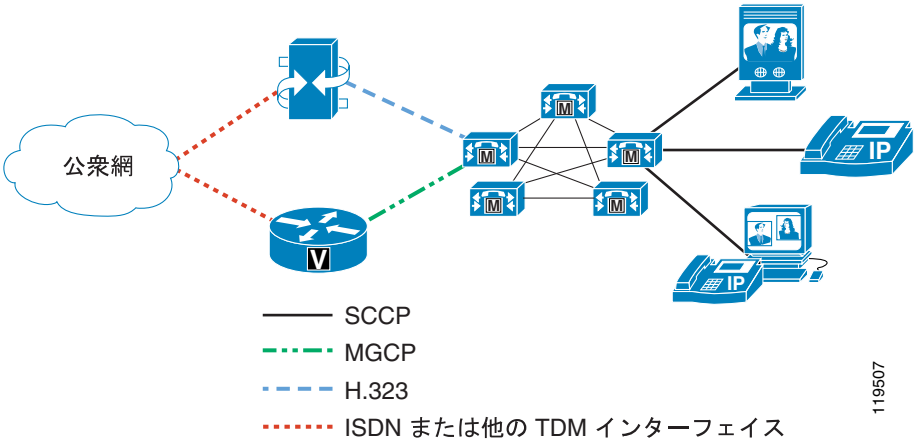
- H.323 と H.320 のみをサポートします。
- スタンドアロン デバイスです。Cisco IOS ルータまたは Cisco Catalyst スイッチに統合することはできません。
- T1/E1-PRI および ISDN BRI のみサポートします。
- G.711、G.722、G.722.1、G.723.1、および G.728 のみ をサポートし、G.729 オーディオはサポートしません。
- H.245 Empty Capabilities Set（ECS）をサポートします。

- Cisco 音声ゲートウェイに固有の、多数の管理機能とトラブルシューティング機能をサポートしません。

このように製品間の違いがあるため、Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイは、Cisco 音声ゲートウェイの代わりとしては推奨できません。IP テレフォニーのユーザが通信環境にビデオを追加するには、両方のタイプのゲートウェイを配置して、すべての音声コールに Cisco 音声ゲートウェイを使用し、Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイをビデオ コールのみに使用する必要があります。また、配置する Cisco IOS ゲートウェイのモデルによっては、公衆網サービス プロバイダーから音声とビデオに別個の回線を調達する必要がある場合もあります。

音声ゲートウェイとビデオ ゲートウェイを別々にする場合は（図 4-6 を参照）、着信コールと発信コールの両方に対するルート プランも別々にする必要があります。着信コールの場合、Direct Inward Dial（DID; ダイヤルイン）内線を 1 つしか持たないユーザが音声コールとビデオ コールの両方を受信することはできません。通常、各ユーザは、あらかじめ音声コール用の DID を持っています。そのシナリオにビデオを導入する場合は、何か別の方法でユーザにダイヤルする必要があります。たとえば、第 2 の DID 番号を使用する方法や、ビデオ ゲートウェイのメイン番号にダイヤルし、音声自動応答装置（IVR）から促されてユーザのビデオ内線に入るなどの方法があります。発信コールの場合は、単一の公衆網アクセス コードを音声コールとビデオ コールの両方に使用することができません。通常、ユーザはすでに音声用の既知のアクセス コード（多くの米国企業における 9 など）を持っていますが、そのシナリオにビデオを導入した場合、ビデオ コールを発信するユーザは何か別のアクセス コードをダイヤルする必要があります。

図 4-6　音声と IP ビデオ テレフォニーに別々の公衆網回線を使用する Unified CM システム



2 つのタイプのゲートウェイを導入するための、もう 1 つの考慮事項は、それらのゲートウェイの配置です。通常、企業は多数の公衆網ゲートウェイ リソースを中央サイト（複数の場合もある）に集約し、それぞれの支店も、いくつかのローカル ゲートウェイ リソースを持っています。たとえば、Cisco Catalyst 6500 ゲートウェイを中央サイトに配置し、そのゲートウェイに複数の T1/E1 回線を接続する一方で、各支店に Cisco Integrated Services Router（ISR）と、ローカル CO へのアナログまたはデジタルのトランクが配備されている場合があります。このシナリオにビデオを導入するユーザは、ビデオに必要な公衆網回線の数と、ビデオ ゲートウェイの配置場所も決定する必要があります。たとえば、少数の IP/VC 3500 シリーズ ゲートウェイのみを中央サイトに配置するのか、それとも各支店にもゲートウェイを配置するのか、といったことです。

最後に、トール バイパスを設けるためには IP ネットワーク内でコールをどのようにリモート ゲートウェイへルーティングするのか、および IP ネットワークが使用不能になったり、コールを完了できるだけの帯域幅がない場合に、公衆網上でコールをどのように再ルーティングするのかを考慮してください。具体的には、ビデオ コール用の自動代替ルーティング（AAR）を起動するのか、といったことです。

公衆網からの着信コールのルーティング

公衆網からの着信コールをルーティングするには、次のいずれかの方法を使用します。

- Unified CM クラスタ内にあるビデオ対応デバイスごとに、少なくとも 2 つの異なる電話番号を割り当て、1 つの回線を音声用、もう 1 つをビデオ用とします。この方法では、外部の（公衆網）発信者はビデオを有効にするために、正しい番号をダイヤルする必要があります。
- ビデオ コールの場合は、外部の発信者にビデオ ゲートウェイのメイン番号をダイヤルしてもらいます。Cisco Unified Videoconferencing ゲートウェイは統合 IVR を提供し、発信者に相手側の内線番号の入力を求めます。次に、Unified CM は、それがビデオ コールであることを認識し、宛先デバイスを呼び出します。この方法では、発信者はそれぞれの着信側ごとに 2 つの異なる DID 番号を覚える必要はありませんが、着信ビデオ コールをダイヤルするという余分な手順が増えます。

（注） 外部のビデオ エンドポイントは、IVR プロンプトに着信側の内線番号を入力するために、DTMF をサポートしている必要があります。

次の例は、2 番目の方法を示しています。

ユーザの Cisco Unified IP Phone 7960 は、Cisco Unified Video Advantage を実行している PC に接続されています。IP Phone の内線番号は 51212 で、完全修飾 DID 番号は 1-408-555-1212 です。DID 番号をダイヤルするだけで、音声専用コールの公衆網からそのユーザに到達できます。CO は、Cisco 音声ゲートウェイに接続した T1-PRI 回線（複数の場合もある）を通じて、その DID 番号にコールを送信します。ゲートウェイでコールが受信されると、Unified CM はゲートウェイが音声専用であることを認識し、そのコール用に 1 つの音声チャネルのみのネゴシエーションを行います。逆に、公衆網からビデオ コールのためにそのユーザに到達するには、ビデオ ゲートウェイのメイン番号をダイヤルした後、ユーザの内線番号を入力する必要があります。たとえば、1-408-555-1000 をダイヤルするとします。CO は、Cisco Unified Videoconferencing 3500 シリーズ ビデオ ゲートウェイに接続した T1-PRI 回線（複数の場合もある）を通じて、その番号にコールを送信します。ゲートウェイでコールが受信されると、IVR プロンプトが発信元に、到達すべき相手の内線番号の入力を求めます。発信者が DTMF トーンで内線番号を入力すると、Unified CM はゲートウェイにビデオ機能があることを認識し、そのコール用に音声とビデオの両方のチャネルをネゴシエートします。

ゲートウェイの番号操作

Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイは、公衆網から受信したコールの番号を操作できません。Q.931 Called Party Number フィールドで渡されたものと正確に同じ数の番号を受け取り、それらすべてを Unified CM に送信します。したがって、Unified CM は番号を操作して、宛先デバイスの電話番号（DN）と照合する必要があります。たとえば、CO スイッチからゲートウェイへの回線が 10 桁を渡すように設定されていて、着信側の内線番号が 5 桁しかない場合、Unified CM は、一致する DN を検索する前に、先頭の 5 桁を削除する必要があります。この番号操作は、次のいずれかの方法で実装できます。

- IP/VC ゲートウェイからの着信コールを伝達する H.323 ゲートウェイ デバイスまたは H.225 ゲートキーパー制御トランクの、Significant Digits フィールドを設定します。

  この方法では、Unified CM に、着信番号の下位 N 桁だけに注目するよう指示できます。たとえば、Significant Digits を 5 に設定すると、Unified CM は着信番号の最後の 5 桁以外を無視します。これは最も簡単な方法ですが、そのゲートウェイから受信したすべてのコールに影響を及ぼします。したがって、可変長の内線番号がある場合、この方法は推奨できません。

- トランスフォーメーション パターンを設定し、それを IP/VC ゲートウェイからの着信コールを伝達する H.323 ゲートウェイ デバイスまたは H.225 ゲートキーパー制御トランクのコーリング サーチ スペースに格納します。

  この方法では、Unified CM は受信した完全な桁数でコールを照合し、着信番号を修正してから、得られた変更後の番号に対して番号分析を続行できます。この方法は前の方法に比べてわずかながら複雑ですが、柔軟性があり、コールの照合と修正をきめ細かく行うことができます。

公衆網への発信コールのルーティング

発信コールを公衆網へルーティングするには、次のいずれかの方法を使用します。

- 音声コールとビデオ コールに異なるアクセス コード（異なるルート パターン）を割り当てます。たとえば、ユーザが 9 の後にコール先の公衆網電話番号をダイヤルすると、それがコールを音声ゲートウェイに送るルート パターンと一致します。同様に、数字の 8 を、ビデオ ゲートウェイにコールを渡すルート パターンとして使用することもできます。
- Unified CM クラスタ内にあるビデオ対応デバイスごとに、少なくとも 2 つの異なる電話番号を割り当て、1 つの回線を音声用、もう 1 つをビデオ用とします。その後、2 つの回線に異なるコーリング サーチ スペースを指定します。ユーザが第 1 の回線上でアクセス コード（たとえば 9）をダイヤルすると音声ゲートウェイにつながり、同じアクセス コードを第 2 の回線上でダイヤルするとビデオ ゲートウェイにつながります。この方法では、ユーザが 2 つの異なるアクセス コードを覚える必要がありませんが、コールの発信時に電話機で正しい回線を押す必要があります。

ゲートウェイ サービス プレフィックス

Cisco Unified Videoconferencing ゲートウェイは、発信コールの速度を定義するためにサービス プレフィックスを使用します。ゲートウェイでサービス プレフィックスを設定するときは、次のいずれかの速度を選択する必要があります。

- Voice-only
- 128 kbps
- 256 kbps
- 384 kbps
- 768 kbps
- Auto（動的に決定され、128 kbps ～ 768 kbps の範囲の任意のコール速度をサポート）

（注） 上記の各速度は、64 kbps の倍数を表します。56 kbps のダイヤリング用として、サービス プレフィックスの設定ページには、各チャネルを 56 kbps に制限するチェックボックスがあります。したがって、制限モードを有効にした 128 kbps サービスは 112 kbps サービスになり、制限モードを有効にした 384 kbps サービスは 336 kbps になり、その他も同様です。

IP エンドポイントから公衆網へ向かうコールは、ゲートウェイがそのコールにどのサービスを使用するかを決定できるように、着信番号の先頭にサービス プレフィックスを含んでいる必要があります。オプションとして、番号の先頭にサービス プレフィックスを含んでいないコールに使用する、デフォルト プレフィックスを設定できます。この方法は、非常に複雑になる可能性があります。ユーザは、求めるコール速度を得るためにダイヤルすべきプレフィックスを覚えておく必要があるからです。また、管理者は、Unified CM で複数の（速度ごとに 1 つずつ）ルート パターンを設定する必要があります。ただし、Auto 速度を使用するとその手間を最小にできます。コールの大多数が 1 チャネルあたり 64 kbps（たとえば、128 kbps、384 kbps、512 kbps、768 kbps など）を使用して行われる場合には、Auto サービスを使用できます。その場合、1 チャネルあたり 56 kbps（たとえば、112 kbps、336 kbps など）のコールを行うまれなケースに備えて、1 つだけ別のサービスを作成すれば済みます。

ゲートウェイは、# をダイヤル末尾の文字として認識するので、サービス プレフィックスの中に必ず # 文字を使用することをお勧めします。この文字をサービス プレフィックスに入れておくと、ゲートウェイのメイン番号をダイヤルして IVR に接続してからオフネット番号にダイヤルするといった料金詐欺にゲートウェイが使用されることを防止できます。# は、サービス プレフィックスの先頭（推奨）と末尾どちらでもかまいません。たとえば、ビデオ コールで公衆網に到達するためのアクセス コードが 8 であれば、サービス プレフィックスを #8 または 8# として設定することをお勧めします。あるいは、上記のように 2 つのサービス プレフィックスを使用する場合は、Auto の 64 kbps サービスに #80 を使用し、Auto の 56 kbps サービスに #81 を使用するという方法もあります。

サービス プレフィックスを使用することの欠点は、IP/VC ゲートウェイにコールを送信するときに、Unified CM で着信番号の前にサービス プレフィックスを付加する必要があることです。ユーザに # をダイヤルさせるのはあまり使いやすくないので、ダイヤルされた番号の前に Unified CM が # を付加するように設定することをお勧めします。たとえば、公衆網にビデオ コールをダイヤルするアクセス コードが 8 の場合、Unified CM でルート パターンを 8.@ として設定し、ルート パターン設定の中で、そのルート パターンがダイヤルされたときは必ず前に #8 を付加するように、着信番号変換規則を設定します。あるいは、上記のようにサービス プレフィックスを 2 つ使用する場合は、80.@ を Auto 64 kbps サービス（着信番号の前に # を付ける）に使用し、81.@ を Auto 56 kbps サービス（着信番号の前に # を付ける）に使用するという方法もあります。

自動代替ルーティング（AAR）

IP ネットワークにコールを処理できるだけの帯域幅がない場合、Unified CM はコール アドミッション制御メカニズムを使用して、コールの処理方法を決定します。「IP ビデオ テレフォニー」（P.16-1）の説明のように、Unified CM は設定に従って、次のいずれかの処理を実行します。

- コールに失敗し、発信側に対してビジー トーンを再生し、発信側の画面に Bandwidth Unavailable メッセージを表示します。
- ビデオ コールを音声専用コールとして再試行します。
- 自動代替ルーティング（AAR）を使用し、公衆網ゲートウェイなどの代替パス上でコールを再ルーティングします。

最初の 2 つのオプションについては、「IP ビデオ テレフォニー」（P.16-1）の章に説明があります。ここでは、AAR オプションについて説明します。

音声コールまたはビデオ コールに AAR を使用できるようにするには、発信側デバイスと着信側デバイスを AAR グループのメンバーとして設定し、着信側デバイスに外部電話番号マスクを設定する必要があります。外部電話番号マスクによって、ユーザの内線用の完全修飾 E.164 アドレスが指定されます。また、AAR グループによって、コールが公衆網上で正しくルーティングされるために、着信側デバイスの外部電話番号マスクの前に付加すべき数字が示されます。

たとえば、ユーザ A が San Jose AAR グループに属し、ユーザ B が San Francisco AAR グループに属しているとします。ユーザ B の内線番号は 51212 で、外部電話番号マスクは 6505551212 です。AAR グループは、San Jose と San Francisco の AAR グループ間のコールに対して、番号の前に 91 を付加するよう設定されています。この場合、ユーザ A が 51212 をダイヤルし、2 つのサイト間の IP WAN 上にそのコールを処理できるだけの帯域幅がない場合、Unified CM はユーザ B の外部電話番号マスクである 6505551212 を選択し、その前に 91 を付加して 916505551212 への新規コールを生成し、ユーザ A 用の AAR コーリング サーチ スペースを使用します。

ビデオ コールにも同じロジックが適用されますが、プロセスに 1 つだけ手順が追加されます。ビデオ対応デバイスに対して、Retry Video Call as Audio というフィールドが存在します。「IP ビデオ テレフォニー」（P.16-1）の章で説明するように、このオプションを有効（オン）にした場合、Unified CM は AAR を実行しないで、同じコール（つまり、51212 へのコール）を音声専用コールとして再試行します。このオプションを無効（オフ）にした場合、Unified CM は AAR を実行します。Unified CM のデフォルトでは、すべてのビデオ対応デバイスで Retry Video Call as Audio オプションが有効（オン）

になります。したがって、ビデオ コールで AAR を使用できるようにするには、Retry Video Call as Audio オプションを無効（オフ）にする必要があります。また、ロケーション間で Resource Reservation Protocol（RSVP; リソース予約プロトコル）に基づいたコール アドミッション制御ポリシーが使用されている場合は、RSVP ポリシーを音声ストリームとビデオ ストリームの両方について Mandatory に設定する必要があります。

さらに、Unified CM は、着信側デバイスだけを見て Retry Video Call as Audio オプションが有効か無効かを判断します。したがって、上記のシナリオで AAR プロセスが実行されるためには、ユーザ B の電話機で Retry Video Call as Audio オプションが無効にされている必要があります。

最後に、デバイスは 1 つの AAR グループだけに所属できます。AAR グループによって、どの数字を前に付加するかが決定されるため、再ルーティングされたコールにどのゲートウェイが使用されるかにも影響があります。前項で述べたように、公衆網への発信コール ルーティングの設定に何を選択したかに応じて、AAR によって再ルーティングされるビデオ コールは、ビデオ ゲートウェイでなく音声ゲートウェイに送られる可能性もあります。したがって、AAR グループと AAR コーリング サーチ スペースの構築は入念に行い、必ず正しい数字が付加され、AAR に正しいコーリング サーチ スペースが使用されるようにしてください。

こうした考慮事項により、大規模な企業環境での AAR の設定がかなり複雑になる可能性がありますが、エンドポイントのタイプが 2 つのどちらかに限定されている場合（IP Phone が音声専用コール用で、Tandberg T-1000 などのシステムがビデオ コール専用など）には AAR の実装が容易です。エンドポイントが音声とビデオの両方のコールに対応している場合（Cisco Unified Video Advantage または Cisco IP Video Phone 7985G など）は、AAR の設定が非常に複雑になることがあります。したがって、音声とビデオのエンドポイントが混在する大企業では、ユーザごとに AAR の重要性をよく考え、専用のビデオ会議室や経営幹部用ビデオ システムなど、一部のビデオ デバイスだけに AAR を使用してください。表 4-13 に、さまざまなデバイス タイプで AAR を使用するのが適切なシナリオのリストを示します。

表 4-13　デバイス タイプ別の AAR 使用条件

デバイス タイプ	デバイスを使用したコールの宛先	AAR の必要性	備考
IP Phone	他の IP Phone およびビデオ対応デバイス	あり	ビデオ対応デバイスにコールするときでも、発信元デバイスが音声専用なので、コールを音声ゲートウェイにルーティングするように AAR を設定できます。
Cisco Unified Video Advantage の搭載された IP Phone、または Cisco IP Video Phone 7985G	他のビデオ対応デバイスのみ	あり	デバイスは必ずビデオ コールに使用されるので、AAR グループを設定できます。
	IP Phone およびその他のビデオ対応デバイス	なし	音声専用コールではビデオ コールと異なるルーティングを行うように AAR グループを設定するのは困難です。
Sony 社製または Tandberg 社製の SCCP エンドポイント	他のビデオ対応デバイスのみ	あり	デバイスは必ずビデオ コールに使用されるので、AAR グループを設定できます。
	IP Phone およびその他のビデオ対応デバイス	なし	音声専用コールではビデオ コールと異なるルーティングを行うように AAR グループを設定するのは困難です。
H.323 または SIP クライアント	他のビデオ対応デバイスのみ	あり	デバイスは必ずビデオ コールに使用されるので、AAR グループを設定できます。
	IP Phone およびその他のビデオ対応デバイス	なし	音声専用コールではビデオ コールと異なるルーティングを行うように AAR グループを設定するのは困難です。

最低料金選択機能

Least-Cost Routing（LCR; 最低料金選択機能）と Tail-End Hop-Off（TEHO; テールエンド ホップオフ）は、VoIP ネットワークでは非常によく知られており、ビデオ コールにも利用できます。一般的にどちらの用語も、長距離電話番号へのコールが IP ネットワークを通じて宛先に最も近いゲートウェイにルーティングされ、通話料金が安くなるような、コール ルーティング ルールの設定方法を指しています。Cisco Unified CM Release 4.1 の場合、LCR は基本的に TEHO と同じ意味です。Unified CM は、次に示すような豊富な番号分析機能と番号操作機能を使用して、この機能をサポートします。

- パーティションとコーリング サーチ スペース
- トランスレーション パターン
- ルート パターンとルート フィルタ
- ルート リストとルート グループ

LCR をビデオ コール用に設定するのは、音声コールの場合よりも少し複雑で、その理由は次のとおりです。

- この章ですでに述べたように、ビデオ コールには独自の専用ゲートウェイが必要です。
- ビデオ コールには、音声コールをはるかに上回る帯域幅が必要です。

専用ゲートウェイに関しては、LCR をビデオ コールに使用するかどうかを決めるための基礎となるロジックは、「自動代替ルーティング（AAR）」（P.4-43）の項で説明したロジックとほとんど同じです。音声とビデオ用にさまざまなタイプのゲートウェイが必要になるため、LCR で音声コールを 1 つのゲートウェイに送り、ビデオ コールを別のゲートウェイに送るために必要なすべてのパーティション、コーリング サーチ スペース、トランスフォーメーション パターン、ルート パターン、ルート フィルタ、ルート リスト、およびルート グループを設定するのは、かなり複雑な作業になる可能性があります。

帯域幅の要件に関しては、LCR を使用するかどうかは、特定のロケーションとの間を結ぶビデオ コールの LCR をサポートできるだけの帯域幅が、使用している IP ネットワークにあるかどうかで決まります。現在の帯域幅が十分でない場合は、IP ネットワークをアップグレードしてビデオ コール用の空きを作ったり、ローカル ゲートウェイを導入して公衆網上でコールをルーティングしたりするためのコストと、ビデオ コールの利点を比較する必要があります。たとえば、ある中央サイトに 1.544 Mbps の T1 フレーム リレー回線を介して支店が接続されているとします。その支店内には、20 人のビデオ機能を持つユーザがいます。1.544 Mbps の T1 回線は、最大でほぼ 4 つの 384 kbps ビデオ コールを処理できます。この場合、中央サイトまでビデオ コールをルーティングして、通話料金を節約することに意味があるかどうかが問題です。サポートするコールの数に応じて、1.544 Mbps の T1 回線をもっと高速のものにアップグレードしなければならない場合もあります。ビデオには、そうしたアップグレードに要する毎月の追加料金に見合うだけの重要性があるのでしょうか。もしないのなら、その支店に IP/VC ビデオ ゲートウェイを導入すると、LCR に煩わされずに済みます。しかし、各支店へのローカル IP/VC ゲートウェイの配置も安価には行えないため、最終的には、ビデオから公衆網へのコールがビジネスにとってどれほど重要であるかを判断しなければなりません。ビデオが重要でないなら、帯域幅をアップグレードしたりビデオ ゲートウェイを購入したりするよりも、Retry Video Call as Audio 機能を使用し、使用可能な帯域幅を超過した場合にビデオ コールを音声専用コールとして再ルーティングした方がよいこともあります。コールが音声専用までダウングレードされると、LCR を実行するためのローカル ゲートウェイ リソースと帯域幅は、もっと手ごろな価格で設定しやすいものになります。

ISDN B チャネル バインディング、ロールオーバー、およびビジーアウト

H.320 ビデオ チャネル ボンディング手法には、px64 と p*64（ISO-13871）の 2 種類があります。Cisco ビデオ機器はすべてのコールに対して px64 を使用しますが、Polycom や Tandberg などの他のビデオ機器は 2 チャネル コール（128 kbps のビデオ）に対して px64 を使用し、2 チャネルを超える場合（192 kbps ～ 1 Mbps のビデオなど）には ISO-13871 を使用します。Cisco IOS Release 12.4.20T

では、Cisco IOS H.320 ゲートウェイで ISO-13871 ボンディング手法がサポートされており、これによって最大速度 1 Mbps のビデオ コールがサポートされます。この機能により、Cisco IOS ルータを音声コールとビデオ コールの両方に対応する統合ゲートウェイとして使用できます。

H.320 ビデオは、複数の ISDN チャネルをまとめて使用することで、フルモーション ビデオの受け渡しに必要な速度を実現します。このボンディング メカニズムの問題の 1 つは、着信 ISDN ビデオ コールを受信した時点でゲートウェイにはそのコールに必要なチャネル数がわからず、コールを受け入れて発信元デバイスから必要な追加チャネル数を指示されて、初めてそれがわかることです。その要求を満たせるだけの B チャネルがないと、コールは切断されます。したがって、そのような状況が発生する可能性を最小にするよう、慎重なトラフィック エンジニアリングが必要です。基本的に、次に着信する可能性があるコールを処理できる、十分な B チャネルを常に使用可能にしておく必要があります。

この B チャネルの問題は、次の 2 つのケースで発生します。

- 公衆網から IP ネットワークへの着信コール
- IP ネットワークから公衆網への発信コール

着信コール

着信コールについて、次のシナリオを考えてみます。

> ある会社に Cisco 3526 IP/VC ゲートウェイがあり、それが ISDN PRI 回線でセントラル オフィス（CO）のスイッチに接続されています。この場合、ISDN PRI 回線は 23 の B チャネルを提供します。ビデオ コールが公衆網から 384 kbps で受信されます。このコールは 6 つの B チャネルを使用するので、残りの空きは 17 になります。最初のコールがまだアクティブな間に、第 2 と第 3 の 384 kbps のコールがその回線上で受信されます。それぞれのコールが 6 チャネルを使用するので、残りの空きは 5 チャネルになります。第 4 の 384 kbps のコールが受信されると、ゲートウェイはそのコールに応答しますが、十分な B チャネルの空きがないこと（残りチャネルは 5 つだけだが、コールに必要なチャネルは 6 つ）を認識し、接続を解除します（「16: Normal Call Clearing」を理由とした Q.931 RELEASE COMPLETE を送信）。第 4 のコールを試みた発信側は、コールの失敗の原因がわからず、番号を繰り返しリダイヤルしてコールを発信しようとします。

Cisco Unified Videoconferencing ゲートウェイでは、こうした問題が起きる可能性を最小にするために、ゲートウェイが一定の使用率しきい値（総帯域幅に対するパーセンテージとして設定）に到達したときに、ゲートウェイから CO へ残りの B チャネル（この例では 5 チャネル）をビジーアウトする要求を送信するように設定できます。

さらに、トランク グループ内で CO から複数の ISDN 回線をプロビジョニングできます。最初の回線がビジーアウトしきい値に到達した時点で、コールはグループ内の次の PRI へロールオーバーされます。Cisco 3540 IP/VC ゲートウェイは 2 つの ISDN PRI 接続を提供し、両方のポートにまたがったボンディング チャネルをサポートします。たとえば、ポート 1 の空きが 5 チャネルしかなく、ポート 2 がアイドル状態であるため、23 チャネルが使用可能であるとします。この場合、ポート 1 から 5 チャネル、ポート 2 から 1 チャネルを使用してボンディングすることにより、第 4 の 384 kbps のコールに成功できます。これにより、コントローラ 2 上に残る空きは 22 チャネルとなり、ある時点で着信コールが再びビジーアウトしきい値に到達します。その時点で、ポート 2 上の残りのチャネルはビジーアウトされ、それ以後のすべての着信コールは原因コード「Network Congestion」で拒否されます。
Cisco Unified Videoconferencing ゲートウェイでは、異なるゲートウェイにまたがってチャネルを結合したり、同じ Cisco 3544 シャーシ内にあるさまざまな Cisco 3540 ゲートウェイ モデルにまたがってチャネルを結合したりすることができないため、ボンディングできる最大ポート数は 2 つです。CO スイッチは、トランク グループ内の第 3 または第 4 の PRI にコールをロールオーバーできます（ほとんどの CO が最大 6 回線のトランク グループをサポートしています）が、たとえば、PRI 番号 1 と PRI 番号 2 の間でチャネルをボンディングできても、PRI 番号 1 と PRI 番号 3 の間でボンディングすることはできません。

上記のビジーアウト ロジックは、すべてのコールが同じ速度で行われることを前提としています。たとえば、あるポート上で 384 kbps の 2 つのコールがアクティブなときに、128 kbps のコールが着信したとします。このコールは 2 チャネルしか使用しないため、3 つのコールに合計 14 チャネル（6+6+2 = 14）が使用され、回線上に 9 チャネルの空きが残ります。ところが、ビジーアウトしきい値が（すべてのコールが 384 kbps で行われると想定して）18 チャネルに設定されていると、このビジーアウトしきい値でまだ使用可能なチャネルは 4 つだけになります。この時点で別の 384 kbps のコールが着信すると、そのコールは、残りの 4 チャネルではコールのサポートに不十分なため、失敗します。また、18 チャネルというビジーアウトしきい値にまだ達していない（14 チャネルしか使用されていない）ので、回線はビジーアウトされず、コールは次の回線にロールオーバーされません。この状態は、既存のコールの 1 つが切断されるまで続きます。このような状況を避けるため、すべてのコールを単一のコール速度に標準化できるようにすることが重要です。

発信コール

発信コールでも着信コールと同じ状況が起きる可能性がありますが、ビジーアウトの発生の仕方は異なります。Cisco 3500 シリーズの IP/VC ゲートウェイは、Resource Availability Indicator および Resource Availability Confirm（RAI/RAC）というメッセージをサポートしています。RAI/RAC メッセージは H.225 RAS 仕様で定義されており、ゲートウェイが満杯でコールをそれ以上ゲートキーパーにルーティングできないことを、ゲートウェイからゲートキーパーに伝えるために使用されます。ゲートウェイはビジーアウトしきい値に達すると、ステータスが True の RAI メッセージをゲートキーパーに送信します。True は「これ以上のコールの送信不可」を意味し、False は「送信可」を意味します。ゲートウェイは、ビジーアウトしきい値を下回るとすぐに RAI=False を送信します。発信コールのビジーアウトしきい値は着信コールのビジーアウトしきい値とは別のもので、それぞれ別々に設定できるので、着信コールを次の空き回線にロールオーバーしても発信コールは引き続き受け入れられ、その逆も同様です。たとえば、RAI しきい値を 12 チャネルに設定し、ISDN ビジーアウトしきい値を 18 チャネルに設定できます。その場合、384 kbps の 2 つのコールがアクティブのとき、発信コールは次の空きゲートウェイにロールオーバーされますが、3 番目の 384 kbps の着信コールは引き続き受け入れられます。同じように効率的に発信コールのビジーアウト フェールオーバーを実現する方法として、RAI/RAC 方式ではなく、次項で述べるように Unified CM のルート グループとルート リストの構造を使用する方法があります。

Unified CM でのゲートウェイの設定

Unified CM では、次のいずれかの方法で Unified Videoconferencing ゲートウェイを設定できます。

- H.323 ゲートウェイとして設定し、Unified CM でコールをそのゲートウェイに直接ルーティングします。
- ゲートキーパーへの H.225 ゲートキーパー制御トランクを設定し、ゲートキーパーを通じてそのゲートウェイにコールをルーティングします。

ゲートウェイが 1 つだけであれば、多くの場合、トランクを介してゲートウェイに到達するよりも、Unified CM で直接設定した方が簡単です。ロード バランシングと冗長性を得るために複数のゲートウェイを使用している場合は、それらのゲートウェイをすべて Unified CM で設定し、ルート グループとルート リストの中に配置する方法があります。または、ゲートキーパーへの H.225 トランクを設定してゲートウェイ間の RAI/RAC を使用し、コールの送信先となるゲートウェイをゲートキーパーが Unified CM に指示するように設定する方法があります。

公衆網から Unified CM への着信コールの場合、各 Cisco Unified Videoconferencing ゲートウェイを 1 つのゲートキーパーに登録する方法と、それらのゲートウェイを、すべての着信コール要求の送り先とする最大 3 台の Unified CM サーバの IP アドレスを使用して設定する方法があります。この方法は、ピアツーピア モードと呼ばれます。どちらの方法でも最終的な目標は、各ゲートウェイが受信したす

べての着信コールを Unified CM に送り、Unified CM がコールのルーティング方法を決定できるようにすることです。コールをゲートウェイから Unified CM にルーティングするようゲートキーパーを設定する方法の詳細については、「ゲートキーパー」（P.16-22）を参照してください。

コール シグナリング ポート番号

デフォルトでは、Cisco Unified Videoconferencing ゲートウェイは、ウェルノウン ポート 1720 の代わりに TCP ポート 2720 を監視します。ただし、同様にデフォルトで、Unified CM は H.323 コールをポート 1720 に送信します。ゲートウェイで監視するポートは変更できます。また、Unified CM からの送信先ポートを Unified CM の H.323 ゲートウェイ デバイス設定で変更することもできます。いずれの方法でも、ゲートウェイへの発信コールが成功するためには、両側で一致している必要があります。

着信方向では、Cisco Unified Videoconferencing ゲートウェイは、ピアツーピア モードで動作するように設定された場合、コールをポート 1720 で Unified CM に送信します。ゲートキーパーに登録するように設定された場合、Unified CM は、ランダムに生成されたポート番号をすべてのゲートキーパー制御トランクに使用します。この方法では、Unified CM が同じゲートキーパーに対して複数のトランクを持つことができます。このポート番号は、Unified CM からゲートキーパーへの Registration Request（RRQ）に含まれているため、ゲートウェイから Unified CM への着信 H.225 セットアップ メッセージは、このポート番号に送られます。ただし、ゲートウェイが Unified CM で H.323 ゲートウェイ デバイスとして直接設定されている場合、Unified CM はコールが H.225 トランクの TCP ポートに着信したことを無視し、発信元 IP アドレスをデータベースに設定されている H.323 ゲートウェイ デバイスと照合します。一致するデバイスが見つからない場合、Unified CM はそのコールがトランクに着信したかのように扱います。

発信方向に関しては、Unified CM がゲートキーパー制御 H.225 トランクを使用してゲートウェイに到達している場合は、ゲートキーパーが Unified CM に、どの TCP ポートを使用してゲートウェイに到達すべきかを知らせます。ゲートウェイが Unified CM で H.323 ゲートウェイ デバイスとして設定されている場合（ピアツーピア モード）、Unified CM は、ポート 2720（デフォルト）か 1720（ゲートウェイで監視ポートが変更された場合）にコールを送るように設定されている必要があります。

コール シグナリング タイマー

H.320 ボンディングに固有の遅延のため、ビデオ コールは音声コールよりも接続に時間がかかる場合があります。Unified CM のいくつかのタイマーは、デフォルトで音声コールをできるだけ高速に処理するように調整されているため、それが原因でビデオ コールが失敗する場合があります。したがって、H.320 ゲートウェイ コールをサポートするには、次のタイマーをデフォルト値から変更する必要があります。

- H.245TCSTimeout
- Media Exchange Interface Capability Timer
- Media Exchange Timer

これらの各タイマーを、Unified CM Administration の Service Parameters で 25 まで増やすことをお勧めします。このパラメータは、クラスタ全体のサービス パラメータなので、既存の H.323 Cisco 音声ゲートウェイへの音声コールも含めて、あらゆるタイプの H.323 デバイスへのコールに影響を与えることに注意してください。

音声ゲートウェイのベアラ機能

H.323 コールは、どのタイプのコールを行うかを示すために、H.225/Q.931 Bearer Capabilities Information Element（bearer-caps）を使用します。音声専用コールでは、bearer-caps が「speech」または「3.1 KHz Audio」に設定され、ビデオ コールでは bearer-caps が「Unrestricted Digital

Information」に設定されます。一部のデバイスでは、Unrestricted Digital Information の bearer-caps をサポートしていません。Unified CM が H.323 ビデオ コールとしてコールを試みると、これらのデバイスへのコールは失敗する場合があります。

Unified CM は、次の要因に基づいて、どの bearer-caps を設定するかを決定します。

- 発信側デバイスまたは着信側デバイス（あるいはその両方）がビデオ対応かどうか
- それらのデバイス間のコールにビデオを許可するように Unified CM のリージョンが設定されているかどうか

Unified CM では、ビデオ コールをオーディオとして再試行する機能をサポートしており、この機能は設定を介して有効にすることができます。Unified CM がビデオ コールの bearer-caps を「Unrestricted Digital」に設定し、コールが失敗すると、Unified CM は同じコールの bearer-caps を「speech」に設定したオーディオ コールとして再試行します。

H.323 を使用する場合、Cisco IOS ゲートウェイは、コールの設定で受信するベアラ機能に基づいて、コールを音声またはビデオとして処理できます。SIP を使用する場合、ゲートウェイはコールのネゴシエーションのため、ISDN 機能を SDP に変換します。

Cisco 音声ゲートウェイが Unified CM との通信に MGCP を使用している場合、この問題は発生しません。それは、Unified CM の MGCP プロトコル スタック上ではビデオがサポートされておらず、しかも、MGCP モードでは、Unified CM が公衆網への D チャネル シグナリングを完全に制御するためです。

CHAPTER 5

Cisco Unified CM トランク

Cisco Unified Communications Manager（Unified CM、旧称 Cisco Unified CallManager）は、外部デバイスとの接続用に何種類かの IP トランクをサポートしています。Unified CM で設定できるトランクは、H.225（H.323）、SIP、およびクラスタ間トランクの 3 種類あります。この章では、これらのトランクの一般的な機能および特徴について説明します。Unified CM トランクの特定用途の詳細については、このマニュアルのその他の関連する章を参照してください。

この章では、次のトピックについて説明します。

Unified CM トランクの用途の詳細については、次に示す章の各項を参照してください。

この章の新規情報

表 5-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 5-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
発番号の正規化	「発番号の正規化および SIP トランク」（P.5-23）
Cisco Unified SIP Proxy	「Cisco Unified SIP Proxy」（P.5-6）
コーデック タイプの選択	「IP トランク上でのコーデック選択」（P.5-24）
設計に関する推奨事項	「IP トランクを配置するときの設計に関する推奨事項」（P.5-25）
SIP トランクの拡張機能	「SIP トランクの概要」（P.5-4）

表 5-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報 （続き）

新規トピックまたは改訂されたトピック	説明箇所
ルート リストを使用する場合の発信コールのロード バランシング	「発信コールのロード バランシング」（P.5-12）
SRTP および SIP トランク	「SIP トランクでの SRTP」（P.5-23）
H.323 および SIP トランク経由のビデオ コーデックのサポート	表 5-2

H.323 および SIP トランクの比較

Cisco Unified CM トランク接続は、H.323 と SIP の両方のトランクをサポートしています。多くの場合、H.323 または SIP のいずれを使用するかは、各プロトコルで提供される固有な機能により異なります。また、お客様の好みや、異なるベンダーの製品間で提供される相互運用性におけるプロトコルの成熟度および品質など、トランク プロトコルの選択に影響を与える外部的要素もたくさんあります。

シスコ デバイス間のトランク接続の場合、H.323 または SIP のいずれを使用するかは、比較的、簡単に決定できます。他のベンダーの製品およびサービス プロバイダー ネットワークとのトランク接続の場合、お客様がどの機能を必要としているか、および 2 つのベンダーの製品間での相互運用性の範囲を理解することが重要です。

表 5-2 に、Unified CM クラスタ間での H.323 および SIP トランクを介して提供される機能の一部についての比較を示します。

表 5-2　Cisco Unified CM トランクでの H.323 および SIP 機能の比較

機能	H.323	H.323 を介した QSIG	SIP
発呼回線（番号）ID 表示	あり	あり	あり
発呼回線（番号）ID 表示禁止	あり	あり	あり
発信者名 ID 表示	あり	あり	あり
発信者名 ID 表示禁止	あり	あり	あり
接続回線（番号）ID 表示	あり	あり	あり
接続回線（番号）ID 表示禁止	あり	あり	あり
接続者名 ID 表示	あり	あり	あり
接続者名 ID 表示禁止	あり	あり	あり
アラート名	なし	あり	あり
転送（ブラインドまたは在席）	あり / あり	あり / あり	あり / あり
自動転送（すべて）	あり	あり	あり
自動転送（通話中）	あり	あり	あり
自動転送（無応答）	あり	あり	あり
呼完了（ビジーサブスクライバ）	なし	あり	なし
呼完了（無応答）	なし	あり	なし
サブスクライブ / 通知、パブリッシュ - 表示	なし	なし	あり
メッセージ待機インジケータ（MWI：ランプ点灯 / 消灯）	なし	あり	あり

表 5-2　Cisco Unified CM トランクでの H.323 および SIP 機能の比較 （続き）

機能	H.323	H.323 を介した QSIG	SIP
パス交換	なし	あり	なし
コール保留 / 復帰	あり	あり	あり
Music On Hold（ユニキャストおよびマルチキャスト）	あり	あり	あり
DTMF リレー	H.245 アウトオブバンド（OOB）[1]	H.245 アウトオブバンド（OOB）[1]	RFC 2833、KPML（OOB）、Unsolicited Notify（OOB）
SIP Early Offer	該当なし	該当なし	あり：発信コールのための MTP が必要
SIP 遅延オファー	該当なし	該当なし	あり
H.323 Fast Start	あり：発信 Fast Start のための MTP が必要	あり：発信 Fast Start のための MTP が必要	該当なし
H.323 Slow Start	あり	あり	該当なし
オーディオ コーデック	G.711、G.722、G.723、G.729、G722	G.711、G.722、G.723、G.729、G722	G.711、G.722、G.723、G.729、G722、iLBC、AAC
MTP でのコーデック	G.711、G.722、G.723、G.729	G.711、G.722、G.723、G.729	G.711、G.729
ビデオ	あり	あり	あり
ビデオ コーデック	H.261、H.263、H.263+、H.264 AVC	H.261、H.263、H.263+、H.264 AVC	H.261、H.263、H.263+、H.264 AVC
T.38 Fax	あり	あり	あり
シグナリング認証	なし	なし	ダイジェスト、TLS
シグナリング暗号化	なし	なし	TLS
メディア暗号化	SRTP	SRTP	SRTP

1. H.323 トランクは、特定の接続の種類で、RFC 2833 に規定されたシグナリングをサポートします。

H.323 トランクの概要

H.323 トランクは、他の Unified CM クラスタや、ゲートウェイなどの他の H.323 デバイスに対する接続性を提供します。H.323 トランクは、Unified CM がクラスタ内通信用にサポートするオーディオおよびビデオ コーデックのほとんどをサポートします。ただし、ワイドバンド オーディオおよびワイドバンド ビデオについてはサポートしません。

H.323 トランクは、Empty Capabilities Set（ECS）を使用して、保留 / 保留解除や転送などの付加コール サービスを提供します。この方式は、メディア ストリーム（またはチャネル）を停止または終了し、同一または別のエンドポイント アドレスに対してメディア ストリームを開始または起動するための標準の H.245 メカニズムです。この方式を使用すると、Unified CM は、コールをアクティブにしたままでも、メディア ストリームの送信元および宛先を迅速に制御することができます。

たとえば、H.323 トランクを使用した 2 つのクラスタ（A と B）間のコールについて考えます。クラスタ A のユーザがクラスタ B のユーザを保留にした場合、2 人のユーザ間のメディア ストリームは終了し、クラスタ B のユーザはクラスタ A の Music On Hold（MoH）サーバに接続されます。MoH サーバは、ユーザにメディア（音楽ファイル）を送信するよう指示されます。クラスタ A のユーザがコールを保留解除すると、MoH ストリームが終了し、2 人のユーザ間で双方向メディア ストリームが再開されます（Unified CM は、付加コール サービス用に H.450 をサポートしていません）。このケースでは、MoH は ECS 動作の一例です。Cisco Unified CM 7.1(2) から、H.323 トランクがマルチキャスト MoH をサポートするようになったので、H.323 トランクの Media Resource Group List（MRGL; メディア リソース グループ リスト）にはユニキャストとマルチキャスト MoH リソースの両方を含めることができます（詳細については、「Music on Hold」（P.7-1）を参照してください）。

H.323 トランク上のコールに使用される帯域幅を制御するには、Unified CM で設定される 、各トランクに割り当てられる *リージョン*を使用します。リージョンは、そのリージョンのコールごとの音声コーデック タイプとビデオ帯域幅を指定することで、コールに割り当てられる帯域幅の量を制限します。そのリージョンと別のリージョン間のコールは、指定された帯域幅の制限内にする必要があります。H.323 トランク上でコールを発信するデバイスが、より限定的なリージョン内にある場合や、ビデオなどの特定のコーデックをサポートしない場合、そのデバイスはそのコールに使用可能なコーデックのサブセットになっています。

H.323 トランクは、H.245 を使用したアウトオブバンド DTMF と RTP Named Telephone Event（RFC-2833）を使用したインバンド DTMF の両方で DTMF シグナリングをサポートします。設定オプションはありません。H.323 トランクがどのような場合にどの方式を使用するかについては、「メディア リソース」（P.6-1）を参照してください。

SIP トランクの概要

SIP トランクは、ゲートウェイ、プロキシ、ボイスメール システム、および他の Unified CM クラスタなど、他の SIP デバイスへの接続性を提供します。Cisco Unified CM 5.*x* 以降のリリースでは、SIP トランクの主な拡張機能が提供され、Cisco Unified CM 4.*x* での制限（たとえば、単一コーデックのサポート、ビデオ サポートの欠如、RFC 2833 DTMF サポートに必須のメディア ターミネーション ポイント（MTP）など）が解消されています。

Cisco Unified CM 6.*x* での SIP トランクに対する主な拡張機能としては、iLBC および AAC コーデックや SIP PUBLISH のサポートがあります。SIP PUBLISH は、パフォーマンスを向上させることで、SIP トランクを介して IP Phone プレゼンス情報を Cisco Unified Presence に送信するための、Cisco Unified CM 6.*x* に適したメカニズムを提供します。

Cisco Unified CM 7.*x* での SIP トランクに対する主な拡張機能としては、次のものがあります。

- 初期 SIP INVITE 要求の発信における G.729 コーデックのサポート
- コンテンツをシグナリングして、発信側および送信側の名前や番号を表示するかどうかを指定する、Privacy、P-Asserted-Identity および P-Preferred-Identity ヘッダーの使用
- Secure Real-Time Transport Protocol（SRTP）を使用したメディア暗号化
- 発信側番号の正規化のサポート

SIP トランクの新規拡張機能の全リストについては、次の Web サイトで入手可能な Cisco Unified Communications Manager の製品リリース ノートを参照してください。

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

クラスタ間トランキングに使用した場合、SIP トランクは Annex M1 を使用した QSIG Tunneling をサポートしません。

H.323 トランクと同様に、SIP トランク経由のコール用に選択されるコーデックは、SIP コール セットアップ メッセージから取得したリモート エンドポイントの機能、ローカル エンドポイントの機能、トランクとローカル エンドポイント間のリージョン間コーデック設定によって決定されます。

（注）　可能であれば、G.729 などの低品質なコーデックよりも、G.722 や G.711 などの高品質なコーデックが選択されます。このルールの例外は、リージョン間のリンクが **lossy** としてマークされている場合です。この場合は、可能であれば iLBC コーデックが使用されます。

サービス プロバイダー ネットワークに対する IP PSTN および IP トランク

Cisco Unified CM では、H.323 と SIP の両方のトランクがサポートされるため、サービス プロバイダーは、企業カスタマーへの非 TDM PSTN 接続の提供を開始できます。非 TDM インターフェイスを配置することで得られるコスト削減という明らかなメリットのほかに、多くの場合、これらの IP ベース PSTN 接続では、従来の PSTN インターフェイスより優れた音声機能が提供されます。

IP トランキング プロトコルとして H.323 または SIP のいずれを採用するかは、通常、サービス プロバイダーによって異なりますが、現在では SIP ベースのサービスが利用可能なサービスの中心になってきています。これは主として、企業内で SIP の人気が高まっていることに加え、プレゼンスなどの追加機能や多くのマルチメディア アプリケーション（インスタント メッセージングなど）のサポートが提供されることが背景にあります。長期的に見ると、SIP のほうが、Unified Communications プロトコルとして幅広く使用されるようになると思われます。

SIP と H323 の規格はいずれも、一定の統合においてオープン スタンダードとなっているので（オプションおよび必須の要件が数多くあります）、ベンダー間における相互運用性の程度は、通常、これらのプロトコルの成熟度が高まるにつれて改善されます。そのため、Cisco Unified Border Element（旧称 Cisco Multiservice IP-to-IP Gateway Software）は、相互運用性に関する数多くの機能、および他のベンダーの H323 および SIP ネットワークと接続するときのセッション ボーダー コントローラとして通常の境界ポイントを提供します。

Cisco Unified Border Element

Cisco Unified Border Element（旧称 Cisco Multiservice IP-to-IP Gateway Software）は、企業およびサービス プロバイダーの Cisco Unified Communications ネットワーク間で、幅広いシグナリングおよびメディア機能を提供します。Cisco Unified Border Element は、次のものを対象として、ネットワーク間インターフェイス ポイントを提供します。

- アドレスおよびポート トランスレーション（プライバシーおよびトポロジ隠蔽）
- シグナリング インターワーキング（H.323 および SIP）
- メディア インターワーキング（DTMF、FAX、モデムおよびコーデック トランスコーディング）
- QoS および帯域幅管理（ToS/DSCP を使用した QoS マーキング、および RSVP やコーデック フィルタリングによる帯域幅拡張）
- 課金および CDR 正規化

Cisco Unified Border Element は、Cisco 2800 および 3800 シリーズの Integrated Service Routers（ISR）、Cisco AS5350XM および AS5400XM Media Gateways、Cisco 7200VXR および Cisco 7301 シリーズのルータおよびゲートウェイ プラットフォームで使用できる、認可を受けた Cisco IOS アプリケーションです。

Cisco Unified Border Element は、任意の IP PSTN 配置に使用することをお勧めします。

Cisco Unified SIP Proxy

Cisco Unified SIP Proxy は、Cisco 3800 シリーズの Integrated Services Router（ISR; 統合サービス ルータ）のネットワーク モジュール スロットに差し込むことができる Cisco NME-522 ネットワーク モジュールで SIP プロキシ機能を提供します。この ISR は、ネットワーク モジュールのホスティングやプロキシの実行専用にする必要はなく、上記の Cisco Unified Border Element の実行など、その他のネットワーク機能にも同時に使用することができます。

Cisco Unified SIP Proxy は、Unified CM SIP トランクを使用するネットワークに次のような利点を提供します。

- 集約とルーティング

  Unified SIP Proxy は、各サーバがフルメッシュ構成で他のすべてのサーバに接続する必要なしに、SIP サーバを相互に接続することができます。

- スケーラビリティ

  Unified SIP Proxy は、企業や IP-PSTN サービス プロバイダーとのコールを終端するために使用できます。プロキシは次に、そのコールを Unified Border Element のプールに分配します。Unified Border Element を追加して容量を増やすこともできます。

- 可用性とロード バランシング

  Unified SIP Proxy は、使用可能な Unified Border Element のプールにコールを分配し、各 Unified Border Element のステータスをモニタリングすることで、信頼できるコールの完了を実現します。

- メッセージの正規化

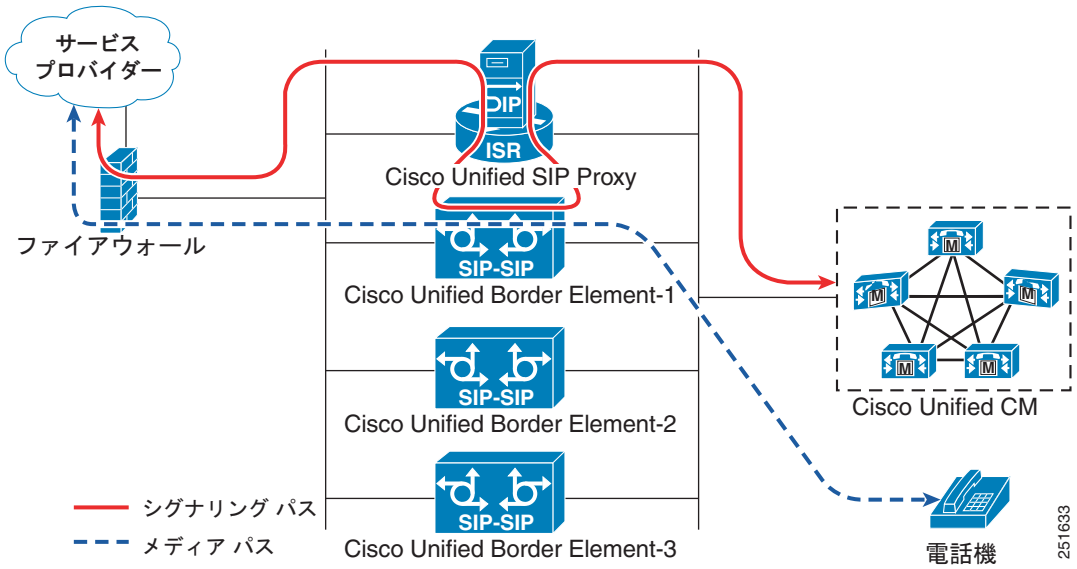
  Unified SIP Proxy は、メッセージが Unified SIP Proxy を通過する際に、そのヘッダーや内容を操作する手段を提供することにより、SIP プロトコルのメッセージングにおける違いを隠す役割を果たします。

Cisco Unified SIP Proxy と Cisco Unified Border Element を配置する場合は、次の設計上の考慮事項を検討する必要があります。

- スケーラブルな接続が必要となる場合は、Unified SIP Proxy を使用します。容量の追加は、新しい Unified Border Element を追加するのと同じくらい簡単です。
- 接続されている Unified Border Element がいずれも過負荷にならないように、Unified SIP Proxy 上でロード バランシングの方式を設定します。
- Unified CM または Unified Border Element の障害を検出して対処できるように、Unified SIP Proxy にトランクのモニタリングをセットアップします。

図 5-1 に、Cisco Unified SIP Proxy と Cisco Unified Border Element を使用したコール フローを示します。

図 5-1　Cisco Unified SIP Proxy と Cisco Unified Border Element のコール フロー



サービス プロバイダーへのコールを発信するために、Unified CM は Unified SIP Proxy にコールを送信します。Unified SIP Proxy は要求が Unified CM から発信されたと判断し、Unified Border Element にコールを転送します。Unified Border Element はコールを終端および再発信して Unified SIP Proxy に戻します。Unified SIP Proxy はコールが Unified Border Element から発信されたと判断し、今度はサービス プロバイダーにコールを転送します。このように、メディアは Unified Border Element を介して、発信した電話機からサービス プロバイダーまで直接確立されます。

Cisco Unified SIP Proxy のインストールと設定の詳細については、次の Web サイトで入手可能な製品マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps10140/tsd_products_support_model_home.html

H.323 トランク

Unified CM では、次の主要なタイプの H.323 トランクを設定できます。

- 「クラスタ間トランク（非ゲートキーパー制御）」（P.5-7）
- 「クラスタ間トランク（ゲートキーパー制御）」（P.5-8）
- 「H.225 トランク（ゲートキーパー制御）」（P.5-8）

クラスタ間トランク（非ゲートキーパー制御）

このトランクは、最も単純で、単一のマルチクラスタ キャンパスまたは分散型コール処理配置で他の Unified CM クラスタに接続するために使用されます。このトランクは、コール アドミッション制御にゲートキーパーを使用しません。ただし、帯域幅制御が必要な場合は、Unified CM で設定されたロケーションを使用できます。

このタイプのトランクを定義する場合、同一の宛先クラスタに最大 3 つのリモート Unified CM サーバを定義できます。トランクは、定義されているすべてのリモート Unified CM サーバに自動的にロードバランスされます。リモート クラスタでは、対応するクラスタ間トランク（非ゲートキーパー制御）

を設定することが重要です。このトランクには、最初のクラスタでリモート Unified CM サーバとして定義されているサーバと同じサーバを含む Unified CM Group を割り当てます。クラスタ間トランクによって接続された各 Unified CM クラスタでも、同様の設定が必要です。

たとえば、クラスタ 1 にクラスタ 2 へのトランクがあり、クラスタ 2 にクラスタ 1 へのトランクがある場合は、次の設定が必要になります。

- クラスタ 1
  - サーバ B、C、および D を、クラスタ 2 へのトランクに関連付けられたデバイス プールで定義されている Unified CM Group のメンバーとして設定します。
  - 非ゲートキーパー制御トランクに、クラスタ 2 のリモート サーバ D、E、および F を設定します。
- クラスタ 2
  - サーバ D、E、および F を、クラスタ 1 へのトランクに関連付けられたデバイス プールで定義されている Unified CM Group のメンバーとして設定します。
  - 非ゲートキーパー制御トランクに、クラスタ 1 のリモート サーバ B、C、および D を設定します。

クラスタ間トランク（ゲートキーパー制御）

クラスタ数が多くなる場合は、クラスタ間非ゲートキーパー制御トランクの代わりに、クラスタ間ゲートキーパー制御トランクを使用する必要があります。ゲートキーパー制御トランクを使用する主な利点は、クラスタとフェールオーバー時間を全体的に管理できることです。非ゲートキーパー制御トランクでは、一般に、トランクのフル メッシュを設定する必要があります。ただし、この作業は、クラスタ数が増加すると管理負担になる場合があります。また、クラスタ内のサブスクライバ サーバが到達不能になった場合は、5 秒（デフォルト）でコールの試行がタイムアウトします。クラスタ全体が到達不能になった場合、コール障害または公衆網を介した再ルーティングのいずれかが発生するまでの試行回数は、トランク用に定義されたリモート サーバの数と、ルート リストまたはルート グループ内のトランクの数によって異なります。リモート サーバと非ゲートキーパー制御トランクの数が多いと、コール遅延が過剰になることがあります。

ゲートキーパー制御トランクを使用する場合は、ゲートキーパーに登録されている他のすべてのクラスタとゲートキーパーを介して通信できるトランクを 1 つだけ設定します。クラスタまたはサブスクライバが到達不能になった場合、ゲートキーパーは自動的に、コールをクラスタ内の別のサブスクライバに送信するか、または他のサブスクライバが存在しなければコールを拒否します。その結果、ほとんど遅延させることなく、公衆網を介して（必要な場合）コールを再ルーティングすることができます。単一の Cisco ゲートキーパーを使用すると、100 のクラスタすべてが、それぞれ 1 つのトランクを、相互にコールできるすべてのクラスタに登録できます。非ゲートキーパー制御トランクを使用する場合、この同じトポロジでは、各クラスタに 99 のトランクを設定する必要があります。クラスタ間ゲートキーパー制御トランクは、他の Unified CM と通信する場合だけ使用する必要があります。これは、このトランクを他の H.323 デバイスで使用すると、付加サービスに問題が発生することがあるためです。また、Release 3.2 よりも前の Unified CM との下位互換性を確保する場合は、クラスタ間ゲートキーパー制御トランクを使用する必要があります。

H.225 トランク（ゲートキーパー制御）

H.225 ゲートキーパー制御トランクは、本質的にはクラスタ間ゲートキーパー制御トランクと同じですが、Unified CM クラスタ Release 3.2 以降のほか、ゲートウェイ、会議システム、およびクライアントなどの他の H.323 デバイスと連携動作する機能を持つ点が異なります。この機能は、コールごとに検出メカニズムを通じて実現されます（この検出プロセスの詳細については、「Unified CM における H.323 の動作」（P.5-15）を参照してください）。このタイプのトランクは、すべての Unified CM クラスタが Release 3.2 以降の場合に推奨される H.323 トランクです。

ゲートキーパー トランクの冗長性、復元性、およびロード バランシング

冗長性は、設計の要件に応じて、複数の方法で実現できます。最も簡単に実現するには、ゲートキーパー制御トランクを設定し、そのトランクに割り当てられたデバイス プールに関連付けられている Unified CM Group に、最大 3 つのサブスクライバを割り当てます。この設定により、すべてのサーバが、同じテクノロジー プレフィックスとともに、同じゾーン内の同じゲートキーパーに登録されます。ただし、h323_id に使用される H.323 トランクの名前には、「*_n*」というサフィックスが付加されます。ここで、*n* はクラスタ内のノード番号です。この ID は自動的に生成され、変更できません。単一のトランクを設定しても、ゲートキーパーは、複数のトランク、つまり Unified CM Group 内のサブスクライバごとに 1 つのトランクを登録します。

追加の冗長性要件がある場合は、別のゲートキーパー制御トランクに、Unified CM Group にある別の名前と別のサブスクライバを設定できますが、それ以外のパラメータはすべて最初のトランクと同じになります。この 2 つ目のトランクによって、追加のサブスクライバがゲートキーパーに登録されます。

標準のサブスクライバ ペアを構成する 2 つのサーバから Unified CM Group を構成し、このグループを含むデバイス プールを割り当てることをお勧めします（サブスクライバの冗長性の詳細については、「コール処理サブスクライバ」（P.8-8）を参照してください）。各クラスタ全体で完全な冗長性を実現するには、4 つの異なるデバイス プールを使用する 4 つのトランクが必要になります。結果的に、8 つのサブスクライバがゲートキーパーに登録されます（3 つのトランクとさらに大きい Unified CM Group を使用しても同じ結果となります）。

登録時、Unified CM とゲートキーパー間では複数のパラメータが受け渡しされます。Unified CM は、ゲートキーパーの Registration Admission Status（RAS）メッセージ用に、一時的なユーザ データグラム プロトコル（UDP）ポートを使用します。このポートは、通常であれば、UDP 1719 です。ただし、Unified CM は、特定のサーバからの RAS メッセージの発信元での H.323 デーモンを正確に特定できる必要があります。したがって、Unified CM は一定範囲の UDP ポートを使用して、動的に割り当てます。

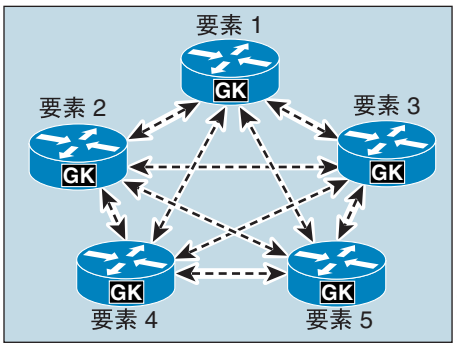
登録プロセス時、トランクは、その Unified CM Group にある他のサブスクライバに関する次の情報を登録します。

- H.225 コール シグナリング ポート
- h323_id
- CanMapAlias サポート
- テクノロジー プレフィックス
- H.225 コール シグナリング アドレス

推奨されるクラスタ化ゲートキーパーが使用されている場合、ゲートキーパーは、代替ゲートキーパー アドレスのリストを返します。このリストは、プライマリ ゲートキーパーで障害が発生した場合や使用可能なリソースが不足した場合に使用されることがあります。

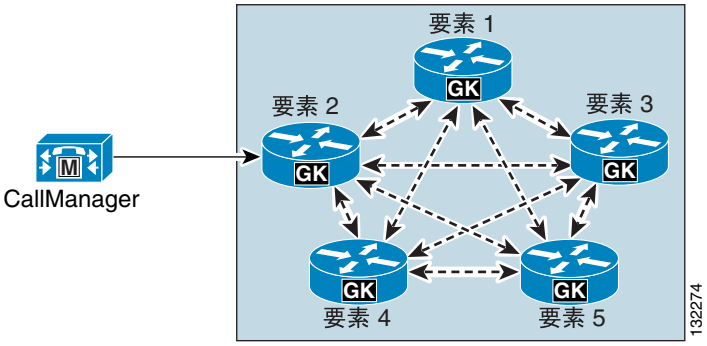
図 5-2 は、Gatekeeper Update Protocol（GUP）を使用して通信する、ゲートキーパーのクラスタを示しています（ゲートキーパーの詳細については、「コール処理」（P.8-1）の章を参照してください）。

図 5-2　ゲートキーパー クラスタ



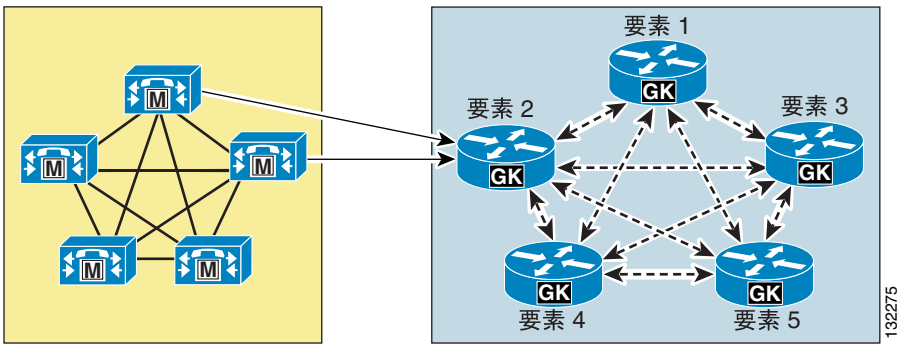
H.323 トランクの Unified CM Group にサブスクライバが 1 つだけ含まれている場合、Unified CM の設定済みゲートキーパーとゲートキーパー クラスタの間の接続は 1 つだけになります（図 5-3 を参照）。

図 5-3　単一の Unified CM サブスクライバを使用する H.323 トランク



トランクに関連付けられた Unified CM Group に複数のサブスクライバが含まれている場合、Unified CM クラスタとゲートキーパー クラスタ間には追加の接続が確立されます（図 5-4 を参照）。

図 5-4　複数の Unified CM サブスクライバを使用する H.323 トランク



このアプローチによってサブスクライバ障害やゲートキーパー障害に対する冗長性が確保されるのは、登録完了後です。これは、トランクの登録時に代替ゲートキーパーの通信が行われるためです。ただし、このアプローチでは、設定済みのゲートキーパーが初期登録時やリセット後に使用不能である場合には、冗長性が確保されません。これは、代替ゲートキーパーのリストがダイナミックであり、データベースに格納されないためです。冗長性のレベルを上げたりロード バランシングを追加したりするに

は、ゲートキーパー クラスタにある追加のゲートキーパーを Unified CM で設定します。たとえば、元のトランクがエレメント 2 に登録されている場合は、追加のゲートキーパーをエレメント 4 として設定できます（図 5-5 を参照）。

図 5-5　ロード バランシングと追加の冗長性のために設定された追加のゲートキーパー

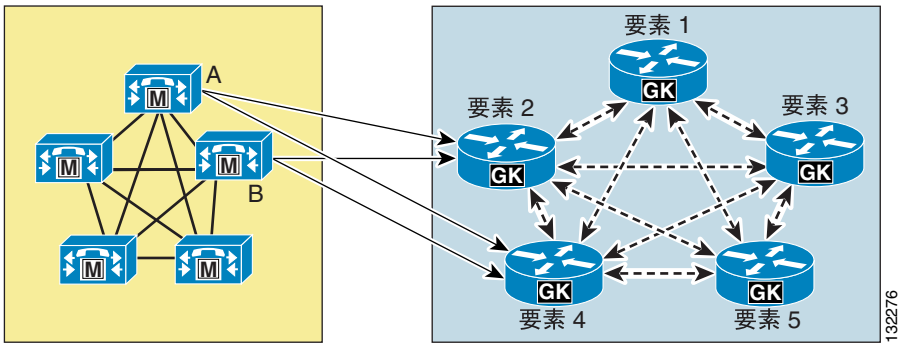


図 5-5 の例の場合、Unified CM の設定には次のコンポーネントが含まれます。

- エレメント 2 とエレメント 4 の 2 つのゲートキーパー
- サブスクライバ サーバ A および B を含む Unified CM Group に対して定義された 2 つの H.323 トランク

このアプローチを使用すると、初期設定時にエレメント 2 またはエレメント 4 が到達不能であっても（つまり、起動中またはトランクのリセット中でも）、引き続き Unified CM クラスタが登録できるようになります。

Unified CM クラスタに着信するコールのロード バランシングは、デフォルトで自動的に行われます。これは、ゲートキーパーが、ゾーン内の登録済みサブスクライバのいずれかをランダムに選択するためです。この動作が期待と異なる場合は、ゲートキーパーで **gw-priority** コンフィギュレーション コマンドを使用して、このデフォルト動作を変更することができます（例 5-1 を参照）。

例 5-1　gw-priority コマンドを使用してコールを特定のトランクに送信する

```
gatekeeper
 zone local SJC cisco.com 10.0.1.10
 zone prefix SJC 1408....... gw-priority 10 sjc-trunk_2
 zone prefix SJC 1408....... gw-priority 9 sjc-trunk_3
 zone prefix SJC 1408....... gw-default-priority 0
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
 endpoint ttl 60
```

では、H.323 トランクは Unified CM で sjc-trunk として設定されています。また、クラスタ内のサブスクライバのノード番号を示すために、「_2」と「_3」のサフィックスが Unified CM サブスクライバによって自動的に付加されています。例 5-1 したがって、この例では、最初の選択肢としてノード 2 を使用します。このノードは、このトランクの Unified CM Group において最もプライオリティの高い Unified CM となる必要があります。このケースでは、ノード 3 は 2 番目の選択肢となります。

gw-default-priority 0 を使用するかどうかは任意です。この例で使用したのは、このゾーンで登録するよう不用意に設定される可能性のある他のトランクが一切使用されないようにするためです。

発信コールのロード バランシング

ほとんどの場合、標準方式で Unified CM Group をデバイスに割り当てれば、コール処理サブスクライバからの IP トランクを介した発信コールのコール分配に十分に対応できます。IP トランク コールは、コール処理サブスクライバからランダムに発信されるように思えますが、このランダム コール発信では、コール処理が減り、クラスタ内での Intra-Cluster Communication Signaling（ICCS）トラフィックも減るというトレードオフがあります。コール処理サーバにおける発信 IP トランク コールのロード バランシングは、次に説明するように、逆効果となることがあります。これは、クラスタ内での予測可能なコール発信によりもたらされるメリットよりも、発信 IP トランク コールを発信させるためにクラスタ内の別のサーバに通信を拡張する 1 つのサブスクライバの登録電話からのコールにより増加する ICCS トラフィック量によるデメリットが上回るためです。

（注）　発信トランクの選択に役立つルート リストが使用される設定では、サブスクライバの選択は上記の説明と異なる場合があります。Unified CM は、発信側エンドポイントが登録され、トランクもホストしているサブスクライバを選ぶのではなく、ルート リストとトランクの両方をホストするサブスクライバを選択する場合があります。このため、発信トランクの選択によって、サブスクライバ間の ICCS トラフィックが最小化されることはなくなります。ルート リストを使用する場合の ICCS トラフィックを最小化するために、ルート リストに関連付けられる Unified CM Group では、トランクに関連付けられる Unified CM Group のサブスクライバ セットとは異なるサブスクライバ セットを使用することをお勧めします。

H.323 トランクを介した発信コールの開始において、選択されるサーバは、Unified CM クラスタ内での次の主な要因により決定されます。

- どの Unified CM サーバに、選択されたトランクのアクティブ H.323 デーモンがあるか
- 選択されたサーバのアクティブ H.323 デーモンがある Unified CM サーバに、コールを発信する電話が登録されているか

IP トランクの場合、サーバ選択プロセスは、たとえば、PSTN へのコール発信に使用できるゲートウェイの選択や、複数のゲートウェイでのコール分配の提供にルート リストおよびルート グループを使用できる、ゲートウェイとの H.323 接続の場合ほど直感的ではありません。ルート リストおよびルート グループ プロセスは、トランク選択およびコール分配でも使用できますが、H.323 コールを発信するサーバの選択を行うセカンド プロセスが発生します。つまり、ルート リストおよびルート グループ設定により、発信トランクが選択された後、その選択されたトランクに対する Unified CM Group の 1 台のサーバを、H.323 コールを発信するサーバとして選択しなければなりません。

すべての IP トランクにおいて、この発信コールのサーバ選択プロセスは、次のようになります。

- 選択されたトランクのアクティブ H.323 デーモンが、コールを発信する電話またはデバイスが登録される Unified CM サーバにある場合（つまり、このサーバがトランクの Unified CM Group にリストされているサーバに含まれる場合）、H.323 コールを発信するサーバとして、この Unified CM サーバを使用します。
- 選択されたトランクのアクティブ H.323 デーモンが、コールを発信する電話またはデバイスが登録される Unified CM サーバにない場合、選択されたトランクの Unified CM Group から、ラウンドロビン方式でサーバを 1 台選択します。

（注）　トランクの Unified CM Group で定義されているすべてのサーバは、そのトランクのアクティブ H.323 デーモンを実行します。トランクの Unified CM Group 内で定義されている各サーバでは、各 H.323 トランクに対して、一意な H.323 デーモンが作成されます。

IP トランクを介した発信コールに対して、予測可能および確定的なロード バランシングを提供するには、上記のトランク選択動作を考慮する必要があります。

サブスクライバに基づいた発信 IP トランク コールのロード バランシングは、次のように実現できます。

- 発信トランク コールをクラスタのコール処理サーバの 1 つのサブセットだけでロード バランシングするには、複数のトランクを定義して、各トランクの Unified CM Group にサブスクライバを 1 つだけ割り当てます。
- Unified CM Group 内でサブスクライバの冗長性を確保する場合、発信トランク コールの予測可能なサブスクライバ ロード バランシングを提供する最も簡単な方法は、電話の登録に使用されるサブスクライバと、トランク コールを開始するサブスクライバを別々にすることです。

たとえば、発信トランク コールをクラスタの 4 つのサブスクライバに分散するには、次のタスクを実行します。

- 4 つの Unified CM Group に対して 4 つの H.323 トランクを設定し、これらすべてを、循環コール分配を使用するルート グループに含めます。
- Unified CM Group は、次のように定義されます。
  - グループ A: サブスクライバ A
  - グループ B: サブスクライバ B
  - グループ C: サブスクライバ C
  - グループ D: サブスクライバ D

バックアップ サブスクライバが定義されていない場合、指定されたトランクのプライマリ サブスクライバで障害が発生すると、Unified CM は、ルート グループの次のトランクに発信コールを再ルーティングします。

上記の例の場合、サブスクライバ A、B、C、D を次のように使用することで、提供される各トランクの各 Unified CM Group 内でバックアップ サブスクライバを定義できます。

- グループ A: サブスクライバ A; サブスクライバ B
- グループ B: サブスクライバ B; サブスクライバ C
- グループ C: サブスクライバ C; サブスクライバ D
- グループ D: サブスクライバ D; サブスクライバ A

ただし、電話登録や H.323 デーモン サブスクライバのコロケーションに基づいた発信トランク コールのサブスクライバ選択を回避するため、クラスタ内のすべての電話は、他のコール処理サーバ（たとえば、サブスクライバ、E、F、G、H）に登録し、必要に応じて、Unified CM Group を使用してサーバ冗長性を確保する必要があります。

発信トランク コールをクラスタの 8 つのすべてのサブスクライバに分散するには、次のタスクを実行します。

- 8 つの異なる Unified CM Group に対して 8 つの H.323 トランクを設定し、各グループにサブスクライバを 1 つだけ含め、すべてのトランクを循環ルート グループに含めます。
- Unified CM Group は、次のように定義されます。
  - サブスクライバ A
  - サブスクライバ B
  - サブスクライバ C
  - サブスクライバ D
  - サブスクライバ E
  - サブスクライバ F
  - サブスクライバ G
  - サブスクライバ H

メディア ターミネーション ポイントを使用する H.323 トランク

メディア ターミネーション ポイント（MTP）は、一般に、H.323 トランクの通常動作には必要ありません。ただし、通信相手となるデバイスが、H.323 Version 1 である場合、付加サービス用に Empty Capabilities Set（ECS）をサポートしていない場合、または H323 FastStart を必要とする場合には必要です。

MTP が必要かどうかをテストするには、次の簡単な手順を使用します。

1. 電話機から H.323 トランクを介して他のデバイスにコールを発信します。このコールは通常どおりに発信する必要があります。
2. コールを保留にしてから、保留解除します。コールがドロップする場合は、Unified CM と他のデバイス間の相互運用性を保証するために MTP を使用することをお勧めします。

H323 発信 FastStart コール接続

大規模な WAN トポロジを介して IP Phone から発信されるコールに対して、着信側がオフフックで応答する場合、音声クリッピングが発生します。H.323 トランクまたはゲートウェイが、Unified CM サーバから分離されている場合、コールのセットアップ時に大量の H.245 メッセージが交換されるため、著しい遅延が発生します。

FastStart 機能を使用すると、2 つのパーティ間でメディア接続を確立するために必要な情報が、コール セットアップの H.225 段階で交換されるため、H.245 メッセージが不要になります。この接続では、コール セットアップ時に 1 回のラウンドトリップ WAN 遅延が発生しますが、着信側がコールに応答するときに、発信側で音声クリッピングが発生することはありません。

Unified CM は、H.323 発信 FastStart コールを確立するために、メディア ターミネーション ポイント（MTP）を使用します。Unified CM は、MTP を割り当て、受信チャネルを開くことで、発信 FastStart コールを開始します。次に、H.323 Fast Connect プロシージャにより、FastStart 要素を含む SETUP メッセージが着信側エンドポイントに送信されます。この FastStart 要素には、MTP の受信チャンネルに関する情報が含まれています。

その他の MTP の使用

MTP は、H.323 トランク上でコールを発信する他のデバイスからのメディア ストリームを終端させる場合や、同じ音声ペイロードでメディア ストリームを再発信する場合に非常に役立ちます。ただし、そのような場合、IP アドレスは MTP のアドレスに変更されます。この事実に留意して、次のシナリオで MTP を使用します。

- 企業内の電話機、ゲートウェイ、および他のデバイスがすべて RFC 1918 プライベート アドレスを使用する場合は、すべての音声およびビデオ デバイスにネットワーク アドレス変換（NAT）を使用しなくても、引き続きパブリック ネットワーク上の他のシステムに接続できます。パブリック ネットワークと通信する Unified CM サブスクライバがパブリック IP アドレスを使用している場合、シグナリングはルーティングされます。また、すべての MTP もパブリック アドレスを使用している場合、RFC 1918 アドレスを持つデバイスからのメディアは MTP で終端され、再度発信されます。ただし、今度は、パブリック ネットワーク上でルーティング可能なパブリック アドレスが割り当てられます。このアプローチを使用すると、RFC 1918 アドレスを持つ何万台ものデバイスが、パブリック ネットワークと通信できるようになります。この同じ方式を使用すると、企業ネットワークにあるデバイスが他の企業またはサービス プロバイダーと通信するときに、そのデバイスの実際の IP アドレスを隠すことができます。

- 信頼性境界を設定すると、ファイアウォールを通過させることや、アクセス コントロール リスト（ACL）を使用したアクセスを許可することができます。通常、メディアがファイアウォールを通過できるようにするには、アプリケーション レイヤ ゲートウェイ（ALG）またはフィックスアップを使用して、動的にメディア ストリームにアクセス許可を与えるか、または、ファイアウォールを越えて通信する必要のある音声デバイスすべてで使用するための広範囲のアドレスおよびポートを割り当てます。H.323 トランクを使用し、ファイアウォールまたは ACL を通過するすべてのコールには、MTP から発信されるメディアが割り当てられます。このメディアでは、単一の IP アドレスまたは狭い範囲の IP アドレスを使用できます。

これらの方法を両方使用する場合、**MTP Required** チェックボックスをオンにすると、デフォルトで、H.323 トランク上のコールが許可されます。このことは、MTP リソースが使用不能の場合や、使い果たされた場合でも同様です。このデフォルト動作により、コールの音声パスが使用不能になる場合があります。この動作を変更するには、H.323 セクションにある Unified CM サービス パラメータ **Fail Call if MTP allocation fails** を **True** に設定します。

Unified CM における H.323 の動作

この項では、H.323 プロトコルを Unified CM で使用および実装する方法、および特定の機能が所定どおりに動作する仕組みとその理由について説明します。

理解するうえで最も重要な点は、どのサブスクライバがコール シグナリング デーモンを実行するかということです。このデーモンは、H.323 コールを発信および受信する部分的なコードです。これは、通常、H.225 デーモン（H.225D）と呼ばれます。H.225 は、H.323 プロトコルの一部で、主に呼制御を担当します。H.245 は、H.323 のもう 1 つの主要コンポーネントで、コールのメディア制御を担当します。

特定の H.323 デバイスに対する Unified CM Group のリストに含まれているサブスクライバによって、デーモンを実行するサブスクライバと実行時期が決定されます。この点は非常に重要です。これは、不適切なサブスクライバに送信されたコールは、拒否される場合があるためです。たとえば、この状況が発生するのは、Cisco IOS H.323 ゲートウェイに、Unified CM クラスタ内のサブスクライバ C にコールを送信するダイヤル ピアが設定されているものの、そのゲートウェイの Unified CM Group のリストにはサブスクライバ A および B しか含まれていない場合です。そのような場合、コールは失敗するか、またはデーモンがサブスクライバ上に設定されていれば H.323 トランク デーモンによって処理されます。

次のシナリオは、H.225D がサブスクライバ上に作成される仕組みとその時期について説明しています。

- H.323 クライアント

  H.225D は、H.323 クライアントに関連付けられた Unified CM Group で使用可能な、最もプライオリティの高いサブスクライバ上だけでアクティブになります。

  H.323 クライアントがゲートキーパー制御の場合、RasAggregator デバイスは、ゲートキーパー制御の H.323 クライアントに関連付けられた Unified CM Group で使用可能な、最もプライオリティの高いサブスクライバから登録されます。

  RasAggregator は、次の 2 つの特殊機能を提供するためにゲートキーパー ゾーンで登録される特殊なデバイスです。

  - H.323 クライアントが DHCP を使用している場合は、DNS を使用している Unified CM でそのクライアントを使用できません。ただし、クライアントが Dynamic DNS をサポートしている場合は除きます。RasAggregator を使用すると、Unified CM は、コールを発信するたびに、ゲートキーパーに登録されている特定の H.323 クライアントの IP アドレスを取得できます。ゲートキーパー登録は、H.323 クライアントの E.164 アドレスを含む標準の RAS ARQ メッセージを使用して行われます。ゲートキーパーは、E.164 アドレスを解決し、IP アドレスを ACF メッセージで Unified CM に返します。

– また、RasAggregator を使用すると、H.323 クライアントによるコールはすべて Unified CM を経由するようになり、クライアント自身の間では直接やり取りされないことが保証されます。これにより、ダイヤリング規則とコーデック制限が適用されることが保証されます。

- H.323 ゲートウェイ

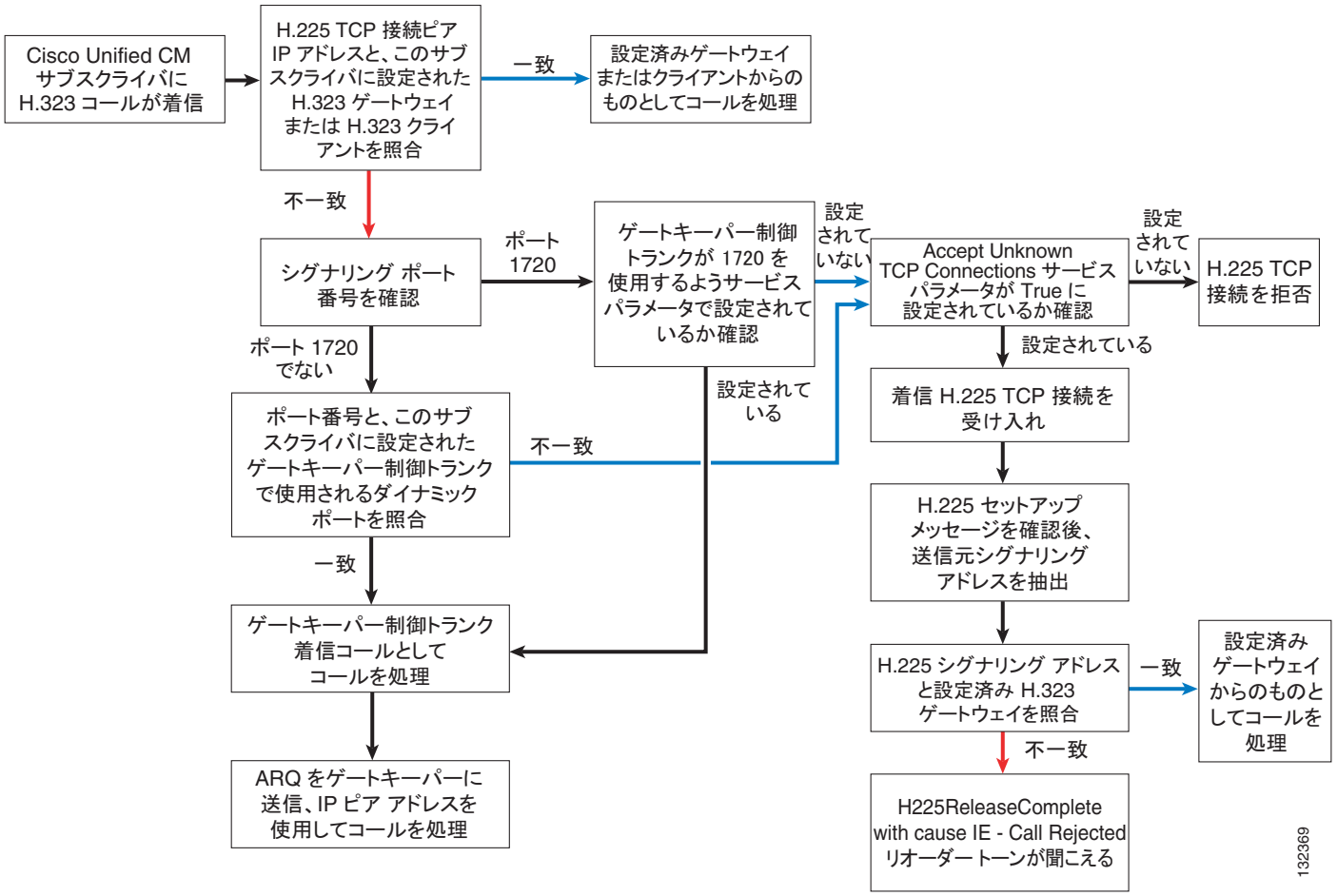
  H.225D は、H.323 ゲートウェイに関連付けられた Unified CM Group にあるすべてのサブスクライバ上でアクティブになります。

- H.323 トランク

  H.225D は、H.323 トランクに関連付けられた Unified CM Group にあるすべてのサブスクライバ上でアクティブになります。RAS デーモンは、関連付けられている Unified CM Group にあるすべてのサブスクライバから、トランクをゲートキーパーに登録します。

Unified CM クラスタ内のサブスクライバに H.323 コールが着信すると、コールを受け入れるかまたは拒否するか、受け入れる場合はどの H.225D がコールを受信するかなど、さまざまな決定が下されます。図 5-6 は、このプロセスの仕組みを示しています。

図 5-6　H.323 コールの受け入れまたは拒否を判別するプロセス



Unified CM の H.323 プロトコルには、次の追加機能が含まれています。

- Protocol Auto Detect

  この機能では、コールごとに、発信側デバイスが Cisco Unified CM Release 3.2 以降を使用しているかどうかを判別できます。コールを受信するたびに、Unified CM は H.225 User-to-User Information Element（UUIE）を検索します。この UUIE は、もう一方の側が別の Unified CM であるかどうかを示します。UUIE が見つかった場合、Cisco Unified CM は常に Intercluster Trunk Protocol を使用します。UUIE が見つからない場合は、設定済みのプロトコルをそのデバイスに対して使用します。この機能を使用すると、H.225 ゲートキーパー制御トランクは、コールごとに Intercluster Trunk Protocol と H.225 を切り替えることができます。これにより、Unified CM クラスタと他の H.323 デバイスを組み合わせてゲートキーパーを使用することができます。Intercluster Trunk Protocol は、H.225 と類似していますが、特定の機能を Unified CM クラスタ間で正しく動作させる仕組みが異なります。

- Tunneled Q.SIG または H.323 Annex M1

  Cisco Unified CM 4.1(3) のリリースから、この機能はすべての H.323 トランク上で有効にできるようになりました。これにより、特定の H.323 Annex M1 機能を、Unified CM クラスタと、同じく H.323 Annex M1 をサポートする他の確認済みシステムとの間に実装することができます。これらの機能には、次のものがあります。

  - パス交換
  - メッセージ待機インジケータ（MWI）
  - コールバック

- 代替エンドポイント

  この機能をサポートするゲートキーパー、たとえば Cisco Multimedia Conference Manager（MCM）Gatekeeper などに登録する場合、Unified CM はゲートキーパーに対し、H.323 トランクへのコールの代替宛先を通知できます。この代替エンドポイントまたは代替宛先は、この H.323 トランクが呼び出されたときに、ゲートキーパーによって発信側デバイスに送信されます。代替エンドポイントは、ゲートキーパーに登録されている H.323 トランクに関連付けられた Unified CM Group のリストに含まれている他のサブスクライバです。

- 代替ゲートキーパー

  この機能をサポートするゲートキーパーに H.323 トランクが登録される場合（たとえば、Cisco ゲートキーパー クラスタ）、Unified CM には、このゲートキーパーが失敗した場合や独自のリソースを使い果たした場合に、登録、コール アドミッション要求、および他の RAS 機能を処理できる他のゲートキーパーに関する情報が動的に通知されます。

- CanMapAlias

  H.323 トランクは、ゲートキーパーに Admission Request（ARQ; 許可要求）を送信すると、Admission Confirmation message（ACF; アドミッション確認）で異なる E.164 番号を受信する場合があります。このことは、元の着信番号をこの新しい番号で置き換える必要があることを示しています。この機能では、Gatekeeper Transaction Message Protocol（GKTMP）を使用して Cisco ゲートキーパーと通信するルート サーバが必要になります。

  （注） CanMapAlias は、着信番号に関してだけサポートされます。

- 帯域幅要求

  H.323 トランクは、ゲートキーパーの帯域幅情報をアップデートし、特定のコールに割り当てられた帯域幅の要求量が変更されたことを示すことができます。この機能は、デフォルトでは無効になっています。この機能を制御するには、H.323 セクションにある Unified CM サービス パラメータ **BRQ Enabled** を **True** に設定します。この機能は、H.323 トランク上でビデオを使用するとき

に特に重要です。これは、元の帯域幅要求が許容最大限の量を要求するためです。この機能を有効にすると、コール アドミッション制御が、コールのセットアップ中にネゴシエートされた実際の帯域幅を使用することが保証されます。

SIP トランク

H.323 トランクの場合と同様、SIP トランクを配置するときに設計に関して考慮すべき事項がいくつかあります。この項では、これらの設計に関する考慮事項について説明します。

配置に関する一般的な考慮事項

SIP ベース PBX またはサービス プロバイダー IP PSTN 接続など、サードパーティ デバイスとの SIP トランク接続では、Unified CM からの発信コールにディレイド オファーを使用し、Unified CM への着信コールに遅延オファーまたはアーリー オファーのいずれかを使用することをお勧めします。発信コールに遅延オファーを使用すると、MTP リソースを SIP トランクに割り当てる必要がなくなります。ただし、発信側および着信側エンドポイントで DTMF トランスポート タイプが一致しない場合（つまり、Unified CM により MTP が動的に挿入される場合）は例外です。

前述のとおり、Cisco Unified Border Element は、Unified CM から音声サービス プロバイダーへの任意の IP PSTN SIP トランク接続に配置することをお勧めします。

SIP 遅延オファー、アーリー オファーおよび DTMF については、以降の項で詳しく説明しています。

DTMF Transport

DTMF 情報を SIP エンドポイント間で転送する方法はいくつかあります。一般的に、これらの方法は、アウトオブバンド（OOB）およびインバンド シグナリングに分類できます。インバンド DTMF 転送方式では、RTP ストリーム内でそのままの、またはシグナリングされた DTMF トーンのいずれかが送信されます。これらは、発信側または着信側、あるいはその両方のエンドポイントで処理および解釈される必要があります。アウトオブバンド（OOB）シグナリング方式では、DTMF トーンは RTP パス外で、エンドポイントに対して直接転送されるか、必要に応じてこれらのトーンの解釈または転送、あるいはその両方を行う Cisco Unified CM などのコール エージェントを介して転送されます。

アウトオブバンド（OOB）SIP DTMF シグナリング方式には、Unsolicited Notify（UN）、Information（INFO）および Key Press Markup Language（KPML）が含まれます。KPML（RFC 4730）は、シスコが推奨する OOB シグナリング方式ですが、現時点では、市場で広く利用されていません。現在、KPML をサポートするとされる製品は、Cisco Unified CM、Cisco IOS ゲートウェイ（Release 12.4 以降）、および Cisco IP Phone の一部のモデルだけです。Unsolicited Notify は、非標準方式で、Cisco IOS ゲートウェイ（Release 12.2 以降）だけで使用されます。INFO は、Unified CM ではサポートされていません。

インバンド DTMF 転送方式は、RTP メディア ストリームのそのままのトーン、または RFC 2833 を使用した RTP ペイロードのシグナリングされたトーンのいずれかで DTMF トーンを送信します。RFC 2833 は、SIP 製品ベンダーにおいて、主流の DTMF トーン送受信方式となっていて、シスコ音声製品の大部分でサポートされています。

インバンド シグナリング方式では、RTP メディア ストリームの DTMF トーンが送信されるため、セッションの SIP エンドポイントは、使用される転送方式（たとえば、RFC 2833）をサポートするか、このインバンド シグナリングを解釈し変換する方式を提供しなければなりません。2 つのエンポイントで、呼制御に Back-To-Back User Agent（B2BUA）サーバ（たとえば、Cisco Unified CM）が使用されていて、これらのエンドポイントで、各デバイスと呼制御ボックス間で異なる DTMF 方式がネゴシエートされる場合、DTMF の違いをどのように扱うか、つまり、MTP 挿入または OOB 方式のい

ずれを介するかが、この呼制御ボックスにより決定されます。Unified CM では、DTMF 転送方式の不一致（たとえば、インバンドとアウトオブバンド DTMF）は、メディア ターミネーション ポイント（MTP）を挿入することで解決されます。MTP は、インバンド DTMF シグナリング（RFC 2833）で RTP ストリームを終端させ、RTP ストリームから DTMF トーンを抽出して、これらのトーンをアウトオブバンドで Unified CM に転送します。ここで、これらのトーンは、アウトオブバンド シグナリングをサポートするエンドポイントに転送されます。この場合、DTMF 変換ではどの MTP コーデックも使用できるため、MTP は、2 つのエンドポイント間のメディア パスに常に存在します。

インバンド DTMF トーンは、RTP メディア ストリームでそのままの（可聴）トーンとして転送することもできます。ただし、この転送方式は、シスコ製品では広くサポートされていないため、通常、エンドツーエンド DTMF 転送メカニズムとしてはお勧めできません。インバンド オーディオ DTMF トーンは、通常、G.711 a-law または mu-law コーデックを使用した場合だけ、その再生成が信頼できるため、低帯域幅コーデックでの使用には適していません。インバンド オーディオだけが、唯一使用できる DTMF 転送メカニズムである場合、Cisco Unified Border Element を使用して、インバンド オーディオ DTMF シグナリングを RFC 2833 シグナリングに変換できます。

Unified CM SIP トランクでは、DTMF Signaling Method を **No Preference** に設定することをお勧めします。このように設定することで、Unified CM は、最適な DTMF 転送方式を選択し、MTP 割り当てを最小に抑えることができます。

SIP ディレイド オファーおよびアーリー オファー

Cisco Unified CM は、RFC 3264 で定義されているように、SIP セッションの確立に SIP オファー/アンサー モデルを使用します。この場合、オファーは、SIP メッセージ本文で送信される Session Description Protocol（SDP）フィールドに含まれます。このオファーは、通常、デバイスでサポートされるメディア特性（メディア ストリーム、コーデック、方向属性、IP アドレス、使用されるポート）を定義します。オファーを受信するデバイスは、対応する一致メディア ストリームおよびコーデック、これを受け入れるかどうか、メディア ストリーム受信に使用する IP アドレスおよびポートに関するアンサーを、その SIP 応答の SDP フィールドで送信します。Unified CM は、このオファー/アンサー モデルを使用して、主要な SIP 標準、RFC 3261 で定義されているように、SIP セッションを確立します。

RFC 3261 は、SDP メッセージをオファーおよびアンサーで送信できる 2 つの方式を定義します。これらの方式は、一般的にディレイド オファーおよびアーリー オファーとして知られていて、この仕様では、ユーザ エージェント クライアント/サーバにより両方の方式がサポートされていなければなりません。簡単に言うと、メッセージ本文で SDP を使用して送信される初期 SIP Invite は、アーリー オファーを定義し、メッセージ本文で SDP を使用せずに送信される初期 SIP Invite は、遅延オファーを定義します。

アーリー オファーでは、セッションの開始側（発信側デバイス）は、初期 Invite に含まれる SDP でその機能（たとえば、サポートされるコーデック）を送信します（これにより、着信側デバイスは、セッションに適切なコーデックを選択できます）。遅延オファーでは、セッションの開始側は、その機能を初期 Invite で送信せず、着信側デバイスからその機能（たとえば、着信側デバイスでサポートされるコーデックのリスト）が送られるまで待機します（これにより、発信側デバイスは、セッションで使用されるコーデックを選択できます）。

遅延オファーおよびアーリー オファーは、すべての標準ベースの SIP スイッチで使用できる 2 つのメディア機能交換オプションです。ほとんどのベンダーは、遅延オファーまたはアーリー オファーのいずれかを選択しています。また、それぞれに独自の利点や制限事項があります。

（注） Unified CM は、一方で遅延オファーをサポートし、もう一方でアーリー オファーをサポートできます。この機能は、通常、SIP トランクを介して Unified CM に接続する SIP スイッチで、発着信コールに提供および選択されるコーデックを制御する場合に便利です（つまり、Unified CM からの遅延オ

ファー発信および Unified CM へのアーリー オファー着信を使用する場合、サービス プロバイダーは、いかなる場合でもオファーを送信し、これにより、すべてのコールに提供されるコーデックを決定できます)。

アーリーメディア

場合によって、SIP セッションで、2 つの SIP エンドポイント間でのメディア機能交換を終了する前に、メディア パスをセットアップする必要があります。そのため、SIP プロトコルでは、初期オファーがエンドポイントで受信された後で、初期メディアを確立できます。初期メディアを使用する理由は、次のようにいくつかあります。

- 着信側デバイスでは、一定時間を超えるシグナリング遅延が発生したコールに対するオーディオ カットスルー遅延（クリッピング）の効果を軽減させるか、ネットワークベース音声メッセージを発信側に提供する場合に、初期メディア RTP パスを確立します。
- 発信側デバイスでは DTMF または音声での IVR システムにアクセスする場合に、初期メディア RTP パスを確立します。

Unified CM は、アーリー オファーおよびディレイド オファーの両方のコールに対して初期メディアをサポートしています。

（注） 「*アーリー オファー*」と「*初期メディア*」という用語は混乱しやすいですが、同じではないので注意してください。

メディア ターミネーション ポイント

メディア ターミネーション ポイント（MTP）は、通常、Unified CM SIP トランクからの遅延オファー コールには必要ありません。そのため、遅延オファーは、Unified CM SIP トランクからの発信コールのコール セットアップ方式として推奨します。Unified CM からの発信アーリー オファー コールでは、MTP リソースが必要で（SIP トランクの **MTP required** チェックボックスが選択され、提供されるコーデックが選択されている)、これは、コールの期間中、メディア パスに存在します。

Unified CM からのコール発着信では、エンドポイントは、RFC 2833 またはアウトオブバンド DTMF 方式（たとえば、KPML）エンドツーエンドのいずれを使用するかネゴシエートできます。エンドポイント間で共通の DTMF 方式をネゴシエートできない場合、Cisco Unified CM 5.*x* 以降のリリースでは、MTP が動的に挿入されます。Cisco Unified CM 5.*x* 以降リリースは、遅延オファー（SDP を使用しない Invite）をデフォルトでサポートします。遅延オファーは、SIP RFC 3261 仕様の必須部分ですが、SIP アプリケーションによってはサポートされていません。そのような場合は、SIP Trunk 設定で MTP を事前に割り当てておくことにより、SIP トランクでアーリー オファーがサポートされるように設定する必要があります。

MTP は、次の 3 種類の形式で利用できます。

- Cisco IOS ゲートウェイでのソフトウェアベースの MTP。任意の Cisco IOS T-train ソフトウェア リリースで使用できます。Cisco 3845 統合サービス ルータで最大 500 セッション（コール）まで拡張できます。
- Cisco IOS ゲートウェイでのハードウェアベースの MTP。任意の Cisco IOS T-train ソフトウェア リリースで使用できます。ハードウェア MTP は、オンボード DSP リソースを使用し、Cisco ルータ プラットフォームでサポートされる DSP 数に従ってコールを拡張します。
- Cisco Media Convergence Server（MCS）で Cisco IP Voice Media Streaming Application を使用するソフトウェアベースの MTP。

次の設定例は、Cisco IOS ソフトウェアベース MTP の場合の例です。

```
!
```

```
sccp local Vlan5
sccp ccm 10.10.5.1 identifier 5 version 5.0.1
! Communications Manager IP address (10.10.5.1)
sccp
!
sccp ccm group 5
 bind interface Vlan5
 associate ccm 5 priority 1
 associate profile 5 register MTP000E83783C50
! MTP name (MTP000E83783C50) … must match the Unified CM MTP name.
!
dspfarm profile 5 mtp
 description software MTP
 codec g711ulaw
 codec pass-through
 maximum sessions software 500
 associate application SCCP
```

G.729 コーデックがアーリー オファーで選択される場合、Cisco IOS ゲートウェイでソフトウェアまたはハードウェアのいずれかの MTP を使用しなければならないので注意してください。MTP の詳細については、「メディア リソース」（P.6-1）の章を参照してください。

SIP Trunk Transport Protocol

SIP トランクは、メッセージ トランスポート プロトコルとして TCP または UDP のいずれかを使用できます。接続状態を保持する、信頼できるコネクション型のプロトコルとしては、TCP の方が適しています。これは、SIP トランクの遠端の宛先デバイスで障害が発生した場合、そのほぼ直後に、代替トランクへのフェールオーバーが実行されるためです。UDP は、コネクション型プロトコルではないため、SIP トランクの終端の宛先デバイスが利用できないかどうかを判別するときに SIP プロトコル スタックに依存します。UDP ベース SIP トランクの場合、Unified CM は、SIP Invite Retry カウントおよび SIP Trying タイマーの値を使用して、遠端のデバイス障害を検出して、これに対応します。デフォルトでは、フェールオーバーには、コールごとに約 64 秒かかりますが、これらのタイマーを調整して、フェールオーバー時間を許容値まで短縮できます。

SIP トランク タイマーの調整の詳細については、次に示す設定例およびテクニカル ノートを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example09186a008082d76a.shtml

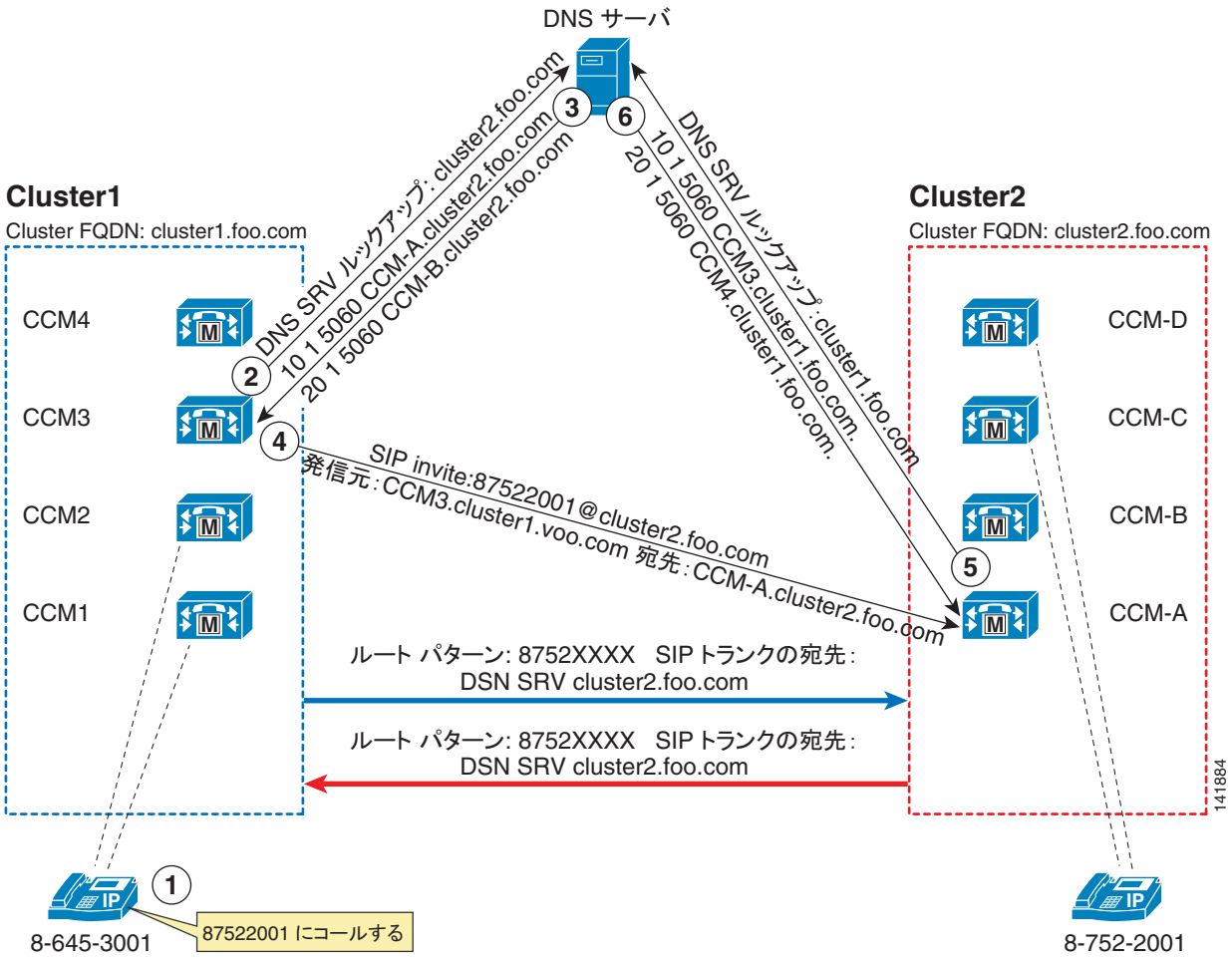
SIP クラスタ間トランク

クラスタ間トランキングに SIP トランクを使用する主な利点の 1 つは、コール存続可能性です。ただし、H.323 トランクと比較した場合、SIP トランクは Annex M1 を使用した QSIG Tunneling をサポートしません。DNS ではなく宛先 IP アドレスを使用する SIP トランクを介した発信コールでは、サブスクライバのロード バランシングは、H.323 トランク コールの場合と同じ方法で実現できます（「発信コールのロード バランシング」（P.5-12）の「H.323」の項を参照してください）。

Cisco Unified CM Release 3.3 以降の H.323 トランクとは異なり、SIP トランクは単一の IP アドレスまたは DNS Server（SRV）レコードだけを指すことができます。DNS SRV 機能のないクラスタ間 SIP トランクにフェールオーバーおよびロード バランシングを提供するためには、複数の SIP トランクを設定します。さらに、その SIP トランクは、ルート グループおよびルート リストのメンバーになる必要があります。また、重要な点として、Unified CM が受け入れるコールが、設定済み SIP トランクのいずれかの宛先アドレスと IP アドレスが一致する SIP デバイスからのコールだけであることにも注意してください。さらに、SIP メッセージの着信ポート番号は、その SIP トランク用に設定されたポート

番号と一致している必要があります。その結果、コールが着信する可能性のある、あらゆる遠端 SIP デバイスのすべての IP アドレスと一致するように、できるだけ多くの SIP トランクに宛先アドレスを設定するようにしてください。この方式は、複数の Unified CM クラスタがある場合には適さないため、その場合は DNS SRV で SIP トランクを使用することをお勧めします。図 5-7 は、DNS SRV を使用したクラスタ間 SIP トランク コールのコール フローを示しています。

図 5-7　DNS SRV を使用したクラスタ間 SIP トランクのコール フロー



注:DNS A ルックアップは、このコール フローから削除されています。

図 5-7 は、このコール フローにおける次の手順を示しています。

1. Cluster1 内の IP Phone が 87522001 にコールします。
2. コールはルート パターン 8752XXXX と一致し、このパターンは cluster2.foo.com の DNS SRV を使用した SIP トランクを指しています。Cluster1 の CCM3 は、このコールを処理するノードです。その SIP トランクはこのノードに登録されているためです。CCM3 は、cluster2.foo.com の DNS SRV ルックアップを送信します。
3. DNS サーバは、CCM-A.cluster2.foo.com と CCM-B.cluster2.foo.com の 2 つのレコードで応答します。CCM-A.cluster2.foo.com のプライオリティの方が高いため、コールはその Unified CM に対して試みられます。SIP Invite が送信される前に、CCM-A.cluster2.foo.com に関して別の DNS ルックアップが行われます。

4. CCM3 は、SIP Invite を 87522001@cluster2.foo.com に送信します。宛先アドレスは CCM-A の IP アドレスに設定されます。
5. Unified CM は、このコールをローカル コールとして解釈します。Uniform Resource Identifier（URI; ユニフォーム リソース識別子）のホスト部分が Cluster FQDN エンタープライズ パラメータと一致しているためです。Cluster2 には、CCM3 の宛先が設定された SIP トランクがありません。したがって、DNS SRV を使用して SIP トランクに設定されたすべてのドメインに対して、DNS SRV ルックアップを行います。その場合、例では cluster1.foo.com の DNS SRV の宛先を持つ単一のトランクが示されています。
6. DNS サーバは 2 つのエントリを返し、そのうちの 1 つが Invite の発信元 IP アドレスと一致します。クラスタはコールを受け入れ、内線 87522001 にコールをルーティングします。

SIP トランクでの SRTP

Secure RTP（SRTP）は、Cisco Unified CM 7.0 以降のリリースでの SIP トランク上でサポートされます。SRTP では、リモート側との暗号化された TLS 接続を使用してトランクを確立する必要があります。SRTP パラメータは、このトランクを介して、SIP SDP メッセージで交換されます。

MTP は SRTP をサポートしていないため、SRTP の場合、トランク設定の MTP Required フラグはオフのままにする必要があります。このフラグをオフにすることで、Unified CM は、遅延オファー コールだけで SRTP をサポートするようになります。ただし、Unified CM により、たとえば、Trusted Relay Point または RSVP エージェントなど、アーリー オファー以外の目的で MTP が動的に挿入される場合、SRTP は MTP を介してサポートされます。

MTP を使用する dtmf-relay は（MTP が、インバンドおよびアウトオブバンド DTMF 信号を変換する必要がある場合）、メディアストリームの DTMF パケットを復号化できないため、SRTP では機能しないので注意してください。

発番号の正規化および SIP トランク

Unified CM 7.0 では、ゲートウェイおよびトランクを介して着信するコールの発番号を正規化形式に変換する機能が導入されました。通常、この形式は、E.164 仕様に従ってグローバルにルーティングできる国際的な番号表現にします。

正規化のプロセスは、着信コールの番号および関連する番号タイプに依存します。番号タイプ パラメータは、発番号のプレフィックスとして付加する適切な番号を選択するときに使用できます。番号タイプは、Unknown、Subscriber、National、または International のいずれかです。これらの番号タイプがどのように使用されるかについての詳細および例については、「ダイヤル プラン」（P.10-1）の章を参照してください。

Unified CM の H.323 トランクおよび H.323 ゲートウェイの設定ページで 4 つの番号タイプのそれぞれに対してプレフィックス番号を指定できます。H.323 では、これらの番号タイプをシグナリング時に転送できます。対照的に、SIP では、番号タイプ情報をそのシグナリング時に転送できません。そのため、SIP トランク上の SIP ゲートウェイを介して Unified CM に着信するコールでは、発番号が local、regional、national のいずれかであるかが示されません。番号タイプ情報がない場合、Unified CM は、発番号に正しいプレフィックスを適用できません。

SIP トランクでは番号タイプを転送できないため、発番号の正規化は、コールが Unified CM に送られる前に実行する必要があります。この変換は、たとえば、着信 SIP ゲートウェイで実行できます。次の設定例は、このような変換を実行するために Cisco IOS ゲートウェイで定義できる変換規則を示しています。

```
voice translation-rule 1
 rule 1 // /+4940/ type subscriber subscriber
 rule 2 // /+49/ type national national
```

```
 rule 3 // /+/ type international international
...
voice translation-profile 1
 translate calling 1
...
dial-peer voice 300 voip
 translation-profile outgoing 1
 destination-pattern .T
 session protocol sipv2
 session target ipv4:9.6.3.12
...
```

上記の例のように設定されている場合、Unified CM との通信に SIP を使用する Cisco IOS ゲートウェイは、+ 記号を含む、E.164 形式に正規化された発信側情報番号を送信します。この Unified CM 設定では、番号タイプが「unknown」のすべてのコールが、このゲートウェイから受信されます。プレフィックスを追加する必要はありません。

変換規則の設定の詳細については、次のサイトから利用できる『*Voice Translation Rules*』マニュアルを参照してください。

http://www.cisco.com/en/US/tech/tk652/tk90/technologies_tech_note09186a0080325e8e.shtml

Unified CM は、発信コールの発番号を、正規化されたグローバル形式に設定できます。SIP トランクから発信されるコールの番号タイプは unknown になります。Cisco IOS ゲートウェイは、除去が行われない場合はこの番号タイプを International に変更し、接続サービス プロバイダーにより要求された場合は除去と番号タイプ変更の両方を実行しなければなりません。

IP トランク上でのコーデック選択

通信エンティティ間でメディアを確立するには、これらのエンティティが、使用する 1 つ以上のコーデックに同意する必要があります。このコーデック（ビデオの場合は複数のコーデック）は、関連エンティティでサポートされる複数のコーデックの同意点、および Unified CM の設定済みポリシーから決定します。Unified CM のポリシーは、リージョン設定で指定されます。オーディオのリージョン内コーデック、およびビデオ（オーディオを含む）のリージョン内帯域幅設定により、それぞれのリージョンに含まれるデバイス間で使用されるコーデックのセットが決まります。このコーデック設定は、これらのリージョンで通信を行うデバイスに許可される最大帯域幅だけを指定するもので、すべてのコールで使用される正確なコーデックを指定するわけではないので注意してください。これらのエンティティで、複数のコーデックを共有し、リージョン間設定で、複数のコーデックの選択が許可されている場合、Unified CM は、品質が最高のコーデックを選択します。

たとえば、トランクと IP Phone 間のリージョン間オーディオ コーデック設定が G.729（低帯域幅コーデック）に設定されていて、両方のエンドポイントで G.729 をサポートしている場合、このコーデックが選択されます。ただし、リージョン間コーデックが G.711（高帯域幅コーデック）に設定されていて、両方のエンドポイントで G.711、G.722、G.729 がサポートされている場合、G.722 が最高のオーディオ品質を提供するため、Unified CM はこのコーデックを選択します。また、例外として、iLBC コーデックが選択されることがあります。両方のエンドポイントで iLBC コーデックをサポートしている場合、このコーデックの使用が可能な場合、およびリージョン内設定でリージョン間の **Link Loss Type** が **lossy** に指定されている場合、iLBC が使用されます。この選択は、最高品質のコーデックを使用するという規則より優先されます。

（注）　**MTP Required** がトランクで選択されている場合、他の設定に関係なく、MTP に指定されるコーデックが使用されます。この場合、リージョン間コーデック設定は、このコーデックを許可するように適切に設定されていなければなりません。

Cisco Unified CM トランクおよび緊急サービス

IP トランクは、緊急 911 コールを送信できない場合があります。また、中央集中型 PSTN トランクのように、発信側のロケーションに適した Public Safety Answering Point（PSAP）に緊急 911 コールを送信できない場合があります。そのため、お客様は、緊急 911 コールおよび発信側のロケーションを適切な PSAP に送信できるかどうか、IP トランク サービス プロバイダーの機能を注意して調査する必要があります。Cisco Emergency Responder を使用すると、緊急 911 コールに対する、ロケーションに固有な発番号を IP トランク サービス プロバイダーに提供できる場合があります。

また、中央集中型 IP または PSTN トランクが、WAN 輻輳または障害のために、リモート ロケーションからの緊急 911 コールに一時的に応答できなくなることもあります。そのため、リモート ロケーションでは、常に、緊急 911 コールを送信できる PSTN へのローカル ゲートウェイを使用できなければなりません。詳細については、「Emergency Services」（P.11-1）を参照してください。

IP トランクを配置するときの設計に関する推奨事項

Cisco Unified CM から IP トランクを配置する場合、次のガイドラインとベスト プラクティスを参考にしてください。

- トランク プロトコルを選択します。使用しているシステムの要件および必要な機能に基づいて、H.323 または SIP のいずれのトランクを使用するかを選択します。たとえば、PBX との接続に Q.SIG トンネリングが必要な場合は H.323 を使用します。また、トランクの選択は、配置した Unified CM のバージョンにより異なる場合もあります。SIP トランク機能は、通常、Unified CM 5.1(2) 以降のリリースで拡張されているため、これらのいずれかのバージョンを使用する場合 SIP を選択してください。
- Unified CM 4.*x* での SIP トランクでは、常に、発信コールに MTP が必要です。また、これらのトランクは、音声通信の場合は G.711 コーデックに限定されます。予測される同時コール数に対応できるだけの十分な MTP リソースを確保するようにしてください。
- Unified CM 5.*x* 以降のリリースでの SIP トランクでは、各発信コールに MTP を割り当てるかどうかを選択できます。デフォルトでは、MTP は使用されません。リモート エンドでアーリー オファー（初期 INVITE の オファー SDP）が必要ない場合、ディレイド オファーを使用して、MTP リソース使用を最適化してください。
- 監視されている場合、音声クリッピングは、トランクで PRACK を有効にすることで、最小化または削減できます。このパラメータは、Cisco CallManager サービスの Service Parameters で有効にすることができます（SIP Rel1XX Enabled）。
- セキュリティ設定や SIP トランクを介して受け入れられるメッセージのタイプなどの他の操作パラメータは、SIP Trunk Security Profile で有効にすることができます。ここでは、TLS およびダイジェスト認証のパラメータだけでなく、トランクが Presence Subscription、Out-Of-Dialog REFER メッセージ、Replaces ヘッダー、または Unsolicited Notification を受け入れるかどうかを指定するパラメータも設定できます。
- サービス プロバイダー ネットワークに接続する場合、Cisco Unified Border Element を使用することをお勧めします。企業とサービス プロバイダーのネットワーク間への境界ポイント提供のほか、Cisco Unified Border Element は、2 つのネットワーク間での SIP シグナリング相互運用性の拡張にも使用できます。

- Unified CM 7.*x* では、G.711 のほかに、低帯域幅コーデック G.729 をアーリー オファーで使用できます。ただし、アーリー オファーでシグナリングできるのは、これらのコーデックのいずれか 1 つだけです。アーリー オファーでの複数のコーデックの使用、または Unified CM から遅延オファー コールへのアーリー オファー コールへの変換は、Cisco Unified Border Element の Delayed Offer to Early Offer 機能により実行できます。
- SIP トランクを介して SRTP を使用する場合、Unified CM でサポートされる唯一のモードは、遅延オファーです。

CHAPTER 6

メディア リソース

メディア リソースとは、ソフトウェア ベースまたはハードウェア ベースのエンティティであり、接続中のデータ ストリームに対してメディア処理を行うものです。メディア処理機能には、複数のストリームを混合して 1 つの出力ストリームを作成する機能（会議）、ある接続から別の接続（メディア ターミネーション ポイント）にストリームを渡す機能、ある圧縮タイプから別の圧縮タイプにデータ ストリームを変換する機能（トランスコーディング）、エコー キャンセレーション、シグナリング、TDM 回線からの音声ストリームの終端（コーディング/デコーディング）、ストリームのパケット化、オーディオのストリーミング（Annunciator）などが含まれます。

この章を使用して、以下で説明するメディア リソースが配置に必要かどうかを判断してください。また、必要なリソースがソフトウェアベースの機能で提供できるか、リソースを実装するために Digital Signal Processor（DSP; デジタル シグナル プロセッサ）をプロビジョニングする必要があるかを判断してください。リソースについては個別の項で説明しますが、上位機能を実装するために、同じ基本リソース（DSP と Cisco IP Voice Media Streaming Application）が共有されることがあります。

この章では、次の機能を中心に説明します。

- 「音声インターフェイス」（P.6-2）
- 「オーディオ会議」（P.6-10）
- 「ビデオ会議」（P.6-14）
- 「セキュア会議」（P.6-15）
- 「トランスコーディング」（P.6-16）
- 「メディア ターミネーション ポイント（MTP）」（P.6-19）
- 「SIP トランク」（P.6-22）
- 「H.323 トランクおよびゲートウェイ」（P.6-24）
- 「Trusted Relay Point」（P.6-27）
- 「Annunciator」（P.6-27）
- 「Cisco RSVP Agent」（P.6-29）
- 「Cisco IP Voice Media Streaming Application」（P.6-29）

次の機能の詳細については、それぞれの項を参照してください。

- 「Music on Hold」（P.7-1）
- 「Unified CM の RSVP 対応ロケーション」（P.9-18）

ハードウェアおよびソフトウェアの依存関係の詳細については、「ハードウェアおよびソフトウェアのキャパシティ」（P.6-30）の項を参照してください。

Cisco Unified Communications Manager（Unified CM）のメディア リソースは、メディア リソース グループおよびメディア リソース グループ リストを使用して制御できます。リソースのプールを作成すると、使用する特定のハードウェアまたはソフトウェアを制御できます。プールを使用して、物理的な場所に基づいてリソースをグループ化することをお勧めします。さまざまなコール処理モデルに基づく設計ガイドラインについては、「一般的な設計ガイドライン」（P.6-33）の項を参照してください。

この章の新規情報

表 6-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 6-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
WS-SVC-CMM-ACT および WS-6608-T1/WS-6608-E1 モジュールのオーディオ会議に関するキャパシティ	「オーディオ会議のリソース」（P.6-11）
Cisco 2900 および 3900 シリーズの Integrated Services Router Generation 2（ISR G2; サービス統合型ルータ第 2 世代）	「Cisco 2900 および 3900 シリーズ プラットフォーム」（P.6-31）
Cisco IOS メディア リソース	「Cisco IOS ベースのメディア リソースの冗長性とフェールオーバーに関する考慮事項」（P.6-10）
カンファレンス ブリッジでの MTP の使用	「カンファレンス ブリッジでの MTP の使用」（P.6-26）
PVDM3 DSP	表 6-3 表 6-8 この章の各項で説明
推奨される DSP プロファイルの設定	「トランスコーディング リソース」（P.6-17）
セキュア会議	「セキュア会議」（P.6-15）
Trusted Relay Point（TRP）	「Trusted Relay Point」（P.6-27）
G.729 コーデック用の MTP としてのハードウェア DSP の使用	「MTP リソース」（P.6-26）
ビデオ会議	「ビデオ会議」（P.6-14）
音声品質	「メディアの機能と音声品質」（P.6-34）

音声インターフェイス

音声インターフェイスは、Time-Division Multiplexing（TDM; 時分割多重）インターフェイス上のレッグと VoIP（Voice over IP）接続上のレッグの 2 つのコール レッグを持つコールに適用されます。TDM レッグは、コーディング/デコーディングとストリームのパケット化を実行するハードウェアで必ず終端します。この終端機能は、同じハードウェア モジュール、ブレード、またはプラットフォーム上にあるデジタル シグナル プロセッサ（DSP）リソースによって実行されます。Cisco TDM ゲートウェイ上の DSP ハードウェアはすべて、音声ストリームを終端できます。また、特定のハードウェアは、会議やトランスコーディングなどの他のメディア リソース機能を実行することもできます（「オーディオ会議」（P.6-10）および「トランスコーディング」（P.6-16）を参照）。

表 6-4 ～ 表 6-9 は、各ハードウェア プラットフォームでサポートできるコールの数を示しています。この数は、ハードウェア上の DSP チップセットのタイプと DSP の個数によって決まります。ハードウェアには、アップグレードおよび変更ができない固定 DSP リソース、またはアップグレード可能なモジュラ DSP リソースのどちらかが搭載されています。表 6-4 ～表 6-9 は、モジュラ（アップグレード可能な）ハードウェアに関する、ハードウェア モジュールごとの DSP の最大数も示しています。

サポートされるコールの数は、コールに使用されるコーデックの計算の複雑度や、DSP に設定された複雑度モードによって異なります。Cisco IOS を使用すると、ハードウェア モジュールの複雑度モードを設定できます。ハードウェア プラットフォームは、中複雑度と高複雑度の 2 つの複雑度モードを持つものと、中複雑度と高複雑度のほかにフレックス モードを持つものもあります。

中複雑度モードと高複雑度モード

モジュールでサポートできるコール数を確認するには、表 6-4 ～表 6-9 でモジュールを見つけ、モジュールに搭載できる DSP の個数と、必要なコーデック タイプを確認します。たとえば、フレックス モードに設定された 3 つの C5510 DSP を持つ NM-HD-2VE モジュールは、DSP ごとに 8 つの G.729 コールをサポートできます。合計すると、フレックス モードで G.729 コーデックを使用して 24 コールをサポートできます。フレックス モードで G.711 コーデックを使用する場合は、同じハードウェアで 48 コールをサポートできます。

表 6-2 に示されているように、中複雑度モードでサポートされている場合、コーデックは、高複雑度モード設定された DSP でもサポートされます。ただし、サポートされるコール数は減少します。

各 DSP は、中複雑度モード、高複雑度モード、またはフレックス モード（C5510 のみ）のいずれかとして個別に設定できます。DSP は、コールのコーデックに関する実際の複雑度に関係なく、設定されている複雑度に応じてすべてのコールを処理します。着信コールの実際の複雑度と同じかそれ以上の複雑度が設定されたリソースが使用可能になっている必要があります。そうでない場合、コールは失敗します。たとえば、コールに高複雑度コーデックが必要な場合、DSP リソースが中複雑度モードに設定されていると、コールは失敗します。ただし、高複雑度モードに設定された DSP に対して中複雑度コールが試行された場合、コールは成功し、Cisco IOS は高複雑度モードのリソースを割り当てます。

サポートされているコールの最大数を確認するには、目的のハードウェアを含む表 6-4 ～表 6-9 で該当する行を見つけます。C5510 に基づく DSP の場合は、表 6-2 で中複雑度と高複雑度の列を調べて、目的のコーデックを処理できる複雑度モードを確認します。次に、目的の複雑度モードで、DSP ごとにサポートされているコールの最大数を確認します。PVDM3 DSP の場合は、表 6-3 を使用します。PVDM3 の中複雑度の動作モードには、この表でリストされている低複雑度コーデックと中複雑度コーデックの両方が含まれることに注意してください。

フレックス モード

フレックス モードは、C5510 チップセットを使用するハードウェア プラットフォーム上、および PVDM3 DSP 上だけで使用可能であり、このモードでは、設定時にコーデックの複雑度を指定する必要がありません。フレックス モードの DSP は、処理能力が足りる限り、サポートされているすべてのコーデック タイプのコールを受け入れます。各コールのオーバーヘッドは、Millions of Instructions Per Second（MIPS）単位の処理能力を計算することで動的にトラッキングされます。Cisco IOS は、受信されたコールごとに MIPS の計算を実行し、新しいコールが開始されるたびにそのバジェットから MIPS クレジットを差し引きます。表 6-2 の Flex Mode 列に示されているように、1 つのコールによって消費される MIPS 数は、コールのコーデックによって異なります。着信コールに必要な MIPS 以上の MIPS クレジットが残っている限り、DSP は新しいコールを許可します。表 6-2 の Flex Mode 列は、サポートされているコーデックをコールごとの MIPS 数別に分類し（コールごとに 15、30、または 40 MIPS）、各種ハードウェアに使用可能な MIPS バジェットを示しています。

同様に、PVDM3 DSP モジュールでは、クレジットベースのシステムを使用します。各モジュールには、メディア ストリームを処理するモジュールのキャパシティの単位を表す固定数の「クレジット」が割り当てられています。音声インターフェイス、トランスコーディングなどの各メディア動作には、クレジットによるコストが割り当てられています。DSP リソースは、メディア処理用に割り当てられているので、そのコスト値は、使用可能なクレジットから差し引かれます。使用可能なクレジットを使い果たすと、DSP モジュールのキャパシティがなくなり、要求された操作に対応するには不十分となります。PVDM3 DSP のクレジット割り当て規則は、より複雑です。適切なサイジングを行うには、Cisco Unified Communications Sizing Tool（Unified CST）を使用します。適切なログイン認証を持つシスコの従業員またはシスコ代理店は、このツールを http://tools.cisco.com/cucst で入手できます。

フレックス モードは、同じハードウェアで複数のコーデックのコールをサポートする必要がある場合に便利です。これは、フレックス モードでは、DSP が中複雑度または高複雑度として設定されている場合よりも多くのコールをサポートできるためです。ただし、フレックス モードではリソースのオーバーサブスクリプションが許可されています。オーバーサブスクリプションになると、すべてのリソースが使用された場合にコール障害が発生するリスクが生じます。フレックス モードを使用すると、物理 TDM インターフェイスを使用する場合よりも DSP リソースの数を削減できます。

たとえば、各 DSP のバジェットは 240 MIPS となり、バジェットの合計は NM-HD-2VE モジュールごとに 720 MIPS となります。NM-HDV2 モジュールの場合、DSP ごとのバジェットは同じく 240 MIPS ですが、使用可能な MIPS の合計数については、選択項目や PVDM の数によって異なるため、表 6-4 で確認してください。

中複雑度モードまたは高複雑度モードと比べると、フレックス モードには、DSP ごとに最も多くの G.711 コールをサポートできるという利点があります。中複雑度モードでは、DSP は 8 つの G.711 コールをサポートできますが、フレックス モードでは 16 の G.711 コールをサポートします。

音声インターフェイスの DSP リソース

表 6-4 ～表 6-9 は、DSP チップセット別に分類されており、DSP サポートに関する情報を、プラットフォーム、DSP 密度、および DSP ごとにサポートされる音声インターフェイス（またはコール）の数別に示しています。表 6-2 および表 6-3 は、ハードウェア モジュールでサポートされるコーデックを複雑度モードごとに示しています。

表 6-2　C5510 DSP によってサポートされるコーデック（複雑度モード別）

中複雑度	高複雑度	フレックス モード
G.711（a-law、mu-law）	G.711（a-law、mu-law）	*コールごとに 15 MIPS の場合：*
FAX/モデム パススルー	FAX/モデム パススルー	• G.711（a-law、mu-law）
クリア チャネル	クリア チャネル	• FAX/モデム パススルー
G.726（32K、24K、16K）	G.726（32K、24K、16K）	• クリア チャネル
FAX リレー	FAX リレー	*コールごとに 30 MIPS の場合：*
G.729（a、ab）	G.729	• G.726（32K、24K、16K）
	G.729（a、b、ab）	• FAX リレー
	G.728	• G.729
	G.723.1（32K、24K、16K）	• G.729（a、b、ab）
	G.723.1a（5.3K、6.3K）	*コールごとに 40 MIPS の場合：*
	モデム リレー	• G.728
		• G.723.1（32K、24K、16K）
		• G.723.1a（5.3K、6.3K）
		• モデム リレー

表 6-3　PVDM3 DSP によってサポートされるコーデック（複雑度モード別）

低複雑度	中複雑度	高複雑度	超高複雑度
G.711（a-law、mu-law）	G.726	G.729	iSAC
FAX パススルー	FAX リレー	G.729B	
モデム パススルー	G.729A	G.723	
クリア チャネル	G.729AB	G.728	
	G.722	モデム リレー	
	GSMFR	iLBC	
		GSMEFR	

C5510 チップセットをベースとするハードウェアは、中複雑度モードと高複雑度モードのほか、フレックス モードをサポートします（表 6-4 を参照）。

表 6-4　C5510 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュールまたはシャーシ	DSP 構成	DSP およびモジュールごとの音声インターフェイス（コール）の最大数		
		中複雑度（DSP ごとに 8 コール）	高複雑度（DSP ごとに 6 コール）	フレックス モード[1]（DSP ごとに 240 MIPS）
VG-224	4 DSP で固定	適用対象外	プラットフォームごとに 24 コール サポートされるコーデック： • G.711（a-law、mu-law） • G.729a	適用対象外
NM-HD-1V[2]	1 DSP で固定	NM ごとに 4 コール	NM ごとに 4 コール	NM ごとに 240 MIPS
NM-HD-2V	1 DSP で固定	NM ごとに 8 コール	NM ごとに 6 コール	NM ごとに 240 MIPS
NM-HD-2VE	3 DSP で固定	NM ごとに 24 コール	NM ごとに 18 コール	NM ごとに 720 MIPS
NM-HDV2 NM-HDV2-2T1/E1 NM-HDV2-1T1/E1	次の DSP を 1 ～ 4 つ： PVDM2-8[3]（½ DSP） PVDM2-16（1 DSP） PVDM2-32（2 DSP） PVDM2-48（3 DSP） PVDM2-64（4 DSP）	PVDM ごとのコール数： 4 8 16 24 32	PVDM ごとのコール数： 3 6 12 18 24	PVDM ごとの MIPS： 120 240 480 720 960
2801 2811	次の DSP を 1 ～ 2 つ： PVDM2-8[3]（½ DSP） PVDM2-16（1 DSP） PVDM2-32（2 DSP） PVDM2-48（3 DSP） PVDM2-64（4 DSP）	PVDM ごとのコール数： 4 8 16 24 32	PVDM ごとのコール数： 3 6 12 18 24	PVDM ごとの MIPS： 120 240 480 720 960
2821 2851	次の DSP を 1 ～ 3 つ： PVDM2-8[3]（½ DSP） PVDM2-16（1 DSP） PVDM2-32（2 DSP） PVDM2-48（3 DSP） PVDM2-64（4 DSP）	PVDM ごとのコール数： 4 8 16 24 32	PVDM ごとのコール数： 3 6 12 18 24	PVDM ごとの MIPS： 120 240 480 720 960
3825 3845	次の DSP を 1 ～ 4 つ： PVDM2-8[3]（½ DSP） PVDM2-16（1 DSP） PVDM2-32（2 DSP） PVDM2-48（3 DSP） PVDM2-64（4 DSP）	PVDM ごとのコール数： 4 8 16 24 32	PVDM ごとのコール数： 3 6 12 18 24	PVDM ごとの MIPS： 120 240 480 720 960

1. フレックス モードでは、サポートされるコールの最大数は、コールごとに使用される MIPS 数によって異なります（表 6-2 を参照）。
2. NM-HD-1V モジュールを使用する場合、音声インターフェイス（コール）の数は、モジュール上の物理ポートの数によって制限されます。
3. PVDM2-8 のキャパシティは C5510 の半分です。

C5421 チップセットをベースとするハードウェアでは、DSP が中複雑度または高複雑度として設定することができます。表 6-5 は、DSP ごとのコール密度を、表 6-2 は、複雑度モードごとにサポートされるコーデックを示しています。

表 6-5　C5421 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュール	DSP 構成	DSP およびモジュールごとのコールの最大数	
		中複雑度（DSP ごとに 8 コール）	高複雑度（DSP ごとに 8 コール）
NM-HDA-4FXS	2 DSP で固定 *または* 1 つの DSP-HDA-16（4 DSP）で固定	NM ごとに 16 コール NM ごとに 16 コール	NM ごとに 8 コール NM ごとに 16 コール
AIM-VOICE-30 AIM-ATM-VOICE-30	4 DSP で固定	AIM ごとに 30 または 60 コール	AIM ごとに 16 または 30 コール

C549 チップセットをベースとするハードウェアでは、DSP が中複雑度または高複雑度として設定することができます。表 6-6 は、DSP ごとのコール密度を、表 6-2 は、複雑度モードごとにサポートされるコーデックを示しています。

表 6-6　C549 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュール	DSP 構成	DSP およびモジュールごとのコールの最大数	
		中複雑度（DSP ごとに 4 コール）	高複雑度（DSP ごとに 2 コール）
NM-HDV NM-HDV-FARM	1 ～ 5 つの PVDM-12（PVDM-12 ごとに 3 DSP）	NM ごとに 12、24、36、48、または 60 コール	NM ごとに 6、12、18、24、または 30 コール
1751[1] 1760	次の DSP を 1 ～ 2 つ： PVDM-256K-4（1 DSP） PVDM-256K-8（2 DSP） PVDM-256K-12（3 DSP） PVDM-256K-16HD（4 DSP） PVDM-256K-20HD（5 DSP）	NM ごとのコール数： 4 または 8 8 または 16 12 または 24 16 または 32 20	NM ごとのコール数： 2 または 4 4 または 8 6 または 12 8 または 16 10
	次の個数で固定：	PA ごとのコール数：	PA ごとのコール数：
PA-VXA-1TE1-24+	7 DSP	28	14
PA-VXA-1TE1-30+	8 DSP	32	16
PA-VXB-2TE1+	12 DSP	48	24
PA-VXC-2TE1+	30 DSP	120	60
PA-MCX-2TE1 PA-MCX-4TE1 PA-MCX-8TE1	固定（オンボード DSP なし）	PA-VX(*x*) によって異なる[2]	PA-VX(*x*) によって異なる[2]

1. 1751 は、最大 8 つの DSP（32 チャネル）をサポートします。また、これらのモジュールは、2 の倍数単位の PVDM を指定して発注できます。ただし、合計で 31 チャネルを超えることはできません。部品番号は、チャネル数を示しています。
2. マルチチャネル ポート アダプタは、混合バックプレーン全体で PA-VXA、PA-VXB、または PA-VXC の未使用の DSP を使用します。

C542 チップセットをベースとするハードウェアは、次のコーデックをサポートします。

- G.711（a-law、mu-law）
- FAX/モデム パススルー
- クリア チャネル
- G.726（32K、24K、16K）
- FAX リレー
- G.729
- G.729（a、b、ab）
- G.728
- G.723.1（32K、24K、16K）
- G.723.1a（5.3K、6.3K）
- モデム リレー

表 6-7 は、DSP ごとのコール密度を示しています。

表 6-7　C542 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュール[1]	DSP 構成	DSP およびモジュールごとのコールの最大数
NM-1V	2 DSP で固定	DSP ごとに 1 コール NM ごとに 2 コール
NM-2V	4 DSP で固定	DSP ごとに 1 コール NM ごとに 4 コール

1. これらのモジュールは、複雑度モードを備えていませんが、すべてのコーデックを均等にサポートします。

表 6-8 は、PVDM3 DSP ごとのコール密度を示しています。

表 6-8　Cisco IOS ISR G2 プラットフォーム上の PVDM3 DSP での音声インターフェイス

ハードウェア プラットフォーム[1]	DSP 構成	DSP あたりの最大コール数			
		低複雑度コーデック	中複雑度コーデック	高複雑度コーデック	超高複雑度コーデック
2901 2911	次の DSP を 1 ～ 2 つ： PVDM3-16 PVDM3-32 PVDM3-64 PVDM3-128 PVDM3-192 PVDM3-256	 16 32 64 128 193 258	 12 22 44 97 140 194	 10 14 28 60 89 121	 8 12 24 50 74 101
2921 2951	次の DSP を 1 ～ 3 つ： PVDM3-16 PVDM3-32 PVDM3-64 PVDM3-128 PVDM3-192 PVDM3-256	 16 32 64 128 193 258	 12 22 44 97 140 194	 10 14 28 60 89 121	 8 12 24 50 74 101
3925 3945	次の DSP を 1 ～ 4 つ： PVDM3-16 PVDM3-32 PVDM3-64 PVDM3-128 PVDM3-192 PVDM3-256	 16 32 64 128 193 258	 12 22 44 97 140 194	 10 14 28 60 89 121	 8 12 24 50 74 101

1. Cisco 2900 および 3900 シリーズの Integrated Services Router（ISR; サービス統合型ルータ）は、PVDM2 DSP もサポートしています。これらの DSP でのさまざまな複雑度モードにおけるコール キャパシティは、Cisco 2800 および 3800 シリーズの ISR と同じです。Cisco 2900 および 3900 シリーズの ISR マザーボード上の DSP スロットに PVDM2 DSP を挿入するには、アダプタが必要となります。

表 6-9 は、DSP リソースに対応する非 IOS ハードウェアを示しています。すべての非 IOS ハードウェア プラットフォームでは、DSP 構成が固定されています（表 6-9 を参照）。

表 6-9　非 IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュールまたはプラットフォーム	DSP 構成	DSP およびモジュールごとのコールの最大数	サポートされるコーデック
WS-6608-T1 WS-6608-E1	64 の C549 で固定 （ポートごとに 8 つの DSP、カードごとに 8 つのポート）	DSP ごとに 4 コール モジュールごとに 256 コール[1]	G.711 a-law、mu-law G.729a
WS-6624-FXS	12 の C549 で固定	DSP ごとに 2 コール モジュールごとに 24 コール	G.711 a-law、mu-law G.729a

表 6-9　非 IOS ハードウェア プラットフォーム上の DSP リソース （続き）

ハードウェア モジュールまたはプラットフォーム	DSP 構成	DSP およびモジュールごとのコールの最大数	サポートされるコーデック
VG-248	12 の C5409 で固定	DSP ごとに 4 コール プラットフォームごとに 48 コール	G.711 a-law、mu-law G.729a
WS-SVC-CMM-ACT	4 つの Broadcom 1500 で固定	DSP ごとに 32 コール モジュールごとに 128 コール	G.711（10 ～ 30 ms） G.729（10 ～ 60 ms） G.723（30 ～ 60 ms）
WS-SVC-CMM-6T1	12 の C5441 で固定	DSP ごとに 15 コール モジュールごとに 144 コール	G.711（10、20、30 ms） G.729（10、20、30、40、50、60 ms）
WS-SVC-CMM-6E1	12 の C5441 で固定	DSP ごとに 15 コール モジュールごとに 180 コール	G.711（10、20、30 ms） G.729（10、20、30、40、50、60 ms）
WS-SVC-CMM-24FXS	3 つの C5441 で固定	DSP ごとに 15 コール モジュールごとに 24 コール	G.711 a-law、mu-law G.729 G.729a
ATA-188[2]	1 つの Komodo 3880 で固定	プラットフォームごとに 2 コール	G.711 a-law、mu-law G.729

1. 物理ポートの数に基づいて、T1 の場合は最大 192 コール、E1 の場合は最大 240 コールが可能です。T1 または E1 に対して DSP が設定されていない場合は、最大 256 の DSP リソースが使用可能です。
2. ATA モジュールには複雑度が定義されていません。このモジュールは G.711、G.729、および G.723 のみをサポートします。

Cisco IOS ベースのメディア リソースの冗長性とフェールオーバーに関する考慮事項

メディア リソースに関する高可用性設計には、冗長なメディア リソースを含める必要があります。これらのリソースが Cisco IOS ベースのリソースである場合は、単一プラットフォームの障害を防ぐために各リソースを複数の Cisco IOS プラットフォームに分散できます。また、各リソースを異なるプライマリ Unified CM サーバに登録することも可能です。

Cisco IOS は、フェールオーバー機能のモードとして「グレースフル」と「即時」の 2 種類をサポートしています。デフォルトのフェールオーバー方法はグレースフルで、この場合はすべてのメディア アクティビティが停止して初めてリソースがバックアップ Unified CM サーバに登録されます。それに対して即時フェールオーバーでは、プライマリの障害が検出されるとすぐにリソースがバックアップ Unified CM サーバに登録されます。冗長性のない 1 組のメディア リソースしかない状況では、即時フェールオーバーを使用することをお勧めします。

オーディオ会議

カンファレンス ブリッジとは、複数の参加者を 1 つのコールに参加させるリソースです。そのデバイス上で 1 つの会議に許可される最大ストリーム数まで、所定の会議用に任意の数の接続を受け入れることができます。会議に接続されているメディア ストリームと、その会議に接続されている参加者との間には、1 対 1 の対応があります。カンファレンス ブリッジは、ストリームを混合し、接続されている通話者ごとに固有の出力ストリームを作成します。所定の通話者の出力ストリームは、接続されている

全通話者からのストリームの合成から、当事者の入力ストリームを除いたものです。一部のカンファレンス ブリッジは、会議で通話量が最も多い 3 名の通話者だけを混合し、その合成ストリーム（通話量が最も多い通話者の 1 人である場合は、当事者の入力ストリームをマイナスしたもの）を各参加者に配信します。

オーディオ会議のリソース

ハードウェア カンファレンス ブリッジは、ソフトウェア カンファレンス ブリッジのすべての機能を備えています。さらに、一部のハードウェア カンファレンス ブリッジは、G.729 や G.723 などの複数の Low Bit-Rate（LBR; 低ビット レート）ストリーム タイプをサポートできます。この機能により、一部のハードウェア カンファレンス ブリッジが混合モードの会議を処理できるようになります。混合モードの会議では、ハードウェア カンファレンス ブリッジは、G.729 および G.723 のストリームを G.711 ストリームにトランスコードし、混合します。その後、混合したストリームを、ユーザに戻すために適切なストリーム タイプにエンコードします。G.711 会議しかサポートしないハードウェア カンファレンス ブリッジもあります。

Unified CM の制御下にあるすべてのカンファレンス ブリッジは、Unified CM との通信に Skinny Client Control Protocol（SCCP）を使用します。

Unified CM は、Unified CM クラスタに登録されている会議リソースから、カンファレンス ブリッジを割り当てます。ハードウェアとソフトウェアの両方の会議リソースを同時に Unified CM に登録でき、Unified CM は、どちらのリソースからでも、カンファレンス ブリッジを割り当て、使用することができます。Unified CM は、会議割り当て要求を処理するときに、これらのカンファレンス ブリッジのタイプを区別しません。

リソースがサポートできる会議の数、および 1 つの会議の最大参加者数は、リソースによって異なります。

Unified CM システムでは、次のタイプのカンファレンス ブリッジ リソースが使用されます。

- 「ソフトウェア オーディオ カンファレンス ブリッジ（Cisco IP Voice Media Streaming Application）」（P.6-11）
- 「ハードウェア オーディオ カンファレンス ブリッジ（Cisco NM-HDV2、NM-HD-1V/2V/2VE、2800 シリーズおよび 3800 シリーズ ルータ）」（P.6-12）
- 「ハードウェア オーディオ カンファレンス ブリッジ（PVDM3 DSP を搭載した Cisco 2900 シリーズおよび 3900 シリーズ ルータ）」（P.6-12）
- 「ハードウェア オーディオ カンファレンス ブリッジ（Cisco WS-SVC-CMM-ACT）」（P.6-13）
- 「ハードウェア オーディオ カンファレンス ブリッジ（Cisco NM-HDV および 1700 シリーズ ルータ）」（P.6-13）
- 「ハードウェア オーディオ カンファレンス ブリッジ（Cisco Catalyst WS-X6608-T1 および WS-X6608-E1）」（P.6-13）
- 「組み込み会議」（P.6-14）
- 「ビデオ会議」（P.6-14）

ソフトウェア オーディオ カンファレンス ブリッジ（Cisco IP Voice Media Streaming Application）

ソフトウェア ユニキャスト カンファレンス ブリッジは、G.711 音声ストリームと Cisco Wideband オーディオ ストリームを混合できる標準の会議ミキサーです。Wideband または G.711 a-law および mu-law ストリームの任意の組み合せが、同じ会議に接続される場合があります。所定の設定でサポートできる会議数は、カンファレンス ブリッジ ソフトウェアが実行されるサーバと、アプリケーションで有効になっている他の機能によって決まります。Cisco IP Voice Media Streaming Application は、複数の機能に使用することもできるリソースで、設計ではすべての機能を同時に考慮する必要があります（「Cisco IP Voice Media Streaming Application」（P.6-29）を参照）。

ハードウェア オーディオ カンファレンス ブリッジ（Cisco NM-HDV2、NM-HD-1V/2V/2VE、2800 シリーズおよび 3800 シリーズ ルータ）

Cisco IOS で会議リソースとして設定されている DSP は、会議機能のみに特化した DSP にファームウェアをロードします。このような DSP は、他のメディア機能には使用できません。

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- C5510 DSP チップセットに基づき、NM-HDV2 およびルータ シャーシは PVDM2 モジュールを使用して DSP を提供します。
- PVDM2 ハードウェアの DSP は、音声インターフェイス、会議、メディア ターミネーション、またはトランスコーディングとして個別に設定されます。そのため、1 つの PVDM の複数の DSP を異なるリソース タイプとして使用できます。DSP は、まず音声インターフェイスに割り当ててから、必要に応じて他の機能に割り当ててください。
- NM-HDV2 には、任意の組み合せで PVDM2 モジュールを取り付け可能な 4 つのスロットがあります。その他のネットワーク モジュールの DSP 数は固定されています。
- これらの DSP に基づく会議には、最大 8 人が参加できます。会議が始まるときに、8 つのポジションのすべてが予約されます。Cisco IOS Release 12.4(15)T から、この参加者数の上限は 32 に増えました。
- PVDM2-8 には、PVDM2-16 と比較して処理キャパシティが半分の DSP があるため、½ DSP と表示されています。たとえば、PVDM2-8 の DSP が G.711 用に設定されている場合、(0.5 × 8) ブリッジ/DSP = 4 カンファレンス ブリッジを提供できます。
- 表 6-2 および表 6-4 を使用して、特定のハードウェアでプロビジョニングできる DSP の数を判断してください。
- Cisco IOS の DSP ファーム設定によって、ファームで受け付けることができるコーデックを指定します。会議および G.711 用に設定されている DSP ファームは、8 つの会議を提供します。G.711 コールと G.729 コールの両方を受け付けるように設定されている場合、ストリームのトランスコーディングの実行用にリソースが予約されるため、1 つの DSP で 2 つの会議が提供されます。
- NM-HDV2 の I/O は 400 ストリームに制限されています。そのため、割り当てられている会議リソースの数がこの制限を超えないように注意してください。G.711 会議が設定されている場合、（48 × 8）参加者 = 384 ストリームになるため、1 つの NM に割り当てることができる DSP は 6（参加者がそれぞれ 8 人の合計 48 の会議）までです。すべての会議を G.711 コーデックと G.729 コーデックの両方に設定した場合、各 DSP は、参加者がそれぞれ 8 人の会議を 2 つだけ提供します。この場合、NM に搭載できる最大 16 の DSP が設定されると、256 ストリームが可能になります。
- 会議は、GSM コーデックを利用したコールをネイティブに受け付けることはできません。これらのコールが会議に参加するには、個別にトランスコーダが必要です。
- NM-HDV2 などの PVDM2 ベースのハードウェアは、単一のシャーシで同時に音声インターフェイスに使用できますが、同時に他のメディア リソース機能には使用できません。PVDM-256K および PVDM2 に基づく DSP は、異なる DSP ファーム設定を持つため、ルータで同時に設定できるのは 1 つだけです。

ハードウェア オーディオ カンファレンス ブリッジ（PVDM3 DSP を搭載した Cisco 2900 シリーズおよび 3900 シリーズ ルータ）

各 DSP タイプによってサポートされる会議の数は、各会議の参加者数とその会議で使用されるコーデックの関数です。各メディア処理機能（DSP によってホストされる会議を含む）では、使用可能なクレジットの一部が消費されます。特定の会議で消費されるクレジット数は、参加者数とその会議で使用されるコーデックの関数です。適切なサイジングを行うには、Cisco Unified Communications Sizing Tool（Unified CST）を使用します。適切なログイン認証を持つシスコの従業員またはシスコ代理店は、このツールを http://tools.cisco.com/cucst で入手できます。

ハードウェア オーディオ カンファレンス ブリッジ（Cisco WS-SVC-CMM-ACT）

この DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- このハードウェアの DSP は、音声インターフェイス、会議、メディア ターミネーション、またはトランスコーディングとして個別に設定されます。そのため、1 つのモジュールの複数の DSP を異なるリソース タイプとして使用できます。DSP は、まず音声インターフェイスに割り当ててください。
- 各 ACT ポート アダプタには、個別に設定可能な 4 つの DSP が含まれています。各 DSP は、32 人の会議参加者をサポートします。CMM モジュールごとに最大 4 つの ACT ポート アダプタを設定できます。
- この Cisco Catalyst ベースのハードウェアには、ブリッジごとに 128 人まで参加できるカンファレンス ブリッジを提供できる DSP リソースが用意されています。1 つのカンファレンス ブリッジが単一の ACT ポート アダプタ上にある複数の DSP にまたがることはできますが、カンファレンス ブリッジが複数の ACT ポート アダプタにまたがることはできません。
- これらのカンファレンス ブリッジでは、追加のトランスコーダ リソースなしで、G.711 コーデックおよび G.729 コーデックがサポートされます。ただし、その他のコーデックを使用する場合は、トランスコーダ リソースが必要になることがあります。

ハードウェア オーディオ カンファレンス ブリッジ（Cisco NM-HDV および 1700 シリーズ ルータ）

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- このハードウェアは、C549 DSP チップセットに基づく PVDM-256K タイプのモジュールを利用します。
- このハードウェアを使用する会議は、1 つのブリッジで 6 人まで参加可能なブリッジを提供します。
- リソースは DSP ごとにカンファレンス ブリッジとして設定されます。
- NM-HDV は 5 つまでの PVDM-256K モジュールを使用でき、Cisco 1700 シリーズ ルータは、1 つまたは 2 つの PVDM-256K モジュールを使用できます。
- 各 DSP は、G.711 コールまたは G.729 コールを受け付け可能な 1 つのカンファレンス ブリッジを提供します。
- Cisco 1751 は、シャーシ 1 つで 5 つの電話会議に制限されています。Cisco 1760 は、シャーシごとに 20 の電話会議をサポートします。
- NM-HDV2 などの PVDM2 ベースのハードウェアは、単一のシャーシで同時に音声インターフェイスに使用できますが、同時に他のメディア リソース機能には使用できません。PVDM-256K および PVDM2 に基づく DSP は、異なる DSP ファーム設定を持つため、ルータで同時に設定できるのは 1 つだけです。

ハードウェア オーディオ カンファレンス ブリッジ（Cisco Catalyst WS-X6608-T1 および WS-X6608-E1）

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- このハードウェアには、物理的にそれぞれのポートに関連付けられた 8 つの DSP があり、カードごとに 8 つのポートがあります。DSP の設定はポート レベルで行われるため、1 つのポートに関連付けられているすべての DSP が同じ機能を実行します。
- カンファレンス ブリッジには最大 32 人が参加でき、各ポートが 32 のカンファレンス ブリッジをサポートします。
- G.711 または G.723 の会議では、ポートごとに 32 の会議が可能です。G.729 コールを使用する場合は、ポートごとに 24 の会議が可能です。

組み込み会議

一部の電話機モデルには、3 方向の会議を可能にする組み込み会議リソースが用意されています。このブリッジは、割り込み機能によってのみ呼び出され、通常の会議リソースとしては使用されません。このブリッジが用意されている電話機の詳細については、「Unified Communications エンドポイント」（P.20-1）を参照してください。このブリッジは、G.711 コールのみを受け付けます。

ビデオ会議

ビデオ対応エンドポイントには、オーディオ会議と同じように使用できるビデオ会議の機能があります。ビデオ会議は、SCCP デバイスから Conf、Join、または cBarge ソフトキーを使用して Ad-Hoc 会議として呼び出すことができます。

会議のビデオ部分は次の 2 つのモードで操作できます。

- Voice-Activated（音声起動）

  このモードでは、主要参加者（最後に発言した参加者または最も声の大きい参加者）がビデオ エンドポイントに表示されます。この方法では、ビデオ部分は音声部分に追随（または音声部分を追跡）します。このモードは、1 人の参加者がほとんどの時間発言し続けるような場合（講師による講習やグループ トレーニングなど）に最適です。

- Continuous-Presence（連続表示）

  このモードでは、すべての（または選択した）ビデオ エンドポイントが同時に継続して表示されます。会議の音声部分は主要発言者に追随（または主要発言者を追跡）します。Continuous-Presence はより一般的なモードで、さまざまなサイトの発言者間で会議や討論を行う場合に最適です。

ビデオ会議リソースには次の 2 種類があります。

- ソフトウェア ビデオ カンファレンス ブリッジ

  ソフトウェア ビデオ カンファレンス ブリッジは、ソフトウェアだけを使用して会議のビデオと音声を処理します。Cisco Unified MeetingPlace Express VT は、Ad Hoc ビデオ会議をサポートするソフトウェア ビデオ カンファレンス ブリッジです。Cisco Unified MeetingPlace Express VT でサポートされるのは、Voice-Activated モードのビデオ会議だけです。

- ハードウェア ビデオ カンファレンス ブリッジ

  ハードウェア ビデオ カンファレンス ブリッジには、ビデオ会議に使用されるハードウェア DSP が搭載されています。この種のビデオ カンファレンス ブリッジには、Cisco 3500 シリーズ Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）があります。ほとんどのハードウェア ビデオ カンファレンス ブリッジは、音声専用のカンファレンス ブリッジとしても使用できます。ハードウェア ビデオ カンファレンス ブリッジには次の利点があります。

  - ビデオ トランスレーティング
  - 高いビデオ解像度
  - スケーラビリティ

ビデオ カンファレンス ブリッジには、オーディオ会議のリソースと同じように、デバイス プールまたはエンドポイント用の Media Resource Group（MRG; メディア リソース グループ）および Media Resource Group List（MRGL; メディア リソース グループ リスト）について同様の特性を設定できます。

Cisco Unified CM 7.*x* には、インテリジェント ブリッジ選択機能があります。この機能を使用すると、会議でビデオ エンドポイントを使用するか、またビデオ エンドポイントが利用できるかに基づいてビデオ会議リソースを割り当てることができます。会議にビデオ エンドポイントがない場合は、使用可能なオーディオ カンファレンス ブリッジが選択されます。この機能の詳細については、「インテリジェント ブリッジ選択機能」（P.16-17）を参照してください。

セキュア会議

セキュア会議は、通常の会議機能を使用して会議用メディアのセキュリティを確保し、メディアが危険にさらされないようにする手法です。これを実現するには、まずデバイスを認証してデバイスが信頼できることを確認し、同様に会議リソースも認証してから、会議メディアを暗号化します。これにより、会議のすべての参加者が認証され、その会議に関するメディアが暗号化されて送受信されます。この会議のセキュリティ レベルはさまざまです（承認レベルや暗号化レベルなど）。ほとんどの場合、会議のセキュリティ レベルは、会議の参加者の最低のセキュリティ レベルによって決まります。たとえば、ある 1 人の参加者がセキュアなエンドポイントを使用していない場合は、その会議全体が非セキュアになります。また、いずれかのエンドポイントが、認証はされているものの暗号化に対応していない場合には、その会議は認証モードになります。

セキュア会議には次の利点があります。

- 会議機能を高度なセキュリティ レベルで提供する。
- 会議コールの不正な捕捉や暗号解読を防ぐ。

セキュア会議を設計する際は、次の要素について検討してください。

- デバイス（電話機や会議リソース）のセキュリティ レベル
- コール シグナリングのセキュリティに関するオーバーヘッド
- SRTP メディアのセキュリティに関するオーバーヘッド
- 帯域幅に対する影響（セキュアな参加者が WAN 経由で参加する場合）
- NAT やファイアウォールなどの中間デバイスがセキュア コールの通過をサポートするかどうか

セキュア会議は、次の制約や制限を受ける場合があります。

- コール シグナリングのセキュリティ保護について、一部のプロトコルが IPSec に依存する場合があります。
- セキュア会議は、Unified CM と Unified CM Express の間でカスケードできません。
- セキュア会議は音声コール専用です。
- MTP とトランスコーダはセキュア コールをサポートしません。したがって、会議へ参加しているいずれかのコールで MTP またはトランスコーダが使用されている場合、その会議はセキュアにはなりません。
- 細かいセキュリティ ポリシーが必要となる場合があります。
- セキュア会議は、すべてのコーデックで使用できるとは限りません。

プラットフォームとネットワーク モジュール

DSP ファーム会議でのメディアおよびシグナリング暗号化（SRTP/TLS）機能は、オンボード DSP モジュールまたは NM-HDV2 ネットワーク モジュールを搭載した次のプラットフォームでサポートされています。

- Cisco 2600XM シリーズ マルチサービス ルータ
- Cisco 2691 マルチサービス プラットフォーム
- Cisco 2801 サービス統合型ルータ
- Cisco 2811 サービス統合型ルータ
- Cisco 2821 サービス統合型ルータ
- Cisco 2851 サービス統合型ルータ
- Cisco 3725 マルチサービス アクセス ルータ

- Cisco 3745 マルチサービス アクセス ルータ
- Cisco 3825 サービス統合型ルータ
- Cisco 3845 サービス統合型ルータ

DSP モジュールでサポートされている TI 5510 DSP の最大数は次のとおりです。

- NM-HDV2：4 つの PVDM2 で最大 16 個の TI 5510 DSP
- Integrated Services Router（ISR; サービス統合型ルータ）のオンボード PVDM2：2 つの PVDM2 で最大 8 個の TI 5510 DSP
- Integrated Services Router Generation 2（ISR G2; サービス統合型ルータ第 2 世代）オンボード PVDM3：単一ルータ シャーシで最大 4 つの PVDM3-256 DSP

表 6-10 に、各種 Network Module（NM; ネットワーク モジュール）でサポートされているセッションと会議の最大数をコーデック タイプ別に示します。

表 6-10　ネットワーク モジュールでサポートされているセッションと会議の最大数

コーデック タイプ	NM-HDV2（16 個の TI 5510 DSP）	NM-HD-2VE（3 個の TI 5510 DSP）	NM-HD-1V および NM-HD-2V（1 個の TI 5510 DSP）
G.711	16 セッション、64 会議	12 セッション、96 会議	4 セッション、32 会議
G.729	16 セッション、16 会議	3 セッション、24 会議	1 セッション、8 会議

トランスコーディング

トランスコーダは、あるコーデックからの入力ストリームを、別のコーデックを使用する出力ストリームに変換するデバイスです。同じコーデックを異なるサンプリング レートで利用する 2 つのストリームを接続することもできます。Unified CM システムでは、通常、G.711 音声ストリームと低ビットレート圧縮音声ストリームの G729a との間の変換を行うために、トランスコーダを使用します。次の場合には、どのようなときにトランスコーダ リソースが必要かが決まります。

- システム全体で単一のコーデックが使用されている。

  システムのすべてのコールに対して単一のコーデックが設定されている場合、トランスコーダ リソースは必要ありません。G.711 コーデックは、すべてのベンダーでサポートされています。単一サイトの配置では、通常、帯域幅を節約する必要がなく、単一のコーデックを使用できます。このシナリオで最も一般的に選択されるのは G.711 です。

- システムで複数のコーデックが使用され、すべてのエンドポイントがすべてのコーデック タイプに対応している。

  複数のコーデックを使用する最も一般的な理由は、LAN コールには G.711 を使用してコール品質を最大にし、帯域幅が制限されている WAN を通過するコールには低帯域幅コーデックを使用して帯域幅効率を最大にするためです。低帯域幅コーデックには、G.729a を使用することをお勧めします。G.729a は、すべての Cisco Unified IP Phone モデル、およびその他のほとんどの Cisco Unified Communications デバイスでサポートされるため、トランスコーディングの必要がなくなります。Unified CM では、リージョン間でその他の低帯域幅コーデックも設定できますが、現在の電話機モデルはこのコーデックをサポートしないため、トランスコーダが必要になります。ゲートウェイへのコールには 1 つのトランスコーダが必要で、別の IP Phone へのコールには 2 つのトランスコーダが必要です。すべてのデバイスが G.711 と G.729 の両方をサポートし、両方で設定されている場合は、デバイスがコールごとに適切なコーデックを使用するため、トランスコーダを使用する必要はありません。

- システムで複数のコーデックが使用され、一部のエンドポイントが G.711 だけをサポートしているか、または G.711 だけを使用するように設定されている。

  この条件は、システムで G.729a を使用し、このコーデックをサポートしないデバイスがある場合、または G.729a をサポートするデバイスが G.729a を使用するように設定されていない場合に発生します。この場合はトランスコーダが必要です。サードパーティ ベンダーのデバイスは、G.729 をサポートしない場合があります。また、G.729 をサポートしていても、Cisco Unity で設定されていないということもあります。Cisco Unity は G.729a でのコールの受け付けをサポートしますが、コーデックはソフトウェアで実装され、CPU に負荷がかかります。同時に 10 のコールが発生するだけで CPU 使用率が高くなるため、多くの配置では Cisco Unity で G.729 を無効にして、Unity サーバの外にある専用のトランスコーディング リソースにトランスコーディング機能の負荷を分散します。システムに Cisco Unity が含まれている場合は、Unity で G.729a コールを受け付けるか、または G.711 だけを使用するように設定するかを決定します。

（注） Release 2.0 以前の Cisco Unified MeetingPlace Express は、G.711 だけをサポートしています。以前のバージョンの Cisco Unified MeetingPlace Express へのコールに対して G.729 が設定されている環境では、トランスコーダ リソースが必要です。

設計を最終決定するには、必要なトランスコーダの数と、トランスコーダを配置する場所を検討する必要があります。複数のコーデックが必要な場合は、すべてのコーデックをサポートしないエンドポイントの数、これらのエンドポイントを配置する場所、これらのリソースにアクセスする他のグループ、これらのデバイスがサポートする同時コールの最大数、およびネットワーク上でこれらのリソースを配置する場所を検討する必要があります。

トランスコーディング リソース

トランスコーディングを実行するには、DSP リソースが必要です。これらの DSP リソースは、音声モジュール、および次の項で示すトランスコーディング用のハードウェア プラットフォームに配置することができます。

ハードウェア トランスコーダ（Cisco NM-HDV2、NM-HD-1V/2V/2VE、2800、および 3800 シリーズ ルータ）

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- トランスコーディングは、G.711 mu-law または a-law と G.729a、G.729ab、G.722、iLBC および GSM との間で使用できます。1 つの DSP で 8 セッションをサポートできます。

（注） G.711 と G.722 との間にトランスコーディングが必要ない場合は、Cisco IOS の dspfarm profile 設定に G.722 を入れないことをお勧めします。これは、Unified CM が、トランスコーディングを必要とするコールのコーデックとして G.722 を選択しないようにするためです。これらの DSP リソースは G.711 とその他のコーデック間だけをトランスコーディングできるので、G.722 とその他のコーデック（G.711 を除く）間のトランスコーディングにこれらのリソースを使用しようとすると失敗します。

- Cisco Unified IP Phone は、G.729 コーデックの G.729a バリアントだけを使用します。新規 DSP ファーム プロファイルのデフォルトは、G.729a/G.729ab/G.711u/G.711a です。単一の DSP が同時に提供できる機能は 1 つだけなので、プロファイルで設定する最大セッション数は、リソースを無駄にしないように、8 の倍数で指定する必要があります。
- トランスコーディングは、G.711mu-law/G.711a-law と G.729/G729b との間でも使用できますが、通常、Unified CM システムでは使用されません。1 つの DSP で 6 セッションをサポートできます。

- 特定のプラットフォームまたはネットワーク モジュールで使用できる DSP の数を確認するには、「音声インターフェイスの DSP リソース」（P.6-5）の項を参照してください。

ハードウェア トランスコーダ（Cisco WS-SVC-CMM-ACT）

この DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- トランスコーディングは、G.711 mu-law または a-law と G.729a、G.729b、または G.723 との間で使用できます。
- 1 つの ACT ごとに、個別に DSP プールに割り当て可能な 4 つの DSP があります。
- CCM-ACT は、DSP ごとに 16（ACT ごとに 64）のトランスコーディングされたコールをサポートします。ACT は、リソースをコールではなくストリームとしてレポートします。単一のトランスコーディングされたコールは、2 つのストリームで構成されます。

ハードウェア トランスコーダ（Cisco NM-HDV および 1700 シリーズ ルータ）

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- このハードウェアは、C549 DSP チップセットに基づく PVDM-256K タイプのモジュールを利用します。
- NM-HDV は、4 つまでの PVDM-256K モジュールを使用できます。Cisco 1700 シリーズ ルータは、1 ～ 2 の PVDM-256K モジュールを使用できます。
- NM-HDV モジュールと NM-HDV2 モジュールは、単一のシャーシで同時に音声インターフェイスに使用できますが、同時に他のメディア リソース機能には使用できません。会議、MTP、またはトランスコーディングに対して同時にアクティブにできる DSP ファームのタイプは 1 つだけです（NM-HDV または HM-HDV2）。
- G.711 mu-law または a-law から G.729、G.729a、G.729b、または G.729ab コーデックへのトランスコーディングがサポートされます。
- 1 つの DSP で 2 つのトランスコーディング セッションを提供できます。
- Cisco 1751 のシャーシは 16 セッションに制限されています。Cisco 1760 のシャーシは 20 セッションに制限されています。

ハードウェア トランスコーダ（Cisco WS-X6608）

この DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- DSP はポート レベルで機能に割り当てられます。1 つのポートで 24 のトランスコーディング セッションを提供できます。
- ブレードごとに 8 つのポートがあります。
- トランスコーディングは、G.711 mu-law または a-law と G.729a、G.729ab、G.729、または G.729b との間で使用できます。

トランスコーダは、Media Termination Point（MTP; メディア ターミネーション ポイント）と同じ機能も実行できます。トランスコーダ機能と MTP 機能の両方が必要な場合、トランスコーダがシステムによって割り当てられます。MTP 機能が必要な場合、Unified CM はトランスコーダまたは MTP をリソース プールから割り当てます。リソースの選択はメディア リソース グループによって決まります（「メディア リソース グループとメディア リソース グループ リスト」（P.6-33）の項を参照）。

ハードウェア トランスコーダ（PVDM3 DSP）

PVDM3 DSP は、Cisco 2900 シリーズおよび 3900 シリーズのサービス統合型ルータによってホストされており、任意のコーデックとのセキュアなトランスコーディングと非セキュア トランスコーディングの両方をサポートしています。音声インターフェイスおよび会議と同様に、各トランスコーディング セッションでは、各 PVDM3 DSP タイプの使用可能なクレジットが差し引かれます。使用可能なクレ

ジットによって、DSP の合計キャパシティが決まります。適切なサイジングを行うには、Cisco Unified Communications Sizing Tool（Unified CST）を使用します。適切なログイン認証を持つシスコの従業員またはシスコ代理店は、このツールを http://tools.cisco.com/cucst で入手できます。

メディア ターミネーション ポイント（MTP）

MTP は、2 つの全二重メディア ストリームを受け入れるエンティティです。MTP はこの 2 つのストリームをブリッジし、これらのストリームを個々にセットアップおよび終了できるようにします。ある接続の入力ストリームから受信されるストリーミング データは、他の接続の出力ストリームに渡され、逆も同様です。MTP には次のような多くの用途があります。

- 「ストリームの再パケット化」（P.6-19）
- 「DTMF 変換」（P.6-19）
- プロトコル固有の用途
  - 「SIP Early Offer」（P.6-22）
  - 「H.323 付加サービス」（P.6-24）
  - 「H.323 発信時の Fast Connect」（P.6-24）

ストリームの再パケット化

MTP は、G.711 a-law 音声パケットから G.711 mu-law パケット（およびその逆）にトランスコードしたり、パケット化周期が異なる（使用するサンプル サイズが異なる）2 つの接続をブリッジしたりすることができます。再パケット化するには、Cisco IOS MTP に DSP リソースが必要です。

DTMF 変換

コール中にメニュー システムのナビゲート、データの入力、またはその他の操作の目的で遠端のデバイスに信号を送信する際は、DTMF トーンが使用されます。これらは、呼制御の一部としてコール セットアップ中に送信される DTMF トーンとは異なる方法で処理されます。IP 上で DTMF を送信する方法はいくつかありますが、2 つの通信エンドポイントで共通の手順がサポートされていない場合があります。このような場合、Unified CM はメディア パスに動的に MTP を挿入して、DTMF 信号をエンドポイント間で変換できます。残念ながら、このようなコールには MTP リソースが 1 つずつ必要となるため、この方法は拡張性に欠けています。必要な MTP リソースの最適な量は、以降の項に従い、システム内のエンドポイント、トランク、およびゲートウェイの組み合せに基づいて判断してください。

MTP の挿入が必要であると判断された場合に使用可能な MTP リソースがないとき、Unified CM はサービス パラメータの「Fail call if MTP allocation fails」の設定に従って、そのコールを続行するかどうかを決定します。この設定のデフォルト値は False で、コールは続行されます。

Named Telephony Event（RFC 2833）

RFC 2833 で定義されている Named Telephony Event（NTE）は、コール メディアが確立された後で、あるエンドポイントから別のエンドポイントに DTMF を送信する方式です。トーンは、すでに確立されている RTP ストリームを使用して、パケット データとして送信されます。これらのトーンは、RTP ペイロード タイプ フィールドによってオーディオとは区別されます。たとえば、コールのオーディオをセッションで送信する際は、そのオーディオを G.711 データとして識別する RTP ペイロード タイプを使用できます。DTMF パケットの送信時には、そのパケットを NTE として識別する RTP ペイロード タイプが使用されます。ストリームの受信側は、G.711 パケットと NTE パケットを別々に利用します。

Key Press Markup Language（RFC 4730）

Key Press Markup Language（KPML）は RFC 4730 で定義されています。DTMF をインバンドで送信する NTE とは異なり、KPML はシグナリング チャネルを使用して（つまり、out-of-band（OOB; アウトオブバンド）で）、DTMF 番号を含む SIP メッセージを送信します。

KPML 手順では、DTMF 番号の登録に SIP SUBSCRIBE メッセージが使用されます。DTMF 番号自体は、XML で符号化された本体を含む NOTIFY メッセージで送信されます。

Unsolicited Notify（UN）

Unsolicited Notify 手順は、主に Cisco IOS SIP ゲートウェイにおいて、SIP NOTIFY メッセージを使用して DTMF 番号を転送するために使用されます。KPML とは異なり、これらの NOTIFY メッセージは非請求メッセージで、これらのメッセージを受信するために事前に SIP SUBSCRIBE メッセージで登録が行われることはありません。ただし、KPML と同様に、Unsolicited Notify メッセージもアウトオブバンドです。

また、KPML には XML で符号化されたメッセージ本体が含まれますが、Unsolicited Notify の NOTIFY メッセージの本体はそれとは異なり、DTMF イベントを表す 10 文字の符号化された数字、ボリューム、および継続時間です。

H.245 Signal、H.245 Alphanumeric

H.245 は、H.323 ネットワークで使用されるメディア制御プロトコルです。メディア特性のネゴシエートに使用されるほか、DTMF 転送用のチャネルも提供します。H.245 はシグナリング チャネルを利用するため、DTMF 番号はアウトオブバンド（OOB）で送信されます。Signal 方式は、Alphanumeric 方式よりも多くの DTMF イベント情報（DTMF イベントの実際の継続時間など）を伝送します。

シスコ独自の RTP

この方法は DTMF 番号をインバンドで（つまり、RTP パケットと同じストリームで）送信します。ただし、DTMF パケットはメディア パケットとは符号化方法が異なり、別のペイロード タイプが使用されます。この方法は Unified CM ではサポートされていませんが、Cisco IOS ゲートウェイではサポートされています。

SCCP

SCCP は、Unified CM により、Unified CM に登録されている SCCP ベースの各種デバイスを制御するために使用されます。SCCP は、Unified CM と制御デバイス間で DTMF 番号を転送するアウトオブバンド メッセージを定義します。

エンドポイント間の DTMF

同じクラスタ内の Unified CM サーバに登録されたエンドポイントには、次の規則が適用されます。

- SIP 以外の 2 つのエンドポイント間のコールには、MTP は必要ありません。

  SIP 以外のすべての Cisco Unified Communications エンドポイントはさまざまなシグナリング パスによって DTMF を Unified CM に送信し、Unified CM は受け取った DTMF を異なるエンドポイント間で転送します。たとえば、IP Phone は Unified CM への SCCP メッセージを使用して DTMF を送信します。この DTMF は H.245 シグナリング イベントによって H.323 ゲートウェイに送信されます。Unified CM は、異なるシグナリング方式の間で DTMF を転送できます。

- 2 つの Cisco SIP エンドポイント間のコールには、MTP は必要ありません。

  Cisco SIP エンドポイントはすべて NTE をサポートしているため、DTMF はエンドポイント間で直接送信され、変換は不要です。すべてのエンドポイントが Cisco SIP デバイスの場合、DTMF を変換する MTP は必要ありません。

- SIP エンドポイントと SIP 以外のエンドポイントの組み合せの場合、MTP が必要になることがあります。

  使用するデバイスで NTE がサポートされているかどうかを確認するには、表 6-11 を参照してください。NTE のサポートは SIP に限定されていないため、その他の呼制御プロトコルを使用するデバイスでサポートされていることがあります。たとえば、SCCP または SIP スタックを実行する Cisco Unified IP Phone は、両方のモードで NTE をサポートします。一部のデバイスは、複数の方式で DTMF をサポートします（たとえば、SCCP スタックを使用する Cisco Unified IP Phone 7960 は、NTE を他のデバイスに送信することも、SCCP を Unified CM に送信することもできます）。Cisco Wireless IP Phone 7920 などの別のデバイスは SCCP だけを送信でき、さらに別のデバイスは NTE だけを送信できます（SIP スタックを使用する Cisco Unified IP Phone 7960 など）。Unified CM は、エンドポイントのペアの機能に基づき、MTP をコール単位に動的に割り当てることができます。表 6-11 を使用して、MTP をプロビジョニングする必要があるかどうかを判断してください。

表 6-11　DTMF 方式をサポートするエンドポイント

エンドポイント プロトコル スタック：エンドポイント	DTMF 方式		
	SCCP	NTE	KPML[1]
SCCP スタック 7910、7920、7935、7936 VG248 DPA-7610、DPA-7630	あり	なし	なし
CTI ポート、ファーストパーティ制御	あり	なし	あり
SCCP スタック VG224 7902、7905、7911、7912、7931、7937、7940、7941、7942、7945、 7960、7961、7962、7965、7970、7971、7975 将来の新しい電話機モデル	あり	あり	なし
SIP スタック 3911、7905、7911、7912、7940、7941、7942、7945、 7960、7961、7962、7965、7970、7971、7975 将来の新しい電話機モデル	なし	あり	次のエンドポイントについては、あり： 7911、7941、7942、7945、7961、7962、7965、7970、7971、7975、および将来の新しい電話機モデル 次のエンドポイントについては、なし： 3911、7905、7912、7940、7960

1. Key Press Markup Language（KPML）

SIP トランク

SIP トランク設定は、SIP ユーザ エージェント（別の Cisco Unified CM クラスタや SIP ゲートウェイなど）との通信をセットアップする際に使用されます。

SIP Early Offer

SIP は Session Description Protocol（SDP）によってメディア情報をネゴシエートします。これにより、一方が提示したメディア セットに他方が応答する形で、使用するメディアがある組み合わせに決定します。SIP では、発信側が初期 INVITE メッセージによって初期オファーを送信するか、発信側がそうしなかった場合は着信側が最初の信頼性のある応答で初期オファーを送信できます。デフォルトでは、Unified CM は初期オファーを含めずに初期 INVITE を送信します。初期 INVITE にオファーを付けたい場合には MTP リソースが必要です。この初期オファーは、G.711 コーデックだけに限定されています。

また、INVITE メッセージに初期オファーが含まれているかどうかにかかわらず、着信 INVITE メッセージに MTP リソースは必須ではないことにも注意してください。

SIP トランク上の DTMF リレー

Unified CM で MTP が必要になるのは、2 つのエンドポイントの間で DTMF を送信する共通の方式がない場合、またはシステム設定で MTP を割り当てるように指定した場合です。

Unified CM によって MTP が割り当てられるかどうかは、両方の通信エンドポイントの機能と中間デバイスの設定（該当する場合）によって決まります。たとえば、SIP トランクでの DTMF 交換の処理について特定の方法（KPML を使用して DTMF を伝送する、NTE を使用するように通信エンドポイントに指示する、など）が設定されている場合があります。

SIP トランクの MTP に関する要件

SIP トランク パラメータの MTP Required は、デフォルトではオフになっています。

SIP トランクで MTP リソースが必要かどうかを判断するには、次の手順に従います。

1. この SIP トランクで定義されている対向の SIP デバイスが、SIP Early Offer を含まない着信コールを受け入れられるかどうかを確認します。

   受け入れられない場合は、MTP Required チェックボックスをオンにします。こうすると、このトランクで発行されたすべてのコール（着信と発信の両方）に対して使用可能な MTP が挿入されます。MTP はコールの発信に Early Offer を使用します。この MTP は、必要に応じて DTMF 変換も実行します。

   受け入れられる場合は、MTP Required チェックボックスをオフにします。この場合は、次の手順に従って、DTMF 変換のために MTP を動的に挿入するかどうかが決定されます。MTP による DTMF 変換は、どのコーデックを使用している場合でも実行できます。

2. トランクの DTMF Signaling Method を選択します。このパラメータは、そのトランクでの DTMF 選択の動作を制御します。すべてのコールについて、DTMF 方式を一致させるために、必要に応じて使用可能な MTP が割り当てられます。

   a. DTMF Signaling Method : No Preference

      このモードでは、Unified CM は、最も適切な DTMF シグナリング方式を選択することで、MTP の使用を最小限に抑えようとします。

両方のエンドポイントが NTE をサポートしている場合は、MTP は必要ありません。エンドポイントが NTE をサポートしているかどうかを確認するには、表 6-11 を参照してください。

両方のデバイスがいずれかのアウトオブバンド DTMF メカニズムをサポートしている場合、Unified CM は SIP トランク上で KPML を使用します。たとえば、上記のように設定された SIP トランク上で、SCCP を使用する Cisco Unified IP Phone 7936（SCCP メッセージングだけを使用して DTMF をサポートします）が、SIP を使用する Cisco Unified IP Phone 7970（NTE および KPML を使用して DTMF をサポートします）と通信する場合がこれに該当します。MTP が必要となる唯一のケースは、一方のエンドポイントがアウトオブバンドだけをサポートしていて、他方のエンドポイントが NTE だけをサポートしている場合です（たとえば、7936 SCCP 電話機と 7960 SIP 電話機が通信する場合）。

b. DTMF Signaling Method：RFC 2833

トランク全体の DTMF シグナリング方式を制限することにより、一方または両方のエンドポイントが NTE をサポートしていない場合に MTP を強制的に割り当てます。この設定では、MTP が割り当てられないのは、両方のエンドポイントが NTE をサポートしている場合だけです。

c. DTMF Signaling Method：OOB and RFC 2833

このモードでは、SIP トランクを通じて KPML と NTE ベースの両方の DTMF が送信されます。これは MTP の使用される可能性が最も高いモードです。MTP リソースが必要とされない唯一のケースは、両方のエンドポイントが NTE といずれかの OOB DTMF 方式（KPML または SCCP）の両方をサポートしている場合です。

（注）　Cisco IP Phone は、DTMF を SCCP 経由で受信した場合、エンドユーザに対して DTMF を再生しますが、NTE で受信したトーンは再生しません。ただし、DTMF を別のエンドユーザに送信する必要はありません。DTMF を必要とするエンドポイント（公衆網ゲートウェイ、アプリケーション サーバなど）と対応するコールを発信するエンドポイントについてのみ検討する必要があります。

SIP ゲートウェイでの DTMF の設定

Cisco SIP ゲートウェイは、その設定に応じて、DTMF メカニズムとして KPML、NTE、または Unsolicited Notify をサポートします。システムにはさまざまなエンドポイントが混在している場合があるため（表 6-11 を参照）、複数の方式をゲートウェイに同時に設定することで、MTP の要件を最小限に抑えることができます。

Cisco SIP ゲートウェイでは、SIP ダイヤル ピアの DTMF リレー方式として、**sip-kpml** と **rtp-nte** の両方を設定します。このように設定すると、NTE だけをサポートするものや OOB 方式だけをサポートするものも含めて、すべてのタイプのエンドポイント間で MTP リソースなしに DTMF 交換を実現できます。この設定では、ゲートウェイは NTE と KPML の両方を Unified CM とネゴシエートします。Unified CM のエンドポイントで NTE がサポートされていない場合は、DTMF 交換に KPML が使用されます。両方の方式のネゴシエーションが成功した場合、ゲートウェイは NTE を使用して DTMF 番号を受信し、KPML へのサブスクライブは行いません。

Cisco SIP ゲートウェイでは、DTMF に独自の Unsolicited Notify（UN）方式を使用することもできます。UN 方式は、DTMF トーンを表すテキストをメッセージ本体に含む SIP Notify メッセージを送信します。この方式は Unified CM でもサポートされており、**sip-kpml** が有効でない場合に使用されます。DTMF リレー方式として **sip-notify** を設定します。この方式はシスコ独自のものである点に注意してください。

NTE だけをサポートする SIP ゲートウェイでは、NTE をサポートしないエンドポイントと通信する場合、MTP リソースの割り当てが必要となります。

次の例では、Cisco SIP ゲートウェイ設定で KPML と NTE を有効にしています。

```
dial-peer voice 10 voip
dtmf-relay sip-kpml rtp-nte
```

H.323 トランクおよびゲートウェイ

H.323 プロトコルでは、次の 3 つの理由で MTP が呼び出されます。

- 「DTMF 変換」（P.6-19）
- 「H.323 付加サービス」（P.6-24）
- 「H.323 発信時の Fast Connect」（P.6-24）

H.323 付加サービス

MTP は、付加サービスに使用され、Empty Capabilities Set（ECS）機能を使用している H.323v2 の OpenLogicalChannel および CloseLogicalChannel 要求機能をサポートしていない H.323 エンドポイントの機能を拡張することができます。この要件はあまり発生しません。すべての Cisco H.323 エンドポイント、およびほとんどのサードパーティのエンドポイントが ECS をサポートしています。必要に応じて、MTP が割り当てられ、H.323 エンドポイントに代わってコールに接続されます。MTP が H.323 コールで要求され、使用できるものがない場合、コールは処理されますが、付加サービスを呼び出すことはできません。

H.323 発信時の Fast Connect

H.323 では、Fast Connect という手順が定義されています。これは、コール セットアップ時に交換されるパケット数を削減し、メディアを確立する時間を短縮します。この手順は制御チャネルのシグナリングに fastStart 要素を使用します。H.323 を利用する 2 つのデバイスのネットワーク遅延が高いときは、この遅延がメディアを確立する時間に影響を与えるため、この手順が役立ちます。Unified CM は、コール セットアップの方向に基づき、着信 fastStart と発信 fastStart を区別します。MTP 要件が同じではないため、この区別は重要です。着信 fastStart の場合、MTP は必要ありません。H.323 トランクの発信コールは、fastStart が有効なとき、MTP を必要とします。問題になるのは、多くの場合、着信コールだけです。問題を解決するには、発信 fastStart を有効にせずに着信 fastStart を使用します。

H.323 トランク上の DTMF リレー

H.323 トランクは、H.245 アウトオブバンド方式による DTMF のシグナリングをサポートします。Unified CM 5.0 およびそれ以降のリリースの H.323 クラスタ間トランクは、NTE による DTMF もサポートします。H.323 トランクには DTMF 設定オプションはありません。DTMF 転送方式は Unified CM によって動的に選択されます。

異なるクラスタにある 2 つのエンドポイントが H.323 トランクを使用して接続する場合は、次のケースが起こり得ます。

- 両方のエンドポイントが SIP の場合は、NTE が使用されます。DTMF のために MTP は必要ありません。

- 一方のエンドポイントが SIP で、KPML と NTE の両方をサポートしていて、他方のエンドポイントが SIP でない場合は、SIP エンドポイントから Unified CM に KPML で DTMF が送信され、トランクでは H.245 が使用されます。DTMF のために MTP は必要ありません。
- 一方のエンドポイントが SIP で、NTE だけをサポートしていて、他方のエンドポイントが SIP でない場合は、トランクで H.245 が使用されます。この場合はコールに対して使用可能な MTP が割り当てられます。MTP は、SIP エンドポイントがある Unified CM クラスタで割り当てられます。

たとえば、SIP を使用する Cisco Unified IP Phone 7970 が、SCCP を使用する Cisco Unified IP Phone 7970 と通信する場合は、SIP トランク経由で接続されるときは NTE が使用され、H.323 トランク経由で（H.245 方式を使用するトランクを使用して）通信するときは OOB 方式が使用されます。

コールがある H.323 トランクから着信し、そのコールを別の H.323 トランクにルーティングする場合、両方のエンドポイントが SIP のときは、DTMF 用に NTE が使用されます。どちらか一方のエンドポイントが SIP でないときは、H.245 が使用されます。一方が NTE だけをサポートする SIP エンドポイントで、他方が SIP でない場合は、MTP が割り当てられます。

H.323 ゲートウェイでの DTMF の設定

H.323 ゲートウェイは、H.245 Alphanumeric、H.245 Signal、NTE、およびメディア ストリームのオーディオによる DTMF リレーをサポートします。現時点では、H.323 ゲートウェイ用の Unified CM において NTE オプションはサポートされていないため、使用できません。これに適したオプションは H.245 Signal です。他のエンドポイントに Unified CM と共通のシグナリング機能がない場合、H.323 ゲートウェイへのコールを確立するために、MTP が必要です。たとえば、SIP スタックを実行している Cisco Unified IP Phone 7960 は NTE だけをサポートするため、H.323 ゲートウェイを使用する場合は MTP が必要です。

H.323 ゲートウェイでの DTMF 方式に推奨される設定を示します。

```
dial-peer voice 10 voip
dtmf-relay h.245-signal
```

CTI ルート ポイント

CTI ルート ポイントは、CTI イベントを使用して CTI アプリケーションと通信します。DTMF の観点では、CTI ルート ポイントは、すべての OOB 方式をサポートし、RFC 2833 はサポートしないエンドポイントと見なすことができます。そのようなエンドポイントで DTMF 変換に MTP が必要となるケースは、RFC 2833 だけをサポートする別のエンドポイントと通信する場合だけです。

電話コールのファーストパーティ制御を持つ CTI ルート ポイントは、コールのメディア ストリームに参加し、MTP の挿入を必要とします。CTI によるコールのサードパーティ制御が可能で、メディアが CTI で制御されているデバイスを通過する場合、MTP が必要かどうかは制御されるデバイスの機能によって異なります。

例 6-1　NTE 変換用に MTP を必要とするコール フロー

例として、ファーストパーティ制御（CTI ポートがメディアの終端）の CTI ルート ポイントがあり、IVR メニューをナビゲートするために DTMF を使用するシステムに統合されているシステムを考えます。システムのすべての電話機が SCCP を実行している場合、MTP は必要ありません。この場合、Unified CM が CTI ポートを制御し、IP Phone からの DTMF を SCCP 経由で受信します。Unified CM が、DTMF 変換を提供します。

ただし、SIP スタックを実行している電話機（NTE だけをサポートしていて、KPML をサポートしていない電話機）がある場合は、MTP が必要です。NTE はメディア ストリームの一部なので、Unified CM は受信しません。MTP がメディア ストリームの中に呼び出され、SCCP を使用する 1 つのコール レッグと NTE を使用する 2 番目のコール レッグを持ちます。MTP は Unified CM による SCCP の制御下にあり、Unified CM の制御下で NTE から SCCP への変換を実行します。KPML をサポートしている新しい電話機では、MTP は必要ありません。

カンファレンス ブリッジでの MTP の使用

会議の参加者の 1 つ以上のデバイスで RFC 2833 が使用されている場合は、MTP が電話会議で使用されます。会議機能が呼び出されると、Unified CM によって、RFC 2833 だけをサポートする、その電話会議のすべての参加者のデバイスに MTP リソースが割り当てられます。これは、使用されるカンファレンス ブリッジの DTMF 機能とは無関係に行われます。

MTP リソース

次のタイプのデバイスは、MTP として使用できます。

ソフトウェア MTP（Cisco IP Voice Media Streaming Application）

ソフトウェア MTP とは、サーバに Cisco IP Voice Media Streaming Application をインストールすることによって設定されるデバイスです。インストールされたアプリケーションが、MTP アプリケーションとして設定されると、そのアプリケーションは、Unified CM ノードに登録され、サポートする MTP リソース数を Unified CM に知らせます。ソフトウェア MTP デバイスは、G.711 ストリームだけをサポートします。IP Voice Media Streaming Application は、複数の機能に使用することもできるリソースで、設計ガイダンスではすべての機能を同時に考慮する必要があります（「Cisco IP Voice Media Streaming Application」（P.6-29）を参照）。

ソフトウェア MTP（Cisco IOS に基づく）

- ルータでソフトウェアベースの MTP を提供する機能は、Cisco 3800 シリーズ ルータでは Cisco IOS Release 12.3(11)T、その他のルータ モデルでは Release 12.3(8)T4 から使用できるようになりました。
- この MTP によって、G.711 mu-law および a-law、G.729a、G.729、G.729ab、G.729b、およびパススルーのコーデックを設定できます。ただし、同時に設定できるコーデックは 1 つだけです。これらの内の一部のコーデックは、Unified CM では実装していません。
- ルータ設定では、最大 500 の個別ストリームが可能で、250 のトランスコーディングされたセッションをサポートします。この数の G.711 ストリームを使用すると、5 MB のトラフィックが生成されます。

ハードウェア MTP（Cisco NM-HDV2、NM-HD-1V/2V/2VE、2800 および 3800 シリーズ ルータ）

- このハードウェアは、PVDM-2 モジュールを使用して DSP を提供します。
- 各 DSP は、16 の G.711 mu-law または a-law MTP セッション、または 6 つの G.729 または G.729b MTP セッションを提供できます。

ハードウェア MTP（PVDM3 を搭載した Cisco 2900 および 3900 シリーズ ルータ）

- これらのルータでは、マザーボード上の PVDM3 DSP をネイティブに使用するか、またはマザーボードやサービス モジュール上のアダプタによる PVDM2 を使用します。
- 各 DSP タイプのキャパシティの範囲は、16 G.711 a-law または mu-law セッション（PVDM3-16 の場合）から、256 G.711 セッション（PVDM3-256 の場合）までとなります。

ハードウェア MTP（Cisco WS-SVC-CMM-ACT）

- このモジュールには、個別に設定できる 4 つの DSP があります。
- 各 DSP は、128 の G.711 mu-law または a-law MTP セッションをサポートします。

ハードウェア MTP（Catalyst WS-X6608-T1 および WS-X6608-E1）

- サポートされるコーデックは、G.711 mu-law または a-law、G.729、または G.729b です。
- 設定はポート レベルで行います。モジュールごとに 8 つのポートを使用できます。
- MTP リソースとして設定されたポートごとに、24 のセッションが提供されます。

（注）　Cisco IOS でハードウェア MTP リソースを設定している場合は、G.729 または G.729b コーデックは設定できません。ただし、他のすべての MTP リソースが使い果たされた場合、または使用できない場合には、Unified CM はハードウェア トランスコーディング リソースを MTP として使用できます。

Trusted Relay Point

Trusted Relay Point（TRP）はメディア ストリームに挿入可能なデバイスの一種で、そのストリームのコントロール ポイントとして機能します。TRP を使用すると、そのストリームにさらに処理を加えることができます。また、ストリームが任意の特定のパスを通るようにする手段として TRP を使用することも可能です。TRP 機能を使用するためには 2 つの要素が存在します。1 つは CUCM 上で論理的に TRP を設定すること。もう 1 つは実際に TRP として動作するコールのアンカーポイントとなるデバイスです。TRP 機能は MTP デバイスをアンカーポイントとして使用する際に使うことができます。

Unified CM の個々の電話機に関する設定に、その電話機へのコールまたはその電話機からのコールに対して TRP を呼び出すための設定パラメータが新しく追加されました。TRP リソースの管理には、メディア リソース プール メカニズムが利用されます。その電話機のメディア リソース プールには、TRP として呼び出し可能なデバイスが含まれている必要があります。

TRP を QoS 強制メカニズムとして使用する例については、「ネットワーク インフラストラクチャ」（P.3-1）の章を参照してください。冗長ファイアウォールを備えた冗長なデータ センターでメディア ストリームのアンカー ポイントとして TRP を利用する例については、「音声セキュリティ」（P.19-1）の章を参照してください。

Annunciator

Annunciator は Cisco IP Voice Media Streaming Application のソフトウェア機能で、これを使用すると、音声メッセージや各種コールプログレストーンをシステムからユーザに流すことができます。この機能は、複数の片方向 RTP ストリームを Cisco IP Phone やゲートウェイなどのデバイスに送信できます。さらに、SCCP メッセージを使用して、RTP ストリームを確立します。この機能を使用するには、デバイスが SCCP に対応している必要があります。トーンとアナウンスは、システムで事前に定義されています。アナウンスでは、ローカリゼーションがサポートされています。また、適切な .wav ファイルを置き換えて、アナウンスをカスタマイズすることもできます。Annunciator は、トランスコーディング リソースを使用しないで、G.711 a-law および mu-law、G.729、および Wideband コーデックをサポートすることができます。

次の機能には、Annunciator リソースが必要です。

- Cisco Multilevel Precedence Preemption（MLPP）

  この機能には、次のようなコール失敗の状態に応じて再生されるストリーミング メッセージが用意されています。

  - 優先順位の高い既存のコールが原因で、プリエンプション処理できない。
  - 優先順位アクセス制限に到達した。
  - 試行された優先順位レベルが許可されていない。
  - 着信番号が、プリエンプション処理またはコール ウェイティングに対応していない。
- SIP トランクを介した統合

  SIP エンドポイントには、トーンを生成し、RTP ストリームでインバンドで送信する機能があります。SCCP デバイスにはこの機能がないため、SIP エンドポイントと統合した場合、DTMF トーンの生成または受け入れ時には Annunciator と MTP が併用されます。次のタイプのトーンがサポートされます。
  - コールプログレストーン（ビジー、アラート、およびリングバック）
  - DTMF トーン
- Cisco IOS ゲートウェイとクラスタ間トランク

  これらのデバイスには、コールプログレストーン（リングバック トーン）のサポートが必要です。
- システム メッセージ

  次のようなコール失敗の状態では、システムはエンドユーザにストリーミング メッセージを再生します。
  - ダイヤル番号をシステムが認識できない。
  - サービスが中断したためコールがルーティングされない。
  - 番号が通話中で、その番号がプリエンプション処理またはコール ウェイティング用に設定されていない。
- 会議

  電話会議の間、システムは、参加者がブリッジに参加、またはブリッジから退出したことをアナウンスするときに、割り込み音を再生します。

Cisco IP Voice Media Streaming Application をサーバ上でアクティブにすると、Annunciator がシステム内に自動的に作成されます。Media Streaming Application を非アクティブにすると、Annunciator も削除されます。単一の Annunciator インスタンスは、パフォーマンス要件を満たす場合は、Unified CM クラスタ全体にサービスを提供できます（「Annunciator のパフォーマンス」（P.6-28）を参照）。そうでない場合は、追加の Annunciator をクラスタ用に設定する必要があります。追加の Annunciator を設定するには、クラスタ内の他のサーバ上で Cisco IP Voice Media Streaming Application をアクティブにします。

Annunciator は、そのデバイス プールで定義されたとおり、一度に 1 つの Unified CM に登録されます。デバイス プールに対してセカンダリが設定されている場合、Annunciator は自動的にセカンダリ Unified CM にフェールオーバーします。障害発生時に再生されるアナウンスはいずれも保持されません。

Annunciator はメディア デバイスと見なされるため、メディア リソース グループ（MRG）に含めて、電話機およびゲートウェイで使用される Annunciator の選択を制御することができます。

Annunciator のパフォーマンス

デフォルトでは、Annunciator は 48 のストリームを同時にサポートするように設定されています。この設定値は、Unified CM サービスが同一のサーバ（共存）上で動作する Annunciator に推奨される最大値です。サーバの接続性が 10 Mbps しかない場合は、設定を下げて同時ストリームを 24 にします。

Cisco CallManager Service を含まないスタンドアロン サーバでは、最大 255 のアナウンス ストリームを同時にサポートできます。デュアル CPU と高性能ディスク システムを持つ高性能サーバでは、最大 400 のストリームをサポートできます。複数のスタンドアロン サーバを追加して、必要な数のストリームをサポートすることができます。

Cisco RSVP Agent

トポロジ対応型のコール アドミッション制御を提供するために、Unified CM は 1 つまたは 2 つの RVSP Agent をコール セットアップ時に呼び出し、IP WAN で RSVP 予約を実行します。これらのエージェントは、RSVP 機能を提供するように設定された MTP またはトランスコーダ リソースです。RSVP リソースは、Unified CM による MTP またはトランスコーダ リソースの割り当てという観点から見て、通常の MTP またはトランスコーダと同様に処理されます。

Cisco RSVP Agent 機能は、Cisco IOS Release 12.4(6)T で最初に導入されました。RSVP および Cisco RSVP Agent の詳細については、「コール アドミッション制御」（P.9-1）の章を参照してください。

Cisco IP Voice Media Streaming Application

Cisco IP Voice Media Streaming Application は、ソフトウェアに次のリソースを組み込みます。

- Music on Hold（MoH）
- Annunciator
- ソフトウェア カンファレンス ブリッジ
- メディア ターミネーション ポイント（MTP）

Media Streaming Application をアクティブにすると、上記の各リソースが 1 つずつ自動的に設定されます。Annunciator、ソフトウェア カンファレンス ブリッジ、または MTP が必要ない場合は、Cisco IP Voice Media Streaming Application の Run Flag サービス パラメータを無効にして、これらのリソースを無効にすることをお勧めします。

複数のリソースが必要になる状況や、それらのリソースによって Media Streaming Application にかかる負荷を慎重に検討してください。各リソースには、処理可能な接続の最大数を制御するサービス パラメータと、関連付けられたデフォルト設定があります。デフォルト設定を変更しない限り、制限付きで 4 つのリソースすべてを同じサーバ上で実行できます。ただし、配置においてデフォルトを超える数のリソースが 1 つでも必要になった場合は、そのリソースを独自の専用サーバ上で実行するように設定します（そのサーバ上では、その他すべてのリソースおよび Cisco CallManager Service を実行しないでください）。

Annunciator は、IP Voice Media Streaming Application でのみ使用できる唯一のメディア リソースです。会議、MTP、および Music On Hold（MoH; 保留音）はすべて、Unified CM サーバの外に置くことができます。Unified CM では MTP および会議リソースを無効にして、これらの機能には外部の専用リソースを用意することをお勧めします。

また、IP Voice Media Streaming Application は、コール処理を担当するパブリッシャ、または任意の Unified CM サーバとは異なるサーバ上で実行することを強くお勧めします。メディア リソースのために CPU 負荷が増加すると、コール処理のパフォーマンスに悪影響が発生する可能性があります。User Datagram Protocol（UDP; ユーザ データグラム プロトコル）トラフィックは、Unified CM サーバ上で受信されなければならないので、セキュリティ上の問題が発生する恐れがあります。

ハードウェアおよびソフトウェアのキャパシティ

この項では、DSP を含むネットワークモジュールおよびシャーシのキャパシティ、ネットワーク モジュールを含むシャーシのキャパシティ、およびハードウェアに対するソフトウェアの依存性に関するデータを提供します。

PVDM

表 6-12、表 6-13、および表 6-14 に、PVDM の 2 つのモデルまたは固定構成ネットワーク モジュールに配置できる DSP の数を示します。PVDM3 モジュールは、PVDM2 モジュールと PVDM-256K モジュールよりも新しく、これらの 3 つのタイプは交換できません。

表 6-12　PVDM-256K モジュールあたりの DSP 数

モジュール	DSP 数
PVDM-256K-4	1 DSP
PVDM-256K-8	2 DSP
PVDM-256K-12	3 DSP
PVDM-256K-16HD	4 DSP
PVDM-256K-20HD	5 DSP

表 6-13　PVDM2 モジュールまたは固定構成ハードウェアあたりの DSP 数

ハードウェア モジュールまたはシャーシ	DSP 数
PVDM2-8	½ DSP
PVDM2-16	1 DSP
PVDM2-32	2 DSP
PVDM2-48	3 DSP
PVDM2-64	4 DSP
NM-HD-1V NM-HD-2V	1 DSP
NM-HD-2VE	3 DSP

表 6-14　PVDM3 モジュールあたりの DSP 数

ハードウェア モジュール	DSP テクノロジー
PVDM3-16	1 つの DSP、シングル コア
PVDM3-32	1 つの DSP、シングル コア
PVDM3-64	1 つの DSP、デュアル コア
PVDM3-128	1 つの DSP、3 コア
PVDM3-192	2 つの DSP : 一方にデュアル コア、もう一方に 3 コア
PVDM3-256	2 つの DSP、両方に 3 コア

PVDM3 DSP モジュールは、Cisco 2900 シリーズおよび 3900 シリーズ プラットフォームでサポートされており、Cisco IOS Release 15.0(1) M 以降が必要です。

表 6-15 に、各ハードウェア プラットフォームおよびネットワークモジュールでメディア リソース機能をサポートするために必要な、Cisco IOS ソフトウェアの最小バージョンを示します。

表 6-15　メディア サポートに必要な使用可能 PVDM2 スロット数と Cisco IOS のバージョン

シャーシまたはネットワーク モジュール	PVDM2 スロット数	メディア用 Cisco IOS 最小リリース
2801	2	12.3(11)T
2811	2	12.3(8)T4
2821 または 2851	3	12.3(8)T4
3825 または 3845	4	12.3(11)T
NM-HDV2	4	

Cisco 2900 および 3900 シリーズ プラットフォーム

Cisco 2900 および 3900 シリーズ プラットフォームは、Integrated Services Router Generation 2（ISR G2; サービス統合型ルータ第 2 世代）とも呼ばれます。これらのルータでは、マザーボード上で使用可能な DSP スロットに直接挿入できる PVDM3 DSP モジュールをサポートしています。PVDM2 DSP モジュールについても、アダプタ カードを使用することにより、マザーボード上に取り付けることができます。

ISR G2 ルータでは、アダプタ カードを使用することにより、サービス モジュール スロットでの NM-HD カードと NM-HDV2 カードもサポートしています。

次のガイドラインおよび考慮事項は、これらのプラットフォームでホストされる DSP リソースに適用されます。

- Cisco 2900 および 3900 シリーズ ルータでは、オンボード（マザーボード）の DSP スロットに挿入された PVDM3 DSP だけがサポートされます。PVDM2 DSP は、アダプタ カードを使用して、これらのスロットに取り付けることができます。
- PVDM2 モジュールと PVDM3 モジュールは、同じマザーボード上で同時に使用することはできません。
- DSP は、同じ DSP タイプ間でだけ共有できます。たとえば、マザーボードに PVDM3 DSP が挿入されており、サービス モジュールに PVDM2 DSP が挿入されている場合、サービス モジュールの複数の DSP は相互に共有できますが、マザーボード上の DSP は、サービス モジュールの DSP とは共有できません。
- PVDM3 DSP では、Cisco FAX リレーを除き、PVDM2 DSP がサポートしているすべての機能をサポートします。

PVDM2 とは異なり、PVDM3 DSP には、すべてのメディア機能に対して単一のソフトウェア イメージがあります。

Cisco 2800 および 3800 シリーズ プラットフォーム

Cisco 2800 および 3800 シリーズ ルータはすべて、2 つの AIM スロットを備えていますが、AIM-VOICE-30 または AIM-ATM-VOICE-30 カードをサポートしません。これは、これらのカードの機能は、マザーボード上に取り付けられた PVDM2 モジュールによって代わりに提供されるためです。

ネットワーク モジュール

NM-HDV2、NM-HD-*xx*、および NM-HDV モジュールは、表 6-16 に示されている Cisco IOS プラットフォームに取り付けることができます。その場合の最大モジュール数は、表のとおりです。

表 6-14 内の 3 つのモジュール ファミリはすべて 1 つのシャーシに取り付けることができます。ただし、会議機能とトランスコーディング機能は、NM-HDV ファミリと、残りのファミリのどちらか（NM-HD-*xx* または NM-HDV2）との両方で同時に使用することはできません。また、NM-HDV（TI-549）、NM-HD-*xx*、および NM-HDV2（TI-5510）を、1 つのシャーシ内で同時に会議およびトランスコーディングに使用することはできません。

NM-HDV モジュールと NM-HDV-FARM モジュールは、同じシャーシに混在できます。すべてのシャーシがこれらのモジュールをフル装備できるわけではありません。表 6-13 では、各タイプのハードウェア プラットフォームがサポートする最大モジュール数を示しています。

表 6-16　プラットフォーム タイプごとのモジュール スロット数

Cisco IOS プラットフォーム	スロット数
2691、2811、2821、2851	1
3620[1]、3725、3825	2
3640	3
3745、3845	4
3660	6

1. Cisco 3620 ルータは 2 つの NM スロットを備えていますが、サポートする NM-HDV モジュールは 1 つだけです。

表 6-17　プラットフォーム タイプでサポートされるモジュール

	プラットフォームでサポートされるモジュール		
Cisco IOS プラットフォーム	NM-HDV2	NM-HD-1V NM-HD-2V NM-HD-2VE	NM-HDV NM-HDV-FARM
VG2001 26002 36203 3640	なし	なし	あり
3660	なし	あり	あり
2600XM、2691、 3725、3745 2811、2821、2851 3825、3845	あり	あり	あり

（注）　Cisco VG200、2620、2621、および 3620 は、NM-HDV-FARM をサポートせず、さらに MTP、会議、およびトランスコーディングもサポートしません。Cisco 2801 には NM スロットがありません。

NM-HDV の DSP 要件の計算

状況によっては、NM－HDV に DSP が最大数搭載されないことがあります。サンプリング レートは通常、システム デフォルトから変更されません。サンプリング レートを変更する必要がない場合は、この問題を無視してかまいません。

Voice Activity Detection（VAD; 音声アクティビティ検出）を有効または無効にしたサンプル レート 20、30、40、60 ms の場合（または、VAD を有効にした 10 ms の場合）、PVDM を最大数である 5 個搭載した NM-HDV または NM-HDV-FARM を構成して、使用可能な DSP リソースを 60 得ることが可能です。

VAD を無効にした 10 ms サンプリング レートの場合、フル装備の NM-HDV 上のすべての DSP を利用することは不可能です。パケット レートが、NM-HDV のキャパシティである毎秒 6600 パケット（pps）を超えないことを確認するには、さらに次の計算が必要です。

100 pps (音声インターフェイス数) + 600 pps (会議数) + 200 pps (トランスコーディング セッション数) < 6600 pps

正確な要件を判別するには、適切なログイン認証を持つシスコ従業員およびシスコ代理店が次の Web サイトで入手できる包括的 DSP Calculator を使用します。

http://tools.cisco.com/cucst

一般的な設計ガイドライン

Unified CM のメディア リソース グループ（MRG）とメディア リソース グループ リスト（MRGL）のコンストラクトは、この章で説明されているリソースの編成とアクセスの方法を制御するために使用されます。この項では、これらのコンストラクトを効率的に利用する方法について説明します。また、さまざまな Unified CM 配置モデルに固有の考慮事項についても説明します。

メディア リソース グループとメディア リソース グループ リスト

メディア リソース グループとメディア リソース グループ リストは、リソースの割り当て方法を制御する方式を提供するもので、リソースに対するアクセス権、リソースの場所、特定のアプリケーションのリソース タイプなどが含まれます。この項では、読者がメディア リソース グループを理解しているものとして、次の設計上の考慮事項について詳しく説明します。

- システムは、ユーザ インターフェイスに表示されず、すべてのリソースが作成時にメンバーとなるデフォルト メディア リソース グループを定義します。メディア リソースの使用側は、まず、設定で指定されている任意のメディア リソース グループ（MRG）またはメディア リソース グループ リスト（MRGL）のリソースを使用します。必要なリソースが使用できない場合、デフォルト MRG でリソースが検索されます。単純な配置では、デフォルトの MRG だけを使用することがあります。
- MRG を使用してリソースへのアクセスを制御する場合は、リソースを明示的に別のグループに設定することによって、デフォルト MRG の外に移動する必要があります。すべてのコールに対する最後の手段としてのみリソースを使用できるようにする場合は、そのリソースをデフォルト グループに残しておくことができます。また、リソースの制御が必要ない場合も、デフォルト グループに残しておくことができます。

- MRG には、複数のタイプのリソースが含まれていることがあります。必要な機能に基づいて、適切なリソースがグループから割り当てられます。MTP とトランスコーダは、特別な例です。トランスコーダは MTP としても使用できます。
- MRG の用途の 1 つは、類似したタイプのリソースのグループ化です。カンファレンス ブリッジ リソースがサポートする参加者の数は異なります。MRG を使用して、カンファレンス ブリッジのサイズ別に会議リソースをグループ化できます。
- メディア リソース グループ（MRG）とメディア リソース グループ リスト（MRGL）を使用して、複数の Unified CM 間でリソースを共有します。MRG と MRGL を使用しない場合、リソースは、1 つの Unified CM からしか使用できません。
- また、MRG と MRGL を使用すると、地理的なロケーションに基づいてリソースを分離できます。その結果、WAN 帯域幅を節約できる場合もあります。
- MRGL は、設定にリストされている順序で MRG を使用します。ある MRG に必要なリソースがない場合、次の MRG が検索されます。すべての MRG が検索され、リソースが見つからない場合、検索は終了します。
- MRG から類似のリソースを割り当てるアルゴリズムでは、類似したリソース間での負荷分散が試みられます。リソースが使用されると、その MRG のポインタは次のデバイスにインクリメントされます。1 つのデバイスが複数の MRG に存在することがあります。この場合、このデバイスがメンバーであるすべてのグループのポインタに影響を与えます。MTP が必要で、トランスコーダが同じグループに存在する場合、すべての MTP が使用されるまで、MTP が常に割り当てられます。すべての MTP が使用されると、トランスコーダが MTP として使用されます。同じグループにキャパシティの異なるリソースがある場合、ロード シェアリングはキャパシティに基づいてリソースを割り当てようとします。システムはリソース間で負荷を分散しますが、上記の要素により、動作がラウンドロビンになることはあまりありません。
- Unified CM Administration には MRG のデバイスがアルファベット順に表示されますが、割り当てられる順序は設定データベースの順序に基づきます。この順序は変更できません。メディア リソースを特定の順序で割り当てるには、リソースごとに別の MRG を作成し、MRGL を使用して割り当て順序を指定します。
- メディア リソース自身には、別のメディア リソースを呼び出さない設定が必要です。たとえば、MTP がコールに挿入され、この MTP で設定されているコーデックが、このコールに対して Unified CM が必要とするコーデックと異なる場合、トランスコーダも呼び出されます。よくある間違いは、Unified CM が G.729a を必要とする場合に、MTP を G.729 または G.729b に設定することです。

メディアの機能と音声品質

メディアを操作するいずれのプロセスも、メディアの品質を低下させる可能性があります。たとえば、ネットワーク（IP または TDM）上で送信するための音声ストリームのエンコーディングと、相手側でのデコーディングは情報の損失を招き、結果として音声ストリームは元の音声を正確に再生しません。同じ音声ストリームの複数のエンコーディングおよびデコーディングの手順を含む、ネットワーク経由のメディア通過パスが存在する場合、エンコーディングおよびデコーディングの操作が繰り返されるたびに音声品質は低下していきます。通常、このようなパスは回避する必要があります。このことは特に、G.729 などの Low-bandwidth Codecs（LBC; 低帯域幅コーデック）に当てはまります。G.729 にはすでに低い Mean Opinion Score（MOS; 平均オピニオン評点、音声品質の主観的評価）が付いているので、エンコーディングとデコーディングの操作の繰り返しによってこの評点はただちに、許容できない品質まで低下します（詳細については、http://www.cisco.com で「Mean Opinion Score」を参照してください）。

このようなパスが回避できない場合には、G.711 または G.722 コーデックなどの帯域幅が比較的高く、低圧縮のコーデックを使用することによって通常、音声品質を向上させることができます。このようなパスが予想される場合には、これらのコーデックの使用をお勧めします。このようなシナリオで、低帯域幅で高圧縮のコーデックを使用することはお勧めできません。

配置モデル

ここでは、MTP リソースとトランスコーディング リソースが、どこで、いつ使用されるかを説明します。具体的には、次の 3 つの企業 IP テレフォニー配置のモデルと、4 つ目のアプリケーション シナリオで示します。

- 「単一サイト配置」（P.6-35）は、1 つのサイト内の 1 つ以上のコール処理エージェントから構成され、音声トラフィックは IP WAN を介して伝送されません。
- 「集中型コール処理を使用するマルチサイト WAN 配置」（P.6-35）は、IP WAN を通じて接続された複数のサイトにサービスを提供する、単一のコール処理エージェントから構成されます。
- 「分散型コール処理を使用するマルチサイト WAN 配置」（P.6-36）は、IP WAN を通じて接続される複数のリモート サイトのそれぞれに置かれている、コール処理エージェントから構成されます。
- 「IP 公衆網アクセス」（P.6-37）は、MTP リソースを必要とするもう 1 つのシナリオです。このシナリオは、上記の配置モデルのすべてに適用されます。

単一サイト配置

単一サイト配置では、低ビット レート（LBR）コーデックを使用する根拠となっている低速リンクが不要のため、トランスコーディングの必要はありません。H.323v2 に準拠していない相当数のデバイス（旧バージョンの Microsoft NetMeeting や特定のビデオ デバイスなど）が存在する場合、なんらかの MTP リソースが必要なことがあります。SIP エンドポイントがある場合は、DTMF 変換用に MTP リソースが必要になることがあります（「Named Telephony Event（RFC 2833）」（P.6-19）を参照）。

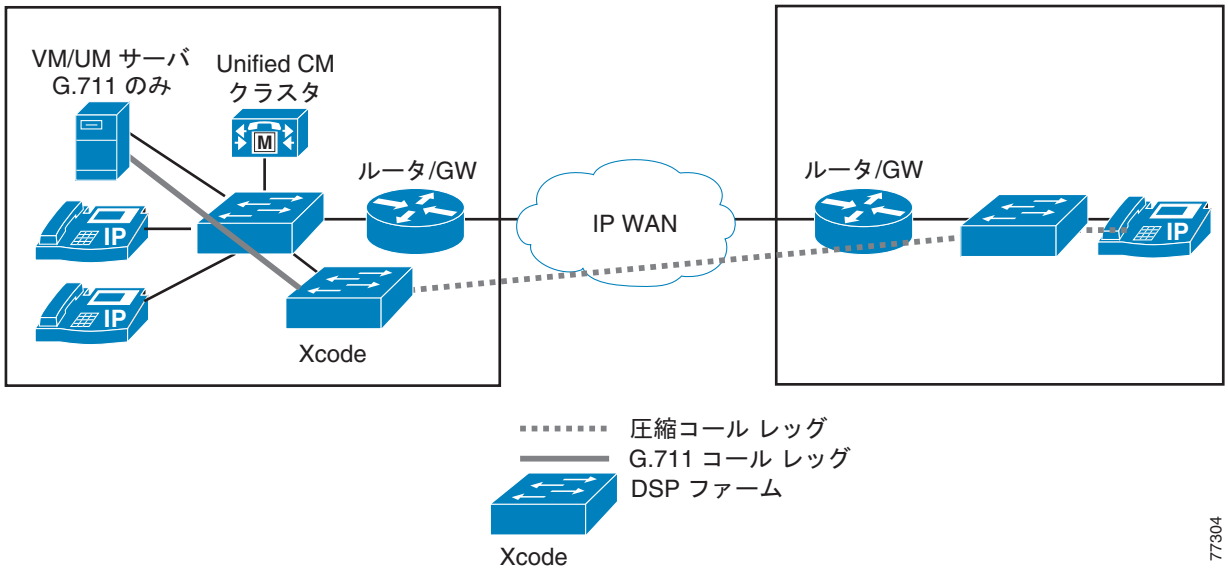
集中型コール処理を使用するマルチサイト WAN 配置

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

WAN 帯域幅は一般に制限されるので、WAN を通過するときは、G.729 などの低ビット レート コーデックを使用するようにコールが設定されます（図 6-1 を参照）。

IP Phone 間の音声圧縮は、Unified CM の *リージョン*と *ロケーション*を使用して簡単に設定されます。リージョンは、そのリージョン内のデバイスが使用する圧縮のタイプ（たとえば、G.711 または G.729）を指定します。ロケーションは、そのロケーションのデバイスに出入りするコールに使用可能な、合計帯域幅量を指定します。

図 6-1　集中型コール処理を使用する WAN のトランスコーディング



Unified CM は、MRG（メディア リソース グループ）を使用して、クラスタ内の Unified CM サーバ間で、MTP リソースとトランスコーディング リソースの共有を可能にします。さらに、異なるリージョンを通過するコールに LBR コーデック（たとえば、G.729a）を使用する場合、トランスコーディング リソースが使用されるのは、エンドポイントの一方（または両方）が、LBR コーデックを使用できない場合だけです。

図 6-1 では、Unified CM がトランスコーダが必要であることを認識し、高帯域幅コーデックを使用するデバイスの MRGL または MRG に基づいてトランスコーダを割り当てます。この場合、VM/UM サーバが、使用するトランスコーダ デバイスを決定します。この Unified CM の動作は、トランスコーダ リソースが高帯域幅デバイスの近くに正しく配置されていることを前提としています。VM/UM サーバ用のトランスコーダがリモート サイトに配置されるようにこのシステムが設計されていた場合、G.711 は WAN を経由して送信されるため、設計の意図が失われます。結果として、G.711 のみのデバイスを使用する複数のサイトがある場合に WAN で LBR が実行されていると、これらの各サイトがトランスコーダ リソースを必要とします。

その他のリソースの配置も重要です。たとえば、リモート サイトの 3 つの電話機で会議が発生し、会議リソースが中央（コール処理）サイトにある場合、3 つのメディア ストリームが WAN で伝送されます。会議リソースがローカルにあれば、コールは WAN を経由しません。WAN の帯域幅とコール アドミッション制御を設計するときは、この要素を考慮する必要があります。

分散型コール処理を使用するマルチサイト WAN 配置

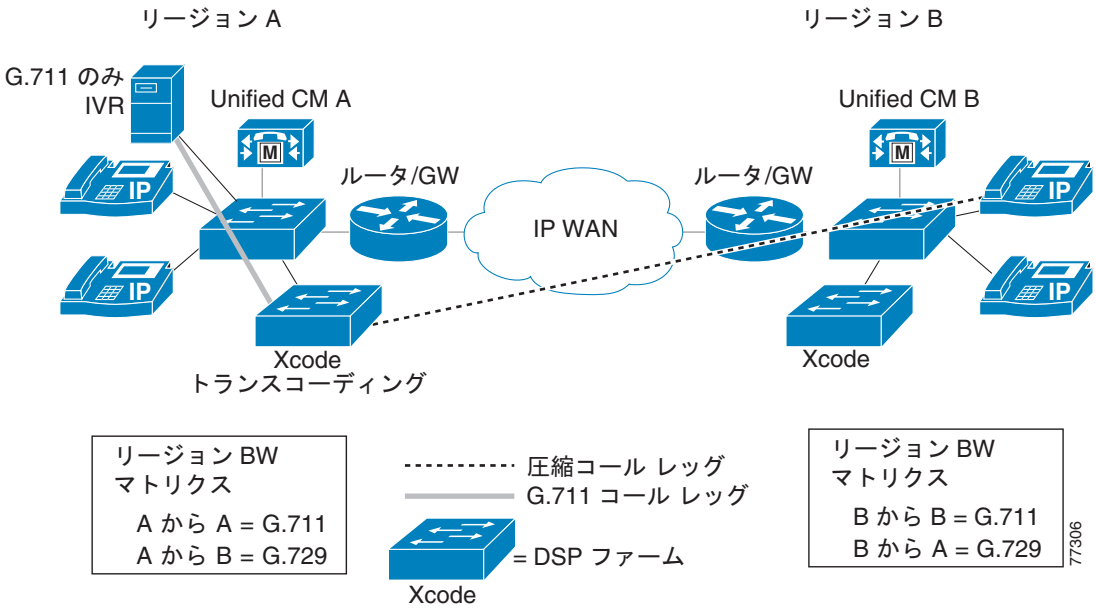
分散型コール処理配置では、IP WAN を介して複数のサイトが接続されます。各サイトには Unified CM クラスタが含まれ、単一サイト モデルか、集中型コール処理モデルになります。サイト間のコール アドミッション制御には、ゲートキーパーを使用できます。

WAN 帯域幅は一般に制限されているので、WAN を通過するときは、LBR コーデック（たとえば、G.729a）を使用するように、サイト間のコールが設定されていることがあります。H.323v2 クラスタ間トランクは、Unified CM クラスタの接続に使用されます。Unified CM は、ハードウェア MTP が使用される場合、MTP サービスを通じた圧縮音声コール接続もサポートします（図 6-2 を参照）。

次の状況では、分散型コール処理配置に、トランスコーディング サービスと MTP サービスが必要になる場合があります。

- 現行バージョンの Cisco アプリケーションを使用する場合は、トランスコーディング リソースの使用を回避できるため、回避することをお勧めします。特別な例として、特定のデバイスの G.711 を回避できないことがあります。
- 一部のエンドポイント（たとえば、映像エンドポイント）が、H.323v2 機能をサポートしません。

図 6-2　トランスコーディングを使用したクラスタ間コール フロー



Unified CM は、MRG（メディア リソース グループ）を使用して、クラスタ内の Unified CM サーバ間で、MTP リソースとトランスコーディング リソースの共有を可能にします。さらに、クラスタ間トランクを介したコールの場合、MTP リソースとトランスコーディング リソースは、必要な場合だけ使用されます。したがって、LBR コーデックをサポートしないアプリケーションに対して MTP サービスを設定する必要がなくなります。

次の特性が、分散型コール処理配置に適用されます。

- トランスコーディングを必要とするクラスタ間コールだけが、MTP サービスを使用します。たとえば、コールの両方のエンドポイントが G.729 コーデックを使用できる場合、トランスコーディング リソースは使用されません。
- クラスタ内のサーバ間で MTP リソースを共有すると、リソースの使用効率が向上します。

IP 公衆網アクセス

MTP リソースとトランスコーディング リソースのもう 1 つのアプリケーション シナリオには、従来の公衆網ではなく、IP 公衆網へのアクセスをカスタマーに提供するサービス プロバイダーを含みます。このようなシナリオでは、ゲートキーパーがサービス プロバイダーのネットワークに置かれます。ダイヤル プランを単純化するために、各カスタマーは、エンドポイントに割り当てられている個々の IP アドレスを隠せるように、MTP を使用してコールを固定する必要があります。その後、サービス プロバイダーのセントラル オフィスは、従来の公衆網を介してリレーし、他のカスタマーとの IP 接続を提供できます。図 6-3 は、この配置モデルを示しています。

図 6-3　IP 公衆網アクセスの例

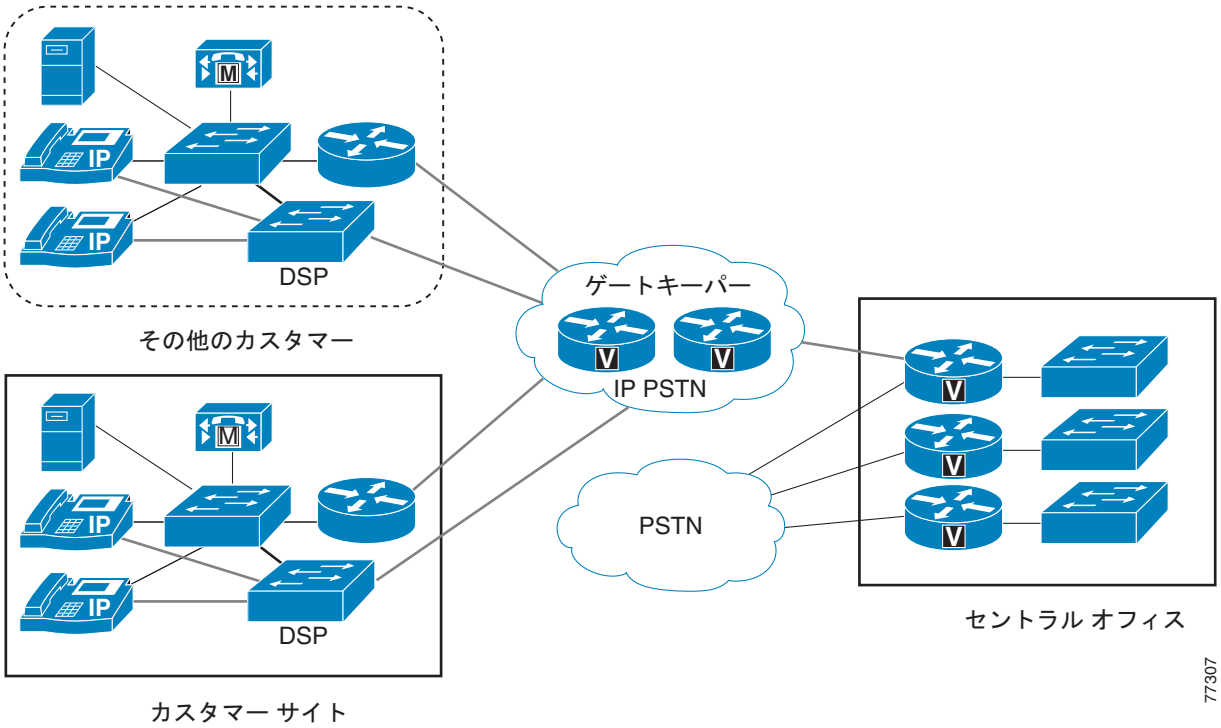


図 6-3 のカスタマー サイトは、前述の 3 つの配置モデル（単一サイト、集中型コール処理を使用するマルチサイト WAN、分散型コール処理を使用するマルチサイト WAN）の任意の 1 つを使用できることに注意してください。

カスタマー サイトから IP 公衆網までの H.323 トランクは、エンドポイントの IP アドレスがマスクされたままであるように、MTP を使用して設定される必要があります。したがって、すべての外部コールが MTP リソースを使用します。ただし、MTP リソースは、リソースの使用効率を高めるために、Unified CM クラスタ内で共有できます。MTP を利用してアドレスを隠蔽するこの手法は、SIP トランクでも使用できます。

CHAPTER 7

Music on Hold

Music on Hold（MoH）は、Cisco Unified Communications システムに組み込みの機能です。この機能は、発信者の通話が保留、転送、一時保留（コール パーク）、または ad-hoc 会議に追加されるときに、発信者に音楽を流します。MoH の実装は、比較的簡単ですが、ユニキャストおよびマルチキャスト トラフィック、MoH コール フロー、設定オプション、サーバの動作と要件について基本的な理解が必要です。この章では、Cisco エンタープライズ IP テレフォニー配置用に MoH リソースを設計し、プロビジョニングする方法について説明します。

Cisco Unified Communications Manager（Unified CM）は、さまざまなメディア リソースにアクセスできます。メディア リソースとは、ソフトウェアベースまたはハードウェアベースのエンティティであり、接続されている音声データ ストリームに対して何らかのメディア処理を行うものです。メディア処理機能には、複数のストリームを混合して 1 つの出力ストリームを作成する機能、ある接続から別の接続にストリームを渡す機能、ある圧縮タイプから別の圧縮タイプにデータ ストリームをトランスコードする機能が含まれます。

Unified CM は、次のタイプのメディア リソースを割り当て、使用します。

- メディア ターミネーション ポイント（MTP）リソース
- トランスコーディング リソース
- ユニキャスト会議リソース
- Annunciator リソース
- Music on Hold リソース

メディア リソース全般の詳細については、「メディア リソース」（P.6-1）の章を参照してください。

この章では、MoH 機能の設計について次の項目を説明します。

この章の新規情報

表 7-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 7-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
ゲートウェイに関する推奨事項	「推奨されるユニキャスト/マルチキャスト ゲートウェイ」（P.7-3）
クラスタ間トランクを介したマルチキャスト MoH	「分散型マルチサイト配置」（P.7-20）

MoH の基本的な配置

発信者に保留音が聞こえるようにするには、Unified CM の MoH 機能を有効にする必要があります。MoH 機能には、次の 2 つの主な要件があります。

- MoH オーディオ ストリーム ソースを流す MoH サーバ
- 通話を保留にするときに、MoH サーバが流す MoH ストリームを使用するように設定された Unified CM

統合 MoH 機能により、ユーザは、オンネットとオフネットのユーザを保留にするときに、ストリーミング ソースから音楽を流すことができます。このソースは、保留になったオンネットまたはオフネット デバイスに音楽を流します。オンネット デバイスには、IVR（音声自動応答装置）またはコール ディストリビュータによって保留、確認保留、またはコール パーク保留にされた端末デバイスやアプリケーションが含まれます。オフネット ユーザには、メディア ゲートウェイ統合プロトコル（MGCP）、Session Initiation Protocol（SIP）、および H.323 ゲートウェイを通じて接続されたユーザが含まれます。また、MoH 機能は、Foreign Exchange Station（FXS）ポートを通じて Cisco IP ネットワークに接続された、一般電話サービス（POTS）の電話機にも使用できます。統合 MoH 機能には、メディア サーバ、データベース管理、呼制御、メディア リソース マネージャ、およびメディア制御の機能領域が含まれます。MoH サーバは、音楽リソースとストリームを提供します。

MoH 機能は、Unified CM Administration インターフェイスを介して設定できます。エンド デバイスまたは機能が通話を保留にすると、Unified CM は、その保留デバイスを MoH メディア リソースに接続します。基本的に、Unified CM は、MoH サーバとの接続を確立するように、エンド デバイスに指示します。保留にされたデバイスが復帰すると、そのデバイスは MoH リソースから切り離され、通常のアクティビティを再開します。

ユニキャストおよびマルチキャスト MoH

Unified CM は、次の 2 つのタイプの MoH トランスポート メカニズムをサポートします。

- ユニキャスト
- マルチキャスト

ユニキャスト MoH は、MoH サーバから MoH オーディオ ストリームを要求するエンドポイントに直接送信されるストリームで構成されます。ユニキャスト MoH ストリームは、サーバとエンドポイント デバイス間のポイントツーポイント片方向オーディオ Real-Time Transport Protocol（RTP）ストリームです。ユニキャスト MoH は、ユーザまたは接続ごとに別々のソース ストリームを使用します。ユーザまたはネットワーク イベントを介して保留になるエンドポイント デバイスが増えるにつれて、MoH

ストリームの本数も増加します。したがって、20 台のデバイスが保留になっている場合、サーバとこれらのエンドポイント デバイス間のネットワーク上で、RTP トラフィックとしてストリームが 20 本生成されます。このような MoH ストリームが生成されると、ネットワークのスループットと帯域幅に対してマイナスの影響を与える可能性があります。しかし、ユニキャスト MoH が非常に役立つのは、マルチキャストが使用可能になっていないネットワークの場合や、デバイスがマルチキャスト対応になっていないネットワークの場合です。このようなときに、管理者はユニキャスト MoH を使用することで、MoH 機能を利用できます。

マルチキャスト MoH は、MoH サーバからマルチキャスト グループ IP アドレスに送信されるストリームで構成されます。MoH オーディオ ストリームを要求するエンドポイントは、必要に応じてこの IP アドレスに加わることができます。マルチキャスト MoH ストリームは、MoH サーバとマルチキャスト グループ IP アドレス間の、ポイントツーマルチポイント片方向オーディオ RTP ストリームです。マルチキャスト Music on Hold では、複数のユーザが同じオーディオ ソース ストリームを使用して Music on Hold を提供できるようにするので、システム リソースと帯域幅を節約できます。したがって、20 台のデバイスが保留中であっても、ネットワーク上で 1 つの RTP トラフィックのストリームだけしか生成されない場合もあります。したがって、マルチキャストは、ソース デバイスに対する CPU の影響を大幅に削減し、共通パス上の伝送の帯域幅使用量も大幅に削減するので、MoH などのサービスの配置に非常に魅力的なテクノロジーです。しかし、ネットワークがマルチキャスト対応になっていない状況や、エンドポイント デバイスがマルチキャストを処理できない状況では、マルチキャスト MoH に問題が生じます。

IP マルチキャスト ネットワークの設計については、次の Web サイトで入手可能なオンラインの『*IP Multicast SRND*』資料を参照してください。

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

推奨されるユニキャスト / マルチキャスト ゲートウェイ

次の推奨ゲートウェイは、ユニキャスト MoH とマルチキャスト MoH の両方をサポートします。

- MGCP または H.323 を使用する Cisco Communication Media Module（CMM）、Cisco IOS 12.2(13)ZP3 以降のリリース、および Catalyst OS 8.1(1) 以降のリリース
- MGCP または H.323 を使用する Cisco 2800 シリーズおよび 3800 シリーズ ルータと、Cisco IOS 12.3(11)YZ2 以降のリリース
- SIP を使用する Cisco VG224 Analog Voice Gateway、Cisco 2800 シリーズ、および 3800 シリーズ ルータと、Cisco IOS 12.4(22)T 以降のリリース
- MGCP または H.323 を使用する Cisco VG224 Analog Voice Gateway と、Cisco IOS 12.3.11-YZ2 以降のリリース
- Cisco VG248 Analog Phone Gateway

（注）　ユニキャストおよびマルチキャスト MoH をサポートする販売終了したゲートウェイは、他にもあります。

共存 MoH サーバとスタンドアロン MoH

MoH 機能を利用するには、Unified CM クラスタに含まれているサーバを使用する必要があります。MoH サーバは、次のいずれかの方法で設定できます。

- 共存配置

  共存配置では、MoH 機能は Unified CM ソフトウェアも実行している、クラスタ内の任意のサーバ（パブリッシャまたはサブスクライバ）で実行されます。

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

- スタンドアロン配置

  スタンドアロン配置では、MoH 機能は Unified CM クラスタ内の専用サーバに置かれます。この専用サーバの機能は、MoH ストリームをネットワーク内のデバイスに送信することだけです。

MoH の固定ソースとオーディオ ファイル ソース

MoH のソースは、次のいずれかの方法で設定できます。

- Unified CM または MoH サーバ上のオーディオ ファイルを使用した MoH
  - オーディオ ファイルを使用したユニキャスト MoH
  - オーディオ ファイルを使用したマルチキャスト MoH
- 固定音楽ソースを使用した MoH（サウンド カード経由）
  - 固定ソースを使用したユニキャスト MoH
  - 固定ソースを使用したマルチキャスト MoH

MoH は、MoH サーバ上に格納されているオーディオ ファイルから生成できます。オーディオ ファイルは、次の形式のいずれかでなければなりません。

- G.711 A-law または mu-law
- G.729 Annex A
- ワイドバンド

MoH オーディオ ファイルは、MoH Audio File Management ページ（または Music On Hold Audio Source Configuration ページ）でファイル アップロード機能を使用して、.wav フォーマットのオーディオ ファイルを MoH サーバにアップロードすると、Unified CM によって自動的に生成されます。次に、Unified CM は、オーディオ ソース ファイルを指定されたコーデック タイプに適した MoH ソース ファイルに変換し、フォーマットします。MoH イベントが発生すると、MoH サーバは、設定されたオーディオ ソース ファイルを保留中の要求側デバイスにストリーミングします。

（注）　MoH オーディオ ソースの設定前に、.wav フォーマットのオーディオ ソース ファイルをクラスタ内の各 MoH サーバにアップロードしておく必要があります。オーディオ ソース ファイルをアップロードするには、管理者がクラスタ内の各 MoH サーバ上で Unified CM Administration インターフェイスに移動し、MoH Audio File Management ページでファイルのアップロード機能を使用する必要があります。この手順は、オーディオ ソース ファイルごとに実行する必要があります。オーディオ ソースを MoH オーディオ ストリーム番号に割り当て、MoH オーディオ ソースとして設定するには、事前にクラスタ内のすべての MoH サーバにオーディオ ソース ファイルをアップロードしておく必要があります。

録音済みまたはライブ オーディオが必要である場合、固定ソースから MoH を生成できます。このタイプの MoH の場合、サウンド カードが必要です。固定オーディオ ソースは、ローカル サウンド カードのオーディオ入力に接続されます。

このメカニズムにより、ラジオ、CD プレーヤー、または互換性があるその他のサウンド ソースを使用できます。固定オーディオ ソースからのストリームは、リアルタイムで変換され、Unified CM Administration によって設定されたコーデックに対応します。固定オーディオ ソースは、G.711（A-law または mu-law）、G.729 Annex A、およびワイドバンドに変換することができる、リアルタイムで変換可能な唯一のオーディオ ソースです。

固定またはライブ オーディオ ソースを MoH サーバに接続するには、Cisco MoH USB オーディオ サウンド カード（MOH-USB-AUDIO=）を使用する必要があります。この USB サウンド カードは、Cisco Unified CM Release 6.*x* 以降のリリースをサポートするすべての MCS プラットフォームと互換性があります。

（注）　Music On Hold を送信するときに固定オーディオ ソースを使用する場合は、事前に、著作権のあるオーディオ素材の再ブロードキャストについて、その適法性および問題を検討しておく必要があります。起こりうる問題については、貴社の法務部門に相談してください。

Unified CM クラスタに含まれる MoH サーバ

MoH 機能を利用するには、各 MoH サーバが Unified CM クラスタに含まれている必要があります。すべての MoH サーバは、パブリッシャ サーバと設定を共有し、データベース複製スキーマに加わる必要があります。具体的には、MoH サーバはデータベースによって次の情報を共有する必要があります（これらの情報は Unified CM Administration で設定されます）。

- オーディオ ソース：設定されたすべての MoH オーディオ ソースの数と ID
- マルチキャストまたはユニキャスト：これらのソースそれぞれに設定されたトランスポートの種類
- マルチキャスト アドレス：マルチキャストとしてストリーミングするように設定されたソースのマルチキャスト ベース IP アドレス

MoH サーバは、Unified CM クラスタの一部になり、自動的にデータベースの複製に加わります。スタンドアロン MoH サーバを設定するには、最初に、そのサーバに Unified CM を通常どおりにインストールします。次に、Cisco CallManager サービスを無効にし（スタンドアロン MoH サーバ上でのみ）、Cisco IP Voice Media Streaming Application を有効にします。

基本的な MoH と MoH コール フロー

ここでは、Unified CM で実装される MoH の基本的な動作、および標準的なコール フローのシナリオについて説明します。

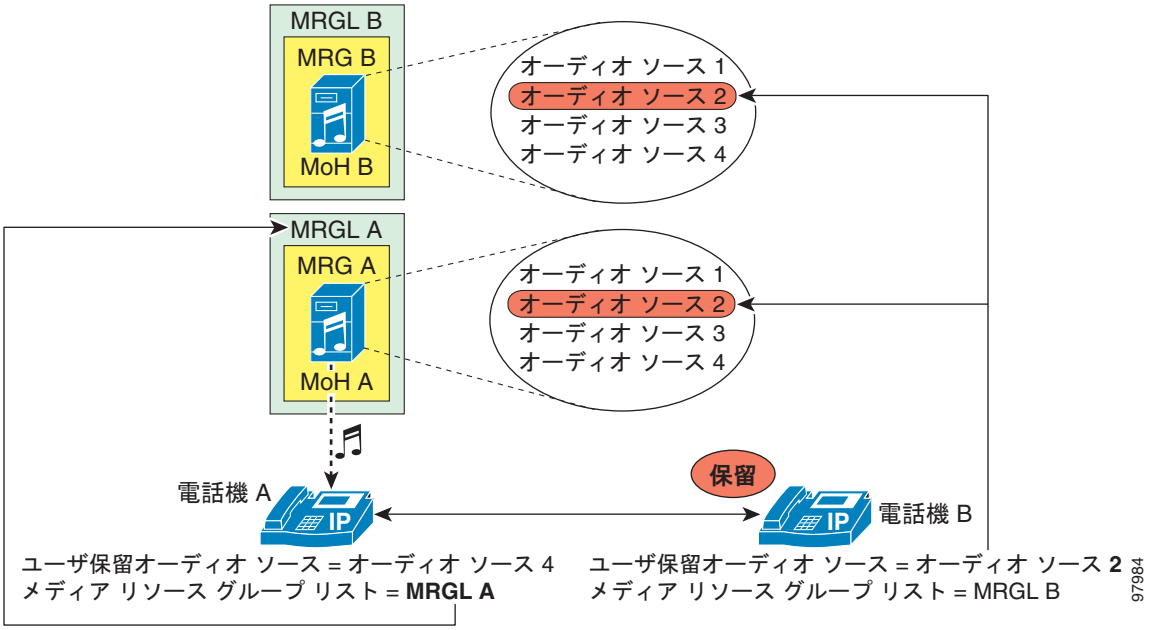
基本的な MoH

Cisco Unified Communications 環境における基本的な MoH の動作は、保留側と被保留側から構成されます。*保留側*とは、通話を保留にするエンドポイント ユーザまたはネットワーク アプリケーションです。一方、*被保留側*とは、保留にされたエンドポイント ユーザまたはデバイスです。

エンドポイントが受信する MoH ストリームは、エンドポイントを保留にするデバイス（保留側）のユーザ保留 MoH オーディオ ソースと、保留にされたエンドポイント（被保留側）に設定されたメディア リソース グループ リスト（MRGL）との組み合せによって決まります。保留側に対して設定されたユーザ保留 MoH オーディオ ソースによって、保留側が通話を保留にしたときに流されるオーディオ ファイルが決まります。被保留側に設定された MRGL は、被保留側が MoH ストリームを受信する元のリソースまたはサーバを指定します。

簡単に言えば、保留側の設定により、再生されるオーディオ ファイルが決まり、被保留側の設定により、そのファイルを再生するリソースまたはサーバが決まります。図 7-1 の例に示すように、電話機 A および B が通話中であるときに、電話機 B（保留側）で電話機 A（被保留側）を保留にする場合、電話機 A には、電話機 B に対して設定された MoH オーディオ ソース（オーディオ ソース 2）が聞こえます。ただし、電話機 A はこの MoH オーディオ ストリームを、電話機 A に対して設定された MRGL（リソースまたはサーバ）（MRGL A）から受信します。

図 7-1　ユーザ保留オーディオ ソースとメディア リソース グループ リスト（MRGL）



MRGL により、ユニキャスト専用デバイスが MoH ストリームを受信するサーバが決まるので、ユニキャスト専用デバイスを設定する場合は、ユニキャスト MoH リソースまたはメディア リソース グループ（MRG）を指定する MRGL を使用する必要があります。同様に、マルチキャスト対応デバイスは、マルチキャスト MRG を指定する MRGL を使用して設定する必要があります。

MoH 構成の設定値

MRGL、およびユーザ保留オーディオ ソースとネットワーク保留オーディオ ソースの設定値は、Unified CM Administration 内の複数の箇所で指定できます。それぞれの箇所で別々の設定値（優先順位あり）を設定できます。

個々のケースにユーザ オーディオ ソース設定値とネットワーク オーディオ ソース設定値のいずれかを適用するか決定するために、Unified CM は、次の優先順位で、*保留側*デバイスに対するこれらの設定値を使用します。

1. ディレクトリまたは回線設定（ゲートウェイなど、回線定義のないデバイスには、このレベルはありません）
2. デバイス設定値
3. 共通のデバイス設定
4. クラスタ全体のデフォルト設定

特定の保留側のオーディオ ソースを決定しようとする場合、Unified CM はまず、ディレクトリまたは回線レベルで設定されたユーザ（またはネットワーク）オーディオ ソースを調べます。このレベルが定義されていない場合、Unified CM は、保留側デバイスで設定されたユーザ（またはネットワーク）オーディオ ソースを調べます。このレベルが定義されていない場合、Unified CM は、保留側デバイス

の共通プロファイルに設定されたユーザ（またはネットワーク）オーディオ ソースを調べます。このレベルが定義されていない場合、Unified CM は、Unified CM システム パラメータで設定された、クラスタ全体のデフォルト オーディオ ソース ID を調べます（デフォルトでは、このオーディオ ソース ID は、ユーザ保留オーディオ ソースとネットワーク保留オーディオ ソースの両方に対して 1 に設定されています。これは、SampleAudioSource です）。

Unified CM は、*被保留側*デバイスの MRGL 設定値も、次の優先順位で使用します。

1. デバイス設定値
2. デバイス プールの設定値
3. システムのデフォルト MoH リソース

特定の被保留側の MRGL を決定しようとする場合、Unified CM は、デバイス レベルで設定された MRGL を調べます。このレベルが定義されていない場合、Unified CM は、被保留側デバイスのデバイス プールに対して設定された MRGL を調べます。このレベルが定義されていない場合、Unified CM は、システムのデフォルト MoH リソースを使用します。システムのデフォルト MoH リソースとは、MRG に割り当てられていないリソースであり、これらのリソースは常にユニキャストです。

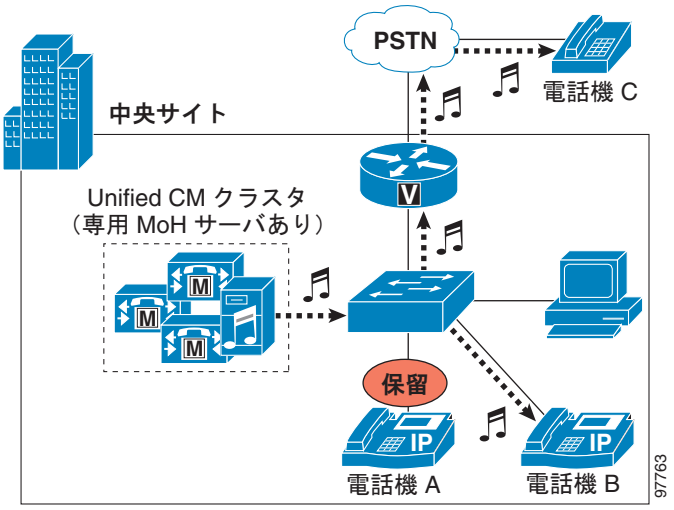
ユーザ保留とネットワーク保留

ユーザ保留には次のタイプがあります。

- IP Phone またはその他のエンドポイント デバイスでのユーザ保留
- MoH がゲートウェイにストリーミングされる公衆網でのユーザ保留

図 7-2 は、これらの 2 つのタイプのコール フローを示しています。電話機 A が電話機 B と通話中であるときに、電話機 A（保留側）で Hold ソフトキーを押すと、MoH サーバから電話機 B（被保留側）に音楽ストリームが送信されます。この音楽ストリームは、IP ネットワーク内の被保留側だけでなく、電話機 A が電話機 C を保留にする場合と同様に、公衆網上の被保留側にも送信できます。電話機 C の場合、MoH ストリームは音声ゲートウェイ インターフェイスに送信され、公衆網電話機に適したフォーマットに変換されます。電話機 A が Resume ソフトキーを押すと、被保留側（電話機 B または C）は、音楽ストリームから切り離され、電話機 A に再び接続されます。

図 7-2　ユーザ保留の基本的な例

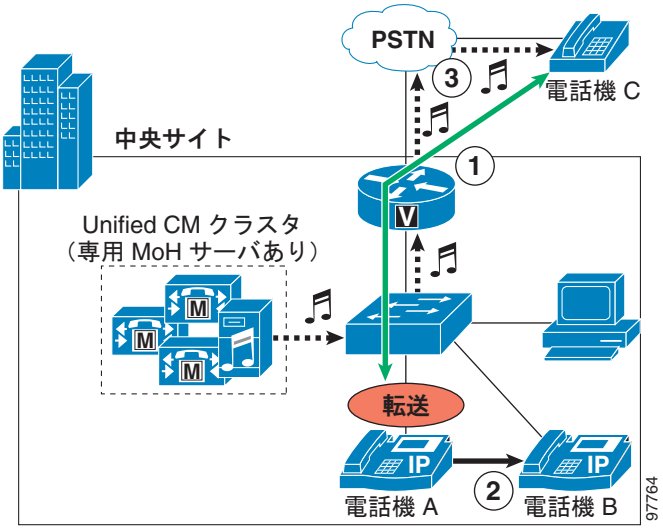


ネットワーク保留には次のタイプがあります。

- コール転送
- コール パーク
- 会議セットアップ
- アプリケーション ベースの保留

図 7-3 は、コール転送のコール フローを示しています。電話機 A が公衆網電話機 C からコールを受信する（ステップ 1）と、電話機 A はそのコールに応答し、電話機 B に転送します（ステップ 2）。転送プロセス時に、電話機 C は、ゲートウェイを介して MoH サーバから MoH ストリームを受信します（ステップ 3）。電話機 A が転送アクションを完了した後、電話機 C は音楽ストリームから切り離され、電話機 B（転送の宛先）に転送されます。このプロセスは、コール パークや会議セットアップなどの他のネットワーク保留操作の場合と同じです。

図 7-3　　コール転送のネットワーク保留の基本的な例



ユニキャストとマルチキャスト MoH コール フロー

MoH 操作は、通常の電話のコール フローに非常によく似ています。MoH サーバは、被保留側デバイスが必要に応じて接続または切断されるエンドポイント デバイスの役目をします。しかし、ユニキャストとマルチキャストの MoH コール フローの動作には、明らかな相違点があります。ユニキャスト MoH コール フローは、Unified CM から MoH サーバへのメッセージによって初期化されます。このメッセージは、被保留側デバイスの IP アドレスにオーディオ ストリームを送信するように、MoH サーバに指示します。一方、マルチキャスト MoH コール フローは、Unified CM から被保留側デバイスへのメッセージによって初期化されます。このメッセージは、設定されたマルチキャスト MoH オーディオ ストリームのマルチキャスト グループ アドレスに加わるように、エンドポイント デバイスに指示します。

MoH コール フローの詳細については、「ユニキャストとマルチキャスト MoH コール フローの詳細」（P.7-21）の項を参照してください。

MoH 設定上の考慮事項およびベスト プラクティス

ここでは、堅牢な MoH ソリューションの設計に役立つ、MoH 設定上の考慮事項とベスト プラクティスについて説明します。

コーデックの選択

MoH 配置に複数のコーデックが必要な場合、CM Service Parameters Configuration の IP Voice Streaming Media App サービス パラメータでコーデックを設定します。Clusterwide Parameters セクションの下の Supported MoH Codecs リストの中から、必要なコーデック タイプを選択してください。デフォルトでは、G.711 mu-law のみが選択されています。別のコーデック タイプを選択するには、リストをスクロールさせて該当するコーデックをクリックしてください。複数選択する場合は、CTRL キーを押したまま、マウスを使用して、リストをスクロールさせて複数のコーデックを選択します。選択終了後、Update ボタンをクリックしてください。

（注） MoH オーディオ ストリームに G.729 コーデックを使用する場合、このコーデックは会話用に最適化されているので、音楽用としては最低限のオーディオ品質であることに注意してください。

マルチキャスト アドレッシング

マルチキャスト MoH を設定するには、適切な IP アドレッシングが重要です。IP マルチキャストのアドレス範囲は 224.0.1.0 ～ 239.255.255.255 です。しかし、IANA（Internet Assigned Numbers Authority）は、公衆マルチキャスト アプリケーション用に 224.0.1.0 ～ 238.255.255.255 の範囲のアドレスを割り当てています。公衆マルチキャスト アドレスを MoH に使用しないことを強くお勧めします。代わりに、プライベート ネットワーク上の管理制御アプリケーション用に予約されている、239.1.1.1 ～ 239.255.255.255 の範囲内の IP アドレスを使用するように、マルチキャスト MoH オーディオ ソースを設定することをお勧めします。

さらに、次の理由で、ポート番号ではなく、IP アドレスでインクリメントするように、マルチキャスト オーディオ ソースを設定することも必要です。

- 保留にされた IP Phone は、ポート番号ではなく、マルチキャスト IP アドレスに加わる。

  Cisco IP Phone には、マルチキャスト ポート番号という概念はありません。したがって、特定のオーディオ ストリームに対して設定されているすべてのコーデックが、同じマルチキャスト IP アドレス（別々のポート番号であっても）に送信される場合、1 本のストリームしか必要ない場合であっても、すべてのストリームが IP Phone に送信されます。IP Phone は 1 本の MoH ストリームしか受信できないので、不必要なトラフィックでネットワークが飽和状態になる可能性があります。

- IP ネットワーク ルータは、ポート番号ではなく、IP アドレスに基づいて、マルチキャストをルーティングする。

  ルータには、マルチキャスト ポート番号という概念はありません。したがって、同じマルチキャスト グループ アドレス（別々のポート番号であっても）に送信される複数のストリームを検出すると、ルータは、そのマルチキャスト グループのすべてのストリームを転送します。必要なストリームは 1 本だけなので、ネットワーク帯域幅が過剰に利用され、その結果、ネットワークの輻輳が発生する可能性があります。

MoH オーディオ ソース

オーディオソースは、Unified CM クラスタ内のすべての MoH サーバ間で共有されるため、各オーディオソースファイルはクラスタ内の各 MoH サーバにアップロードしておく必要があります。クラスタごとに最大 51 の固有オーディオ ソースを設定できます（50 のオーディオ ファイル ソースと、サウンド カードを介した 1 つの固定/ライブ ソース）。追加のソースを提供する方法については、「複数の固定またはライブ オーディオ ソースの使用」（P.7-10）および「支店ルータからのマルチキャスト MoH」（P.7-17）の項を参照してください。

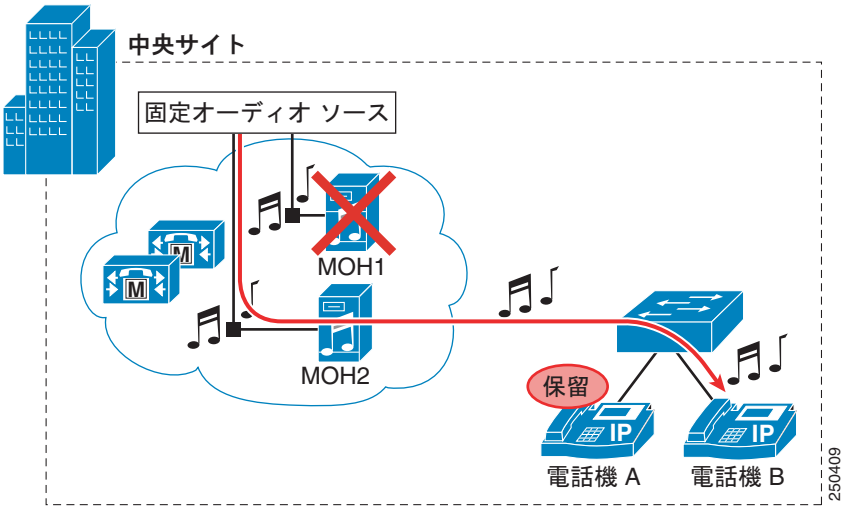
マルチキャストストリームに使用する、これらのオーディオソースには、**Allow Multicasting（マルチキャストの許可）**と **Play continuously（連続再生）（繰り返し）**を必ず有効にしてください。オーディオソースの連続再生を指定していない場合、MoH オーディオソースは、最初の保留にされた通話者のみが受け取り、追加された通話者は受け取りません。

複数の固定またはライブ オーディオ ソースの使用

Unified CM では、1 つのオーディオソースのみ設定できることに留意することが重要です。ただし、Unified CM クラスタ内の各 MoH サーバ は、Cisco MoH USB オーディオサウンドカード（MOH-USB-AUDIO）を介して 1 つの固定オーディオソースをストリーミングすることができます。複数の固定オーディオソースが必要な場合、追加の MoH サーバを追加して、これら複数のソースを提供することができます。各 MoH サーバのサウンドカードには、同じ、または別のオーディオを提供することができます。管理者は、MRG および MRGL の選択に基づいて、どの MoH サーバを選択するかを決定できます。複数のオーディオソースがこの方式で設定された場合、保留側の **User/Network Hold MoH Audio Source（ユーザ/ネットワーク保留 MoH オーディオソース）**は、固定オーディオソース（Unified CM に設定された 1 つの固定オーディオソース）に設定する必要があります。次に、被保留側の MRGL がその固定オーディオソースをデバイスにストリームする MoH サーバを決定します。

オーディオソースが同じ場合、この方式は固定オーディオソースの冗長性にも備えています。たとえば、図 7-4 には、2 つの MoH サーバがあり、それぞれは、ラジオ局のライブフィードからのオーディオをストリームするオーディオソースに接続された MOH-USB-AUDIO サウンドカードを備えています。電話機 B の MRGL には、まず MOH1 サーバを含む MRG が、次に MOH2 サーバを含む MRG が含まれます。電話機 A のユーザ/ネットワーク保留オーディオ ソースが固定オーディオソースに設定されているときに、コールが電話機 A と電話機 B の間で確立され、電話機 B が電話機 A によって保留にされた場合、電話機 B は、MOH1 サーバからライブフィードオーディオソースを受信します。MOH1 サーバがダウンしている（または利用可能なキャパシティがない）ときに、電話機 A が電話機 B を保留にすると、電話機 B は MOH2 サーバからライブフィードオーディオソースを受信します。

図 7-4　固定オーディオソース冗長性の例



（注）　マルチキャスト オーディオ ソースとしてラジオのライブ ブロードキャストを使用すると、法律上の問題が発生する恐れがあります。起こりうる問題については、貴社の法務部門に相談してください。

同一 Unified CM クラスタ内のユニキャストとマルチキャスト

状況に応じて、管理者は、1 つの Unified CM クラスタを設定することにより、ユニキャストとマルチキャストの両方の MoH ストリームを処理できます。この設定が必要なのは、マルチキャストをサポートしないデバイス、またはエンドポイントがテレフォニー ネットワークに含まれている場合、あるいはネットワークの一部でマルチキャストが使用可能になっていない場合です。

クラスタがユニキャストとマルチキャストの両方の MoH オーディオ ストリームをサポートできるようにするには、次のいずれかの方法を使用してください。

- 別々の MoH サーバを配置します。一方のサーバをユニキャスト MoH サーバとして設定し、もう一方のサーバをマルチキャスト MoH サーバとして設定します。
- 2 つのメディア リソース グループ（MRG）を備えた 1 台の MoH サーバを配置します。各グループには同じ MoH サーバが含まれますが、1 つの MRG はオーディオストリームはマルチキャスト用に設定し、もう 1 つはユニキャスト用に設定します。

どちらの場合も、少なくとも 2 つの MRG、および少なくとも 2 つのメディア リソース グループ リスト（MRGL）を設定する必要があります。ユニキャスト MoH を必要とするエンドポイントには、1 つのユニキャスト MRG と 1 つのユニキャスト MRGL を設定します。同様に、マルチキャスト MoH を必要とするエンドポイントには、1 つのマルチキャスト MRG と 1 つのマルチキャスト MRGL を設定します。

別々の MoH サーバを配置する場合、一方のサーバをマルチキャスト無効（ユニキャスト専用）に設定し、もう一方の MoH サーバをマルチキャスト有効に設定してください。ユニキャスト専用 MoH メディア リソースとマルチキャスト使用可能 MoH メディア リソースを、ユニキャスト MRG とマルチキャスト MRG にそれぞれ割り当てます。マルチキャスト MRG には **Use Multicast for MoH Audio** ボックスにチェックマークが付き、ユニキャスト MRG にはチェックマークが付いていないことを確認してください。また、これらのユニキャスト MRG とマルチキャスト MRG をそれぞれの MRGL に割り当てます。この場合、MRG がマルチキャストを使用するように設定されているかどうか、また MoH ストリームを流す元のサーバに基づいて、MoH ストリームのユニキャストまたはマルチキャストが行われます。

単一の MoH サーバをユニキャスト MoH とマルチキャスト MoH の両方に対して配置する場合は、サーバをマルチキャスト用に設定します。同じオーディオ ソースをユニキャスト MRG とマルチキャスト MRG の両方に割り当て、マルチキャスト MRG に対して **Use Multicast for MoH Audio** ボックスにチェックマークを付けます。この設定により、MRG がマルチキャストを使用するように設定されているかどうかだけに基づいて、MoH ストリームのユニキャストまたはマルチキャストが行われます。

（注）　ユニキャスト MRG を設定する場合は、混乱しないようにしてください。これは、MoH メディア リソースをユニキャスト MRG に追加する場合であっても、リソース名の最後に、[Multicast] が追加されるからです。このラベルは、リソースがマルチキャスト対応であるという単なる表示です。リソースがユニキャストとして送信されるか、マルチキャストとして送信されるかを決定するのは、**Use Multicast for MoH Audio** ボックスのチェックの有無です。

さらに、適切な MRGL を使用するように、個々のデバイスまたはデバイス プールを設定する必要があります。1 つまたは複数のデバイス プールにすべてのユニキャスト デバイスを含め、ユニキャスト MRGL を使用するようにこれらのデバイス プールを設定できます。あるいは、1 つまたは複数のデバイス プールにすべてのマルチキャスト デバイスを含め、マルチキャスト MRGL を使用するようにこれらのデバイス プールを設定することもできます。オプションとして、該当するユニキャスト MRGL またはマルチキャスト MRGL を使用するように、個々のデバイスを設定できます。最後に、個々のデバイス、または（電話デバイスの場合）個々の回線かディレクトリ番号ごとに、ユーザ保留オーディオ ソースおよびネットワーク保留オーディオ ソースを設定して、適切なオーディオ ソースを割当ます。

マルチキャスト MoH とユニキャスト MoH の両方を同じクラスタに配置する方法を選択する場合は、必要なサーバの数を考慮することが重要です。単一の MoH サーバをユニキャストとマルチキャストの両方に使用すると、クラスタ全体に必要な MoH サーバの数が減ります。マルチキャスト MoH サーバとユニキャスト MoH サーバを別々に配置すると、クラスタ内に必要なサーバの数が明らかに増えます。

冗長性

完全な冗長性のある MoH 動作を確保するために複数の MoH サーバを設定し、配置することをお勧めします。最初の MoH サーバに障害が発生したり、要求を処理するために必要なリソースがなくなったために使用不能になると、2 番目のサーバが自動的に MoH 機能を引き継ぎ、要求に応答します。適切な冗長構成のために、クラスタ内の 2 つ以上の MoH サーバから各 MRG にリソースを割り当ててください。

マルチキャストとユニキャストの両方の MoH が必要な環境では、ネットワーク内のすべてのエンドポイントの MoH 冗長性が確保されるように、必ず両方のトランスポート タイプに冗長性をもたせてください。

Quality of Service（QoS）

時間に依存する重要なリアルタイム アプリケーション（音声など）に遅延または損失がないように、1 つのネットワーク上のデータと音声のコンバージェンスには、適切な QoS が必要です。音声トラフィック用の適切な QoS を確保するには、ストリームがネットワークに入り、通過するときに、ストリームのマーク付け、分類、およびキューイングを行って、音声ストリームを重要度の低いトラフィックよりも優先的に処理する必要があります。MoH サーバは、DSCP（Differentiated Services Code Point）値 46 または PHB（Per Hop Behavior）値 EF（ToS 値 0xB8 に相当）を使用して、オーディオ ストリーム トラフィックに、音声ベアラトラフィックと同じマークを自動的に付けます。したがって、ネットワーク上で QoS が適切に設定されている限り、MoH ストリームは、音声 RTP メディア トラフィックとして分類され、プライオリティ キューイングとして扱われます。

MoH サーバと Unified CM サーバ間のコール シグナリング トラフィックは、デフォルトで DSCP 値 24 または PHB 値 CS3（ToS of 0x60 に相当）を使用して自動的にマーキングされます。したがって、ネットワーク上で、QoS が適切に設定されている限り、他のすべてのコール シグナリングと同様、ネットワーク内で、このコール シグナリング トラフィックは、適切に分類されキューに入れられます。

MoH リソース用のハードウェアとキャパシティ プランニング

MoH リソースも、他のすべてのメディア リソースと同じように、ハードウェアを配置し、設定した後、予想されたネットワークのコール量を確実にサポートするために、キャパシティ プランニングが非常に重要です。このため、MoH リソースのハードウェア キャパシティを認識し、このキャパシティとの関連からマルチキャストとユニキャストの MoH の役割を考慮することが重要です。

サーバ プラットフォームの最大同時セッション数

表 7-2 は、サーバ プラットフォームと、そのプラットフォームがサポートできる最大同時 MoH セッション数をリストしています。MoH セッションがこの最大同時セッション数を超えてから、さらに負荷が増えると、MoH 品質の低下、不規則な MoH 動作、または MoH 機能の喪失までも発生する恐れがあるので、ネットワークのコール量が最大同時セッション数を超えないようにしてください。

表 7-2　サーバ プラットフォーム タイプごとの最大 MoH セッション数

サーバ プラットフォーム	サポートされるコーデック	サポートされる MoH セッション数
MCS 7816 MCS 7825	G.711（A-law および mu-law） G.729a ワイドバンド オーディオ	共存サーバまたはスタンドアロンサーバ： 250 MoH セッション[1]
MCS 7835 MCS 7845	G.711（A-law および mu-law） G.729a ワイドバンド オーディオ	共存サーバまたはスタンドアロンサーバ： 500 MoH セッション

1. Unified CM クラスタごとに最大 51 の固有オーディオ ソースを設定できます。

次の MoH サーバー設定パラメータは、MoH サーバのキャパシティに影響を与えます。

- **Maximum Half Duplex Streams**

  このパラメータにより、ユニキャスト MoH に配置できるデバイスの数が決まります。デフォルトでは、この値は 250 に設定されています。

  Maximum Half Duplex Streams パラメータは、次の公式から得られた値に設定する必要があります。

  （サーバーおよび配置キャパシティ）–（[マルチキャスト MoH ソースの数] × [有効な MoH コーデックの数]）

  次の例を参考にしてください。

MCS-7835 スタンドアロン MoH サーバ	マルチキャスト MoH オーディオ ソース	有効な MoH コーデック（G.711 mu-law と G.729）	**Maximum Half Duplex Streams**
500	- (12	× 2)	= **476**

したがって、この例では、Maximum Half Duplex Streams パラメータは 476 未満の値で設定されます。

このパラメータには、プラットフォームや配置タイプ（共存またはスタンドアロン）に基づいて、表 7-2 に示すキャパシティよりも大きい値を絶対に設定しないでください。

- **Maximum Multicast Connections**

  このパラメータにより、マルチキャスト MoH に配置できるデバイスの数が決まります。

  Maximum Multicast Connections パラメータは、必要に応じてすべてのデバイスを確実にマルチキャスト MoH に配置できるような数に設定する必要があります。MoH サーバが生成できるマルチキャストストリームは、有限ですが（最大 204）、多数の保留デバイスを各マルチキャスト ストリームに加えることができます。このパラメータは、同時にマルチキャスト MoH に配置される可能性のあるデバイスの数、またはそれよりも大きい数に設定する必要があります。一般的なマルチキャスト トラフィックは、生成されるストリームの数に基づいて決まりますが、Unified CM では、マルチキャスト MoH に実際に配置されたデバイスの数または各マルチキャスト MoH ストリームに加えられたデバイスの数が適用されます。この方式は、マルチキャスト トラフィックが通常トラッキングされる方法と異なりますが、このパラメータを適切に設定することが重要です。

  （注）　Unified CM クラスタごとに設定できる固有オーディオ ソースの上限は 51 で、MoH ストリームに使用可能なコーデックの上限は 4 つであるため、MoH サーバごとのマルチキャスト ストリームの最大数は 204 です。

これらのパラメータを適切に設定しないと、MoH サーバ リソースが十分に使用されない、またはサーバがネットワーク負荷を処理できないといった問題が発生する可能性があります。

（注）　表 7-2 にリストされている最大セッションの上限は、ユニキャスト、マルチキャスト、またはユニキャストとマルチキャストの同時セッションに適用されます。この上限は、トランスポート メカニズムに関係なく、プラットフォームがサポートできる推奨最大セッション数を示しています。

リソースのプロビジョニングとキャパシティ プランニング

共存またはスタンドアロンの MoH サーバ設定のプロビジョニングを行う場合、ネットワーク管理者は、MoH オーディオ ストリームに使用されるトランスポート メカニズムのタイプを考慮する必要があります。ユニキャスト MoH を使用する場合、保留される各デバイスには、別々の MoH ストリームが必要です。しかし、マルチキャスト MoH と単一のオーディオ ソースのみを使用する場合、保留にするタイプのデバイス数に関係なく、設定されているコーデック タイプごとに必要な MoH ストリームは 1 つだけです。

たとえば、30,000 台の電話機のあるクラスタがあり、保留率が 2% である（すべてのエンドポイント デバイスの 2% だけが、常に保留になる）場合、600 の MoH ストリームまたはセッションが必要です。ユニキャスト専用の MoH 環境の場合、次の計算で示されているように、この負荷を処理するには、2 つの共存（またはスタンドアロン）MoH サーバが必要です。

[（MCS 7835 または 7845 共存サーバごとに 500 セッション）×（共存サーバ 1 台）] +
[（MCS 7816 または 7825 共存サーバごとに 250 セッション）×（共存サーバ 1 台）] >
600 セッション

一方、たとえば、36 の固有 MoH オーディオ ストリームがあるマルチキャスト専用 MoH 環境には、次の計算で示されているように、1 つの共存 MoH サーバ（MCS 7816 または 7825）だけが必要です。

（MCS 7816 または 7825 共存サーバごとに 250 セッション）×（共存サーバ 1 台）> 36 セッション

36 の固有マルチキャスト ストリームは、次のいずれかの方法でプロビジョニングできます。

- 単一のコーデックを使用して 36 の固有オーディオ ソースをストリーミングする。
- 2 つのコーデックだけを使用して 18 の固有オーディオ ソースをストリーミングする。
- 3 つのコーデックだけを使用して 12 の固有オーディオ ソースをストリーミングする。
- 4 つのコーデックすべてを使用して 9 つの固有オーディオ ソースをストリーミングする。

上記の例で示されているように、マルチキャスト MoH は、ユニキャスト MoH よりも、サーバ リソースを大幅に節約できます。

上記の例では、2% の保留率は、30,000 台の電話機に基づくものであり、保留になる可能性があるネットワーク内のゲートウェイまたはその他のエンドポイント デバイスを考慮していません。こうしたその他のデバイスは、電話機と同じように保留になる可能性があるので、保留率を計算するときは、これらのデバイスも考慮する必要があります。

上記の計算では、MoH サーバの冗長性を見込んでいません。MoH サーバに障害が発生する場合、またはユーザの 2% 以上が同時に保留になる場合、このシナリオでは、オーバーフローが発生したり負荷が増えたときに処理するための MoH リソースがありません。MoH リソースの計算には、冗長性に配慮して十分に余裕のあるキャパシティを含める必要があります。

MoH に対する IP テレフォニー配置モデルの影響

各種 IP テレフォニー配置モデルにより、MoH の構成設計にはさらに考慮事項が発生します。配置モデルの選択が、MoH のトランスポート メカニズム（ユニキャストまたはマルチキャスト）、リソースのプロビジョニング、およびコーデックの決定に影響を与える場合があります。ここでは、各種配置モデルに関連した問題について説明します。

配置モデルの詳細については、「Unified Communications の配置モデル」（P.2-1）の章を参照してください。

単一サイト キャンパス（すべての配置に関連）

単一サイト キャンパス配置は、通常、LAN インフラストラクチャに基づくものであり、大量のトラフィックに対して十分な帯域幅が用意されています。LAN インフラストラクチャでは一般に帯域幅が制限されないので、単一サイト配置内のすべての MoH オーディオ ストリームには、G.711（A-law または mu-law）コーデックの使用をお勧めします。G.711 は、IP テレフォニー環境に、最適な音声と音楽のストリーミング品質を提供します。

MoH サーバの冗長性も考慮する必要があります。MoH サーバが過負荷になるか、使用不能になった場合でも、複数の MoH サーバを設定し、それらのサーバを優先順に MRG に割り当てておくと、別のサーバが制御を引き継いで、MoH ストリームを流すことができます。

ネットワーク テクノロジーの多様性が増すにつれて、大規模な単一サイト キャンパスでは、一部のエンドポイント デバイスがマルチキャストをサポートできなくなる可能性があります。このため、ユニキャストとマルチキャストの両方の MoH リソースを配置する必要があります。たとえば、無線 IP Phone は、無線テクノロジーの動作により、マルチキャストをサポートしません。したがって、無線 IP Phone を配置する場合は、マルチキャストとユニキャストの両方の MoH を設定する必要があります。

オフネット コールとアプリケーション処理コールが、保留時に期待された MoH ストリームを受け取るには、適切な MRGL とオーディオ ソースを使用してすべてのゲートウェイとその他のデバイスを設定するか、それらを適切なデバイス プールに割り当ててください。

集中型マルチサイト配置

集中型コール処理を使用するマルチサイト IP テレフォニー配置には、一般的に、中央以外の複数のサイトとの WAN 接続が含まれます。これらの WAN リンクは、通常、帯域幅とスループットの障害になります。これらのリンク上での帯域幅使用量を最小限にするには、WAN を通過するすべての MoH オーディオ ストリームとして G.729 コーデックを使用することをお勧めします。G.729 コーデックは、音楽アプリケーションではなく、音声用に最適化されています。したがって、MoH トランスポートに G.729 がもたらす品質の低下よりも、帯域幅の節約がはるかに重要な問題である WAN 上でのみ、G.729 を使用してください。さらに、マルチキャスト トラフィックにより、帯域幅を大幅に節約できるので、WAN を介してエンドポイントにオーディオを流す場合は、常にマルチキャスト MoH を使用する必要があります。

WAN を介して G.729 を使用するときに MoH ストリームの音声品質が問題になる場合は、WAN を介した MoH オーディオ ストリームに G.711 コーデックを使用し、音声コールには引き続き G.729 を使用します。WAN を介した MoH ストリームの送信に G.711 コーデックを使用し、WAN を介した音声コールの送信に G.729 コーデックを使用するには、Unified CM リージョンにすべての MoH サーバだけを配置し、そのリージョンが他のリージョンとの間で G.711 を使用するように設定します。この設定により、WAN の一方の側にある 2 つの電話機間でコールを発信するときは、それぞれのリージョンの間で G.729 コーデックが使用されます。ただし、一方の通話者がコールを保留にした場合、MoH オーディオ ストリームは G.711 を使用して符号化されます。これは、G.711 が、MoH サーバのリージョンと、保留にされた電話機のリージョンとの間で使用するコーデックとして設定されているためです。

コール アドミッション制御と MoH

IP テレフォニー トラフィックが WAN リンク上を流れる場合は、コール アドミッション制御（CAC）が必要です。このようなリンク上では使用可能な帯域幅が制限されているので、適切なコール アドミッション制御がないと、音声メディア トラフィックの遅延または損失が起きる可能性が高くなります。詳細については、「コール アドミッション制御」（P.9-1）を参照してください。

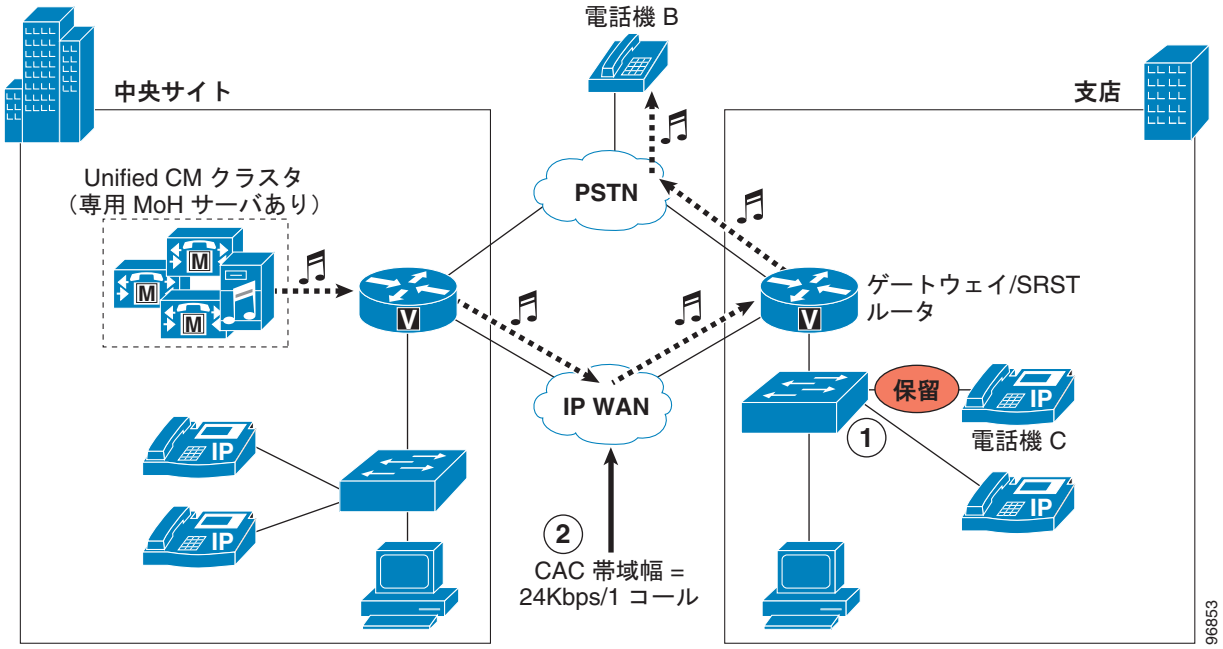
Unified CM の（静的ロケーションまたは RSVP 対応ロケーションのいずれかに基づく）コール アドミッション制御は、WAN を通過するユニキャスト MoH ストリームをトラッキングできますが、マルチキャスト MoH ストリームはトラッキングできません。したがって、WAN 帯域幅が完全にサブスクライブされた場合であっても、マルチキャスト MoH ストリームは、コール アドミッション制御によって WAN へのアクセスを拒否されません。ストリームは WAN を介して送信され、その結果、オーディオ ストリームの品質が低下し、WAN を通過するその他のすべてのコールの品質も低下する可能性があります。マルチキャスト MoH ストリームがこのオーバーサブスクリプション状態にならないようにするには、帯域幅を追加して Low-Latency Queuing（LLQ）音声プライオリティ キューを設定することによって、すべてのダウンストリーム WAN インターフェイス上で QoS 設定を余分にプロビジョニングする必要があります。MoH ストリームは単方向であるため、ダウンストリーム インターフェイス（中央サイトからリモート サイトへ）の音声プライオリティ キューのみを余分にプロビジョニングする必要があります。WAN リンクを通過する可能性があるすべての固有マルチキャスト MoH ストリームに対して、十分な帯域幅を追加してください。たとえば、4 つの固有マルチキャスト オーディオ ストリームが WAN を通過する可能性がある場合、音声プライオリティ キューに 96 Kbps を追加します（4 × 24 Kbps（G.729 オーディオ ストリームごと）= 96 Kbps）。

図 7-5 は、集中型マルチサイト配置におけるコール アドミッション制御と MoH の例を示しています。この例の場合、IP Phone C が公衆網電話機（電話機 B）とコール中であると想定します。この時点では、WAN 上で帯域幅は消費されていません。電話機 C で Hold ソフトキーを押すと（ステップ 1）、電話機 B は、WAN を介して中央サイトの MoH サーバから MoH ストリームを受信するので、リンク上の帯域幅を消費します。コール アドミッション制御でこの帯域幅を考慮すべきかどうかは、MoH ストリームのタイプに応じて決まります。マルチキャスト MoH が流れる場合、コール アドミッション制御は、24 Kbps が消費されているとは見なしません（したがって、ダウンストリーム WAN インターフェ

イス上の QoS はそれに応じてプロビジョニングされなければなりません）。しかし、ユニキャスト MoH が流れる場合、コール アドミッション制御は、使用可能な WAN 帯域幅から 24 Kbps を差し引きます（ステップ 2）。

（注）　上記の例では、ユニキャスト MoH を WAN 上で流すことを示唆しているように見えますが、これは、MoH とのロケーションベースのコール アドミッション制御をわかりやすく示すための例に過ぎません。また、この設定の推奨または保証を意味するものではありません。前述のように、WAN を介した MoH オーディオ ストリームの送信用のトランスポート メカニズムには、マルチキャスト MoH をお勧めします。

図 7-5　ロケーションベースのコール アドミッション制御と MoH



支店ルータからのマルチキャスト MoH

Cisco Unified Survivable Remote Site Telephony（SRST）Release 3.0 から、MoH は支店の SRST ルータのフラッシュを介して、リモートまたは支店のサイト内でマルチキャストできるようになりました。SRST Release 3.2 から、MoH は支店の SRST ルータのアナログ ポートに接続されているライブ フィードを介して、支店のサイト内でマルチキャストできるようになりました。これらの 2 つの方式によって支店のルータから MoH をマルチキャストすると、Cisco Unified Communications MoH の機能が次の シナリオの両方において向上します。

- 非フォールバック モード

  WAN が稼動中で、電話機が Unified CM で制御されている場合、この設定では、ローカルに発信される MoH を提供し、WAN を介してリモート支店サイトに MoH を転送する必要がなくなります。

- フォールバック モード

  SRST がアクティブで、支店のデバイスが中央サイトの Unified CM との接続を失った場合、支店のルータが継続して MoH をマルチキャストします。

いずれかのシナリオでライブ フィード オプションを使用している場合、ライブ フィードの入力を監視することにより、SRST ルータでは冗長性が確保され、ライブ フィードの接続が切断されても、フラッシュ内のファイルから MoH をストリームするようになります。マルチキャスト MoH を流す際に使用できるマルチキャスト アドレスとポート番号は、SRST ルータごとに 1 つのみです。このため SRST ルータではライブフィードとフラッシュファイルの両方からのストリーミングを同時に実行することはできません。また、SRST ルータでは、フラッシュから流すことのできるオーディオ ファイルは 1 つのみです。

（注）　SRST 機能が実際に使用されるかどうかに関係なく、SRST ライセンスが必要です。ライセンスが必要なのは、支店ルータのフラッシュから MoH を流すための設定が SRST コンフィギュレーション モードで行われるため、および SRST 機能が使用されない場合でも少なくとも 1 つの **max-ephones** と 1 つの **max-dn** を設定する必要があるためです。

非フォールバック モード

非フォールバック モード中（WAN が稼動していて、SRST がアクティブでない場合）、支店の SRST ルータは、マルチキャスト MoH をすべてのローカル Cisco Unified Communications デバイスに流すことができます。これを実現するには、支店ルータ上で設定された内容と同じマルチキャスト IP アドレスとポート番号をもつオーディオ ソースを使用して、Unified CM MoH サーバを設定する必要があります。このシナリオでは、マルチキャスト MoH オーディオ ストリームが、常に SRST ルータから発信されるので、中央サイトの MoH サーバのオーディオ ソースが WAN を通過する必要はありません。

中央サイトのオーディオ ストリームが WAN を通過しないようにするには、次のいずれかの方法を使用してください。

- 最大のホップ カウントを設定する

  中央サイトの MoH オーディオ ソースが、中央サイトの LAN より先に流れないように、最大ホップ カウントまたは TTL を十分に小さく設定します。

- WAN インターフェイス上でアクセス コントロール リスト（ACL）を設定する

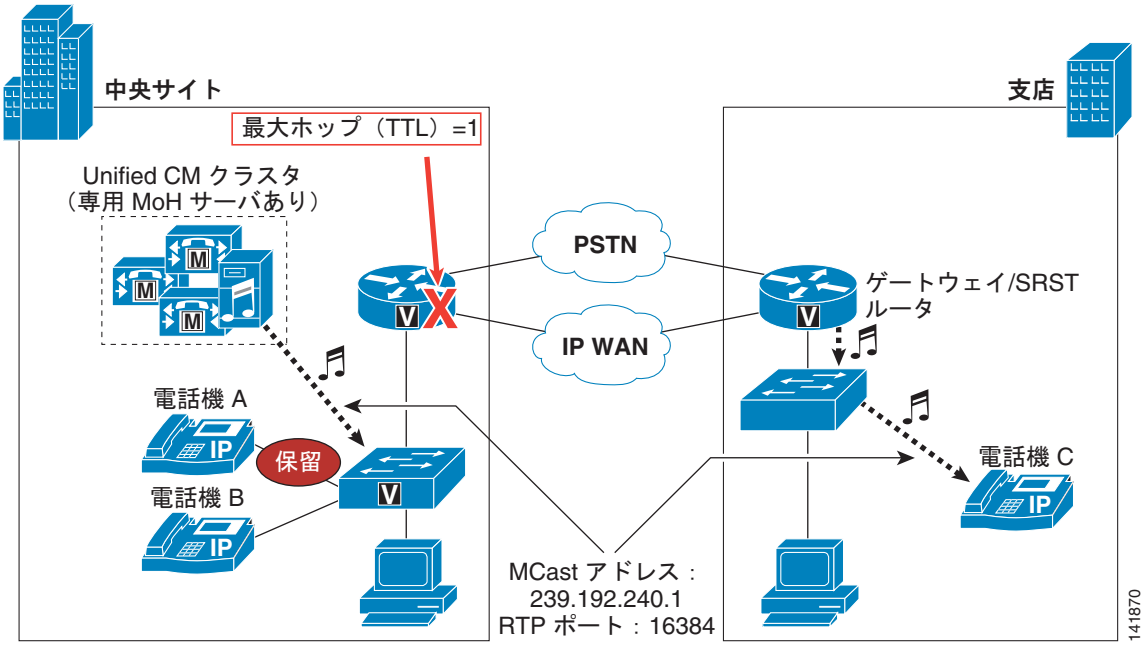
  中央サイトの WAN インターフェイス上で ACL を設定して、マルチキャスト グループ アドレス宛のパケットがインターフェイスから発信されないようにします。

- WAN インターフェイス上でマルチキャスト ルーティングを無効にする

  WAN インターフェイス上ではマルチキャスト ルーティングを設定しないでください。設定しなければ、マルチキャスト ストリームが WAN に転送されないことが保証されます。

図 7-6 は、フォールバック モードでないときに支店のルータからマルチキャスト MoH を流す仕組みを示しています。電話機 A で電話機 C を保留にすると、電話機 C は、ローカル SRST ルータからマルチキャスト MoH を受信します。この図では、MoH サーバは、（RTP ポート 16384 上で）239.192.240.1 にマルチキャスト オーディオ ソースを流します。しかし、最大ホップ数が 1 に制限されているので、このストリームは、ローカル MoH サーバのサブネットから WAN を通過して外に出ないことが保証されています。同時に、支店の SRST ルータまたはゲートウェイは、フラッシュまたはライブ フィードからオーディオ ストリームをマルチキャストします。このストリームも、マルチキャスト アドレスとして 239.192.240.1 を使用し、RTP ポート番号として 16384 を使用します。電話機 A で Hold ソフトキーを押すと、電話機 C は、SRST ルータから発信された MoH オーディオ ストリームを受信します。

図 7-6　支店ルータのフラッシュからのマルチキャスト MoH



この方法を使用してマルチキャスト MoH を配信する場合は、Unified CM クラスタ内のすべてのデバイスが、同じユーザ保留およびネットワーク保留オーディオ ソースを使用するように設定し、すべての支店ルータに同じマルチキャスト グループ アドレスとポート番号を設定します。保留側のユーザまたはネットワーク保留オーディオ ソースは、オーディオ ソースを特定するときに使用されるため、クラスタ内に複数のユーザまたはネットワーク保留オーディオ ソースを設定する場合、リモートの被保留側が常にローカルの MoH ストリームを受信することを保証する手段はありません。たとえば、中央サイトの電話機に設定されているオーディオ ソースが、そのユーザおよびネットワーク保留オーディオ ソースとして、グループ アドレス 239.192.254.1 を使用するものとします。この電話機がリモート デバイスを保留にすると、ローカル ルータのフラッシュの MoH ストリームがマルチキャスト グループ アドレス 239.192.240.1 に送信される場合でも、リモート デバイスは 239.192.254.1 に加わろうとします。代わりに、ネットワーク内のすべてのデバイスがマルチキャスト グループ アドレス 239.192.240.1 でユーザ/ネットワーク保留オーディオ ソースを使用するように設定し、すべての支店ルータが 239.192.240.1 でフラッシュからマルチキャストするように設定すると、リモート デバイスはすべて、そのローカル ルータから MoH を受信します。

マルチキャスト MoH を流すように設定された複数の支店ルータを含むネットワークでは、Unified CM クラスタ内に 51 を超える固有 MoH オーディオ ソースを含めることができます。支店サイトの各ルータは、固有オーディオ ソースをマルチキャストできます。ただし、すべてのルータが同じマルチキャスト グループ アドレス上でこのオーディオをマルチキャストする必要があります。また、中央サイトの MoH サーバは、この同じマルチキャスト グループ アドレス上で MoH ストリームをマルチキャストできます。したがって、100 の支店サイトそれぞれがオーディオ をマルチキャストする場合、クラスタには 実際には 101 の固有 MoH オーディオ ソース（100 の支店ストリームと 1 つの中央サイト ストリーム）が含まれることになります。中央サイトで 51 を超える固有オーディオ ストリームが必要な場合は、「複数の固定またはライブ オーディオ ソースの使用」（P.7-10）で説明されている方法を参照してください。

フォールバック モード

フォールバック モード中（WAN がダウンしていて SRST がアクティブな場合）、支店の SRST ルータはシャーシ内のすべてのアナログ ポートとデジタル ポートに、マルチキャスト MoH を流すことができます。これによりアナログ電話機および公衆網電話機に MoH を流すことができます。Cisco Unified SRST Release 4.0 から、フォールバックモード中の SCCP IP phone もマルチキャスト MoH ストリームを受信できるようになりました。このとき、SIP IP Phone は保留音を受け取ります。

支店のルータに対して、フォールバック モードのマルチキャスト MoH を設定する方法は、通常の設定方法と同じです。ただし、ルータに対して設定するマルチキャスト アドレスは、目的の動作によって異なります。支店のルータから、デバイスにマルチキャスト MoH をフォールバック モードでのみ流す必要がある場合（たとえば、リモート デバイスで受信する MoH が非フォールバック モード中に中央サイトの MoH サーバから発信される場合）、SRST ルータに設定したマルチキャスト アドレスとポート番号が、中央サイトの MoH サーバのいずれのオーディオ ソースと重複しないようにする必要があります。重複していると、リモート デバイスは、設定されているユーザ/ネットワーク保留オーディオ ソースに応じて、ローカル ルータのフラッシュから MoH を継続的に受信することがあります。

支店の SRST/ゲートウェイ ルータに、マルチキャスト MoH を設定すると、ルータはフォールバック モードでないときにも、MoH ストリームのマルチキャストを継続することに注意してください。

また、Cisco Unified SRST Release 4.0 から、フォールバック モードを設定して、SRST モードの Cisco Unified Communications Manager Express（Unified CME）を 使用できるようになりました。フォールバック モードの動作は同じですが、コンフィギュレーション コマンドが多少異なります。SRST コマンドは、Cisco IOS **call-manager-fallback** コンストラクトで入力しますが、SRST モードの Unified CME では、コマンドは t**elephony-service** で入力します。

SRST を介して MoH をマルチキャストする方法は 4 つあります。

- 支店ルータのフラッシュからの SRST マルチキャスト MoH
- ライブ フィードからの SRST マルチキャスト MoH
- SRST モードの Unified CME での支店ルータフラッシュからのマルチキャスト MoH
- SRST モードの Unified CME でのライブ フィードからのマルチキャスト MoH

Cisco SRST と Unified CME の設定の詳細については、次の Web サイトで入手可能な『*Cisco Unified SRST System Administrator Guide*』および『*Cisco Unified Communications Manager Express System Administrator Guide*』を参照してください。

http://www.cisco.com

分散型マルチサイト配置

分散型コール処理を使用するマルチサイト IP テレフォニー配置には、通常、サイト間の WAN または MAN 接続が含まれます。これらの低速リンクは、通常、帯域幅とスループットの障害になります。リンク上での帯域幅使用量を最小限にするには、リンクを通過するすべての MoH オーディオ ストリームとして G.729 コーデックを使用することをお勧めします。ただし G.729 コーデックは、音楽用ではなく、音声用に最適化されているので、MoH トランスポートに G.729 がもたらす品質の低下よりも、帯域幅の節約がはるかに重要な問題である WAN/MAN 上でのみ、G.729 を使用してください。

集中型マルチサイト配置の場合とは異なり、WAN を介して流れる MoH オーディオ ストリーム用に G.711 が必要になる可能性がある状況では、分散型マルチサイト環境で MoH オーディオ ストリームが G.711 を使用するように強制することはできません。MoH サーバが別の Unified CM リージョンに配置されている状況で、このリージョンとクラスタ間トランクまたは SIP トランクのリージョンとの間で G.711 コーデックが設定されている場合でも、2 つのクラスタ間のコールが一方の電話機によって保留

にされたときは、元の音声コールのコーデックが保持されます。これらのクラスタ間コールは、一般に、帯域幅の節約のために G.729 を使用して符号化されるため、一方のクラスタからの MoH ストリームも G.729 を使用して符号化されます。

Cisco Unified CM 7.1(2) 以降のリリースでは、Intercluster Trunk（ICT; クラスタ間トランク）または SIP トランクを使用するクラスタ間コールでのマルチキャスト MoH をサポートしています。この機能により、1 つの Unified CM クラスタ内のエンドポイントで別の Unified CM クラスタからストリーミングされたマルチキャスト MoH を聞くことができるようになるとともに、クラスタ間帯域幅をより効率的に使用できるようになります。この機能を活かすには、適切に設計された IP マルチキャスト環境が必要です。IP マルチキャストの詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html

Unified CM の初期のリリースでは、クラスタ間コールで利用できるのはユニキャスト MoH だけであり、ICT または SIP トランクで MoH が必要である場合に、各 Unified CM クラスタに少なくとも 1 つのユニキャスト MoH リソースを設定する必要があります。

分散型クラスタ間環境では、適切なマルチキャスト アドレス管理も、設計上の重要な考慮事項です。分散型ネットワーク全体で流れるリソースの重複を防止するために、いかなる MoH オーディオ ソース マルチキャスト アドレスも、配置内のすべての Unified CM クラスタに対して固有でなければなりません。

WAN を介したクラスタ化

その名前が示すように、クラスタオーバー WAN 配置には、他のマルチサイト配置と同様、低速 WAN リンクが含まれます。したがって、これらの配置にも、G.729 コーデック、マルチキャスト トランスポート メカニズム、および低速 WAN リンクを介した MoH トラフィックに対して欠かせない安定した QoS の、3 つの要件が必要です。

さらに、このタイプの設定では、WAN の各端部に MoH サーバ リソースを配置することも必要です。WAN に障害が発生した場合には、WAN の各端部のデバイスは、ローカルに配置された MoH サーバから、引き続き MoH オーディオ ストリームを受信できます。さらに、適切な MoH 冗長設定がきわめて重要です。WAN の各端部のデバイスには、MRGL を指定する必要があります。この MRGL の MRG には、少なくとも 1 つのローカル リソースが最優先になった MoH リソースの優先順位リストが必要です。プライマリ サーバが使用不能になるか、要求を処理できない場合に備えて、この MRG に対して、MoH リソースを追加設定しておく必要があります。WAN のローカル側のリソースは使用不能になった場合に備えて、リスト内で他に少なくとも 1 つの MoH リソースは、リモート側の MoH リソースを指定しておく必要があります。

ユニキャストとマルチキャスト MoH コール フローの詳細

次の各項では、SCCP および SIP エンドポイントの両方について、ユニキャストとマルチキャスト MoH コール フローの詳細な図と説明を示します。

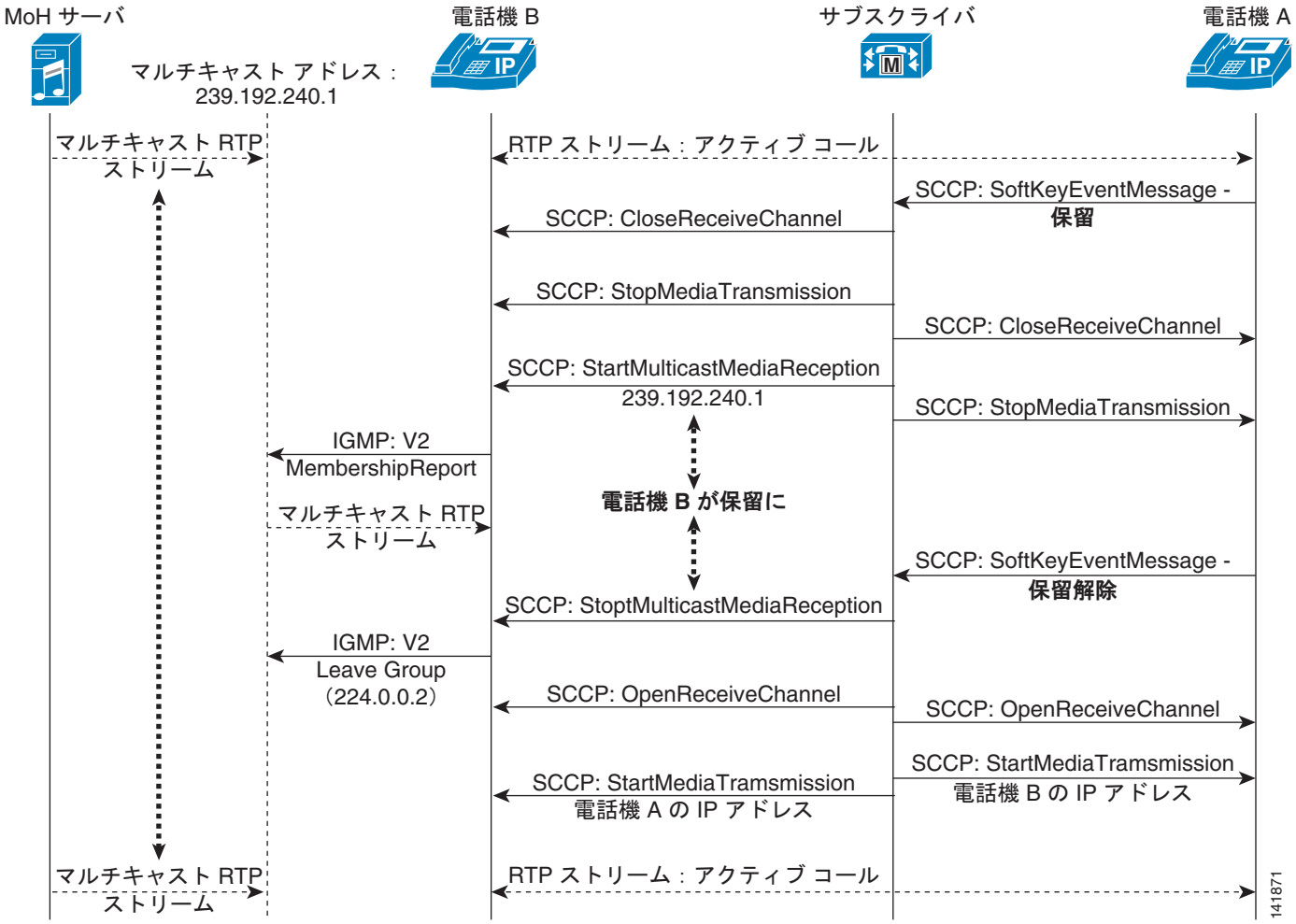
SCCP コール フロー

ここでは、Skinny Client Control Protocol（SCCP）エンドポイントでの Music On Hold のコール フローについて説明します。

SCCP マルチキャスト コール フロー

図 7-7 は、標準的な SCCP マルチキャスト コール フローを示しています。この図に示されているように、電話機 A で Hold ソフトキーが押されると、Unified CM は、Close Receive Channel（受信チャネルのクローズ）と Stop Media Transmission（メディア送信の停止）を電話機 A と電話機 B の両方に指示します。このアクションは、実質的に、RTP 双方向オーディオ ストリームを停止させます。次に、Unified CM は、マルチキャスト グループ アドレス 239.192.240.1 から、Start Multicast Media Reception（マルチキャスト メディア受信の開始）を電話機 B（被保留側）に指示します。その後、電話機 B はインターネット グループ管理プロトコル（IGMP）V2 の Membership Report メッセージを発行して、電話機 B がこのグループに加わることを示します。

図 7-7　SCCP マルチキャスト MoH コール フローの詳細



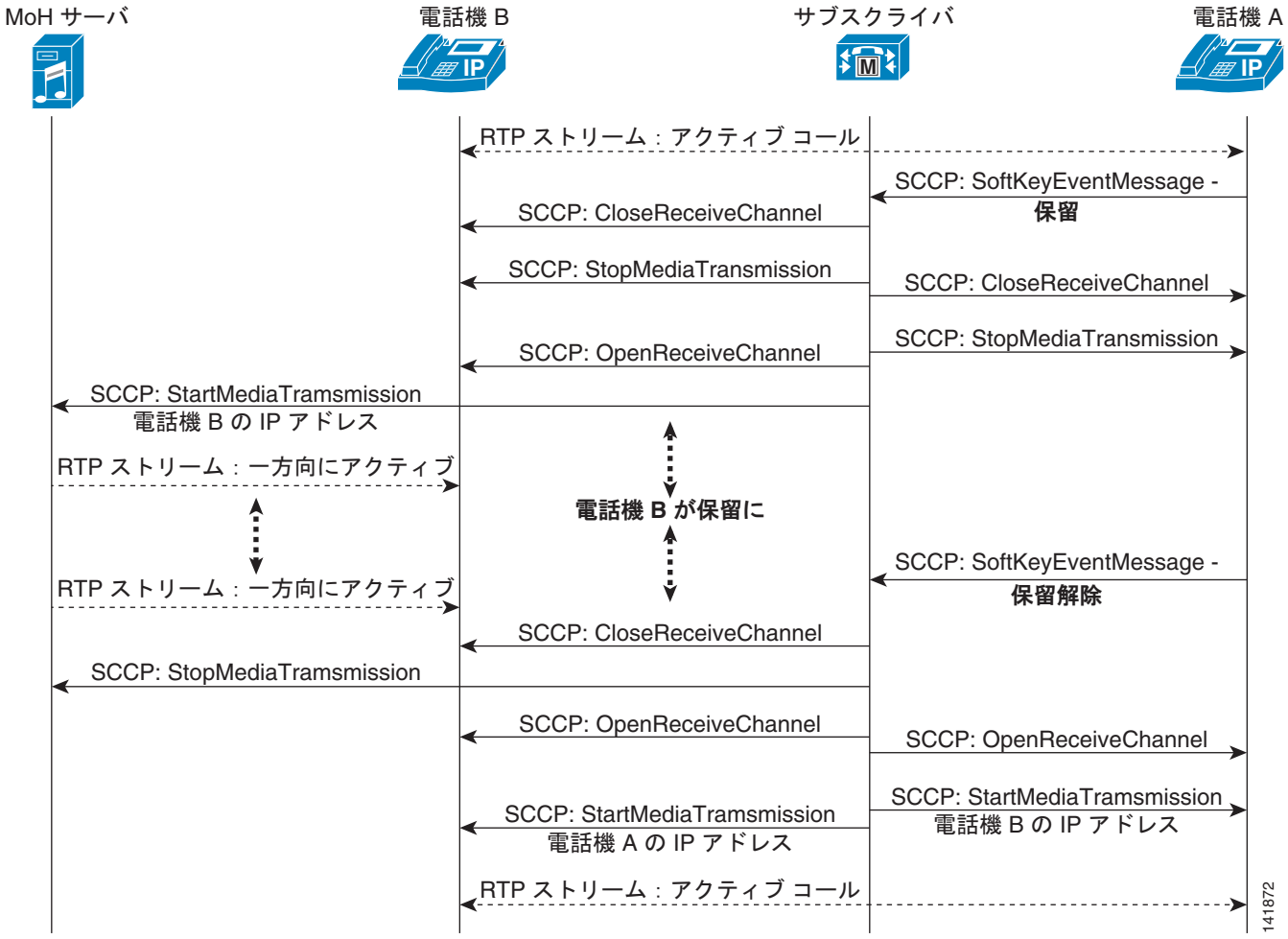
一方、MoH サーバがこのマルチキャスト グループ アドレスに RTP オーディオを送信しているので、電話機 B はそのマルチキャスト グループに加わった後、MoH ストリームの受信を開始します。電話機 A で Resume ソフトキーが押されると、Unified CM は、電話機 B に Stop Multicast Media Reception（マルチキャスト メディア受信の停止）を指示します。電話機 B は、マルチキャスト ストリームが必要なくなったことを示すために、IGMP V2 の Leave Group メッセージを 224.0.0.2 に送信します。これにより、実質的に MoH セッションが終了します。次に、Unified CM は、電話機 A と電話機 B 間の通話の開始時に送信するように、両方の電話機に一連の Open Receive Channel（受信チャネルのオープン）メッセージを送信します。その後すぐに、Unified CM は、互いの IP アドレスへの Start Media Transmission（メディア送信の開始）を両方の電話機に指示します。電話機は、RTP 双方向オーディオ ストリームを介して再び接続されます。

（注）　図 7-7 と図 7-8 のコール フロー図では、双方向 RTP オーディオ ストリームを使用して、初期化コールが電話機 A と電話機 B の間で行われることを前提としています。これらの図は、コール フローを示しているので、適切な MoH 動作に必要な関連トラフィックのみが記載されています。したがって、インタラクションがわかりやすいように、キープアライブ、確認応答、およびその他のトラフィックは省略されています。各図の初期化イベントは、電話機 A によって実行される Hold ソフトキー アクションです。

SCCP ユニキャスト コール フロー

図 7-8 は、SCCP ユニキャスト MoH コール フローを示しています。このコール フロー図では、電話機 A で Hold ソフトキーが押されると、Unified CM は、Close Receive Channel（受信チャネルのクローズ）と Stop Media Transmission（メディア送信の停止）を電話機 A と電話機 B の両方に指示します。このアクションは、実質的に、RTP 双方向オーディオ ストリームを停止させます。この時点まで、ユニキャストとマルチキャストの MoH コール フローは、まったく同じように動作します。

図 7-8　SCCP ユニキャスト MoH コール フローの詳細



次に、Unified CM は、Open Receive Channel（受信チャネルのオープン）を電話機 B（被保留側）に指示します。これは、マルチキャストの場合とまったく異なっています。マルチキャストでは、Unified CM は、Start Multicast Media Reception（マルチキャスト メディア受信の開始）を被保留側に指示します。次に、Unified CM は、MoH サーバに、電話機 B の IP アドレスへの Start Media

Transmission（メディア送信の開始）を指示します。これも、マルチキャスト MoH コール フローとはまったく異なる動作です。マルチキャストの場合、マルチキャスト グループ アドレスに加わるように、電話機に指示します。この時点で、MoH サーバは、片方向ユニキャスト RTP 音楽ストリームを電話機 B に送信します。電話機 A で Resume ソフトキーが押されると、Unified CM は、Stop Media Transmission（メディア送信の停止）を MoH サーバに指示し、Close Receive Channel（受信チャネルのクローズ）を電話機 B に指示して、実質的に MoH セッションを終了させます。マルチキャスト シナリオの場合と同じように、Unified CM は、一連の Open Receive Channel（受信チャネルのオープン）メッセージおよび Start Media Transmissions（メディア送信の開始）メッセージを電話機 A と電話機 B に相互の IP アドレスを使用して送信します。電話機は、RTP 双方向オーディオ ストリームを介して再び接続されます。

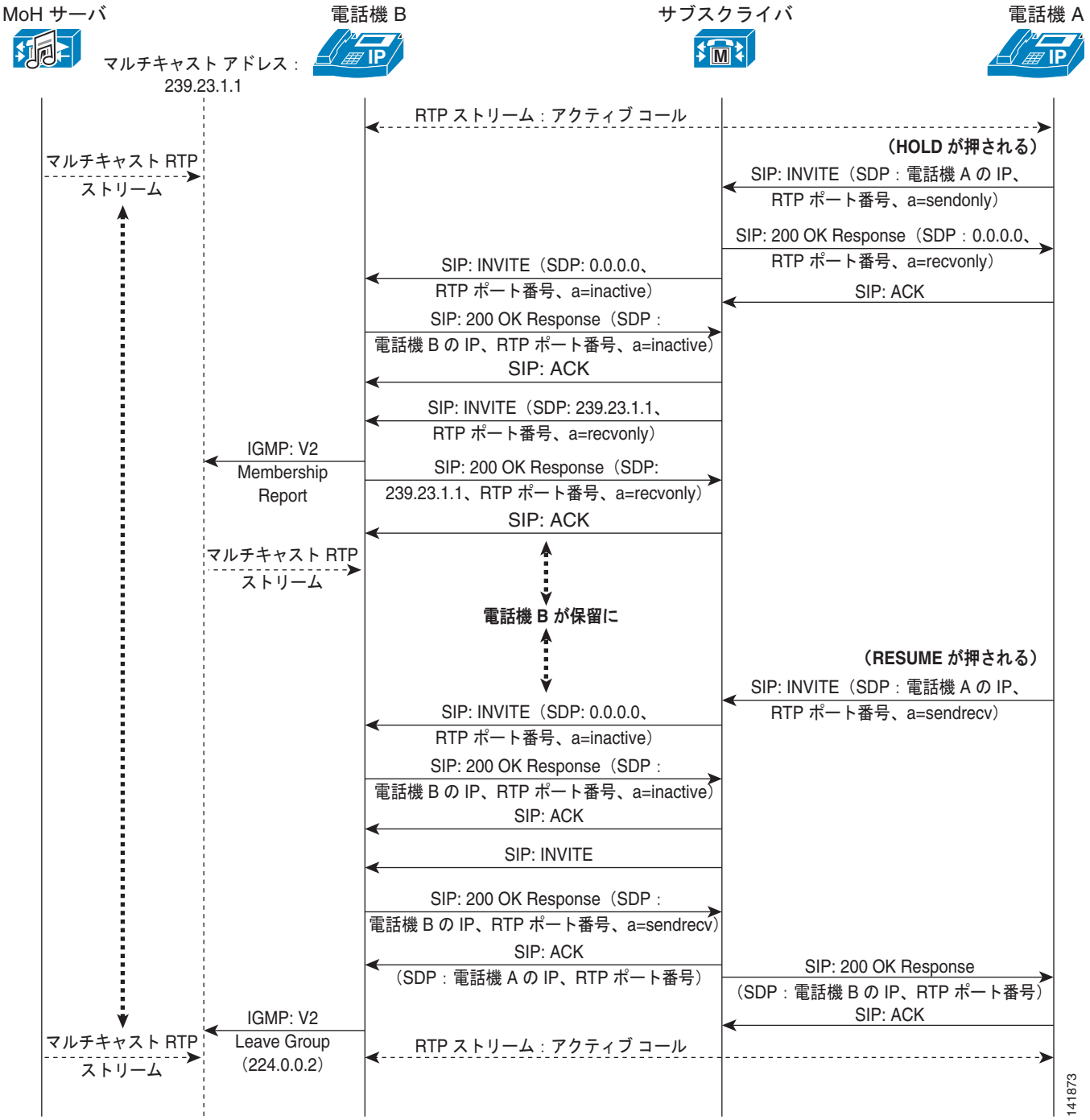
SIP コール フロー

ここでは、Session Initiation Protocol（SIP）エンドポイントでの Music On Hold のコール フローについて説明します。

SIP マルチキャスト コール フロー

図 7-9 は、標準的な SIP マルチキャスト コール フローを示しています。この図に示されているように、電話機 A で Hold ソフトキーが押されると、電話機 A は SIP INVITE を送信します。このときの Session Description Protocol（SDP）接続情報は電話機 A の IP アドレスを示し、メディア属性は sendonly を示しています。Unified CM は、SDP 接続情報が 0.0.0.0、メディア属性が recvonly を示す SIP 200 OK Response を介して、RTP ストリームを切断するよう電話機 A に指示します。電話機 B は、Unified CM からの SIP INVITE を介して RTP ストリームを切断するように指示されます。このときの SDP 接続情報は 0.0.0.0 を示し、メディア属性は inactive です。電話機 B から Unified CM に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されると、Unified CM は SIP INVITE を電話機 B に送信します。このときの SDP 接続情報は MoH マルチキャスト グループ アドレス（この場合は 239.23.1.1）を示し、メディア属性は sendonly です。

図 7-9　SIP マルチキャスト MoH コール フローの詳細



次に、図 7-9 の電話機 B は IGMP V2 の Membership Report メッセージを発行して、電話機 B がこのマルチキャスト グループに加わることを示します。さらに、電話機 B は、前の SIP INVITE に応答して、SDP メディア属性が sendonly を示す SIP 200 OK Response を Unified CM に返します。一方、MoH サーバがこの MoH マルチキャスト グループ アドレスに RTP オーディオを送信しているので、電話機 B はそのマルチキャスト グループに加わった後、一方向 MoH ストリームの受信を開始します。

電話機 A のユーザが Resume ソフトキーを押すと、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は電話機 A の受信 RTP ポートおよび sendrecv を示しています。Unified CM は、SDP 接続情報が 0.0.0.0、メディア属性が inactive を示す SIP INVITE を介して、電話機 B にマルチキャスト MoH ストリームから切断するように指示します。電話機 B から Unified CM に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されます。

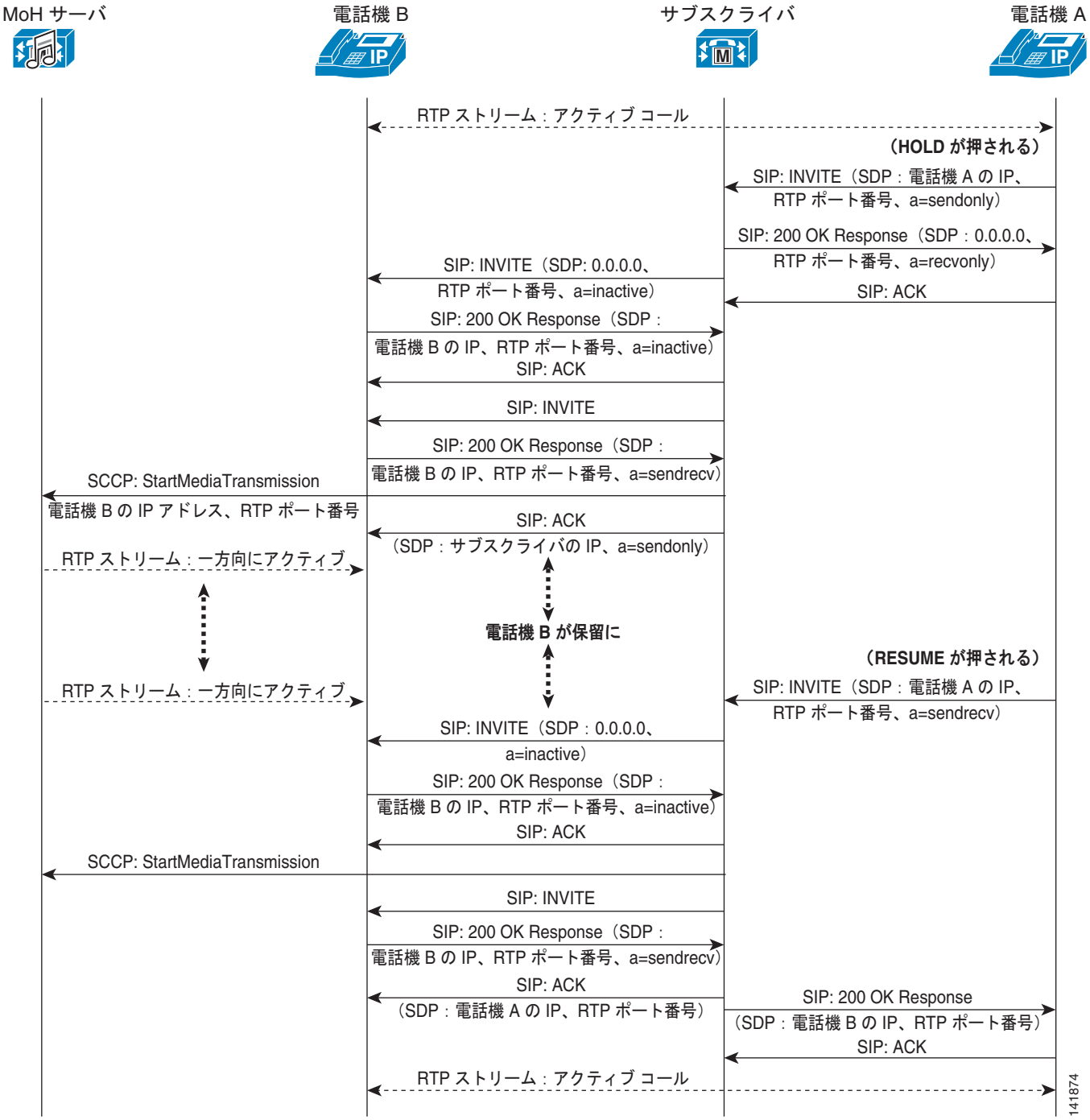
次に、Unified CM は電話機 B に SIP INVITE を送信し、電話機 B はそれに対して、SDP 接続情報が電話機 B の IP アドレスを示し、メディア属性が電話機 B の受信 RTP ポートおよび sendrecv を示す SIP 200 OK Response で応答します。Unified CM はそれに応答し、SDP 接続情報が電話機 A の IP アドレスを示し、メディア属性が電話機 A の受信 RTP ポート番号の SIP ACK を電話機 B に送信します。同様に、Unified CM は、SIP 200 OK Response を電話機 A の最初の保留解除 SIP INVITE に転送します。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポート番号です。電話機 B は、マルチキャスト ストリームが必要なくなったことを示すために、IGMP V2 の Leave Group メッセージを 224.0.0.2 に送信します。最後に、電話機 A と電話機 B の間に RTP 双方向オーディオ ストリームが再確立されます。

（注）　図 7-9、図 7-10、および図 7-11 のコール フロー図では、双方向 RTP オーディオ ストリームを使用して、初期化コールが電話機 A と電話機 B の間で行われることを前提としています。これらの図は、コール フローを示しているので、適切な MoH 動作に必要な関連トラフィックのみが記載されています。したがって、インタラクションがわかりやすいように、キープアライブ、一部の確認応答、進行状況表示、およびその他のトラフィックは省略されています。各図の初期化イベントは、電話機 A によって実行される Hold ソフトキー アクションです。

SIP ユニキャスト コール フロー

図 7-10 は、SIP ユニキャスト MoH コール フローを示しています。この図に示されているように、電話機 A で Hold ソフトキーが押されると、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は sendonly を示しています。Unified CM は、SDP 接続情報が 0.0.0.0、メディア属性が recvonly を示す SIP 200 OK Response を介して、RTP ストリームを切断するよう電話機 A に指示します。電話機 B は、Unified CM からの SIP INVITE を介して RTP ストリームを切断するように指示されます。このときの SDP 接続情報は 0.0.0.0 を示し、メディア属性は inactive です。次に、電話機 B から Unified CM に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されます。この時点まで、ユニキャストとマルチキャストの MoH コール フローはまったく同じです。

図 7-10　SIP ユニキャスト MoH コール フローの詳細



Unified CM は電話機 B に SIP INVITE を送信し、電話機 B は、それに対して、SDP 接続情報が電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポートおよび sendrecv を示す SIP 200 OK Response で応答します。Unified CM は、SCCP の StartMediaTransmission メッセージを MoH サーバに送信して、電話機 B のアドレスおよび受信 RTP ポート番号を伝えます。この後、Unified CM から電話機 B への SIP ACK が続き、このときの SDP 接続情報には Unified CM の IP アドレス、メディア属性には sendonly が示されます。一方、MoH サーバが RTP オーディオを送信しているので、電話機 B は一方向 MoH ストリームの受信を開始します。

電話機 A のユーザが Resume ソフトキーを押すと、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は電話機 A の受信 RTP ポートおよび sendrecv を示しています。Unified CM は、SDP 接続情報が 0.0.0.0、メディア属性が inactive を示す SIP INVITE を介して、電話機 B にマルチキャスト MoH ストリームから切断するように指示します。電話機 B から Unified CM に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されます。その後、Unified CM は、SCCP の StopMediaTransmission メッセージを MoH サーバに送信します。これによって、MoH サーバは電話機 B への MoH ストリームの転送を停止します。

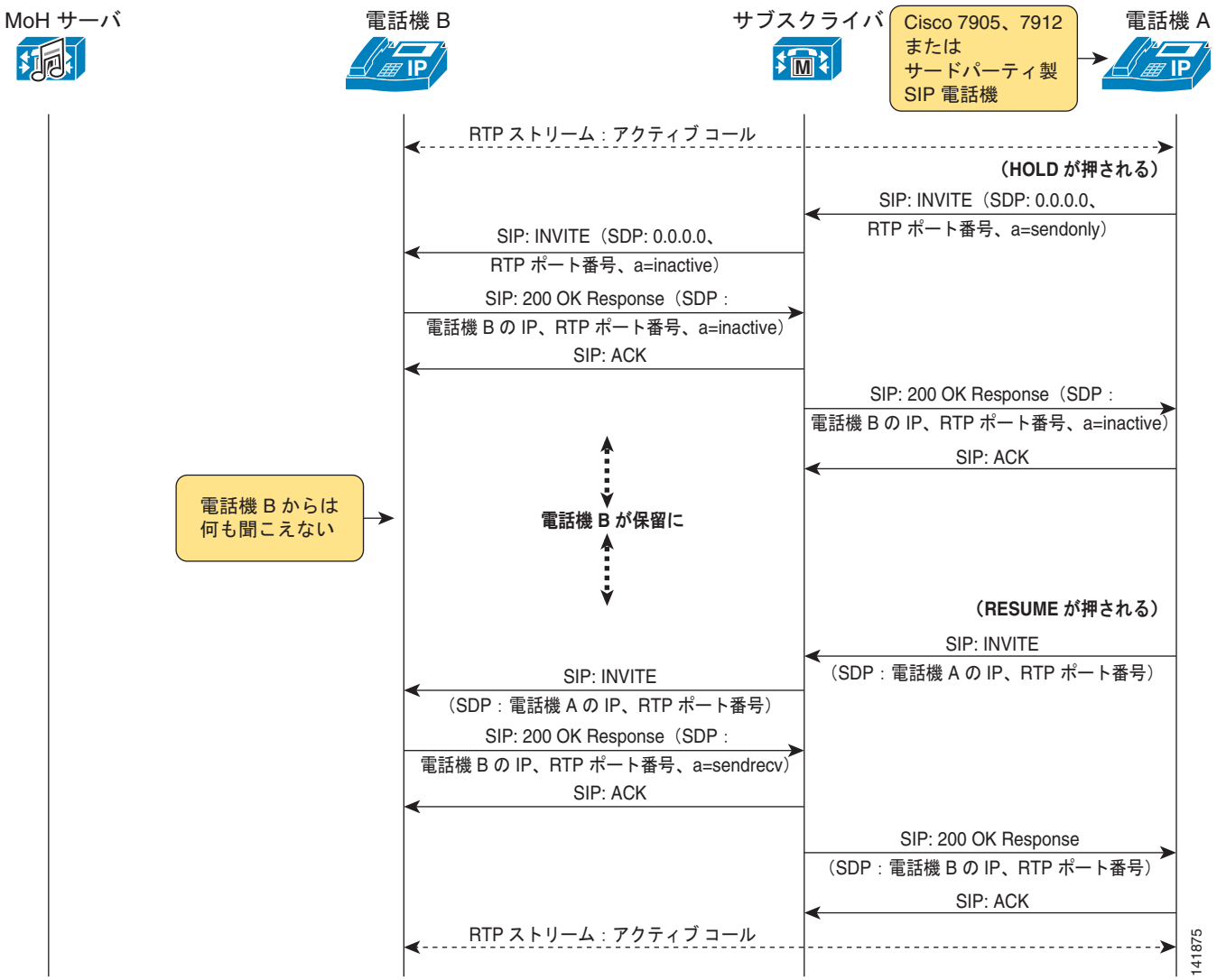
次に、Unified CM は電話機 B に SIP INVITE を送信し、電話機 B はそれに対して、SDP 接続情報が電話機 B の IP アドレスを示し、メディア属性が電話機 B の受信 RTP ポートおよび sendrecv を示す SIP 200 OK Response で応答します。Unified CM はそれに応答し、SDP 接続情報が電話機 A の IP アドレスを示し、メディア属性が電話機 A の受信 RTP ポート番号の SIP ACK を電話機 B に送信します。同様に、Unified CM は、SIP 200 OK Response を電話機 A の最初の保留解除 SIP INVITE に転送します。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポート番号です。最後に、電話機 A と電話機 B の間に RTP 双方向オーディオ ストリームが再確立されます。

SIP メディア保留コール フロー

図 7-11 は、RFC 2543 のメディア保留コール フローを示しています。このコール フローが発生するのは、コールを保留にする電話機（この場合は電話機 A）が Cisco Unified IP Phone 7905、7912、またはサードパーティ製の SIP 電話機の場合だけです。この図に示されているように、電話機 A で Hold ソフトキーが押されると、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は 0.0.0.0 を示し、メディア属性は sendonly を示しています。電話機 B は、Unified CM からの SIP INVITE を介して RTP ストリームを切断するように指示されます。このときの SDP 接続情報は 0.0.0.0 を示し、メディア属性は inactive です。次に、電話機 B から Unified CM に SIP 200 OK Response が返されます。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポート番号および inactive を示します。そして、Unified CM は、電話機 A の最初の保留 SIP INVITE に応答して、SIP 200 OK Response を電話機 A に返します。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポートおよび inactive を示します。

この時点で、電話機 B は保留状態ですが MoH を受信していないため、電話機 B のユーザには何も聞こえません。

図 7-11　SIP メディア保留コール フローの詳細



電話機 A のユーザが Resume ソフトキーを押すと、電話機 A は、SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は電話機 A の受信 RTP ポートを示しています。次に、Cisco Unified CM は、SDP 接続情報が電話機 A の IP アドレスを示し、メディア属性が電話機 A の受信 RTP ポートを示す SIP INVITE を電話機 B に送信します。それに対して、電話機 B が SIP 200 OK Response で応答します。このときの SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポートおよび sendrecv を示します。同様に、Unified CM は、SIP 200 OK Response を電話機 A の最初の保留解除 SIP INVITE に転送します。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポートを示します。最後に、電話機 A と電話機 B の間に RTP 双方向オーディオ ストリームが再確立されます。

（注）　メディア保留が以上のように発生するのは、Cisco Unified IP Phone 7905 または 7912 およびサードパーティ製の SIP 電話機がコールを保留にする場合だけです。また、これらの電話機は、他の Cisco Unified IP Phone モデルによって保留にされたときに MoH を受信し、そのシナリオのコール フローは、図 7-9 および図 7-10 に示したフローとほぼ同じようになります。

CHAPTER 8

コール処理

この章では、Cisco Unified Communications Manager（Unified CM）におけるスケーラブルで復元性のあるコール処理システムを設計するためのガイドラインを示します。ここでは、次に示す個々の要件に基づいて、Unified CM に適切なハードウェアおよび配置シナリオを選択する方法についても説明します。

- 規模：ユーザ、ロケーション、ゲートウェイ、アプリケーションなどの数
- パフォーマンス：コールのレート
- 復元性：冗長性の規模

この章では、次のトピックについて説明します。

- 「Unified CM クラスタのガイドライン」（P.8-2）

  ここでは、Unified CM の最小ハードウェア要件について説明します。また、Unified CM サーバで有効にすることができる各種の機能サービス、およびそれぞれの目的についても説明します。

- 「Unified CM プラットフォームのキャパシティ プランニング」（P.8-15）

  ここでは、Cisco Unified CM キャパシティ ツールの使用に関するガイドラインを示します。このツールは、IP テレフォニー配置のプランニング時に使用する必要があります。Cisco Unified CM キャパシティ ツールは、特定の配置要件に基づいて、Unified CM サーバ上で使用されるリソースについてのガイダンスを提供します。

- 「コンピュータ/テレフォニー インテグレーション（CTI）」（P.8-18）

  この項では、Cisco Computer Telephony Integration（CTI; コンピュータ/テレフォニー インテグレーション）アーキテクチャ、CTI のコンポーネントとインターフェイス、CTI の機能、および CTI のプロビジョニングとキャパシティ プランニングについて説明します。

- 「ゲートキーパーの設計上の考慮事項」（P.8-26）

  ここでは、Cisco Unified Communications の配置でゲートキーパーをどのように使用できるかについて説明します。シスコのゲートキーパーは、もう 1 台のスタンバイ ゲートキーパーとペアにすることも、クラスタ化してさらに高いパフォーマンスと復元性を実現することもできます。ゲートキーパーは、コール ルーティングとコール アドミッション制御に使用することもできます。

- 「Unified CM と Unified CM Express の相互運用性」（P.8-36）

  ここでは、分散型コール処理配置における Cisco Unified CM と Cisco Unified Communications Manager Express（Unified CME）間での H.323 と SIP での統合について説明します。

この章の新規情報

表 8-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 8-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
コンピュータ/テレフォニー インテグレーション（CTI）	「コンピュータ/テレフォニー インテグレーション（CTI）」（P.8-18）
WAN を介した CTI およびクラスタ化	「WAN を介した CTI アプリケーションおよびクラスタ化」（P.8-21）
CTI のキャパシティ制限	「Unified CM のキャパシティ プランニング」（P.8-22）
NIC チーミング	「ネットワークの耐障害性に対応する NIC チーミング」（P.8-4）
サーバのキャパシティ プランニング	「Unified CM プラットフォームのキャパシティ プランニング」（P.8-15）
標準サーバおよび高可用性サーバの定義の変更	表 8-2
トレース ファイルのキャパシティ	「Unified CM プラットフォームのキャパシティ プランニング」（P.8-15）
分散型コール処理環境における複数の Unified CME 間のビデオ コール	「SIP 経由での Unified CM と Unified CME の相互運用性に関する設計上の一般的な考慮事項」（P.8-40）

Unified CM クラスタのガイドライン

Unified CM アーキテクチャでは、複数の物理サーバを 1 つの IP PBX システムとして連携させることができます。このサーバ グループを*クラスタ*と呼びます。Unified CM サーバのクラスタは、設計上の制限事項を遵守している限り、IP ネットワークを介して分散していてもかまいません。クラスタを使用することで、空間的な冗長性、およびそれに伴う復元性を IP Communications システムの設計にもたらすことができます。

ここでは、Unified CM クラスタを形成しているサーバが実行する各種の機能について説明し、必要な規模、パフォーマンス、および復元性を達成するようにサーバを配置する方法について、ガイドラインを示します。

ハードウェア プラットフォーム

Unified CM クラスタでは、必要となる規模、パフォーマンス、および冗長性に応じて、さまざまなタイプのサーバを利用します。利用するサーバの範囲は、冗長性のないシングル プロセッサのサーバから、冗長性の高いマルチプロセッサ ユニットにまで及びます。

表 8-2 では、クラスタ内で使用できる一般的なサーバのタイプとその主な特性を一緒に示しています。

表 8-2　Cisco Unified CM サーバのタイプ

サーバ タイプ	Cisco サーバ モデル	特性
標準サーバ（高可用性でない）	MCS 7815、MCS 7816、または同等のサーバ	• 単一プロセッサ • 単一電源装置 • 非 RAID SATA ハードディスク
RAID 搭載の標準サーバ	MCS 7825 または同等のサーバ	• 単一プロセッサ • 単一電源装置 • RAID 0/1 搭載の SATA コントローラをサポート
RAID 搭載の標準サーバ（Cisco Unified Communications Manager Business Edition（Unified CMBE）用）	MCS 7828[1]	• 単一プロセッサ • 単一電源装置 • RAID 0/1 搭載の SATA コントローラをサポート
高可用性サーバ	MCS 7835、MCS 7845、または同等のサーバ	• 複数のプロセッサ • 複数の電源装置 • RAID 1 搭載の複数の Serial Attached SCSI（SAS）ドライブ

1. Cisco MCS 7828 は Unified CMBE のみをサポートします。

Cisco Unified CM は、特定の Cisco MCS 7815、7816、7825、7835、および 7845 の各サーバでサポートされます。あるいは、シスコですでに確認されている、次の最小要件を満たすサーバであれば、お客様が用意した HP サーバおよび IBM サーバでもサポートされます。

- プロセッサ速度：2.0 GHz 以上
- 物理メモリ サイズ：2 GB 以上
- 物理ハード ディスク サイズ：72 GB 以上

現在サポートされているハードウェア コンフィギュレーションの全リストについては、次の Web サイトにあるドキュメントを参照してください。

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

サーバは、IP ネットワークに加えて電源と冷却についても可用性の高い環境に配置する必要があります。建物の電力が必要な可用性を備えていない場合は、サーバの電力を無停電電源装置（UPS）から供給する必要があります。二重化電源を備えたサーバについても、それぞれの電源を 2 つの異なる電力源に接続しておくと、1 つの電源回路が故障しただけでサーバに障害が発生することを回避できます。

IP ネットワークへの接続性によっても、最大限のパフォーマンスと可用性が保証されます。Unified CM サーバは、イーサネットに 100 Mbps 全二重で接続する必要があります。小規模な配置で 100 Mbps が使用可能でない場合、10 Mbps 全二重を使用してください。多くのサーバはオプションとして、ギガビット イーサネットを使用する機能も備えています。サーバが全二重を使用してネットワークに接続していることを確認してください。全二重接続は、スイッチ ポートおよびサーバ NIC の設定で 10 Mbps と 100 Mbps が可能です。1000 Mbps の場合は、NIC およびスイッチ ポートの両方で速度とデュプレックス モードの設定に Auto/Auto を使用することをお勧めします。デフォルトは Auto/Auto であり、この設定は以前の Unified CM リリースからアップグレード後のデフォルトでもあります。

（注）　サーバ ポートまたはイーサネット スイッチ ポートのどちらか一方が Auto モードのままであり、もう一方のポートが手動で設定される場合、ミスマッチが生じます。ベスト プラクティスは、サーバ ポートとイーサネット スイッチ ポートの両方を手動で設定することです。ただし、ギガビット イーサネット ポートの場合は、Auto/Auto に設定する必要があります。

ネットワークの耐障害性に対応する NIC チーミング

NIC チーミング機能は、サーバを 2 枚の NIC、つまり 2 本のケーブルでイーサネットに接続できるようにするものです。NIC チーミングは、障害の発生したポートから正常なポートに作業負荷を転送することによって、ネットワークのダウンタイムを防止します。NIC チーミングは、ロード バランシングまたはインターフェイス速度向上用には使用できません。

2 枚のイーサネット ネットワーク インターフェイス カードを備えた Hewlett-Packard（HP）サーバ プラットフォームと IBM サーバ プラットフォームでは、ネットワークの耐障害性に対応する NIC チーミングをサポートできます。

（注）　Cisco MCS 7815 プラットフォーム（または HP や IBM と同等のプラットフォーム）には、ネットワーク インターフェイス ポートが 1 つしかないため、NIC チーミングは実行できません。

クラスタ化に関する一般的なガイドライン

すべての Unified CM クラスタに次のガイドラインが適用されます。

（注）　1 つのクラスタに複数のサーバ プラットフォームを組み合せることができますが、クラスタ内のすべてのサーバでは、同じ Unified CM ソフトウェア リリースを実行する必要があります。

- 通常の環境では、同一 LAN または MAN 内にクラスタのすべてのメンバーを入れます。クラスタのすべてのメンバーを同一の VLAN またはスイッチに配置することは、お勧めしません。
- 冗長性を持たせるには、クラスタのメンバーを次のように配置して、インフラストラクチャや建物で発生した障害によって受ける影響を最小限に抑える必要があります。
  - 同じディストリビューション スイッチまたはコア スイッチに、複数のアクセス スイッチが接続されている
  - 複数のディストリビューション スイッチまたはコア スイッチに、複数のアクセス スイッチが接続されている
  - 同じ LAN または MAN の中に複数の建物がある
- クラスタが IP WAN にわたって構築されている場合、「IP WAN を介したクラスタ化」（P.2-22）の項を参照して、IP WAN を介したクラスタ化のガイドラインに従ってください。

Unified CM クラスタのサービス

Unified CM クラスタの内部には、それぞれ固有のサービスを提供する複数のサーバが存在します。これらの各サービスは、同じ物理サーバ上で他のサービスと共存できます。たとえば、小規模なシステムでは、1 台のサーバがデータベース パブリッシャ、バックアップ サブスクライバ、Music On Hold（MoH）サーバ、TFTP サーバ、CTI Manager、およびカンファレンス ブリッジを兼ねることができます。クラスタの規模とパフォーマンスを強化する必要が高まった場合は、これらのサービスの多くを 1 台の専用物理サーバに移行する必要があります。

1 つのクラスタに、20 のサーバを組み込めるようになりました。20 のサーバのうち、最大 8 つのサーバが、コール処理を提供する Cisco CallManager サービスを実行できます。残りのサーバは、専用データベース パブリッシャ、トリビアル ファイル転送プロトコル（TFTP）専用サーバ、または Music On Hold（MoH）サーバとして設定できます。メディア ストリーミング アプリケーション（カンファレンス ブリッジやメディア ターミネーション ポイント）も、クラスタに登録される別個のサーバで有効にできます。

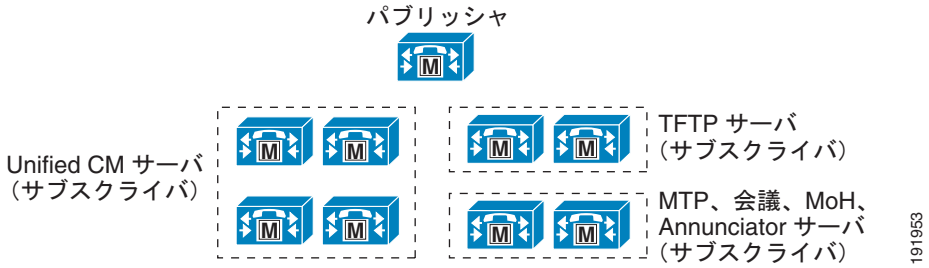
（注）　シスコは、クラスタ内のすべてのサーバに同じサーバ モデルを使用することをお勧めしますが、個々のハードウェア バージョンがすべてサポートされており、すべてのサーバが同じバージョンの Unified CM を実行している場合は、クラスタ内でサーバ モデルを混在させることができます。ただし、クラスタ内の異なるサーバ モデル間のキャパシティの相違を考慮する必要があります。これは、クラスタ全体のキャパシティが、クラスタ内の最小サーバのキャパシティによって最終的に決まる場合があるためです。クラスタ内のすべてのサーバが同じモデル タイプである場合は、異なるベンダー製のサーバをクラスタ内に混在させることもできます。この場合は、キャパシティへの悪影響はありません。コール処理機能については、「Unified CM プラットフォームのキャパシティ プランニング」（P.8-15）の項を参照してください。

Cisco MCS 7816 または同等のサーバを含んだクラスタを配置するときは、クラスタ内に最大 2 台のサーバが必要です。1 台をパブリッシャ、TFTP サーバ、バックアップ コール処理サーバにし、もう 1 台をプライマリ コール処理サーバにします。Cisco MCS 7816 または同等のサーバ上では、この構成で最大 500 台の電話機がサポートされます。これよりキャパシティの大きいサーバを使用して 2 サーバ クラスタを配置する場合も、クラスタ内のユーザ数が 1,250 を超えないようにすることをお勧めします。1,250 ユーザを超える場合は、専用パブリッシャと別個のサーバをプライマリおよびセカンダリのコール処理サービス用にお勧めします。そのため、クラスタ内のサーバ数が増えます。

MCS 7825 以上のサーバを備えたシングル サーバ クラスタを配置することもできます。MCS 7825 または同等のサーバでは、上限は 500 ユーザです。これより可用性の高いサーバを使用する場合も、シングル サーバ クラスタのユーザ数が 1,000 を超えないようにする必要があります。シングル サーバ構成では、Survivable Remote Site Telephony（SRST）も配置して、Unified CM が使用不可になっている間にサービスが提供されるようにしない限り、冗長性はありません。シスコでは、実稼動環境でシングル サーバ配置を採用することはお勧めしません。ロード バランシングは、パブリッシャがバックアップ コール処理サブスクライバである場合には実装できません。

図 8-1 では、一般的な Unified CM クラスタを示しています。

図 8-1　一般的な Unified CM クラスタ



クラスタ内通信

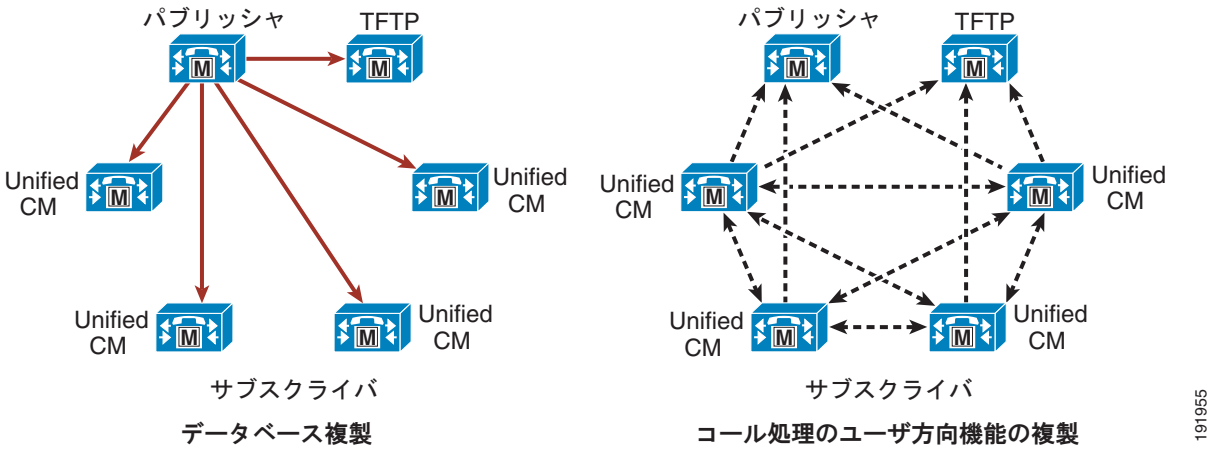
クラスタ内通信（Unified CM クラスタ内の通信）には、2 種類あります（図 8-2 および図 8-3 を参照）。1 つは、すべてのデバイス設定情報を含んでいるデータベースを配布するためのメカニズムです（図 8-2 の「データベース複製」を参照）。コンフィギュレーション データベースは、パブリッシャ サーバに保存され、読み取り専用のコピーがクラスタのサブスクライバ メンバーに複製されます。

データベースの変更のほとんどはパブリッシャで加えられ、サブスクライバ データベースに伝達されます。そのため、クラスタのメンバー全体で設定の一貫性が確保され、データベースの空間的な冗長性が容易になります。

ユーザ方向のコール処理機能に対するデータベースの変更は、IP Phone が登録されるサブスクライバ サーバで行われます。次にサブスクライバ サーバが、これらのデータベース変更をクラスタにある他のすべてのサーバに複製し、ユーザ方向機能に冗長性を提供します（図 8-2 の「コール処理のユーザ方向機能の複製」を参照）。これらの機能には、次のものがあります。

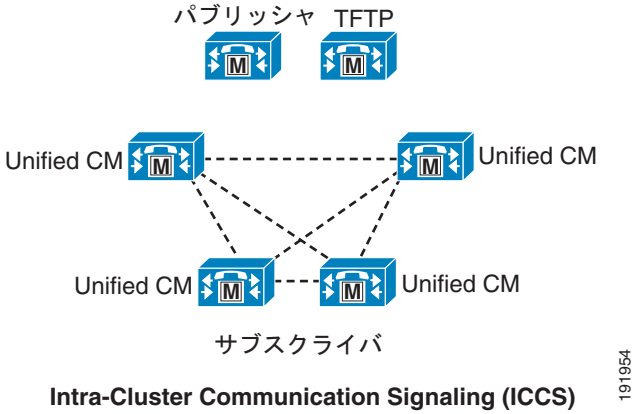
- Call Forward All（CFA）
- Message Waiting indicator（MWI; メッセージ待機インジケータ）
- プライバシーの有効 / 無効
- エクステンション モビリティのログイン / ログアウト
- ハント グループのログイン / ログアウト
- デバイス モビリティ
- エンド ユーザおよびアプリケーション ユーザの Certificate Authority Proxy Function（CAPF）ステータス
- クレデンシャルのハッキングと認証

図 8-2　データベースおよびユーザ方向機能の複製



Intra-Cluster Communication Signaling（ICCS）と呼ばれる、もう 1 つのクラスタ内通信は、デバイスの登録、ロケーションの帯域幅、共有メディア リソースなどのランタイム データの伝搬と複製です（図 8-3 を参照）。この情報は、Cisco CallManager サービスを実行している、クラスタのすべてのメンバー全体で共有されます。クラスタのメンバーと関連ゲートウェイとの間で、コールの最適なルーティングが確保されます。

図 8-3　Intra-Cluster Communication Signaling（ICCS）

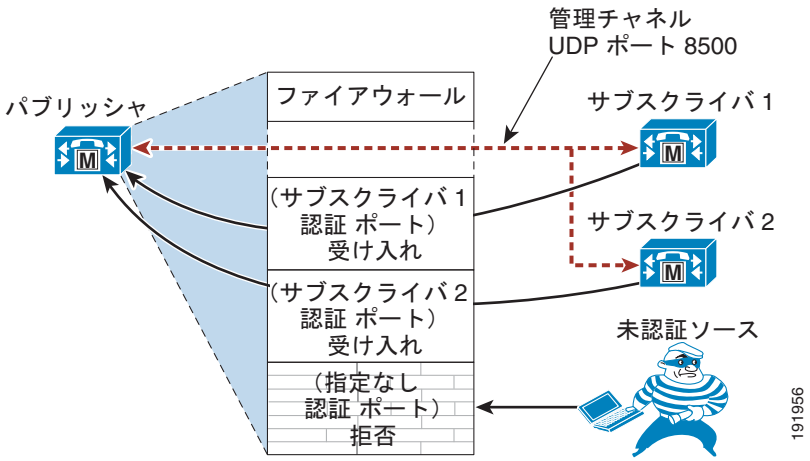


Intra-Cluster Communication Signaling (ICCS)

クラスタ内セキュリティ

Unified CM クラスタ内の各サーバが内部で動的ファイアウォールを実行します。Unified CM のアプリケーション ポートは、送信元 IP フィルタリングを使用して保護されます。動的ファイアウォールは、認証済みサーバまたは信頼できるサーバに対してだけ、これらのアプリケーション ポートを開きます（図 8-4 を参照）。

図 8-4　クラスタ内セキュリティ



このセキュリティ メカニズムは、単一の Unified CM クラスタ内のサーバ間にのみ適用できます。Unified CM のサブスクライバは、パブリッシャのデータベースにアクセスする前に、クラスタ内で認証されます。クラスタ内通信およびデータベース複製は、認証済みサーバ間でのみ発生します。インストール時にサブスクライバは、事前共有キー認証メカニズムでパブリッシャに対して認証されます。認証プロセスに必要な手順は次のとおりです。

1. セキュリティ パスワードを使用してパブリッシャ サーバをインストールします。
2. Unified CM Administration を使用することによって、パブリッシャ上にサブスクライバ サーバを設定します。
3. パブリッシャ サーバのインストール時に使用されたのと同じセキュリティ パスワードを使用して、サブスクライバ サーバをインストールします。

4. サブスクライバのインストール後、サーバは、UDP 8500 を使用する管理チャネル上でパブリッシャとの接続を確立しようとします。サブスクライバは、ホスト名、IP アドレスなどのすべてのクレデンシャルをパブリッシャに送信します。クレデンシャルは、インストール時に使用されたセキュリティ パスワードを使用して認証されます。
5. パブリッシャは、独自のセキュリティ パスワードを使用してサブスクライバのクレデンシャルを確認します。
6. その情報が有効な場合、パブリッシャは、自身の動的ファイアウォール テーブルに、信頼できる送信元としてサブスクライバを追加します。サブスクライバは、データベースへのアクセスを許可されます。
7. サブスクライバは、パブリッシャから他のサブスクライバ サーバのリストを取得します。すべてのサブスクライバが互いに管理チャネルを確立し、メッシュ トポロジが作成されます。

パブリッシャ

パブリッシャはすべてのクラスタに必要なサーバで、現在はクラスタごとに 1 つのみ配置できます。このサーバは、最初にインストールする必要があります。クラスタ内の他のすべてのメンバーに対して、データベース サービスを提供します。パブリッシャ サーバは、コンフィギュレーション データベースに完全な読み取りと書き込みのアクセスができる唯一のサーバです。1,250 ユーザを超える大規模なシステムの場合には、管理操作によるテレフォニー サービスへの影響を防止するために、専用パブリッシャをお勧めします。専用パブリッシャのサーバ上で、コール処理サービスまたは TFTP サービスが実行されることはありません。それ以外のサーバは、TFTP および Unified CM サービスを実行します。

クラスタ内のサブスクライバ サーバは、初期化時にローカル データベースを使用しようとします。これによって、Cisco CallManager サービスの初期化時間が短縮されます。Unified CM の以前のバージョンでは、クラスタ内のサーバは、初期化時にパブリッシャのデータベースを使用しようとしました。パブリッシャが使用不可になっている場合は、自身のハード ドライブにあるローカルの読み取り専用コピーを使用しました。

パブリッシャ用のハードウェア プラットフォームは、クラスタの規模とパフォーマンスを基準として選択します。パブリッシャは、コール処理サブスクライバと同等のパフォーマンスを持つものにすることをお勧めします。可能な場合には、パブリッシャを高可用性サーバにして、ハードウェアの障害による影響を最小限に抑えるようにします。

コール処理サブスクライバ

Unified CM ソフトウェアをインストールするときに、パブリッシャとサブスクライバという 2 タイプのサーバを定義できます。これらの用語は、データベース間の関係をインストール時に定義するために使用されています。ソフトウェアをインストールしたときに使用可能になるのは、データベース サービスとネットワーク サービスだけです。すべてのサブスクライバは、パブリッシャにサブスクライブして、データベース情報のコピーを取得します。

コール処理サブスクライバは、Cisco CallManager サービスが使用可能になっているサーバです。このサービスをサブスクライバ上で使用可能にするには、シングル サーバ ライセンスが必要です。パブリッシャが使用不可になっていると、サーバ上で Cisco CallManager サービスを使用可能にできません。パブリッシャはライセンス サーバとして機能し、Cisco CallManager サービスをアクティブにするために必要なライセンスを配布するからです。このサービスが使用可能になった時点で、このサーバはコール処理機能を実行できるようになります。電話、ゲートウェイ、メディア リソースなどのデバイスが登録やコール発信を実行できるのは、このサービスが使用可能になっているサーバに対してのみです。Unified CM では、クラスタ内の 8 つまでのサーバで Cisco CallManager サービスを使用可能にできます。

選択した冗長性方式に応じて（「コール処理の冗長性」（P.8-9）を参照）、コール処理サブスクライバは、プライマリ（アクティブ）サブスクライバまたはバックアップ（スタンバイ）サブスクライバのどちらかになります。ロード バランシングを実装する場合は、サブスクライバがプライマリ サブスクライバとバックアップ サブスクライバの両方を兼ねることもあります。クラスタの設計を計画するときは、通常はコール処理サブスクライバにこの機能を割り当てます。大規模なクラスタや高性能クラスタでは、コール処理サービスをパブリッシャおよび TFTP サーバ上で使用可能にしないでください。コール処理サブスクライバは、採用する冗長性方式に応じて、通常は専用ペアまたは共有ペアのどちらかで運用します。1：1 冗長性では、専用ペアを使用します。2：1 冗長性では、各ペアに含まれるサーバ 1 台（バックアップ サーバ）を共有する、2 組のサーバを使用します。

ハードウェア プラットフォームは、サーバの規模、パフォーマンス、冗長性、およびコストに応じて選択します。規模とパフォーマンスについては、「Unified CM プラットフォームのキャパシティ プランニング」（P.8-15）の項で説明しています。冗長性については、「コール処理の冗長性」（P.8-9）の項で説明しています。

コール処理の冗長性

Unified CM では、次の冗長性設定の中から選択できます。

- 2:1 冗長性方式：プライマリ サブスクライバ 2 台ごとに、1 つの共用セカンダリまたはバックアップ サブスクライバを設置します。
- 1:1 冗長性方式：プライマリ サブスクライバごとに、1 つのセカンダリまたはバックアップ サブスクライバを設置します。

1:1 冗長性方式では、フェールオーバー期間だけがクラスタに影響を与えるアップグレードが可能です。このフェールオーバー メカニズムは、Skinny Client Control Protocol（SCCP）IP Phone のフェールオーバー レート、毎秒約 125 台の登録を実現できるように拡張されました。Session Initiation Protocol（SIP）電話機のフェールオーバー メカニズムでは、毎秒約 40 台の登録です。

クラスタは、サービスへの影響なしにアップグレードできます。2 つのバージョン（リリース）の Unified CM を同じサーバ上に置いて、一方をアクティブ パーティションに、もう一方を非アクティブ パーティションに入れることができます。すべてのサービスとデバイスで、すべての Unified CM 機能に対して、アクティブ パーティションの Unified CM バージョンが使用されます。アップグレード時に、クラスタ操作はアクティブ パーティションにある現在のリリースの Unified CM を使用して続行されながら、アップグレード バージョンが非アクティブ パーティションにインストールされます。アップグレード プロセスの完了後は、サーバをリブートし非アクティブ パーティションをアクティブ パーティションに切り替えて、新しいバージョンの Unified CM を実行できます。

Unified CM のアップグレード

1:1 冗長性方式で、クラスタをアップグレードする手順は、次のとおりです。

ステップ 1　新しいバージョンの Unified CM をパブリッシャにインストールします。リブートはしないでください。

ステップ 2　新しいバージョンの Unified CM をすべてのサブスクライバに同時にインストールします。リブートはしないでください。

ステップ 3　パブリッシャのみをリブートします。新しいバージョンの Unified CM に切り替え、データベースが初期化されるまでしばらく待ちます。

ステップ 4　TFTP サーバを 1 台ずつリブートします。新しいバージョンの Unified CM に切り替え、コンフィギュレーション ファイルが再作成されるまで待ってから、クラスタ内の他のサーバをアップグレードします。

ステップ 5　Music On Hold（MoH）専用サーバを 1 台ずつリブートします。新しいバージョンの Unified CM に切り替えます。

ステップ 6　バックアップ サブスクライバを 1 台ずつリブートします。新しいバージョンの Unified CM に切り替えます。50/50 ロード バランシングが設定されている場合、このステップは一部のユーザに影響を与えることがあります。

ステップ 7　プライマリ サブスクライバからバックアップ サブスクライバに、デバイスをフェールオーバーします。

ステップ 8　プライマリ サブスクライバを 1 台ずつリブートします。新しいバージョンの Unified CM に切り替えます。

このアップグレード方法では、異なるバージョンの Unified CM ソフトウェアを実行しているサブスクライバ サーバにデバイスが登録される期間（フェールオーバー期間を除く）がありません。

2:1 冗長性方式では、クラスタ内のサーバ数を減らすことができますが、その結果、アップグレード時に障害が発生する可能性があります。

（注）　7,500 台以上の IP Phone が 2 つのプライマリ サブスクライバに登録される場合は、1:1 冗長性を使用する必要があります。これは、1 つのバックアップ サブスクライバで 7,500 台以上のバックアップ登録はできないからです。

（注）　アップグレードを行う前に、障害回復フレームワークを使用して、Unified CM および Call Detail Record（CDR; コール詳細レコード）データベースを外部ネットワーク ディレクトリにバックアップすることをお勧めします。このようにしておくと、アップグレードが失敗した場合のデータ損失を防止できます。

コール処理サブスクライバの冗長性

次の図では、Unified CM でコール処理の冗長性を実現するための一般的なクラスタ構成を示しています。

図 8-5　基本的な冗長性方式

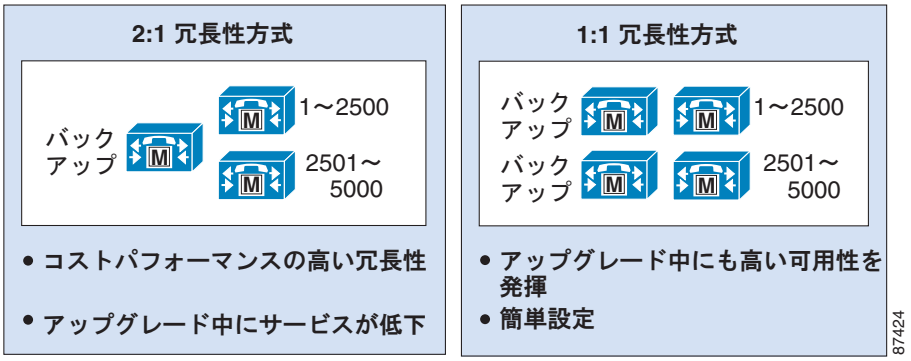


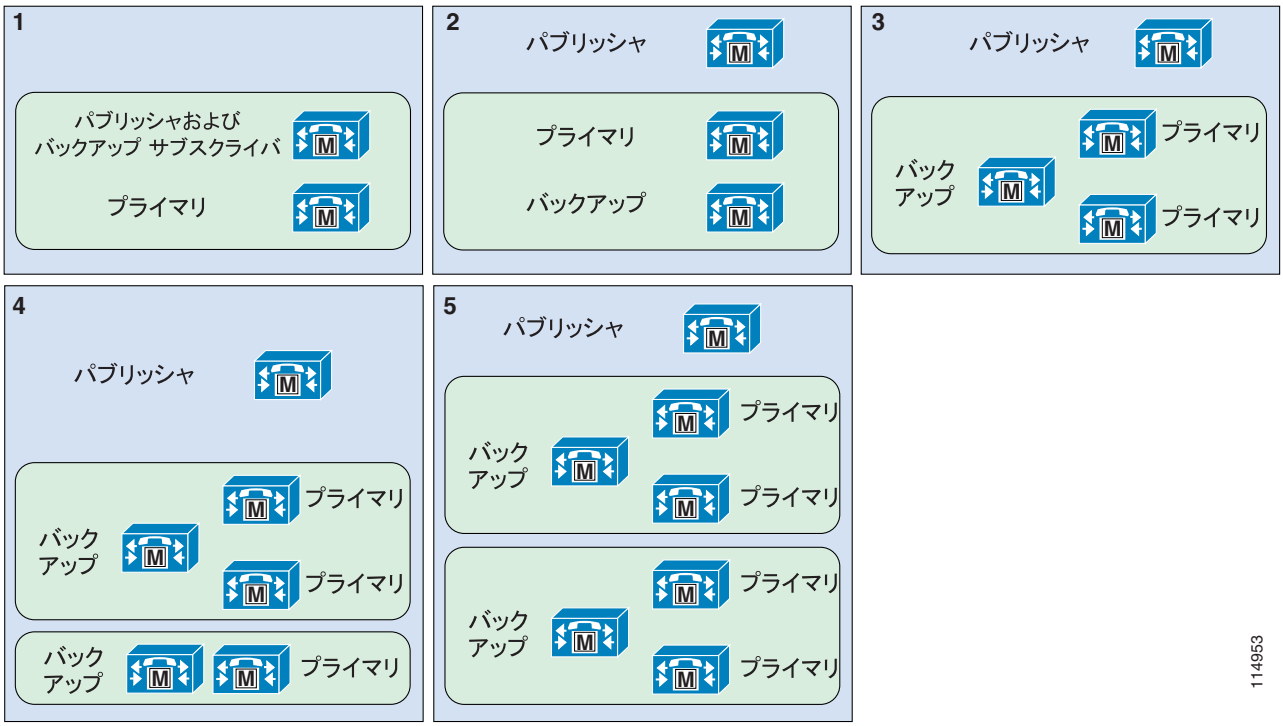
図 8-5 では、利用できる 2 つの基本的な冗長性方式を示しています。どちらの場合でも、バックアップ サーバは、障害の発生するプライマリ コール処理サーバ 1 台分以上の処理能力を備えている必要があります。2：1 冗長性方式の場合、バックアップ サーバは、個々の配置の要件に応じて、障害の発生するコール処理サーバ 1 台分、または両方のプライマリ コール処理サーバに相当する処理能力を備えている必要があります。サーバのキャパシティの選定およびハードウェア プラットフォームの選択については、「Unified CM プラットフォームのキャパシティ プランニング」（P.8-15）の項で説明しています。

図 8-6　　1：1 冗長構成のオプション

図 8-6 に示した 5 つは、すべて 1：1 冗長性のオプションを示しています。オプション 1 は、1,250 人未満のユーザをサポートするクラスタに使用します。オプション 2 ～ 5 は、クラスタを徐々に拡張した様子を示しています。正確な規模は、選択したハードウェア プラットフォームや必要なハードウェア プラットフォームによって異なります。

この図では、パブリッシャとコール処理サブスクライバのみ示していることに注意してください。

図 8-7　　2：1 冗長構成のオプション



（注）　Unified CM グループあたり最大 3 つのコール処理サブスクライバを定義できます。追加のバックアップ用に 3 次サブスクライバを追加すると、上記の冗長性方式を 2:1:1 または 1:1:1 冗長性に拡張できます。ただし、WAN を介したクラスタ化による配置で 3 次サブスクライバ サーバを使用する場合（「リモート フェールオーバー配置モデル」（P.2-32）を参照）を除き、リモート サイトに配置されたエンドポイント デバイスに 3 次サブスクライバによる拡張性を使用することはお勧めしません。これは、エンドポイントで 3 次サブスクライバへの接続を確認する必要がある場合、SRST へのフェールオーバーがさらに遅延するためです。

ロード バランシング

通常、プライマリが使用可能な場合、バックアップ サーバに登録されたデバイスはありません。このモデルには、次のような特長があります。

- トラブルシューティングが容易：すべてのコール処理がプライマリ サーバで行われるため、トレースおよび警告通知の取得が簡単になります。
- 設定が少ない：すべてのデバイスがプライマリ サーバに登録されるため、追加で Unified CM の冗長性グループまたはデバイス プールを各種のデバイス用に定義する必要性を 50% 減らすことができます。

1:1 冗長性方式を使用すると、プライマリ サーバとバックアップ サーバのペア上でデバイスを分散することができます。ロード バランシングを使用すると、Unified CM の冗長性グループとデバイス プールの設定値を使用して、デバイスにかかる負荷の半分までをプライマリ サブスクライバからセカンダリ サブスクライバに移すことができます。このモデルには、次のような特長があります。

- ロード シェアリング：コール処理の負荷が複数のサーバ上に分散され、応答時間をより速くすることができます。

- フェールオーバーとフェールバックが高速：すべてのデバイス（たとえば、IP Phone、CTI ポート、ゲートウェイ、トランク、ボイスメール ポートなど）がすべてのアクティブ サブスクライバにわたって分散されるため、プライマリ サブスクライバに障害が発生した場合に、セカンダリ サブスクライバにフェールオーバーするデバイスは一部のみです。この方法で、サーバが使用不能になる影響を 50% 減らすことができます。

50/50 ロード バランシングを計画するには、ロード バランシングを使用しない場合のクラスタのキャパシティを計算し、次に、デバイスおよびコールの量に基づいて、負荷をプライマリ サブスクライバとバックアップ サブスクライバに分散します。プライマリ サーバやバックアップ サーバの障害に対処できるようにするには、プライマリとバックアップのサブスクライバの合計負荷が、サブスクライバ サーバ 1 台分の負荷を超えないようにします。

TFTP サーバ

TFTP サーバ プラットフォームには、主に次の 2 つの機能があります。

- MoH などのサービスのためのファイル、電話やゲートウェイなどのデバイスのコンフィギュレーション ファイル、電話および一部のゲートウェイのアップグレード用バイナリ ファイル、およびさまざまなセキュリティ ファイルの提供。
- コンフィギュレーション ファイルおよびセキュリティ ファイルの生成。シスコの TFTP サービスが生成するファイルのほとんどは、署名済みであり、ダウンロード用として提供する前に暗号化されることもあります。

TFTP サービスは、クラスタ内の任意のサーバで使用可能にすることができます。ただし、何らかの設定を変更すると、TFTP サービスがコンフィギュレーション ファイルを再生成するため、1,250 ユーザを超えるクラスタでは、他のサービスが影響を受ける場合があります。このため、1,250 ユーザを超えるクラスタ、エクステンション モビリティを使用するクラスタ、または設定の変更を伴うその他の機能を備えたクラスタでは、特定のサーバを TFTP サービス専用にすることをお勧めします。

TFTP サーバは、設定情報を取得するために電話および MGCP ゲートウェイが使用します。TFTP サービスを使用可能にできるサーバの数に制限はありませんが、より大規模なクラスタのために TFTP サーバを 2 台配置して、TFTP サービスのための冗長性を確保しておくことをお勧めします。クラスタ内に 3 台以上の TFTP サーバを配置できますが、そのような構成ではすべての TFTP サーバ上ですべての TFTP ファイルを再構築するために時間がかかります。DHCP を使用して TFTP オプションを設定する場合、または静的に TFTP オプションを設定する場合は、TFTP サーバの IP アドレス アレイ（複数の IP アドレス）を定義します。このように定義すると、半数のデバイスでは TFTP サーバ A をプライマリとして使用し、TFTP サーバ B をバックアップとして使用するように割り当てて、他の半数のデバイスでは、TFTP サーバ B をプライマリとして使用し、TFTP サーバ A をバックアップとして使用するように割り当てることができます。TFTP 専用サーバのパフォーマンスを向上させるには、サービス パラメータを設定して、サーバ上で許容する同時 TFTP セッションの数を増やします。

Unified CM クラスタをアップグレードするときは、パブリッシャの後に TFTP サーバをアップグレードし、次にその他のサーバをアップグレードすることを強くお勧めします。また、TFTP サーバをアップグレードした後は、すべてのコンフィギュレーション ファイルが再作成されるように十分な間隔を空けます。一般的な Cisco TFTP の BuildDuration 時間を使用するか、リアルタイム モニタリング ツールを使用して Cisco TFTP の DeviceBuildCount を監視して、これらの増加が止まるまで監視します。このアップグレード順序に従うと、新しいバイナリと設定変更が、クラスタ内の他のサービスをアップグレードする前に有効になります。電話やゲートウェイの個々のバイナリまたはファームウェア ロードを手動で追加する場合は、ファイルを必ずクラスタ内の各 TFTP サーバにコピーしてください。

TFTP サーバのハードウェア プラットフォームには、コール処理サブスクライバと同じものを使用することをお勧めします。

CTI Manager

CTI Manager は、クラスタ内で TAPI または JTAPI コンピュータ/テレフォニー インテグレーション（CTI）を使用するアプリケーションに必要となるものです。CTI Manager は、CTI アプリケーションと Cisco CallManager サービスの仲介者として機能します。アプリケーションの認証機能を提供し、許可済みのデバイスを制御および監視できるようにします。CTI アプリケーションはプライマリ CTI Manager と通信し、障害発生時にはバックアップ CTI Manager に切り替えます。CTI Manager は、コール処理サブスクライバ上でのみ使用可能にする必要があります。したがって、クラスタ内では最大で 8 つの CTI Manager を使用できます。復元性、パフォーマンス、および冗長性を最大限まで高めるには、CTI アプリケーションの負荷をクラスタ内の複数の CTI Manager に分散することをお勧めします。

一般に、アプリケーションによって制御または監視されるデバイスは、CTI Manager に使用するものと同じサーバ ペアに関連付けることをお勧めします。たとえば、IVR（interactive voice response; 音声自動応答装置）アプリケーションでは 4 つの CTI ポートが必要になります。1：1 冗長性と 50/50 ロード バランシングを使用する場合は、これらを次のように設定します。

- 2 つの CTI ポートは、サーバ A をプライマリ、サーバ B をバックアップ（セカンダリ）とする Unified CM 冗長性グループを持つようにします。残りの 2 つの CTI ポートは、サーバ B をプライマリ、サーバ A をバックアップとする Unified CM 冗長性グループを持つようにします。
- IVR アプリケーションは、サーバ A 上の CTI Manager をプライマリ、サーバ B をバックアップとして使用するように設定します。

上の例は、サーバ A 上の CTI Manager で障害が発生した場合の冗長性を備えており、IVR コールの負荷を 2 つのサーバに分散することもできています。この方法では、Unified CM サーバの障害による影響も最小限に抑えることができます。

CTI Manager の詳細については、「コンピュータ/テレフォニー インテグレーション（CTI）」（P.8-18）を参照してください。

IP Voice Media Streaming Application

会議や Music On Hold などのメディア リソースは、Cisco CallManager サービスと同じ物理サーバ上で動作している IP Voice Media Streaming Application サービスによって提供されます。

メディア リソースには、次のものがあります。

- Music On Hold（MoH）：保留状態になっているデバイス、会議に転送または追加されるデバイスに対して、マルチキャストまたはユニキャストの保留音を提供できます（「Music on Hold」（P.7-1）を参照）。
- Annunciator サービス：電話番号を間違えていることや、コール ルーティングが使用不可になっていることを伝える場合に、トーンの代わりに音声アナウンスを流します（「Annunciator」（P.6-27）を参照）。
- カンファレンス ブリッジ：Ad Hoc 会議と Meet-Me 会議のための、ソフトウェア ベースの会議を提供します（「オーディオ会議」（P.6-10）を参照）。
- Media Termination Point（MTP; メディア ターミネーション ポイント）サービス：H.323 クライアント、H.323 トランク、および Session Initiation Protocol（SIP）トランク用の機能を提供します（「メディア ターミネーション ポイント（MTP）」（P.6-19）を参照）。

クラスタ内でメディア リソースを実行する場合は、メディアの処理とネットワークに関する要件が追加される場合に備えて、すべてのガイドラインに準拠することが重要です。一般に、マルチキャスト MoH および Annunciator には専用サーバを使用せず、ユニキャスト MoH およびソフトウェア ベースの大規模な会議と MTP には図 8-1 で示している専用のメディア リソース サブスクライバを使用することをお勧めします（これらのサービスが、「メディア リソース」（P.6-1）および「Music on Hold」（P.7-1）の章で説明している設計ガイドラインの範囲内にない場合は除きます）。

音声アクティビティ検出

クラスタ内で音声アクティビティ検出（VAD）も使用不可にしておくことをお勧めします。デフォルトでは、Unified CM サービス パラメータで VAD は使用不可になっています。H.323 および SIP ダイヤルピア上で使用不可にするには、**no vad** コマンドを使用してください。

Unified CM のアプリケーション

Unified CM 上では、Cisco Unified CM Assistant、エクステンション モビリティ、WebDialer などのさまざまなタイプのアプリケーションを使用可能にすることができます。これらのアプリケーションに関する設計ガイドラインの詳細については、「Cisco Unified CM アプリケーション」（P.24-1）の章を参照してください。

Unified CM プラットフォームのキャパシティ プランニング

Unified CM には、タイプの異なるデバイスを登録できます。たとえば、IP Phone、ボイスメール ポート、CTI（TAPI または JTAPI）デバイス、ゲートウェイ、および DSP リソース（トランスコーディングや会議）などです。これらの各デバイスは、登録先となるサーバ プラットフォームのリソースを必要とします。必要なリソースには、メモリ、プロセッサ使用、およびディスク I/O が含まれます。各デバイスは、トランザクション（通常、コールの形式）中に、追加のサーバ リソースを消費します。たとえば、1 時間あたり 6 回のコールだけを行うデバイスが消費するリソースは、1 時間あたり 12 回のコールを行うデバイスより少なくなります。

この項で示す推奨事項は、Unified CM キャパシティ ツールを、デフォルトのトレース レベルと CDR を有効にして使用し、その結果として得た計算に基づいています。コール処理に直接関係しない他の機能を使用不可にしたり、縮小したり、再設定したりすると、より高いレベルのパフォーマンスが得られます。こうした機能の一部を増やすと、システムのコール処理機能に影響を与える可能性があります。これらの機能には、トレース、コール詳細レコード、複雑なダイヤル プラン、およびサーバ上に共存するその他のサービスが含まれます。複雑なダイヤル プランには、複数のライン アピアランス、多くのパーティション、コーリング サーチ スペース、ルート パターン、変換、ルート グループ、ハント グループ、ピックアップ グループ、ルート リスト、自動転送の拡張使用、共存サービス、およびその他の共存アプリケーションが含まれています。こうした機能はすべて、Unified CM サーバ内の追加リソースを消費します。

システム パフォーマンスを向上させるために、次のテクニックを活用すると便利なオプションが提供されます。

- 特定プラットフォーム用にサポートされている最大量まで、サーバに追加の保証メモリを取り付ける。MCS 7825 および MCS 7835、または同等のサーバ クラスの大規模構成では、これらのサーバの RAM を倍に増やすことをお勧めします。このメモリ アップグレードが必要かどうかは、Cisco Real Time Monitoring Tool（RTMT; リアルタイム監視ツール）を使用して検証することで判別できます。サーバが物理メモリを最大量近くまで使用すると、オペレーティング システムは、ディスクへのスワップを開始します。このスワッピングが発生した場合は、追加の物理メモリを取り付ける必要があることを示しています。
- 多数のゲートウェイ、ルート パターン、トランスレーション パターン、およびパーティションを含む非常に大きなダイヤル プランを持つ Unified CM クラスタでは、Cisco CallManager サービスの初回始動時に、初期化に長い時間がかかる場合があります。デフォルトの時間内にシステムが初期化されない場合、システム初期化タイマー（Unified CM サービス パラメータ）を変更して、設定の初期化時間を延長してください。システム初期化時間の詳細については、Unified CM Administration のサービス パラメータに関するオンライン ヘルプを参照してください。

Cisco Unified CM には、次のガイドラインが適用されます。

- クラスタ内では、Cisco CallManager サービスを使用して最大 8 台のサーバを使用可能にすることができます。それ以外のサーバは、TFTP、パブリッシャ、Music on Hold などの専用機能に使用できます。
- 各クラスタは、最大 30,000 台のセキュアでない SCCP または SIP 電話機をサポートできます。
- 各クラスタは、最大 27,000 台のセキュアな SCCP または SIP 電話機をサポートできます。
- MCS 7825 または MCS 7835 サーバで構成されている Unified CM クラスタには、最大 500 のロケーションを構成できます。
- MCS 7825 または MCS 7835 サーバで構成されているクラスタは、最大 600 台の H.323 デバイス（ゲートウェイ、トランク、クライアント）、デジタル MGCP デバイス、および SIP トランクをサポートできます。
- MCS 7845 サーバで構成されている Unified CM クラスタには、最大 2,000 のロケーションを構成できます（「Unified CM によるロケーションおよびリージョンのサポート」（P.8-17）を参照）。
- MCS 7845 サーバで構成されているクラスタは、最大 2100 台の H.323 デバイス（ゲートウェイ、トランク、クライアント）、デジタル MGCP デバイス、および SIP トランクをサポートできます（「Unified CM によるゲートウェイおよびトランクのサポート」（P.8-18）を参照）。
- Unified CM の推奨される最大トレース設定は、System Diagnostic Interface（SDI）および Signaling Description Layer（SDL）の両方のトレースに対して 2 MB のファイルを 2,000 本、合計でファイル 4,000 本です。プロセスごとにファイルの最大数が設定され、各プロセスに許容されるファイル数は SDL に対して 2,000 本、SDI に対して 2,000 本となります。その他すべてのコンポーネントのトレース設定は、126 MB の限度内（たとえば、それぞれ 2 MB のファイルが 63 本）で設定する必要があります。これらの値が上限として推奨されます。コール レートの高い環境での特定のトラブルシューティングでファイルの最大数を増やす必要がある場合を除き、ほとんどの環境ではデフォルト設定で十分なトレースを収集できます。

Unified CM がサポートできるユーザの最大数は、サーバ プラットフォームによって異なります（表 8-3 を参照）。

表 8-3　サーバ プラットフォームごとの最大デバイス数

サーバ プラットフォームの特性	サーバ 1 台あたりの最大ユーザ数[1]	高可用性サーバ[2]	高性能サーバ
Cisco MCS 7845（すべてのサポート モデル）	7500	あり	あり
Cisco MCS 7835（すべてのサポート モデル）	2500	あり	なし
Cisco MCS 7825（すべてのサポート モデル）	1000	なし	なし
Cisco MCS 7815 または MCS 7816（すべてのサポート モデル）[3]	500[4]	なし	なし

1. 高可用性サーバでないプラットフォームは、非冗長インストレーションで最大 500 の IP Phone をサポートできます。
2. 高可用性サーバは、電源装置とハードディスクの両方の冗長性をサポートします。
3. MCS 7815 サーバおよび MCS 7816 サーバは、1+1 冗長性（最大 2 サーバ）のみをサポートし、他のサーバを含むクラスタのメンバーになることはできません。
4. MCS 7815 サーバは最大 300 のユーザをサポートします。

サポートされるプラットフォーム、サードパーティ プラットフォーム、個々のハードウェア設定の最新情報については、次の Web サイトにあるオンライン資料を参照してください。

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

Unified CM によるロケーションおよびリージョンのサポート

Cisco Unified Communications Manager 7.1(2) 以降のリリースでは、Cisco MCS-7845 サーバを使用した場合で 2000 のロケーションと 2000 のリージョンがサポートされます。最大 2000 のロケーションおよびリージョンを展開するには、[Clusterwide Parameters] > [System] > [Location and Region] および [Clusterwide Parameters] > [System] > [RSVP] の設定メニューで次のサービス パラメータを設定する必要があります。

- [Intraregion Audio Codec Default]
- [Interregion Audio Codec Default]
- [Intraregion Video Call Bandwidth Default]
- [Interregion Video Call Bandwidth Default]
- [Default inter-location RSVP Policy]

リージョンを追加する際は、[Audio Codec] および [Video Call Bandwidth] の値に [Use System Default] を設定します。RSVP コール アドミッション制御を使用している場合は、[RSVP Setting] パラメータにも [Use System Default] を選択します。

個々のリージョンおよびロケーションについてこれらの値をデフォルトから変更すると、サーバの初期化とパブリッシャのアップグレードにかかる時間に影響します。合計 2000 のリージョンと 2000 のロケーションを使用する場合、そのうち最大 200 のリージョンおよびロケーションでデフォルト以外の値を使用するように変更できます。合計 1000 以下のリージョンおよびロケーションを使用する場合、そのうち最大 500 のリージョンおよびロケーションでデフォルト以外の値を使用するように変更できます。表 8-4 は、これらの制限を要約したものです。

表 8-4　デフォルト以外の値を使用できるリージョンおよびロケーションの数

デフォルト以外の値を使用するリージョンおよびロケーションの数	リージョンの最大数	ロケーションの最大数
0 ～ 200	2000	2000
200 ～ 500	1000	1000

（注） 音声コーデック値は、音声コールと FAX コールの両方に使用されます。リージョン間コーデック値として G.729 を使用する場合、FAX コールには T.38 FAX リレーを使用してください。WAN で FAX パススルーを使用する場合は、[Interregion Audio Codec] をデフォルト値から G.711 に変更するか、デフォルト以外のコーデック値 G.711 を使用する各ロケーションに FAX マシンのリージョンを追加します（表 8-4 内の制限に従います）。

（注） 使用している MCS モデルに関係なく、多数のリモート サイトを包含する設計には、Unified CM クラスタのスケーラビリティ（リージョン、ロケーション、ゲートウェイ、メディア リソースなど）に影響する可能性ある相互依存変数が多数存在するため、シスコ代理店またはシスコのシステム エンジニ

アが常に Cisco Unified Communications Sizing Tool（http://tools.cisco.com/cucst）を使用して、それらの設計をすべて検証する必要があります。Sizing Tool を使用して、設計基準を満たすために必要なサーバまたはクラスタの正確な台数を決定します。

Unified CM によるゲートウェイおよびトランクのサポート

Cisco Unified Communications Manager 7.1(2) 以降のリリースでは、Cisco MCS-7845 サーバを使用する場合で 2100 台のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）がサポートされます。

クラスタ内のアクティブなゲートウェイ、トランク、およびメディア リソースの数を増やす場合は、すべてのコール処理サーバに対してこれらのデバイスの登録を均等に分散させて、クラスタ内の 1 台または複数台のサーバの CPU に対する過負荷を回避することが重要です。

（注）　使用している MCS モデルに関係なく、多数のゲートウェイおよびトランクを包含する設計については、Unified CM クラスタのスケーラビリティ（リージョン、ロケーション、ゲートウェイ、メディア リソースなど）に影響する可能性ある相互依存変数が多く存在するため、シスコ代理店またはシスコのシステム エンジニアが常に Cisco Unified Communications Sizing Tool（http://tools.cisco.com/cucst）を使用して、それらの設計をすべて検証する必要があります。Sizing Tool を使用して、設計基準を満たすために必要なサーバまたはクラスタの正確な台数を決定します。

キャパシティの計算

キャパシティ プラニング ツールはシスコ代理店と従業員が使用できる機能で、大規模構成の Unified Communications システムのキャパシティの計算に役立ちます。システムの選定でサポートが必要な場合は、シスコ代理店またはシスコのシステム エンジニア（SE）にお問い合せください。

シスコ代理店と従業員は、各ツールを次の Web サイトで入手できます。

- Cisco Unified Communications Sizing Tool は次の Web サイトで入手可能です。

  http://tools.cisco.com/cucst

- Cisco Unified CM キャパシティ ツールは次の Web サイトで入手可能です。

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

これらのツールの両方のマニュアルを参照して、どちらのツールがシステムの設計に最適かを判断してください。

コンピュータ / テレフォニー インテグレーション（CTI）

Cisco コンピュータ / テレフォニー インテグレーション（CTI）を利用すると、Cisco Unified CM で使用可能な豊富な機能セットだけでなく、サードパーティ製のアプリケーションも使用できるようになります。これらの Cisco CTI 対応アプリケーションによって、ユーザの生産性が向上し、コミュニケーションが活発になるとともに、高品質のカスタマー サービスを提供できるようになります。Cisco CTI を使用すると、サードパーティ製デスクトップ アプリケーションで Microsoft Outlook 内から通話を行ったり、着信コールの発信者 ID に基づいてウィンドウを開いたり、アプリケーションを起動したりすることができます。また、課金のためにコールと連絡先をリモートで追跡することもできます。

Cisco CTI 対応のサーバ アプリケーションでは、企業ネットワーク全体での適切な対応先のルーティングや、自動応答や音声自動応答装置（IVR）などの自動発信者サービスの提供に加えて、対応先の記録および分析に役立つメディアの取り込みも行えます。

CTI アプリケーションは一般に、次の 2 つの主なカテゴリに分類できます。

- ファーストパーティ製のアプリケーション：監視、制御、メディア ターミネーション

  ファーストパーティ製の CTI アプリケーションは、コールのセットアップ、終了、およびメディア ターミネーション用の CTI ポートおよびルート ポイントなどのデバイスを登録するように設計されています。これらのアプリケーションはメディア パスに直接配置されているので、インバンド DTMF などのメディア レイヤのイベントに応答できます。ファーストパーティ製の CTI アプリケーションには音声自動応答装置や Cisco Attendant Console などがあり、これらのアプリケーションはコールを監視および制御しながら、コール メディアとも対話します。

- サードパーティ製のアプリケーション：監視および制御

  サードパーティ製の CTI アプリケーションもコールを監視および制御しますが、メディア ターミネーションは直接制御しません。

  - モニタリング アプリケーション

    Cisco IP デバイスの状態を監視する CTI アプリケーションは、モニタリング アプリケーションと呼ばれます。オンフックまたはオフフックのステータスを表示する、またはその情報を使用してユーザの可用性をプレゼンスの形式で示すビジーランプフィールド アプリケーションは、どちらもサードパーティ製の CTI モニタリング アプリケーションの例です。

  - 呼制御アプリケーション

    Cisco CTI を使用して、アウトバンド シグナリングを使用する Cisco IP デバイスをリモート制御するアプリケーションは、呼制御アプリケーションです。Cisco IP デバイスをリモート制御するように設定された Cisco Unified Personal Communicator は、呼制御アプリケーションの良い例です。

  - モニタリング + 呼制御アプリケーション

    これらは、Cisco IP デバイスを監視および制御するすべての CTI アプリケーションです。Cisco Unified Contact Center Enterprise は、エージェントのステータスを監視し、エージェント デスクトップを介してエージェント電話機も制御するため、監視と制御を兼ね備えたアプリケーションの良い例です。

（注）　ここでモニタリング アプリケーション、呼制御アプリケーション、モニタリング + 呼制御アプリケーションの違いを列挙しましたが、この細かな違いはアプリケーション開発者には見えないようになっています。Cisco CTI を使用するすべての CTI アプリケーションは、モニタリングおよび監視の両方に有効です。

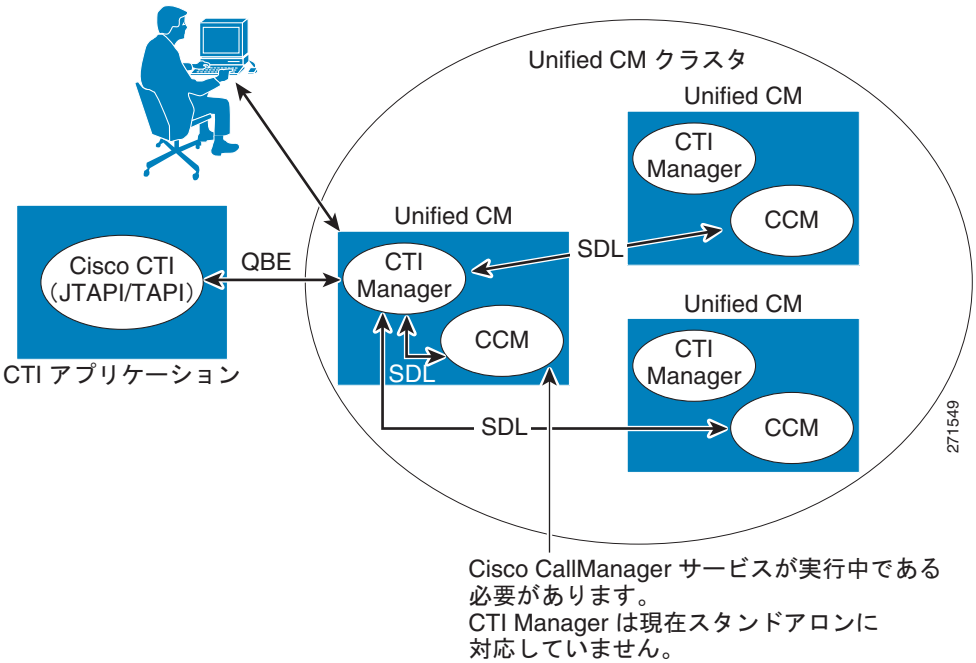
CTI のアーキテクチャ

Cisco CTI は、次のコンポーネントで構成されます（図 8-8 を参照）。これらは互いに対話し、Cisco Unified CM で使用可能なテレフォニー機能セットを各アプリケーションで利用できるようにします。

- CTI 対応アプリケーション：特定のテレフォニー機能を提供するために作成されたシスコ製またはサードパーティ製のアプリケーション。
- JTAPI および TAPI：Cisco CTI でサポートされる 2 つの標準インターフェイス。開発者は、好みの方式のライブラリを使用してアプリケーションを作成できます。
- Unified JTAPI および Unified TSP クライアント：外部メッセージを Cisco Unified CM で使用される内部の Quick Buffer Encoding（QBE）メッセージに変換します。

- Quick Buffer Encoding（QBE）：Unified CM の内部通信メッセージ。
- プロバイダー：アプリケーションと CTI Manager との接続の論理的な表現であり、通信を容易にするために使用されます。プロバイダーは、アプリケーションにデバイス イベントおよびコール イベントを送付しながら、アプリケーションによるデバイスのリモート制御を可能にする制御命令を受け付けます。
- Specification and Description Language（SDL）：Unified CM の内部通信メッセージ。
- パブリッシャおよびサブスクライバ：Cisco Unified Communications Manager（Unified CM）サーバ。
- CCM：Cisco CallManager サービス（ccm.exe）。テレフォニー処理エンジンです。
- CTI Manager（CTIM）：プライマリまたはセカンダリ モードで動作する 1 つ以上の Unified CM サブスクライバで実行され、Cisco IP デバイスを制御および監視できるようにテレフォニー アプリケーションを認証および許可するサービス。

図 8-8　Cisco CTI のアーキテクチャ



アプリケーションを認証および許可すると、CTIM は、テレフォニー アプリケーションと Cisco CallManager サービスの仲介者として機能します（このサービスは呼制御エージェントです。全体の製品名である Cisco Unified Communications Manager と混同しないでください）。CTIM はテレフォニー アプリケーションから送信される要求に応答し、その要求を Unified CM システムで内部的に使用される Specification and Description Language（SDL）メッセージに変換します。Cisco CallManager サービスからのメッセージも CTIM によって受信され、処理のために適切なテレフォニー アプリケーションに転送されます。

CTIM は、Cisco CallManager サービスがアクティブになっているクラスタの Unified CM サブスクライバ サーバでアクティブにできます。これによって、Unified CM クラスタ内で 8 つまでの CTIM をアクティブにできます。スタンドアロンの CTIM はサポートされていません。

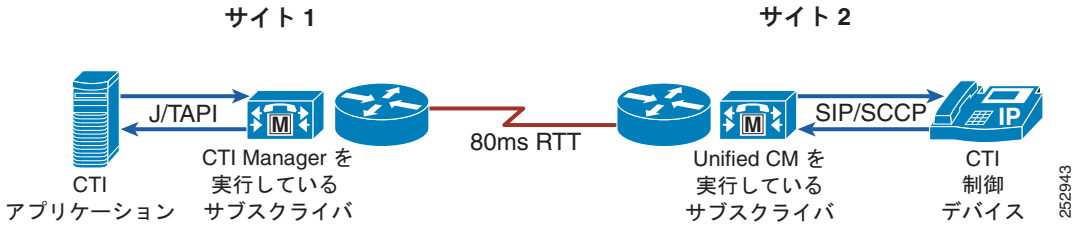
WAN を介した CTI アプリケーションおよびクラスタ化

WAN を介したクラスタ化を採用した配置では、次の 2 つのシナリオがサポートされます。

- WAN を介した CTI Manager（図 8-9 を参照）

  このシナリオでは、CTI アプリケーションとそれに関連付けられた CTI Manager が WAN の一方の側（サイト 1）に配置され、Unified CM サブスクライバに登録される監視および制御対象のデバイスが他方の側（サイト 2）に配置されます。WAN を介したクラスタ化の Round-Trip Time（RTT; ラウンドトリップ時間）は、現在サポートされている限度値 80 ms を超えることはできません。CTI トラフィックに必要な帯域幅を計算するには、「ローカル フェールオーバー配置モデル」（P.2-26）にある公式を使用します。この帯域幅は、「ローカル フェールオーバー配置モデル」（P.2-26）の説明に従って計算した Intra-Cluster Communication Signaling（ICCS）帯域幅や、音声に必要な帯域幅（RTP トラフィック）とは別に必要であることに注意してください。

図 8-9　　WAN を介した CTI



- WAN を介した TAPI および JTAPI アプリケーション（WAN を介した CTI アプリケーション）（図 8-10 を参照）

  このシナリオでは、CTI アプリケーションが WAN の一方の側（サイト 1）に配置され、関連付けられた CTI Manager が他方の側（サイト 2）に配置されます。このシナリオでは、CTI アプリケーション開発者またはプロバイダーの責任において、アプリケーションが実装された RTT に適応できるかどうかを確認します。場合によっては、アプリケーションが CTI Manager と同じ場所にある場合よりも、フェールオーバー時間およびフェールバック時間が長くなることがあります。このような場合、アプリケーション開発者またはプロバイダーは、そのような状況におけるアプリケーションの動作に関するガイダンスを示す必要があります。

図 8-10　　WAN を介した JTAPI

（注） WAN を介した TAPI および JTAPI のサポートは、アプリケーションに依存します。Cisco Unified CM 7.1(2) での WAN を介した TAPI および JTAPI のサポートは新機能であるため、ユーザとアプリケーション開発者またはプロバイダーの両者が、使用するアプリケーションに WAN を介したクラスタ化が含まれる配置との互換性があることを確認する必要があります。

Unified CM のキャパシティ プランニング

Unified CM では、次に示す CTI のキャパシティがサポートされます。

CTI 接続の制限

Cisco Unified CM 7.1(2) 以降、CTI の接続のキャパシティ制限は、次のように最新のサーバ クラスに基づいて増加されています。

- Cisco MCS 7825-H3/I3 は、専用サブスクライバとして使用する場合にサーバごとに 900 個の CTI 接続、またはクラスタごとに 3,600 個の CTI 接続をサポートします。パブリッシャおよびサブスクライバ ノードが組み合わされた Cisco MCS 7825-H3/I3 は、800 個の CTI 接続をサポートします。
- Cisco MCS 7835-H2/I2 は、サーバごとに 2,000 個の CTI 接続またはクラスタごとに 8,000 個の CTI 接続をサポートします。
- Cisco MCS 7845-H2/I2 は、サーバごとに 5,000 個の CTI 接続またはクラスタごとに 20,000 個の CTI 接続をサポートします。

以前のサーバ クラスおよびバージョン 7.1(2) よりも前の Cisco Unified CM リリースは、次の CTI キャパシティ制限をサポートします。

- Cisco MCS 7825 および MCS 7835 は、サーバごとに 800 個の CTI 接続、またはクラスタごとに 3,200 個の CTI 接続をサポートします。
- Cisco MCS 7845 は、サーバごとに 2,500 個の CTI 接続またはクラスタごとに 10,000 個の CTI 接続をサポートします。

注：

- Cisco CTI 対応の IP デバイスは常に、クラスタ内のすべてのノードに対して均等に分散させる必要があります。
- JTAPI アプリケーションの場合、CTI 接続は各 JTAPI アプリケーションと Unified CM サーバ間の単一の TCP/IP 接続です。
- TAPI アプリケーションの場合、CTI 接続は TAPI アプリケーション サーバにある Cisco TSP と Unified CM サーバ間の単一の TCP/IP 接続です。単一の TSP に接続している TAPI アプリケーションが（同じサーバ上に）複数ある場合があります。その場合、それらのすべての TAPI アプリケーションでは 単一の CTI 接続が使用されます。
- 各 CTI 接続は、1 つのアプリケーションまたは CTI の「プロバイダー」セッションを処理します。
- CTI パフォーマンス モニタ（perfmon）の CTI Connection Active を使用すると、特定の Unified CM サーバ上の CTI 接続の合計数を確認できます。

CTI に関連付けられる制御されるデバイスの制限

Cisco Unified CM 7.1(2) 以降、制御される関連デバイスに対する CTI のキャパシティ制限は、次のように最新のサーバ クラスに基づいて増加されています。

- Cisco MCS 7825-H3/I3 は、専用サブスクライバとして使用する場合にサーバごとに 900 台の CTI デバイス、またはクラスタごとに 3,600 台の CTI デバイスをサポートします。パブリッシャおよびサブスクライバ ノードが組み合わされた Cisco MCS 7825-H3/I3 は、800 台の CTI デバイスをサポートします。
- Cisco MCS 7835-H2/I2 は、サーバごとに 2,000 台の CTI デバイスまたはクラスタごとに 8,000 台の CTI 接続をサポートします。
- Cisco MCS 7845-H2/I2 は、サーバごとに 5,000 台の CTI デバイスまたはクラスタごとに 20,000 台の CTI デバイスをサポートします。

以前のサーバ クラスおよびバージョン 7.1(2) よりも前の Cisco Unified CM リリースは、次の CTI キャパシティ制限をサポートします。

- Cisco MCS 7825 および MCS 7835 は、サーバごとに 800 台の CTI デバイス、またはクラスタごとに 3,200 台の CTI デバイスをサポートします。
- Cisco MCS 7845 は、サーバごとに 2,500 台の CTI デバイスまたはクラスタごとに 10,000 台の CTI デバイスをサポートします。

注：

- Cisco CTI 対応の IP デバイスは常に、クラスタ内のすべてのノードに対して均等に分散させる必要があります。
- 制御されるデバイスの制限は、アクティブなアプリケーションにのみ適用されます。非アクティブ（無効）なアプリケーションに関連付けられている制御されるデバイスは、制限にはカウントされません。
- 制御されるデバイスの制限では、デバイスごとに 1 つまたは 2 つの CTI 制御回線が想定されています。同じデバイスに 2 つ以上の CTI 制御回路がある場合、CTI のキャパシティ プランニングではそれぞれが別個のデバイスとしてカウントされます（たとえば、デバイスごとに 2 つの CTI 制御回線を持つ 400 台のデバイスは、400 台の CTI 制御デバイスと同じカウントになりますが、3 つの CTI 制御回線を持つ 400 台のデバイスは 800 台の CTI デバイスとしてカウントされます）。別のデバイスで共有される回線も、その回線が CTI アプリケーションによって制御される場合は制限の対象としてカウントされます。
- 制御されるデバイスの制限では、CTI 制御デバイスごとに最大 3 つの共有回線を使用できることも想定されています。同じデバイスに 2 つ以上の共有回線がある場合、CTI のキャパシティ プランニングではそれぞれが別個のデバイスとしてカウントされます。
- 制御されるデバイスの制限では、各デバイスが最大 3 つの CTI アプリケーションによって監視および制御されることも想定されています。
- 制御されるデバイスの制限には、デバイスにある CTI 制御回線が 1 つであるか 2 つであるかに関係なく、デバイスごとに 1 時間で 6 件のコールという基本コールが想定されています。これ以上のコールがシナリオに含まれる（転送や会議など）場合や、コール レートが高い場合は、制限に影響します（適切なサイジングを行うには、Cisco Unified Communications Sizing Tool を使用します。適切なログイン認証を持つシスコ従業員およびシスコ代理店は、このツールを http://tools.cisco.com/cucst で入手できます）。
- CTI アプリケーションに関連付けられている制御されたデバイスの数が多くなるほど、アプリケーションの初期化と Unified CM フェールオーバー / フェールバック処理時間が長くなります。これは、アプリケーションがアクティブにデバイスを制御していない場合でも当てはまります。
- CTI パフォーマンス モニタ（perfmon）の Devices Open と Lines Open を使用すると、特定の Unified CM サーバ上でアプリケーションによって現在制御されているデバイスと回線の合計数を確認できます。

Cisco Unified Communications Manager Business Edition では、このサーバの CTI デバイスの最大数は 500 です。

プロビジョニング

CTI Manager

CTI Manager は、Unified CM クラスタ内の少なくとも 1 つ（おそらくすべて）のコール処理サブスクライバで有効にする必要があります。クライアント側のインターフェイス（TAPI TSP または JTAPI クライアント）では IP アドレスを 2 つずつ使用できます。これらの IP アドレスは、CTIM サービスを実

行している Unified CM サーバを指します。CTI アプリケーションの冗長性を確保するため、図 8-11 のとおり、クラスタの少なくとも 2 つの Unified CM サーバで、CTIM サービスをアクティブにすることをお勧めします。

冗長性、フェールオーバー、およびロード バランシング

冗長性が必要な CTI アプリケーションでは、TAPI TSP または JTAPI クライアントは 2 つの IP アドレスで設定できるため、障害発生時には代替の CTI Manager を使用できます。ここで注意すべきは、2 つの CTI Manager 間で情報が共有されていないため、この冗長性はステートフルではありません。そのため、フェールオーバーの際に、再初期化が必要になることがあります。

CTI Manager がフェールオーバーした場合、必要な処理は、現在アクティブになっている CTI Manager で CTI アプリケーションのログイン プロセスをやり直すことだけです。ただし、Unified CM サーバ自体に障害が発生した場合は、障害が発生した Unified CM や現在アクティブになっている Unified CM などのすべてのデバイスを再登録し、その後で CTI アプリケーションのログイン プロセスを実行する必要があるため、再初期化プロセスは時間がかかります。

ロード バランシングが必要な CTI アプリケーションや、この設定を利用できる CTI アプリケーションは、図 8-11 に示すように、2 つの CTI Manager に同時に接続できます。

図 8-11　　冗長性とロード バランシング

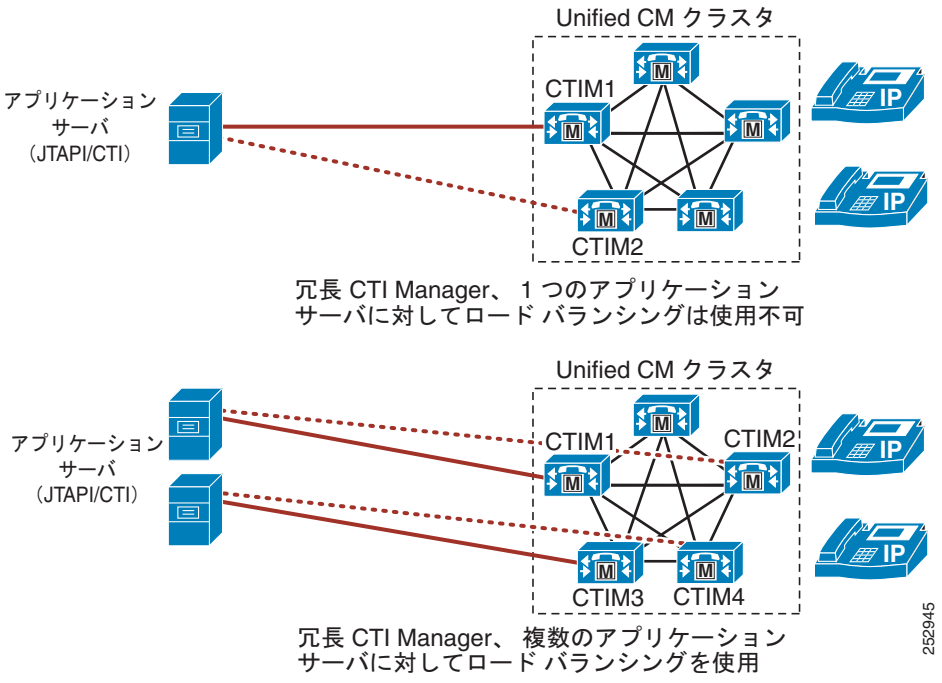


図 8-12 は、このタイプの Cisco Unified Contact Center Enterprise（Unified CCE）の設定例を示しています。このタイプの設定には、次の特性があります。

- Unified CCE は冗長性のために 2 つの Peripheral Gateway（PG; ペリフェラル ゲートウェイ）を使用します。
- 各 PG は異なる CTI Manager にログインします。
- 一度に 1 つの PG しかアクティブになりません。

図 8-12　Cisco Unified Contact Center Enterprise での CTI の冗長性

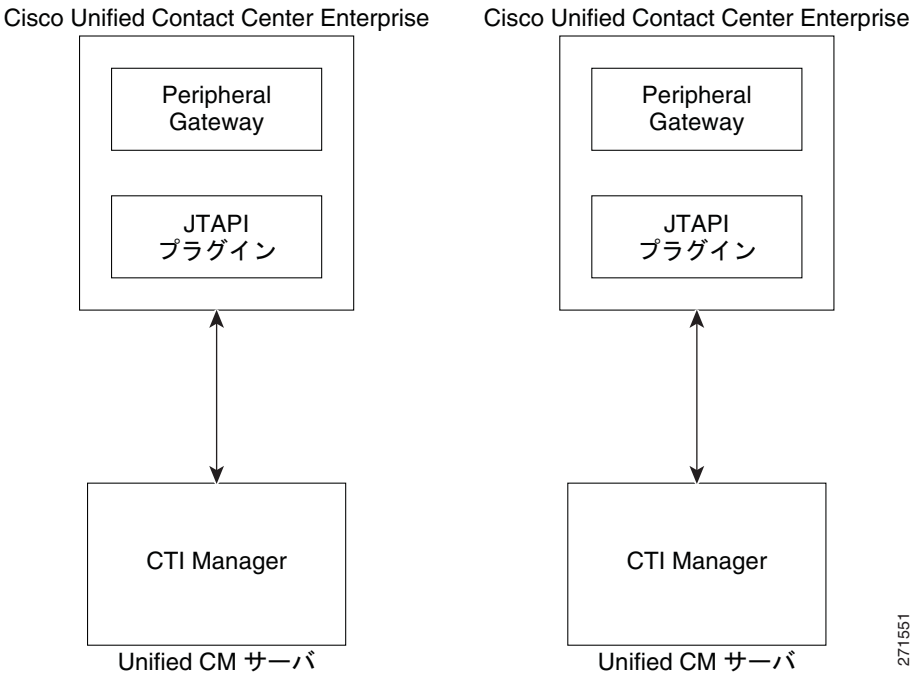
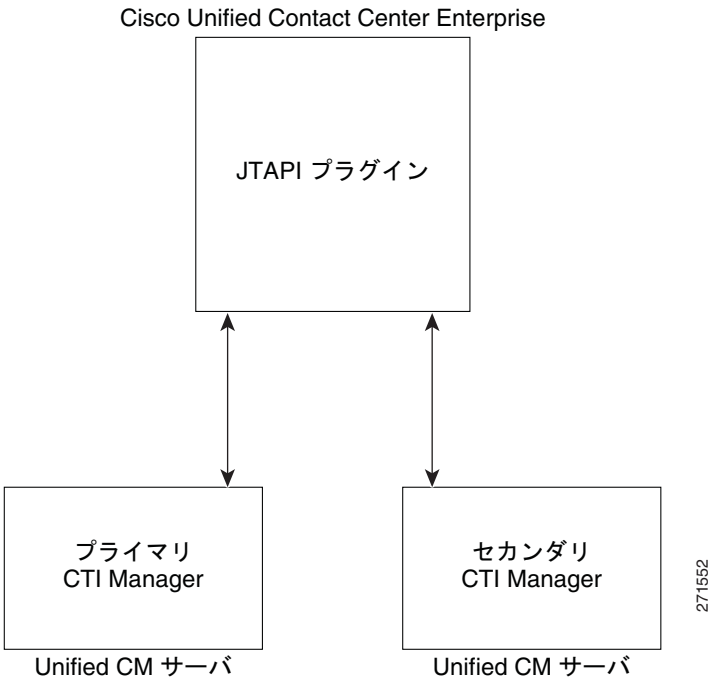


図 8-13 は、このタイプの Cisco Unified Contact Center Express（Unified CCX）の設定例を示しています。このタイプの設定には、次の特性があります。

- Unified CCX では、各 CTI Manager 用に 1 つずつ、合計で 2 つの IP アドレスを設定できます。
- プライマリ CTI Manager への接続が失われた場合、Unified CCX はセカンダリ CTI Manager にフェールオーバーします。

図 8-13　Cisco Unified Contact Center Express での CTI の冗長性



実装

アプリケーションの作成に関するガイダンスとサポートについて、アプリケーション開発者は次の Web サイトの Cisco Developer Connection で相談してください。

http://developer.cisco.com/web/cdc/community

ゲートキーパーの設計上の考慮事項

1 台の Cisco IOS ゲートキーパーで、分散型コール処理環境で最大 100 の Unified CM クラスタに対してコール ルーティングとコール アドミッション制御をサポートできます。複数のゲートキーパーを設定すると、数千の Unified CM クラスタをサポートできます。Cisco IOS ゲートキーパーを使用して、H.323 ゲートウェイと Unified CM 間の通信とコール アドミッション制御をサポートすることによって、ハイブリッド Unified CM とトール バイパス ネットワークを実装することもできます。

ゲートキーパーのコール アドミッション制御は、ポリシーベースの方式であり、使用可能なリソースの静的設定を必要とします。ゲートキーパーは、ネットワーク トポロジを認識しないので、ハブアンドスポーク トポロジに制限されます。

Cisco 2600、2800、2900、3600、3700、3800、3900、および 7200 シリーズ ルータはすべて、ゲートキーパー機能をサポートします。冗長性、ロード バランシング、および階層コール ルーティング用に、さまざまな方法で Cisco IOS ゲートキーパーを設定できます。この項では、ゲートキーパー ネットワークを構築するための設計要件について検討します。ただし、コール アドミッション制御やダイヤル プラン解決については扱いません。これらについては、「コール アドミッション制御」（P.9-1）と「ダイヤル プラン」（P.10-1）の章でそれぞれ説明しています。

ゲートキーパーの詳細については、次の Web サイトで入手可能な『*Cisco IOS H.323 Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps6441/products_installation_and_configuration_guides_list.html

ハードウェア プラットフォームの選択

ゲートキーパーのプラットフォームは、1 秒間あたりのコール数、および同時発生コール数に基づいて選択します。1 秒間あたりのコール数が多いほど、Cisco 3800、3900、7200 シリーズ ルータなどの高性能な CPU が必要になります。同時発生コールの数が大きいほど、より多くのメモリが必要になります。ゲートキーパー プラットフォームの詳細については、次の Web サイトで入手可能な『*Cisco IOS H323 Gatekeeper Data Sheet*』を参照してください。

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps4139/data_sheet_c78_561921.html

ゲートキーパー プラットフォームの選択に関する追加情報については、シスコ代理店またはシスコのシステム エンジニア（SE）にお問い合せください。

ゲートキーパーの冗長性

ゲートキーパーが、クラスタ間通信にすべてのコール ルーティングとアドミッション制御機能をサポートする場合は、冗長性が必要です。ゲートキーパーの冗長性をサポートする方法として、Hot Standby Router Protocol（HRSP; ホットスタンバイ ルータ プロトコル）、ゲートキーパー クラスタリング、および冗長ゲートキーパー トランクという 3 つの方法を使用できます。次の項では、これらの方法について説明します。

（注）　可能な場合、ゲートキーパーの冗長性をサポートするには、ゲートキーパー クラスタリングを使用することをお勧めします。冗長性に HSRP を使用するのは、ソフトウェア機能セットでゲートキーパー クラスタリングが利用できない場合だけにしてください。

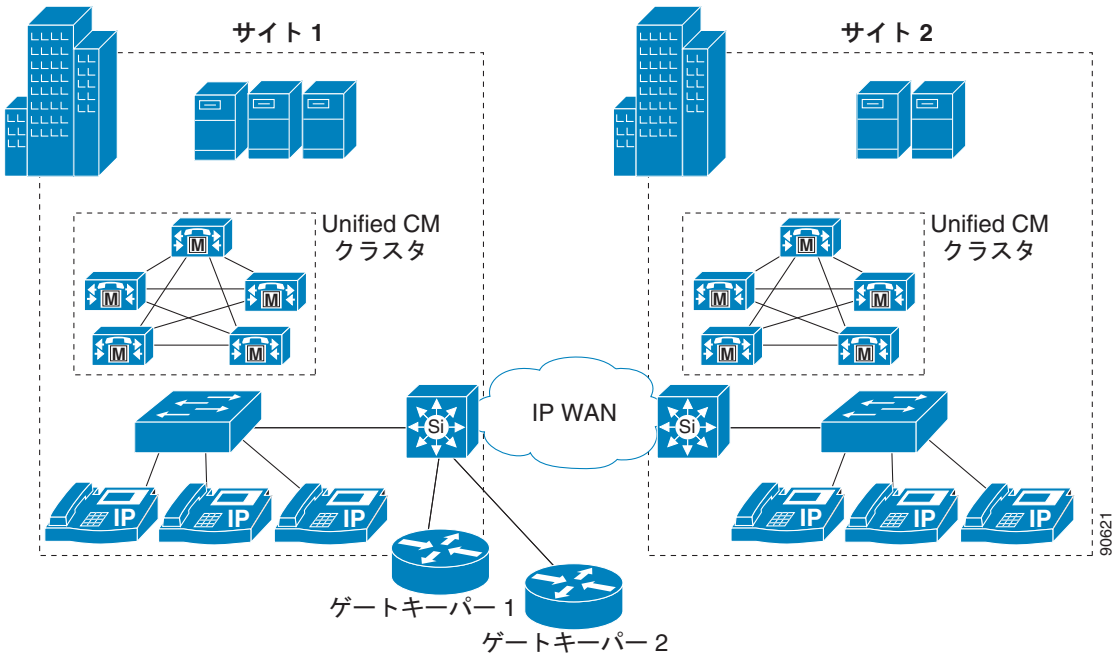
ホットスタンバイ ルータ プロトコル（HSRP）

HSRP には、次のガイドラインが適用されます。

- 一度に 1 つのゲートキーパーしかアクティブになりません。
  - スタンバイ ゲートキーパーは、プライマリに障害が発生した場合でなければ、コールを処理しません。
  - ロード バランシング機能は使用できません。
- すべてのゲートキーパーが同じサブネットまたはロケーションに存在しなければなりません。
- フェールオーバー後に以前の状態情報が使用できません。
- フェールオーバー後、スタンバイ ゲートキーパーは、すでにアクティブになっているコールを認識しないので、帯域幅のオーバーサブスクリプションが発生する可能性があります。
- コールの発信前に、HSRP スタンバイ ゲートキーパーにエンドポイントを再登録する必要があるので、フェールオーバーには相応の時間がかかることがあります。フェールオーバー時間は、登録タイマーの設定に依存します。

図 8-14 では、ゲートキーパーの冗長性に HSRP を使用するネットワーク設定を示しています。

図 8-14　HSRP を使用するゲートキーパー冗長性



例 8-1 では、図 8-14 のゲートキーパー 1 の設定を示しています。例 8-2 では、ゲートキーパー 2 の設定を示しています。イーサネット インターフェイス上の HSRP 設定を除いて、両方の設定は同一です。

例 8-1　ゲートキーパー 1 の設定

```
interface Ethernet0/0
 ip address 10.1.10.2 255.255.255.0
  standby ip 10.1.10.1
  standby priority 110

gatekeeper
 zone local GK-Site1 customer.com 10.1.10.1
 zone local GK-Site2 customer.com
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth interzone default 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

例 8-2　ゲートキーパー 2 の設定

```
interface Ethernet0/0
 ip address 10.1.10.3 255.255.255.0
 standby ip 10.1.10.1

gatekeeper
 zone local GK-Site1 customer.com 10.1.10.1
 zone local GK-Site2 customer.com
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth interzone default 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
```

```
no shutdown
```

ここでは、例 8-1 と例 8-2 について説明します。

- 各ルータには、それぞれが共有する仮想 IP アドレスを識別するために、HSRP 用に **standby** コマンドが設定されます。ゲートキーパー 1 は、コマンド **standby priority 110** を使用して、プライマリとして設定されています。
- Unified CM トランク登録をサポートするために、各 Unified CM クラスタはローカル ゾーンとしてルータ上で設定されます。最初のゾーンに定義されている IP アドレスは、HSRP の使用する仮想 IP アドレスと一致する必要があることに注意してください。
- ゾーン間とクラスタ間のコール ルーティングを可能にするために、両方のルータでゾーンごとにゾーン プレフィックスが設定されます。
- 各ルータで、両方のサイトの帯域幅ステートメントが設定されます。シスコでは、**bandwidth interzone** コマンドを使用することをお勧めします。**bandwidth total** コマンドは、設定内容によっては機能しないことがあるためです。
- ローカルで解決されないすべてのコールを、ローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できるように、**gw-type-prefix 1# default-technology** コマンドが両方のルータで設定されます。この例では、すべての Unified CM トランクは、1# プレフィックスに登録されるように設定されています。
- 冗長 Unified CM トランク上にできるコール ルーティング ループを回避するために、**arq reject-unknown-prefix** コマンドが両方のルータで設定されます。

HSRP に関するこの他の高度な情報については、次の Web サイトにあるオンライン ドキュメントを参照してください。

- http://www.cisco.com/en/US/docs/internetworking/case/studies/cs009.html
- http://www.cisco.com/en/US/tech/tk648/tk362/technologies_q_and_a_item09186a00800a9679.shtml
- http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094afd.shtml

ゲートキーパー クラスタリング（代替ゲートキーパー）

ゲートキーパー クラスタリング（代替ゲートキーパー）により、「ローカル」ゲートキーパー クラスタの設定が可能になります。各ゲートキーパーは、一部の Unified CM トランクのプライマリ、およびその他のトランクの代替として機能します。GUP（Gatekeeper Update Protocol）は、ローカル クラスタ内のゲートキーパー間で状態情報を交換するために使用されます。GUP は、クラスタ内のゲートキーパーごとに CPU 使用率、メモリ使用率、アクティブ コール数、および登録されたエンドポイント数をトラッキングし、報告します。GUP メッセージングで次のパラメータにしきい値を設定すると、ロード バランシングがサポートされます。

- CPU 使用率
- メモリ使用率
- アクティブ コール数
- 登録されたエンドポイント数

ゲートキーパー クラスタリング（代替ゲートキーパー）により、ステートフル冗長性とロード バランシングが使用可能になります。ゲートキーパー クラスタリングは、次の機能を提供します。

- ローカルとリモートのクラスタ
- ローカル クラスタ内の最大 5 つのゲートキーパー
- ローカル クラスタ内のゲートキーパーを、別々のサブネットまたはロケーションに配置可能

- フェールオーバーの遅延なし（代替ゲートキーパーはすでにエンドポイントを認識しているので、完全な登録プロセスを実行する必要はありません）
- クラスタ内のゲートキーパーは、状態情報を渡し、ロード バランシングを行う

図 8-15 では、Unified CM 分散型コール処理を行う 3 つのサイト、およびローカル クラスタで設定された 3 つの分散型ゲートキーパーを示しています。

図 8-15　ゲートキーパー クラスタリング

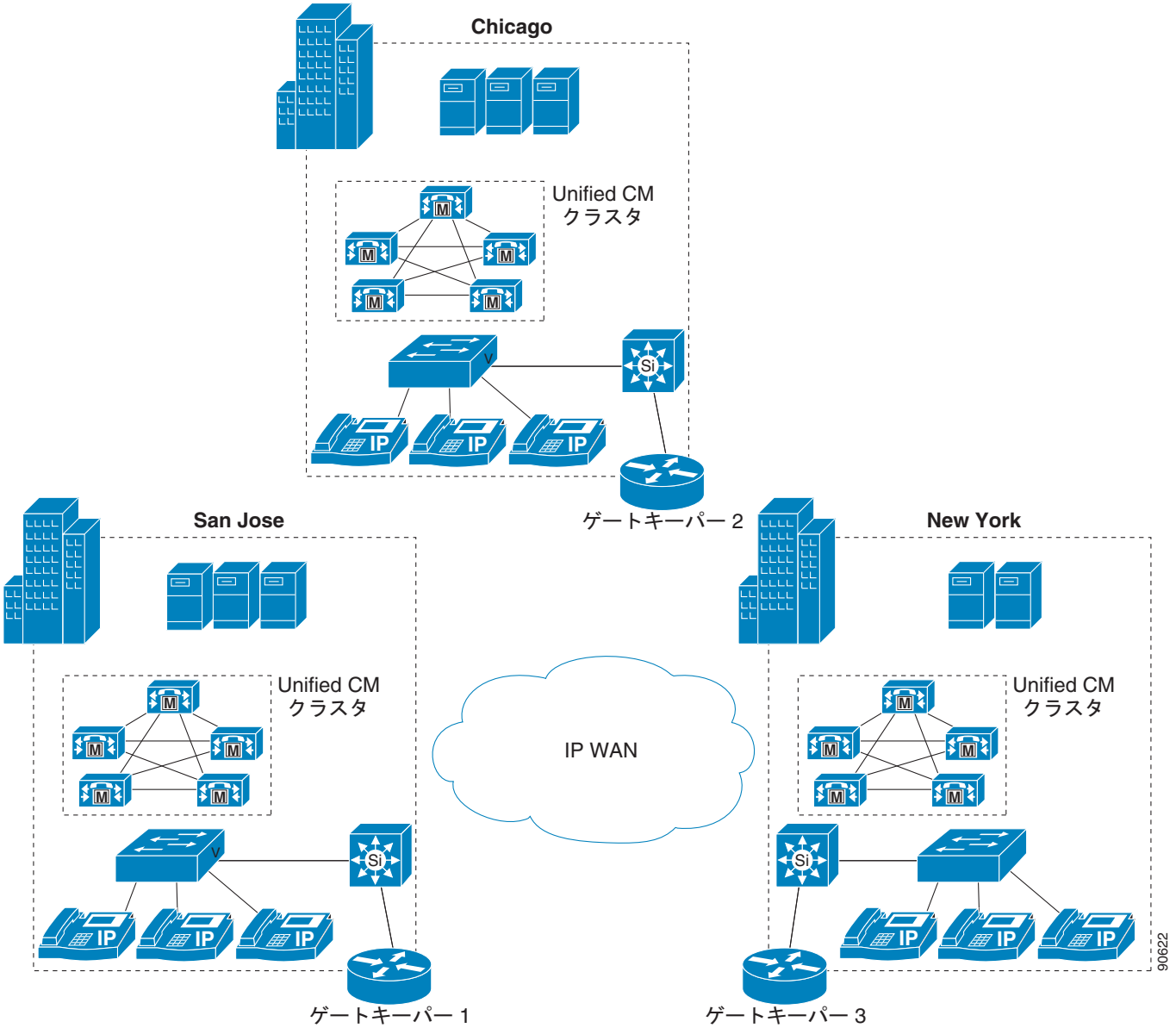


図 8-15 では、ゲートキーパー 2 はゲートキーパー 1 のバックアップ、ゲートキーパー 3 はゲートキーパー 2 のバックアップ、ゲートキーパー 1 はゲートキーパー 3 のバックアップです。

例 8-3 では、ゲートキーパー 1（SJC）の設定を示し、例 8-4 は、ゲートキーパー 2（CHC）の設定を示しています。ゲートキーパー 3（NYC）の設定は、他の 2 つの例を参照してください。

例 8-3　ゲートキーパー 1 のゲートキーパー クラスタリング設定

```
gatekeeper
 zone local SJC cisco.com 10.1.1.1
 zone local CHC_GK1 cisco.com
 zone local NYC_GK1 cisco.com
!
 zone cluster local SJC_Cluster SJC
  element SJC_GK2 10.1.2.1 1719
  element SJC_GK3 10.1.3.1 1719
 !
 zone cluster local CHC_Cluster CHC_GK1
  element CHC 10.1.2.1 1719
  element CHC_GK3 10.1.3.1 1719
 !
 zone cluster local NYC_Cluster NYC_GK1
  element NYC 10.1.3.1 1719
  element NYC_GK2 10.1.2.1 1719
 !
 zone prefix SJC 40852.....
 zone prefix NYC_GK1 21251.....
 zone prefix CHC_GK1 72067.....
 gw-type-prefix 1#* default-technology
 load-balance cpu 80 memory 80
 bandwidth interzone SJC 192
 bandwidth interzone NYC_GK1 160
 bandwidth interzone CHC_GK1 160
 arq reject-unknown-prefix
 no shutdown
```

例 8-4　ゲートキーパー 2 のゲートキーパー クラスタリング設定

```
gatekeeper
 zone local CHC cisco.com 10.1.2.1
 zone local SJC_GK2 cisco.com
 zone local NYC_GK2 cisco.com
!
 zone cluster local CHC_Cluster CHC
  element CHC_GK3 10.1.3.1 1719
  element CHC_GK1 10.1.1.1 1719
!
 zone cluster local SJC_Cluster SJC_GK2
  element SJC  10.1.1.1 1719
  element SJC_GK3 10.1.3.1 1719
 !
  zone cluster local NYC_Cluster NYC_GK2
  element NYC_GK1 10.1.1.1 1719
  element NYC 10.1.3.1 1719
 !
 zone prefix SJC_GK2 40852.....
 zone prefix NYC_GK2 21251.....
 zone prefix CHC 72067.....
 gw-type-prefix 1#* default-technology
 load-balance cpu 80 memory 80
 bandwidth interzone CHC_Voice 160
 bandwidth interzone SJC_Voice2 192
 bandwidth interzone NYC_Voice3 160
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 8-3 と例 8-4 について説明します。

- Unified CM トランク登録をサポートするために、各 Unified CM クラスタにはローカル ゾーンが設定されます。

- ローカル ゾーンごとにクラスタが定義され、他のゲートキーパー上のバックアップ ゾーンはエレメントとしてリストされます。エレメントは、バックアップが使用される順にリストされます。
- ゾーン間とクラスタ間のコール ルーティングを可能にするために、ゾーンごとにゾーン プレフィックスが設定されます。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Unified CM トランクは、1# プレフィックスに登録されるように設定されています。
- **load-balance cpu 80 memory 80** コマンドは、CPU とメモリの使用率を制限します。ルータがどちらかの制限に達すると、新しい要求はすべて拒否され、使用率がしきい値以下に下がるまで、リスト内の最初のバックアップが使用されます。
- サイトごとに帯域幅ステートメントが設定されます。シスコでは、**bandwidth interzone** コマンドを使用することをお勧めします。**bandwidth total** コマンドは、設定内容によっては機能しないことがあるためです。
- **arq reject-unknown-prefix** コマンドは、冗長 Unified CM トランク上にできるコール ルーティング ループを回避します。

クラスタ内のすべてのゲートキーパーは、すべての Unified CM トランク登録状態を把握しています。ゲートキーパーをプライマリ リソースとして使用するトランクの場合、フラグ フィールドはブランクです。クラスタ内の別のゲートキーパーをプライマリ ゲートキーパーとして使用するトランクの場合、フラグ フィールドは A（代替）に設定されます。すべてのエンドポイントをプライマリまたは代替として登録すると、すべてのコールをローカル側で解決できるようになり、別のゲートキーパーにロケーション要求（LRQ）を送信する必要はありません。

例 8-5 では、ゲートキーパー 1（SJC）での **show gatekeeper endpoints** コマンドからの出力を示します。

例 8-5　ゲートキーパー エンドポイントの出力

```
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type        Flags
--------------- ----- --------------- ----- ---------         ----        -----
10.1.1.12       1307  10.1.1.12       1254  SJC               VOIP-GW
    H323-ID: SJC-to-GK-trunk_1
10.1.1.12       4422  10.1.1.12       4330  SJC               VOIP-GW
    H323-ID: SJC-to-GK-trunk_2
10.1.2.12       4587  10.1.2.12       4330  CHC_GK1           VOIP-GW     A
    H323-ID: CHC-to-GK-trunk_1
10.1.3.21       2249  10.1.3.21       1245  NYC_GK1           VOIP-GW     A
    H323-ID:  NYC-to-GK-trunk_1
Total number of active registrations = 4
```

ディレクトリ ゲートキーパーの冗長性

HSRP を使用するか、複数の同じディレクトリ ゲートキーパーを設定すると、ディレクトリ ゲートキーパーの冗長性を実装できます。同じゾーン プレフィックスを使用して、複数のリモート ゾーンをもつゲートキーパーを設定するとき、このゲートキーパーには、次のいずれかの方法が使用できます。

- シーケンシャル LRQ

  冗長リモート ゾーン（ゾーン プレフィックスが一致）にコストが割り当てられ、LRQ は、コスト値に基づいた順序で、一致するゾーンに送信されます。順次 LRQ を使用すると、一致するすべてのゲートキーパーに LRQ を送信しないので、WAN 帯域幅の節約になります。

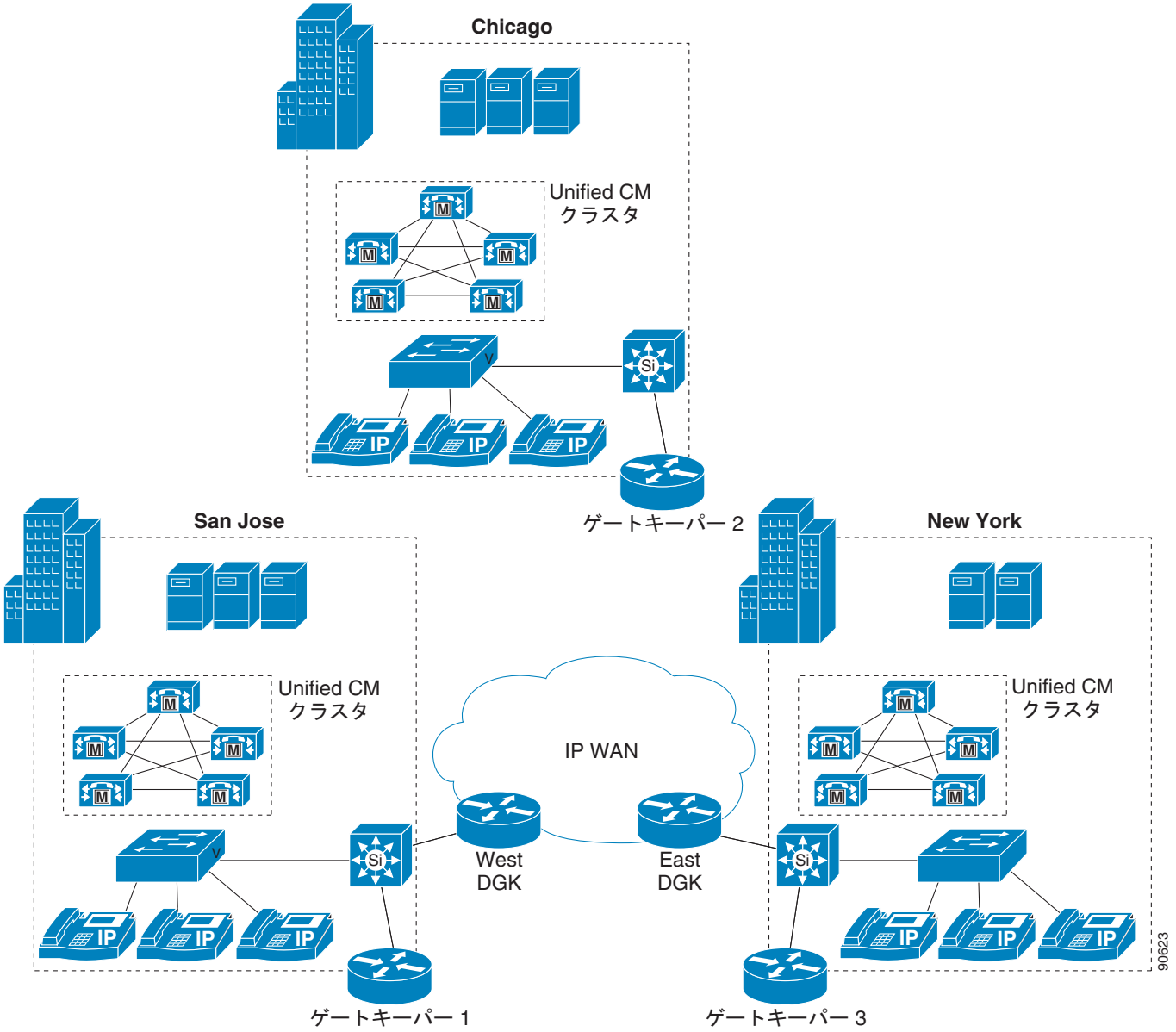
- LRQ ブラスト

  LRQ は、冗長ゾーン（ゾーン プレフィックスが一致）に同時に送信されます。ロケーション確認（LCF）で応答する最初のゲートキーパーが、使用されます。

順次 LRQ を使用して複数のアクティブ ディレクトリ ゲートキーパーを使用することをお勧めします。これによって、ディレクトリ ゲートキーパーを別々のロケーションに配置することができます。HSRP を使用するには、両方のディレクトリ ゲートキーパーを同じサブネットに置く必要があります。この場合常に 1 つのゲートキーパーしかアクティブにすることができません。

図 8-16 では、2 つのアクティブ ディレクトリ ゲートキーパーを備えた Unified CM 分散型コール処理環境を示しています。

図 8-16　冗長ディレクトリ ゲートキーパー



例 8-6 および例 8-7 では、図 8-16 の 2 つのディレクトリ ゲートキーパーの設定を示しています。

例 8-6　　West ディレクトリ ゲートキーパーの設定

```
gatekeeper
 zone local DGKW customer.com 10.1.10.1
 zone remote SJC customer.com 10.1.1.1
 zone remote CHC customer.com 10.1.2.1
 zone remote NYC customer.com 10.1.3.1
 zone prefix SJC 408.......
 zone prefix CHC 720.......
 zone prefix NYC 212.......
 lrq forward-queries
 no shutdown
```

例 8-7　　East ディレクトリ ゲートキーパーの設定

```
gatekeeper
 zone local DGKE customer.com 10.1.12.1
 zone remote SJC customer.com 10.1.1.1
 zone remote CHC customer.com 10.1.2.1
 zone remote NYC customer.com 10.1.3.1
 zone prefix SJC 408.......
 zone prefix CHC 720.......
 zone prefix NYC 212.......
 lrq forward-queries
 no shutdown
```

ここでは、例 8-6 と例 8-7 について説明します。

- 両方のディレクトリ ゲートキーパーはまったく同じように設定されます。
- ディレクトリ ゲートキーパー用にローカル ゾーンが設定されます。
- リモート ゲートキーパーごとに、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のリモート ゾーンにゾーン プレフィックスが設定されます。ワイルドカード（*）をゾーン プレフィックスに使用すると設定を簡潔化できますが、ドット（.）を使用する方がきめ細かく設定できます。コールは DGK ゾーンにルーティングされないので、DGK ゾーンにはプレフィックスは必要ありません。
- **lrq forward-queries** コマンドは、ディレクトリ ゲートキーパーが、別のゲートキーパーから受信した LRQ を転送できるようにします。

（注） ディレクトリ ゲートキーパーは、アクティブ エンドポイント登録を含まず、いかなる帯域幅管理も行いません。

例 8-8、例 8-9、および例 8-10 では、図 8-16 のゲートキーパー 1 ～ 3 の設定を示しています。

例 8-8　　ゲートキーパー 1（SJC）の設定

```
zone local SJC customer.com 10.1.1.1
 zone remote DGKW customer.com 10.1.10.1
 zone remote DGKE customer.com 10.1.12.1
 zone prefix SJC 408.......
 zone prefix DGKW ..........
 zone prefix DGKE ..........
 bandwidth remote 192
 gw-type-prefix 1# default-technology
 arq reject-unknown-prefix
 no shutdown
```

例 8-9　　ゲートキーパー 2（CHC）の設定

```
gatekeeper
 zone local GK-CHC customer.com 10.1.2.1
 zone remote DGKE customer.com 10.1.12.1
 zone remote DGKW customer.com 10.1.10.1
 zone prefix CHC 720.......
 zone prefix DGKE ..........
 zone prefix DGKW ..........
 bandwidth remote 160
 gw-type-prefix 1# default-technology
 arq reject-unknown-prefix
 no shutdown
```

例 8-10　　ゲートキーパー 3（NYC）の設定

```
gatekeeper
 zone local NYC customer.com 10.1.3.1
 zone remote DGKE customer.com 10.1.12.1
 zone remote DGKW customer.com 10.1.10.1
 zone prefix NYC 212.......
 zone prefix DGKE ..........
 zone prefix DGKW ..........
 bandwidth remote 160
 gw-type-prefix 1# default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 8-8、例 8-9、および例 8-10 について説明します。

- Unified CM トランク登録をサポートするために、各 Unified CM クラスタにはローカル ゾーンが設定されます。
- ディレクトリ ゲートキーパーごとに、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、ローカル ゾーンと両方のリモート ゾーンにゾーン プレフィックスが設定されます。両方のディレクトリ ゲートキーパー プレフィックスは、10 個のドットです。一致するゾーン プレフィックスが設定されるとき、デフォルトで順次 LRQ が使用されます。ゲートキーパーは、コストが最低のディレクトリ ゲートキーパーに LRQ を送信します。応答がない場合、ゲートキーパーは、2 番目のディレクトリ ゲートキーパーに LRQ の送信を試みます。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Unified CM トランクは、1# プレフィックスに登録されるように設定されています。
- **arq reject-unknown-prefix** コマンドは、冗長 Unified CM トランク上にできるコール ルーティング ループを回避します。

Unified CM と Unified CM Express の相互運用性

この項では、H.323 または SIP トランキング プロトコルを使用している Cisco Unified CM と Cisco Unified Communications Manager Express（Unified CME）に関して、マルチサイト IP テレフォニー配置における相互運用性およびインターネットワーキングの要件について説明します。ここでは、Unified CM の制御する電話機と Unified CME の制御する電話機との間での推奨する配置を中心に説明します。

この項では、次のトピックについて取り上げます。

Unified CM と Unified CME 間の相互運用性の概要

Cisco Unified CME は、Cisco IP SIP Phone 7905G、7906G、7911G、7912G、7940G、7960G、7941G、7942G、7945G、7961G、7962G、7965G、7970G、7971G、7975G、8961、9951、9971 に加え、Cisco IP SCCP Phone 6921、6941、6961、7905G、7906G、7911G、7912G、7914、7920、7921G、7931G、7935、7936、7940G、7960G、7941G、7942G、7945G、7961G、7962G、7965G、7970G、7971G、7975G、7985G、および Cisco IP Communicator をサポートします。

すべてのコール シグナリングは、使用されるエンドポイントに関係なく、Unified CME を通して送信されます。ただし、SCCP エンドポイントが同じ Unified CME 上にある場合は、メディアは Unified CME を経由しないで流れることができます（フロー アラウンド）。SIP エンドポイントが同じ Unified CME 上にある場合は、Unified CME Release 4.1 以降ではメディアは Unified CME を経由しないで流れることができますが（フロー アラウンド）、4.1 よりも前のリリースでは Unified CME を経由して流れます（フロー スルー）。

（注）「*フロー アラウンド*」とは、メディアが電話機間で直接送信されることを意味します。「*フロー スルー*」とは、メディアは電話機間で直接送信されず、Unified CME を通じて送信されることを意味します。

H.323 または SIP をトランキング プロトコルとして使用して、Unified CM と Unified CME を相互接続できます。本社または中央サイトに Unified CM を配置して、支店の Unified CME システムと連携させる場合、ネットワーク管理者は、プロトコルの仕様と WAN トランク全体でサポートされる機能を慎重に検討して、SIP または H.323 のいずれかのプロトコルを選択する必要があります。以前は、H.323 トランクを使用して Unified CM と Unified CME を接続する方法が主流でしたが、SIP 電話機と SIP トランクのより高度な機能が Unified CM と Unified CME に追加されたことで、この状況は変わりました。この項ではまず、Unified CM と Unified CME の相互運用性のトランキング プロトコルとは無関係のいくつかの機能について説明し、次に SIP トランクと H.323 トランクを使用するための最も一般的な設計シナリオとベスト プラクティスを紹介します。

コール タイプとコール フロー

一般に、Unified CM と Unified CME のインターワーキングを使用すると、SIP トランクまたは H.323 トランク全体で、SCCP IP Phone から SIP IP Phone へのコール、またはその逆のコールをすべて組み合せることができます。コールは、Unified CM と Unified CME SIP 間、または SCCP IP Phone との間で、転送（ブラインドまたは打診）または自動転送することができます。

H.323 トランク経由で Unified CM に接続していると、Unified CME は Unified CM のコールを自動検出できます。Unified CME を終端とするコールが転送または自動転送されると、Unified CME はコールを再生成し、ヘアピンコールによって他の Unified CME または Unified CM に適切にコールをルーティングします。Unified CME は必要に応じて、SIP トランクまたは H.323 トランク全体の VoIP コールについて、Unified CM からのコール レッグをヘアピンします。H.450 以外でサポートされる Unified CM ネットワークで自動検出を可能にする方法と、H450.2、H450.3、または SIP の付加サービスを有効または無効にする方法の詳細については、http://www.cisco.com/en/US/products/sw/voicesw/ps4625/tsd_products_support_series_home.html で入手可能な Unified CME の製品マニュアルを参照してください。

SIP トランク経由で Unified CM に接続すると、Unified CME は Unified CM のコールを自動検出しません。デフォルトでは、Unified CME は常に、コール転送の SIP Refer メッセージまたは自動転送の SIP 302 Moved Temporarily メッセージを使用して、コールをリダイレクトしようとします。リダイレクトが失敗すると、Unified CME はヘアピンコールを試みます。

Music on Hold

Unified CM では G.711 形式と G.729 形式の両方で MoH ストリームを有効にできますが、Unified CME で MoH をストリームできるのは G.711 形式のみです。そのため、保留になったコールの MoH オーディオを Unified CME で制御する場合は、G.711 MoH ストリームと G.729 コール レッグの間でトランスコーディングするためのトランスコーダが必要です。

Ad Hoc および Meet-Me のハードウェア会議

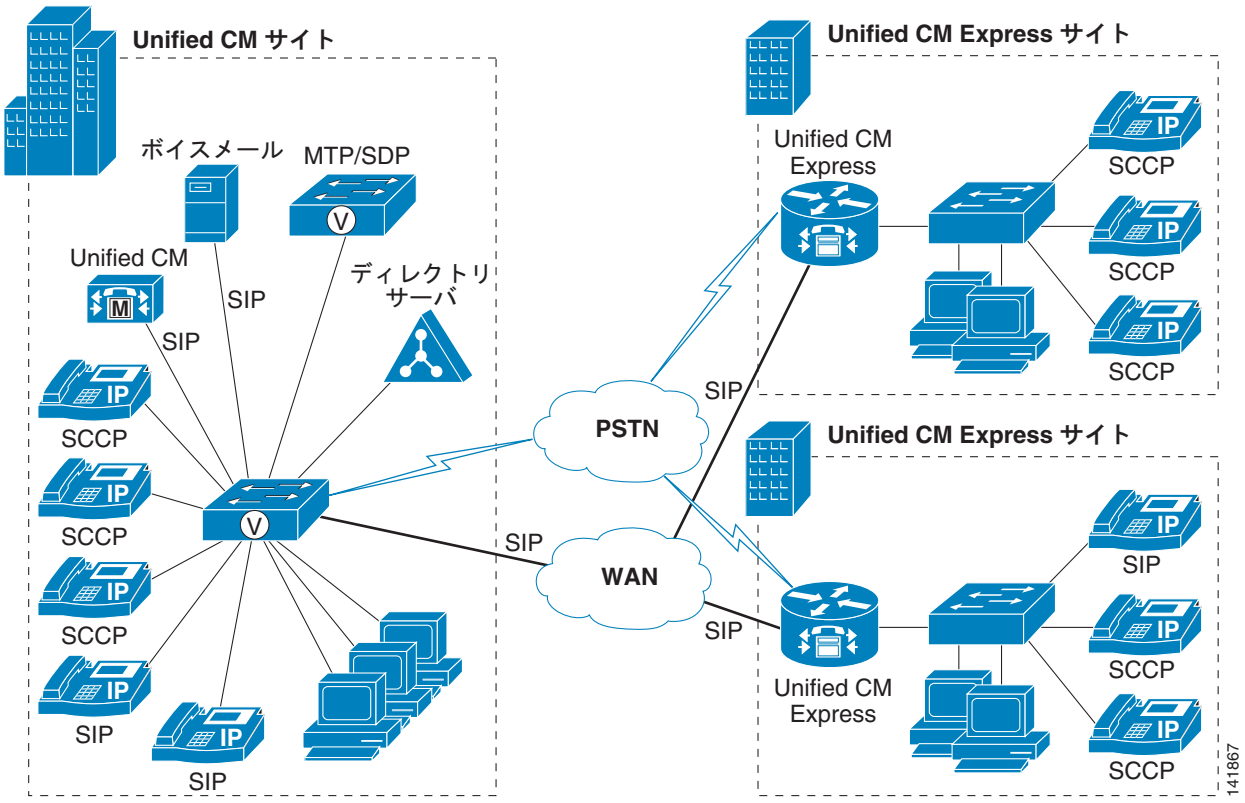
Ad Hoc 会議と Meet-Me 会議の両方に、ハードウェアの DSP リソースが必要です。SIP、H.323、PSTN のいずれを経由して接続している場合でも、Unified CM 電話機と Unified CME 電話機は、ネットワークから到達できるかぎり、Ad Hoc 会議に招待または追加されて、会議の参加者になることができます。アクティブな会議のセッション中にコールを保留にしても、その会議のセッションの参加者には音楽は聞こえません。

Ad Hoc 会議と Meet-Me 会議に必要でサポートされる DSP リソースと、会議に参加できる最大人数については、http://www.cisco.com/en/US/products/sw/voicesw/ps4625/tsd_products_support_series_home.html で入手可能な Unified CME の製品マニュアルを参照してください。

分散型コール処理を使用したマルチサイト配置における SIP 経由の Unified CM と Unified CME の相互運用性

Unified CM は、SIP インターフェイスを使用する Unified CME と直接通信することができます。図 8-17 は、SIP トランク インターフェイスを使用して Unified CM が Cisco Unified CME と直接ネットワーク接続されている Cisco Unified Communications マルチサイト配置を示しています。

図 8-17　SIP トランクを使用して Unified CM と Unified CME を接続したマルチサイト配置



ベスト プラクティス

図 8-17 に示した配置モデルを使用する場合は、次のガイドラインに従い、ベスト プラクティスを参考にしてください。

- **Accept Replaces Header** を選択した SIP トランク セキュリティ プロファイルを設定します。
- 作成した SIP トランク セキュリティ プロファイルを使用して SIP トランクを Unified CM 上に設定し、再ルーティング CSS も指定します。再ルーティング CSS は、どこで SIP ユーザ（転送者）が別のユーザ（被転送者）を第三者ユーザ（転送先）に振り向けることができるか、および SIP 302 Redirection Response と Replaces を持つ INVITE を使用して SIP ユーザがどの機能を呼び出せるかを決定するために使用します。
- SIP トランクの場合、Unified CME 上で SCCP エンドポイントを使用しているときに、メディア ターミネーション ポイント（MTP）を使用可能にする必要はありません。ただし、Unified CME 上に SIP エンドポイントがある場合は、メディア ターミネーション ポイントを Unified CM 上で使用して、SIP プロトコルで遅延オファー / アンサー交換の処理（Session Description Protocol なしの INVITE 受信）ができるようにする必要があります。

- Unified CM ダイヤル プラン設定（ルート パターン、ルート リスト、ルート グループ）を使用して、SIP トランク経由で Unified CME にコールをルーティングします。
- Unified CM のデバイス プールとリージョンを使用して、サイト内では G.711 コーデックを設定し、リモートの Unified CME サイトに対しては G.729 コーデックを設定します。
- Unified CME の **voice services voip** で **allow-connections sip to sip** コマンドを設定して、SIP-to-SIP コール接続を許可します。
- SIP エンドポイントの場合は、**voice register global** で **mode cme** コマンドを設定し、Unified CME の SIP 電話機ごとに **voice register pool** コマンドで **dtmf-relay rtp-nte** を設定します。
- SCCP エンドポイントの場合は、Unified CME の **telephony-service** で **transfer-system full-consult** コマンドと **transfer-pattern .T** コマンドを設定します。
- Unified CME の **session protocol sipv2** および **dtmf-relay [sip-notify** | **rtp-nte]** により、SIP WAN インターフェイスの voip ダイヤル ピアを設定し、Unified CM を宛先としてコールを転送またはリダイレクトします。

この SIP 配置モデルを使用した Unified CME の設定例については、例 8-11 を参照してください。

設計上の考慮事項

この項ではまず、一部の主要な領域における SIP 経由での Unified CM と Unified CME の相互運用性に関するいくつかの特徴と設計上の考慮事項について説明します。主要な領域には、コール転送や自動転送のための付加サービス、短縮ダイヤル ボタンや電話帳のコール リストの Busy Lamp Field（BLF）通知のためのプレゼンス サービス、パートナー アプリケーションとの統合や、Unified CM 電話機と Unified CME 電話機間のクリックダイヤルに対するサードパーティ製電話による制御のための Out-Of-Dialog Refer（OOD-Refer）などが含まれます。この項では、SIP 経由での Unified CM と Unified CME の相互運用性に関する設計上の一般的な考慮事項についても説明します。

付加サービス

SIP Refer メッセージや SIP 302 Moved Temporarily メッセージを Unified CME または Unified CM でのコール転送や自動転送などの付加サービスに使用して、転送先または自動転送先に対して新しいコールを開始するよう、被転送者または自動転送される電話機（被転送者）に指示することができます。SIP Refer メッセージまたは SIP 302 Moved Temporarily メッセージがサポートされている場合、コール転送や自動転送のシナリオにはヘアピンは不要です。

ただし、DID マッピングがない内線が存在する場合や、Unified CM または Unified CME に、SIP 302 Moved Temporarily メッセージの DID にコールをルーティングするダイヤル プランがない場合は、**supplementary-service** を無効にする必要があります。**supplementary-service** が無効になっていると、Unified CME はコールをヘアピンするか、re-INVITE の SIP メッセージを Unified CM に送信して、新しい着信者 ID へメディア パスを置き換えます。それ以降のコール転送に複数の Unified CME が関係する場合でも、シグナリングとメディアの両方がヘアピンされます。転送されたコールでも、**supplementary-service** は無効にできます。この場合、SIP Refer メッセージ は Unified CM に送信されませんが、被転送者と転送先がヘアピンされます。

（注）　付加サービスを無効にするには、**voice service voip** または **dial-peer voice** xxxx voip で **no supplementary-service sip moved-temporarily** コマンドか **no supplementary-service sip refer** コマンドを実行します。

次の例は、付加サービスが無効になっているときのコール フローを示しています。

- Unified CM の電話機 B が Unified CME の電話機 A にコールします。電話機 A は電話機 C（Unified CM 電話機、同一または異なる Unified CME 上にある Unified CME 電話機、公衆網電話機のいずれか）に自動転送（Forward All、Forward Busy、Forward No Answer）するように設定されています。

  Unified CME は Unified CM に SIP 302 Moved Temporarily メッセージを送信しませんが、Unified CM 電話機 B と電話機 C の間でコールをヘアピンします。

- Unified CM の電話機 B が Unified CME の電話機 A にコールします。電話機 A はコールを電話機 C（Unified CM 電話機、Unified CME 電話機、公衆網電話機のいずれか）に転送します。

  Unified CME は Unified CM に SIP Refer メッセージを送信しませんが、Unified CM 電話機 B と電話機 C の間でコールをヘアピンします。

SIP 経由での Unified CM と Unified CME の相互運用性に関する設計上の一般的な考慮事項

- Unified CM への SIP トランクを使用する基本的なコールと付加機能には、Unified CME 4.1 以降のリリースを使用します。
- SIP 302 Moved Temporarily メッセージまたは SIP Refer メッセージが Unified CM でサポートされていない場合は、**supplementary-service** を無効にします。無効にしないと、Unified CM はコールを転送先または自動転送先にルーティングできません。
- SIP-to-SIP コール シナリオでは、Refer メッセージがデフォルトで転送者から被転送者に送信され、被転送者は転送先への新しいコールをセットアップします。コールが転送先につながるまで、転送者にはデフォルトでリングバック トーンが聞こえます。Unified CME の **supplementary-service** が無効になっている場合、Unified CME は、被転送者と転送先の間でコールが接続されるとすぐにインバンドのリングバック トーンを提供します。
- プレゼンス サービスは、SIP トランク経由の Unified CM と Unified CME でのみサポートされます。
- OOD-Refer 機能を使用すると、サードパーティ製アプリケーションで SIP REFER メソッドを使用して、Unified CM または Unified CME の 2 つのエンドポイントを接続できます。OOD-Refer を使用する場合は、次の点を考慮してください。
  - Unified CM と Unified CME はどちらも、OOD-Refer 機能が有効になるよう設定する必要があります。
  - 保留、転送、および会議は、OOD-Refer トランザクション中はサポートされませんが、Unified CME によってブロックされることもありません。
  - コール転送がサポートされるのは、OOD-Refer コールが接続状態になった後のみで、コールの接続前はサポートされません。そのため、接続前はコールの transfer-at-alert はサポートされません。
- TLS のシグナリング制御はサポートされますが、SRTP は SIP トランク経由ではサポートされません。
- ビデオは、SIP 電話機でも SIP トランク経由でもサポートされません。
- SIP トランク経由の SRTP は、Unified CM 用 Cisco IOS Release 12.4（15）T のゲートウェイ機能です。SRTP サポートは、SIP トランク経由での Unified CM と Unified CME のインターワーキングでは使用できません。

（注） 複数の公衆網接続（Unified CM に 1 つと Unified CME に 1 つ）が存在する場合、公衆網エンドポイントに対する Unified CM エンドポイントと Unified CME エンドポイント間の完全在席転送は失敗します。複数の公衆網接続を使用する場合にはブラインド転送の使用を推奨し、この設定は **telephony-service** で **transfer-system full-blind** として行います。

（注） Cisco Unified CME は、SIP トランクを介した複数の Unified CME 間のビデオ コールをサポートします。この機能は、Unified CME だけを使用する分散型コール処理配置で適用されます。SIP トランクを介した Unified CM と Unified CME との間のビデオ コールは現在サポートされていません。設定の詳細については、http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_and_configuration_guides_list.html で入手可能な『*Cisco Unified Communications Manager Express System Administrator Guide*』を参照してください。

設定例

次の例は、この項で説明した設計上の考慮事項とベスト プラクティスの一部を示しています。

例 8-11　SIP を使用する Cisco Unified CME の設定

```
voice service voip
    allow-connections sip to sip
    sip
    registrar server
dial-peer voice 1 voip       /* To Unified CM endpoints */
    destination-pattern xxxx
    session protocol sipv2
    session target ipv4:10.10.10.20
    session transport udp    /* tcp can be used here also */
    dtmf-relay rtp-nte
    codec g729r8             /* Voice class can also be used */
    no vad
voice register global
    mode cme
    source-address 10.10.10.21 port 5060
    create profile
voice register pool 1
    id mac 0007.0E8B.5777
    type 7940
    number 1 dn 1
    codec g729r8      /* Voice class can also be used */
    dtmf-relay rtp-nte
telephony-service
 load 7960-7940 P0S3-07-04-11
 ip source-address 10.10.10.22 port 2000
 create cnf-files
 keepalive 45
 max-conferences 8 gain -6
 moh music-on-hold.au
 transfer-system full-consult /* full-blind can also be used */
 transfer-pattern .T
```

分散型コール処理を使用したマルチサイト配置における H.323 経由の Unified CM と Unified CME の相互運用性

分散型コール処理を使用したマルチサイト WAN 配置で、H.323 接続経由の Unified CM と Unified CME の相互運用性を実現する配置オプションは 2 つあります。1 番目のオプションは、Cisco Unified Border Element を Unified CM のフロントエンド デバイスとして配置する方法であり、リモートの Unified CME システムとはピアツーピア H.323 で接続します。Cisco Unified Border Element が Unified CM と Unified CME との間のダイヤル プラン解決を実行し、同時に両者間のコール シグナリング メッセージを終端し、再発信します。Cisco Unified Border Element は、Unified CM など、付加サービスの H.450 をサポートしないシステムのためにプロキシ デバイスとして機能し、Empty Capability Set（ECS）を使用して付加サービスを呼び出します。また、Cisco Unified Border Element は、Unified CM クラスタ用の公衆網ゲートウェイとしても動作できるため、公衆網ゲートウェイを別に用意する必要がありません。

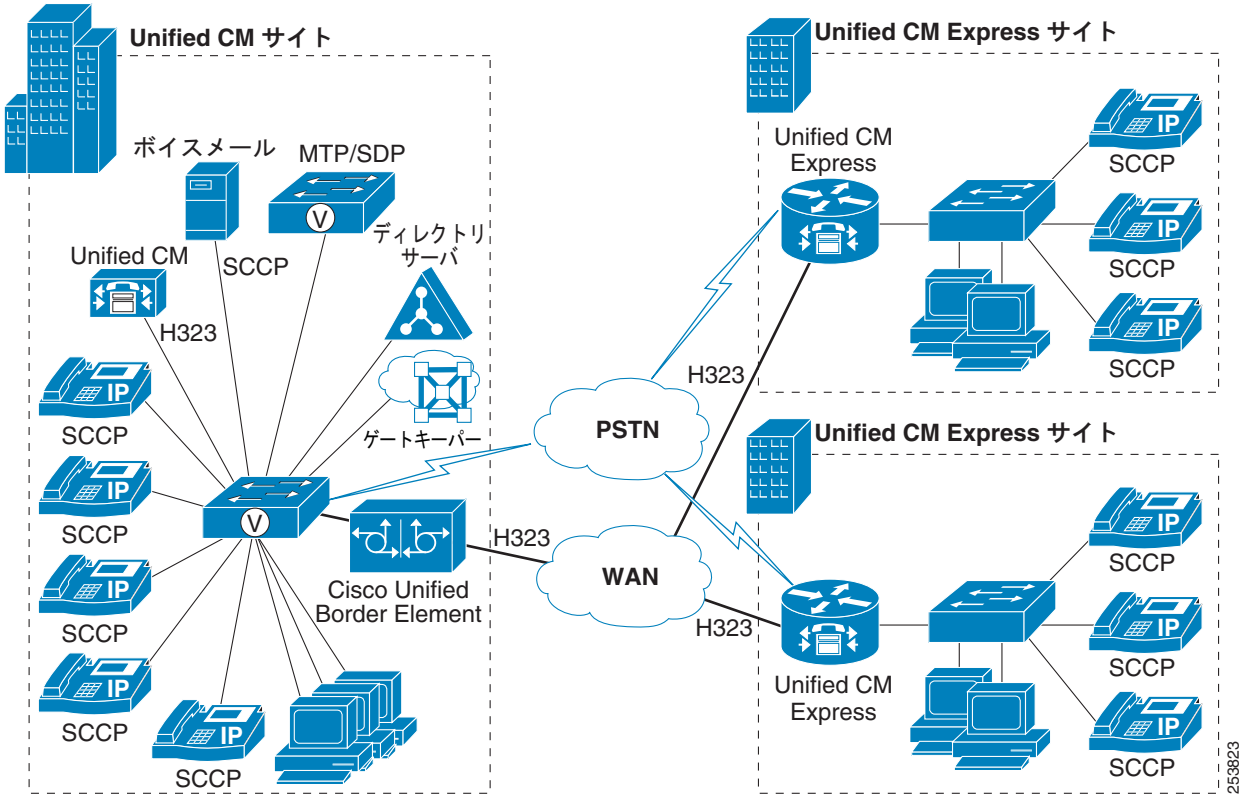
2 番目のオプションは、中継ゾーン ゲートキーパー経由で配置する方法です。Unified CM、Unified CME、および Cisco Unified Border Element はすべて、VoIP ゲートウェイ デバイスとして中継ゾーン ゲートキーパーに登録されます。中継ゾーン ゲートキーパーが Unified CM と Unified CME 間のダイヤル プラン解決と帯域幅制限を実行します。また、中継ゾーン ゲートキーパーは、ECS と H.450 との間で相互作用するコール パスに Cisco Unified Border Element を挿入し、付加サービスを呼び出します。中継ゾーン ゲートキーパーと Cisco Unified Border Element の詳細については、「コール アドミッション制御」（P.9-1）の章を参照してください。

これらの 2 つの配置オプションには、次の相違点があります。

- 1 番目のオプションでは、Cisco Unified Border Element は H.323 ゲートウェイ デバイスとして Unified CM に登録され、2 番目のオプションでは、VoIP ゲートウェイ デバイスとして中継ゾーン ゲートキーパーに登録されます。
- 1 番目のオプションでは、Cisco Unified Border Element が Cisco Unified Border Element の VoIP ダイヤルピア設定に基づくダイヤル プラン解決を実行し、2 番目のオプションでは、中継ゾーン ゲートキーパーがゲートキーパーのダイヤル プラン設定に基づくダイヤル プラン解決を実行します。
- 1 番目のオプションでは、両方のコール レッグを監視するコール アドミッション制御メカニズムがなく、2 番目のオプションでは、中継ゾーン ゲートキーパーがゲートキーパー ゾーンベースのコール アドミッション制御を実行します。
- 2 番目のオプションでは、中継ゾーン ゲートキーパーは Unified CM のインフラストラクチャ ゲートキーパーとして機能し、Unified CM クラスタ間、Unified CM クラスタと H.323 VoIP ゲートウェイのネットワーク間、および Unified CM クラスタとサービス プロバイダーの H.323 VoIP 転送ネットワーク間のすべてのダイヤル プラン解決および帯域幅制限を管理することもできます。

図 8-18 は、中継ゾーン ゲートキーパーと Cisco Unified Border Element を使用する Unified CM と Unified CME 間の H.323 統合を示しています。

図 8-18　Cisco Unified Border Element または中継ゾーン ゲートキーパーを使用して Unified CM と Unified CME を接続するマルチサイト配置



ベスト プラクティス

この項では、2 番目の配置オプション（中継ゾーン ゲートキーパー）で、図 8-18 に示した配置モデルを使用する場合のガイドラインとベスト プラクティスについて説明します。

- Unified CM と中継ゾーン ゲートキーパーとの間にゲートキーパー制御の H.225 トランクを設定します。メディア ターミネーション ポイント（MTP）のリソースがトランクに必要になるのは、Unified CME が 発信 H.323 fast-start コールを開始しようとしたときのみです。
- トランクの両端の H.323 デバイスが、遠端デバイスによって先に TCS が送信されるのを待っていて、H.245 接続が数秒後にタイムアウトになる場合、デッドロック状態が発生しないようにするため、**Wait For Far End H.245 Terminal Capability Set**（TCS）オプションをオフにする必要があります。
- Unified CM サービス パラメータ **Send H225 user info message** を **H225 info for Call Progress Tone** に設定し、Unified CM から Unified CME に H.225 Info message を送信して、リングバック トーンまたは保留音を再生できるようにします。
- Unified CM ダイヤル プランの設定（ルート パターン、ルート リスト、およびルート グループ）を使用して、Unified CME を宛先とするコールをゲートキーパー制御の H.225 トランクに送信します。
- Unified CME と Cisco Unified Border Element を H.323 ゲートウェイとして中継ゾーン ゲートキーパーに登録します。

- Cisco Unified Border Element 上で **allow-connection h323 to h323** コマンドを設定して、H.323-to-H.323 コール接続を許可します。このコマンドは、Unified CME に対して設定するためのオプションです。Cisco Unity Connection を Unified CME で使用する場合は、**allow-connection h323 to sip** を設定します。
- コール転送や自動転送などの付加サービスでは、2 つのエンドポイントが同じ Unified CME 支店ロケーションに存在する場合に、コールのメディア ヘアピンが発生します。

（注）　2 つの配置オプションにおける設定の違いは、1 番目のオプションでは、Unified CM で Cisco Unified Border Element を H.323 ゲートウェイ デバイスとして設定する必要があることだけです。上記のその他の設定ガイドラインは、どちらのオプションも同じです。

（注）　複数の公衆網接続（Unified CM に 1 つと Unified CME に 1 つ）が存在する場合、公衆網エンドポイントに対する Unified CM エンドポイントと Unified CME エンドポイント間の完全在席転送は失敗します。複数の公衆網接続を使用する場合にはブラインド転送の使用を推奨し、この設定は **telephony-service** で **transfer-system full-blind** として行います。

Cisco Unified Border Element と Unified CME の設定例については、例 8-12 と例 8-13 を参照してください。

設計上の考慮事項

H.323 配置では、Unified CME はコール転送、H.450.2、および H.450 標準の一部としての H.450.3 を使用した自動転送をサポートします。ただし、Unified CM は H.450 をサポートしません。また、コール転送、自動転送、保留または保留解除などの付加サービスは、Empty Capabilities Set（ECS）を使用して行われます。そのため、コールが Unified CM と Unified CME との間で転送または自動転送されると、Cisco Unified Border Element を使用して、コールはヘアピンされ、ルーティングされます。前の項の 2 つの配置モデルとして説明したように、ゲートキーパーは使用される場合と使用されない場合があります。この項では、H.323 経由の Unified CM と Unified CME の相互運用性の設計上の考慮事項とベスト プラクティスを示します。

コール転送および自動転送などの付加サービス

Unified CME は、H.450.12 プロトコルを使用して H.450.*x* 機能を自動的に検出することで、H.450 をサポートしない Unified CM を自動検出します。Unified CME は、Unified CM と Unified CME 間のコールに VoIP ヘアピン ルーティングを使用します。コールが終端すると、Unified CME は必要に応じてコールを再発信およびルーティングして、Unified CM 電話機からのコールをヘアピンします。

（注）　Unified CME は、Unified CM が H.450 をサポートしないことを検出すると、Unified CME でシグナリングとメディアの両方をヘアピンして、コールをヘアピンします。そのため、コールを WAN を介して転送または自動転送すると、消費される帯域幅の量は 2 倍になります（たとえば、Unified CM 電話機が Unified CME 電話機にコールして、Unified CME 電話機がコールを 2 番目の Unified CM 電話機に転送すると、Unified CME は、2 台の Unified CM 電話機間のコールでも、シグナリングとメディアの両方をヘアピンします）。この WAN での 2 倍の帯域幅消費を避けるために、Cisco Unified Border Element を使用して H.450 タンデム ゲートウェイとして機能させ、コール転送または自動転送などの付加サービスで H.450-to-ECS マッピングを可能にすることをお勧めします。

サポートされるコール フロー

Unified CME は Back-To-Back User Agent（B2BUA; バックツーバック ユーザ エージェント）なので、コール フローは SCCP 電話機から SCCP 電話機へ、および SCCP 電話機から SIP 電話機へと機能します。SIP 電話機のコールは H.323 トランク経由で機能しますが、付加機能はサポートされません。

セキュリティ

Unified CME は TLS 経由でセキュア シグナリングを提供します。Unified CME 4.2 は SRTP 経由でメディア暗号化のサポートを追加します。Unified CM はまた、TLS 経由でセキュア シグナリング、および SRTP 経由でセキュア メディアをサポートします。ただし、セキュア Unified CM とセキュア Unified CME との間のインターワーキングはまだサポートされていません。

ビデオ

Unified CME を使用してビデオ機能を実装する場合は、次の設計上の考慮事項に従ってください。

- Unified CM と Unified CME のすべてのエンドポイントは、ビデオ対応エンドポイントとして設定する必要があります。ビデオ コーデックとビデオ形式は、すべてのビデオ対応エンドポイントで一致する必要があります。
- Unified CM と Unified CME は基本的なビデオ コールをサポートしますが、コール転送や自動転送などの付加サービスは、Unified CM と Unified CME 間のビデオ コールではサポートされません。Unified CME で付加サービスをサポートするには、すべての Unified CME と音声ゲートウェイで H.450 を有効にする必要があります。Unified CM は H.450 をサポートしないため、Unified CM 電話機と Unified CME 電話機間で付加サービスが必要な場合、ビデオ コールは音声専用コールに戻ります。
- 電話会議は音声専用に戻ります。
- ビデオ トラフィックが WAN を通過するには、WAN 帯域幅は 384 kbps の最小ビデオ ビットレートを満たす必要があります。
- ビデオの基本的なコールは SCCP 電話機でのみサポートされ、SIP 電話機ではサポートされません。

ISDN 経由の H.320 ビデオ

ISDN 経由で H.320 ビデオ機能を実装する場合は、次の設計上の考慮事項に従ってください。

- PRI または BRI インターフェイス経由で H.320 エンドポイントに直接接続する場合、Unified CME および Cisco IOS ルータは現在、128 kbps のビデオ コールのみをサポートしています。
- Unified CME および PSTN ゲートウェイで H.320 を有効にして、Unified CM と相互作用するようにするには、音声専用コールと区別するために、ビデオ コールには別個のダイヤル ピアを使用します。Unified CME の **voice-port** 設定で **bear-cap speech** を設定します。
- H.320 は付加サービスをサポートしません。

H.323 経由での Unified CM と Unified CME の相互運用性に関する設計上の一般的な考慮事項

- H.450.12 を使用して Unified CM を自動検出するように Unified CME を設定し、Unified CM 電話機と Unified CME 電話機間のコールをヘアピンします。
- SCCP-to-SCCP コールまたは SCCP-to-SIP コールの場合は、H.323 トランクを Unified CM と Unified CME との間に配置できます。
- TLS を使用するセキュア シグナリングには、Unified CME 4.0 以降のリリースを配置しますが、SRTP 経由でのセキュア メディアには、Unified CME 4.2 以降のリリースを配置します。ただし、会議はセキュアでなく、Unified CM 電話機と Unified CME 電話機間のセキュアな相互運用性もサポートされていません。
- H.320 のサポートによって ISDN 経由で音声、ビデオ、およびデータ転送を統合するには、Unified CME 4.1 以降のリリースを配置します。

- ビデオを配置するのは SCCP 電話機用（基本的なコールのサポートを使用）で、SIP 電話機用ではありません。
- MTP 機能はビデオと互換性がありません。ビデオ コールを機能させるには、MTP 機能を無効（オフ）にする必要があります。
- Unified CM と Unified CME 間の IP 接続が正常に機能することを確認します。
- Unified CME の各ローカル ゾーンと Unified CM のロケーション（ローカル SCCP）で、ローカル ビデオのセットアップが正常に機能することを確認します。
- 既存の音声ダイヤル プランのインフラストラクチャを使用します。
- ビデオ トラフィック シェーピングの場合は、次のガイドラインに従ってください。
  - CoS 4 を使用するビデオ コールのビデオ チャネルと音声チャネルが、リップシンクを維持し、ビデオと音声専用コールを区別するようにします。
  - 音声トラフィックとビデオ トラフィックを異なるキューに配置します。
  - 音声トラフィックとビデオ トラフィックに Priority Queuing（PQ; プライオリティ キューイング）を使用します。音声専用コールとビデオ（音声ストリーム + ビデオ ストリーム）コールには、分類に基づいて 2 つの異なるポリシーが必要です。ビデオ コールの音声ストリームには、ビデオ コールのビデオ ストリームと同じマークが付けられているため、ビデオ コールの音声コールは保護されています。
- ビデオは、帯域幅が 768 kbps 未満のリンクには配置しないでください。
- リンク速度が 768 kbps 以上で、オーバーサブスクリプションを防止する適切なコール アドミッション制御を使用している場合は、PQ にビデオ トラフィックを配置しても、音声パケットの遅延が大幅に改善されることはありません。
- スピードが 768 kbps 以上の場合はフラグメンテーションを設定する必要はありません。
- ビデオ パケットには cRTP は推奨しません（ビデオ パケットは大きいため、cRTP はビデオには役立ちません）。
- 音声トラフィックとビデオ トラフィックがリンク容量に占める割合が 33% を超えないようにします。
- ビデオ帯域幅を計算する場合、オーバーヘッドを考慮して、コールの合計ビデオ データ レートに 20% を加算します。

H.323 経由で Unified CME を Unified CM に統合する方法の詳細については、次の Web サイトで入手可能な『*Cisco Unified CME Solution Reference Network Design Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_implementation_design_guides_list.html

設定例

次の例は、この項で説明した設計上の考慮事項とベスト プラクティスの一部を示しています。

例 8-12　Cisco Unified Border Element の設定

```
voice service voip
    allow-connections h323 to h323
    supplementary-service h450.2
    supplementary-service h450.3
    supplementary-service h450.12
    h323
        emptycapability
    h225 id-passthru
    h225 connect-passthru
h245 passthru tcsnonstd-passthru
interface Loopback0
```

```
    ip address 2.1.1.1 255.255.255.0
    h323-gateway voip interface
h323-gateway voip id BORDERGW-zone ipaddr 1.1.1.1 1719
    h323-gateway voip h323-id BORDERGW
    h323-gateway voip bind srcaddr 2.1.1.1
dial-peer voice 1 voip        /* To Unified CM endpoints */
    destination-pattern 4...
    session target ras
    dtmf-relay h245-alphanumeric
    codec g729r8
    no vad
dial-peer voice 1 voip        /* To Unified CME endpoints */
    destination-pattern 3....
    session target ras
    dtmf-relay h245-alphanumeric
    codec g729r8
    no vad
```

例 8-13　H.323 を使用する Cisco Unified CME の設定

```
voice service voip
    h323
interface Loopback0
    ip address 3.1.1.1 255.255.255.0
    h323-gateway voip interface
    h323-gateway voip id CME-zone ipaddr 1.1.1.1 1719
    h323-gateway voip h323-id CME
    h323-gateway voip bind srcaddr 3.1.1.1
dial-peer voice 1 voip       /* To Unified CM endpoints */
    destination-pattern 4...
    session target ras
    session transport tcp
    codec g729r8             /* Voice class can also be used */
    no vad
telephony-service
 ip source-address 3.1.1.1 port 2000
 create cnf-files
 keepalive 45
 max-conferences 8 gain -6
 moh music-on-hold.au
 transfer-system full-blind /* Used with multiple PSTN connections */
 transfer-pattern .T
```

例 8-14　中継ゾーン ゲートキーパーの設定

```
gatekeeper
 zone local CCM-zone customer.com 1.1.1.1 outvia BORDERGW-zone
 zone local CME-zone customer.com outvia BORDERGW-zone
 zone local BORDERGW-zone customer.com
 no zone subnet CCM-zone default enable
 no zone subnet CME-zone default enable
 no zone subnet BORDERGW-zone default enable
 zone subnet CCM-zone 4.1.1.1/32 enable
 zone subnet CME-zone 3.1.1.1/32 enable
 zone subnet BORDERGW-zone 2.1.1.1/32 enable
 zone prefix CCM-zone 4...
 zone prefix CME-zone 3...
 bandwidth interzone zone CCM-zone <bandwidth value>
 bandwidth interzone zone CME-zone <bandwidth value>
 bandwidth interzone zone BORDERGW-zone <bandwidth value>
```

```
 no shutdown
```

例 8-15　Unified CME ビデオの設定

```
voice service voip
  supplementary-service h450.12 advertise-only

 h323
         call start slow
….

telephony-service
 video
       maximum bit-rate <0-10000000>
  load 7970 TERM70.6-0-2-0s
  ip source-address 10.10.10.1 port 2000
 service phone videoCapability 1 !!! Enable Video Capability Service, case sensitive
create cnf-files
….

ephone  1
```

CHAPTER 9

コール アドミッション制御

コール アドミッション制御機能は、すべての IP テレフォニー システム（特に IP WAN 経由で接続された複数のサイトで構成されるシステム）に不可欠なコンポーネントです。コール アドミッション制御の機能と必要性をわかりやすく説明するために、図 9-1 の例について考えます。

図 9-1　　コール アドミッション制御が必要な理由

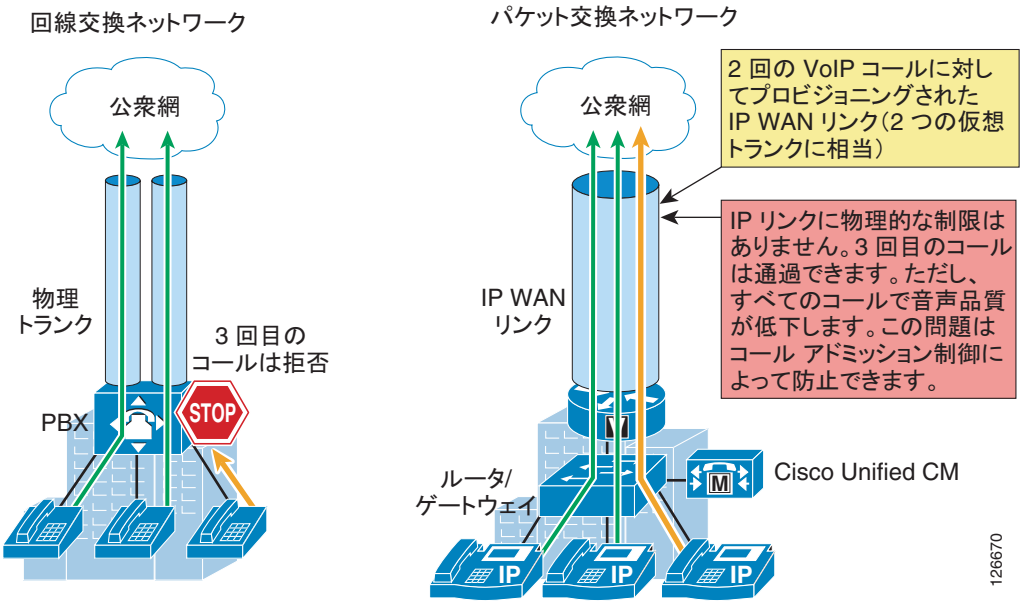


図 9-1 の左側で示すように、従来の TDM ベースの PBX は、回線交換ネットワークの一部として動作します。このネットワークでは、回線はコールがセットアップされるたびに確立されます。このため、レガシー PBX が公衆網または他の PBX に接続されている場合は、一定数の物理トランクを設定する必要があります。公衆網または他の PBX 宛てのコールをセットアップする必要があるとき、PBX は、使用可能なトランクの中からトランクを選択します。使用可能なトランクがない場合、コールは PBX によって拒否され、発信者にはネットワーク ビジー信号が聞こえます。

次に、図 9-1 の右側に示している IP テレフォニー システムについて考えます。このシステムは、パケット交換ネットワーク（IP ネットワーク）を基盤としているため、IP テレフォニー コールをセットアップするために回線を確立する必要はありません。サンプリング音声を含んでいる IP パケットが、他のタイプのデータ パケットとともに、IP ネットワーク経由でルーティングされるだけです。音声パケットは、QoS（Quality Of Service）を使用してデータ パケットと区別されますが、帯域幅リソースは、特に IP WAN リンクでは無限ではありません。このため、ネットワークの管理者が、一定量の「優先」帯域幅を各 IP WAN リンク上の音声トラフィック専用として割り当ててください。ただし、設定した帯域幅がすべて使用される状態になった場合は、IP テレフォニー システムで以後のコールを拒

否して、IP WAN リンク上のプライオリティ キューのオーバーサブスクリプションを防止する必要があります。オーバーサブスクリプションが発生すると、すべての音声コールで品質が低下します。この機能はコール アドミッション制御と呼ばれ、IP WAN を利用したマルチサイト配置で良好な音声品質を保証するために不可欠なものです。

エンド ユーザ環境の満足度を維持するには、コール アドミッション制御機能を常にコール セットアップ段階で実行する必要があります。このようにすることで、ネットワーク リソースを使用できない場合に、エンド ユーザにメッセージを表示したり、異なるネットワーク（公衆網などの）を通じてコールを再ルーティングしたりすることができるようになります。

この章では、次の主要トピックについて説明します。

- 「コール アドミッション制御の設計上の推奨事項」（P.9-62）

  この項では、この章で説明する原理とメカニズムにすでに精通している読者向けに、コール アドミッション制御に関する主なベスト プラクティス、推奨事項、および注意事項の概要を示します。

- 「コール アドミッション制御の原理」（P.9-3）

  この項では、IP ベースのテレフォニー システムにおけるコール アドミッション制御の 2 つの基本的な方法である、トポロジ対応とトポロジ非対応のコール アドミッション制御について説明します。

- 「コール アドミッション制御の要素」（P.9-12）

  この項では、Cisco Unified Communications システムのさまざまなコンポーネント、たとえば Cisco Unified Communications Manager ロケーション、Cisco IOS ゲートキーパー、RSVP、Cisco Unified Border Element などで使用できるコール アドミッション制御メカニズムについて説明します。

- 「コール アドミッション制御の設計」（P.9-37）

  この項では、上の項で説明したメカニズムを適用し、組み合せる方法について、IP WAN のトポロジ（単純なハブアンドスポーク、2 層ハブアンドスポーク、MPLS、またはその他のトポロジ）に基づいて、および採用する Cisco Unified Communications Manager 配置モデルに基づいて示します。

この章の新規情報

表 9-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 9-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
Cisco RSVP Agent	「Unified CM の RSVP 対応ロケーション」（P.9-18）
Cisco Multiservice IP-to-IP Gateway（IP-IP ゲートウェイ）という名称を Cisco Unified Border Element に変更	「RSVP 機能のある Cisco IOS Gatekeeper および Cisco Unified Border Element」（P.9-29） 「Cisco Unified Border Element による方法」（P.9-60）
Unified CM ロケーションおよびリージョン	「ロケーションおよびリージョンの設定」（P.9-14） 「Unified CM によるロケーションおよびリージョンのサポート」（P.9-15）

コール アドミッション制御の原理

すでに述べたように、コール アドミッション制御は、IP ベースのテレフォニー システムのコール処理エージェントの機能です。したがって理論上は、IP ベースのテレフォニー システムと同じ数のコール アドミッション制御メカニズムが存在する可能性があります。しかし、ほとんどの既存のコール アドミッション制御メカニズムは、次の 2 つの主なカテゴリのいずれかになります。

- トポロジ非対応コール アドミッション制御：コール処理エージェント内の静的設定に基づくもの
- トポロジ対応コール アドミッション制御：使用可能なリソースに関するコール処理エージェントとネットワーク間の通信に基づくもの

以下の項では、トポロジ非対応コール アドミッション制御の原理とその制限について分析し、次にトポロジ対応コール アドミッション制御の原理を示します。

トポロジ非対応コール アドミッション制御

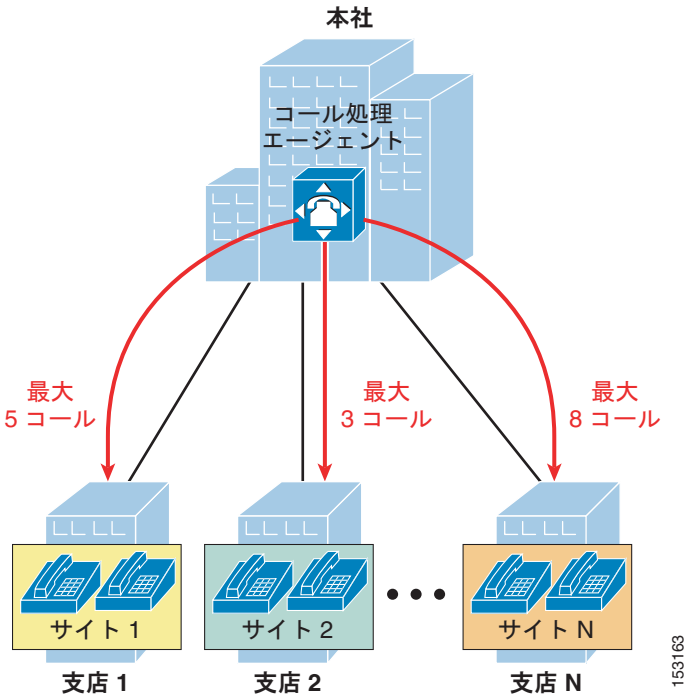
トポロジ非対応コール アドミッション制御とは、IP WAN で接続されたリモート サイトとの間の同時コール数を制限することを目的とし、コール処理エージェントまたは IP ベースの PBX 内の静的設定に基づくメカニズムです。

図 9-2 に示すように、このようなメカニズムのほとんどは、一般に企業 IP WAN に接続される地理上の支店に対応する、論理的な「サイト」エンティティの定義に依存しています。

各支店にあるすべてのデバイスを対応するサイト エンティティに割り当てた後に、管理者がそのサイトを宛先または発信元とするコールの許容最大数（または帯域幅の最大量）を設定するのが一般的です。

新しいコールの確立が必要になるたびに、コール処理エージェントは発信エンドポイントおよび終端エンドポイントが属するサイトをチェックし、（関係する両サイトのコール数または帯域幅の量に関して）コールに利用できるリソースがあるかどうか確認します。チェックが成功した場合、そのコールは確立され、両サイトのカウンタが減少します。チェックに失敗した場合、コール処理エージェントは事前に設定されたポリシーに基づいてコールの処理方法を決定できます。たとえば、発信者のデバイスにネットワーク ビジー信号を送信したり、公衆網接続を通じて再ルーティングを試行します。

図 9-2　トポロジ非対応コール アドミッション制御の原理



トポロジ非対応のコール アドミッション制御メカニズムは静的設定に依存しているため、一般に比較的単純な IP WAN トポロジのネットワークだけに配置できます。実際、このようなメカニズムのほとんどでは、図 9-3 に示すような単純なハブアンドスポーク トポロジまたは単純な MPLS ベースのトポロジ（MPLS サービスがサービス プロバイダーによって提供される場合）が必要です。

図 9-3　トポロジ非対応コール アドミッション制御に適したドメイン

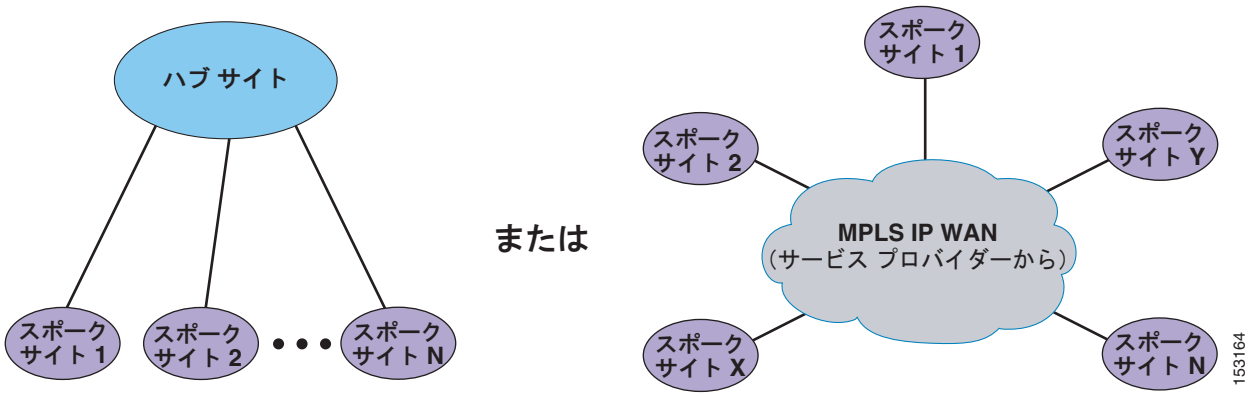


図 9-3 に示すようなハブアンドスポーク ネットワークまたは MPLS ベースのネットワークで、各スポーク サイトはコール処理エージェント内の「サイト」に割り当てられ、その「サイト」のコール数または帯域幅の量は、そのスポークを IP WAN に接続する IP WAN リンク上の音声またはビデオ（あるいはその両方）に利用可能な帯域幅と一致するように設定されます。

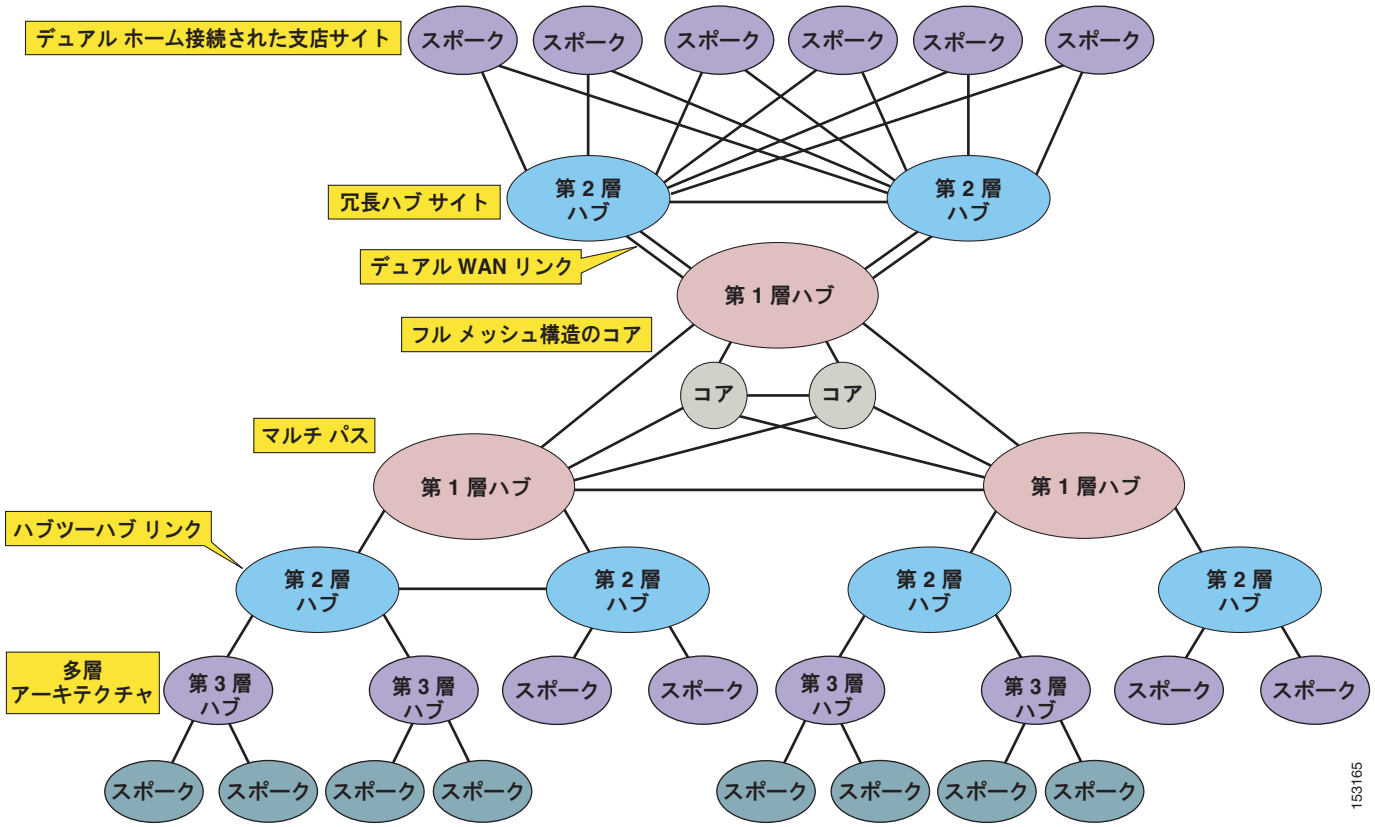
スポーク サイトからハブ サイトへの冗長リンクと、2 つのスポーク サイトを直接接続するリンクがないことに注意してください。次の項では、トポロジ非対応コール アドミッション制御で、このようなリンクが問題を発生させる理由について説明します。

トポロジ非対応コール アドミッション制御の制限

現在の企業ネットワークでは、高可用性は共通の要件であり、そのために IP WAN ネットワーク接続に冗長性が求められることがあります。

代表的な企業ネットワークにおける IP WAN トポロジについて考えると、純粋なハブアンドスポークトポロジの前提を複雑にする数多くの特性があることがわかります。図 9-4 は、このようなネットワーク特性のいくつかを 1 つの図にまとめたものです。すべての特性が一度に現れるのは大規模な企業ネットワークだけですが、多くの IP WAN ネットワークでも最低 1 つの特性が存在していることがよくあります。

図 9-4　代表的な企業ネットワークのトポロジ特性



「コール アドミッション制御の設計」（P.9-37）の項で説明するように、複雑なネットワーク トポロジにトポロジ非対応コール アドミッション制御メカニズムを適用できる場合がありますが、この方法を利用できる場合と、実現できる動作に関して制限があります。たとえば、冗長性がネットワーク要件となっている IP WAN を通じてハブ サイトに接続される支店サイトの単純なケースについて考えます。一般的に、冗長性は次のいずれかの方法で実現できます。

- IP WAN へのプライマリ リンクとバックアップ リンクを備えた 1 台のルータ
- ロード バランシング設定で 2 つのアクティブな WAN リンクを備えた 1 台のルータ
- それぞれが IP WAN に接続され、ロード バランシングされたルーティングを行う 2 つのルータ プラットフォーム

図 9-5 の例では、プライマリ リンクとバックアップ リンクを備えた 1 台のルータの場合と、2 つのアクティブなロード バランシング リンクを備えた 1 台のルータの場合に、トポロジ非対応コール アドミッション制御メカニズムを適用しようとしています（2 つのルータ プラットフォームの場合のコール アドミッション制御に対する影響は、後者の例と同じです）。

図 9-5　デュアル リンクが存在する場合のトポロジ非対応コール アドミッション制御

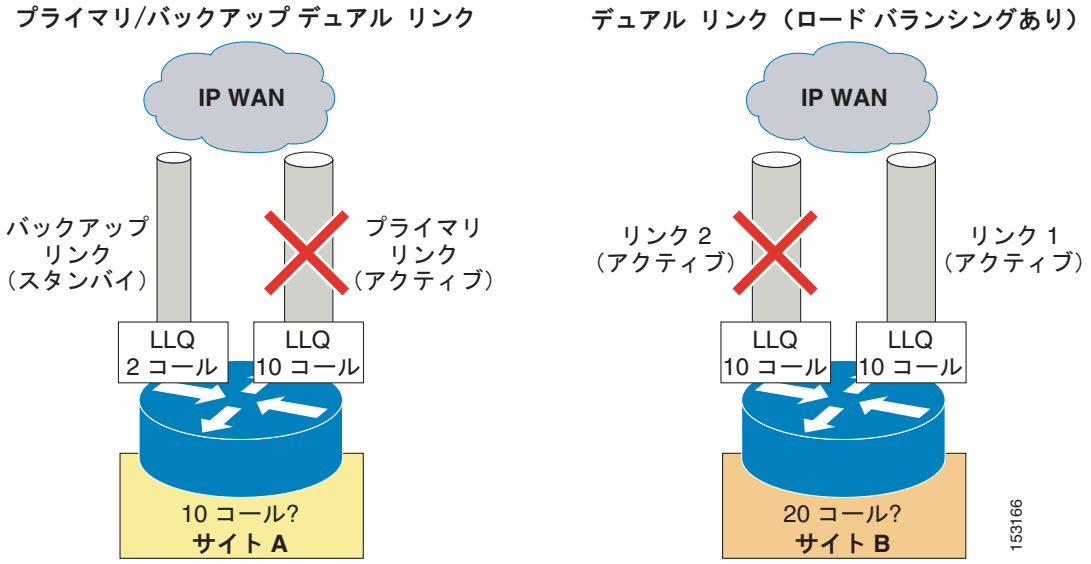


図 9-5 の最初の例で、支店 A は通常、最大 10 の同時コールが可能になるよう、Low Latency Queuing（LLQ; 低遅延キューイング）帯域幅がプロビジョニングされたプライマリ リンクを通じて、IP WAN に接続されます。このプライマリ リンクに障害が発生した場合、小さい方のバックアップ リンクがアクティブになり、IP WAN への接続を維持します。ただし、このバックアップ リンクの LLQ 帯域幅は、最大 2 つの同時コールだけが可能なようにプロビジョニングされています。

この支店にトポロジ非対応コール アドミッション制御メカニズムを配置するには、コール処理エージェントで「サイト」A を定義し、一定のコール数（または帯域幅の量）を設定する必要があります。サイト A の最大値として 10 コールを使用する場合、プライマリ リンクの障害時にバックアップ リンクにオーバーランが発生し、すべてのアクティブなコールで音声の品質が低下する可能性があります。これに対して、最大値を 2 コールにした場合、プライマリ リンクがアクティブなときは、残りの 8 コールに対してプロビジョニングされた帯域幅を使用できません。

次に、IP WAN に接続する 2 つのアクティブなリンクを備えた支店 B について考えます。各リンクは、最大 10 の同時コールが可能なようにプロビジョニングされ、ルーティング プロトコルは各リンク間のロード バランシングを自動的に実行します。この支店にトポロジ非対応コール アドミッション制御メカニズムを配置する場合、コール処理エージェントで「サイト」B を定義し、一定のコール数（または帯域幅の量）を設定する必要があります。支店 A の場合と同様に、2 つのリンクの容量を増強し、サイト B の最大値として 20 コールを使用する場合、一方のリンクの障害時に、もう一方のリンクで LLQ のオーバーランが発生する可能性があります。たとえば、リンク #2 に障害が発生した場合、サイト B を宛先または発信元とする 20 の同時コールが引き続き可能です。これらのコールは、すべてリンク #1 を通じてルーティングされるようになるため、オーバーランが発生し、すべてのコールで音声品質が低下します。これに対して、最大 10 の同時コールでサイト B を設定した場合、（両方のリンクが動作している）通常の条件では、使用可能な LLQ 帯域幅が十分に活用されなくなります。

上記の 2 つの単純な例は、実際の企業ネットワークでの IP WAN 帯域幅のプロビジョニングが非常に複雑で、コール処理エージェント内の静的に設定されたエントリにまとめられない場合があることを示しています。このようなネットワークでトポロジ非対応コール アドミッション制御を配置すると、管理者は推測をしたり、回避策を取ったり、最適ではないネットワーク リソースの使用を許容したりする必要があります。

単純なハブアンドスポークに従わないネットワーク トポロジが存在する場合にコール アドミッション制御を提供する最適な方法は、次の項で説明するようにトポロジ対応コール アドミッション制御を実装することです。

（注）　一部の IP テレフォニー システムは、ネットワークで検知された輻輳に基づくフィードバック メカニズムで、従来のトポロジ非対応コール アドミッション制御を拡張します。これにより、音声品質が低下した場合、コールが強制的に公衆網経由になります。コール処理エージェントはコールの確立後に実行されることと、輻輳が発生している正確な場所を認識しないという理由から、この方法はまだ真のトポロジ対応コール アドミッション制御と同等ではありません。この章の最初に述べたように、効果的に運用するには、コールをセットアップする前にコール アドミッション制御を実行する必要があります。

トポロジ対応コール アドミッション制御

トポロジ対応コール アドミッション制御とは、IP WAN リンクを通じた同時コール数を制限することを目的とするメカニズムであり、任意のネットワーク トポロジに適用でき、またトポロジの変更にも動的に適応できます。

このような目的を達成するには、トポロジ対応コール アドミッション制御は、コール処理エージェント（または IP ベースの PBX）とネットワーク間のネットワーク リソースの可用性に関するリアルタイム通信を利用する必要があります。ネットワークは分散エンティティであるため、リアルタイムの通信にはシグナリング プロトコルが必要です。

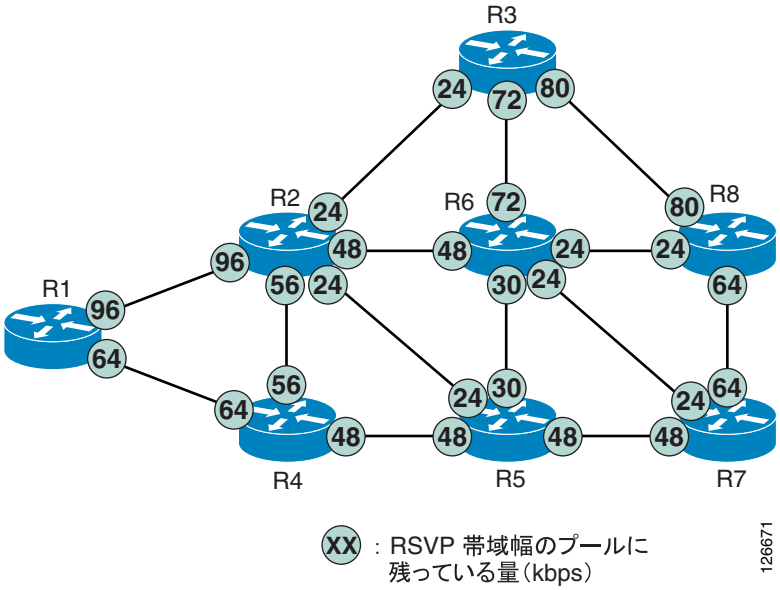
Resource Reservation Protocol（RSVP; リソース予約プロトコル）は、アプリケーションが IP ネットワークを通じて動的に帯域幅を予約できるようにするための、業界初のシグナリングプロトコルです。RSVP を使用すると、アプリケーションはネットワークを通じたデータ フロー（音声コールなど）のために一定の帯域幅を要求し、実際のリソースの可用性に基づいて予約結果の通知を受け取ることができます。

音声コールまたはビデオ コールのためのコール アドミッション制御の特定のケースで、IP ベースの PBX は、2 つのリモート サイト間でコール セットアップ プロセスを RSVP 予約と同期し、予約の結果に基づいてルーティングの決定を行います。分散型ネットワークに対応し、動的に機能する性質を持っているため、RSVP はあらゆるネットワーク トポロジにわたって帯域幅を予約できます。つまり、本格的なトポロジ対応コール アドミッション制御メカニズムを提供します。

RSVP がネットワークで帯域幅予約を実行する方法の基本的な原理を理解するために、図 9-6 に示す簡単な例について考えます。この例では、メッセージ交換とプロトコルの動作自体については説明しません。機能によってもたらされる結果を中心に説明します。RSVP メッセージ交換の詳細については、「RSVP の原理」（P.3-47）を参照してください。

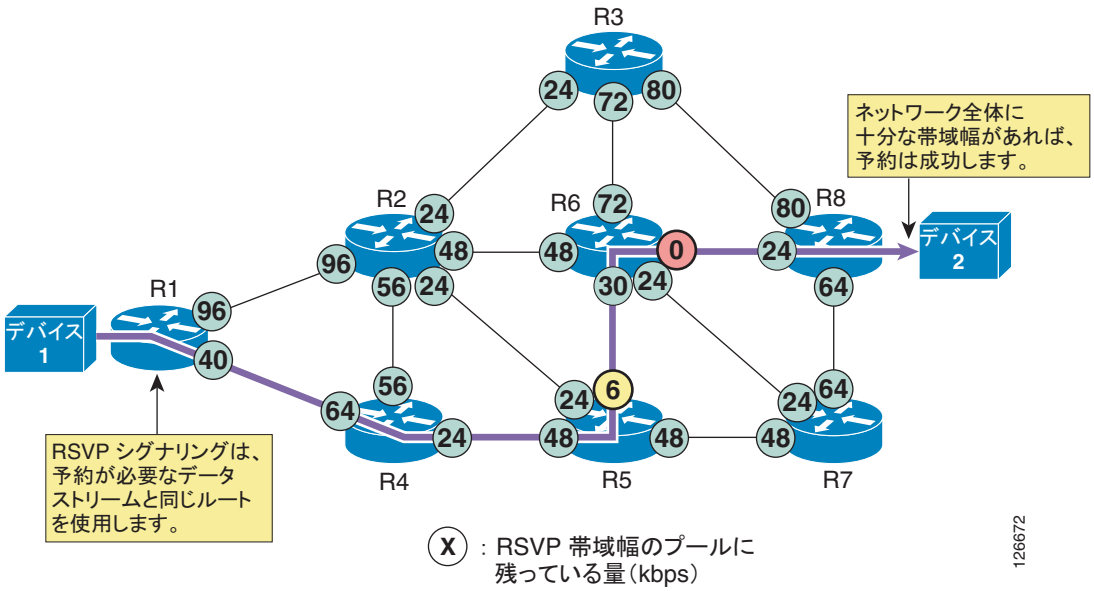
図 9-6 に示すネットワークの各ルータ インターフェイスで、RSVP が有効になっているとします。円で囲まれた数値は、各インターフェイス上に残っている使用可能な RSVP 帯域幅の量を表しています。

図 9-6　RSVP の原理を示すためのサンプル ネットワーク



ここで、RSVP 対応のアプリケーションが、2 つのデバイス間でのデータ ストリーム用に一定の帯域幅を予約するとします。このシナリオを図 9-7 に示します。この図では、デバイス 1 からデバイス 2 への個々のデータ ストリームで、24 Kbps の帯域幅を要求することを示しています。

図 9-7　予約が成功する RSVP シグナリング

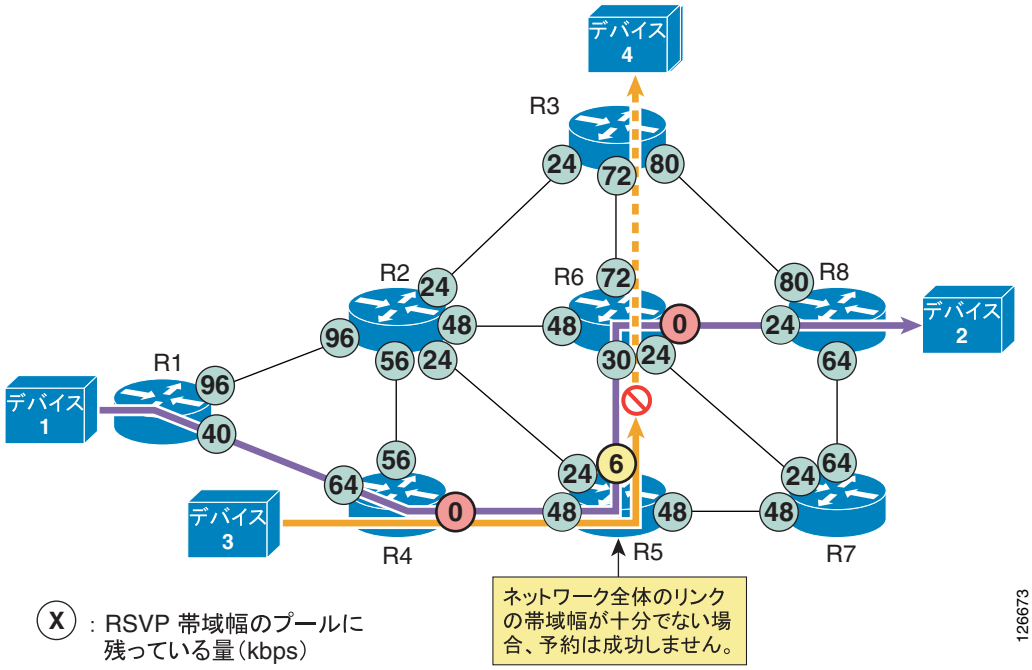


ここでは、図 9-7 について説明します。

- RSVP は、自身ではルーティングを実行しません。代わりに、下位レイヤで機能しているルーティング プロトコルを使用して、予約要求の宛先を決定します。トポロジの変更に対応するためにルーティングのパスが変化すると、RSVP は、自身の予約を予約が存在する新しいパスに合せて調整します。
- RSVP プロトコルは、デバイス 1 からデバイス 2 へのパスにあるすべての RSVP 対応ルータ上で、使用可能な帯域幅リソースを確認することによって、エンドツーエンドの予約を確立しようとします。図 9-7 に示すように、RSVP メッセージがネットワークを進んでいくとき、発信側ルータ インターフェイスでは、使用可能な RSVP 帯域幅が 24 Kbps ずつ減分されます。
- 使用可能な帯域幅がすべての発信側インターフェイスで十分にあり、この新しいデータ ストリームを受け付けることができる場合は、予約が成功し、アプリケーションに通知されます。
- RSVP 予約は単方向です。この例では、予約はデバイス 1 からデバイス 2 に向かって確立され、逆方向については確立されません。音声会議やビデオ会議などの双方向アプリケーションがある場合は、各方向について 1 つずつ、2 つの予約を確立する必要があります。
- RSVP は、RSVP をサポートしないルータ ノードでは透過的に動作します。RSVP に対応しないルータがパスに存在していても、それらのルータは単に RSVP メッセージを無視して、他の IP パケットと同様に渡すだけであり、予約を確立することは可能です（プロトコルのメッセージと動作の詳細については、「RSVP の原理」（P.3-47）を参照してください）。ただし、エンドツーエンドでの QoS を確保するには、この RSVP 非対応のルータが制御するリンク上で、帯域幅の輻輳が発生しないようにする必要があります。

デバイス 1 とデバイス 2 の間で予約が正常に確立された後に、別のアプリケーションがデバイス 3 とデバイス 4 の間で 24 Kbps の予約を要求したとします（図 9-8 を参照）。

図 9-8　予約が成功しない RSVP シグナリング



ここでは、図 9-8 について説明します。

- RSVP プロトコルは、デバイス 3 からデバイス 4 へのパスにあるすべての RSVP 対応ルータ上で、使用可能な帯域幅リソースを確認することによって、エンドツーエンドの予約を確立しようとします。図 9-8 に示すように、RSVP メッセージがネットワークを進んでいくとき、発信側ルータ インターフェイスでは、使用可能な RSVP 帯域幅が 24 Kbps ずつ減分されます。
- この例では、R6 に対する R5 の発信側インターフェイス上に、この新しいデータ ストリームを受け付けるための使用可能な帯域幅が十分にありません。このため、予約は失敗し、アプリケーションに通知されます。パスに含まれている各発信側インターフェイス上の使用可能な RSVP 帯域幅は、以前の値に戻されます。
- 次にどのように処理するかは、アプリケーションが決定します。データの転送を放棄することも、何らかの方法で QoS 保証のないベストエフォート型トラフィックとして送信することもできます。

ここで、前の項で紹介した二重接続される支店 A および B の例に、RSVP に基づくトポロジ対応コール アドミッション制御方法を適用できます。

図 9-9 に示すように、支店 A には 10 コール用にプロビジョニングされた LLQ を備えるプライマリ リンクと、2 つのコールだけを許容するバックアップ リンクがあります。この方法で RSVP は、RSVP 帯域幅が LLQ 帯域幅と一致するように、両方のルータ インターフェイスで設定されます。支店 A は、他の支店を宛先または発信元とするすべてのコールの RSVP 予約を要求するために、コール処理エージェント内でも設定されます。これで、コールは、ルーティング プロトコルによって決定されるパスに自動的に従う RSVP 予約の結果に基づいて、許可または拒否されるようになります。通常の条件下では（プライマリ リンクがアクティブな場合）、最大 10 コールが許容されます。プライマリ リンクの障害時には、最大 2 コールだけが許容されます。

ポリシーは、一般にコール アドミッション制御に障害が発生した場合の動作を決定するために、コール処理エージェント内で設定できます。たとえば、コールを拒否したり、公衆網を通じて再ルーティングしたり、異なる DSCP マーキングでのベストエフォート コールとして IP WAN を通じて送信したりすることができます。

図 9-9　　デュアル リンクのトポロジ対応コール アドミッション制御

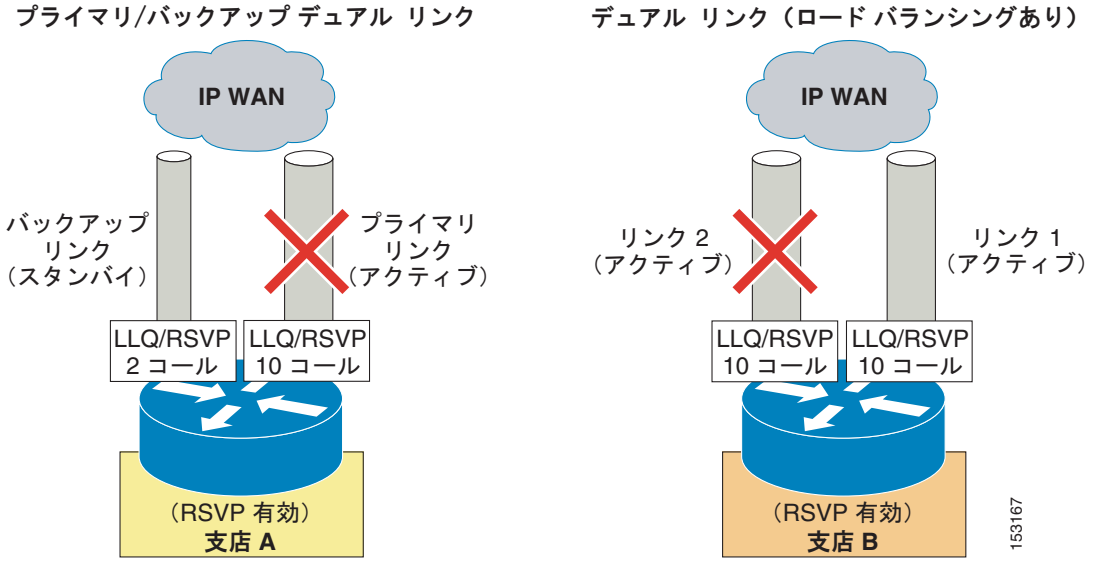


図 9-9 の右側に示すように、2 つのロード バランシング リンクを通じて IP WAN に接続される支店 B にも、同様の考慮事項が該当します。RSVP は、LLQ 設定と一致する帯域幅の値（この場合は、10 コールに対して十分な帯域幅）で、2 つのルータ インターフェイスのそれぞれで有効になります。支店 B は、他の支店との間のコール用に RSVP 予約を要求するため、コール処理エージェント内でも設定

されます。このときも、コールはルーティング プロトコルが決定するパスに沿って、使用可能な実際の帯域幅に基づいて許可または拒否されるようになります。したがって、2 つのリンクを通じた完全に均等なロード バランシングの場合、（両方のリンクが動作している）通常の条件下で最大 20 コールを許容できます。2 つのリンクのいずれかに障害が発生した場合は、最大 10 コールだけが許容されます。

10 を超えるコールがアクティブなときに 2 つのリンクのいずれかに障害が発生した場合、一部のコールは新しいパスでの予約の再確立に失敗します。この時点で、コール処理エージェントは通知を受け、設定されたポリシーに基づいて対応することができます（追加のコールをドロップしたり、ベストエフォート コールとして再マーキングします）。

要するに、トポロジ対応コール アドミッション制御によって、管理者は任意のネットワーク トポロジでコール品質を保護し、トポロジの変更に自動的に適応し、すべての状況の下でネットワーク リソースを最適に使用することができます。

MPLS ネットワークの特別な考慮事項

コール アドミッション制御の点から見ると、ネットワークの「ハブ」での RSVP のサポートに関して、MPLS に基づくネットワークは従来のレイヤ 2 WAN サービスに基づくネットワークとは異なっています。従来のレイヤ 2 WAN は、ほとんどの場合、RSVP への参加を有効にできる企業管理のルータから構成されます。MPLS ネットワークではネットワーク全体（クラウド）が「ハブ サイト」であるため、RSVP を有効にするための企業管理のハブ ロケーションは存在しません（詳細については、「単純な MPLS トポロジ」（P.9-45）を参照してください）。したがって、MPLS 環境でトポロジ対応コール アドミッション制御を提供するには、RSVP のサポート用にネットワークの Customer Edge（CE）デバイスを設定する必要があります。

RSVP は CE で有効にする必要があるため、この機器の制御は重要です。この機器が企業で管理されていない場合、サービス プロバイダーに問い合せて、WAN インターフェイスで RSVP が有効になっているかどうか、およびその実装で RSVP アプリケーション ID などの高度な機能がサポートされるかどうかを確認する必要があります。

RSVP メッセージは、RSVP 非対応 MPLS クラウドを透過的に通過するため、エンドツーエンドの RSVP 機能で問題は生じません。CE の WAN インターフェイスで RSVP を設定すると、そのプライオリティ キューにオーバーランが発生しなくなります。RSVP 予約は単方向であるため、RSVP が MPLS クラウドで有効になっていない場合、Provider Edge（PE）ルータでプライオリティ キューを保護するには、次の規則に従う必要があります。

- メディア ストリームを両方向で同じサイズにする。
- メディアを対称的にルーティングする。

RSVP PATH メッセージは、通過する RSVP 対応ルータの出口 IP アドレスを記録します。PATH メッセージの情報は、RSVP RESV メッセージを同じルートで返信するために使用されます。このメカニズムのため、CE と PE 間の WAN リンクにルーティング可能な IP アドレスがないと、RSVP 予約は失敗します。

MPLS ネットワークがこれらの規則に従っていない場合は、RSVP を実装する前にシスコのアカウント チームにお問い合せください。

コール アドミッション制御の要素

Cisco Unified Communications システムには、コール アドミッション制御機能を実行する複数のメカニズムがあります。この項では、次のカテゴリに従って、すべてのメカニズムの設計と設定のガイドラインについて説明します。

- トポロジ非対応メカニズム
  - 「Unified CM の静的ロケーション」（P.9-12）
  - 「Cisco IOS ゲートキーパー ゾーン」（P.9-16）
- トポロジ対応メカニズム
  - 「Unified CM の RSVP 対応ロケーション」（P.9-18）
  - 「RSVP 機能のある Cisco IOS Gatekeeper および Cisco Unified Border Element」（P.9-29）

（注）　Cisco Unified CM 5.0 では、以前のリリースですでに存在していた*ロケーション*の概念を拡張することによって、トポロジ対応コール アドミッション制御が導入されています。したがって、このマニュアルでは以前のトポロジ非対応メカニズムを*静的ロケーション*と呼び、新しいトポロジ対応メカニズムを *RSVP 対応ロケーション*と呼ぶことにします。

Unified CM の静的ロケーション

Unified CM では、集中型コール処理配置において、コール アドミッション制御を実装するために、*静的ロケーション*と呼ばれている単純なメカニズムを取り入れています。Unified CM でデバイスを設定するときは、そのデバイスをロケーションに割り当てることができます。各ロケーションとの間のコールに対しては、特定の帯域幅が割り当てられます。Unified CM で設定するロケーションは、仮想ロケーションであり、実際の物理ロケーションではありません。Unified CM は、デバイスの物理的なロケーションを認識しません。このため、デバイスをある物理ロケーションから別のロケーションに移動する場合は、システム管理者がロケーション設定を手動でアップデートして、Unified CM がそのデバイスの帯域幅割り当てを正しく計算できるようにする必要があります。各デバイスは、デフォルトでは Hub_None ロケーションに配置されます。ロケーション Hub_None は、デフォルトで設定される特別なロケーションで、無制限の音声およびビデオの帯域幅が割り当てられます。ロケーション Hub_None は削除できません。支店ロケーションにあるデバイスが Hub_None ロケーションに設定されている場合、その支店デバイスが宛先または発信元となっている電話コールはすべて、コール アドミッション制御の対象となりません。

Unified CM では、各ロケーションに対して音声およびビデオの帯域幅プールを定義できます。ロケーションの音声帯域幅とビデオ帯域幅が **Unlimited** に設定されている場合、そのロケーションでは帯域幅を無限に使用できるため、そのロケーションが宛先または発信元となる音声コールとビデオ コールは、Unified CM ではすべて許可されます。帯域幅の値が有限のキロビット / 秒（Kbps）に設定されている場合は、アクティブになっているすべてのコールで使用されている合計帯域幅が、その設定値以下になっている場合に限り、Unified CM は、そのロケーションで入出力されるコールを許可します。ロケーションのビデオ帯域幅を **None** に設定した場合、このロケーションが宛先または発信元となるすべてのビデオ コールは拒否されます。ただし、このロケーションの内部でやり取りされるビデオ コールには影響しません。

ビデオ コールの場合、ビデオ ロケーションの帯域幅については、コールのビデオ部分と音声部分の両方を考慮に入れる必要があります。したがって、ビデオ コールの場合、帯域幅が音声帯域幅プールから差し引かれることは一切ありません。

ロケーションでメンバーシップを指定できるデバイスには、次のものがあります。

- IP Phone
- CTI ポート
- H.323 クライアント
- CTI ルート ポイント
- カンファレンス ブリッジ
- Music On Hold（MoH）サーバ
- ゲートウェイ
- トランク

静的ロケーションのコール アドミッション制御メカニズムでは、通話中のコール タイプ変更も考慮に入れる必要があります。たとえば、サイト間でビデオ コールを確立する場合、Unified CM は、それぞれのロケーションから適切なビデオ帯域幅を差し引きます。このビデオ コールが、ビデオ非対応のデバイスに転送する過程で音声専用コールに変更された場合、Unified CM は割り当てた帯域幅をビデオ プールに戻し、適切な帯域幅を音声プールから割り当てます。音声からビデオに変更されるコールについては、これとは逆の帯域幅割り当て変更が発生します。

表 9-2 に、さまざまなコールのタイプ（ビットレート）において静的ロケーション アルゴリズムが要求する帯域幅を示します。音声コールでは、Unified CM は、メディア ビット レートにレイヤ 3 オーバーヘッドを加えて計算します。たとえば、G.711 音声コールは、ロケーションの音声帯域幅プールから割り当てられた 80 kbps を消費します。ビデオ コールでは、Unified CM は、音声ストリームとビデオ ストリームの両方に対して、メディア ビット レートだけを計算します。たとえば、384 kbps の速度のビデオ コールに対して、Unified CM はビデオ帯域幅プールから 384 kbps を割り当てます。

表 9-2　静的ロケーション アルゴリズムが要求する帯域幅

コールのビットレート	静的ロケーションの帯域幅の値
G.711 音声コール（64 Kbps）	80 kbps
G.729 音声コール（8 Kbps）	24 kbps
128 Kbps ビデオ コール	128 kbps
384 Kbps ビデオ コール	384 kbps
512 Kbps ビデオ コール	512 kbps
768 Kbps ビデオ コール	768 kbps

コーデックおよび静的ロケーションの帯域幅値の全リストについては、次の Web サイトで入手可能な『*Cisco Unified Communications Manager System Guide*』の「*Call Admission Control*」の項で、帯域幅計算の情報を参照してください。

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

たとえば、使用可能な音声帯域幅 256 Kbps およびビデオ帯域幅 384 Kbps を指定した、支店 1 のロケーションの設定があるとします。この場合、支店 1 は最高 3 つの G.711 音声コール（コールごとに 80 Kbps）、または 10 個の G.729 音声コール（コールごとに 24 Kbps）、または両方のコールの組み合せ（256 Kbps を超えないこと）をサポートできます。このロケーションでは、使用されているビデオ コーデックおよび音声コーデックに応じて、さまざまな数のビデオ コールをサポートすることもできます（たとえば、384 kbps の帯域幅を要求する 1 つのビデオ コール、またはそれぞれ 128 kbps の帯域幅を要求する 3 つのビデオ コールをサポートできます）。

（注） コール アドミッション制御は、同じロケーション内のデバイス間のコールには適用されません。

あるロケーションから他のロケーションにコールが発信されると、Unified CM は、両方のロケーションから適切な帯域幅を差し引きます。たとえば、2 つのロケーション間の G.729 コールによって、Unified CM は、両方のロケーションで使用可能な帯域幅から 24 kbps を差し引きます。コールが完了すると、Unified CM は、帯域幅を差し引かれたロケーションに帯域幅を戻します。いずれかの支店ロケーションで十分な帯域幅がない場合、コールは Unified CM によって拒否され、発信者はネットワーク ビジー トーンを受け取ります。発信側デバイスが、ディスプレイを備えた IP Phone である場合、そのデバイスには、「Not Enough Bandwidth」というメッセージも表示されます。

サイト間コールがコール アドミッション制御によって拒否された場合、Unified CM は Automated Alternate Routing（AAR）機能を使用して、公衆網接続を通じて宛先にコールを自動的に再ルーティングできます。AAR 機能の詳細については、「Automated Alternate Routing」（P.10-87）を参照してください。

（注）　AAR が呼び出されるのは、帯域幅が不足しているために、ロケーション ベースのコール アドミッション制御によってコールが拒否される場合だけです。IP WAN が使用不可の場合や、接続に関するその他の問題によって着信側デバイスが Unified CM に登録されない状態になった場合には、AAR は呼び出されません。このような場合、コールは着信側デバイスの Call Forward No Answer フィールドで指定されている宛先に転送されます。

ロケーションおよびリージョンの設定

ロケーションとリージョンを組み合せて設定することで、ネットワーク リンクの特性を定義します。リージョンでは、リンクで使用する圧縮のタイプまたはビット レート（8 kbps や G.729、64 kbps や G.722/G.711 など）を定義し、ロケーションでは、リンクに使用できる帯域幅の量を定義します。システム内の各デバイスを、（デバイス プールによる）リージョンおよび（デバイス プールまたはデバイス自体での直接設定による）ロケーションの両方に割り当てます。

Unified CM では、*ロケーション*を設定することにより、次の要素を定義できます。

- 物理的なロケーション（支店など）。
- WAN 内のロケーションとの間でやり取りされる音声コールおよび FAX コールに利用できる帯域幅。Unified CM では、ロケーションベースのコール アドミッション制御にこの帯域幅値が使用されます。
- WAN 内のロケーションとの間でやり取りされるコールに利用できるビデオ帯域幅。Unified CM では、ロケーションベースのコール アドミッション制御にこの帯域幅値が使用されます。
- ロケーション間の RSVP コール アドミッション制御の設定（可能な設定は、[No Reservation]、[Optional]、[Optional (Video Desired)]、[Mandatory]、および [Mandatory (Video Desired)] です）。

Unified CM では、*リージョン*を設定することにより、次の要素を定義できます。

- リージョン内コールに使用される音声コーデック。
- リージョン間コールに使用される音声コーデック。
- リージョン内コールとリージョン間コールに使用されるコールごとのビデオ帯域幅。
- リージョン間コールのリンク損失タイプ（可能なリンク損失タイプは [Low Loss] および [Lossy] です）。

Unified CM によるロケーションおよびリージョンのサポート

Cisco Unified Communications Manager 7.1(2) 以降のリリースでは、Cisco MCS-7845 サーバを使用した場合で 2000 のロケーションと 2000 のリージョンがサポートされます。最大 2000 のロケーションおよびリージョンを展開するには、[Clusterwide Parameters] > [System] > [Location and Region] および [Clusterwide Parameters] > [System] > [RSVP] の設定メニューで次のサービス パラメータを設定する必要があります。

- [Intraregion Audio Codec Default]
- [Interregion Audio Codec Default]
- [Intraregion Video Call Bandwidth Default]
- [Interregion Video Call Bandwidth Default]
- [Default inter-location RSVP Policy]

リージョンを追加する際は、[Audio Codec] および [Video Call Bandwidth] の値に [Use System Default] を設定します。RSVP コール アドミッション制御を使用している場合は、[RSVP Setting] パラメータにも [Use System Default] を選択します。

個々のリージョンおよびロケーションについてこれらの値をデフォルトから変更すると、サーバの初期化とパブリッシャのアップグレードにかかる時間に影響します。合計 2000 のリージョンと 2000 のロケーションを使用する場合、そのうち最大 200 のリージョンおよびロケーションでデフォルト以外の値を使用するように変更できます。合計 1000 以下のリージョンおよびロケーションを使用する場合、そのうち最大 500 のリージョンおよびロケーションでデフォルト以外の値を使用するように変更できます。表 9-3 は、これらの制限を要約したものです。

表 9-3　デフォルト以外の値を使用できるリージョンおよびロケーションの数

デフォルト以外の値を使用するリージョンおよびロケーションの数	リージョンの最大数	ロケーションの最大数
0 ～ 200	2000	2000
200 ～ 500	1000	1000

（注） 音声コーデック値は、音声コールと FAX コールの両方に使用されます。リージョン間コーデック値として G.729 を使用する場合、FAX コールには T.38 FAX リレーを使用してください。WAN で FAX パススルーを使用する場合は、[Interregion Audio Codec] をデフォルト値から G.711 に変更するか、デフォルト以外のコーデック値 G.711 を使用する各ロケーションに FAX マシンのリージョンを追加します（表 9-3 内の制限に従います）。

（注） 使用している MCS モデルに関係なく、多数のリモート サイトを包含する設計には、Unified CM クラスタのスケーラビリティ（リージョン、ロケーション、ゲートウェイ、メディア リソースなど）に影響する可能性ある相互依存変数が多数存在するため、シスコ代理店またはシスコのシステム エンジニアが常に Cisco Unified Communications Sizing Tool（http://tools.cisco.com/cucst）を使用して、それらの設計をすべて検証する必要があります。Sizing Tool を使用して、設計基準を満たすために必要なサーバまたはクラスタの正確な台数を決定します。

Cisco IOS ゲートキーパー ゾーン

Cisco IOS ゲートキーパーは、Cisco Unified CM、Cisco Unified Communications Manager Express（Unified CME）、レガシー PBX に接続されている H.323 ゲートウェイなどのデバイス間で、コール ルーティングとコール アドミッション制御を提供できます。H.323 Registration Admission Status（RAS）プロトコルを使用してこれらのデバイスと通信し、コールをネットワークにルーティングします。

ゲートキーパーのコール アドミッション制御は、ポリシーベースの方式であり、使用可能なリソースの静的設定を必要とします。ゲートキーパーは、ネットワーク トポロジを認識しないので、単純なハブアンドスポーク トポロジに制限されます。トポロジの詳細な例については、「コール アドミッション制御の設計」（P.9-37）の項を参照してください。

Cisco 2600、3600、3700、2800、3800、および 7200 シリーズのルータはすべて、ゲートキーパー機能をサポートします。冗長性、ロード バランシング、および階層コール ルーティング用に、さまざまな方法で Cisco IOS ゲートキーパーを設定できます。ここでは、ゲートキーパー機能のコール アドミッション制御の面を中心に説明します。冗長性とスケーラビリティに関する考慮事項については、「ゲートキーパーの設計上の考慮事項」（P.8-26）を参照してください。コール ルーティングに関する考慮事項については、「ゲートキーパーを使用する Cisco IOS でのコール ルーティング」（P.10-112）を参照してください。

Cisco IOS ゲートキーパーのコール アドミッション制御機能は、ゲートキーパーの *ゾーン*の概念に基づいています。ゾーンは、エンドポイント、ゲートウェイ、マルチポイント コントロール ユニット（MCU）などの、ゲートキーパーに登録される H.323 デバイスの集合です。アクティブになることができるゲートキーパーは、ゾーンごとに 1 つのみです。1 つのゲートキーパーには、ローカル ゾーンを 100 個まで定義できます。ローカル ゾーンは、当該のゲートキーパーがアクティブに処理しているゾーンです。つまり、このゾーンに割り当てられている H.323 デバイスは、すべて当該ゲートキーパーに登録されます。

複数のゲートキーパーを同一ネットワークに配置している場合、ゾーンがローカル ゾーンとして設定されるのは、1 つのゲートキーパー上のみです。他のゲートキーパーでは、このゾーンはリモート ゾーンとして設定されます。この設定によって、あるゾーンが宛先になっているコールを、そのゾーンを「所有」しているゲートキーパー（つまり、そのゾーンがローカル ゾーンとして設定されているゲートキーパー）に転送するようにゲートキーパーに指示しています。

ゲートキーパーで許可されるコールの数を管理する、つまりコール アドミッション制御機能を利用するには、**bandwidth** コマンドを使用します。このコマンドにはいくつかのオプションがありますが、この機能と密接に関連するのは次のオプションです。

- **interzone** オプションによって、特定のローカル ゾーンで送受信されるすべてのコールの帯域幅の量を制御します。
- **total** オプションによって、特定のローカル ゾーンを宛先または発信元とするすべてのコール、そのローカル ゾーン内のすべてのコールの帯域幅の量を制御します。
- **session** オプションによって、特定のローカル ゾーンのコール 1 件あたりの帯域幅の量を制御します。
- **remote** オプションによって、すべてのリモート ゾーンで送受信される帯域幅の総量を制御します。

すべてのアクティブなコールに対してゲートキーパーによって差し引かれる帯域幅の値は、レイヤ 2、IP、および RTP のオーバーヘッドを除いた、コールのビットレートの倍です。たとえば、64 Kbps を使用する G.711 音声コールは、ゲートキーパーでは 128 Kbps と認識され、384 Kbps のビデオ コールは 768 Kbps と認識されます。表 9-4 に、一般に利用されているいくつかのコールビットレートにおいて、ゲートキーパーが使用する帯域幅の値を示します。

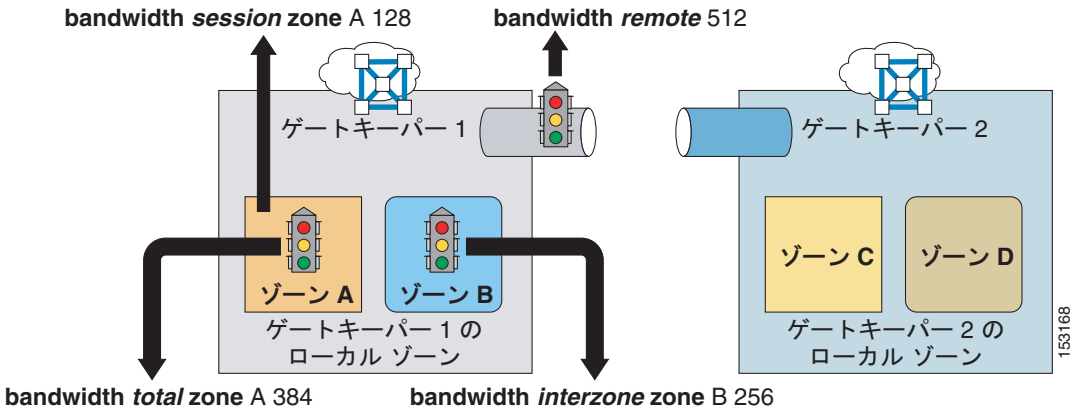
表 9-4　さまざまなコールビットレートにおけるゲートキーパーの帯域幅設定

コールのビットレート	ゲートキーパーの帯域幅の値
G.711 音声コール（64 Kbps）	128 kbps
G.729 音声コール（8 Kbps）	16 kbps
128 Kbps ビデオ コール	256 kbps
384 Kbps ビデオ コール	768 kbps
512 Kbps ビデオ コール	1024 kbps
768 Kbps ビデオ コール	1536 kbps

（注）　コール ARQ（アドミッション要求）に対する帯域幅計算には、RTP ヘッダー圧縮（cRTP）やその他のトランスポートのオーバーヘッドは含まれません。インターフェイス キューのプロビジョニング方法の詳細については、「帯域幅のプロビジョニング」（P.3-59）を参照してください。

実際のネットワークでの **bandwidth** コマンドの利用方法を深く理解するために、図 9-10 に示す例について考えます。

図 9-10　Cisco IOS ゲートキーパーの bandwidth コマンドの例



すべてのコールが G.711 コーデックを使用する音声専用コールであるとすると、図 9-10 に示すコンフィギュレーション コマンドについて、次のことがいえます。

- 1 回のコールに対してゾーン A で任意のデバイスによって要求される帯域幅の最大量は、128 kbps です。つまり、64 kbps よりも高いビットレートのコーデックを使おうとするコールは拒否されます。
- ゾーン A のデバイスに関係するすべてのコール（ゾーン内、またはその他のゾーンとの間）で使用される帯域幅の最大量は、384 kbps です。つまり、ゾーン A のデバイスに関係する最大 3 つのアクティブなコールが存在できます。
- ゾーン B のデバイスとその他のゾーンのデバイス間のすべてのコールによって使用される帯域幅の最大量は、256 kbps です。つまり、ゾーン B のデバイスと、ゾーン A、C、および D のデバイスの間には、最大 2 つのアクティブなコールが存在できます。
- ゲートキーパー GK 1 で登録されたデバイスと、その他のゲートキーパーで登録されたデバイスとの間のすべてのコールで使用される帯域幅の最大量は、512 kbps です。つまり、ゾーン A およびゾーン B のデバイスと、ゾーン C および ゾーン D のデバイスの間には、最大 4 つのアクティブなコールが存在できます。

Unified CM の RSVP 対応ロケーション

Cisco Unified CM Release 5.0 では、リソース予約プロトコル（RSVP）に基づくトポロジ対応コール アドミッション制御メカニズムが導入されました。このプロトコルは、すべてのネットワーク トポロジに適用可能で、従来のハブアンドスポーク トポロジの制限を緩和します。Cisco RSVP Agent は Cisco IOS の機能であり、Unified CM が RSVP ベースのコール アドミッション制御を実行できるようにするものです。Cisco RSVP Agent 機能は、Cisco IOS Release 12.4（6）T で導入され、Cisco 2800 シリーズ、および 3800 シリーズの Integrated Services Routers プラットフォームで使用できます。Cisco RSVP Agent は、Cisco IOS Advanced IP Services Image Release 12.4（15）T5 以上を使用する次のルータ プラットフォームでもサポートされています。

- Cisco 7200 シリーズ ルータ（NPE-G1 または NPE-G2 搭載）
- Cisco 7201 シリーズ ルータ
- Cisco 7301 シリーズ ルータ

Cisco RSVP Agent は、Unified CM で、メディア ターミネーション ポイント（MTP）または RSVP をサポートするトランスコーダ デバイスのいずれかとして登録されます。エンドポイント デバイスが帯域幅の予約を必要としてコールを行う場合、Unified CM は、帯域幅を予約するためのエンドポイントに対するプロキシとして機能する Cisco RSVP Agent を呼び出します。

図 9-11 は、Unified CM とさまざまなその他のデバイス間で使用されるシグナリング プロトコルと、特定のロケーションで WAN を通じたコールのために関連付けられる RTP ストリームを示しています。WAN を通じたすべてのコールで、Unified CM は、ローカル Cisco RSVP Agent にメディア ストリームを送信するようエンドポイント デバイスに指示します。このローカル Cisco RSVP Agent は、リモート ロケーションにある Cisco RSVP Agent への RSVP 予約と同期された別のコール レッグを発信します。図 9-11 は、次のシグナリング プロトコルを示しています。

- Skinny Client Control Protocol（SCCP）による Unified CM への Cisco RSVP Agent の登録
- SCCP または Session Initiation Protocol（SIP）による Unified CM への IP Phone の登録
- Media Gateway Control Protocol（MGCP）、SIP、または H.323 プロトコルによる Unified CM への公衆網ゲートウェイの登録

図 9-11　RSVP をサポートするロケーションのプロトコル フロー

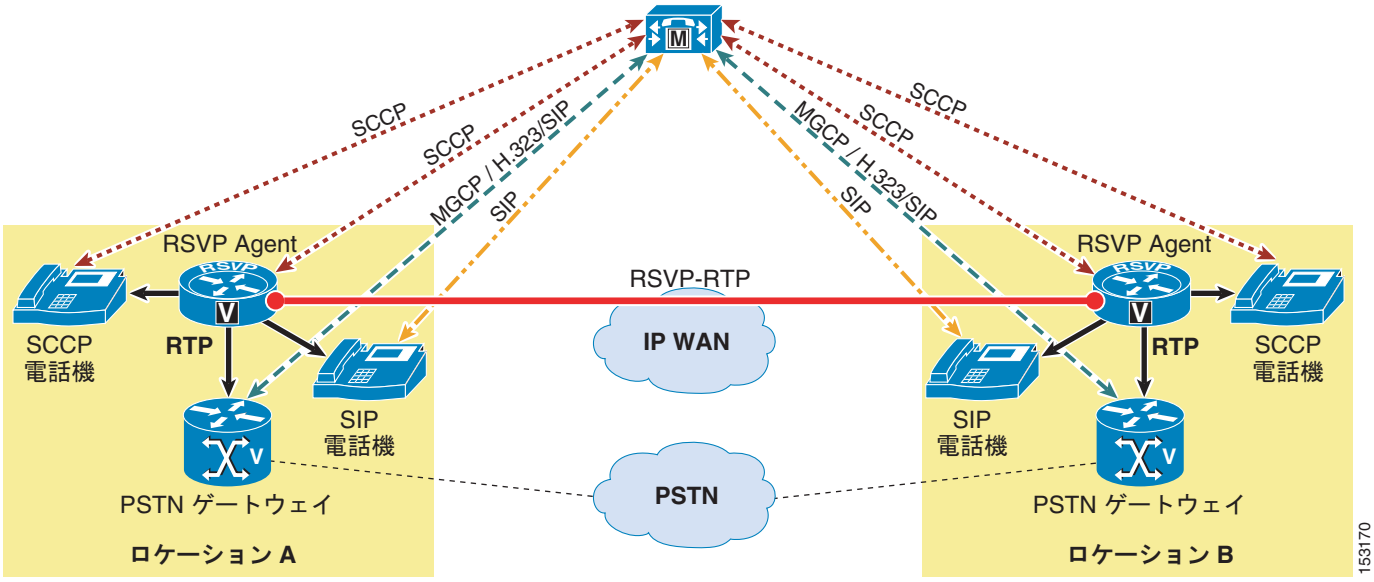
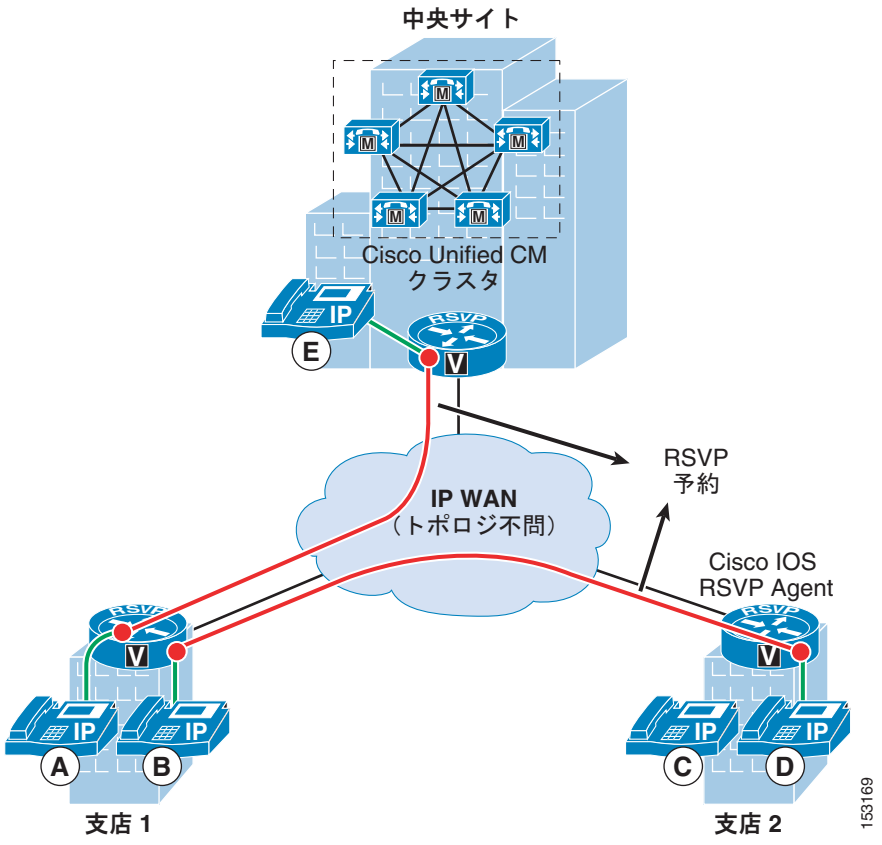


図 9-12 は、Unified CM クラスタ内の代表的な Cisco RSVP Agent 配置を示しています。これには、中央サイト、支店 1、および支店 2 の 3 つのロケーションが含まれます。3 つのロケーションを接続する IP WAN は、任意のトポロジ タイプにすることができ、ハブアンドスポーク トポロジに制限されません。メディア パスで RSVP 予約を必要とする 2 つのロケーション間のコールに対して、Cisco RSVP Agent のペアが、Unified CM から動的に呼び出されます。Cisco RSVP Agent は、Cisco RSVP Agent と同じロケーションにある IP Phone の RSVP 予約を行うためにプロキシとして動作します。たとえば、支店 1 の電話機 A が中央サイトの電話機 E をコールする場合、RSVP 予約が、支店 1 ロケーションと中央サイト ロケーションの Cisco RSVP Agent 間で確立されます（図 9-12 の赤線）。

このコールのメディア ストリームに対しては、3 つのコール レッグがあります。第 1 のコール レッグは電話機 A と支店 1 の Cisco RSVP Agent との間、第 2 のコール レッグは支店 1 と中央サイトの Cisco RSVP Agent との間、第 3 のコール レッグは中央サイトの Cisco RSVP Agent と電話機 E との間です。同様に、支店 1 の電話機 B が、支店 2 の電話機 D をコールした場合、RSVP 予約が支店 1 と支店 2 の Cisco RSVP Agent 間で確立されます。この場合、2 つの支店ロケーション間のコールのメディア ストリームは、中央サイト経由で送信されません。静的ロケーションに基づき、コール アドミッション制御を使用して、従来のハブアンドスポーク トポロジを通じて行われるコールとは異なっています。

（注）　RSVP 対応ロケーションおよび Cisco RSVP Agent を使用すると任意の WAN トポロジがサポートされますが、これらはロケーションに対するデバイスの静的な割り当てに基づいています。つまり、ある物理的なサイトから別のサイトにデバイスを移動するたびに、Unified CM の設定を更新する必要があります。

図 9-12　Cisco RSVP Agent の概念



Cisco RSVP Agent のプロビジョニング

同時コール（セッションとも呼ばれる）に対する Cisco RSVP Agent の容量は、次の要因によって変化します。

- ソフトウェアベースの MTP 機能では、ルータ プラットフォームおよび相対的な CPU 負荷によってセッション容量が決まる（http://www.cisco.com/en/US/products/ps6832/products_data_sheets_list.html で入手可能な『*Cisco RSVP Agent Data Sheet*』を参照）。
- ハードウェアベースの MTP およびトランスコーダの機能では、使用可能な DSP の数によってセッション容量が制限される（DSP のサイジングの考慮事項については、「メディア リソース」（P.6-1）を参照してください）。

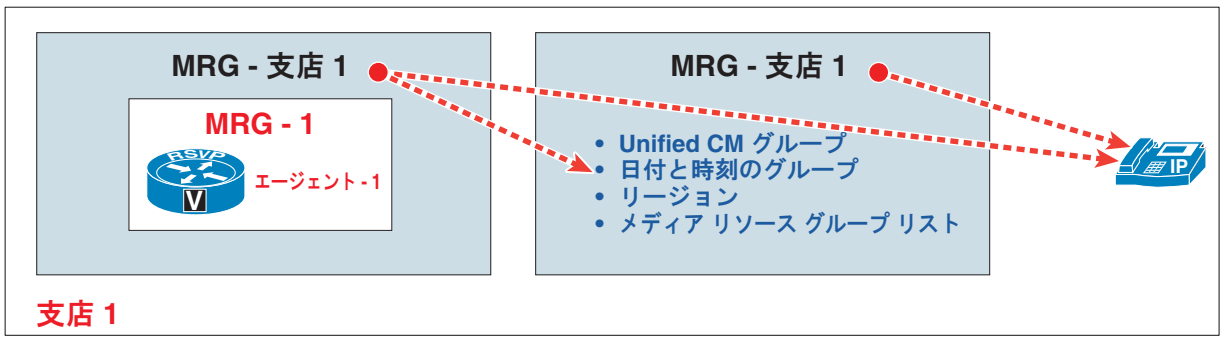
サポートされるプラットフォーム、要件、およびキャパシティの詳細については、次の Web サイトで入手可能な『*Cisco RSVP Agent Data Sheet*』を参照してください。

http://www.cisco.com/en/US/products/ps6832/products_data_sheets_list.html

ソフトウェアベースの MTP 機能に関して、『*Cisco RSVP Agent Data Sheet*』は、Cisco RSVP Agent 専用のルータおよび 75% の CPU 使用率を基準としたセッション容量のガイドラインを示しています。これらの数値は、特定の Cisco IOS リリースに適用されるものであり、大まかなガイドラインと見なす必要があります。特定のサービス、設定、トラフィック パターン、ネットワーク トポロジ、ルーティング テーブル、およびその他の要因の異なる組み合せは、特定の配置のパフォーマンスに著しい影響を与え、サポートされる同時セッション数が減少することがあります。実稼動環境でマルチサービス ルータを配置する前に、慎重に計画および検証試験を行うことをお勧めします。

Cisco RSVP Agent は、デバイス プール、メディア リソース グループ（MRG）、およびメディア リソース グループ リスト（MRGL）の設定の組み合せでエンドポイント デバイスに関連付けることができます。Cisco RSVP Agent は MRG に含めることができ、MRG は MRGL の要素になることができます。MRGL は、直接またはデバイス プールを通じてエンドポイント デバイスに割り当てることができます。図 9-13 に示しているように、MRGL- 支店 1 は、直接または Device Pool-Branch 1 から IP Phone に関連付けることができます。一般に、エンドポイント デバイスがメディア リソースの一意のセットを要求する場合は、エンドポイント デバイス MRGL を直接割り当てます。それ以外の場合は、エンドポイント デバイスが配置されているデバイス プールに MRGL を割り当てます。

図 9-13　　IP Phone への MRGL の割り当て



Unified CM は、MTP、トランスコーダ、会議リソース、および Annunciator など、その他の従来のメディア リソースを割り当てるのと同じ方法で、Cisco RSVP Agent を割り当てます。

他の従来のメディア リソースと同じ MRG で、Cisco RSVP Agent を設定しないようにしてください。設定すると、コールが RSVP に関係しない場合であっても、MTP デバイスを必要とするコールに Cisco RSVP Agent が割り当てられます。

図 9-14 は、Cisco RSVP Agent ロード バランシングが MRG および MRGL 設定によって実装される様子を示しています。同じ MRG 内のすべての Cisco RSVP Agent に対して、Unified CM は、ラウンドロビン方式で Cisco RSVP Agent に対してロード バランシングおよび割り当てを行います。

図 9-14　　Cisco RSVP Agent のロード バランシング

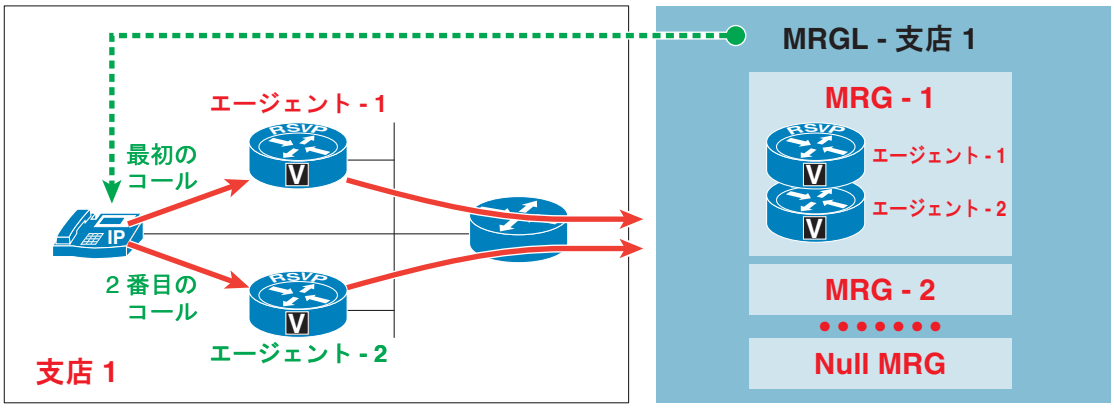


図 9-14 に示すように、MRG-1 の両方の Cisco RSVP Agent が使用可能な場合、最初のコールに対して Agent-1 が選択され、2 番目のコールに対して Agent-2 が選択されます。MRG-1 でいずれの Cisco RSVP Agent も使用できない場合、Unified CM はコールに適した Cisco RSVP Agent が見つかるまで、MRG-2、MRG-3、および残りの MRG の検索を試行します。MRG に明示的に含まれていない Cisco RSVP Agent は、デフォルトで Null MRG に含まれています。Null MRG は常に MRGL 設定の最後の MRG として黙示的に含まれていますが、Unified CM Administration には表示されません。Null MRG の Cisco RSVP Agent は、Unified CM クラスタの任意のエンドポイント デバイスからアクセスできます。したがって、常に MRG で Cisco RSVP Agent を設定することをお勧めします。Unified CM のメディア リソース割り当てプロセスおよび関連するベスト プラクティスの詳細については、「メディア リソース」（P.6-1）を参照してください。

Cisco RSVP Agent の登録

Cisco RSVP Agent は、RSVP をサポートする MTP またはトランスコーダ デバイスとして、Unified CM に登録されます。Cisco RSVP Agent は、MTP デバイスとして登録する場合、トランスコーディング機能をサポートしません。トランスコーディング機能をサポートするには、Cisco RSVP Agent をトランスコーダ デバイスとして Unified CM に登録する必要があります。

登録のスイッチオーバーとスイッチバック

プライマリ Unified CM に障害が発生した場合、Cisco RSVP Agent はセカンダリ Unified CM にスイッチオーバーします。プライマリ Unified CM が障害から回復すると、Cisco RSVP Agent はプライマリ Unified CM に登録をスイッチバックします。Cisco RSVP Agent 登録のスイッチオーバーとスイッチバックを設定するには、次のコマンドを使用します。

```
sccp ccm group
 switchover method immediate
 switchback method guard timeout 7200
!
gateway
  timer receive-rtp 180
```

- **switchover method immediate** は、プライマリ Unified CM サーバの障害が検出されたら、すぐにセカンダリ Unified CM サーバに登録をスイッチオーバーすることを指定します。使用可能な DSP リソースは、スイッチオーバーが完了するとすぐに、新しいコールで利用できるようになります。

- **switchback method guard timeout 7200** コマンドは、プライマリ Unified CM が障害から回復した後の登録のスイッチバック メカニズムを指定します。このコマンドを設定すると、Cisco RSVP Agent は最後のアクティブなコールの切断後に、プライマリ Unified CM への登録の正常なスイッチバックを開始します。保護タイマーの期限内に登録の正常なスイッチバックが開始されない場合、Cisco RSVP Agent は即時のスイッチバック メカニズムを使用してすぐに Unified CM に登録します。保護タイマーのデフォルト値は 7200 秒で、60 ～ 172800 秒の範囲で静的に設定できます。
- ゲートウェイ コンフィギュレーション モードでの **timer receiver-rtp** コマンドは、RSVP 予約のための RTP クリーンアップ タイマーを定義します。障害が発生した場合、既存のコール用の RSVP 予約は、RTP クリーンアップ タイマーの期限が切れるまで有効です。このタイマーのデフォルト値は、1200 秒です。このタイマーは可能な最小値である 180 秒に設定することをお勧めします。

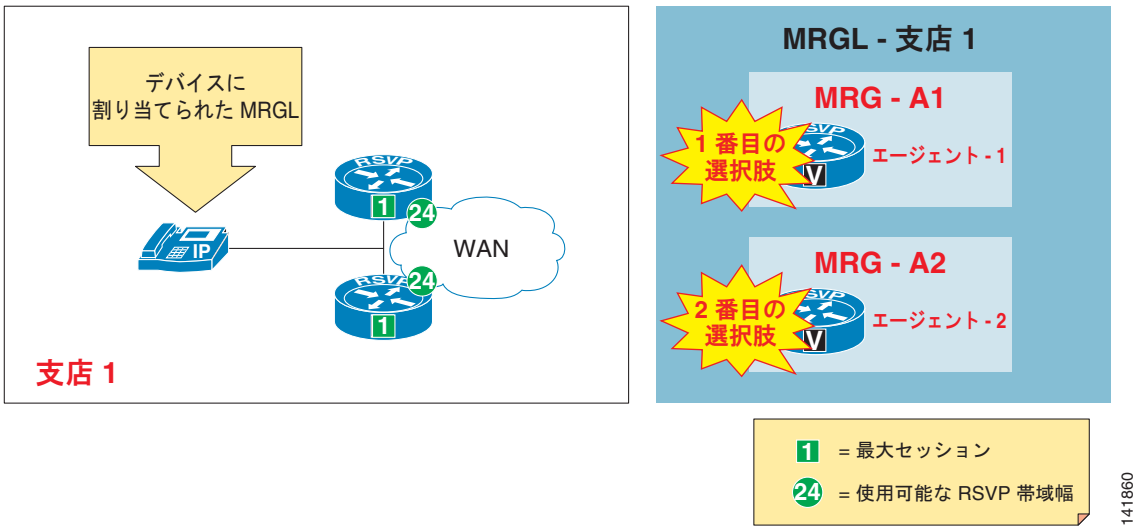
最大セッション サポート

Cisco RSVP Agent は、Cisco RSVP Agent ルータに搭載されるソフトウェアベースのリソース（CPU）とハードウェアベースのリソース（DSP）に基づく、コールまたはセッションの最大数をサポートしています。**dspfarm profile** コンフィギュレーション モードの **maximum sessions** コマンドは、Cisco RSVP Agent が処理できるコールの最大数を指定します。Cisco RSVP Agent は、この設定に基づいてセッション容量を Unified CM に通知します。セッションの最大数は、コールが Cisco RSVP Agent を通過するごとに 1 つずつ減少します。カウンタが 0 になると、Cisco RSVP Agent には使用可能なリソースがないと見なされ、Unified CM はそれ以降のコールでその Cisco RSVP Agent をスキップします。

図 9-15 は、2 つの Cisco RSVP Agent がある支店サイトを示しています。Cisco RSVP Agent は WAN ルータと共存し、Cisco RSVP Agent の冗長性は、同じ MRGL の別の MRG に 2 つの Cisco RSVP Agent を割り当てることによって実現されます。MRG-1 の Agent-1 が使用できないか、セッション容量を超えている場合、Unified CM は支店 1 を宛先または発信元とする RSVP コールのために、MRG-2 に Agent-2 を割り当てようとします。Agent-1 の容量に達したときに Agent-2 が選択されるようにするには、Cisco RSVP Agent の WAN インターフェイスで設定する **ip rsvp bandwidth** でサポートされるコール数と正確に一致するセッションの最大数を設定することをお勧めします。この例では、両方の Cisco RSVP Agent を **maximum sessions 1** に設定する必要があります。この推奨事項は、WAN を経由するすべてのコールが同じタイプのコーデックを使用し、WAN 経由のコール数を正確に計算できることを前提としています。このコール数は、使用可能な RSVP 帯域幅をコールごとに必要な帯域幅で割ることによって計算します。

（注） セッションの最大数が **ip rsvp bandwidth** 設定でサポートされるコール数よりも大きい場合でも、Unified CM はそのコールを Cisco RSVP Agent に送りますが、使用可能な帯域幅がないため RSVP 予約は失敗します。Unified CM は、コール アドミッション制御失敗の通常の処理に従います（コールを拒否するか、AAR 機能を呼び出します）。

図 9-15　Cisco RSVP Agent での最大セッションの設定



パススルー コーデック

パススルー コーデックを使用すると、Cisco IOS Enhanced MTP デバイスは、ストリームのメディア エンコーディングを認識していなくても、エンドポイントから受信した RTP メディア ストリームを終端することができます。つまり、メディア ストリームの UDP パケットは、デコードされずに MTP を通過します。この方法により、MTP は、Unified CM で定義されるすべての音声、ビデオ、およびデータのコーデックをサポートできます。MTP はメディア ストリームをデコードしないため、パススルー コーデックは暗号化（SRTP）メディア ストリームでも使用できます。実際にビデオおよび SRTP メディア ストリームが MTP を使用するには、パススルー コーデックをサポートする必要があります。パススルー コーデックで設定した場合、Cisco RSVP Agent はパケットの IP/UDP ヘッダーのソース IP アドレスを独自の IP アドレスで置き換えて、パケットを通過させます。

Cisco RSVP Agent は、次のすべての条件が満たされる場合にだけ、パススルー コーデックを使用します。

- コールに関与する 2 つのエンドポイント デバイスの音声コーデック能力が一致し、リージョン設定により同一のコーデックの使用がコールに対して許可されている。つまり、コールにトランスコーダ デバイスを挿入する必要はありません。
- **MTP Required** が、いずれのエンドポイント デバイスに対しても設定されていない。
- すべての中間リソース デバイスが、パススルー コーデックをサポートしている。

（注）　Cisco RSVP Agent が MTP デバイスとして登録され、トランスコーダ デバイスをコールに挿入する必要がある場合、Cisco RSVP Agent の dspfarm MTP プロファイルで設定されるコーデックは、Unified CM Administration で設定されるリージョン間コーデックと一致している必要があります。たとえば、G.729 コーデックが Unified CM Administration で設定されるリージョン間コーデックの場合は、dspfarm MTP プロファイルでも G.729 コーデックを設定する必要があります。

次の例は、Cisco 2800 IOS プラットフォーム上の Cisco RSVP Agent 設定を示しています。

```
interface Loopback0
 ip address 10.11.1.100 255.255.255.255
!
sccp local Loopback0
sccp ccm 20.11.1.50 identifier 1 priority 1 version 5.0.1
sccp ccm 20.11.1.51 identifier 2 priority 2 version 5.0.1
```

```
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate ccm 2 priority 2
 associate profile 1 register RSVPAgent
 switchover method immediate
 switchback method guard timeout 7200
!
dspfarm profile 1 mtp
 codec pass-through
 codec g729ar8
 rsvp
 maximum sessions software 100
 associate application SCCP
```

RSVP ポリシー

Unified CM は、ロケーション ペアごとに異なる RSVP ポリシーを適用できます。RSVP ポリシーは、Unified CM Administration で設定できます。RSVP ポリシーでは、RSVP 予約試行が失敗した場合に、Unified CM がコールを許可するかどうかが定義されます。次の RSVP ポリシー設定は、任意の 2 つのロケーション間で設定できます。

- No Reservation

  RSVP 予約試行は行われず、静的ロケーション コール アドミッション制御だけが、Unified CM で実行されます。

- Mandatory

  Unified CM は、音声ストリームに対する（コールがビデオ コールの場合はビデオ ストリームに対する）RSVP 予約が成功するまで、終端エンドポイント デバイスを呼び出しません。

- Mandatory (Video Desired)

  ビデオ ストリームの予約はできないが、音声ストリームの予約に成功した場合、ビデオ コールは音声専用コールとして処理できます。

- Optional (Video Desired)

  音声ストリームとビデオ ストリームの両方に対して予約が得られなかった場合、コールはベストエフォートの音声専用コールとして処理できます。Cisco RSVP Agent は、ベストエフォートとしてメディア パケットを再マーキングします。

- Use System Default

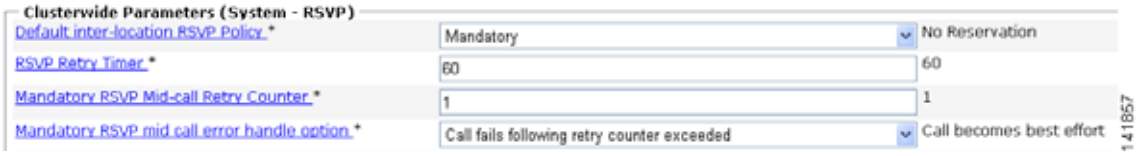
  ロケーション ペアの RSVP ポリシーが、クラスタ全体の RSVP ポリシーと一致します。デフォルトのクラスタ全体の RSVP ポリシーは、No Reservation です。Unified CM Administration でデフォルトの RSVP ポリシーを変更するには、[System] > [Service Parameters] > [Cisco CallManager Service] > [Default Inter-location RSVP Policy] を選択します。

（注） Optional (video desired) ポリシーでは、RSVP 予約が失敗しただけでなく、Cisco RSVP Agent も使用できない場合にだけ、IP WAN コールをベストエフォートとして処理できます。この場合、Unified CM は、ベストエフォートとしてトラフィックを再マーキングするように SCCP デバイスおよび MGCP デバイスに指示します。しかし、H.323 デバイスと SIP デバイスではこの再マーキングを行うことができないため、デフォルトの QoS マーキングでトラフィックの送信が続けられます。後者の場合にプライオリティ キューのオーバーサブスクリプションを防ぐため、IP WAN ルータで Access

Control List（ACL; アクセス コントロール リスト）を設定し、ソース IP アドレスが Cisco RSVP Agent のアドレスの場合に、DSCP EF または AF41 とマークされたパケットだけを許可することをお勧めします。

図 9-16 では、クラスタ全体の RSVP パラメータのデフォルト設定と推奨設定の両方を示しています。RSVP ポリシーは、**Mandatory** または **Mandatory (Video Desired)** に設定することをお勧めします。これらの設定では、帯域幅の予約とコールの音声品質が保証されます。クラスタ全体の RSVP ポリシーを設定するための最も効率的な方法としては、Cisco CallManager Service Service Parameter Configuration のクラスタ全体の RSVP パラメータに **Default Inter-location RSVP Policy** を設定し、ロケーション設定の RSVP 設定を **Use System Default** のままにします。

図 9-16　　クラスタ全体の RSVP パラメータの設定



クラスタ全体の RSVP パラメータ設定には、**Mandatory RSVP mid call error handle option** という名前のサービス パラメータがあります。RSVP ポリシーを **Mandatory** または **Mandatory (Video Desired)** に設定した場合、このパラメータは Unified CM がコール中の RSVP 予約試行の失敗に基づいて既存の RSVP を処理する方法を指定します。コール中の RSVP 予約試行は、WAN の障害後にネットワークのコンバージェンスや、既存の音声専用コールがビデオ コールになることなどでトリガーされることがあります。ネットワークのコンバージェンスでは、Cisco RSVP Agent は、新たにコンバージされたパスを通じてメディア ストリームの送信が開始されるだけでなく、新しいパスを通じて新しい RSVP 予約も試行されます。

Mandatory RSVP mid call error handle option のデフォルト設定は、**Call Becomes Best Effort** です。デフォルト オプションの設定では、Unified CM はコール中の RSVP 予約試行が失敗しても既存のコールを保持しますが、RTP ストリームはベストエフォートとしてマークされます（DSCP 0）。このパラメータは、**Call Fails Following Retry Counter Exceeded** オプション付きで設定することをお勧めします。このオプションを設定すると、Unified CM は RSVP 予約試行が一定の試行回数を超えて失敗し続けた場合に、コールを切断します。再試行カウンタのデフォルト値は 1 です。これは **RSVP Mandatory mid-call retry counter** サービス パラメータで定義され、**RSVP retry timer** のデフォルト値は 60 秒です。再試行カウンタと再試行タイマーの両方のサービス パラメータを、デフォルト値で設定することをお勧めします。両方のパラメータをデフォルト値に設定すると、Unified CM はコール中の RSVP 再試行が失敗した場合に、60 秒待機してからそのコールを切断します。この 60 秒間は、RSVP 予約が存在せず、RTP ストリームはベストエフォートとしてマーキングされるため、音声品質が低下することがあります。

静的ロケーションから RSVP コール アドミッション制御への移行

この項の例では、従来の静的ロケーション コール アドミッション制御から RSVP ベースのコール アドミッション制御メカニズムに移行するためのベスト プラクティスを示します。

図 9-17 では、静的ロケーション コール アドミッション制御メカニズムによるコール処理の集中型配置を示しています。Hub_None ロケーションや 3 箇所の支店など、Unified CM クラスタには 4 つのロケーションがあります。説明を簡単にするために、この例で使用する帯域幅は音声ストリームの帯域幅だけを示しています。表 9-5 と表 9-6 は、256 kbps の帯域幅で静的にプロビジョニングされるすべての支店ロケーションと、**Unlimited** の帯域幅でプロビジョニングされる Hub_None ロケーションを示しています。ロケーションの任意のペア間の RSVP 設定は **Use System Default** で設定され、クラスタ全体の RSVP 設定はデフォルト値 **No Reservation** で設定されます。

図 9-17　静的ロケーションでのコール アドミッション制御の設定

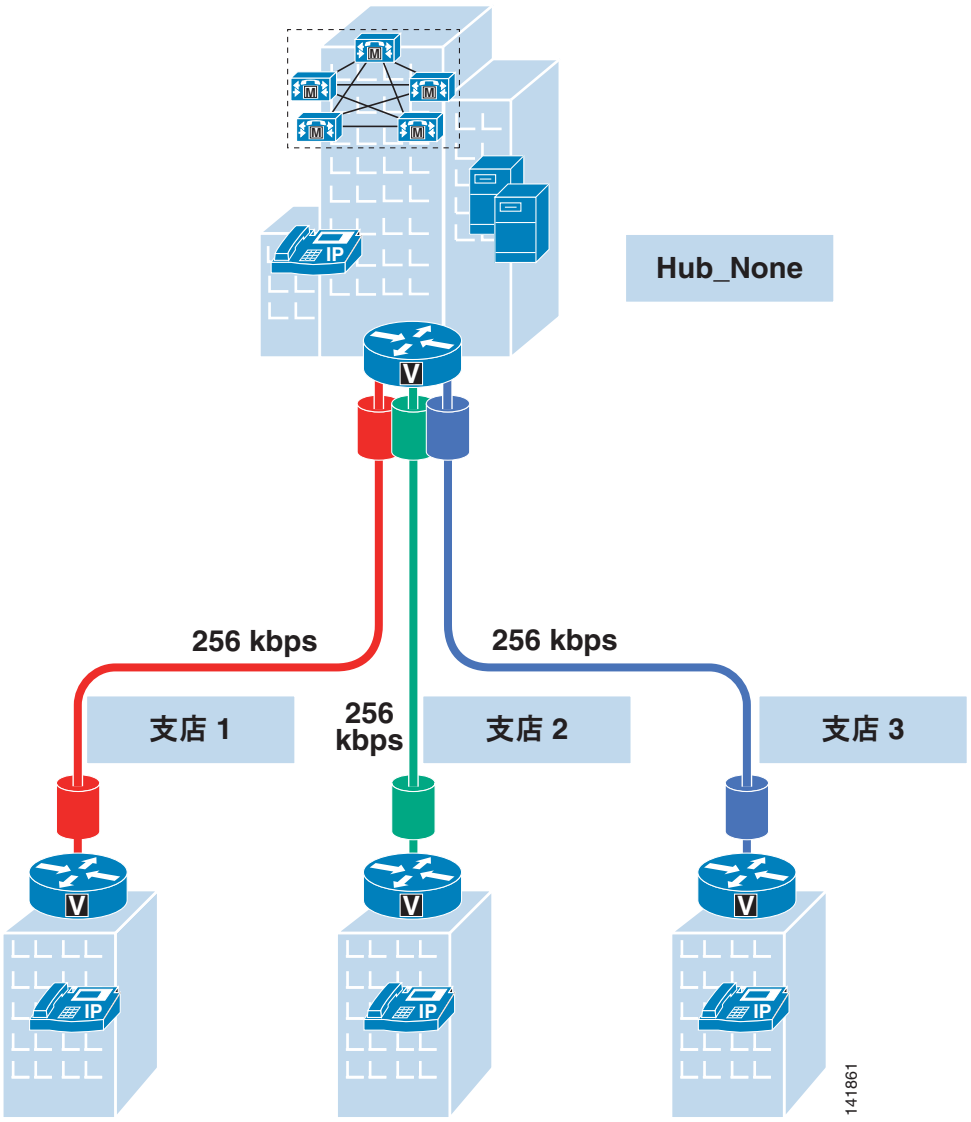


表 9-5　図 9-17 の例でのロケーションと帯域幅の設定

ロケーション名	帯域幅
Hub_None	Unlimited
支店 1	256 kbps
支店 2	256 kbps
支店 3	256 kbps

表 9-6　図 9-17 の例での RSVP ポリシー

ロケーション ペア		ポリシー
任意	任意	No Reservation

RSVP ベースのコール アドミッション制御に移行するには、ロケーションを一度に 1 つずつ移行することをお勧めします。たとえば、支店 1 が最初に移行するロケーションの場合は、次の手順に従います。

- 支店 1 ロケーションで Cisco RSVP Agent を設定し、支店 1 の MRG および MRGL に割り当てて、支店 1 の IP Phone に関連付けます。
- Hub_None ロケーションで別の Cisco RSVP Agent を設定し、Hub_None ロケーションを含む残りの 3 つのロケーションのすべての IP Phone に関連付けられた MRG および MRGL に、Cisco RSVP Agent を含めます。Cisco RSVP Agent を、Null MRG または支店 1 MRG に含めないでください。含めると、支店 1 の IP Phone が Hub_None ロケーションで Cisco RSVP Agent を使用して、RSVP 予約を行う可能性があります。
- 支店 1 の帯域幅を **Unlimited** に設定します。
- 支店 1 とその他の任意のロケーション間の RSVP 設定を **Mandatory** に設定します。たとえば、支店 1 と支店 2 の IP Phone 間のコールに対して、音声ストリームは Hub_None ロケーションを通じたヘアピンのままになります。支店 1 ロケーションと Hub_None ロケーション間の最初のコール レッグに対して、RSVP 予約は、支店 1 と Hub_None の Cisco RSVP Agent 間に行われます。Hub_None ロケーションと支店 2 ロケーション間の 2 番目のコール レッグに対して、Unified CM は、支店 2 ロケーションの帯域幅の可用性をチェックすることにより、静的ロケーションに基づくコール アドミッション制御を実行します。

表 9-7 と表 9-8 は、支店 1 での移行後のロケーションの帯域幅と RSVP ポリシー設定を示しています。

表 9-7　支店 1 への移行後のロケーションと帯域幅の設定

ロケーション名	帯域幅
Hub_None	Unlimited
支店 1	Unlimited
支店 2	256 kbps
支店 3	256 kbps

表 9-8　支店 1 への移行後の RSVP ポリシー

ロケーション ペア		ポリシー
支店 1	任意	Mandatory
その他すべてのロケーション	その他すべてのロケーション	No Reservation

表 9-9 と表 9-10 は、クラスタ全体の移行後のロケーションの帯域幅と RSVP ポリシー設定を示しています。クラスタ全体の移行が完了すると、サイト間のコールでは 2 つの Cisco RSVP Agent 間で RSVP 予約を直接行う必要があり、音声ストリームは帯域幅予約パスを通じて転送されます。

次の手順を使用すると、支店 2 および支店 3 を RSVP コール アドミッション制御に移行できます。

- 支店 2 ロケーションで Cisco RSVP Agent を設定し、支店 2 の IP Phone に関連付けられた支店 2 の MRG および MRGL に割り当てます。Hub_None ロケーションの Cisco RSVP Agent が支店 2 の IP Phone からアクセスされなくなるように、Hub_None ロケーションの Cisco RSVP Agent を支店 2 の MRG から削除してください。
- 支店 2 の帯域幅を **Unlimited** に設定します。
- 支店 2 とその他の任意のロケーション間の RSVP 設定を **Mandatory** に設定します。

- 支店 3 ロケーションで Cisco RSVP Agent を設定し、支店 3 の IP Phone に関連付けられた支店 3 の MRG および MRGL に割り当てます。Hub_None ロケーションの Cisco RSVP Agent が支店 3 の IP Phone からアクセスされなくなるように、Hub_None ロケーションの Cisco RSVP Agent を支店 3 の MRG から削除してください。
- 支店 3 の帯域幅を **Unlimited** に設定します。
- 支店 3 とその他の任意のロケーション間の RSVP 設定を **Mandatory** に設定します。

表 9-9　移行の完了後のロケーションと帯域幅の設定

ロケーション名	帯域幅
Hub_None	Unlimited
支店 1	Unlimited
支店 2	Unlimited
支店 3	Unlimited

表 9-10　移行完了後の RSVP ポリシー

ロケーション ペア		ポリシー
任意	任意	Mandatory

RSVP のアプリケーション ID

RSVP アプリケーション ID は、Unified CM が音声トラフィックとビデオ トラフィックの両方に識別子を追加できるようにするメカニズムです。これにより、Cisco RSVP Agent は、受け取った識別子に基づいていずれかのトラフィックに個別の帯域幅制限を設定できます。ネットワークに RSVP アプリケーション ID を配置するには、Cisco RSVP Agent ルータおよび Cisco Unified CM Release 5.0 で、Cisco IOS Release 12.4（6）T 以降を使用する必要があります。RSVP アプリケーション ID 文字列は、クラスタ全体の RSVP パラメータ設定の 2 つのサービス パラメータ（**RSVP Audio Application ID** と **RSVP Video Application ID**）で設定できます。

Unified CM は SCCP を使用して、RSVP アプリケーション ID を Cisco RSVP Agent に伝達します。Cisco RSVP Agent も、RSVP シグナリング メッセージ（RSVP Path メッセージや Resv メッセージなど）に RSVP アプリケーション ID を挿入し、ダウンストリームまたはアップストリームの RSVP ルータにこれらのメッセージを送信します。

RSVP アプリケーション ID は、静的ロケーション モデルとは異なるモデルを使用して、音声トラフィックおよびビデオ トラフィックの帯域幅を分離します。静的ロケーションでは、ビデオ コールの音声ストリームとビデオ ストリームはどちらもビデオ帯域幅カウンタから差し引かれます。RSVP アプリケーション ID を使用する場合、音声ストリームは音声帯域幅プールから差し引かれ、ビデオ ストリームはビデオ帯域幅プールから差し引かれます。コール アドミッション制御モデルのこの変更により、音声コール用に一定の帯域幅を予約し、プライオリティ キューで使用可能なすべての帯域幅を使用できるようになりました。このため、ビデオ コールが行われていない場合に、音声コール用にすべての使用可能な帯域幅を使用できます。プライオリティ キューに使用可能な帯域幅が十分にある場合、オプションとしてビデオ用のコールを有効にできます。ビデオ対応コールが消費できる帯域幅の量に制限を設定できますが、音声コールが使用可能なすべての帯域幅を消費している場合は、ビデオ コールを発信できないことがあります。RSVP アプリケーション ID、RSVP ポリシー、および LLQ の設定方法の詳細については、「RSVP のアプリケーション ID」（P.3-57）を参照してください。

RSVP 機能のある Cisco IOS Gatekeeper および Cisco Unified Border Element

Cisco Unified Border Element（旧称：Cisco Multiservice IP-to-IP Gateway）を使用すると、Unified CM クラスタ間、H.323 ゲートウェイ間、またはこれらの 2 者間の IP WAN 接続に関して、ハブアンドスポーク トポロジにおける制約を緩和できます。

Cisco IOS 機能が、IP ネットワーク間で H.323 Voice over IP（VoIP）コールおよびビデオ会議コールを使用するためのメカニズムを提供します。Cisco Unified Border Element ゲートウェイの主な目的は、管理ドメインを通過する VoIP コールとビデオ コールにコントロール ポイントと境界を提供することです。このゲートウェイは、PSTN-to-IP ゲートウェイとほぼ同じ機能を実行しますが、公衆網レッグと IP コール レッグの代わりに、通常は 2 つの IP コール レッグに加入します。

企業の IP Communications 環境において、Cisco Unified Border Element が備える最も興味深い機能は、このゲートウェイを通過する各コールのための RSVP 予約を生成できることです。「トポロジ対応コール アドミッション制御」（P.9-7）の項で説明しているように、RSVP は、トポロジ対応型のコール アドミッション制御メカニズムを提供するためのネットワーク ベース シグナリング プロトコルです。トポロジがハブアンドスポークである必要はなく、任意のネットワーク トポロジで機能します。

（注）　RSVP 機能のある Cisco Unified Border Element の配置に関するシスコのサポートの詳細については、http://www.cisco.com で入手可能な『*Cisco Unified Border Element Application Guide*』を参照してください。

結果として、コール フローに 2 つの Cisco Unified Border Element を挿入し、両者間で RSVP を有効にすることで、任意の IP WAN トポロジ上でコール アドミッション制御を実行できます。図 9-18 に、2 つのサイト A と B による基本的な例を示します。それぞれ Unified CM クラスタがあり、任意のトポロジを持つ IP WAN を通じて接続されています。各サイトには、Cisco Unified Border Element も配置されており、2 つの Unified CM クラスタは、すべてのサイト間コールを、ローカル Cisco Unified Border Element を指しているトランクを通じてルーティングするように設定されています。サイト A とサイト B の間でコールがセットアップされると、次のイベントが発生します。

- サイト A の Unified CM が、サイト A の Cisco Unified Border Element に向かう H.323 トランク（図中のコール レッグ 1）を通じてコールをセットアップします。
- サイト A の Cisco Unified Border Element が、サイト B の Cisco Unified Border Element に向かう別のコールを確立しようとしますが、まず RSVP を使用して、IP WAN パスに沿って帯域幅リソースを確保します。
- RSVP 予約が成功すると、2 つの Cisco Unified Border Element 間にコール レッグ 2 が確立されます。
- サイト B の Cisco Unified Border Element が、サイト B の Unified CM クラスタに向かう別のコール（図中のコール レッグ 3）を生成します。

図 9-18　RSVP コール アドミッション制御のための Cisco Unified Border Element の簡単な例

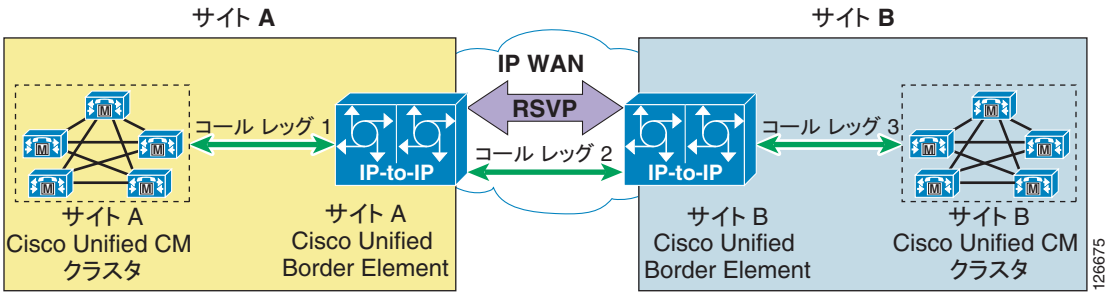


図 9-18 の例は、Unified CM クラスタ間のすべてのコールが、Cisco Unified Border Element ペアを通じてルーティングされる単純なシナリオです。しかし、多くの実稼動環境では、このアプローチは十分にスケーラブルで柔軟なものとは言えません。このような場合は、Cisco IOS ゲートキーパーを使用することで、Unified CM クラスタ、H.323 ゲートウェイ、H.323 ビデオ会議エンドポイント、Cisco Unified Border Element の間に幅広い通信オプションを配置できるようになります。

（注）　この項で説明した Cisco Unified Border Element 関係のシナリオは、すべて複数の Unified CM クラスタ間のコールに関するものです。同じ Unified CM クラスタに登録されているエンドポイント間で、コールに Cisco Unified Border Element を挿入することはお勧めしません。同じ Unified CM クラスタに登録されているエンドポイント間の RSVP ベースのコール アドミッション制御については、「Unified CM の RSVP 対応ロケーション」（P.9-18）を参照してください。

中継ゾーン（Via-Zone）ゲートキーパー

従来の Cisco IOS ゲートキーパー機能は、*中継ゾーン ゲートキーパー*という概念を通じて、Cisco Unified Border Element に対応するように拡張されました。中継ゾーン ゲートキーパーがレガシー ゲートキーパーと異なっている点は、コール ルーティングでの LRQ メッセージと ARQ メッセージの使用方法です。中継ゾーン ゲートキーパーを使用しても、通常のゲートキーパー機能を維持したまま、追加機能によって拡張されます。レガシー ゲートキーパーは、着信する LRQ を着信番号に基づいて検査します。具体的には、LRQ の destinationInfo 部分にある dialedDigits フィールドを検査します。中継ゾーン ゲートキーパーは、着信番号を検査する前に LRQ の発信地点を検査します。LRQ が、中継ゾーン ゲートキーパーのリモート ゾーン設定にリストされているゲートキーパーから送信されている場合、ゲートキーパーは、ゾーンのリモート設定に **invia** キーワードまたは **outvia** キーワードが含まれているかどうかを確認します。設定にこれらのキーワードが含まれている場合、ゲートキーパーは新しい中継ゾーン処理を使用します。含まれていない場合は、従来の処理を使用します。

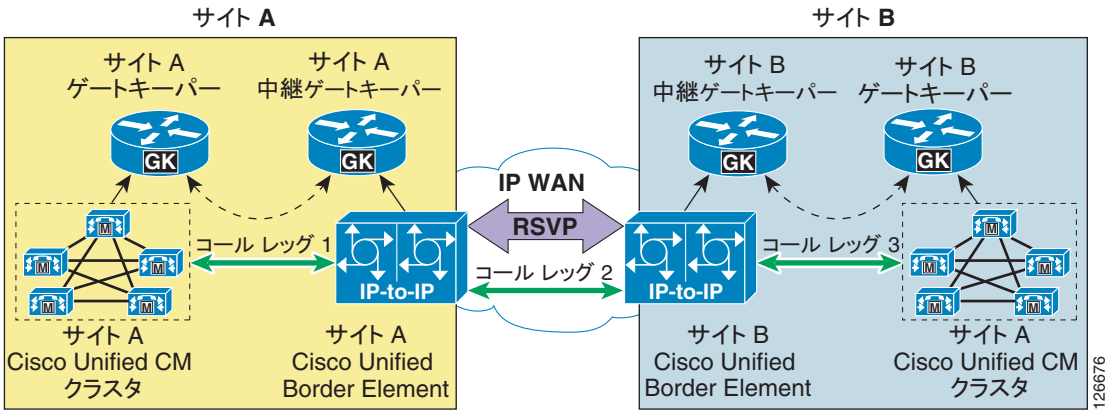
ARQ メッセージの場合、ゲートキーパーは宛先ゾーンに **outvia** キーワードが設定されているかどうかを調べます。**outvia** キーワードが設定されていて、**outvia** キーワードを使用して命名されているゾーンがゲートキーパーに対してローカルである場合は、そのゾーンの Cisco Unified Border Element がポイントされている ACF が返され、コールは Cisco Unified Border Element に転送されます。**outvia** キーワードを使用して命名されているゾーンがリモートである場合、ゲートキーパーは、ロケーション要求をリモート ゾーンのゲートキーパーではなく outvia ゲートキーパーに送信します。**invia** キーワードは、ARQ の処理では使用されません。

図 9-19 に、Cisco Unified Border Element と中継ゾーン ゲートキーパーを Unified CM クラスタおよびレガシー ゲートキーパーと連携するように使用して、コール ルーティングとコール アドミッション制御を提供する方法の例を示します。このシナリオには、次の考慮事項が適用されます。

- サイト A の Unified CM クラスタは、サイト A のゲートキーパーを使用して、コールをクラスタ間で直接ルーティングする。

- サイト A のゲートキーパーは、サイト B の E.164 番号に転送されるすべてのコールを、サイト A の中継ゾーン ゲートキーパーに送信する。
- サイト A の中継ゾーン ゲートキーパーは、サイト A のゲートキーパーを発信元または宛先とするすべてのコールに対して、Cisco Unified Border Element を挿入する。
- サイト A の Cisco Unified Border Element は、コールをサイト B の Cisco Unified Border Element に送信する前に、RSVP 予約を試行する。
- サイト B の Unified CM クラスタ、ゲートキーパー、および Cisco Unified Border Element は、サイト A のそれぞれと同様の方法で設定されている。

図 9-19　中継ゾーン ゲートキーパーを使用した RSVP のための Cisco Unified Border Element



設計上のベスト プラクティス

Cisco Unified Border Element を Unified CM と連携するように配置して、IP WAN で RSVP コール アドミッション制御を使用できるようにする場合は、次に示す設計上のベスト プラクティスに従ってください。

- 1 つ以上の Cisco Unified Border Element を通じて、他の Unified CM クラスタとの音声通信またはビデオ通信用に Unified CM のトランクを設定する場合は、ゲートキーパー制御 H.225 トランクを使用します。Cisco IOS Release 12.4（6）T 以降および Cisco Unified CM Release 4.1 以降を使用すると、Cisco Unified Border Element を通じた保留と保留解除、転送、会議などの付加サービスを呼び出すための MTP リソースが不要になります。相互運用性を確保するには、次の項目を設定する必要があります。
  - Unified CM Administration のトランク設定ページで、**Media Termination Point required** フィールドをオフ（デフォルト設定）のままにして、**Wait for Far End H.245 Terminal Capability Set** フィールドもオフにします。
  - Unified CM Administration の Unified CM に関する Advanced Service Parameters ページで、**Send H225 User Info Message** フィールドを **H225 Info For Call Progress Tone** に設定します。
  - 付加サービスを呼び出す場合に Unified CM との相互運用性を確保するには、Cisco Unified Border Element で次の Cisco IOS コマンドを設定します。

```
voice service voip
   h323
       emptycapability
       h245 passthru tcsnonstd-passthru
```

- 一部の配置では、プロキシ機能を提供し、エンドポイント デバイスに代わってシグナリング ストリームおよびメディア ストリームを終端させるために、MTP リソースが優先されます。MTP リソースが必要な場合は、クラスタ間トランクを介してコールするときに IP WAN 帯域幅の使用が増大するのを避けるために、Cisco Unified Border Element と同じサイトに MTP リソースを配置することをお勧めします。これらの MTP リソースは、ソフトウェア ベース（Cisco MCS サーバや Cisco IOS ルータなど）でも、ハードウェア ベース（Cisco コミュニケーション メディア モジュールを備えた Catalyst 6500 や、NM-HDV ネットワーク モジュールを備えた Cisco IOS ルータなど）でもかまいません。使用できる MTP リソースの完全なリストについては、「メディア リソース」（P.6-1）の章を参照してください。ただし、MTP を使用すると、コールが持続しているすべての期間にわたって、メディア パケットは最初の MTP リソースを通じて転送されます。以後にコール転送が発生した場合は、ヘアピンが発生する可能性があります。**Media Termination Point required** オプションが H.225 トランクでオフになっている場合、ビデオ コールは Cisco Unified Border Element を通じてクラスタ間で確立されないことに注意してください（MTP はビデオ コールをサポートしていないため）。
- すべてのクラスタ間コールで Cisco Unified Border Element を使用する場合にだけ、Unified CM で H.323 ゲートウェイとして Cisco Unified Border Element を設定します。この場合でも、Cisco Unified Border Element はゲートキーパーを使用してリモートの宛先を解決することができます。
- クラスタ間コールの解決、およびクラスタ間コールを Cisco Unified Border Element を通じてルーティングするか、直接ルーティングするかの判定にゲートキーパーを使用する場合は、Unified CM にゲートキーパー制御のクラスタ間トランクを設定します。このアプローチでは、より柔軟でスケーラビリティのある配置になります。
- Cisco Unified Border Element に対して Cisco Unified CM 3.3（2）以降と互換性があるのは、Cisco IOS Release 12.3（1）以降です。Cisco IOS Release 12.4(6)T 以降を使用することをお勧めします。
- ゲートキーパーと中継ゾーン ゲートキーパーの機能は、それぞれ別のルータ プラットフォーム上で実行して、分離します。各 Cisco Unified Border Element に対して、専用の中継ゾーン ゲートキーパーを配置する必要があります。
- 中継ゾーン ゲートキーパー機能と Cisco Unified Border Element 機能は、同じルータ プラットフォーム上で実行（共存）することができます。ただし、「冗長性」（P.9-33）の項で説明しているスケーラビリティの要件に注意してください。
- 同じ Unified CM クラスタに制御されているエンドポイント間では、コールに Cisco Unified Border Element を使用しないでください。
- 同じ Unified CM クラスタに制御されているエンドポイント間では、トポロジ対応コール アドミッション制御を提供するために RSVP 対応ロケーションを使用します。
- Cisco Unified Border Element に対して RSVP 予約を有効にする場合は、ダイヤル ピア設定で次のオプションを使用します。

```
req-qos guaranteed-delay audio
req-qos guaranteed-delay video
acc-qos guaranteed-delay audio
acc-qos guaranteed-delay video
```

この設定を行うと、各音声コールまたはビデオ コールに対して、Cisco Unified Border Element は遅延保証付きのサービスを使用して RSVP 予約を要求します。要求された QoS と許容可能な QoS の両方がこの RSVP サービスを指定している場合、コールが成功するためには RSVP 予約が必須になります（予約を確立できない場合はコールが失敗します）。設定の詳細については、「設定のガイドライン」（P.9-34）を参照してください。

冗長性

冗長性とスケーラビリティを実現するには、複数の Cisco Unified Border Element を同じ中継ゾーン ゲートキーパーおよび同じ中継ゾーンに登録します。中継ゾーン ゲートキーパーは、ラウンドロビン アルゴリズムを使用して、同じ中継ゾーンに含まれているすべての Cisco Unified Border Element に着信コールを自動的に分配します。

Cisco Unified Border Element に障害が発生すると、そのゲートウェイは中継ゾーン ゲートキーパーへの登録を失います。ゲートキーパーは、使用可能リソースのリストからそのゲートウェイを削除します。

Cisco Unified Border Element に対して、最大負荷しきい値を手動で設定することもできます。ある Cisco Unified Border Element で回線の使用率が一定の割合を超えると、そのゲートウェイは新しいコールの処理用としては選択されなくなり、回線の使用率が一定の割合を下回ると、再び使用可能になります。このように設定するには、次の Cisco IOS コマンドを使用します。

- Cisco Unified Border Element 上：

  ```
  ip circuit max-calls max-call-number
  ```

  上記のコマンドは、コール レッグに対する Cisco Unified Border Element の合計セッション容量を指定します。デフォルト値は、予約されたコール レッグ 1000 です。Cisco Unified Border Element が処理するコールは、使用可能な IP 回路から 2 つのセッションを使用します。1 つは着信コール レッグ用で、もう 1 つは発信コール レッグ用です。一般的な H.323 ゲートウェイと同様に、Cisco Unified Border Element は、H.323 バージョン 4 プロトコルを使用してセッション容量情報を中継ゾーン ゲートキーパーに自動的に送信します。

- ゲートキーパー上：

  ```
  endpoint resource-threshold onset onset-threshold abatement abatement-threshold
  ```

  上記のコマンドは、中継ゾーン ゲートキーパーに、Cisco Unified Border Element などのそれぞれのゲートウェイのコール量をモニタリングさせます。ゲートウェイがそのセッション容量情報をアドミッション要求（ARQ）または解除要求（DRQ）メッセージでレポートすると、中継ゾーン ゲートキーパーはアクティブ コールをカウントします。特定のゲートウェイのアクティブ コール容量の使用率が上限（範囲 = 1 ～ 99、デフォルト = 90）を超えると、中継ゾーン ゲートキーパーはそのゲートウェイへのコールの送信を停止します。ゲートウェイのアクティブ コール量が下限（範囲 = 1 ～ 99、デフォルト = 70）を下回ると、中継ゾーン ゲートキーパーはそのゲートウェイへのコールの送信を再開します。これらのしきい値はグローバル値で、特定のゲートキーパーに登録されているすべてのゲートウェイに影響します。

上記のコマンド両方を設定すると、中継ゾーン ゲートキーパーは Cisco Unified Border Element の現在のセッション容量の使用率を計算することができ、十分な容量リソースがない Cisco Unified Border Element にコールを送信しないようにすることができます。設定しないと、ゲートキーパーのコール アドミッション制御が失敗し、アドミッション拒否（ARJ）またはロケーション拒否（LRJ）メッセージが発信元デバイスに返される場合があります。

これらのコマンドの詳細については、次の Web サイトで入手できる Cisco IOS コマンド解説資料を参照してください。

http://www.cisco.com

設定のガイドライン

ここでは、図 9-20 に示したネットワーク ダイアグラムに基づく簡単な設定例を示します。この項は、詳細なコマンド リファレンス ガイドを意図したものではなく、一般的な配置シナリオに役立つガイドラインをまとめたものです。Cisco Unified Border Element および中継ゾーン ゲートキーパーを設定する方法の詳細については、次の Web サイトで入手可能な、Cisco Unified Border Element のオンライン ドキュメントで説明しています。

http://www.cisco.com

図 9-20　中継ゾーン ゲートキーパーを使用した Cisco Unified Border Element の設定例

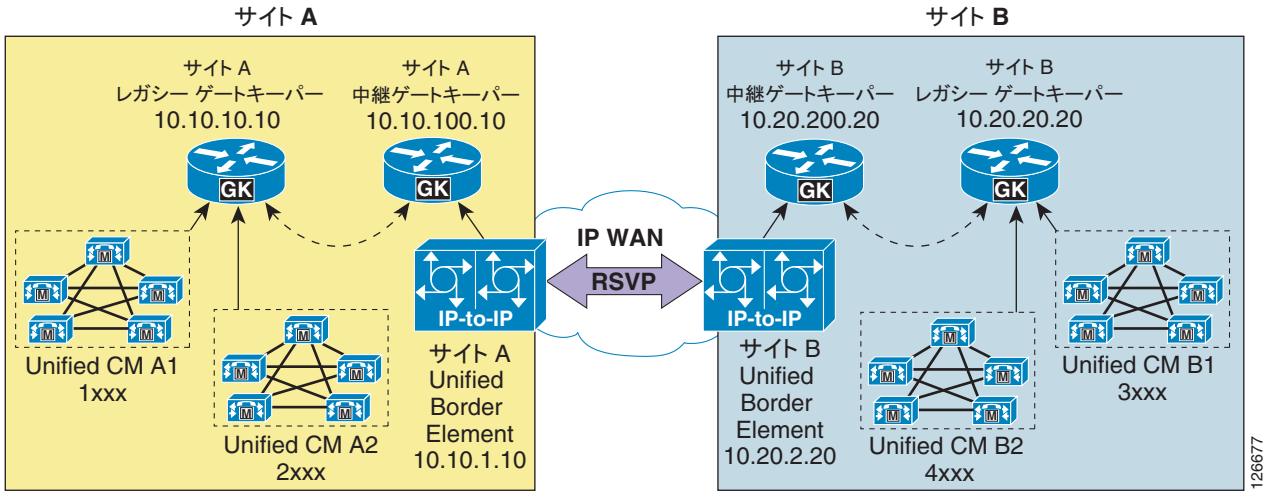


図 9-20 に示すネットワークでは、サイト A に内線番号 1*xxx* のクラスタ A1 と、内線番号 2*xxx* のクラスタ A2 の 2 つの Unified CM クラスタが存在しているとします。サイト B にも、内線番号 3*xxx* のクラスタ B1 と、内線番号 4*xxx* のクラスタ B2 の 2 つの Unified CM クラスタが存在します。

次の各項に、サイト A にあるデバイスに関連する設定を示します。サイト A の内部でやり取りされるコールは、（サイト A のレガシー ゲートキーパーを使用して）Unified CM クラスタ間で直接ルーティングされるのに対して、サイト B に向かうコールは、2 つの Cisco Unified Border Element を通じて（それぞれのレガシー ゲートキーパーと中継ゾーン ゲートキーパーを使用して）ルーティングされます。

Unified CM

クラスタ A1 とクラスタ A2 は、どちらもゲートキーパー制御クラスタ間トランクを使用します。これは、MTP を必要とせず、サイト A のレガシー ゲートキーパーを指すクラスタ間トランク（ICT）です。

[34]XXX ルート パターンは、ゲートキーパーおよび Cisco Unified Border Element を通じてサイト B のクラスタに到達するために、ルート リストおよびルート グループを通じて ICT を指しています。

他のルート パターン（クラスタ A1 の 2XXX とクラスタ A2 の 1XXX）は、ルート リストおよびルート グループを通じて ICT を指すことで、クラスタ A1 と A2 がゲートキーパーを通じて互いに通信できるようにしています。

クラスタ間で Cisco Unified Border Element と RSVP を使用して付加サービスをサポートするには、ICT のパラメータ「Calling Party Selection」を「Last Redirect Number」または「First Redirect Number」に設定して、コールを確立する必要があります。

レガシー ゲートキーパー

サイト A のレガシー ゲートキーパーは、クラスタ A1 と A2 の間ではコールを直接ルーティングし、サイト B に向かうコール（内線番号 3*xxx* と 4*xxx*）については、すべてサイト A の中継ゾーン ゲートキーパーに送信します。例 9-1 に、関連する設定を示します。

例 9-1　　サイト A のレガシー ゲートキーパー設定

```
gatekeeper
 zone local CCM-A1 customer.com 10.10.10.10
 zone local CCM-A2 customer.com
 zone remote A-VIAGK customer.com 10.10.100.10
 zone prefix CCM-A1 1...
 zone prefix CCM-A2 2...
 zone prefix A-VIAGK 3...
 zone prefix A-VIAGK 4...
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

中継ゾーン ゲートキーパー

サイト A の中継ゾーン ゲートキーパーは、サイト B の Unified CM クラスタ（内線番号 3*xxx* と 4*xxx*）に向かうコールをサイト B の中継ゾーン ゲートキーパーに送信し、サイト B で発着信されるコールに使用される Cisco Unified Border Element を呼び出します。サイト A のクラスタに向かうコールは、サイト A のレガシー ゲートキーパーにルーティングされ、Cisco Unified Border Element は呼び出されません。例 9-2 に、関連する設定を示します。

例 9-2　　サイト A の中継ゾーン ゲートキーパー設定

```
gatekeeper
 zone local A-VIAGK customer.com 10.10.100.10
 zone remote CCM-A1 customer.com 10.10.10.10
 zone remote CCM-A2 customer.com 10.10.10.10
 zone remote B-VIAGK customer.com 10.20.200.20 invia A-VIAGK outvia A-VIAGK
 zone prefix B-VIAGK 3...
 zone prefix B-VIAGK 4...
 zone prefix CCM-A1 1...
 zone prefix CCM-A2 2...
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

例 9-2 に示す設定には、次の考慮事項が適用されます。

- B-VIAGK リモート ゾーンに関連するコマンドラインの **invia** キーワードと **outvia** キーワードが、このゾーンの中継ゾーン ゲートキーパーの処理をアクティブにします。つまり、B-VIAGK リモート ゾーンが宛先または発信元となるすべてのコールについて、中継ゾーン ゲートキーパーは、A-VIAGK ローカル ゾーンに登録されている Cisco Unified Border Element リソースを呼び出します。
- CCM-A1 リモート ゾーンおよび CCM-A2 リモート ゾーンに関連するコマンドラインには、**invia** キーワードと **outvia** キーワードがありません。このため、標準のゲートキーパー処理が適用され、これらのゾーンで発着信されるコールに対しては、Cisco Unified Border Element は呼び出されません。

Cisco Unified Border Element

サイト A の Cisco Unified Border Element は、サイト B の Unified CM クラスタ（内線番号 3*xxx* と 4*xxx*）に向かう音声コールとビデオ コールについては、RSVP 予約を要求します。一方で、サイト A の Unified CM クラスタ（内線番号 1*xxx* と 2*xxx*）に向かうコールについては要求しません。例 9-3 に、関連する設定を示します。

例 9-3　サイト A の Cisco Unified Border Element 設定

```
voice service voip
   allow-connections h323 to h323
   h323
      emptycapability
      h245 passthru tcsnonstd-passthru
!
gateway
!
interface FastEthernet0/1
   ip address 10.10.1.10 255.255.255.0
   ip rsvp bandwidth 200
   ip rsvp data-packet classification none
   ip rsvp resource-provider none
   h323-gateway voip interface
   h323-gateway voip id A-VIAGK ipaddr 10.10.100.10
   h323-gateway voip h323-id A-CUBE
   h323-gateway voip bind srcaddr 10.10.1.10
   h323-gateway voip tech-prefix 1#
!
dial-peer voice 5 voip
   session target ras
   incoming called-number [3-4]...
   codec g729r8
!
dial-peer voice 10 voip
   destination-pattern [3-4]...
   session target ras
   req-qos guaranteed-delay audio
   req-qos guaranteed-delay video
   acc-qos guaranteed-delay audio
   acc-qos guaranteed-delay video
   codec g729r8
!
dial-peer voice 15 voip
session target ras
   incoming called-number [1-2]...
   req-qos guaranteed-delay audio
   req-qos guaranteed-delay video
   acc-qos guaranteed-delay audio
   acc-qos guaranteed-delay video
   codec g729r8
!
dial-peer voice 20 voip
   destination-pattern [1-2]...
   session target ras
   codec g729r8
```

例 9-3 に示す設定には、次の考慮事項が適用されます。

- **emptycapability** コマンドは、Unified CM と Cisco Unified Border Element 間の H.245 Empty Capabilities Set（ECS）を有効にして、確立されたコールに対して付加サービスを呼び出します。
- **req-qos guaranteed-delay** [**audio** | **video**] コマンドで、ダイヤルピア 10 または 15 を使用する音声コールとビデオ コールについて、Cisco Unified Border Element が遅延保証付きの RSVP 予約を要求することを指定します。
- **acc-qos guaranteed-delay** [**audio** | **video**] コマンドで、音声コールとビデオ コールに関して許容可能な最小限の QoS レベルも、遅延保証付き RSVP 予約であることを指定します。これは、RSVP 要求が失敗した場合はコールも失敗するので、RSVP 予約を必須にすることを意味します。RSVP 予約がオプションになるように（予約が失敗した場合でもコールが成功するように）Cisco Unified Border Element を設定するには、代わりに **acc-qos best-effort** [**audio** | **video**] コマンドを使用します。

コール アドミッション制御の設計

ここでは、各種の Unified CM 配置モデルおよび次の IP WAN トポロジに対して、コール アドミッション制御メカニズムを適用する方法について説明します。

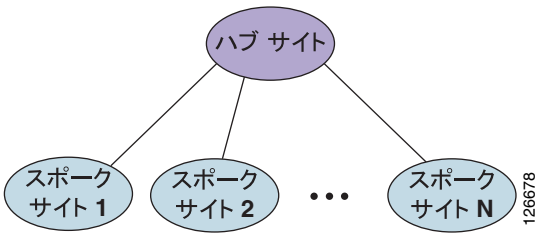
- 「単純なハブアンドスポーク トポロジ」（P.9-37）
- 「2 層ハブアンドスポーク トポロジ」（P.9-41）
- 「単純な MPLS トポロジ」（P.9-45）
- 「汎用トポロジ」（P.9-52）

これらの項では、採用する Unified CM 配置モデルに基づいて、トポロジごとにそれぞれ別の設計考慮事項を示します。

単純なハブアンドスポーク トポロジ

図 9-21 に、スター トポロジとも呼ばれる単純なハブアンドスポーク トポロジを示します。このタイプのネットワーク トポロジでは、すべてのサイト（*スポーク サイト*と呼ばれる）が、1 つの IP WAN リンクを通じて中央サイト（*ハブ サイト*と呼ばれる）に接続されます。スポーク サイト間には直接のリンクが存在しないため、スポーク サイト間の通信は、すべてハブ サイトを経由する必要があります。

図 9-21　　単純なハブアンドスポーク トポロジ



この項の設計上の考慮事項は、従来のレイヤ 2 IP WAN テクノロジーを使用する単純なハブアンドスポーク トポロジに適用されます。

- フレーム リレー
- ATM

- フレーム リレー /ATM 間サービス インターワーキング
- 専用回線

MPLS テクノロジーに基づいた IP WAN 配置については、「単純な MPLS トポロジ」（P.9-45）の項を参照してください。

以降では、採用する Unified CM 配置モデルごとに、単純なハブアンドスポーク トポロジに関する設計上のベスト プラクティスを示します。

- 「集中型の Unified CM 配置」（P.9-38）

  1 つまたはそれ以上の Unified CM クラスタをハブ サイトに配置し、スポーク サイトには電話とゲートウェイだけを配置します。

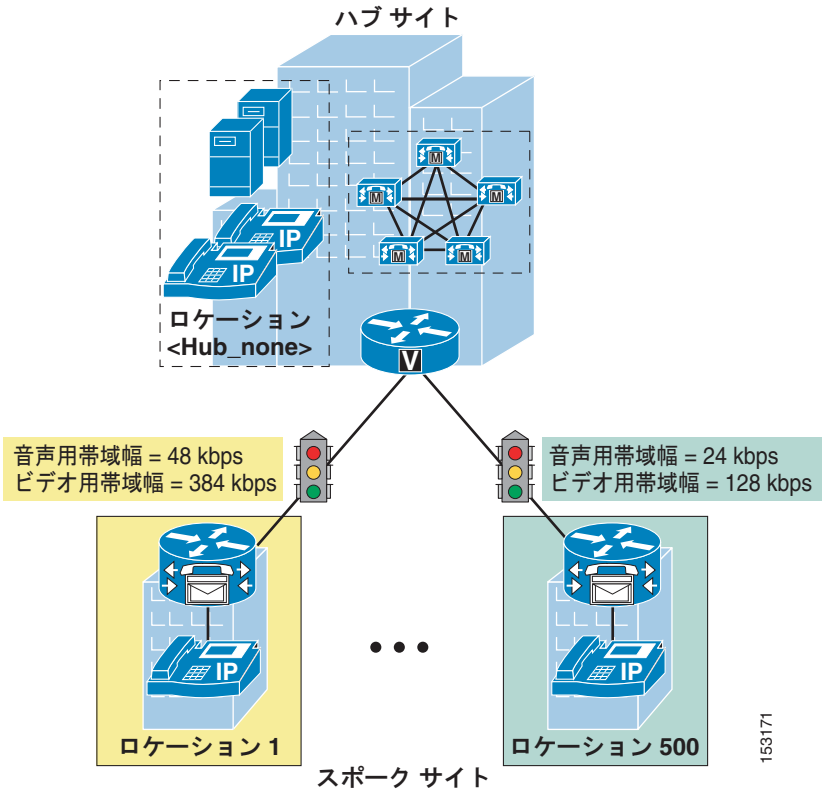
- 「分散型の Unified CM 配置」（P.9-39）

  Unified CM クラスタまたは Cisco Unified Communications Manager Express（Unified CME）を各サイトに配置します。

集中型の Unified CM 配置

単純なハブアンドスポーク トポロジ上にあり、集中型コール処理を使用するマルチサイト WAN 配置では、Unified CM の静的*ロケーション*を使用してコール アドミッション制御を実装します。図 9-22 に、このメカニズムをこのようなトポロジに適用する方法の例を示します。

図 9-22　静的ロケーションを使用した単純なハブアンドスポーク トポロジのコール アドミッション制御



コール アドミッション制御に対して静的ロケーションを使用する場合は、次のガイドラインに従ってください。

- 各スポーク サイトの Unified CM に対しては、個別にロケーション設定が必要です。

- 各サイトの音声コールとビデオ コールに対する帯域幅の上限を、そのサイトに使用されているコーデックのタイプに応じて、適切に設定します（帯域幅の推奨設定については、表 9-2 を参照してください）。
- 各スポーク サイトのすべてのデバイスを適切なロケーションに割り当てます。
- ハブ サイトのデバイスは、Hub_None ロケーションのままにします。
- あるデバイスを別のロケーションに移した場合、ロケーションの設定も変更します。
- Unified CM は、ロケーションを 2000 箇所までサポートします。
- WAN の帯域幅が十分にない場合に、公衆網を介した自動ルーティングを実行する必要があるときは、Unified CM 上で Automated Alternate Routing（AAR）機能を設定します（「Automated Alternate Routing」（P.10-87）を参照）。
- 同じハブ サイトに複数の Unified CM クラスタを配置する場合は、クラスタ間トランク デバイスを Hub_None ロケーションのままにします。ダイヤル プランの解決には、ゲートキーパーを使用できます。ただし、この場合、ゲートキーパーのコール アドミッション制御は必要ありません。これは、すべての IP WAN リンクがロケーション アルゴリズムによって制御されるためです。

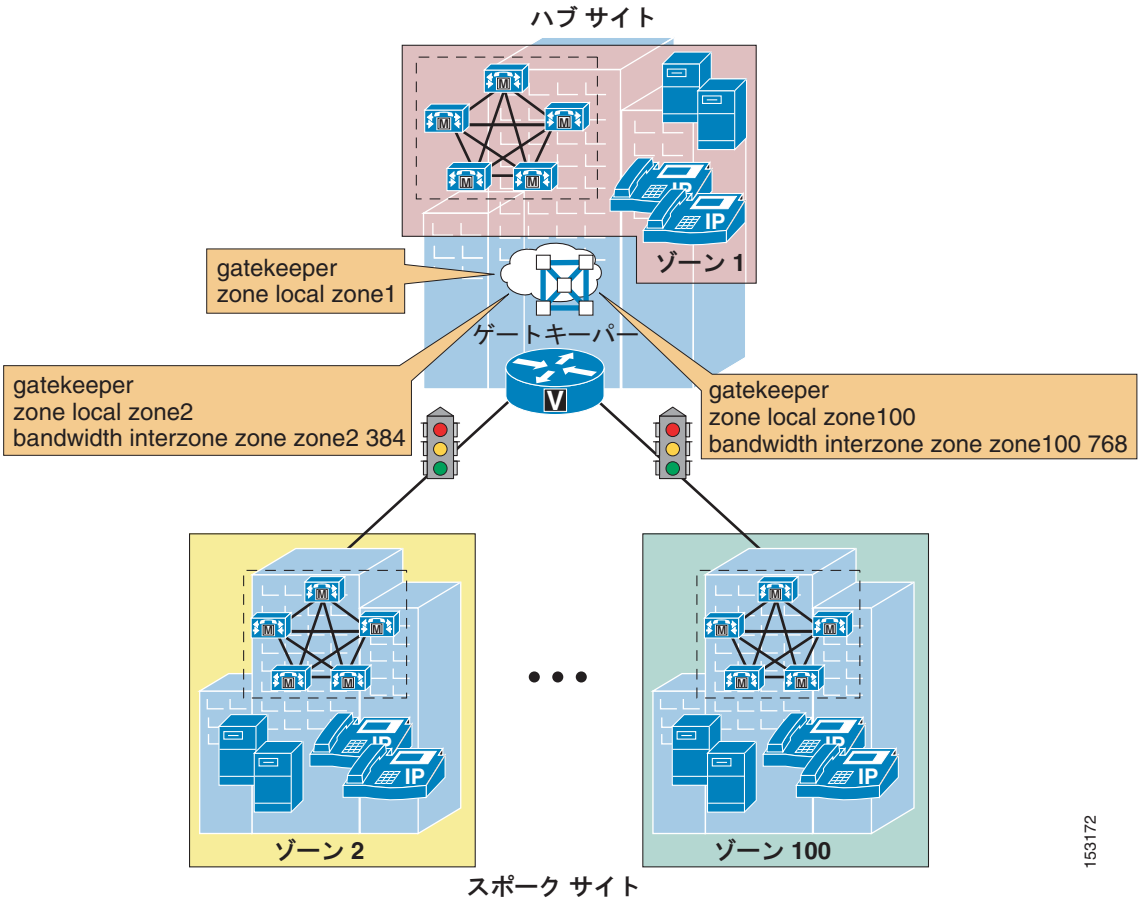
（注）　1 つ以上のサイトに IP WAN への二重接続があり、両方のリンクで使用可能な帯域幅を最大限に利用する場合は、「汎用トポロジ」（P.9-52）の項で説明しているように、トポロジ対応コール アドミッション制御を配置することをお勧めします。詳細については、「トポロジ非対応コール アドミッション制御の制限」（P.9-5）を参照してください。

分散型の Unified CM 配置

単純なハブアンドスポーク トポロジの分散型コール処理配置では、Cisco IOS ゲートキーパーを使用してコール アドミッション制御を実装できます。この設計では、コール処理エージェント（Unified CM クラスタ、Cisco Unified Communications Manager Express（Unified CME）、または H.323 ゲートウェイなど）は Cisco IOS ゲートキーパーに登録し、エージェントが IP WAN コールを発信しようとするたびにゲートキーパーに照会を行います。Cisco IOS ゲートキーパーは、各コール処理エージェントを、特定の帯域幅制限があるゾーンに関連付けます。したがって、Cisco IOS ゲートキーパーは、ゾーンに出入りする IP WAN 音声コールが消費する最大帯域幅量を制限することができます。

図 9-23 では、ゲートキーパーを使用したコール アドミッション制御を示しています。つまり、コール処理エージェントは、IP WAN コールを発信するときに、まずゲートキーパーに許可を要求します。ゲートキーパーが許可を与えると、コール処理エージェントは、IP WAN を介してコールを発信します。ゲートキーパーが要求を拒否する場合、コール処理エージェントは別のパス（たとえば、公衆網）を試行するか、単にコールを廃棄させることができます。

図 9-23　ゲートキーパーを使用したハブアンドスポーク トポロジのコール アドミッション制御



ゲートキーパーを使用してコール アドミッション制御を配置する場合は、次のガイドラインに従ってください。

- Cisco Unified Communications Manager Express（Unified CME）と H.323 ゲートウェイの混在環境の場合は、Unified CM で H.225 ゲートキーパー制御トランクを設定します。
- Unified CM クラスタだけに基づく環境の場合は、Unified CM でクラスタ間ゲートキーパー制御トランクを設定します。
- Unified CM で設定したゾーンが、そのサイトの正しいゲートキーパー ゾーンと一致するようにします。
- デバイス プールの Unified CM 冗長性グループにリストされている各 Unified CM サブスクライバは、ゲートキーパー制御トランクをゲートキーパーに登録します（最大で 3 つまで）。
- コールは、Unified CM クラスタ内に登録済みのトランク間にロードバランスされます。
- Unified CM は、複数のゲートキーパーおよびトランクをサポートします。
- トランクをルート グループとルート リスト コンストラクトに配置すると、自動公衆網フェールオーバーを提供できます。詳細については、「ダイヤル プラン」（P.10-1）を参照してください。
- Unified CM、Unified CME、または H.323 ゲートウェイをサポートしている各サイトに対するゲートキーパーのゾーンは、個別に設定します。
- **bandwidth interzone** コマンドをゲートキーパーに使用して、そのゲートキーパーに直接登録済みの Unified CM クラスタ、Unified CME サーバ、および H.323 デバイス間の帯域幅の制御を行います（コーデック タイプ別の帯域幅の設定については、表 9-4 を参照してください）。

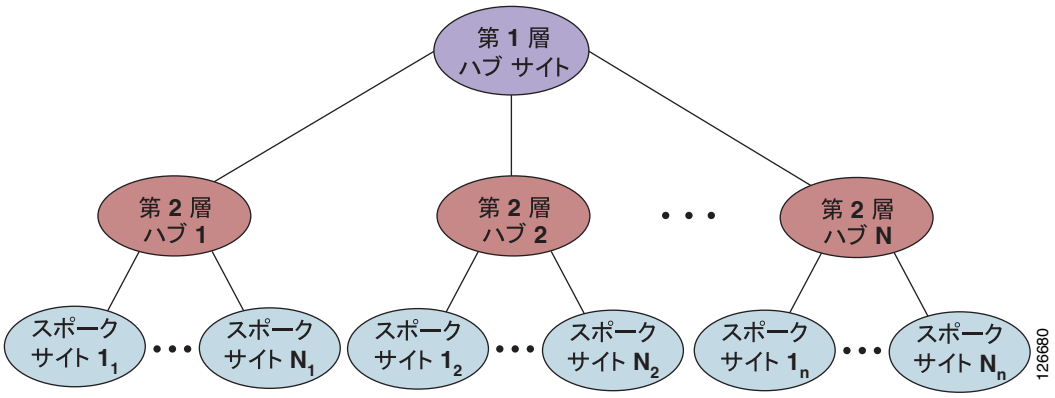
- 1 つの Cisco IOS ゲートキーパーで、100 までのゾーンまたはサイトをサポートできます。
- ゲートキーパーの冗長性は、ゲートキーパー クラスタリング（代替ゲートキーパー）または Cisco ホットスタンバイ ルータ プロトコル（HSRP）を使用すると実装することができます。HSRP は、ソフトウェア機能セットにゲートキーパー クラスタリングが使用可能ではない場合に限り使用します。

（注）　1 つ以上のサイトに IP WAN への二重接続があり、両方のリンクで使用可能な帯域幅を最大限に利用する場合は、「汎用トポロジ」（P.9-52）の項で説明しているように、トポロジ対応コール アドミッション制御を配置することをお勧めします。詳細については、「トポロジ非対応コール アドミッション制御の制限」（P.9-5）を参照してください。

2 層ハブアンドスポーク トポロジ

図 9-24 では、2 層ハブアンドスポーク トポロジを示しています。このタイプのネットワーク トポロジは 3 階層のサイト、つまり第 1 層ハブ サイト、第 2 層ハブサイト、およびスポーク サイトから構成されます。スポーク サイトのグループが 1 つの第 2 層ハブ サイトに接続され、各第 2 層ハブ サイトは 1 つの第 1 層ハブ サイトに接続されます。単純なハブアンドスポーク トポロジであるため、スポーク サイト間には直接のリンクが存在しません。したがって、スポーク サイト間の通信は、すべて第 2 層ハブ サイトを経由する必要があります。同様に、第 2 層ハブ サイト間には直接のリンクが存在しないため、これらのハブ サイト間の通信は、すべて第 1 層ハブ サイトを経由する必要があります。

図 9-24　　2 層ハブアンドスポーク トポロジ



この項の設計上の考慮事項は、従来のレイヤ 2 IP WAN テクノロジーを使用する 2 層ハブアンドスポーク トポロジに適用されます。

- フレーム リレー
- ATM
- フレーム リレー /ATM 間サービス インターワーキング
- 専用回線

MPLS テクノロジーに基づいた IP WAN 配置については、「単純な MPLS トポロジ」（P.9-45）の項を参照してください。

以降では、採用する Unified CM 配置モデルごとに、2 層ハブアンドスポーク トポロジに関する設計上のベスト プラクティスを示します。

- 「集中型の Unified CM 配置」（P.9-42）

  1 つまたはそれ以上の Unified CM クラスタを第 1 層ハブ サイトに配置し、第 2 層ハブ サイトとスポーク サイトには電話とゲートウェイだけを配置します。

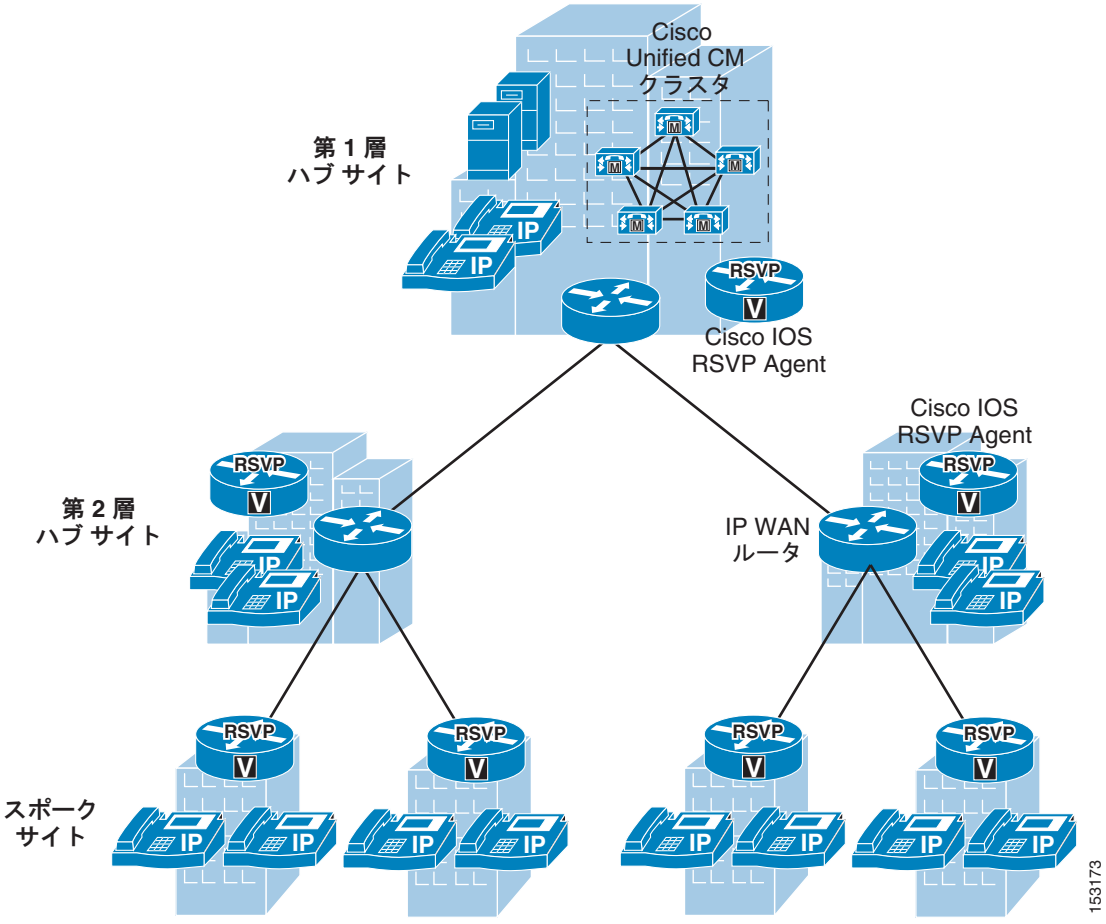
- 「分散型の Unified CM 配置」（P.9-44）

  Unified CM クラスタを第 1 層ハブ サイトと第 2 層ハブ サイトに配置し、スポーク サイトにはエンドポイントとゲートウェイだけを配置します。

集中型の Unified CM 配置

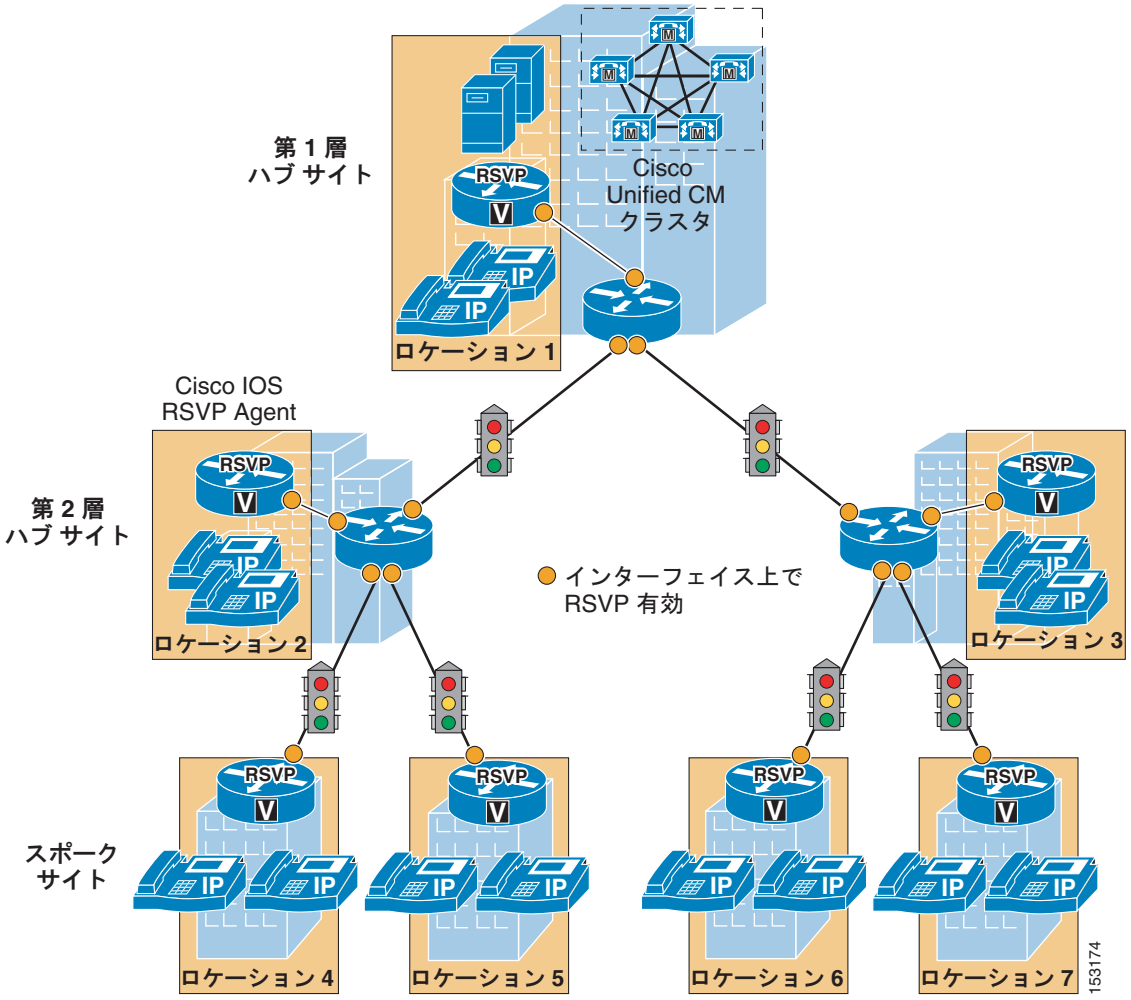
図 9-25 では、2 層ハブアンドスポーク IP WAN トポロジに配置された単一の Unified CM 集中型クラスタを示しています。このシナリオでは、Unified CM クラスタを第 1 層ハブ サイトに配置し、すべての第 2 層ハブ サイトとスポーク サイトにはエンドポイントとゲートウェイだけを配置します。

図 9-25　集中型の Unified CM での 2 層ハブアンドスポーク トポロジ



このシナリオでは、トポロジ対応コール アドミッション制御を配置する必要があります。そのため、単一の Unified CM クラスタにとっては、RSVP 対応ロケーションを使用することになります。図 9-26 では、このメカニズムを配置する方法を示しています。

図 9-26　RSVP 対応ロケーションを使用した 2 層ハブアンドスポーク トポロジのコール アドミッション制御



これらの配置には、次のガイドラインが適用されます。

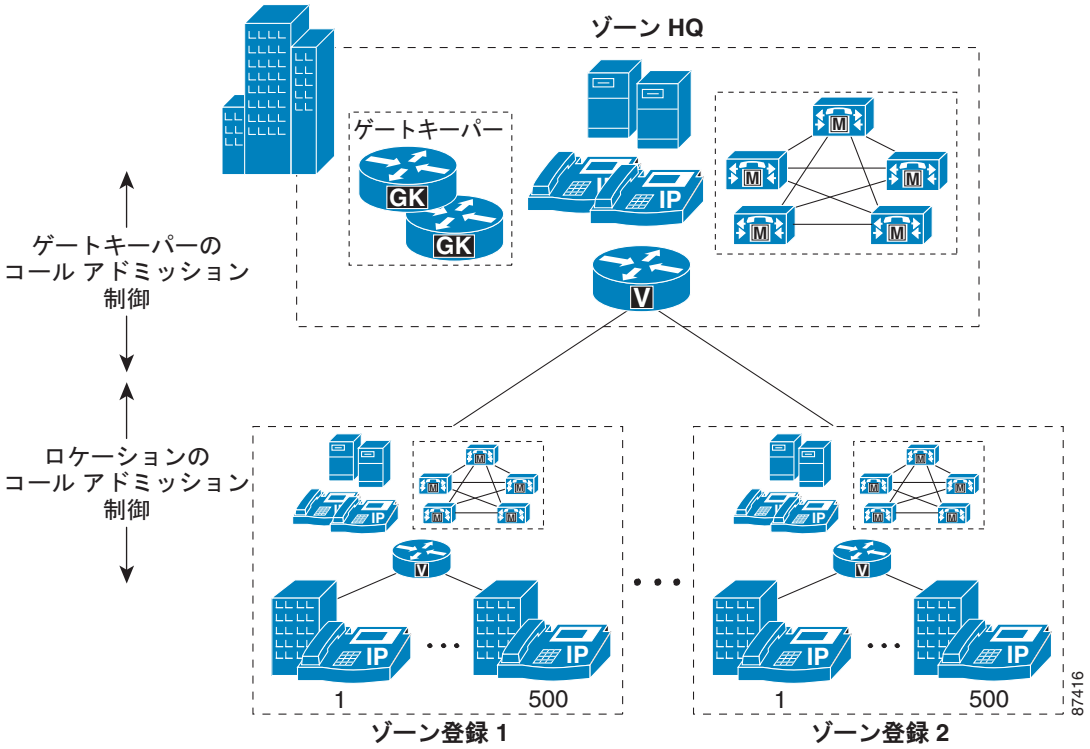
- 各サイトの Cisco IOS ルータで Cisco IOS RSVP Agent 機能を有効にします。比較的小さなサイトでは、このルータは IP WAN ルータおよび公衆網ゲートウェイと一体になっていることがあり、比較的大きなサイトでは異なるプラットフォームとなっている場合があります。
- Unified CM で、各サイトのロケーションを定義し、すべての帯域幅の値を **Unlimited** のままにします。
- 各サイトにあるすべてのデバイスを該当するロケーションに割り当てます（これにはエンドポイント、ゲートウェイ、会議リソース、および Cisco RSVP Agent 自体が含まれます）。
- 各 Cisco RSVP Agent が、そのサイトのすべてのデバイスのメディア リソース グループ リスト（MRGL）のメディア リソース グループ（MRG）に属するようにします。
- Unified CM サービス パラメータで、**Default inter-location RSVP Policy** を **Mandatory** または **Mandatory (video desired)** に設定し、**Mandatory RSVP mid-call error handle option** を **Call fails following retry counter exceeded** に設定します。

- 輻輳が発生する可能性のあるネットワークですべての WAN インターフェイス上の RSVP を有効にし、プライオリティ キューのプロビジョニングに基づいて RSVP 帯域幅を設定します。
- Cisco RSVP Agent が IP WAN ルータと共存していない場合、そのエージェントを WAN ルータに接続する LAN インターフェイスで RSVP を有効にします（図 9-26 を参照）。

分散型の Unified CM 配置

2 層ハブアンドスポーク トポロジを採用していて、第 1 層ハブ サイトと第 2 層ハブ サイトに Unified CM がある配置にコール アドミッション制御を提供するには、図 9-27 に示されているように静的ロケーションとゲートキーパー ゾーン メカニズムを組み合せて対応します。

図 9-27　コール アドミッション制御にロケーションおよびゲートキーパー メカニズムを組み合せる方式



ゲートキーパー ゾーンを静的ロケーションと組み合せてコール アドミッション制御を実行する場合は、次の推奨事項に従ってください。

- ローカル Unified CM を使用していないサイト（つまり、スポーク サイト）には、静的ロケーションに基づくコール アドミッション制御を使用します。
- Unified CM クラスタ間（つまり、第 1 層ハブ サイトと第 2 層ハブ サイト間）には、ゲートキーパー ベースのコール アドミッション制御を使用します。
- ローカル Unified CM を使用していない各サイトには、そのサイトをサポートしている Unified CM クラスタ内にロケーションを設定します。
- 各サイトの帯域幅の上限を、そのサイトに使用されているコーデックのタイプに応じて、適切に設定します（帯域幅の設定については、表 9-2 と表 9-4 を参照してください）。
- Unified CM に設定された各デバイスをロケーションに割り当てます。あるデバイスを別のロケーションに移した場合、ロケーションの設定も変更します。

- Unified CM は、ロケーションを 2000 箇所までサポートします。
- 各 Unified CM クラスタは、ゲートキーパー制御のトランクをゲートキーパーに登録します。
- ゲートキーパーでは、各 Unified CM クラスタに対してゾーンを設定し、**bandwidth interzone** コマンドを使用して各クラスタを宛先および発信元とするコール数を制御します。

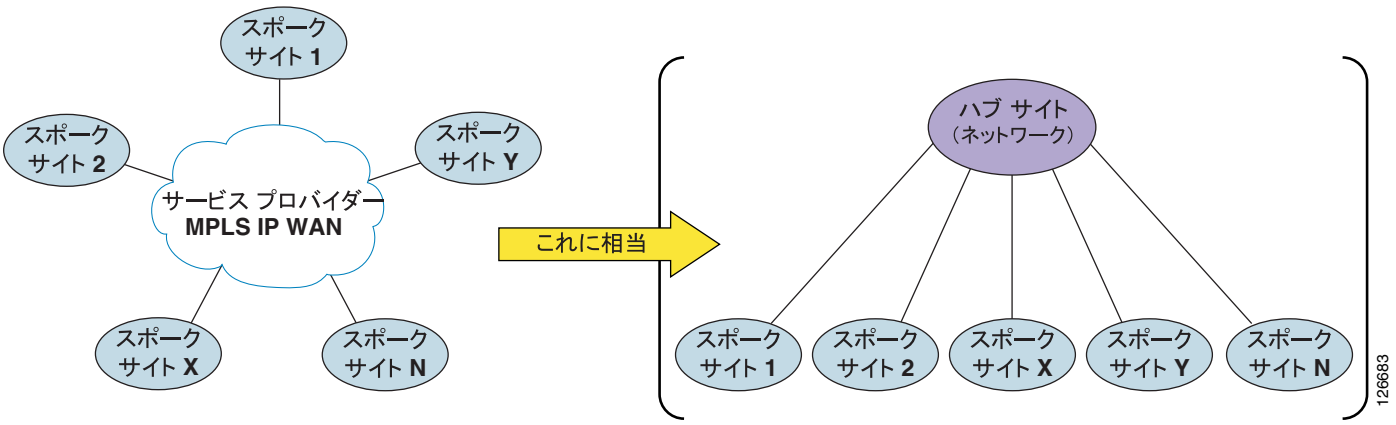
（注）　1 つ以上のサイトに IP WAN への二重接続があり、両方のリンクで使用可能な帯域幅を最大限に利用する場合は、「汎用トポロジ」（P.9-52）の項で説明しているように、トポロジ対応コール アドミッション制御を配置することをお勧めします。詳細については、「トポロジ非対応コール アドミッション制御の制限」（P.9-5）を参照してください。

単純な MPLS トポロジ

図 9-28 では、Multiprotocol Label Switching（MPLS）テクノロジー ベースの（サービス プロバイダーからの）IP WAN を示しています。サービス プロバイダーの提供する従来のレイヤ 2 WAN サービスと MPLS ベースのサービスのデザイン上の大きな違いは、MPLS を使用すると、IP WAN のトポロジはハブアンドスポークに準拠していないということです。すべてのサイト間の接続にはフルメッシュ接続方式を採用します。

このトポロジの違いは、ネットワークを企業側での IP ルーティングという観点から見たとき、各サイトが、他のどのサイトからも IP ホップ 1 つ分しか離れていないことを意味します。したがって、他のサイトに到達するためにハブ サイトを経由する必要はありません。事実上、「ハブ サイト」という概念が存在しません。すべてのサイトが対等と見なされ、各サイトで異なっているのは、IP WAN を介して使用することのできる帯域幅の量のみです。

図 9-28　サービス プロバイダーからの MPLS IP WAN、およびこれに相当するトポロジ



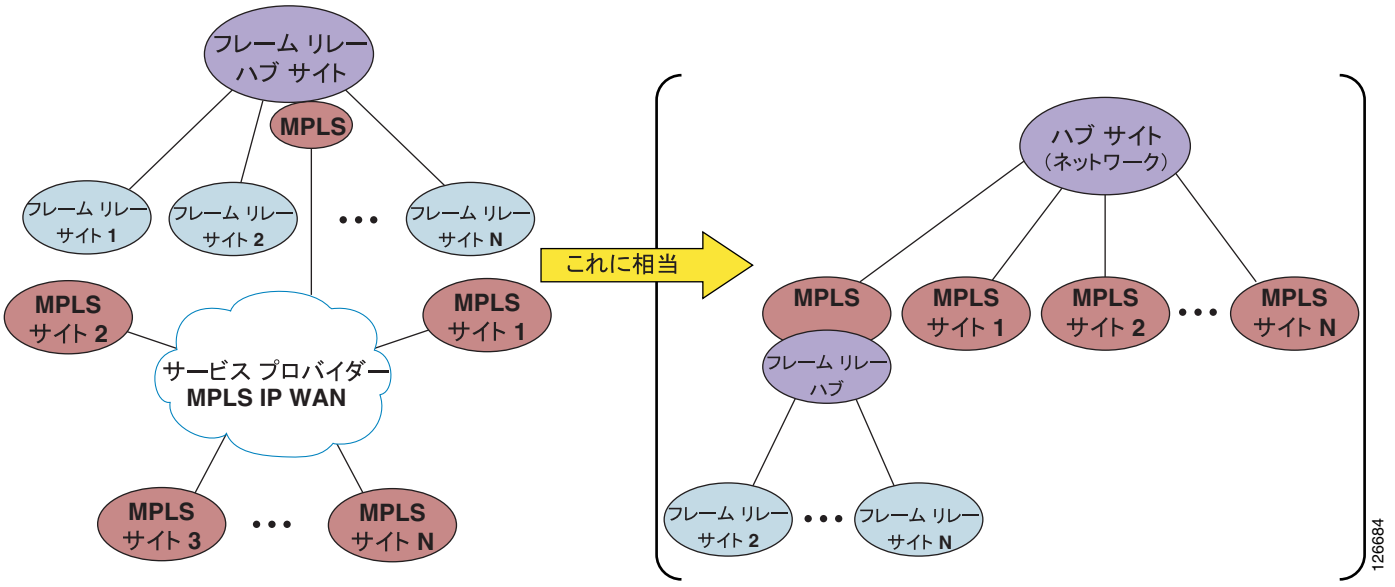
これまでに検討した内容に基づくと、コール アドミッション制御という観点から見たとき、MPLS に基づくサービス プロバイダー IP WAN サービスは、実質的には、ハブ サイトのないハブアンドスポーク トポロジに相当することが簡単にわかります（図 9-28 を参照）。事実上、ネットワーク自体をハブ サイトと見なすことができます。企業サイトは、いずれも（本社、つまり中央サイトを含めて）スポーク サイトに相当します。このように見方を変えると、コール アドミッション制御の実行方法も異なってきます。この方法については、以降で説明します。

上で検討した内容の中で、ここで例外として言及する価値があるのは、マルチサイト配置において、MPLS ベースの WAN がフレーム リレーや ATM などの従来のレイヤ 2 テクノロジー ベースの IP WAN と共存している場合です。このようなシナリオは、実際に発生する可能性があります。たとえば、ネットワークが移行の途中段階にある場合や、企業合併などの状況が発生した場合です。

図 9-29 に示すように、従来のレイヤ 2 テクノロジー（フレーム リレーなど）ベースのハブアンドスポーク IP WAN を MPLS ベースの IP WAN と統合すると、ネットワーク トポロジは単純なハブアンドスポークやフルメッシュではなく、2 層ハブアンドスポークになります。

この場合、MPLS ネットワークが第 1 層ハブ サイトを表し、MPLS 対応のフレーム リレー ハブ サイト、および MPLS ベースのサイトが第 2 層ハブ サイトを表し、フレーム リレー スポーク サイトがスポーク サイトを表します。したがって、このような配置での設計上の考慮事項については、「2 層ハブアンドスポーク トポロジ」（P.9-41）の項を参照してください。

図 9-29　MPLS サイトとフレーム リレー サイトの共存、およびこれに相当するトポロジ



以降では、採用する Unified CM 配置モデルごとに、MPLS ベースのトポロジに関する設計上のベストプラクティスを示します。

- 「集中型の Unified CM 配置」（P.9-47）

  1 つまたはそれ以上の Unified CM クラスタを 1 つのサイトだけに配置し、その他のすべてのサイトにはエンドポイントとゲートウェイだけを配置します。

- 「分散型の Unified CM 配置」（P.9-50）

  Unified CM クラスタを複数のサイトに配置し、その他のすべてのサイトには、エンドポイントとゲートウェイだけを配置します。

（注）　ここでは、サービス プロバイダーによって MPLS サービスが提供されている企業の配置を中心に説明します。MPLS ネットワークが企業自体によって配置される場合、次の 2 つのいずれかの条件が満たされる限り、コール アドミッション制御は効果的に実行できます。最初の条件は、MPLS ネットワークでのルーティングが、ネットワークがハブアンドスポークになるように設定されていること、2 番目の条件は、輻輳が末端部分でしか発生しないように、MPLS ネットワークの核の部分の帯域幅を非常に大きく設定していることです。

（注）　1 つ以上のサイトに IP WAN への二重接続があり、両方のリンクで使用可能な帯域幅を最大限に利用する場合は、「汎用トポロジ」（P.9-52）の項で説明しているように、トポロジ対応コール アドミッション制御を配置することをお勧めします。ロード バランシング リンクが存在する場合は、対称的なルーティングを保証するために特に注意が必要です。詳細については、「トポロジ非対応コール アドミッション制御の制限」（P.9-5）および 「MPLS ネットワークの特別な考慮事項」（P.9-11）を参照してください。また、シスコのアカウント チームにお問い合せください。

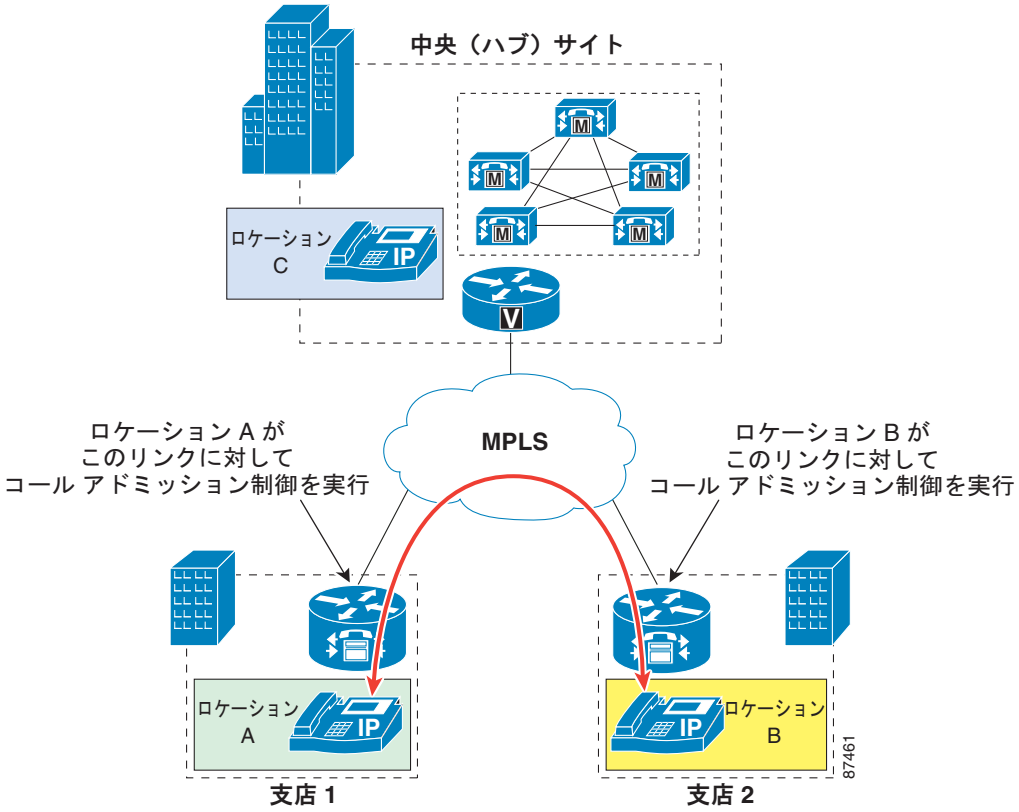
集中型の Unified CM 配置

MPLS トポロジ上で集中型コール処理を使用するマルチサイト WAN 配置では、Unified CM の静的ロケーションを使用してコール アドミッション制御を実装します。

ハブアンドスポーク WAN トポロジ（フレーム リレー、ATM など）では、支店サイトとのリンクはすべて、中央サイトで終端します。フレーム リレーを例にすると、支店ルータからのすべての PVC（Permanent Virtual Circuits; 相手先固定接続）は、中央サイトのヘッドエンド ルータに集約されています。この例では、帯域幅に対する課金は WAN リンクの支店エンドで行われているので、中央サイドではデバイスにコール アドミッション制御を適用する必要はありません。したがって、Unified CM ロケーションの設定では中央サイトのデバイスのロケーションは Hub_None のままにしておきます。一方、各支店のデバイスは適切なコール アドミッション制御を受けるために各支店のロケーションに指定される必要があります。

MPLS WAN ネットワークでは、すべての支店はレイヤ 3 で隣接していると見なされるため、中央サイトに接続する必要はありません。図 9-30 では、スポークツースポーク配置による 2 つの支店間のコールを説明しています。

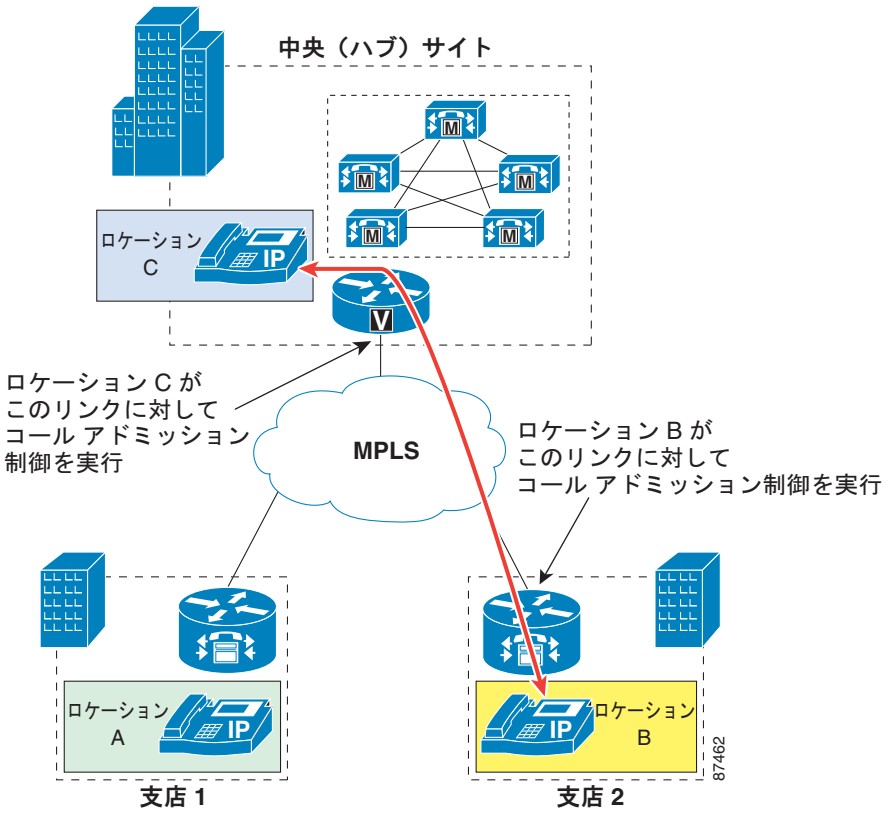
図 9-30　MPLS 配置におけるスポークツースポーク コール



また、MPLS WAN では、中央サイト WAN に接続しているリンクは支店の WAN リンクのすべてを集約していません。中央サイトに存在するすべてのデバイスは、個々のデバイスに対応するコール アドミッション制御ロケーション（つまり、Hub_None ロケーションではありません）に指定されています。したがって、このスポークツースポーク設定では支店のリンクとは無関係に、コール アドミッション制御は中央サイト リンク上で実行される必要があります（図 9-31 を参照）。

（注）　トランクなどの一部のデバイスはメディアを終端しないで、通常は Hub_None ロケーションのままにします。ただし、トランクで MTP が要求される場合にコール アドミッション制御のエラーを回避するためには、トランクは Hub_None 以外のロケーションに割り当てる必要があり、トランクの MRGL 内のすべての MTP は、そのロケーションに関連付けられたサイトに物理的に配置する必要があります。MTP はロケーションに直接割り当てることができず、その MTP を選択したデバイスのロケーションを継承するため、この設定が必要です。

図 9-31　MPLS 配置におけるハブとのコール

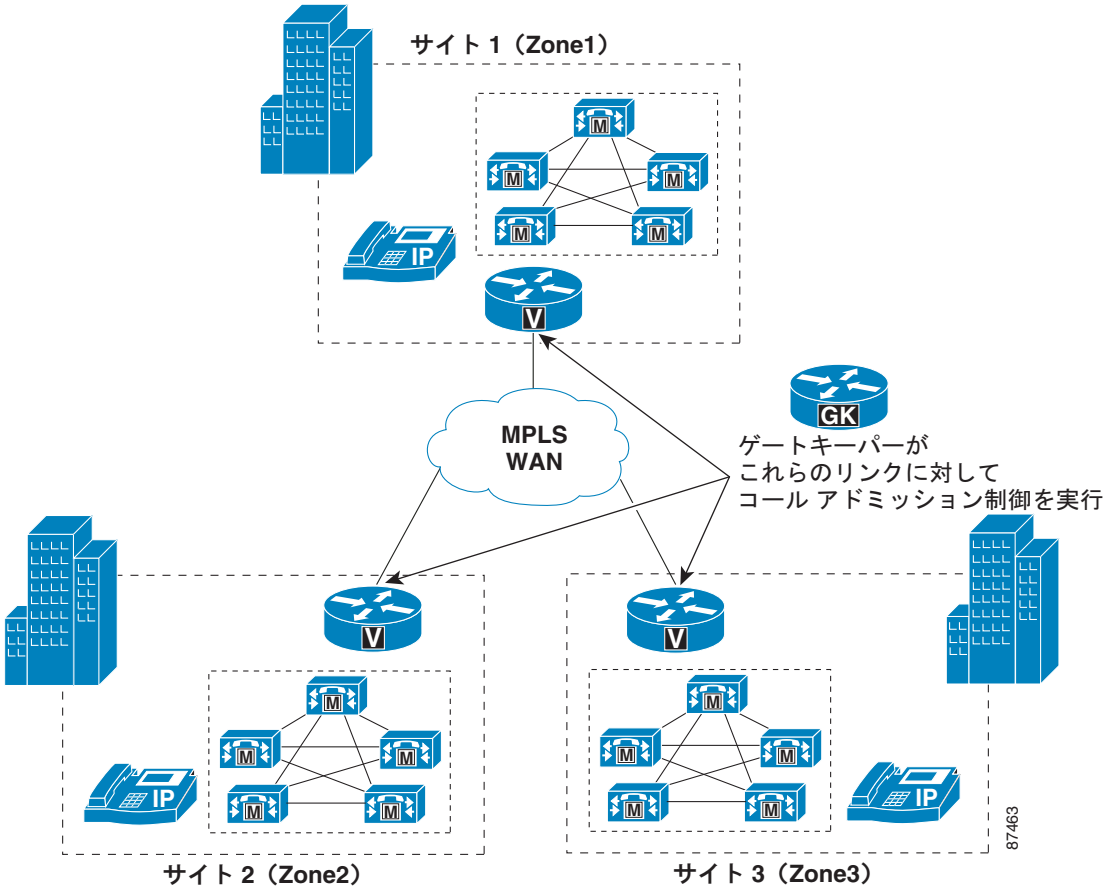


特定サイトに許されている帯域幅がすべて消費されてしまっている場合は、Unified CM が備えている Automated Alternate Routing（AAR）機能を使用して、公衆網へ自動的にフェールオーバーさせることができます（AAR の詳細については、「Automated Alternate Routing」（P.10-87）を参照してください）。

分散型の Unified CM 配置

支店ロケーションのない複数のサイトに Unified CM クラスタが設定されていて、どのサイト間も MPLS WAN でリンクされているマルチ サイト配置の場合は、ゲートキーパーがダイヤル プランを解決し、サイト間のコール アドミッション制御を行い、個々のサイトを異なるゲートキーパー ゾーンに格納します。この同様のメカニズムは、レイヤ 2 WAN テクノロジーをベースにしたハブアンドスポークトポロジにも適用されています（図 9-32 を参照）。

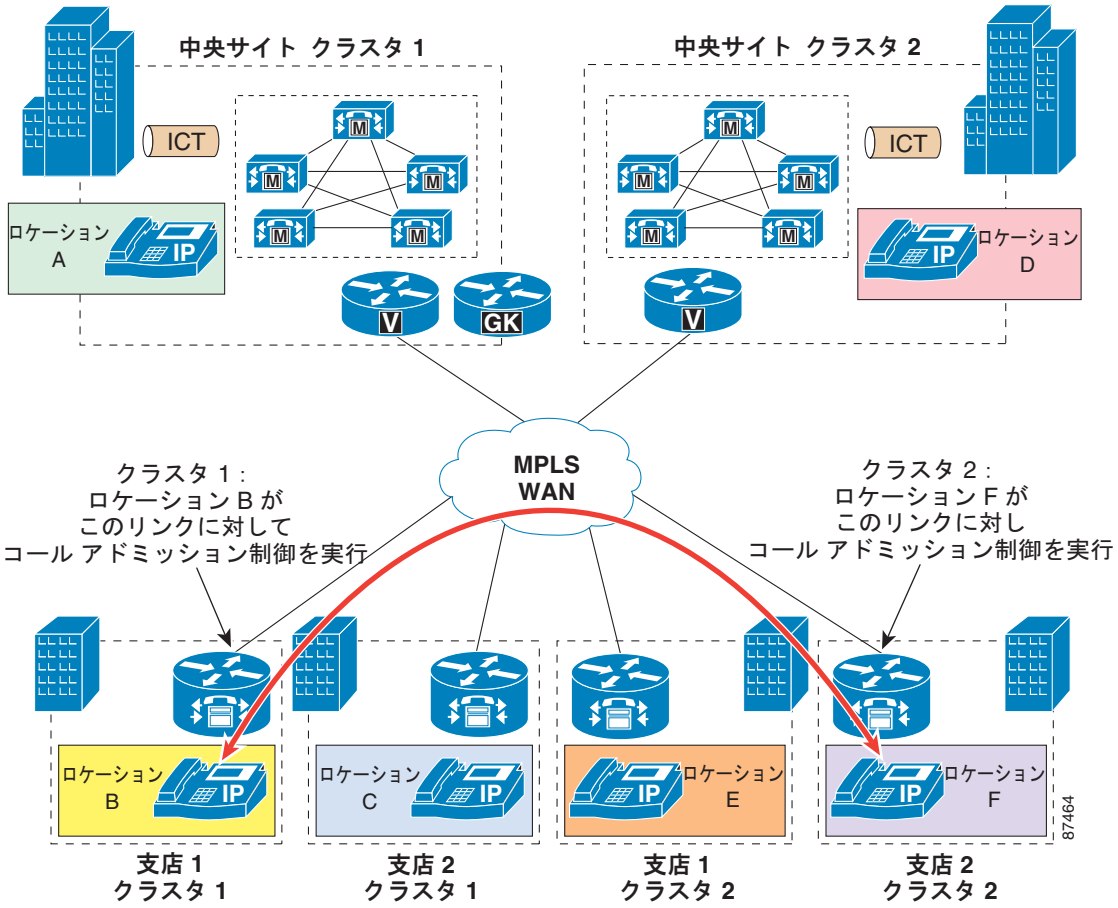
図 9-32　MPLS を使用した分散型配置におけるゲートキーパー コール アドミッション制御



支店サイトが必要な配置では、クラスタ間のダイヤル プランの解決にゲートキーパーを使用することもできますが、コール アドミッション制御にはゲートキーパーを使用しないことをお勧めします。

異なるクラスタに属している支店間にコールが発生した場合は、音声パスはその支店間で直接確立できるので、支店のクラスタから中央サイトへメディアを転送する必要はありません。したがって、コール アドミッション制御は各支店の WAN リンクに対してのみ必要です。（図 9-33 を参照）。

図 9-33　クラスタ間トランク（ICT）によるマルチ クラスタ接続



Unified CM の集中型配置で見られるように、メディアを各サイトで終端するデバイス（各クラスタに対する中央サイトを含む）は、適切に設定されているロケーションに指定されている必要があります。

クラスタ間トランクで重要なことは、これは単なるシグナリング デバイスであって、クラスタ間トランクのメディアを転送する役目をもたないということです。したがって、クラスタ間トランクのロケーションの指定は、Hub_None のままにしておきます。トランクが MTP を必要とする場合は例外です。この場合は、トランクと MTP の両方を、それらが存在するサイトのロケーションに配置する必要があります。

特定のサイトに許されている帯域幅を消費してしまっている場合は、次の 2 つの方式を組み合せて、公衆網へ自動的にフェールオーバーすることができます。

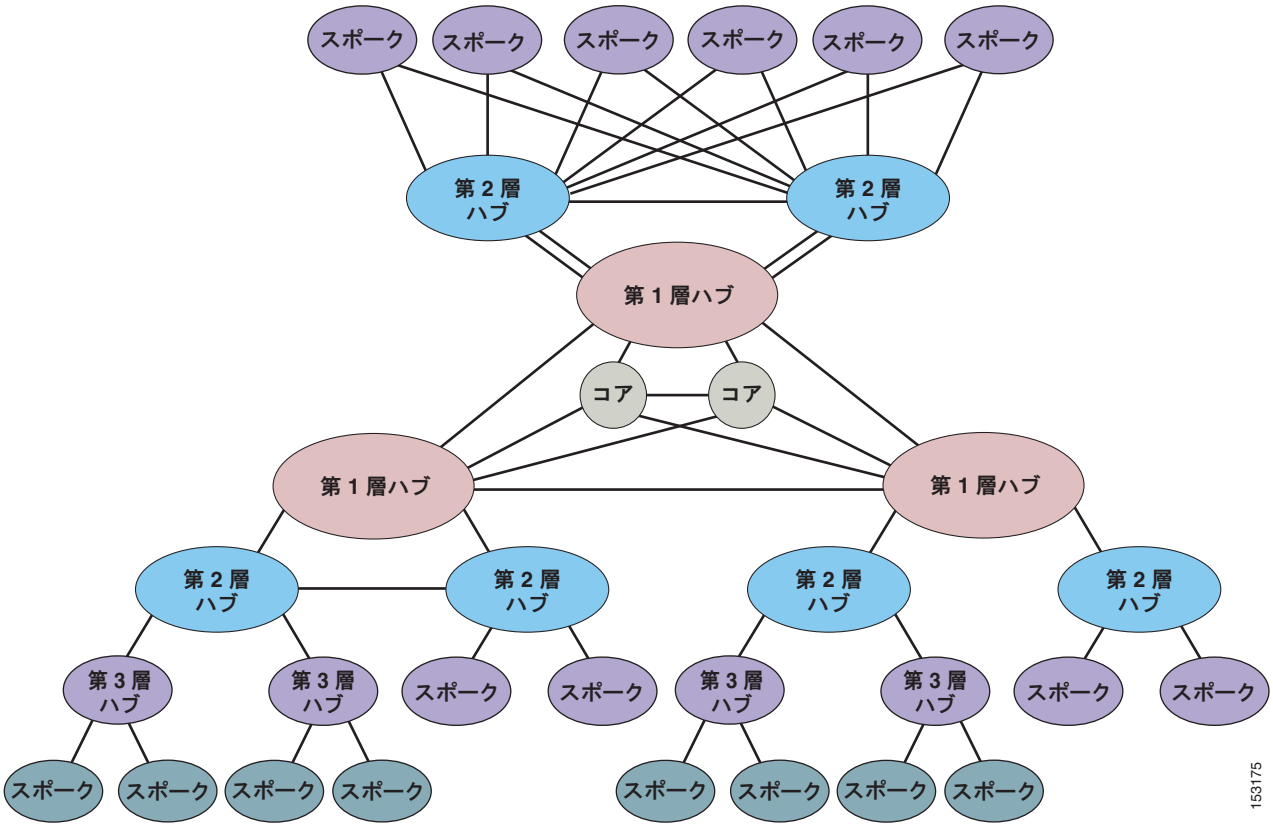
- マルチ Unified CM クラスタに対するコールには、ルート リストおよびルートグループで対応
- Unified CM クラスタ内のコールには、Automated Alternate Routing（AAR）機能で対応（AAR の詳細については、「Automated Alternate Routing」（P.10-87）を参照してください）

汎用トポロジ

この章の説明における汎用トポロジとは、単純なハブアンドスポーク、2 層ハブアンドスポーク、または単純な MPLS ベースのネットワークに変換できないネットワーク トポロジです。

図 9-34 に示すように、汎用トポロジでは、フルメッシュの機能、ハブアンドスポークの機能、部分メッシュの機能、またはこれらのすべての組み合せを 1 つのネットワーク内で実現できます。これは、サイト間の二重接続、および 1 つのサイトから別のサイトへのマルチ パスを表すこともあります。

図 9-34　汎用トポロジ



このようなネットワークは複雑な性質を持つため、RSVP に基づくトポロジ対応コール アドミッション制御メカニズムを採用する必要があります。このメカニズムは、特にトポロジの形態が次のような場合に、帯域幅を適切に制御できます。

- さまざまなハブ サイトにデュアル ホーム接続されたリモート サイト
- プライマリ/バックアップ設定またはアクティブ/アクティブ ロード バランシング設定のいずれかによる、任意の 2 つのサイト間の複数の IP WAN リンク
- 冗長ハブまたは専用接続を備えたデータ センター
- フル メッシュ構造のコア ネットワーク
- 任意の 2 つのサイト間の複数の等コスト IP パス
- 多層アーキテクチャ

以降では、採用する Unified CM 配置モデルごとに、汎用ネットワーク トポロジに関する設計上のベスト プラクティスを示します。

- 「集中型の Unified CM 配置」（P.9-53）

  1 つまたはそれ以上の Unified CM クラスタを特定のサイトに配置し、その他のすべてのサイトにはエンドポイントとゲートウェイだけを配置します。

- 「分散型の Unified CM 配置」（P.9-56）

  Unified CM クラスタを複数のサイトに配置し、その他のすべてのサイトには、エンドポイントとゲートウェイだけを配置します。

集中型の Unified CM 配置

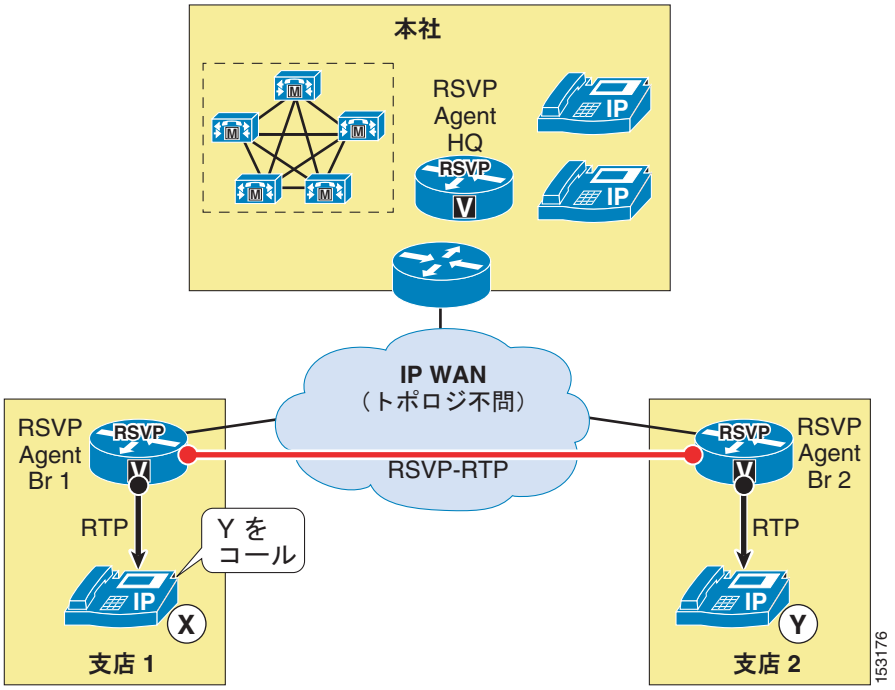
汎用トポロジを使用した Unified CM の集中型配置は、次の 2 つのサブタイプに分類できます。

- 「単一の Unified CM クラスタ」（P.9-53）
- 「同じ場所にある Unified CM クラスタ」（P.9-54）

単一の Unified CM クラスタ

この項の推奨事項は、図 9-35 に示すように、汎用ネットワーク トポロジで採用される単一の Unified CM クラスタに適用されます。

図 9-35　汎用トポロジにおける単一の Unified CM クラスタ



このタイプの配置には、次の考慮事項が適用されます。

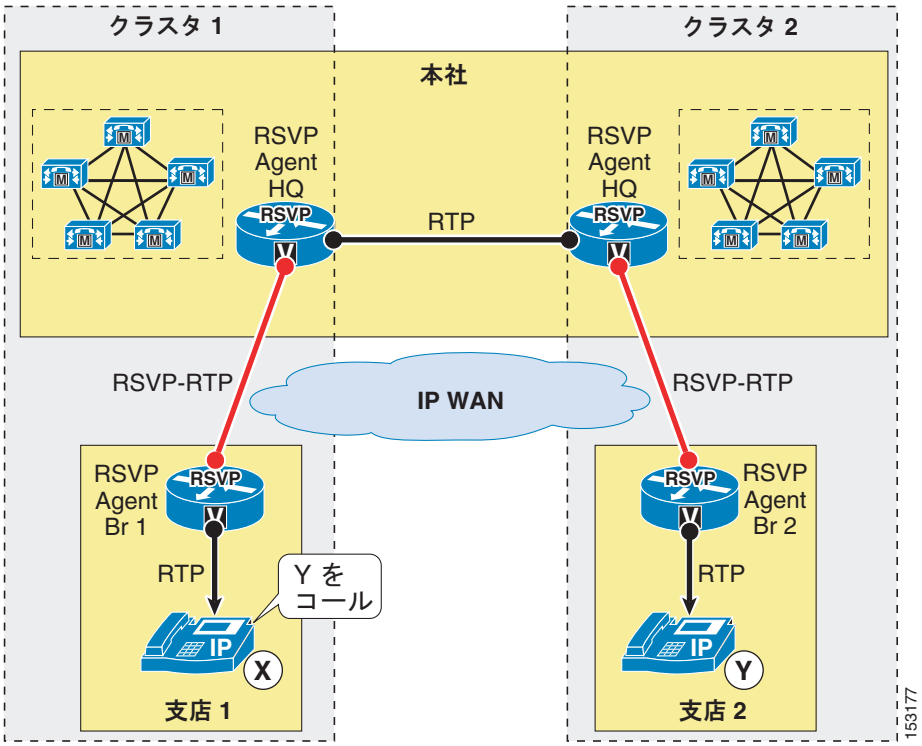
- Unified CM が存在する中央サイトなど、各サイトの Cisco IOS ルータで Cisco IOS RSVP Agent 機能を有効にします。比較的小さなサイトでは、このルータは IP WAN ルータおよび公衆網ゲートウェイと一体になっていることがあり、比較的大きなサイトでは異なるプラットフォームとなっている場合があります。
- Unified CM で、各サイトのロケーションを定義し、すべての帯域幅の値を **Unlimited** のままにします。
- 各サイトにあるすべてのデバイスを適切なロケーションに割り当てます（これにはエンドポイント、ゲートウェイ、会議リソース、および Cisco RSVP Agent 自体が含まれます）。
- 各 Cisco RSVP Agent が、そのサイトのすべてのデバイスのメディア リソース グループ リスト（MRGL）のメディア リソース グループ（MRG）に属するようにします。
- Unified CM サービス パラメータで、**Default inter-location RSVP Policy** を **Mandatory** または **Mandatory (video desired)** に設定し、**Mandatory RSVP mid-call error handle option** を **Call fails following retry counter exceeded** に設定します。
- 輻輳が発生する可能性のあるネットワークですべての WAN インターフェイス上の RSVP を有効にし、プライオリティ キューのプロビジョニングに基づいて RSVP 帯域幅を設定します（「RSVP 設計上のベスト プラクティス」（P.3-59）を参照）。
- 音声コールとビデオ コールに対して個別に帯域幅をプロビジョニングする必要がある場合は、同じ WAN ルータ インターフェイス上で RSVP アプリケーション ID も設定する必要があります。
- Cisco RSVP Agent が IP WAN ルータと共存していない場合、そのエージェントを WAN ルータに接続する LAN インターフェイスで RSVP を有効にします。

同じ場所にある Unified CM クラスタ

この項の推奨事項は、複数の Unified CM が同じ LAN または MAN にある配置に適用されます。Unified CM クラスタが存在するサイトが、高速リンクを通じて接続されている場合は、同じ考慮事項が有効なこともあります。ただし、そのリンクのプライオリティ キューに輻輳が発生せず、音声とビデオ用の帯域幅を無制限と見なせることが条件になります。

図 9-36 では、所定のサイト（本社）にある 2 つの Unified CM クラスタ、およびエンドポイントとゲートウェイを持つ複数のリモート サイトの配置を示しています。これらのリモート サイトは、クラスタ 1（たとえば支店 1）またはクラスタ 2（たとえば支店 2）のいずれかによって制御されます。

図 9-36　汎用トポロジにおける同じ場所にある Unified CM クラスタ



「単一の Unified CM クラスタ」（P.9-53）に示すガイドラインに加えて、このタイプの配置では次のベスト プラクティスに従ってください。

- 各クラスタに対して、クラスタ間トランクを定義して他のクラスタとの通信を有効にします。ゲートキーパーはダイヤル プラン解決のために使用できますが、コール アドミッション制御のためには不要です。
- 中央サイト（図 9-36 の例では本社）にあるすべてのデバイスで使用される同じロケーションにクラスタ間トランクを割り当てます。
- クラスタ間トランクが、MRGL を指定するデバイス プールに割り当てられるようにします。この MRGL は、中央サイトにある Cisco RSVP Agent（図 9-36 のクラスタ 1 では Cisco RSVP Agent HQ 1）を含む MRG を指します。
- クラスタ内でコール アドミッション制御に障害が発生した場合に備えて、AAR 機能を使用して自動公衆網フェールオーバーを提供します。
- クラスタ間でコール アドミッション制御に障害が発生した場合に備えて、ルート リストとルート グループ コンストラクトを使用して、自動公衆網フェールオーバーを提供します。
- メディア トラフィックとシグナリング トラフィックの両方は、異なるクラスタに属する 2 つの支店サイト間のコールに対して、中央サイトを通じたヘアピンになります（図 9-36 に示すように支店 1 の電話機 X と支店 2 の電話機 Y 間のコールは本社サイトを通じたヘアピンになります）。

分散型の Unified CM 配置

汎用ネットワーク トポロジで Unified CM の分散型配置にコール アドミッション制御を提供するには、関係する Unified CM クラスタの数によって、次の 2 つの方法が可能です。

- 「リモート Cisco RSVP Agent による方法」（P.9-57）

  このソリューションは、帯域幅に制限のある IP WAN で接続された異なるサイトに、3 つ以下の Unified CM クラスタが配置される場合に適用されます。

- 「Cisco Unified Border Element による方法」（P.9-60）

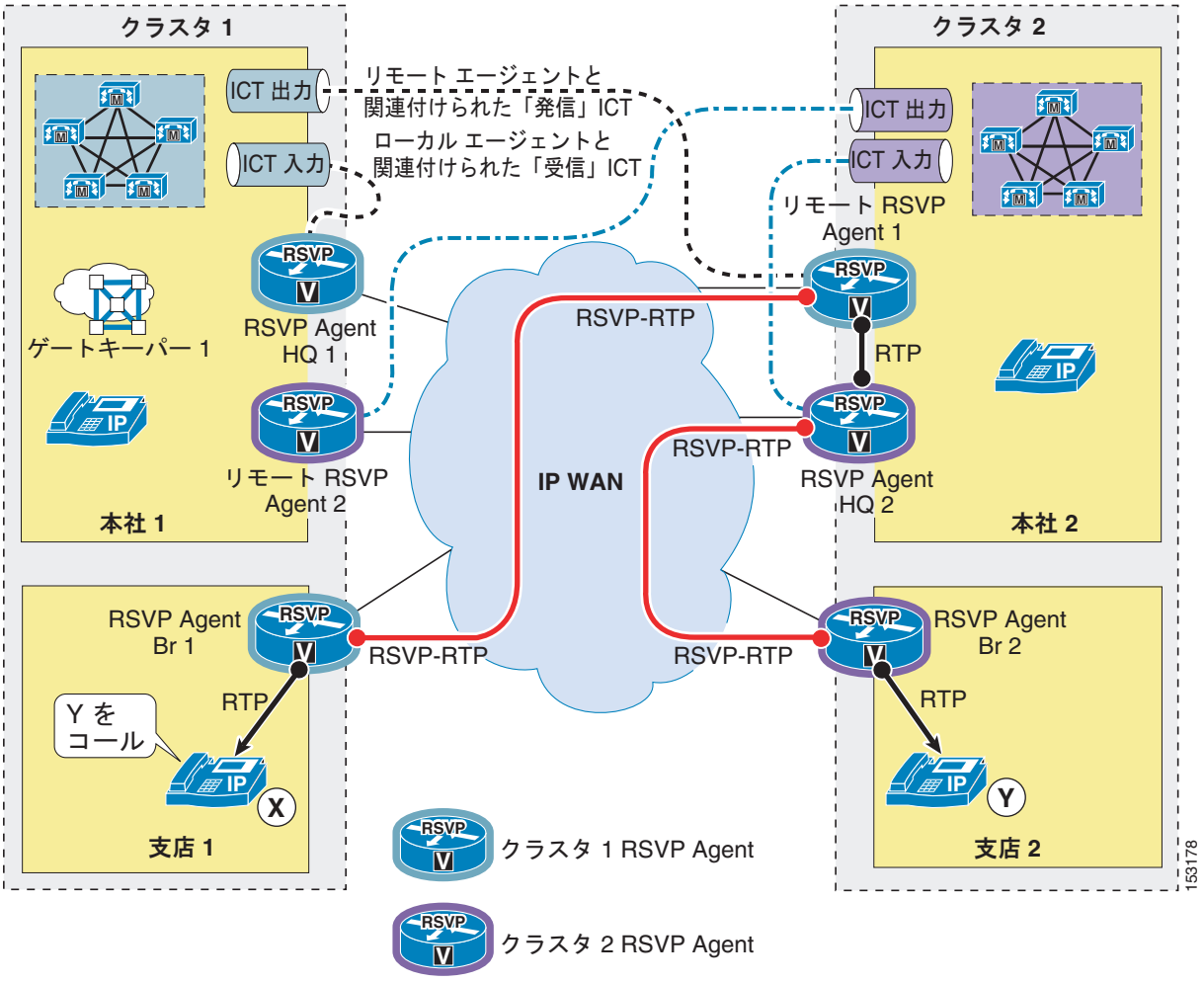
  このソリューションは、帯域幅に制限のある IP WAN で接続された異なるサイトに、任意の数の Unified CM クラスタが配置される場合に適用されます。

（注）　高速 IP WAN で接続されたサイトに Unified CM クラスタが配置される場合は、「同じ場所にある Unified CM クラスタ」（P.9-54）の項にある説明のように、このシナリオを扱うことができます。ただし、IP WAN リンクのプライオリティ キューに輻輳が発生しないことが条件になります。

リモート Cisco RSVP Agent による方法

異なるサイトに 3 つ以下の Unified CM クラスタが配置された汎用トポロジでコール アドミッション制御を提供するには、図 9-37 に示すように、「リモートの」Cisco RSVP Agent を定義することで、RSVP 対応ロケーションの概念を拡張してクラスタ間コールに対応できます。

図 9-37　汎用トポロジでの分散型クラスタ用のリモート Cisco RSVP Agent による方法



（注）　簡単にするため、この項の説明は図 9-37 に示すように、2 つの Unified CM クラスタの例に基づいています。3 つの Unified CM クラスタの配置については、項の末尾に注記を示しておきます。

「単一の Unified CM クラスタ」（P.9-53）の項に示すガイドラインに加えて、このような配置では次のベスト プラクティスに従ってください。

- 各クラスタでは、他のクラスタとの通信を可能にする 2 つのクラスタ間トランク（ICT）を定義します。1 つは「発信」クラスタ間トランク、もう 1 つは「着信」クラスタ間トランクです。
- ダイヤル プラン解決のために（コール アドミッション制御ではなく）Cisco IOS ゲートキーパーを設定し、Unified CM クラスタあたり 1 つのゾーンを定義します。次の例を参考にしてください。

```
gatekeeper
  zone local cluster1 customer.com 10.10.10.10
```

```
  zone local cluster2 customer.com
```

- 各クラスタでは、そのクラスタの通常ゾーン内のゲートキーパーに着信トランクを登録します（たとえば、クラスタ 1 の着信トランクはゾーン cluster1 に登録し、クラスタ 2 の着信トランクはゾーン cluster2 に登録します）。
- 各クラスタで、特別に作成したゾーン内のゲートキーパーに着信トランクを登録します。次の例を参考にしてください。

```
gatekeeper
  zone local cluster1 customer.com 10.10.10.10
  zone local cluster2 customer.com
  zone local cluster1-to-cluster2 customer.com
  zone local cluster2-to-cluster1 customer.com
```

- 他のクラスタに対する発信コールが着信クラスタ間トランクを使用するように、Unified CM ダイヤル プランを設定します（たとえば、クラスタ 1 では、ルート リストとルート グループ コンストラクトを通じて発信トランクを指す 2XXX ルートを設定します）。
- 特定のクラスタを宛先とするコールがその着信トランクにルーティングされるように、ゲートキーパー ダイヤル プランを設定します。次の例を参考にしてください。

```
gatekeeper
  zone local cluster1 customer.com 10.10.10.10
  zone local cluster2 customer.com
  zone local cluster1-to-cluster2 customer.com
  zone local cluster2-to-cluster1 customer.com
  zone prefix cluster1 1...
  zone prefix cluster2 2...
```

- そのサイトに配置されているすべてのデバイスと同じロケーションに着信トランクを割り当てます（たとえば、クラスタ 1 の着信トランクは本社 1 のロケーションに割り当て、クラスタ 2 の着信トランクは本社 2 のロケーションに割り当てます）。
- 新しく作成したロケーションに発信トランクを割り当てます（たとえば、クラスタ 2 に向かうクラスタ 1 の発信トランクは本社 2 に対するリモートのロケーションに割り当て、クラスタ 1 に向かうクラスタ 2 の発信トランクは本社 1 に対するリモートのロケーションに割り当てます）。
- Unified CM が設置されている 2 つの各サイトで、ローカル クラスタに登録された Cisco RSVP Agent のインスタンスを配置します（たとえば、本社 1 サイトに Cisco RSVP Agent HQ1 を配置し、本社 2 サイトに Cisco RSVP Agent HQ2 を配置します）。
- 該当のサイトに配置されているすべてのデバイスと同じロケーションにローカル Cisco RSVP Agent を割り当てます（たとえば、Cisco RSVP Agent HQ1 は本社 1 のロケーションに割り当て、Cisco RSVP Agent HQ2 は本社 2 のロケーションに割り当てます）。
- 各クラスタで、デバイス プールを通じて着信トランクによって使用される MRGL など、中央サイトに配置されたすべてのデバイスの MRGL に含まれる MRG にローカル Cisco RSVP Agent を割り当てます。
- Unified CM クラスタが存在する 2 つの各サイトで、その他の Unified CM クラスタに登録された Cisco RSVP Agent のインスタンスを追加します（たとえば、リモート Cisco RSVP Agent 1 はクラスタ 1 に登録され、本社 2 サイトに配置されます（このサイトにはクラスタ 2 があります）。一方、リモート Cisco RSVP Agent 2 は クラスタ 2 に登録され、本社 1 サイトに配置されます（このサイトにはクラスタ 1 があります）。
- 発信トランク用に作成されたロケーションに、これらのリモート Cisco RSVP Agent を割り当てます（たとえば、リモート Cisco RSVP Agent 1 はクラスタ 1 内の本社 2 に対するリモートのロケーションに割り当て、リモート Cisco RSVP Agent 2 はクラスタ 2 内の本社 1 に対するリモートのロケーションに割り当てます）。

- 各クラスタで、（デバイス プールを通じて）発信トランクで使用される MRGL に含まれる MRG に、リモート Cisco RSVP Agent を割り当てます。

（注）　論理的には区別されますが、リモート Cisco RSVP Agent インスタンスは、他のクラスタに登録されたローカル Cisco RSVP Agent と同じルータ プラットフォームに存在することがあります。たとえば、図 9-37 で、リモート Cisco RSVP Agent 1 と Cisco RSVP Agent HQ2 が実際に同じルータ プラットフォーム上に配置されている可能性があります。また、リモート Cisco RSVP Agent 2 と Cisco RSVP Agent HQ1 についても同じことが当てはまります。

図 9-37 で、支店 1 の電話機 X が支店 2 の電話機 Y にコールを発信した場合、Unified CM クラスタ 1 は、発信トランクを通じてゲートキーパーにそのコールをルーティングします。電話機 X は支店 1 のロケーションに割り当てられ、発信トランクは本社 2 に対するリモートのロケーションに関連付けられているため、Unified CM クラスタ 1 は、Cisco RSVP Agent Br 1 とリモート Cisco RSVP Agent 1 の間で IP WAN を通じて RSVP 予約を開始します（後者はクラスタ 2 とともに本社 2 に配置されています）。

次に、ゲートキーパーは、そのゾーン プレフィックス設定に基づいて、クラスタ 2 の着信トランクにコールをルーティングします。

その後、Unified CM クラスタ 2 は、（本社 1 のロケーションに関連付けられた）着信トランクおよび（支店 2 のロケーションに関連付けられた）電話機 Y からコールを受信し、Cisco RSVP Agent HQ2 と Cisco RSVP Agent Br 2 の間で IP WAN を通じてもう 1 つの RSVP 予約を開始します。

このコールは、5 つのコール レッグ（リモート RSVP Agent 1 と RSVP Agent HQ2 が共存している場合は 4 つのコール レッグ）にわたって確立され、そのうち 2 つは IP WAN を通過し、RSVP に対応しています。

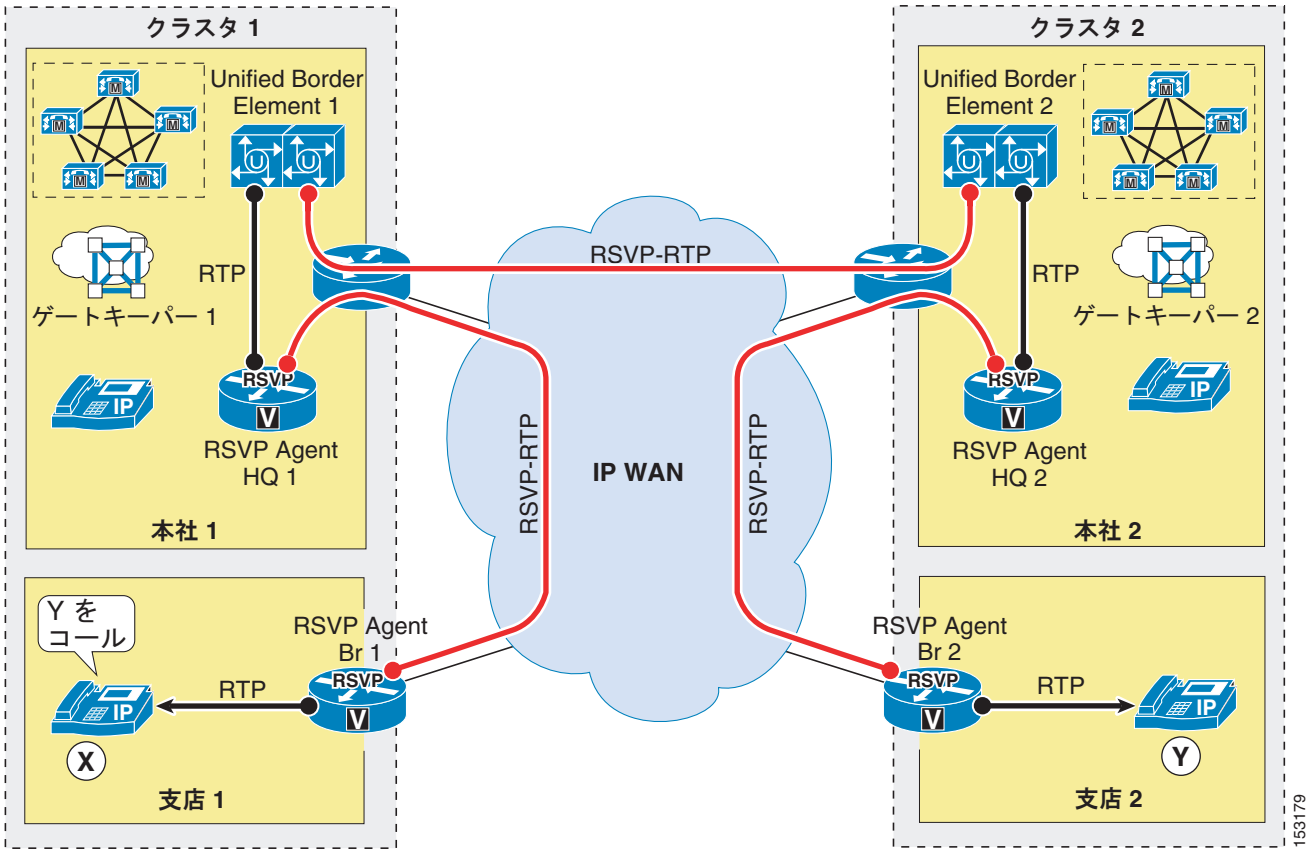
（注）　3 つの Unified CM クラスタのある配置では、同じ検討事項が適用されます。ただし、クラスタあたり 1 つの発信トランクを用意する代わりに、コールされる他の 2 つの各クラスタに対して 1 つずつ、2 つの発信トランクが必要です。同様に、各クラスタには、それぞれ他の 2 つのクラスタの一方に配置される 2 つのリモート Cisco RSVP Agent が必要です。

Cisco Unified Border Element による方法

前の項で説明したリモート Cisco RSVP Agent による方法の複雑さは、Unified CM クラスタの数とともに急速に増大します。したがって、最大 3 つのクラスタに限定されます。

異なるサイトに 4 つ以上の Unified CM クラスタが配置された汎用トポロジでコール アドミッション制御を提供するには、図 9-38 に示すように、クラスタ内のコールに対する RSVP 対応ロケーションと、クラスタ間のコールに対する RSVP 対応 Cisco Unified Border Element を組み合せます。

図 9-38　汎用トポロジでの分散型クラスタ用の Cisco Unified Border Element による方法



「単一の Unified CM クラスタ」（P.9-53）の項に示すガイドラインに加えて、このような配置では次のベスト プラクティスに従ってください。

- 各クラスタに対して、ゲートキーパー制御クラスタ間トランクを定義して、他のクラスタとの通信を有効にします（ゲートキーパー ゾーンはダイヤル プラン解決に使用されますが、このシナリオでコール アドミッション制御のためには必要ありません）。
- そのクラスタの中央サイトに配置されたすべてのデバイスで使用される同じロケーションにクラスタ間トランクを割り当てます。
- クラスタ間トランクが、MRGL を指定するデバイス プールに割り当てられるようにします。この MRGL は、中央サイトにある Cisco RSVP Agent（たとえば、図 9-38 のクラスタ 1 では Cisco RSVP Agent HQ1）を含む MRG を指します。
- 各クラスタで、そのクラスタの中央サイトに 汎用トポロジでの分散型クラスタ用の Cisco Unified Border Element による方法 を配置し、このゲートウェイを有効にして、IP WAN を通じた VoIP コールに RSVP を使用します。

- それぞれのゾーンを宛先または発信元とするすべてのコールに対してローカル汎用トポロジでの分散型クラスタ用の Cisco Unified Border Element による方法 が呼び出されるように、各クラスタで中継ゾーン ゲートキーパーとしてゲートキーパーを設定します（ゲートキーパーは、Cisco Unified Border Element と共存する場合があることに注意してください）。
- クラスタ内でコール アドミッション制御に障害が発生した場合に備えて、AAR 機能を使用して自動公衆網フェールオーバーを提供します。
- クラスタ間でコール アドミッション制御に障害が発生した場合に備えて、ルート リストとルート グループ コンストラクトを使用して、自動公衆網フェールオーバーを提供します。
- メディア トラフィックとシグナリング トラフィックの両方は、異なるクラスタに属する 2 つの支店サイト間のコールに対して、それぞれのクラスタの中央サイトを通じたヘアピンになります（図 9-38 に示すように支店 1 の電話機 X と支店 2 の電話機 Y 間のコールは本社 1 および本社 2 サイトを通じたヘアピンになります）。

（注）　論理的には区別されますが、Cisco RSVP Agent、ゲートキーパー、および Cisco Unified Border Element は、同じルータ プラットフォームに存在することがあります。たとえば、図 9-38 に示すシナリオで、Cisco Unified Border Element 1、ゲートキーパー 1、および Cisco RSVP Agent HQ1 は、Cisco Unified Border Element 2、ゲートキーパー 2、および Cisco RSVP Agent HQ2 と同様に、同じルータ プラットフォームに存在することがあります。

図 9-38 で、支店 1 の電話機 X が支店 2 の電話機 Y にコールを発信した場合、Unified CM のクラスタ 1 は、クラスタ間トランクを通じて ゲートキーパー 1 にそのコールをルーティングします。電話機 X は支店 1 のロケーションに割り当てられ、クラスタ間トランクは本社 1 のロケーションに関連付けられているため、Unified CM のクラスタ 1 は、Cisco RSVP Agent Br 1 と Cisco RSVP Agent HQ1 の間で IP WAN を通じて RSVP 予約を開始します。

次に、ゲートキーパー 1 は、中継ゾーン設定に基づいて Cisco Unified Border Element 1 にコールをルーティングし、Cisco Unified Border Element 1 は、IP WAN を通じて Cisco Unified Border Element 2 と RSVP 予約を確立します。一方、Cisco Unified Border Element 2 は、ゲートキーパー 2 を通じて Unified CM のクラスタ 2 と通信します。

その後、Unified CM のクラスタ 2 は、本社 2 のロケーションに関連付けられたクラスタ間トランクから、（支店 2 のロケーションに関連付けられた）電話機 Y に向けられたコールを受信し、Cisco RSVP Agent HQ2 と Cisco RSVP Agent Br 2 の間で IP WAN を通じてもう 1 つの RSVP 予約を開始します。

このコールは、7 つのコール レッグにわたって確立され、そのうち 3 つは IP WAN を通過し、RSVP に対応しています。

コール アドミッション制御の設計上の推奨事項

ここでは、さまざまな Cisco Unified Communications Manager（Unified CM）配置でコール アドミッション制御を提供するためのベスト プラクティスについて、簡単に概要を示します。

次の推奨事項は、単一の Unified CM クラスタによる配置に適用されます。

- デュアル リンクのない単純なハブアンドスポーク トポロジでは、Unified CM 静的ロケーションを使用します。ハブ サイト デバイスは Hub_None ロケーションのままにします。
- デュアル リンクのない Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）トポロジでは、（中央サイトを含む）すべてのサイトのデバイスを 1 つのロケーションに割り当てて、Unified CM 静的ロケーションを使用します。
- その他のトポロジでは、Unified CM RSVP 対応ロケーションを使用します。サイト間のデフォルト RSVP ポリシーには、**Mandatory** または **Mandatory (video desired)** ポリシーをお勧めします。Cisco RSVP Agent 機能は、比較的小さなサイトでは IP WAN ルータで有効化されている場合もあります。また、比較的大きなサイトではスタンドアロン プラットフォームで実行される場合もあります。

次の推奨事項は、複数の Unified CM クラスタによる配置に適用されます。

- デュアル リンクのない単純なハブアンドスポーク トポロジでは、Unified CM クラスタが存在するサイト間の Cisco IOS ゲートキーパー ゾーンを使用します。
- Unified CM クラスタが第 1 レベルおよび第 2 レベルのハブ サイトに配置された、デュアル リンクのない 2 層ハブアンドスポーク トポロジでは、第 1 レベルと第 2 レベルのハブ サイト間のリンクに Cisco IOS ゲートキーパー ゾーンを使用し、第 2 レベルのハブ サイトとスポーク サイト間のリンクには Unified CM 静的ロケーションを使用します。
- デュアル リンクのない MPLS トポロジでは、すべてのサイトを 1 つのロケーションに配置し、ゲートキーパー ゾーンなしで、Unified CM 静的ロケーションを使用します。MTP が必要な場合を除いて、クラスタ間トランクは Hub_None ロケーションのままにします。クラスタ間コール ルーティング用にはゲートキーパーを使用できますが、コール アドミッション制御では必要ありません。
- その他のトポロジと 3 つ以下のクラスタでは、RSVP 対応ロケーションおよび「リモート エージェント」方法を使用します。
- その他のトポロジと 3 つを超えるクラスタでは、各クラスタ内で RSVP 対応のロケーションを使用し、クラスタ間では RSVP 対応の Cisco Unified Border Element を持つゲートキーパーを使用します。

CHAPTER 10

ダイヤル プラン

ダイヤル プランは、IP テレフォニー システムの重要な要素の 1 つであり、すべてのコール処理エージェントにとって不可欠となる部分です。概説すると、ダイヤル プランは、コールをどのようにルーティングするかをコール処理エージェントに指示する役割を果たします。具体的には、ダイヤル プランは次の機能を実行します。

- エンドポイントのアドレッシング

  システム内部の宛先への到達は、すべてのエンドポイント（IP Phone、FAX マシン、アナログ電話機など）とアプリケーション（ボイスメール システム、自動アテンダント、会議システムなど）にディレクトリ番号（DN）を割り当てることで実現しています。

- パスの選択

  発信側デバイスによっては、同じ宛先に到達する場合でも、複数のパスから選択することができます。また、プライマリ パスが使用不可になっている場合にはセカンダリ パスを使用できます。たとえば、IP WAN に障害が発生した場合は、コールを公衆網を介して透過的に再ルーティングできます。

- コール特権

  特定の宛先へのアクセスを許可または拒否することによって、複数のデバイス グループにそれぞれ別のサービス クラスを割り当てることができます。たとえば、ロビーにある電話からはシステム内部および市内の公衆網宛先にしか到達できないようにし、その一方で、幹部社員の電話からは無制限に公衆網アクセスできるようにします。

- 番号操作

  特定の状況では、ダイヤルされたストリングをコールのルーティング前に操作する必要があります。たとえば、オンネットのアクセス コードを使用してダイヤルされたコールを公衆網を通じて再ルーティングするときや、省略コード（オペレータにつなぐ場合の 0 など）を内線番号に展開するときです。

- コールのカバレッジ

  特殊なデバイス グループを作成し、特定のサービスの着信コールを複数のルール（トップダウン、循環ハント、最長アイドル時間、またはブロードキャスト）に従って処理することができます。

この章では、ダイヤル プランの主な側面について、次の項目を説明します。

- 「Unified CM 7.x におけるダイヤル プラン機能拡張」（P.10-2）

  ここでは、Cisco Unified Communications Manager（Unified CM）7.*x* リリースで導入された、新しいダイヤル プラン機能について説明します（前提条件：この章の他の項で説明されている、ダイヤル プランの概念について理解していること）。

- 「プランニングの考慮事項」（P.10-6）

  この項では、IP テレフォニー ダイヤル プランのプランニングに関係するプロセスを詳しく説明します。取り扱う範囲は、内線番号に使用される桁数から、企業内部のダイヤル プラン アーキテクチャ全般までです（前提条件：ダイヤル プラン一般について、ある程度の知識があること）。

- 「設計上の考慮事項」（P.10-12）

  この項では、マルチサイト IP テレフォニー ネットワーク、エンドポイントのアドレッシング方式、サービス クラスを作成するためのアプローチ、およびコール カバレッジ機能について、設計と配置のガイドラインを示します（前提条件：Cisco Unified Communications Manager および Cisco IOS の操作知識があることを推奨）。

- 「ダイヤル プランの要素」（P.10-58）

  この項では、Cisco Unified Communications ダイヤル プランの要素について詳しく説明します。取り扱うトピックには、コール ルーティングのロジック、コール特権、および各種シスコ製品における番号操作の方法が含まれています（前提条件：Cisco Unified Communications Manager および Cisco IOS の操作知識があることを推奨）。

詳細については、次の Web サイトから入手可能な『*Cisco Unified Communications Manager System Guide*』、『*Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*』、およびその他の製品マニュアルを参照してください。

http://www.cisco.com

この章の新規情報

表 10-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 10-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
Cisco Unified Communications Manager におけるダイヤル プラン機能拡張	「Unified CM 7.x におけるダイヤル プラン機能拡張」（P.10-2）
論理パーティション	「論理パーティション」（P.10-5） 「論理パーティション」（P.10-106）
番号タイプと着信側の設定	「着信側の設定（ゲートウェイ別）」（P.10-4） 「着信側の設定（ゲートウェイ別）」（P.10-75）

Unified CM 7.*x* におけるダイヤル プラン機能拡張

Cisco Unified Communications Manager（Unified CM）7.*x* リリースでは、次の新しいダイヤル プラン機能が導入されました。

- 「ローカル ルート グループ」（P.10-3）
- 「+ ダイヤリングのサポート」（P.10-3）
- 「発番号変換」（P.10-4）
- 「着番号変換」（P.10-4）
- 「着信側の設定（ゲートウェイ別）」（P.10-4）

- 「論理パーティション」（P.10-5）

また、これらの新機能により Unified CM システムで次のことができるようになりました。

- 発信者の物理的な場所に基づいたコールのルーティング。
- International Telecommunication Union（ITU; 国際電気通信連合）の E.164 勧告に記載されているようなグローバル形式で発番号および着番号を表示する。
- ローカル ダイヤリング手順に基づいた形式でユーザへのコールを表示する。
- 発番号、着番号、それらに対応する番号タイプのローカル要件に適合する形式で外部ネットワークへのコール（たとえば公衆網）を表示する。
- 発信番号の数字と番号タイプに基づき、ゲートウェイからの着信コールについての発番号をグローバル形式で生成する。
- 一部の国の法的要件に準拠するため、各エンドポイントのジオロケーションに適用されるポリシーに基づいて、エンドポイント間のコールの確立と通話切替機能の開始を制御する。

新しいダイヤル プランの概要

次の項では、Cisco Unified Communications Manager Release 7.0 で導入された新しいダイヤル プランについて説明します。

ローカル ルート グループ

ローカル ルート グループでは、ゲートウェイへのオフネット コールのパターンを作成する機能を提供します。このパターンは、発信側への近さで選択されます。たとえば、ルート オフネット、特定の国のすべてのサイトに対する国内通話に対して、1 つのパターンを定義できます。すべてのサイトの電話機をこのパターンに一致するように設定できます。このパターンはその後、発信側電話機に関連付けられたローカル ルート グループに基づいて、コールをルーティングします。これによって、サイト 1 の電話機がサイト 1 のゲートウェイを介してコールをルーティングできるようにします。一方、サイト 2 の電話機（こちらも同じパターンを使用）はサイト 2 のゲートウェイを介してコールをルーティングします。

この機能は、Unified CM 7.0 よりも前のリリースと比較した場合、オフネット コールのサイト固有のルーティング設定を簡素化します。

+ ダイヤリングのサポート

電話番号には、他の国から宛先に到達するのに必要な国際ダイヤル アクセス コードを表すために、+ 記号を使用することができます。たとえば、+1 408 526 4000 は、米国にあるシスコ本社の国際表記です。この番号にコールするには、フランスの企業テレフォニー ユーザは通常 0 00 1 408 526 4000 とダイヤルする必要がありますが、英国の発信者は 9 00 1 408 526 4000 とダイヤルする必要があります。いずれの場合でも、+ をそれぞれの発信者に関連のある、適切なオフネット アクセス コード（企業テレフォニー システムで定められているとおり）に、また国際アクセス コード（公衆網キャリアで定められているとおりに）に置き換える必要があります。

Unified CM 7.*x* を使用すると、システムは + で定義された宛先に直接、コールをルーティングできます。たとえば、ユーザは、シスコの米国本社の WiFi 電話の短縮ダイヤル エントリを + 1 408 526 4000 とプログラムし、フランス、英国、または企業内の任意の場所でローミングしているときに、直接ダイヤルすることができます。それぞれの場所で、システムは宛先番号を地域で定められた番号ストリングに変換して、コールが正しくルーティングされるようにします。

この機能によりユーザは、システムを使用して ITU E.164 勧告に記述されている形式で表現される電話番号に変換し、正しくルーティングすることができます。そのためユーザが番号を手動で編集してローカル ダイヤリング手順に適合させる必要はありません。

発番号変換

Unified CM を介してルーティングされるコールに関連付けられている発番号は、電話機または公衆網に表示される前に適合させることが必要な場合があります。たとえば、+1 408 526 4000 からのコールは、宛先の電話機が米国またはカナダにある場合は、発信元が 408 526 4000 と表示されるようにする必要があります。一方、同じ番号からのコールで、宛先の電話機がフランスにある場合は、発信元が 00 1 408 526 4000 と表示されるようにする必要があります。これは主に、地域の公衆網によって定められる慣習的形式で発信側番号が表示されるようにするのが目的で、慣れ親しんだ形式でコールの発信元を識別できます。

ゲートウェイに配信されるコールでは、ゲートウェイが接続している電話通信業者が定める番号に、発番号を適合させる必要があります。たとえば、フランスにあるゲートウェイに配信される +1 408 526 4000 からのコールでは、発信番号を 00 1 408 526 4000 と表し、発番号タイプを International に設定することが必要な場合があります。同様に、カナダにあるゲートウェイに配信される同じ番号からのコールでは、発信側番号を 408 526 4000 とし、発番号タイプを National に設定することが必要な場合があります。

この機能では、発番号を Unified CM システム内のコール ルーティングで使用される形式から、電話機のユーザまたはオフクラスタ ネットワークで定められる形式に適合させることができます。

（注）　一部のサービス プロバイダーでは、機器に技術的な制限、または企業ポリシーや政府の規制の理由から、外国の電話番号を表す発番号を受け付けない場合があります。

着番号変換

Unified CM を介してルーティングされるコールに関連付けられている着信番号は、公衆網に提示される前に適合させる必要がある場合があります。たとえば、カナダにあるゲートウェイを介して公衆網に出る場合、+1 408 526 4000 に対して発信されるコールでは、着番号を 1 408 562 4000 に変換し、番号タイプを National に設定する必要があります。同じコールがフランスのゲートウェイに対して再ルーティングされた場合、着番号を 00 1 408 526 4000 に変換し、番号タイプを International に設定する必要があります。

着番号を操作し、着信番号の番号タイプを設定することによって、この機能では着番号がオフクラスタ ネットワークで定められる形式に適合するようにします。

着信側の設定（ゲートウェイ別）

デジタル インターフェイス（たとえば、ISDN PRI）を介してゲートウェイに着信するときに、コールに関連付けられた発番号もまた、発信番号を Unknown、Subscriber、National、または International のいずれかに区別する番号タイプと関連付けられています。組み合せると、着信コールの発信番号と、それに関連付けられた番号タイプにより、発信者の識別情報を特定することができます。これは、着信コールの発番号に対して適切な数字を除去したり、プレフィックスを付加したりすることにより実行されます。着信側の設定では、4 つの発信番号タイプのそれぞれで、発番号に対して数字を除去したり、プレフィックスを付加したりする個別の組み合わせを適用できるようにします。

たとえば、2 つのコールがドイツのハンブルグにあるゲートウェイに着信するとします。どちらのコールも発番号は 691234567 です。最初のコールは、番号タイプ Subscriber に関連付けられています。これは、発信者がハンブルグにいることを意味します。このためシティ コードはハンブルグの（40）と

なり、国コードはドイツの（49）になります。そのため、着信コールを完全に表すと +49 40 69 1234567 となります。この番号は、番号タイプ Subscriber の着信コールの発番号に対して +49 40 をプレフィックスとして付加することにより得られます。

2 つ目のコールは、番号タイプ National に関連付けられています。これは、発信者がドイツにいることを意味します。そしてこの番号にはすでに適切なシティ コード（69 がフランクフルトのシティ コード）が含まれていますが、国コードはドイツ（49）になります。2 つ目の着信コールを完全に表すと +49 69 1234567 となります。この番号は、番号タイプ National の 2 つ目の着信コールの発番号に対して +49 をプレフィックスとして付加することにより得られます。

この機能によりシステムは、着番号と番号タイプに基づいて着信コールの発番号をグローバル化できます。Unified CM の以前のバージョンでは、これらの設定はクラスタ全体のサービス パラメータを使用することによって実行されました。Unified CM 7.0 では、この機能でゲートウェイごとの設定を取り入れたことにより、番号タイプごとのさまざまなプレフィックスを、異なるゲートウェイに着信するコールに適用できるようになりました。設定は、優先順位順にゲートウェイ上、ゲートウェイのデバイス プール上、またはクラスタ全体のサービス パラメータ上で設定できます。空白のエントリはプレフィックスとして数字が付加されないことを意味します。より優先順位の低い設定から設定を継承するには、エントリを [Default] に設定する必要があります。

所定の番号タイプ内のすべてのコールに対しては、最初に受信された発番号に関係なく、プレフィックスの付加および番号削除の動作が適用されます。

（注） SIP トランク、または SIP ゲートウェイからのコールはすべて発番号タイプ Unknown に関連付けられています。

特に、SIP ゲートウェイおよび SIP トランクに効果的に実装された SIP プロトコルによって、すべてのコールの着番号の番号タイプが Unknown になります。このため、Unified CM では、異なる発番号カテゴリに異なる発番号変更を適用できません。

Unified CM 7.1 では、着信側の設定に Calling Search Space（CSS; コーリング サーチ スペース）の使用が導入されました。これらの CSS を使用することで、発信側トランスフォーメーション パターンに基づいて発信側に変更を適用することができます。これらのパターンでは、正規表現を使用して大文字と小文字を区別したサブセットが照合され、各サブセットに別個の番号操作が実施されます。この新しい機能によって、Unified CM は異なる発番号カテゴリに異なる発番号変更を適用することができます。たとえば、公衆網への接続に使用される SIP トランクは、番号タイプが Unknown に設定されたローカル、国内、および海外からのコールを送信できます。各コールの発番号を使用して、番号タイプ Unknown に関連付けられたトランクの CSS 内の発信側トランスフォーメーション パターンが照合されるので、Unified CM は異なる発番号カテゴリに異なる発番号変更を適用できます。

論理パーティション

インドなどの一部の国には、企業外部でコールを接続するときに、企業の音声インフラストラクチャにローカル公衆網だけを使用することを義務付けた電気通信規制があります。

このため、音声システムを 2 つのシステムに論理的にパーティション化する必要があります。2 つのシステムとは、企業内の Closed User Group（CUG; 非公開ユーザ グループ）通信用とローカル公衆網へのアクセス用です。ロケーション A の企業ユーザからロケーション B の別の企業ユーザへのコールは、CUG システム内で確立できますが、ロケーション A の企業ユーザから公衆網の宛先へのコールは、そのロケーションにかかわらず、ロケーション A の公衆網へのローカル アクセスを経由する必要があります。

既存のダイヤル プラン ツールを使用すると、コールが CUG の外側のエンドポイント間で行われる場合にそのコールを防止できますが、コールが進行しているときにはその新しいコール レッグの確立を防止できません。たとえば、英国ロンドンの企業ユーザが企業ネットワークを介してインドのデリにある同僚にコールするとします。コールが確立されると、デリのユーザは、ロンドンからのコールを受信

した回線と同じ回線からインドのカスタマーとの会議に切り替えることになります。この非公開ユーザ グループ以外の宛先への通話切替（同じ回線上）は、Unified CM 内の既存のダイヤル プラン ツール（コーリング サーチ スペースやパーティションなど）を使用するだけでは防止できません。

Unified CM 7.1 には、論理パーティション機能が導入されました。この機能を利用することで、発信側だけでなく、会議や転送などの通話切替機能にも適用されるポリシーを確立し、実施することができます。

プランニングの考慮事項

ダイヤル プランは、テレフォニー システムの根本となる構成要素です。ユーザがどのように宛先に到達するかを規定する規則を定義しているので、まさにユーザ エクスペリエンスの中心部分になります。このような規則には、次のものがあります。

- 内線番号ダイヤリング：システム上の内線番号に到達するために、何桁ダイヤルする必要があるか。
- 内線番号アドレッシング：内線番号の識別に何桁を使用するか。
- ダイヤリング権限：特定のタイプのコールを許可するかどうか。
- パスの選択：たとえば、オンネット コールには IP ネットワークを使用する。または、国内公衆網コールにはあるキャリアを使用し、国際コールには別のキャリアを使用する。
- ネットワークが輻輳した場合の代替パス自動選択：たとえば、優先使用する国際キャリアがコールを処理できない場合に、国際コールに国内キャリアを使用する。
- 特定番号のブロック：たとえば、有料情報サービスへのコール。
- 着信番号の変換：たとえば、10 桁の番号としてダイヤルされたコールの最後の 5 桁のみを保持する。
- 発信番号の変換：たとえば、公衆網に発信するとき、発信者の内線番号をオフィスのメイン番号に置き換える。

IP テレフォニー システムに適したダイヤル プランは、従来の TDM テレフォニー システム用に設計するダイヤル プランと基本的には違いません。ただし、IP ベースのシステムによって、ダイヤル プランの構造にいくつかの新しい選択肢が生まれています。たとえば、個々のサイトにいるテレフォニー ユーザは、以前はそれぞれ別の独立 TDM システムによって処理されていましたが、IP ベースのテクノロジーは柔軟であるため、1 つの IP ベース システムに包含できるようになりました。このような新しい選択肢が IP ベースのシステムによってもたらされたため、ダイヤル プランの見方を再検討する必要があります。この項では、ダイヤル プランの設計にかかわる要件を正しく導き出すために、システムの設計担当者が検討する必要のあるいくつかの要素について説明します。

ダイヤルされたパターンの認識

ユーザが電話機でダイヤルする番号並びは、一般的にパターンに従っています。たとえば、多くの企業では、同じオフィス ロケーション内で行われるコールに 5 桁の省略ダイヤリング パターンを使用しています。また、多くの企業では、外部へのダイヤリングを表すのに 1 桁のアクセス コードを用い、その直後に何桁かの番号をダイヤルして、ローカル公衆網の番号または長距離公衆網の番号に到達します（たとえば、ローカル番号への到達には 9 に続く 7 桁の番号を使用し、長距離の通話先への到達には 9 の後に 1 と 10 桁の番号をダイヤルします）。

システム管理者は、このようなパターンのシステムによる認識を計画し、あらかじめ決められたパターンに対応するストリングが検出されると同時にシステムが素早く反応し、ユーザがダイヤル後に遅延を感じない（または、その遅延が最小になる）ようにする必要があります。

Skinny Client Control Protocol（SCCP）を使用する電話機、およびダイヤル時に Key Press Markup Language（KPML）を使用する SIP 電話機の場合、Cisco Unified Communications Manager（Unified CM）にパターン認識を実装するには、ルート パターン、トランスレーション パターン、電話機の DN などを設定します。ユーザが 1 つの桁をダイヤルするたびに、電話機から Unified CM へシグナリング メッセージが送信され、一致するパターンを認識する差分処理が行われます。ユーザ入力に含まれる個々のキー操作が収集されるたびに、Unified CM の番号分析は次のような適切なユーザ フィードバックを提供します。

- 電話機が最初にオフフックになったときにダイヤル トーンを再生する。
- 番号がダイヤルされたらダイヤル トーンを停止する。
- 特定の番号のシーケンスがダイヤルされた場合、たとえば、オフネット アクセス コードの 9 がダイヤルされたときなどに、2 次ダイヤル トーンを提供する。

番号のダイヤリングが完了すると、Unified CM はユーザ フィードバックとしてコールプログレストーンを提供します。たとえば、通話先がアラート段階ならばリングバック トーン、通話先が無効であればリオーダー トーンを再生します。

SIP（Session Initiation Protocol）を実行する IP Phone には、設定に SIP ダイヤル規則というパターン認識命令を使用できます。この命令を使用すると、電話機内でパターン認識の大部分のタスクを実行できます。あるパターンが認識されると、SIP 電話機はユーザの入力に対応する番号にコールを発信するために、Unified CM に発信要求を出します。この動作は SIP INVITE と呼ばれ、SCCP プロトコルを実行している IP Phone からのコールと同じように、Unified CM のダイヤル プランによる制御対象となります。ただし、Unified CM の番号分析は完全なダイヤル ストリングを使用して行われます（ユーザが入力したすべての桁が、1 つのブロックとして Unified CM に渡されて処理されます）。この動作モードでは、番号ストリングのダイヤル中のユーザ フィードバックは、電話機が提供できるものだけに制限されます（「SIP ダイヤル規則」（P.10-64）を参照）。ストリングが合成された後も、Unified CM はユーザ フィードバックとしてコールプログレストーンを提供できます。

ダイヤリング手順によるグループ分け

ほとんどのテレフォニー ユーザは、ローカル手順に従って電話番号をダイヤルするのに慣れています。これらはオフィス ロケーション内の宛先へのコール（サイト内コール）、企業内の宛先で異なるサイト間（サイト間コール）、企業外部の宛先（オフネット コール）に適用されるさまざまなダイヤリング ルールで構成されます。これらのさまざまなタイプのコールで使用される形式は、ユーザのプリファレンスおよび地域の公衆網のダイヤリング要件によって異なります。

オンネットとオフネットのダイヤリング

同じテレフォニー ネットワーク上で発信され、終端するコールは、オンネットワーク（オンネット）と見なされます。これとは逆に、A 社で発信され、B 社で終端するコールは、通常は最初に A 社のネットワーク、次に公衆網、最後に B 社のネットワークというように、複数のテレフォニー ネットワークを通じてルーティングする必要があります。発信者から見ると、コールはオフネットワーク（オフネット）でルーティングされています。着信側から見ると、コールはオフネットで発生しています。

TDM システムでは、PBX または Centrex システムがテレフォニー システムのオンネット境界になります。TDM システムは、通常は 1 つのサイトの外側まで伸びていることはありません。伸びている場合も、その TDM システムは、大規模なシステム ハブの外周上に配置されていないサイトを含んでいないのが普通です。

IP テレフォニーの重要な特性の 1 つは、オンネットと見なすことのできるコール境界を拡張する機能です。たとえば、6 つの支店を保有している企業に所属するテレフォニー ユーザが、着信側が同じサイトにいる場合は省略ダイヤリング（4 桁の内線番号など）を使用して同僚にコールし、他のサイトにいる別の同僚にコールするときは、完全な公衆網番号をダイヤルしているとします。IP ベース システムを使用す

ると、すべてのユーザが同じ IP ネットワークで処理されるため、6 つの支店を 4 桁の省略ダイヤリング プランで経済的に結ぶことが可能になります。IP ネットワークを優先パスとして使用し、IP ネットワークが輻輳した場合のセカンダリ パスとして、公衆網への自動オーバーフローを使用します。

省略ダイヤリング

公衆網から直接到達可能な、ダイヤルイン（DID）機能を使用した内線番号があるとします。オフネットの公衆網発信者が DID 内線番号に到達するには、完全修飾公衆網番号（たとえば、1 415 555 1234）をダイヤルする必要があります。しかし、オンネットの発信者については、DID 番号の最後のいくつかの桁をダイヤルするだけでこの内線番号に到達する機能を利用することを考えています。4 桁の省略ダイヤル プランを使用すると、この例のオンネットの発信者は、1234 のみダイヤルすればこの内線番号に到達します。

ダイヤリングは通常、次の 4 種類に分けられます。

- サイト内、オンネットの内線番号ダイヤリング

  多くのシステムで、サイト内での 4 桁または 5 桁のダイヤリングに対応しています。たとえば、カリフォルニア州の San Jose にいるシスコ従業員は、5 桁の番号ストリング 64000 を使用して、シスコの受付番号にコールできます。

- サイト間、オンネットの内線番号ダイヤリング

  たとえば、すべてのシスコ オフィスのシスコ従業員は San Jose の受付番号に 8 526 4000 でダイヤルできます。数字の 8 は、サイト間アクセス コードです。52 は San Jose のサイト コードです。

  この形式は、オンネットでコールをルーティングする、オフネット形式を使用する代替方法よりも短いです（たとえば、カナダにいるシスコ従業員が、オンネットでコールをルーティングして、9 1 408 526 4000 とダイヤルして San Jose のシスコの受付番号に到達できるようになります）。ダイヤリング形式はオフネットの宛先への到達に使用される形式によく似ていますが、システム内のオフネット形式でダイヤルされたオンネットの宛先へのコールを保持するようにシステムは設定されています。

- サイト間、オフネット ダイヤリング

  サイト間のコールのルーティングは公衆網に渡すことができます。たとえば、San Francisco のあるサイトからの、New York の別のサイトへのコールは、上記で説明したオンネットまたはオフネット形式のいずれかでダイヤルできますが、公衆網を介してオフネットでルーティングされます。

- オフネット ダイヤリング

  宛先がオフネットで、会社のダイヤル プランの外部にあるコールの場合、Unified Communications システムでは、ユーザにとってシンプルで、地域で有効なダイヤリング形式を提供する必要があります。

内線ダイヤリングの重複の防止

テレフォニー システムは、どの内線番号にも明確な方法で到達できるように設定する必要があります。この目標を達成するには、ダイヤル プランが次の要件を満たす必要があります。

- すべてのオンネット内線ダイヤリングを、グローバルに一意なものにする。たとえば、4 桁の省略オンネット ダイヤル プランを使用するシステムで、サイト A とサイト B のどちらの内線番号についても、サイト C から 4 桁のみダイヤルして到達することが要件である場合、サイト A に内線番号 1000 があり、サイト B の別の内線番号も 1000 である状態は許されません。
- 個々のダイヤル ストリングは、部分的にも重複していない。

- たとえば、4 桁の省略ダイヤル プランにおいて、9 をオフネット アクセス コードとして使用する場合（公衆網コールを発信する場合など）、内線番号を 9XXX にすることはできません。このように設定すると、コールがすぐにはルーティングされない状況が発生します。たとえば、ユーザが 9141 をダイヤルしたとします。システムは、追加の数字が入力されるか（ユーザが 9 1 415 555 1234 をダイヤルしようとしている場合など）、桁間タイムアウトに達するまで待機し、その後でコールを内線番号 9141 にルーティングします。同様に、オペレータ コード（たとえば 0）を使用する場合にも、0XXX の内線番号範囲全体を 4 桁の固定ダイヤル プランから除外する必要があります。
- 長さが異なっていても、ストリングが重複していることは許されません。たとえば、システムで内線番号 1000 と 10000 を使用すると、1000 にダイヤルする場合、ユーザは桁間タイムアウトに達するまで待たされることになります。

ダイヤリング ストリングの長さ

内線番号にダイヤルするときの必要桁数は、ダイヤル可能な内線番号の数によって決まります。たとえば、4 桁の省略ダイヤル プランでは、内線番号が 10,000 個（0000 ～ 9999）を超える場合には対応できません。0 と 9 をオペレータ コードおよびオフネット アクセス コードとしてそれぞれ予約する場合、この番号範囲は、さらに 8,000 個（1000 ～ 8999）まで減ります。

固定オンネット ダイヤル プラン

ダイヤル プランは、システム内のすべての内線番号に一定の方法で到達するように設計できます。つまり、任意のオンネット発信地点から、特定の内線番号に一定の桁数で到達することができます。ユーザにとって簡潔であるため、固定ダイヤリングを使用することをお勧めします。各種のオンネット ロケーションから発信するときに、番号をダイヤルするための方法をユーザがいくつも覚えておく必要がありません。

たとえば、任意のオンネット ロケーションから 1234 をダイヤルすると電話機 A に着信するとします。この場合、発信側の電話が同じオフィスまたは別のサイトのどちらにあっても、企業のダイヤル プランは固定と見なすことができます。

企業のサイト数が少ない場合は、このアプローチを容易に採用できます。企業の内線番号とサイトの数が多くなるほど、固定ダイヤル プランを設計するときに次の点が問題になってきます。

- 内線番号の数は、ダイヤル プラン用に予定した桁数で対応できる範囲を超える場合もあります。たとえば、8,000 個（内線番号 0XXX と 9XXX を除外するものと想定）を超える内線番号が必要になった場合は、5 桁以上使用する省略ダイヤル プランが必要になります。
- オンネット短縮内線番号を DID 番号と同じものにする場合、地域通信事業者から新しい DID 範囲を取得するときに、その範囲が既存のオンネット省略ダイヤルの範囲と競合してはなりません。たとえば、4 桁の固定省略ダイヤル プランを使用しているシステムに、DID 範囲 415 555 1XXX があるとします。DID 範囲 650 556 1XXX の取得も検討している場合は、オンネット ダイヤリングの桁数を 5 に増やすことが望ましくなります。この例では、5 桁のオンネット範囲 51XXX と 61XXX は重複することがありません。
- ほとんどのシステムでは、一定の範囲をオフネット アクセス コードとオペレータ ダイヤリング用に除外する必要があります。9 と 0 が予約コードになっているシステムで、9 または 0 で始まるオンネット内線番号ダイヤリングに対応できるダイヤル プランは、（固定もそれ以外も）存在しません。つまり、ダイヤル プランで最初の数字として 9 または 0 を使用する必要がある場合は、最初の数字が 9 または 0 である DID 範囲を使用できません。たとえば、5 桁の省略ダイヤル プランを使用する場合、DID 範囲 415 559 XXXX（およびこのサブセット）は使用できません。この例で

は、代替策として、省略ダイヤリングの長さを 6 桁以上に増やすか、末尾の 5 桁が 9 で始まる DID 範囲を使用しないようにするという方法があります。または DID 番号がオンネットの内線番号と一致させる必要もありません。

桁数を選定し、必要な範囲（たとえば、9 または 0 で始まる範囲）を除外したら、残りのダイヤリング スペースをすべてのサイトに分配する必要があります。

ほとんどのシステムでは、2 つの範囲を除外する必要があります。このため、ダイヤル範囲の先頭となる可能性が残っている数字は、8 つです。表 10-2 では、一般的な 4 桁の固定ダイヤル プランにおける、ダイヤリング スペースの分配例を示しています。

表 10-2　一般的な 4 桁固定ダイヤル プランでの番号割り当て

範囲	用途	DID 範囲	DID 以外の範囲
0XXX	除外（0 はオフネット アクセス コードとして使用される）		
1XXX	サイト A の内線番号	418 555 1XXX	適用対象外
2XXX	サイト B の内線番号	919 555 2XXX	適用対象外
3XXX	サイト C の内線番号	415 555 30XX	3[1-9]XX
4[0-4]XX	サイト D の内線番号	613 555 4[0-4]XX	適用対象外
4[5-9]XX	サイト E の内線番号	450 555 4[5-9]XX	適用対象外
5XXX	サイト A の内線番号	418 555 5XXX	適用対象外
6XXX	サイト F の内線番号	514 555 6[0-8]XX	69XX
7XXX	将来的にサポート	XXX XXX 7XXX	7XXX
8XXX	将来的にサポート	XXX XXX 8XXX	8XXX
9XXX	除外（9 はオフネット アクセス コードとして使用される）		

表 10-2 の例では、さまざまなサイトが次の方法に従って番号を割り当てられています。

- サイト A（企業の本社）では、必要な内線番号が 1,000 個を超えるため、2 つの番号範囲（1XXX と 5XXX）全体を確保しています。対応する DID 範囲も、このサイトの地域通信事業者から取得する必要があります。
- サイト B は、1 つの範囲全体（2XXX）を割り当てられているため、内線番号を 1,000 個まで使用できます。
- サイト C も 1 つの範囲全体を割り当てられていますが、100 個の DID 内線番号（415 555 30XX）と 900 個の DID 以外の内線番号に分割されています。DID 内線番号がさらに必要になった場合は、DID 以外の範囲にある、まだ割り当てられていない番号を使用することができます。
- サイト D と E は、4XXX 範囲からそれぞれ 500 個ずつ番号を割り当てられています。対応する DID 範囲は、それぞれのサイトの 4XXX 範囲の部分と一致している必要があります。DID 範囲がサイトごとに異なっているため（おそらく、別の公衆網サービス プロバイダーから取得したことが原因）、サイト間で範囲を分割するには、密接な連携作業が必要です。特定の範囲内で割り当てられるサイトの数が多くなるほど、範囲全体をすべて使用することは困難になり、場合によっては不可能になります。
- サイト F の範囲は、900 個の DID 番号（6[0-8]XX）と 100 個の DID 以外の番号（69XX）に分割されています。
- 範囲 7XXX と 8XXX は、将来の使用に備えて予約されています。

新しいダイヤル プランを実装する場合、プラン立案者の主な目標の 1 つは、電話番号の変更が必要になるのを避けることです。また、既存の電話システムで内線番号範囲が重複している場合、過去に問題がなくても、固定ダイヤル プランでは許容されない場合があります。

可変長のオンネット ダイヤル プラン

サイトの数が多いシステムや、サイトの内線番号範囲が重複しているシステムでは、次の特性を備えた可変長ダイヤル プランを使用すると効果的です。

- サイトの内部では、オンネット内線番号へのコールに対して、省略ダイヤリング（4 桁の内線番号など）を引き続き使用できる。
- サイト間では、ユーザはアクセス コードをダイヤルし、次にサイト コードと宛先のオンネット内線番号をダイヤルする。
- オフネット コールの場合は、アクセス コードの次に公衆網番号をダイヤルする必要がある。

アクセス コードとダイヤル コードを使用すると（表 10-3 を参照）、固定省略ダイヤル プランであれば重複となる内線番号を、オンネット ダイヤル プランで区別できるようになります。

表 10-3　サイト コードの一般的な使用方法

サイト コード	範囲	用途	DID 範囲	DID 以外の範囲
1	1XXX	サイト A の内線番号	418 555 10XX	1[1-9]XX
2	1XXX	サイト B の内線番号	919 555 1XXX	適用対象外
3	1XXX	サイト C の内線番号	907 555 1XXX	適用対象外

表 10-3 では、サイト A、B、C はそれぞれ独自に 4 桁範囲 1XXX を割り当てられています。従来のテレフォニー システムでは、サイト A からサイト B へのコールはオフネット コールとしてルーティングする必要がありました。新しいシステムでは、これらのコールをオンネット コールとしてダイヤルできます。

サイト A からは、ユーザは 1234 をダイヤルするだけで内線番号 1234 に到達できます。一方で、サイト B からサイト A の内線番号 1234 に対して、サイト B にある内線番号 1234 と競合することなく到達するには、ダイヤル プラン側で対応する必要があります。このため、各サイトにサイト コードが割り当てられています。

サイト B から、単にサイト A のコードを目的の内線番号と組み合せてダイヤルすることだけでは不十分です。この場合、11234 はサイト B の内線番号 1123 と部分的に重複しているため、桁間タイムアウトの問題が発生します。代わりに、サイト間オンネット アクセス コードとして 8 を割り当てると、サイト B から 81234 をダイヤルしてサイト A の内線番号 1234 にコールできるようになります。

オンネットのオフサイト内線番号にダイヤルするために必要な桁数は、次の要素によって決まります。

- サイト間アクセス コードに使用する 1 桁
- サイト コードに使用する N 桁（N は、必要となるサイト コードの数に見合う数値。たとえば、システムに 13 のサイトがある場合、サイト コードには少なくとも 2 桁が必要）
- 宛先サイトのローカル ダイヤル プランで必要となる桁数

たとえば、システムに 75 のサイトがあり、各サイトが 4 桁の省略ダイヤリングを使用している場合は、8 + SS + XXXX という形式が必要になります。8 はオンネット アクセス コード、SS は 2 桁のサイト コード、XXXX は 4 桁の内線番号で、合計 7 桁です。

オンネットとオフネットのアクセス コード

ほとんどの企業のテレフォニー システムでは、オフネットの宛先にコールを振り分けるためのオフネット アクセス コード専用として、1 つの数字（たとえば 9）を割り当てることが一般的です。可変長のオンネット ダイヤル プランでは、他のサイトにあるオンネット内線番号宛てのコールをダイヤルするために、オンネット アクセス コードとして、振り分け用の数字（たとえば 8）がもう 1 つ必要です。これらの 2 つのアクセス コードをオペレータ アクセス コード（たとえば 0）とともに使用するので、ダイヤルされたストリングの先頭の数字となる可能性のある 10 個の数字からは、3 つが暗黙的に除外されます。この制限事項は、次の両方の理由から、好ましいものとは言えません。

- ユーザは、オンネットとオフネットの違いを理解し、適切なアクセス コードを選択する必要がある。
- 3 つのダイヤリング範囲全体を除外することによって、著しい制約や、一部の割り当て済み内線番号範囲との競合が生じる恐れがある。たとえば、サイトですでに 8 で始まる省略ダイヤリング範囲を使用している場合、この数字をアクセス コードとして使用するには、変更作業が必要になります。

同じオフネット アクセス コード（たとえば 9）をすでにすべてのサイトで使用しているシステムでは、同じコードをオフネットとオンネットの両方のオフサイト宛先に使用することをお勧めします。このアプローチには、主に次の 2 つの暗黙的要件があります。

- 部分的な重複や待ちが発生することを避けるには、アクセス コードの後に続く桁数を一定にする必要がある。
- テレフォニー システムは、ダイヤルされるすべてのオンネット番号をオフネット番号として認識し、IP ネットワーク経由でルーティングできる必要がある。このタスクは、Unified CM クラスタが 1 つしかない小規模システムの場合は単純ですが、複数の Unified CM クラスタがある大規模システムでは複雑なものになります。

事前の計画

IP ベースのシステムを実装するときは、ユーザの普段の操作手順を変更する必要が生じる場合もあります。新しいシステムのプランニングでは、この実装をできる限りユーザから見えないようにすることが望ましいのですが、それぞれ別のテレフォニー システム上にあった複数のサイトの統合に対応するには、ダイヤリング手順の調整が必要になることもあります。たとえば、企業全体にわたる新しいグローバルなダイヤル プランに対応するには、ユーザが他のサイトにいる別のユーザに到達する方法、サイト内コールに使用している桁数、ときには内線番号までも変更することが必要な場合もあります。ユーザが何度もダイヤル プラン変更を経験することを避けるには、企業規模の拡大を見越しておくようにします。企業が成長すると、複数のダイヤリング リージョンへのサイトの追加、オンネット内線番号の必要数の増加、公衆網番号の再割り当て（たとえば、エリア コードの分割など）、他国への事業展開が発生する可能性があります。

設計上の考慮事項

この項では、マルチサイト配置について、ダイヤル プランの設計に関する次の考慮事項について説明します。

- 「新しいデザイン アプローチ」（P.10-13）では、Cisco Unified Communications システム リリース 7.0 の新しいダイヤル プラン機能を使用して、配置に当てはまるガイドラインとベスト プラクティスを示します。
- 「マルチサイト配置用の設計ガイドライン」（P.10-21）では、すべてのマルチサイト配置モデルに当てはまるガイドラインとベスト プラクティスを示します。

- 「ダイヤル プラン アプローチの選択」（P.10-25）では、固定オンネット ダイヤリングおよび可変長オンネット ダイヤリングのダイヤル プランを作成するためのさまざまなアプローチを紹介し、この 2 番目のオプションについては、分割アドレッシングとフラット アドレッシングを紹介します。
- 「SIP 電話機でのダイヤルされたパターン認識の導入」（P.10-38）では、SIP ダイヤル規則を利用して、SIP 電話機が特定のダイヤリング パターンを認識できるようにする方法について説明します。
- 次の各項では、2 つのダイヤル プラン アプローチについて詳しく分析し、それぞれの設定ガイドラインを示します。
  - 「固定オンネット ダイヤル プランの配置」（P.10-26）
  - 「フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置」（P.10-29）
- 次の各項では、Unified CM でサービス クラスを設定する方法について、2 つの代替方法を示します。
  - 「従来のアプローチによる Unified CM のサービス クラスの構築」（P.10-40）
  - 「回線 / デバイス アプローチによる Unified CM のサービス クラスの構築」（P.10-44）
- 「H.323 を使用している Cisco IOS でのサービス クラスの構築」（P.10-52）では、H.323 プロトコルを実行している Cisco IOS ルータにサービス クラスを実装する方法を説明します。
- 「コール カバレッジの配置」（P.10-55）では、ハント リストと回線グループを使用して Unified CM にコール カバレッジ機能を実装する場合の、ガイドラインとベスト プラクティスを示します。

新しいデザイン アプローチ

Unified CM 7.0 で導入された新機能の組み合せにより、発信元ユーザと通信事業者で定められるローカル形式のコールを受け入れることができるようになり、着信番号と発信番号のグローバル表現を使用してコールをオンネットでルーティングできるようになります。また、宛先のユーザまたはネットワークで定められるローカル形式で電話機またはゲートウェイにコールを送信できます。ダイヤル デザイン アプローチの 3 つの側面は、次のように要約できます。

- 「ローカル化されたコールの着信」（P.10-13）
- 「グローバル化されたコールのルーティング」（P.10-17）
- 「ローカル化されたコールの発信」（P.10-17）

ローカル化されたコールの着信

Unified Communications システム（複数のサイトがさまざまなリージョンまたは国に存在する）では、ユーザのさまざまなダイヤリング手順や、ゲートウェイの接続先のサービス プロバイダーのさまざまなシグナリング要件を満たす必要があります。各地域で異なる場合があるため、システムはローカル ダイヤリング手順とシグナリング要件を、コールが正しくルーティングされる形式に「変換」できるようにする必要があります。そのため、システムは多くのローカル化された着信要件を満たすだけではなく、あらゆる宛先パターンをグローバル化した 1 つの形式も作成する必要があります。

ローカル化されたコールの電話機への着信

電話機またはビデオ端末などのエンドポイントから発信されるコールは通常、ローカル ダイヤリング手順に慣れているユーザによってダイヤルされます。米国内の企業ユーザは、カリフォルニア州 San Jose にあるシスコ本社に到達するために 9 1 408 526 4000 とダイヤルするのに慣れていますが、一方で英国のユーザは 9 00 1 408 526 4000 とダイヤルし、フランスのユーザは 0 00 1 408 526 4000 とダイヤルします。これら 3 つのダイヤル形式は、企業のオフネット アクセス コード（9 は米国、英国、0

はフランス）、国際アクセス コード（00 は英国とフランス、米国の場合、宛先は国内のため必要なし）、宛先番号の表現（国コード（1）を含む）を表します。これら 3 つの各ユーザ グループは、同じグローバル化された宛先番号（+1 408 526 4000）をダイヤルしますが、それぞれのローカル ダイヤリング手順を付加します。これら 3 つの各手順で、ローカル ダイヤリング手順のグローバルな記号として + を使用できます。

企業テレフォニー システムでは、ユーザのローカル ダイヤリング手順を正しく解釈できる必要があります。上記の 3 つの手順すべてで、ユーザはローカル ダイヤリング形式を使用して共通の宛先に到達します。ユーザ入力を認識するようにシステムを設定し、コールが正しい宛先にルーティングされ、送信されるようにします。コールはさまざまな形式で発信される可能性があるため、システムはそれらのさまざまな各形式に一致するパターン認識を用意する必要があります。

Unified CM のトランスレーション パターンはローカル化されたユーザ入力を電話機からダイヤルされたものとして、Unified Communications システム内のコールのルーティングに使用するグローバル形式に変換します。これらのパターンでは、次のものを含む、ローカル化されたすべてのダイヤリング手順が認識されるようにする必要があります。

- サイト内、オンネットのダイヤリング
- オフネットのローカル、国内、国際ダイヤリング
- 緊急コール、ディレクトリおよびオペレータ サービスなどのローカル サービス
- 通信事業者選択コードなど

上で説明した 3 つのコール例の場合、次のトランスレーション パターンが別々のパーティションに設定され、次のコーリング サーチ スペース（CSS）に配置されます。

- 米国の電話：9.1!（ドットの前の番号を削除して、先頭に + を付加します）
- 英国の電話：900.!（ドットの前の番号を削除して、先頭に + を付加します）
- フランスの電話：000.!（ドットの前の番号を削除して、先頭に + を付加します）

いずれの場合でも、地域で有効なダイヤルされたストリングは、グローバル化された形式の + 1 408 526 4000 に変換されます。

同一サイト内の 2 人のユーザ間のコール、または異なるサイト間にいるユーザ間のコールなどのオンネットの宛先の場合、トランスレーション パターンを使用して宛先番号のグローバル化されたオンネット形式を生成する必要があります。サイト コードを使用してオンネット ダイヤリングを行ったり、電話の完全修飾公衆網アドレスをオンネット番号として使用したりしている場合に、該当します。

たとえば、San Jose サイトにいる 2 人のユーザがお互いにコールするために 5 桁の短縮ダイヤリングを使用するとします。ユーザ A は、51234 とダイヤルしてユーザ B にコールします。このサイトで固有のトランスレーション パターンが設定され、5 で始まる 5 桁の任意のストリングが認識されます。そして着信番号はグローバル化されたオンネット形式の 800151234 に変換されます。トランスレーション パターンは、「5XXXX、先頭に 8001 を付加」として設定されます。

システム内の他のサイトにある内線 51234 との混同を避けるため、トランスレーション パターンはサイト固有（San Jose サイトの電話機のみにある CSS に含まれる）である必要があります。上の例では、オンネットのグローバル形式は、サイト間アクセス コード（8）とサイト コード（001）を使用して実装されます。システムがオンネット番号として、電話機の完全修飾公衆網アドレスを使用していた場合、トランスレーション パターンでは先頭に +140855 を付加するのではなく、グローバル化されたオンネット番号の +1 408 555 1234 を生成します。

（注） 設定が簡単になるため、可能な場合は、フラット アドレッシングを使用する可変長のオンネット ダイヤリング（VLOD）を推奨します。分割アドレッシングを使用する VLOD がサポートされていますが、この設定は複雑です。

グローバル形式を使用した着信コールの許可

電話機でも、グローバル形式のダイヤル番号でダイヤルされたストリングを提供します。Cisco Unified Personal Communicator などのソフトウェア エンドポイントの場合、+ ダイヤリングは直接、電話機のテレフォニー ユーザ インターフェイス（TUI）から調整でき、ユーザによるクリックダイヤル アクションから生成できます。タイプ B の IP Phone で、TUI でキーパッドから + をダイヤルできなくても、Missed Calls および Received Calls ディレクトリには + が含まれる番号のエントリが含まれます。ユーザがそれらのディレクトリからダイヤルするとき、Unified CM に入るコールには、+ で始まる着信番号になります。

（注）　タイプ A およびタイプ B 電話機の定義については、「ダイヤル プランの要素」（P.10-58）を参照してください。

電話機のダイヤル プランによってこれらのコールが正しく処理されるようにするには、ローカル化された形式のダイヤル番号だけではなく、グローバル化された形式も許可されるようにする必要があります。図 10-1 に、どのようにこれを実現するかを示します。

図 10-1　ローカル化およびグローバル化された TUI の許可

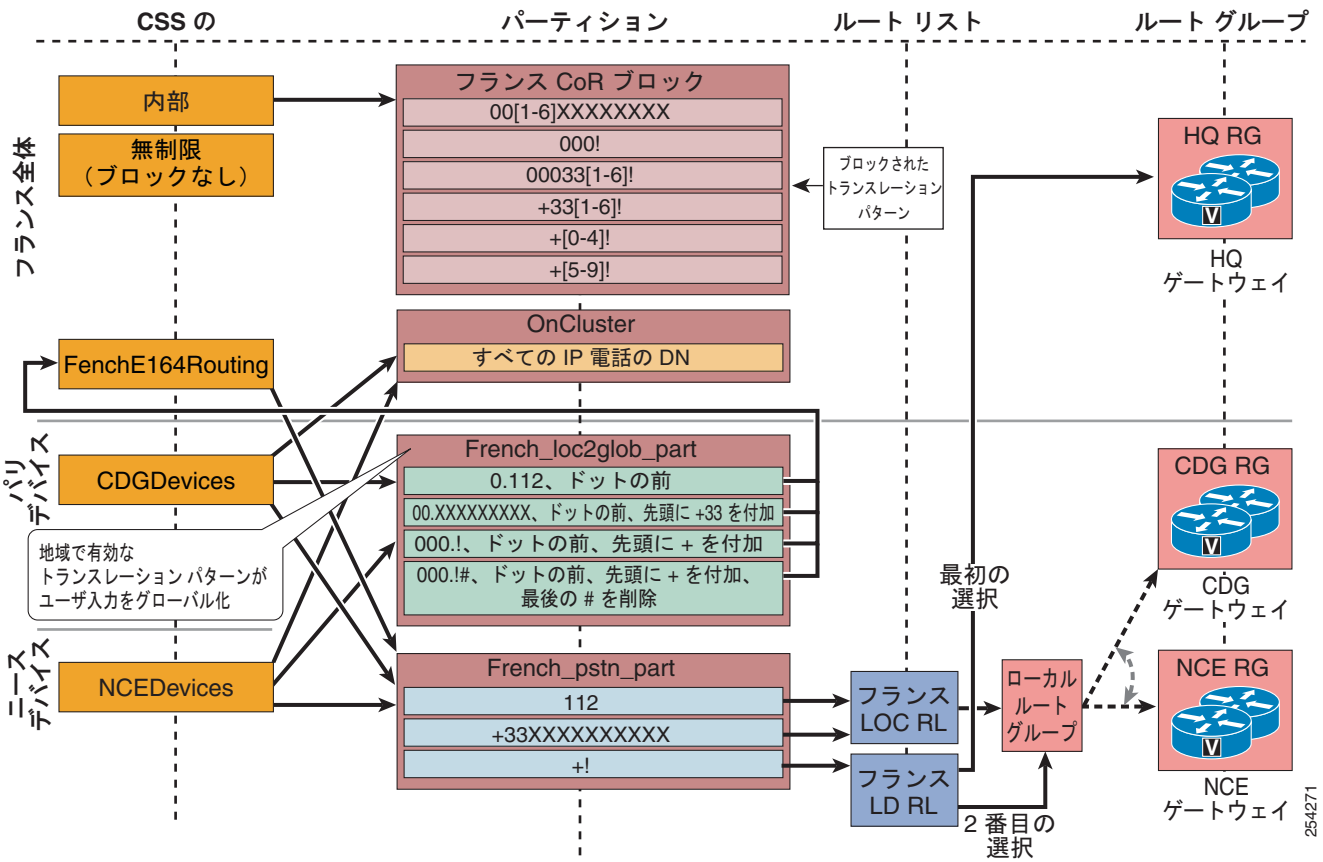


図 10-1 では、フランスの IP Phone ユーザは 0 00 1 408 555 1234 とダイヤルして宛先に接続してから、コールを解除します。着信側はフランスのユーザにコール バックし、接続してから、コールを解除します。その後フランスのユーザは Received コール ディレクトリに移り、最後の受信コールのエントリ（+1 408 555 1234）を選択し、Dial を押します。この例では、フランスのユーザは別々の 2 つのコールを同じ宛先に向けて開始します。最初のコールの場合、フランスのダイヤリング手順に合わせてローカル化された宛先番号の形式が使用されます。対応するトランスレーション パターン 000.! に対して

ユーザ入力がマッチングされます。いったん変換されると、ルーティング パターン +! がコールのルーティングに使用されます。2 つ目のコールの場合、宛先番号のグローバル化された形式が使用され、ルーティング パターン +! が直接使用されます。

サイトごとに設定されているコーリング サーチ スペースでは通常、次のことができます。

- サイトの、ローカル化されたサイト内のダイヤリング手順
- サイトにいるユーザの、ローカル化されたオフネットのダイヤリング手順
- 緊急コールなどの適用できるローカル テレフォニー サービス、ディレクトリおよびオペレータ サービス
- オンネットおよびオフネット番号のグローバル化された形式

上記リストの最初の項目を除いて、コール ルーティングを行うために使用されるローカル化されたパターンは、通常、同一のダイヤリング ドメイン内のサイト間で再利用できます（フランスのすべてのサイトは、オフネットの番号を同じようにダイヤルします。英国のすべてのサイト、米国のサイトなども同じ）。ただし、それぞれのサイトには、独自のサイト内の省略ダイヤリング トランスレーション パターンを設定する必要があります。それは、San Jose にいるユーザが、たとえば 51234 とダイヤルしたときに（New York にいるユーザが 51234 とダイヤルした場合と比べて）、混同しないようにするためです。サイト内形式の省略番号から宛先が同じのグローバル化されたオンネット形式への変換は、サイト固有のトランスレーション パターンを使用して行われる必要があります。このパターンでは、各サイトに、サイト固有のコーリング サーチ スペースが設定されている必要があります。

ローカル化されたコールのゲートウェイへの着信

外部ネットワーク（たとえば、公衆網）による Unified Communications システムに送信される着信番号と発信番号は通常、ローカル化されます。番号の形式は、トランク グループのサービス プロバイダーの設定によって異なります。ゲートウェイが公衆網トランク グループに接続されると、システム管理者は公衆網サービス プロバイダーに問い合せて、この特定のトランク グループで使用される、適切なシグナリング ルールを決定します。トランク グループからシステムにコールが送信されると、発信番号と着信番号についての情報の一部は明示的に、一部の情報は暗黙的に示されます。この情報を使用して、システムはコールのグローバル化された発番号および着番号を生成する必要があります。

着番号のグローバル化は、次の方法のいずれかによって実行できます。

- ゲートウェイ設定で、[Call Routing Information] > [Inbound Calls] の設定を行います。ここで有効桁数を元の着信番号から取得し、プレフィックスをストリング（着信番号のグローバル化に使用する）に追加します。プレフィックスの数字は、適用可能な + 記号および国コード、エリア コード、シティ コードの追加に使用されます。
- ゲートウェイのコーリング サーチ スペースによって参照される、トランスレーション パターンをパーティションに配置します。トランスレーション パターンは、ゲートウェイに接続されているトランクで使用する着番号の形式に一致するよう設定する必要があります。また、グローバル形式に変換する必要があります。プレフィックスの数字は、適用可能な + 記号および国コード、エリア コード、シティ コードの追加に使用されます。

発番号のグローバル化は、着信側の設定を使用して行う必要があります。この設定は、直接ゲートウェイ上で、またはゲートウェイを制御するデバイス プールのいずれかで設定します。

（注） 管理者がプレフィックスを Default に設定した場合、コール処理で次のレベル設定（デバイス プールまたはサービス パラメータ）を使用することを示します。それ以外の場合、フィールドが空白でなければ、設定された値がプレフィックスとして使用されます。フィールドが空白の場合、プレフィックスは何も割り当てられません。

たとえば、シスコの米国本社（+1 408 526 4000）に対して、米国の番号からコールが発信されるとします。そうするとコールはカリフォルニア州 San Jose にあるゲートウェイに送信されます。ゲートウェイに送信された着信番号は 526 4000 です。この情報は、Cisco Unified Communications システムがコールの完全な宛先番号を生成するのに十分です。この特定のトランク グループのサービス プロバイダーによって送信されたコールは、ゲートウェイに接続されたトランク グループの特性に基づいて暗示される国コードとエリア コードを継承します。これは、トランク グループによって処理されたすべての宛先 DID 番号が北米番号計画の国コード（1）、エリア コード 408 を継承していることを前提とします。そのため、この番号の生成されたグローバル形式は +1 408 526 4000 です。ゲートウェイに送信された発信番号は 555 1234 で、番号タイプは Subscriber に設定されています。この番号タイプは、国コードとエリア コードが、トランク グループで設定済みの特性から継承されたものであることを示します。このようにして、システムは発信番号が +1 408 555 1234 であると認識します。

別のコールで、発信番号が 33158405858、番号タイプが International の場合、これは発信番号のグローバル形式が +33158405858 と表現されるということを示します。

グローバル化されたコールのルーティング

すべてのケースに共通のグローバル形式で表現される宛先の場合、すべてのローカル形式を生成できる宛先番号のグローバル形式を採用する必要があります。+ 記号は ITU の E.164 勧告で使用されるメカニズムで、すべての公衆網番号をグローバル一意形式で表現することができます。この形式は、完全修飾公衆網番号と呼ばれることもあります。

システムはルーティング パターン（+ 記号を含むグローバル化された着信番号とマッチングする）を使用して設定できます。このような同一のルーティング パターンは、Standard Local Route Group を示すルーティング リストとルーティング グループを指します。このため、発信エンドポイントのデバイス プールから出口ゲートウェイを特定できるため、グローバルのルーティング パターンを作成することができます。宛先が選択されると、地域設定と要件にコールを適合させるのに必要なすべてのタスク（発番号と着番号）が実行されます。

ローカル化されたコールの発信

着信番号および発信番号のグローバル形式を使用して、コールが宛先にルーティングされる場合、コールが宛先に送信されるときに次のローカル化の操作について考慮する必要がある場合があります。

電話機の発番号のローカル化

コールが電話機に送信されると、発信番号はグローバル形式に変換されます。これは着信側からは認識できません。ユーザは通常、国内の発信者からのコールでは、発信者の番号が省略形式で表示されることを望みます。

たとえば、米国にいるユーザは、米国の発信者からの着信コールが、10 桁の国番号で表示され、+ 記号または国コード（1）がないものを好みます。グローバル電話番号が +1 408 555 1234 のユーザは、+1 408 526 4000 とコールすると、着信番号は、電話が鳴っている間、発番号として 408 555 1234 と表示されます。これを実現するために、システム管理者は発信側トランスフォーメーション パターンを +1.!（ドットの前の番号を削除）と設定する必要があります。発信側トランスフォーメーション パターンは、宛先電話機の発信側トランスフォーメーション パターン CSS（デバイス プール レベルで設定）に含まれるパーティションに配置されます。+1 408 555 1234 からのコールが電話機に送信されると、設定済みの発信側トランスフォーメーション パターンとマッチングされます。これにより +1 が削除され、電話が鳴っているときに発番号が 408 555 1234 と表示されます。

（注） Missed Calls と Received Calls ディレクトリに格納されている発番号は、グローバル化された形式のままのため、ディレクトリに格納された番号ストリングを手動で編集せずに、ワンタッチでダイヤルできます。

（注）　多くの電話機ユーザは公衆網番号のグローバル化形式に慣れつつあります。それは主に、国境を越える携帯電話が一般に使われているためです。システム管理者は、着信番号をグローバル形式で表示させたい場合は、電話機の発信側トランスフォーメーション パターンの設定を行うことができます。

ゲートウェイの発番号のローカル化

コールがゲートウェイに送信されると、発番号は、トランク グループを提供する公衆網サービス プロバイダーの要件に合わせる必要があります（このトランク グループにはゲートウェイが接続されています）。発番号トランスフォーメーション パターンは、発信側番号の番号ストリングと番号タイプの変更に使用できます。通常、ゲートウェイの国コードを示す発番号では、+ 記号を削除し、国コードを明示するように変更する必要があります。また、それらを国のプレフィックスに置き換える必要があります。また、発番号の番号タイプを National に変更する必要があります。ゲートウェイが特定のエリア、シティ コードを示すトランク グループに接続されている場合、+ 記号、国コード、ローカル エリア コードの特定の組み合せは通常、適切なローカル プレフィックスに置き換える必要があります。また、番号タイプは Subscriber にする必要があります。

たとえば、San Francisco のユーザからのコール（+1 415 555 1234）が、最初の選択肢として San Francisco のゲートウェイ、2 番目の選択肢として Chicago のゲートウェイを指定したルーティング リストを介してルーティングされるとします。San Francisco のゲートウェイは 2 つの発信側トランスフォーメーション パターンを使用して設定されます。

- +1415.XXXXXXX（ドットの前の番号を削除）、番号タイプ：subscriber
- +1.!（ドットの前の番号を削除）、番号タイプ：national

コールが San Francisco のゲートウェイに送信されると、発番号は両方の発信側トランスフォーメーション パターンとマッチングされます。ただし、最初のパターンの方がより正確に一致しているため、発番号の処理にはこちらが選択されます。このようにして、変換された番号は 5551234、発信側タイプは Subscriber に設定されます。

ゲートウェイがコールを処理できなかった場合（たとえば、すべてのポートがビジーだった、など）、コールは公衆網に発信するために Chicago のゲートウェイに送信されます。Chicago ゲートウェイは次の 2 つの発信側トランスフォーメーション パターンを使用して設定されます。

- +1708.XXXXXXX（ドットの前の番号を削除）、番号タイプ：subscriber
- +1.!（ドットの前の番号を削除）、番号タイプ：national

コールが Chicago のゲートウェイに送信されると、発番号は 2 番目の発信側トランスフォーメーション パターンのみとマッチングされます。そのため、ゲートウェイに送信される発番号は 4155551234 となり、発番号タイプは National に設定されます。

ゲートウェイの着番号のローカル化

コールがゲートウェイに送信されると、着番号は、ゲートウェイが接続されているトランク グループを提供する公衆網サービス プロバイダーの要件に合せる必要があります。着番号トランスフォーメーション パターンは、着番号と着番号タイプの変更に使用できます。通常、ゲートウェイの国コードを示す着番号では、+ 記号を削除し、国コードを明示するように変更する必要があります。また、それらを国のプレフィックスに置き換える必要があります。また、着番号の番号タイプを National に変更する必要があります。ゲートウェイが特定のエリア、シティ コードを示すトランク グループに接続されている場合、+ 記号、国コード、ローカル エリア コードの特定の組み合せは通常、適切なローカル プレフィックスに置き換える必要があります。また、番号タイプは Subscriber にする必要があります。

たとえば、San Francisco のユーザへのコール（+1 415 555 2222）が、最初の選択肢として San Francisco のゲートウェイ、2 番目の選択肢として Chicago のゲートウェイを指定したルーティング リストを介してルーティングされるとします。San Francisco のゲートウェイは 2 つの着信側トランスフォーメーション パターンを使用して設定されます。

- +1415.XXXXXXX（ドットの前の番号を削除）、番号タイプ：subscriber
- +1.!（ドットの前の番号を削除）、番号タイプ：national

コールが San Francisco のゲートウェイに送信されると、着番号は両方の着信側トランスフォーメーション パターンとマッチングされます。ただし、最初のパターンの方がより正確に一致しているため、着番号の処理にはこちらが選択されます。このようにして、変換された番号は 5552222、着信側タイプは Subscriber となります。

ゲートウェイがコールを処理できなかった場合（たとえば、すべてのポートがビジーだった、など）、コールは公衆網に発信するために Chicago のゲートウェイに送信されます。Chicago ゲートウェイは次の 2 つの着信側トランスフォーメーション パターンを使用して設定されます。

- +1708.XXXXXXX（ドットの前の番号を削除）、番号タイプ：subscriber
- +1.!（ドットの前の番号を削除）、番号タイプ：national

コールが Chicago のゲートウェイに送信されると、着番号は 2 番目の着信側トランスフォーメーション パターンのみとマッチングされます。そのため、ゲートウェイに送信される着番号は 4155552222 となり、着番号タイプは National に設定されます。

（注） コールがゲートウェイに発信されると、発信側および着信側トランスフォーメーション パターンが、発信および着信番号にそれぞれ適用されます。

（注） SIP では番号タイプが示されません。そのため、SIP ゲートウェイでは、Unified CM によって設定された着信側または発信側の番号タイプの表示を受信できません。

新しいデザイン アプローチの利点

Unified CM 7.*x* の新機能により有効になったダイヤル プラン デザイン アプローチの利点は、次のとおりです。

- コールのルーティング、特にローカルから公衆網に発信する場合の簡素化された設定。
- システム機能の簡素化された設定と拡張機能。次のものがあります。
  - Automated Alternate Routing（AAR）
  - Emergency Responder（ER）サイト固有のフェールオーバー
  - Call Forward Unregistered（CFUR）
  - テールエンド ホップオフ（TEHO）
  - Cisco Unified Personal Communicator などのソフト クライアントからの E.164 番号のクリック ダイヤル（+ 記号を含む）
  - ローミング中のエクステンション モビリティ ユーザまたはローミング デバイスから発信された短縮ダイヤルの適合コール ルーティング
  - 電話機ディレクトリ エントリ（デュアルモードの電話機を含む）からのワンタッチ ダイヤリング

- IP Phone ディレクトリの Missed Calls および Received Calls リストからのワンタッチ ダイヤリング

Automated Alternate Routing（AAR）

AAR 宛先マスクがグローバル化された形式に入力されている場合、およびすべての AAR CSS がグローバル化された形式で宛先にコールをルーティングできる場合、システム管理者は AAR グループを設定することができます。それは、この機能が、特定の宛先に到達するために、発信電話機の公衆網アクセスの地域要件に基づいてどの数字をプレフィックスとして付加するかを決定する唯一の機能であるためです。

さらに、ほとんどの場合、この AAR CSS の唯一の機能では、コールを発信電話機と同じ場所にあるゲートウェイにルーティングします。そのため、Standard Local Route Group を含むルーティング リストを指す 1 つだけのルート パターン（+!）を使用して設定できます。この 1 つのルーティング パターンを使用してルーティングされるコールは常に発信エンドポイントに関連付けられた ローカル ルート グループを介してルーティングされるため、どのリージョン、どの国にいるとしても、すべてのサイトのすべての電話でこの 1 つの AAR CSS を使用できます。

Cisco Emergency Responder

Cisco Emergency Responder（ER）へのコールのルーティングは通常、911 CTI ルート ポイントを、プライマリ ER サーバに接続、また 912 CTI ルート ポイントはバックアップ ER サーバに接続するように設定することによって行われます。

どちらの ER サーバも利用できない場合、911 コールは、公衆網が発信側電話機と同じ場所にあるゲートウェイに発信されるように指示できます。設定は次のようにします。

- Call Forward No Answer（CFNA）への 911 CTI ルート ポイントおよび 912 への Call Forward Busy（CFB）、912 CTI ルート ポイントのパーティションを含むコーリング サーチ スペースを介して。
- CFNA への 912 CTI ルート ポイントおよび 911 への CFB、グローバル パーティションを含むコーリング サーチ スペースを介して。グローバル パーティションは Standard Local Route Group を含むルート リストを指す ルート パターン 911 を含む。

どちらの CTI ルート ポイントも登録解除された場合、911 へのコールは、発信電話機のデバイス プールで決定されたとおりにローカル ルート グループに転送されます。デバイス モビリティが設定されている場合、ローミング電話機は訪問したサイトのデバイス プールと関連付けられます。このため訪問したサイトの Local Route Group と関連付けられます。

Call Forward Unregistered（CFUR）

Call Forward Unregistered 機能によって処理されるコールが、発信側電話機と同じ場所にあるゲートウェイを使用するようにするには、電話機の CFUR 宛先を、公衆網番号のグローバル化された + 形式を使用して設定します。CFUR CSS は、標準ローカル ルート グループを指す 1 つのルート パターン（+!）のみを使用して設定できます。この 1 つのルーティング パターンを使用してルーティングされるコールは常に発信エンドポイントに関連付けられたローカル ルート グループを介してルーティングされるため、どのリージョン、どの国にいるとしても、すべてのサイトのすべての電話で同じ CSS を使用できます。

テールエンド ホップオフ（TEHO）

公衆網接続料金を低くするため、システム管理者は、IP ネットワークを使用してオフネットの宛先にコールをルーティングし、公衆網への出口点を着信番号のできるだけ近くにします。同時に、コールの優先 TEHO ルートが使用できない場合、発信電話のローカル ゲートウェイを使用してコールを公衆網に送信する必要がある場合もあります。これは、特定の番号タイプの TEHO ルーティングに参加しているすべての電話で、特定の宛先番号に一致するルート パターンと一致するように設定し、その番号が最初のエントリとして、選択した TEHO 出口ゲートウェイを含むルート リストを、2 番目のエントリとして標準ローカル ルート グループを指すように設定することによって実現できます。

マルチサイト配置用の設計ガイドライン

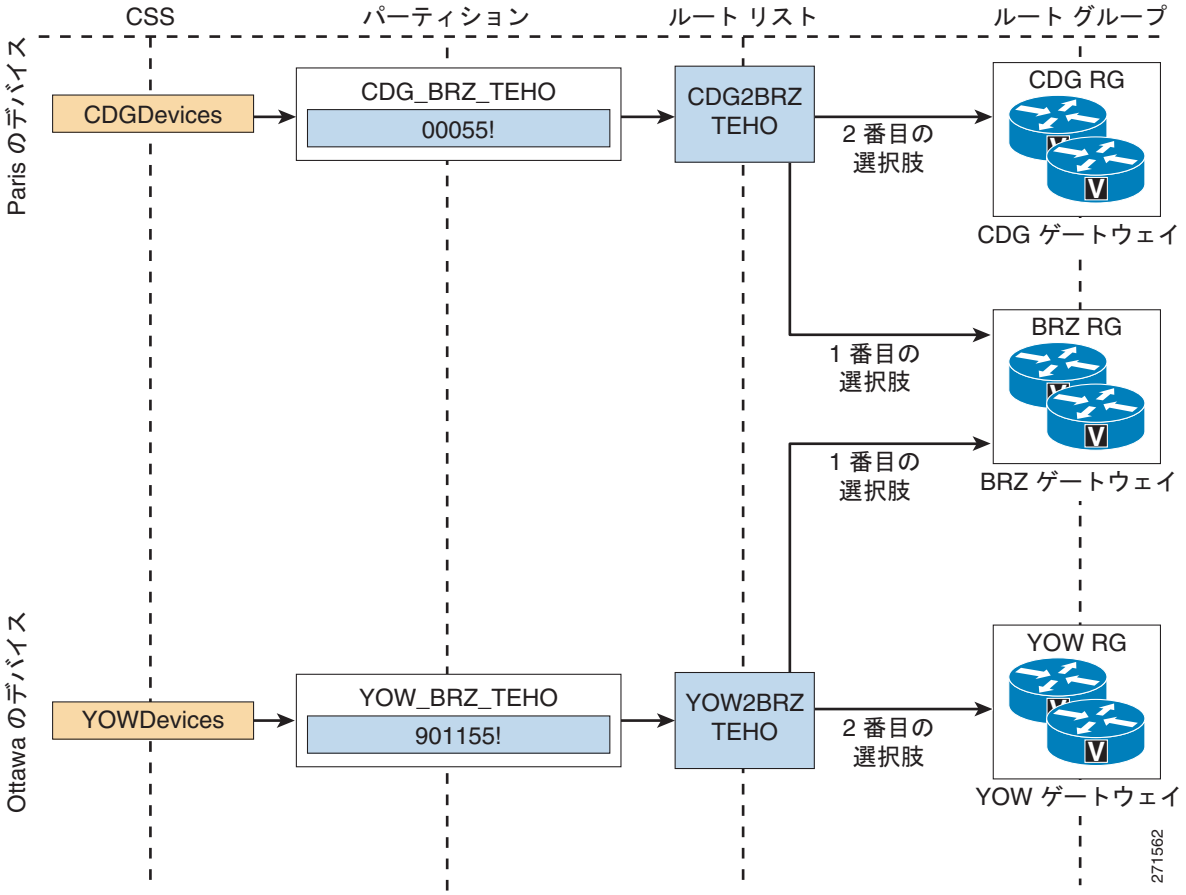
あらゆるマルチサイト IP テレフォニー配置に対して、次のガイドラインとベスト プラクティスが共通して適用されます。複数の Unified CM クラスタが関係する配置については、「マルチクラスタ システムに関する追加の考慮事項」（P.10-24）の項も参照してください。

- ルーティング ループを防ぐには、すべての公衆網ゲートウェイのコーリング サーチ スペースに、同じゲートウェイにコールを送信できるルート リストおよびルート グループに割り当てられている外部ルート パターンが含まれているパーティションを含めないでください。
- 地域通信事業者（LEC）との間で DID 範囲を取り決めるときは、サイト内で重複が発生しない DID 範囲を選択するようにしてください。たとえば、サイト内で 4 桁ダイヤリングを使用していて、1,000 個の DID ブロックが 2 つ必要な場合、ブロック (408)555-1XXX と (408)444-1XXX は 4 桁番号に短縮すると重複し、着信変換と発信変換が実行されるとさらに複雑になります。
- 緊急番号をダイヤルする方法は、複数用意します。たとえば、北米の場合には、911 と 9.911 の両方を Unified CM で緊急ルート パターンとして設定します。
- Automated Alternate Routing（AAR; 自動代替ルーティング）を配置する場合は、IP Phone 上に設定されている外部電話番号マスクまたは AAR 宛先マスクが、各種 AAR グループによって付加されるどのプレフィックスとも競合しないようにする必要があります。たとえば、複数の国にわたる配置の場合、0 などの国内アクセス コードは、それらがグローバル E.164 アドレスの一部でない限り、マスクに含めないでください。AAR を設定する最も簡単な方法は、電話機の完全な E.164 アドレス（+ 記号を含む）として AAR 宛先マスクを設定することです。
- 強制的にオンネットの宛先にダイヤルすることができますが、公衆網コールとしてダイヤルすると、クラスタ内のオンネットにルーティングされます。このためには、各サイトの E.164 DID 範囲に一致するトランスレーション パターンを追加し、このパターンによって、宛先内線番号に一致するように番号を操作します。たとえば、1234 とダイヤルすることによって DN にオンネットで到達可能な場合で、システム内の誰かがこの同じ宛先を 9 1 415 555 1234 とダイヤルしたとき、トランスレーション パターン 9 1 415 555.1XXX（ドットの前のすべての番号を削除し、変換後の番号にオンネットでコールをルーティングします）を作成することにより、強制的にコールをオンネットのままにすることができます。ただし、「オンネット強制」トランスレーション パターンを含んだパーティションを除外し、公衆網を指す標準ルート パターンを含んだパーティションを含むように、AAR コーリング サーチ スペースを設定してください。IP WAN が帯域幅外になったときに自動公衆網フェールオーバーができるようになります。
- N 個のサイトがある集中型コール処理クラスタでは、次のいずれかの方法を使用することで、テールエンド ホップオフ（TEHO）を実装できます。
  - 集中型フェールオーバーを使用する TEHO

    この方法では、N 個のルート パターンをグローバル パーティション内に設定します。各パターンが、適切なリモート サイト ルート グループを最初の選択肢として保持し、中央サイト ルート グループを 2 番目の選択肢として保持しているルート リストを指すようにします。
  - ローカル フェールオーバーを使用する TEHO

この方法では、N 個のルート パターンを N セット、サイト固有のパーティション内に設定します。各パターンが、適切なリモート サイト ルート グループを最初の選択肢として保持し、ローカル サイト ルート グループを 2 番目の選択肢として保持しているルート リストを指すようにします。たとえば図 10-2 では、ブラジル、Paris（フランス）のあるサイトへのローカル フェールオーバー TEHO ルーティングには専用のルート パターン、およびブラジルの TEHO ゲートウェイを最初の選択肢、Paris のゲートウェイを 2 番目の選択肢としてコールをルーティングするためのルート リストが必要です。パターンはサイト固有のルート リストにリンクしているため、他のサイトで再利用することはできません。同様に、Ottawa（カナダ）にあるサイトで、カナダでは、Ottawa 固有のルート リストを指す専用のルート パターンで、Ottawa にあるゲートウェイへのローカル フェールオーバーを許可する必要があります。

図 10-2　ローカル ルート グループを持たない TEHO



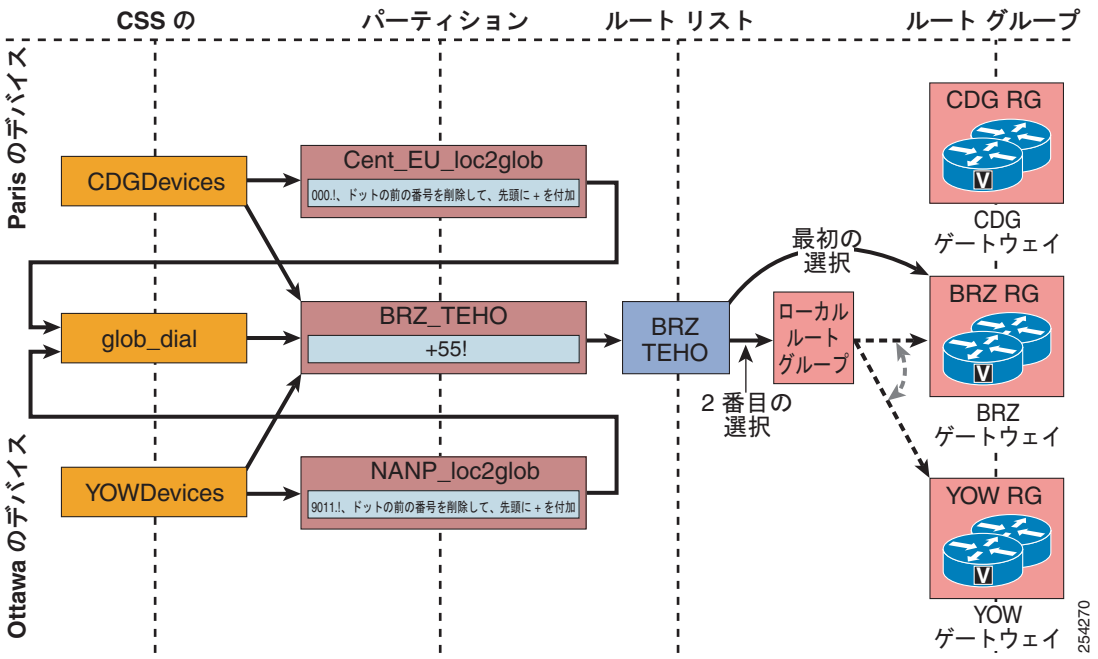
2 番目の方法では、リモート ゲートウェイや IP WAN が使用不可になった場合に、最も優れたフェールオーバー シナリオを実現できる一方で、ダイヤル プランが非常に複雑になります。最初の方法では、必要になるのは N 個のルート パターンと N 個のルート リストであるのに対して、少なくとも N^2 個のルート パターンと N^2 個のルート リストが必要になるためです。

- ローカル ルート グループを持つ TEHO のローカル フェールオーバー

  ローカル ルート グループでは TEHO ルートのローカル フェールオーバーが、サイトごとのルート パターンを作成せずに実装できるようにします。図 10-3 の例の場合、Paris と Ottawa のサイトで単一の TEHO パターンとルート リストが使用されます。これら 2 つのサイトのユーザ入力は同じではないため（フランスのユーザはブラジルの宛先をカナダのユーザとは異なる方法でダイヤルする）、設定は、ユーザ入力をグローバル化するトランスレーション パ

ターンに依存します。最初のエントリがブラジルのルート グループ、2 番目のエントリが標準ローカル ルート グループであるルート リストを指す、単一の、クラスタ全体のルート パターンの照合に、グローバル形式が使用されます。ローカル ルート グループは、発信側デバイスが Paris のデバイス プールにある場合は Paris のルート グループに、発信側デバイスが Ottawa のデバイス プールにある場合は Ottawa のルート グループによって解決されます。

図 10-3　　ローカル ルート グループを持つ TEHO



- 国内の番号計画で許容される場合は、長距離電話としてダイヤルされたローカル公衆網コールを捕捉し、適切な省略形式に変換するための追加トランスレーション パターンを各サイトに設定することをお勧めします。このトランスレーション パターンには、サイト内の電話からのみアクセスできるようにします。このように設定することで、AAR 設定も簡潔化できます（「同じローカル ダイヤリング エリアに複数のサイトがある場合の特別な考慮事項」（P.10-91）を参照）。
- Multilevel Precedence and Preemption（MLPP）機能を使用して、緊急コールに高い優先順位を割り当てないでください。緊急時のコールは、IP テレフォニー システムに緊急コールとして表示されない場合もあります。また、メインの緊急サービス ルーティング番号に新たにコールが発信された場合、既存の緊急コールが終了する恐れがあります。たとえば、緊急時に通常の 10 桁の番号へコールを発信し、医療専門家に連絡することが必要になる場合があります。このコールのプリエンプション処理により、進行中の緊急通信が中止され、緊急時の処理が遅延することがあります。また、救急隊員からの着信コールも MLPP でプリエンプション処理される危険性があります。

（注）　多数のゲートウェイ、ルート パターン、トランスレーション パターン、およびパーティションを含む非常に大きなダイヤル プランを持つ Unified CM クラスタでは、Cisco CallManager Service の初回始動時に、初期化に長い時間がかかる場合があります。デフォルトの時間内にシステムが初期化されない場合、サービス パラメータを変更して、設定の初期化時間を延長してください。サービス パラメータの詳細については、Unified CM Administration オンライン ヘルプのサービス パラメータに関する説明を参照してください。

マルチクラスタ システムに関する追加の考慮事項

複数サイトの配置（複数の Unified CM クラスタを含む）のダイヤルプランを設計する場合は、前の項で説明した考慮事項に加えて、次のベスト プラクティスに従ってください。

- DID 範囲を複数の Unified CM クラスタにわたって分割することは避けます。分割した場合、経路の集約が不可能になり、クラスタ間ルーティングが非常に困難になります。各 DID 範囲は、それぞれ単一の Unified CM クラスタに配置してください。
- 1 つのリモート サイト内にある複数のデバイスを、静的ロケーションに基づいたコール アドミッション制御を使用して複数の Unified CM クラスタに分割することは避けます。静的ロケーション ベースのコール アドミッション制御が意味を持つのは、1 つのクラスタ内のみです。それぞれ別のクラスタに属している複数のデバイスを同じリモート サイトに配置すると、クラスタ間で使用可能な帯域幅を分割する必要があるため、IP WAN 帯域幅が効率よく使用されなくなります。各リモート サイトは、それぞれ単一の Unified CM クラスタに配置してください。RSVP をロケーションのコール アドミッション制御メカニズムとして使用するよう Unified CM に設定できるため、単一サイトの合計 WAN 帯域幅を、さまざまなクラスタに属する電話機間で効率よく共有できます。RSVP ベースのコール アドミッション制御を最も効率よく使用するには、RSVP を使用するよう、リモート サイト内にあるすべての電話機に設定する必要があります。
- Unified CM クラスタ間でのコール ルーティングには、ゲートキーパー制御クラスタ間トランクを使用します。このようにすると、ネットワーク内でクラスタを簡単に追加および修正できるようになり、他のクラスタをすべて再設定しなくても済みます。
- Unified CM とゲートキーパー間の接続には、冗長性を持たせます。このためには、ゲートキーパー クラスタを使用するか、複数のサーバが設定された Unified CM グループを使用しているデバイス プールに対して、クラスタ間トランクを割り当てます。
- コールをゲートキーパーに送信するときは、着信番号を完全な E.164 アドレスへと展開します。このようにすると、IP WAN が使用不可になった場合の公衆網フェールオーバーが簡単になります。これは、コールを公衆網ゲートウェイ経由で再ルーティングするための追加の番号操作が必要ないためです。また、リモート サイトごとのダイヤル長情報を使用してローカル（発信側）Unified CM を設定する必要がなくなります。
- ゲートキーパー内に、Unified CM クラスタごとにゾーンを 1 つ設定します。クラスタ（ゾーン）ごとに、そのクラスタの所有するすべての DN 範囲に一致するゾーン プレフィックス ステートメントを追加します。
- 次のガイドラインに従うと、複数の Unified CM クラスタにわたってテールエンド ホップオフ（TEHO）を実装することができます。
  - 関係する E.164 範囲の個々のルート パターンを、送信元（発信元）Unified CM クラスタに追加します。これらのパターンでは、IP WAN ルート グループを最初の選択肢として保持し、Standard Local Route Group を 2 番目の選択肢として保持するルート リストを指すようにします。
  - Cisco IOS ゲートキーパー設定に、関係するすべての E.164 範囲のゾーン プレフィックス ステートメントを追加します。これらのステートメントでは、適切な Unified CM クラスタを指すようにします。
  - 宛先 Unified CM クラスタに含まれているクラスタ間トランク コーリング サーチ スペースに、ローカル公衆網番号に一致するルート パターンを備えたパーティションを含めます。また、必要に応じて、適切な着番号トランスフォーメーション パターンを使用して番号操作を適用します（たとえば、コールを公衆網に送信する前にエリア コードを除去します）。

分散型コール処理配置の Cisco IOS ゲートキーパーを設定する方法の詳細については、「ゲートキーパーの設計上の考慮事項」（P.8-26）を参照してください。

ダイヤル プラン アプローチの選択

「プランニングの考慮事項」（P.10-6）で紹介したように、IP テレフォニー システムの内部宛先用のダイヤル プランには、主に次の 2 つのアプローチがあります。

- 固定オンネット ダイヤル プラン：個々の内部宛先には、発信者が同じサイトにいるか、別のサイトにいるかにかかわらず、同じ方法でダイヤルします。
- 可変長オンネット ダイヤル プラン：内部宛先がサイト内にある場合、複数のサイトにわたっている場合とは別の方法でダイヤルします。通常、サイトの内部でやり取りされるコールの場合は 4 桁または 5 桁の省略ダイヤリングを使用し、複数サイトにわたるコールの場合は、完全な E.164 アドレスを使用するか、オンネット アクセス コード、サイト コード、内線番号をこの順序で使用します。

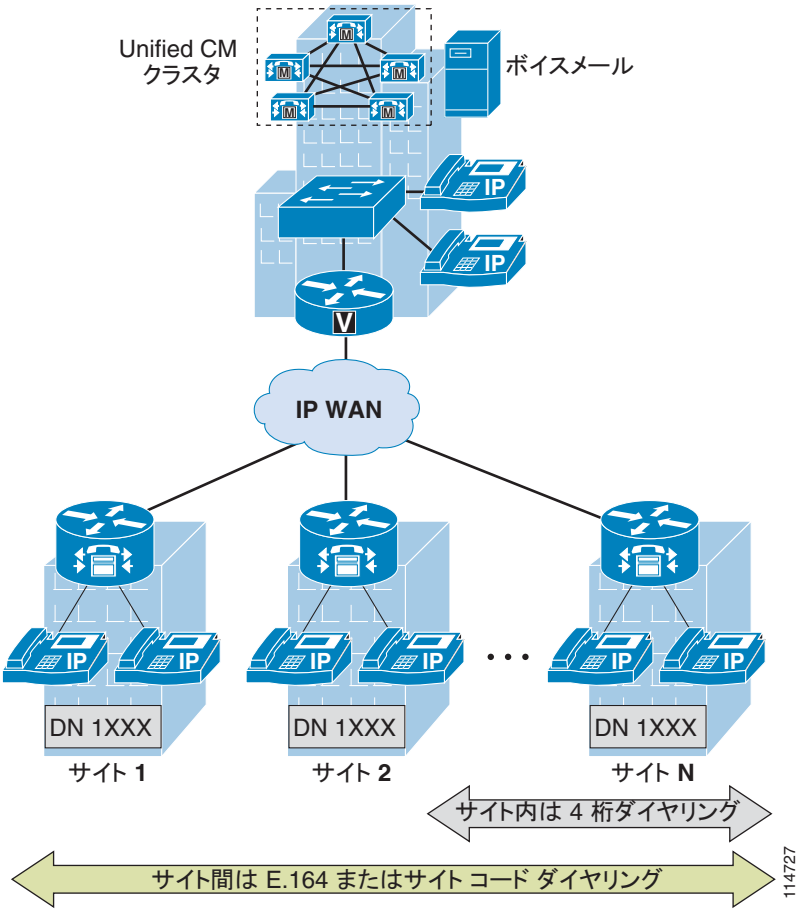
どちらのアプローチが最適かを判断するには、次の基本的な設計上の質問について検討すると役立ちます。

- IP テレフォニー システムによってサービスされるサイトは、最終的にいくつあるか。
- サイト間または支店間の発信パターンは何か。
- サイト内で、および別のサイトに到達するために、ユーザは何をダイヤルするか。
- オンネットサイト間コールに適用されるコール制限はあるか。
- ほとんどのサイト間コールで使用される転送ネットワークは何か（公衆網または IP WAN）。
- CTI アプリケーションが使用されている場合、それは何か。
- サイト コードを使用して、オンネット ダイヤリング構造を標準化する予定はあるか。

固定オンネット ダイヤル プランは、設計と設定が最も簡単です。ただし、このプランが最も適しているのは中小規模の配置であり、サイトおよびユーザの数が大きくなるほど、実用には適さなくなります。このプランについては、「固定オンネット ダイヤル プランの配置」（P.10-26）の項で詳しく説明および分析しています。

可変長オンネット ダイヤル プランは、スケーラビリティが優れていますが、設計と設定も複雑になります。図 10-4 では、可変長オンネット ダイヤル プラン アプローチを使用する大規模配置について、一般的な要件を示しています。

図 10-4　大規模マルチサイト配置の一般的なダイヤリング要件



Unified CM では、ダイヤル プランに可変長のオンネット ダイヤリングを実装するための主な方法は、フラット アドレッシングに依存します。内部の内線番号を、すべて同じパーティションに配置します。この方法は、通常はサイト間コールのオンネット サイト コードに基づいています。詳細については、「フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置」（P.10-29）の項を参照してください。このアプローチは、サイト間コールに完全な E.164 アドレスを使用している場合でも使用できることがあります。「サイト コードを使用しない配置に関する特別な考慮事項」（P.10-36）の項を参照してください。

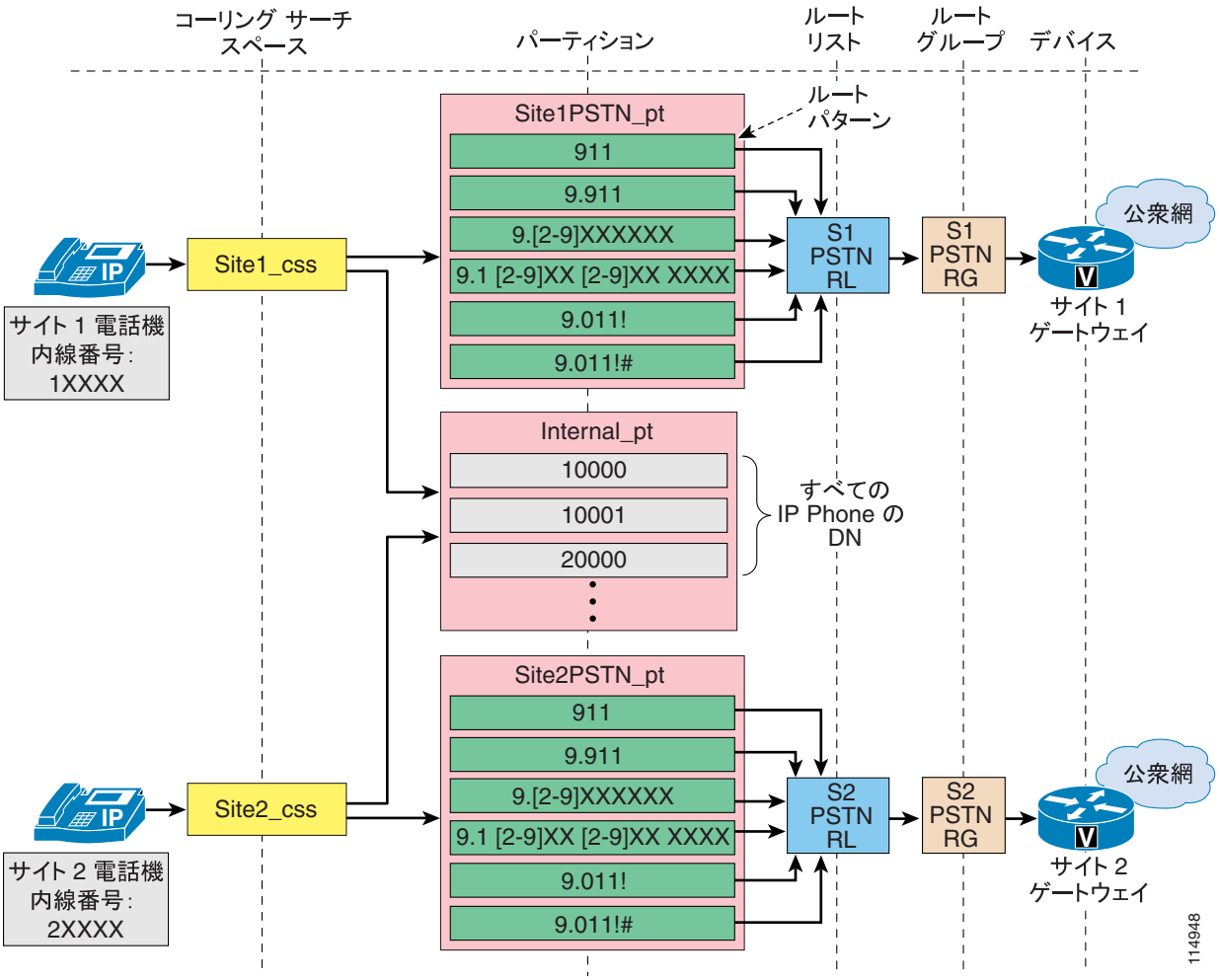
固定オンネット ダイヤル プランの配置

固定オンネット ダイヤル プランを実装するには、次のガイドラインに従います。

- 短縮内線番号を使用して、すべての電話を一意的に識別する。
- すべての電話 DN を単一のパーティションに配置する。
- 各サイトで、選択したサービス クラス アプローチに従って、公衆網ルート パターンを 1 つまたは複数のサイト固有パーティションに配置する。

図 10-5 では、単一 Unified CM クラスタ配置での実装例を示しています。

図 10-5　固定オンネット ダイヤル プランの配置の例



次の両方の条件に当てはまる場合は、このアプローチを使用します。

- 内部内線番号の識別用に選択した桁数を考慮したとき、使用可能な DID 範囲どうしが重複していない。
- IP テレフォニー システムによって処理されるサイトの数は、長期的に見て大幅に増加することがない。

次の各項では、固定オンネット ダイヤル プランのフレームワークで使用される各種のコールについて、実装の詳細およびベスト プラクティスを分析します。

- 「クラスタ内でのサイト間コール」（P.10-28）
- 「発信公衆網コールと IP WAN コール」（P.10-28）
- 「着信コール」（P.10-28）
- 「ボイスメール コール」（P.10-28）

クラスタ内でのサイト間コール

すべての内部 DN に対して、あらゆるデバイスのコーリング サーチ スペースから直接到達することができるため、すべてのオンネット コール（サイト内およびサイト間）が自動的に使用可能になります。Unified CM で特に設定する必要はありません。

発信公衆網コールと IP WAN コール

公衆網コールは、サイト固有のパーティションとルート パターンを使用することで可能になります。このため、緊急コールと市内電話は、ローカルの支店ゲートウェイを通じてルーティングすることができます。長距離電話と国際コールは、企業のポリシーに応じて、同じ支店ゲートウェイを通じてルーティングすることも（図 10-5 を参照）、中央ゲートウェイを通じてルーティングすることもできます。この 2 番目の方法で必要になるのは、サイトごとの追加ルート リストのみです。このリストには、中央サイト ゲートウェイを指す第 1 位ルート グループ、およびローカル支店ゲートウェイを指す第 2 位ルート グループ（省略可）を含めます。サイト固有のコール ルーティングを許可しながら、公衆網コールでのサイト間のルート パターンの再利用を許可するには、Standard Local Route Group を参照するルート リストを使用できます。

別の Unified CM クラスタまたは Cisco Unified Communications Manager Express（Unified CME）への短縮ダイヤリングも、ゲートキーパーを介して可能になります。これらの IP WAN コールについては、ゲートキーパーに送信する前に、トランスレーション パターンを通じて省略ストリングを完全な E.164 に展開することをお勧めします。

緊急コール

緊急コールの処理に Cisco Emergency Responder を使用する場合は、コールを Cisco Emergency Responder へ送信するために使用される CTI ルート ポイントを含むパーティションを、図 10-5 に示したようなサイト固有の 911 パターンではなく、すべての支店内にあるすべての電話機のコーリング サーチ スペースに含める必要があります。内部パーティション内での DN の重複は許容されないので、Cisco Emergency Responder は発信側の電話機を識別できます。Cisco Emergency Responder に関する考慮事項の詳細については、「Emergency Services」（P.11-1）の章と、次の Web サイトで入手可能な Cisco Emergency Responder 製品資料を参照してください。

http://www.cisco.com

着信コール

着信公衆網コールで必要となるのは、Unified CM に設定されている内線番号の長さに合せて、余分な桁を除去することのみです。この操作は、ゲートウェイの設定によって、またはゲートウェイのコーリング サーチ スペースに含まれているトランスレーション パターンを通じて実行できます。

ボイスメール コール

各内線番号は、いずれもシステム内部では一意です。したがって、この内線番号を使用してボイスメール システム内にボイスメール ボックスを設定することができます。ボイスメール システムにコールを送信するために、または Unified CM 内のメッセージ待機インジケータ（MWI）をオンにするために、変換を実行する必要はありません。

ただし、ユーザが公衆網からボイスメール システムにアクセスする場合は、ユーザを訓練して、ボイスメール ボックスにアクセスするときに内線番号を入力してもらうようにする必要があります。

フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置

フラット アドレッシングを使用する可変長オンネット ダイヤル プランを実装するには、電話の DN を、オンネット アクセス コード、サイト コード、および内線番号を含んだ一意のストリング（たとえば、8-123-1000）として定義します。これらの DN を同じグローバル パーティションに配置すると、サイト コードを使用したサイト間コールを使用できるようになり、サイト固有のパーティション内にトランスレーション パターンを定義すると（サイトごとに 1 トランスレーション パターンと 1 パーティション）、サイトの内部では省略ダイヤリングを使用できるようになります。

サイト内でユーザが通常ダイヤルしている 4 桁または 5 桁の番号を使用して、Directory Number 設定ページの Line Text Label パラメータを設定すると、この内部構造をエンドユーザから見えないようにすることができます。AAR を使用可能にし、ユーザが自分の DID 番号を IP Phone のディスプレイで見られるようにするには、外部電話番号マスクについても、対応する公衆網番号を使用して設定する必要があります。

表 10-4 では、各サイトでのコーリング サーチ スペースとパーティションの基本的な関係を示しています。ただし、サービス クラスの実装に必要となる追加の要素は考慮に入れていません。

表 10-4　フラット アドレッシングを使用する可変長ダイヤル プランのコーリング サーチ スペースとパーティション

コーリング サーチ スペース	パーティション	パーティションの内容
Site1_css	Site1Translations_pt	サイト 1 の省略ダイヤリングのためのトランスレーション パターン
	Site1PSTN_pt	サイト 1 の公衆網ルート パターン（サービス クラスに基づいて、他にもパーティションが必要）
	Internal_pt	すべての IP Phone の DN（一意形式）
…		
SiteN_css	SiteNTranslations_pt	サイト N の省略ダイヤリングのためのトランスレーション パターン
	SiteNPSTN_pt	サイト N の公衆網ルート パターン（サービス クラスに基づいて、他にもパーティションが必要）
	Internal_pt	すべての IP Phone の DN（一意形式）

次の条件に 1 つ以上当てはまる場合は、このアプローチを使用します。

- オンネットのサイト間コールで、ダイヤリング制限が必要ない。
- サイト コードを使用するグローバル オンネット番号計画を使用する予定がある。
- サイト間コールは、通常は IP WAN を通じてルーティングされる。
- CTI ベースのアプリケーション（Cisco Emergency Responder など）がサイト間で使用される。

（注） オンネットのサイト間コールにダイヤリング制限を適用する必要がある場合や、サイト コードを使用するオンネット番号計画を使用する予定がない場合は、それらのニーズに対応可能なこのアプローチの変型について、「サイト コードを使用しない配置に関する特別な考慮事項」（P.10-36）の項を参照してください。

このアプローチには、次の考慮事項が適用されます。

- サイト内の 4 桁コールの宛先番号は、IP Phone のディスプレイでは一意の内部 DN へと展開されます。
- Placed Calls ディレクトリでは、ユーザがダイヤルしたとおりに元の 4 桁のストリングが表示されます。
- 発信番号、および Missed Calls ディレクトリと Received Calls ディレクトリの番号は、一意の内部 DN として表示されます。
- IP WAN が使用不可になって支店の電話が SRST モードになっている場合でも、4 桁ダイヤリング機能をそのまま使用できるようにするには、SRST ルータの **call-manager-fallback** 設定に変換規則を適用する必要があります。
- 支店の電話が SRST モードになっている場合、一意の内部 DN を IP Phone のディスプレイ上で 4 桁番号としてマスクする Line Text Label は、使用できません。代わりに、ユーザには完全な内部 DN が表示されます。

フラット アドレッシング アプローチを配置する方法をわかりやすくするために、図 10-6 に示す架空の顧客ネットワークについてもう一度考えます。この場合、可変長オンネット ダイヤル プランが必要になることは決定していて、各サイトの内部では 4 桁ダイヤリングを使用し（各サイトで 1XXX 内線番号範囲を利用）、サイト間のダイヤリングでは、オンネット アクセス コード（この例では 8）、3 桁のサイト コード、および 4 桁の内線番号で構成される 8 桁のストリングを使用します。3 桁のサイト コードは、米国にあるサイトの場合は NANP エリア コードから生成され、欧州にあるサイトの場合は E.164 国コードとサイト識別子から生成されます。表 10-5 では、選択されたサイト コードを示しています。

表 10-5　図 10-6 の顧客ネットワークのサイト コード

	San Jose	New York	Dallas	London	Paris	Milan
サイト コード	408	212	972	442	331	392

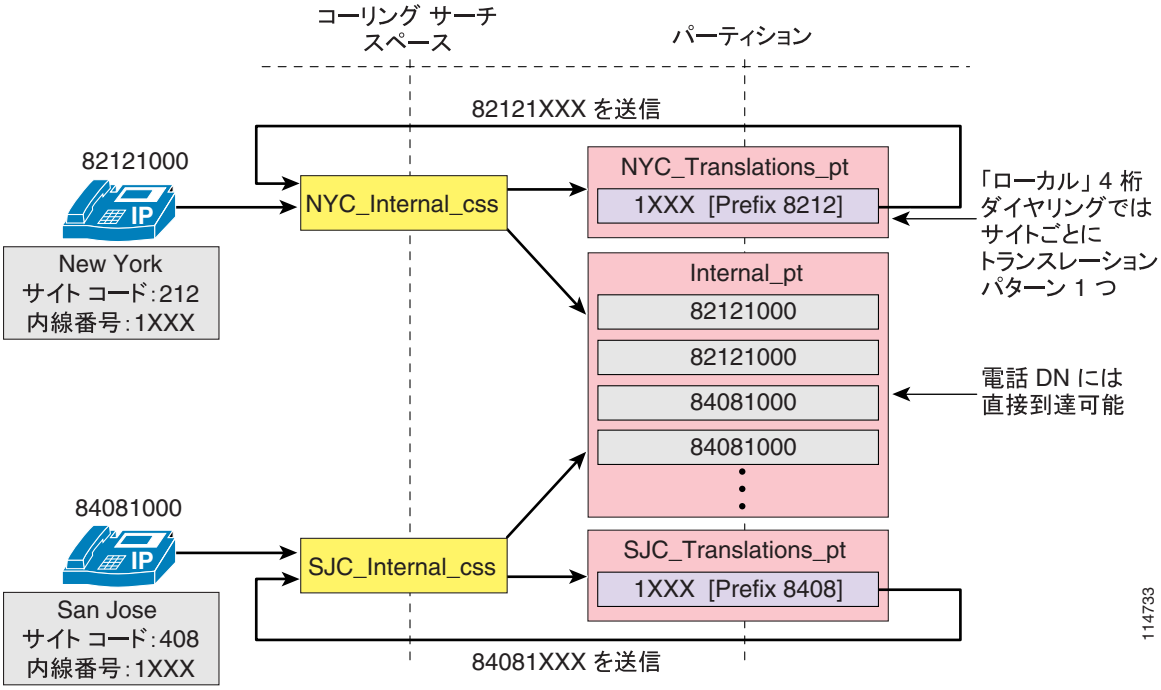
次の各項では、この例の US クラスタを使用して、フラット アドレッシング アプローチのフレームワークで使用される各種のコールについて、実装の詳細とベスト プラクティスを分析します。

- 「クラスタ内でのサイト間コール」（P.10-31）
- 「発信公衆網コールと IP WAN コール」（P.10-32）
- 「着信コール」（P.10-35）
- 「ボイスメール コール」（P.10-35）
- 「サイト コードを使用しない配置に関する特別な考慮事項」（P.10-36）

クラスタ内でのサイト間コール

図 10-6 では、US クラスタでのサイト間コールの設定例を示しています。

図 10-6　フラット アドレッシング法におけるクラスタ内部のサイト間コール



サイトとパーティション間の接続性をサポートするために、次のガイドラインに従ってください。

- オンネット アクセス コード 8 を含めて、一意の DN をすべてグローバル パーティション（この例では Internal_pt）に配置します。
- サイトごとにパーティションを 1 つ作成し、それぞれのパーティションの中に、4 桁番号をそのサイトの完全修飾 8 桁番号に展開するトランスレーション パターンを配置して、サイト内部で省略ダイヤリングを使用できるようにします。
- 各サイトで、Internal_pt パーティションとローカル トランスレーション パーティションの両方を電話のコーリング サーチ スペースに含めます。

Unified CM に設定されている DN にオンネット アクセス コードを含めると、すべての電話から直接アクセスできるパーティションの中にすべての内部内線番号を配置できるようになり、同時に、IP Phone 上のすべてのコール ディレクトリの中に、直接にリダイヤル可能な番号が確実に入力されます。

（注）　ただし、オンネット アクセス コードとサイト コードの組み合せが、どのサイトのローカル省略ダイヤリング範囲とも重複しないようにする必要があります。

発信公衆網コールと IP WAN コール

各種の公衆網コールをどのようにルーティングするかに応じて（集中型ゲートウェイと分散型ゲートウェイ）、設定が異なります。

欧州（EU）クラスタへのサイト間コールに対してオンネット接続を提供するには、次のオプションがあります。

オプション 1：8 桁番号のみ

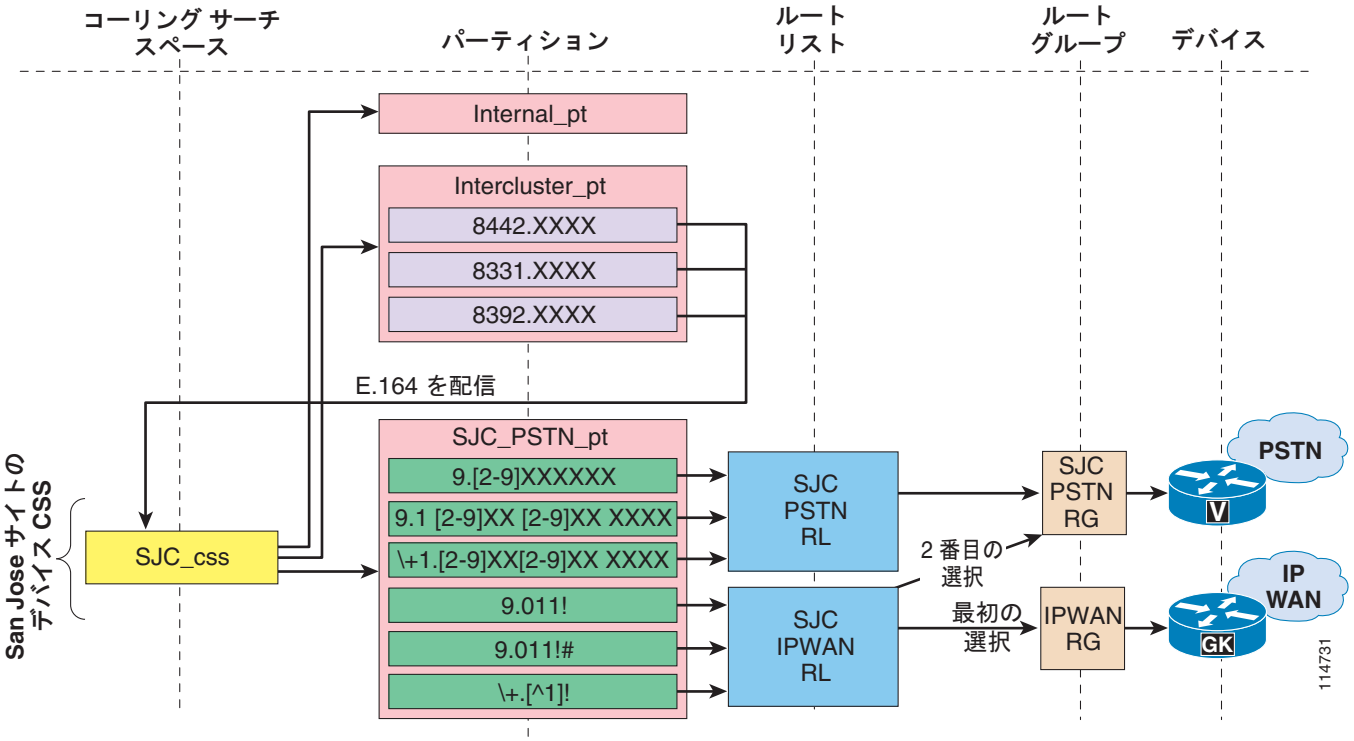
このオプションでは、単一のルート パターンを利用します。このパターンはすべての 8 桁範囲（8XXXXXXX）に一致し、ゲートキーパー制御クラスタ間トランクのみを含んだルート リストまたはルート グループを指しています。ゲートキーパーは、サイト コードをゾーン プレフィックスとして使用するように設定します。

このソリューションは、他のクラスタのサイト コードや E.164 範囲に関する情報が必要ないため、簡潔で保守が容易です。ただし、IP WAN が使用不可になった場合、自動公衆網フェールオーバーは提供されません。ユーザは、公衆網アクセス コードと宛先の E.164 アドレスを使用して、手動で再ダイヤルする必要があります。

オプション 2：8 桁番号と E.164 アドレス（集中型公衆網フェールオーバーを使用）

このオプションでは、図 10-7 に示すように、欧州の 8 桁範囲に一致し、それらを対応する E.164 番号に変換するグローバルな一連のトランスレーション パターンを使用します。これらのトランスレーション パターンでは、中央サイト（この場合は San Jose）のコーリング サーチ スペースを使用するので、コールは中央サイトの公衆網パーティションにある国際公衆網ルート パターンに一致します。各サイトの国際公衆網ルート パターンは、IP WAN ルート グループを最初の選択肢として保持し、ローカル公衆網ルート グループを 2 番目の選択肢として保持しているルート リストを指しています。ゲートキーパーは、E.164 アドレスをゾーン プレフィックスとして使用するように設定します。

図 10-7　IP WAN コールに集中型公衆網フェールオーバーを使用する、フラット アドレッシング法における発信の公衆網コールと IP WAN コール



（注）　図 10-7 の設定例は、サービス クラスを構築するための回線/デバイス アプローチが使用されていることを前提としています。ただし、従来のアプローチを使用する場合も同じ考慮事項が適用されます。

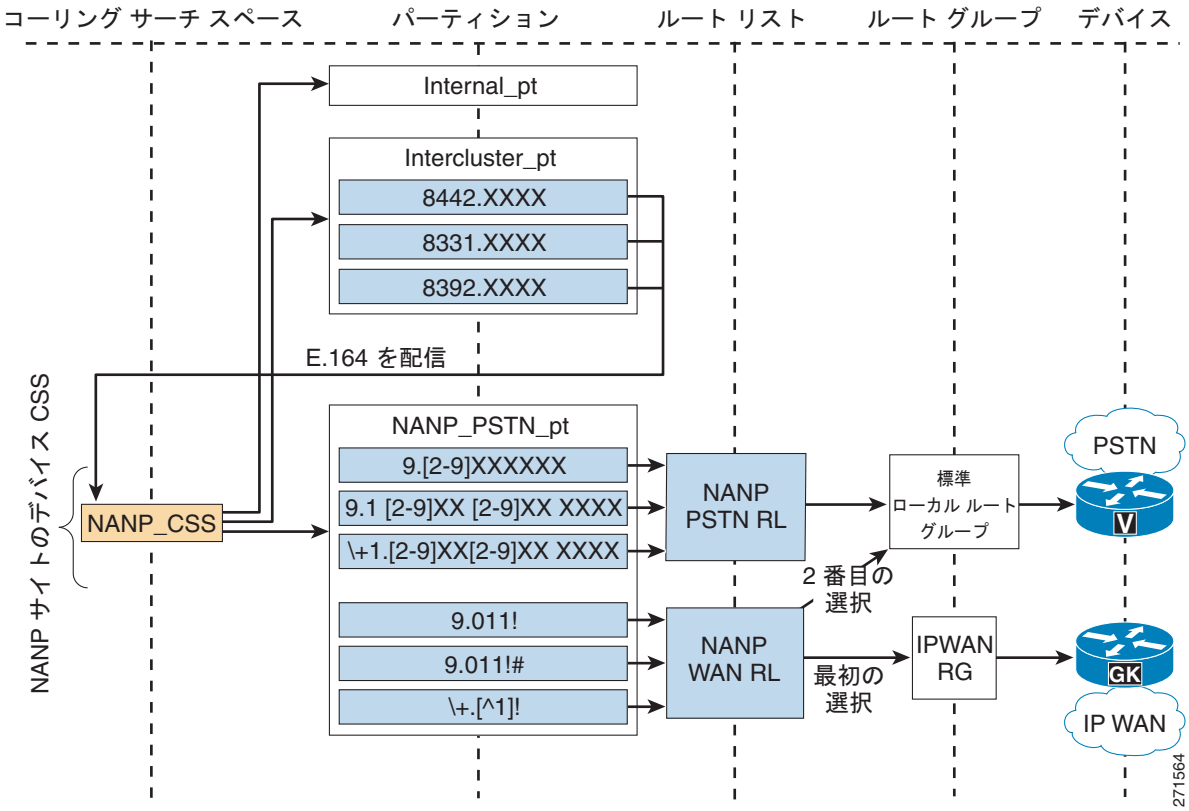
このソリューションは、オプション 1 で説明したソリューションよりもわずかに設定および保守作業が増えます。これは、他のクラスタのサイト コードと E.164 範囲に関する情報を設定し、保守する必要があるためです。その一方で、IP WAN が使用不可になった場合には、自動公衆網フェールオーバーが提供されます。公衆網フェールオーバーは、中央サイトのゲートウェイのみを使用して提供されます。このため、IP WAN 帯域幅の使用効率は最適なものにはなりません。

また、公衆網コールとしてダイヤルされた欧州サイトへのコールは、IP WAN が使用可能な場合、ローカル ゲートウェイを使用する自動公衆網フェールオーバーによって、自動的にオンネットになります。

オプション 3：8 桁番号と E.164 アドレス（分散型公衆網フェールオーバーを使用）

このオプションでは、図 10-8 に示すように、欧州の 8 桁範囲に一致し、それらを対応する E.164 番号に変換するグローバルな一連のトランスレーション パターンを使用します。トランスレーション パターンでは、グローバル コーリング サーチ スペース（北米番号計画内（NANP）のすべてのサイトで使用）を使用し、コールは NANP の公衆網パーティション内の国際公衆網ルート パターンとマッチングします。国際公衆網ルート パターンは、IP WAN ルート グループを最初の選択肢として保持し、標準ローカル ルート グループを 2 番目の選択肢として保持しているルート リストを指しています。ゲートキーパーは、E.164 アドレスをゾーン プレフィックスとして使用するように設定します。

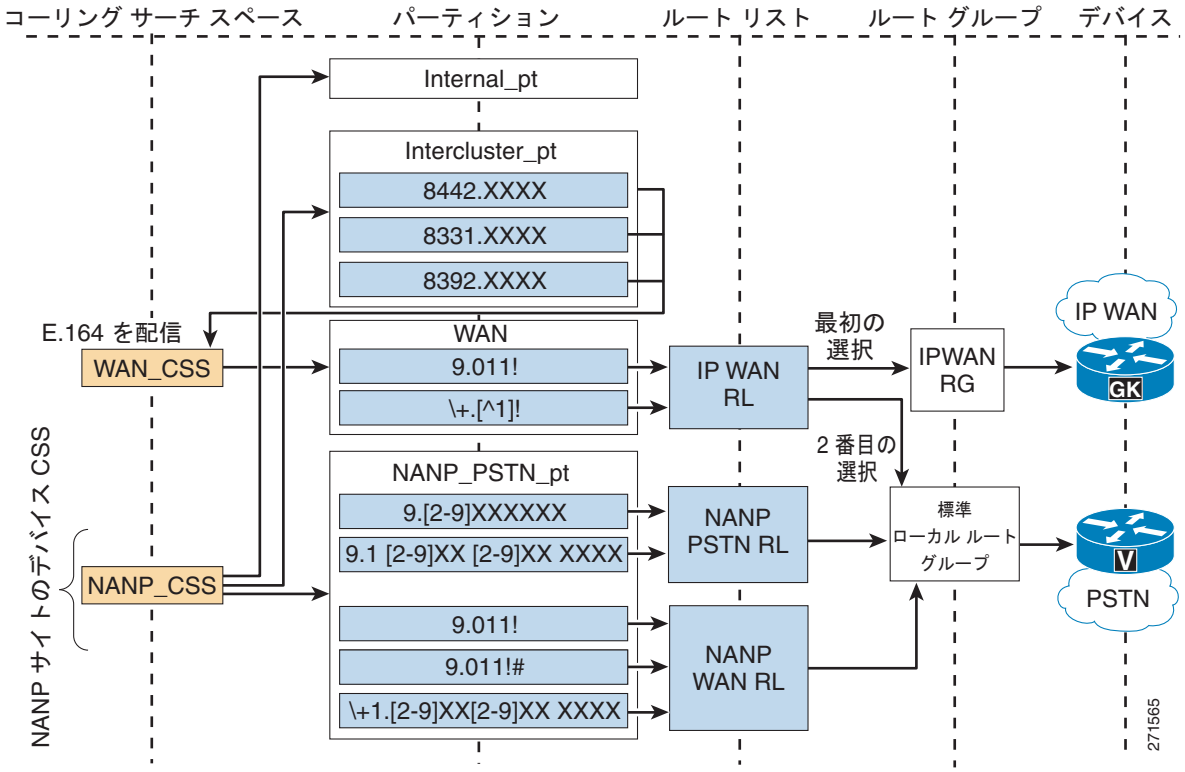
図 10-8　IP WAN コールに分散型公衆網フェールオーバーを使用する、フラット アドレッシング法における発信の公衆網コールと IP WAN コール



IP WAN が使用不可になった場合には、このソリューションによりローカル サイトのゲートウェイを使用して自動公衆網フェールオーバーが提供されるため、IP WAN 帯域幅の使用効率は最適なものになります。ローカル ルート グループ コンストラクトの出現により、このアプローチは実質的に 2 番目の選択肢に優先します。このコンストラクトは同じレベルの設定を必要としますが、ローカル公衆網フェールオーバーを行えるためです。

このソリューションでも、公衆網コールとしてダイヤルされた欧州サイトへのコールは、IP WAN が使用可能な場合、ローカル ゲートウェイを使用する自動公衆網フェールオーバーによって、オプション 2 と同様に自動的にオンネットになります。これは実質的に、NANP サイトから発信されたすべてのオフネットの欧州でのコールに TEHO 機能の形式を提供します。オンネットの宛先としてダイヤルされたコールのみが IP WAN に送信される場合は、発信側でオンネットのクラスタ間宛先としてダイヤルされた場合にのみ IP WAN にコールを送信するよう、アプローチを変更できます。図 10-9 に、このアプローチを示します。

図 10-9　クラスタ間コールのみの IP WAN アクセス



着信コール

着信公衆網コールでは、8 桁の内部番号を取得して宛先の電話に到達するには、E.164 番号を操作する必要があります。この要件は、次の方法のいずれかで満たすことができます。

- Unified CM の Gateway Configuration ページにある Num Digits フィールドと Prefix Digits フィールドを設定して、必要な番号を除去してプレフィックスを付加するようにします。
- クラスタ内でオンネット サイト間コールを強制するトランスレーション パターンを設定した場合は、公衆網アクセス コードをゲートウェイ上の着信番号にプレフィックスとして付加するだけで、それらのパターンを再利用することができます。
- H.323 ゲートウェイを使用している場合は、コールを Unified CM に送信する前に、ゲートウェイ内の変換規則を使用して番号を操作できます。

3 番目のアプローチは、支店が SRST モードになっている場合、設定済みの変換規則を再利用して IP Phone に着信公衆網接続を提供できる利点があります。

ボイスメール コール

8 桁の各内線番号は、いずれもシステム内部では一意です。したがって、この内線番号を使用してボイスメール システム内にボイスメール ボックスを設定することができます。ボイスメール システムにコールを送信するために、または Unified CM 内のメッセージ待機インジケータ（MWI）をオンにするために、変換を実行する必要はありません。ユーザは、メールボックス番号の入力を求められたときに、8 桁のオンネット番号を使用する必要があることに注意してください。

サイト コードを使用しない配置に関する特別な考慮事項

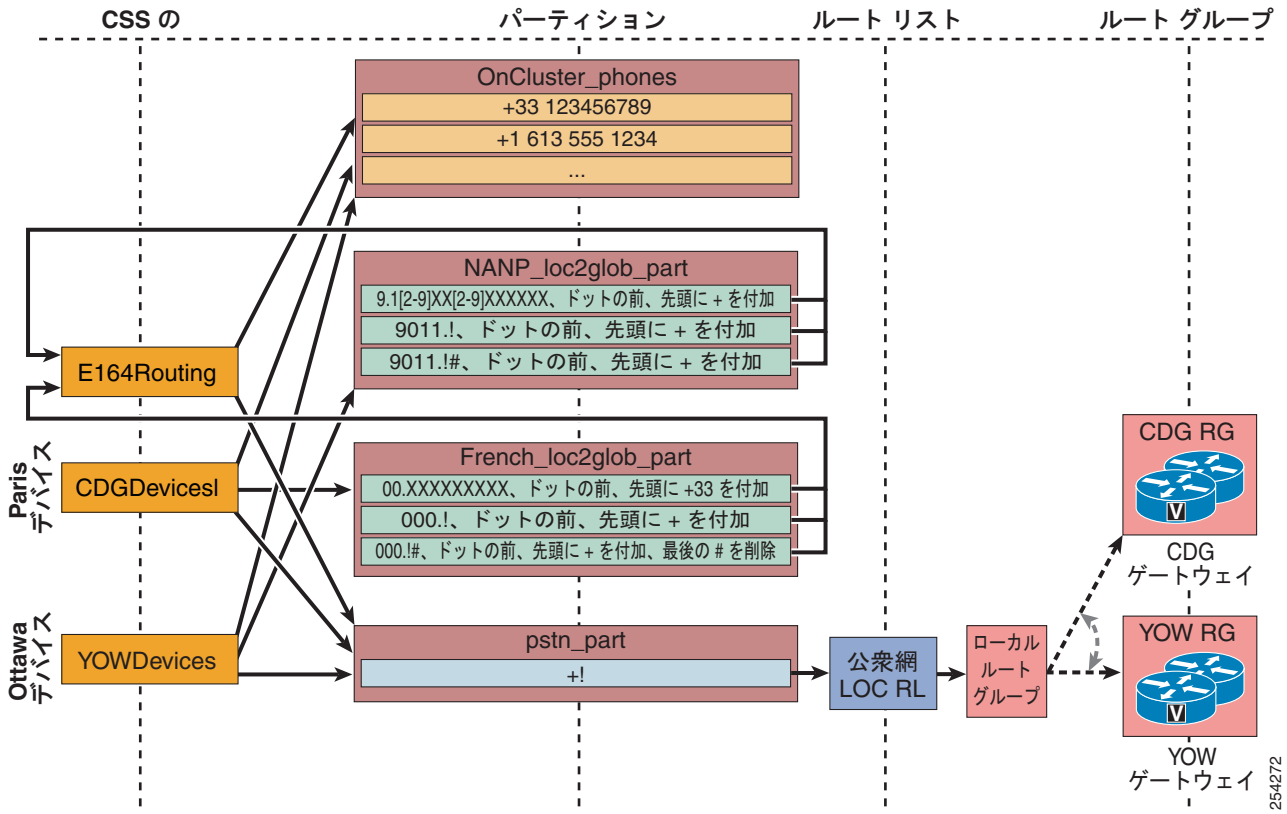
このシナリオは、フラット アドレッシング アプローチの変型であり、サイト コードに基づいてオンネット番号計画を定義することに依存しません。このシナリオでは、サイト内コールは 4 桁番号としてダイヤルします。その一方で、サイト間コールは通常の公衆網コールとしてダイヤルするため、コールは Unified CM によって代行受信され、IP WAN を通じてルーティングされます。

このメカニズムを実装するには、図 10-10 に示すように、次のガイドラインに従います。

- 電話 DN は、完全な E.164 アドレスとして定義し、すべて同じパーティション（この例では OnCluster_phones）に配置します。
- トランスレーション パターンで、ローカル化されたユーザ入力を許可し、完全な E.164 番号を取得できるようにグローバル化するよう設定します。グローバル化された番号は CSS E164Routing を介してルーティングされます。この例では、2 つのデバイスのコーリング サーチ スペースのみを必要とします。1 つは、Paris のサイトからのローカル化されたユーザ入力を受け入れますが、すべてのフランスのサイトで再利用できます。もう 1 つは Ottawa サイトからのユーザ入力を受け入れますが、すべての NANP サイトで再利用できます。
- 公衆網パーティション（この例では pstn_part）を設定し、コールをルーティングするための適切なルート パターンとルート リストを作成します。この例では、単一の、クラスタ全体のルート パターン +!（ローカル ルート グループへのすべてのグローバル化された宛先公衆網コールをルーティングできます）を使用します。

Paris のユーザが番号をダイヤルすると、French_loc2glob_part パーティションにあるトランスレーション パターンを使用してグローバル化され、変換された番号は E164Routing CSS を介してルーティングされます。宛先番号がオンクラスタの DN の場合、同時に OnCluster_Phones パーティションの完全一致のパターンと、pstn_part パーティションの汎用パターンに同時に一致します。ベストマッチ プロセスでは、オンクラスタ電話機の完全一致 DN を選択し、コールを宛先にルーティングします。ダイヤルした宛先がクラスタ上の電話機ではない場合は、E164Routing CSS を介してルーティングされたグローバル化された番号は pstn_part パーティションの +! パターンのみと一致し、変換されたコールは公衆網にルーティングされます。

図 10-10　サイト コードを使用せずにフラット アドレッシングを使用する可変長ダイヤル プラン



この設定変数では、ダイヤリング ルールを簡素化して、使用しやすくします。宛先がサイト内にある場合、省略ダイヤリング（見やすくするために 図 10-10 では省略）を使用します。宛先がサイト外にある場合、オンネットかオフネットかにかかわらず、オフネット公衆網形式でダイヤルします。

- 実質上オンネット公衆網コールを強制することになるため、AAR を設定して、IP WAN の帯域幅が十分にない場合でも公衆網経由でコールを発信できるようにしてください。
- 「発信履歴」ディレクトリには、ユーザがダイヤルしたとおりに番号ストリングが表示されます。たとえば、ユーザが 1000 をダイヤルして電話機 +16135551000 へのコールが発信された場合、「発信履歴」のディレクトリには 1000 が表示されます。これにより、ダイヤル ストリングを編集しなくても番号を直接リダイヤルできます。
- 「不在履歴」と「発信履歴」のディレクトリには、電話機にコールが提供されたときに表示されたとおりの電話番号が表示されます。DN は + を使用して E.164 番号として設定されます。ワンタッチ ダイヤリングが可能です。図 10-10 で、電話機のデバイス CSS は、+ 記号を含むグローバル化された E.164 形式を使用して、直接 DN にコールをルーティングできます。

SIP 電話機でのダイヤルされたパターン認識の導入

SIP 電話機のダイヤルされたパターンの認識機能では、企業内のユーザから予測される一般的なダイヤリング手順の傾向を考慮する必要があります。一般に、ほとんどの企業では次のパターンの組み合せが使用されます。

- 同じサイト内でのコールのための省略ダイヤリング パターン（固定オンネット ダイヤル プランの場合、省略ダイヤリング パターンがサイト間コールに使用される場合があります）
- サイト コードとオンネット アクセス コード（たとえば 8）を使用しているときに可変オンネット ダイヤル プランで一般的に使用されるサイト間ダイヤリング パターン
- ローカル コール用のオフネット ダイヤリング パターン
- 長距離コール用のオフネット ダイヤリング パターン
- 緊急コール パターン（オフネット アクセス コードありとなし）
- 国際コール用のオフネット ダイヤリング パターン

表 10-6 と表 10-7 は、次のダイヤル プラン特性を持つ企業で採用できる SIP ダイヤル規則の例を示しています。

- 省略ダイヤリングは 4 桁（サイト間コールに省略ダイヤリングが使用されるかどうかは無関係）
- サイト間コールではオンネット アクセス コードとして 8 を使用し、その後にサイト コードと DN を表す 7 桁が続く
- 緊急ダイヤリングは 911 および 9911 として許可
- ローカルの 7 桁コールでは 9 をオフネット アクセス コードとして使用し、その後に 7 桁が続く
- ローカルの 10 桁コールでは 9 をオフネット アクセス コードとして使用し、その後に 10 桁が続く
- 長距離コールは 91 と 10 桁をダイヤル
- 国際コールは、9011 の後に不定の桁数が続き、ダイヤリングを # で終了可能

パターン認識は、桁間タイムアウトや Dial キー操作の必要なく、Unified CM に自動的に転送されるユーザ番号入力の収集の自動化だけに関係しています。サービス クラスの実施はすべて、Unified CM の中から選択された各種のコーリング サーチ スペースによって処理されます。すべての電話機を SIP ダイヤル規則を使用して設定し、たとえば、一部の電話機に無制限のサービス クラスが割り当てられていなくても国際ダイヤリングを認識できるようにするのは、その理由からです。

上記のダイヤル プラン特性は、フラット アドレッシングを使用する代表的な可変長オンネット ダイヤル プランです（「フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置」（P.10-29）を参照）。パターン認識の観点から見ると、このダイヤル プランは、固定オンネット ダイヤル プラン、および分割アドレッシングを使用する可変長オンネット ダイヤル プランと互換性があります（「固定オンネット ダイヤル プランの配置」（P.10-26）を参照）。

表 10-6 と表 10-7 の各パターンに対して、同等の Unified CM 表記のパターンを示してあります。これらの表は、7905_7912 と 7940_7960_OTHER の両方のケースについて、SIP ダイヤル規則を示しています。

（注）　7905_7912 の SIP ダイヤル規則は 128 文字までに制限され、7940_7060_OTHER の SIP ダイヤル規則は 8K（8,192）文字までに制限されています。

表 10-6　7940_7960_OTHER ダイヤル規則

説明	パターン	タイムアウト	効果
省略形の 2XXX	2...	0	これら 6 個の範囲の組み合せは、すべてのサイトで使用できる 4 桁の省略ダイヤリング パターンを表します。[2-7]XXX と一致するいずれかのストリングがダイヤルされると、そのストリングはすぐに、Unified CM に送信されます（timeout = 0）。
省略形の 3XXX	3...	0	
省略形の 4XXX	4...	0	
省略形の 5XXX	5...	0	
省略形の 6XXX	6...	0	
省略形の 7XXX	7...	0	
サイト間ダイヤリングの 8.XXXXXXX	8,.....	0	8 が認識されると 2 次ダイヤル トーンが再生され、さらに 7 桁が収集されます。その後、すぐに Unified CM への転送が行われます（timeout = 0）。
緊急の 911	9,11	0	9 が認識されると 2 次ダイヤル トーンが再生され、番号 11 が収集されます。その後、すぐに Unified CM への転送が行われます（timeout = 0）。
緊急の 9.911	9,911	0	9 が認識されると 2 次ダイヤル トーンが再生され、番号 911 が収集されます。その後、すぐに Unified CM への転送が行われます（timeout = 0）。
ローカル公衆網の 7 桁	9,.....	3	9 が認識されると 2 次ダイヤル トーンが再生され、さらに 7 桁が収集されます。ローカル公衆網の 10 桁ダイヤリングが設定されていると、ユーザは 3 秒のタイムアウトの間にダイヤリングを続行できます。
ローカル公衆網の 10 桁	9,.....	0	9 が認識されると 2 次ダイヤル トーンが再生され、さらに 10 桁が収集されます。その後、すぐに Unified CM への転送が行われます（timeout = 0）。
長距離	9,1.....	0	9 が認識されると 2 次ダイヤル トーンが再生され、さらに 10 桁が収集されます。その後、すぐに Unified CM への転送が行われます（timeout = 0）。
6 秒の桁間タイムアウトによる国際ダイヤル	9,011*	6	9 が認識されると 2 次ダイヤル トーンが再生され、その後、011 と不定の桁数が収集されます。ユーザは、不完全なストリングへのコールをトリガーすることなく、6 秒のタイムアウトの間にダイヤリングを一時停止できます。
ダイヤリングの終わりとして # を使用した国際ダイヤル	9,011*#	0	9 が認識されるとすぐに 2 次ダイヤル トーンが再生され、その後、011 と不定の桁数が収集され、# によって終了します。Unified CM にすぐに転送されます（timeout = 0）。
オペレータ	0	0	0 が検出されると Unified CM にすぐに転送されます（timeout = 0）。

表 10-7　7905_7912 ダイヤル規則

説明	パターン	効果
省略形の 2XXX	2...t0	これら 6 個の範囲の組み合せは、すべてのサイトで使用できる 4 桁の省略ダイヤリング パターンを表します。[2-7]XXX と一致するいずれかのストリングがダイヤルされると、そのストリングはすぐに、Unified CM に送信されます（t 0）。
省略形の 3XXX	3...t0	
省略形の 4XXX	4...t0	
省略形の 5XXX	5...t0	
省略形の 6XXX	6...t0	
省略形の 7XXX	7...t0	
サイト間ダイヤリングの 8.XXXXXXX	8.....t0	番号 8 とそれに続く 7 桁が収集された後、すぐに Unified CM に転送されます（t0）。
緊急の 911	911t0	番号 911 が収集され、すぐに Unified CM に転送されます（t0）。
緊急の 9.911	9911t0	番号 9911 が収集され、すぐに Unified CM に転送されます（t0）。
ローカルの 7 桁と LD	9.....t4>#....t1	番号 9 とそれに続く 7 桁が収集され、さらに 4 秒間に最大 4 桁までダイヤルできます。さらに 4 桁を入力した場合、それらは 1 秒後に Unified CM に送信されます。# は、9 と 7 桁が入力された後の終了文字として認識されます。
国際	9011>#t6-	番号 9 011 と、それに続く不定の桁数が収集されます。ユーザは、不完全なストリングへのコールをトリガーすることなく、6 秒のタイムアウトの間にダイヤリングを一時停止できます。# を終了文字として使用できます。
オペレータ	0	0 が検出されると Unified CM にすぐに転送されます（timeout = 0）。

Unified CM のサービス クラスの構築

Unified CM では、従来のアプローチおよび回線/デバイス アプローチという、ユーザおよびデバイスにサービス クラスを定義、適用する 2 つの主要なアプローチを用意しています。それぞれのアプローチで扱う基本的な要素には、許可するコールの種類（たとえば、local、national、または international）およびコールが取るパス（たとえば、IP ネットワーク、ローカル ゲートウェイ、または中央ゲートウェイ）が含まれます。どちらの要素もコーリング サーチ スペースを使用します。次の項では、Unified CM システムで使用される、サービス クラスを実装するための 2 つの主要なアプローチについて説明します。どちらのアプローチも回線とデバイスのコーリング サーチ スペースの基本的な機能に基づいています。

デバイスのコーリング サーチ スペースは、電話機の IP アドレスで定められているように、ネットワークのどの場所に電話機が物理的に存在しているか、デバイス モビリティが設定されているかどうかに基づいて動的に特定できます。詳細については、「デバイス モビリティ」（P.10-92）を参照してください。

従来のアプローチによる Unified CM のサービス クラスの構築

Unified CM では、次のようにパーティションおよびデバイス コーリング サーチ スペースを外部ルート パターンと組み合せると、IP テレフォニー ユーザにサービス クラスを定義することができます。

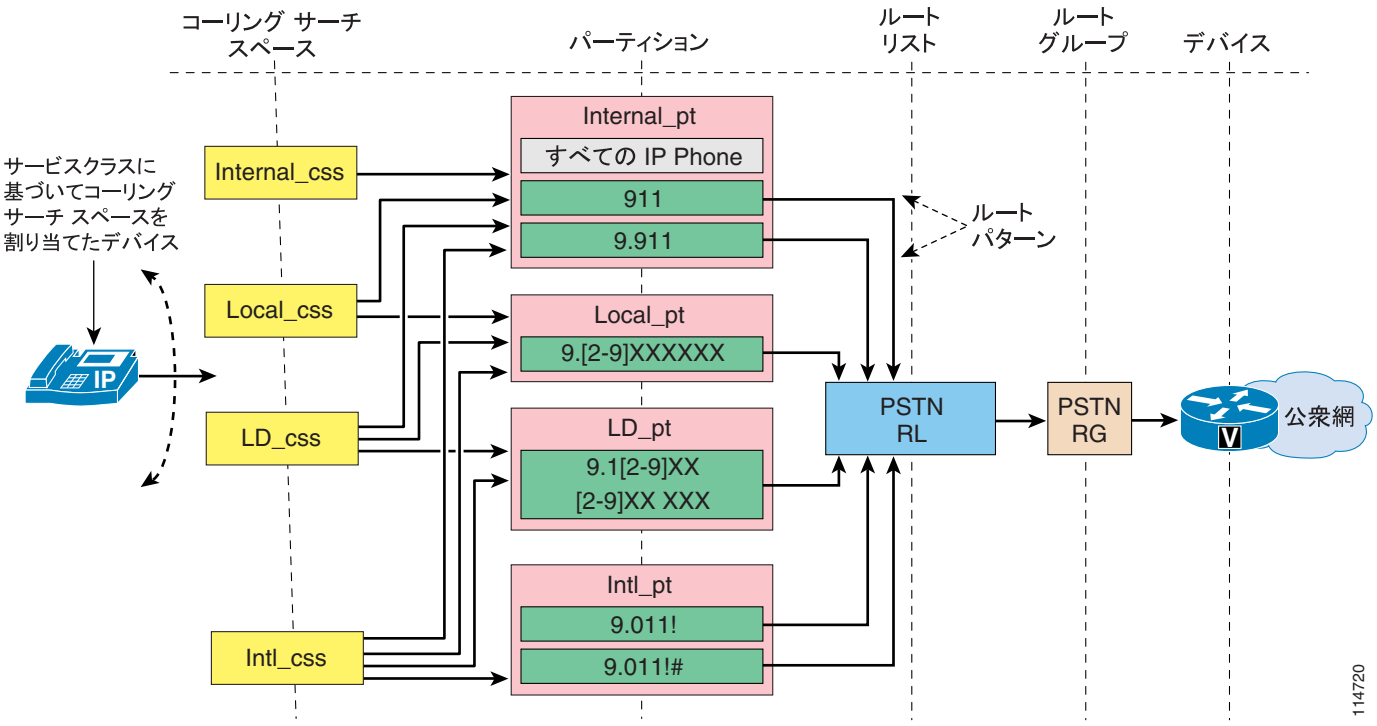
- 外部ルート パターンをコール可能な宛先に関連したパーティションに置きます。1 つのパーティションにすべてのルート パターンを含めることができますが、コール可能な宛先に応じてルート パターンをパーティションに関連付けると、より高度なコール制限ポリシーを実現できます。たとえば、同じパーティションにローカル ルート パターンと国際ルート パターンを入れる場合、すべ

てのユーザは、ローカルの宛先と海外の宛先の両方と通信できます。ただし、これは好ましくない場合があります。ルート パターンは、さまざまなサービス クラスの到達可能性ポリシーに従って、それぞれのパーティションに分類することをお勧めします。

- 各コーリング サーチ スペースがそのコール制限ポリシーに関連したパーティションのみに到達できるように設定します。たとえば、ローカル コーリング サーチ スペースが内部パーティションとローカル パーティションを指定するように設定します。その結果、このコーリング サーチ スペースに割り当てられるユーザは、内部コールおよびローカル コールしか発信できません。
- Unified CM のデバイス ページで電話機を設定して、これらのコーリング サーチ スペースを電話機に割り当てます。このように設定すると、デバイス上に設定されているすべての回線が自動的に同じサービス クラスを受信します。

図 10-11 では、単純な単一サイト配置の例を示しています。

図 10-11　従来のアプローチを使用するサービス クラスの基本的な例



このアプローチでは、デバイス コーリング サーチ スペースが次の 2 つの論理機能を実行します。

- パスの選択

  コーリング サーチ スペースは、特定のパーティションを含んでいます。このパーティションは、ルート リストとそれに関連したルート グループを通じて、特定の公衆網ゲートウェイを指している特定のルート パターンを含んでいます。

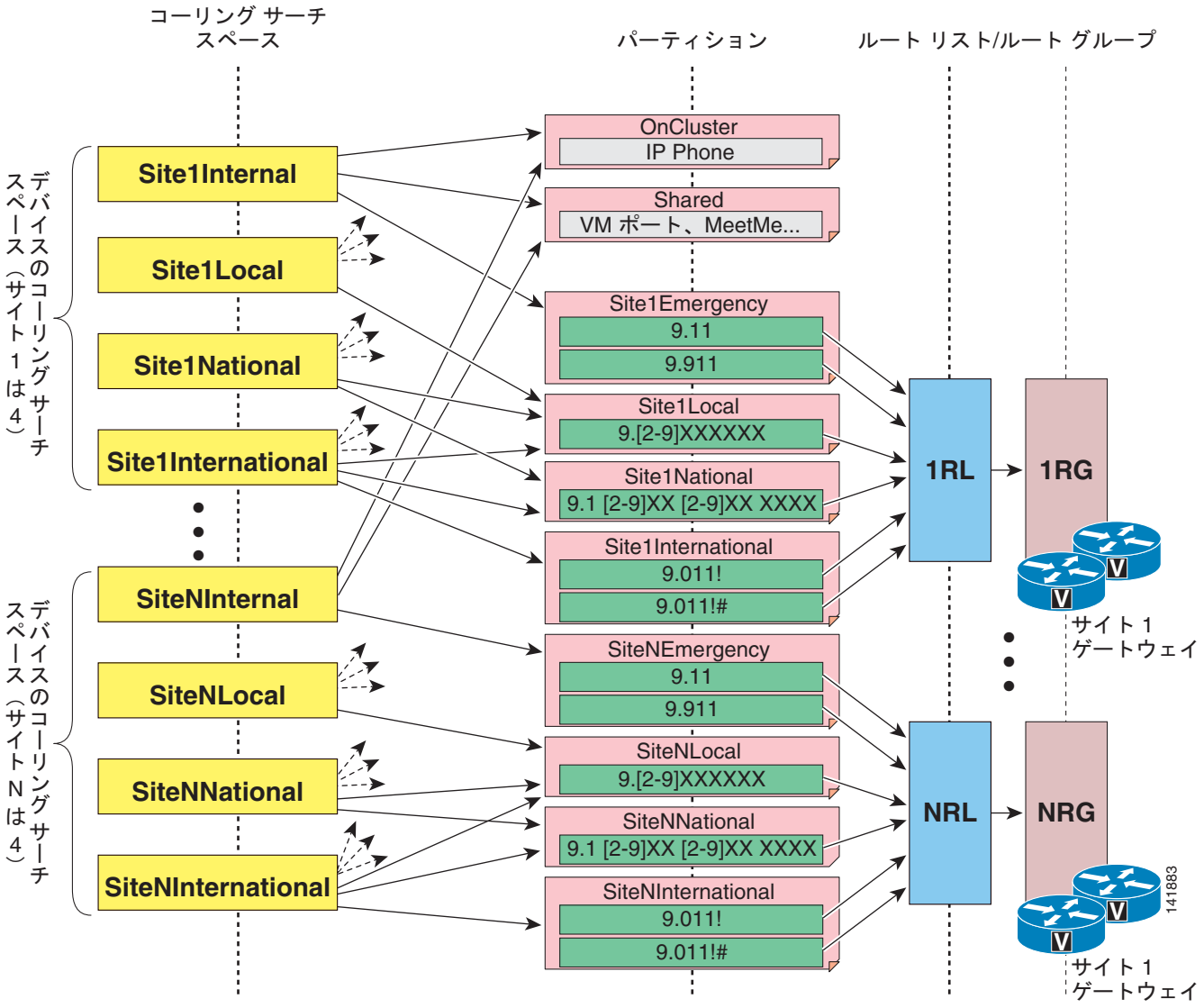
- サービス クラス

  特定のパーティションのみをデバイス コーリング サーチ スペースに含めて、他のパーティションを含めないようにすると、特定のユーザ グループに対して実質上のコール制限が適用されます。

結果として、このアプローチを集中型コール処理のマルチサイト配置に適用する場合は、パーティションとコーリング サーチ スペースを各サイトに複製する必要があります。これは、図 10-12 に示すように、サイトごとにサービス クラスを作成し、同時に、ローカル支店ゲートウェイから発信される公衆網コールをルーティングする必要があるためです。または、Standard Local Route Group を参照する

ルート リストを指すルート パターンを設定できます。こうすると、実際の出口ゲートウェイが、発信電話機のデバイス プールによって決定されます。これにより、コール ルーティングのサイト特性を保持しながら、サイト間のパターンを再利用できます。

図 10-12　　従来のアプローチで必要となるコーリング サーチ スペースとパーティション



集中型コール処理を行う複数サイト配置に対してこのダイヤル プラン アプローチを適用するときに、サイト間でオンネット ダイヤリングを構成するために、すべての IP Phone の DN をすべてのサイトのコーリング サーチ スペースからアクセス可能なオンクラスタまたは内部のパーティションに置きます。これは、IP Phone の DN が重複している場合は不可能であることに注意してください。

従来のアプローチにおけるエクステンション モビリティの考慮事項

エクステンション モビリティ機能を使用する場合、電話機のダイヤル制限は、その電話機へのログイン（またはログアウト）中の機能の 1 つになります。ログアウトされた電話機は、他の電話機やサービス（たとえば、米国では 911）のコールを制限する必要があります。一般に、公衆網を通じた市内または市外通話へのアクセスは制限されます。逆に、ユーザがログインしている電話機は、そのユーザのダイヤリング権限に応じてコールを許可し、それらのコールを適切なゲートウェイ（たとえば、同じ場所に配置されているローカル コール用の支店ゲートウェイ）にルーティングする必要があります。

エクステンション モビリティを使用する場合、サービス クラスを構築するための従来のアプローチでコール制限を適用するには、次のガイドラインを考慮してください。

- 各サイトで、すべての IP Phone のデバイス コーリング サーチ スペースを、公衆網緊急サービスのみを（ローカル ゲートウェイを使用して）指すように設定します。
- エクステンション モビリティに使用される IP Phone がログアウト状態になっている場合の回線コーリング サーチ スペースを、内部番号のみを指すように設定します。
- 各エクステンション モビリティ ユーザについて、デバイス プロファイル内の回線コーリング サーチ スペースを、個々のユーザのサービス クラスで許可されている内部番号と追加公衆網ルート パターンを（ここでも、企業ポリシーに従って適切なゲートウェイを使用して）指すように設定します。

通常はサイト 1 を拠点としているエクステンション モビリティ ユーザが、サイト 2 の IP Phone にログインすると、公衆網コールのパス選択が次のように変更されます。

- 緊急コールは、サイト 2 の公衆網ゲートウェイを使用して正しくルーティングされます。緊急サービスは、サイト 2 にある IP Phone のデバイス コーリング サーチ スペースによって提供されるためです。
- この他のすべての公衆網コールは、エクステンション モビリティ ユーザのプロファイル（具体的には、デバイス プロファイル内に設定されている回線コーリング サーチ スペース）に従ってルーティングされます。これは、通常、これらの公衆網コールが 2 つの WAN リンクを通過し、サイト 1 のゲートウェイを使用して公衆網にアクセスすることを意味します。

この動作を修正し、エクステンション モビリティ ユーザが別のサイトにローミングしている場合でも、公衆網コールが常にローカル公衆網ゲートウェイを通じてルーティングされるようにするには、次のいずれかの方法を使用します。

- ローカル公衆網ルート パターンは、デバイス コーリング サーチ スペースに含めて、デバイス プロファイル内の回線コーリング サーチ スペースからは削除します。この方法によって、ローカルの公衆網コールは、同じ場所にある支店ゲートウェイを通じてルーティングされるようになります。ただし、同時に、ユーザは IP Phone にログインしなくてもこれらのコールをダイヤルできるようになります。長距離電話と国際コールについては、エクステンション モビリティ ユーザのデバイス プロファイルに従ってルーティングされます。したがって、このソリューションが適しているのは、通常これらのコールが中央ゲートウェイを通じてルーティングされている場合のみです。
- 各ユーザに対して、ユーザがローミングするサイトごとに 1 つずつ、複数のデバイス プロファイルを定義します。各デバイス プロファイルの設定では、回線コーリング サーチ スペースが、そのサイトのローカル ゲートウェイを使用する公衆網ルート パターンを指すようにします。ローミングするユーザおよびローミング先となるサイトが非常に多い場合、この方法は設定と管理の負荷が大きくなります。
- 次の項（「回線/デバイス アプローチによる Unified CM のサービス クラスの構築」（P.10-44））で説明する回線/デバイス アプローチを実装します。

（注）　Cisco Emergency Responder を使用する場合は、デバイスに設定するサイト固有のコーリング サーチ スペースに、Cisco Emergency Responder を指す 911 CTI ルート ポイントを含むパーティションを含める必要があります。その同じパーティションに、同じ 911 CTI ルート ポイントを指すトランスレーション パターン 9.911 も含めると、ユーザは 9911 をダイヤルして救急サービスに連絡することができます。

回線 / デバイス アプローチによる Unified CM のサービス クラスの構築

前の項で説明した従来のアプローチは、集中型コール処理を使用した大規模なマルチサイト配置に適用する場合、結果的にパーティションとコーリング サーチ スペースの数が非常に多くなることがあります。このような構成にする必要があるのは、デバイス コーリング サーチ スペースを使用して、パス選択（外部コールにどの公衆網ゲートウェイを使用するか）とサービス クラスの両方を決定しているためです。

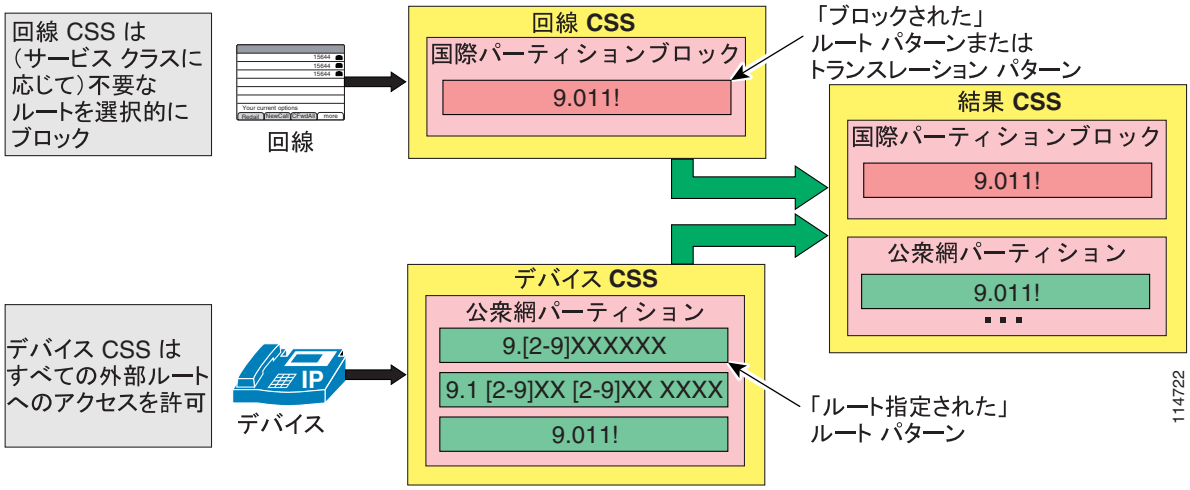
これらの 2 つの機能を回線コーリング サーチ スペースとデバイス コーリング サーチ スペースに分配すると、必要となるパーティションとコーリング サーチ スペースの総数を大幅に減らすことができます。この手法を *回線 / デバイス アプローチ* と呼びます。

所定の各 IP Phone の回線コーリング サーチ スペースとデバイス コーリング サーチ スペースが Unified CM でどのように組み合されているか、および回線コーリング サーチ スペースのパーティションが、結果のコーリング サーチ スペースでどのようにして最初に表示されるのか（「Unified CM におけるコール特権」（P.10-79）を参照）に注目すると、回線 / デバイス アプローチでは、一般に次の規則を適用できます。

- デバイス コーリング サーチ スペースは、コール ルーティング情報（たとえば、どのゲートウェイを公衆網コール用に選択するか）を提供するために使用します。
- 回線コーリング サーチ スペースは、サービス クラス情報（たとえば、どのコールを許可するか）を提供するために使用します。

これらの規則がどのように適用されるのかをわかりやすくするために、図 10-13 に示す例について考えます。このデバイス コーリング サーチ スペースは、国際番号を含めて、すべての公衆網番号へのルート パターンが入ったパーティションを保持しています。このルート パターンは、ルート リストおよびルート グループを通じて、公衆網ゲートウェイを指しています。

図 10-13　回線 / デバイス アプローチにおける重要な概念



同時に、回線コーリング サーチ スペースは、トランスレーション パターンが 1 つのみ入ったパーティションを保持しています。このパターンは国際番号に一致し、ブロック パターンとして設定されています。

したがって、結果のコーリング サーチ スペースには、国際番号に一致する 2 つの同一パターンが保持されています。最初に表示されるのは、回線コーリング サーチ スペースに含まれているブロック パターンです。結果として、この回線からの国際通話はブロックされます。

回線コーリング サーチ スペースでは、トランスレーション パターンの代わりに、ルート パターンを使用してコールをブロックすることもできます。ブロック ルート パターンを設定するには、まず、使用されていない IP アドレスを使用して「ダミー」ゲートウェイを作成し、そのゲートウェイを「ダミー」ルート リストおよびルート グループに配置します。次に、ダミー ルート リストを指すようにルート パターンを設定します。コールをブロックするルート パターンとトランスレーション パターンの主な違いは、ブロックされている番号をエンドユーザがダイヤルしようとしたときの対応です。次に例を示します。

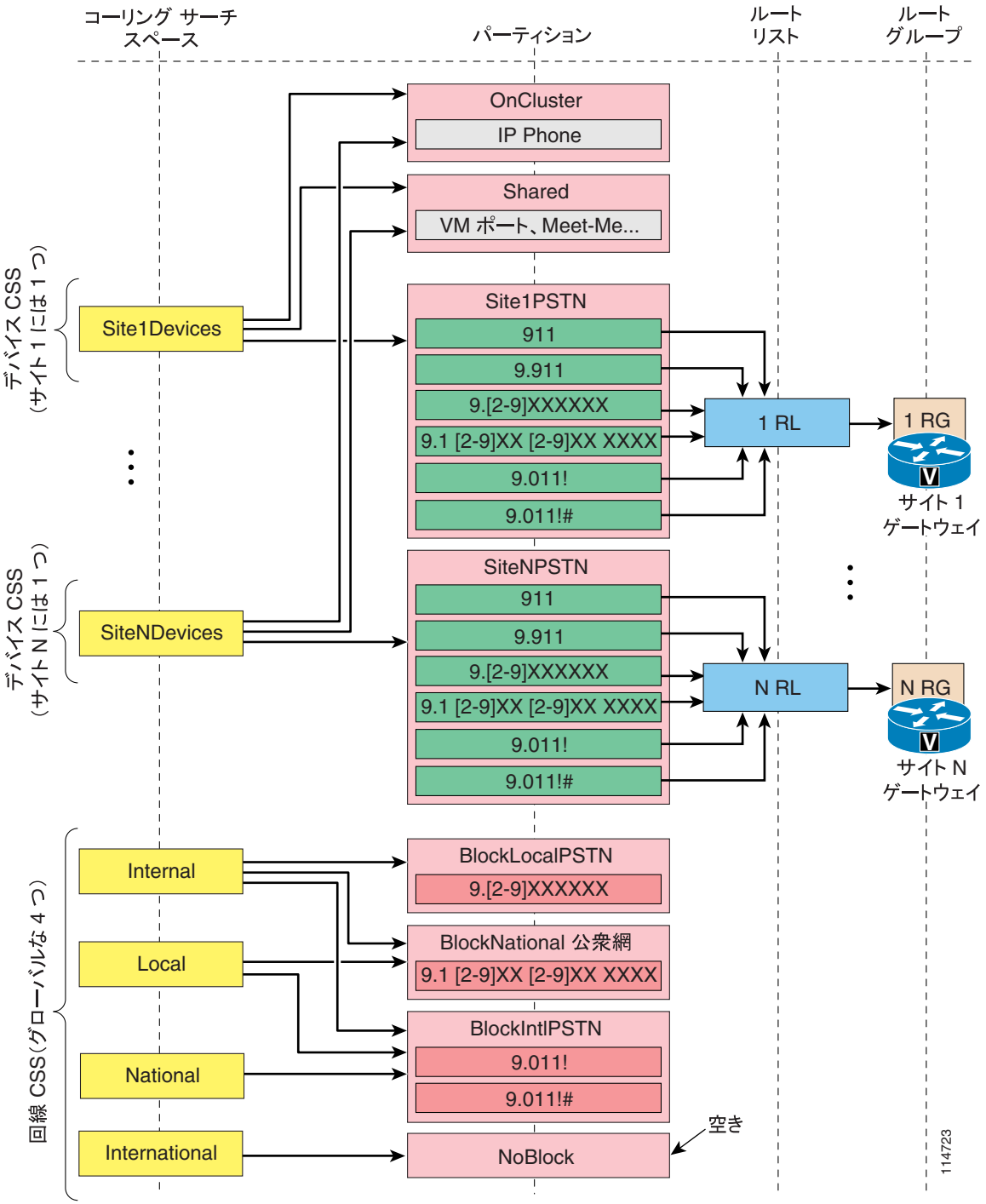
- ルート パターンを使用した場合、エンド ユーザは番号を最後までダイヤルでき、ダイヤルが完了して初めてユーザにファーストビジー トーンが再生されます。
- トランスレーション パターンを使用した場合は、エンド ユーザのダイヤルしている番号が許可パターンに一致する可能性がなくなると、その時点ですぐにファーストビジー トーンが再生されます。この動作は、SCCP を実行している IP Phone、または SIP を実行し、電話機に SIP ダイヤル規則が設定されていないタイプ B の IP Phone を前提にしています。

集中型コール処理を使用するマルチサイト配置に対して回線/デバイス アプローチを実装する場合は、さらに次のガイドラインに従ってください。

- サイトごとに無制限のコーリング サーチ スペースを作成し、電話機のデバイス コーリング サーチ スペースに割り当てます。このコーリング サーチ スペースには、電話機のロケーションに適したゲートウェイ（たとえば、同じ場所に配置されている緊急サービス用の支店ゲートウェイと、長距離電話用の中央ゲートウェイ）にコールをルーティングするルート パターンを備えたパーティションが含まれていなければなりません。
- ユーザのダイヤリング権限に含まれていないタイプのコールに対するブロック トランスレーション/ルート パターンを備えたパーティションを含むコーリング サーチ スペースを作成し、ユーザの回線に割り当てます。たとえば、ユーザが国際コール以外のすべてのタイプのコールを利用できる場合、そのユーザの回線は、9.011! ルート パターンをブロックするコーリング サーチ スペースを使用して設定する必要があります。

図 10-14 は、N 個のサイトがあるマルチサイト配置に対して、これらのガイドラインを適用する方法の例を示しています。

図 10-14　回線 / デバイス アプローチで必要となるコーリング サーチ スペースとパーティション



この方法の利点として、サイトごとに必要なサイト固有の無制限コーリング サーチ スペースが支店に 1 つのみであるという点があります。ダイヤリング権限は、ブロック ルート パターン（サイトに依存しない）の使用により実装されるので、同じセットのブロック コーリング サーチ スペースをすべての支店で使用できます。

結果として、必要なコーリング サーチ スペースの合計数とパーティションの合計数を計算するには、次の公式を使用できます。

合計パーティション数 =（サービス クラス数）+（サイト数）+（すべての IP Phone の DN 用に 1 パーティション）

合計コーリング サーチ スペース数 =（サービス クラス数）+（サイト数）

（注） これらの値は、最低限必要となるパーティション数とコーリング サーチ スペース数を表しています。特殊なデバイスやアプリケーションには、他のコール処理エージェント用のオンネット パターンと同様に、追加のパーティションやコーリング サーチ スペースが必要になることがあります。

（注） Cisco Emergency Responder を使用する場合は、911 CTI ルート パターンと 9.911 トランスレーション パターンをグローバルなオンクラスタ パーティションに含めることができます。

サイトの数が多い集中型コール処理配置に対して回線 / デバイス アプローチを適用すると、必要となるパーティションとコーリング サーチ スペースの数が大幅に減少します。たとえば、100 のリモート サイトと 4 つのサービス クラスがある配置の場合、従来のアプローチでは、少なくとも 401 のパーティションと 400 のコーリング サーチ スペースが必要です。回線 / デバイス アプローチでは、105 のパーティションと 104 のコーリング サーチ スペースしか必要ありません。

ただし、回線 / デバイス アプローチが成立するのは、特定サービス クラスの使用を制限する必要のある公衆網コールのタイプ（たとえば、市内電話、長距離電話、国際コール）を、グローバルに識別できる場合です。使用している国の国内番号計画が原因で、コール タイプをグローバルに識別することができない場合、このアプローチの効果は、（設定の省力化に関しては）上の公式に示したものよりも小さくなります。

たとえば、フランスでは、番号計画は 5 桁のエリア コード（01 ～ 05、および携帯電話の 06 エリア コード）に基づいており、この後に 8 桁の加入者番号が続きます。ここで重要となる特徴は、各公衆網宛先に到達するとき、同じローカルエリアからコールするときも、別のエリアからコールするときも、必ず同じ番号（たとえば、Paris の番号は 01XXXXXXXX、Nice の番号は 04XXXXXXXX など）をダイヤルすることです。つまり、「長距離電話」であるかどうかは、発信者がどのエリアにいるかに応じて変化します。このため、1 つのパーティションと 1 つのルート パターンでは、長距離電話へのアクセスをブロックできません。たとえば、発信者が Paris にいる場合、014455667788 へのコールは市内電話ですが、発信者が Nice や Lyon にいる場合は長距離電話です。

このような場合は、市内電話と長距離電話が同じ方法でダイヤルされるエリアごとに 1 つずつ、一連のブロック用コーリング サーチ スペースとパーティションを追加設定する必要があります。フランスの例では、表 10-8 に示すように、各エリア コードに対して 1 つずつ、5 組のブロック用コーリング サーチ スペースとパーティションを追加で定義する必要があります。

表 10-8　フランス国内番号計画に適用される回線 / デバイス アプローチ

コーリング サーチ スペース	パーティション	ブロック ルート パターン
Internal_css	BlockAllNational_pt	0.0[1-6]XXXXXXXX
	BlockIntl_pt	0.00!, 0.00!#
Local01_css	BlockLD01_pt	0.0[2-6]XXXXXXXX
	BlockIntl_pt	0.00!, 0.00!#
Local02_css	BlockLD02_pt	0.0[13-6]XXXXXXXX
	BlockIntl_pt	0.00!, 0.00!#

表 10-8　フランス国内番号計画に適用される回線/デバイス アプローチ （続き）

コーリング サーチ スペース	パーティション	ブロック ルート パターン
Local03_css	BlockLD03_pt	0.0[124-6]XXXXXXXX
	BlockIntl_pt	0.00!, 0.00!#
Local04_css	BlockLD04_pt	0.0[1-356]XXXXXXXX
	BlockIntl_pt	0.00!, 0.00!#
Local05_css	BlockLD05_pt	0.0[1-46]XXXXXXXX
	BlockIntl_pt	0.00!, 0.00!#
LD_css	BlockIntl_pt	0.00!, 0.00!#
Intl_css	NoBlock_pt	なし

回線/デバイス アプローチのガイドライン

回線/デバイス アプローチを使用する場合は、次のガイドラインを考慮してください。

- このアプローチが機能するには、回線コーリング サーチ スペース内に設定するブロック パターンの詳細度が、デバイス コーリング サーチ スペース内に設定したルート パターンと少なくとも同等になっている必要があります。エラーが発生することを避けるために、ブロックの対象となるパターンは、可能な場合にはルーティングを許可するパターンよりも詳細に設定することをお勧めします。@ ワイルドカード内に定義されるパターンは非常に詳細なものになるため、このワイルドカードの取り扱いには十分に注意してください。
- オンネット DN がダイヤルされると、AAR がトリガーされます。これらの DN へのアクセスは、上で説明したものと同じプロセスで制御できます。AAR は、再ルーティングされるコールには別のコーリング サーチ スペースを使用します。ほとんどの場合、AAR コーリング サーチ スペースは、サイト固有の無制限デバイス コーリング サーチ スペースと同じものでかまいません。このコーリング サーチ スペースは、エンドユーザによって直接ダイヤルされることがないためです。
- Call Forward All 動作に対する回線/デバイス アプローチのガイドラインについては、「自動転送コーリング サーチ スペース」（P.10-83）の項を参照してください。

（注）　回線とデバイスの優先順位は、CTI デバイス（CTI ルート ポイントと CTI ポート）に関しては逆になります。これらのデバイスの場合、結果のコーリング サーチ スペースでは、デバイス コーリング サーチ スペースに含まれているパーティションが、回線コーリング サーチ スペースよりも前に配置されます。そのため、パターン選択を連結の順序だけに頼らず、ブロックされるパターンの精度が許可されるパターンの精度よりも、すべてのケースで確実に高くなるよう注意しなければ、回線/デバイス アプローチを Cisco IP SoftPhone などの CTI デバイスに適用できません。

グローバル化された番号とサービス クラス

コーリング サーチ スペースに対する回線/デバイス アプローチを使用しているシステム管理者は、エンドポイントの回線 CSS で使用されるブロック パターンがローカル化された形式だけではなく、グローバル化された形式のコールもブロックする可能性があることに注意してください。ローカル化された形式の番号は local、regional、national に分類されますが、グローバル化された形式は分類されません。これによりサービス クラスの不一致が生じます。直接ユーザ ダイヤリングはサービス クラスに従属するのに対して、不在履歴リストと着信履歴リストからのワンタッチ ダイヤリングは従属しません。

たとえば、カナダのオンタリオ州 Ottawa にローカル サービス クラスを作成するとします。Ottawa のすべてのローカル コールはエリア コード 613 と 819 に分類され、ローカル コーリングは 10 桁のダイヤリングを使用して実行されます。ローカル化されたユーザ入力のみが Ottawa の電話機で許可されている場合、9[2-9]XX[2-9]XXXXXX の形式で行われたコールのみを許可することにより、「ローカル」

サービス クラスを電話機に適用できます。国内の（長距離）宛先に行われたすべてのコールは、国際電話（9 の後に 011）のように、異なるダイヤリング形式（オフネットのアクセス コード 9 の後に国内振り分けコード 1、その後に番号）で始まります。コールの形式によりクラスが定義されます。

ワンタッチ ダイヤルを実行する場合、電話機のダイヤル プランでローカル番号のグローバル形式が許可されます。ルート パターン +1 613 [2-9]XX XXXX ともう 1 つのパターン +1 819 [2-9]XX XXXX を追加して、ローカル コールが不在履歴または着信履歴コール リストからワンタッチ ダイヤルできるようにします。

ただし、すべての 613 および 819 エリア コード宛先がローカル コールとなるわけではないので、さらに複雑です。ローカル化されたパターンにより、ユーザがローカル宛先に対してのみコールを開始することを許可された場合（ダイヤル ストリングの先頭で 9 819 または 9 613 とダイヤル）、グローバル化されたパターンでは、エリア コード 613 または 819 のローカル以外の番号からのコールの受信が許可され、受信コール リストに移動し、番号をワンタッチ ダイヤルで返し、グローバル化されたパターンと照合します。このような場合、ルート パターンのグローバル形式は、ローカル コーリング エリアそのものを表すように修正する必要があります。上の例では、Ottawa のローカル コーリング エリア内のエリア コード 613 および 819 の正確なサブセットの定義を含みます。

回線/デバイス アプローチにおけるエクステンション モビリティの考慮事項

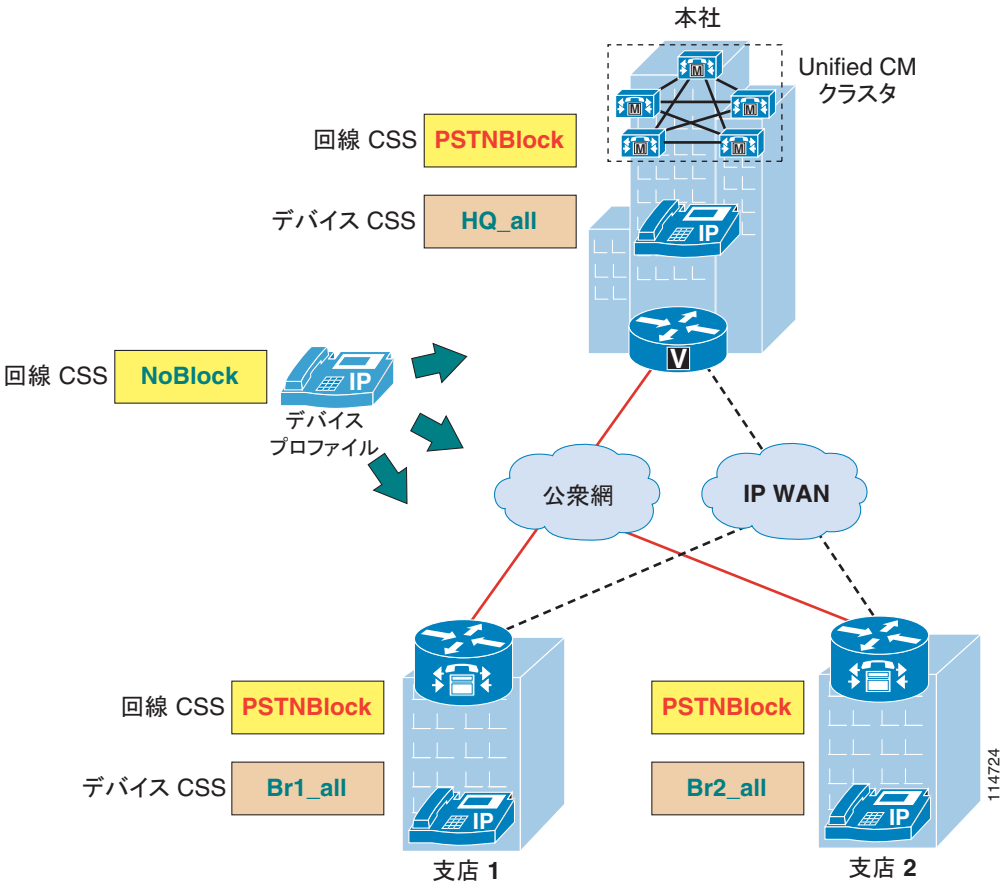
エクステンション モビリティ機能を使用する場合、電話機のダイヤル制限は、回線/デバイス アプローチを使用することによって、その電話機へのログイン（またはログアウト）中の機能の 1 つとして自然な方法で実装できます。ログアウトされた電話機は、他の電話機やサービス（たとえば、米国では 911）のコールを制限する必要があります。一般に、公衆網を通じた市内または市外通話へのアクセスは制限されます。逆に、ユーザがログインしている電話機は、そのユーザのダイヤリング権限に応じてコールを許可し、それらのコールを適切なゲートウェイ（たとえば、同じ場所に配置されているローカル コール用の支店ゲートウェイ）にルーティングする必要があります。

サービス クラスの構築に回線/デバイス アプローチを使用する場合は、前の項で説明したものと同じ規則を、エクステンション モビリティのデバイス プロファイル コンストラクトに適用するだけで済みます。エクステンション モビリティ使用時にコール制限を適用するには、次のガイドラインを考慮してください。

- 一致する可能性のあるすべての公衆網ルート パターンが入っていて、それらのパターンを適切にルーティングする（たとえば、緊急コールと市内電話にはローカル ゲートウェイを使用し、長距離電話には中央ゲートウェイを使用する）サイト固有のパーティションを指すように、各サイトのすべての IP Phone のデバイス コーリング サーチ スペースを設定します。
- ユーザがログインしていないときでも許可されるコール（たとえば、内部内線番号と緊急サービス）以外のコールをすべてブロックするブロック トランスレーション/ルート パターンを備えたグローバル コーリング サーチ スペースを指すように、すべての IP Phone の回線コーリング サーチ デバイス（または、デフォルト ログアウト デバイス プロファイルの回線コーリング サーチ スペース）を設定します。
- エクステンション モビリティ ユーザごとに、特定のサービス クラスに対して許可しない公衆網コールを選択してブロックする（たとえば、国際コールのみをブロックする）ブロック トランスレーション/ルート パターンを備えたグローバル コーリング サーチ スペースを指すように、回線コーリング サーチ スペースをデバイス プロファイル内に設定します。一部のユーザに無制限のコール特権を与える必要がある場合は、それらのユーザを空のパーティションを備えた回線コーリング サーチ スペースに割り当てます。

エクステンション モビリティに回線/デバイス アプローチを使用することの主な利点は、図 10-15 に示すように、集中型コール処理を使用するマルチサイト配置において、ユーザがホーム サイト以外の支店サイトにある IP Phone にログインしている場合でも、適切なコール ルーティングが保証されることです。

図 10-15　回線 / デバイス アプローチを使用したエクステンション モビリティ



この章ですでに説明したように、デバイス プロファイル内に設定した回線コーリング サーチ スペースは、ユーザがエクステンション モビリティを通じてログインすると、物理 IP Phone 上に設定されている回線コーリング サーチ スペースを置き換えます。コール ルーティングはデバイス コーリング サーチ スペースによって正しく処理されるため、ログイン操作は、単に電話のロックを解除するために使用されます。ログイン操作によって、（ブロック パターンを含んでいる）電話の回線コーリング サーチ スペースが削除され、（この単純化した例では、ブロック パターンを保持していない）デバイス プロファイルの回線コーリング サーチ スペースに置き換えられます。

コール ルーティングがすべてデバイス コーリング サーチ スペースの内部で実行されるのに対して、回線コーリング サーチ スペースは、単にブロック パターンを導入するだけです。このため、ユーザは、ホーム サイト以外のサイトにログインした場合、そのサイトのローカル ダイヤリング手順を自動的に継承します。たとえば、電話の DN は 8 桁番号として定義されているものの、各サイトの内部では、ローカル トランスレーション パターンによって 4 桁ダイヤリングが提供されているとします。この場合、別のサイトにローミングしたユーザは、ホーム サイトにいる同僚に 4 桁のみダイヤルして到達することはできなくなります。4 桁の番号は、ユーザがログインしたホスト サイトの規則に従って変換されるためです。

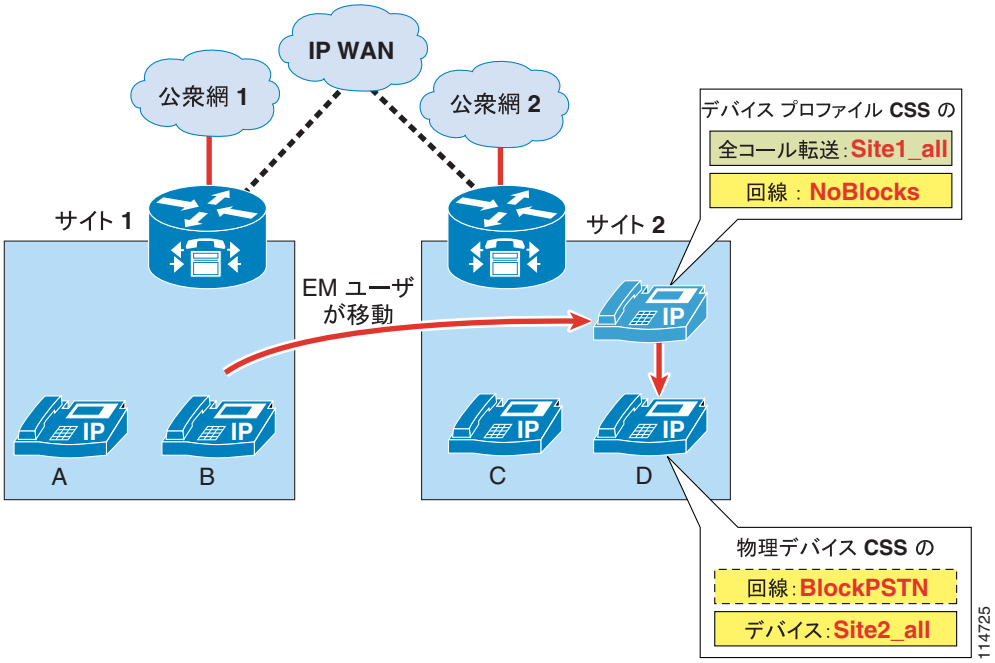
つまり、回線 / デバイス アプローチをエクステンション モビリティに使用する場合は、エンドユーザがログイン先サイトのダイヤリング手順に従う必要があります。

自動転送の考慮事項

エクステンション モビリティを使用する集中型コール処理環境に対して回線/デバイス コーリング サーチ スペース アプローチを適用する場合、ユーザがすべてのコールを外部公衆網番号に転送できるようにする必要があるときは、自動転送の動作に注意する必要があります。

図 10-16 では、エクステンション モビリティ ユーザが通常はサイト 1 を拠点としていて、そのデバイス プロファイルでは、無制限に公衆網コールを発信し、すべての着信コールを任意の公衆網番号に転送することが許可されています。

図 10-16　回線/デバイス アプローチを使用したエクステンション モビリティにおける自動転送の考慮事項



「自動転送コーリング サーチ スペース」（P.10-83）の項で説明したように、Forward All コーリング サーチ スペースは、回線およびデバイスのコーリング サーチ スペースとは連結されないため、Site1_all に設定する必要があります。Site1_all は、サイト 1 のゲートウェイを使用するすべての公衆網ルートを含んでいます。

このユーザがサイト 2 に移動して電話機 D にログインすると、ユーザのデバイス プロファイルに従って、このプロファイルの回線コーリング サーチ スペースと Forward All コーリング サーチ スペースが物理デバイスに適用されます。直接公衆網コールの場合、使用されるコーリング サーチ スペースは、回線とデバイスのコーリング サーチ スペースを連結したものです。電話 D のデバイス コーリング サーチ スペース（Site2_all）は、サイト 2 のゲートウェイを正しく指しています。

このユーザが、すべてのコールを公衆網番号に転送するように電話を設定すると、転送されるすべてのコールは、Site1_all コーリング サーチ スペースを使用します。Site1_all は、サイト 1 のゲートウェイを指したままです。この状態になると、次のような動作が発生します。

- 着信公衆網コールは、サイト 1 のゲートウェイで IP ネットワークに入り、同じゲートウェイ内で公衆網にヘアピンされます。
- サイト 1 の電話（電話機 A など）から発信されるコールは、サイト 1 のゲートウェイを通じて公衆網に正しく転送されます。
- サイト 2 の電話（電話機 C など）から発信されるコールは、WAN を経由してサイト 1 に到達し、サイト 1 のゲートウェイを通じて公衆網にアクセスします。同じ Unified CM クラスタ内の他のサイトから発信されるコールに対しても、同じ動作が適用されます。

ネットワークを設計し、ユーザをトレーニングするときは、この動作に注意してください。

H.323 を使用している Cisco IOS でのサービス クラスの構築

次のシナリオでは、H.323 プロトコルを実行している Cisco IOS ルータにサービス クラスを定義する必要があります。

- 集中型コール処理を使用する Cisco Unified CM マルチサイト配置
- Cisco Unified Communications Manager Express（Unified CME）配置

集中型コール処理を使用した Unified CM マルチサイト配置では、通常、Unified CM 内のパーティションとコーリング サーチ スペースを使用してサービス クラスが実装されます。ただし、支店サイトと中央サイト間の IP WAN 接続が失われた場合は、Cisco SRST が支店 IP Phone の制御を取得し、パーティションとコーリング サーチ スペースに関する設定は、IP WAN 接続が復旧するまですべて使用できなくなります。したがって、SRST モードで動作している支店ルータ内にサービス クラスを実装することが望ましくなります。

同様に、Cisco Unified CME Express 配置の場合も、ルータには IP Phone 用のサービス クラスを実装するメカニズムが必要です。

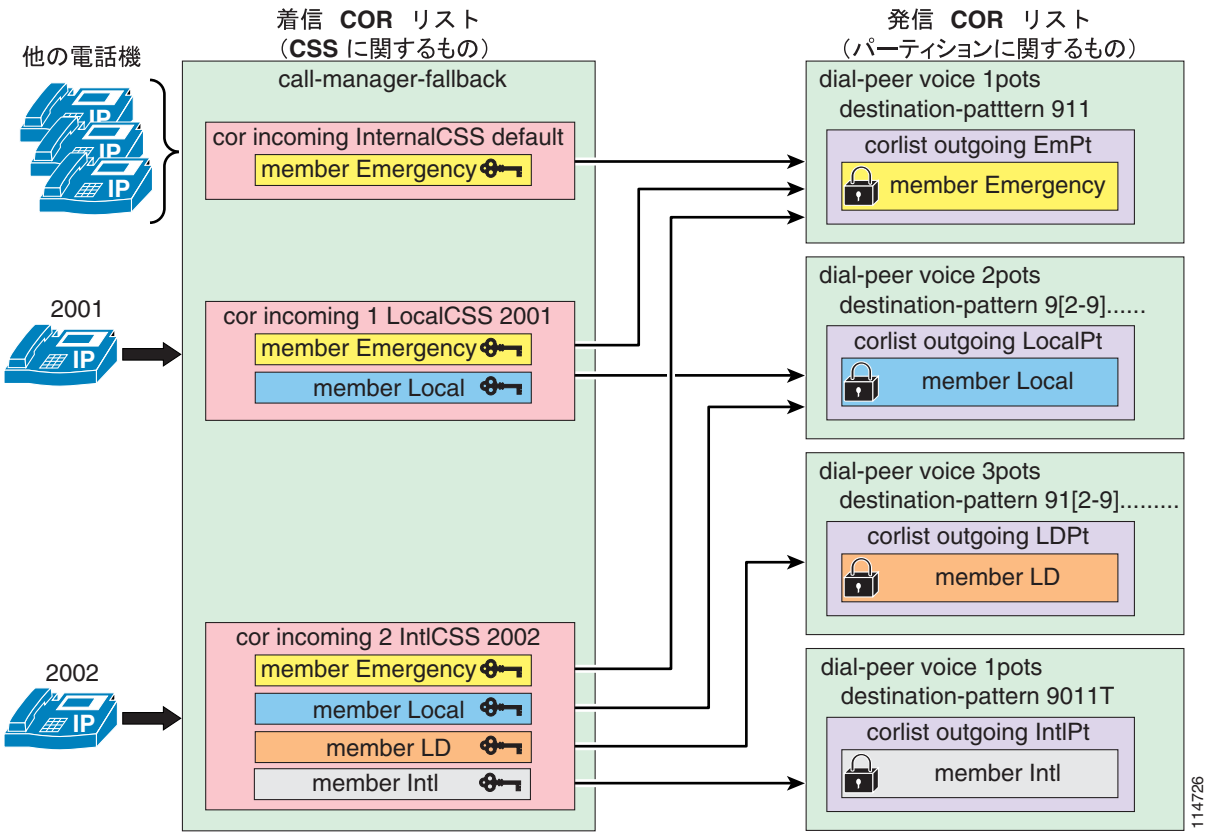
どちらの事例でも、制限クラス（COR）機能を使用して、サービス クラスを Cisco IOS ルータ内に定義します（COR の詳細については、「H.323 ダイヤル ピアを使用する Cisco IOS のコール特権」（P.10-121）を参照）。

次の主要ガイドラインに従うと、COR 機能を調整して、Cisco Unified CM のパーティションとコーリング サーチ スペースという概念を再現することができます。

- 区別する必要のあるコールのタイプごとに、タグを定義する。
- 各コール タイプをルーティングするそれぞれの POTS ダイヤル ピアに対して、メンバー タグを 1 つだけ含んだ、「基本的な」発信 COR リスト（パーティションに相当）を割り当てる。
- 各種のサービス クラスに属している IP Phone に対して、メンバー タグのサブセットを含んだ、「複雑な」着信 COR リスト（コーリング サーチ スペースに相当）を割り当てる。

図 10-17 では、SRST に基づいた実装例を示しています。DN が 2002 の IP Phone は、無制限の公衆網アクセスを許可され、DN が 2001 の IP Phone は、ローカル公衆網アクセスのみを許可されています。その他のすべての IP Phone は、内部番号と緊急サービスにのみアクセスできるように設定されています。

図 10-17　COR を使用した Cisco SRST 用サービス クラスの構築



次の手順では、図 10-17 のような Cisco IOS ソリューションの実装例とガイドラインを示します。

ステップ 1　**dial-peer cor custom** コマンドを使用して、各種コールの内容をわかりやすく表しているタグを定義します（この例では、Emergency、VMail、Local、LD、Intl）。

```
dial-peer cor custom
  name Emergency
  name VMail
  name Local
  name LD
  name Intl
```

ステップ 2　**dial-peer cor list** コマンドを使用して、パーティションとして使用される基本的な COR リストを定義します。各リストには、タグを 1 つのみメンバーとして含めます。

```
dial-peer cor list EmPt
  member Emergency

dial-peer cor list VMailPt
  member VMail

dial-peer cor list LocalPt
  member Local

dial-peer cor list LDPt
  member LD

dial-peer cor list IntlPt
  member Intl
```

ステップ 3　**dial-peer cor list** コマンドを使用して、コーリング サーチ スペースとして使用される比較的複雑な COR リストを定義します。各リストには、必要となるサービス クラスに従って、タグのサブセットをメンバーとして含めます。

```
dial-peer cor list InternalCSS
  member Emergency
  member VMail

dial-peer cor list LocalCSS
  member Emergency
  member VMail
  member Local

dial-peer cor list LDCSS
  member Emergency
  member VMail
  member Local
  member LD

dial-peer cor list IntlCSS
  member Emergency
  member VMail
  member Local
  member LD
  member Intl
```

ステップ 4　**corlist outgoing** *corlist-name* コマンドを使用して、基本的な「パーティション」COR リストを、対応する POTS ダイヤル ピアに割り当てる発信 COR リストとして設定します。

```
dial-peer voice 100 pots
  corlist outgoing EmPt
  destination-pattern 911
  no digit-strip
  direct-inward-dial
  port 1/0:23

dial-peer voice 101 pots
  corlist outgoing VMailPt
  destination-pattern 914085551234
  forward-digits 11
  direct-inward-dial
  port 1/0:23

dial-peer voice 102 pots
  corlist outgoing LocalPt
  destination-pattern 9[2-9].....
  forward-digits 7
  direct-inward-dial
  port 1/0:23

dial-peer voice 103 pots
  corlist outgoing LDPt
  destination-pattern 91[2-9]..[2-9].....
  forward-digits 11
  direct-inward-dial
  port 1/0:23

dial-peer voice 104 pots
  corlist outgoing IntlPt
  destination-pattern 9011T
  prefix-digits 011
  direct-inward-dial
  port 1/0:23
```

ステップ 5　**cor incoming** コマンドを **call-manager-fallback** コンフィギュレーション モードで使用して、「コーリング サーチ スペース」として機能する複雑な COR リストを、各種の電話 DN に割り当てる着信 COR リストとして設定します。

```
call-manager-fallback
  cor incoming InternalCSS default
  cor incoming LocalCSS 1 3001 - 3003
  cor incoming LDCSS 2 3004
  cor incoming IntlCSS 3 3010
```

SRST 用の COR を配置する場合は、次の制限事項に注意してください。

- Cisco IOS Release 12.2(8)T 以降で使用可能な SRST バージョン 2.0 では、**call-manager-fallback** で許容される **cor incoming** ステートメントの数は、最大で 5（デフォルト ステートメント含まず）です。
- Cisco IOS Release 12.3(4)T 以降で使用可能な SRST バージョン 3.0 では、**call-manager-fallback** で許容される **cor incoming** ステートメントの数は、最大で 20（デフォルト ステートメント含まず）です。

したがって、デフォルト以外の特権を持つユーザの電話 DN が連続しておらず、SRST サイトが比較的大きい場合は、SRST モードのサービス クラスの数を減らして、これらの制限値を超えずにすべての DN に対応できるようにする必要があります。

上の例は Cisco SRST に基づいていますが、Cisco Unified Communications Manager Express（Unified CME）配置にも同じ概念を適用することができます。ただし、次の考慮事項があります。

- Unified CME を使用している場合は、サービス クラスを表現している COR リスト（コーリング サーチ スペースに相当するもの）を個々の IP Phone に直接割り当てることができます。割り当てるには、**cor** {**incoming** | **outgoing**} *corlist-name* コマンドを **ephone-dn** *dn-tag* コンフィギュレーション モードで使用します。
- COR リストの設定されていない IP Phone は、COR の一般規則に従って、発信 COR リストの内容に関係なくすべてのダイヤル ピアに無制限にアクセスできます。Unified CME は、すべての電話にデフォルトの制限を適用する、**cor incoming** *corlist-name* **default** コマンドに相当するメカニズムを備えていません。

コール カバレッジの配置

コール カバレッジ機能は、多くの IP テレフォニー配置で重要となる機能です。顧客サービスを重視する多くの企業では、顧客のコールを適切なサービス部門に迅速にルーティングすることが必須になります。この項では、ハント パイロット、ハント リスト、および回線グループに基づいたハンティング メカニズムを使用して、Cisco Unified CM Release 4.1 でコールを分配する場合の設計ガイドラインを中心に説明します。ここでは、次のトピックを主に扱います。

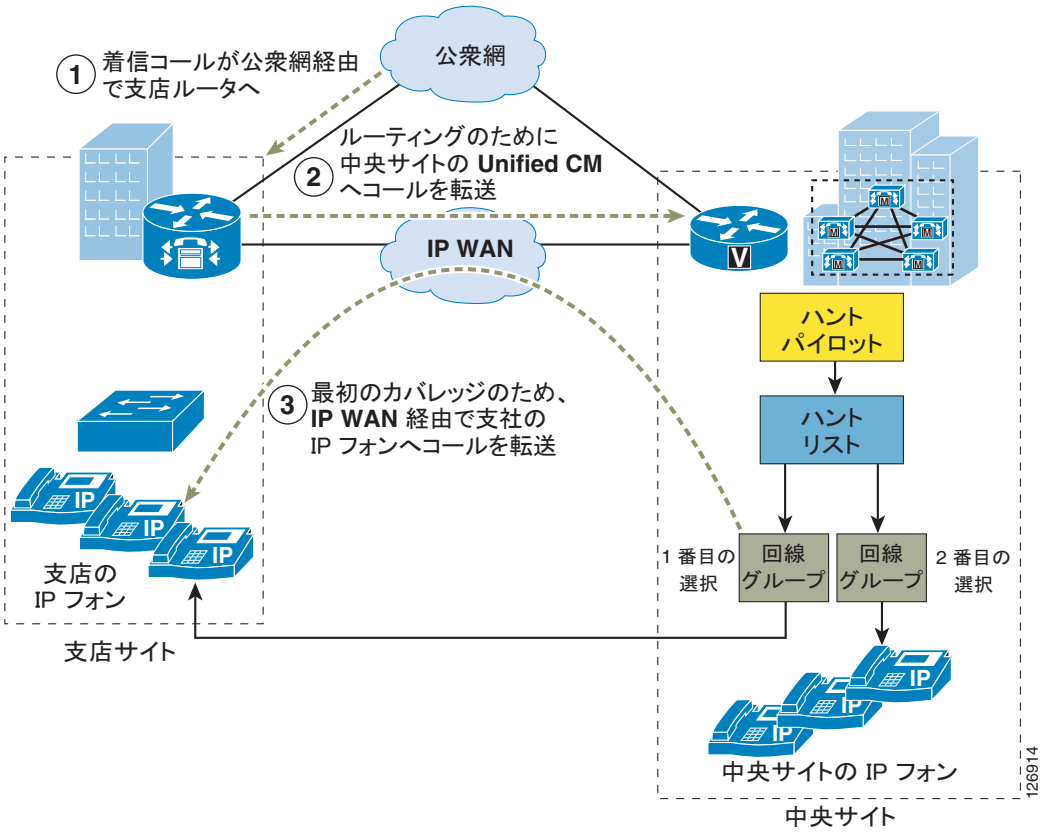
- 「マルチサイト集中型コール処理モデルへのコール カバレッジの配置」（P.10-56）
- 「マルチサイト分散型コール処理モデルへのコール カバレッジの配置」（P.10-57）

（注）　コール カバレッジ機能自体はコール キューを提供せず、発信側には、コールの宛先が見つかるまでリングバック トーンが送信されます。プロンプトや Music On Hold などを提供するため、シスコでは Cisco Unified Customer Voice Portal（CVP）などの多数のコンタクト センター テクノロジーを用意しています。シスコから入手可能なコンタクト センター テクノロジーの詳細については、http://www.cisco.com/go/ucsrnd で入手可能な資料を参照してください。

マルチサイト集中型コール処理モデルへのコール カバレッジの配置

図 10-18 では、マルチサイトの集中型コール処理配置における、ハント リストの設定例を示しています。この例では、最初にリモート オフィスのオペレータを通じてハント パイロット コールが分配されることを前提としています。コールは、応答されなかった場合やコール アドミッション制御によって拒否された場合、中央サイトのオペレータまたはボイスメールにルーティングされます。

図 10-18　　集中型コール処理配置における複数のサイト間でのコール カバレッジ



集中型の IP テレフォニー システムでは、Automated Alternate Routing（AAR）や Survivable Remote Site Telephony（SRST）などの機能を有効にすることで、高い可用性を実現できます。AAR 機能や SRST 機能を有効にしたうえでコール カバレッジ機能を配置する場合は、次のガイドラインを考慮してください。

- Automated Alternate Routing（AAR）

  回線グループのメンバーは、複数のロケーションおよびリージョンに割り当てることができます。ロケーションを通じて実装したコール アドミッション制御は、想定どおりに動作します。ただし、ハント パイロットから分配されているコールは、WAN の帯域幅が不足していたためにいずれかの回線グループ メンバーへのコールが Unified CM によってブロックされた場合には、AAR を使用して再ルーティングされることはありません。代わりに、Unified CM はコールを使用可能な次のメンバーまたは回線グループに分配します。

（注） AAR のみを使用する場合は、回線グループ内でボイスメール ポートを使用することを強くお勧めします。

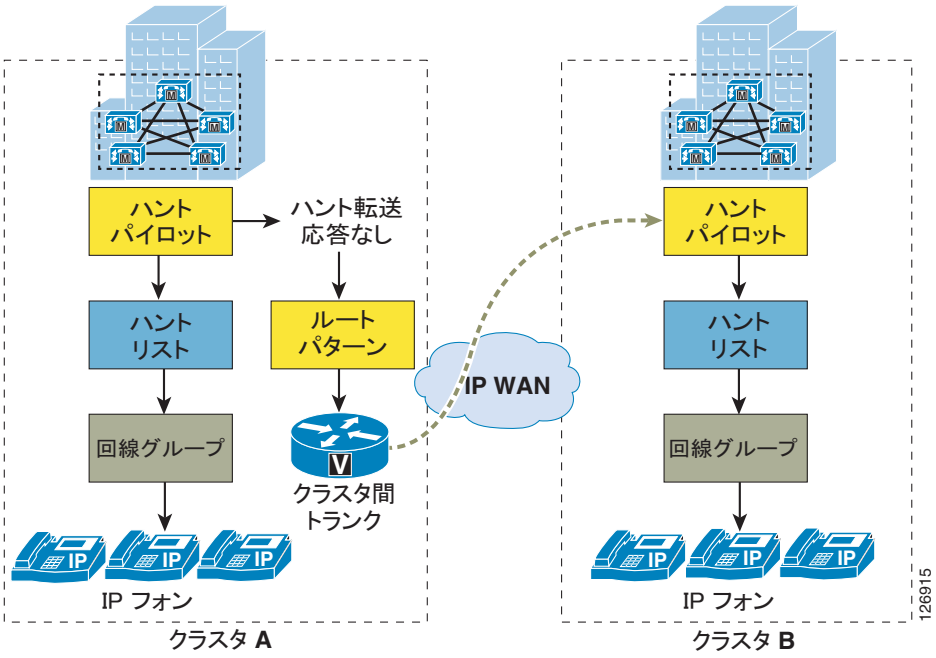
- Survivable Remote Site Telephony（SRST）
  - Unified CM がハント パイロットのコールを受信したとき、その回線グループ メンバーの一部が、SRST モードで動作しているリモート サイトにある場合、Unified CM はそれらのメンバーをスキップし、使用可能な次の回線グループ メンバーにコールを分配します。Unified CM から見ると、SRST モードで動作しているメンバーは未登録であり、ハント パイロットのコールは未登録メンバーには転送されません。
  - SRST モードで動作しているルータがハント パイロットのコールを受信したときは、コール カバレッジ機能を使用できません。このコールは、使用可能な登録済み内線番号にコールを再ルーティングする設定が追加されていない場合、失敗します。**alias** コマンドまたは **default-destination** コマンドを Cisco IOS の **call-manager-fallback** モードで使用すると、ハント パイロットを宛先とするコールをオペレータ内線またはボイスメールに再ルーティングすることができます。

マルチサイト分散型コール処理モデルへのコール カバレッジの配置

Cisco Unified CM Release 4.1 以降では、ルート グループをハント リストに追加することができなくなりました。このため、ハント リストを使用して、コールを他のクラスタまたはリモート ゲートウェイに送信することはできません。ただし、Cisco Unified CM Release 4.1 で導入されたハント パイロットのハント オプション設定を使用して、ゲートウェイまたはトランクを指すルート パターンに対応付けることができます。

図 10-19 は、クラスタ間トランクを使用する分散型コール処理配置における、ハント リストの設定例を示しています。この例では、ハント パイロットのコールが最初にクラスタ A の内部に配置されます。コールに対する応答がない場合は、ルート パターンに一致する Forward Hunt No Answer 設定を使用して、コールがコール分配のためにクラスタ B に再ルーティングされます。このルート パターンは、クラスタ B に向かうクラスタ間トランクを指しています。

図 10-19　分散型コール処理配置におけるクラスタ間でのコール カバレッジ



ヒント　分散型コール処理配置では、Cisco VoIP ゲートウェイとゲートキーパーを使用して、着信するハント パイロット コールのロード シェアリングを管理できます。あるクラスタ内でコールに応答がなかった場合は、そのコールを別のクラスタにオーバーフローしてサービスを提供できます。コールは、ゲートウェイまたはトランクを通じて IVR 処理に送信することもできます。Tool Command Language（TCL）IVR アプリケーションは、Cisco IOS ゲートウェイ上に実装できます。

ガイドライン

コール カバレッジ機能を分散型コール処理モデルに配置する場合、コールが複数のクラスタに分配されると、ルート パターンは発信または着信のルート グループ デバイス上で実行される番号変換を考慮に入れて、ルート パターンを適切に設定する必要があります。番号変換が実行されない場合、設定するルート パターンとハント パイロットは、すべてのクラスタ上で同一にする必要があります。同一でない場合は、コールが適切に分配されません。

ハント パイロットのスケーラビリティ

トップダウン、循環、および最長アイドル時間の各アルゴリズムを使用してコール カバレッジを配置する場合は、次のガイドラインを参考にすることをお勧めします。

- Unified CM クラスタは、最大で 15,000 のハント リスト デバイスをサポートします。
- ハント リスト デバイスは、1,500 個のハント リストそれぞれに 10 台の IP Phone を入れた組み合せにすることも、750 個のハント リストそれぞれに 20 台の IP Phone を入れた組み合せにすることもできます。ただし、ハント リストの数が多い場合は、その数に応じて、Unified CM のサービス パラメータで指定するダイヤル プラン初期化タイマーの値を大きくする必要があります。ダイヤル プラン初期化タイマーは、ハント リストを 1,500 個設定する場合、600 秒に設定することをお勧めします。

（注）　コール カバレッジにブロードキャスト アルゴリズムを使用する場合、ハント リスト デバイスの数は、Busy Hour Call Attempts（BHCA）の数によって制限されます。ブロードキャスト アルゴリズムを使用して、10 台の電話機を含むハント リストまたはハント グループを指すハント パイロットに対して 10 回の BHCA を行うことは、10 回の BHCA を行う 10 台の電話機と同じです。

- 1 つの回線グループ内に、コールをすべての DN に同時に送信することを目的として設定するディレクトリ番号の数は、最大で 35 までにすることをお勧めします。また、ブロードキャスト回線グループの数は、BHCC によって決まります。Unified CM システム内に複数のブロードキャスト回線グループがある場合、回線グループ内のディレクトリ番号の数は、35 よりも少なくする必要があります。すべてのブロードキャスト回線グループの Busy Hour Call Attempt（BHCA）の数が、1 秒あたり 35 コール セットアップを超えないようにします。

ダイヤル プランの要素

この項では、Cisco Unified Communication システムに含まれている次のダイヤル プラン要素について、設計と設定のガイドラインを示します。

- 「SCCP 電話機でのユーザ入力」（P.10-60）
- 「タイプ A の SIP 電話機でのユーザ入力」（P.10-61）
- 「タイプ B の SIP 電話機でのユーザ入力」（P.10-62）

IP Phone でのユーザ インターフェイス

さまざまな種類の IP 電話で、キーパッド入力が使用でき、視覚的な情報をさまざまな方法で提供します。この章では説明のため、次のタイプの電話機を定義します。

- タイプ A 電話機：Cisco Unified IP Phone 7905、7912、7940、および 7960
- タイプ B 電話機：Cisco Unified IP Phone 7911、7941、7942、7945、7961、7962、7965、7970、7971、および 7975

IP Phone での発信側の変換

発信側トランスフォーメーション パターンを使用すると、電話機へのコールのルーティングに使用する発信側のグローバル形式の番号を、ユーザ指定のローカル形式に適応させることができます。

トランスフォーメーション パターンは、照合される発番号の数値表現で構成されます。使用される構文は、ルート パターン、トランスフォーメーション パターン、ディレクトリ番号などのその他パターンの構文と同じです。

変換演算子には、数字破棄命令（ドット前の番号など）、発信側トランスフォーメーション マスク、プレフィックス番号が含まれます。この演算子によって、発信側電話番号表示（Default、Allowed、または Restricted）が制御されます。発信側トランスフォーメーション パターンを設定することで、発信側の外部電話番号マスクを発番号として使用できます。

パーティションおよびコーリング サーチ スペースによって、どの発信側トランスフォーメーション パターンをどの電話機に適用するかどうかが制御されます。電話機では、デバイス プールの発信側トランスフォーメーション コーリング サーチ スペース（CSS）またはデバイス固有の発信側トランスフォーメーション CSS を優先順位の低い順に使用できます。電話機に送信されるコールは、着信側トランスフォーメーション パターンを使用して処理されるのではありません。

電話機の場合、発信側トランスフォーメーション パターンは、電話機が鳴っている間に表示される番号には影響しますが、Missed Calls や Received Calls などのコール ディレクトリに格納される番号には影響しません。このディレクトリには、変換前の元の形式のまま格納されます。

電話機での + ダイヤリングのサポート

タイプ A およびタイプ B 電話機では、キーパッドを使用して + 記号をダイヤルすることはできませんが、Cisco Unified Personal Communicator エンドポイントでは、コンピュータのキーパッドにより、またはエンドポイントのクリック ダイヤル機能を使用しているときに入力ストリングの一部として + 記号を入力できます。

タイプ A の電話機では、+ 記号の表示はサポートされていません。

タイプ B の電話機および Cisco Unified Personal Communicator では、着信コールは + を番号の一部として発番号として表示できます。コールが電話機に送信されたとき、鳴っている電話機に表示される番号は、設定済みの任意の発番号トランスフォーメーション パターンによって処理されますが、Missed および Received コール ディレクトリに格納される番号は、変換前の元の番号です。これにより、+ 記号を発信番号として含む以前に受信したコールのワンタッチ ダイヤルが可能になります。

例 10-1　　+ ダイヤリングを使用する発番号

New York にあるタイプ B 電話機が +1 408 526 4000 からのコールを受信します。発信側トランスフォーメーション パターンは、電話機のデバイス プールの発信側変換 CSS に配置されています。パターンの 1 つは +1.!（ドットの前の番号を削除）と設定されています。

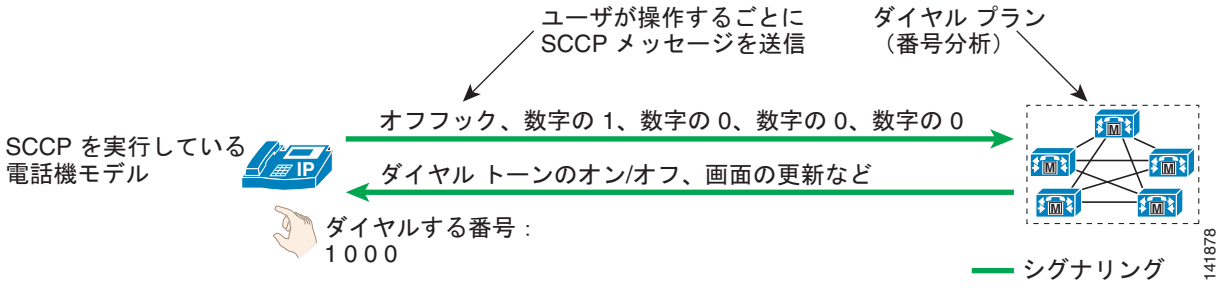
コールが鳴ると、着信側電話機に着番号 4085264000 が表示されます。コールに応答して解除された後、受信コールディレクトリに最新のコールが +1 408 526 4000 と表示されます。

SCCP 電話機でのユーザ入力

SCCP を使用する IP Phone は、すべてのユーザ入力イベントをただちに Unified CM に報告します。たとえば、ユーザがオフフックにするとすぐに、その電話機が登録されている Unified CM サーバに電話機からシグナリング メッセージが送信されます。電話機は 1 つの端末と考えることができ、Unified CM サーバに設定されたダイヤル プランによって、ユーザ入力に起因するすべての決定がその端末で下されます。

その他のユーザ イベントが電話機で検出されると、そのイベントは個別に Unified CM にリレーされます。オフフックして 1000 をダイヤルしたユーザは、電話機から Unified CM に 5 つの独立したシグナリング イベントをトリガーすることになります。その結果としてユーザに提供されるフィードバック、たとえば画面メッセージ、ダイヤル トーンの再生、2 次ダイヤル トーン、リングバック、リオーダーなどは、Unified CM がダイヤル プラン設定に基づいて電話機へ発行するコマンドです（図 10-20 を参照）。

図 10-20　　SCCP 電話機でのユーザ入力とフィードバック



SCCP を実行する IP Phone 上にダイヤル プラン情報を設定する必要はなく、また設定できません。ダイヤル プラン機能は、ユーザ入力が収集されたときのダイヤリング パターンの認識も含めて、すべて Unified CM クラスタに含まれています。

ユーザのダイヤルしたパターンが Unified CM に拒否された場合は、そのパターンが Unified CM の番号分析でベストマッチになるとすぐに、そのユーザに対してリオーダー トーンが再生されます。たとえば、1 分刻みで課金される番号計画エリア（または市外局番）976 へのコールがすべて拒否される場合は、ユーザが 91976 をダイヤルするとすぐに、そのユーザの電話機にリオーダー トーンが送信されます。

タイプ A の SIP 電話機でのユーザ入力

タイプ A 電話機はタイプ B 電話機と動作が少し異なり、タイプ B 電話機では Key Press Markup Language（KPML）がサポートされていますが、タイプ A 電話機ではサポートされません（「タイプ B の SIP 電話機でのユーザ入力」（P.10-62）を参照）。

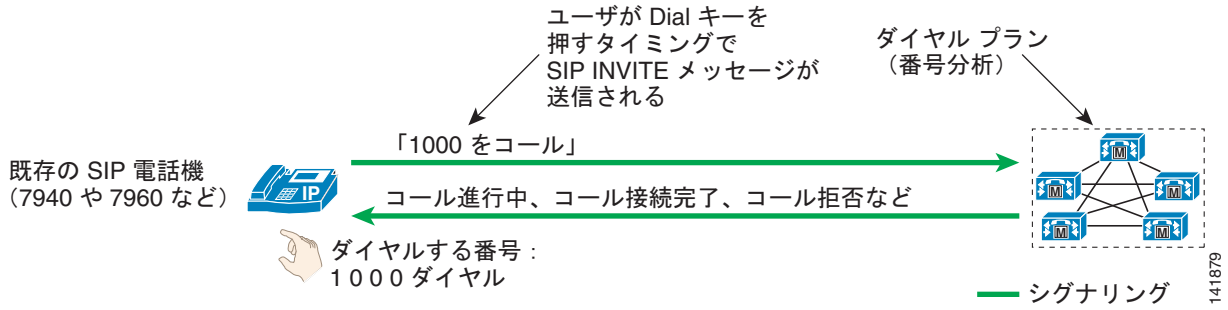
SIP を使用するタイプ A の IP Phone には、次の 2 つの異なる動作モードがあります。

- 「電話機に SIP ダイヤル規則が設定されていない場合」（P.10-61）
- 「電話機に SIP ダイヤル規則が設定されている場合」（P.10-62）

電話機に SIP ダイヤル規則が設定されていない場合

図 10-21 は、電話機にダイヤル プラン規則が設定されていない SIP タイプ A 電話機の動作を表しています。このモードでは、電話機はユーザが # キーを押すか Dial ソフトキーを押すまで、すべてのユーザ入力イベントを蓄積します。この機能は、多くの携帯電話で使用されている「送信」ボタンによく似ています。たとえば、内線 1000 にコールするユーザは、1、0、0、0 を押した後に Dial ソフトキーまたは # キーを押す必要があります。その後、電話機は Unified CM に SIP INVITE メッセージを送信し、内線 1000 へのコールの要求を示します。コールが Unified CM に到達すると、その電話機のダイヤル プラン設定に従います。その設定には、Unified CM のダイヤル プランに実装されているすべてのサービス クラスおよびコール ルーティング ロジックが含まれます。

図 10-21　ダイヤル規則が設定されていないタイプ A の SIP 電話機でのユーザ入力とフィードバック



ユーザが番号をダイヤルした後に Dial ソフトキーや # キーを押さなかった場合、電話機は桁間タイムアウト（デフォルトでは 15 秒）だけ待ってから、SIP INVITE メッセージを Unified CM に送信します。図 10-21 の例では、1、0、0、0 をダイヤルして桁間タイムアウトの時間だけ待つと、電話機は 10 秒後に内線 1000 にコールをつなぎます。

（注） ユーザが Redial ソフトキーを押した場合は、ただちに処理が行われるため、ユーザは Dial キーを押したり、桁間タイムアウトを待ったりする必要がありません。

ユーザが Unified CM に拒否されるパターンをダイヤルした場合、そのユーザはパターン全体を入力して Dial キーを押し、INVITE メッセージを Unified CM に送信した後でなければ、コールが拒否されたという通知（リオーダー トーン）は発信元に送信されません。たとえば、NPA 976 へのコールが拒否される場合は、919765551234 をダイヤルして Dial を押してから、リオーダー トーンが再生されます。

電話機に SIP ダイヤル規則が設定されている場合

SIP ダイヤル規則を使用すると、ユーザがダイヤルしたパターンを電話機が認識できます。認識作業が完了すると、SIP INVITE メッセージが Unified CM に自動的に送信され、ユーザは Dial キーを押したり、桁間タイムアウトを待ったりする必要がありません（詳細については、「SIP ダイヤル規則」（P.10-64）を参照してください）。

たとえば、企業の支店で同一支店内の電話機間のコールに 4 桁の内線番号をダイヤルする必要がある場合は、4 桁のパターンを認識するように電話機を設定すれば、ユーザが Dial キーを押したり、桁間タイムアウトを待ったりする必要がありません（図 10-22 を参照）。

図 10-22　ダイヤル規則が設定されているタイプ A の SIP 電話機でのユーザ入力とフィードバック

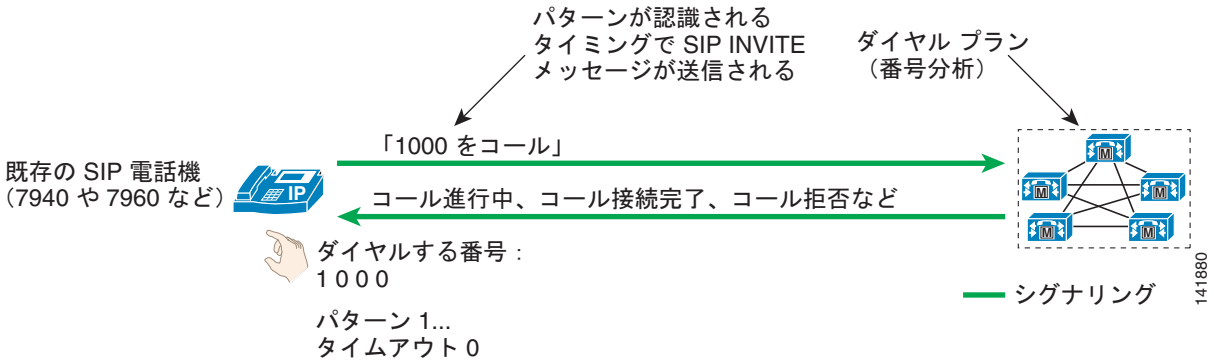


図 10-22 で、電話機は 1 で始まる 4 桁のパターンをすべて認識するように設定され、それに対応するタイムアウト値が 0 に設定されています。このパターンと一致するすべてのユーザ入力操作によって、SIP INVITE メッセージがすぐに Unified CM に送信され、ユーザが Dial キーを押す必要はありません。

SIP ダイヤル規則を使用するタイプ A 電話機では、電話機上に明示的に設定されていないパターンをダイヤルすることもできます。ダイヤルされたパターンが SIP ダイヤル規則と一致しない場合、ユーザは Dial キーを押すか、桁間タイムアウトを待ちます。

特定のパターンが電話機で認識され、それが Unified CM によってブロックされる場合、ユーザがダイヤル ストリング全体をダイヤルした後でなければ、コールがシステムで拒否されたという通知を受け取ることができません。たとえば、電話機に 919765551234 という形式でダイヤルされたコールを認識するように SIP ダイヤル規則が設定され、そのコールが Unified CM ダイヤル プランによってブロックされる場合、ユーザはダイヤリングの終了時（最後の 4 のキーを押した後）にリオーダー トーンを受信します。

タイプ B の SIP 電話機でのユーザ入力

タイプ B 電話機はタイプ A 電話機と動作が少し異なり、タイプ B 電話機では Key Press Markup Language（KPML）がサポートされていますが、タイプ A 電話機ではサポートされません（「タイプ A の SIP 電話機でのユーザ入力」（P.10-61）を参照）。

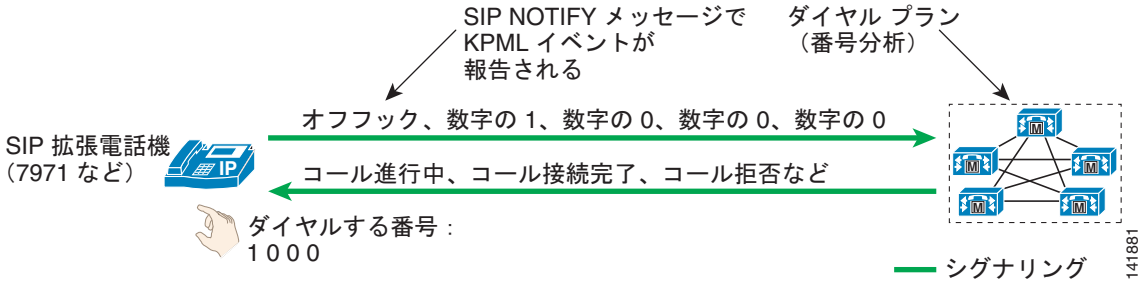
SIP を実行するタイプ B の IP Phone には、次の 2 つの異なる動作モードがあります。

- 「電話機に SIP ダイヤル規則が設定されていない場合」（P.10-63）
- 「電話機に SIP ダイヤル規則が設定されている場合」（P.10-63）

電話機に SIP ダイヤル規則が設定されていない場合

タイプ B の IP Phone は、Key Press Markup Language（KPML）に基づいて、ユーザによるキー操作を報告する機能を提供します。ユーザ入力イベントの 1 つ 1 つにより、Unified CM に対して KPML をベースとした独自のメッセージが生成されます。ユーザの個々の操作をすぐに Unified CM にリレーするという点では、この操作モードは SCCP を実行している電話機の操作モードと非常によく似ています（図 10-23 を参照）。

図 10-23　ダイヤル規則が設定されていないタイプ B の SIP 電話機でのユーザ入力とフィードバック



ユーザのすべてのキー操作によって、Unified CM に対する SIP NOTIFY メッセージがトリガーされることで、ユーザが押したキーに対応する KPML イベントが報告されます。このメッセージ機能により、Unified CM の番号分析はユーザが合成する部分パターンをその都度認識し、無効な番号がダイヤルされるとすぐにリオーダー トーンを再生するなど、適切なフィードバックを提供することができます。

ダイヤル規則なしに SIP を実行しているタイプ A の IP Phone とは異なり、タイプ B の SIP 電話機には、ユーザ入力の終わりを示す Dial キーがありません。図 10-23 では、1000 をダイヤルするユーザは、最後の 0 をダイヤルした後、Dial キーを押さなくても、コールプログレストーン（リングバック トーンかリオーダー トーン）を受け取ります。この動作は、SCCP プロトコルを実行する電話機のユーザ インターフェイスとの整合性がとれています。

電話機に SIP ダイヤル規則が設定されている場合

タイプ B の IP Phone では、ダイヤルされたパターンの認識が電話機によって行われるように SIP ダイヤル規則を設定できます（図 10-24 を参照）。

図 10-24　ダイヤル規則が設定されているタイプ B の SIP 電話機でのユーザ入力とフィードバック

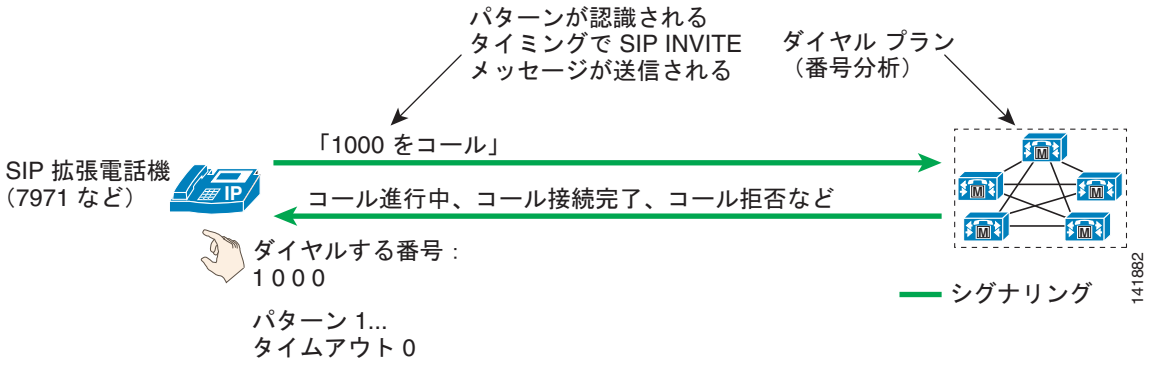


図 10-24 で、電話機は 1 で始まる 4 桁のパターンすべてを認識するように設定され、それに対応するタイムアウト値が 0 に設定されています。このパターンと一致するすべてのユーザ入力操作によって、Unified CM への SIP INVITE メッセージの送信がトリガーされます。

（注）　SIP ダイヤル規則がタイプ B の IP Phone に実装されるとすぐに、KPML ベースのダイヤリングは無効になります。ユーザが SIP ダイヤル規則と一致しない番号ストリングをダイヤルした場合は、個々の桁のイベントが、いずれも Unified CM にリレーされません。その代わり、ダイヤリングが完了すると（桁間タイムアウトの発生後）、ダイヤルされたストリング全体が Unified CM にまとめて送信されます。

SIP ダイヤル規則を使用するタイプ B 電話機では、電話機上に明示的に設定されていないパターンをダイヤルする方法は 1 つだけです。ダイヤルされたパターンが SIP ダイヤル規則と一致しない場合、ユーザは桁間タイムアウトを待った後でなければ、Unified CM に SIP NOTIFY メッセージが送信されません。タイプ A の IP Phone とは異なり、タイプ B の IP Phone にはオンフック ダイヤルを使用した場合を除いて、ダイヤリングの終わりを示す Dial キーがありません。その場合、ユーザはいつでも「Dial」キーを押すことで、ダイヤルしたすべての桁の Unified CM への送信をトリガーできます。

（注）　タイプ B 電話機を SRST ルータに登録した場合、設定した SIP ダイヤル規則は無効になります。

特定のパターンが電話機で認識され、それが Unified CM によってブロックされる場合、ユーザがダイヤル ストリング全体をダイヤルした後でなければ、コールがシステムで拒否されたという通知を受け取ることができません。たとえば、電話機に 919765551234 という形式でダイヤルされたコールを認識するように SIP ダイヤル規則が設定され、そのコールが Unified CM ダイヤル プランによってブロックされる場合、ユーザはダイヤリングの終了時（4 のキーを押した後）にリオーダー トーンを受信します。

SIP ダイヤル規則

Cisco Unified CM には、ユーザ入力が収集されたときに電話機でパターン認識を実行できるように、SIP ダイヤル規則機能が備わっています。たとえば、誰もが知る 911 というパターンを認識したら Unified CM にメッセージを送信し、すぐに緊急コールが開始されるように電話機を設定できます。それと同時に、ユーザが国際電話番号の可変長のパターンを入力できるようにも設定できます。

注意すべき重要な点は、SIP ダイヤル規則を使用して電話機にパターン認識を設定しても、Unified CM のサービス クラスとルート プランの設定の方が優先されることです。ある電話機が長距離通話のパターンを認識するように設定されていても、その電話機がローカル コールのみを許可するサービスクラスに割り当てられていると、Unified CM がそのコールをブロックします。

SIP ダイヤル規則には、それらの規則を設定する電話機のモデルに基づいて、次の 2 つのタイプがあります。

- 7905_7912（Cisco Unified IP Phone 7905 および 7912 に使用）
- 7940_7960_OTHER（上記以外のすべての IP Phone モデルに使用）

ダイヤル規則の一部として使用できる基本的なダイヤル パラメータは、次の 4 つです。

- パターン

  このパラメータは、パターンの実際の数値表現です。数字、ワイルドカード、2 次ダイヤル トーンを再生する命令を含めることができます。次の表は、2 つのタイプのダイヤル規則について、値とその効果を示しています。

	ダイヤル規則のタイプ	
パターン	**7905_7912**	**7940_7960_OTHER**
数字の 0 ～ 9	対応する数字。	対応する数字。
.	任意の数字（0 ～ 9）と一致します。	任意の文字（0 ～ 9、*、#）と一致します。
-	続けて追加の数字が入力される場合があることを示します。個々の規則の末尾に置く必要があります。	適用対象外
#	入力終了キー。ダイヤル規則の中に文字位置を示す > 文字を置くと、その文字位置以後は # キーが入力終了として認識されます。たとえば、9>#... と指定すると、9 が押された後は、いつでも # 文字が認識されます。	適用対象外
t*n*	*n* 秒のタイムアウト値を示します。たとえば、1...t3 は 1000 と一致し、3 秒後に Unified CM への Invite の送信をトリガーします。	適用対象外
r*n*	最後の文字を *n* 回繰り返します。たとえば、1.r3 は 1... に相当します。	適用対象外
S	パターンに修飾子 S が含まれていると、このパターン以後の他のダイヤル規則がすべて無視されます。実質的に、S によって規則照合が終了します。	適用対象外
*	入力終了キー。ダイヤル規則の中に文字位置を示す > 文字を置くと、その文字位置以後は * キーが入力終了として認識されます。	1 文字以上と一致します。たとえば、パターン 1* は 10、112、123456 などと一致します。
,	適用対象外	電話機で 2 次ダイヤル トーンを再生します。たとえば、8,.... と指定すると、ユーザには 8 を押した後に 2 次ダイヤル トーンが聞こえます。

- IButton

  このパラメータは、ダイヤル パターンの適用対象となるボタンを指定します。ユーザが回線ボタン 1 でコールを開始しようとしている場合は、ボタン 1 用に指定されたダイヤル パターンのみが適用されます。このオプション パラメータを設定しなかった場合、ダイヤル パターンは電話機の

すべての回線に適用されます。このパラメータは、Cisco SIP IP Phone 7940、7941、7942、7945、7960、7961、7962、7965、7970、7971、および 7975 のみに適用されます。ボタン番号は、画面横にあるボタンの上から下の順に対応し、一番上のボタンが 1 になります。

- Timeout

  このパラメータは、システムがタイムアウトになり、ユーザが入力した番号にダイヤルするまでの時間を秒単位で指定します。ダイヤルされた番号がすぐにダイヤルされるようにするには、0 を指定します。このパラメータは、7940_7960_OTHER ダイヤル規則にのみ適用されます。このパラメータを省略した場合は、電話機のデフォルトの桁間タイムアウト値（デフォルトは 10 秒）が使用されます。

- User

  このパラメータは、ダイヤルされた番号に自動的に追加されるタグを表します。有効な値は、**IP**（Unified CM 以外の SIP コール エージェントが配置される場合）と **Phone** です。このパラメータは、7940_7960_OTHER ダイヤル規則にのみ適用されます。このパラメータはオプションであり、Unified CM が唯一のコール エージェントとなる配置では省略してください。

（注） Cisco Unified IP Phone 7905 および 7912 は、パターンを SIP ダイヤル規則内で作成された順に選択します。これに対し、その他の電話機モデルでは、最長一致のパターンが選択されます。次の表は、ユーザが 95551212 をダイヤルした場合に選択されるパターンを示しています。

SIP ダイヤル規則	7905_7912	7940_7960_OTHER
…… 9…….	最初に一致するパターンの ……. が選択されます。	最長一致パターンの 9……. が選択されます。

Unified CM におけるコール ルーティング

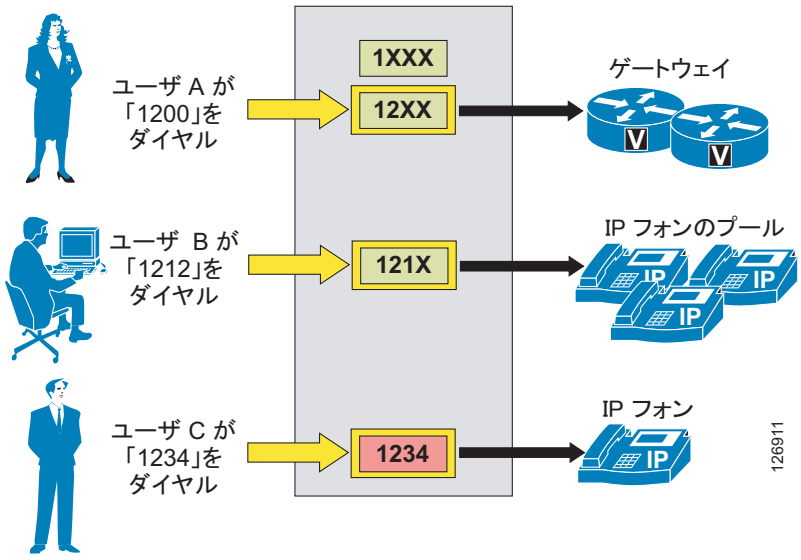
Unified CM 内に設定されるダイヤリング宛先は、すべて内部のコール ルーティング テーブルにパターンとして追加されます。このような宛先としては、IP Phone 回線、ボイスメール ポート、ルート パターン、トランスレーション パターン、および CTI ルート ポイントがあります。

番号がダイヤルされると、Unified CM では closest-match ロジックを使用し、コール ルーティング テーブルにあるすべてのパターンの中から一致パターンを選択します。一致する可能性のあるパターンが複数ある場合は、次の基準に基づいて宛先パターンを選択します。

- ダイヤルされたストリングに一致するもの。
- 一致する可能性のあるパターンのうち、ダイヤルされたストリング以外に一致するパターンが最も少ないもの。

たとえば、図 10-25 の場合を考えます。ここでは、コール ルーティング テーブルにパターン 1XXX、12XX、および 1234 が保持されています。

図 10-25　Unified CM のコール ルーティング ロジックの例



ユーザ A がストリング 1200 をダイヤルすると、Unified CM は、この番号をコール ルーティング テーブル内のパターンと比較します。この場合は、一致する可能性のあるパターンが 2 つあります（1XXX と 12XX）。両方ともダイヤルされたストリングに一致していますが、1XXX は合計 1,000 個のストリングに一致する一方で（1000 ～ 1999）、12XX は 100 個のストリングに一致します（1200 ～ 1299）。したがって、12XX がこのコールの宛先として選択されます。

ユーザ B がストリング 1212 をダイヤルした場合、一致する可能性のあるパターンは 3 つあります（1XXX、12XX、および 121X）。上で説明したように、1XXX に一致するストリングは 1,000 個あり、12XX に一致するストリングは 100 個あります。しかし、121X に一致するストリングは 10 個しかありません。したがって、このパターンがコールの宛先として選択されます。

ユーザ C がストリング 1234 をダイヤルした場合、一致する可能性のあるパターンは 3 つあります（1XXX、12XX、および 1234）。上で説明したように、1XXX に一致するストリングは 1,000 個あり、12XX に一致するストリングは 100 個あります。しかし、1234 に一致するストリングは 1 個しかありません（ダイヤルされたストリング）。したがって、このパターンがコールの宛先として選択されます。

（注）　Cisco Unified CM でディレクトリ番号（DN）を設定すると、それぞれのデバイス（IP Phone など）が登録済みかどうかにかかわらず、その番号はコール ルーティング テーブルに配置されます。この仕様によって、アプリケーション（およびそのプライマリ パターン）が未登録である場合、セカンダリの一致パターンを利用してフェールオーバー機能を提供することができなくなりました。プライマリ パターンがコール ルーティング テーブルに必ず存在するため、セカンダリ パターンに一致するかどうかは検索されません。

パターンにおける + 記号のサポート

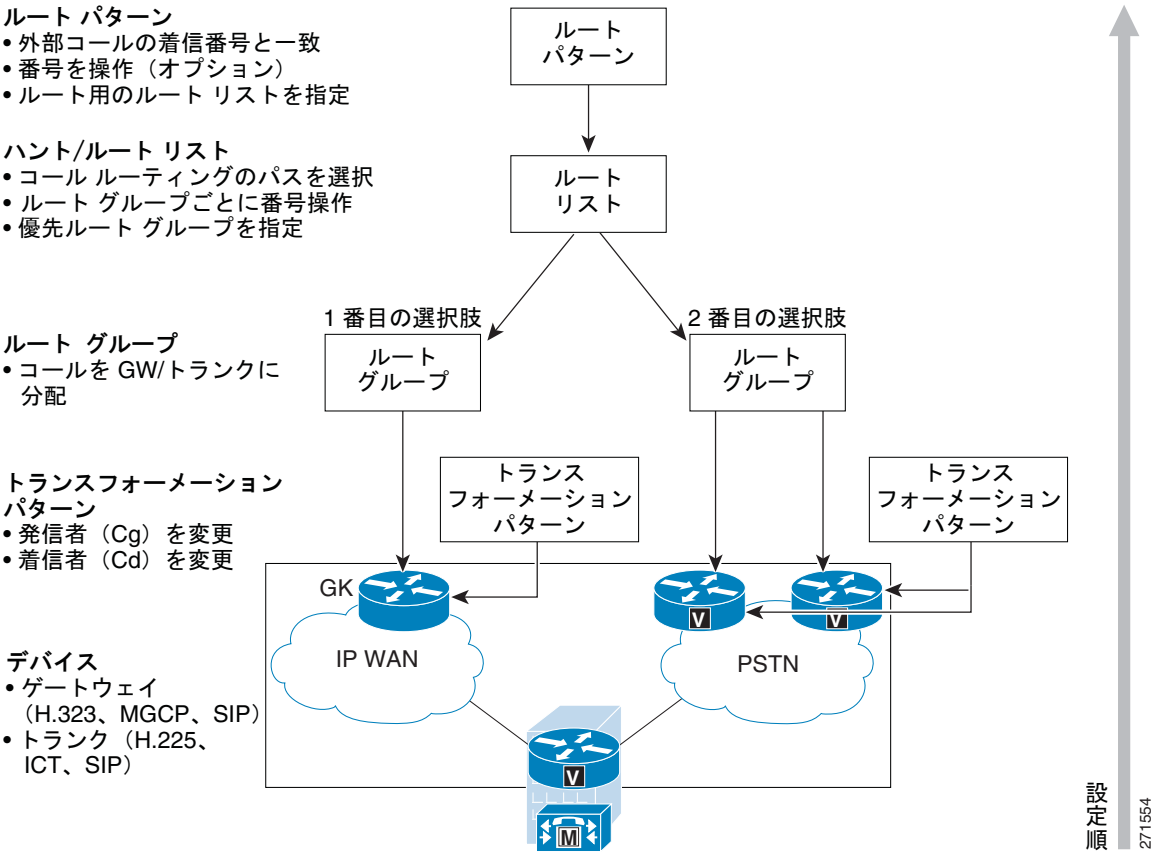
Unified CM 内のすべてのパターン（ルート パターン、トランスレーション パターン、ディレクトリ番号など）では、+ 記号を使用できます。+ を文字どおりの意味で使用するには、+ の前にエスケープ文字 \ を入力することで、先行文字の 1 つ以上のインスタンスを意味する正規表現演算子の + と区別します。次の例を参考にしてください。

- \+14085264000 は +14085264000 を意味します。
- 2+ は 2、22、222 などを意味します。

Unified CM の外部ルート

Unified CM は、同じクラスタ内の内部宛先にコールをルーティングする方法を自動的に「認識」します。公衆網ゲートウェイ、H.323 ゲートキーパー、またはその他の Unified CM クラスタなどの外部宛先の場合、外部ルート コンストラクト（次の項で説明）を使用して、明示的にルーティングを設定する必要があります。このコンストラクトは、3 層式のアーキテクチャに基づいています。このアーキテクチャでは、複数層のコール ルーティングと共に、番号操作も可能です。Unified CM は、外部ダイヤル ストリングと一致する設定済みルート パターンを検索し、それを使用して、対応するルート リストを選択します。ルート リストには、コールに使用可能なパスが優先順位順に並べられています。これらのパスは、ルート グループと呼ばれ、従来の PBX でトランク グループと呼ばれていたものに非常によく似ています。図 10-26 では、Unified CM 外部ルート コンストラクトの 3 層式アーキテクチャを示しています。

図 10-26　外部ルート パターンのアーキテクチャ



次の各項では、Unified CM の外部ルート コンストラクトの個々の要素について説明します。

- 「ルート パターン」（P.10-69）
- 「ルート リスト」（P.10-72）
- 「ルート グループ」（P.10-73）
- 「ルート グループ デバイス」（P.10-75）

ルート パターン

ルート パターンは、コールを外部エンティティにルーティングするために Unified CM で設定された、数字とワイルドカードを組み合せたストリング（たとえば、9.[2-9]XXXXXX）です。ルート パターンでは、コールをルーティングするゲートウェイを直接指すことも、ルート リストを指すこともできます。ルート リストはルート グループを指しており、最終的にゲートウェイを指します。

ルート パターン、ルート リスト、およびルート グループ コンストラクトを完全パスで指定することを強くお勧めします。その理由は、この構造を使用するとコール ルーティング、番号操作、および将来のダイヤル プランの拡張を最も柔軟に行うことができるからです。

@ ワイルドカード

- @ ワイルドカードは、特殊なマクロ関数であり、特定の国の番号計画全体を表す一連のパターンに拡張されます。たとえば、フィルタ処理されていない単一のルート パターン（たとえば、9.@）を北米番号計画を使用して設定すると、実際には、Unified CM の内部ダイヤル プラン データベースに 166 個の個別ルート パターンが追加されます。
- その他の国別番号計画を受け入れるように Unified CM を設定できます。この作業が完了すると、ルート パターン設定ページの Numbering Plan フィールドで選択した値に応じて、同じ Unified CM クラスタ内で、複数の番号計画に対して @ ワイルドカードを使用できるようになります。詳細については、次の Web サイトで入手可能な『*Cisco Unified CallManager Dial Plan Deployment Guide*』を参照してください。

  http://www.cisco.com/en/US/products/sw/voicesw/ps5629/prod_maintenance_guides_list.html
- @ ワイルドカードは、いくつかの中小規模の配置では十分に実務で使用できますが、大規模な配置では、管理とトラブルシューティングが困難になる可能性があります。これは、@ ワイルドカードを利用する場合、ルート フィルタを使用して、管理者が特定のパターンをブロックする必要があるためです（「ルート フィルタ」（P.10-69）を参照してください）。

ルート フィルタ

- ルート フィルタは、@ ワイルドカードによって作成されるルート パターン数を減らすために、@ ルート パターンと一緒にのみ使用します。@ ワイルドカードを含まないパターンに適用されるルート フィルタは、発生するダイヤル プランに影響を与えません。
- ルート フィルタと一緒に入力する論理式は、NOT-SELECTED フィールドを除いて、最大 1024 文字にすることができます。
- ルート フィルタ内の論理文節数が増えるにつれて、設定ページのリフレッシュ時間も増え、容認できないほど長くなる場合があります。
- 大規模な配置の場合、@ ワイルドカードとルート フィルタではなく、明示ルート パターンを使用してください。この方法を利用すると、管理とトラブルシューティングも容易になります。これは、Unified CM で設定されているすべてのパターンが、ルート パターン設定ページから簡単に参照できるからです。

国際および可変長ルート パターン

- 国際間の宛先は、通常、任意の桁数を表す ! ワイルドカードを使用して設定されます。たとえば、北米では通常、国際コール用にルート パターン 9.011! が設定されています。欧州諸国のほとんどでは、0.00! ルート パターンを使用することで同じ結果が得られます。
- ! ワイルドカードは、ダイヤルされた番号の長さが変化する国では配置にも使用されます。このような場合、Unified CM は、ダイヤルがいつ完了するかわからないので、コールの送信前に 15 秒待機します。この遅延は、次の方法のいずれかで短縮できます。

- ダイヤルの終わりを指定する T302 タイマー（サービス パラメータ TimerT302_msec）の値を減らします。ただし、ユーザがダイヤルを終了する前のコールの早期送信を防止するために、4 秒以上に設定します。
- # ワイルドカードで終了する同じパターンのルートパターンを設定し（たとえば、北米の場合 9.011!#、欧州の場合 0.00!#）、ダイヤルの終わりを示すために # をダイヤルするようにユーザに指示します。この処理は、携帯電話で送信ボタンを押すことに相当します。

重複送信と重複受信

国内の番号計画を静的ルート パターンで定義することが難しい国では、Unified CM に重複送信および重複受信を設定することができます。

重複送信とは、エンドユーザがダイヤルする番号を Unified CM で収集しながら、番号がダイヤルされると同時に公衆網に渡すことを意味します。重複送信を可能にするには、ルート パターン設定ページの Allow Overlap Sending チェックボックスをオンにします。以前の Unified CM リリースで重複送信を使用可能にするには、SendingCompleteIndicator サービス パラメータを False に設定します。ルート パターンには、公衆網アクセス コード（たとえば、北米では 9、欧州諸国の多くでは 0）を含めるだけです。

重複受信とは、ダイヤルされる番号を PRI 公衆網ゲートウェイから Unified CM で 1 つずつ受信し、ストリングのダイヤルが完了するまで待機し、その後でコールを内部宛先にルーティングすることを意味します。重複受信を可能にするには、OverlapReceivingFlagForPRI サービス パラメータを True に設定します。以前の Unified CM リリースでは、パラメータ名は OverlapReceivingForPriFlag です。

ルート パターンにおける番号操作

- コールで最終的に利用するルート グループに関係なく、ルート パターンで設定する番号操作は、発番号および着番号に影響を与えます。ルート リスト ビューにあるそのメンバーのルート グループに設定される番号操作が影響するのは、ルートに対してだけです。つまり、コールの発信に使用するルート グループに設定されている変換のみが実行されます。
- ルート リスト ビューにあるそのルート グループの番号操作は、ルート パターンに設定される番号操作よりも優先されます。
- ルート パターンやルート リストに設定される番号変換による発番号および着番号は、選択したルート グループに含まれるデバイスに設定されているトランスフォーメーション パターンで処理されます。
- ルート パターンで番号操作を設定する場合、コール詳細レコード（CDR）は、番号操作が行われた後のダイヤル番号を記録します。ルート グループのみで番号操作を設定する場合、CDR は、番号操作が行われる前の実際のダイヤル番号を記録します。
- 同様に、ルート パターンでの番号操作を設定すると、発信側の IP Phone ディスプレイには、操作後の番号が示されます。ルート グループのみで番号操作を設定する場合、この操作はエンドユーザには見えなくなります。

発呼回線 ID

- 発呼回線 ID の表示は、ゲートウェイで使用可能または使用不可にすることができます。また、サイトの要件に基づいて、ルート パターンで操作することもできます。
- Use Calling Party's External Phone Number Mask オプションを選択する場合、外部コールは、コールを発信する IP Phone に指定された発呼回線 ID を使用します。このオプションを選択しない場合、Calling Party Transform Mask フィールドに指定されたマスクが、発信者番号識別の生成に使用されます。

緊急プライオリティ

- Urgent Priority チェックボックスは、一般に、パターンに一致したコールを T302 タイマーの満了を待たずにすぐルーティングする目的で使用されます。たとえば、北米でパターン 9.911 と 9.[2-9]XXXXXX が設定されている場合、ユーザが 9911 をダイヤルすると、Unified CM は T302 タイマーが満了するまで待機し、その後でコールをルーティングします。これは、9911 の後に数字が入力されて、9.[2-9]XXXXXX に一致する可能性があるためです。9911 ルート パターンについて緊急プライオリティを有効にすると、Unified CM はユーザが 9911 とダイヤルした直後にルーティング処理を実行し、T302 タイマーの満了までは待機しません。
- Urgent Priority チェックボックスをオンにした場合に実行されるのは、設定済みのパターンがダイヤルされた番号とのベストマッチになったとき、その直後に T302 タイマーを満了させることです。つまり、緊急パターンが他のパターンよりも高い優先順位を持っているわけではありません。「Unified CM におけるコール ルーティング」（P.10-66）の項で説明した closest-match ロジックは、依然として有効です。

  たとえば、ルート パターン 1XX が緊急パターンとして設定され、パターン 12! が通常のルート パターンとして設定されているとします。ユーザが 123 とダイヤルした場合、Unified CM は 3 番目の数字を受信した直後にはルーティング処理を実行しません。1XX は緊急パターンであっても、ベストマッチではないからです（12! が合計 10 個のパターンに一致するのに対して、1XX は 100 個のパターンに一致）。パターン 12! では、ユーザがさらに番号を入力する可能性があるため、Unified CM は 桁間タイムアウトを待ってから、コールをルーティングする必要があります。

  別の例として、パターン 12[2-5] に緊急のマークが付けられ、12! が通常のルート パターンとして設定されているとします。ユーザが 123 とダイヤルすると、パターン 12[2-5] はベストマッチになります（12[2-5] が合計 4 個のパターンに一致するのに対し、12! は 10 個のパターンに一致）。緊急プライオリティ パターンがベストマッチなので、T302 タイマーは打ち切られ、それ以上のユーザ入力は想定されません。Unified CM は、パターン 12[2-5] を使用してコールをルーティングします。

コール分類

- このルート パターンを使用しているコールは、オンネットまたはオフネットのコールとして分類することができます。このルート パターンを使用すると、オフネット間でのコール転送を禁止したり、オンネット通話者がいないカンファレンス ブリッジを終了したりすることによって、料金詐欺を防止できます（これらの機能は、どちらも Unified CM Administration の Service Parameters を使用して制御します）。
- Allow device override チェックボックスをオンにすると、コールは、関連するゲートウェイまたはトランク上で、コール分類設定に基づいて分類されるようになります。

強制アカウント コード（FAC）

- Forced Account Codes（FAC; 強制アカウント コード）チェックボックスを使用すると、個々のルート パターンを使用して発信コールが制限されます。ルート パターンに対して FAC を有効にすると、ユーザは、目的のコール受信者に到達するための承認コードを入力するように要求されます。
- ユーザのダイヤルした番号が、FAC が有効になったルート パターンを通じてルーティングされるものである場合、システムは承認コードの入力を求めるトーンを再生します。コールを確立するには、ユーザ承認コードが、ダイヤルされた番号のルーティングに必要となる承認レベルを満たしているか、そのレベルを超えている必要があります。
- コール詳細レコード（CDR）に表示されるのは、承認名のみです。承認コードは CDR には表示されません。
- FAC 機能は、Allow overlap sending チェックボックスがオンの場合は使用できません。

クライアント識別コード（CMC）

- Client Matter Code（CMC; クライアント識別コード）チェックボックスを使用すると、個々のルート パターンを使用して特定番号へのコールがトラッキングされます。たとえば、企業で使用すると、特定のクライアントへのコールをトラッキングできます。
- ルート パターンに対して CMC を有効にすると、ユーザは目的の宛先に到達するためのコードを入力するように要求されます。
- ユーザのダイヤルした番号が、CMC が有効になったルート パターンを通じてルーティングされるものである場合、システムはコードの入力を求めるトーンを再生します。コールを確立するには、ユーザが正しいコードを入力する必要があります。
- クライアント識別コードは、コール詳細レコードに表示されます。これは、クライアントの課金およびアカウンティングに関するレポートを生成するための、CDR の分析およびレポート ツールで使用できるようにするためです。
- CMC 機能は、Allow overlap sending チェックボックスがオンの場合は使用できません。
- CMC と FAC を両方とも有効にすると、ユーザは番号をダイヤルするとき、FAC の入力を求められたら入力し、次のプロンプトで CMC を入力します。

ルート リスト

ルート リストは、発信コールに使用できるパス（ルート グループ）が優先順位順に並べられたリストです。ルート リストの標準的な用途は、リモートの宛先に 2 つのパスを指定することです。この場合、第一選択のパスは、IP WAN を介したパスであり、第二選択のパスは、公衆網ゲートウェイを介したパスです。

ルート リストには次の特性があります。

- 複数のルート パターンが同一ルート リストを指すことができます。
- ルート リストは、所定の宛先への代替パスの役目をするルート グループが、優先順位順に並べられたリストです。たとえば、ルート リストを使用して最低料金選択機能をサポートすることができます。この場合、リスト内のプライマリ ルート グループが、コールあたりのコストがより低くなるようにします。プライマリ ルート グループが「all trunks busy（全トランク使用中）」状態、または IP WAN リソースの不足により使用できない場合だけ、セカンダリ ルート グループが使用されます。
- ルート リスト内の各ルート グループは、独自の番号操作を行うことができます。たとえば、ルート パターンが 9.@ であるときに、ユーザが 9 1 408 555 4000 をダイヤルした場合、IP WAN ルート グループは 9 1 を削除し、公衆網ルート グループは 9 だけを削除することが可能です。
- 複数のルート リストに、同じルート グループを含むことができます。ルート グループの番号操作は、そのルート グループを指定する特定のルート リストに関連しています。
- ルート パターンまたはルート グループ内で複数の番号操作を実行すると、変換が実行される順序が、コールに使用される、変換結果の発番号および着番号に影響を与える可能性があります。Unified CM は、次に示す主要なタイプの番号操作を表示されている順に実行します。
  1. 番号を破棄する
  2. 発着信側変換
  3. 番号をプレフィックスとして付加する
  4. 発着信側トランスフォーメーション パターン

ルート グループ

ルート グループは、一般にゲートキーパーまたはリモート Unified CM クラスタとのゲートウェイ（MGCP 、SIP、または H.323）、H.323 トランク、または Cisco Unified Border Element である特定のデバイスを制御し、それを指定します。Unified CM は、割り当てられている分配アルゴリズムに従ってコールをデバイスに送信します。Unified CM では、トップダウン アルゴリズムと循環アルゴリズムをサポートしています。

発信側および着信側トランスフォーメーション パターン

発信側トランスフォーメーション パターンを使用すると、発番号のグローバル形式を、ゲートウェイ、トランクなどのルート グループ デバイスに接続されているオフクラスタ ネットワークで必要となるローカル形式に適応させることができます。

着信側トランスフォーメーション パターンを使用すると、着番号のグローバル形式を、ゲートウェイ、トランクなどのルート グループ デバイスに接続されているオフクラスタ ネットワークで必要となるローカル形式に適応させることができます。

（注）　着信側トランスフォーメーション パターンは、電話機に影響を与えません。また、デバイス プールの着信側トランスフォーメーション パターン CSS も、そのパターンが割り当てられている電話機に影響を与えません。

両方のトランスフォーメーション パターン タイプは、一致する発番号または着番号の数値表現で構成されます。使用される構文は、ルート パターン、トランスフォーメーション パターン、ディレクトリ番号などのその他パターンの構文と同じです（図 10-27 を参照）。

変換演算子には、数字破棄命令（ドット前の番号など）、発信側トランスフォーメーション マスク、プレフィックス番号が含まれます。この演算子によって、発信側電話番号表示（Default、Allowed、または Restricted）が制御されます。発信側トランスフォーメーション パターンを設定することで、発信側の外部電話番号マスクを発番号として使用できます。

パーティションおよびコーリング サーチ スペースによって、どの発信側トランスフォーメーション パターンをどのゲートウェイまたはトランクに適用するかどうかが制御されます。ゲートウェイまたはトランクでは、関連するデバイス プールの発信側変換 CSS またはデバイス固有の発信側変換 CSS を優先順位の低い順に使用できます。同じメカニズムを使用して、着信側トランスフォーメーション パターンの適用を制御します。

[Call Routing Information] > [Outbound Calls] の [Gateway Configuration] ページで設定された発信側および着信側トランスフォーメーション パターンは、ゲートウェイに送信される発番号または着番号と、発信側または着信側の番号タイプおよび番号計画に影響します。[Incoming Calling Party Settings] で適用される発信側トランスフォーメーション パターンは、ゲートウェイから送信されるコールに適用されます。

図 10-27　発信側および着信側トランスフォーメーション パターン

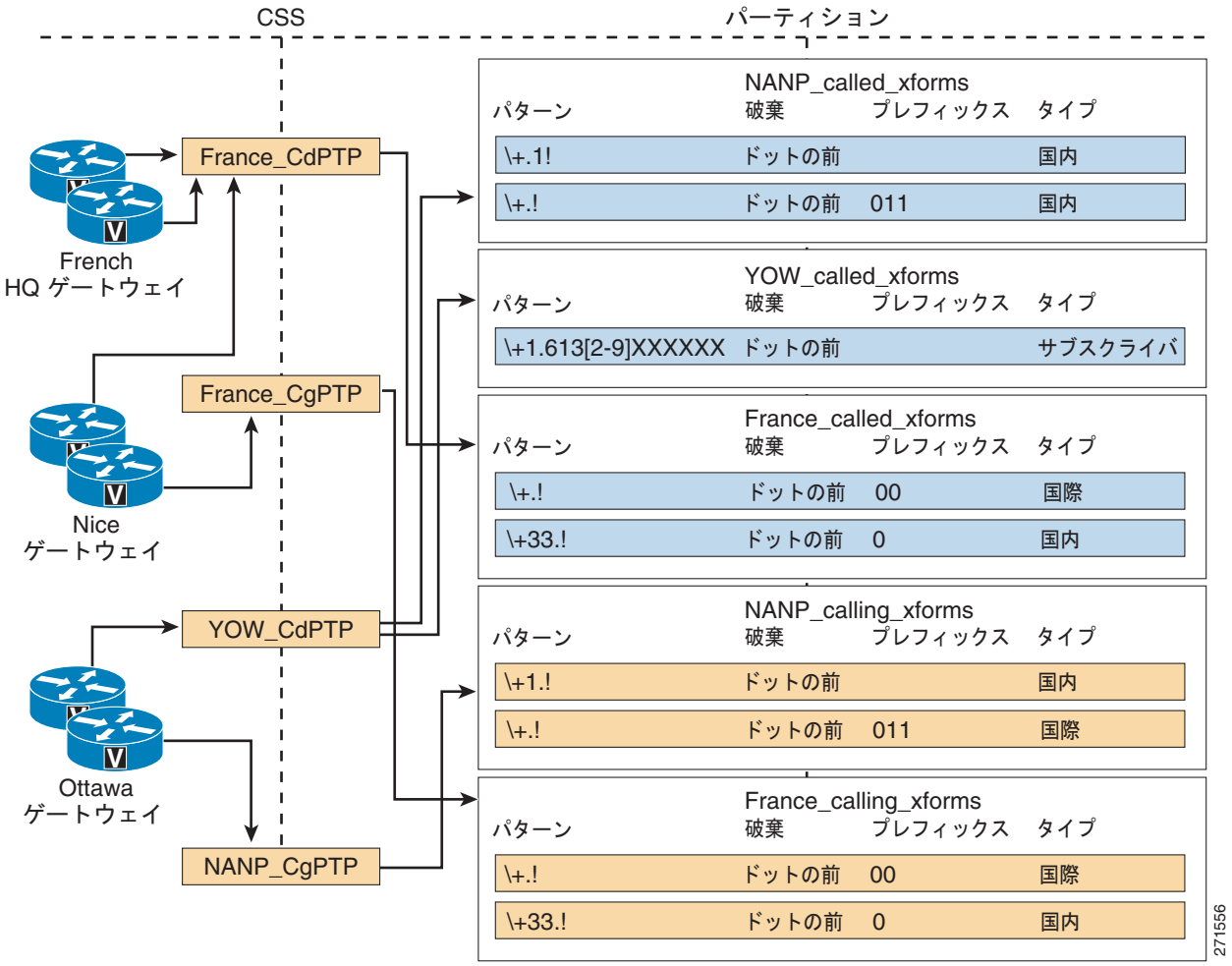


図 10-27 は、発信側および着信側トランスフォーメーション パターンを、さまざまな公衆網で公衆網に接続しているゲートウェイの異なるグループに適用する方法を示しています。

北米番号計画（NANP）では、カナダの Ottawa（空港コード YOW）にあるゲートウェイは、パーティション NANP_calling_xforms が含まれている、発信側変換 CSS NANP_CgPTP に割り当てられます。発番号が +1 で始まる（つまり、NANP 内から発信される）コールは、パーティション NANP_calling_xforms 内で設定されている両方のパターンに一致します。best-match ロジックの後、最初のパターンが選択され、発番号から + 記号と NANP 国コード 1 が削除されます。残りの発番号部分は公衆網に送信される発番号として使用され、番号タイプは National に設定されます。

たとえば、+1 613 555 1234 からのコールを YOW ゲートウェイに送信した場合、その発番号は 613 555 1234 に変換され、番号タイプは National に設定されます。

同じ発信側からのコールをフランスにあるゲートウェイに送信した場合には、一連の異なる発信側トランスフォーメーション パターンが適用されます。たとえば、+1 613 555 1234 からのコールをフランスの Nice（空港コード NCE）にあるゲートウェイに送信した場合、パーティション France_calling_xforms に含まれている発信側トランスフォーメーション パターンが適用されます。この場合、発番号は 001 613 555 1234 に変換され、番号タイプは International に設定されます。

（注）　コールをゲートウェイに送信すると、発番号変換が無効になることがあります。多くのサービス プロバイダーでは、現地のサービス契約や規制で定められているように、特定の範囲外で発番号を使用することを許可していません。

同じプロセスは、着番号トランスフォーメーション パターンにも適用されます。Ottawa ゲートウェイの場合、割り当てられた受信側変換 CSS は YOW_CdPTP です。これは、パーティション NANP_Called_xforms および YOW_Called_xforms に含まれています。番号計画エリア 613 内の宛先番号に発信されるコールは、これらの 2 つのパーティションに含まれているすべてのパターンに一致します。ただし、ベストマッチ プロセスによってパターン \+1.613[2-9]XXXXXX が選択されます。

たとえば、Ottawa ゲートウェイ経由で +1 613 555 9999 にコールを発信すると、着番号は 516 555 9999 に変換され、番号タイプは Subscriber に設定されます。

着信側の設定（ゲートウェイ別）

個々のゲートウェイには、優先順位に従ってデバイス プール レベルまたはサービス パラメータ レベルで着信側の設定を行うことができます。各番号タイプ（Subscriber、National、International、または Unknown）には、Unified CM で適切なプレフィックス番号を設定できます。さらに、番号を削除したり、着番号として指定した番号にプレフィックス番号を付けたりすることができます。表記形式は PP:SS です。PP はプレフィックスとして付加される番号を表し、SS は削除される桁数を表します。最初に番号削除操作が着信側の番号で実行され、次にその結果の番号にプレフィックス番号が付加されます。たとえば、プレフィックス番号フィールドを +33:1 と設定し、着信側の番号が 01 58 40 58 58 である場合、+33 1 58 40 58 58 となります。

Cisco Unified CM 7.1 では、発信側トランスフォーメーション パターンをコールに適用するために使用するコーリング サーチ スペースを各番号タイプに設定できます。コーリング サーチ スペースには、発信側トランスフォーメーション パターンだけが存在するパーティションが保持される必要があります。これによって、厳密に番号タイプに基づくのではなく、発番号の構造に基づいた変更を発番号に適用することができます。発信側トランスフォーメーション パターンでは、正規表現を使用して発番号が照合されます。複数の一致項目から選択するには、best-match プロセスが使用され、選択されたパターンの発信側変換がコールに適用されます。

ルート グループ デバイス

ルート グループ デバイスは、ルート グループによってアクセスされるエンドポイントであり、一般に、ゲートキーパーまたはリモート Unified CM とのゲートウェイまたはトランクで構成されます。次のタイプのデバイスは、Unified CM で設定できます。

- メディア ゲートウェイ コントロール プロトコル（MGCP）ゲートウェイ
- SIP ゲートウェイ
- H.323 ゲートウェイ
- H.225 トランク、ゲートキーパー制御：ゲートキーパーを介した標準 H.323 ゲートウェイとのトランク
- クラスタ間トランク、非ゲートキーパー制御：別の Unified CM クラスタとの直接トランク
- クラスタ間トランク、ゲートキーパー制御：ゲートキーパーを介した他の Unified CM クラスタまたは H.323 ゲートウェイとのトランク
- SIP トランク：別の Unified CM クラスタとのトランク、Cisco Unified Border Element、Session Border Controller、または SIP プロキシ

（注）　H.225 トランクとクラスタ間トランク（ゲートキーパー制御）はどちらも、相手方エンドポイントが標準 H.323 ゲートウェイであるか、Unified CM であるかを自動的に検出し、それに応じて H.225 または Intercluster Trunk プロトコルを選択します。

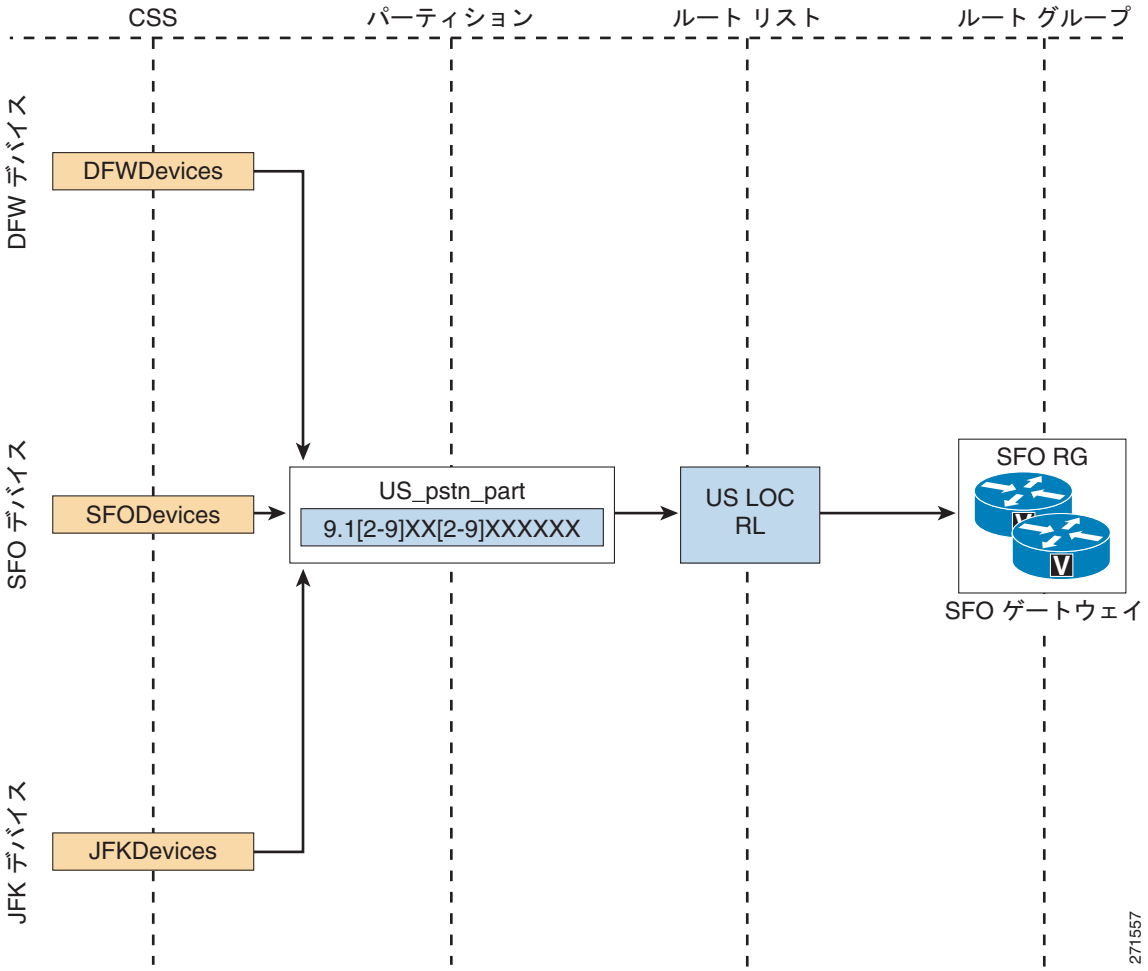
ローカル ルート グループ

デバイス プールは、ローカル ルート グループに関連付けることができます。ローカル ルート グループを使用したルート パターンには、固有の特性があります。つまり、コールの発信元デバイスに基づいて出口ゲートウェイを動的に選択できます。それに対し、静的ルート グループを使用したルート パターンによってルーティングされるコールでは、コールの発信元デバイスに関係なく、コールが同じゲートウェイにルーティングされます。

例 10-2　　ローカル ルート グループと非ローカル ルート グループの比較

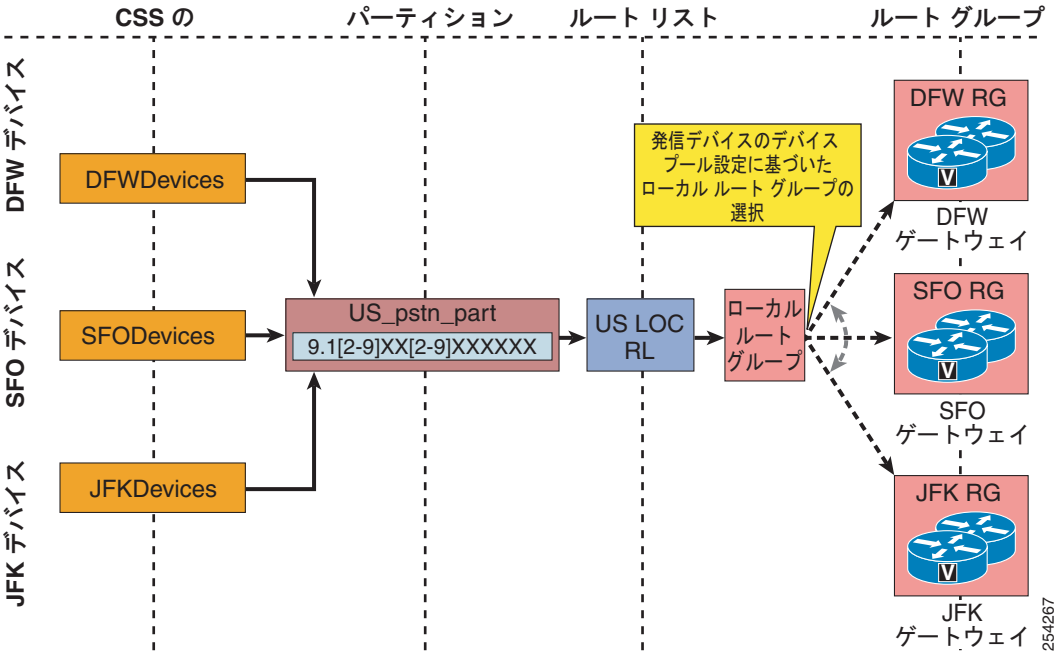
図 10-28 では、9.1[2-9]XX[2-9]XXXXXX と定義されたルート パターンは、San Francisco ゲートウェイを含む非ローカル ルート グループを参照するルート リストを指しています。このルート パターンが Dallas、San Francisco、および New York の電話機のコーリング サーチ スペースに含まれているパーティションにある場合、それらの 3 つの都市にあるデバイスからの国内コールの出口は San Francisco の公衆網となります。

図 10-28　非ローカル ルート グループの動作



一方、図 10-29 に示すように、同じルート パターンを変更して、標準ローカル ルート グループを含むルート リストを指すようにした場合、Dallas サイトから発信されるコールの出口は Dallas ゲートウェイを経由した公衆網となり、New York サイトから発信されるコールの出口は New York ゲートウェイを経由した公衆網となり、San Francisco サイトから発信されるコールの出口は San Francisco ゲートウェイを経由した公衆網となります。

図 10-29　ローカル ルート グループの動作



デバイス モビリティ機能を使用すると、ローミングしている現在のサブネットに基づいて、デバイス プールをエンドポイントに割り当てることができます。これにより、電話機の現在のサイトに基づいた、ローカル ルート グループの割り当てが可能になります。

例 10-3　デバイス モビリティ

電話機を San Francisco サイトから New York サイトに移動するとします。電話機の新しい IP アドレス（New York サイトに関連付けられた IP サブネット部分）に基づいて、New York のデバイス プールがその電話機に割り当てられます。ローミング電話機によって発信される次のコールは、標準ローカル ルート グループを含むルート リストを使用したルートと一致し、New York ゲートウェイを経由してルーティングされます。

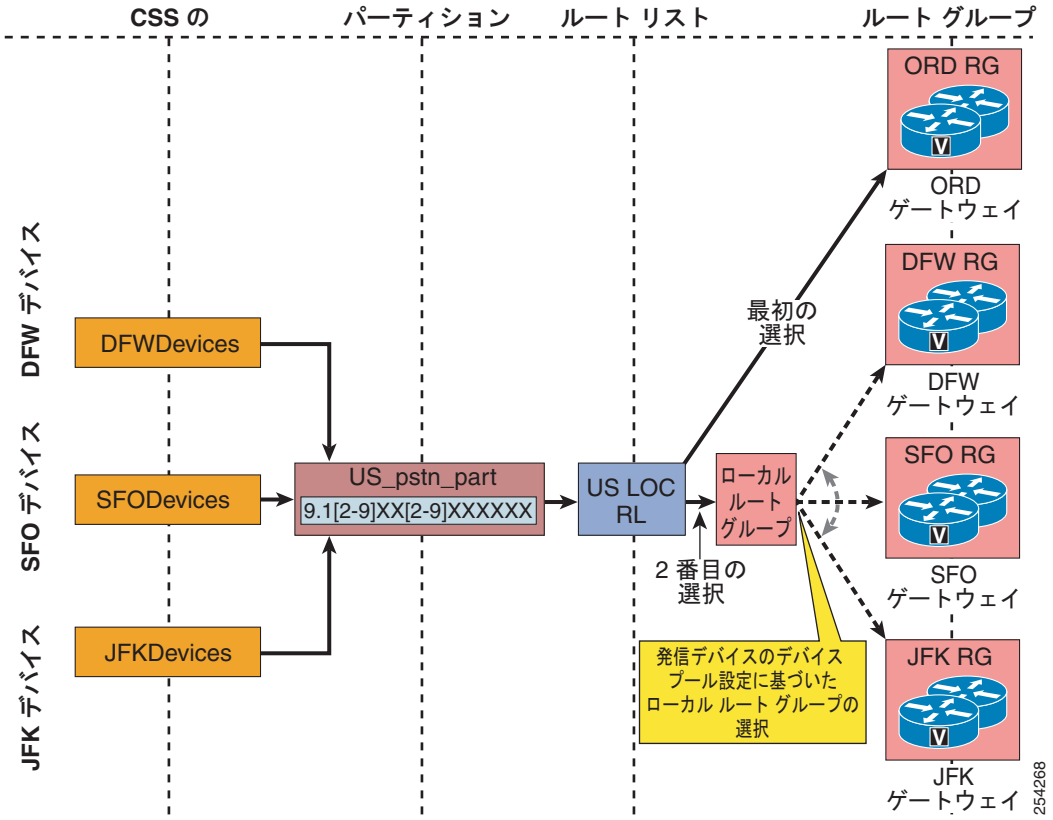
公衆網へのローカル フェールオーバーを使用した中央ゲートウェイ

中央ゲートウェイが設定されているシステムの場合、ローカル ルート グループによって、公衆網へのローカル フェールオーバーが簡素化されます。発信側サイトでゲートウェイへのローカル フェールオーバーが許可されているときに、単一のルート リストを使用することで、複数サイトの公衆網コールをルーティングすることができます。

例 10-4　中央ゲートウェイとローカル フェールオーバー

ある会社が、Chicago にあるトランクのグループに有利な公衆網相互接続レートをネゴシエートするとします。ルート リストに、1 番目の項目として Chicago にあるゲートウェイを含むルート グループが含まれ、2 番目の項目として標準ローカル ルート グループが含まれている場合、処理されるコールは最初に Chicago にある低コストの推奨ゲートウェイに送信されます。Chicago ゲートウェイが使用可能でない、フリー ポートがない、あるいは発信側電話機と Chicago ゲートウェイ間で使用できる帯域幅が十分でない場合は、発信側電話機のデバイス プール設定でローカル ルート グループによって決定されている、2 番目の項目を使用して、発信側電話機と同じ場所にあるゲートウェイを経由したコールのルーティングが試行されます（図 10-30 を参照）。

図 10-30　公衆網へのローカル フェールオーバーを使用した中央ゲートウェイ



Unified CM におけるコール特権

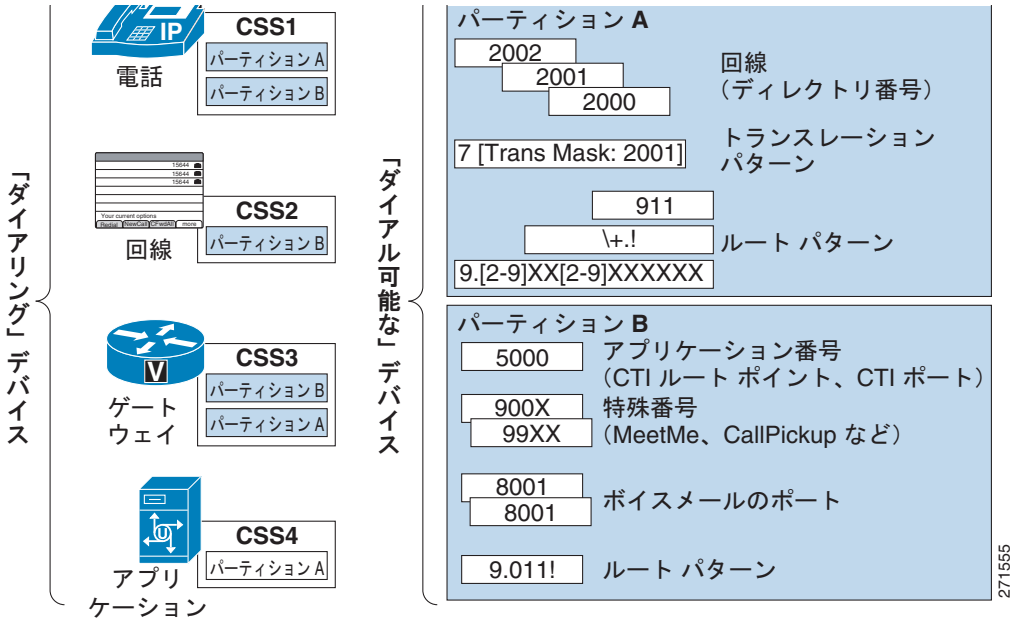
ダイヤリング特権は、特定のエンドポイント（電話、ゲートウェイ、または CTI アプリケーションなど）にどのタイプのコールを許可する（または禁止する）かを制御するために設定されます。Unified CM で処理されるすべてのコールは、次の要素の設定で実装されたダイヤリング特権の対象になります。

- 「パーティション」（P.10-80）
- 「コーリング サーチ スペース」（P.10-81）

*パーティション*は、同じアクセス可能性を持つディレクトリ番号（DN）のグループです。*コーリング サーチ スペース*は、特定のデバイスからどのパーティションがアクセス可能であるかを指定します。デバイスは、コーリング サーチ スペースに含まれているパーティション内の DN だけを呼び出すことができます。

図 10-31 に示すように、パーティション内に配置できるすべての項目は、ダイヤリングの対象となるパターンを持っています。このような項目としては、電話回線、ルート パターン、トランスレーション パターン、CTI ルート グループ回線、CTI ポート回線、ボイスメール ポート、および Meet-Me 会議番号があります。逆に、コーリング サーチ スペースを持つ項目は、コールをダイヤルできるすべてのデバイスです。たとえば、電話機、電話回線、ゲートウェイ、アプリケーション（CTI ルート グループまたはボイスメール ポート経由）などです。

図 10-31　パーティションとコーリング サーチ スペース

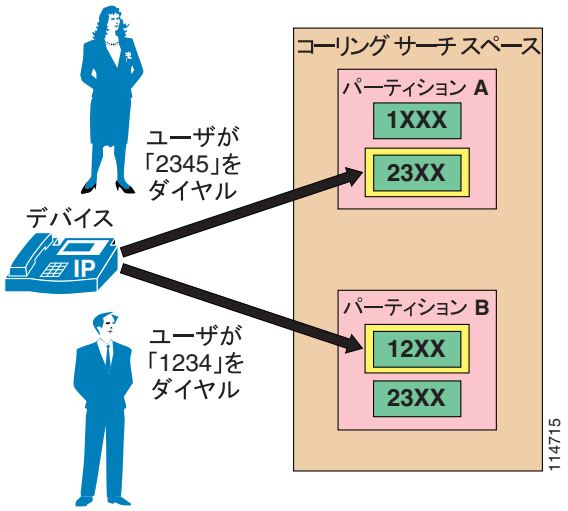


パーティション

パーティションに含めることができるダイヤル プラン項目には、IP Phone のディレクトリ番号、トランスレーション パターン、ルート パターン、CTI ルート ポイント、およびボイスメール ポートがあります。「Unified CM におけるコール ルーティング」（P.10-66）で説明するように、複数のダイヤル プラン項目（ディレクトリ番号、ルート パターンなど）が重複する場合、Unified CM は、ダイヤルされた番号と一致するか、または最も近い（最も固有性の高い一致）項目を選択します。2 つのダイヤル プラン項目が、ダイヤルされたパターンに等しく一致した場合、Unified CM は、コールを発信するデバイスのコーリング サーチ スペース内で最初に表示されているダイヤル プラン項目を選択します。

たとえば、図 10-32 について考えます。ルート パターン 1XXX と 23XX はパーティション A の一部であり、ルート パターン 12XX と 23XX はパーティション B の一部です。発信側デバイスのコーリング サーチ スペースには、パーティション A:パーティション B の順にパーティションがリストされています。このデバイスのユーザが 2345 をダイヤルすると、Unified CM では、パーティション A のルート パターン 23XX を一致項目として選択します。これは、このパターンが発信側デバイスのコーリング サーチ スペースで最初に示されているためです。ただし、ユーザが 1234 をダイヤルした場合には、Unified CM ではパーティション B のルート パターン 12XX を一致項目として選択します。これは、パーティション A の 1XXX よりも一致率が大きいためです。コーリング サーチ スペースに含まれているパーティションの順序は、closest-match ロジックに基づいて均等一致項目が複数あった場合に、競合を解消する要素としてのみ使用されます。

図 10-32　マッチング ロジックにおけるパーティション順序の影響



（注）　均等一致項目が同じパーティションに複数ある場合、Unified CM は、ローカルのダイヤル プラン データベース内で最初にリストされている項目を選択します。ダイヤル プラン データベース内でダイヤル プラン項目がリストされる順序は、設定することができません。したがって、同じパーティション内で均等一致項目が共存しないようにすることを強くお勧めします。これはこのような場合に発生するダイヤル プラン ロジックが予測できないからです。

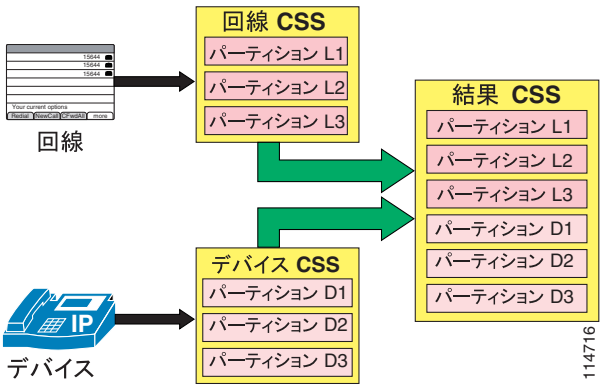
日時に基づいてパーティションをアクティブまたは非アクティブにすることができます。パーティションをアクティブまたは非アクティブにするには、まず、Unified CM Administration で期間とスケジュールを設定し、次に個々のタイム スケジュールを各パーティションに割り当てます。スケジュールに指定した日時の範囲外では、このパーティションは非アクティブになります。このパーティションに含まれているパターンは、Unified CM コール ルーティング エンジンによってすべて無視されます。この機能の詳細については、「時間帯ルーティング」（P.10-105）を参照してください。

コーリング サーチ スペース

コーリング サーチ スペースは、特定のデバイスからどのパーティションがアクセス可能であるかを指定します。所定のコーリング サーチ スペースが割り当てられるデバイスは、そのコーリング サーチ スペースにリストされているパーティションだけにアクセスできます。そのコーリング サーチ スペース以外のパーティションの DN へのダイヤルは失敗します。発信者にはビジー信号が聞こえます。

IP Phone 回線とデバイス（電話機）自体の両方でコーリング サーチ スペースを設定する場合、Unified CM は、この 2 つのコーリング サーチ スペースを図 10-33 に示すように連結し、デバイスのコーリング サーチ スペースの前に、回線のコーリング サーチ スペースを置きます。

図 10-33　IP Phone の回線とデバイスのコーリング サーチ スペース（CCS）の連結



（注）　デバイス モビリティを使用しない場合、デバイスのコーリング サーチ スペースは静的となり、デバイスをネットワークの別の場所に移動しても同じままです。デバイス モビリティを有効にした場合、電話機の IP アドレスによって決定されている、ネットワークで電話機が物理的に配置されている場所に基づいて、デバイスのコーリング サーチ スペースを動的に決定できます。詳細については、「デバイス モビリティ」（P.10-92）を参照してください。

同じルート パターンが、2 つのパーティション（回線のコーリング サーチ スペースに含まれているパーティションとデバイスのコーリング サーチ スペースに含まれているパーティション）に指定されている場合、Unified CM は、「パーティション」（P.10-80）の項で説明している規則に従って、パーティションの連結リスト内で最初にリストされているルート パターン（この場合、回線のコーリング サーチ スペースに関連したルート パターン）を選択します。

回線とデバイスのコーリング サーチ スペースを設定する方法に関する推奨事項については、「従来のアプローチによる Unified CM のサービス クラスの構築」（P.10-40）と 「回線 / デバイス アプローチによる Unified CM のサービス クラスの構築」（P.10-44）の項を参照してください。

結合されたコーリング サーチ スペース（デバイスと回線）の最大長は、各パーティション名間の区切り文字を含めて、1024 文字です（たとえば、ストリング「partition_1:partition_2:partition_3」は 35 文字です）。したがって、コーリング サーチ スペース内の最大パーティション数は、パーティション名の長さに応じて変動します。また、コーリング サーチ スペースの文節は、デバイスのコーリング サーチ スペースと回線のコーリング サーチ スペースを結合するので、個々のコーリング サーチ スペースの最大文字の上限は、512 文字（結合されたコーリング サーチ スペース文節の上限 1024 文字の半分）です。

したがって、パーティションとコーリング サーチ スペースを作成するときは、コーリング サーチ スペースに含める予定のパーティション数を基準にして、パーティション名を短くしてください。コーリング サーチ スペースの設定の詳細は、次の Web サイトで入手可能なオンラインの『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

http://www.cisco.com

パーティションまたはコーリング サーチ スペースを設定する前に、すべての DN は、<None> という名前が付いた特別なパーティションに置かれ、すべてのデバイスには、<None> という名前が付いたコーリング サーチ スペースが割り当てられます。カスタム パーティションとコーリング サーチ スペースを作成する場合は、作成するどのコーリング サーチ スペースにも、<None> パーティションが含まれています。一方、<None> コーリング サーチ スペースには、<None> パーティション*だけ*が入っています。

（注）　<None> パーティションに残っているどのダイヤル プラン項目も、コールを発信する*任意*のデバイスから暗黙的に到達可能です。したがって、予期しない結果を避けるために、<None> パーティションにダイヤル プラン項目を残さないように強くお勧めします。

（注）　<None> と定義されたままのコーリング サーチ スペースを残さないでください。そのままにしておくと、ダイヤル プランの動作が予測困難になる可能性があります。

トランスフォーメーション パターンの特別な考慮事項

発信側および着信側トランスフォーメーション パターンは、パーティションにも配置されます。それらのパーティションは、コーリング サーチ スペース（CSS）に含まれますが、コール特権を制御するためのものではありません。トランスフォーメーション パターンのパーティションの役割は、どの変換をどのゲートウェイ、トランク、または電話機に適用するかを選択することです。発信側トランスフォーメーション パターン CSS に含まれるパーティションには、発信側トランスフォーメーション パターンのみが含まれていなければなりません。同様に、着信側トランスフォーメーション パターン CSS に含まれるパーティションには、着信側トランスフォーメーション パターンのみが含まれていなければなりません。

自動転送コーリング サーチ スペース

（注）　この機能が電話機によってアクティブになっている場合、Call Forward All 動作は、宛先番号が個々のユーザによって入力されるその他の自動転送動作とは異なります。

自動転送コーリング サーチ スペースを有効にする方法を決定することができます。Calling Search Space Activation Policy（コーリング サーチ スペースのアクティベーション ポリシー）によって指定されている、選択可能なオプションは次の 3 つです。

- Use System Default

  Calling Search Space Activation Policy を Use System Default に設定した場合、クラスタ全体のサービス パラメータである CFA CSS Activation Policy によって、使用される Forward All コーリング サーチ スペースが決定されます。CFA CSS Activation Policy サービス パラメータは、With Configured CSS または With Activating Device/Line CSS に設定できます（下記参照）。デフォルトでは、CFA CSS Activation Policy サービス パラメータは With Configured CSS に設定されています。

- With Configured CSS

  With Configured CSS オプションを選択した場合、Directory Number Configuration ウィンドウで明示的に設定されている Forward All コーリング サーチ スペースと Forward All のセカンダリ コーリング サーチ スペースによって、不在転送のアクティブ化と自動転送が制御されます。Forward All コーリング サーチ スペースを None に設定した場合、Forward All に対して CSS は設定されません。そのため、パーティションおよびディレクトリ番号に対する不在転送のアクティブ化の試行は失敗します。不在転送のアクティブ化中に、Forward All コーリング サーチ スペースおよび Forward All のセカンダリ コーリング サーチ スペースの変更は発生しません。

- With Activating Device/Line CSS

  Forward All コーリング サーチ スペースを明示的に設定せずに、ディレクトリ番号のコーリング サーチ スペースとデバイスのコーリング サーチ スペースの組み合せを使用する場合には、Calling Search Space Activation Policy に対して With Activating Device/Line CSS を選択します。Forward All が電話機によってアクティブになっている場合にこのオプションを選択すると、Forward All

コーリング サーチ スペースと Forward All のセカンダリ コーリング サーチ スペースに、ディレクトリ番号のコーリング サーチ スペースとアクティブ化デバイスのデバイス コーリング サーチ スペースが自動的に入力されます。Unified CM Administration で Forward All 宛先を設定する場合、Forward All のコーリング サーチ スペースと Forward All のセカンダリ コーリング サーチ スペースは自動的に入力されないため、明示的に設定する必要があります。その 2 つのコーリング サーチ スペースが連結され、連結されたコーリング サーチ スペースを使用することで、Call Forward All 宛先として入力されている番号を検証します。詳細については、「回線 / デバイス アプローチによる Unified CM のサービス クラスの構築」（P.10-44）を参照してください。

不在転送が電話機によってアクティブになっているときに、Forward All コーリング サーチ スペースを None に設定した場合にこの設定（Calling Search Space Activation Policy を With Activating Device/Line に設定）を使用すると、ディレクトリ番号のコーリング サーチ スペースとアクティブになっているデバイス コーリング サーチ スペースを使用することで、不在転送の試行を検証します。

（注）　通常、Call Forward All 設定では、2 つの要件を満たす必要があります。その 2 つの要件とは、デバイスでコールの転送が許可されている宛先を制御することと、さまざまな発信地点から発信するコールが Call Forward All 宛先に転送されるときに最適なコール ルーティングを実現することです。両方の要件を満たすためには、回線 / デバイス ダイヤル プラン アプローチによる宛先の制御を可能にする With Configured CSS アクティベーション ポリシーを使用することをお勧めします。Call Forward All CSS を使用して、ブロック パターンによる制限セットを実装します。通常のサービス クラスを Call Forward All に使用する場合、Call Forward All CSS は、回線で設定されているのと同じコーリング サーチ スペースに設定できます。その後、標準ローカル ルート グループにコールをルーティングするように、Secondary Calling Search Space for Call Forward All を設定する必要があります。デバイスのデバイス プールで設定されている、発信側（転送）デバイスのローカル ルート グループに基づいて、コールのルーティングに使用される実際のルート グループがコール時に決定されます。

SIP を実行しているタイプ A の IP Phone では、Call Forward All がその電話機自体から起動された場合、転送されるコールにデバイスの Rerouting Calling Search Space が使用されます。Forward All 動作が Unified CM User ページまたは Unified CM Administrative ページから起動される場合、その電話機から開始される Forward All 動作とは無関係になります。

たとえば、SIP を実行するタイプ A の IP Phone に、Unified CM ページで内線 3000 への Forward All が指定されているとします。同時に、その電話機自体には、内線 2000 への Forward All が設定されています。この場合、その電話機に対するすべてのコールは、内線 3000 に転送されます。

（注）　SIP を実行するタイプ A の IP Phone では、Unified CM User ページまたは Administrative ページからの Forward All の起動は、電話機に反映されません。電話機には、コールの転送に関する確認は何も表示されません。

SCCP を実行する IP Phone または SIP を実行するタイプ B の IP Phone から Forward All が起動された場合、ユーザ入力は入力と同時に、設定済みの Forward All コーリング サーチ スペースの中で許可されるパターンと比較されます。無効な宛先パターンが設定されていると、ユーザにはリオーダー トーンが聞こえます。SIP を実行するタイプ A の IP Phone から Forward All が起動された場合、Forward All ユーザ入力は電話機上にローカルに保管され、Unified CM 内のコーリング サーチ スペースとは照合されません。ユーザ入力が無効な宛先に対応している場合でも、ユーザへの通知はありません。その電話機へのコールに対しては、電話機が無効な宛先番号に対して SIP 再ルーティング動作を開始しようとしたときに、リオーダー トーンが再生されます。

その他の自動転送タイプ

さまざまな自動転送タイプ（Forward Busy、Forward No Answer、Forward No Coverage、Forward on CTI Failure、Forward Unregistered）に対して設定されているコーリング サーチ スペースは、他のどのコーリング サーチ スペースとも連結されないスタンドアロン値です。

Call Forward 設定（Forward All を除く）は、内部または外部のコール タイプ別に設定することができます。たとえば、電話機で外部発信者のボイスメールに Call Forward No Answer を設定しても、発信者がネットワーク上の別の IP Phone から発信している社員である場合には、ボイスメールを携帯電話番号に転送することができます。これを可能にするには、内線と外線の Call Forward 設定に対して、異なる設定を使用します。

Forward All コーリング サーチ スペースが <None> のままになっている場合、処理の結果は Unified CM のリリースによって異なり、予想することは困難です。このため、自動転送コーリング サーチ スペースを設定する場合は、次のベスト プラクティスに従うことをお勧めします。

- 自動転送コーリング サーチ スペースは、常に <None> 以外の値を使用して設定する。この設定により混乱を避けることができ、トラブルシューティングが容易になります。転送されるコールにどのコーリング サーチ スペースが使用されるかについて、ネットワーク管理者が正確に把握できるためです。
- Call Forward Busy コーリング サーチ スペースと Call Forward No Answer コーリング サーチ スペースは、ボイスメール パイロットおよびボイスメール ポートの DN に到達可能で、かつ外部公衆網番号以外の値を使用して設定する。
- Call Forward All コーリング サーチ スペースと Forward All のセカンダリ コーリング サーチ スペースは、どちらも企業のポリシーに従って設定する。多くの企業では、コールを社内の番号にしか転送できないように制限しています。この方法によって、ユーザが IP Phone の回線を長距離電話の番号に転送したり、私用電話の長距離通話料金がかからないようにするためにローカル IP Phone の番号に公衆網からダイヤルしたりすることを防止します。

Call Forward Unregistered（CFUR）機能は、一時的に登録から外されている宛先の電話機に発信されたコールを再ルーティングする手段です。CFUR の設定は、主に次の 2 つの要素で構成されます。

- 宛先の選択

  DN が登録から外されているときに、コールを次のいずれかの宛先に再ルーティングできます。

  - ボイスメール

    ボイスメールのチェックボックスをオンにし、CFUR コーリング サーチ スペースを設定して、ボイスメールのパイロット番号を含めることで、コールをボイスメールに送信できます。

  - 公衆網を経由した電話機への到達に使用するディレクトリ番号

    このアプローチが適切となるのは、WAN リンクがダウンするサイト内に電話機がある場合です。そのサイトに Survivable Remote Site Telephony（SRST）が装備されている場合は、電話機（および同じ場所にある 公衆網ゲートウェイ）が同じ場所にある SRST ルータに再登録されます。その後、電話機は、その公衆網 DID 番号に発信されたコールの受信を行うことができます。

    この場合、適切な CFUR 宛先は、対応する元の宛先 DN の PSTN DID 番号です。宛先フィールドにこの PSTN DID を設定します。+ 記号を含む E.164 形式で設定することをお勧めします（たとえば、+1 415 555 1234）。これによって、同じオフネット アクセス コードと公衆網プレフィックスを登録から外された電話機として使用するかどうかに関係なく、発信側電話機のローカル ルート グループによる CFUR 宛先の処理が可能になります。

- コーリング サーチ スペース

  Unified CM では、着信側 DN の CFUR コーリング サーチ スペースを使用することで、設定済みの宛先番号へのコールのルーティングを試行します。CFUR コーリング サーチ スペースは、対象の電話機に設定され、登録から外されている電話機に発信するすべてのデバイスで使用されます。

つまり、すべての発信側デバイスでは、ルート パターン、ルート リスト、ルート グループの同じ組み合せを使用して、コールを発信します。標準ローカル ルート グループを参照するルート リストを指すパターンを使用して、コール を CFUR 宛先にルーティングするために、CFUR コーリング サーチ スペースを設定することをお勧めします。これによって、発信側デバイスに基づいて公衆網への出口ゲートウェイが選択されるようになります。

電話機が単にネットワークから切断されている場合と同様に、電話機が登録から外されている一方で、電話機の DID 番号に関連付けられているゲートウェイが依然として Unified CM の制御下にある場合に、Call Forward Unregistered 機能を使用すると、テレフォニー ルーティング ループが発生することがあります。このような場合、電話機への初期化コールによって、電話機の DID への最初のコールが公衆網経由で試行されます。次に、同じ電話機の DN に到達するために、その結果の着信公衆網コールによって、別の CFUR 試行がトリガーされ、さらに、公衆網を経由して公衆網の中央ゲートウェイから別の CFUR コールがトリガーされます。システム リソースが使い果たされるまで、このサイクルが繰り返されます。

MaximumForwardUnRegisteredHopsToDn サービス パラメータによって、DN に対して同時に許可される CFUR コールの最大数が制御されます。デフォルト値 0 は、カウンタが無効であることを意味します。公衆網経由で CFUR を再ルーティングするように DN を設定した場合には、ループを防止する必要があります。このサービス パラメータを値 1 に設定すると、CFUR のメカニズムで 1 つのコールを発信するとすぐに、CFUR 試行が停止されます。CFUR が設定されている場合には、この設定によって、1 つのコールだけをボイスメールに転送することも可能です。このサービス パラメータを値 2 に設定すると、最大 2 人の同時発信者が、ボイスメールに対して CFUR 設定が設定されている DN のボイスメールに到達でき、CFUR 設定によって公衆網を経由してコールが送信される DN に対して、発生する可能性があるループを 2 つに制限できます。

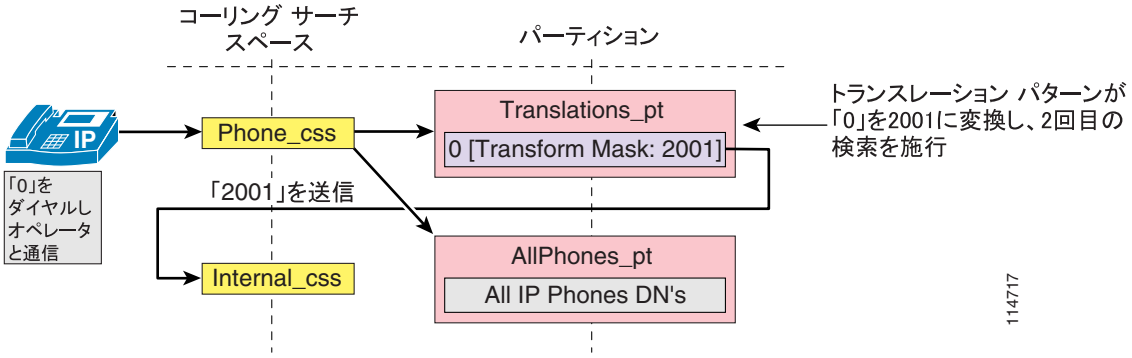
（注） Call Forward Unregistered コールを DN に関連付けられている PSTN DID に送信するために、エクステンション モビリティの DN を設定しないでください。ログアウト状態になっている、エクステンション モビリティ プロファイルの DN は登録から外されていると見なされます。そのため、ログアウト状態の DN の公衆網 DID 番号へのコールによって、ルーティング ループがトリガーされます。ログアウト状態になっている、エクステンション モビリティの DN へのコールがボイスメールに確実に送信されるように、対応する Call Forward Unregistered パラメータを設定してコールがボイスメールに送信されることを確認します。

トランスレーション パターン

トランスレーション パターンは、Unified CM で最も強力な番号操作ツールであり、あらゆるタイプのコールに対して使用できます。トランスレーション パターンは、ルート パターンと同じ一般規則に従い、同じワイルドカードを使用します。ルート パターンと同じように、トランスレーション パターンをパーティションに割り当てます。しかし、ダイヤルされた数字がトランスレーション パターンと一致する場合、Unified CM は、ゲートウェイなどの外部エンティティにコールをルーティングしません。代わりに、まず変換を実行した後、トランスレーション パターン内で設定されたコーリング サーチ スペースを使用して、コールを再度ルーティングします。

トランスレーション パターンは、図 10-34 の例に示すように、さまざまな用途に使用することができます。

図 10-34　トランスレーション パターンの応用例



この例では、管理者は、0 をダイヤルすると到達できるオペレータ サービスをユーザに提供し、一方で定型の内部番号計画をそのまま維持することを考えています。IP Phone は、Translations_pt パーティションを（他のパーティションとともに）含んでいる Phone_css コーリング サーチ スペースを使用して設定されています。このパーティションには、トランスレーション パターン 0 が定義されています。設定済みの Called Party Transform Mask によって、ダイヤルされたストリング（0）を新しいストリング 2001 で置き換えるように Unified CM に指示しています。2001 は、オペレータの電話機の DN に対応しています。2 回目の（この場合は 2001 の）ルックアップが、Internal_css コーリング サーチ スペースを使用して、コール ルーティング エンジンを通じて強制的に実行されます。この時点で、AllPhones_pt パーティションに含まれている実際のオペレータ DN（2001）までコールを伸ばすことができます。

（注）　ダイヤルされた番号をトランスレーション パターンを使用して操作すると、その変換後の番号が、コール詳細レコード（CDR）に記録されます。ただし、番号操作がルート リスト内で発生した場合、CDR には変換後の番号ではなく、ダイヤルされた元の番号が表示されます。IP Phone の Placed Calls ディレクトリには、常にユーザがダイヤルしたストリングがそのまま表示されます。

Automated Alternate Routing

Automated Alternate Routing（AAR）機能を使用すると、Unified CM で音声メディア用の代替パスを確立することができます。このパスが確立されるのは、同じクラスタ内の 2 つのエンドポイント間にある優先パスで、コール アドミッション制御用のロケーション メカニズムによって決定される使用可能な帯域幅が使い果たされたときです。

AAR 機能の主な適用対象は、WAN 経由で接続されているサイトを使用する配置です。たとえば、支店 A の電話から支店 B の電話にコールする場合、支店間の WAN リンクで使用可能な帯域幅（ロケーション メカニズムによって計算）が不足しているときは、AAR によって公衆網経由でコールを再ルーティングできます。コールの音声パスは、発信元の電話からローカルの（支店 A の）公衆網ゲートウェイまでは IP ベース、このゲートウェイから公衆網を経由して支店 B のゲートウェイまでは TDM ベース、支店 B のゲートウェイから宛先の IP Phone までは IP ベースです。

AAR による処理は、ユーザには見えません。ユーザが着信側電話のオンネット（たとえば 4 桁の）ディレクトリ番号にしかダイヤルできないように AAR を設定すると、公衆網などの代替ネットワーク経由で宛先に到達するときに、ユーザによる追加入力が不要になります。

（注）　AAR では、CTI ルート ポイントがコールの発信元や宛先になることはサポートしていません。また、ユーザが複数のサイトにわたってローミングする場合、AAR はエクステンション モビリティ機能と共存できません。詳細については、「エクステンション モビリティ」（P.10-94）を参照してください。

AAR を正常に動作させるには、AAR の次の主要要素を指定する必要があります。

- 「宛先公衆網番号の確立」（P.10-88）
- 「必要なアクセス コードの付加」（P.10-88）
- 「適切なダイヤル プランおよびルートの選択」（P.10-90）

宛先公衆網番号の確立

コールを再ルーティングするには、公衆網などの代替ネットワーク経由でルーティングできる宛先番号を使用する必要があります。AAR では、ダイヤルされた番号を使用してコールのオンクラスタでの宛先を特定し、その番号を着信側の AAR 宛先マスクと結合します。AAR 宛先マスクが設定されていない場合には、その代わりに外部電話番号マスクが使用されます。ダイヤルされた番号と適切なマスクを結合することで、代替ネットワークによってルーティング可能な、完全修飾番号を生成する必要があります。

または、AAR 設定でボイスメールのチェックボックスをオンにすることで、コールをボイスメールのパイロット番号に転送できます。この選択では、発信者によってダイヤルされた元の番号を利用しませんが、ボイスメール プロファイル設定に従ってコールがルーティングされます。

（注）　デフォルトでは、ディレクトリ番号設定によってコールの AAR レッグがコール履歴に保持されます。これによって、音声メッセージング システムへの転送で適切なボイスメールボックスが選択されます。「Remove this destination from the call forwarding history」を選択した場合には、コールの AAR レッグがコール履歴に保持されません。そのため、ボイスメールボックスが自動的に選択されなくなり、発信者に汎用ボイスメール グリーティングが提供されます。

AAR 宛先マスクを使用することで、外部電話番号マスクと無関係に、宛先の電話番号を決定することができます。たとえば、会社の発信者 ID ポリシーに基づいて、電話機の外部電話番号マスクをオフィスの代表電話番号（415 555 1000 など）にする必要がある場合、AAR に電話機固有の公衆網番号を提供するために、AAR 宛先マスクを +1 415 555 1234 に設定できます。

たとえば、San Francisco にある電話機 A（DN = 2345）から、New York にある電話機 B 上に設定されているオンネット DN（1234）にダイヤルするとします。ロケーションベースのコール アドミッション制御によってコールが拒否された場合、AAR は New York の電話機の外部電話番号マスク（+1212555XXXX）を取得して使用し、公衆網上でルーティング可能な番号（+12125551234）を導出します。

AAR 宛先マスクを設定して + 記号を含む完全修飾 E.164 番号を生成することが最善の方法となります。その理由は、この方法によって AAR 設定全体が大幅に簡素化されるためです。たとえば、Paris にある電話機は AAR 宛先マスク +33 1 58 04 58 58 で設定されます。この番号は完全修飾 E.164 番号であるため、発信側電話機がフランスやカナダにあるか、世界のどこにあるかに関係なく、発信側電話機の公衆網へのゲートウェイによって要求されるルーティング可能な PSTN 番号を導出するために、Cisco Unified Communications システムに必要なすべての情報がこの番号に含まれています。次の項では、このアプローチについて詳しく説明します。

必要なアクセス コードの付加

AAR 宛先で + 記号を含む完全修飾 E.164 番号を生成する場合

これが最も単純なケースです。AAR 宛先には、ワイルドカードとして + が含まれています。+ は、各ゲートウェイで必要となる適切なアクセス コードに置き換えられます。適切なルート パターンにルーティングされるように宛先番号が準備されます。その後、適切な着信側トランスフォーメーション パターンによって宛先番号が公衆網への出口点で変換されます。

例 1：カナダの Ottawa にある電話機が Paris にある電話機に発信していますが、WAN の帯域幅が不足しているために AAR がトリガーされます。AAR 宛先は +33 1 58 04 58 58 です。発信側電話機の AAR コーリング サーチ スペースには、コールを標準ローカル ルート グループにルーティングするルート パターン \+! が含まれています。コールは、Ottawa にあるローカル ゲートウェイにルーティングされ、そこで、着信側トランスフォーメーション パターンによって + が適切な国際アクセス コード 011 に置き換えられます。その結果、011 33 1 58 04 58 58 にコールが発信されます。

例 2：フランスの Nice にある電話機が Paris にある電話機に発信していますが、WAN の帯域幅が不足しているために AAR がトリガーされます。AAR 宛先は +33 1 58 04 58 58 です。発信側電話機の AAR コーリング サーチ スペースには、コールを標準ローカル ルート グループにルーティングするルート パターン \+! が含まれています。コールは、Nice にあるローカル ゲートウェイにルーティングされ、そこで、着信側トランスフォーメーション パターンによって + 33 が適切な国内アクセス コード 0 に置き換えられます。その結果、01 58 04 58 58 にコールが発信されます。

AAR 宛先マスクで国コードを含む番号を生成する場合

宛先番号（国コードが含まれると前提）が元の支店のダイヤル プランによって正常にルーティングされるためには、プレフィックスが必要になる場合があります。また、発信地点が別のエリア コードまたは別の国に配置されている場合、ダイヤルされたストリングの一部として、国際ダイヤル アクセス コード（たとえば、00 、011）などの他のプレフィックスが必要になる場合があります。

AAR を設定する場合は、DN を AAR グループ内に配置します。AAR グループのペアごとに、同じ AAR グループ内で発信または終端するコールのプレフィックス番号も含めて、その 2 グループ間のコールで DN に追加するプレフィックス番号を設定できます。

一般的な規則として、複数の DN が各国間で同じダイヤリング構造を共有している場合は、それらの DN を同じ AAR グループに配置します。たとえば、UK 国外にある UK ダイヤル番号のすべての電話機は、9 を PSTN アクセス コードとして使用し、その後に国際アクセス コードの 00 が続きます。フランスおよびベルギーにあるすべての電話機は、0 を PSTN アクセス コードとして使用し、その後に国際アクセス コードの 00 が続きます。NANP にあるすべての電話機は、9 を PSTN アクセス コードとして使用し、その後に国際アクセス コードの 011 が続きます。

これによって、AAR グループ設定は次のようになります。

AAR グループ	NANP	Cent_EU	UK
NANP	9	9011	9011
Cent_EU	000	000	000
UK	900	900	9

例 3：カナダの Ottawa にある電話機が Paris にある電話機に発信していますが、WAN の帯域幅が不足しているために AAR がトリガーされます。AAR 宛先は 33 1 58 04 58 58 です。発信側電話機の AAR グループは NANP であり、宛先番号の AAR グループは Cent-EU です。したがって、プレフィックス 9011 が付加されます。発信側電話機の AAR コーリング サーチ スペースには、コールを Ottawa のルート リストにルーティングして 9 を削除する、サイト固有のルート パターン 9011! が含まれています。コールは、Ottawa にあるローカル ゲートウェイにルーティングされます。その結果、011 33 1 58 04 58 58 にコールが発信されます。

例 4：ベルギーの Brussels にある電話機が Paris にある電話機に発信していますが、WAN の帯域幅が不足しているために AAR がトリガーされます。AAR 宛先は 33 1 58 04 58 58 です。発信側電話機および宛先番号の AAR グループは Cent-EU です。したがって、プレフィックス 000 が付加されます。発信側電話機の AAR コーリング サーチ スペースには、コールを Brussels のルート リストにルーティングして先行する 0 を削除する、サイト固有のルート パターン 000! が含まれています。コールは、Brussels にあるローカル ゲートウェイにルーティングされます。その結果、00 33 1 58 04 58 58 にコールが発信されます。

ボイスメールの考慮事項

AAR は、コールをボイスメールに転送することができます。通常、オフネット アクセス コードなしでボイスメールのパイロット番号がダイヤルされます（ボイスメールのパイロット番号が 8 555 1000 などの完全修飾のオンネット番号である場合）。コールをボイスメールに送信するために AAR を設定すると、AAR グループ メカニズムによって、設定済みのアクセス コードも付加されます。この設定には、AAR グループを作成する必要があります。AAR グループは、必要な AAR 宛先がボイスメール（たとえば、vmail_aar_grp）となっているすべての DN によって使用されます。他の AAR グループの DN からコールを受信するときに、このボイスメールの AAR グループでプレフィックス番号を使用しないことを確認してください。

例 : San Francisco サイトおよび New York サイトにある DN が、AAR グループ NANP で設定され、そのグループにある任意の 2 つの DN 間のコールに 9 が付加されるとします。San Francisco にある DN を設定して AAR コールをボイスメールに送信した場合（たとえば、8 555 1000）、985551000 にコールが発信されますが、そのコールは失敗します。その代わりに、San Francisco にある DN を AAR グループ vmail で設定します。次の表に示すように、AAR グループ NANP から AAR グループ vmail へのコールのプレフィックス番号は <none> です。これで、コールが正常に 85551000 に発信されます。

AAR グループ	NANP	Cent_EU	UK	vmail
NANP	9	9011	9011	<none>
Cent_EU	000	000	000	<none>
UK	900	900	9	<none>

（注） デバイス モビリティを使用しない場合、DN ドメインの AAR グループ設定は、デバイスがネットワークの別の場所に移動しても同じままです。デバイス モビリティを使用した場合、電話機の IP アドレスによって決定された、ネットワークで電話機が物理的に配置されている場所に基づき、ARR グループを動的に決定できます。詳細については、「デバイス モビリティ」（P.10-92）を参照してください。

適切なダイヤル プランおよびルートの選択

AAR コールは、発信元の電話と同じロケーションにあるゲートウェイを通じて出力する必要があります。これによって、完成されたダイヤル ストリングが、発信元サイトのダイヤル プランを通じて送信されます。このように設定するには、Unified CM Administration のデバイス設定ページで、適切な AAR コーリング サーチ スペースを選択します。AAR コーリング サーチ スペース内で、オフネット ダイヤル プラン項目（たとえば、ルート パターン）を、同じ場所にあるゲートウェイを指し、公衆網にコールを転送する前にアクセス コードを削除するように設定します。

たとえば、San Francisco サイトの電話を設定する場合は、91-NPA-NXX-XXXX としてダイヤルされた長距離電話を許可し、アクセス コード（9）を削除して San Francisco のゲートウェイに送信する AAR コーリング サーチ スペースを使用します。

ローカル ルート グループを使用し、さらに完全修飾 E.164 アドレス（+ 記号を含む）を AAR 宛先マスクとして使用すると、AAR コーリング サーチ スペース設定を大幅に簡素化することできます。単一のパーティションで設定され、単一のルート パターン \+! が含まれ、さらに標準ローカル ルート グループを備えた単一のルート リストを指している単一のコーリング サーチ スペースを使用することで、クラスタ全体のすべてのサイトですべてのコールをルーティングすることができます。これは、適切なゲートウェイ固有の着信側トランスフォーメーション パターンを利用して、宛先番号のユニバーサル形式を、各サイトでコールが送信されるサービス プロバイダー ネットワークで必要となるローカル形式に適応させます。

（注）　オンネット社内コールを強制的に公衆網コールとしてダイヤルする追加のルート パターンを設定した場合は、それらのパターンが AAR 機能のものと一致しないことを確認します。詳細については、「マルチサイト配置用の設計ガイドライン」（P.10-21）を参照してください。

（注）　コール アドミッション制御による再ルーティングされたコールの拒否を避けるため、AAR 機能は、各エンドポイントとそれに関連する公衆網へのゲートウェイとの間で、IP パスとして LAN を使用する必要があります。したがって、AAR ダイヤル プランでは、公衆網へのアクセスに集中型ゲートウェイを使用することはできません。

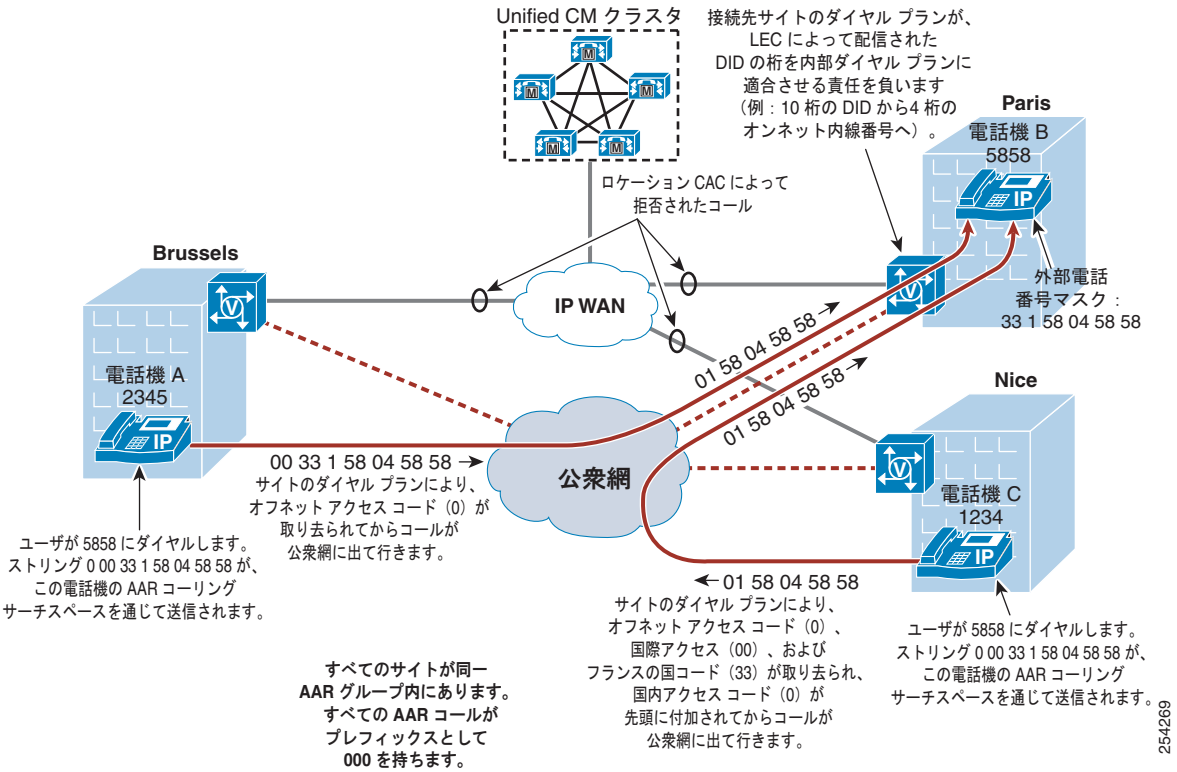
（注）　デバイス モビリティを設定した場合、電話機の IP アドレスによって決定されている、ネットワークで電話機が物理的に配置されている場所に基づいて、ARR コーリング サーチ スペースを動的に決定できます。詳細については、「デバイス モビリティ」（P.10-92）を参照してください。

同じローカル ダイヤリング エリアに複数のサイトがある場合の特別な考慮事項

場合によっては、同じ AAR グループに属する電話機のサイト間でダイヤリングを使用できるように AAR ダイヤル ストリングをローカルに修正する必要があります。たとえば、フランスにある 2 つのサイトが、同じ国コード 33 を共有しているとします（図 10-35 を参照）。この場合は、0 00 33 1 58 04 58 58 としてダイヤルされた番号を 01 58 04 58 58 に変換する必要があります。この変換が必要となるのは、AAR 設定で着信側トランスフォーメーション パターンを利用しない場合だけです。

この変換を実行する最良の方法は、サイト固有のトランスレーション パターン 00033.[1-6]XXXXXXXX を設定することです（ドットの前の番号を削除して、先頭に 0 を付加します）。このトランスレーション パターンは、フランスのサイトの AAR コーリング サーチ スペースのメンバー パーティションにのみ配置します。ベルギーのサイトからは、この同じ宛先に 0 00 33 1 58 04 58 58 として到達する必要があります。

図 10-35　サイト間 AAR コールにおけるダイヤル番号の変換



（注）　AAR 機能は、宛先の電話が到達不能であることが検出されてもトリガーしません。したがって、WAN の障害によって AAR 機能がトリガーすることはありません。

この状況を十分に理解するために、London（英国）、Paris（フランス）、Nice（フランス）にサイトがある Unified CM クラスタの例を考えます。Paris の DID 範囲の E.164 アドレスは、+33145678XXX です。ただし、フランスの公衆網内からコールする場合、これらの内線には、通常は 0145678XXX として到達します。London のオフィスにいる人物が Paris のオフィスに公衆網経由でダイヤルする場合、そのストリングは 90033145678XXX です。一方で、Nice のオフィスにいる人物が Paris のオフィスに公衆網経由でダイヤルする場合、そのストリングは 00145678XXX です。

単一の単純な ARR 設定を使用して上記の 3 つのケースを可能にするには、完全修飾 E.164 番号（+ 記号を含む）で AAR 宛先マスクを設定することが最善の方法となります。これによって、発信側電話機ごとに解釈できる宛先番号が作成されます。

デバイス モビリティ

デバイス モビリティには、IP ネットワーク内にあるデバイスのモビリティが向上するように設計された機能が備わっています（たとえば、本来 San Francisco で使用するように設定されている電話機を物理的に New York に移動させます）。デバイスは依然として同じ Unified CM クラスタに登録されますが、電話機が置かれている新しいサイトに基づいて、デバイスの一部の動作が調整されます。これらの変更は、電話機のある IP サブネットによってトリガーされます。

ローミングするとき、電話機はデバイスの現在のサブネットに関連付けられているデバイス プールに関連付けられているパラメータを継承します。ダイヤル プランから見て、次の 5 つの主要な設定パラメータの機能は、電話機の物理的な場所により変更できます。変更するこれらのパラメータについて、デバイスはホーム ロケーションの外部をローミングしているが、ホーム デバイスのモビリティ グループ内にいると見なされます。

- ローカル ルート グループ

  ローミング デバイス プールのローカル ルート グループが使用されます。たとえば、San Francisco から New York にデバイスがローミングする場合、パターンが標準ローカル ルート グループを呼び出すルート リストを指している場合は常に、公衆網へのコールのルーティングに New York デバイス プールのローカル ルート グループが使用されます。

- 発信側変換 CSS

  ローミング デバイス プールの発信側変換 CSS が使用されます。これにより、電話機は発信側電話番号表示モード（訪問した場所にある電話機の慣習的表示モード）を継承できます。

- デバイス コーリング サーチ スペース

  デバイス設定ページで設定されているデバイス コーリング サーチ スペースではなく、ローミング デバイス プールのデバイス モビリティ コーリング サーチ スペースが使用されます。たとえば、デバイスが San Francisco から New York にローミングしているとき、New York デバイス プールのデバイス モビリティ コーリング サーチ スペースが、ローミング電話機のデバイス コーリング サーチ スペースとして使用されます。サービス クラスに対して回線/デバイス アプローチを使用している場合、このアプローチは公衆網コールが取るパスを確立し、ローカルな New York ゲートウェイにルーティングします。

- AAR コーリング サーチ スペース

  デバイス設定ページで設定されている AAR コーリング サーチ スペースではなく、ローミング デバイス プールの AAR モビリティ コーリング サーチ スペースが使用されます。たとえば、デバイスが San Francisco から New York にローミングしているとき、New York デバイス プールの AAR コーリング サーチ スペースが、ローミング電話機の AAR コーリング サーチ スペースとして使用されます。このコーリング サーチ スペースは発信 AAR 公衆網コールが取るパスを確立し、ローカルな New York ゲートウェイにルーティングします。

- DN の AAR グループ

  着信 AAR コールの場合、DN のホスト電話機がローミングしているかどうかにかかわらず、DN に割り当てられている AAR グループが保持されます。これにより、AAR 宛先番号に対して確立された到達可能性の特性が保持されます。

  発信 AAR コールの場合、発信 DN の AAR グループでは、DN の設定ページで選択された AAR グループではなく、ローミング デバイス プールの AAR グループが使用されます。この AAR グループは、ローミング デバイス上のすべての DN に適用されることに注意してください。たとえば、New York から Paris にローミングするデバイス上のすべての DN（どちらの場所も同じデバイス モビリティ グループであることを前提とする）は、Paris デバイス プールの発信コールに対して設定されている AAR グループを継承します。この AAR グループはローミング デバイス上のすべての DN に割り当てられます。また、ローミング電話機上の DN から行われた AAR コールに対して適切なプレフィックスを付加することを許可します。

ローミング中の Call Forward All

デバイスが同一のデバイス モビリティ グループ内をローミングしているとき、Unified CM ではローカル ゲートウェイへの到達にデバイス モビリティ CSS を使用します。ユーザが電話機で Call Forward All を設定している場合、CFA CSS が None に設定されていて、CFA CSS Activation Policy が With Activating Device/Line CSS に設定されていると、次のようになります。

- デバイスがホーム ロケーションにあるときに CFA CSS としてデバイス CSS と 回線 CSS が使用されます。
- デバイスが同一のデバイス モビリティ グループ内をローミングしているとき、CFA CSS としてローミング デバイス プールからのデバイス モビリティ CSS と回線 CSS が使用されます。
- デバイスが別のデバイス モビリティ グループ内をローミングしているとき、CFA CSS としてデバイス CSS と回線 CSS が使用されます。

「デバイス モビリティ」（P.21-1）の章で、この機能について説明します。

エクステンション モビリティ

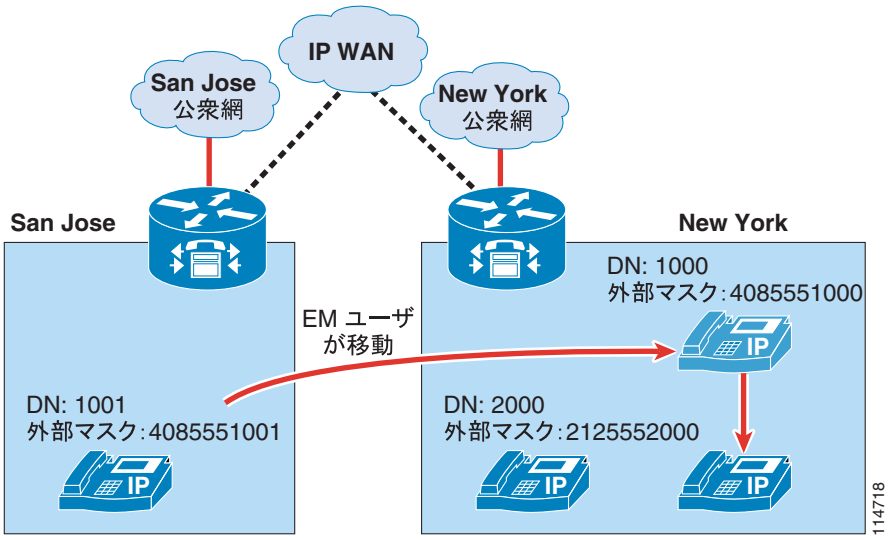
エクステンション モビリティ機能を使用すると、ユーザが IP Phone にログインしたとき、内線番号、短縮ダイヤル、メッセージ待機インジケータ（MWI）ステータス、コール特権を含めて、そのユーザのプロファイルが自動的にその電話機に適用されるようになります。このメカニズムは、それぞれのエクステンション モビリティ ユーザに関連付けられる、デバイス プロファイルを作成することで成り立っています。デバイス プロファイルは、実質的には仮想 IP Phone であり、1 つまたはそれ以上の回線を設定したり、コール特権や短縮ダイヤルなどを定義したりできます。

IP Phone がログアウト状態になっている（つまり、エクステンション モビリティ ユーザがログインしていない）とき、この IP Phone の特性は、デバイス設定ページと回線設定ページによって決まります。ユーザが IP Phone にログインすると、デバイス設定は変更されませんが、既存の回線設定は Unified CM データベースに保存され、ユーザのデバイス プロファイルの回線設定によって置き換えられます。

エクステンション モビリティの重要な利点の 1 つは、ユーザがどこにいるかにかかわらず、同じ Unified CM クラスタによって制御されている IP Phone にユーザがログインできれば、そのユーザに対して、そのユーザ固有の内線番号で到達できることです。集中型コール処理を使用しているマルチサイト配置に対してエクステンション モビリティを適用すると、地理的に互いに分離している複数のサイトに対して、この機能を展開することができます。

ただし、エクステンション モビリティ機能を「Automated Alternate Routing」（P.10-87）の項で説明している AAR 機能と組み合せる場合は、一定の制限事項があります。図 10-36 に示した例について考えます。エクステンション モビリティと AAR を集中型コール処理の Unified CM クラスタに配置していて、San Jose と New York にそれぞれ 1 つのサイトがあります。

図 10-36　エクステンション モビリティと AAR



この例では、通常、San Jose を拠点としているエクステンション モビリティ ユーザが、DN 1000 と DID 番号 (408) 555-1000 を持っているとします。このユーザの外部電話番号マスクは、4085551000 と設定されています。このユーザが New York サイトに移動し、ログインします。さらに、San Jose と New York 間の IP WAN 帯域幅がすべて使用されているとします。

San Jose にいる内線番号 1001 のユーザが 1000 にコールすると、AAR がトリガーされ、発信側の AAR コーリング サーチ スペースと発信側、着信側の AAR グループに基づいて、914085551000 への新しいコールが、San Jose の電話機によって試行されます。このコールは、San Jose のゲートウェイを使用して公衆網にアクセスしますが、DID (408) 555-1000 が同じゲートウェイによって所有されているため、公衆網はコールをこのゲートウェイに戻します。San Jose のゲートウェイは、内線番号 1000 を持つ電話へのコールを確立しようとしますが、この電話は現在 New York にあります。New York にアクセスするための帯域幅を使用できないため、AAR 機能がもう一度呼び出され、次の 2 つのうち、いずれかのシナリオが発生します。

- ゲートウェイの AAR コーリング サーチ スペースに外部公衆網ルート パターンが含まれている場合、ループが開始され、San Jose サイトにあるすべての公衆網トランクが使い果たされる。
- 逆に、ゲートウェイの AAR コーリング サーチ スペースに内部の番号のみが含まれている場合は、コールが失敗し、発信者にはファースト ビジー トーンが聞こえる。この場合は、1 つの公衆網コールが発生して 1 つが受信されるため、コールのセットアップ中、San Jose のゲートウェイでは 2 つの公衆網トランクが使用されます。

ヒント　ここで説明したようなルーティング ループを防止するには、ゲートウェイ設定ページでコーリング サーチ スペースを設定するときに、必ず内部の宛先のみを含め、同じゲートウェイを含んでいるルート グループやルート リストを指すルート パターンを一切含めないようにします。

この例では、エクステンション モビリティが Cisco Unified Communications の動的な側面を利用しているため、サイト間のコール ルーティングで IP ネットワークを使用する必要があることを中心に説明しています。公衆網に定義されている E.164 番号は静的なものであり、公衆網ネットワークはエクステンション モビリティ ユーザの移動を認識しません。AAR 機能は、コール ルーティングを公衆網に依存しているため、ホーム サイト以外のサイトに移動したエクステンション モビリティ ユーザに対して、この機能を使用して到達することはできません。

（注）　ただし、エクステンション モビリティ ユーザが自分のホーム サイトと同じ AAR グループに属するリモート サイトに移動した場合には、使用可能な IP WAN 帯域幅が十分にないとき、そのユーザは AAR 機能を使用して他のサイトへのコールを発信することができます。これは、コールの発信元の電話機の AAR コーリング サーチ スペースによってそれらのコールのパスが決定されるためです。この AAR コーリング サーチ スペースはユーザがエクステンション モビリティにログイン、またはログアウトしても変更されません。また、このスペースは訪問したリモート サイトのゲートウェイを使用するように設定する必要があります。

ヒント　登録解除されたエクステンション モビリティ プロファイル DN がボイスメールにコールを送信するように設定してください。詳細については、「自動転送コーリング サーチ スペース」（P.10-83）を参照してください。

Cisco Unified Mobility 固有の考慮事項

Cisco Unified Mobility（「Cisco Unified Mobility」（P.25-4）についての項を参照）では、コールのルーティングに直接影響を与える機能に依存しています。ダイヤル プランに関連する Cisco Unified Mobility パラメータの影響を理解するには、次の例について考えてみます。

（注）　この説明で必要なパラメータのみを、ここで示しています。

ユーザ Paul は、次のように設定された IP Phone を所有しています。

DN：8 555 1234

DID 番号：+1 408 555 1234

外部電話番号マスク：408 555 1234

回線コーリング サーチ スペース：P_L_CSS

デバイス コーリング サーチ スペース：P_D_CSS

Paul の DN は、次のように設定されたリモート宛先プロファイル（RDP）に関連付けられています。

コーリング サーチ スペース：P_RDP_CSS

再ルーティング コーリング サーチ スペース：P_RDP_Rerouting_CSS

発信側変換 CSS：P_CPT_CSS

Paul の RDP は、次のように設定されたリモート宛先に関連付けられています。

宛先番号：+1 514 000 9876（これは Paul の携帯電話番号。シングルモードまたはデュアルモードのいずれかの電話機）

Paul または Ringo の DID 番号にかけられた公衆網からのコールは、次のように設定されたゲートウェイによって処理されます。

コーリング サーチ スペース：GW_CSS

有効桁：7

プレフィックス DN：8

ユーザ Ringo は、次のように設定された IP Phone を所有しています。

DN：8 555 0001

DID 番号：408 555 0001

外部電話番号マスク：408 555 0000（これは企業の代表番号）

回線コーリング サーチ スペース：R_L_CSS

デバイス コーリング サーチ スペース：R_D_CSS

次の項では、コール ルーティングでの上記のモビリティ パラメータの影響について説明します。

リモート宛先プロファイル

リモート宛先プロファイル（RDP）はディレクトリ番号（たとえば、ユーザの IP Phone の DN）およびリモート宛先（たとえば、ユーザの携帯電話番号）と関連付けられています。RDP は IP Phone と、リモート宛先として設定された外部番号（たとえば、携帯電話）間のやり取りを制御します。

（注）　リモート宛先は、オンクラスタ DN を宛先番号として設定することはできません。

リモート宛先プロファイルの再ルーティング コーリング サーチ スペース

リモート宛先プロファイルに関連付けられている DN にコールが発信された場合、コールは DN と、リモート宛先として設定されている番号の両方にコールします。

発信者が宛先 IP Phone に到達できるかどうかは、発信者のコーリング サーチ スペース設定によって制御されます。ただし、コールがリモート宛先に分岐（転送）されるかどうか（たとえば、携帯電話）は、着信側モビリティ ユーザの再ルーティング コーリング サーチ スペースによって制御されます。

例：
Ringo は、自分の IP Phone から 8 555 1234 とダイヤルすることによって Paul にコールします。Paul の IP Phone が鳴り、彼の携帯電話も鳴ります。

Ringo が Paul の DN に到達できるかどうかは、Ringo の IP Phone の回線およびデバイス コーリング サーチ スペースによって制御されています。ダイヤルした宛先（8 555 1234）は、連結されたコーリング サーチ スペース R_L_CSS および R_D_CSS にあるパーティションにあります。

このコールが Paul の携帯電話に分岐（転送）されるようにするには、設定されたリモート宛先（+1 514 000 9876）がコーリング サーチ スペース P_RDP_Rerouting_CSS にあるパターンと一致する必要があります。

（注）　Ringo の電話機に割り当てられたダイヤリング特権で外部コールが許可されていなくても、リモート宛先へのコールは、Paul のリモート宛先プロファイルに関連付けられた再ルーティング コーリング サーチ スペースによって処理されます。

リモート宛先プロファイルのコーリング サーチ スペース

Cisco Unified CM 6.0 では、リモート宛先と定義された番号から発信されたコールのルーティングに RDP のコーリング サーチ スペースが使用されます。このスペースは DN の回線 CSS と関連付けられています。連結の順序は、回線 CSS の後に RDP の CSS です。

クラスタに発信された外部コールの発番号がリモート宛先として定義される番号と一致した場合、発番号は、一致したリモート宛先に関連付けられた回線の DN に置き換えられます。また、コールのルーティングに使用されるコーリング サーチ スペースは、次のスペースを連結したものです。

- 一致したリモート宛先番号に関連付けられた DN の回線コーリング サーチ スペース
- 一致したリモート宛先に関連付けられた RDP のコーリング サーチ スペース

Unified CM 6.1 およびそれ以降のリリースでは、新しいサービス パラメータ（Inbound Calling Search Space for Remote Destination）が、クラスタのリモート宛先のいずれかから発信されたコールのルーティングに使用されるコーリング サーチ スペースを制御します。デフォルト設定は Trunk or Gateway Inbound Calling Search Space です。これはすべての着信コールをトランクまたはゲートウェイの設定済み CSS を使用してルーティングします。サービス パラメータが Remote Destination Profile + Line Calling Search Space に設定されている場合、動作はすべての Unified CM 6.*x* リリースで同じになります。この新しいサービス パラメータには、発番号の置換に影響はありません。

（注）　Unified CM 6.1 およびそれ以降のリリースのデフォルト動作は、リモート宛先と定義された番号から発信された着信コールのルーティングに関して、Unified CM 6.0 の動作とは異なります。コールのルーティングが簡素化されるため、シスコは Unified CM 6.1 のデフォルト設定を使用することをお勧めします。

同じクラスタ内のリモート宛先として定義されているすべての番号は、クラスタに着信する任意の外部コールで一致するものを検索します。

次の例では、Unified CM 6.1 およびそれ以降のリリースで、Inbound Calling Search Space for Remote Destination サービス パラメータが Trunk or Gateway Inbound Calling Search Space に設定されていることを前提としています。

例：
Paul は、Ringo の卓上電話にコールするために自分の携帯電話を使用しています。コールは公衆網からゲートウェイに着信します。発番号は 514 000 9876 で着番号は 408 555 0001 です。コールは Ringo の電話機にルーティングされます。Ringo の電話機に発番号として表示される番号は、Paul の卓上電話番号 8 555 1234 です。これにより、Paul の携帯電話番号は表示されず、Missed および Received コール リストから発信された Ringo のコールが Paul の IP Phone を鳴らします。このようにして企業モビリティ機能の完全なセットが使用できるようになります。

コールがゲートウェイに着信するとき、公衆網では発番号を 514 000 9876、着番号を 408 555 0001 と表示します。ゲートウェイの設定は着信番号の末尾から 7 桁の有効桁を保持し、先頭に 8 のプレフィックスを付加し、宛先番号として 8 555 0001 を生成します。

システムは発番号が Paul のリモート宛先番号と一致するかどうかを検出します。一致を検出すると、次の処理が行われます。

1. 発番号を Paul の DN、8 555 1234 に変更します。
2. 着信ゲートウェイのコーリング サーチ スペースを使用して、コールを着信番号にルーティングします。具体的には、ルーティングは GW_CSS コーリング サーチ スペースを介して行われます。

ゲートウェイにより提示される宛先（着信）番号は、電話機の DN である必要があります。また、上記のステップ 1 で示した発信側の置換では、Missed/Received コール リストからワンタッチ ダイヤルを使用した方法を示しています。

（注）　リモート宛先番号をパーティションに分類する方法はありません。複数のユーザ グループ（異なる会社、請負業者など）で同じクラスタを使用している場合、この点に注意する必要があります。Unified CM 6.1 およびそれ以降のリリースで、Inbound Calling Search Space for Remote Destination サービス パラメータが Trunk or Gateway Inbound Calling Search Space に設定されている場合、発信番号がリモート宛先に一致するかどうかにかかわらず、コールのルーティングは、着信トランクまたはゲートウェイの CSS に基づきます。ただし、発番号の置換は、発信側がリモート宛先に一致した場合でも行われます。これは、テナントのリモート宛先番号から別のテナントの DID 番号へのコールが、発信側のオンネット エクステンション DN と一致する、変換済み発番号で提示されることを意味します。

（注）　発番号が使用できない着信外部コールは、着信ゲートウェイの CSS に従ってルーティングされます。これは、SIP または H.323 トランクなどの IP トランクからの着信コールにも当てはまります。

リモート宛先プロファイルの発信側変換 CSS とトランスフォーメーション パターン

企業の IP Phone からモビリティ対応の DN に発信されたコールは、企業の 宛先 IP Phone の DN と、1 つ（または複数の）外部宛先の両方に分岐（転送）されます。これによる 1 つの課題は、それぞれの宛先電話機のダイヤル プランに適合した発番号を送信することです。これは、Missed および Received コール リストからのコールのリダイヤルを可能にするために必要です。企業の電話機の場合、発番号はリダイヤル可能な企業の電話番号である必要があります。公衆網のリモート宛先の場合（自宅の電話機または携帯電話）、発番号は、発信側 IP Phone と関連付けられている企業の番号から、公衆網からリダイヤル可能な番号（一般に、発信側電話機の DID 番号）に変換する必要があります。

コールがモビリティ対応の企業 DN に発信された場合、発信者の発番号に一致するものを検索するために、関連付けられたリモート宛先プロファイルのコーリング サーチ スペースが使用されます。このスペースには、トランスフォーメーション パターンを含むパーティションが含まれています。

トランスフォーメーション パターンは、企業形式から公衆網形式への発番号の適合を制御しています。トランスフォーメーション パターンは、着信番号ではなく、発番号をマッチングするという点で、Unified CM の他のすべてのパターンと異なります。マッチング処理は、正規表現（たとえば、8 555 XXXX）を使用して行われます。そして変換処理では、発信側 DN の外部電話番号マスクのほかに、トランスフォーメーション パターンを使用し、番号をプレフィックスとして付加することができます。

一致すると、設定済みのすべての変換が実行されます。そして一致したリモート宛先プロファイルに関連付けられているすべてのリモート宛先への到達に、変換後の発番号が使用されます。

例：
Ringo が Paul にコールすると、Paul の IP 電話には発番号が 8 555 0001 と表示され、Paul の携帯電話には 408 555 0001 と表示されるようにします。

この場合、次のパラメータを使用してトランスフォーメーション パターンを作成します。

Pattern：8 555 XXXX

Partition：SJ_Calling_Transform

Use calling party's external phone number mask：チェックしない

Calling Party Transformation mask：555 XXXX

Prefix Digits (outgoing calls)：408

パーティション SJ_Calling_Transform がコーリング サーチ スペース P_CPT_CSS に配置されていることを確認する必要もあります。

Ringo からのコールが Paul の電話機に固定されている場合、2 つの別々のコール レッグが試行されます。最初のコール レッグは Paul の IP Phone を鳴らし、発信者の DN を発番号（つまり 8 555 0001）と表示します。2 番目のコール レッグは Paul のリモート宛先プロファイルを介して試行されます。参照されるすべてのパーティションのトランスフォーメーション パターン内にある 8 555 0001 の一致を検索するために、RDP の発信側変換 CSS（P_CPT_CSS）が使用されます。パターン 8 555 XXXX はパターン SJ_Calling_Transform でマッチングされます。トランスフォーメーション マスクが発番号に適用され、555 0001 が生成されます。プレフィックス番号が追加され、リモート宛先にコールが発信された場合に変換された発番号 408 555 0001 が使用されます。

この例では、Ringo の DID 番号と異なる番号に設定されているため、外部電話番号マスクを使用していないことに注意してください。これにより、オフネットの宛先に提示される発番号が発信者と着信側で異なっている必要がある場合に、柔軟性が提供されます。Ringo から Paul へのコールは同僚間のも

のであるため、Ringo の DID 番号が公開されるのは許容されると見なされます。Ringo の次のコールは顧客に対するものである可能性があります。この場合、企業の代表番号 408 555 0000 が、宛先に提示されるのに最も望ましい発番号です。

（注）　発信側トランスフォーメーション コーリング サーチ スペースには <none> パーティションが暗黙的に含まれていません。そのため、<none> パーティションに残っているトランスフォーメーション パターンはどの発信側トランスフォーメーション コーリング サーチ スペースにも適用されません。これは Unified CM 内の他のすべてのパターンと異なります。Unified CM では、<none> パーティション内に残るすべてのパターンは暗黙的にすべてのコーリング サーチ スペースに含まれます。

適用ダイヤル規則

リモート宛先と定義される番号は、着信コールを企業のモビリティ コールとして識別し、固定するためにも使用されます。公衆網がコールを識別する形式は、企業のダイヤル プランがコールを外部番号にダイヤルする場合の形式と異なることがよくあります。適用ダイヤル規則は、リモート宛先で、コールをリモート宛先に分岐（転送）する際に必要な形式に設定するために使用できます。これらの規則では、リモート宛先として設定された番号から、数字を削除したり、数字をプレフィックスとして付加したりすることができます。

例：
番号 514 000 9876 は Paul のリモート宛先番号として設定されています。この番号は、企業に着信するコールを識別するために公衆網が使用する形式に対応します。ただしこれは、発信コールで企業のダイヤル プランが使用する形式（91 をプレフィックスとして付加する必要があります）とは異なります。この場合、リモート宛先の形式を企業ダイヤル プランの形式に適合させるために、適用ダイヤル規則を作成する必要があります。

適用ダイヤル規則：

名前：514000_ten

説明：プレフィックス 91 を 514000 で始まる 10 桁の番号に付加するために使用

番号の先頭：514000

桁数：10

削除する桁数：0

パターンで付加するプレフィックス：91

この例では、Paul の携帯電話から企業へかけられたコールは、514 000 9876 からのものと識別されます。これは、Paul の番号がリモート宛先と設定されている形式に一致します。このため、マッチングが行われ、Paul の卓上電話コールの固定をトリガーします。またオンネットの宛先に表示される発番号の最適化も行われます（たとえば、コールが Ringo の DID 番号に対して行われた場合、Ringo にはその着信が 8 555 1234 から来たものと表示されます）。

コールが Paul の企業 DN 番号に対して行われた場合、Paul のリモート宛先番号に分岐（転送）されたコール レッグは、上記の適用ダイヤル規則によって処理されます。ストリング 514 000 は Paul のリモート宛先番号の先頭と一致します。また、この番号は 10 桁であるため、数字は削除されず、91 がプレフィックスとして付加されます。これにより、Paul のリモート宛先プロファイル コーリング サーチ スペース（この場合は P_RDP_CSS）を介してルーティングされる番号として、91 514 000 9876 が生成されます。

（注）　このアプローチでは、IP Phone から行われたコールのルーティングのためにすでに定義済みのコーリング サーチ スペースを再利用する機能を提供します。発信コールに対してプレフィックスを付加する必要のない新しいコーリング サーチ スペース（つまり、直接 514 000 9876 にコールをルーティングできる）は好ましくありません。外部パターンとオンネット パターンが重複する状況が発生する可能性があるためです。

Immediate Divert（iDivert）

Immediate Divert（iDivert）機能は、コールを直接ボイスメールに送信するために使用します。コールが鳴っているとき（着信）、コールが保留中のとき、またはコールが接続されたときに呼び出すことができます。iDivert 機能では、着信コールが呼び出した電話機のボイスメール ボックスまたは着信側のボイスメール ボックスのいずれかに迂回されます。拡張機能は、転送されたコールやアプリケーションによってリダイレクトされたコールなどの迂回されたコールにのみ適用可能です。

Cisco Unified CM 5.1 の iDivert 機能拡張

iDivert 機能は Cisco Unified CM 5.1 で拡張され、呼び出した電話機のボイスメール ボックス（従来の処理）または着信側のボイスメール ボックス（拡張された処理）のいずれかに着信コールを迂回させることができるようになりました。拡張機能は、転送されたコールやアプリケーションによってリダイレクトされたコールなどの迂回されたコールにのみ適用可能です。

次の例を参考にしてください。

> 電話機 A が電話機 B にコールするとします（電話機 B のコールは電話機 C に転送されます）。電話機 C が鳴っているとき、電話機 C 側にいるユーザは iDivert ソフトキーをアクティブにします。これにより、2 つの選択肢が提供されます。1 つ目の選択肢では、コールが発信側のボイスメール（この場合、電話機 B のボイスメール ボックス）に送信されます。2 つ目の選択肢では、コールが iDivert 呼び出し側のボイスメール（この場合、電話機 C のボイスメール ボックス）に送信されます。コールが鳴っているとき、接続中、または保留中の場合のいずれかに、電話機 C がこの機能を呼び出しても、同じ選択肢を選択できます。

iDivert 機能を呼び出す前に、コールが Auto Call Pickup、Call Transfer、Call Park、Call Park Reversion、Conference、または MeetMe Conference によって処理されると、コールは「迂回された」コールとは見なされなくなり、この場合で使用できる iDivert 機能は、従来の iDivert 処理だけになります（つまり、コールを呼び出し側のボイスメールに送信します）。たとえば、電話機 A が電話機 B にコールするとします。電話機 B のコールは電話機 C に転送され、その後電話機 C はコールを電話機 D に転送します。コールに適用された最後のアクションが電話機 D への転送であるため、これは迂回されたコールでは*ありません*。電話機 D が iDivert 機能を呼び出すと、コールは電話機 D のボイスメール ボックスに送信されます。

上で説明した iDivert の完全な機能を有効にするには、Unified CM サービス パラメータ **Use Legacy Immediate Divert** を **False** に設定します。有効にすると、拡張された iDivert は自動的に QSIG トランクを介してこの機能を使用することを許可します。このため、呼び出し側のボイスメール ボックスが、QSIG を介して接続されているテレフォニー システムでホストできます。

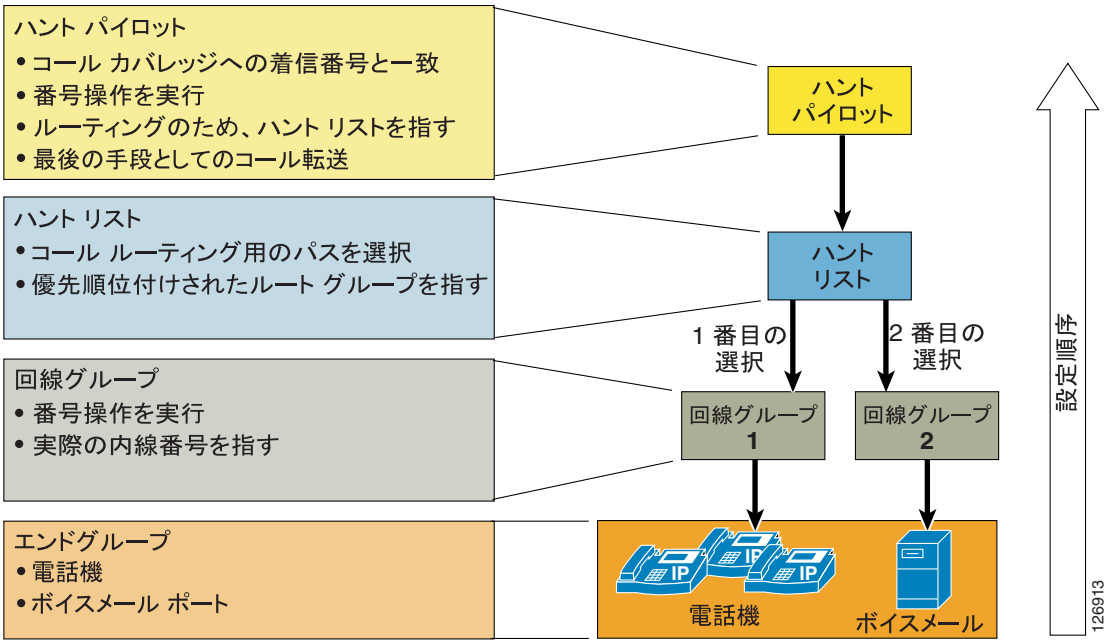
iDivert が、QSIG を使用して他の電話システムに接続しているクラスタで使用している場合、コールを受信したときに従来の iDivert 機能のみ（使用できる選択肢はコールを呼び出し側のボイスメールに送信することのみ）が電話機に提供されます。たとえば、電話機 A および B がクラスタ 1 にあり、電話機 X が QSIG に接続された別のテレフォニー システムであるとします。電話機 A が電話機 X にコールし、電話機 X のコールが電話機 C に転送されます。コールが電話機 C に接続されると、iDivert は、QSIG パスの置き換えが実行されていない場合に限り、従来（呼び出し側のボイスメール）と拡張（着信側のボイスメール）の宛先の両方を提供します。QSIG パスの置き換え後、電話機 C が iDivert を呼び出した場合、選択可能な宛先は電話機 C のボイスメール ボックスのみです。

ハント リストと回線グループ

*ハント パイロット*は、通常はコール カバレッジや、Skinny Client Control Protocol（SCCP）エンドポイントを通じたコール分配に使用されます。コールの分配には、ハント コンストラクトを使用できます。このハント コンストラクトは、3 層式のアーキテクチャに基づいています。外部コールのルーティングに使用されるアーキテクチャに似たこのアーキテクチャでは、複数層のコール ルーティングと共に、番号操作も可能です。

Unified CM は、着信番号と一致する設定済みハント パイロットを検索し、それを使用して、対応するハント リストを選択します。ハント リストには、コールに使用可能なパスが優先順位順に並べられています。これらのパスは、*回線グループ*と呼ばれます。図 10-37 では、Unified CM のハント コンストラクトの 3 層式アーキテクチャを示しています。

図 10-37　　Unified CM のハント コンストラクトの 3 層式アーキテクチャ



ハント パイロット

ハント パイロットは、コールをディレクトリ番号にルーティングするために Unified CM で設定された、ルート パターンのように数字とワイルドカードを組み合せたストリング（たとえば、9.[2-9]XXXXXX）です。ハント パイロットは、ハント リストを直接指しています。ハント リストは回線グループを指しており、回線グループは、最終的に SCCP エンドポイントを指しています。

ハンティングが次のいずれかまたは両方の理由で失敗した場合、コールを最終的な宛先にリダイレクトすることができます。

- すべてのハンティング オプションを使い果たしても、コールはまだ応答されていない。
- タイムアウト期間が満了した。

このコール リダイレクションは、Hunt Pilot 設定ページの Hunt Forward Settings セクションで設定します。このリダイレクトの宛先は、次のいずれかから選択できます。

- Unified CM の内部コール ルーティング テーブルに含まれている、特定のパターン。

- 個人用プリファレンス。このプリファレンスは、元々の着信番号の Call Forward No Coverage 設定を指しています。

たとえば、個人用プリファレンス オプションを実装するには、Forward No Answer フィールドに従ってコールをハント パイロットへリダイレクトするようにユーザの電話を設定して、コールに応答できるユーザが他にいないかどうか検索できるようにします。すべてのハンティング オプションが使い果たされたか、タイムアウト期間が満了したためにコール ハンティングが失敗した場合、コールを当初の宛先ユーザが設定している宛先に転送することができます。たとえば、ユーザの DN 設定ページにある Forward No Coverage フィールドにボイスメール番号を設定すると、ハンティングが失敗した場合、コールはそのユーザのボイスメール ボックスに送信されます。

ハント パイロットの処理するコールには、次の考慮事項が適用されます。

- コール ピックアップとグループ コール ピックアップは、ハント パイロットが分配するコールではサポートされません。回線グループのメンバーは、回線グループの他のメンバーに提供されたハント パイロット コールについては、メンバー同士が同じコール ピックアップ グループに属している場合でもピックアップできません。
- ハント パイロットは、自身の回線グループのメンバーとハント パイロットが別のパーティションに配置されている場合でも、コールを自身の回線グループのいずれかのメンバーに分配できます。ハント パイロットが分配するコールは、すべてのパーティションおよびコーリング サーチ スペース制限を上書きします。

ハント リスト

ハント リストは、コール カバレッジに使用できるパス（回線グループ）が優先順位順に並べられたリストです。ハント リストには次の特性があります。

- 複数のハント パイロットが同一ハント リストを指すことができます。
- ハント リストは、ハント パイロット番号へのコールが行われたときに提供される代替電話機セットとして機能する回線グループが、優先順位順に並べられたリストです。たとえば、特定のサイトにある一連の電話機の中から、コールを受け取る電話機を見つけるために使用できます。コールが受け取られない場合、ハント リストは第 2 のサイトにある電話機を指定する、第 2 の回線グループを通じたコールの提供を試みます。
- ハント リストは、番号操作は一切実行しません。
- 複数のハント リストに、同じ回線グループを含めることができます。

回線グループ

回線グループのメンバーは、Unified CM が制御しているユーザ内線番号です。このため、コールを回線グループのメンバー間に分配するときは、Unified CM がコールを制御します。コールが応答されなかった場合や、内線番号が使用中または未登録の場合は、ハント オプションをコールに適用できます。

回線グループは、コールが分配される順序を制御し、次の特性を持っています。

- 回線グループは、特定の内線番号（通常は、IP Phone 内線番号またはボイスメール ポート）を指しています。
- 1 つの内線番号が複数の回線グループに含まれていることがあります。
- コンピュータ/テレフォニー インテグレーション（CTI）ポートと CTI ルート ポイントは、回線グループに追加できません。したがって、CTI アプリケーション（Cisco Customer Response Solutions（CRS）や IP 音声自動応答装置（IP IVR）など）を通じて制御されるエンドポイントには、コールを分配できません。

- Unified CM は、割り当てられている分配アルゴリズムに従ってコールを各デバイスに分配します。Unified CM は、次のアルゴリズムをサポートしています。
  - トップダウン
  - 循環
  - 最長アイドル時間
  - ブロードキャスト
- No-Answer、Busy、Not-Available のいずれかのイベントが発生すると、分配されたコールを回線グループがハント オプションに基づいて内線番号にリダイレクトします。Unified CM は、次のハント オプションをサポートしています。
  - 次のメンバーにアクセスし、その後はハント リスト内の次のグループにアクセスする。
  - 次のメンバーにアクセスするが、次のグループにはアクセスしない。
  - 残りのメンバーをスキップして、次のグループに直接アクセスする。
  - ハンティングを停止する。

ハント グループのログアウト

ユーザは、HLog ソフトキーをアクティブにすることによって、ハント グループからログアウトできます。いったんアクティブにすると、この機能では実質的に、電話機上で設定されているすべての回線が、どのハント グループにも含まれていないように動作させます。電話機には「Logged out of Hunt Group」と表示されます。回線グループにシェアドラインが含まれている場合、デバイス上でログアウト状態のシェアドラインのすべてのインスタンスは呼び出されません。反対に、デバイス上でログイン状態のシェアドラインのすべてのインスタンスは呼び出されません。

どのハント グループにも含まれていない回線は、HLog 機能の状態に関係なく、通常どおり呼び出されます。

HLog 機能は Unified CM Administration からアクティブにできます。デフォルトでは、HLog ソフトキーはソフトキー テンプレートでは設定されません。いったん、ソフトキー テンプレートに追加されると、電話機が接続状態、保留状態、またはオンフック状態のときに HLog ボタンがディスプレイに表示されます。

Hunt Group Logoff Notification サービス パラメータでは、回線グループから来るコールがログオフ状態の電話機に着信した場合の着信音のオプションを提供します。Hunt Group Logoff Notification サービス パラメータは、Service Parameters Configuration ページの Clusterwide Parameters (Device - Phone) セクションにあります。この機能を有効にするには、TFTP サーバ上に有効な着信音ファイルがあることを確認してください。無効なファイル名が指定されると、何も音が再生されません。

ハント アルゴリズムとハント オプションの詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

http://www.cisco.com

回線グループ デバイス

回線グループ デバイスは、回線グループがアクセスするエンドポイントであり、次のいずれかのタイプに該当します。

- Skinny Client Control Protocol（SCCP）エンドポイント（Cisco Unified IP Phones など）
- SIP エンドポイント
- ボイスメール ポート（Cisco Unity）

- H.323 クライアント
- MGCP ゲートウェイに接続されている FXS

時間帯ルーティング

この機能を使用するには、次の要素を設定します。

- 期間
- タイム スケジュール

期間を利用すると、営業開始時刻と終了時刻を設定できます。この開始時刻と終了時刻は、コールをルーティングできる期間を示しています。これらの時刻に加えて、毎週または毎年発生するイベントを設定することもできます。さらに、Start Time オプションと End Time オプションにある No business hours を選択して、休業時間を設定することもできます。このオプションを選択した場合は、すべての着信コールがブロックされます。

タイム スケジュールは、パーティションに割り当てられている特定の期間をグループにまとめたものです。このタイム スケジュールによって、指定した期間中にパーティションがアクティブまたは非アクティブのどちらになっているかが判断されます。一致したパターンやダイヤリング パターンには、そのダイヤリング パターンの配置されているパーティションがアクティブになっている場合のみ到達できます。

図 10-38 では、同じコール パターン（8000）を持つ 2 つのハント パイロットが、2 つのパーティション（RTP_Partition、SJC_Partition）内に設定されています。これらのパーティションには、一連の定義済み期間を保持したタイム スケジュールがそれぞれ割り当てられています。たとえば、RTP の電話には、ハント パイロット 1 を使用することで、月曜日から金曜日の午前 8 時～ 午後 12 時（東部標準時。GMT - 5.00）まで、および日曜日の午前 8 時から午後 5 時まで到達できます。同様に、SJC の電話には、ハント パイロット 2 を使用することで、月曜日から金曜日の午前 8 時～午後 5 時（太平洋標準時。GMT - 8.00）まで、および土曜日の午前 8 時～午後 5 時まで到達できます。この例では、どちらのハント パイロットも 7 月 4 日は非アクティブです。

図 10-38　時間帯ルーティング

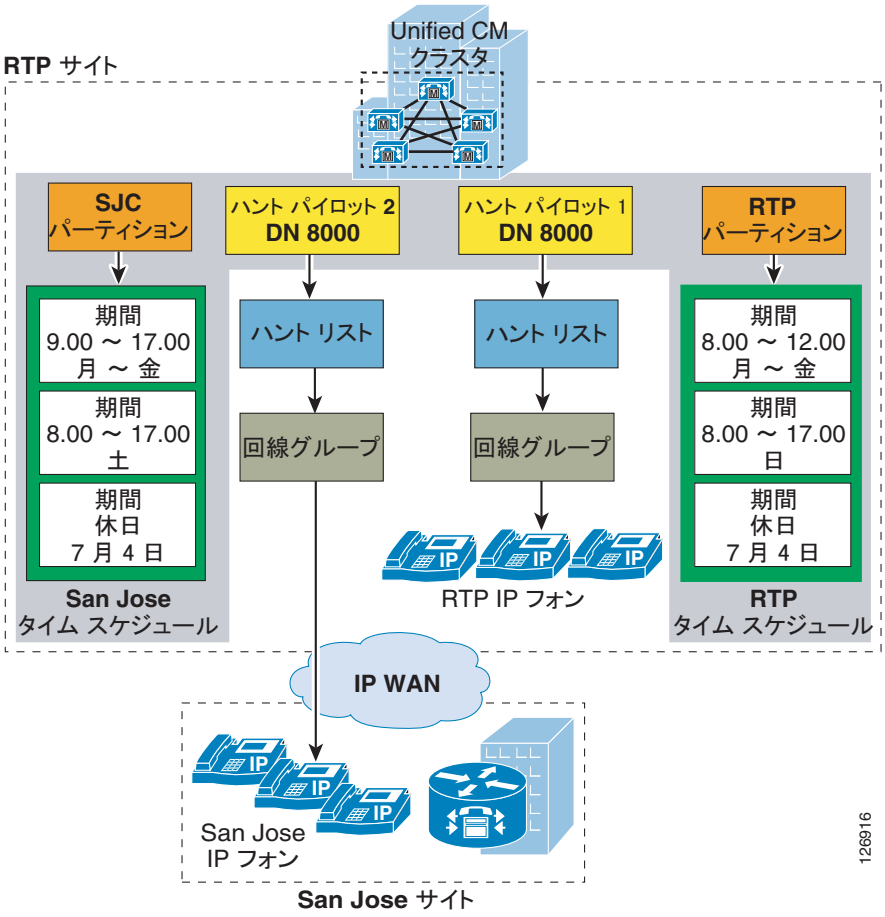


図 10-38 の例では、水曜日の午後 3 時にハント パイロット（8000）に着信したコールは、SJC の電話に転送されます。一方、このハント パイロットに 7 月 4 日にコールした人は、別のパターンが 8000 に一致しない限り、ファースト ビジー トーンを受信します。

論理パーティション

論理パーティションには、次の要素が含まれます。

- デバイス タイプ。電話機は *interior* として分類され、ゲートウェイとトランクは *border* として定義されます。表 10-9 に、各デバイスのエンドポイント タイプを示します。
- ジオロケーション。エンドポイントにはポリシーの決定に使用される住所が割り当てられます。
- ジオロケーション フィルタ。ポリシーの決定は、ジオロケーション オブジェクトのサブセットに対して行うことができます。
- ポリシー。エンドポイント間の通信は、それらの相対的な（フィルタ処理された）ジオロケーションとデバイス タイプに基づいて許可または拒否されます。

（注）　コールのすべての参加者が *interior* として分類されないと、ポリシーは適用されません。つまり、同じクラスタにある電話機間のコールに論理パーティション ポリシーが適用されることはありません。

（注）　ジオロケーションは、Unified CM で設定するコール アドミッション制御用のロケーションや、デバイス モビリティに使用される物理ロケーションと混同されることはありません。

表 10-9　デバイス タイプ

論理パーティションのデバイス タイプ	Cisco Unified Communications Manager デバイス
Border	• ゲートウェイ（H.323 ゲートウェイなど） • Inter-cluster Trunk（ICT）（ゲートキーパー制御および非ゲートキーパー制御の両方） • H.225 トランク • SIP トランク • MGCP ポート（E1、T1、PRI、BRI、FXO）
Interior	• 電話機（SCCP、SIP、またはサードパーティ） • CTI ルート ポイント • VG224 アナログ電話 • MGCP ポート（FXS） • Cisco Unity ボイスメール（SCCP）

論理パーティションのデバイス タイプ

Unified CM は、エンドポイントを *interior* または *border* に分類します。この分類は固定されており、システム管理者が変更することはできません。

ジオロケーションの作成

(RFC) 4119 規格には、ジオロケーションの基本情報が記されています。ジオロケーションには、次のオブジェクトによって指定される住所形式が使用されます。

- 名前
- 説明
- 2 文字の省略形を使用した国名
- 州、地区、または地域（A1）
- 国または行政区（A2）
- 市町村（A3）
- 自治区（A4）
- 地区（A5）
- 街（A6）
- N や W など、街の先頭の方角指示（PRD）
- SW など、街の末尾のサフィックス（POD）
- 通りや区画など、住所のサフィックス（STS）
- 番地（HNO）

- A、1/2 など、番地のサフィックス（HNS）
- ランドマーク（LMK）
- 部屋番号など、ロケーションの補足情報（LOC）
- フロア（FLR）
- 会社または居住者の名前（NAM）
- 郵便番号（PC）

（注）　Unified CM では、ジオロケーションを手動で定義する必要があります。

ジオロケーションの割り当て

デバイスには、優先順位に従ってデバイス ページ、デバイス プール、またはエンタープライズ パラメータで設定されたデフォルトのジオロケーションのいずれかからジオロケーションが割り当てられています。

ジオロケーション フィルタの作成

ジオロケーション フィルタでは、異なるエンドポイントのジオロケーションを比較するときに使用するジオロケーション オブジェクトを定義します。たとえば、電話機のグループには、それらの電話機が置かれている部屋やフロアを除いて、同じジオロケーションが割り当てられる可能性があります。ポリシーによっては、同じ建物内のエンドポイントを同じ非公開ユーザ グループに所属するものと見なし、通信を許可する場合もあります。各電話の実際のジオロケーションは異なりますが、フィルタ処理されたジオロケーションは同じになります。この方法は、ジオロケーションの最上位のフィールドだけにポリシーを適用する必要がある場合に役立ちます。たとえば、異なる都市にある電話機とゲートウェイ間の通信を拒否し、同じ都市内の電話機とゲートウェイ間の通信は許可するポリシーは、都市よりも詳細なオブジェクトを無視してフィルタ処理された相対的なジオロケーションを基にすることができます。

ジオロケーション フィルタの割り当て

電話機は、デバイス プールのフィルタの割り当てを継承します。ゲートウェイとトランクには、優先順位に従ってデバイスまたはデバイス プール レベルでジオロケーション フィルタを設定できます。

論理パーティション ポリシーの設定

論理パーティション ポリシーは、ジオロケーション ID 間に設定されます。ジオロケーション ID は、フィルタ処理されたジオロケーションとデバイス タイプの組み合わせになります。フィルタ処理されたジオロケーションを取得するには、デバイスのジオロケーションを呼び出し、デバイスに関連付けられたジオロケーション フィルタを適用します。

ポリシーは、ジオロケーション オブジェクトのセットとデバイス タイプの組み合わせ（ソース ジオロケーション ID）として、そのようなもう 1 つの組み合わせ（ターゲット ジオロケーション ID）と関係付けて作成されます。関係が一致すると、設定されている「許可」または「拒否」の処理がコール レッグに適用されます。

（注）　ポリシーに設定されているジオロケーション オブジェクトのセットはそれぞれ、1 つのデバイス タイプに関連して考慮されます。たとえば、国 = インド、州 = カルナタカ、市 = バンガロールのようなジオロケーション オブジェクトのセットは、バンガロールの電話機に対する処理に関してはデバイス タイプ Interior に関連付ける必要があり、バンガロールのゲートウェイに対する処理に関してはデバイス タイプ Border に別に関連付ける必要があります。

論理パーティション ポリシーの適用

ユーザの操作によって新しいコール レッグが作成された場合（たとえば、ユーザが第 3 の発信者を既存のコールに参加させる場合）、Unified CM は各参加者ペアのジオロケーション ID と事前に設定されたポリシーのジオロケーション ID を照合します。

（注）　2 つのデバイスのジオロケーション ID が論理パーティションによって評価されている場合、両方のデバイスのデバイス タイプが Interior であれば、ポリシーは適用されません。つまり、同じクラスタ内の IP 電話間のコール、会議、転送などが論理パーティション ポリシーによって拒否されることはありません。

たとえば、インドのバンガロールにある電話機 A と B、およびカナダのオタワにあるゲートウェイ C について考えます。電話機 A から電話機 B にコールします。いずれのデバイスのタイプも Interior であるため、ポリシーは呼び出されません。コールが確立され、次に電話機 A のユーザが会議を起動し、それによってゲートウェイ C が引き込まれます。処理が許可される前に、Unified CM は A と C のジオロケーション ID、および B と C のジオロケーション ID をチェックして、事前に設定されたポリシーとの照合を行います。ポリシーの一致によって処理が拒否された場合、新しいコール レッグは確立できません。

（注）　Unified CM のデフォルト ポリシーは拒否です。つまり、コール レッグを許可するように明示的にポリシーを設定していなければ、コール レッグは拒否されます。

この例では、バンガロールの Interior デバイスがオタワの Border デバイスに接続できるように明示的にポリシーを設定していない限り、コール レッグは拒否されます。

H.323 ダイヤル ピアを使用する Cisco IOS でのコール ルーティング

H.323 プロトコルを使用する Cisco IOS ルータ上でのコール ルーティング ロジックは、ダイヤル ピア コンストラクトに依存しています。ダイヤル ピアは、静的ルートに似たものです。コールの発信地点と終端地点、およびコールがネットワークで通過するパスを定義しています。ダイヤル ピアは、コールの発信元と宛先のエンドポイントを指定するため、およびコール接続の各コール レッグに適用される特性を定義するために使用します。ダイヤル ピアに含まれている属性によって、ダイヤルされるどの番号をルータが収集し、テレフォニー デバイスに転送するかが決まります。

ダイヤル ピアおよびその設定の詳細については、次の Web サイトで入手可能な『*Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*』の「*Configuring Dial Plans, Dial Peers, and Digit Manipulation*」を参照してください。

http://www.cisco.com

ダイヤル ピアを使用したコール ルーティングを理解するための鍵の 1 つは、着信コール レッグと発信コール レッグ、つまり着信ダイヤル ピアと発信ダイヤル ピアという概念です。Cisco IOS ルータを経由する各コールは、2 つのコール レッグを持っていると見なされます。1 つはルータに入るもので、1 つはルータから出るものです。ルータに入るコール レッグが *着信コール レッグ*であり、ルータから出るコール レッグが *発信コール レッグ*です。

コール レッグには、主に次の 2 つのタイプがあります。

- ルータを公衆網、アナログ電話機、または PBX に接続する、従来の TDM テレフォニー コール レッグ
- ルータを他のゲートウェイ、ゲートキーパー、または Unified CM に接続する、IP コール レッグ

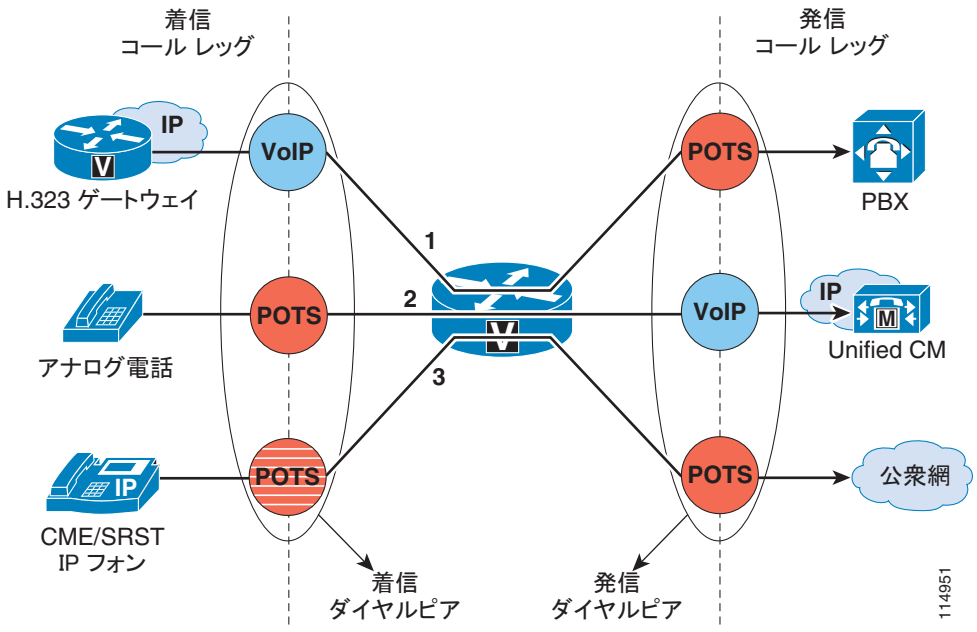
Cisco IOS は、ルータを通過するすべてのコールについて、1 つのダイヤル ピアを各コール レッグに関連付けます。ダイヤル ピアにも、関連付け先となるコール レッグのタイプに応じて、次に示す主に 2 つのタイプがあります。

- 従来の TDM テレフォニー コール レッグに関連付けられる、POTS ダイヤル ピア
- IP コール レッグに関連付けられる、VoIP ダイヤル ピア

図 10-39 では、Cisco IOS ルータを通過する、次の各種コールの例を示しています。

- コール 1 は、IP ネットワークにある別の H.323 ゲートウェイから、ルータに接続されている従来の（たとえば、PRI インターフェイス経由の）PBX までです。このコールに対しては、着信 VoIP ダイヤル ピアと発信 POTS ダイヤル ピアが選択されます。
- コール 2 は、ルータの FXS ポートに接続されているアナログ電話機から、IP ネットワークにある Unified CM クラスタまでです。このコールに対しては、着信 POTS ダイヤル ピアと発信 VoIP ダイヤル ピアがルータによって選択されます。
- コール 3 は、Cisco Unified Communications Manager Express（Unified CME）または SRST の制御する IP Phone から、ルータ上の公衆網インターフェイス（たとえば、PRI インターフェイス）までです。このコールに対しては、自動生成の POTS ダイヤル ピア（ルータ上に設定されている **ephone** に対応します）と発信 POTS ダイヤル ピアが選択されます。

図 10-39　着信ダイヤル ピアと発信ダイヤル ピア



着信コール レッグを着信ダイヤル ピアと対応付けるために、ルータは、セットアップ メッセージ内の情報要素（着信番号/DNIS と発信番号/ANI）が 4 つの設定可能ダイヤル ピア属性と一致するかどうか調べることによって、ダイヤル ピアを選択します。ルータは、これらの項目が一致するかどうかを次の順序で調べます。

1. 着信番号と **incoming called-number**
2. 発信番号と **answer-address**
3. 着信番号と **destination-pattern**
4. 着信音声ポートと設定済み音声ポート

ルータで必要となるのは、これらの条件のいずれか 1 つのみ一致することです。すべての属性をダイヤル ピア内に設定する必要はなく、すべての属性がコール セットアップ情報に一致している必要はありません。ルータがダイヤル ピアを選択するために必要な条件は 1 つのみです。ルータは、1 つのダイヤル ピアが一致するとすぐに検索を停止し、コールは設定済みのダイヤル ピア属性に従ってルーティングされます。一致するダイヤル ピアが他にある場合でも、最初に一致したピアのみが使用されます。

ルータが発信ダイヤル ピアを選択する方法は、着信 POTS ダイヤル ピアに **direct-inward-dial**（DID）が設定されているかどうかによって異なります。

- 着信 POTS ダイヤル ピアに DID が設定されていない場合、ルータは 2 ステージ ダイヤリングを実行し、着信ダイヤル ストリングを 1 桁ずつ収集します。1 つのダイヤル ピアが宛先パターンに一致すると、ルータは一致したダイヤル ピアの設定済み属性を使用して、コールをただちに発信します。
- 着信 POTS ダイヤル ピアに DID が設定されている場合、ルータは着信番号全体を使用して、発信ダイヤル ピアに含まれている宛先パターンに一致するかどうかを調べます。DID を使用する場合は、コールのルーティングに必要な番号がセットアップ メッセージにすべて含まれているため、番号をそれ以上収集する必要がありません。複数のダイヤル ピアがダイヤル ストリングに一致した場合、一致するすべてのダイヤル ピアが*ハント グループ*の形成に使用されます。ルータは、発信コール レッグを確立できるまで、ハント グループに含まれているすべてのダイヤル ピアを使用して確立を試行します。

デフォルトでは、ハント グループ内のダイヤル ピアは、次の基準を使用して、この順序に従って選択されます。

1. 電話番号の最長一致

   この方法では、ダイヤルされた番号と一致している部分が最も長い宛先パターンが選択されます。たとえば、あるダイヤル ピアがダイヤル ストリング 345.... を使用して設定され、2 番目のダイヤル ピアが 3456789 を使用して設定されている場合、ルータはまず 3456789 を選択します。2 つのダイヤル ピアのうち、正確に一致している部分が最も長いためです。

2. 明示的プリファレンス

   この方法では、**preference** ダイヤル ピア コマンドで設定した優先順位を使用します。プリファレンスの数値が小さくなるほど、優先順位が高くなります。最高の優先順位は、プリファレンス順位 0 のダイヤル ピアに与えられます。同じ宛先パターンを持つ複数のダイヤル ピアに対して同じ優先順位が定義されている場合、ダイヤル ピアはランダムに選択されます。

3. ランダム選択

   この方法では、すべての宛先パターンが同等の重みになります。

このデフォルト選択順序を変更することも、**dial-peer hunt** グローバル コンフィギュレーション コマンドを使用して、別のダイヤル ピア ハンティング方法を選択することもできます。このほかの選択基準は、*最長待機時間*です。最後に選択された時点から、最も長く待機している宛先パターンを選択します（Unified CM 回線グループの*最長アイドル時間*に相当します）。

Cisco IOS ルータ上で H.323 ダイヤル ピアを設定するときは、次のベスト プラクティスに従ってください。

- 着信公衆網コールが DNIS 情報に基づいて宛先に直接ルーティングされるようにするには、**direct-inward-dial** 属性を使用して、次のようにデフォルト POTS ダイヤル ピアを作成します。

```
dial-peer voice 999 pots
  incoming called-number .
  direct-inward-dial
  port 1/0:23
```

- ルータを Unified CM クラスタに接続されている H.323 ゲートウェイとして使用する場合は、同じ宛先パターンを持ち、2 つの異なる Unified CM サーバを指す VoIP ダイヤル ピアを少なくとも 2 つ設定して、冗長性を実装します。プライマリとセカンダリの Unified CM サーバ間での優先順位を選択するには、**preference** 属性を使用します。次に **preference** 属性の使用例を示します。

```
dial-peer voice 100 voip
 preference 1

!--- Make this the first choice dial peer.

 ip precedence 5
 destination-pattern 1...
 session target ipv4:10.10.10.2

!--- This is the address of the primary Unified CM.

 dtmf-relay h245-alpha


dial-peer voice 101 voip
 preference 2

!--- This  is the second choice.

 ip precedence 5
 destination-pattern 1...
 session target ipv4:10.10.10.3

!--- This is the address of the secondary Unified CM.

 dtmf-relay h245-alpha
```

ゲートキーパーを使用する Cisco IOS でのコール ルーティング

H.323 ゲートキーパーは、H.323 ネットワークにあるエンドポイント（Cisco Unified Communications Manager Express（Unified CME）および Unified CM クラスタ）、H.323 端末、ゲートウェイ、マルチポイント コントロール ユニット（MCU）など）を管理するためのオプション ノードであり、それらのエンドポイントにコール ルーティング機能とコール アドミッション制御機能を提供します。エンドポイントは、H.323 Registration Admission Status（RAS）プロトコルを使用してゲートキーパーと通信します。

エンドポイントは、起動するとゲートキーパーへの登録を試行します。他のエンドポイントとの通信が必要な場合は、E.164 アドレスや電子メール アドレスなど、自身のシンボリック エイリアスを使用して、コールを開始するための許可を要求します。ゲートキーパーは、そのコールを許可してもよいと判断した場合、宛先の IP アドレスを発信元エンドポイントに返します。この IP アドレスは、宛先エンドポイントの実際の IP アドレスではなく、中継アドレスである場合もあります。たとえば、Cisco Unified Border Element や、コール シグナリングをルーティングするゲートキーパーのアドレスです。

H.323 プロトコル、および H.323 エンドポイントとゲートキーパーとのメッセージ交換の詳細については、次の Web サイトで入手可能な『*Cisco IOS H.323 Configuration Guide*』を参照してください。

http://www.cisco.com

Cisco 2600、3600、3700、2800、3800、および 7200 シリーズのルータはすべて、ゲートキーパー機能をサポートします。冗長性、ロード バランシング、および階層コール ルーティング用に、さまざまな方法で Cisco IOS ゲートキーパーを設定できます。ここでは、ゲートキーパー機能のコール ルーティング機能を中心に説明します。冗長性とスケーラビリティに関する考慮事項については、「ゲートキーパーの冗長性」（P.8-27）を参照してください。コール アドミッション制御に関する考慮事項については、「Cisco IOS ゲートキーパー ゾーン」（P.9-16）を参照してください。

Cisco IOS ゲートキーパーのコール ルーティングは、次のタイプの情報に基づいています。

- 静的に設定されている情報（ゾーン プレフィックスや、デフォルト テクノロジー プレフィックスなど）
- 動的な情報（登録フェーズで H.323 デバイスが提供した E.164 アドレスやテクノロジー プレフィックスなど）
- コールごとの情報（着信番号やテクノロジー プレフィックスなど）

ゾーンは、エンドポイント、ゲートウェイ、MCU などの、ゲートキーパーに登録される H.323 デバイスの集合です。アクティブになることができるゲートキーパーは、ゾーンごとに 1 つのみです。1 つのゲートキーパーには、ローカル ゾーンを 100 個まで定義できます。

H.323 エンドポイントがゲートキーパーに登録すると、エンドポイントはゾーンに割り当てられます。また、処理できるコールの種類（音声、ビデオ、ファクスなど）を指定するテクノロジー プレフィックスとともに、処理を担当している 1 つまたはそれ以上の E.164 アドレスを登録することもできます。

ゾーンごとに、ゲートキーパー上で 1 つまたはそれ以上の *ゾーン プレフィックス*を設定できます。ゾーン プレフィックスは、番号とワイルドカードを含んだストリングであり、ゲートキーパーがコール ルーティングの判断に使用します。ゾーン プレフィックス ストリングでは、次の文字を使用できます。

- 0 ～ 9 までのすべての数字。それぞれが特定の 1 桁に対応
- ドット（.）ワイルドカード。いずれかの 1 桁の 0 ～ 9 までの数字に対応
- * ワイルドカード。1 またはそれ以上の桁の 0 ～ 9 までの数字に対応

ゲートキーパーのコール ルーティング動作を理解するには、メッセージ解析ロジックについて考えると役立ちます。図 10-40 では、アドミッション要求（ARQ）の解析ロジックを示しています。エンドポイントは、コールを初期化するために、ARQ（Admission Request ; アドミッション要求）をゲートキーパーに送信します。ARQ には、宛先つまり着信側の H.323 ID または E.164 アドレスのどちらか、および送信元つまり発信側の E.164 アドレスまたは H.323 ID が含まれています。

ARQ に E.164 アドレスが入っている（Unified CM では、ARQ には常に E.164 アドレスが入っています）場合、ARQ にはテクノロジー プレフィックスが含まれている場合と、含まれていない場合があります。ARQ にテクノロジー プレフィックスが含まれている場合、ゲートキーパーはテクノロジー プレフィックスを着信番号から削除します。ARQ にテクノロジー プレフィックスが含まれていない場合、ゲートキーパーは、デフォルトのテクノロジー プレフィックスが設定されていれば、それを使用します（「集中型ゲートキーパー設定」（P.10-116）の項の **gw-type-prefix** コマンドを参照）。このように取得したテクノロジー プレフィックスは、メモリに格納され、ゲートキーパーはコール ルーティング アルゴリズムに基づく処理を続行します。

次に、ゲートキーパーは、着信番号が設定済みのいずれかのゾーン プレフィックスに一致しないかどうかを調べます。一致する可能性のあるエントリが複数ある場合は、一致する部分の最も長いものが使用されます。一致するゾーン プレフィックスがない場合、未知のプレフィックスを持つコールを受け付けるようにゲートキーパーが設定されているときは、ゲートキーパーは宛先ゾーンが発信元ゾーンと同じであると想定します。

この時点で、ゲートキーパーは選択された宛先ゾーン内を検索して、着信番号に一致する登録済み E.164 アドレスがあるかどうかを調べます。一致が見つかると、コールに関して要求した帯域幅が使用可能になっていて、着信側エンドポイントがゲートキーパーに登録されている場合、ゲートキーパーはアドミッション確認（ACF）を送信します。ACF には、宛先エンドポイントの IP アドレスが入っています。帯域幅が使用不能であるか、着信側エンドポイントが登録されない場合、ゲートキーパーは、発信側エンドポイントに ARJ（Admission Reject ; アドミッション拒否）を戻します。

一致する E.164 アドレスが宛先ゾーン内に登録されていない場合、ゲートキーパーは、以前に格納したテクノロジー プレフィックスを使用して、そのゾーンに登録されているゲートウェイをコールの宛先として選択します。ゲートキーパーが ACF または ARJ のどちらを発信元エンドポイントに送信するかは、帯域幅の可用性とエンドポイントの登録に関する、上と同じ考慮事項に基づいて決まります。

送信元エンドポイントは、ゲートキーパーから ACF を受信した後、ACF で戻された IP アドレスを使用して、直接セットアップ メッセージを宛先エンドポイントに送信できます。

図 10-40　　ARQ のゲートキーパー アドレス解決

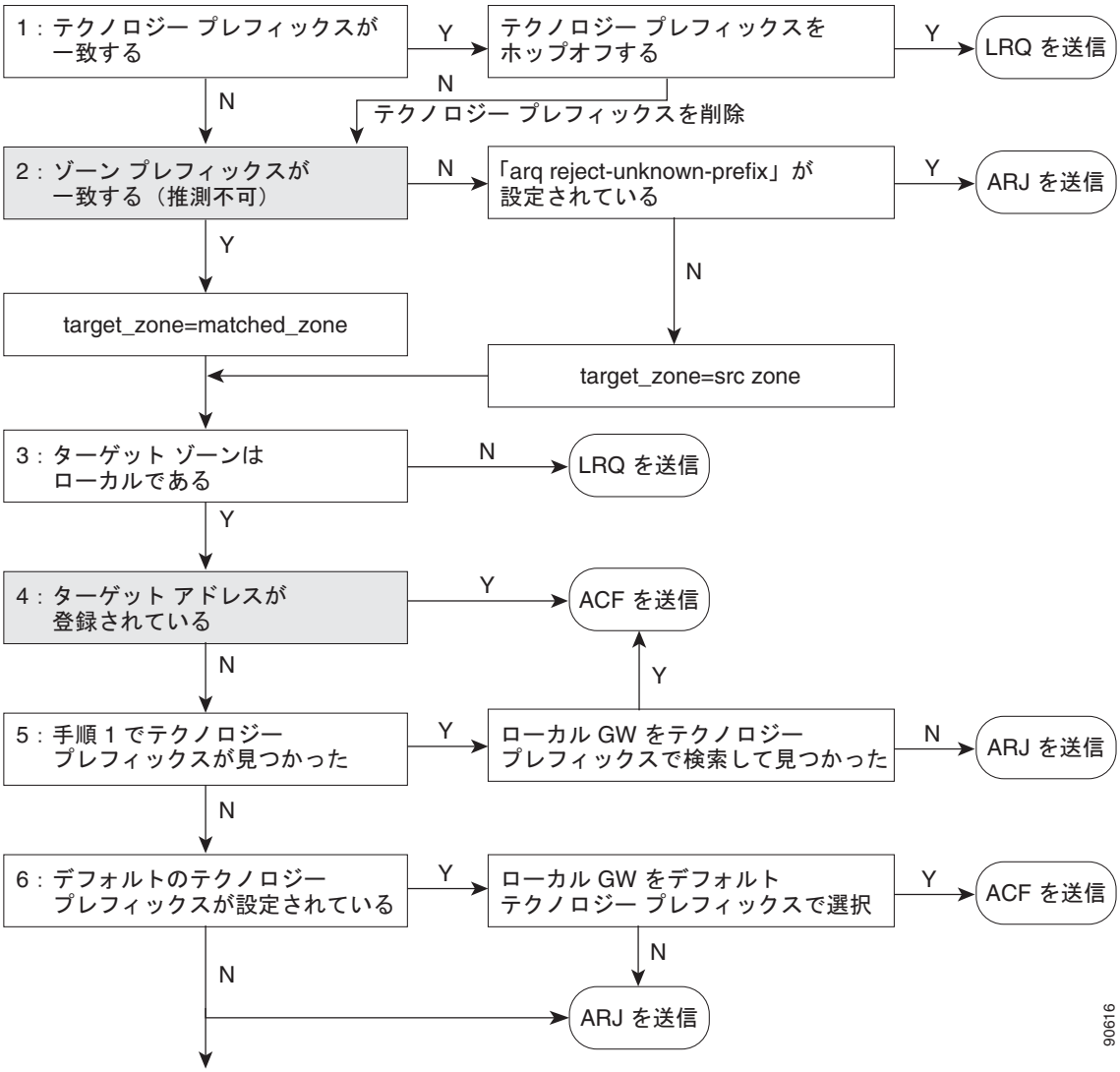
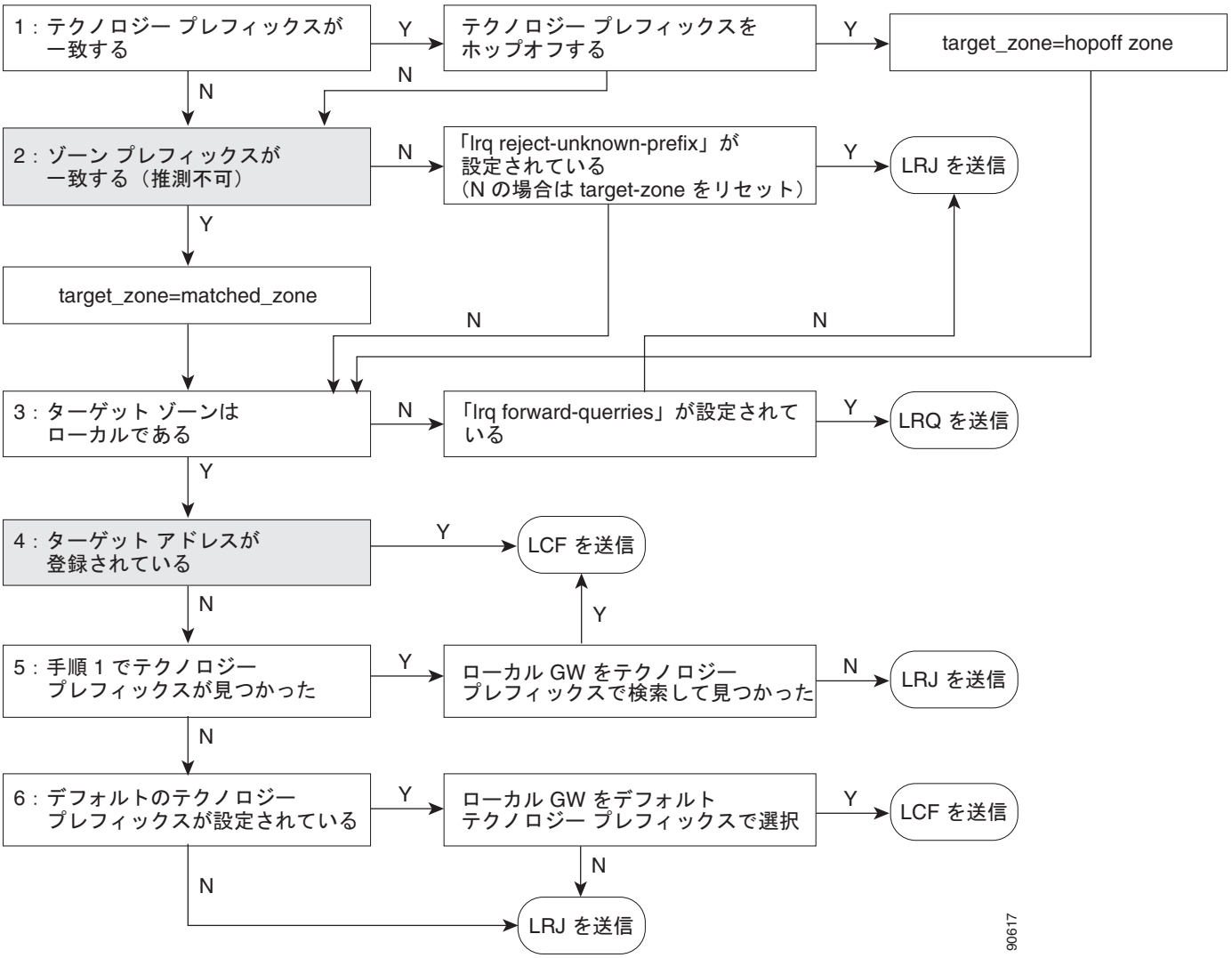


図 10-41 では、ロケーション要求（LRQ）の解析ロジックを示しています。LRQ メッセージは、ゲートキーパー間で交換され、ゾーン（リモート ゾーン）間のコールに使用されます。たとえば、ゲートキーパー A が ARQ をローカル ゾーンのゲートウェイから受信し、その ARQ は、リモート ゾーンのデバイスに対するコール アドミッションを要求しているとします。ゲートキーパー A は、ゲートキーパー B に LRQ メッセージを送信します。ゲートキーパー A は、ゲートキーパー B に LRQ メッセージを送信します。ゲートキーパー B は、自身がゾーン間コール要求を許可するように設定されているかどうか、および要求されたリソースが登録されているかどうかに応じて、この LRQ メッセージにロケーション確認（LCF）メッセージまたはロケーション拒否（LRJ）メッセージで応答します。

図 10-41　　LRQ のゲートキーパー アドレス解決



従来の Cisco IOS ゲートキーパー機能は、*中継ゾーン ゲートキーパー*という概念を通じて、Cisco Unified Border Element に対応するように拡張されました。配置の例については、「RSVP 機能のある Cisco IOS Gatekeeper および Cisco Unified Border Element」（P.9-29）を参照してください。

中継ゾーン ゲートキーパーがレガシー ゲートキーパーと異なっている点は、コール ルーティングでの LRQ メッセージと ARQ メッセージの使用方法です。中継ゾーン ゲートキーパーを使用しても、通常のクラスタおよび機能はそのまま使用できます。レガシー ゲートキーパーは、着信する LRQ を着信番号に基づいて検査します。具体的には、LRQ の destinationInfo 部分にある dialedDigits フィールドを

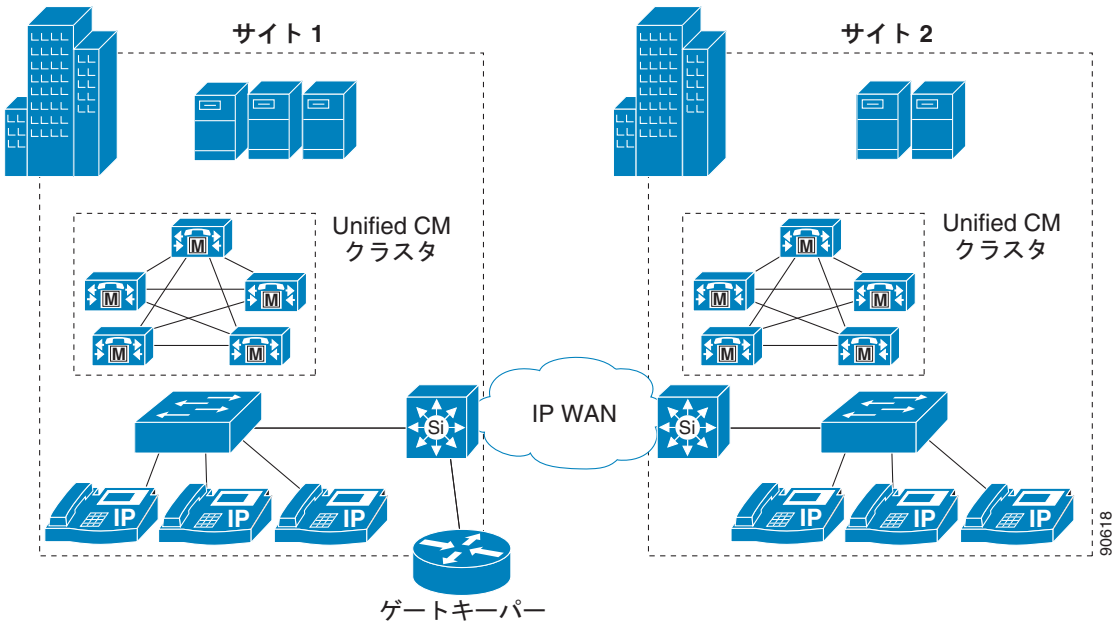
検査します。中継ゾーン ゲートキーパーは、着信番号を検査する前に LRQ の発信地点を検査します。LRQ が、中継ゾーン ゲートキーパーのリモート ゾーン設定にリストされているゲートキーパーから送信されている場合、ゲートキーパーは、ゾーンのリモート設定に **invia** キーワードまたは **outvia** キーワードが含まれているかどうかを確認します。設定にこれらのいずれかのキーワードが含まれている場合、ゲートキーパーは中継処理をします。含まれていない場合は、従来の処理をします。

ARQ メッセージの場合、ゲートキーパーは宛先ゾーンに **outvia** キーワードが設定されているかどうかを調べます。**outvia** キーワードが設定されていて、**outvia** キーワードを使用して命名されているゾーンがゲートキーパーに対してローカルである場合は、そのゾーンの Cisco Unified Border Element がポイントされている ACF が返され、コールは Cisco Unified Border Element に転送されます。**outvia** キーワードを使用して命名されているゾーンがリモートである場合、ゲートキーパーは、ロケーション要求（LRQ）をリモート ゾーンのゲートキーパーではなく **outvia** ゲートキーパーに送信します。**invia** キーワードは、ARQ の処理では使用されません。

集中型ゲートキーパー設定

単一のゲートキーパーは、クラスタ間のコール ルーティング、および最大 100 の Unified CM クラスタに対するコール アドミッション制御をサポートできます。図 10-42 では、2 つの Unified CM クラスタと単一の集中型ゲートキーパーを備えた分散型コール処理環境を示しています。

図 10-42　　2 つのクラスタをサポートする集中型ゲートキーパー



例 10-5 では、図 10-42 のゲートキーパー設定を示しています。

例 10-5　　集中型ゲートキーパーの設定

```
gatekeeper
 zone local GK-Site1 customer.com 10.1.10.100
 zone local GK-Site2 customer.com
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth interzone GK-Site1 160
 bandwidth interzone GK-Site2 160
 gw-type-prefix 1#* default-technology
```

```
arq reject-unknown-prefix
no shutdown
```

ここでは、図 10-42 について説明します。

- Unified CM トランク登録をサポートするために、各 Unified CM クラスタにはローカル ゾーンが設定されます。
- ゾーン間とクラスタ間のコール ルーティングを可能にするために、ゾーンごとにゾーン プレフィックスが設定されます。
- サイトごとに帯域幅ステートメントが設定されます。シスコでは、**bandwidth interzone** コマンドを使用することをお勧めします。**bandwidth total** コマンドを使用すると、設定内容によっては問題が発生することがあるためです。帯域幅はキロビット/秒（kbps）単位で測定されます。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Unified CM トランクは、1# プレフィックスに登録されるように設定されています。

  テクノロジー プレフィックスは、発信されているコールのタイプを示しています。テクノロジー プレフィックスとして使用される個々の値は任意のものであり、ネットワーク管理者が定義します。配置全体で常に同じ値を使用する必要があります。

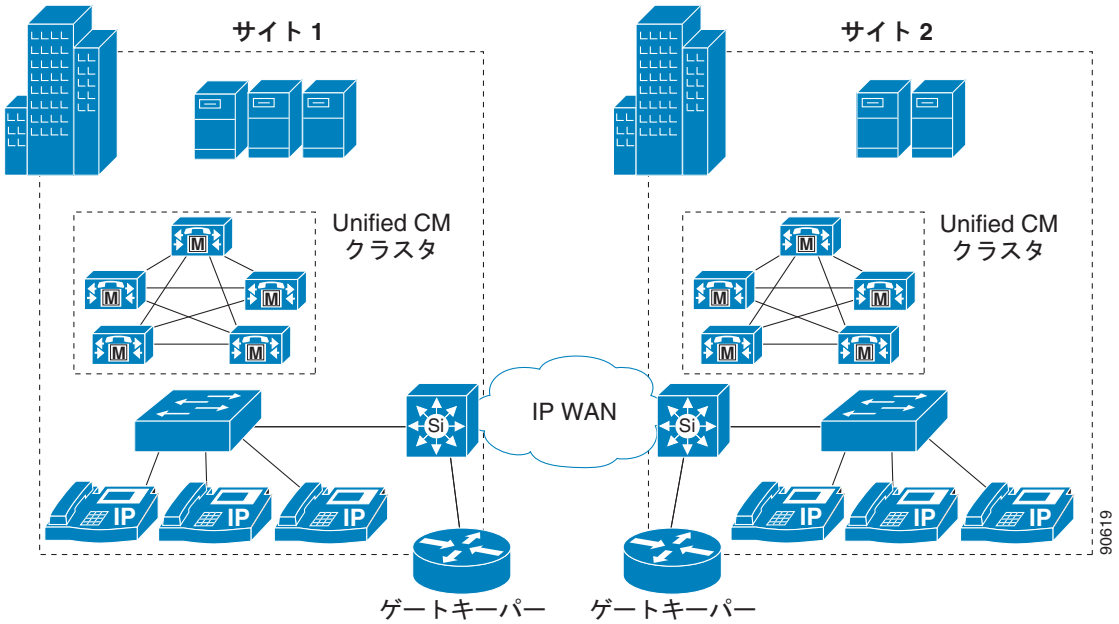
  テクノロジー プレフィックスは、E.164 アドレス（電話番号）のプレフィックスとして送信され、コールが音声であるか、ビデオであるか、その他のタイプであるかを示します。# シンボルは、一般に、プレフィックスと E.164 番号を区別するために使用します。プレフィックスが含まれていない場合、コールのルーティングにはデフォルトのテクノロジー プレフィックスが使用されます。配置全体で 1 つのデフォルト テクノロジー プレフィックスだけが使用される場合があります。

  Cisco IOS ゲートウェイは、プレフィックスが設定されていれば、自動的に発信コールにテクノロジー プレフィックスを追加します。ゲートウェイは、自動的に着信 H.323 コールからプレフィックスを除去します。Unified CM は、ゲートキーパー制御 H.323 トランクの設定ページで指定されているテクノロジー プレフィックスを使用して、ゲートキーパーに登録することができます。ただし、このテクノロジー プレフィックスは、ゲートキーパーに向かう発信コールに自動的に追加されることはありません。また、Unified CM に向かう着信コールから自動的に除去されることもありません。トランスレーション パターンとゲートウェイ コンフィギュレーションを使用して着信番号を操作すると、テクノロジー プレフィックスを必要に応じて追加または除去できます。
- **arq reject-unknown-prefix** コマンドは、冗長 Unified CM トランク上にできるコール ルーティング ループを回避します。

分散型ゲートキーパー設定

帯域幅を節約するため、または WAN 障害時に H.323 ゲートウェイにローカル コール ルーティングをサポートするために、ゲートキーパーを分散させることができます。図 10-43 は、2 つのクラスタと 2 つのゲートキーパーを備えた分散型コール処理環境を示しています。

図 10-43　　2 つのクラスタをサポートする分散型ゲートキーパー



例 10-6 では、図 10-43 のサイト 1 に対するゲートキーパー設定を示しています。

例 10-6　　サイト 1 のゲートキーパー設定

```
gatekeeper
 zone local GK-Site1 customer.com 10.1.10.100
 zone remote GK-Site2 customer.com 10.1.11.100
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth remote 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 10-6 について説明します。

- ローカル Unified CM クラスタ トランクの登録用に、ローカル ゾーンが設定されます。
- サイト 2 のゲートキーパーへのコール ルーティング用に、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のゾーンにゾーン プレフィックスが設定されます。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Unified CM トランクは、1# プレフィックスに登録されるように設定されています。

- **arq reject-unknown-prefix** コマンドは、冗長 Unified CM トランク上にできるコール ルーティング ループを回避します。

例 10-7 は、図 10-43 のサイト 2 に対するゲートキーパー設定を示しています。

例 10-7　　サイト 2 のゲートキーパー設定

```
gatekeeper
 zone local GK-Site2 customer.com 10.1.11.100
 zone remote GK-Site1 customer.com 10.1.10.100
 zone prefix GK-Site2 212.......
 zone prefix GK-Site1 408.......
 bandwidth remote 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 10-7 について説明します。

- ローカル Unified CM クラスタ トランクの登録用に、ローカル ゾーンが設定されます。
- サイト 1 のゲートキーパーへのコール ルーティング用に、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のゾーンにゾーン プレフィックスが設定されます。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Unified CM トランクは、1# プレフィックスに登録されるように設定されています。
- **arq reject-unknown-prefix** コマンドは、冗長 Unified CM トランク上にできるコール ルーティング ループを回避します。

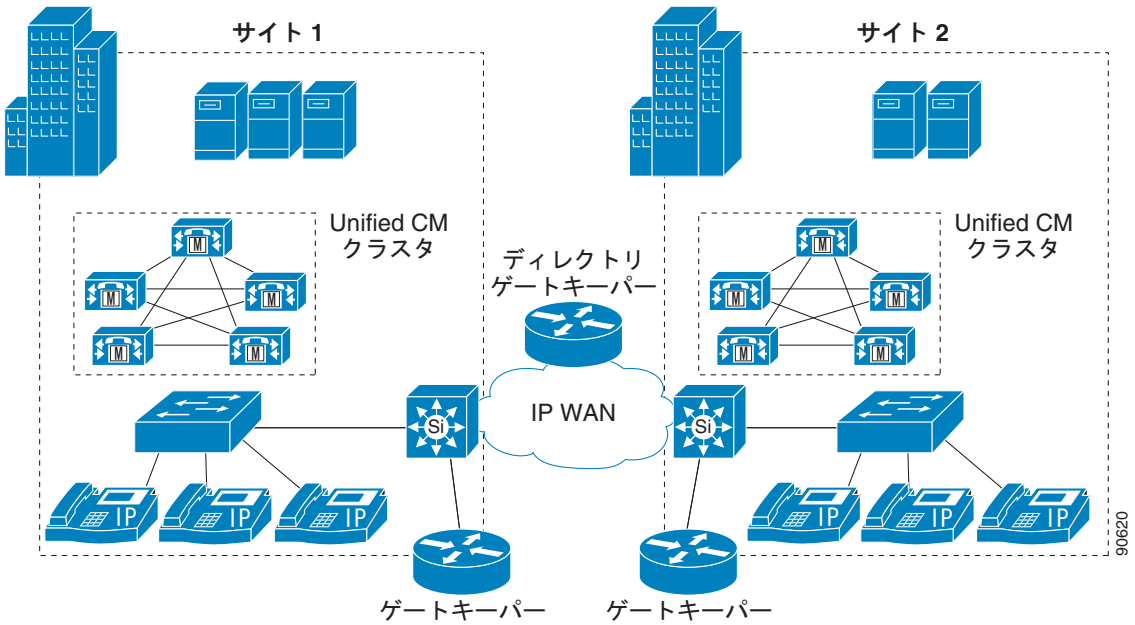
ディレクトリ ゲートキーパーを使用した分散型ゲートキーパー設定

ゲートキーパー ルーティング テーブルを更新するために使用できるゲートキーパー プロトコルがないので、ディレクトリ ゲートキーパーを使用すると、分散型ゲートキーパー設定のスケーラビリティとマネージャビリティの向上に役立ちます。ディレクトリ ゲートキーパーを実装すると、各サイトのゲートキーパー設定が簡単になり、ゾーン間通信の大部分の設定をディレクトリ ゲートキーパーでできるようになります。

ディレクトリ ゲートキーパーがない場合、ゲートキーパーに新しいゾーンを追加するたびに、ネットワーク上のすべてのゲートキーパーに項目を追加する必要があります。しかし、ディレクトリ ゲートキーパーを使用すると、ローカル ゲートキーパーとディレクトリ ゲートキーパーのみで新しいゾーンを追加できます。ローカル ゲートキーパーは、コール要求をローカル側で解決できない場合、ゾーン プレフィックスが一致するディレクトリ ゲートキーパーにその要求を転送します。

図 10-44 では、ローカル コール ルーティング用の分散型ゲートキーパー、およびゲートキーパー間のコール ルーティングをサポートするディレクトリ ゲートキーパーを備えた、Unified CM 分散型コール処理環境を示しています。

図 10-44　ディレクトリ ゲートキーパーを備えた分散ゲートキーパー



例 10-8 では、図 10-44 のサイト 1 に対するゲートキーパー設定を示しています。この例では、サイト 1 とサイト 2 のゲートキーパー設定がほぼ同じなので、ここでは、サイト 1 だけについて説明します。

例 10-8　ディレクトリ ゲートキーパーを使用したサイト 1 のゲートキーパー設定

```
gatekeeper
 zone local GK-Site1 customer.com 10.1.10.100
 zone remote DGK customer.com 10.1.10.101
 zone prefix GK-Site1 408.......
 zone prefix DGK ..........
 bandwidth remote 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 10-8 について説明します。

- ローカル Unified CM クラスタ トランクの登録用に、ローカル ゾーンが設定されます。
- ディレクトリ ゲートキーパー用にリモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のゾーンにゾーン プレフィックスが設定されます。
- ディレクトリ ゲートキーパーのゾーン プレフィックスは、10 個のドットを使用して設定されます。このパターンは、未解決の任意の 10 桁のダイヤル ストリングと一致します。1 つのゾーンに複数のゾーン プレフィックスを設定して、異なる長さのダイヤル ストリングを一致させることができます。ディレクトリ ゲートキーパーのゾーン プレフィックスにもワイルドカード（*）を使用できますが、この方法はコール ルーティングの問題が発生する場合があります。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Unified CM トランクは、1# プレフィックスに登録されるように設定されています。

- **arq reject-unknown-prefix** コマンドは、冗長 Unified CM トランク上にできるコール ルーティング ループを回避します。

例 10-9 では、図 10-44 の例のディレクトリ ゲートキーパー設定を示しています。

例 10-9　　ディレクトリ ゲートキーパー設定

```
gatekeeper
 zone local DGK customer.com 10.1.10.101
 zone remote GK-Site1 customer.com 10.1.10.100
 zone remote GK-Site2 customer.com 10.1.11.100
 zone prefix GK-Site1 408*
 zone prefix GK-Site2 212*
 lrq forward-queries
 no shutdown
```

ここでは、例 10-9 について説明します。

- ディレクトリ ゲートキーパー用にローカル ゾーンが設定されます。
- リモート ゲートキーパーごとに、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のリモート ゾーンにゾーン プレフィックスが設定されます。設定を簡単にするために、ゾーン プレフィックスでワイルドカード（*）が使用されます。コールは DGK ゾーンにルーティングされないので、DGK ゾーンにはプレフィックスが必要ありません。
- **lrq forward-queries** コマンドは、ディレクトリ ゲートキーパーが、別のゲートキーパーから受信した LRQ を転送できるようにします。

H.323 ダイヤル ピアを使用する Cisco IOS のコール特権

H.323 を使用する Cisco IOS ベースのシステム（H.323 ゲートウェイ、SRST、および Cisco Unified Communications Manager Express（Unified CME）を含む）にコール特権を実装するには、制限クラス（COR）機能を使用します。この機能は、ネットワークの設計に柔軟性をもたらし、管理者は、すべてのユーザに関して任意のコールをブロックできるようになります（たとえば、米国では 900 番号へのコール）。また、個々の発信者のコール試行に対して、それぞれ別のコール特権を適用できます（一部のユーザには国際通話を許可し、他のユーザには許可しない、など）。

COR 機能の中心となる基本的メカニズムは、着信と発信の *COR リスト*を定義することで成立しています。このリストは既存のダイヤル ピアに関連付けるもので、着信および発信という概念は、Cisco IOS ルータに対してのものです（ダイヤル ピアの場合と同様）。各 COR リストは、メンバーの番号を含めることで定義します。この番号は、Cisco IOS 内に定義済みの単純なタグです。

コールがルータを通過するときには、Cisco IOS ダイヤル ピア ルーティング ロジックに基づいて、着信ダイヤル ピアと発信ダイヤル ピアが選択されます。選択されたダイヤル ピアに COR リストが関連付けられている場合は、コールをルーティングする前に、さらに次のチェックが実行されます。

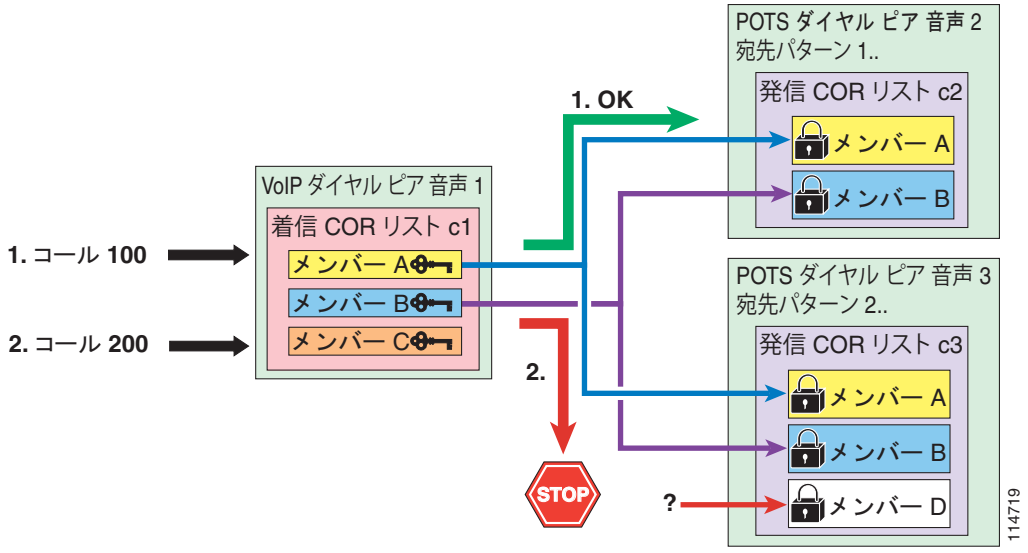
- 発信ダイヤル ピアに関連付けられている発信 COR リストのメンバーが、着信ダイヤル ピアに関連付けられている着信 COR リストのメンバーのサブセットである場合、コールは許可されます。
- 発信ダイヤル ピアに関連付けられている発信 COR リストのメンバーが、着信ダイヤル ピアに関連付けられている着信 COR リストのメンバーのサブセットでは*ない*場合、コールは拒否されます。

COR リスト ステートメントが一切適用されていないダイヤル ピアが存在する場合は、次のプロパティが適用されます。

- ダイヤル ピア上に着信 COR リストが設定されていない場合は、デフォルトの着信 COR リストが使用されます。デフォルト着信 COR リストは最高の優先順位を持っているため、発信 COR リストの内容にかかわらず、このダイヤル ピアは他のすべてのダイヤル ピアにアクセスできます。
- ダイヤル ピア上に発信 COR リストが設定されていない場合は、デフォルトの発信 COR リストが使用されます。デフォルト発信 COR リストは優先順位が最も低いため、着信 COR リストの内容にかかわらず、他のすべてのダイヤル ピアがこのダイヤル ピアにアクセスできます。

この動作の内容を最もよく表しているのが、図 10-45 に示す例です。この例では、1 つの VoIP ダイヤル ピアと 2 つの POTS ダイヤル ピアが定義されています。

図 10-45　　COR の動作の例



この VoIP ダイヤル ピアは、メンバー A、B、C を持つ着信 COR リスト c1 に関連付けられています。着信 COR リストのメンバーは、「鍵」だと考えることができます。

最初の POTS ダイヤル ピアは、宛先パターン 1.. を持っており、メンバー A と B を持つ発信 COR リスト c2 に関連付けられています。2 番目の POTS ダイヤル ピアは、宛先パターン 2.. を持っており、メンバー A、B、D を持つ発信 COR リスト c3 に関連付けられています。発信 COR リストのメンバーは、「錠」だと考えることができます。

コールが成功するには、発信ダイヤル ピアの発信 COR リストにあるすべての「錠」を開けるための「鍵」を、着信ダイヤル ピアの着信 COR リストがすべて持っている必要があります。

図 10-45 に示した例では、宛先が 100 になっている最初の VoIP コールがルータに受信されます。Cisco IOS コール ルーティング ロジックによって、着信コール レッグが VoIP ダイヤル ピアに、発信コール レッグが最初の POTS ダイヤル ピアに対応付けられます。次に、COR ロジックが適用されます。c1 着信 COR リストは、c2 発信 COR リストの錠（A と B）に必要な鍵をすべて持っているため、コールは成功します。

次に、宛先が 200 になっている 2 番目の VoIP コールがルータで受信されます。Cisco IOS コール ルーティング ロジックによって、着信コール レッグが VoIP ダイヤル ピアに、発信コール レッグが 2 番目の POTS ダイヤル ピアに対応付けられます。次に、COR ロジックが適用されます。c1 着信 COR リストは、c3 発信 COR リスト（D）に必要な「鍵」を 1 つ持っていないため、コールは拒否されます。

Cisco IOS で COR 機能を設定するには、次の手順に従います。

ステップ 1　コマンド **dial-peer cor custom** を使用して、COR リスト メンバーとして使用される「タグ」を定義します。

ステップ 2　コマンド **dial-peer cor list** *corlist-name* を使用して、COR リストを定義します。

ステップ 3　COR リストを既存の VoIP ダイヤル ピアまたは POTS ダイヤル ピアに関連付けます。このためには、ダイヤル ピアの設定で、コマンド **corlist** {**incoming** | **outgoing**} *corlist-name* を使用します。

Cisco IOS Release 12.2(8)T 以降では、COR 機能を SRST 制御の IP Phone に適用できます。IP Phone は、SRST ルータに対して動的に登録を実行します。このため、SRST では、IP Phone が Cisco Unified CM クラスタへの接続を失うときまで、個々の IP Phone について事前には一切把握していません。したがって、COR 機能の SRST 用の設定は、電話の DN に基づいています。SRST ルータに登録するとき、IP Phone は自身の DN をルータに通知して、SRST ルータが IP Phone を適切な COR リストに割り当てられるようにします。

SRST によって制御される IP Phone のための COR を設定するには、コマンド **cor** {**incoming** | **outgoing**} *corlist-name* {*corlist-number starting-number – ending-number* | **default**} を **call-manager-fallback** コンフィギュレーション モードで使用します。

このコマンドには、次の制限事項があります。

- Cisco IOS Release 12.2(8)T 以降で使用可能な SRST バージョン 2.0 では、**call-manager-fallback** で許容される **cor** {**incoming** | **outgoing**} ステートメントの数は、最大で 5（デフォルト ステートメント含まず）です。
- Cisco IOS Release 12.3(4)T 以降で使用可能な SRST バージョン 3.0 では、**call-manager-fallback** で許容される **cor** {**incoming** | **outgoing**} ステートメントの数は、最大で 20（デフォルト ステートメント含まず）です。

COR 機能は、Cisco IOS Release 12.2(8)T 以降を使用する Cisco Unified Communications Manager Express（Unified CME）にも配置できます。個々の IP Phone は、Unified CME で具体的に設定されます。したがって、COR リストを IP Phone 自体に直接適用することができます。このためには、コマンド **cor** {**incoming** | **outgoing**} *corlist-name* を各 IP Phone の **ephone-dn** *dn-tag* コンフィギュレーション モードで使用します。

これらの概念を実際に適用する方法の例については、「H.323 を使用している Cisco IOS でのサービス クラスの構築」（P.10-52）の項を参照してください。

Cisco SRST と Cisco Unified CallManager Express の設定の詳細については、次の Web サイトで入手可能な『*Cisco SRST System Administrator Guide*』および『*Cisco Unified Communications Manager Express System Administrator Guide*』を参照してください。

http://www.cisco.com

H.323 ダイヤル ピアを使用する Cisco IOS での番号操作

H.323 を実行している Cisco IOS ルータでは、番号操作は音声トランスレーション プロファイルを通じて実行されます。このプロファイルは、音声コールの発信番号（ANI）または着信番号（DNIS）の番号を操作するために、またはコールの番号タイプを変更するために使用されるものです。

音声トランスレーション プロファイルは、Cisco IOS Release 12.2(11)T 以降で使用できます。このプロファイルは、コールが着信ダイヤル ピアに対応付けられる前、またはコールが発信ダイヤル ピアによって転送される前に、電話番号を別の番号に変換するために使用します。たとえば、社内で 5 桁の内線番号をダイヤルすると、別のサイトにいる従業員に到達できるとします。コールが他のサイトに公衆

網を通じてルーティングされ、到達する場合は、発信側のゲートウェイで音声トランスレーション プロファイルを使用する必要があります。これによって、5 桁の内線番号が公衆網で認識される 10 桁の形式に変換されます。

音声トランスレーション プロファイルを設定するには、**voice translation-rule** および **voice translation-profile** Cisco IOS コマンドを使用します。これらのコマンドでは、変換の対象となる番号ストリングを正規表現を使用して定義します。次に、この操作を発信番号、着信番号、リダイレクト先着信番号のいずれに関連付けるのかを指定します。音声トランスレーション プロファイルを定義した後に、次の任意の要素に適用することができます。

- 特定の音声ポート上で終端する、すべての着信 POTS コール レッグ
- ルータに入るすべての着信 VoIP コール レッグ
- 特定の VoIP ダイヤル ピアまたは POTS ダイヤル ピアに関連付けられている発信コール レッグ
- SRST 制御の IP Phone 上で終端する、すべての着信または発信コール レッグ
- SRST 制御のすべての IP Phone によって発信されるコールのための着信コール レッグ

（注）　**voice translation-rule** コマンドを使用する音声トランスレーション プロファイルは、以前に **translation-rule** コマンドで提供されていた機能を置き換え、拡張するものです。この新しいコマンドの構文は、以前のコマンドで使用されていた構文とは異なります。詳細については、http://www.cisco.com で入手可能な『*Cisco IOS Voice Command Reference*』（Release 12.2(11)T 以降）の **voice translation-rule** を参照してください。

音声トランスレーション プロファイルの一般的な用途は、IP WAN が使用不可になっていてルータが SRST モードで動作している場合でも、支店サイトからのオンネット サイト間ダイヤリング手順をそのまま維持できるようにすることです。たとえば、中央サイトが San Jose にあり、3 つのリモート サイトが San Francisco、New York、Dallas にある単純な配置について考えます。表 10-10 では、この例の DID 範囲と内部サイト コードを示しています。

表 10-10　変換規則応用例の DID 範囲とサイト コード

	San Jose	San Francisco	New York	Dallas
DID 範囲	(408) 555-1XXX	(415) 555-1XXX	(212) 555-1XXX	(972) 555-1XXX
サイト コード	1	2	3	4

サイト間のコールは、オンネット アクセス コード 8 の次に 1 桁のサイト コードと着信側の 4 桁内線番号をダイヤルすることによって、通常は IP WAN 経由で発生します。IP WAN がダウンしていて Cisco SRST がアクティブな場合にも、これらのダイヤリング手順を維持できるようにするには、内部の番号を E.164 番号に再変換してから公衆網に送信する必要があります。次に、San Francisco ルータの設定例を示します。

```
voice translation-rule 1
  rule 1 /^81/ /91408555/
  rule 2 /^83/ /91212555/
  rule 3 /^84/ /91972555/

voice translation-profile on-net-xlate
  translate called 1

call-manager-fallback
  translation-profile outgoing on-net-xlate

dial-peer voice 2 pots
  destination-pattern 91[2-9]..[2-9].....
```

```
port 1/0:0
  direct-inward-dial
  forward-digits 11
```

この設定では、San Francisco サイトが SRST モードになっているときにユーザが 831000 をダイヤルすると、ルータは **voice translation-rule 1** の **rule 2** と一致するものと判定し、着信番号を 912125551000 に変換します。この新しい番号が使用され、発信ダイヤル ピア（**dial-peer voice 2**）と一致するものと判定されます。

ダイヤル ピアおよびその設定の詳細については、次の Web サイトで入手可能な『*Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*』の「*Configuring Dial Plans, Dial Peers, and Digit Manipulation*」を参照してください。

http://www.cisco.com

Cisco IOS の正規表現構文の詳細については、次の Web サイトで入手可能な『*Cisco IOS Terminal Services Configuration Guide*』の「*Regular Expressions*」を参照してください。

http://www.cisco.com/en/US/docs/ios/termserv/configuration/guide/tsv_reg_express_ps6441_TSD_Products_Configuration_Guide_Chapter.html

CHAPTER 11

Emergency Services

Last revised on: August 5, 2008

Emergency services are of great importance in the proper deployment of a voice system. This chapter presents a summary of the following major design considerations essential to planning for emergency calls:

This chapter presents some information specific to the 911 emergency networks as deployed in Canada and the United States. Many of the concepts discussed here are adaptable to other locales. Please consult with your local telephony network provider for appropriate implementation of emergency call functionality.

In the United States, some states have already enacted legislation covering the 911 functionality required for users in a multi-line telephone system (MLTS). The National Emergency Number Association (NENA) has also produced the *Technical Information Document on Model Legislation Enhanced 911 for Multi-Line Telephone Systems*, available online at

http://www.nena.org/media/files/MLTS_ModLeg_Nov2000.pdf

The Federal Communications Commission (FCC) has also drafted a proposed new section to Title 47, Part 68, Section 319, which is available at

http://www.apcointl.org/about/pbx/worddocs/mltspart68.doc

This chapter assumes that you are familiar with the generic 911 functionality available to residential PSTN users in North America. For more information on the subject, refer to the following URL for a description of the current state of E911 services in North America:

http://www.nena.org/florida/Directory/911Tutorial%20Study%20Guide.pdf

Planning for 911 Functionality

This section highlights some of the functionality requirements for lifeline calls in multi-line telephone systems (MLTS). In the context of this section, lifeline calls are 911 calls serviced by the North American public switched telephone network (PSTN).

When planning an MLTS deployment, first establish all of the physical locations where phone services are needed. The locations can be classified as follows:

- Single building deployments, where all users are located in the same building.
- Single campus deployments, where the users are located in a group of buildings situated in close proximity.
- Multisite deployments, where users are distributed over a wide geographical area and linked to the telephony call processing site via WAN connectivity.

The locations, or type of deployment, affect the criteria used to design and implement 911 services. The following sections describe the key criteria, along with typical and exceptional situations for each. When analyzing and applying these criteria, consider how they are affected by the phone locations in your network.

Public Safety Answering Point (PSAP)

The public safety answering point (PSAP) is the party responsible for answering the 911 call and arranging the appropriate emergency response, such as sending police, fire, or ambulance teams. The physical location of the phone making the 911 call is the primary factor in determining the appropriate PSAP for answering that call. Generally, each building is serviced by one local PSAP.

To determine the responsible PSAP for a given location, contact a local public safety information service such as the local fire marshal or police department. Also, the phone directory of the local exchange carrier usually lists the agency responsible for servicing 911 calls in a given area.

Typical Situation

- For a given street address, there is only one designated PSAP.
- For a given street address, all 911 calls are routed to the same PSAP.

Exceptional Situation

- The physical size of the campus puts some of the buildings in different PSAP jurisdictions.
- Some of the 911 calls need to be routed to an on-net location (campus security, building security).

911 Network Service Provider

After identifying the responsible PSAPs, you must also identify the 911 network service providers to which each PSAP is connected. It is commonly assumed that PSAPs receive 911 phone calls from the PSTN, but that is not the case. Instead, 911 calls are carried over dedicated, regionally significant networks, and each PSAP is connected to one or more such regional networks. In the majority of cases, the incumbent Local Exchange Carrier (LEC) is the 911 network service provider for a PSAP. Some exceptions include military installations, university campuses, federal or state parks, or other locations where the public safety responsibility falls outside the jurisdiction of the local authorities and/or where a private network is operated by an entity other than a public local exchange carrier.

If you are in doubt about the 911 network service provider for a given PSAP, contact the PSAP directly to verify the information.

Typical Situation

- For a given street address, the 911 network service provider is the incumbent Local Exchange Carrier (LEC). For a location served by Phone Company X, the corresponding PSAP is also served by Phone Company X.
- All 911 calls are routed directly to an off-net location, or all 911 calls are routed directly to an on-net location.

Exceptional Situation

- The local exchange carrier (LEC) through which the MLTS interfaces to the PSTN is *not* the same LEC that serves as 911 network service provider to the PSAP. (For example, the phone system is served by Phone Company X, but the PSAP is connected to Phone Company Y.) This situation might require either a special arrangement between the LECs or special, dedicated trunks between the phone system and the PSAP's 911 network service provider.
- Some LECs may not accept 911 calls on their networks. If this is the case, the only two options are to change LECs or to establish trunks (dedicated to 911 call routing) connected to a LEC that can route 911 calls to the appropriate PSAPs.
- Some (or all) of the 911 calls have to be routed to an on-net location such as campus security or building security. This situation can easily be accommodated during the design and implementation phases, but only if the destination of 911 calls for each phone has been properly planned and documented.

Interface Points into the Appropriate 911 Networks

For larger telephony systems, 911 connectivity might require many interface points. Typically, more than one E911 selective router is used within a LEC's territory, and these routers usually are *not* interconnected.

For example, an enterprise with a large campus could have the following situation:

- Building A located in San Francisco
- Building B located in San Jose
- San Francisco Police Department and San Jose Police Department are the appropriate PSAPs
- San Francisco Police Department and San Jose Police Department are served by the same 911 network service provider
- However, San Francisco Police Department and San Jose Police Department are served by different E911 selective routers operated by that same 911 network service provider!

This type of situation would require two separate interface points, one per E911 selective router. The information pertaining to the E911 selective router territories is generally kept by the incumbent LEC, and the local account representative for that LEC should be able to provide an enterprise customer with the pertinent information. Many LECs also provide the services of 911 subject matter experts who can consult with their own account representatives on the proper mapping of 911 access services.

Typical Situation

- For single-site deployments or campus deployments, there is usually only one PSAP for 911 calls.

- If access to only one PSAP is required, then only one interface point is required. Even if access to more than one PSAP is required, they might be reachable from the same E911 selective router, through the same centralized interface. If the enterprise's branch sites are linked via a WAN (centralized call processing), it is desirable to give each location its own local (that is, located inside each branch office) access to 911 to prevent 911 isolation during WAN failure conditions where Survivable Remote Site Telephony (SRST) operation is activated.

Exceptional Situation

- The physical size of the campus puts some of the buildings in different PSAP jurisdictions, *and*
- Some of the 911 calls have to be routed to different E911 selective routers, through different interface points.

Note Some of the information required to establish the geographical territories of PSAPs and E911 selective routers is available online or from various competitive local exchange carrier (CLEC) information web sites. (For example, https://clec.att.com/clec/hb/shell.cfm?section=782 provides some valuable data about the territory covered by AT&T in California and Nevada.) However, Cisco strongly recommends that you obtain proper confirmation of the appropriate interface points from the LEC prior to the design and implementation phases of 911 call routing.

Interface Type

In addition to providing voice communications, the interfaces used to present 911 calls to the network must also provide identification data about the calling party.

Automatic Number Identification (ANI) refers to the E.164 number of the calling party, which is used by networks to route a 911 call to the proper destination. This number is also used by the PSAP to look up the Automatic Location Identification (ALI) associated with a call.

911 calls are source-routed, which means that they are routed according to the calling number. Even though different locations are all dialing the same number (911), they will reach different PSAPs based on their location of origin, which is represented by the ANI (calling number).

You can implement 911 call functionality with either of the following interface types:

- Dynamic ANI assignment
- Static ANI assignment

While dynamic ANI assignment scales better (because it supports multiple ANIs) and lends itself to all but the smallest of applications, static ANI assignment can be used in a wider variety of environments, from the smallest to the largest systems.

Dynamic ANI (Trunk Connection)

The dynamic aspect of ANI refers to the fact that a system has many phones sharing access to the 911 network across the same interface, and the ANI transmitted to the network might need to be different for each call.

There are two main types of dynamic ANI interfaces:

- Integrated Services Digital Network Primary Rate Interface (ISDN-PRI, or simply PRI)
- Centralized Automatic Message Accounting (CAMA).

PRI

This type of interface usually connects a telephony system to a PSTN Class 5 switch. The calling party number (CPN) is used at call setup time to identify the E.164 number of the calling party.

Most LECs treat the CPN differently when a call is made to 911. Depending upon the functionality available in the Class 5 switch and/or upon LEC or government policy, the CPN may not be used as the ANI for 911 call routing. Instead, the network may be programmed to use the listed directory number (LDN) or the bill-to number (BTN) for ANI purposes.

If the CPN is not used for ANI, then 911 calls coming from a PRI interface all look the same to the 911 network because they all have the same ANI, and they are all routed to the same destination (which might not be the appropriate one).

Some LECs offer a feature to provide CPN transparency through a PRI interface for 911 calls. With this feature, the CPN presented to the Class 5 switch at call setup is used as ANI to route the call. The feature name for this functionality varies, depending on the LEC. (For example, SBC calls it Inform 911 in California.)

Note The CPN *must* be a routable E.164 number, which means that the CPN must be entered in the routing database of the associated E911 selective router.

Note For Direct Inward Dial (DID) phones, the DID number could be used as the ANI for 911 purposes, but only if it is properly associated with an Emergency Service Number in the 911 service provider's network. For non-DID phones, use another number. (See Emergency Location Identification Number Mapping, page 11-7, for more information.)

Many Class 5 switches are connected to E911 selective routers through trunks that do not support more than one area code. In such cases, if PRI is used to carry 911 calls, then the only 911 calls that will be routed properly are those whose CPN (or ANI) have the same Numbering Plan Area (NPA) as the Class 5 switch.

Example

An MLTS is connected to a Class 5 switch in area code 514 (NPA = 514). If the MLTS were to send a 911 call on the PRI trunk, with a CPN of **450**.555.1212, the Class 5 switch would send the call to the E911 selective router with an ANI of **514**.555.1212 (instead of the correct **450**.555.1212), yielding inappropriate routing and ALI lookup.

To use PRI properly as a 911 interface, the system planner must ensure that the CPN will be used for ANI and must properly identify the range of numbers (in the format NPA NXX TNTN) acceptable on the link. For example, if a PRI link is defined to accept ANI numbers within the range 514 XXX XXXX, then only calls that have a Calling Party Number with NPA = 514 will be routed appropriately.

CAMA

Centralized Automatic Message Accounting (CAMA) trunks also allow the MLTS to send calls to the 911 network, with the following differences from the PRI approach:

- CAMA trunks are connected directly into the E911 selective router. Extra mileage charges may apply to cover the distance between the E911 selective router and the MLTS gateway point.
- CAMA trunks support 911 calls only. The capital and operational expenses associated with the installation and operation of CAMA trunks support 911 traffic only.

- CAMA trunks for the MLTS market may be limited to a fixed area code, and the area code is typically implied (that is, not explicitly sent) in the link protocol. The connection assumes that all calls share the same deterministic area code, therefore only 7 or 8 digits are sent as ANI.

Note Cisco supports CAMA-based 911 functionality through the VIC-2CAMA, VIC-2FXO, and VIC-4FXO trunk cards.

Static ANI (Line Connection)

Static ANI provides a line (rather than a trunk) connection to the PSTN, and the ANI of the line is associated with all 911 calls made on that line, regardless to the CPN of the calling phone. A plain old telephone service (POTS) line is used for this purpose.

POTS lines are one of the simplest and most widely supported PSTN interfaces. A POTS line usually comes fully configured to accept 911 calls. In addition, the existing E911 infrastructure supports 911 calls from POTS lines very well.

The POTS approach has the following attributes:

- The operational costs associated with a POTS line are low.
- The POTS line can even serve as a backup line in case of power failure.
- The POTS line number can be used as the callback number entered into the ALI database.
- POTS lines represent the lowest cost 911 support for locations where user density does not justify local PRI or CAMA access into the PSTN.
- POTS lines are ubiquitous in PSTN installations.

All outgoing 911 calls through this type of interface are treated the same by the E911 network, and the tools that enable Cisco Unified Communications Manager to control the ANI presented to the E911 network (such as calling party transformation masks) are irrelevant because the ANI can be only the POTS line's number.

Emergency Response Location Mapping

The National Emergency Number Association (NENA) has recently proposed model legislation to be used by state and federal agencies in enacting the rules that govern 911 in enterprise telephony systems. One of the concepts in the NENA proposal is that of the emergency response location (ERL), which is defined as:

> *A location to which a 911 emergency response team may be dispatched. The location should be specific enough to provide a reasonable opportunity for the emergency response team to quickly locate a caller anywhere within it.*

Rather than having to identify each phone's location individually, the requirement allows for the grouping of phones into a "zone," the ERL. The maximum size of the ERL may vary, depending upon local implementation of the legislation, but we will use 7000 square feet (sq ft) as a basis for discussion in this section. (The concepts discussed here are independent of the maximum ERL size that may be allowed in any given state or region.)

An emergency location identification number (ELIN) is associated with each ERL. The ELIN is a fully qualified E.164 number, used to route the call within the E911 network. The ELIN is sent to the E911 network for any 911 call originating from the associated ERL. This process allows more than one phone to be associated with the same fully qualified E.164 number for 911 purposes, and it can be applied to DID and non-DID phones alike.

Note This document does not attempt to present the actual requirements of any legislation. Rather, the information and examples presented here are for the purposes of discussion only. The system planner is responsible for verifying the applicable local requirements.

For example, assume a building has a surface area of 70,000 sq ft and 100 phones. In planning for 911 functionality, the building can be divided into 10 zones (ERLs) of 7000 sq ft each, and each phone can be associated with the ERL where it is located. When a 911 call is made, the ERL (which could be the same for multiple phones) is identified by sending the associated ELIN to the PSAP. If the phones were evenly distributed in this example, each group of 10 phones would have the same ERL and, therefore, the same ELIN.

The various legislations define a minimum number of phones (for example, 49) and a minimum surface area (for example, 40,000 sq ft) below which the requirements for MLTS 911 are not applicable. But even if the legislation does not require 911 functionality for a given enterprise, it is always best practice to provision for it.

Emergency Location Identification Number Mapping

In general, you must associate a single fully qualified E.164 number, known as the emergency location identification number (ELIN), with each ERL. (However, if using Cisco Emergency Responder, you can configure more than one ELIN per ERL.) The ELIN is used to route the call across the E911 infrastructure and is used by the PSAP as the index into the ALI database.

ELINs must meet the following requirements:

- They must be routable across the E911 infrastructure. (See the examples in the section on Interface Type, page 11-4.) If an ELIN is not routable, 911 calls from the associated ERL will, at best, be handled according to the default routing programmed in the E911 selective router.
- Once the ERL-to-ELIN mapping of an enterprise is defined, the corresponding ALI records must be established with the LEC so that the ANI and ALI database records serving the PSAP can be updated accurately.

The ELIN mapping process can be one of the following, depending on the type of interface to the E911 infrastructure for a given ERL:

- Dynamic ANI interface

  With this type of interface, the calling party number identification passed to the network is controlled by the MLTS. The telephony routing table of the MLTS is responsible for associating the correct ELIN with the call, based on the calling phone's ERL. Within Cisco Unified Communications Manager, the calling party number can be modified by using transformation masks for calls made to 911. For example, all phones located in a given ERL can share the same calling search space that lists a partition containing a translation pattern (911) and a calling party transformation mask that would replace the phone's CPN with the ELIN for that location.

- Static ANI interface

  With this type of interface, the calling party number identification passed to the network is controlled by the PSTN. This is the case if the interface is a POTS line. The ELIN is the phone number of the POTS line, and no further manipulation of the phone's calling party identification number is possible.

PSAP Callback

The PSAP might have to reach the caller after completion of the initial conversation. The PSAP's ability to call back relies on the information that it receives with the original incoming call.

The delivery of this information to the PSAP is a two-part process:

1. The Automatic Number Identification (ANI) is first sent to the PSAP. The ANI is the E.164 number used to route the call. In our context, the ANI received at the PSAP is the ELIN that the MLTS sent.
2. The PSAP then uses the ANI to query a database and retrieve the Automatic Location Identification (ALI). The ALI provides the PSAP attendant with information such as:
   - Caller's name
   - Address
   - Applicable public safety agency
   - Other optional information, which could include callback information. For example, the phone number of the enterprise's security service could be listed, to aid in the coordination of rescue efforts.

Typical Situation

- The ANI information is used for PSAP callback, which assumes that the ELINs are dialable numbers.
- The ELINs are PSTN numbers associated with the MLTS. If someone calls the ELIN from the PSTN, the call will terminate on an interface controlled by the MLTS.
- It is the responsibility of the MLTS system administrator to program the call routing so that calls made to any ELIN in the system will ring a phone (or multiple phones) in the immediate vicinity of the associated ERL.
- Once the ERL-to-ELIN mapping is established, it needs be modified only when there are changes to the physical situation of the enterprise. If phones are simply added, moved, or deleted from the system, the ERL-to-ELIN mapping and its associated ANI/ALI database records need not be changed.

Exceptional Situation

- Callback to the immediate vicinity of the originating ERL may be combined with (or even superseded by) routing the callback to an on-site emergency desk, which will assist the PSAP in reaching the original caller and/or provide additional assistance with the emergency situation at hand.
- The situation of the enterprise could change, for example, due to area code splits, city or county service changes requiring a new distribution of the public safety responsibilities, new buildings being added, or any other change that would affect the desired routing of a call for 911 purposes. Any of these evens could require changes in the ERL-to-ELIN mapping and the ANI/ALI database records for the enterprise.

Nomadic Phone Considerations

All discussions in this chapter thus far have relied upon the assumption that the phone locations are static. If, however, phones are moved across ERL boundaries, then 911 calls from the newly relocated phone will not be routed correctly. Because it is now physically located in a different ERL, the phone should use the ELIN of its current ERL. If the configuration is not changed in the Cisco Unified Communications Manager (Unified CM) database, the following events will occur:

- The ELIN of the previous ERL will be used to route calls on the E911 infrastructure.
- The egress point from the IP network to the E911 infrastructure might be incorrect.
- The callback functionality provided to the PSAP might reach the wrong destination.
- The ALI information provided to the PSAP might result in the dispatching of emergency response personnel to the wrong location.
- The location-based call admission control for the phone might not properly account for the WAN bandwidth usage of the phone, yielding possible over-subscription or under-subscription of WAN bandwidth resources.

The only way to remedy this situation is to manually update the phone's configuration (including its calling search space and location information) in Unified CM to reflect its new physical location.

Cisco Emergency Responder

Ease of administration for moves, adds, and changes is one of the key advantages of IP telephony technology. To provide for moves, adds, and changes that automatically update 911 information without user intervention, Cisco has developed a product called the Cisco Emergency Responder (Cisco ER).

Cisco ER provides the following primary functionality:

- Dynamic association of a phone to an ERL, based on the detected physical location of the phone.
- Dynamic association of the ELIN to the calling phone, for callback purposes. In contrast to non-ER scenarios outlined in preceding sections, Cisco ER enables the callback to ring the exact phone that initiated the 911 call.
- On-site notification to designated parties (by pager, web page, or phone call) to inform them that there is an emergency call in progress. The pager and web page notifications include the calling party name and number, the ERL, and the date and time details associated with the call. Phone notification provides the information about the calling number from which the emergency call was placed.

For more information on Cisco ER, refer to the section on Cisco Emergency Responder Considerations, page 11-13, and to the Cisco ER product documentation available online at

http://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html

The key functionality of Cisco ER relies on the detection of the phone's location by discovery of the network port (Layer 2 port, such as a Fast Ethernet switched port) from which the phone made the 911 call. The discovery mechanism relies on two main assumptions:

- The wired infrastructure of the enterprise is well established and does not change sporadically.
- The infrastructure is available for Cisco ER to browse; that is, Cisco ER can establish Simple Network Management Protocol (SNMP) sessions to the underlying network infrastructure and can scan the network ports for the discovery of connected phones.

Once Cisco ER discovers the originating port for the call, it associates the call with the pre-established ERL for the location of that port. This process also yields an association with a pre-established ELIN for the location and the selection of the appropriate egress point to the E911 infrastructure, based on the originating ERL.

With Cisco ER, the ERL-to-ELIN mapping process described in the preceding sections still applies, but with one variation: without Cisco ER, each ERL is associated with only one ELIN, but Cisco ER allows for the use of two or more ELINs per ERL. The purpose of this enhancement is to cover the specific case of more than one 911 call originating from a given ERL within the same general time period, as illustrated by the following examples.

Example 1

- Phone A and phone B are both located within ERL X, and ERL X is associated with ELIN X.
- Phone A makes a 911 call at 13:00 hours. ELIN X is used to route the call to PSAP X, and PSAP X answers and releases the call. Then, at 13:15 hours, phone B makes a 911 call. ELIN X is again used to route the call to PSAP X.
- PSAP X, after releasing the call from phone B, decides to call back phone A for further details pertaining to phone A's original call. The PSAP dials ELIN X, and gets phone B (instead of the desired phone A).

To work around this situation, Cisco ER allows you to define a pool of ELINs for each ERL. This pool provides for the use, in a round-robin fashion, of a distinct ELIN for each successive call. With the definition of two ELINs for ERL X in our example, we now have the situation described in Example 2.

Example 2

- Phone A and phone B are both located within ERL X. ERL X is associated with both ELIN X1 and ELIN X2.
- Phone A makes a 911 call at 13:00 hours. ELIN X1 is used to route the call to PSAP X, and PSAP X answers and releases the call. Then, at 13:15 hours, phone B makes a 911 call, and ELIN X2 is used to route this call to PSAP X.
- PSAP X, after releasing the call from phone B, decides to call back phone A for further details pertaining to phone A's original call. The PSAP dials ELIN X1 and gets phone A.

Of course, if a third 911 call were made but there were only two ELINs for the ERL, the situation would allow for callback functionality to properly reach only the last two callers in the sequence.

Emergency Call String

It is highly desirable to configure a dial plan so that the system easily recognizes emergency calls, whether an access code (for example, 9) is used or not. The emergency string for North America is generally 911. Cisco strongly recommends that you configure the system to recognize both the strings 911 and 9911.

Cisco also strongly recommends that you explicitly mark the emergency route patterns with Urgent Priority so that Unified CM does *not* wait for the inter-digit timeout (Timer T.302) before routing the call.

Other emergency call strings may be supported concurrently on your system. Cisco highly recommends that you provide your telephony system users with training on the selected emergency call strings.

Also, it is highly desirable that users be trained to react appropriately if they dial the emergency string by mistake. In North America, 911 may be dialed in error by users trying to access a long distance number through the use of 9 as an access code. In such a case, the user should remain on the line to

confirm that there is no emergency, and therefore no need to dispatch emergency personnel. Cisco ER's on-site notification capabilities can help in identifying the phone at the origin of such spurious 911 calls by providing detailed accounts of all calls made to 911, including calls made by mistake.

Gateway Considerations

Consider the following factors when selecting the gateways to handle emergency calls for your system:

Gateway Placement

Within the local exchange carrier (LEC) networks, 911 calls are routed over a locally significant infrastructure based on the origin of the call. The serving Class 5 switches are connected either directly to the relevant PSAP for their location or to an E911 selective router, which itself is connected to a group of PSAPs significant for its region.

With Cisco's IP-based enterprise telephony architecture, it is possible to route calls on-net to gateways that are remotely situated. As an example, a phone located in San Francisco could have its calls carried over an IP network to a gateway situated in San Jose, and then sent to the LEC's network.

For 911 calls, it is critical to chose the egress point to the LEC network so that emergency calls are routed to the appropriate local PSAP. In the example above, a 911 call from the San Francisco phone, if routed to a San Jose gateway, could not reach the San Francisco PSAP because the San Jose LEC switch receiving the call does not have a link to the E911 selective router serving the San Francisco PSAP. Furthermore, the San Jose area 911 infrastructure would not be able to route the call based on a San Francisco calling party number.

As a rule of thumb, route 911 calls to a gateway physically co-located with the originating phone. Contact the LEC to explore the possibility of using a common gateway to aggregate the 911 calls from multiple locations. Be aware that, even if the 911 network in a given region lends itself to using a centralized gateway for 911 calls, it might be preferable to rely on gateways co-located with the calling phones to prevent 911 call routing from being impacted during WAN failures.

Gateway Blocking

It is highly desirable to protect 911 calls from "all trunks busy" situations. If a 911 call needs to be connected, it should be allowed to proceed even if other types of calls are blocked due to lack of trunking resources. To provide for such situations, you can dedicate an explicit trunk group just for 911 calls.

It is acceptable to route emergency calls exclusively to an emergency trunk group. Another approach is to send emergency calls to the same trunk group as the regular PSTN calls (if the interface permits it), with an alternative path to a dedicated emergency trunk group. This latter approach allows for the most flexibility.

As an example, we can point emergency calls to a PRI trunk group, with an alternate path (reserved exclusively for emergency calls) to POTS lines for overflow conditions. If we put 2 POTS lines in the alternate trunk group, we are guarantying that a minimum of two simultaneous 911 calls can be routed in addition to any calls that were allowed in the main trunk group.

If the preferred gateway becomes unavailable, it may be acceptable to overflow emergency calls to an alternate number so that an alternate gateway is used. For example, in North America calls dialed as 911 could overflow to an E.164 (non-911) local emergency number. This approach does not take advantage of the North American 911 network infrastructure (that is, there is no selective routing, ANI, or ALI services), and it should be used only if it is acceptable to the applicable public safety authorities and only as a last resort to avoid blocking the emergency call due to a lack of network resources.

Answer Supervision

Under normal conditions, calls made to an emergency number should return answer supervision upon connection to the PSAP. The answer supervision may, as with any other call, trigger the full-duplex audio connection between the on-net caller and the egress interface to the LEC's network.

With some North American LECs, answer supervision might not be returned when a "free" call is placed. This may be the case for some toll-free numbers (for example, 800 numbers). In exceptional situations, because emergency calls are considered "free" calls, answer supervision might not be returned upon connection to the PSAP. You can detect this situation simply by making a 911 test call. Upon connection to the PSAP, if audio is present, the call timer should record the duration of the ongoing call; if the call timer is absent, it is very likely that answer supervision was not returned. If answer supervision is not returned, Cisco highly recommends that you contact the LEC and report this situation because it is most likely not the desired functionality.

If this situation cannot be rectified by the Local Exchange Carrier, it would be advisable to configure the egress gateway *not* to require answer supervision when calls are placed to the LEC's network, and to cut through the audio in both directions so that progress indicator tones, intercept messages, and communications with the PSAP are possible even if answer supervision is not returned.

By default, Cisco IOS-based H.323 gateways must receive answer supervision in order to connect audio in both directions. To forego the need for answer supervision on these gateways, use the following commands:

- **progress_ind alert enable 8**

  This command provides the equivalent of receiving a progress indicator value of 8 (in-band information now available) when alerting is received. This command allows the POTS side of the gateway to connect audio toward the origin of the call.

- **voice rtp send-recv**

  This command allows audio cut-through in both the backward and forward directions before a Connect message is received from the destination switch. This command affects all Voice over IP (VoIP) calls when it is enabled.

Be advised that, in situations where answer supervision is not provided, the call detail records (CDRs) will not accurately reflect the connect time or duration of 911 calls. This inaccuracy can impede the ability of a call reporting system to document the relevant statistics properly for 911 calls.

In all cases, Cisco highly recommends that you test 911 call functionality from all call paths and verify that answer supervision is returned upon connection to the PSAP.

Cisco Emergency Responder Considerations

Device mobility brings about special design considerations for emergency calls. Cisco Emergency Responder (Cisco ER) can be used to track device mobility and to adapt the system's routing of emergency calls based on a device's dynamic physical location.

Emergency Responder Version Compatibility with Unified CM

Emergency Responder 1.3(1) is required for compatibility with Cisco Unified CM 5.0. For a full description of the compatibility between Emergency Responder and Unified CM software versions, refer to the *Cisco Emergency Responder Administration Guide 1.3(1)*, available at

http://www.cisco.com

Device Mobility Across Call Admission Control Locations

In a centralized call processing deployment, Cisco ER cannot fully support device movement across call admission control locations because Unified CM does not know about device movements. For example, if you physically move a phone from Branch A to Branch B but the phone's call admission control location remains the same (for example, Location_A), then it is possible that calls made to 911 from that phone would be blocked due to call admission control denial if all available bandwidth to Location_A is in use for other calls. This call blocking occurs even if the phone, now in location B, is physically co-located with the gateway used to connect to the PSAP for location B.

For the same reasons, Cisco ER cannot support device movement across gatekeeper-controlled call admission control zones. However, Cisco ER can fully support device movements within a call admission control location.

In centralized call processing deployments, Cisco ER automatically supports device movement within branches. However, if a device is moved between branches, manual intervention is required to adapt the device's location and region parameters before Cisco ER can fully support 911 calls.

Default Emergency Response Location

If Cisco ER cannot directly determine the physical location of a phone, it assigns a default emergency response location (ERL) to the call. The default ERL points all such calls to a specific PSAP. Although there is no universal recommendation as to where calls should be sent when this situation occurs, it is usually desirable to choose a PSAP that is centrally located and that offers the largest public safety jurisdiction. It is also advisable to populate the ALI records of the default ERL's emergency location identification numbers (ELINs) with contact information for the enterprise's emergency numbers and to offer information about the uncertainty of the caller's location. In addition, it is advisable to mark those ALI records with a note that a default routing of the emergency call has occurred.

Soft Clients

In cases where soft clients such as Cisco IP Communicator are used within the enterprise, Cisco ER can provide device mobility support. However, if the soft client is used outside the boundaries of the enterprise (for example, VPN access from a home office or hotel), Cisco ER will not be able to determine the location of the caller. Furthermore, it is unlikely that the Cisco system would have a gateway properly situated to allow sending the call to the appropriate PSAP for the caller's location.

It is a matter of enterprise policy to allow or not to allow the use of soft clients for 911 calls. It is highly advisable to disallow 911 calls by policy for soft clients that can roam across the internet. Nevertheless, if such a user were to call 911, the best-effort system response would be to route the call to either an on-site security force or a large PSAP close to the system's main site.

The following paragraph is an example notice that you could issue to users to warn them that emergency call functionality is not guaranteed to soft client users:

> *Emergency calls should be placed from phones that are located at the site for which they are configured (for example, your office). A local safety authority might not answer an emergency call placed from a phone that has been removed from its configured site. If you must use this phone for emergency calls while away from your configured site, be prepared to provide the answering public safety authority with specific information regarding your location. Use a phone that is locally configured to the site (for example, your hotel phone or your home phone) for emergency calls when traveling or telecommuting.*

Test Calls

For any enterprise telephony system, it is a good idea to test 911 call functionality, not only after the initial installation, but regularly, as a preventive measure.

The following suggestions can help you carry out the testing:

- Contact the PSAP to ask for permission before doing any tests, and provide them with the contact information of the individuals making the tests.
- During each call, indicate that it is *not* an actual emergency, just a test.
- Confirm the ANI and ALI that the call taker has on their screen.
- Confirm the PSAP to which the call was routed.
- Confirm that answer supervision was received by looking at the call duration timer on the IP phone. An active call timer is an indication that answer supervision is working properly.

PSAP Callback to Shared Directory Numbers

Cisco ER handles the routing of inbound calls made to emergency location identification numbers (ELINs). In cases where the line from which a 911 call was made is a shared directory number, the PSAP callback will cause all shared directory number appearances to ring. Any of the shared appearances can then answer the call, which means that it may not be the phone from which the 911 call originated.

Multi-Cluster Considerations

Enterprise telephony systems based on multiple Unified CM clusters can benefit from the functionality of Cisco Emergency Responder (Cisco ER).

The *Cisco Emergency Responder Administration Guide* provides detailed descriptions of the terms used herein, as well as the background information required to support the following discussion. Of specific interest is the chapter on *Planning for Cisco Emergency Responder*. This documentation is available at

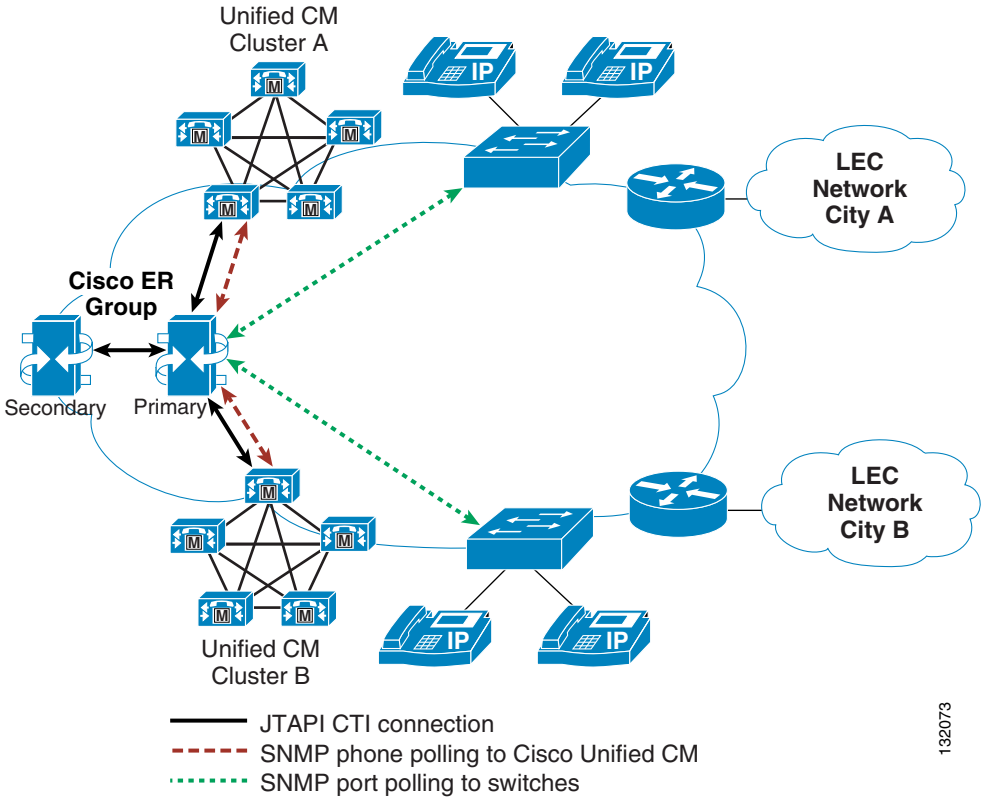
http://www.cisco.com

Single Cisco ER Group

A single Emergency Responder group can be deployed to handle emergency calls from two or more Unified CM clusters. The design goal is to ensure that any phone's emergency call is routed to the Cisco ER group, which will assign an ELIN and route the call to the appropriate gateway based on the phone's location.

One advantage of using a single Cisco ER group is that all ERLs and ELINs are configured into a single system. A phone registered on any cluster will be located by the single Cisco ER group because that group is responsible for polling all of the system's access switches. Figure 11-1 illustrates a single Cisco ER group interfaced with two Unified CM clusters.

Figure 11-1 A Single Cisco ER Group Connected to Two Unified CM Clusters



The single Cisco ER group in Figure 11-1 interfaces with the following components:

- Each Unified CM cluster via SNMP, to collect information about their respective configured phones
- All of the enterprise's switches via SNMP, so that any cluster's phone, connected to any switch, can be located. This connection is not required if the phone locations are being identified based on IP subnets. For details on configuring IP subnet-based ERLs, refer to the chapter on Configuring Cisco Emergency Responder in the *Cisco Emergency Responder Administration Guide*, available at

  http://www.cisco.com
- Each Unified CM cluster via JTAPI, to allow for the call processing required by any phone that dials 911 – for example, identification of the calling phone's ERL, assignment of the ELIN, redirection of the call to the proper gateway (based on the calling phone's location), and the handling of the PSAP callback functionality

The version of the JTAPI interface used by Cisco Emergency Responder is determined by the version of the Unified CM software to which it is connected. At system initialization, Cisco ER interrogates the Unified CM cluster and loads the appropriate JTAPI Telephony Service Provider (TSP). Because there can be only one version of JTAPI TSP on the Cisco ER server, all Unified CM clusters to which a single Cisco ER group is interfaced *must* run the same version of Unified CM software.

For some deployments, this software version requirement might present some difficulties. For instance, during a Unified CM upgrade, different clusters will be running different versions of software, and some of the clusters will be running a version of JTAPI that is not compatible with the version running on the Cisco ER servers. When this situation occurs, emergency calls from the cluster running a version of JTAPI different than that of the Cisco ER group might receive the call treatment provided by the Call Forward Busy settings of the emergency number's CTI Route Point.

When considering if a single Cisco ER group is appropriate for multiple Unified CM clusters, apply the following guidelines:

- Make Unified CM upgrades during an acceptable maintenance window when emergency call volumes are as low as possible (for example, after hours, when system use is at a minimum).
- Use a single Cisco ER group only if the quantity and size of the clusters allow for minimizing the amount of time when dissimilar versions of JTAPI are in use during software upgrades.

For example, a deployment with one large eight-server cluster in parallel with a small two-server cluster could be considered for use with a single Cisco ER group. In this case, it would be best to upgrade the large cluster first, thus minimizing the number of users (those served by the small cluster) that might be without Cisco ER service during the maintenance window of the upgrade. Furthermore, the small cluster's users can more appropriately be served by the temporary static routing of emergency calls in effect while Cisco ER is not reachable because they can be identified by the single ERL/ELIN assigned to all non-ER calls made during that time.

Note Emergency Responder version 1.3(1) is required if any of the Unified CM clusters are running Cisco Unified CM Release 4.2 or 5.0.

Multiple Cisco ER Groups

Multiple Cisco ER groups can also be deployed to support multi-cluster systems. In this case, each ER group interfaces with the following components:

- A Unified CM cluster via the following methods:
  - SNMP, to collect information about its configured phones
  - JTAPI, to allow for the call processing associated with redirection of the call to the proper gateway or, in the case of roaming phones, the proper Unified CM cluster
- The access switches (via SNMP) to which most of the phones associated with the Unified CM of the Cisco ER group are most likely to be connected

This approach allows Unified CM clusters to run different versions of software because each is interfaced to a separate Cisco ER group.

To allow phones to roam between various parts of the network and still be tracked by Cisco ER, you might have to configure the Cisco ER groups into a Cisco ER cluster. For details on Cisco ER clusters and groups, refer to the chapter on *Planning for Cisco Emergency Responder* in the *Cisco Emergency Responder Administration Guide*, available at

http://www.cisco.com

Figure 11-2 presents a sample topology illustrating some of the basic concepts behind Cisco ER clustering.

Figure 11-2 Multiple Cisco ER Groups

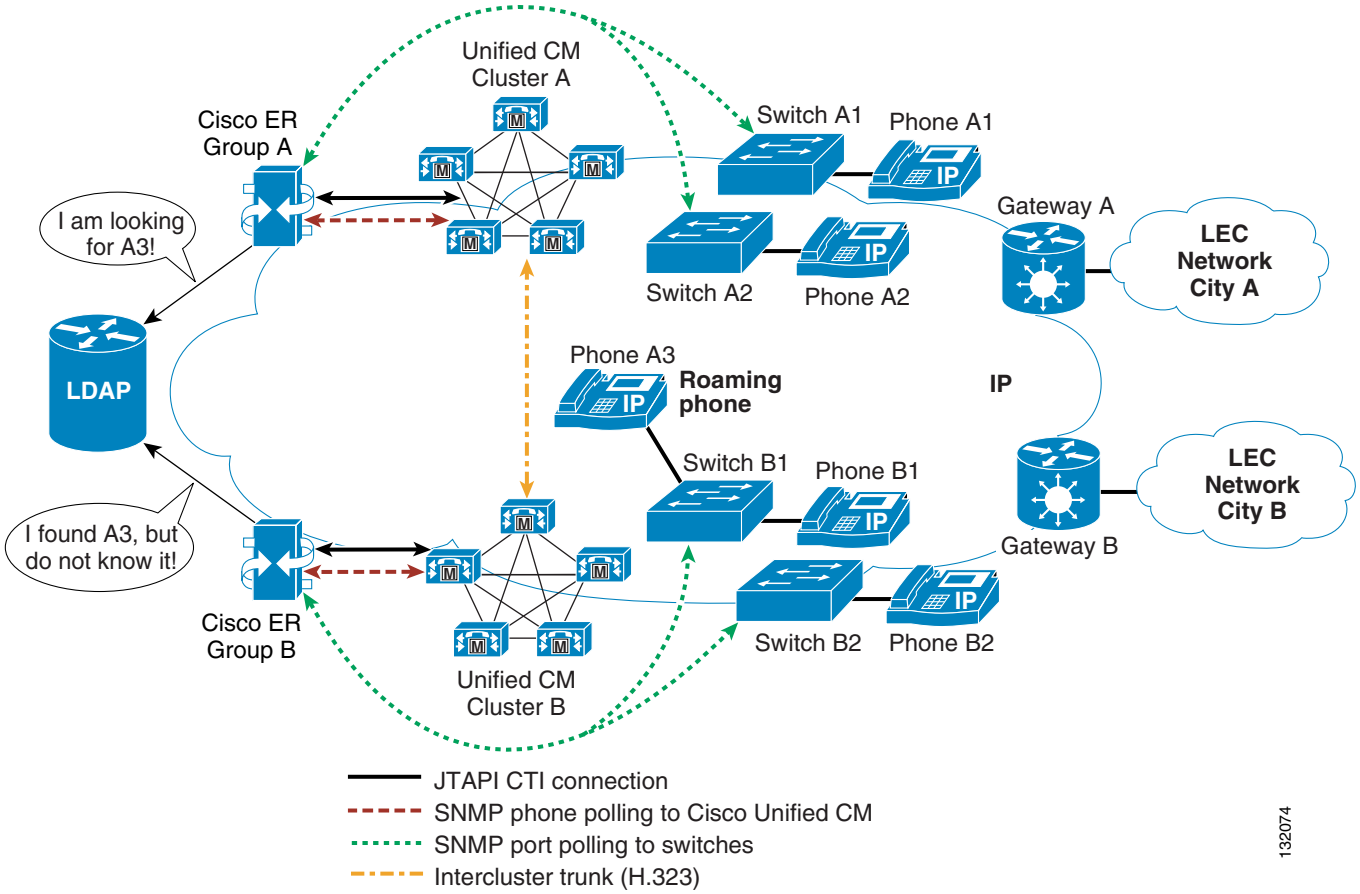


Figure 11-2 illustrates the following topology:

- Cisco ER group A is interfaced to Unified CM cluster A to access switches A1 and A2, and it is deemed to be the home Cisco ER group of all phones registered to Unified CM cluster A.
- Likewise, Cisco ER group B is interfaced to Unified CM cluster B to access switches B1 and B2, and it is deemed to be the home Cisco ER group of all phones registered to Unified CM cluster B.

Note Emergency Responder 1.3(1) requires that all ER groups in an ER cluster run the same version of software. Therefore, if any of the Unified CM clusters are using Cisco Unified CM Release 4.2 or 5.0, then all of the ER groups must use Emergency Responder 1.3(1).

Phone Movements Within the Tracking Domain of a Cisco ER Group

The emergency call processing for phones moving between access switches controlled by the same home Cisco ER group is the same as the processing done for a deployment with a single Unified CM cluster. For example, a phone moving between access switches A1 and A2 remains registered with Unified CM cluster A, and its location is determined by Cisco ER group A both before and after the move. The phone is still under full control of Cisco ER group A, for both the discovery of the phone by Unified CM cluster A and the determination of the phone's location by switch A2. The phone is therefore not considered to be an unlocated phone.

Phone Movements Between the Various Tracking Domains of a Cisco ER Cluster

A Cisco ER cluster is essentially a collection of Cisco ER groups that share location information through a Lightweight Directory Access Protocol (LDAP) database. Each group shares the location of any phone it finds on an access switch or in an IP subnet. However, any phone found in the Cisco ER group's own Unified CM cluster is deemed to be *unknown*, and its information is not shared.

Cisco ER groups also share information about phones that cannot be located within a Cisco ER group's tracking domain (in switches or IP subnets) but which are known to be registered in the group's associated Unified CM cluster. Such phones are deemed *unlocated*.

If a phone is roaming between access switches monitored by different Cisco ER groups, those groups must be configured in a Cisco ER cluster so they can exchange information about the phone's location. For example, phone A3 is registered with Unified CM cluster A, but it is connected to an access switch controlled by Cisco ER group B. Cisco ER group A is aware that phone A3 is registered with Unified CM cluster A, but group A cannot locate phone A3 in any of the site A switches. Therefore, phone A3 is deemed *unlocated* by Cisco ER group A.

Cisco ER group B, on the other hand, has detected the presence of phone A3 in one of the switches that it monitors. Because the phone is not registered with Unified CM cluster B, phone A3 is advertised through the Cisco ER LDAP database as an *unknown* phone.

Because the two Cisco ER groups are communicating through an LDAP database, they can determine that Cisco ER group B's *unknown* phone A3 is the same as Cisco ER group A's *unlocated* phone A3.

The Unlocated Phone page in Cisco ER group A will display the phone's host name along with the remote Cisco ER group (in this, case Cisco ER group B).

Emergency Call Routing within a Cisco ER Cluster

Cisco ER clustering also relies on route patterns that allow emergency calls to be redirected between pairs consisting of a Unified CM cluster and a Cisco ER. For more details, refer to the section on *Creating Route Patterns for Inter-Cisco Emergency Responder-Group Communications* in the *Cisco Emergency Responder Administration Guide*, available at

http://www.cisco.com

If phone A3 places an emergency call, the call signaling flow will be as follows:

1. Phone A3 sends the emergency call string to Unified CM cluster A for processing.
2. Unified CM cluster A sends the call to Cisco ER group A for redirection.
3. Cisco ER group A determines that phone A3 is located in Cisco ER group B's tracking domain, so it redirects the call to a route pattern that points to Unified CM cluster B.
4. Unified CM cluster A sends the call to Unified CM cluster B.
5. Unified CM cluster B sends the call to Cisco ER group B for redirection.
6. Cisco ER group B identifies the ERL and ELIN associated with phone A3's location and redirects the call to Unified CM cluster B. The calling number is transformed into the ELIN associated with the ERL of phone A3, and the called number is modified to route the call to the proper gateway.
7. Unified CM cluster B routes the call according to the new called number information obtained from Cisco ER group B.
8. Unified CM cluster B sends the call out the gateway toward the Emergency PSTN network.

Scalability Considerations for Cisco ER Clustering

In a Cisco ER cluster, the quantity of phones roaming outside the tracking domain of their home Cisco ER group is a scalability factor that you must kept within the limits set forth in the section on *Network Hardware and Software Requirements* in the *Cisco Emergency Responder Administration Guide 1.2(3)*, available at:

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

With the Cisco MCS 7845 server platform and version 1.2(3) of the Cisco ER software, a Cisco ER cluster can support a maximum of 3000 roaming phones. For deployments that have to exceed this limit (for instance, large campus deployments with multiple Unified CM clusters), phone movement can be tracked by IP subnets. By defining the IP subnets in each of the Cisco ER groups and by assigning each ERL with one ELIN per Cisco ER group, you can virtually eliminate roaming phones because all phones in the campus will be part of the tracking domain of their respective Cisco ER group.

ALI Formats

In multi-cluster configurations, there might be instances where the physical locations of ERLs and ELINs defined in a single Cisco ER group span the territory of more than one phone company. This condition can lead to situations where records destined for different phone companies have to be extracted from a common file that contains records for multiple LECs.

Cisco ER exports this information in ALI records that conform to National Emergency Number Association (NENA) 2.0, 2.1, and 3.0 formats. However, many service providers do not use NENA standards. In such cases, you can use the ALI Formatting Tool (AFT) to modify the ALI records generated by Cisco ER so that they conform to the formats specified by your service provider. That service provider can then use the reformatted file to update their ALI database.

The ALI Formatting Tool (AFT) enables you to perform the following functions:

- Select a record and update the values of the ALI fields. AFT allows you to edit the ALI fields to customize them to meet the requirements of various service providers. You service provider can then read the reformatted ALI files and use them to update their ELIN records.
- Perform bulk updates on multiple ALI records. Using the bulk update feature, you can apply common changes to all the records that you have selected, to one area code, or to one area code and one city code.
- Selectively export ALI records based on area code, city code, or a four-digit directory number. By selecting to export all the ALI records in an area code, for example, you can quickly access all the ELIN records for each service provider, thereby easily supporting multiple service providers.

Given the flexibility of the AFT, a single Cisco ER group can export ALI records in multiple ALI database formats. For a Cisco ER group serving a Unified CM cluster with sites in the territories of two LECs, the basic approach is as follows:

1. Obtain an ALI record file output from Cisco Emergency Responder in standard NENA format. This file contains the records destined for multiple LECs.
2. Make a copy of the original file for each required ALI format (one copy per LEC).
3. Using the AFT of the first LEC (for example, LEC-A), load a copy of the NENA-formatted file and delete the records of all the ELINs associated with the other LECs. The information to delete can usually be identified by NPA (or area code).
4. Save the resulting file in the required ALI format for LEC-A, and name the file accordingly.
5. Repeat steps 3 and 4 for each LEC.

For more information about the ALI formatting tools, refer to the online documentation available at

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

For LECs not listed at this URL, the output from Unified CM can be formatted using standard text file editing tools, such as spreadsheet programs and standard text editors.

CHAPTER 12

Third-Party Voicemail Design

Last revised on: May 22, 2009

This chapter discusses various options for deploying third-party voicemail systems with Cisco Unified Communications Manager (Unified CM).

Note This chapter does not discuss how to size a voicemail system for ports and/or storage. For this type of information, contact your voicemail vendor, who should be better able to discuss the individual requirements of their own system based upon specific traffic patterns.

There are many voicemail vendors, and it is not uncommon for customers to want to continue to use an existing voicemail system when deploying Unified CM. With this requirement in mind, Cisco provides support for the industry standard voicemail protocol known as Simplified Message Desk Interface (SMDI). SMDI is a serial protocol that provides all the necessary call information required for a voicemail system to answer calls appropriately.

An alternative to SMDI for voicemail integration is QSIG, which allows a third-party PBX to connect to Unified CM via a Primary Rate Interface (PRI) T1/E1 trunk. Each method has its own pros and cons, and the method you employ will largely depend on how your voicemail system is integrated to your current PBX.

This section covers the following aspects of integrating third-party voicemail systems with Unified CM:

What's New in This Chapter

Table 12-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 12-1 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:
Digital set emulation (DSE) is no longer supported.	No longer described in this document
The Cisco Analog Interface Module WS-6624 is no longer supported and should be replaced by the Cisco VG224 or VG248 Analog Phone Gateway.	SMDI, page 12-2
The Cisco Digital PBX Adapter (DPA) is no longer supported.	No longer described in this document

SMDI

Unified CM supports use of Simplified Message Desk Interface (SMDI) protocol through either of the following methods:

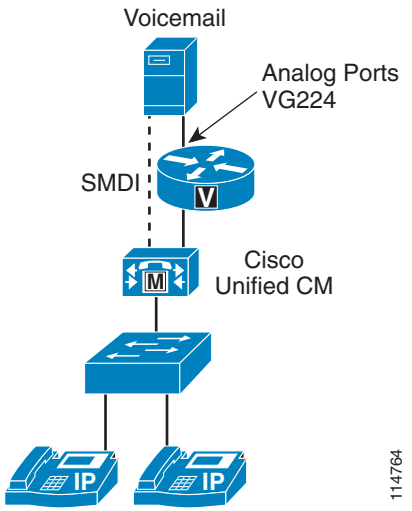
- Cisco Messaging Interface, page 12-2
- Cisco VG248, page 12-4

Cisco Messaging Interface

The Cisco Messaging Interface (CMI) is a Unified CM service that should be run only on the publisher server. This service intercepts calls destined for voicemail and generates appropriate SMDI messages, which are then delivered to one of the server's Component Object Model (COM) ports. The CMI service is compatible with any MGCP gateway that supports analog FXS ports or T1 CAS E&M; however, the VG224 and the gateways based on Cisco Integrated Services Routers (ISR) with Cisco IOS Release 12.4(9)T are the only other gateways that support positive disconnect supervision (see Positive Disconnect Supervision, page 12-9) and are therefore the only gateways currently recommended for use with the CMI service.

Figure 12-1 illustrates the use of SMDI through the CMI service in Unified CM.

Figure 12-1 SMDI via Unified CM



Through the CMI, Unified CM supports integration with virtually any voicemail system that can provide SMDI with analog FXS ports, including (but not limited to) the following:

- Octel 100, 200/300, and 250/350
- Intuity Audix
- Siemens PhoneMail
- Centigram/BayPoint (OnePoint and NuPoint Messenger)
- Lyrix ECS
- IBM Message Center

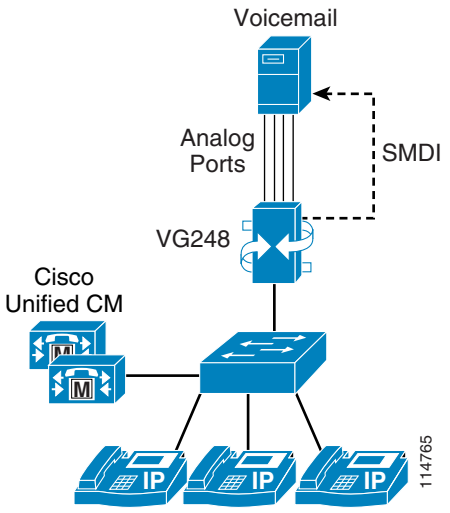
Note Prior to Cisco Unified Communications Manager Release 5.0 (for example, Cisco Unified CallManager 4.*x*), customers could connect directly to the EIA/TIA-232 serial ports located on the rear of the MCS servers in order to connect to the Cisco Messaging Interface; however, these serial interfaces are no longer available with Cisco Unified Communications Manager 5.0 or later releases. In order to connect an EIA/TIA-232 cable to Cisco Unified Communications Manager 5.0 or later releases, use a Cisco certified serial-to-USB adapter with the part number USB-SERIAL-CA=.

Cisco VG248

The Cisco VG248 is an SCCP gateway that supports 48 analog FXS ports and generates SMDI locally (that is, it runs independent of the CMI service). As with the WS-X6624 and VG224 modules, the VG248 also supports positive disconnect supervision.

Figure 12-2 illustrates the use of SMDI with the VG248.

Figure 12-2 SMDI via the VG248



Voicemail integration through the VG248 provides the following features and advantages:

- Multiple SMDI links per Unified CM
- SMDI failover capability
- Independence from the location of the voicemail system

The VG248 is also capable of supporting two other serial protocols that are sometimes used for voicemail integration: NEC Message Center Interface (MCI) and Ericsson MD110 proprietary protocol.

Considerations When Using FXS Ports

If your voicemail system is equipped with analog FXS ports, use the following Cisco gateways to integrate with the voicemail system:

- VG224

  Use this gateway when there is no physical Catalyst 6500 chassis slot available and when automatic failover of the serial port is not deemed necessary.

- VG248

  Use this gateway when full failover is required for the serial port as well as voice ports, when serial protocols other than SMDI are required (such as NEC MCI or Ericsson MD110), or when no Catalyst 6500 chassis slot is available.

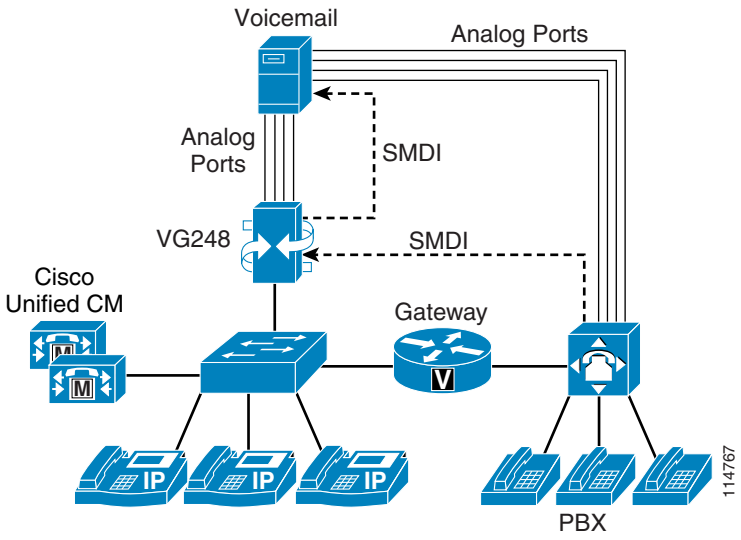
Dual PBX Integration

Dual PBX integration is a useful option for enterprises that want to maintain existing voicemail services while migrating from their current PBX to IP Telephony.

Note Most voicemail vendors do not support this scenario due to its complex nature, but some will provide support on a "site-specific" basis if requested. Consult with your voicemail vendor before attempting to implement this solution.

The Cisco VG248 has inherent multiplexing capabilities that enable it to provide dual integration. The VG248 can combine information from an existing serial link with its own link, and then present a single serial stream to the voicemail system. (See Figure 12-3.)

Figure 12-3 Dual Integration via the VG248 and SMDI



The VG248 works with any voicemail system that has SMDI capability and analog FXS ports. The following prerequisites are required prior to implementation, assuming a dual integration is required:

- Uniform dial plan
- Transfer and reconnect sequences
- Connectivity between the PBX and Unified CM

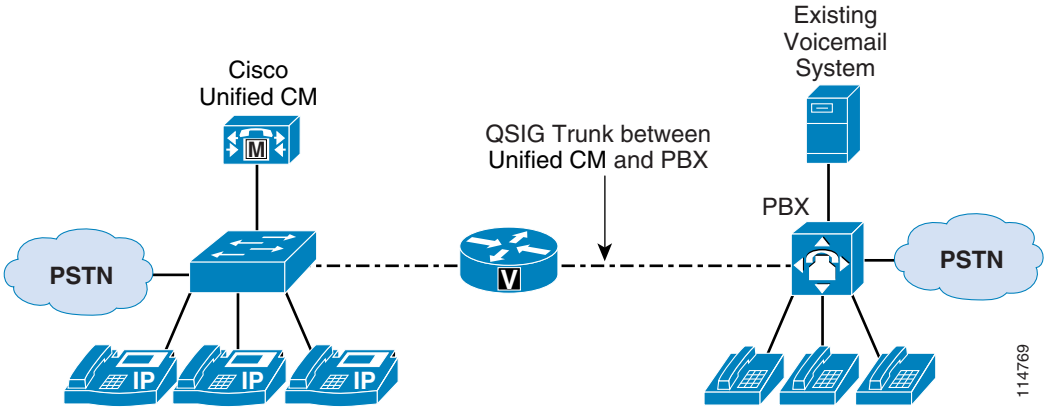
Centralized Voicemail

In a centralized voicemail deployment, two or more PBXs share a single voicemail system. The sharing is achieved by integrating the voicemail system to only one PBX and then utilizing an inter-PBX private networking protocol to extend voicemail services to remote subscribers. The networked PBXs look and act like one large PBX to the voicemail system. Various PBX manufactures have developed proprietary protocols that enable the delivery of such services as well as providing feature transparency to subscribers across a large network (for example, Avaya DCS, Nortel MCDN, Siemens CorNet, Alcatel ABC, NEC CCIS, and Fujitsu FIPN).

The primary motivation for using a centralized voicemail system stems form the desire to offer voicemail services to IP Telephony subscribers from the existing voicemail system so that the subscribers do not have to learn a new telephony user interface (TUI).

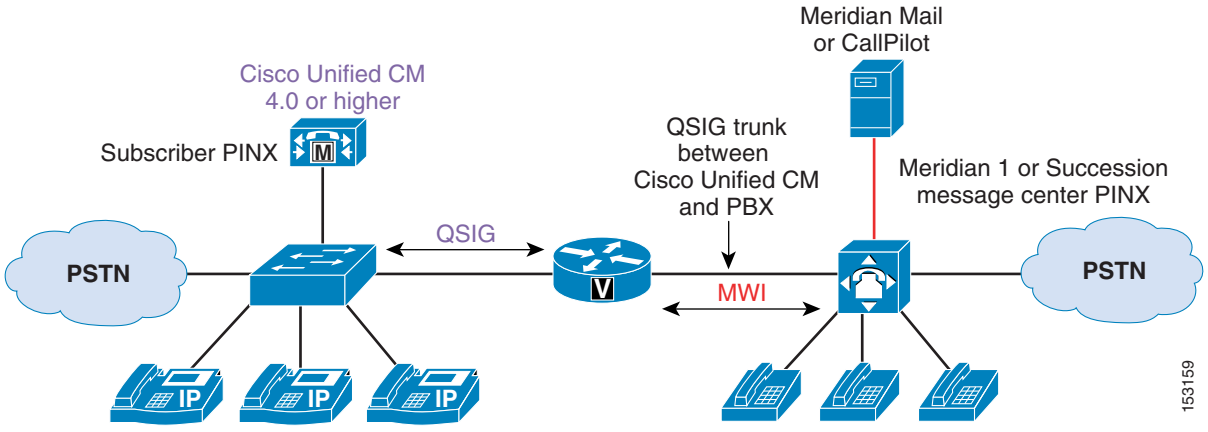
Some voicemail systems are capable of supporting multiple PBXs (dual PBX integration) via protocols such as Simple Messaging Desktop Interface (SMDI) or QSIG PRI. In some circumstances, these solutions are either not possible because the voicemail vendor may choose not to support this configuration, or a dual integration is simply not technically possible because the voicemail system cannot support dissimilar PBX integrations simultaneously. In such circumstances, a centralized voicemail deployment provides an alternative solution to dual integration. (See Figure 12-4.)

Figure 12-4 Centralized Voicemail with Unified CM and QSIG



If you want to use an existing voicemail system, consider the make and model of that system. If the voicemail system in question is from the same manufacturer as the PBX system, then full voicemail functionality is typically available to Unified CM subscribers. See Figure 12-5 for an example of a Nortel system and Figure 12-6 for an Avaya system.

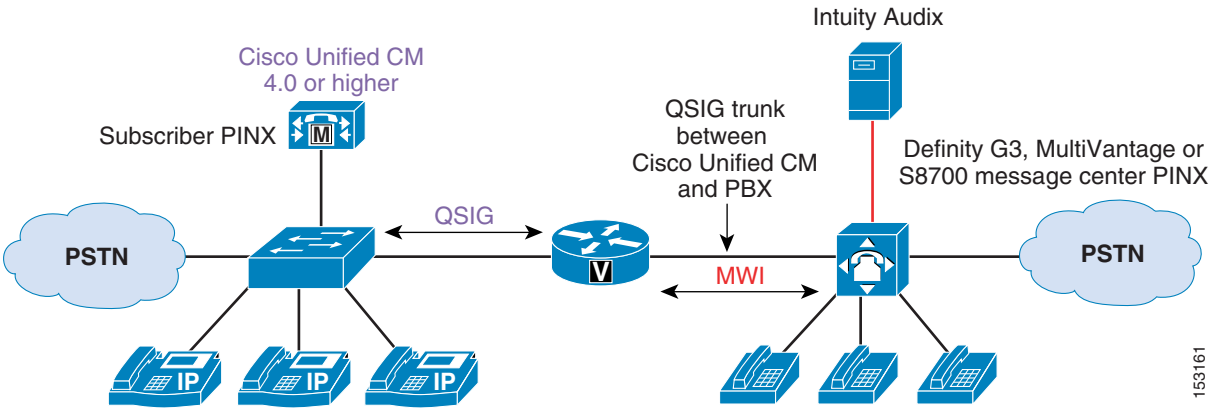
Figure 12-5 Nortel M1 Centralized Voicemail with Meridian Mail or CallPilot



The system in Figure 12-5 has the following characteristics:

- Voicemail services are available to all subscribers.
- Voicemail is hosted on the message center PINX.
- QSIG MWI works only with Meridian Mail or CallPilot.

Figure 12-6 Avaya G3 Centralized Voicemail with Intuity Audix



The system in Figure 12-6 has the following characteristics:

- Voicemail services are available to all subscribers.
- Voicemail is hosted on the message center PINX.
- QSIG MWI works only with Avaya Intuity Audix.

Note that the term *centralized voicemail* does not refer to the voicemail system itself. Centralized voicemail is a function of the PBX's inter-PBX networking protocol (either a proprietary protocol such as Avaya DCS, Nortel MCDN, or Siemens CorNet or a standards-based protocol such as QSIG or DPNSS), which is needed to deliver the voicemail features.

The following important terms and concepts apply to centralized voicemail:

- Message center Private Integrated Services Network Exchange (PINX) — This is the PBX that is "hosting" the voicemail system (the PBX directly connected to the voicemail system).
- Subscriber PINX — This is the PBX that is "remote" from the voicemail system (not directly connected to the voicemail system).

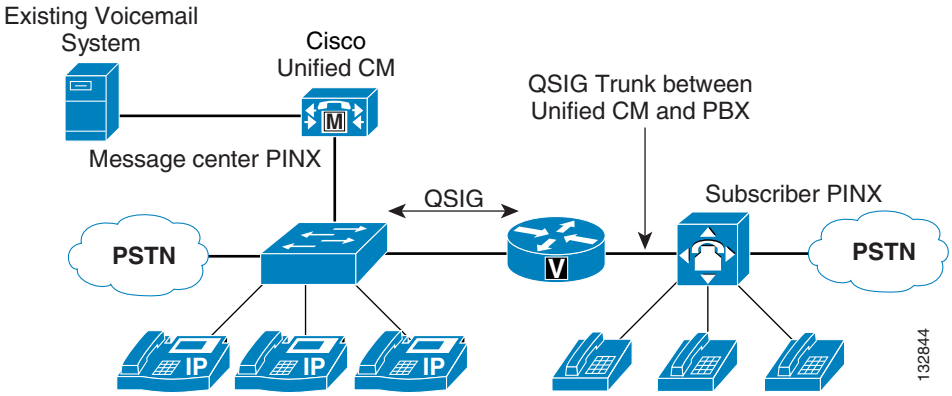
A centralized voicemail configuration requires a suitable inter-PBX networking protocol such as QSIG. This protocol must also deliver the following minimum level of feature support:

- Message Waiting Indication (MWI)
- Transfer — Needed to ensure that the correct calling and called party IDs are delivered to the voicemail system.
- Divert — Needed to ensure that the correct calling and called party IDs are delivered to the voicemail system.

Other features might also be required, depending on how the voicemail system will be used. For example, if the voicemail system is also serving as an automated attendant, then the Path Replacement feature is needed to prevent calls from hair-pinning.

Not all PBXs are capable of serving as the message center PINX. In this case, consider relocating the voicemail system to Unified CM and have Unified CM act as the message center PINX, with the PBX acting as the subscriber PINX. (See Figure 12-7.)

Figure 12-7 Centralized Voicemail with Unified CM Acting as Message Center PINX



Support

Cisco cannot guarantee that another vendor's product will act in a particular manner, nor can Cisco specify what is required in terms of configuration changes or upgrades to another vendor's product. It is the responsibility of the customer to ask these questions and seek confirmation directly from the supplier and/or vendor of each product.

Cisco can assist you in determining which particular questions to ask your supplier and/or vendor, such as: "What do I have to do to my PBX to enable remote PBX users, connected via QSIG, to have a mailbox as well as full access to all voicemail features such as MWI?"

To help with PBX interoperability, Cisco has tested a number of different PBXs with Unified CM and has documented these tests in the form of Application Notes. These documents, while not a guarantee of success, do provide some level of guidance in terms of features supported as well as configuration details for both Unified CM and the PBX. Application Notes for Unified CM have already been written for the leading PBXs, and they cover the scenario of centralized voicemail with Unified CM acting as the message center PINX. The Application Notes are available at

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

Note It is not feasible for Cisco to test other vendors' PBXs acting as the message center PINX. Cisco has neither the facilities nor the expertise to configure these systems, therefore customers must request this information directly from their supplier and/or vendor.

Summary

- Centralized voicemail is a function of the inter-PBX networking protocol, not the voicemail system itself.
- Not all PBXs can act as the message center PINX. Customers *must* confirm this feature with their PBX supplier and/or vendor; Cisco cannot provide or support this feature on the PBX.

- Unified CM can act as the message center PINX, thus providing customers with an alternative if their PBX cannot perform this function.
- Confirm if Path Replacement is needed. Cisco Unified CM Release 4.1 and later supports this feature.

Positive Disconnect Supervision

Positive disconnect supervision is a signal sent from a PBX port to the voicemail system to indicate that the far-end device has gone on-hook. This signal typically takes the form of a drop in loop current for approximately 600 ms, causing the voicemail system to terminate the session.

Without this signal, the voicemail system would be unaware that the far-end device has gone on-hook and would continue to record whatever supervisory tones the PBX provides under this condition. (For example, some PBXs play dial tone while others play busy tone.) The voicemail system would continue to record these tones until the maximum message time has expired. (For example, if the mailbox has a limit of 3 minutes per message and a caller hangs up after 30 seconds, then the voicemail system would continue to record such tones for another 2.5 minutes in the absence of positive disconnect supervision.) This unnecessary recording can be annoying to subscribers and can impact system performance by increasing disk usage as well as causing higher port usage times. Some voicemail systems are able to deal with this scenario by monitoring for known tones and then deleting them, but system performance is still impacted in this case.

A similar issue exists when subscribers call into their mailboxes to check for messages. If a user simply hangs up without disconnect supervision, the voicemail system will stay on the line waiting for a valid response before any activity timers eventually expire. In this scenario, the main impact is from the additional port usage time incurred.

For these reasons, positive disconnect supervision must be provided by the analog ports connecting to the voicemail system.

Summary of Third-Party Voicemail Integration

There are other methods for connecting voicemail systems to Unified CM (such as Microsoft TAPI and PRI ISDN trunks in conjunction with SMDI), but these methods are uncommon. The vast majority of third-party voicemail integrations use the Cisco VG248 or they use the CMI service in conjunction with the VG224, therefore they are the recommended solutions.

Today there are other potential methods of voicemail integration, such as H.323 or SIP. However, due to the varying methods of vendor implementation, features supported, and other factors, these third-party voicemail integrations will have to be evaluated on a per-customer basis. Customers are advised to contact their Cisco Account Team and/or Cisco Partner to discuss these options further.

Note Cisco does not test or certify any third-party voicemail systems. Within the industry, it is generally considered to be the responsibility of the voicemail vendor to test and/or certify their products with various PBX systems. Cisco does, of course, test its interfaces to such equipment and will support these interfaces regardless of which third-party voicemail system is connected.

CHAPTER 13

シスコの音声メッセージング

この章では、Cisco Unified Communications System Release 7.*x* で利用可能な音声メッセージング ソリューションについて説明します。この章では、シスコの音声メッセージング製品である Cisco Unity、Cisco Unity Connection、および Cisco Unity Express を取り上げ、これらの製品を Cisco Unified Communications Manager（Unified CM）と共に配置するための設計ガイドラインとベスト プラクティスを説明します。

（注） 以前のバージョンのソリューション リファレンス ネットワーク デザイン（SRND）のドキュメントでは、この章の情報が、Cisco Unity の章と Cisco Unity Express の章に分かれていました。

このガイドでは、Unified CM に関するメッセージング配置のシナリオが中心ですが、特に、集中型 Unified CM 配置の Survivable Remote Site Telephony（SRST）フォールバック サポートで使用される場合には、適宜、Cisco Unified Communications Manager Express（Unified CME）についても説明します。

この章では、次のトピックについて取り上げます。

この章ではまず、Cisco メッセージング ソリューションのポートフォリオの各製品について簡単に説明した後、企業向け Unified Communications ソリューションにおける各製品の位置付けに関する簡単な概要を示します。次に、メッセージング配置モデルを基盤として、ボイスメール統合を説明します。ここではまず、さまざまなメッセージング配置モデルを定義した後、さまざまな Unified CM コール処理配置モデルにおける各メッセージング配置モデルの位置付けを説明します。この項では、Cisco Unity と Unity Connection を一緒に説明します。Cisco Unity Express については、別に専用の項を設けて、それがサポートする配置モデルを説明します。この項では、数多くのシステムレベルの設計上の考慮事項とベスト プラクティスについて説明します。

次の FAX 統合の項では、サポートされている FAX 統合のタイプについて説明します。この項は、製品のタイプ別に編成されています。最後に、ベスト プラクティスに関する項では、それまでに言及されていないが製品の重要な側面であり、ソリューションにおいて、それぞれのメッセージング製品の配置にあたって考慮すべき一般的なベスト プラクティスと設計ガイドラインを中心に説明します。

これはハイレベルな設計上の議論であり、Unified CM を使用した Unified Communications System に音声メッセージング製品をどのように組み込むかが焦点となることに留意してください。各製品の設計ガイドラインおよびサードパーティ性のメッセージングとテレフォニー システムの相互運用性に関する情報については、http://www.cisco.com で製品別の設計ガイドを参照してください。

この章の新規情報

表 13-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 13-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
Cisco Unity Express のベスト プラクティス	「Cisco Unity Express の配置に関するベスト プラクティス」（P.13-42）
Cisco Unified Messaging Gateway がサポートするモジュール、キャパシティ、ベスト プラクティス	「Cisco Unified Messaging Gateway によるボイスメール ネットワーキング」（P.13-31）
シスコの音声メッセージング ポートフォリオ	「音声メッセージング ポートフォリオ」（P.13-2）
Cisco Unity Express の配置モデルの詳細	「Cisco Unity Express の配置モデル」（P.13-21）
デジタル ネットワーキング	「分散型メッセージングと集中型コール処理」（P.13-10）
拡張メッセージ待機インジケータ（eMWI）	「拡張メッセージ待機インジケータ（eMWI）」（P.13-37）
フェールオーバーの動作と配置	「メッセージングの冗長性」（P.13-17）
FAX 統合	「FAX 配置」（P.13-27）
LDAP 統合	「分散型メッセージングと集中型コール処理」（P.13-10）
Microsoft Exchange の統合	「音声メッセージング ポートフォリオ」（P.13-2）

音声メッセージング ポートフォリオ

Cisco Unified Communications のメッセージング ポートフォリオは、Cisco Unity、Cisco Unity Connection、および Cisco Unity Express の 3 つの主なメッセージング製品で構成されます。それぞれの製品が対応する要件は異なりますが、互いに他の製品と重なり合う機能とスケーラビリティを備えています。Voice Mail Networking を使用することで連携して動作することもできます。また、Cisco Unified Messaging Gateway を利用して、非常にスケーラブルな形でこれを実現することも可能です。これについては、この章で後ほど説明します。

これらの製品を検討する場合、それらに搭載されたメッセージング オプションを理解し、特定の配置要件に適したオプションを判断するためには、製品が該当するメッセージング タイプを考慮することが役立ちます。このようなメッセージング タイプは、次の定義を参考に決定してください。

- *ボイスメール専用*とは、いずれのメッセージング クライアント経由でもボイスメールにアクセスできないテレフォニー ボイスメール統合を指します。
- *統合メッセージング*とは、メッセージング クライアントを介したテレフォニー アクセスおよびボイスメール専用のアクセスを備えたボイスメールを指します。

- *ユニファイド メッセージング*とは、メッセージング クライアントを介したテレフォニー アクセスならびにボイスメール、電子メール、FAX アクセスを備えたボイスメールを指します。

上のメッセージング タイプと定義に基づき、次の 3 つのメッセージング製品のオプションが用意されています。

- Cisco Unity

  このソリューションは、大企業組織のニーズに対応して、強力な音声メッセージング、統合メッセージング、ユニファイド メッセージングのオプションを提供するとともに、Microsoft Exchange（Exchange 2007 を含む）と Lotus Domino に統合します。

- Cisco Unity Connection

  このオプションは、10,000 ユーザ以下の中規模企業用に、統合メッセージング、音声認識、およびコール転送ルールを管理しやすいシステムに組み合わせます。または最大 5 つのシステムをネットワーク接続して、最大 50,000 ユーザの大規模企業をサポートすることも可能です。500 ユーザ以下の組織では、Cisco Unity Connection をシングル サーバ ソリューションとして、Cisco Unified Communications Manager Business Edition で使用することができます。

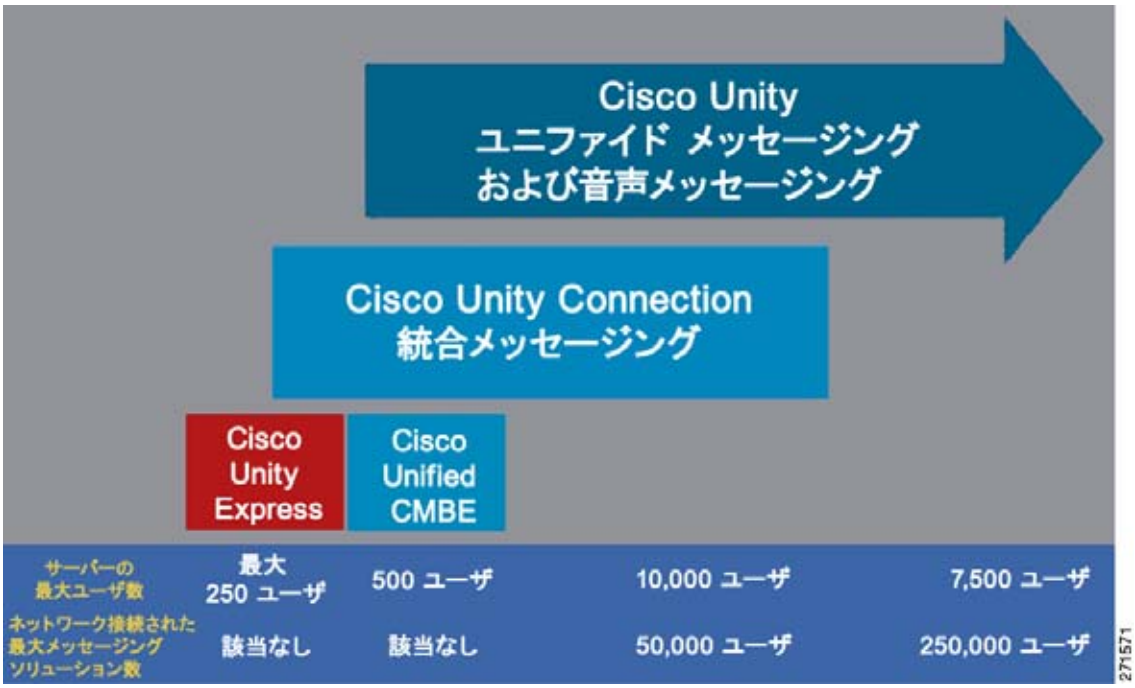
- Cisco Unity Express

  このオプションは、中小規模企業および 250 ユーザ以下の支店用に、特定の Cisco 統合サービス ルータで、コスト効率の高い音声メッセージングおよび統合メッセージング、自動応答、および Iinteractive Voice Response（IVR; 音声自動応答装置）の各機能を提供します。

製品機能の完全な比較については、http://www.cisco.com で「*Cisco Unified Messaging Feature Comparison*」を参照してください。

図 13-1 は、スケーラビリティについての比較を示します。1 行目は、単一のサーバでサポートされる最大ユーザ数を示します。2 行目は、各製品のフル メッシュ構造のデジタル ネットワーク配置を指します。Cisco Unified Messaging Gateway（UMG）を利用してさまざまな製品をネットワーク化すると、サポートされるユーザ数が飛躍的に増加しますが、この数はネットワーク ノード数と UMG がサポートする最大ユーザ数に直接関連します。スケーラビリティの詳細については、「Cisco Unified Messaging Gateway によるボイスメール ネットワーキング」（P.13-4）を参照してください。

図 13-1　シスコの音声メッセージング ソリューション



Cisco Unified Messaging Gateway によるボイスメール ネットワーキング

Cisco Unified Messaging Gateway（UMG）は、インテリジェント ボイス メッセージング ルーティング、システム ディレクトリの管理、メッセージング形式、およびスケーラブルなボイス メッセージング フレームワークを提供することによって、エンドツーエンドのネットワーク接続されたボイス メッセージング ソリューションを可能にします。Cisco UMG は、Cisco Unity、Cisco Unity Express、Cisco Unity Connection、および Avaya Interchange をサポートします。

図 13-1 のネットワーク接続されたメッセージングの最大ユーザ数は、フルメッシュのデジタル ネットワーキング環境でサポートされる最大ユーザ数です。Cisco Unified Messaging Gateway を利用した VPIM ネットワーキング ソリューションは、最大 500,000 人のユーザまたはサブスクライバをサポートできます。

この章では、Cisco Unity、Cisco Unity Connection、および Cisco Unity Express と Cisco Unified CallManager の統合について、設計上の側面を中心に説明します。この章では、次のコンポーネントとバージョンを中心に説明します。

- Cisco Unified Communications Manager（Unified CM）7.*x*
- Cisco Unified Communications Manager Express（Unified CME）4.*x*
- Cisco Unity 7.*x* および 4.*x*
- Cisco Unity Connection 7.*x*
- Cisco Unity Express 3.2

Cisco Unified CM 7.*x* には、セッション開始プロトコル（SIP）トランクの機能が搭載されているので、SIP プロキシ サーバを配置することなく、直接 Cisco Unity および Unity Connection と統合することができます。

以前のリリースの Cisco Unity、Unity Connection、Unity Express、および Unified CM または Unified CM Express の詳細については、http://www.cisco.com で入手可能な資料を参照してください。

上で説明したように、この章で扱う設計に関するトピックは、ボイスメールのみの設定、ユニファイド メッセージング設定、および統合メッセージング設定に適用されます。さらに、この章では、Microsoft Exchange（2000、2003、または 2007）メッセージ ストアまたは Lotus Domino メッセージ ストアおよび Microsoft Windows（2000 または 2003）と共に Cisco Unity を配置する場合の設計上の問題についても説明します。この章では、Microsoft NT 4.0 や Exchange 5.5 による配置、および Microsoft NT 4.0 や Exchange 5.5 からのアップグレードは扱いません。Cisco Unity Connection および Unity Express は外部メッセージ ストアに依存しません。Cisco Unity Connection 7.0 は、Exchange 統合をサポートしますが、Cisco Unity と異なり、Exchange 統合に依存しません。

シスコ以外のメッセージング システムとの統合など、Cisco Unity または Cisco Unity Connection に関するその他の設計情報については、http://www.cisco.com で入手可能な『*Design Guide for Cisco Unity*』または『*Design Guide for Cisco Unity Connection*』をそれぞれ参照してください。

Cisco Unity Express に関するその他の設計情報については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

シスコ以外のメッセージング システムとの統合など、Cisco Unified Messaging Gateway に関するその他の設計情報については、http://www.cisco.com で入手可能な Cisco Unified Messaging Gateway の製品マニュアルを参照してください。

メッセージング配置モデル

この章では、Cisco Unity、Cisco Unity Connection、および Cisco Unity Express について、さまざまなメッセージング配置モデルの概要を示します。Cisco Unity、Unity Connection、およびさまざまなメッセージング コンポーネントに固有の配置モデルや設計上の考慮事項の詳細については、http://www.cisco.com で入手可能な『*Design Guide for Cisco Unity*』または『*Design Guide for Cisco Unity Connection*』をそれぞれ参照してください。Cisco Unity Express については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

Cisco Unity と Unity Connection は、次の 3 つの主なメッセージング配置モデルをサポートしています。

- 単一サイト メッセージング
- 集中型メッセージングを使用するマルチサイト WAN 配置
- 分散型メッセージングを使用するマルチサイト WAN 配置

Cisco Unity Express もまた、次の 3 つの主なメッセージング配置モデルをサポートしています。

- 単一サイト メッセージング
- 分散型メッセージングを使用するマルチサイト WAN 配置
- Cisco Unified CME により分散型メッセージングを使用するマルチサイト WAN 配置

（注）　Cisco Unity Express 3.2 は、最大 10 の Unified CME を持つ集中型ボイス メッセージングをサポートします。詳細については、http://www.cisco.com で Cisco Unified Communications Manager Express の資料を参照してください。

Cisco Unified CM と Unified CME のコール処理配置モデルは、Cisco Unity、Unity Connection、および Unity Express のメッセージング配置モデルに依存しませんが、互いに対して考慮が必要な暗黙的要件があります。

3 つのメッセージング配置モデルに加えて、Cisco Unity はメッセージング冗長性もサポートしています（「メッセージングの冗長性」（P.13-17）を参照）。Cisco Unity Connection 7.0 以降、メッセージング冗長性もアクティブ/アクティブ設定で利用できるようになりました。詳細については、http://www.cisco.com で入手できる『*Design Guide for Cisco Unity Connection*』を参照してください。

すべてのメッセージング配置モデルが、ボイスメール、統合メッセージング、およびユニファイド メッセージングのインストールをサポートしています。これらの設定には、次の定義が適用されます。

- *ボイスメール専用*とは、いずれのメッセージング クライアント経由でもボイスメールにアクセスできないテレフォニー ボイスメール統合を指します。
- *統合メッセージング*とは、メッセージング クライアントを介したテレフォニー アクセスおよびボイスメール専用のアクセスを備えたボイスメールを指します。
- *ユニファイド メッセージング*とは、メッセージング クライアントを介したテレフォニー アクセスならびにボイスメール、電子メール、FAX アクセスを備えたボイスメールを指します。

表 13-2 は、これらのタイプのメッセージングをサポートするシスコ製品を示します。

表 13-2　各製品でサポートされるメッセージング環境

メッセージング タイプ	Cisco Unity	Cisco Unity Connection	Cisco Unity Express
ボイスメール専用	あり	あり	あり
統合メッセージング	あり	あり	あり
ユニファイド メッセージング	あり	なし	なし

単一サイト メッセージング

このモデルでは、メッセージング システムとメッセージング インフラストラクチャ コンポーネントがすべて、同じサイトのアベイラビリティの高い同じ LAN 上に置かれます。サイトは、単一サイトである場合も、高速 Metropolitan Area Network（MAN; メトロポリタン エリア ネットワーク）を介して相互接続されたキャンパス サイトである場合もあります。メッセージング システムのクライアントもすべて、単一（またはキャンパス）サイトに置かれます。このモデルの際立った特徴は、リモート クライアントが存在しないことです。

集中型メッセージング

このモデルでは、単一サイト モデルと同様に、メッセージング システムとメッセージング インフラストラクチャ コンポーネントがすべて、同じサイトに置かれます。サイトは、1 つの物理的なサイトである場合も、高速 MAN を介して相互接続されたキャンパス サイトである場合もあります。ただし、単一サイト モデルとは異なり、メッセージング クライアントをローカルとリモートの両方に置くことができます。

メッセージング クライアントはメッセージング システムに対してローカルでもリモートでも可能であるため、Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）クライアント：ViewMail for Outlook（VMO）、および Telephone Record and Playback（TRaP; 電話での録音および再生）機能とメッセージストリーミング機能を使用する際に、特別な設計上の考慮事項が適用されます。リモート クライアントは、TRaP を使用すべきではありません。また、リモート クライアントは、再生前にメッセージをダウンロードするように設定する必要があります。ローカルクライアントとリモートクライアントで機能や操作が異なるとユーザが混乱する恐れがあるため、音声ポートで TRaP を無効にし、クライアントがローカルであるかリモートであるかに関係なく、メッセージをダウンロード

するように設定し、TRaP を使用しないように GUI クライアントを設定する必要があります。これはまた、Cisco Unity Connection 7.0 で新しく導入された Unity Connection IMAP クライアントの ViewMail for Outlook（VMO）にも適用されます。

Cisco Unity Telephone User Interface（TUI; 電話ユーザ インターフェイス）は、ローカル クライアントとリモート クライアントの両方に対して同様に動作します。

分散型メッセージング

分散型メッセージング モデルは、共通のメッセージング バックボーンを持つ複数の単一サイト メッセージング システムで構成されます。複数のロケーションを持つことができ、各ロケーションに独自のメッセージング システムとメッセージング インフラストラクチャ コンポーネントが置かれます。すべてのクライアント アクセスが各メッセージング システムに対してローカルであり、メッセージング システムは、すべてのロケーションにまたがるメッセージング バックボーンを共有します。分散型メッセージング システムからのメッセージ送信は、フルメッシュタイプまたはハブアンドスポーク タイプのメッセージ ルーティング インフラストラクチャによって、メッセージング バックボーンを介して行われます。WAN によって、メッセージング インフラストラクチャ コンポーネントを、サービス提供先のメッセージング システムから切り離すことはできません。

分散型メッセージングは、基本的に、共通のメッセージング バックボーンを持つ複数の単一サイト メッセージング モデルです。このルールの例外は、PBX-IP Media Gateway（PIMG）統合と T1-IP Media Gateway（TIMG）統合です。PIMG 統合と TIMG 統合は、設計に関するこのドキュメントでは説明しません。PIMG または TIMG の詳細については、http://www.cisco.com で入手できる Cisco Unity の統合ガイドを参照してください。

分散型メッセージング モデルは、ローカルおよびリモートの GUI クライアント、TRaP、およびメッセージのダウンロードに関して、集中型メッセージングと同じ設計基準を持っています。

メッセージングと Unified CM 配置モデルの組み合わせ

ここでは、さまざまなメッセージング配置モデルを Unified CM コール処理配置モデルに統合する場合の設計上の考慮事項について説明します。表 13-3 では、Cisco Unity、Unity Connection、および Unity Express によってサポートされるメッセージング配置モデルとコール処理配置モデルのさまざまな組み合わせを示します。

表 13-3　サポートされているメッセージングと Unified CM コール処理配置モデルの組み合わせ

モデル タイプ	Cisco Unity	Cisco Unity Connection	Cisco Unity Express
単一サイト メッセージングと単一サイト コール処理	あり	あり	あり
集中型メッセージングと集中型コール処理	あり	あり	なし[1]
分散型メッセージングと集中型コール処理	あり	あり	あり
集中型メッセージングと分散型コール処理	あり	あり	なし[1]
分散型メッセージングと分散型コール処理	あり	あり	あり
集中型メッセージングと WAN を介したクラスタ化	あり	あり	なし
分散型メッセージングと WAN を介したクラスタ化	あり	あり	あり

1. Unified CME による集中型ボイスメール メッセージングが Cisco Unity Express 3.2 以降サポートされていますが、これは Unified CM コール処理配置モデルには適用されません。

この項では、次のトピックについて取り上げます。

- Cisco Unity と Unity Connection メッセージングおよび Unified CM の 配置モデル
- Cisco Unity Express の配置モデル

各トピックではメッセージングと Unified CM の配置モデルの組み合わせを定義した後、そのモデルに適用可能なシスコのボイスメール メッセージング製品と、そのモデルの組み合わせに関する設計上の考慮事項について説明します。ここでは、各製品のすべての組み合わせを取り上げるわけではありません。いくつかの例を示し、各製品のベスト プラクティスと設計上の考慮事項を説明します。ここでの説明は、基本となるメッセージング配置モデルと Unified CM とのインタラクションの理解を促すためのものであり、すべての可能性を詳細に説明することは意図していません。

サイト分類の詳細、およびメッセージング配置モデルとコール処理配置モデルのサポートされている組み合せの詳細な分析については、http://www.cisco.com で入手可能な『*Design Guide for Cisco Unity*』および『*Design Guide for Cisco Unity Connection*』を参照してください。

Cisco Unity と Unity Connection メッセージングおよび Unified CM の配置モデル

ここでは、Cisco Unity と Unity Connection によってサポートされるメッセージング配置モデルとコール処理配置モデルのさまざまな組み合わせを示します。

集中型メッセージングと集中型コール処理

集中型メッセージングでは、ボイス メッセージング サーバを Unified CM クラスタと同じサイトに置くことができます。集中型コール処理では、サブスクライバがクラスタおよびメッセージング サーバに対して、リモートとローカルのどちらにも存在できます（図 13-2 を参照）。リモートユーザが中央のサイトのリソース（音声ポート、IP Phone、Tail-End Hop-Off（TEHO; テールエンドホップオフ）の場合の公衆網ゲートウェイなど）にアクセスする場合、そのコールはゲートキーパー コール アドミッション制御にとって透過的になります。したがって、Unified CM でリージョンとロケーションを設定して、コール アドミッション制御を提供する必要があります（「帯域幅の管理」（P.13-32）を参照）。IP Phone または MGCP ゲートウェイにリージョン間コールを発信する場合、IP 電話は設定済みのリージョン間コーデックを自動的に選択します。Cisco Unity メッセージング配置では、WAN を通過する（リージョン間）コールのために、音声ポートが Unified CM トランスコーディング リソースを使用するように、ネイティブ トランスコーディングを無効にする必要があります。Cisco Unity でこの機能を無効にする方法の詳細については、「ネイティブ トランスコーディング動作」（P.13-33）を参照してください。

図 13-2　集中型メッセージングと集中型コール処理

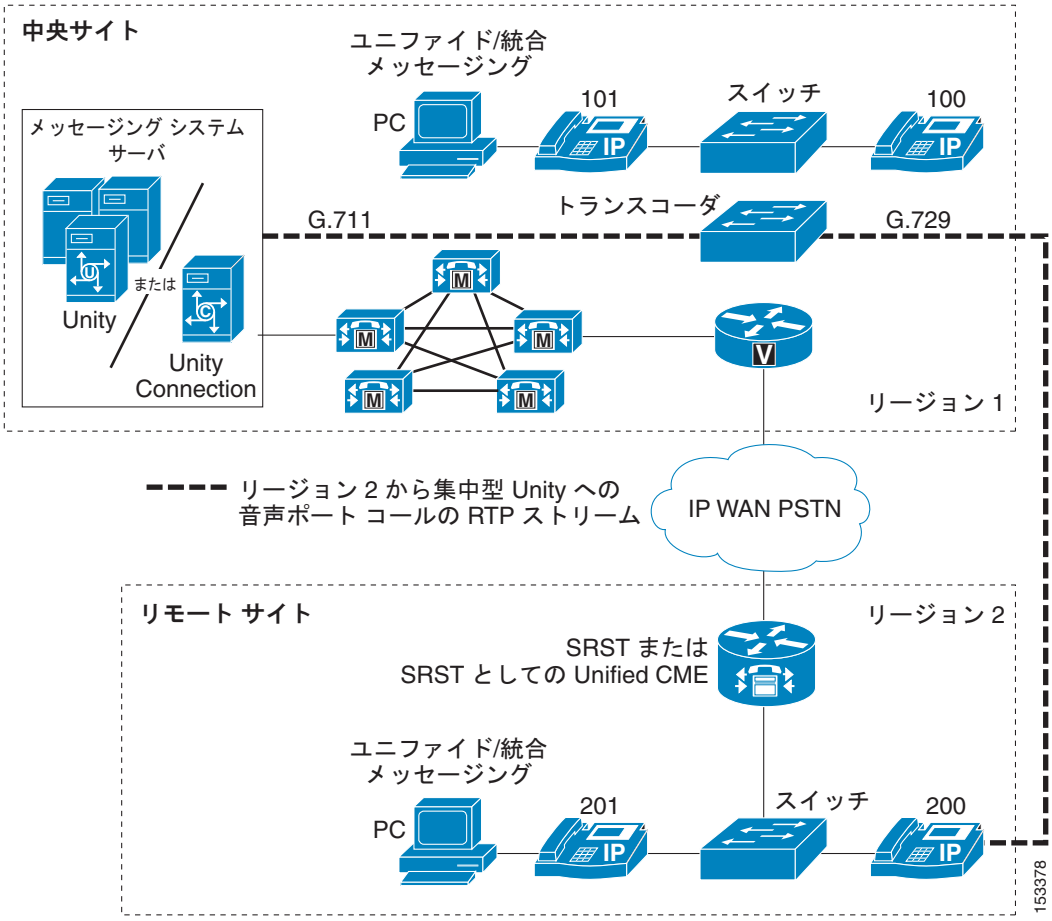


図 13-2 では、リージョン 1 と 2 が、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。Cisco Unity または Unity Connection サーバ上でネイティブ トランスコーディングは無効になっています。

図 13-2 で示しているように、内線番号 200 からリージョン 1 のボイスメール ポートにコールが発信されると、エンドポイントではリージョン間の G.729 コーデックが使用されますが、RTP ストリームがトランスコードされ、音声ポート上では G.711 が使用されます。この例では、Cisco Unity または Unity Connection サーバ上のネイティブ トランスコーディングが無効になっています。Unified CM トランスコーディング リソースは、ボイスメール システムと同じサイトに置く必要があります。

AAR によってルーティングされるボイスメール コールで RDNIS が送信されないことによる影響

集中メッセージング環境では、WAN がオーバーサブスクリプションの状態になった場合に、Unified CM の機能である Automated Alternate Routing（AAR; 自動代替ルーティング）が、公衆網を介してコールを中央サイトのメッセージング ストアにルーティングできます。ただし、公衆網を介してコールが再ルーティングされる場合、Redirected Dialed Number Information Service（RDNIS）が損なわれることがあります。Cisco Unity または Unity Connection がメッセージング クライアントに対してリモートである場合は、正しくない RDNIS 情報によって、AAR が外線を介して再ルーティングするボイスメール コールに影響が及ぼされることがあります。RDNIS 情報が正しくない場合、コールはダイヤル先のユーザのボイスメール ボックスに到達せず、自動アテンダント プロンプトを受信します。発信者は、到達を試みているユーザの内線番号を再入力するように要求されることがあります。この動作は、主に、電話通信事業者がネットワークを介した RDNIS を保証できない場合の問題です。通信事業者が RDNIS の正常な送信を保証できない理由は数多くあります。通信事業者に問い合せて、回

線のエンドツーエンドで RDNIS の送信を保証しているかどうかを確認してください。オーバーサブスクリプションの状態になった WAN に対して AAR を使用する代わりの方法は、単に、オーバーサブスクリプションの状況で発信者にリオーダー トーンが聞こえるようにすることです。

分散型メッセージングと集中型コール処理

分散型メッセージングは、テレフォニー環境内に複数のメッセージング システムが分散されており、各メッセージング システムがローカル メッセージング クライアントだけにサービスを提供することを意味します。このモデルは集中型メッセージングとは異なります。集中型メッセージングでは、メッセージング システムに対してローカルなクライアントとリモートのクライアントの両方が存在します。

図 13-3 では、集中型コール処理を使用する分散型メッセージング モデルを示しています。他のマルチサイト コール処理モデルと同様に、WAN 帯域幅を管理するためにリージョンとロケーションを使用する必要があります。このモデルでは、Cisco Unity でネイティブ トランスコーディングを無効にする必要もあります。

SRST モードの Cisco Unified Communications Manager Express（Unified CME）は、IP 電話および Cisco Unity または Unity Connection ボイスメール ポートの両方のコール処理バックアップに使用されます。このフォールバック サポートは、リモート サイト（たとえば、図 13-3 のリージョン 2）に配置され、WAN 障害などのために電話機と Unified CM との接続が失われた場合に、バックアップのコール処理を提供します。またリモート サイトのユーザに対し、WAN 障害時に、ローカルの Cisco Unity または Unity Connection サーバへのアクセスと MWI のサポートを提供します。SRST モードの Unified CME の詳細については、http://www.cisco.com で入手可能な Unified CME の製品マニュアルを参照してください。

図 13-3　分散型メッセージングと集中型コール処理

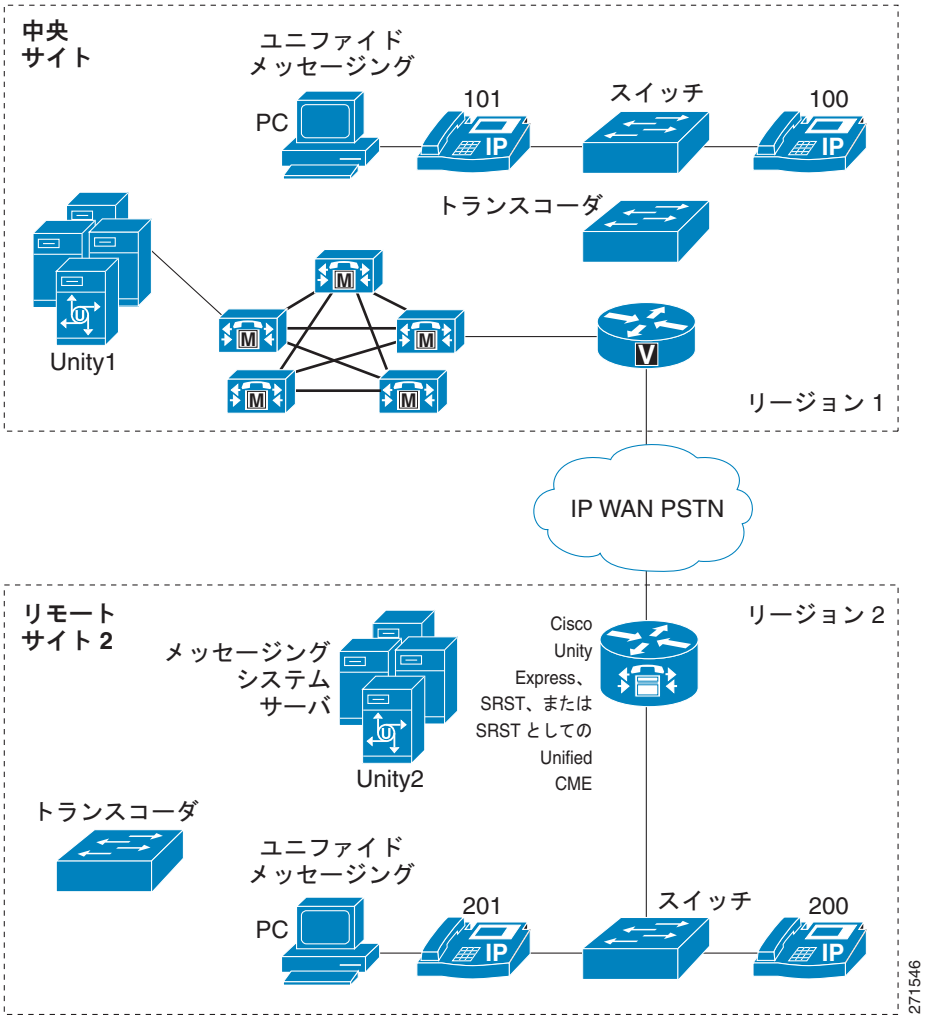


図 13-3 の構成では、トランスコーダ リソースが各 Cisco Unity メッセージ システム サイトに対してローカルである必要があります。リージョン 1 と 2 は、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。Cisco Unity サーバ上でネイティブ トランスコーディングは無効になっています。

Unified CM サーバに設定されているコーリング サーチ スペースとデバイス プールによって、両方の Cisco Unity または Unity Connection サーバの音声メッセージング ポートに、適切なリージョンとロケーションが割り当てられる必要があります。さらに、テレフォニー ユーザをボイスメール ポートの特定のグループに関連付けるために、Unified CM ボイスメール プロファイルを設定する必要があります。コーリング サーチ スペース、デバイス プール、およびボイスメール プロファイルを設定する方法の詳細については、http://www.cisco.com で入手可能な、該当するバージョンの『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

メッセージング システムは相互に「ネットワーク接続」され、内部ユーザと外部ユーザの両方に単一のメッセージング システムを提供します。分散 Unity サーバ向けの Cisco Unity ネットワーク機能については、次の Web サイトで入手可能な『*Networking in Cisco Unity Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html

また Cisco Unity Connection では新たにデジタル ネットワーキングがサポートされ、複数の Cisco Unity Connection を相互にネットワーク接続できます。最大 5 個のノード（シングルまたはアクティブ/アクティブ ペア）を相互接続すると、ディレクトリ内で最大 50,000 のエンティティをサポートできます。Cisco Unity Connection は、Microsoft Active Directory などの企業ディレクトリに統合して、ユーザを同期化し、デジタル ネットワーキングを同時に使用することができます。この設定では、各 Cisco Unity Connection サーバまたはサーバ ペアが、企業ディレクトリから最大 10,000 ユーザを同期化できます。Cisco Unity Connection でのデジタル ネットワーキングまたはディレクトリ統合の詳細については、http://www.cisco.com で入手できる『*Design Guide for Cisco Unity Connection*』を参照してください。

Cisco Unity と Unity Connection および SRST モードの Unified CME

SRST モードの Unified CME を使用すると、Cisco Unity サーバと Unity Connection サーバの両方をリモート サイトに置き、中央サイトの Unified CM に登録して、リモート ロケーションにある Unified CME にフォールバックすることができます。WAN リンクがダウンし、電話機が SRST モードの Unified CME にフェールオーバーすると、Cisco Unity と Unity Connection のボイスメール ポートも SRST モードの Unified CME にフェールオーバーします。これにより、リモートサイトのユーザが、WAN の障害時に、MWI 機能も含めてボイスメールにアクセスできるようになります。

このシナリオには、次の各項目が必要です。

- Cisco Unified CME 4.0 以降
- Cisco Unity 4.0（5）以降と TSP バージョン 8.1（3）以降
- Cisco Unity Connection 2.*x* 以降

（注）　Unified CM から SRST モードの Unified CME へ、またはその逆方向にフェールオーバーが発生した場合、Cisco Unity または Unity Connection サーバから MWI を再同期する必要があります。

メッセージング配置モデルの組み合わせ

複数のメッセージング モデルを同じ配置で組み合せることができます。ただし、その配置は、上記の項で示したすべてのガイドラインに従う必要があります。図 13-4 では、集中型メッセージングと分散型メッセージングの両方が同時に採用されるユーザ環境を示しています。

図 13-4　結合された配置モデル

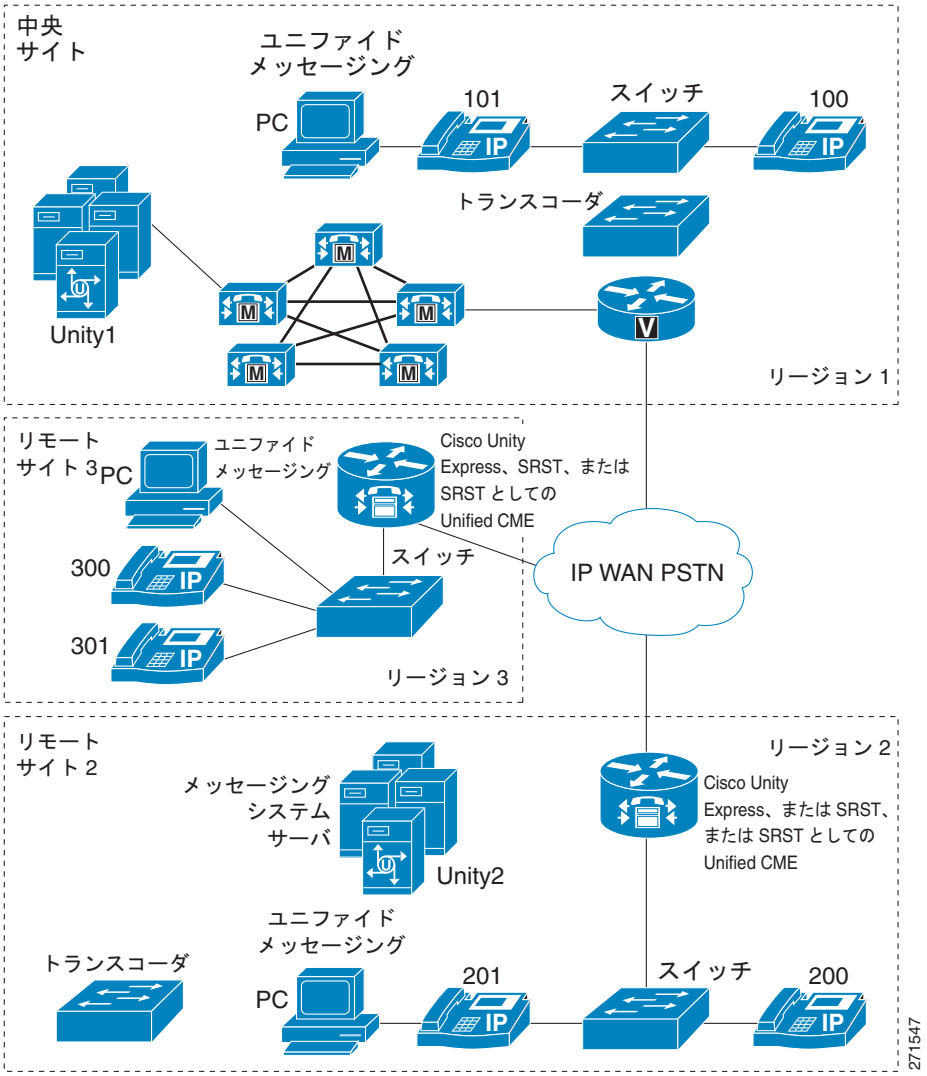


図 13-4 では、2 つのメッセージング モデルの組み合わせを示しています。リージョン 1 と 3 は集中型メッセージングと集中型コール処理を使用し、リージョン 2 は分散型メッセージングと集中型コール処理を使用しています。すべてのリージョンが、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。

図 13-4 では、中央サイトとサイト 3 の間で、集中型メッセージングと集中型コール シグナリングが使用されています。中央サイトのメッセージング システムは、中央サイトとサイト 3 の両方のクライアントにメッセージング サービスを提供します。サイト 2 は、集中型コール処理を使用する分散型メッセージング モデルを使用しています。サイト 2 に置かれているメッセージング システム（Unity2）は、サイト 2 の中にいるユーザだけにメッセージング サービスを提供します。この配置では、両方のモデルが、この章に記載されているそれぞれの設計上のガイドラインに従っています。トランスコーディン

グ リソースは各メッセージング システム サイトに対してローカルに置かれ、サイト 2 のユーザが中央サイトのユーザにメッセージを残す場合のように、（メッセージング システムに対して）リモートのサイトからメッセージング サービスにアクセスするクライアントをサポートします。

また、SRST モードの Cisco Unified Communications Manager Express（Unified CME）は、IP 電話および Cisco Unity または Unity Connection ボイスメール ポートの両方のコール処理バックアップに使用されます。このフォールバック サポートは、リモート サイト（たとえば、図 13-4 のリージョン 2）に配置され、WAN 障害などのために電話機と Unified CM との接続が失われた場合に、バックアップのコール処理を提供します。またリモート サイトのユーザに対し、WAN 障害時に、ローカルの Cisco Unity または Unity Connection サーバへのアクセスと MWI のサポートを提供します。SRST モードの Unified CME の詳細については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

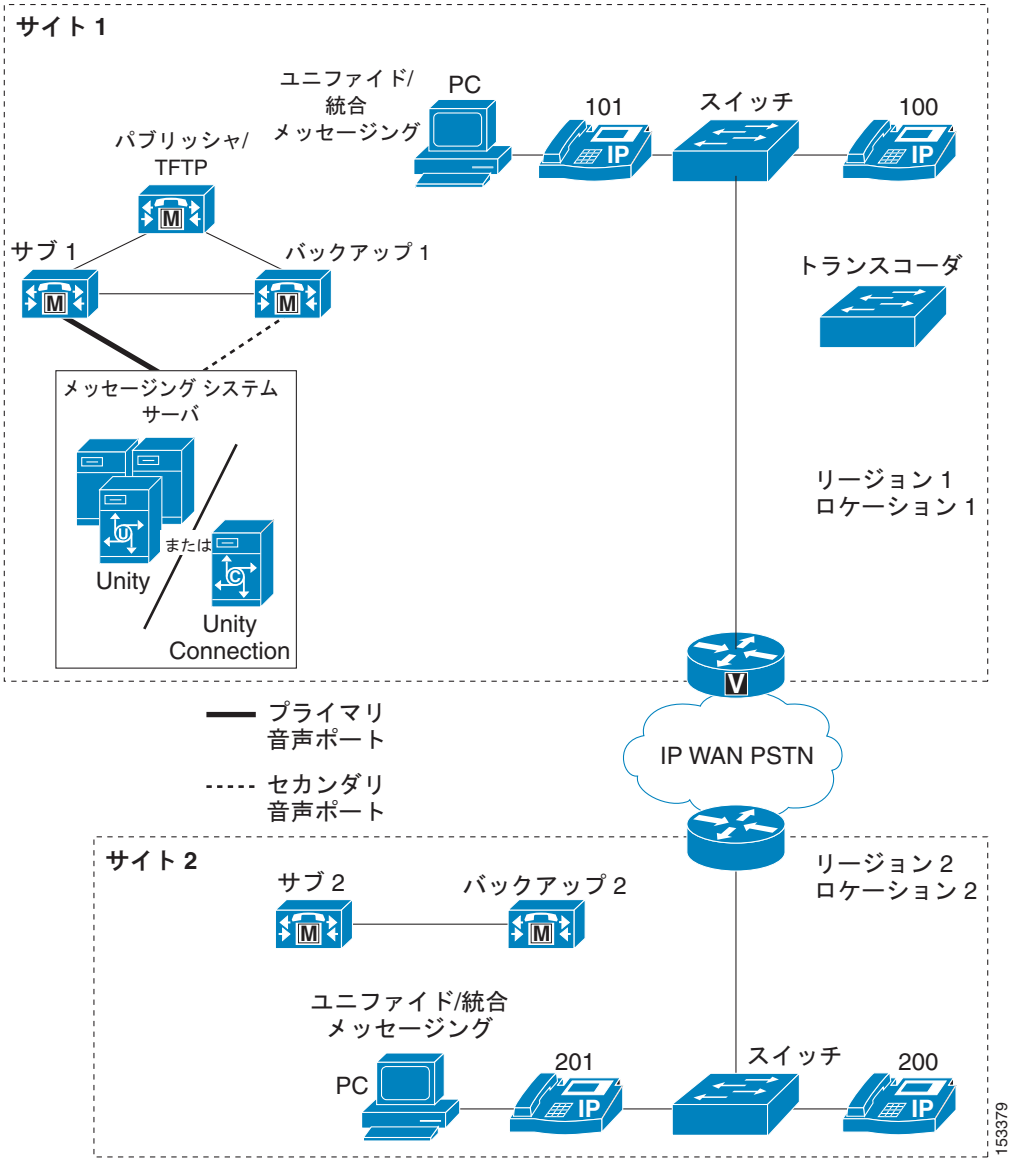
集中型メッセージングと WAN を介したクラスタ化

ここでは、集中型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介した Unified CM クラスタ化を一緒に配置する場合の Cisco Unity の設計上の問題について説明します。このモデルで WAN に障害が発生した場合は、WAN が復元されるまで、すべてのリモート メッセージング サイトがボイスメール機能を失います（図 13-5 を参照）。

WAN を介したクラスタ化は、ローカル フェールオーバーをサポートしています。ローカル フェールオーバーでは、各サイトが、物理的にそのサイトに置かれているバックアップ サブスクライバ サーバを持ちます。ここでは、Cisco Unity 集中型メッセージングと、WAN を介したクラスタ化のローカル フェールオーバーを一緒に配置する方法を中心に説明します。

詳細については、「IP WAN を介したクラスタ化」（P.2-22）の項を参照してください。

図 13-5　Cisco Unity 集中型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介したクラスタ化



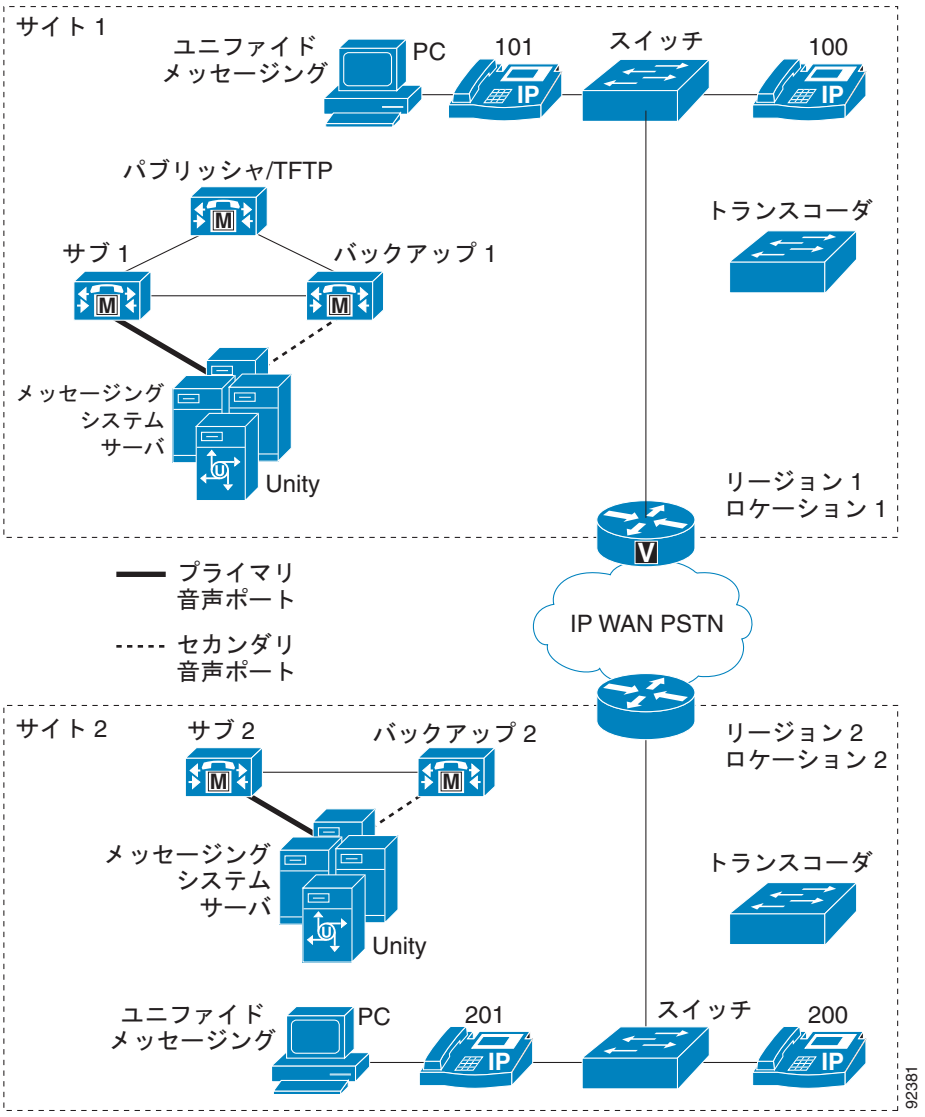
クラスタ化されたサーバ間の最小帯域幅の要求については、「ローカル フェールオーバー配置モデル」（P.2-26）の項を参照してください。

Unified CM による WAN 経由のクラスタ化では、Cisco Unity と同様、最大 8 サイトがサポートされます。ボイスメール ポートは、Cisco Unity メッセージング システムが置かれているサイトだけに設定されます（図 13-5 を参照）。ボイスメール ポートは、WAN を介してリモート サイトに登録されません。他のサイトのメッセージング クライアントは、プライマリ サイトのすべてのボイスメール リソースにアクセスします。WAN に障害が発生すると、リモート サイトは集中型メッセージング システムにアクセスできなくなるため、WAN を介してリモート サイトに音声ポートを設定してもメリットがありません。ユニファイドメッセージングの場合、帯域幅を考慮して、ボイスメールポートで TRaP を無効にし、すべてのメッセージングクライアントがそのローカル PC にボイスメールメッセージをダウンロードするようにする必要があります。

分散型メッセージングと WAN を介したクラスタ化

Cisco Unity メッセージング サーバも配置されたローカル フェールオーバー サイトでは、集中型メッセージング モデルと同様に、音声ポートがローカル Unified CM サブスクライバ サーバに登録されます。音声ポートの設定については、「Unified CM クラスタとの音声ポート統合」（P.13-39）および「専用 Unified CM バックアップ サーバを使用する音声ポート統合」（P.13-41）を参照してください。

図 13-6　Cisco Unity 分散型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介したクラスタ化



WAN を介したクラスタ化を含む単純分散型メッセージング実装では、クラスタ内の各サイトに、独自の Cisco Unity メッセージング サーバとメッセージング インフラストラクチャ コンポーネントが置かれます。すべてのサイトにローカル Cisco Unity メッセージング システムが置かれるわけではなく、一部のサイトで、ローカル メッセージング クライアントがリモート メッセージング サーバを使用する場合、その配置は分散型メッセージングと集中型メッセージングの組み合わせモデルとなります（「メッ

セージング配置モデルの組み合わせ」（P.13-13）を参照）。このモデルで WAN に障害が発生した場合は、WAN が復元されるまで、集中型メッセージングを使用するすべてのリモート サイトがボイスメール機能を失います。

ローカル メッセージング サーバを持たない各サイトは、そのすべてのメッセージング クライアントに対して単一のメッセージング サーバを使用する必要がありますが、そのようなサイトのすべてが同じメッセージング サーバを使用する必要はありません。たとえば、サイト 1 とサイト 2 のそれぞれがローカル メッセージング サーバを持っているとします。その場合、サイト 3 のすべてのクライアントがサイト 2 のメッセージング サーバを使用し（そのメッセージング サーバに登録し）、サイト 4 のすべてのクライアントがサイト 1 のメッセージング サーバを使用するようにすることができます。ローカル Cisco Unity メッセージング サーバを持つサイトには、トランスコーダ リソースが必要です。

他の分散型コール処理配置と同様に、これらのサイト間のコールはゲートキーパー コール アドミッション制御にとって透過的です。したがって、Unified CM でリージョンとロケーションを設定してコール アドミッション制御を提供する必要があります（「帯域幅の管理」（P.13-32）を参照）。

分散 配置された Cisco Unity サーバは、デジタルでネットワーク接続することもできます。このトピックの詳細については、http://www.cisco.com で入手可能な『*Cisco Unity Networking Guide*』を参照してください。配置される特定のメッセージング ストアに固有の Networking Guide が用意されています。

メッセージングの冗長性

ここでは、Cisco Unity と Cisco Unity Connection に関するメッセージングの冗長性について説明します。Cisco Unity Express は、メッセージングの冗長性をサポートしていません。

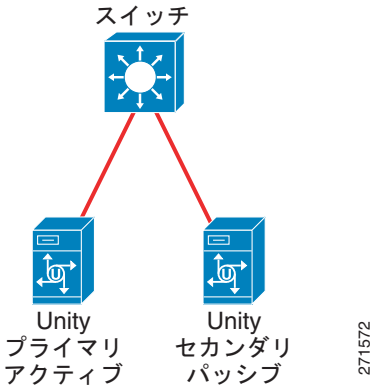
Cisco Unity

Cisco Unity は、2 種類の冗長性をサポートしています。1 つ目は単純に Unity フェールオーバー（ローカル メッセージング フェールオーバー）と呼ばれ、システム障害のフェールオーバーが提供されます。2 つ目は、スタンバイ冗長性と呼ばれ、地理的な複数の場所にわたる障害回復機能を提供します。Cisco Unity フェールオーバーとスタンバイ冗長性の比較については、『*Cisco Unity Design Guide*』を参照してください。

Cisco Unity フェールオーバーは、プライマリとセカンダリの 2 つのサーバがアクティブ/パッシブ冗長ペアとして設定されます。プライマリ サーバはアクティブの状態でコールを受け付け、セカンダリは非アクティブでコールを受け付けません。プライマリ サーバでサブスクライバや設定に関するデータを変更されると、その変更内容がセカンダリ サーバに自動的に複製されます。何らかの理由でプライマリ サーバが機能しなくなった場合、セカンダリ サーバが自動的にアクティブ サーバになりコールの受け付けを開始します。その間、プライマリ サーバは一時的に非アクティブになります。

図 13-7 に示しているように、ローカル メッセージング フェールオーバーを実装できます。ローカル フェールオーバーでは、プライマリ Cisco Unity サーバとセカンダリ Cisco Unity サーバの両方が、アベイラビリティの高い同じ LAN 上の同じサイトに置かれます。

図 13-7　Cisco Unity メッセージングのローカル フェールオーバー



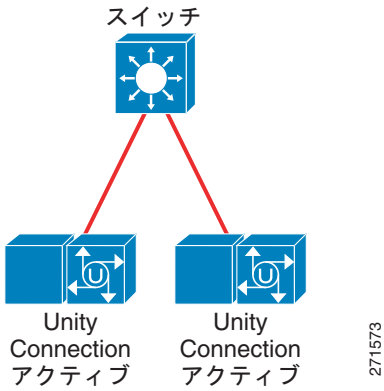
Cisco Unity Standby Redundancy はまた、地理的な複数の場所にわたる障害回復機能も提供します。この場合もプライマリとセカンダリの 2 つのサーバを使用しますが、それらは通常、別の都市にある異なるデータ センターにインストールされます。プライマリ サーバがインストールされたデータ センターが自然災害やその他の大規模災害に遭遇した場合、障害回復設備にいる（またはリモートでアクセスできる）誰かが、セカンダリ サーバを手動でアクティブ化すると、セカンダリ サーバがコールの受付を開始します。スタンバイ冗長性またはフェールオーバー（ローカル メッセージング フェールオーバー）の要件に関する詳細については、http://www.cisco.com で入手できる『*System Requirements for Cisco Unity Release 7.x*』を参照してください。

Cisco Unity Connection

Cisco Unity Connection は、プライマリとセカンダリの 2 つのサーバをアクティブ/アクティブのサーバ ペアに設定したアクティブ/アクティブ冗長モデルで、メッセージング冗長性とロード バランシングをサポートします。アクティブ/アクティブ冗長モデルでは、プライマリとセカンダリの両方のサーバが、コールおよび HTTP 要求と IMAP 要求をアクティブに受け付けます。この機能は、Cisco Unity Connection release 7.0 の新機能です。詳細については、http://www.cisco.com で入手できる『*Design Guide for Cisco Unity Connection*』を参照してください。

図 13-8 は、Cisco Unity Connection のアクティブ/アクティブ メッセージング冗長性を示します。

図 13-8　Cisco Unity Connection メッセージングの冗長性



Cisco Unity と Cisco Unity Connection の SIP トランクの実装には、いずれもメッセージング冗長機能のためのコール分岐（転送）が必要です。現在、Unified CM が SIP トランクのコールの分岐（転送）をサポートしていないため、Unified CM で SIP トランクが使用されている場合、Cisco Unity フェールオー

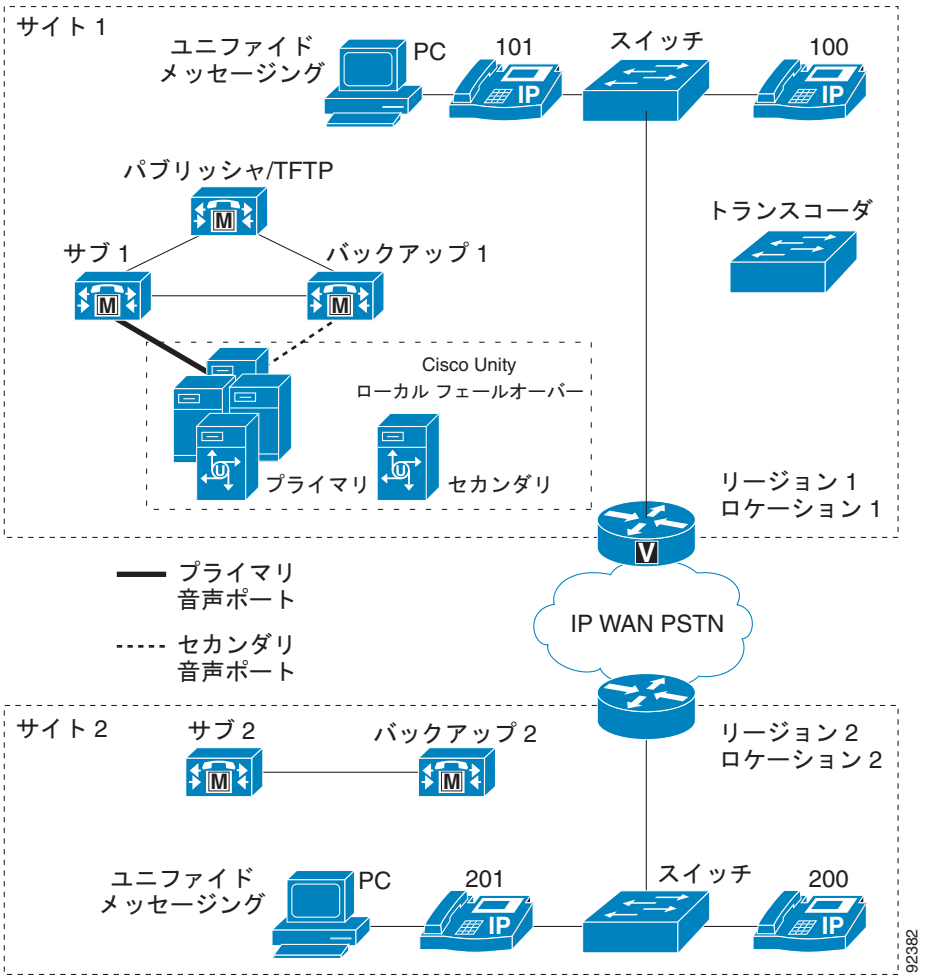
バーは利用できません。ただし、アクティブ/アクティブ冗長性の Cisco Unity Connection サーバ ペアで SIP トランクを使用している場合は、2 つの異なる SIP トランクをサーバ ペアの各サーバに 1 つずつ設定し、それらを同じルート リストに関連付けられた同じルート グループに追加することをお勧めします。この設定では、Unified CM から 2 つのサーバに対するロードバランシング コールが可能です。

Cisco Unity フェールオーバーと WAN を介したクラスタ化

Cisco Unity ローカル フェールオーバーと WAN を介したクラスタ化を配置する場合は、「集中型メッセージングと WAN を介したクラスタ化」（P.13-14）および 「分散型メッセージングと WAN を介したクラスタ化」（P.13-16）で説明している設計プラクティスを適用します。正常な動作時、プライマリ Cisco Unity サーバからの音声ポートは WAN を通過しません。

図 13-9 では、Cisco Unity ローカル フェールオーバーを示しています。プライマリ Cisco Unity サーバとセカンダリ Cisco Unity サーバの両方が物理的に同じサイトに置かれていることに注意してください。Cisco Unity フェールオーバーは、Unified CM の WAN を介したクラスタ化で使用可能な最大数までリモート サイトをサポートします。

図 13-9　Cisco Unity ローカル フェールオーバーと WAN を介したクラスタ化



Cisco Unity フェールオーバーの設定については、http://www.cisco.com で入手できる『*Cisco Unity Failover Configuration and Administration Guide*』を参照してください。

すでに述べたように、WAN 経由のハイ アベイラビリティを運用するために Cisco Unity フェールオーバーを設定することができますが、この配置にはいくつかの要件があります。たとえば、地理的に離れた複数のデータ センターでの完全な冗長性が重要な場合、この設定でインストール操作を成功させるために、満たすべき特定の要件があります。これらの要件については、http://www.cisco.com で入手できる『*System Requirements for Cisco Unity Release 7.x*』を参照してください。

集中型メッセージングと分散型 Unified CM クラスタ

Cisco Unity および Unity Connection は、複数の Unified CM クラスタによる集中型メッセージング設定に配置することもできます（図 13-10 を参照）。複数統合および 複数の Unified CM クラスタに伴なう MWI の考慮事項の詳細については、「テレフォニー統合」（P.13-36）の項を参照してください。

図 13-10　Cisco Unity または Unity Connection と複数の Unified CM クラスタの統合

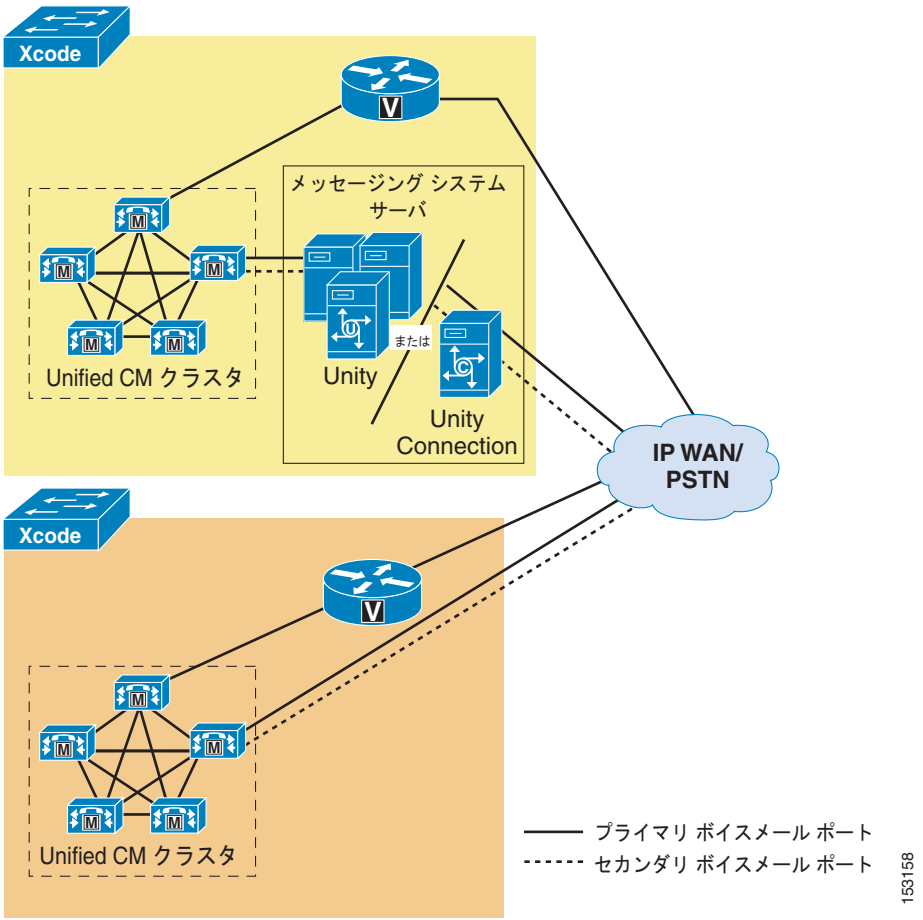


図 13-10 の設定では、クラスタ 1 とクラスタ 2 の両方のサイトのメッセージング クライアントが、物理的にクラスタ 1 に置かれている Cisco Unity または Unity Connection メッセージング インフラストラクチャを使用します。

Cisco Unity Express の配置モデル

ここではまず、Cisco Unity Express を概観し、製品に関する情報を提供します。次に、配置モデルについての項では、集中型と分散型の両方のコール処理における分散型音声メッセージングを中心に、Cisco Unity Express に関してサポートされている 3 つの配置モデルを紹介し、次いで配置の特徴と設計ガイドラインを示します。最後に、Cisco Unity Express と Unified CM 、さらには Cisco Unity Express と Unified SRST または SRST モードの Unified CME の間で使用されるシグナリング コール フローとさまざまなプロトコルについて説明します。

Cisco Unity Express の概要

Cisco Unity Express は、Cisco 2800 および 3800 シリーズの Integrated Services Router（ISR; 統合型サービス ルータ）または Cisco Unified Communications 500（UC 500）プラットフォームに直接統合される Cisco Unity Express Enhanced Network Module（NME-CUE）または Cisco Unity Express Advanced Integration Module（AIM-CUE）上に展開されます。または Cisco 1861 ISR 上にプレインストール済みのハードウェアにプリロードして納入されます。Cisco Unity Express はさまざまな設定が可能であり、ボイスメールと統合メッセージング、自動応答セッション、またはオプションの IVR といったサービスを同時にサポートし、最大 24 のポートで、8 ～ 250 人のユーザをサポートします。Cisco Unity Express 3.0 以降のリリースでは、NME-CUE モジュールと 24 のポートをサポートします。

（注）　Cisco Unity Express NM-CUE と NM-CUE-EC モジュールは、販売およびサポートが終了しており、Cisco Unity Express Enhanced Network Module（NME-CUE）に置き換えられています。販売終了とサポート終了のお知らせについては、http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps5745/ps5520/end_of_life_notice_c51-453045.html を参照してください。

（注）　小規模企業向け Cisco Unified Communications 500 シリーズは、Cisco Unified Communications Manager Express（Unified CME）と Cisco Unity Express をサポートしますが、Cisco Unified CM 対応の SRST はサポートしません。小規模企業向け Cisco Unified Communications 500 シリーズは、最大 5 つのサイトをサポートします。

Cisco Unity Express は、Cisco Unified Communications Manager、Unified SRST、Cisco Unified Communications Manager Express（Unified CME）と共に、ボイスメール ソリューションとして配置できます。Unified CME 統合と Unified CM 統合の間で Cisco Unity Express を変換またはバックアップと復元を行うことはできません。Unified CM のインストールで使用していた Cisco Unity Express モジュールを Unified CME で使用する場合、またはその逆の場合は、再イメージ化が必要です。これには、ソフトウェアとライセンスを再適用する必要があり、すべての設定とボイスメール メッセージを含むデータが失われます。以前のリリースでは、Cisco Unity Express は Unified CME または Survivable Remote Site Telephony（SRST）ルータとの共存配置に限定されていました。しかし、Cisco IOS Release 12.3(11)T での H.323-to-SIP コール ルーティング機能の導入に伴ない、Unified CM または Unified CME と合わせて展開する場合、Cisco Unity Express と SRST または Unified CME を、それぞれ異なるルータに置けるようになりました。

Cisco Unity Express は、SIP を使用して Cisco Unified Communications Manager Express（Unified CME）と通信し、Cisco Unity Express は、JTAPI を使用して Cisco Unified Communications Manager（Unified CM）に接続します。Cisco Unity Express は Unified CM と接続されると、実行されている Unified CM のバージョンを自動的に検出し、それ自体の JTAPI ライブラリのバージョンと比較します。Unified CM リリースが変更されていることが検出されると、Cisco Unity Express は自動的に再起動し、接続されている Unified CM のバージョンに合わせて、正しい JTAPI ライブラリで再設定を行います。

Unified CM と Unified CME の相互運用性の詳細については、「Unified CM と Unified CM Express の相互運用性」（P.8-36）を参照してください。

Unified CME でサポートされている配置モデルの詳細については、http://www.cisco.com で入手可能な Cisco Unified Communications Manager Express の設計に関する資料を参照してください。

配置モデル

Cisco Unity Express は、単一のサイトとして配置することも、Cisco Unified Communications Manager（Unified CM）または Unified Communications Manager Express（Unified CME）の分散型ボイスメールおよび自動応答（AA）ソリューションとして配置することもできます。ただし、Cisco Unity Express は、次のようなすべての Cisco Unified CM 配置モデルでサポートされます。

- 単一サイト配置
- 集中型コール処理を使用するマルチサイト WAN 配置
- 分散型コール処理を使用するマルチサイト WAN 配置

図 13-11 は、Cisco Unity Express を統合した集中型コール処理配置を、図 13-12 は、分散型コール処理配置を示しています。

Unified CME によって制御される Cisco Unity Express サイト、および Unified CM によって制御されるその他のサイトは、H.323 または SIP トランキング プロトコルを使用して相互接続することができます。Cisco Unity Express は Unified CM または Unified CME のいずれかと統合できますが、両方と同時に統合はできません。

（注）　Cisco Unity Express 3.2 は、最大 10 の Unified CME を持つ集中型配置モデルをサポートします。

図 13-11　集中型コール処理配置における Cisco Unity Express

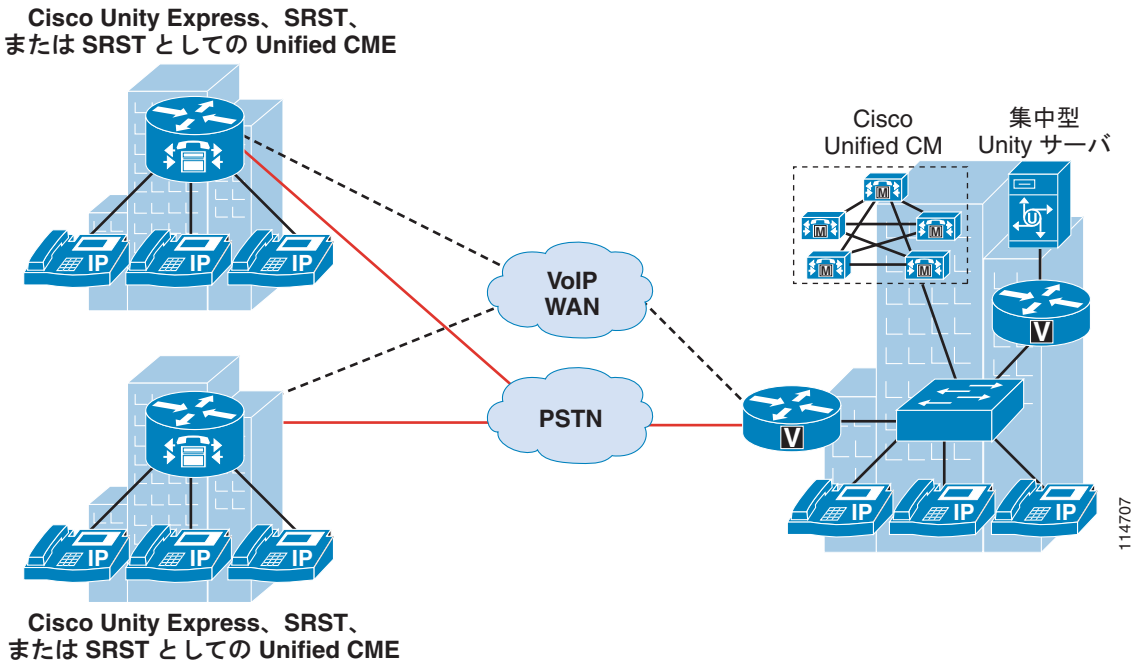
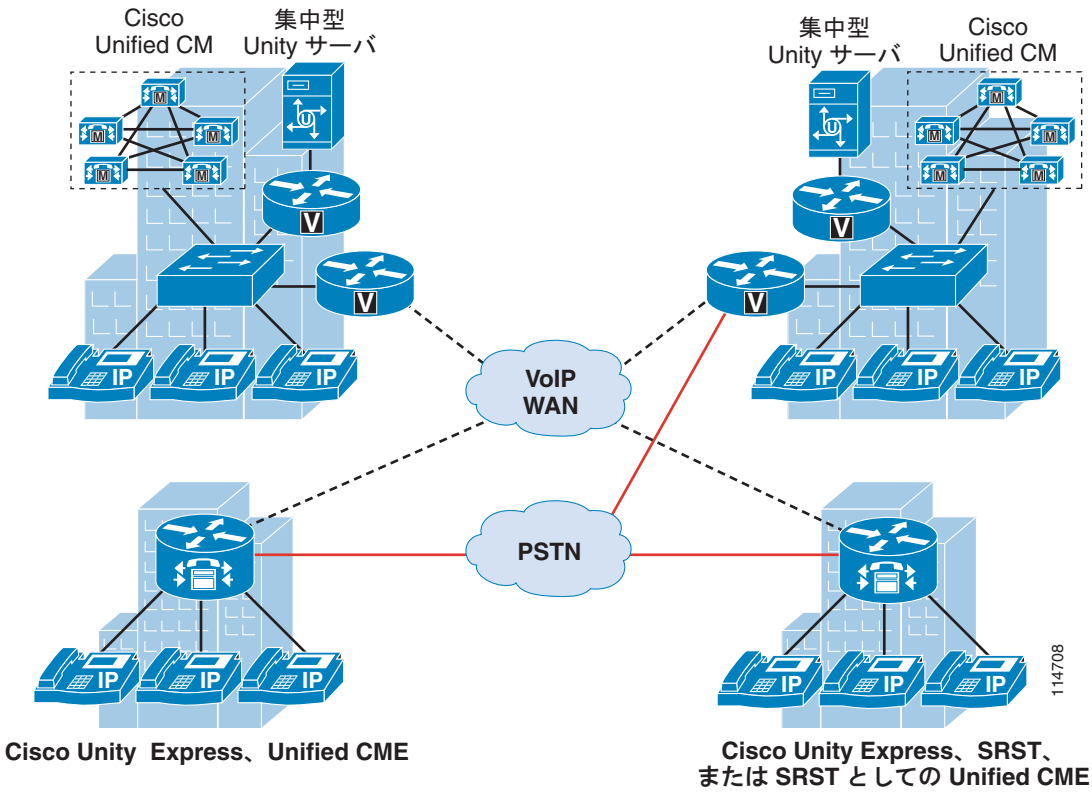


図 13-12　分散型コール処理配置における Cisco Unity Express



Cisco Unity Express を使用した最も一般的な配置モデルは、集中型コール処理を使用したマルチサイト WAN モデルです。このモデルでは、Cisco Unity Express が、小規模なリモート オフィスでボイスメール機能を提供し、中央の Cisco Unity システムが本社および大規模なリモート サイトにボイスメール機能を提供します。

Unified CM ネットワーク配置に次の条件のいずれかが該当する場合は、分散型ボイスメール ソリューションとして Cisco Unity Express を使用してください。

- WAN の可用性にかかわらず、ボイスメールと AA アクセスのサバイバビリティを確保する必要がある。
- 利用可能な WAN の帯域幅が不十分なために、WAN を介して中央のボイスメール サーバにアクセスするボイスメール コールがサポートできない。
- ローカル コミュニティに対して割り当てられている AA または 支店サイトの公衆網の電話番号のカバレッジが地域的に制限されているため、市外通話料金を支払わずにこれらの番号をダイヤルして中央の AA サーバに接続できない。
- 公衆網を使用して支店にかけた場合、コールが支店の AA から同じ支店内の内線番号に転送される可能性が高い。
- 経営理念上、リモート オフィスが、独自のボイスメールや AA テクノロジーを選択することを許可されている。

集中型または分散型の Unified CM 配置では、Cisco Unity Express に対して次の特徴とガイドラインが適用されます。

- 単一の Cisco Unity Express は、単一の Unified CM クラスタに統合できます。

- Cisco Unity Express は、JTAPI アプリケーションと コンピュータ/テレフォニー インテグレーション（CTI）Quick Buffer Encoding（QBE）プロトコルを使用して、Unified CM に統合できます。CTI ポートと CTI ルート ポイントは、Cisco Unity Express ボイスメールと自動応答（AA）アプリケーションを制御します。
- Cisco Unity Express は、Skinny Client Control Protocol（SCCP）を実行する Cisco Unified IP Phone に、ボイスメール機能を提供します。Cisco Unity Express 2.3 以降のリリースは、Unified CM 5.*x* 以降のリリースを使用した Session Initiation Protocol（SIP）の IP 電話もサポートします。
- Cisco Unity Express 対応の Unified CM には、次の CTI ポートが定義されています。
  - 自動応答機能エントリ ポイント（Cisco Unity Express は、最大 5 つの異なる AA を設定できるので、ルート ポイントも最大 5 つまで必要になることがあります）
  - ボイスメールのパイロット番号
  - グリーティング管理システム（GMS）パイロット番号（オプション。GMS を使用しない場合は、このルート ポイントを定義する必要はありません）
- Cisco Unity Express 対応の Unified CM には、次の CTI ルート ポイントが定義されています。
  - 12 または 25 のメールボックス システム（4 ポート）
  - 50 のメールボックス AIM-CUE システム（6 ポート）
  - 250 のメールボックス NME-CUE システム（24 ポート）
- 各 Cisco Unity Express サイトには、最大 250 のメールボックスがあります。250 を超えるメールボックスを配置する場合は、Cisco Unity またはその他のボイスメール ソリューションの使用を検討してください。
- 各 Cisco Unity Express メールボックスは、必要に応じて最大 2 つの異なる内線に関連付けることができます。
- Cisco Unity Express と共に配置されたオフィスでは、自動応答機能をそのオフィスに置くことも（Cisco Unity Express の AA アプリケーションを使用）、中央サイトに置くことも（ボイスメールのみに Cisco Unity Express を使用）できます。
- Cisco Unity Express は、Voice Profile for Internet Mail (VPIM) version 2 経由で、他の Cisco Unity Expresses または Cisco Unity とネットワーク接続できます。これにより、Cisco Unity Express サブスクライバは、別のリモート Cisco Unity Express または Cisco Unity サブスクライバとの間で、メッセージの送受信や転送を行うことができます。
- Cisco Unity Express では、フェールオーバー用の Unified CM を最大 3 つまで指定できます。3 つの Unified CM のいずれにも IP 接続できなくなった場合、Cisco Unity Express は、Survivable Remote Site Telephony（SRST）コール シグナリングに切り替えて、AA 応答サービス、IP 電話へのメールボックス アクセス、および支店に着信する公衆網コールを提供します。
- Cisco Unity Express の自動応答機能は、内線によるダイヤルと名前によるダイヤルの機能をサポートしています。内線によるダイヤルの操作では、発信側が、ネットワーク内の任意のユーザ エンドポイントにコールを転送できます。名前によるダイヤル操作では、Cisco Unity Express 内部のディレクトリ データベースを使用し、外部の LDAP や Active Directory データベースとのインタラクションを行いません。
- Unified CM を使用した集中型 Cisco Unity Express はサポートされていません。
- Cisco Unity Express は、SIP 電話を制御する Cisco Unified CM や Unified CME がない純粋な SIP ネットワークではサポートされません。
- Cisco Unity Express は、Unified CME または SRST ルータ、あるいは公衆網ゲートウェイと別のルータ上に配置できます。

- Unified CME または SRST 以外のルータ上に Cisco Unity Express を配置する場合、コマンド、**allow-connections h323 to sip** を使用して H.323 から SIP へのルーティングを行います。

図 13-13 は、Unified CM と Cisco Unity Express の間のコール フローに関係するプロトコルを示します。

図 13-13　Cisco Unity Express と Unified CM の間で使用されるプロトコル

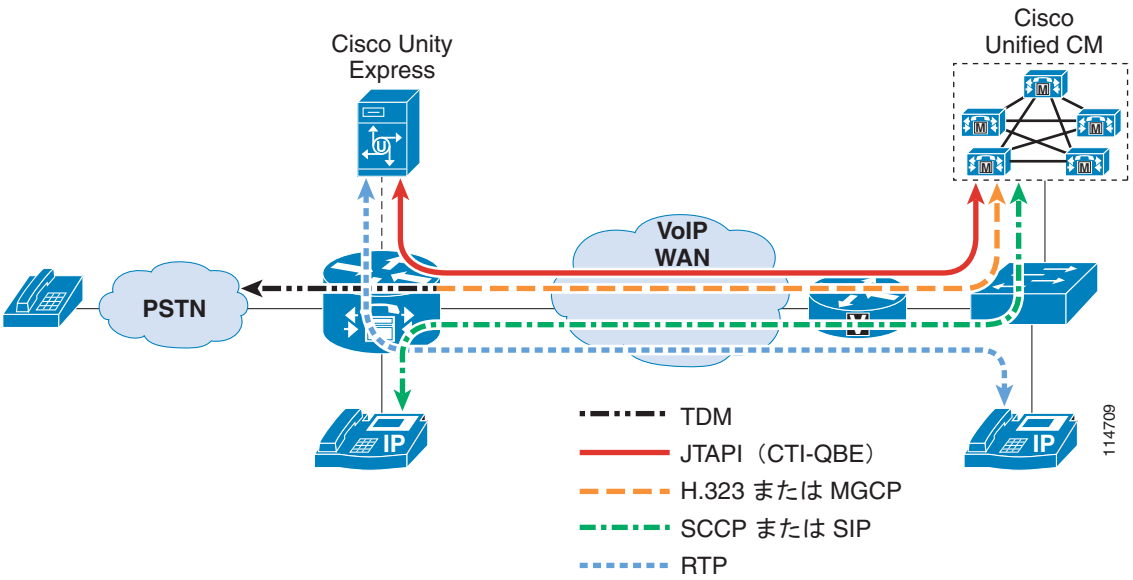


図 13-13 は、次のシグナリングとメディア フローを示しています。

- 電話機は、Unified CM から SCCP または SIP を介して制御されます。
- Cisco Unity Express は、Unified CM から JTAPI（CTI-QBE）を介して制御されます。
- 電話機の Message Waiting indicator（MWI; メッセージ待機インジケータ）は、メールボックスの内容の変化を CTI-QBE 経由で Unified CM に伝達する Cisco Unity Express と、それに対してランプの状態変更の MWI メッセージを電話機に送信する Unified CM によって制御されます。
- 音声ゲートウェイは、H.323、SIP、または MGCP 経由で Unified CM と通信します。
- Real-Time Transport Protocol（RTP）ストリーム フローは、エンドポイント間の音声トラフィックを搬送します。

図 13-14 は、WAN リンクがダウンした場合に、SRST または SRST モードの Unified CME のルータと Cisco Unity Express の間のコール フローに関係するプロトコルを示しています。

図 13-14　Cisco Unity Express と SRST または SRST モードの Unified CME のルータの間で使用されるプロトコル

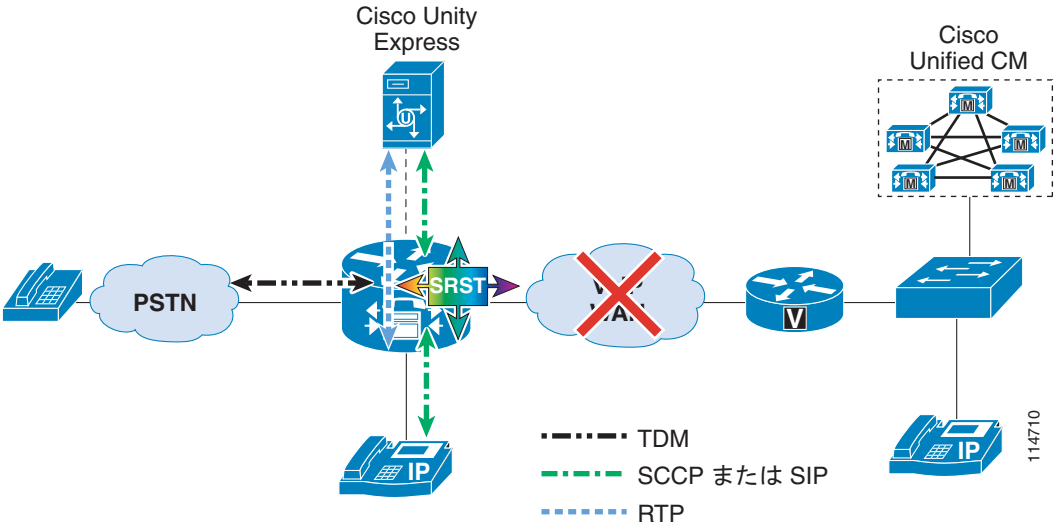


図 13-14 は、次のシグナリングとメディア フローを示しています。

- 電話機は、SRST または SRST モードの Unified CME のルータから SCCP または SIP 経由で制御されます。
- Cisco Unity Express は、内部 SIP インターフェイス経由で SRST ルータと通信します。
- 以前のリリースの Cisco Unity Express では、SRST モードでの MWI の変更はサポートされていませんが、通常動作で音声メッセージを送信および検索することができます。しかし、Unified CM に電話機を再登録するまで、電話機の MWI ランプはそのままです。その時点で、すべての MWI ランプの状態が、ユーザの Cisco Unity Express ボイスメール ボックスの現在の状態に自動的に再同期されます。Cisco Unity Express 3.0 以降のリリースでは、SRST モードで MWI がサポートされています。
- Cisco Unity Express 2.3 以降のリリースでは、Unified CME と SRST モードの両方で、MWI 通知を生成する SIP Subscriber/Notify と Unsolicited Notify をサポートするようになりました。
- RTP ストリーム フローは、エンドポイント間の音声トラフィックを搬送します。
- SRST は、MWI 通知を受信するように登録された 各 ephone-dns の MWI について、Cisco Unity Express にサブスクライブします。

（注）　Unified CM MWI（JTAPI）は、SIP MWI 方式に依存しません。

FAX 配置

FAX 配置は、Unified Communications の実装の重要な側面です。ここでは、FAX 配置や統合のすべての側面を網羅する意図はなく、初歩的な知識だけを紹介します。Cisco Unity や Unity Connection を使用した FAX 配置については、これらの製品に関する FAX 統合や FAX 配置を詳細に説明する他のドキュメントへの参照を示します。この項で主眼となるのは、Cisco Unity Express の FAX 配置です。

Cisco Unity と Unity Connection の FAX 配置

Cisco Unity 7.*x* は、数多くの FAX 統合をサポートします。サポートされている FAX 統合の詳細については、http://www.cisco.com で入手可能な『*Cisco Unity Install and Upgrade Guide*』を参照してください。

Cisco Unity Connection 7.*x* は、Cisco Fax Server をサポートしています。詳細については、http://www.cisco.com で入手できる『*Design Guide for Cisco Unity Connection*』を参照してください。

Cisco Unity Express の FAX 配置

Cisco Unity Express 3.0 以降のリリースでは、FAX の発着信が両方サポートされています。発信 FAX では、FAX を FAX マシンに出力できます。Cisco Unity Express では、音声コールと FAX コールの両方に単一の DID 番号番号を使用することも、別の DID 番号を使用することもできます。単一の DID 番号のアプローチでは、すべてのユーザがボイスメールと FAX の両方に対して 1 つの番号を使用します。異なる DID 番号の場合は、各ユーザに FAX 用と音声内線用の 2 つの番号が提供されます。いずれの場合も、音声メッセージと FAX メッセージの両方が、同じメールボックスに格納されます。

FAX のサポートは、Cisco IOS ゲートウェイの T.37 FAX サポートに依存しています。T.37 Store-and-Forward Cisco IOS FAX ゲートウェイは、オンランプ処理とオフランプ処理で構成される T.37 Store-and-Forward FAX アプリケーションを使用します。Cisco Unity Express は、単一 DID 機能は FAX 検出アプリケーションによってサポートしますが、FAX とボイス メールに異なる DID を使用する場合は、FAX ゲートウェイ上にオンランプ アプリケーションを設定する必要があります。オンランプ ゲートウェイとして動作する Cisco FAX ゲートウェイは、エンドユーザから FAX を受信して TIFF ファイルに変換し、標準の Multipurpose Internet Mail Extension（MIME）電子メール メッセージを作成して TIFF ファイルを添付した後、指定された SMTP サーバ（Cisco Unity Express）にその FAX メール メッセージを転送して保管します。オフランプ ゲートウェイは、POTS をダイヤルしてリモートの FAX マシンと通信することにより、ネットワークから FAX マシン（G3 FAX デバイス）または公衆網に発信されるコールを処理します。

Cisco IOS FAX ゲートウェイは、次の FAX 機能をサポートします。

- FAX パススルーとアップスピード付き FAX パススルー
- Cisco FAX リレー
- T.38 FAX リレー
- T.37 Store-and-Forward FAX
- FAX 用 IVR アプリケーション

オンランプまたはオフランプ FAX 処理は、同じゲートウェイ上にも、異なるゲートウェイ上にも置くことができます。

（注）　Cisco Unity Express は、Cisco IOS FAX ゲートウェイのみをサポートします。サードパーティ製の FAX ゲートウェイは、サポートされていません。

Cisco IOS FAX ゲートウェイの機能の詳細については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

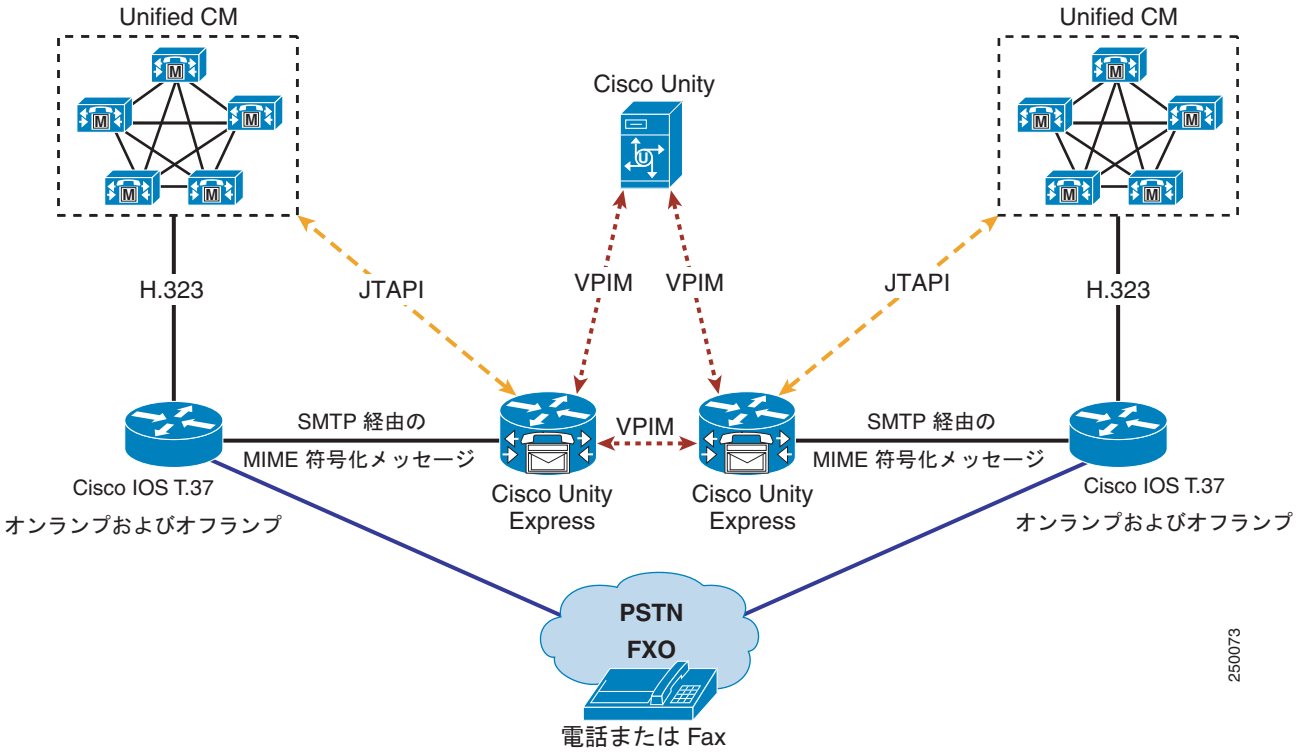
Cisco Unity Express は、次の FAX 配置シナリオをサポートします。

- Cisco Unity Express、オンランプ、およびオフランプ アプリケーションが、すべて同じ音声ゲートウェイに存在する。
- Cisco Unity Express とオンランプ アプリケーションは同じ音声ゲートウェイにあるが、オフランプ アプリケーションが別の音声ゲートウェイ上で実行される。
- Cisco Unity Express とオフランプ アプリケーションは同じ音声ゲートウェイにあるが、オンランプ アプリケーションが別の音声ゲートウェイ上で実行される。
- Cisco Unity Express、オンランプ アプリケーション、およびオフランプ アプリケーションが、それぞれ別の音声ゲートウェイ上で実行される。

（注）　着信 FAX コールの同じゲートウェイに、Cisco Unity Express の複数のインスタンスを統合できません。

図 13-15 では、Unified CM を使用した Cisco Unity Express の FAX 配置シナリオの例を示しています。

図 13-15　Unified CM を使用した Cisco Unity Express の FAX 配置シナリオ



コールが FAX コールの場合、Cisco Unity Express が Unified CME と Unified CM のいずれと統合されているかにかかわらず、発信 Multimedia Mail over IP（MMoIP; マルチメディア メール オーバー IP）ダイヤル ピアが、FAX を TIFF ファイルが添付された電子メール メッセージに変換し、そのメッセージを SMTP 経由で Cisco Unity Express に送信します。

Cisco Unity Express は、FAX 検出アプリケーションを使用して、単一 DID 機能をサポートします。FAX 検出アプリケーションが持つ制限のため、次のいずれかが発生すると、FAX コールが切断され、FAX の再送信が必要となります。

- アプリケーションがそれを FAX コールだと検出する前に、FAX コールがピックアップされて切断された。
- エンドユーザがコールをピックアップし、CNG（FAX）トーンを聞いてコールを FAX（MMoIP）ダイヤル ピアに転送しようとした。

FAX コールと音声コールに別の DID を 使用する場合は、FAX ゲートウェイ上にオンランプ アプリケーションを設定することをお勧めします。

Cisco Unity Express と Unified CM を使用して FAX 機能を配置する場合、次の特徴とガイドラインが適用されます。

- Cisco Unity Express は、アナログ FAX マシンからの FAX サービスのみをサポートします。
- 管理者は、FAX サポートを必要とするメールボックスで、FAX を有効にする必要があります。
- FAX とボイスメールの両方に単一の DID を使用するシナリオのサポートに必要な FAX 検出アプリケーションは、発信側ゲートウェイ上で実行する必要があります。
- Cisco Unity Express は、VPIM エンコードされたボイス メッセージまたは FAX を、ネットワーク上にあるもう一方の Cisco Unity Express または Cisco Unity サーバに SMTP 経由で送信します。
- Cisco Unity Express は、Unified CME と Unified CM のいずれと統合されている場合でも、Cisco Unity との相互運用によって、Cisco Unity との間で FAX メッセージと音声メッセージを VPIM 経由で送受信および転送することができます。
- FAX メッセージは、システム レベルで設定されている FAX 番号を使用して出力できます。この番号は、ユーザが Telephony User Interface（TUI; テレフォニー ユーザ インターフェイス）または Voice View Express（VVE）を使用して FAX の出力を試みると表示されます。ユーザはこの番号を変更して、別の FAX マシンに FAX メッセージを出力することができます。
- Cisco Unity Express は、FAX メッセージの同報通信をサポートしていません。
- Cisco Unity Express は、FAX メッセージの配信が遅延または失敗した場合、それぞれ、Delayed Delivery Record（DDR）または Non-Delivery Receipt（NDR）を送信します。
- Cisco Unity Express は、FAX セッションの合計数と同数の合計 TUI セッションをサポートします。
- Cisco Unity Express は、発信 FAX 用に 1 つ、着信 FAX コール用に 1 つの Cisco FAX ゲートウェイと統合します。着信コールと発信コールには、同じゲートウェイを使用することも、別のゲートウェイを使用することも可能です。着信 FAX コールの同じ FAX ゲートウェイに、Cisco Unity Express の複数のインスタンスを統合できません。
- FAX と音声に異なる DID 番号を使用する場合は、ユーザに対して固有の FAX DID 番号を割り当てます。
- Cisco Unity Express は、音声番号でのメールボックス ログインはサポートしていますが、FAX DID 番号でのログインはサポートしていません。
- Cisco Unity Express は、Cisco Unity Express が SRST モードの場合に、FAX 機能をサポートします。SRST モードの Cisco Unity Express は、WAN を介する必要なく、同じ SRST サイト内のユーザ間で FAX 機能が動作します。

ボイスメール ネットワーキング

ここでは、Cisco Unity Express のボイスメール ネットワーキングに関する具体的な考慮事項を取り上げます。また、Cisco Unified Messaging Gateway を使用したボイスメール ネットワーキングのハイレベルな概要についても説明します。Cisco Unity または Cisco Unity Connection のボイスメール ネットワーキングに固有の情報については、http://www.cisco.com で入手可能な『*Design Guide for Cisco Unity*』または『*Design Guide for Cisco Unity Connection*』をそれぞれ参照してください。

ボイスメール ネットワーキングでは、Cisco Unity、Cisco Unity Connection、Cisco Unity Express などのシステム間で、組み込みの Simple Mail Transfer Protocol（SMTP; 簡易メール転送プロトコル）サーバおよび Voice Profile for Internet Mail（VPIM）バージョン 2 プロトコルのサブセットを使用して、ボイスメール メッセージの送受信、返信、転送を行えます。3 つのボイスメール メッセージング製品はすべて、VPIM メッセージングにより、製品間の相互運用性をサポートしています。

Cisco Unity Express のボイスメール ネットワーキング

Cisco Unity Express は、Cisco Unity 4.0.3 以降のリリース、さらには Cisco Unity Connection 1.2 および 2.0 と通信します。Cisco Unity Express は、リモート サイト間のメッセージ配信に、SMTP（RFC 2821）を使用します。Cisco Unity Express ボイスメール ネットワーキングは、次の機能を提供します。

- サブスクライバは、発信側のシステム上でロケーション設定されたリモート Cisco Unity Express または Cisco Unity サブスクライバとの間で、メッセージの送受信や転送を行うことができます。
- サブスクライバはまた、リモート システムから受信したメッセージに対して返信できます。
- サブスクライバは、配布リストの受信者にも、Cisco Unity から発信される個別のメッセージの受信者にもなることができます。

Cisco Unity Express のボイスメール ネットワーキングには、次の特徴と設計上の考慮事項が適用されます。

- Cisco Unity Express ボイスメール ネットワーキングは、既知のロケーション ID とユーザ内線番号によるブラインド アドレスを使用します。
- Cisco Unity Express ボイスメール ネットワーキングは、5 文字のロケーション コード（アドレスの確認のみに使用）によってリモート ロケーションを定義できます。
- メッセージは動的にエンコードされ、SMTP セッションのネゴシエーションによって .wav または G.726 エンコード形式が決定されます。
- Cisco Unity Express ボイスメール ネットワーキングは、G.711 .wav ファイルと G.726 メッセージ エンコードを交換できます。
- 低帯域幅のサイトには、G.726 を使用します。G.726 は、SMTP のネゴシエーションに関係なく、32 kbps Adaptive Differential Pulse Code Modulation（ADPCM; 適応的差分パルス符号変調）形式を強制的に使用します。
- 送信者の音声名は、VPIM メッセージに含めることも、省略することもできます。メッセージに音声名を含めない場合、VPIM メッセージの再生時に、名前の確認として送信者の内線番号とロケーションだけが告げられます。Cisco Unity Express では、特定のリモート ロケーションに対して **send spoken name** が設定されている場合、VPIM メッセージに送信者の音声名が含められます。
- Cisco Unity Express ボイスメール ネットワーキングは、1 時間経過してもメッセージが送信されない場合、送信者に通知します。また、6 時間経過しても配信できない場合、または受信者のメールボックスが一杯か存在しない場合に、Non-Delivery Receipt（NDR）を送信します。
- Cisco Unity Express ボイスメール ネットワーキングは、リモート ロケーション テーブルに定義されたロケーションからの着信セッションのみを受け付ける、組み込みの SMTP サーバを使用します。

- 各 Cisco Unity Express には、メッセージが最終的にそれにルーティングされるように、独自の電子メール ドメイン名またはサブドメイン名を設定する必要があります。
- Cisco Unity を使用したネットワーキングでは、Cisco Unity Express ロケーションに、ドメイン名またはサブドメイン名を設定する必要があります。
- Cisco Unity Express は、6 時間にわたって 15 分ごとに、受信者へのメッセージ配信を試みます（いずれの値も変更できません）。
- 各 Cisco Unity Express では、2 つの SMTP 送受信セッションを同時に使用できます。
- Cisco Unity Express は、合計 500 のリモート サイトをサポートします。

Cisco Unified Messaging Gateway によるボイスメール ネットワーキング

Cisco Unified Messaging Gateway は、Cisco 統合サービス ルータ（ISR）の Cisco ネットワーク モジュール（NME-UMG または NME-UMG-EC）上で実行される Linux ベースのソフトウェアです。Unified Messaging Gateway は、Cisco Unity、Cisco Unity Connection、Cisco Unity Express のハブとして動作して、VPIM v2 ボイスメール システムをハブアンドスポーク構造または階層構造でネットワーク化することができます。このアプローチにより、ボイスメール システム間の VPIM 接続を劇的に削減し、各システムでの設定作業を簡素化できます。各ボイスメール システム（Cisco Unity、Cisco Unity Connection、Cisco Unity Express、または Avaya Interchange）は、それ自体と Cisco Unified Messaging Gateway との接続を設定するだけで十分です。これにより、Unified Messaging Gateway がシステム間のメッセージのルーティングと配信を処理します。中規模から大規模の分散した拠点を持つ企業が、Cisco Unified Communications ソリューションに移行するためには、このエンドツーエンドのメッセージ ネットワーキング機能が必要です。

Cisco Unified Messaging Gateway には、次の利点があります。

- VPIM を使用した複数の自律的ボイスメール ネットワークで、インテリジェント ルーティングを可能にします。
- スケーラブルなボイスメール ネットワークを提供し、VPIM ネットワークを介してサードパーティ製のボイスメール システム（Avaya Interchange など）との相互運用性を確保します。
- ボイスメール VPIM ネットワークの追加や拡張が容易になります。

Cisco Network Module NME-UMG 上で動作する Cisco Unified Messaging Gateway は、最大 250 のノードと 12,500 人のサブスクライバをサポートします。また NME-UMG-EC モジュール上で動作する Unified Messaging Gateway は、最大 1000 のノードと 50,000 人のサブスクライバをサポートします。サブスクライバの数は、Unified Messaging Gateway に登録された 1 つの Cisco Unity Express が 50 人のサブスクライバをサポートすると想定して計算されています。Unified Messaging Gateway のキャパシティは、サポートされる最大ノード数と、サポートされる最大サブスクライバ数の両方が関係し、片方が増加すると、他方が減少します。たとえば、ネットワーク上に多数のサブスクライバを持つ Cisco Unity や Avaya のエンドポイントがある場合、Unified Messaging Gateway に登録できるノードの数は、250（NME-UMG の場合）または 1000（NME-UMG-EC）の場合を大幅に下回ります。

Cisco Unified Messaging Gateway を配置する場合は、次のガイドラインに従ってください。

- NME-UMG モジュールは NME-UMG-EC モジュールにアップグレードできないので、250 ノードを超えることが予想される場合は、ネットワークのアップグレードを前もって計画してください。
- Cisco Unity Express 3.1 以降のリリースは、Cisco Unified Messaging Gateway に自動的に登録し、ディレクトリの情報を交換しますが、Cisco Unity、Cisco Unity Connection、Avaya Interchange は、Unified Messaging Gateway 上で手動でプロビジョニングする必要があります。
- 冗長性のために 2 つの Unified Messaging Gateway（プライマリとバックアップ）を配置します。

- 最大 10,000 ノードの大規模な配置の場合、最大 20 の Messaging Gateway（10 のプライマリと 10 のバックアップ）を配置します。

（注） Cisco Unified Messaging Gateway を使用したボイスメール ネットワーキングは、小規模企業向け Cisco Unified Communications 500 シリーズには該当しません。これは、Cisco Unified Communications 500 シリーズが、分散型環境でわずか 5 つのサイトしかサポートしないからです。

小規模企業向け Cisco Unified Communications 500 シリーズの配置に関する詳細については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

分散型メッセージング ソリューションとしての VPIM の詳細、およびCisco Unified Messaging Gateway の設計上のガイドラインについては、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

ボイス メッセージングのベスト プラクティス

ここでは、これまでに言及されていないが、ソリューションの中で、製品の重要な側面として考慮すべき一般的なベスト プラクティスとガイドラインを説明します。これらのベスト プラクティスとガイドラインは、Cisco Unity および Cisco Unity Connection のグループと、Cisco Unity Express のグループに分けて説明します。

Unified CM を使用した Cisco Unity と Cisco Unity Connection のベストプラクティス

この項の説明は、Cisco Unity と Unity Connection に適用されます。Cisco Unity Express については、「Cisco Unity Express の配置に関するベスト プラクティス」（P.13-42）を参照してください。

帯域幅の管理

Unified CM は、帯域幅を管理するためのさまざまな機能を備えています。リージョン、ロケーション、およびゲートキーパーさえも使用して、Unified CM は、WAN リンクを介して伝送される音声コールの数によって既存の帯域幅がオーバーサブスクリプションの状態になることがなく、音声品質が低下しないことを保証できます。Cisco Unity および Unity Connection は、帯域幅の管理とコールのルーティングを Unified CM に依存しています。コール（音声ポート）が WAN リンクを通過することのある環境に Cisco Unity または Unity Connection を配置する場合、このようなコールはゲートキーパーベースのコール アドミッション制御にとって透過的になります。このような状況は、Cisco Unity または Unity Connection サーバが分散クライアントにサービスを提供している場合（分散型メッセージングまたは分散型コール処理）、または Unified CM がリモートに置かれている場合（分散型メッセージングまたは集中型コール処理）、いつでも発生します。Unified CM は、コール アドミッション制御用のリージョンとロケーションを提供します。

図 13-16 では、集中型メッセージングと集中型コール処理を使用する小規模なサイトで、リージョンとロケーションを連携させて使用可能な帯域幅を管理する方法を示しています。リージョンとロケーションの詳細については、9-1 ページの「コール アドミッション制御」の章を参照してください。

図 13-16　ロケーションとリージョン

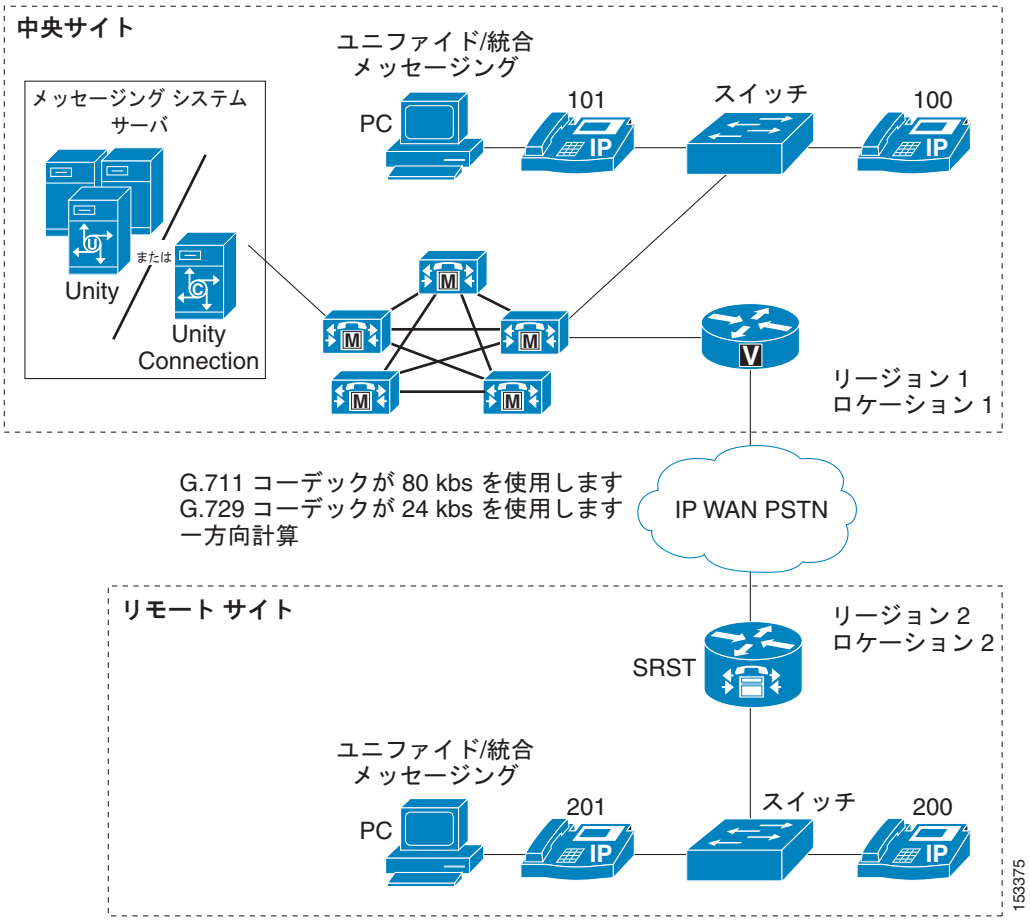


図 13-16 では、リージョン 1 と 2 が、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。ロケーション 1 と 2 は、両方 24 kbps に設定されています。ロケーションの帯域幅は、ロケーション間コールの場合にだけ配分されます。

リージョン内（G.711）コールは、ロケーションの使用可能な帯域幅に対して配分されません。たとえば、内線番号 100 が内線番号 101 をコールする場合、このコールはロケーション 1 の使用可能帯域幅 24 kbps に対して配分されません。ただし、G.729 を使用するリージョン間コールは、ロケーション 1 とロケーション 2 の両方の帯域幅割り当て 24 kbps に対して配分されます。たとえば、内線番号 100 が内線番号 200 をコールすると、このコールは接続されますが、追加の（同時）リージョン間コールでは、リオーダー（ビジー）トーンが聞こえます。

ネイティブ トランスコーディング動作

Cisco Unity と Unity Connection では、IP エンドポイントと Cisco Unity または Unity Connection サーバとの間でコールがネゴシエートされたコーデックと、録音または再生のコーデック形式が異なる場合、ネイティブ トランスコーディングが行われます。コールが G.729 でネゴシエートされ、システム全体の録音形式が G.711 で行われる場合、サーバはそのコールをネイティブにトランスコードする必要があります。Cisco Unity と Unity Connection のネイティブ トランスコーディングは、外部ハードウェア トランスコーダを使用せず、サーバのメイン CPU を使用します。ネイティブ トランスコーディングという名称はここから来ています。

Cisco Unity の動作

デフォルトで、Cisco Unity サーバは、Skinny Client Control Protocol（SCCP）や SIP 経由のテレフォニー統合で、G.711 と G.729 をサポートします。Cisco Unity ではまた、デフォルトのシステム全体のメッセージング録音 形式が G.711 に設定されています。ネイティブ トランスコーディングを無効にするには、システムの録音形式と SCCP または SIP 統合コーデックのアドバタイズメントを同一に設定することをお勧めします。たとえば、Unified CM の SCCP ポートまたは SIP トランクを使用して Cisco Unity を実装する場合、アドバタイズされるコーデックから G.729 を削除して、ポートまたはトランクが G.711 のみをアドバタイズするように設定できます。またデフォルトのシステム全体の録音形式を G.711 のままにすることにより、このシステムとネゴシエートされたすべてのコールが G.711 になり、録音もその形式で行われるため、メッセージング サーバ上でネイティブにトランスコードする必要がなくなります。

Cisco Unity でのネイティブ トランスコーディングの無効化

Cisco Unity での SCCP 統合の場合に限り、Unified CM がハードウェア トランスコーダを音声ポートコールに割り当てるようにするには、レジストリ設定によって、Cisco Unity サーバ上でネイティブ トランスコーディングを無効（オフ）にする必要があります。このレジストリ設定は **Audio - Enable G.729a codec support** と呼ばれます。これを設定するためのツールは、http://www.CiscoUnityTools.com で入手可能な Advanced Settings Tool です（SIP で統合するときに Cisco Unity のネイティブ トランスコーディングを無効にする方法の詳細については、http://www.cisco.com で入手可能な特定の Cisco Unity リリースの『*Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity*』を参照してください。

デフォルトでは、コーデック レジストリ キーが存在しないため、ネイティブ トランスコーディングは有効（オン）です。Advanced Settings Tool により、使用可能な 2 つのコーデックのうちのどちらか 1 つを選択できる新しいレジストリ キーが追加されます。その後、Cisco Unity は、1 つのコーデックだけをサポートすることを Unified CM に「アドバタイズ」します。音声ポートを終端または起点とするコールが、Cisco Unity サーバに設定されているタイプと異なるコーデックを使用している場合、Unified CM はそのコールに外部トランスコーディング リソースを割り当てます。Unified CM 上でトランスコーディング リソースを設定する方法の詳細については、「メディア リソース」（P.6-1）の章を参照してください。

（注）　現在、Unified CM 対応の Cisco Unity TAPI Service Provider（TSP）は、Skinny Client Control Protocol（SCCP）音声ポートに対して G.729 と G.711 mu-law だけをサポートしています（a-law はサポートされていません）。mu-law から a-law への変換には、Unified CM 自体や統合サービス ルータ（ISR）など、ソフトウェアのメディア ターミネーション ポイント（MTP）が必要です。

Advanced Settings Tool を使用して 1 つのコーデックだけをアドバタイズする場合は、Cisco Unity サーバのシステム プロンプトが、使用されるコーデックと同じである必要があります。デフォルトでは、システム プロンプトは G.711 です。コーデックが G.711 に設定されている場合、システム プロンプトは正常に機能します。ただし、G.729 が選択されている場合は、システム プロンプトを変更する必要があります。システム プロンプトを変更する方法の詳細については、http://www.cisco.com で入手可能な『*Cisco Unity System Administration Guide*』を参照してください。システム プロンプトが、レジストリで選択されているコーデックと同じでない場合は、エンド ユーザに、理解不能なシステム プロンプトが聞こえます。

Cisco Unity Connection の動作

Cisco Unity Connection は、Cisco Unity と異なる方法でトランスコーディング操作を処理します。Cisco Unity Connection では、Cisco Unity Connection SCCP または SIP シグナリングによってサポートされているすべてのコーデック形式（G.711 mu-law、G.711 a-law、G.729、iLBC、および G.722）のコールは、常にリニア PCM にトランスコードされます。リニア PCM の録音は、general configuration settings でシステム全体に指定されたシステム レベルの録音形式（リニア PCM、G.711 mu-law/a-law、G.729a、または G.726）にエンコードされます（G.711 mu-law がデフォルト）。したがって、Cisco Unity Connection では、トランスコーディングの全体的な影響が、Cisco Unity の場合と大きく異なります。この章ではこれ以降、発信側デバイスと Unity Connection の間でネゴシエートされるコーデックを「ライン コーデック」、システムレベルの録音形式として設定されたコーデックを「録音コーデック」と呼びます。

トランスコーディングは、本来すべての接続で発生するので、ライン コーデックと録音コーデックが違っても、システムへの影響にほとんど違いはありません。ただし、iLBC または G.722 を使用する場合は例外です。G.722 と iLBC は、トランスコードに要する処理能力が大きいので、システムに対する影響も大きくなります。G.722 と iLBC は、G.711 mu-law の約 2 倍のリソースを必要とします。そのため、G.722 または iLBC 接続の場合、システムは G.711 mu-law 接続の半分しかサポートできません。

原則として、デフォルトのコーデックは G.711 のままにしておくことをお勧めします。設定がディスク容量に制約される場合は、G.729a や G.726 などの低ビット レート コーデックを録音形式として設定できますが、オーディオ品質は G.711 オーディオの忠実度とは異なることに留意してください。また、G.722 がライン上のデバイスで使用されている場合は、リニア Pulse Code Modulation（PCM; パルス符号変調）が、録音のオーディオ品質を高めるオプションです。ただし、この場合はディスク使用量が増加し、ディスク容量に影響を及ぼします。

また録音コーデックを変更したり、特定のライン コーデックのみをアドバタイズしたりする理由がいくつかあります。SCCP 統合または SIP 統合の際に、システムレベルの録音形式やアドバタイズされるコーデックについて決定する場合は、次の要因を検討してください。

- 大部分のエンドポイントと Cisco Unity Connection の間で、どのコーデックがネゴシエートされるか。これは、Cisco Unity Connection によるアドバタイズメントが必要なコーデックとそうでないコーデックの判断に役立ちます。次に、たとえば多くのクライアントを G.722 や iLBC によって Cisco Unity Connection に接続する必要がある場合など、大きな処理能力を必要とする Cisco Unity Connection のネイティブ トランスコーディングの代わりに、Unified CM が、ハードウェア トランスコーディング リソースを提供する必要がある場合を決定することができます。
- どのタイプの GUI クライアント（Web ブラウザ、電子メール クライアント、メディア プレーヤーなど）で録音を取得するか、またその GUI クライアントはどのコーデックをサポートするか。
- 選択したコーデックは、どの程度の品質のサウンドを生成するか。コーデックの中には、他のコーデックより高品質なものがあります。たとえば、G.711 は G.729a より品質が高く、高い音質が求められる場合に適切です。
- 1 秒間の録音にどの程度のディスク容量が必要か。

表 13-4 では、Cisco Unity Connection がサポートするコーデック形式の特徴を概観します。

表 13-4　コーデックの特徴

録音形式（コーデック）	オーディオ品質	サポート状況	ディスク容量（帯域幅）
リニア PCM	高品質	広範なサポート	16 kbps
G.711 mu-law および a-law	中程度の品質	広範なサポート	8 kbps
G.729a	低品質	限定的なサポート	1 kbps
G.726	中程度の品質	中程度のサポート	3 kbps

Cisco Unity Connection が SIP または SCCP ポートでサポートするコーデックをアドバタイズする方法を変更するには、Cisco Unity とは異なる設定を行います。Cisco Unity Connection がコーデックをアドバタイズする方法の変更の詳細については、『*System Administration Guide for Cisco Unity Connection*』を参照してください。アドバタイズするコーデックとして選択できるのは、G.711 mu-law、G.711 a-law、G.729、iLBC、および G.722 です。また優先順位の高い順にコーデックを記載したリストもあります。SCCP 統合では、コーデックがアドバタイズされ、ネゴシエートされるコールのポートとデバイスのロケーションに基づいて Unified CM がコーデックをネゴシエートするので、コーデックの順序は意味を持ちません。しかし SIP 統合では、順位のリストが意味を持ちます。コーデックに優先順位を設定にすると、Cisco Unity Connection は両方のプロトコルをサポートするものの、指定された一方のみの使用が適していることをアドバタイズします。

Cisco Unity Connection Administration でシステムレベルの録音形式を変更する方法の詳細については、『*System Administration Guide for Cisco Unity Connection*』をそれぞれ参照してください。

Unified CM との統合

Cisco Unified CM は、Cisco Unity と Unity Connection のどちらにも SCCP または SIP で統合できます。ここでは、電話機、SIP トランク、および音声ポートに関して、その統合の詳細を説明します。

テレフォニー統合

Cisco Unity は、複数の異なるテレフォニー統合をサポートするので、ユーザを特定のテレフォニー統合に関連付けることができます。メッセージ待機インジケータ（MWI）ポートも特定の統合に関連付けられるので、その特定の統合に関連付けられたポートを通じて MWI 要求が行われます。

Cisco Unity Connection でも、この機能はほぼ同じです。ユーザは、1 つ以上のポート グループを含む電話機システムに関連付けられます。ポート グループは、MWI ポートに関連付けられているので、MWI 要求は、その特定のポート グループに関連付けられたポートを通じて行われます。

Cisco Unity テレフォニー統合は、Cisco Unity Telephony Integration Manager（UTIM）によって設定し、Cisco Unity Connection の電話システムとポート グループは、System Administrator によって設定します。

Cisco Unity と Unity Connection がサポートできるテレフォニー統合の数が無制限になり、システムあたりのポート数によってのみ制限されるようになりました。この機能は、SCCP 統合と SIP 統合のいずれでも同じ方法で動作します。詳細については、http://www.cisco.com で入手可能な該当する Cisco Unity または Cisco Unity Connection のアドミニストレーション ガイドを参照してください。

複数クラスタを接続するオプションとして、クラスタごとに Cisco Unity に統合を追加するという方法と別に、Unified CM は Annex M.1（Message Tunneling for QSIG のメッセージ トンネリング）をサポートしています。これにより、管理者は、Unified CM クラスタの間にあるクラスタ間トランク（ICT）で QSIG を有効にすることができます。ICT で QSIG を有効にすると、複数のクラスタがサポートされている場合でも、Cisco Unity は 1 つの Unified CM クラスタのみに統合され、この 1 つのクラスタでのみ、MWI をオン / オフするポートを指定する必要があります。Unified CM の Annex M.1 機能によって、MWI 要求をそれらの ICT 経由で伝搬し、適切な Unified CM クラスタとそのクラスタ内の電話機に伝達できます。他のクラスタから発信されたすべてのコールは、その 1 つのクラスタに統合された Cisco Unity サーバに転送できます。ICT で Annex M.1 が有効になっていれば、他のクラスタで MWI ポートを指定する必要はありません。

Annex M.1 の詳細については、http://www.cisco.com で入手可能な『*Cisco Unified Communications Manager System Guide*』を参照してください。

拡張メッセージ待機インジケータ（eMWI）

Enhanced Message Waiting Indicator（eMWI; 拡張メッセージ待機インジケータ）は、従来の MWI の拡張機能であり、音声メッセージ数を視覚的に示します。従来の MWI は、新しい音声メッセージの着信時またはユーザのボイスメール ボックスからの削除時に電話機のメッセージ ランプをオンまたはオフにするという、2 値形式で機能します。eMWI は、Cisco Unity および Cisco Unity Connection の両方で機能し、Cisco Unified IP Phone 8900 および 9900 シリーズの SIP 電話機でサポートされています。

（注）　Cisco 8900 および 9900 シリーズの SIP 電話機は、Cisco Unified Communications Manager 7.1.3 以降のリリースでサポートされています。詳細については、http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html で入手可能な『*Cisco Unified Communications Manager Software Compatibility Matrix*』を参照してください。

eMWI は、ユーザのボイスメール ボックス内の再生されていないメッセージを視覚的に示します。メッセージのステータスは色で示されます。再生されていないメッセージは、電話機の画面上に赤で示されます。eMWI は、SIP と SCCP の統合によって、Cisco Unity と Cisco Unity Connection の両方の Unified CM でサポートされます。eMWI は、システムが SRST または SRSV モードで動作している場合は機能しません。Cisco Unity Connection との統合では、Cisco Unity Connection サーバ上に保存されたメッセージだけが eMWI で示され、外部 IMAP サーバに保存されたメッセージは示されません。

eMWI は、Unified CM を使用する分散型コール処理環境で機能します。1 つのクラスタによってクラスタ間トランク（H.323 または SIP）を介したボイス メッセージング サーバへの接続を提供する、分散型コール処理と集中型ボイス メッセージングが統合されたシステムでは、クラスタ間トランクを介した eMWI の更新がサポートされ、エンド デバイスに表示されます（図 13-17 を参照）。

（注）　eMWI は、クラスタ間トランク（H.323 または SIP）を介した集中型メッセージングを使用する分散型コール処理環境でも機能します。

図 13-17　拡張メッセージ待機インジケータ（eMWI）

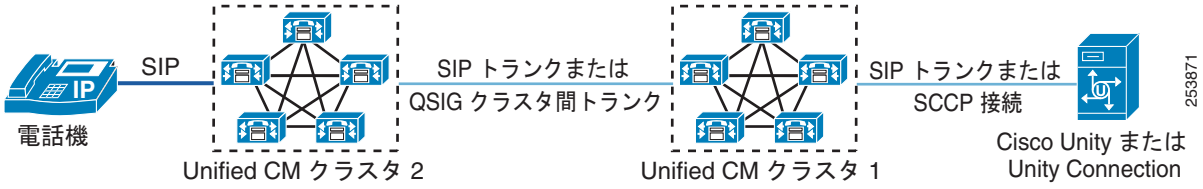


図 13-18 は、集中型ボイス メッセージングを使用する分散型コール処理環境でのクラスタ間トランク（H.323 または SIP）を介した eMWI を示しています。

図 13-18　分散型コール処理および集中型ボイス メッセージングを使用した eMWI

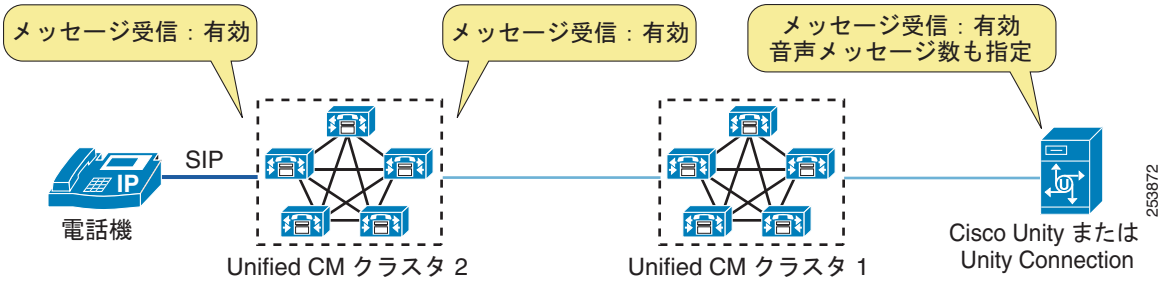


図 13-18 に示すように、クラスタ 2 およびその音声メッセージング ソリューションでは eMWI をサポートしていますが、クラスタ 1 ではサポートしていません。音声メッセージ数を含む eMWI 更新が、音声メッセージング ソリューションからクラスタ 2 の電話機に送信された場合、クラスタ 1 は、音声メッセージ数を含まない、標準の MWI だけをクラスタ 2 に転送します。

eMWI には、次のガイドラインが適用されます。

- すべてのクラスタで eMWI がサポートされている必要がある。内部クラスタで eMWI がサポートされていない場合、着信側のクラスタは、ボイスメール数が含まれていない、標準の MWI だけを受信します。
- 標準の MWI では、ランプ状態の変更（オンまたはオフ）だけを送信するため、大量のトラフィックは生成されない。ただし、eMWI を有効化すると、メッセージング システムからのメッセージ数も送信されるため、トラフィック量が増える可能性があります。トラフィック量は、メッセージ数および変更通知数によって変わります。

ボイスメール統合のための Unified CM SIP トランクの設定

Cisco Unified CM は、回線側 デバイスの SIP のサポートに加え、トランク側の SIP もサポートしています。このような機能により、Unified CM は SIP で直接 Cisco Unity および Unity Connection と統合できるようになり、SIP プロキシ サーバが必要なくなりました。

ただし、Unified CM は SIP トランクを介したボイスメールの直接統合が可能ですが、Skinny Client Control Protocol（SCCP）ポートと同じ Voicemail Port Wizard を持っていません。ある程度の手動設定が必要です。基本的な統合シナリオでは、SIP トランクの設定に次の手順が必要です。

ステップ 1　Unified CM Administration で SIP プロファイルを作成します。それには、[Device] > [Device Setting] > [SIP Profile] の順に選択します。

このとき、ボイスメール統合に固有のものは特にありませんが、管理機能を簡単にし、一貫したものにするため、実際のボイスメール統合に固有の SIP プロファイルを作成し、それに応じた名前を付けるようにしてください。

ステップ 2　Unified CM Administration で SIP トランク セキュリティ プロファイルを作成します。それには、[System] > [Security Profile] > [SIP Trunk Security Profile] の順に選択します。

SIP トランク セキュリティ プロファイルの着信ポート番号はボイスメールに固有のもので、Cisco Unity または Unity Connection サーバが Unified CM クラスタへの接続に使用する SIP ポート番号の数値です。また、[Accept Unsolicited Notification] をオン（有効）にし、Cisco Unity および Unity Connection が Unified CM に Message Waiting Indicator（MWI）イベントを通知できるようにします。

（注）　MWI 機能は Unsolicited NOTIFY で処理されます。SIP 統合で MWI DN を設定する必要はありません（MWI DN は、SCCP 統合に必要です）。

ステップ 3　Unified CM Administration で SIP Trunk を作成します。それには、[Device] > [Trunk [Add New]] の順に選択します。トランクの作成ページで、設定済みの SIP Profile と SIP Trunk Security Profile を対応するフィールドに指定します。また、Unity または Unity Connection サーバを宛先アドレスに設定し、[Unattended Port] をオンに（有効に）します。[Redirecting Number IE Deliver - Outbound] もオンに（有効に）します。

（注）　Unattended Port の例外として、複数の Cisco Unity サーバを 1 つの Unified CM クラスタに接続し、ライブ応答またはクロスサーバ ログオンが設定されている場合があります。このシナリオでは、Unattended Port をオフ（無効）のままにすると、あるサーバのボイスメール ポートからのコール転送が、他のサーバで終端されるようにできます。現在のところ、この例外は Unity だけに適用されます。

ステップ 4　ルート パターンを作成し、ボイスメール SIP トランクを宛先として指定します。

ステップ 5　ステップ 4 で設定したルートパターンと同じ番号のボイスメール パイロット番号を作成します。

ステップ 6　対応するボイスメール パイロット番号を使用して、ボイスメール プロファイルを作成します。

Unified CM クラスタとの音声ポート統合

単一サイト メッセージング環境に Cisco Unity を配置する場合、Unified CM クラスタとの統合は SCCP 音声ポートまたは SIP トランクを介して行われます。Unified CM サブスクライバに障害が発生した場合でも（Unified CM フェールオーバー）、ユーザおよび外部コールが引き続き音声メッセージングにアクセスできるように、設計上の考慮事項には、Cisco Unified CM サブスクライバ間の音声ポートの適切な配置についても考慮する必要があります。（図 13-19 を参照）。

図 13-19　Unified CM クラスタと統合された Cisco Unity サーバ（専用バックアップ サーバなし）

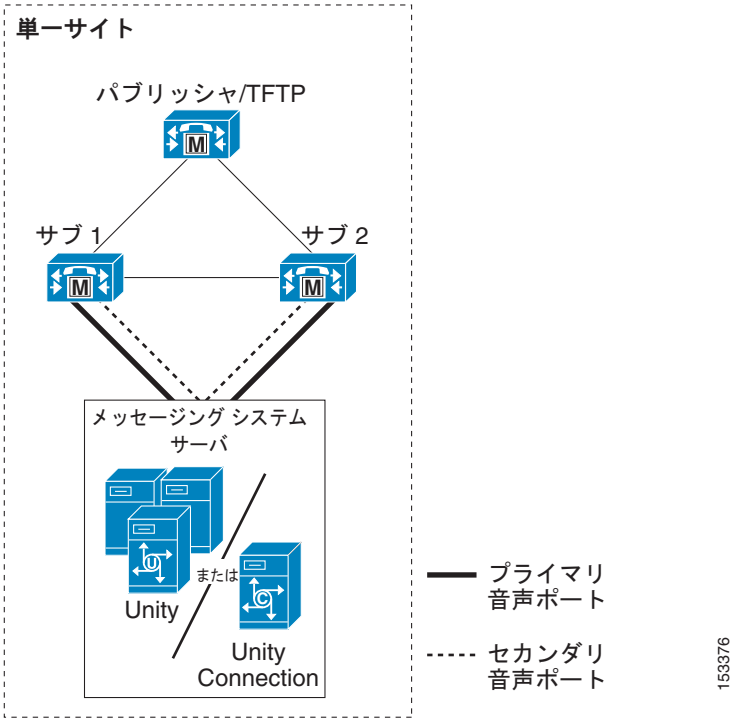


図 13-19 の Unified CM クラスタは、1 対 1 のサーバ冗長性および 50/50 のロード バランシングを採用しています。正常な動作時には、各サブスクライバ サーバがアクティブで、サーバの全コール処理負荷の最大 50% を処理します。1 台のサブスクライバ サーバに障害が発生すると、残りのサブスクライバ サーバが、障害の発生したサーバの負荷を担います。

この設定では、ボイスメール ポートのグループが 2 つ使用され、各グループに、ライセンスのある音声ポートの合計数の半分が含まれています。1 つのグループは、プライマリ サーバが Sub1 で、セカンダリ（バックアップ）サーバが Sub2 になるように設定されています。もう 1 つのグループは、Sub2 がプライマリ サーバで、Sub1 がバックアップになるように設定されています。

MWI 専用ポートや他の特殊なポートが、2 つのグループ間で等しく分散されていることを確認してください。音声ポートの設定中は、命名規則に特に注意してください。Cisco Unity Telephony Integration Manager（UTIM）ユーティリティでポートの 2 つのグループを設定する場合は、必ずデバイス名プレフィックスがグループごとに固有となるようにし、Unified CM Administration でボイスメール ポートを設定するときと同じデバイス名を使用します。この例では、デバイス名プレフィックスがポートのグループごとに固有になっています。グループ Sub1 ではデバイス名プレフィックスとして CiscoUM1 が使用され、Sub2 では CiscoUM2 が使用されています。

着信ボイスメール ポートと発信ボイスメール ポート（MWI、メッセージ通知、および TRaP 用）の比率に関する設計上の詳細情報については、http://www.cisco.com で入手可能な『*Cisco Unity System Administration Guide*』を参照してください。

（注） デバイス名プレフィックスは、ポートのグループごとに固有で、Unified CM Administration に設定されているボイスメール ポートの命名規則と一致する必要があります。

Unified CM Administration では、この例のポートの半分が固有なデバイス名プレフィックス CiscoUM1 を使用して登録されるように設定され、残りの半分が一意のデバイス プレフィックス（CiscoUM2）を使用して登録されるように設定されています（表 13-5 を参照）。表 13-5 に示すように、ポートが Unified CM に登録される場合、半分がサブスクライバ Sub1 に登録され、残りの半分が Sub2 に登録されます。

表 13-5　Unified CM Administration でのボイスメール ポート設定

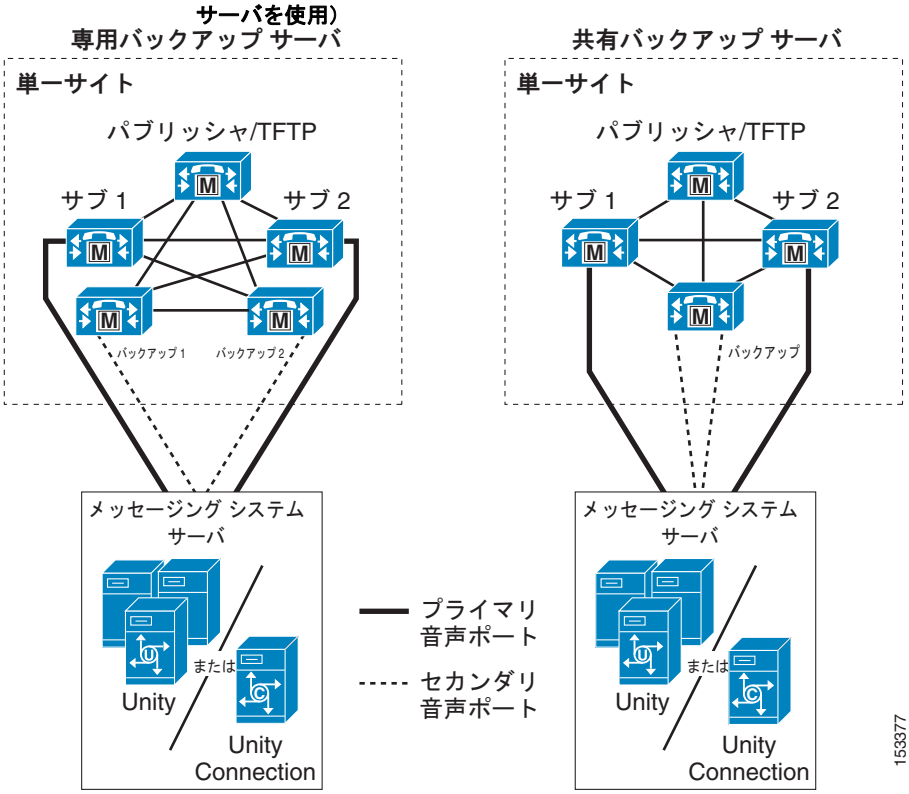
デバイス名	説明	デバイス プール	SCCP セキュリティ プロファイル	ステータス	IP アドレス
CiscoUM1-VI1	Unity1	Default	Standard Profile	sub1 に登録	1.1.2.9
CiscoUM1-VI2	Unity1	Default	Standard Profile	sub1 に登録	1.1.2.9
CiscoUM1-VI3	Unity1	Default	Standard Profile	sub1 に登録	1.1.2.9
CiscoUM1-VI4	Unity1	Default	Standard Profile	sub1 に登録	1.1.2.9
CiscoUM2-VI1	Unity1	Default	Standard Profile	sub2 に登録	1.1.2.9
CiscoUM2-VI2	Unity1	Default	Standard Profile	sub2 に登録	1.1.2.9
CiscoUM2-VI3	Unity1	Default	Standard Profile	sub2 に登録	1.1.2.9
CiscoUM2-VI4	Unity1	Default	Standard Profile	sub2 に登録	1.1.2.9

（注） Unified CM Administration でボイスメール ポートに使用される命名規則は、Cisco UTIM で使用されるデバイス名プレフィックスと一致する必要があります。一致しないと、ポートの登録に失敗します。

専用 Unified CM バックアップ サーバを使用する音声ポート統合

この Unified CM クラスタ構成では、各サブスクライバ サーバが 50% を超えるコール処理負荷で動作できます。各プライマリ サブスクライバ サーバは、専用バックアップ サーバまたは共有バックアップ サーバを持ちます（図 13-20 を参照）。正常な動作時、バックアップ サーバはコールを処理しませんが、サブスクライバ サーバの障害時またはメンテナンス時に、バックアップ サーバはそのサブスクライバ サーバのすべての負荷を担います。

図 13-20　単一の Unified CM クラスタと統合された Cisco Unity サーバ（バックアップ サブスクライバ サーバを使用）



この場合のボイスメール ポートの設定は、50/50 のロードバランシング クラスタに似ています。ただし、もう 1 台のサブスクライバ サーバをセカンダリ サーバとして使用するように音声ポートを設定せず、個別の共有バックアップ サーバまたは専用バックアップ サーバを使用します。共有バックアップ サーバと共にクラスタ化された Unified CM では、両方のサブスクライバ サーバのセカンダリ ポートが、単一のバックアップ サーバを使用するように設定されます。

音声ポート名（デバイス名プレフィックス）は、Cisco UTIM グループごとに固有で、Unified CM サーバ上で使用されるデバイス名と同じである必要があります。

Cisco Unity でボイスメール ポートを設定するには UTIM ツールを使用します。Cisco Unity Connection では、Unity Connection Administration コンソールの Telephony Integration セクションを使用します。詳細については、http://www.cisco.com で入手可能な Cisco Unity または Cisco Unity Connection のアドミニストレーション ガイドを参照してください。

Cisco Unity Express の配置に関するベスト プラクティス

Cisco Unity Express を配置する場合は、次のガイドラインとベスト プラクティスを使用してください。

- ボイスメールの宛先として Cisco Unity Express を持つ IP 電話が、Cisco Unity Express をホストするルータと同じ LAN セグメントに置かれていることを確認します。
- Cisco Unity Express を使用して配置するサイトで無中断の自動応答機能（AA）と電子メール アクセスが必要な場合は、Cisco Unity Express、SRST、および公衆網の音声ゲートウェイがすべて同じ物理サイトに置かれていることを確認します。Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）やその他の冗長性ルータ設定は、現在、Cisco Unity Express ではサポートされていません。
- 各メールボックスは、プライマリ内線番号とプライマリ E.164 番号に関連付けることができます。通常、この番号は、公衆網の発信者が使用する direct-inward-dial（DID）番号です。プライマリ E.164 番号が他の番号に設定されている場合、SRST モード時に正しいメールボックスに到達するように、Cisco IOS 変換パターンを使用して、プライマリ内線番号かプライマリ E.164 番号に一致させます。

Unified CM とのボイスメール統合

- 各 Cisco Unity Express サイトは、ボイスメール用と AA 用（ライセンスされ、購入している場合）に CTI ルート ポイントを 1 つずつ関連付ける必要があります。またライセンスされた Cisco Unity Express ポートと同じ数の CTI ルート ポイントを設定する必要があります。Cisco Unity Express の数が、「コール処理」（P.8-1）の章に示すスケーラビリティ ガイドラインを超えないことを確認します。
- Cisco Unity Express は、Unified CM 上の JTAPI ユーザに関連付けられます。単一の JTAPI ユーザをシステム内の Cisco Unity Express の複数のインスタンスに関連付けることは可能ですが、Unified CM 内の専用の JTAPI ユーザをそれぞれ単一の Cisco Unity Express に関連付けることをお勧めします。
- Unified CM を以前のバージョンからアップグレードした場合、JTAPI ユーザのパスワードは、Unified CM で自動的にリセットされます。したがって、管理者は、アップグレードの後、JTAPI パスワードが Cisco Unity Express と Unified CM の間で同期化され、Cisco Unity Express を Unified CM に登録できることを確認する必要があります。
- CTI ポートと CTI ルート ポイントは、特定の場所で定義することができます。Unified CM と Cisco Unity Express の間で、ロケーションベースのコール アドミッション制御を使用することをお勧めします。RSVP を使用することもできます。
- Cisco Unity Express と Unified CM の間を通過する WAN のシグナリング トラフィックのための、適切な Quality of Service（QoS）と帯域幅を確保します。各 Cisco Unity Express サイトの CTI-QBE シグナリングのために、20kbps の帯域幅をプロビジョニングします。詳細については、「ネットワーク インフラストラクチャ」（P.3-1）の章を参照してください。
- Unified CM から Cisco Unity Express への CTI-QBE シグナリング パケットは、AF31（0x68）という DSCP 値でマーキングされています。Unified CM は、CTI-QBE シグナリングに TCP ポート 2748 を使用します。
- Unified CM JTAPI ライブラリは、すべての発信 QBE シグナリング パケットに、適正な IP Precedence ビットを設定します。その結果、Cisco Unity Express と Unified CM の間のすべてのシグナリングに、適正な QoS ビットが設定されます。

Cisco Unity Express コーデックと DTMF のサポート

Cisco Unity Express へのコールは、G.711 のみを使用します。ローカルのトランスコーダを使用して、WAN を通過する G.729 コールを G.711 コールに変換することをお勧めします。Unified CM リージョンは、リージョン内コールに G.711 音声コーデックを、リージョン間コールに G.729 音声コーデックを使用するように設定できます。

Cisco Unity Express サイトにトランスコーディング機能がない場合、必要な数の G.711 ボイスメールに対応する十分な帯域幅を WAN 上にプロビジョニングします。IP 電話と Cisco Unity Express デバイス（CTI ポートと CTI ルート ポイント）の間のコールに G.711 音声コーデックを使用するように、Unified CM リージョンを設定します。

Cisco Unity Express は、DTMF リレーのみをサポートし、インバンド DTMF トーンはサポートしていません。Cisco Unity Express では、DTMF は、SIP または JTAPI のいずれかの呼制御チャネルを介してアウトオブバンドで搬送されます。Cisco Unity Express 2.3 は、RFC 2833 を使用した、Cisco Unity Express への G.711 SIP コールをサポートします。

JTAPI、SIP トランクおよび SIP 電話機のサポート

Cisco Unified CM 5.1 以降のリリースは、SIP トランク プロトコルをサポートしますが、Cisco Unity Express は、Unified CM との通信に JTAPI を使用します。Cisco Unity Express は、SCCP 電話機と SIP 電話機の両方をサポートします。

- SRST を使用できるように SIP トランクを設定し、（JTAPI によって）SIP 電話機をサポートするように Unified CM を設定します。
- Cisco Unity Express 3.0 は、トランスコーダ経由で G.729 SIP コールをサポートします。また Cisco IOS Release 12.3(11)XW で RFC 2833 がトランスコーダをパススルーする能力が追加されています。
- Cisco Unity Express は、Unified CM からのスロースタート コールの場合、コール設定のためのディレイド メディア（delayed media、INVITE メッセージ内に SDP なし）をサポートします。
- Cisco Unity Express は、ブラインド転送と打診転送の両方をサポートしますが、デフォルトの転送モードは、SIP コールで REFER を使用した打診転送（半自動）です。転送モードを、REFER を使用する打診転送または BYE/ALSO を使用するブラインド転送に明示的に変更するには、Cisco Unity Express コマンド ライン インターフェイスを使用します。リモート エンドで REFER がサポートされていない場合は、BYE/ALSO が使用されます。
- Cisco Unity Express は、音声メッセージ通知のためのアウトコールをサポートしています。また、打診転送もサポートしています。これらのいずれのコール設定時でも、Cisco Unity Express は INVITE に対する 3*xx* 応答を受信できます。Cisco Unity Express は、INVITE に対する 301（Moved Permanently）と 302（Moved Temporarily）応答のみを処理します。これには、3*xx* 応答の Contact ヘッダーに含まれ、新しい INVITE の送信に使用する URL が必要です。305（Use Proxy）応答は、サポートされていません。

（注）　Cisco Unified CM 7.*x* または 6.*x* との相互運用性には、少なくとも Cisco Unity Express release 3.2 または 3.0 がそれぞれ必要です。

Cisco Unity Express の詳細については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

CHAPTER 14

Cisco Unified MeetingPlace

この章では、Cisco Unified Communications 環境における Cisco Unified MeetingPlace（Unified MP）のシステム レベルの設計と実装について説明します。Unified MP のシステム設計に関係のない ハードウェア要件やソフトウェア コンポーネント設定については説明しません。このようなトピックについては、http://www.cisco.com で入手可能な Unified MP の製品マニュアルを参照してください。

この章の新規情報

この章を構成する項のほとんどは、初期リリースの Cisco Unified MeetingPlace 7.0 に関する項を再編成して書き直したものです。Unified MP 7.0 のリリース以降に初めてこのマニュアルを読む場合は、この章全体に目を通すことをお勧めします。表 14-1 に、まったく新しいトピックと 7.0 から大幅に変更されたトピックを示します。

表 14-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
WebConnect を使用したマルチサイト Unified MP のサポートが削除されました。	
Reservationless Single Number Access（RSNA）のサポートが 2 台の Unified MP システムに制限されています。	「RSNA に関する設計上の考慮事項」（P.14-6）
Cisco Unified Border Element との SIP 統合は、Unified MP の今後のリリースでサポートされることになりました。	
Unified MP の冗長性に関する情報が更新されました。	「冗長性」（P.14-19）
Unified MP の容量に関する情報が更新されました。	「容量とサイジング」（P.14-14）

Cisco Unified MeetingPlace のコンポーネント

この項では、Unified MP 配置内のさまざまなコンポーネントについて簡単に説明します。

Unified MP アプリケーション サーバ

Unified MP アプリケーション サーバは、Linux オペレーティング システムと IBM Informix Dynamic Server（IDS）データベースを実行している Cisco Media Convergence Server（MCS）7835H2 または 7845H2 プラットフォーム上にインストールされます。このサーバは、マスター コンポーネントとして機能し、他のコンポーネントを制御します。Unified MP アプリケーション サーバによって、SIP B2BUA のサポートと Cisco Unified CM などの他のコール処理デバイスへの SIP 接続が可能になります。Unified MP アプリケーション サーバを使用すれば、Cisco Webex および Simple Message

Transfer Protocol（SMTP）を使用した電子メールや HTTP/HTTPS を使用した Microsoft Outlook などの外部アプリケーションと統合が可能です。LDAP ディレクトリとの統合は、社内ディレクトリと Unified CM の統合を通して実現されます。

Unified MP Web コラボレーション サーバ

Unified MP Web コラボレーション サーバは、ライセンスおよびインストール オプションに応じてさまざまな機能をサポートします。Web スケジューリング、Web 参加者リスト、およびシングル サインオンが基本バンドルの一部として組み込まれています。Unified MP Web コラボレーション サーバは、クラスタ化してスケーラビリティと冗長性を向上させることができます。加えて、Unified MP は、シングル配置において、内部（イントラネット上）と外部（非武装地帯（DMZ）内）の Web サーバ クラスタをサポートします。Unified MeetingPlace では、音声 / ビデオ会議用の共用ライセンス モデルが使用されますが、Web 会議と音声 / ビデオ会議用のライセンス数を同じにする必要はありません。複数の Web サーバを配置した場合のライセンスは、内部と外部のどちらかの Web サーバに関連付けられるのではなく、すべての Web サーバで使用されます。

Unified MP Web コラボレーション サーバは、GWSIM プロトコルを使用して Unified MP アプリケーション サーバと情報をやり取りします。Unified MP アプリケーション サーバと Unified MP Web コラボレーション ソフトウェアをインストールすると、自動的に Unified MP GWSIM がインストールされます。

Unified MP メディア サーバ

Unified MP メディア サーバは、音声 / ビデオ会議を提供するオンボード DSP リソースが搭載された Cisco Unified Videoconferencing 3515 システムと 3545 システムです。Unified MP メディア サーバは、SIP プロトコルと Unified MP メディア制御プロトコルを介して Unified MP アプリケーション サーバから制御されます。Unified MP メディア サーバを配置すると、エンド ユーザは 1 つの共通の番号で音声 / ビデオ会議に接続できます。

Unified MP Notes Gateway

Unified MP Notes Gateway を使用すれば、IBM Lotus Notes Domino サーバと統合して、ユーザ カレンダーを通した Unified MP スケジューリング、通知、および参加が可能になります。このゲートウェイの機能は、Unified MP for Outlook に似ています。主な違いは、Unified MP for Notes がサーバ ベースであるのに対して、Unified MP for Outlook がクライアント ベースであることです。

Unified MP LCS Gateway

Unified MP Live Communications Server（LCS）Gateway を使用すれば、Microsoft Office Communicator ユーザがテキスト ベースのインスタント メッセージング セッションを Unified MP によってホストされたビデオ会議に移行するためのサービスが提供されます。

Unified MP Conference Manager

Unified MP Conference Manager は、Unified MP 上でヘルプデスク タスクを実行するシステム ツールです。このツールを使用すれば、複数の Unified MP システムを接続して、会議の予定や開催を管理できます。Unified MP Conference Manager は、GUI ベースのクライアントです。クライアントと Unified MP アプリケーション サーバ間の通信は、TCP ポートの 80 と 443 上で行われます。

Unified MP 配置モデル

この項では、単一サイト、マルチサイト、単一番号アクセスを含む、さまざまな Unified MP 配置モデルに関する設計上の考慮事項と推奨事項について説明します。配置モデルには多くのバリエーションが存在しますが、ここではすべてのバリエーションを検証するのではなく、基本的な実装だけを紹介します。

単一サイトでの Unified MP の配置

単一サイト配置モデルは、すべてのサーバ コンポーネントとユーザが単一のサイトに設置され、単一の LAN で相互接続される基本配置モデルです（図 14-1 を参照）。このモデルは、Unified MP と Unified CM クラスタが同じ場所に設置され、SIP 経由で統合されます。単一サイト配置モデルには、次のような特徴があります。

- Unified MP メディア サーバをアクティブな Unified MP アプリケーション サーバと同じ場所に設置する必要があります。
- アクティブな Unified MP アプリケーション サーバと Unified MP Web コラボレーション サーバ間の往復遅延は、150 ms 以下にする必要があります。
- 単一サイトでの Unified MP 配置には、Microsoft Exchange、Microsoft LCS、IBM Lotus Notes、Directory Services、Jabber Messenger、および Sametime Connect との統合を含めることができます。
- 「セグメント化会議アクセス オプション」（P.14-7）の項で説明されているように、Segmented Meeting Access を設定することによって、外部 Web 会議アクセスが使用可能になります。単一サイトでは、内部と外部の両方のクラスタ内で Web 会議サーバを設定して容量と冗長性を向上させることができます。
- オプションで、Unified MP の音声、ビデオ、および Web レコーディングと会議添付ファイルを外部の SAN/NAS ストレージ サーバ上に保存できます。
- Unified MP 7.*x* では、サードパーティ製の IP PBX エンドポイントとの直接統合がサポートされていません。サードパーティ製の IP PBX と統合するためには、Unified MP 7.*x* のフロントエンドとして Cisco Unified CM 6.1（2）以降のリリースを配置する必要があります。
- ネットワーク タイム プロトコル（NTP）を実装して、Unified MP コンポーネントのクロックをネットワーク タイム サーバまたはネットワーク対応クロックに同期可能にする必要があります。NTP によって会議の正確なスケジューリングが保証されることから、Unified MP にとって重要なネットワーク サービスと言えます。Unified MP アプリケーション サーバのインストール中に外部の NTP ソースを指定することができます。他の Unified MP コンポーネントは自動的にこのアプリケーション サーバに同期されます。
- 冗長性を向上させるために、単一サイトでの Unified MP 配置を単一または二重のデータセンター環境に配置できます。これについては、「冗長性」（P.14-19）の Unified MP アプリケーション サーバに関する項でさらに詳しく説明します。

図 14-1　単一サイトでの Unified MP の配置

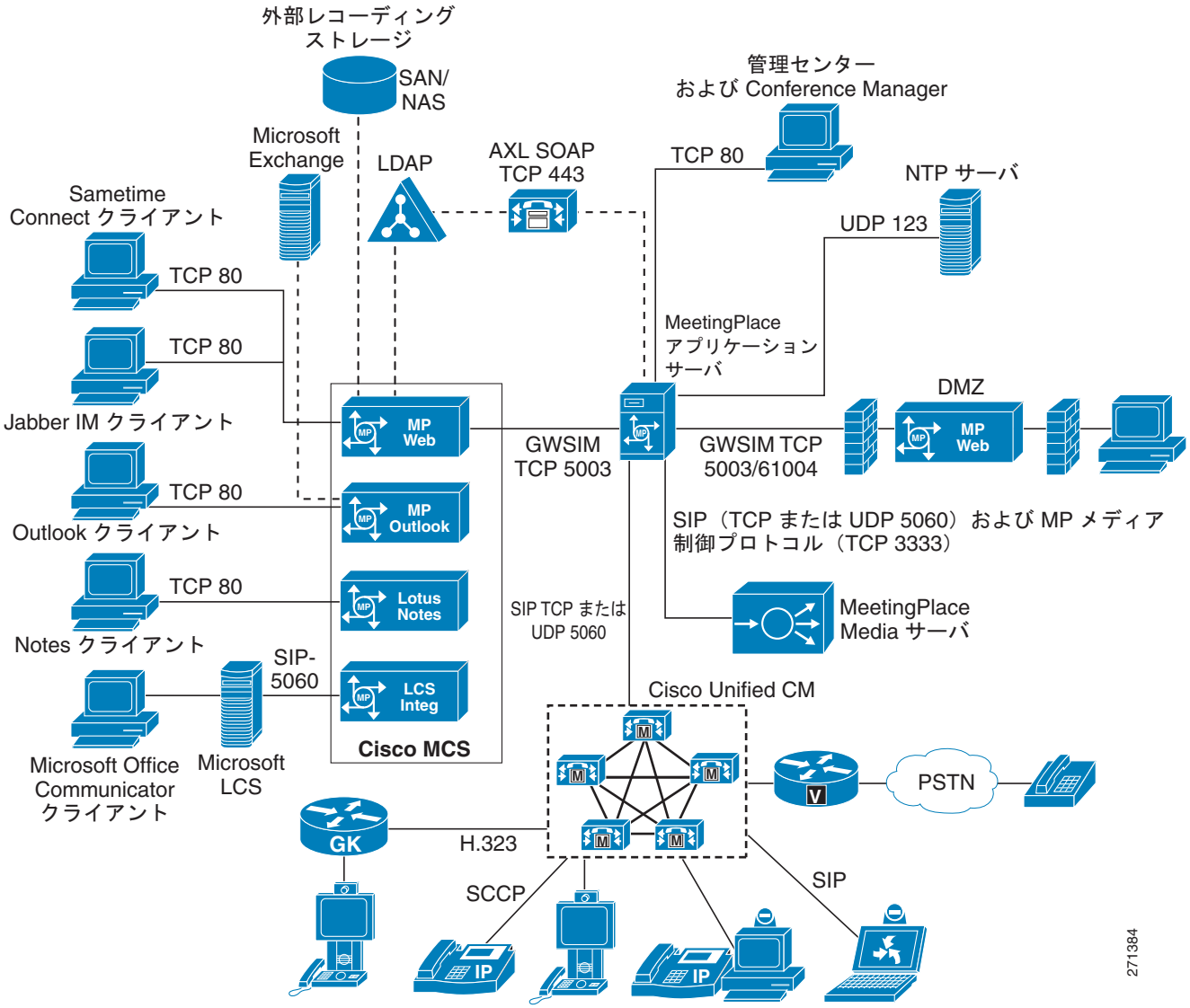


図 14-1 で Cisco MCS と記述された枠は、1 つ以上の Cisco Unified MeetingPlace コンポーネントをインストール可能な Cisco Media Convergence Server（MCS）を表しています。これらのコンポーネントの詳細については、「Cisco Unified MeetingPlace のコンポーネント」（P.14-1）の項を参照してください。

コンポーネント別の着信および発信ポートの詳細リストについては、http://docwiki.cisco.com で入手可能な『*Cisco Unified MeetingPlace, Release 7.0 -- Network Requirements*』を参照してください。

（注）　Unified MP 7.*x* アプリケーション サーバには、フロントエンドで Microsoft Outlook と統合するための機能が組み込まれています。この統合は、Unified MP アプリケーション サーバと通信して会議をスケジュールする Outlook プラグインの形態で実現されます。Outlook は、ユーザが Unified MP Web コラボレーション サーバの Web インターフェイスを通して会議をスケジュールし、それを Outlook カレンダーに追加できるように、バックエンドで統合することもできます。このバックエンドの Outlook 統合はオプションです。Unified MP 7.0(1) では、Unified MP Outlook Application ゲートウェイ コンポーネントを代替 Cisco Media Convergence Server（MCS）にインストールする必要があります。Unified MP 7.0(2) 以降のリリースでは、Outlook とのバックエンド統合が Unified MP アプリケーション サーバに組み込まれており、別途の Cisco Media Convergence Server（MCS）は不要になりました。

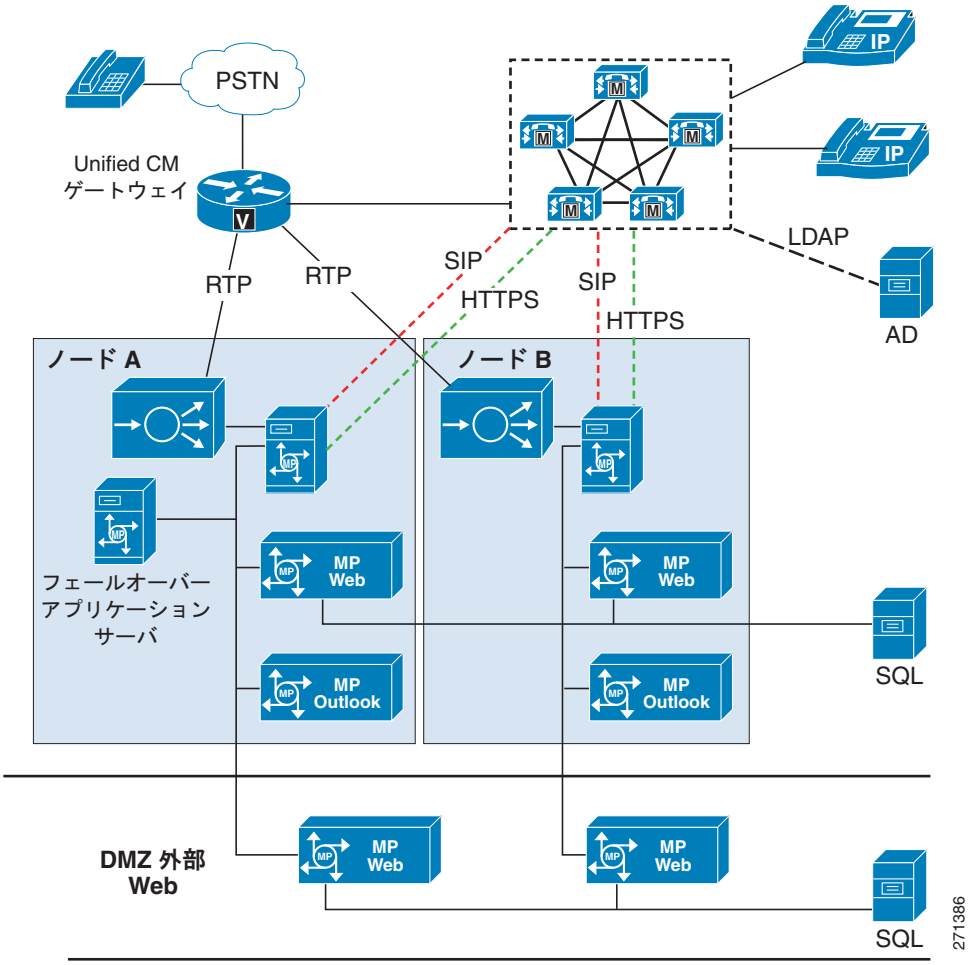
予約不要シングル ナンバー アクセスの配置

予約不要シングル ナンバー アクセス（RSNA）は、1 つのアクセス番号で複数の Unified MP 予約不要システムにアクセスする概念です。RSNA 機能を使用すれば、複数の Unified MP Web 会議サーバで同じ SQL データベースを共有し、1 つのサーバとしてユーザ コミュニティに公開できます。エンド ユーザのプロファイルの場所に関係なく、Unified MP は、プロファイル番号または会議 ID を入力したエンド ユーザを自動的に該当するサーバに誘導します。RSNA を実装した場合は、予約オプションやスケジュール済み会議オプションが使用できなくなります。RSNA は次の条件下で必要になります。

- 予約不要会議の使用が単一の Unified MP システムの容量を超える可能性がある。
- お客様の要件として、すべての Unified MP システムに単一の会議番号でアクセスしたい。
- 1 台の Unified MP メディア サーバが故障した場合に備えてフェールオーバー サポートが必要である。
- Unified MP 7.*x* で RSNA 配置を使用したビデオ会議がサポートされている。

図 14-2 に、RSNA 配置を示します。

図 14-2　予約不要シングル ナンバー アクセスの配置



RSNA に関する設計上の考慮事項

- RSNA では、参加しているすべての Unified MP システム上でユーザ プロファイルを同期させる必要があります。通常、この処理は Unified MP Directory Service 経由で行われます。
- RSNA では、着信に SIP REFER メソッドが使用され、このメソッドは Unified MP アプリケーション サーバと Unified CM でサポートされています。
- H.323 VoIP ゲートウェイを使用する場合は、H.323 と SIP のインターワーキングを実装して、Unified MP に到着する前に H.323 を SIP に変換する必要があります。この処理は、Unified CM を使用して H.323 VoIP ゲートウェイと RSNA を相互作用させることによって実現されます。H.323 と SIP のインターワーキングを実行するには、Unified CM 6.1（2）以降のリリースが必要です。
- RSNA は、最大 2 台の予備 Unified MP システムをサポートします。

セグメント化会議アクセス オプション

この配置オプションは、前述したすべての配置モデルに適用できます。

Cisco Unified MP は、外部公開会議用に Web コラボレーション サーバの非武装地帯（DMZ）内の設置がサポートされます。これをセグメント化会議アクセス（SMA）と言います。外部参加者はこのサーバを Web コラボレーションに利用しますが、内部会議の内部参加者は内部の Web サーバを Web コラボレーションに利用します。内部参加者が外部会議に参加すると、参加者は内部の Web コラボレーション サーバによって外部の Web コラボレーション サーバにリダイレクトされます。外部参加者の音声は、VoIP ゲートウェイ（Cisco Unified CM と相互運用される）を介して Unified MP に送られ、Unified MP メディア サーバに送られます。表 14-2 に、DMZ Web サーバと内部ネットワーク上のさまざまな Unified MP コンポーネント間の通信を可能にするために社内ファイアウォール上で開けておく必要のあるポートを示します。

表 14-2　Cisco Unified MeetingPlace で使用されるポート

プロトコル	ポートの種類	ポート	ポートの使用元
HTTP または HTTPS	TCP	80（1627）、443	Web
RTMP	TCP	1627	Web
GWSIM	TCP	5003、61004	Cisco Unified MP アプリケーション サーバ
SQL	TCP	1433	データベース

（注） 外部ユーザが内部の SAN/NAS サーバに保存された会議レコーディングにアクセスできるようにするには、社内ファイアウォール上の SAN/NAS サーバで使用されているポートを開く必要があります。特定のポート要件については、SAN/NAS デバイスの製品マニュアルを参照してください。

SMA を実装するには、内部 Web サーバと DMZ Web サーバを配置する必要があります。SMA の詳細については、http://www.cisco.com で入手可能な Cisco Unified MeetingPlace の製品マニュアルを参照してください。

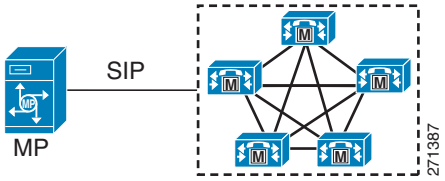
Unified MP と SIP および H.323 コール処理エージェントの統合

この項では、SIP 経由の Unified MP と Unified CM の統合に関する設計指針と推奨事項について説明します。H.323 に準拠したコール処理エージェントとの統合は、Unified CM の SIP/H.323 プロトコル インターワーキング機能を使用することによって実現されます。

SIP

Unified MP 7.*x* は、SIP トランク経由で Cisco Unified CM と直接統合されます。図 14-3 に、この統合方式を示します。

図 14-3　Unified CM との SIP 統合



Unified CM で Unified MP アプリケーション サーバの宛先アドレスを使用して SIP トランクを設定してから、ルート パターンを使用して SIP トランク経由のコールを Unified MP に経路設定する必要があります。Unified MP 呼制御で Unified CM コール処理サブスクライバの IP アドレスまたはホスト名を使用して SIP プロキシ サーバを設定する必要もあります。「冗長性」（P.14-19）に関する項に、冗長性を向上させるための追加のガイドラインがあります。Unified CM と Unified MP の統合設定の詳細については、次の URL で入手可能な『*Installation and Upgrade Guide for Cisco Unified MeetingPlace*』を参照してください。

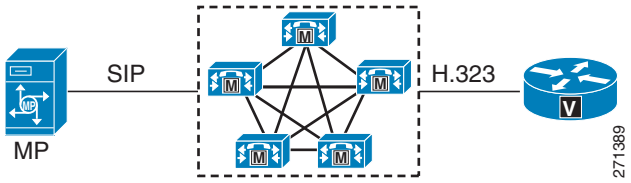
http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html

Unified MP は、Early Offer（EO; アーリー オファー）と Delayed Offer（DO; 遅延オファー）の両方の SIP Invite メッセージの受信をサポートします。Unified MP 7.0(2) 以降のリリースは発信コールで EO SIP Invite を開始しますが、Unified MP 7.0(1) は発信コールで DO SIP Invite を開始します。デフォルトで、Unified CM は、DO SIP Invite を使用してコールを Unified MP に送信します。Unified CM は EO を使用するように設定できますが、そのためにはメディア ターミネーション ポイント（MTP）リソースを使用する必要があります。詳細については、「SIP ディレイド オファーおよびアーリー オファー」（P.5-19）の項を参照してください。

H.323

Unified MP 7.*x* は、ネイティブで H.323 をサポートしません。そのため、H.323 VoIP ゲートウェイやゲートキーパーなどの H.323 デバイスと統合するには、Cisco Unified CM 6.1（2）以降のリリースを Unified MP アプリケーション サーバの手前に配置して H.323 と SIP 間のプロトコル変換機能を提供する必要があります（図 14-4 を参照）。

図 14-4　Unified CM 経由の H.323 統合



H.323 ビデオ エンドポイント

H.323 ビデオ エンドポイントが組み込まれた配置の場合は、H.323 ビデオ エンドポイントを登録可能なゲートキーパーを配置することをお勧めします（H.323 ビデオ エンドポイントとゲートキーパーを使用した配置については、図 14-1 を参照してください）。

Unified MP 7.*x* では、Unified CM が SIP フロントエンドとして機能し、ゲートキーパー用の SIP/H.323 プロトコル インターワーキングが実行されるため、H.323 ビデオ エンドポイントとゲートキーパーを配置するときに RAS アグリゲータ トランクが不要になりました。したがって、ゲートキーパーに登録されたビデオ エンドポイント向けのコールが必要な場合は、Unified CM が番号操作と帯域幅制御を行います。次の例は、ゲートキーパー設定を示しています。

```
gatekeeper
 zone local ccmtrunk cisco.com 1.1.1.1! Unified CM registers with gatekeeper in ccmtrunk
zone
 zone local video-ep cisco.com! Video endpoint registers with gatekeeper in video-ep zone
 no zone subnet ccmtrunk default enable
 zone subnet ccmtrunk 2.2.2.2/32 enable
 no zone subnet video-ep default enable
 zone subnet video-ep 3.3.3.3/32 enable
 zone prefix ccmtrunk 1... gw-priority 10 ccm_trunk_1  ! Calls to Unified MP is sent to
Unified CM
 gw-type-prefix 1#* default-technology
 no use-proxy video-endpoint default inbound-to terminal
 no use-proxy video-endpoint default outbound-from terminal
 no shutdown
```

コール アドミッション制御、QoS、および帯域幅

コール アドミッション制御、Quality of Service（QoS）、および適切な帯域割り当てが、音声とビデオの品質を保証するための主なメカニズムです。この項では、これらのメカニズムの Unified MP への適用方法について説明します。

コール アドミッション制御

Unified MP を使用したコール アドミッション制御は、Unified CM がコール処理エージェントとして実行する必要があります。Unified CM のコールアドミッション制御は、Unified MP アプリケーション サーバへの SIP トランクが関連付けられたロケーションで使用可能な帯域幅に基づいて実行できます。また、Unified CM は、コール アドミッション制御も提供可能なリソース予約プロトコル（RSVP）の使用をサポートします。コール アドミッション制御戦略の詳細については、「コール アドミッション制御」（P.9-1）の章を参照してください。

QoS マーキング

コール シグナリング

Unified MP アプリケーション サーバからの SIP シグナリング トラフィックは CS3（DSCP 0x18）とマークされますが、GWSIM トラフィックはマークされません。

メディア ストリーム

デフォルトで、Unified MP メディア サーバからの音声ストリームは EF（DSCP 0x2E）とマークされ、ビデオ ストリームは AF41（DSCP 0x22）とマークされます。

Web コラボレーション トラフィック

Unified MP Web コラボレーション サーバからの Web コラボレーション トラフィックは、ベストエフォート（DSCP 0x00）とマークされます。

帯域幅

呼制御帯域幅

呼制御帯域幅は非常に狭いですが、重要です。Unified MP アプリケーション サーバと Unified CM または Cisco Unified Border Element を同じ場所に設置することによって、呼制御に伴う問題の回避が容易になります。離れた場所に設置する場合は、信頼できる動作を保証するための適切な QoS プロビジョニングが必要になります。

GWSIM

GWSIM トラフィックは、Unified MP アプリケーション サーバと Unified MP Web コラボレーション サーバ間を流れます。GWSIM トラフィックは少量ですが、重要なトラフィックであるため、適切な動作を保証するために、すべての Unified MP Web コラボレーション サーバを Unified MP アプリケーション サーバと同じ場所に設置することをお勧めします。WAN でコンポーネントを分断する場合は、信頼できる動作を保証するための適切な QoS プロビジョニングが必要になります。

Unified MP アプリケーション サーバと Unified MP Web コラボレーション サーバ間のトラフィックには一部のデータベース同期が含まれているため、一時的に集中する場合がありますが、このトラフィックはリアルタイムではありません。

リアルタイム トランスポート プロトコル（RTP）トラフィック帯域幅

RTP トラフィックは、音声とビデオのトラフィックで構成されます。Unified MP メディア サーバは、音声コーデックとして G.711、G.729、G.722、および iLBC をサポートし、ビデオ コーデックとして H.261、H.263、および H.264 をサポートします。

「容量とサイジング」（P.14-14）で説明されているように、Unified MP 上の容量は、選択したコーデックによって異なります。コーデックの種類別の推定帯域幅については、「ネットワーク インフラストラクチャ」（P.3-1）と「IP ビデオ テレフォニー」（P.16-1）の章を参照してください。

Web コラボレーション帯域幅

Web コラボレーションでは、最も広い帯域幅が使用されます。特に、WAN リンク経由のリモート ユーザの場合にトラフィックが増大します。リモート サイトにいるユーザが WAN 経由で Web コラボレーションを実施する場合は、特別の考慮が必要になります。このようなユーザ用のクライアント フラッシュ セッション帯域幅または余剰帯域幅の設定値を下げて、WAN 上の負荷を減らす必要があります。Web コラボレーション データはユニキャストで配信されるため、最大データ バーストにリモート サイトのクライアント数を掛ける必要があります。たとえば、100 人のユーザがリモート サイトを利

用しており、そのうちの 10 人が同時に Web コラボレーションを実施しているとします。リモート サーバから各ユーザへのデータ内で 1.5 Mbps のバーストが発生する場合は、15 Mbps のバーストが WAN 接続上で発生する可能性があります。

過剰な Web コラボレーション データまたはその他のソースによって WAN リンクが輻輳すると、パケット損失、再送信、および遅延の増大が原因ですべてのトラフィックが低下します。輻輳が継続すれば、すべてのリモート コラボレーション セッションに悪影響が及びます。クライアントの Web コラボレーション セッションに関する次の設定によって、参加者がデータを受信する速度だけでなく、プレゼンターがデータを送信する速度が制御されます。

- モデム：28 kbps 以下の帯域幅
- DSL：250 kbps 以下の帯域幅
- LAN：1,500 kbps 以下の帯域幅

高解像度のイメージや写真が共有されている場合は、1,500 kbps を超える帯域幅バーストが使用できます。複雑さが標準以上のプレゼンテーションまたはドキュメントを共有する場合は、サイズの大きな複雑なイメージが埋め込まれていない限り、1,500 kbps を超えるバーストを発生させないでください。輻輳が発生しても帯域幅設定値が自動的に調整されないため、手動で調整する必要があります。帯域幅設定値はデフォルトで LAN に設定されます。また、各 Web コラボレーション セッションの初期化時に設定する必要があります。以前の設定に関係なく、新しいセッションは LAN に設定されます。

より良いユーザ エクスペリエンスを提供するためには、Web 会議に LAN または DSL 接続を使用することをお勧めします。LAN 接続では、各参加者は 1,500 kbps のダウンストリーム帯域幅を使用し、プレゼンターも 1,500 kbps のアップストリーム帯域幅を使用する必要があります。DSL 接続では、各参加者は 600 kbps のダウンストリーム帯域幅を使用し、プレゼンターも 600 kbps のアップストリーム帯域幅を使用する必要があります。この Web 会議帯域幅要件は、デフォルトの会議室解像度設定（800 x 600 ピクセル）に基づいています。会議室解像度がデフォルトの設定値よりも下または上に設定された場合は、それに応じて Web 会議帯域幅要件も低下または上昇します。モデム接続を使用する場合は、Unified MP Web Conferencing の他にアプリケーションを実行しないことをお勧めします。使用可能な帯域幅が制限されます。

DTMF サポート

Unified MP は、次の標準的なデュアルトーン マルチ周波数（DTMF）送信方式をサポートします。

- SIP 使用時の RFC2833 および KPML DTMF 送信
- インバウンド アコースティック DTMF 送信

DTMF 送信の詳細については、「メディア リソース」（P.6-1）の章を参照してください。

Unified CM 経由の外部ディレクトリ統合

Unified CM 5.0 以降を使用した外部ディレクトリと Unified MP の統合によって、次の 2 つの機能が提供されます。

- Unified MP での自動プロファイル作成
- サードパーティ製ディレクトリを使用した外部認証

Unified MP と Unified CM および外部 LDAP ディレクトリを統合すると、ユーザが初めて Unified MP にログインしたときに自動的にユーザ プロファイルが作成されます。ユーザはこのプロファイルを使用してその場で会議をスケジュールしてシステムを使用できます。外部 LDAP ディレクトリを統合する場合は、Web 経由でログインを試みるエンド ユーザに対して LDAP ベースのユーザ認証を使用する必要があります。

Unified MP ユーザは、Unified CM が統合された外部の社内ディレクトリに対して認証する必要があります。Unified MP のディレクトリ統合サービスによって、Unified MP 登録ユーザにシングル サインオン機能が提供されます。この機能を使用すれば、一度認証されたユーザは、ユーザ クレデンシャルを入力し直さなくても、ネットワーク上のすべてのリソースとアプリケーションにアクセスできます。Unified MP のユーザ認証方式の詳細については、http://www.cisco.com で入手可能な Unified MP の製品マニュアルを参照してください。

Unified MP では、Unified CM でサポートされているものと同じ外部 LDAP システムとバージョンのみがサポートされます。Unified MP は、Cisco AVVID XML Layer（AXL）Simple Object Access Protocol（SOAP）over secure HTTP（HTTPS）経由で Unified CM と統合されます。Unified MP では、外部 LDAP システムから直接ユーザ プロファイルを同期させることができません。

Unified CM は、次のディレクトリ サーバをサポートします。

- Microsoft Active Directory 2000、2003、および 2007
- Netscape および SunOne LDAP Directory Server バージョン 4 およびバージョン 5
- Cisco Unified CM ディレクトリ

  Unified CM ディレクトリからのユーザ データの同期化によって、Unified MP システムで、Unified CM で設定された Cisco Unified Communications ユーザをサポートできます。

Unified CM ディレクトリ統合の詳細については、「LDAP ディレクトリ統合」（P.17-1）の章を参照してください。

Unified MP と Cisco WebEx の統合

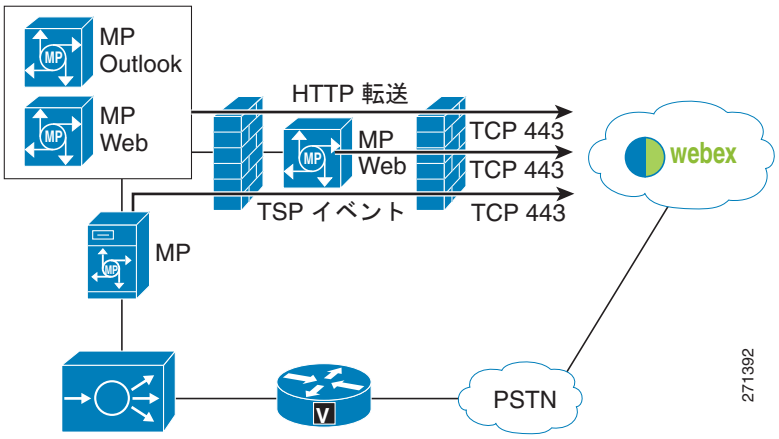
Cisco Unified MP と WebEx の統合によって、オンプレミスとオンデマンド ホスト型のコラボレーション ソリューションが提供されます。Unified MP と WebEx の統合を実装する場合は Unified MP のライセンスが必要ありません。また、WebEx を Web 会議プロバイダーとして使用する場合は Unified MP Web ユーザ ライセンス（UL）が必要ありません。次のどちらかのオプションを使用して Unified MP と WebEx を統合できます。

オプション 1：Unified MP Scheduling を使用した Unified MP と Webex の統合

このオプションを使用すれば、Unified MP 登録ユーザは、Unified MP の Web ユーザ インターフェイスまたは Outlook Calendar プラグインを介して会議をスケジュールできます。この統合オプションでは、Unified MP によって音声会議が提供され、WebEx によって Web 会議が提供されます。WebEx Meeting Center が、WebEx 会議テンプレートとして提供されます。WebEx 会議は、最初の会議参加者が Web 会議に参加した時点で自動的に作成されるため、Unified MP 上で会議がスケジュールされても WebEx には通知されません。この統合オプションではビデオ会議が使用できません。代わりに、WebEx によって基本的な Web カメラ ビデオ ストリーミングが提供されます。

図 14-5 に、このオプションを示します。WebEx 会議テンプレートの詳細については、http://www.cisco.com で入手可能な Cisco WebEx の製品マニュアルを参照してください。

図 14-5　Cisco Unified MP と WebEx の統合（オプション 1）



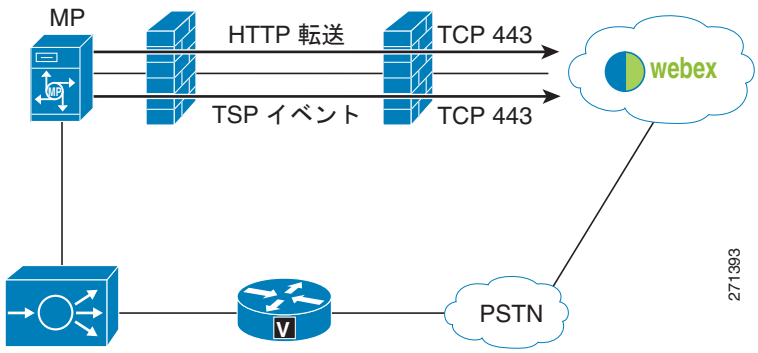
会議参加者は、同期化された Web と音声のレコーディングを作成できます。音声レコーディングによって、公衆網経由で WebEx Media Tone Network から Unified MP メディア サーバへのアウトダイヤル イベントが呼び出されます。Unified MP Web ユーザ インターフェイスからは記録済み会議にアクセスできないため、ユーザは WebEx アカウントにログインして記録済み会議にアクセスする必要があります。

ユーザが WebEx 会議に参加すると、Unified MP によって認証が行われてから、ユーザの要求が Unified MP Web コラボレーション サーバ（内部または外部）に送信され、そこから、セキュア HTTP 経由で WebEx Media Tone Network にリダイレクトされます。このリダイレクト動作はユーザにはまったく認識されません。また、ユーザ認証はオンプレミス Unified MP システムでだけ実行されます。すべての会議に関するサービス要求は、Unified MP アプリケーション サーバと WebEx 間のテレフォニー サービス プロバイダー（TSP）アプリケーション プログラミング インターフェイス（API）コール経由で交換および処理されます。

オプション 2：WebEx Scheduling を使用した Unified MP と Webex の統合

このオプションを使用すれば、ユーザは、WebEx Web ユーザ インターフェイスまたは WebEx Outlook Calendar プラグインを介して会議をスケジュールできます。このオプションでは、Unified MP によって音声会議が提供され、WebEx によって Web 会議が提供されます。また、Unified MP によって、予約不要音声会議が提供され、参加者は会議主催者が参加するまで待合室に入れられます。この統合オプションではビデオ会議が使用できません。代わりに、WebEx によって基本的な Web カメラ ビデオ ストリーミングが提供されます。図 14-6 に、このオプションを示します。

図 14-6　Cisco Unified MP と WebEx の統合（オプション 2）



会議参加者は、電話などの音声ユーザ インターフェイスを介して音声のみのレコーディングを開始することも、WebEx 会議室から音声と Web のレコーディングを開始することもできます。音声レコーディングによって、公衆網経由で WebEx Media Tone Network から Unified MP メディア サーバへのアウトダイヤル イベントが呼び出されます。Unified MP Web ユーザ インターフェイスからは記録済み会議にアクセスできないため、ユーザは WebEx アカウントにログインして記録済み会議にアクセスする必要があります。

Unified MP 登録ユーザが WebEx 会議をスケジュールする、または、Unified MP Web ユーザ インターフェイスから My WebEx リンクにアクセスしようとすると、WebEx によって自動的に Unified MP ユーザ プロファイルに基づくユーザ アカウントが作成されます。ユーザ名、パスワード、ファースト ネーム、ラスト ネーム、電子メール アドレスなどの一部の Unified MP ユーザ プロファイルが WebEx に継承されます。WebEx サイトは特定のお客様専用であり、WebEx ユーザ プロファイルは Unified MP ユーザ プロファイルをベースにしていることから、ユーザ プロファイルが矛盾しないようにする必要があります。

（注）　WebEx サービスを使用する場合は、お客様と Cisco WebEx の間で交わされた契約に基づいて料金が発生します。WebEx サービス料金は、Cisco Unified MP の実装やライセンスとは別です。

容量とサイジング

Unified MP 7.0(2) 以降のリリースは、最大 1500 の音声セッション（グローバル音声モードの設定は **G.711**、**G.729**）、300 のビデオ セッション（グローバル ビデオ モードの設定は**標準レート**）、および 1000 の Web セッションを同時にサポートします。

Unified MP メディア サーバ

Unified MP Application Administration でのグローバル音声モード設定によって、システムの音声容量が決定されます。グローバル音声モードは次のどちらかの方法で設定できます。

- G.711、G.729：この設定では、Unified MP メディア サーバ内の 1 つの音声ブレードで最大 250 個の音声ポートがサポートされます。サポートされるシステムの最大限度である 1500 の同時音声セッションに達するには、6 つの音声ブレードが必要となります。
- G.711、G.722、G.729、iLBC：この設定では、1 つの音声ブレードで最大 166 個の音声ポートがサポートされます。6 つの音声ブレードの場合、これらの追加コーデックを使用してサポートされる同時音声セッションの最大数は 996 です。

Unified MP Application Administration でのグローバル ビデオ モード設定によって、システムのビデオ容量が決定されます。グローバル ビデオ モードは、次の 2 つの方法で設定できます。

- 標準レート（最大 384 kbps のビデオ コール スピード）：このモードでは、Unified MP メディア サーバの Enhanced Media Processor（EMP）で最大 48 個のビデオ ポートをサポートできます。
- 高レート（最大 2048 kbps のビデオ コール スピード）：このモードでは、EMP で最大 24 個のビデオ ポートをサポートできます。

Unified MP でサポートされるビデオ形式の全リストについては、http://docwiki.cisco.com で入手可能な『*Cisco Unified MeetingPlace, Release 7.0 -- Video Endpoint Compatibility*』ページの「*Video Format Support*」の項を参照してください。

Unified MP メディア サーバは、Cisco Unified Videoconferencing 3515 マルチポイント コントロール ユニット（MCU）または Cisco Unified Videoconferencing 3545 システムにすることができます。Unified Videoconferencing 3515 メディア サーバは、音声ブレードと EMP がプレインストールされた

固定プラットフォームです。Unified Videoconferencing 3545 メディア サーバは、複数の音声ブレードまたは EMP のさまざまな組み合せをサポートするシャーシで構成されたモジュール式プラットフォームです。

仮想カスケーディング

Unified Videoconferencing 3545 メディア サーバに複数の音声ブレードと EMP がインストールされている場合は、メディア サーバで仮想カスケーディングを使用して、ある音声ブレードまたは EMP から別の音声ブレードまたは EMP への音声ストリームとビデオ ストリームがオーバーフローされます。音声ブレードには、音声セッション容量を減少させないカスケーディング ポートが組み込まれています。単一の EMP を Unified MP システムに配置することによって、すべてのビデオ ポートがビデオ会議に使用できます。複数の EMP を配置した場合は、メディア サーバによって自動的にカスケーディング用のビデオ ポートが予約されます。標準レート ビデオの場合は、カスケーディング用に 8 個のビデオ ポートが予約され、40 個のビデオ ポートが他の目的に使用できます。高レート ビデオの場合は、カスケーディング用に 4 個のビデオ ポートが予約され、20 個のビデオ ポートが他の目的に使用できます。次の 2 つの例は、カスケーディング時の音声ポートとビデオ ポートの使用方法を示しています。

例 14-1　音声会議

Unified Videoconferencing 3545 メディア サーバが、2 つの音声ブレードおよび 2 つの EMP と一緒に配置されます。会議が 350 個の音声ポートを使用してスケジュールされ、グローバル音声モードが G.711 と G.729 用に設定されます。

- メディア サーバで、最初の音声ブレードから 251 個のポートが割り当てられます。そのうちの 250 個のポートが音声参加者用に使用され、1 個のポートがビデオ カスケーディングまたは 2 番目の音声ブレードとの接続に使用されます。
- メディア サーバで、2 番目の音声ブレードから 101 個のポートが割り当てられます。そのうちの 100 個のポートが音声参加者用に使用され、1 個のポートがビデオ カスケーディングに使用されます。

例 14-2　ビデオ会議

Unified Videoconferencing 3545 システム メディア サーバが、2 つの音声ブレードおよび 2 つの EMP と一緒に配置されます。この例では、会議が 65 個のビデオ ポートでスケジュールされ、グローバル ビデオ モードが標準レート ビデオ用に設定されます。

- メディア サーバで、最初の EMP から 41 個のポートが割り当てられます。そのうちの 40 個のポートがビデオ参加者用に使用され、1 個のポートがビデオ カスケーディングまたは 2 番目の音声ブレードとの接続に使用されます。
- メディア サーバで、2 番目の EMP から 26 個のポートが割り当てられます。そのうちの 25 個のポートがビデオ参加者用に使用され、1 個のポートがビデオ カスケーディングに使用されます。

Unified MP 音声会議のサイジングに関するガイドライン

Unified MP 音声会議容量を計算するために次の 3 つの方法をお勧めします。

ナレッジ ワーカの数に基づく計算

20 人のナレッジ ワーカごとに 1 つずつの音声ユーザ ライセンス（UL）を用意することをお勧めします。ナレッジ ワーカとは、Cisco Unified MP を頻繁に使用するユーザを指します。

たとえば、40 人のナレッジ ワーカが使用するシステムの場合は、2 つの音声 UL を用意する必要があります。

平均月間使用時間に基づく計算

音声会議の平均使用時間（1 か月あたりの平均時間（分））がわかっている場合は、表 14-3 を使用して Unified MP 音声会議容量を計算します。

表 14-3　平均月間使用時間に基づく Unified MP 音声会議容量

平均月間使用時間（分）	ベースライン使用時間（1 か月およびユーザ ライセンスあたりの時間（分））
20,000 ～ 50,000	1,500
50,000 ～ 500,000	2,000
500,000 ～ 1,000,000	3,000
1,000,000 ～ 2,000,000	3,500
2,000,000 ～ 8,000,000	4,000

ピーク時の使用時間に基づく計算

一般的に、音声会議のピーク時の使用時間は、既存の音声会議システムのログまたはサービス プロバイダーの請求書から得られます。余裕をもった会議容量を確保するために、実際のピーク時使用時間よりも 20 ～ 30% 多い容量を用意することをお勧めします。

（注）　ユーザ ライセンス（音声、Web、またはビデオ）は、個別のユーザに付与されるのではなく、Unified MP システムを使用しているすべてのユーザで共有されたシステム規模のリソースに付与されます。

システム サイジングに影響を及ぼす要素

次の要素は、システム ベースライン ポートの要件に関する上述の方式による推定値に加え、システム サイジングにも影響を及ぼします。

- Cisco Unified MeetingPlace で「オペレータスケジュール」モデルからユーザスケジュールまたは予約なしモデルに移行するには、場合によっては、20% を別途ベースラインに追加する必要があります。
- 平均規模の会議では、1 回の会議につきデフォルトで 4.5 人の発信者がいます。この値がデフォルトとは異なる場合、実際の状況に応じた値を使用します。
- 次の条件に適合する場合、必要に応じてベースラインの推定値を増やします。

  （1 日の推定会議数）＊（推定ユーザ数）＞ベースラインの 80%
- 1 つの会議の最大値が推定値の 20% を超える場合、それに合わせて推定値を増やします。
- 専用ポートが必要になる継続して行う会議がある場合、その追加ポート（（会議数）＊（専用の発信者））をベースラインに追加します。

ポートの合計数には、ベースラインに、上述のすべての要素が追加されます。

Unified MeetingPlace 容量の拡張を計画している場合、次の条件がシステムに適用されるかどうかについても考慮してください。

- 推定ポート容量の合計が、表 14-4 に記載されている最大サポート ポートの 80% を超えます。
- G.711 以外のオーディオ コーデックが推奨されます。ただし、Cisco Integrated Services Router（ISR; サービス統合型ルータ）に基づくトランスコーダは、会議で他のコーデック タイプの最大容量を達成する必要がある場合に使用できます。
- Line Echo Cancellation（LEC）は、エコー キャンセレーションを提供する統合 MeetingPlace ではなく、外部デバイス（ISR など）によって提供されます。

Unified MP ビデオ会議のサイジングに関するガイドライン

Unified MP ビデオ会議容量を計算するために次の 3 つの方法をお勧めします。

ナレッジ ワーカの数に基づく計算
40 人のナレッジ ワーカごとに 1 つずつの音声 UL を用意することをお勧めします。

音声会議 UL 数に基づく計算
既存の音声会議 UL 数の 17 ～ 25% の範囲のビデオ会議容量を用意することをお勧めします。この割合は、ビデオ会議に関するビジネス要件と Unified MP システムの規模によって異なります。

既存のビデオ MCU に基づく計算
既存のビデオ会議システムをそのまま置き換えることをお勧めします。既存のシステムのビデオ会議ライセンスは、Unified MP UL で置き換えることができます。

Unified MP Web コラボレーション サーバ

Cisco MCS-7845H2/I2 サーバ上にインストールした場合は、Unified MP Web コラボレーション サーバで最大 500 個の Web セッションまたは 500 個の Web ユーザ ライセンス（UL）をサポートできます。Unified MP Web サーバは、2 台の MCS-7845H2/I2 Unified MP Web コラボレーション サーバを使用してクラスタ化し、システムあたり最大で 1,000 個の Web セッションにまで容量を増やすことができます。この設定では、1,000 人が参加する単一の Web 会議または 50 人ずつが参加する 20 件の Web 会議をサポートできます。

（注）　高度に冗長なシステムの場合は、最大 3 台の外部 Web サーバに加えて、最大 3 台の内部 Web サーバのクラスタを配置できます。これによって、ロード バランシングと冗長性の確保が可能になります。ただし、単一の Unified MP システムでは、すべての Unified MP Web サーバを通して最大 1,000 個の Web セッションしかサポートされません。

その代わり、単一の Cisco MCS-7835H2/I2 サーバで、最大 250 個の Web セッションまたは 250 個の Web UL をサポートできます。Cisco MCS-7835H2/I2 サーバをクラスタ化（最大 3 台）して容量と冗長性を増やすこともできます。

（注）　Unified MP Web サーバ モデルの混在はお勧めできません。Unified MP Web サーバの場合は、デフォルトでサーバ全体の負荷分散が行われますが、MCS モデルの種類に応じた負荷分散はできません。そのため、同じ MCS モデル上に Unified MP Web サーバを配置することをお勧めします。

Unified MP Web 会議用に Secure Socket Layer（SSL）トランスポート レイヤ セキュリティ（TLS）が実装されている場合は、Web 会議容量が変化しません。そのため、SSL/TLS を使用して Web 会議を保護することをお勧めします。

Unified MP Web 会議のサイジングに関するガイドライン

Unified MP Web 会議容量を計算するために次の 4 つの方法をお勧めします。

ナレッジ ワーカの数に基づく計算
40 人のナレッジ ワーカごとに 1 つずつの音声 UL を用意することをお勧めします。

音声会議 UL 数に基づく計算

既存の音声会議 UL 数の 33 ～ 50% の範囲の Web 会議容量を用意することをお勧めします。この割合は、Web 会議に関するビジネス要件と Unified MP システムの規模によって異なります。

ピーク時の使用時間に基づく計算

一般的に、Web 会議のピーク時の使用時間は、既存の Web 会議システムのログまたはサービス プロバイダーの請求書から得られます。余分な会議容量を確保するために、実際のピーク時使用時間よりも 20% 多い容量を用意することをお勧めします。

既存の Web 会議システムに基づく計算

既存の Web 会議システムをそのまま置き換えることをお勧めします。既存のシステムの Web 会議ライセンスは、Unified MP UL で置き換えることができます。

（注）　浮動ポート数として Unified MP UL 数の 20% を用意し、余剰ポート数として総 UL 数の 30% を用意することをお勧めします。

展開時におけるシステム容量の制限

表 14-4 に、Unified MeetingPlace バージョンおよび Cisco Media Convergence Server（MCS）モデルによるシステム容量の制限を示します。

表 14-4　ポートの最大容量

Cisco Unified MeetingPlace のリリースとサーバ モデル	高容量モード ポートの最大数	複数コーデック ポートの最大数	ユーザの推定最大人数	1 日の会議の推定最大開催数	1 か月の音声の推定最大使用時間（分）	Web 会議セッションの最大数
Release 7.*x*、（MCS 7845）	1,500（LEC なし G.711 および G.729）	適用対象外	30,000	1,500	600 万	3 MeetingPlace Web（非 SSL[1]）では 1,000、または 1,000 WebEx SaaS[2]
Release 7.*x*、（MCS 7845）	適用対象外	996	20,000	996	390 万	3 MeetingPlace Web（非 SSL[1]）では 1,000、または 1,000 WebEx SaaS[2]

1. SSL = Secure Sockets Layer
2. SaaS = Software-as-a-Service

上記は、新しいシステムの音声ポートの個数を決める際のガイドラインを示したものです。このガイドラインは、業界の標準的な会議システム使用状況を前提に作成されています。実際にはこの数値は、タイムゾーンが複数にまたがるかどうか、営業時間内容（24 時間無休か 8 時間週休 2 日か）、ユーザの会議に関する慣習など、さまざまな要因によって変わります。ガイドラインでは、典型的な使用状況として「Unified MP 音声会議のサイジングに関するガイドライン」（P.14-15）に記載されている公式をベースとしています。

既存のサービス プロバイダーが現在の会議ピーク時間のポート使用量か、数か月間のポート使用量を月単位で提供できる場合、オンプレミス Unified MeetingPlace システムでの推定値を算出する際にはその数値も使用する必要があります。ただし経験上、使用量の増大を見込んでおく必要があります。実際の Unified MeetingPlace の使用量データがある場合、既存のシステムから実際の会議ポート使用量

を収集して必要なポート数を判断してください。実際の会議の使用状況に基づくと、実際のシステムでサポートできるユーザ数がこれよりも増えるか減る可能性があります。また、実際のシステムでサポートされる会議数も、これより増えるか減る可能性があります。

Unified MeetingPlace システムをインストールすると、Monthly Port Utilization Report をモニタすることで実際の使用状況を確認し、使用量の増加や実際の使用状況のパターンを測定することができます。

冗長性

この項では、次の Unified MP コンポーネントの冗長性に関する考慮事項について説明します。

- 「Unified MP アプリケーション サーバ」（P.14-19）
- 「Unified MP メディア サーバ」（P.14-21）
- 「Unified MP Web コラボレーション サーバ」（P.14-22）
- 「呼制御」（P.14-22）

Unified MP アプリケーション サーバ

Unified MP 7.*x* を使用すれば、1 次と予備の Unified MP アプリケーション サーバを使用できます。フェールオーバー配置内の各 Unified MP アプリケーション サーバには、その物理ネットワーク インターフェイス カード（NIC）に関連付けられた共通の IP アドレスと仮想ネットワーク インターフェイスに関連付けられた一意の IP アドレスが設定されます。両方の Unified MP アプリケーション サーバで同じ IP アドレスを共有するための要件は、両方のアプリケーション サーバを同じ仮想 LAN（VLAN）または IP サブネットに接続することです。このことは、両方のサーバが単一のデータ センター内に存在する場合は問題になりません。ただし、デュアル データ センター設計は、両方のデータ センターが同じ VLAN（IP サブネット）上に存在する場合にのみサポートされます。すべての Unified MP コンポーネントと同様に Unified CM もこの共有 IP アドレスを使用してデータをやり取りします。スタンバイ サーバの物理 NIC（共有 IP アドレスを含む）は、プライマリ サーバが故障して手動フェールオーバー プロセスが開始されるまで、無効にされます。予備サーバには、次のネットワーク接続要件があります。

- 1 次と同じ VLAN（IP サブネット）に接続されている。
- 予備と 1 次間の往復遅延時間は 250 ms 未満である。
- 予備と 1 次間のパケット損失は 1% 未満である。
- 予備と 1 次間の帯域幅は 384 kbps 以上である。

1 次サーバと予備サーバ間の Informix データベース レプリケーションに仮想ネットワーク インターフェイスが使用されます。データベース レプリケーションでは、ユーザ、グループ、および会議に関係するデータベース テーブルが 1 次サーバと予備サーバ間で同期されることが保証されます。TCP ポートの 2008 は、アプリケーション サーバ間のデータベース レプリケーションに使用されるため、ファイアウォールが配置されている場合は開く必要があります。1 次サーバと予備サーバの仮想ネットワーク インターフェイスを同じ VLAN に配置することをお勧めします。**failoverUtil** という名前のサーバのコマンド ライン インターフェイス（CLI）経由でアクセスするユーティリティを使用して、1 次と予備の Unified MP アプリケーション サーバをセットアップし、両サーバ間のデータベース レプリケーションを設定します。**failoverUtil** ユーティリティの詳細については、次の URL で入手可能な『*Configuration Guide for Cisco Unified MeetingPlace*』を参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html

（注）　Unified MP アプリケーション サーバが故障すると、通話中のコールが失われます。ユーザは、予備のアプリケーション サーバが 1 次サーバに昇格されてから、会議にリダイアルする必要があります。Unified MP アプリケーション サーバでは、自動フェールオーバー メカニズムが利用できません。

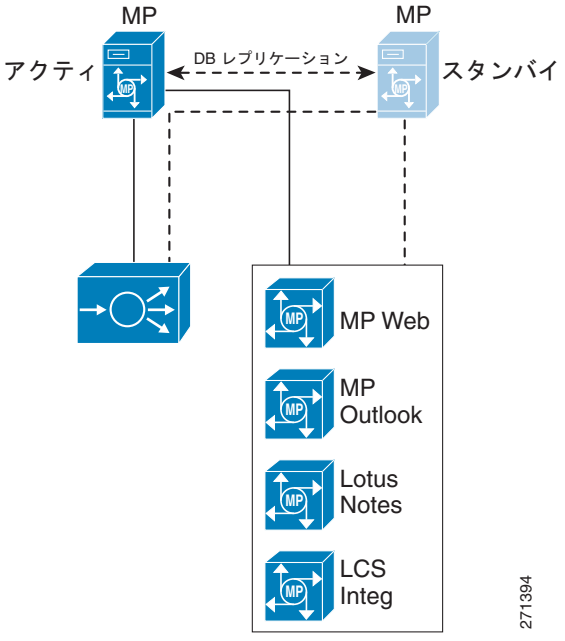
Unified MP 7.*x* ソリューションに関するその他の重要な要件は、アクティブな Unified MP アプリケーション サーバとアクティブな Unified MP メディア サーバを同じ場所に設置する必要があることです。そのため、シングル データ センター設計とデュアル データ センター設計に関する考慮事項は多少異なります。

シングル データ センター設計

シングル データ センター設計では、地理的に同じ場所で Unified MP Application サーバのフェールオーバーが発生します。この種の配置では、一般に、一連の Unified MP メディア サーバが 1 次と予備の Unified MP アプリケーション サーバで共有されます。1 次 Unified MP アプリケーション サーバが故障した場合は、Unified MP メディア サーバを予備（現在の 1 次）サーバに同期させる必要があります。Unified MP Web コラボレーション サーバも共有されます。図 14-7 に、シングル データ センター配置における Unified MP アプリケーション サーバのフェールオーバー プロセスを示します。

（注）　高度に冗長なソリューションでは、シングル データ センター内に予備の Unified MP メディア サーバと Unified MP Web コラボレーション サーバのセットを配置することもできます。

図 14-7　シングル データ センター配置における Unified MP アプリケーション サーバのフェールオーバー

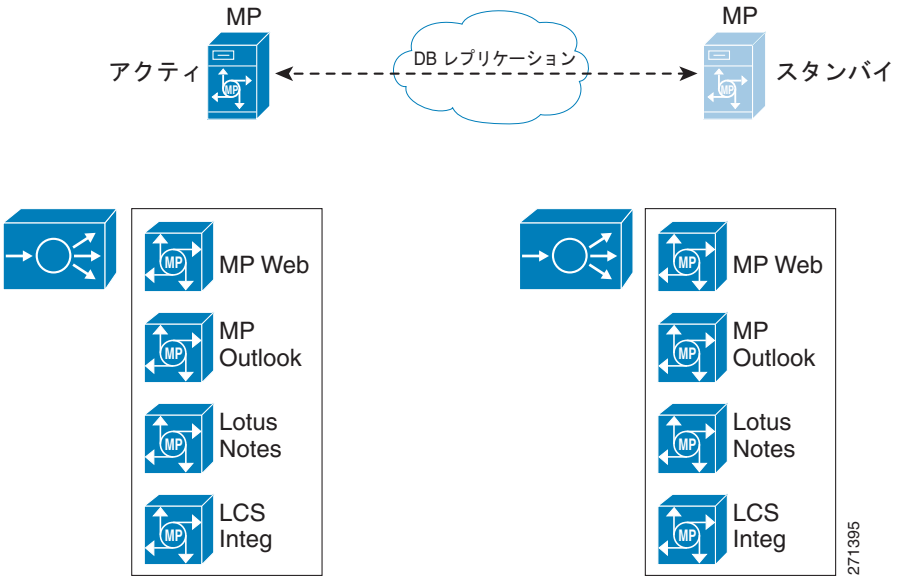


デュアル データ センター設計

デュアル データ センター設計では、Unified MP アプリケーション サーバのフェールオーバーが IP WAN 上の地理的に異なる場所で発生します。また、1 次と予備のアプリケーション サーバが地理的に離れていますが、両方のサーバを同じ VLAN に接続して適切なフェールオーバー動作を保証する必要があります。この種の配置では、予備アプリケーション サーバを余分な Unified MP メディア サーバと同じ場所に設置して、それらと同期させる必要があります。予備データ センター内で Unified MP メディア サーバの音声ブレードとビデオ ブレードの数が異なる場合は、予備アプリケーション サーバが 1 次サーバに昇格されるフェールオーバー シナリオでシステム容量が減少する可能性があります。

通常の設計と同様に、アクティブな Unified MP アプリケーション サーバと Unified MP Web コラボレーション サーバ間の往復遅延が 150 ms を超えないようにする必要があるため、予備データ センターでの往復時間が 150 ms を超える場合にのみ余分な Web サーバが必要になります。図 14-8 に、デュアル データ センター配置における Unified MP アプリケーション サーバのフェールオーバー プロセスを示します。

図 14-8　デュアル データ センター配置における Unified MP アプリケーション サーバのフェールオーバー



Unified MP メディア サーバ

Unified MP アプリケーション サーバは、システム内の代替 Unified MP メディア サーバ（音声ブレードまたはビデオ ブレード）へのフェールオーバーを自動的に実行します。たとえば、音声ブレードとの接続断を検出した場合、アプリケーション サーバは、以降の音声セッションがアクティブな音声ブレードに接続されるように、そのブレードをアクティブな音声ブレードのリストから削除します。音声またはビデオ ブレードの障害時に Unified MP メディア サーバの容量が減少しないようにするには、アプリケーション サーバにメディア サーバを追加するのが 1 つの方法です。アプリケーション サーバはライセンスされたセッション数を超えることはありません。もう 1 つの方法は、専用の Unified MP メディア サーバを備えた予備の Unified MP アプリケーション サーバに戻すことです（デュアル データ センター設計と同様）。この 2 つの方法は二者択一ではありません。専用の Unified MP メディア サーバを備えた予備の Unified MP アプリケーション サーバは、メディア サーバを追加することで、さらに冗長性を高めることができます。

Unified MP Web コラボレーション サーバ

複数の Unified MP Web コラボレーション サーバをクラスタ化して、Web サーバの容量と冗長性を向上させることができます。Unified MP Web コラボレーション クラスタには、最大で 3 台の Web 会議サーバを含めることができます。各 Web サーバが 1 台の Unified MP アプリケーション サーバに接続され、外部または Web 会議サーバのいずれかに配置可能な SQL データベースが共有されます。冗長性を最大化するために、Web サーバ クラスタ用の外部 SQL データベースの使用をお勧めします。1 台の Web 会議サーバが使用不能になった場合は、アクティブな会議がクラスタ内の別のサーバにフェールオーバーされます。Web 会議 URL 内で使用されている DNS 名にマップされた Web サーバがオフラインの場合に、これらの要求を処理するための Unified MP Web サーバを設置する必要があります。クラスタ内の別の Web サーバがオフラインの場合は、その Web サーバへの以降の Web 会議の転送が Unified MP Web サーバによって中断され、処理は正常に継続されます。

Unified MP 7.*x* は、内部 Unified MP Web コラボレーション クラスタと外部 Unified MP Web コラボレーション クラスタの同時配置をサポートします（クラスタあたり最大 3 台の Web サーバ）。ただし、それぞれのクラスタで別々の SQL データベースを使用する必要があります。内部クラスタは、すべての Web 会議サーバが社内ファイアウォールの背後に実装され、エンド ユーザにフル アクセス（会議のスケジューリングと参加）が提供されることを意味します。外部クラスタは、すべての Web 会議サーバが DMZ 内部に実装され、参加のみのアクセスがエンド ユーザに提供されることを意味します。

Unified MP Web コンポーネントによって、デフォルトで、Web サーバ クラスタに対する負荷分散が提供されます。ユーザが会議に参加すると、Unified MP Web サーバによってクラスタ内のすべての Web 会議サーバの負荷がチェックされ、負荷が最低のサーバにそのユーザが割り当てられます。Unified MP Web サーバ上の負荷分散は、クラスタ内のすべての Unified MP Web サーバで Web セッションを共有することによって実現されます。したがって、3 台の Web サーバを含むクラスタでは、通常の処理中に 3 台すべてのサーバ上で同時に会議が発生する可能性があります。Unified MP Web コラボレーション サーバ容量の詳細については、「容量とサイジング」（P.14-14）の Unified Web コラボレーション サーバの項を参照してください。

呼制御

Unified MP では、Cisco Unified CM コール処理用のサブスクライバを複数指定した、SIP アウトダイヤルを定義できます。冗長性を確保するには、Unified CM クラスタ内の代替コール処理サブスクライバにコールを転送するように複数の SIP プロキシ サーバを設定する必要があります。Unified MP アプリケーション サーバからは、「SIP proxy server 1」との接続が失われない限り、発信コールが「SIP proxy server 1」にのみ送信され、「SIP proxy server 2」には送信されないことに注意してください。その場合にのみ、Unified MP からは、リストで次に使用可能なコール処理エージェントに SIP INVITE メッセージが自動的に送信されます。コール処理エージェントの失敗が既存のコールに影響を与えないようにする必要があります。ユーザが切断すると、既存のメディア接続が失われます。

（注）「**SIP プロキシ サーバ**」という用語は、単に Unified MP アプリケーション サーバの設定ページに見られる用語であり、すべての SIP プロキシ サーバとの統合がサポートされることを意味するものではありません。Unified MP がサポートするのは、Cisco Unified CM クラスタとの SIP 統合だけです。

着信コールの場合は、クラスタ内のすべてのコール処理サブスクライバから Unified CM 内の単一の設定済み SIP トランクにアクセスできます。フェールオーバー Unified MP アプリケーション サーバを配置した場合は、Unified CM で 2 つ目の SIP トランクを設定する必要があります。この 2 つ目の SIP トランクは、フェールオーバー アプリケーション サーバが実際にアクティブにされるフェールオーバー

シナリオ中のコールに対してのみ使用されるように配慮する必要があります。Unified CM と Unified MP の統合設定の詳細については、次の URL で入手可能な『*Installation and Upgrade Guide for Cisco Unified MeetingPlace*』を参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html

ゲートキーパーの冗長性の詳細については、「コール処理」（P.8-1）の章を参照してください。

CHAPTER 15

Cisco Unified MeetingPlace Express

Cisco Unified MeetingPlace Express 2.0 は音声、ビデオ、および Web コラボレーションに使用されるリッチメディア アプライアンスです。この章では、Cisco Unified MeetingPlace Express（Unified MPE）を Cisco Unified Communications 環境に統合する場合のシステム レベルでの設計に関する考慮事項について説明します。製品に関する詳細については、次から入手可能な Cisco Unified MeetingPlace Express の製品マニュアルを参照してください。

http://www.cisco.com

この章の新規情報

表 15-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 15-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
キャパシティとサイジング情報	「容量とサイジング」（P.15-15）
Segmented Meeting Access（SMA）オプションを使用した Unified MPE の導入	「セグメント化会議アクセス オプション」（P.15-9）
サポートされるプロトコル	「サポートされるプロトコル」（P.15-3）

概要

Cisco Unified MeetingPlace Express（Unified MPE）は中規模市場から小規模企業を対象とした音声、ビデオ、および Web 会議ソリューションです。ソリューションでは H.323 や Session Initiation Protocol（SIP; セッション イニシエーション プロトコル）などの一般的な業界プロトコルを採用しており、ネットワーク上の多様なデバイスとの相互運用性を保証します。Unified MPE では、スケジュール済みおよび予約なしの音声、ビデオ、および Web 会議がサポートされます。音声、ビデオ、および Web 会議は Unified MPE システム固有のソフトウェア制御のミキシング機能によってミキシングされます。ビデオ ミキシング機能は Cisco Unified Videoconferencing MCU 3500 システムを使用せず、システムに搭載された高度ビデオ ソリューションに統合できません。Unified MPE のスケジュール システムでは、基本的なビデオ会議機能や音声起動会議などの機能のみがサポートされます。高度なビデオ会議機能が必要な場合は、スタンドアロンの Cisco Unified Videoconferencing MCU 3500 または Cisco Unified MeetingPlace システムを使用してください。

Unified MPE Video Telephony（Unified MPE VT）は Unified MPE と同じテクノロジーを採用していますが、異なる製品で、ad-hoc システムとしてのみ販売されています。Unified MPE VT は Cisco Unified Communications Manager に登録できるビデオ会議メディア リソースとして配置され、ad-hoc ビデオ会議機能を提供します。スケジュール済み会議または予約なし会議はサポートされません。また、Unified MPE に関連して導入することもできません。1 台の Cisco Media Convergence Server には、Unified MPE または Unified MPE VT のいずれかをインストールできますが、両方を同時にインストールできません。

（注）　いずれも類似したテクノロジーに基づいていますが、Unified MPE と Unified MPE VT の設計基準は一部異なります。たとえば、G.729 オーディオ コーデックは Unified MPE でサポートされますが、Unified MPE VT ではサポートされません（この場合、Unified CM がトランスコーダを提供する必要があります）。Unified MPE VT の詳細は、Unified MPE VT データシートを http://www.cisco.com/en/US/products/ps6533/products_data_sheets_list.html で参照してください。

サポートされる会議機能

次のコール処理エージェントと統合すると、Unified MPE でさまざまな会議機能をサポートできます。

- Unified CM 4.1 以降と併用すると、スケジュール済みおよび予約なしの音声、ビデオ、および Web 会議をサポートします。
- Cisco Unified Communications Manager Express（Unified CME）と併用すると、スケジュール済みおよび予約なし音声会議および Web 会議がサポートされます。
- Survivable Remote Site Telephony（SRST）と併用すると、スケジュール済みおよび予約なし音声会議および Web 会議がサポートされます。

サポートされるビデオ

Unified MPE によって提供されるビデオ会議に参加する H.323、SIP、または Unified CM SCCP エンドポイントはすべて Mid-call video escalation 機能を備えている必要があります。ITU-T H.323 仕様または SIP RFC-3261 に準拠する業界標準ビデオ エンドポイントはすべて Unified MPE のビデオ セッションに参加できます。また、ソニー、Tandberg、または Polycom などのサポートされるサードパーティ製の SCCP エンドポイントはすべて Unified CM のさまざまなリリースで利用できます。H.323 業界エンドポイントは Cisco IOS Gatekeeper または Unified CM のいずれかに登録でき、Unified MPE ダイアルイン番号に Unified MPE システムへの呼ルーティングを提供する必要があります。

Unified MPE ビデオ セッションに参加するビデオ エンドポイントでは、次のビデオ属性がサポートされる必要があります。

- Common Intermediate Format（CIF）に準拠した H.263 または H.264 ビデオ コーデック
- G.711 または G.729a オーディオ コーデック
- 通話切替ビデオ エスカレーション（エンドポイントは初めに Unified MPE にダイアルインし、会議 ID を入力します。ビデオ ポートがスケジュール済みの場合は、ビデオがアクティブである必要があります）。
- RFC-2833、SIP KPML、または H.323 帯域外 DTMF サポート

- Unified MPE では H.263 および H.264 ビデオ コーデックがサポートされますが、ビデオ ストリームのコーデックを別の種類にトランスコードできません。システム管理者は、ビデオ会議タイプごとにビデオ コーデック設定を詳細に指定する必要があります。会議をスケジュールする担当者は、利用可能な会議タイプをリストから選択します。Unified MPE Profiles ユーザには、ユーザ エクスペリエンスを制御する次の 3 つのレベルのいずれかが割り当てられます。

  1. ビデオ会議への参加、ビデオ会議の開催、およびビデオ ポートの予約が可能
  2. ビデオ会議への参加、ビデオ ポートが利用可能な場合（別の会議にスケジュールされていない）のみビデオ会議の開催が可能
  3. ビデオ会議への参加が可能

ビデオ会議に参加できるビット レートは 64 ～ 768 kbps です。設定上限を超過するビット レートの参加者は会議に参加できません。参加者のビット レートが上限以下の場合は、システム全体のキャパシティ プールに余裕ができ、ほかの参加者が利用できます。Unified MPE では、異なるコール スピードをレート変換できません。したがって、確立されたビデオ セッションに使用されるビット レートは、会議ごとに、参加している最も遅いビット レートに合わされます。

Unified MPE のビデオ会議では音声起動モードが使用されます。このモードでは、参加者の中から声が最も大きく、長時間話している参加者を判断して会議の主要発言者を選択します。発言中の参加者のビデオ ストリームは、会議に接続されたすべてのエンドポイントに送信され、前回の発言者のビデオ ストリームは発言中の参加者に送信されます。会議中に条件が変わると、Unified MPE は自動的に新しい主要な発言者を選択し、その参加者が表示されるようにビデオを切り替えます。発言中の参加者（イメージ 1 つまたは 1x1 レイアウト）は Common Intermediate Format（CIF）次元のみを使用します。

サポートされるプロトコル

表 15-2 には Cisco Unified Communications 環境で Unified MPE によって使用される標準プロトコルとトランスポート レイヤが一覧表示されています。

表 15-2　Unified MPE によってサポートされるプロトコル

プロトコル	トランスポート	ポート	使用方法
SSH	TCP	22	セキュアなアクセス、音声会議イベント
RTMP	TCP	1935	Web 会議（オプション）
HTTP、HTTPS	TCP	80、443	Web 管理、Web 会議、Cisco Unified Personal Communicator、Microsoft Outlook[1]、HTTPS 経由で AXL/SOAP を Unified CM に接続（直接統合）
SIP	UDP	5060	SIP
H.225	TCP	1720	H.323 で Unified CM またはゲートキーパーに接続
H.245	TCP	62000 ～ 62999	H.323 で Unified CM またはゲートキーパーに接続
RTP	UDP	16384 ～ 32767	音声パケット
RTP	UDP	20480 ～ 24576	ビデオ パケット
NTP	UDP	123	ネットワーク タイム プロトコル[2]
SMTP	TCP	25	E メール通知（サーバに発信）
SNMP	UDP	161	SNMP

1. HTTP または HTTPS を使用して Unified MPE サーバと通信するプラグインによって Microsoft Outlook が統合されます。
2. Unified MPE を使用して会議をスケジュールし、正確な時刻を記載した会議の通知を送信できるよう Unified MPE は適切な NTP サーバに関連付けてください。

DTMF サポート

Unified MPE では次の標準 Dual Tone Multifrequency（DTMF）転送方法がサポートされます。

- H.323 の使用時、H.245 Alphanumeric および H.245 Signal DTMF 送信
- SIP 使用時の RFC2833 および KPML DTMF 送信

DTMF 送信に関する詳細は、「メディア リソース」（P.6-1）の章を参照してください。

配置モデル

ここでは、Unified MPE を次の Cisco Unified Communications 配置モデルと統合する場合の推奨設計について説明します。

- 「単一サイト」（P.15-4）
- 「集中型コール処理を使用するマルチサイト WAN」（P.15-6）
- 「分散型コール処理を使用するマルチサイト WAN」（P.15-7）
- 「WAN を介したクラスタ化」（P.15-8）

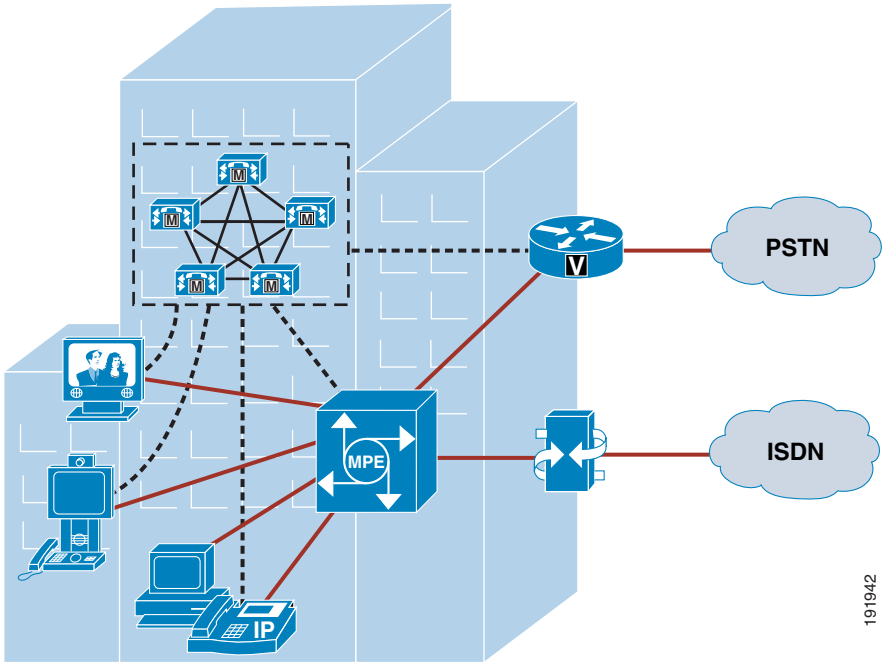
次の配置モデルに加えて非武装地帯（DMZ）が含まれる配置についても説明します。DMZ が含まれる配置では、Segmented Meeting Access（SMA）を使用して実装します。上記に一覧表示された配置モデルはそれぞれ SMA オプションをサポートします（「セグメント化会議アクセス オプション」（P.15-9）を参照）。さまざまな配置モデルの設計ルールの詳細については、「Unified Communications の配置モデル」（P.2-1）の章を参照してください。

単一サイト

単一サイトの配置では、すべてのコール処理および参加者はローカルです。このモデルでは、Unified MPE から Unified CM に H.323 または SIP によって接続されます（図 15-1 を参照）。単一サイトの配置では、G.711 コーデックを使用することをお勧めします。これは、マルチサイト設置の場合より帯域幅が重要ではないためです。H.323 ビデオ エンドポイントは Cisco IOS Gatekeeper または Unified CM のいずれかに登録でき、Unified MPE ダイアルイン番号に Unified MPE システムへの呼

ルーティングを提供できます。Cisco Unified Videoconferencing 3500 Series Gateways を配置することで、H.320 ビデオ クライアント（DTMF 送信の H.245 Alphanumeric または H.245 Signal をサポート）がビデオ会議に参加できるようになります。

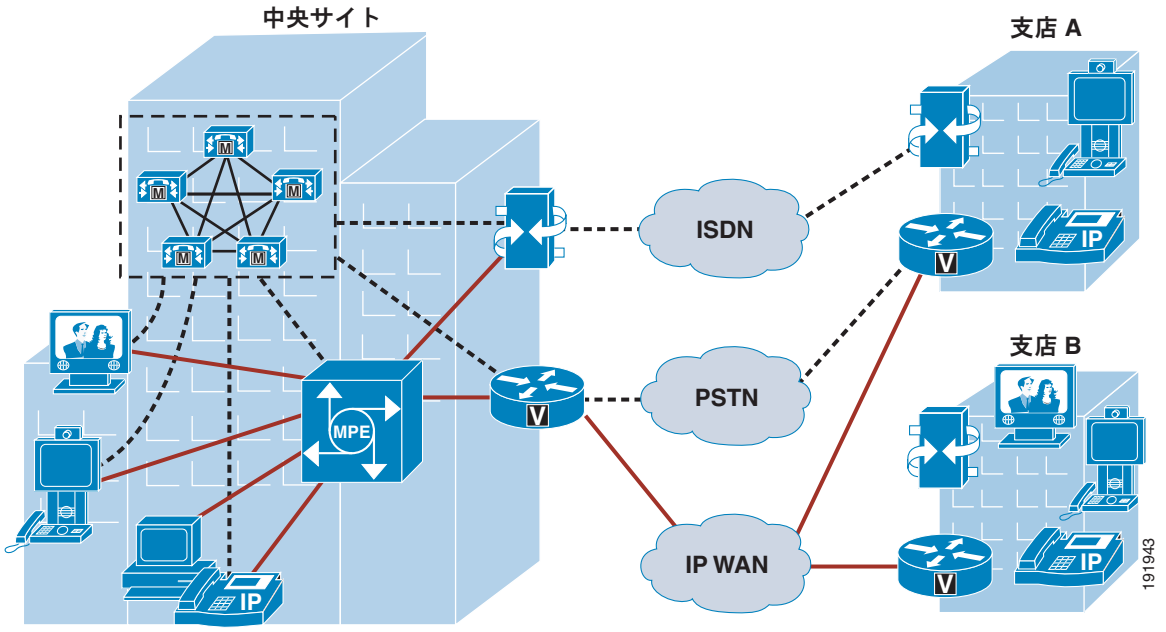
図 15-1　　単一サイトの配置



集中型コール処理を使用するマルチサイト WAN

集中型コール処理を使用するマルチサイト WAN 配置では通常、コール処理が発生する中央サイトに Unified MPE サーバを配置します（図 15-2 を参照）。

図 15-2　集中型コール処理を使用するマルチサイト WAN 配置



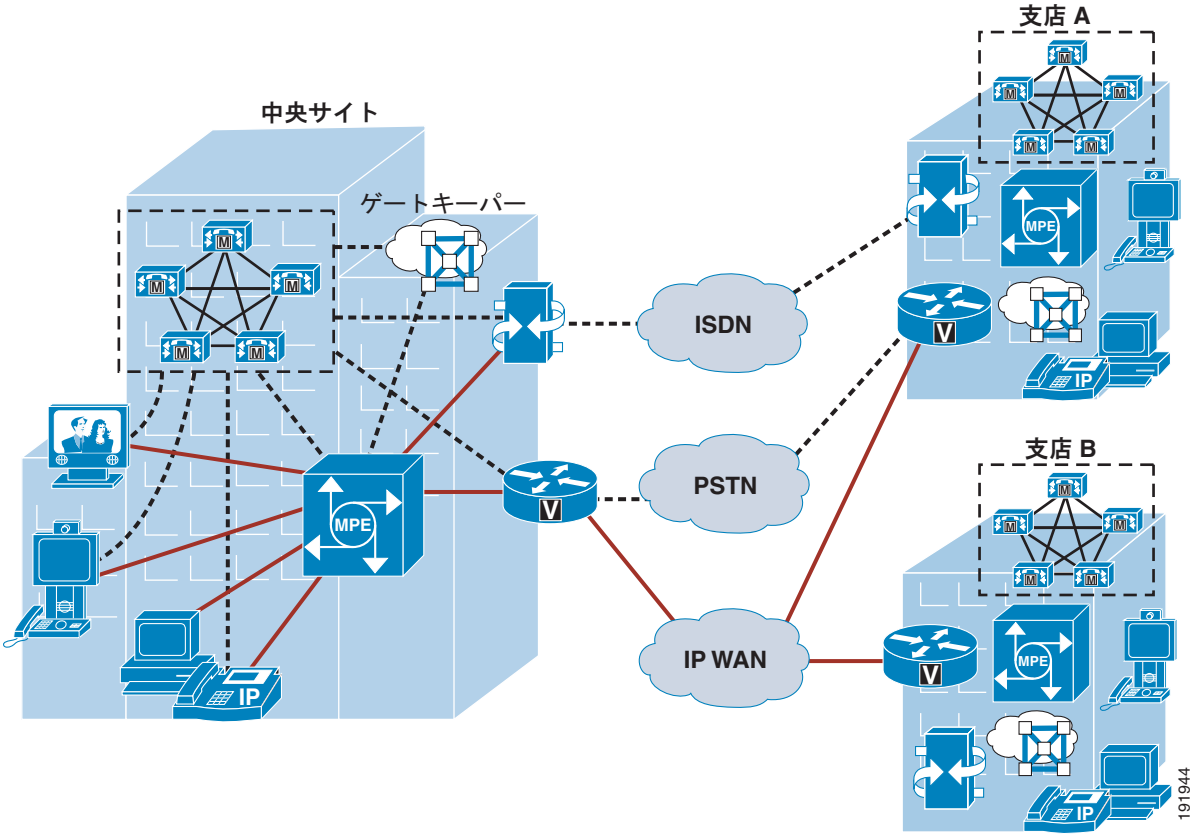
リモート参加者はローカル参加者と異なり、通常次の事項を考慮する必要があります。

- G.711 mu-law および a-law コーデック サポートに加え、IP WAN 全体の最適な帯域幅を使用できるように Unified MPE ではネイティブで G.729a をサポートします。
- ネイティブ G.729a コーデックのサポートにはさまざまな Unified MPE システム リソースが必要です。単一の G.729a オーディオ コールには、システム キャパシティ プール全体から 5 SRU 消費します。G.729a または G.711 以外のコーデックから G.711 コーデックへのトランスコーディングに外部コード変換リソースを配置すると、Unified MPE のスケーラビリティが向上します。ビデオ会議は外部トランスコーディング リソースとの互換性がないため、外部トランスコーディング リソースは音声会議でのみ使用してください。
- Web コラボレーションにはプロビジョニングが必要な大幅な帯域幅を要します（「Web アプリケーションと画面の共有に関する帯域幅の考慮事項」（P.15-10）を参照）。
- 通常のオペレーションでは、遠隔地のオフィスから送信されるすべての音声、ビデオおよび Web トラフィックは、IP WAN 経由で送信され、中央サイトの Unified MPE で終端します。Unified CM フォールバック モードでは、会議に参加するにはリモート エンドポイントから PSTN 経由で音声トラフィックが、中央サイトに設置された Unified MPE に送信されます。Unified CM フォールバック モードで動作しているエンドポイントに対してビデオ会議はサポートされません。
- 既存の Cisco Unified Communications と同一の QoS およびコール アドミッション制御メカニズムが必要です。コール アドミッション制御を目的とする場合、中央サイトで Unified MPE をテレフォニー ゲートウェイとして扱います。

分散型コール処理を使用するマルチサイト WAN

分散型コール処理を使用したマルチサイト WAN 配置では通常、Unified MPE は、Unified CM のローカル サイトに配置されます。図 15-3 では、分散型コール処理を使用したマルチサイト WAN 配置の例を挙げます。

図 15-3　分散型コール処理を使用したマルチサイト WAN 配置



分散型コール処理モデルの各サイトは、次のいずれかになります。

- 独自のコール処理エージェントを使用する単一サイト
- 集中型コール処理サイトとそれに関連したすべてのリモート サイト
- Voice over IP（VoIP）ゲートウェイを備えたレガシー PBX

これまでに説明した 2 種類のコール処理モデルの設計考慮事項は、分散型コール処理マルチサイト WAN 配置にも適用できます。

Unified MPE は単一のサーバで、カスケード化またはミラーリングされておらず冗長性機能を備えていません。したがって、一般的に単一サイトの単一の稼動中サーバが使用されます。Unified MPE サーバ間で通信することはありません（たとえば、図 15-3 のように中央サイトに設置された Unified MPE サーバと支店 A に設置されたサーバ間での通信）。

支店サイトのコール処理エージェント（たとえば、図 15-3 の支店 B）は中央サイトの Unified MPE に直接コールをルーティングできます。これを実行するには中央サイトの Unified MPE を指す H.323 ゲートウェイまたは SIP トランクを支店コール処理に定義します。できるだけ複数のコール処理エージェントが同一の Unified MPE を指さないようにしてください。支店 B に設置された Unified CM から中央サイトの Unified MPE にコールをルーティングするには、最初に中央サイトの Unified CM に

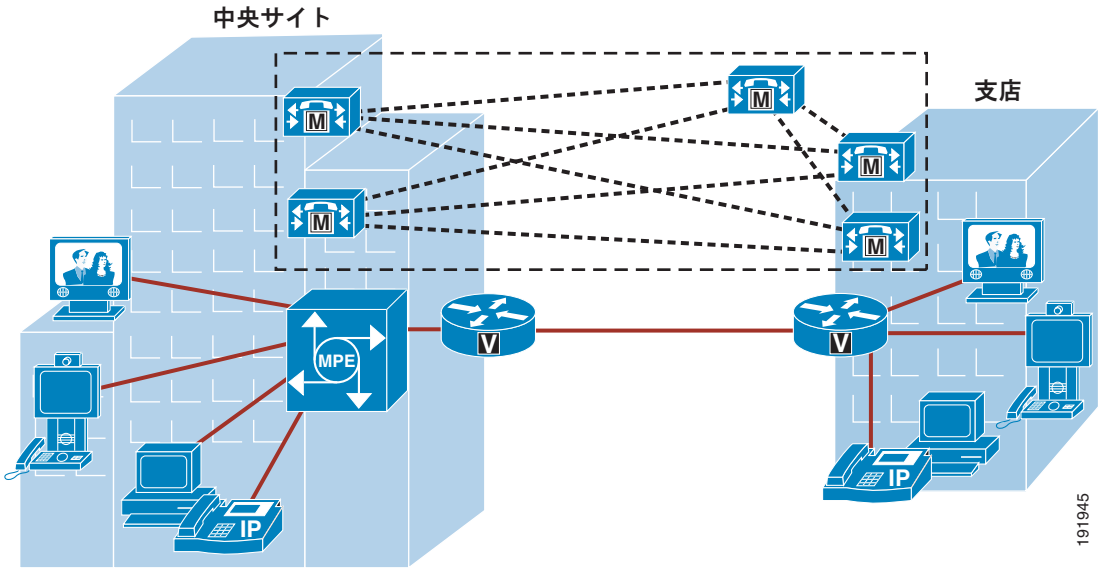
コールをルーティングし、中央サイトの Unified CM によってコールが Unified MPE に転送されるように配置してください。コール アドミッション制御は中央サイトのコール処理エージェントまたはクラスタ間コール処理の役割を果たすゲートキーパーによって実行されます。

WAN を介したクラスタ化

WAN を介したクラスタ化を使用した配置では、Unified CM クラスタは 1 つ以上のロケーションで分割されます。クラスタは大容量、高速の WAN または MAN リンクによって分割されます（図 15-4 を参照）。このコール処理モデルでは、すべての優先 Intra-Cluster Communication Signaling（ICCS）トラフィックは任意の 2 つの Unified CM 6.0 サーバ間について、片方向の最大遅延の合計ラウンドトリップ時間（RTT）が 40 ms 以下でなければなりません。また、Unified CM 6.1 以降のリリースでは 80 ms RTT 以下でなければなりません。

（注）　WAN 経由のクラスタ化には、RTT 要件に加えて、帯域幅に厳しい要件があります。詳細については、「IP WAN を介したクラスタ化」（P.2-22）を参照してください。

図 15-4　　WAN を介したクラスタ化



Unified MPE にはサーバ間の冗長性機能がないので、このコール処理モデルに備えられている高可用性を十分に活用できません。

このモデルに関する Unified MPE の設置および設計の考慮事項は、「分散型コール処理を使用するマルチサイト WAN」（P.15-7）で説明されている従来の設置モデルと同じです。

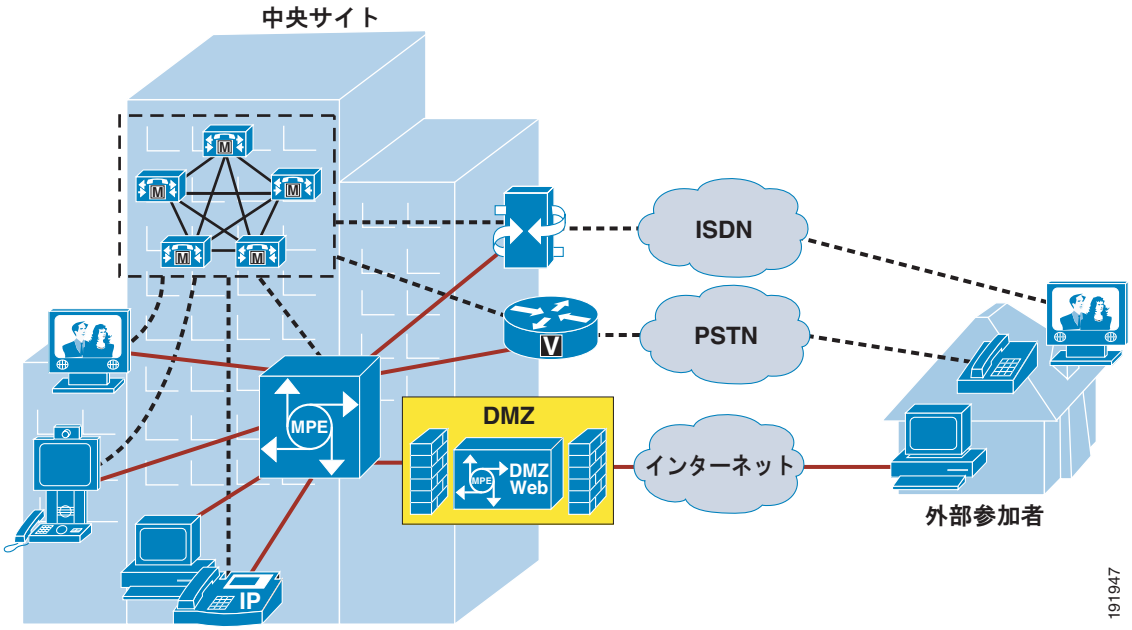
マルチサイトの冗長性を付加し、分散型コラボレーション システムを構築するには、Cisco Unified MeetingPlace の配置も検討してください。詳細については、「Cisco Unified MeetingPlace」（P.14-1）の章を参照してください。

セグメント化会議アクセス オプション

Unified MPE を非武装地帯（DMZ）に配置すると、外部ユーザ（プライベート ネットワーク外部のユーザ）が Unified MPE の会議に参加できるようになります。また、プライベート ネットワーク上に音声、ビデオ、およびプライベート会議を維持したまま外部ユーザがインターネット経由で会議に参加できるようになります。これをセグメント化会議アクセス（SMA）と言います。この設置オプションでは、プライベート Web 会議および公開 Web 会議を区別して、音声、ビデオ、および Web 会議の配置に安全性を確保します。ほとんどのお客様シナリオに強く推奨されるアプローチで、この章で既に説明した任意の設置モデルにも適用できます。

SMA 設計には 2 台のサーバが必要です。1 台は、内部ネットワーク上に設置する Unified MPE サーバで、もう 1 台は、公開会議に使用する DMZ 内の Unified MPE Web サーバです。図 15-5 に標準的な SMA 配置図を示します。

図 15-5　デュアルサーバ DMZ 配置



プライベート会議（音声、ビデオ、および Web）はすべて内部 Unified MPE サーバでホストされます。このサーバは内部ネットワーク上に存在しますが、DMZ にはありません。内部参加者は、プライベート会議と公開会議のいずれもスケジュールできますが、外部参加者は公開会議に参加のみできます。公開会議の場合、Web および音声ストリームが内部参加者から内部 Unified MPE サーバに送信されますが、外部参加者からは、Web トラフィックがインターネット経由で DMZ 内部の Unified MPE Web サーバ に送信されます。外部ユーザの音声ストリームは、内部ネットワーク上の音声ゲートウェイを介して内部 Unified MPE サーバ に接続されます。公開 Web コラボレーションの場合、会議は 2 つの Unified MPE Web インスタンスによってホストされます。1 つは内部ネットワーク上の内部 Unified MPE サーバで実行され、もう 1 つは DMZ 上の Unified MPE Web サーバで実行されます。

Unified MPE DMZ Web サーバ上の Web コンポーネントは内部 Unified MPE サーバの統合された Web コンポーネントと Web 会議情報を TCP ポート 1935 経由で Real Time Messaging Protocol（RTMP）を使用して共有します。TCP ポート 1935 を使用して接続を確立できない場合は、TCP ポート 443（HTTPS）を使用して接続を試みます。HTTPS 経由で接続を確立できない場合は、TCP ポート 80 を使用して接続を試みます。これにより、RTMP が HTTP 内部でトンネリングされます。内部 Unified MPE サーバによって音声会議イベントも SSH プロトコルを使用して外部 Unified MPE Web サーバに送信されます（TCP ポート 22）。2 つのサーバ間で通信するため、内部ファイアウォールの

Web ポート（TCP 1935、443、または 80）と音声ポート（TCP 22）のいずれも開放している必要があります。Web ユーザ ライセンス（UL）は内部 Unified MPE サーバと Unified MPE DMZ Web サーバで共有されています。

次のポートを内部企業ファイアウォールで開いてください。開いていない場合は、内部 Unified MPE サーバと Unified MPE DMZ Web サーバ間の通信がブロックされます。

- Web 会議の場合、TCP ポート 1935、80、または 443 のいずれか。
- 音声会議イベントをリレーするには、内部ネットワーク上のサーバから TCP ポート 22 経由で Secure Shell（SSH）を使用してアクセスする必要があります。また、Cisco Technical Assistance Center（TAC）では、Unified MPE を適切にサポートするため、SSH によるアクセスが必要な場合があります。

このデュアルサーバを使用した SMA 配置オプションにはシステムのスケーラビリティを向上する別の方法があります。この場合、2 台目の Unified MPE DMZ Web サーバ を、Web 会議すべてをホストするように設計します。この場合、DMZ 要件に従うことなく、Unified MPE を配置できます。2 台目の Web のみのサーバは、プライベート Web 会議には内部（DMZ ではない内部ネットワーク上）に配置し、外部参加者を公開 Web 会議に参加できるようにする場合、DMZ 上に配置します。このように配置することで、内部 Unified MPE サーバはシステム リソースをすべて音声およびビデオ 会議に割り当てることができるようになります。この配置では、内部 Unified MPE サーバによって音声会議とビデオ会議の要求のみがサービスされるので、G.729a コーデック会議および高帯域幅ビデオ会議のキャパシティを向上できます。内部参加者はプライベート会議と公開会議のいずれの場合も Web 会議すべてで常に Web トラフィックを 2 台目の Web サーバに送信します。この配置はお客様の用途に応じて特定の高キャパシティが要求される場合にのみ使用してください。通常の配置で使用することはお勧めしません。MCS モデルと関連するキャパシティの完全な一覧は Unified MPE 2.0 データシートを次からダウンロードしてください。

http://www.cisco.com/en/US/products/ps6533/products_data_sheets_list.html

コール アドミッション制御、帯域幅、および QoS

ここでは、Unified MPE 配置のコール アドミッション制御、帯域幅、および QoS に関する重要な考慮事項について説明します。

コール アドミッション制御

Unified MPE は、コール アドミッション制御を目的として使用する場合、テレフォニー ゲートウェイとして扱います。Unified CM は Unified MPE によってホストされる音声およびビデオ会議で、静的ロケーション コール アドミッション制御および RSVP 対応ロケーション アドミッション制御を実行できます。コール アドミッション制御の詳しい説明については、「コール アドミッション制御」（P.9-1）の章を参照してください。

Web アプリケーションと画面の共有に関する帯域幅の考慮事項

ユーザの共有するコンテンツに応じて画面の共有には多くの帯域幅が消費されます。多くの色調、写真が含まれるコンテンツなどは多くの帯域幅を必要とします。メディア イメージ、写真、または高解像度画像を共有すると、ネットワーク帯域幅に多くのキャパシティが必要になります。増加した帯域幅と画面共有の持つバースト性を考慮して次の事項を検討する必要があります。

設計上の考慮事項

100 Mbps の LAN 接続を使用すると、同時に実行できる Web コラボレーション セッション数が制限されます。可能な限り 2 スイッチ ポートへの接続には 1 Gbps 接続を使用します。

リモート サイトにいるユーザが WAN 経由で Web コラボレーションを実施する場合は、特別の考慮が必要になります。このようなユーザ用のクライアント フラッシュ セッション帯域幅または余剰帯域幅の設定値を下げて、WAN 上の負荷を減らす必要があります。Web コラボレーション データはユニキャストで配信されるため、最大データ バーストにリモート サイトのクライアント数を掛ける必要があります。たとえば、100 人のユーザがリモート サイトを利用しており、そのうちの 10 人が同時に Web コラボレーションを実施しているとします。リモート サーバからユーザに送信されるバースト データが 1.5 Mbps の場合、WAN 上のバーストは 15 Mbps になります。

過剰な Web コラボレーション データまたはその他のソースによって WAN リンクが輻輳すると、パケット損失、再送信、および遅延の増大が原因ですべてのトラフィックが低下します。輻輳が継続すれば、すべてのリモート コラボレーション セッションに悪影響が及びます。

クライアントの Web コラボレーション セッションに関する次の設定によって、参加者がデータを受信する速度だけでなく、プレゼンターがデータを送信する速度が制御されます。

- **Modem** ：帯域幅の上限を 28 kbps に設定
- **DSL** ：帯域幅の上限を 250 kbps に設定
- **LAN** ：帯域幅の上限を 1,500 kbps に設定

高解像度の画像または写真が共有された場合は、1,500 kbps 以上の帯域幅バーストに対応できます。複雑さが標準以上のプレゼンテーションまたはドキュメントを共有する場合は、サイズの大きな複雑なイメージが埋め込まれていない限り、1,500 kbps を超えるバーストを発生させないでください。輻輳が発生しても帯域幅設定値が自動的に調整されないため、手動で調整する必要があります。帯域幅のデフォルト値は LAN に基づきます。したがって、コラボレーション セッションの初期化時に設定してください。以前の設定に関係なく、新しいセッションは LAN に設定されます。

帯域幅の設定は、Web コラボレーション クライアント画面の次のロケーションで変更できます。

- 接続速度
  - Unified MPE から各ユーザに配信されるデータの速度を制御します。
  - プレゼンターから Unified MPE データが送信されるデータの速度を制御します。
  - プレゼンターのデータ送信速度は参加者がデータを受信するレートを制御しません。
- 余剰帯域幅の最適化
  - ユーザすべてにデータが送信されるレートを制御します。
  - 現在、WAN 帯域幅の利用に影響を及ぼす可能性があるデータ バーストの問題が発生しています。

（注） プレゼンターと参加者のクライアント Web インターフェイスにある My Connection Speed 設定は独立しています。プレゼンターのデータ送信速度は参加者がデータを受信するレートを制御しません。プレゼンターから Unified MPE へのデータ速度がモデム速度（28 kbps）に設定され、参加者のデータ受信速度が LAN の速度（1,500 kbps）に設定されている場合、参加者のデータ受信速度は最大 1,500 kbps です。

（注） Optimize Room Bandwidth 設定はユーザに送信されるレートを低減しますが、依然データの配信によってバーストが発生する可能性があり、WAN リンクを輻輳します。参加者のクライアントで My Connection Speed を変更すると、バーストを抑制し、データを安定したレートでクライアントに配信できます。Optimize Room Bandwidth 設定のバーストに関する問題は今後のリリースで対応される予定です。

イメージごとのビット数を制限すると、クライアントの解像度設定も使用帯域幅に影響します。640x480 ピクセルに設定された会議室では通常、1280x1024 ピクセルに設定された場合に比べて 3 分の 1 以下のトラフィックが生成されます。

推奨設計のまとめ

- Unified MPE インターフェイスを 1 Gbps で LAN に接続します。
- リモート ユーザが参加する会議では、リモート ユーザは My Connection Speed を **DSL** に設定します。輻輳が発生した場合、設定を **Modem** に下げるか、画像の解像度を下げます。

QoS

パケット損失、遅延、および遅延変動などの品質低下を最小限に抑えるため、Quality of Service（QoS）をネットワークに実装してください。これにより、会議中の高いユーザ エクスペリエンスを得ることができます。Unified MPE ではトラフィックのマーキングと分類に Differentiated Services Code Point（DSCP）メカニズムを採用しています。

Unified MPE から送信されるトラフィックは次の通り分類またはマーキングされます。

- SIP、H.323、および呼制御：マーキングなし
- 音声メディア（RTP）：EF としてマーキング（Unified MPE で変更可能）
- ビデオ メディア（RTP）：AF41 としてマーキング（Unified MPE で変更可能）
- Web トラフィック（HTTP および HTTPS）：マーキングなし
- Flash Web コラボレーション（RTMP）：マーキングなし

音声および呼制御トラフィック

音声および呼制御トラフィックは標準的に分類してください。詳しくは、「ネットワーク インフラストラクチャ」（P.3-1）の章を参照してください。Unified MPE とコール処理エージェントの接続が WAN 接続を経由する場合、呼制御トラフィックのマーキングを CS3（DSCP 24）に変更します。

Web インターフェイス トラフィック

主要 Web に推奨される優先順位はありません。Unified MPE に送信される Web トラフィックは他の内部 Web アプリケーション サーバのトラフィックと同様に扱います。

Flash Web コラボレーション トラフィック

大量の帯域幅が消費され、前の章で説明したようにデータにはバースト性があるので、WAN 全体で Web コラボレーション トラフィックを優先することはお勧めしません。Web コラボレーション トラフィックを優先する場合は、他の優先データとは異なる下位の分類を割り当てます。

Unified CM 経由の外部ディレクトリ統合

Unified CM 経由で Unified MPE を外部ディレクトリと統合すると、次の 2 つの機能が主に利用できるようになります。

- Unified MPE での自動プロファイル作成
- サードパーティ製ディレクトリを使用した外部認証

Unified MPE が Unified CM に統合されると（外部 LDAP を使用して統合）、ユーザが初めて Unified MPE にログインする際、ユーザ プロファイルが自動的に作成されます。ユーザはこのプロファイルを使用してその場で会議をスケジュールしてシステムを使用できます。

Unified MPE にログインするには、ユーザは正しいユーザ ID とパスワードのプロファイルが Unified MPE でネイティブに設定されている必要があります。あるいは、ユーザは Unified CM が統合されている企業外部ディレクトリで認証されている必要があります。

Cisco Unified CM 3.3 以降のリリースおよび、4.*x* の外部 LDAP ディレクトリとの正常な統合には、Unified CM LDAP プラグインのアプリケーションが必要ですが、Unified CM 5.*x*、6.*x*、および 7.*x* では外部 LDAP システムに対するスキーマの変更は不要です。Unified MPE では、Unified CM でサポートされている外部 LDAP システムおよびバージョンのみがサポートされます。Unified MPE は Cisco AVVID XML Layer（AXL）Simple Object Access Protocol（SOAP）を使用して Unified CM 5.*x*、6.*x*、および 7.*x* と統合されます。Unified MPE では LDAP を直接使用して企業外部ディレクトリと統合できません。

（注）　LDAP 統合は Cisco Unified Communications Manager Express（Unified CME）、音声ゲートウェイ、または SIP システムではサポートされません。

詳細については、『*Administrator's Configuration and Maintenance Guide for Cisco MeetingPlace Express*』を次から参照してください。

http://www.cisco.com

H.323 および SIP を使用した Unified CM との統合

Unified CM との統合には複数の方法があります。ここでは、そのうちの H.323 および SIP 直接統合を使用した 2 つの方法を解説します。3 つ目の方法については、（H.323 経由のゲートキーパー）次のセクションで説明します。

Unified MPE システムは、IP ゲートウェイ ソフトウェアを搭載しており、標準ベースの H.323 および SIP システムと統合できます。ただし、これらのシステムの統合ポイントには Unified CM が頻繁に使用されます。Unified CM と統合すると、Unified MPE でホストされる会議のダイヤル プラン解決、通話料金詐欺の防止、および、コール アドミッション制御を実行できるようになります。これにより、Unified MPE システムの構成を変更することなく任意の呼制御システムから Unified MPE に着信コールを送信できるようになります（音声ユーザ ライセンスが適用されるまで Unified MPE によって受信はブロックされません。ライセンスが適用されると、発信者にはビジー トーンが発信されます）。H.323 または SIP ゲートウェイ（同時は不可）への発信ダイヤル要求に必要なのは Unified MPE の「outdial」設定のみです。Unified MPE には通話料金詐欺の防止やルーティングなどを提供する機能が搭載されていないため、発信ダイヤル コールはこれらの機能があるコール処理システムを使用して解決します。

Unified MPE 音声システムおよびビデオ システムにダイヤルインできる番号は最大 4 つパブリッシュできます。パブリッシュされた番号は通知テンプレートで自動的に利用できるようになります。番号には次のタイプがあります。

- フリー ダイヤル（例：800-XXX-XXXX）
- DID または Direct CO（例：408-XXX-XXXX）国際通話の場合）
- ローカルの 3 桁、4 桁、または 5 桁の内部番号（例：4000）
- プライベート ネットワーク ダイヤル プラン（例：774-4000）

H.323 ゲートウェイ

最も手軽に統合するには Unified MPE を Unified CM で H.323 ゲートウェイとして定義します。この方法を実行する場合、管理者は Unified CM で Unified MPE システムにコールをルーティングする定義済みの H.323 ゲートウェイを使用する 1 つ以上のルート パターンも設定します。

SIP トランク

Unified MPE を SIP 接続経由で Unified CM に統合するには、SIP トランクを Unified CM から Unified MPE に直接設定できます。この統合には次の設計ルールが適用されます。

- SIP トランクから Unified MPE に個別の SIP セキュリティ プロファイルを作成して関連付ける必要があります。セキュリティ プロファイルではトランスポートを UDP に設定します。デフォルトでは TCP が設定されていますが、Unified MPE では利用できません。
- SIP トランクには Unified MPE で SIP アーリーオファーと SIP 遅延オファーの両方がサポートされているため、MTP は不要です。SIP トランクの MTP Required オプションのチェックボックスはオンに*しない*でください。
- 関連メディア リソース グループ リストで MTP が利用可能であることを確認します。一部のエンドポイントでは Unified MPE へのコールが完了すると動的に MTP を呼び出すことができます。

（注） 任意のビデオ セッションで Cisco Unified Personal Communicator を使用する場合は、SIP トランクを Unified CM と統合することをお勧めします。

ゲートキーパーの統合

Unified MPE は、ここで紹介する設計の考慮事項に従ってゲートキーパー環境に統合することができます。ゲートキーパーの登録方法は、単一の E.164 アドレスを使用してゲートウェイとして行います。Unified MPE のビデオ会議では常にオーディオのみのセッションとして開始され、システムによってビデオ対応エンドポイントが特定されるとビデオ会議にエスカレーションされます。Unified MPE から帯域幅要求（BRQ）メッセージがゲートキーパーに送信され、ビデオ エンドポイントとのメディア機能の交信が開始される前に要求される帯域幅が確認されます。ビデオにエスカレーションするために必要な帯域幅がない場合は、オーディオのみセッションが持続されます。

ゲートキーパー環境で使用する Unified MPE システムを設計する際、ここで紹介する設計上の考慮事項に配慮してください。

設計上の考慮事項

（注） Unified MPE は特定のゾーンに登録されません。複数のローカル ゾーンが存在する場合は、デフォルトの（または初期の）ローカル ゾーンが常に使用されます。

Unified MPE で強制的に特定のローカル ゾーンを使用するには、Unified MPE を登録しないすべてのゾーンで **no zone** コマンドを使用します。たとえば、次のコマンドを入力すると、Unified MPE（アドレスは 10.20.110.50 を指定）が強制的に testzone2 に登録されます。

```
gatekeeper
    zone local mp2-gk1 mp2.com 10.20.105.50
    zone local testzone2 mp2.com
    no zone subnet mp2-gk1 10.20.110.50/32 enable
```

（注）　Unified MPE 直接会議のダイアルイン機能では、追加のゲートキーパー設定が必要です。

Unified MPE は単一の E.164 アドレスを使用して H.323 ゲートウェイ として登録されます。したがって、会議への直接ダイアルインの内線番号は、手動でゲートキーパーに次の例で示すいずれかを入力しないとゲートキーパーを介して接続できません。

オプション 1：ルーティングにゾーン プレフィックスを使用する（推奨）

この例では内線番号 1000 ～ 1009 を Unified MPE にルーティングします。

```
gatekeeper
    zone local mp2-gk1 mp2.com 10.20.105.50
    zone prefix mp2-gk1 100.
    gw-type-prefix 1#* default-technology gw ipaddr 10.20.110.50 1720
```

オプション 2：静的 E.164 アドレスを使用する（非推奨）

```
gatekeeper
    alias static 10.20.110.50 1720 gkid mp2-gk1 gateway voip ras 10.20.110.50 62675 e164
1005 e164 1008 e164 1007 e164 1006


show gatekeeper endpoints

CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type    Flags
--------------- ----- --------------- ----- ---------         ----    -----
10.20.110.50    1720  10.20.110.50    62675 mp2-gk1           UNKN-GW S
    E164-ID: 1000
    H323-ID: MeetingPlace
    E164-ID: 1005 (static)
    E164-ID: 1008 (static)
    E164-ID: 1007 (static)
    E164-ID: 1006 (static)
```

容量とサイジング

1 台の Cisco Media Convergence Server（MCS）7845 H2 上の Unified MPE は G.711 コーデックを使用した音声会議で最大 200 の ユーザを同時にサポートします。また、ビデオ会議では最大 150（384 kbps まで、ビデオ エンドポイントの音声 ポートが 1 つ、会議で使用されるビデオ ポートが 1 つの場合）、Web 会議では最大 200 のユーザを同時にサポートできます。Segmented Meeting Access オプションをすべての Web 会議 が 2 台目の MCS 7845 H2 でホストされるように配置されている場合は、同時にサポートされるユーザの上限はオーディオのみの場合は 200、ビデオの場合は 200、Web 会議の場合は 200 になります。Segmented Meeting Access の配置オプションの詳細は、「セグメント化会議アクセス オプション」（P.15-9）を参照してください。

（注）　旧サーバ モデルを配置するとキャパシティが低下します。MCS モデルと関連するキャパシティの完全なリストは Unified MPE 2.0 データ シート（http://www.cisco.com/en/US/products/ps6533/products_data_sheets_list.html）を参照してください。

システム リソース ユニット（SRU）

G.729a コーデックと高帯域ビデオ会議（384 kbps 以上）の使用はシステム全体のキャパシティに影響します。Unified MPE のシステム キャパシティを推定する場合、システム リソース ユニット（SRU）の概念を理解する必要があります。システムで利用可能な SRU は、配置された Media Convergence Server（MCS）の種類に基づいて決定されます。結果は特定のコーデックとビデオを指定すると、Web 管理センターの 会議設定ページで参照できます。ユーザ セッション 1 つに必要な音声、ビデオ、または Web SRU はそれぞれ対応するシステムの音声、ビデオ、または Web ユーザ ライセンス（UL）を 1 つ使用します。

ビット レートが 384 kbps 以下のビデオ セッションには 1 SRU が必要です。384 ～ 768 kbps のビデオ セッションには 2 SRU 必要です。G.711 コーデックを使用した音声セッションには 1 SRU、G.729a コーデックを使用した音声セッションには 5 オーディオ SRU が必要です。Web 会議 にはユーザ セッションあたり、2 SRU 必要です。

参加者が G.711 コーデックを使用して 384 kbps ビデオ ビット レート（またはそれ以下）でビデオ会議に参加すると、Unified MPE によって 2 SRU、ビデオ ユーザ ライセンス（UL）1 つ、オーディオ UL 1 つがこの参加者に割り当てられます。同じビデオ エンドポイントが G.729a コーデックを使用して会議に参加した場合、コールの音声とビデオ部分に 6 SRU が割り当てられます。

Unified MPE では、システムのキャパシティ計算にフロー コントロール ビット レートは考慮されません。たとえば、384 kbps の参加者が会議に 768 kbps ビデオ セッション ビット レートで参加すると、セッション ビット レートは 384 kbps まで低減されますが、既存のセッションでは Unified MPE によってビデオ UL が 2 つ維持されます。

（注）　ソリューション エキスパート ツールは設計基準に基づいて MCS モデル サイズを特定する支援をします。このツールは（適切なログイン認証を経て）http://www.cisco.com/go/sx から利用できます。

冗長性

ここでは次の冗長性について説明します。

- 「Unified MPE サーバの冗長性」（P.15-16）
- 「ゲートキーパーを使用した冗長性」（P.15-17）
- 「H.323 ゲートウェイ統合を使用した冗長性」（P.15-17）
- 「SIP トランク統合を使用した冗長性」（P.15-18）

Unified MPE サーバの冗長性

Unified MPE は冗長性が組み込まれていないスタンドアロン サーバですが、一部のサーバ コンポーネント自体に冗長性が備えられています。ミラーリングされたドライブ、二重化電源、冗長ファンなどによって内部サーバに高度の冗長性と可用性が実現されます。Unified MPE には Ethernet ポートが 2 つ備えられていますが、それぞれは異なる目的で使用されます。1 つは呼制御、Web スケジューリング、管理インターフェイス、およびメディアに使用します。もう 1 つは Web コラボレーションに使用します。

Unified MPE サーバ間のカスケード化された会議は実行できません。Segmented Meeting Access（SMA）オプションを使用すると、Unified MPE サーバと Unified MPE DMZ Web サーバで内部データベースを共有します。Unified MPE はスタンドアロン サーバですが、同じ Unified CM ディレクトリを使用して複数の Unified MPE サーバを配置できます。この構成では、共通のディレクトリから別

のサーバにログインできるので、通常使用するサーバが停止した場合でも素早く会議をスケジュールしなおすことができます。このオプションでは完全にライセンスが取得された複数の Unified MPE サーバ が必要です。

ゲートキーパーを使用した冗長性

着信コール

着信コールに関連した冗長性はゲートキーパーの冗長性です。これは発信コールにも適用されます。ゲートキーパーの冗長性は次のいずれかの方法によって実装できます。

- 代替ゲートキーパー

  この方法では、ゲートキーパーは冗長ゲートキーパー クラスタに設定されます。Unified MPE では定義済みのゲートキーパーを使用して登録されます。登録が完了すると、ゲートキーパーによって Unified MPE にクラスタの代替ゲートキーパーが通知されます。このゲートキーパーはエラー発生時に使用されます。

- ゲートキーパーのホットスタンバイ ルータ プロトコル（HSRP）

  この方法では、2 つのゲートキーパーによって単一の HSRP IP アドレスが共有されます。エラーが発生すると、Unified MPE は同じゲートキーパー IP アドレスを使用してセカンダリ ゲートキーパーに登録されます。

（注）　代替ゲートキーパー情報は登録時に送信され、Unified MPE に恒久的に保存されていないため、プライマリ ゲートキーパーにアクセスできない場合にサーバを起動または再起動すると Unified MPE は代替ゲートキーパーに登録できません。

ゲートキーパーの冗長性に関する詳細については、「ゲートキーパーの冗長性」（P.8-27）を参照してください。

発信コール

冗長性を得るために、単一クラスタ内の複数の Unified CM サーバを単一のゲートキーパーに登録できます。この場合、Unified MPE からの発信ダイヤルを完了するのに、ゲートキーパーによってアクティブな Unified CM が選択されます。

前セクション（「着信コール」（P.15-17））で説明したように、ゲートキーパーの冗長性は発信コールにも適用されます。

H.323 ゲートウェイ統合を使用した冗長性

着信コール

Unified MPE を H.323 ゲートウェイとして統合すると、着信コールはクラスタ内の利用可能な Unified CM サーバから送信されます。サーバが停止すると、着信コールはクラスタ内の別のサーバから自動的に送信されます。

発信コール

Unified MPE では、Unified CM、Unified CME、およびその他の H.323 対応コール処理エージェントをポイントする複数の H.323 発信ダイヤル接続を定義できます。発信コールは発信ダイヤル コール エラーが発生するまで Unified MPE によってリストの 1 つ目にある H.323 対応コール処理エージェントに継続して送信されます。エラーが発生すると、Unified MPE によって H.225 セットアップ メッセー

ジがリストにある次の利用可能なコール処理エージェントに自動的に送信されます。コール処理エージェントが停止しても既存のコールには影響しません。ユーザが切断すると、既存のメディア接続が失われます。

SIP トランク統合を使用した冗長性

着信コール

SIP トランクを使用して Unified MPE を統合すると、着信コールはクラスタ内の利用可能な Unified CM サーバ から送信されます。サーバが停止すると、着信コールはクラスタ内の別のサーバから自動的に送信されます。

発信コール

Unified MPE では、Unified CM、Unified CME、およびその他の SIP 対応コール処理エージェントをポイントする複数の SIP 発信ダイヤル接続を定義できます。発信コールは発信ダイヤル コール エラーが発生するまで Unified MPE によってリストの 1 つ目にある SIP 対応コール処理エージェントに継続して送信されます。エラーが発生すると、Unified MPE によって SIP INVITE メッセージがリストにある次の利用可能なコール処理エージェントに自動的に送信されます。コール処理エージェントが停止しても既存のコールには影響しません。ユーザが切断すると、既存のメディア接続が失われます。

（注）　Unified MPE では H.323 と SIP 接続を同時に使用した発信ダイヤル機能は利用できません。H.323 および SIP 発信ダイヤル機能は Unified MPE で片方のみ利用できます。

その他の重要な設計上の考慮事項

ここでは、これまでに説明していないその他の重要な設計上の考慮事項について説明します。

ネットワーク接続

- Unified MPE では接続にネットワーク インターフェイス カード（NIC）が 2 枚使用されています。ここでは、両方の NIC は同じサブネットに取り付けて、同じデフォルト ゲートウェイを指定します。NIC が異なるサブネットに取り付けられると接続の問題が発生します。
- Unified MPE サーバの IP アドレスを変更するには、**net** コマンドを使用して、サーバに SSH 経由で接続します。ログインには **mpxadmin** を使用します。その他の方法で IP アドレスを変更すると Unified MPE の設定が正しく変更されない場合があり、設定エラーの原因となります。システムのホスト名とドメイン名を変更するには、パッチを適用します。パッチは Cisco Technical Assistance Center（TAC）から入手できます。

IP テレフォニー ゲートウェイ

- Unified MPE で使用するゲートウェイは「ゲートウェイ」（P.4-1）の章で説明されている標準の推奨設定を行います。
- Unified MPE に影響する主な ゲートウェイに関する問題はエコー キャンセレーションです。この問題が発生した場合、ゲートウェイのテール割り当てを 128 ms に増加することをお勧めします。

CHAPTER 16

IP ビデオ テレフォニー

シスコは、IP ビデオ テレフォニー ソリューションを Cisco Unified Communications Manager（Unified CM, formerly Cisco Unified CallManager）Release 4.0 で導入しました。ビデオは Unified CM に完全に統合され、シスコおよびシスコの戦略パートナーから多くのビデオ エンドポイントも入手できるようになりました。Cisco Unified Video Advantage は、Cisco Unified IP Phone と同様に、簡単に配置、管理、および使用できます。

この章の新規情報

表 16-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

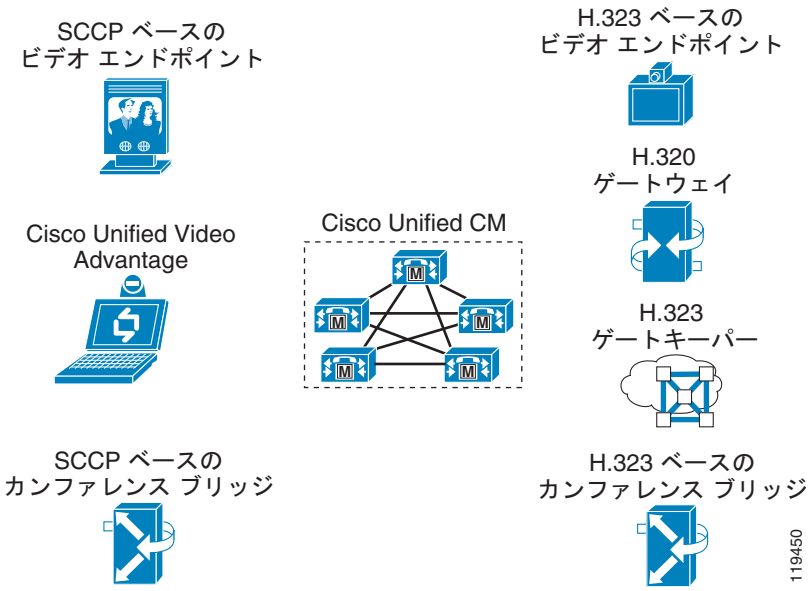
表 16-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
カンファレンス ブリッジの選択	「インテリジェント ブリッジ選択機能」（P.16-17）
Cisco IP Communicator の SIP オプション	「Cisco IP SoftPhone および Cisco IP Communicator」（P.16-47）

IP ビデオ テレフォニー ソリューションのコンポーネント

Cisco IP ビデオ テレフォニー ソリューションは、Cisco Unified Communications Manager（Unified CM）、H.323 電話会議、セッション開始プロトコル（SIP）電話会議、および Skinny Client Control Protocol（SCCP）電話会議に対応する Cisco Unified Videoconferencing 3500 シリーズ Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）、Cisco Unified Videoconferencing 3500 シリーズ H.320 ゲートウェイ、Cisco IOS H.323 ゲートキーパー、Cisco Unified Video Advantage、Cisco IP Video Phone 7985、サードパーティ製の SCCP ビデオ エンドポイント ソリューション、および Polycom、Tandberg、Sony などのパートナーが取り扱っている既存の H.323 または SIP 準拠製品で構成されます（図 16-1 を参照）。

図 16-1　IP ビデオ テレフォニーのコンポーネント



管理に関する考慮事項

この項では、ビデオ テレフォニーに関係する Unified CM Administration の次の構成要素について説明します。

- 「プロトコル」（P.16-2）
- 「リージョン」（P.16-3）
- 「トポロジ対応ロケーション」（P.16-6）
- 「Retry Video Call as Audio」（P.16-8）
- 「Wait for Far-End to Send TCS」（P.16-10）

プロトコル

Unified CM は、多くのプロトコルをサポートします。任意のデバイスから任意の別のデバイスを呼び出すことができますが、ビデオは SCCP、H.323、および SIP デバイスでのみサポートされます。具体的には、Cisco Unified CM Release 7.*x* において、次のプロトコルではビデオがサポートされません。

- コンピュータ/テレフォニー インテグレーション（CTI）アプリケーション（TAPI および JTAPI）
- メディア ゲートウェイ コントロール プロトコル（MGCP）

したがって、現在 Unified CM でサポートされるコールのタイプは、表 16-2 に示すとおりです。

表 16-2　Unified CM Release 7.x でサポートされるコールのタイプ

発信デバイス タイプ	着信デバイス タイプ				
	SCCP	H.323	MGCP	TAPI/JTAPI	SIP
SCCP	音声とビデオ	音声とビデオ	音声のみ	音声のみ	音声とビデオ
H.323	音声とビデオ	音声とビデオ	音声のみ	音声のみ	音声とビデオ

表 16-2　Unified CM Release 7.x でサポートされるコールのタイプ （続き）

発信デバイス タイプ	着信デバイス タイプ				
	SCCP	H.323	MGCP	TAPI/JTAPI	SIP
MGCP	音声のみ	音声のみ	音声のみ	音声のみ	音声のみ
TAPI/JTAPI	音声のみ	音声のみ	音声のみ	音声のみ	音声のみ
SIP	音声とビデオ	音声とビデオ	音声のみ	音声のみ	音声とビデオ

表 16-3 は、現在 Unified CM でサポートされている音声とビデオのアルゴリズムおよびプロトコルを示しています。

表 16-3　Unified CM Release 7.x でサポートされる機能

H.323	SCCP	SIP
H.261	H.261	H.261
H.263、H.263+	H.263、H.263+	H.263、H.263+
H.264	H.264	H.264
Cisco VT Camera Wideband ビデオ コーデック（H.323 クラスタ間トランクのみ）	Cisco VT Camera Wideband ビデオ コーデック	
G.711 A-law および mu-law	G.711 A-law および mu-law	G.711 A-law および mu-law
G.723.1	G.723.1	G.723.1
G.728	G.728	G.728
G.729、G.729a、G.729b、G.729ab	G.729、G.729a、G.729b、G.729ab	G.729、G.729a、G.729b、G.729ab
G.722	G.722	G.722
G.722.1		
H.224 遠端カメラ制御（Unified CM でサポートされますが、すべてのエンドポイントでサポートされるわけではありません） プロトコル インターワーキングなし	H.224 遠端カメラ制御（Unified CM でサポートされますが、すべてのエンドポイントでサポートされるわけではありません）プロトコル インターワーキングなし	H.224 遠端カメラ制御（Unified CM でサポートされますが、すべてのエンドポイントでサポートされるわけではありません） プロトコル インターワーキングなし
アウトオブバンド DTMF（H.245 英数字） RFC2833 AVT Tones（SIP コールへの H.323 クラスタ間トランクの場合のみ）	アウトオブバンド DTMF RFC2833 AVT Tones	RFC2833 AVT Tones Unsolicited SIP Notify KPML
	Cisco ワイドバンド オーディオ	

リージョン

リージョンを設定するときは、Unified CM Administration の 2 つのフィールド、Audio Codec と Video Bandwidth を設定します。オーディオ設定ではコーデック タイプを指定し、ビデオ設定では許可する帯域幅の量を指定します。ただし、表記は異なりますが、Audio Codec フィールドと Video

Bandwidth フィールドは、実際には似た機能を実行します。Audio Codec フィールドは、音声のみのコールおよびビデオ コールの音声チャネルに許可される最大ビットレートを定義します。たとえば、リージョンの Audio Codec を G.711 に設定した場合、Unified CM はそのリージョンの音声チャネルに許可される最大帯域幅として 64 kbps を割り当てます。この場合、Unified CM は G.711、G.722、G.728、iLBC、または G.729 を使用するコールを許可します。ただし、Audio Codec を G.729 に設定すると、Unified CM は、音声チャネルに許可される帯域幅の最大量として 8 kbps だけを割り当てます。この場合、iLBC、G.728、G.711、および G.722 はすべて 8 kbps より多く帯域幅を使用するため、G.729 を使用するコールだけが許可されます。

（注）　両方のエンドポイントが G.711 と G.722 をサポートしている場合、ワイドバンド コーデックである G.722 がネゴシエートされます。

（注）　Audio Codec 設定は、ビデオ コールの音声チャネルにも適用されます。

Video Bandwidth フィールドは、コールのビデオ チャネルに許可される最大ビットレートを定義します。ただし、従来のビデオ会議製品での慣例に従い、このフィールドに使用する値には、音声チャネルの帯域幅も含めます。たとえば、G.711 の音声を使用する 384 kbps のコールを許可するには、Video Bandwidth フィールドに 320 kbps ではなく 384 kbps を設定します。

つまり、Audio Codec フィールドは音声のみのコールおよびビデオ コールの音声チャネルに使用する最大ビットレートを定義し、Video Bandwidth フィールドは、ビデオ コールに許可される最大ビットレート（コールの音声部分を含む）を定義します。

各デバイスは、表 16-4 で示すように、特定の音声コーデックのみをサポートするため、正しい音声コーデックの帯域幅制限を選択することが重要です（特定のエンドポイントでサポートされるコーデックの最新リストについては、そのエンドポイントの製品マニュアルを参照してください）。

表 16-4　エンドポイント デバイスでサポートされている音声コーデックのタイプ

コーデック タイプ	Cisco 7900 シリーズ IP Phone	SCCP サードパーティ製ビデオ エンドポイント	一般的な H.323 または SIP エンドポイント	Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイ	Cisco Unified Videoconferencing 3500 シリーズ MCU
G.729	あり	あり、モデルによる	なし	なし	あり、モデルによる
G.728	なし	あり、モデルによる	あり	あり（トランスコーダを使用）	あり、モデルによる
G.711	あり	あり	あり	あり	あり
G.722	あり、モデルによる	あり	あり	あり（トランスコーダを使用）	あり、モデルによる
Cisco ワイドバンド オーディオ	あり、モデルによる	なし	なし	なし	なし

表 16-4 で示すように、リージョンを G.729 に設定した場合、ビデオ会議デバイスによっては、このタイプのコーデックをサポートできないものがあります。たとえば、Cisco Unified Video Advantage エンドポイントと Tandberg T1000 エンドポイントとの間のコールは失敗します。または、このコールに Unified CM が音声変換リソースを割り当てます。

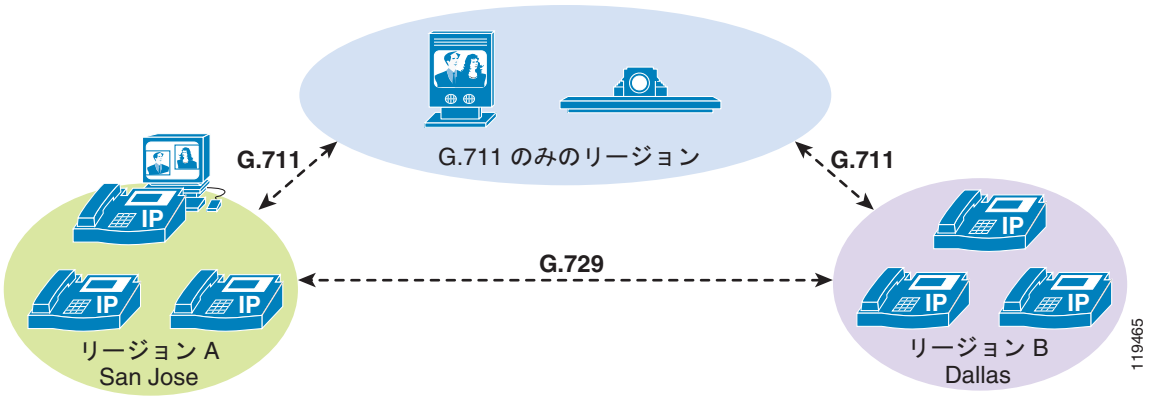
Cisco Unified CM Release 5.0 では、Cisco IOS Enhanced Media Termination Point に基づく音声変換リソースが導入されました。これによって、パススルー コーデックによるビデオ ストリームのサポートを継続しながら、ビデオの音声ストリームのトランスコーディングができます。パススルー コーデックは、トランスコーディングが必要なストリームには使用できないため、ビデオ ストリームにのみ使用されます。パススルー コーデックを使用するには、次の 3 つの条件をすべて満たす必要があります。

- 2 つのエンドポイント デバイスのコーデック能力が一致している。
- どちらのエンドポイントでも、**MTP Required** が*オフ*になっている。
- すべての中間リソース デバイス（MTP およびトランスコーダ）がパススルー コーデックをサポートしている。

従来のトランスコーダは、現在、パススルー機能をサポートしていません。そのため、コールは音声のみとして接続され、G.729 と G.711 の間でトランスコーディングされます。Cisco IOS Enhanced Transcoder を使用せずにこの状態を防止するには、G.711 を使用するようにリージョンを設定する必要があります。ただし、G.711 に設定されたリージョンは、2 つの IP Phone 間の音声コールにも G.711 を使用します。この場合、WAN で消費される帯域幅が増えます。

帯域幅を節約するために音声のみのコールに G.729 を使用し、ビデオ コールに G.711 を使用する場合は、G.729 をサポートしないビデオ エンドポイント用に G.711 を使用するリージョンを設定し、IP Phone 用に G.729 を使用する別のリージョンを設定する必要があります（図 16-2 を参照）。この方式を使用すると、必要なリージョンの数が増えますが、望ましいコーデックと帯域幅の割り当てが得られます。

図 16-2　ビデオ コールに G.711 を使用し、音声のみのコールに G.729 を使用



（注） ビデオを禁止するリージョンのペアを設定できます。このリージョン ペアにある 2 つのビデオ対応デバイスが相互に通話しようとした場合、Retry Video Call as Audio がオンになっていれば、音声のみとして接続されます。オフになっている場合は、AAR 再ルーティング ロジックが実行されます。

表 16-5 は、設定例とその結果を示しています。

表 16-5　さまざまなリージョン設定のシナリオ

リージョン設定	Retry Video as Audio の設定	結果
リージョンでビデオを許可する。	有効	ビデオ コールは許可される。
リージョンでビデオを許可する。	無効	ビデオ コールは許可される。

表 16-5　さまざまなリージョン設定のシナリオ （続き）

リージョン設定	Retry Video as Audio の設定	結果
リージョンでビデオを許可しない。	有効	ビデオ コールは音声として処理される。
リージョンでビデオを許可しない。	無効	AAR が設定されていない場合、ビデオ コールは失敗する（ビジー トーンが再生され、「Bandwidth Unavailable」メッセージが表示される）。

Video Bandwidth フィールドには、1 ～ 8128 kbps の値を指定できます。ただし、H.323 および H.320 ビデオ会議デバイスとの互換性を維持するために、このフィールドには常に、56 または 64 kbps の倍数の値を入力することをお勧めします。したがって、このフィールドの有効な値としては 112 kbps、128 kbps、224 kbps、256 kbps、336 kbps、384 kbps などがあります。

エンドポイントで要求されるコール速度がリージョンに設定されている帯域幅値を超えた場合、Unified CM は自動的に、リージョン設定で許可された値に適合するようにコールをネゴシエートします。たとえば、H.323 エンドポイントが別の H.323 エンドポイントを 768 kbps で呼び出しているが、リージョンは最大 384 kbps を許可するように設定されていたとします。発信側からの着信 H.225 セットアップ要求はコール速度として 768 kbps を提示しますが、Unified CM は、着信側への発信 H.225 セットアップ メッセージで、この値を 384 kbps に変更します。そのため、着信側エンドポイントは、開始するコールが 384 kbps であると認識し、このレートでコールがネゴシエートされます。発信側エンドポイントは、要求した帯域幅として 768 kbps を提示しますが、ネゴシエートされた帯域幅は 384 kbps になります。

ただし、リージョンの Video Bandwidth を「None」に設定した場合は、着信側デバイスの Retry Video Call as Audio が有効かどうかに応じて、Unified CM はコールを終了するか（この場合、H.225 Release Complete メッセージを発信側に送信）、音声のみのコールとして通過を許可します（「Retry Video Call as Audio」（P.16-8）を参照）。

トポロジ対応ロケーション

ロケーション間のコールで使用できる帯域幅の量を制限する方式は、2 種類あります。Cisco Unified CM 4.0 では、ロケーションでのビデオ コールのサポートが導入されました。具体的には、Cisco Unified CM のロケーション オプションによって、あるロケーションと別のロケーションの間のすべてのコールに許可される合計帯域幅が定義されます。この合計帯域幅の値は、従来のハブアンドスポーク ネットワーク トポロジに十分に対応します。Cisco Unified CM Release 5.*x* では、リソース予約プロトコル（RSVP）に基づくトポロジ対応ロケーションを使用して、2 つのサイト間のパスに十分な帯域幅があるかどうかを判断するオプションが用意されています。RSVP を使用すると、複雑なトポロジに対応するホップ単位のチェックが可能になり、RSVP アプリケーション ID を使用して音声帯域幅とビデオ帯域幅を個別にサポートできます。

（注）　静的ロケーションと RSVP ベースのロケーションは、異なるモデルを使用して、音声コールとビデオ コールを区別します。詳細については、「コール アドミッション制御」（P.9-1）を参照してください。

RSVP ベースのロケーションでは、RSVP ポリシーの概念が採用されています。多くのポリシー オプションがありますが、主に次の 2 つのカテゴリに分けられます。

- コールを完了するために、ビデオ ストリームの RSVP 予約が必須。コールは失敗するか（ビジー トーンが再生され、「Bandwidth Unavailable」メッセージが表示される）、Automated Alternate Routing（AAR）によってコールの再ルーティングが試行されます。
- ビデオ ストリームの RSVP 予約が望ましい。

最初に、リージョンに設定された音声コーデックとビデオ帯域幅で、ビデオ コールの最大速度（ビットレート）が定義されます。予約要求として、最大ビット レートを使用してコールのオーディオ ストリームとビデオ ストリームの RSVP 予約が Cisco RSVP Agent から送信されます。ビデオ ストリームの RSVP 予約が失敗した場合、Unified CM は RSVP ポリシーの設定をチェックし、このコールの処理方法を決定します。オーディオ ストリームのポリシーがオプションの場合、コールは音声のみとして継続します。オーディオ ストリームの RSVP ポリシーが必須の場合は、オーディオ ストリームも RSVP 予約の取得に失敗した場合を除いて、コールは音声のみとして継続します。予約に失敗した場合、コールは失敗するか（ビジー トーンが再生され、「Bandwidth Unavailable」メッセージが表示される）、Automated Alternate Routing（AAR）によってコールの再ルーティングが試行されます（トポロジ対応ロケーションの詳細については、「コール アドミッション制御」（P.9-1）を参照してください）。

（注）　ビデオ優先ポリシーを使用しているときに、ビデオ予約に失敗した場合、コールは音声のみとして完了します。ただし、ユーザはビデオが失敗した原因を示す、視覚的な表示または音声によるフィードバックを受けることができません。

静的ロケーションを設定するときも、Unified CM Administration の 2 つのフィールド、Audio Bandwidth と Video Bandwidth を設定します。ただし、リージョンと異なり、静的ロケーションの Audio Bandwidth は音声のみのコールにのみ適用され、Video Bandwidth はビデオ コールの音声チャネルとビデオ チャネルの両方に適用されます。音声帯域幅とビデオ帯域幅は、別々に維持されます。これは、両方のタイプのコールが帯域幅の単一割り当てを共有すると、音声コールが使用可能な帯域幅のすべてを使用してビデオ コール用の帯域幅が残らなくなる（または、その逆になる）可能性が高いためです。また、音声とビデオの個別の帯域幅プールは、ネットワーク上のスイッチおよびルータでのキューの設定方法に対応します。通常、音声トラフィック用のプライオリティ キューと、ビデオ トラフィック用の独立したプライオリティ キューまたはクラスベース WFQ があります。詳細については、「WAN の QoS」（P.3-40）を参照してください。

Audio Bandwidth フィールドと Video Bandwidth フィールドのどちらにも、None、Unlimited、または数値を指定する 3 つのフィールドがあります。ただし、これらのフィールドに入力する値は、2 つの異なる計算モデルを使用します。Audio Bandwidth フィールドに入力する値には、コールに必要なレイヤ 3 ～ 7 のオーバーヘッドを含める必要があります。たとえば、ロケーションとの間で単一の G.729 コールを許可する場合は、値として 24 kbps を入力します。G.711 コールの場合は、値として 80 kbps を入力します。一方、Video Bandwidth フィールドには、オーバーヘッドを含めない値を入力する必要があります。たとえば、128 kbps コールの場合は 128 kbps を入力し、384 kbps コールの場合は 384 kbps を入力します。リージョンの Video Bandwidth フィールドで使用する値と同様に、ロケーションの Video Bandwidth フィールドにも、56 kbps または 64 kbps の倍数の値を使用することをお勧めします。

たとえば、企業に 3 サイトのネットワークがあるとします。San Francisco ロケーションには、San Jose メイン キャンパスに接続された 1.544 Mbps T1 回路があります。システム管理者は、このロケーションとの間で、4 つの G.729 音声コールと 1 つの 384 kbps（または 2 つの 128 kbps）ビデオ コールを許可します。Dallas ロケーションには、San Jose メイン キャンパスに接続された 2 つの 1.544 Mbps T1 回路があります。管理者は、このロケーションとの間で、8 つの G.711 音声コールと 2 つの 384 kbps ビデオ コールを許可します。この例で、管理者は、San Francisco ロケーションと Dallas ロケーションに次の値を設定します。

ロケーション	必要な音声コールの数	Audio Bandwidth フィールドの値	必要なビデオ コールの数	Video Bandwidth フィールドの値
San Francisco	4、G.729 を使用	96 kbps（4 * 24 kbps）	1、384 kbps	384 kbps
Dallas	8、G.711 を使用	640 kbps（8 * 80 kbps）	2、384 kbps	768 kbps

エンドポイントで要求されるコール速度がロケーションに設定されている値を超えた場合、リージョンの場合とは異なり、Unified CM がロケーション設定で許可された値に適合するように、*自動的にコール速度をネゴシエートすることはありません*。コールは拒否されるか、音声のみのコールとして再試行されます（着信側デバイスで Retry Video as Audio 設定が有効の場合）。そのため、リージョンのビデオ帯域幅は、ロケーションのビデオ帯域幅の値よりも低い値に設定する必要があります。たとえば、2 つのリージョン（リージョン A とリージョン B）があり、これら 2 つのリージョン間のビデオ帯域幅が 768 kbps に設定されている場合、リージョン A のデバイスがビデオ帯域幅が 384 kbps に設定されているロケーションにあると、これら 2 つのリージョン間のすべてのコールが失敗するか、音声のみのコールになります（Retry Video Call as Audio の設定による）。

Retry Video Call as Audio

このチェックボックスは、Cisco Unified IP Phone 7940、7941、7942、7945、7960、7961、7962、7965、7970、7971、7975、および Cisco IP Video Phone 7985、サードパーティ製の SCCP ビデオ エンドポイント、すべての H.323 および SIP デバイス（クライアント、ゲートウェイ、およびすべてのタイプの H.323 トランク）など、ビデオをサポートするすべてのエンドポイント タイプで使用できます。このオプションがアクティブ（オン）のときに、デバイスに到達できるだけの帯域幅がない場合（たとえば、Unified CM リージョンまたはロケーションで、そのコールのビデオが許可されない場合）、Unified CM はそのコールを音声のみのコールとしてリトライします。このオプションが非アクティブ（オフ）のときは、Unified CM はコールを音声のみとして再試行することなく、コールを失敗させるか、Automated Alternate Routing（AAR; 自動代替ルーティング）パスが設定されている場合は可能な限り再ルーティングします。デフォルトでは、このリトライ オプションは有効（オン）です。

この機能は、次のシナリオだけに適用されます。

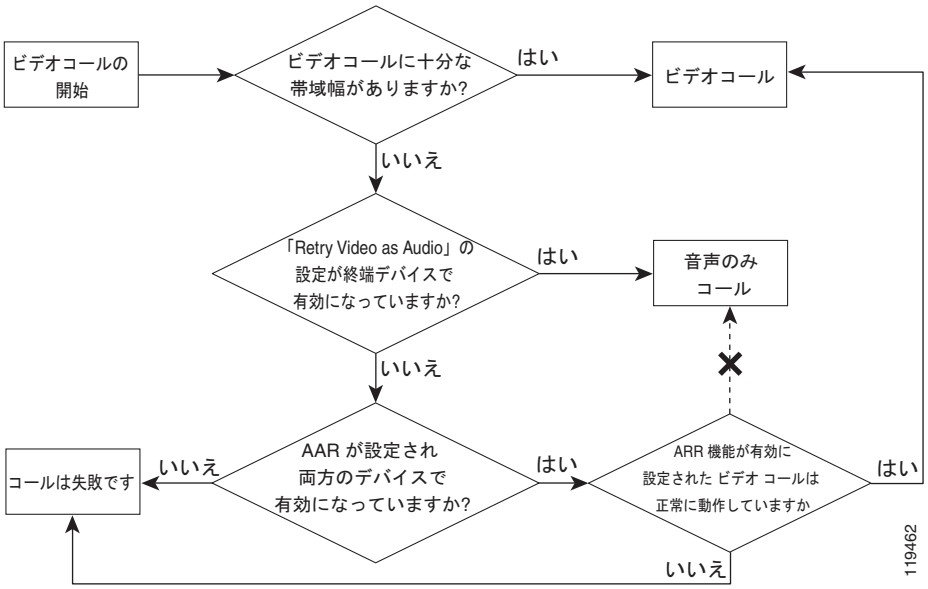
- ビデオを許可しないようにリージョンが設定されている。
- ビデオを許可しないようにロケーションが設定されている。または、ロケーションが RSVP ポリシーを使用しない場合は、要求されたビデオ速度が、そのロケーションで使用可能なビデオ帯域幅を超えている。
- Unified CM クラスタ間のコールの場合、要求されたビデオ速度がゲートキーパーのゾーン帯域幅制限を超えている。

Retry Video Call as Audio オプションは、終端（着信側）デバイスでのみ有効です。そのため、発信側デバイスでは宛先ごとに異なるオプション（再試行または AAR）を使用できる柔軟性があります。

帯域幅の制限が原因でビデオ コールが失敗した場合、自動代替ルーティング（AAR）が有効であれば、Unified CM は失敗したコールをビデオ コールとして AAR の宛先に再ルーティングしようとします。AAR が有効でない場合、失敗したコールによって、発信者にビジー トーンとエラー メッセージが送信されます（図 16-3 を参照）。発信側のデバイスのタイプによって、失敗したコールは次のいずれかになります。

- 発信側デバイスが LCD 画面付き SCCP エンドポイントの場合、発信者にはビジー トーンが聞こえ、メッセージ「Bandwidth Unavailable」がデバイスに表示されます。
- 発信側デバイスが LCD 画面なしの SCCP エンドポイントの場合（Cisco Unified IP Phone 7902 など）、発信者にはビジー トーンが聞こえます。
- 発信側デバイスが H.323 または SIP デバイス、またはゲートウェイで接続された公衆網デバイスの場合、発信者にはビジー トーンが聞こえ、Unified CM が適切なエラー メッセージ（Q.931 Network Congestion 原因コードなど）を H.323、SIP、または MGCP デバイスに送信します。

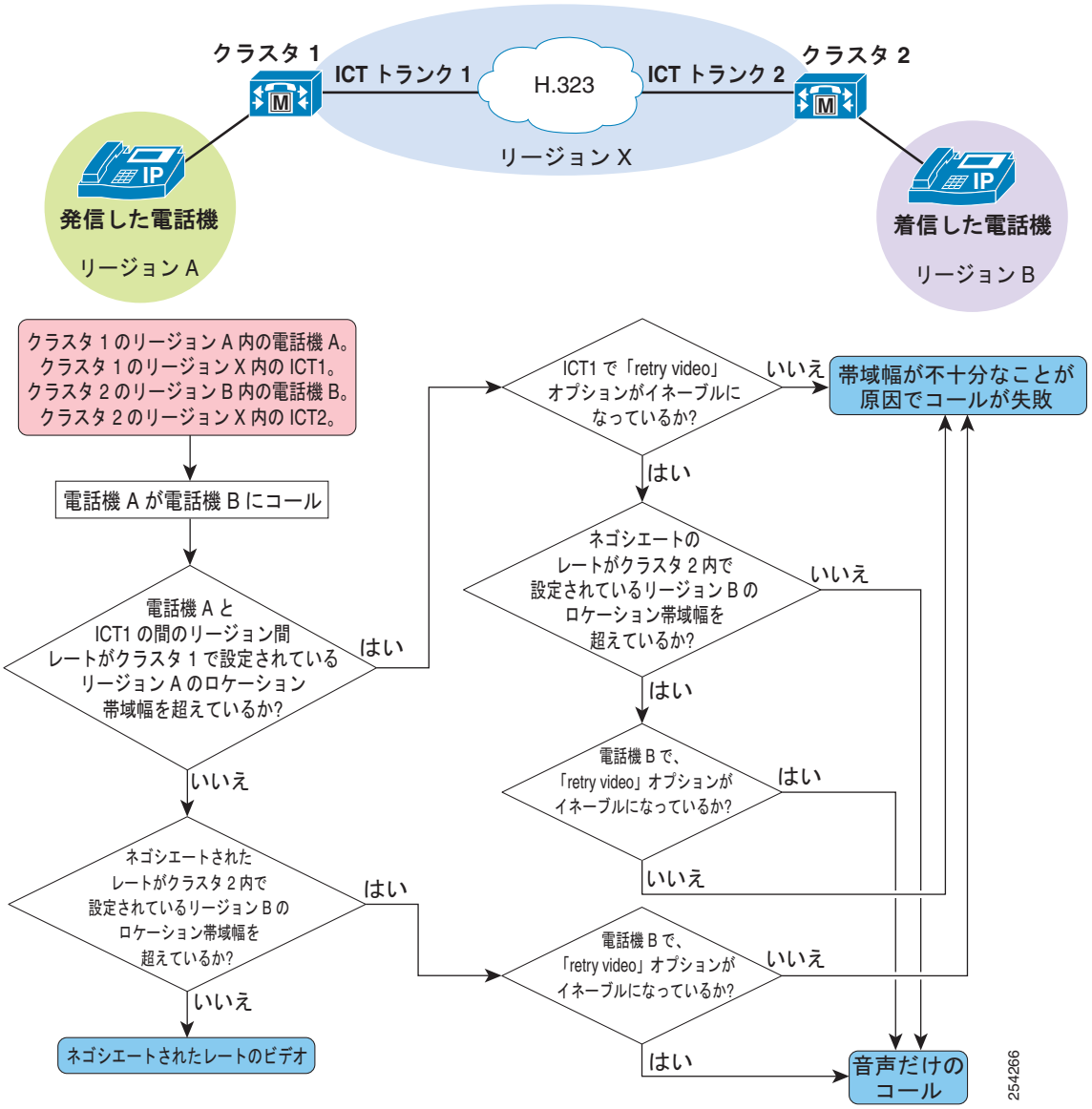
図 16-3　　ビデオ コールで起こり得るシナリオ



AAR の使用方法の詳細については、「コール アドミッション制御」（P.9-1）の章を参照してください。

図 16-4 は、非ゲートキーパー制御クラスタ間トランクを使用する、2 つのクラスタ間のコールの手順を示しています。

図 16-4　非ゲートキーパー制御クラスタ間トランクを使用する 2 つのクラスタ間のコール フロー



Wait for Far-End to Send TCS

このチェックボックスは、H.323 クライアント、H.323 ゲートウェイ、H.225 ゲートキーパー制御トランクなど、すべての H.323 デバイスで使用できます。この機能は、H.323 コールの H.245 機能交換フェーズに関係します。この機能を有効にすると、Unified CM は、Unified CM が Terminal Capabilities Set（TCS; 端末機能セット）を H.323 デバイスに送信する前に、リモート H.323 デバイスが TCS を Unified CM に送信するまで待機します。このオプションが無効の場合、Unified CM は待機せず、すぐに TCS をリモート H.323 デバイスに送信します。

デフォルトでは、Wait for Far-End to Send TCS オプションが有効（オン）です。ただし、次の場合はオフ（無効）にする必要があります。

- Unified CM と通信する H.323 デバイスも、遠端が TCS を送信するまで待機する。

  この場合、どちらの側も TCS を送信しないためデッドロックが発生し、数秒後に H.245 接続がタイムアウトします。遠端が TCS を送信するまで待機するデバイスの例としては、一部の H.323 ルーテッドモード ゲートキーパー、H.320 ゲートウェイ、H.323 プロキシ（IP-to-IP ゲートウェイ）、一部の H.323 マルチポイント カンファレンス ブリッジがあります。これらのデバイスが遠端からの TCS の送信を待機する理由は、Unified CM が待機する理由と同じです。TCS を他方に転送する前に、接続の両端が TCS を送信するまで待機するためです。

- クラスタ間トランクを介して別の Unified CM クラスタと通信している。

（注）　クラスタ間トランクおよびゲートキーパー制御クラスタ間トランクでは、Wait for Far-End to Send TCS オプションは常に無効で、有効にはできません。

多くのシナリオで、Unified CM は、2 つのエンドポイント デバイス（相互に通話しようとする 2 つの H.323 クライアントなど）を接続するソフトウェア スイッチの役割を実行します。このような場合、両方のデバイスが TCS メッセージを送信するまで Unified CM が待機することが最良です。Unified CallManager が各デバイスの機能を認識することで、それぞれに送信する TCS に関して（特に、リージョンおよびロケーションの設定に応じて）最適な判断ができます。この場合、Wait for Far-End to Send TCS 機能は有効にする必要があります。

ただし、その他の H.323 デバイス（H.323 デバイスを H.320 デバイスに接続する H.320 ゲートウェイなど）が、複数の参加者を接続する機能を実行することもあります。また、ゲートウェイも、コールのセットアップ方法に関して最適な選択ができるように、両端が TCS メッセージを送信するまで待機します。Unified CM とゲートウェイの両方が、相手側から TCS が送信されるまで待機すると、デッドロックが発生します。このデッドロック状態を防止するには、Wait for Far-End to Send TCS 機能を無効（オフ）にします。

たとえば、図 16-5 で示す次のコール シナリオについて考えます。

- シナリオ 1：Cisco Unified Video Advantage が H.320 エンドポイントを呼び出す。
- シナリオ 2：H.323 クライアントが H.320 エンドポイントを呼び出す。

これらのシナリオでは、どちらの場合も、Wait for Far-End to Send TCS 機能は、デフォルト設定である有効（オン）のままにします。

図 16-5　Wait for Far-End to Send TCS 機能が有効（オン）のシナリオ

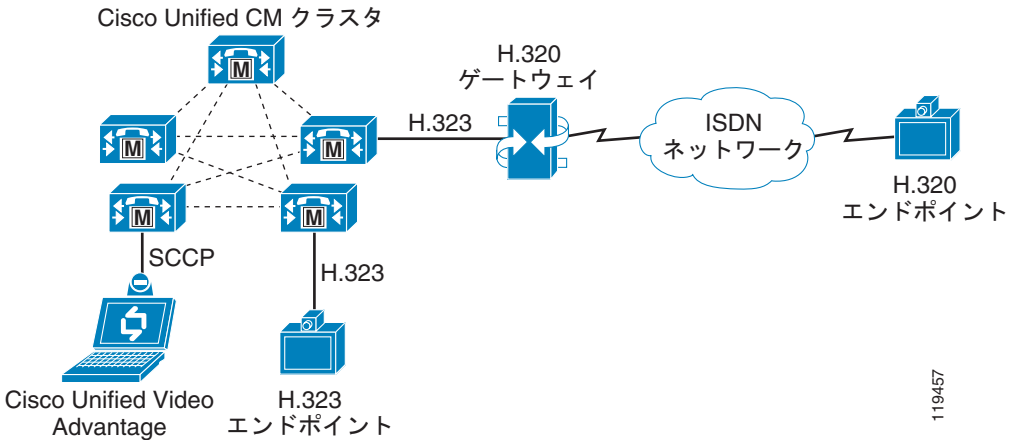


図 16-5 のシナリオ 1 では、登録時に SCCP デバイスがメディア機能を Unified CM に提供しているため、Unified CM はすでに Cisco Unified Video Advantage クライアントの機能を認識しています。しかし、ゲートウェイがコールの H.245 フェーズで TCS を Unified CM に送信するまで、Unified CM は H.320 ゲートウェイの機能を認識しません。同様に、H.320 エンドポイントが TCS をゲートウェイに送信するまで、H.320 ゲートウェイは、Unified CM に送信する TCS を判断できません。この場合、H.320 エンドポイントがゲートウェイに TCS を送信し、ゲートウェイが Unified CM に TCS を送信し、判断に使用できる両端のエンドポイントからの TCS を Unified CM が受信するため、Wait for Far-End to Send TCS 機能は有効のままにしておく方が適切です。

図 16-6 は、次のコール シナリオを示しています。これらのシナリオでは、Wait for Far-End to Send TCS 機能を無効にしないとコールが失敗します。

- シナリオ 1 : Cisco Unified Video Advantage が、ISDN ネットワークを介してリモート クラスタにある別の Cisco Unified Video Advantage を呼び出す。
- シナリオ 2 : H.323 クライアントが、ISDN ネットワークを介してリモート クラスタにある別の H.323 クライアントを呼び出す。

図 16-6　Wait for Far-End to Send TCS 機能が無効（オフ）のシナリオ

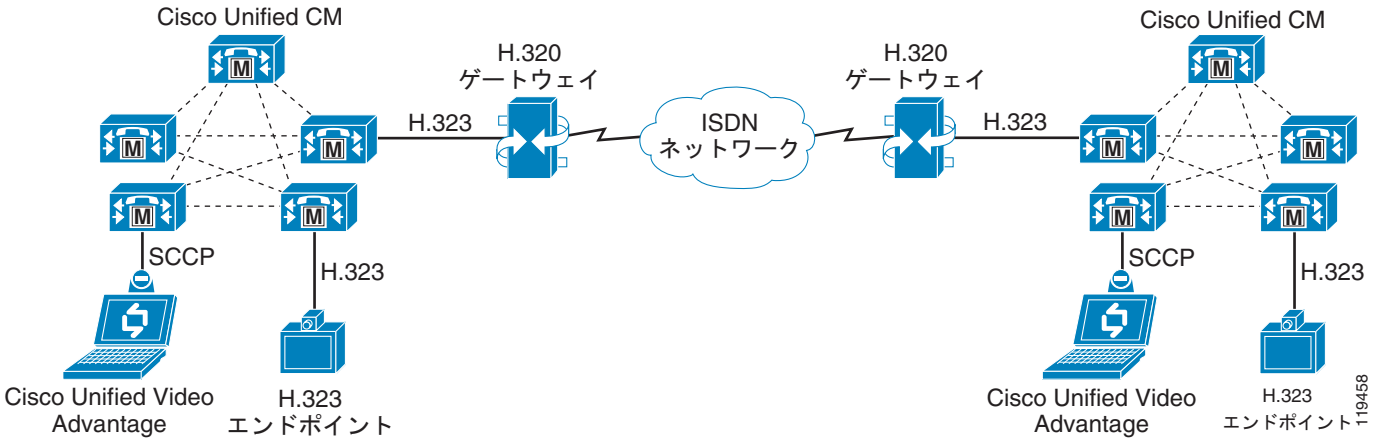


図 16-6 のどちらのシナリオでも、両方の Unified CM がゲートウェイから TCS を受信するまで待機し、両方のゲートウェイも ISDN 側からの TCS を受信するまで待機するため、デッドロックが発生します。コールは数秒後にタイムアウトし、失敗します。ユーザから見ると、発信者にはコールが進行中であることを示すリングバック トーンが聞こえ、着信側には着信コールを示す呼び出し音が聞こえます。着信側がコールに応答しようとすると、デッドロックのために H.245 フェーズが失敗し、コールは両方で切断されて失敗します。

このようなシナリオの問題の回避策としては、Unified CM で H.320 ゲートウェイを表すデバイスで、Wait for Far-End to Send TCS オプションを無効（オフ）にすることをお勧めします。H.320 ゲートウェイに到達するように Unified CM を設定した方法に応じて、このデバイスは H.225 ゲートキーパー制御トランクまたは H.323 ゲートウェイ デバイスになります。

ただし、Wait for Far-End to Send TCS オプションを無効にすると、交換された初期機能がリモート デバイスで機能しなくなることがあります。たとえば、Unified CM リージョンが 768 kbps ビデオに設定されていても、H.320 デバイスが 384 kbps しかサポートしないことがあります。また、選択された音声コーデックがリモート側で機能しないことがあります。この場合、初期ネゴシエートされた論理チャネルを切断し、正しい速度とコーデックで再開する必要があります。多くのレガシー H.323 および H.320 デバイスは、この状態を正しく処理せず、Unified CM が CloseLogicalChannel メッセージを送信して異なる値でチャネルと再ネゴシエートすると、コールを切断します。そのため、Wait for Far-End to Send TCS オプションを無効にする場所とタイミングには注意が必要です。

マルチポイント会議

3 者以上が同じビデオ コールに同時に参加するには、マルチポイント コントロール ユニット（MCU）が必要です。MCU は、次のメイン コンポーネントで構成されています。

- Multipoint Controller（MC）
- Multipoint Processor（MP）

MC は、メディア ネゴシエーション、コール シグナリング、コールに使用する MP の選択など、会議のコール セットアップと切断のすべての面を処理します。MP は、すべての音声パケットおよびビデオ パケットを処理します。MC が MP を制御し、1 つの MC で複数の MP を制御できます。MP は、ソフトウェアベースのものも、ハードウェアベースのものもあります。ソフトウェアベースの MP は、通常、高度なトランスコーディング、レート変換（複数の速度）、構成機能は実行できません。

1999 年以降、シスコは Cisco Unified Videoconferencing 3500 シリーズ H.323 Multipoint Conference Unit（MCU）を提供してきました。このファミリの最初の製品は、Cisco Unified Videoconferencing 3510 です。このモデルは販売終了となり、Unified CallManager との互換性もありません。2002 年、シスコは、Cisco Unified Videoconferencing 3511 および 3540 を導入しました。これらのモデルは大幅に機能が改善され、古い 3510 モデルにはなかったスケーラビリティが実現されていますが、推奨されるプラットフォームは、第 3 世代の MCU モデル（Cisco Unified Videoconferencing 3515 および 3545）です。3515 および 3545 は、ポートごとにエンコーダが実装されたハードウェア アーキテクチャが採用され、ビデオ会議エンドポイントと会議参加者が使用できるビット レート、ビデオ形式、および会議機能の制限を撤廃することにより、事前設定の要件が大幅に緩和されています。

2003 年、シスコは Cisco Unified Videoconferencing 35*xx* モデルにソフトウェア バージョン 3.2+ を導入し、Skinny Client Control Protocol（SCCP）のサポートを追加しました。SCCP サポートは、Cisco Unified Videoconferencing 3510 では使用できません。また、Cisco Unified Videoconferencing MCU では、次の 3 つのタイプの MP が使用できます。

- 3510、3515、および 3540 の各 MCU に内蔵されたソフトウェアベースの MP
- Rate Matching（RM）モジュール（Cisco Unified Videoconferencing 3540 シャーシ専用のソフトウェアベースのモジュール）
- Enhanced Media Processor（EMP）（Cisco Unified Videoconferencing 3540 および 3545 シャーシ専用のモジュールまたは Cisco Unified Videoconferencing 3511 および 3515 モデルの内蔵コンポーネントとして使用できるハードウェアベースのソリューション）

（注） 3545 MCU は、ソフトウェアベースの MP がないので、EMP が必要です。

Cisco Unified CM Release 4.0（およびそれ以降）は、SCCP、H.323、および SIP の各モードで Cisco Unified Videoconferencing 3511、3515、3540、および 3545 の各モデルをサポートします。各プロトコルにはさまざまな機能が用意され、さまざまな理由で使用されます。そのため、3 つのプロトコルすべてを実行するように、これらの各 MCU が搭載されています。Cisco Unified Videoconferencing 3511 は、SCCP モードまたは H.323 および SIP モードで実行するように設定できます。Cisco Unified Videoconferencing 3515、3540、3545 モデルは、3 つのプロトコルすべてを同時に実行し、使用可能な MP リソースの合計数を 3 つの間で分け合うように設定できます。

シグナリング プロトコルに関係なく、MCU は、音声ストリームとビデオ ストリームを各参加者から受信し、これらのストリームをすべての他の参加者に、組み合せたビューで送信するという同じ基本機能を提供します。マルチポイント テレビ会議のビューには、次の 2 つのタイプがあります。

- Voice-Activated（音声起動）（切り替え）
- Continuous-Presence（連続表示）

Voice-Activated（音声起動）

Voice-Activated 会議は、すべての参加者の音声ストリームとビデオ ストリームを取得し、主要な発言者を決定し、主要な発言者のビデオ ストリームだけをすべての他の参加者に送信します。参加者には、主要な発言者の全画面イメージが表示されます（現在の発言者には、前の主要な発言者が表示されます）。すべての参加者からの音声ストリームが混合され、全員が他の全員の発言を聞くことができますが、ビデオは主要な発言者のものだけが表示されます。

次のいずれかの方法で、主要な発言者を選択できます。

- Voice-Activated モード

  このモードを使用すると、MCU は、最も声が大きく、発言が長い会議参加者を判断して、主要な発言者を自動的に選択します。声の大きさを判断するために、MCU は各参加者の音声信号の強さを計算します。会話中に条件が変わると、MCU は自動的に新しい主要な発言者を選択し、その参加者が表示されるようにビデオを切り替えます。ホールド タイマーによって、ビデオの頻繁な切り替えが防止されます。主要な発言者になるには、指定された秒数以上発言し、他のすべての参加者よりも際立つ必要があります。

- MCU の Web ベースの会議制御ユーザ インターフェイスによる主要な発言者の手動選択

  会議コントローラ（議長）は MCU の Web ページにログインし、参加者を強調表示することで、その参加者を主要な発言者として選択できます。この処理によって音声アクティビティ検出は無効になり、議長が新しい主要な発言者を選択するか、Voice-Activated モードを再度有効にするまで、主要な発言者は固定されます。

- 参加者リストを自動的に 1 人ずつ循環するように MCU を設定

  この方式を使用すると、MCU は設定された時間だけ各参加者で止まり、リスト上の次の参加者に切り替えます。会議コントローラ（議長）は、Web インターフェイスでこの機能をオンまたはオフにできます（オフにすると、Voice-Activated モードが再度有効になります）。

Continuous-Presence（連続表示）

Continuous-Presence 会議では、一部の参加者またはすべての参加者が合成ビューで同時に表示されます。ビューには 2 ～ 16 の長方形（参加者）をさまざまなレイアウトで表示できます。各レイアウトには、長方形の 1 つを Voice-Activated にする機能があり、合成ビューに表示できる長方形の数よりも参加者の方が多い会議で役立ちます。たとえば、4 画面のビューを使用していて、コールの参加者が 5 人のとき、同時に表示される参加者は 4 人だけです。この場合、長方形の 1 つを Voice-Activated にすると、主要な発言者に応じて参加者 4 と参加者 5 をその長方形で切り替えることができます。他の 3 つの長方形に表示される参加者は固定で、すべての長方形は、会議制御 Web ベース ユーザ インターフェイスで操作できます。

（注）　Continuous-Presence には、Cisco Unified Videoconferencing MCU の Enhanced Media Processor（EMP）が必要です。

MP リソース

どちらのタイプの会議でも、MP リソースによって、MCU がサポートできるビデオ形式、トランスレーティング、およびトランスコーディング機能が決まります。エンドポイントが異なる速度で会議に接続している場合は、レート変換対応 MP が必要です。RM モジュールと EMP モジュールは、どちらも速度間のレート変換に対応しています。レート変換対応 MP が使用できない場合、MCU はすべてのエンドポイントにフローコントロール メッセージを送出し、最も遅いエンドポイントの最大受信レートに合せて転送速度を下げるように指示します。たとえば、3 人の参加者が 384 kbps の会議に接続し、4 番目の参加者が 128 kbps で参加した場合、MCU は他の 3 人の参加者にフローコントロール メッセージを送信し、128 kbps の参加者に合せて転送速度を下げるように指示します。この方式を使用す

ると、1 人の参加者の性能が低いことで、すべての参加者の品質が低下します。レート変換対応 MP を使用した場合、128 kbps のストリームが 384 kbps に（および、その逆に）変換され、各参加者がそれぞれの接続で許可される最大の品質を使用できます。

Continuous-Presence 会議でも、レート変換対応 MP は非常に重要です。MCU に内蔵されたソフトウェアベースの MP は、すべての入力ストリームを組み合せ、得られた組み合せを各参加者に送信します。たとえば、4 人の参加者が 384 kbps で G.711 音声を使用して Continuous-Presence 会議に接続している場合、各参加者は 320 kbps のビデオと 64 kbps の音声を MCU に転送します。MCU は 4 つの入力ビデオ ストリームを取得し、4 画面の合成ビューに組み合せます。MCU は混在する 64 kbps の音声と共に、1280 kbps のビデオを各エンドポイントに転送します。その結果、エンドポイントごとに合計 1344 kbps になります。この方式は Asynchronous Continuous Presence と呼ばれ、帯域幅要件、コール アドミッション制御メカニズム、一部のデバイスとの相互運用性に悪影響を与えることがあります。

（注）　Asynchronous Continuous Presence は使用しないことを強くお勧めします。

RM モジュールまたは EMP モジュールを使用すると、MCU は各入力ストリームを組み合せる前に、合計出力帯域幅が入力帯域幅と一致するようにレート変換できます。たとえば、MCU が 4 画面のレイアウトを使用し、各参加者が 320 kbps のビデオと 64 kbps の音声を MCU に転送する場合、MCU は原則として各入力ストリームを 80 kbps にレート変換し、4 画面のビューが 320 kbps のビデオになるように組み合せ（4 × 80 kbps）、混合された 64 kbps 音声とこのビデオを組み合せて、最終的な組み合せを各参加者に転送します。この方式は、Synchronous Continuous Presence と呼ばれます。すべての Continuous-Presence 会議で、Synchronous Continuous Presence モードを使用することを強くお勧めします。ただし、このモードを使用するには、各 MCU にレート変換対応 MP（RM、EMP など）が必要で、MCU のコストが上がります。

（注）　MCU が内蔵された H.323 および SIP クライアントの場合、Unified CM は、H.323 クライアントで第 2 のコールの生成を許可しません。そのため、内蔵 MCU の機能は無効になります。

SCCP MCU リソース

すでに説明したように、Cisco Unified Videoconferencing 3511、3515、3540、および 3545 MCU はいずれも、これらのモデルのソフトウェア バージョン 3.2+ および Cisco Unified CM Release 4.0 から SCCP をサポートしています。SCCP モードで設定すると、Unified CM が MC 機能を提供し、MCU が MP 機能を提供します。SCCP MCU は、Unified CM で完全に制御されます。

SCCP MCU リソースを呼び出すのは、次のイベントだけです。

- SCCP エンドポイント（IP Phone やサードパーティ製 SCCP ビデオ エンドポイントなど）のユーザが、Conf、Join、または cBarge ソフトキーを押して Ad-Hoc 会議を呼び出した。
- SCCP エンドポイント（IP Phone やサードパーティ製 SCCP ビデオ エンドポイントなど）のユーザが、MeetMe ソフトキーを押して、予約なしの Meet-Me 会議を呼び出した。

これらのタイプの会議の参加者には、任意のタイプのエンドポイント（サポートされる任意のゲートウェイ タイプを介して Unified CM がサポートする任意のシグナリング プロトコルを使用するビデオ デバイスおよび非ビデオ デバイス）が含まれます。ただし、SCCP MCU リソースを呼び出せるのは、SCCP エンドポイントだけです。つまり、H.323 ビデオ エンドポイントは SCCP MCU リソースを呼び出せませんが、SCCP ビデオ エンドポイントがリソースを呼び出し、H.323 ビデオ参加者をコールに参加させることはできます。たとえば、SCCP エンドポイントのユーザは、Conf ソフトキーを押し、H.323 クライアントのディレクトリ番号をダイヤルして、もう一度 Conf ソフトキーを押すと、トランザクションを完了できます。H.323 クライアントは、参加者として SCCP MCU 会議に参加します。

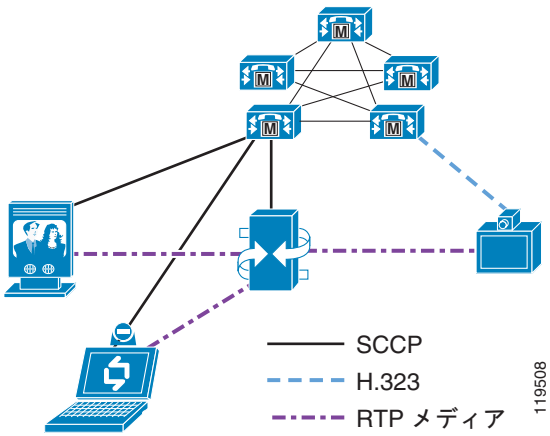
ただし、Conf、Join、または cBarge ソフトキーで開始された Ad-Hoc 会議の場合、他の参加者が使用するシグナリング プロトコルは、保留機能および MCU に音声チャネルとビデオ チャネルを転送する機能をサポートしている必要があります。H.323 デバイス（H.323 クライアント、H.323 ゲートウェイ、H.320 ゲートウェイ、およびすべてのタイプの H.323 トランク）の場合、Unified CM は、H.245 仕様で定義されている Empty Capabilities Set（ECS）方式を使用してこの機能を実現しています。H.323 エンドポイントが Unified CM からの ECS メッセージの受信をサポートしていない場合、切断されるか、クラッシュしてリブートする可能性もあります。この問題の回避策としては、H.323 デバイスで「MTP Required」オプションを有効（オン）にして、MTP デバイスを含まないメディア リソース グループ リスト（MRGL）をこのデバイスに割り当て、Unified CM のサービス パラメータ **Fail Call if MTP Allocation Fails** を **False** に設定します（詳細については、「メディア リソース グループとメディア リソース グループ リスト」（P.16-16）を参照してください）。この設定を行うと、電話機のソフトキーはグレーアウトされます。ユーザはこのエンドポイントで、保留、既存のコールとの会議、既存のコールへの参加、このエンドポイントを含む既存のコールへの割り込みなど、付加サービスを呼び出せなくなります。

（注）　ここで説明した回避策には MTP デバイスを含まない MRGL が必要になるため、RSVP ベースのコール アドミッション制御を使用している場合、この回避策は使用できません。

MeetMe ソフトキーによる予約なしの会議の場合は、他のエンドポイントで使用されているシグナリング プロトコルが保留および転送をサポートしている必要はありません。これらのタイプの会議では、各エンドポイントが、会議を開始した SCCP クライアントで割り当てられた MeetMe ダイヤルイン番号をダイヤルします。

図 16-7 は、H.323 エンドポイントと SCCP エンドポイントを同じ SCCP 会議に参加させる方法を示しています。この例では、SCCP エンドポイントで Conf ソフトキーによって会議が開始され、3 人のメンバーが招待されています。

図 16-7　SCCP エンドポイントと H.323 エンドポイントの間の Ad-Hoc 会議



SCCP 会議は、Voice-Activated モードと Continuous-Presence をサポートします。さらに、SCCP 会議は、MCU に内蔵されたソフトウェアベースの MP、Rate Matching（RM）モジュール、および Enhanced Media Processor（EMP）モジュールをサポートします。

メディア リソース グループとメディア リソース グループ リスト

Unified CM は、メディア リソース グループ（MRG）とメディア リソース グループ リスト（MRGL）を使用して、指定されたエンドポイントに使用するカンファレンス ブリッジ リソースを決定します。リソースをグループ化する方法は完全に自由ですが、地理的な配置（指定されたサイトのすべてのエン

ドポイントが、最も近い MCU を使用する）またはエンドポイントのタイプ（ビデオ対応エンドポイントがビデオ対応 MCU を使用し、音声のみのエンドポイントは別のカンファレンス ブリッジ リソースを使用する）でグループ化することが一般的です。SCCP デバイスのユーザが Conf、Join、または MeetMe ソフトキーをアクティブにした場合、Unified CM は発信側エンドポイントの MRGL を使用して、使用するカンファレンス ブリッジを決定します。

Unified CM は、次の基準をリストの順に適用して、使用するカンファレンス ブリッジ リソースを選択します。

1. メディア リソース グループ リスト（MRGL）にリストされているメディア リソース グループ（MRG）の優先順位
2. 選択された MRG の中で、最も使用されていないリソース

このように選択されるため、ユーザがビデオ対応 SCCP エンドポイントで Conf、Join、または MeetMe ソフトキーをアクティブにしたときにビデオ対応 MCU が選択されるようにするには、ビデオ対応 SCCP エンドポイントの MRGL の最上位にビデオ対応 MCU を置く必要があります。ただし、エンドポイントによっては、ビデオ専用エンドポイントでないことがあります。たとえば、Cisco Unified Video Advantage と組み合せて使用される IP Phone は、ほとんどの場合は音声のみのコールに使用され、まれにビデオに使用されることもあります。したがって、この電話機の MRGL の最上位に MCU を配置すると、ビデオ対応の参加者がいない音声のみの会議にも、この MCU が常に選択されます。このシナリオでは、音声のみの会議で MCU リソースが浪費され、ビデオ会議の要求が発生したときに使用できなくなることがあります。このようなビデオ リソースの浪費をなくすために、Unified CM 7.*x* には、インテリジェント ブリッジ選択機能があります。

インテリジェント ブリッジ選択機能

Cisco Unified CM 7.*x* には、インテリジェント ブリッジ選択機能があります。この機能を使用すると、会議のエンドポイントの機能に基づいて、ビデオ会議リソースを割り当てることができます。ビデオ会議の起動時に複数のビデオ エンドポイントが存在し、ビデオ会議リソースが使用可能な場合、インテリジェント ブリッジ選択機能は、会議に使用するリソースを選択します。ビデオ会議リソースが 1 つも使用できない場合、またはビデオ会議にビデオ対応エンドポイントが 1 つも存在しない場合、インテリジェント ブリッジ選択機能は、会議で使用可能なオーディオ リソースを選択します。

インテリジェント ブリッジ選択機能は、セキュア会議に対しセキュアなカンファレンス ブリッジを選択する付加機能を提供します。ただし、セキュアなカンファレンス ブリッジ接続は、デバイス機能に依存します。Unified CM は、ビデオまたはオーディオ カンファレンス ブリッジの代わりに、セキュアなカンファレンス ブリッジを割り当てることがあります。インテリジェント ブリッジ選択機能の動作は、サービス パラメータの設定によって、柔軟に変更できます。

インテリジェント ブリッジ選択機能では、次のタイプのエンドポイントがビデオ対応として扱われます。

- Cisco Unified Video Advantage（IP Phone の PC ポートに接続された PC 上で実行する必要があります）
- Cisco Unified IP Phone 7985G
- Cisco Unified Personal Communicator
- H.323 クライアント（サードパーティ製ビデオ エンドポイント）
- SIP Advanced エンドポイント（サードパーティ製ビデオ エンドポイント）
- ビデオ コール用メディア ターミネーション ポイント（MTP）のない SIP トランク
- ビデオ コール用 MTP のない H.323 トランク

インテリジェント ブリッジ選択機能は、カンファレンス ブリッジの他の選択方式と比べて、次のような利点があります。

- 会議タイプによるカンファレンス ブリッジ選択：セキュア、ビデオ、または音声会議

- メディア リソース設定の簡素化
- 他のブリッジ選択方式では音声のみの会議に占有されかねない、MCU ビデオ ポートの適正な使用

（注）　Meet-Me 会議は、インテリジェント ブリッジ選択機能を使用しません。

H.323 および SIP MCU リソース

H.323 または SIP モードで設定すると、MCU は MC 機能を提供し、Unified CM への H.323 または SIP ピアのように動作します。H.323 および SIP MCU 会議は多くの方法で呼び出せますが、それらの方法は主に次の 2 つのカテゴリに分類できます。

- スケジュール済み
- 予約なし

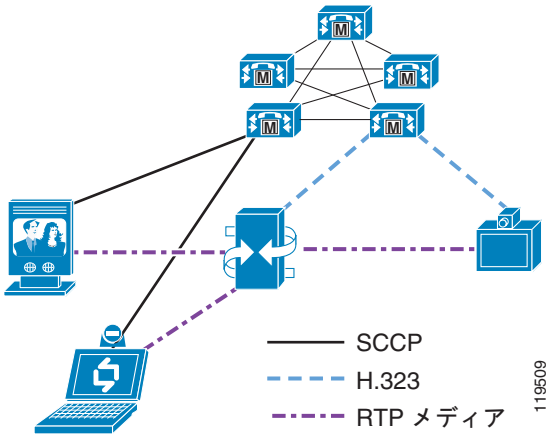
スケジュール済みの会議は、コールの前に、スケジューリング アプリケーションを使用して MCU リソースを予約します。スケジューリング機能は、通常、Cisco Unified MeetingPlace や Cisco Unified Video Conferencing Manager などの Web ベースのユーザ インターフェイスで提供されます。スケジューリング アプリケーションは、通常、会議の日付と時刻、会議用に予約されているポートの数、ダイヤルイン情報をユーザに提供する招待情報を生成します。または、会議の開始時に参加者の一部、またはすべてにダイヤル アウトするようにスケジューリング システムを設定できます。

予約なしの会議の場合、MCU には、オンデマンドで使用できる一定の数のリソースがあります。会議を作成するため、ユーザはいつでも MCU にダイヤルインするだけで済みます。そのユーザが最初にダイヤルした参加者である場合、MCU は、サービス テンプレートで定義された設定を使用して、動的に新しい会議を作成します（サービス テンプレートの詳細については、「サービス テンプレートとプレフィックス」（P.16-19）を参照してください）。同じ会議番号にダイヤルインした後続のユーザは、この会議に参加します。

スケジュール済みまたは予約なしの H.323 または SIP 会議の作成と参加は、任意のタイプのエンドポイントで実行できます。たとえば、SCCP エンドポイントが H.323 MCU にダイヤルインして、H.323 エンドポイントと同様に予約なしの会議を作成できます。

図 16-8 は、H.323 エンドポイントと SCCP エンドポイントを同じ H.323 会議に参加させる方法を示しています。この例では、H.323 MCU にダイヤルインして新しい予約なしの会議を作成した SCCP エンドポイントによって会議が開始され、他の 2 人の参加者が、後で会議にダイヤルインしています。

図 16-8　予約なしの会議の SCCP および H.323 エンドポイント



H.323 および SIP 会議は、Voice-Activated モードと Continuous-Presence モードの両方をサポートします。さらに、H.323 会議は、MCU に内蔵されたソフトウェアベースの MP、Rate Matching（RM）モジュール、および Enhanced Media Processor（EMP）モジュールなど、すべての MP タイプをサポートします。

サービス テンプレートとプレフィックス

MCU のサービスは、各会議に関係する設定を定義します。異なるタイプの会議に、異なるサービスを定義できます。各サービスは、少なくとも、次の設定を定義します。

- 会議の速度（ビデオ ビットレート）

  レート変換対応 MP を使用している場合、この設定に複数の速度が含まれることがあります。

- 参加者の最小数および最大数

  最小数は、会議の開始時に予約されるポートの数を定義します。最大数は、MCU がこの会議への参加を許可する参加者の最大数を定義します。

- ビデオ コーデック タイプ（H.261、H.263、または H.264）
- フレーム レート（15 または 30 fps）
- 解像度（QCIF または CIF）
- MP リソース（Auto、MP、RM、または EMP）
- 表示するビデオ レイアウト（Voice-Activated または Continuous-Presence）

  会議には複数のレイアウトを含めることができ、会議の参加者数が増減したときに変化する動的レイアウトもあります。

- H.323 と SIP、または SCCP

  「SCCP service」チェックボックスが有効（オン）の場合、サービスは SCCP 会議で使用されます。このボックスが無効（オフ）の場合、サービスは H.323 および SIP 会議で使用されます。

H.323 および SIP サービスでは、特定のサービスに到達するために、エンドポイントがダイヤルするサービス プレフィックスに各サービスが割り当てられます。サービス プレフィックスは会議番号の前半の番号を形成し、後半の番号で会議 ID を定義します。この形式によって、同じサービス プレフィックスで複数の会議を同時に実行できます。たとえば、サービス プレフィックスを 555 にして、会議の完全なダイヤル文字列を 7 桁にできます。この方式では、4 桁の会議 ID を使用でき、会議番号は 5550000 ～ 5559999 の範囲になります。ユーザは、会議にアクセスするために全文字列をダイヤルする必要があります。コールを受信すると、MCU はダイヤルされた番号を解析し、サービス プレフィックスとの照合を試行します。ダイヤルされたサービス プレフィックスを判断すると、MCU は残りの番号を会議 ID として使用します。会議 ID がまだ存在しない場合、MCU は、その ID で新しい予約なしの会議を作成します。会議がすでに存在する場合は、その会議にユーザが追加されます。

MCU で H.323 と SIP の両方を同時に有効にする場合は、両方のプロトコルでダイヤル プランを同じにする必要があります。H.323 と SIP の間には、SCCP との間にあるような区別がありません。会議が SIP で作成された場合、MCU はこの会議を H.323 を介して登録します。ゲートキーパーまたは SIP プロキシが登録を拒否した場合、会議は失敗します。

SCCP サービスでもサービス プレフィックスを定義する必要がありますが、ユーザは SCCP サービスに「ダイヤル」インしないため、番号自体に意味はありません。プレフィックスは、Unified CM と SCCP MCU リソースとの間の SCCP 登録メッセージでのみ使用されます。ユーザは、Conf、Join、または cBarge ソフトキーを使用して SCCP MCU 会議にアクセスするか（Ad-Hoc）、Unified CM で割り当てられた MeetMe 番号をダイヤルして会議に参加します（予約なし）。そのため、SCCP サービス プレフィックスに指定した番号は関係ありません。999999 など、任意の番号を自由に指定できます。このプレフィックスは、MCU と Unified CM との間の SCCP シグナリングの外側には公開されません（つまり、ダイヤルすることも、ゲートキーパへの MCU の登録に含むこともできません）。

MCU のサイジング

MCU がサポートできる会議のタイプと数の決定には、複数の要因が関与します。サイジングに関連するこれらの要因は、次の項で説明するように、MCU のモデルによって異なります。

Cisco Unified Videoconferencing 3515 および 3545

現在の MCU モデルは、Cisco Unified Videoconferencing 3515 と 3545 です。Cisco Unified Videoconferencing 3515 MCU は固定数のポートをサポートし、Cisco Unified Videoconferencing 3545 MCU は最大 3 個の 24 ポート EMP モジュールを受け付けるモジュラ システムです。以前のバージョンのハードウェアと異なり、3515 と 3545 は全ポートが完全に処理されるので、ポートの容量や同時にサポートされる会議の数を減少させることなく、サポートされているあらゆる接続速度、ビデオおよびオーディオ コーデック、ビデオ解像度を利用できます。いずれの MCU も、動作には EMP が必要です。3515 は EMP がオンボードに装着されていますが、3545 は少なくとも 1 つの別モジュールが必要です。

したがって、これらの MCU のサイズ計算は、単純に次の要素で決まります。

- MCU がサポートできる合計ポート数
- MCU が各プロトコル専用に割り当てられるポート数

（注）　1 つの SCCP 会議が複数の EMP にまたがることはできません。各 SCCP 会議は、最大 24 人の参加者をサポートします。

Cisco Unified Videoconferencing 3511 および 3540

Cisco Unified Videoconferencing 3511 と 3540 は従来の MCU モデルです。Cisco Unified Videoconferencing 3511 MCU は固定数のポートをサポートし、Cisco Unified Videoconferencing 3540 MCU はさまざまなモジュール サイズを受け付けるモジュラ システムです。使用可能なポートの合計数を計算するときは、Audio Transcoder Daughter Card と Rate Matching（RM）モジュールまたは Enhanced Media Processor（EMP）モジュールをサポートできるように考慮する必要もあります。そのため、MCU のサイズを計算するときは、次の要素を考慮します。

- MCU がサポートできるポート数

  この値は、会議の速度によって異なります。速度が高いほど、サポートされるポートの数は減少します。

- Audio Transcoding Daughter Card がサポートできるポート数

  この値は、会議で使用する音声コーデックによって異なります。

- RM または EMP モジュールがサポートできる会議数

  この値は、トランスレーティングが必要な参加者の数および会議で使用するビューの数によって異なります。

サポートされるポート数に関する特定の情報については、Cisco.com で入手可能な MCU ハードウェアの製品マニュアルを参照してください。可能なバリエーションの数は無限に近いため、具体的な設計ガイダンスをこのマニュアルで示すことは非常に困難です。多くのお客様では、最終的に、SCCP Ad-Hoc 会議、H.323 および SIP の予約なしの会議、および H.323 および SIP のスケジュール済み会議が混在することになります。MCU は、正しい速度とビデオ レイアウトでこれらのすべてのタイプの会議に対応できるサイズにする必要があります。言うまでもなく、この判断はとても複雑です。特定の環境での MCU のサイジングにあたっては、代理店にご相談ください。

ダイヤルイン会議の IVR

ダイヤルイン会議は、通常、Interactive Voice Response（IVR; 音声自動応答装置）システムを使用して、参加する会議の会議 ID とパスワード（設定されている場合）の入力をユーザに求めます。次のタイプの IVR と Cisco Unified Videoconferencing 3500 シリーズ MCU を使用できます。

- MCU に内蔵された IVR
- Cisco Unified IP IVR

MCU の内蔵 IVR には、次の特性があります。

- 会議のパスワードのプロンプトだけを再生できる。

  最初に会議 ID のプロンプトの再生はできません。つまり、ユーザは参加する会議の会議番号をダイヤルする必要があり、次にその会議のパスワードの入力を求められます。
- インバンドとアウトオブバンド（H.245 英数字）の両方の DTMF をサポートする。
- より柔軟性の高いメニューまたは機能を提供するようにカスタマイズできない。

  カスタマイズできるのは、ユーザに対して再生される録音済み音声ファイルだけです。

ダイヤルイン番号を 1 つにして、会議 ID を入力するようにユーザに求めるには、Cisco Unified IP IVR と MCU を組み合せて使用します。

Cisco Unified IP IVR には、次の特性があります。

- （特に）会議 ID とパスワードのプロンプトを再生できる。
- アウトオブバンド DTMF だけをサポートする。

  つまり、発信側デバイスはアウトオブバンド DTMF 方式（H.323 デバイスの H.245 英数字など）をサポートしている必要があります。これらのアウトオブバンド DTMF メッセージは、次に、Unified CM によって Cisco IP IVR サーバにリレーされます。発信側デバイスがインバンド DTMF トーンだけをサポートしている場合、Cisco IP IVR サーバが発信側デバイスを認識しないため、そのデバイスは会議に参加できません。
- 高いカスタマイズ性があり、より柔軟性の高いメニューおよび他の高度な機能を提供できる。

  カスタマイズには、ユーザの会議への参加を許可する前にユーザのアカウントをバックエンド データベースで検証すること、議長が参加するまで参加者をキューに入れることなどが含まれます。

（注）　Cisco Unified IP IVR はアウトオブバンド シグナリングのみをサポートするため、インバンド DTMF トーンを使用する H.323 エンドポイントでは機能しません。

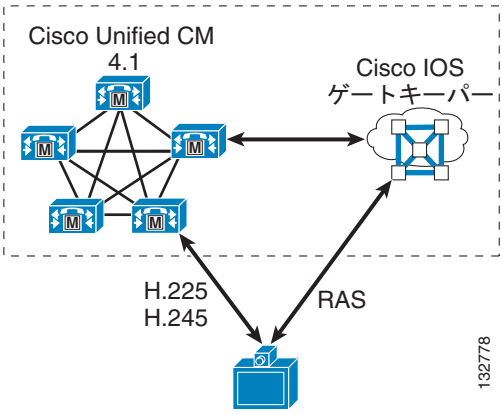
Cisco Unified IP IVR を使用する場合、ユーザは、MCU に直接ルーティングするルート パターンをダイヤルする代わりに、コールを Cisco Unified IP IVR サーバにルーティングする CTI ルート ポイントをダイヤルします。会議 ID の DTMF ディジットを収集した後、Cisco Unified IP IVR は、MCU にコールをルーティングするルート パターンにコールをルーティングします。この転送操作では、発信側デバイスがメディア チャネルの終了と新しい宛先への再開をサポートしている必要があります。たとえば、Cisco Unified IP IVR を呼び出す H.323 ビデオ デバイスは、最初に Cisco Unified IP IVR サーバへの音声チャネルをネゴシエートします。次に、適切な DTMF ディジットが入力された後、MCU に転送します。この時点で Unified CM が、エンドポイントと Cisco Unified IP IVR サーバとの間の音声チャネルを終了し、エンドポイントと MCU の間で新しい論理チャネルを開く Empty Capabilities Set（ECS）プロシージャを呼び出します。このプロシージャについては、この章ですでに説明しています。H.323 ビデオ エンドポイントが Unified CM からの ECS の受信をサポートしていない場合、コールが切断されるか、最悪の場合、クラッシュしてリブートします。

ゲートキーパー

Unified CM にビデオ サポートが導入されるまで、H.323 ビデオ会議ネットワークは、デバイス登録管理、コール ルーティング、および帯域幅制御を実行するゲートキーパーに依存していました。以前は Multimedia Conference Manager（MCM）と呼ばれていた Cisco IOS Gatekeeper が、これらの機能を提供します。ただし、シスコ製品を含むほとんどのゲートキーパーは、一般的なエンタープライズクラスの PBX で期待される機能と比較して、基本的なコール ルーティング機能だけを提供します。H.323 ビデオ コールのルーティングに使用する場合、Unified CM が基本的なゲートキーパー機能を補足し、完全なエンタープライズクラスの PBX 機能を H.323 ビデオ コールに提供します。

Unified CM とゲートキーパーはチームとして機能し、H.323 ビデオ エンドポイントを管理します。ゲートキーパーがすべての Registration, Admission, and Status（RAS）シグナリングを処理し、Unified CM がすべての H.225 コール シグナリングと H.245 メディア ネゴシエーションを処理します。そのため、図 16-9 で示すように、ネットワークの H.323 エンドポイントに RAS シグナリング プロシージャが必要な場合は、ゲートキーパーと Unified CM サーバを同時に配置する必要があります。

図 16-9　H.323 エンドポイントに RAS シグナリングを提供する Unified CM と Cisco IOS Gatekeeper



次のいずれかの条件が該当する場合、RAS シグナリングが常に必要になります。

- エンドポイントが固定 IP アドレスを使用しない。

  エンドポイントが静的 IP アドレスを使用する場合、Unified CM は、エンドポイントを探すために RAS プロシージャを必要としません。エンドポイントは静的 IP アドレスを使用して Unified CM Administration でプロビジョニングされ、この H.323 クライアントのディレクトリ番号へのコールは、直接静的 IP アドレスにルーティングされます。エンドポイントが静的 IP アドレスを使用しない場合、Unified CM はこのエンドポイントにコールをルーティングするたびに、ゲートキーパーに照会してエンドポイントの現在の IP アドレスを取得する必要があります。

- E.164 アドレスへのコール発信のために、エンドポイントで RAS プロシージャを必要とする。

  ほとんどの H.323 ビデオ会議エンドポイントは、IP アドレスでダイヤルする場合に限り、別のエンドポイントに直接ダイヤルできます（ユーザが宛先エンドポイントの IP アドレスをドット付き 10 進表記で入力し、コール ボタンを押す）。ただし、ユーザが E.164 形式の番号（IP アドレスのドット付き 10 進表記ではない数値）または H.323-ID（*ユーザ名*または*ユーザ名*@ *ドメイン*の形式）をダイヤルする場合、ほとんどのエンドポイントは、現在、これらの宛先タイプを解決する方法としてゲートキーパーへの RAS 照会だけを提供します。ただし、E.164 アドレスへのコールが RAS プロシージャをスキップし、H.225 SETUP メッセージを指定された IP アドレスに直接送信するように設定できるエンドポイントの数が増えています。この操作方式は、ピアツーピア モードと呼ばれます。このモードを使用する例としては Tandberg 社製 H.323 エンドポイントがあり、

登録するゲートキーパー アドレスを設定することも、使用する Unified CM サーバの IP アドレスを設定することもできます。後者の場合、エンドポイントはすべてのコールを指定された IP アドレスに直接送信し、ゲートキーパーの RAS プロシージャを必要としません。

H.323 ビデオ エンドポイントの RAS プロシージャの管理に加え、ゲートキーパーは、大規模なマルチサイト分散コール処理環境でのダイヤル プラン解決および Unified CM クラスタ間の帯域幅制限の管理において、重要な役割を果たしています。ゲートキーパーは、組織内の多数の H.323 VoIP ゲートウェイを統合できます。また、エンタープライズ IP Telephony ネットワークとサービス プロバイダー VoIP 転送ネットワークの間でセッション ボーダー コントローラとして機能します。

そのため、Cisco IP Video Telephony 配置に関しては、Cisco IOS Gatekeeper は次の役割の一方または両方を実行できます。

- エンドポイント ゲートキーパー

  エンドポイント ゲートキーパーは、H.323 クライアント、MCU、および H.320 ビデオ ゲートウェイを宛先または発信元とするコール、およびこれら相互間のコールのすべての RAS プロシージャを管理するように設定されます。エンドポイント ゲートキーパーは、Unified CM がすべての H.225 コール ルーティングおよび H.245 メディア ネゴシエーションを実行できるように、これらのすべてのコールを適切な Unified CM クラスタに転送します。

- インフラストラクチャ ゲートキーパー

  インフラストラクチャ ゲートキーパーは、Unified CM クラスタ間、Unified CM クラスタと H.323 VoIP ゲートウェイのネットワーク間、および Unified CM クラスタとサービス プロバイダーの H.323 VoIP 転送ネットワーク間のすべてのダイヤル プラン解決および帯域幅制限（コール アドミッション制御）を管理するように設定されます。

以前の Cisco Unified CM リリースでは、エンドポイント ゲートキーパーとインフラストラクチャ ゲートウェイは別々のルータで実行する必要があり、各エンドポイント ゲートキーパーは単一の Unified CM クラスタだけにサービスを提供できました。企業内に複数の Unified CM クラスタがある場合は、Cisco Unified CM クラスタごとに、個別のエンドポイント ゲートキーパーを配置する必要がありました。現在のリリースの Cisco Unified CM では、これらの役割を単一のゲートキーパーに組み合せて、1 つ以上の Cisco Unified CM クラスタのエンドポイント ゲートキーパーとして使用しながら、クラスタ間またはクラスタと他の H.323 VoIP ネットワーク間のコールを管理するインフラストラクチャ ゲートキーパーとして使用できます。ただし、（特に）次の理由により、これらの役割は複数のゲートキーパーに分割することをお勧めします。

- スケーラビリティ

  配置する Cisco IOS ルータ プラットフォーム、および煩雑時のコール量の概算によっては、負荷を処理するゲートキーパーが複数必要になることがあります。

- 地理的な復元性

  1 台のゲートキーパーでネットワーク全体をカバーすることは、大規模な国際 VoIP ネットワークにおいて、賢明な方法ではありません。複数のゲートキーパーをネットワーク全体に（一般的には地理的に）分散して配置すると、1 つのゲートキーパーが故障した場合に、より適切に障害を切り分けることができます。

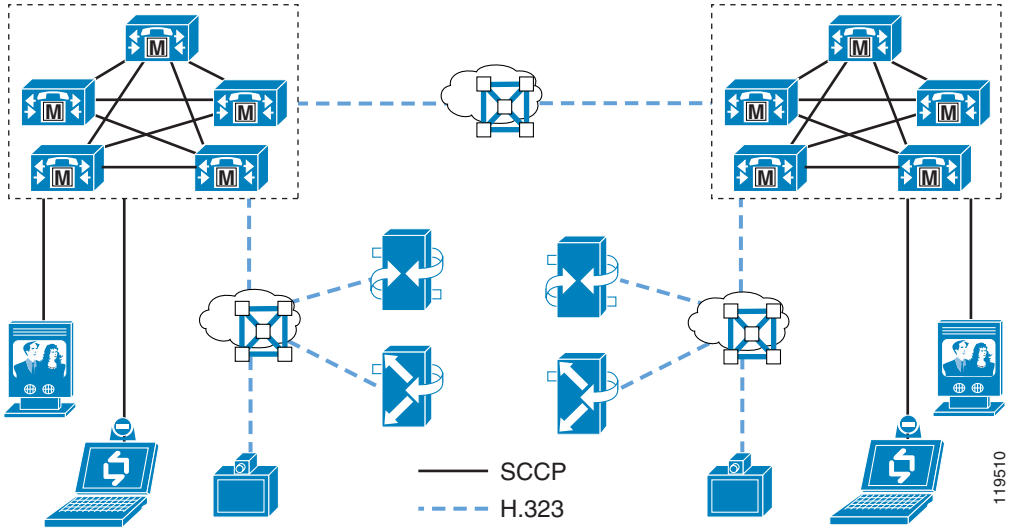
- 非互換性

  ゲートキーパーの設定の中には、グローバルな性質（そのゲートキーパーに登録されているすべてのエンドポイントに関連する性質）を持つものがあります。たとえば、コマンド **arq reject-unknown-prefix** は、一部の H.323 VoIP 転送環境では便利ですが、Unified CM へのコールをルーティングするエンドポイント ゲートキーパーで使用される **gw-type-prefix** < *プレフィックス*> **default-technology** コマンドと衝突します。Cisco IOS では両方のコマンドを同じゲートキーパーで設定することは禁止されていませんが、**arq reject-unknown-prefix** コマンドが優先されるため、不明な番号へのコールは Unified CM にルーティングされず、拒否されます。この場合は、H.323 VoIP 転送ネットワーク用に 1 つのゲートキーパーを使用し、別のゲートキーパーを Unified CM クラスタに使用します。

非互換性のもう 1 つの例は、冗長性のためにゲートキーパーを設定する際に発生することがあります。Cisco Voice Gateways や Unified CM など、ほとんどの Cisco H.323 音声デバイスは、Gatekeeper Update Protocol（GUP）を使用して相互に同期するゲートキーパー クラスタとしてゲートキーパーを設定可能な H.323v3 Alternate Gatekeeper 機能をサポートします。ただし、多くの H.323 ビデオ エンドポイントは Alternate Gatekeeper をサポートしないため、冗長性のために Hot Standby Routing Protocol（HSRP; ホットスタンバイ ルータ プロトコル）を使用するようにゲートキーパーを設定する必要があります。これらの 2 つの冗長性方式を同じゲートキーパーに混在させ、組み合せることはできません。この場合、Alternate Gatekeeper をサポートするエンドポイント用にゲートキーパー クラスタを使用するか、サポートしないエンドポイント用にゲートキーパーの HSRP ペアを使用するかを決定します。

図 16-10 は、2 つの Unified CM クラスタがあるネットワーク シナリオを示しています。各クラスタは、SCCP クライアント、H.323 クライアント、H.323 MCU、および H.320 ゲートウェイで構成されています。H.323 クライアント、MCU、および H.320 ゲートウェイの RAS 部分を管理するために、エンドポイント ゲートキーパーを各クラスタに配置します。別のインフラストラクチャ ゲートキーパーが、クラスタ間のダイヤル プラン解決と帯域幅を管理します。この図ではゲートキーパーの冗長性は示されていませんが、これらの各ゲートキーパーは、実際には Alternate Gatekeeper または HSRP ベースの冗長性を持つように設定された複数のゲートキーパーです。

図 16-10　　2 つの Unified CM クラスタと必要なゲートキーパー



サポートされるゲートキーパー プラットフォーム

Cisco Unified CM 4.1 以降を使用するエンドポイント ゲートキーパーとして機能するには、Cisco IOS Gatekeeper で Cisco IOS Release 12.3(11)T 以降を実行する必要があります。インフラストラクチャ ゲートキーパーの最小 Cisco IOS リリース要件については、「Recommended Hardware and Software Combinations」（P.A-1）を参照してください。

次のルータ プラットフォームが Cisco IOS Gatekeeper をサポートしています。

- Cisco 2600XM シリーズおよび 2691
- Cisco 2800 シリーズ
- Cisco 3640、3640A、3660
- Cisco 3725 および 3745

- Cisco 3825 および 3845
- Cisco 7200 シリーズ、7301、および 7400 シリーズ

ルータ プラットフォームで使用する必要があるリリースと機能を判断するには、次の URL にある *Cisco Feature Navigator* を使用します（Cisco.com ログイン アカウントが必要）。

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide_chapter09186a00804193ef.html

この資料には、Cisco IOS Release 12.3(11)T が統合音声およびビデオ サービスを提供すると記載されています。そのため、これが推奨される最小リリースになります。

エンドポイント ゲートキーパー

次の条件の両方が該当する場合は、エンドポイント ゲートキーパーが必要です。

- クラスタに H.323 クライアント、H.323 MCU、または H.320 ゲートウェイ（集合的に H.323 エンドポイントと呼ぶ）が含まれている。これらのタイプのエンドポイントが存在しない場合（たとえば、すべてのクライアントが SCCP エンドポイントで、MCU も H.320 ゲートウェイもない場合）、エンドポイント ゲートキーパーは不要です。
- 次の条件のいずれかに当てはまる。
  - E.164 アドレスへのコール発信のために、H.323 エンドポイントで RAS プロシージャを必要とする。すでに述べたように、ピアツーピア コール シグナリングに対応するデバイスが増えています。これらのデバイスは、ゲートキーパーに登録する必要はありません。
  - H.323 エンドポイントが静的 IP アドレスを使用しない。

エンドポイント ゲートキーパーの役割は、これらの H.323 エンドポイントを登録する場所を提供し、エンドポイントとの通信の RAS 部分を処理するだけです。エンドポイント ゲートキーパーは、これらのエンドポイントが宛先または発信元となるコール、またはこれらのエンドポイント間のすべてのコール要求に対応して、Unified CM がすべてのコール ルーティング機能および帯域幅制御機能を実行できるように、コールを適切な Unified CM サーバに転送します。このコール ルーティング制御および帯域幅制御を実現するには、H.323 トランクをゲートキーパーに登録するように Unified CM を設定し、ゾーンへのコール、ゾーンからのコール、またはゾーン内のコールをすべてこれらのトランクにルーティングするようにゲートキーパーを設定します。

Cisco Unified CM では、RASAggregator トランクという H.323 トランクを使用してエンドポイント ゲートキーパーに登録する必要があります。このタイプのトランクは、すべての H.323 クライアント、H.323 MCU、または H.320 ゲートウェイ ゾーンに使用されます。一方、ゲートキーパー制御クラスタ間トランクおよびゲートキーパー制御 H.225 トランクは、インフラストラクチャ ゲートキーパーとの統合に使用されます。

H.323 クライアントのプロビジョニング

H.323 クライアントは、他の電話機とほぼ同じ方法でプロビジョニングされます。新しい電話機（モデル タイプ = H.323 Client）を作成し、ディレクトリ番号を割り当て、コーリング サーチ スペース、デバイス プールなどを割り当てます。Unified CM で H.323 クライアントは、次のいずれかの方法で設定します。使用する方法は、クライアントが静的 IP アドレスを使用するかどうか、クライアントで E.164 アドレスをダイヤルする RAS プロシージャが必要かどうかによって異なります。

- ゲートキーパー制御

  このタイプの設定は、静的 IP アドレスが割り当てられていないクライアント（DHCP 割り当てアドレスを使用するクライアント）で、E.164 アドレスをダイヤルする RAS プロシージャが必要な場合に使用します。これらのクライアントとの通信には、RASAggregator トランクを使用します（図 16-11 および図 16-12 を参照）。

- 非ゲートキーパー制御、非同期

  このタイプの設定は、静的 IP アドレスが割り当てられているクライアントで、E.164 アドレスをダイヤルする RAS プロシージャが必要な場合に使用します。Unified CM はゲートキーパーを必要とせずに直接シグナルを送信して IP アドレスを解決できますが、クライアントは Unified CM に直接シグナルを送信できず、ダイヤルしようとしている E.164 アドレスを解決するためにゲートキーパーに照会する必要があります（非同期通信）。このタイプのクライアントをサポートするには、実際にはすべてのクライアントが静的 IP アドレスを使用していても、ゲートキーパーのゾーンごとに 1 つ以上のゲートキーパー制御クライアントを Unified CM で定義する必要があります。この場合、非ゲートキーパー制御クライアントは、実際には存在しない「ダミー」クライアントになります。定義する目的は、ゲートキーパーがクライアントから Unified CM へのコールをルーティングできるように、RASAggregator トランクを作成することだけです（図 16-13 および図 16-14 を参照）。

- 非ゲートキーパー制御、同期

  このタイプの設定は、クライアントが静的 IP アドレスを持ち、ピアツーピア シグナリングに対応している（E.164 番号をダイヤルする RAS プロシージャが必要ない）場合に使用します。Unified CM は直接シグナルを送信でき、クライアントは Unified CM に直接シグナルを送信できます（同期通信）。このタイプのクライアントには、ゲートキーパーまたは RASAggregator トランクが不要です（図 16-15 および図 16-16 を参照）。

図 16-11 から図 16-16 は、これら 3 つのシナリオで使用されるコール シグナリング フローを示しています。

図 16-11　Unified CM からゲートキーパー制御クライアントへのコール

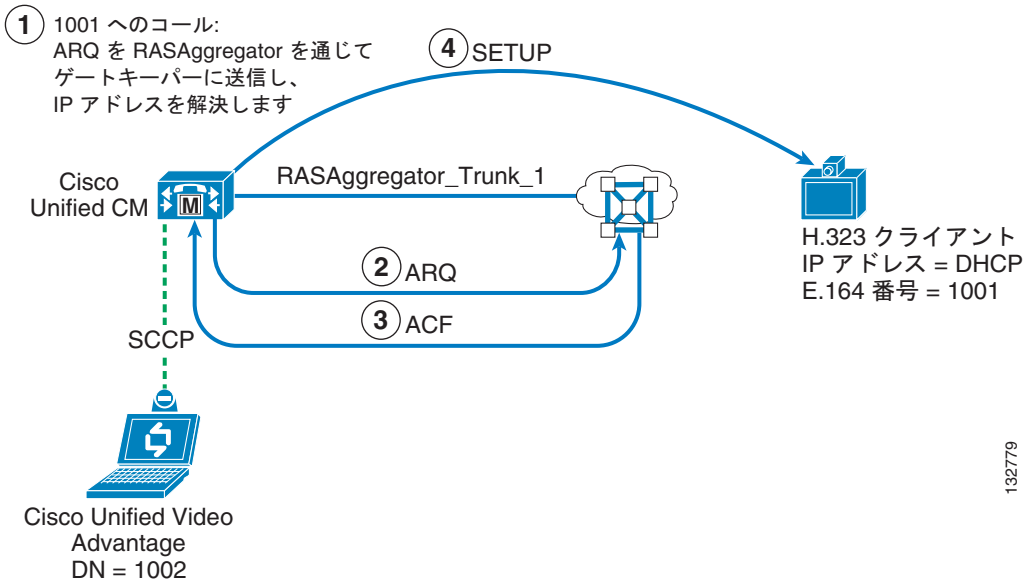


図 16-12　ゲートキーパー制御クライアントから Unified CM へのコール

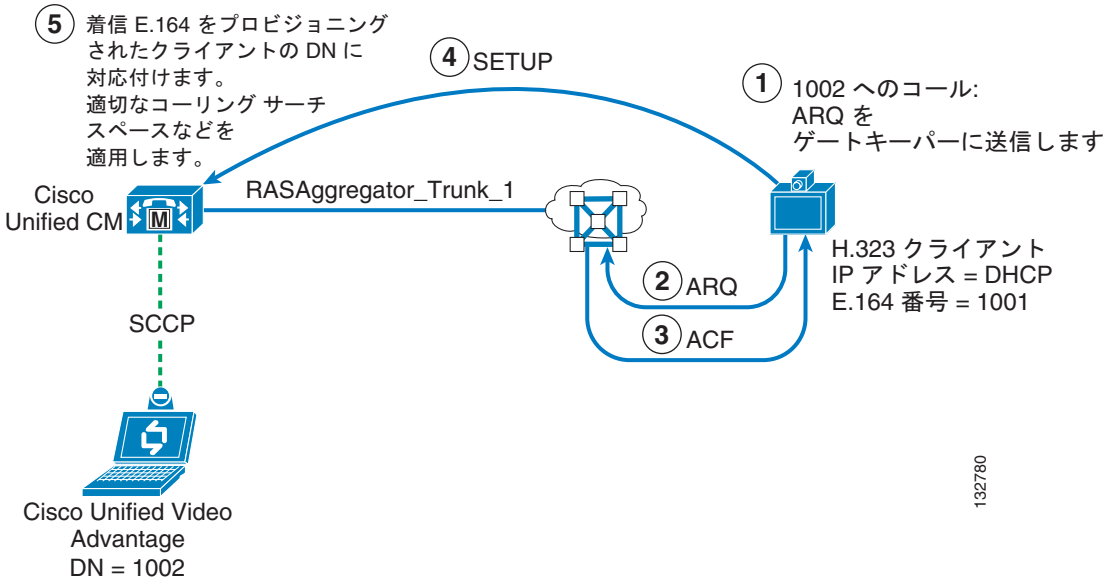


図 16-13　Unified CM から非ゲートキーパー制御クライアントへのコール（非同期）

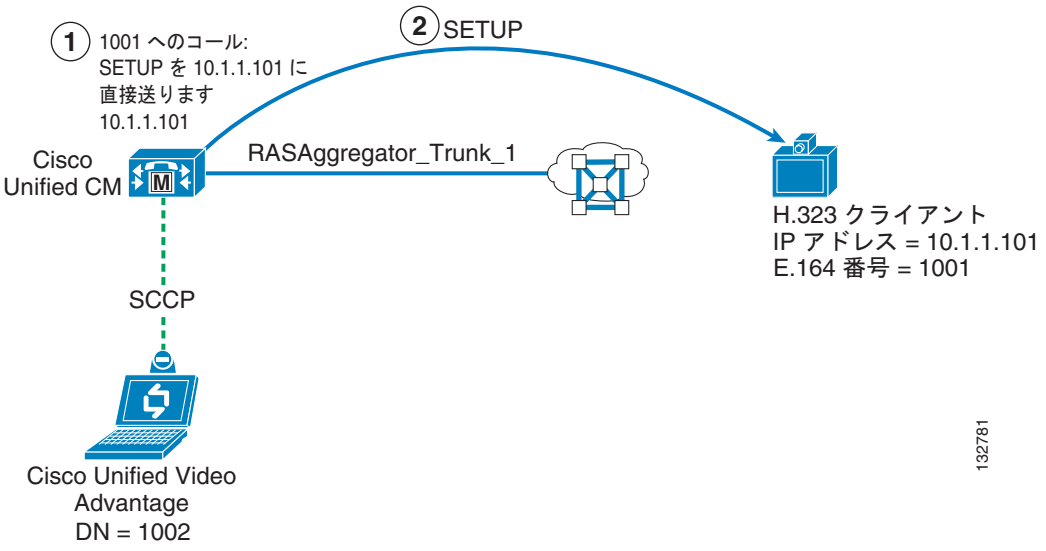


図 16-14　非ゲートキーパー制御クライアントから Unified CM へのコール（非同期）

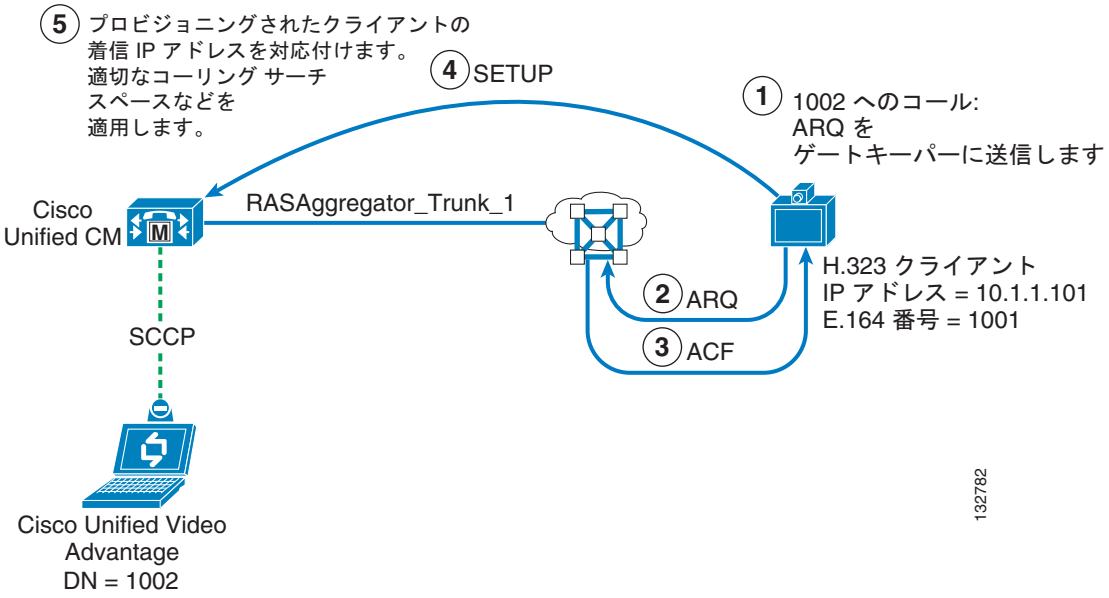


図 16-15　Unified CM から非ゲートキーパー制御クライアントへのコール（同期）

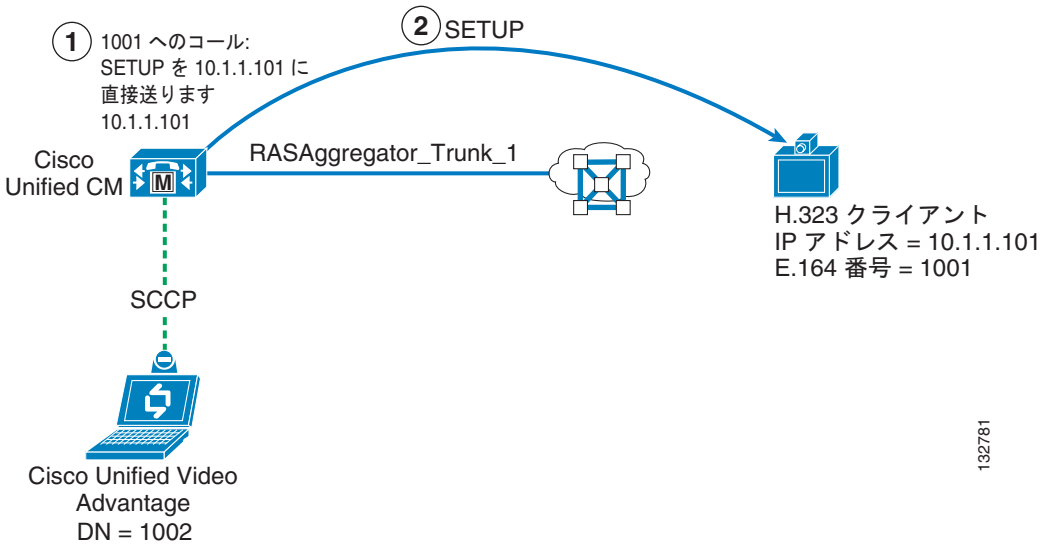
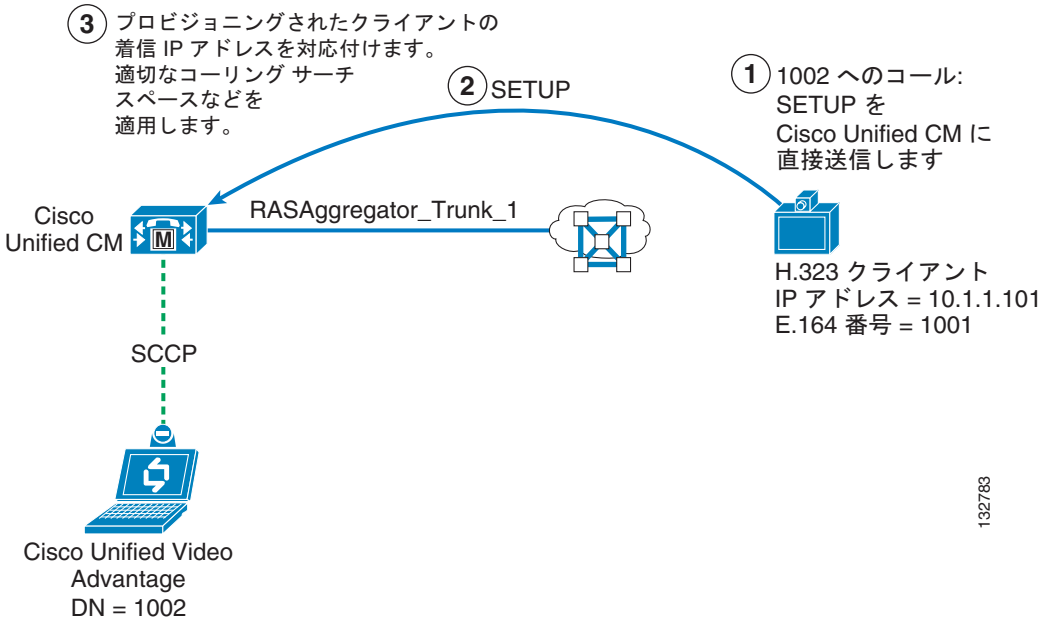


図 16-16　非ゲートキーパー制御クライアントから Unified CM へのコール（同期）



ゲートキーパー制御クライアント

H.323 クライアントをゲートキーパー制御として設定するときは、任意の英数字文字列（わかりやすい名前など）を [Device Name] フィールドに入力し、[Gatekeeper-controlled] ボックスをオンにして、次のフィールドに入力します。

- [Device Pool]

  クライアントで使用するデバイス プール。同じゾーンに登録されているすべての H.323 クライアント（ゲートキーパー制御と非ゲートキーパー制御の両方）が、同じデバイス プールを使用する必要があります。間違ってエンドポイントの間で異なるデバイス プールが割り当てられた場合、Unified CM は複数の RASAggregator トランクをゾーン内で登録し、着信コールが間違った RASAggregator トランクに転送されても、Unified CM で拒否されます。

- [Gatekeeper]

  ゲートキーパー IP アドレスのドロップダウン リスト。ゲートキーパー制御 H.323 クライアントを設定する前に、Unified CM でゲートキーパーを定義する必要があります。

- [Technology Prefix]

  テクノロジー プレフィックスは RASAggregator トランクで使用され、ゲートキーパーのクライアント ゾーンに登録されます。このテクノロジー プレフィックスは、ゲートキーパーでデフォルト テクノロジー プレフィックスとして設定された値と一致している必要があります。同じゾーンに登録されているすべてのゲートキーパー制御 H.323 クライアントが、同じテクノロジー プレフィックスを使用する必要があります。間違ってエンドポイントの間で異なるテクノロジー プレフィックスが割り当てられた場合、Unified CM は複数の RASAggregator トランクをゾーン内で登録し、着信コールが間違った RASAggregator トランクに転送されても、Unified CM で拒否されます。このプレフィックスには **1#** を使用することをお勧めします。

- [Zone Name]

  ゲートキーパーで設定されているクライアント ゾーンの名前（大文字と小文字が区別されます）。同じゾーンに登録されているすべてのゲートキーパー制御 H.323 クライアントが、同じゾーン名を使用する必要があります。間違ってエンドポイントの間で異なるゾーン名（このフィールドは大文字と小文字が区別されます）が割り当てられた場合、Unified CM は複数の RASAggregator トランクをゲートキーパーに登録しようとし（ただし、ゾーン名が不正なトランクは登録に失敗します）、着信コールが間違った RASAggregator トランクに転送されても、Unified CM で拒否されます。

また、Unified CM サービス パラメータの [Send Product ID and Version ID] を [True] に設定する必要があります。このパラメータによって、RASAggregator トランクをゲートキーパーに H323-GW として登録できます。それによりゲートキーパーは、クライアント ゾーンへの H.323 コール、クライアント ゾーンからの H.323 コール、クライアント ゾーン内の H.323 コールのすべてを RASAggregator トランクに転送できます。

非ゲートキーパー制御クライアント

H.323 クライアントを非ゲートキーパー制御としてプロビジョニングする場合は、クライアントの静的 IP アドレスを [Device Name] フィールドに入力し、[Gatekeeper-controlled] セクションの下のその他のすべての設定をブランク（オフ）のままにします。コールがこのディレクトリ番号にルーティングされると、Unified CM は静的 IP アドレスを使用してクライアントに転送します。

クライアントがピアツーピア モードを使用するように設定されている場合、これ以上の設定は不要です。クライアントで E.164 アドレスにコールを発信する RAS プロシージャが必要な場合は、RASAggregator トランクを作成するために、次のフィールドに入力して、ダミーのゲートキーパー制御 H.323 クライアントも設定する必要があります。

- [Device Name]

  クライアント ゾーンの RASAggregator トランクの作成を目的とするダミー クライアントとして、クライアントを識別するためのわかりやすい名前。

- Device Pool

  非ゲートキーパー制御 H.323 クライアントを設定するときに選択したデバイス プール。ダミー クライアントに割り当てられたデバイス プールが、実際のクライアントに割り当てられたデバイス プールと異なる場合、実際のクライアントからの着信コールが Unified CM で拒否されることがあります。

- [Gatekeeper]

  ゲートキーパー IP アドレスのドロップダウン リスト。ダミーのゲートキーパー制御 H.323 クライアントを設定する前に、Unified CM でゲートキーパーを定義する必要があります。

- [Technology Prefix]

  テクノロジー プレフィックスは RASAggregator トランクで使用され、ゲートキーパーのクライアント ゾーンに登録されます。このテクノロジー プレフィックスは、ゲートキーパーでデフォルト テクノロジー プレフィックスとして設定された値と一致している必要があります。このプレフィックスには **1#** を使用することをお勧めします。

- [Zone Name]

  ゲートキーパーで設定されているクライアント ゾーンの名前（大文字と小文字が区別されます）。

また、Unified CM サービス パラメータの [Send Product ID and Version ID] を [True] に設定する必要があります。このパラメータによって、RASAggregator トランクをゲートキーパーに H323-GW として登録できます。それによりゲートキーパーは、クライアント ゾーンへの H.323 コール、クライアント ゾーンからの H.323 コール、クライアント ゾーン内の H.323 コールのすべてを RASAggregator トランクに転送できます。

H.323 MCU のプロビジョニング

H.323 MCU は、Unified CM で H.323 ゲートウェイとしてプロビジョニングされてから、これらのデバイスにコールをルーティングするルート パターンが設定されます。H.323 ゲートウェイをプロビジョニングするときは、MCU の静的 IP アドレスおよび TCP シグナリング ポートを [Device Name] フィールドに入力する必要があります。コールが MCU に関連付けられたルート パターンと一致すると、Unified CM は静的 IP アドレスと TCP ポートを使用して、MCU に到達します。

（注）　Cisco Unified Videoconferencing 3500 シリーズ MCU は、デフォルトでは TCP ポート 1720 を監視しません（Cisco Unified Videoconferencing 3500 シリーズ MCU は、デフォルトでポート 2720 を監視します）。監視している TCP ポートを確認し、1720 に変更するか、正しいポートを Unified CM でプロビジョニングする必要があります。

MCU がピアツーピア モードを使用するように設定されている場合は、これ以上の設定は不要です（Cisco Unified Videoconferencing MCU は、現在、ピアツーピア モードをサポートしていませんが、一部のサードパーティ製 MCU がサポートしています）。MCU で E.164 アドレスにコールを発信する RAS プロシージャが必要な場合は、RASAggregator トランクを作成するために、次のフィールドに入力して、ダミーのゲートキーパー制御 H.323 クライアントも設定する必要があります。

- [Device Name]

  MCU ゾーンの RASAggregator トランクの作成を目的とするダミー クライアントとして、クライアントを識別するためのわかりやすい名前。

- Device Pool

  MCU を表す H.323 ゲートウェイを設定するときに選択したデバイス プール。ダミー クライアントに割り当てられたデバイス プールが、MCU を表す H.323 ゲートウェイに割り当てられたデバイス プールと異なる場合、MCU からの着信コールが Unified CM で拒否されることがあります。

- [Gatekeeper]

  ゲートキーパー IP アドレスのドロップダウン リスト。ダミーのゲートキーパー制御 H.323 クライアントを設定する前に、Unified CM でゲートキーパーを定義する必要があります。

- [Technology Prefix]

  テクノロジー プレフィックスは RASAggregator トランクで使用され、ゲートキーパーの MCU ゾーンに登録されます。このテクノロジー プレフィックスは、ゲートキーパーでデフォルト テクノロジー プレフィックスとして設定された値と一致している必要があります。このプレフィックスには **1#** を使用することをお勧めします。

- [Zone Name]

  ゲートキーパーで設定されている MCU ゾーンの名前（大文字と小文字が区別されます）。

また、Unified CM サービス パラメータの [Send Product ID and Version ID] を [True] に設定する必要があります。このパラメータによって、ゲートキーパーがクライアント ゾーンへの H.323 コール、クライアント ゾーンからの H.323 コール、MCU ゾーン内の H.323 コールのすべてを RASAggregator トランクに転送できるように、RASAggregator トランクをゲートキーパーに H323-GW として登録できます。

MCU サービス プレフィックス

H.323 MCU は、実行中の予約なしまたはスケジュール済みの H.323 会議に到達するダイヤルイン番号として、E.164 アドレスまたはテクノロジー プレフィックス（MCU ではサービス プレフィックスとも呼ばれる）を使用できます。MCU 管理画面で [MCU Mode] を [Gateway] ではなく [MCU] に設定して、E.164 アドレスを使用するように MCU を設定することをお勧めします。使用している MCU のモデルで **MCU** 設定を使用できない場合は、次の特別な設定を使用して、他の H.323 エンドポイントから MCU に発信されたコールを適切にルーティングします。

MCU が **Gateway** モードに設定されている場合、または、別のベンダーの MCU で、（何らかの理由で）会議 ID を E.164 アドレスではなくテクノロジー プレフィックスとして登録する必要がある場合は、MCU のサービス プレフィックスの先頭を **#** 文字にする必要があります。たとえば、MCU サービス プレフィックスが 8005551212 の場合、MCU でサービス プレフィックスを #8005551212 としてプロビジョニングする必要があります。その結果、他の H.323 エンドポイントが 8005551212 とダイヤルすると、ゲートキーパーは登録済みの一致するテクノロジー プレフィックスを検索するのではなく、コールを発信したエンドポイントのゾーンでデフォルト テクノロジー プレフィックスと共に登録された RASAggregator トランクにコールをルーティングします。Unified CM は、コールを MCU にルーティングする前に、着信番号の先頭に # 文字を付加する必要があります。この文字は、MCU を表す H.323 ゲートウェイに関連付けられたルート パターンに付加されます。そのため、SCCP クライアントから MCU へのコールでも、着信番号にこの # 文字が付加されます。

MCU が **MCU** モードで設定されている場合、または E.164 アドレスを会議 ID に使用する別のベンダーの MCU である場合、# 文字を付加する必要はありません。MCU がピアツーピア モードを使用しているため、テクノロジー プレフィックスをゲートキーパーに登録する必要がない場合もこの条件は当てはまらず、# 文字を付加する必要はありません。

H.320 ゲートウェイのプロビジョニング

H.323 MCU と同様に、H.320 ゲートウェイも、Unified CM で H.323 ゲートウェイとしてプロビジョニングされてから、これらのデバイスにコールをルーティングするルート パターンが設定されます。H.323 ゲートウェイをプロビジョニングするときは、H.320 ゲートウェイの静的 IP アドレスおよび TCP シグナリング ポートを [Device Name] フィールドに入力する必要があります。コールがゲートウェイに関連付けられたルート パターンと一致すると、Unified CM は静的 IP アドレスと TCP ポートを使用して、ゲートウェイに到達します。

（注）　Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイは、デフォルトでは TCP ポート 1720 を監視しません（Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイは、デフォルトでポート 1820 を監視します）。監視している TCP ポートを確認し、1720 に変更するか、正しいポートを Unified CM でプロビジョニングする必要があります。

ゲートウェイがピアツーピア モードを使用するように設定されている場合は、これ以上の設定は不要です。ゲートウェイで E.164 アドレスにコールを発信する RAS プロシージャが必要な場合は、RASAggregator トランクを作成するために、次のフィールドに入力して、ダミーのゲートキーパー制御 H.323 クライアントも設定する必要があります。

- [Device Name]

  ゲートウェイ ゾーンの RASAggregator トランクの作成を目的とするダミー クライアントとして、クライアントを識別するためのわかりやすい名前。

- Device Pool

  H.320 ゲートウェイを表す H.323 ゲートウェイを設定するときに選択したデバイス プール。ダミー クライアントに割り当てられたデバイス プールが、ゲートウェイに割り当てられたデバイス プールと異なる場合、ゲートウェイからの着信コールが Unified CM で拒否されることがあります。

- [Gatekeeper]

  ゲートキーパー IP アドレスのドロップダウン リスト。ダミーのゲートキーパー制御 H.323 クライアントを設定する前に、Unified CM でゲートキーパーを定義する必要があります。

- E.164

  このフィールドの入力は必須です。Unified CM で「non-dialable」値にしてください。

- [Technology Prefix]

  テクノロジー プレフィックスは RASAggregator トランクで使用され、ゲートキーパーのゲートウェイ ゾーンに登録されます。このテクノロジー プレフィックスは、ゲートキーパーでデフォルト テクノロジー プレフィックスとして設定された値と一致している必要があります。このプレフィックスには **1#** を使用することをお勧めします。

- [Zone Name]

  ゲートキーパーで設定されているゲートウェイ ゾーンの名前（大文字と小文字が区別されます）。

また、Unified CM サービス パラメータの [Send Product ID and Version ID] を [True] に設定する必要があります。このパラメータによって、RASAggregator トランクをゲートキーパーに H323-GW として登録できます。それによりゲートキーパーは、クライアントゾーンへの H.323 コール、クライアントゾーンからの H.323 コール、クライアントゾーン内の H.323 コールのすべてを RASAggregator トランクに転送できます。

ゲートウェイ サービス プレフィックス

H.320 ゲートウェイは、ユーザが ISDN の宛先に到達するためにダイヤルするプレフィックスとして、テクノロジー プレフィックス（ゲートウェイではサービス プレフィックスとも呼ばれる）を使用します。コールを正しくルーティングするには、ゲートウェイのサービス プレフィックスを # 文字で始まるように設定する必要があります。たとえば、ISDN 番号に到達するためにクライアントがダイヤルするゲートウェイのサービス プレフィックスが 9 の場合、#9 としてゲートウェイでサービス プレフィックスをプロビジョニングする必要があります。この場合、H.323 クライアントが 9 と公衆網番号をダイヤルした場合（918005551212 など）、ゲートキーパーは登録済みの一致するテクノロジー プレフィックスを検索するのではなく、デフォルト テクノロジー プレフィックスと共に登録された Unified CM トランクにコールをルーティングします。Unified CM は、コールをゲートウェイにルーティングする前に、着信番号の先頭に # 文字を付加する必要があります。ゲートウェイがピアツーピア モードを使用しているため、テクノロジー プレフィックスをゲートキーパーに登録する必要がない場合は、この条件は当てはまらず、# 文字を付加する必要がありません。

ゲートキーパー ゾーンの設定

前の項では、Unified CM Administration でエンドポイントをプロビジョニングする方法について説明しました。適切なゾーン定義でエンドポイント ゲートキーパーを設定する必要もあります。Unified CM で、エンドポイントの各タイプ（クライアント、MCU、またはゲートウェイ）にゾーンを設定する必要があり、オプションとして、これらのエンドポイントに関連付けられている各デバイス プールにゾーンを設定します。

各ゾーンは、ゾーンを宛先または発信元とするコール、ゾーン内で発信されるコールのすべてを、ゾーンに登録されている RASAggregator トランクにルーティングするように設定されます。エンドポイント ゲートキーパーでゾーンを設定するには、次のコマンド構文を使用します。

```
zone local <zone_name> <domain_name> <ip_address> invia <zone_name>
outvia <zone_name> enable-intrazone
```

コマンド引数 **invia** は他のゾーンからこのゾーンに発信されたコールに適用され、**outvia** はこのゾーンから他のゾーンに発信するコールに適用されます。**enable-intrazone** は、ゾーン内で発信したコールに適用されます。次の項で、これらのコマンドの使用方法を示します。

クライアント ゾーン

各エンドポイント ゲートキーパー内で設定の必要なクライアント ゾーンの数は、次の要素で決まります。

- H.323 クライアントの関連付け先となるデバイス プール

  デバイス プールは、各 H.323 クライアントの 1 次、2 次、および 3 次 Unified CM サーバを決定します。すべての H.323 クライアントを同じデバイス プールに割り当てた場合、エンドポイント ゲートキーパーで定義する必要があるクライアント ゾーンは 1 つだけです。つまり、H.323 クライアントで使用するデバイス プールごとに、ゲートキーパーで個別のクライアント ゾーンを設定する必要があります。

- エンドポイント ゲートキーパーが単一の Unified CM クラスタにサービスを提供するのか、複数の Unified CM クラスタにサービスを提供するのか

  各クライアント ゾーンは、特定の RASAggregator トランクにコールをルーティングするように設定されます。そのため、1 つのエンドポイント ゲートキーパーを使用して複数の Unified CM クラスタにサービスを提供する場合は、ゲートキーパーがサービスを提供するクラスタごとに、個別のクライアント ゾーンを定義する必要があります。

説明のために、3 つの例でクライアント ゾーンの設定方法を示します。例 16-1 は、すべての H.323 クライアントが同じデバイス プールに関連付けられた単一の Unified CM クラスタに定義される、単一のクライアント ゾーンを示しています。例 16-2 は、H.323 クライアントが 2 つの異なるデバイス プールに分割された単一の Unified CM クラスタを示しています。例 16-3 は、H.323 クライアントがクラスタごとに 2 つの異なるデバイス プールに分割された 2 つの Unified CM クラスタを示しています。

（注） 以下の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に ! のマークを付けてあります。

例 16-1　単一の Unified CM クラスタと単一のデバイス プールのクライアント ゾーン

```
gatekeeper
zone local clients domain.com invia clients outvia clients enable-intrazone
gw-type-prefix 1# default-technology
no use-proxy clients default inbound-to terminal
no use-proxy clients default outbound-from terminal
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 16-2　単一の Unified CM クラスタと 2 つのデバイス プールのクライアント ゾーン

```
gatekeeper
zone local dp1-clients domain.com invia dp1-clients outvia dp1-clients enable-intrazone
zone local dp2-clients domain.com invia dp2-clients outvia dp2-clients enable-intrazone
gw-type-prefix 1# default-technology
no use-proxy dp1-clients default inbound-to terminal
no use-proxy dp1-clients default outbound-from terminal
no use-proxy dp2-clients default inbound-to terminal
no use-proxy dp2-clients default outbound-from terminal
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 16-3　クラスタあたり 2 つのデバイス プールのある 2 つの Unified CM クラスタのクライアント ゾーン

```
gatekeeper
zone local clstr1-dp1-clients domain.com invia clstr1-dp1-clients outvia
clstr1-dp1-clients enable-intrazone
zone local clstr1-dp2-clients domain.com invia clstr1-dp2-clients outvia
clstr1-dp2-clients enable-intrazone
zone local clstr2-dp1-clients domain.com invia clstr2-dp1-clients outvia
clstr2-dp1-clients enable-intrazone
zone local clstr2-dp2-clients domain.com invia clstr2-dp2-clients outvia
clstr2-dp2-clients enable-intrazone
gw-type-prefix 1# default-technology
no use-proxy clstr1-dp1-clients default inbound-to terminal
```

```
no use-proxy clstr1-dp1-clients default outbound-from terminal
no use-proxy clstr1-dp2-clients default inbound-to terminal
no use-proxy clstr1-dp2-clients default outbound-from terminal
no use-proxy clstr2-dp1-clients default inbound-to terminal
no use-proxy clstr2-dp1-clients default outbound-from terminal
no use-proxy clstr2-dp2-clients default inbound-to terminal
no use-proxy clstr2-dp2-clients default outbound-from terminal
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

プロキシ使用の無効化

以前は Cisco Multimedia Conference Manager（MCM）と呼ばれていた Cisco IOS Gatekeeper は、H.323 プロキシ機能を提供していましたが、廃止される予定です。この機能は Unified CM と互換性がありませんが、端末（クライアント）との間のすべてのコールにプロキシを使用するゲートキーパーのコマンドは、まだデフォルトで有効になっています。この機能はクライアント ゾーンごとに、次のコマンド構文で無効にする必要があります。

```
gatekeeper
no use-proxy <zone_name> default [inbound-to | outbound-from] terminals
```

Cisco MCM プロキシは、Cisco IOS Multiservice IP-to-IP Gateway と、それに関連付けられた中継ゾーン対応 Cisco IOS Gatekeeper というソリューションに置き換えられました。このマニュアルでは IP-to-IP ゲートウェイについては説明していませんが、Cisco Unified CM は、RASAggregator トランクをゲートキーパーに登録することで中継ゾーンと IP-to-IP ゲートウェイの構成を活用し、効果的に IP-to-IP ゲートウェイを模倣し、ゲートキーパーが IP-to-IP ゲートウェイであるかのように、すべての invia、outvia、および enable-intrazone コールを RASAggregator トランクにルーティングしています。

クライアント ゾーン プレフィックス

H.323 クライアント ゾーンには、デフォルト テクノロジー プレフィックス以外のゾーン プレフィックスまたはテクノロジー プレフィックスを設定する必要がありません。代わりに、**invia**、**outvia**、**enable-intrazone**、および **gw-type-prefix** <*1#*> **default-technology** コマンドによって、発信されたすべてのコールが、コールを発信したゾーンに関連付けられた RASAggregator トランクにルーティングされます。

MCU ゾーン

各エンドポイント ゲートキーパー内で設定の必要な MCU ゾーンの数は、次の要素で決まります。

- MCU の関連付け先となるデバイス プール

  デバイス プールは、各 MCU の 1 次、2 次、および 3 次 Unified CM サーバを決定します。すべての MCU を同じデバイス プールに割り当てた場合、エンドポイント ゲートキーパーで定義する必要がある MCU ゾーンは 1 つだけです。つまり、MCU で使用するデバイス プールごとに、ゲートキーパーで個別の MCU ゾーンを設定する必要があります。

- エンドポイント ゲートキーパーが単一の Unified CM クラスタにサービスを提供するのか、複数の Unified CM クラスタにサービスを提供するのか

  各 MCU ゾーンは、特定の RASAggregator トランクにコールをルーティングするように設定されます。そのため、1 つのエンドポイント ゲートキーパーを使用して複数の Unified CM クラスタにサービスを提供する場合は、ゲートキーパーがサービスを提供するクラスタごとに、個別の MCU ゾーンを定義する必要があります。

説明のために、3 つの例で MCU ゾーンの設定方法を示します。例 16-4 は、すべての MCU が同じデバイス プールに関連付けられた単一の Unified CM クラスタに定義される、単一の MCU ゾーンを示しています。例 16-5 は、MCU が 2 つの異なるデバイス プールに分割された単一の Unified CM クラスタを示しています。例 16-6 は、MCU が 2 つの異なるデバイス プールに分割された 2 つの Unified CM クラスタを示しています。

（注）　以下の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に ! のマークを付けてあります。

例 16-4　単一の Unified CM クラスタと単一のデバイス プールの MCU ゾーン

```
gatekeeper
zone local MCUs domain.com invia MCUs outvia MCUs enable-intrazone
gw-type-prefix 1# default-technology
! no use-proxy MCUs default inbound-to [MCU | gateway]
! no use-proxy MCUs default outbound-from [MCU | gateway]
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 16-5　単一の Unified CM クラスタと 2 つのデバイス プールの MCU ゾーン

```
gatekeeper
zone local dp1-MCUs domain.com invia dp1-MCUs outvia dp1-MCUs enable-intrazone
zone local dp2-MCUs domain.com invia dp2-MCUs outvia dp2-MCUs enable-intrazone
gw-type-prefix 1# default-technology
! no use-proxy dp1-MCUs default inbound-to [MCU | gateway]
! no use-proxy dp1-MCUs default outbound-from [MCU | gateway]
! no use-proxy dp2-MCUs default inbound-to [MCU | gateway]
! no use-proxy dp2-MCUs default outbound-from [MCU | gateway]
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 16-6　クラスタあたり 2 つのデバイス プールのある 2 つの Unified CM クラスタの MCU ゾーン

```
gatekeeper
zone local clstr1-dp1-MCUs domain.com invia clstr1-dp1-MCUs outvia clstr1-dp1-MCUs
enable-intrazone
zone local clstr1-dp2-MCUs domain.com invia clstr1-dp2-MCUs outvia clstr1-dp2-MCUs
enable-intrazone
zone local clstr2-dp1-MCUs domain.com invia clstr2-dp1-MCUs outvia clstr2-dp1-MCUs
enable-intrazone
zone local clstr2-dp2-MCUs domain.com invia clstr2-dp2-MCUs outvia clstr2-dp2-MCUs
enable-intrazone
gw-type-prefix 1# default-technology
! no use-proxy clstr1-dp1-MCUs default inbound-to [MCU | gateway]
! no use-proxy clstr1-dp1-MCUs default outbound-from [MCU | gateway]
! no use-proxy clstr1-dp2-MCUs default inbound-to [MCU | gateway]
! no use-proxy clstr1-dp2-MCUs default outbound-from [MCU | gateway]
! no use-proxy clstr2-dp1-MCUs default inbound-to [MCU | gateway]
! no use-proxy clstr2-dp1-MCUs default outbound-from [MCU | gateway]
! no use-proxy clstr2-dp2-MCUs default inbound-to [MCU | gateway]
! no use-proxy clstr2-dp2-MCUs default outbound-from [MCU | gateway]
! no arq reject-unknown-prefix
endpoint ttl 60
```

```
no shutdown
```

プロキシ使用の無効化

デフォルトでは、Cisco IOS Gatekeeper は MCU またはゲートウェイとの間のコールにプロキシを使用しないように設定されています。ただし、これらのタイプのエンドポイントでプロキシの使用を有効にした場合は、次のコマンド構文を使用して、各 MCU ゾーンで無効にする必要があります。

```
gatekeeper
no use-proxy <zone_name> default [inbound-to | outbound-from] [MCU | gateway]
```

MCU を MCU として登録する場合は、**no use-proxy** コマンドの最後で **MCU** 引数を使用します。MCU をゲートウェイとして登録する場合は、**gateway** 引数を使用します。

MCU ゾーン プレフィックス

H.323 MCU ゾーンには、デフォルト テクノロジー プレフィックス以外のゾーン プレフィックスまたはテクノロジー プレフィックスを設定する必要がありません。代わりに、**invia**、**outvia**、**enable-intrazone**、および **gw-type-prefix** *<1#>* **default-technology** コマンドによって、発信されたすべてのコールが、コールを発信したゾーンに関連付けられた RASAggregator トランクにルーティングされます。

MCU が E.164 アドレスではなくテクノロジー プレフィックスとしてサービス プレフィックスを登録する場合は、すでに説明したように、# 文字を MCU のサービス プレフィックスに付加する特殊な設定を使用します（「MCU サービス プレフィックス」（P.16-32）を参照）。Cisco IOS Gatekeeper がテクノロジー プレフィックスへのコールの中継ゾーンを選択する方法が原因となり、エンドポイントが MCU のサービス プレフィックスをダイヤルしたときに、ゲートキーパーが登録済みの一致するテクノロジー プレフィックスを見つけると、コールは失敗します。ゲートキーパーが一致するテクノロジー プレフィックスを見つけずに、コールを発信したゾーンに関連付けられている RASAggregator トランクにコールをルーティングするように、クライアントが # 文字をダイヤルしないようにする必要があります。

H.320 ゲートウェイ ゾーン

各エンドポイント ゲートキーパー内で設定の必要な H.320 ゲートウェイ ゾーンの数は、次の要素で決まります。

- H.320 ゲートウェイの関連付け先となるデバイス プール

  デバイス プールは、各 H.320 ゲートウェイの 1 次、2 次、および 3 次 Unified CM サーバを決定します。すべてのゲートウェイを同じデバイス プールに割り当てた場合、エンドポイント ゲートキーパーで定義する必要があるゲートウェイ ゾーンは 1 つだけです。つまり、H.320 ゲートウェイで使用するデバイス プールごとに、ゲートキーパーで個別のゲートウェイ ゾーンを設定する必要があります。

- エンドポイント ゲートキーパーが単一の Unified CM クラスタにサービスを提供するのか、複数の Unified CM クラスタにサービスを提供するのか

  各ゲートウェイ ゾーンは、特定の RASAggregator トランクにコールをルーティングするように設定されます。そのため、1 つのエンドポイント ゲートキーパーを使用して複数の Unified CM クラスタにサービスを提供する場合は、ゲートキーパーがサービスを提供するクラスタごとに、個別のゲートウェイ ゾーンを定義する必要があります。

説明のために、3 つの例でゲートウェイ ゾーンの設定方法を示します。例 16-7 は、すべての H.320 ゲートウェイが同じデバイス プールに関連付けられた単一の Unified CM クラスタに定義される、単一のゲートウェイ ゾーンを示しています。例 16-8 は、ゲートウェイが 2 つの異なるデバイス プールに分割された単一の Unified CM クラスタを示しています。例 16-9 は、ゲートウェイが 2 つの異なるデバイス プールに分割された 2 つの Unified CM クラスタを示しています。

（注）　以下の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に **!** のマークを付けてあります。

例 16-7　単一の Unified CM クラスタと単一のデバイス プールのゲートウェイ ゾーン

```
gatekeeper
zone local gateways domain.com invia gateways outvia gateways enable-intrazone
gw-type-prefix 1# default-technology
! no use-proxy gateways default inbound-to gateway
! no use-proxy gateways default outbound-from gateway
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 16-8　単一の Unified CM クラスタと 2 つのデバイス プールのゲートウェイ ゾーン

```
gatekeeper
zone local dp1-gateways domain.com invia dp1-gateways outvia dp1-gateways enable-intrazone
zone local dp2-gateways domain.com invia dp2-gateways outvia dp2-gateways enable-intrazone
gw-type-prefix 1# default-technology
! no use-proxy dp1-gateways default inbound-to gateway
! no use-proxy dp1-gateways default outbound-from gateway
! no use-proxy dp2-gateways default inbound-to gateway
! no use-proxy dp2-gateways default outbound-from gateway
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 16-9　クラスタあたり 2 つのデバイス プールのある 2 つの Unified CM クラスタのゲートウェイ ゾーン

```
gatekeeper
zone local clstr1-dp1-gateways domain.com invia clstr1-dp1-gateways outvia
clstr1-dp1-gateways enable-intrazone
zone local clstr1-dp2-gateways domain.com invia clstr1-dp2-gateways outvia
clstr1-dp2-gateways enable-intrazone
zone local clstr2-dp1-gateways domain.com invia clstr2-dp1-gateways outvia
clstr2-dp1-gateways enable-intrazone
zone local clstr2-dp2-gateways domain.com invia clstr2-dp2-gateways outvia
clstr2-dp2-gateways enable-intrazone
gw-type-prefix 1# default-technology
! no use-proxy clstr1-dp1-gateways default inbound-to gateway
! no use-proxy clstr1-dp1-gateways default outbound-from gateway
! no use-proxy clstr1-dp2-gateways default inbound-to gateway
! no use-proxy clstr1-dp2-gateways default outbound-from gateway
! no use-proxy clstr2-dp1-gateways default inbound-to gateway
! no use-proxy clstr2-dp1-gateways default outbound-from gateway
! no use-proxy clstr2-dp2-gateways default inbound-to gateway
! no use-proxy clstr2-dp2-gateways default outbound-from gateway
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

プロキシ使用の無効化

デフォルトでは、Cisco IOS Gatekeeper はゲートウェイとの間のコールにプロキシを使用しないように設定されています。ただし、これらのタイプのエンドポイントでプロキシの使用を有効にした場合は、次のコマンド構文を使用して、各 H.320 ゲートウェイ ゾーンで無効にする必要があります。

```
gatekeeper
no use-proxy <zone_name> default [inbound-to | outbound-from] gateway
```

ゲートウェイ ゾーン プレフィックス

H.320 ゲートウェイ ゾーンには、ゾーン プレフィックスを設定する必要がありません。代わりに、**invia**、**outvia**、**enable-intrazone**、および **gw-type-prefix** *<1#>* **default-technology** コマンドによって、発信されたすべてのコールが、コールを発信したゾーンに関連付けられた RASAggregator トランクにルーティングされます。

また、すでに説明したように、ゲートウェイのサービス プレフィックスに # 文字を付加する特殊な設定を使用する必要があります（「ゲートウェイ サービス プレフィックス」（P.16-34）を参照）。Cisco IOS Gatekeeper がテクノロジー プレフィックスへのコールの中継ゾーンを選択する方法が原因となり、エンドポイントがゲートウェイのサービス プレフィックスをダイヤルしたときに、ゲートキーパーが登録済みの一致するテクノロジー プレフィックスを見つけると、コールは失敗します。ゲートキーパーが一致するテクノロジー プレフィックスを見つけずに、コールを発信したゾーンに関連付けられている RASAggregator トランクにコールをルーティングするように、クライアントが # 文字をダイヤルしないようにする必要があります。

ゾーン サブネット

すでに説明したように、H.323 仕様では、単一のゲートキーパーで複数のゾーンを管理できます。ただし、ゲートキーパーには、デバイスから Registration Request（RRQ）を受信したときに、そのエンドポイントをどのゾーンに配置するかを判断する手段が必要です。RRQ メッセージには、エンドポイントがどのゾーンへの登録を希望するかを示す Gatekeeper Identifier フィールドが含まれています。ただし、多くの H.323 ビデオ エンドポイントはこのフィールドを設定せず、ゲートキーパーに複数のゾーンが定義されている場合、ゲートキーパーはエンドポイントを配置するゾーンを認識できません。そのため、**zone subnet** コマンドを使用して、エンドポイントと関連付けられたゾーンをゲートキーパーに示す必要があります。このコマンドは、各ゾーンへの登録が許可される IP アドレスまたは IP の範囲を定義します。コマンド構文には、ネットワーク マスクの入力が必要です。そのため、32 ビット（/32）のネットワーク マスクを入力して特定のホスト アドレスを指定するか、それよりも小さなネットワーク マスクを指定してアドレスの範囲を指定します。

MCU、H.320 ゲートウェイ、および Unified CM サーバは通常、固定 IP アドレスを使用しますが、H.323 クライアントは DHCP アドレスを使用できます。そのため、**zone subnet** コマンドは MCU ゾーンおよびゲートウェイ ゾーンにのみ定義し、クライアント ゾーンは任意の IP アドレスを許可できるようにオープンのままにすることをお勧めします。例 16-10 で示すように、Unified CM サーバが MCU ゾーンおよびゲートウェイ ゾーンに登録することも許可する必要があることに注意してください。

（注） 以下の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に ! のマークを付けてあります。

例 16-10　ゾーン サブネットの定義

```
gatekeeper
no zone subnet MCUs default enable
zone subnet MCUs [MCUs_IP_addr]/32 enable
zone subnet MCUs [RASAggregators_IP_addr]/32 enable
```

```
no zone subnet gateways default enable
zone subnet gateways [gateways_IP_addr]/32 enable
zone subnet gateways [RASAggregators_IP_addr]/32 enable
! zone subnet clients default enable
no zone subnet clients [MCUs_IP_addr]/32 enable
no zone subnet clients [gateways_IP_addr]/32 enable
```

例 16-10 の設定では、MCU ゾーンの MCU および RASAggregator を MCU ゾーンに登録することを明示的に許可しています。また、ゲートウェイ ゾーンのゲートウェイおよび RASAggregator をゲートウェイ ゾーンに登録することを明示的に許可しています。また、MCU およびゲートウェイをクライアント ゾーンに登録できないように明示的に拒否しています。その他のすべての IP アドレス（クライアント ゾーンの RASAggregator を含む）は、クライアント ゾーンに登録することが暗黙的に許可されています。

エンドポイントの存続可能時間

エンドポイントは、簡易な Registration Request（RRQ）をゲートキーパーに定期的に送信し、登録状態を維持します。これらの RRQ を送信する間隔は、Time to Live（TTL; 存続可能時間）値とも呼ばれます。エンドポイントは、使用する TTL を RRQ の本体で指定できます。ゲートキーパーは、エンドポイントが要求した TTL 値を受け入れて Registration Confirm（RCF）応答でエコーするか、異なる TTL 値を RCF で指定してエンドポイントの要求を上書きします。

TTL 値が RRQ で指定されていない場合は、ゲートキーパーが RCF 応答で指定する必要があります。この場合、エンドポイントはゲートキーパーが指定した TTL に従います。Cisco IOS Gatekeeper は、エンドポイントが指定したすべての TTL 値に従います。ただし、多くの H.323 ビデオ エンドポイントは、RRQ で TTL 値を指定しません。この場合、Cisco IOS Gatekeeper は、デフォルト値として 1800 秒（30 分）の TTL 値を指定します。Cisco IOS Gatekeeper は、エンドポイントからメッセージを受信せずに TTL 間隔の 3 倍の時間（3 × 30 分 = 90 分）が経過すると、そのエンドポイントの登録をフラッシュします。

TTL 値を大きくすると、静的 IP アドレスを使用しない H.323 クライアントで問題が発生することがあります。たとえば、デフォルト TTL 値の 1800 秒を使用した場合、クライアントをネットワークから切断し、別のロケーションに移動して異なる DHCP アドレスを受け取った場合、TTL 間隔の 3 倍が経過して、ゲートキーパーがそのエンドポイントの元の登録をフラッシュするまで、ゲートキーパーへの登録に失敗します（Registration Reject（RRJ）の理由値「duplicate alias」）。

したがって、ネットワークに悪影響が生じない範囲で、TTL 値はできるだけ小さくするようにしてください。Cisco IOS Gatekeeper では、60 秒から 3600 秒の任意の値に TTL 値を設定できます。ほとんどの場合、60 秒でうまく動作するはずです。ただし、すでにゲートキーパーの使用率が高い場合は、TTL をデフォルトの 1800 秒から 60 秒に調整すると、負荷が過大になることがあります。

TTL 値を設定するには、次のコマンド構文を使用します。

gatekeeper
endpoint ttl <*seconds*>

エンドポイント ゲートキーパーの要約

この項では、エンドポイント ゲートキーパーに関する重要なポイントを要約し、前の例で使用したテクニックを組み合せたいくつかの設定例を示します。

- エンドポイントのタイプ（クライアント、MCU、および H.320 ゲートウェイ）ごとに、エンドポイント ゲートキーパーに個別のゾーンを設定します。エンドポイントが複数のデバイス プールに関連付けられている場合は、エンドポイントのタイプごとに複数のゾーンを設定します。

- 各ゾーンに登録する RASAggregator トランクを設定します。このトランクは、Unified CM Administration でゲートキーパー制御 H.323 クライアントを設定したときに、自動的に作成されます。ただし、非ゲートキーパー制御 H.323 クライアント、H.323 MCU、および H.320 ゲートウェイに対しては、ゾーンの RASAggregator トランクを作成するために、ダミーのゲートキーパー制御 H.323 クライアントを設定する必要があります。
- RASAggregator トランクを IP-to-IP ゲートウェイとしてゲートキーパーに登録するには、デバイス パラメータ [Send Product ID and Version ID] を [True] に設定します。このように設定すると、ゲートキーパーは各ローカル ゾーン定義に適用される **invia**、**outvia**、**enable-intrazone**、および **gw-type-prefix** *<1#>* **default-technology** の各コマンドを使用することによって、ゾーンを宛先または発信元とするコール、またはゾーン内で発信されるコールのすべてについて、RASAggregator を選択できます。
- エンドポイント ゾーンにゾーン プレフィックスを関連付ける必要はありません。エンドポイントが何をダイヤルしても、ゲートキーパーは一致するゾーン プレフィックスまたはテクノロジー プレフィックスを見つけることなく、コールを発信したゾーンに関連付けられている RASAggregator トランクにコールをルーティングする必要があります。ゲートキーパーで、ダイヤルされた番号と MCU またはゲートウェイのテクノロジー プレフィックスが間違って一致することを防ぐために、すべての MCU およびゲートウェイ サービス プレフィックスを # 文字でマスクし、MCU またはゲートウェイに関連付けられているルート パターンに # 文字を付加します。
- Gatekeeper Identifier（ゾーン名）の指定機能をサポートしていない H.323 エンドポイントがある場合は、登録するゾーン サブネットを設定します。
- すべてのゾーンで、古い MCM プロキシの使用を無効にします。
- ゲートキーパーの負荷が過大にならない範囲で、できるだけ低い値でエンドポイント登録の存続可能時間（TTL）を設定します。ゲートキーパーが数百のエンドポイント登録を処理するような極端なケースでは、TTL を 60 秒に設定すると、管理できない量の RAS トラフィックが発生することがあります。小規模な環境では、60 秒でうまく動作するはずです。

例 16-11 は、単一の Unified CM クラスタにサービスを提供するエンドポイント ゲートキーパーの設定を示しています。このクラスタは、単一のデバイス プールを使用して、すべての H.323 ビデオ エンドポイント タイプにサービスを提供します。

（注） 以下の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に **!** のマークを付けてあります。

例 16-11　単一のクラスタと単一のデバイス プールのエンドポイント ゲートキーパー設定

```
gatekeeper
zone local clients domain.com invia clients outvia clients enable-intrazone
zone local MCUs domain.com invia MCUs outvia MCUs enable-intrazone
zone local gateways domain.com invia gateways outvia gateways enable-intrazone
! zone subnet clients default enable
no zone subnet clients [MCUs_IP_addr]/32 enable
no zone subnet clients [gateways_IP_addr]/32 enable
no zone subnet MCUs default enable
zone subnet MCUs [MCUs_IP_addr]/32 enable
zone subnet MCUs [RASAggregators_IP_addr]/32 enable
no zone subnet gateways default enable
zone subnet gateways [gateways_IP_addr]/32 enable
zone subnet gateways [RASAggregators_IP_addr]/32 enable
no use-proxy clients inbound-to terminals
no use-proxy clients outbound-from terminals
! no use-proxy MCUs inbound-to [MCU | gateway]
! no use-proxy MCUs outbound-from [MCU | gateway]
```

```
! no use-proxy gateways inbound-to gateway
! no use-proxy gateways outbound-from gateway
gw-type-prefix 1# default-technology
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 16-12 は、2 つの Unified CM クラスタにサービスを提供するエンドポイント ゲートキーパーの設定を示しています。各クラスタには、H.323 ビデオ エンドポイント用に 2 つの異なるデバイス プールがあります。

例 16-12　2 つのクラスタと 2 つのデバイス プールのエンドポイント ゲートキーパー設定

```
gatekeeper
zone local clstr1-dp1-clients domain.com invia clstr1-dp1-clients outvia
clstr1-dp1-clients enable-intrazone
zone local clstr1-dp1-MCUs domain.com invia clstr1-dp1-MCUs outvia clstr1-dp1-MCUs
enable-intrazone
zone local clstr1-dp1-gateways domain.com invia clstr1-dp1-gateways outvia
clstr1-dp1-gateways enable-intrazone
zone local clstr1-dp2-clients domain.com invia clstr1-dp2-clients outvia
clstr1-dp2-clients enable-intrazone
zone local clstr1-dp2-MCUs domain.com invia clstr1-dp2-MCUs outvia clstr1-dp2-MCUs
enable-intrazone
zone local clstr1-dp2-gateways domain.com invia clstr1-dp2-gateways outvia
clstr1-dp2-gateways enable-intrazone
zone local clstr2-dp1-clients domain.com invia clstr2-dp1-clients outvia
clstr2-dp1-clients enable-intrazone
zone local clstr2-dp1-MCUs domain.com invia clstr1-dp2-MCUs outvia clstr2-dp1-MCUs
enable-intrazone
zone local clstr2-dp1-gateways domain.com invia clstr2-dp1-gateways outvia
clstr2-dp1-gateways enable-intrazone
zone local clstr2-dp2-clients domain.com invia clstr2-dp2-clients outvia
clstr2-dp2-clients enable-intrazone
zone local clstr2-dp2-MCUs domain.com invia clstr2-dp2-MCUs outvia clstr2-dp2-MCUs
enable-intrazone
zone local clstr2-dp2-gateways domain.com invia clstr2-dp2-gateways outvia
clstr2-dp2-gateways enable-intrazone
! zone subnet clstr1-dp1-clients default enable
no zone subnet clstr1-dp1-clients [clstr1-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr1-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr2-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr2-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr1-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr1-dp2 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr2-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr2-dp2 gateways_IP_addr]/32 enable
! zone subnet clstr1-dp2-clients default enable
no zone subnet clstr1-dp2-clients [clstr1-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr1-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr2-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr2-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr1-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr1-dp2 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr2-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr2-dp2 gateways_IP_addr]/32 enable
! zone subnet clstr2-dp1-clients default enable
no zone subnet clstr2-dp1-clients [clstr1-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr1-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr2-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr2-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr1-dp1 gateways_IP_addr]/32 enable
```

```
no zone subnet clstr2-dp1-clients [clstr1-dp2 gateways_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr2-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr2-dp2 gateways_IP_addr]/32 enable
zone subnet clstr2-dp2-clients default enable
no zone subnet clstr2-dp2-clients [clstr1-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr1-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr2-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr2-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr1-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr1-dp2 gateways_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr2-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr2-dp2 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp1-MCUs default enable
zone subnet clstr1-dp1-MCUs [clstr1-dp1 MCUs_IP_addr]/32 enable
zone subnet clstr1-dp1-MCUs [clstr1-dp1 RASAggregators_IP_addr]/32 enable
no zone subnet clstr1-dp2-MCUs default enable
zone subnet clstr1-dp2-MCUs [clstr1-dp2 MCUs_IP_addr]/32 enable
zone subnet clstr1-dp2-MCUs [clstr1-dp2 RASAggregators_IP_addr]/32 enable
no zone subnet clstr2-dp1-MCUs default enable
zone subnet clstr2-dp1-MCUs [clstr2-dp1 MCUs_IP_addr]/32 enable
zone subnet clstr2-dp1-MCUs [clstr2-dp1 RASAggregators_IP_addr]/32 enable
no zone subnet clstr2-dp2-MCUs default enable
zone subnet clstr2-dp2-MCUs [clstr2-dp2 MCUs_IP_addr]/32 enable
zone subnet clstr2-dp2-MCUs [clstr2-dp2 RASAggregators_IP_addr]/32 enable
no zone subnet clstr1-dp1-gateways default enable
zone subnet clstr1-dp1-gateways [clstr1-dp1 gateways_IP_addr]/32 enable
zone subnet clstr1-dp1-gateways [clstr1-dp1 RASAggregators_IP_addr]/32 enable
no zone subnet clstr1-dp2-gateways default enable
zone subnet clstr1-dp2-gateways [clstr1-dp2 gateways_IP_addr]/32 enable
zone subnet clstr1-dp2-gateways [clstr1-dp2 RASAggregators_IP_addr]/32 enable
no zone subnet clstr2-dp1-gateways default enable
zone subnet clstr2-dp1-gateways [clstr2-dp1 gateways_IP_addr]/32 enable
zone subnet clstr2-dp1-gateways [clstr2-dp1 RASAggregators_IP_addr]/32 enable
no zone subnet clstr2-dp2-gateways default enable
zone subnet clstr2-dp2-gateways [clstr2-dp2 gateways_IP_addr]/32 enable
zone subnet clstr2-dp2-gateways [clstr2-dp2 RASAggregators_IP_addr]/32 enable
no use-proxy clstr1-dp1-clients inbound-to terminals
no use-proxy clstr1-dp1-clients outbound-from terminals
no use-proxy clstr1-dp2-clients inbound-to terminals
no use-proxy clstr1-dp2-clients outbound-from terminals
no use-proxy clstr2-dp1-clients inbound-to terminals
no use-proxy clstr2-dp1-clients outbound-from terminals
no use-proxy clstr2-dp2-clients inbound-to terminals
no use-proxy clstr2-dp2-clients outbound-from terminals
! no use-proxy clstr1-dp1-MCUs inbound-to [MCU | gateway]
! no use-proxy clstr1-dp1-MCUs outbound-from [MCU | gateway]
! no use-proxy clstr1-dp2-MCUs inbound-to [MCU | gateway]
! no use-proxy clstr1-dp2-MCUs outbound-from [MCU | gateway]
! no use-proxy clstr2-dp1-MCUs inbound-to [MCU | gateway]
! no use-proxy clstr2-dp1-MCUs outbound-from [MCU | gateway]
! no use-proxy clstr2-dp2-MCUs inbound-to [MCU | gateway]
! no use-proxy clstr2-dp2-MCUs outbound-from [MCU | gateway]
! no use-proxy clstr1-dp1-gateways inbound-to gateway
! no use-proxy clstr1-dp1-gateways outbound-from gateway
! no use-proxy clstr1-dp2-gateways inbound-to gateway
! no use-proxy clstr1-dp2-gateways outbound-from gateway
! no use-proxy clstr2-dp1-gateways inbound-to gateway
! no use-proxy clstr2-dp1-gateways outbound-from gateway
! no use-proxy clstr2-dp2-gateways inbound-to gateway
! no use-proxy clstr2-dp2-gateways outbound-from gateway
gw-type-prefix 1# default-technology
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

アプリケーション

Cisco Unified Communications には、Unified CM の機能を拡張し、高度な機能と他の通信メディアとの統合を提供する幅広いアプリケーションのポートフォリオが用意されています。これらの多くのアプリケーションは、特にビデオをサポートしていなくても、IP ビデオ テレフォニー デバイスと組み合せて使用できます。たとえば、Cisco Unified CM は、TAPI/JTAPI プロトコルを使用する CTI アプリケーションのビデオ チャネルのネゴシエーションをサポートしていませんが、CTI アプリケーションをビデオ コールと組み合せて使用する妨げにはなりません。この項では、シスコおよびサードパーティ製のアプリケーションのいくつかについて検討し、ビデオ コールに対して高度なコール トリートメントを提供できるかどうかについて説明します。

CTI アプリケーション

次のアプリケーションは、コンピュータ/テレフォニー インテグレーション（CTI）インターフェイスに基づいています。

Cisco Emergency Responder

Cisco Emergency Responder（ER）は、緊急コール（911）を適切な Public Safety Answering Point（PSAP）にルーティングします。また、PSAP が事故のあった物理的な正しい場所に応答し、コールが切断された場合はコールバックできるように、発信元デバイスの正しい発信元回線 ID を PSAP に提供します。Cisco ER は、JTAPI を使用して Unified CM に統合されています。緊急コールは CTI ルートポイント経由で Cisco ER にルーティングされ、Cisco ER は、コールの転送先 PSAP および表示する発信元回線 ID を判断します。Cisco ER は、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）と Cisco Discovery Protocol（CDP; シスコ検出プロトコル）を使用して、エンドポイントが接続されている物理ポートと特定の Cisco Catalyst Ethernet スイッチを検出することによって、ネットワークの各エンドポイントを追跡し、物理的な場所を判断します。CDP を使用できない場合は、代わりに IP サブネットを使用してエンドポイントを探すように Cisco ER を設定できます。Cisco ER は、この情報をスイッチの物理的な場所に関連付け、データベースに情報を格納します。

Cisco Unified Video Advantage と Cisco IP Video Phone 7985 はどちらも、Cisco ER 検出の目的で CDP をサポートしています。Cisco Unified Video Advantage は、スイッチに CDP メッセージを直接送信しませんが、このサポート用として、関連付けられた Cisco Unified IP Phone を利用します。その結果、Video Telephony ユーザが 911 をダイヤルすると、Cisco ER は正しい PSAP にコールをルーティングできます。

サードパーティ製の SCCP ビデオ エンドポイントは CDP をサポートしないため、Cisco ER は、IP サブネットでこれらのエンドポイントを追跡する必要があります。これにより、Cisco ER はコールを正しい PSAP にルーティングできます。

H.323 ビデオ会議クライアントは CDP をサポートしないため、Cisco ER は、IP サブネットでこれらのエンドポイントを追跡する必要があります。これにより、Cisco ER はコールを正しい PSAP にルーティングできます。ただし、H.323 デバイスのコールを Cisco ER でルーティングするには、H.323 デバイスが Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Unified CM からの ECS の受信をサポートしていない場合、Cisco ER が処理する 911 へのコールは失敗します。

Cisco Unified Communications Manager Assistant

Cisco Unified Communications Manager Assistant を使用すると、アシスタントが、関連するマネージャに対応できます。Unified CM Assistant は、JTAPI を使用して Unified CM に統合されています。Unified CM Assistant は特にビデオ対応というわけではありませんが、ビデオ対応の電話機でも Unified CM Assistant は問題なく使用できます。Unified CM Assistant がコールを処理し、コールが最終的な宛先デバイスに転送されると、コールの 2 つのデバイスが互いに直接通信し、この時点でビデオ チャネルを確立できます。たとえば、ビデオ対応エンドポイントがマネージャのディレクトリ番号をダイヤルし、アシスタントが Unified CM Assistant アプリケーションを使用してコールをカバーした場合、コールの最初の処理ではビデオは確立されていないことがあります。しかし、アシスタントが発信者をマネージャに転送すると、Unified CM がビデオ チャネルをネゴシエートできるようになります。ただし、H.323 デバイスを Unified CM Assistant と相互運用するには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Unified CM からの ECS の受信をサポートしていない場合、Unified CM Assistant が代行受信したコールは、アシスタントがマネージャにコールを転送しようとしたときに失敗します。

Cisco Unified IP Interactive Voice Response と Cisco Unified Contact Center

Cisco Unified IP Interactive Voice Response（Unified IP IVR）および Cisco Unified Contact Center（Unified CC）は、JTAPI を使用して Unified CM に統合されています。ビデオ対応デバイスが IVR アプリケーション（ヘルプ デスクなど）にコールを発信した場合、発信者がアプリケーション サーバに接続している間（発信者が IVR メニューをブラウズしている間、またはヘルプデスクのメンバーがコールを受け付けるまでキューで待機している間）、通信は音声のみになります。ただし、IVR アプリケーションがコールを最終的な宛先に転送すると、その時点でビデオ チャネルをネゴシエートできるようになります。H.323 デバイスを Cisco Unified IP IVR および Unified CC と相互運用するには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Unified CM からの ECS の受信をサポートしていない場合、Cisco Unified IP IVR または Unified CC が代行受信したコールは、アプリケーションが最終的な宛先に発信者を転送しようとしたときに失敗します。

IVR アプリケーションは、多くの場合、DTMF トーンを使用して IVR メニューのオプションを選択します。別の方法としては音声認識があり、電話機のキーを押す代わりに、発信者が IVR サーバに向かってコマンドを発音します。Cisco Unified IP IVR と Unified CC はどちらも、JTAPI を使用して Unified CM に統合されているため、アウトオブバンド シグナリング メッセージで DTMF トーンを渡します。現在、市販されている多くの H.323 デバイスは、インバンド DTMF トーンを使用しています。このような H.323 クライアントでは、DTMF を使用して IP IVR または Unified CC メニューをナビゲートできません。ただし、これらの H.323 クライアントは、IVR サーバが対応していれば、音声認識を使用できます。Cisco Unified Video Advantage などのビデオ対応デバイス、サードパーティ製の SCCP ビデオ デバイス、および DTMF に H.245 英数字アウトオブバンド シグナリングを使用する H.323 エンドポイントは、DTMF トーンを使用して IVR メニューをナビゲートできます。

Cisco Attendant Console

Cisco Attendant Console は、JTAPI を使用して Unified CM に統合されています。Attendant Console は、着信コールを処理する管理用デバイスとして使用されます。Attendant Console は、特にビデオをサポートしているわけではありませんが、コールが最終的な宛先に転送されると、ビデオ チャネルをネゴシエートできるようになります。ただし、H.323 デバイスを Attendant Console と相互運用するには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Unified CM からの ECS の受信をサポートしていない場合、Attendant Console が代行受信したコールは、コンソール担当者が最終的な宛先に発信者を転送しようとしたときに失敗します。

Cisco IP SoftPhone および Cisco IP Communicator

Cisco IP SoftPhone は、TAPI を使用して Unified CM と統合されており、スタンドアロン ソフトフォンまたは関連付けられている SCCP ハードウェア電話機を制御するソフトウェア インターフェイスとして設定できます。Cisco IP SoftPhone は、特にビデオをサポートしているわけではありませんが、Cisco Unified Video Advantage クライアントが関連付けられている IP Phone と組み合せて使用できます。Cisco IP SoftPhone は、サードパーティ製の SCCP ビデオ デバイスの制御には使用できません。

Cisco IP Communicator は、SCCP クライアントなので Cisco 7970 シリーズ IP Phone のように動作するという点で、IP SoftPhone と異なります。

バージョン 2.0 では、両方のアプリケーションが同じ PC 上に存在する場合、Cisco IP Communicator を Cisco Unified Video Advantage 2.0 に関連付けることができます。詳細については、「Unified Communications エンドポイント」（P.20-1）の章を参照してください。

Cisco IP Communicator 2.1 ではまた、Cisco IP Communicator デバイスを作成または追加する際のデバイス プロトコルとして、SIP を選択できます。

コラボレーション ソリューション

エンドポイント間のビデオ通信を提供するために、次のテクノロジーが使用されることがあります。

T.120 アプリケーション共有

T.120 プロトコルを使用して、ドキュメント、ホワイトボード、およびテキストを会議の参加者で共有するビデオ会議エンドポイントがあります。Unified CM は、T.120 チャネルのネゴシエートをサポートしません。T.120 の代わりに、Cisco MeetingPlace やサードパーティのコラボレーション ソリューションのような Web ベースのコラボレーション ソリューションを使用することをお勧めします。

Cisco Unified MeetingPlace

Cisco Unified MeetingPlace は、ハイエンドな音声およびビデオ会議ソリューションと、会議のスケジューリングおよび参加に使用する Web ベースのフロントエンドを結合します。詳細については、「Cisco Unified MeetingPlace」（P.14-1）の章を参照してください。

無線ネットワーキング ソリューション

ビデオは帯域幅に大きな影響を与えるため、802.11b/g などの共有無線メディアをビデオ エンドポイントに使用することは*お勧めしません*。

ビデオ エンドポイントが、実稼動中の IP Phone と無線帯域幅を共有しないように注意する必要があります。ビデオは帯域幅の大半を消費するため、ビデオ、音声、およびデータを同じ無線メディアでサポートすることは困難です。

Cisco Unified Video Advantage は、関連付けられた物理 IP Phone への物理イーサネット接続に依存します。ユーザが物理イーサネット インターフェイスと、Aironet 802.11b Wireless Adapter の両方を同じ PC にインストールすることはよくあります。このような設定は、無線インターフェイスがネットワークへの優先パスになった場合に、Cisco Unified Video Advantage がこのインターフェイス経由では関連付けられないため、Cisco Unified Video Advantage で問題が発生する原因になります。常に、物理イーサネット インターフェイスを優先パスにすることをお勧めします。また、ユーザが IP Phone の背面の PC ポートに接続するときは、間違って優先されないように Aironet Adapter を無効にするように指示してください。

Cisco Unified IP Phone 7920 および 7921

Cisco Unified Wireless IP Phone 7920 および 7921 は、ビデオをサポートしません。ビデオ エンドポイントからも Cisco Unified Wireless IP Phone にコールを発信できますが、音声のみのコールとしてネゴシエートされます。無線 IP Phone ユーザは、コールの保留、転送、または会議への参加ができます。発信者が H.323 ビデオ エンドポイントの場合、これらの付加サービスを機能させるには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。

XML サービス

現在、特に Cisco Unified Video Advantage クライアント ソリューション、Cisco IP Video Phone 7985、またはサードパーティ製の SCCP ビデオ エンドポイント用に作成された XML アプリケーションはありません。ただし、これらのエンドポイントのうち、少数のサードパーティ製エンドポイント以外は、XML アプリケーションをサポートします。Cisco Unified Video Advantage は Cisco Unified IP Phone を使用するため、これらの電話機モデルでサポートされる XML アプリケーションは Unified Video Advantage でも動作します。

ほとんどのサードパーティ製 SCCP ビデオ エンドポイントは XML をサポートしますが、現在、すべての XML アプリケーションがそれらのエンドポイントで動作するわけではありません。たとえば、Cisco エクステンション モビリティおよび Berbee InformaCast 製品は、現在、サードパーティ製の SCCP エンドポイントで動作しない代表的な 2 つの XML アプリケーションです。これらのアプリケーションをサポートするには、エンドポイントのファームウェア アップグレードと、場合によっては Unified CM Administration の変更が必要になります。

CHAPTER 17

LDAP ディレクトリ統合

ディレクトリ（電話帳）は、多数の読み取りや検索、および随時の書き込みや更新用に最適化される特殊なデータベースです。ディレクトリには、一般に、社員の情報、ユーザ ポリシー、ユーザ特権、グループ メンバシップなど、頻繁に変更されないデータが企業ネットワーク上に保存されます。

ディレクトリは拡張可能です。つまり、ディレクトリに保存された情報のタイプを変更し、拡大することができます。「*ディレクトリ スキーマ*」という語は、保存されている情報のタイプ、そのコンテナ（または属性）、およびユーザやリソースとの関係を定義します。

Lightweight Directory Access Protocol（LDAP）は、ディレクトリに保存されている情報にアクセスし、変更するための標準方式をアプリケーションに提供します。この機能により、企業は、すべてのユーザ情報を、複数のアプリケーションで利用できる単一リポジトリに集中化させることができます。追加、移動、および変更が簡単なので、保守コストも大幅に削減されます。

この章では、Cisco Unified Communication Manager（Unified CM）に基づく Cisco Unified Communications システムを社内 LDAP ディレクトリと統合する場合の、設計上の主な原則について説明しています。この章の構成は、次のとおりです。

- 「ディレクトリ統合とは」（P.17-2）

  ここでは、一般的な企業の IT 部門における社内 LDAP ディレクトリとの統合に関して、さまざまな要件を分析します。

- 「IP テレフォニー エンドポイントのディレクトリ アクセス」（P.17-3）

  ここでは、Cisco Unified Communications エンドポイントのディレクトリ アクセスを有効にする技術的なソリューションについて説明し、そのソリューションに基づく設計上のベスト プラクティスを示します。

- 「Unified CM とのディレクトリ統合」（P.17-5）

  ここでは、LDAP 同期機能や LDAP 認証機能などを含む、Cisco Unified CM でのディレクトリ統合に関して、技術的なソリューションについて説明し、設計上のベスト プラクティスを示します。

この章で説明する考慮事項は、Cisco Unified CM とそれにバンドルされているアプリケーション（Cisco エクステンション モビリティ、Cisco Unified Communications Manager Assistant、WebDialer、Bulk Administration Tool、および Real-Time Monitoring Tool）に適用されます。

Cisco Unity については、次の Web サイトで入手可能な『*Cisco Unity Design Guide*』、および『*Cisco Unity Data and the Directory*』、『*Active Directory Capacity Planning*』、『*Cisco Unity Data Architecture and How Cisco Unity Works*』の各ホワイト ペーパーを参照してください。

http://www.cisco.com

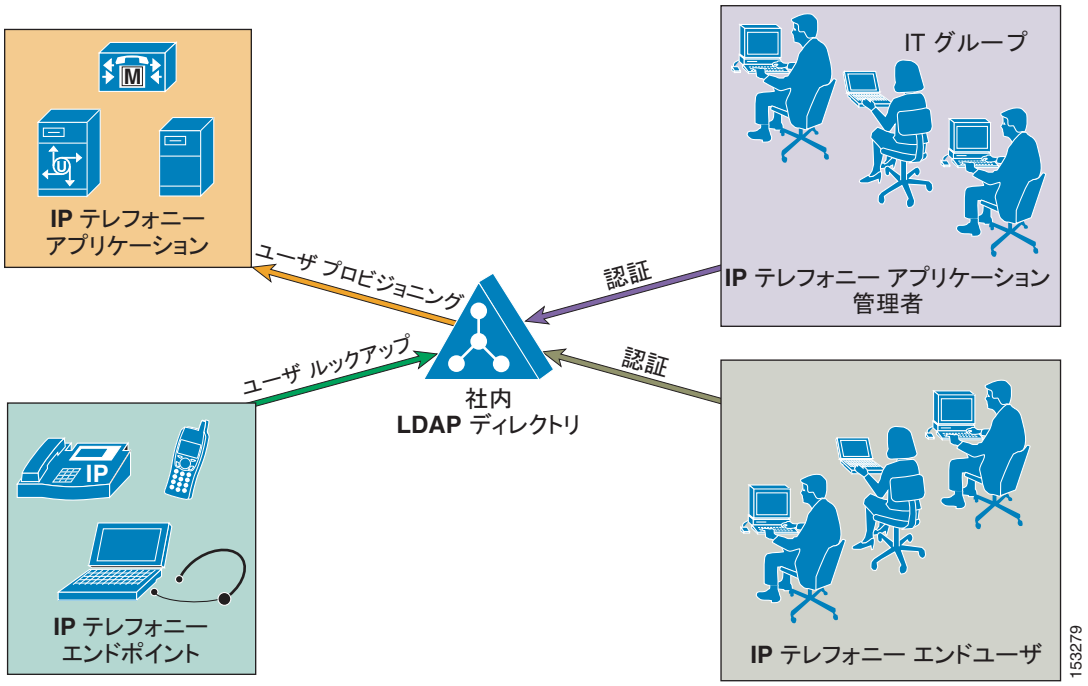
この章の新規情報

この章の項の多くは、読みやすさを高めるために再編成して書き直したものであり、新しい情報も一部追加されています。LDAP ディレクトリと Cisco Unified Communications システムの統合に取り掛かる前に、この章全体を読むことをお勧めします。

ディレクトリ統合とは

音声アプリケーションと社内 LDAP ディレクトリとの統合は、多くの企業の IT 部門にとって一般的な作業です。ただし、統合の正確な範囲は企業によって異なるため、図 17-1 に示すように、1 つ以上の具体的かつ独立した要件として表すことができます。

図 17-1　　ディレクトリ統合のさまざまな要件



たとえば、1 つの一般的な要件は、IP 電話またはその他の音声エンドポイントやビデオ エンドポイントからユーザ ルックアップ（「個人別電話帳」サービスと呼ばれることもあります）を有効にし、ユーザがディレクトリで番号を検索した後に、連絡先に迅速にダイヤルできるようにすることです。

もう 1 つの要件は、社内ディレクトリから音声アプリケーションやビデオ アプリケーションのユーザ データベースを、ユーザに自動的に提供することです。この方法により、社内ディレクトリの変更のたびにコア ユーザ情報を手動で追加、削除、または修正する必要がなくなります。

一般に、社内ディレクトリ クレデンシャルを使用して、音声アプリケーションやビデオ アプリケーションのエンドユーザと管理者を認証することも必要です。ディレクトリ認証を有効にすることで、IT 部門は 1 つのログオン機能を提供し、さまざまな企業アプリケーションに対して各ユーザが保持する必要のあるパスワードの数を減らすことができます。

表 17-1 に示すように、Cisco Unified Communications システムに関係する場合、「*ディレクトリ アクセス*」という用語は、IP テレフォニー エンドポイントのユーザ ルックアップの要件を満たすメカニズムおよびソリューションを意味します。また、「*ディレクトリ統合*」という用語は、ユーザ プロビジョニングおよび（エンド ユーザと管理者の両方の）認証の要件を満たすメカニズムおよびソリューションを意味します。

表 17-1　ディレクトリの要件とシスコのソリューション

要件	シスコのソリューション	Cisco Unified CM の機能
エンドポイントのユーザ ルックアップ	ディレクトリ アクセス	Cisco Unified IP Phone Services SDK
ユーザ プロビジョニング	ディレクトリ統合	LDAP 同期
IP テレフォニー エンド ユーザの認証	ディレクトリ統合	LDAP 認証
IP テレフォニー アプリケーション管理者の認証	ディレクトリ統合	LDAP 認証

この章では、これ以降、Cisco Unified CM に基づく Cisco Unified Communications システムで、これらの要件にどのように対処するかについて説明します。

（注） 「*ディレクトリ統合*」という用語については、管理ポリシーおよびセキュリティ ポリシーを集中化するために、Microsoft Active Directory ドメインにアプリケーション サーバを追加する機能といった解釈もあります。Cisco Unified CM は、カスタマイズした組み込みオペレーティング システムで実行するアプライアンスであり、Microsoft Active Directory ドメインに追加できません。Cisco Unified CM のサーバ管理は、Cisco Real-Time Monitoring Tool（RTMT）によって行われます。アプリケーションに合わせた強力なセキュリティ ポリシーが組み込みオペレーティング システム内にすでに実装されています。

IP テレフォニー エンドポイントのディレクトリ アクセス

この項では、Cisco Unified Communications エンドポイント（Cisco Unified IP Phone など）からユーザ ルックアップを実行するように、LDAP 準拠のディレクトリ サーバへの社内ディレクトリ アクセスを設定する方法について説明します。Unified CM やその他の IP テレフォニー アプリケーションがユーザ プロビジョニングおよび認証のために社内ディレクトリに統合されているかどうかに関係なく、この項で説明しているガイドラインが適用されます。

ディスプレイ画面を持つ Cisco Unified IP Phone では、ユーザが電話機の Directories ボタンを押すと、ユーザ ディレクトリを検索できます。IP Phone は、Hyper-Text Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）を使用して、要求を Web サーバに送信します。Web サーバからの応答には、電話機が解釈して表示する特定の Extensible Markup Language（XML）オブジェクトが含まれています。

デフォルトでは、Cisco Unified IP Phone は、Unified CM の組み込みデータベースに対してユーザ ルックアップを実行するように設定されます。ただし、社内 LDAP ディレクトリでルックアップを実行するように、この設定を変更できます。変更した場合、電話機は HTTP 要求を外部 Web サーバに送信します。このサーバはプロキシとして動作し、要求を LDAP 照会に変換します。そして、その LDAP 照会が社内ディレクトリによって処理されます。LDAP 応答は、Web サーバによって XML オブジェクトにカプセル化され、HTTP を使用して電話機に返信されて、エンド ユーザに伝えられます。

図 17-2 では、Unified CM が社内ディレクトリに統合されていない配置において、このメカニズムを示しています。このシナリオでは、Unified CM がメッセージ交換にかかわっていないことに注意してください。図 17-2 の右側に表示されている Unified CM Web ページの認証メカニズムは、ディレクトリ ルックアップの設定とは関係ありません。

図 17-2　Cisco Unified IP Phone Services SDK を使用する Cisco Unified IP Phone のディレクトリ アクセス

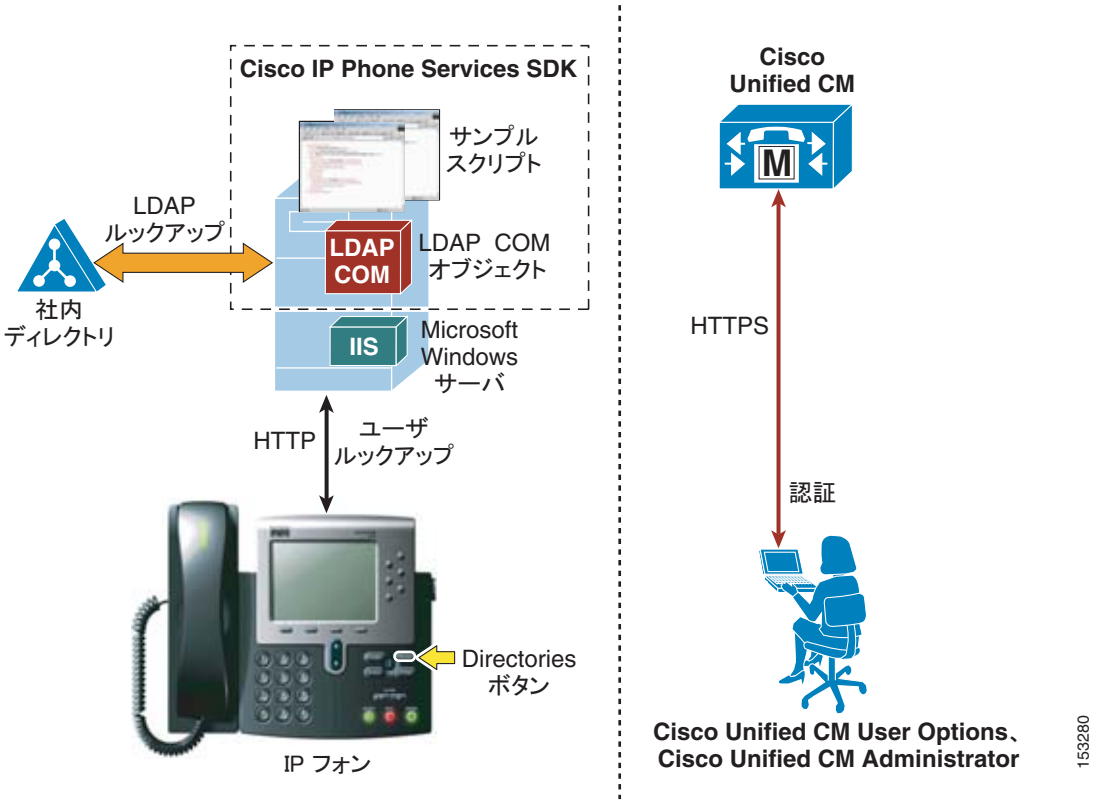


図 17-2 に示す例では、Web サーバのプロキシ機能は、Cisco Unified IP Phone Services Software Development Kit（SDK; ソフトウェア開発キット）バージョン 3.3(4) 以降に組み込まれている Cisco LDAP Search Component Object Model（COM; コンポーネント オブジェクト モデル）サーバによって提供されます。次の Web サイトの Cisco Developer Community から最新の Cisco Unified IP Phone Services SDK をダウンロードできます。

http://developer.cisco.com/web/ipps/home

IP Phone Services SDK は、IIS 4.0 以降を実行する Microsoft Windows Web サーバにはインストールできますが、Unified CM サーバにはインストールできません。SDK には、単純なディレクトリ ルックアップ機能を提供するサンプル スクリプトが入っています。

IP Phone Services SDK を使用する社内ディレクトリ ルックアップ サービスを設定するには、次の手順を実行します。

ステップ 1　社内 LDAP ディレクトリを指すようにサンプル スクリプトのいずれかを修正するか、SDK に付属の『LDAP Search COM Programming Guide』を使用して独自のスクリプトを作成します。

ステップ 2　Unified CM で、外部 Web サーバ上のスクリプトの URL を指すように URL Directories パラメータ（[System] > [Enterprise Parameters]）を設定します。

ステップ 3　変更を有効にするために電話機をリセットします。

（注）　ユーザのサブセットだけにサービスを提供する場合は、Enterprise Parameters ページではなく、Phone Configuration ページ内で URL Directories パラメータを直接設定します。

まとめると、Cisco Unified IP Phone Services SDK によるディレクトリ アクセスには、次の設計上の考慮事項が適用されます。

- ユーザ ルックアップは、LDAP 準拠の社内ディレクトリに対してサポートされる。
- Microsoft Active Directory に照会する場合、スクリプトがグローバル カタログ サーバを指すようにし、スクリプト設定でポート 3268 を指定することにより、グローバル カタログに対してルックアップを実行できる。この方法では、通常はルックアップが高速化します。グローバル カタログに記載されているユーザの属性がすべてではないことに注意してください。詳細については、Microsoft Active Directory のマニュアルを参照してください。
- この機能が有効であっても Unified CM に影響はなく、LDAP ディレクトリ サーバに最小限の影響しか及ばない。
- SDK に付属のサンプル スクリプトでは、最小限のカスタマイズだけが可能である（たとえば、返送されたすべての番号の前に番号ストリングを付けられる）。もっと高度な操作のためには、カスタム スクリプトを作成する必要があり、スクリプトの作成に役立つプログラミング ガイドが SDK に付属しています。
- この機能は、社内ディレクトリに対する Unified CM ユーザのプロビジョニングまたは認証を必要としない。

Unified CM とのディレクトリ統合

この項では、社内 LDAP ディレクトリに対するユーザ プロビジョニングと認証を考慮した、Cisco Unified CM でのディレクトリ統合のメカニズムおよびベスト プラクティスについて説明します。この項では、次のトピックについて取り上げます。

- 「Cisco Unified Communications Directory のアーキテクチャ」（P.17-7）

  ここでは、Unified CM 7.*x* ユーザ関連アーキテクチャの概要を示します。

- 「LDAP 同期」（P.17-10）

  ここでは、LDAP 同期の機能について説明し、この機能の配置に関する設計上のガイドラインを Microsoft Active Directory に関する追加の考慮事項と共に示します。

- 「LDAP 認証」（P.17-18）

  ここでは、LDAP 認証の機能について説明し、この機能の配置に関する設計上のガイドラインを Microsoft Active Directory に関する追加の考慮事項と共に示します。

表 17-2 に、Cisco Unified Communication Manager での同期と認証用に現在サポートされている LDAP ディレクトリを示します。

表 17-2　LDAP ディレクトリのサポート

LDAP ディレクトリのタイプ	Cisco Unified CM 5.*x*	Cisco Unified CM 6.*x*	Cisco Unified CM 7.*x*
Microsoft AD 2000 Microsoft AD 2003 Microsoft AD 2008 Microsoft ADAM 2003 Microsoft LDS 2008	あり	あり	あり Microsoft ADAM および LDS には、Cisco Unified CM 7.1(3) 以降のリリースが必要です。
Netscape 4.x	あり	あり	サポート終了[1]
iPlanet 5.0	あり	あり	サポート終了[1]
iPlanet 5.1 SunOne 5.2	あり	あり	あり
SunOne 6.x	なし	あり	あり
OpenLDAP 2.3.39 OpenLDAP 2.4	なし	なし	あり[2]

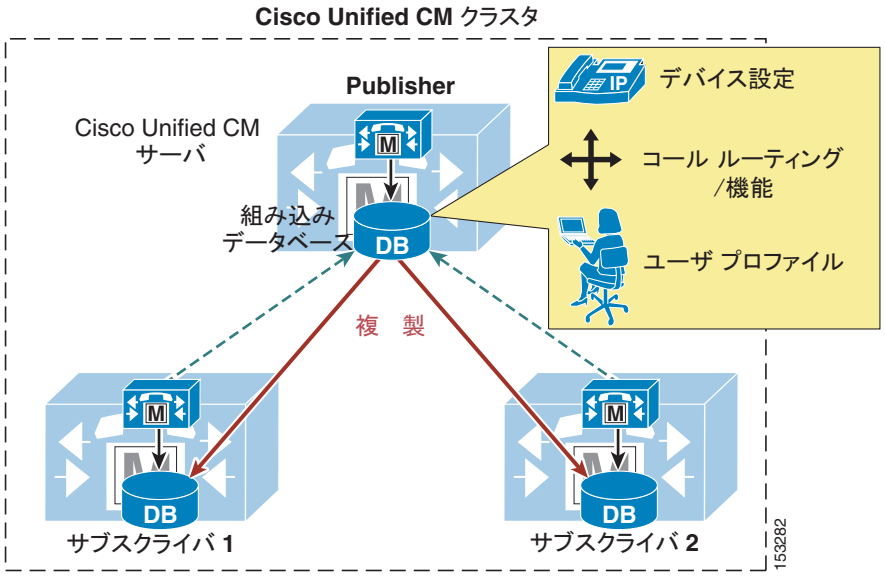
1. ディレクトリ ベンダーによると、このソリューションは販売終了になりました。
2. このディレクトリ タイプは、Cisco Unified CM 7.1(2) 以降のリリースだけでサポートされています。

（注）　表 17-2 に示されているすべての Microsoft Directory 製品には、Cisco Unified CM による同等のサポートがあります。この文書内の AD の参照はすべて、この表内のすべての Microsoft 製品に適用できます。

Cisco Unified Communications Directory のアーキテクチャ

図 17-3 は、Unified CM クラスタの基本アーキテクチャを示しています。組み込みデータベースには、デバイス関連データ、コール ルーティング、機能のプロビジョニング、およびユーザ プロファイルなど、すべての設定情報が保存されます。データベースは CM クラスタ内のすべてのサーバ上に存在し、パブリッシャ サーバからすべてのサブスクライバ サーバに自動的に複製されます。

図 17-3　Cisco Unified CM のアーキテクチャ



デフォルトでは、Unified CM Administration Web インターフェイスを介してすべてのユーザを手動でパブリッシャ データベースにプロビジョニングします。Cisco Unified CM には、次の 2 つのユーザ タイプがあります。

- エンド ユーザ：実在の人間でかつ対話形式のログインに関連付けられているすべてのユーザ。このカテゴリには、すべての IP テレフォニー ユーザの他、User Groups and Roles 設定（以前のバージョンの Unified CM にある Cisco Multilevel Administration 機能に相当）を使用する場合の Unified CM 管理者も含まれます。
- アプリケーション ユーザ：Cisco Unified Communications の他の機能またはアプリケーション（Cisco Attendant Console、Cisco Unified Contact Center Express、Cisco Unified Communication Manager Assistant など）に関連付けられているすべてのユーザ。これらのアプリケーションは Unified CM に対して認証する必要がありますが、この内部「ユーザ」は対話形式のログインを行わず、単にアプリケーション間の内部通信だけを処理します。

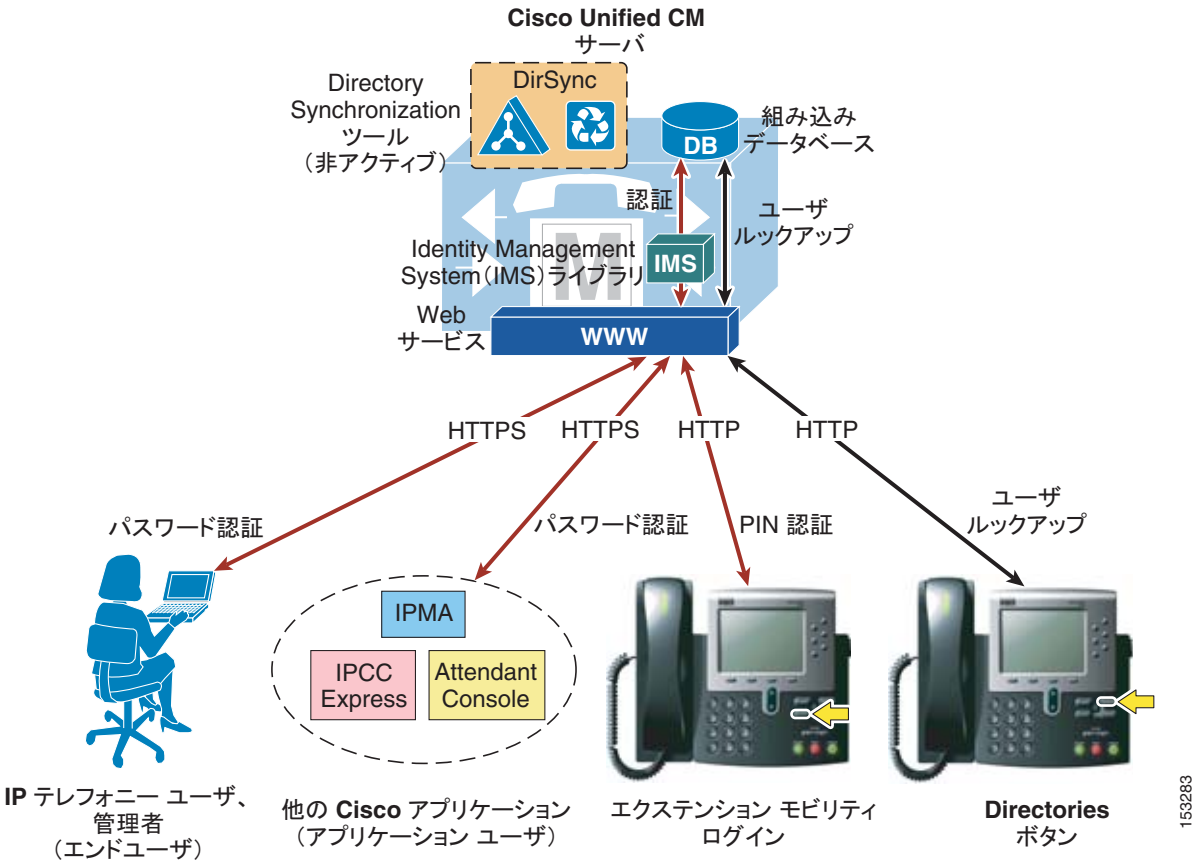
表 17-3 では、Unified CM データベースにデフォルトで作成されるアプリケーション ユーザのリストを、それらのユーザが使用される機能またはアプリケーションと共に示しています。Cisco Unified Communications の他のアプリケーションを統合する場合に、追加のアプリケーション ユーザを手動で作成できます（たとえば、Cisco Attendant Console の **ac** アプリケーション ユーザ、Cisco Unified Contact Center Express の **jtapi** アプリケーション ユーザなど）。

表 17-3　Unified CM のデフォルトのアプリケーション ユーザ

アプリケーション ユーザ	使用される機能またはアプリケーション
CCMAdministrator	Unified CM Administration（デフォルトは「スーパー ユーザ」）
CCMQRTSecureSysUser	Cisco Quality Reporting Tool
CCMQRTSysUser	
CCMSysUser	シスコ エクステンション モビリティ
IPMASecureSysUser	Cisco Unified Communications Manager Assistant
IPMASysUser	
WDSecureSysUser	Cisco WebDialer
WDSysUser	

これらの考慮事項に基づいて、図 17-4 に、ルックアップ、プロビジョニング、認証などのユーザ関連操作に対する Unified CM でのデフォルト動作を示します。

図 17-4　Unified CM のユーザ関連操作に対するデフォルト動作



エンド ユーザは、HTTPS 経由で Unified CM User Options ページにアクセスし、ユーザ名およびパスワードで認証します。ユーザ グループと役割によって管理者として設定されている場合、エンド ユーザは同じクレデンシャルで Unified CM Administration のページにもアクセスできます。

同様に、シスコの他の機能とアプリケーションは、それぞれのアプリケーション ユーザに関連付けられたユーザ名およびパスワードで、HTTPS 経由で Unified CM に対して認証します。

HTTPS メッセージによって伝送される認証確認は、Unified CM の Web サービスにより、Identity Management System（IMS）という内部ライブラリにリレーされます。デフォルト設定では、IMS ライブラリは、組み込みデータベースに対してエンド ユーザとアプリケーション ユーザの両方を認証します。このように、IP 通信システムにおける「現実の」ユーザと内部アプリケーション アカウントの両方が、Unified CM に設定されたクレデンシャルを使用して認証されます。

エンド ユーザは、IP Phone からエクステンション モビリティ サービスにログインするときに、ユーザ名と数値パスワード（PIN）で認証することもできます。この場合、認証確認は HTTP 経由で Unified CM に伝送されますが、やはり Web サービスにより IMS ライブラリにリレーされ、IMS ライブラリは組み込みデータベースに対してクレデンシャルを認証します。

さらに、Directories ボタンを介して IP テレフォニー エンドポイントによって実行されるユーザ ルックアップでは、HTTP 経由で Unified CM の Web サービスと通信し、組み込みデータベースのデータにアクセスします。

エンド ユーザとアプリケーション ユーザの区別の重要性は、社内ディレクトリとの統合が必要な場合に明らかになります。前の項で説明したように、この統合は次の 2 つの独立したプロセスによって実現されます。

- LDAP 同期

  このプロセスでは、Unified CM の Cisco Directory Synchronization（DirSync）という内部ツールを使用して、社内 LDAP ディレクトリから多数のユーザ属性を（手動または定期的に）同期します。この機能を有効にすると、ユーザは社内ディレクトリから自動的にプロビジョニングされます。この機能はエンド ユーザだけに適用され、アプリケーション ユーザは独立したままで、引き続き Unified CM Administration インターフェイスを介してプロビジョニングされます。要約すると、エンド ユーザは社内ディレクトリで定義され、Unified CM データベースに同期されますが、アプリケーション ユーザは Cisco Unified CM データベースに保存されるだけで、社内ディレクトリで定義する必要はありません。

- LDAP 認証

  このプロセスは、LDAP の標準的なシンプルバインド操作を使用して、IMS ライブラリによる社内 LDAP ディレクトリに対するユーザ クレデンシャルの認証を可能にします。この機能を有効にすると、エンド ユーザ パスワードは社内ディレクトリに対して認証されますが、アプリケーション ユーザ パスワードは引き続きローカルで Unified CM データベースに対して認証されます。Cisco エクステンション モビリティの PIN も引き続きローカルで認証されます。

Unified CM データベースに対して内部でアプリケーション ユーザを維持および認証すると、社内 LDAP ディレクトリの可用性とは無関係に、これらのアカウントを使用して Unified CM と通信するすべてのアプリケーションと機能に対して復元性が提供されます。

Cisco エクステンション モビリティの PIN も Unified CM データベース内で維持されます。これは、これらの PIN はリアルタイム アプリケーションの必須部分であり、リアルタイム アプリケーションは社内ディレクトリの応答性に依存しないようにする必要があるためです。

次の 2 つの項では、LDAP 同期と LDAP 認証についてさらに詳しく説明し、両方の機能に関して設計上のベスト プラクティスを示します。

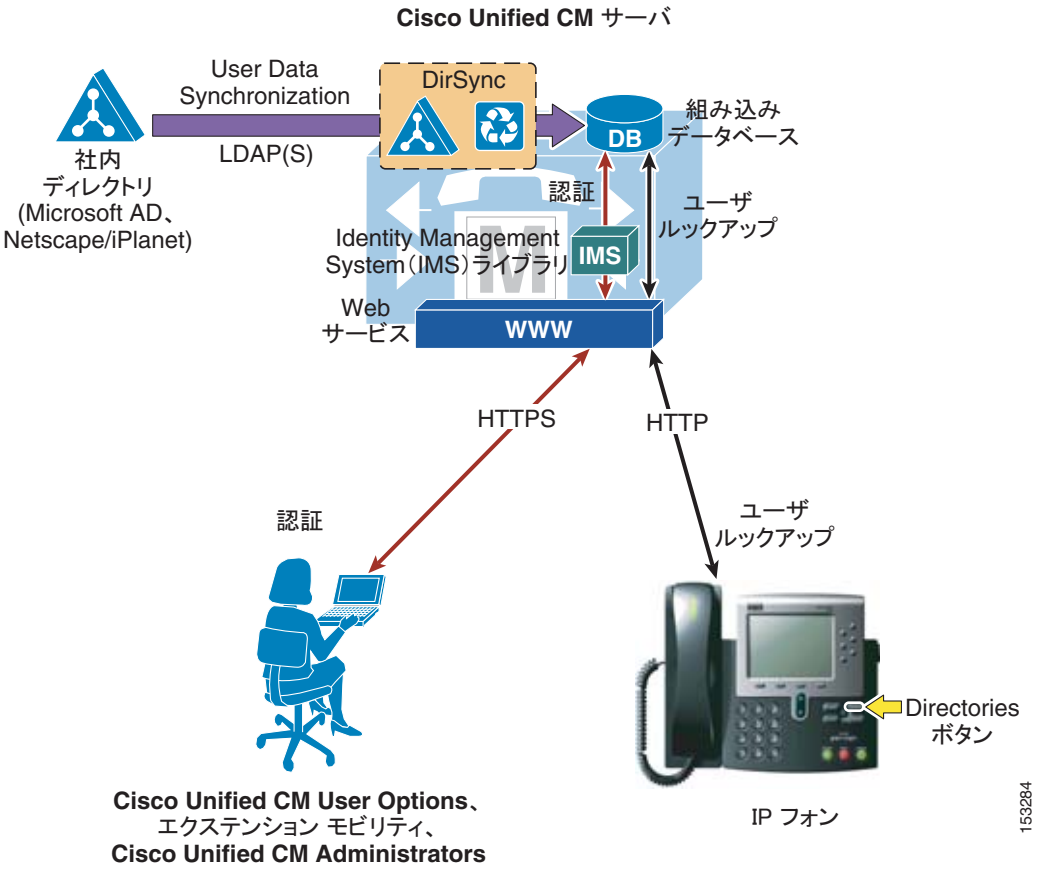
（注）　「IP テレフォニー エンドポイントのディレクトリ アクセス」（P.17-3）の項で説明したように、外部 Web サーバで Cisco Unified IP Phone Services SDK を設定することにより、エンドポイントからのユーザ ルックアップを社内ディレクトリに対して実行することもできます。

LDAP 同期

Unified CM を社内 LDAP ディレクトリに同期すると、管理者は Unified CM データ フィールドをディレクトリ属性にマッピングすることにより、ユーザを容易にプロビジョニングできるようになります。LDAP ストアに保持されている重要なユーザ データは、スケジュールまたはオンデマンド ベースで Unified CM データベース内の対応する適切なフィールドにコピーされます。社内 LDAP ディレクトリのステータスは、中央リポジトリのままとなります。Unified CM は、ユーザ データを保存するための統合データベースを備え、またユーザ アカウントおよびデータを作成して管理するための Web インターフェイスを、Unified CM Administration 内に備えています。LDAP 同期を有効にすると、ローカル データベースは引き続き使用されますが、エンドユーザ アカウントを作成する Unified CM ファシリティが無効になります。その後、エンドユーザ アカウントの管理は、LDAP ディレクトリのインターフェイスを介して実施されます（図 17-5 を参照）。アプリケーション ユーザのアカウントは引き続き、Unified CM Administration Web インターフェイスを使用して作成し、管理できます。

ユーザ アカウント情報は、LDAP ディレクトリから Unified CM パブリッシャ サーバにあるデータベースにインポートされます。LDAP ディレクトリからインポートされた情報は、Unified CM から変更できません。Cisco Unified Communications に固有の追加のユーザ情報は、Unified CM によって管理され、ローカル データベースだけに保存されます。たとえば、デバイスとユーザのアソシエーション、短縮ダイヤル、自動転送設定、およびユーザ PIN はすべて Unified CM が管理するデータの例であり、社内 LDAP ディレクトリには存在しません。次に、ユーザ データは組み込みデータベース同期メカニズムによって、Unified CM パブリッシャ サーバからサブスクライバ サーバに伝達されます。

図 17-5　　ユーザ データ同期の有効化



LDAP 同期をアクティブにすると、一度に 1 つのタイプの LDAP ディレクトリだけをクラスタ用にグローバルに選択できます。また、LDAP ディレクトリ ユーザの 1 つの属性が選択されて [Unified CM User ID] フィールドにマッピングされます。Unified CM はデータへのアクセスに標準 LDAPv3 を使用します。

Cisco Unified CM は、標準属性からデータをインポートします。ディレクトリ スキーマの拡大は必要ありません。表 17-4 に、Unified CM の各フィールドへのマッピングに使用できる属性を示します。[Unified CM User ID] フィールドにマッピングされるディレクトリ属性のデータは、そのクラスタのすべてのエントリ内で固有のものである必要があります。[Cisco UserID] フィールドにマッピングされる属性はディレクトリに格納される必要があり、**sn** 属性はデータと一緒に格納される必要があります。そうしないと、このインポート処理時にこれらのレコードはスキップされます。エンド ユーザ アカウントのインポート中に使用するプライマリ属性が Unified CM データベースのいずれかのアプリケーション ユーザと一致する場合、そのエンド ユーザはスキップされます。

表 17-4 では、LDAP ディレクトリから対応する Unified CM ユーザ フィールドにインポートされた属性を示していて、またこれらのフィールド間のマッピングについて説明しています。Unified CM ユーザ フィールドの中には、複数の LDAP 属性の 1 つからマッピングされるものもあります。

表 17-4　同期化された LDAP 属性と対応する Unified CM フィールド名

Unified CM のユーザ フィールド	Microsoft Active Directory	Netscape、iPlanet、または Sun ONE	OpenLDAP[1]
User ID	*次のいずれか* sAMAccountName mail employeeNumber telephoneNumber userPrincipalName	*次のいずれか* uid mail employeeNumber telephonePhone	*次のいずれか* uid mail employeeNumber telephonePhone
First Name	givenName	givenname	givenname
Middle Name	*次のいずれか* middleName initials	initials	initials
Last Name	sn	sn	sn
Manager ID	manager	manager	manager
Department	department	departmentnumber	departmentnumber
Phone Number	次のいずれか telephoneNumber ipPhone	telephonenumber	telephonenumber
Mail ID	*次のいずれか* mail sAMAccountName	*次のいずれか* mail uid	*次のいずれか* mail uid

1. このディレクトリ タイプは、Cisco Unified CM 7.1(2) 以降のリリースだけでサポートされています。

表 17-5 に、Dirsynch プロセスによってインポートされ、Unified CM データベースにコピーされるが、管理者ユーザの設定 Web ページには表示されない追加属性のリストを示します。Microsoft OCS を使用する場合、属性 msRTCSIP-PrimaryUserAddress は AD に格納されます。この表は、完全な情報を提供する目的で記載されています。

表 17-5　表示されない同期化 LDAP 属性

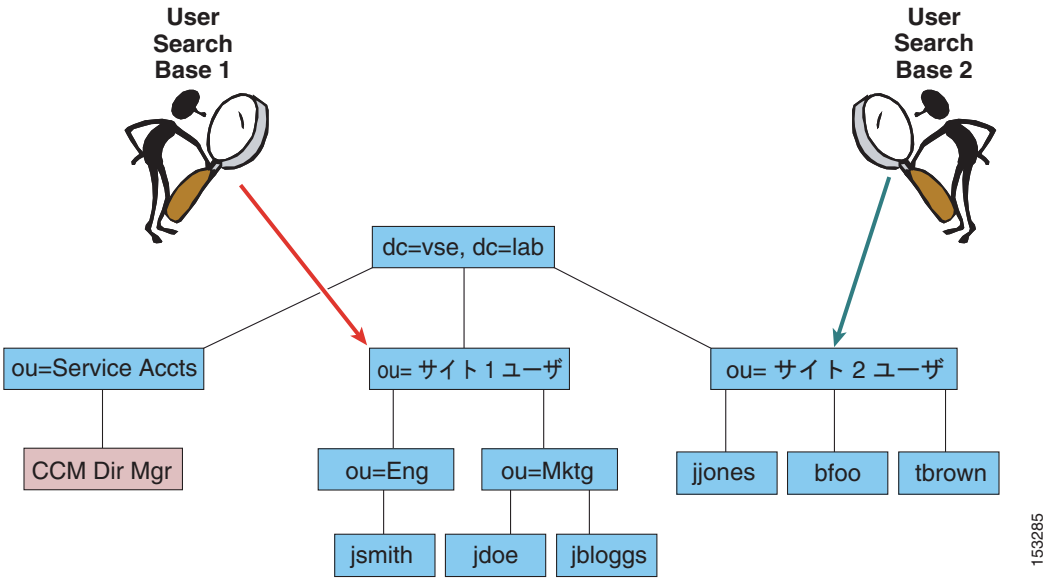
Unified CM のユーザ フィールド	Microsoft Active Directory	Netscape、iPlanet、または Sun ONE	OpenLDAP[1]
objectGUID	objectGUID	適用されない	適用されない
OCSPrimaryUserAddress	msRTCSIP-PrimaryUserAddress 1	適用されない	適用されない
Title	title	Title	title
Home Phone Number	homePhone	Homephone	hometelephonenumber
Mobile Phone Number	mobile	Mobile	Mobiletelephonenumber
Pager Number	pager	Pager	pagertelephonenumber

1.　このディレクトリ タイプは、Cisco Unified CM 7.1(2) 以降のリリースだけでサポートされています。

同期は、Serviceability Web ページで有効にする Cisco DirSync というプロセスによって実行されます。このプロセスを有効にすることで、システムに 1 ～ 5 つの同期アグリーメントを設定できます。アグリーメントでは、LDAP ツリー内で Unified CM がインポートするユーザ アカウントの検索を開始する場所となる検索ベースを指定します。Unified CM は、特定の同期アグリーメントについて検索ベースで指定したドメインの領域に存在するユーザだけをインポートできます。

図 17-6 は、2 つの同期アグリーメントを示しています。一方の同期アグリーメントでは、User Search Base 1 を指定し、ユーザ jsmith、jdoe、jbloggs をインポートします。もう一方の同期アグリーメントでは、User Search Base 2 を指定し、ユーザ jjones、bfoo、tbrown をインポートします。CCMDirMgr アカウントは、ユーザ検索ベースで指定した場所の下位に存在しないので、インポートされません。ユーザを LDAP ディレクトリの構造に編成すると、その構造を使用して、どのユーザ グループをインポートするかを制御できます。この例では、単一の同期アグリーメントを使用してドメインのルートを指定することもできましたが、その検索ベースでは Service Accts もインポートしていたと考えられます。検索ベースではドメイン ルートを指定する必要はなく、ツリーのどの場所でも指定できます。

図 17-6　ユーザ検索ベース



データを Unified CM データベースにインポートするために、LDAP Manager Distinguished Name として設定で指定されたアカウントを使用して、システムが LDAP ディレクトリへのバインドを実行し、データベースの読み取りがこのアカウントで実行されます。Unified CM のログインのために、LDAP

ディレクトリでアカウントが使用可能である必要があります。ユーザ検索ベースで指定したサブツリー内のすべてのユーザ オブジェクトの読み取り可能な権限を持つ、固有のアカウントを作成することをお勧めします。同期アグリーメントでは、そのアカウントがドメイン内の任意の場所に存在できるように、アカウントの完全認定者名を指定します。図 17-6 の例では、CCMDirMgr が同期に使用するアカウントです。

アカウントのインポートは、LDAP Manager Distinguished Name アカウントの権限を使用して制御できます。この例では、ou=Eng への読み取りアクセスはできるが ou=Mktg への読み取りアクセスはできないようにこのアカウントを制限した場合、Eng の下位にあるアカウントだけがインポートされます。

同期アグリーメントには、複数のディレクトリ サーバを指定して冗長性を実現する機能があります。同期の試行時に使用するディレクトリ サーバを 3 つまで、順序付きのリストにして設定に指定できます。これらのサーバでの試行が、リストの最後まで順に行われます。どのディレクトリ サーバも応答しない場合、同期には失敗しますが、設定済みの同期スケジュールに従って再試行されます。

同期のメカニズム

同期アグリーメントでは、同期を開始する時刻を指定し、再同期の期間を時間、日、週、月のいずれかの単位（最小値は 6 時間）で指定します。同期アグリーメントは、特定の時刻に 1 回だけ実行するように設定することもできます。

Unified CM パブリッシャ サーバで同期を初めて有効にすると、社内ディレクトリに存在するユーザ アカウントが Unified CM データベースにインポートされます。そして、その後のプロセスに従って、既存の Unified CM エンドユーザ アカウントがアクティブになってデータが更新されるか、新しいエンドユーザ アカウントが作成されます。

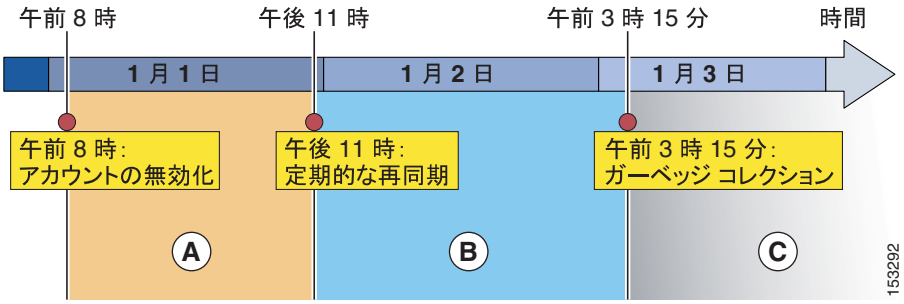
1. エンドユーザ アカウントがすでに Unified CM データベースに存在するときに同期アグリーメントを設定した場合、Unified CM ですべての既存のアカウントは非アクティブとマークされます。同期アグリーメントの設定で、Unified CM UserID への LDAP データベース属性のマッピングを指定します。同期中に LDAP データベースのアカウントが既存の Unified CM アカウントと一致すると、その Unified CM アカウントは再びアクティブとマークされます。
2. 同期の完了後、アクティブに設定されなかったアカウントは、ガーベッジ コレクション プロセスの実行時に Unified CM から永続的に削除されます。ガーベッジ コレクションは、午前 3 時 15 分の定時に自動的に実行されるプロセスで、設定はできません。Unified CM は同期が設定されている間はアカウントを管理できないので、LDAP ディレクトリ アカウントと一致しない Unified CM アカウントの削除が必要です。
3. 後で社内ディレクトリに変更を加えると、スケジューリングされた次回の同期期間に、完全な再同期として Microsoft Active Directory から同期が行われます。これに対して、iPlanet および Sun ONE の各ディレクトリ製品は、ディレクトリに変更が加えられると差分同期を実行します。次の項では、2 つのシナリオのそれぞれの例を示します。

（注）　ユーザを LDAP から Unified CM データベースに同期した後で同期設定を削除すると、その設定によってインポートされたユーザには、データベース内で非アクティブのマークが付きます。その後、これらのユーザはガーベッジ コレクションによって削除されます。

Active Directory でのアカウント同期

図 17-7 は、LDAP 同期と LDAP 認証の両方を有効にした Unified CM 配置について、イベントのスケジュールの例を示しています。再同期は、毎日午後 11 時に設定されています。

図 17-7　Active Directory での変更の伝達



最初の同期の後、アカウントの作成、削除、または無効化は、図 17-7 に示すスケジュールに従って、次の手順で説明するように Unified CM に伝達されます。

1. 1 月 1 日の午前 8 時に、AD でアカウントを無効にするか削除します。これ以降、期間 A 中は、Unified CM が認証を AD にリダイレクトするため、このユーザのパスワード認証（たとえば、Unified CM User Options ページ）は失敗します。ただし、PIN は Unified CM データベースに保存されているため、PIN 認証（たとえば、エクステンション モビリティ ログイン）は今までどおり成功します。
2. 定期的な再同期が 1 月 1 日 午後 11 時にスケジュールされています。このプロセス中に、Unified CM がすべてのアカウントを検証します。AD で無効にするか削除したアカウントは、この時点で Unified CM データベースでは非アクティブとしてタグ付けされます。1 月 1 日の午後 11 時より後に、アカウントが非アクティブとマークされると、Unified CM による PIN 認証とパスワード認証は両方とも失敗します。
3. アカウントのガーベッジ コレクションは毎日午前 3 時 15 分の定時に発生します。このプロセスは、24 時間以上非アクティブとマークされたレコードの Unified CM データベースからユーザ情報を永続的に削除します。この例では、1 月 2 日の午前 3 時 15 分に実行するガーベッジ コレクションでは、アカウントが非アクティブになってまだ 24 時間が経過していないので、アカウントを削除しません。したがって、アカウントは 1 月 3 日の午前 3 時 15 分に削除されます。この時点で、ユーザ データは Unified CM から永続的に削除されます。

期間 A の開始時にアカウントを AD で作成していた場合、そのアカウントは期間 B の開始時に実行される定期的な再同期で Unified CM にインポートされ、Unified CM ですぐにアクティブになります。

iPlanet または Sun ONE でのアカウント同期

iPlanet および Sun ONE 製品は差分同期アグリーメントをサポートし、Microsoft Active Directory とは異なる同期スケジュールを使用します。同期には、Internet Engineering Task Force（IETF）ドラフトで定義され、多くの LDAP 実装でサポートされている永続検索メカニズムが使用されます。図 17-8 では、LDAP 同期と LDAP 認証の両方を有効にした Unified CM 配置について、この同期スケジュールの例を示しています。

図 17-8　　iPlanet および Sun ONE での変更の伝達

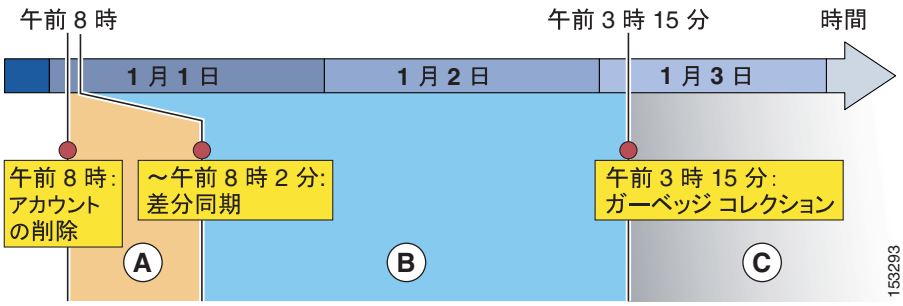


図 17-8 の例は、次の手順から構成されます。

1. 1 月 1 日の午前 8 時にアカウントが社内ディレクトリから削除され、これにより、差分更新データが LDAP サーバから Unified CM に送信されます。Unified CM は、データに対応するコピーを非アクティブに設定します。LDAP 認証が設定されているので、LDAP サーバがレコードを削除するとすぐに、ユーザはパスワードによるログインができなくなります。また、Unified CM レコードが非アクティブとマークされると、PIN をログインに使用できません。
2. 期間 B 中は、ユーザのレコードは非アクティブですが、まだ Unified CM に存在します。
3. 1 月 2 日の午前 3 時 15 分にガーベッジ コレクションが実行されるときは、レコードが非アクティブになってまだ 24 時間が経過していません。データは 1 月 3 日の期間 C の開始時まで Unified CM データベースに残り、ガーベッジ コレクション プロセスがこの日の午前 3 時 15 分に再び実行され、レコードが 24 時間以上にわたって非アクティブであったことを確認します。その結果、レコードはデータベースから永続的に削除されます。

ディレクトリで新規に作成したアカウントは、差分更新データによって同様に Unified CM に同期し、差分更新データが受信されるとすぐに使用できます。

セキュリティの考慮事項

アカウントのインポート中は、LDAP ディレクトリから Unified CM データベースに、パスワードも PIN もコピーされません。Unified CM で LDAP 同期が有効でない場合、エンド ユーザのパスワードは Unified CM Administration を使用して管理されます。パスワードと PIN は、暗号化形式で Unified CM データベースに保存されます。PIN は常に Unified CM で管理されます。LDAP ディレクトリ パスワードを使用してエンド ユーザを認証する場合は、「LDAP 認証」（P.17-18）の項を参照してください。

Unified CM および LDAP サーバで Secure LDAP（SLDAP）を有効にすることにより、Unified CM パブリッシャ サーバとディレクトリ サーバ間の接続を保護できます。Secure LDAP を使用すると、Secure Socket Layer（SSL）接続で LDAP 送信ができます。Unified CM Platform Administration 内で SSL 証明書をアップロードすることにより、Secure LDAP を有効にできます。詳細な手順については、http://www.cisco.com で入手可能な Unified CM の製品マニュアルを参照してください。SLDAP を有効にする方法については、LDAP ディレクトリ ベンダーのドキュメンテーションを参照してください。

LDAP 同期のベスト プラクティス

Cisco Unified CM で LDAP 同期を配置する場合は、設計と実装に関する次のベスト プラクティスに従ってください。

- 社内ディレクトリ内で特定のアカウントを使用し、Unified CM 同期アグリーメントがそのディレクトリに対して接続および認証できるようにする。目的の検索ベース内にあるすべてのユーザ オブジェクトを最低限の「読み取り」権限を 設定し、期限切れにならないようにパスワードを設定した状態で、Unified CM 専用のアカウントを使用することをお勧めします。ディレクトリ内のこのアカウントのパスワードは、Unified CM 内のアカウントのパスワード設定と同期し続ける必要があります。サービス アカウントのパスワードがディレクトリ内で変更された場合は、必ず Unified CM でアカウント設定をアップデートしてください。
- 所定のクラスタにあるすべての同期アグリーメントは、同じ LDAP サーバ ファミリ（Microsoft AD、iPlanet、または Sun ONE）と統合する必要がある。
- 複数のアグリーメントが同時に同じ LDAP サーバに照会することがないように、同期アグリーメントのスケジューリングに時間差を設ける。待機期間中（オフピーク時間）の同期時刻を選択します。
- ユーザ データのセキュリティが必要である場合、Unified CM Administration の [LDAP Directory] 設定ページで [Use SSL] フィールドのチェックボックスをオンにして、Secure LDAP（SLDAP）を有効にする。
- Unified CM UserID フィールドへのマッピングのために選択した LDAP ディレクトリ属性が、そのクラスタのすべての同期アグリーメント内で固有であることを確認する。
- UserID として選択した属性は、Unified CM で定義したアプリケーション ユーザのいずれかの属性と同じであってはならない。
- 同期前の Unified CM データベースにある既存のアカウントは、LDAP ディレクトリからインポートされたアカウントの属性に一致する場合だけ維持される。Unified CM UserID に一致する属性は、同期アグリーメントによって確認されます。
- 冗長性が得られるように、2 台以上の LDAP サーバを設定する。ホスト名の代わりに IP アドレスを使用すると、Domain Name System（DNS; ドメイン ネーム システム）の可用性に依存しなくなります。
- エンドユーザ アカウントは LDAP ディレクトリの管理ツールによって管理し、これらのアカウントのシスコ固有データは Unified CM Administration Web ページによって管理する。
- AD の配置については、ObjectGUID がユーザの主要属性として Unified CM で内部的に使用される。[Unified CM User ID] に対応する AD 内の属性は、AD 内で変更できます。たとえば、sAMAccountname を使用している場合、ユーザは自分の sAMAccountname を AD で変更することができ、Unified CM 内で対応するユーザ レコードは更新されます。

  その他すべての LDAP プラットフォームでは、User ID にマッピングされる属性が Unified CM におけるそのアカウントの主要属性となります。LDAP 内の属性を変更すると、Unified CM に新しいユーザが作成され、元のユーザには非アクティブのマークが付きます。

Microsoft Active Directory に関する追加の考慮事項

ドメインの同期アグリーメントでは、ドメイン外のユーザや子ドメイン内のユーザは同期されません。同期プロセス中は Unified CM が AD 照会に従わないためです。図 17-9 の例では、すべてのユーザをインポートするために 3 つの同期アグリーメントが必要です。Search Base 1 ではツリーのルートを指定しますが、子ドメインのいずれかに存在するユーザはインポートしません。範囲は VSE.LAB に限定されており、残りの 2 つのドメインに対し、そのユーザをインポートするように別々のアグリーメントが設定されています。

図 17-9　複数の Active Directory ドメインでの同期

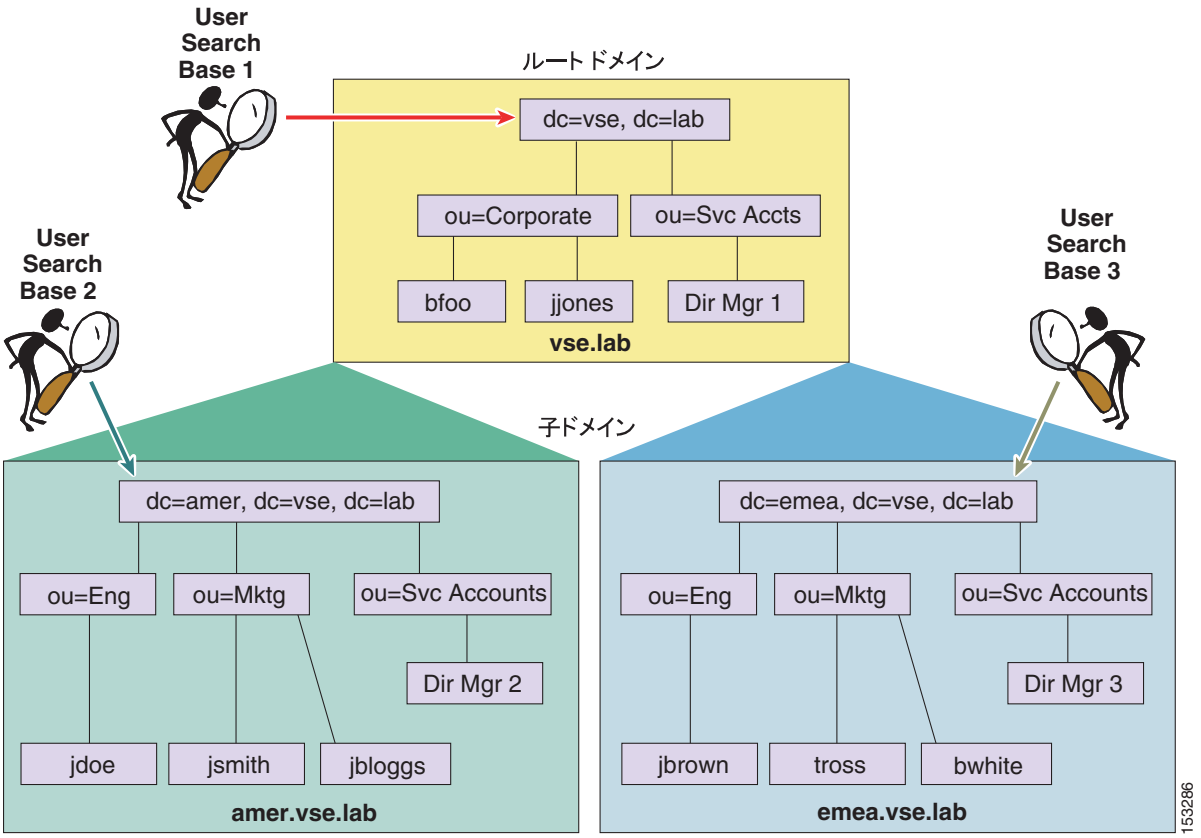
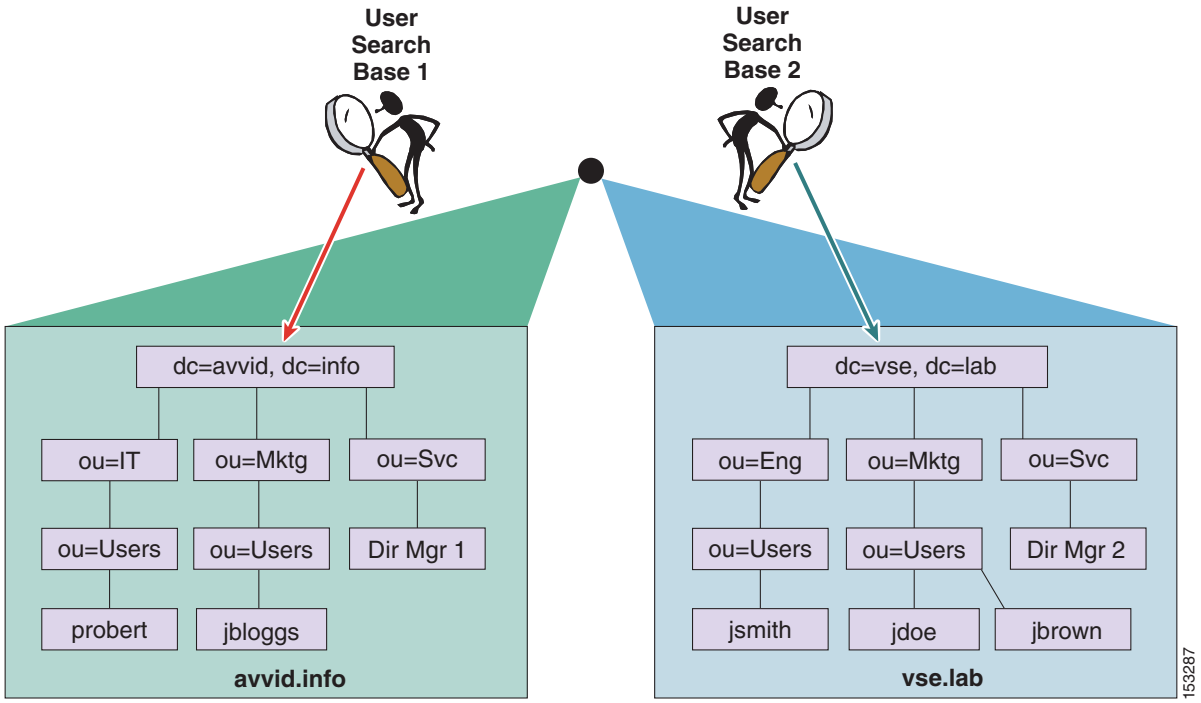


図 17-9 では、ドメインとサブドメインのそれぞれに少なくとも 1 つの Domain Controller（DC; ドメイン コントローラ）が関連付けられ、3 つの同期アグリーメントはそれぞれ適切なドメイン コントローラを指定します。DC にある情報は、その DC が存在するドメイン内のユーザの情報だけなので、すべてのユーザをインポートするために 3 つの同期アグリーメントが必要です。

図 17-10 に示すように、複数のツリーを含む AD フォレストで同期を有効にした場合も、上記と同じ理由で複数の同期アグリーメントが必要です。さらに、UserPrincipalName（UPN）属性がフォレスト全体で固有であることが Active Directory によって保証され、この属性は Unified CM UserID にマッピングする属性として選択する必要があります。マルチツリーの AD シナリオで UPN 属性を使用する場合の追加の考慮事項については、「Microsoft Active Directory に関する追加の考慮事項」（P.17-22）の項を参照してください。

図 17-10　複数の AD ツリー（不連続なネームスペース）での同期

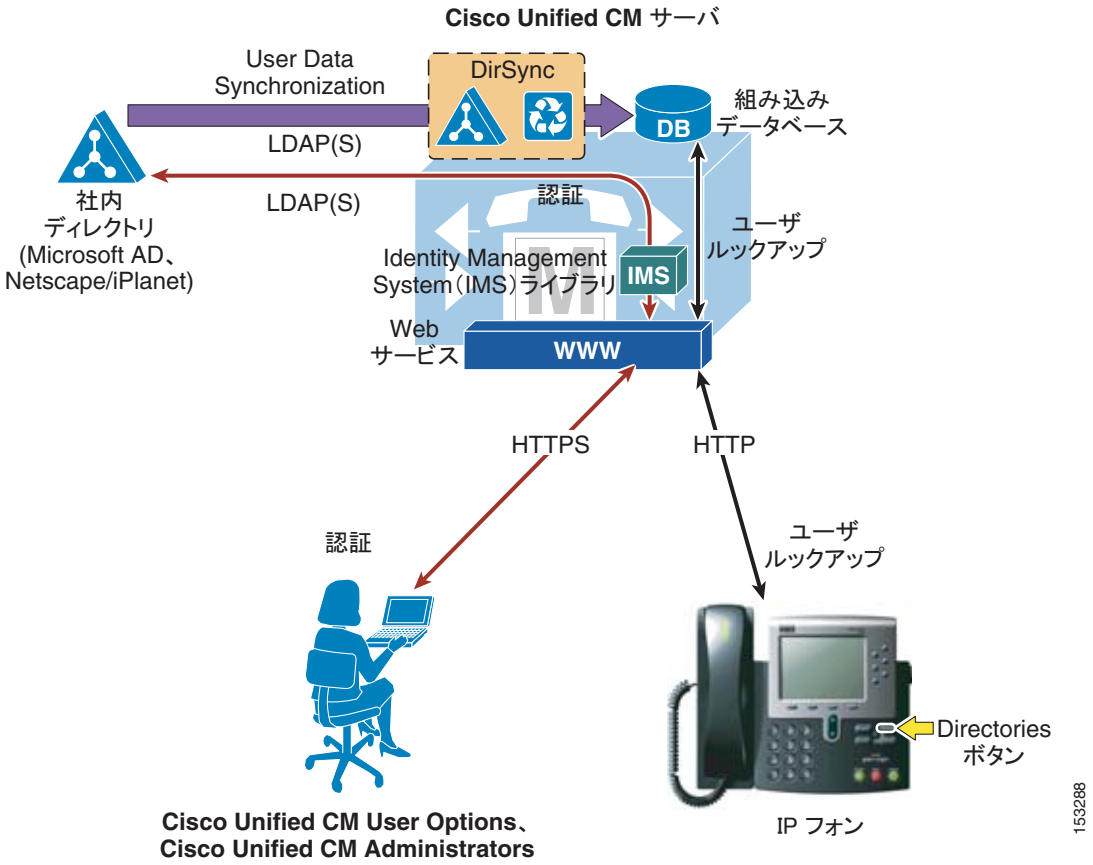


アカウントの同期を実行すると、Unified CM から AD に LDAP サーチ フィルタが送信されます。その中に、AD で無効のマークが付いているアカウントを戻さないという条件があります。ログインの失敗回数を超えた場合など、AD によって無効のマークが付けられたアカウントには、そのアカウントが無効である間に同期が実行された場合に非アクティブのマークが付けられます。

LDAP 認証

LDAP 認証機能を使用すると、組み込みデータベースを使用する代わりに、社内 LDAP ディレクトリに対して Unified CM でエンド ユーザ パスワードを認証できます。図 17-11 に示すように、Unified CM 内の IMS モジュールと社内ディレクトリ サーバ間で確立した LDAPv3 接続によって、この認証が実現されます。

図 17-11　LDAP 認証の有効化



認証を有効にするために、クラスタ全体に単一の認証アグリーメントを定義できます。認証アグリーメントは、冗長性を得るために LDAP サーバを 3 つまで設定でき、必要に応じて保護接続 Secure LDAP（SLDAP）もサポートします。認証は、LDAP 同期を使用しているときに限り有効にできます。

認証を有効にした場合の Unified CM の動作説明を、次に示します。

- エンド ユーザ パスワードは、シンプル バインド操作によって社内ディレクトリに対して認証される。
- アプリケーション ユーザ パスワードは、Unified CM データベースに対して認証される。
- エンド ユーザ PIN は、Unified CM データベースに対して認証される。

この動作は、リアルタイム Unified Communications システムの操作を社内ディレクトリの可用性に依存しないようにしながら、シングル ログオン機能をエンド ユーザに提供するという原則に従ったものです。図 17-12 に図示します。

図 17-12　エンド ユーザ パスワード、アプリケーション ユーザ パスワード、エンド ユーザ PIN の認証

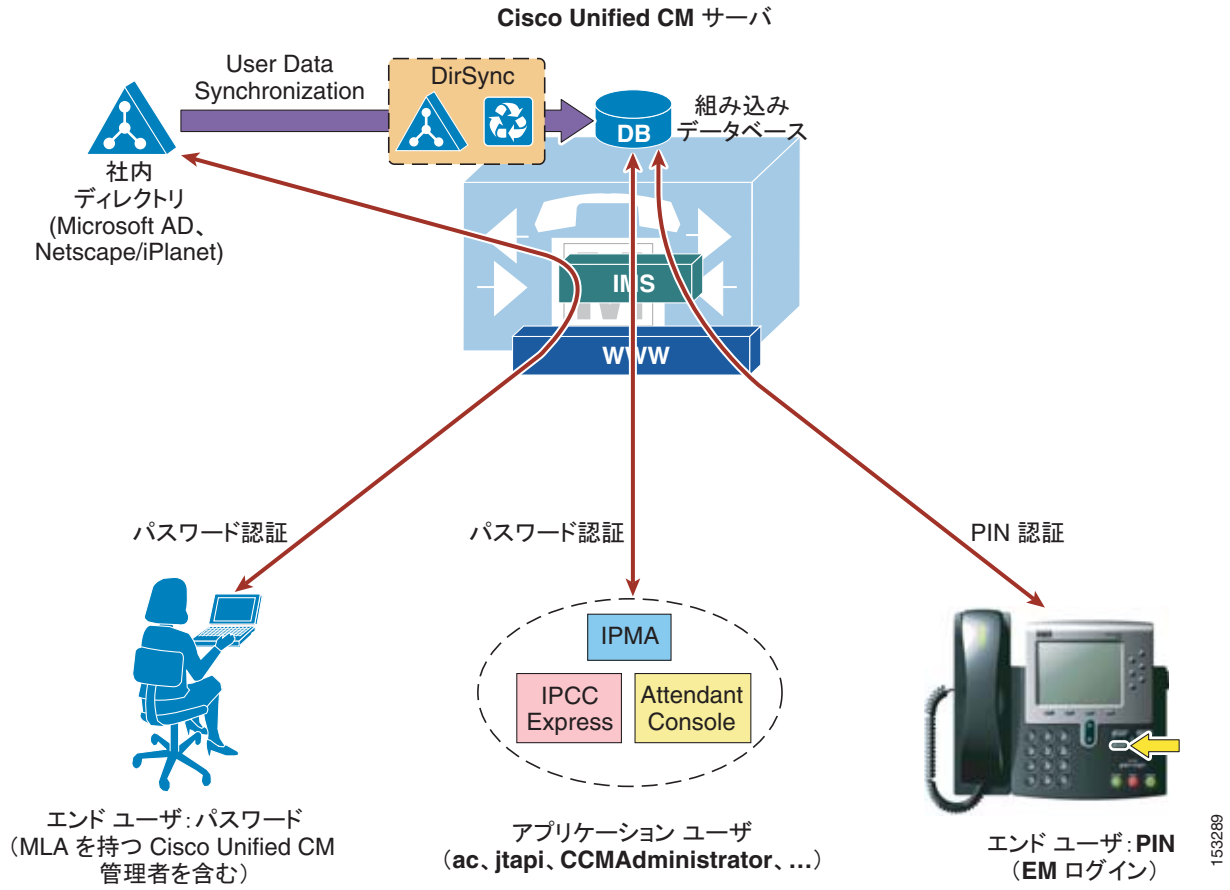
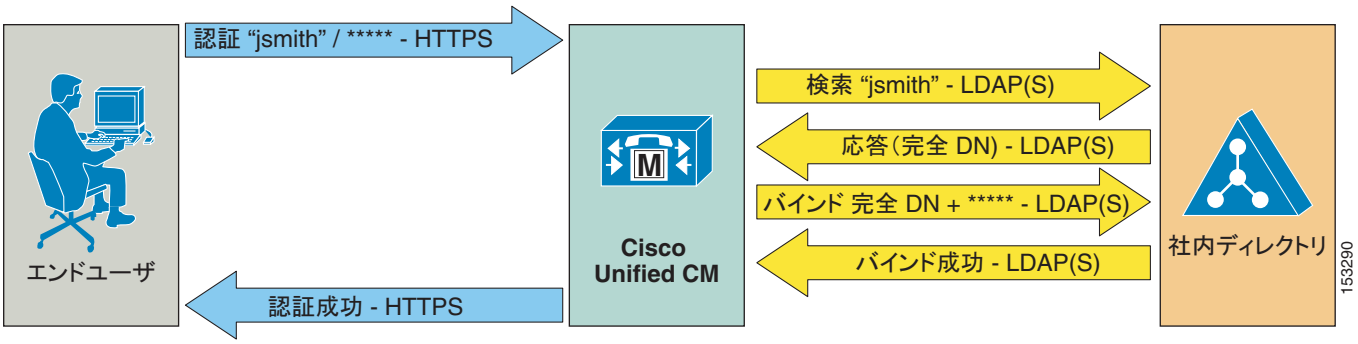


図 17-13 は、エンド ユーザを社内 LDAP ディレクトリに対して認証するために Unified CM で採用された、次のプロセスを示しています。

1. ユーザは、HTTPS 経由で [Unified CM User Options] ページに接続し、ユーザ名とパスワードで認証を試行します。この例では、ユーザ名は jsmith です。
2. Unified CM はユーザ名 jsmith に関する LDAP 照会を発行し、[LDAP Authentication] 設定ページの [LDAP Search Base] で指定された値を、この照会の範囲として使用します。SLDAP を有効にした場合、この照会は SSL 接続を通じて行われます。
3. 社内ディレクトリ サーバは、LDAP 経由で、ユーザ jsmith の完全 Distinguished Name（DN; 認定者名）で応答します（たとえば、「cn=jsmith, ou=Users, dc=vse, dc=lab」）。
4. 次に Unified CM は、LDAP バインド操作を使用して、ユーザに提供された完全な DN とパスワードを渡すことにより、ユーザのクレデンシャルの検証を試みます。
5. LDAP バインドが成功した場合、Unified CM は、要求された設定ページにユーザが進むことを許可します。

図 17-13　認証プロセス



Cisco Unified CM で LDAP 認証を配置する場合は、設計と実装に関する次のベスト プラクティスに従ってください。

- 社内ディレクトリ内に特定のアカウントを作成し、Unified CM がそのディレクトリに対して接続および認証できるようにする。目的の検索ベース内にあるすべてのユーザ オブジェクトを「読み取る」ように最小権限を設定し、期限切れにならないようにパスワードを設定した状態で、Unified CM 専用のアカウントを使用することをお勧めします。ディレクトリ内のこのアカウントのパスワードは、Unified CM 内のアカウントのパスワード設定と同期し続ける必要があります。アカウントのパスワードがディレクトリ内で変更された場合は、必ず Unified CM でアカウント設定を更新してください。LDAP 同期も有効にする場合、両方の機能に同じアカウントを使用できます。
- LDAP Manager Distinguished Name および LDAP Password で前述のアカウントのクレデンシャルを指定し、LDAP User Search Base ですべてのユーザが存在するディレクトリ サブツリーを指定することにより、Unified CM で LDAP 認証を有効にする。
- 冗長性が得られるように、2 台以上の LDAP サーバを設定する。ホスト名の代わりに IP アドレスを使用すると、Domain Name System（DNS; ドメイン ネーム システム）の可用性に依存しなくなります。
- この方法では、シングル ログオン機能をすべてのエンド ユーザに提供する。エンド ユーザは、Unified CM User Options ページにログインすると、社内ディレクトリ クレデンシャルを使用できるようになります。
- 社内ディレクトリ インターフェイスでエンドユーザ パスワードを管理する。認証を有効にすると、Unified CM Administration のページにパスワード フィールドが表示されなくなります。
- Unified CM Administration の Web ページまたは [Unified CM User Options] ページでエンドユーザ PIN を管理する。
- Unified CM Administration の Web ページでアプリケーション ユーザのパスワードを管理する。アプリケーション ユーザは他の Cisco Unified Communications アプリケーションとの通信やリモート 呼制御を容易にすること、また、実際のユーザには関連付けられないことに留意してください。
- 対応するエンド ユーザを Unified CM Administration の Web ページから Unified CM Super Users ユーザ グループに追加することにより、Unified CM 管理者のシングル ログオンを有効にする。カスタマイズしたユーザ グループおよびロールを作成することにより、複数レベルの管理者権利を定義できます。

Microsoft Active Directory に関する追加の考慮事項

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

ただし、重要な制限があります。グローバル カタログは Employee ID 属性を伝送しないので、Employee ID をログインとして使用する場合には、この方法は使用できません。この属性には、ドメイン コントローラだけを使用できます。

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

Microsoft AD から同期するユーザが複数のドメインに属していると、認証へのグローバル カタログの使用がさらに効率的になります。Unified CM は、照会に従う必要がなく、すぐにユーザを認証できるためです。このような場合は、Unified CM がグローバル カタログ サーバを指すようにし、LDAP User Search Base をルート ドメインの最上位に設定します。

複数のツリーを含む Microsoft AD フォレストの場合には、追加の考慮事項が適用されます。単一の LDAP 検索ベースでは複数のネームスペースを扱えないので、Unified CM は別のメカニズムを使用して、これらの不連続なネームスペース間でユーザを認証する必要があります。

「LDAP 同期」（P.17-10）の項で説明したように、複数のツリーがある AD フォレストで同期をサポートするために、UserPrincipalName（UPN）属性を Unified CM 内でユーザ ID として使用する必要があります。ユーザ ID が UPN の場合、Unified CM Administration の LDAP Authentication 設定ページで [LDAP Search Base] フィールドへの入力はできませんが、その代わりに「LDAP user search base is formed using userid information.」という注意が表示されます。

実際には、図 17-14 に示すように、ユーザごとに UPN サフィックスからユーザ検索ベースが導き出されます。この例では、Microsoft Active Directory フォレストは avvid.info と vse.lab という 2 つのツリーで構成されます。同じユーザ名が両方のツリーに表示される場合があるため、同期プロセス中および認証プロセス中は UPN を使用してデータベースのユーザを固有に識別するように、Unified CM が設定されています。

図 17-14　複数のツリーがある Microsoft AD フォレストでの認証

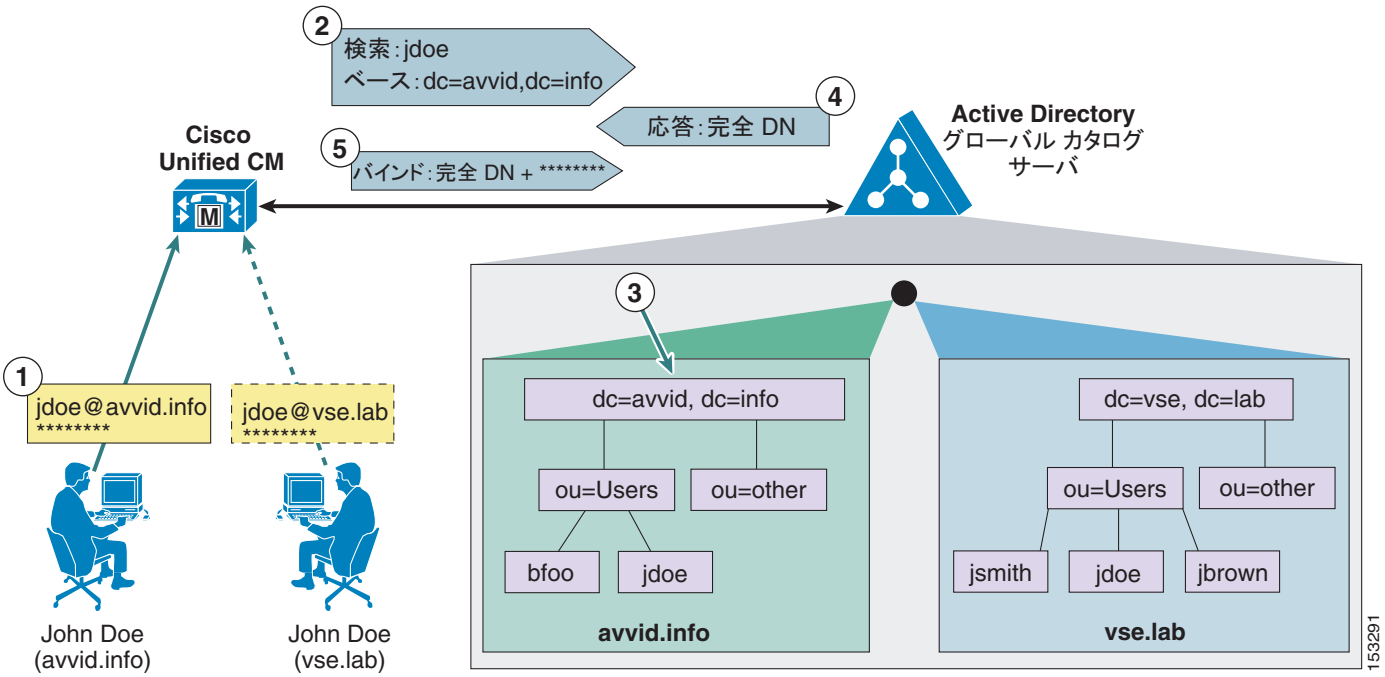


図 17-14 に示すように、John Doe という名前のユーザが avvid.info ツリーと vse.lab ツリーの両方に存在します。次の手順は、UPN が jdoe@avvid.info となる第 1 のユーザに対する認証プロセスを示しています。

1. ユーザは、ユーザ名（UPN に対応するもの）とパスワードを使用し、HTTPS 経由で Unified CM に対して認証します。
2. Unified CM は、Microsoft Active Directory グローバル カタログ サーバに対して LDAP 照会を実行し、UPN で指定したユーザ名（@ 記号よりも前の部分）を使用して、UPN サフィックス（@ 記号より後の部分）から LDAP 検索ベースを得ます。この場合、ユーザ名は jdoe で、LDAP 検索ベースは「dc=avvid, dc=info」です。
3. Microsoft Active Directory は、LDAP 照会で指定したツリーのユーザ名に対応する正しい認定者名を識別します。この場合は、「cn=jdoe, ou=Users, dc=avvid, dc=info」です。
4. Microsoft Active Directory は LDAP 経由で、このユーザの完全認定者名を使用して Unified CM に応答します。
5. Unified CM は、提供された認定者名とユーザが最初に入力したパスワードで LDAP バインドを試行し、その後は図 17-13 に示す標準的な場合と同様に、認証プロセスが続行されます。

（注）　複数のツリーを含む Microsoft AD フォレストでの LDAP 認証のサポートは、上記の方法だけで行われます。したがってサポートは、ユーザの UPN サフィックスが、そのユーザが存在するツリーのルートドメインに対応する配置だけに限定されます。AD では、異なる UPN サフィックスが許可されたエイリアスを使用できます。UPN サフィックスがツリーの実際のネームスペースから分離されている場合は、Microsoft Active Directory フォレスト全体で Unified CM ユーザを認証できなくなります（ただし、その場合でも、別の属性をユーザ ID として使用し、統合をフォレスト内の単一のツリーに限定することはできます）。

Unified CM データベース同期のサイジング

Unified CM データベース同期機能には、LDAP ストアから Unified CM パブリッシャ データベースへユーザ設定データ（属性）のサブセットをインポートするメカニズムがあります。ユーザ アカウントの同期が発生すると、各ユーザの LDAP アカウント情報が、そのユーザの特定の Unified Communications 機能を有効にするために必要な追加データと関連付けられることがあります。認証も有効な場合、パスワード確認のための LDAP ストアへのバインドに、ユーザのクレデンシャルを使用します。同期や認証が有効な場合に、エンド ユーザのパスワードは Unified CM データベースには格納されません。

ユーザ アカウント情報はクラスタ固有です。各 Unified CM パブリッシャ サーバは、このクラスタから Unified Communications サービスを受けているユーザの固有のリストを保持しています。同期アグリーメントはクラスタ固有で、各パブリッシャにはユーザ アカウント情報の独自コピーがあります。

Unified CM データベースは、設定された、または同期された最大 60,000 のユーザ アカウントをサポートします。ディレクトリ同期のパフォーマンスを最適化するには、次の点を考慮してください。

- 電話機や Web ページからのディレクトリ ルックアップには、Unified CM データベースまたは IP Phone Service SDK を使用できる。ディレクトリ ルックアップ機能に Unified CM データベースを使用する場合、LDAP ストアから設定された、または同期されたユーザだけがディレクトリに表示されます。ユーザのサブセットを同期すると、ユーザのそのサブセットだけがディレクトリ ルックアップに表示されます。
- ディレクトリ ルックアップに IP Phone Services SDK を使用する場合に、LDAP に対する Unified CM ユーザの認証が不要であれば、Unified CM クラスタにログインするユーザのサブセットだけに同期を制限できます。
- クラスタが 1 つだけであり、LDAP ストア内のユーザ数が 60,000 未満である場合、Unified CM データベースにディレクトリ ルックアップを実装するには、LDAP ディレクトリ全体をインポートできます。
- 複数のクラスタが存在し、LDAP 内のユーザ数が 60,000 未満である場合、すべてのユーザをすべてのクラスタにインポートすることで、すべてのエントリがディレクトリ ルックアップに確実に含まれるようにすることができます。
- LDAP 内のユーザ アカウント数が 60,000 を超えており、ユーザ セット全体をすべてのユーザに表示する必要がある場合には、Unified IP Phone Services SDK を使用して Unified CM からディレクトリ ルックアップをオフロードする必要がある。
- 同期と認証の両方を有効にすると、Unified CM データベースに設定または同期されたユーザ アカウントはそのクラスタにログインできるようになる。同期するユーザの決定は、ディレクトリ ルックアップ サポートの決定に影響します。

（注）　シスコでは、クラスタごとに最大 60,000 のユーザ アカウントの同期をサポートしていますが、この制限を強制していません。60,000 を超えるユーザ アカウントを同期化すると、ディスク容量のスターベージョン、データベース パフォーマンスの低速化、およびアップグレードの長時間化を招くことがあります。

同期を制御するための LDAP 構造の使用

多数の LDAP ディレクトリの配置には、Organizational Unit Name（OU; 組織ユニット名）を使用して、ユーザを論理的順序や、場合によっては階層的順序でグループ化します。ユーザを複数の OU に編成する構造が LDAP ディレクトリにある場合、インポートされるユーザのグループを制御するためにこの構造を使用することもできます。各個別 Unified CM 同期アグリーメントは、単一の OU を指定します。サブ OU 内であっても、指定 OU の下にある全アクティブ アカウントがサポートされます。OU

内のユーザだけが同期されます。ユーザを含む複数の OU がクラスタで必要な場合、複数の同期アグリーメントが必要です。Unified Communications リソースを割り当てられていないユーザが OU に含まれている場合は、これらの OU をディレクトリ同期から省くことをお勧めします。

AD に同じ手法を使用して、コンテナを定義できます。同期アグリーメントでは、ディレクトリ ツリーの特定のコンテナを指定でき、それによってインポートの範囲を制限できます。

使用できる同期アグリーメントは 5 つだけなので、多数の OU やコンテナを持つ LDAP の配置では、この手法はすぐに使い果たされてしまいます。複数の OU がある環境でユーザを同期するには、同期サービス アカウントに割り当てる権限を制御するという方法があります。複数のユーザが存在するツリー ノードに同期アグリーメントを設定してから、システム アカウントの読み取りアクセスをサブツリーの選択部分に制限します。このアクセスを制限する方法については、LDAP ベンダーのドキュメンテーションを参照してください。

CHAPTER 18

IP Telephony Migration Options

Last revised on: December 15, 2008

This chapter describes several methods for migrating from separate standalone voice, video, and collaboration systems to an integrated Cisco Unified Communications System. The major topics discussed in this chapter include:

What's New in This Chapter

Table 18-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 18-1 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:
Migration of collaboration systems	Migration of Voice and Desktop Collaboration Systems, page 18-6
Migration of video systems	Video Migration, page 18-5

IP Telephony Migration

There are two main methods for migrating to an IP Telephony system (or any other phone system, for that matter):

- Phased Migration, page 18-2
- Parallel Cutover, page 18-3

Neither method is right or wrong, and both depend upon individual customer circumstances and preferences to determine which option is most suitable.

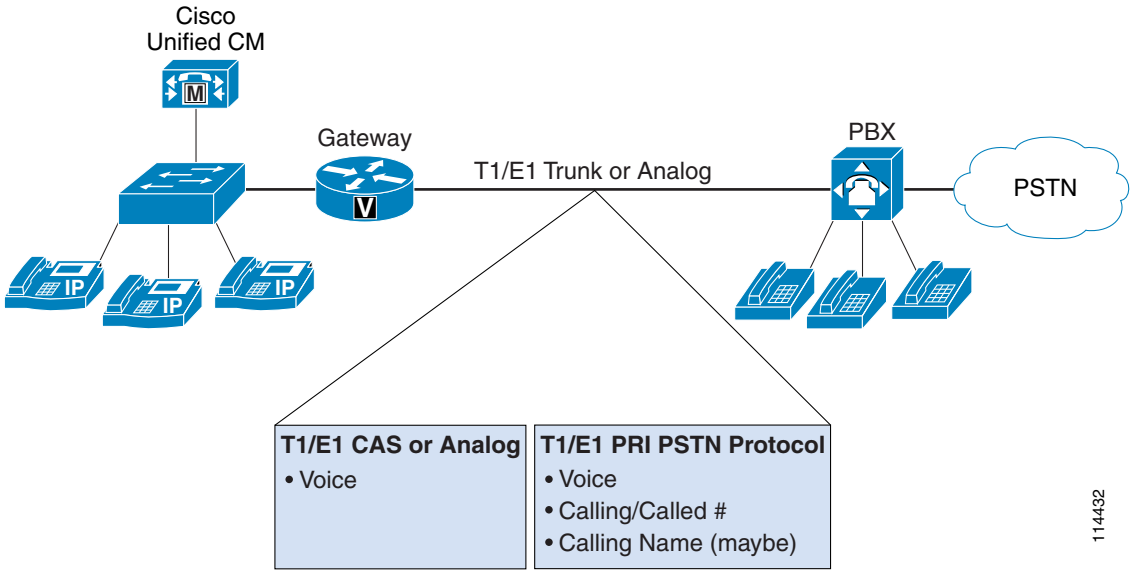
IP Telephony migration also involves The Need for QSIG in Multisite Enterprises, page 18-3.

Phased Migration

This approach typically entails a small initial IP Telephony deployment that is connected to the main corporate PBX. The choice of which signaling protocol to use is determined by the required features and functionality as well as by the cost of implementation. Cisco Unified Communications Manager (Unified CM) can support either regular PSTN-type PRI or QSIG PRI as well as H.323 and SIP. Of these options, T1/E1 QSIG provides the highest level of feature transparency between the two systems.

PSTN-type PRI provides for basic call connectivity as well as Automatic Number Identification (ANI). In some instances, the protocol also supports calling name information, as illustrated in Figure 18-1.

Figure 18-1 Features Supported by Signaling Protocols



This level of connectivity is available to *all* PBXs; that is, if the PBX can connect to the public network via PRI, then it can connect to Unified CM because Unified CM can be configured as the "network" side of the connection.

Cisco Unified CM, Release 3.3 and later, incorporates the International Standards Organization (ISO) variant of QSIG. The QSIG protocol allows for additional feature transparency between PBXs from different vendors, over and above the features that can be obtained from PSTN-type PRI, and it is therefore more appropriate for large enterprises that are already operating complex networks. (Refer to The Need for QSIG in Multisite Enterprises, page 18-3.)

With either PSTN-type PRI or QSIG, the process of phased migration is similar: move subscribers from the PBX to Unified CM in groups, one group at a time, until the migration is complete.

The Cisco San Jose campus, consisting of some 23,000 subscribers housed in approximately 60 buildings, was migrated to IP Telephony in this manner and took just over one year from start to finish. We converted one building per weekend. All subscribers in the selected building were identified, and their extensions were deleted from the PBX on a Friday evening. At the same time, additions were made to the PBX routing tables so that anyone dialing those extension numbers would then be routed over the correct PRI trunk for delivery to Unified CM. During the weekend, new extensions were created in Unified CM for the subscribers, and new IP phones were delivered to their appropriate locations, ready for use by Monday morning. This process was simply repeated for each building until all subscribers had been migrated.

Parallel Cutover

This approach begins with implementation of a complete IP Telephony infrastructure that is redundant, highly available, QoS-enabled, and equipped with Ethernet ports that are powered inline. Once the infrastructure is complete, the IP Telephony application can then be deployed. All IP phones and gateways can be fully configured and deployed so that subscribers have two phones on their desk simultaneously, an IP phone as well as a PBX phone. This approach provides the opportunity to test the system as well as allowing subscribers time to familiarize themselves with their new IP phones. Outbound-only trunks can also be connected to the IP Telephony system, giving subscribers the opportunity to use their new IP phones to place external calls as well as internal calls.

Once the IP Telephony system is fully deployed, you can select a time slot for bringing the new system into full service by transferring the inbound PSTN trunks from the PBX to the IP Telephony gateways. You can also leave the PBX in place until such a time as you are confident with the operation of the IP Telephony system, at which point the PBX can be decommissioned.

A parallel cutover has the following advantages over a phased migration:

- If something unexpected occurs, the parallel cutover provides a back-out plan that allows you to revert to the PBX system by simply transferring the inbound PSTN trunks from the IP Telephony gateways back to the PBX.
- The parallel cutover allows for verification of the IP Telephony database configuration before the system carries live PSTN traffic. This scenario can be run for any length of time prior to the cutover of the inbound PSTN trunks from the PBX to the IP Telephony gateways, thereby ensuring correct configuration of all subscriber information, phones, gateways, the dial plan, and so forth.
- Training can be carried out at a more relaxed pace by allowing subscribers to explore and use the IP Telephony system at their own leisure before the cutover of the inbound PSTN trunks.
- The system administrator does not have to make special provisions for "communities of interest." With a phased approach, you have to consider maintaining the integrity of call pick-up groups, hunt groups, shared lines, and so forth. These associations can be easily accounted for when moving the complete site in a parallel cutover.

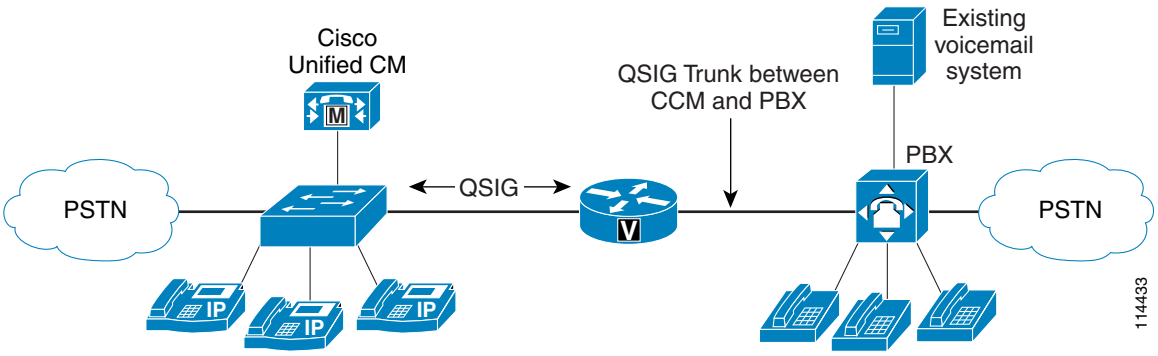
One disadvantage of the parallel cutover is that it requires the IP Telephony solution to be fully funded from the beginning because the entire system must be ready prior to bringing it into service. With a phased migration, on the other hand, you can purchase individual components of the system when they are needed, and this approach does not prevent you from starting with a small trial system prior to moving to full deployment.

The Need for QSIG in Multisite Enterprises

While some enterprises consist of only one location, others consist of many sites, some of which may potentially be spread over large distances. PBX networks for multisite enterprises are usually connected using T1 or E1 PRI trunks (depending on location) running a proprietary protocol such as Avaya DCS, Nortel MCDN, Siemens CorNet, NEC CCIS, Fujitsu FIPN, or Alcatel ABC, among others. These proprietary networking protocols enable the PBXs to deliver a high level of feature transparency between subscribers.

QSIG was developed to enable the interconnection of PBXs from different vendors, thereby allowing similar levels of feature transparency. Cisco first added QSIG to Unified CM Release 3.3 to enable Unified CM to be part of a large enterprise network. (See Figure 18-2.)

Figure 18-2 QSIG Used Between Cisco Unified CM and a PBX



QSIG as implemented in Cisco Unified CM Release 4.1 supports the following features:

- Basic call
- Direct Inward Dialing (DID)
- Calling number
- Called number
- Connected name
- Transfer (by join)
- Message Waiting Indication (MWI)
- Divert (by forward-switching)
- Calling name restriction
- Calling number restriction
- Divert (by re-route)
- Divert (responding to “check restriction” request)
- Alerting name (on-ringing)
- Path Replacement
- Callback — Call Completion Busy Subscriber (CCBS) and Call Completion No Reply (CCNR)

By supporting QSIG, Unified CM can be introduced into a large enterprise network while also maintaining feature transparency between subscribers. PBX locations can then be converted to IP Telephony whenever convenient.

However, unless you already have QSIG enabled on your PBX or have a specific need for its additional features and functionality, the cost of upgrading the PBX might be hard to justify if it will be retired within a short period of time. For example, why spend $30,000 on enabling the PBX for QSIG if you plan to retire the PBX in two or three months?

Summary of IP Telephony Migration

Although both methods of IP Telephony migration work well and neither method is right or wrong, the parallel cutover method usually works best in most cases. In addition, large enterprises can improve upon either migration method by using QSIG to enable Unified CM to become part of the enterprise network.

Cisco has a lab facility dedicated to testing interoperability between Unified CM and PBX systems. The results of that testing are made available as Application Notes, which are posted at

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

The Application Notes are updated frequently, and new documents are continuously added to this website. Check the website often to obtain the latest information.

Video Migration

Typically one of the following scenarios will exist in an enterprise network:

- A dedicated H.323 video network consisting of a Multipoint Control Unit (MCU) along with either desktop or room-based endpoints
- ISDN-enabled room-based endpoints

Before attempting to integrate any form of video with Unified Communications, you must consider the dial plan(s) between the two distinct networks. The dial plans must be compatible, with no overlapping numbers present.

Dedicated H.323 Video Network

Integration of video with Unified Communications is best achieved by the deployment of an H.323 gatekeeper because this method provides connectivity between the two networks. A gatekeeper provides for dial-plan resolution as well as call admission control.

A Cisco Unified Border Element can also be deployed to provide the following capabilities:

- Ability to handle differences in network addressing (for example, 10.x.x.x and 192.x.x.x)
- Number translations (adding or modifying calling/called numbers)
- Multiple layers of call admission control, such as RSVP and simultaneous call accounting as well as bandwidth accounting
- Resolution of interworking issues such as DTMF, SIP-to-H.323 conversions, and resolution of dial-plan numbers to IP addresses

Use of the Cisco Unified Border Element is best suited for enterprises that want to maintain separate networks for reasons of management and/or feature support.

The physical migration of H.323 endpoints can be achieved by simply moving them to the Unified Communications system, in which case they would continue to be supported as either H.323 endpoints or in some cases even SIP endpoints, assuming that option is supported. H.323 MCUs can also be migrated to the Unified Communications system and would be connected via an H.323 gatekeeper. This method is best suited for customers who wish to migrate fully to a Unified Communications solution and do not wish to support multiple networks.

ISDN Endpoints

Customers have the option of continuing to place/receive calls via the PSTN from/to a Unified Communications system, much as they would operate these endpoints prior to migration. PSTN calls to the Unified Communications system can be eliminated by implementing a toll-bypass configuration that connects the ISDN interface(s) to an IP gateway, thereby making use of the customer's IP network.

Additionally, some endpoints offer the capability to connect directly via IP (H.323 and/or SIP), and this method is preferred over a toll-bypass implementation.

Migration of Voice and Desktop Collaboration Systems

Typically these systems fall into one of two categories:

- Hosted via PSTN access
- On-premises

Hosted Systems

Customers may migrate from a hosted solution to an on-premises solution by first building out the on-premises system and then choosing an appropriate time to begin using this new system. This method is best suited for enterprises that are increasing in size and want to reduce ongoing subscription costs.

On-Premises System

These systems can be considered separately in terms of voice and desktop collaboration; in other words, a collaboration session can be carried out by using a separate solution for voice along with another solution for the desktop. Migration from these systems to Unified Communications can be accomplished by moving the voice and desktop solutions independently from each other.

This method is best suited for customers who wish to move to a collaboration solution that offers both consistency and simplicity across both voice collaboration and desktop collaboration. The Unified Communications solution provides the ability to record a conference that includes both voice and desktop collaboration along with the ability to dial out to conference attendees.

CHAPTER 19

音声セキュリティ

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

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

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

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

この章の新規情報

表 19-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 19-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
ネットワーク バーチャライゼーション	「ネットワーク バーチャライゼーションの保護」（P.19-46）

セキュリティの概要

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

セキュリティ ポリシー

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

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

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

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

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

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

要約すると、セキュリティ ポリシーを定義するには、次のプロセスに従います。

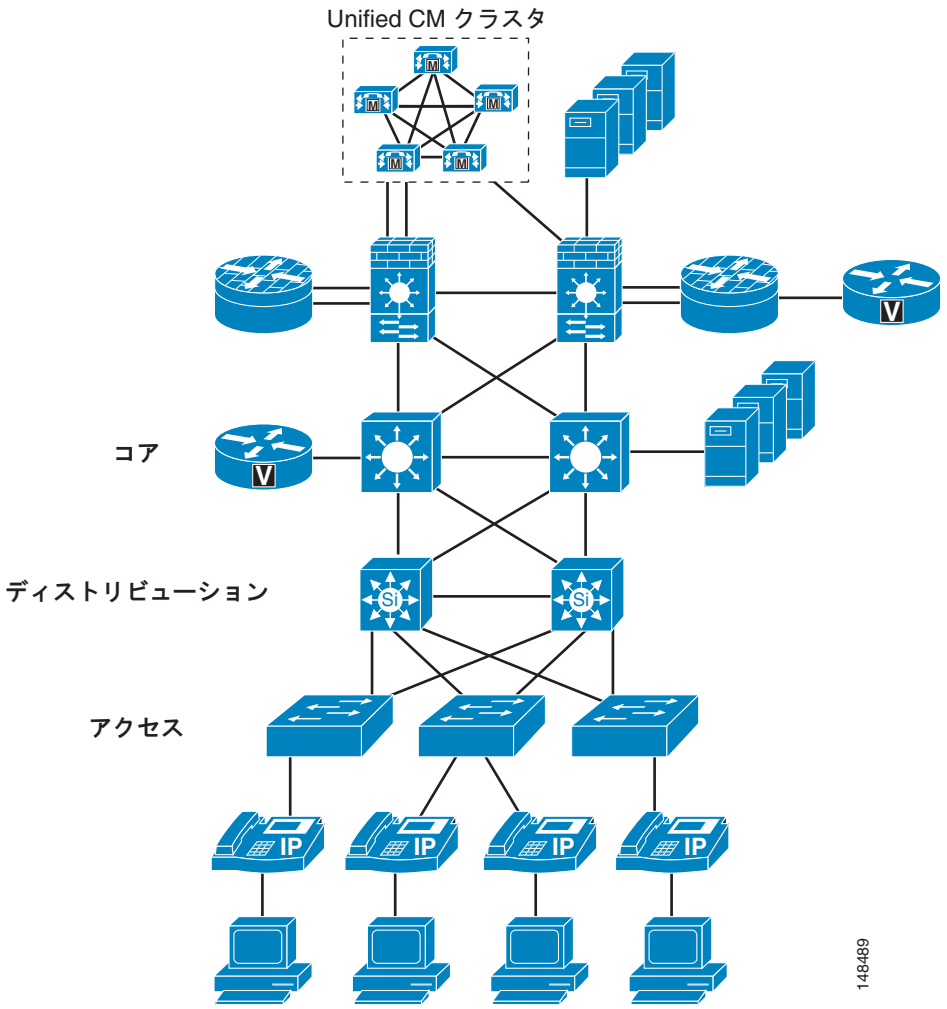
- ネットワーク上のデータを定義する。
- データの重要性を定義する。
- データの重要性に基づいてセキュリティを適用する。

レイヤ化したセキュリティ

この章では、最初にユーザが PC に接続できる電話機ポートについて説明します。また、電話機がネットワークを介して、アクセス スイッチ、ディストリビューション レイヤ、コア レイヤ、最後にデータセンターに到達する方法について説明します（図 19-1 を参照）。アクセス ポートからネットワーク自体に至るまで、セキュリティ レイヤの上にレイヤを構築します。各機能について説明するにあたり、社内セキュリティ ポリシーの観点から考慮する必要がある、それぞれの利点と欠点について説明します。

たとえば、図 19-1 は、IP テレフォニー ネットワークを使用することの利点と欠点の両方を示しています。音声製品は IP を使用してすべてのデバイスに接続するため、ネットワーク内の任意の場所に配置できます。この特性を使用すると、ネットワークの設計者は、IP テレフォニー アプリケーションを配置するうえで物理的にも論理的にも簡単な場所に、デバイスを配置できます。しかし、簡単に配置できるということは、セキュリティがより複雑になることを意味します。接続性があるところであればネットワーク内のどこにでも、IP テレフォニー デバイスを配置できるからです。

図 19-1　　セキュリティ レイヤ



インフラストラクチャの保護

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

ネットワーク全体のセキュリティを向上させるためにデータ ネットワークで実行できる、多くのベストプラクティスがあります。たとえば、攻撃者がパスワードをクリア テキスト形式で見ることができないように、Telnet（パスワードをクリア テキスト形式で送信します）を使用して任意のネットワーク デバイスに接続する代わりに、Secure Shell（SSH、Telnet の安全な形式）を使用できます。Cisco.com Web サイトでは、ネットワーク内のセキュリティ全般に関する多数のマニュアルを入手できます。導入済みのセキュリティ ポリシーと共にこれらのマニュアルを使用し、インフラストラクチャで必要なセキュリティを判別してください。

ビデオ インフラストラクチャ

ゲートキーパー機能を提供する Cisco IOS 機能セット（IP/H323 機能セットと EnterprisePlus/H323 MCU 機能セット）は Telnet だけをサポートし、Secure Shell（SSH）はサポートしません。Telnet ではユーザ名とパスワードがクリア テキスト形式で送信されるため、Access Control List（ACL; アクセス コントロール リスト）を使用して、Telnet によるルータへの接続をだれに許可するかを制御することをお勧めします。また、ゲートキーパーには、安全なネットワーク セグメントにあるホストから常に接続するように努めてください。

Cisco Unified Videoconferencing 3500 シリーズ MCU および H.320 ゲートウェイは Telnet、FTP、HTTP、および SNMP をサポートします。これらの IP/VC デバイスは TACACS または RADIUS の認証をサポートしません。限定数の管理アカウントのみをデバイスにローカルで設定できます。ユーザ名とパスワードは Telnet、FTP、HTTP、SNMP のすべての通信でクリア テキスト形式で送信されます。これらのデバイスには、安全なネットワーク セグメントにあるホストからアクセスすることをお勧めします。これらのデバイスを不正アクセスから保護するにはファイアウォール、アクセス コントロール リスト、Cisco Authentication Proxy、およびその他の Cisco セキュリティ ツールも使用する必要があります。

次のリンクは、Cisco.com で入手可能なセキュリティ関連マニュアルをリストしています。

- Best Practices for Cisco Switches（ログイン認証が必要）

  http://cisco.com/en/US/partner/products/hw/switches/ps663/products_tech_note09186a0080094713.shtml

- Cisco SAFE: A Security Blueprint for Enterprise Networks

  http://www.cisco.com/en/US/prod/collateral/wireless/wirelssw/ps1953/product_implementation_design_guide09186a00800a3016.pdf

物理的なセキュリティ

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

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

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

IP アドレッシング

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

このマニュアルの他の項で説明されているとおり（「キャンパス アクセス レイヤ」（P.3-4）を参照）、RFC 1918 に基づいた IP アドレッシングを使用する必要があります。このアドレッシング方式では、ネットワークの IP アドレッシングをやり直すことなく、IP テレフォニー システムをネットワークに配置できます。音声エンドポイントの IP アドレスは適切に定義されていて理解しやすいので、RFC 1918 を使用すると、ネットワーク内の制御をより適切に実行できます。すべての音声エンドポイントが 10.x.x.x. のネットワーク内でアドレッシングされていると、アクセス コントロール リスト（ACL）、およびこれらのデバイスが受信または送信するデータのトラックは単純になります。

利点

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

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

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

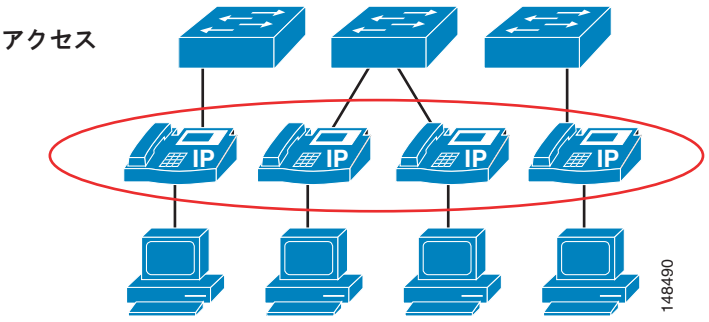
欠点

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

電話機のセキュリティ

Cisco Unified IP Phone には、IP テレフォニー ネットワーク上のセキュリティを強化するための組み込み型の機能があります。これらの機能を電話機単位で有効または無効にして、IP テレフォニー配置のセキュリティを強化できます。セキュリティ ポリシーは、電話機の配置に応じて、これらの機能を有効にする必要があるかどうか、および有効にする必要がある場所を判別するのに役立ちます（図 19-2 を参照）。

図 19-2　電話機レベルでのセキュリティ



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

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803fe693.html

電話機の PC ポート

電話機には、通常、PC を接続するための電話機の背面のポートを、オンまたはオフにする機能があります。この機能は、そのタイプの制御が必要な場合に、ネットワークにアクセスするためのコントロール ポイントとして使用できます。

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

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

利点

電話機の PC ポートを無効にすると、電話機からネットワークへのアクセスを禁止する必要があるエリアに電話機を配置できます。これにより、電話機の背面の PC ポートが有効であればアクセス可能だったはずのネットワークへのアクセスが制御されます。

欠点

電話機の PC ポートが無効な場合、ネットワーク アクセスを必要としているユーザで、アクセスのための承認を得ているユーザごとに、ネットワーク アクセスを提供する個別のイーサネット ポートを追加する必要があります。ユーザは、イーサネット ジャックを電話機から切断し、別のデバイスに接続することを試行できます。

Cisco Unified Video Advantage が正しく動作するには、PC ポートとビデオ機能の両方を有効にする必要があります。その他の設定は無効にしてもかまいません。

Gratuitous ARP

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

Gratuitous ARP は、攻撃者がネットワークの音声セグメントにアクセスできた場合に、攻撃者が電話機からのシグナリングや RTP 音声ストリームを取り込むことから電話機を保護するのに役立ちます。この機能で保護されるのは電話機だけです。インフラストラクチャの残りの部分は、Gratuitous ARP 攻撃から保護されません。スイッチ ポートには電話機とネットワーク デバイスの両方を保護する機能があるので、Cisco インフラストラクチャを実行している場合、この機能はそれほど重要ではありません。これらのスイッチ ポートの機能の説明については、「スイッチ ポート」（P.19-13）を参照してください。

利点

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

欠点

別の電話機から発信されたかネットワークを経由して到達するダウンストリーム シグナリングおよび RTP 音声ストリームは、電話機のこの機能では保護されません。保護されるのは、この機能が有効になっている電話機からのデータのみです（図 19-3 を参照）。

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

図 19-3　Gratuitous ARP は導入先の電話機は保護するが他のトラフィックは保護しない

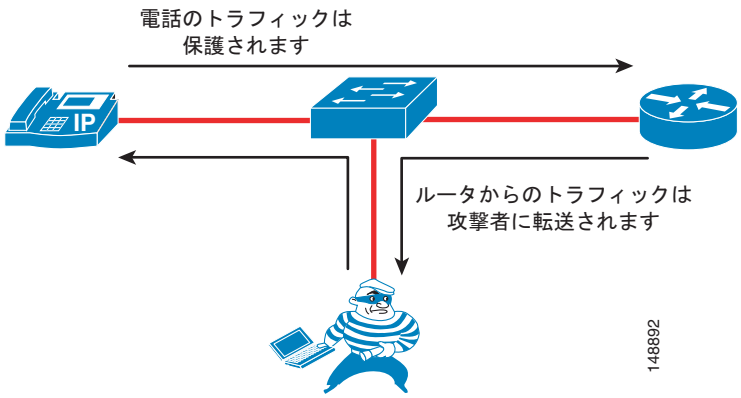


図 19-3 が示しているとおり、Gratuitous ARP 機能を持つ電話機からのトラフィックは保護されますが、エンドポイントに、データ フローを保護する機能がない可能性があるので、攻撃者が別のエンドポイントからのトラフィックを見ることができる場合があります。

PC Voice VLAN へのアクセス

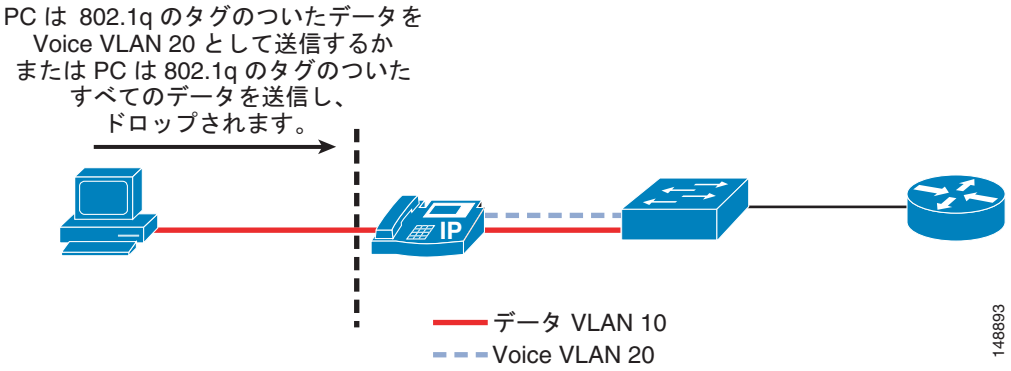
スイッチから電話機までに 2 つの VLAN が存在するので、電話機は、望まないアクセスから Voice VLAN を保護する必要があります。電話機では、電話機の背面から Voice VLAN に入り込む、望まないアクセスを防止できます。PC Voice VLAN Access 機能は、電話機の背面にある PC ポートから Voice VLAN への任意のアクセスを防止します。この機能を無効にすると、電話機の PC ポートに接続されたデバイスが、電話機の背面の PC ポートに到達する Voice VLAN を宛先とした 802.1q タグ付き情報を送信することにより、VLAN を「ジャンプ」して Voice VLAN にアクセスすることは許可されません。設定している電話機に応じて、この機能は 2 つの方法のいずれかで動作します。高機能の電話機では、電話機の背面の PC ポートに着信する Voice VLAN を宛先とした、すべてのトラフィックをブロックします。図 19-4 に示す例の場合、PC が、電話機の PC ポートに対して Voice VLAN トラフィック（このケースでは 200 の 802.1q タグ付き）の送信を試行すると、そのトラフィックはブロックされます。この機能が動作する他の方法は、電話機の PC ポートに着信する、802.1q タグ付きのすべてのトラフィック（Voice VLAN トラフィックに限らない）をブロックする方法です。

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

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

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

図 19-4　電話機の PC ポートから Voice VLAN へのトラフィックのブロック



利点

PC Voice VLAN Access 機能は、攻撃者が、電話機の背面にある PC ポートを経由して、制御されていないデータを Voice VLAN に送信することを防止します。

欠点

電話機に接続されているデバイスが 802.1q タグ付きパケットを送信することが、通常は許可されている場合、これらのパケットはドロップされます。ほとんどのエンド ステーションでは、アクセス レイヤでこの機能を実行することが許可されていません。この機能がネットワーク内で通常の動作と見なされる場合、この機能が動作することは許可されません。

Web アクセス

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

利点

電話機の Web アクセスを有効にすると、電話機やネットワークの問題をデバッグするときにその電話機を使用できます。電話機からの Web アクセスを無効にすると、ユーザまたは攻撃者は、IP テレフォニー ネットワークに関する情報をその電話機から入手できません。

欠点

電話機からの Web アクセスを無効にすると、ネットワークや IP テレフォニーの問題をデバッグするのがより困難になります。Web サーバがグローバルで無効だが、デバッグの参考として必要な場合、Unified CM の管理者は、電話機のこの機能を有効にする必要があります。この Web ページにアクセスする機能は、ネットワークの ACL で制御できます。ネットワーク オペレータは、この機能を使用して、必要なときに Web ページにアクセスできます。

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

ビデオ機能

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

利点

Cisco Unified Video Advantage が正しく機能するには、PC ポートとビデオ機能が必要です。

欠点

これらの機能を有効にすると、電話機の保護に ACL を使用していない場合に、PC から電話機への通信が許可される可能性があります。

アクセス設定

各 Cisco Unified IP Phone にはネットワーク設定ページがあり、そのページには、電話機が動作するのに必要な多くのネットワーク要素や詳細情報がリストされます。攻撃者はこの情報を使用して、電話機の Web ページに表示される情報の一部と共に、ネットワーク上で調査を開始できます。たとえば、攻

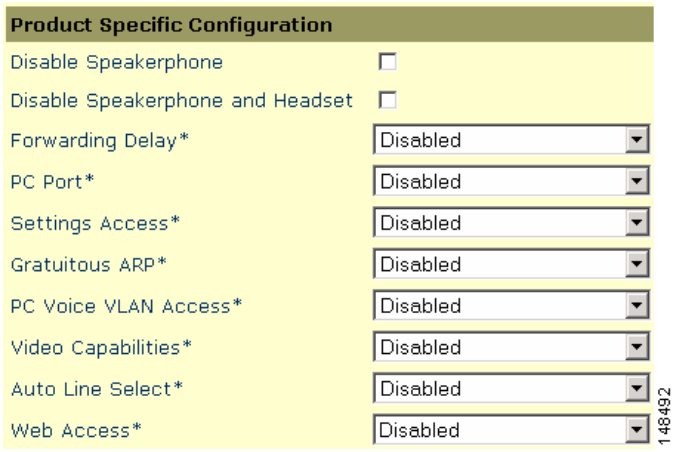
撃者は設定ページを参照して、デフォルト ゲートウェイ、TFTP サーバ、および Unified CM の IP アドレスを判別できます。これらの断片的な情報が、音声ネットワークにアクセスしたり、音声ネットワーク内のデバイスを攻撃したりするのに使用される場合があります。

このアクセスを電話機ごとに無効にすることにより（図 19-5 を参照）、エンド ユーザまたは攻撃者が、Unified CM IP アドレスや TFTP サーバ情報などの追加情報を取得するのを防止できます。

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

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

図 19-5　Unified CM の Phone Configuration ページ



利点

電話機設定ページへのアクセスを無効にすると、エンド ユーザおよび攻撃を仕掛けようとしている人が、ネットワークに関する詳細情報や音声システムで使用される IP テレフォニー情報を見ることはできません。この機能を無効にしたときに保護される情報には、電話機の IP アドレス、電話機の登録先の Unified CM などの情報が含まれます。

欠点

電話機設定ページへのアクセスを無効にすると、エンド ユーザは、スピーカー ボリューム、連絡先、呼び出しタイプなど、通常は制御可能な多くの電話機設定を変更できなくなります。電話機インターフェイスについてエンド ユーザに課される制限により、このセキュリティ機能を使用することが現実的ではない場合があります。ただし、管理者が電話機設定ページへのアクセスを無効にするのではなく制限する場合は、アクセス不可にはなりません。

電話機の認証および暗号化

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

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

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

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

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

利点

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

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

欠点

Unified CM は、メディア サービスが使用されていない単一クラスタにおける、2 つの Cisco Unified IP Phone の間のコールの、認証、完全性、および暗号化をサポートしています。ただし、すべてのデバイスまたは電話機の認証、完全性、または暗号化を提供しているわけではありません。ご使用のデバイスがこれらの機能をサポートしているかどうかを判別するには、次の Web サイトで入手可能なマニュアルを参照してください。

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

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

アクセス セキュリティ

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

Voice VLAN と Video VLAN

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

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

Sony 社製および Tandberg 社製の SCCP エンドポイントは、Cisco Discovery Protocol（CDP）または 802.1Q VLAN ID タギングをサポートしません。したがって、標準的な環境では、音声 VLAN をネイティブ VLAN として使用するようにポートを手動で設定してある場合を除き、これらのデバイスはデータ VLAN に存在します。ソニー社製および Tandberg 社製のエンドポイントは、設定のダウンロードのために TFTP サーバと通信し、SCCP シグナリングのために Unified CM と通信し、RTP オーディオ/ビデオ メディア チャネルのために他のエンドポイントと通信します。したがって、データ VLAN と TFTP サーバの間で TFTP プロトコルを許可し、データ VLAN と Unified CM サーバの間で TCP ポート 2000 を許可し、データ VLAN と音声 VLAN の間で RTP メディア用の UDP ポートを許可する必要があります。

H.323 クライアント、Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）、およびゲートウェイは、H.323 プロトコルを使用して Unified CM と通信します。Unified CM H.323 トランク（H.225 やインタークラスタ トランクのほかに、RAS アグリゲーター トランク タイプなど）は、ウェルノウン TCP ポート 1720 ではなくランダムなポート範囲を使用します。したがって、これらのデバイスと Unified CM サーバの間で広範囲の TCP ポートを許可する必要があります。MCU とゲートウェイはインフラストラクチャ デバイスと見なされ、通常は Unified CM サーバに隣接するデータ センターに存在します。一方、H.323 クライアントは通常はデータ VLAN に存在します。

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

利点

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

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

欠点

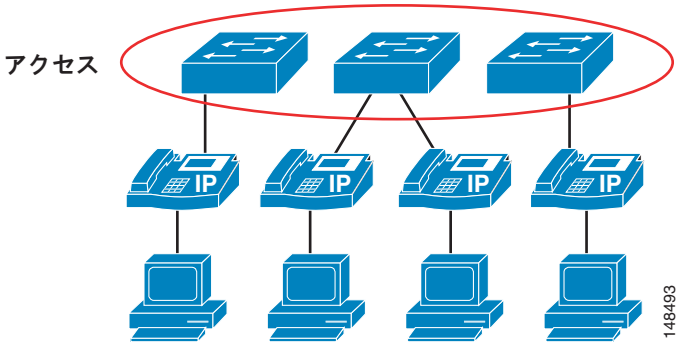
通常は電話機に送られる CDP メッセージから情報が収集され、その情報が一部のネットワークを検出するために使用される可能性があります。Unified CM で音声またはビデオ用に使用可能なすべてのデバイスが、音声 VLAN の検出に CDP を使用できるわけではありません。

スイッチ ポート

Cisco スイッチ インフラストラクチャには、データ ネットワークを保護するために使用できる多くのセキュリティ機能があります。この項では、ネットワーク内の IP テレフォニー データを保護するため、Cisco Access Switch で使用できるいくつかの機能について説明します（図 19-6 を参照）。この項では、現在のすべての Cisco スイッチで使用可能なすべてのセキュリティ機能について説明するのではなく、シスコが製造する多くのスイッチで使用されている一般的なセキュリティ機能をリストします。ネットワーク内に配置された特定の Cisco デバイスで使用可能なセキュリティ機能の追加情報については、次の Web サイトで入手可能な適切な製品マニュアルを参照してください。

http://www.cisco.com

図 19-6　電話機が接続される代表的なアクセス レイヤ設計



ポートセキュリティ：MAC CAM フラッディング

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

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

MAC フラッディング攻撃を抑制するには、ポート セキュリティまたはダイナミック ポート セキュリティのいずれかを使用できます。許可メカニズムとしてポート セキュリティを使用する必要がないカスタマーの場合、特定のポートに接続する機能に対応する数の MAC アドレスを持つダイナミック ポート セキュリティを使用できます。たとえば、1 台のワークステーションが接続されているポートの場合、取得する MAC アドレスの数を 1 に制限できます。1 台の Cisco Unified IP Phone と、その背後に 1 台のワークステーションが接続されているポートの場合、電話機の PC ポートに 1 台のワークステーションを接続するには、取得する MAC アドレスの数を 2 に設定できます（1 つは IP Phone 用、1 つは電話機の背後にあるワークステーション用）。以前であれば、トランク モードでポートを設定する

旧来の方法により、この場合の設定は 3 つの MAC アドレスになります。電話機ポートの設定でマルチ VLAN アクセス モードを使用する場合、この場合の設定は 2 つの MAC アドレスになります。1 つは電話機用、1 つは電話機に接続された PC 用です。PC ポートに接続するワークステーションがない場合、そのポートの MAC アドレスの数は 1 に設定する必要があります。これらの設定は、スイッチ上のマルチ VLAN アクセス ポート用です。トランク モードに設定されているポート（電話機と PC が接続されているアクセス ポートでは推奨されていない配置）では、設定が異なる場合があります。

ポート セキュリティ：ポート アクセスの防止

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

この期間は、固定タイマーまたは非活動タイマー（非持続アクセス）のいずれかで決定するか、永続的に割り当てることができます。永続的に MAC アドレスを割り当てる機能は、Cisco 6000 スイッチでは*自動設定*と呼ばれ、Cisco Catalyst 4500、2550、2750、または 2950 スイッチでは*スティッキ*と呼ばれます。どちらの場合も、スイッチのリロードまたはリブートが発生しても、取得された MAC アドレスはポートで保持されます。

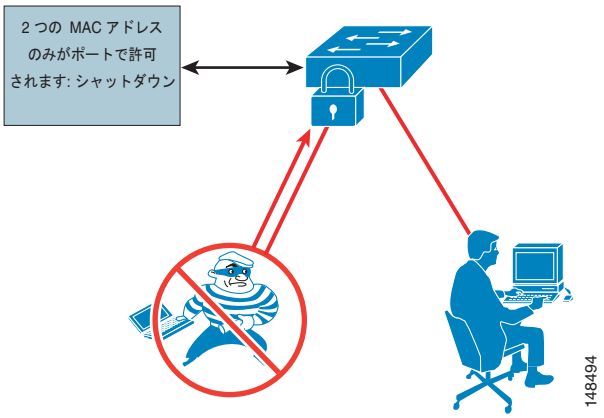
自動設定またはスティッキを使用した永続的な MAC アドレス割り当ては、コマンドを使用すればクリアできます。現在、Cisco Catalyst スイッチング プラットフォーム全体で最も一般的なデフォルト動作は、非持続動作です。この動作は、Cisco CatOS Release 7.6（1）が持続的になる前に、唯一有効だった動作です。デバイス モビリティに対し、スタティック ポート セキュリティまたは持続性のあるダイナミック ポート セキュリティによるプロビジョニングは行われません。最重要の要件ではありませんが、MAC フラッディング攻撃は、特定の MAC アドレスへのアクセスを制限することを目的としているポート セキュリティにより暗黙的に防止されます。

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

ポート セキュリティ：不良ネットワーク拡張の防止

ハブまたは無線アクセス ポイント（AP）を経由する不良なネットワーク拡張を防止します。ポート セキュリティは 1 つのポートでの MAC アドレスの数を制限するので、ポート セキュリティを、IT で作成されたネットワークへのユーザ拡張を抑制するためのメカニズムとして使用することもできます。たとえば、ユーザ方向のポート、または単一の MAC アドレス用にポート セキュリティが定義された電話機のデータ ポートに、ユーザが無線 AP を接続した場合、無線 AP 自体がその MAC アドレスを占有し、背後にあるデバイスはネットワークにアクセスできません（図 19-7 を参照）。一般的に、MAC フラッディングを停止するのに適切な設定は、不良アクセスを抑制するためにも適切です。

図 19-7　MAC アドレス数の制限による不良ネットワーク拡張の防止



利点

ポート セキュリティは、攻撃者がスイッチの CAM テーブルに対してフラッディングを実行したり、すべての受信 6 トラフィックをすべてのポートに送信するハブに VLAN を転送したりするのを防止します。また、エンドポイントにハブまたはスイッチを追加することにより、認可されていないネットワークの拡張を防止します。

欠点

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

設定例

（注）　この設定例は、これらの機能をサポートするために適切なコード レベルを実行しているスイッチに基づいています。電話機へのトランク モードは実行されません。

次の例は、データ ポートにデバイスが接続されている電話機に対して、ダイナミック ポート セキュリティを使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

```
switchport access vlan 10
switchport mode access
switchport voice vlan 20
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

（注）　電話機ファームウェア リリース（電話ロード）8.3(3) を適用すると、Link Layer Discovery Protocol（LLDP）機能がサポートされるようになります。LLDP を認識しない **switchport port-security maximum** コマンドと組み合わせて使用すると、スイッチポートでセキュリティ違反が発生する場合があります。これは、許可される MAC アドレス上限数を LLDP に対応するように設定することで回避できます。LLDP に関する問題は電話機の起動時に発生します。LLDP をサポートしないスイッチによって電話機から送信された LLDP パケットは異なる固有の MAC アドレスとして認識され、設定した許可されている MAC アドレス数の 1 つとして数えられます。LLDP を認識するスイッチは LLDP トラフィックを固有な MAC アドレスとして認識しないためこの問題は発生しません。http://www.cisco.com でお使いの電話機負荷と Cisco Unified Communications Manager の組み合わせとお使いのスイッチ モデルとソフトウェアバージョンが LLDP サポートしているかを確認してください。

上記の例のコマンドは、次の機能を実行します。

- **switchport port-security** *x/x* **enable**

  このコマンドは、指定したモジュール/ポートでポート セキュリティを有効にします。

- **switchport port-security violation restrict**

  このコマンドが、推奨されている設定です。デフォルトでは、ポートを無効にします。ポートを **restrict** すると、ポートは、MAC アドレスの最大数に達するまで MAC アドレスを取得し、その後は新しい MAC アドレスの取得を停止します。ポートの設定がデフォルトの **disable** の場合、MAC アドレスの最大数に達すると、ポートはエラーを無効化し、電話機の電源を切ります。ポートを再有効化するデフォルト タイマーは、5 分です。導入済みのセキュリティ ポリシーによっては、ポートを無効にすることにより電話機をシャットダウンせずに、ポートを制限した方が適切な場合があります。

- **switchport port-security aging time 2**

  このコマンドは、MAC アドレスからのトラフィックがない状態で、その MAC アドレスをポートで保持する時間を設定します。一部のスイッチと電話機の間の CDP 通信を考慮に入れると、推奨されている最小時間は 2 分です。

- **switchport port-security aging type inactivity**

  このコマンドは、取得した MAC アドレスをタイムアウトするために、ポートで使用されるエージングのタイプを定義します。

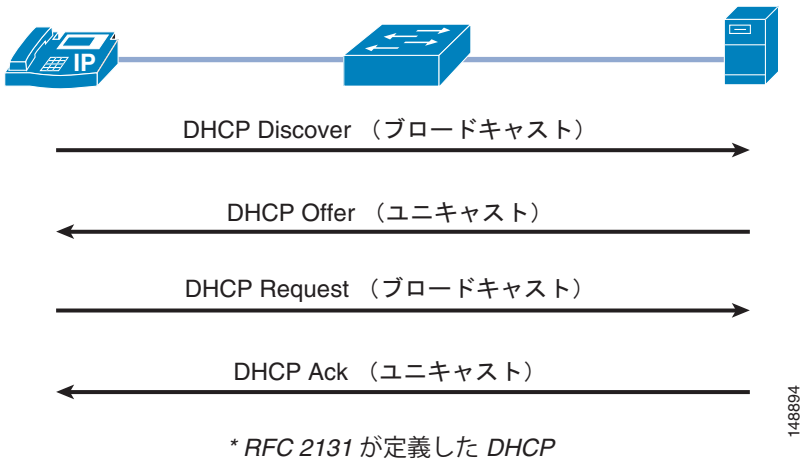
DHCP スヌーピング：不正な DHCP サーバ攻撃の防止

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

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

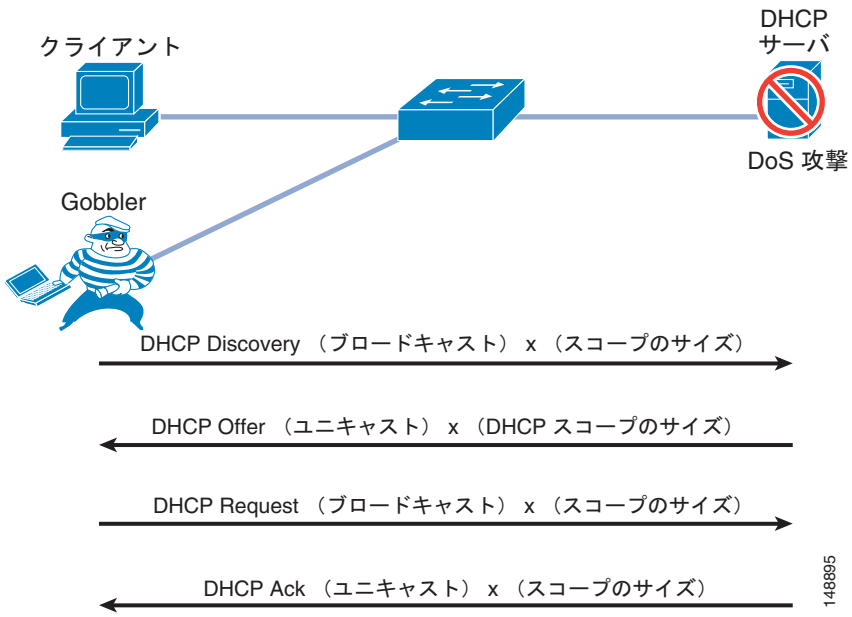
図 19-8 は、DHCP サーバに IP アドレスを要求するネットワーク接続デバイスの通常の操作を示しています。

図 19-8　DHCP 要求の通常の操作



ただし、攻撃者は、単一の IP アドレスではなく、VLAN 内で使用可能なすべての IP アドレスを要求できます（図 19-9 を参照）。これは、ネットワークへのアクセスを試みている正当なデバイスのための IP アドレスが存在しないことを意味します。IP アドレスがないと、電話機は Unified CM に接続できません。

図 19-9　攻撃者は VLAN で使用可能なすべての IP アドレスを取得できる



利点

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

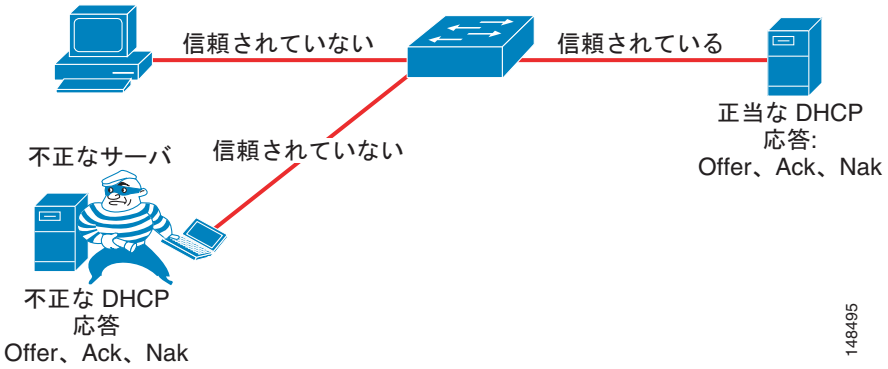
欠点

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

DHCP スヌーピング：DHCP スターベーション攻撃の防止

Gobbler などのツールを使用した DHCP アドレス スコープ スターベーション攻撃は、DHCP DoS 攻撃（サービス拒絶攻撃）を仕掛けるために使用されます。Gobbler ツールは、ランダムに生成される異なる送信元 MAC アドレスから DHCP 要求を実行するので、ポート セキュリティを使用して MAC アドレスの数を制限することにより、Gobbler ツールが DHCP アドレス スペースをスタービングするのを防止できます（図 19-10 を参照）。ただし、高度な DHCP スターベーション ツールでは、1 つの送信元 MAC アドレスから DHCP 要求を実行でき、DHCP ペイロード情報も多様です。DHCP スヌーピングを有効にすると、信頼されていないポートで、送信元 MAC アドレスと DHCP ペイロード情報が比較され、それらが一致しない場合は要求が失敗します。

図 19-10　DHCP スヌーピングを使用した DHCP スターベーション攻撃の防止



利点

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

欠点

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

設定例

次の例は、データ ポートにデバイスが接続されている電話機に対して、DHCP スヌーピングを使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

- グローバル コマンド

```
ip dhcp snooping vlan 10, 20
no ip dhcp snooping information option
ip dhcp snooping
```

- インターフェイス コマンド

```
no ip dhcp snooping trust (Default)
ip dhcp snooping limit rate 10 (pps)
ip dhcp snooping trust
```

上記の例のグローバル コマンドは、次の機能を実行します。

- **ip dhcp snooping vlan 10, 20**

  このコマンドは、DHCP スヌーピングが有効になっている VLAN を特定します。

- **No ip dhcp snooping information option**

  DHCP アドレスをリースするのに Option 82 情報が要求されないようにするため、このコマンドを使用する必要があります。Option 82 情報は DHCP サーバでサポートされている必要がありますが、ほとんどの企業サーバは、この機能をサポートしていません。Option 82 は Cisco IOS DHCP サーバでサポートされています。

- **ip dhcp snooping**

  このコマンドは、スイッチで、グローバル レベルでの DHCP スヌーピングを有効にします。

上記の例のインターフェイス コマンドは、次の機能を実行します。

- **no ip dhcp snooping trust**

  このコマンドは、DHCP サーバからポートに着信する情報をすべて信頼しないようにインターフェイスを設定します。

- **ip dhcp snooping limit rate 10**

  このコマンドは、DHCP スヌーピングが最初に設定されるときにインターフェイスで設定される、デフォルトのレート制限を設定します。この値は、導入済みのセキュリティ ポリシーに合せて変更できます。

- **ip dhcp snooping trust**

  このコマンドは、DHCP サーバから DHCP 情報を送信するときに経由するポートに対して実行します。DHCP 情報の送信元のポートを信頼できない場合、いずれのデバイスも DHCP アドレスを受信しません。この情報がクライアントに到達するようにするには、DHCP サーバが接続されている最低 1 つのポート（アクセス ポートまたはトランク ポート）を設定する必要があります。このコマンドは、固定 IP アドレスが与えられていて、IP アドレスを取得するために DHCP を使用しないポートに接続されている、任意のデバイスを信頼するためにも使用できます。DHCP サーバへのアップリンク ポート、または DHCP サーバへのトランク ポートも信頼する必要があります。

DHCP スヌーピング：バインディング情報

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

次の例は、DHCP スヌーピングからのバインディング情報を示しています。

- Cisco IOS のバインディング情報の表示

```
show ip dhcp snooping binding
MacAddress          IpAddress    Lease(sec)    Type            VLAN Interface
----------          ---------    ----------    -------------   ---- ---------
00:03:47:B5:9F:AD   10.120.4.10      193185    dhcp-snooping   10   FastEthernet3/18
```

- Cisco CatOS のバインディング情報の表示

```
ngcs-6500-1> (enable) show dhcp-snooping bindings
MacAddress          IpAddress       Lease(sec)      VLAN      Port
------------------  --------------- ----------      ----      -----
00-10-a4-92-bf-dd   10.10.10.21          41303      10        2/5
```

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

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

Dynamic ARP Inspection の要件

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

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

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

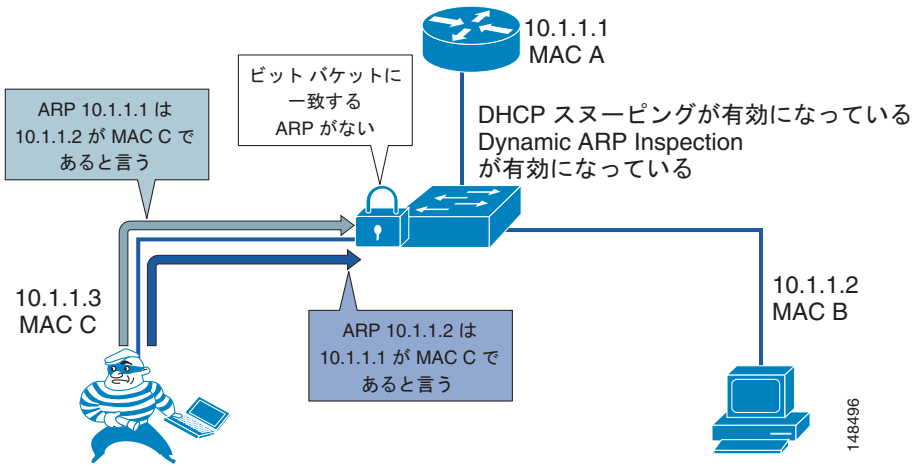
ただし、Gratuitous ARP は、別のステーションの身分を不正にかたること目的とした悪質なプログラムにより悪用される可能性もあります。悪質なステーションが、相互に通信しているその他の 2 つのステーションのトラフィックを自らにリダイレクトすると、GARP メッセージを送信したハッカーが中間者になります。ettercap などのハッカー プログラムは、このことを精密に行うため、GARP メッセージをブロードキャストするのではなく、「プライベートな」GARP メッセージを特定の MAC アドレスに発行します。これにより、攻撃の犠牲者は、自分のアドレスに対する GARP パケットを見ることが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

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

DAI の使用

Dynamic ARP Inspection（DAI）では、ARP 応答または Gratuitous ARP メッセージを正当化するために、DHCP バインディングが存在している必要があります。ホストで、アドレスを取得するための DHCP が使用されていない場合、そのホストを信頼するか、ホストの IP アドレスと MAC アドレスを対応付けるために ARP 検査用のアクセス コントロール リスト（ACL）を作成する必要があります（図 19-11 を参照）。DHCP スヌーピングと同様、DAI は VLAN ごとに有効化されます。すべてのポートは、デフォルトで、信頼できないポートとして定義されます。DAI で DHCP スヌーピングからのバインディング情報を活用するには、DAI を有効化する前に、VLAN で DHCP スヌーピングを有効化する必要があります。DAI を有効化する前に DHCP スヌーピングを有効化しないと、VLAN 内のいずれのデバイスも、ARP を使用して、デフォルト ゲートウェイを含む VLAN 内の他のデバイスに接続できません。その結果、VLAN 内のすべてにデバイスに対するサービスを、自ら拒否することになります。

図 19-11　　DHCP スヌーピングおよび DAI を使用した ARP 攻撃の防止



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

利点

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

欠点

この機能が正しく設定されていないと、認定ユーザへのネットワーク アクセスが拒否される場合があります。DHCP スヌーピング バインディング テーブルにデバイスのエントリがない場合、そのデバイスでは、ARP を使用してデフォルト ゲートウェイに接続できず、そのためトラフィックを送信できません。固定 IP アドレスを使用する場合、これらのアドレスを DHCP スヌーピング バインディング

テーブルに手動で入力する必要があります。リンクがダウンのときに、DHCP を再度使用して IP アドレスを取得することをしないデバイスがある場合（一部の UNIX または Linux マシンはこのように動作します）、DHCP スヌーピング バインディング テーブルをバックアップする必要があります。

設定例

次の例は、DHCP スヌーピングおよび Dynamic ARP Inspection を使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

- グローバル コマンド

```
ip dhcp snooping vlan 10,20 (required)
no ip dhcp snooping information option (required without option 82 dhcp server)
ip dhcp snooping (required)
ip arp inspection vlan 10,20
ip dhcp snooping database tftp://172.26.168.10/tftpboot/cisco/ngcs-dhcpdb
```

- インターフェイス コマンド

```
ip dhcp snooping trust
ip arp inspection trust
no ip arp inspection trust (default)
ip arp inspection limit rate 15 (pps)
```

上記の例のグローバル コマンドは、次の機能を実行します。

- **ip arp inspection vlan 10,20**

  このコマンドは、Dynamic ARP Inspection（DAI）が有効になっている VLAN を特定します。

- **ip arp inspection trust**

  ip dhcp snooping trust と同様、このコマンドは、ルータなどの信頼済みデバイスが ARP メッセージに応答するのを許可します。このコマンドは、使用するルータ用のポートで設定する必要があります。そのように設定しないと、ルータは DHCP スヌーピング バインディング テーブルに含まれないので、ルータはいずれの ARP 要求にも応答できません。

- **no ip arp inspection trust**

  この設定は、VLAN 上のすべてのポートのデフォルト設定です。信頼を有効にする必要があります。

- **ip arp inspection limit rate 15 (pps)**

  このコマンドは、インターフェイス上の ARP メッセージで許可されている、1 秒あたりのパケット数の最大数のグローバル デフォルト値を設定します。この値を超えると、インターフェイスは無効になります。この動作が問題になる場合は、制限を増加または減少させるか、**none** に設定することができます。

- **ip dhcp snooping database tftp://172.26.168.10/tftpboot/cisco/ngcs-dhcpdb**

  このコマンドは、DHCP スヌーピング バインディング テーブルのバックアップを TFTP サーバに作成します。DHCP スヌーピング バインディング テーブルは、ブートフラッシュ、FTP、RCP、スロット 0、および TFTP にバックアップできます。

上記の例のインターフェイス コマンドは、次の機能を実行します。

- **no ip arp inspection trust**

  このコマンドは、ポート上で DAI を有効にし、DHCP スヌーピング バインディング テーブルを基にすべての ARP をチェックします。

- **ip arp inspection limit rate 15 (pps)**

  このコマンドは、インターフェイス上の ARP メッセージで許可されている、1 秒あたりのパケット数の最大数を指定します。インターフェイスが、指定された数を超える ARP メッセージを 1 秒間に受信する場合、ポートは無効化されます。導入済みのセキュリティ ポリシーによっては、デ

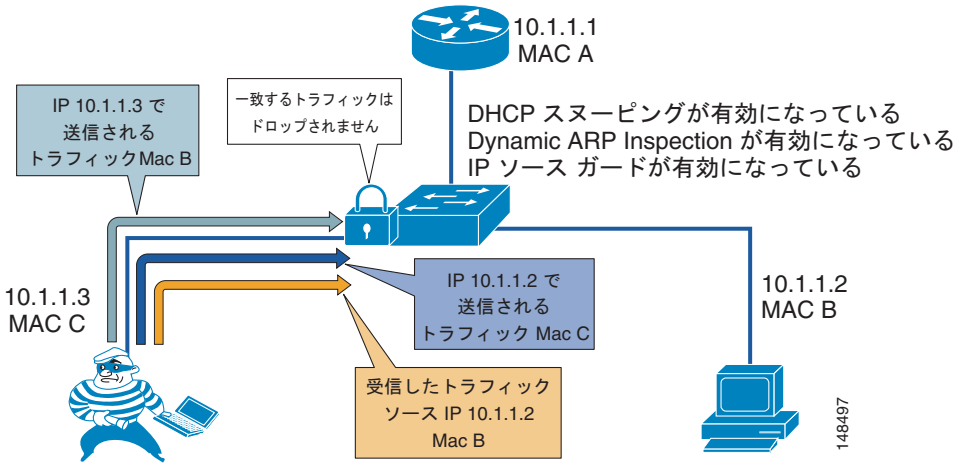
フォルト値（15 pps）が最適な設定の場合があります。1 秒間に 15 個を超える ARP メッセージをポートが受信するときに電話機を無効化しない場合は、レート制限を **none** に設定できます。この設定では、電話機は有効なままです。

IP ソース ガード

ARP スプーフィングに加えて、攻撃者は IP アドレス スプーフィングも仕掛ける場合があります。この方法は、セカンド パーティに対して DoS 攻撃を行うときに一般的に使用されます。この方法ではサード パーティを介してパケットが送信されるため、攻撃システムの ID がマスクされます。単純な例として、攻撃者は、攻撃先のセカンド パーティの IP アドレスを送信元にしながら、サードパーティ システムに ping することがあります。ping の応答は、サードパーティ システムからセカンド パーティに転送されます。スプーフィングされた IP アドレスを基にしたアグレッシブ SYN フラッディングは、サーバを TCP ハーフセッションで氾濫させる別の一般的なタイプの攻撃です。

IP ソース ガード（IPSG）機能を呼び出すと、DHCP スヌーピング バインディング テーブルの内容に基づいて ACL が動的に作成されます。この ACL は、トラフィックの送信元が DHCP バインディング時に発行された IP アドレスであることを保証し、スプーフィングされた他のアドレスによりトラフィックが転送されるのを防止します。DHCP スヌーピングは IP ソース ガードの前提条件ですが、DAI は前提条件ではありません。ただし、IP アドレス スプーフィングに加えて ARP ポイズニングおよび中間者攻撃を防止するため、IP ソース ガードだけでなく DAI も有効にすることをお勧めします（図 19-12 を参照）。

図 19-12　IP ソース ガードを使用したアドレス スプーフィングの防止



IP アドレス スプーフィングを使用すると、攻撃者は、アドレスを手動で変更するか、アドレス スプーフィングを行うように設計された hping2 などのプログラムを実行することにより、有効なアドレスになりすますことができます。インターネット ワームは、送信元を偽装するためスプーフィング技法を使用する場合があります。

設定例

次の例は、IP ソース ガードを使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

- IP ソース ガードを有効にする前に有効にする必要があるコマンド

```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
```

- インターフェイス コマンド：このコマンドは、DHCP Option 82 を指定せずに IP ソース ガードを有効にします。

```
ip verify source vlan dhcp-snooping
```

追加情報

ネットワーク セキュリティに関する追加情報については、次の Web サイトで入手可能な Cisco マニュアルを参照してください。

- http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper0900aecd8015f0ae.shtml
- http://www.cisco.com/en/US/prod/collateral/wireless/wirelssw/ps1953/product_implementation_design_guide09186a00800a3016.pdf

Quality of Service（QoS）

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

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

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

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

利点

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

欠点

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

アクセス コントロール リスト

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

VLAN アクセス コントロール リスト

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

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

VLAN ACL の設定については、次の製品マニュアルを参照してください。

- Cisco Catalyst 3750 スイッチ

  http://www.cisco.com/en/US/products/hw/switches/ps5023/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 4500 シリーズ スイッチ

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 6500 シリーズ スイッチ

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

次の例は、Cisco 7960 IP Phone のトラフィックだけが VLAN でブートおよび機能するのを許可する、VLAN ACL を示しています（インライン コメントは、ACL の各行の目的を示しています）。この例の VLAN ACL は、Cisco Unified CM Release 4.1 で使用するポート用です。この例では、次の IP アドレス範囲を使用します。

- 電話機の範囲は 10.0.20.*
- サーバの範囲は 10.0.10.*
- ゲートウェイの範囲は 10.0.30.*
- デフォルト ゲートウェイは 10.0.10.2 および 10.0.10.3
- DNS サーバの IP アドレスは 10.0.40.3

（注） アプリケーションがアップデートされたとき、または OS がアップデートされたとき（またはその両方）、ポートは変更されます。この注意事項は、電話機を含む、ネットワーク内のすべての IP テレフォニー デバイスに適用されます。製品で使用されるポートの最新のリストを取得するには、ネットワーク上で実行している製品のバージョンに応じて適切なマニュアルを参照してください。『*Cisco Unified Communications Manager TCP and UDP Port Usage*』ガイドは http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html から入手できます。

```
20 permit udp host 10.0.10.2 eq 1985 any
30 permit udp host 10.0.10.3 eq 1985 any
!permit HSRP from the routers
40 permit udp any any eq bootpc
50 permit udp any any eq bootps
!permit DHCP activity
60 permit udp 10.0.10.0 0.0.0.255 range 32768 61000 10.0.20.0 0.0.0.255 eq tftp
70 permit udp 10.0.20.0  0.0.0.255 range 1024 5000 10.0.10.0 0.0.0.255 range 32768 61000
80 permit udp 10.0.10.0 0.0.0.255 range 32768 61000 10.0.20.0  0.0.0.255 range 1024 5000
!permit the tftp traffic from the tftp server and phone
90 permit udp 10.0.10.0 0.0.0.255 range 32768 61000 host 10.0.40.3 eq domain
100 permit udp host 172.19.244.2 eq domain 10.0.10.0 0.0.0.255 range 32768 61000
!permit DNS to and from the phone
110 permit tcp 10.0.10.0 0.0.0.255 range 32768 61000 10.0.20.0  0.0.0.255 eq 2000
120 permit tcp 10.0.20.0  0.0.0.255 eq 2000 10.0.10.0 0.0.0.255 range 32768 61000
!permit signaling to and from the phone.
130 permit udp 10.0.10.0 0.0.0.255 range 16384 32767 10.0.10.0 0.0.0.255 range 16384 32767
140 permit udp 10.0.0.0 0.0.255.255 range 16384 32767 10.0.10.0 0.0.0.255 range 16384
32767
150 permit udp 10.0.10.0 0.0.0.255 range 16384 32767 10.0.0.0 0.0.255.255 range 16384
43767
!permit all phones to send udp to each other
160 permit tcp 10.0.10.0 0.0.0.255 range 32768 61000 10.0.20.0  0.0.0.255 eq www
170 permit tcp 10.0.20.0  0.0.0.255 eq www 10.0.10.0 0.0.0.255 range 32768 61000
180 permit tcp 10.0.20.0  0.0.0.255 range 32768 61000 10.0.10.0 0.0.0.255 eq www
190 permit tcp 10.0.10.0 0.0.0.255 eq www 10.0.20.0  0.0.0.255 range 32768 61000
!permit web access to and from the phone
200 permit Intelligent Contact ManagementP any any
!allow all icmp - phone to phone, gateway to phone, and NMS to phone
220 permit udp 10.0.30.0 0.0.0.255 rang 16384 327676 10.0.10.0 0.0.0.255 rang 16384 32767
!permit udp to the gateways in the network for pstn access
```

この ACL の例が示しているとおり、ネットワーク内で適切に定義された IP アドレスは、ACL を配置することを容易にします。

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

- Cisco Catalyst 3750 スイッチ

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

- Cisco Catalyst 4500 シリーズ スイッチ

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

- Cisco Catalyst 6500 シリーズ スイッチ

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

利点

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

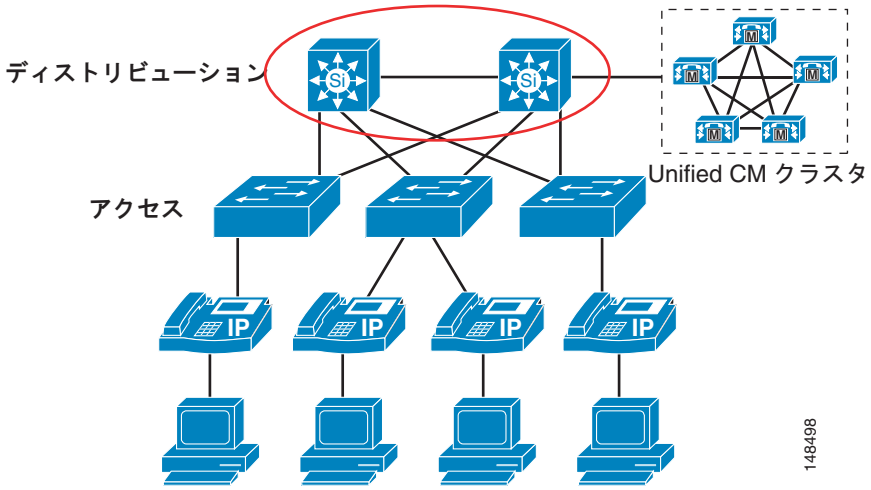
欠点

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

ルータのアクセス コントロール リスト

VLAN ACL と同様、ルータにも、ポートごとにインバウンド ACL およびアウトバウンド ACL の両方を処理する機能があります。最初のレイヤ 3 デバイスは、音声およびデータ VLAN を使用するときの音声データと別タイプのデータとの間の境界ポイントです。境界ポイントでは、2 つのタイプのデータが、相互にトラフィックを送信することが許可されます。VLAN ACL とは異なり、ルータ ACL は、ネットワーク内のすべてのアクセス デバイスには配置されません。その代わり、ネットワーク全体にルーティングするすべてのデータを準備する場所である、エッジ ルータで適用されます。これは、各 VLAN のデバイスがネットワーク内でアクセス可能なエリアを制御するために、レイヤ 3 ACL を適用するのに最適な場所です。レイヤ 3 ACL をネットワーク全体に配置することにより、トラフィックが収束する場所で、デバイスを相互に保護できます（図 19-13 を参照）。

図 19-13　　レイヤ 3 のルータ ACL



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

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

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

この例では、次の IP アドレス範囲を使用します。

- 電話機の範囲は 10.0.20.*
- IP テレフォニー サーバの範囲は 10.0.10.*
- ゲートウェイの範囲は 10.0.30.*
- ネットワーク内の他のすべてのデバイスの範囲は 192.168.*.*

```
10 deny ip 192.168.0.0 0.0.255.255 10.0.10.0 0.0.0.255
!deny all non voice devices to the voip servers
```

```
20 deny 192.168.0.0 0.0.255.255 10.0.30.0 0.0.0.255
!deny all non voice devices to the voip gateways
30 deny 192.168.0.0 0.0.255.255 10.0.20.0 0.0.0.255
!deny all non voice devices to communicate with the phones ip addresses
```

利点

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

欠点

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

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

ゲートウェイおよびメディア リソース

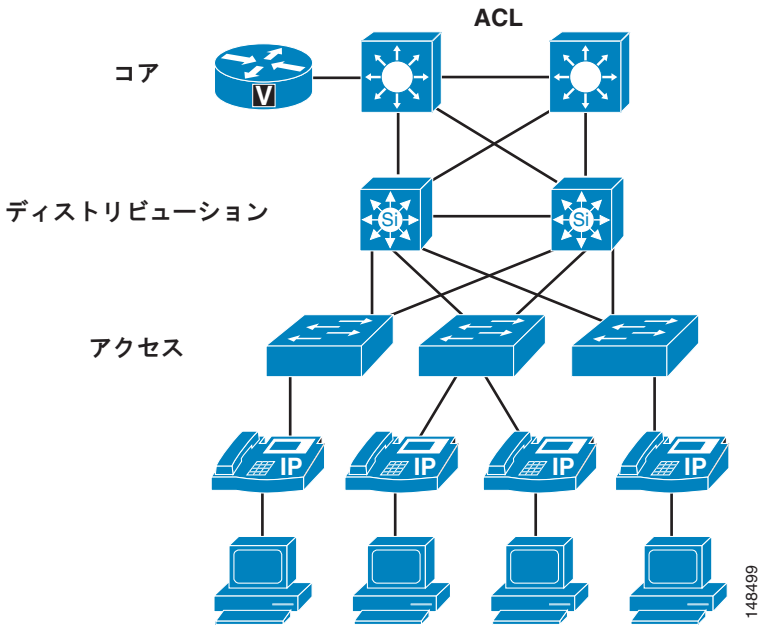
ゲートウェイおよびメディア リソースは、IP テレフォニー コールを公衆網コールに変換するデバイスです。外部コールがかけられた場合、ゲートウェイまたはメディア リソースは、IP テレフォニー ネットワークにおいてすべての音声 RTP ストリームが流れる数少ない場所の 1 つです。

IP テレフォニー ゲートウェイおよびメディア リソースは、ネットワーク内のほぼすべての場所に配置できるので、導入済みのセキュリティ ポリシーによっては、IP テレフォニー ゲートウェイまたはメディア リソースを保護することが、他のデバイスを保護することより難しいと見なされる場合があります。しかし、ネットワーク内のどこで信頼が確立されているかによりますが、ゲートウェイおよびメディア リソースを簡単に保護できる場合もあります。ゲートウェイおよびメディア リソースが Unified CM により制御される方法が関係していますが、シグナリングがゲートウェイまたはメディア リソースに到達するために通るパスがネットワーク内で安全と見なされている部分にある場合、単純な ACL を使用して、ゲートウェイまたはメディア リソースに送る、またはそこから戻るシグナリングを制御することができます。ゲートウェイ（またはメディア リソース）と Unified CM のロケーションの間のネットワークが安全と見なされない場合は（ゲートウェイがリモートの支店に置かれている場合など）、インフラストラクチャを使用してゲートウェイおよびメディア リソースへの IPSec トンネルを構築することにより、シグナリングを保護できます。ほとんどのネットワークでは、通常、2 つの方式（ACL および IPSec）の組み合せにより、これらのデバイスが保護されています。

H.323 ビデオ会議デバイスでは、ネットワークのどの H.323 クライアントからでも H.225 トランクのためにポート 1720 をブロックするように、ACL を記述できます。この方法では、ユーザが互いに H.225 セッションを直接開始するのをブロックします。シスコ デバイスでは H.225 にさまざまなポートを使用する場合があるので、どのポートが使用されるかを確認するには、使用する機器の製品マニュアルを参照してください。可能であれば、シグナリングの制御に必要な ACL が 1 つだけになるように、ポートを 1720 に変更します。

ここでは、ネットワークのエッジで QoS を使用しているので、攻撃者が Voice VLAN に侵入してゲートウェイおよびメディア リソースの場所を判別できた場合、ポートの QoS により、攻撃者がゲートウェイまたはメディア リソースに送信できるデータの量が制限されます（図 19-14 を参照）。

図 19-14　IPSec、ACL、および QoS を使用したゲートウェイおよびメディア リソースの保護



電話機で SRTP を有効にしている場合、一部のゲートウェイおよびメディア リソースでは、電話機からのゲートウェイ及びメディア リソースに対する Secure RTP（SRTP）をサポートします。ゲートウェイまたはメディア リソースが SRTP をサポートしているかどうかを判別するには、次の Web サイトで入手可能な適切な製品マニュアルを参照してください。

http://www.cisco.com

IPSec トンネルの詳細については、次の Web サイトで入手可能な『*Site-to-Site IPSec VPN Solution Reference Network Design（SRND）*』を参照してください。

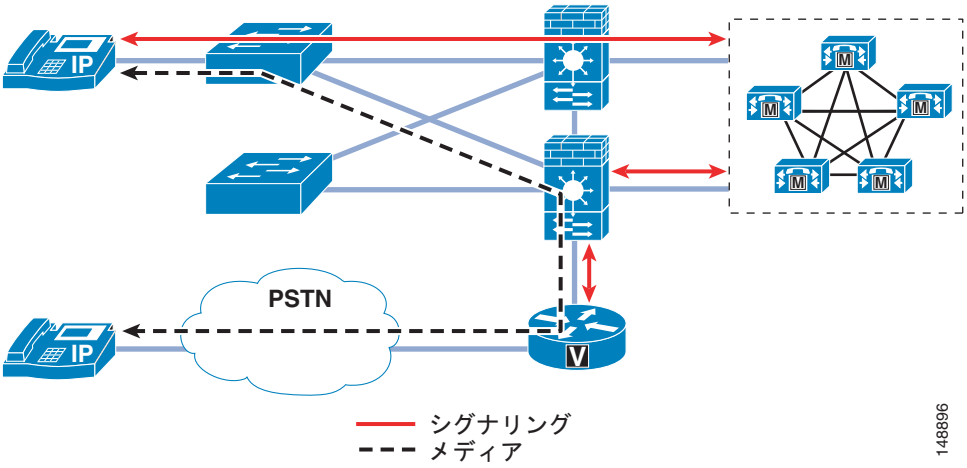
http://www.cisco.com/go/designzone

ゲートウェイの周囲へのファイアウォールの配置

コールの送信元である電話機と、公衆網ネットワークへのゲートウェイとの間にファイアウォールを配置する場合、注意が必要な問題が生じます。ステートフル ファイアウォールは、Unified CM、ゲートウェイ、および電話機の間のシグナリング メッセージの内容を参照し、コールの実行を許可するための RTP ストリーム用のピンホールを開けます。通常の ACL で同じことを行うには、RTP ストリームで使用されるポート範囲全体を、ゲートウェイに対して開放する必要があります。

ネットワーク内にゲートウェイを配置する方法は 2 つあります。つまり、ファイアウォールの背後に配置する方法と、ファイアウォールの前面に配置する方法です。ゲートウェイをファイアウォールの背後に配置する場合、そのゲートウェイを使用している電話機からのすべてのメディアは、ファイアウォールを通過する必要があります。また、これらのストリームがファイアウォールを通過するようにするには、追加の CPU リソースが必要です。次に、ファイアウォールでは、これらのストリームの制御が追加され、ゲートウェイが DoS 攻撃から保護されます（図 19-15 を参照）。

図 19-15　ファイアウォールの背後に配置されたゲートウェイ



ゲートウェイを配置する 2 番目の方法は、ファイアウォールの外側に配置する方法です。電話機からゲートウェイに送信される唯一のデータ タイプは RTP ストリームなので、そのゲートウェイに送信可能な RTP トラフィックの量は、アクセス スイッチの QoS 機能により制御されます。Unified CM からゲートウェイに送信されるのは、コールをセットアップするためのシグナリングだけです。ネットワーク内で、信頼できるエリアにゲートウェイが配置されている場合、Unified CM とゲートウェイの間で許可する必要がある唯一の通信は、そのシグナリングです（図 19-15 を参照）。RTP ストリームはファイアウォールを通過しないので、この配置方式では、ファイアウォールの負荷が低下します。

利点

ACL とは異なり、ほとんどのファイアウォール設定では、シグナリングがファイアウォールを経由している限り、Unified CM が電話機とゲートウェイに対して、それらの 2 つのデバイスの間で使用するように指示している RTP ストリーム ポートだけが開放されます。また、ファイアウォールには、DoS 攻撃用の追加機能や、対象トラフィックを参照して、攻撃者が禁止動作を行っていないかどうかを判別するための Cisco Intrusion Detection System（IDS）シグニチャがあります。

欠点

「ファイアウォール」（P.19-31）の項で説明するように、ファイアウォールが、電話機からゲートウェイへのすべてのシグナリングおよび RTP ストリームを調べる場合、キャパシティが問題になることがあります。また、音声データ以外のデータがファイアウォールを通過する場合、ファイアウォールを通過するコールがファイアウォールにより影響されないように、CPU 使用率を監視する必要があります。

ファイアウォールと H.323

H.323 は、エンドポイント間のメディア ストリームのセットアップ、および Unified CM と H.323 ゲートウェイ間でアクティブ状態と要求される接続時間の間、H.245 を利用します。以降のコール フローに対する変更には H.245 を使用します。

デフォルトではシスコファイアウォールによって H.245 セッションと関連するコールの RTP ストリームが追跡されます。また、RTP トラフィックが 5 分以上ファイアウォールを通過しない場合、H.245 セッションのタイムアウトも実行します。1 つ以上の H.323 ゲートウェイと他のエンドポイントがすべてファイアウォールの一方にあるトポロジでは、RTP トラフィックはファイアウォールによって認識されません。H.245 セッションは 5 分後にファイアウォールによってブロックされ、そのストリームの制御が停止されます。ただし、ストリーム自体には影響しません。この場合、付加サービスなどは利用できなくなります。

トポロジを利用するには、コマンド **timeout h323 [***hr:min:sec***]** を使用して、ファイアウォールのデフォルト動作を変更し、予想されるコール所要時間に十分な値を設定します。たとえば、朝一番からシフトが終わるまでパーマネント コールがスケジュールされているモバイル エージェントの所要時間を増加する場合です。この場合、所要時間にはエージェントのシフトを超過する値を設定します。

利点

デフォルトの値を変更することでエンドポイントすべてがファイアウォールに対して同じ側に存在している場合に H.323 がコールすべての機能を維持できるというメリットがあります。

欠点

タイムアウト機能はファイアウォール側にあるコール エージェントの保護を強化しますが、タイムアウトが増加するとこの機能の価値が低下します。

ファイアウォール

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

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

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

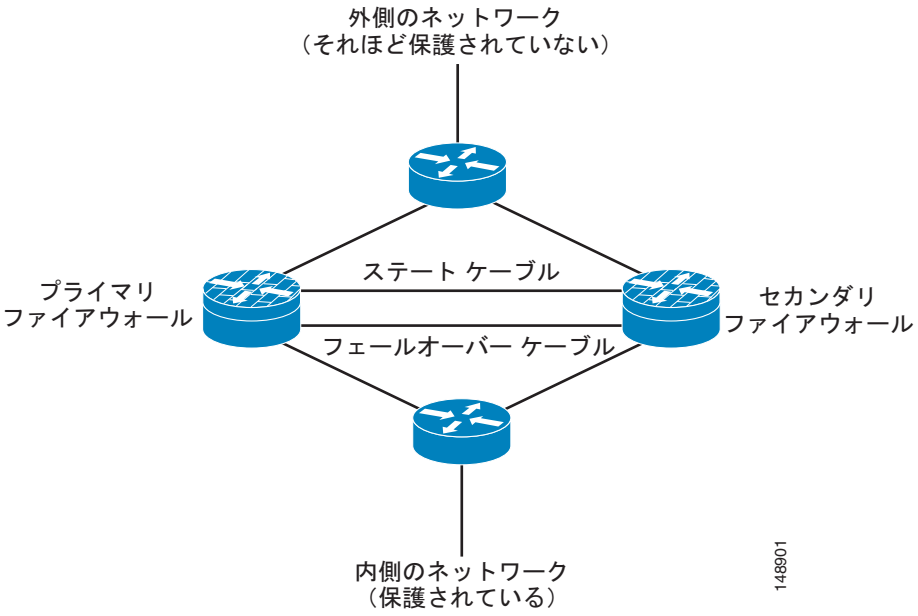
ファイアウォールを配置する方法はいくつもあります。この項では、ルーテッドおよびトランスペアレントの両方のシナリオにおける、アクティブ/スタンバイ モードの ASA、PIX、および FWSM について集中的に説明します。この項で説明する各設定は、ファイアウォール設定の音声セクション内で、シングル コンテキスト モードで設定されたものです。

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

ASA または PIX と FWSM の機能性の相違点

図 19-16 は、ネットワーク内の冗長ファイアウォールを論理的に表現しています。配置方法は、ルーテッド設定とトランスペアレント設定で同じです。

図 19-16　冗長ルーテッドまたは透過ファイアウォール



Cisco Adaptive Security Appliance（ASA）および Cisco Private Internet Exchange（PIX）は、Cisco Firewall Cisco Firewall Services Modules（FWSM）とは異なる方法で動作します。ASA または PIX 内では、より信頼性が高いインターフェイスに ACL がない限り、そのインターフェイスからのすべてのトラフィックは信頼され、そこから出て、より信頼性が低いインターフェイスに到達することが許可されます（図 19-17 を参照）。たとえば、ASA の内部インターフェイスまたはデータ センター インターフェイスからのすべてのトラフィックは、ASA から出て、ASA の外部インターフェイスに到達することが許可されます。ASA/PIX 上のより信頼性の高いインターフェイスに任意の ACL を適用すると、他のすべてのトラフィックは拒否（DENY）され、ファイアウォールは FWSM と同様に機能するようになります（図 19-18 を参照）。

図 19-17　Cisco ASA または PIX の機能

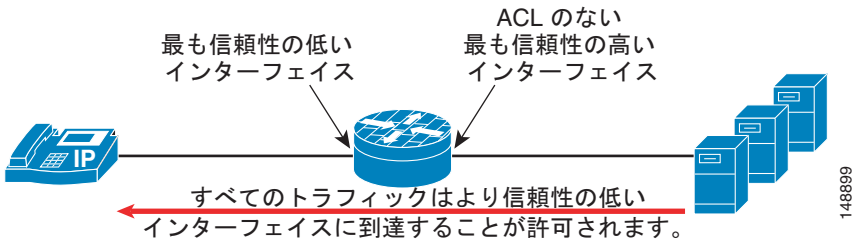
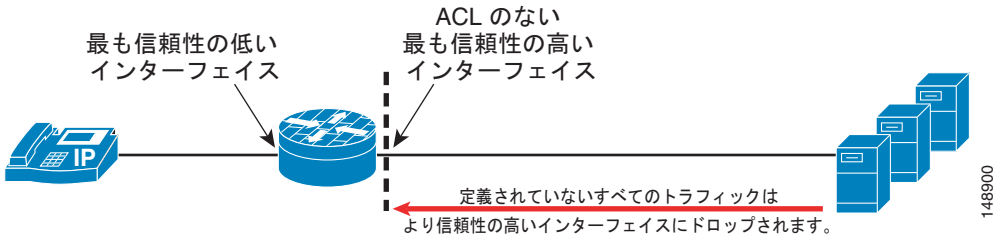


図 19-18　Cisco FWSM の機能



ファイアウォールの全般的な利点

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

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

ファイアウォールの全般的な欠点

ファイアウォールでは、すべての IP テレフォニー アプリケーション サーバまたはアプリケーションがサポートされているわけではありません。ファイアウォール、またはファイアウォール内の ALG でサポートされていない一部のアプリケーションには、Cisco Unity ボイスメール サーバ、Attendant Console、Cisco Unified Contact Center Enterprise、および Cisco Unified Contact Center Express が含まれます。トラフィックがファイアウォールを経由して流れるのを許可するため、これらのアプリケーション用の ACL を書き込むことができます。

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

バージョン 3.0 よりも前の Cisco FWSM では、SCCP フラグメンテーションがサポートされていません。電話機、Unified CM、またはゲートウェイから別の IP テレフォニー デバイスに送信される SCCP パケットが断片化されている場合、断片化されたパケットが FWSM を通過するのは許可されません。断片化が、バージョン 2.*x* のコードを実行する FWSM で発生した場合、シグナリング トラフィック用

のファイアウォールの ALG 機能を使用せずに、ACL を使用する必要があります。この設定では、FWSM を通過するシグナリング トラフィックが許可されますが、シグナリングがファイアウォールを通過するときにパケットの検査は実行されません。

他のアプリケーションが SCCP と同じポート（TCP 2000）を使用している場合、他のアプリケーションが SCCP インスペクションの影響を受ける場合があります。SCCP TCP ポートに送信されるトラフィックはすべて SCCP トラフィックであるかがインスペクションされます。SCCP トラフィックではない場合、トラフィックはドロップされます。

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

http://www.cisco.com

ルーテッド ASA および PIX

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

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

利点

ルーテッド ASA または PIX ファイアウォールは、QoS、NAT、およびボックスへの VPN 終端をサポートしています。これらの機能は、トランスペアレント モードではサポートされていません（「トランスペアレント ASA および PIX」（P.19-35）を参照）。

図 19-16 は、アクティブ スタンバイ モードのルーテッド設定とトランスペアレント設定の両方における、ファイアウォールの論理配置を示しています。ルーテッド設定では、ASA または PIX 上の各インターフェイスに IP アドレスが与えられます。トランスペアレント モードでは、ASA または PIX をリモートで管理するための IP アドレスの他には、インターフェイス上に IP アドレスは与えられません。

欠点

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

トランスペアレント ASA および PIX

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

利点

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

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

欠点

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

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

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

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

ASA TLS プロキシ機能

この機能によって ASA ファイアウォールに暗号化音声シグナリングをインスペクションする機能が追加されます。エンドポイント デバイスに暗号化シグナリングが設定されている場合はシグナリングをインスペクションできないため、アプリケーション レイヤ ゲートウェイによって NAT フィックスアップなどの機能を実行できません。シグナリングを TLS プロキシ機能経由で送信することで ASA で TLS セッションに参加できます。これにより、ASA はシグナリング ストリームを解読して必要なフィックスアップなど実行した上で再びシグナリングを暗号化します。

ASA ファイアウォールを IP 電話機と ASA ファイアウォールが登録されている Unified CM の間に設置すると TLS プロキシが TLS セッションに挿入されます。暗号化シグナリングが設定された電話機では TLS を電話機と Unified CM のトランスポートとして使用します。TLS プロキシを使用する場合、1 つの電話機登録に対して 2 つの TLS セッションが存在します。1 つは電話機と ASA の間、もう 1 つは ASA と Unified CM の間です。

ASA はシグナリングのインスペクションが可能なため、ALG を備えた唯一のファイアウォールで、暗号化シグナリングのコールを制御する方法が装備されています。

VPN 設計がリモート電話機の安全性を確保する最適なソリューションではない場合、ASA がデバイスを保護する代替方法です。

TLS プロキシは電話機で使用される Certificate Trust List（CTL）に信頼されるエンティティとして追加されています。CTL ファイルには電話機との信頼関係が求められるすべてのサーバを含む 16 のエントリを格納することができます。したがって、特定のクラスタで使用できる設定された TLS プロキシ数は Certificate Trust List のエントリ残数によって制限されます。

ASA および PIX の設定例

次の設定例は、ファイアウォールが ASA および PIX ソフトウェア Release 7.04 の音声に対して動作するように設定するための、ポートおよび **inspect** コマンドをリストしています。これはあくまでも例にすぎません。任意のファイアウォールを配置する前に、ネットワーク内で使用されているすべてのアプリケーションから取得したポート リストを確認する必要があります。この設定例は、音声セクションのみを示しています。

```
!
!
object-group service remote-access tcp
 description remote access
 !Windows terminal
 port-object range 3389 3389
 !VNC
 port-object range 5800 5800
 !VNC
 port-object range 5900 5900
 port-object range 8080 8080
 port-object eq ssh
 !SSH
 port-object eq ftp-data
 !FTP data transport
  port-object eq www
 !HTTP Access
 port-object eq ftp
 !FTP
 port-object eq https
 !HTTPS Access
object-group service voice-protocols-tcp tcp
 description TCP voice protocols
 CTI/QBE
```

```
 port-object range 2428 2428
 !SIP communication
 port-object eq ctiqbe
 !SCCP
 port-object range 2000 2000
 !Secure SCCP
 port-object range 2443 2443
object-group service voice-protocols-udp udp
 !TFTP
 port-object eq tftp
 !MGCP Signaling
 port-object range 2427 2427
 !DNS
 port-object eq domain
 !RAS
 port-object range 1719 1719
 !SIP

!Object Group applied for remote-access
access-list OUTSIDE extended permit tcp any any object-group remote-access
!Object Group applied for voice-protocols-tcp
access-list OUTSIDE extended permit tcp any any object-group voice-protocols-tcp
!Object Group applied for voice-protocols-udp
access-list OUTSIDE extended permit udp any any object-group voice-protocols-udp
! Object Group applied for remote-access
access-list inside_access_in extended permit tcp any any object-group remote-access
! Object Group applied for voice-protocols-tcp
access-list inside_access_in extended permit tcp any any object-group voice-protocols-tcp
! Object Group applied for voice-protocols-udp
access-list inside_access_in extended permit udp any any object-group voice-protocols-udp

!Failover config
ip address 172.19.245.3 255.255.255.248 standby 172.19.245.4
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
!Lowest and fastest setting for failover
failover polltime interface 3
failover link failover_state GigabitEthernet0/2
failover interface ip failover 192.168.1.1 255.255.255.0 standby 192.168.1.2
failover interface ip failover_state 192.168.0.1 255.255.255.0 standby 192.168.0.2

!
!Default inspection with inspects enabled
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect h323 h225
  inspect h323 ras
  inspect skinny
  inspect sip
  inspect tftp
  inspect mgcp
```

FWSM ルーテッド モード

ルーテッド モードでは、FWSM がネットワークのルータ ホップと見なされます。このモードでは、接続されているネットワークの間で NAT が実行されます。また、OSPF またはパッシブ RIP（シングル コンテキスト モード）を使用できます。ルーテッド モードでは、コンテキストあたり最大 256 個のインターフェイスがサポートされています。シングル モードでは、すべてのコンテキストの合計で最大 1,000 個のインターフェイスがサポートされています。

利点

ネットワーク内のルーテッド デバイスとして、FWSM は、ルーティング機能、およびトランスペアレント モードで使用可能でない他のすべての機能をサポートしています。

欠点

トランスペアレント モードとは異なり、ルーテッド デバイスはネットワーク上で参照することができ、それが原因で攻撃ポイントになる場合があります。ネットワークにデバイスを配置するには、IP アドレッシングとルーティングの設定を変更する必要があります。

FWSM トランスペアレント モード

トランスペアレント モードでは、FWSM は「Bump In The Wire」または「ステルス ファイアウォール」として動作し、ルータ ホップではありません。FWSM はインターフェイスの内側と外側で同じネットワークに接続しますが、各インターフェイスは異なる VLAN に置かれている必要があります。ダイナミック ルーティング プロトコルまたは NAT は必要ありません。ただし、ルーテッド モードと同様、トランスペアレント モードでも、トラフィックの通過を許可する ACL が必要です。トランスペアレント モードでは、オプションで EtherType ACL を使用して、非 IP トラフィックを許可することもできます。トランスペアレント モードでは、内側インターフェイスと外側インターフェイスの 2 つのインターフェイスのみがサポートされています。

透過ファイアウォールを使用すると、ネットワーク設定を簡素化できます。トランスペアレント モードは、ファイアウォールを攻撃者から見えないようにするためにも便利です。ルーテッド モードではブロックされるトラフィックのために、透過ファイアウォールを使用することもできます。たとえば、透過ファイアウォールで、EtherType ACL を使用したマルチキャスト ストリームを許可できます。

利点

この設定には、ファイアウォールがルーティングを一切行わないため、攻撃者がファイアウォールを見つけることができないという利点があります。この設定では、ファイアウォールに合せてルーティングを変更する必要がないので、より簡単に既存のネットワークにファイアウォールを配置できます。またこの設定は、ファイアウォール内でいずれのルーティングも行わないため、ファイアウォールの管理やデバッグも簡単に実行できます。また、非 IP トラフィックと IP マルチキャスト トラフィック、静的 ARP インスペクション、および MAC 移動検出と静的 MAC をブリッジできます。

欠点

トランスペアレント モードでフェールオーバーを使用するときにループを回避するには、Bridge Port Data Unit（BPDU）転送をサポートしているスイッチ ソフトウェアを使用し、BPDU を許可するように FWSM を設定する必要があります。トランスペアレント モードでは、NAT、ダイナミック ルーティング、またはユニキャストのリバース パス フォワーディング（RPF）チェックはサポートされていません。トランスペアレント モードの FWSM に NAT 0 はありません。

FWSM の設定例

次の設定例では、ファイアウォールを FWSM ソフトウェア Release 2.3.**x** の音声に対応させるために使用する、ポートと *inspect* コマンドをリストします。これは例にすぎないので、ファイアウォールを配置する前に、使用中のネットワークで使用されているすべてのアプリケーションからポートのリストを取得して確認する必要があります。この設定例は、音声セクションのみを示しています。

```
fixup protocol h323 H225 1720
!Enable fixup  h3232 h225

fixup protocol h323 ras 1718-1719
!Enable fixup h323 RAS

fixup protocol mgcp 2427
!Enable fixup  mgcp

fixup protocol skinny 2000
!Enable fixup

fixup protocol tftp 69
!Enable fixup

object-group service VoiceProtocols tcp
  description Unified CM Voice protocols
  port-object eq ctiqbe
  port-object eq 2000
  port-object eq 3224
  port-object eq 2443
  port-object eq 2428
  port-object eq h323
!Defining the ports for TCP voice

object-group service VoiceProtocolsUDP udp
  description UDP based Voice Protocols
  port-object range 2427 2427
  port-object range 1719 1719
  port-object eq tftp
!Defining the ports for UDP voice

object-group service RemoteAccess tcp
  description Remote Acces
  port-object range 3389 3389
  port-object range 5800 5809
  port-object eq ssh
  port-object range 5900 5900
  port-object eq www
  port-object eq https
!Defining remote access TCP ports

access-list inside_nat0_outbound extended permit ip any any
!

access-list phones_access_in extended permit tcp any any object-group RemoteAccess log
notifications interval 2
access-list phones_access_in extended permit tcp any any object-group VoiceProtocols log
notifications interval 2
access-list phones_access_in extended permit udp any any object-group VoiceProtocolsUDP
log notifications interval 2
access-list phones_access_in extended deny ip any any log notifications interval 2
access-list outside_access_in extended permit tcp any any object-group VoiceProtocols log
notifications interval 2
```

```
access-list outside_access_in extended permit tcp any any object-group RemoteAccess log
notifications interval 2
access-list outside_access_in extended permit udp any any object-group VoiceProtocolsUDP
log notifications interval 2
!Access lists applying the object groups defined above for inside and outside interfaces

access-list outside_access_in extended deny ip any any log notifications interval 2
access-list inside_access_in extended deny ip any any
!Deny all other traffic

access-list phones_nat0_outbound extended permit ip any any
!

failover
failover lan unit primary
failover lan interface flan vlan 4050
failover polltime unit 1 holdtime 5
failover polltime interface 15
!Failover config - 15 seconds
failover interface-policy 50%
failover link flin vlan 4051
failover interface ip flan 1.1.1.1 255.255.255.252 standby 1.1.1.2
failover interface ip flin 1.1.1.5 255.255.255.252 standby 1.1.1.6
nat (inside) 0 access-list inside_nat0_outbound_V1
access-group outside_access_in in interface outside
access-group inside_access_in in interface inside
```

データ センター

データ センター内では、IP テレフォニー アプリケーション サーバで必要なセキュリティについて、セキュリティ ポリシーを定義する必要があります。Cisco Unified Communications サーバは IP に基づいているので、データ センター内にある、時間に敏感なほかのデータに適用するセキュリティを、これらのサーバにも適用することができます。

データ センターの間で WAN でのクラスタ化が使用されている場合、データ センター内とデータ センター間の両方に適用されている追加のセキュリティは、クラスタ内のノード間で許可されている最大往復時間に収まる必要があります。ネットワーク内のアプリケーション サーバ用に導入されている現在のセキュリティ ポリシーに、Cisco IP テレフォニー サーバが含まれている場合、そのセキュリティを使用する必要があります。また、すでに配置されている任意のインフラストラクチャ セキュリティを使用することもできます。

データ アプリケーションに適したデータ センター セキュリティを設計するには、次の Web サイトで入手可能な『*Data Center Networking: Server Farm Security SRND*』（『*Server Farm Security in the Business Ready Data Center Architecture*』）のガイドラインに従うことをお勧めします。

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

アプリケーション サーバ

Unified CM セキュリティ機能のリスト、および有効にする方法については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Security Guide*』を参照してください。

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

任意の Unified CM セキュリティ機能を有効にする前に、それらの機能が、ネットワーク内のこれらのタイプのデバイスに関する企業セキュリティ ポリシーで指定されている、セキュリティ要件を満たしていることを確認してください。

Unified CM およびアプリケーション サーバ上の Cisco Security Agent

Cisco Security Agent は、IP テレフォニーおよび IP テレフォニー サービスを提供するのにシスコが使用するアプリケーション サーバのほとんどで使用されています。Cisco Security Agent ソフトウェアは、サーバとの間のトラフィックの動作と、サーバ上でアプリケーションが実行される方法を調べて、すべてが正常かどうかを判別する、ホスト侵入防御ソフトウェアです。異常と見なされるものが見つかった場合、Cisco Security Agent ソフトウェアはそのアクティビティが発生するのを阻止します。

管理対象外 Cisco Security Agent

シスコは、自社サーバ用のデフォルト Cisco Security Agent ポリシーを開発しました。このポリシーにより、IP テレフォニー サーバで必要なすべての機能は正しく機能し、同時に、既知および不明な攻撃が IP テレフォニー サーバに影響することは防止されます。このソフトウェアは、アプリケーションとオペレーティング システムを、ウイルスやワーム攻撃から保護します。これらのタイプの侵入からの最大限の保護を得るには、常に最新バージョンの Cisco Security Agent ソフトウェアがサーバにインストールされていることを確認してください。管理対象外エージェントがサーバにインストールされていると、攻撃のログは、エージェントがインストールされているシステムでのみ参照できます。特定のタイプのアラームが発生したので書き込まれた可能性があるログ ファイルをチェックするには、各システムにログインする必要があります。管理対象外 Cisco Security Agent はデフォルトで Unified CM のインストール時にインストールされます。

利点

管理対象外 Cisco Security Agent は、既知および不明の攻撃、ワーム、およびウイルスから各システムを保護します。

欠点

Cisco Security Agent を管理対象外モードで実行すると、アラームは相関されません。システムのログ ファイルを参照するには、各システムに個別にアクセスする必要があります。

管理対象 Cisco Security Agent

（注） Cisco Unified CM 7.*x* では現在、管理対象 Cisco Security Agent 機能はサポート*されません*。

アンチウイルス

（注） Cisco Unified CM 7.*x* では現在、アンチウイルス ソフトウェアはサポート*されません*。

サーバに関する一般的なガイドライン

Unified CM およびその他の IP テレフォニー アプリケーション サーバは、通常のサーバとして扱わないでください。システムの設定時に行う任意の操作が、開始を試みているコール、または進行中のコールに影響する場合があります。他のビジネスクラス アプリケーションと同様、大規模な設定の変更は、電話の会話を遮断することがないようメンテナンス時間帯で行う必要があります。

アプリケーション サーバ用の標準的なセキュリティ ポリシーは、IP テレフォニー サーバには不十分な場合があります。電子メール サーバや Web サーバとは異なり、音声サーバでは、画面をリフレッシュしたり、メッセージを再送信したりすることは許可されていません。音声通信は、リアルタイムのイベントです。IP テレフォニー サーバ用のセキュリティ ポリシーでは、音声システムの設定または管理に関連付けられていない作業が、IP テレフォニー サーバで決して行われないことを保証する必要があります。ネットワーク内のアプリケーション サーバで通常のアクティビティと見なされるアクティビティ（インターネット サーフィンなど）でも、IP テレフォニー サーバで行うことはできません。

また、シスコは IP テレフォニー サーバ用に適切に定義されたパッチ システムを提供しています。IT 組織内のパッチ ポリシーに基づいて、このパッチ システムを適用する必要があります。シスコシステムズにより承認されている場合を除き、OS ベンダーのパッチ システムを使用する通常の方法でシステムにパッチを適用しないでください。すべてのパッチは、シスコシステムズの指示に従ってシスコまたは OS ベンダーからダウンロードし、パッチ インストール プロセスに応じて適用する必要があります。

セキュリティ警告を受け取るには、次の Web サイトでシスコの通知サービスに加入してください。

http://www.cisco.com/cisco/support/notifications.html

（注）　このリンクにアクセスするには、Cisco.com ログイン アカウントが必要です。

上記のサイトには、IP テレフォニー サーバに重要なパッチを適用する必要が生じたときに電子メールで通知する通知ツールも含まれています。

利点

アプリケーション サーバを他のアプリケーション サーバのようではなく PBX のように扱う場合、一般的なサーバ セキュリティ プラクティスを実施すると、ウイルスやワームを減らすのに役立ちます。

欠点

追加のセキュリティ機能を設定すると、一部の Unified CM 機能が低下する場合があります。また、アップグレードを正常に実行するには、追加のセキュリティで無効になっている一部のサービスを有効にする必要があるため、アップグレード中は特に注意が必要です。

配置例

この項では、ロビーに設置された電話機およびファイアウォールの配置について、セキュリティ面を考慮した実施例を示します。このようなタイプと同様の配置を扱うには、適切なセキュリティ ポリシーを適用する必要があります。

ロビーに設置された電話機の例

この項の例は、物理的なセキュリティが低いロビー エリアのようなエリアで使用する、電話機およびネットワークを設定する 1 つの方法を示しています。この例に出てくる機能は、いずれもロビーに設置する電話機で要求されている機能ではありませんが、導入済みのセキュリティ ポリシーで、より強固なセキュリティが必要とされている場合は、この例でリストされている機能を使用できます。

いずれのユーザも電話機の PC ポートからネットワークにアクセスできないようにするため、電話機の背面の PC ポートを無効にして、ネットワーク アクセスを制限する必要があります（「電話機の PC ポート」（P.19-6）を参照）。また、攻撃を仕掛けようとしている人が、ロビーに設置された電話の接続先ネットワークの IP アドレスを参照できないように、電話機の設定ページも無効にする必要があります（「アクセス設定」（P.19-9）を参照）。電話機の設定を変更できないという欠点は、通常、ロビーに設置された電話機では問題になりません。

ロビーに設置された電話機が移動される可能性は非常に低いため、電話機には固定 IP アドレスを使用できます。固定 IP アドレスを使用すると、攻撃者が電話機を切断して接続することにより新しい IP アドレスを取得するのを防止できます（「IP アドレッシング」（P.19-5）を参照）。また、電話機が抜かれると、ポートの状態が変化し、電話機は Unified CM から登録解除されます。ロビーに設置された電話機のポートでこのイベントをトラッキングするだけで、だれかがネットワークへの接続を試行しているかどうかを判別できます。

電話機のスタティック ポート セキュリティを使用し、MAC アドレスを取得することを許可しない場合、攻撃者は、そのアドレスを発見できたときに、自らの MAC アドレスをその電話機の MAC アドレスに変更しなければなりません。ダイナミック ポート セキュリティを無制限タイマーと共に使用して、MAC アドレスを取得する（取得したアドレスは解除しない）場合、MAC アドレスを追加する必要はありません。これにより、電話機を交換しない限り、MAC アドレスをクリアするためにスイッチポートを変更せずにすみます。MAC アドレスは、電話機の底面のラベルにリストされています。MAC アドレスをリストすることがセキュリティの問題と見なされる場合は、ラベルを除去し、デバイスを識別するための Lobby Phone というラベルに置き換えることができます（「スイッチ ポート」（P.19-13）を参照）。

ポートまたはポートが接続されているスイッチに関する情報を攻撃者がイーサネット ポートから参照できないように、単一の VLAN を使用し、ポートで Cisco Discovery Protocol（CDP）を無効にできます。この場合、電話機の E911 緊急コール用のスイッチに CDP エントリは与えられません。緊急番号をダイヤルするときは、ロビーに設置された各電話機に、ラベル、またはローカル セキュリティ用の情報メッセージのいずれかが必要です。

ポート上に DHCP は存在しないため、DHCP スヌーピング バインディング テーブルに静的エントリを定義できます（「DHCP スヌーピング：不正な DHCP サーバ攻撃の防止」（P.19-16）を参照）。DHCP スヌーピング バインディング テーブルに静的エントリを定義すると、VLAN で Dynamic ARP Inspection を有効にして、攻撃者が、ネットワーク上のレイヤ 2 ネイバーの 1 つに関する他の情報を取得するのを防止できます（「Dynamic ARP Inspection の要件」（P.19-20）を参照）。

DHCP スヌーピング バインディング テーブルに静的エントリが定義されていると、IP ソース ガードを使用できます（「IP ソース ガード」（P.19-23）を参照）。攻撃者が MAC アドレスと IP アドレスを取得でき、パケットの送信を開始した場合、正しい IP アドレスが設定されたパケットだけを送信できます。

電話機が動作するのに必要なポートと IP アドレスのみを許可する、VLAN ACL を書き込むことができます（「VLAN アクセス コントロール リスト」（P.19-25）を参照）。次の例には、ネットワークへのアクセスを制御するための、レイヤ 2 または最初のレイヤ 3 デバイスのポートに適用可能な非常に小規模な ACL が含まれています（「ルータのアクセス コントロール リスト」（P.19-27）を参照）。この例は、ロビー エリアで使用されている Cisco 7960 IP Phone に基づいています。電話機への Music on Hold または電話機からの HTTP アクセスは使用しません。

この例では、次の IP アドレス範囲を使用します。

- ロビーに設置された電話機の IP アドレスは 10.0.40.5
- Unified CM クラスタのアドレス範囲は 10.0.20.*
- DNS サーバの IP アドレスは 10.0.30.2
- HSRP ルータの IP アドレスは 10.0.10.2 および 10.0.10.3
- ネットワーク内の他の電話機の IP アドレスの範囲は 10.0.*.*

```
10 permit icmp any any
! Allow all icmp - phone to phone, gateway to phone and NMS to phone

20 permit udp host 10.0.10.2 eq 1985 any
!Allow HSRP information in, do not allow out

30 permit udp host 10.0.10.3 eq 1985 any
! Allow in from HSRP neighbor

40 permit udp host 10.0.40.5 range 32768 61000 10.0.20.0 0.0.0.255 eq tftp
! Using ip host from ephemeral port range from phone to the TFPT server  port 69 (start of
tftp)

50 permit udp 10.0.20.0 0.0.0.255 range 1024 5000 host 10.0.40.5 range 32768 61000
!Using IP subnet from TFTP server with ephemeral port range to ip host and ephemeral port
range for phone

60 permit udp host 10.0.40.5 range 32768 61000 10.0.20.0 0.0.0.255 range 1024 5000
! Using host from phone to TFTP server with ephemeral port range to ip range and ephemeral
port range for TFTP (continue the TFTP conversation)

70 permit udp host 10.0.40.5 range 32768 61000 host 10.0.30.2 eq domain
! Using IP host and ephemeral port range from phone to DNS server host

80 permit udp host 10.0.30.2 eq domain host 10.0.40.5 range 32768 61000
! Using IP from DNS server to phone host ip and ephemeral port range

90 permit tcp 10.0.40.5 range 32768 61000 10.0.20.0 0.0.0.255 eq 2000
! Using IP host and ephemeral port range from phone to Unified CM cluster for SCCP


100 permit tcp 10.0.20.0 0.0.0.255 eq 2000 host 10.0.40.5 range 32768 61000
! Using IP range and SCCP port to phone IP host and ephemeral port range


110 permit udp 10.0.0.0 0.0.255.255 range 16384 32767 host 10.0.40.5 range 16384 32767
! Using IP range and ephemeral port range from all phones or gateways outside a vlan to
the IP host to phone

120 permit udp host 10.0.40.5 range 16384 32767 10.0.0.0 0.0.255.255 range 16384 43767
! Using IP host and ephemeral port range from vlan to all other phones or gateways

130 permit udp host 172.19.244.3 range 1024 5000 host 10.0.40.5 eq snmp
!From IP host of NMS server and ephemeral port range (Different for Windows vs Sun) to IP
host of phones and SNMP port (161)
```

```
140 permit udp host 10.0.40.5 eq snmp host 172.19.244.3 range 1024 5000
! From IP host of phone with SNMP port (161) to IP host of NMS server and ephemeral port
range
```

ロビーに設置された電話機用の基本的な QoS の例

音声ストリームを G.729 に設定し、ポートに送信可能なトラフィックの量を、QoS を使用して制限します（「Quality of Service（QoS）」（P.19-24）を参照）。QoS 最大値を超えても、トラフィックは、一般的な企業ネットワークで優先度が最低のトラフィックである CS1 つまり Scavenger Class にリセットされます。

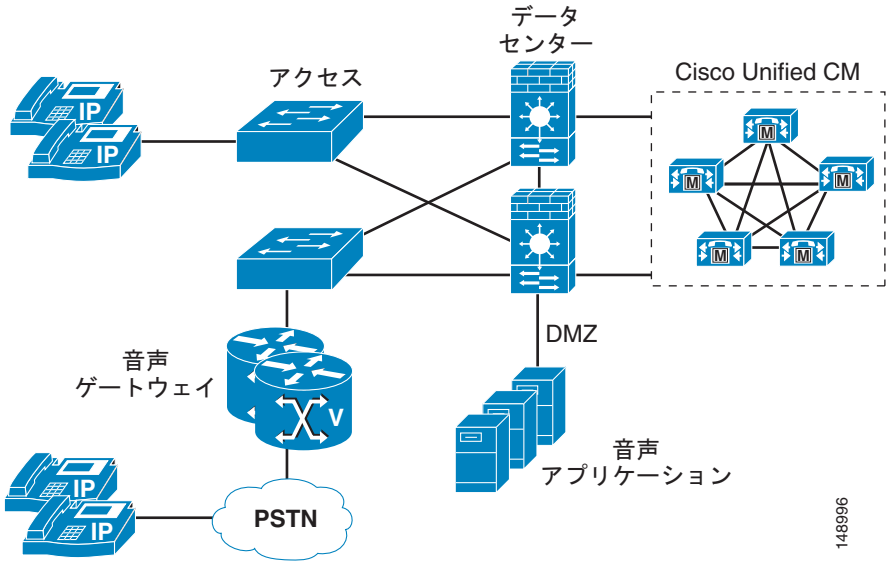
```
CAT2970(config)#mls qos map policed-dscp 0 24 46 to 8
! Excess traffic marked 0 or CS3 or EF will be remarked to CS1
CAT2970(config)#
CAT2970(config)#class-map match-all LOBBY-VOICE
CAT2970(config-cmap)# match access-group name LOBBY-VOICE
CAT2970(config-cmap)#class-map match-all LOBBY-SIGNALING
CAT2970(config-cmap)# match access-group name LOBBY-SIGNALING
CAT2970(config-cmap)#exit
CAT2970(config)#
CAT2970(config)#policy-map LOBBY-PHONE
CAT2970(config-pmap)#class LOBBY-VOICE
CAT2970(config-pmap-c)# set ip dscp 46 ! Lobby phone VoIP is marked to DSCP EF
CAT2970(config-pmap-c)# police 48000 8000 exceed-action policed-dscp-transmit
! Out-of-profile Lobby voice traffic (g.729) is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class LOBBY-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24 ! Signaling is marked to DSCP CS3
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
! Out-of-profile Signaling traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 56000 8000 exceed-action policed-dscp-transmit
! Out-of-profile data traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)#exit
CAT2970(config)#
CAT2970(config)#interface GigabitEthernet0/1
CAT2970(config-if)# service-policy input LOBBY-PHONE ! Applies policy to int
CAT2970(config-if)#exit
CAT2970(config)#
CAT2970(config)#ip access list extended LOBBY-VOICE
CAT2970(config-ext-nacl)# permit udp any any range 16384 32767 ! VoIP ports
CAT2970(config-ext-nacl)#
CAT2970(config-ext-nacl)#ip access list extended LOBBY-SIGNALING
CAT2970(config-ext-nacl)# permit tcp any any range 2000 2002 ! SCCP ports
CAT2970(config-ext-nacl)#end
CAT2970#
```

ファイアウォールの配置例（集中型配置）

この項の例は、データ センター内において、背後に Unified CM を配置するファイアウォールの 1 つの展開方法を示しています（図 19-19 を参照）。この例では、Unified CM は、すべての電話機がファイアウォールの外側から 1 つのクラスタに接続される集中型配置として置かれています。この配置内のネットワークには、社内データ センター内でルーテッド モードで設定されたファイアウォールがすでに含まれているので、ゲートウェイの配置を決定する前に負荷が確認されます。ファイアウォールの平均的な負荷を確認した後、CPU に対するファイアウォールの負荷を 60% 未満に保つため、すべての

RTP ストリームがファイアウォールを横断しないようにすることが決定されました（「ゲートウェイの周囲へのファイアウォールの配置」（P.19-29）を参照）。ゲートウェイはファイアウォールの外側に配置されています。Unified CM でゲートウェイとの間の TCP データ フローを制御するため、ネットワーク内の ACL を使用します。電話機の IP アドレスは適切に定義されているので、ACL は、電話機からの RTP ストリームを制御するためネットワークにも書き込まれます（「IP アドレッシング」（P.19-5）を参照）。音声アプリケーション サーバは非武装地帯（DMZ）に配置されています。Unified CM との間のアクセス、およびネットワーク上のユーザへのアクセスを制御するため、ファイアウォールで ACL を使用します。この設定では、インスペクションを使用してファイアウォールを通過する RTP ストリームの量を制限します。これにより、既存のネットワークに新しい音声アプリケーションを追加したときの、ファイアウォールに対する影響を最小限に抑えられます。

図 19-19　　ファイアウォールの配置例



ネットワーク バーチャライゼーションの保護

ここではバーチャル ネットワーク間の通信に同種接続を提供するのに伴う問題と、この問題を解決するための手法について説明します。バーチャル ルート フォワーディングとネットワーク バーチャライゼーションについての知識が必要です。これらのテクノロジーに関するネットワーク設計原理については、http://www.cisco.com/go/designzone で入手可能なネットワーク バーチャライゼーションの資料を参照してください。

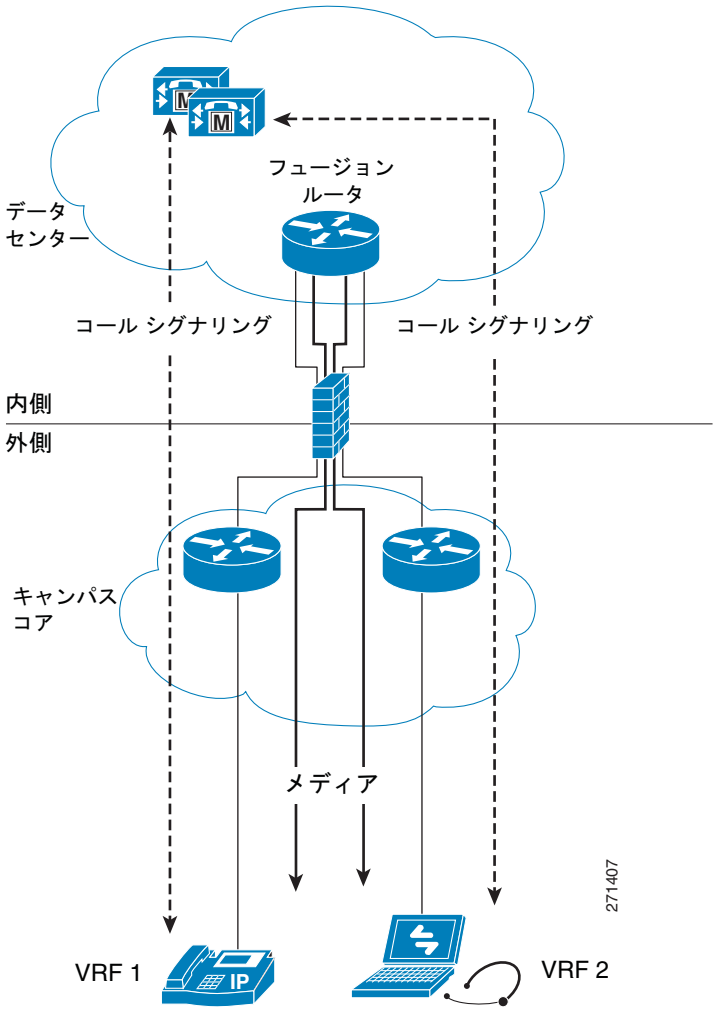
ここで紹介する内容は、バーチャライゼーションを使用した Unified Communication ソリューションのセキュリティの強化を保証するものではありません。既存のインフラストラクチャに Unified Communications レイヤに配置できる内容を説明することを目的としています。バーチャライゼーション テクノロジーのメリットとデメリットを評価するには、ネットワーク バーチャライゼーションに関する資料を参照してください。

バーチャライゼーション テクノロジーに基づいたネットワークでは、トラフィックがレイヤ 3 で論理的に区別され、バーチャル ネットワークにはそれぞれルーティング テーブルが存在します。ルーティング情報の欠如により、異なるバーチャル ネットワーク間では通信できません。この環境はユーザ エンドポイントがデータセンター内のデバイスとのみ通信するクライアントサーバ配置に最適ですが、ピアツーピア通信では問題が発生します。部門別、場所別、トラフィックのタイプ（データまたは音声）別など、バーチャル ネットワークの配置にかかわらず、異なるバーチャル プライベート ネットワーク ルーティングおよび転送（VRF）テーブルのエンドポイントに相互に通信する機能が備えられていな

いという問題の中核は変わりません。図 19-20 で示されているソリューションでは、ある VRF に設置されたソフトウェア ベースの電話機と別の VRF に設置されたハードウェア電話機との通信に、データセンターに設置された共有 VRF を使用しています。このソリューションは、他の異なる状況にも適用できるかもしれません。ネットワーク バーチャライゼーションで は、データセンターとキャンパス ネットワーク間の境界に対する、データセンターの防御を実装することが要求されます。以降では、この実装方法について説明します。

シナリオ 1：単一のデータ センター

図 19-20　単一のデータ センター



このシナリオは最も簡単に実装できます。通常のネットワーク バーチャライゼーション実装への増設として実装します。この設計では、パケットを任意の VRF にルーティングできる機能を備えたデータセンター ルータが組み込まれています。このルータはフュージョン ルータと呼ばれます（フュージョン ルータの構成に関する詳細については、ネットワーク バーチャライゼーションの資料を参照してください）。このピアツーピアの通信トラフィックを可能にする配置シナリオは、VRF 間のルーティングとデータ センターのセキュアなアクセスを実現するファイアウォール機能の役割をフュージョン ルータが担います。

このシナリオには、次の主な要件が適用されます。

- キャンパス ルータによってパケットがデフォルトのルーティング経由でフュージョン ルータに向けて他のキャンパス VRF に送信されます。つまり、すべてのルータ ホップはデフォルトでフュージョン ルータにルーティングされる必要があります。データ センターで共有されている VRF にはそれぞれのキャンパス VRF に関するルート情報が保持されています。共有 VRF を除くすべての VRF は直接接続されていません。
- Unified CM はデータ センターの共有 VRF に配置されています。共有 VRF 内の通信が妨げられることはありません。
- 共有 VRF はデータ センターに設置されています。複数のデータ センターが存在している場合は、共有 VRF はデータ センターすべてを網羅します。

データ センター側のアプリケーション レイヤ ゲートウェイによって TFTP と SCCP または外部から送信された SIP セッションをデータ センターの Unified CM クラスタ宛てに送信するポートを開放するアクセス リストが指定されます。TFTP は電話機が TFTP サーバから設定とソフトウェア イメージをダウンロードするのに必要です。また、電話機を Unified CM クラスタに登録するため、SCCP または SIP が必要です。使用される特定のソフトウェア バージョンに適切なポート番号については Unified CM の製品マニュアルを参照してください。

このシナリオでは、VRF それぞれの通信デバイスから送信されたコール シグナリングは、すべてアプリケーション レイヤ ゲートウェイを経由してシグナリングをインスペクションすることでアプリケーション レイヤ ゲートウェイが動的に必要な VRF それぞれの UDP ピンホールを開き、ファイアウォール外部から送信された RTP トラフィックをフュージョン ルータ宛てに通します。ファイアウォールでインスペクションされないと、外部エンドポイントから送信された RTP ストリームそれぞれはファイアウォールを通過できません。呼制御シグナリングのインスペクションにより、ファイアウォールを通じた UDP トラフィックのフォワーディングが可能になります。

利点

この配置モデルは、VRF 対応ネットワーク上で通信デバイスのピアツーピア接続を可能にします。アプリケーション レイヤ ゲートウェイによって共有 VLAN とフュージョン ルータに安全にアクセスすることができます。

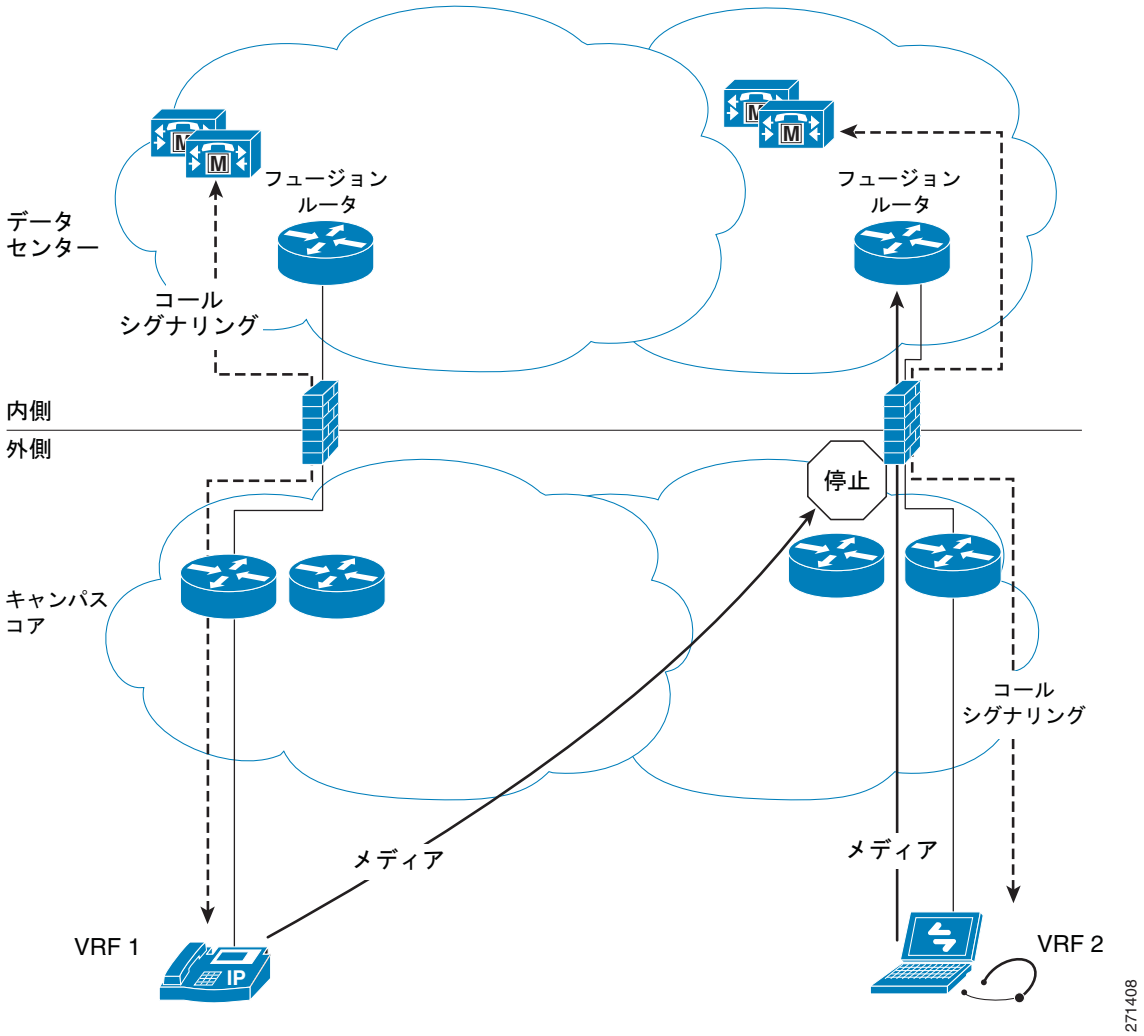
欠点

エンドポイント間の異なる VRF のメディア ストリームはすべて、最短パスを通過しません。メディアはフュージョン ルータ経由でルーティングされるためデータ センターにバックホールされます。

シナリオ 2：冗長なデータ センター

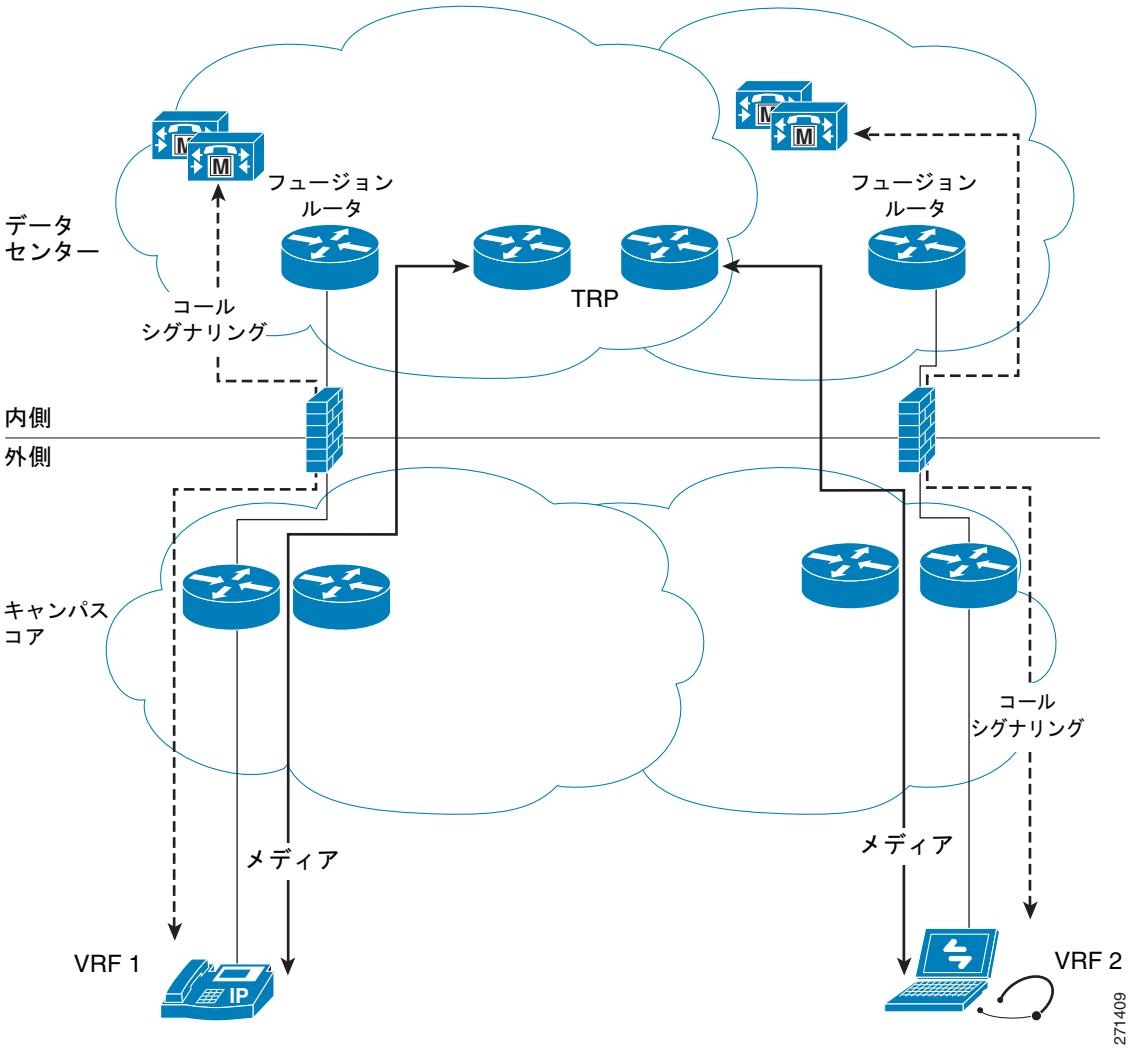
冗長なデータ センターの場合、シナリオは複雑化します。コール セットアップ シグナリングが対応する RTP ストリームによって使用される同一のアプリケーション レイヤ ゲートウェイを確実に通過するようにします。シグナリングとメディアが異なるパスを通過すると、UDP ピンホールが開かれません。図 19-21 は問題を抱えるシナリオの例を示します。左のハードウェア電話機は左のデータ センターのサブスクライバによって制御されています。対応する呼制御シグナリングは左のファイアウォールを通過します。RTP ストリームを通過させるため、このファイアウォールのピンホールが開かれています。しかし、このルーティングでは RTP メディア ストリームが必ず同じパスを通過するとは限りません。また、右のファイアウォールによってストリームはブロックされます。

図 19-21　異なるパスを通過するコール シグナリングとメディア



この問題を解決するには、Trusted Relay Point（TRP）機能を使用します（図 19-22 を参照）。データ センターそれぞれのサブスクライバは メディアを固定する TRP を起動して、メディア ストリームが適切なファイアウォールを確実に通過するようにします。左のデータ センター内のサブスクライバによって制御されている電話機が左データ センターの TRP を起動し、右のデータ センター内のサブスクライバによって制御されている電話機が右データ センターの TRP を起動する必要があります。TRP は、コール シグナリングとまったく同じルーティング パスを通過することを保証するメディアに対して、特定のホスト ルートを有効にする IP アドレスを提供します。このアドレスを使用してシグナリングとメディアは同じファイアウォールを通過するため、問題を解決することができます。

図 19-22　TRP を備えた冗長なデータ センター



TRP は、デバイスが利用されるコールでデバイス レベルで起動されるメディア ターミネーション ポイント リソースです。デバイスにはそれぞれ TRP を起動するかどうかを設定するチェックボックスがあります。

まとめ

この章では、ネットワーク内の音声データを保護するために有効にできるセキュリティのうち、一部のみを取り上げました。ここで取り上げた手法は、ネットワーク内のすべてのデータを保護するためにネットワーク管理者が使用できる、すべてのツールのサブセットにすぎません。逆に、ネットワーク全体のデータで必要なセキュリティのレベルによっては、これらのツールでさえ、ネットワークで有効にする必要がない場合もあります。セキュリティの方法は、注意深く選択してください。ネットワーク内のセキュリティが高くなると、それに応じて、複雑度や問題のトラブルシューティングも増加します。各企業の責任で、リスクと組織の要件の両方を定義し、ネットワークとネットワークに接続されたデバイスに適切なセキュリティを適用する必要があります。

CHAPTER 20

Unified Communications エンドポイント

この章では、さまざまなタイプの Unified Communications エンドポイントとその機能、および QoS 推奨事項について要約します。これらのエンドポイントは、次の主要なタイプに分類できます。

- 「アナログ ゲートウェイ」（P.20-3）
- 「Cisco Unified IP Phone」（P.20-8）
- 「ソフトウェアベースのエンドポイント」（P.20-18）
- 「無線エンドポイント」（P.20-20）
- 「Cisco Unified IP Conference Station」（P.20-26）
- 「ビデオ エンドポイント」（P.20-27）
- 「サードパーティ製 SIP IP Phone」（P.20-32）

上記の各項では、それぞれのエンドポイント タイプについて詳細情報を示します。加えて、「QoS の推奨事項」（P.20-33）の項では QoS 設定のリストを示し、「エンドポイント機能の要約」（P.20-48）の項ではエンドポイントの全機能のリストを示します。

この章の新規情報

表 20-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 20-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
Cisco IP Communicator	「Cisco IP Communicator」（P.20-19） 表 20-14
Cisco Unified Client Services Framework	「Cisco Unified Client Services Framework」（P.20-19）
Cisco Unified IP Phone 拡張モジュール	「Cisco Unified IP Phone 拡張モジュール 7914、7915、7916」（P.20-14）

表 20-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報 （続き）

新規トピックまたは改訂されたトピック	説明箇所
Cisco Unified IP Phones 6900 シリーズ	「Cisco Unified IP Phones 6900 シリーズの配置に関する考慮事項」（P.20-15） 「Cisco Unified IP Phone 6921」（P.20-9） 「Cisco Unified IP Phone 6941」（P.20-11） 「Cisco Unified IP Phone 6961」（P.20-10） 表 20-9 表 20-11
Cisco Unified IP Phones 8900 シリーズおよび 9900 シリーズ	「Cisco Unified IP Phone 8900 および 9900 シリーズの配置に関する考慮事項」（P.20-15） 「Cisco Unified IP Phone 8961」（P.20-13） 「Cisco Unified IP Phone 9951」（P.20-14） 「Cisco Unified IP Phone 9971」（P.20-14） 表 20-12
Cisco Unified SIP Phone 3911	「Cisco Unified SIP Phone 3911」（P.20-8） 表 20-8
Cisco Unified Wireless IP Phone 7925G	「無線エンドポイント」（P.20-20） 表 20-13
Cisco VG202 および VG204 ゲートウェイ	「Cisco VG202 および VG204 ゲートウェイ」（P.20-7） 表 20-6
電話機の機能	「エンドポイント機能の要約」（P.20-48）
Bluetooth デバイスのサポート	「Bluetooth のサポート」（P.20-26）

エンドポイントを選択する際の推奨事項

次のリストに、IP テレフォニー エンドポイントを選択する際の基本的な推奨事項の要約を示します。

- 低密度アナログ接続には、Cisco Analog Telephone Adapter（ATA）または低密度アナログ インターフェイス モジュールを使用する。
- 中密度から高密度のアナログ接続には、高密度アナログ インターフェイス モジュール、24-FXS ポート アダプタ搭載の Cisco Communication Media Module（CMM; コミュニケーション メディア モジュール）、Catalyst 6500 24-FXS アナログ インターフェイス モジュール、Cisco VG224、または Cisco VG248 を使用する。
- XML やその他の電話ベースのサービスをほとんど、あるいはまったく使用しない音声中心のユーザには、Cisco Unified IP Phones 6921、6941、および 6961 を使用する。
- トラフィックの発生量が少量で、コール機能に制限を受けるテレフォニー ユーザには、Cisco Unified SIP Phone 3911 または Cisco Unified IP Phone 7902G、7905G、7906G、7910G、7910G+SW、7911G、7912G、7912G-A を使用する。
- トラフィックの発生量が中程度で、トランザクション タイプのテレフォニー ユーザには、Cisco Unified IP Phone 7931G、7940G、7941G、7941G-GE、7942G、または 7945G を使用する。

- テレフォニー トラフィックの発生量が中程度から大量の、マネージャおよびアシスタントには、Cisco Unified IP Phone 7960G、7961G、7961G-GE、7962G、7965G、または 8961 を使用する。
- テレフォニー トラフィックの発生量が多い、拡張コール機能を使用する経営幹部には、Cisco Unified IP Phone 7970G、7971G-GE、7975G、9951、または 9971 を使用する。
- 外勤職員および在宅勤務者には、Cisco IP Communicator を使用する。
- モバイル IP Phone が必要なユーザには、Cisco Unified Wireless IP Phone 7921G または 7925G を使用する。
- ビデオ コールの発信には、Cisco Unified IP Phone または Cisco IP Communicator に関連付けられた Cisco Unified Video Advantage、Cisco IP Video Phone 7985G、または Sony 社製と Tandberg 社製の SCCP エンドポイントのいずれかを使用する。
- 音声、ビデオ、ドキュメント共有、および単一の統合インターフェイスからの現在の情報にアクセスするには、Cisco Unified Personal Communicator を使用する。
- 正式な会議環境には、Cisco Unified IP Conference Station 7936 または 7937G を使用する。

アナログ ゲートウェイ

アナログ ゲートウェイには、ルータ ベースのアナログ インターフェイス モジュール、24-FXS ポート アダプタ搭載の Cisco コミュニケーション メディア モジュール（CMM）、Catalyst 6500 24-FXS アナログ インターフェイス モジュール、Cisco VG202、Cisco VG204、Cisco VG224、Cisco VG248、および Cisco Analog Telephone Adapter（ATA）186、188 が内蔵されています。アナログ ゲートウェイは通常、FAX マシン、モデム、TDD/TTY、およびアナログ電話機などのアナログ デバイスを VoIP ネットワークに接続するために使用します。これにより、アナログ信号を IP ネットワーク上でパケット化して送信できるようになります。

アナログ インターフェイス モジュール

ルータベースの Cisco アナログ インターフェイス モジュールには、低密度インターフェイス モジュール（NM-1V、NM-2V、NM-HD-1V、NM-HD-2V、NM-HD-2VE、NM-HDV2、NM-HDV2-1T1/E1、および NM-HDV2-2T1/E1）と高密度インターフェイス モジュール（NM-HDA-4FXS および EVM-HD-8FXS/DID）があります。Cisco アナログ インターフェイス モジュールは、公衆網やその他の従来の電話機器（PBX、アナログ電話機、FAX、キー システムなど）を、Cisco マルチサービス アクセス ルータに接続するためのものです。Cisco アナログ インターフェイス モジュールは、低密度から高密度までのアナログ デバイスを、コール機能に制限がある IP ネットワークに接続する場合に最適です。

低密度アナログ インターフェイス モジュール

低密度アナログ インターフェイス モジュールには、NM-1V、NM-2V、NM-HD-1V、NM-HD-2V、NM-HD-2VE、NM-HDV2、NM-HDV2-1T1/E1、および NM-HDV2-2T1/E1 があります。NM-1V と NM-2V には、1 つまたは 2 つの音声インターフェイス カード（VIC）があります。このインターフェイス カードには、2 ポート FXS VIC（VIC-2FXS）、2 ポート FXO VIC（VIC-2FXO、VIC-2FXO-M1/M2/M3、および VIC-2FXO-EU）、2 ポート ダイヤルイン方式 VIC（VIC-2DID）、2 ポート E&M VIC（VIC-2E/M）、2 ポート CAME（Centralized Automated Message Accounting）VIC（VIC-2CAMA）、および 2 ポート BRI VIC（VIC-2BRI-S/T-TE および VIC-2BRI-NT/TE）があります。NM-1V および NM-2V は、それぞれ最大で 2 個および 4 個の FXS 接続を処理できます。

（注）　NM-1V と NM-2V は、Cisco 2800 および 3800 シリーズのプラットフォームではサポートされていません。Cisco 2800 および 3800 シリーズのプラットフォームでは、VIC-2DID、VIC4-FXS/DID、VIC2-2FXO、VIC-2-4FXO、VIC2-2FXS、VIC2-2E/M、および VIC2-2BRI-NT/TE を含む音声インターフェイス カードは、オンボードの高速 WIC スロットでサポートされています。

NM-HD-1V と NM-HD-2V には、それぞれ 1 つおよび 2 つの VIC があります。NM-HD-2VE には、2 つの VIC または 2 つの音声 /WAN インターフェイス カード（VWIC）、または 1 つの VIC と 1 つの VWIC の組み合せが含まれます。NM-HD-1V、NM-HD-2V、および NM-HD-2VE は、それぞれ最大で 4 個、8 個、および 8 個の FXS 接続または FXO 接続を処理できます。NM-HDV2、NM-HDV2-1T1/E1、および NM-HDV2-2T1/E1 は、最大 4 個の FXS 接続または FXO 接続を処理するデジタル T1/E1 またはアナログ /BRI インターフェイス カードのいずれかに対応させることができます。これら 3 つのインターフェイス モジュールの相違点は、NM-HDV2-1T1/E1 には 1 つの組み込み T1/E1 ポートがあるのに対し、NM-HDV2-2T1/E1 には 2 つの組み込み T1/E1 ポートがあることです。

音声インターフェイス カードには、2 ポートおよび 4 ポート FXS VIC（VIC2-2FXS および VIC-4FXS/DID）、2 ポートおよび 4 ポート FXO VIC（VIC2-2FXO および VIC2-4FXO）、2 ポート ダイヤルイン方式 VIC（VIC-2DID）、2 ポート E&M VIC（VIC2-2E/M）、および 2 ポート BRI VIC（VIC2-2BRI-NT/TE）があります。音声 /WAN インターフェイス カードには、音声および WAN 接続両用の 1 ポートおよび 2 ポート RJ-48 マルチフレックス トランク（MFT）T1/E1 VWIC（VWIC-1MFT-T1、VWIC-2MFT-T1、VWIC-2MFT-T1-DI、VWIC-1MFT-E1、VWIC-2MFT-E1、VWIC-2MFT-E1-DI、VWIC-1MFT-G703、VWIC-2MFT-G703、VWIC2-1MFT-T1/E1、VWIC2-2MFT-T1/E1、VWIC2-1MFT-G703、および VWIC2-2MFT-G703）があります。G.703 インターフェイス カードは主としてデータ接続用ですが、場合によっては音声アプリケーションをサポートするように設定できます。

高密度アナログ インターフェイス モジュール

高密度アナログ インターフェイス モジュールには NM-HDA-4FXS と EVM-HD-8FXS/DID があります。NM-HDA-4FXS には 4 つのオンボード FXS ポートがあり、次のオプションから 2 つの拡張モジュールを取り付けることができます。

- EM-HDA-8FXS：8 ポート FXS インターフェイス カード
- EM-HDA-4FXO/EM2-HDA-4FXO：4 ポート FXO インターフェイス カード

NM-HDA-4FXS は、4 つの組み込み FXS ポートと 2 つの EM-HDA-4FXO または EM2-HDA-4FXO 拡張モジュールで最大 12 アナログ ポート（4 FXS および 8 FXO）の構成になるか、または 4 つの組み込み FXS ポートと 1 つの EM-HDA-8FXS 拡張モジュールおよび 1 つの EM-HDA-4FXO または EM2-HDA-4FXO 拡張モジュールで最大 16 アナログ ポート（12 FXS および 4 FXO）の構成になります。2 つの 8 ポート FXS 拡張モジュールを使用する構成はサポートされていません。NM-HDA には、追加の DSP リソースを提供するドーター モジュール（DSP-HDA-16）用のコネクタもあり、8 つの高複雑度コールまたは 16 の中複雑度コールを追加処理できます。

（注）　EM2-HDA-4FXO は、EM-HDA-FXO と同じ密度と機能をサポートしますが、最大 15,000 フィートのループ長のサポートや、グラウンドスタート シグナリング モードで使用して回線状態が悪い場合のパフォーマンス向上などの拡張機能があります。

EVM-HD-8FXS/DID は、基本ボード モジュール上に 8 つの独立したポートがあり、FXS または DID シグナリング用に構成可能です。また、EVM-HD-8FXS/DID には、次のオプションから 2 つの拡張モジュールを取り付けることができます。

- EM-HDA-8FXS：8 ポート FXS インターフェイス カード

- EM-HDA-6FXO：6 ポート FXO インターフェイス カード
- EM-HDA-3FXS/4FXO：3 ポート FXS および 4 ポート FXO インターフェイス カード
- EM-4BRI-NT/TE：4 ポート BRI インターフェイス カード

これらの拡張モジュールは任意の組み合せで使用でき、EVM-HD-8FXS/DID あたり最大 24 FXS ポートの構成になります。

アナログ インターフェイス モジュールでサポートされているプラットフォームおよび Cisco IOS 要件

Cisco アナログ インターフェイス モジュールにサポートされるプラットフォームは、Cisco 2600、2800、3600、3700、および 3800 シリーズです。表 20-2 は、1 プラットフォームあたりにサポートされるインターフェイス モジュールの最大数を示し、表 20-3 は、Cisco IOS ソフトウェアの最低限必要なバージョンを示しています。

表 20-2　各プラットフォームでサポートされるアナログ インターフェイス モジュールの最大数

	サポートされているインターフェイス モジュールの最大数				
プラットフォーム	NM-1V、-2V	NM-HDA-4FXS	EVM-HD	NM-HD-1V、-2V、-2VE	NM-HDV2、-1T1/E1、-2T1/E1
Cisco2600XM	1	1	なし	1	1
Cisco 2691	1	1	なし	1	1
Cisco 3640	3	3	なし	3	なし
Cisco 3660	6	6	なし	6	なし
Cisco 3725	2	2	なし	2	2
Cisco 3745	4	4	なし	4	4
Cisco 2811	なし	1	1	1	1
Cisco 2821	なし	1	1	1	1
Cisco 2851	なし	1	1	1	1
Cisco 3825	なし	2	1	2	2
Cisco 3845	なし	4	2	4	4

表 20-3　アナログ インターフェイス モジュールの Cisco IOS 最小要件

	必要な Cisco IOS ソフトウェア対応リリース				
プラットフォーム	NM-1V、-2V	NM-HDA-4FXS	EVM-HD	NM-HD-1V、-2V、-2VE	NM-HDV2、-1T1/E1、-2T1/E1
Cisco2600XM	12.2(8)T	12.2(8)T	なし	12.3.4T	12.3(7)T
Cisco 2691	12.2(8)T	12.2(8)T	なし	12.3.4T	12.3(7)T
Cisco 3640	12.0(1)T 以降	12.2(8)T 以降	なし	12.3.4T	なし
Cisco 3660	12.0(1)T 以降	12.2(8)T 以降	なし	12.3.4T	なし
Cisco 3725	12.2(8)T 以降	12.2(8)T	なし	12.3.4T	12.3(7)T
Cisco 3745	12.2(8)T 以降	12.2(8)T	なし	12.3.4T	12.3(7)T

表 20-3　アナログ インターフェイス モジュールの Cisco IOS 最小要件 （続き）

プラットフォーム	必要な Cisco IOS ソフトウェア対応リリース				
	NM-1V、-2V	NM-HDA-4FXS	EVM-HD	NM-HD-1V、-2V、-2VE	NM-HDV2、-1T1/E1、-2T1/E1
Cisco 2811	なし	12.3.8T4	12.3.8T4	12.3.8T4	12.3.8T4
Cisco 2821	なし	12.3.8T4	12.3.8T4	12.3.8T4	12.3.8T4
Cisco 2851	なし	12.3.8T4	12.3.8T4	12.3.8T4	12.3.8T4
Cisco 3825	なし	12.3(11)T	12.3(11)T	12.3(11)T	12.3(11)T
Cisco 3845	なし	12.3(11)T	12.3(11)T	12.3(11)T	12.3(11)T

Cisco コミュニケーション メディア モジュール（CMM）

Cisco CMM は、Catalyst 6000 および Cisco 7600 シリーズ スイッチに、高密度アナログ、T1、および E1 ゲートウェイ接続を提供するライン カードです。Cisco CMM は、最大 72 個の FXS 接続を処理できます。CMM は MGCP または H.323 ゲートウェイとして動作し、最大 480 個の IP Phone に Survivable Remote Site Telephony（SRST）サービスを提供します。

Cisco CMM に含まれるインターフェイス ポート アダプタは、24 ポート FXS アナログ ポート アダプタ（WS-SVC-CMM-24FXS）、6 ポート T1 インターフェイス ポート アダプタ（WS-SVC-CMM-6T1）、6 ポート E1 インターフェイス ポート アダプタ（WS-SVC-CMM-6E1）、および会議 / トランスコーディング ポート アダプタ（WS-SVC-CMM-ACT）です。表 20-4 は、互換性があるポート アダプタの最低限のソフトウェア要件を示しています。

表 20-4　CMM ポート アダプタのソフトウェア要件

	WS-SVC-CMM-24FXS	WS-SVC-CMM-6T1	WS-SVC-CMM-6E1	WS-SVC-CMM-ACT
Cisco IOS リリース	12.3(8)XY	12.3(8)XY	12.3(8)XY	12.3(8)XY
CatOS リリース	7.3(1)	7.3(1)	7.3(1)	7.6.8
Native IOS リリース	12.1(15)E	12.1(14)E	12.1(13)E	12.1(13)E
CMM ごとの最大ポート アダプタ数	3	3	3	4

WS-X6624-FXS アナログ インターフェイス モジュール

Cisco WS-X6624-FXS アナログ インターフェイス モジュールは、高密度アナログ デバイスを IP テレフォニー ネットワークに接続するための MGCP ベースのデバイスで、24 個のアナログ ポートを提供します。

（注）　WS-X6624 FXS アナログ インターフェイスは販売終了になりました。

Cisco VG202 および VG204 ゲートウェイ

Cisco VG202 および VG204 アナログ ゲートウェイは、Cisco IOS ベースで低密度の 2 ポートおよび 4 ポート ゲートウェイであり、アナログ電話、FAX マシン、モデム、およびその他のアナログ デバイスを会社の音声システムに接続できます。これらのゲートウェイは、Skinny Client Control Protocol（SCCP）または Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）ゲートウェイのいずれかとして、Unified CM に直接統合できます。これらのゲートウェイが MGCP モードで動作している場合に Unified CM クラスタとの接続が失われると、H.323 を介した Survivable Remote Site Telephony（SRST）へのフェールオーバーを実行します。

また、これらのゲートウェイは SIP プロトコルをサポートしており、Unified CM に SIP トランクを介して接続できます。ただし、このモードでは、Unified CM との SCCP または MGCP 統合で利用可能ないくつかの機能を利用できません。

Cisco VG224 ゲートウェイ

Cisco VG224 アナログ ゲートウェイは、アナログ デバイスを IP テレフォニー ネットワークに接続するための、Cisco IOS の 24 ポート高密度ゲートウェイです。Cisco IOS Release 12.4(2)T 以降では、Cisco VG224 は、Skinny Client Control Protocol（SCCP）または Cisco Unified Communications Manager（Unified CM）を搭載したメディア ゲートウェイ コントロール プロトコル（MGCP）エンドポイントとして機能することができ、フェールオーバーのシナリオでは Survivable Remote Site Telephone（SRST）ルータに復帰できます。Cisco VG224 は、Cisco Unified CM Release 3.1 以降をサポートしています。また、Cisco VG224 は、モデム パススルー、モデム リレー、FAX パススルー、および FAX リレーもサポートしています。さらに、Cisco VG224 は、Cisco Unified Communications Manager Express（Unified CME）および Cisco Unified Survivable Remote Site Telephone（SRST）上で SCCP サポートの アナログ電話を接続するために使用することができます。

Cisco VG248 ゲートウェイ

Cisco VG248 は、アナログ電話機、FAX マシン、モデム、スピーカーフォンのようなアナログ デバイスを企業の Cisco Unified CM（Release 3.1 以降）および音声ネットワークに接続するための、48 ポートの高密度 Skinny Client Control Protocol（SCCP）ゲートウェイです。また、Cisco VG248 は、Simplified Message Desk Interface（SMDI）、NEC Message Center Interface（MCI）、または Ericsson のボイスメール プロトコルと互換性があるレガシー ボイスメール システムおよび PBX との Unified CM の統合もサポートしています。Cisco VG248 は、Survivable Remote Site Telephone（SRST）へのフェールオーバーをサポートしています。

Cisco ATA 186 および 188

Cisco Analog Telephone Adaptor（ATA）186 または 188 は、IP テレフォニー ネットワークに 2 つのアナログ デバイスを接続でき、低密度アナログ デバイスを IP ネットワークに接続する場合に最適です。

Cisco ATA 186 と 188 の相違点は、前者には 10 Base-T イーサネット接続が 1 つしかないのに対し、後者には、自らの接続用と、共存する PC または他のイーサネットベース デバイスの接続用の 2 つの 10/100 Base-T イーサネット接続を提供する統合イーサネット スイッチがあることです。Cisco ATA 186 および 188 は、次のいずれかの方法で設定できます。

- Cisco ATA Web 設定ページ
- Cisco ATA 音声設定メニュー
- TFTP サーバからダウンロードした設定ファイル

SCCP ベースの ATA は、SCCP IP Phone のように動作します。別のエンドポイントから電話をかけられるように、Cisco ATA 186 または 188 を、SIP プロキシ サーバに登録された SIP クライアントとして設定することができます。Cisco ATA 186 または 188 は、SIP 要求を開始するときはユーザ エージェント クライアント（UAC）として、要求に応答するときはユーザ エージェント サーバ（UAS）として動作できます。Cisco Unified CM 5.*x* には、Cisco ATA 186 または 188 に対するネイティブ SIP サポートはありません。

Cisco Unified IP Phone

Cisco IP Phone 製品には、ベーシック IP Phone、ビジネス IP Phone、マネージャ IP Phone、およびエグゼクティブ IP Phone があります。

Cisco ベーシック IP Phone

Cisco ベーシック IP Phone は、コール機能に制限があり、予算上の要求がある、トラフィック量の少ないユーザに最適です。ベーシック IP Phone には、Cisco Unified SIP Phone 3911、および Cisco Unified IP Phone 7902G、7905G、7906G、7910G、7910G+SW、7911G、7912G が内蔵されています。

Cisco Unified SIP Phone 3911

Cisco Unified SIP Phone 3911 は単一回線をサポートし、電話機の背面に 1 つの 10/100 Base-T イーサネット ポートを備えています。Cisco Unified SIP Phone 3911 は、2 行の液晶ディスプレイ（LCD）画面と半二重のスピーカーフォンを備えています。電源は、IEEE 802.3af、または電源アダプタ（CP-PWR-CUBE-3）によるローカル電源で供給します。この電話機は SIP だけをサポートします。

Cisco Unified IP Phone 7902G

Cisco Unified IP Phone 7902G は単一回線をサポートし、電話機の背面に 1 つの 10 Base-T イーサネット ポートを備えています。Cisco Unified IP Phone 7902G に液晶（LCD）画面はありません。
Cisco Unified IP Phone 7902G は SCCP をサポートしていますが、SIP をサポートしていません。

Cisco Unified IP Phone 7905G

Cisco Unified IP Phone 7905G は単一回線をサポートし、電話機の背面に 1 つの 10 Base-T イーサネット ポートを備えています。スピーカーは、一方向のリッスン モードでだけ動作します。
Cisco Unified IP Phone 7905G は SCCP と SIP をサポートしていますが、この 2 つのコール シグナリング プロトコルで機能とユーザ インターフェイス（UI）に一貫性はありません。

Cisco Unified IP Phone 7906G

Cisco Unified IP Phone 7906G は単一回線をサポートし、電話機の背面に 1 つの 10/100 Base-T イーサネット ポートを備えています。スピーカーは、一方向のリッスン モードでだけ動作します。電源は、IEEE 802.3af、Cisco インライン パワー、または電源アダプタ（CP-PWR-CUBE-3）によるローカル電源で供給します。Cisco Unified IP Phone 7906G は SCCP と SIP をサポートする、Cisco デスクトップ IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco デスクトップ IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンドユーザの操作性は、SCCP または SIP のいずれの呼制御シグナリングを使用している場合でも一貫しています。

Cisco Unified IP Phone 7910G、7910G+SW

Cisco Unified IP Phone 7910G は単一回線だけをサポートし、スピーカーは、一方向のリッスン モードでだけ動作します。Cisco Unified IP Phone 7910G には、カスタマイズされた電話機ボタン テンプレート中で管理者が設定できる 6 つの機能アクセス キーもあり、エンドユーザにさまざまなコール機能を提供します。この電話機モデルには機能アクセス キーが 6 つしかないため、1 つの電話機ボタン テンプレートは、エンドユーザにすべてのコール機能を提供することができません。Cisco Unified IP Phone 7910G と 7910+SW の両方とも SCCP をサポートしていますが、SIP はサポートしていません。Cisco Unified IP Phone 7910G と 7910G+SW の唯一の相違点は、前者には 10 Base-T イーサネット ポートが 1 つあるのに対し、後者には 10/100 Base-T イーサネット ポートが 2 つあることです。

Cisco Unified IP Phone 7911G

Cisco Unified IP Phone 7911G は単一回線だけをサポートし、2 つの 10/100 Base-T イーサネット接続を備えています。スピーカーは、一方向のリッスン モードでだけ動作します。
Cisco Unified IP Phone 7911G は SCCP と SIP をサポートする、Cisco デスクトップ IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco デスクトップ IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンドユーザの操作性は、SCCP または SIP のいずれの呼制御シグナリングを使用している場合でも一貫しています。

Cisco Unified IP Phone 7912G

Cisco Unified IP Phone 7912G は単一回線だけをサポートし、2 つの 10/100 Base-T イーサネット接続を備えています。スピーカーは、一方向のリッスン モードでだけ動作します。Cisco Unified IP Phone 7912G は SCCP と SIP をサポートしていますが、この 2 つのコール シグナリング プロトコルで機能とユーザ インターフェイス（UI）に一貫性はありません。

（注）　Cisco Unified IP Phones 7902G、7905G、7910G、7910G+SW、および 7912G は販売終了になりましたが、Cisco Unified Communications Manager 7.*x* によりサポートされることに変わりありません。

Cisco ビジネス IP Phone

Cisco ビジネス IP Phone は、スピーカーやヘッドセットなどの拡張コール機能を使用し、テレフォニー トラフィックの使用量が中程度のトランザクション タイプの社員に最適です。ビジネス IP Phone には、Cisco Unified IP Phone 7931G、7940G、7941G、7941G-GE、7942G、および 7945G があります。

Cisco Unified IP Phone 6921

Cisco Unified IP Phone 6921 は、そのハードウェアの特性と工業設計を Cisco Unified IP Phone 6900 シリーズの他のモデルと共有しています。

Cisco Unified IP Phone 6921 は、最大 2 つのディレクトリ番号をサポートし、2 つの 10/100 Base-T イーサネット接続および全二重スピーカーフォンを装備しています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 6961

Cisco Unified IP Phone 6961 は、そのハードウェアの特性と工業設計を Cisco Unified IP Phone 6900 シリーズの他のモデルと共有しています。

Cisco Unified IP Phone 6961 は、最大 12 つのディレクトリ番号をサポートし、2 つの 10/100 Base-T イーサネット接続を装備しています。また、全二重スピーカーフォンも装備しています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 7931G

Cisco Unified IP Phone 7931G は、24 の点灯ライン キーに割り当てることができる最大 24 のディレクトリ番号をサポートし、小売業、営業、および製造業のユーザに最も適しています。Cisco Unified IP Phone 7931G は 2 つの 10/100 Base-T イーサネットを持ち、SIP および SCCP の両方をサポートしています。他の Cisco Unified IP Phone で使用可能なプログラムマブル ソフトキー のサポートに加えて、Cisco Unified IP Phone 7931G には、保留、リダイアル、および転送の各機能に対応する 3 つの専用キーがあります。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 7940G

Cisco Unified IP Phone 7940G は、最大 2 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。Cisco Unified IP Phone 7940G は SCCP と SIP をサポートしていますが、この 2 つのコール シグナリング プロトコルで機能とユーザ インターフェイス（UI）に一貫性はありません。たとえば、SCCP を使用した Cisco Unified IP Phone 7940G はすべてのセキュリティ機能を備えていますが、SIP では以前に実装されていたセキュリティ機能を備えていません。SCCP を使用した Cisco Unified IP Phone 7940G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP を使用した Cisco Unified IP Phone 7940G にはビデオ サポートがありません。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 7941G

Cisco Unified IP Phone 7941G は、最大 2 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。Cisco Unified IP Phone 7941G は SCCP と SIP をサポートする、Cisco Unified IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンドユーザの操作性は、SCCP または SIP のいずれの呼制御シグナリングを使用している場合でも一貫しています。

SCCP ではサポートされ、SIP ではサポートされない機能がいくつかあります。たとえば、SCCP を使用した Cisco Unified IP Phone 7941G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP にはビデオ サポートがありません。SCCP を使用した Cisco Unified IP Phone 7941G は保留音をサポートしているのに対し、SIP はサポートしていません。この電話機は高解像度の 4 ビット グレースケール ディスプレイを備え、機能の使用方法や Extensible Markup Language（XML）アプリケーションの拡張、およびダブル バイト言語のサポートに対応します。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 7941G-GE

Cisco Unified IP Phone 7941G-GE は、最大 2 つのディレクトリ番号の設定が可能で、2 つの 10/100/1000 Base-T イーサネット接続を備えている点を除いて、Cisco Unified IP Phone 7941G と同等です。ギガビット スループット機能の追加により、共存する PC 上の高ビット レートで広い帯域幅を必要とするアプリケーションに対応します。

Cisco Unified IP Phone 7942G

Cisco Unified IP Phone 7942G は、7941G と同様に、最大 2 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。7941G の他の機能およびプロトコル サポートに加えて、7942G では G.722 ワイドバンド コーデック のサポートもあり、また、高忠実度の音声通信用のスピーカー、マイク、受話器が更新されています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 7945G

Cisco Unified IP Phone 7945G は、7942G の機能を拡張しています。7942G と同様に 7945G は、最大 2 つのディレクトリ番号を持つことができますが、7942G と異なり 7945G は、2 つの 10/100/1000 Base-T イーサネット接続、および 5 方向のナビゲーション ボタン セットも備えています。G.722 ワイドバンド コーデック、および高忠実度のスピーカー、マイク、受話器のサポートに加えて、7945G はバックライト TFT カラー ディスプレイを備えており、通信情報、時間節約アプリケーション、および機能使用状況に簡単にアクセスできます。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco マネージャ IP Phone

Cisco マネージャ IP Phone は、スピーカーやヘッドセットなどの拡張コール機能を使用し、テレフォニー トラフィックの使用量が中程度から大量の、マネージャおよびアシスタントに最適です。ビジネス IP Phone には、Cisco Unified IP Phone 7960G、7961G、7961G-GE、7962G、7965G があります。

Cisco Unified IP Phone 6941

Cisco Unified IP Phone 6941 は、そのハードウェアの特性と工業設計を Cisco Unified IP Phone 6900 シリーズの他のモデルと共有しています。

Cisco Unified IP Phone 6941 は、最大 4 つのディレクトリ番号をサポートし、2 つの 10/100 Base-T イーサネット接続を装備しています。また、全二重スピーカーフォンも装備しています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 7960G

Cisco Unified IP Phone 7960G は、最大 6 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。Cisco Unified IP Phone 7960G は SCCP と SIP をサポートしていますが、この 2 つのコール シグナリング プロトコルで機能とユーザ インターフェイス（UI）に一貫性はありません。たとえば、SCCP を使用した Cisco Unified IP Phone 7960G はすべてのセキュリティ機能を備えていますが、SIP では以前に実装されていたセキュリティ機能を備えていません。SCCP を使用した Cisco Unified IP Phone 7960G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP を使用した Cisco Unified IP Phone 7960G にはビデオ サポートがありません。SCCP を使用した

Cisco Unified IP Phone 7960G は Cisco Unified IP Phone 拡張モジュール 7914 をサポートしているのに対し、SIP は拡張モジュールをサポートしていません。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 7961G

Cisco Unified IP Phone 7961G は、最大 6 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。Cisco Unified IP Phone 7961G は SCCP と SIP をサポートする、Cisco Unified IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンドユーザの操作性は、SCCP または SIP のいずれの呼制御シグナリングを使用している場合でも一貫しています。

SCCP ではサポートされ、SIP ではサポートされない機能がいくつかあります。たとえば、SCCP を使用した Cisco Unified IP Phone 7961G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP にはビデオ サポートがありません。SCCP を使用した Cisco Unified IP Phone 7961G は保留音をサポートしているのに対し、SIP はサポートしていません。SCCP を使用した Cisco Unified IP Phone 7961G は Cisco Unified IP Phone 拡張モジュール 7914 をサポートしているのに対し、SIP は拡張モジュールをサポートしていません。この電話機は高解像度の 4 ビット グレースケール ディスプレイを備え、機能の使用方法や Extensible Markup Language（XML）アプリケーションの拡張、およびダブル バイト言語のサポートに対応します。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 7961G-GE

Cisco Unified IP Phone 7961G-GE は、最大 6 つのディレクトリ番号の設定が可能で、2 つの 10/100/1000 Base-T イーサネット接続を備えている点を除いて、Cisco Unified IP Phone 7961G と同等です。ギガビット スループット機能の追加により、共存する PC 上の高ビット レートで広い帯域幅を必要とするアプリケーションに対応します。

Cisco Unified IP Phone 7962G

Cisco Unified IP Phone 7962G は、7961G と同様に、最大 6 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。7961G の他の機能およびプロトコル サポートに加えて、7962G では G.722 ワイドバンド コーデック のサポートもあり、また、高忠実度の音声通信用のスピーカー、マイク、および 受話器が更新されています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 7965G

Cisco Unified IP Phone 7965G は、7962G の機能を拡張しています。7962G と同様に 7965G は、最大 6 つのディレクトリ番号を持つことができますが、7962G と異なり 7965G は、2 つの 10/100/1000 Base-T イーサネット接続、および 5 方向のナビゲーション ボタン セットも備えています。G.722 ワイドバンド コーデック、および高忠実度のスピーカー、マイク、受話器に加えて、7965G はバックライト TFT カラー ディスプレイを備えており、通信情報、時間節約アプリケーション、および機能使用状況に簡単にアクセスできます。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 8961

Cisco Unified IP Phone 8961 は、Cisco IP Phone 製品の中では高度な機能を提供します。8961 は、最大 5 つのディレクトリ番号、2 つの 10/100/1000 Base-T イーサネット接続、および 1 つの 5 方向のナビゲーション ボタン セットをサポートします。また、8961 は、5 つのセッション キー、ヘッドセット用の 1 つの USB ポート、ユーザ エクスペリエンスを向上させるための、固定ハード ボタンに割り当てられた最も一般的なコール機能（保留、転送、会議）を備えています。さらに、8961 は、ワイドバンド オーディオ ヘッドセット、スピーカー、ハンドセットを備え、MIDlet および XML アプリケーションをサポートします。8961 は、Unified CM 7.1(3) 以降のリリースでサポートされています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco エグゼクティブ IP Phone

Cisco エグゼクティブ IP Phone は、拡張コール機能を使用する、トラフィック量の多い経営幹部ユーザに最適です。エグゼクティブ IP Phone には、Cisco Unified IP Phone 7970G、7971G-GE、および 7975G があります。

Cisco Unified IP Phone 7970G

Cisco Unified IP Phone 7970G は、最大 8 つのディレクトリ番号の設定が可能で、高解像度のカラー タッチ スクリーンを備え、他の Cisco Unified IP Phone よりも多くのアクセス キーがあります。Cisco Unified IP Phone 7970G は SCCP と SIP の両方をサポートする、Cisco デスクトップ IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco デスクトップ IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンドユーザの操作性は、SCCP または SIP のいずれの呼制御シグナリングを使用している場合でも一貫しています。

SCCP ではサポートされ、SIP ではサポートされない機能がいくつかあります。たとえば、SCCP を使用した Cisco Unified IP Phone 7970G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP にはビデオ サポートがありません。SCCP を使用した Cisco Unified IP Phone 7970G は保留音をサポートしているのに対し、SIP はサポートしていません。SCCP を使用した Cisco Unified IP Phone 7970G は Cisco Unified IP Phone 拡張モジュール 7914 をサポートしているのに対し、SIP は拡張モジュールをサポートしていません。この電話機は高解像度の 4 ビット グレースケール ディスプレイを備え、機能の使用方法や Extensible Markup Language（XML）アプリケーションの拡張、およびダブル バイト言語のサポートに対応します。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 7971G-GE

Cisco Unified IP Phone 7971G-GE は、最大 8 つのディレクトリ番号の設定が可能で、2 つの 10/100/1000 Base-T イーサネット接続を備えている点を除いて、Cisco Unified IP Phone 7970G と同等です。ギガビット スループット機能の追加により、共存する PC 上の高ビット レートで広い帯域幅を必要とするアプリケーションに対応します。

（注）　Cisco Unified IP Phone は、アクセス スイッチからのインライン パワー、またはローカルの壁面コンセントからの電源供給に加えて、Cisco Unified IP Phone パワー インジェクタによる電源供給も可能です。Cisco Unified IP Phone パワー インジェクタを使用すると、インライン パワーをサポートしない Cisco スイッチまたは Cisco 以外のスイッチに、Cisco Unified IP Phone を接続できます。Cisco Unified IP

Phone パワー インジェクタは、すべての Cisco Unified IP Phone と互換性があり、Cisco PoE と IEEE 802.3af PoE の両方をサポートしています。2 つの 10/100/1000 Base-T イーサネット接続を備え、一方をスイッチのアクセス ポートに接続し、もう一方を Cisco Unified IP Phone に接続します。

Cisco Unified IP Phone 7975G

Cisco Unified IP Phone 7975G は、7971G-GE と同様に、最大 8 つのディレクトリ番号の設定が可能で、2 つの 10/100/1000 Base-T イーサネット接続を備えています。ただし、7971G-GE と異なり、7975G には、G.722 ワイドバンド コーデックおよび高忠実度のスピーカー、マイク、および受話器が追加されています。7975G には、タッチ スクリーン カラー ディスプレイも備わっています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 9951

Cisco Unified IP Phone 9951 は、Cisco IP Phone 製品の中では高度な機能を提供します。9951 は、最大 5 つのディレクトリ番号、2 つの 10/100/1000 Base-T イーサネット接続、および 1 つの 5 方向のナビゲーション ボタン セットをサポートします。また、9951 は、5 つのセッション キー、1 つの USB ポート、Bluetooth ヘッドセットのサポート、ユーザ エクスペリエンスを向上させるための、固定ハード ボタンに割り当てられた最も一般的なコール機能（保留、転送、会議）を備えています。さらに、9951 は、ワイドバンド オーディオ ヘッドセット、スピーカー、ハンドセットを備え、MIDlet および XML アプリケーションをサポートします。9951 は、Unified CM 7.1(3) 以降のリリースでサポートされています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 9971

Cisco Unified IP Phone 9971 は、Cisco IP Phone 製品の中では高度な機能を提供します。9971 は、最大 6 つのディレクトリ番号、2 つの 10/100/1000 Base-T イーサネット接続、および 1 つの 5 方向のナビゲーション ボタン セットをサポートします。また、9971 は、6 つのセッション キー、2 つの USB ポート、Bluetooth ヘッドセットのサポート、タッチ スクリーン、802.11a/b/g 無線インターフェイス、ユーザ エクスペリエンスを向上させるための、固定ハード ボタンに割り当てられた最も一般的なコール機能（保留、転送、会議）を備えています。さらに、9971 は、ワイドバンド オーディオ ヘッドセット、スピーカー、ハンドセットを備え、MIDlet および XML アプリケーションをサポートします。9971 は、Unified CM 7.1(3) 以降のリリースでサポートされています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco Unified IP Phone 拡張モジュール 7914、7915、7916

Cisco Unified IP Phone 拡張モジュール 7914、7915、7916 は、いくつかの回線の状態が電話機の現在の回線容量を超えていることを判断する必要があるアシスタントなどに適しています。

Cisco Unified IP Phone 拡張モジュール 7914、7915、および 7916 は、追加のボタンと LCD によって、Cisco Unified IP Phone 7960G、7961G、7961G-GE、7962G、7965G、7970G、7971G-GE、または 7975G の機能を拡張します。Cisco Unified IP Phone 拡張モジュール 7914 ではモジュールあたり 14 のボタンが提供され、Cisco Unified IP Phone 拡張モジュール 7915 および 7916 ではモジュールあたり 24 のボタンが提供されます。Cisco Unified IP Phones 796*x*G および 797*x*G は、最大 2 つの Cisco Unified IP Phone 拡張モジュールをサポートできます。IP Phone で Cisco インライン パワーまたは IEEE802.3af PoE を使用している場合には、Cisco Unified IP Phone 拡張モジュール 7914、7915、7916 に外部電源アダプタ（CP-PWR-CUBE-3）を使用する必要があります。

（注）　1 台の電話機で 2 つの拡張モジュールを使用する場合、2 番目のモジュールを 1 番目のモジュールと同じモデルにする必要があります。

Cisco Unified IP Phones 6900 シリーズの配置に関する考慮事項

Cisco Unified IP Phones 6900 シリーズは、Cisco Unified IP Phone 6921、6941、および 6961 モデルで構成されています。これらの IP 電話は、均一の工業設計、回線ごとに 1 つのコール、最もよく使用される保留、転送、会議などのユーザ機能用のハード キー、およびコール シグナリング プロトコルとしてだけの SCCP の使用など、共通の特性を共有します。

このシリーズの IP 電話はすべて回線ごとに 1 つのコールをサポートします。すでにアクティブ コールのある回線への着信コールは、ビジーとして処理されます。つまり、設定によってボイスメールまたは別のディレクトリ名に転送されるか、（転送が設定されていない場合）コールは完了せず、ビジー トーンが発信者に返されます。転送する代わりに第 2 のコールが電話機に表示されるようにするには、プライマリと同じディレクトリ番号に第 2 の回線を設定する必要があります。この第 2 の回線はプライマリと別のパーティションにある必要があり、プライマリ回線はコールを第 2 の回線に転送するように設定する必要があります。パーティションの設定の詳細については、「ダイヤル プラン」（P.10-1）を参照してください。

Cisco Unified IP Phones 6900 シリーズには、Direct Transfer や Direct Transfer Across Lines などの新しいコール機能が導入され、Join や Join Across Lines 機能も提供されています。これらの機能は、複数の回線をまたがるコールに対して動作でき、これらの動作は電話機上のプライマリ回線だけを監視する Computer Telephony Integration（CTI; コンピュータ/テレフォニー インテグレーション）アプリケーションに対して不透明にすることができます。したがって、これらのアプリケーションを適切に動作させ、電話機能を制御できるようにするには、これらのコール機能を無効にする必要があります。これらの機能は、優先順位の高い順に特定の電話機設定、プロファイルを共有する電話機グループに適用できる [Common Device Profile] 設定、企業全体の電話機設定のいずれかで無効にすることができます。

Cisco Unified IP Phone 8900 および 9900 シリーズの配置に関する考慮事項

Cisco Unified IP Phone 8961、9951、および 9971 は、共通のハードウェアおよびソフトウェア プラットフォーム、強化されたアクセサリのサポート、ユニークなユーザ エクスペリエンスを共有する IP Phone ファミリに属します。ユーザ エクスペリエンスには、保留、転送、会議などの一般的なコール機能用の専用ハード キー、（複数の同時コールをより直感的な処理を容易にする）回線とは別の一連のセッション ボタン、ワイドバンド アコースティック対応ハンドセット、マイク、スピーカーが含まれます。モデルに応じて、この IP Phone ファミリは、タッチ スクリーン、USB および Bluetooth ヘッドセット、SDIO、IEEE 802.11a/b/g 無線インターフェイスなどのさまざまなユーザ アクセサリとハードウェア機能をサポートします。

これらの電話機は SIP シグナリング プロトコルだけを実行し、XSI および Java MIDlet アプリケーションをサポートします。

Cisco Unified IP Phone 8961、9951、および 9971 は、Cisco Unified IP Phone 3900、6900、および 7900 シリーズよりも高度な機能を備えています。これらの電話機を配置するには、次に説明する複数の事項について考慮する必要があります。

ファームウェアのアップグレード

通常、デフォルトでは IP 電話機は、UDP ベースのプロトコルである Trivial File Transfer Protocol（TFTP; トリビアル ファイル転送プロトコル）を使用して 1 つまたは複数の Unified CM サブスクライバ サーバに統合された TFTP サーバからそのイメージをアップグレードします。このようにして、すべての電話機はこれらの TFTP サーバからそのイメージを直接取得します。この方法は、電話機の数が比較的少ない場合や、すべての電話機が実質的に帯域幅の制限がない LAN 環境を持つ単一のキャンパス領域に存在する場合に効果的です。

集中型コール処理を使用する大規模な配置の場合は、低速 WAN リンクで中央データ センターに接続された支店の電話機をアップグレードするのに WAN を介した大量のデータ トラフィックが必要になることがあります。それぞれの電話機に対して同じファイル セットが WAN を複数回通過することになります。このような大量のデータを転送することは WAN 帯域幅を浪費するだけでなく、各データ転送がお互いに帯域幅を求めて競合するため長時間かかることがあります。また、TFTP プロトコルの特性により、一部の電話機でアップグレードが強制的に中止され、既存のバージョンのコードに戻る場合があります。

（注）　7900 シリーズの電話機と異なり、Cisco Unified IP Phone 9900 および 8900 シリーズはアップグレード中にも使用できます。9900 および 8900 シリーズの電話機は、アクティブな状態を保持しつつ、メモリに新しいファームウェアをダウンロードおよび格納します。これらの電話機はダウンロードが正常に行われた後に新しいファームウェアでリブートされます。

WAN を介して電話機をアップグレードすることが必要なため生じた問題を緩和するのに 2 つの方法が存在します。1 つの方法はアップグレードのためだけにローカル TFTP サーバを使用することです。管理者は TFTP サーバを支店（特に大量の電話機が存在する支店あるいは WAN リンクが高速または堅牢でない支店）に設置し、支店の電話機がその特定の TFTP サーバを新しいファームウェアのためだけに使用するように設定できます。この変更により、電話機が新しいファームウェアをローカルに取得します。このアップグレード方法では、管理者が支店の TFTP サーバに電話機のファームウェアを事前にロードし、関連する電話機の設定の「load server」パラメータの TFTP サーバ アドレスを手動で設定する必要があります。支店のルータを TFTP サーバとして使用できることに注意してください。

WAN リソースを大量に使用せずに電話機をアップグレードする 2 つ目の方法は、Peer File Sharing（PFS; ピア ファイル共有）機能を使用することです。この機能では、支店の各モデルの 1 つの電話機だけが中央 TFTP サーバからそれぞれの新しいファームウェア ファイルをダウンロードします。電話機がファームウェア ファイルをダウンロードしたら、この電話機はそのファイルを支店の他のすべての電話に配布します。支店に 1 種類の電話機しかない場合は、ファームウェアが WAN 全体で 1 度だけ転送されます。この方法では、load server の方法で必要な手動によるロードと設定を回避できます。

PFS 機能は、同じ支店のサブネット内の電話機が階層形式（チェーン形式）で配置されている場合にアップグレードが要求されると動作します。これは、電話機間でメッセージを交換し、実際にダウンロードを実行する「ルート」電話機を選択することによって行われます。ルート電話機は TCP 接続を使用してチェーンの 2 つ目の電話機にファームウェア ファイルを送信し、2 つ目の電話機はチェーンの 3 つ目の電話機にファームウェア ファイルを送信し、というようにチェーンのすべての電話機がアップグレードされるまでこの作業が繰り返されます。ルート電話機は完全な電話ファームウェアを構成するファイルに応じて異なる場合があることに注意してください。

アップグレード プロセスの完了後、システム管理者は Unified CM 管理ページ（[Device] -> [Device Settings] -> [Firmware Load Information]）にアクセスしてすべての電話が正常にアップグレードされているかどうかを確認できます。ここでは、デフォルトのイメージ レベルでないすべての電話にフラグが付けられます。

無線インターフェイスを介したネットワーク接続

Cisco Unified IP Phone 9971 には IEEE 802.11a/b/g 無線インターフェイスが搭載されています。この機能により、電話機を配置するうえでの柔軟性が提供されます。ただし、無線アクセス可能によってなこれらの電話機を配置する前に次の点を考慮してください。

- ユーザはネットワーク アクセスのために PC を電話機の PC ポートに接続できない。
- 無線インターフェイスが動作するように電話機背面のネットワーク ポートは未接続のままにしておく。電話機が有線ネットワークを利用可能であることを検出した場合、電話機は無線インターフェイスの接続を解除し、有線接続を使用します。
- 電話機は外部電源により電力供給する必要がある。
- 2.4 GHz 無線と Bluetooth との間には干渉に関する既知の問題が存在する。Bluetooth ヘッドセットと 802.11b/g の共存は可能ですが、コール機能が制限されることがあります。この共存モードではマルチキャスト Music On Hold（MoH; 保留音）がサポートされないことに注意してください。この共存モードが 2.4 GHz IEEE 802.11g で使用される場合、12 Mbps 以上のデータレートで無線インターフェイスを使用することをお勧めします。Bluetooth が有効な場合の干渉の問題を避けるためには、5.0 GHz IEEE 802.11a 無線接続を使用することをお勧めします。
- 無線アクセス密度を考慮する必要がある。
- 有線モードではファームウェアのダウンロードが低速になることがある。
- 電話機に 2 つの異なる Media Access Control（MAC; メディア アクセス制御）アドレスを設定する必要はない。無線と有線の両方の設定には、設定メニューで示された MAC アドレスを使用する必要があります。
- Cisco Emergency Responder は、有線 IP 電話機の場合とは異なりスイッチ ポートではなく IP アドレスだけによって無線 IP 電話機を追跡する。したがって、無線で接続された電話機の場所情報は有線電話機の場合ほど正確ではありません。

Power over Ethernet（PoE）

Cisco Unified IP Phone 9971 および 9951 は、PoE の旧 IEEE 802.3af と新しく策定された 802.3at 標準の両方をサポートします。新しい標準は最大 30 W の電力に対応しています。これらの電話機自体はこの値よりも少ない電力（12.95 W）を消費するため 802.3af 電力標準で対応できます。ただし、Key Extension Module（各 5 W）や USB デバイスなどの電力を消費する他の機器が存在する場合は、IEEE 802.3at 標準が提供できるよりも多くの電力が必要になることがあります。この場合は、コンセントを使用して電話機に電力を供給してください。電話機には、必要な電力が使用できない場合にユーザに警告する電力管理機能があります。

IEEE 802.3at 標準は非常に新しいため、電力を電話機に供給する既存のスイッチをこの新しい標準にアップグレードしなければならないことがあります。

アプリケーション

Cisco Unified IP Phone 8961、9951、および 9971 には CTI を通じて電話機を監視するアプリケーションによる処理が必要な JTAPI イベントを生成するコール機能が導入されています。これらのコール機能により、ユーザは処理中の転送や会議を中止したり、同じ回線または異なる回線でコールの参加や直接転送を実行したりできます。監視アプリケーションがこれらのイベントを適切に処理するバージョンにアップグレードされていない場合は、アプリケーションが電話のビューやコール状態を電話機自体と同期しなくなるなどの、予期しないアプリケーション動作が発生することがあります。したがって、デフォルトではすべてのアプリケーションはこれらの電話機の監視または制御が制限されています。

これらの新しいイベントを適切に処理するようアップグレードされたアプリケーションやアプリケーションがこれらのイベントの影響を受けないことが確認されたアプリケーションの場合は、管理者がアプリケーションに関連付けられたアプリケーションまたはエンドユーザ設定で **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** という新しく定義されたロールを有効にできます。このロールが有効にならないと、アプリケーションはこれらの電話機を監視または制御できません。

SRST、Unified CME、および Unified CME as SRST のサポート

Cisco Unified IP Phone 8961、9951、および 9971 は、Unified CM クラスタとの WAN 接続が失われた場合に Survivable Remote Site Telephony（SRST）にフェールオーバーすることがあります。ただし SRST モードで利用可能な機能セットは、電話機が Unified CM に登録されている場合よりもかなり少なくなります。

Cisco Unified Communications Manager Express（Unified CME）または Unified CME as SRST では、現在これらの電話機はサポートされていません。

ソフトウェアベースのエンドポイント

ソフトウェアベースのエンドポイントには、Cisco Unified Personal Communicator および Cisco IP Communicator があります。ソフトウェアベースのエンドポイントは、クライアント PC にインストールされたアプリケーションであり、登録と管理は Unified CM で行います。

Cisco Unified Personal Communicator

Cisco Unified Personal Communicator は、Microsoft Windows または Macintosh 上で動作するソフトウェア アプリケーションです。Cisco Unified Personal Communicator は、幅広い通信のアプリケーションおよびサービスを 1 つのデスクトップ アプリケーションに統合し、人々が効率的にコミュニケーションできるようにします。Cisco Unified Personal Communicator を使用すると、音声、ビデオ、コール管理、在籍情報、および Web 会議などのさまざまの強力なコミュニケーション ツールにアクセスできます。統合アプリケーションには、Cisco Unified Communications Manager（Unified CM）、Cisco Unified Presence、Cisco Unity、Cisco Unity Connection、Cisco Unified MeetingPlace、Cisco Unified MeetingPlace Express、Cisco Unified Videoconferencing and MeetingPlace Express VT、および Lightweight Directory Access Protocol（LDAP）バージョン 3（v3）サーバがあります。Cisco Unified Personal Communicator の詳細については、「Cisco Unified Presence」（P.22-1）の章を参照してください。

サーバごとに許可されるデバイスの制限とは関係なく、Unified CM で設定できる最大 CTI デバイス数に制限があります。Cisco Unified Personal Communicator に適用される CTI デバイスの制限は、次のとおりです。

- Cisco Media Convergence Server（MCS）7825 または 7835 の場合、1 台あたり最大 800 台の Cisco Unified Personal Communicator。MCS 7825 または 7835 サーバの場合、1 クラスタあたり最大 3,200 台の Cisco Unified Personal Communicator。
- Cisco Media Convergence Server（MCS）7845 の場合、1 台あたり最大 2,500 台の Cisco Unified Personal Communicators。MCS 7845 サーバの場合、1 クラスタあたり 最大 10,000 Cisco Unified Personal Communicator。

上記の Cisco Unified Personal Communicator の最大限度には、次の前提が適用されます。

- 各 Cisco Unified Personal Communicator は、見積もりで 6 コール以下の Busy Hour Call Attempt（BHCA）を処理します。

- CTI デバイスを必要とする他の CTI アプリケーションが、その Unified CM クラスタで設定されていません。

Cisco IP Communicator

Cisco IP Communicator は、コンピュータに IP Phone 機能を与える Microsoft Windows ベースのアプリケーションです。このアプリケーションを使用すると、出張中やオフィス内など、企業ネットワークにユーザがどの場所からアクセスする場合でも高品質の音声コールが可能になります。リモート ユーザと在宅勤務者にとって最適なソリューションです。Cisco IP Communicator は配置が簡単で、現在 IP 通信で利用可能な最新テクノロジーや先端機能のいくつかが採用されています。

Cisco IP Communicator は SCCP および SIP をサポートするスタンドアロン デバイスであるため、さまざまな IP テレフォニー配置モデルに含まれる IP Phone の設計に関するガイドラインは、Cisco IP Communicator にも当てはまります。詳細については、「Unified Communications の配置モデル」（P.2-1）の章を参照してください。

サポートされる機能に関するエンドユーザ環境は、SCCP または SIP のいずれの呼制御シグナリングを使用している場合でも同じです。SCCP ではサポートされ、SIP ではサポートされない機能がいくつかあります。たとえば、SCCP を使用した Cisco IP Communicator は、ビデオ コールの発信に関して CiscoUnified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP にはビデオ サポートがありません。さらに、SCCP を使用した Cisco IP Communicator は保留音をサポートしているのに対し、SIP はサポートしていません。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.20-48）を参照してください。

Cisco IP Communicator 2.1 は、イメージおよびシグナリング認証をサポートしています。Cisco Unified CM 4.*x* 以降と接続している場合、Cisco IP Communicator 2.1 は、認証を使用した Transport Layer Security（TLS）相互認証もサポートし、これにより、Cisco IP Communicator が別の Cisco Unified IP Phone になりすますことができなくなります。Certificate Authority Proxy Function（CAPF）および Locally Significant Certificate（LSC）では、セキュリティを双方向認証で実装されます。Cisco IP Communicator 2.1 は、デバイス認証のための Certificate Trust List（CTL）もサポートしています。

Cisco Unified Client Services Framework

Cisco Unified Client Services Framework は、Microsoft Windows ベースのソフトウェア アプリケーションであり、オーディオ、ビデオ、Web コラボレーション、ビジュアル ボイスメールなどの Unified Communications サービスを統合する基礎となるフレームワークをプレゼンスおよびインスタント メッセージング アプリケーションに提供します。Cisco Unified Client Services Framework を使用することで、ユーザは Cisco Unified Communications Manager（Unified CM）、Cisco Unity、Cisco Unity Connection、Cisco Unified MeetingPlace、および Lightweight Directory Access Protocol（LDAP）バージョン 3（v3）サーバに接続するさまざまな通信サーバにアクセスできます。Cisco Unified Client Services Framework を使用する Cisco Unified Communications の統合の詳細については、「Cisco Unified Presence」（P.22-1）の章を参照してください。

Cisco Unified Client Services Framework は Cisco Unified CM の新規デバイスであり、ソフトフォン モードまたはデスクフォン モードのいずれかで動作して Unified IP Phone を制御します。

ソフトフォン モードの動作

Cisco Unified Client Services Framework がソフトフォン モードで動作する場合、Cisco Unified CM に新規デバイスを設定する必要があります。すると、Cisco Unified Client Services Framework は SIP ベースの単一回線である Cisco Unified IP Phone として動作し、Cisco Unified IP Phone の完全な登録と冗長性メカニズムをサポートするようになります。

デスクフォン モードの動作

Cisco Unified Client Services Framework がデスクフォン モードで動作する場合、このアプリケーションでは関連付けられた Cisco Unified IP Phone の制御に CTI/JTAPI（Java Telephony API ）が使用されます。Unified Client Services Framework では、Unified CM の Cisco CallManager Cisco IP Phone Services（CCMCIP）サービスを使用して、制御する有効な Cisco Unified IP Phones のリストを提供します。

Cisco Unified Client Services Framework を配置する際は、次の設計上の考慮事項に注意してください。

- 管理者は、組織における Unified Client Services Framework のインストール、配置、および設定方法を決定する必要がある。アプリケーションのインストールには Altris などの有名なインストール パッケージを使用し、TFTP サーバ、CTI Manager、CCMCIP サーバ、ボイスメール パイロット、LDAP サーバ、LDAP ドメイン名、および LDAP 検索コンテキストといった必要なコンポーネントのユーザ レジストリ設定にグループ ポリシーを使用することをお勧めします。
- Unified Communications とバックエンドのディレクトリ コンポーネントのシームレスな統合を可能にするため、Cisco Unified Client Services Framework ユーザのユーザ ID とパスワードの設定は、LDAP サーバに保存されているユーザのユーザ ID とパスワードに一致する必要がある。
- Cisco Unified CM のディレクトリ番号設定と LDAP の電話番号属性は、完全な E.164 番号で設定する必要がある。プライベート企業ダイヤル プランを使用できますが、それに伴ってアプリケーション ダイヤル ルールとディレクトリ ルックアップ ルールの使用が必要になる場合があります。
- Cisco Unified IP Phone の制御にデスクフォン モードを使用する場合は、CTI を使用する。したがって、Unified CM 配置のサイジングを行うときは、CTI の使用を必要とする他のアプリケーションも考慮に入れる必要があります。

無線エンドポイント

Cisco 無線エンドポイントは、無線アクセス ポイント（AP）経由で無線 LAN（WLAN）インフラストラクチャを使用して、テレフォニー機能を提供します。このタイプのエンドポイントは、エリア内でモバイル ユーザの必要性がある環境で、従来の有線電話機では不適切であったり問題が生じたりする場合に理想的です（無線ネットワークの設計の詳細については、「無線 LAN インフラストラクチャ」（P.3-73）を参照してください）。

Cisco では、次の Voice over WLAN（VoWLAN）IP Phone を提供しています。

- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified Wireless IP Phone 7925G
- Cisco Unified IP Phone 9971

すべてが、組み込み型の無線アンテナを備えた、ハードウェアベースの電話機です。Cisco Unified Wireless IP Phone 7921G および 7925G、ならびに無線で接続された Cisco Unified IP Phone 9971 では、ネットワークへの 802.11b 接続、802.11g 接続、または 802.11a 接続が有効になります。Cisco Unified Wireless IP Phone は Skinny Client Control Protocol（SCCP）を使用して Unified CM に登録

されますが、Cisco Unified IP Phone 9971 は Session Initiation Protocol（SIP; セッション開始プロトコル）を使用して登録されます。これらの電話機の詳細については、次の Web サイトで入手可能な該当する電話機マニュアルを参照してください。

http://www.cisco.com

サイト調査

Cisco Unified Wireless IP Phone を配置する前に、サイト全体の調査を実行して、無線周波数（RF）カバレッジを提供するのに最適な AP の数と場所を判別する必要があります。サイト調査では、最適なカバレッジを提供するアンテナ タイプや RF 干渉の送信元が存在している可能性がある場所を考慮する必要があります。また、サイト調査では Cisco Unified Wireless IP Phone の Site Survey ツール（7921G と 7925G の場合は [Settings] > [Status] > [Site Survey]、9971 の場合は [Applications Button] > [Administrator Settings] > [Network Setup] > [WLAN Setup] を選択してアクセス）を使用する必要があります。追加のサードパーティ ツールもサイト調査で使用できますが、アンテナの感度と調査アプリケーションの制限によって各エンドポイントまたはクライアント無線の動作が異なるため、Cisco Unified Wireless IP Phone 7921G および 7925G、ならびに Cisco Unified IP Phone 9971 を使用して最終サイト調査を実行することを強くお勧めします。

認証

無線の Cisco Unified IP Phone を無線ネットワークに接続するには、最初に次のいずれかの認証方式を使用して、AP に関連付けて通信する必要があります。

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

  この方法では、クライアントと EAP 準拠のリモート認証、認可、アカウンティングのサーバとの間に Protected Access Credential（PAC）でセキュア認証トンネルが確立されると、無線で接続された Cisco Unified IP Phone をユーザ名とパスワードで AP に対し 802.1X で認証できます。認証時、無線デバイスとの間のトラフィックは TKIP または WEP を使用して暗号化されます。802.1X 認証方式および PAC 認証トンネル交換を使用するには、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、ユーザ データベースへのアクセスを提供します。

- Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）

  この方法では、クライアントと Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）を持つ TLS プロトコルを使用する認証サーバ間でセキュア認証トンネルが確立されると、無線で接続された Cisco Unified IP Phone をユーザ名とパスワードで AP に対し 802.1x で認証できます。認証時、無線デバイスとの間のトラフィックは TKIP または WEP を使用して暗号化されます。TLS は、ユーザおよびサーバ認証とダイナミック セッション キーの生成の両方で証明書を使用する機能を提供します。認証に使用される証明書は、製造元でインストールされる証明書（MIC）、またはユーザによりインストールされる証明書のいずれかになります。EAP-TLS は Cisco Unified IP Phone 9971 ではサポートされていません。

- Protected Extensible Authentication Protocol（PEAP）

  この方法では、クライアントと認証サーバとの間で暗号化された SSL/TLS トンネルを通して、ユーザ名とパスワードにより、無線で接続された Cisco Unified IP Phone は AP に対して 802.1x で認証できます。暗号化された SSL/TLS トンネルはサーバ側の公開キー証明書を使用して作成され、Microsoft's Challenge Handshake Authentication Protocol（MS-CHAP）のバージョン 2 を使用した認証情報の交換の暗号化、およびユーザ クレデンシャルの盗難防止を確実にします。認証時、無線デバイスとの間のトラフィックは TKIP または WEP を使用して暗号化されます。PEAP は Cisco Unified IP Phone 9971 ではサポートされていません。

- Wi-Fi Protected Access（WPA）

  この方法では、ユーザ名とパスワードによって、無線で接続された Cisco Unified IP Phone を AP に対し 802.1X で認証できます。認証時、無線デバイスとの間のトラフィックは Temporal Key Integrity Protocol（TKIP）を使用して暗号化されます。802.1X 認証方式を使用するには、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、ユーザ データベースへのアクセスを提供します。

- Wi-Fi Protected Access 2（WPA2）

  この方法は WPA の 802.11i 拡張版であり、無線デバイスとの間のトラフィックを暗号化するために、TKIP ではなく、高度暗号化規格（AES）を使用します。

- Wi-Fi Protected Access Pre-Shared Key（WPA-PSK）

  この方法では、Cisco Unified Wireless IP Phone および AP 上の共有キーの設定により、無線で接続された Cisco Unified IP Phone を AP に対し認証できます。認証時、無線デバイスとの間のトラフィックは TKIP を使用して暗号化されます。この認証方法は、企業での配置には推奨しません。

- Wi-Fi Protected Access 2 Pre-Shared Key（WPA2-PSK）

  この方法は WPA-PSK の 802.11i 拡張版であり、無線デバイスとの間のトラフィックを暗号化するために、TKIP ではなく、AES を使用します。

- Cisco Centralized Key Management（Cisco CKM）

  この方法では、ユーザ名とパスワードによって、無線で接続された Cisco Unified IP Phone を AP に対し 802.1x で認証できます。認証時、無線デバイスとの間のトラフィックは WEP 128 または TKIP を使用して暗号化されます。802.1X 認証方法には、Cisco ACS などの EAP 準拠の RADIUS 認証サーバが必要です。このサーバは、最初の認証要求のためにユーザ データベースへのアクセスを提供します。以降の認証要求は、AP において無線ドメイン サービス（WDS）によって検証されるため、再認証時間が短縮され、高速で安全なローミングが保証されます。

- Cisco LEAP

  この方法では、ユーザ名とパスワードに基づいて、無線で接続された Cisco Unified IP Phone と AP を相互に認証できます。認証時に動的なキーが生成され、Cisco Unified Wireless IP Phone と AP の間のトラフィックの暗号化に使用されます。ユーザ データベースへのアクセスを提供するため、Cisco Secure Access Control Server（ACS）などの、LEAP 準拠の Radius 認証サーバが必要です。

- 共有キー

  この方法では、無線で接続された Cisco Unified IP Phone と AP に、静的な 10 文字（40 ビット）または 26 文字（128 ビット）のキーを設定します。この方法は AP ベースの認証方法で、一致するキーがデバイスに存在する場合にネットワークへのアクセスが許可されます。

- Open 認証

  この方法では、無線 IP 電話機と AP の間で、識別情報を交換する必要はありません。この方法では音声またはシグナリングの安全な交換が提供されず、偽装したデバイスを AP に関連付けることができるため、この方法は*お勧めしません*。

キャパシティ

各 AP のキャパシティは、AP 無線タイプ、関連するクライアント無線タイプ、使用可能なデータ レート、およびチャネル使用率などの種々の要素により異なります。

802.11b クライアントを持つ 11 Mbps のデータ レート 802.11b 専用 AP の場合、AP は最大 7 つのアクティブな G.711 音声ストリームまたは 8 つの G.729 ストリームをサポートできます。これらの数を超えると、音声パケットのドロップや遅延、またはコールのドロップが原因で、品質が低下する場合があります。AP レートが 11 Mbps より低く設定されている場合、各 AP のコール キャパシティが低下します。

802.11a を 54 Mbps のデータ レートで使用する場合、アクティブ音声ストリームの最大数は、AP あたり 14 ～ 18 に増加します。

54 Mbps のデータ レートの 802.11g 環境の場合、理論上のアクティブ音声ストリームの最大数も、AP あたり 14 ～ 18 に増加します。ただし、ほとんどの 802.11g 環境は混合されたものであり、802.11b クライアント（したがって 11 Mbps のデータ レート）および 802.11g クライアントが含まれるため、キャパシティは通常かなり低くなり、AP あたりのアクティブ音声ストリームの最大数は 8 ～ 12 になります。

802.11 無線タイプに関係なく、コール キャパシティは、データ トラフィックのためにチャネル使用率が高い場合は低下する場合があります。

コール キャパシティ、無線タイプ、およびデータ レートの詳細については、次の Web サイトで入手可能な『*Voice over Wireless LAN Design Guide*』の最新バージョンの 設計上の推奨事項を参照してください。

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

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

これらのアクティブ コール キャパシティの限界と Erlang 比率に基づいて、各 AP がサポートできる Cisco Unified Wireless IP Phone の数を計算できます。たとえば、802.11b クライアントを持つ 802.11b AP で、標準的なユーザ対コールのキャパシティ比率を 3:1 とすると、使用するコーデックが G.711 か G.729 かに応じて、1 つの AP で 21 ～ 24 台の Cisco Unified Wireless IP Phone をサポートできます。また、802.11a クライアントを持つ 54 Mbps のデータ レートの 802.11a AP で、ユーザ対コールのキャパシティ比率を 3:1 とすると、1 つの AP で 42 ～ 54 台の Cisco Unified Wireless IP Phone 7921G をサポートできます。ただし、これらの数には、他の Cisco Unified Wireless IP Phone が AP にローミングする可能性は加味されていません。実際は、AP あたりの電話機の数は上記の数より少なくなります。

これらのキャパシティは、音声アクティビティ検出（VAD）が無効で、パケット化のサンプル サイズが 20 ミリ秒（ms）であることを前提としています。VAD とは、コール中に音声が発生しないときに RTP パケットを送信しないことにより、帯域幅を節約するメカニズムです。ただし、VAD の有効化または無効化は、Unified CM で、クラスタ全体のグローバル設定パラメータで設定します（Unified CM では無音圧縮と呼ばれます）。したがって、無線で接続された Cisco Unified IP Phone で VAD を有効にすると、VAD は Unified CM クラスタ内のすべてのデバイスで有効になります。全体の音声品質を良好に保つため、VAD（無音圧縮）を *disabled* のままにすることをお勧めします。

サンプリング レートを 20 ms に設定すると、片方向の音声コールで 50 パケット / 秒（pps）が生成されます。通常は、サンプル レートを 20 ms に設定するようにお勧めします。それより大きいサンプル サイズ（30 または 40 ms）を使用すると、AP あたりの同時コールの数を増分できますが、エンドツーエンドの遅延も大きくなります。また、サンプル サイズを大きくすると、1 つのパケットが失われたときに欠落する会話の量が大きくなるため、無線環境で許容される音声パケットの損失率は大幅に減少します。音声サンプリング サイズの詳細については、「帯域幅のプロビジョニング」（P.3-59）を参照してください。

電話機設定

Cisco Unified Wireless IP Phone の設定については、次の URL で入手可能な『*Cisco Unified Wireless IP Phone 7921G Administration Guide*』と『*Cisco Unified Wireless IP Phone 7925G Administration Guide*』を参照してください。

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

Cisco Unified Wireless Network 上の Cisco Unified IP Phone 9971 の設定と配置については、次の URL で入手可能な『*Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps10453/tsd_products_support_series_home.html

ローミング

現在、Cisco Unified Wireless IP Phone は、レイヤ 2（同一の VLAN またはサブネット内）にローミングし、引き続きアクティブなコールを保持できます。レイヤ 2 ローミングは、次の状況で発生します。

- 無線で接続された Cisco Unified IP Phone の初期ブートアップ中に、電話機は初めて新しい AP にローミングします。
- 無線で接続された Cisco Unified IP Phone が、現在関連付けられている AP からビーコンまたは応答を受信しない場合、電話機はその AP が使用不可であると見なし、新しい AP へのローミングと関連付けを試行します。
- Cisco Unified Wireless IP Phone と無線で接続された Cisco Unified IP Phone 9971 は利用可能な AP ローミング ターゲットのリストを保持します。現在の AP の状態が変更されると、電話機は、使用可能な AP ローミング ターゲットのリストを参照します。ローミング ターゲットの 1 つが、より適切な選択肢であると判別された場合、電話機はその新しい AP にローミングします。
- 無線で接続された Cisco Unified IP Phone の設定済みの SSID または認証タイプが変更された場合、電話機は AP にローミングして再度関連付けする必要があります。

ローミングで適格な AP ローミング ターゲットの判別を試行するとき、無線 IP Phone は、次の変数を使用して、関連付ける最適な AP を判別します。

- Relative Signal Strength Indicator（RSSI）

  無線で接続された IP 電話機が、シグナルの長さと、RF カバレッジ エリア内で使用可能な AP の品質を判別するときに使用されます。電話機は、RSSI 値が最高で、認証/暗号化タイプが一致する AP との関連付けを試行します。

- QoS Basic Service Set（QBSS）

  AP が、チャネル利用率情報を無線電話機に通信するのを可能にします。チャネル利用率が高い AP は VoIP トラフィックを効率的に処理できない場合があるため、電話機は、QBSS 値を使用して、別の AP へのローミングを試行する必要があるかどうかを判別します。

- Wi-Fi Multimedia Traffic Specification（WMM TSPEC）

  WMM TSPEC は 802.11e QoS メカニズムであり、新しい AP が、現在の使用率に基づく、電話機の帯域幅要件を処理できるかどうかを判断するためにローミングしながら、電話機が TSPEC 表示を通して帯域幅および優先順位処理を要求できるようにすることによって、無線 IP Phone のローミングを支援します。

デバイスがレイヤ 3 で移動する場合、デバイスはネイティブ VLAN の境界を超えて AP から別の AP に移動します。WLAN ネットワーク インフラストラクチャが自律分散型 AP で構成されている場合、Cisco Catalyst 6500 シリーズ Wireless Services Module（WiSM）によって、無線で接続された Cisco Unified Wireless IP Phone は、IP アドレスを保持し、アクティブ コールを維持しながらレイヤ 3 で

ローミングできます。シームレスなレイヤ 3 ローミングは、クライアントが同じモビリティ グループ内で移動するときだけに行われます。Cisco WiSM およびレイヤ 3 ローミングの詳細については、次の Web サイトで入手可能な Cisco WiSM 製品資料を参照してください。

http://www.cisco.com

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

WPA や EAP などのより強力な認証方法を使用すると、情報交換の回数が増加し、ローミング中の遅延が大きくなります。遅延の増加を防止するには、Cisco Centralized Key Management（Cisco CKM）を使用して認証を管理します。レイヤ 2 または レイヤ 3 のどちらの場合も、Cisco CKM を使用すれば、検知できる遅延を発生させずにローミングすることができます。Cisco CKM は、Access Control Server（ACS）に送信する必要がある認証要求の数を減らすことによって、ACS の負荷も軽減します。

（注）　二重帯域 WLAN（2.4 GHz と 5 GHz の両方の帯域を持つ WLAN）では、同じ SSID の 802.11b/g と 802.11a との間でのローミングは、クライアントが両方のボードをサポートできれば可能です。ただし、これにより、音声パスにギャップが発生する場合があります。これらのギャップを防止するには、音声通信に 1 つの帯域だけを使用します。

AP コール アドミッション制御

Unified CM またはゲートキーパー内のコール アドミッション制御メカニズムは、WAN 帯域幅の利用率を制御し、既存のコールの QoS を提供できますが、どちらのメカニズムも、コールの開始時にしか適用されません。静的なデバイス間のコールでは、このタイプのコール アドミッション制御で十分です。しかし、2 つのモバイル無線デバイス間のコールの場合、無線デバイスが 1 つの AP から別の AP へと順にローミングする可能性があるため、AP レベルにもコール アドミッション制御メカニズムが必要です。

Cisco AP および無線音声クライアントには、コール アドミッション制御に使用される 2 つのメカニズムがあります。

- QoS Basic Service Set（QBSS）

  QBSS はビーコン情報要素であり、この情報要素により、AP は チャネル利用率情報を無線 IP 電話機に通信できます。前述のとおり、電話機はこの QBSS 値を使用して、別の AP にローミングする必要があるかどうかを判別します。QBSS 値が低いと、その AP がローミング先として適切な候補であることを示し、QBSS 値が高いと、電話機がその AP にローミングするべきでないことを示しています。

  この QBSS 情報は便利ですが、コールが適切な QoS を保持しているか、またはコールを処理するのに十分な帯域幅が存在することを保証しないので、真のコール アドミッション制御メカニズムではありません。無線で接続された Cisco Unified IP Phone が、高い QBSS を持つ AP に関連付けられている場合、AP は、コールのセットアップを拒否し、発信側の電話機に Network Busy メッセージを送信することにより、コールが開始または受信されるのを防止します。しかし、無線 IP Phone と別のエンドポイントの間でコールがセットアップされた後は、電話機が、高い QBSS を持つ AP にローミングして関連付けを行うことができ、それによりその AP で使用可能な帯域幅のオーバーサブスクリプションが発生する場合があります。

- Wi-Fi Multimedia Traffic Specification（WMM TSPEC）

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

Bluetooth のサポート

Cisco Unified Wireless IP Phone 7925G と Cisco Unified IP Phone 9971 の両方は Bluetooth 対応デバイスです。これらの Cisco Unified IP Phone 内の Bluetooth 無線またはモジュールにより、電話機で Bluetooth ヘッドセットがサポートされるようになります。Bluetooth デバイスは 802.11 b および g デバイスとして同じ 2.4 GHz 無線帯域を使用するため、Bluetooth および 802.11 b または g デバイスが互いに干渉して、接続上の問題が発生する場合があります。

Bluetooth モジュールと 802.11 WLAN モジュールが Cisco Unified Wireless IP Phone 7925G および Cisco Unified IP Phone 9971 で共存し、Bluetooth と 802.11b/g 無線との間の無線干渉が大幅に減少する一方で、これらの無線で接続された電話機の Bluetooth 無線は近くに配置されている他の 802.11 b または g デバイスと干渉を起こすことがあります。802.11 b および g WLAN 音声デバイスの干渉または中断（これにより、音質低下、未登録、コール セットアップ の遅延のすべて、またはいずれかが発生する場合があります）の可能性があるため、すべての WLAN 音声デバイスを、5 GHz 無線帯域を使用する 802.11a に配置することをお勧めします。無線電話機を 802.11a 無線帯域に配置することで、Bluetooth デバイスによって引き起こされる干渉を回避できます。

（注）　Cisco Unified Wireless IP Phone 7925G で Bluetooth 無線ヘッドセットを使用すると、電話のバッテリ電力消費が増加し、バッテリ寿命が短くなります。

Cisco Unified IP Conference Station

Cisco Unified IP Conference Station は、会議室のスピーカーフォン テクノロジーと、Cisco Unified Communications テクノロジーを結合します。Cisco Unified IP Conference Station は、360 度の室内カバレッジを提供する会議環境に最適です。

Cisco では、次の IP conference phone を提供しています。

- Cisco Unified IP Conference Station 7936
- Cisco Unified IP Conference Station 7937G

どちらの IP conference phone もコール シグナリング プロトコルとして SCCP を使用します。

Cisco Unified IP Conference Station 7936 は、外部スピーカー 1 つと組み込み型のマイク 3 つを備えています。Cisco Unified IP Conference Station 7936 には、Cisco Unified CM Release 3.3（3）SR3 以降が必要です。Cisco Unified IP Conference Station 7936 は、バックライト付きのピクセルベース LCD 画面も備えています。大きい部屋でマイクのカバレッジを拡張するため、オプションの拡張マイクも接続できます。

Cisco Unified IP Conference Station 7937G には、ワイドバンド アコースティック、拡張された室内カバレッジ、大型バックライト LCD、および追加ソフトキーが加えられています。Cisco Unified IP Conference Station 7937G は、IEEE 802.3af Power over Ethernet もサポートしており、また、外部電源アダプタ（シスコ部品番号 CP-PWR-CUBE-3）も使用できます。Cisco Unified IP Conference Station 7937G には、Cisco Unified CM Release 4.1 以降が必要です。

ビデオ エンドポイント

Cisco Unified CM 5.*x* は、次のタイプのビデオ対応エンドポイントをサポートしています。

- Cisco Unified IP Phone 7911、7940、7941、7942、7945, 7960, 7961, 7962、7965、7970、7971、または 7975 に関連付けられている Cisco Unified Video Advantage、あるいは Skinny Client Control Protocol（SCCP）を実行している Cisco IP Communicator に関連付けられている Cisco Unified Video Advantage
- Cisco IP Video Phone 7985
- SCCP を実行している Tandberg 社製 2000 MXP、1500 MXP、1000 MXP、770 MXP、550 MXP、T-1000、および T-550 モデル
- SCCP を実行している Sony 社製 PCS-1、PCS-TL30、および PCS-TL50 モデル
- H.323 および SIP クライアント（Polycom、Sony、PictureTel、EyeBeam、Tandberg、VCON、VTEL、Microsoft NetMeeting など）
- Cisco Unified Personal Communicator（ソフトフォン モードで動作）

SCCP ビデオ エンドポイント

SCCP ビデオ エンドポイントは、Unified CM に直接登録し、Trivial File Transfer Protocol（TFTP）でその設定をダウンロードします。サポートされる多くの機能および付加サービスとしては、保留、転送、会議、パーク、ピックアップとグループ ピックアップ、Music On Hold、シェアドライン アピアランス、マッピング可能ソフトキー、自動転送（busy、no answer、unconditional）などがあります。

Cisco Unified Video Advantage

Cisco Unified Video Advantage は、Windows 2000、Windows XP、または Windows Vista が動作しているパーソナル コンピュータにインストールできる Windows ベースのアプリケーションおよび USB カメラです。Skinny Client Control Protocol を実行している Cisco Unified IP Phone 7911、7940、7941、7942、7945、7960、7961、7962、7965、7970、7971 または 7975 の PC ポートに PC を物理的に接続すると、Cisco Unified Video Advantage アプリケーションは電話機と「アソシエーション」を行い、それによってユーザはいつもの電話操作が可能になり、ビデオ機能も追加されます。Cisco Unified Video Advantage Release 2.0 では、このアソシエーションを同じ PC 上で SCCP を実行している Cisco IP Communicator にも関連付けることもできます。

システム管理者は、このアソシエーションをどの IP Phone に許可するかを制御するために、Unified CM Administration の IP Phone 設定ページで **Video Capabilities: Enabled/Disabled** 設定の切り替えを行います。この機能を有効にすると、カメラを表すアイコンが IP Phone ディスプレイの右下に表示されます。デフォルトでは、Cisco Unified Video Advantage は無効になっています。Bulk Administration Tool を使用すると、この設定を多数の電話機で一度に修正することもできます。注意する点としては、Cisco Unified Video Advantage がハードウェア IP Phone で動作するには **PC Port: Enabled/Disabled** 設定も有効にする必要がありますが、**PC Access to Voice VLAN** 設定を有効にする必要はありません。

上記のハードウェア IP Phone とのアソシエーションのために、Cisco Unified Video Advantage は Cisco Discovery Protocol（CDP; シスコ検出プロトコル）ドライバを PC のイーサネット インターフェイスにインストールします。CDP を使用すると、PC と ハードウェア IP Phone は相互に自動検出できるようになります。このため、Cisco Unified Video Advantage を動作させるために、ユーザは PC または ハードウェア IP Phone 上で何も設定する必要はありません。したがって、ユーザがビデオ対応ハードウェア IP Phone に PC を差し込めば、自動的にアソシエーションが行われます（図 20-1 を参照）。

Cisco Unified Video Advantage 2.0 は、同じ PC 上で SCCP を実行している Cisco IP Communicator 存在を検出するために CDP を使用することはありません。代わりに、Cisco IP Communicator プロセスから送信されたプライベート Windows メッセージを監視します。Cisco IP Communicator が検出されると、アソシエーション プロセスは、ハードウェア IP 電話機に対する場合とまったく同じ動作をします（図 20-2 を参照）。

（注）　Cisco Unified Video Advantage をインストールすると、CDP パケット ドライバが PC のすべてのイーサネット インターフェイスにインストールされます。新しい Network Interface Card（NIC; ネットワーク インターフェイス カード）を追加するか、古い NIC を新しいものと置き換えたときは、Cisco Unified Video Advantage を再インストールして、CDP ドライバが新しい NIC にもインストールされるようにしてください。

図 20-1　Cisco Unified Video Advantage の動作の概要

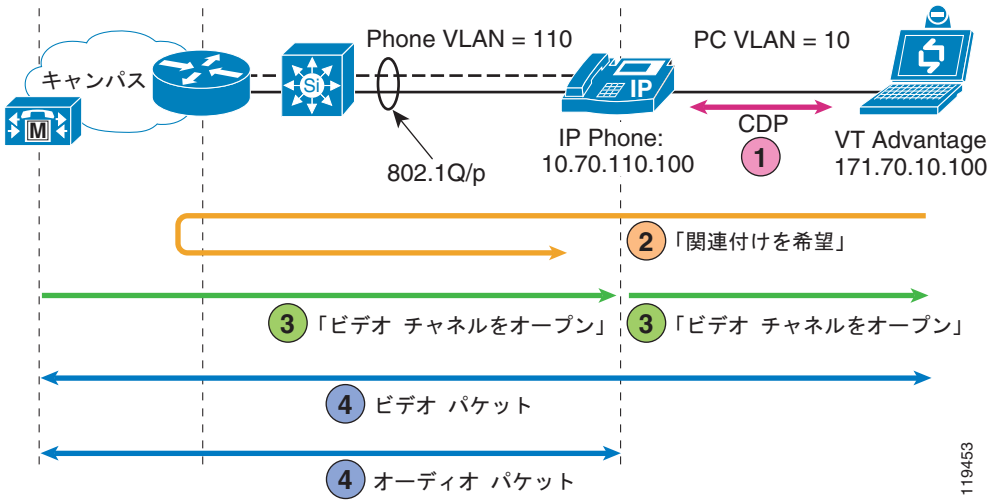


図 20-1 は次のイベントを示しています。

1. IP Phone と PC exchange Cisco Discovery Protocol（CDP）メッセージ。電話機は、その隣接した CDP デバイス の IP アドレスから TCP ポート 4224 の PC アソシエーション パケットを監視します。
2. PC は、アソシエーション メッセージを 電話機に TCP/IP で開始します。アソシエーション パケットは、VLAN 間 でレイヤ 3 までルーティングされます。ファイアウォールと Access Control List（ACL; アクセス コントロール リスト）の両方またはいずれかは、TCP ポート 4224 を許可する必要があります。
3. 電話機は、Cisco Unified Video Advantage と Unified CM の間で SCCP プロキシとして機能します。Unified CM は、コール用のチャネルをオープンするように電話機に指示し、電話機は PC に対してそのメッセージのプロキシを行います。

4. 電話機は音声を送受信し、PC はビデオを送受信します。音声トラフィックもビデオトラフィックも、DSCP AF41 としてマーキングされています。ビデオ トラフィックは UDP ポート 5445 を使用します。

図 20-2　Cisco IP Communicator の Cisco Unified Video Advantage への関連付け

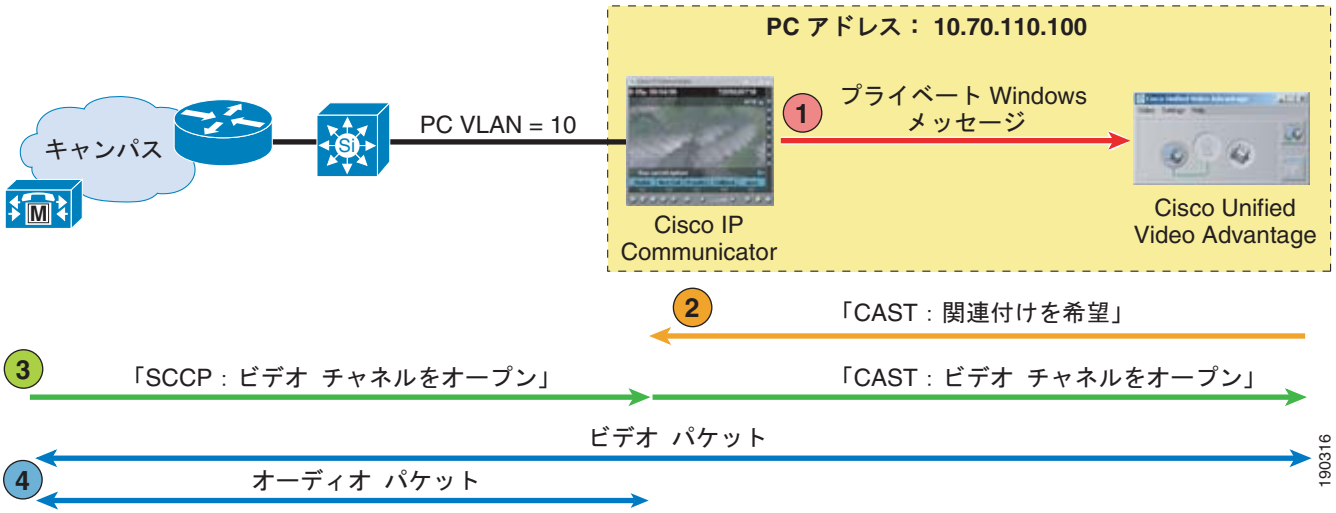


図 20-2 は次のイベントを示しています。

1. Cisco IP Communicator は、プライベート Windows メッセージを Cisco Unified Video Advantage に送信します。このメッセージには、Cisco IP Communicator の IP アドレスと CAST メッセージのポート番号が含まれています。
2. Cisco Unified Video Advantage は、CAST メッセージを Cisco IP Communicator に TCP/IP で開始します。CAST メッセージは接続アドレスであるため、PC から出力されません。
3. Cisco IP Communicator は、Cisco Unified Video Advantage と Unified CM との間の SCCP プロキシとして機能します。Unified CM は、IP Communicator にコール用のビデオ チャネルをオープンするように指示し、IP Communicator は、CAST プロトコル を介して Cisco Unified Video Advantage にそのメッセージのプロキシを行います。
4. Cisco IP Communicator は音声を送受信し、Cisco Unified Video Advantage はビデオを送受信します。音声トラフィックもビデオトラフィックも、DSCP AF41 としてマーキングされています。ビデオ トラフィックは UDP ポート 5445 を使用します。

Cisco Unified Video Advantage を使用したコールの発信では、オーディオは IP Phone で処理されますが、ビデオは PC で処理されます。2 台のデバイス間に同期メカニズムが存在しないため、ジッタ、遅延、断片化パケット、および不良パケットを最小限に抑えるために QoS が不可欠です。

ハードウェア IP Phone を使用する場合、電話機 は音声 VLAN 内に存在しますが、PC はデータ VLAN 内に存在します。つまり、アソシエーションが行われるために、レイヤ 3 のルーティング パスが音声 VLAN とデータ VLAN の間に必要です。これらの VLAN の間にアクセス コントロール リスト（ACL）またはファイアウォールがある場合は、アソシエーション プロトコル（両方向で TCP ポート 4224 を使用）の通過を許可するように設定する必要があります。Cisco IP Communicator を使用すると、この通信が PC 内で発生し、通過するレイヤ 3 境界はありません。

Cisco Unified Video Advantage は、Differentiated Services Code Point（DSCP）によるトラフィックの分類をサポートしています。Unified CM は、電話機に送信する SCCP メッセージに DSCP 値を指定します。オーディオだけのコールの発信時に IP Phone は、SCCP 制御トラフィックに DSCP CS3、オーディオ RTP メディア トラフィックに DSCP EF とマーキングします。ただし、ビデオ コールの発信時には、IP Phone は SCCP 制御トラフィックに DSCP CS3、オーディオ RTP メディア トラフィッ

クに DSCP AF41 とマーキングし、Cisco Unified Video Advantage アプリケーションからはビデオ RTP メディア トラフィックにも DSCP AF41 とマーキングされます。IP Phone と Cisco Unified Video Advantage アプリケーションの両方が「アソシエーション」プロトコル メッセージに DSCP CS3 とマーキングするのは、それがシグナリング トラフィックであると考慮され、SCCP など、他のすべてのシグナリング トラフィックと一緒にグループ分けされるためです。

（注）　Cisco Unified CM Release 4.0 では、Cisco Unified IP Phone 7970 および 7971 にセキュリティ機能が追加されました。これによって、Transport Layer Security（TLS）および Secure RTP（SRTP）を使用して、シグナリング トラフィックとオーディオ メディア トラフィックの認証と暗号化が可能です。アソシエーション プロトコルでは、この認証または暗号化が使用されることはなく、ビデオ RTP メディア ストリームが暗号化されることもありません。ただし、SCCP シグナリングとオーディオ RTP メディア ストリームは、暗号化が設定されていれば暗号化されます。

（注）　音声 VLAN をデータ VLAN と同じ設定にしないでください。接続に問題が起きる可能性があります。

考慮すべき点として、Cisco Unified Video Advantage は、PC 上で実行する他のアプリケーションと同様に、システム パフォーマンスに実際に影響します。Cisco Unified Video Advantage 1.0 は、H.263 と Cisco VT Camera ワイドバンド ビデオ コーデックという、2 タイプのビデオ コーデックをサポートしています。Cisco Unified Video Advantage 2.0 は、H.263 と H.264 という、2 タイプのコーデックをサポートしています。Cisco VT Camera ワイドバンド ビデオ コーデックでは、PC への要求が最少になりますが、ネットワークへの要求は最多になります。H.263 では、ネットワークへの要求は少なく、PC への要求は多くなります。最後に、H.264 では、ネットワークへの要求が最少になりますが、PC への要求は最多になります。したがって、利用可能な帯域幅がネットワークに豊富にある場合は、Cisco VT Camera ワイドバンド ビデオ コーデックを使用すると PC 上で CPU およびメモリ リソースを節約できます。

H.263 および H.264 のコーデックは、最高 1.5 Mbps までの範囲をサポートしています。要約すると、Cisco Unified Video Advantage を配置するときに、お客様が PC パフォーマンスとネットワーク使用率のバランスをとる必要があります。

システム要件

PC 要件の詳細については、次の Web サイトで入手可能な『*Cisco Unified Video Advantage Data Sheet*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps5662/products_data_sheet0900aecd8044de04.html

Cisco IP Video Phone 7985G

Cisco IP Video Phone 7985G は、パーソナル デスクトップ ビデオ電話機です。PC 上で実行するアプリケーションである Cisco Unified Video Advantage とは異なり、Cisco IP Video Phone 7985G は、ビデオ機能が統合された独立型の電話機です。この電話機は、ビデオ コールの発信用に 8.4 インチのカラー LCD 画面とビデオ カメラを備えています。最高 8 つのライン アピアランスをサポートし、2 つの 10/100 Base-T イーサネット接続と、Directories、Messages、Settings、および Services の各ボタンを備えています。他の Cisco Unified IP Phone と同様に、Cisco IP Video Phone 7985G は CDP を使用して VLAN および CoS の情報を接続スイッチから取得し、802.1p/q マーキングで使用します。

Cisco Unified Video Advantage と Cisco IP Video Phone 7985G でサポートされるコーデック

表 20-5 は、Cisco Unified Video Advantage と Cisco IP Video Phone 7985G でサポートされるコーデックをリストしています。

表 20-5　Cisco Unified Video Advantage と Cisco IP Video Phone 7985G でサポートされるコーデック

コーデックまたは機能	Cisco Unified Video Advantage	Cisco IP Video Phone 7985G
H.264	あり（Release 2.0）	あり
H.263	あり	あり
H.261	なし	あり
G.711	あり	あり
G.722	なし	あり
G.722.1	なし	なし
G.723.1	なし	なし
G.728	なし	なし
G.729	あり	あり
Cisco Wideband	あり（Release 1.0）	なし
最高帯域幅	Release 1.0 の場合は 7 Mbps、Release 2.0 の場合は 1.5 Mbps	768 kbps
ビデオ解像度	CIF、QCIF	NTSC：4SIF、SIF PAL：4CIF、QCIF、SQCIF

サードパーティ製 SCCP ビデオ エンドポイント

ビデオ エンドポイントの 2 つの製造業者である Sony 社と Tandberg 社は現在、次の製品で Cisco Skinny Client Control Protocol（SCCP）をサポートしています。Sony 社製と Tandberg 社製の両方のエンドポイントでの SCCP は Cisco Unified IP Phone 7940 での SCCP に従ってモデル化されています。複数のライン アピアランス、ソフトキー、およびボタン（Directories、Messages、Settings、Services）など、Cisco Unified IP Phone 7940 ユーザ インターフェイスにある機能のほとんどが、Sony 社製エンドポイントと Tandberg 社製エンドポイントでもサポートされています。Sony 社製と Tandberg 社製のエンドポイントは、TFTP サーバの IP アドレス検出用に DHCP の Option 150 フィールドもサポートし、TFTP サーバから設定をダウンロードします。ただし、Sony 社製および Tandberg 社製のエンドポイントのソフトウェア アップグレードは、TFTP を介しては行われません。代わりに、ベンダーから提供されるツールを使用して、お客様が各エンドポイントを手動でアップグレードする必要があります（Tandberg 社製では FTP による方法が使用され、Sony 社製では FTP または物理メモリスティックが使用されます）。Sony 社製および Tandberg 社製のエンドポイントは、最大で 3 台の Unified CM サーバに登録され、1 次サーバが通信不能になったときに、2 次サーバまたは 3 次サーバにフェールオーバーします。

Sony 社製および Tandberg 社製のエンドポイントは Cisco Unified IP Phone 7940 および 7960 のソフトキー機能と類似したソフトキー機能をサポートしていますが、実際の機能サポートはベンダーおよびモデルによって異なります。サポートされる機能については、製造業者のマニュアルで確認してください。現在、一部のプラットフォーム上にない機能として、次のものがあります。

- Messages ボタン

- Directories ボタン（発信コール、受信コール、不在コール、および社内ディレクトリ）
- Settings ボタンと Services ボタン
- 一部の XML サービス（エクステンション モビリティや Berbee InformaCast など）

Sony 社製および Tandberg 社製のエンドポイントは SCCP を使用するため、エンドポイントでのビデオ コールのダイヤルは、Cisco Unified IP Phone でのオーディオ コールのダイヤルと似ています。Cisco Unified IP Phone に慣れているユーザであれば、Sony 社製および Tandberg 社製のエンドポイントも直感的に使いこなせるはずです。ユーザ インターフェイスの主な相違点は、Sony 社製および Tandberg 社製のエンドポイントに電話機のようなボタン キーパッドや受話器がないことです。代わりに、リモート コントロールを使用して機能にアクセスし、番号をダイヤルします。

（注）　Sony 社製および Tandberg 社製のエンドポイントは、Cisco Discovery Protocol（CDP）または IEEE 802.Q/p をサポートしていません。したがって、その接続先のイーサネット スイッチで、VLAN ID および Quality of Service の信頼境界を手動で設定する必要があります（詳細については、「ネットワーク インフラストラクチャ」（P.3-1）を参照してください）。

Sony 社製と Tandberg 社製の SCCP エンドポイントでサポートされているコーデック

サードパーティ製 SCCP エンドポイントのコーデック サポートは、ベンダー、モデル、およびソフトウェア バージョンによって異なります。サポートされるコーデックについては、ベンダーの製品マニュアルで確認してください。

サードパーティ製 SIP IP Phone

サードパーティ製電話機には、機能アクセス ボタン（固定または可変）など、呼制御シグナリング プロトコルとは関係しない、固有のローカル機能が備わっています。基本的な SIP RFC サポートでは、特定のデスクトップ機能が Cisco Unified IP Phone と同じになるように対応し、特定機能の相互運用性にも対応します。ただし、これらのサードパーティ製 SIP 電話機は、Cisco Unified IP Phone の機能をフル装備しているわけではありません。

シスコは、新しい Unified CM および Cisco Unified Communication Manager Express（Unified CME）の SIP 機能を利用するソリューションの開発に携わっている、Cisco Technology Development Partner Program の一員としての主要なサードパーティ ベンダーと協力して活動しています。このようなベンダーとしては、IPCelerate（教育スペース用の統一クライアント）、RIM（Blackberry 7270 無線 LAN ハンドセット）、および IP blue（ソフトフォン）があります。シスコは、サードパーティ ベンダーの Grandstream とも協力して Grandstream GXP 2000 のテストを行い、相互運用性を保証しています。

シスコは、tekVizion が提供する独立したサードパーティのテストおよび相互運用性検証プロセスにも参加しています。tekVizion が提供するこの独立サービスは、サードパーティ ベンダーのエンドポイントが Unified CM および Unified CME との相互運用性をテストおよび検証できるようにするために確立されました。

シスコの回線側 SIP 相互運用性およびサードパーティ検証の詳細については、http://www.cisco.com を参照してください。

QoS の推奨事項

この項では、IP テレフォニー エンドポイントで配置される一般的な Cisco Catalyst スイッチでの、基本的な QoS ガイドラインおよび設定について説明します。詳細については、次の Web サイトで入手可能な『*Quality of Service*』を参照してください。

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

Cisco VG224 および VG248

アナログ ゲートウェイは、信頼できるエンドポイントです。Cisco VG224 および VG248 ゲートウェイの場合、VG248 パケットの DSCP 値を信頼するようにスイッチを設定します。次の項では、Cisco VG224 および VG248 アナログ ゲートウェイで配置される一般的な Cisco Catalyst スイッチを設定するためのコマンドをリストします。

（注）　次の項では、*vvlan_id* は Voice VLAN ID を表し、*dvlan_id* はデータ VLAN ID を表します。

Cisco 2950

```
CAT2950(config)#interface interface-id
CAT2950(config-if)#mls qos trust dscp
CAT2950(config-if)#switchport mode access
CAT2950(config-if)#switchport access vlan vvlan_id
```

（注）　**mls qos trust dscp** コマンドは、Enhanced Image（EI）でだけ使用できます。

Cisco 2970 または 3750

```
CAT2970(config)#mls qos
CAT2970(config)interface interface-id
CAT2970(config-if)#mls qos trust dscp
CAT2970(config-if)#switchport mode access
CAT2970(config-if)#switchport access vlan vvlan_id
```

Cisco 3550

```
CAT3550(config)#mls qos
CAT3550(config)interface interface-id
CAT3550(config-if)#mls qos trust dscp
CAT3550(config-if)#switchport mode access
Cat3550(config-if)#switchport access vlan vvlan_id
```

Cisco 4500（SUPIII、IV、または V 使用）

```
CAT4500(config)#qos
CAT4500(config)interface interface-id
CAT4500(config-if)#qos trust dscp
CAT4500(config-if)#switchport mode access
CAT4500(config-if)#switchport access vlan vvlan_id
```

Cisco 6500

```
CAT6500>(enable)set qos enable
```

```
CAT6500>(enable)set port qos 2/1 vlan-based
CAT6500>(enable)set vlan vvlan_id mod/port
CAT6500>(enable)set port qos mod/port  trust trust-dscp
```

Cisco ATA 186 および IP Conference Station

Cisco Analog Telephone Adaptor（ATA）186 および IP Conference Station は、信頼されているエンドポイントであるため、それらの QoS 設定は、「Cisco VG224 および VG248」（P.20-33）の項で説明されている設定とまったく同じです。

Cisco ATA 188 および IP Phone

Cisco Analog Telephone Adaptor（ATA）188 および IP Phone の場合、Voice VLAN をデータ VLAN から分離することをお勧めします。Cisco ATA 186、7902、7905、7906、7910、および IP Conference Station の場合は、従来どおり、Voice VLAN とデータ VLAN を分離することと、Auxiliary VLAN を設定することをお勧めします。これにより、同じアクセス レイヤの設定を、異なる IP Phone モデルや ATA に使用できます。またエンドユーザは、IP Phone または ATA を、スイッチ上の異なるアクセス ポートに接続して、同じ処理を受けることができます。Cisco ATA 186、7902、7905、7906、7910、および IP Conference Station の場合、これらのデバイスは PC に接続されていないため、接続された PC からのフレームの CoS 値を上書きするためのコマンドは何の効果もありません。

次の項では、一般的に配置されている Cisco Catalyst スイッチ上の IP Phone に対して実行できるコンフィギュレーション コマンドをリストします。

Cisco 2950

```
CAT2950(config)#
CAT2950(config)#class-map VVLAN
CAT2950(config-cmap)# match access-group name VVLAN
CAT2950(config-cmap)#class-map DVLAN
CAT2950(config-cmap)# match access-group name DVLAN
CAT2950(config-cmap)#exit
CAT2950(config)#
CAT2950(config)#policy-map IPPHONE-PC
CAT2950(config-pmap)# class VVLAN
CAT2950(config-pmap-c0#  set ip dscp 46
CAT2950(config-pmap-c)#  police 1000000 8192 exceed-action-drop
CAT2950(config-pmap)# class DVLAN
CAT2950(config-pmap-c0#  set ip dscp 0
CAT2950(config-pmap-c)#  police 5000000 8192 exceed-action-drop
CAT2950(config-pmap-c)#exit
CAT2950(config-pmap)#exit
CAT2950(config)#
CAT2950(config)#interface interface-id
CAT2950(config-if)#mls qos trust device cisco-phone
CAT2950(config-if)#mls qos trust cos
CAT2950(config-if)#switchport mode access
CAT2950(config-if)#switchport voice vlan vvlan_id
CAT2950(config-if)#switchport access vlan dvlan_id
CAT2950(config-if)#service-policy input IPPHONE-PC
CAT2950(config-if)#exit
CAT2950(config)#
CAT2950(config)#ip access-list standard VVLAN
CAT2950(config-std-nacl)# permit voice_IP_subnet wild_card_mask
CAT2950(config-std-nacl)#exit
CAT2950(config)#ip access-list standard DVLAN
CAT2950(config-std-nacl)# permit data_IP_subnet wild_card_mask
```

```
CAT2950(config-std-nacl)#end
```

（注）　**mls qos map cos-dscp** コマンドは、Enhanced Image（EI）でだけ使用できます。Standard Image（SI）では、このコマンドを使用できません。CoS から DSCP へのデフォルトのマッピングは、次のとおりです。

CoS 値	0	1	2	3	4	5	6	7
DSCP 値	0	8	16	24	32	40	48	56

Cisco 2970、3560 または 3750

```
CAT2970(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT2970(config)# mls qos map policed-dscp 0 24 to 8
CAT2970(config)#
CAT2970(config)#class-map match-all VVLAN-VOICE
CAT2970(config-cmap)# match access-group name VVLAN-VOICE
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT2970(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-ANY
CAT2970(config-cmap)# match access-group name VVLAN-ANY
CAT2970(config-cmap)#
CAT2970(config-cmap)# policy-map IPPHONE-PC
CAT2970(config-pmap)#class VVLAN-VOICE
CAT2970(config-pmap-c)# set ip dscp 46
CAT2970(config-pmap-c)# police 128000 8000 exceed-action drop
CAT2970(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-ANY
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)# exit
CAT2970(config)#
CAT2970(config)#
CAT2970(config)#interface interface-id
CAT2970(config-if)# switchport voice vlan vvlan_id
CAT2970(config-if)# switchport access vlan dvlan_id
CAT2970(config-if)# mls qos trust device cisco-phone
CAT2970(config-if)# service-policy input IPPHONE-PC
CAT2970(config-if)# exit
CAT2970(config)#
CAT2970(confiig)#ip access list extended VVLAN-VOICE
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384 32767
dscp ef
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-CALL-SIGNALING
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 2000 2002 dscp
cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any eq 2443 dscp cs3
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any eq 5060 dscp cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 5060 5061 dscp
cs3
```

```
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-ANY
CAT2970(config-ext-nacl)# permit ip Voice_IP_Subnet  Subnet_Mask any
CAT2970(config-ext-nacl)# end
CAT2970#
```

Cisco 3550

```
CAT3550(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT3550(config)# mls qos map policed-dscp 0 24 26 46 to 8
CAT3550(config)#class-map match-all VOICE
CAT3550(config-cmap)# match ip dscp 46
CAT3550(config-cmap)#class-map match-all CALL SIGNALING
CAT3550(config-cmap)# match ip dscp 24
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VVLAN-VOICE
CAT3550(config-cmap)# match vlan vvlan_id
CAT3550(config-cmap)# match class-map VOICE
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT3550(config-cmap)# match vlan vvlan_id
CAT3550(config-cmap)# match class-map CALL SIGNALING
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all ANY
CAT3550(config-cmap)# match access-group name ACL_Name
CAT3550(config-cmap)#
CAT3550(config-cmap)# class-map match-all VVLAN-ANY
CAT3550(config-cmap)# match vlan vvlan_id
CAT3550(config-cmap)# match class-map ANY
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all DVLAN-ANY
CAT3550(config-cmap)# match vlan dvlan_id
CAT3550(config-cmap)# match class-map ANY
CAT3550(config-cmap)#
CAT3550(config-cmap)#policy-map IPPHONE-PC
CAT3550(config-pmap)# class VVLAN-VOICE
CAT3550(config-pmap-c)# set ip dscp 46
CAT3550(config-pmap-c)# police 128000 8000 exceed-action drop
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class VVLAN-CALL-SIGNALING
CAT3550(config-pmap-c)# set ip dscp 24
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class VVLAN-ANY
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class DVLAN-ANY
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT3550(config-pmap-c)#exit
CAT3550(config-pmap)#exit
CAT3550(config)#interface interface-id
CAT3550(config-if)# switchport voice vlan vvlan_id
CAT3550(config-if)# switchport access vlan dvlan_id
CAT3550(config-if)# mls qos trust device cisco-phone
CAT3550(config-if)# service-policy input IPPHONE-PC
CAT3550(config-if)# exit
CAT3550(config)#
CAT3550(confiig)#ip access list standard ACL_ANY
CAT3550(config-std-nacl)# permit any
CAT3550(config-std-nacl)# end
CAT3550#
```

Cisco 4500（SUPIII、IV、または V 使用）

```
CAT4500(config)# qos map cos 5 to dscp 46
CAT4500(config)# qos map cos 0 24 26 46 to dscp 8
CAT4500(config)#
CAT4500(config)#class-map match-all VVLAN-VOICE
CAT4500(config-cmap)# match access-group name VVLAN-VOICE
CAT4500(config-cmap)#
CAT4500(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT4500(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
CAT4500(config-cmap)#
CAT4500(config-cmap)#class-map match-all VVLAN-ANY
CAT4500(config-cmap)# match access-group name VVLAN-ANY
CAT4500(config-cmap)#
CAT4500(config-cmap)# policy-map IPPHONE-PC
CAT4500(config-pmap)#class VVLAN-VOICE
CAT4500(config-pmap-c)# set ip dscp 46
CAT4500(config-pmap-c)# police 128 kps 8000 byte exceed-action drop
CAT4500(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT4500(config-pmap-c)# set ip dscp 24
CAT4500(config-pmap-c)# police 32 kps 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c)# class VVLAN-ANY
CAT4500(config-pmap-c)# set ip dscp 0
CAT4500(config-pmap-c)# police 32 kps 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c)# class class-default
CAT4500(config-pmap-c)# set ip dscp 0
CAT4500(config-pmap-c)# police 5 mpbs 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c)# exit
CAT4500(config-pmap)# exit
CAT4500(config)#
CAT4500(config)#
CAT4500(config)#interface interface-id
CAT4500(config-if)# switchport voice vlan vvlan_id
CAT4500(config-if)# switchport access vlan dvlan_id
CAT4500(config-if)# qos trust device cisco-phone
CAT4500(config-if)# service-policy input IPPHONE-PC
CAT4500(config-if)# exit
CAT4500(config)#
CAT4500(confiig)#ip access list extended VVLAN-VOICE
CAT4500(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384 32767
dscp ef
CAT4500(config-ext-nacl)# exit
CAT4500(config)#ip access list extended VVLAN-CALL-SIGNALING
CAT4500(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 2000 2002 dscp
cs3
CAT4500(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any eq 2443 dscp cs3
CAT4500(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any eq 5060 dscp cs3
CAT4500(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 5060 5061 dscp
cs3
CAT4500(config-ext-nacl)# exit
CAT4500(config)#ip access list extended VVLAN-ANY
CAT4500(config-ext-nacl)# permit ip Voice_IP_Subnet  Subnet_Mask any
CAT4500(config-ext-nacl)# end
CAT4500#
```

Cisco 6500

```
CAT6500> (enable) set qos cos-dscp-map 0 8 16 24 32 46 48 56
CAT6500> (enable) set qos policed-dscp-map 0, 24, 26, 46:8
CAT6500> (enable)
CAT6500> (enable) set qos policer aggregate VVLAN-VOICE rate 128 burst 8000 drop
```

```
CAT6500> (enable) set qos policer aggregate VVLAN-CALL-SIGNALING rate 32 burst 8000
policed-dscp
CAT6500> (enable) set qos policer aggregate VVLAN-ANY rate 5000 burst 8000 policed-dscp
CAT6500> (enable) set qos policer aggregate PC-DATA rate 5000 burst 8000 policed-dscp
CAT6500> (enable)
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 46 aggregate VVLAN-VOICE udp
Voice_IP_Subnet Subnet_Mask any range 16384 32767
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 24 aggregate VVLAN-CALL-SIGNALING tcp
Voice_IP_Subnet Subnet_Mask any  range 2000 2002
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 24 aggregate VVLAN-CALL-SIGNALING tcp
Voice_IP_Subnet Subnet_Mask any eq 2443
CAT6500> (enable)  set qos acl ip IPPHONE-PC dscp 24 aggregate VVLAN-CALL-SIGNALING tcp
Voice_IP_Subnet Wildcard_bits any  range 5060 5061
CAT6500> (enable)  set qos acl ip IPPHONE-PC dscp 24 aggregate VVLAN-CALL-SIGNALING udp
Voice_IP_Subnet Wildcard_bits  any  eq 5060
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 0 aggregate VVLAN-ANY Voice_IP_Subnet
Subnet_Mask any
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 0 aggregate PC-DATA any
CAT6500> (enable) commit qos acl IPPHONE-PC
CAT6500> (enable) set vlan vvlan_id mod/port
CAT6500> (enable) set port qos mod/port trust-device ciscoipphone
CAT6500> (enable) set qos acl map IPPHONE-PC mod/port
CAT6500> (enable)
```

（注） DSCP の再マーキングは、レイヤ 3 対応のスイッチが行う必要があります。アクセス レイヤ スイッチ（Cisco Catalyst 2950 with Standard Image または Cisco 3524XL など）にこの機能がない場合、DSCP の再マーキングは分散レイヤ スイッチで行う必要があります。

ソフトウェアベースのエンドポイント

Cisco Unified Personal Communicator および Cisco Unified Video Advantage を搭載した Cisco IP Communicator は両方とも音声とビデオの機能を備えており、パケット分類および DSCP 再マーキング用の ACL とポリシー マップを使用する場合に、2 つの問題が生じます。第 1 に、Cisco Unified Personal Communicator は、ソース音声とビデオ ストリームに対して、同じ IP アドレスと UDP ポート範囲を使用します。IP アドレス と ポート番号に基づく ACL は、適切な DSCP 再マーキング を適用するために音声コールとビデオ コールを区別するほど十分にきめ細かく対応していません。第 2 に、Cisco IP Communicator は、その音声パケットを送信するために、同じ IP アドレス と UDP ポートを使用します。同様に、ACL は、音声専用コールのボイス ストリームと、ビデオ コールのボイス ストリームを区別するほど十分にきめ細かく対応していません。したがって、パケット分類および DSCP 再マーキングのために ACL とポリシー マップを使用することは、ソフトウェア ベースのエンドポイントに適した QoS ソリューション にはなりません。

Cisco Unified Personal Communicator も Cisco Unified Video Advantage を搭載した Cisco IP Communicator も、シグナリング パケットおよびメディア パケットを、ネットワークに入力されるにつれて正しくマーキングするため、着信トラフィックの DSCP マーキングを信頼してトラフィック ポリシーとレート制限を適用するようにポリシー マップを設定することをお勧めします。次の項では、一般的に配置されている Cisco Catalyst スイッチ上の Cisco Unified Personal Communicator および Cisco IP Communicator に対して実行できるコンフィギュレーション コマンドをリストします。

（注） Cisco Catalyst 2950 シリーズ スイッチを、ソフトウェアベースのエンドポイント QoS の実装で使用することは推奨されていません。その理由は、Cisco 2950 が、FastEthernet ポートで 1 Mbps の増分だけサポートしているからです。これにより、許可されていないネットワーク トラフィックにかなり大きいホールが発生し、コール シグナリングまたはメディアの模倣が発生することがあります。

Cisco 2970、3560 または 3750

```
CAT2970 (config)#mls qos
CAT2970 (config)#mls qos map policed-dscp 0 24 26 46 to 8
CAT2970 (config)#
CAT2970 (config)#class-map match-all SOFTWARE-BASED-ENDPOINT-VOICE
CAT2970 (config-cmap)#  match access-group name SOFTWARE-BASED-ENDPOINT-VOICE
CAT2970 (config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-VIDEO
CAT2970 (config-cmap)#  match access-group name SOFTWARE-BASED-ENDPOINT-VIDEO
CAT2970 (config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-SIGNALING
CAT2970 (config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-SIGNALING
CAT2970 (config-cmap)#exit
CAT2970 (config)#
CAT2970 (config)#policy-map SOFTWARE-BASED-ENDPOINT
CAT2970 (config-pmap-c)#class SOFTWARE-BASED-ENDPOINT-VOICE
CAT2970 (config-pmap-c)# police 128000 8000 exceed-action drop
CAT2970 (config-pmap-c)#class SOFTWARE-BASED-ENDPOINT-VIDEO
CAT2970 (config-pmap-c)# police 50000000 8000 exceed-action policed-dscp-transmit
CAT2970 (config-pmap-c)#class SOFTWARE-BASED-ENDPOINT-SIGNALING
CAT2970 (config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970 (config-pmap-c)#class class-default
CAT2970 (config-pmap-c)# set ip dscp 0
CAT2970 (config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT2970 (config-pmap-c)# exit
CAT2970 (config-pmap)#exit
CAT2970 (config)#
CAT2970 (config)#interface FastEthernet interface-id
CAT2970 (config-if)# switchport access vlan dvlan_id
CAT2970 (config-if)# switchport mode access
CAT2970 (config-if)# service-policy input SOFTWARE-BASED-ENDPOINT
CAT2970 (config-if)# exit
CAT2970 (config)#ip access-list extended SOFTWARE-BASED-ENDPOINT-SIGNALING
CAT2970 (config-ext-nacl)#permit ip PC_Subnet_Source wildcard_bits any dscp 24
CAT2970 (config-ext-nacl)#exit
CAT2970 (config)#ip access-list extended SOFTWARE-BASED-ENDPOINT-VIDEO
CAT2970 (config-ext-nacl)#permit ip PC_Subnet_Source wildcard_bits any dscp 34
CAT2970 (config-ext-nacl)#exit
CAT2970 (config)#ip access-list extended SOFTWARE-BASED-ENDPOINT-VOICE
CAT2970 (config-ext-nacl)# permit ip PC_Subnet_Source wildcard_bits any dscp 46
CAT2970 (config-ext-nacl)#exit
CAT2970 (config)#exit
```

Cisco 3550

```
3550(config)#class-map match-all SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-cmap)#match access-group name SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-cmap)#exit
3550(config)#
3550(config)#policy-map SOFTWARE-BASED-ENDPOINT
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-pmap)# police 128000 8000 exceed-action drop
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-pmap)# police 50000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-pmap)# police 32000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class class-default
3550(config-pmap)# set ip dscp 0
3550(config-pmap)# police 5000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)# exit
```

```
3550(config)#exit
3550(config)#
3550(config)#interface FastEthernet interface_id
3550(config-if)# switchport access vlan dvlan_id
3550(config-if)# switchport mode access
3550(config-if)# service-policy input SOFTWARE-BASED-ENDPOINT
3550(config-if)# exit
3550(config)#ip access-list extended SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-ext-nacl)#permit ip PC_Subnet_Source wildcard_bits any dscp 24
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-ext-nacl)#permit ip PC_Subnet_Source wildcard_bits any dscp 34
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-ext-nacl)# permit ip PC_Subnet_Source wildcard_bits any dscp 46
3550(config-ext-nacl)#exit
3550(config)#exit
```

Cisco 6500

```
CAT6500> (enable) set qos enable
CAT6500> (enable) set qos policed-dscp-map 0, 24, 26, 34, 46:8
CAT6500> (enable)
CAT6500> (enable) set qos policer aggregate SOFTWARE-BASED-ENDPOINT-VOICE rate 128 burst
8000 drop
CAT6500> (enable) set qos policer aggregate SOFTWARE-BASED-ENDPOINT-VIDEO rate 5000 burst
8000 policed-dscp
CAT6500> (enable) set qos policer aggregate SOFTWARE-BASED-ENDPOINT-SIGNAL rate 32 burst
8000 policed-dscp
CAT6500> (enable) set qos policer aggregate SOFTWARE-BASED-ENDPOINT-DEFAULT rate 5000
burst 8000 policed-dscp
CAT6500> (enable)
CAT6500> (enable) set qos acl ip SOFTWARE-BASED-ENDPOINT trust-dscp aggregate
SOFTWARE-BASED-ENDPOINT-VOICE ip PC_Subnet_Source wildcard_bits any dscp-field 46
CAT6500> (enable) set qos acl ip SOFTWARE-BASED-ENDPOINT trust-dscp aggregate
SOFTWARE-BASED-ENDPOINT-VIDEO ip PC_Subnet_Source wildcard_bits any dscp-field 34
CAT6500> (enable) set qos acl ip SOFTWARE-BASED-ENDPOINT trust-dscp aggregate
SOFTWARE-BASED-ENDPOINT-SIGNAL ip PC_Subnet_Source wildcard_bits any dscp-field 24
CAT6500> (enable) set qos acl ip SOFTWARE-BASED-ENDPOINT  dscp 0 aggregate
SOFTWARE-BASED-ENDPOINT-DEFAULT any
CAT6500> (enable) commit qos acl SOFTWARE-BASED-ENDPOINT
CAT6500> (enable) set vlan dvlan_id mod/port
CAT6500> (enable) set port qos mod/port trust untrusted
CAT6500> (enable) set qos acl map SOFTWARE-BASED-ENDPOINT  mod/port
```

Cisco Unified Wireless IP Phones

デフォルトでは、Cisco Unified Wireless IP Phone および無線で接続された Cisco Unified IP Phones 9971 は、Per-Hop Behavior（PHB）値 CS3、または Differentiated Services Code Point（DSCP）値 24（ToS 値 0x60 に相当）を使用して SCCP シグナリング メッセージをマーキングし、PHB 値 EF、または DSCP 値 46（ToS 値 0xB8 に相当）を使用して RTP 音声パケットをマーキングします。AP でキューイングが正しく設定されており、アップストリームの最初のホップのスイッチが AP のポートを信頼するように設定されている場合、無線 IP Phone のトラフィックは、有線 IP Phone のトラフィックと同じように処理されます。この方法により、LAN と WLAN 環境で QoS 設定の一貫性を保つことができます。

また、Cisco Unified Wireless IP Phone および Cisco Unified IP Phone 9971 は、無線で接続されたときに Cisco Discovery Protocol（CDP）を使用してその存在を AP に自動的にアナウンスします。CDP パケットは無線 IP Phone から AP に送信され、これらのパケットにより電話機が特定されます。これにより、AP は、その IP Phone へのすべてのトラフィックを高プライオリティ キューに入れることができます。

設定例が示しているとおり、AP から送られるパケットは信頼されている必要があり、各パケットの VLAN タグに基づいて DSCP マーキングを保持またはダウンとマーキングする必要があります。このように、音声 VLAN 上の Cisco Unified Wireless IP Phone が送信元であるパケットは、適切な DSCP マーキングを保持する必要があり、データ VLAN 上のデータ デバイスが送信元であるパケットは、DSCP 値 0 に再マーキングする必要があります。

Cisco 3550

```
CAT3550(config)#mls qos
CAT3550(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VOICE-SIGNALING
CAT3550(config-cmap)#match ip dscp 24
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VOICE
CAT3550(config-cmap)#match ip dscp 46
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-DATA
CAT3550(config-cmap)#match any
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-VVLAN-VOICE
CAT3550(config-cmap)#match vlan vvlan-id
CAT3550(config-cmap)#match class-map VOICE
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-VVLAN-VOICE-SIGNALING
CAT3550(config-cmap)#match vlan vvlan-id
CAT3550(config-cmap)#match class-map VOICE-SIGNALING
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-DVLAN
CAT3550(config-cmap)#match vlan dvlan-id
CAT3550(config-cmap)#match class-map INGRESS-DATA
CAT3550(config-cmap)#
CAT3550(config-pmap-c)#policy-map INGRESS-QOS
CAT3550(config-pmap)#class INGRESS-VVLAN-VOICE
CAT3550(config-pmap-c)#set ip dscp 46
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class INGRESS-VVLAN-VOICE-SIGNALING
CAT3550(config-pmap-c)#set ip dscp 24
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class INGRESS-DVLAN
CAT3550(config-pmap-c)#set ip dscp 0
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class class-default
CAT3550(config-pmap-c)#set ip dscp 0
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#interface interface id
CAT3550(config-if)#description Wireless Access Point
CAT3550(config-if)#switchport access dvlan-id
CAT3550(config-if)#switchport voice vvlan-id
CAT3550(config-if)#mls qos trust dscp
CAT3550(config-if)#service-policy input INGRESS-QOS
```

Cisco 6500

```
CAT6500> (enable) set qos enable
CAT6500> (enable) set qos cos-dscp-map 0 8 16 24 32 46 48 56
```

```
CAT6500> (enable)
CAT6500> (enable) set qos acl ip AP-VOICE-INGRESS trust-dscp ip any any
CAT6500> (enable) set qos acl ip AP-DATA-INGRESS dscp 0 ip any any
CAT6500> (enable)
CAT6500> (enable) set qos acl map AP-VOICE-INGRESS vvlan-id input
CAT6500> (enable) set qos acl map AP-DATA-INGRESS dvlan-id input
CAT6500> (enable)
CAT6500> (enable) set port qos mod/port vlan-based
CAT6500> (enable)
CAT6500> (enable) set port qos mod/port trust trust-dscp
CAT6500> (enable)
```

ビデオ テレフォニー エンドポイント

ここでは、次のタイプのエンドポイント デバイスでトラフィックがどのように分類されるかについて説明します。

- 「Cisco Unified Video Advantage と Cisco Unified IP Phone」（P.20-42）
- 「Cisco IP Video Phone 7985G」（P.20-44）
- 「Sony 社製と Tandberg 社製の SCCP エンドポイント」（P.20-45）
- 「H.323 と SIP のビデオ エンドポイント」（P.20-46）

Cisco Unified Video Advantage と Cisco Unified IP Phone

ユーザの PC 上にある Cisco Unified Video Advantage アプリケーションは、DSCP を使用したビデオ トラフィックの分類をサポートし、レイヤ 3 だけで分類を行えます。Cisco Unified Communications の設計上の現在のベスト プラクティスとしては、電話機が接続されたアップストリーム イーサネット スイッチを、電話機からの 802.1p CoS を信頼するよう設定する必要があります。PC パケットは 802.1Q タグを持つ可能性が低いため、802.1p CoS ビットはサポートできません。このように PC が 802.1p をサポートしないため、次のオプションで Cisco Unified Video Advantage に QoS を実現できます。

オプション 1

現在の QoS モデルで信頼を IP Phone にまで広げた場合、ネットワークへの着信時に音声パケットとシグナリング パケットは正しくマーキングされます。ポートに UDP ポート 5445 と一致する ACL を追加すると、ビデオ メディア チャネルも PHB AF41 に分類されます。この ACL がないと、ビデオ メディアは Best Effort に分類されて、画像の品質低下やリップシンクの問題が起きます。同じ ACL を使用すると、TCP ポート 4224（CS3 と分類）を使用した、Cisco Unified Video Advantage PC と IP Phone 間の CAST 接続の照合も可能ですが、このことで得られる利点はほとんどありません。データ VLAN 上にある PC からのシグナリング パケットは、同じ高速ポート経由で音声 VLAN に返されます。したがって、パケットで輻輳が発生する可能性は非常に低くなります。

次の例は、このオプションの設定方法を示しています。

```
3550(config)#class-map match-all SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-cmap)#match access-group name SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-cmap)#exit
3550(config)#
3550(config)#policy-map SOFTWARE-BASED-ENDPOINT
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-VOICE
```

```
3550(config-pmap)# police 128000 8000 exceed-action drop
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-pmap)#set ip dscp 34
3550(config-pmap)# police 50000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-pmap)#set ip dscp 24
3550(config-pmap)# police 32000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class class-default
3550(config-pmap)# set ip dscp 0
3550(config-pmap)# police 5000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)# exit
3550(config)#exit
3550(config)#
3550(config)#interface FastEthernet interface_id
3550(config-if)# switchport access vlan dvlan_id
3550(config-if)# switchport mode access
3550(config-if)# service-policy input SOFTWARE-BASED-ENDPOINT
3550(config-if)# exit
3550(config)#ip access-list extended SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-ext-nacl)#permit ip PC_Subnet_Source wildcard_bits any dscp 24
3550(config-ext-nacl)#permit tcp PC_Subnet_Source wildcard_bits eq 4224 any
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-ext-nacl)#permit ip PC_Subnet_Source wildcard_bits any dscp 34
3550(config-ext-nacl)#permit udp PC_Subnet_Source wildcard_bits eq 5445 any
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-ext-nacl)# permit ip PC_Subnet_Source wildcard_bits any dscp 46
3550(config-ext-nacl)#exit
3550(config)#exit
```

オプション 2

『*Enterprise QoS Solution Reference Network Design Guide*』のバージョン 3.1（http://www.cisco.com/go/designzone で入手可能）には、別の方法が示されています。この方法で推奨されていることは、CoS を信頼する代わりに、着信トラフィックの DSCP を信頼するようにポートを変更し、一連の Per-Port/Per-VLAN アクセス コントロール リストに着信パケットを通過させることです。このアクセス コントロール リストでは、そのとき他の基準とともに TCP/UDP ポートに基づいてパケットが照合され、適切なレベルにポリシングされます。たとえば、DSCP を信頼するようにスイッチ ポートが設定されている状態では、Cisco Unified Video Advantage はビデオ パケットに DSCP AF41 とマーキングします。パケットは ACL で照合されますが、その照合は、パケットが UDP ポート 5445 を使用し、DSCP AF41 とマーキングされ、データ VLAN 上に着信していることに基づいて行われます。この ACL は、その後、DSCP を信頼してトラフィックを N kbps（N はポートごとに許可するビデオ帯域幅）にポリシングするために、クラス マップまたはポリシー マップで使用されます。類似した ACL やポリシング機能が、音声 VLAN 内の IP Phone からの音声パケットやシグナリング パケットに存在します。

次の例は、このオプションの設定方法を示しています。

```
3550(config)#class-map match-all SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-cmap)#match access-group name SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-cmap)#exit
3550(config)#
3550(config)#policy-map SOFTWARE-BASED-ENDPOINT
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-pmap)# police 128000 8000 exceed-action drop
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-VIDEO
```

```
3550(config-pmap)#set ip dscp 34
3550(config-pmap)# police 50000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-pmap)#set ip dscp 24
3550(config-pmap)# police 32000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class class-default
3550(config-pmap)# set ip dscp 0
3550(config-pmap)# police 5000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)# exit
3550(config)#exit
3550(config)#
3550(config)#interface FastEthernet interface_id
3550(config-if)# switchport access vlan dvlan_id
3550(config-if)# switchport mode access
3550(config-if)# service-policy input SOFTWARE-BASED-ENDPOINT
3550(config-if)# exit
3550(config)#ip access-list extended SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-ext-nacl)#permit tcp PC_Subnet_Source wildcard_bits eq 4224 any dscp 24
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-ext-nacl)#permit udp PC_Subnet_Source wildcard_bits eq 5445 any dscp 34
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-ext-nacl)# permit ip PC_Subnet_Source wildcard_bits any dscp 46
3550(config-ext-nacl)#exit
3550(config)#exit
```

Cisco IP Video Phone 7985G

他の多くの Cisco Unified IP Phone と同様に、Cisco IP Video Phone 7985G は、電話機からの発信トラフィック用に 802.1p/Q タギングをサポートしています。また、Cisco IP Video Phone 7985G は PC アクセス用に別のイーサネット インターフェイスを備えているため、接続デバイスからの発信トラフィックもサポートしています。Cisco Unified Communications の設計上の現在のベスト プラクティスとしては、電話機が接続されたアップストリーム イーサネット スイッチを、電話機からの 802.1p CoS を信頼するよう設定する必要があります。信頼を電話機の PC ポートにまで広げないことをお勧めしますが、スイッチでサポートされているときは、音声、ビデオ、およびシグナリングのトラフィックの最大量を制限するようにポリシング機能を設定することをお勧めします。

次に、このタイプの設定例を示します。

```
3550(config)#class-map match-all C7985-ENDPOINT-VOICE
3550(config-cmap)#match access-group name C7985-ENDPOINT-VOICE
3550(config-cmap)#class-map match-all C7985-ENDPOINT-VIDEO
3550(config-cmap)# match access-group name C7985-ENDPOINT-VIDEO
3550(config-cmap)#class-map match-all C7985-ENDPOINT-SIGNALING
3550(config-cmap)# match access-group name C7985-ENDPOINT-SIGNLAING
3550(config-cmap)#exit
3550(config)#
3550(config)#policy-map C7985-ENDPOINT
3550(config-pmap)#class C7985-ENDPOINT-VOICE
3550(config-pmap)# police 128000 8000 exceed-action drop
3550(config-pmap)#class C7985-ENDPOINT-VIDEO
3550(config-pmap)#set ip dscp 34
3550(config-pmap)# police 50000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class C7985-ENDPOINT-SIGNALING
3550(config-pmap)#set ip dscp 24
3550(config-pmap)# police 32000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class class-default
3550(config-pmap)# set ip dscp 0
3550(config-pmap)# police 5000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)# exit
```

```
3550(config)#exit
3550(config)#
3550(config)#interface FastEthernet interface_id
3550(config-if)# switchport access vlan dvlan_id
3550(config-if)# switchport mode access
3550(config-if)# service-policy input C7985-ENDPOINT
3550(config-if)# exit
3550(config)#ip access-list extended C7985-ENDPOINT-SIGNALING
3550(config-ext-nacl)#permit ip Voice_IP_Subnet Subnet_Mask any dscp 24
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended C7985-ENDPOINT-VIDEO
3550(config-ext-nacl)#permit ip Voice_IP_Subnet Subnet_Mask any dscp 34
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended C7985-ENDPOINT-VOICE
3550(config-ext-nacl)# permit ip Voice_IP_Subnet Subnet_Mask any dscp 46
3550(config-ext-nacl)#exit
3550(config)#exit
```

Sony 社製と Tandberg 社製の SCCP エンドポイント

Sony 社製と Tandberg 社製の SCCP エンドポイントは、DSCP を使用してレイヤ 3 でメディア パケットおよびシグナリング パケットを正しくマーキングします。ただし、802.1Q をサポートしていないため、802.1p CoS を使用して分類できません。UDP と TCP のポート照合オプションを使用した場合、SCCP シグナリングを CS3 として、またビデオ メディアを AF41 として正しく分類できますが、UDP ポートが音声だけのコールで使用されている場合は判別ができないため、EF としての分類が必要になります。そのような場合、コール アドミッション制御メカニズムは帯域幅を正しく処理できません。この状況を避けるために、Sony 社製または Tandberg 社製のエンドポイントからのトラフィックを分類して信頼する方法として実行可能なオプションは、次の 1 つだけです。

オプション 1

Sony 社製または Tandberg 社製のエンドポイントで使用されているポート上で DSCP を信頼します。スイッチで許可されている場合は、そのポート上で受信可能な EF、AF41、CS3 トラフィックの最大量を制限するようにポリシング機能を設定します。そのポートに接続された他のデバイスは、DSCP を使用してパケットが分類されていても、信頼できるとは限りません。このオプションは、Sony 社製または Tandberg 社製のシステムがオフィスや小規模な会議室に固定的に設置されている場合に適しています。

Sony 社製または Tandberg 社製のデバイスは CDP をサポートしていないため、このエンドポイントを音声 VLAN に配置する必要がある場合は、VLAN に配置するときに手動の修正が必要です。音声 VLAN にエンドポイントを直接配置することの利点は、システム内の他の IP テレフォニー エンドポイントと同様に扱えることです。欠点は、ポートが音声 VLAN に直接アクセスするため、セキュリティ上のリスクが発生する可能性があることです。一方、Sony 社製または Tandberg 社製のエンドポイントをデータ VLAN に残すこともできますが、Unified CM に対する SCCP シグナリングを許可し、UDP メディア ストリームが音声コール中またはビデオ コール中にデータ VLAN および音声 VLAN 間を通過できるようにするには、データ VLAN と音声 VLAN 間のアクセスでのプロビジョニングが必要です。

次の例は、このオプションの設定方法を示しています。

```
CAT2970(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT2970(config)# mls qos map policed-dscp 0 24 to 8
CAT2970(config)#class-map match-all VVLAN-VOICE
CAT2970(config-cmap)# match access-group name VVLAN-VOICE
CAT2970(config-cmap)#class-map match-all VVLAN-VIDEO
CAT2970(config-cmap)# match access-group name VVLAN-VIDEO
CAT2970(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT2970(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
```

```
CAT2970(config-cmap)#class-map match-all VVLAN-ANY
CAT2970(config-cmap)# match access-group name VVLAN-ANY
CAT2970(config-cmap)# policy-map SCCP-VIDEO-ENDPOINT
CAT2970(config-pmap)#class VVLAN-VOICE
CAT2970(config-pmap-c)# set ip dscp 46
CAT2970(config-pmap-c)# police 128000 8000 exceed-action drop
CAT2970(config-pmap)#class VVLAN-VIDEO
CAT2970(config-pmap-c)# set ip dscp 34
CAT2970(config-pmap-c)# police 1500000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-ANY
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)# exit
CAT2970(config)#interface interface-id
CAT2970(config-if)# switchport voice vlan vvlan_id
CAT2970(config-if)# mls qos trust device cisco-phone
CAT2970(config-if)# service-policy input SCCP-VIDEO-ENDPOINT
CAT2970(config-if)# exit
CAT2970(confiig)#ip access list extended VVLAN-VOICE
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384 32767
dscp ef
CAT2970(config-ext-nacl)# exit
CAT2970(confiig)#ip access list extended VVLAN-VIDEO
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384 32767
dscp af41
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-CALL-SIGNALING
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 2000 2002 dscp
cs3
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any eq 5060 dscp cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 5060 5061 dscp
cs3
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-ANY
CAT2970(config-ext-nacl)# permit ip Voice_IP_Subnet  Subnet_Mask any
CAT2970(config-ext-nacl)# end
```

H.323 と SIP のビデオ エンドポイント

このタイプのエンドポイントは、H.323 および SIP ビデオ エンドポイントにはさまざまなものがあり、実装と機能も多様なため、QoS の点で大きな課題があります。これらのエンドポイントには主に 2 つの QoS オプションがあります。1 つは、H.323 または SIP のビデオ エンドポイントに依存してすべてのトラフィックのマーキングを正しく行う方法で、もう 1 つは、使用する TCP ポートおよび UDP ポートの詳細な認識に依存する方法です。

オプション 1

エンドポイントがメディア トラフィックおよびシグナリング トラフィックのマーキングを正しく行った場合は（シグナリングには SIP、H.225、H.245、および RAS が含まれる）、その分類を信頼できます。エンドポイントで 802.1Q（結果的に 802.1p CoS）がサポートされる可能性は低いため、この場合は IP Precedence または DSCP を使用します。分類タイプの選択は、そのベンダー、モデル、およびソフトウェア バージョンに左右されます。

（注）　H.323 または SIP のエンドポイントがそのパケットのマーキングを正しく行う可能性は非常に低くなります。

オプション 2

送信元、宛先、または TCP と UDP の両方のポート番号（多くは、IP アドレスも含む）を組み合せて使用することによって、トラフィックを正しく照合および分類する ACL を定義できます。さらに、ポリシング機能も適用し、ネットワークで許可されるトラフィック クラスごとにその量を制限することもお勧めします。このオプションには、オプション 1 と同様に、音声だけのコールを誤って分類する可能性があります。

次の例は、このオプションの設定方法を示しています。

```
CAT2970(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT2970(config)# mls qos map policed-dscp 0 24 to 8
CAT2970(config)#
CAT2970(config)#class-map match-all VVLAN-VIDEO
CAT2970(config-cmap)# match access-group name VVLAN-VIDEO
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT2970(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-ANY
CAT2970(config-cmap)# match access-group name VVLAN-ANY
CAT2970(config-cmap)#
CAT2970(config-cmap)# policy-map SCCP-VIDEO-ENDPOINT
CAT2970(config-pmap)#class VVLAN-VIDEO
CAT2970(config-pmap-c)# set ip dscp 34
CAT2970(config-pmap-c)# police 1500000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-ANY
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)# exit
CAT2970(config)#interface interface-id
CAT2970(config-if)# switchport voice vlan vvlan_id
CAT2970(config-if)# mls qos trust device cisco-phone
CAT2970(config-if)# service-policy input SCCP-VIDEO-ENDPOINT
CAT2970(config-if)# exit
CAT2970(config)#
CAT2970(confiig)#ip access list extended VVLAN-VIDEO
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384 32767
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-CALL-SIGNALING
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any eq 1719 dscp cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any eq 1720 dscp cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 11000 65535
dscp cs3
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any eq 5060 dscp cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 5060 5061 dscp
cs3
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-ANY
CAT2970(config-ext-nacl)# permit ip Voice_IP_Subnet  Subnet_Mask any
CAT2970(config-ext-nacl)# end
```

（注）　上記の設定方法は、音声専用コールの場合でも、音声トラフィックをビデオ トラフィックと同様にマーキングします。シグナリングおよびRTP ポートの使用方法はベンダーごとに異なるため、上記の例での使用方法と異なる場合は、適切なポート範囲を使用する必要があります。

エンドポイント機能の要約

次の各表は、この章で説明した各種のエンドポイント デバイスでサポートされる機能を要約したものです。

- 表 20-6 は、Cisco アナログ ゲートウェイの Cisco Unified Communications 機能を要約したものです。
- 表 20-7 は、Skinny Client Control Protocol（SCCP）を使用する Cisco ベーシック IP Phone の機能を要約したものです。
- 表 20-8 は、Session Initiation Protocol（SIP）を使用する Cisco ベーシック IP Phone の機能を要約したものです。
- 表 20-9 は、SCCP を使用する Cisco ビジネス IP Phone の機能を要約したものです。
- 表 20-10 は、SIP を使用する Cisco ビジネス IP Phone の機能を要約したものです。
- 表 20-11 は、SCCP プロトコルを使用する Cisco ビジネス、マネージャ、およびエグゼクティブの各 IP Phone の機能を要約したものです。
- 表 20-12 は、SIP プロトコルを使用する Cisco ビジネス、マネージャ、およびエグゼクティブの各 IP Phone の機能を要約したものです。
- 表 20-13 は、Cisco Unified IP Phone 7921G、7925G、7936、7937G、7985G などの専用エンドポイントの機能を要約したものです。
- 表 20-14 は、Cisco Unified Personal Communicator および Cisco IP Communicator を含むソフトウェア ベースのデバイスの機能を要約したものです。

表 20-6　Cisco アナログ ゲートウェイの機能

機能	アナログ インターフェイス カード	Ws-svc-cmm-24fxs	Ws-x6624 FXS	VG202	VG204	VG224	VG248	ATA 186 および 188
イーサネット接続	×	×	×	○[1]	○[1]	○[1]	○[2]	○[3]
アナログ ポートの最大数	24[4]	72	24	2	4	24	48	2
発信者 ID	○	×	×	○	○	○	○	○
コール ウェイティング	×	×	×	○	○	○	○	○
コール ウェイティング時の発信者 ID	×	×	×	○	○	○	○	○
保留	×	×	×	○	○	○[5]	○	○
コール転送	×	×	×	○	○	○[5]	○	○
自動転送	×	×	×	○	○	○	○[6]	○
自動応答	×	×	×	×	×	×	×	×
Ad Hoc 会議	×	×	×	○	○	○	○	○

表 20-6　Cisco アナログ ゲートウェイの機能 （続き）

機能	アナログ インター フェイス カード	Ws-svc -cmm -24fxs	Ws-x6624 FXS	VG202	VG204	VG224	VG248	ATA 186 および 188
Meet-Me 会議	×	×	×	○	○	×	×	○
コール ピックアップ	×	×	×	○	○	○	×	○
グループ ピックアップ	×	×	×	○	○	○	×	○
リダイヤル	×	×	×	○	○	○	○[7]	○[7]
短縮ダイヤル	×	×	×	○	○	○	○	○
オンフック ダイヤル	×	×	×	×	×	×	×	×
ボイスメールへのアクセス	○	○	○	○	○	○	○	○[8]
メッセージ待機インジケータ（MWI）	×	×	×	○	○	×	○	○[8]
Stutter Dial Tone または Audible Message Waiting Indication（AMWI）	×	×	×	○	○	○	○	○[8]
Survivable Remote Site Telephony（SRST）サポート	×	×	×	○	○	○	○	○
Music on Hold（MoH）	○	○	○	○	○	×	○	○
消音	×	×	×	×	×	×	×	×
Multilevel Precedence and Preemption（MLPP）	×	×	×	○	○	×	×	×
割り込み	×	×	×	×	×	×	×	×
C 割り込み	×	×	×	×	×	×	×	×
ワンボタン割り込み	×	×	×	×	×	×	×	×
回線をまたいで参加	×	×	×	×	×	×	×	×
プログラム可能な回線キー	×	×	×	×	×	×	×	×
「Single Call per Line」ユーザ エクスペリエンス	×	×	×	×	×	×	×	×
ビジー ランプ フィールド	×	×	×	×	×	×	×	×
+ ダイヤリングを使用する発番号の標準化	×	×	×	×	×	×	×	×
コール保持	×	×	×	×	×	×	○[9]	×
コール アドミッション制御	○	×	×	×	×	×	×	×
ローカル ボイス ビジーアウト	○	×	×	×	×	×	×	×
PLAR（Private Line Automatic Ringdown）	○	×	×	×	×	×	×	○
ハント グループ	○	×	×	×	×	×	×	×
ダイヤル プランのマッピング	○	×	×	×	×	×	×	×
監視切断	○	×	×	×	×	×	×	×
シグナリング パケット ToS 値のマーキング	0x68	0x68[10]	0x68	0x68	0x68	0x68	0x68	0x68

表 20-6　Cisco アナログ ゲートウェイの機能 （続き）

機能	アナログ インター フェイス カード	Ws-svc -cmm -24fxs	Ws-x6624 FXS	VG202	VG204	VG224	VG248	ATA 186 および 188
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
FAX パススルー	○[11]	○	○[12]	○	○	○	○[11]	○
FAX リレー	○	○	×	○	○	○	○	×
Skinny Client Control Protocol（SCCP）	×	×	×	○	○	○	○	○
セッション開始プロトコル（SIP）	×	×	×	○	○	○	×	○
H.323	○	○	×	○	○	○	×	○
メディア ゲートウェイ コントロール プロトコル（MGCP）	○	○	○	○	○	○	×	○[13]
G.711	○	○	○	○	○	○	○	○
G.722	×	×	×	×	×	×	×	×
G.723	○	○	×	×	×	×	×	○
G.726	○	×	×	×	×	×	×	×
G.729	○	○	○	○	○	○	○	○
音声アクティビティ検出（VAD）	○	○	×	○	○	○	×	○
コンフォート ノイズ生成（CNG）	○	○	×	○	○	○	×	○

1. 2 つの 10/100 Base-T。
2. 1 つの 10/100 Base-T。
3. ATA 188 では 2 つの 10/100 Base-T、ATA 186 では 1 つの 10 Base-T。
4. EVM-HD-8FXS/DID は、基本ボード上に 8 つのポートがあり、FXS または DID シグナリング用に構成可能です。また、EM-HDA-8FXS には 2 つの拡張モジュールを取り付けることができます。
5. H.323 および SIP での呼制御。
6. Call Forward All。
7. リダイヤル。
8. SCCP および SIP バージョンだけ。
9. VG248 バージョン 1.2 以降でサポート。
10. UDP ポート 2427 では MGCP シグナリングをマーキングしますが、TCP ポート 2428 ではベストエフォート型の MGCP キープアライブ パケットをマーキングします。
11. FAX パススルーおよび FAX リレー。
12. FAX パススルー。
13. Unified CM は、ATA を使用する MGCP をサポートしていません。

表 20-7　SCCP を使用する Cisco Basic IP Phone

機能	7902G	7905G	7906G	7910G	7910 +SW	7911G	7912G/G-A
イーサネット接続	○[1]	○[1]	○[2]	○[1]	○[3]	○[3]	○[3]
イーサネット スイッチ（PC ポート）	×	×	○	×	○	○	○[4]
Cisco Power-Over-Ethernet（PoE）	○	○	○	○	○	○	○

表 20-7　SCCP を使用する Cisco Basic IP Phone （続き）

機能	7902G	7905G	7906G	7910G	7910 +SW	7911G	7912G/G-A
IEEE 802.3af Power-Over-Ethernet（PoE）	×	×	○	×	×	○	×
ローカリゼーション	×	○	○	×	×	○	○
ディレクトリ番号	1	1	1	1	1	1	1
回線あたりの最大コール数	200	200	200	200	200	200	200
液晶ディスプレイ	×	○	○	○	○	○	○
発信者 ID	×	○	○	○	○	○	○
コール ウェイティング	×	○	○	○	○	○	○
コール ウェイティング時の発信者 ID	×	○	○	○	○	○	○
保留	○	○	○	○	○	○	○
ブラインド転送	×	×	×	×	×	×	×
初期在席転送	○	○	○	○	○	○	○
打診転送	○	○	○	○	○	○	○
自動転送	○	○	○	○	○	○	○
自動応答	×	○[5]	○[5]	×	×	○[5]	○[5]
Ad Hoc 会議	○	○	○	○	○	○	○
Meet-Me 会議	×	○	○	○	○	○	○
コール ピックアップ	×	○	○	○	○	○	○
グループ ピックアップ	×	○	○	○	○	○	○
リダイヤル	○[6]	○[6]	○[6]	○[6]	○[6]	○[6]	○[6]
短縮ダイヤル	○	○	○	○	○	○	○
オンフック ダイヤル	×	○	○	○	○	○	○
ボイスメールへのアクセス	○	○	○	○	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	○	○	○	○
Stutter Dial Tone または Audible Message Waiting Indication（AMWI）	×	×	○	×	×	○	×
ビデオ コール	×	×	×	×	×	×	×
Survivable Remote Site Telephony（SRST）サポート	○	○	○	○	○	○	○
ユニキャスト MoH	○	○	○	○	○	○	○
マルチキャスト MoH	○	○	○	○	○	○	○
保留音	○	○	○	○	○	○	○
スピーカー	×	○[5]	○[5]	○[5]	○[5]	○[5]	○[5]
ヘッドセット ジャック	×	×	×	×	×	×	×
消音	×	×	×	○	○	×	×
Multilevel Precedence and Preemption（MLPP）	○	○	○	○	○	○	○
割り込み	×	×	○	×	×	○	○
C 割り込み	×	○	○	×	×	○	○

表 20-7　SCCP を使用する Cisco Basic IP Phone （続き）

機能	7902G	7905G	7906G	7910G	7910 +SW	7911G	7912G/G-A
ワンボタン割り込み	×	×	×	×	×	×	×
回線をまたいで参加	×	×	×	×	×	×	×
プログラム可能な回線キー	×	×	×	×	×	×	×
「Single Call per Line」ユーザ エクスペリエンス	×	×	×	×	×	×	×
ビジー ランプ フィールド	×	×	×	×	×	×	×
+ ダイヤリングを使用する発番号の標準化	×	×	×	×	×	×	×
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	○	○	○	○
シグナリングおよびメディア暗号化	×	×	○	×	×	○	×
シグナリングの完全性	×	×	○	×	×	○	×
製造元でインストールされる証明書（X.509v3）	×	×	○	×	×	○	×
現場でインストールされる証明書	×	×	○	×	×	○	×
サードパーティの XML サービス	×	○	○	×	×	○	○
外部マイクおよびスピーカー	×	×	×	×	×	×	×
ダイヤル プラン	×	×	×	×	×	×	×
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	○	○	○	○	○	○	○
G.722	×	×	○	×	×	○	×
G.723	×	×	×	×	×	×	×
G.726	×	○	×	×	×	×	×
G.729	○	○	○	○	○	○	○
iLBC	×	×	○	×	×	○	×
ワイドバンド オーディオ	×	×	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×	×	×
音声アクティビティ検出（VAD）	○	○	○	○	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○	○	○	○	○
DTMF：H.245	×	×	×	×	×	×	×
DTMF：SCCP	○	○	○	○	○	○	○
DTMF：RFC2833	×	×	○	×	×	○	×
DTMF：KPML	×	×	×	×	×	×	×
DTMF：無指定の NOTIFY	×	×	×	×	×	×	×

1. 1 つの 10 Base-T。
2. 1 つの 10/100 Base-T。
3. 2 つの 10/100 Base-T。

4. Cisco Unified IP Phone 7912G-A は、イーサネット スイッチの拡張バージョンを備えています。
5. 一方向のオーディオ モニタ モード。
6. リダイヤル。

表 20-8　SIP を使用する Cisco Basic IP Phone

機能	3911	7905G	7906G	7911G	7912G/G-A
イーサネット接続	○[1]	○[2]	○[1]	○[3]	○[1]
イーサネット スイッチ（PC ポート）	×	×	○	○	○[4]
Cisco Power-Over-Ethernet（PoE）	×	○	○	○	○
IEEE 802.3af Power-Over-Ethernet（PoE）	○	×	○	○	×
ローカリゼーション	○	×	○	○	×
ディレクトリ番号	1	1	1	1	1
回線あたりの最大コール数	2	2	50	50	2
液晶ディスプレイ	○	○	○	○	○
発信者 ID	○	○	○	○	○
コール ウェイティング	○	○	○	○	○
コール ウェイティング時の発信者 ID	○	○	○	○	○
保留	○	○	○	○	○
ブラインド転送	×	○	○	○	○
初期在席転送	○	×	○	○	×
打診転送	○	○	○	○	○
自動転送	○[5]	○[5]	○	○	○[5]
自動応答	×	×	○[6]	○[6]	×
Ad Hoc 会議	○	○	○	○	○
Meet-Me 会議	×	×	○	○	×
コール ピックアップ	×	×	○	○	×
グループ ピックアップ	×	×	○	○	×
リダイヤル	○[7]	○[7]	○	○	○[7]
短縮ダイヤル	○[8]	○[8]	○	○	○[8]
オンフック ダイヤル	○	○	○	○	○
ボイスメールへのアクセス	○	○	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	○	○
Stutter Dial Tone または Audible Message Waiting Indication（AMWI）	○	×	○	○	×
ビデオ コール	×	×	×	×	×
Survivable Remote Site Telephony（SRST）サポート	○	○	○	○	○
ユニキャスト MoH	○	○	○	○	○
マルチキャスト MoH	×	×	○	○	×
保留音	×	×	×	×	×

表 20-8　SIP を使用する Cisco Basic IP Phone （続き）

機能	3911	7905G	7906G	7911G	7912G/G-A
スピーカー	○[6]	○[6]	○[6]	○[6]	○[6]
ヘッドセット ジャック	×	×	×	×	×
消音	○	×	×	×	×
Multilevel Precedence and Preemption（MLPP）	×	×	×	×	×
割り込み	×	×	○	○	×
C 割り込み	×	×	○	○	×
ワンボタン割り込み	×	×	×	×	×
回線をまたいで参加	×	×	×	×	×
プログラム可能な回線キー	×	×	×	×	×
「Single Call per Line」ユーザ エクスペリエンス	×	×	×	×	×
ビジー ランプ フィールド	×	×	×	×	×
+ ダイヤリングを使用する発番号の標準化	×	×	×	×	×
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	○	○
シグナリングおよびメディア暗号化	×	×	○	○	×
シグナリングの完全性	×	×	○	○	×
製造元でインストールされる証明書（X.509v3）	×	×	○	○	×
現場でインストールされる証明書	×	×	○	○	×
サードパーティの XML サービス	×	×	○	○	×
外部マイクおよびスピーカー	×	×	×	×	×
ダイヤル プラン	○	○	○	○	○
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	○	○	○	○	○
G.722	×	×	○	○	×
G.723	×	×	×	×	×
G.726	×	×	×	×	×
G.729	○[9]	○[9]	○[9]	○[9]	○[9]
iLBC	×	×	○	○	×
ワイドバンド オーディオ	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×
音声アクティビティ検出（VAD）	○	○	○	○	○
コンフォート ノイズ生成（CNG）	×	○	○	○	○
DTMF：H.245	×	×	×	×	×

表 20-8　SIP を使用する Cisco Basic IP Phone （続き）

機能	3911	7905G	7906G	7911G	7912G/G-A
DTMF：SCCP	×	×	×	×	×
DTMF：RFC2833	○	○	○	○	○
DTMF：KPML	×	×	○	○	×
DTMF：無指定の NOTIFY	×	×	○	○	×

1. 1 つの 10/100 Base-T。
2. 1 つの 10 Base-T。
3. 2 つの 10/100 Base-T。
4. Cisco Unified IP Phone 7912G-A は、イーサネット スイッチの拡張バージョンを備えています。
5. Cisco Unified IP Phone 7905G、7912G で SIP を使用する場合、CFWDALL が電話機に設定されているときは、Unified CM で電話機の設定が認識されないため、CFWDALL が機能するには電話機を使用中の状態にする必要があります。この動作は、休止中でも CFWDALL が機能する SCCP 電話機とは異なっています。CFWDALL が Unified CM の User ページで有効にされている場合、Unified CM はこの変更を処理できますが、コールが転送されることを示す状況表示行は電話機にありません。Unified CM の User ページでの CFWDALL 設定は、電話機の設定よりも優先されます。
6. Cisco Unified SIP Phone 3911 は半二重のスピーカー フォンを備えているのに対し、Cisco Unified IP Phone 7905G、7906G、7911G、および 7912G/GA は片通話モードをサポートしています。
7. リダイヤル。
8. 短縮ダイヤルは、これらのモデルの電話機だけに設定可能です。
9. これらの IP 電話機のモデルは、G.729b または G.729ab をサポートしていません。

表 20-9　SCCP を使用する Cisco ビジネス IP Phone

機能	6921	6961	7931G	7940G	7941G/G-GE	7942G	7945G
イーサネット接続	○[1]	○[1]	○[1]	○[1]	○[2]	○[2]	○[2]
イーサネット スイッチ（PC ポート）	○	○	○	○	○	○	○
Cisco Power-Over-Ethernet（PoE）	×	×	×	○	○[3]	○	×
IEEE 802.3af Power-Over-Ethernet（PoE）	○	○	○	×	○[3]	○	○
ローカリゼーション	○	○	○	○	○	○	○
ディレクトリ番号	2	12	24	2	2	2	2
回線あたりの最大コール数	1	1	1	200	200	200	200
液晶ディスプレイ	○	○	○	○	○	○	○
発信者 ID	○	○	○	○	○	○	○
コール ウェイティング	○[4]	○[4]	○	○	○	○	○
コール ウェイティング時の発信者 ID	○	○	○	○	○	○	○
保留	○	○	○	○	○	○	○
ブラインド転送	×	×	×	×	×	×	×
初期在席転送	○	○	○	○	○	○	○
打診転送	○	○	○	○	○	○	○
自動転送	○	○	○	○	○	○	○
自動応答	○	○	○	○	○	○	○
Ad Hoc 会議	○	○	○	○	○	○	○
Meet-Me 会議	○	○	○	○	○	○	○

表 20-9　SCCP を使用する Cisco ビジネス IP Phone （続き）

機能	6921	6961	7931G	7940G	7941G/G-GE	7942G	7945G
コール ピックアップ	○	○	○	○	○	○	○
グループ ピックアップ	○	○	○	○	○	○	○
リダイヤル	○	○	○[5]	○[5]	○[5]	○[5]	○[5]
短縮ダイヤル	○	○	○	○	○	○	○
オンフック ダイヤル	○	○	○	○	○	○	○
ボイスメールへのアクセス	○	○	○	○	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	○	○	○	○
Stutter Dial Tone または Audible Message Waiting Indication（AMWI）	○	○	○	×	○	○	○
ビデオ コール	×	×	×	○	○	○	○
Survivable Remote Site Telephony（SRST）サポート	×	×	○	○	○	○	○
ユニキャスト MoH	○	○	○	○	○	○	○
マルチキャスト MoH	○	○	○	○	○	○	○
保留音	○	○	○	○	○	○	○
スピーカー	○	○	○	○	○	○	○
ヘッドセット ジャック	○	○	○	○	○	○	○
消音	○	○	○	○	○	○	○
Multilevel Precedence and Preemption（MLPP）	×	×	○	○	○	○	○
割り込み	×	×	○	○	○	○	○
C 割り込み	×	×	○	○	○	○	○
ワンボタン割り込み	×	×	○	×	○	○	○
回線をまたいで参加	○	○	○	○	○	○	○
プログラム可能な回線キー	×	×	○	×	○	○	○
「Single Call per Line」ユーザ エクスペリエンス	○	○	○	×	×	×	×
ビジー ランプ フィールド	×	×	○	○	○	○	○
+ ダイヤリングを使用する発番号の標準化	○	○	○	○	○	○	○
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	○	○	○	○
シグナリングおよびメディア暗号化	×	×	○	○	○	○	○
シグナリングの完全性	○	○	○	○	○	○	○
製造元でインストールされる証明書（X.509v3）	○	○	○	×	○	○	○
現場でインストールされる証明書	×	×	○	○	○	○	○
サードパーティの XML サービス	○	○	○	○	○	○	○
外部マイクおよびスピーカー	×	×	○	○	○	○	○
ダイヤル プラン	×	×	×	×	×	×	×

表 20-9　SCCP を使用する Cisco ビジネス IP Phone （続き）

機能	6921	6961	7931G	7940G	7941G/G-GE	7942G	7945G
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	○	○	○	○	○	○	○
G.722	×	×	○	×	○	○	○
G.723	×	×	×	×	×	×	×
G.726	×	×	×	×	×	×	×
G.729	○	○	○	○	○	○	○
iLBC	×	×	○	×	×	○	○
ワイドバンド オーディオ	×	×	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×	×	×
音声アクティビティ検出（VAD）	○	○	○	○	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○	○	○	○	○
DTMF：H.245	×	×	×	×	×	×	×
DTMF：SCCP	○	○	○	○	○	○	○
DTMF：RFC2833	○	○	○	○	○	○	○
DTMF：KPML	×	×	×	×	×	×	×
DTMF：無指定の NOTIFY	×	×	×	×	×	×	×

1. 2 つの 10/100 Base-T イーサネット接続。
2. Cisco Unified IP Phones 7941G および 7942G は、2 つの 10/100 Mbps イーサネット接続を備えており、Cisco Unified IP Phones 7941G-GE および 7945G は、2 つの 10/100/1000 Mbps イーサネット接続を備えています。
3. Cisco Unified IP Phone 7941G は Cisco Prestandard Power over Ethernet（PoE）および IEEE 802.3af PoE をサポートしており、Cisco Unified IP Phone 7941G-GE は IEEE 802.3af PoE だけをサポートしています。
4. Cisco Unified IP Phones 6921 および 6961 にコール ウェイティングを実装するには、両方の回線（異なるパーティション内）に同じ DN を設定し、第 1 の回線が通話中に第 2 の回線に転送されるようにします。
5. リダイヤル。

表 20-10　SIP を使用する Cisco ビジネス IP Phone

機能	7931G	7940G	7941G/G-GE	7942G	7945G
イーサネット接続	○[1]	○[1]	○[2]	○[2]	○[2]
イーサネット スイッチ（PC ポート）	○	○	○	○	○
Cisco Power-Over-Ethernet（PoE）	×	○	○[3]	○	×
IEEE 802.3af Power-Over-Ethernet（PoE）	○	×	○[3]	○	○
ローカリゼーション	○	×	○	○	○
ディレクトリ番号	24	2	2	2	2
回線あたりの最大コール数	1	2	50	50	50
液晶ディスプレイ	○	○	○	○	○
発信者 ID	○	○	○	○	○
コール ウェイティング	○	○	○	○	○
コール ウェイティング時の発信者 ID	○	○	○	○	○

表 20-10　SIP を使用する Cisco ビジネス IP Phone （続き）

機能	7931G	7940G	7941G/G-GE	7942G	7945G
保留	○	○	○	○	○
ブラインド転送	×	○	○	○	○
初期在席転送	○	○	○	○	○
打診転送	○	○	○	○	○
自動転送	○	○[4]	○	○	○
自動応答	○	○[5]	○[6]	○	○
Ad Hoc 会議	○	○[7]	○	○	○
Meet-Me 会議	○	×	○	○	○
コール ピックアップ	○	×	○	○	○
グループ ピックアップ	○	×	○	○	○
リダイヤル	○[8]	○[8]	○[8]	○[8]	○[8]
短縮ダイヤル	○[9]	○[9]	○	○	○
オンフック ダイヤル	○	×	○	○	○
ボイスメールへのアクセス	○	○	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	○	○
Stutter Dial Tone または Audible Message Waiting Indication（AMWI）	○	×	○	○	○
ビデオ コール	×	×	×	×	×
Survivable Remote Site Telephony（SRST）サポート	○	○	○	○	○
ユニキャスト MoH	○	○	○	○	○
マルチキャスト MoH	○	○	○	○	○
保留音	○	×	×	×	×
スピーカー	○	○	○	○	○
ヘッドセット ジャック	○	○	○	○	○
消音	○	○	○	○	○
Multilevel Precedence and Preemption（MLPP）	×	×	×	×	×
割り込み	○	×	○	○	○
C 割り込み	○	×	○	○	○
ワンボタン割り込み	○	×	○	○	○
回線をまたいで参加	○	×	○	○	○
プログラム可能な回線キー	○	×	○	○	○
「Single Call per Line」ユーザ エクスペリエンス	○	×	×	×	×
ビジー ランプ フィールド	○	×	○	○	○
+ ダイヤリングを使用する発番号の標準化	○	×	○	○	○

表 20-10　SIP を使用する Cisco ビジネス IP Phone （続き）

機能	7931G	7940G	7941G/G-GE	7942G	7945G
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	○	○
シグナリングおよびメディア暗号化	○	×	○	○	○
シグナリングの完全性	○	×	○	○	○
製造元でインストールされる証明書（X.509v3）	○	×	○	○	○
現場でインストールされる証明書	○	×	○	○	○
サードパーティの XML サービス	○	○[10]	○	○	○
外部マイクおよびスピーカー	○	○	○	○	○
ダイヤル プラン	○	○	○	○	○
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	○	○	○	○	○
G.722	○	×	○	○	○
G.723	×	×	×	×	×
G.726	×	×	×	×	×
G.729	○[11]	○[11]	○[11]	○[11]	○[11]
iLBC	○	×	×	○	○
ワイドバンド オーディオ	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×
音声アクティビティ検出（VAD）	○	○	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○	○	○
DTMF：H.245	×	×	×	×	×
DTMF：SCCP	×	×	×	×	×
DTMF：RFC2833	○	○	○	○	○
DTMF：KPML	○	×	○	○	○
DTMF：無指定の NOTIFY	×	×	×	×	×

1. 2 つの 10/100 Base-T イーサネット接続。
2. Cisco Unified IP Phones 7941G および 7942G は、2 つの 10/100 Mbps イーサネット接続を備えており、Cisco Unified IP Phones 7941G-GE および 7945G は、2 つの 10/100/1000 Mbps イーサネット接続を備えています。
3. Cisco Unified IP Phone 7941G は Cisco Prestandard Power over Ethernet（PoE）および IEEE 802.3af PoE をサポートしており、Cisco Unified IP Phone 7941G-GE は IEEE 802.3af PoE だけをサポートしています。
4. Cisco Unified IP Phone 7905、7912、7940、または 7960 で SIP を使用する場合、CFWDALL が電話機に設定されているときは、Unified CM で電話機の設定が認識されないため、CFWDALL が機能するには電話機を使用中の状態にする必要があります。この動作は、休止中でも CFWDALL が機能する SCCP 電話機とは異なっています。CFWDALL が Unified CM の User ページで有効にされている場合、Unified CM はこの変更を処理できますが、コールが転送されることを示す状況表示行は電話機にありません。Unified CM の User ページでの CFWDALL 設定は、電話機の設定よりも優先されます。
5. この機能は、電話機でローカルに設定できます。
6. 一方向のオーディオ モニタ モード。
7. IP を使用する Unified IP Phone 7940 でサポートされているのは、Ad Hoc 会議用のローカル ミキシングと最大 3 者による会議だけです。

8. リダイヤル。
9. 短縮ダイヤルは、電話機だけで設定可能です。
10. 限定的なサポート。
11. これらの IP 電話機のモデルは、G.729b または G.729ab をサポートしていません。

表 20-11　Cisco マネージャ、およびエグゼクティブ IP Phone（SCCP 使用）

機能	6941	7960G	7961G/G-GE	7962G	7965G	7970G	7971G-GE	7975G
イーサネット接続	○[1]	○[1]	○[2]	○[2]	○[2]	○[1]	○[3]	○[3]
イーサネット スイッチ（PC ポート）	○	○	○	○	○	○	○	○
Cisco Power-Over-Ethernet（PoE）	×	○	○[4]	○	×	○	×	×
IEEE 802.3af Power-Over-Ethernet（PoE）	○	×	○[4]	○	○	○	○	○
ローカリゼーション	○	○	○	○	○	○	○	○
ディレクトリ番号	4	6	6	2	6	8	8	8
回線あたりの最大コール数	1	200	200	200	200	200	200	200
液晶ディスプレイ	○	○	○	○	○	○	○	○
発信者 ID	○	○	○	○	○	○	○	○
コール ウェイティング	○[5]	○	○	○	○	○	○	○
コール ウェイティング時の発信者 ID	○	○	○	○	○	○	○	○
保留	○	○	○	○	○	○	○	○
ブラインド転送	×	×	×	×	×	×	×	×
初期在席転送	○	○	○	○	○	○	○	○
打診転送	○	○	○	○	○	○	○	○
自動転送	○	○	○	○	○	○	○	○
自動応答	○	○	○	○	○	○	○	○
Ad Hoc 会議	○	○	○	○	○	○	○	○
Meet-Me 会議	○	○	○	○	○	○	○	○
コール ピックアップ	○	○	○	○	○	○	○	○
グループ ピックアップ	○	○	○	○	○	○	○	○
リダイヤル	○	○[6]	○[6]	○[6]	○[6]	○[6]	○[6]	○[6]
短縮ダイヤル	○	○	○	○	○	○	○	○
オンフック ダイヤル	○	○	○	○	○	○	○	○
ボイスメールへのアクセス	○	○	○	○	○	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	○	○	○	○	○
Stutter Dial Tone または Audible Message Waiting Indication（AMWI）	○	×	○	○	○	○	○	○
ビデオ コール	×	○	○	○	○	○	○	○
Survivable Remote Site Telephony（SRST）サポート	×	○	○	○	○	○	○	○
ユニキャスト MoH	○	○	○	○	○	○	○	○
マルチキャスト MoH	○	○	○	○	○	○	○	○

表 20-11　Cisco マネージャ、およびエグゼクティブ IP Phone（SCCP 使用）（続き）

機能	6941	7960G	7961G/G-GE	7962G	7965G	7970G	7971G-GE	7975G
保留音	○	○	○	○	○	○	○	○
スピーカー	○	○	○	○	○	○	○	○
ヘッドセット ジャック	○	○	○	○	○	○	○	○
消音	○	○	○	○	○	○	○	○
Multilevel Precedence and Preemption（MLPP）	×	○	○	○	○	○	○	○
割り込み	○	○	○	○	○	○	○	○
C 割り込み	×	○	○	○	○	○	○	○
ワンボタン割り込み	×	×	○	○	○	○	○	○
回線をまたいで参加	○	○	○	○	○	○	○	○
プログラム可能な回線キー	○	×	○	○	○	○	○	○
「Single Call per Line」ユーザ エクスペリエンス	○	×	×	×	×	×	×	×
ビジー ランプ フィールド	○[7]	○	○	○	○	○	○	○
+ ダイヤリングを使用する発番号の標準化	○	×	○	○	○	○	○	○
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	○	○	○	○	○
シグナリングおよびメディア暗号化	×	○	○	○	○	○	○	○
シグナリングの完全性	○	○	○	○	○	○	○	○
製造元でインストールされる証明書（X.509v3）	○	×	○	○	○	○	○	○
現場でインストールされる証明書	×	○	○	○	○	○	○	○
サードパーティの XML サービス	○	○	○	○	○	○	○	○
外部マイクおよびスピーカー	×	○	○	○	○	○	○	×
ダイヤル プラン	×	×	×	×	×	×	×	×
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	○	○	○	○	○	○	○	○
G.722	×	×	○	○	○	○	○	○
G.723	×	×	×	×	×	×	×	×
G.726	×	×	×	×	×	×	×	×
G.729	○	○	○	○	○	○	○	○
iLBC	○	×	×	○	○	×	×	○
ワイドバンド オーディオ	×	×	×	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×	×	×	×
音声アクティビティ検出（VAD）	○	○	○	○	○	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○	○	○	○	○	○

表 20-11　Cisco マネージャ、およびエグゼクティブ IP Phone（SCCP 使用）（続き）

機能	6941	7960G	7961G/G-GE	7962G	7965G	7970G	7971G-GE	7975G
DTMF：H.245	×	×	×	×	×	×	×	×
DTMF：SCCP	○	○	○	○	○	○	○	○
DTMF：RFC2833	○	○	○	○	○	○	○	○
DTMF：KPML	×	×	×	×	×	×	×	×
DTMF：無指定の NOTIFY	×	×	×	×	×	×	×	×

1. 2 つの 10/100 Base-T イーサネット接続。
2. Cisco Unified IP Phones 7961G および 7962G は 2 つの 10/100 Mbps イーサネット接続を備えており、Cisco Unified IP Phones 7961G-GE および 7965G は 2 つの 10/100/1000 Mbps イーサネット接続を備えています。
3. 2 つの 10/100/100 Mbps イーサネット接続。
4. Cisco Unified IP Phone 7961G は Cisco Prestandard PoE と IEEE 802.3af PoE の両方をサポートしており、Cisco Unified IP Phone 7961G-GE は IEEE 802.3af POE だけをサポートしています。
5. Cisco Unified IP Phone 6941 にコール ウェイティングを実装するには、その 2 つの回線に同じ DN（異なるパーティション）を設定し、第 1 の回線が通話中に第 2 の回線に転送されるようにします。
6. リダイヤル。
7. 短縮ダイヤルに限る。コール履歴エントリは対象外。

表 20-12　Cisco マネージャ、およびエグゼクティブ IP Phone（SIP 使用）

機能	7960G	7961G/G-GE	7962G	7965G	7970G	7971G-GE	7975G	8961	9951	9971
イーサネット接続	○[1]	○[2]	○[2]	○[2]	○[1]	○[3]	○[3]	○[3]	○[3]	○[3]
イーサネット スイッチ（PC ポート）	○	○	○	○	○	○	○	○	○	○
Cisco Power-Over-Ethernet（PoE）	○	○[4]	○	×	○	×	×	×	×	×
IEEE 802.3af Power-Over-Ethernet（PoE）	×	○[4]	○	○	○	○	○	○	○	○
IEEE 802.3at Power-Over-Ethernet（PoE）	×	×	×	×	×	×	×	×	○	○
USB ポート	×	×	×	×	×	×	×	○	○	○
Bluetooth ヘッドセット	×	×	×	×	×	×	×	×	○	○
IEEE 802.11a/b/g	×	×	×	×	×	×	×	×	×	○
ローカリゼーション	×	○	○	○	○	○	○	○	○	○
ディレクトリ番号	6	6	6	6	8	8	8	5	5	6
回線あたりの最大コール数	2	50	50	50	50	50	50	50	50	50
液晶ディスプレイ	○	○	○	○	○	○	○	○	○	○
発信者 ID	○	○	○	○	○	○	○	○	○	○
コール ウェイティング	○	○	○	○	○	○	○	○	○	○
コール ウェイティング時の発信者 ID	○	○	○	○	○	○	○	○	○	○
保留	○	○	○	○	○	○	○	○	○	○
ブラインド転送	○	×	×	×	×	×	×	×	×	×

表 20-12　Cisco マネージャ、およびエグゼクティブ IP Phone（SIP 使用）（続き）

機能	7960G	7961G/G-GE	7962G	7965G	7970G	7971G-GE	7975G	8961	9951	9971
初期在席転送	○	○	○	○	○	○	○	○	○	○
打診転送	○	○	○	○	○	○	○	○	○	○
自動転送	○[5]	○	○	○	○	○	○	○	○	○
自動応答	○[6]	○	○	○	○	○	○	○	○	○
Ad Hoc 会議	○[7]	○	○	○	○	○	○	○	○	○
Meet-Me 会議	×	○	○	○	○	○	○	○	○	○
コール ピックアップ	×	○	○	○	○	○	○	○	○	○
グループ ピックアップ	×	○	○	○	○	○	○	○	○	○
リダイヤル	○[8]	○[8]	○[8]	○[8]	○[8]	○[8]	○[8]	○[8]	○[8]	○[8]
短縮ダイヤル	○	○	○	○	○	○	○	○	○	○
オンフック ダイヤル	×	○	○	○	○	○	○	○	○	○
ボイスメールへのアクセス	○	○	○	○	○	○	○	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	○	○	○	○	○	○	○
Stutter Dial Tone または Audible Message Waiting Indication（AMWI）	×	○	○	○	○	○	○	○	○	○
ビデオ コール	×	×	×	×	×	×	×	×	×	×
Survivable Remote Site Telephony（SRST）サポート	○	○	○	○	○	○	○	○	○	○
ユニキャスト MoH	○	○	○	○	○	○	○	○	○	○
マルチキャスト MoH	○	○	○	○	○	○	○	○	○	○
保留音	×	×	×	×	×	×	×	×	×	×
スピーカー	○	○	○	○	○	○	○	○	○	○
ヘッドセット ジャック	○	○	○	○	○	○	○	○	○	○
消音	○	○	○	○	○	○	○	○	○	○
Multilevel Precedence and Preemption（MLPP）	×	×	×	×	×	×	×	×	×	×
割り込み	×	○	○	○	○	○	○	×	×	×
C 割り込み	×	○	○	○	○	○	○	○	○	○
ワンボタン割り込み	×	○	○	○	○	○	○	○	○	○
回線をまたいで参加	×	○	○	○	○	○	○	○	○	○
プログラム可能な回線キー	×	○	○	○	○	○	○	○	○	○
「Single Call per Line」ユーザ エクスペリエンス	×	×	×	×	×	×	×	×	×	×
ビジー ランプ フィールド	×	○	○	○	○	○	○	○	○	○
+ ダイヤリングを使用する発番号の標準化	×	○	○	○	○	○	○	○	○	○

表 20-12　Cisco マネージャ、およびエグゼクティブ IP Phone（SIP 使用）（続き）

機能	7960G	7961G/G-GE	7962G	7965G	7970G	7971G-GE	7975G	8961	9951	9971
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	○	○	○	○	○	○	○
シグナリングおよびメディア暗号化	×	○	○	○	○	○	○	○	○	○
シグナリングの完全性	×	○	○	○	○	○	○	○	○	○
製造元でインストールされる証明書（X.509v3）	×	○	○	○	○	○	○	○	○	○
現場でインストールされる証明書	×	○	○	○	○	○	○	○	○	○
サードパーティの XML サービス	○[9]	○	○	○	○	○	○	○	○	○
Java MIDlet アプリケーション	×	○	○	○	○	○	○	○	○	○
外部マイクおよびスピーカー	○	○	○	○	○	○	○	○	○	○
ダイヤル プラン	○	○	○	○	○	○	○	○	○	○
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	○	○	○	○	○	○	○	○	○	○
G.722	×	○	○	○	○	○	○	○	○	○
G.723	×	×	×	×	×	×	×	×	×	×
G.726	×	×	×	×	×	×	×	×	×	×
G.729	○[10]	○[10]	○[10]	○[10]	○[10]	○[10]	○[10]	○	○	○
iLBC	×	×	○	○	×	×	○	○	○	○
iSAC	×	×	×	×	×	×	×	○	○	○
ワイドバンド オーディオ	×	×	×	×	×	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×	×	×	×	×	×
ワイドバンド アコースティック	×	×	○	○	×	×	○	○	○	○
音声アクティビティ検出（VAD）	○	○	○	○	○	○	○	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○	○	○	○	○	○	○	○
DTMF：H.245	×	×	×	×	×	×	×	×	×	×
DTMF：SCCP	×	×	×	×	×	×	×	×	×	×
DTMF：RFC2833	○	○	○	○	○	○	○	○	○	○

表 20-12　Cisco マネージャ、およびエグゼクティブ IP Phone（SIP 使用）（続き）

機能	7960G	7961G/G-GE	7962G	7965G	7970G	7971G-GE	7975G	8961	9951	9971
DTMF：KPML	×	○	○	○	○	○	○	○	○	○
DTMF：無指定の NOTIFY	×	×	×	×	×	×	×	×	×	×

1. 2 つの 10/100 Base-T イーサネット接続。
2. Cisco Unified IP Phones 7961G および 7962G は 2 つの 10/100 Mbps イーサネット接続を備えており、Cisco Unified IP Phones 7961G-GE および 7965G は 2 つの 10/100/1000 Mbps イーサネット接続を備えています。
3. 2 つの 10/100/100 Mbps イーサネット接続。
4. Cisco Unified IP Phone 7961G は Cisco Prestandard PoE と IEEE 802.3af PoE の両方をサポートしており、Cisco Unified IP Phone 7961G-GE は IEEE 802.3af PoE だけをサポートしています。
5. Cisco Unified IP Phone 7905、7912、7940、または 7960 で SIP を使用する場合、CFWDALL が電話機に設定されているときは、Unified CM で電話機の設定が認識されないため、CFWDALL が機能するには電話機を使用中の状態にする必要があります。この動作は、休止中でも CFWDALL が機能する SCCP 電話機とは異なっています。CFWDALL が Unified CM の User ページで有効にされている場合、Unified CM はこの変更を処理できますが、コールが転送されることを示す状況表示行は電話機にありません。Unified CM の User ページでの CFWDALL 設定は、電話機の設定よりも優先されます。
6. この機能は、電話機でローカルに設定できます。
7. IP を使用する Cisco Unified IP Phone 7960G でサポートされているのは、Ad Hoc 会議用のローカル ミキシングと最大 3 者による会議だけです。
8. リダイヤル。
9. 限定的なサポート。
10. これらの IP 電話機のモデルは、G.729b または G.729ab をサポートしていません。

表 20-13　専用エンドポイント

機能	7921G	7925G	7936	7937G	7985G
イーサネット接続	×	×	○[1]	○[1]	○[2]
イーサネット スイッチ（PC ポート）	×	×	×	×	○
Cisco Power-Over-Ethernet（PoE）	×	×	×	×	×
IEEE 802.3af Power-Over-Ethernet（PoE）	×	×	×	○	○
ローカリゼーション	○	○	×	○	○
ディレクトリ番号	6	6	1	1	2
回線あたりの最大コール数	2	2	2	6	100
液晶ディスプレイ	○	○	○	○	○
発信者 ID	○	○	○	○	○
コール ウェイティング	○	○	○	○	○
コール ウェイティング時の発信者 ID	○	○	○	○	○
保留	○	○	○	○	○
ブラインド転送	×	×	×	×	×
初期在席転送	○	○	○	○	○
打診転送	○	○	○	○	○
自動転送	○	○	○	○	○
自動応答	○	○	×	○	○
Ad Hoc 会議	○	○	○	○	○

表 20-13　専用エンドポイント （続き）

機能	7921G	7925G	7936	7937G	7985G
Meet-Me 会議	○	○	○	○	○
コール ピックアップ	○	○	○	○	○
グループ ピックアップ	○	○	○	○	○
リダイヤル	○[3]	○[3]	○	○	○
短縮ダイヤル	○	○	×	○	○
オンフック ダイヤル	○	○	○	○	○
ボイスメールへのアクセス	○	○	×	○	○
メッセージ待機インジケータ（MWI）	○	○	×	×	○
Stutter Dial Tone または Audible Message Waiting Indication（AMWI）	×	×	×	×	×
ビデオ コール	×	×	×	×	○
Survivable Remote Site Telephony（SRST）サポート	○	○	○	○	○[4]
ユニキャスト MoH	○	○	○	○	○
マルチキャスト MoH	○	○	○	○	×
保留音	○	○	○	○	○
スピーカー	○	○	○	○	○
ヘッドセット ジャック	○	○	×	×	○
消音	○	○	○	○	○
Multilevel Precedence and Preemption（MLPP）	○	○	×	○	○
割り込み	○	○	×	○	○
C 割り込み	○	○	×	○	○
ワンボタン割り込み	×	×	×	×	×
回線をまたいで参加（Join Across Lines）	×	×	×	×	×
プログラム可能な回線キー	×	×	×	×	×
「Single Call per Line」ユーザ エクスペリエンス	×	×	×	×	×
ビジー ランプ フィールド	×	×	×	×	×
+ ダイヤリングを使用する発番号の標準化	×	×	×	×	×
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	×	○	×
シグナリングおよびメディア暗号化	○	○	×	×	×
シグナリングの完全性	○	○	×	×	×
製造元でインストールされる証明書（X.509v3）	○	○	×	×	×
現場でインストールされる証明書	○	○	×	×	×
サードパーティの XML サービス	○	○	×	○	×
外部マイクおよびスピーカー	○	○[5]	×	○[6]	×

表 20-13　専用エンドポイント （続き）

機能	7921G	7925G	7936	7937G	7985G
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0x88
G.711	○	○	○	○	○
G.722	○	○	×	○	○
G.723	×	×	×	×	×
G.726	×	×	×	×	×
G.729	○	○	○	○	○
iLBC	○	○	×	×	×
ワイドバンド オーディオ	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×
H.261	×	×	×	×	○
H.263	×	×	×	×	○
H.263+	×	×	×	×	○
H.264	×	×	×	×	○
音声アクティビティ検出（VAD）	○	○	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○	○	○
DTMF：H.245	×	×	×	×	×
DTMF：SCCP	○	○	○	○	○
DTMF：RFC2833	×	×	×	○	×

1. 1 つの 10/100 Base-T。
2. 2 つの 10/100 Base-T。
3. リダイヤル。
4. SRST ではオーディオだけがサポートされます。
5. Bluetooth ヘッドセットがサポートされています。
6. 無線ラペルマイクがサポートされています。

表 20-14　ソフトウェア ベースのエンドポイントの機能

機能	Unified Personal Communicator	SCCP を使用する IP Communicator	SIP を使用する IP Communicator
ディレクトリ番号	1	8	8
発信者 ID	○	○	○
コール ウェイティング	○	○	○
コール ウェイティング時の発信者 ID	○	○	○
保留	○	○	○
コール転送	○[1]	○	○
自動転送	×	○	○
自動応答	○	○	○

表 20-14　ソフトウェア ベースのエンドポイントの機能 （続き）

機能	Unified Personal Communicator	SCCP を使用する IP Communicator	SIP を使用する IP Communicator
Ad Hoc 会議	○[2]	○	○
Meet-Me 会議	×[3]	○	×
Web 会議	○	×	×
コール ピックアップ	×	○	○
グループ ピックアップ	×	○	○
リダイヤル	○[4]	○[4]	○[4]
短縮ダイヤル	○[5]	○	○
オンフック ダイヤル	○	○	○
ボイスメールへのアクセス	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○
Stutter Dial Tone または Audible Message Waiting Indication（AMWI）	×	○[6]	○[6]
ビデオ コール	○	○[7]	×
Survivable Remote Site Telephony（SRST）サポート	×	○	○
ユニキャスト Music On Hold	○	○	○
マルチキャスト Music On Hold（MoH）	○	○	○
保留音	×	○	×
消音	○	○	○
Multilevel Precedence and Preemption（MLPP）	×	○	×
割り込み	×	○	○
C 割り込み	×	○	○
ワンボタン割り込み	×	○	×
回線をまたいで参加	×	○	×
プログラム可能な回線キー	×	○	×
「Single Call per Line」ユーザ エクスペリエンス	×	×	×
ビジー ランプ フィールド	×	○	○
+ ダイヤリングを使用する発番号の標準化	×	○	×
Gratuitous Address Resolution Protocol（GARP）を無効にする	×	×	×
シグナリングおよびメディア暗号化	×	○	○
シグナリングの完全性	×	×	×
製造元でインストールされる証明書（X.509v3）	×	×	×

表 20-14　ソフトウェア ベースのエンドポイントの機能 （続き）

機能	Unified Personal Communicator	SCCP を使用する IP Communicator	SIP を使用する IP Communicator
現場でインストールされる証明書	×	×	×
サードパーティの XML サービス	×	○	○
シグナリング パケット ToS 値のマーキング	×	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8
Skinny Client Control Protocol（SCCP）	×	○	×
セッション開始プロトコル（SIP）	○	×	○
G.711	○	○	○
G.722	×	○[6]	○[6]
G.723	×	×	×
G.726	×	×	×
G.729	○	○	×
iLBC	○	○[6]	○[6]
ワイドバンド オーディオ	×	○	×[8]
ワイドバンド ビデオ	×	×	×
H.261	×	×	×
H.263	○	×	×
H.264	○	×	×
音声アクティビティ検出（VAD）	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○
DTMF：H.245	×	×	×
DTMF：SCCP	×	○	×
DTMF：RFC2833	○	○	○
DTMF：KPML	○	×	○

1. Cisco Unified Personal Communicator は明示的な転送機能を備えていません。Cisco Unified Personal Communicator ユーザがコールを転送するには、2 つのコールをマージした後に接続解除して転送結果を取得します。
2. Cisco Unified Personal Communicator は、「consult, then merge」機能（IP Phone での会議に相当）をサポートしていませんが、電話会議の **merge**（IP Phone での **join** に相当）はサポートしています。
3. Cisco Unified Personal Communicator は Meet-Me 会議を作成できませんが、ユーザは正しい番号をダイヤルして会議に参加することができます。
4. リダイヤル。
5. Cisco Unified Personal Communicator は Unified CM 短縮ダイヤル ページをサポートしていませんが、同様の方法で個人連絡表などの Contacts（buddy）リストからのクリックコールをサポートしています。
6. この機能は、Cisco IP Communicator Release 2.1 ではサポートされていません。
7. Cisco IP Communicator を Cisco Unified Video Advantage と組み合わせて SCCP モードで動作させると、ビデオコールがサポートされます。
8. Cisco IP Communicator 2.1 は、ワイドバンド オーディオをサポートしていません。

CHAPTER 21

デバイス モビリティ

Cisco Unified Communications Manager（Unified CM）では、ロケーション、リージョン、コーリング サーチ スペース、メディア リソースなど、さまざまな設定を使用して、サイト、つまり物理ロケーションが識別されます。特定のサイトにある Cisco Unified IP Phone は、これらの設定により静的に設定されます。Unified CM では、適切なコールの確立、コール ルーティング、メディア リソースの選択などのためにこれらの設定を使用します。一方、Cisco IP Communicator や Cisco Unified Wireless IP Phone などのモバイル電話機がそれらのホーム サイトからリモート サイトに移動されたときに、それらのモバイル電話機では電話機に静的に設定されているホーム設定を保持しています。この結果 Unified CM では、リモート サイトの電話機にあるこれらのホーム設定を使用します。この状況は、コール ルーティング、コーデックの選択、メディア リソースの選択、およびその他のコール処理機能における問題の原因となる場合があるため望ましくありません。

Cisco Unified CM では、デバイス モビリティという機能を使用します。この機能により、Unified CM では、IP 電話がホーム ロケーションにあるのか、ローミング ロケーションにあるのかを判別できます。Unified CM では、デバイスの IP サブネットを使用して、その IP 電話の正確な場所を判別します。クラスタ内でのデバイス モビリティを使用できるようにすることで、モバイル ユーザは 1 つのサイトから別のサイトにローミングでき、このときサイト固有の設定を取得します。次に、Unified CM では、これらの動的に割り当てられた設定を使用して、コール ルーティング、コーデックの選択、メディア リソースの選択などを行います。

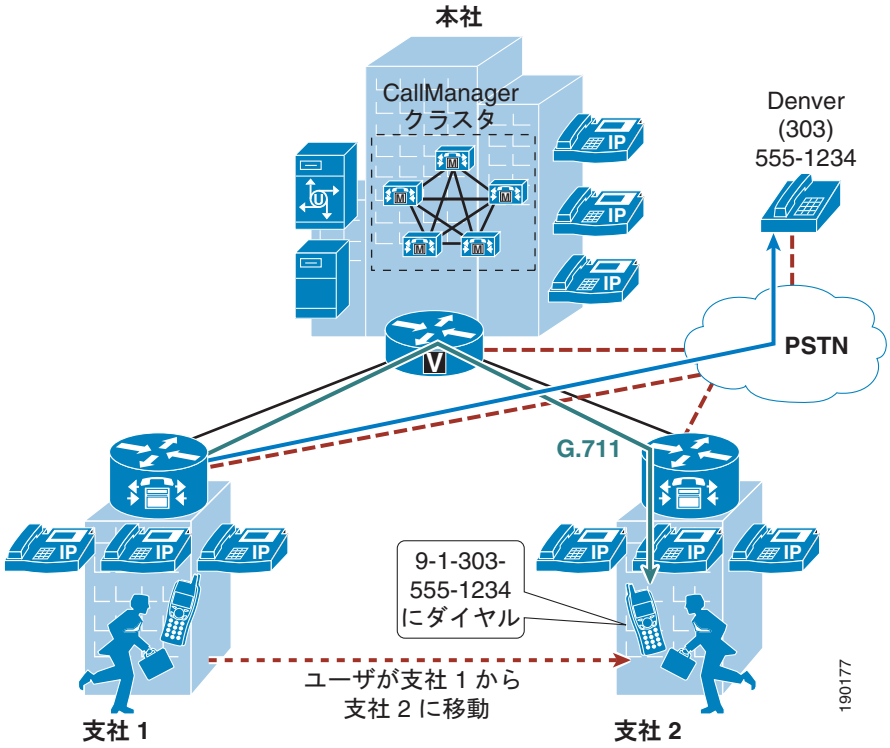
この章では、Unified CM クラスタ内にデバイス モビリティを実装する場合の設計上の考慮事項について説明します。

デバイス モビリティの必要性

この項では、Unified CM クラスタに多くのモバイル ユーザが含まれている場合のデバイス モビリティの必要性について説明します。

図 21-1 は、本社サイト（HQ）にあり、デバイス モビリティ機能を備えない Unified CM クラスタを含んでいる架空のネットワークを示しています。このクラスタには、支店 1 と支店 2 の 2 つのリモート サイトがあります。サイト内コールでは、いずれも G.711 音声コーデックが使用されます。一方サイト間コール（IP WAN を経由するコール）では、いずれも G.729 音声コーデックが使用されます。各サイトには、外部コールのための公衆網ゲートウェイがあります。

図 21-1　　リモート サイトを 2 つ持つネットワークの例



支店 1 のユーザが支店 2 に移動し、Denver にいる公衆網ユーザに通話すると、次のような動作が発生します。

- Unified CM では、そのユーザが支店 1 から支店 2 に移動したことを認識していません。公衆網への外部コールが WAN を経由して支店 1 のゲートウェイに送られ、そこから公衆網に出ます。これにより、モバイル ユーザの公衆網コールすべてに、引き続きそのユーザのホーム ゲートウェイが使用されます。
- このモバイル ユーザと支店 1 ゲートウェイは、同じ Unified CM リージョンおよびロケーションに存在しています。ロケーション ベースのコール アドミッション制御は、異なるロケーションに存在しているデバイスおよび G.711 音声コーデックを使用するリージョン内コールにだけ適用可能です。したがって、IP WAN を経由する支店 1 ゲートウェイへのコールでは G.711 コーデックが使用され、コール アドミッション制御のための Unified CM によるトラッキングは行われません。この動作の結果、リモート リンクすべてが低速リンクである場合に、IP WAN 帯域幅のオーバー サブスクリプションが発生する場合があります。

- モバイル ユーザが、複数の支店 2 ユーザを Denver にいる公衆網ユーザとの既存のコールに追加することで、会議を作成します。モバイル ユーザは支店 1 ゲートウェイの会議リソースを使用します。したがって、すべての会議ストリームが IP WAN 経由で流れます。

デバイス モビリティ機能

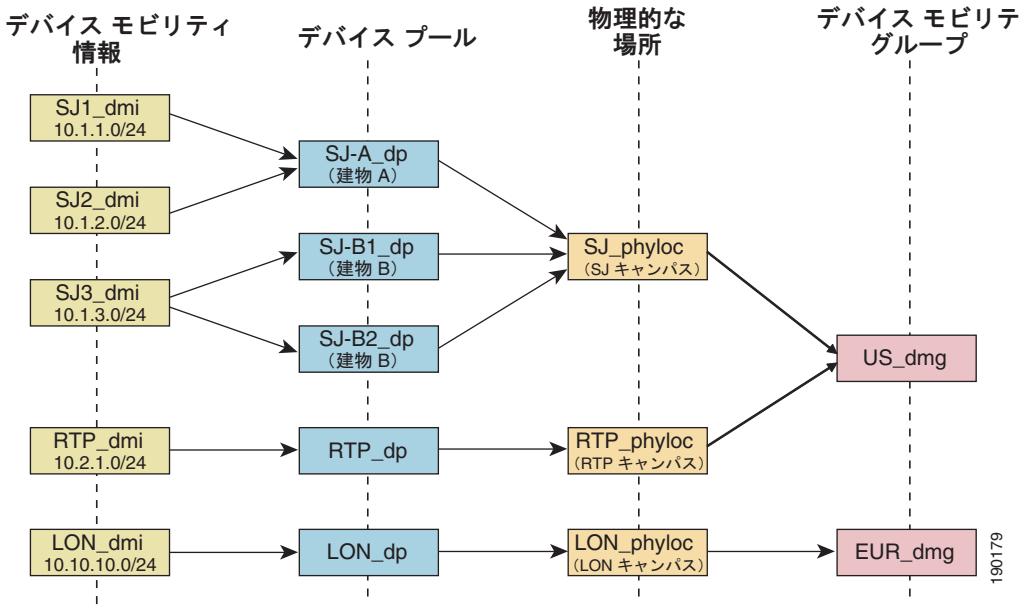
Unified CM デバイス モビリティ機能は、上記の問題を解決するために有用です。この項では、この機能の動作方法を簡単に説明します。ただし、この機能の詳細説明については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

デバイス モビリティには次のような要素が含まれます。

- デバイス モビリティ情報 : IP サブネットを設定し、デバイス プールを IP サブネットに関連付けます。
- デバイス モビリティ グループ : ダイヤリング パターンが類似しているサイトの論理グループを定義します（たとえば、図 21-2 の US_dmg および EUR_dmg）。
- 物理ロケーション : デバイス プールの物理ロケーションを定義します。言い換えると、この要素では、IP 電話およびデバイス プールに関連付けられているその他のデバイスの地理的なロケーションを定義します（たとえば、図 21-2 に示されている San Jose の IP 電話は、すべて物理ロケーション SJ_phyloc を使用して定義されています）。

図 21-2 は、この 3 つの用語すべての関係を示します。

図 21-2　デバイス モビリティ コンポーネントの関係

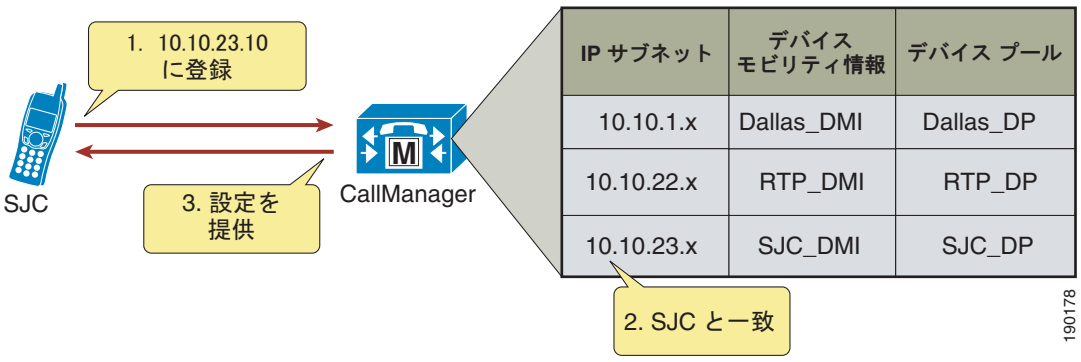


Unified CM では、デバイスの IP サブネットに基づいてデバイス プールを IP 電話に割り当てます。次の手順は、図 21-3 に図示がありますが、この動作を説明したものです。

1. IP 電話では、その電話の IP アドレスを Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）登録メッセージに含めて送信することにより、Unified CM への登録を試行します。
2. Unified CM では、デバイスの IP サブネットを抽出し、デバイス モビリティ情報に設定されているサブネットと照合します。

3. サブネットが一致すると、Unified CM では、デバイス プール設定に基づいて、デバイスに新規設定を提供します。

図 21-3　　電話登録プロセス



Unified CM では、デバイス プール設定にある新規のパラメータ一式を使用して、デバイス モビリティに対応します。これらのパラメータは、次の 2 つの主要なタイプについてのパラメータです。

- ローミングに依存する設定

  これらの設定にあるパラメータは、デバイスがデバイス モビリティ グループの内部または外部をローミングしているときに、デバイス レベルの設定より優先されます。この設定には、次のパラメータが含まれます。

  - 日付/時刻グループ
  - リージョン
  - メディア リソース グループ リスト
  - ロケーション
  - ネットワーク ロケール
  - SRST リファレンス
  - 物理ロケーション
  - デバイス モビリティ グループ

  ローミングに依存する設定は、主に、適切なコール アドミッション制御および音声コーデックの選択を実施するために有用です。これは、ロケーションおよびリージョンの設定は、デバイスのローミング デバイス プールに基づいて使用されるためです。

  さまざまなコール アドミッション制御手法については、「コール アドミッション制御」（P.9-1）の章を参照してください。

  ローミングに依存する設定により、メディア リソース グループ リスト（MRGL）も更新されて、Music on Hold、会議、トランスコーディングなどで適切なリモート メディア リソースが使用されるようになり、これによりネットワークが効率的に使用されます。

  ローミングに依存する設定により、Survivable Remote Site Telephony（SRST）ゲートウェイも更新されます。モバイル ユーザは、ローミング中に別の SRST ゲートウェイに登録します。この登録が、ローミング電話機が SRST モードであるときのダイヤリング動作に影響することがあります。ダイヤル プランの設計に関する考慮事項の詳細については、「ダイヤル プラン」（P.10-1）の章を参照してください。

- デバイス モビリティ関連の設定

  これらの設定にあるパラメータは、デバイスがデバイス モビリティ グループの内部をローミングしているときにだけ、デバイス レベルの設定より優先されます。この設定には、次のパラメータが含まれます。

  - デバイス モビリティ コーリング サーチ スペース
  - AAR コーリング サーチ スペース
  - AAR グループ

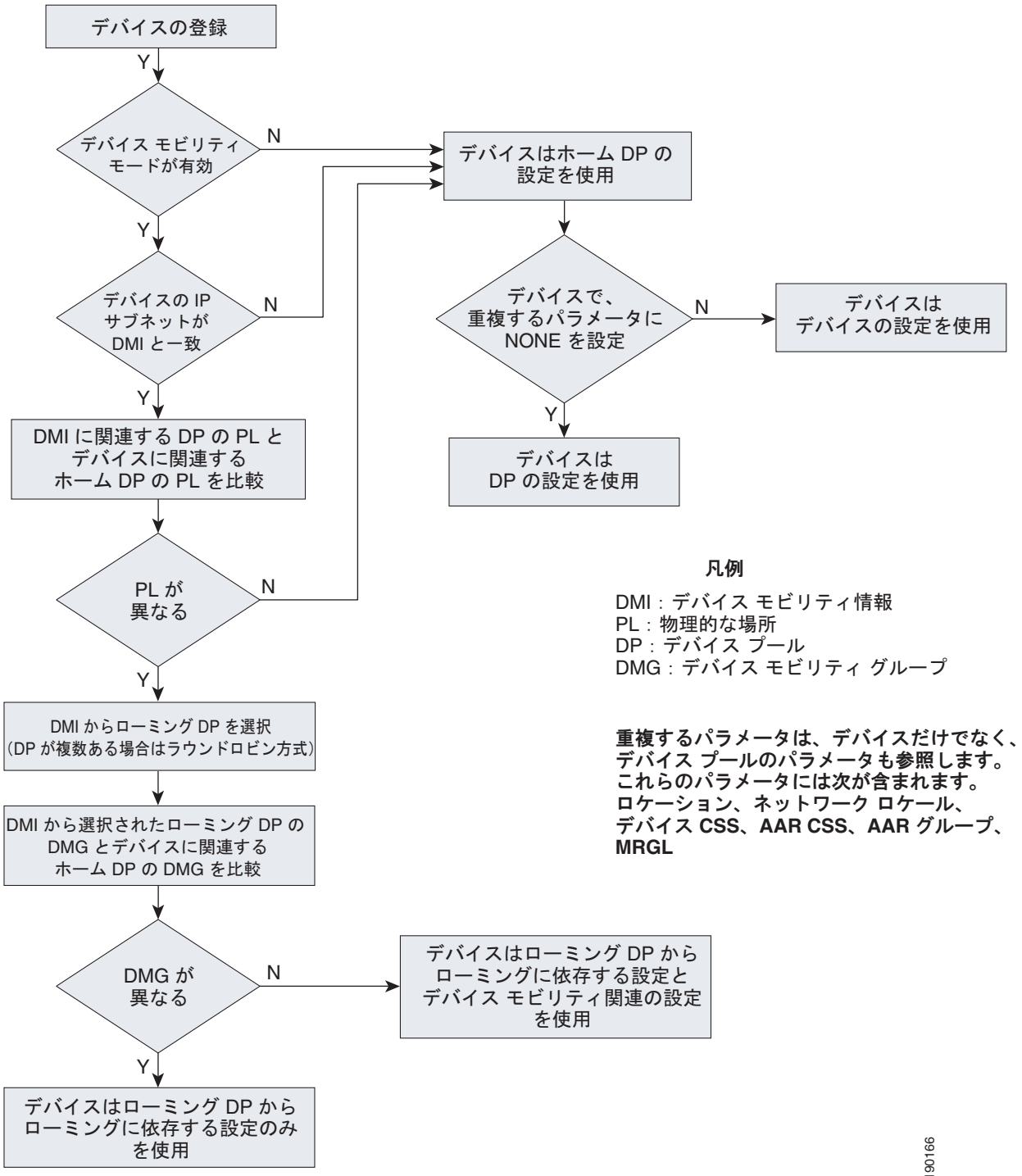
  コーリング サーチ スペースは、ダイヤルできるパターンまたは到達できるデバイスを指示するため、デバイス モビリティ関連の設定は、ダイヤル プランに影響します。

前述したように、デバイス モビリティ グループは、ダイヤリング パターンが類似したサイト（たとえば、同じ公衆網アクセス コードを持つサイトなど）の論理グループを定義します。このガイドラインを使用すると、すべてのサイトがサイト固有のコーリング サーチ スペースに類似したダイヤリング パターンを持ちます。ダイヤリング動作が異なるサイトは、異なるデバイス モビリティ グループに属します。デバイス モビリティ グループ内をローミングするユーザは、新規コーリング サーチ スペースを受け取った後であっても、ダイヤリング動作をリモート ロケーションで維持できます。デバイス モビリティ グループの外部をローミングするユーザは、自身のホーム コーリング サーチ スペースを使用するため、やはり、ダイヤリング動作をリモート ロケーションで維持できます。

一方、異なるダイヤリング パターンを持つサイト（たとえば、異なる公衆網アクセス コードを持つサイト）によってデバイス モビリティ グループを定義した場合は、このデバイス モビリティ グループ内をローミングするユーザは、一部のロケーションでは同じダイヤリング動作を維持できない場合があります。ユーザは、各ロケーションで新規コーリング サーチ スペースを受け取った後で、異なるロケーションにおいて異なる番号をダイヤルする必要がある場合があります。この動作は、ユーザを混乱させるおそれがあります。

デバイス モビリティ機能の動作を図 21-4 のフローチャートに示します。

図 21-4　デバイス モビリティ機能の動作



Cisco Unified CM 7.*x* では、デバイス モビリティ機能の動作は、パブリッシャ サーバに依存しなくなりました。パブリッシャが使用できない場合、モバイル ユーザはコール処理（サブスクライバ）サーバに登録され、ローミング デバイス プール設定を使用します。

デバイス モビリティ機能には、次のガイドラインが適用されます。

- 図 21-4 にリストされている重複するパラメータがデバイスおよびデバイス プールで同じ設定を持つ場合は、デバイスではこれらのパラメータに NONE を設定できます。次にこれらのパラメータをデバイス プールに設定する必要があります。この方法を実施すると、デバイスにすべてのパラメータを個別に設定する必要がないため、設定の量を大幅に削減できます。
- サイトごとに物理ロケーション 1 つを定義してください。1 つのサイトが複数のデバイス プールを持つことができます。
- 公衆網または外部/オフネット アクセスのダイヤリング パターンが類似したサイトを、同じデバイス モビリティ グループを使用して定義してください。公衆網または外部/オフネット アクセスのダイヤリング パターンが異なるサイトを、同じデバイス モビリティ グループを使用して定義することはできます。ただし、使用されているさまざまなダイヤリング パターンまたはアクセス コードについてユーザに適切な手引きを行う必要があります。
- 企業のポリシーに応じて、未定義のサブネットすべてに対応する、IP サブネット 0.0.0.0 の「catch-all」デバイス モビリティ情報を定義できます。このデバイス モビリティ情報は、ネットワーク リソースのアクセスまたは使用を制限できるデバイス プールを割り当てるために使用できます（たとえば、ローミング中にこのデバイス プールに関連付けられているデバイスからのコールすべてをブロックするコーリング サーチ スペース NONE を使用してデバイス プールを設定できます）。ただし、これを行う場合、管理者は、911 およびその他の緊急コールであってもブロックされるという事実を承知する必要があります。コーリング サーチ スペースは、911 またはその他の緊急コールだけにアクセスを許すパーティションを含めて設定できます。

ダイヤル プランの設計に関する考慮事項

デバイス モビリティ機能を使用する場合、電話機のダイヤリング動作は電話機のローミング（またはホーム）ロケーションに依存します。前述したように、デバイス プール内のデバイス モビリティ関連設定が、コール フローの動作に影響します。これは、コーリング サーチ スペースが、Unified CM 内の宛先パターンの到達可能性を示すためです。この項では、デバイス モビリティのための複数のダイヤル プラン アプローチについて説明します。

さまざまなダイヤル プラン アプローチの詳細については、「ダイヤル プラン」（P.10-1）の章を参照してください。

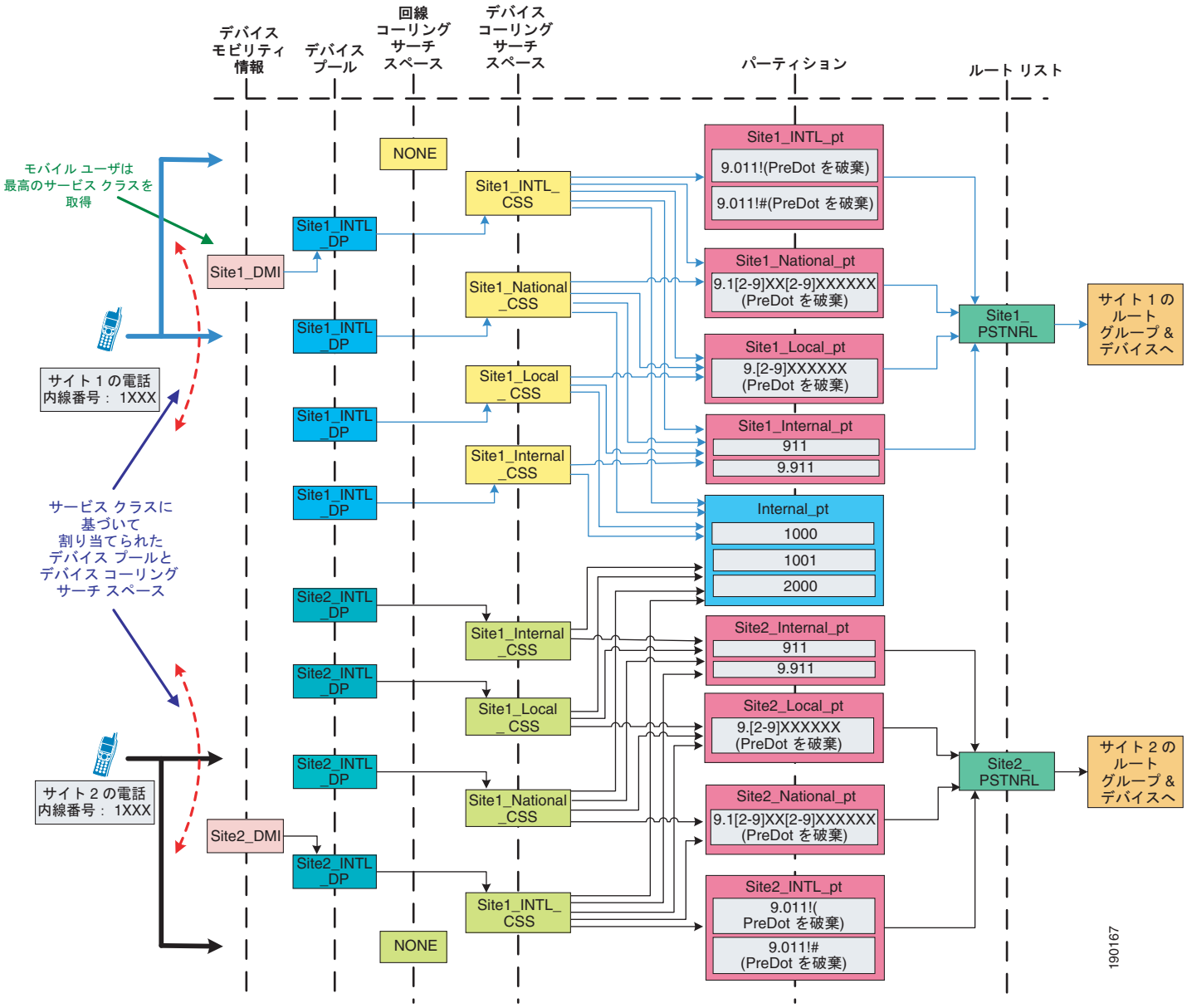
サービス クラスを構築するためのデバイス モビリティの考慮事項

ローミング中のモバイル ユーザは、一般に、ホーム ロケーションにいるときと同じコール特権を持つ必要があります。「ダイヤル プラン」（P.10-1）の章では、サービス クラスを構築するための 2 つのアプローチについて説明します（「従来のアプローチ」（P.21-7）および「回線/デバイス アプローチ」（P.21-9））。

従来のアプローチ

図 21-5 は、クラスタ内でデバイス モビリティを使用する場合に、サービス クラスを構築するための従来のアプローチの例を示します。

図 21-5　サービス クラスを構築するための従来のアプローチ



このアプローチには、次のガイドラインが適用されます。

- 電話デバイスのコーリング サーチ スペースを使用して、内部または外部の宛先に対するコール ルーティングのパスを選択します。コーリング サーチ スペースに NONE を設定しません。
- 電話デバイスのコーリング サーチ スペースを使用して、コール特権を割り当てます。
- サイトごとのデバイス プールを作成し、必要なサービス クラスに基づいてコーリング サーチ スペースをそれに割り当てます。上記の例では、国際コーリング サーチ スペース（Site1_INTL_CSS）がデバイス プールに割り当てられています。デバイス上の設定のほうがホーム ロケーションにあるデバイス プール設定より優先されるため、ユーザは、引き続き電話デバイスのコーリング サーチ スペースを使用します。

- IP 電話のデバイス モビリティとエクステンション モビリティを有効にすることができます。ただし、モバイル ユーザは、IP 電話の回線コーリング サーチ スペースがサービス クラスを定義するために使用される場合があることを承知する必要があります。「ダイヤル プラン」（P.10-1）の章で説明されている従来のアプローチを使用する場合のエクステンション モビリティの考慮事項に従ってください。モバイル ユーザのエクステンション モビリティとデバイス モビリティの両方を有効にする場合は、回線/デバイス アプローチを使用することをお勧めします。
- 同じサービス クラスまたはコール特権をクラスタ内のモバイル ユーザすべてに割り当てます。図 21-5 の例では、サイト 1 のユーザは、ホーム デバイス コーリング サーチ スペースとして Site1_National_CSS を持ち、サイト 2 のモバイル ユーザは、ホーム デバイス コーリング サーチ スペースとして Site1_INTL_CSS を持ちます。両方のユーザがサイト 2 にローミングすると、Site2_INTL_DP デバイス プールにより両方のユーザに Site2_INTL_CSS コーリング サーチ スペースが割り当てられます。これにより、サイト 1 からのモバイル ユーザに異なるサービス クラスが与えられます。複数のデバイス プールが作成され、それぞれに異なるコーリング サーチ スペースが割り当てられたとしても、ホーム ロケーションと同じサービス クラスを持つ正しいローミング デバイス プールを割り当てることはできません。これは、デバイス プールの割り当てが、ユーザの能力に基づいてではなく IP サブネットに基づいて行われるためです。
- 一部のモバイル ユーザの持つサービス クラスが異なる場合は、各サイトをデバイス モビリティ グループとして定義することを検討してください。この方式を使用すると、モバイル ユーザが、ローミングの際にコール特権を維持することが保証されます。ただし、この方式では、外部公衆網コールすべてが、ホーム ゲートウェイを使用してルーティングされます。
- お客様の都合でモバイル ユーザにさまざまなサービス クラスが必要とされ、各サイトをデバイス モビリティ グループとして定義することではこの要件を満たせない場合は、回線/デバイス アプローチを使用することを検討してください。

回線/デバイス アプローチ

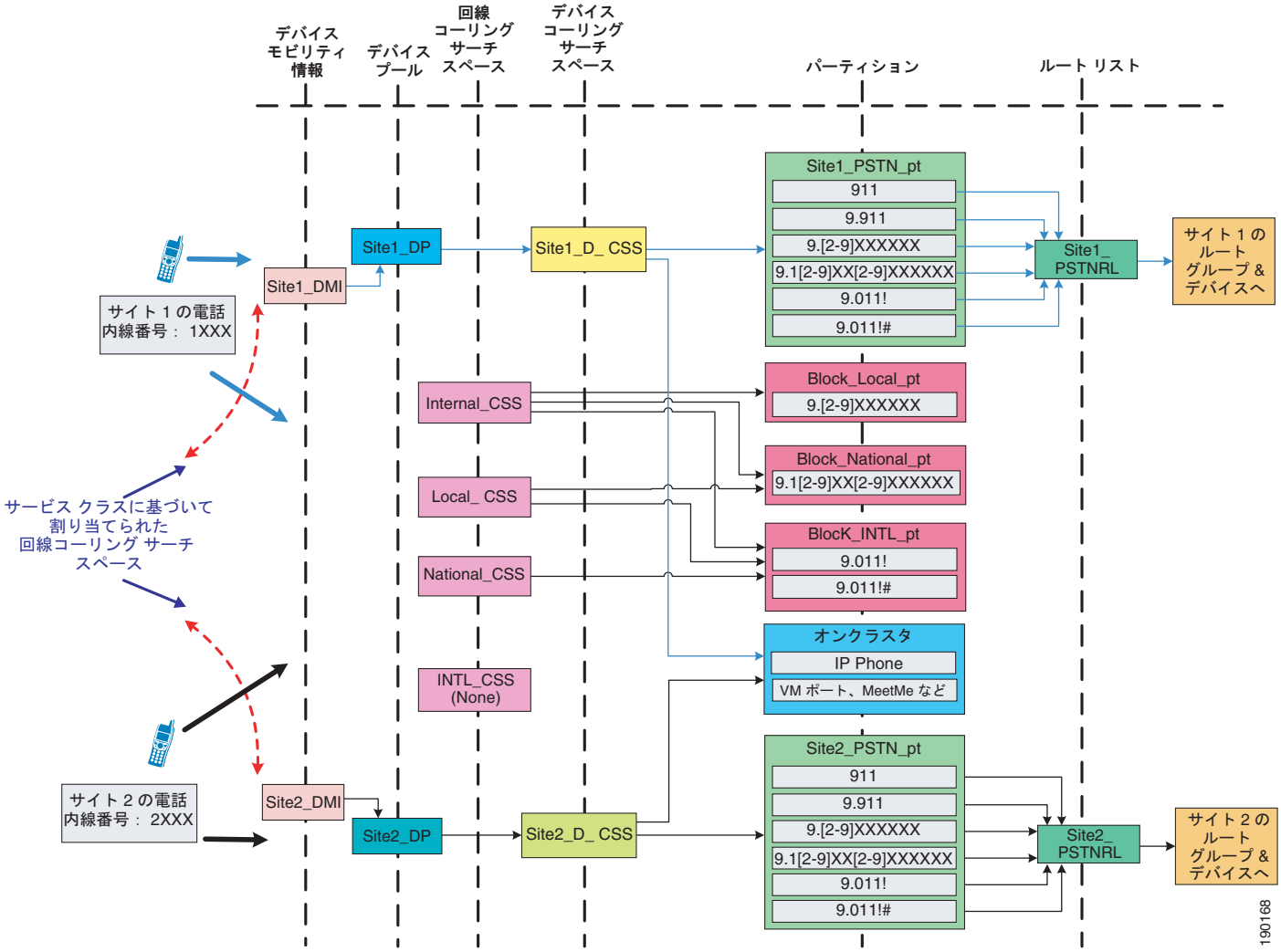
Unified CM では、所定の IP 電話の回線およびデバイスのコーリング サーチ スペースを連結します。回線/デバイス アプローチにおいては、次の概念が重要です。

- デバイス コーリング サーチ スペースは、コール ルーティング情報を提供します。
- 回線コーリング サーチ スペースは、サービス クラス情報を提供します。

デバイス モビリティ機能を使用すると、デバイス コーリング サーチ スペースは、電話機のロケーションに基づいて、動的に電話機に関連付けられます。デバイス モビリティを使用する場合に、回線/デバイスにおける重要な概念は、引き続き同じです。回線コーリング サーチ スペースがサービス クラス情報を提供する一方、選択されたローミングまたはホーム デバイス コーリング サーチ スペースは、コール ルーティング情報を提供します。

図 21-6 は、クラスタ内でデバイス モビリティを使用する場合に、回線/デバイス アプローチを使用してサービス クラスを構築する例を示します。

図 21-6　サービス クラスを構築するための回線 / デバイス アプローチ



回線 / デバイス アプローチを使用して、サービス クラスを構築することをお勧めします。このモデルでは、次の公式が示すように、必要なデバイス プールの数が大幅に削減されるため、デバイス モビリティを使用するうえで重要な利点があります。

合計デバイス プール数 =（サイト数）

このアプローチには、次の設計上の考慮事項が適用されます。

- 電話デバイスのコーリング サーチ スペースは NONE に設定できます。デバイス プールのコーリング サーチ スペース設定が電話デバイスに割り当てられます。この方法では、電話機にデバイス コーリング サーチ スペースを個別に設定する必要がないため、設定の量を大幅に削減できます。
- 同じサービス クラスまたはコール特権をすべてのモバイル ユーザに設定することに関して制限はありません。サービス クラスは、回線コーリング サーチ スペースを使用して定義されるため、モバイル ユーザはローミング中に同じサービス クラスを維持します。
- モバイル ユーザはプロファイルのデバイス モビリティとエクステンション モビリティの両方を有効にすることができます。

ダイヤル プラン モデルの選択

「ダイヤル プラン」（P.10-1）の章で説明したように、ダイヤル プラン モデルには主に 3 つのアプローチがあります。

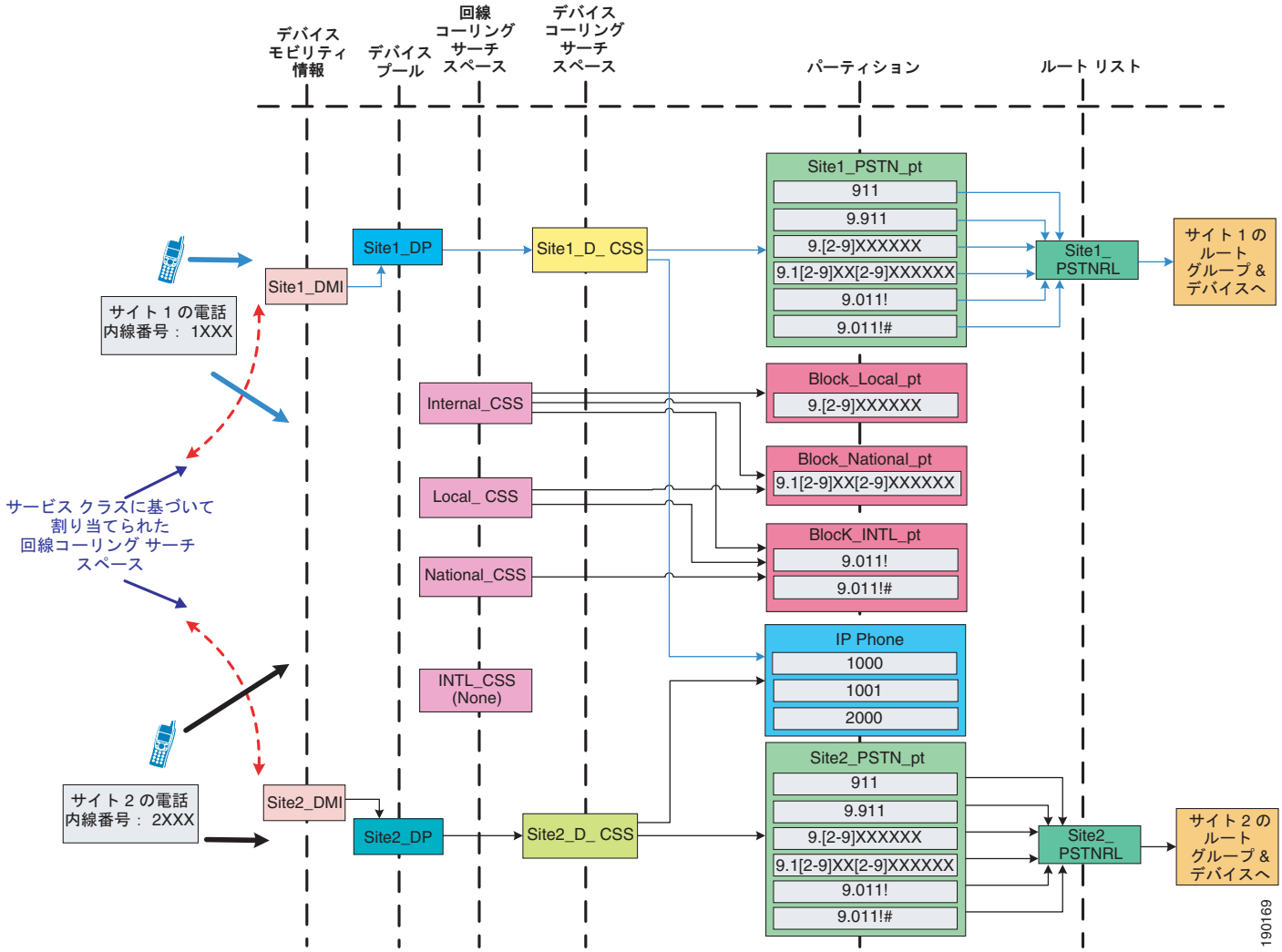
- 定型オンネット ダイヤリング
- 分割アドレッシングの可変長のオンネット ダイヤリング
- フラット アドレッシングの可変長のオンネット ダイヤリング

次の項では、サービス クラスを構築するためのアプローチと組み合わされたさまざまなダイヤル プラン モデルを示します。

回線/デバイス アプローチを使用する定型オンネット ダイヤリング

図 21-7は、デバイス モビリティのための固定オンネット ダイヤル プランを示します。

図 21-7　デバイス モビリティのための固定オンネット ダイヤル プラン



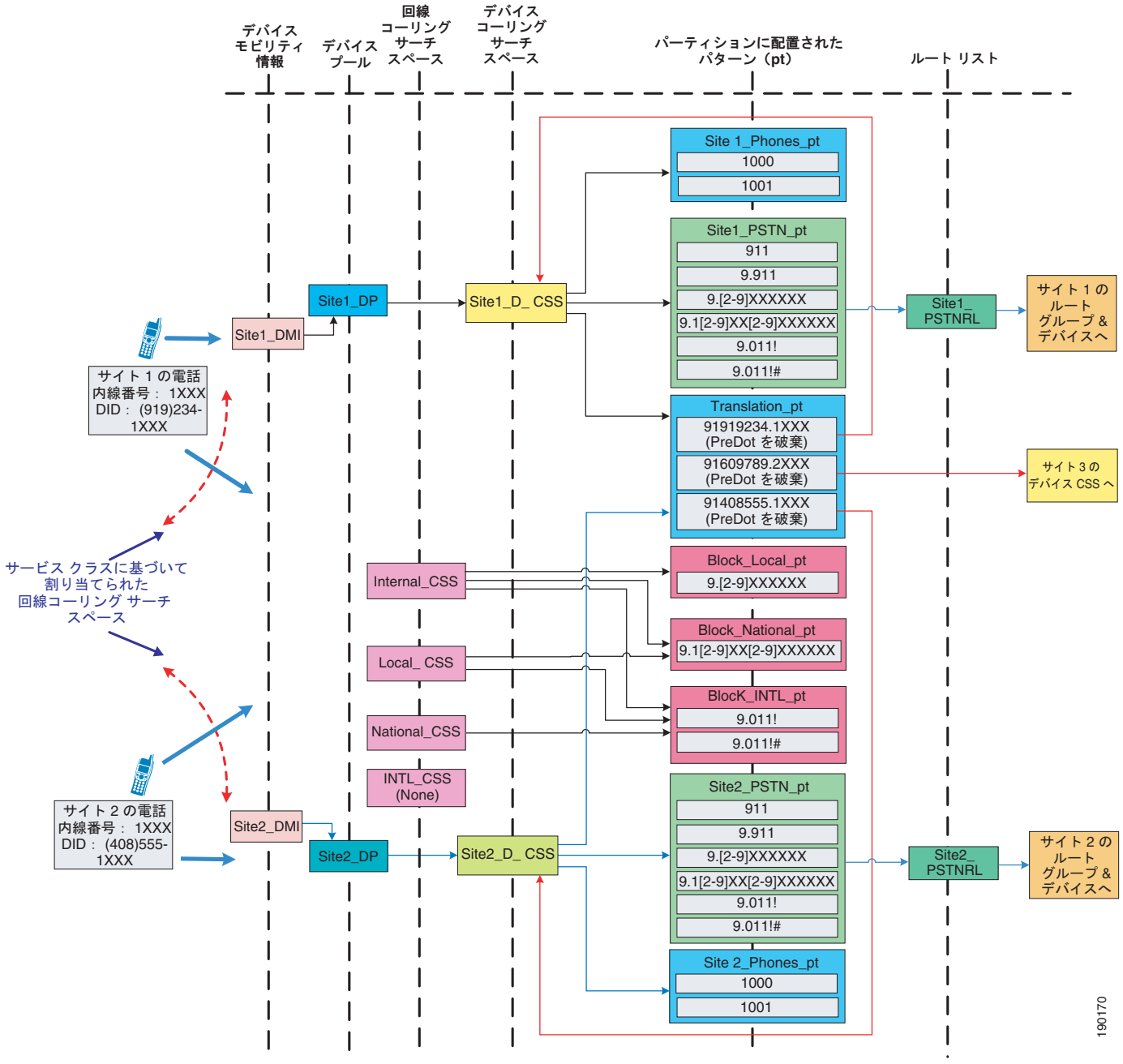
これは、最も基本的なダイヤル プラン モデルであり、次の特性があります。

- モバイル ユーザは、すべてのロケーションから省略ダイヤリング（図 21-7 の例に示されている 4 桁）を使用できます。
- 内線用の省略された短縮ダイヤルが、ローミング ロケーションにいるユーザの電話機で引き続き動作します。
- モバイル ユーザがリモート ロケーションにいるときは、「ローミング」コーリング サーチ スペースが使用されます。サイトすべての公衆網コールに同じアクセス コードを設定することをお勧めします。公衆網アクセス コードが同じでないと、ユーザは、さまざまなアクセス コードを知る必要があります。

回線/デバイス アプローチを使用する、分割アドレッシングの可変長のオンネット ダイヤリング

図 21-8 は、デバイス モビリティのための分割アドレッシングによる可変長オンネット ダイヤリング プランを示します。

図 21-8　デバイス モビリティのための分割アドレッシングによる可変長オンネット ダイヤリング プラン



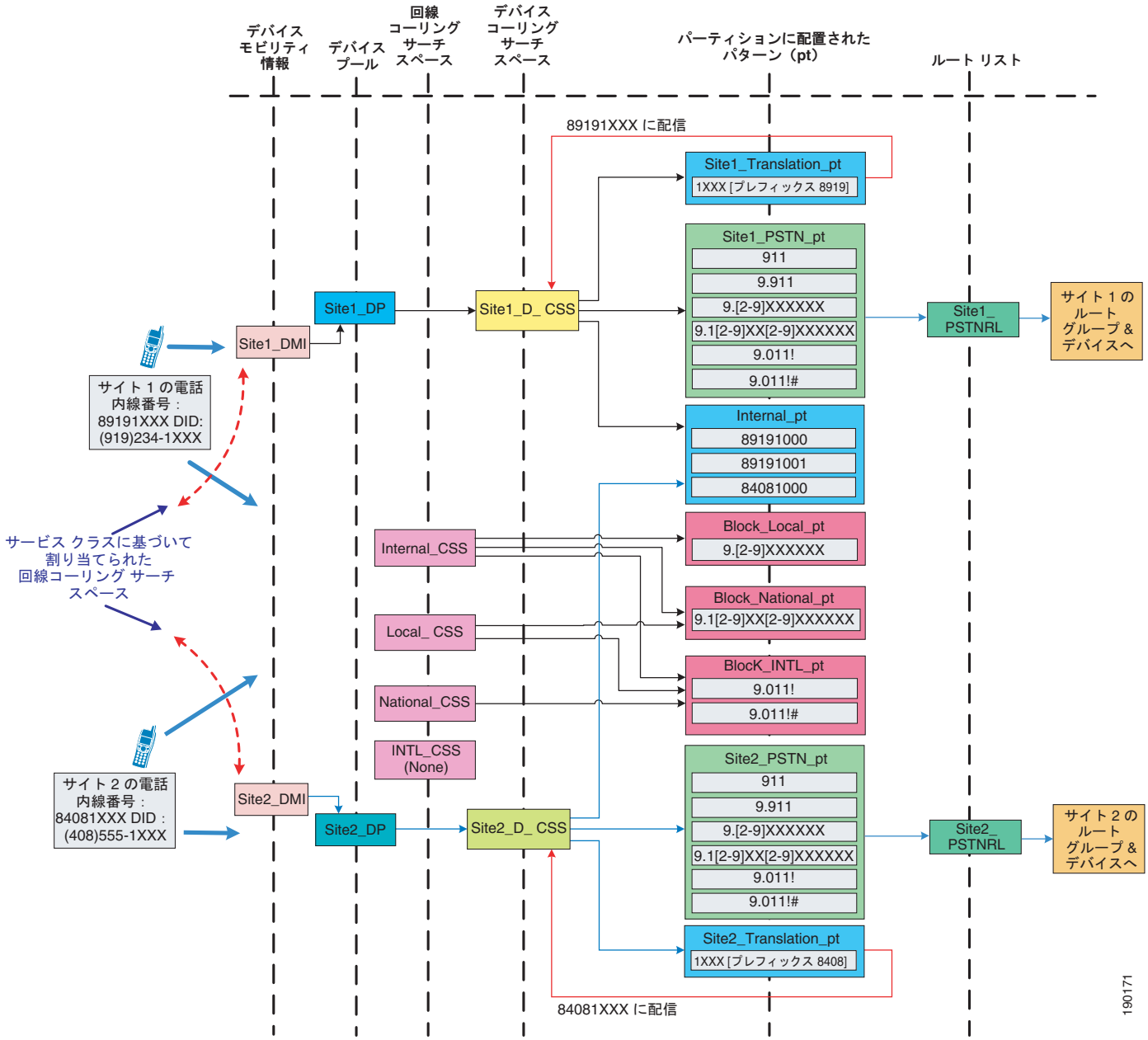
次の設計上の考慮事項が、図 21-8 のダイヤル プラン モデルに適用されます。

- モバイル ユーザがローミング ロケーションから省略ダイヤリングを使用すると、コールが誤った宛先にルーティングされることがあります。図 21-8 の例で、サイト 1 のモバイル ユーザ 1 の内線が 1000 であり、サイト 2 に移動するとします。ユーザ 1 がサイト 1 にいるユーザと通話しようと 1001 をダイヤルすると、コールは代わりにサイト 2 の内線 1001 にルーティングされます。この動作が望ましくない場合は、各サイトをデバイス モビリティ グループとして定義することを検討してください。ただし、ユーザは、外部公衆網コールすべてで、モバイル電話では引き続きホーム ゲートウェイが使用され、したがって WAN 大域幅が消費されることを承知しておく必要があります。
- 公衆網およびトランスレーション パーティションへのアクセスだけを持つローミング ユーザのために追加のデバイス コーリング サーチ スペースを設定できます。この設定には、サイトごとに 1 つ以上の追加のデバイス プールとコーリング サーチ スペースが必要です。したがって、*N* 個のサイトには、*N* 個のデバイス プールおよび *N* 個のコーリング サーチ スペースが必要です。ただし、この設定では、各サイトをデバイス モビリティ グループとして定義する必要がありません。
- 省略された短縮ダイヤルを使用しないでください。すべてのロケーションでユーザが短縮ダイヤルを使用できるようにする普遍的な方法で短縮ダイヤルを設定することをお勧めします。たとえば、ユーザは、E.164 番号を使用するか、サイト コードおよびアクセス コードを使用して短縮ダイヤルを設定できます。
- 複数のサイトの内線番号が重複していると、ローミング ユーザがリモート SRST ゲートウェイに登録されたときに問題を引き起こすことがあります。図 21-8 の例で、サイト 1 のモバイル ユーザ A の内線が 1000 であり、サイト 2 に移動するとします。さらに、サイト 2 の WAN リンクがダウンし、電話機がサイト 2 の SRST ゲートウェイに登録されることになったとします。SRST ゲートウェイにおける内線 1000 への着信コールは、実際のサイト 2 の内線 1000 のほかに、内線番号が 1000 であるモバイル ユーザにもルーティングされます。この結果、コールが適切にルーティングされないことがあります。この問題は、ネットワーク全体で一意の内線番号を使用することにより回避できます。

回線/デバイス アプローチを使用する、フラット アドレッシングの可変長のオンネット ダイヤリング

図 21-9は、デバイス モビリティのためのフラット アドレッシングによる可変長オンネット ダイヤリング プランを示します。

図 21-9　デバイス モビリティのためのフラット アドレッシングによる可変長オンネット ダイヤリング プラン



次の設計上の考慮事項が、図 21-9 のダイヤル プラン モデルに適用されます。

- モバイル ユーザは、別のサイトにローミングした後では、コールが誤った宛先にルーティングされるおそれがあるため、省略ダイヤリングを使用できません。この動作が望ましくない場合は、各サイトをデバイス モビリティ グループとして定義することを検討してください。ただし、ユーザは、外部公衆網コールすべてで、モバイル電話では引き続きホーム ゲートウェイが使用され、したがって WAN 大域幅が消費されることを承知しておく必要があります。
- 公衆網および内部電話機パーティションへのアクセスだけを持つローミング ユーザのために追加のデバイス コーリング サーチ スペースを設定できます。この設定には、サイトごとに 1 つ以上の追加のデバイス プールとコーリング サーチ スペースが必要です。したがって、*N* 個のサイトには、*N* 個のデバイス プールおよび *N* 個のコーリング サーチ スペースが必要です。ただし、この設定では、各サイトをデバイス モビリティ グループとして定義する必要がありません。
- リモート SRST ゲートウェイに登録されているモバイル ユーザは、一意な内線番号を持ちます。ただし、モバイル ユーザは、リモート SRST ゲートウェイに登録されているときは、公衆網ユーザがモバイル ユーザと通話できないことを承知しておく必要があります。

VPN を使用するための設計ガイドライン

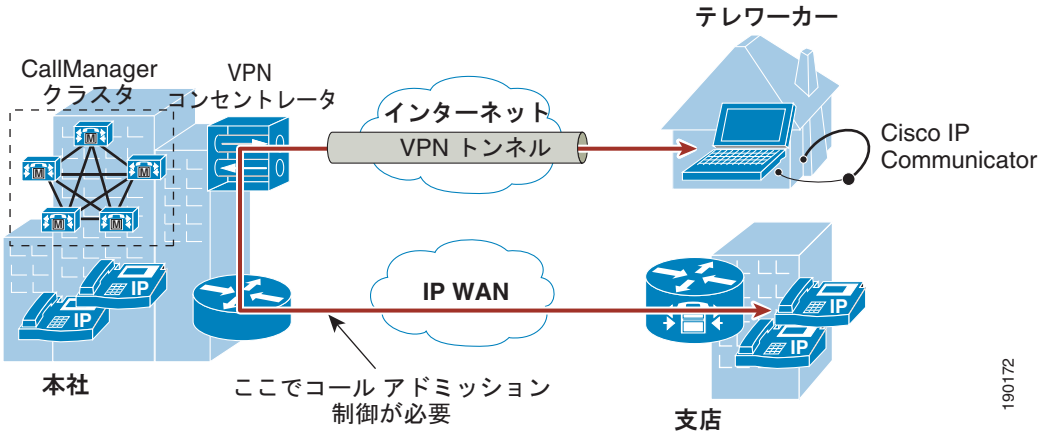
この項では、IP ソフトウェア電話または Cisco IP Communicator のデバイス モビリティ機能を有効にするための設計ガイドラインを簡単に説明します。大部分のユーザは、インターネット経由のバーチャル プライベート ネットワーク（VPN）接続を使用して Unified CM クラスタに接続するソフトフォンを持つことができます。

VPN の導入については、次の URL で入手可能なさまざまな VPN 設計ガイドを参照してください。

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

図 21-10 では、VPN 経由で Unified CM クラスタに接続されている IP ソフトフォン ユーザの例を示します。

図 21-10　Cisco IP Communicator への VPN 接続



VPN ユーザは、次のガイドラインに従う必要があります。

- VPN コンセントレータによって配布または所有されている IP サブネットを指定してデバイス モビリティ情報（DMI）を設定します。
- VPN コンセントレータと同じ場所にあるデバイスに使用されるデバイス プールと同じデバイス プールに DMI を関連付けます。ただし、コール特権、ネットワーク ロケールなどのパラメータを考慮する必要があります。

- 直近の VPN コンセントレータを使用するようユーザに指示してください。

これらのガイドラインにより、企業 WAN でコール アドミッション制御が正しく適用されます。

CHAPTER 22

Cisco Unified Presence

Cisco Unified Presence は、Cisco Unified Communications システムの価値を高める多くのコンポーネントから構成されています。プレゼンス機能の中心的なコンポーネントである Cisco Unified Presence サーバは、ユーザの可用性ステータスと通信能力に関する情報を収集します。ユーザの可用性ステータスは、ユーザが電話機などの通信デバイスをアクティブに使用しているかどうかを示します。ユーザの通信能力は、ビデオ会議、Web コラボレーション、インスタント メッセージング、基本オーディオなど、ユーザが使用できる通信の種類を示します。

Cisco Unified Presence サーバによって取り込まれた集約的ユーザ情報は、Cisco Unified Personal Communicator と Cisco Unified Communications Manager の 2 つのアプリケーションがユーザの生産性を高めるのに役立ちます。これらのアプリケーションは、最も効果的な通信形態を判断することにより、ユーザ間のコミュニケーションの効率性を高めます。

この章では、Cisco Unified Communications システムにおけるプレゼンスの基本概念を説明し、プレゼンス ソリューションのさまざまなコンポーネントを最適に配置するためのガイドラインを示します。Cisco Unified Presence は、Cisco Unified Communications Manager（Unified CM）5.*x* 以降のリリースと一緒に配置する必要があります。Cisco Unified CM 4.*x* 以前のリリースは Cisco Unified Presence をサポートしていません。

この章では、次のトピックについて取り上げます。

この章の新規情報

表 22-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 22-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
Cisco Unified Communications Manager Business Edition	「Cisco Unified Presence の配置ガイドライン」（P.22-33）
Cisco Unified Personal Communicator	「Cisco Unified Personal Communicator」（P.22-38）

表 22-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報 （続き）

新規トピックまたは改訂されたトピック	説明箇所
Cisco WebEx	「Cisco Unified Personal Communicator の設計上の考慮事項」（P.22-41）
WAN を介したクラスタ化と地理的冗長性	「WAN を介したクラスタ化」（P.22-23）
クラスタ	「Cisco Unified Presence サーバ クラスタ」（P.22-11）
配置モデル	「Cisco Unified Presence の配置モデル」（P.22-14）
フェデレーション配置	「フェデレーション配置」（P.22-24）
IBM Sametime	「Integrating Cisco Unified Presence と IBM Sametime Server 7.5.1 の統合のためのガイドライン」（P.22-45）
LDAP 検索コンテキスト	「Cisco Unified Personal Communicator の設計上の考慮事項」（P.22-41）
Microsoft Exchange Server	「Cisco Unified Presence のカレンダー統合」（P.22-28）
モビリティ統合	「Cisco Unified Presence のモビリティ統合」（P.22-29）
マルチクラスタ配置	「マルチクラスタ配置」（P.22-21）
カレンダーでの多言語サポート	「多言語カレンダーのサポート」（P.22-29）
パフォーマンス	「Cisco Unified Presence サーバのパフォーマンス」（P.22-17）
ディレクトリ番号の逆ルックアップ	「Cisco Unified Presence と Microsoft Live Communications Server 2005 または Office Communications Server 2007 との統合のためのガイドライン」（P.22-44）
サードパーティ製オープン API	「Cisco Unified Presence のサードパーティ製 Open API」（P.22-31）

プレゼンス

*プレゼンス*とは、ユーザが特定のデバイス セットで通信する能力とその意志を意味します。プレゼンスでは、次の段階またはアクティビティが実行されます。

- ユーザ ステータスのパブリッシュ

  ユーザ ステータスの変化は、ユーザによるキーボード操作、電話機の使用、またはデバイスのネットワーク接続が認識されてへのデバイス接続などが認識されることで自動的にパブリッシュされます。

- このステータスの収集

  パブリッシュされた情報は、すべての利用可能なソースから収集され、プライバシー ポリシーが適用され、現在のステータスが集約および同期されてから、保存されたうえで消費されます。

- 情報の消費

  デスクトップ アプリケーション、カレンダー アプリケーション、およびデバイスが、ユーザ ステータス情報を使用して、エンドユーザにリアルタイムの更新情報を提供します。これにより、エンド ユーザは、適切な通信方法を判断できるようになります。

ステータス情報は、デバイスやユーザが実行可能な機能（音声、ビデオ、Web コラボレーションなど）と、デバイスやユーザの状態（利用可能、ビジー、通信中など）の両方を示します。Presence ステータスは、コンピュータへのログインや電話機のオフフックなどの自動イベントによって決定されるか、またはユーザがステータス変更ピックリストから Do Not Disturb を選択したなど、ユーザによるステータス変更の明確な通知イベントによって決定されます。

プレゼンスに関する用語として、ウォッチャ、プレゼンス エンティティ（*presentity*）、およびプレゼンス サーバがあります。プレゼンス エンティティとは、その現在のステータスを PUBLISH または REGISTER メッセージによってプレゼンス サーバにパブリッシュするエンティティです。プレゼンス エンティティは、通信クラスタ内外の directory number（DN; ディレクトリ番号）または SIP の uniform resource identifier（URI; ユニフォーム リソース識別子）です。*ウォッチャ*（デバイスまたはユーザ）は、プレゼンス サーバに SUBSCRIBE メッセージを送信することにより、プレゼンス エンティティに関するプレゼンス ステータスを要求します。これに対しプレゼンス サーバは、要求されたプレゼンス エンティティの現在のステータスが含まれた NOTIFY メッセージをウォッチャに返します。

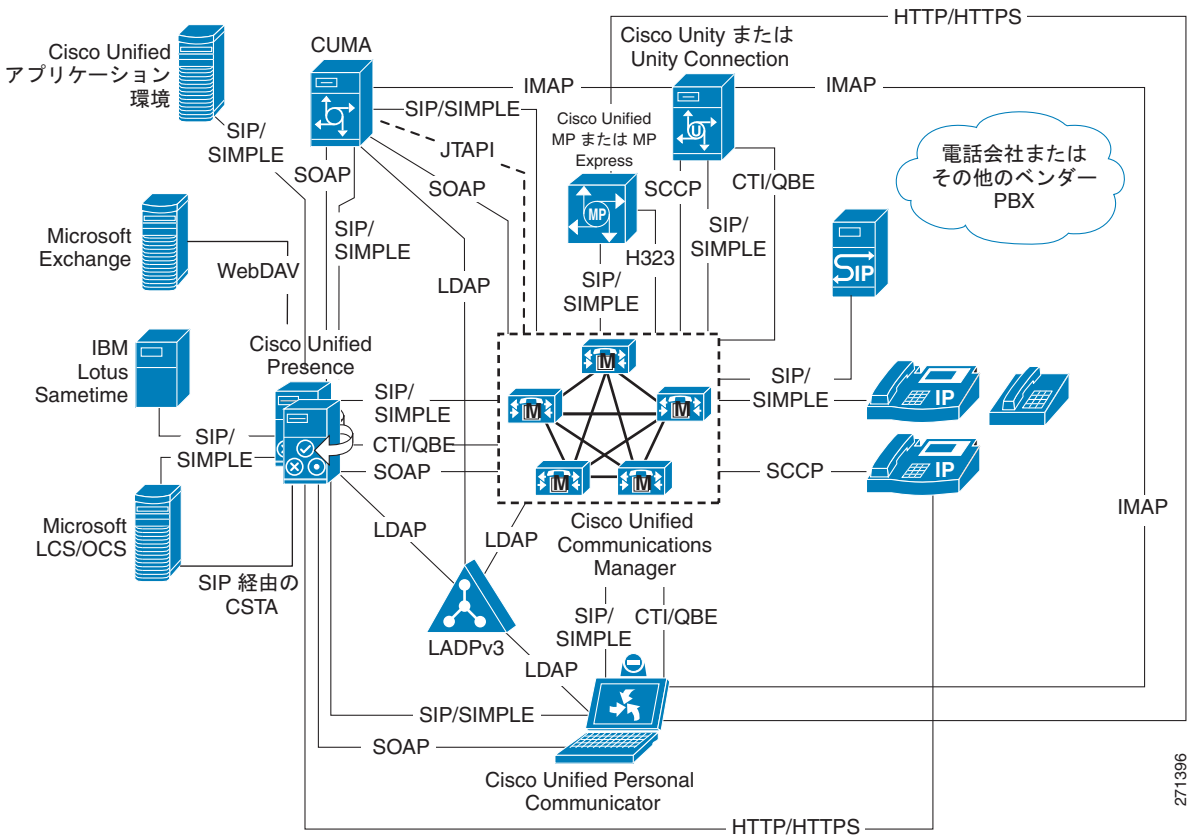
プレゼンスに SIP を使用するのは、それが音声、ビデオ、Web、電子メール、プレゼンス、およびインスタント メッセージングなどのすべての主要な通信サービスを単一のインフラストラクチャ上に統合するからです。SIP は拡張可能なプロトコルであり、指定された要求のルーティングや、適切な場所への応答をすでに実行している既存の SIP ネットワークに、プレゼンス イベントなどのパッケージを追加できます。SIP はこれらのサービスを連係させることによって、強固な統合を実現するとともに、このような複合的な通信サービス配信の管理の複雑さを軽減します。

Cisco Unified Presence のコンポーネント

Cisco Unified Presence には、次のコンポーネントが含まれています（図 22-1 を参照）。

- Cisco Unified Presence サーバ
- Cisco Unified Communications Manager（Unified CM）
- Cisco Unified Personal Communicator
- Cisco Unified MeetingPlace または MeetingPlace Express
- Cisco Unity または Unity Connection
- Cisco Unified Videoconferencing または Cisco Unified MeetingPlace Express VT
- Lightweight Directory Access Protocol（LDAP）Server v3.0
- Cisco Unified IP Phone
- サードパーティ製のプレゼンス サーバ

図 22-1　Cisco Unified Presence のコンポーネント



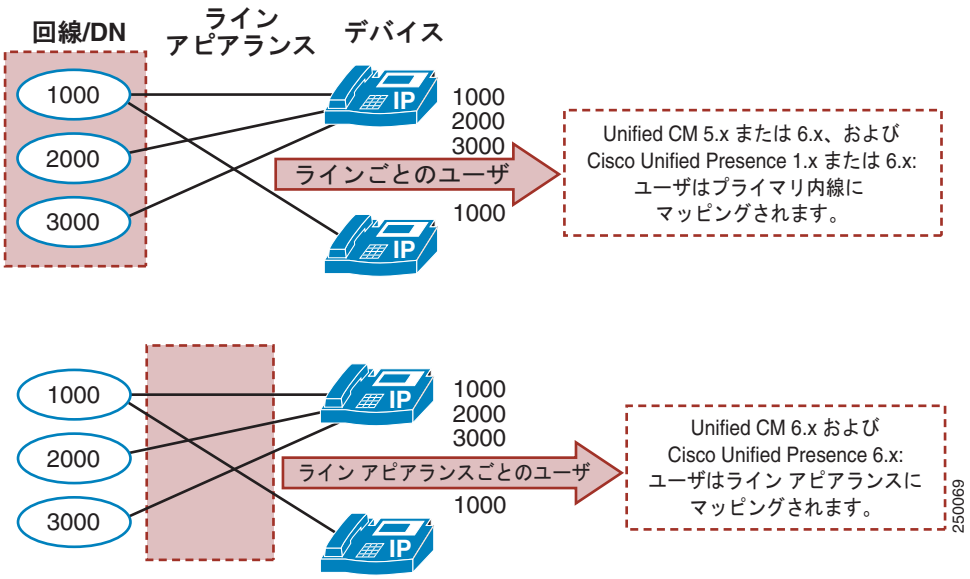
Cisco Unified Presence ユーザ

ユーザのプレゼンスは通常、ユーザのプレゼンス ステータス、システム上のユーザ数、またはユーザのプレゼンス機能で示されます。

Cisco Unified Presence での定義のとおり、ユーザは Cisco Unified CM でデフォルトでエンド ユーザとして指定されており、プライマリ内線が設定されている必要があります。ユーザは実質的にディレクトリ番号に結合されているので、プレゼンス ステータスは、ユーザのプライマリ内線の状態を反映し、ユーザが関連付けられているデバイスの状態は反映されません（図 22-2 を参照）。

Cisco Unified CM でエンド ユーザとして指定されたユーザには、プライマリ内線の設定や、ライン アピアランスの関連付けが可能です。CUP PUBLISH Trunk サービス パラメータを使用する場合は、ユーザにプライマリ内線を設定するだけでなく、ライン アピアランスと関連付ける必要があります。ライン アピアランスに関連付けることによって、ユーザは実質的にライン アピアランス（特定のデバイスのディレクトリ番号）に結合されるので、より詳細できめ細かいプレゼンス情報を集約できます。ユーザを複数のライン アピアランスにマップすることも、各ライン アピアランスに複数のユーザ（最大 5 人）を割り当てることも可能です。エンド ユーザをライン アピアランスに関連付けることをお勧めします（図 22-2 を参照）。

図 22-2　プライマリ内線またはライン アピアランスに関連付けられたエンド ユーザ



この章では、*プレゼンス ユーザ*という概念が随所で使用されます。Cisco Unified Presence で定義されるユーザの意味を常に念頭に置いてください。

Unified CM Presence

ユーザのプレゼンス要求は、クラスタ内かクラスタ外かに関係なく、すべて Cisco Unified CM で処理されます。

ウォッチャが、プレゼンス エンティティと同じ Unified CM クラスタ内にある場合、要求を送信した Unified CM ウォッチャは、プレゼンス ステータスなどの応答を直接受信します。

プレゼンス エンティティがクラスタ外にある場合、Unified CM は、SIP トランク経由で外部のプレゼンス エンティティに照会します。ウォッチャが、SUBSCRIBE コーリング サーチ スペースとプレゼンス グループ（いずれも「Unified CM のプレゼンス ポリシー」（P.22-8）の章を参照）に基づいて外部プレゼンスをモニタする権限を持つ場合、SIP トランクはプレゼンス要求を外部プレゼンス エンティティに転送し、外部プレゼンス エンティティからの応答を待って、現在のプレゼンス ステータスをウォッチャに返します。

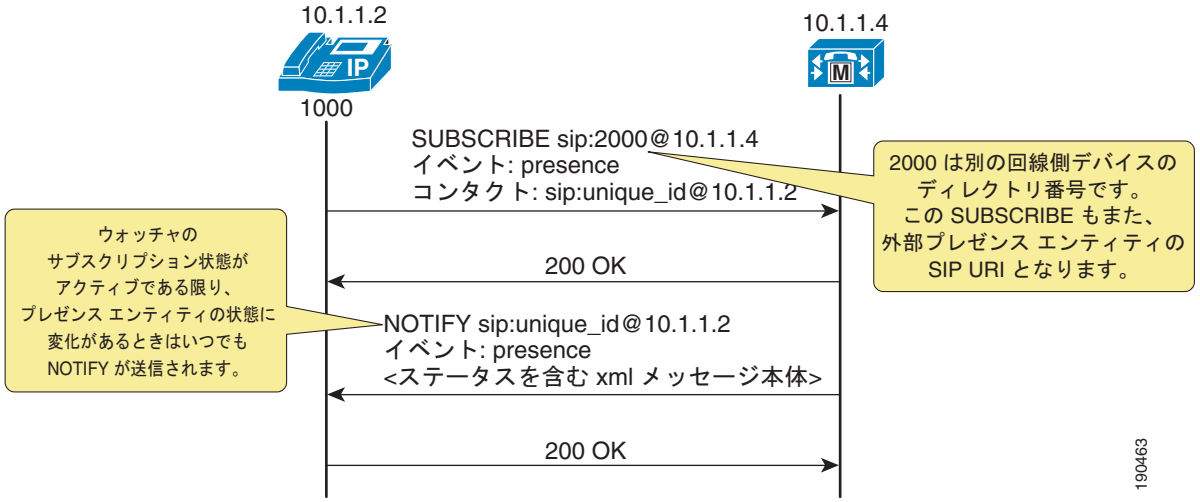
Unified CM クラスタ外のウォッチャは、プレゼンス要求を SIP トランクに送信します。Unified CM がそのプレゼンス エンティティをサポートしている場合、現在のプレゼンス ステータスを応答として返します。Unified CM がそのプレゼンス エンティティをサポートしていない場合、SIP エラー応答によってプレゼンス要求を拒否します。

SIP を使用した Unified CM Presence の配置

Unified CM で、*SIP 回線*という用語は、Unified CM に直接接続され、登録されている SIP 対応のエンドポイントを表し、*SIP トランク*という用語は、SIP をサポートするトランクを表します。プレゼンス ウォッチャとして動作する SIP 回線側エンドポイントは、指定されたプレゼンス エンティティのプレゼンス ステータスを要求する SIP SUBSCRIBE メッセージを Unified CM に送信します。

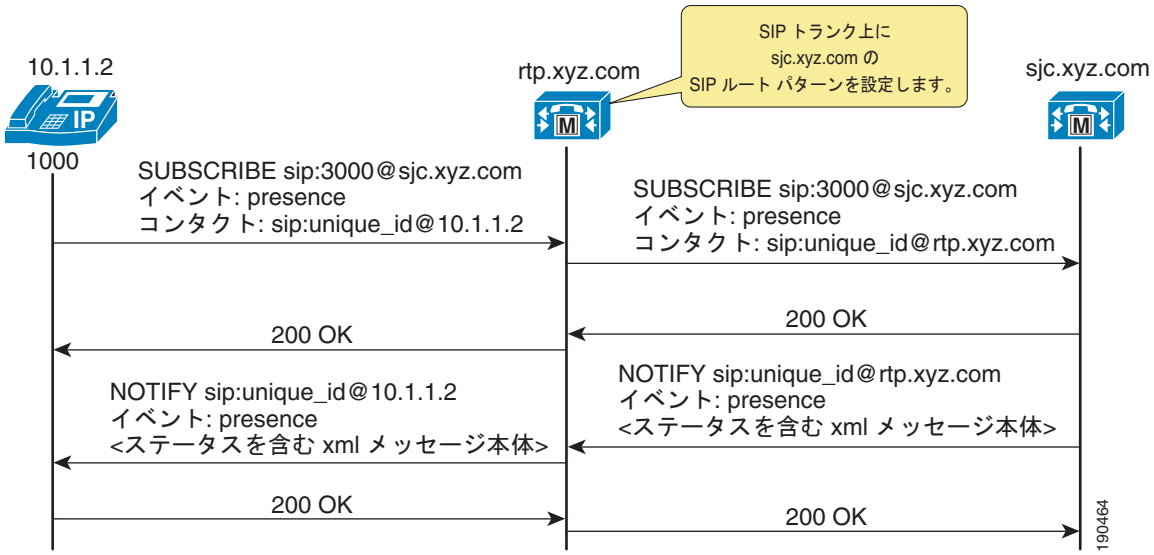
そのプレゼンス エンティティが Unified CM クラスタ内にある場合、Unified CM は、SIP 回線側プレゼンス要求に対し、プレゼンス エンティティの現在のステータスを示す SIP NOTIFY メッセージをプレゼンス ウォッチャに応答として送信します（図 22-3 を参照）。

図 22-3　SIP 回線の SUBSCRIBE/NOTIFY の交換



そのプレゼンス エンティティが Unified CM クラスタ外にある場合、Unified CM は、SUBSCRIBE コーリング サーチ スペース、プレゼンス グループ、および SIP ルート パターンに基づいて、SUBSCRIBE 要求を外部の適切な SIP トランクにルーティングします。Unified CM は、プレゼンス エンティティのステータスを示す SIP NOTIFY 応答をトランクで受信すると、SIP 回線側プレゼンス要求に対し、プレゼンス エンティティの現在のステータスを示す SIP NOTIFY メッセージをプレゼンス ウォッチャに送信して応答します（図 22-4 を参照）。

図 22-4　SIP トランクの SUBSCRIBE/NOTIFY の交換



Unified CM クラスタの外側にあるディレクトリ番号または SIP URI に対する SUBSCRIBE メッセージは、Unified CM 内の SIP トランク上で送受信されます。SIP トランクは、別の Unified CM とのインターフェイスとして動作するか、Cisco Unified Presence サーバとのインターフェイスとして動作することができます。

SCCP を使用した Unified CM Presence

Unified CM では、Skinny Client Control Protocol（SCCP）回線側エンドポイントがプレゼンス ウォッチャとして動作することができます。SCCP トランクは存在しません。SCCP エンドポイントは、Unified CM に SCCP メッセージを送信して、指定したプレゼンス エンティティのプレゼンス ステータスを要求することができます。

そのプレゼンス エンティティが Unified CM クラスタ内にある場合、Unified CM は、SCCP 回線側プレゼンス要求に対し、プレゼンス エンティティの現在のステータスを示す SCCP メッセージをプレゼンス ウォッチャに送信して応答します

そのプレゼンス エンティティが Unified CM クラスタ外にある場合、Unified CM は、SUBSCRIBE コーリング サーチ スペース、プレゼンス グループ、および SIP ルート パターンに基づいて、SUBSCRIBE 要求を外部の適切な SIP トランクにルーティングします。Unified CM は、プレゼンス エンティティのステータスを示す SIP NOTIFY 応答をトランクで受信すると、SCCP 回線側プレゼンス要求に対し、プレゼンス エンティティの現在のステータスを示す SCCP メッセージをプレゼンス ウォッチャに送信して応答します。

Unified CM の短縮ダイヤルのプレゼンス

Unified CM は、Busy Lamp Field（BLF; ビジー ランプ フィールド）短縮ダイヤルを使用した短縮ダイヤルのプレゼンス機能をサポートしています。BLF 短縮ダイヤルは、短縮ダイヤルとプレゼンス インジケータの両方の機能を備えています。ただし、BLF 短縮ダイヤルを設定できるのは管理者のみで、システム ユーザは BLF 短縮ダイヤルを設定できません。

管理者は、対象のディレクトリ番号に対し、宛先の Unified CM クラスタまたは SIP トランク内のディレクトリ番号に解決可能な BLF 短縮ダイヤルを設定する必要があります。SIP URI に対して、BLF 短縮ダイヤル用に、BLF SIP 回線側エンドポイントを設定することもできますが、SCCP 回線側エンドポイントの設定はできません。BLF 短縮ダイヤルのインジケータは、回線レベルのインジケータであり、デバイス レベルのインジケータではありません。

次の Cisco Unified IP Phone は、SCCP に対する BLF 短縮ダイヤルをサポートしています。

- Cisco Unified IP Phone 7914G
- Cisco Unified IP Phone 7921G
- Cisco Unified IP Phone 7940G
- Cisco Unified IP Phone 7960G
- Cisco Unified IP Phone 7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G
- Cisco Unified IP Phone 拡張モジュール 7915、7916

次の Cisco Unified IP Phone は、SIP に対する BLF 短縮ダイヤルをサポートしています。

- Cisco Unified IP Phone 7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7961G、7961G-GE、7962G、および 7965G

- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G
- Cisco Unified IP Phone 拡張モジュール 7915、7916

Cisco Unified IP Phones 7905、7906、7911、および 7912 は、BLF 短縮ダイヤルをサポートしていません。

図 22-5 では、電話機のさまざまなタイプの BLF 短縮ダイヤルのインジケータを示しています。

図 22-5　　短縮ダイヤルのプレゼンスのインジケータ

状態	アイコン	LED
アイドル		
ビジー		
不明		

190465

Unified CM の履歴のプレゼンス

Unified CM は、コール履歴リストに関するプレゼンス機能をサポートしています（電話機の Directories ボタン）。コール履歴リストのプレゼンス機能は、Unified CM Administration 内の **BLF for Call Lists** エンタープライズ パラメータによって制御されます。**BLF for Call Lists** エンタープライズ パラメータは、電話機の Directories ボタンを使用するすべてのページ（不在着信、着信履歴、発信履歴、個人ディレクトリ、社内ディレクトリ）に影響を及ぼし、グローバルに設定されます。

コール履歴リストのプレゼンス機能は、次の Cisco Unified IP Phone で SCCP と SIP の両方に対してサポートされています。

- Cisco Unified IP Phone 7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G

Cisco Unified IP Phone 7905G、7906G、7911G、7912G、7940G、7960G は、コール履歴リストのプレゼンス機能をサポートしていません。

コール履歴リストのプレゼンス インジケータには、図 22-5 のアイコン列と同じインジケータが使用されます。LED インジケータはありません。

Unified CM のプレゼンス ポリシー

Unified CM には、プレゼンス ステータスを要求するユーザに対して、ポリシーを設定する機能があります。このポリシーを設定するには、まずプレゼンス ステータスに関する SIP SUBSCRIBE メッセージを特にルーティングするコーリング サーチ スペースを設定します。次に、ユーザを関連付けることのできるプレゼンス グループを設定し、そのグループに対し、他のグループのユーザのプレゼンス ステータスを表示するためのルールを指定します。

Unified CM の SUBSCRIBE コーリング サーチ スペース

Unified CM のプレゼンス ポリシーの第 1 の側面は、SUBSCRIBE コーリング サーチ スペースです。Unified CM は、SUBSCRIBE コーリング サーチ スペースを使用して、ウォッチャ（電話機またはトランク）から送信されるプレゼンス要求（Event フィールドが Presence に設定された SUBSCRIBE メッセージ）のルーティング方法を決定します。SUBSCRIBE コーリング サーチ スペースは、ウォッチャに関連付けられ、ウォッチャが「確認」できるパーティションをリストします。このメカニズムによって、プレゼンス SUBSCRIBE 要求を通常のコール処理コーリング サーチ スペースから独立してルーティングするという詳細な制御が可能になります。

SUBSCRIBE コーリング サーチ スペースは、デバイス別またはユーザ別に割り当てることができます。ユーザがエクステンション モビリティを使用してデバイスにログインするか、管理によってデバイスに割り当てられると、開始されるサブスクリプションにユーザ設定が適用されます。

SUBSCRIBE コーリング サーチ スペースを <None> に設定すると、BLF 短縮ダイヤルとコール履歴リストのプレゼンス ステータスが機能しなくなり、サブスクリプション メッセージが「user unknown」として拒否されます。有効な SUBSCRIBE コーリング サーチ スペースを指定すると、インジケータが動作し、SUBSCRIBE メッセージが受け入れられて、適切にルーティングされます。

（注） <None> と定義されたままのコーリング サーチ スペースを残さないでください。コーリング サーチ スペースを <None> に設定したままにすると、プレゼンス ステータスやダイヤル プランの動作が予測困難になる可能性があります。

Unified CM のプレゼンス グループ

Unified CM のプレゼンス ポリシーの第 2 の側面は、プレゼンス グループです。プレゼンス グループには、デバイス、ディレクトリ番号、およびユーザを割り当てることができます。すべてのユーザは、デフォルトで Standard Presence Group に割り当てられています。プレゼンス グループは、定義済みのプレゼンス グループとのユーザのアソシエーションに基づいて、ウォッチャがモニタできる対象を制御します（たとえば、Contractors（協力会社）から Executives（重役）のモニタは禁止するが、逆は許可するなど）。ユーザがエクステンション モビリティ経由でデバイスにログインするか、管理によってデバイスに割り当てられると、開始されるサブスクリプションにプレゼンス グループのユーザ設定が適用されます。

複数のプレゼンス グループが定義されている場合は、Inter-Presence Group Subscribe Policy サービス パラメータが使用されます。1 つのグループと別のグループとの関係が、許可や禁止ではなく Use System Default 設定による場合、このサービス パラメータの値が有効になります。Inter-Presence Group Subscribe Policy サービス パラメータが **Disallowed** に設定されている場合、SUBSCRIBE コーリング サーチ スペースが許可していても、Unified CM は要求をブロックします。Inter-Presence Group Subscribe Policy サービス パラメータは、コール履歴リストがあるプレゼンス ステータスにのみ適用され、BLF 短縮ダイヤルには使用されません。

依存関係レコードを有効にすると、プレゼンス グループは、関連付けられたすべてのディレクトリ番号、ユーザ、およびデバイスをリストできます。依存関係レコードを使用することで、管理者はグループレベルの設定に関する特定の情報を検索できます。ただし、Dependency Record Enterprise パラメータを有効にすると、CPU の使用量が大きくなるので注意してください。

Unified CM のプレゼンス ガイドライン

システム管理者は、Unified CM で Unified CM Administration の中から、ユーザの電話機の状態のプレゼンス機能の設定と制御が可能です。Unified CM 内でプレゼンスを設定する場合は、次のガイドラインに従ってください。

- ユーザの電話機の状態のプレゼンス ステータスを表示できる適切なモデルの Cisco Unified IP Phone を選択します。
- プレゼンス ユーザのプレゼンス ポリシーを定義します。
  - SUBSCRIBE コーリング サーチ スペースを使用して、ウォッチャ プレゼンスベースの SIP SUBSCRIBE メッセージが正しい宛先にルーティングされるように制御します。
  - プレゼンス グループを使用して同類のユーザのセットを定義し、他のユーザ グループのプレゼンス ステータスの更新を許可するか禁止するかを定義します。
- コール履歴リストのプレゼンス機能はグローバルに有効になりますが、プレゼンス ポリシーを使用してユーザ ステータスをセキュリティ保護することができます。
- BLF 短縮ダイヤルは管理制御され、プレゼンス ポリシー設定の影響を受けません。

（注）　Cisco Unified Communications Manager Business Edition（Unified CMBE）は、Unified CM によってユーザ プレゼンス機能を設定および制御する場合とほぼ同じ方法で使用できます。詳細については、「Cisco Unified Communications Manager Business Edition」（P.27-1）を参照してください。

Cisco Unified Presence サーバ

Cisco Unified Presence サーバは、標準ベースの SIP と SIP for Instant Messaging and Presence Leveraging Extensions（SIMPLE）を使用して、すべての SIP または SIMPLE アプリケーションを Cisco Unified Communications System に統合するための、共通の境界ポイントを提供します。Cisco Unified Presence はまた、Simple Object Access Protocol（SOAP）経由の設定インターフェイスと、Representational State Transfer（REST）経由のプレゼンス インターフェイスを備えた HTTP インターフェイスを提供します。Cisco Unified Presence サーバは、これらの標準ベースの SIP、SIMPLE、および HTTP インターフェイスを使用して、ユーザの能力と属性を収集、集約、および配布します。

Cisco Unified Presence サーバの中心となるコンポーネントは、ユーザの可用性ステータスと通信能力に関する情報を収集する SIP Presence Engine に加え、プレゼンスに関連する SIP メッセージングと一般的な SIP メッセージングのルーティングのため SIP Proxy/Registrar で構成されます。アプリケーション（シスコ製またはサードパーティ製）にプレゼンスを統合することによって、エンド ユーザ エクスペリエンスと効率性を向上させるサービスを提供できます。Cisco Unified Presence サーバには、Cisco Unified IP Phone でインスタント メッセージングとプレゼンス ステータスを利用するための IP Phone Messenger アプリケーションがデフォルトで含まれています。Cisco Unified Presence サーバによってサポートされるクライアント、Cisco Unified Personal Communicator というクライアント、インスタント メッセージングとプレゼンス ステータスを統合します。

Cisco Unified Presence サーバはまた、Microsoft Live Communications Server 2005 または Office Communications Server 2007、および Unified CM に接続された Cisco Unified IP Phone 用の Microsoft Office Communicator クライアントとの相互運用性もサポートしています。Microsoft Office Communicator クライアントの相互運用性には、クリックツーダイヤル機能、電話制御機能、および Cisco Unified IP Phone のプレゼンス ステータスが含まれます。

Cisco Unified Presence サーバ クラスタ

Cisco Unified Presence サーバは、Unified CM が使用するのと同じ基盤のアプライアンス モデルとハードウェアを使用し、管理インターフェイスとほぼ同一です。サポートされるプラットフォームの詳細については、次の Web サイトで入手可能な『*Cisco Unified Presence Server Administration Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps6837/prod_maintenance_guides_list.html

Cisco Unified Presence は、6 つのサーバで構成され、そのうち 1 つはパブリッシャに指定されています。これは、Unified CM のパブリッシャおよびサブスクライバと同じアーキテクチャ概念を採用しています。Cisco Unified Presence クラスタの内部では、個別のサーバがサブクラスタにグループ化されています。1 つのサブクラスタには、最大 2 つのサーバを関連付けることができ、単一の Cisco Unified Presence クラスタは、最大 3 つのサブクラスタを図 22-6 に示す基本トポロジまたは図 22-7 に示す高可用性トポロジに配置することができます。Cisco Unified Presence クラスタはまた、1 つのサブクラスタには高可用性のために 2 つのサーバを設置し、その他のサブクラスタは 1 つのサーバだけを設置した混合サブクラスタに構成することもできます（図 22-8 を参照）。Cisco Unified Presence サーバは独自のクラスタを形成し、Unified CM クラスタの一部として正式に統合されているわけではありません。

図 22-6　Cisco Unified Presence の基本的配置

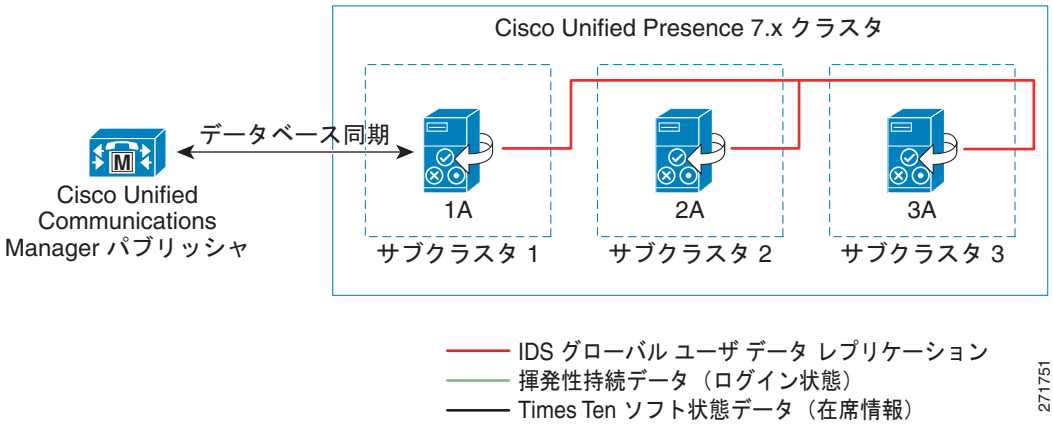


図 22-7　Cisco Unified Presence の高可用性配置

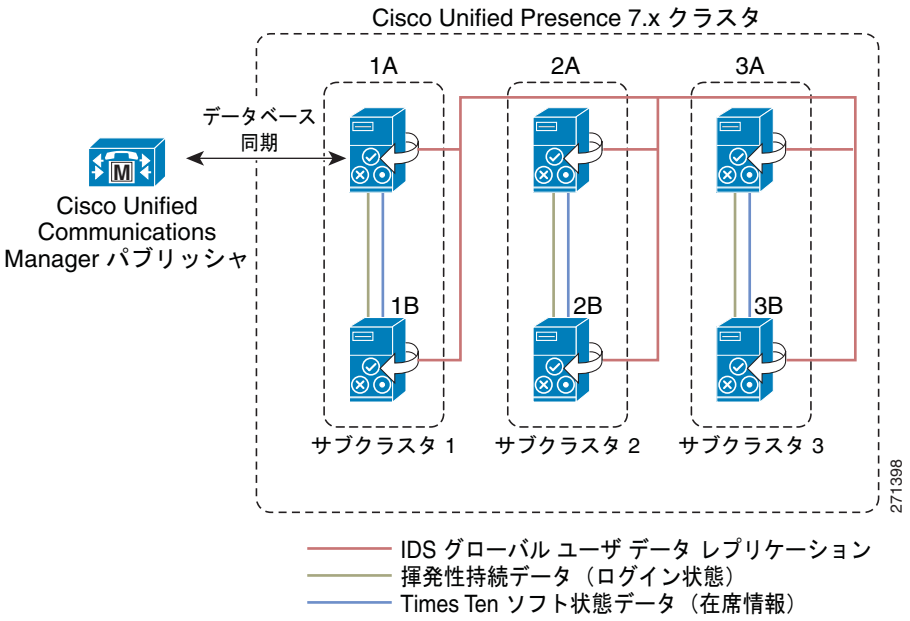
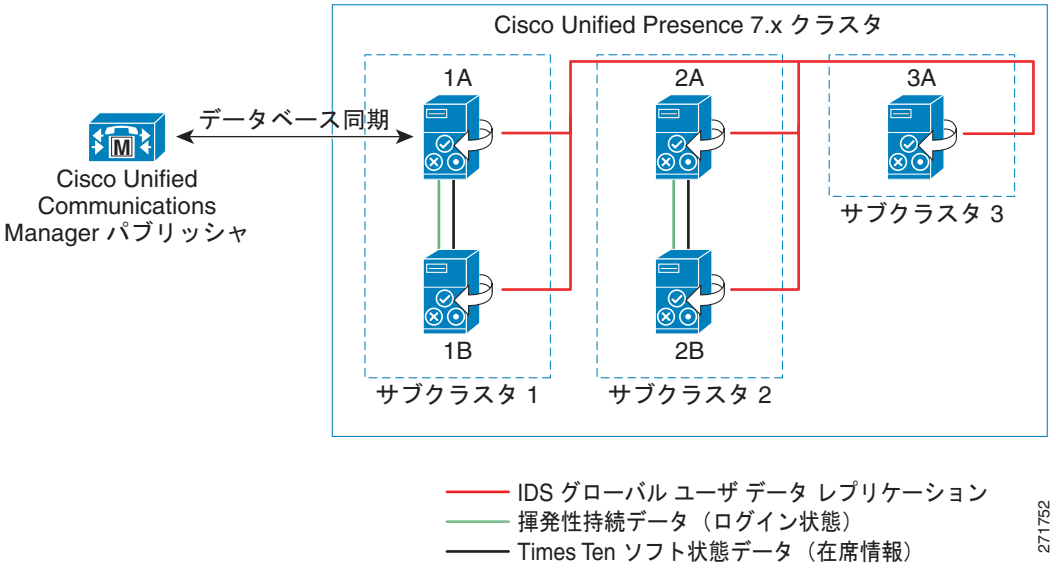


図 22-8　Cisco Unified Presence の混合配置



Cisco Unified Presence パブリッシャは、ユーザ情報とデバイス情報を共有することによって、Unified CM パブリッシャが使用するデータベースを利用し、それを拡張します。Cisco Unified Presence クラスタは、1 つの Unified CM クラスタのみをサポートするので、Cisco Unified Presence のすべてのユーザは、同じ Unified CM クラスタ内で定義する必要があります。

クラスタ内トラフィックは、Cisco Unified Presence と Unified CM の間、および Cisco Unified Presence パブリッシャとサブスクライバ サーバの間に非常に低いレベルで加わります。両方のクラスタは、共通のホスト ファイルを共有し、IPTables を使用した強力な信頼関係を備えています。これらは、データベースとサービスのレベルでは別個の異なるクラスタであり、それぞれの Cisco Unified

Presence サーバと Unified CM クラスタは別々に管理する必要があります。現在、クラスタ内トラフィックには、Transport Layer Security（TLS; トランスポート レイヤ セキュリティ）や IPSec は使用されていません。

Cisco Unified Presence サーバの外部システムとのインターフェイスは、UDP、TCP、TLS 経由で SIP トラフィックを送信します。TLS 相互認証には、Cisco Unified Presence サーバと外部システムの間の証明書のインポートとエクスポートが必要です。TLS サーバ認証（Cisco Unified Presence サーバが、検証用の TLS 証明書をクライアント デバイスに提示）では、HTTP ダイジェスト認証によって、エンド ユーザを検証します。

Cisco Unified Presence パブリッシャは、ユーザ情報とデバイス情報を共有することによって、Simple Object Access Protocol（SOAP）インターフェイスを使用して、AVVID XML Layer Application Program Interface（AXL API）経由で Unified CM パブリッシャと直接通信します。最初の設定時に、Cisco Unified Presence パブリッシャは、Unified CM ユーザおよびデバイス データベース全体の初期同期を実行します。すべての Cisco Unified Presence ユーザは、Unified CM End User 設定で設定されます。同期の際、Cisco Unified Presence は、Unified CM データベースからこれらのユーザをそれ自体のデータベースに入力しますが、その管理インターフェイスからエンドユーザ設定を提供することはありません。

Unified CM から最初に Cisco Unified Presence データベースを同期する場合、少し時間がかかることがあります。所要時間は、データベース内の情報量と現在システムにかかっている負荷によって異なります。それ以降は、新しいユーザ情報やデバイス情報が Unified CM に追加されたときに、Unified CM から Cisco Unified Presence へのデータベースの同期がリアルタイムで実行されます。プランニング用には、1 つの Cisco Unified Presence パブリッシャを使用して、Unified CM との初期データベース同期を実行する場合のガイドラインとして、表 22-2 の値を使用してください。

表 22-2　Cisco Unified Presence パブリッシャの同期の所要時間

サーバ プラットフォーム	ユーザ数	同期の所要時間
Cisco MCS 7816	500	5 分
Cisco MCS 7825	1,000	5 分
Cisco MCS 7835	1,000	5 分
	10,000	25 分
Cisco MCS 7845	1,000	5 分
	10,000	20 分
	30,000	70 分

プランニング用には、1 つの Cisco Unified Presence パブリッシャとサブスクライバ サーバを使用して、Unified CM との初期データベース同期を実行する場合のガイドラインとして、表 22-3 の値を使用してください。

表 22-3　Cisco Unified Presence パブリッシャとサブスクライバ サーバの同期の所要時間

サーバ プラットフォーム	ユーザ数	同期の所要時間
Cisco MCS 7816	500	5 分
Cisco MCS 7825	1,000	10 分
Cisco MCS 7835	1,000	10 分
	10,000	50 分

表 22-3　Cisco Unified Presence パブリッシャとサブスクライバ サーバの同期の所要時間 （続き）

サーバ プラットフォーム	ユーザ数	同期の所要時間
Cisco MCS 7845	1,000	10 分
	10,000	40 分
	30,000	140 分

（注）　Cisco Unified Presence サーバによる Unified CM からの初期データベース同期の際、同期エージェントがアクティブな間は、管理作業を一切行わないでください。

データベース エントリが更新中でなければ、Real-Time Monitoring Tool（RTMT）を使用してクリティカル アラーム、**Cisco Unified Presence ServerSyncAgentAXLConnectionFailed** をモニタすることで、同期エージェントとの接続が切断されていないかを確認できます。

Cisco Unified Presence サーバの冗長性

Unified CM は、オプションとして、次の冗長性設定から選択することができます。

- 2:1 冗長性方式：プライマリ サブスクライバ 2 台ごとに、1 つの共用バックアップ サブスクライバを設置します。
- 1:1 冗長性方式：プライマリ サブスクライバごとに、1 つのバックアップ サブスクライバを設置します。

Unified CM の冗長性の詳細については、「コール処理」（P.8-1）の章を参照してください。

Cisco Unified Presence クラスタは、6 つのサーバで構成されていますが、これを複数のサブクラスタ（最大 3 つのサブクラスタ）に構成して可用性を高めることができます。サブクラスタには最大 2 つのサーバが含まれ、フェールオーバー イベントの発生時には、サブクラスタの片方のサーバに関連付けられたユーザが、自動的にサブクラスタの他方のサーバを使用できるようになります。Cisco Unified Presence はサブクラスタ間のフェールオーバー機能は提供していません。

Cisco Unified Presence クラスタを高可用性を確保して配置する場合、フェールオーバー時にサブクラスタ内の 1 つのサーバに対してオーバーサブスクリプションにならないよう、サーバあたりの最大ユーザ数を考慮する必要があります。Cisco Unified Presence クラスタを配置する場合は、クラスタ内のすべてのサーバに同等のハードウェアを使用してください。

Cisco Unified Presence の配置モデル

Unified CM では、次の配置モデルを選択できます。

- 単一サイト
- 集中型コール処理を使用するマルチサイト WAN
- 分散型コール処理を使用するマルチサイト WAN
- WAN を介したクラスタ化

Cisco Unified Presence は、すべての Unified CM 配置モデルでサポートされます。ただし、初期ユーザ データベース同期のために、Cisco Unified Presence パブリッシャを Unified CM パブリッシャと共存させることをお勧めします。すべての Cisco Unified Presence サーバは、次の場合を除き、Cisco Unified Presence クラスタ内に共存する必要があります。

- データセンターの地理的冗長性と WAN を介したクラスタ化

  詳細については、「WAN を介したクラスタ化」（P.22-23）を参照してください。

- Cisco Unified Customer Voice Portal（Unified CVP）

  Cisco Unified Presence クラスタは、Cisco Unified Customer Voice Portal 配置の要件に従い、2 つのサイト間に最大 2 つのサーバ（各サイトに 1 つずつのサーバ）を置いて単一のクラスタを構成し、SIP プロキシ機能のみ（プレゼンス機能なし）を提供することができます。この配置では、5 Mbps 以上の帯域幅を確保し（主としてインストールおよび設定用）、遅延を 80 ms Round-trip Tme（RTT; ラウンド トリップ時間）以下に抑える必要があります。Unified CVP の詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『*Cisco Unified Customer Voice Portal SRND*』を参照してください。

Unified CM の配置モデルの詳細については、「Unified Communications の配置モデル」（P.2-1）の章を参照してください。

Cisco Unified Presence の配置は、高可用性の要件、合計ユーザ数、および使用するサーバ ハードウェアに依存します。Cisco Unified Presence クラスタの各サーバには、同様のハードウェアを使用することをお勧めします。設定と配置手順の詳細については、次の Web サイトで入手可能な『*Cisco Unified Presence Deployment Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

高可用性用の Cisco Unified Presence クラスタには、サブクラスタごとに 2 つのサーバが必要です。これにより、ユーザはサブクラスタ内のサーバ間でフェールオーバーを実行できますが、サポートされる合計ユーザ数とフェールオーバー時間は、有効にする機能、連絡先リストの平均サイズ、およびサーバ上のトラフィック レートによって異なります。Cisco Unified Presence サブクラスタは、2 台のサーバ構成にすると、常に高可用性構成として動作します。高可用性は、アクティブ/スタンバイ モデルまたはアクティブ/アクティブ モデルを使用して配置することができます。これらのモードは、Sync Agent サービス パラメータの Assignment Mode によって制御されます。

Cisco Unified Presence でアクティブ/スタンバイ モード（User Assignment Mode を **None** に設定）を実現するには、手動により、ユーザをサブクラスタの 1 番目のサーバに割り当て、2 番目のサーバにはユーザを 1 人も割り当てないが、すべての処理を同期させ、サブクラスタの 1 番目のサーバに障害が発生した場合のフェールオーバーに備えます。たとえば、図 22-7 では、最初のユーザをサーバ 1A、2 番目のユーザをサーバ 2A、3 番目のユーザをサーバ 3A、4 番目のユーザをサーバ 1A、5 番目のユーザをサーバ 2A、6 番目のユーザをサーバ 3A、というように割り当てています。これにより、ユーザはすべて、クラスタの「A」サーバに均等に割り当てられます。

Cisco Unified Presence のアクティブ/アクティブ モード(User Assignment Mode を **balanced** に設定)では、自動的にユーザがクラスタ内のすべてのサーバに均等に割り当てられます。各サーバは同期され、クラスタ内の他のサーバの障害時には、フェールオーバーが可能です。たとえば、図 22-7 では、最初のユーザをサーバ 1A、2 番目のユーザをサーバ 2A、3 番目のユーザをサーバ 3A、4 番目のユーザをサーバ 1B、5 番目のユーザをサーバ 2B、6 番目のユーザをサーバ 3B、というように割り当てます。ユーザは、クラスタ内のすべてのサーバに均等に割り当てられます。

User Assignment Mode を balanced に設定した Cisco Unified Presence のアクティブ/アクティブ配置では、使用される機能、ユーザの連絡先リストのサイズ、および生成されるトラフィック（ユーザ データ プロファイル）に応じた柔軟な冗長構成が可能です。Cisco Unified Presence の完全な冗長性モードのアクティブ/アクティブ配置では、機能に関係なく、サポートされる合計ユーザ数を半分にする必要があります（たとえば、Cisco MCS 7845 をバランス型の高可用性冗長構成で配置する場合、1 つのサブクラスタでサポートされるユーザ数は、最大 5000 人になります）。Cisco Unified Presence の非冗長モードのアクティブ/アクティブ配置では、使用される機能、ユーザの連絡先リストの平均サイズ、および生成されるトラフィックをさらに詳細に検討する必要があります。たとえば、プレゼンスとインスタント メッセージングを有効にし、カレンダーとモビリティ統合を無効にした配置で、連絡先リストが平均 30 ユーザ、ユーザ データ プロファイルが少数のプレゼンスとインスタント メッセージングの更新の場合、サブクラスタあたり 5000 以上のユーザをサポートできます（Cisco MCS 7845 の場合）。

高可用性構成でない Cisco Unified Presence クラスタ配置の場合、サブクラスタの各サーバは、最大数までユーザをサポートできます。サーバを 1 つだけ置いたサブクラスタを配置した後、2 番目のサーバを追加する前に最大 3 つのサブクラスタを作成することをお勧めします。サブクラスタに 2 番目のサーバを追加した後でも、サブクラスタは高可用性配置と同様に動作しますが、オンライン サーバが容量の上限（有効な Cisco Unified Presence 機能、ユーザの連絡先リストのサイズ、およびユーザによって生成されるトラフィック量に基づく）に達すると、サーバに障害が発生した場合にフェールオーバーできないことがあります。

Cisco Unified Presence の配置例

例 22-1　単一の Unified CM クラスタ、Cisco Unified Presence を使用せず

配置要件

- 4,000 ユーザから 13,000 ユーザまで拡張可能
- 単一の Cisco Unified Communications Manager クラスタ
- 高可用性は不要

ハードウェア：

- Cisco MCS 7845 サーバ

配置：

- 3 つの単一サーバのサブクラスタ、User Assignment Mode = balanced に設定

例 22-2　2 つの Unified CM クラスタ、Cisco Unified Presence を使用せず

配置要件

- 11,000 ユーザから 24,000 ユーザまで拡張可能
- 2 つの Cisco Unified Communications Manager クラスタ
- 高可用性は不要

ハードウェア：

- Cisco MCS 7845 サーバ

配置：

- 2 つの Cisco Unified Presence クラスタ（各 Cisco Unified Communications Manager クラスタに 1 つずつ）、各クラスタに 3 つのサブクラスタ、各サブクラスタに 1 つずつサーバがあり、すべて User Assignment Mode = balanced に設定

例 22-3　単一の Unified CM クラスタで Cisco Unified Presence を使用

配置要件

- 500 ユーザから 2,500 ユーザまで拡張可能
- 単一の Cisco Unified Communications Manager クラスタ
- 高可用性が必須

ハードウェア：

- Cisco MCS 7835 サーバ

配置：

- 1 つの 2 サーバのサブクラスタ、User Assignment Mode = balanced に設定

例 22-4　単一の Unified CMBE クラスタと Cisco Unified Presence

配置要件

- 100 ユーザから 500 ユーザまで拡張可能
- 単一の Cisco Unified Communications Manager Business Edition（Unified CMBE）
- 高可用性が必須

ハードウェア：

- Cisco MCS 7825 サーバ

配置：

- 1 つの 2 サーバのサブクラスタ、User Assignment Mode = balanced に設定

例 22-5　複数の Unified CM Clusters で Cisco Unified Presence を使用

配置要件

- 5,000 ユーザから 40,000 ユーザまで拡張可能
- 複数の Cisco Unified Communications Manager クラスタ
- 高可用性が必須

ハードウェア：

- Cisco MCS 7845 サーバ

配置：

- 複数の Cisco Unified Presence クラスタ構成では、すべてのクラスタ間にクラスタ ピアをセットアップする必要があります。まず各 Cisco Unified Presence クラスタに、最大 5,000 ユーザに対応する 2 サーバのサブクラスタを 1 つ構築した後、既存の Cisco Unified Presence クラスタにサブクラスタを追加します。単一の Cisco Unified Presence クラスタが多数のユーザに対応する場合、使用する User Assignment Mode サービス パラメータは、通常、システム管理者によって指示されます。サブクラスタごとに 1 つのサーバをモニタする場合は、アクティブ/スタンバイ モードが適切です。ユーザを均等に分散する場合は、アクティブ/アクティブ モードが適切です。

Cisco Unified Presence サーバのパフォーマンス

Cisco Unified Presence サーバ クラスタは、シングル サーバとマルチサーバの両方の構成をサポートします。ただし、複数のサーバを使用する場合、各サーバは、パブリッシャ サーバと同じタイプのサーバ プラットフォームを使用する必要があります。

表 22-4 は、Cisco Unified Presence サーバのハードウェア プラットフォーム要件と、プラットフォームごとにサポートされる最大ユーザ数を示します（たとえば、Cisco Unified Presence クラスタを 3 台の Cisco MCS 7845 サーバによって配置し、それぞれのサーバが独自のサブクラスタを構成する場合、合計 15,000 ユーザがサポートされます）。

表 22-4　Cisco Unified Presence サーバ プラットフォームとサポートされるユーザ数

サーバ プラットフォーム	プラットフォームごとにサポートされるユーザ数
Cisco MCS 7816	500
Cisco MCS 7825	1000
Cisco MCS 7835	2500
Cisco MCS 7845	5000

ハードウェア仕様の詳細については、次の Web サイトで入手可能な Media Convergence Server の資料を参照してください。

http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_models_home.html

Cisco Unified Presence のライセンス

ユーザ プレゼンス機能は、Unified CM Administration で、Licensing Capabilities Assignment を使用して割り当てます。ユーザは Unified CM からプレゼンス機能をライセンスされるので、Cisco Unified Presence を Cisco Unified CM と統合する必要があります。

チェックボックスは、Unified Presence 用と Unified Personal Communicator 用に 1 つずつ用意されています。ユーザがプレゼンス SIP メッセージの更新を送受信できるようにするには、そのユーザに対して Unified Presence のチェックボックスをオンにする必要があります。そうでない場合は、そのユーザに関するプレゼンス メッセージやステータスの更新が許可されません。Cisco Unified Personal Communicator を使用できるようにするには、そのユーザに対して Unified Personal Communicator のチェックボックスをオンにする必要があります。

ユーザに対して、チェックボックス（Enable CUP および Enable CUPC）を 1 つオンにするごとに、デバイス ライセンスユニットが 1 つ消費されます。消費されているデバイス ライセンス ユニット数（つまり、プレゼンスが有効なユーザ数）のレポートを表示するには、Unified CM で License Unit Calculator を使用します。Unified CM のライセンスの詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

http://www.cisco.com

Unified CM は、複数のデバイスを使用するプレゼンス ユーザに対して、付加ライセンスを使用できる機能を提供します。この機能により、すでに Cisco Unified IP Phone を使用しているプレゼンス ユーザは、Cisco Unified Personal Communicator をあわせて使用する場合も、3 デバイス ライセンス ユニットではなく 1 デバイス ライセンス ユニットで済みます。付加ライセンスを有効にするには、Unified CM で Cisco Unified Personal Communicator の Primary Phone オプションを使用します。プライマリ Phone が Cisco Unified Personal Communicator に関連付けられている場合、付加ライセンスが有効になり、ライセンス ユニット計算に反映されます。

Cisco Unified Presence の配置

Cisco Unified Presence は、次のいずれかの構成で配置できます。

- 「シングルクラスタ配置」（P.22-19）
- 「マルチクラスタ配置」（P.22-21）
- 「WAN を介したクラスタ化」（P.22-23）
- 「フェデレーション配置」（P.22-24）

シングルクラスタ配置

図 22-9 は、Cisco Unified Presence コンポーネント間のインターフェイスと、基本機能におけるそれらのコンポーネント間での対話を示します。Cisco Unified Presence の管理と設定の詳細については、次の Web サイトで入手可能な Cisco Unified Presence のインストール、管理、設定の各ガイドを参照してください。

http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

図 22-9　Cisco Unified Presence コンポーネント間の対話

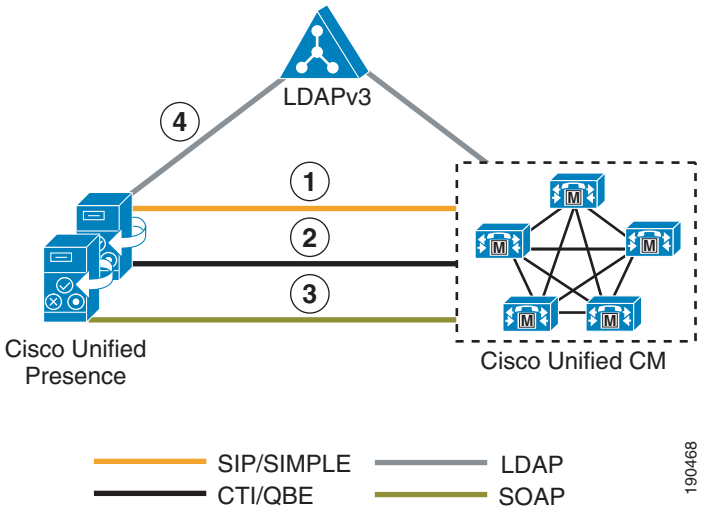


図 22-9 は、Cisco Unified Presence コンポーネント間の次の対話を示します。

1. Cisco Unified Presence サーバと Unified CM 間の SIP 接続は、すべての電話機の状態のプレゼンス情報の交換を処理します。

   a. Unified CM の設定では、Cisco Unified Presence サーバをアプリケーション サーバとして Unified CM に追加する必要があります。また SIP トランクが Cisco Unified Presence サーバを指す必要があります。SIP トランクに設定するアドレスは、Cisco Unified Presence サーバに対して解決される Domain Name System（DNS; ドメイン ネーム システム）サーバ（SRV）の完全修飾ドメイン名（QDN）、または個別の Cisco Unified Presence サーバの IP アドレスです。Cisco Unified Presence 7.0(3) 以降のリリースは、管理者が Cisco Unified Presence の管理ページからシステム トポロジ ページにノードを追加すると、Cisco Unified Communications Manager アプリケーション サーバ エントリの設定を AXL/SOAP で自動的に処理します。

   b. Cisco Unified Presence の設定は、Unified CM Presence Gateway で行われ、Unified CM とプレゼンス情報が交換されます。設定されるのは次の情報です。

      Presence Gateway: *server_fqdn*:5070

      （注）　*server_fqdn* は、Unified CM パブリッシャの FQDN、Unified CM サブスクライバ サーバに解決される DNS SRV FQDN、または IP アドレスです。

ネットワーク内の DNS の可用性が非常に高く、DNS SRV の利用が可能な場合、Cisco Unified Presence パブリッシャとサブスクライバの DNS SRV FQDN を使用して、Unified CM 上に SIP トランクを設定します。また、Unified CM サブスクライバの DNS SRV FQDN を同等の重み付けで使用し、Cisco Unified Presence サーバ上に Presence Gateway を設定します。この設定により、プレゼンス情報の交換に使用するすべてのサーバ間でプレゼンス メッセージングが均等に振り分けられます。

DNS が高可用性でない場合、またはネットワーク内で信頼できるオプションでない場合は、IP アドレスを使用する。IP アドレスを使用すると、単一のサブスクライバが指されるので、プレゼンス メッセージング トラフィックを複数の Unified CM サブスクライバ間で均等に振り分けることはできません。

Unified CM では、PUBLISH メソッド（SUBSCRIBE/NOTIFY ではなく）を設定し、Cisco Unified Presence への SIP トランク インターフェイス上で使用できるようにする CUP PUBLISH Trunk というサービス パラメータによって、通信をさらに簡素化し、使用帯域幅を削減します。CUP PUBLISH Trunk サービス パラメータを有効にした場合、ユーザをプライマリ内線だけでなく、ライン アピアランスと関連付ける必要があります。

2. Cisco Unified Presence と Unified CM の間の Computer Telephony Integration Quick Buffer Encoding（CTI-QBE）接続は、Cisco Unified Presence サーバ上のユーザのすべての CTI 通信を処理して、Unified CM 上の電話機を制御します。この CTI 通信は、Cisco Unified Personal Communicator が Desk Phone モードで Click to Call を行う場合、または Microsoft Office Communicator が Microsoft Live Communications Server 2005 または Office Communications Server 2007 によって Click to Call を行う場合に実行されます。

   a. Unified CM の設定では、ユーザを CTI Enabled グループに関連付け、そのユーザに割り当てられたプライマリ内線で CTI 制御を有効にする必要があります（Directory Number ページのチェックボックス）。CTI Manager Service もまた、Cisco Unified Presence パブリッシャおよびサブスクライバとの通信に使用される各 Unified CM サブスクライバ上でアクティブにする必要があります。Microsoft Live Communications Server 2005 または Office Communications Server 2007 との統合には、Unified CM で、CTI Enabled グループと役割を使用して、アプリケーション ユーザを設定する必要があります。

   b. Cisco Unified Personal Communicator と連携して使用するための Cisco Unified Presence の CTI 設定（CTI サーバおよびプロファイル）は、Unified CM とのデータベースの同期時に自動的に作成されます。すべての Cisco Unified Personal Communicator CTI 通信は、Cisco Unified Presence サーバ経由ではなく、直接 Unified CM で実行されます。

      Microsoft Live Communications Server 2005 または Office Communications Server 2007 と連携して使用するための Cisco Unified Presence の CTI 設定（CTI ゲートウェイ）では、CTI ゲートウェイ アドレス（Cisco Unified Communications Manager アドレス）とプロバイダー（Unified CM で設定されたアプリケーション ユーザ）を設定する必要があります。スケーラビリティを拡大させるため、最大 8 個の Cisco Unified Communications Manager アドレスをプロビジョンすることができます。Cisco Unified Presence サーバ の CTI ゲートウェイ設定で使用できるのは、IP アドレスのみです。

3. AXL/SOAP インターフェイスは、Unified CM からのデータベースの同期を処理して、Cisco Unified Presence データベースにデータを入力します。

   a. Unified CM では、その他の設定は必要ありません。

   b. Cisco Unified Presence セキュリティ設定では、AXL 設定内の Unified CM AXL アカウントのユーザとパスワードを設定する必要があります。

      Sync Agent サービス パラメータである User Assignment をデフォルトの [balanced] に設定すると、Cisco Unified Presence クラスタ内のすべてのサーバに対して、すべてのユーザが均等にロードバランスされます。管理者は、User Assignment サービス パラメータを [None] に変更して、Cisco Unified Presence クラスタ内の特定のサーバに手動でユーザを割り当てられます。

4. LDAP インターフェイスは、ログイン時に、Cisco Unified Personal Communicator ユーザの LDAP 認証に使用します。LDAP 同期と認証の詳細については、「LDAP ディレクトリ統合」（P.17-1）の章を参照してください。

   Unified CM は、手動設定によるすべてのユーザ エントリまたは LDAP からの直接の同期を処理し、Cisco Unified Presence がすべてのユーザ情報を Unified CM から同期させます。Cisco Unified Personal Communicator ユーザが Cisco Unified Presence サーバにログインし、

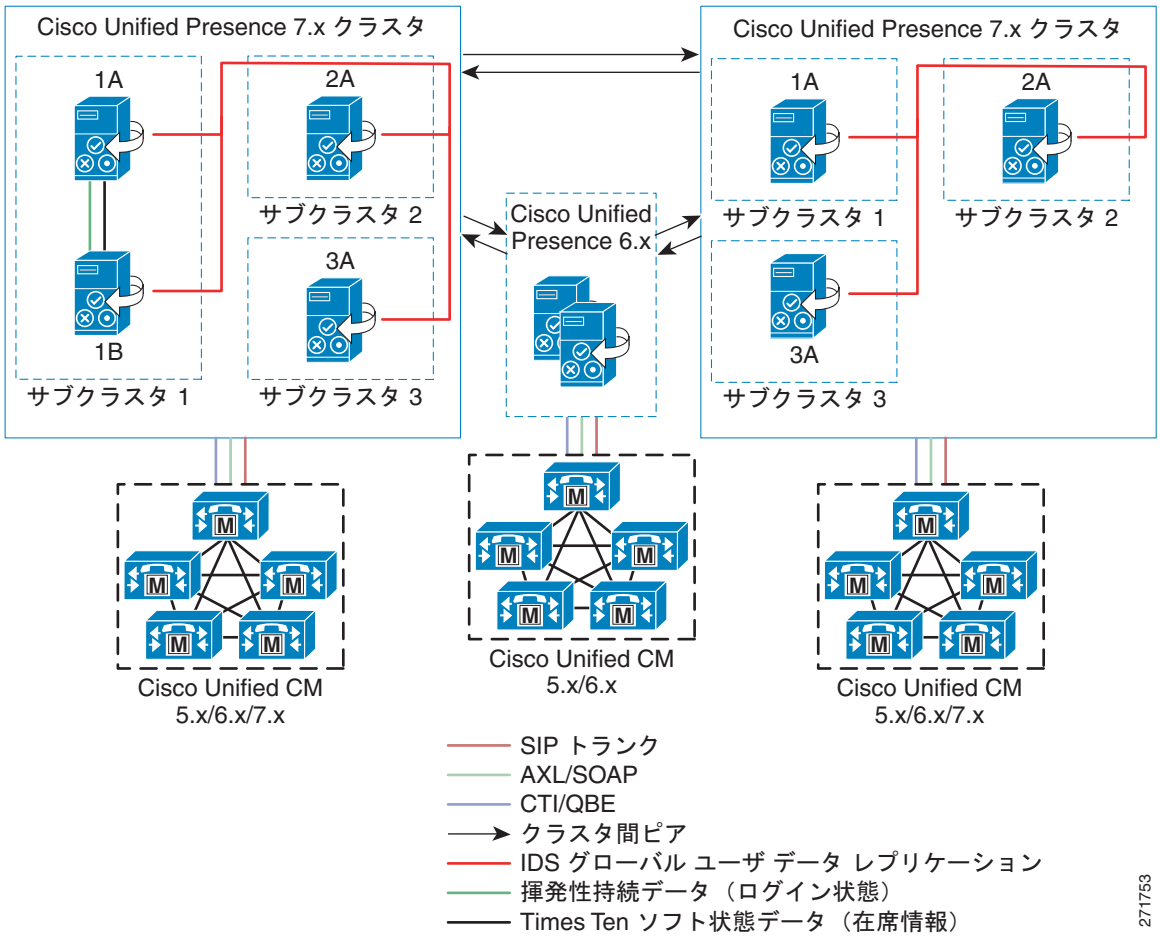
Unified CM で LDAP 認証が有効な場合、Cisco Unified Presence は直接 LDAP に移動し、Bind 操作によって Cisco Unified Personal Communicator ユーザを認証します。Cisco Unified Personal Communicator の認証が完了すると、Cisco Unified Presence は情報を Cisco Unified Personal Communicator に転送してログインを続行します。

Microsoft Active Directory を使用する場合は、パラメータの選択を慎重に考慮してください。大規模な Active Directory 実装が存在し、設定で Domain Controller が使用されている場合、Cisco Unified Presence で十分なパフォーマンスが得られないことがあります。Active Directory の応答時間を改善するために、場合によっては、ドメイン コントローラをグローバル カタログに強化し、LDAP ポートを 3268 に設定する必要があります。

マルチクラスタ配置

前の節まででは、単一の Cisco Unified Presence クラスタが、単一の Unified CM クラスタと通信する配置トポロジについて説明しました。しかし単一のクラスタ内だけの通信では、プレゼンスやインスタント メッセージングの機能には限りがあります。そこで、プレゼンスとインスタント メッセージングの能力と機能を拡張できるよう、これらのスタンドアロンのクラスタにピア関係を設定することで、同じドメイン内の複数のクラスタ間で通信できるようになります。図 22-10 は、複数のクラスタやサイトを相互接続した場合の Cisco Unified Presence クラスタ間のピア関係を示します。この機能により、1 つのクラスタ内のユーザが、同じドメイン内の異なるクラスタにいるユーザと通信したり、プレゼンスをサブスクライブしたりすることができます。

図 22-10　Cisco Unified Presence の Multi-Cluster 配置



フルメッシュのプレゼンス トポロジを作成するには、それぞれの Cisco Unified Presence クラスタと、同じドメイン内の個々の Cisco Unified Presence クラスタとの間に、個別のピア関係が設定されている必要があります。このクラスタ間ピアに設定されているアドレスは、リモートの Cisco Unified Presence クラスタ サーバに対して解決される DNS SRV FQDN、または単純に Cisco Unified Presence クラスタ サーバの IP アドレスです。

各 Cisco Unified Presence クラスタ間のインターフェイスには、AXL/SOAP インターフェイスと SIP インターフェイスの 2 つが使用されます。AXL/SOAP インターフェイスは、ホーム クラスタ アソシエーションのためにユーザ情報の同期を処理しますが、これは完全なユーザ同期ではありません。SIP インターフェイスは、サブスクリプション トラフィックと通知トラフィックを処理し、同じドメイン内のリモート Cisco Unified Presence クラスタでユーザが検出された場合、SIP インターフェイスが SIP URI のホスト部分を書き換えた後にユーザを転送します。

Cisco Unified Presence のマルチクラスタ配置を容易にするため、Cisco Unified Presence クラスタ内のすべてのユーザを単一のサブクラスタ上に設定できるように、各 Cisco Unified Presence クラスタのサイジングを行うことを推奨します。また、Cisco Unified Presence クラスタで、サーバのバックエンド サブスクリプション トラフィックが増加しないように、decomposed list のサービス パラメータを有効にすることをお勧めします。

Cisco Unified Presence をマルチクラスタ環境に配置する場合、プレゼンス ユーザ プロファイルを決定する必要があります。プレゼンス ユーザ プロファイルは、マルチクラスタ プレゼンス配置の規模とパフォーマンスおよびサポート可能なユーザ数の決定に役立ちます。プレゼンス ユーザ プロファイルによって、一般的なユーザの連絡先（バディ）の数、およびそれらの連絡先の多くがローカル クラスタのユーザか、リモート クラスタのユーザかが確定します。

Cisco Unified Presence クラスタ間で生成されるトラフィックは、プレゼンス ユーザ プロファイルの特徴に直接比例します。たとえば、プレゼンス ユーザ プロファイル A は、30 個の連絡先を持ち、その 20% がローカルの Cisco Unified Presence クラスタのユーザで、80% がリモートの Cisco Unified Presence クラスタのユーザだとします。またプレゼンス ユーザ プロファイル B は、30 個の連絡先を持ち、その 50% がローカルの Cisco Unified Presence クラスタのユーザで、50% がリモートの Cisco Unified Presence クラスタのユーザだとします。この場合、プレゼンス ユーザ プロファイル B は、リモート クラスタ トラフィック量が小さいので、ネットワーク パフォーマンスが若干高く、帯域幅利用率が小さくなります。

WAN を介したクラスタ化

Cisco Unified Presence クラスタは、Wide Area Network（WAN; ワイド エリア ネットワーク）をはさんで配置されたサブクラスタのノードの 1 つを使用して配置できます。これにより、サイトをまたがるノード間でサブクラスタの地理的冗長性とユーザの高可用性が実現します。次のガイドラインは、Cisco Unified Presence の配置と WAN を介したクラスタ化のプランニング時に使用する必要があります。

- データセンターの地理的冗長性とリモート フェールオーバー

  Cisco Unified Presence クラスタは、単一サブクラスタ トポロジで 2 つのサイトの間に配置できます。このトポロジでは、サブクラスタの一方のサーバが 1 つの地理的サイトに置かれ、サブクラスタの他方のサーバが別のサイトに置かれます。残りのサブクラスタ（これらのサブクラスタ内のノード）はすべて、Cisco Unified Presence パブリッシャと共存したままにする必要があります。この配置では、5 Mbps 以上の帯域幅を確保し、遅延を 80 ms ラウンド トリップ時間（RTT）以下に抑え、TCP によるメソッド イベント ルーティングを行う必要があります。

- 高可用性と規模

  Cisco Unified Presence の高可用性により、サブクラスタ内の 1 つのノードのユーザは、サブクラスタ内の別のノードに自動的にフェールオーバーされます。最大 2 つのノードで構成される Cisco Unified Presence サブクラスタでは、リモート フェールオーバーは基本的に 2 つのサイト間（ノードごとに 1 つのサイト）で行われます。スケーラブルな高可用性の Cisco Unified Presence クラスタは、最大 3 つのサブクラスタによる構成が可能です。したがって、スケーラブルな高可用性のリモート フェールオーバー トポロジは、次のような 2 つのサイトで構成されます。

  - サイト A : サブクラスタ 1 ノード A、サブクラスタ 2 ノード A、およびサブクラスタ 3 ノード A
  - サイト B : サブクラスタ 1 ノード B、サブクラスタ 2 ノード B、およびサブクラスタ 3 ノード B

  この配置では、サブクラスタごとに 5 Mbps 以上の帯域幅を確保し、遅延を 80 ms ラウンド トリップ時間（RTT）以下に抑え、TCP によるメソッド イベント ルーティングを行う必要があります。この配置に追加される新しい各サブクラスタは、データベースと状態の複製を処理するために、さらに 5 Mbps の専用帯域幅が必要です。

- ローカル フェールオーバー

  2 つのサイト間の Cisco Unified Presence クラスタ 配置では、サイトごとに 1 つのサブクラスタ トポロジ（単一ノードまたは高可用性構成のデュアル ノード）を構成することもできます。この場合、一方のサブクラスタを 1 つの地理的サイトに置き、他方のサブクラスタを別の地理的サイトに置きます。このトポロジにより、ユーザは、異なるサイトまたは場所にフェールオーバーする必要なしに、（高可用性または高可用性でない）ローカル サイトに残ることができます。この配置で

は、それぞれのサイトの各サブクラスタ間に 5 Mbps 以上の専用帯域幅を確保し、遅延を 80 ms ラウンド トリップ時間（RTT）以下に抑え、TCP によるメソッド イベント ルーティングを行う必要があります。

- 帯域幅と遅延に関する考慮事項

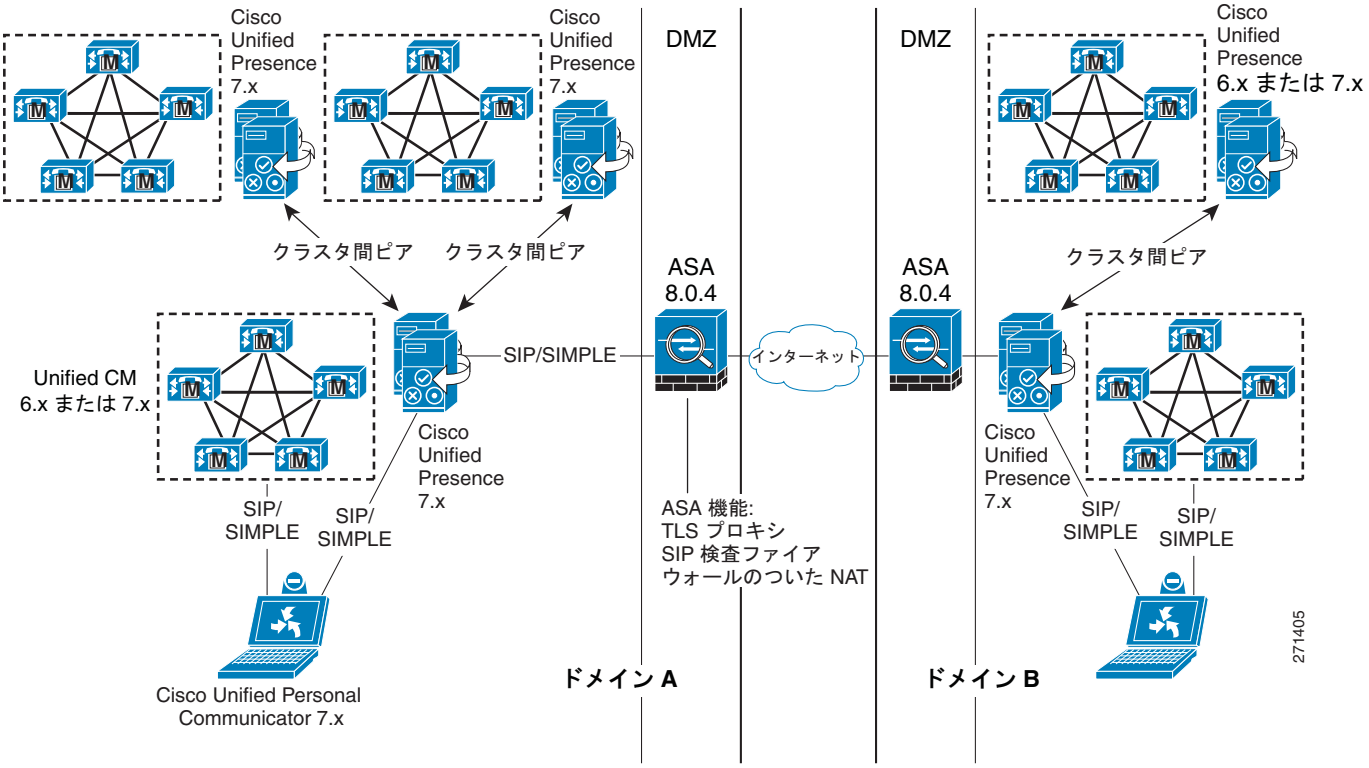
  WAN をはさんでノードが分割されたトポロジを持つ Cisco Unified Presence クラスタでは、ユーザのクライアント内の連絡先数が、帯域幅の要件や配置の基準に影響を及ぼす可能性があります。Cisco Unified Presence クラスタ内およびクラスタ間で生成されるトラフィックは、プレゼンス ユーザ プロファイルの特性、ひいては配置に必要な帯域幅に正比例します。帯域幅が狭い（10 Mbps 以下）環境のクライアントでは、リモート連絡先を 25% 以下にすることをお勧めします。最大ラウンドトリップ遅延は、常に 80 ms 以下にする必要があります。

フェデレーション配置

Cisco Unified Presence は企業間通信に対応するため、異なるドメイン間でプレゼンス情報やインスタント メッセージング通信を共有するドメイン間フェデレーションを搭載しています。ドメイン間フェデレーションの構築には、2 つの明示的な DNS ドメインを設定し、さらに DMZ にセキュリティ アプライアンス（Cisco Adaptive Security Appliance）を置いて、フェデレーション接続を企業で終端させる必要があります。

図 22-11 は、ドメイン A とドメイン B という 2 つの異なるドメインの間の、基本的なドメイン間フェデレーション配置を示します。DMZ の Adaptive Security Appliance（ASA）は、TLS プロキシと ASA バージョン 8.0.4 で導入された SIP 検査機能によって TLS 接続を終端するために使用されています。ASA から受信するすべての着信フェデレーション トラフィックは、単一の Cisco Unified Presence クラスタ経由でルーティングされ、クラスタ間ピアリングによってドメイン内の適切なホーム クラスタに伝達されます。すべての発信トラフィックは、Cisco Unified Presence クラスタから送信され、ASA 経由でフェデレーション リンクを介して伝達されます。

図 22-11　ドメイン間フェデレーション



ドメイン間フェデレーション設定では、図 22-12 に示すように、Cisco Unified Presence と Microsoft Office Communications Server（OCS）の間の特定のフェデレーションも可能です。Cisco Unified Presence は、Microsoft Office Communications Server（OCS）または Live Communications Server（LCS）とのドメイン間フェデレーションによって、基本プレゼンス（応対可能、不在、ビジー、オフライン）とポイントツーポイントのインスタント メッセージングを提供します。高度なプレゼンス機能（通話中、会議中、休暇中など）や高度なインスタント メッセージング機能はサポートされていません。

図 22-12　Microsoft Office Communications Server とのフェデレーション

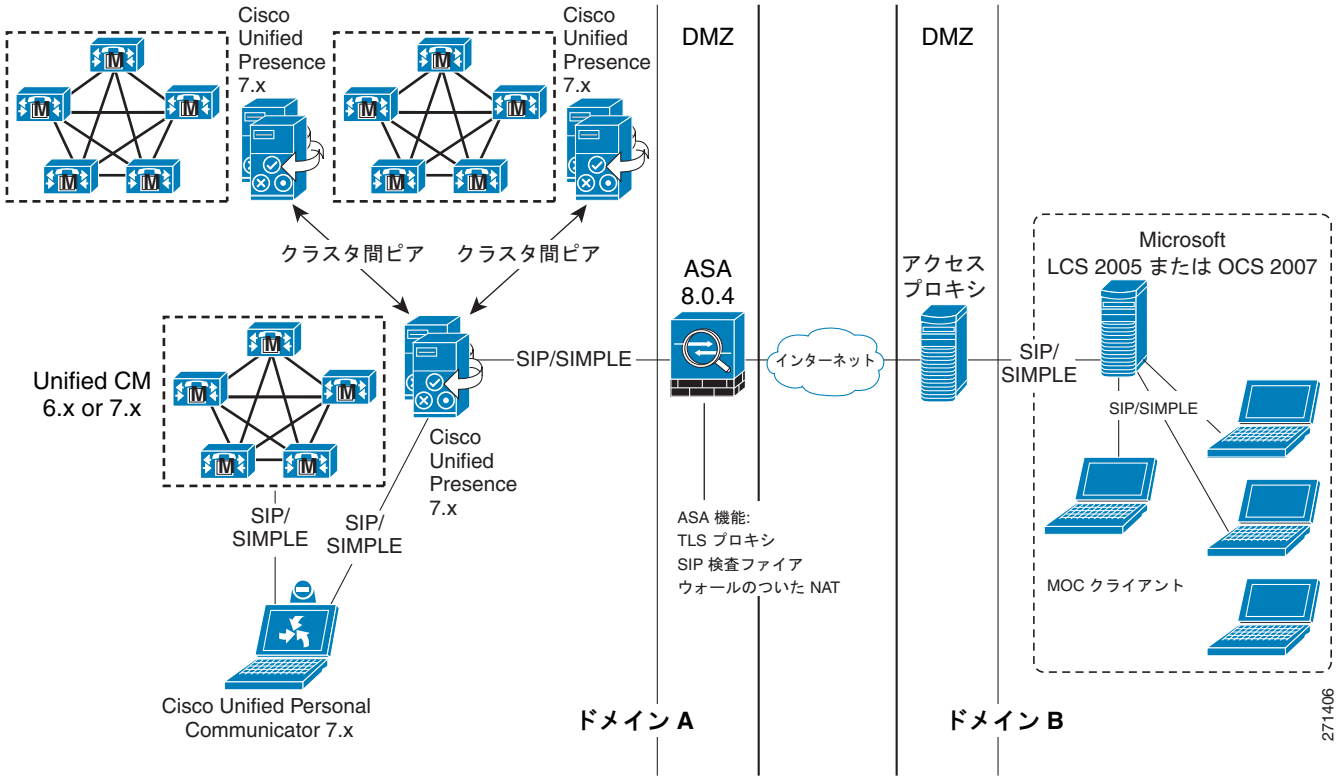


表 22-5 は、Cisco Unified Presence と Microsoft Office Communications Server の間の状態のマッピングを示します。

表 22-5　プレゼンス ステータスのマッピング

シスコでのステータス	シスコのランプの色	Microsoft Office Communications Server でのステータス
不在	赤	退席中
割込不可	赤	取り込み中
取り込み中	赤	取り込み中
電話中	黄色	取り込み中
会議中	黄色	取り込み中
退席中	黄色	退席中
応対可能	緑	応対可能
応対不可 / オフライン	グレー	オフライン

（注）　Cisco Unified Presence は、他のドメインが、DNS SRV によって Cisco Unified Presence サーバを検出できるように、ドメインに関する DNS SRV レコードをパブリッシュする必要があります。Microsoft Office Communications Server または Live Communications Server 配置では、Cisco Unified Presence が Access Edge サーバ上の Public IM Provider として設定されているので、このようなパブリッシュが必要です。Cisco Unified Presence サーバが DNS SRV を使用している Microsoft ドメインを検出できない場合、Cisco Unified Presence で外部ドメインの静的ルートを設定する必要があります。

Cisco Unified Presence のフェデレーション配置は、Adaptive Security Appliance と Cisco Unified Presence サーバ間にロード バランサを使用することで、冗長性のある構成にすることができます。または、冗長構成の Adaptive Security Appliance によって冗長性を実現することもできます。

フェデレーション配置に関するその他の設定と配置上の考慮事項については、次の Web サイトで入手可能な『*Integration Guide for Configuring Cisco Unified Presence Release 7.0 for Inter-Domain Federation*』を参照してください。

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

Cisco Unified Presence サーバのポリシー

Cisco Unified Presence サーバのポリシーは、管理者ではなく、ユーザが設定します。ユーザがポリシー ルールに変更を加えなければ、すべてがオープンで利用可能なデフォルトのルールが適用されます。すべてのポリシー設定は、https://<*cup_server_address*>/ccmuser/ の Cisco Unified Presence ユーザ ページにある User Options 領域で制御できます。

ユーザは、これらのルールが適用されるウォッチャのアクセス コントロール リスト（ACL）が入ったルール セットを設定できます。各ルール セットには、次の 3 種類のルールがあります。

- 表示ルール
  - ブロック：ウォッチャに対して応対不可のプレゼンス ステータスが表示され、ユーザのデバイス ステータスは表示されません。
  - Reachability Only：ウォッチャに対して全体のプレゼンスだけが表示され、デバイスの詳細情報は表示されません。
  - すべての状態（デフォルト）：ウォッチャに対して全体のプレゼンスに加え、フィルタリングされていないデバイス ステータス情報がすべて表示されます。
- プレゼンス ルール
  - 優先順位ベールのルール（最初に一致した項目）に従ってプレゼンス（away、available、busy、unavailable、do not disturb、unknown）が表示されます。
  - デバイス タイプ、メディア タイプ、カレンダー ベースのルール（たとえば、携帯電話が busy またはカレンダーが busy の場合は、全体のプレゼンスを busy とする。インスタント メッセージング デバイスのいずれかが do-not-disturb の場合、全体のプレゼンスを do-not-disturb とする）。
- フィルタリング ルール
  - 特定のデバイス タイプ、メディア タイプ、またはカレンダーのプレゼンス ステータスを除外します。

フィルタリング ルールはプレゼンスの判定に先立って適用されるので、フィルタリングされたデバイスのステータスが、ユーザのプレゼンス ステータスに影響を与えることはありません。ユーザはまた、プレゼンス ルールとフィルタリング ルールに使用するデバイス タイプ（たとえば、携帯電話、オフィスの電話など）を定義できます。

Cisco Unified Presence のカレンダー統合

Cisco Unified Presence は、Microsoft Exchange 2003 または 2007 のカレンダー モジュール インターフェイスを使用してカレンダー ステータスを取得し、それをプレゼンス ステータスに集約することができます。Microsoft Exchange の統合は、Microsoft Active Directory 2003 および Active Directory 2008 と Windows Server 2003 および Windows Server 2008 でサポートされます。Microsoft Exchange は、WebDAV プロトコル（RFC 2518）の拡張である Outlook Web Access（OWA）経由でカレンダー データを提供します。Microsoft Exchange との統合は、カレンダー アプリケーション用の別のプレゼンス ゲートウェイによって実現されます。管理者が Outlook 対応のプレゼンス ゲートウェイを設定すると、ユーザは自分のプレゼンス ステータスをカレンダー情報に集約するかどうかを切り替えられるようになります（表 22-6 を参照）。

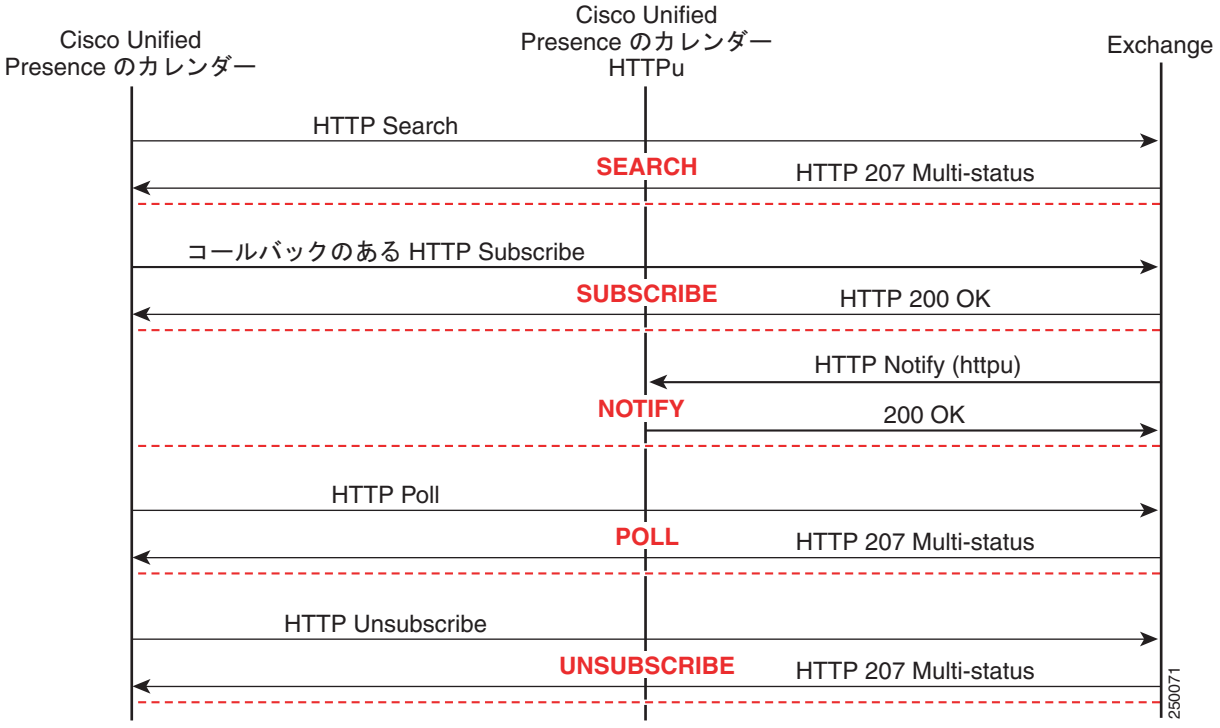
表 22-6　カレンダー ステータスと集約されたプレゼンス ステータス

Cisco Unified Presence のステータス	カレンダー ステータス
応対可能	空き時間 / 仮承諾
アイドル / ビジー	取り込み中
退席中	Out of office

カレンダー情報の取得に使用される交換 ID は、そのユーザの LDAP 構造の電子メール ID から取得されます。電子メール ID が存在しない場合、または LDAP が使用されていない場合は、Cisco Unified Presence のユーザ ID が交換 ID としてマッピングされます。

Cisco Unified Presence サーバから Microsoft Exchange Server へのカレンダー ステータスに関するサブスクリプションによって、情報が収集されます。図 22-13 は、このやり取りを示します。

図 22-13　Cisco Unified Presence と Microsoft Exchange の間の通信



この機能を使用するには、UDP HTTP（HTTPu）監視ポートのポート アドレスを新しいサービス パラメータとして使用する必要があります。このポートは、Microsoft Exchange が、カレンダー イベントの特定のサブスクリプション識別情報に対する変更を示す通知（NOTIFY によって示される）を送信するポートです。

SEARCH トランザクションは、一定の期間についてユーザのカレンダーを検索します。このトランザクションは、ユーザが、カレンダー情報をプレゼンス ステータスに含めるようにプレゼンスを設定した場合に呼び出されます。検索結果は、空き時間 / ビジー トランザクションのリストに変換されます。SUBSCRIBE メッセージは、フォルダ /exchange/user*X*/Calendar で、ユーザの空き時間 / ビジー状態に関する変更が生じた場合に通知を求めるサブスクリプションを示します。POLL メソッドは、クライアントが特定のイベントを受信したこと、またはそれに対して応答したことを確認します。UNSUBSCRIBE メッセージは、それまでの 1 つ以上のサブスクリプションを終了します。

（注）　Cisco Unified Presence は、単一のまたは複数の Microsoft Exchange Server を使用して配置できます。Microsoft Exchange 配置では、複数の Exchange Server で構成されるクラスタが使用できるので、Cisco Unified Presence は、Cisco Unified Presence がステータスを要求するユーザをホストしている Exchange Server への REDIRECT メッセージを受け入れます。

多言語カレンダーのサポート

カレンダー統合配置の要件で複数の言語を指定する場合は、次の設計ガイドラインに従ってください。

- Cisco Unified Presence には、Cisco Unified Communications Manager と同様に、ユーザが必要なロケールを選択できるように適切なロケールがインストールされている必要があります。
- Cisco Unified Presence は、カレンダー統合用に Unified Communications の標準ロケールをすべてサポートしています。
- エンド ユーザ用ページ、または管理用の Bulk Administration Tool によって、ユーザに目的のロケールが設定される必要があります。
- Presence Gateway のタイプ Outlook は、Microsoft Exchange に設定する必要があります。Cisco Unified Presence は、最初の照会とともに適切なロケール フォルダを送信します。照会は必要に応じて、フロントエンドまたはクライアント アクセス用 Microsoft Exchange Server の最初の応答によってリダイレクトされます。
- IP Phone Messenger および会議通知機能を使用する場合は、ユーザのロケールを、電話機の IP Phone Messenger サービスが使用されているロケールと同じに設定する必要があります。

Cisco Unified Presence のモビリティ統合

Cisco Unified Presence は、連絡先リストとプレゼンス ステータスを Cisco Unified Mobility Advantage と Cisco Unified Mobile Communicator と統合することができます。Cisco Unified Mobile Communicator は、引き続き Cisco Unified Mobility Advantage と直接通信を行いますが、Cisco Unified Mobility Advantage は、AXL/SOAP および SIP 経由で Cisco Unified Presence とやり取りします。

Cisco Unified Mobility Advantage が、Cisco Unified Presence との間で管理セッションを確立するには、その前に Cisco Unified Presence と Cisco Unified Mobility Advantage 上でアプリケーション ユーザを設定する必要があります。Cisco Unified Mobile Communicator のエンドユーザ ログインにより、Cisco Unified Presence に対してシステム設定、ユーザ設定、連絡先リスト、プレゼンス ルール、およびアプリケーション ダイヤル ルールを求める Cisco Unified Mobility Advantage SOAP 要求が生成されます。その後、Unified Communicator Change Notifier（UCCN）設定と Presence SIP サブスクリプションが実行されます。図 22-14 は、Cisco Unified Mobility Advantage と Cisco Unified Presence の間の対話を示します。

図 22-14　Cisco Unified Mobile Communicator のコール フロー

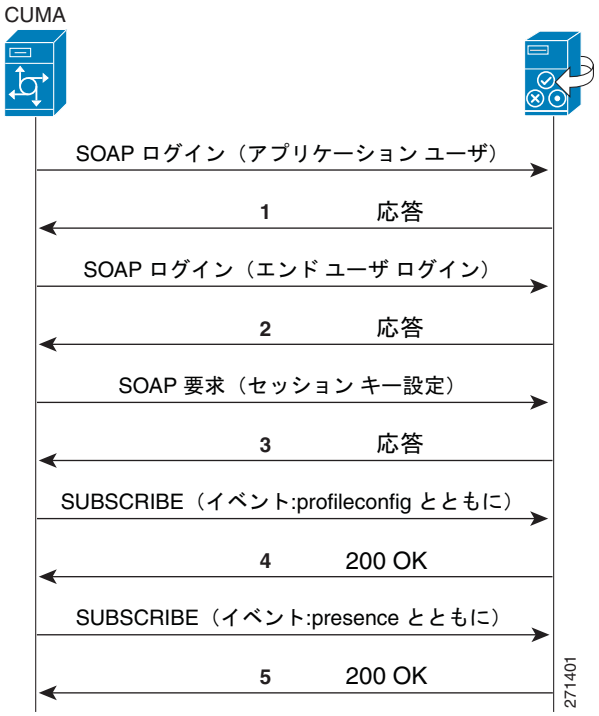


図 22-14 のコールフローは、次の一連のイベントを示しています。

1. Cisco Unified Mobility Advantage が、スーパーユーザ アプリケーション ユーザ（CCMAdministrator）経由で Cisco Unified Presence に対して SOAP ログイン要求を開始し、Cisco Unified Presence がセッション キーを返します。このアプリケーション ユーザは、Cisco Unified Presence と Cisco Unified Mobility Advantage の両方で作成しておく必要があります。
2. Cisco Unified Mobile Communicator エンドユーザがログインし、Cisco Unified Presence がセッション キーを返します。
3. Cisco Unified Mobility Advantage が、ユーザの代わりに（セッション キーを使用して）**get-all-config** SOAP 要求を開始し、システム設定、ユーザ設定、連絡先リスト、プレゼンス ルール、およびアプリケーション ダイヤル ルールを取得します。
4. Cisco Unified Mobility Advantage が、Unified Communicator Change Notifier（UCCN）サブスクリプションをユーザの **profileconfig** イベント パッケージとともに送信します。
5. Cisco Unified Mobility Advantage が、Presence サブスクリプションをユーザの **presence** イベント パッケージとともに送信します。

Cisco Unified Mobility Advantage を Cisco Unified Presence と統合する場合は、次の要件に従ってください。

- Cisco Unified Mobility Advantage は、単一の Cisco Unified Communications Manager クラスタと単一の Cisco Unified Presence クラスタに配置する必要があります。
- 1 つの Cisco Unified Mobility Advantage 配置で、1000 人を超える Cisco Unified Mobile Communicator ユーザの統合はできません。
- Cisco Unified Presence クラスタには、3 つ以上のノードを置くことはできません。

Cisco Unified Presence のサードパーティ製 Open API

Cisco Unified Presence は、SIP/SIMPLE に加え、HTTP を介してサードパーティ製アプリケーションを統合することができます。HTTP インターフェイスは、設定インターフェイスのほか、Representational State Transfer（REST）経由のプレゼンス インターフェイスを備えています。サードパーティ製の Open API は、プレゼンスへのアクセス メカニズムとして、リアルタイム イベンティング モデルとポーリング モデルの 2 つのメカニズムを持っています。

リアルタイム イベンティング モデル

リアルタイム イベンティング モデルでは、Cisco Unified Presence 上でアプリケーション ユーザを使用することにより、ユーザがそのセッション キーを使用してログインできるようになります。ユーザはログインすると、Representational State Transfer（REST）を使用してプレゼンスの更新について登録とサブスクリプションを行います。図 22-15 は、サードパーティ製の Open API のリアルタイム イベンティング モデルにおける Cisco Unified Presence との対話を示します。

図 22-15　サードパーティ製 Open API リアルタイム イベンティング モデル

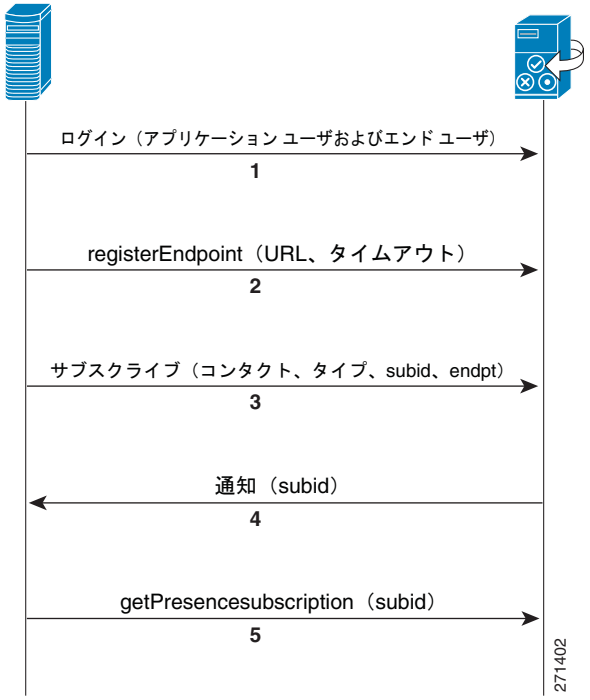


図 22-15 のコールフローは、次の一連のイベントを示しています。

1. アプリケーションが、スーパーユーザ アプリケーション ユーザ（APIUser）経由で Cisco Unified Presence に対して SOAP ログイン要求を開始し、Cisco Unified Presence がセッション キーを返します。これにより、アプリケーションはセッションキーを使用してエンドユーザをログインさせられるようになります（実質的には、エンドユーザがアプリケーション経由でログインします）。
2. エンド ユーザが、アプリケーションユーザ セッション キーを使用してエンドポイントを登録します。
3. アプリケーションが、ユーザの代わりに（セッション キーを使用して）サブスクライブ要求を開始し、ユーザ情報、連絡先リスト、およびプレゼンス ルールを取得します。
4. Cisco Unified Presence が、非保護の通知を送信します。
5. アプリケーションが、ユーザのプレゼンス ステータスを要求します。

ポーリング モデル

ポーリング モデルでは、Cisco Unified Presence 上でアプリケーション ユーザを使用することにより、ユーザがそのセッション キーを使用してログインできるようになります。ユーザがログインすると、アプリケーションは、ここでも Representational State Transfer（REST）を使用して、定期的にプレゼンスの更新を要求します。図 22-16 は、サードパーティ製の Open API のポーリング モデルにおける Cisco Unified Presence との対話を示します。

図 22-16　　サードパーティ製オープン API ポーリング モデル

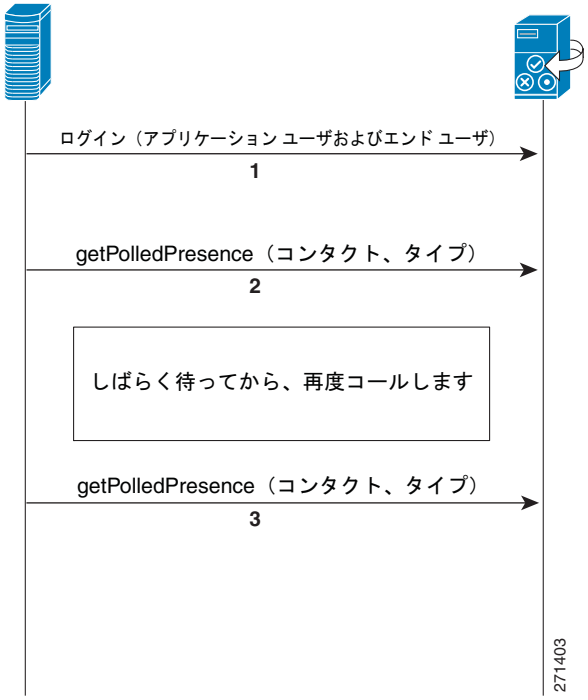


図 22-16 のコールフローは、次の一連のイベントを示しています。

1. アプリケーションが、スーパーユーザ アプリケーション ユーザ（APIUser）経由で Cisco Unified Presence に対して SOAP ログイン要求を開始し、Cisco Unified Presence がセッション キーを返します。これにより、アプリケーションはセッションキーを使用してエンドユーザをログインさせられるようになります（実質的には、エンドユーザがアプリケーション経由でログインします）。
2. アプリケーションがプレゼンス ステータスを要求します。イベンティング モデルは省略されます。

（注）　ポーリング モデルでは、基本プレゼンスと高度なプレゼンスの両方が取得できますが、Presence サーバの負荷が大きくなります。

いずれかのモデルのサードパーティ製の Open API を Cisco Unified Presence と統合する場合は、次の要件に従ってください。

- プレゼンス インターフェイスに対する証明書（sipproxy.der）と設定インターフェイスに対する証明書（tomcat_cert.der）が必要です。
- 1 つの Cisco Unified Presence 配置で、1000 人を超えるサードパーティ製の Open API ユーザの統合はできません。
- パフォーマンスの向上を図るには、サードパーティ製 Open API ユーザを Cisco Unified Presence クラスタにあるすべてのサーバに均等に振り分けてください。

Cisco Unified Presence のサードパーティ製 Open API の詳細については、次の Web サイトの Cisco Developer Services を参照してください。

http://www.cisco.com/web/developer/

開発者向けの情報は、Cisco Developer Community にも用意されています。次の Web サイトからログインしてアクセスしてください。

http://developer.cisco.com/

Cisco Unified Presence の配置ガイドライン

- LDAP 統合が可能な場合、すべてのユーザ情報（番号、ID など）は、単一のソースから Unified CM との LDAP 同期を使用してプルする必要があります。ただし、LDAP server および LDAP 同期が有効でない Unified CM の両方を含む配置の場合、管理者は、ユーザのディレクトリ番号のアソシエーションの設定にあたって、Unified CM と LDAP の両方に一貫した設定を行う必要があります。
- Cisco Unified Presence は、Differentiated Services Code Point（DSCP）により、レイヤ 3 IP パケットをマーキングします。Cisco Unified Presence は、SIP プロキシの下の Differential Service Value サービス パラメータ（デフォルトは DSCP 24（PHB CS3））に基づいて、すべてのコール シグナリング トラフィックにマーキングします。
- Cisco Unified Presence のプレゼンス ポリシーは、ユーザが作成した定義されたルール セットによって、厳格に制御されます。
- Cisco Unified Presence パブリッシャとサブスクライバは、Unified CM パブリッシャと共存する必要があります。
- サービス パラメータ CUP PUBLISH Trunk を使用して、Cisco Unified Presence サーバ との SIP 通信トラフィックを簡素化します。
- Unified CM のプレゼンス ユーザは、プライマリ内線だけでなく、ライン アピアランスと関連付けます。これにより、デバイスとユーザのプレゼンス ステータスの詳細度が向上します。サービス パラメータ CUP PUBLISH Trunk を使用している場合、Unified CM 内のプレゼンス ユーザをライン アピアランスと関連付けます。
- サーバ ハードウェアとクラスタ トポロジの特性を決定する際は、プレゼンス ユーザ プロファイル（ユーザ アクティビティおよび連絡先リストの連絡先とサイズ）を考慮する必要があります。
- クラスタ全体として最高のパフォーマンスを得るには、Assignment Mode Sync Agent パラメータに、デフォルトの [balanced] を使用します。
- Cisco Unified Presence 7.*x* は、Unified CM 5.*x*、6.*x*、および 7.*x* と互換性があります。
- Cisco Unified Communications Manager Business Edition（Unified CMBE）7.*x* は、LDAP 同期をサポートしています。これは、Unified CMBE を Cisco Unified Presence と統合する場合に有効にする必要があります。

Cisco Unified Presence によって使用されるポートの完全なリストについては、次の Web サイトで入手可能な『*Port Usage Information for Cisco Unified Presence*』を参照してください。

http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html

Cisco IP Phone Messenger アプリケーション

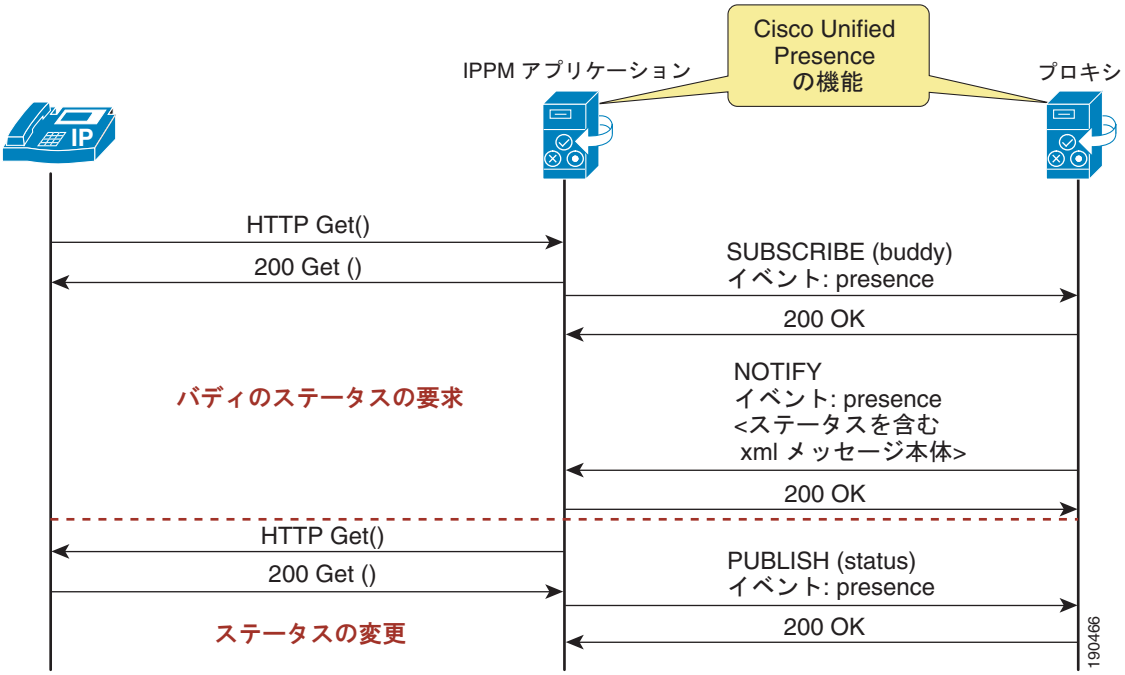
Cisco IP Phone Messenger は、ユーザが、バディ リストの作成、バディの集約プレゼンス情報の監視、およびバディの Cisco Unified IP Phone または準拠する SIP や SIMPLE クライアントまたはゲートウェイとのインスタント メッセージの交換などを行うための Cisco Unified の IP 電話サービスです。

Cisco Unified Presence のコンポーネントである Cisco IP Phone Messenger（IPPM）アプリケーションは、HTTP と SIP メッセージングの間のプロトコル変換プログラムとして動作します。IPPM アプリケーションは、Cisco Unified IP Phones との通信には XML over HTTP（http://www.cisco.com/go/apps）を使用し、SIP プロキシ/レジストラ サーバとの通信には SIP を使用します。IPPM は、異なるパーティション内にあり、同じディレクトリ番号を持つ 2 つのデバイスを区別します。また、ユーザがエクステンション モビリティ経由でログインした場合も、同様に動作します。ただし、新しいユーザがログインするには、Cisco Unified Presence パブリッシャが必要です。

IPPM アプリケーションは、次のプレゼンス機能を提供します（図 22-17 を参照）。

- バディの集約されたプレゼンス ステータスを表示します。
- 手動によるプレゼンス ステータス（Available、Busy、Do Not Disturb）を上書きします。
- 電話機へのログイン時に、すべての電話機バディのプレゼンス ステータスに対し SUBSCRIBE を呼び出します。電話機からのログアウト時に、Expires=0（サブスクリプションの終了）に設定して SUBSCRIBE を呼び出します。
- プレゼンス エンジンからの NOTIFY メッセージの受信時に、IPPM アプリケーションで、バディのプレゼンス ステータスを更新します。
- 電話機（Phone Messenger Service）と Web インターフェイス（http://<*cup_server_address*>/ccmuser）のどちらからでも連絡先リストが管理できます。

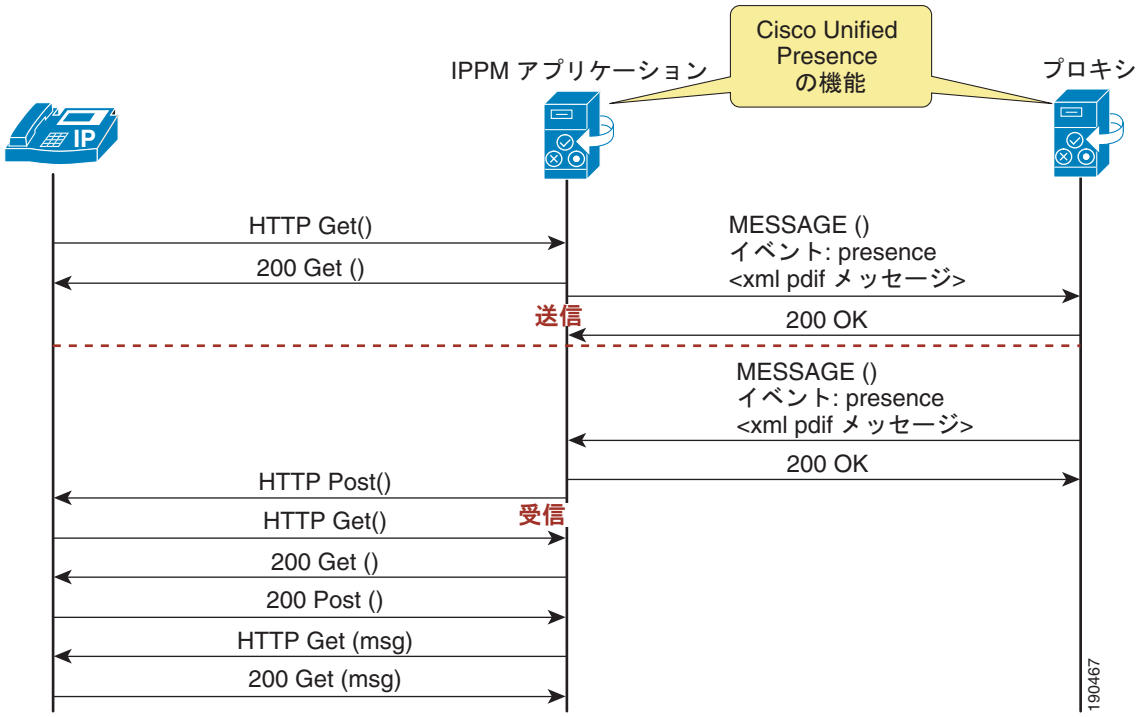
図 22-17　　IPPM プロトコル変換とプレゼンス



IPPM アプリケーションは、次のインスタント メッセージング（IM）機能を提供します（図 22-18 を参照）。

- 電話機の HTTP インスタント メッセージを変換して、SIP MESSAGE メッセージを発信します。
- 着信の SIP MESSAGE メッセージを HTTP インスタント メッセージに変換して電話機に出力します。
- バディ情報の画面または IM の画面から、バディにダイヤルバックできます。
- 電話機（Phone Messenger Service）から、メッセージ履歴が管理できます。
- ユーザは、システム全体または個人的な定型文の IM メッセージを設定したり、メッセージを作成したりすることができます。

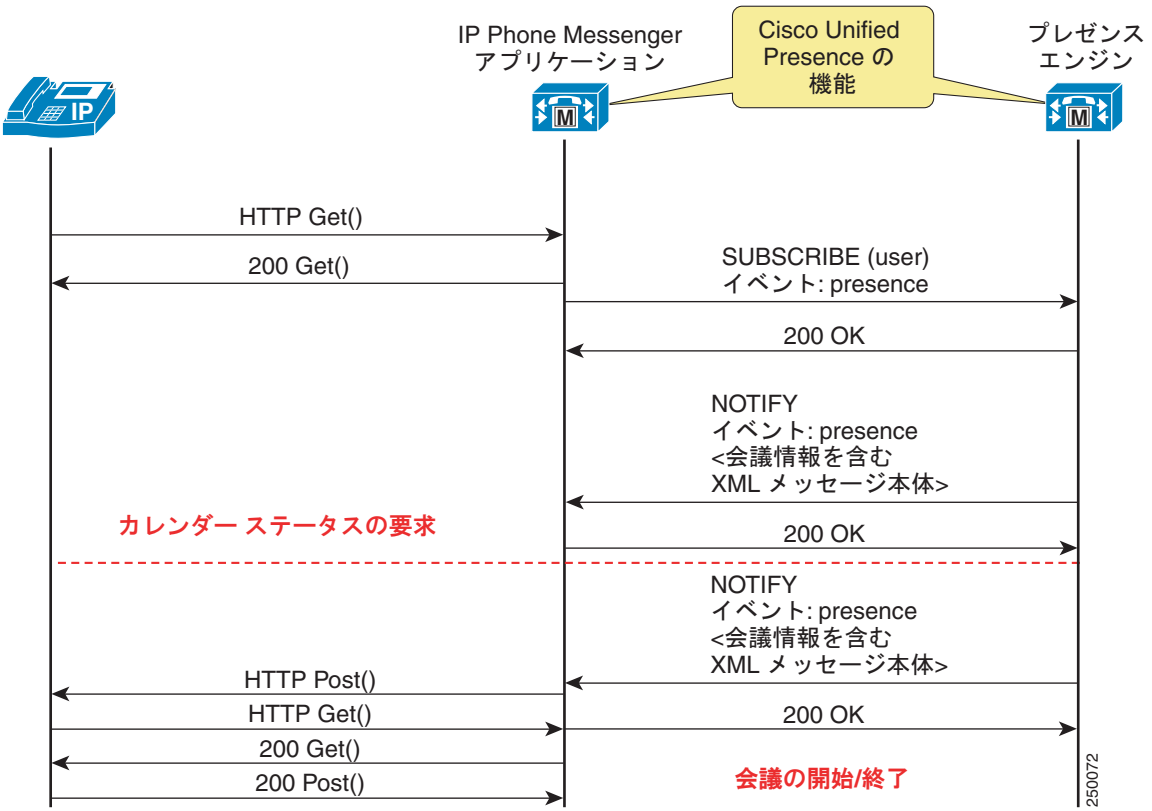
図 22-18　IPPM プロトコル変換とインスタント メッセージ



IPPM アプリケーションは、次の会議通知機能を提供します（図 22-19 を参照）。

- ユーザはデスクトップ カレンダー クライアントにログインすることなく、Cisco Unified Presence から登録済みの IPPM 電話機宛に対し、会議のリマインダを送信できます。
- （参加、ダイヤル、またはコールバックにより）IPPM サービスから会議に参加できる機能が用意されています。
- 会議のリマインダ機能をブロックするかどうかは、エンドユーザ用設定ページから制御できます。
- ユーザは、会議の参加者リストを会議の詳細画面に表示できます。これにより、IPPM モジュールからプレゼンス エンジンに、参加者のプレゼンス ステータスを照会する SUBSCRIBE メッセージが参加者ごとに送信されます。これで、現在の対応可能性に基づいて、参加者リストに記載されているユーザに、会議のリマインダとインスタント メッセージを送信することができます。

図 22-19　IPPM プロトコル変換と会議の通知



次の Cisco Unified IP Phone は、SCCP を使用した Cisco IP Phone Messenger をサポートしています。

- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7912G
- Cisco Unified IP Phone 7940G
- Cisco Unified IP Phone 7960G
- Cisco Unified IP Phone 7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G
- Cisco Unified IP Phone 7985G
- Cisco Unified IP Phone 7920 および 7921G
- Cisco IP Communicator

次の Cisco Unified IP Phone は、SIP を使用した Cisco IP Phone Messenger をサポートしています。

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7941G、7941G-GE、7942G、および 7945G

- Cisco Unified IP Phone 7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G

Cisco IP Phone 7905、7912、7940、および 7960 では、SIP を使用した IP Phone Messenger をサポートしていません。

Cisco Unified Communications System の現在の IP 電話サービスには、IP アドレスまたは HTTP Service URL の DNS A レコード エントリが設定されていますが、IP 電話サービスが冗長性が設定されていない場合、これがシングル ポイント障害になる可能性があります。

IP 電話サービスの冗長性が設定されていない場合、IP Phone Messenger 配置は、Cisco Unified Presence パブリッシャおよびサブスクライバの両方にわたって設定して、ロードバランスする必要があります。

次の例に示すように、Unified CM で、IP Phone Messenger に対して、Cisco Unified Presence パブリッシャを使用する電話サービスと、Cisco Unified Presence サブスクライバを使用するサービスの 2 つを設定します。

- PhoneMessenger1：

  http://publisher.cups.com:8081/ippm/default?name=#DEVICENAME#

- PhoneMessenger2:

  http://subscriber.cups.com:8081/ippm/default?name=#DEVICENAME#

Cisco IP Phone Messenger を使用して、次のいずれかの方法で、Cisco Unified IP Phones を配置することができます。

- シングル電話サービス

  シングル電話サービスでは、Cisco Unified IP Phone の半分が Cisco Unified Presence パブリッシャを指し（上の例の PhoneMessenger1）、残りの半分が Cisco Unified Presence サブスクライバを指す（上の例の PhoneMessenger2）ように設定します。

  利点：管理者が設定によって IP Phone Messenger ユーザをロードバランスできます。

  欠点：その電話機が動作する Cisco Unified Presence サーバに障害が発生した場合、ユーザが IP Phone Messenger サービスを利用できなくなります。

- デュアル電話サービス

  デュアル電話サービスでは、すべての Cisco Unified IP Phone が 2 つの IP Phone Messenger サービスを持つように設定します（上の例では、PhoneMessenger1 と PhoneMessenger2 の両方）。

  利点：その電話機が動作する Cisco Unified Presence サーバに障害が発生した場合、ユーザは、2 番目のサーバ上で動作する IP Phone Messenger サービスの使用を試みることができます。

  欠点：この方法では、Services メニューからどの IP Phone Messenger サービスを 選択するかが、電話のユーザにゆだねられています。この方法は、どちらかの Cisco Unified Presence サーバを選択するユーザが他方を選択するユーザより多くなり、その結果、片方の Cisco Unified Presence サーバにユーザが偏る可能性があります。

次の例に示すように、IP Phone Services の冗長性を使用すれば（「IP Phone Service の冗長性」（P.24-8）を参照）、IP Phone Messenger を、サーバ ロード バランサ（SLB）IP アドレスを使用する単一の電話サービスとして Unified CM 上に設定できます。

- PhoneMessenger:

  http://*slb_ip_address*:8081/ippm/default?name=#DEVICENAME#

Cisco IP Phone Messenger の帯域幅に関する考慮事項

ユーザのメッセージ履歴と連絡先リストは、いずれも Cisco Unified Presence データベースに保存され、大量のデータが含まれる可能性があります。ユーザが IP Phone Messenger アプリケーションにログインするたびに、メッセージ履歴や連絡先リストがダウンロードされます。したがって、帯域幅に不安がある場合は、Cisco Unified Presence の管理ページで [IP Phone Messenger] の下の [Max Instant Message History Size] と [Max Contact List Size] を設定して、メッセージ履歴のサイズと連絡先リスト サイズを制限することができます。

ユーザは、Session Timer パラメータを設定して、ユーザが現在のセッションにログインしている時間を制御したり、Refresh Interval パラメータを設定して、プレゼンス ステータスが更新される比率を制御したりすることができます。現在、管理者はこれらのパラメータを制御することができないので、デフォルト設定（Session Timer = 480 分、Refresh Interval = 30 分）が使用される可能性が最も高いと考えられます。

Cisco Unified Personal Communicator

Cisco Unified Personal Communicator は、よく使う通信アプリケーションやサービスを単一のデスクトップ ソフトウェア アプリケーションとして統合します。Cisco Unified Personal Communicator では、次のアプリケーションが利用されています。

- Lightweight Directory Access Protocol（LDAP）：ディレクトリや連絡先情報の検索
- Cisco Unified Communications Manager（Unified CM）：IP テレフォニー
- Cisco Unity または Unity Connection：音声メッセージング
- Cisco Unified MeetingPlace、MeetingPlace Express、または WebEx：Web 会議
- Cisco Unified Videoconferencing：マルチポイント ビデオ
- Cisco Unified MeetingPlace Express VT：マルチポイント音声、Web、およびビデオ スイッチング
- Cisco Unified Presence：設定、認証、サービス、インスタント メッセージング、およびプレゼンス情報

Cisco Unified Personal Communicator は、Desk Phone モード（ユーザのデスクトップフォンの CTI 制御による Click to Call）と Soft Phone モード（ソフトウェア クライアント操作）で使用でき、Apple Macintosh および Microsoft Windows プラットフォーム上でサポートされています。Cisco Unified Personal Communicator のコール シグナリング機能は、Cisco Unified IP Phone での機能とほぼ同じです。Cisco Unified Personal Communicator でサポートされるすべての機能のリストについては、「Unified Communications エンドポイント」（P.20-1）の章を参照してください。

Cisco Unified Personal Communicator の配置

図 22-20 は、Cisco Unified Personal Communicator のインターフェイスとさまざまなコンポーネント、および Cisco Unified Personal Communicator でプロトコル交換に使用されるポートを示します。Cisco Unified Personal Communicator におけるポートの使用の詳細については、次の Web サイトで入手可能な『*Release Notes for Cisco Unified Personal Communicator*』を参照してください。

http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

図 22-20　Cisco Unified Personal Communicator のコンポーネント

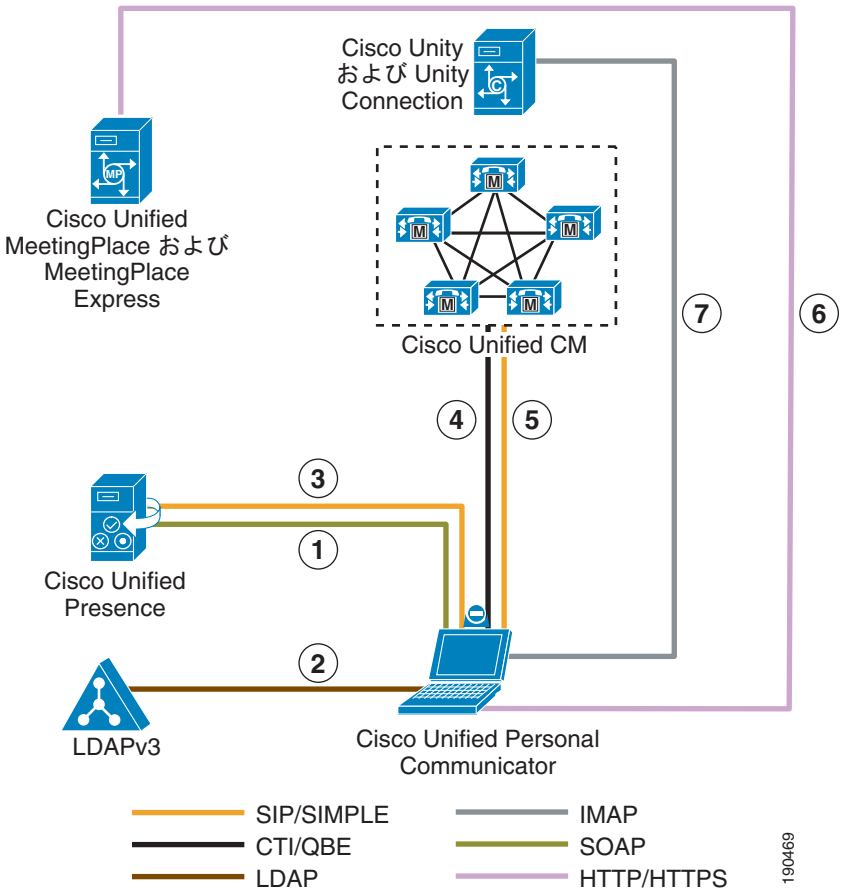


図 22-20 は、Cisco Unified Personal Communicator のコンポーネント間の次の対話を示します。

1. Cisco Unified Personal Communicator ユーザは、SOAP 経由で TLS を使用してログインし、さまざまなインターフェイス コンポーネントの設定プロファイルを入手します。Cisco Unified Presence サーバ は、証明書の検証を実行しないので、Cisco Unified Personal Communicator の認証サーバではありません。ただし、この TLS 接続は、Cisco Unified Personal Communicator と Cisco Unified Presence の間で交換されたすべての設定情報を保護します。Cisco Unified Personal Communicator ユーザが LDAP 経由で認証される場合、Cisco Unified Presence は、このログイン期間の間、そのユーザについて LDAP へのバインドを実行した後、次の処理に進みます。
2. Cisco Unified Personal Communicator は、すべてのユーザ固有情報（電話番号や連絡先など）について、LDAP サーバにバインドします。

   Microsoft Active Directory を使用する場合は、パラメータの選択を慎重に考慮してください。大規模な Active Directory 実装が存在し、設定で Domain Controller が使用されている場合、Cisco Unified Personal Communicator で十分なパフォーマンスが得られないことがあります。Active Directory の応答時間を改善するために、場合によっては、ドメイン コントローラをグローバル カタログに強化し、LDAP ポートを 3268 に設定する必要があります。
3. Cisco Unified Personal Communicator は、そのユーザについての SIP REGISTER と、連絡先リストのすべてのユーザについての SIP SUBSCRIBE を Cisco Unified Presence に送信します。連絡先リストでユーザ ステータスの更新が必要な場合は、Cisco Unified Presence から SIP NOTIFY が着信します。ユーザ ステータスが手動または自動で変更されている場合は、SIP PUBLISH が送信されます。

4. Cisco Unified Personal Communicator が Desk Phone モードに設定されている場合、Unified CM の CTI Manager によって電話機制御のための接続が確立されます。
5. Cisco Unified Personal Communicator は、SIP REGISTER を Unified CM に送信してメディア交換（音声およびビデオ）を可能にし、SIP NOTIFY でメッセージ待機インジケータ（MWI）のステータスを受信します。
6. 2 人の Cisco Unified Personal Communicator ユーザ間のコールは、会話のセッションから、Cisco Unified MeetingPlace や MeetingPlace Express で HTTP（S）を使用した共有専用の Web コラボレーション セッションへとエスカレーションすることができます。それぞれの接続で MeetingPlace ユーザ ライセンスを 1 つずつ使用するので、エスカレーションを開始するユーザは、MeetingPlace Express プロファイルが必要です。
7. ボイスメールを開始したコールは、Cisco Unity または Unity Connection で IMAP を使用して通信が行われます。

Cisco Unified Personal Communicator と Cisco Unified Presence の間、および Cisco Unified Personal Communicator と Unified CM の間のすべての SIP トラフィック、プレゼンス、およびコール設定は暗号化されず、TCP または UDP 経由で実行されます。Cisco Unified Personal Communicator は、標準の SIMPLE インターフェイスを使用してプレゼンス情報を交換します。

Cisco Unified Presence クラスタ内のすべてのユーザは、情報交換の前に、サーバに割り当てる必要があります。Cisco Unified Presence は、デフォルトで自動的にユーザがクラスタ内のすべてのサーバに均等に割り当てられます。管理者は、User Assignment Mode Sync Agent サービス パラメータをデフォルトの **balanced** から **None** に変更してユーザの割り当て先を制御することができます。このパラメータを **None** に変更すると、**System** > **Topology** メニューでユーザを割り当てられます。

Cisco Unified Personal Communicator の配置は、基本の配置と、自動冗長機能を持つ高可用性配置があります。Cisco Unified Presence の 2 サーバ構成のサブクラスタでは、サブクラスタの片方のサーバに関連付けられたユーザが、自動的に他方のサーバにも認識されるので、設定されたサーバでの通信が中断した場合の自動フェールオーバーが可能です（図 22-21 を参照）。

図 22-21　Cisco Unified Presence の 2 サーバ構成のサブクラスタにおけるフェールオーバー

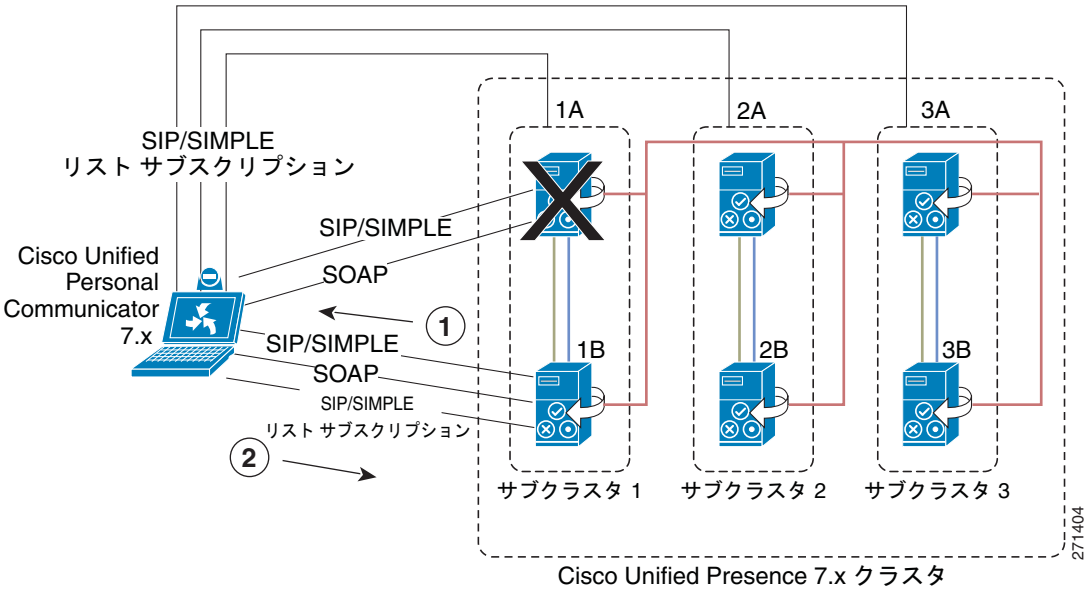


図 22-21 に示すように、Cisco Unified Presence サーバ 1A の障害時には、次の一連のイベントが発生します。

1. Cisco Unified Presence サーバ 1B が、Cisco Unified Personal Communicator に NOTIFY を送信し、サーバ 1A での Presence と Unified Client Change Notifier（UCCN）サブスクリプション状態を終了します。
2. Cisco Unified Personal Communicator が Cisco Unified Presence サーバ 1B に SUBSCRIBE メッセージを送信し、その Presence と UCCN サブスクリプション状態を再度アクティブにします。

Cisco Unified Presence がフェデレーション配置の設定を完了すると、Cisco Unified Personal Communicator では、フェデレーションの連絡先の追加も可能になります。これによりユーザは、既存のドメイン内の連絡先だけでなく、他のドメインのユーザを連絡先として入力し、制御できます。この追加の連絡先機能によって、ユーザは、通信可能なリストやドメインのブロックなどのプライバシーの制御もできます。

フェデレーションの詳細については、次の Web サイトで入手可能な『*Integration Guide for Configuring Cisco Unified Presence Release 7.0 for Inter-Domain Federation*』を参照してください。

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

Cisco Unified Personal Communicator の設計上の考慮事項

Cisco Unified Personal Communicator の必須インターフェイスには、Cisco Unified Presence、Cisco Unified Communications Manager（Unified CM）、および LDAP v3 準拠サーバがあります。Cisco Unified Personal Communicator のオプションのインターフェイスは、Cisco Unity、Cisco Unity Connection、Cisco Unified MeetingPlace、Cisco Unified MeetingPlace Express、Cisco Unified Videoconferencing、Cisco Unified MeetingPlace Express VT です。ソリューションの設計とサイジングを検討する際は、すべてのコンポーネントについて、次のスケーラビリティに関するインパクトを考慮する必要があります。

- クライアントのスケーラビリティ

  Cisco Unified Presence サーバ ハードウェアの配置が決まれば、クラスタがサポートできるユーザの数が決定されます。Cisco Unified Personal Communicator の配置は、クラスタ内のすべてのサーバに対し、すべてのユーザを均等に割り当てる必要があります。これは、User Assignment Mode Sync Agent サービス パラメータを [balanced] に設定すれば、自動的に処理されます。

  連絡先リストには、連絡先を最大 200 まで設定できます。

- LDAP 検索コンテキスト

  LDAP フィルタを指定して、特定のオブジェクト クラスのみを検索する機能を使用すると、ディレクトリからコンピュータを除いたユーザだけを取得することができます。これには、検索コンテキストの末尾に &(objectclass=user) を追加します。次の例を参考にしてください。

  cn=user,**dc**=example,**dc**=com;&(objectclass=user)

  複数の LDAP 検索コンテキストを指定するには、Cisco Unified Presence Administration の LDAP Search Context フィールドで、# をデリミタとして使用します。次の例では、サポートされる形式を示します。

  ou=test,**dc**=example,**dc**=com#**ou**=testing,**dc**=example,**dc**=com

  Cisco Unified Personal Communicator は、両方の組織ユニットを「test」、「testing」の順に検索します。

  LDAP 検索コンテキスト フィールドに指定できるのは最大 255 文字なので、サポートされる組織ユニットは、個別の検索コンテキストのサイズと文字数に応じて異なる可能性があります。

- IMAP のスケーラビリティ

  IMAP 接続数は、メッセージング統合のプラットフォームのオーバーレイ（Cisco Unity or Cisco Unity Connection）によって決定されます。特定の設定のサイジングについては、http://www.cisco.com で入手可能な Cisco Unity または Cisco Unity Connection の製品マニュアルを参照してください。

- Web 会議

  Web 会議に同時に参加できる参加者の数は、Cisco Unified MeetingPlace または Cisco Unified MeetingPlace Express Web ライセンスによって決定されます。特定の設定のサイジングについては、http://www.cisco.com で入手可能な Cisco Unified MeetingPlace または Cisco Unified MeetingPlace Express の製品マニュアルを参照してください。

  Cisco Unified Personal Communicator は、パスワードを必要としない Cisco WebEx 会議をサポートします。Cisco WebEx サーバでは、[All meetings must have a password] オプションがデフォルトで選択されています。Cisco Unified Personal Communicator が Cisco WebEx 会議を起動するためには、このオプションの選択を解除する必要があります。

- ビデオのサイジング容量

  ビデオ会議とスイッチングは、Cisco Unified Videoconferencing MCU のサイジングと設定に応じて決定されます。または、音声、ビデオ、Web の同時参加者数については、Cisco Unified MeetingPlace Express VT によって決まります。特定の設定のサイジングについては、http://www.cisco.com で入手可能な Cisco Unified MeetingPlace Express VT の製品マニュアルを参照してください。

Cisco Unified Personal Communicator は Unified CM と相互接続します。そのため、Cisco Unified Personal Communicator 音声またはビデオ コールを開始した場合、Unified CM の現在の機能に関する次のガイドラインが適用されます。

- CTI のスケーラビリティ

  Desk Phone モードでは、Cisco Unified Personal Communicator からのコールが、Unified CM 上の CTI インターフェイスを使用します。したがって、「コール処理」（P.8-1）の章に明記された CTI の制限を遵守してください。Unified CM クラスタのサイジングを行う際は、これらの CTI デバイスを含める必要があります。

- コール アドミッション制御

  Cisco Unified Personal Communicator は、Unified CM ロケーションまたは RSVP 経由で、音声またはビデオ コールに対してコール アドミッション制御を適用します。

- コーデックの選択

  Cisco Unified Personal Communicator の音声およびビデオ コールは、Unified CM リージョン設定よるコーデックの選択を利用します。

- ダイヤル規則

  Cisco Unified Personal Communicator は、ローカルのダイヤル規則のダウンロードや保存を一切行いません。したがって、ダイヤル プランを維持するために、Unified CM に対し、アプリケーション ダイヤル規則の設定が必要になることがあります（たとえば、ユーザが 18005551212 とダイヤルしたが、5 桁しか必要でない場合、Unified CM は、「1 で始まる 11 桁の番号 = 末尾の 5 桁のみを保持」というアプリケーション ダイヤル規則を適用します）。

Cisco Unified Personal Communicator には、帯域幅に関する次の考慮事項も適用されます。

- Cisco Unified Personal Communicator のすべての設定と連絡先は、Cisco Unified Presence データベースに保存され、大量のデータが含まれる可能性があります。現在、通信リストは 50 ユーザが上限ですが、連絡先リストのサイズには上限がありません。したがって、プレゼンス データの交換に利用される帯域幅を考慮に入れておく必要があります。

- Cisco Unified MeetingPlace の音声、ビデオ、Web コラボレーション セッションについては、「Cisco Unified MeetingPlace」（P.14-1）の章を参照してください。
- Cisco Unified MeetingPlace Express の Web コラボレーション セッションについては、「Cisco Unified MeetingPlace Express」（P.15-1）の章を参照してください。
- ビデオ コールについては、「IP ビデオ テレフォニー」（P.16-1）の章を参照してください。
- Cisco Unity または Unity Connection については、「シスコの音声メッセージング」（P.13-1）の章の「帯域幅の管理」（P.13-32）の節を参照してください。

Cisco Unified Personal Communicator は、Differentiated Services Code Point（DSCP）により、レイヤ 3 IP パケットをマーキングします。Cisco Unified Personal Communicator は、コール シグナリング トラフィックを DSCP 24（PHB CS3）の値でマーキングします。またボイス メディア トラフィックを DSCP 46（PHB EF）の値でマーキングします。ただしパーソナル コンピュータ トラフィックは、通常、信頼されていないため、PC でアプリケーションによって施された DSCP マーキングは、ネットワークで除去されます。したがって、アクセス ルータやスイッチは、Cisco Unified Personal Communicator が利用するポート範囲で、これらの DSCP マーキングを許可するように設定する必要があります。トラフィック マーキングの詳細については、次の Web サイトで入手可能な『*Enterprise QoS Solution Reference Network Design (SRND)*』を参照してください。

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

サードパーティ製プレゼンス サーバ統合

Cisco Unified Presence は、SIP アプリケーションと SIMPLE アプリケーションを Cisco Unified Communications ソリューションに統合するための、SIP と SIP for Instant Messaging and Presence Leveraging Extensions（SIMPLE）に基づくインターフェイスを提供します。これにより、サードパーティ製のプレゼンス サーバやアプリケーションをこの SIP/SIMPLE と連携して設定し、統合して、プレゼンス集約やフェデレーションを提供することができます。

Microsoft Communications Server

Microsoft Live Communications Server 2005 または Office Communications Server 2007、および Microsoft Office Communicator のすべてのセットアップ、設定、および配置については、次の Web サイトの資料を参照してください。

http://www.microsoft.com/

シスコは、Microsoft Communications 製品の設定、配置、またはベスト プラクティス手順は提供していませんが、Cisco Unified Presence と Microsoft Live Communications Server 2005 または Office Communications Server 2007 との統合に関する次のガイドラインを提供しています。

シスコシステムズは、機能の相互運用性と、Cisco Unified Presence を Microsoft Live Communications Server 2005 に統合するための設定手順を示すアプリケーション ノートを作成しました。アプリケーション ノートは、次の Web サイトで入手できます。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/pbx/interop/notes/602270nt.pdf

シスコシステムズはまた、機能の相互運用性と、Cisco Unified Presence を Microsoft Office Communications Server 2007 に統合するための設定手順を示すアプリケーション ノートを作成しました。アプリケーション ノートは、次の Web サイトで入手できます。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/pbx/interop/notes/617030nt.pdf

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns784/712410.pdf

シスコシステムズはまた、Cisco Unified Presence を Microsoft Office Communications Server 2007 に統合するためのガイドを作成しました。この『*Integration Note for Configuring Cisco Unified Presence with Microsoft LCS/OCS for MOC Call Control*』は、次の Web サイトで入手可能です。

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

Cisco Unified Presence と Microsoft Live Communications Server 2005 または Office Communications Server 2007 との統合のためのガイドライン

次のガイドラインは、Cisco Unified Presence サーバを Microsoft Live Communications Server 2005 または Office Communications Server 2007 に統合する場合に適用されます。

- Cisco Unified Presence と Microsoft Live Communications Server 2005 または Office Communications Server 2007 の間の通信には、SIP/SIMPLE インターフェイスが使用されます。ただし、Microsoft Live Communications Server 2005 または Office Communications Server 2007 は、SIP 経由の Computer-Supported Telecommunications Applications（CSTA）トラフィックをトンネルします。したがって、Cisco Unified Presence サーバ上の CTI ゲートウェイは、Click to Call の電話制御のために CSTA-CTI 変換を処理するように設定する必要があります。
- リモート通話コントロール対応の Microsoft Office Communications Server 2007 または Live Communications Server 2005 と共に配置する Cisco Unified Presence は、1 対のサーバを持つ単一のサブクラスタから成る Cisco Unified Presence クラスタで構成する必要があります。
- 次の表では、プラットフォームごとのサポートされるユーザ数を示します。

Cisco Unified Presence のプラットフォーム	Cisco Unified Communications Manager のプラットフォーム	サーバごとのサポートされるユーザ数	Microsoft Office Communicator のクラスタごとのサポートされるユーザ数
MCS 7825、7835、または 7845	MCS 7825	900	3,600
MCS 7825、7835、または 7845	MCS 7835	1,000	4,000
MCS 7825、7835、または 7845	MCS 7845	3,375	13,500

- エンド ユーザ ID は、LDAP、Unified CM、および Microsoft Live Communications Server 2005 または Office Communications Server 2007 で同一に設定する必要があります。これにより、Microsoft Live Communications Server 2005 または Office Communications Server 2007 の Active Directory（AD）での認証や Unified CM のエンドユーザ設定との競合、さらには Unified CM 上でのユーザの電話機の制御との競合を防止できます。

  Active Directory については、General、Account、および Live Communications のユーザのプロパティですべて同一の ID を使用することをお勧めします。Cisco Unified Presence の全ユーザの一貫性を維持するために、Unified CM で LDAP 同期と LDAP 認証を有効にする必要があります。
- Microsoft Live Communications Server 2005 または Office Communications Server 2007 のホスト認証に Cisco Unified Presence のパブリッシャとサブスクライバを含める必要があります。
- Live Communications Server 2005 または Office Communications Server 2007 のプロパティの設定で、SIP メッセージが静的 IP アドレスによって Cisco Unified Presence にルーティングされるように設定する必要があります。

- Cisco Unified Presence サーバの発着信のアクセス制御リスト（ACL）で、Microsoft Live Communications Server 2005 または Office Communications Server 2007 との通信を許可する必要があります。
- Unified CM で各ユーザのプレゼンスを有効するだけでなく、Cisco Unified Presence サーバ設定で、各ユーザに Microsoft Office Communicator の使用を許可する必要があります。
- Microsoft Office Communicator のログイン時に、Microsoft Office Communicator と Microsoft Communications Server 間での設定情報の交換や、Cisco Unified Presence サーバ CTI ゲートウェイとの初期通信のために必要となる帯域幅を考慮に入れる必要があります。
- Microsoft Office Communications Server 2007 では、必要なパラメータの名前が Live Communications Server 2005 から変更されています。Live Communications Server 2005 で定義されている TEL URI パラメータは、Office Communications Server 2007 の Line URI と同じです。また Live Communications Server 2005 の Remote Call Control SIP URI パラメータは、Office Communications Server 2007 の Server URI と同じです。
- ディレクトリ番号からそれに対応するユーザを検索する逆ルックアップの問題に対処するには、次の Web サイトで入手可能な『*Release Notes for Cisco Unified Presence*』のガイドラインの資料を使用してください。

  http://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html

IBM Sametime 7.5

シスコ システムズでは、IBM Sametime Server 7.5.1 と Cisco Unified Communications の最適な統合のための次のガイドラインを提供していますが、IBM Communications 製品の設定、配置、またはベスト プラクティス手順を強くお勧めしているわけではありません。

IBM Sametime Server 7.5.1 のすべてのセットアップ、設定、および配置については、次の Web サイトを参照してください。

http://www.ibm.com/

シスコは、IBM Communications 製品に関する設定、配置、またはベスト プラクティス手順は提供していませんが、IBM Sametime Server 7.5.1 と Cisco Unified Communications システムの統合に関して次のガイドラインを提供しています。

Integrating Cisco Unified Presence と IBM Sametime Server 7.5.1 の統合のためのガイドライン

IBM Sametime 7.5.1 クライアント内に統合された クリック ツー コールおよびクリック ツー会議機能は、IBM Sametime Server 7.5.1 上に存在する Cisco Call Control プラグイン経由で処理されます。クリック ツー コールおよびクリック ツー会議機能のための Cisco Unified Communications との統合は、Unified CM との SIP トランク インターフェイス経由で処理されます。プレゼンス機能のための Cisco Unified Communications との統合は、Cisco Unified Presence との SIP/SIMPLE インターフェイス経由で処理されます。

- クリック ツー コールおよびクリック ツー会議機能のための Unified CM SIP トランクの Out-Of-Dialog Refer（OOD-Refer）処理ができるように設定する必要があります。IBM Sametime Server 7.5.1 と通信する SIP トランクの SIP Trunk Security Profile で、Accept Out-of-dialog REFER チェックボックスをオンにします。
- IBM Sametime Server 7.5.1 に存在する Cisco Call Control プラグインは、ラウンドロビン方式で使用される Unified CM の設定済みリストを保持します。このリストには、アウトオブダイアログ REFER SIP トランクで設定した Unified CM サブスクライバの IP アドレスが含まれています。

  Unified CM のリストは、DNS SRV でも設定できますが、この SRV ロジックは、冗長性のみに使用されロード バランシングには使用されないので、この設定はお勧めできません。

- IBM Sametime Server 7.5.1 を使用した配置トポロジは、これら 2 つのシステムのキャパシティの違いから、通常、複数の Unified CM クラスタと統合されます。Unified CM のリストをラウンドロビン方式で使用する Cisco のクリック ツー コール プラグリンを利用すると、ユーザのホーム クラスタとは異なるクラスタに、REFER が送信されることがあります。Unified CM は、このコール設定を受信すると、REFER を処理し、適切な宛先に対して、このコール設定を完了させる INVITE を生成します。
- Cisco Call Control プラグインでは、トラフィック マーキングが完全に実装されていません。次の Web サイトで入手可能な『*Enterprise QoS Solution Reference Network Design (SRND)*』を参照してください。

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

CHAPTER 23

Cisco Collaboration クライアントおよびアプリケーション

（注） この章は、このドキュメントの現在のリリースに新たに追加されました。Cisco Unified Communications システムにコラボレーション クライアントおよびアプリケーションを配置する前に、この章全体を読むことをお勧めします。

Cisco Collaboration クライアントおよびアプリケーションは統合的なユーザ エクスペリエンスを実現し、Cisco Unified Communications システムの機能と操作性を拡張します。これらのクライアントおよびアプリケーションは、オンライン会議、プレゼンス通知、インスタント メッセージング、オーディオ、ビデオ、ボイスメールなど、多数のアプリケーションを使い勝手の良い 1 つのコラボレーション クライアントに統合することにより、企業境界内外のコラボレーションを可能にします。

多数のコラボレーション クライアントおよびアプリケーションを使用でき、Cisco Unified Communications システムに統合する場合のアーキテクチャ ビュー、配置に関する考慮事項、プランニング、および設計ガイドラインがそれぞれに用意されています。この章を使用して、どのコラボレーション クライアントおよびアプリケーションが配置に最も適しているかを確認してください。

- Cisco WebEx Connect

  Cisco WebEx Connect は、コラボレーティブな Software-as-a-Service（SaaS）型プラットフォームであり、開発者、パートナー、およびカスタマーはこれを利用して、コラボレーティブ ソリューションを経由した到達可能範囲を拡大できる強力なコラボレーティブ ビジネス ソリューションを作成できます。Cisco WebEx Connect は、企業クラスのセキュリティ、スケーラビリティ、パフォーマンス、および可用性を強制的に確立するとともに、Cisco Unified Communications ソリューションとの透過的な通信を可能にするための、拡張可能なオープン型コラボレーション プラットフォームを実現します。Cisco WebEx Connect には、Cisco WebEx Connect Client と Cisco WebEx Connect Platform の 2 つの主要コンポーネントがあります。

- Cisco Unified Personal Communicator

  Cisco Unified Personal Communicator は、デスクトップ（PC または Mac）上のリッチ メディア インターフェイスから音声、ビデオ、Web 会議、インスタント メッセージング、ボイスメール、およびプレゼンス情報への容易なアクセスを可能にするユーザ向けのデスクトップ アプリケーションです。Cisco Unified Personal Communicator の利用によって、チーム間の生産性は高まり、ナレッジ ワーカは便利なユーザ インターフェイスを通じていつでもどこでも簡単にコラボレートし、通信をエスカレーションすることが可能になります。詳細については、「Cisco Unified Presence」（P.22-1）の章を参照してください。

- Cisco Unified Mobile Communicator

  Cisco Unified Mobile Communicator は、携帯電話から Cisco Unified Communications アプリケーションにアクセスし、利用する機能をユーザに提供するモビリティ ソリューションです。Cisco Unified Mobile Communicator および Cisco Mobile グラフィカル クライアントは、Cisco Unified Mobility Advantage ソフトウェアを実行しているサーバと連動して、携帯電話の機能にアクセスし、制御するためのリッチ ユーザ インターフェイスを提供します。このシステムは既存の社内 LDAP ディレクトリに統合されるため、ユーザはすべてのデバイス上で単一のクレデンシャル セットを使用できます。詳細については、「シスコ モビリティ アプリケーション」（P.25-1）の章を参照してください。

Cisco WebEx Connect のアーキテクチャ

Cisco WebEx Connect には、Cisco WebEx Connect Client および Cisco WebEx Connect Platform の 2 つの主要コンポーネントがあります。Cisco WebEx Connect は、セキュリティ、スケーラビリティ、パフォーマンス、アベイラビリティを強制的に確立するための拡張可能なオープン型コラボレーション プラットフォームを実現します。

Cisco WebEx Connect Client

Cisco WebEx Connect Client は、エンド ユーザのパーソナル コンピュータにインストールするリッチ クライアントであり、多数の機能が装備されています。Cisco WebEx Connect Client は、Microsoft Windows XP、Vista、または Windows 7 オペレーティング システムが搭載された任意のパーソナル コンピュータにインストールできます。現在、Apple Macintosh および Linux オペレーティング システムはサポートされていません。

Cisco WebEx Connect サイト管理者は、エンド ユーザのユーザ ID とパスワードを別個に作成するのではなく、シングル サインオンを使用して、エンド ユーザによる Cisco WebEx Connect に対する認証および署名を可能にすることができます。WebEx Connect でのシングル サインオンの詳細については、次の Web サイトにある『*WebEx Connect: User Provisioning and SSO* Developer Technical Note』を参照してください。

http://developer.webex.com/c/document_library/get_file?folderId=11835&name=DLFE-244.pdf

プレゼンス

Cisco WebEx Connect（C6 リリース以降）では、プレゼンス機能に Extensible Messaging and Presence Protocol（XMPP）を利用しています。XMPP は、リアルタイム通信用のオープン テクノロジーであり、インスタント メッセージング、プレゼンス、マルチパーティ チャット、音声コールとビデオ コール、コラボレーション、軽量なミドルウェア、コンテンツのシンジケーション、および Extensible Markup Language（XML）データの汎用ルーティングなど、広範なアプリケーションの実行を可能にします。XMPP の詳細については、次のソースを参照してください。

- 「XMPP Standards Foundation」（http://www.xmpp.org/）
- XMPP Community の Web ページ（http://www.jabber.org/）

XMPP は、他のほとんどのインスタント メッセージングおよびプレゼンス ネットワークの標準として採用されているため、Cisco WebEx Connect のプレゼンス情報と、XMPP をサポートする他のプレゼンス クラウドのフェデレーションが可能です。Cisco WebEx Connect ユーザには、フェデレーションによって Instant Messaging（IM; インスタント メッセージング）の連絡先リストに他のネットワーク

からユーザを容易に追加でき、各ユーザのプレゼンスを確認できるという利点があります。他のネットワークとのプレゼンスのフェデレーションについては、「Cisco WebEx Connect に関する設計上の考慮事項」（P.23-10）を参照してください。

エンドユーザのプレゼンス ステータスは、Cisco WebEx Collaboration Cloud 内の Cisco WebEx プレゼンス サーバによって保持されます。

インスタント メッセージング

ユーザは、他の Cisco WebEx Connect ユーザのほか、他のインスタント メッセージング プラットフォーム上のユーザにセキュアなインスタント メッセージを送信できます。Cisco WebEx Connect ユーザは、インスタント メッセージング セッションから PC 間の VoIP コール、音声会議、ビデオ会議、デスクトップ共有セッション、または WebEx 会議へと容易にエスカレーションすることができます。また、Cisco WebEx Connect ユーザは、インスタント メッセージング セッション中に他のユーザとファイルを交換することもできます。

Cisco WebEx Connect ユーザ間のインスタント メッセージング セッションはセキュリティで保護され、クライアントから Cisco WebEx Collaboration Cloud への通信には TLS 暗号化が使用されます。TLS 暗号化は、Cisco WebEx のデフォルトで有効になります。WebEx Connect サイト管理者がサイト単位で無効にすることはできません。必要に応じて、AES 256 ビット暗号化を使用して、インスタント メッセージ自体をエンドツーエンドで暗号化することもできます。他の XMPP クライアントが暗号化をサポートしている場合は、TLS 暗号化を使用して、Cisco WebEx Connect ユーザとその XMPP クライアント間のすべてのインスタント メッセージング セッションを暗号化することができます。

スペース

スペースは、チーム メンバーに非同期のコラボレーション環境を提供します。主要コンポーネントは、持続性のあるグループ ディスカッションと SaaS ベースのドキュメント管理システムです。スペース所有者は、スペースに参加するように企業ネットワーク内外からユーザを招待することができます。スペースは、スペースのメンバーだけに通知されます。スペースのすべてのコンテンツは、Cisco WebEx Collaboration Cloud 内に安全に保存され、暗号化されます。

スペースは、Cisco WebEx Connect で任意に使用できます。カスタマーは、スペースなしの Cisco WebEx Connect のプロビジョニングを選択することもできます。スペースの設定の詳細については、次の Web サイトにある『*Cisco WebEx Connect Administrator's Guide*』を参照してください。

http://www.webex.com/webexconnect/orgadmin/help/index.htm

カレンダーの統合

Cisco WebEx Connect は、エンド ユーザのコンピュータでローカルに実行する Microsoft Outlook カレンダーと統合されます。Microsoft Exchange Server または Cisco WebEx Mail のいずれかと通信するには、エンド ユーザのコンピュータに Microsoft Outlook クライアントを設定する必要があります。エンド ユーザが Web メール、Microsoft Outlook Web Access（OWA）、または Cisco WebEx Web メールしか所有していない場合、カレンダーの統合は機能しません。

Cisco WebEx Meeting Center の統合

Cisco WebEx Meeting Center と Cisco WebEx Connect の統合を有効にするには、Cisco WebEx Connect クライアントまたは Cisco WebEx Connect ドメイン管理ページで特定の設定情報を指定します。この統合を有効にすると、Cisco WebEx Connect から直接 Cisco WebEx Meeting Center 会議をス

ケジュールできるので、ユーザは各自の Cisco WebEx Connect クライアントから容易に WebEx Web 会議をスケジュールし、開始することができます。Cisco WebEx Meeting Center の統合は、組織の管理者が設定することも、エンド ユーザがクライアントで設定することもできます。

管理者として Cisco WebEx Meeting Center を設定する方法については、次の Web サイトにあるドキュメンテーションを参照してください。

http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?17673.htm

Cisco Unified Communications の統合

Cisco WebEx Connect は、Cisco Unified Communications Manager を使用した Cisco WebEx Connect 内からの直接のクリックコールを設定できます。Cisco Unified Communications は、配置トポロジとニーズに応じて次のいずれかの方法で Cisco WebEx Connect に統合できます。

- Cisco WebEx Connect Unified Communications Widget（Computer Telephony Integration [CTI; コンピュータ テレフォニー インテグレーション] WebDialer を使用したクリックコール、ボイスメール、および短縮ダイヤル）
- Cisco Unified Communications Integration™ for Cisco WebEx Connect

Cisco WebEx Connect Unified Communications Widget

Cisco WebEx Connect Unified Communications Widget（CTI WebDialer、ボイスメール、および短縮ダイヤル）は、Cisco WebEx Connect Widget フレームワーク内で実行し、REST インターフェイス（JSON/HTTP）経由で Web アプリケーションと通信します。Web アプリケーションは、REST を使用した Lightweight Directory Access Protocol（LDAP; 軽量ディレクトリ アクセス プロトコル）照会用の LDAP Web サービス、REST 経由のログインおよびプレゼンス管理用のプレゼンス ログイン サービス、AVVID XML Layer（AXL）/Simple Object Access Protocol（SOAP）経由の短縮ダイヤル アクセス、およびバックエンド システムの設定を可能にする管理ポイントを提供します。

CTI WebDialer ウィジェットにより、ユーザはクリックコール統合および機能を利用できます。Cisco WebEx Connect 内の番号（4 桁以上）にはハイパーリンクが設定され、ユーザはその番号をクリックするだけで、電話機のキーパッドで電話番号を入力せずにコールを開始することができます。Unified CM で CTI モニタリングを有効にして、WebEx Connect 管理ページで Unified CM 統合を有効にする必要があります。

Cisco WebEx Connect 管理ページの設定方法については、次の Web サイトを参照してください。

http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?cs_singleptprov.htm

Cisco Unified Communications Integration™ for Cisco WebEx Connect

Cisco Unified Communications Integration™ for Cisco WebEx Connect は、Client Services Framework を使用した Unified CM と Cisco WebEx Connect の強固な統合を可能にして、Cisco WebEx Connect クライアント内での完全な呼制御を有効にします。Client Services Framework は、デスクトップ クライアントをオーディオ エンドポイントとするソフトフォン呼制御にも、デスクトップ クライアントが Cisco Unified IP Phone を制御するデスクトップフォン制御にも対応し、いずれの場合も WebEx Connect の [Phone] タブに表示されます（図 23-1 を参照）。

図 23-1　WebEx Connect ユーザ インターフェイス

クリックコール機能用に連絡先を入力して使用する方法は、次のとおりです。

- WebEx Connect 内に表示されるハイパーリンクの番号をクリックします。この番号が有効な内線番号または有効な番号である場合、デスクトップフォンの統合を使用していればエンドユーザの IP 電話とのコール、またはソフトフォンの統合を使用していればローカル PC とのコールを発信するためのコマンドが、Cisco Unified Communications Integration™ から Unified CM に送信されます。
- PC 上の Microsoft Outlook の個人用アドレス帳にある連絡先名を検索するか、ソフトフォンのディレクトリ ボックスを使用して電話番号を入力します。ユーザは、電話番号または連絡先名を入力し、番号を強調表示して、ダイヤル キーを押すだけです。
- デスクトップフォンの統合を使用している場合は IP 電話から、またはソフトフォン統合を使用している場合はローカルのダイヤル パッドから手動でコールします。呼制御は、WebEx Connect クライアントからも利用できます。

Cisco WebEx Connect Platform

Cisco WebEx Connect Platform は、同期および非同期コラボレーションに対応したマルチテナント型 Software-as-a-Service（SaaS）プラットフォームです。WebEx Connect Platform は、Cisco WebEx Collaboration Cloud 内でホストされます。

Cisco WebEx Software-as-a-Service 製品の詳細については、次の Web サイトを参照してください。

http://www.cisco.com/en/US/products/ps10352/products_category_technologies_overview.html

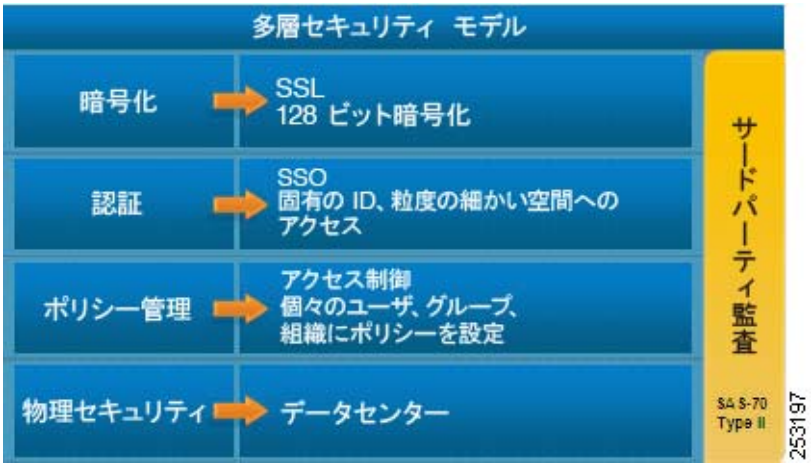
Cisco WebEx Collaboration Cloud の詳細については、次の Web サイトを参照してください。

http://www.cisco.com/en/US/prod/ps10352/collaboration_cloud.html

セキュリティ

図 23-2 は、WebEx セキュリティ モデルの機能層を構成する、相互に関連する独立した要素を示しています。

図 23-2　　WebEx セキュリティ モデル



最下位層は、Cisco WebEx データセンターの物理セキュリティを示しています。すべての従業員は、広範なバックグラウンド チェックを通過し、データセンターに入るためのデュアルファクタ認証を実行する必要があります。

次のレベルのポリシー管理では、WebEx Connect 組織管理者が、個々のユーザ、グループ、または Cisco WebEx Connect 組織全体に異なるポリシーを設定することによってアクセス制御レベルを設定し、管理できます。外部ユーザまたはドメインに固有のブラック リストまたはホワイト リスト ポリシーを作成して、インスタント メッセージング交換を制限したり、許可したりすることができます。Cisco WebEx Connect 組織モデルでは、ユーザ ベース全体に固有の役割やグループを作成することもでき、管理者は特定の権限を役割やグループに割り当てたり、組織全体に対してアクセス制御などのポリシーを設定したりすることができます。

Cisco WebEx Connect へのアクセスは、認証層で制御されます。いずれのユーザも固有のログインとパスワードを所有します。パスワードが保存されたり、クリア テキストの E メールで送信されたりすることはありません。パスワードを変更できるのは、エンドユーザ自身だけです。管理者は、次のログイン時にエンドユーザがパスワードを変更するように、パスワードのリセットを選択することができます。また、管理者は、Cisco WebEx Connect と企業の Active Directory との間の Single Sign On（SSO; シングル サインオン）統合を使用して、エンドユーザのアクセス管理を簡略化することもできます。

暗号化層では、TLS 暗号化プロトコルを使用して、Cisco WebEx Connect ユーザ間のすべてのインスタント メッセージング通信が暗号化されるようにします。Cisco WebEx Connect ユーザと他の XMPP クライアント ユーザ間のすべてのインスタント メッセージング通信は、TLS 暗号化を使用してデフォルトで暗号化されます。Cisco Unified Communications Integration™ for Cisco WebEx Connect を PC（ソフトフォン）モードで使用した音声通話は、Secure Real-time Transport Protocol（SRTP）を使用して暗号化できます。これらの設定は、Cisco WebEx Connect サイト管理者によって、またはエンドユーザによって Cisco WebEx Connect クライアント設定の [Unified Communications] タブで制御できます。

Cisco WebEx Connect Platform では、SAS70 Type II 監査などのサードパーティの監査を使用して、カスタマーに半年ごとに別個のセキュリティ レポートを提供します。カスタマーは、シスコのセキュリティ組織に要求すればいつでもこのレポートを確認できます。

Cisco WebEx Connect の配置

Cisco WebEx Connect は、可用性の高い冗長なトポロジに配置することができます。Cisco WebEx Connect Software-as-a-Service アーキテクチャの配置は、この項で説明する各種のネットワークおよびデスクトップ要件で構成されます。

高可用性

マルチテナント型 Software-as-a-Service アーキテクチャを使用する利点は、グループ内の個々のサーバに障害が発生した場合に、Cisco WebEx Connect Platform で使用可能な別のサーバに透過的に要求をルーティングできることにあります。

Cisco WebEx Network Operations Team は、Cisco WebEx Network Operations Center（NOC）から Cisco WebEx Collaboration Cloud を毎日 24 時間アクティブに監視します。Cisco WebEx テクノロジーの概要については、次の Web サイトを参照してください。

http://www.cisco.com/en/US/products/ps10352/products_category_technologies_overview.html

冗長性、フェールオーバー、および障害回復

Cisco WebEx のグローバル サイト バックアップ アーキテクチャは、電源異常、自然災害による停電、放電過多、その他のタイプのサービス中断を処理します。グローバル サイト バックアップでは、手動と自動の両方のフェールオーバーをサポートします。手動フェールオーバー モードは通常、メンテナンス時間枠で使用されます。自動フェールオーバー モードは、サービス中断によるリアルタイム フェールオーバーの場合に使用されます。

グローバル サイト バックアップは、エンド ユーザに対して自動的かつ透過的であり、すべてのユーザが利用でき、フェールオーバー可能なユーザ数の制限もありません。

グローバル サイト バックアップには、次の 3 つのコンポーネントがあります。

- グローバル サイト サービス：ネットワーク レベルでトラフィックの監視とスイッチングを行います。
- データベース複製：プライマリ サイトでのデータ トランザクションをバックアップ サイトに確実に転送します。
- ファイル複製：ファイル変更が、プライマリ サイトとバックアップ サイト間で同期されるようにします。

ネットワーク要件

WebEx Connect は、Software-as-a-Service アプリケーションです。エンド ユーザが WebEx Connect にログインするには、エンド ユーザの PC をインターネットに接続する必要があります。標準のインターネット接続があれば、利用することができます。エンド ユーザが遠隔地で作業している場合、WebEx Connect にログインするために企業の Virtual Private Network（VPN; バーチャル プライベート ネットワーク）経由で接続する必要はありません。

容量と帯域幅の要件

エンドユーザが WebEx Connect にログインして、プレゼンス、インスタント メッセージング、および Voice over IP（VoIP）コーリングなどの基本機能を利用するために必要なものは、56 kbps ダイヤル アップ インターネット接続だけです。ただし、小規模のオフィスや支店でファイル転送、ビデオ会議、およびチーム スペースなどの高度な機能を利用するには、512 kbps 以上のブロードバンド接続が必要です。

デスクトップ要件

WebEx Connect クライアントは現在、Microsoft Windows クライアントだけでサポートされています。表 23-1 に、Cisco WebEx Connect をインストールして実行するために最低限必要なデスクトップ要件を示します。

表 23-1　Cisco WebEx Connect をインストールして実行するための最低デスクトップ要件

コンポーネント	IM とプレゼンスだけを搭載した Cisco WebEx Connect	IM、プレゼンス、およびスペースを搭載した Cisco WebEx Connect	Cisco Unified Communications Integration™ for Cisco WebEx Connect
オペレーティング システム	Windows XP SP3 Windows Vista 32 ビット	Windows XP SP3 Windows Vista 32 ビット	Windows XP SP3 Windows Vista 32 ビット
CPU	Intel Pentium プロセッサ	Intel Pentium プロセッサ（1.8 GHz）	Intel Pentium プロセッサ（2.4 GHz）
ディスク容量	80 MB	80 MB	200 MB
ブラウザ	Internet Explorer 6.0/7.0 Mozilla Firefox 3.0	Internet Explorer 6.0/7.0 Mozilla Firefox 3.0	Internet Explorer SP2 for XP Internet Explorer 7 for Vista Mozilla Firefox 3.0
I/O ポート	USB 2.0（ビデオ カメラ用）	USB 2.0（ビデオ カメラ用）	USB 2.0（ビデオ カメラ用）
E メール プログラム（Microsoft Outlook との統合を可能にする Cisco WebEx Connect 設定を選択していることを確認してください）	Microsoft Outlook 2003 または 2007	Microsoft Outlook 2003 または 2007	Microsoft Outlook 2003 または 2007

表 23-1　Cisco WebEx Connect をインストールして実行するための最低デスクトップ要件 （続き）

コンポーネント	IM とプレゼンスだけを搭載した Cisco WebEx Connect	IM、プレゼンス、およびスペースを搭載した Cisco WebEx Connect	Cisco Unified Communications Integration™ for Cisco WebEx Connect
音声	全二重方式サウンド カードおよびヘッドセット	全二重方式サウンド カードおよびヘッドセット	全二重方式サウンド カードおよびヘッドセット
ビデオ	1.8 GHz 以上の CPU、解像度 800x600、256 色以上、および Web カメラ	1.8 GHz 以上の CPU、解像度 800x600、256 色以上、および Web カメラ	1.8 GHz 以上の CPU、解像度 800x600、256 色以上、および Web カメラ

ポートと IP アドレスの範囲

Cisco WebEx Connect では、ポート 80 および 443 を使用します。デフォルトでは、サードパーティ製の XMPP クライアントで XMPP 通信用にポート 5222 が使用されます。表 23-2 と表 23-3 に、Cisco Unified Communications Integration™ for Cisco WebEx Connect で使用するポートを示します。

表 23-2　Cisco Unified Client Services Framework で着信トラフィックに使用されるポート

ポート	Protocol	Cisco Unified Communications Integration™ for Cisco WebEx Connect のポート使用法
16384 ～ 32766	UDP	オーディオおよびビデオ用の Receives Real-Time Transport Protocol（RTP）メディア ストリームを受信する。これらのポートは、Cisco Unified Communications Manager で設定されます。デバイス コンフィギュレーション ファイルの詳細については、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html にある『*Cisco Unified Communications Manager System Guide*』を参照してください。

表 23-3　Cisco Unified Client Services Framework で発信トラフィックに使用されるポート

ポート	Protocol	Cisco Unified Communications Integration™ for Cisco WebEx Connect のポート使用法
69	UDP	Trivial File Transfer Protocol（TFTP）ファイルをダウンロードするために TFTP サーバに接続する。
389	TCP	連絡先を検索するために LDAP サーバに接続する。
2748	TCP	Cisco Unified Communications Manager の CTIManager コンポーネントである CTI ゲートウェイに接続する。
5060	UDP/TCP	Session Initiation Protocol（SIP; セッション開始プロトコル）コール シグナリングを提供する。
5061	TCP	セキュアな SIP コール シグナリングを提供する。
8443	TCP	現在割り当てられているデバイスのリストを取得するために、Cisco Unified Communications Manager IP Phone サーバに接続する。

表 23-3　Cisco Unified Client Services Framework で発信トラフィックに使用されるポート （続き）

ポート	Protocol	Cisco Unified Communications Integration™ for Cisco WebEx Connect のポート使用法
8191	TCP	Simple Object Access Protocol（SOAP）Web サービスを提供するためにローカル ポートに接続する。
16384 ～ 32766	UDP	オーディオおよびビデオ用の RTP メディア ストリームを送信する。

Cisco WebEx サービスは、IP アドレス 66.163.32.0 ～ 66.163.63.25、および 209.197.192.0 ～ 209.197.223.255 の範囲で提供されます。Cisco WebEx では随時 IP アドレスを再割り当てできるので、これらの範囲に基づいて Access Control List（ACL; アクセス制御リスト）を設定することはお勧めしません。

ファイアウォール ドメインのホワイト リスト

アクセス制御リストは、webex.com ドメインおよび webexconnect.com ドメインと、この両ドメインのすべてのサブドメインからのすべての通信を許可するように明確に設定する必要があります。WebEx Connect Platform からエンドユーザにユーザ名とパスワードを通知する E メールが送信されます。これらの E メールは mda.webex.com ドメインから発信されます。

インスタント メッセージング ロギング

Cisco WebEx Connect インスタント メッセージング通信は、ユーザがログインしているパーソナル コンピュータのローカル ハード ドライブに記録されます。インスタント メッセージのロギングは、Org Admin ツールを使用して有効にすることができる、Cisco WebEx Connect の機能です。インスタント メッセージのロギングを Cisco WebEx Connect に対して有効にすると、インスタント メッセージは記録され、次のパスに保持されます。

file:///c:/Documents and Settings/user/*_Connect/Archive/_username*

エンドユーザは、ロギングの詳細、ロギングの有効化または無効化、およびログの保存期間を設定できます。これらの設定は、Cisco WebEx Connect クライアント設定の [General IM] で行います。

Cisco WebEx Connect の以前のリリースで使用していた Cisco WebEx Connect Advanced Auditor には、Cisco WebEx Connect の C6 リリースとの互換性はありません。詳細な監査機能や e-Discovery（電子情報の開示）機能を必要とする場合は、サードパーティ製のソリューションを利用することも検討してください。現在シスコでは、インスタント メッセージング通信の詳細な監査や中央集中型ロギングをサポートしていません。

Cisco WebEx Connect に関する設計上の考慮事項

Cisco WebEx Connect の設計および配置は、Cisco Unified Communications Manager およびサードパーティ製アプリケーションのほか、Cisco WebEx Connect Client および Cisco WebEx Connect Platform とのインターフェイスによって成り立っています。Cisco WebEx Connect を配置する際は、以降の項に示す設計上の考慮事項を使用してください。

1 つの管理対象の Connect ドメインあたり 1 つの Unified CM 統合

WebEx Connect の現在のリリースでは、1 つの管理対象の Connect ドメインのすべてのエンド ユーザが同一の Unified CM 統合を使用する必要があります。Connect ロードマップには、エンドユーザのサブグループの作成が必要です。これらのサブグループがいったん有効になれば、管理者は別の Unified CM 統合を別のサブグループに割り当てることができます。

Unified CM CTI Manager

Cisco Unified Communications Widgets for Cisco WebEx Connect と統合している場合、CTI WebDialer からはクリックコール機能だけを使用できます。その他のコール フローやコール制御機能は使用できません。

サポートされている CTI の最大限度については、「コール処理」（P.8-1）の章を参照してください。Cisco Unified Communications Widgets for Cisco WebEx Connect で CTI WebDialer を使用する際には、また、Cisco Unified Communications Integration™ for Cisco WebEx Connect でのデスクトップ フォン制御モードには、CTI の数値が重要になります。

サードパーティ製の XMPP クライアントから Cisco WebEx Connect Platform への接続

シスコでは、他の XMPP クライアントによる Cisco WebEx Connect Platform への接続を公式にサポートしていませんが、XMPP プロトコルの性質上、エンドユーザはさまざまな XMPP クライアントを使用してプレゼンス クラウドに接続することができます。XMPP ソフトウェア クライアントのリストは、次の Web サイトで入手できます。

http://xmpp.org/software/clients.shtml

組織のポリシーは、サードパーティ製の XMPP クライアントに適用できません。また、エンドツーエンド暗号化、デスクトップ共有、ビデオ コール、PC 間コール、および電話会議などの機能は、サードパーティ製のクライアントではサポートされていません。WebEx Connect 以外の XMPP IM クライアントでの Connect ドメインに対する認証を可能にするには、Domain Name System Service（DNS SRV; ドメイン ネーム システム サービス）レコードを更新する必要があります。[Configuration and IM Federation] の Cisco WebEx Connect サイト管理スペースに、特定の DNS SRV エントリを見つけることができます。

[Configuration and XMPP IM Clients] の Cisco WebEx Connect サイト管理スペースで、Connect 以外の XMPP クライアントの使用を明示的に許可する必要があります。

サードパーティ製 XMPP クライアントを使用したインスタント メッセージおよびプレゼンス フェデレーション

Cisco WebEx Connect ネットワークは、GoogleTalk および Jabber.org などの XMPP ベースのインスタント メッセージング ネットワークとフェデレーションすることができます。XMPP に基づいた公衆インスタント メッセージング ネットワークのリストは、次の Web サイトで入手できます。

http://xmpp.org/

WebEx Connect は、IBM Lotus Sametime XMPP ゲートウェイ経由で IBM Lotus Sametime と、また、Microsoft Office Communications Server XMPP ゲートウェイ経由で Microsoft Office Communications Server とフェデレーションすることができます。これらのサードパーティ製 XMPP ゲートウェイを使

用する場合、IBM Lotus Sametime や Microsoft Office Communications Server の配置のバックエンドで設定を有効にする必要があります。シスコではこれらの設定を公式にサポートしていません。また、クライアント間の相互運用性も保証していません。

現在、WebEx Connect には Yahoo! Messenger および Windows Live Messenger との相互運用性はありませんが、フェデレーション ゲートウェイ経由で AIM とフェデレーションすることはできます。

その他のリソースおよびドキュメンテーション

『*Cisco WebEx Connect Administrator's Guide*』は、次の Web サイトで入手できます。

http://www.webex.com/webexconnect/orgadmin/help/index.htm

Cisco WebEx Connect のエンドユーザ向けガイドは、次の Web サイトで入手できます。

http://www.webex.com/webexconnect/help/wwhelp/wwhimpl/js/html/wwhelp.htm

CHAPTER 24

Cisco Unified CM アプリケーション

Cisco Unified CM アプリケーションは、基礎的な IP テレフォニーに多数の動作および機能の拡張を提供します。External eXtensible Markup Language（XML）生産性向上アプリケーションまたは IP Phone Service は、Web サーバまたはほとんどの Cisco Unified IP Phone 上のクライアント（あるいはその両方）で実行できます。たとえば、ユーザのデスク上の IP Phone を使用して、株式相場、天気情報、フライト情報など各種の Web ベースの情報を取得できます。また、カスタム IP Phone サービス アプリケーションを作成すると、ユーザが在庫を追跡したり、時間単位で顧客に課金したり、会議室の環境（照明、ビデオ画面、室温など）を制御できます。Cisco Unified CM には、次に示すような追加機能を提供する統合アプリケーションも多数あります。

- Cisco Extension Mobility（EM）

  Extension Mobility（EM）機能では、モバイル ユーザがその電話機にログインすることで、一時的に Cisco Unified IP Phone をそのユーザ用に 設定できます。

- Cisco Unified Communications Manager Assistant（Unified CM Assistant）

  Unified CM Assistant は、アシスタントが 1 人以上のマネージャあて着信電話コールを処理できるようにする Cisco Unified CM に統合されたアプリケーションです。

- Cisco Unified Communications Manager Attendant Console

  Unified CM Attendant Console では、組織内で 1 人以上の受付係がコールに応答およびコールを転送（または送信）することができます。

- Cisco WebDialer

  WebDialer は Cisco Unified CM のクリックコール アプリケーションで、ユーザはサポートされる任意の電話デバイスを使用して自分の PC から簡単にコールを発信できます。

場合によっては、これらの統合アプリケーションが追加機能を提供するために、IP Phone Service を呼び出すこともあります。

この章では、次の Cisco Unified CM アプリケーションについて説明します。

この章の新規情報

表 24-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 24-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
Cisco Unified Communications Manager Attendant Console	「Cisco Unified Communications Manager Attendant Console」（P.24-35）
Cisco Unified Department、Business、および Enterprise Attendant Console	「Cisco Unified Department、Business、および Enterprise Attendant Console」（P.24-47）
Extension Mobility Redundancy のオプション	「EM の冗長性」（P.24-14）
Extension Mobility セキュリティ	「EM Security」（P.24-16）
Extension Mobility サービス パラメータ	「EM のサービス パラメータ」（P.24-11）
IP Phone Services の動作	「Cisco Unified CM サービスと IP Phone Service のエンタープライズ サービス パラメータ」（P.24-3）
Redirector のキャパシティ	「WebDialer のパフォーマンスとスケーラビリティ」（P.24-61）
WebDialer API のアップデート	「WebDialer のアーキテクチャ」（P.24-57）
WebDialer の電話機のサポート	「WebDialer の電話機のサポート」（P.24-52）
WebDialer の冗長性	「デバイスと到達可能性の冗長性」（P.24-60）
WebDialer のサイジング	「WebDialer のパフォーマンスとスケーラビリティ」（P.24-61）

IP Phone サービス

Cisco Unified IP Phone Service は、Web クライアントやサーバ、および Cisco Unified IP Phone の XML 機能を利用するアプリケーションです。Cisco Unified IP Phone のファームウェアには、限定的な Web ブラウジング機能を可能にするマイクロブラウザが含まれています。これらの電話サービス アプリケーションを、ユーザのデスクトップ電話機上で直接実行することで、付加価値サービスが提供され、生産性も向上する可能性があります。この章で *phone service* という用語は、Cisco Unified IP Phone を宛先および発信元としてコンテンツを送受信するアプリケーションを指します。

IP Phone Service をサポートする電話機

次の電話機は IP Phone Service をサポートしています。

- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified IP Phone 7940G、7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7960G、7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G

IP Phone Service は次の IP Phone でも実行できます。ただし、これらの電話機モデルは、テキストベースの XML アプリケーションだけをサポートします。

- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7912G および 7912G-A
- Cisco Unified Wireless IP Phone 7920

上記のすべての IP Phone は、電話機と実行中の電話サービスを含む Web サーバの間でユーザ インターフェイス（UI）を有効にするために、Cisco が定義する XML オブジェクトの限定されたセットを処理できます。

上記の電話機は、Skinny Client Control Protocol（SCCP）と Session Initiation Protocol（SIP）の両方で電話サービスをサポートすることに注意してください。

Cisco Unified CM サービスと IP Phone Service のエンタープライズ サービス パラメータ

IP Phone Service を使用可能にするために、システム 管理者は Cisco Unified Serviceability インターフェイスの下で Cisco Unified IP Phone Service のネットワーク サービス が有効になっていることを必ず確認してください。また、次の項で説明するように、IP Phone Service に対して設定およびカスタマイズのためのオプションを提供するエンタープライズ サービス パラメータがいくつかあります。

IP Phone Service の Cisco Unified CM サービス

IP Phone Service の機能は、Unified CM 上の Cisco Unified IP Phone Service ネットワーク サービスの Cisco CallManager に依存しています。この機能は Unified CM がサーバにインストールされると、デフォルトでインストールされ、アクティブになります。

IP Phone Service の エンタープライズ パラメータ

この IP Phone Service に関連するいくつかのエンタープライズ パラメータがあります。Cisco Unified CM 7.*x* では、Service Provisioning のエンタープライズ パラメータは新しいパラメータです。この新しいパラメータは IP 電話にプロビジョニングされるサービス方法の動作に影響を与えます。設定できるオプションは次の通りです。

- 内部

  Phone Service は管理者によってプロビジョニングされ、IP 電話には設定ファイルが登録のサイクル時に TFTP を介してダウンロードされ、設定済のサービス リストを受信します。電話機の URL エンタープライズ パラメータに指定されたサービス、メッセージ、および URL ディレクトリ は使用されません。プロビジョニングされた有効な Java MIDlet サービスがインストールされ、実行可能になります。この設定はデフォルトです。この設定を使用すると、設定済みのサービスのリストを受信するために最初に IP 電話を IP Phone Service に接続する必要がなくなります。代わりに、必要なサービスに直接アクセスできます。

- 外部 URL

  TFTP を介して取得した設定ファイルの Phone Service はプロビジョニングされていません。電話機では、Phone URL エンタープライズ パラメータ で指定された Phone Services の URL だけを使用します。Java MIDlet が実行できないのは、インストールし実行するように内部的にプロビジョニングされているためです。この動作は本リリース 7.0 に先立つ Unified CM と同じです。

- 両方

  最初、設定ファイルにあるプロビジョニングされた任意の Phone サービスが表示されます。その後に、IP phone で、サービス、メッセージ、またはディレクトリ のボタンを押したときに、対応する URL を介して動的に取得された任意のサービスが続きます。設定ファイルのプロビジョニングされた任意の Java MIDlet がインストールされ、実行して利用できます。

（注） Service Provisioning エンタープライズ パラメータ は、共通 Phone Profile 構成にセットすることで上書きでます。または、実際の電話機に設定します（これは両方よりも優先度が高い）。

このパラメータは 3 個のレベルで階層的に構成されています。3 個のレベルとはエンタープライズ パラメータ 、共通 Phone Profile 構成、および電話機構成です。エンタープライズ パラメータには、上記に列挙される 3 個の値があり、その共通 Phone Profile 構成および電話機構成のフィールドには追加のデフォルト値があります。つまり、上記のレベルへの設定は異なります。

次の項目は、Cisco Unified CM Enterprise Service Parameters 設定ページの Phone URL Parameters 項の下にある、設定パラメータの一部リストを表しています。これら項目は IP Phone Service および IP Phone の XML 処理に関連しています。

- URL Authentication（デフォルト値 = http://<*CM_IP_address*>:8080/ccmcip/authenticate.jsp）

  この URL は、Cisco Unified CM の authenticate.jsp サービスを指します。このサービスは、Cisco Unified IP Phones と Cisco Unified CM の間で認証プロキシ サービスを提供します。この URL は、電話サービスによって電話機に直接行われた「push」要求を検証するために使用されます。これは、インストール時に自動的に設定されます。このパラメータに値を指定しない場合、電話サービスは電話機にコンテンツをプッシュできません。

- URL Directories（デフォルト値 = http://<*CM_IP_address*>:8080/ccmcip/xmldirectory.jsp）

  この URL は、Cisco Unified CM 上の xmldirectory.jsp サービスを指します。このサービスは、ユーザが電話機の Directories（またはブック アイコン）ボタンを押したときに表示されるディレクトリ メニューを生成して返信します。この URL は、インストール時に自動的に設定されます。このパラメータに値を指定しないと、ユーザが Directories ボタンを押したときに、ディレクトリ メニューを利用できません。

- URL Idle（デフォルト値 = < *ブランク*>）

  指定された場合、この URL は、電話機がアイドル状態のときに電話機の画面に表示されるテキストまたはイメージを提供するサービスを指します。このパラメータは、サービスを開始するまでの電話機のアイドル時間を示す URL Idle Time パラメータと密接に関連しています。デフォルトで、このパラメータはインストール時にブランクのままになります（設定されません）。

- URL Idle Time（デフォルト値 = 0）

  このパラメータは、電話機が URL Idle サービスを開始するまでに待機する時間を秒単位で示します。デフォルトで、このパラメータはインストール時に 0（ゼロ）に設定され、電話機がアイドル状態にならないことを示します。

- URL Information（デフォルト値 = http://<*CM_IP_address*>:8080/ccmcip/GetTelecasterHelpText.jsp）

  この URL は、Cisco Unified CM 上の GetTelecasterHelpText.jsp サービスを指します。このサービスは、ユーザが（キーパッドの右側にある）Help（「i」または「?」）ボタンを押したときに電話機のキーおよびコール統計に関する画面上の電話機ヘルプを生成して返信します。この URL は、インストール時に自動的に設定されます。このパラメータに値を指定しないと、Help ボタンを押したときにヘルプ情報が表示されません。

- URL Services（デフォルト値 = http://<*CM_IP_address*>:8080/ccmcip/getservicesmenu.jsp）

  この URL は、Cisco Unified CM 上の getservicesmenu.jsp サービスを指します。このサービスは、ユーザが Services（または地球のアイコン）ボタンを押したときに電話機のユーザ加入電話サービスのリストを表示します。これは、インストール時に自動的に設定されます。このパラメータに値を指定しないと、Services ボタンを押したときに加入サービスのリストが表示されません。

IP Phone Service のアーキテクチャ

IP Phone サービスは、次のような複数の方法で開始できます。

- ユーザ起動（プル）

  IP Phone ユーザが Services ボタンを押すと、ユーザ加入電話サービスのリストを表示するために、HTTP GET メッセージが Cisco Unified CM に送信されます。図 24-1 は、この機能を示しています。

- 電話機起動（プル）

  IP Phone ファームウェア内で、アイドル時間の値は URL Idle Time パラメータによって設定できます。このタイムアウト値を超えた場合、IP Phone のファームウェア自体が URL Idle パラメータで指定されるアイドル状態の URL の場所に対して、HTTP GET を開始します。

- 電話サービス起動（プッシュ）

  電話サービス アプリケーションは、電話機に HTTP POST メッセージを送信することによって、IP Phone にコンテンツをプッシュできます。

（注） 電話サービスを呼び出すために電話機の Web クライアントが使用されるユーザ起動および電話機起動のプル機能とは異なり、電話サービス起動のプッシュ機能は、電話機の（クライアントではなく）Web サーバに（HTTP POST を通じて）コンテンツをポストすることによって、電話機上の処理を呼び出します。

図 24-1 は、ユーザが開始する IP Phone サービス処理の詳細を示しています。ユーザが Services ボタンを押したときに Services Provisioning で外部 URL にセットされる場合、デフォルトでは、HTTP GET メッセージが IP Phone から Cisco Unified CM の getservicesmenu.jsp スクリプトに送信されます（ステップ 1）。URL Services パラメータを変更することによって、異なるスクリプトを指定できます（「IP Phone Service の エンタープライズ パラメータ」（P.24-3）を参照）。getservicesmenu.jsp スクリプトは、個々のユーザが加入している電話サービス URL ロケーションのリストを返します（ステップ 2）。HTTP 応答は、IP Phone にこのリストを返します（ステップ 3）。ユーザによって選択される追加の電話サービス メニュー オプションは、ユーザと選択された電話サービス アプリケーションを含む Web サービス間で HTTP メッセージングを継続します（ステップ 4）。

（注） Service Provisioning エンタープライズ パラメータが内部にセットされる場合は、ステップ 1 からステップ 3 まで がバイパスされ、電話サービスの処理はステップ 4 から開始します。

図 24-1　ユーザ起動の IP Phone Service のアーキテクチャ

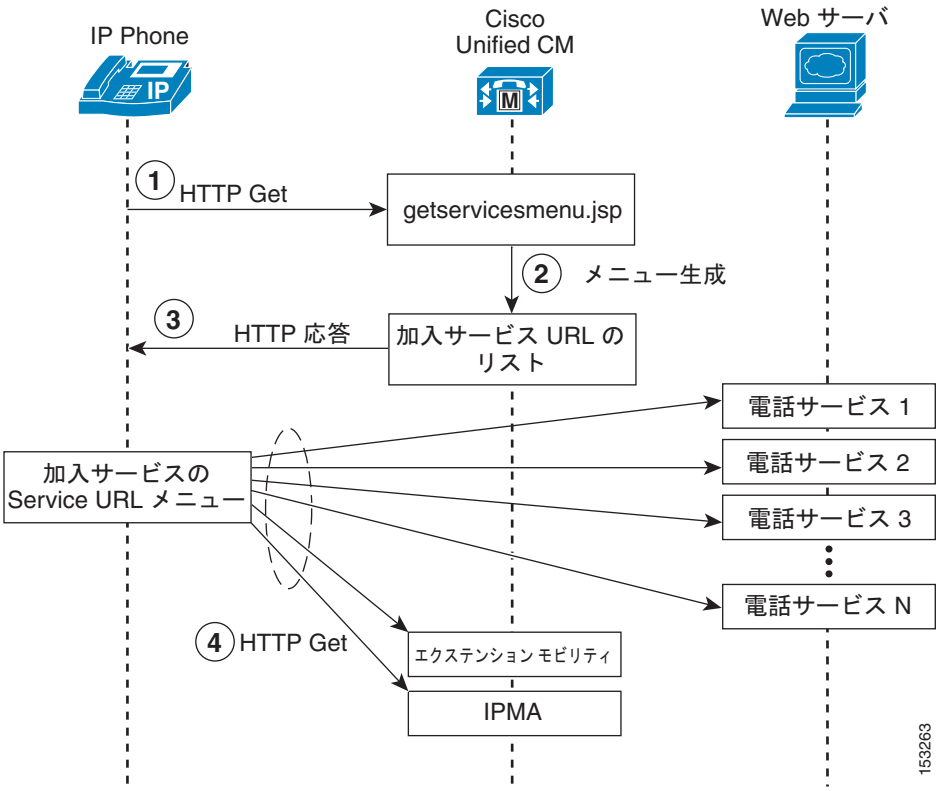
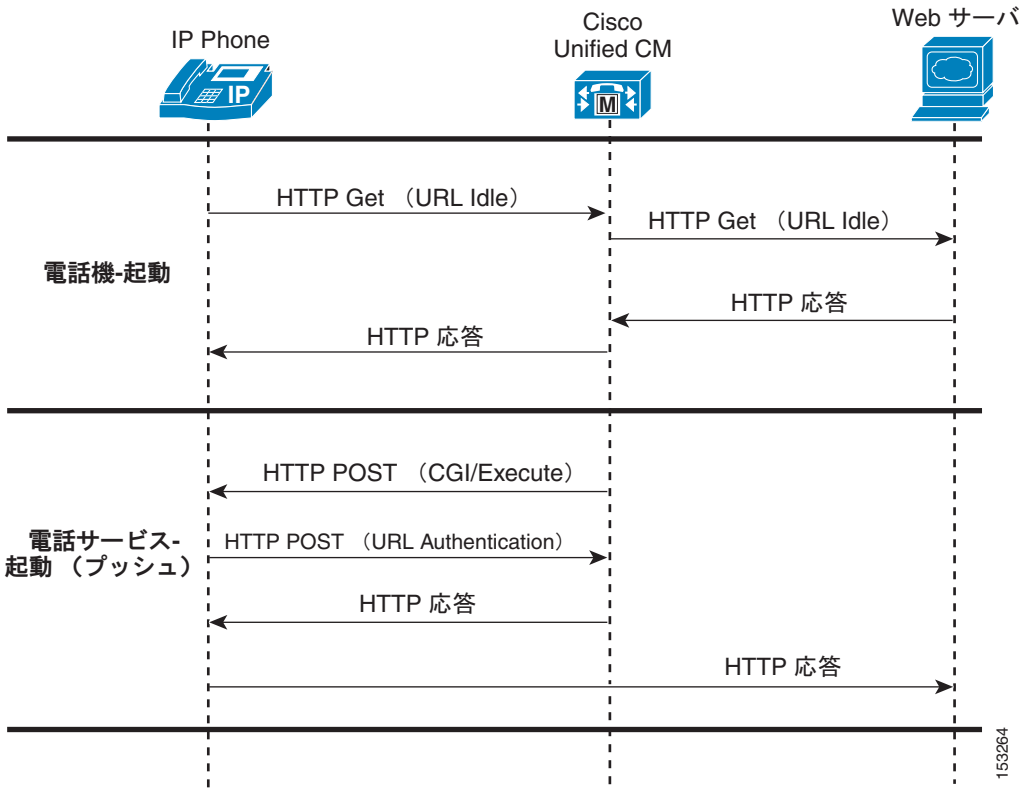


図 24-2 は、電話機起動と電話サービス起動の両方のプッシュ機能の例を示しています。電話機起動の機能の例で、電話機は、URL Idle Time に達したときに URL Idle パラメータで指定されるロケーションに HTTP GET を自動的に送信します（「IP Phone Service の エンタープライズ パラメータ」(P.24-3)を参照）。HTTP GET は、Cisco Unified CM を通じて外部 Web サーバに転送されます。この Web サーバは HTTP 応答を返し、この応答は Cisco Unified CM によって電話機にリレーされ、電話機は画面にテキストまたはイメージ（あるいはその両方）を表示します。

電話サービス起動のプッシュの例で、外部 Web サーバ上の電話サービスは電話機の Web サーバに対して、Common Gateway Interface（CGI）または Execute 呼び出しで HTTP POST を送信します。CGI または Execute 呼び出しを実行する前に、電話機は URL Authentication パラメータで指定されるプロキシ認証サービスを使用して要求を認証します（「IP Phone Service の エンタープライズ パラメータ」(P.24-3)を参照）。このプロキシ認証サービスは、電話機に対する直接の要求を検証するための、電話機と Cisco Unified CM ディレクトリ間のインターフェイスを提供します。要求が認証された場合、Cisco Unified CM は電話機に HTTP 応答を転送します。次に、電話機の Web サーバは要求された処理を実行し、電話機は外部 Web サーバに HTTP 応答を返します。認証に失敗した場合、Cisco Unified CM は、HTTP 否定応答を転送し、電話機は要求された CGI または Execute 処理を実行しないで、HTTP 否定応答を外部 Web サーバに転送します。

図 24-2　電話機起動および電話サービス起動の IP Phone Service のアーキテクチャ



XML Services に加えて、[Service Category] が [Java MIDlet] の新しいサービスを作成できます。Java MIDlet タイプのサービスが起動されると、設定された Service URL には、MIDlet JAD ファイルを取得できる URL を含みます。アプリケーション サーバは JAD ファイルの要求を受信すると、そのサーバは適切な JAR ファイルを対応デバイスに返します。この対応デバイスでは、電話の MIDlet インストーラがダウンロードし、処理しまします。

Cisco IP Phone の Java MIDlet サポートの詳細については、http://www.cisco.com の Cisco IP Phone データ シートを参照してください。

（注）　電話機はその設定ファイルを TFTP を介してダウンロードした後、電話機はリストのサービスが変わっていないかどうか判断するためサービス設定を解析し、変わっている場合にはそのローカル（持続）サービス設定を更新します。任意の変更されたサービスが Java MIDlets（これら Java MIDlets は明示的にプロビジョニングされ、電話機に保存される）の場合は、次に、電話機は必要なインストール、アップグレード、ダウングレード、および設定ファイルにプロビジョニングされたものに応じる処理のアンインストールを順次案内します。MIDlet インストールが失敗の場合、電話機がその設定ファイルをチェックする次回（ブート、リセット、または再スタート時）に MIDlet インストールを再試行します。

管理者は、設定されたサービスの [Service Type] を [IP Phone Services]、[Directories]、または [Messages] のいずれかに指定する追加機能を使用できます。これは、ユーザが IP phone で新しいサービスにアクセスするため押すボタンを管理する柔軟性を管理者に与えます。新しいサービスはオプションとして Enterprise Subscriptions と同様に設定できます。これにより、それらサービスは個々の電話機ごとに加入を更新する必要がなく、自動的にすべての IP phone に表示されます。さらに、サービスは Unified CM データベースからそのサービスを削除する必要がなく有効にできたり無効にできたりします。

（注）　Missed Calls、Placed Calls、および Corporate Directory などのデフォルトのサービスも無効にできます。これは、管理者が Service URL で指定されたデフォルト サービスをもとにしてカスタム サービスを作成できるようにします。

IP Phone Service の冗長性

電話機のユーザに対して信頼性の高いサービスを確保するには、システムの障害時に冗長システムにシームレスに移行することにより、高レベルのシステムの可用性を維持する必要があります。

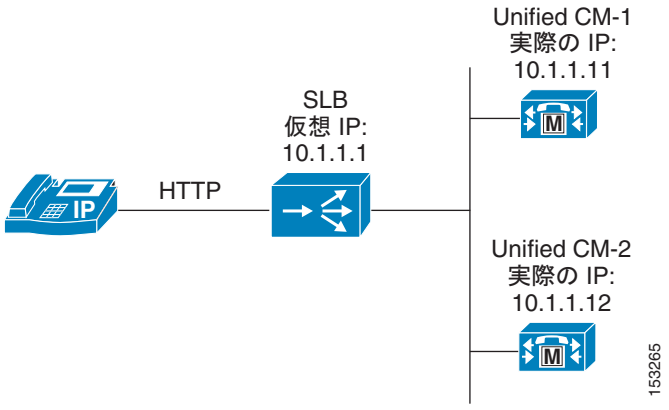
Services Provisioning で内部にセットされる場合、電話機は加入した電話サービスが設定された設定ファイルを受信し、これら（および対応するサービス URL）をフラッシュ メモリに保存します。これにより電話機は、最初に Cisco CallManager IP Phone service を参照せずにサービス URL に直接アクセスできます。Services Provisioning で内部にセットされる場合、Corporate および Personal Directories デフォルト サービス には電話機に組み込まれた追加レベルの冗長性もあります。これらサービスが選択された場合、電話機は適切な URL ストリング を使用して現在登録されている Unified CM に、HTTP メッセージの送信を試行します。したがって、電話機のデバイス プールの Unified CM Group の設定が、これらサービスの冗長性を提供します。

Services Provisioning が External URL 、または両方にセットされる場合、電話サービスのほとんどのバックエンド処理は Web サーバで発生しますが、電話機はやはり加入電話サービスのそれらサービス URL を通知するには Unified CM に依存します。図 24-1 および図 24-2 に示す IP Phone サービス機能のアーキテクチャおよびメッセージ フローでは、次の 2 つの主な障害のシナリオを検討する必要があります。

障害シナリオ 1：Cisco Unified CallManager の Cisco Unified IP Phone Service サーバの障害

この場合の冗長性は、図 24-3 に示すように、一種の Server Load Balancing（SLB; サーバ ロード バランシング）に依存します。この SLB では、1 つ以上の Cisco Unified CM サーバを指すために仮想 IP アドレスが使用されます。この仮想 IP アドレスは、URL Services パラメータの設定時に使用されます。このため、Cisco Unified CM サーバに障害が発生しても、電話機の Services ボタンが押されたときに、IP Phone Service 加入リストは電話機に正常に返されます。また、Cisco Unified CM サーバで実行される Extension Mobility および Unified CM Assistant などの電話サービスも、この方法によって冗長性を持つ可能性があります（「EM の冗長性」（P.24-14）および 「Unified CM Assistant の冗長性」（P.24-30）を参照）。

図 24-3　　電話サービスに冗長性を提供する方法



障害シナリオ 2：特定の IP Phone Service をホストしている外部 Web サーバの障害

このシナリオでは、Cisco Unified CM サーバへの接続は保持されますが、ユーザ加入電話サービスをホストしている Web サーバへのリンクに障害が発生します。Services ボタンが押されたときに IP Phone は引き続き Cisco Unified CM サーバにアクセスできるため、これは冗長性を提供するための比較的容易なシナリオです。この場合、IP Phone は Web サーバにアクセスする他の任意 HTTP クライアントに似ています。このため、（図 24-3 に示すような）SLB 機能を再び使用して、電話機から、ユーザ加入電話サービスをホストしている 1 つ以上の冗長 Web サーバに HTTP 要求を転送できます。

IP Phone Service のスケーラビリティ

Cisco Unified IP Phone サービスの大部分は、HTTP クライアントとして機能します。ほとんどの場合、加入サービスのロケーションへの転送サーバとしてだけ Cisco Unified CM が使用されます。Cisco Unified CM は電話サービスへの転送サーバとして機能するため、ユーザが Service キーを押して電話サービスを要求したときに、Cisco Unified CM へ与えるパフォーマンスの影響は最小限になります。

（注）　Extension Mobility および Unified CM Assistant 電話サービスの場合、Cisco Unified CM は転送サーバ以上の役割を果たすので、パフォーマンスへの影響を検討する必要があります。これらのアプリケーションの特定のパフォーマンスおよびスケーラビリティの考慮事項については、「エクステンション モビリティ（EM）」（P.24-9）および 「Unified CM Assistant」（P.24-18）の項を参照してください。

IP Phone はクライアントまたはサーバのいずれかであるため、IP Phone サービスで使用される必要帯域幅の推定は、Web 運用サーバにある HTTP コンテンツと同じテキストにアクセスする HTTP ブラウザの帯域幅の推定に似ています。

IP Phone Service のガイドラインと制限

統合 Extension Mobility および Unified CM Assistant アプリケーションの電話サービスを除き、IP Phone サービスは独立した Web サーバに存在する必要があります。Cisco Unified CM サーバで Extension Mobility および Unified CM Assistant 以外の電話サービスを実行することはサポートされていません。

エクステンション モビリティ（EM）

Cisco Extension Mobility（EM; エクステンション モビリティ）機能では、ユーザがその電話機にログインすることで、一時的に Cisco Unified IP Phone をユーザ個別の設定に設定 することが可能です。ユーザがログインすると、IP Phone には、回線番号、短縮ダイヤル、サービス リンク、およびその他のユーザ固有の電話機のプロパティなど、ユーザの個別のデバイス プロファイル情報が設定されます。たとえば、ユーザ X がデスクに向かって電話機にログインした場合は、そのユーザのディレクトリ番号、短縮ダイヤル、およびその他のプロパティがその電話機に表示されますが、ユーザ Y が別のときに同じデスクを使用した場合は、ユーザ Y の情報が表示されます。EM 機能では、認証されたユーザのデバイス プロファイルに従って電話機が動的に設定されます。このアプリケーションの利点は、電話機が EM をサポートしている限り、物理的な場所に関係なく、ユーザが Cisco Unified CM クラスタ内の任意の電話機で自分の内線番号に接続できることです。

EM Phone のサポート

次の Skinny Client Control Protocol（SCCP）電話機は EM をサポートしています。

- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7912G および 7912G-A
- Cisco Unified Wireless IP Phone 7920 および 7921G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7940G、7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7960G、7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G
- Cisco IP Communicator

次の Session Initiation Protocol（SIP）電話機は、EM をサポートしています。

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G

（注） EM は、SIP ロードを実行している Cisco Unified IP Phone 7905G、7912G、7940G、または 7960G ではサポートされません。

Cisco Unified CM および EM のサービス パラメータ

EM アプリケーションを有効にするには、システム管理者は Cisco Unified CM Serviceability インターフェイスからいくつかの Cisco Unified CallManager サービスをアクティブにし、起動する必要があります。また、EM サービス パラメータは、EM アプリケーションの動作を決定するための設定およびカスタマイズのオプションを提供します。

EM 用の Cisco Unified CallManager サービス

EM アプリケーションは Cisco Extension Mobility 機能サービスに依存します。これらのサービスは、Serviceability ページから手動でアクティブにする必要があります。

EM は次のネットワーク サービス にも依存します。これらのサービスは、インストール時にすべての Unified CM ノードで自動的にアクティブにされます。

- Cisco Extension Mobility Application
- Cisco CallManager Cisco IP Phone Services

Cisco エクステンション モビリティ アプリケーション サービスは、EM ユーザ電話機と Cisco エクステンション モビリティ サービスとの間のインターフェイスを提供します。また、Cisco エクステンション モビリティ アプリケーション サービスは、クラスタ内の変更通知インジケータにサブスクライ

ブして、アクティブな Cisco エクステンション モビリティ サービスがあるクラスタ内のノードのリストを維持します。クラスタ内の変更通知にサブスクライブすることによって、EM サービス パラメータに変更を加えた後に、Cisco Tomcat ネットワーク サービスおよび Cisco エクステンション モビリティ機能サービスを再起動する必要がなくなります。

Cisco Unified CallManager の Cisco Unified IP Phone Service サービスは、EM 電話サービスへのアクセスを提供するために必要です。EM 電話サービスの定義に使用される URL は、次のとおりです。

http://<*Unified-CM_Server_IP-Address*>/emapp/EMAppServlet?device=#DEVICENAME#

次の例を参考にしてください。

http://10.1.1.1/emapp/EMAppServlet?device=#DEVICENAME#

EM のサービス パラメータ

次の項目は、エクステンション モビリティ機能に関連する Cisco EM サービス パラメータの一部のリストです。

- Validate IP Address（デフォルト値 = False）

  このパラメータは、EM ログインおよびログアウトの制限を有効にするかどうかを示します。この値を False に設定した場合、ログインおよびログアウトの制限は有効にはなりません。この値を true に設定した場合、ログインおよびログアウトの制限は有効になり、EM は IP アドレスを検証するためにログインおよびログアウト要求の送信を試行します。

- Trusted List of IP Addresses（デフォルト値 = <ブランク>）

  このパラメータは、Validate IP Address を true に設定した場合にのみ有効になります。このパラメータは、IP アドレスおよびホスト名のセミコロン区切りストリングを有効にする 1024 文字サイズのテキスト フィールドです。EM は、このリストを EM ログインおよびログアウトの IP アドレス検証確認のソースとして使用を試みます。

- Allow Proxy（デフォルト値 = False）

  このパラメータは、Validate IP Address を true に設定した場合にのみ有効になります。このパラメータは、ログインおよびログアウト要求がプロキシを介して有効かどうかを示します。この値を False に設定した場合、EM はプロキシ サーバを介するすべてのログインおよびログアウト要求を拒否します。この値を true に設定した場合、EM はプロキシ サーバの IP アドレスの検証を EM ログインおよびログアウト要求をプロキシして試行します。

- EM Device Cache Size（デフォルト値 = 10000）

  このパラメータは、Validate IP Address を true に設定した場合にのみ有効になります。このパラメータは、EM によって保持されるデバイス キャッシュのサイズを設定するテキスト フィールドです。このパラメータに高い値を設定すると、EM に保存できるエントリ数が増加します。このパラメータに低い値を設定すると、保存できるエントリ数が減少します。

- Enforce Maximum Login Time（デフォルト値 = False）

  このパラメータは、Maximum Login Time に達したときに、EM ユーザを自動的にログアウトするかどうかを示します。デフォルトでは、この値は False に設定され、EM ユーザを自動的にログアウトしません。

- Maximum Login Time（デフォルト値 = 8:00）

  このパラメータは、EM ユーザが自動的にログアウトするまでにログイン状態を維持できる時間と分（*hh*:*mm*）を示します。Enforce Maximum Login Time パラメータを True に設定した場合にだけ、指定した時刻に自動ログアウトが行われます。

- Multiple Login Behavior（デフォルト値 = Multiple Logins Not Allowed）

  このパラメータは、同時に複数のデバイスにログインすることを EM ユーザに許可するかどうかを示します。デフォルトでは、1 人のユーザの複数のログインは許可されず、1 台のデバイスにログオンしているときに別のデバイスにログインしようとすると、次のメッセージが表示されます。

  Login Unsuccessful
  [25]User logged in elsewhere.

- Remember the Last User Logged In（デフォルト値 = False）

  このパラメータは、デバイスへのログインに前回使用されたユーザ ID を、次回同じデバイスにログインしようとするときまで記録するかどうかを示します。この値を True に設定すると、前回のログインに使用されたユーザ ID 情報は Cisco Unified CM データベースのテーブルに次回の効率的な取得のため保存されます。次回のログイン試行時に、電話機のログイン画面の UserID フィールドには、保存されたユーザ ID の値があらかじめ表示されます。

- Clear the call log（デフォルト値 = False）

  このパラメータは、EM ログインおよびログアウト時に、Directories ボタン メニューに指定されたコール ログをクリアするかどうかを指定します。このパラメータは、Missed Calls、Received Calls、および Placed Calls のログに影響を与えます。この値を True に設定した場合、これらのログはログインおよび手動ログアウト時にクリアされます。

  例外として、ユーザを自動的にログアウトする場合、これらのログはクリアされません。したがって、Maximum Login Time に達してユーザを電話機から自動的にログアウトするときに、ログはクリアされません（Enforce Maximum Login Time が True に設定されている場合）。同様に、Cisco Unified CM 管理者が、電話機またはデバイスの設定画面の Extension セクションで Log Out ボタンをクリックした場合も、ログはクリアされません。

Extension Mobility サービス パラメータの全リストについては、「*Cisco Extension Mobility*」章を参照してください。次の Web サイトで入手できる『*Cisco Unified Communications Manager Features and Services Guide*』の

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

EM のアーキテクチャ

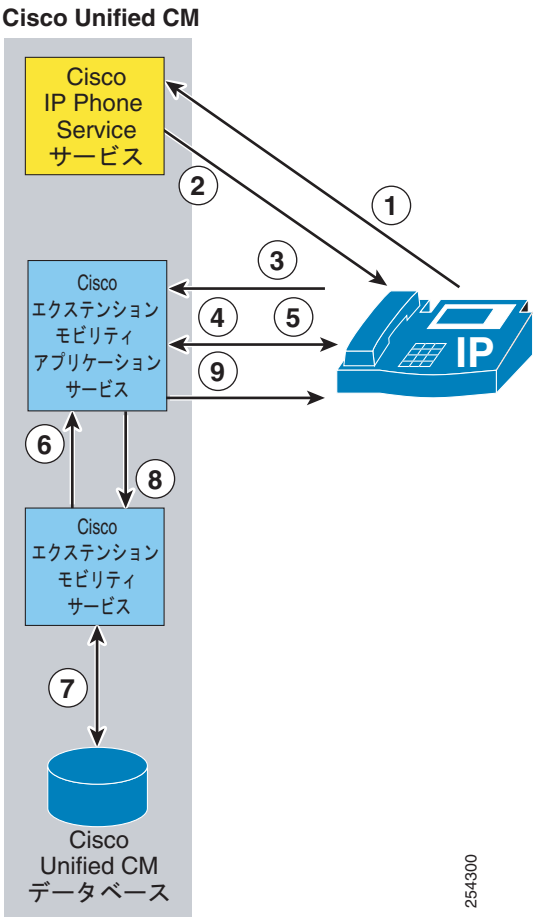
図 24-4 は、EM アプリケーションのメッセージ フローとアーキテクチャを示しています。電話機のユーザが EM アプリケーションにアクセスする場合、次の一連のイベントが発生します。

1. ユーザが電話機の Services ボタンを押すと、Enterprise Parameter 設定ページの URL Services パラメータで指定した URL へのコールが生成されます（「IP Phone Service の エンタープライズ パラメータ」（P.24-3）を参照）（図 24-4 のステップ 1 も参照）。
2. HTTP/XML コールが IP Phone Service に対して生成され、このコールはユーザの電話機が加入しているすべてのサービスのリストを返します（図 24-4 のステップ 2 を参照）。

（注）　Services Provisioning エンタープライズ パラメータが内部に設定されている場合、ステップ 1 および 2 はバイパスされます。一方、Services Provisioning が外部 URL または両方に設定されている場合、ユーザが回線ボタンまたは短縮ダイヤル ボタンを押して、Extension Mobility Application サービスへの直接コールを生成できるように、Service URL ボタンはユーザの電話機で EM の設定ができます。ステップ 1 および 2 もバイパスされます。

3. 次に、ユーザはエクステンション モビリティ電話サービスのリストを選択します。この選択によって、電話機と Cisco エクステンション モビリティ サービス間のインターフェイスの役割を果たすエクステンション モビリティ アプリケーション サービスに対して HTTP コールが生成されます（図 24-4 のステップ 3 を参照）。
4. 次に、エクステンション モビリティ アプリケーション サービスは、ユーザ ログイン クレデンシャル（ユーザ ID および PIN）を要求している電話機に XML 応答を返すか、またはユーザがすでにログインしている場合は、ユーザに電話機からログオフするかどうかを尋ねる応答を返します（図 24-4 のステップ 4 を参照）。
5. ユーザがログインしようとしている場合、そのユーザは電話機のキーパッドを使用して有効なユーザ ID および PIN を入力する必要があります。ユーザが Submit ソフトキーを押した後に、入力したユーザ ID および PIN を含む応答が、エクステンション モビリティ アプリケーション サービスに返されます（図 24-4 のステップ 5 を参照）。
6. 次に、エクステンション モビリティ アプリケーションは、このログイン情報を エクステンション モビリティ サービスに転送します。このサービスは、Cisco Unified CM データベースと対話して、ユーザのクレデンシャルを検証します（図 24-4 のステップ 6 を参照）。
7. ユーザのクレデンシャルの検証に成功したときに、エクステンション モビリティ サービスも Cisco Unified CM データベースと対話して、適切なユーザ デバイス プロファイルを読み取って選択し、デバイスのプロファイルに基づいて電話機の設定に必要な変更を書き込みます（図 24-4 のステップ 7 を参照）。
8. これらの変更が加えられると、エクステンション モビリティ サービスは、エクステンション モビリティ アプリケーション サービスに成功応答を返します（図 24-4 のステップ 8 を参照）。
9. 次にエクステンション モビリティ アプリケーション サービスは電話機にリセット メッセージを送信し、電話機はリセットされ、新しい電話設定を受け入れます（図 24-4 のステップ 9 を参照）。

図 24-4　EM アプリケーションのアーキテクチャとメッセージ フロー



EM の冗長性

図 24-4 に示す EM アーキテクチャに従って、Cisco Unified CM データベースの読み取りおよび書き込みが要求されます。EM はユーザに面した機能であって、データベースの書き込みは、EM がサブスクライバ ノードで実行できるかどうかに関係します。したがって、Unified CM パブリッシャが利用できない場合、その場合でも EM ログインおよびログアウトはできます。

冗長性の見地から、次の 3 個のコンポーネント レベルの冗長性ついては、全面的な EM の復元性を得るよう検討する必要があります。

- Cisco CallManager Cisco IP Phone Services

  （「IP Phone Service の冗長性」（P.24-8）を参照）。

- EM IP 電話サービス

  EM IP 電話サービスは、電話機のログインおよびログアウトをするために、ユーザによって IP 電話サービス メニュー（または、もう一つの選択肢として、サービス回線ボタンから）から選択されたサービスです。この電話サービスは、特定の Unified CM ノードで実行している Cisco Extension Mobility Application サービス を指します。前にも示したように、Cisco EM Application サービスはユーザ（または、電話機）と Cisco Extension Mobility サービス間のインターフェイスの役割を提供します。EM IP 電話サービスでは、単一の IP アドレスまたは ホスト名だけを指すことができます。

- Cisco Extension Mobility サービス

  Cisco Extension Mobility サービスには、EM ログインおよびログアウトが必要です。このサービスは Cisco EM Application サービスからユーザ クレデンシャルを取得し、次にローカル Unified CM データベースへの書き込みおよびローカル Unified CM データベースから読み込みをします。

Cisco CallManager Cisco IP Phone Services（または、URL Services）と EM IP 電話サービス コンポーネントに冗長性を持たせるため、複数の Unified CM ノードに対する EM ログインおよびログアウト要求を処理するフロント エンドとして Server Load Balancer（SLB; サーバ ロード バランサ）を使用することをお勧めします。この設計では、図 24-3 に示すとおり、SLB の機能によって仮想 IP アドレスまたは Domain Name System（DNS; ドメイン ネーム システム）による解決可能なホスト名が提供されます。この仮想 IP アドレスまたはホスト名が、IP 電話からの EM ログインおよびログアウト要求の宛先アドレスとして使用されます。SLB は、Cisco EM Application サービスが有効なサブスクライバ ノードの実際の IP アドレスにこれらの EM 要求を分配するように設定されます。

Cisco Application Control Engine（ACE）または Cisco IOS SLB 機能など多くの SLB デバイスは、障害発生時の複数のサーバと自動転送要求のステータスを監視するように設定できます。URL Services および EM IP 電話サービスの SLB 仮想 IP アドレス（または DNS ホスト名）を使用することによって、ノードの障害発生時にも両方のコンポーネントを確実に使用できるので、EM ログインおよびログアウトが継続されます。

（注）　クラスタ内の複数のサブスクライバ ノードでは、Cisco EM Application サービスを有効にして冗長性を持たせることができますが、クラスタ内で所定の時間にログインおよびログアウト要求をアクティブに処理できるサブスクライバ ノードは 2 台に限られます。SLB デバイス設定では、この設計基準をサポートする必要があります。

（注）　複数の IP リストを持つ DNS レコードを使用した冗長な設計はお勧めできません。DNS 要求に対して複数の IP アドレスが戻ると、電話はタイムアウトを待ってから次にリストされた IP アドレスを試します。ほとんどの場合は、この動作よりエンド ユーザにとって許容できない遅延が発生します。また、このために Cisco EM アプリケーション サービスが有効である複数のサブスクライバ ノードによってログインおよびログアウト要求が処理される場合がありますが、そのような処理はサポートされていません。

Cisco Extension Mobility Application サービスはクラスタの変更通知にサブスクライブするので、Cisco Extension Mobility サービスがアクティブになっているクラスタ内の全ノードのリストが維持されます。したがって、Cisco Extension Mobility サービス コンポーネントに冗長性を提供するには、クラスタ内の複数のノードでこのサービスを実行する必要があり、Cisco Extension Mobility Application サービスは Cisco Extension Mobility サービスを実行しているいずれかのノードに自動フェールオーバー機能を提供します。

EM Security

Cisco Unified CM releases 7.0 および 6.1（3）以降では、EM 機能に、要求のソース IP アドレスを検証することによって EM ログインおよびログアウト要求にオプション レベルのセキュリティを提供します。デフォルトでは、EM はこの要求の検証を実行しません。したがって、EM セキュリティを有効にするには、管理者はクラスタ全体のサービス パラメータ Validate IP Address を true に設定する必要があります。このパラメータが有効になった時点で、EM サービス はEM ログインおよびログアウト要求を検証するため表示されている順に次の 3 個のソースを使用します。

1. 信頼できるデバイスのキャッシュ

   初期化時に、EM サービスはすべての EM 対応デバイスに対して最初に Unified CM データベースを照会します。次に、Unified CM に登録されているデバイスの IP アドレス マッピングを取得するため、Real-Time Information Server (RIS) Data Collector サービスを照会します。キャッシュに含まれているデバイスから IP アドレスへのマッピングの数は EM Device Cache Size サービス パラメータで指定されたキャッシュのサイズによって制限されます。

2. IP サービス パラメータの信頼できるリスト

   このサービス パラメータは、信頼できる IP アドレスのセミコロン区切りリストを管理者が提供することができます。これは、組織がログインおよびログアウト要求をユーザに代わって実行する別個のアプリケーションまたはプロキシ サーバを検証できます。

3. 新規 RIS Data Collector の照会

   信頼できるデバイスのキャッシュまたは IP サービス パラメータの信頼できるリストに一致するものが無い場合、要求しているデバイスに対する特定の照会が RIS Data Collector サービスに対して行われます。キャッシュ作成後にデバイスが登録されている場合、またはキャッシュがフル状態の場合、ログインおよびログアウト要求は検証できます。

ログインまたはログアウト要求が受信されるたびに、IP アドレス確認のための EM サービスが有効である場合、EM は最初に信頼できるデバイスのキャッシュへデバイスから IP マッピングの試行を行い、IP アドレスの検証を実行します。そのデバイスのマップされている IP アドレスがログインまたはログアウト要求のソース IP アドレスと一致する場合、その要求は実行されます。キャッシュにデバイスが見つからない場合、または IP アドレスが一致しない場合は、EM サービスは IP サービス パラメータの信頼できるリストをチェックします。ログインまたはログアウトを要求するソース IP アドレスがこのリストで探せた場合、要求は実行されます。IP アドレスがここで検証されない場合、次に EM サービスは要求するデバイスの新しい RIS Data Collector 照会を作成します。この照会への応答にログインまたはログアウトを要求するソース IP アドレスを含む場合、EM はログインを実行し、EM デバイス キャッシュのサイズを超えない場合には、この device-to-IP マッピングを信頼できるデバイスのキャッシュに追加します。このステップ中に IP アドレスが検証されない場合、要求するデバイスでエラーが表示されます。

EM ログインおよびログアウト HTTP 要求を処理する Web プロキシを実装する組織は、Allow Proxy サービス パラメータを true に設定する必要があります。プロキシ サーバは、HTTP 要求を転送している間に、そのホスト名と共に HTTP ヘッダーの via-field をセットします。デバイスと Unified CM の間に複数のプロキシ サーバがある場合で、すべてのサーバで要求が転送される場合は、次に HTTP ヘッダーの via-field にはフォワーディング パスで各プロキシ サーバのホスト名のカンマ区切りリストが必要になります。Allow Proxy サービス パラメータは、true に設定されている場合、Web プロキシを介して受信した EM ログインおよびログアウトが可能です。また、プロキシされた EM 要求はプロキシ サーバのソース IP アドレスを使用する場合、その IP アドレスは IP サービス パラメータの信頼できるリストにも設定する必要があります。

EM のガイドラインと制限

次のガイドラインと制限は、Cisco Unified CM テレフォニー環境内の EM の配置と動作に関連して適用されます。

- EM は、単一の Cisco Unified CM クラスタ内だけでサポートされます。

  現在、クラスタ間で EM はサポートされていません。ある Cisco Unified CM クラスタの EM ユーザは、2 番目のクラスタでそのユーザに対して別個のデバイス プロファイルおよびユーザ ID が作成されない限り、2 番目のクラスタで電話機にはログオンできません。

- EM ユーザは、Automated Alternate Routing（AAR）または Voice over PSTN（VoPSTN）、あるいはその両方の配置モデルが使用されている場合、クラスタ内のロケーションまたはサイト間で移動できません。

  EM 機能は、コール ルーティングを IP ネットワークの使用に依存します。E.164 公衆網番号は静的で、公衆網はホーム サイトからの EM ユーザのディレクトリ番号（DN）の移動を考慮に入れられないため、公衆網を通じたコール ルーティングにはより多くの問題が伴います。AAR は、VoPSTN 配置モデルと同様に、コール ルーティングを公衆網に依存します。いずれの場合も、ロケーションおよびサイト間の EM ユーザの移動は、ユーザの移動するすべてのサイトが同じ AAR グループに属する場合にだけサポートされます。詳細については、「エクステンション モビリティ」（P.10-94）を参照してください。

- Extension Mobility Service の再起動またはサービスを実行中のノードは自動ログアウトに影響を与えます。

  Cisco Extension Mobility を停止するまたは再起動する場合、システムは最大ログイン間隔が経過後のすでにログインされているユーザを自動ログアウトしません。これら電話機は手動でログアウトする必要があります。

EM のパフォーマンスとキャパシティ

Cisco EM アプリケーションは、次のクラスタ全体のログインおよびログアウトのキャパシティをサポートしています。

- Cisco MCS-7845H2/I2 サーバは、1 分あたり最大 250 回の順次ログインまたはログアウト（あるいはその両方）をサポート
- Cisco MCS-7835H2/I2 サーバは、1 分あたり最大 235 回の順次ログインまたはログアウト（あるいはその両方）をサポート
- Cisco MCS-7825H2/I2 サーバは、1 分あたり最大 200 回の順次ログインまたはログアウト（あるいはその両方）をサポート

（注）　旧サーバ モデルを配置するとキャパシティが低下します。

Cisco Extension Mobility ログインおよびログアウト機能は、ログイン/ログアウトのクラスタ キャパシティを増加するためにサブスクライバ ノードのペアに分散できます。EM 負荷を 2 つのサブスクライバ ノード間で均等に分散するには、電話機を 2 つのグループに分割し、1 つのサブスクライバ ノードを指しているある EM 電話サービスに加入している電話機の 1 つのグループと 2 番目のサブスクライバ ノードを指している 2 番目の EM 電話サービスに加入している電話機の別のグループを共に備えます。EM 負荷がこの方法で分散され、2 つの MCS-7845H2/I2 サーバの間で均等な場合、1 分あたりクラスタ全体のセキュリティは最大で 375 回の順次ログインまたはログアウト（あるいはその両方）になります。

（注）　クラスタ内の複数のサブスクライバ ノードで Cisco EM Application サービスを使用可能にして、冗長性を持たせることができます。ただし、キャパシティを高めるため、クラスタ内で所定の時間に EM ログインおよびログアウト要求をアクティブに処理できるサブスクライバ ノードは 2 台に限られます。

（注）　EM セキュリティの有効化はパフォーマンスを低下しません。

EM 相互作用：Unified CM Assistant、Attendant Console、および WebDialer

Unified CM Assistant Manager ユーザおよびアテンダント コンソール ユーザは、それぞれの電話機へのログインに EM を使用できます。このような他のアプリケーションでの EM の使用に関する詳細とおよびガイドラインについては、「Unified CM Assistant と EM の相互作用」（P.24-35）を参照してください。

WebDialer ユーザも、EM を使用してそれぞれの電話機にログオンできます。詳細については、「WebDialer と EM の相互作用」（P.24-62）を参照してください。

Unified CM Assistant

Cisco Unified CM Assistant は、Unified CM に統合されたアプリケーションです。これを使用すると、1 人または複数のマネージャに代わってアシスタントが着信コールを処理できます。Unified CM Assistant Console デスクトップ アプリケーションまたは Unified CM Assistant Console 電話サービスをアシスタントの電話機で使用すると、アシスタントが手早くマネージャの状態を確認し、コールをどうするかを決定できます。自分の電話機のソフトキーおよびサービス メニューを使用するか、または PC インターフェイスを介してキーボード ショートカット、ドロップダウン メニューを使用するか、あるいはマネージャのプロキシ回線へのコールのドラッグ アンド ドロップすることによって、アシスタントはコールを処理できます。

Unified CM Assistant Phone のサポート

次の SCCP 電話機が Unified CM Assistant をサポートしています。

- Cisco Unified IP Phone 7940G、7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7960G、7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G

次の SIP 電話機が Unified CM Assistant をサポートしています。

- Cisco Unified IP Phone 7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G

（注）　Cisco Unified IP Phone Expansion Module 7914 は、Cisco Unified IP Phone 7960G、7961G、7961G-GE、7962G、7965G、7970G、7971G-GE、または 7975G のすべての電話機でサポートされています。電話機あたり最大 2 つの Cisco 7914 Module がサポートされています。

Cisco Unified CM および Unified CM Assistant のサービス パラメータ

Unified CM Assistant アプリケーションを有効にするには、システム管理者は Cisco Unified Serviceability インターフェイスから複数の Cisco Unified CM 機能サービスをアクティブにし、起動する必要があります。また、Unified CM Assistant サービス パラメータは、Unified CM Assistant アプリケーションとサービスの動作を決定するための設定およびカスタマイズのオプションを提供します。

Unified CM Assistant 用の Cisco Unified CM サービス

Unified CM Assistant アプリケーションは次の機能サービスに依存します。これらのサービスは、Serviceability ページから手動でアクティブにする必要があります。

- Cisco IP Manager Assistant
- Cisco CTIManager

Unified CM Assistant アプリケーションは、Cisco IP Phone Services ネットワーク サービスの Cisco CallManager にも依存します。このアプリケーションは、インストール時に Unified CM で自動的にアクティブになります。

Cisco CM IP Manager Assistant サービスは、Cisco CTIManager サービスおよび Unified CM データベースと対話すると共に、Unified CM Assistant Console アプリケーションおよび Manager Configuration アプリケーション用のインターフェイスを提供します。Cisco CTIManager サービスは、電話とコールの制御のために Cisco CallManager サービス および Cisco IP Manager Assistant サービスを相互接続します。

Cisco Unified IP Phone Service は、マネージャおよびアシスタントの電話機から Unified CM Assistant 電話サービスへのアクセスを提供するために必要です。Unified CM Assistant 電話サービスを定義するために使用される URL は、次のとおりです。

http://<*Server_IP-Address*>:8080/ma/servlet/MAService?cmd=doPhoneService&Name=#DEVICENAME#

（ここで、<*Server_IP-Address*> は、クラスタ内のいずれかのノードの IP アドレスです）

（注）　シスコは、Unified CM Assistant 電話サービスの 2 つのインスタンスを設定することをお勧めします。1 つの Unified CM Assistant 電話サービス インスタンスは、主 Unified CM Assistant サーバを指して、別の電話サービス インスタンスはバックアップ Unified CM Assistant サーバを指します。この方法で主電話サービスと従電話サービスを設定することによって、補助電話コンソールの冗長性を提供できます。詳細については、「デバイスと到達可能性の冗長性」（P.24-32）を参照してください。

Unified CM Assistant のサービス パラメータ

次の項目は、Unified CM Assistant 機能に関連する Cisco IP Manager Assistant サービス パラメータの一部のリストです。

- CTIManager Connection Security Flag（デフォルト値 = Non Secure）

  このパラメータは、Cisco IP Manager Assistant サービスと CTIManager との間でセキュアな Transport Layer Security（TLS; トランスポート レイヤ セキュリティ）接続を使用するかどうかを決定します。有効な場合は、アプリケーション ユーザの IPMASecureSysUser のインスタンス ID に対して設定した Certificate Authority Proxy Function（CAPF）プロファイルを使用して、セキュアな接続が設定されます。このインスタンス ID は、サービス パラメータの CAPF Profile Instance ID for Secure Connection to CTIManager で指定する必要があります。

  （注）　アプリケーション ユーザの IPMASecureSysUser は、インストール時に自動的に作成されるシステム アカウントです。削除できません。

- CAPF Profile Instance ID for Secure Connection to CTIManager（デフォルト値 = <None>）

  CAPF Profile Instance ID は、IPMASecureSysUser アプリケーション ユーザに対して、Unified CM Assistant サーバと CTIManager との間で確立される TLS 接続またはインスタンスを識別するために使用される、数値または文字（あるいはその両方）の一意のストリングです。CTI Manager Connection Security Flag パラメータを True に設定した場合、このパラメータに値を設定する必要があります

- CTIManager (Primary) IP Address（デフォルト値 = <ブランク>）

  このパラメータは、Cisco Unified CM Assistant サーバがコールの処理に使用するプライマリ CTIManager の IP アドレスを指定します。プライマリ CTIManager は、各 Unified CM Assistant サーバで設定できます。

- CTIManager (Backup) IP Address（デフォルト値 = <ブランク>）

  このパラメータは、プライマリ CTIManager がダウンしている場合に、この Cisco Unified CM Assistant サーバがコールの処理に使用するバックアップ CTIManager の IP アドレスを指定します。バックアップ CTIManager は、各 Unified CM Assistant サーバで設定できます。

- Cisco IPMA Server（Primary）IP Address（デフォルト値 = <ブランク>）

  このパラメータは、プライマリ Cisco Unified CM Assistant サーバの IP アドレスを指定します。これはクラスタ全体のパラメータで、プライマリとバックアップという 2 つの Unified CM Assistant サーバ だけを設定できます。

- Cisco IPMA Server（Backup）IP Address（デフォルト値 = <ブランク>）

  このパラメータは、バックアップ Cisco Unified CM Assistant サーバの IP アドレスを指定します。バックアップ サーバは、プライマリ Unified CM Assistant サーバに障害が発生した場合に、Unified CM Assistant 機能を提供します。これはクラスタ全体のパラメータです。

- Cisco Unified IPMA Assistant Console Heartbeat Interval（デフォルト値 = 30）

  このパラメータは、IPMA サーバが、各 Unified CM Assistant Console デスクトップ アプリケーションにキープアライブ メッセージ（一般に、ハートビートと呼ばれる）を送信する頻度を秒単位で指定します。Unified CM Assistant Console デスクトップ アプリケーションは、指定された時間が経過するまでにプライマリ サーバからキープアライブ メッセージを受信しないと、バックアップ IPMA サーバへのフェールオーバーを開始します。

- Cisco IPMA Assistant Console Request Timeout（デフォルト値 = 30）

  このパラメータは、Unified CM Assistant Console デスクトップ アプリケーションが、アクティブまたはプライマリ IPMA サーバからの応答の受信を待機する時間を秒単位で指定します。

- Cisco IPMA RNA Forward Calls（デフォルト値 = False）

  このパラメータを True に設定した場合、Cisco IPMA RNA Timeout パラメータで指定される RNA 値が経過すると、アシスタントの電話機へのコールを、マネージャの次の応答可能なアシスタントに無応答時（RNA）転送することができます。このパラメータを False に設定した場合、コールは最初のアシスタントをいつまでも呼び続けるか、または、ボイスメール プロファイルが設定されているときはボイスメールにコールが転送されます。

- Cisco IPMA RNA Timeout（デフォルト値 = 10）

  このパラメータは、Cisco Unified CM Assistant サーバが、応答のないコールを次の応答可能なアシスタントに RNA 転送するまで待機する時間を秒単位で指定します。RNA 転送は、Cisco IPMA RNA Forward Calls パラメータを True に設定した場合にだけ発生します。回線でボイスメール プロファイルが設定され、他のアシスタントを利用できない場合は、タイムアウトするとボイスメールにコールが転送されます。

Advanced Service Parameters

次のサービス パラメータは、デフォルトでは隠れている、**Advanced** ボタンまたはアイコンをクリックした時のみ使用できます。

- Enable Multiple Active Mode（デフォルト値 = False）

  このパラメータを True に設定した場合、Unified CM Assistant キャパシティが増加したため、複数の Unified CM Assistant ペアを設定できます。

- Pool 2: Cisco IPMA Server（Primary）IP Address（デフォルト値 = <ブランク>）

  このパラメータは、Pool 2 でプライマリ Cisco Unified CM Assistant サーバの IP アドレスを指定します。これはクラスタ全体のパラメータで、このプールにはプライマリとバックアップという 2 つの Unified CM Assistant サーバだけを設定できます。

- Pool 2: Cisco IPMA Server（Backup）IP Address（デフォルト値 = <ブランク>）

  このパラメータは、Pool 2 でバックアップ Cisco Unified CM Assistant サーバの IP アドレスを指定します。バックアップ サーバは、Pool 2 でプライマリ Unified CM Assistant サーバに障害が発生した場合に、Unified CM Assistant サービスを提供します。これはクラスタ全体のパラメータです。

- Pool 3: Cisco IPMA Server（Primary）IP Address（デフォルト値 = <ブランク>）

  このパラメータは、Pool 3 でプライマリ Cisco Unified CM Assistant サーバの IP アドレスを指定します。これはクラスタ全体のパラメータで、このプールにはプライマリとバックアップという 2 つの Unified CM Assistant サーバだけを設定できます。

- Pool 3: Cisco IPMA Server（Backup）IP Address（デフォルト値 = <ブランク>）

  このパラメータは、Pool 3 でバックアップ Cisco Unified CM Assistant サーバの IP アドレスを指定します。バックアップ サーバは、Pool 3 でプライマリ Unified CM Assistant サーバに障害が発生した場合に、Unified CM Assistant サービスを提供します。これはクラスタ全体のパラメータです。

Unified CM Assistant サービス パラメータの全リストについては、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Features and Services Guide*』の Unified CM Assistant 情報を参照してください。

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

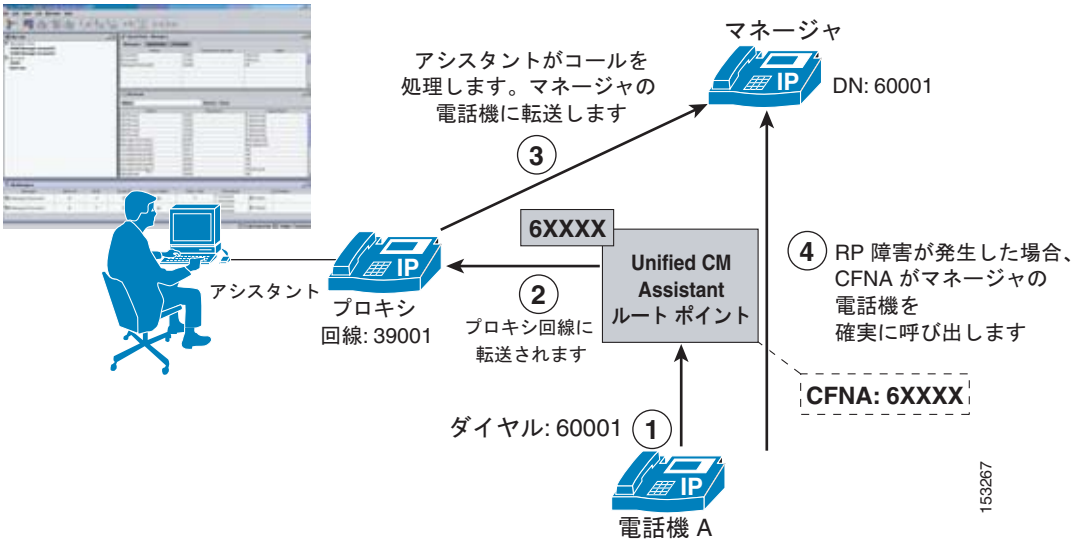
Unified CM Assistant の機能とアーキテクチャ

Unified CM Assistant アプリケーションは、プロキシ回線モードとシェアドライン モードの 2 つのモードで動作できます。各モードの動作と機能は異なり、それぞれに長所と短所があります。どちらのモードも、1 つのクラスタ内で設定できます。ただし、同一のアシスタントでモードを混合させることはできません。1 人以上のマネージャにサポートを提供している 1 人のアシスタントは、シェアドライン モードまたはプロキシ回線モードのいずれかでこれらのマネージャをサポートできます。

Unified CM Assistant のプロキシ回線モード

図 24-5 は、プロキシ回線モードでの Unified CM Assistant の単純なコール フローを示しています。この例で、電話機 A は、ディレクトリ番号（DN）60001 でマネージャの電話機をコールします（ステップ 1）。CTI/Unified CM Assistant Route Point（RP）は、6XXXX に設定された DN に基づいてこのコールを代行受信します。次に、マネージャの DN に基づいて、コールはルート ポイントにより、アシスタントの電話機上のマネージャのプロキシ回線（DN : 39001）に転送されます（ステップ 2）。次に、アシスタントはコールに応答または処理し、必要に応じてマネージャの電話機にコールを転送します（ステップ 3）。Unified CM Assistant アプリケーションまたは Unified CM Assistant RP に障害が発生した場合に、マネージャの DN へのコールがマネージャの電話機を直接呼び出すよう、RP の Call Forward No Answer（CFNA）の 6XXXX 設定による呼び出しメカニズムが存在します（ステップ 4）。

図 24-5　　Unified CM Assistant のプロキシ回線モード

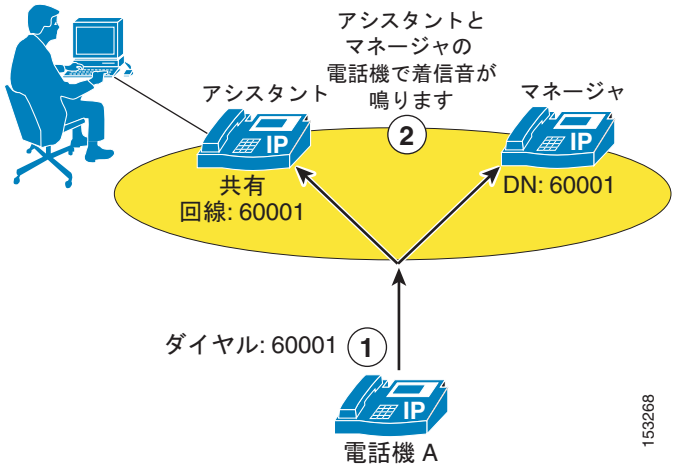


（注）　図 24-5 に示す CFNA による呼び出しメカニズムでは、Unified CM Assistant RP のディレクトリ番号設定ページの Forward No Answer Internal フィールドと Forward No Answer External フィールドの両方で、Unified CM Assistant RP ディレクトリ番号と同じ集約番号桁の設定が必要です。また、これらの各コール転送パラメータの Calling Search Space（CSS; コーリング サーチ スペース）フィールドは、Unified CM Assistant RP または Unified CM Assistant アプリケーションに障害が発生した場合に マネージャの電話機の DN に到達できるように、マネージャの電話機の DN が設定されたパーティションを含むコーリング サーチ スペースで設定する必要があります。

Unified CM Assistant のシェアドライン モード

図 24-6 は、シェアドライン モードでの Unified CM Assistant の単純なコール フローを示しています。この例で、電話機 A は、アシスタントの電話機のシェアドラインであるディレクトリ番号（DN）60001 でマネージャの電話機をコールします（ステップ 1）。このコールは、アシスタントとマネージャの電話機の両方で着信音を鳴らします。ただし、マネージャが Do Not Disturb（DND）機能を呼び出した場合、着信音が鳴るのはアシスタントの電話機だけになります（ステップ 2）。

図 24-6　Unified CM Assistant のシェアドライン モード



Unified CM Assistant のシェアドライン モードでは、マネージャの電話機へのコールを代行受信するために Unified CM Assistant RP は必要ありません。ただし、マネージャの電話機および Unified CM Assistant Console デスクトップ アプリケーションの Do Not Disturb（DND）機能は、Cisco IP Manager Assistant および Cisco CTIManager サービスに依存します。さらに、Unified CM Assistant シェアドライン モードでは、コール フィルタリング、コール代行受信、アシスタント選択、Assistant Watch などの機能は使用できません。

Unified CM Assistant のアーキテクチャ

Unified CM Assistant アプリケーションのアーキテクチャは、その機能と同様に、そのアーキテクチャについても理解することが重要です。図 24-7 は、Unified CM Assistant のメッセージ フローとアーキテクチャを示しています。Unified CM Assistant のマネージャおよびアシスタント ユーザに対して Unified CM Assistant を設定すると、次の一連の対話とイベントが発生します。

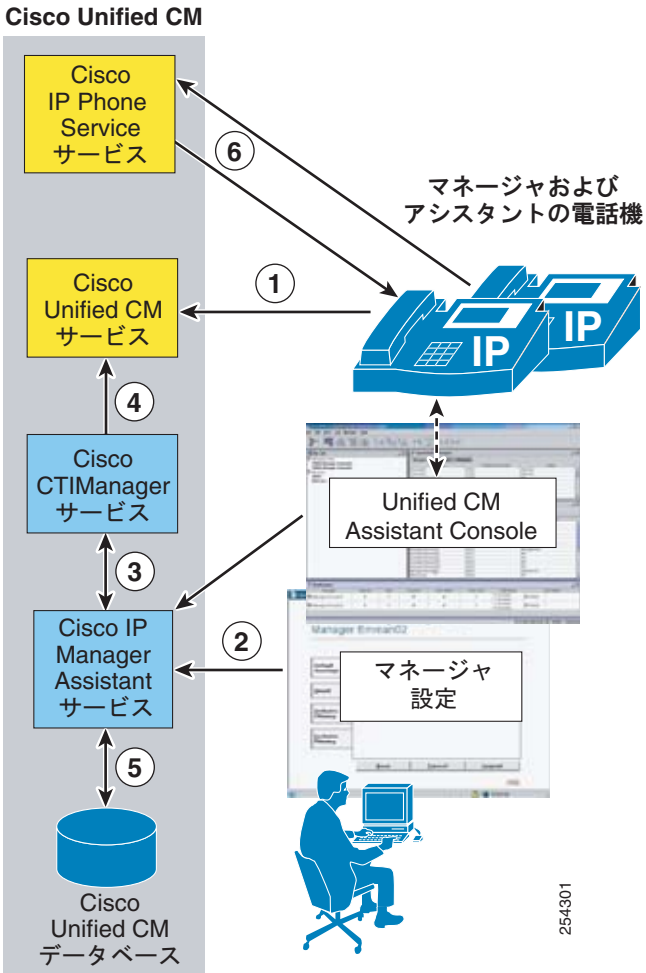
1. マネージャとアシスタントの電話機は Cisco Unified CallManager サービスに登録され、コール フロー処理にキーパッドとソフトキーが使用されます（図 24-7 のステップ 1 を参照）。
2. Unified CM Assistant Console デスクトップ アプリケーションと Manager Configuration Web ベース アプリケーションは、どちらも Cisco IP Manager Assistant サービスと通信およびインターフェイスします（図 24-7 のステップ 2 を参照）。
3. 次に、Cisco IP Manager Assistant サービスは、回線監視情報および電話制御情報を交換するために、CTIManager サービスと対話します（図 24-7 のステップ 3 を参照）。
4. CTIManager サービスは、Unified CM Assistant 電話制御情報を Cisco CallManager Service に渡し、さらに Unified CM Assistant RP をも制御します（図 24-7 のステップ 4 を参照）。
5. それと並行して、Cisco IP Manager Assistant サービスは、Unified CM データベースとの間で、Unified CM Assistant アプリケーション情報の読み取りと書き込みを行います（図 24-7 のステップ 5 を参照）。

6. マネージャは、Services ボタンを押すことにより、Unified CM Assistant 電話サービスを呼び出して、その電話機が加入している（Unified CM Assistant 電話サービスを含む）すべてのサービスのリストを返す IP Phone Service サービスへのコールを生成できます（図 24-7 のステップ 6 を参照）。

Unified CM Assistant 電話サービスは Cisco IP Manager Assistant サービスで制御され、電話機を使用してマネージャによって加えられた設定の変更は、Cisco IP Manager Assistant サービスを通じて処理および伝達されます。

（注）　Services Provisioning エンタープライズ パラメータが内部に設定されている場合、ステップ 1 および 2 はバイパスされます。一方、Services Provisioning が外部 URL または両方に設定されている場合、ユーザが回線ボタンまたは短縮ダイヤル ボタンを押して、Cisco IP Manager Assistant サービスへの直接コールを生成できるように、Service URL ボタンはユーザの電話機で Unified CM Assistant 電話サービス の設定ができます。ステップ 1 および 2 もバイパスされます。

図 24-7　Unified CM Assistant のアーキテクチャ



（注）　図 24-7 は、同じノードですべてが実行されている IP Phone Service、Cisco CallManager、CTIManager、および Cisco IP Manager Assistant サービスを示していますが、この設定は必須ではありません。これらのサービスではクラスタ内の複数のノードに分散できますが、説明を簡単にするためにここでは同じノードにあるものとしています。

Unified CM Assistant のダイヤル プランの考慮事項

ダイヤル プラン設定は、プロキシ回線モードで設定される Unified CM Assistant では非常に重要です。マネージャの DN に対するコールが Unified CM Assistant RP で代行受信され、アシスタントの電話機に転送されることを保証するには、Unified CM Assistant RP およびアシスタントの電話機上のマネージャのプロキシ回線を除いて、すべてのデバイスからマネージャの DN に到達できないように、コーリング サーチ スペースおよびパーティションを設定する必要があります。

図 24-8 は、ダイヤル プラン コンポーネント内の各種デバイスのコーリング サーチ スペース、パーティション、および設定に対する最小要件を持つ、プロキシ回線モードの Unified CM Assistant ダイヤル プランの例を示しています。プロキシ回線モードでは 3 個のパーティションが必要です。図 24-8 の例では、次のパーティションになります。

- すべての Unified CM Assistant RP DN を含む Assistant_Route_Point パーティション
- すべてのアシスタントとその他のユーザの電話機 DN を含む Assistant_Everyone パーティション
- すべてのマネージャの電話機の DN を含む Assistant_Manager パーティション

また、2 つのコーリング サーチ スペースが必要です。図 24-8 の例では、次のコーリング サーチ スペースになります。

- Assistant_Route_Point パーティションおよび Assistant_Everyone パーティションを含む ASSISTANT_EVERYONE_CSS コーリング サーチ スペース
- Assistant_Manager パーティションおよび Assistant_Everyone パーティションを含む MANAGER_EVERYONE_CSS コーリング サーチ スペース

これは、この例でのダイヤル プランの範囲です。ただし、コール ルーティングが必要に応じて動作するように、適切なコーリング サーチ スペースでさまざまな電話機および Unified CM Assistant RP DN または回線を適切に設定することも重要です。この場合、すべてのユーザの回線、アシスタントのプライマリ（またはパーソナル）回線、およびマネージャの電話回線は、これらの回線すべてが Assistant_Everyone パーティションおよび Assistant_Route_Point パーティションのすべての DN に到達できるように、ASSISTANT_EVERYONE_CSS コーリング サーチ スペースで設定します。テレフォニー ネットワーク内のデバイスで設定されるインターコムなどの回線は、この同じコーリング サーチ スペースで設定します。すべてのマネージャのプロキシ回線およびすべての Assistant_RP 回線は、これらの回線すべてが Assistant_Manager パーティションのマネージャ DN および Assistant_Everyone パーティションに属するすべての DN に到達できるように、MANAGER_EVERYONE_CSS コーリング サーチ スペースで設定します。この方法により、ダイヤル プランでは、アシスタントの電話機の Assistant_RP 回線およびマネージャのプロキシ回線だけが、マネージャの電話機 DN に直接到達できるように確保します。

図 24-8　Unified CM Assistant のプロキシ回線モードのダイヤル プランの例

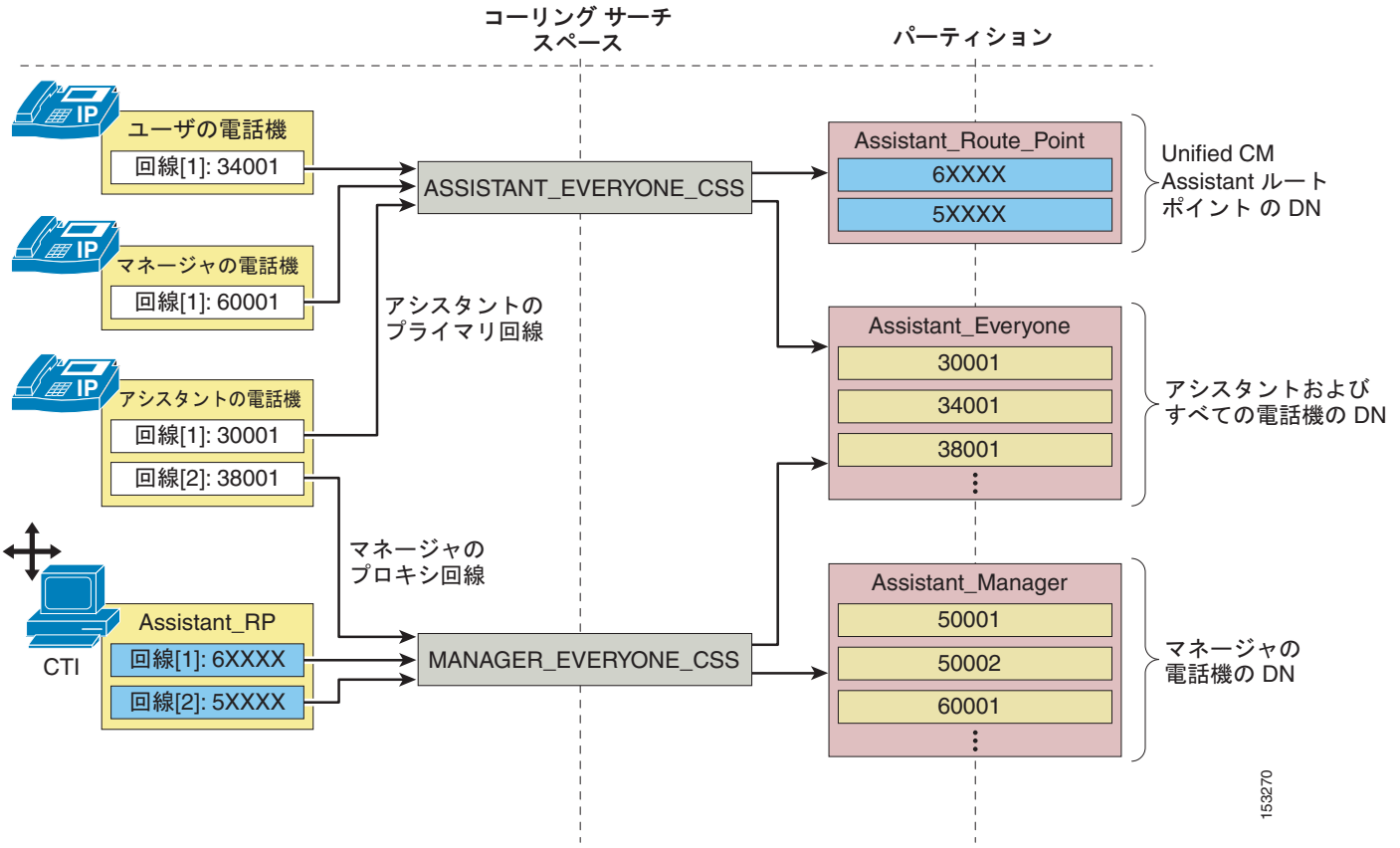


図 24-8 の例では、プロキシ回線モードでの Unified CM Assistant に関するダイヤル プランの最小要件を示しています。ただし、実際のテレフォニー ネットワークには、ほとんどの場合、Unified CM Assistant のコーリング サーチ スペースおよびパーティションとの統合が必要な追加または既存のダイヤル プラン要件があります。図 24-9 は、このような統合ダイヤル プランを示しています。この例では、前述したダイヤル プランは、2 つの追加のパーティションと 1 つの追加のコーリング サーチ スペースを処理する必要があります。図 24-9 では On Cluster パーティションが追加され、追加の電話機 DN もいくつか含まれています。On Cluster パーティションは、既存のデバイスがこれらの追加 DN に到達できるように、既存の Unified CM Assistant コーリング サーチ スペースの両方（ASSISTANT_EVERYONE_CSS および MANAGER_EVERYONE_CSS）に追加されています。UNRESTRICTED_CSS コーリング サーチ スペースも、既存のダイヤル プランに追加されています。このコーリング サーチ スペースは Assistant_Route_Point、Assistant_Everyone、および新たに追加した On Cluster パーティションで設定します。また、PSTN という 2 番目の新しいパーティションが追加されています。これには、共通ルート リスト（RL）、ルート グループ（RG）、およびボイス ゲートウェイ メカニズムを通じて、公衆網にコールをルーティングするために使用されるルート パターンのセットが含まれています。この PSTN パーティションは、UNRESTRICTED_CSS コーリング サーチ スペースの一部として設定します。

電話機およびデバイス回線のコーリング サーチ スペースの設定は、新しく追加したパーティションおよびコーリング サーチ スペースを組み込むために調整することができます。ただし、Assistant_RP およびアシスタントの電話機のマネージャ プロキシ回線は、MANAGER_EVERYONE_CSS コーリング サーチ スペースに割り当てたままにする必要があります。この例で、マネージャには公衆網への無制限アクセスが与えられる可能性があるため、マネージャの電話回線は、最初に設定された ASSISTANT_EVERYONE_CSS コーリング サーチ スペースから、新しい UNRESTRICTED_CSS に移動されています。

図 24-9　Unified CM Assistant のプロキシ回線モードのダイヤル プラン統合の例

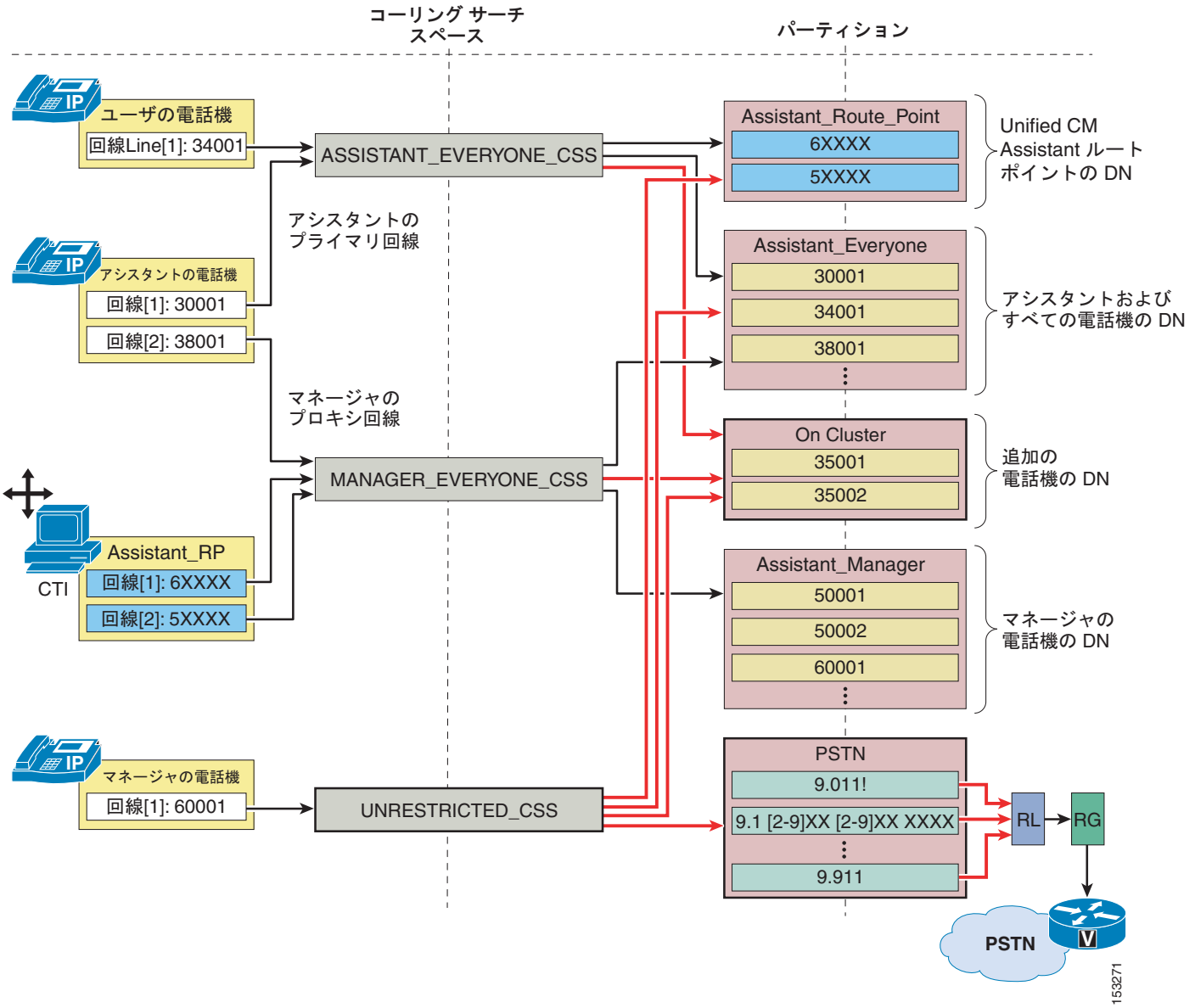


図 24-9 に示すように、追加のパーティションとコーリング サーチ スペースを新規または既存の Unified CM Assistant ダイヤル プランに統合することはできますが、基になるプロキシ回線モードのメカニズムが影響を受けないように注意する必要があります。

Unified CM Assistant シェアドライン モードでは、特別なダイヤル プランのプロビジョニングは必要ありません。注意の必要な Unified CM Assistant RP またはプロキシ回線が存在しないため、マネージャとアシスタントの電話機は、ネットワーク内の他の電話機と同様にコーリング サーチ スペースおよびパーティションで設定できます。シェアドライン モードに関する唯一の要件は、シェアドラインの機能を実現できるように、マネージャとアシスタントの DN が同じパーティションに属する必要があることです。

Unified CM Assistant Console

Unified CM Assistant Console デスクトップ アプリケーションまたはUnified CM Assistant Console 電話サービスは、アシスタントがマネージャの代わりにコールを処理するために必要です。このデスクトップ アプリケーションは、コールを処理するためのグラフィカル インターフェイスをアシスタントに提供しますが、電話サービスはコールを処理するためのメニュー方式インターフェイスを提供します。デスクトップ アプリケーションとIP 電話サービスの両方では、アシスタントがマネージャの電話機の設定および環境の設定ができて、回線ステータスおよび可用性を監視できます。また、このデスクトップ アプリケーションは、クリックコール短縮ダイヤルおよびディレクトリ エントリなど別の機能を備えています。この別の機能も従来のソフトキーおよびメニュー アプローチを使用してアシスタントの電話機で行うことができます。

Unified CM Assistant Console のインストール

Unified CM Assistant Console デスクトップ アプリケーションは、次の URL からインストールできます。

https://<*Server_IP-Address*>:8443/ma/Install/IPMAConsoleInstall.jsp

（ここで、<*Server_IP-Address*> は、クラスタ内のいずれかのノードの IP アドレスです）

Unified CM Assistant Console 電話サービスは、いかなるインストールも必要がありません。アシスタントの電話機をコンソールとして使用可能にするには、アシスタントの電話機を Unified CM Assistant 電話サービスにサブスクライブします（これは、マネージャの電話機もサブスクライブする必要があることと同じサービスです）。

Unified CM Assistant Console の QoS

インストール後に、マネージャに代わってコールを処理するには、アシスタントがユーザ ID とパスワード（Cisco Unified CM の End-user ディレクトリで設定されている）を入力してアプリケーションにログオンし、Go Online アイコンまたはメニュー項目をクリックして、ステータスを 「online」に切り替える必要があります。ユーザがログインし、オンライン状態になると、デスクトップ アプリケーションは TCP ポート 2912 でUnified CM Assistant サーバ と通信します。このアプリケーションは、トラフィックを受信する場合に一時的な TCP ポートを選択します。Cisco Unified CM 上の Unified CM Assistant サーバは、呼制御（コール フローの生成と処理）のためにデスクトップ アプリケーションとインターフェイスするので、TCP ポート 2912 で Cisco Unified CM から受信されたトラフィックは、Cisco Unified CM によって 24 の Differentiated Services Code Point（DSCP）または CS3 の Per Hop Behavior（PHB）として、QoS マーキングされます。この方法により、Unified CM Assistant 電話制御トラフィックは、その他のすべてのコール シグナリング トラフィックと同様に、ネットワークを通じてキューに入れることができます。

対称的なマーキングとキューを保証するため、Cisco Unified CM の TCP ポート 2912 を宛先とする Unified CM Assistant Console アプリケーション トラフィックも、DSCP 24（PHB CS3）としてマーキングする必要があります。これにより、このトラフィックが、Cisco Unified CM および Unified CM Assistant サーバに向かうネットワーク パスに沿って適切なコール シグナリング キューに配置されます。Unified CM Assistant Console アプリケーションは、すべてのトラフィックをベストエフォートとしてマーキングします。つまり、スイッチ ポート レベル（または、可能な限りコンソール PC に近いネットワーク パスに沿った場所で）Access Control List（ACL; アクセス コントロール リスト）を適用することで、アプリケーション PC から送信され、TCP ポート 2912 の Cisco Unified CM を宛先とするトラフィックを、DSCP 0（PHB Best Effort）から DSCP 24（PHB CS3）に再マーキングする必要があります。

Unified CM Assistant Console のディレクトリ ウィンドウ

Assistant Console デスクトップ アプリケーションのディレクトリ ウィンドウを使用すると、アシスタントは Cisco Unified CM Directory エンドユーザを検索できます。ディレクトリ ウィンドウの Name フィールドに入力する検索文字列は、Unified CM Assistant サーバに送信され、Cisco Unified CM データベースに対して検索が直接実行されます。次に、Unified CM Assistant サーバによって、検索照会への応答がデスクトップ アプリケーションに返されます。

デスクトップ アプリケーションのディレクトリ検索によって生じる追加のトラフィックはわずかですが、1 つ以上の Unified CM Assistant コンソール アプリケーションがリモート サイトで実行されている集中型のコール処理配置では、このトラフィックが問題になることがあります。1 つのエントリが得られるディレクトリ検索では、Unified CM Assistant サーバからデスクトップ アプリケーションへの約 1 キロビットのトラフィックが発生します。1 回の検索あたり最大 25 のエントリを取得できるため、デスクトップ アプリケーションで実行される検索ごとに最大約 25 キロビットのトラフィックが生成されることがあります。ただし、Unified CM Assistant サーバからの低速 WAN リンクを通じて、複数の Unified CM Assistant Console デスクトップ アプリケーションでディレクトリ検索が実行されると、輻輳、遅延、およびキューの発生する可能性が高くなります。また、ディレクトリ検索トラフィックは、デスクトップに対するその他すべての Unified CM Assistant トラフィックと同様に、TCP ポート 2912 の Cisco Unified CM から発生します。つまり、ディレクトリ検索トラフィックも DSCP 24（PHB CS3）としてマーキングされるため、コール シグナリング トラフィックと同様にキューに入れられます。このため、ディレクトリ検索によって、呼制御トラフィックの輻輳、オーバーラン、または遅延が生じる可能性があります。

（注）　ディレクトリ検索で 25 を超えるエントリが生成される場合、アシスタントには、ダイアログボックスを介して警告メッセージ「Your search returned more than 25 entries.Please refine your search.」が表示されます。

ネットワーク輻輳の可能性を考慮に入れて、管理者は Unified CM Assistant Console ユーザに次の操作の実行を推奨することをお勧めします。

- ディレクトリ ウィンドウ検索機能の使用を制限する。
- 返されるエントリの数を減らすため、この機能を使用するときは、Name フィールドにできる限り多くの情報を入力し、ワイルドカードやブランクでの検索は実行しない。

これらの推奨事項は、次のいずれかの条件が該当する場合は特に重要です。

- クラスタ内に多数の Unified CM Assistant Assistants が存在する。
- Cisco Unified CM または Unified CM Assistant サーバ（あるいはその両方）から低速 WAN リンクによって分離されている多数のアシスタントが存在する。

Unified CM Assistant Phone Console の QoS

Unified CM Assistant Phone Console 電話サービスを使用してマネージャに代わってコールを処理するには、アシスタントがユーザ ID と PIN（Unified CM の End-user ディレクトリで設定されている）を入力してアプリケーションにログオンする必要があります。ユーザがログインしている状態になると、電話コンソール サービスは HTTPS および SCCP を使用して Unified CM と通信します。Unified CM Assistant コール生成およびコール処理の呼制御トラフィックは、SCCP を使用して電話と Unified CM の間で送信されます。デフォルトでは、このトラフィックは 24 の Differentiated Services Code Point（DSCP）または CS3 の Per Hop Behavior（PHB）として、QoS マーキングされます。こうして、コール シグナリング トラフィックと同様にネットワークを通じてキューに入れられ確保します。したがって、追加の QoS の設定またはマーキングの必要はありません。

Unified CM Assistant の冗長性

Unified CM Assistant アプリケーションの冗長性は、次の 2 つのレベルで実現できます。

- コンポーネント レベルとサービス レベルでの冗長性

  このレベルでの冗長性については、Unified CM Assistant サービスまたはサーバの冗長性、および CTIManager サービスの冗長性に関して検討する必要があります。同様に、パブリッシャの冗長性の欠如、およびこのコンポーネントの障害の影響も検討する必要があります。

- デバイス レベルと到達可能性レベルでの冗長性

  このレベルでの冗長性については、アシスタントとマネージャの電話機、Unified CM Assistant ルート ポイント、Unified CM Assistant Console デスクトップ アプリケーション、および電話サービス に関連して検討し、さらにアシスタントとマネージャの到達可能性に関する冗長性として検討する必要があります。

サービスとコンポーネントの冗長性

図 24-7 に示すように、Unified CM Assistant 機能は、主に Cisco IP Manager Assistant サービスおよび Cisco CTIManager サービスに依存します。いずれの場合も、冗長性はプライマリおよびバックアップのメカニズムを使用して自動的に組み込まれます。Unified CM Assistant サーバ（Cisco IP Manager サービスを実行しているノード）のアクティブおよびバックアップのペアは最大で 3 個まで定義できます。つまり、単一クラスタ内で合計 6 つの Unified CM Assistant サーバになります。アクティブおよびバックアップ Unified CM Assistant サーバ ペアは Cisco IPMA Server IP Address、Pool 2 、Cisco IPMA Server IP Address、および Pool 3 Cisco IPMA Server IP Address サービス パラメータ（「Unified CM Assistant のサービス パラメータ」（P.24-20）を参照）を使用して設定されます。これらのパラメータを設定することで、必要な Unified IP Assistant サービスに冗長性が与えられます。いずれかのプライマリ Unified CM Assistant に障害が発生した場合、バックアップまたはスタンバイ Unified CM Assistant サーバが Unified CM Assistant サービス要求を処理できます。Unified CM Assistant サーバの各ペアでは、任意の時点でアクティブになり、要求を処理する Unified CM Assistant サーバは 1 つだけです。その別の Unified CM Assistant サーバはスタンバイ状態になり、アクティブなサーバに障害が発生しない限り、要求を処理しません。

また、CTIManager (Primary) IP Address および CTIManager (Backup) IP Address サービス パラメータを使用して、2 つの CTIManager サーバまたはサービスを各 Unified CM Assistant サーバ用に定義できます（「Unified CM Assistant のサービス パラメータ」（P.24-20）を参照）。これらのパラメータを設定すると、CTIManager サービスに冗長性を与えることができます。このため、プライマリ CTIManager に障害が発生した場合でも、CTIManager サービスはバックアップ CTIManager から提供できます。クラスタ ノードのすべての Unified IP Assistant および CTIManager サービスに障害が発生した場合は、Unified CM Assistant ルート ポイントおよび Unified CM Assistant Console デスクトップ アプリケーションがダウンし、その結果 Unified CM Assistant アプリケーション全体がダウンします。ただし、前にも説明したように、Unified CM Assistant に障害が発生した場合、CFNA による呼び出しメカニズムは引き続き動作し、マネージャへのコールは直接マネージャの電話にルーティングできます。

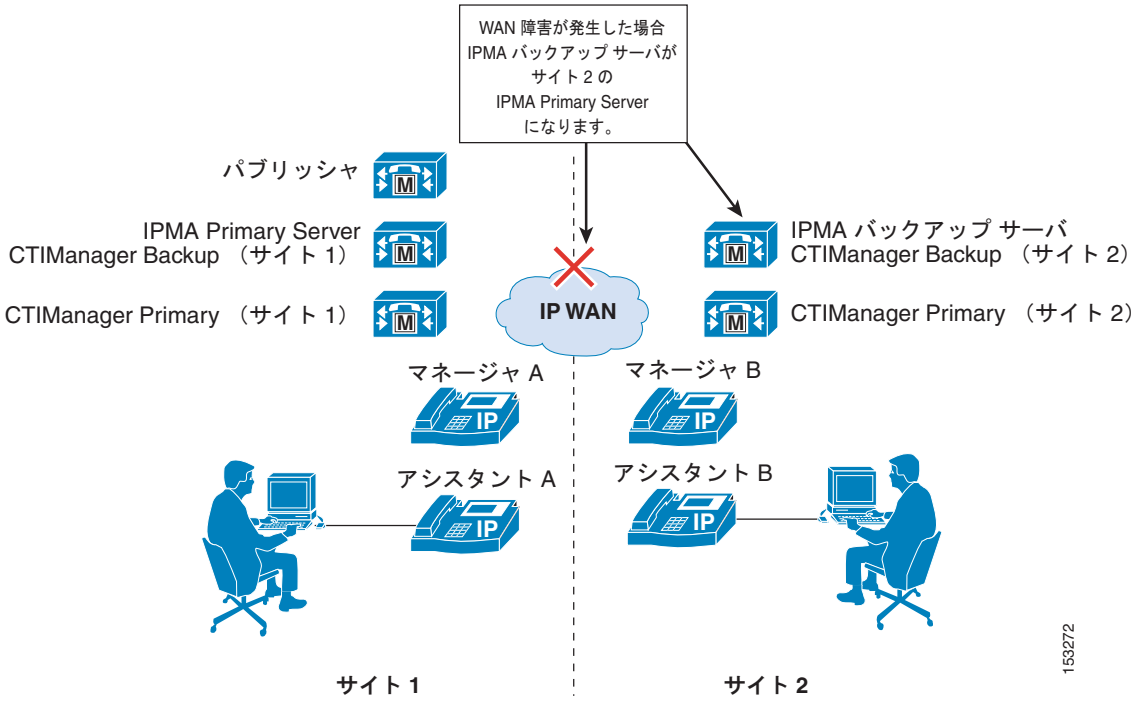
（注）　Unified IP Assistant シェアドライン モードで設定した場合、Unified CM Assistant および CTIManager サービスが障害によって完全に停止しても、電話機は 1 本の回線を共有し続けるため、アシスタントは引き続きマネージャの代わりにコールを処理できます。ただし、Unified CM Assistant Console デスクトップ アプリケーションと DND の機能は、使用できなくなります。

図 24-10 は、WAN を通じたクラスタ化で、2 サイトの配置による Unified CM Assistant および CTIManager のプライマリ サーバとバックアップ サーバの冗長設定を示しています。最大限の冗長性を実現するため、サイト 1 のノードはプライマリ Unified CM Assistant サーバとして設定し、サイト 2

のノードはバックアップ Unified CM Assistant サーバとして設定します。WAN に障害が発生した場合、既存のプライマリ Unified CM Assistant サーバはサイト 2 から到達できなくなるため、サイト 2 のバックアップ Unified CM Assistant サーバがプライマリ Unified CM Assistant サーバになります。このようにすることで、クラスタオーバー WAN 環境で、Unified CM Assistant サーバは WAN の障害に対して冗長性を持つことができます。さらに、サイト 1 とサイト 2 の両方でプライマリおよびバックアップ CTIManager を設定すると、CTIManager は WAN の障害に対する冗長性を持ち、各サイトで CTIManager の障害に対して追加の冗長性が提供されます。

（注）　図 24-10 で説明するシナリオは、特別な状況を示しています。通常の動作時に、Unified CM Assistant サーバの任意ペアを同時にアクティブにすることはできません。Unified CM Assistant サーバのアクティブおよびバックアップ ペアがネットワークを通じて通信できる場合、一方のサーバはバックアップ モードとなり、要求を処理できません。

図 24-10　WAN を通じた 2 サイト クラスタ化による Unified CM Assistant の冗長性



前に説明したように、パブリッシャは、Unified CM Assistant 情報を Unified CM データベースへ書き込みする時に単一の障害点となります。パブリッシャに障害が発生しても、Unified CM Assistant アプリケーションのすべての部分が引き続き動作します。ただし、Unified CM Assistant アプリケーション設定を変更できなくなります。パブリッシャが回復するまで、Unified CM Assistant Console デスクトップ アプリケーション、Manager Configuration Web ベース アプリケーション、電話機のソフトキー、または Unified CM Assistant 電話サービスを通じて設定を変更できません。この条件には、Do Not Disturb、DivertAll、Assistant Watch、コール フィルタリングなどの機能の有効化や無効化、およびコール フィルタとアシスタント選択設定の変更が含まれます。

デバイスと到達可能性の冗長性

デバイス レベルでの Unified CM Assistant の冗長性は、いくつかのメカニズムに依存しています。まず第 1 に、マネージャおよびアシスタントの電話機と Unified CM Assistant RP は、デバイス登録用のデバイス プールと Cisco Unified CM グループ設定の組み合せによって提供される組み込み冗長性に依存します。

また、一部のデバイスは、追加の冗長性および機能のためにコンポーネント サービスに依存します。たとえば、Unified CM Assistant RP は呼制御機能に関して CTIManager にも依存するため、前の項で説明したプライマリおよびバックアップ CTIManager に依存する必要があります。
Unified CM Assistant Console デスクトップ アプリケーションも、冗長性と機能がコンポーネント サービスに依存します。Assistant Console デスクトップ アプリケーションは、マネージャの着信コールの処理を持続できるように、プライマリ Unified CM Assistant サーバからバックアップ サーバ（およびその反対）への自動フェールオーバーをサポートしています。この自動フェールオーバーに要する時間は、Cisco Unified IPMA Assistant Console Heartbeat Interval および
Cisco Unified IPMA Assistant Console Request Timeout のサービス パラメータを使用して制御できます（「Unified CM Assistant のサービス パラメータ」（P.24-20）を参照）。ハートビートまたはキープアライブの頻度は、Unified CM Assistant サーバの障害がデスクトップ アプリケーションですばやく検出されるように設定しますが、キープアライブをあまり頻繁に送信することで、ネットワークに悪影響を与えないように注意してください。多数の Assistant Console アプリケーションが使用されている場合、この考慮事項は特に重要です。

Unified CM Assistant Console 電話サービスは、Unified CM Assistant Console デスクトップ アプリケーションとは異なり、プライマリ Unified CM Assistant サーバに障害が発生した場合の冗長性には手動で調整する必要があります。この状態の表示　プライマリ Unified CM Assistant サーバがダウンした場合、電話コンソールを使用しているアシスタントにはこの状態の表示が見えません。ただし、アシスタント電話では、ソフトキー を使用するときにメッセージ「Host not found Exception」を受信します。バックアップ Unified CM Assistant サーバで電話コンソールを引き続き使用するには、ユーザは IP Services メニューから再びログインして、セカンダリ Unified CM Assistant 電話サービスを手動で選択する必要があります。

マネージャおよびアシスタントの到達可能性に確実に冗長性を与えるフェールオーバー メカニズムは、他にもいくつかあります。第 1 に、（プロキシ回線モードで）Unified CM Assistant アプリケーションを通じてマネージャのアシスタントに送信されるコールは、設定した時間の経過後にそのコールへの応答がない場合、次の応答可能なマネージャのアシスタントに転送します。設定した時間の経過後に次のアシスタントがコールに応答しない場合、そのコールは次の応答可能なマネージャのアシスタントに再び転送され、それ以降も同様に転送が続けられます。このメカニズムは、Cisco IPMA RNA Forward Calls および Cisco IPMA RNA Timeout のサービス パラメータを使用して設定します
（「Unified CM Assistant のサービス パラメータ」（P.24-20）を参照）。第 2 に、前述したように、クラスタ ノードのすべての Unified IP Assistant と CTI サービスに障害が発生した場合、
Unified CM Assistant RP は使用できなくなります。ただし、Unified CM Assistant RP の CFNA 設定に基づいて、すべてのマネージャの DN に対するコールはマネージャの電話機に直接呼び出され、マネージャの到達可能性に十分な冗長性が与えられます。

Unified CM Assistant のガイドラインと制限

Unified CM Assistant には、重複および共有内線番号に関して次の制限があり、ディレクトリ番号のプロビジョニングを計画する場合に注意する必要があります。

- プロキシ回線モードの Unified CM Assistant では、アシスタントの電話機のプロキシ回線番号は、異なるパーティション間でも一意にする必要があります。
- プロキシ回線モードの Unified CM Assistant では、2 人のマネージャは異なるパーティション間でも、同じ Unified CM Assistant 制御回線番号（DN）を持つことができません。

Multiple Active Mode を有効にして複数の Unified CM Assistant サーバ プールを使用する場合は、Unified CM Assistant サーバ プールの間でマネージャおよびアシスタントが均等に分散されるようにして、適切なサーバ プール（1 から 3）がエンド ユーザ Manager Configuration ページの Assistant Pool フィールドで選択されることを確認します。マネージャに連携したアシスタントは、そのマネージャが設定されたプールに自動的に割り当てられます。

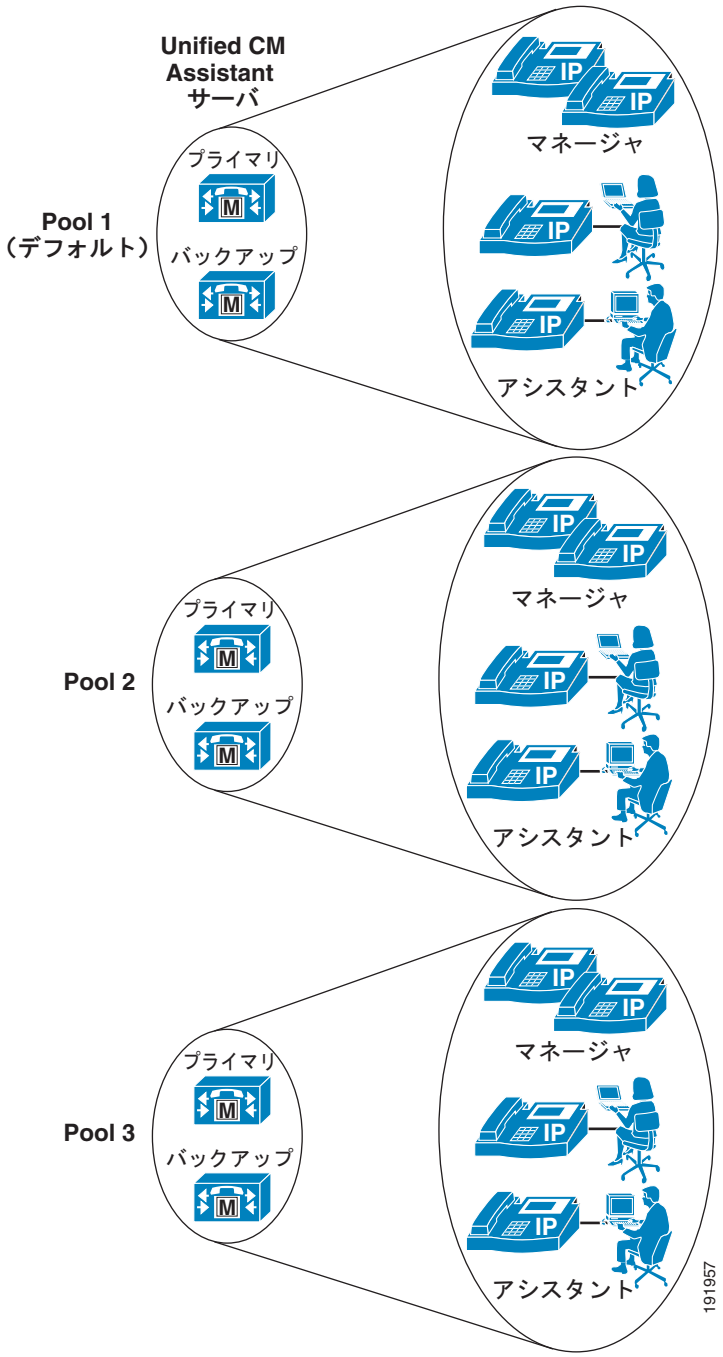
Unified CM Assistant のパフォーマンスとキャパシティ

Cisco Unified CM Assistant アプリケーションは、次のキャパシティをサポートしています。

- マネージャあたり最大 10 人のアシスタントを設定できる。
- 1 人のアシスタントに対して最大 33 人のマネージャを設定できる（マネージャ毎に 1 つの Unified CM Assistant 制御回線がある場合）。
- クラスタあたり最大 3500 人のアシスタントと 3500 人のマネージャを、Cisco MCS 7845 を使用して設定できる（合計 7000 人）。
- クラスタあたり最大でプライマリおよびバックアップ Unified CM Assistant サーバを 3 ペアを配置できる。ただし、Enable Multiple Active Mode サービス パラメータを True に設定し、Unified CM Assistant サーバ の 2 番目および 3 番目プールを設定した場合（「Unified CM Assistant のサービス パラメータ」（P.24-20）を参照）。

Unified CM Assistant 最大でアシスタント 3500 人とマネージャ 3500 人（合計 7000 人）のキャパシティを実現するには、マルチの Unified CM Assistant サーバ プールを定義する必要があります。図 24-11 に示しているように、最大 3 個のプールを設定できます。各プールはプライマリおよびバックアップ Unified CM Assistant サーバおよびマネージャとアシスタントのグループで構成されています。Pool 1 の Unified CM Assistant サーバは Cisco IPMA Server（Primary/Backup）の IP Address サービス パラメータで設定し、Pool 2 のサーバは Pool2 で Cisco IPMA Server（Primary/Backup）の IP Address アドバンスト パラメータで設定し、および Pool 3 のサーバは Pool3 で Cisco IPMA Server（Primary/Backup）の IP Address アドバンスト パラメータで設定します（「Unified CM Assistant のサービス パラメータ」（P.24-20）を参照）。

図 24-11　Unified CM Assistant Server Pools 環境下のマルチ アクティブ モード



Cisco Unified CM Assistant アプリケーションは、回線監視および電話制御のために CTIManager と対話します。Unified CM Assistant ようのまたはマネージャ電話用の各回線（インターコム回線を含む）が CTI 回線を CTIManager と共に必要になります。また、各 Unified CM Assistant ルート ポイントは、CTI 回線インスタンスが CTIManager と共に必要になります。Unified CM Assistant を設定する場合、必要な CTI 回線または接続の数について、CTI 回線または接続に対する全体的なクラスタ制限と合わせて考慮する必要があります（クラスタごとの CTI 接続制限の詳細については、「Unified CM の

キャパシティ プランニング」（P.8-22）を参照してください）。追加の CTI 回線が別のアプリケーションに必要になる場合、これらの CTI 回線によって Unified CM Assistant のキャパシティが制限される場合があります。

Unified CM Assistant と EM の相互作用

Unified CM Assistant のマネージャは、EM を使用して、プロキシ回線モードとシェアドライン モードの両方でそれぞれの電話機にログインできます。ただし、そのマネージャは、エンドユーザ ディレクトリの Cisco Unified CM Assistant Manager 設定ページで、Mobile Manager として設定する必要があります。Unified CM Assistant と組み合せて EM を使用する場合、ユーザが EM を使用して複数の電話機にログインできないようにする必要があります。この動作は、EM サービス パラメータの Multiple Login Behavior を使用して有効または無効にできます（「EM のサービス パラメータ」（P.24-11）を参照）。クラスタ内で同じユーザによる複数の EM ログインが必要な場合、EM を使用する Unified CM Assistant のマネージャに、複数の電話機にログインしないよう指示する必要があります。マネージャが EM で 2 つの異なる電話機にログインすることを許可すると、2 人のマネージャは異なるパーティション間でも同じ Unified CM Assistant 制御回線番号（DN）を持つことができないという、前述の制限に違反することになります。

（注）　Unified CM のアシスタントは、Mobile Assistant の概念がないため、EM を使用してそれぞれの電話機にログインできません。

アテンダント コンソール

アテンダント コンソールの統合によって、受付係は、組織内でその目的のために特別に設計されたデスクトップ アプリケーションからコールに応答したり、コールを転送または送信したりすることができます。アテンダント コンソールからは社内ディレクトリにアクセスでき、場合によっては、特定のユーザの回線状態を監視できます。Cisco Unified Communications ポートフォリオには、次の 2 つのタイプのアテンダント コンソールが用意されています。

- 「Cisco Unified Communications Manager Attendant Console」（P.24-35）
- 「Cisco Unified Department、Business、および Enterprise Attendant Console」（P.24-47）

Cisco Unified Communications Manager Attendant Console

Cisco Unified Communications Manager Attendant Console（Unified CM Attendant Console）は、コンソール担当者の Windows PC にインストールされたクライアント/サーバ Java アプリケーションです。Unified CM Attendant Console アプリケーションは、Unified CM サブスクライバ ノードで有効な Cisco CallManager Attendant Console Server サービスに接続して、ログイン サービス、回線状態の監視、およびディレクトリ サービスを実現します。複数の Unified CM Attendant Console から 1 つの Cisco CallManager Attendant Console Server サービスに接続できます。

（注）　Cisco Unified Communications Manager Attendant Console は販売を終了しており、Cisco Unified Communications Manager 7.0 以降のリリースの新規インストールでは使用できなくなりました。以前のリリースの既存の Cisco Unified Communications Manager ユーザは、7.0 にアップグレードしても、Cisco Unified Communications Manager Attendant Console をそのまま使用できます。販売終了発表の

詳細については、
http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps7046/ps7282/end_of_life_notice_c51-499091.html を参照してください。

Unified CM Attendant Console の電話機のサポート

次の SCCP 電話機は、Unified CM Attendant Console 機能をサポートしています。

- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7912G および 7912G-A
- Cisco Unified IP Phone 7940G、7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7960G、7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G
- Cisco IP Communicator

SIP 電話機では、Unified CM Attendant Console をサポートしていません。

Unified CM Services および Unified CM Assistant Console のサービス パラメータ

Unified CM Attendant Console アプリケーションを有効にするには、システム管理者が Cisco Unified Serviceability インターフェイスからいくつかの Unified CM 機能サービスをアクティブにし、起動する必要があります。また、Unified CM Attendant Console サービス パラメータには、Unified CM Attendant Console アプリケーションの動作を決定する設定オプションおよびカスタマイズ オプションがあります。

Unified CM Attendant Console 用の Unified CM サービス

Unified CM Attendant Console アプリケーションは次の機能サービスに依存します。これらのサービスは、Serviceability ページから手動でアクティブにする必要があります。

- Cisco CallManager Attendant Console Server
- Cisco CTIManager

Cisco CallManager Attendant Console Server サービスは Unified CM Attendant Console Desktop アプリケーションへのインターフェイスを提供し、Cisco CTIManager サービスおよび Unified CM データベースと対話します。Cisco CTIManager サービスは、電話とコールの制御のために Cisco CallManager サービス および Cisco CallManager Attendant Console Server サービスとインターフェイスし、対話します。また、Unified CM Attendant Console Desktop アプリケーションともインターフェイスします。

Unified CM Attendant Console のサービス パラメータ

次の項目は、Unified CM Attendant Console の機能に関連する Cisco CallManager Attendant Console Server サービス パラメータの一部のリストです。

- Directory Sync Period（デフォルト値 = 3）

  このパラメータは、Unified CM Attendant Console サーバの AutoGenerated.txt ファイルと Unified CM のエンドユーザ ディレクトリの同期のための間隔を、時間単位で指定します。エンドユーザ ディレクトリへの変更は、この間隔が経過するまで AutoGenerated.txt ファイルに反映されません。

- JTAPI Username（デフォルト値 = ac）

  このパラメータは、Unified CM Attendant Console サーバが CTIManager にログインし、通信するために使用するアプリケーション ユーザ名を指定します。

- Device Authentication Application Username（デフォルト値 = ACDeviceAuthenticationUser）

  このパラメータは、Unified CM Attendant Console サーバがコンソール担当者の電話機の認証に使用するアプリケーション ユーザ名を指定します。

Attendant Console サービス パラメータの全リストについては、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Features and Services Guide*』の Unified CM Attendant Console 情報を参照してください。

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

Unified CM Attendant Console デバイス認証アプリケーション ユーザ

Unified CM Attendant Console を適切に動作させるには、**ac** というアプリケーション ユーザ名を Unified CM に設定する必要があります。ac アプリケーション ユーザは、Unified CM Attendant Console サーバが CTIManager と対話するために必要です。このアプリケーション ユーザが設定されていないと、コンソール担当者はコールを受信できません。

（注）　アプリケーション ユーザは、Cisco Unified CM データベース内のエンド ユーザとは異なり、ディレクトリ内のエンド ユーザとは別に保存されます。したがって、ディレクトリ検索ではアプリケーション ユーザ エントリが返されません。Cisco Unified CM のアプリケーション ユーザとエンド ユーザの詳細については、「LDAP ディレクトリ統合」（P.17-1）を参照してください。

ac ユーザには、アプリケーション ユーザの設定ページで次のグループ アクセス権を設定する必要があります。

- Standard CTI Allow Control of All Devices
- Standard CTI Allow Call Park Monitoring
- Standard CTI Enabled

ac アプリケーション ユーザを「Standard CTI Allow Control of All Devices」でグループ アクセス権を設定することによって、CTI Super Provider 機能を有効にします。Super Provider 機能によって、Unified CM Attendant Console アプリケーションは任意のデバイスまたは回線を制御および監視（CTI を介して）できます。これにより、コンソール担当者の電話機および ac アプリケーション ユーザへの Unified CM Attendant Console パイロット ポイントを関連付ける必要がなくなり、設定を簡潔化できます。

管理者は、このアプリケーション ユーザ名を ac 以外の名前に変更できます。ac 以外のユーザ名に設定した場合、JTAPI Username サービス パラメータに新しいユーザ名を設定する必要があります（「Unified CM Attendant Console のサービス パラメータ」（P.24-37）を参照）。

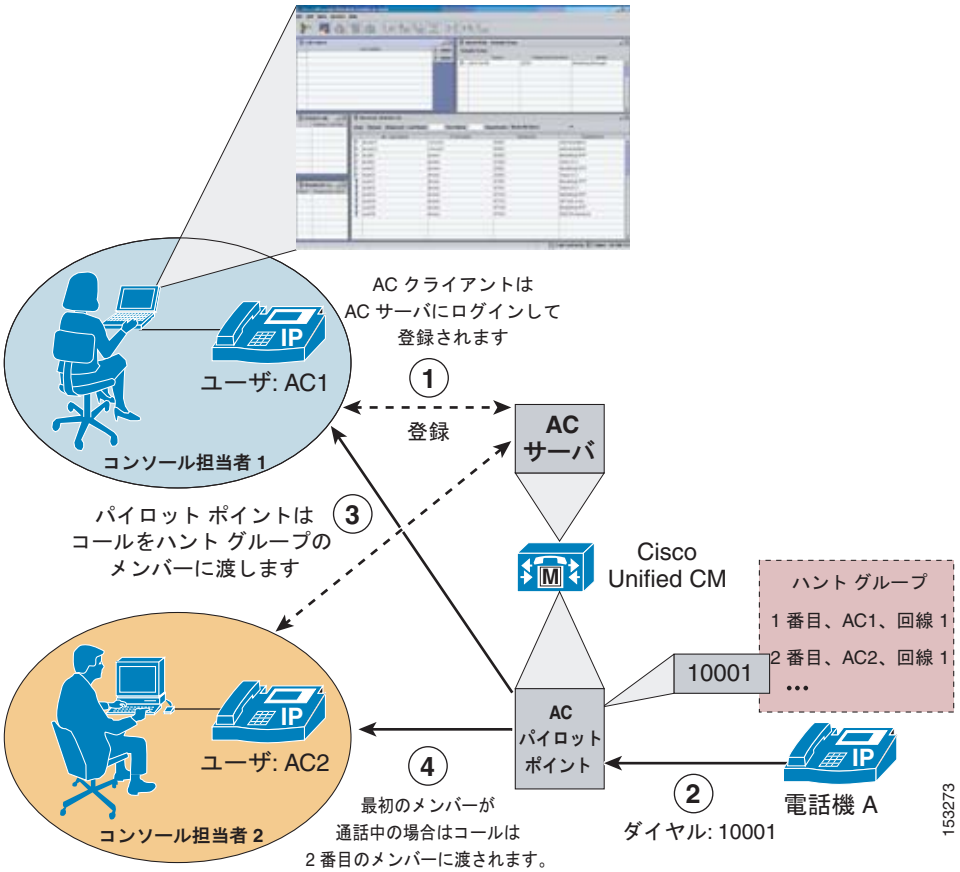
ac ユーザの追加 および上記のグループ アクセス権の割り当てに加えて、ACDeviceAuthenticationUser という名のデバイス認証アプリケーション ユーザを作成します。設定後、すべてのコンソール担当者の電話機はこのアプリケーション ユーザに関連付けられます。このアプリケーション ユーザは、コンソール担当者の電話機を認証するために Unified CM Attendant Console サーバによって使用されます。このアプリケーション ユーザ アカウントのためにグループ アクセス権を設定する必要はありません。

管理者が ACDeviceAuthenticationUser の代わりに異なるアプリケーション ユーザ アカウント名の使用を選択する場合、Device Authentication Application Username サービス パラメータ（「Unified CM Attendant Console のサービス パラメータ」（P.24-37）を参照）は設定したアプリケーション ユーザ名に一致するよう変更する必要があります。

Unified CM Attendant Console の機能とアーキテクチャ

図 24-12 は、Unified CM Attendant Console の基本的な機能と動作の例を示しています。まず、Unified CM Attendant Console クライアントが Unified CM の Unified CM Attendant Console サーバにログインして登録します（ステップ 1）。次に、電話機 A は Unified CM の Unified CM Attendant Console パイロット ポイントに設定されたディレクトリ番号（DN）10001 をコールします（ステップ 2）。Unified CM Attendant Console パイロット ポイントはこのコールを代行受信し、ハント グループ設定に基づいて、使用可能なメンバーの 1 つにコールを転送します。この場合、コールは Attendant ユーザ AC1 の電話機の回線 1 に送信されます（ステップ 3）。AC1 がまだ最初のコールで通話しているときに、パイロット ポイント番号 10001 に 2 番目のコールが着信した場合、そのコールはハント グループの別の使用可能なメンバーにルーティングされます。この場合、そのコールは、Attendant ユーザ AC2 の電話機の回線 1 に転送されます（ステップ 4）。

図 24-12　Unified CM Attendant Console の基本動作



コールをルーティングするには、パイロット ポイントが次のいずれかのルーティング アルゴリズムに基づいて、ハント グループの次の使用可能なメンバーを決定します（パイロット ポイントの「Route Calls to」フィールドで設定します）。

- First available

  このアルゴリズムでは、着信コールが、使用可能なグループの最初のメンバーにルーティングされます。

- Longest idle

  このアルゴリズムでは、着信コールが、アイドル状態（コールの処理なし）の最も長かったメンバーにルーティングされます。

- Circular hunting

  このアルゴリズムでは、着信コールが、使用可能なメンバーにラウンドロビン方式でルーティングされます。

- Broadcast hunting

  このアルゴリズムでは、着信コールがキューに入れられ、すべての使用可能なメンバーの Unified CM Attendant Console デスクトップ アプリケーションに対して同時に通知が送信されます。

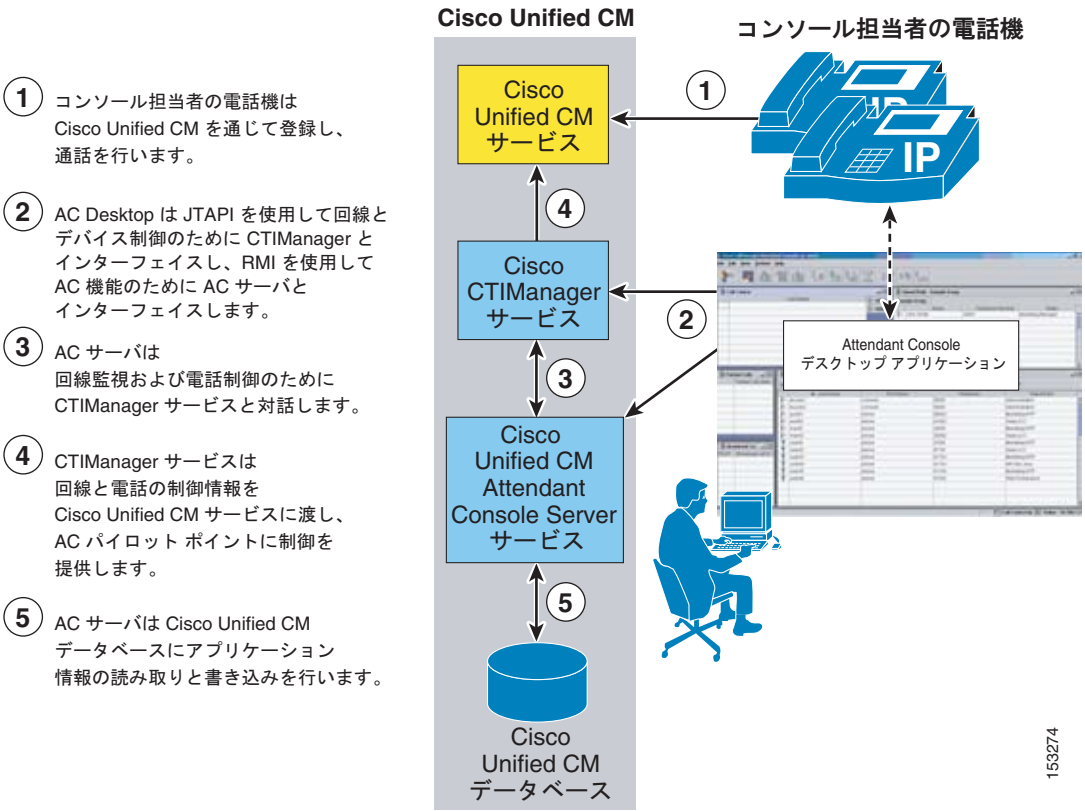
図 24-12 に示す例では、First Available アルゴリズムを使用しています。ハント グループのルーティング アルゴリズム、および Broadcast ルーティング アルゴリズムのキュー設定は、すべて Cisco Unified CM の Pilot Point 設定ページで設定します。

Unified CM Attendant Console のアーキテクチャ

Unified CM Attendant Console アプリケーションについては、その機能と同様にアーキテクチャを理解することも大切です。図 24-13 は、Unified CM Attendant Console のメッセージ フローとアーキテクチャを示しています。Unified CM Attendant Console がアテンダント コンソール ユーザ用に設定されている場合、次の一連の対話とイベントが発生します。

1. コンソール担当者の電話機は Cisco CallManager サービスに登録され、コール フロー処理にキーパッドとソフトキーが使用されます（図 24-13 のステップ 1 を参照）。
2. Attendant Console デスクトップ アプリケーションは、JTAPI を使用して電話と回線の制御のために CTIManager サービスと通信し、インターフェイスします。また、デスクトップ アプリケーションは Unified CM Attendant Console の機能を利用するため、Remote Method Invocation（RMI）を介して Unified CM Attendant Console サービスおよびサーバとインターフェイスします（図 24-13 のステップ 2 を参照）。
3. 次に、Unified CM Attendant Console サーバは、回線監視情報および電話制御情報を交換するために、CTIManager サービスと対話します（図 24-13 のステップ 3 を参照）。
4. 同様に、CTIManager サービスは Unified CM Attendant Console 電話制御情報を Cisco CallManager サービスに渡し、Unified CM Attendant Console パイロット ポイントも制御します（図 24-13 のステップ 4 を参照）。
5. それと並行して、Unified CM Attendant Console サーバは、Unified CM データベースとの間で Unified CM Attendant Console アプリケーション情報の読み取りと書き込みを行います（図 24-13 のステップ 5 を参照）。

図 24-13　Unified CM Attendant Console のアーキテクチャ



（注）　図 24-13 は、すべて同じノードで実行されている Cisco CallManager、CTIManager、および Cisco CallManager Attendant Console Server サービスを示していますが、この設定は必須ではありません。これらのサービスはクラスタ内の複数のノードに分散できますが、説明を簡単にするためにここでは同じノードにあるものとしています。

Attendant Console デスクトップ アプリケーション

Attendant Console デスクトップ アプリケーションは、グラフィカルな仮想コンソールを通じてコールを処理するため、コンソール担当者で使用されます。コール処理に加えて、このアプリケーションは、クリックダイヤルの短縮ダイヤルとディレクトリ エントリ、環境の設定、ディレクトリおよび短縮ダイヤル ウィンドウでの他のユーザに対する回線ステータスおよび可用性の表示など、追加の機能を備えています。

Attendant Console のインストール

Attendant Console デスクトップ アプリケーションは、次の URL からダウンロードできます。

https://<*Server_IP-Address*>:8443/plugins/CiscoAttendantConsoleClient.exe

（ここで、<*Server_IP-Address*> は、クラスタ内のいずれかのノードの IP アドレスです）

CiscoAttendantConsoleClient.exe ファイルは、コンソール担当者の PC にダウンロードしたら、インストールも実行する必要があります。

Attendant Console の QoS

Attendant Console デスクトップ アプリケーションのインストール後、コンソール担当者は、（Unified CM の Cisco Unified CM Attendant Console User ページの設定に従って）Unified CM Attendant Console のユーザ ID およびパスワードを入力して、このコンソール アプリケーションにログオンします。

（注）　Unified CM Attendant Console のユーザ ID は、Unified CM Attendant Console デスクトップ アプリケーションへのログインに必要であり、エンドユーザ ディレクトリに設定されたユーザおよび Unified CM のアプリケーション ユーザとは異なります。これらのユーザはエンドユーザ ディレクトリとは別に保存されるため、ディレクトリ検索で Unified CM Attendant Console ユーザ エントリは返されません。

Unified CM Attendant Console ユーザがログオンすると、Unified CM Attendant Console デスクトップ アプリケーションは、主に Remote Method Invocation（RMI）および Java Telephony Application Programming Interface（JTAPI）プロトコルを使用して、Unified CM と通信します。RMI は、登録、キープアライブ、および情報交換などの、デスクトップ クライアントと Unified CM Attendant Console サーバとの間の通信に使用されます。RMI トラフィックは、TCP ポート 1101 ～ 1129 の Unified CM、および 1 つ以上の一時的な、TCP ポートのデスクトップ アプリケーションから発生します。すべての RMI トラフィックは、ベストエフォートとしてマーキングされます。

JTAPI トラフィックは、Unified CM 上の CTIManager と Unified CM Attendant Console デスクトップ アプリケーションとの間で、デバイスおよび回線制御情報と呼制御トラフィックを伝送します。JTAPI トラフィックは、TCP ポート 2748 の Unified CM、および一時的な、TCP ポートのデスクトップ アプリケーションから発生します。

CTIManager と Unified CM Attendant Console クライアント間の JTAPI トラフィックは呼制御（コール フローの生成と処理）に使用されるため、24 の DSCP（CS3 の PHB）で、Unified CM により QoS マーキングされます。この方法により、その他のすべてのコール シグナリング トラフィックと同様にネットワークを通じて、Unified CM Attendant Console 電話制御トラフィックをキューに入れること

ができます。対称的なマーキングとキューを保証するため、Unified CM TCP ポート 2748 を宛先とする Attendant Console アプリケーション トラフィックも DSCP 24（PHB CS3）としてマーキングする必要があります。これにより、このトラフィックが、Unified CM および CTIManager に向かうネットワーク パスに沿って適切なコール シグナリング キューに配置されます。ただし、Unified CM Attendant Console クライアント アプリケーションはすべてのトラフィックをベストエフォートとしてマーキングするため、アクセス コントロール リスト（ACL）は、このトラフィックに適切に再マーキングするように設定する必要があります。

Unified CM Attendant Console サーバおよびデスクトップ クライアントのマーキングは、次のようにまとめることができます。

- Unified CM は、24 の DSCP（CS3 の PHB）で TCP ポート 2748 から発生するすべての JTAPI トラフィックを適切にマーキングします。
- Attendant Console デスクトップ アプリケーションは、Unified CM TCP ポート 2748 を宛先とする JTAPI トラフィックをベストエフォートとしてマーキングします。つまり、ACL は、0 の DSCP から 24 の DSCP（CS3 の PHB）まで、アプリケーションが Unified CM および Unified CM Attendant Console サーバに送信する JTAPI トラフィックを再マーキングするように、スイッチ ポート レベルで適用する必要があります。

Attendant Console のディレクトリ ウィンドウ

Attendant Console デスクトップ アプリケーションのディレクトリ ウィンドウを使用すると、コンソール担当者は Unified CM テレフォニー環境内のエンドユーザを検索できます。一般に、ディレクトリのリストは、Unified CM ディレクトリ自体の検索ではなく、ディレクトリ ファイルの検索によって取得されます。Unified CM Attendant Console アプリケーション ユーザがディレクトリ ウィンドウに検索条件を入力すると、次のいずれかのディレクトリ ファイルが検索されます。

- User list

  このディレクトリ ファイルは、ローカル PC またはローカル ドライブ パスに格納されています。このファイルを検索するには、Attendant Settings ダイアログボックスの Advanced タブの Path Name of Local Directory File フィールドで、その名前と場所を設定する必要があります。このフィールドでファイル名と場所が設定されていない場合、このオプションはスキップされ、ディレクトリ検索はその他のいずれかのディレクトリ ファイルに対して実行されます。

- AutoGenerated.txt

  このディレクトリ ファイルは、Unified CM Attendant Console サーバによって Unified CM データベースのエンドユーザ テーブルから自動的に生成され、Unified CM サーバに格納されています。ローカル ディレクトリのユーザ リスト ファイルが設定されていない場合、Unified CM Attendant Console デスクトップ アプリケーションは、Unified CM からこのファイルを自動的にダウンロードします。AutoGenerated.txt ファイルは、このファイルの情報が正確になるように、Unified CM Attendant Console サーバにより定期的にエンドユーザ ディレクトリから再生成または同期されます。この同期の頻度は、[Directory Sync Period] Unified CM Attendant Console サービス パラメータで決定されます（「Unified CM Attendant Console のサービス パラメータ」（P.24-37）を参照）。デフォルトでは、このパラメータは 3 時間に設定されるため、AutoGenerated.txt ファイルは 3 時間ごとに更新されます。

- CorporateDirectory.txt

  このファイルは、Cisco Unified CM Attendant Console User File Upload ツール（[Application] > [Cisco Unified CM Attendant Console]）を使用して、管理者が Unified CM に手動でインポートした場合にだけ使用できます。アップロードされると、Unified CM サーバの AutoGenerated.txt ファイルがこのファイルで置き換えられます。したがって、ローカル ユーザ リスト ファイルが設定されていない場合、Unified CM Attendant Console デスクトップ アプリケーションは AutoGenerated.txt ファイルではなくこのファイルをダウンロードします。

Unified CM Attendant Console デスクトップ アプリケーションが起動するたびに、上記のいずれかのディレクトリ ファイルがダウンロード（AutoGenerated または Corporate Directory.txt ファイルの場合）およびロードされます。アプリケーションが動作している限り、そのディレクトリ ファイルは、Attendant Settings ダイアログボックスの Advanced タブの Directory Reload Interval 設定に基づいて定期的にダウンロードまたは再ロード（あるいはその両方）が行われます。すべてのディレクトリ ファイルは、各行が 1 つのユーザ エントリのカンマ区切り形式になります。

デスクトップ アプリケーション内で、ディレクトリ ウィンドウ検索のためにディレクトリ ファイルをダウンロードすることで生成される追加のトラフィックは一般にわずかですが、いくつかの理由のために問題が生じることがあります。第 1 に、Unified CM ディレクトリ サイズが大きい場合、コンソール アプリケーションでダウンロードされる、ディレクトリ全体を含んだディレクトリ ファイルによって、ネットワークに大量のトラフィックが発生することがあります。この要因に、ネットワーク内の多数の Unified CM Attendant Console デスクトップ アプリケーションがある、ダウンロード間隔が短い、集中型のコール処理が配置されている、コンソール アプリケーションが低速 WAN リンクを通じてリモート サイトで実行される、などの条件が加わると、ネットワーク輻輳、遅延、およびキューの発生する可能性が非常に高くなります。

デスクトップ アプリケーション用 PC でローカル ユーザ リスト ファイルを使用すると、ネットワーク帯域幅や輻輳に関する多くの問題が解消されますが、Unified CM Attendant Console デスクトップのディレクトリ ウィンドウ内の [Advanced search] 機能で問題が発生しやすくなります。Unified CM Attendant Console デスクトップ アプリケーションのディレクトリ ウィンドウ内のその他のすべてのディレクトリ検索は、ローカル ユーザ リスト ファイルまたはダウンロードされたファイルのいずれかに対して実行されますが、ディレクトリ ウィンドウの [Advanced] ボタンで開く [Advanced search] ウィンドウを使用して実行する検索には例外があります。Advanced search ウィンドウを使用した検索では、ディレクトリ ファイル検索規則がバイパスされ、実行時に Unified CM エンドユーザ ディレクトリに対して直接生成されます。つまり、定期的なディレクトリ ファイルのダウンロード以上に、ネットワーク上に追加のトラフィックが生じます。さらに、Advanced search 機能を使用してダウンロードできるエントリ数には制限がありません。このようなリアルタイム検索と取得で追加のネットワーク負荷が発生するだけでなく、返されるエントリに制限がないため、この追加の負荷は非常に大きくなることがあります。ディレクトリ ファイルのダウンロードと Advanced directory search の両方で発生するトラフィックは、ベストエフォートとしてマーキングされる RMI プロトコルを使用するため、ネットワーク パスでプライオリティ ボイス メディアおよびプロビジョニングされたコール シグナリング キューに輻輳の発生するリスクはありません。ただし、Unified CM Attendant Console デスクトップ アプリケーション ディレクトリのトラフィックによって、ベストエフォート キューの輻輳が発生し、ディレクトリ トラフィックおよびその他のベストエフォート ネットワーク データ トラフィックのドロップにつながる可能性が残ります。

Unified CM Attendant Console デスクトップ アプリケーションのディレクトリ ファイルのダウンロードおよびディレクトリ検索では、ネットワークの輻輳が発生する可能性があるため、次の対策を取ることをお勧めします。

- 管理者は、すべての Attendant Console ユーザに、Advanced directory search 機能の使用制限を求める必要があります。さらに、ユーザがこの機能を使用する場合は、返されるエントリの数を減らすために、Advanced search のパラメータ フィールドにできる限り多くの情報を入力してもらう必要があります。
- 集中型のコール処理配置シナリオでは、低速 WAN リンクを通じた Unified CM からのディレクトリ ファイルの定期的なダウンロードをなくすために、リモート サイト Unified CM Attendant Console ユーザに対して Unified CM Attendant Console クライアント PC またはネットワーク共有のユーザ リスト ファイルを利用する必要があります。最小限の管理オーバーヘッドでこの目標を達成する 1 つの方法は、各リモート サイトのローカル ネットワーク共有にユーザ リスト ファイルを提供することです。ディレクトリから自動的に生成され、次にオフピーク時間または深夜にリモート ネットワーク共有にロードされたユーザ リスト ファイルがあるか調べる必要があります。これにより、ピーク業務時間中にネットワーク輻輳が発生する可能性を抑えます。このようにすると、毎朝、Unified CM Attendant Console ユーザがデスクトップ コンソールを起動するときに、このアプリケーションは最新のディレクトリ ユーザ リストをダウンロードできます。

これらの推奨事項は、次の 1 つ以上の条件が該当する場合は特に重要です。

- Unified CM クラスタ内に多数の Unified CM Attendant Console ユーザが存在する。
- 低速 WAN リンクによって Unified CM サーバから分離された多数の Unified CM Attendant Console ユーザが存在する。
- エンドユーザ ディレクトリが非常に大きい。

Unified CM Attendant Console の冗長性

Unified CM Attendant Console アプリケーションの冗長性は、次の 2 つのレベルで実現できます。

- コンポーネント レベルとサービス レベルでの冗長性

  このレベルでの冗長性については、Unified CM Attendant Console サービスまたはサーバの冗長性、および CTIManager サービスの冗長性に関して検討する必要があります。同様に、パブリッシャの冗長性の欠如、およびこのコンポーネントの障害の影響も検討する必要があります。

- デバイス レベルと到達可能性レベルでの冗長性

  このレベルでの冗長性は、コンソール担当者の電話機、Unified CM Attendant Console パイロット ポイント、および Attendant Console デスクトップ アプリケーションに関連して検討し、さらにコンソール担当者とパイロット ポイントの到達可能性に関する冗長性として検討する必要があります。

サービスとコンポーネントの冗長性

図 24-13 に示すように、Unified CM Attendant Console 機能は、主に Cisco CallManager Attendant Console Server サービスおよび Cisco CTIManager サービスに依存します。いずれの場合にも、冗長性は Unified CM クラスタ アーキテクチャに組み込まれます。Unified CM Attendant Console Server サービスと CTIManager サービスの両方に対する冗長性は、各サービスが実行されるクラスタ内のノード数によって決定されます。冗長性は、サーバで障害が発生しても必要なサービスを提供し続けることができる障害の最大数で決まります。この数は、公式（N - 1）で表現でき、N はサービスを実行しているサーバの数です。たとえば、クラスタ内の 3 台のサーバが Cisco CallManager Attendant Console Server サービスを実行している場合は、N = 3 です。このサービスの冗長性を計算すると、(3 - 1)、つまり 2 になります。したがって、最大 2 台のサーバの障害に対して冗長性が確保されることになります。CTIManager の冗長性は、同じ公式を使用して計算できます。これらのサービスで最大限の冗長性を得るには、クラスタ内のすべてのコール処理ノードで Unified CM Attendant Console Server サービスと CTIManager サービスの両方を実行することをお勧めします。これに対し、最小限の冗長性を得るには、これらの各サービスを、クラスタ内の少なくとも 2 つのコール処理ノードで実行する必要があります。

パブリッシャは、Unified CM データベースへの Unified CM Attendant Console アプリケーション情報の書き込み時に単一の障害点となります。Unified CM Attendant Console アプリケーションに対するパブリッシャの障害の影響はわずかです。パブリッシャに障害が発生しても、Unified CM Attendant Console アプリケーションのすべての部分が引き続き動作します。ただし、Unified CM Attendant Console アプリケーション設定を変更できなくなります。パブリッシャが復元するまで、Unified CM Attendant Console パイロット ポイント、ハント グループ、およびコンソール担当者の電話機の設定は変更できません。

デバイスと到達可能性の冗長性

デバイス レベルの Unified CM Attendant Console の冗長性は、いくつかのメカニズムに依存しています。まず第 1 に、コンソール担当者の電話機と Unified CM Attendant Console パイロット ポイントは、デバイス登録用のデバイス プールと Unified CM グループ設定の組み合せによって提供される組み込み冗長性に依存します。

また、一部のデバイスは、追加の冗長性および機能のためにコンポーネント サービスに依存します。たとえば、Unified CM Attendant Console パイロット ポイントは呼制御機能で CTIManager にも依存するため、前の項で説明した CTIManager の冗長性に依存する必要があります。

Attendant Console デスクトップ アプリケーションも、冗長性および機能がコンポーネント サービスに依存します。Unified CM Attendant Console デスクトップ アプリケーションは、着信コールの処理を継続できるように、冗長 Unified CM Attendant Console Servers サービスと CTIManager サービス間の自動フェールオーバーをサポートしています。Unified CM Attendant Console デスクトップ アプリケーションから見ると、これらのサービスの冗長性は以下に説明するように、Unified CM グループ メカニズムによって決定されます。第 1 に、Unified CM Attendant Console デスクトップ アプリケーションが起動され、コンソール担当者がログインすると、このアプリケーションはデバイス プールおよび Unified CM グループ設定に基づいて、Unified CM のリストをダウンロードします。このリストは、ローカル PC の GlobalSettings.xml ファイルに保存され、デスクトップ用の CTIManager サービスの冗長性を決定します。

（注）　Attendant Settings ダイアログボックスの Basic タブの Attendant Server Host Name フィールドまたは IP Address フィールドには、コンソール担当者の電話機に対して Unified CM グループで設定したプライマリ Unified CM サーバの IP アドレスを入力することをお勧めします。このように入力すると、障害が発生した場合、コンソール担当者の電話機と Unified CM Attendant Console デスクトップ アプリケーションの両方が、電話機に設定された Unified CM グループの次のサーバに同時にフェールオーバーします。

次に、デスクトップ アプリケーションは Unified CM Attendant Console サーバの冗長性に関して、デバイス プールおよび（コンソール担当者の電話機がメンバーとなっている）Unified CM Attendant Console パイロット ポイントの Unified CM グループに依存します。いずれの場合にも、Unified CM グループには最大 3 台のサーバを設定できるため、最大 3 次の冗長性が実現します。

デスクトップ アプリケーションに対して、これらのサービスの冗長性をさらに与えるには、Attendant Settings ダイアログボックスの Advanced タブの Call Processing Server Host Names フィールドまたは IP Addresses フィールドを使用します。このフィールドで Unified CM サーバのカンマ区切りリストを設定すると、Unified CM グループ メカニズムを超える冗長性を実現できます。ただし、この追加の冗長性はグループ メカニズムを使い切った場合にだけ役に立つため、不要なことがあります。この追加の冗長性は、実際上、コンソール担当者の電話機と Unified CM Attendant Console パイロット ポイントに登録サービスを提供している最初の 3 つのサーバが使用できない（つまり、コンソール担当者の電話機と Unified CM Attendant Console パイロット ポイントも使用できない）場合にだけ利用されます。電話機とパイロット ポイントが使用できない場合、デスクトップ アプリケーションは使用できません。

最後に、Unified CM Attendant Console パイロット ポイントでハント グループ メカニズムに組み込まれた到達可能性の冗長性（これにより、所定の冗長性が着信コールの発信者に提供されます）のほかに、追加の冗長性を Unified CM Attendant Console パイロット ポイントの障害に対して提供することもできます。Unified CM Attendant Console パイロット ポイントに障害が発生した場合、パイロット ポイント番号をダイヤルする着信コールの発信者にはビジー トーンが聞こえます。パイロット ポイントにフェールオーバー メカニズムを提供するには、パイロット ポイント回線設定画面の [Call Forward No Answer (CFNA)] フィールドで、別の Unified CM Attendant Console パイロット ポイント番号を設定します。この CFNA メカニズムによって、障害の発生したパイロット ポイントへの発信者は、コールの処理およびルーティングのために別のパイロット ポイントに確実に転送されます。

Unified CM Attendant Console に関するガイドラインと制限

Unified CM Attendant Console は JTAPI レベルでパーティションを認識するため、Attendant Console デスクトップ アプリケーションは回線制御という点に関してパーティションを認識します。これに対し、他の Unified CM Attendant Console コンポーネントはパーティションを認識しなかったり、重複や共有内線番号に関していくつかの制限があったりします。ディレクトリ番号のプロビジョニングを計画する場合は、次のガイドラインに注意してください。

- ハント グループ
  - シェアドラインは、ハント グループ メンバーが使用することはできません。
  - 重複内線番号は、ハント グループ メンバーが使用することはできません。
  - ハント グループ メンバーのディレクトリ番号は、Unified CM 回線グループに追加できません。
- パイロット ポイント
  - シェアドラインは、パイロット ポイントのディレクトリ番号として使用できません。
  - パイロット ポイントのディレクトリ番号は、Unified CM 回線グループに追加できません。
- コンソール ディレクトリと短縮ダイヤル ウィンドウ

  コンソール ディレクトリおよび短縮ダイヤルのウィンドウ内の回線ステータス表示では、シェアドラインと重複内線番号については何もわかりません。このため、共有または重複回線が見つかった場合は、最近変更された回線インスタンスのステータスだけが表示されます。

また、ハント グループ メンバーのディレクトリ番号があるすべてのパーティションを含むコーリング サーチ スペースを、必ずすべての Unified CM Attendant Console パイロット ポイントに設定してください。このように設定しないと、1 つ以上のメンバーが到達不可能になります。

Unified CM Attendant Console のパフォーマンスとキャパシティ

Cisco Unified CM Attendant Console アプリケーションは、次のキャパシティをサポートしています。

- クラスタあたり最大 500 のコンソール担当者。
- クラスタあたり最大 500 のパイロット ポイント。
- Cisco MCS-7845 サーバあたり最大 125 のコンソール担当者とパイロット ポイント ペア。
- Cisco MCS-7835 サーバあたり最大 100 のコンソール担当者とパイロット ポイント ペア。
- Cisco MCS-7825 サーバあたり最大 75 のコンソール担当者とパイロット ポイント ペア。
- Cisco MCS-7845 サーバは最大 1250 の Unified CM Attendant Console デバイスをサポートします。
- Cisco MCS-7835 サーバは最大 1000 の Unified CM Attendant Console デバイスをサポートします。
- Cisco MCS-7825 サーバは最大 750 の Unified CM Attendant Console デバイスをサポートします。

（注） Unified CM Attendant Console デバイスのキャパシティ数は、ハント パイロットとハント パイロット メンバーの間で分割できます。たとえば、MCS-7845 サーバでは Unified CM Attendant Console デバイスの最大数は 1250 です。このキャパシティをさまざまな方法で割り当てることができます。125 のハント パイロットを用意して各ハント パイロットに 10 メンバーを含めたり、10 のハント パイロットを用意して各ハント パイロットに 125 メンバーを含めたりすることができます。

最大で 500 のコンソール担当者および 500 のパイロット ポイントをサポートするには、コンソール担当者およびパイロット ポイントはMCS-7845 サーバあたり 125 ペア以下、MCS-7835 サーバあたり 100 ペア以下、およびMCS-7825 サーバあたり 75 ペア以下、のグループで複数のサーバを通じて分散する必要があります。

Cisco Unified CM Attendant Console アプリケーションは、回線監視および電話機制御のために CTIManager と対話します。コンソール担当者の電話機の各回線が、CTIManager への接続に必要です。また、各 Unified CM Attendant Console パイロット ポイントは、CTIManager からの CTI 回線が必要になります。Unified CM Attendant Console アプリケーションを設定する場合、必要な CTI 回線または接続の数については、CTI 回線または接続に対する全体的なクラスタ制限に関して検討する必要があります（クラスタごとの CTI 接続制限の詳細については、「Unified CM のキャパシティ プランニング」（P.8-22）を参照してください）。追加の CTI 回線が別のアプリケーションに必要になる場合、これらの CTI 回線によって Unified CM Attendant Console アプリケーションのキャパシティが制限される場合があります。

Unified CM Attendant Console と EM の相互作用

Unified CM Attendant Console ユーザは、EM を使用してそれぞれの電話機にログインできます。ただし、コンソール担当者の電話機で設定が変更されるたびに、Unified CM Attendant Console デスクトップ アプリケーションでは、Unified CM Attendant Console ユーザがアプリケーションからログアウトしてログインし直す必要があります。EM ログイン（またはログアウト）によって電話機で設定が変更されるため、Unified CM Attendant Console と EM を組み合せて使用する場合、ユーザは EM を使用してそれぞれの電話機にログインしてから、Unified CM Attendant Console デスクトップ アプリケーションにログインします。これによって、デスクトップ アプリケーションからログアウトしてログインし直す必要がなくなります。

また、EM および Unified CM Attendant Console ユーザの DN は、Device Members ではなく User Members として Unified CM Attendant Console パイロット ポイントのハント グループに追加する必要があります。このようにすると、EM を使用してそれぞれの電話機にログインしていないために利用不可となっている Unified CM Attendant Console ユーザに、着信コールがルーティングされなくなります。ハント グループの User Members は、ユーザ名と回線番号の両方で設定されます。これに対して、Device Members は、ディレクトリ番号だけで設定されます。パイロット ポイントは、ディレクトリ番号がビジーでないことだけを確認してから、Device Members にコールをルーティングします。パイロット ポイントは、コンソール担当者の電話機の回線番号が使用可能で、Unified CM Attendant Console ユーザがログオンし、オンラインであることを確認してから、User Members にコールをルーティングします。このため、User Members として EM Unified CM Attendant Console ユーザをハント グループに追加することにより、EM Unified CM Attendant Console ユーザがログインしている場合にだけ、ユーザの電話機にコールを送信することができます。

Cisco Unified Department、Business、および Enterprise Attendant Console

Cisco Unified Department、Business、および Enterprise Attendant Console には、コンソール担当者の Windows PC にインストールするクライアント アテンダント コンソール アプリケーションが用意されています。また、Unified CM とは別の物理サーバにインストールされたアテンダント コンソール サーバ アプリケーションも必要です。アテンダント コンソール アプリケーションはアテンダント コンソール サーバ アプリケーションと通信し、アテンダント コンソール サーバ アプリケーションは Secure Socket Layer（SSL）接続で CTI および AVVID XML Layer（AXL）を介して安全に Unified CM と通信します。複数のアテンダント コンソールを 1 つのアテンダント コンソール サーバに接続できます。アテンダント コンソールの Department、Business、および Enterprise バージョンは、サポートされるオペレータ クライアントの数やサポートされるディレクトリ エントリの数など、各種の機能の制限がそれぞれ異なります。

機能とアーキテクチャ

図 24-14 は、Cisco Unified Department、Business、または Enterprise Attendant Console 統合のハイレベルなアーキテクチャを示しています。ソリューションの機能と動作を理解することにより、アーキテクチャ自体の理解も深まります。次の一連の手順（図 24-14 を参照）は、アテンダント コンソールへの一般的なコールに関係するイベントを示しています。

1. コールが Unified CM に入ります。着信番号は CTI ルート ポイントに設定されたディレクトリ番号と一致します。
2. CTI ルート ポイントは、アテンダント コンソール サーバ アプリケーションによって CTI が制御され、サーバに設定されているキュー Direct Dial In（DDI）に関連付けられます。
3. アテンダント コンソール サーバ アプリケーションは、コールを直接 Computer Telephony（CT）ゲートウェイ デバイスのいずれかに内部的にリダイレクトします。このプロセスの一環として、アテンダント コンソール サーバ アプリケーションは、コールを CTI ポートにリダイレクトする CTI リダイレクト メッセージを CTI Manager サービスに送信します。

（注）　CTI リダイレクト メッセージでは、コールは接続されません。コールへの応答はなく、メディア接続もありません。

4. アテンダント コンソール サーバ アプリケーションはここで、コールを CT ゲートウェイ デバイスに関連付け、CTI ポートでそのコールを制御します。
5. この時点で、コールは、キュー DDI に関連付けられたシステム内のアテンダント コンソール クライアント アプリケーションに送信されます。
6. コンソール担当者がアテンダント コンソール クライアント アプリケーションを介してコールに応答することを選択すると、別の CTI リダイレクト メッセージが CTI Manager サービスに送信され、それによってコールが CTI ポートから応答するコンソール担当者の電話機に転送されます。コールは、コンソール担当者の電話機の設定に応じて、その電話機のハンドセットまたはヘッドセットに自動的に接続します。コンソール担当者の電話機および発信側のゲートウェイまたは電話機のリージョンとロケーションの設定によって、メディアに使用されるコーデックが決定します。
7. 別の内線番号への転送が必要である場合、コンソール担当者はアテンダント コンソール クライアント アプリケーションを介して転送を開始し、アテンダント コンソール サーバ アプリケーションに転送を伝達します。
8. アテンダント コンソール サーバ アプリケーションはそのコールを内部的にサービス キューに関連付け、CTI リダイレクト メッセージを CTI Manager サービスに送信します。これによって、コールはコンソール担当者の電話機からアテンダント コンソール サーバ アプリケーションによって制御される CTI ポートにリダイレクトされます。

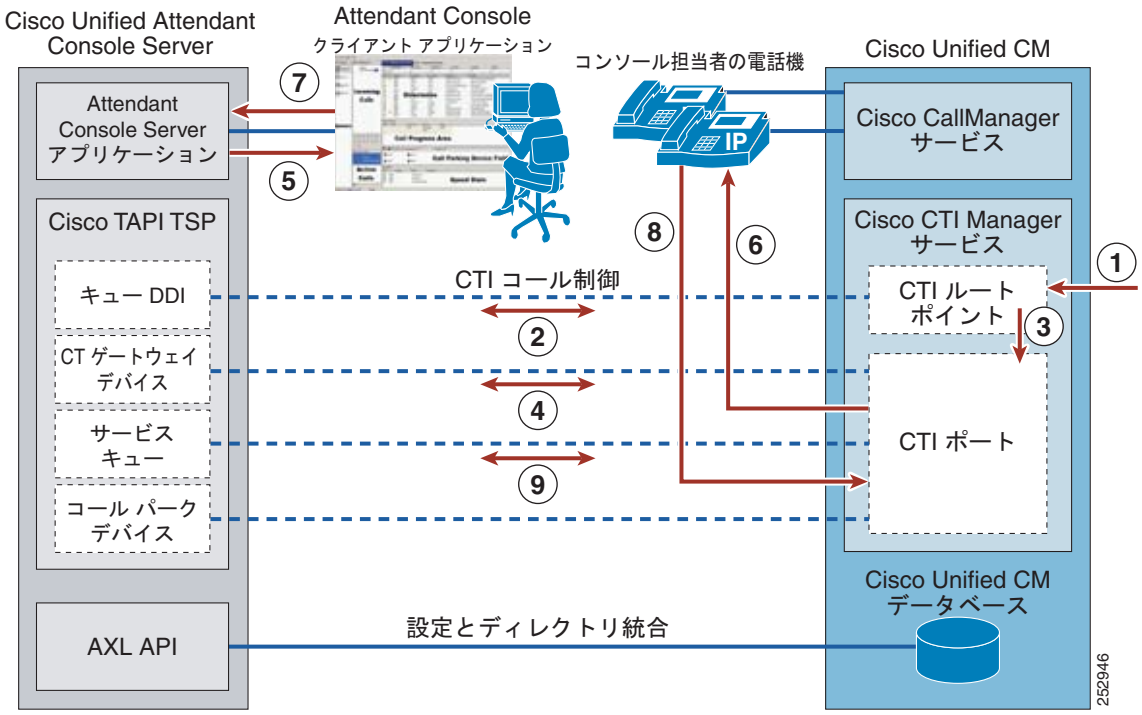
（注）　コール転送はコンソール担当者の電話機から発信される場合もありますが、その場合はアテンダント コンソール サーバ アプリケーションがコール フローから外れ、拡張機能（転送再コール機能など）は利用できなくなります。

9. この段階で、サービス キューは転送を実行する前にコールに実際に応答するので（短い接続があります）、アテンダント コンソール サーバ アプリケーションにインストールされた Cisco TAPI Wave ドライバが起動します。この CTI ポートおよびコール開始ゲートウェイまたは電話機のリージョンとロケーションの設定によって、メディアに使用されるコーデックが決定します。設定されている CTI ポートの Music on Hold（MoH）オーディオ ソースも、発信者に聞こえる MoH に影響します。転送はこのように実行されるので、応答がない場合、アテンダント コンソール クライアント アプリケーションが引き続きコールを制御します。最終的な相手がコールを受信すると、アテンダント コンソール サーバ アプリケーションはコール フローから外れます。

（注）　アテンダント コンソール サーバ アプリケーションにインストールされる Cisco TAPI Wave ドライバは、G.711 コーデックだけをサポートします。サービス キューおよびコール パーク デバイスに対応する CTI ポートを設定する場合は、これらの CTI ポートに、G.711 の使用を指示する他のデバイスとのリージョンが設定されるようにシステムを設計するか、そうでなければトランスコーディング メディア リソースを装備します。

（注）　Cisco TAPI Wave ドライバによる G.711 a-law コーデックのサポートは、Cisco Unified CM 7.1(2) および Cisco TSP 7.1(3.3) 以降のリリースで導入されました。

図 24-14　Cisco Unified Department、Business、および Enterprise Attendant Console のアーキテクチャ



アテンダント コンソール サーバ アプリケーションのコール パーク機能では、Unified CM の固有のコール パーク機能は使用されません。代わりに、コール パーク デバイスを使用する独自のコール パーク機能が使用されます。コール パーク デバイスは、図 24-14 のステップ 7 ～ 9 にあるように、サービス キューとほとんど同様に機能します。転送と同様に、コール パーク デバイスを利用することで、コールのパーク中にアテンダント コンソール サーバ アプリケーションがコールを制御できるようになります。Cisco TAPI Wave Driver のコーデック制限（G.711 だけをサポート）は、コール パーク デバイスがかかわるコールにも影響します。

冗長性

CTI と AXL 通信の両方について、統合の両側に冗長性を備えることを検討する必要があります。

CTI に関しては、アテンダント コンソール サーバ アプリケーションは Cisco Telephony Service Provider（TSP）プラグイン（Unified CM からダウンロード）を使用して、CTI Manager サービスと通信します。Cisco TSP では、プライマリとバックアップの CTI Manager サービスを設定できます。

プライマリの CTI Manager サービスがオフラインになった場合の復元性を高めるため、クラスタ内の少なくとも 2 つの Unified CM サブスクライバ ノードで CTI Manager サービスを有効にすることをお勧めします。現在、アテンダント コンソール サーバ アプリケーションに対する復元性の機能はありません。したがって、アテンダント コンソール サーバに障害が発生した場合の復元性を得るには、キュー DDI に関連付けられたすべての CTI ルート ポイントに Call Forward No Answer（CFNA）の宛先を設定します。アテンダント コンソール サーバ アプリケーションがオフラインになると、コールは自動的に CFNA の設定に従います。たとえば、宛先を 1 台の IP 電話に関連付けられたハント パイロット番号またはディレクトリ番号（DN）にすることができます。

AXL 通信を有効にするには、Unified CM ノードで Cisco AXL Web Service をアクティブにします。複数の Unified CM ノードで Cisco AXL Web Service を有効にすることができますが、アテンダント コンソール サーバ アプリケーションには Unified CM 接続用に 1 つのエントリしか設定できません。障害が発生した場合、管理者は Cisco AXL Web Service を実行するバックアップ用の Unified CM ノードにこのエントリをアップデートできます。

また、Unified CM には、Unified Department、Business、および Enterprise Attendant Console ソリューションとの統合用に一連の CTI ルート ポイントおよび CTI ポートが用意されています。これらのデバイスにはデバイス プールがあり、そのため Unified CM グループに割り当てられて、登録を維持する役割を果たす Unified CM コール処理ノードの優先順位別リストが示されます。Unified CM グループ内のプライマリの Unified CM がオフラインである場合、CTI ルート ポイントと CTI ポートはセカンダリの Unified CM ノードを登録できるので、CTI ルート ポイントおよびポート自体の高可用性が実現します。

ガイドラインと制限

次の設計上のガイドラインと制限は、Unified CM テレフォニー環境内の Cisco Unified Department、Business、および Enterprise Attendant Console の配置および動作に関して適用されます。

- 次の一般的な設計指針は、アテンダント コンソール サーバ アプリケーション コンポーネントに適用します。
  - キュー DDI

    1 つの固有なキュー DDI が、特にアテンダント コンソールにルーティングされる、システム内の固有の着信ディレクトリ番号ごとに必要です。
  - CT ゲートウェイ デバイス

    キュー DDI に入るすべての着信コールは、直接 CT ゲートウェイ デバイスにリダイレクトされます。CT ゲートウェイ デバイスが所定の時間に予想される最大着信コール数を処理するのに十分な台数になるよう、システムを設計してください。
  - サービス キュー

    コンソール担当者がコールを転送するか、コールを保留にするたびに、サービス キューが必要になります。システム内のすべてのコンソール担当者が所定の時間に転送する、または保留にするコールの最大数を維持できるだけの十分なサービス キューが用意されるように、システムを設計する必要があります。コンソール担当者ごとに 3 つか 4 つのサービス キューを用意することが一般的なガイドラインですが、シナリオによってはさらに多くのキューが必要になる場合もあります。
  - コール パーク デバイス

    コンソール担当者がアテンダント コンソール クライアント アプリケーションを介してコール パーク機能を起動するたびに、コール パーク デバイスが必要になります。この機能では、Unified CM の固有のコール パーク機能は使用されません。所定の時間にシステム内のすべてのコンソール担当者がパークするコールの最大数を処理できるだけの十分なコール パーク デバイスが用意されるように、システムを設計してください。

- アテンダント コンソール サーバ アプリケーションに設定されたすべてのキュー DDI、CT ゲートウェイ デバイス、サービス キュー、およびコール パーク デバイスによって、Unified CM 内の CTI ルート ポイントまたは CTI ポートが作成されます。また、Unified Department、Business、または Enterprise Attendant Console の統合を処理するために必要な CTI 接続の数も、クラスタごとの CTI 接続制限までカウントされます（クラスタごとの CTI 接続制限の詳細については、「Unified CM のキャパシティ プランニング」（P.8-22）を参照してください）。
- インストールされた Cisco TSP の各インスタンスは、最大 255 の CTI ポートをサポートします。
- アテンダント コンソール サーバ アプリケーションにインストールされる Cisco TAPI Wave ドライバは、G.711 コーデックだけをサポートします。サービス キューおよびコール パーク デバイスに対応する CTI ポートを設定する場合は、これらの CTI ポートに、G.711 の使用を指示する他のデバイスとのリージョンが設定されるようにシステムを設計するか、そうでなければトランスコーディング メディア リソースを装備します。
- アテンダント コンソール サーバ アプリケーションは、エンドユーザ デバイスの Busy Lamp Field（BLF; ビジー ランプ フィールド）モニタリングを可能にしますが、このアプリケーションでは、BLF 短縮ダイヤル機能を実現する Unified CM 内の同一機能は使用されないことに注意してください。代わりに、アテンダント コンソール サーバ アプリケーションは、CTI を介して Unified CM と通信することで、監視対象デバイスの回線状態情報を取得します。
- Quality of Service（QoS）に関しては、アテンダント コンソール サーバ アプリケーション、アテンダント コンソール クライアント アプリケーション、および Cisco TSP はすべて Best Effort としてマークされたトラフィック（DSCP=0）を送信します。このトラフィックが WAN または通常輻輳するリンクを経由する場合は、ネットワークを介して優先的に処理されるようにパケットにマーキングする必要があります。これらのアプリケーションに関連付けられた TCP ポート番号の完全なリストについては、次の Web サイトで適切なログイン認証によって入手可能な Unified Department、Business、または Enterprise Attendant Console の設計ガイドを参照してください。

  http://www.cisco.com/go/ac
- アテンダント コンソール サーバ アプリケーションは、パーティションを認識しません。したがって、複数のパーティションに同じディレクトリ番号（DN）が存在する場合、監視対象のデバイスの DN に誤りが生じる可能性があります。
- Cisco Unified Department、Business、および Enterprise Attendant Console は、Cisco Unified Presence Server にも統合できます。このタイプの統合の詳細については、次の Web サイトで入手できる適切な Unified Department、Business、または Enterprise Attendant Console 管理ガイドを参照してください。

  http://www.cisco.com/en/US/products/ps7282/prod_maintenance_guides_list.html
- 各種の Unified Department、Business、および Enterprise Attendant Console のパフォーマンスとキャパシティについては、次の Web サイトで入手できる製品マニュアルを参照してください。

  http://www.cisco.com/en/US/products/ps7282/tsd_products_support_series_home.html

WebDialer

WebDialer は Cisco Unified CM のクリックコール アプリケーションで、ユーザがサポートされる任意の電話デバイスを使用して自分の PC から簡単にコールを発信できます。管理者が CTI リンクを管理したり、JTAPI または TAPI アプリケーションを作成したりするために必要なものはありません。Cisco WebDialer には、独自のユーザ インターフェイスと認証メカニズムを提供するための、簡単な Web アプリケーションと HTTP または Simple Objects Access Protocol（SOAP）が用意されているからです。Cisco Unified Communications Widget の**クリックコール**アプリケーションは SOAP インターフェイスを使用し、現在は次の Web サイトでダウンロードすることができます（ログイン認証が必要です）。

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

WebDialer の電話機のサポート

次の SCCP 電話機は WebDialer をサポートしています。

- Cisco Unified IP Phone 7902G
- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7912G および 7912G-A
- Cisco Unified Wireless IP Phone 7920、7921G、および 7925G
- Cisco Unified IP Phone 7935G、7936G、および 7937G
- Cisco Unified IP Phone 7940G、7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7960G、7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G
- Cisco Unified IP Phone 7985G
- Cisco IP Communicator

また、次の SIP 電話機は WebDialer をサポートしています。

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G
- Cisco IP Communicator

（注） Cisco Unified Personal Communicator は、デスクフォン モードで実行しているときに限り WebDialer をサポートします。Cisco Unified Personal Communicator がデスクフォン モードである場合、WebDialer によってサポートされる電話機モデルである限り、WebDialer を使用してデスク電話にクリックコール機能を備えることができます。ソフトフォン モードの Cisco Unified Personal Communicator は、WebDialer をサポートしません。

Unified CM および WebDialer のサービス パラメータ

WebDialer アプリケーションを有効にするには、システム管理者は Cisco Unified Serviceability インターフェイスからいくつかの Unified CM 機能サービスをアクティブにし、起動する必要があります。また、WebDialer サービス パラメータは、WebDialer アプリケーションおよびサービスの動作を決定するための設定およびカスタマイズのオプションを提供します。

WebDialer 用の Unified CM サービス

WebDialer アプリケーションは次の機能サービスに依存します。これらのサービスは、Serviceability ページから手動でアクティブにする必要があります。

- Cisco WebDialer Web Service
- Cisco CTIManager

Cisco WebDialer Service は Web ベースのクリックコール、デスクトップ ベースのアプリケーション、および Unified CM 間のインターフェイス ポイントです。Cisco CTIManager Service は、Unified CM のコール処理およびデータベース レイヤと対話することで WebDialer から受信される要求を処理します。電話機および呼制御機能の最終結果がアプリケーションでは見えるようになっています。

WebDialer サービス パラメータ

次の項目は、WebDialer 機能に関連する Cisco WebDialer Web Service サービス パラメータの一部のリストです。

- CTIManager Connection Security Flag（デフォルト値 = Non Secure）

  このパラメータは、Cisco WebDialer Web サービスと CTIManager との間でセキュアなトランスポート レイヤ セキュリティ（TLS）接続を使用するかどうかを決定します。有効な場合は、アプリケーション ユーザの WDSecureSysUser のインスタンス ID に対して設定した Certificate Authority Proxy Function（CAPF）プロファイルを使用して、セキュアな接続が設定されます。このインスタンス ID は、サービス パラメータの CAPF Profile Instance ID for Secure Connection to CTIManager で指定する必要があります。

  （注）　アプリケーション ユーザの WDSecureSysUser は、インストール時に自動的に作成されるシステム アカウントです。削除できません。

- CAPF Profile Instance ID for Secure Connection to CTI Manager（デフォルト値 = <None>）

  CAPF Profile Instance ID は、WDSecureSysUser アプリケーション ユーザに対して Cisco WebDialer Web サービスと CTIManager との間で確立される TLS 接続またはインスタンスを識別するために使用される、数値または文字（あるいはその両方）の一意のストリングです。CTI Manager Connection Security Flag パラメータを True に設定した場合、このパラメータに値を設定する必要があります

- Primary Cisco CTIManager（デフォルト値 = 127.0.0.1）

  このパラメータは、要求の処理時に WebDialer が使用するところの CTIManager サービスが実行している Unified CM サブスクライバの IP アドレスを指定します。これはクラスタ全体のパラメータです。

- Backup Cisco CTIManager（デフォルト値 = <ブランク>）

  このパラメータは、要求の処理時に WebDialer が使用するところのバックアップ インスタンスの CTIManager サービスが実行している Unified CM サブスクライバの IP アドレスを指定します。これはクラスタ全体のパラメータです。

- List of WebDialers（デフォルト値 = <ブランク>）

  このパラメータは、企業内のすべての WebDialer の IP アドレスとポート番号を指定します。複数のエントリを区切るにはスペースを使用します。このパラメータは、Redirector 機能が必要な場合にだけ入力する必要があります。

- User Session Expiry（デフォルト値 =0）

  このパラメータは、ユーザ セッションまたはブラウザ クッキーが期限切れになる期間を時間単位で指定します。この値が 0 であると、セッションまたはブラウザ クッキーには期限がありません。

WebDialer サービス パラメータの全リストについては、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Features and Services Guide*』の Cisco WebDialer 情報を参照してください。

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

WebDialer の機能とアーキテクチャ

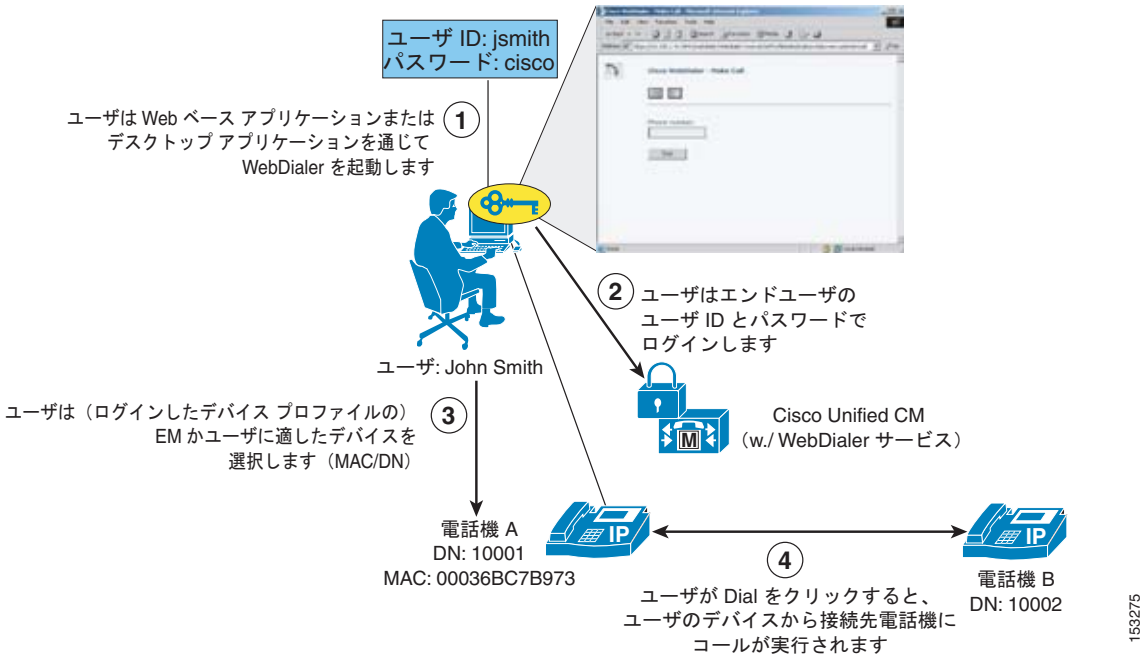
WebDialer アプリケーションには、WebDialer サーブレットと Redirector サーブレットの 2 つのサーブレットが含まれています。サブスクライバ サーバで Cisco WebDialer Web サービスがアクティブである場合、両方のサーブレットが有効になります。これらのサーブレットは関連していますが、それぞれ異なる機能を提供し、同時に実行するように設定できます。

WebDialer サーブレット

図 24-15 は、単純な WebDialer の例を示しています。この例で、ユーザ John Smith は、Unified Communications Widget のクリック コールなどの Web ベース アプリケーションまたはデスクトップ アプリケーションから WebDialer を起動します（ステップ 1）。WebDialer は、ログイン クレデンシャル要求で応答します。ユーザは、Unified CM エンドユーザ ディレクトリで設定される有効なユーザ ID とパスワードで応答する必要があります。この場合、John Smith は userID = jsmith および password = cisco を送信します（ステップ 2）。次に、このログインに基づいて、WebDialer は Cisco WebDialer Preferences 設定ページで応答し、ユーザは「User permanent device」または「Use Extension Mobility」のいずれかを示す必要があります（ユーザが EM デバイス プロファイルを持つと想定して）。この場合、ユーザ John Smith は、「User permanent device」を選択し、設定ページのドロップダウン メニューからその電話機に対して適切な MAC アドレス（SEP00036BC7B973）とディレクトリ番号（10001）を選択します（ステップ 3）。最後に、コールする電話番号を要求する画面が表示され（この値はすでに表示されていることがあります）、ユーザは [Dial] をクリックする必要があります。この場合、John Smith が 10002 と入力し、Dial をクリックすると、その電話機から番号 10002 の電話機 B へのコールが自動的に生成されます（ステップ 4）。

（注） ユーザが以前に WebDialer アプリケーションにログインし、Web ブラウザおよびサーバの Cookie がまだアクティブになっている場合、次の要求時に再ログインは求められません。Cookie がブラウザでクリアされるか、または WebDialer サーバの再起動によってクリアされた場合は、再ログインが要求されます。一方、ユーザ Web ブラウザ クッキーは期限を WebDialer サービス パラメータ で設定できます。これは、WebDialer サービス パラメータ で設定された通り所定の時間が経過した後、自動的に期限切れになります（「WebDialer サービス パラメータ」（P.24-53）を参照）。

図 24-15　WebDialer サーブレットの動作



Redirector サーブレット

Redirector サーブレットは、マルチクラスタまたは分散型のコール処理環境において、WebDialer 機能を提供します。この機能を使用すると、すべての Unified CM クラスタ間で単一の企業全体の Web ベース WebDialer アプリケーションを使用できます。図 24-16 は、WebDialer アプリケーションの一部として Redirector サーブレットの基本的な動作を示しています。この例で、この企業には 3 個の Unified CM クラスタとして、New York、Chicago、および San Francisco があります。3 個のクラスタはすべて、単一の WebDialer アプリケーションで設定されます。San Francisco クラスタは、Redirector として指定されます。企業全体の Redirector として San Francisco の WebDialer を指定するには、各クラスタ WebDialer サーバに独自の IP アドレス、および San Francisco の WebDialer IP アドレスで指定されたサービス パラメータ List of WebDialer が必要です（「WebDialer サービス パラメータ」（P.24-53）を参照）。

（注）　Cisco Unified CM 7.1(2) 以降のリリースでは、[List of WebDialers] も [Application Server] メニューから設定できます。詳細については、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html にある『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

San Francisco の WebDialer サーバには、独自の IP アドレスと、企業内のその他の WebDialer サーバすべてのアドレスが設定されます。この例に基づいて、各 WebDialer サーバの List of WebDialers サービス パラメータ フィールドは、次のように設定されます。

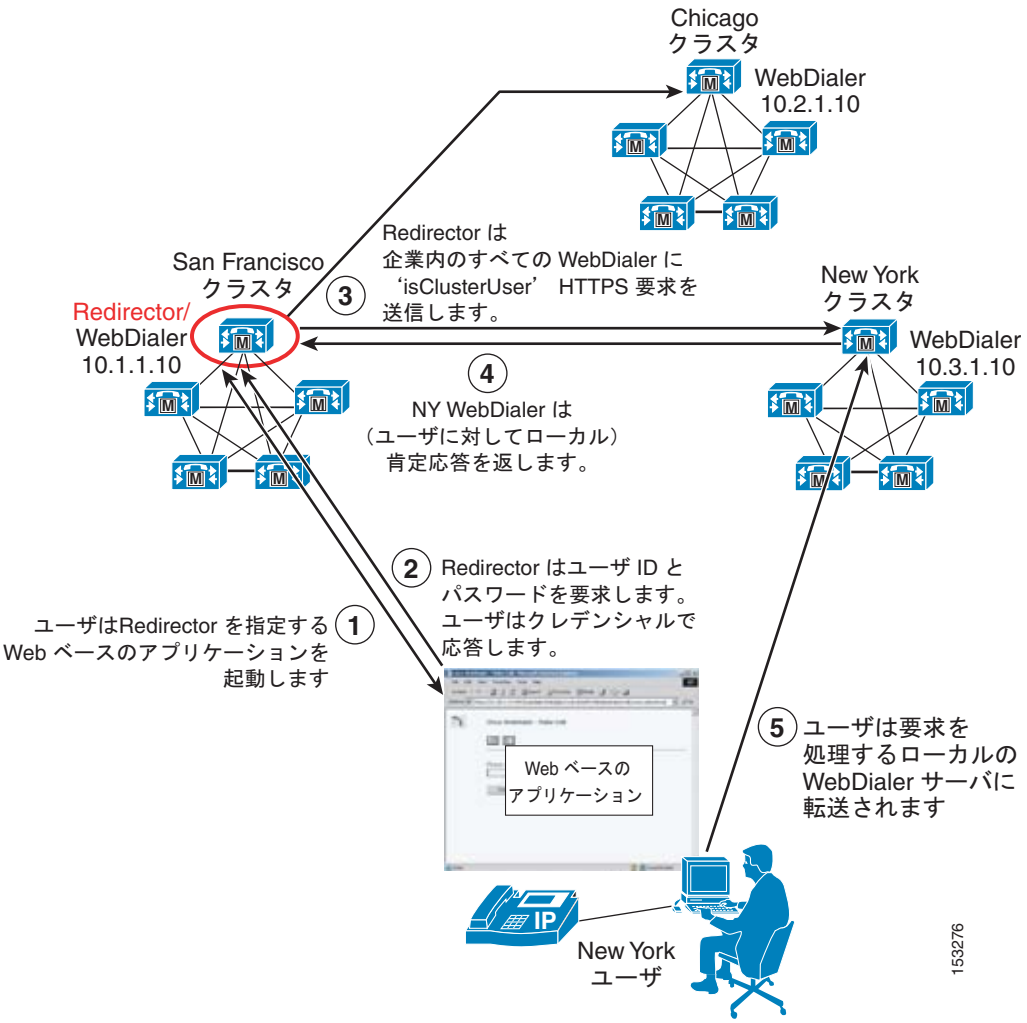
- New York の WebDialer：List of WebDialers: 10.1.1.10:8443 10.3.1.0:8443
- Chicago の WebDialer：List of WebDialers: 10.1.1.10:8443 10.2.1.0:8443
- San Francisco の WebDialer：List of WebDialers: 10.1.1.10:8443 10.2.1.0:8443 10.3.1.0:8443

企業全体の Web ベース アプリケーションは San Francisco の Redirector を指し、New York のユーザから起動されます（図 24-16 のステップ 1 を参照）。次に、Redirector はユーザのログインを要求し、New York ユーザは自分のユーザ ID とパスワードで応答します（図 24-16 のステップ 2 を参照）。

（注）　ユーザが以前に WebDialer アプリケーションにログインし、Web ブラウザおよびサーバの Cookie がまだアクティブになっている場合、次の要求時に再ログインは求められません。一方、ユーザ Web ブラウザ クッキーは期限を WebDialer サービス パラメータ で設定できます。これは、WebDialer サービス パラメータ で設定された通り所定の時間が経過した後、自動的に期限切れになります（「WebDialer サービス パラメータ」（P.24-53）を参照）。

次に、Redirector は、（List of WebDialers サービス パラメータの設定に従って）企業内のすべての WebDialer に isClusterUser HTTPS 要求を同時に送信します。この例で、要求は Chicago および New York の WebDialer サーバに送信されます（図 24-16 のステップ 3 を参照）。New York ユーザは New York クラスタに対してローカルであるため、New York の WebDialer は肯定応答を返します（図 24-16 のステップ 4 を参照）。最後に、New York ユーザはアプリケーション要求を処理するローカル WebDialer サーバに転送されます（図 24-16 のステップ 5 を参照）。この転送はユーザに通知されません。ただし、ブラウザのアドレス バーの URL は、ユーザが Redirector から WebDialer サーバに転送されたときに変更されます。

図 24-16　Redirector サーブレットの動作



（注）　Redirector アプリケーションは、Unified CM データベースでのユーザ認証の必要な企業全体のアプリケーションであるため、すべての Unified CM クラスタですべてのエンドユーザのユーザ ID を一意にすることを強くお勧めします。一意でない場合、Redirector アプリケーションが isClusterUser 要求に対する複数の肯定応答を受信する可能性があります。この場合、Redirector アプリケーションによって、ユーザは自分のローカル WebDialer サーバを手動で選択するように求められます。このため、ユーザは自分のローカル サーバを知っている必要があります。正しくないサーバを選択した場合、WebDialer 要求は失敗します。

WebDialer のアーキテクチャ

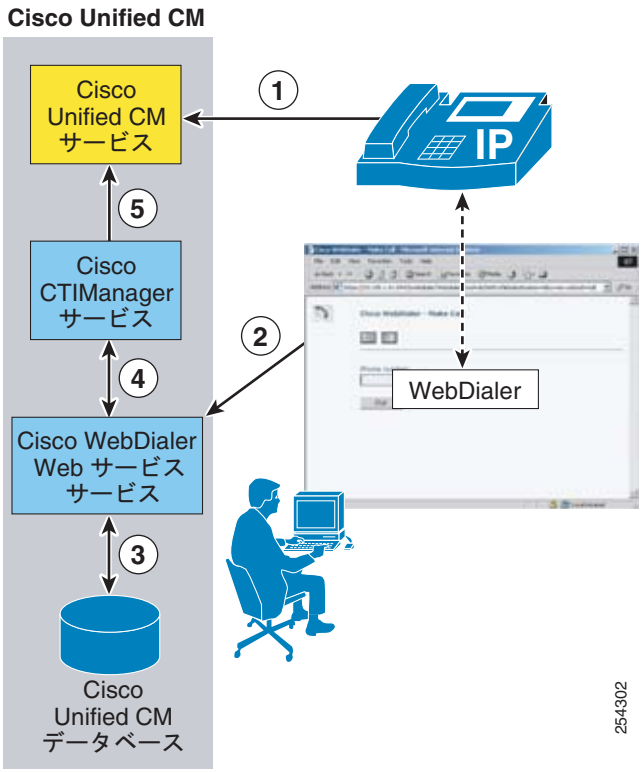
WebDialer アプリケーションのアーキテクチャは、その機能と同様に、そのアーキテクチャについても理解することが重要です。図 24-17 は、WebDialer のメッセージ フローとアーキテクチャを示しています。次の一連の対話とイベントが発生します。

1. WebDialer ユーザの電話機は、Cisco CallManager サービスを通じて登録し、コールの発信と受信を行います（図 24-17 のステップ 1 を参照）。
2. ユーザの PC 上の WebDialer アプリケーションは、次のいずれかのインターフェイスを通じて Cisco WebDialer Web Service と通信します（図 24-17 のステップ 2 を参照）。
   - HTML over HTTPS

     このインターフェイスは、HTTPS プロトコルに基づいて Web ベースのアプリケーションで使用されます。これは、Redirector サーブレットへのアクセスを提供する唯一のインターフェイスです。
   - Simple Object Access Protocol（SOAP）over HTTPS

     このインターフェイスは、SOAP インターフェイスに基づいてデスクトップ アプリケーションで使用されます。
3. WebDialer Web サービスは、Unified CM データベースからユーザおよび電話の情報を読み取ります（図 24-17 のステップ 3 を参照）。
4. 次に、WebDialer Web サービスは、回線と電話の制御情報を交換するために、CTIManager サービスと対話します（図 24-17 のステップ 4 を参照）。
5. CTIManager サービスは、WebDialer 電話制御情報を Cisco CallManager サービスに渡します（図 24-17 のステップ 5 を参照）。

図 24-17　WebDialer のアーキテクチャ



（注）　図 24-17 は、すべて同じノードで実行されている Cisco Unified CallManager、CTIManager、および WebDialer Web Service サービスを示していますが、この設定は必須ではありません。これらのサービスはクラスタ内の複数のノードに分散できますが、説明を簡単にするためにここでは同じノードにあるものとしています。

WebDialer の URL

Web ベースのアプリケーションから HTML-over-HTTPS インターフェイスを通じて WebDialer アプリケーションにアクセスするには、次の URL を使用します。

- WebDialer サーブレット

  https://<*Server-IP_Addr*>:8443/webdialer/Webdialer?destination=<*Number_to_dial*>

  （ここで、<*Server_IP-Address*> は、Cisco WebDialer Web Service サービスを実行しているクラスタ内のノードの IP アドレスで、<*Number_to_dial*> は WebDialer ユーザがダイヤルする番号です）

- Redirector サーブレット

  https://<*Server-IP_Addr*>:8443/webdialer/Redirector?destination=<*Number_to_dial*>

  （ここで、<*Server_IP-Address*> は、Cisco WebDialer Web Service サービスを実行している企業内のノードの IP アドレスで、<*Number_to_dial*> は WebDialer ユーザがダイヤルする番号です）

図 24-18 は、Cisco WebDialer アプリケーションをコールするクリックコール Web ベース アプリケーションで使用される、HTML ソース コードの例を示しています。この例で、HTML ソース ビューの URL https://10.1.1.1:8443/webdialer/Webdialer?destination=30271 は、Web ブラウザ ビュー内のユーザ Steve Smith 用の「Phone: 30721」リンクに対応しています。ユーザがこのリンクをクリックする

と、WebDialer アプリケーションが起動し、ログイン後に Dial をクリックすると、そのユーザの電話機から Steve Smith の電話機へのコールが生成されます。URL を https://10.1.1.1:8443/webdialer/Redirector?destination=30271 に変更すると、Redirector を使用するクリックコール アプリケーションで同じコードを使用できます。

図 24-18　WebDialer URL の HTML の例

HTML ソース ビュー:

```
<html>
<center><h3>WebDailer クリック ダイヤル HTML サンプル</h3></center>
<b>ユーザ名:</b> Adams, Sally<br>
<b>E メール:</b> <a href=“mailto:sadams@cisco.com”>a><br>
<b>電話:</b> <a href=“ https://10.1.1.1:8443/webdialer/Webdialer?destination=23923 “>23923</a><br>
<b>部門:</b> 人事部<br>
<br>
<b>ユーザ名:</b> Smith, Steve<br>
<b>E メール:</b> <a href=“mailto:ssmith@cisco.com”>ssmith</a><br>
<b>電話:</b> <a href=“ https://10.1.1.1:8443/webdialer/Webdialer?destination=30271 “>30271</a><br>
<b>部門:</b> 人事部
<hr>
</html>
```

Web ブラウザ ビュー:

WebDailer クリック ダイヤル HTML サンプル

ユーザ名: Adams, Sally
E メール: sadams
電話: 23923
部門: 人事部

ユーザ名: Smith, Steve
E メール: ssmith
電話: 30271
部門: 人事部

153278

デスクトップ アプリケーションのクリックコールで使用される SOAP-over-HTTPS ソース コードの情報および例については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Developers Guide*』の WebDialer API Programming 資料を参照してください。

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

WebDialer の冗長性

WebDialer アプリケーションの冗長性は、次の 2 つのレベルで実現できます。

- コンポーネント レベルとサービス レベルでの冗長性

  このレベルでの冗長性については、冗長性を、WebDialer サービスおよび CTIManager サービスの冗長性に関して検討する必要があります。同様に、パブリッシャの冗長性の欠如、およびこのコンポーネントの障害の影響も検討する必要があります。

- デバイス レベルと到達可能性レベルでの冗長性

  このレベルでの冗長性については、ユーザの電話機および WebDialer ユーザ インターフェイスに関連して検討する必要があります。

サービスとコンポーネントの冗長性

図 24-17 に示すように、WebDialer 機能は、主に Cisco WebDialer Web Service および Cisco CTIManager サービスに依存します。WebDialer サービスの場合は、List of WebDialers サービス パラメータ（「WebDialer サービス パラメータ」（P.24-53）を参照）に複数の WebDialer サーバの IP アドレスをリストし、クラスタ内の複数のノードでサービスを有効にすることで、冗長性を実現します。CTIManager の場合、冗長性は、プライマリおよびバックアップのメカニズムを使用して自動的に組み込まれます。Primary Cisco CTIManager および Backup Cisco CTIManager のサービス パラメータを使用すると、クラスタ内に 2 つの CTIManager サーバまたはサービスを定義できます（「WebDialer サービス パラメータ」（P.24-53）を参照）。これらのパラメータを設定すると、CTIManager サービスに冗長性を与えることができます。このため、プライマリ CTIManager に障害が発生した場合でも、CTIManager サービスはバックアップ CTIManager から提供できます。Web ベース（またはデスクトップ）アプリケーションが指している WebDialer サーバに障害が発生し、クラスタ ノード上のプライマリおよびバックアップ CTIManager サービスにも障害が発生した場合、WebDialer アプリケーションはダウンします。WebDialer サービスは Unified CM パブリッシャに依存しません。

デバイスと到達可能性の冗長性

デバイス レベルでの WebDialer の冗長性は、いくつかのメカニズムに依存しています。まず第 1 に、ユーザの電話機は、デバイス登録用のデバイス プールと Unified CM グループ設定の組み合せによって提供される組み込み冗長性に依存します。

複数の WebDialer サービスは冗長性を提供するために複数の Unified CM サブスクライバ を実行できます。しかしながら、多くのアプリケーションは複数の IP アドレスを処理するようには備わっていません。企業では、複数の WebDialer サーバのプレゼンスをマスクして Server Load Balancer（SLB; サーバ ロード バランサ）使用することをお勧めします。SLB 機能は、仮想 IP アドレスまたは DNS-resolvable hostname を 実現します。この DNS-resolvable hostname は、WebDialer および Redirector サーバの実 IP アドレスのフロントエンドになるものです。Cisco Application Control Engine（ACE）または Cisco IOS SLB 機能など多くの SLB デバイスは、複数の WebDialer サーバおよび障害イベント発生時に自動的な転送要求のステータスを監視する設定ができます。SLB 機能は、追加のクリックコール キャパシティを必要とする場合、ロード バランサ WebDialer 要求も設定できます。代替えとして、DNS Service（SRV）レコードも冗長性の提供に使用できます。

企業の配置では、リンク コストもまた重要な考慮事項です。Cisco ACE Global Site Selector（GSS）アプライアンスは、リンク コストおよびロケーションをロード バランシング アルゴリズム追加することで、その他の機能の 1 つとして、SLB 機能のキャパシティ を拡張します。ACE および GSS の詳細については、http://www.cisco.com を参照してください。

WebDialer のガイドラインと制限

次のガイドラインと制限は、Unified CM テレフォニー環境内の WebDialer の配置と動作に関連して適用されます。

- 管理者は、すべての WebDialer ユーザが Unified CM エンドユーザ ディレクトリの電話機またはデバイス プロファイルに関連付けられることを確認します。
  - 電話機が関連付けられていない状態でユーザが Cisco WebDialer Preferences 画面の「Use permanent device」を選択すると、Dial ボタンを押したときに次のメッセージが表示されます。

    「No supported device configured for user」
  - デバイス プロファイルが関連付けられていない状態で（またはプロファイルを使用してログインしないで）ユーザが Cisco WebDialer Preferences 画面の Use Extension Mobility を選択すると、Dial ボタンを押したときに次のメッセージが表示されます。

「Call to <*dialed_ number*> failed: User not logged in on any device」

（注）　WebDialer および EM アプリケーションは組み合せて使用できます。WebDialer と EM の相互作用の詳細については、「WebDialer と EM の相互作用」（P.24-62）を参照してください。

- List of WebDialers サービス パラメータ（「WebDialer サービス パラメータ」（P.24-53）を参照）を設定するときは、WebDialer IP アドレスと同時にポート番号 8443 を指定する必要があります。
- Client Matter Codes（CMC; クライアント識別コード）または Forced Authorization Codes（FAC; 強制承認コード）を使用している場合、WebDialer ユーザはトーンが聞こえたときに、電話機のキーパッドを使用して適切なコードを入力する必要があります。トーンが聞こえたときに適切なコードを入力しないと、コールの失敗を示すリオーダー トーンが聞こえます。

WebDialer のパフォーマンスとスケーラビリティ

WebDialer および Redirector サービスは Unified CM クラスタ内で複数のサブスクライバ ノードを実行でき、次のキャパシティ がサポートされています。

- 各 WebDialer サービスは、ノードごとに 1 秒あたり最大 2 コール要求（1 時間あたり 7,200 コール）まで処理できます。
- 各 Redirector サービスは、1 秒あたり最大 8 コール要求まで処理できます。

次の一般式が WebDialer の 1 秒あたり のコール数の決定に使用できます。

（WebDialer のユーザ数）×（(Average BHCA）/（3600 秒/時間））

この計算を行う場合、特に WebDialer サービス使用し、開始しているユーザあたり BHCA の数を適切に推定することが重要です。次に、見本の組織でこれら WebDialer デザインの計算を使用する例を示します。

例 24-1　WebDialer のコール数 1 秒あたりの計算

会社 XYZ は、WebDialer サービスを使用してクリックコール アプリケーションを稼動させることを考えています。その事前のトラフィック分析結果は次の資料の通りです。

- 10,000 人をクリックコール機能で有効にする。
- 各ユーザの平均 6 BHCA
- すべてのコールの 50% が発信で、50% が着信
- 計画では、すべての発信のうち、WebDialer サーバを使用して開始する発信を 30% と見積もる。

（注）　これらの値は、WebDialer 配置のサイジングの演習を示すために使用した例です。ユーザのダイヤル特性は、組織から組織へ 広範にわたって変化します。

10,000 のユーザで各 6 BHCA では、合計 60,000 BHCA に相当します。ただし、WebDialer 配置のサイジングの計算は、発信コールのみの割合を占めます。このサイジングの例で最初の情報では、合計 BHCA の 50%が発信です。これは、WebDialer を使用する有効なクリックコールが、すべてのユーザのうち、合計で 30,000 placed BHCA という結果になります。

この発信数のうち、WebDialer サービスを使用して開始されるところの百分率（%）は、組織から組織で変化します。この例の組織では、ユーザが利用するいくつかのクリックコール アプリケーションは、WebDialer を使用して開始する発信の 30% と計画されています。

WebDialer を使用の場合（30,000 placed BHCA）* 0.30 = 9,000 placed BHCA

9,000 BHCA の負荷をサポートするのに必要な WebDialer サーバの数を判別するには、この値を煩雑する時間に維持する必要のある平均の Busy Hour Call Attempt（BHCA）1 秒あたりに変換します。

（9,000 call attempts / 時間）*（時間 /3600 秒）= 2.5 cps

各 WebDialer サービスは最大で 2 cps をサポートできます。したがって、この例では、WebDialer サービスを実行するため 2 つのノードを設定する必要があります。これは、将来の WebDialer 拡張使用に利用できます。障害が発生時に WebDialer キャパシティを維持するため、冗長性を提供する追加のバックアップ WebDialer サーバを設置する必要があります。

Cisco WebDialer アプリケーションは、電話制御のために CTIManager と対話することに留意してください。有効にすると、各 WebDialer サービスは単一持続性 CTI 接続を CTIManager に開きます。また、各 WebDialer の個々の MakeCall（または EndCall）要求は一時的な CTI 接続を生成します。WebDialer コール レートの処理に必要な CTI 接続の数も、クラスタごとの CTI 接続制限に対して適用されます（クラスタごとの CTI 接続制限の詳細については、「Unified CM のキャパシティ プランニング」（P.8-22）を参照してください）。

WebDialer と EM の相互作用

WebDialer ユーザは、EM を使用してそれぞれの電話機にログインできます。EM ユーザは、Cisco WebDialer Preferences ページで Use Extension Mobility 設定を選択するだけで、WebDialer を使用できます。

CHAPTER 25

シスコ モビリティ アプリケーション

シスコ モビリティ アプリケーションを使用すれば、モバイル ワーカーはどこからでも会社の IP コミュニケーション環境の機能を利用することができます。モビリティ ユーザは、デスクトップフォンだけでなく、1 つまたは複数のリモート電話機で会社の電話番号にかかってきた電話に出ることができます。また、モビリティ ユーザは、まるで社内から電話をかけているかのようにリモート電話機から電話をかけることもできます。さらに、モビリティ ユーザは、保留、転送、会議などのエンタープライズ機能だけでなく、携帯電話上でのボイルメール、会議、プレゼンスなどのエンタープライズ アプリケーションも利用できます。これによって、ユーザは外出先でも生産性を持続させることができます。

Cisco Unified Communications ソリューションに付属のモビリティ機能は、Cisco Unified Communications Manager（Unified CM）を通して提供され、Cisco Unified Mobile Communicator アプリケーションと組み合せて使用できます。

Cisco Unified Mobility では、次のモビリティ アプリケーション機能が提供されます。

- モバイル コネクト

  シングル ナンバー リーチとも呼ばれるモバイル コネクトを使用すれば、1 つの会社の電話番号で Cisco Unified Communications ユーザの IP 卓上電話と携帯電話の両方を同時に呼び出すことができます。モバイル コネクト ユーザは、着信コールをデスクトップフォンでも携帯電話でも受けることができ、通話中のコールを妨げることなく別の電話に転送することができます。

- 通話切替機能

  通話切替機能により、モビリティ コールの通話中に、携帯電話の保留、保留解除、転送、会議、およびリダイレクト コール パーク機能を呼び出すことができます。これらの機能は、携帯電話のキーによって呼び出され、保留音やカンファレンス ブリッジといった企業のメディア リソースを活用します。

- シングル企業ボイスメール ボックス

  シングル企業ボイスメール ボックスは、ユーザの会社の電話番号に着信し、さらに携帯電話に転送されたコールに応答がなかった場合に、携帯電話のボイスメール システムではなく、会社のボイスメール システムにコールを蓄積します。これにより、ボイスメール ボックスが 1 箇所に統合され、ユーザは複数のボイスメール システムでメッセージを確認する必要がなくなります。

- 2 ステージ ダイヤリング機能付きモバイル ボイス アクセスとエンタープライズ機能アクセス

  2 ステージ ダイヤリング機能付きモバイル ボイス アクセスとエンタープライズ機能アクセスによって、まるで会社の IP 卓上電話からかけているかのように、携帯電話から発信することができます。長距離電話や国際電話、または通常は企業外部から到達不能なシステム上の内部の DID 以外の内線番号へのコールにおいてこれらの機能を使用すると、通話料金を節約できます。また、企業でこれらの 2 ステージ ダイヤリング機能を使用すると、中央で一括管理されたコール詳細レコードによって、ユーザのコール発信を容易に追跡管理できるようになります。さらに、これらの機能によって、発信者 ID を送信する際にユーザの携帯電話番号を隠すことができます。代わりに、発信者 ID として、ユーザの会社の電話番号が送信されます。これによって、ユーザへの返信コールは会社の電話番号にかけられるため、コールを会社で一括管理できます。

Cisco Unified Mobile Communicator アプリケーションには、バックホール データ チャネルの使用を通してユーザの携帯電話にエンタープライズ ユニファイド コミュニケーション機能を提供するスマートフォン モバイル クライアントが含まれます。このデータ公衆網が音声サービスに利用されます。チャネルは、インターネット上のサービス プロバイダー データ サービスによって送信され、Cisco Adaptive Security Appliance（ASA）で終端処理されてから、企業の Unified Communications インフラストラクチャ内のさまざまなアプリケーションやコンポーネントとインターフェイスする Unified Mobility Advantage サーバに転送されます。音声サービスでは、公衆網およびモバイル ボイス ネットワークが利用されます。

Cisco Unified Mobile Communicator アプリケーションと統合可能なエンタープライズ アプリケーションおよび機能を次に示します。

- ユーザ認証およびディレクトリ ルックアップ用の Microsoft Active Directory を使用した LDAP ディレクトリ
- ユーザの企業ボイスメール ボックスのメッセージ待機インジケータおよび視覚ナビゲーション用の Cisco Unity または Unity Connection を使用したボイスメール
- 会議通知の受信用の Cisco Unified MeetingPlace を使用した会議とコラボレーション
- Cisco Unified Personal Communicator などの他のクライアントやアプリケーションとのプレゼンス情報の交換やバディ リストの同期化を可能にする、Cisco Unified Presence とのプレゼンス統合
- ユーザの卓上電話からのコール履歴ログの受信およびエンタープライズ IP テレフォニー インフラストラクチャ経由のダイヤリング用の Cisco Unified Communications Manager（Unified CM）を使用したエンタープライズ コール ログと Dial-via-office
- その他の Cisco Unified Mobile Communicator クライアントを使用したテキスト メッセージの送受信用のメッセージング

さまざまなエンタープライズ ユニファイド コミュニケーション アプリケーションとの統合機能の提供に加えて、Cisco Unified Mobile Communicator モバイル クライアントと Unified Mobility を統合してモバイル コネクトやシングル企業ボイスメール ボックスなどのさまざまな機能を利用できます。

特に断りがない限り、この章で説明するさまざまなアプリケーションと機能は、すべての Cisco Unified Communications 配置モデルに適用されます。

この章では、まず、Unified Mobility の特徴、機能、および設計と配置に関する考慮事項について説明します。その後で、Unified Mobility のさまざまなメリットと Cisco Unified Mobile Communicator を統合することによってその機能が利用できるという事実を前提として、Cisco Unified Mobile Communicator を検証します。この検証には、次のモビリティ アプリケーションおよび機能のアーキテクチャ、機能性、および設計と配置の意味に関する説明が含まれます。

- 「Cisco Unified Mobility」（P.25-4）
- 「モバイル コネクト」（P.25-5）
- 「モバイル ボイス アクセスとエンタープライズ機能アクセス」（P.25-16）
- 「Cisco Unified Mobile Communicator」（P.25-34）

この章の新規情報

表 25-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 25-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
モバイル コネクト コールの許可または拒否用のアクセス リスト	「モバイル コネクト コールの許可または拒否用のアクセス リスト」（P.25-14）
Nokia Symbian および Apple iPhone のハンドセットに対する Cisco Unified Mobile Communicator 7.*x* クライアントのサポート	「Cisco Unified Mobile Communicator の電話サポートとデータ プラン要件」（P.25-34）
Cisco Unified Presence のフェデレーションと Dial-via-office を含む Cisco Unified Mobile Communicator の特徴と機能	「Cisco Unified Mobile Communicator の機能」（P.25-38）
Cisco Unified Mobile Communicator の冗長性に関する考慮事項	「Cisco Unified Mobile Communicator の冗長性」（P.25-46）
Cisco Unified Mobility Advantage のスケーラビリティ	「Cisco Unified Mobile Communicator の性能と容量」（P.25-46）
セキュリティ、認証、およびファイアウォールの要件など、Cisco Unified Mobile Communicator を配置する場合の設計上の推奨事項	「Cisco Unified Mobile Communicator の配置に関する設計上の推奨事項」（P.25-47）
Unified Mobility に対する公衆網利用の最小化に関する説明を含む、Unified Mobility を配置する場合の設計上の推奨事項	「Unified Mobility を配置するための設計上の推奨事項」（P.25-32）
ダイレクト コール パーク通話切替機能	「通話切替機能」（P.25-10）
Cisco Mobile iPhone デュアルモード クライアントおよび Nokia Call Connect デュアルモード クライアントのサポートを含む、デュアルモード電話機のソリューション	「デュアルモードの電話機とクライアント」（P.25-48）
モバイル コネクトの有効化と無効化	「モバイル コネクトの有効化と無効化」（P.25-14）
Unified Mobility の保守とトラブルシューティング	「Unified Mobility の保守とトラブルシューティング」（P.25-28）
SIP VoiceXML ゲートウェイに対するモバイル ボイス アクセスのサポート	「モバイル ボイス アクセスとエンタープライズ機能アクセス」（P.25-16）
iPhone に関する新しい Dial-via-office 転送機能	「Cisco Unified Mobile Communicator の機能」（P.25-38）
会議通知からのクリックツージョインに関する iPhone の新機能	「Cisco Unified Mobile Communicator の機能」（P.25-38）
Cisco Unified Mobile Communicator 7.1 以降のリリースに対する Microsoft Exchange 要件の削除	「Cisco Unified Mobile Communicator の機能」（P.25-38）
Unified Mobility Advantage プロキシ サーバと ASA TLS プロキシの交換	「Cisco Unified Mobile Communicator のアーキテクチャ」（P.25-37）
Cisco MCS-7825 Media Convergence Server での Cisco Unified Mobility Advantage のサポート	「Cisco Unified Mobile Communicator の性能と容量」（P.25-46）

表 25-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報 （続き）

新規トピックまたは改訂されたトピック	説明箇所
モバイル コネクト コールにおける Redirected Dialed Number Identification Service（RDNIS）または SIP の Diversion ヘッダーのサポート	「Unified Mobility を配置するための設計上の推奨事項」（P.25-32）
Unified CM 7.1(2) 以降のリリースでのサービス プロバイダー VoIP ベース SIP トランクのサポート	「Unified Mobility に関するガイドラインと制約事項」（P.25-30）

Cisco Unified Mobility

Cisco Unified Mobility は、Cisco Unified Communications Manager（Unified CM）に組み込まれたネイティブなモビリティ機能を意味し、モバイル コネクト、モバイル ボイス アクセス、およびエンタープライズ機能アクセスの各機能が含まれます。

Unified Mobility の機能は、Unified CM の設定によって異なります。したがって、この設定だけでなく、論理コンポーネントの特性も理解することが重要です。

図 25-1 に、Unified Mobility に関する設定要件を示します。まず、ユーザに関しては、モビリティ ユーザの会社の電話機は、電話番号、パーティション、コーリング サーチ スペースなどの該当する回線レベル設定値を使用して設定されます。この他に、会社の電話機のデバイス レベルの設定には、デバイス プール、共通デバイス設定、コーリング サーチ スペース、メディア リソース グループ リスト、ユーザとネットワークの保留音源などのパラメータが含まれます。ユーザの会社の電話機に関するこれらの回線およびデバイス設定のすべてが、着信コールと発信コールのコール ルーティングや保留音（MoH）の動作に影響を与えます。

次に、Unified Mobility 機能が利用できるように、モビリティ ユーザごとのリモート接続先プロファイルを設定する必要があります。リモート接続先プロファイルは、ユーザの会社の電話回線と同じ電話番号、パーティション、およびコーリング サーチ スペースを使用して回線レベルで設定します。これによって、リモート接続先プロファイルと会社の電話機の間で回線が共有されます。リモート接続先プロファイル設定には、デバイス プール、コーリング サーチ スペース、コーリング サーチ スペースの再ルーティング、およびユーザとネットワークの保留音源に関するパラメータが含まれます。リモート接続先プロファイルは、その設定にユーザの回線レベルの会社の電話機の設定が反映されますが、回線レベルの設定とプロファイル レベルの設定を組み合せることによって、ユーザのリモート接続先電話機に継承されるコール ルーティングおよび MoH 動作が決定される仮想電話機と見なす必要があります。リモート接続先プロファイルと会社の電話機の間で共有されるユーザの会社の電話番号を使用すれば、その番号に電話することによってユーザのリモート接続先に転送することができます。

図 25-1　Cisco Unified Mobility の設定アーキテクチャ

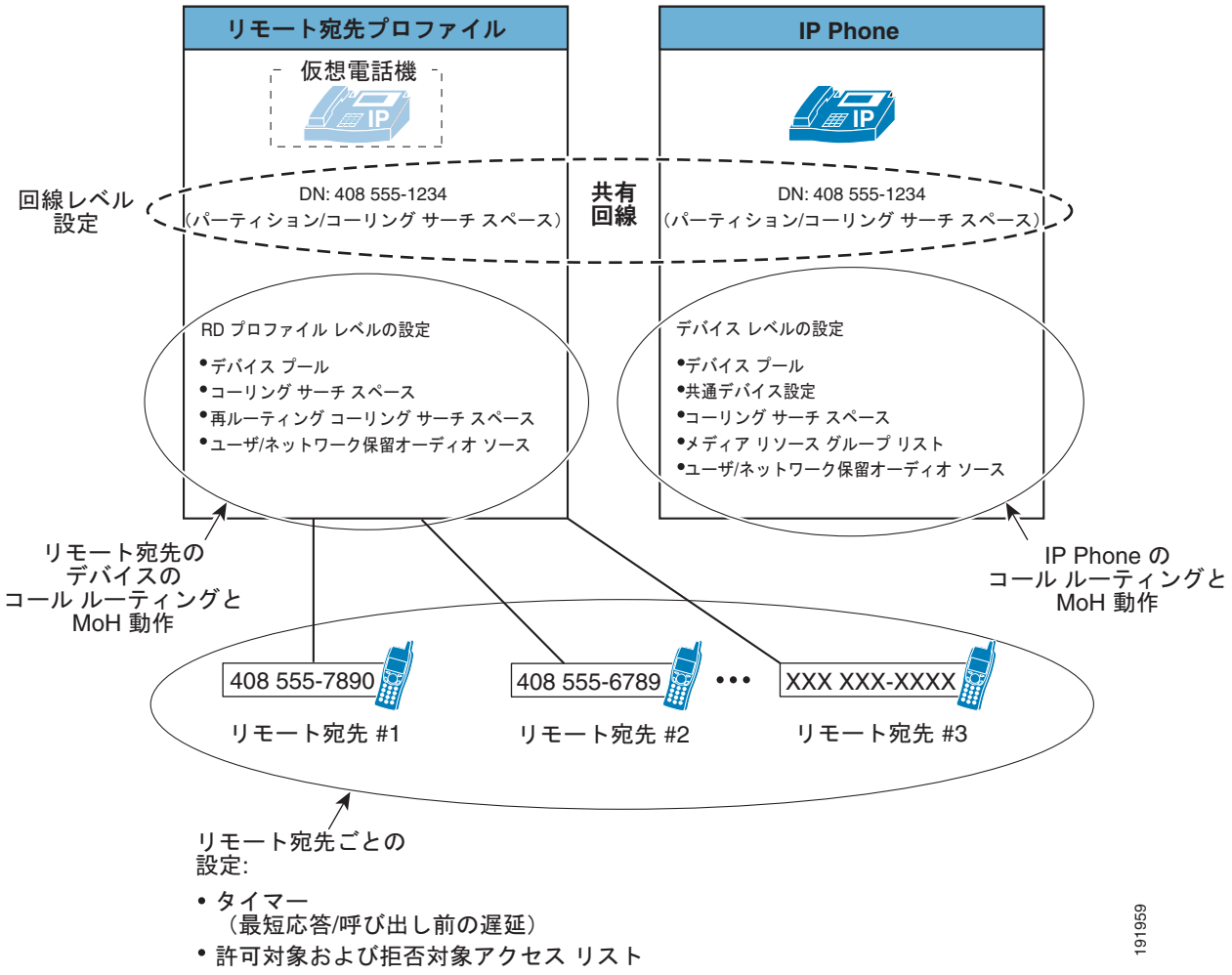


図 25-1 に示すように、モビリティ ユーザは、1 つまたは複数のリモート接続先をリモート接続先プロファイルに関連付けることができます。リモート接続先は、ユーザを呼び出すための単一の公衆網電話番号を表しています。ユーザは、最大で 10 個のリモート接続先を定義できます。リモート接続先ごとにコール ルーティング タイマーを設定して、コールを特定のリモート電話に転送する時間だけでなく、コールを転送する前に待機する時間とリモート電話でコールを受ける準備ができるまでの時間を調整できます。また、モビリティ ユーザは、リモート接続先ごとに、リモート電話に転送する特定の電話番号からのコールを許可または拒否するフィルタを設定できます。

モバイル コネクト

モバイル コネクト機能を使用すれば、企業ユーザへの着信コールをそのユーザのデスクトップフォンだけでなく、最大 10 個の設定可能なリモート接続先に転送できます。一般的に、ユーザのリモート接続先は携帯電話です。コールがデスクトップフォンとリモート接続先電話機の両方に転送されれば、ユーザはどちらかの電話機で応答できます。ユーザは、リモート接続先電話機のいずれかまたは IP デスクトップフォンでコールに応答したときに、そのコールを別の電話機でハンドオフするか、ピックアップするかを選択できます。

モバイル コネクトの電話機サポート

モバイル コネクトは、次の電話機モデルでサポートされます。

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7941G、7941G-GE、7942G、および 7945G
- Cisco Unified IP Phone 7961G、7961G-GE、7962G、および 7965G
- Cisco Unified IP Phone 7970G、7971G-GE、および 7975G
- Cisco IP Communicator

これらすべての電話機で、Skinny Client Control Protocol（SCCP）と Session Initiation Protocol（SIP; セッション開始プロトコル）を使用した Mobility ソフトキーによるモバイル コネクト リモート接続先ピックアップがサポートされます。

次の電話機では、SCCP のみを使用したモバイル コネクトがサポートされます。

- Cisco Unified IP Phone 7905G
- Cisco Unified Wireless IP Phone 7920、7921G、および 7925G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7940G
- Cisco Unified IP Phone 7960G

IP デスクトップフォンでピックアップした場合はリモート接続先電話機を切るだけでいいため、リモート電話で受けたモバイル コネクト コールは、リモート接続先電話機の種類に関係なく、前述したどの IP 電話機モデルにも転送できます。このようなシナリオのピックアップ機能は、Unified CM と、リモート接続先への発信コールを処理した会社の公衆網ゲートウェイで処理されます。

（注） SIP を実行している Cisco Unified IP Phone 7905G、7912G、7912G-A、7940G、および 7960G と SCCP を実行している Cisco Unified IP Phone 7912G および 7912G-A をモバイル コネクトと一緒に使用すれば、着信時にデスクトップフォンとリモート接続先電話機の両方を呼び出すことができます。ただし、コールに応答すると、デスクトップフォンのピックアップとリモート接続先電話機のピックアップのどちらかが使用できなくなります。

モバイル コネクトに関する Unified CM サービス パラメータ

次のリストは、モバイル コネクト機能に関連した Cisco CallManager サービスの Unified CM サービス パラメータの一部を示しています。

- Enterprise Feature Access Code for Hold（デフォルト値：*81）

  このパラメータは、保留通話切替機能に使用される機能アクセス コードを指定します。このコードは、ユーザが手動で入力します。また、このコードは、DTMF シーケンスとしてリモート接続先電話機から会社のゲートウェイに送信され、Unified CM に中継されます。

- Enterprise Feature Access Code for Exclusive Hold（デフォルト値：*82）

  このパラメータは、独占保留通話切替機能に使用される機能アクセス コードを指定します。リモート接続先電話機で独占保留が呼び出された場合は、ユーザのデスクトップフォンでそのコールをピックアップまたは保留解除できません。このコードは、ユーザが手動で入力します。また、このコードは、DTMF シーケンスとしてリモート接続先電話機から会社のゲートウェイに送信され、Unified CM に中継されます。

- Enterprise Feature Access Code for Resume（デフォルト値：*83）

  このパラメータは、保留解除通話切替機能に使用される機能アクセス コードを指定します。このコードは、ユーザが手動で入力します。また、このコードは、DTMF シーケンスとしてリモート接続先電話機から会社のゲートウェイに送信され、Unified CM に中継されます。

- Enterprise Feature Access Code for Transfer（デフォルト値：*84）

  このパラメータは、転送通話切替機能に使用される機能アクセス コードを指定します。このコードは、ユーザが手動で入力します。また、このコードは、DTMF シーケンスとしてリモート接続先電話機から会社のゲートウェイに送信され、Unified CM に中継されます。

- Enterprise Feature Access Code for Conference（デフォルト値：*85）

  このパラメータは、会議通話切替機能に使用される機能アクセス コードを指定します。このコードは、ユーザが手動で入力します。また、このコードは、DTMF シーケンスとしてリモート接続先電話機から会社のゲートウェイに送信され、Unified CM に中継されます。

- Inbound Calling Search Space for Remote Destination（デフォルト値 : Trunk or Gateway Inbound Calling Search Space）

  このパラメータによって、設定されたリモート接続先電話機から会社へのコールに関する着信コール ルーティングの特性が決定されます。デフォルトで、コール先の公衆網ゲートウェイまたはトランクのインバウンド コーリング サーチ スペース（CSS）が着信コールの経路設定に使用されます。このパラメータの値が Remote Destination Profile + Line Calling Search Space に設定された場合は、リモート接続先プロファイル CSS（と回線 CSS の組み合せ）が着信コールの経路設定に使用されます。このパラメータは、リモート接続先電話機以外からの着信コール ルーティングには影響しません。

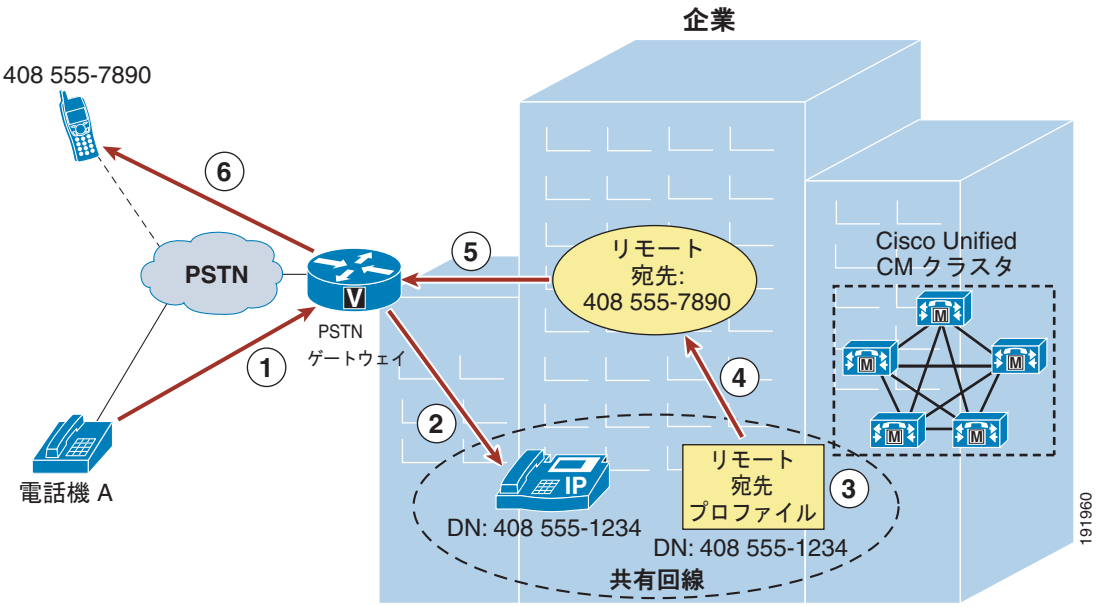
- Enable Enterprise Feature Access（デフォルト値：False）

  このパラメータによって、システムのエンタープライズ機能アクセスを有効にするかどうかが決定されます。リモート接続先電話機からの保留、保留解除、転送などの通話切替機能を呼び出す場合と 2 ステージ ダイヤリング機能を使用する場合は、このパラメータを True に設定する必要があります。

モバイル コネクトの機能

図 25-2 に、基本的なモバイル コネクトのコール フローを示します。この例では、公衆網上の 電話機 A からモバイル コネクト ユーザの会社の電話番号（DN）408-555-1234 に電話をかけます（ステップ 1）。コールが会社の公衆網ゲートウェイから Unified CM を経由して DN 408-555-1234 の IP 電話機に転送され（ステップ 2）、この電話が鳴り出します。コールは、同じ DN を共有するユーザのリモート接続先プロファイルにも転送されます（ステップ 3）。次に、コールがユーザのリモート接続先プロファイルに関連付けられたリモート接続先（この場合は 408-555-7890）に発信されます（ステップ 4）。リモート接続先への発信コールが公衆網ゲートウェイを介してルーティングされます（ステップ 5）。最後に、番号が 408 555-7890 のリモート接続先公衆網電話機で呼出音が鳴ります（ステップ 6）。どちらの電話機でも応答することができます。

図 25-2　モバイル コネクト



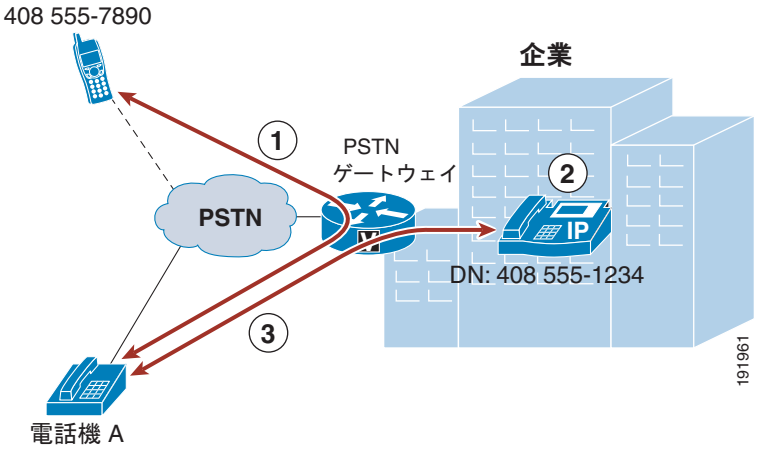
通常、モバイル コネクト ユーザの設定済みリモート接続先は、Global System for Mobile Communications（GSM）またはセルラー ネットワーク上の携帯電話です。ただし、公衆網による到達可能な任意の接続先をユーザのリモート接続先として設定できます。さらに、モバイル コネクト ユーザは 10 件までリモート接続先を設定できるため、着信コールは最大で 10 台の公衆網電話機とユーザのデスクトップフォンを呼び出すことができます。デスクトップフォンまたはリモート接続先電話機のいずれかでコールに応答すると、他のリモート接続先またはデスクトップフォン（デスクトップフォンで応答しなかった場合）に転送されたすべてのコール レッグがクリアされます。リモート接続先で着信コールに応答した場合は、2 つのゲートウェイ ポートを使用している会社の公衆網ゲートウェイ内で音声メディア パスがヘアピンされます。モバイル コネクト機能を配置する場合はこの利用を考慮する必要があります。

（注）　図 25-2 に示すようにモバイル コネクトを動作させるには、End User 設定ページでユーザ レベルの Enable Mobility チェックボックスがオンになっており、少なくとも 1 つのユーザの設定済みリモート接続先で Enable Mobile Connect チェックボックスがオンになっていることを確認します。

デスクトップフォンのピックアップ

図 25-3 に示すように、ユーザがリモート接続先デバイスでモバイル コネクトに応答した場合（ステップ 1：この場合は 408 555-7890）は、ユーザはデスクトップフォンの Resume ソフトキーを押すだけで、いつでもリモート接続先でコールを一旦切ってから、デスクトップフォンでピックアップできます（ステップ 2：この場合は DN 408 555-1234）。電話機 A を使用している元の発信者とデスクトップフォンとの間でコールが再開されます（ステップ 3）。

図 25-3　デスクトップフォンのピックアップ



デスクトップフォンのピックアップは、設定済みのリモート接続先電話機で会社の固定コールの通話が行われたあと、その電話が切られた場合にいつでも実行できます。

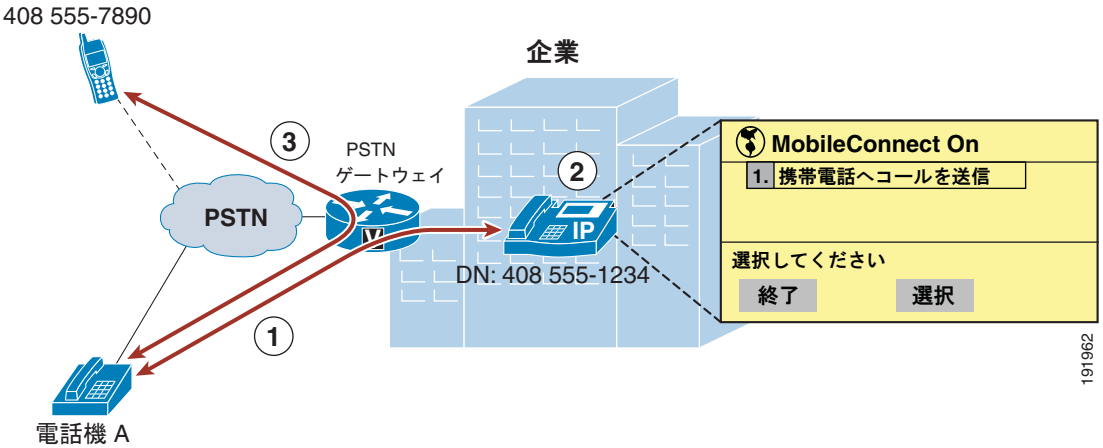
（注）　会社の固定コールは、1 つ以上のコール レッグが会社の公衆網ゲートウェイ経由で接続され、会社の DID コールへのリモート接続先として、または、モバイル コネクト、モバイル ボイス アクセス、またはエンタープライズ機能アクセス コールとして開始されたすべてのコールを指します。

デスクトップフォンでコールをピックアップまたは保留解除するためのオプションは、一定時間しか使用できません。そのため、モバイル コネクト ユーザは、必ず、着信電話機が切れていることを確認してから、リモート接続先電話機を切るようにしてください。これによって、他の誰かがデスクトップフォンでコールを保留解除できないことが保証されます。デフォルトで、リモート接続先電話機が切られてから 10 秒間はコールをデスクトップフォンでピックアップできます。ただし、この時間は設定可能であり、[End User] 設定ページで Maximum Wait Time for Desk Pickup パラメータを変更することによって、ユーザごとに 0 ～ 30,000 ミリ秒に設定できます。リモート接続先電話機で通話切替機能を呼び出した後は、デスクトップフォンのピックアップも実行できます。ただし、このような場合は、Maximum Wait Time for Desk Pickup パラメータの設定が、ピックアップに使用できる時間に影響しません。通話切替保留されたコールは、リモート電話機とデスクトップフォンのどちらかで手動で保留解除されるまで、保留のままで、デスクトップフォンでピックアップできます。

リモート接続先電話のピックアップ

図 25-4 に、モバイル コネクトのリモート接続先電話機のピックアップ機能を示します。電話機 A からモバイル コネクト ユーザの会社の DN 408 555-1234 が呼び出され、そのコールがユーザのデスクトップフォンで応答されて通話中である場合（ステップ 1）は、ユーザが Mobility ソフトキーを押す必要があります。この電話機でモバイル コネクト機能が有効になっており、リモート接続先ピックアップが使用できる場合、ユーザは Select ソフトキーを押します（ステップ 2）。ユーザのリモート接続先電話機に対するコール（この場合は 408 555-7890）が実行され、リモート電話機が鳴り出します。リモート電話機でコールが応答されると、電話機 A と、番号が 408 555-7890 のモバイル コネクト ユーザのリモート電話機との間でコールが再開されます（ステップ 3）。

図 25-4　リモート接続先電話のピックアップ



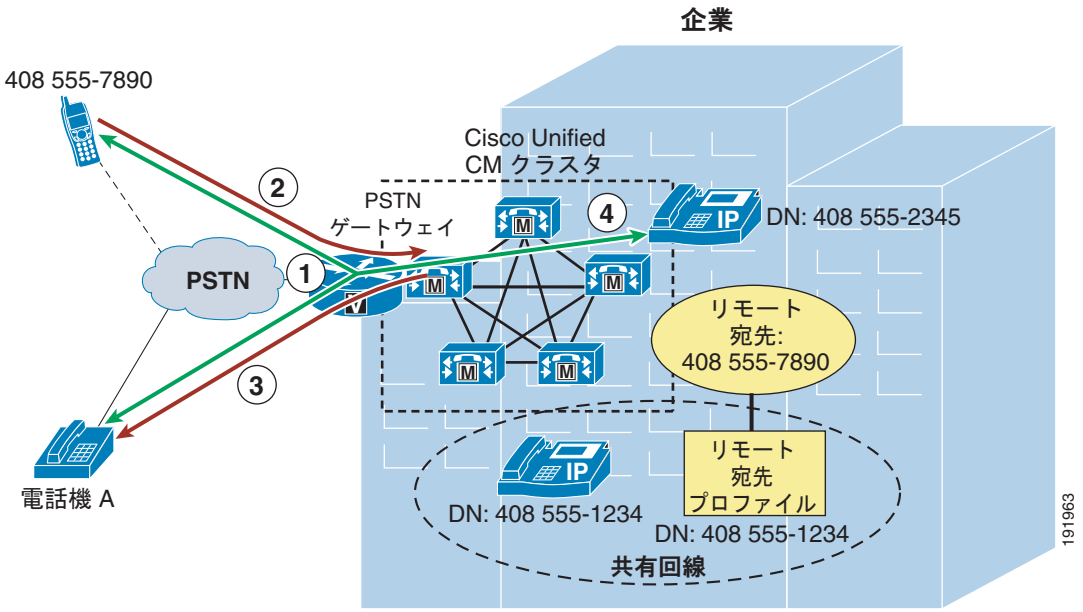
モバイル コネクト ユーザに対して複数のリモート接続先が設定されている場合は、Select ソフトキーを押したときに各リモート接続先が呼び出され、ユーザは好きな電話機をピックアップできます。

（注）　図 25-4 に示すように、リモート接続先電話機のピックアップを動作させるには、1 つ以上のユーザの設定済みリモート接続先で Mobile Phone チェックボックスがオンになっていることを確認してください。加えて、Mobility ソフトキーをすべてのモビリティ ユーザの関連するデスクトップフォン ソフトキー テンプレートに追加する必要があります。Mobile Phone チェックボックスをオンにして、Mobility ユーザがモビリティ ソフトキーを使用できるようにしなければ、リモート接続先電話機のピックアップ機能が使用できません。

通話切替機能

図 25-5 に示すように、ユーザがリモート接続先電話機でモバイル コネクト コールに応答（ステップ 1：この場合は 408 555-7890）したら、会社の公衆網ゲートウェイ経由でリモート接続先電話機から Unified CM に DTMF 番号が送信されることによって、保留、保留解除、転送、会議、ダイレクト コール パークなどの通話切替機能を呼び出すことができます（ステップ 2）。通話切替機能の保留、転送、会議、またはダイレクト コール パークが呼び出されると、Unified CM から電話の相手に MoH が送信されます（ステップ 3：この場合は Phone A）。通話中のコールを別の電話機やダイレクト コール パーク番号に転送したり、会社の会議リソースを使用して新しい電話機で会議に参加できます（ステップ 4）。

図 25-5　モビリティ通話切替機能



Unified CM に転送された一連の DTMF 番号によって、リモート接続先電話機で通話切替機能が呼び出されます。Unified CM で受信されるこれらの番号シーケンスが、設定済みの保留、独占保留、保留解除、転送、および会議用のエンタープライズ機能アクセス コード（「モバイル コネクトに関する Unified CM サービス パラメータ」（P.25-6）を参照）と照合され、該当する機能が実行されます。

（注）　ダイレクト コール パークの通話切替機能を有効にするには、ダイレクト コール パーク番号とコール パーク取得プレフィックスを使用して Cisco Unified CM を設定する必要があります。

（注）　転送、会議、およびダイレクト コール パークの通話切替機能を実行するために、コールに応答して、ユーザ入力（PIN 番号、通話切替機能アクセス コード、およびターゲット番号を含む）を取得し、必要なコール レッグを作成して転送、会議、またはダイレクト コール パークの処理を完了させる、システム設定のエンタープライズ機能アクセス DID への 2 つ目のコール レッグがリモート接続先電話機で生成されます。

通話切替機能は、手動で機能アクセス コードを入力し、適切なキー シーケンスを入力することによってアクセスします。表 25-2 に、通話切替機能にアクセスするためのキー シーケンスを示します。

表 25-2　手動通話切替機能のキー シーケンス

通話切替機能	エンタープライズ機能アクセス コード（デフォルト）	手動キー シーケンス
保留	*81	入力：*81
独占保留	*82	入力：*82
保留解除	*83	入力：*83
転送	*84	1. 入力：*82（独占保留） 2. エンタープライズ機能アクセス DID への新しいコールの発信 3. 接続時の入力：<*PIN_number*> # *84 # <*Transfer_Target/DN*> # 4. 転送ターゲットでの応答時（打診転送の場合）またはリングバック時（初期在席転送の場合）の入力：*84
ダイレクト コール パーク	該当なし	1. 入力：*82（独占保留） 2. エンタープライズ機能アクセス DID への新しいコールの発信 3. 接続時の入力：<*PIN_number*> # *84 # <*Directed_Call_Park_Number*> # *84 # **（注）** パークされたコールを取得するには、モバイル ボイス アクセスまたはエンタープライズ機能アクセス 2 ステージ ダイヤリングを使用してコールをダイレクト コール パーク番号に発信する必要があります。ダイヤルするダイレクト コール パーク番号が入力する際、適切なコール パーク取得プレフィックスを付加する必要があります。
会議	*85	1. 入力：*82（独占保留） 2. エンタープライズ機能アクセス DID への新しいコールの発信 3. 接続時の入力：<*PIN_number*> # *85 # <*Conference_Target/DN*> # 4. 会議ターゲットによる応答時の入力：*85

（注） 保留や会議などの通話切替機能のためのメディア リソース割り当ては、リモート接続先プロファイル設定で決定されます。リモート接続先プロファイル用に設定されたデバイス プールのメディア リソース グループ リスト（MRGL）が、会議通話切替機能のためのカンファレンス ブリッジの割り当てに使用されます。リモート接続先プロファイルのユーザ保留音源およびネットワーク保留 MoH 音源の設定とデバイス プールのメディア リソース グループ リスト（MRGL）の組み合せが、保留デバイスに送信する MoH ストリームの決定に使用されます。

シングル企業ボイスメール ボックス

Unified Mobility とモバイル コネクトを組み合せることによって、1 つのボイスメール ボックスで会社のすべてのビジネス コールに対応することもできます。これによって、ユーザは、会社の電話番号にかかってくる電話用に用意された複数のメールボックス（会社、携帯電話、自宅など）をチェックする必要がなくなります。この機能の実装を支援するために、Remote Destination 設定ページで通常の自動転送タイマーと組み合せて使用できる一連のタイマーが利用できます。これらのタイマーの目的は、コールが無応答呼び出しでボイルメール ボックスに転送されたときに、そのコールがリモート接続先のボイスメール ボックスではなく、会社のボイルメール ボックスに転送されることを保証することです。この動作は、次の 2 つの方法のどちらかで実現できます。

- デスクトップフォンの無応答転送時間をリモート接続先電話機よりも短くします。

  これを実現するために、Unified CM のグローバルな無応答転送タイマー フィールドまたは個々の電話回線の無応答呼び出し期間フィールドを、リモート接続先電話機のリモート接続先ボイスメール ボックスに転送されるまでの呼び出し期間より短い値に設定します。加えて、Remote Destination 設定ページの Delay Before Ringing Timer パラメータを使用して、リモート接続先電話機の呼び出しを遅らせることによって、リモート接続先電話機からそのボイスメール ボックスに転送されるまでの時間を延ばすことができます。ただし、Delay Before Ringing Timer パラメータを調整する場合は、グローバルな Unified CM 無応答転送タイマー（または回線レベルの無応答呼び出し期間フィールド）が、モビリティ ユーザが余裕を持ってリモート接続先電話機の呼び出しに応答できる値に設定されていることを確認する必要があります。Delay Before Ringing Timer パラメータは、リモート接続先ごとに設定することが可能で、デフォルト値は 4,000 ミリ秒です。

- リモート接続先電話機のボイスメール ボックスに転送される前にその電話機の呼出音を停止します。

  この動作は、Remote Destination 設定ページの Answer Too Late Timer パラメータを、リモート接続先電話機が呼び出されてからボイスメール ボックスに転送されるまでの時間より短い値に設定することによって実現できます。これによって、コールがリモート接続先電話機のボイスメール ボックスに転送される前にその電話機の呼出音が停止します。Answer Too Late Timer パラメータは、リモート接続先ごとに設定することが可能で、デフォルト値は 19,000 ミリ秒です。

ユーザのリモート接続先電話機が通話中でコール ウェイティングが使用できない場合、または、ユーザの携帯電話が圏外にある場合でもコールが会社のボイスメール ボックスに転送されることを保証するために、Remote Destination 設定ページの Answer Too Soon Timer パラメータを使用できます。コールがリモート接続先ボイスメールに転送され、すぐに応答された場合は、このパラメータによって、リモート接続先電話機に転送されたコール レッグが切断され、デスクトップフォンで応答する時間または会社のボイスメール システムでコールを処理する時間が増えることが保証されます。Answer Too Soon Timer パラメータは、リモート接続先ごとに設定することが可能で、デフォルト値は 1,500 ミリ秒です。

（注） モビリティ ユーザが、Answer Too Soon Timer が切れてから、手動でリモート接続先に宛先変更した着信コールは、最終的にモバイル ボイスメール ボックスに転送される可能性があります。この発生を防ぐには、ボイスメールに宛先変更する着信コールの呼び出しを無視または無効にするようにモビリティ ユーザに助言する必要があります。これによって、無応答コールは必ず、会社のボイスメール ボックスに転送されることが保証されます。

（注） ほとんどの配置シナリオでは、Delay Before Ringing Timer、Answer Too Late Timer、および Answer Too Soon Timer のデフォルト値で十分であり、変更する必要はありません。

モバイル コネクトの有効化と無効化

モバイル コネクト機能は、次の方法のいずれかを使用して有効または無効にできます。

- Cisco Unified CM Administration ページまたは Cisco Unified CM User Options ページ

  管理者またはユーザが、Mobile Connect チェックボックスをオフにしてその機能を無効にするか、Mobile Connect チェックボックスをオンにしてその機能を有効にします。これをリモート接続先ごとに実行します。

- モバイル ボイス アクセスまたはエンタープライズ機能アクセス

  モビリティ対応ユーザが、モバイル ボイス アクセスまたはエンタープライズ機能アクセスにダイヤルインして、適切なクレデンシャルを入力後に、数字の 2 を入力して有効にするか、数字の 3 を入力して無効にします。モバイル ボイス アクセスでは、単一のリモート接続先またはすべてのリモート接続先のモバイル コネクトを有効/無効にするように促されます。エンタープライズ機能アクセスでは、呼び出しているリモート接続先のモバイル コネクトしか有効/無効にできません。

- デスクトップフォンの Mobility ソフトキー

  ユーザは、電話がオンフック状態のときに Mobility ソフトキーを押して、モバイル コネクトを有効にするか、無効にするかを選択します。この方法では、ユーザのリモート接続先のモバイル コネクトすべてが有効または無効にされます。

- Cisco Unified Mobile Communicator クライアント

  Cisco Unified Mobile Communicator クライアントを実行しているリモート接続先電話機を利用しているユーザは、クライアントの初期設定画面でシングル ナンバー リーチ設定の有効/無効を切り替えることによって、モバイル コネクト機能のステータスを切り替えることができます。これによって、Cisco Unified Mobile Communicator リモート接続先のモバイル コネクトのみが有効または無効になります。

モバイル コネクト コールの許可または拒否用のアクセス リスト

アクセス リストは、Cisco Unified CM 内で設定して、リモート接続先に関連付けることができます。アクセス リストは、モビリティ対応ユーザのリモート接続先に転送される着信コールを許可または拒否（着信コールの発信者 ID に基づく）するために使用されます。さらに、これらのアクセス リストは時刻に基づいて呼び出されます。

アクセス リストは、拒否または許可するモビリティ対応ユーザごとに設定されます。アクセス リストには、特定の番号または番号マスクで構成された 1 つ以上のメンバーまたはフィルタが含まれており、このフィルタが発信側の着信コールの発信者 ID と比較されます。発信者 ID と照合するための特定の番号文字列または番号マスクが含まれることに加えて、アクセス リストには、発信者 ID が使用できない、または、発信者 ID がプライベートに設定されている着信コール用のフィルタも含めることができます。拒否対象のアクセス リストには、アクセス リストに入力された番号からのコールは拒否されるが、その他の番号からのコールは許可されるように、リストの最後に暗黙の「すべて許可」が含まれています。許可対象のアクセス リストには、アクセス リストに入力された番号からのコールは許可されるが、その他の番号からのコールは拒否されるように、リストの最後に暗黙の「すべて拒否」が含まれています。

設定したアクセス リストを Remote Destination 設定画面で設定した Ring Schedule に関連付けると、設定した Ring Schedule と選択したアクセス リストの組み合せによって、リモート接続先ごとのモバイル コネクトの時刻コール フィルタリングが提供されます。Cisco Unified CM Administration インターフェイスを使用している管理者または Cisco Unified CM User Options インターフェイスを使用しているエンド ユーザは、アクセス リストと Ring Schedule を設定してリモート接続先に関連付けることができます。

モバイル コネクトのアーキテクチャ

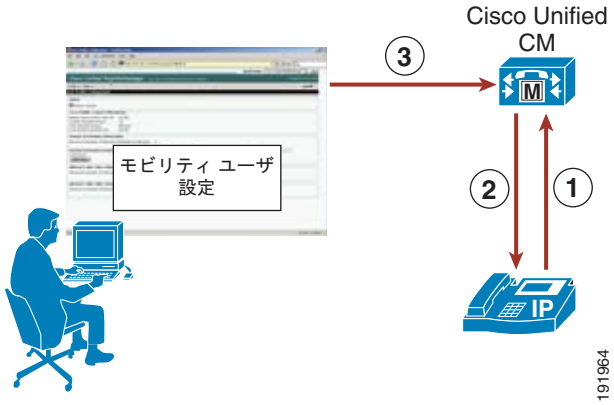
モバイル コネクト機能のアーキテクチャを理解することは、その機能を理解することと同様に重要です。図 25-6 に、モバイル コネクトに必要なメッセージ フローとアーキテクチャを示します。次の相互作用とイベントのシーケンスが、Unified CM、モバイル コネクト ユーザ、およびモバイル コネクト ユーザのデスクトップフォンの間で発生する可能性があります。

1. モバイル コネクト機能の有効化または無効化、あるいはリモート接続先電話機の通話中コールのピックアップを希望しているモバイル コネクト電話機のユーザが、デスクトップフォンの Mobility ソフトキーを押します（図 25-6 のステップ 1 を参照）。
2. Unified CM からモバイル コネクトのステータス（オンまたはオフ）が返されます。ユーザは、電話が接続状態であれば携帯電話にコールを転送するオプションを選択することも、電話がオンフック状態であればモバイル コネクトのステータスを有効/無効にすることもできます（図 25-6 のステップ 2 を参照）。
3. モバイル コネクト ユーザは、Unified CM User Options インターフェイスを使用して、次の URL にある Web ベースの設定ページ経由で独自のモビリティ設定を構成できます。

   http://<*Unified-CM_Server_IP_Address*>/ccmuser/

   ここで、<*Unified-CM_Server_IP_Address*> は、Unified CM パブリッシャ サーバの IP アドレスです（図 25-6 のステップ 3 を参照）。

図 25-6　　モバイル コネクトのアーキテクチャ



モバイル コネクトの冗長性

モバイル コネクト機能には、次のコンポーネントが必要です。

- Unified CM サーバ
- 公衆網ゲートウェイ

各コンポーネントの冗長性または弾力性を向上させて、さまざまな障害シナリオでモバイル コネクトの機能が失われないようにする必要があります。

Unified CM サーバの冗長性

モバイル コネクト機能には、Unified CM サーバが不可欠です。Unified CM Group による電話機とゲートウェイの登録が冗長になっていれば、Unified CM サーバが故障してもモバイル コネクト機能は影響を受けません。

モバイル コネクト ユーザが Unified CM User Options Web インターフェイスを使用してモビリティ設定（リモート接続先とアクセス リスト）を構成できるようにするには、Unified CM パブリッシャ サーバが使用可能である必要があります。パブリッシャがダウンすると、ユーザはモビリティ設定を変更できなくなります。同様に、管理者も Unified CM でモビリティ設定を変更できなくなります。ただし、既存のモビリティ設定と機能は維持されます。最後に、システムでモバイル コネクトのステータスに対する変更を Unified CM パブリッシャ サーバ上に記録する必要があります。Unified CM パブリッシャが使用できない場合は、モバイル コネクトの有効化または無効化が使用できなくなります。

公衆網ゲートウェイの冗長性

モバイル コネクト機能は、新しいコール レッグを公衆網に拡張してモバイル コネクト ユーザのリモート接続先電話機に到達する能力に依存しているため、公衆網ゲートウェイの冗長性は重要です。公衆網ゲートウェイが故障したり、容量不足の場合は、モバイル コネクト コールを完了できません。通常は、会社の IP テレフォニー ダイヤル プランを通して、物理的なゲートウェイの冗長性とコールの再ルーティング機能だけでなく、予想されるコール アクティビティを処理する十分な容量が提供されることによって、公衆網アクセスに冗長性が提供されます。Unified CM が、コール ルーティングの弾力性を確保するための十分な容量、複数のゲートウェイ、およびルート グループとルート リストの構造で構成されていれば、この冗長性によってモバイル コネクト機能の持続性が保証されます。

モバイル ボイス アクセスとエンタープライズ機能アクセス

モバイル ボイス アクセス（システム リモート アクセスとも呼ばれる）とエンタープライズ機能アクセス 2 ステージ ダイヤリングは、モバイル コネクト アプリケーションに組み込まれている機能です。両方の機能を使用すれば、モビリティ対応ユーザは、外出先でも、Unified CM に直接接続されているかのように電話をかけることができます。この機能は、従来のテレフォニー環境では、一般的に、Direct Inward System Access（DISA）と呼ばれています。これらの機能を通して、通話料金を抑えたり、モバイル ユーザごとに通話料を請求するのではなく、直接会社に請求するように配慮することによって、会社にメリットがもたらされます。加えて、これらの機能を使用すれば、ユーザは、発信者 ID を外部に送信するときに、携帯電話やリモート接続先の番号を隠すことができます。代わりに、発信者 ID として、ユーザの会社の電話番号が送信されます。これによって、ユーザへの返信コールは会社の電話番号にかけられるため、コールを会社で一括管理できます。また、モバイル ユーザは、これらの機能を使用して、通常は企業外部から到達不能な内部の内線番号や DID 以外の会社の電話番号にダイヤルできます。

モバイル ボイス アクセスには、H.323 または SIP VoiceXML（VXML）ゲートウェイで応答および処理されるシステム設定の DID 番号を呼び出すことによってアクセスします。VoiceXML ゲートウェイによって、モバイル ボイス アクセス ユーザに対する双方向音声応答（IVR）プロンプトが再生され、ユーザ認証と電話機のキーパッド経由でダイヤルされる番号入力が要求されます。

（注） SIP VXML ゲートウェイでモバイル ボイス アクセスをサポートするには、Unified CM 7.1(3) 以降のリリースが必要です。

エンタープライズ機能アクセス機能には、前述した通話切替機能や会議機能だけでなく、2 ステージ ダイヤリング機能が含まれています。2 ステージ ダイヤリングは、IVR プロンプトを除いて、モバイル ボイス アクセスと同様の方法で動作します。システム設定のエンタープライズ機能アクセス DID が Unified CM によって応答されます。ユーザは、電話機のキーパッドまたはスマート フォン ソフトキーを使用して、認証とダイヤルする番号を入力します。これらの入力はプロンプトなしで受信されます。

モバイル ボイス アクセスとエンタープライズ機能アクセス 2 ステージ ダイヤリングの両方の機能を使用すれば、ユーザは、入力番号に対するコールが接続されたときに、通話切替機能を呼び出したり、モバイル コネクト コールと同様にデスクトップフォンでコールをピックアップしたりすることができます。この動作は、コールが会社のゲートウェイに固定されることによって可能になります。

モバイル ボイス アクセスとエンタープライズ機能アクセスの電話機サポート

モバイル ボイス アクセスとエンタープライズ機能アクセスは、DTMF 番号の送信機能を持つすべての着信公衆網デバイスでサポートされています。これらの機能に対する Cisco Unified IP Phone のサポートは、モバイル コネクトと同様です（「モバイル コネクトの電話機サポート」（P.25-6）を参照）。モバイル ボイス アクセスまたはエンタープライズ機能アクセスの 2 ステージ ダイヤリングを使用するために IP Phone は必要ありませんが、これらの機能のいずれかによって発信された通話中コールをデスクトップフォンでピックアップするには、モバイル コネクトでサポートされている電話機モデルのいずれかを使用する必要があります。

モバイル ボイス アクセスとエンタープライズ機能アクセスに関連した Unified CM のサービスとサービス パラメータ

モバイル ボイス アクセス アプリケーションを正常に機能させるためには、Unified CM 上で特定のサービスを有効にして Cisco Unified Mobility 上で特定のパラメータを設定する必要があります。この項では、このようなサービスとパラメータについて説明します。

モバイル ボイス アクセスに関連した Unified CM のサービス

モバイル ボイス アクセス機能を使用するには、Unified CM Serviceability の設定ページで Cisco Unified Mobile Voice Access Service を手動でアクティブにする必要があります。このサービスは、パブリッシャ ノードでのみアクティブにすることができます。

モバイル ボイス アクセスとエンタープライズ機能アクセスに関連した Unified CM のサービス パラメータ

次のリストは、モバイル ボイス アクセスとエンタープライズ機能アクセス 2 ステージ ダイヤリング機能に関連した Unified CM サービス パラメータの一部を示しています。

- Enable Enterprise Feature Access（デフォルト値：False）

  このパラメータによって、システムのエンタープライズ機能アクセスを有効にするかどうかが決定されます。2 ステージ ダイヤリング機能を使用するだけでなく、リモート接続先電話機から保留、保留解除、転送などの通話切替機能を呼び出す場合は、このパラメータを True に設定する必要があります。

- Enable Mobile Voice Access（デフォルト値：False）

  このパラメータによって、システムのモバイル ボイス アクセスを有効にするかどうかが決定されます。モバイル ボイス アクセスと呼ばれるリモート システム アクセス機能を使用する場合は、このパラメータを True に設定する必要があります。

- Matching Caller ID with Remote Destination（デフォルト値：Complete Match）

  このパラメータは、着信コールに対して、設定済みのリモート接続先の発信者 ID を全体的に照合するか、部分的に照合するかを指定します。この設定に基づいて、発信者 ID が、リモート接続先ごとに設定された接続先番号と全体的または部分的に照合されます。[Partial Match] に設定されて

いる場合は、このパラメータと [Number of Digits for Caller ID Partial Match] サービス パラメータを組み合せて、提供された発信者 ID 内の何桁の数字を照合するかが決定されます。発信者 ID の照合によって、エンタープライズ機能アクセス通話切替機能と 2 ステージ ダイヤリングに加えて、モバイル ボイス アクセスを呼び出すために、リモート接続先をシステムで認識するかどうかが決定されます。

- Number of Digits for Caller ID Partial Match（デフォルト値：10）

  このパラメータによって、発信者 ID の連続する何桁を設定済みのリモート接続先と照合するかが決定されます。このパラメータは、Matching Caller ID with Remote Destination サービス パラメータが Partial Match に設定されている場合にのみ使用されます。

- System Remote Access Blocked Numbers（デフォルト値：<空白>）

  このパラメータは、モバイル ボイス アクセス機能またはエンタープライズ機能アクセス 2 ステージ ダイヤリング機能を使用している場合に、リモート接続先電話機からダイヤルできない番号（911 やその他の緊急電話番号など）のカンマ区切りのリストを指定します。この拒否対象番号のリストは Application Dial Rules が適用された場合にのみ適用されるため、番号は社内からダイヤルする場合と同様に該当する公衆網アクセス コードを付けて入力する必要があります（9911 など）。

これらのシステム パラメータを設定することに加えて、End User 設定ページの Enable Mobile Voice Access チェックボックスをオンにすることによって、ユーザごとにモバイル ボイス アクセスを有効にする必要があります。

モバイル ボイス アクセス IVR VoiceXML ゲートウェイ URL

モバイル ボイス アクセス機能を使用するには、Unified CM VoiceXML アプリケーションを H.323 または SIP ゲートウェイ上にインストールする必要があります。このアプリケーションをロードするための URL は次のとおりです。

http://<*Unified-CM-Publisher_IP-Address*>:8080/ccmivr/pages/IVRMainpage.vxml

ここで、<*Unified-CM-Publisher_IP-Address*> は、Unified CM パブリッシャ ノードの IP アドレスです。

モバイル ボイス アクセス機能

図 25-7 に、モバイル ボイス アクセスのコール フローを示します。この例では、モバイル ボイス アクセス ユーザが公衆網電話機（408 555-7890）からモバイル ボイス アクセス会社の DID DN 408-555-2345 にダイヤルします（ステップ 1）。

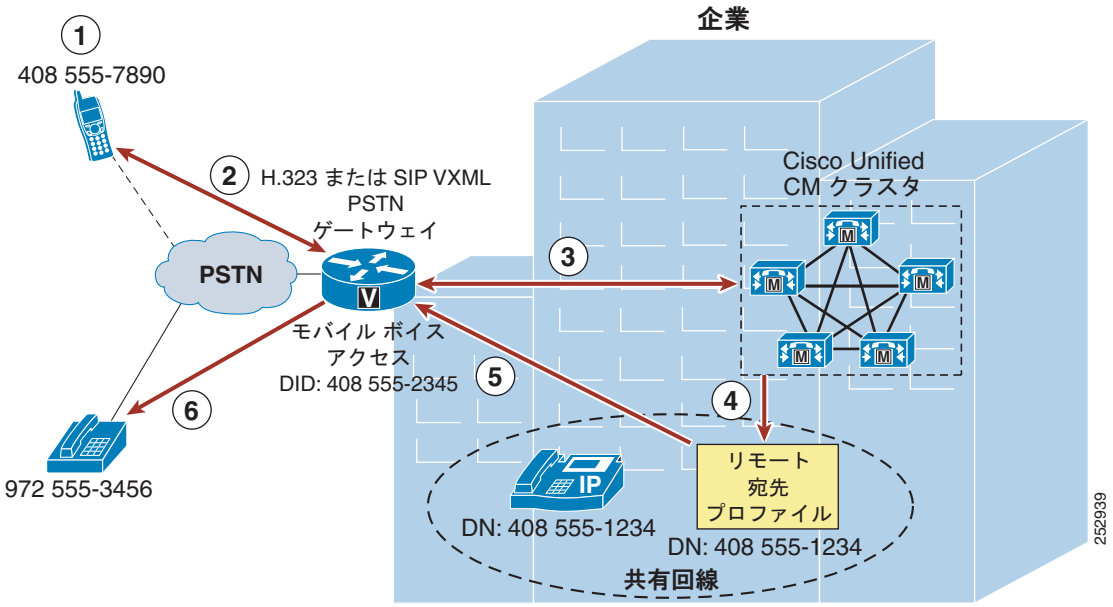
このコールは、VoiceXML ゲートウェイとしても機能する会社の公衆網 H.323 または SIP ゲートウェイに入ります。ユーザは、IVR 経由で、数字のユーザ ID（後ろに # 記号が続く）、PIN 番号（後ろに # 記号が続く）、および 1 の入力と、相手の電話番号が続くモバイル ボイス アクセス コールの発信を要求されます。この場合は、ユーザが相手の番号として 9 1 972 555 3456（後ろに # 記号が続く）を入力します（ステップ 2）。

（注）　モバイル ボイス アクセス ユーザがかけている公衆網電話機が、そのユーザのモバイル コネクト リモート接続先として設定されており、Unified CM で着信コールの発信者 ID とこのリモート接続先を照合可能な場合は、数字のユーザ ID を入力する必要がありません。代わりに、PIN 番号の入力だけが要求されます。

その一方で、IVR プロンプトが Unified CM からゲートウェイに転送され、ゲートウェイでユーザに対してプロンプトが再生され、ゲートウェイでユーザの数字の ID と PIN 番号を含む入力が収集されます。この情報は、認証と 9 1 972 555 3456 へのコールを発信するために Unified CM に転送されます（ステップ 3）。ユーザの認証とダイヤルする番号の受信後に、Unified CM でユーザのリモート接続先

プロファイル経由のコールが発信されます（ステップ 4）。972 555-3456 への発信コールが、公衆網ゲートウェイ経由で経路設定されます（ステップ 5）。最後に、番号が 972 555-3456 の公衆網接続先電話機で呼出音が鳴ります（ステップ 6）。

図 25-7　　モバイル ボイス アクセス



（注）　モバイル ボイス アクセスを図 25-7 のように動作させるには、システム全体の Enable Mobile Voice Access サービス パラメータが True に設定（「モバイル ボイス アクセスとエンタープライズ機能アクセスに関連した Unified CM のサービス パラメータ」（P.25-17）を参照）され、End User 設定ページのユーザごとの Enable Mobile Voice Access チェックボックスがオンになっていることを確認してください。

ヘアピニングを使用したモバイル ボイス アクセス

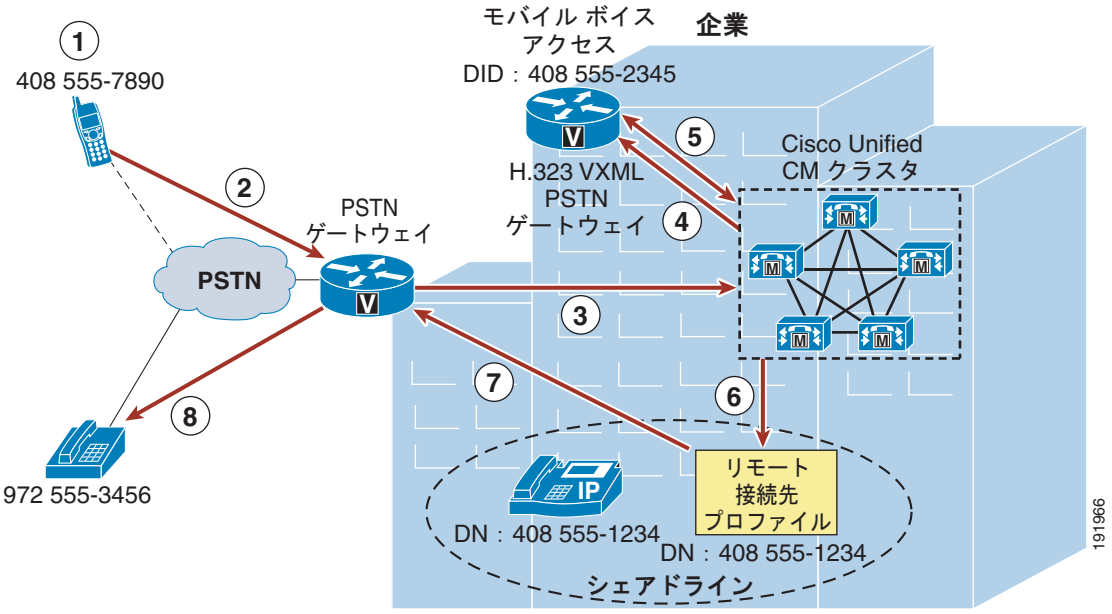
会社の公衆網ゲートウェイで H.323 または SIP が使用されていない配置では、H.323 を実行している別のゲートウェイ上のヘアピニングを使用することによってモバイル ボイス アクセス機能を提供することもできます。ヘアピニングを使用したモバイル ボイス アクセスの場合は、VoiceXML 機能を別の H.323 ゲートウェイに持たせる必要があります。図 25-8 に、ヘアピニングを使用したモバイル ボイス アクセスのコール フローを示します。この例では、前の例と同じく、モバイル ボイス アクセス ユーザが公衆網電話機（408 555-7890）からモバイル ボイス アクセス会社の DID DN 408-555-2345 にダイヤルします（ステップ 1）。コールは、会社の公衆網ゲートウェイに入り（ステップ 2）、Unified CM に転送されてコール処理されます（ステップ 3）。次に、着信コールは、Unified CM から H.323 VoiceXML ゲートウェイにルーティングされます（ステップ 4）。ユーザは、IVR によって、数字のユーザ ID、PIN、および 1 の入力と、相手の電話番号が続くモバイル ボイス アクセス コールの発信を要求されます。この場合も、ユーザが相手の番号として 9 1 972 555 3456（後ろに # 記号が続く）を入力します。

（注）　ヘアピニングを使用したモバイル ボイス アクセスでは、システムを呼び出しているユーザが発信者 ID によって自動的に特定されません。代わりに、PIN 番号を入力する前に、手動でリモート接続先の番号を入力する必要があります。ユーザが自動的に特定されない理由は、ヘアピニングを使用する配置では、公衆網ゲートウェイにおいて最初にコールを Unified CM にルーティングして、ヘアピンされるモバイル ボイス アクセス ゲートウェイに到達する必要があるためです。コールが最初に Unified CM にルーティングされるため、発信番号が携帯の番号から会社の電話番号に変換されてから、コールがモバイル ボイス アクセス ゲートウェイによって処理されます。このため、モバイル ボイス アクセス ゲートウェイでは、発信番号と設定されているリモート接続先との照合を行うことができず、ユーザはリモート接続先番号の入力を求められます。これは、ヘアピニングを使用する配置に特有の現象です。通常のモバイル ボイス アクセスのフローにおいては、モバイル ボイス アクセス機能はローカル ゲートウェイで利用できるため、公衆網ゲートウェイで最初にコールを Unified CM にルーティングしてからモバイル ボイス アクセスにアクセスする必要がありません。

その一方で、H.323 VoiceXML ゲートウェイでは、ユーザ入力が収集されて、Unified CM に転送されます。その後、転送された IVR プロンプトが公衆網ゲートウェイおよびモバイル ボイス アクセス ユーザに対して再生されます。Unified CM では、ユーザ入力を受信すると、ユーザを認証して、適切な IVR プロンプトをユーザ入力に基づいて H.323 VoiceXML ゲートウェイに転送します（ステップ 5）。ダイヤルする番号の受信後に、Unified CM でユーザのリモート接続先プロファイルを使用してコールが発信されます（ステップ 6）。972 555-3456 への発信コールが、公衆網ゲートウェイ経由でルーティングされます（ステップ 7）。最後に、番号が 972 555-3456 の公衆網接続先電話機で呼出音が鳴ります（ステップ 8）。

ヘアピニングを使用した各モバイル ボイス アクセス コールでは、音声メディア パスは、2 つのゲートウェイ ポートを使用している会社の公衆網ゲートウェイ内だけではなく、H.323 VoiceXML ゲートウェイでもヘアピンされます。

図 25-8　　ヘアピニングを使用したモバイル ボイス アクセス



（注）　モバイル ボイス アクセスをヘアピニング モードで配置する場合は、公衆網ゲートウェイでのモバイル ボイス アクセス DID と Cisco Unified CM 内のモバイル ボイス アクセス電話番号（**Media Resources - Mobile Voice Access**）を別々の番号として設定することをお勧めします。そうすれば、Unified CM

内のトランスレーション パターンを使用して、モバイル ボイス アクセス DID の着信番号を設定済みのモバイル ボイス アクセス電話番号に変換できます。Unified CM 内で設定されたモバイル ボイス アクセス電話番号は管理者にしか表示されないため、DID と電話番号間の変換をエンド ユーザが意識する必要はなく、エンド ユーザのダイヤリング動作に変更は生じません。この方法は、マルチクラスタ環境でのモビリティ コール ルーティング問題を回避するために推奨されています。この推奨事項は、非ヘアピニング モードのモバイル ボイス アクセスには当てはまりません。

（注）　ヘアピニング モードのモバイル ボイス アクセスは、H.323 VXML ゲートウェイだけでサポートされています。

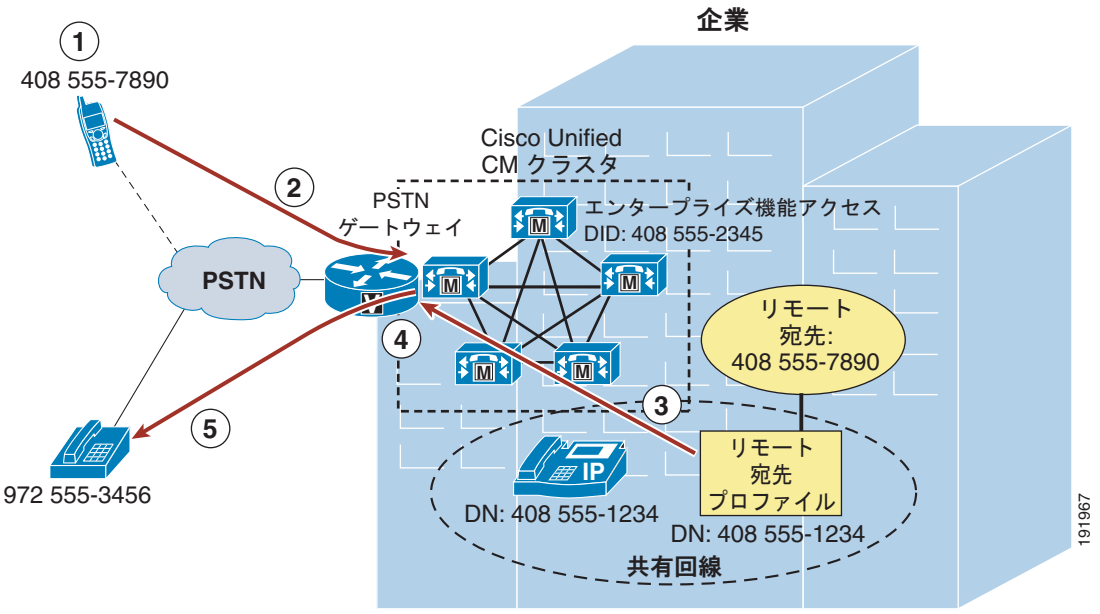
2 ステージ ダイヤリングを伴うエンタープライズ機能アクセス

図 25-9 に、エンタープライズ機能アクセス 2 ステージ ダイヤリングを示します。この例では、モビリティ ユーザがリモート接続先電話機（408 555-7890）からエンタープライズ機能アクセス DID 408 555-2345 にダイヤルします（ステップ 1）。コールが接続されると、Unified CM で認証されるユーザの PIN（後ろに # 記号が続く）で始まる DTMF 番号を公衆網ゲートウェイ経由で Unified CM に送信するためにリモート接続先電話機が使用されます。次に、2 ステージ ダイヤリング対象コールが試みられることを示す 1（後ろに # 記号が続く）と相手の電話番号が送信されます。この場合は、ユーザが接続先番号として 9 1 972 555 3456 と入力します（ステップ 2）。

（注）　モバイル ボイス アクセスとは違って、エンタープライズ機能アクセスでは、エンド ユーザ アカウントに対して発信者 ID と PIN を照合するためにリモート接続先として設定された電話機から、すべての 2 ステージ ダイヤリング対象コールを発信する必要があります。エンタープライズ機能アクセスにおいては、モビリティ ユーザが自身を識別するためのリモート接続先番号または ID をシステムに入力するための仕組みは用意されていません。同一性は、着信コールの発信者 ID と入力された PIN の組み合せを通してのみ確立することができます。

次に、発信コールがユーザのリモート接続先プロファイル経由で開始され（ステップ 3）、公衆網番号 972 555-3456 へのコールが会社の公衆網ゲートウェイ経由で経路設定されます（ステップ 4）。最後に、公衆網電話機が呼び出されます（ステップ 5：この場合は 972 555-3456）。モバイル ボイス アクセスと同様に、各エンタープライズ機能アクセス 2 ステージ ダイヤリング対象コールの音声メディア パスは、2 つのポートを使用している公衆網ゲートウェイ内でヘアピンされます。

図 25-9　エンタープライズ機能アクセス 2 ステージ ダイヤリング機能



（注）　エンタープライズ機能アクセス 2 ステージ ダイヤリングを図 25-9 のように動作させるには、システム全体の Enable Enterprise Feature Access サービス パラメータが True に設定されていることを確認してください（「モバイル ボイス アクセスとエンタープライズ機能アクセスに関連した Unified CM のサービス パラメータ」（P.25-17）を参照）。

デスクトップフォンとリモート接続先電話機のピックアップ

モバイル ボイス アクセス機能とエンタープライズ機能アクセス機能はモバイル コネクトと緊密に統合されているため、モバイル ボイス アクセスまたはエンタープライズ機能アクセス 2 ステージ ダイヤリング対象コールが確立されていれば、ユーザはモバイル コネクト機能を利用して、最初に着信した電話機をオン フックしてデスクトップフォンの Resume ソフトキーを押すだけで、または、通話切替保留機能を使用して、通話中のコールをデスクトップフォンでピックアップできます。さらに、その後で、ユーザの設定済みリモート接続先電話機で Mobility ソフトキーを押して Send Call to Mobile Phone を選択することによって、そのコールをピックアップできます。

モバイル コネクトの有効化と無効化

モバイル ボイス アクセスとエンタープライズ機能アクセスのユーザにまるで社内にいるかのように公衆網から電話がかけられる能力を提供することに加えて、H.323 または SIP VoiceXML ゲートウェイ上のモバイル ボイス アクセスで提供される機能とエンタープライズ機能アクセスで提供される機能によって、電話機のキーパッド経由でリモート接続先ごとのモバイル コネクト機能をリモートで有効または無効にできる能力もユーザに提供されます。1 を入力して電話をかけるのではなく、ユーザは、2 を入力してモバイル コネクト機能を有効にし、3 を入力してモバイル コネクト機能を無効にします。

モバイル ボイス アクセスを使用するにあたって、複数のリモート接続先を設定する場合は、モバイル コネクト機能を有効または無効にするリモート接続先の電話番号を入力するように要求されます。エンタープライズ機能アクセスでは、呼び出しているリモート接続先電話機のモバイル コネクトしか有効/無効にできません。

モバイル ボイス アクセスとエンタープライズ機能アクセスの番号拒否

管理者は、モバイル ボイス アクセスとエンタープライズ機能アクセスの 2 ステージ ダイヤリングのユーザが、それらの機能の使用中は特定の番号にダイヤルできないようにすることができます。オフネット コールに対してこれらの機能を使用している場合に特定の番号へのコールを制限または拒否するには、System Remote Access Blocked Numbers サービス パラメータ フィールドでそのような番号のカンマ区切りのリストを設定できます（「モバイル ボイス アクセスとエンタープライズ機能アクセスに関連した Unified CM のサービス パラメータ」（P.25-17）を参照）。このパラメータに拒否する番号を設定したら、モバイル ボイス アクセスまたはエンタープライズ機能アクセスが使用されている場合は、ユーザのリモート接続先電話機からそれらの番号にダイヤルできなくなります。管理者が拒否したい番号には、911 などの緊急電話番号を含めることができます。拒否する番号を設定する場合は、会社のユーザが該当するプレフィックスまたは振り分け用の数字を付けてダイヤルするようにそれらの番号が設定されていることを確認してください。たとえば、緊急電話番号を拒否対象としているときに、9911 をダイヤルしなければならない場合は、System Remote Access Blocked Numbers フィールドに設定する番号を 9911 にする必要があります。

モバイル ボイス アクセスおよびエンタープライズ機能アクセスのアクセス番号

Unified CM システムでは、1 つのモバイル ボイス アクセス電話番号と 1 つのエンタープライズ機能アクセス番号だけを設定することもできますが、これらの内部で設定された番号にアクセス可能な外部番号を複数使用できます。たとえば、米国の New York City に配置されたシステム、San Jose のリモートサイト、および London の海外サイトがある場合を考えます。システムのモバイル ボイス アクセス電話番号が 555-1234 に設定されている場合でも、各ロケーションのゲートウェイを設定して、ローカル DID 番号またはフリーダイヤル DID 番号をこのモバイル ボイス アクセス電話番号にマッピングできます。たとえば、New York のゲートウェイの DID である +1 212 555 1234 と +1 800 555 1234 の両方をモバイル ボイス アクセス番号にマッピングし、さらに San Jose のゲートウェイの DID +1 408 666 5678 および London のゲートウェイの DID +44 208 777 0987 もシステムのモバイル ボイス アクセス番号にマッピングできます。システム管理者は、複数のローカル DID 番号またはフリーダイヤル DID 番号を用意することによって、2 ステージ ダイヤリング対象コールが常にローカルまたはフリーダイヤルのコールとしてシステムに発信されるようにすることができ、さらにテレフォニー関連コストを削減できます。

リモート接続先の設定と発信者 ID の照合

モバイル ボイス アクセス機能およびエンタープライズ機能アクセス 2 ステージ ダイヤリング機能に加えて、通話切替機能の転送と会議のユーザを認証するときに、発信元のリモート接続先電話機の発信者 ID がシステム内で設定されたすべてのリモート接続先に対して照合されます。この発信者 ID の照合は、リモート接続先番号の設定方法、システム上で Application Dial Rules が設定されているかどうか、Matching Caller ID with Remote Destination パラメータが Partial Match と Complete Match のどちらに設定されているかなどの複数の要因に左右されます（「モバイル ボイス アクセスとエンタープライズ機能アクセスに関連した Unified CM のサービス パラメータ」（P.25-17）を参照）。

この照合の特性を制御するために、次の 2 つのアプローチを検討してください。

Application Dial Rules の使用

このアプローチでは、発信者 ID が公衆網から供給されているかのようにリモート接続先を設定します。たとえば、リモート接続先電話機の発信者 ID を公衆網から 4085557890 として供給する場合は、Remote Destination 設定ページでこの番号を設定する必要があります。モバイル コネクト コールを適切にこのリモート接続先に経路設定するには、Application Dial Rules を使用して必要な公衆網アクセス コードなどの数字を前に付加する必要があります。たとえば、公衆網にかける場合は 9 が必要で、長距離電話にかける場合は 1 が必要な場合は、[Prefix With Pattern] フィールドを 91 に設定した

Application Dial Rules を作成する必要があります。このアプローチを使用する場合は、Matching Caller ID with Remote Destination パラメータを Complete Match のデフォルト設定のままにする必要があります。

（注）　Application Dial Rules はモバイル コネクト、モバイル ボイス アクセス、およびエンタープライズ機能アクセスのコールに適用されるだけでなく、Cisco WebDialer、Cisco Unified CM Assistant、および Cisco Unified Personal Communicator アプリケーションから発信されたコールにも適用されます。したがって、すべてのアプリケーションを通してダイヤリング動作が期待どおりに機能するように、これらの規則を慎重に設定する必要があります。

Application Dial Rules の代わりとして、適切な公衆網振り分け用数字を先頭に付加するために、Cisco Unified CM ルート リストおよびルート グループ構造内部のトランスレーション パターンまたは数字プレフィックス メカニズムを使用できます。

部分発信者 ID 照合の使用

このアプローチでは、リモート接続先が、システムから公衆網にダイヤルされたかのように設定されます。たとえば、リモート接続先の番号が 14085557890 で、システムから公衆網にアクセスするために 9 を入力する必要がある場合は、Remote Destination 設定ページでこの番号を 914085557890 に設定する必要があります。このアプローチでは、Application Dial Rules を必要としませんが、Matching Caller ID with Remote Destination サービス パラメータを Partial Match に設定し、Number of Digits for Caller ID Partial Match をリモート接続先発信者 ID に対して照合すべき連続桁数を表す数字に設定する必要があります（「モバイル ボイス アクセスとエンタープライズ機能アクセスに関連した Unified CM のサービス パラメータ」（P.25-17）を参照）。たとえば、リモート接続先の発信者 ID が 14085557890 で、リモート接続先が 914085557890 に設定されている場合は、Number of Digits for Caller ID Partial Match を 10 または 11 に設定するのが理想的です。この例では、このパラメータをさらに少ない桁数に設定できます。ただし、システム内のすべての設定済みリモート接続先を一意的に識別できるように十分な連続桁数が照合されることを保証してください。部分発信者 ID 照合を使用したときに完全な一致が見つからず、複数の設定済みリモート接続先が一致した場合は、システムで一致するリモート接続先番号が存在しないものとして処理されます。したがって、モバイル ボイス アクセスの場合は、PIN を入力する前にリモート接続先番号/ID を手動で入力する必要があります。エンタープライズ機能アクセスには、ユーザがリモート接続先番号を入力するメカニズムがありません。そのため、この機能を使用する場合は、一致が一意的にしか発生しないことを保証してください。

（注）　公衆網サービス プロバイダーが可変長の発信者 ID を送信する場合は、着信コールごとの一意的な発信者 ID の一致が保証できない可能性があるため、部分発信者 ID 照合の使用はお勧めできません。このようなシナリオでは、完全発信者 ID 照合の使用をお勧めします。

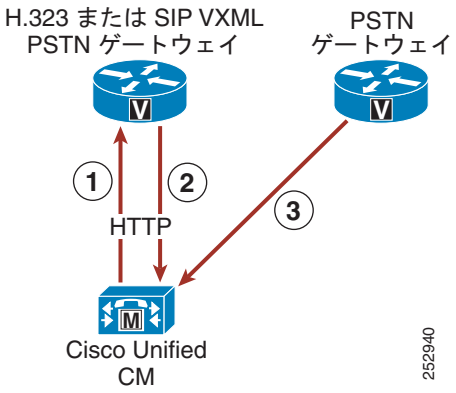
モバイル ボイス アクセスとエンタープライズ機能アクセスのアーキテクチャ

モバイル ボイス アクセスとエンタープライズ機能アクセスのアーキテクチャを理解することは、それらの機能性を理解することと同じくらい重要です。図 25-10 は、モバイル ボイス アクセスとエンタープライズ機能アクセスに必要なメッセージ フローとアーキテクチャを示しています。Unified CM、公衆網ゲートウェイ、および H.323 または SIP VXML ゲートウェイの間には、次の一連の対話とイベントが発生します。

1. Unified CM から HTTP 経由で IVR プロンプトとインストラクションが H.323 または SIP VXML ゲートウェイに転送されます（図 25-10 のステップ 1 を参照）。これによって、VXML ゲートウェイで着信モバイル ボイス アクセス発信者に対してこれらのプロンプトを再生できます。

2. H.323 または SIP VXML ゲートウェイでは、HTTP を使用してモバイル ボイス アクセス ユーザの入力が Unified CM に戻されます（図 25-10 のステップ 2 を参照）。
3. 公衆網ゲートウェイでは、リモート接続先電話機からのエンタープライズ機能アクセス 2 ステージ ダイヤリングおよび通話切替機能に関するユーザまたはスマート フォンのキー シーケンスに応答して DTMF 番号が転送されます（図 25-10 のステップ 3 を参照）。

図 25-10　モバイル ボイス アクセスとエンタープライズ機能アクセスのアーキテクチャ



（注）　図 25-10 では公衆網ゲートウェイとは別のボックスとして H.323 または SIP VoiceXML ゲートウェイが描かれていますが、これはアーキテクチャ上の要件ではありません。公衆網ゲートウェイで H.323 または SIP 以外のプロトコルを実行する必要がなければ、VoiceXML 機能と公衆網ゲートウェイ機能を同じボックスで処理できます。H.323 または SIP ゲートウェイは、モバイル ボイス アクセス VoiceXML 機能に不可欠です。

モバイル ボイス アクセスとエンタープライズ機能アクセスの冗長性

モバイル ボイス アクセス機能とエンタープライズ機能アクセス機能には、モバイル コネクト機能と同じコンポーネントと冗長性メカニズムが必要です（「モバイル コネクトの冗長性」（P.25-15）を参照）。Unified CM Group は、公衆網ゲートウェイ登録の冗長性に欠かせません。同様に、公衆網の物理ゲートウェイとゲートウェイ接続の冗長性を提供する必要があります。公衆網と会社間の冗長なアクセスは、ゲートウェイが故障した場合に、リモート接続先電話機からモバイル ボイス アクセス機能とエンタープライズ機能アクセス機能にアクセスするために必要です。ただし、必要に応じて、H.323 または SIP VoiceXML ゲートウェイに対して物理的な冗長性を提供できますが、Unified CM 上には、Cisco Unified Mobile Voice Access サービス用の冗長性メカニズムがありません。このサービスは、パブリッシャ ノードでしか有効にして実行することができません。そのため、パブリッシャ ノードが無効な場合は、モバイル ボイス アクセス機能が使用できません。エンタープライズ機能アクセスと 2 ステージ ダイヤリング機能には、このようなパブリッシャとの依存関係がないため、モビリティ ユーザに同等の機能性（IVR プロンプトが再生されない）を提供できます。

Unified Mobility

Cisco Unified Mobility ソリューションでは、Cisco Unified CM を介してモビリティ機能が提供されます。機能には、モバイル コネクト、モバイル ボイス アクセス、およびエンタープライズ機能アクセスが含まれます。この機能を配置する場合は、ダイヤル プランの意味、ガイドラインと制約事項、および性能と容量に関する考慮事項を理解しておくことが重要です。

Cisco Unified Mobility のダイヤル プランに関する考慮事項

Unified Mobility を適切に設定してプロビジョニングするには、リモート接続先プロファイル設定のコール ルーティング動作とダイヤル プランの意味を理解しておくことが重要です。

リモート接続先プロファイルの設定

Unified Mobility を設定する場合は、Remote Destination Profile 設定ページにある次の 2 つの設定を考慮する必要があります。

- コーリング サーチ スペース

  この設定と電話番号または回線レベルのコーリング サーチ スペース（CSS）を組み合せて、モビリティ ダイヤル対象コール用にアクセス可能なパーティションが決定されます。この設定は、モバイル ボイス アクセスとエンタープライズ機能アクセス 2 ステージ ダイヤリングを含む、リモート接続先電話機からのモビリティ ユーザによるコールだけでなく、通話切替の転送機能と会議機能の組み合せによるコールにも影響します。この CSS と回線レベルの CSS の組み合せの中に、ユーザのリモート接続先電話機から発信されたビジネス コールのためにアクセスする必要のあるすべてのパーティションが含まれていることを確認してください。

- コーリング サーチ スペースの再ルーティング

  この設定によって、ユーザのリモート接続先電話機にコールが送信されたときにアクセスするパーティションが決定されます。このことは、すべてのモバイル コネクト コールに当てはまります。ユーザの会社の電話番号へのコールもモバイル コネクト経由でユーザのリモート接続先に送信される場合は、この CSS によってシステムからリモート接続先電話機に到達する方法が決定されます。したがって、CSS を通して、公衆網または Global System for Mobile Communication（GSM）ネットワークに到達するために、適切なルート パターンとゲートウェイを含むパーティションにアクセスできる必要があります。

リモート接続先プロファイル ルーティング CSS を設定する場合は、この CSS 内のルート パターンが、ユーザのデスクトップフォンへの着信コールを経路設定するゲートウェイと同じコール アドミッション制御ロケーションにあるゲートウェイを指すようにすることをお勧めします。これによって、コールをリモート接続先に経路設定するときに、2 地点間の帯域幅不足によるコール アドミッション制御拒否が発生しなくなります。さらに、WAN 帯域幅が不十分な場合は、初期モバイル コネクト コールの経路設定後のコール アドミッション制御チェックで拒否されないため、同じコール アドミッション制御ロケーション内のゲートウェイに着信コール レッグと発信コール レッグを経路設定することによって、このコール中の以降のデスクトップフォンまたはリモート接続先のピックアップ動作で WAN 帯域幅のオーバーサブスクリプションが発生する可能性のあるコール アドミッション制御の必要がなくなることが保証されます。

同様に、発信モバイル ボイス アクセスまたはエンタープライズ機能アクセス 2 ステージ ダイヤリング コール ルーティング用のリモート接続先プロファイル CSS を設定する場合は、このコーリング サーチ スペース内のルート パターンが、モバイル ボイス アクセスまたはエンタープライズ機能アクセス DID への着信コール レッグを処理するゲートウェイと同じコール アドミッション制御ロケーションにあるゲートウェイを指すようにすることをお勧めします。これによって、ダイヤル先番号への初期発信コール ルーティング中に帯域幅不足によるコール アドミッション制御拒否が発生しないことが保証されま

す。ただし、デスクトップフォンがモバイル ボイス アクセスまたはエンタープライズ機能アクセス DID が転送されるゲートウェイとは異なるコール アドミッション制御ロケーション内に存在する場合は、以降のデスクトップフォンのピックアップによって、WAN 帯域幅のオーバーサブスクリプションが発生する可能性があることに注意してください。

最後に、モビリティ対応ユーザへの着信公衆網コールは、必ず、会社のデスクトップフォンの DID に基づいてホーム ロケーション ゲートウェイに入るため、モビリティ対応ユーザが、別のサイトでのエクステンション モビリティ ログインまたは別のコール アドミッション制御ロケーションへのデスクトップフォンの物理的移動が原因でコール アドミッション制御ロケーションを移動していた場合は、着信コールが入るゲートウェイと同じコール アドミッション制御ロケーション内に配置された発信ゲートウェイを指すことがほとんど不可能になります。そのため、モビリティ対応ユーザがエクステンション モビリティを使用して、ホーム ロケーション外部のコール アドミッション制御ロケーション内の電話機にログインしたり、コール アドミッション制御ロケーション間でデバイスを物理的に移動したりするシナリオや配置は避けることをお勧めします。このようなシナリオを回避または制限することができない場合は、コール アドミッション制御拒否が原因のコール レッグ障害またはデスクトップフォンやリモート接続先のピックアップ アクティビティが原因の WAN オーバーサブスクリプションが発生する確率が高くなります。

自動発信者 ID 照合とエンタープライズ コール アンカリング

理解しておく必要のある Unified Mobility ダイヤル プランのもう一つの側面は、設定済みのリモート接続先電話機からの着信コールに対する自動発信者 ID 識別に関するシステム動作です。着信コールがシステムに入ると、そのコールに対して提供された発信者 ID が設定済みのすべてのリモート接続先電話機と比較されます。一致するものが見つかった場合は、そのコールが自動的にその会社のものと固定されるため、ユーザは通話切替機能を呼び出したり、通話中のコールをデスクトップフォンでピックアップすることができます。この動作は、着信コールがモバイル ボイス アクセスまたはエンタープライズ機能アクセスを使用したモビリティ コールとして開始されていない場合でも、モビリティ ユーザのリモート接続先電話機からの着信コールすべてに対して行われます。

（注）　設定済みのリモート接続先番号に対する自動着信コール発信者 ID 照合は、Matching Caller ID with Remote Destination サービス パラメータが Partial Match と Complete Match のどちらに設定されているかの影響を受けます。この設定に関する詳細については、「リモート接続先の設定と発信者 ID の照合」（P.25-23）を参照してください。

自動エンタープライズ コール アンカリングに加えて、設定済みのリモート接続先電話機から会社に電話がかかった場合の着信コール ルーティングと発信コール ルーティングも考慮する必要があります。設定済みのリモート接続先からのコールに対する着信コール ルーティングは、Inbound Calling Search Space for Remote Destination サービス パラメータの設定によって次の 2 つの方法のどちらかで発生します（「モバイル コネクトに関する Unified CM サービス パラメータ」（P.25-6）を参照）。デフォルトで、このサービス パラメータは、**Trunk or Gateway Inbound Calling Search Space** に設定されます。このサービス パラメータがデフォルト値に設定されている場合は、設定済みのリモート接続先からの着信コールが、公衆網ゲートウェイの着信コーリング サーチ スペース（CSS）またはコールが入るトランクを使用して経路設定されます。一方、Inbound Calling Search Space for Remote Destination パラメータが **Remote Destination Profile + Line Calling Search Space** に設定されている場合は、リモート接続先からの着信コールが、公衆網ゲートウェイの着信 CSS またはトランクをバイパスして、代わりに、リモート接続先プロファイル CSS（と回線レベル CSS の組み合せ）を使用して経路設定されます。

リモート接続先電話機からの着信コールの特性を考えると、このような着信コールへのアクセスを社内の電話機に到達させるために必要なすべてのパーティションに提供するためには、コーリング サーチ スペースが適切に設定されていることを確認する必要があります。これによって、リモート接続先電話機からの適切なコール ルーティングが保証されます。

（注）　設定済みのリモート接続先電話機からではない着信コールでは、必ず、トランクまたはゲートウェイ着信 CSS が使用されるため、Inbound Calling Search Space for Remote Destination サービス パラメータの影響を受けません。

モバイル ボイス アクセスまたはエンタープライズ機能アクセス コールの発信コール ルーティングでは、必ず、リモート接続先プロファイル回線 CSS とデバイス レベル CSS を連結したものが使用されるため、オフネットまたは公衆網アクセスに必要なすべてのルート パーティションへのアクセスを提供するためには、これらのコーリング サーチ スペースが適切に設定されていることを確認する必要があります。これによって、リモート接続先電話機からの適切な発信コール ルーティングが保証されます。

発信者 ID 変換

設定済みのリモート接続先番号によってクラスタに発信されたコールは、自動的に、発信者 ID または発番号が、発信元のリモート接続先電話機の番号から関連する会社のデスクトップフォンの番号に変更されます。たとえば、408 555-7890 という番号のリモート接続先電話機が設定され、555-1234 という番号の会社のデスクトップフォンに関連付けられている場合は、クラスタ内の任意の電話番号に向けられたユーザのリモート接続先電話機からのコールがすべて、自動的に、発信者 ID が 408 555-7890 のリモート接続先電話番号から 555-1234 の会社の電話番号に変更されます。これによって、アクティブ コールの発信者 ID 表示とコール履歴ログの発信者 ID に、ユーザの携帯電話の番号ではなく、会社の卓上電話の番号が反映され、すべての返信コールがユーザの会社の電話番号に対して発信され、このようなコールが会社に固定されることが保証されます。

同様に、リモート接続先電話機から外部の公衆網接続先へのコールと、モバイル ボイス アクセスやエンタープライズ機能アクセス 2 ステージ ダイヤリング経由で会社に固定されたコール、つまり、モバイル コネクトの結果として公衆網に分岐されたコールも、発信者 ID が発信元のリモート接続先電話機の番号から関連する会社の電話番号に変更されます。

最後に、発番号を会社の電話番号ではなく、会社の DID 番号として外部の公衆網電話機に供給する場合は、発信側のトランスフォーメーション パターンを使用できます。発信側のトランスフォーメーション パターンを使用して発信者 ID を会社の電話番号から会社の DID に変換することによって、外部の接続先からの返信コールは、完全な会社の DID 番号でダイヤルされていることから、その会社に固定されます。このような変換とダイヤル プランの意味については、「Cisco Unified Mobility 固有の考慮事項」（P.10-96）を参照してください。

Unified Mobility の保守とトラブルシューティング

Unified Mobility の機能と動作は、Cisco Unified CM 配置内の通常の方法を使用してトレースできます。モビリティ動作とコール フローが、他のコール フローと同様にさまざまなシステム トレースとログ ファイルに記録されます。さまざまな Unified Mobility 機能の全体的な正常性と使用状況をトレースするために、Real Time Monitoring Tool（RTMT）のパフォーマンス カウンタを使用できます。また、呼詳細レコードから、さまざまなモビリティ コール タイプに関する正確な情報が提供されます。

モバイル コネクト、エンタープライズ機能アクセス 2 ステージ ダイヤリング、およびデスクトップフォンとリモート接続先のピックアップ、シングル企業ボイスメール ボックス、通話切替機能などのその他の機能のコール フローと動作が、その他の通常のコール動作と同様に、Cisco CallManager サービスによって、SDI と SDL のシステム ログに記録されます。モバイル ボイス アクセス動作とコール フローは、Cisco Unified Mobile Voice Access サービスによって、ccmivr ログ ファイルに記録されます。ccmivr ファイルには、IVR プロンプトの要求、ダウンロード、および再生だけでなく、プロンプトに対する応答時のユーザ入力を含む、すべてのモバイル ボイス アクセス動作が記録されます。これ

らの機能に関するほとんどすべての情報が記録されることを保証するには、CM Service Group Cisco CallManager のサービス トレース レベルを Detailed に設定して、Cisco Unified Mobile Voice Access のサービス トレース レベルを Debug に設定する必要があります。

（注）　Detailed と Debug へのトレース レベルの設定によって、CPU の使用率が増加する可能性があります。このようなトレース レベルの設定は、問題を積極的に解決しなければならない場合にのみ使用してください。

RTMT ツールでは、次のパフォーマンス カウンタを表示して、Unified Mobility の正常性と使用状況を追跡できます。

Unified Mobility

- ¥Cisco Mobility Manager¥MobileCallsAnchored

  アクティブなモバイル コネクト、モバイル ボイス アクセス、エンタープライズ機能アクセス 2 ステージ ダイヤリング、またはリモート接続先からの着信コールが通話中で会社のゲートウェイに固定されるたびにインクリメントされます。このカウンタは、一定期間収集することによって、コール固定のピークを判断できます。

モバイル コネクト

- ¥Cisco Mobility Manager¥MobilityFollowMeCallsAttempted

  会社の電話番号へのコールがモバイル コネクト経由でリモート接続先に転送されるたびにインクリメントされます。

- ¥Cisco Mobility Manager¥MobilityFollowMeCallsIgnoredDueToAnswerTooSoon

  リモート接続先に転送されたモバイル コネクト コールが、最短応答タイマーが切れる前に応答されたことで、キャンセルされるたびにインクリメントされます（シングル企業ボイスメール ボックスの機能）。

モバイル ボイス アクセス

- ¥Cisco Mobility Manager¥MobilityIVRCallsAttempted

  モビリティ ユーザがモバイル ボイス アクセスを使用して電話をかけ、数字の 1（電話をかける意志を示す）、相手の電話番号、# 記号の順に入力するたびにインクリメントされます。

- ¥Cisco Mobility Manager¥MobilityIVRCallsSucceeded

  モバイル ボイス アクセスを使用してダイヤルされた電話機が呼び出されるたびにインクリメントされます。

- ¥Cisco Mobility Manager¥MobilityIVRCallsFailed

  モバイル ボイス アクセスを使用してダイヤルされた番号が、不正な番号入力または Cisco Unified CM 内の不十分なコール ルーティング パスが原因で呼び出しに失敗するたびにインクリメントされます。

Unified Mobility コールでは、システムとの間のその他のコールと同様に、呼詳細レコード（CDR）が生成されます。この呼詳細レコードを調査することによって、モビリティ コール フローの特性、コールの発信方法、およびコールの終了場所を判断できます。これによって、モビリティ コールの正確なコール アカウンティングが可能になります。次のガイドラインは、モビリティに関するコール レコードの評価に適用されます。

- リモート接続先でモバイル コネクト コールに応答した場合は、デフォルトで、呼詳細レコードの接続先番号フィールドに応答したリモート接続先の番号が表示されません。ただし、Show Line Group Member DN in finalCalledPartyNumber CDR Field Cisco Unified CM サービス パラメータが True に設定されている場合は、そのコールに応答したリモート接続先が CDR の接続先番号フィールドに表示されます。

- すべてのモバイル ボイス アクセスのコール フローに関する呼詳細レコードは、Mobility_IVR というコール タイプ指定でマークされ、モバイル ボイス アクセス コールごとに 1 つずつの呼詳細レコードが生成されます。
- エンタープライズ機能アクセス 2 ステージ ダイヤリングを使用して発信されたコールの場合は、2 つずつの呼詳細レコードが生成されます。一方の呼詳細レコードがユーザからエンタープライズ機能アクセス DID に発信された着信コールに対応し、もう一方の呼詳細レコードがモビリティ ユーザがダイヤルした番号に転送された発信コールに対応します。

表 25-3 に、一般的な設定上の問題または症状と問題ごとの解決策を示します。

表 25-3　一般的な設定上の問題のトラブルシューティング

一般的な問題または症状	解決策
ユーザがデスクトップフォンの Mobility ソフトキーを押すと、「You are not a valid Mobile Phone User」というメッセージが画面上に表示されます。	ユーザのデスクトップフォンの Owner User ID フィールドに適切なユーザ ID を設定します。
ユーザがデスクトップフォンの Mobility ソフトキーを押してリモート接続先ピックアップを実行した場合は、モバイル コネクト ステータスだけが表示され、「Send Call to Mobile Phone」は表示されません。	Remote Destination 設定画面で Mobile Phone チェックボックスがオンになっていることを確認してください。
ユーザがデスクトップフォンの Mobility ソフトキーを押してリモート接続先ピックアップを実行し、「Send Call to Mobile Phone」がオンになっている場合は、「Failed to send call to Mobile Phone」というメッセージが表示されます。	Remote Destination Profile 画面で、公衆網へのコールの経路設定を許可するように Rerouting Calling Search Space が設定されていることを確認してください。
モビリティ対応ユーザの会社の電話番号への着信コールは、そのユーザのリモート接続先に転送されません。	Remote Destination 設定画面： • Enable Mobile Connect チェックボックスがオンになっていることを確認します。 • 会社の電話番号に関する Line Association チェックボックスがオンになっていることを確認します。 • アクセス リストが設定されておらず、リモート接続先へのコールの転送が拒否されていることを確認します。 Remote Destination Profile 設定画面： • 公衆網へのコールの到達を許可する適切な CSS 再ルーティングが設定されていることを確認します。
ユーザが相手の電話番号と # をダイヤルしたときに、モバイル ボイス アクセス コールとエンタープライズ機能アクセス 2 ステージ ダイヤリング コールがファースト ビジー トーンを伴って失敗します。	Remote Destination Profile 画面で、公衆網へのコールの到達を許可する適切な Calling Search Space が設定されていることを確認します。

Unified Mobility に関するガイドラインと制約事項

次のガイドラインと制約事項は、Unified CM テレフォニー環境内のモバイル コネクトの配置と動作に関連して適用されます。

- モバイル コネクトは、PRI TDM 公衆網接続でだけサポートされます。T1 接続または E1-CAS、FXO、FXS、および BRI 公衆網接続はサポートされません。この PRI 要件は、完全な機能サポートを保証するためには、Cisco Unified CM で公衆網からの迅速な応答と切断の指示を受信する必要があることに基づいています。応答指示は、モバイル コネクト コールが特定のリモート接続先

で応答されたときに、Cisco Unified CM でデスクトップフォンとその他のリモート接続先の呼び出しを停止するために必要です。加えて、応答指示は、シングル企業ボイスメール ボックス機能をサポートするために必要です。最後に、切断指示はデスクトップフォンピックアップのために必要です。PRI 公衆網接続では、必ず、応答指示または切断指示が提供されます。

- Cisco IOS Unified Border Element によって Unified CM SIP トランクとサービス プロバイダー トランクとの間に境界ポイントが提供されており、通話切替機能（またはその他の DTMF 依存の機能）が使用されていない場合には、SIP トランク VoIP 公衆網接続でもモバイル コネクトがサポートされます。VoIP 公衆網接続では、通話切替機能はサポートされません。VoIP ベースの公衆網接続では、VoIP ベースの公衆網接続によって提供されるエンドツーエンドのシグナリング パスによって、Unified CM に迅速な応答と切断の指示を提供できます。
- モバイル コネクトでは、ユーザあたり最大 2 つの同時コールをサポートできます。それ以上の着信コールは、自動的に、ユーザのボイスメールに転送されます。
- モバイル コネクトは、Multilevel Precedence and Preemption（MLPP）と連動しません。コールが MLPP によって割り込まれた場合は、そのコールに対するモバイル コネクト機能が無効になります。
- モバイル コネクト サービスでは、ビデオ コールに応答できません。デスクトップフォンで受信されたビデオ コールは携帯電話でピックアップできません。
- Unified CM の Forced Authorization Code（FAC; 強制承認コード）機能と Client Matter Code（CMC; クライアント識別コード）機能が、モバイル ボイス アクセスと連動しません。
- リモート接続先は、別のクラスタまたはシステム上の時分割多重（TDM）装置またはオフシステム IP 電話にする必要があります。IP 電話は、リモート接続先と同じ Unified CM クラスタ内に設定できません。

ガイドラインと制約事項の詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Features and Services Guide*』の最新版で Cisco Unified Mobility に関する情報を参照してください。

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

Cisco Unified Mobility の性能と容量

Cisco Unified Mobility では、次の容量がサポートされます。

- MCS-7845 サーバを使用したクラスタあたり最大 15,000 人のモビリティ対応ユーザ
- MCS-7835 サーバを使用したクラスタあたり最大 10,000 人のモビリティ対応ユーザ
- MCS-7825 サーバを使用したクラスタあたり最大 4,000 人のモビリティ対応ユーザ
- MCS-7845 ノードあたり最大 3,750 台のリモート接続先またはクラスタあたり 15,000 台のリモート接続先
- MCS-7835 ノードあたり最大 2,500 台のリモート接続先またはクラスタあたり 10,000 台のリモート接続先
- MCS-7825 ノードあたり最大 1,000 台のリモート接続先またはクラスタあたり 4,000 台のリモート接続先

（注）　モビリティ対応ユーザは、リモート接続先プロファイルを持ち、1 つ以上のリモート接続先が設定されているか、単にモビリティ ID が設定されているだけのユーザとして定義されます。

サポートされるモビリティ対応ユーザの最大数は、ユーザごとに設定されたリモート接続先またはモビリティ ID の数に依存します。前述したモビリティ対応ユーザの最大数は、ユーザあたり 1 つのリモート接続先またはモビリティ ID を想定しています。ユーザあたりのリモート接続先数またはモビリティ ID 数が増加するほど、サポートされるモビリティ対応ユーザ数が減少します。

（注）　モビリティ ID は、システム内のリモート接続先と同様に設定され、リモート接続先と同じ容量になります。ただし、リモート接続先と違って、モビリティ ID は、リモート接続先プロファイルではなく、直接電話機に関連付けられます。モビリティ ID は、デュアルモードの電話機と Cisco Unified Mobile Communicator クライアントにのみ適用されます。

上の数字が最大容量です。ただし、結果的に、Cisco Unified Mobility のスケーラビリティと性能は、モビリティ ユーザ数、ユーザごとのリモート接続先数またはモビリティ ID 数、およびそれらのユーザの Busy Hour Call Attempt（BHCA）レートに依存します。ユーザあたりの複数のリモート接続先またはユーザあたりの高い BHCA によって、Cisco Unified Mobility の容量が減少します。確実に適切なサイジングを行うには、Cisco Unified Communications Sizinig Tool（Unified CST）を使用して、適切な Unified Mobility の容量とシステム全体の容量を決定します。Unified CST は、次の URL（適切なログイン アカウントが必要）で入手できます。

http://tools.cisco.com/cucst

Unified Mobility を配置するための設計上の推奨事項

Unified Mobility を配置する場合は、次の設計上の推奨事項に従ってください。

- 公衆網ゲートウェイ プロトコルで、アウトオブバンド DTMF リレーが使用できる、または、インバンド DTMF をアウトオブバンド DTMF に変換するためのメディア ターミネーション ポイント（MTP）が割り当てられていることを確認します。公衆網接続用の Cisco IOS ゲートウェイを使用している場合は、アウトオブバンド DTMF リレーがサポートされます。ただし、サードパーティ製ゲートウェイでは、一般的なアウトオブバンド DTMF 方式がサポートされない可能性があるため、結果として、MTP が必要になる場合があります。エンタープライズ機能アクセス 2 ステージ ダイヤリング機能と通話切替機能を使用するには、Cisco Unified CM で DTMF 番号をアウトオブバンドで受信する必要があります。

  （注）　インバンド DTMF をアウトオブバンド DTMF に変換するために MTP 上でリレーする場合は、十分な MTP 容量が提供されることを確認してください。エンタープライズ機能アクセス 2 ステージ ダイヤリングまたは通話切替機能の高い使用頻度が予想される場合は、ハードウェア ベースの MTP または Cisco IOS ソフトウェア ベースの MTP をお勧めします。

- Unified Mobility を配置する前に、公衆網プロバイダーと連携して次のことを保証する必要があります。
  - 会社へのすべての着信コールに関する発信者 ID が、サービス プロバイダーから供給される。これは、エンタープライズ機能アクセス 2 ステージ ダイヤリングまたは通話切替転送、会議、およびダイレクト コール パーク機能が必要な場合の要件です。
  - 発信コールの発信者 ID は、サービス プロバイダーに制限されない。これは、モビリティ対応ユーザが、一般的な会社のシステム番号やその他の意味のない発信者 ID ではなく、リモート接続先にいる元の発信者の 発信者 ID を受信することが期待される場合の要件です。

（注）　プロバイダーによっては、トランク上の発信コールの発信者 ID が、そのトランクで処理される DID に制限される場合があります。そのため、発信者 ID が制限されない別の PRI トランクをプロバイダーから入手する必要があります。無制限の PRI トランクを要求すると、プロバイダーによっては、このトランク経由で緊急電話番号にコールを送信または発信しないことが記された署名付きの同意書を要求される場合があります。

（注）　プロバイダーによっては、[Redirected Dialed Number Identification Service (RDNIS)] フィールドまたは SIP の Diversion ヘッダーにトランクで処理される DID が含まれている限り、そのトランクには発信コールの発信者 ID を無制限で許可します。Cisco Unified CM 7.1(3) 以降は、ゲートウェイまたはトランクの設定ページで [Redirecting Number IE Delivery] > [Outbound] チェックボックスをオンにすることによって、リモート接続先に分岐されたコールの RDNIS または SIP の Diversion ヘッダーにユーザの企業番号を取り入れることができます。RDNIS または SIP の Diversion ヘッダーに対応し、発信コールの発信者 ID を無制限で許可しているかどうかは、サービス プロバイダーに問い合わせてください。

- 一般に、モビリティ コール フローには複数の公衆網コール レッグが含まれるため、Unified Mobility にとって公衆網ゲートウェイ リソースの計画と配置が極めて重要です。モビリティ対応ユーザ数が多い場合は、公衆網ゲートウェイ リソースを増やす必要があります。公衆網利用を制限または削減するために、次の方法が推奨されています。
  - モビリティ対応ユーザあたりのリモート接続先数を 1 つに制限します。これによって、着信コールをユーザのリモート接続先に転送するために必要な DS0 数が削減されます。コールがユーザの会社の電話番号に送られると、そのコールがリモート接続先のいずれかで応答されなくても、設定済みのリモート接続先ごとに 1 つずつの DS0 が消費されます。コールがリモート接続先で応答されなくても、リモート接続先あたり 1 つの DS0 が 10 秒間も使用される可能性があります。
  - アクセス リストを使用して、着信コールの発信者 ID に基づいて、特定のリモート接続先へのコールの拡張を拒否または制限します。現在は、時刻に基づいてアクセス リストを呼び出すことができるため、これによって、エンド ユーザまたは管理者がアクセス リストを頻繁に更新する必要がなくなります。
  - 不要になったモバイル コネクトを無効にしたり、会社の番号に電話がかけられた場合の DS0 の使用をさらに制限するようにエンド ユーザを教育します。モバイル コネクトが無効になっている場合は、着信コールでデスクトップフォンの呼出音が鳴りますが、誰も電話に出なければ、そのコールが会社のボイスメールに転送されます。
- ロケーション間の WAN 帯域幅の不足によってコール アドミッション制御が拒否される可能性と、デスクトップフォンのピックアップまたはリモート接続先のピックアップによって WAN 帯域幅のオーバーサブスクリプションが発生する可能性があるため、リモート接続先プロファイル CSS と CSS の再ルーティングを設定して、CSS 内のルート パターンが、着信コール レッグが到達するゲートウェイと同じコール アドミッション制御ロケーション内に配置されたゲートウェイを指すようにすることをお勧めします。詳細については、「リモート接続先プロファイルの設定」（P.25-26）を参照してください。

Cisco Unified Mobile Communicator

Cisco Unified Mobile Communicator は、携帯電話から Cisco Unified Communications アプリケーションにアクセスし、利用する機能をユーザに提供するモビリティ ソリューションです。Cisco Unified Mobile Communicator および Cisco Mobile グラフィカル クライアントは、Cisco Unified Mobility Advantage ソフトウェアを実行しているサーバと連動して、携帯電話の機能をアクセスおよび制御するためのリッチ ユーザ インターフェイスを提供します。このシステムは既存の社内 LDAP ディレクトリに統合されるため、ユーザはすべてのデバイス上で単一のクレデンシャル セットを使用できます。また、Unified Mobile Communicator と Unified Mobility Advantage 間のすべてのトラフィックが、Secure Socket Layer（SSL）プロトコルによって保護されます。Unified Mobile Communicator は、携帯電話ユーザに次の機能を提供します。

- 社内および個人ディレクトリへのアクセス
- プレゼンスとバディの会社との同期化
- 社内ボイスメールへのビジュアル アクセス
- デスクトップフォンの不在コール、発信コール、および受信コールの履歴確認
- セキュア Store-and-Forward テキスト メッセージング
- 会議通知の受信
- Cisco Unified CM を使用した Dial-via-office

（注）　上記に記載されている機能が、サポート対象のすべてのハンドセットまたはモバイル オペレーティング システムで利用できる機能のすべてではありません。

Cisco Unified Mobile Communicator の電話サポートとデータ プラン要件

Cisco Unified Mobile Communicator クライアント アプリケーションはさまざまなモバイル デバイスで動作しますが、その洗練された機能性によって、サポートされる電話機が制限されるようなデバイス要件が最小限に抑えられています。

Cisco Unified Mobile Communicator 7.*x* は、次のモバイル オペレーティング システムまたはハンドセットで実行するように設計されています。

- Windows Mobile 6.0 または 6.1 Standard
- Nokia Symbian および Nokia S60 Third Edition（Nokia ハンドセット）
- ファームウェア バージョン 3.0.1 以降が実行されている Apple iPhone 3G または 3GS（iPhone ハンドセット）
- Research In Motion（RIM）Blackberry（Blackberry ハンドセット）

（注）　iPhone および Blackberry デバイス対応の Cisco Unified Mobile Communicator クライアントは、Cisco Mobile と呼ばれています。

ハンドセット モデルのサポートは、モバイル オペレーティング システム（OS）によって異なりますが、特定のハンドセット サポート認証は必要ありません。各モバイル OS について、シスコでは最低限の要件をサポートするハンドセットを必要とします。これらの要件はモバイル OS ごとに異なりますが、次のリストにハンドセットがサポート対象となるための一般的な要件を示します。

- モバイル OS の特定のバージョン（OS ごとに異なる）
- 特定のフォーム ファクタ、スクリーン サイズ、およびキーボード テクノロジー（オペレーティング システムごとに異なる）
- 認定された認証局（VeriSign または GeoTrust）からのルート認証のインストール
- サードパーティ アプリケーションのインストールまたは実行に対する制限なし

（注）　実際のユーザ エクスペリエンスはデバイスによって異なる可能性があります。

特定のハンドセット要件の詳細については、次の Web サイトで入手可能な『*Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator*』を参照してください。

http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html

サポートされているデバイスの提供に加えて、ユーザは、サポートされているデータ プランでそのデバイスを使用する必要があります。クライアントは、General Packet Radio Service（GPRS; 汎用パケット無線サービス）や Universal Mobile Telecommunications System（UMTS; ユニバーサル移動体通信システム）などの Mobile Data Network（MDN; モバイル データ ネットワーク）を使用して、Cisco Unified Mobility Advantage サーバと通信します。クライアントとサーバは SSL を使用してすべてのデータ トラフィックを保護しますが、クライアントは、Unified Mobility Advantage 管理者がインストール中に指定したポート上の MDN を使用してサーバとの接続を開始します。

このポートが従来と異なる可能性があるため、クライアントは、MDN に無制限プランでアクセスできる必要があります。それに反して、多くのオペレータは、クライアントにポート 80 上の HTTP アクセスのみを許可するローエンドの「Web 専用」プランを提供します。この種のプランは、Unified Mobile Communicator と互換性がないため、機能しない可能性があります。代わりに、ユーザは、クライアントからサーバ上の任意のポートへの任意の TCP トラフィックを許可するプランに加入する必要があります。このプランは、VPN プランと呼ばれることがあります。ただし、Unified Mobility Advantage サーバが動的で変換済みのアドレスを適切にマップするため、クライアントはルーティング可能な IP アドレスや固定 IP アドレスを必要としません。

Cisco Unified Mobile Communicator クライアントはすべてのアプリケーション統合と機能を会社へのデータ接続に依存しているため、このデータ接続が極めて重要です。この重要な接続で消費される帯域幅には、かなりのばらつきがあります。これらの接続のさまざまな特性を考えると、分単位やバイト単位のプランではなく、無制限のデータ プランを強くお勧めします。ただし、配置によっては、無制限のデータ プランに非常に多くのコストがかかる場合があります。帯域幅を見積もって計画する目的でシスコが行った調査によれば、Unified Mobile Communicator ユーザは、ビジュアル ボイスメール機能を使用しなければ、月平均で、約 5.6 MB の帯域幅を消費します。もちろん、帯域幅の消費は、エンドユーザの振る舞いによって大きく異なります。たとえば、大量のディレクトリ ルックアップを実行したり、大量のテキスト メッセージを送信したり、大量の Dial-via-office コールを発信したりするユーザは、このような機能をほとんど使用しないユーザよりも広い帯域幅を消費します。したがって、5.6 MB/月という平均値はほとんど参考になりません。ビジュアル ボイスメールを使用した場合は、1 分間のボイルメール メッセージで約 354 kb が消費されます。つまり、約 2 時間のビジュアル メッセージでこの月平均のすべてが消費される計算です。このことから、ビジュアル ボイスメールの使用中は帯域幅の要求が異常に高くなることが容易にわかります。

Cisco Unified Mobile Communicator と Cisco Unified CM の統合

Cisco Unified Mobile Communicator ソリューションでのエンタープライズ コール ログ統合、Dial-via-office 機能、および Unified Mobility 統合をサポートするには、Cisco Unified Mobility Advantage サーバを Unified CM に統合する必要があります。これには、管理者が Unified CM に対していくつかの設定手順を実行する必要があります。エンタープライズ コール ログ統合では、Cisco Unified CM 内でアプリケーション ユーザ アカウントを設定して、Unified Mobile Communicator ユーザのデスクトップフォンをそのアカウントに関連付ける必要があります。このアカウントは、Unified Mobility Advantage サーバですべての Unified Mobile Communicator ユーザのデスクトップフォンを監視して、不在コール、受信コール、および発信コールを収集するために使用されます。アプリケーション ユーザ アカウント数は最大 250 台の監視対象デバイスに制限され、Unified Mobility Advantage サーバの設定によって最大 4 つのアカウント名が許可されるため、最大 1,000 人のユーザが利用できます。Cisco Unified CM 内の各アプリケーション ユーザ アカウントを Standard CTI End Users グループと Standard CTI Enabled グループの両方に割り当てる必要があります。

Dial-via-office 機能と Unified Mobility との統合では、各ユーザの Unified Mobile Communicator デバイスを Cisco Unified CM 内のデバイスとして設定し、このデバイスにユーザの会社の電話番号（ユーザのデスクトップフォンと同じ電話番号）を設定して、ユーザの携帯電話の GSM 番号に設定されたモビリティ ID をこのデバイスに関連付ける必要があります。

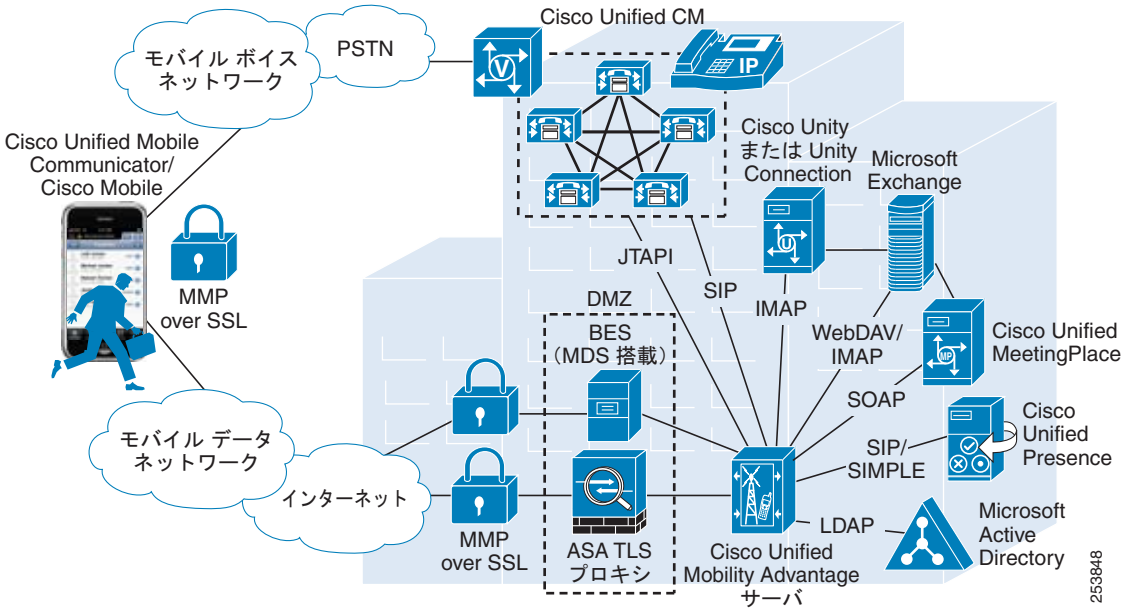
エンタープライズ コール ログ統合、Dial-via-office、および Unified Mobility 統合の設定手順を含む、Unified CM との統合の詳細については、次の Web サイトで入手可能な Cisco Unified Mobility Advantage のインストールおよび設定マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps7270/prod_installation_guides_list.html

Cisco Unified Mobile Communicator のアーキテクチャ

このソリューションは、Cisco Unified Mobile Communicator、Adaptive Security Appliance (ASA) TLS プロキシ、および Cisco Unified Mobility Advantage サーバという主要な 3 つのコンポーネントで構成されています（図 25-11 を参照）。図 25-11 に示すように、Cisco Unified Mobility Advantage サーバは既存の Unified Communications アプリケーションおよび企業システムにアクセスします。

図 25-11　Cisco Unified Mobile Communicator のアーキテクチャ



モバイル デバイス上で Unified Mobile Communicator が起動するとユーザ セッションが開始されます。アプリケーションが開始すると、Microsoft Active Directory パスワードの入力が要求されます（プロビジョニング中にデバイスがユーザ アカウントに関連付けられるため、クライアントはユーザ ID を収集する必要がありません）。次に、クライアントが、Mobile Data Network を使用して ASA TLS プロキシへの SSL 接続を開始します。この接続は、インターネットからの着信接続としてプロキシで検出されます。この接続に使用されるプロトコルは、Mobility Multiplexing Protocol（MMP）です。このプロトコルは、ハンドセットのバッテリ寿命を節約するように最適化されています。MMP プロトコルは、標準ベースの SSL パケットにカプセル化されます。

SSL 接続が確立されると、ASA から Unified Mobility Advantage サーバに要求が渡され、そこでユーザが LDAP ディレクトリに対して認証されます。SSL トラフィックを運搬する TCP 接続はクライアントによって維持されるため、サーバはアドレス変換や動的クライアント アドレスなどに関係なく、トラフィックをクライアントに委ねることができます。クライアントの接続期間を通して、ASA TLS プロキシがクライアントからの着信パケットを復号し、厳格なパケット検査を実施してパケットが有効で許可されたユーザからのものであることを保証します。検査に合格したパケットは、ASA プロキシが再び暗号化して、Cisco Unified Mobility Advantage サーバに渡します。

Unified Mobile Communicator クライアント ユーザを認証するための LDAP クレデンシャルの使用に加えて、Unified Mobility Advantage サーバでもその他のバックエンド アプリケーション システムに接続するためにクレデンシャルが使用されます。たとえば、Microsoft Exchange サーバにユーザとして接続し、カレンダー、個人連絡表、および会議通知にアクセスするためにこの情報が使用されます。

ASA を TLS プロキシとファイアウォールの両方として配置するか、ASA を DMZ 内の TLS プロキシとしてだけ配置して外部ファイアウォールに依存するかに関係なく、2 つのポートを設定して、それらを外向きのファイアウォールまたはインターフェイス（インターネットと DMZ 間）と内向きのファイアウォールまたはインターフェイス（DMZ と会社間）の両方に対して開く必要があります。外部と内部の両方のファイアウォールに対して、次の一連の範囲に含まれるポートを開く必要があります。

- 外部ファイアウォール ポート
  - 5400 ～ 5500 の範囲のクライアント接続ポート（TCP/SSL）
  - 9000 ～ 9100 の範囲のプロビジョニング ポート（HTTP）
- 内部ファイアウォール ポート
  - 5400 ～ 5500 の範囲のクライアント接続ポート（TCP/SSL）
  - 9000 ～ 9100 の範囲のプロビジョニング ポート（HTTP）

（注）　デフォルトのクライアント接続ポート（TCP/SSL）は 5443 で、デフォルトのプロビジョニング ポート（HTTP）は 9080 です。

（注）　iPhone または Blackberry ハンドセットだけを配置している場合、これらのハンドセットはプロビジョニング ポートを介して Cisco Unified Mobile Communicator クライアントをダウンロードしないため、ファイアウォールのプロビジョニング ポートを開く必要はありません。このクライアントは、iPhone ハンドセットの場合は Apple App Store からダウンロードされ、Blackberry ハンドセットの場合は Blackberry Enterprise Server（BES）を介してハンドセットにプッシュされます。

Microsoft Active Directory（AD）環境では、LDAP サーバに関するサーバ固有の要件はありません。適切なドメインに属していればどのドメイン コントローラも動作します。Unified Mobility Advantage サーバからこのサーバに対して LDAP バージョン 3 の認証および検索要求が発行され、予期したとおりに AD ドメイン経由で伝播されます。Exchange サーバが複数存在する環境では、Cisco Unified Mobility Advantage サーバが AD に問い合せてユーザごとの適切なサーバを決定します。

Cisco Unified Mobile Communicator の機能

Cisco Unified Mobile Communicator は、ユーザが社外からモバイル デバイスを使用して社内のさまざまな Unified Communications アプリケーションにアクセスして利用できるようにします。次の企業アプリケーションを Unified Mobile Communicator ソリューションに統合できます。各アプリケーションからは後述するような機能が提供されます。

Cisco Unified Mobile Communicator ソリューションと統合できるサポート対象のアプリケーションおよびバージョンの全リストについては、次の Web サイトで入手可能な『*Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator*』を参照してください。

http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html

LDAP ディレクトリ

Cisco Unified Mobility Advantage サーバと Microsoft Active Directory が統合されます。Unified Mobile Communicator クライアント接続の認証に Active Directory が使用されるため、この統合が必要になります。ユーザの Active Directory アカウント パスワードが Cisco Unified Mobility Advantage サーバまたは Unified Mobile Communicator クライアントに保存されることはありません。クライアン

トの認証メカニズムの提供に加えて、クライアントからのディレクトリ ルックアップを解決し、ユーザがモバイル デバイスから社内ディレクトリを検索できるようにするためにも Active Directory が使用されます。図 25-11 に示すように、Active Directory との統合は LDAP 経由で行われます。

Cisco Unified CM

Cisco Unified Mobility Advantage サーバと Cisco Unified CM を統合することで、デスクトップフォン コール ログの同期化、Dial-via-office 機能、および Unified Mobility 統合を提供できます。

デスクトップフォンのコール ログ統合

コール ログ統合を有効にされた Unified Mobile Communicator ユーザは、Unified Mobile Communicator クライアント上でデスクトップフォンからのコール履歴リスト（不在コール、発信コール、および着信コール）を確認できます。

図 25-11 に示すように、Unified Mobility Advantage サーバと Unified CM の間で JTAPI 接続が確立されます。この JTAPI 接続では、CTI を使用してユーザのデスクトップフォンのプライマリ回線に対する着信コールと発信コールが監視されます。コール ログは、デスクトップフォンから Unified Mobile Communicator クライアントの方向にのみ同期化されることに注意してください。Unified Mobile Communicator クライアントからデスクトップフォンの方向には同期化されません。

Dial-via-office

Dial-via-office 機能を使用すれば、Cisco Unified CM テレフォニー インフラストラクチャと会社の公衆網ゲートウェイを使用して、Cisco Unified Mobile Communicator クライアントを実行している携帯電話からコールを開始できます。図 25-11 に示すように、この機能は、Unified Mobility Advantage サーバと Unified CM 間の SIP 接続上の SIP シグナリングによって実現されます。

Unified Mobile Communicator ユーザが携帯電話から発信したすべてのコールに対して、Unified Mobility Advantage 管理者が Dial-via-office の使用を命令することができます。ただし、設定されている緊急番号または直接通話番号へのコールでは、Dial-via-office 命令が無視されます。管理者は、Unified Mobile Communicator ユーザに、Dial-via-office 機能を使用するかどうかといつ使用するかを決めさせることもできます。このとき、エンド ユーザは、コール（モバイル ボイス ネットワークに送信される設定済みの緊急電話番号または直接通話番号へのコール以外）の発信時に必ず Dial-via-office を使用する、または、コールごとにプロンプトを出力するように電話機を設定することができます。

Cisco Unified Mobile Communicator ソリューションでサポートされている Dial-via-office には、次の 2 つのタイプがあります。

- 「Dial-via-office リバース コールバック」（P.25-39）
- 「Dial-via-office 転送」（P.25-40）

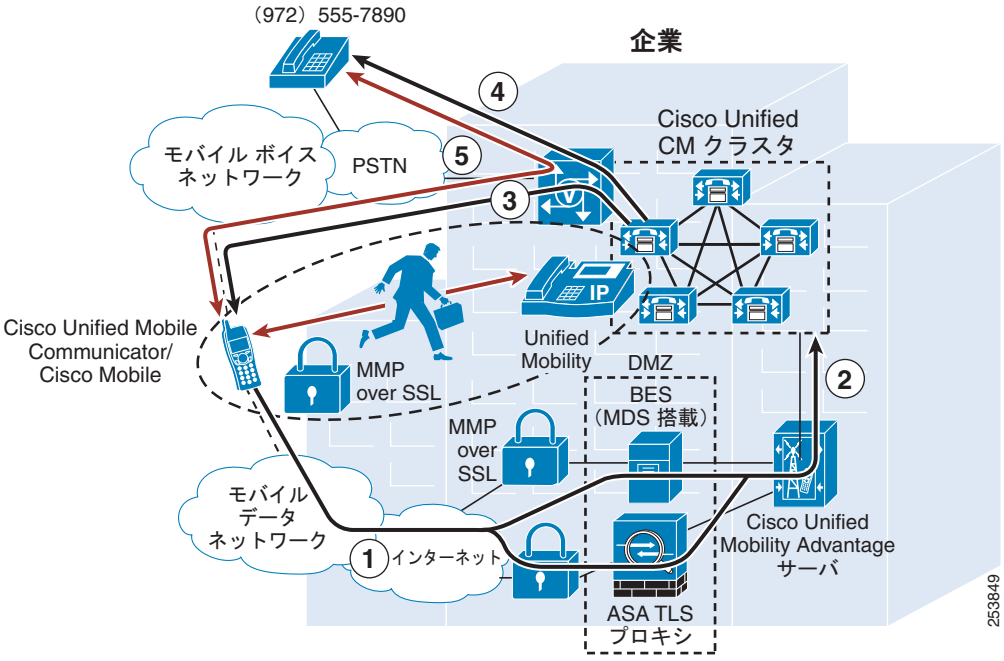
Dial-via-office リバース コールバック

図 25-12 に、Dial-via-office リバース コールバックのコール フローを示します。この例では、Unified Mobile Communicator ユーザが、公衆網電話機（972-555-7890）に電話をかけようとしています。ユーザが、番号をダイヤルするか、コンタクト リストまたはディレクトリ リストから番号を選択すると、会社と Cisco Unified Mobility Advantage サーバへのデータ接続上で SIP INVITE が生成されます（ステップ 1）。この SIP INVITE は、MMP プロトコルにカプセル化され、クライアントと Cisco Unified Mobility Advantage サーバ間の（クライアント タイプに応じて）ASA または BES サーバ経由のセキュアな接続によって送信されます。この要求は、SIP 接続経由で Cisco Unified Mobility Advantage サーバから Cisco Unified CM に転送されます（ステップ 2）。次に、Unified CM によって、会社の公衆網ゲートウェイを使用して、ユーザの携帯電話番号へのコールバックが生成されます（ステップ 3）。Unified CM からの着信コールがモバイル デバイスで自動応答されると、ユーザが呼び出した番号または選択した番号にコールが転送されます（ステップ 4：この場合は 972-555-7890）。コー

ルが遠端で応答されると、会社の公衆網ゲートウェイでコールが固定されます（ステップ 5）。コールが会社のゲートウェイに固定されたため、ユーザは、このコール中の任意の時点で Unified Mobility のデスクトップフォン ピックアップ機能を使用したり、Unified Mobility の通話切替機能を呼び出すことができます。

（注）　ユーザの携帯電話からのすべての音声またはメディアは、必ずモバイル ボイス ネットワーク上を通過します。メディアが会社へのデータ接続を通過することはありません。モバイル データ ネットワーク接続は、コール シグナリング トラフィックとその他のアプリケーションの相互作用以外には使用されません。

図 25-12　Cisco Unified Mobile Communicator、Dial-via-office リバース コールバック



Cisco Unified Mobile Communicator に Dial-via-office リバース コールバック機能が搭載されたほか、Unified Mobile Communicato クライアント設定内でコールバック先の代替番号を指定するオプションも追加されました。たとえば、コールバックを携帯電話で受信するのではなく、会議室の電話に転送することができます。

（注）　Dial-via-office リバース コールバック機能の呼び出し時に、Unified CM からのコールバックがユーザ指定の代替番号に転送された場合は、そのコールをデスクトップフォンでピックアップしたり、通話切替機能を呼び出すことはできなくなります。

Dial-via-office リバース コールバックは、Windows Mobile、Nokia、および Blackberry のモバイル ハンドセットでサポートされています。

Dial-via-office 転送

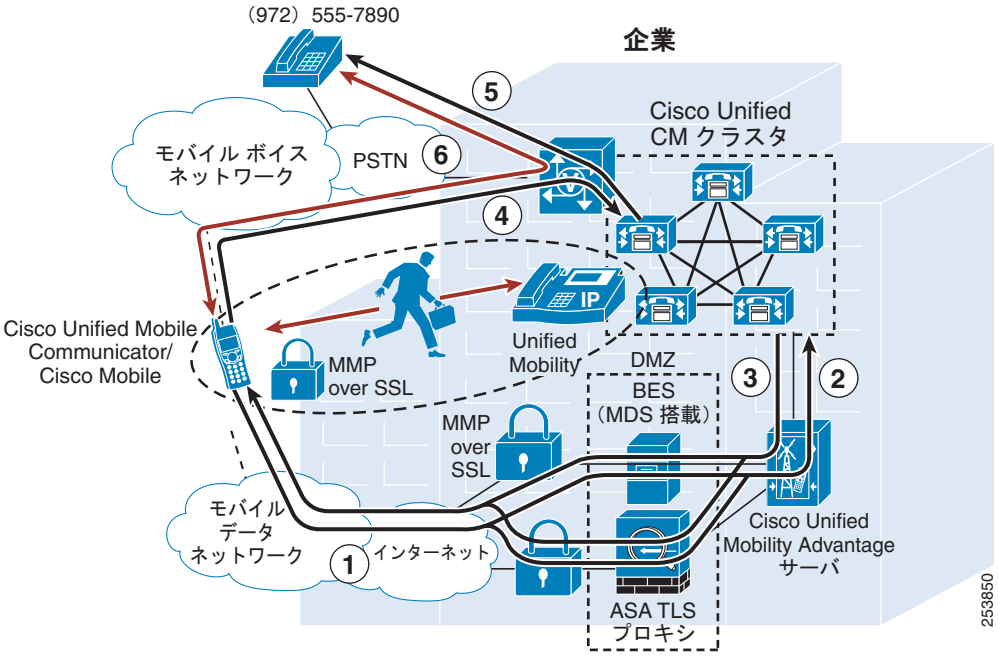
図 25-13 に、Dial-via-office 転送のコール フローを示します。この例では、Unified Mobile Communicator ユーザが、公衆網電話機（972-555-7890）に電話をかけようとしています。ユーザが、番号をダイヤルするか、コンタクト リストまたはディレクトリ リストから番号を選択すると、会社と Cisco Unified Mobility Advantage サーバへのデータ接続上で SIP INVITE が生成されます（ステッ

プ 1）。この SIP INVITE は、MMP プロトコルにカプセル化され、クライアントと Cisco Unified Mobility Advantage サーバ間の（クライアント タイプに応じて）ASA または BES サーバ経由のセキュアな接続によって送信されます。この要求は、SIP 接続経由で Cisco Unified Mobility Advantage サーバから Cisco Unified CM に転送されます（ステップ 2）。次に Unified CM から、設定されているシステム全体のエンタープライズ機能アクセス番号を使用して Cisco Unified Mobility Advantage サーバに応答があり、そこから（クライアント タイプに応じて）ASA または BES サーバ経由のセキュアな接続によってユーザのモバイル デバイスに転送されます（ステップ 3）。モバイル デバイスで番号が受信されると、Cisco Unified Mobile Communicator クライアントは、モバイル デバイスからエンタープライズ機能アクセス番号へのコールを自動的に発信します（ステップ 4）。Unified CM でこのコールが受信されると、ユーザに設定されたモビリティ ID に対して着信コールの発信者 ID が照合されます。着信コールの発信者 ID がユーザに設定されたモビリティ ID と一致すると、システムから、ユーザがダイヤルまたは選択した番号にコールが発信されます（ステップ 5。この場合は 972-555-7890）。コールが遠端で応答されると、会社の公衆網ゲートウェイでコールが固定されます（ステップ 6）。コールが会社のゲートウェイに固定されたため、ユーザは、このコール中の任意の時点で Unified Mobility のデスクトップフォン ピックアップ機能を使用したり、Unified Mobility の通話切替機能を呼び出すことができます。

（注）　Dial-via-office 転送コールを正常に実行するには、Unified CM で公衆網ネットワークから受信する着信コールの発信者 ID が、Dial-via-office コールを発信する Unified Mobile Communicator デバイスに設定されたモビリティ ID 番号と一致する必要があります。公衆網から着信コールの発信者 ID が送信されない、あるいはその発信者 ID がユーザに設定されたモビリティ ID と一致しない場合、Dial-via-office 転送コールは失敗します。

（注）　ユーザの携帯電話からのすべての音声またはメディアは、必ずモバイル ボイス ネットワーク上を通過します。メディアが会社へのデータ接続を通過することはありません。モバイル データ ネットワーク接続は、コール シグナリング トラフィックとその他のアプリケーションの相互作用以外には使用されません。

図 25-13　Cisco Unified Mobile Communicator、Dial-via-office 転送



（注）　バージョン 3.1 よりも前の iPhone ファームウェアでは、Dial-via-office コールは自動的に完了せず、ユーザが手動で操作してコールを完了する必要があります。図 25-13 のステップ 3 で、ユーザに対してクライアントにダイアログボックスが表示されます。ステップ 4 でエンタープライズ機能アクセス番号へのコールを発信するには、ユーザは [Call] を選択する必要があります。

Cisco Unified Mobile Communicator から、Dial-via-office 転送コール用に Unified CM によって送信されるエンタープライズ機能アクセス番号にダイヤルできるようにするには、送信される番号が完全な E.164 番号であり、モバイル ボイス ネットワークを介してダイヤルできることが必要です。Unified CM 内の [Enterprise Feature Access Directory Number] フィールド（[Call Routing] > [Mobility Configuration] の下）で設定された番号が完全な E.164 番号ではない場合、管理者は、Cisco CallManager サービスの Dial-via-Office Forward Service Access Number サービス パラメータに、Unified CM 内で設定されたエンタープライズ機能アクセス ディレクトリ番号に対応する完全な E.164 番号を設定する必要があります。[Dial-via-Office Forward Service Access Number] サービス パラメータが設定されていないと、Unified CM から、設定されたエンタープライズ機能アクセス番号がそのまま送信されます。この番号は完全な E.164 番号ではないため、Cisco Unified Mobile Communicator から Unified CM システムへのコール（図 25-13 のステップ 4）は失敗し、Dial-via-office 転送機能は動作不能になります。

たとえば、エンタープライズ機能アクセス ディレクトリ番号が Unified CM 内で 51234 として設定されているとします。[Dial-via-Office Forward Service Access Number] が設定されていない場合、Unified CM はそのエンタープライズ機能アクセス番号 51234 を Unified Mobility Advantage に転送し、その結果、Unified Mobile Communicator デバイスのコール ダイアログに 51234 と表示されます。ユーザが [Call] オプションを選択すると、電話機からモバイル ボイス ネットワークを介して 51234 へのコールが試行されますが、このコールは失敗します。ただし、[Dial-via-Office Forward Service Access Number] が 9195551234 と設定されている場合には、Unified CM から Unified Mobility Advantage にエンタープライズ機能アクセス番号 9195551234 が転送されます。これにより、ユーザが [Call] オプションを選択すると、コールは適切にモバイル ボイス ネットワークと公衆網を介して企業にルーティングされます。

Dial-via-office 転送は、Cisco Mobile、つまり iPhone および Blackberry 対応の Cisco Unified Mobile Communicator クライアントでサポートされています。

Unified Mobility の統合

コール ログ統合と Dial-via-office のための Unified CM との統合に加えて、Unified Mobile Communicator ユーザは、Unified Mobility と統合してモバイル コネクトを利用できます。これによって、ユーザの会社の電話番号への着信コールを携帯電話に転送できるようになります。以前のバージョンの Unified CM と違って、Unified CM 7.*x* 以降のリリースでの Cisco Unified Mobile Communicator クライアントと Unified Mobility の統合は、Unified CM 内で Cisco Unified Mobile Communicator デバイスに直接関連付けられた設定済みのモビリティ ID を経由して実現されます。以前のバージョンの Unified CM では、Unified Mobile Communicator クライアントが、リモート接続先プロファイルに関連付けられたリモート接続先を経由して Unified Mobility と統合されました。Unified CM 内のモビリティ ID の設定は、リモート接続先と同じです。また、リモート接続先番号と発信者 ID の照合の設定に関するガイドライン（「リモート接続先の設定と発信者 ID の照合」（P.25-23）を参照）がすべて、モビリティ ID の設定にも適用されます。Unified Mobile Communicator 7.*x* クライアント インターフェイス内でユーザは、[General] 設定メニューで [Moblie Connect (Single Number Reach)] を有効または無効にすることができます。

Cisco Unified Presence

Unified Mobile Communicator ユーザが企業ネットワークに対して自分のプレゼンス ステータスや利用可能性を更新できるように、Unified Mobility Advantage サーバと Cisco Unified Presence を統合できます。同様に、Unified Mobile Communicator クライアントは、ユーザのバディ リスト、ディレクトリ リスト、コンタクト リスト、ボイスメール メッセージ リスト、およびコール履歴ログ内で他の社内クライアントに関するプレゼンス情報を受信します。プレゼンス ステータスとバディ リストは、Unified Mobile Communicator クライアントとユーザの Cisco Unified Personal Communicator クライアントの間で同期化されます。Unified Mobile Communicator ユーザは、クライアント上で自分の利用可能性を調整したり、Microsoft Exchange パーソナル カレンダーの利用可能性とデスクトップフォンの回線状態に基づく利用可能性の自動更新を利用することができます。図 25-11 に示すように、Cisco Unified Presence との統合は、Unified Mobility Advantage サーバと Cisco Unified Presence サーバ間の SIP/SIMPLE 接続を通して実現されます。

（注）　Cisco Mobile、つまり iPhone 対応の Unified Mobile Communicator クライアントには、プレゼンス ステータスは表示されず、プレゼンス ステータスのアップデートの送受信もサポートされていません。

Cisco Unity と Unity Connection ボイスメール

Unified Mobility Advantage サーバは、Cisco Unity（Unified Messaging または Integrated Messaging モード）および Cisco Unity Connection ボイスメール システムと統合して Unified Mobile Communicator クライアントにユーザの会社のボイスメール ボックスに関するメッセージ待機インジ

ケータ（MWI）を提供できます。この統合によって、ユーザは、モバイル デバイスを使用して視覚的にボイスメール ボックスをナビゲートすることもできます。ボイスメール ボックス内のすべてのメッセージのリストをナビゲートできます。このリストには次の情報が含まれています。

- メッセージが残された時間
- メッセージ長
- メッセージを残した人物の発信者 ID または名前（可能な場合）
- メッセージの優先順位指定
- メッセージを残した人物の現在のプレゼンスまたは利用可能性の指定（その人物が会社のプレゼンス インフラストラクチャにプレゼンス ステータスを提供している場合）

ユーザがリストからメッセージを選択すると、Unified Mobile Communicator クライアントによってデータ接続を通してメッセージがダウンロードされます。ユーザは、ボイスメール システム上でそのメッセージを再生して、削除または保存することができます。Cisco Unified Mobile Communicator クライアントによるボイスメール メッセージのステータスに対する変更（メッセージに対する再生済みのマーキングやメッセージの削除など）は、ボイスメール システムに伝播され、ユーザのデスクトップフォンと Cisco Unified Personal Communicator などのその他のクライアントに適切に反映されます。ボイスメール メッセージは任意の順序でナビゲートできます。図 25-11 に示すように、Unified Mobility Advantage サーバと Cisco Unity または Unity Connection は IMAP プロトコルを使用して統合されます。

Cisco Unified MeetingPlace

Unified Mobile Communicator ユーザが MeetingPlace 会議の開催通知または招待を受信できるように、Unified Mobility Advantage サーバと Cisco Unified MeetingPlace を統合できます。この会議通知には、会議の議題、日時、ダイヤルイン番号、および会議 ID が含まれています。ユーザは、ダイヤルイン番号をクリックすれば呼び出すことができます。

（注）　クリックツージョインは、Cisco Mobile、つまり iPhone および Blackberry 対応の Cisco Unified Mobile Communicator だけでサポートされています。その他すべての Cisco Unified Mobile Communicator クライアントについては、コールが接続された後、ユーザが手動で会議 ID を入力する必要があります。

Cisco Unified MeetingPlace との統合は、Unified Mobility Advantage サーバから会議システムで使用されている Microsoft Exchange サーバへの直接接続を経由して実現されます。図 25-11 に示すように、この接続では、Web-based Distributed Authoring and Versioning（WebDAV）プロトコルが使用されます。バージョン 7.1 よりも前の Cisco Unified Mobile Communicator クライアントでは、Outlook プラグインでスケジュールされた会議コールに関する Cisco Unified MeetingPlace 通知だけが受信されていました。Cisco Unified Mobile Communicator 7.1 以降は、会議の通知を受信するために Outlook プラグインを使用して会議をスケジュールする必要がなくなりました。Unified MeetingPlace Web ユーザ インターフェイスを使用してスケジュールされた会議についても、会議通知を受信できるようになりました。

Cisco Unified Mobile Communicator クライアント（Cisco Mobile を含む）で会議通知を受信するには、Cisco Unified MeetingPlace 会議通知電子メール テンプレートを変更して、各会議通知に **cump://** のプレフィックスが付いたリンクを含める必要があります。Cisco Unified Mobility Advantage サーバでは、ユーザの Exchange メールボックス内に含まれるすべての会議通知でこのリンクが検索されます。会議通知にこのリンクが含まれていない場合、会議の通知はクライアントで受信されず、表示もさ

れません。Cisco Unified MeetingPlace 会議通知電子メール テンプレートで必要な変更の詳細については、次の Web サイトで入手可能な Cisco Unified Mobility Advantage の設定マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html

Cisco Unified Mobility Advantage 7.1(3) 以降は MeetingPlace との統合により、会議通知がサポートされるだけでなく、パスワードや会議 ID の入力を必要としない会議へのクリックツージョインも可能です。図 25-11 のとおり、このクリックツージョイン機能は、MeetingPlace サーバの Web Services API への SOAP コールによって実施されます。バージョン 7.1(3) では、会議通知のための MeetingPlace との統合は引き続き WebDAV プロトコルを使用して Exchange を介して実行できますが、Cisco MeetingPlace Express は SOAP を介したクリックツージョインをサポートしないために削除されました。

（注）　クリックツージョインは、Cisco Mobile、つまり iPhone および Blackberry 対応の Unified Mobile Communicator クライアントだけでサポートされています。

Cisco WebEx によって Cisco Unified MeetingPlace 会議の Web 共有機能が提供される配置においては、iPhone および Blackberry Cisco Mobile クライアントは、iPhone および Blackberry で Cisco WebEx Meeting Center アプリケーションを相互に起動します（このアプリケーションがデバイスにインストール済みであることが前提です）。この相互起動が動作するには、Cisco Unified MeetingPlace システムが Cisco WebEx と正常に統合されている必要があります。

Microsoft Exchange

Cisco Unified MeetingPlace の会議統合に関する Microsoft Exchange との通信に加えて、Cisco Unified Mobility Advantage サーバと Microsoft Exchange を WebDAV 経由で統合すれば、Exchange に保存されたユーザの個人的なコンタクト リストの維持管理が容易になります。Exchange との統合によって、ユーザのプレゼンス ステータスを Exchange カレンダーの利用可能性に基づいて自動的に更新することもできます。Cisco Unified Mobile Communicator および Unified Mobility Advantage 7.1(3) よりも前のソリューションには、Cisco Unified MeetingPlace と統合しない場合や、個人的なコンタクト リストおよびカレンダー統合を利用しない場合でも、Microsoft Exchange との統合が必要です。バージョン 7.1(3) 以降は Microsoft Exchange との統合は任意であり、統合が必要であるのは、会議通知、個人的なコンタクト リスト、またはカレンダー統合が必要である場合にかぎられます。

安全なテキスト メッセージング

前述したアプリケーションと機能の統合に加えて、Unified Mobile Communicator ユーザは、Unified Mobile Communicator クライアントを使用している他のユーザに安全なテキスト メッセージを送信することもできます。このメッセージ交換は、Cisco Unified Mobility Advantage サーバ内でネイティブに実施されます。これらのメッセージは、モバイル データ接続を使用して交換されるため、SMS プロバイダーの利用料がかかります。

（注）　Cisco Mobile、つまり iPhone 対応の Unified Mobile Communicator クライアントでは、Cisco Unified Mobility Advantage サーバを使用した安全なテキスト メッセージングをサポートしていません。

Cisco Unified Mobile Communicator の冗長性

Cisco Unified Mobile Communicator クライアントは、アプリケーションの相互作用と機能を Cisco Unified Mobility Advantage Server にバックホールされるモバイル データ ネットワーク上のデータ接続に完全に依存しています。このデータ接続が、GPRS ネットワーク内の障害、モバイル データ ネットワークとの接続断、あるいは ASA TLS プロキシ、BES サーバ、または Cisco Unified Mobility Advantage サーバの故障が原因で失われた場合は、企業アプリケーションにアクセスできなくなります。この種の障害が発生した場合、ユーザは、Unified Mobile Communicator にアクセスしてさまざまなアプリケーション統合を利用できなくなります。たとえば、ディレクトリ ルックアップの実行、他のクライアントへのテキスト メッセージの送信、ビジュアル ボイスメールへのアクセス、個人連絡先へのアクセス、メッセージ待機インジケータの受信、会議通知の受信、バディ リストとプレゼンス情報の更新または同期化、Dial-via-office 機能を使用した発信などができなくなります。

（注）　Cisco Unified Mobile Communicator クライアントと Cisco Unified Mobility Advantage 間のデータ接続または Cisco Unified Mobility Advantage と Cisco Unified CM 間の接続に障害がある場合、クライアントは、Dial-via-office が強制されていても、直接通話に戻ります。

会社へのデータ接続が使用できない場合は、Unified Mobile Communicator から提供される機能を利用できなくなりますが、モバイル ボイス ネットワークを使用してモバイル デバイスで電話をかけたり、電話に出ることができます。加えて、Unified CM 上でユーザと携帯電話が Unified Mobility に統合されている場合は、モバイル コネクト機能だけでなく、モバイル ボイス アクセスやエンタープライズ機能アクセスなどの機能も使用できます。

Cisco Unified Presence、Cisco Unified CM、Cisco Unity および Unity Connection などの企業アプリケーションに不具合がある場合は、構成によりそれらのアプリケーションの特性に応じて特定の機能が利用できなくなります。ただし、ほとんどの場合、Unified Mobility Advantage サーバ内に複数のアダプタを設定できますし、さまざまなアプリケーションに対する冗長性が提供されていれば、アプリケーションまたはアプリケーション サーバに障害が発生しても機能性を維持できます。

Cisco Unified Mobile Communicator の性能と容量

Cisco Unified Mobility Advantage サーバでは、次のユーザの容量をサポートしています。

- Cisco MCS 7845-H2/I2 では、最大 1,000 台の Unified Mobile Communicator クライアントをサポートする。
- Cisco MCS 7825-H4/I4（Cisco Unified Mobility Advantage 7.1(3) 以降のリリースを実行）では、最大 500 台の Unified Mobile Communicator クライアントをサポートする。
- Cisco MCS 7825-H2/I2 または 7825-H3/I3（Cisco Unified Mobility Advantage 7.0(2) 以降のリリースを実行）では、最大 250 台の Unified Mobile Communicator クライアントをサポートする。

1 箇所で 1,000 人を超える Unified Mobile Communicator ユーザをサポートするには、追加の Unified Mobility Advantage サーバをインストールする必要があります。ただし、1 台の Cisco Unified Mobility Advantage サーバに関連付けるように設定された Unified Mobile Communicator クライアントは、別のサーバ上のクライアントにテキスト メッセージを送信できません。

エンタープライズ コール ログ統合のために Unified Mobile Communicator と Cisco Unified CM を統合した場合は、Unified Mobility Advantage サーバと Unified CM CTIManager が連携してデスクトップフォンの回線を監視します。コール ログ統合が有効にされた Unified Mobile Communicator ごとに、Cisco Unified Mobility Advantage サーバが CTIManager への CTI 接続を確立します。そのため、すべてのユーザに対してコール ログ統合が有効にされた MCS 7845 を実行しているフル実装の Unified Mobility Advantage サーバと一緒に Unified Mobile Communicator を配置した場合は、1,000 個の CTI

接続が消費されます。この理由から、Unified Mobile Communicator とコール ログ統合を配置する際は、次に示す CTI 接続に対するクラスタ全体の制限に関して、必要な CTI 接続の数を検討する必要があります。

- Cisco MCS 7845-H2/I2 サーバを使用する場合は、Unified CM クラスタごとに 20,000 個の CTI 接続
- Cisco MCS 7845-H1/I1 サーバを使用する場合は、Unified CM クラスタごとに 10,000 個の CTI 接続
- Cisco MCS 7835-H2/I2 サーバを使用する場合は、Unified CM クラスタごとに 8,000 個の CTI 接続
- Cisco MCS 7825-H3/I3 および 7825-H4 サーバを使用する場合は、Unified CM クラスタごとに 3,600 個の CTI 接続
- その他の Cisco MCS 7825 および MCS 7835 サーバを使用する場合は、Unified CM クラスタごとに 3,200 個の CTI 接続

他のアプリケーション用の CTI 接続が必要な場合は、コール ログ統合を有効にする Unified Mobile Communicator ユーザの容量を制限できます。

Dial-via-office と Unified Mobility 機能のための Unified Mobile Communicator と Unified CM の統合では、各 Unified Mobile Communicator を Unified CM デバイスとして設定し、携帯の番号をモビリティ ID として設定する必要があります。したがって、これらの統合を実施する場合は、Unified CM 電話機とモビリティ対応ユーザの機能全体を検証する必要もあります。

Cisco Unified Mobile Communicator の配置に関する設計上の推奨事項

Cisco Unified Mobile Communicator を配置する際は、次の設計上の考慮事項に従ってください。

- Cisco Unified Mobility Advantage サーバはすべての企業サービスおよびアプリケーションの統合ポイントであるため、セキュリティ上の理由から、このサーバは企業ファイアウォールの後ろに配置する必要があります。
- Cisco Adaptive Security Appliance（ASA）は、Cisco Unified Mobile Communicator クライアントと Cisco Unified Mobility Advantage サーバとの通信用のプロキシ サーバとして機能するため、企業 DMZ には ASA を配置する必要があります。
- 認証局から SSL 認証を取得する必要があります。この認証は、Cisco Unified Mobile Communicator クライアントと Cisco Unified Mobility Advantage サーバ間に流れるデータの暗号化を有効にするために必要です。
- 携帯電話にはルート認証のインポートに関する機能制限があるため、SSL 認証は、VeriSign または GeoTrust などの有名な認証局から取得する必要があります。VeriSign や GeoTrust からのルート認証は通常、ほとんどのモバイル ハンドセットで利用できます。
- 社内ファイアウォールのファイアウォール ポートを開いて、インターネット上の Cisco Unified Mobile Communicator クライアントから DMZ 内の ASA、および DMZ 内の ASA から社内の Cisco Unified Mobility Advantage サーバに接続できるようにする必要があります。次のファイアウォール ポートを開く必要があります。
  - クライアント接続ポート（SSL）: 5400 ～ 5500 の範囲の 1 つの TCP ポート（デフォルト ポートは 5443）
  - プロビジョニング ポート（HTTP）: 9000 ～ 9100 の範囲の 1 つの TCP ポート（デフォルト ポートは 9080）

（注）　iPhone または Blackberry ハンドセットだけを配置している場合、これらのハンドセットはプロビジョニング ポートを介して Cisco Unified Mobile Communicator クライアントをダウンロードしないため、ファイアウォールのプロビジョニング ポートを開く必要はありません。このクライアントは、iPhone ハンドセットの場合は Apple App Store からダウンロードされ、Blackberry ハンドセットの場合は Blackberry Enterprise Server（BES）を介してハンドセットにプッシュされます。

- Cisco Unified Mobile Communicator ユーザを認証するため、Microsoft Active Directory が必要です。すべての Cisco Unified Mobile Communicator ユーザは Microsoft Active Directory 内に有効なアカウントを持つ必要があります。そうしないと、認証に失敗し、このソリューションが提供する機能やサービスを利用できません。
- 常に、適切なバックエンド企業アプリケーション サーバが配置され、必要な Cisco Unified Mobile Communicator ソリューション機能に基づいて適切に設定されていることを確認します。サポートされている機能および必要なバックエンド アプリケーション サーバの全リストについては、次の Web サイトで入手可能な『*Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator*』を参照してください。

  shttp://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html
- Blackberry 対応の Unified Mobile Communicator クライアントである Cisco Mobile を配置する場合、Blackberry Enterprise Server（BES）および Mobile Data Services（MDS）も配置して、これを Unified Mobility Advantage サーバに直接統合する必要があります。Blackberry デバイス上の Cisco Mobile クライアントは、会社の ASA には接続せず、セキュアな Research In Motion（RIM）モバイル Network Operations Center（NOC; ネットワーク オペレーション センター）および NOC から会社の BES サーバへのセキュアな接続を使用して Unified Mobility Advantage サーバに接続します。

デュアルモードの電話機とクライアント

モバイル ユーザ、携帯電話、携帯通信事業者サービスが普及するにつれて、単一のデバイスを使用して社内および社外の両方で音声サービスとデータ サービスを使用できることがますます魅力的なソリューションとなっています。企業においてデュアルモード電話機、およびそこで実行されるクライアントを使用すると、単一の携帯電話を使用して、社内にいるユーザに対してカスタマイズされた音声サービスとデータ サービスを提供し、さらに一般的な音声サービスとデータ サービス用のバックアップ プロバイダーとして携帯通信事業者ネットワークを利用できます。社内で音声サービスとデータ サービスを利用可能にし、デュアルモード電話機に対してネットワーク接続を提供することによって、企業はこれらのサービスをローカルでより安価な接続コストで提供できます。たとえば、企業ネットワーク上で発信される Voice over IP（VoIP）コールは、通常、モバイル ボイス ネットワーク上で発信される同じコールよりもコストが少なく済みます。

この項では、デュアルモード電話機のアーキテクチャについて説明します。また、企業の WLAN ネットワークとモバイル ボイス ネットワークとの間でアクティブな音声コールを移動する場合のハンドオフに関する考慮事項を含む、デュアルモードの電話機とクライアントによって提供される機能について

説明します。この項では、一般的なデュアルモード ソリューション アーキテクチャおよび機能について説明したあと、2 つの特定のデュアルモード クライアントのさまざまな機能および統合に関する考慮事項について説明します。

- Cisco Mobile：iPhone モバイル デバイス対応のデュアルモード クライアントで、企業の WLAN ネットワーク上で VoIP コールを発信する機能、および社内ディレクトリとボイスメール サービスにアクセスする機能を提供します。
- Nokia Call Connect：Nokia モバイル デバイス対応のデュアルモード クライアントで、企業の WLAN ネットワーク上で VoIP コールを発信する機能、および社内ディレクトリやその他のアプリケーションおよびサービスにアクセスする機能を提供します。

さらに、この項では、デュアルモードの電話機とクライアントの高可用性およびキャパシティ プランニングの考慮事項についても説明します。

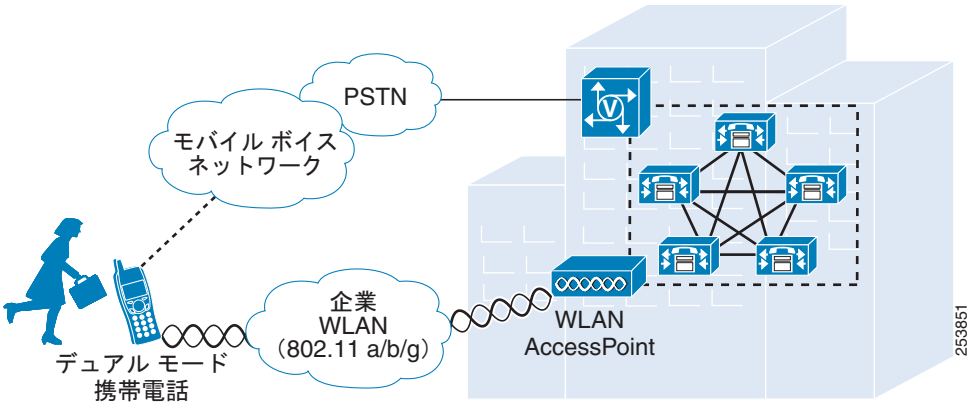
デュアルモード電話機のアーキテクチャ

デュアルモード電話機には、従来の携帯電話ネットワーク テクノロジーまたはモバイル ネットワーク テクノロジーを使用した音声とデータの携帯通信事業者ネットワークへの接続、および IEEE 802.11 標準を使用した Wireless Local Area Network（WLAN; 無線ローカル エリア ネットワーク）への接続の両方を可能にする、2 つの物理インターフェイスまたは無線機が備えられています。

（注）　この項で*デュアルモード電話機*という用語を使用する場合、802.11 に準拠した無線機、および音声とデータの通信事業者ネットワークへの接続用の携帯電話無線機を備えたデバイスを指します。Digital Enhanced Cordless Telecommunications（DECT）やその他の規格に準拠した無線機、または複数の携帯電話無線機を備えたデュアルモード デバイスは、この項のデュアルモード電話機には含まれません。

図 25-14 に、デュアルモード デバイスを Cisco Unified Communications システムに統合するための基本的なデュアルモード ソリューション アーキテクチャを示します。デュアルモード電話機が企業の WLAN に関連付けられて、デュアルモード クライアントが会社の電話機として Cisco Unified CM に登録されます。登録されると、デュアルモード デバイスは、基礎となる企業の Cisco IP テレフォニー ネットワークを利用して、コールを発信および受信します。デュアルモード電話機は、企業の WLAN 接続が利用できない場合にだけ、モバイル ボイス ネットワークを利用してコールを発信および受信します。デュアルモード電話機が企業の WLAN に関連付けられており、クライアントが Unified CM に登録されている場合、その電話機にはユーザの会社の電話番号を使用して到達できます。ユーザの会社の電話番号へのコールが着信すると、デュアルモード電話機の呼出音が鳴ります。ユーザが Cisco デスクトップ IP Phone を持っている場合は、デュアルモード クライアントを登録すると、ユーザの会社の電話番号で共有回線インスタンスが使用可能になり、コールが着信すると、ユーザのデスクトップフォンとデュアルモード電話機の両方の呼出音が鳴ります。登録が解除されると、デュアルモード クライアントは、デュアルモード電話機で会社の電話番号に着信したコールを受信しなくなります。ただし、ユーザに対して Cisco Unified Mobility が有効になっており、ユーザの携帯の番号でモバイル コネクト（またはシングル ナンバー リーチ）がオンになっている場合には、会社の電話番号に着信したコールが受信されます。

図 25-14　デュアルモード電話機のアーキテクチャ



モバイル ボイス ネットワークとモバイル データ ネットワーク、および WLAN ネットワークの両方に同時に接続するために、デュアルモード電話機では、Dual Transfer Mode（DTM; デュアル転送モード）がサポートされている必要があります。デバイスで DTM がサポートされていると、デバイスの携帯電話無線機と WLAN インターフェイスの両方からデバイスに到達可能になり、両方のインターフェイスでコールを発信および受信できます。モバイル ボイス ネットワークおよびモバイル データ ネットワークでデュアル接続デバイスがサポートされていない場合には、適切なデュアルモード クライアント操作が実行できない場合があります。

Voice over Wireless LAN ネットワークのインフラストラクチャ

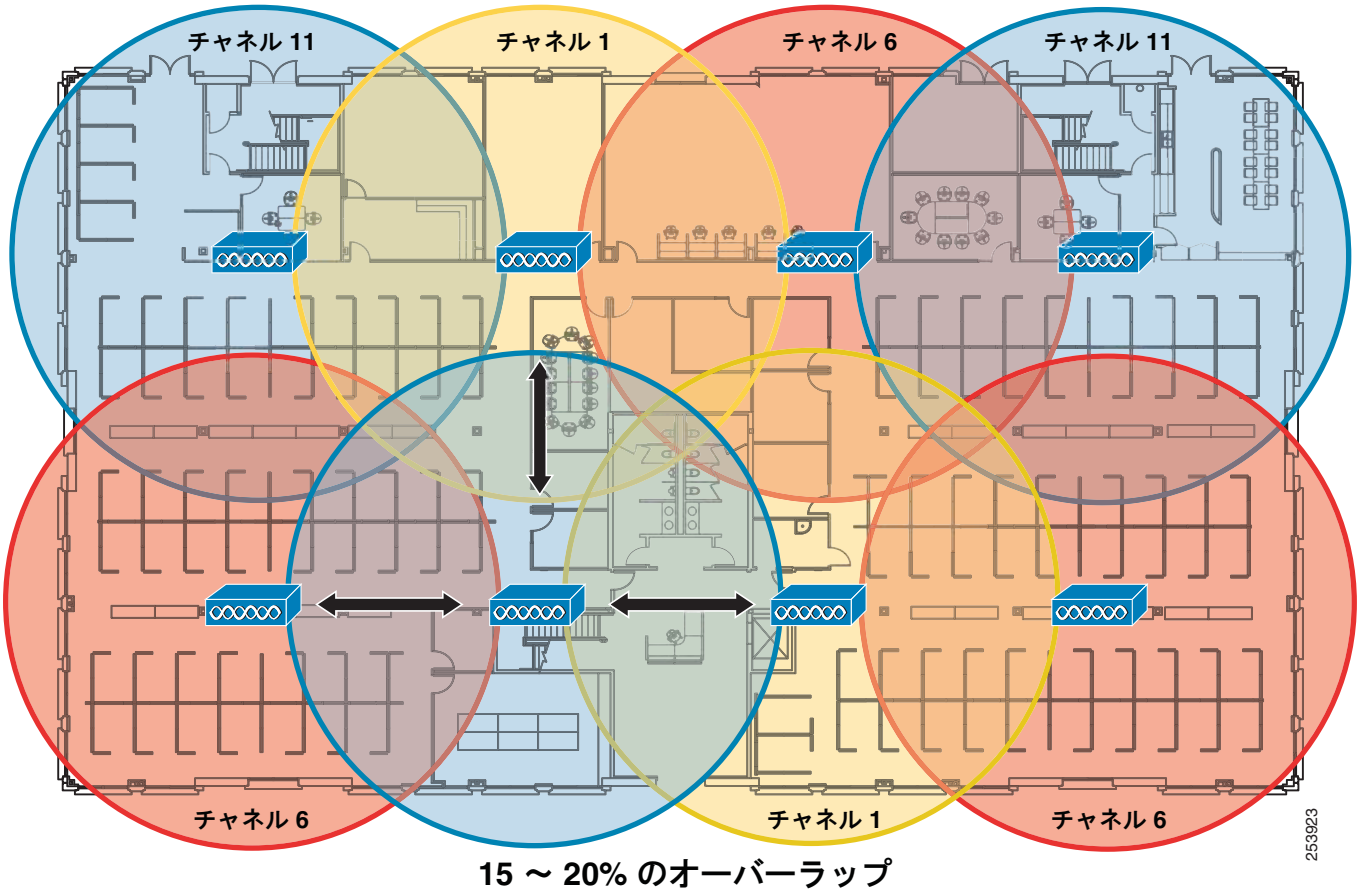
さまざまなデュアルモード機能、およびこれらの機能がエンタープライズ テレフォニー インフラストラクチャに与える影響について考慮する前に、適切に調整され、QoS に対応し、高可用性を備えた WLAN ネットワークを計画して配置することが重要です。デュアルモード電話機は、重要なシグナリング トラフィック、コールのセットアップやさまざまなアプリケーションへのアクセスのためのその他のトラフィック、およびリアルタイムの音声メディア トラフィックにおいて、基礎となる WLAN インフラストラクチャを利用するため、データ トラフィックおよびリアルタイムの音声メディア トラフィックの両方に最適化された WLAN ネットワークの配置が必要になります。WLAN ネットワークの配置が適切でないと、多くの干渉が発生し、容量が低下するため、音声品質が低下するだけでなく、コールがドロップされたり、つながらなかったりする可能性もあります。このように配置された WLAN は、音声コールの発信および受信に使用できなくなります。したがって、デュアルモード電話機を配置する場合は、Voice over WLAN（VoWLAN）の配置が正常に行われるように、配置前、配置中、配置後に WLAN Radio Frequency（RF; 無線周波数）実地調査を実施して、適切なセル境界、設定、機能設定、容量、および冗長性を判断する必要があります。実稼動環境への配置の前に、WLAN の配置に対してデュアルモード電話機のデバイス タイプまたはクライアントごとにテストを実施して、統合および動作が適切に行われるようにする必要があります。QoS を含む最適な VoWLAN サービス（Cisco Unified Wireless Network など）が提供されるように配置および設定された WLAN を使用することによって、デュアルモード電話機を正常に配置できます。

WLAN ネットワークは、1 箇所以上の無線 Access Point（AP; アクセス ポイント）から構成されます。無線 AP は、無線デバイスに対して無線ネットワーク接続を提供します。無線 AP は、無線ネットワークと有線ネットワークとの間の境界ポイントとなります。ネットワークのカバー領域および容量を拡張するために、物理的なネットワーク敷設領域に複数の AP が分散して配置されます。AP は、ネットワーク内に自律的に配置して、各 AP が他のすべての AP とは独立して設定、管理、および運用されるようにすることも、WLAN コントローラによってすべての AP が設定、管理、および制御されるように管理して配置することもできます。後者の方法において、WLAN コントローラは、AP の管理、および AP 設定と AP 間ローミングの処理を担当します。いずれの場合も、VoWLAN が正常に配置されるには、次の一般的なガイドラインに従って AP を配置する必要があります。

- 図 25-15 に示すように、WLAN チャネル セル オーバーラップ AP は、2.4 GHz（802.11b/g）の配置においては、20% のセル オーバーラップを確保して配置する必要があります。5 GHz（802.11a）の配置におけるチャネル オーバーラップは、15 ～ 20% の範囲である必要があります。

  このようにオーバーラップさせることによって、デュアルモード デバイスがロケーション内で移動した場合に AP 間で正常にローミングして、ボイス ネットワーク接続およびデータ ネットワーク接続を維持できます。2 つの AP 間で正常にローミングしたデバイスは、音声品質や音声パスに目立った変更なしにアクティブな音声コールを維持できます。

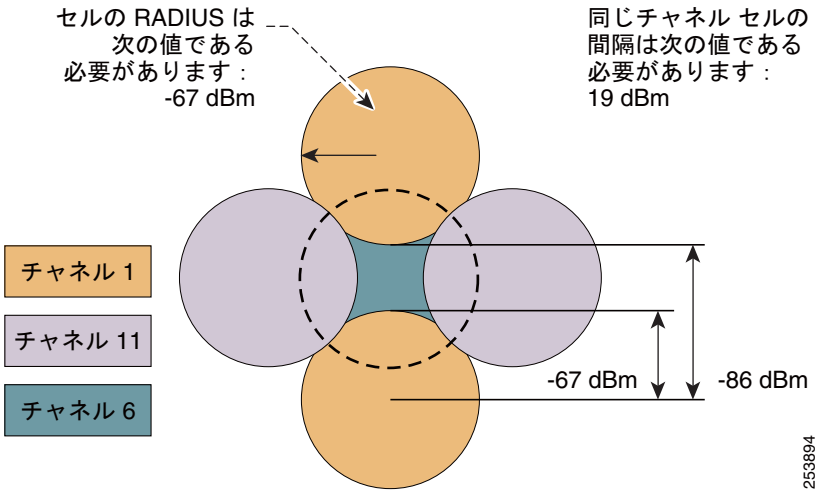
図 25-15　　WLAN チャネル セル オーバーラップ



- 図 25-16 に示すように、WLAN セル半径および同一チャネル セル分離 AP は、-67 デシベル / ミリワット（dBm）のセル パワー レベル境界（またはチャネル セル半径）で配置する必要があります。また、同一チャネルのセル境界の分離は、約 19 dBm にする必要があります。

  約 -67 dBm（またはそれ未満）のセル半径にすることで、リアルタイムの音声トラフィックで問題となるパケット損失を最小限に抑えることができます。19 dBm の同一チャネル セル分離は、AP またはクライアントにおいて、同じチャネルに関連付けられている他のデバイスとの同一チャネル干渉が発生しないようにするために重要です。同一チャネル干渉が発生すると、音声品質が低下するためです。セル半径についての -67 dBm のガイドラインは、2.4 GHz（802.11b/g）と 5 GHz（802.11a）の両方の配置に該当します。

図 25-16　WLAN セル半径および同一チャネル セル分離



（注）　19 dBm の同一チャネル セル分離は、単純化されたものであり、理想的な状態を示しています。ほとんどの配置においては、このような 19 dBm の分離を実現することができません。最も重要な RF 設計基準は、-67 dBm のセル半径と、セル間の 15 ～ 20% の推奨オーバーラップです。これらの制約を遵守して設計することによって、チャネルの分離が最適化されます。

デュアルモード電話機の接続用に WLAN ネットワークを配置または調整する場合、配置するデバイス数に対して弾力性と十分なカバレッジを確保するために、高可用性と容量について考慮することも重要です。WLAN ネットワークは、同一チャネル セルがオーバーラップすることなく、適切で冗長な数のセルによるカバレッジが保証されるように配置する必要があります。同一チャネル セルがオーバーラップしない十分なセル カバレッジ、および AP 間のローミングを容易に実行可能にするための異なるチャネル セルの十分なオーバーラップを提供することによって、デュアルモード クライアントのネットワーク接続で高可用性を確保できます。必要なコール キャパシティを処理するのに十分な数の AP を配置することによって、VoWLAN の配置においてオーバーサブスクリプションが発生する確率を大幅に減少できます。AP のコール キャパシティは、単一チャネル セル領域内でサポートできる同時 VoWLAN コール数に基づきます。VoWLAN のコール キャパシティの一般的なルールは次のとおりです。

- 2.4 GHz（802.11b/g）チャネル セルあたり最大 14 の同時 VoWLAN コール。802.11b だけの配置、またはアクティブな 802.11b クライアントの数が非常に多い配置においては、チャネル セルあたり最大で 7 の同時 VoWLAN コールがサポートされます。
- 5 GHz（802.11a）チャネル セルあたり最大 20 の同時 VoWLAN コール。

これらのコール キャパシティ値は、RF 環境、VoWLAN デュアルモード ハンドセット機能、および基礎となる WLAN システム機能に大きく依存します。一部の配置では、実際の容量はこれよりも小さくなることもあります。

（注）　同じ AP に関連付けられている 2 台のデュアルモード電話機間の単一のコールは、2 つの同時 VoWLAN コールであると見なされます。

ほとんどの無線 AP およびデュアルモード電話機クライアントでは、企業の WLAN に安全にアクセスできるように、さまざまなセキュリティ オプションも用意されています。WLAN インフラストラクチャとデュアルモード電話機の両方でサポートされており、企業のセキュリティ ポリシーおよびセキュリティ要件に一致するセキュリティの方法を必ず選択してください。

Cisco Unified Wireless Network のインフラストラクチャの詳細については、「無線 LAN インフラストラクチャ」（P.3-73）を参照してください。Voice over WLAN 設計の詳細については、次の Web サイトで入手可能な『*Voice over Wireless LAN Design Guide*』を参照してください。

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

（注）　ほとんどのデュアルモードの電話機とクライアントは、パブリックまたはプライベートの WLAN アクセス ポイントやホットスポットに接続し、インターネットを経由して会社に接続して呼制御やその他の Unified Communications サービスを利用できますが、このように接続した場合の音声品質は保証されません。デュアルモードの電話機とクライアントを接続する場合は、エンタープライズ クラスの音声に最適化された WLAN ネットワークをお勧めします。ほとんどのパブリックまたはプライベートの WLAN AP およびホットスポットは、データ アプリケーションおよびデバイスに合せて調整されています。ほとんどの場合、クライアントの容量がより大きくなるように、AP 無線機は最大パワーに調整され、動的パワー クライアントはネットワーク接続上の最大パワーに合せて調整されます。このような調整方法は、パケットのドロップや損失時に再送信ができるデータ アプリケーションにとっては理想的ですが、パケットのドロップが大量に発生する可能性があるため、音声アプリケーションでは音声品質が非常に悪くなる可能性があります。

デュアルモードの機能

デュアルモード デバイスには、さまざまな機能が用意されています。機能や動作はデバイスによって異なりますが、この項に説明する共通の動作はすべてのデュアルモード デバイスに当てはまります。

エンタープライズ コール ルーティング

デュアルモード電話機では、エンタープライズ テレフォニー インフラストラクチャおよび（少なくとも一部において）呼制御サービスが利用されるため、デュアルモード デバイスが社内にある場合のコール ルーティングの特性と動作を理解しておくことが重要です。

着信コール ルーティング

デュアルモード デバイスは、ユーザの会社の電話番号および内線番号として Unified CM に登録されるため、システムへの着信コールがそのユーザの会社の電話番号に着信した場合、デュアルモード デバイスの呼出音が鳴ります。これは、公衆網または他の Unified CM クラスタや企業 IP テレフォニー システムから発信された着信コール、および同じ Unified CM 内の他のユーザから発信された着信コールにおける動作です。デュアルモード ユーザは、会社の電話番号に関連付けられている他のデバイスまたはクライアントを持っている場合には、これらのデバイスも共有回線として呼び出されます。コールがいずれかのデバイスまたはクライアントで応答されると、他のすべてのデバイスおよびクライアントの呼出音は鳴りやみます。

ユーザに対して Cisco Unified Mobility が有効になっており、ユーザのデュアルモード電話機の携帯の番号でシングル ナンバー リーチが有効になっているシナリオにおいては、着信コールはデュアルモード電話機の電話番号に対応するモビリティ ID に転送される場合があります。ただし、この動作が行われるかどうかは、デュアルモード デバイスが社内にあるかどうか、および Unified CM に登録されているかどうかによります。デュアルモード デバイスが社内にあり、Unified CM に登録されている場合、ユーザの会社の電話番号への着信コールは、デュアルモード デバイスのモビリティ ID に対応する内線番号でモバイル コネクトがオンになっている場合でも、モバイル コネクトによってこの ID には転送されません。Unified CM に登録されている場合にデュアルモード デバイスのモビリティ ID に会社の電話番号への着信コールが転送されない理由は、デバイスが社内にあり、WLAN ネットワークを利用できるということがシステムによって認識されるためです。したがって、企業の公衆網リソースの利用を少なくするために、Unified CM では、公衆網を経由してデュアルモード デバイスのモバイル ボイス ネットワーク インターフェイスにコールを転送する処理は行われません。代わりに、会社の電話番号に対応する WLAN インターフェイスだけが呼び出されます。

デュアルモード デバイスが社外にあるか、または Unified CM に登録されていない場合、ユーザに対して Unified Mobility が有効になっており、モビリティ ID でモバイル コネクトがオンになっていると、設定されたモビリティ ID に従って、会社の電話番号への着信コールがデュアルモード デバイスに転送されます。デュアルモードのデバイスおよびクライアントと Unified Mobility との統合の詳細については、「Cisco Mobile と Cisco Unified Mobility との間の相互作用」（P.25-60）および「Nokia Call Connect と Cisco Unified Mobility との間の相互作用」（P.25-64）を参照してください。

いずれの場合も、デュアルモード デバイスの携帯電話番号に対して直接発信された着信コールは、プロバイダー ネットワークやデバイスの設定でモバイル ネットワーク経由でデバイスにコールを転送しないように設定されている場合を除き、モバイル ネットワーク経由でデュアルモード デバイスの携帯電話無線機に直接ルーティングされます。このようなコールは、ユーザの会社の電話番号に対して発信されたコールではないため、適切な動作です。これらのコールは個人的なコールであると見なされるため、会社経由でルーティングされません。

発信コール ルーティング

デュアルモード デバイスからの発信コールで使用されるインターフェイスは、ロケーション、およびその特定の時刻におけるデバイスの接続状況に応じて異なります。デュアルモード デバイスが社外にあり、Unified CM に登録されていない場合、コールは、通常どおり携帯電話無線機インターフェイスからモバイル ボイス ネットワークにルーティングされます。ただし、社内にあり Unified CM に登録されている場合、デュアルモード デバイスからのすべてのコールは、エンタープライズ テレフォニー インフラストラクチャを利用して WLAN 無線インターフェイスから企業の WLAN ネットワークに発信される必要があります。一部のデュアルモード クライアントでは、企業ネットワーク接続が利用可能になったときにクライアントを自動的に Unified CM に登録するように、1 つ以上の設定を行う必要がある場合があります。デュアルモード クライアントが Unified CM に登録されていない場合、発信コールは常に企業ネットワークではなくモバイル ボイス ネットワークを使用して発信されます。

ダイヤル プラン

企業のダイヤル プランによって、デュアルモード デバイスが社内にあり、Unified CM に登録されている場合のダイヤリング動作が決定されます。たとえば、企業のダイヤル プランの設定で、内部の内線番号に到達するために省略ダイヤリングの使用が許可されている場合、Unified CM に登録されているデュアルモード デバイスではこの省略ダイヤリングを利用できます。デュアルモード ユーザが発信コールにおいて社内で企業のダイヤリング手順を使用し、省略ダイヤリングおよびサイトベースの番号または公衆網振り分け用数字を利用してダイヤルできることは確かに便利ですが、携帯電話ユーザは、携帯電話において、モバイル ボイス ネットワークで発信コールに対して要求される完全な E.164 ダイヤル ストリングを使用して発信コールの番号をダイヤルするため、これは若干不自然なダイヤリング方式となります。

企業におけるエンドユーザ ダイヤリング エクスペリエンスは、最終的には企業のポリシーおよび企業のテレフォニー配置の管理者によって決定されます。ただし、デュアルモード電話機では、必要なダイヤリング ストリングを正規化して、ユーザが社内または社外のいずれからでも同じ番号をダイヤルして特定の着信側接続先に到達できるようにすることをお勧めします。モバイル ネットワークにおけるダイヤリングは、通常完全な E.164（先頭に「+」が付く場合と付かない場合があります）を使用して行われ、携帯電話の連絡先は通常完全な E.164 番号で保存されるため、デュアルモード電話機においては、企業のダイヤル プランは完全な E.164 番号または先頭に「+」を付けた完全な E.164 番号を使用できるように設定することをお勧めします。Unified CM 内で、デュアルモード電話機のこのような発信ダイヤリングを処理するようにダイヤル プランが設定されている場合、ユーザは連絡先を E.164 形式で 1 セットだけ電話機に保存するだけで済みます。これらの連絡先からダイヤルする場合や、完全な E.164 番号を使用して手動でダイヤルする場合、デバイスが社内にあり Unified CM に登録されているか、またはデバイスが社外にありモバイル ボイス ネットワークにだけ接続されているかにかかわらず、コールは常に適切な接続先にルーティングされます。このように企業のダイヤル プランを設定することによって、ユーザはデバイスが社内の Unified CM に登録されているかどうかを気にする必要がなくなるため、最善のエンドユーザ ダイヤリング エクスペリエンスを提供できます。

社内か社外かにかかわらずデュアルモード電話機からの正規化されたダイヤリングを可能にするには、次の考慮事項に注意して Unified CM でダイヤル プランを設定します。

- 企業のダイヤル プランで、デュアルモード電話機からの、通常モバイル ボイス ネットワークで使用されるダイヤル ストリングを処理できるようにします。たとえば、ダイヤル プランでは、携帯電話からモバイル ボイス ネットワークを経由して特定の電話機に到達するためにダイヤルされる +1 408 555 1234 や 408 555 1234 などのストリングを処理できるように設定する必要があります。
- 会社の他の電話番号へのコールにおいては、省略ダイヤリングが設定されているシステムでは、ダイヤル ストリングを変更して、必要に応じて会社の内線番号に再ルーティングできる必要があります。たとえば、企業のダイヤル プランが 5 桁の内部ダイヤルに基づいているとすると、会社の内線番号へのコール ルーティングが処理されるようにシステムを設定して、デュアルモード デバイスが社内にあり Unified CM に登録されているときにコールが発信された場合、+1 408 555 1234 や 408 555 1234 に発信されたコールが変更されて、51234 に再ルーティングされるようにする必要があります。
- 会社のデュアルモード デバイスへのすべての着信コールの発信番号または発信者 ID の先頭に適切な数字を付加して、不在コール、発信コール、および着信コールのコール履歴リストが完全な E.164 形式となるようにします。これにより、デュアルモード デバイスのユーザは、ダイヤル ストリングを編集することなくコール履歴リストからダイヤルできます。ユーザは、社内にいるかまたは社外にいるかにかかわらず、コール履歴リストから番号を選択してリダイヤルできます。たとえば、社内の 51234 からデュアルモード ユーザの会社の電話番号にコールが発信され、そのコールに応答がない場合、発信番号を操作して、デュアルモード デバイスの履歴リストに 408 555 1234 または + 1 408 555 1234 という形式のエントリが残るように Unified CM を設定する必要があります。この番号は、操作しなくても、デュアルモード デバイスが Unified CM に登録されている場合に社内でダイヤルすることも、社外でダイヤルすることもできます。

デュアルモード デバイスの正規化されたダイヤリングの例外の 1 つに、会社の内線番号または電話に内部からだけ到達可能なシナリオがあります（つまり、対応する外部から到達可能な DID 番号がない場合）。このような場合は、省略形式を使用して、外部から到達できない番号をダイヤルできます（手動でダイヤルするか、または連絡先からダイヤルします）。これらの番号は外部では利用できず、社内からだけダイヤルできるため、連絡先リストにこれらの番号を保存する場合には、社内だけで使用できるという何らかのマークが必要となります。さらに、これらの内部専用番号からの着信コールの発信番号をコール履歴リストに保存する場合は、番号が変更されないようにする必要があります。これらの番号には、社内からだけ発信できるためです。すべてのコール履歴リストにおいて、これらの内線番号からのコールは番号を変更しないで保存する必要があります。このように変更しないで保存された番号、つまり省略ダイヤル ストリングは、デバイスが社内にあり Unified CM に登録されているときにだけ正常にダイヤルできます。

緊急サービスおよびダイヤリングの考慮事項

デュアルモード電話機から 911、999、112 などの緊急サービス番号に対してコールを発信する場合、事態は少々複雑になります。デュアルモード デバイスは社内または社外に位置する可能性があるため、緊急時におけるデュアルモード電話機およびそのユーザの位置の通知について考慮する必要があります。携帯電話はすでにプロバイダー ネットワークの位置サービスを利用しています。これらの位置サービスは常に利用可能であり、通常は企業無線ネットワークよりもはるかに正確に位置を特定できるため、緊急コールを発信し、デバイスおよびユーザの位置を特定する場合には、モバイル ボイス ネットワークを利用することをお勧めします。デュアルモード電話機から緊急コールを発信したり位置サービスを利用したりする場合にモバイル ボイス ネットワークだけが利用されるように、Unified CM 内でデュアルモード デバイスを設定して、911、999、112 などの緊急番号へのコールを許可するルート パターンにこれらのデバイスからアクセスできないようにします。さらに、デュアルモード電話機のユーザに対して、すべての緊急コールを企業ネットワークではなくモバイル ボイス ネットワーク経由で発信するように指示します。

会社の発信者 ID

デュアルモード デバイスが社内にあり、Unified CM に登録されている場合、デュアルモード電話機の WLAN インターフェイス経由で発信されるすべてのコールは、ユーザの会社の電話番号が発信者 ID として設定されてルーティングされます。これにより、遠端でコール履歴リストから発信される返信コールはユーザの会社の電話番号に対して発信されることになり、常に会社経由でルーティングされます。デュアルモード ユーザに対して Cisco Unified Mobility が有効になっており、デュアルモードの携帯の番号でモバイル コネクトがオンになっている場合、デュアルモード デバイスが社外にあるときには、会社の電話番号への返信コールも公衆網経由でデュアルモード デバイスに転送されます。

通話切替機能

デュアルモード電話機クライアントが社内にあり、テレフォニー エンドポイントとして Unified CM に登録されている場合、Unified CM でサポートされているコール シグナリング方式を使用して、保留、保留解除、転送、会議などのコール処理付加サービスを呼び出すことができます。Unified CM に登録された IP Phone やクライアントと同様に、これらのデバイスでは、Music On Hold（MoH; 保留音）、カンファレンス ブリッジ、メディア ターミネーション ポイント、トランスコーダなどの企業のメディア リソースを利用できます。

外部コール ルーティング

デュアルモード デバイスが社外にあり、Unified CM に登録されていない場合、このデバイスでは、モバイル ボイス ネットワーク経由でだけコールを発信および受信できます。このため、デュアルモード電話機デバイスが登録されていない場合に発信または受信されるすべてのコールにおいて、Unified CM は関与しません。デュアルモード電話機で社外からコールが発信された場合、ネットワークに送信される発信者 ID は携帯の番号です。このため、応答されなかったコールへの返信コールは、会社経由でルーティングされるのではなく、デュアルモード デバイスの携帯の番号に直接発信されることになります。

デュアルモード電話機が Cisco Unified Mobility と統合されている場合は、デュアルモード デバイスが社外にあり Unified CM に登録されていない場合でも、エンタープライズ 2 ステージ ダイヤリング サービスを利用して会社経由でコールを発信できます。Unified Mobility の 2 ステージ ダイヤリングは、モバイル ボイス アクセスまたはエンタープライズ機能アクセスを使用して実行され、ユーザは会社の DID 番号をダイヤルし、クレデンシャルを入力してから発信番号をダイヤルする必要があります。Unified Mobility の 2 ステージ ダイヤリング機能の詳細については、「モバイル ボイス アクセスとエンタープライズ機能アクセス」（P.25-16）を参照してください。

同様に、デュアルモード電話機が Unified Mobility と統合されている場合、ユーザは、会社の電話番号への着信コールをモバイル コネクト経由で携帯の番号で受信したり、DTMF キー シーケンスを使用して保留、保留解除、転送、会議などの通話切替機能を呼び出したり、デスクトップフォンのピックアップを実行してアクティブなコールを携帯電話から会社のデスクトップフォンに移動したりできます。

追加のサービスおよび機能

コール処理サービスや呼制御サービスに加えて、デュアルモードの電話機とクライアントでは、この項に説明する追加の機能およびサービスを提供できます。

コール ハンドオフ

デュアルモード電話機の配置における非常に重要な側面の 1 つに、ユーザが社内と社外の間を移動したり、ネットワーク接続が携帯電話無線機と WLAN 無線機との間で切り替わったりしたときのコール プリザベーションがあります。デュアルモード電話機のユーザは多くの場合移動するため、デュアルモード ユーザが社内と社外の間を移動するときにアクティブなコールが維持されることが重要です。このため、デュアルモード クライアントおよび基礎となる企業のテレフォニー ネットワークでは、何らかの形式のコール ハンドオフが可能である必要があります。

デュアルモード クライアント、および基礎となる IP テレフォニー インフラストラクチャの両方でサポートされる必要がある 2 種類のコール ハンドオフがあります。

- ハンドアウト

  コール ハンドアウトとは、アクティブなコールをデュアルモード電話機の WLAN インターフェイスからデュアルモード電話機の携帯電話インターフェイスに移動することを指します。このためには、コールが、会社の公衆網ゲートウェイ経由で、企業の WLAN ネットワークからモバイル ボイス ネットワークにハンドアウトされることが必要です。

- ハンドイン

  コール ハンドインとは、アクティブなコールをデュアルモード電話機の携帯電話インターフェイスからデュアルモード電話機の WLAN インターフェイスに移動することを指します。このためには、コールが、会社の公衆網ゲートウェイ経由で、モバイル ボイス ネットワークから企業の WLAN ネットワークにハンドインされることが必要です。

デュアルモード電話機のハンドオフ動作は、デュアルモード クライアントの特性およびその特定の機能に依存しています。手動ハンドオフ機能だけを提供するデュアルモード クライアントもあれば、ネットワークの状態に基づいて自動的にハンドオフを呼び出すことができるデュアルモード クライアントもあります。手動ハンドオフのシナリオにおいては、デュアルモード ユーザは、各自のロケーションおよび必要性に基づいてハンドオフ動作を行い、完了する必要があります。自動ハンドオフでは、デュアルモード クライアントは企業の WLAN AP 信号の増幅または減衰を検知して、WLAN 信号の強度が減衰した場合にはハンドアウトを行う決定をしてハンドアウト動作を実行し、WLAN 信号が増幅した場合にはハンドインを行う決定をしてハンドイン動作を実行できます。

ハンドオフ動作は、電話のコールにおいてエンタープライズ IP テレフォニー インフラストラクチャを最大限に活用するために重要となります。また、これらの動作は、音声の継続性と良好なユーザ エクスペリエンスを提供し、ユーザが元のコールをいったん切ってから再度コールを発信し直す必要がないようにするためにも必要です。

社内ディレクトリ アクセス

一部のデュアルモード クライアントは、ディレクトリ検索や個人的なコンタクト リストを含む社内ディレクトリ サービスにアクセスできます。この機能はデュアルモードのデバイスおよびクライアントに必須の機能ではありませんが、デュアルモード電話機のユーザが携帯電話から社内ディレクトリ情報にアクセスできると、これらのユーザの生産性が向上します。

企業ボイスメール サービス

多くのデュアルモード クライアントでは、企業ボイスメール サービスにアクセスすることもできます。ほとんどのデュアルモード クライアントでは、ユーザの企業ボイスメール ボックスに未読のボイスメールが存在し、デュアルモード電話機が企業の WLAN ネットワークに接続されている場合に、企業メッセージ待機インジケータを受信できます。さらに、デュアルモード クライアントを使用して、企業ボイスメール メッセージを取得することもできます。通常、企業ボイスメール メッセージは、ユーザがボイスメール システム番号にダイヤルし、必要なクレデンシャルを入力してから各自のボイスメール ボックスに移動して取得します。ただし、一部のデュアルモード クライアントは、ボイスメール ボックス内のすべてのメッセージのリストをダウンロードおよび表示し、デュアルモード電話機にダウンロードして再生する個別のメッセージを選択することによって、ボイスメール ボックスからボイスメール メッセージを取得する機能を備えています。この機能は、ビジュアル ボイスメールと呼ばれることもあります。デュアルモード電話機クライアントおよび企業ボイスメール システムの両方において、ネットワーク経由でのボイスメール リストの提供およびメッセージのダウンロードが可能である必要があります。Cisco Unity および Cisco Unity Connection は両方ともビジュアル ボイスメールをサポートしており、デュアルモード クライアントでもこの機能がサポートされている場合にはボイスメール リストの提供およびボイスメールのダウンロードが可能です。

デュアルモード クライアント：Cisco Mobile

Cisco Mobile は、Apple iPhone 対応のデュアルモード クライアントです。Apple の App Store からクライアント アプリケーションをダウンロードし、iTunes を使用して iPhone にインストールすると、iPhone を企業の WLAN ネットワークに関連付けて、SIP 対応の会社の電話機として Unified CM に登録できます。

（注）　Cisco Mobile デュアルモード iPhone クライアントは、Unified CM 7.1(3) 以降のリリースでサポートされます。

Cisco Mobile デュアルモード iPhone クライアントに登録および呼制御サービスを提供するには、Unified CM 内でデバイスが **Cisco Dual-Mode for iPhone** デバイス タイプとして設定される必要があります。次に、企業の WLAN にアクセスして企業の WLAN インフラストラクチャおよびセキュリティ ポリシーに基づいて接続するように iPhone を設定する必要があります。WLAN にアクセスするように iPhone を設定すると、Cisco Mobile クライアントが起動されたときに、デバイスが Unified CM に登録されます。

（注）　7.1(5) よりも前のバージョンの Unified CM では、Cisco Option Package（COP）ファイルを Unified CM にアップロードして、**Cisco Dual-Mode for iPhone** デバイス タイプを使用可能にする必要があります。Unified CM 7.1(5) では、このデバイス タイプはデフォルトでインストールされます。

Unified Mobility と統合し、ハンドオフ機能を利用するには、iPhone の携帯番号を、Unified CM 内の Cisco Dual-Mode for iPhone デバイスに関連付けられたモビリティ ID として設定する必要があります。

Cisco Mobile クライアントは、ファームウェア バージョン 3.0.1 以降が実行されている iPhone の 3G または 3GS モデルでサポートされています。iPhone WLAN インターフェイスでは、802.11b および g ネットワーク接続がサポートされています。

Cisco Mobile クライアントでは、デュアルモード電話サービスだけではなく、企業の Microsoft Active Directory へのアクセスが設定されている場合にはディレクトリ検索サービスが、Cisco Unity Connection 上のユーザのボイスメール ボックスへのアクセスが設定されている場合にはビジュアル ボイスメール サービスが提供されます。

（注）　Cisco Mobile と iPhone 対応の Cisco Unified Mobile Communicator クライアントの両方を同時に配置する場合は、ユーザの企業ボイスメール ボックスにアクセスするように Cisco Mobile を設定しないでください。代わりに、Cisco Mobile クライアントを使用してビジュアル ボイスメール アクセスを行います。これは、Cisco Mobile クライアントの方が機能が豊富で、よりよいユーザ エクスペリエンスを提供できるためです。

Cisco Mobile クライアントは、「Cisco Mobile のハンドオフ」（P.25-59）の項に説明されているように、手動でのハンドアウトだけを実行できます。

Cisco Mobile デュアルモード iPhone クライアント、追加の機能、およびサポートされているハードウェアとソフトウェアのバージョンの詳細については、次の Web サイトで入手可能な Cisco Unified Mobile Communicator のマニュアルを参照してください。

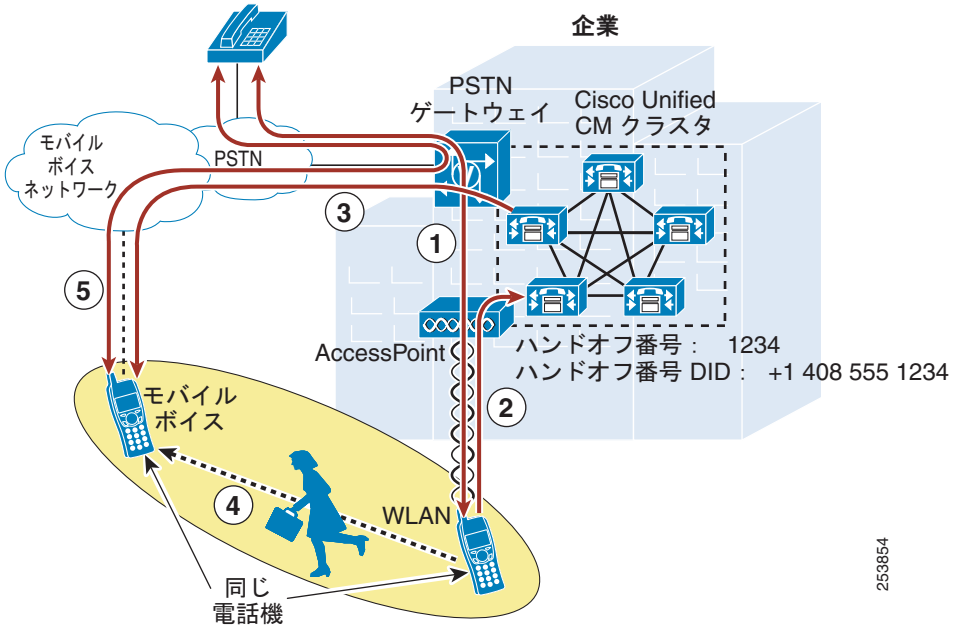
http://cisco.com/en/US/products/ps7271/tsd_products_support_series_home.html

Cisco Mobile のハンドオフ

Cisco Mobile デュアルモード クライアントを適切に配置するには、クライアント内部のハンドオフ動作の特性について理解することが重要です。Cisco Mobile デュアルモード iPhone クライアントによって使用されるハンドオフ方式は、Cisco Dual-Mode for iPhone デバイスの設定ページの [Transfer to Mobile Network] 設定に基づきます。以降では、この設定フィールドが [Use Mobility Softkey (user receives call)] に設定されている場合の方式に基づいて説明します。

図 25-17 に示す動作は、社内の iPhone デュアルモード電話機におけるアクティブなコールが、手動で WLAN インターフェイスから会社の公衆網ゲートウェイ経由でモバイル ボイス ネットワーク（デバイスの携帯電話インターフェイス）に移動されるようすを示しています。図に示すように、企業の WLAN に関連付けられ、Unified CM に登録された iPhone デュアルモード デバイスと、公衆網ネットワーク上の電話機との間に既存のコールがあります（ステップ 1）。これは手動のプロセスであるため、ユーザが Cisco Mobile クライアント内のコール中メニューから [Use Mobile Network] ボタンを選択して、コールをハンドアウトする必要があることを Unified CM に通知する必要があります（ステップ 2）。次に、Unified CM から、この Cisco Mobile デバイスに対応する設定済みのモビリティ ID 番号に対して、会社の公衆網ゲートウェイを経由してコールが発信されます（ステップ 3）。このモビリティ ID へのコールは、モバイル ボイス ネットワーク（iPhone の携帯電話インターフェイス）に対して発信されます。これで、ユーザは、社外に移動して、WLAN ネットワークのカバー領域から離れることができます（ステップ 4）。一方、Unified CM からの着信コールがモバイル ボイス ネットワーク インターフェイスで受信され、ユーザは手動でこのコールに応答し、ハンドアウトを完了する必要があります。携帯電話インターフェイスで着信コールが応答されると、WLAN を通過していた RTP ストリームが公衆網ゲートウェイにリダイレクトされ、Cisco Mobile デュアルモード クライアントと元の公衆網電話機との間のコールは会社のゲートウェイで固定されて、中断されずに継続します（ステップ 5）。

図 25-17　Cisco Mobile デュアルモード ハンドアウト（WLAN からモバイル ボイス ネットワークへ）



Cisco Mobile デュアルモード クライアントには、これとは別に、設定された Unified CM ハンドオフ番号を使用するハンドアウト方法も用意されています。この方法を使用するには、Cisco Dual-Mode for iPhone デバイスの設定ページの [Transfer to Mobile Network] フィールドが [Use Handoff DN Feature (user places call)] に設定されている必要があります。この方法を使用すると、Unified CM にハンドオフを通知して、公衆網ゲートウェイ経由でシステムから iPhone の携帯電話番号にコールを受

信する（図 25-17 のステップ 2 および 3）代わりに、ユーザがハンドオフを呼び出すと、Cisco Mobile クライアントからモバイル ボイス ネットワーク（携帯電話インターフェイス）経由で Unified CM 内に設定されたハンドオフ番号に対応する DID にコールが発信されます（この例では + 1 408 555 1234）。このハンドオフ番号への着信コールがシステムで受信されると、WLAN を通過していた RTP ストリームが公衆網ゲートウェイにリダイレクトされ、Cisco Mobile デュアルモード クライアントと元の公衆網電話機との間のコールは会社のゲートウェイで固定されて、中断されずに継続します。

（注）　Cisco Mobile では、ハンドインはサポートされていません。iPhone のモバイル ボイス ネットワーク（携帯電話インターフェイス）と会社の電話（または会社のゲートウェイでコールが固定された公衆網電話機）との間で通話中のコールがアクティブである場合、コールを iPhone の WLAN インターフェイスに移動するには、コールをいったん切断し、Cisco Mobile クライアントが企業の WLAN に関連付けられて Unified CM に登録されてからリダイヤルするのが唯一の方法です。

Cisco Mobile と Cisco Unified Mobility との間の相互作用

iPhone 対応の Cisco Mobile デュアルモード クライアントは、Cisco Unified Mobility と統合して、Cisco モバイル コネクト、通話切替 DTMF 機能、2 ステージ ダイヤリング、シングル企業ボイスメール ボックス、およびデスクトップフォンのピックアップを利用できます。

Unified Mobility と統合するには、Unified CM 内で、iPhone デュアルモード携帯電話番号を Cisco Dual-Mode for iPhone デバイスに関連付けられたモビリティ ID として設定する必要があります。システム内で携帯の番号がモビリティ ID として設定されると、iPhone デュアルモード デバイスが社外にあり、Unified CM に登録されていない場合に、モバイル コネクトを利用して、ユーザの会社の電話番号への着信コールをモバイル ボイス ネットワークを経由して iPhone デュアルモード デバイスに転送できます。iPhone デュアルモード デバイスが社内にあり、Unified CM に登録されている状況においては、会社の番号への着信コールはデバイスのモバイル ボイス ネットワーク インターフェイスには転送されません。iPhone デュアルモード デバイスが社内にある場合は、デバイスの WLAN インターフェイスだけが着信コールを受信します。これにより、会社の公衆網ゲートウェイ リソースが必要以上に消費されるのを回避できます。

社外にあり、Unified CM に登録されていない場合、iPhone デュアルモード デバイスでは、会社の任意の固定コールに対して、DTMF を使用して通話切替機能を呼び出したり、デスクトップフォンのピックアップを実行したりできます。また、iPhone デュアルモード デバイスでは、コールを発信する場合にモバイル ボイス アクセスとエンタープライズ機能アクセス 2 ステージ ダイヤリング機能を利用して、これらのコールを会社経由でルーティングし、会社の公衆網ゲートウェイに固定できます。

iPhone デュアルモード デバイスに対してモビリティ ID を設定することに加えて、リモート接続先として追加の携帯電話番号またはオフシステム電話番号を設定して、これらの番号を Unified CM 内の Cisco Dual Mode for iPhone デバイスに関連付けることができます。モビリティ ID および追加のリモート接続先を iPhone デバイスに関連付ける場合は、リモート接続先プロファイルを設定する必要はありません。

Cisco Unified Mobility の機能セット、および設計と配置の考慮事項の詳細については、「Cisco Unified Mobility」（P.25-4）を参照してください。

Cisco Mobile と Cisco Unified Mobile Communicator との間の相互作用

Cisco Mobile iPhone デュアルモード クライアントは、iPhone 対応の Cisco Unified Mobile Communicator クライアントと並行して使用できます。両方のクライアントが配置された場合、iPhone デバイスからエンタープライズ IP テレフォニー インフラストラクチャを利用して社内でコールを発信および受信できるだけでなく、ディレクトリ検索、デスクトップフォンのコール ログ統合、プレゼンス、ビジュアル ボイスメール、テキスト メッセージングなどの Unified Mobile Communicator の機能を利用することもできます。

Cisco Mobile iPhone デュアルモード クライアント、および会社の Cisco Unified Mobility Advantage サーバとともに動作する Cisco Mobile クライアントの両方を配置するには、Unified CM 内で Cisco Dual-Mode for iPhone デバイスだけを設定します。設定するすべてのリモート接続先番号とモビリティ ID 番号はシステム内で一意である必要があるため、Cisco Unified Mobile Communicator デバイスは Unified CM 内で iPhone デバイスとして設定しないでください。Unified CM 内では、iPhone の携帯電話番号は、1 つのデバイスに対してだけ設定し、関連付けることができます。この場合は、Cisco Dual-Mode for iPhone デバイスがそのデバイスとなります。iPhone の携帯電話番号をモビリティ ID として設定し、Unified CM 内でこの番号を iPhone デュアルモード デバイスに関連付けることによって、Cisco Mobile デュアルモード クライアントに対して Unified Mobility の統合およびハンドアウト機能を有効にします。

Unified CM 7.1(5) では、Cisco Mobile デュアルモード クライアントと、Cisco Unified Mobility Advantage サーバとともに動作する Cisco Mobile クライアントを統合するには、Unified CM 内の Cisco Dual-Mode for iPhone デバイスの設定ページの [Enable Cisco Unified Mobile Communicator] チェックボックスをオンにします。このチェックボックスをオンにすると、Unified CM 内のデュアルモード デバイス タイプで、デュアルモード クライアントおよび Cisco Unified Mobility Advantage とともに動作する Cisco Mobile クライアントのサポートが提供されます（Dial-via-office 機能を含みます）。

Unified CM 7.1(3) では、[Enable Cisco Unified Mobile Communicator] チェックボックスが使用できないため、Cisco Mobile クライアントと Dial-via-office 機能の両方をサポートすることはできません。ただし、Unified CM 7.1(3) では、会社の Unified Mobility Advantage サーバとともに動作する Cisco Mobile クライアントを iPhone 上で実行し、Dial-via-office 機能以外のすべての Cisco Unified Mobile Communicator 機能を提供できます。

Cisco Mobile iPhone デュアルモード クライアントおよび Cisco Unified Mobile Communicator iPhone クライアントの両方が同じハンドセットに配置されている状況においては、社内ディレクトリ検索およびビジュアル ボイスメールに Cisco Unified Mobile Communicator クライアントを使用することをお勧めします。Cisco Mobile iPhone デュアルモード クライアントにも同様の機能が備えられていますが、Cisco Unified Mobile Communicator の方が機能が豊富で、よりよいユーザ エクスペリエンスが提供されます。

Unified CM 7.1(3) の配置においては、Cisco Mobile デュアルモード iPhone クライアントとともに Dial-via-office 機能を使用することができないため、デバイスが社外にあるときには、ユーザは Unified Mobility の 2 ステージ ダイヤリング機能を利用して、会社経由のコールを発信する必要があります。

Cisco Unified Mobile Communicator のソリューション、機能セット、および設計と配置の考慮事項の詳細については、「Cisco Unified Mobile Communicator」（P.25-34）を参照してください。

デュアルモード クライアント：Nokia Call Connect

Nokia Call Connect は、Nokia モバイル スマート フォン対応のデュアルモード クライアントです。クライアントを Nokia デバイスにインストールすると、企業の WLAN ネットワークに関連付けて、Skinny Client Control Protocol（SCCP）対応の会社の電話機として Unified CM に登録できます。

Nokia デュアルモード デバイスに登録および呼制御サービスを提供するには、Unified CM で Nokia S60 デバイス タイプがサポートされている必要があります。このデバイス タイプは、Nokia が提供する Cisco Option Package（COP）ファイルを Unified CM にロードすると使用可能になります。

Unified CM 内でデュアルモード デバイスを設定したあと、Nokia Call Connect クライアントを Nokia デバイスにロードする必要があります。この作業は、USB、Bluetooth、または赤外線ポートを備えた、Nokia PC Suite を実行するコンピュータを使用して行うことができます。Nokia Call Connect Symbian Installation System（SIS）ファイルを Nokia デバイスにロードしたあと、企業の WLAN にアクセスして企業の WLAN インフラストラクチャおよびセキュリティ ポリシーに基づいて接続するようにデバイスを設定する必要があります。WLAN にアクセスするようにハンドセットを設定すると、Nokia Call Connect クライアントが起動されたときに、デバイスが Unified CM に登録されます。Nokia デュアル

モード デバイスを Unified Mobility と統合して、ユーザがモバイル コネクトなどの機能を利用できるようにするには、Nokia の携帯電話番号をモビリティ ID として設定し、それを Unified CM 内の Nokia S60 デバイスに関連付けます。

（注）　Nokia Call Connect クライアントの SCCP 登録設定を [Always On] に設定して、Nokia デバイスが企業の WLAN ネットワークに関連付けられた場合に Unified CM への登録が試みられるようにすることをお勧めします。また、Nokia デュアルモード電話機の優先コール タイプまたはデフォルト コール タイプの設定を [Internet Call] に設定して、Nokia Call Connect クライアントが Unified CM に登録された場合に、デバイスからの発信コールにおいて常にデュアルモード電話機の WLAN インターフェイス経由でルーティングが試みられるようにすることをお勧めします。これらの推奨設定を行うことにより、Nokia デュアルモード電話機において、ビジネス コールの発信および受信時に可能なかぎりエンタープライズ IP テレフォニー インフラストラクチャを使用できます。

Nokia Call Connect 2.0 クライアントは、Nokia E52、E55、E72、および E75 を含む Nokia S60 3.2 ハンドセットでサポートされています。E51、E61i、E63、E66、E71、および E90 を含む Nokia S60 3.1 ハンドセットもサポートされていますが、自動ハンドオフなどの高度な機能はサポートされない可能性があります。Nokia 携帯電話の WLAN インターフェイスでは、802.11b および g ネットワーク接続がサポートされています。

Nokia Call Connect クライアントでは、デュアルモード電話サービスだけでなく、Unified CM ディレクトリへのアクセスが設定された場合には、ディレクトリ検索サービスも提供されます。また、Cisco デスクトップ IP Phone でサポートされているような企業ベースの XML 電話サービスもサポートされます。

Nokia Call Connect 2.0 以降のクライアントでは、以降の項で説明する自動ハンドアウトおよびハンドインを実行できます。

Nokia Call Connect デュアルモード クライアント、サポートされているハンドセット、ソフトウェア バージョンの詳細、および最新のクライアントと COP ファイルについては、次の Web サイトを参照してください。

http://www.cisco.com/en/US/products/ps10589/tsd_products_support_series_home.html

Nokia Call Connect デュアルモード ハンドオフ

Nokia Call Connect デュアルモード クライアントを適切に配置するには、Nokia デュアルモード クライアント内でのハンドオフ動作の特性を理解することが必要です。

以降の例では、ハンドオフ番号は +1 408 555 1234 であるとします（これは、完全な E.164 形式のハンドオフ番号です）。Nokia Call Connect の Voice Call Continuity（VCC）設定の下の [Cellular Handover number] は、この番号に設定されています。

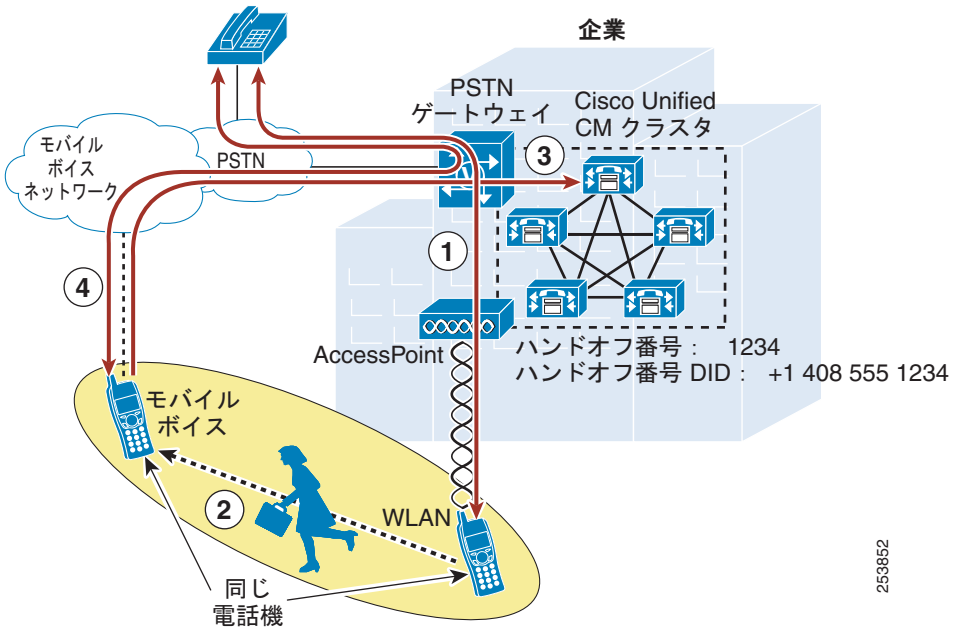
すべての着信コールは、アップストリーム ゲートウェイによって 4 桁に短縮されるため、Unified CM 内に設定するハンドオフ番号は 1234 です。Nokia Call Connect の VCC 設定の下の [VoIP Handover number] は、1234 に設定されています。

ハンドアウト（WLAN から携帯電話へ）

図 25-18 は、社内の Nokia デュアルモード電話機におけるアクティブなコールが、WLAN インターフェイスから会社の公衆網ゲートウェイ経由でモバイル ボイス ネットワーク（デバイスの携帯電話インターフェイス）に移動されるハンドアウト動作を示しています。図に示すように、企業の WLAN に関連付けられ、Unified CM に登録された Nokia デュアルモード デバイスと、公衆網ネットワーク上の電話機との間に既存のコールがあります（ステップ 1）。Nokia デュアルモード ユーザが社外への移動を開始します（ステップ 2）。WLAN 信号強度が 1,000,000 マイクロ秒（1 秒、VCC の [WLAN HO hysteresis] 設定のデフォルト値）にわたって -78 dBm（VCC の [WLAN HO threshold] 設定のデフォルト値）未満に減衰すると、モバイル ボイス ネットワークおよび公衆網経由で会社の公衆網ゲート

ウェイに対して +1 408 555 1234（VCC の [Cellular Handover number] 設定、Unified CM で設定されたハンドオフ番号に対応）へのサイレント バックグラウンド コールが開かれ、Unified CM に送信されます（ステップ 3）。このコールが受信されると、発信番号と、システムに設定されているすべてのモビリティ ID が照合されて、一致するものがある場合には、WLAN を通過していた RTP ストリームが公衆網ゲートウェイにリダイレクトされ、デュアルモード デバイスと元の公衆網電話機との間のコールは会社のゲートウェイで固定されて、中断されずに継続します（ステップ 4）。

図 25-18　Nokia Call Connect デュアルモード ハンドアウト（WLAN からモバイル ボイス ネットワークへ）



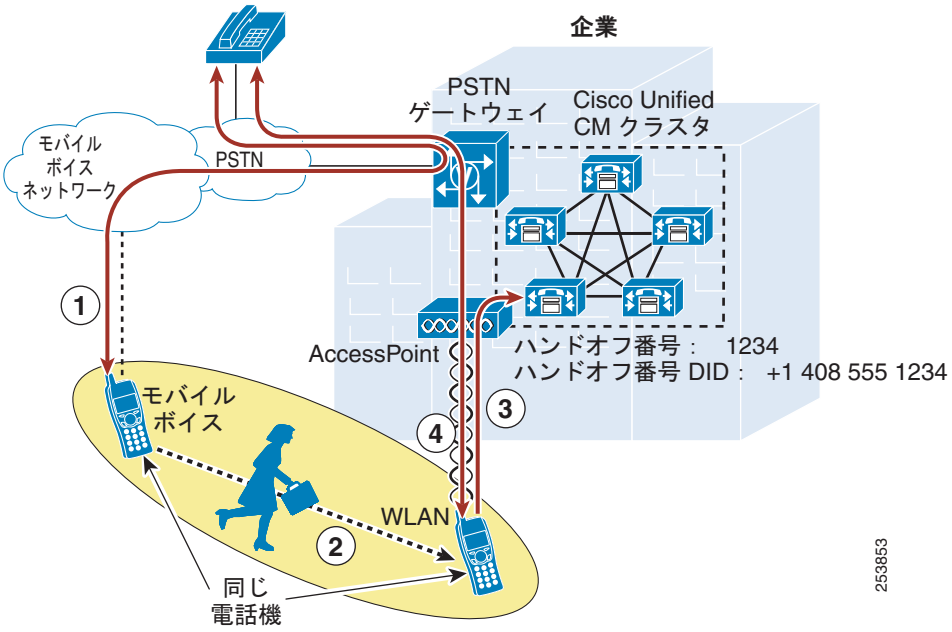
Nokia Call Connect デュアルモード クライアントでは、[Switch to Cellular] または [Handover to GSM] コール中メニュー オプションを使用した手動でのハンドアウトもサポートされています。これらの手動でのハンドアウト方法が利用可能であるかどうか、およびその動作は、デバイス タイプとファームウェアのバージョンに応じて異なります。バージョン 3.1 以前のバージョンのファームウェアが実行されているデバイスでは、[Switch to Cellular] メニュー オプションを選択すると、アクティブなコールが、会社の公衆網ゲートウェイ経由でデバイスのモバイル ボイス ネットワーク インターフェイスにブラインド転送されます。バージョン 3.2 以降のバージョンのファームウェアが実行されているデバイスでは、[Handover to GSM] メニュー オプションを選択すると、[WLAN HO threshold] および [WLAN HO hysteresis] の各 VCC 設定を使用しないで、図 25-18 のステップ 3 に示すように Unified CM のハンドオフ番号を使用した手動ハンドオフが実行されます。

ハンドイン（携帯電話から WLAN へ）

図 25-19 は、社外の Nokia デュアルモード電話機におけるアクティブなコールが、モバイル ボイス ネットワーク インターフェイスから会社の公衆網ゲートウェイ経由でデバイスの WLAN インターフェイスに移動されるハンドイン動作を示しています。図に示すように、モバイル ボイス ネットワーク上の Nokia デュアルモード デバイスと、公衆網ネットワーク上の電話機との間に既存のコールがあります（ステップ 1）。Nokia デュアルモード ユーザが社内に移動し（ステップ 2）、バックグラウンドでデバイスが WLAN インフラストラクチャに関連付けられて、Unified CM に登録されます。登録後、デバイスは、VCC の [WLAN HO hysteresis high] 設定に指定された時間（デフォルトで 60 秒）だけ待機し、1234（VCC の [VoIP Handover number] 設定、Unified CM で設定された Unified CM ハンドオフ番号に対応）へのサイレント バックグラウンド コールを開いたあと、Unified CM に送信します（ステップ 3）。このコールが受信されると、発信元である会社の電話番号と、システムに設定されている

Nokia S60 デュアルモード電話機が照合されて、一致するものがある場合には、モバイル ボイス ネットワーク、公衆網、および会社の公衆網ゲートウェイを通過していたコールが WLAN ネットワークにリダイレクトされ、デュアルモード デバイスと元の公衆網電話機との間のコールは中断されずに継続します（ステップ 4）。

図 25-19　Nokia Call Connect デュアルモード ハンドイン（モバイル ボイス ネットワークから WLAN へ）



Nokia Call Connect の VCC 設定の詳細については、次の Web サイトで入手可能な『*Nokia Call Connect for Cisco User's Guide*』を参照してください。

http://europe.nokia.com/support/download-software/nokia-call-connect-for-cisco

Nokia Call Connect と Cisco Unified Mobility との間の相互作用

Nokia Call Connect デュアルモード クライアントは、Cisco Unified Mobility と統合して、Cisco モバイル コネクト、通話切替 DTMF 機能、2 ステージ ダイヤリング、シングル企業ボイスメール ボックス、およびデスクトップフォンのピックアップを利用できます。

Unified Mobility と統合するには、Unified CM 内で、Nokia デュアルモード電話機の携帯の番号を Nokia S60 デバイスに関連付けられたモビリティ ID として設定する必要があります。システム内で携帯の番号がモビリティ ID として設定されると、Nokia デュアルモード デバイスが社外にあり、Unified CM に登録されていない場合に、モバイル コネクトを利用して、ユーザの会社の電話番号への着信コールをモバイル ボイス ネットワークを経由して Nokia デュアルモード デバイスに転送できます。Nokia デュアルモード デバイスが社内にあり、Unified CM に登録されている状況においては、会社の番号への着信コールはデバイスのモバイル ボイス ネットワーク インターフェイスには転送されません。Nokia デュアルモード デバイスが社内にある場合は、デバイスの WLAN インターフェイスだけが着信コールを受信します。これにより、会社の公衆網ゲートウェイ リソースが必要以上に消費されるのを回避できます。

社外にあり、Unified CM に登録されていない場合、Nokia デュアルモード デバイスでは、会社の任意の固定コールに対して、DTMF を使用して通話切替機能を呼び出したり、デスクトップフォンのピックアップを実行したりできます。また、Nokia デュアルモード デバイスでは、コールを発信する場合にモバイル ボイス アクセスとエンタープライズ機能アクセス 2 ステージ ダイヤリング機能を利用して、これらのコールを会社経由でルーティングし、会社の公衆網ゲートウェイに固定できます。

Nokia デュアルモード デバイスに対してモビリティ ID を設定することに加えて、リモート接続先として追加の携帯電話番号またはオフシステム電話番号を設定して、これらの番号を Unified CM 内の Nokia S60 デバイスに関連付けることができます。モビリティ ID および追加のリモート接続先を Nokia デバイスに関連付ける場合は、リモート接続先プロファイルを設定する必要はありません。

Unified Mobility の機能セット、および設計と配置の考慮事項の詳細については、「Cisco Unified Mobility」（P.25-4）を参照してください。

Nokia Call Connect と Cisco Unified Mobile Communicator との間の相互作用

Nokia Call Connect デュアルモード クライアントは、Nokia 対応の Cisco Unified Mobile Communicator クライアントと並行して使用できます。両方のクライアントが配置された場合、Nokia デバイスからエンタープライズ IP テレフォニー インフラストラクチャを利用して社内でコールを発信および受信できるだけでなく、ディレクトリ検索、デスクトップフォンのコール ログ統合、プレゼンス、ビジュアル ボイスメール、テキスト メッセージング、Dial-via-office などの Unified Mobile Communicator の機能を利用することもできます。

Nokia Call Connect デュアルモード クライアントと Unified Mobile Communicator を統合するには、Unified CM 内の Nokia S60 デバイスの設定ページの [Enable Cisco Unified Mobile Communicator] チェックボックスをオンにします。

Unified CM 内で設定すると、両方のクライアントを Nokia デュアルモード デバイス上で実行できるようになります。ただし、Dial-via-office 機能に対する影響を理解することが重要です。2 つのクライアント内の他のすべての機能は通常どおり動作しますが、Nokia Call Connect クライアントが同じデバイスにインストールされている場合には、Dial-via-office 機能の動作は若干異なります。Unified Mobile Communicator 内の Dial-via-office 機能は、モバイル ボイス ネットワーク（携帯電話インターフェイス）経由でルーティングされたコールに対してだけ実行されます。このため、Nokia Call Connect クライアントから WLAN インターフェイス経由で発信されたコールでは、Dial-via-office は実行されません。この場合コールはすでにエンタープライズ IP テレフォニー インフラストラクチャ経由で発信されているため、これは適切な動作です。

ただし、モバイル ボイス ネットワーク（携帯電話インターフェイス）経由で発信されたコールでは、Unified Mobile Communicator クライアント内の Dial-via-office 設定、または Cisco Unified Mobility Advantage サーバの Dial-via-office 設定に応じて、Dial-via-office 機能が実行されるかどうかが決まります。Unified Mobility Advantage サーバの管理者がユーザに対して Dial-via-office の使用を強制した場合、Unified Mobile Communicator クライアントでは、デバイスの携帯電話インターフェイスから発信されたすべてのコールで Dial-via-office の呼び出しが試みられます。このような状況においては、ユーザは、Unified Mobile Communicator クライアントで設定パラメータ [Allow dial via office for] を [Call from this app] に設定して、Unified Mobile Communicator クライアントから直接発信されたコールでだけ Dial-via-office が呼び出されるようにする必要があります。クライアントをこのように設定することによって、ユーザは、Unified Mobile Communicator クライアントの外部で携帯電話インターフェイス経由でコールが発信された場合に Dial-via-office 機能が実行されないようにすることができます。たとえば、Nokia Call Connect クライアントで企業の WLAN からモバイル ボイス ネットワークへのコールのハンドアウトが試みられている場合には、Nokia デバイスで Dial-via-office を実行することは望ましくありません。ハンドアウト時には、Nokia デュアルモード デバイスの携帯電話インターフェイスから Unified CM ハンドオフ番号に対してコールが発信されます。Dial-via-office が実行されると、追加の不要なコール レッグが作成されて、元のコールのハンドオフに失敗する可能性があります。

同様に、管理者が個々の Unified Mobile Communicator ユーザにクライアント内で独自の Dial-via-office 設定を行うことを許可している場合、ユーザはクライアントを設定して、携帯電話インターフェイス経由でコールの発信が試みられるたびに、直接コールを発信するか、または Dial-via-office を使用して発信するかを選択できるようにすることができます。Unified Mobile Communicator の [When dialing] 設定を [Let me choose] に設定し、[Allow dial via office for] 設定を [Call from this app] に設定することによって、ユーザは、Dial-via-office が使用されるタイミングにつ

いて、各自の意思を最大限反映することができます。いずれの場合でも、ユーザは、Nokia デュアルモード デバイスが社外にあり、Unified CM に登録されていない場合にだけ Dial-via-office を使用する必要があります。

Cisco Unified Mobile Communicator のソリューション、機能セット、および設計と配置の考慮事項の詳細については、「Cisco Unified Mobile Communicator」（P.25-34）を参照してください。

デュアルモード電話機の高可用性

デュアルモード電話機は、その特性上ネットワーク接続に関して非常に高い可用性を備えていますが（企業の WLAN ネットワークが利用できない場合には、モバイル ボイス ネットワークを使用して音声サービスおよびデータ サービスを利用できます）、企業の WLAN および IP テレフォニー インフラストラクチャの高可用性については考慮の余地があります。

まず、企業の WLAN は、冗長な WLAN アクセスが可能になるように配置する必要があります。たとえば、AP およびその他の WLAN インフラストラクチャ コンポーネントは、無線 AP の 1 つに障害が発生しても、デュアルモード デバイスのネットワーク接続には影響がないように配置する必要があります。同様に、常にデュアルモード デバイスがネットワークに安全に接続できるように、WLAN の管理およびセキュリティ インフラストラクチャも高い冗長性を備えた配置にする必要があります。

次に、Unified CM のコール処理サービスおよび登録サービスの高可用性について考慮する必要があります。Unified CM のコール処理サービスを利用する企業内の他のデバイスと同様に、デュアルモード電話機も Unified CM に登録する必要があります。Unified CM クラスタのアーキテクチャにはプライマリおよびバックアップのコール処理サービスおよびデバイス登録サービスが用意されており、冗長な特性を持っているため、1 つの Unified CM サーバ ノードで障害が発生しても、デュアルモード デバイスの登録やコール ルーティングは引き続き利用可能です。

公衆網アクセスについても同様の事項を考慮する必要があります。IP テレフォニー配置と同様、複数の公衆網ゲートウェイおよびコール ルーティング パスを配置して、公衆網への可用性の高いアクセスを確保する必要があります。このことは、デュアルモード電話機の配置に固有の考慮事項ではありませんが、重要な考慮事項です。

デュアルモード電話機のキャパシティ プランニング

デュアルモード電話機におけるキャパシティ プランニングに関する考慮事項は、登録、コール処理、公衆網アクセスなどのサービスのために IP テレフォニー インフラストラクチャおよびアプリケーションを利用する他の IP テレフォニー エンドポイントまたはデバイスと同じです。

社内にデュアルモード電話機を配置する場合、Unified CM における登録の負荷および Unified Mobility の制限について考慮することが重要です。1 つの Unified CM サーバでは、最大 7,500 のデバイスの設定および登録を処理できます。デュアルモード電話機を配置する場合、サーバあたりでサポートされる最大デバイス数を考慮する必要があります。追加の負荷を処理するために、コール処理サブスクライバ ノードを追加で配置する必要がある場合があります。

また、「Cisco Unified Mobility の性能と容量」（P.25-31）で説明したように、1 つの Unified CM クラスタ内のリモート接続先およびモビリティ ID の最大数は 15,000 です。ほとんどのデュアルモード デバイスは、モバイル コネクト、デスクトップフォンのピックアップ、2 ステージ ダイヤリングなどの機能を利用するために Unified Mobility と統合されるため、これらの各デュアルモード デバイスの携帯電話番号は Unified CM クラスタ内にモビリティ ID として設定する必要があります。これは、Unified Mobility との統合を容易にし、一部の場合にはハンドオフを容易にするために必要です。したがって、デュアルモード電話機を Unified Mobility と統合する場合には、Unified CM クラスタにおけるリモート接続先およびモビリティ ID の全体的な容量を考慮して、十分な容量を確保することが重要

です。追加のユーザまたはデバイスがシステム内の Unified Mobility にすでに統合されている場合は、これらのユーザまたはデバイスによって、デュアルモード デバイスで利用可能なリモート接続先およびモビリティ ID の空き容量が制限される可能性があります。

デュアルモード電話機を配置する場合、Unified CM システムおよび公衆網ゲートウェイの全体的なコール処理容量も考慮する必要があります。デュアルモード デバイスの実際の設定および登録を処理する以外に、システムでは、これらの新しいデュアルモード電話機とユーザによって増加する BHCA の影響を吸収するために十分な容量も必要です。同様に、デュアルモード デバイスを処理するのに十分な公衆網ゲートウェイの容量を確保することも重要です。通常、デュアルモード デバイスを持つユーザは頻繁に移動することが多いため、Unified Mobility に統合されているデュアルモード デバイスではこのことは特に重要です。通常、頻繁に移動するユーザは、モバイル ユーザの会社の電話番号への着信コールによって公衆網への 1 つ以上のコールが発信されるモバイル コネクトなどのモビリティ機能や、会社の公衆網ゲートウェイを利用してユーザが会社経由でコールを発信する 2 ステージ ダイヤリングなどを使用することで、会社の公衆網ゲートウェイの負荷を高める傾向にあります。

上記の考慮事項は、デュアルモード電話機に固有のものではありません。これらの考慮事項は、デバイスやユーザが Unified CM に追加されることによって Unified Communications システム全体の負荷が高まるすべての状況に当てはまります。

シスコ代理店と従業員は、Cisco Unified Communications Sizing Tool を使用して、Unified CM を含む Cisco Unified Communications システムの容量を計算できます。この Sizing Tool では、システム全体の容量を計算するための入力としてデュアルモード電話機デバイス数を受け取り、入力された数のデュアルモード デバイスおよびそれらのデバイスがシステムの全体的なサイズに与える影響に対応できる適切なシステム サイズを、デバイスの登録、コール処理（BHCA）、およびゲートウェイの利用負荷に基づいて計算します。システムのサイジングでサポートが必要な場合は、シスコ代理店またはシスコのシステム エンジニア（SE）にお問い合せください。

シスコ代理店と従業員は、Cisco Unified Communications Sizing Tool を http://tools.cisco.com/cucst で入手できます。

デュアルモード電話機の設計上の考慮事項

デュアルモードの電話機とクライアントを配置する場合には、次の設計上の考慮事項を順守してください。

- モバイル ボイス ネットワークとモバイル データ ネットワーク、および WLAN ネットワークの両方に同時に接続するために、デュアルモード電話機では、Dual Transfer Mode（DTM; デュアル転送モード）がサポートされている必要があります。これにより、デバイスの携帯電話無線機と WLAN インターフェイスの両方からデバイスに到達可能になり、両方のインターフェイスでコールを発信および受信できます。モバイル ボイス ネットワークおよびモバイル データ ネットワークでデュアル接続デバイスがサポートされていない場合には、適切なデュアルモード クライアント操作が実行できない場合があります。
- AP は、2.4 GHz（802.11b/g）の配置においては、20% のセル オーバーラップを確保して配置する必要があります。5 GHz（802.11a）の配置におけるチャネル オーバーラップは、15 ～ 20% の範囲である必要があります。このようにオーバーラップさせることによって、デュアルモード デバイスがロケーション内で移動した場合に AP 間で正常にローミングして、ボイス ネットワーク接続およびデータ ネットワーク接続を維持できます。
- パケット損失を最小限に抑えるために、AP は -67 dBm のセル パワー レベル境界（またはチャネル セル半径）で配置する必要があります。また、同一チャネルのセル境界の分離は、約 19 dBm にする必要があります。19 dBm の同一チャネル セル分離は、AP またはクライアントにおいて、同じチャネルに関連付けられている他のデバイスとの同一チャネル干渉が発生しないようにするために重要です。同一チャネル干渉が発生すると、音声品質が低下するためです。

- デュアルモードの電話機とクライアントを接続する場合は、エンタープライズ クラスの音声に最適化された WLAN ネットワークだけを使用することをお勧めします。ほとんどのデュアルモードの電話機とクライアントは、パブリックおよびプライベートの WLAN アクセス ポイントやホットスポットに接続し、インターネットを経由して会社に接続して呼制御やその他の Unified Communications サービスを利用できますが、このように接続した場合の音声品質は保証されません。
- Unified Mobility モバイル コネクト機能では、デュアルモード デバイスが社内にあり、Unified CM に登録されている場合には、着信コールはデュアルモード デバイスの設定されたモビリティ ID には転送されません。これは、企業の公衆網リソースの利用を削減するための仕様です。デュアルモード デバイスは Unified CM に登録されるため、システムでは、デバイスが社内で到達可能であるかどうかを把握できます。社内で到達可能である場合は、コールを公衆網に転送してデュアルモード デバイスのモバイル ボイス ネットワーク インターフェイスを呼び出す必要性がありません。モバイル コネクトでは、デュアルモード デバイスが登録されていない場合にだけ、ユーザの会社の電話番号への着信コールが公衆網のモビリティ ID 番号に転送されます。
- デュアルモード電話機を配置する場合、必要なダイヤリング ストリングを正規化して、ユーザが社内または社外のいずれからでも同じ番号をダイヤルして特定の着信側接続先に到達できるようにすることをお勧めします。モバイル ネットワークにおけるダイヤリングは、通常完全な E.164（先頭に「+」が付く場合と付かない場合があります）を使用して行われ、携帯電話の連絡先は通常完全な E.164 番号で保存されるため、デュアルモード電話機においては、企業のダイヤル プランは完全な E.164 番号または先頭に「+」を付けた完全な E.164 番号を使用できるように設定することをお勧めします。このように企業のダイヤル プランを設定することによって、ユーザはデバイスが社内の Unified CM に登録されているかどうかを気にする必要がなくなるため、最善のエンドユーザ ダイヤリング エクスペリエンスを提供できます。
- デュアルモード電話機のユーザが緊急コールを発信し、デバイスおよびユーザの位置を特定する場合には、モバイル ボイス ネットワークを利用することをお勧めします。これは、通常モバイル プロバイダー ネットワークでは、企業の WLAN ネットワークよりもはるかに信頼性のある位置情報が提供されるためです。デュアルモード電話機から緊急コールを発信したり位置サービスを利用したりする場合にモバイル ボイス ネットワークだけが利用されるように、Unified CM 内でデュアルモード デバイスを設定して、911、999、112 などの緊急番号へのコールを許可するルート パターンにこれらのデバイスからアクセスできないようにします。デュアルモード電話機のユーザに対して、すべての緊急コールを企業ネットワークではなくモバイル ボイス ネットワーク経由で発信するように指示します。
- Cisco Mobile iPhone デュアルモード クライアントおよび Cisco Unified Mobile Communicator iPhone クライアントの両方が同じハンドセットに配置されている状況においては、次のことをお勧めします。
  - Unified CM 内でデュアルモード電話機を Cisco Dual-Mode for iPhone として設定し、iPhone の携帯の番号を関連するモビリティ ID として設定します。モビリティ ID はシステム内で一意である必要があるため、Unified CM 内で対応する Cisco Unified Mobile Communicator クライアント デバイスを設定しないでください。
  - Dial-via-office は、Unified CM 7.1(5) を実行しており、[Enable Cisco Unified Mobile Communicator] チェックボックスがオンの場合にだけ有効化および利用します。Unified CM 7.1(3) を実行している場合、Dial-via-office とデュアルモード クライアントのいずれか一方だけを使用できます。
  - 社内ディレクトリ検索およびビジュアル ボイスメールには、Cisco Unified Mobile Communicator クライアントを使用します。Cisco Mobile iPhone デュアルモード クライアントにも同様の機能が備えられていますが、Cisco Unified Mobile Communicator クライアントの方が機能が豊富で、よりよいユーザ エクスペリエンスが提供されます。

- Nokia Call Connect デュアルモード クライアントと Cisco Unified Mobile Communicator Nokia クライアントの両方が同じハンドセットに配置されている状況においては、デュアルモード デバイスが社内にあり、Unified CM に登録されている場合に Dial-via-office を使用しないでください。次のことをお勧めします。
  - 企業にデュアルモード電話機を配置する場合、Cisco Unified Mobility Advantage Server の管理者は、[Dial Via Office Policy] 設定を使用して Dial-via-office の使用を強制しないでください。代わりに、Dial-via-office を使用するかどうかをユーザが選択できるようにする必要があります。
  - Cisco Unified Mobility Advantage サーバの管理者によって Cisco Unified Mobile Communicator における Dial-via-office の使用が強制されている場合、ユーザは Unified Mobile Communicator クライアント内で [Allow dial via office for] 設定を [Call from this app] に設定して、Unified Mobile Communicator クライアント内から直接発信されたコールでだけ Dial-via-office の呼び出しが試みられるようにする必要があります。クライアントをこのように設定することによって、ユーザは、予期せず Dial-via-office が実行されないようにすることができます。Unified Mobile Communicator クライアントがフォアグラウンドで実行されていない場合、Dial-via-office は呼び出されません。
  - Unified Mobility Advantage の管理者によって Dial-via-office の使用が強制されていない場合、Unified Mobile Communicator ユーザは、[When dialing] 設定を [Let me choose] に、[Allow dial via office for] 設定を [Call from this app] に設定する必要があります。このように設定することによって、ユーザは、Dial-via-office が使用されるタイミングについて、各自の意思を最大限反映することができます。いずれの場合でも、ユーザは、Nokia デュアルモード デバイスが社外にあり、Unified CM に登録されていない場合にだけ Dial-via-office を使用する必要があります。
- デュアルモード デバイスにおいて、ビジネス コールの発信および受信時に可能なかぎりエンタープライズ IP テレフォニー インフラストラクチャが使用されるようにするために、次の Nokia Call Connect クライアント設定を行うことをお勧めします。
  - Nokia Call Connect クライアントの SCCP 登録設定を [Always On] に設定して、Nokia デバイスが企業の WLAN ネットワークに関連付けられた場合に Unified CM への登録が試みられるようにします。
  - Nokia デュアルモード電話機の優先コール タイプまたはデフォルト コール タイプの設定を [Internet Call] に設定して、Nokia Call Connect クライアントが Unified CM に登録された場合に、デバイスからの発信コールにおいて常にデュアルモード電話機の WLAN インターフェイス経由でルーティングが試みられるようにします。

CHAPTER 26

Network Management

Last revised on: June 4, 2010

Network management is a service consisting of a wide variety of tools, applications, and products to assist network system administrators in provisioning, operating, monitoring and maintaining new and existing network deployments. A network administrator faces many challenges when deploying and configuring network devices and when operating, monitoring, and reporting the health of the network infrastructure and components such as routers, servers, switches and so forth. Network management helps system administrators monitor each network device and network activity so that they can isolate and investigate problems in a timely manner for better performance and productivity.

With the convergence of voice and data, the need for unified management is apparent. The Cisco Unified Communications Management Suite offers a set of integrated tools that help to test, deploy, and monitor the Cisco Unified Communications system. A network manager implements the various management phases to strategically manage the performance and availability of Cisco Unified Communications applications including voice, video, contact center, and rich media applications. The network management phases typically include: plan, design, implement, and operate (PDIO). Table 26-1 lists the PDIO phases and the major tasks involved with each phase.

Table 26-1 Network Management Phases and Tasks

Plan & Design	Implement	Operate
Assess the network infrastructure for Cisco Unified Communications capability. (For example, predict overall call quality.) Prepare the network to support Cisco Unified Communications. Analyze network management best practices.	Deploy and provision Cisco Unified Communications. (For example, configure the dial plan, partitioning, user features, and so forth.) Enable features and functionality on the existing infrastructure to support Cisco Unified Communications. (For example, configure voice ports, gateway functionality on routers, and so forth.)	Manage changes for users, services, IP phones, and so forth. Generate reports for operations, capacity planning, executive summaries, and so forth. Track and report on user experiences. (For example, use sensors to monitor voice quality.) Monitor and diagnose problems such as network failures, device failures, call routing issues, and so forth.

This chapter provides the design guidance for the following management tools and products that fit into the implementation and operation phases of Cisco Unified Communications Management:

- Implement & Operate
  - Cisco Unified Provisioning Manager (Unified PM) manages provisioning of initial deployments and ongoing operational activation for IP communications services.
- Operate
  - Cisco Unified Operations Manager (Unified OM) provides comprehensive monitoring with proactive and reactive diagnostics for the entire Cisco Unified Communications system.
  - Cisco Unified Service Monitor (Unified SM) provides a reliable method of monitoring and evaluating voice quality in Cisco Unified Communications systems.
  - Cisco Unified Service Statistics Manager (Unified SSM) provides advanced statistics analysis and reporting capabilities for Cisco Unified Communications deployments.

For a complete list of the features supported by each product, refer to the related product documentation available at http://www.cisco.com.

For information on which software versions are supported with Cisco Unified Communications Manager (Unified CM) 7.*x*, refer to the *Cisco Unified Communications Manager Software Compatibility Matrix*, available at

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html

What's New in This Chapter

Table 26-2 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 26-2 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:
Cisco Unified SM integration with the Network Analysis Module (NAM)	Cisco Network Analysis Module (NAM), page 26-10
Co-residency of Cisco Unified PM, Unified OM, Unified SM, and Unified SSM for up to 10,000 phones	Integration with Cisco Unified Communications Deployment Models, page 26-21
Server performance	Unified SM Server Performance, page 26-12 Cisco Unified Provisioning Manager Server Performance, page 26-20
Support for 45,000 phones for standalone Cisco Unified OM, Unified SM, and Unified SSM deployments	Integration with Cisco Unified Communications Deployment Models, page 26-21
Support for 60,000 phones for standalone Cisco Unified PM	Integration with Cisco Unified Communications Deployment Models, page 26-21

Table 26-2 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:
The information about Cisco Monitor Manager, Monitor Director, and netManager has been removed from this document.	No longer described in this document
VMware support for the Cisco Unified Communications Management Suite	Integration with Cisco Unified Communications Deployment Models, page 26-21

Network Infrastructure Requirements for Cisco Unified Network Management Applications

A well designed network is the foundation for operating and managing a Cisco Unified Communications network. The Cisco Unified Communications network must conform to the following strict requirements:

- Average IP packet loss <= 1%
- Average delay variation (jitter) <=30 ms
- Average one-way packet delay <=150 ms

Domain Name Service (DNS) must be enabled in the network to perform a reverse lookup on the IP address of the device to get the hostname for the device. If DNS is not desired, then host files may be used for IP address-to-hostname resolution.

Network Time Protocol (NTP) must be implemented to allow network devices to synchronize their clocks to a network time server or network-capable clock. NTP is a critical network service for network operation and management because it ensures accurate time-stamps within all logs, traps, polling, and reports on devices throughout the network.

Cisco Discovery Protocol (CDP) must be enabled within the network to ensure proper monitoring. Unified OM's automated device discovery is based on a CDP table. Ping Sweep may be used instead of CDP, but IP phones discovered using Ping Sweep are reported in "unmanaged" state. Simple Network Management Protocol (SNMP) must also be enabled on network devices to allow network management applications such as Unified OM, Cisco Monitor Manager, and Cisco Monitor Director to get information on network devices at configured polling intervals and to receive alerts and faults via trap notification sent by the managed devices.

Server platforms with dual Ethernet network interface cards (NICs) can support NIC teaming for Network Fault Tolerance with Unified OM. This feature allows a server to be connected to the Ethernet via two NICs and, therefore, two cables. NIC teaming prevents network downtime by transferring the workload from the failed port to the working port. NIC teaming cannot be used for load balancing or increasing the interface speed.

Trivial File Transfer Protocol (TFTP) must be enabled in the network to provide the Cisco 1040 Sensor with a TFTP-based process to download its configuration files.

For more information on Cisco Unified Communications network requirements, see the chapter on ネットワーク インフラストラクチャ , page 3-1.

Cisco Unified Operations Manager

Cisco Unified Operations Manager (Unified OM) provides a unified view of the entire Cisco Unified Communications infrastructure and presents the current operational status of each element of the Cisco Unified Communications network. Unified OM also provides diagnostic capabilities for faster problem isolation and resolution. In addition to monitoring Cisco gateways, routers, and switches, Unified OM continuously monitors the operational status of various Cisco Unified Communications elements such as:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unified Communications Manager Express (Unified CME)
- Cisco Unity and Unity Connection
- Cisco Unity Express
- Cisco Unified Contact Center Enterprise (Unified CCE), Unified Contact Center Express (Unified CCX), and Unified Customer Voice Portal (Unified CVP)

Note Cisco Operations Manager Service Level View does not support multiple Cisco Unified System Contact Center Enterprise (SCCE) deployments.

- Cisco Unified Presence
- Cisco Emergency Responder
- Cisco Unified MeetingPlace (Unified MP) and Unified MeetingPlace Express (Unified MPE)
- Cisco Unified IP Phones

For more information on the products and versions supported by Unified OM, refer to the Cisco Unified Operations Manager data sheet available at http://www.cisco.com.

Unified OM monitors the network using Simple Network Management Protocol (SNMP). SNMP is an application-layer protocol using UDP as the transport layer protocol. There are three key elements in SNMP managed network:

- Managed devices — Network devices that have an SNMP agent (for example, Unified CM, routers, switches, and so forth).
- Agent — A network management software module that resides in a managed device. This agent translates the local management information on the device into SNMP messages.
- Manager — Software running on a management station that contacts different agents in the network to get the management information (for example, Unified OM).

The SNMP implementation supports three versions: SNMP v1, SNMP v2c, and SNMP v3. SNMP v3 supports authentication, encryption, and message integrity. SNMP v3 may be used if security is desired for management traffic. Unified OM supports all three versions of SNNP. SNMP v1 and v2c read/write community strings or SNMP v3 credentials must be configured on each device for agent and manager to communicate properly. Unified OM needs only SNMP read access to collect network device information.

For more information on SNMP, refer tot he documentation available at http://www.cisco.com.

Cisco Unified Operations Manager Design Considerations

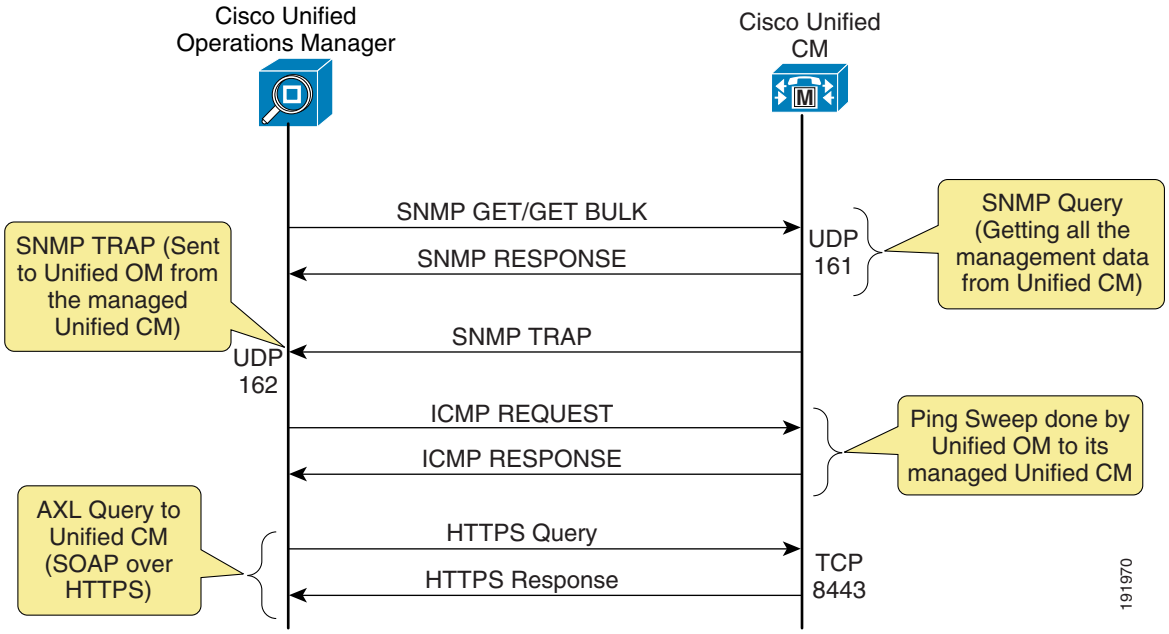
Unified OM interfaces with other devices in the network in the following ways:

- Simple Network Management protocol (SNMP) to manage all Cisco Unified Communications servers.
- AVVID XML layer (AXL) to manage Unified CM. AXL is implemented as a Simple Object Access Protocol (SOAP) over HTTPS web service.
- Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP) to Cisco Unified IP Phones for synthetic tests.
- Internet Control Message Protocol (ICMP) or Ping Sweep for Cisco IOS routers and switches, and for other voice as well as non-voice devices.
- HTTP to the IP phone through Unified CM. Unified OM does not communicate with the IP phone directly, but does so through Unified CM. Thus, HTTP must be configured for Unified CM.
- Syslog for Unified CM faults.
- Windows Management Instrumentation (WMI) for Windows-based PCs and servers.
- Enhanced event processing with Cisco Unified CM remote syslog integration and leveraging Cisco Real-Time Monitoring Tool (RTMT) pre-collected data

Figure 26-1 shows the system-level overview of Unified OM integrated with Unified CM.

Note Cisco Unified Operations Manager supports only SNMP polling and traps. Syslog messages are not supported by the Unified OM server.

Figure 26-1 Unified OM and Unified CM System-Level Integration



Failover and Redundancy

Unified OM provides a choice of the following optional failover and redundancy configurations:

- Warm standby — All unified OM servers are active and polling
- Cold standby — Only one Unified OM server is active and polling

In warm standby mode, one backup Unified OM server can be deployed in the network. All the Unified OM servers are actively polling or collecting information from the network devices. Cisco recommends having a default polling interval on one of the active Unified OM servers, which is referred to as the primary Unified OM server. All the other active or secondary Unified OM servers must be configured with a longer polling interval (for example, 15 minutes). This will help reduce the bandwidth needed for management data as well as prevent the managed devices from frequently responding to SNMP queries from multiple Unified OM servers. A higher-level "manager of managers" must be used to manage multiple Unified OM servers. If the primary Unified OM server fails, the polling interval on the secondary Unified OM server can be reduced to resume normal operation and collection of data.

In cold standby mode, two or more Unified OM servers can be deployed in the network. Only one Unified OM server is actively polling or collecting information from the network devices. Cisco recommends having a default polling interval on the active Unified OM server. which is referred as the primary Unified OM server. All the other secondary Unified OM servers are configured, but polling is disabled on these servers. A higher-level "manager of managers" must be used to manage multiple Unified OM servers. If the primary Unified OM server fails, the polling on the secondary Unified OM server can be enabled to resume normal operation and collection of data.

In both modes, the secondary servers must be backed up periodically with the configuration on the primary servers. This keeps all the servers in synchronization with the configuration and reduces downtime if the primary Unified OM server fails.

Ports and Protocols

Table 26-3 lists the ports used by the various protocol interfaces for Cisco Unified Operations Manager. Cisco recommends opening these ports in the corporate firewall to allow communication between Unified OM and other devices in the network.

Table 26-3 Unified OM Port Utilization

Protocol	Port	Service
UDP	161	SNMP polling
UDP	162	SNMP traps
TCP	80	HTTP
TCP	443	HTTPS
TCP	1741	CiscoWorks HTTP server
UDP	514	Syslog
TCP	8080	Determining status of Unified CM web service
TCP	8443	SSL port between Unified CM and Unified OM

All the management traffic (SNMP) originating from Unified OM or managed devices is marked with a default marking of DSCP 0x00 (PHB 0). The goal of network management systems is to respond to any problem or misbehavior in the network. To ensure proper and reliable monitoring, network management

data must be prioritized. Implementing QoS mechanisms ensures low packet delay, low loss, and low jitter. Cisco recommends marking the network management traffic with an IP Precedence of 2, or DSCP 0x16 (PHB CS2)

If managed devices are behind a firewall, the firewall must be configured to allow management traffic. Unified OM has limited support in a network that uses Network Address Translation (NAT). Unified OM must have IP and SNMP connectivity from the Unified OM server to the NAT IP addresses for the devices behind the NAT. A single Unified OM server cannot manage duplicate IP addresses across NAT domains. If overlapping IP address ranges exist, then a separate Unified OM server must be deployed for each NAT domain.

Bandwidth Requirements

Unified OM polls the managed devices for operational status information at every interval configured, and it has the potential to contain a lot of important management data. Bandwidth must be provisioned for management data, especially if you have a lot of managed devices over a low-speed WAN. The amount of traffic will vary for different types of managed devices. For example, more management messages may be seen when monitoring a Unified OM as compared to monitoring a Cisco Voice Gateway. Also, the amount of management traffic will vary if the managed devices are in a monitored or partially monitored state and if any synthetic tests are performed.

Cisco Unified Operations Manager Server Performance

Unified OM is supported in single-server mode. However, multiple Unified OM servers can be deployed to manage large networks. Each Unified OM can be configured to send management information to a higher-level “manager of managers”. For hardware requirements and capacity information for Unified OM, refer to the *Cisco Unified Operations Manager Data Sheet*, available at

http://www.cisco.com/en/US/products/ps6535/products_data_sheets_list.html

Cisco Unified Service Monitor

Cisco Unified Service Monitor (Unified SM) monitors voice quality of calls on the Cisco Unified Communications network. It relies on Unified CM, the Cisco 1040 Sensor, and the Network Analysis Module (NAM) to monitor and gather voice quality statistics on real calls rather than simulated calls in the network. Then it compares the collected voice quality statistics against a predefined Mean Opinion Score (MOS) threshold. If the voice quality falls below the threshold, Unified SM sends SNMP trap messages to Unified OM to indicate that a potential issue has been identified. Unified SM is also responsible for sending voice quality information to Cisco Unified Service Statistics Manager (Unified SSM) so that Unified SSM can perform call data analysis and generate reports.

Note A set of global call quality thresholds can be defined in Unified SM, one per supported codec type. Different thresholds can be grouped together based on the Cisco 1040 Sensor being implemented or the Unified CM cluster being monitored. Unified SM is bundled with Unified OM, and you may choose to install both Unified OM and Unified SM.

Voice Quality Measurement

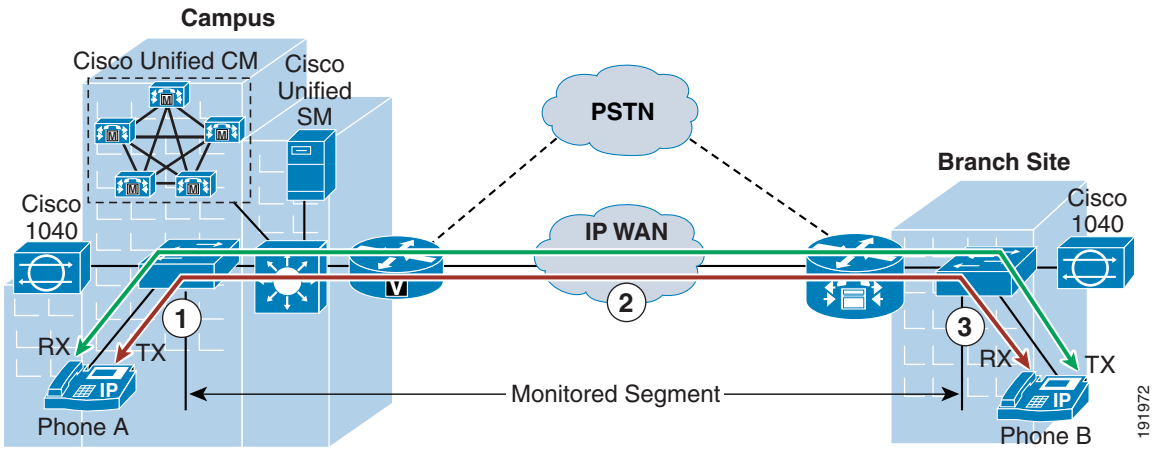
Voice quality is the qualitative and quantitative measure of the sound and conversational quality of the IP phone call. Voice quality measurement describes and evaluates the clarity and intelligibility of voice conversations. Unified SM uses the Cisco 1040 Sensor and Unified CM to monitor and report voice quality information.

Cisco 1040 Sensor Voice Quality Monitoring

The Cisco 1040 Sensor is a hardware device that predicts a subjective quality rating that an average listener might experience on the VoIP calls. It operates by measuring various quality impairment metrics that are included in the IP header of RTP streams, such as packet loss, delay, jitter, and concealment ratio. This computed quality rating is converted to a MOS value. The MOS value is included in Syslog messages that are sent to Unified SM every 60 seconds, thus the Cisco 1040 Sensor monitors the voice quality almost on a real-time basis.

The Cisco 1040 Sensor has two Fast Ethernet interfaces, one of which is used to manage the sensor itself and the other is connected to the Switch Port Analyzer (SPAN) port on the Cisco Catalyst switch to monitor the actual RTP streams. In order to monitor voice quality of calls across the WAN, you must deploy a pair of Cisco 1040 Sensors at both sides of the WAN cloud, as illustrated in Figure 26-2.

Figure 26-2 Voice Quality Monitoring with the Cisco 1040 Sensor



There are two call legs, transmitting and receiving, for each phone. Each call leg can be divided into three segments along the call path. For example, for the transmitting call leg of phone A in Figure 26-2, segment 1 runs between phone A and the campus access switch, segment 2 is between the two access switches, and segment 3 is between the access switch at the branch site and phone B. Both segments 1 and 3 are within a local area network, which presents the fewest transmission impairments to voice quality. Therefore, it is reasonably safe to assume that voice quality degradation will not occur in these two segments, and it is unnecessary to monitor those RTP streams.

Segment 2 spans across the WAN circuit and several network devices along the call path. It is more likely to experience degradation of voice quality due to packet loss, delay, and jitter inherent in the WAN. Therefore, the RTP streams (from campus to branch) should be monitored by the Cisco 1040 Sensor at the branch site. By the same token, the sensor in the central site should monitor the incoming RTP streams in that segment across the WAN. These RTP streams provide important voice quality statistics, and their associated MOS values should be analyzed carefully.

Strategic vs. Tactical Monitoring

There are two strategies for deploying Cisco 1040 Sensors: strategic monitoring and tactical monitoring. With strategic monitoring, the Cisco 1040 Sensor is deployed to continuously monitor all or subsets of IP phones in the network. With tactical monitoring, the Cisco 1040 Sensor is deployed in a site where a voice quality issue has been identified. The Cisco 1040 Sensor complies with FCC Class-B standards, and it can be deployed easily in the enterprise environment.

In a small network, Cisco recommends deploying strategic monitoring to monitor all IP phones on a continuous basis. In a medium to large network, Cisco recommends deploying strategic monitoring to continuously monitor a subset of IP phones, while using tactical monitoring to troubleshoot any voice quality issues experienced by the rest of the IP phones.

Design Considerations for the Cisco 1040 Sensor

Consider the following design factors when deploying a Cisco 1040 Sensor:

- A Cisco 1040 Sensor can monitor 100 simultaneous RTP streams. By monitoring the incoming RTP stream only, as illustrated in Figure 26-2, the Cisco 1040 Sensor can provide the full benefit of monitoring 100 (instead of 50) simultaneous voice calls. An environment with a high call volume tends to require the use of more Cisco 1040 Sensors.
- If there are more RTP streams than the Cisco 1040 Sensor can handle, the Cisco 1040 Sensor will perform sampling of those RTP streams, and the resulting MOS value will be diluted. Cisco recommends that you do not operating the Cisco 1040 Sensor in sampling mode because doing so will result in an inaccurate MOS value.
- The Cisco 1040 Sensor utilizes the Cisco Catalyst switch's SPAN port to monitor the actual RTP streams. Different types of Catalyst switches have different quantities of SPAN ports that can be configured. For example, a maximum of two SPAN ports can be configured on the Cisco Catalyst 6500 and 4500 switches, while the maximum limit for Cisco Catalyst 3550 switch is only one. Therefore, the types of Catalyst switches that have been deployed in the network will determine how many Cisco 1040 Sensors can be deployed.
- If there is a trunking connection between multiple Cisco Catalyst switches and if the call volume is low, there is no need to deploy a Cisco 1040 Sensor for every Catalyst switch. Remote Switch Port Analyzer (RSPAN) can be used so that a single Cisco 1040 Sensor can monitor IP phones on other switches within the same VLAN.
- It is inefficient to deploy a Cisco 1040 Sensor at every site that has just a few IP phones and a small call volume. In such cases, Cisco Enhanced Switched Port Analyzer (ESPAN) can be used so that one Cisco 1040 Sensor can monitor voice streams across multiple networks.

Unified CM Voice Quality Monitoring

Unified CM utilizes the Cisco Voice Transmission Quality (CVTQ) algorithm to monitor voice quality. CVTQ is based on the Klirrfaktor (K-factor) method to estimate the MOS value of voice calls. At the end of each call, Unified CM stores the MOS value in Call Detail Records (CDRs) and Call Management Records (CMRs), which are transferred to Unified SM via Secure File Transfer Protocol (SFTP) every 60 seconds. In order to integrate with Unified CM, Unified SM must be configured as a Billing Application Server in the Unified CM Unified Serviceability configuration web page. Up to three Billing Application Servers can be configured per Unified CM cluster. The following settings must be configured for the Billing Application Server:

- Hostname or IP address of the Unified SM server
- Username and password for SFTP file transfer
- Protocol: SFTP
- Directory path on the Unified SM server to which CDR and CMR files are transferred

CVTQ is supported natively by Unified CM 7.*x* and Cisco Unified IP Phones running in both SCCP and SIP modes. The phone models that support CVTQ include Cisco Unified IP Phones 7906G, 7911G, 7931G, 7940G, 7941G, 7941G-GE, 7942G, 7945G, 7960G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 7971G-GE, and 7975G.

As a comparison to the Cisco 1040 Sensor, which performs a full-depth inspection on various quality impairment metrics, the K-factor method inspects only one dimension of quality impairments, packet loss, which is really a network effect. Thus, CVTQ is a less sophisticated algorithm than the one that the Cisco 1040 Sensor uses to monitor the quality of calls. Cisco recommends using CVTQ to flag a voice quality issue and using the Cisco 1040 Sensor to validate and troubleshoot the issue.

Cisco Network Analysis Module (NAM)

Cisco NAM is a traffic analysis module that leverages Remote Monitoring (RMON) and some SNMP Management Information Bases (MIBs) to enable network administrators to view all layers of the Unified Communications infrastructure to monitor, analyze, and troubleshoot applications and network services such as QoS for voice and video applications. Voice instrumentation added in Cisco NAM 4.0 enables NAM integration with Unified SM 2.2 for call metrics through NAM-embedded data collection and performance analysis.

The Cisco NAM complements the Cisco Unified Communications Management Suite to deliver an enterprise-wide voice management solution. Cisco NAMs are available in different configurations for Cisco Catalyst 6000 Series, 7600 Series, and Integrated Services Routers. The NAM Appliances come with a graphical user interface for troubleshooting and analysis, and they provide a rich feature set for voice quality analysis with RTP and voice control and signaling monitoring. Table 26-4 lists the maximum number of concurrent RTP streams that each type of NAM can support.

Table 26-4 Number of Supported Concurrent RTP Streams per NAM Type

Cisco NAM Type	1040 Sensor	NME-NAM	NAM-2	NAM 2204 Appliance	NAM 2220 Appliance
Number of concurrent RTP streams supported	100	100	400	1500	4000

Unified SM polls the NAM every 60 seconds for voice quality metrics. Unified SM consolidates the data collection module for both the Cisco 1040 Sensor and NAM, and it uses the same method for MOS calculation on both the Cisco 1040 Sensor and NAM. This enables Unified SM to correlate CDR and call stream reports from the Cisco 1040 Sensor and NAM for enhanced analysis.

For more information on Cisco NAM, refer to the following site:

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

Comparison of Voice Quality Monitoring Methods

Cisco 1040 Sensors, CVTQ, and NAM complement each other and provide a total solution for voice quality measurement. The following list notes key differences between voice quality monitoring with the Cisco 1040 Sensor, CVTQ, and Cisco NAM:

- The Cisco 1040 Sensor monitors voice calls based on packet loss, delay, jitter, and concealment ratio. CVTQ monitors voice calls based on packet loss only.
- The Cisco 1040 Sensor and Cisco NAM provide voice quality statistics every 60 seconds. CVTQ provides voice quality statistics after the call is completed.
- The Cisco 1040 Sensor is compatible with all Cisco Unified CM releases and all types of endpoints connecting to the Cisco Catalyst switch. CVTQ supports only Unified CM 4.2 and later releases.
- For inter-cluster calls, the Cisco 1040 Sensor monitors the end-to-end call segment. CVTQ monitors only the call segment within its own cluster.
- Cisco recommends using the Cisco 1040 Sensor to monitor key IP phone devices, gateway devices, and application servers in the network and to investigate and troubleshoot voice quality issues. CVTQ-based voice quality monitoring should be used to gauge the overall voice call quality in the network.

Even if CVTQ is not used, Unified SM uses CDR information to correlate with the NAM report for the following metrics:

- Source and/or destination extension number
- Device types
- Interface through which the call flowed in case of a call to or from a gateway
- Call disconnect reason, where possible
- Exact Unified CM (not just the Unified CM cluster) to which the phone is connected

Failover and Redundancy

A primary and secondary Unified SM can be configured to provide redundancy and failover support to the Cisco 1040 Sensor. After missing three consecutive SCCP keepalive messages from the primary Unified SM, the Cisco 1040 Sensor will try to register with the secondary Unified SM. The Cisco 1040 Sensor will also send Syslog messages to the secondary Unified SM after the registration failover process succeeds.

You can configure up to three Unified SMs, or Billing Application Servers, in Unified CM. Failure of one Unified SM will not preventing the remaining two servers from obtaining CDR and CMR files from Unified CM.

Note The Unified CM publisher server is responsible for transferring CDR and CMR files to Unified SM via SFTP. If the publisher server is unavailable, there is no failover mechanism for Unified SM to obtain the new CDR and CMR files that contain MOS values of calls in the Unified CM cluster. The Cisco Network Analysis Module (NAM) does not provide a secondary Unified SM for failover or high availability support.

Unified SM Server Performance

Unified SM operates only in single-server mode. However, multiple Unified SMs (all connected to Cisco Unified Operations Manager) can be deployed to manage large networks. For hardware requirements and information about Unified SM, refer to the *Cisco Unified Service Monitor Data Sheet*, available at

http://www.cisco.com/en/US/products/ps6536/products_data_sheets_list.html

Unified SM supports the following voice quality monitoring capacities:

- Unified SM supports up to 50 Cisco 1040 Sensors.
- Unified SM supports up to 45,000 IP phones
- Unified SM supports any of the following scenarios:
  - 5,000 sensor-based RTP streams per minute (with Cisco 1040 Sensors or NAM modules)
  - 1,600 CVTQ-based calls per minute
  - 1,500 RTP streams and 666 CVTQ calls per minute
- There is no explicit limit on number of NAM modules or Cisco 1040 Sensors you can have in your system.
- Unified SM automatically selects and monitors all Cisco Unified IP Phones configured in a given Unified CM cluster, and there is no configuration option to monitor only certain IP phones in the cluster.

Note When Unified SM is operating at full capacity, its projected database growth (for Syslog, CDR, and CMR files) is estimated to be about 2.4 GB per day.

Ports and Protocol

Table 26-5 lists the ports used by the various protocol interfaces for Cisco Unified Service Monitor. Cisco recommends opening these ports in the corporate firewall to allow communication between Unified SM and other devices in the network.

Table 26-5 Unified SM Port Utilization

Protocol	Port	Service
TCP	80	HTTP
TCP	443	HTTPS
TCP	1741	CiscoWorks HTTP server
UDP	22	SFTP

Table 26-5 Unified SM Port Utilization (continued)

Protocol	Port	Service
UDP	162	SNMP traps
TCP	43459	Database
UDP	5666	Syslog[1]
TCP	2000	SCCP[2]
UDP	69	TFTP[3]

1. Unified SM receives Syslog messages from the Cisco 1040 Sensor.
2. Unified SM communicates with the Cisco 1040 Sensor via SCCP.
3. The Cisco 1040 Sensor downloads its configuration file via TFTP.

Note The Cisco NAM is accessed remotely over HTTPS with a non-default port. Unified SM will authenticate with each Cisco NAM and maintain the HTTP/S session.

Cisco Unified Service Statistics Manager

The Cisco Unified Service Statistics Manager (Unified SSM) performs advanced call statistics analysis and generates reports for executives, operations, and capacity planning functions. Unified SSM is fully dependent on Unified OM and Unified SM to obtain call statistics information; therefore, Unified OM and Unified SM must be implemented and operating before you deploy Unified SSM. Unified SSM provides both out-of-the-box reports as well as customizable reports that provide visibility into key metrics such as call volume, service availability, call quality, resource utilization, and capacity across the Cisco Unified Communications system. For the detailed information on feature support and functionality, refer to the Cisco Unified Service Statistics Manager product documents available at http://www.cisco.com.

Integration with Unified OM and Unified SM

Unified SSM can integrate with only one Unified OM but multiple Unified SMs. Unified SSM extracts call statistics data from Unified OM and Unified SM databases. The data extraction process is performed by the Unified SSM agent.

The Unified SSM agent facilitates communication between Unified SSM and Unified OM or Unified SM, and it is responsible for transmitting call statistics data from Unified OM or Unified SM to Unified SSM. Unified SSM then stores the extracted data in its own SQL database.

If Unified OM and Unified SM are deployed on the same Cisco Media Convergence Server (MCS) as Unified SSM, there is no need to install the Unified SSM agent on Unified OM or Unified SM. With such a co-resident deployment, Unified SSM is able to extract call statistic data directly from the Unified OM and Unified SM databases instead of transferring the data across the network.

If Unified OM and Unified SM are deployed separately from Unified SSM, then the Unified SSM agent must be installed on every instance of Unified OM and Unified SM. The executable installation file of the Unified SSM agent can be downloaded from the Unified SSM Web Administration page and installed locally on Unified OM and Unified SM. With Unified SSM agents distributed on Unified OM

and Unified SM, Unified SSM is able to control and manage the data extraction process. Unified SSM connects all distributed Unified SSM agents via TCP on port 12124, and Unified SSM agents send call statistics data back to Unified SSM via TCP on port 12126.

There are two different data collection approaches within Unified SSM. The first approach is called *raw data collection*. With this approach, Unified SSM instructs the Unified SSM agent to retrieve all call statistics data directly from the Unified OM and Unified SM databases. All retrieved data is then saved in Unified SSM's database for up to 30 days. The advantage of this approach is that it provides Unified SSM with a comprehensive data source to perform detailed analysis and report generation.

The second approach is called *monitor-based data collection*. With this approach, Unified SSM instructs the Unified SSM agent to transfer the processed call statistics data only. The advantage of this approach is fewer traffic loads over the network, and the processed data can be stored in the Unified SSM database for up to three months. In order to process the original call statistics data in the Unified OM and Unified SM databases, a specific monitor instance must be created in the Unified SSM Administration console and that monitor instance must be associated with the appropriate Unified SSM agent. The monitor instance extracts only the data based on predefined attributes. For example, for Call Volume Monitor, the attributes include number of completed calls on-net, number of failed calls on-net, average duration per call on-net, and so forth. Each monitor instance has a unique list of predefined attributes. The monitor instance then polls and extracts the data every 15 minutes, and the Unified SSM agent aggregates the processed data from its associated monitor instance(s) and send it to Unified SSM every 30 minutes.

For a comprehensive list on all attributes of each monitor type and its configuration guidelines, refer to the Cisco Unified Service Statistics Manager product documents available at http://www.cisco.com.

Note Currently there is no redundancy or failover support with Unified SSM. Unified SSM can still provide reports for more than three months because data is not completely purged but is summarized or aggregated and kept in the Sybase database. Unified SSM must retain the raw data for up to 30 days on the co-resident server.

The following guidelines summarize the integration options for Unified SM, Unified OM, and Unified SSM:

- Unified SSM and Unified OM integrate 1 to 1.
- Unified SSM and Unified SM integrate 1 to 5.
- The Unified SM diagnostics page can launch the Unified OM device detail page for phones and gateways.
- Unified OM reports voice quality details for the NAM. Cross Launch to the NAM user interface from Unified OM quality alerts is supported.
- Unified SM integrates with the Unified OM Service Quality alert dashboard.
- Unified SM integrates with Unified SSM long-term reporting and trending functions.

Unified SSM Server Performance

Unified SSM operates only in a single-server mode. For hardware requirements and information about Unified SSM, refer to the *Cisco Unified Service Statistics Manager Data Sheet*, available at

http://www.cisco.com/en/US/products/ps7285/products_data_sheets_list.html

Ports and Protocol

Table 26-6 lists the ports used by the various protocol interfaces for Cisco Unified Service Statistics Manager. Cisco recommends opening these ports in the corporate firewall to allow communication between Unified SSM and other devices in the network.

Table 26-6 Unified SSM Port Utilization

Protocol	Port	Service
TCP	80	HTTP
TCP	443	HTTPS
TCP	2662	Database
TCP	12130	Syslog
TCP	12124	Unified SSM and Unified SSM agent communication[1]
TCP	12125	Unified SSM and Unified SSM agent communication[2]

1. Unified SSM connects all distributed Unified SSM agents.
2. Unified SSM agents send call statistics data back to Unified SSM.

Cisco Unified Provisioning Manager

The Cisco Unified Provisioning Manager (Unified PM) is a web-based provisioning application based on the Java 2 Enterprise Edition (J2EE) architecture. Unified PM provides a simplified web-based provisioning interface for both new and existing deployments of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Express (Unified CME), Cisco Unity, Cisco Unity Connection, and Cisco Unity Express. Unified PM provides provisioning for both the infrastructure and subscribers (or phone users) for Day 1 and Day 2 needs. Day 1 needs include configuring new deployments and adding more sites or locations; Day 2 needs include services for ongoing moves, adds, and changes on various components of the Cisco Unified Communications solution.

Cisco Unified Provisioning Manager also exposes northbound APIs to allow Cisco and third parties to integrate with external applications such as HR systems, custom or branded user portals, other provisioning systems, and directory servers.

Unified PM can be installed in simple or advanced mode to support up to 60,000 phones and 120,000 lines. In simple mode, Unified PM is installed on one system as a single server to support up to 10,000 phones. Advanced mode allows a two-system installation, where the Unified PM database server is installed on one server and the web and application server are on a separate system to support from 10,000 to 60,000 phones.

For more details on system requirements and installation steps, provisioning users and the infrastructure of supported components, and capacity information, refer to the Cisco Unified Provisioning Manager documentation available at http://www.cisco.com.

Note Unified PM supports Cisco Unified CM, Cisco Unified CME, Cisco Unity, Cisco Unity Connection, and Cisco Unity Express. For more information on component version compatibility, refer to the Unified PM data sheets at http://www.cisco.com/en/US/products/ps7125/products_data_sheets_list.html.

To provide a better understand of how Unified PM can be used as a network management solution for provisioning various Cisco Unified Communications components, this section first presents some of the basic concepts of Unified PM.

Call Processors and Message Processors

Unified PM serves as a provisioning interface for the following components of a Cisco Unified Communications system:

- Call processors
  - Cisco Unified Communication Manager (Unified CM)
  - Cisco Unified Communications Manager Express (Unified CME)
- Message processors
  - Cisco Unity
  - Cisco Unity Connection
  - Cisco Unity Express

The following sections describe some of the Unified PM concepts involved in configuring those components.

Domain

Domains are used for administrative purposes to create multiple logical groups within a system. Domains have the following characteristics:

- A domain can be mapped to a geographical location or an organization unit.
- One domain can contain multiple call processors and multiple optional message processors.
- A given call processor or message processor can be a member of multiple domains.

Service Area

Service areas represent offices. Service areas determine the dial plans and other voice-related configuration settings in the domain. In reality, each office may have multiple service areas. The service area determines attributes such as device group, route partition, and calling search space used within Unified CM. Service areas have the following characteristics:

- Each service area is assigned to single call processor and one optional message processor.
- Each service area should be associated with one dial plan.

Users and Subscribers

A *user* is a person who is authorized to perform various tasks in Unified PM, based on assigned user roles. When installed, Unified PM creates a Unified PM Admin (also called a Super Admin in Unified PM) who has global administrative rights and complete authorization to perform all tasks in Unified PM.

User roles determine the level of access within Unified PM. Domain-specific users can be assigned more than one user role to have rights to specific tasks in a domain. Individual user roles are related to either policy or workflow tasks. A user can be an administrator or a phone user.

A *subscriber* in Unified PM is an entity that uses IP telephony services provided by the underlying voice applications. A subscriber is the same as a phone user in Unified CM. Users in Unified PM can also have services themselves; thus, a user (an administrator) can also be a subscriber (or a phone user).

Work Flow and Managing Orders

When deploying a new site or making moves, adds and changes to an existing site, users make all changes to the underlying systems through a two-stage process of creating an order and then processing that order. You can set policies for both of these stages. For example, you can configure the system so that one group of users can only create and submit orders, while another group of users can view and perform processing-related activities. Unified PM contains an automation engine that performs the order processing, including service activation and business flow, based on how Unified PM is configured.

The workflow coordinates activities of the ordering process (approval, phone assignment, shipping, and receiving).

Configuration Templates

Unified PM enables you to configure Unified CM, Unified CME, and Cisco Unity Express in a consistent way through the use of configuration templates. You can use these templates to configure a new deployment of Unified CM, Unified CME, or Cisco Unity Express; to perform an incremental rollout on an existing Unified CM, Unified CME, or Cisco Unity Express; and to deploy a new service across existing customers.

Batch Provisioning

Creating users and provisioning their services can also be done automatically through batch provisioning for rolling out a new office or transitioning from legacy systems.

Best Practices

The following best practices and guidelines apply when using Unified PM to provision Cisco Unified Communications components for any new and/or existing deployments:

- Managed devices must be up and running before using Unified PM for further day-one activities such as rolling out a new site and day-two activities such as moves, adds, and changes.
- Pre-configuration is required for Cisco Unified CM, Cisco Unity, Unified CME, Survivable Remote Site Telephony (SRST), Cisco Unity Express, and Cisco Unified Presence Server.
- Define the correct domains, service areas, and provisioning attributes.
- Initially keep workflow rules as they were defined out-of-the-box by Cisco.
- Consider the use of Subscriber Types, Advanced Rule settings, and other configuration parameters.

The following basic tasks help support these best practices:

- Add call processors such as Unified CM, and/or Unified CME and message processors such as Cisco Unity, Unity Connection, and/or Unity Express.
- Create domains and assign call processors and message processors to the created domains.
- Provision the voice network by creating and using templates to configure Unified CMs or Unified CMEs, or import current voice infrastructure configurations from an existing deployment.
- Set up the deployment by creating service areas for each domain (typically one per dial plan) and assigning subscriber (user) types to each service area.
- Create administrative users for each domain.
- Order, update, or change subscriber or user services.

Note Unified PM does not provide distributed installation of the application server and database server, nor does it support any of the clustering features of the application server.

For more information on Unified PM, refer to the guide on *Getting Started with Cisco Unified Provisioning Manager Deployment and Best Practices*, available at

http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps7125/white_paper_c07-523344.html

Unified PM Design Considerations

The following design considerations apply to Unified PM:

- Deploy a one-system simple-mode installation of Unified PM for up to 10,000 phones.
- Deploy a two-system or dual-processor Microsoft Windows system in advanced mode, with the Unified PM database installed on a separate system from the web and application server.
- If a two-system advanced-mode installation is used for 10,000 to 60,000 phones, both the database server and the web and application server must be co-located, regardless of the deployment model used.
- One Unified PM can support up to 60,000 phones or 120,000 lines (DNs).
- Set up domains in one of the following ways:
  - Create a single domain for multiple sites, with multiple call processors and multiple message processors.
  - Create a domain for each site, consisting of one call processor and zero or more optional message processors.
  - Create multiple domains if different administrators are required to manage a subset of the subscribers.
- Create multiple service areas for multiple dial plans.
- Create two service areas if more than 15,000 phones and two Cisco Unity servers are deployed.
- Add only the Unified CM publisher as the call processor for Unified CM. Any changes made to the publisher will be synchronized to all the Unified CM subscriber servers.
- Use configuration templates for Unified CM, Unified CME, or Cisco Unity Express.
- Use Cisco IOS commands for Unified CME and Cisco Unity Express configuration templates.
- Add Cisco Unified CM infrastructure data objects for Unified CM configuration templates.
- Change and modify the existing configuration templates for batch provisioning for large quantities of phones and lines (DNs).
- Create multiple domains if you want different domain administrators to manage different sets of subscribers for Day 2 moves, adds, and changes of services (such as phones, lines, and voicemail), even for a single-site deployment.
- Create one service area for one dial plan.
- Create multiple service areas if multiple dial plans are required for the device pools, location, calling search space, and phones.

- Unified PM is an IPv6-aware application with the following characteristics:
  - Unified PM communicates with Unified CM over an IPv4 link. The Unified PM user configuration interface allows users to enter only IPv4 IP addresses because Unified CM has SOAP AXL interfaces in IPv4 only. Therefore, Unified PM must use IPv4 addresses to communicate with the AXL interfaces on Unified CM.
  - Unified PM handles the IPv6 addresses contained in SIP trunk AXL response messages.
  - Support of IPv6-aware functions does not affect support for current Cisco Unified Communications Manager Express, Cisco Unity, Cisco Unity Express, and Cisco Unity Connection devices.

Launching Cisco Unified Operations Manager

Unified PM can launch Cisco Unified Operations Manager (Unified OM) to obtain subscriber or user phone information. Unified PM allows its users to launch Unified OM by means of the Details button on the subscriber record. The Details button launches the IP Phone Details dialog box from Unified OM. To provide the launch point, the hostname or IP address and port number of the Unified OM server must be stored in the configuration file *<Install Dir>*\ sep\ipt.properties file. The following two entries can be edited by the system administrator to store the IP address or hostname and port number information of the Unified OM to be launched (both entries are left empty after Unified PM is installed):

```
dfc.ipt.operationsmanager.host:
dfc.ipt.operationsmanager.port:
```

Unified PM must be stopped and restarted for the changes to take effect. When launched, Unified OM displays its screen in a separate browser window.

Unified PM provides the URL for Cisco Unified Operations Manager (unified OM) to launch the Subscriber Record screen from its Phone Information screen. Refer to the CUOM section in this chapter for more details.

Redundancy and Failover

Once Unified PM is installed and set up, it can be used for Day 1 and Day 2 provisioning activities unless an upgrade or patch update is required. Unified PM currently does not have true redundancy and failover support. When multiple Unified PM systems are deployed, there is no synchronization between their multiple databases.

If Unified PM fails in the middle of the configuration process, changes made to the configured devices from the Unified PM GUI might not be saved and cannot be restored. Administrators must use manual steps to continue the configuration process by using other tools such as telnet or login (HTTP) to the managed devices until Unified PM comes back live. Manually added configuration changes to the managed device will not automatically show up in the Unified PM dashboard or database unless one of the following steps is performed:

- Synchronization from the Unified PM GUI for the call processors (Unified CM and/or Unified CME), message processors (Cisco Unity, Unity Connection, and/or Unity Express), and domains
- Synchronization by using a script under the Microsoft Windows scheduler that comes with the Unified PM installation, to run synchronization periodically (for example, every night)

Unified PM uses the Unified CM publisher server for all the database changes that are replicated to the Unified CM subscriber servers. If the Unified CM publisher fails, access to any of the information on the Unified CM server or cluster (including phones) becomes unavailable if the publisher is the only call processor associated with the domain or service area. Therefore, only certain features are available for provisioning even if other Unified CM servers or subscribers are in the domain or service area. Cisco does not recommend adding more Unified CM subscribers as call processors due to the fact that Unified CM configuration changes cannot be made if the Unified CM publisher server fails and that association of any additional Unified CM subscriber servers will introduce a lot of overhead.

Cisco Unified Provisioning Manager Server Performance

Table 26-7 lists system requirements and capacity information for Unified PM For the most current capacity information, refer to the latest Cisco Unified Provisioning Manager documentation available at http://www.cisco.com.

Table 26-7 Unified PM Capacity and System Requirements

Server Requirements	Up to 1000 Phones	Up to 10,000 Phones	Up to 30,000 Phones	Up to 60,000 Phones
CPU	Single 3.0 GHz Intel P4 processor or equivalent	2.33 GHz or higher quad-core processor or equivalent	Two-machine deployment with both: 2.33 GHz or higher quad-core processor or equivalent, each for the database server and the Web/Application server	Two-machine deployment with both: 2.33 GHz or higher quad-core processor or equivalent, each for the database server and the Web/Application server
Memory	2 GB RAM	4 GB RAM	4 GB RAM on each machine	4 GB RAM on Web/Application server and 8 GB RAM on the database server
Disk space	1x30 GB hard disk	1x60 GB hard disk with SAS or SCSI drives	1x30 GB hard disk on machine for Web and Application servers, and 1x80 GB SAS hard drive in a RAID 1+0 configuration for the database	1x60 GB hard disk on machine for Web and Application servers, and 1x120 GB SAS hard drive in a RAID 1+0 configuration for the database

Unified PM requires a 100 Mbps network interface card (NIC). Unified PM supports an unlimited number of call processors (Unified CM and Unified CME) and message processors (Cisco Unity, Unity Express, and Unity Connection) with up to 60,000 phones or 120,000 lines. Synchronization time depends upon the number of deployed phones and lines (DNs).

Ports and Protocol

Table 26-8 lists the ports used by the various protocol interfaces for Unified PM. Cisco recommends opening those ports in the corporate firewall to allow communication between Unified PM and other devices in the network.

Table 26-8 Unified PM Port Utilization

Protocol	Port	Service
TCP	80	HTTP[1] [2]
TCP	8443	HTTPS[2]
UDP	22	SSH[3]
TCP	23	Telnet[3]
TCP	1433	Database[4]

1. To access the Unified PM Administration web page.
2. Unified PM provisions Unified CM via AVVID XML Layer (AXL) Simple Object Access Protocol (SOAP).
3. For Unified PM to communicate with Unified CME and Cisco Unity Express.
4. For Unified PM to connect to the database of Cisco Unity and Cisco Unity Connection.

Integration with Cisco Unified Communications Deployment Models

This section discusses how to deploy Cisco Unified Network Management applications in various Cisco Unified Communications deployment models. For detailed information on the deployment models, see the chapter on Unified Communications の配置モデル , page 2-1.

The Cisco Unified Communications Management Suite supports both co-residency and VMware environments. The following supported limits and capacities apply to all the deploy models discussed in this chapter:

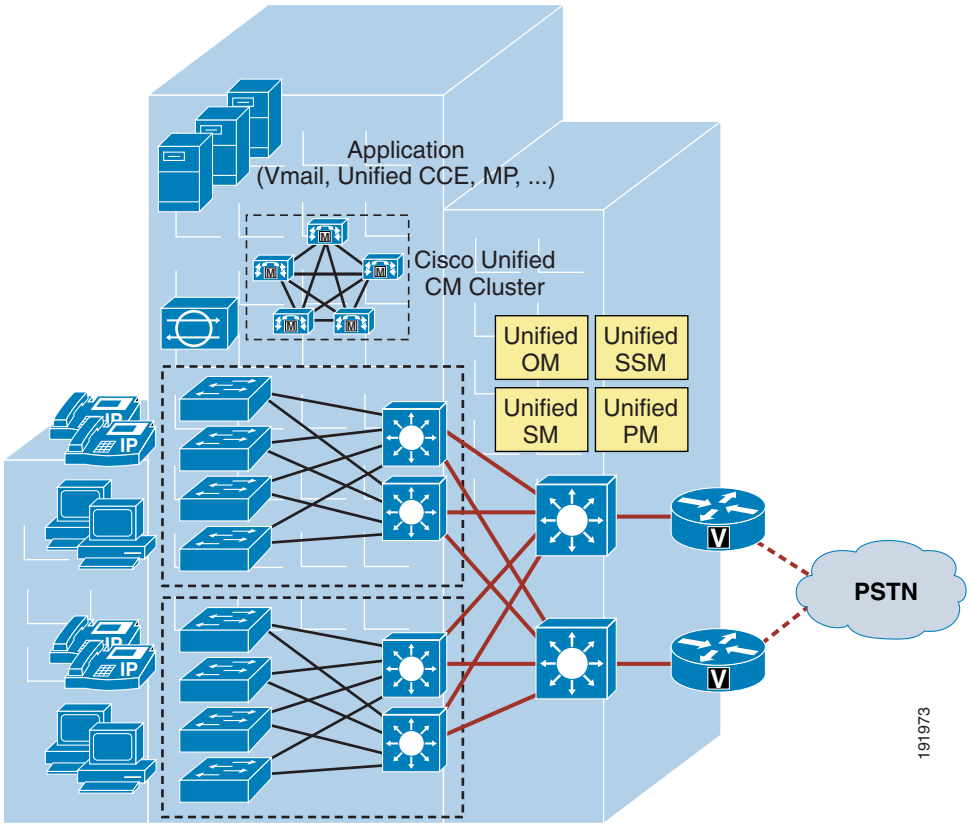
- Co-resident support
  - Unified PM, Unified SM, Unified OM, and Unified SSM can reside on the same physical server for deployments of up to 10,000 phones.
  - Standalone Unified OM, Unified SM, or Unified SSM supports up to 45,000 phones. Standalone Unified PM supports up to 60,000 phones.
- VMware environment
  - Run each Unified PM, Unified OM, Unified SM, and Unified SSM as a dedicated instance on a separate VMware server.
  - The maximum number of Unified OM instances is 3.
  - The maximum number of Unified SM instances is 2.
  - Standalone Unified PM supports up to 30,000 phones in a VMware environment.
  - Standalone Unified OM, Unified SM, or Unified SSM supports up to 30,000 phones in a VMware environment.

Note System hardware requirements for a VMware environment follow all the requirements from VMware in addition to the hardware system requirements specified for each of the deployment models described in this chapter.

Single Site

In the single-site model, Cisco Unified Network Management applications, along with call processing agents, are deployed at a single site (or campus) with no telephony services provided over an IP WAN. An enterprise would typically deploy the single-site model over a LAN or metropolitan area network (MAN). Figure 26-3 illustrates the deployment of Cisco Unified Network Management applications in the single-site model.

Figure 26-3 Single-Site Deployment



The following design characteristics and recommendations apply to the single-site model for deploying Unified OM, Unified SM, Unified SSM, and Unified PM:

- All network management applications can be deployed standalone on a dedicated Cisco Media Convergence Server (MCS) platform. However, Unified OM, Unified SM, and Unified SSM can be deployed co-resident on a shared MCS platform. Such a co-resident deployment provides the benefits of reducing the number of servers in the network and reducing the amount of network traffic that is sent between the various network management applications. The following guidelines indicate when to use co-resident or standalone deployments:
  - For less than 10,000 IP phones, deploy co-resident Unified PM, Unified OM, Unified SM, and Unified SSM. The system requirements for Unified PM, Unified OM, Unified SM, and Unified SSM co-residency can be found in the installation manuals for these products.
  - For more than 10,000 IP phones, deploy standalone Unified PM, Unified OM, Unified SM, and Unified SSM.

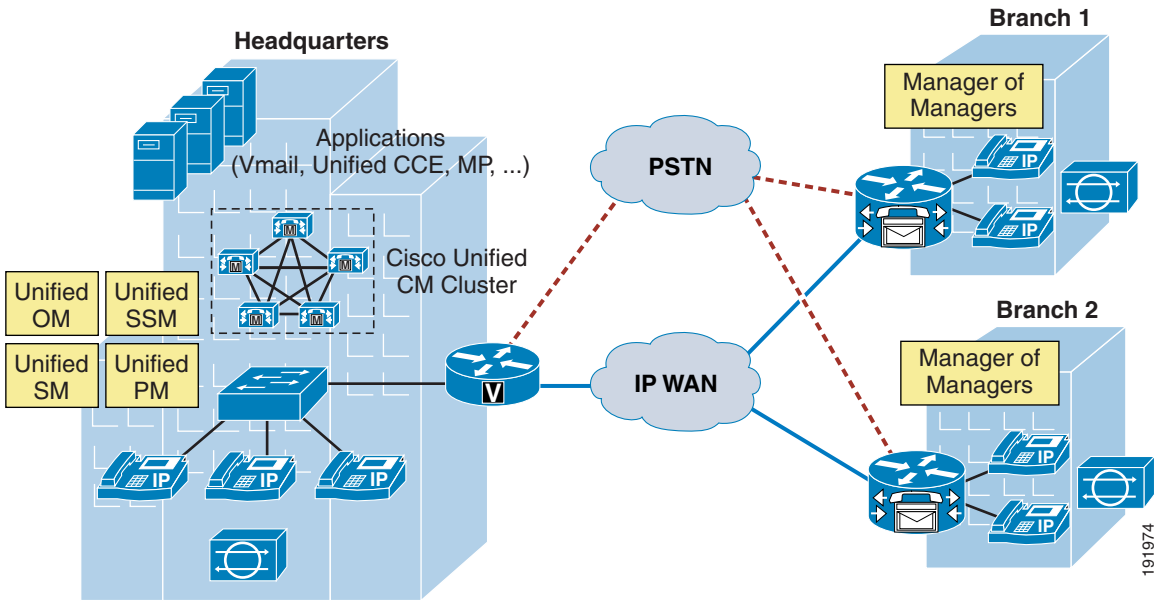
  Note A single Cisco Unified Operations Manager can support a maximum of 500 route lists.

- Cisco recommends deploying CVTQ-based voice quality monitoring to monitor overall voice quality in the network.
- Cisco recommends deploying the Cisco 1040 Sensor to monitor key IP phone devices, gateway devices, and application servers in the network and to investigate and troubleshoot voice quality issues.
- Each Unified OM can support a maximum 45,000 IP phones and 30 Unified CM clusters.
- Unified SM can support, concurrently, a maximum of 90,000 RTP streams per hour being monitored by the Cisco 1040 Sensor and 15,000 CVTQ-based calls per hour being monitored by Unified CM.
- Each Unified SM can support a maximum of 10 Unified CM clusters.
- Each Unified SSM can support a maximum of 45,000 IP phones and 10 Unified CM clusters.
- Each Unified PM can support a maximum of 60,000 IP phones and multiple Unified CM clusters.

Multisite WAN with Centralized Call Processing

The multisite WAN model with centralized call processing is really an extension of single-site model, with an IP WAN between the central site and remote sites. The IP WAN is used to transport voice traffic between the sites and call control signaling between the central site and the remote sites. Figure 26-4 illustrates the deployment of Cisco Unified Network Management applications in a multisite WAN model with centralized call processing.

Figure 26-4 Multisite WAN Deployment with Centralized Call Processing



The following design characteristics and recommendations apply to the multisite model for deploying Unified OM, Unified SM, Unified SSM, and Unified PM with centralized call processing:

- Cisco recommends deploying all network management applications (including Unified OM, Unified SM, Unified SSM, and Unified PM) in the central site to locate them with the call processing agent. The benefit of such an implementation is that it keeps the network management traffic between call processing agent and network management applications within the LAN instead of sending that traffic over the WAN circuit.
- All network management applications can be deployed standalone on a dedicated Cisco Media Convergence Server (MCS) platform. However, Unified OM, Unified SM, and Unified SSM can be deployed co-resident on a shared MCS platform. Such a co-resident deployment provides the benefits of reducing the number of servers in the network and reducing the amount of network traffic that is sent between the various network management applications. The following guidelines indicate when to use co-resident or standalone deployments:
  - For less than 10,000 IP phones, deploy co-resident Unified PM, Unified OM, Unified SM, and Unified SSM. The system requirements for Unified PM, Unified OM, Unified SM, and Unified SSM co-residency can be found in the installation manuals for these products.
  - For more than 10,000 IP phones, deploy standalone Unified PM, Unified OM, Unified SM, and Unified SSM.

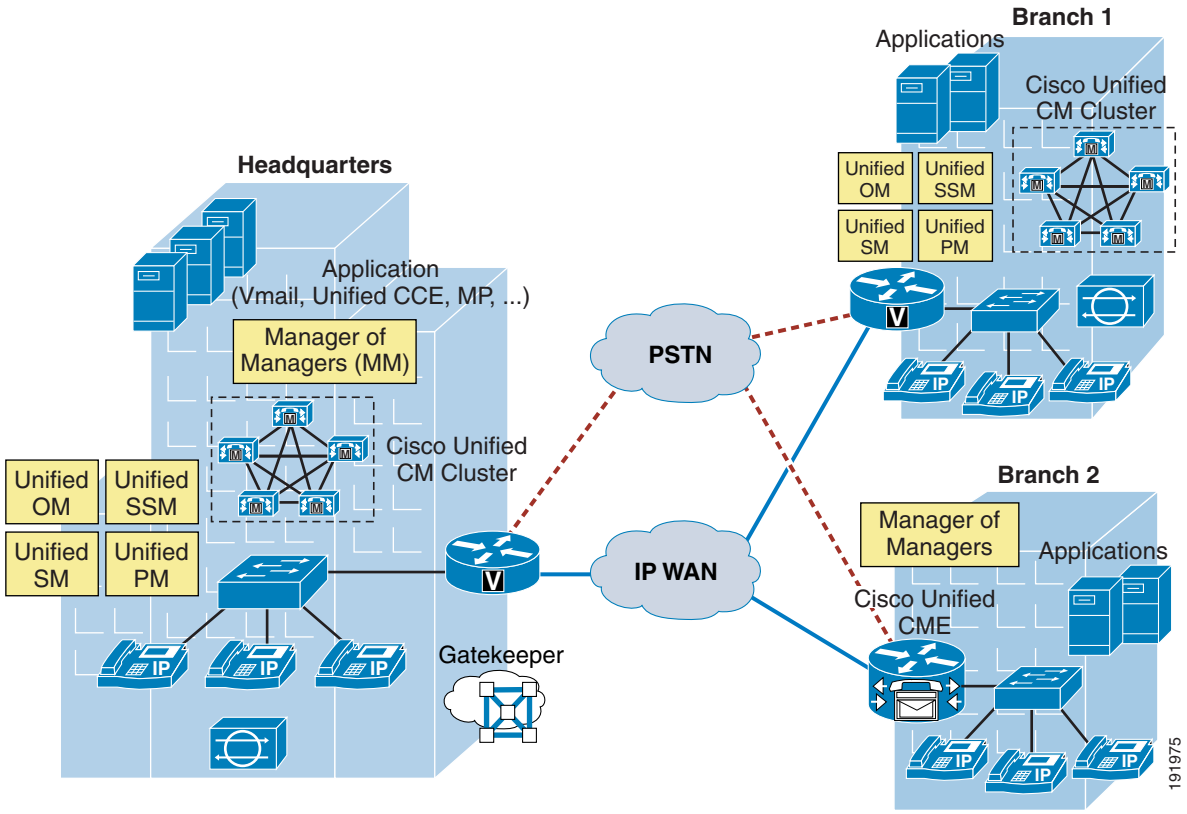
Note A single Cisco Unified Operations Manager can support a maximum of 500 route lists.

- Unified SM supports up to 50 Cisco 1040 Sensors. In order to monitor the voice streams of all 1000 remote sites, you can use Cisco ESPAN so that one Cisco 1040 Sensor can monitor voice streams from different remote sites across the network layer.
- All network management applications can be deployed standalone on a dedicated Cisco Media Convergence Server (MCS) platform. However, there are many scenarios where Unified OM, Unified SM, and Unified SSM can be deployed co-resident on a shared MCS platform. Such a co-resident deployment provides the benefits of reducing the number of servers in the network and reducing the amount of network traffic that is sent between the various network management applications. For detailed information on these deployment options, see the section on Single Site, page 26-22.
- Cisco recommends deploying CVTQ-based voice quality monitoring to monitor overall voice quality in the network.
- Cisco recommends deploying the Cisco 1040 Sensor to monitor key IP phone devices, gateway devices, and application servers in the network and to investigate and troubleshoot voice quality issues.
- Each Unified OM can support a maximum 45,000 IP phones.
- Unified SM can support, concurrently, a maximum of 90,000 RTP streams per hour being monitored by the Cisco 1040 Sensor and 15,000 CVTQ-based calls per hour being monitored by Unified CM.
- Each Unified SSM can support a maximum of 45,000 IP phones.
- Each Unified PM can support a maximum of 60,000 IP phones.

Multisite WAN with Distributed Call Processing

The multisite WAN model with distributed call processing consists of multiple independent sites, each with its own call processing agent connected to an IP WAN. Figure 26-5 illustrates the deployment of Cisco Unified Network Management applications in a multisite WAN model with distributed call processing.

Figure 26-5 Multisite WAN Deployment with Distributed Call Processing



A multisite WAN deployment with distributed call processing has many of the same requirements as a single site or a multisite WAN deployment with centralized call processing in terms of deploying Unified OM, Unified SM, Unified SSM, and Unified PM. Follow the best practices and recommendations from these other models in addition to the ones listed here for the distributed call processing model:

- If only one Cisco Unified Network Management system is deployed to manage multiple Unified CM clusters, Cisco recommends deploying Unified OM, Unified SM, Unified SSM, and Unified PM along with the Unified CM cluster that has the highest call volume and the most endpoints.
- If multiple Cisco Unified Network Management systems are deployed, Cisco recommends utilizing a higher-level “manager of managers” to administer those multiple systems simultaneously.
- All network management applications can be deployed standalone on a dedicated Cisco Media Convergence Server (MCS) platform. However, Unified OM, Unified SM, and Unified SSM can be deployed co-resident on a shared MCS platform. Such a co-resident deployment provides the

benefits of reducing the number of servers in the network and reducing the amount of network traffic that is sent between the various network management applications. The following guidelines indicate when to use co-resident or standalone deployments:

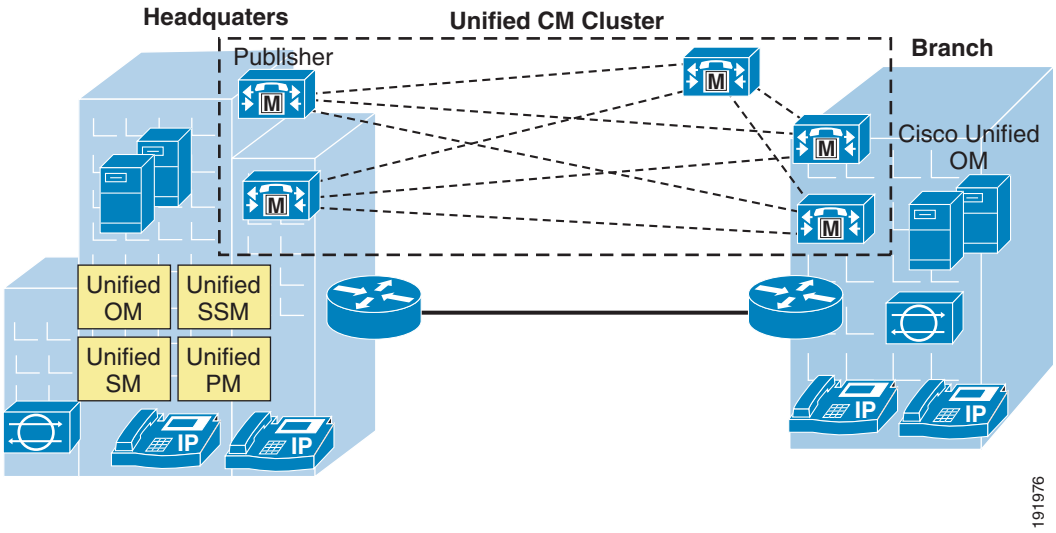
- For less than 10,000 IP phones, deploy co-resident Unified PM, Unified OM, Unified SM, and Unified SSM. The system requirements for Unified PM, Unified OM, Unified SM, and Unified SSM co-residency can be found in the installation manuals for these products.
- For more than 10,000 IP phones, deploy standalone Unified PM, Unified OM, Unified SM, and Unified SSM.

Note A single Cisco Unified Operations Manager can support a maximum of 500 route lists.

Clustering over the WAN

Clustering over the WAN refers to a single Cisco Unified CM cluster deployed across multiple sites that are connected by an IP WAN with QoS features enabled. This deployment model is designed to provide call processing resiliency if the IP WAN link fails. Figure 26-6 illustrates the deployment of Cisco Unified Network Management applications with clustering over the WAN.

Figure 26-6 Clustering over the WAN



Note There is no native high-availability or redundancy support for Unified SM, Unified SSM, or Unified PM with this model.

The following design characteristics and recommendations apply when deploying Unified OM, Unified SM, Unified SSM, and Unified PM with clustering over the WAN:

- Cisco recommends deploying Unified OM, Unified SM, Unified SSM, and Unified PM in the headquarter site where Unified CM publisher is located.
- Cisco recommends deploying a pair of Unified OMs. Deploy the active Unified OM in the headquarter site to manage all the sites under normal conditions. The warm-standby Unified OM should be located in the branch site and should have a longer polling interval. The warm-standby Unified OM will take over for the active server and provide redundancy support (shorten its polling interval) when the active Unified OM is unavailable. Additional WAN bandwidth should be provisioned for the SNMP polling messages of the warm-standby server.
- Cisco recommends deploying CVTQ-based voice quality monitoring to monitor overall voice quality in the network.
- Cisco recommends deploying the Cisco 1040 Sensor to monitor key IP phone devices, gateway devices, and application servers in the network and to investigate and troubleshoot voice quality issues.
- Each Unified OM can support a maximum 45,000 IP phones.
- Unified SM can support, concurrently, a maximum of 90,000 RTP streams per hour being monitored by the Cisco 1040 Sensor and 15,000 CVTQ-based calls per hour being monitored by Unified CM.
- Each Unified SSM can support a maximum of 45,000 IP phones.
- Each Unified PM can support a maximum of 60,000 IP phones.
- All network management applications can be deployed standalone on a dedicated Cisco Media Convergence Server (MCS) platform. However, Unified OM, Unified SM, and Unified SSM can be deployed co-resident on a shared MCS platform. Such a co-resident deployment provides the benefits of reducing the number of servers in the network and reducing the amount of network traffic that is sent between the various network management applications. The following guidelines indicate when to use co-resident or standalone deployments:
  - For less than 10,000 IP phones, deploy co-resident Unified OM, Unified SM, and Unified SSM. The system requirements for Unified OM, Unified SM, and Unified SSM co-residency can be found in the installation manuals for these products.
  - For more than 10,000 IP phones, deploy standalone Unified OM, Unified SM, and Unified SSM.
  - Deploy Unified PM on a separate server.

Note A single Cisco Unified Operations Manager can support a maximum of 500 route lists.

CHAPTER 27

Cisco Unified Communications Manager Business Edition

Cisco Unified Communications Manager Business Edition（Unified CMBE）は、中堅企業のお客様に 1 つのアプリケーション プラットフォームで Cisco Unified Communications Manager（Unified CM）と Cisco Unity Connection の機能を提供します。この章では、このソリューションを検討するに当たって考慮すべき設計上および配置上の留意事項について説明します。

スタンドアロンの Unified CM に適用される概念とガイドラインの多くが、この Business Edition にも適用されます。この章には、Unified CMBE の配置に関連した次のトピックの一部しか含まれていません。

- 「配置モデル」（P.27-2）

  適用可能なベスト プラクティスとメリットに焦点を当てながら、Unified CMBE の配置モデルごとの設計上の特徴および留意事項について説明します。

- 「ダイヤル プラン」（P.27-13）

  Unified CMBE 環境でダイヤル プランを実装するためのベスト プラクティスと推奨事項のリストを提供します。

- 「Survivable Remote Site Telephony（SRST）」（P.27-15）

  マルチサイト Unified CMBE 配置で基本的な呼制御の可用性を提供するオプション機能について説明します。

- 「Unified CMBE のディレクトリ管理」（P.27-17）

  新しい LDAP 同期および認証のサポートに焦点を当てながら、Unified CMBE と Unified CM でのユーザの管理方法の違いについて説明します。

- 「Unified CMBE の移行」（P.27-19）

  Unified CMBE ソリューションから、スタンドアロン サーバ上の Cisco Unified CM と Cisco Unity Connection を使用したソリューションに移行するためのオプションについて説明します。

- 「システムの容量計画とスケーリング」（P.27-19）

  Unified CMBE のオーバーサブスクリプションを回避するためのシステム利用計画に関するいくつかのルールとガイドラインを提供します。

- 「Cisco Unified CM アプリケーション」（P.27-22）

  各 Unified CM アプリケーションに関連した性能と容量の意味合いについて説明します。

この章の新規情報

表 27-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 27-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所
LDAP 同期および認証	「Unified CMBE のディレクトリ管理」（P.27-17）
Cisco MCS 7828 サーバの目的の再定義	「Unified CMBE の移行」（P.27-19）
Unified CMBE 分散配置モデル	「分散型コール処理を使用した Unified CMBE マルチサイト WAN 配置」（P.27-8）

配置モデル

Unified CMBE は、主に、次の 3 種類の配置モデルをサポートします。

- 単一サイト配置
- 集中型コール処理を使用したマルチサイト WAN 配置
- 分散型コール処理を使用したマルチサイト WAN 配置

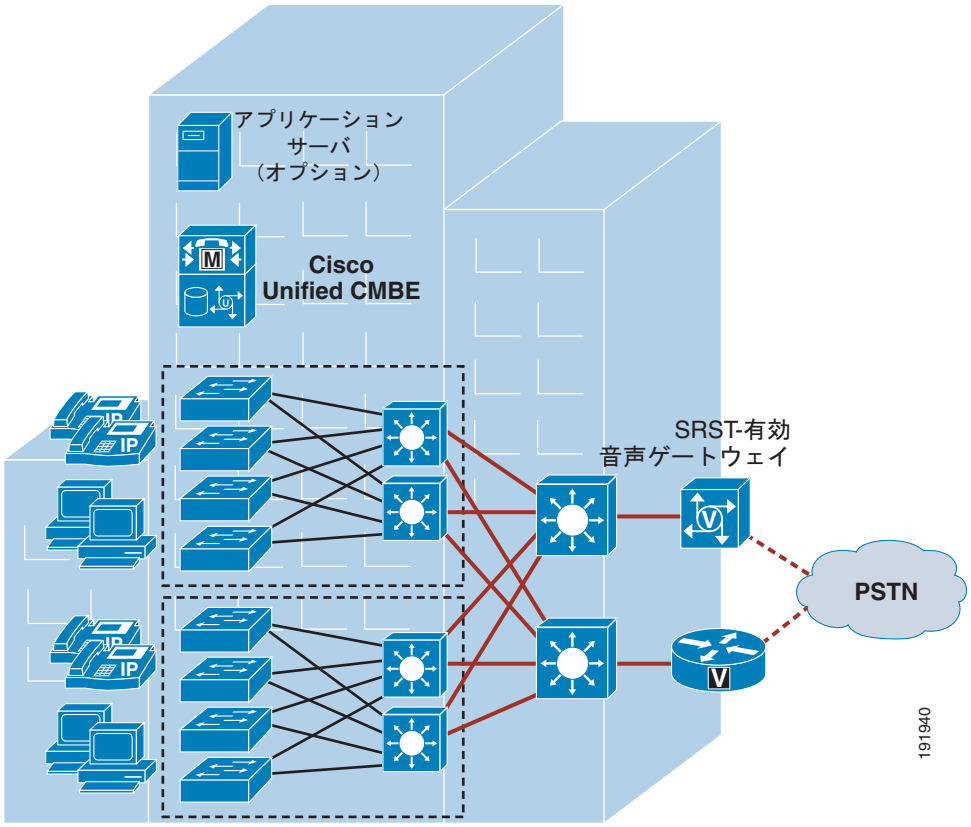
Unified CMBE は、1 つのサーバ上で Cisco Unified CM と Cisco Unity Connection の両方を実行する単一プラットフォーム配置であることから、この 3 つの配置モデルに限定されます。

分散型コール処理を使用したマルチサイト WAN 配置は、Unified CMBE 7.0 の新規モデルで、Unified CM またはその他の Unified CMBE 配置との Unified CMBE インターワーキングを可能にするために追加されました。このモデルで、Unified CMBE は、H.323 クラスタ間トランクと SIP トランクを使用した Unified CM 配置またはその他の Unified CMBE 配置との相互接続をサポートします。

Unified CMBE の単一サイト配置

Unified CMBE の単一サイト モデルは、単一のサイトまたはキャンパスに配置された 1 つのハードウェア プラットフォーム上で動作する Cisco Unified CM と Cisco Unity Connection で構成されます。IP WAN 上のテレフォニー サービスは提供されません。図 27-1 に、Unified CMBE を使用した単一サイト配置のコンポーネントの一部を示します。

図 27-1　Unified CMBE の単一サイト配置



次の設計上の特徴と留意事項が、Unified CMBE の単一サイト配置モデルに適用されます。

- Unified CMBE は、Cisco Media Convergence Server (MCS) 7828-H3 と MCS 7828-I3 のどちらかの単一ハードウェア プラットフォーム上で動作します。

（注）　Unified CMBE は単一ハードウェア プラットフォーム上で動作するため、Unified CM の単一インスタンスしか提供されません（パブリッシャとシングル サブスクライバの複合インスタンスと、セカンダリ サブスクライバ インスタンスが設定できません）。

- Unified CMBE は、最大 500 人のユーザと最大 575 台の Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）の IP 電話機またはビデオ エンドポイントをサポートします（最大ファーム構成は、設定可能なすべての電話機の種類、CTI ポート、および H.323 クライアントを含む、700 台のデバイスからなります）。これらのデバイスの Busy Hour Call Attempts（BHCA）が容量計画で大きな役割を果たします。そのため、システム リソースのオーバーサブスクリプションを避けるために、「システムの容量計画とスケーリング」（P.27-19）のシステム利用計画に関するルールとガイドラインに関する項を参照してください。
- Unified CMBE は、最大 20 台の SIP、MGCP、または H323 デバイス（ゲートウェイ、MCU、トランク、およびクライアント）をサポートします。
- すべての外部コールに対して公衆網が使用されます。
- 会議機能、トランスコーディング機能、およびメディア ターミネーション ポイント（MTP）機能に、デジタル シグナル プロセッサ（DSP）を使用しています。Unified CMBE はカンファレンス ブリッジまたは MTP として設定できますが、この設定は実験環境または概念実証環境でしか推奨

されていません。Unified CMBE は、すでに、複数の重要なコール処理機能とデータベース機能を提供しているため、Unified CMBE をカンファレンス ブリッジまたは MTP として設定すると、システム性能に悪影響を及ぼす可能性があります。

- Unified CMBE は、最大 500 個のメールボックスと 24 個の SCCP ボイスメール ポートをサポートします。24 個のポートは、必要に応じて、自動音声認識（ASR）用、Text-to-Speech（TTS）用、または単純なボイスメール ポートとしてプロビジョニングしてライセンス供与できます。
- Unified CMBE は、次のクライアント アクセス オプションの最大 500 個の同時セッションをサポートします。
  - Cisco Unified Personal Communicator
  - Internet Message Access Protocol（IMAP）
  - Cisco Unity Connection Inbox クライアント
  - Cisco Unity Inbox RSS フィード

（注）　同時セッション数は、アクティブ セッション数を意味します。500 を超える上記クライアント アクセス オプションを使用してユーザを設定できますが、これらのオプションをいくつ組み合せても同時に存在するアクティブ セッション数は最大 500 個です。たとえば、500 人のユーザが利用しているシステムでは、各ユーザを Cisco Unified Personal Communicator、IMAP アクセス、Cisco Unity Inbox、および Inbox RSS フィード用に設定できますが、500 個のアクティブ セッションしかサポートされません。

- Unified CMBE は、最大 15,000 件の Voice Profile for Internet Mail（VPIM）連絡先と 10 箇所のロケーションをサポートします。
- コールを発信するためにゲートキーパーが必要な H.323 クライアント、MCU、および H.323/H.320 ゲートウェイを、Cisco IOS ゲートキーパー（Cisco IOS Release 12.3(8)T 以降）に登録する必要があります。Unified CM は H.323 トランクを使用してゲートキーパーと統合し、そこに登録された H.323 デバイスのコール ルーティングと帯域幅管理サービスを提供します。複数の Cisco IOS ゲートキーパーを使用して、冗長性を提供することもできます。
- マルチポイント ビデオ会議には MCU リソースが必要です。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。
- 公衆 ISDN 網上で H.320 ビデオ会議デバイスと通信するために H.323/H.320 ビデオ ゲートウェイが必要です。
- Unified CMBE は、サイト内でのデバイス間の広帯域オーディオ（G.711、G.722、Cisco Wideband Audio など）をサポートします。
- Unified CMBE は、サイト内でのデバイス間の広帯域ビデオ（384 kbps 以上など）をサポートします。7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec もサポートされます。

（注）　上で指定された上限を超えないようにして、システムをオーバーサブスクライブさせないように注意してください。システムの計画段階で、これらの上限を上回った場合、または上回りそうな場合は、代わりに、スタンドアロンの Cisco Unified CM および Cisco Unity Connection ソリューションを検討してください。詳細については、「システムの容量計画とスケーリング」（P.27-19）を参照してください。

Unified CMBE の単一サイト配置のメリット

単一ハードウェア プラットフォームによる集中型ネットワーク ソリューションによって、大幅な費用対効果と複雑さの低減が期待できます。中堅企業のお客様は、IP テレフォニー用のさまざまな IP ベースのアプリケーションを利用できます。単一サイト配置では、各サイトを完全に分離することも可能です。IP WAN 障害が発生したり、帯域幅が不足してもサービスが中断することはありません。

Unified CMBE の単一サイト配置には、次のようなメリットがあります。

- 配置が容易
- 単一プラットフォームでコール処理、Cisco Unified Mobility、および統合メッセージングに対応
- 管理ユーザとエンド ユーザの両方にシングル サインオン機能を提供する、コール処理および統合メッセージングのための単一管理点
- 集中型ソリューションに共通のインフラストラクチャ
- 単純化および統一されたダイヤル プラン
- G.711 コーデックのみを使用するため、トランスコーディング リソースが不要

Unified CMBE の単一サイト配置に関するベスト プラクティス

Unified CMBE の単一サイト配置を実装する場合は、Unified CM の単一サイト配置モデルのガイドライン、メリット、およびベスト プラクティスを参照してください（一般的な情報については、「Unified Communications の配置モデル」（P.2-1）の章を参照してください）。

加えて、Cisco Unified Survivable Remote Site Telephony（SRST）の多くは、その名のとおり、リモート サイトにおける WAN 障害発生時のバックアップ コール処理用としてリモート サイトに配置されていました。Unified CMBE の単一サイト配置では、SRST を中央サイトで使用できます。

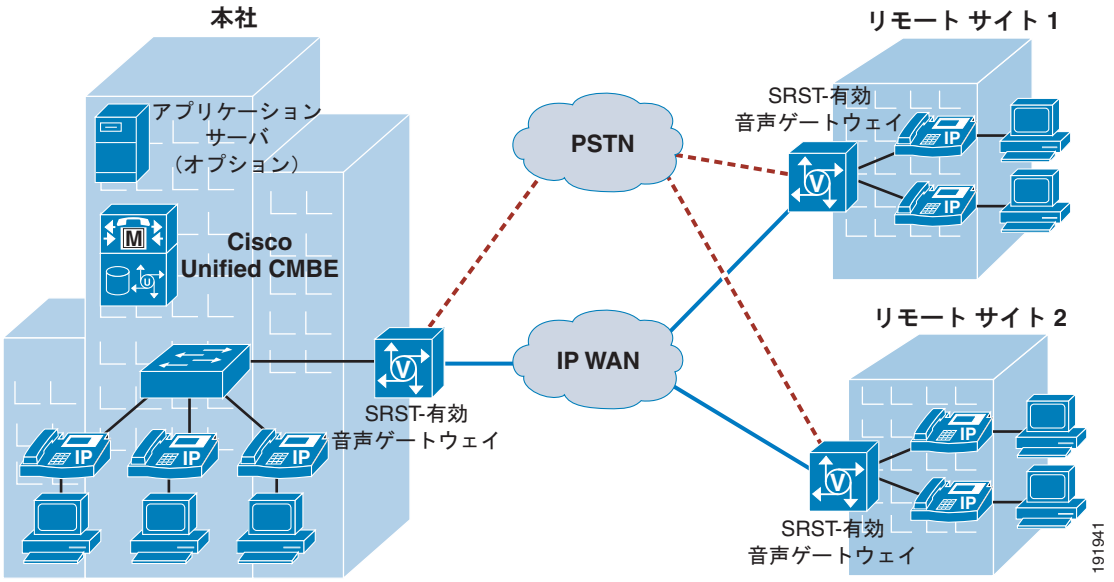
集中型コール処理を使用した Unified CMBE マルチサイト WAN 配置

集中型コール処理を使用した Unified CMBE マルチサイト WAN 配置モデルは、最大 20 サイト（1 つの中央サイトと 19 のリモート サイト）に対してサービスを提供する単一のコール処理アプライアンスで構成されています。また、このモデルは、IP WAN を使用してサイト間で IP テレフォニー トラフィックを送信します。IP WAN は、中央サイトとリモート サイト間の呼制御シグナリングも伝送します。図 27-2 に、代表的な集中型コール処理配置を示します。この配置では、中央サイトのコール処理およびボイスメール サーバとして Unified CMBE が使用され、すべてのリモート サイトを接続するために QoS に対応した IP WAN が使用されます。リモート サイトは、コール処理と統合メッセージングの処理を集中型 Unified CMBE に依存しています。通常は、Interactive Voice Response（IVR）システムなどのその他のアプリケーションも、管理と保守の全体コストを削減するために集中管理されます。

この配置モデルは、集中型コール処理を使用した Unified CM マルチサイト WAN 配置に似ていますが、Unified CMBE 配置モデルでは、単一のハードウェア プラットフォームでコール処理が提供されます（一般的なマルチサイト設計の特徴については、「集中型コール処理を使用するマルチサイト」（P.2-4）を参照してください）。

（注）　このマニュアルで説明する集中型コール処理モデル用のソリューションでは、さまざまなサイトが QoS に対応した IP WAN に接続されます。

図 27-2　集中型コール処理を使用した Unified CMBE マルチサイト WAN 配置



次の設計上の特徴と留意事項が、集中型コール処理を使用した Unified CMBE マルチサイト WAN 配置モデルに適用されます。

- Unified CMBE は、Cisco Media Convergence Server (MCS) 7828-H3 と MCS 7828-I3 のどちらかの単一ハードウェア プラットフォーム上で動作します。

（注）　Unified CMBE は単一ハードウェア プラットフォーム上で動作するため、Unified CM の単一インスタンスしか提供されません（パブリッシャとシングル サブスクライバの複合インスタンスと、セカンダリ サブスクライバ インスタンスが設定できません）。

- Unified CMBE は、最大 500 人のユーザと最大 575 台の Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）の IP 電話機またはビデオ エンドポイントをサポートします（最大ファーム構成は、設定可能なすべての電話機の種類、CTI ポート、および H.323 クライアントを含む、700 台のデバイスからなります）。これらのデバイスの Busy Hour Call Attempts（BHCA）が容量計画で大きな役割を果たします。そのため、システム リソースのオーバーサブスクリプションを避けるために、「システムの容量計画とスケーリング」（P.27-19）のシステム利用計画に関するルールとガイドラインに関する項を参照してください。
- Unified CMBE は、音声ゲートウェイの最大数（20）と一致するように、最大 20 の SRST 対応サイト（1 つの中央サイトと 19 のリモート サイト）をサポートします。
- Unified CMBE は、最大 20 台の SIP、MGCP、または H323 デバイス（ゲートウェイ、MCU、トランク、およびクライアント）をサポートします。
- 会議機能、トランスコーディング機能、およびメディア ターミネーション ポイント（MTP）機能に、デジタル シグナル プロセッサ（DSP）を使用しています。Unified CMBE はカンファレンス ブリッジまたは MTP として設定できますが、この設定は実験環境または概念実証環境でしか推奨されていません。Unified CMBE は、すでに、複数の重要なコール処理機能とデータベース機能を提供しているため、Unified CMBE をカンファレンス ブリッジまたは MTP として設定すると、システム性能に悪影響を及ぼす可能性があります。
- Unified CMBE は、最大 500 個のメールボックスと 24 個の SCCP ボイスメール ポートをサポートします。24 個のポートは、必要に応じて、自動音声認識（ASR）用、Text-to-Speech（TTS）用、または単純なボイスメール ポートとしてプロビジョニングしてライセンス供与できます。

- Unified CMBE は、次のクライアント アクセス オプションの最大 500 個の同時セッションをサポートします。
  - Cisco Unified Personal Communicator
  - Internet Message Access Protocol（IMAP）
  - Cisco Unity Connection Inbox クライアント
  - Cisco Unity Inbox RSS フィード

（注）　同時セッション数は、アクティブ セッション数を意味します。500 を超える上記クライアント アクセス オプションを使用してユーザを設定できますが、これらのオプションをいくつ組み合せても同時に存在するアクティブ セッション数は最大 500 個です。たとえば、500 人のユーザが利用しているシステムでは、各ユーザを Cisco Unified Personal Communicator、IMAP アクセス、Cisco Unity Inbox、および Inbox RSS フィード用に設定できますが、500 個のアクティブ セッションしかサポートされません。

- Unified CMBE は、最大 15,000 件の Voice Profile for Internet Mail（VPIM）連絡先と 10 箇所のロケーションをサポートします。
- Cisco Unified Survivable Remote Site Telephony（SRST）の多くは、その名のとおり、リモート サイトにおける WAN 障害発生時のバックアップ コール処理用としてリモート サイトに配置されていました。Unified CMBE マルチサイト配置では、SRST をリモート サイトだけでなく、中央サイトでも使用できます（詳細については、「Survivable Remote Site Telephony（SRST）」（P.27-15）を参照してください）。

（注）　上で指定された上限を超えないようにして、システムをオーバーサブスクライブさせないように注意してください。システムの計画段階で、これらの上限を上回った場合、または上回りそうな場合は、代わりに、スタンドアロンの Cisco Unified CM および Cisco Unity Connection ソリューションを検討してください（詳細については、「システムの容量計画とスケーリング」（P.27-19）を参照してください）。

IP WAN の接続オプションは、次のとおりです。

- 専用回線
- フレーム リレー
- 非同期転送モード（ATM）
- ATM とフレーム リレーのサービス インターワーキング（SIW）
- マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）
- 音声およびビデオ対応 IP セキュリティ プロトコル VPN（IPSec VPN（V3PN））

WAN エッジに配置するルータでは、プライオリティ キューイングやトラフィック シェーピングなどの Quality of Service（QoS）メカニズムを使用して、恒常的に帯域幅が不足している WAN 上のデータ トラフィックから音声トラフィックを保護する必要があります。加えて、音声トラフィックによる WAN リンクのオーバーサブスクリプションや確立されたコールの品質低下を防止するために、コール アドミッション制御方式が必要です。集中型コール処理配置の場合は、Unified CM 内のロケーション構造がコール アドミッション制御を提供します（ロケーションの詳細については、「Unified CM の静的ロケーション」（P.9-12）の項を参照してください）。

リモート サイトでは、さまざまな Cisco ゲートウェイにより、公衆網を介したアクセスが可能です。IP WAN に障害が起きた場合、または IP WAN 上で使用可能な帯域幅がすべて消費されてしまった場合でも、リモート サイトのユーザは、公衆網アクセス コードをダイヤルして、公衆網を利用してコール

を発信できます。Cisco IOS ゲートウェイ上の SCCP 電話機と SIP 電話機で使用可能な Survivable Remote Site Telephony（SRST）機能を使用すれば、WAN 障害が発生した支店でのコール処理が可能になります。

集中型コール処理を使用した Unified CMBE マルチサイト WAN 配置のメリット

単一ハードウェア プラットフォームによる集中型ネットワーク ソリューションによって、大幅な費用対効果と複雑さの低減が期待できます。中堅企業のお客様は、IP テレフォニー用のさまざまな IP ベースのアプリケーションを利用できます。

集中型コール処理を使用したマルチサイト Unified CMBE 配置には次のようなメリットがあります。

- 単一プラットフォームでコール処理、Cisco Unified Mobility、および統合メッセージングに対応
- 管理ユーザとエンド ユーザの両方にシングル サインオン機能を提供する、コール処理および統合メッセージングのための単一管理点
- 集中型ソリューションに共通のインフラストラクチャ

集中型コール処理を使用した Unified CMBE マルチサイト WAN 配置に関するベスト プラクティス

集中型コール処理を使用した Unified CMBE マルチサイト配置を実装する場合は、集中型コール処理を使用した Unified CM マルチサイト WAN 配置モデルのガイドライン、メリット、およびベスト プラクティスを参照してください（一般的な情報については、「Unified Communications の配置モデル」（P.2-1）の章を参照してください）。

加えて、次のガイドラインに留意してください。

- 可能な場合は、リモート支店とのコール アドミッション制御を提供するために、Unified CM 内のロケーション メカニズムを使用します。このメカニズムをさまざまな WAN トポロジに適用する方法については、「コール アドミッション制御」（P.9-1）の章を参照してください。Unified CMBE は、すべてのコール アドミッション制御メカニズムをサポートします。
- Unified CM とリモート ロケーション間の遅延を最小化して、音声カットスルー遅延（クリッピングとも呼ばれる）を削減します。
- ベアラ トラフィック用の WAN 帯域幅をプロビジョニングする必要がある場合は、集中型コール処理配置モデルを採用することによって、サイト間の音声メディアを WAN ではなく公衆網上で送信できます（詳細については、「集中型コール処理のバリエーションとしての Voice Over the PSTN」（P.2-12）を参照してください）。

分散型コール処理を使用した Unified CMBE マルチサイト WAN 配置

分散型コール処理を使用したマルチサイト WAN 配置は、複数の独立したサイトで構成されており、各サイト専用のコール処理エージェントが、分散したサイト間の音声トラフィックを伝送する IP WAN に接続されています。サイトは次のいずれかにすることができます。

- 独自のコール処理エージェントを使用する単一サイト。コール処理エージェントは、次のいずれかになります。
  - Cisco Unified Communications Manager（Unified CM）
  - Cisco Unified Communications Manager Business Edition（Unified CMBE）
  - Cisco Unified Communications Manager Express（Unified CME）
  - その他の IP PBX

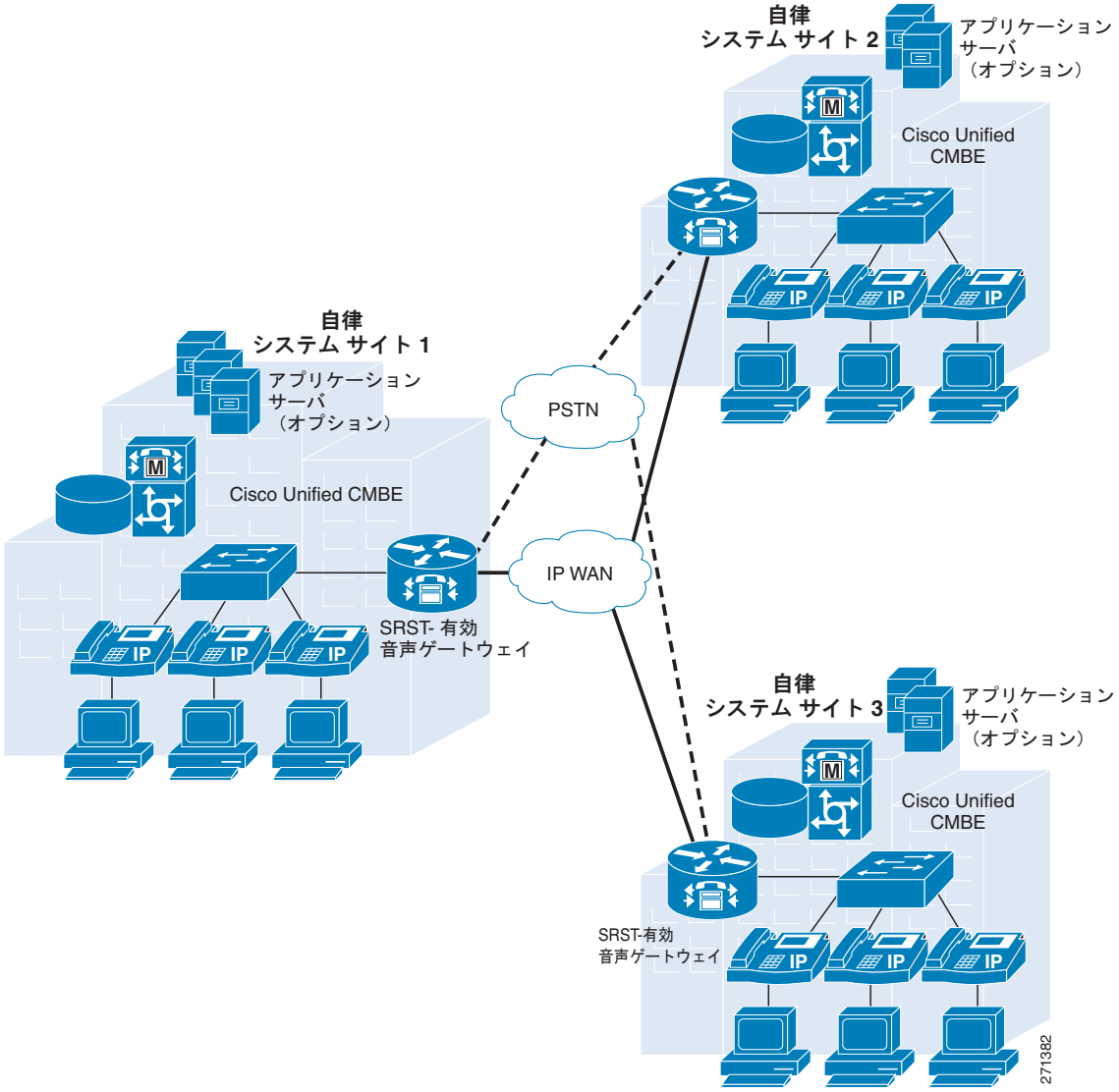
- 集中型コール処理サイトとそれに関連したすべてのリモート サイト
- Voice over IP（VoIP）ゲートウェイを備えたレガシー PBX

Cisco Unified CMBE 7.0 以降のリリースは、マルチサイト分散型コール処理をサポートします。このモデルでは、Unified CMBE が自律システムとして動作するように設計されます。各 Unified CMBE 配置は、自律システムとして、他の配置と完全に独立して動作する必要があり、機能を他の配置内のアプリケーションやインフラストラクチャ コンポーネントに全く依存しないようにする必要があります。また、自律システムとして、クラスタ間トランクまたは SIP トランク経由で他の自律型 Unified CMBE サイトまたは自律型 Unified CM クラスタに接続したり、Unified CMBE システムでサポートされる音声ゲートウェイとトランクの最大数を超えないように、H.323 トランクまたは SIP トランク経由で Unified CME サイトに接続することができます（図 27-3 と図 27-4 を参照）。Unified CMBE をこのように使用して、任意の数のサイトとシステムで構成された最大 20 のロケーションを相互接続することができます。加えて、各 Unified CMBE システムは、3,600 の最大システム BHCA を超えないようにする必要があります（詳細については、「システムの容量計画とスケーリング」（P.27-19）を参照してください）。

自律システムは、次のガイドラインに従う必要があります。

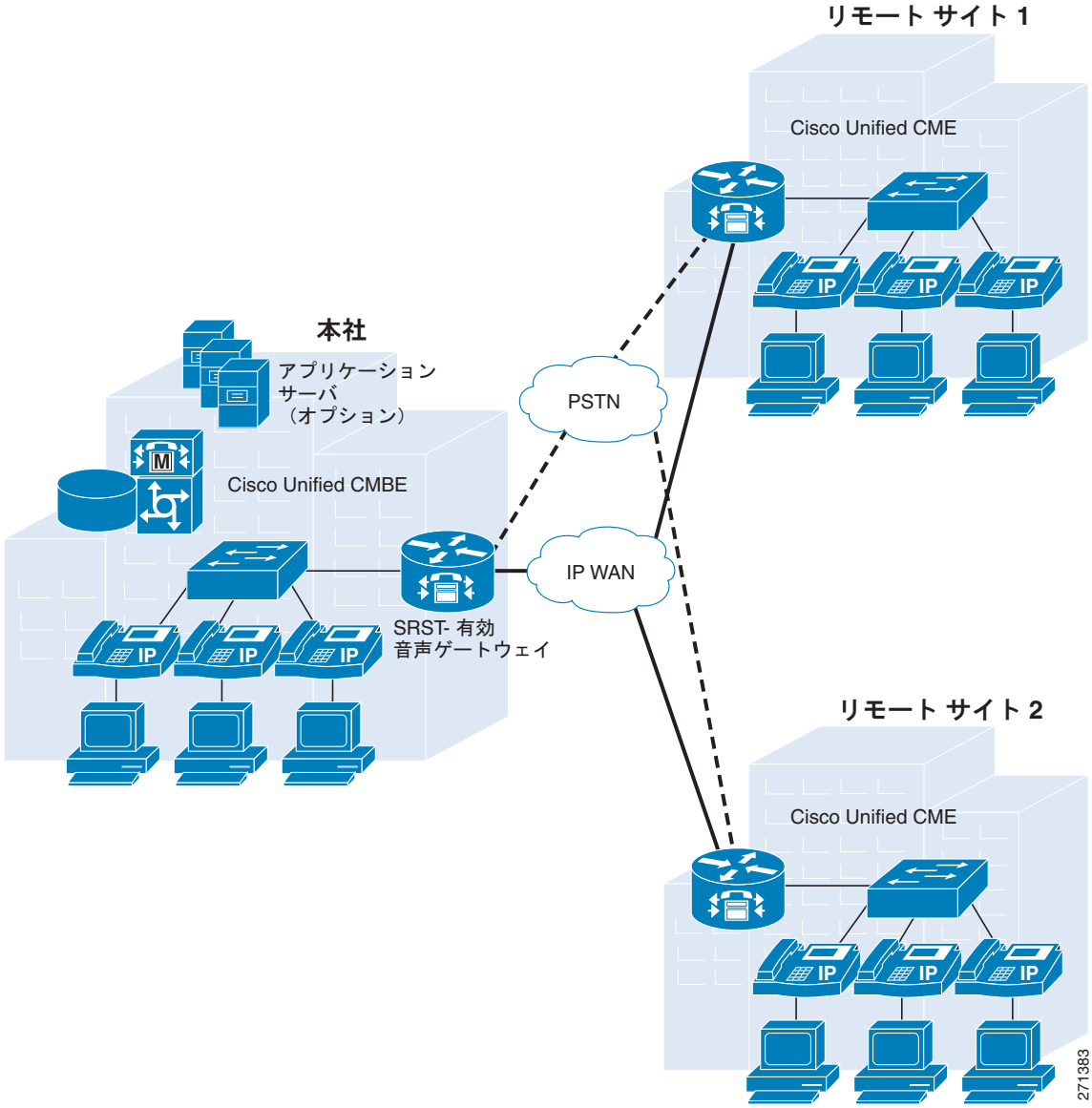
- Unified CMBE アプリケーションは、他の自律システムのデバイス、エンドポイント、またはクライアント用の集中型アプリケーションをホストするのではなく、その自律システム内のリモート サイトにあるデバイス、エンドポイント、およびクライアント専用の集中型アプリケーションをホストする必要があります。
- ダイヤル プラン、デバイス、ユーザ、エンドポイントなどの自律システム用の集中型プロビジョニングは行われません。自律システムは、個別にプロビジョニングされます。
- 自律システムごとに機能セットが異なる可能性があります。たとえば、Unified CMBE と相互作用するための Unified CME を配置する場合は、システムごとにユーザ向けの機能セットが異なる可能性があります。
- Unified CMBE は、集中型コール処理モデルに配置された Unified CM のエンドポイントまたはクライアント用のリモート サイトでバックアップ コール処理エージェントとして機能できません。Unified CMBE は、Survivable Remote Site Telephony の代用ではありません。

図 27-3　分散型コール処理を使用したマルチサイト WAN 内で Unified CMBE に接続された Unified CMBE



Unified CMBE に関連した自律システムの定義については、「分散型コール処理を使用した Unified CMBE マルチサイト WAN 配置」（P.27-8）を参照してください。

図 27-4　分散型コール処理を使用したマルチサイト WAN 内で Unified CME に接続された Unified CMBE



次の設計上の特徴と留意事項が、分散型コール処理を使用した Unified CMBE マルチサイト WAN 配置モデルに適用されます。

- Unified CMBE は、Cisco Media Convergence Server (MCS) 7828-H3 と MCS 7828-I3 のどちらかの単一ハードウェア プラットフォーム上で動作します。

（注）　Unified CMBE は単一ハードウェア プラットフォーム上で動作するため、Unified CM の単一インスタンスしか提供されません（パブリッシャとシングル サブスクライバの複合インスタンスと、セカンダリ サブスクライバ インスタンスが設定できません）。

- Unified CMBE は、Unified CMBE 自律システムごとに、最大 500 人のユーザと最大 575 台の Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）の IP 電話機またはビデオ エンドポイントをサポートします（最大ファーム構成は、設定可能なすべての電話機

の種類、CTI ポート、および H.323 クライアントを含む、700 台のデバイスからなります）。これらのデバイスの Busy Hour Call Attempts（BHCA）が容量計画で大きな役割を果たします。そのため、システム リソースのオーバーサブスクリプションを避けるために、「システムの容量計画とスケーリング」（P.27-19）のシステム利用計画に関するルールとガイドラインに関する項を参照してください。

- Unified CMBE は、音声ゲートウェイの最大数（20）と一致するように、最大 20 の SRST 対応サイト（1 つの中央サイトと 19 のリモート サイト）をサポートします。
- Unified CMBE は、他の自律型 Unified CMBE システム、Unified CM クラスタ、または Unified CME サイトと相互接続するための H.323 クラスタ間トランクまたは SIP トランクを含む、最大 20 台の SIP、MGCP、または H323 デバイス（ゲートウェイ、MCU、トランク、およびクライアント）をサポートします。
- 会議機能、トランスコーディング機能、およびメディア ターミネーション ポイント（MTP）機能に、デジタル シグナル プロセッサ（DSP）を使用しています。Unified CMBE はカンファレンス ブリッジまたは MTP として設定できますが、この設定は実験環境または概念実証環境でしか推奨されていません。Unified CMBE は、すでに、複数の重要なコール処理機能とデータベース機能を提供しているため、Unified CMBE をカンファレンス ブリッジまたは MTP として設定すると、システム性能に悪影響を及ぼす可能性があります。
- Unified CMBE は、最大 500 個のメールボックスと 24 個の SCCP ボイスメール ポートをサポートします。24 個のポートは、必要に応じて、自動音声認識（ASR）用、Text-to-Speech（TTS）用、または単純なボイスメール ポートとしてプロビジョニングしてライセンス供与できます。
- Unified CMBE は、次のクライアント アクセス オプションの最大 500 個の同時セッションをサポートします。
  - Cisco Unified Personal Communicator
  - Internet Message Access Protocol（IMAP）
  - Cisco Unity Connection Inbox クライアント
  - Cisco Unity Inbox RSS フィード

（注） 同時セッション数は、アクティブ セッション数を意味します。500 を超える上記クライアント アクセス オプションを使用してユーザを設定できますが、これらのオプションをいくつ組み合せても同時に存在するアクティブ セッション数は最大 500 個です。たとえば、500 人のユーザが利用しているシステムでは、各ユーザを Cisco Unified Personal Communicator、IMAP アクセス、Cisco Unity Inbox、および Inbox RSS フィード用に設定できますが、500 個のアクティブ セッションしかサポートされません。

- Cisco Unified Survivable Remote Site Telephony（SRST）の多くは、その名のとおり、リモート サイトにおける WAN 障害発生時のバックアップ コール処理用としてリモート サイトに配置されていました。Unified CMBE マルチサイト配置では、SRST をリモート サイトだけでなく、中央サイトでも使用できます（詳細については、「Survivable Remote Site Telephony（SRST）」（P.27-15）を参照してください）。

（注） 上で指定された上限を超えないようにして、システムをオーバーサブスクライブさせないように注意してください。システムの計画段階で、これらの上限を上回った場合、または上回りそうな場合は、代わりに、スタンドアロンの Cisco Unified CM および Cisco Unity Connection ソリューションを検討してください（詳細については、「システムの容量計画とスケーリング」（P.27-19）を参照してください）。

分散型コール処理を使用した Unified CMBE マルチサイト WAN 配置のメリット

分散型コール処理を使用したマルチサイト Unified CMBE 配置には次のようなメリットがあります。

- 複数の自律型 Unified CMBE システムと相互接続でき、各自律システムから次の機能が提供される。
  - 単一のプラットフォームでコール処理、Cisco Unified Mobility、および統合メッセージングに対応
  - 管理ユーザとエンド ユーザの両方にシングル サインオン機能を提供する、コール処理および統合メッセージングのための単一管理点
- 会社の Unified CM 配置と Unified CMBE 配置を相互接続できる。全社で同様の機能セットが提供され、Unified CMBE には専用の管理が適用される。
- IP WAN を使用して、ダイヤル先の公衆網番号により近いリモート サイトのゲートウェイ経由でコールを経路設定することによって、通話料金がかからないようにする。この方法は Tail-End Hop-Off（TEHO）と呼ばれている。
- 音声トラフィックと他の種類のトラフィックで IP WAN を共有することによって、使用可能な帯域幅を最大限利用できる。
- 各サイトにコール処理エージェントを配置することによって、IP WAN 障害が発生しても機能が失われない。

分散型コール処理を使用した Unified CMBE マルチサイト WAN 配置に関するベスト プラクティス

分散型コール処理を使用した Unified CMBE マルチサイト配置を実装する場合は、分散型コール処理を使用した Unified CM マルチサイト WAN 配置モデルのガイドライン、メリット、およびベスト プラクティスを参照してください（一般的な情報については、「Unified Communications の配置モデル」（P.2-1）の章を参照してください）。

加えて、次のガイドラインに留意してください。

- 可能な場合は、リモート支店とのコール アドミッション制御を提供するために、Unified CM 内のロケーション メカニズムを使用します。このメカニズムをさまざまな WAN トポロジに適用する方法については、「コール アドミッション制御」（P.9-1）の章を参照してください。Unified CMBE は、すべてのコール アドミッション制御メカニズムをサポートします。
- Unified CM とリモート ロケーション間の遅延を最小化して、音声カットスルー遅延（クリッピングとも呼ばれる）を削減します。
- 各 Unified CMBE 自律システムで、システム BHCA に対して指定された上限（3600 BHCA）を超えないようにします。分散型の Unified CM サイトまたは Unified CMBE サイトの場合は、特徴付けを誤ると、サイト間のコール量が増える可能性があるため、このことが非常に重要になります。システムの計画段階で、システム BHCA の上限を上回った場合、または上回りそうな場合は、代わりに、スタンドアロンの Cisco Unified CM および Cisco Unity Connection ソリューションを検討してください（詳細については、「システムの容量計画とスケーリング」（P.27-19）を参照してください）。

ダイヤル プラン

Cisco Unified CMBE は、ユーザが 500 人以下、サイト数が 20 以下の中堅企業のお客様に最適化されており、単一のハードウェア プラットフォーム上で音声、ビデオ、モビリティ、およびメッセージングのメリットを統合するコスト効率の良いソリューションを提供します。この種の配置に対してダイヤル プランをプロビジョニングする場合は、ダイヤル プランを単純で管理しやすいものにすることをお

勧めします。一貫性のある 4 桁の簡易ダイヤル プランがこの目標を満たしますが、この種のダイヤル プランがすべてのお客様とすべての配置に適合するわけではありません。ダイヤル プランの詳細については、「ダイヤル プラン」（P.10-1）の章を参照してください。

500 ユーザ未満の単一サイト配置の場合は、オンネット ダイヤリング用の 4 桁の簡易ダイヤル プランを使用すれば、プロビジョニングがかなり容易になります。ダイヤル プランには、次のような特徴を持たせる必要があります。

- ダイヤル プランは一貫している必要があります。より簡単にするには、重複しないようにダイヤル プランの境界を明確にします。たとえば、4 桁で重複する場合は、重複しなくなるまで桁数を増やします（「内線ダイヤリングの重複の防止」（P.10-8）を参照）。
- ダイヤル プランは短くする必要があります（4 桁など）。
- 必要に応じてサイト コードのみを使用します（「可変長のオンネット ダイヤル プラン」（P.10-11）の項でアクセス コードとサイト コードの使用方法を参照）。サイト コードを使用する場合はダイヤル プランが複雑になります。また、サイト数が多い配置では有効ですが、サイト数が少ない配置ではできるだけ避けるべきです。
- 単純なルート プラン設定では @ ワイルドカード マクロを使用します（「ルート パターン」（P.10-69）を参照）。@ ワイルドカードを使用する場合は、プレミアム サービス用の 900 番台などの特別なパターンを除外するために、ルート フィルタを使用しなければならない場合があります。よりスケーラブルなサービス クラス アプローチについては、「Unified CM におけるコール特権」（P.10-79）の項を参照してください。

表 27-2 に、4 桁の簡易ダイヤル プランの例を示します。

表 27-2　一般的な 4 桁固定ダイヤル プランでの番号割り当て

範囲	用途	DID 範囲	DID 以外の範囲
0XXX	除外（0 はオフネット アクセス コードとして使用される）		
1XXX	サイト A の内線番号	206 256 1XXX	該当なし
2XXX	サイト B の内線番号	775 789 2XXX	該当なし
3XXX	サイト C の内線番号	208 424 30XX	3[1-9]XX
4[0-4]XX	サイト D の内線番号	503 321 4[0-4]XX	該当なし
4[5-9]XX	サイト E の内線番号	450 555 4[5-9]XX	該当なし
5XXX	サイト A の内線番号	418 555 5XXX	該当なし
6XXX	サイト F の内線番号	514 555 6[0-8]XX	69XX
7XXX	予約（機能）[1]	XXX XXX 7XXX	7XXX
8XXX	予約（機能）*	XXX XXX 8XXX	8XXX
9XXX	除外（9 はオフネット アクセス コードとして使用される）		

1. 残りの範囲は、IP テレフォニー アプリケーション、Meet-Me 会議用の番号、ボイスメール統合番号などのさまざまな機能に使用できます。

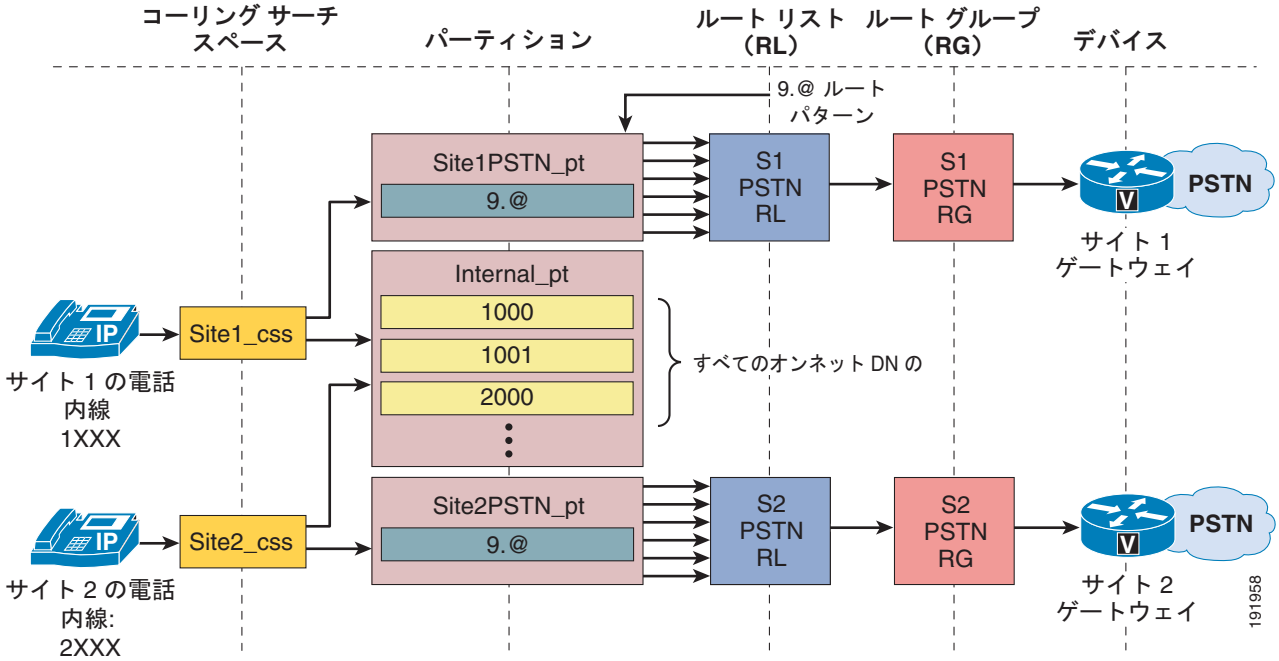
固定オンネット ダイヤル プランの配置

固定オンネット ダイヤル プランを実装するには、次のガイドラインに従います。

- 短縮内線番号を使用して、すべての電話を一意的に識別する。
- すべての電話番号を単一のパーティションに配置する。
- 各サイトで、選択したサービス クラス アプローチに従って、公衆網ルート パターンを 1 つまたは複数のサイト固有パーティションに配置する（「Unified CM におけるコール特権」（P.10-79）を参照）。

図 27-5 に、単一 Unified CM 配置の実装例を示します。内部内線番号を識別するための桁数を検討したときに、使用可能な DID 範囲が重複していなければ、このアプローチを使用してください。

図 27-5　固定オンネット ダイヤル プランの配置例



Survivable Remote Site Telephony（SRST）

Unified CMBE は、単一のハードウェア プラットフォーム上で単一の Unified CM インスタンスを使用して動作するため、デバイスは、呼制御を 2 次または 3 次 Unified CM にフェールオーバーできません。したがって、IP 電話機に対する呼制御機能の高可用性を実現するには、Cisco IOS ルータ上で使用可能な Cisco Unified Survivable Remote Site Telephony（SRST）を使用する必要があります。

SRST の多くは、その名のとおり、集中型コール処理配置のリモート サイトで、WAN 障害が発生して IP 電話機から 1 次、2 次、または 3 次 Unified CM に接続できない場合に高可用性を提供するために使用されていました。Unified CMBE 配置では、SRST を使用してリモート サイトと中央サイトの両方の IP 電話機に高可用性を提供できます。

基本的なコール機能を常に使用可能な状態にしておくことは IP テレフォニー配置設計の重要な側面です。また、Unified CMBE に接続できなくなった場合、それが障害やアップグレード後のアプライアンスの再起動が原因で WAN と中央サイトのどちらで発生した場合でも、IP 電話機のコール処理が損なわれないことを保証することも重要です。

ベスト プラクティスとガイドライン

ゲートウェイの呼制御プロトコルを選択する場合は、次の推奨事項に従ってください。

- SRST を使用しておらず、H.323 または SIP 機能を*必要としない*場合は、公衆網用のメディア ゲートウェイ コントロール プロトコル（MGCP）ゲートウェイを使用します。この実践によって、ダイヤル プランの設定と管理が容易になります。
- SRST を使用している場合は、H.323 や SIP などのステートレスまたはピアツーピアのゲートウェイ 呼制御プロトコルを使用します。MGCP は、堅牢で設定が容易ですが、SRST と一緒に配置したときに次のような欠点がある、ステートフル マスター / スレーブ ゲートウェイ 呼制御プロトコルです。
  - MGCP ゲートウェイ フォールバックがデフォルトの H.323 または SIP セッション アプリケーションに移行します。そのため、SRST モードの外部コール用の H.323 または SIP 設定が必要になります。
  - T1 と E1 PRI に対する MGCP フォールバックが発生した場合にコール プリザベーションが行われません（MGCP アナログと T1 CAS の場合のみ）。代わりに、PRI に対する MGCP フォールバックが発生すると、すべてのアクティブ コールが失われます。H.323 と SIP を使用すれば、SRST モードへのフェールオーバーを伴う T1 および E1 PRI 上でのコール プリザベーションが実現できます。SRST モードの電話機では、公衆網へのダイヤル アウトが可能であり、アクティブ コールはそのまま維持されます。

    逆に、Unified CMBE への接続が可能になったときに同じプロセスが発生します。MGCP PRI が Unified CM に復帰して、PRI 上のすべてのアクティブ コールが失われます。SIP と H.323 を使用すれば、コール プリザベーションが維持されます。

SRST の詳細については、「リモート サイトのサバイバビリティ（呼処理の継続）」（P.2-7）を参照してください。

SRST をバックアップ コール処理エージェントとして使用する場合は、次のガイドラインに従ってください。

- SRST モードでは、サイト間コールか外部コールかに関係なく、すべてのコールに対して公衆網の使用をお勧めします。複数のサイトとの WAN リンクは確立されているが、Unified CM との WAN リンクが確立されていない場合は、このようなリンクをサイト間コールに使用すると有益な場合があります。ただし、コール アドミッション制御または自動代替ルーティング用のメカニズムがない場合は、コールが IP WAN 上でオーバーサブスクライブする可能性があります。そのため、SRST モード中はすべてのコールに対して公衆網を使用するようにすれば、ゲートキーパーなどのコール アドミッション制御用デバイスの設定が簡略化されます。
- フェールオーバーとフェールバックは、なるべく、エンド ユーザに知られないように実施する必要があります。ユーザが Unified CM コール処理を使用して設定したものと同じまたは等価のダイヤル プランを SRST モードで提供するようにすれば、ユーザは、フェールオーバー モード時に新しいダイヤリング パターンとルールのセットを覚える必要がありません。次の推奨事項が、フェールオーバー時のユーザ エクスペリエンスの向上に役立つ可能性があります。
  - 短縮ダイヤル経由で電話をかけるために簡易ダイヤル プランを使用している場合は、ボイス トランスレーション プロファイルとルールを使用して短縮ダイヤルを E.164 番号に変換することによって、正確な番号を公衆網に送出できます。詳細については、次の URL で入手可能な『*Number Translation using Voice Translation Profiles*』を参照してください。

    http://www.cisco.com/en/US/tech/tk652/tk90/technologies_configuration_example09186a00803f818a.shtml
  - 桁間タイムアウトを避けるために、ダイヤルピアをそのままの形で設定します。北米のほとんどの音声構成では、電話番号の桁数がすべて同じなため、すべてのダイヤルピアの宛先パターンが同じ長さの固定長ダイヤル プランで十分です。ただし、音声ネットワーク構成によっては、可変長ダイヤル プランが必要な場合もあります（国際電話など）。

- 桁間タイムアウト タイマーは、# 記号をダイヤルすることによって即座に止めることができます。SRST ゲートウェイが次の桁を待っている間に、ユーザが # 記号をダイヤルした場合は、# 記号がダイヤル完了アクセラレータとして扱われます。# 記号は、宛先パターン内では実際の桁として扱われないため、ダイヤルする文字列の一部としてネットワークに送信されることはありません。
- 集中型コール処理を使用した Unified CM マルチサイト配置では、通常、Unified CM 内のパーティションとコーリング サーチ スペースを使用してサービス クラスが実装されます（「従来のアプローチによる Unified CM のサービス クラスの構築」（P.10-40）と「回線/デバイス アプローチによる Unified CM のサービス クラスの構築」（P.10-44）を参照）。ただし、支店サイトと中央サイト間の IP WAN 接続が失われた場合は、Cisco Unified SRST によって支店の IP 電話機が制御されるため、IP WAN 接続が復旧するまでパーティションとコーリング サーチ スペースに関するすべての設定が使用できなくなります。そのため、SRST モードで動作している支店ルータ内でサービス クラスを実装すると有益な場合があります（「H.323 を使用している Cisco IOS でのサービス クラスの構築」（P.10-52）を参照）。

Unified CMBE のディレクトリ管理

Cisco Unified CMBE では、Cisco Unified CM と Cisco Unity Connection の User Web ページと Administration Web ページにアクセスするためのシングル サインオン機能がエンド ユーザと管理者に提供されます。この機能を使用すれば、Unified CM 管理者は、Unified CM Administration ページにログインすることによって、他の認証を受けずに Unity Connection Administration ページも管理できます。

Unified CMBE では、Unified CM データベースがユーザに関する信頼すべき情報源です。これは、Unified CM Administration Web ページからしかユーザの作成および削除が行えないことを意味します。ユーザを作成すると、Cisco Unity Connection 固有のプロパティを Unity Connection Administration ページから設定できるようになります。同様に、Unified CM Administration ページは、電話統合に関する信頼すべき情報源です。そのため、電話統合は Unified CM 上で設定して、Cisco Unity Connection にインポートします。

リリース 7.0 以降の Unified CMBE で、社内ディレクトリ統合がサポートされています。この機能を使用すれば、Unified CMBE で LDAP 統合を使用して直接既存の社内ディレクトリと統合できます。この機能のメリットは、管理者がユーザを社内ディレクトリから Unified CMBE データベースに自動的にプロビジョニングできることであり、これによって、管理者は個々のディレクトリではなく、1 つのディレクトリだけを管理すれば済むようになります。この方法では、社内ディレクトリが変更されるたびに、対象となるユーザ情報を手動で追加、削除、または修正する必要がありません。もう一つのメリットは、エンド ユーザがシングル サインオン機能を利用できることであり、これによって、アプリケーションで共通ディレクトリが共有され、ネットワーク上のパスワード数が減少します。

Unified CMBE 7.*x* は、次の種類の社内ディレクトリをサポートします。

- Microsoft Active Directory 2000
- Microsoft Active Directory 2003
- Netscape Directory Server 4.x
- iPlanet Directory Server 5.1
- Sun One Directory Server 5.2

Unified CMBE ディレクトリの機能の要約を次に示します。

- アプリケーション ユーザとエンド ユーザが Unified CM から Cisco Unity Connection にインポートされます。
  - Unified CM アプリケーション ユーザは Cisco Unity Connection 管理ユーザとしてインポートされます。
  - Unified CM エンド ユーザは Cisco Unity Connection ボイスメール ユーザとしてインポートされます（ユーザにはプライマリ電話番号を関連付ける必要があります。そうしなければ、Unity Connection へのインポート時に無視されます）。
  - Cisco Unity Connection アプリケーション内ではユーザの作成および削除はできません。
  - Unity Connection Administration ページでは、共通ユーザ プロパティが読み取り専用として扱われます。
  - Cisco Unity Connection ユーザは、対応する Unified CM ユーザがいなければ存在できません。
  - 管理ユーザは、Cisco Unity Connection と Cisco Unified CM の両方で Bulk Administration Tool（BAT）をバッチ モードで使用できます。
- 電話統合が Unified CM から Cisco Unity Connection にインポートされます。
  - 統合は 1 つしか存在しません。
  - ポート グループとポートが Unified CM からインポートされます。
- PIN とパスワードは、Unified CM データベースである中央のデータ ストアに保存されます。これによって、シングル サインオン機能が使用できます。
- Unified CM Administration Web ページで共通ユーザ プロパティが変更されると、即座に、Unity Connection データベースに反映されます。
- 孤立した Unity Connection ユーザは、再度関連付けるか、削除することができます。
- シングル サインオン（SSO）を使用すれば、システム管理者は、Unified CM Administration、Unified CM Serviceability、Unity Connection Administration、Unity Connection Serviceability などの管理されたすべての Web インターフェイスに同時にログインできます。また、エンド ユーザは、Unified CM User ページと Unity の Cisco Personal Communications Assistant に同時にログインできます。
- シングル サインオンは、プラットフォームの OS 管理や災害復旧 Web アプリケーションには適用されません。
- Unified CMBE は、社内ディレクトリの LDAP 同期および認証をサポートします。
  - Unified CM には、システムに追加できるアカウント数の制限がありません。ユーザ数が 3,000 人を超えないようにシステムを管理する必要があります。アプリケーション用のアカウントが必要な場合や、設計によっては追加のアカウントが必要な場合があります。一般的なルールとして、LDAP データベースのサイズに関係なく、インポートするユーザ アカウント数は最小限に抑えます。これによって、最初とそれ以降の定期同期化の速度が改善され、ユーザ アカウントの管理可能性も向上します。
  - ディレクトリ統合の詳細については、「LDAP ディレクトリ統合」（P.17-1）を参照してください。
- 次の Unified CMBE 設定制限は、Cisco Unity Connection との統合にも適用されます。
  - 最大 50 個のサービス クラス
  - 最大 50 個のコール ハンドラ
  - 最大 50 個のコール ルーティング ルール
  - 最大 50 個の公開配布リスト

Unified CMBE の移行

Unified CMBE からスタンドアロンの Unified CM への直接移行は現在サポートされていません。ただし、Unified CM 7.0 以降では、Cisco Media Convergence Server（MCS）7828-H3 または MCS 7828-I3 を新しいクラスタ内の Unified CM パブリッシャまたは既存のクラスタ内のサブスクライバとして再定義できます。ただし、MCS 7828 は Cisco Unity Connection サーバとして再インストールできません。

MCS 7828-H3 と 7828-I3 のプラットフォームを Cisco Unified CM と一緒に使用すると、MCS 7825-H3 および 7825-I3 と同等の性能とスケーラビリティが得られます。MCS 7828 プラットフォームの方がより多くのメモリとディスク スペースを搭載していますが、MCS 7825 プラットフォームの CPU とディスク スピードは同等であり、CPU と I/O Wait の性能がサーバの同等性を示す主要素になります。

（注）　Cisco MCS 7828-H3 と 7828-I3 は Unified CMBE と一緒に出荷されるため、Cisco Unified CMBE ソフトウェア パッケージがなければ注文できません。

システムの容量計画とスケーリング

この項では、Unified CMBE のオーバーサブスクリプションを回避するためのシステム使用計画に関するいくつかのルールとガイドラインを提供します。また、統合されたアプリケーションと、Unified CMBE システムの容量計画を支援可能な一部の計算に関するサポート対象システムの制限についても説明します。

Unified CM には、種類の異なるデバイス（IP 電話、ボイスメール ポート、CTI デバイス、ゲートウェイ、トランスコーディングや会議などの DSP リソースなど）を登録できます。これらのデバイスには、登録先のアプライアンス プラットフォームのリソースが必要です。必要なリソースには、メモリ、プロセッサ使用、およびディスク I/O が含まれます。デバイスは、トランザクション（通常はコールの形態）中により多くのシステム リソースを消費します。たとえば、1 時間あたり 6 回のコールだけを行うデバイスが消費するリソースは、1 時間あたり 12 回のコールを行うデバイスより少なくなります。

この項では、システムがオーバーサブスクライブしないことを保証するための配置計画の側面として、Busy Hour Call Attempts（BHCA）について説明します。Unified CMBE と一緒に Cisco Unified Presence や Cisco Unified MeetingPlace Express などのその他の Cisco Unified Communications アプリケーションを別のサーバ上で使用する予定の場合は、Unified CMBE の性能と容量に影響を与える要素を思い出してください（「Cisco Unified Presence」（P.22-1）と「Cisco Unified MeetingPlace Express」（P.15-1）の章を参照）。BHCA や CTI ポートなどの要素が、数少ない考慮すべきコンポーネントです。

Busy Hour Call Attempts（BHCA; 最繁時呼数）

BHCA は、最繁時のデバイスおよび 1 時間あたりの平均コール回数です（多くのシステムの最繁時は、午前 10:00 ～ 11:00 または午後 2:00 ～ 3:00 です）。Unified CMBE は、最大 3,600 BHCA をサポートします。システム使用の計算では、Unified CMBE がオーバーサブスクライブしないために 3,600 BHCA を超えないようにします。

任意の電話機の BHCA が 4 を超えたときに、BHCA に対する配慮が必要になります。真の BHCA 値は、最繁時における電話機の使用状況の基準測定を実施することによってのみ、決定されます。この使用状況を基準なしで見積もった場合は特に注意が必要です。

デバイスの見積もり

デバイスの見積もりは、この目的の主な 2 つのカテゴリである電話デバイスとトランク デバイスに分けることができます。

電話デバイスは、単一のコール可能なエンドポイントです。これには、Cisco Unified IP Phone 7900 シリーズなどの単体のクライアント デバイス、Cisco IP Communicator や Cisco Unified Presence Client などのソフトウェア クライアント、FXS/FXO ポートや H.323 クライアントなどが含まれます。

トランク デバイスは、複数のコールを複数のエンドポイントまで伝送します。これには、SIP トランクや H323 トランクなどのデバイスから、ゲートウェイ 、MGCP バックホール BRI、PRI トランク、さらにゲートキーパー制御の H323 トランクまでが含まれます。BHCA を見積もる方法は、両方のデバイスでほとんど同じですが、一般に、トランク デバイスは、外部のユーザ グループ（公衆網または PBX 拡張）にアクセスするためにより大きなエンドポイントのグループで使用されるため、BHCA が高くなります。

BHCA に基づく使用状況の特性を参照してデバイス グループ（電話デバイスまたはトランク デバイス）を定義してから、各デバイス グループの BHCA を加算して、システムの総 BHCA を求めることができます。これによって、3,600 BHCA を超えないことが保証されます。たとえば、4 BHCA の 100 台の電話機と 12 BHCA の 80 台の電話機の総 BHCA は次のように計算することができます。

4 BHCA の 100 台の電話機：100 × 4 = 400

12 BHCA の 80 台の電話機：80 × 12 = 960

総電話機 BHCA = (100 × 4) + (80 × 12) = 1360 BHCA

トランク デバイスの場合は、公衆網上で開始または終了するデバイスからのコールの割合がわかっていれば、BHCA を計算することができます。この例では、すべてのデバイス コールの半分が公衆網上で開始または終了している場合、ゲートウェイに対するデバイス BHCA の正味効果（この場合は 1360）は、1360 の半分、つまり、680 になります。したがって、この例での電話デバイスとトランク デバイスに関する総システム BHCA は次のようになります。

総システム BHCA = 1360 + 680 = 2040 BHCA

複数の電話機で回線を共有している場合は、回線を共有している電話機ごとに 1 つずつのコール レッグ（コールごとに 2 コール レッグ）を BHCA に含める必要があります。複数のデバイス グループで共有されている回線は、そのグループの BHCA に影響します。つまり、共有回線に対する 1 つのコールが、回線インスタンスあたり 1 つのコール レッグ、つまり、1 コールの半分として計算されます。BHCA が異なる複数の電話機グループがある場合は、次の方法で BHCA 値を計算します。

共有回線 BHCA = 0.5 ×（共有回線数）×（1 回線あたりの BHCA）

たとえば、次の特徴を持つ 2 つのユーザ クラスがあるとします。

8 BHCA の 100 台の電話機 = 800 BHCA

4 BHCA の 150 台の電話機 = 600 BHCA

また、1 グループあたり 10 本の共有回線があるとして、次の BHCA 値に加算します。

8 BHCA のグループ内の 10 本の共有回線 = 0.5 × 10 × 8 = 40 BHCA

4 BHCA のグループ内の 10 本の共有回線 = 0.5 × 10 × 4 = 20 BHCA

この場合のすべての電話デバイスに関する総 BHCA は、共有回線の BHCA の合計に加算された電話機グループごとの BHCA の合計になります。

800 + 600 + 40 + 20 = 2,720 総 BHCA

この使用レベルは、システム上限の 3,600 BHCA を下回っているため、許容範囲に含まれます。

シングル ナンバー リーチ（SNR）用に Cisco Unified Mobility を使用している場合は、リモート接続先が BHCA に影響することに留意してください。アプライアンスがオーバーサブスクライブするのを防ぐには、この SNR リモート接続先の BHCA を考慮する必要があります。リモート接続先の BHCA を計算するには、「Cisco Unified Mobility」（P.27-24）の項を参照して、その値を総 BHCA 値に加算します。

（注）　Secure RTP（SRTP）を使用したメディア認証と暗号化は、システム リソースとシステム性能に影響を与えます。メディア認証または暗号化の使用を検討している場合は、この事実に留意して適切な調整を行ってください。通常、セキュリティに対応していない 100 台の IP 電話機は、セキュリティに対応した 90 台の IP 電話機と同じ影響をシステム リソースに与えます（10 対 9 の割合）。

考慮すべきもう一つの側面がコール カバレッジです。特殊なデバイス グループを作成し、特定のサービスの着信コールを複数のルール（トップダウン、循環ハント、最長アイドル時間、またはブロードキャスト）に従って処理することができます。これは、Unified CM の 回線グループ設定で実現されます。この要素によっても BHCA が影響を受ける可能性がありますが、それはあくまでもブロードキャストの回線グループ配信アルゴリズム（すべてのメンバーを呼び出す）に関係しているためです。回線グループと配信アルゴリズムの詳細については、http://www.cisco.com で入手可能な『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

Unified CMBE でブロードキャストの配信アルゴリズムが必要な場合は、1 つの回線グループのメンバー数を 3 以下にすることをお勧めします。システムの負荷によっては、この実施によって、システムの BHCA が大きく影響され、サーバのリソースがオーバーサブスクライブする可能性があります。ブロードキャストの配信アルゴリズムを使用する回線グループ数も 3 以下に制限する必要があります。

コンタクト センターの例

この例では、Cisco Unified Contact Center Express が Unified CMBE と統合され、次のようなシステム特性があるものとします。

- 必要な仕様は、最繁時に 1 時間あたり最大 30 コールの 15 人のコンタクト センター エージェントに関するものです。
- 平均使用率が 4 BHCA の非エージェント ユーザが 96 人いて、各ユーザは Cisco Unified Mobility を使用してシングル ナンバー リーチ用の 1 つのリモート接続先を設定できます。
- また、平均使用率が 10 BHCA の非エージェント ユーザが 36 人いて、各ユーザはシングル ナンバー リーチ用の 1 つのリモート接続先を設定できます。
- 20 本の予備共有回線があり、そのうちの 10 本は平均使用プールの 10 ユーザで共有され、残りの 10 本は大量使用プールの 10 ユーザで共有されます。
- 全トランクの合計が 1200 BHCA の 7 個の T1 トランク（最大 161 の同時コールが可能）があります。

（注）　この例では、すべてのゲートウェイ トランクに関する BHCA を 1 つの総トランク BHCA 値にまとめます。この方法は主として、単一サイト配置に適していますが、マルチサイト配置では、さまざまなサイトのトランクによってさまざまな BHCA 要件が設定されるため、複数の BHCA グループ分けが必要になります。

このシステムの BHCA 計算は次のようになります。

30 BHCA の 15 人のコンタクト センター エージェント = 450 BHCA

4 BHCA の 96 人の平均使用ユーザ = 384 BHCA

10 BHCA の 36 人の大量使用ユーザ = 360 BHCA

4 BHCA グループ内の 10 本の共有回線 = 20 BHCA

10 BHCA グループ内の 10 本の共有回線 = 50 BHCA

すべての T1 トランクの総 BHCA = 1,200 BHCA

4 BHCA の 96 人の平均使用ユーザごとの、シングル ナンバー リーチ用の 1 つのリモート接続先 = 192 BHCA（この計算の詳細については、「Cisco Unified Mobility」（P.27-24）を参照してください）。

10 BHCA の 36 人の大量使用ユーザごとの、シングル ナンバー リーチ用の 1 つのリモート接続先 = 180 BHCA（この計算の詳細については、「Cisco Unified Mobility」（P.27-24）を参照してください）。

この場合のすべてのエンドポイント デバイスの総 BHCA は次のとおりです。

(450 + 384 + 360 + 20 + 50 + 192 + 180 + 1200) = 2,836 BHCA

このレベルの使用状況は、システム上限の 3,600 BHCA を下回っているため、許容範囲であり、約 800 BHCA の余裕があります。

Cisco Unified CM アプリケーション

Cisco Unified CM アプリケーションは、基本的な IP テレフォニーの多くの処理と機能を拡張します。Unified CM には、次のような追加機能を提供する統合アプリケーションも多数含まれています。この項では、Unified CM アプリケーションとそれらを Cisco Unified CMBE と一緒に使用した場合の性能と容量を列挙します。Unified CM アプリケーションの詳細については、「Cisco Unified CM アプリケーション」（P.24-1）の章を参照してください。

Cisco Extension Mobility（EM）

Cisco Extension Mobility を使用すれば、Cisco Unified IP Phone にログインして、一時的にその電話機を独自の設定にすることができます。

Unified CMBE 内の EM アプリケーションは、1 分あたり 26 回の連続ログインまたはログアウトをサポートします。1 分あたり 26 回のログイン / ログアウトを超えなければ、EM に対してすべてのユーザを有効にできます。

Cisco Unified Communications Manager Assistant（Unified CM Assistant）

Unified CM Assistant を使用すれば、アシスタントが、関連するマネージャの着信電話コールを受けることができます。

Unified CM Assistant アプリケーションは、次の容量をサポートします。

- マネージャあたり最大 10 人のアシスタントを設定できます。
- 1 人のアシスタントに対して最大 10 人のマネージャを設定できます（Unified CM Assistant によって制御された回線が 1 本ずつ各マネージャに割り当てられている場合）。
- Unified CMBE システムあたり最大 10 人のアシスタントと 10 人のマネージャを設定できます。

Unified CM Assistant アプリケーションは CTIManager と相互作用しながら、回線監視および電話機制御を行います。アシスタントまたはマネージャの電話機の回線ごとに CTIManager への接続が確立されます。加えて、Unified CM Assistant ルート ポイントごとに CTIManager への接続が確立されま

す。Unified CM Assistant を設定する場合は、CTI 接続の総合限度（Cisco Unified CMBE の場合は 500 CTI 接続）に照らして、必要な CTI 接続数を検討する必要があります。他のアプリケーションの CTI 接続を追加する必要がある場合は、Unified CM Assistant の容量が制限される可能性があります。

Cisco Unified Communications Manager Attendant Console（AC）

Unified CMBE を実行しているネイティブな AC アプリケーションは、次の容量をサポートします。

- 最大 6 人の受付係
- 最大 10 個のパイロット ポイント

Cisco Media Convergence Server（MCS）7828 プラットフォームは、最大 50 台の AC デバイスをサポートします。

（注）　AC デバイスの容量数は、パイロット ポイントとパイロット ポイント ハント グループのメンバーで分割することができます。たとえば、AC デバイスの最大数は 50 です。この容量は、メンバーが 50 の 1 個のパイロット ポイントや、各パイロット ポイント ハント グループのメンバーが 5 ずつの 10 個のパイロット ポイントなど、さまざまな方法で分割することができます。

Cisco AC アプリケーションは CTIManager と相互作用しながら、回線監視および電話機制御を行います。受付係の電話機の回線ごとに CTIManager への接続が確立されます。加えて、AC パイロット ポイントごとに CTIManager への接続が確立されます。AC アプリケーションを設定する場合は、CTI 接続の総合限度（Cisco Unified CMBE の場合は 500 CTI 接続）に照らして、必要な CTI 接続数を検討する必要があります。他のアプリケーションの CTI 接続を追加する必要がある場合は、AC アプリケーションの容量が制限される可能性があります。

（注）　Unified CMBE 6.*x* からのアップグレードで、ネイティブ AC がインストールおよび設定されている場合を除いて、Unified CMBE 7.x ではネイティブ AC がサポートされません。

その他のアテンダント コンソール アプリケーションの Cisco Unified Business Attendant Console と Cisco Unified Department Attendant Console も別のアプリケーション サーバ上で使用できます。これらのアプリケーションの場合も上記 AC 容量ガイドラインに従ってください。ただし、これらのアプリケーションはそれぞれ最大 2 人の受付係をサポートすることに留意してください。Cisco Unified Business Attendant Console と Cisco Unified Department Attendant Console の詳細については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

Cisco WebDialer

WebDialer は、サポートされている任意の電話デバイスを使用して PC から簡単にコールを発信できるようにする Unified CM 用のクリックダイヤル アプリケーションです。WebDialer サービスは Unified CM 上で動作し、Unified CMBE の最大 BHCA 容量（1 秒あたり 1 件のコール、つまり、1 時間あたり 3,600 件のコール）をサポートできます。

WebDialer の総 BHCA を計算するには、次の式を使用します。

総 WebDialer BHCA =（ユーザ数）×（ユーザあたりの BHCA）

通常、結果は、Unified CMBE の総ユーザ BHCA と同じになります。ユーザが電話機と WebDialer アプリケーションのどちらからダイヤルしたかに関係なく、予想される BHCA は変わらないはずです。

Cisco Unified Mobility

モバイル コネクト（一般的にはシングル ナンバー リーチ（SNR）と呼ばれている）として知られる Cisco Unified Mobility アプリケーションを使用すれば、Unified CM からの着信コールを最大 4 台の携帯電話や IP 電話などの指定されたクライアント デバイスにリダイレクトできます。

Unified CMBE における Unified Mobility ユーザの容量は、SNR を関連付ける電話機の BHCA に依存します。そのため、サポートされるリモート接続先数は、それらの電話機の BHCA に直接依存します。次にガイドラインを示します。

- デバイス プロファイルごとに最大 4 個のリモート接続先を設定できます。
- BHCA に影響を与えるリモート接続先ごとにコストが関連付けられます。リモート接続先ごとに、1 つずつの追加のコール レッグが使用されます。通常、コールは 2 つのコール レッグで構成されているため、1 つのリモート接続先の呼び出しが 1 つのコールの半分に相当します。そのため、リモート接続先の BHCA は次の式で計算できます。

  リモート接続先 BHCA = 0.5 ×（ユーザ数）×（ユーザまたは電話機の BHCA）

次の例を参考にしてください。

それぞれが 5 BHCA の 300 人のユーザがいて、それぞれのユーザに 1 つずつのリモート接続先（全部で 300 個のリモート接続先）が割り当てられたシステムがあるとすると、リモート接続先 BHCA の計算は次のようになります。

リモート接続先 BHCA = 0.5 × 300 × 5 = 750 BHCA

この例の総ユーザ BHCA は 300 × 5 = 1500 で、リモート接続先 BHCA は 750 です。したがって、この例の総システム BHCA は、配置内にこの 2 つ以外に BHCA 変数が存在しないと仮定すると、1500 +750 = 2250 となります（詳細については、「デバイスの見積もり」（P.27-20）の項を参照してください）。

APPENDIX A

Recommended Hardware and Software Combinations

Last revised on: August 5, 2008

For the most recent information on recommended hardware platforms, software releases, and firmware versions for Cisco Unified Communications System deployments based on Cisco Unified Communications Manager (Unified CM), frequently refer to the latest *Cisco Unified Communications System Release Notes for IP Telephony* available at the following location:

http://www.cisco.com/en/US/products/ps6884/tsd_products_integrated_systems_documentation09186a0080621410.html

Note The platforms and software versions recommended in the *System Release Notes for IP Telephony* are not the only supportable deployment options. They represent the combinations of hardware and software that Cisco has subjected to the most extensive system-level tests. These ongoing tests are conducted using a variety of deployment models, several end-station size categories, and realistic call flows, traffic patterns, and use cases. For information on other possible hardware and software options for Cisco Unified Communications deployments, contact your Cisco account representative.

For additional information on the Cisco Unified Communications System, refer to the documentation available at:

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

GLOSSARY

A

AA	Automated Attendant; 自動応答機能
AAD	Alerts and Activities Display; 警告とアクティビティの表示
AAR	Automated Alternate Routing
AC	Cisco Attendant Console
ACD	Automatic Call Distribution; 自動着信呼分配
ACE	Cisco Application Control Engine
ACF	Admission Confirm; アドミッション確認
ACL	Access Control List; アクセス コントロール リスト
ACS	Access Control Server
AD	Microsoft Active Directory
ADPCM	Adaptive Differential Pulse Code Modulation; 適応的差分パルス符号変調
ADUC	Active Directory Users and Computers; Active Directory ユーザとコンピュータ
AES	Advanced Encryption Standard; 高度暗号化規格
AFT	ALI Formatting Tool; ALI フォーマット ツール
AGM	Cisco Access Gateway Module; Cisco アクセス ゲートウェイ モジュール
ALG	Application Layer Gateway; アプリケーション レイヤ ゲートウェイ
ALI	Automatic Location Identification; 自動ロケーション識別
AMI	Alternate Mark Inversion; 交互マーク反転
AMIS	Audio Messaging Interchange Specification
AMWI	Audible Message Waiting Indication; 音声メッセージ待機インジケータ
ANI	Automatic Number Identification; 自動番号識別
AP	Access Point; アクセス ポイント
API	Application Program Interface; アプリケーション プログラミング インターフェイス

ARJ Admission Reject; アドミッション拒否

ARP Address Resolution Protocol; アドレス解決プロトコル

ARQ Admission Request; アドミッション要求

ASA Cisco Adaptive Security Appliance

ASP Active Server Page

ASR Automatic Speech Recognition; 自動音声認識

ATA Cisco Analog Telephone Adapter

ATM Asynchronous Transfer Mode; 非同期転送モード

AXL AVVID XML Layer

B

BAT Cisco Bulk Administration Tool

BBWC Battery-Backed Write Cache; バッテリ バックアップ付き書き込みキャッシュ

BGP Border Gateway Protocol; ボーダー ゲートウェイ プロトコル

BHCA Busy Hour Call Attempt; 最繁時呼数

BHCC Busy Hour Call Completion; 最繁時呼完了数

BLF Busy Lamp Field; ビジー ランプ フィールド

BPDU Bridge Protocol Data Unit; ブリッジ プロトコル データ ユニット

bps Bits Per Second; ビット / 秒

BRI Basic Rate Interface; 基本速度インターフェイス

BTN Bill-To Number; 請求先番号

C

CA Certificate Authority; 認証局

CAC Call Admission Control; コール アドミッション制御

CAM Content-Addressable Memory; 連想メモリ

CAMA Centralized Automatic Message Accounting

CAPF Certificate Authority Proxy Function

CAR	Cisco CDR Analysis and Reporting; Cisco CDR 分析とレポート
CAS	Channel Associated Signaling; 個別線信号方式
CBWFQ	Class-Based Weighted Fair Queuing; クラスベース WFQ
CCA	Clear Cannel Asessment
CCS	Common Channel Signaling; 共通線信号方式
CDP	Cisco Discovery Protocol; シスコ検出プロトコル
CDR	Call Detail Record; コール詳細レコード
CGI	Common Gateway Interface
CIF	Common Intermediate Format
CIR	Committed Information Rate; 設定情報レート
CKM	Cisco Centralized Key Management
CLEC	Competitive Local Exchange Carrier; 競争的地域通信事業者
CLID	Calling Line Identifier; 発呼回線 ID
CM	Cisco Unified Communications Manager（Unified CM）
CMC	Client Matter Code; クライアント識別コード
CME	Cisco Unified Communications Manager Express（Unified CME）
CMI	Cisco Messaging Interface
CMM	Cisco Communication Media Module; Cisco コミュニケーション メディア モジュール
CNG	Comfort Noise Generation; コンフォート ノイズ生成
CO	Central Office; セントラル オフィス
同じ場所にある（Co-located）	同じ物理的な場所にある複数のデバイスを指します。これらのデバイスの間に WAN または MAN 接続はありません
COM	Component Object Model; コンポーネント オブジェクト モデル
COR	Class Of Restriction; 制限クラス
共存（Co-resident）	同じサーバ上で複数のサービスまたはアプリケーションが実行されている状態
CoS	Class of Service; サービス クラス
CPCA	Cisco Unity Personal Assistant
CPI	Cisco Product Identification ツール
CPN	Calling Party Number; 発番号

CRS Cisco Customer Response Solution

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

CSTA Computer-Supported Telecommunications Applications

CSUF Cross-Stack UplinkFast

CTI Computer Telephony Integration; コンピュータ / テレフォニー インテグレーション

CTL Certificate Trust List

CUBE Cisco Unified Border Element（以前の Cisco Multiservice IP-to-IP Gateway（IP-IP ゲートウェイ））

CUE Cisco Unity Express

CVTQ Cisco Voice Transmission Quality

D

DC Domain Controller; ドメイン コントローラ

DDNS Dynamic Domain Name Server; ダイナミック ドメイン ネーム サーバ

DDR Delayed Delivery Record

DFS Dynamic Frequency Selection; 動的周波数選択

DHCP Dynamic Host Configuration Protocol; ダイナミック ホスト コンフィギュレーション プロトコル

DID Direct Inward Dial; ダイヤルイン

DIT Directory Information Tree; ディレクトリ インフォメーション ツリー

DMVPN Dynamic Multipoint Virtual Private Network; Dynamic Multipoint バーチャル プライベート ネットワーク

DMZ Demilitarized zone; 非武装地帯

DN Directory Number; ディレクトリ番号

DNIS Dialed Number Identification Service; 着信番号識別サービス

DNS Domain Name System; ドメイン ネーム システム

DoS Denial of Service; サービス拒絶

DPA Digital PBX Adapter

DSCP Differentiated Services Code Point

DSE Digital Set Emulation

DSP Digital Signal Processor; デジタル シグナル プロセッサ

DTIM Delivery Traffic Indicator Message

DTMF Dual Tone MultiFrequency

DTPC Dynamic Transmit Power Control; ダイナミック伝送パワー コントロール

DUC Domino Unified Communications Services

E

E&M 受信（recEive）と送信（transMit）、または Ear and Mouth

EAP Extensible Authentication Protocol

EC Echo Cancellation; エコー キャンセレーション

ECM Error Correction Mode; エラー訂正モード

ECS Empty Capabilities Set

EI Enhanced Image

EIGRP Enhanced Interior Gateway Routing Protocol

ELIN Emergency Location Identification Number; 緊急ロケーション識別番号

EM Extension Mobility; エクステンション モビリティ

ER Cisco Emergency Responder

ERL Emergency Response Location; 緊急応答ロケーション

ESF Extended Super Frame; 拡張スーパー フレーム

F

FAC Forced Account Code; 強制アカウント コード

FCC Federal Communications Commission; 米国連邦通信委員会

FIFO First-In, First-Out; ファーストイン ファーストアウト

FQDN Fully Qualified Domain Name; 完全修飾ドメイン名

FR Frame Relay; フレーム リレー

FWSM Firewall Services Module

FXO Foreign Exchange Office

FXS Foreign Exchange Station

G

GARP Gratuitous Address Resolution Protocol

GC Global Catalog; グローバル カタログ

GKTMP Gatekeeper Transaction Message Protocol

GLBP Gateway Load Balancing Protocol

GMS Greeting Management System; グリーティング管理システム

GPO Group Policy Object; グループ ポリシー オブジェクト

GPRS General Packet Radio Service

GSM Global System for Mobile Communication

GSS Global Site Selector

GUI Graphical User Interface; グラフィカル ユーザ インターフェイス

GUP Gatekeeper Update Protocol

H

H.225D H.225 Daemon; H.225 デーモン

HDLC High-Level Data Link Control; ハイレベル データリンク コントロール

HP Hewlett-Packard

HSRP Hot Standby Router Protocol; ホットスタンバイ ルータ プロトコル

HTTP Hyper-Text Transfer Protocol; ハイパーテキスト転送プロトコル

HTTPS Secure HTTP; セキュア HTTP

Hz Hertz; ヘルツ

I

IANA Internet Assigned Numbers Authority

IAPP Inter-Access Point Protocol; アクセス ポイント間プロトコル

ICCS Intra-Cluster Communication Signaling

ICMP Internet Control Message Protocol; インターネット制御メッセージ プロトコル

ICS IBM Cabling System; IBM 配線システム

ICT Intercluster Trunk; クラスタ間トランク

IETF Internet Engineering Task Force; インターネット技術タスク フォース

IGMP Internet Group Management Protocol; インターネット グループ管理プロトコル

IIS Microsoft Internet Information Server

IM Instant Messaging; インスタント メッセージング

IMAP Internet Message Access Protocol

IntServ Integrated Service; 統合サービス

IntServ/DiffServ Integrated Service/Differentiated Service; 統合サービス / ディファレンシエーテッド サービス

IP Internet Protocol; インターネット プロトコル

IPCC Cisco IP Contact Center

IPIPGW IP-to-IP Gateway; IP-to-IP ゲートウェイ

IPPM Cisco IP Phone Messenger

IPSec IP Security

ISO International Standards Organization; 国際標準化機構

ITEM CiscoWorks IP Telephony Environment Monitor

ITU International Telecommunication Union; 国際電気通信連合

IVR Interactive Voice Response; 音声自動応答装置

J

JTAPI Java Telephony Application Programming Interface

K

kbps Kilobits per second; キロビット / 秒

KPML Key Press Markup Language

L

LAN Local Area Network; ローカル エリア ネットワーク

LBR Low Bit-Rate; 低ビット レート

LCD Liquid Crystal Display; 液晶ディスプレイ

LCF Location Confirm; ロケーション確認

LCS Live Communications Server

LDAP Lightweight Directory Access Protocol

LDAPS LDAP over SSL

LDIF LDAP Data Interchange Format

LDN Listed Directory Number

LEAP Lightweight Extensible Authentication Protocol

LEC Local Exchange Carrier; 地域通信事業者

LFI Link Fragmentation and Interleaving

LLDP Link Layer Discovery Protocol

LLQ Low-Latency Queuing; 低遅延キューイング

LRJ Location Reject; ロケーション拒否

LRQ Location Request; ロケーション要求

LSC Label Switch Controller; ラベル スイッチ コントローラ

M

MAC Media Access Control; メディア アクセス制御

MAN Metropolitan Area Network; メトロポリタン エリア ネットワーク

Mbps Megabits per second; メガビット / 秒

MCM Multimedia Conference Manager

MCS Media Convergence Server

MCU Multipoint Control Unit; マルチポイント コントロール ユニット

MDN Mobile Data Network; モバイル データ ネットワーク

MFT Multiflex Trunk; マルチフレックス トランク

MGCP Media Gateway Control Protocol; メディア ゲートウェイ コントロール プロトコル

MIB Management Information Base; 管理情報ベース

MIC Manufacturing Installed Certificate; 製造元でインストールされる証明書

MIME Multipurpose Internet Mail Extension

MIPS Millions of Instructions Per Second

MISTP Multiple Instance Spanning Tree Protocol

MITM Man-In-The-Middle; 中間者

MLA Cisco Multi-Level Administration; Cisco マルチレベル管理

MLP Multilink Point-to-Point Protocol; マルチリンク ポイントツーポイント プロトコル

MLPP Multilevel Precedence and Preemption

MLTS Multi-Line Telephone System

MMoIP Multimedia Mail over IP; マルチメディア メール オーバー IP

MOC Microsoft Office Communicator

MoH Music on Hold; 保留音

MOS Mean Opinion Score; 平均オピニオン評点

MPLS Multiprotocol Label Switching

MRG Media Resource Group; メディア リソース グループ

MRGL Media Resource Group List; メディア リソース グループ リスト

ms Millisecond; ミリ秒

MSP Managed Service Provider; 管理対象サービス プロバイダー

MTP Media Termination Point; メディア ターミネーション ポイント

mW milli-Watt; ミリワット

MWI Message Waiting Indicator; メッセージ待機インジケータ

N

NAT Network Address Translation; ネットワーク アドレス変換

NDR Non-Delivery Receipt

NENA National Emergency Number Association

NFAS Non-Facility Associated Signaling

NIC Network Interface Card; ネットワーク インターフェイス カード

NPA Numbering Plan Area; 番号計画エリア

NSE Named Service Event

NSF Network Specific Facilities

NTE Named Telephony Event

NTP Network Time Protocol; ネットワーク タイム プロトコル

O

OSPF Open Shortest Path First

OU Organizational Unit; 組織ユニット

OWA Outlook Web Access

P

PAC Protected Access Credential

PBX Private Branch eXchange; 構内交換機

PC Personal Computer; パーソナル コンピュータ

PCI Peripheral Component Interconnect

PCM Pulse Code Modulation; パルス符号変調

PD Powered Device; 受電装置

PHB Per-Hop Behavior

PIN Personal Identification Number; 個人識別番号

PINX Private Integrated Services Network Exchange

PIX Private Internet Exchange

PLAR Private Line Automatic Ringdown

PoE Power over Ethernet

POTS Plain Old Telephone Service; 一般電話サービス

pps Packets per second; 1 秒あたりのパケット数

PQ Priority Queue; プライオリティ キュー

PRI Primary Rate Interface; 一次群速度インターフェイス

PSAP Public Safety Answering Point

PSE Power Source Equipment

PSK Pre-Shared Key; 事前共有キー

PSTN Public Switched Telephone Network; 公衆電話交換網

PVC Permanent Virtual Circuit; 相手先固定接続

Q

QBE Quick Buffer Encoding

QBSS QoS Basic Service Set

QoS QoS

QSIG Q signaling; Q シグナリング

R

RADIUS Remote Authentication Dial-In User Service

RAS Registration Admission Status

RCP Remote Copy Protocol; リモート コピー プロトコル

RDNIS Redirected Dialed Number Information Service

RF Radio Frequency; 無線周波数

RFC Request for Comments

RIP Routing Information Protocol

RIS Real-Time Information Server

RMTP Reliable Multicast Transport Protocol

RSNA Reservationless Single Number Access; 予約不要シングル ナンバー アクセス

RSP Route/Switch Processor

RSSI Relative Signal Strength Indicator

RSTP Rapid Spanning Tree Protocol

RSVP Resource Reservation Protocol; リソース予約プロトコル

RTCP Real-Time Transport Control Protocol

RTMP Real-Time Messaging Protocol

RTMT Cisco Real-Time Monitoring Tool

RTP Real-Time Transport Protocol

RTT Round-Trip Time; ラウンドトリップ時間

S

S1、S2、S3、および S4 サービス要求の重大度レベル

SCCP Skinny Client Control Protocol

SCSI Small Computer System Interface

SDI System Diagnostic Interface

SDK Software Development Kit; ソフトウェア開発キット

SDL Signaling Description Layer; 信号配信レイヤ

SDP Session Description Protocol

SE Cisco Systems Engineer; シスコのシステム エンジニア

SF Super Frame; スーパー フレーム

SFTP Secure File Transfer Protocol; セキュア ファイル転送プロトコル

SI Standard Image

SIMPLE SIP for Instant Messaging and Presence Leveraging Extensions

SIP Session Initiation Protocol; セッション開始プロトコル

SIW Service Inter-Working; サービス インターワーキング

SLB Server load balancing; サーバ ロード バランシング

SLDAP Secure LDAP

SMA Segmented Meeting Access; セグメント化会議アクセス

SMDI Simplified Message Desk Interface

SMTP Simple Mail Transfer Protocol; 簡易メール転送プロトコル

SNMP Simple Network Management Protocol; 簡易ネットワーク管理プロトコル

SNTP Simple Network Time Protocol; 簡易ネットワーク タイム プロトコル

SOAP Simple Object Access Protocol

SQL Structured Query Language; 構造化照会言語

SRND Solution Reference Network Design; ソリューション リファレンス ネットワーク デザイン

SRST Survivable Remote Site Telephony

SRTP Secure Real-Time Transport Protocol

SRV Server; サーバ

SS7 Signaling System 7

SSID Service Set Identifier

SSL Secure Socket Layer

STP Spanning Tree Protocol; スパニング ツリー プロトコル

SUP1 Cisco Supervisor Engine 1

SUP2 Cisco Supervisor Engine 2

SUP2+ Cisco Supervisor Engine 2+

SUP3 Cisco Supervisor Engine 3

T

TAC Cisco Technical Assistance Center

TAPI Telephony Application Programming Interface

TCD Telephony Call Dispatcher

TCER Total Character Error Rate

TCL Tool Command Language

TCP Transmission Control Protocol; 伝送制御プロトコル

TCS Terminal Capabilities Set; 端末機能セット

TDD Telephone Device for the Deaf

TDM Time-Division Multiplexing; 時分割多重

TEHO Tail-End Hop-Off; テールエンド ホップオフ

TFTP Trivial File Transfer Protocol; トリビアル ファイル転送プロトコル

TKIP Temporal Key Integrity Protocol

TLS Transport Layer Security; トランスポート レイヤ セキュリティ

ToD Time of Day; 時刻

ToS Type of Service; タイプ オブ サービス

TPC Transmit Power Control; 伝送パワー コントロール

TRaP Telephone Record and Playback; 電話での録音および再生

TRP Trusted Relay Point

TSP Telephony Service Provider; テレフォニー サービス プロバイダー

TTL Time To Live; 存続可能時間

TTS Text-to-speech

TTY Terminal Teletype; ターミナル テレタイプ

TUI Telephony User Interface; テレフォニー ユーザ インターフェイス

U

UAC User Agent Client; ユーザ エージェント クライアント

UAS User Agent Server; ユーザ エージェント サーバ

UCCN Unified Client Change Notifier

UDC Universal Data Connector

UDLD UniDirectional Link Detection; 単方向リンク検出

UDP User Datagram Protocol; ユーザ データグラム プロトコル

UDPTL Unnumbered Datagram Protocol Transport Layer

UMTS Universal Mobile Telecommunications System

UN Unsolicited SIP Notify

UNC Universal Naming Convention; 汎用命名規則

UPS Uninterrupted Power Supply; 無停電電源装置

URI Uniform Resource Identifier; ユニフォーム リソース識別子

USB Universal Serial Bus; ユニバーサル シリアル バス

UTIM Cisco Unity Telephony Integration Manager

UTP Unshielded Twisted Pair; シールドなしツイスト ペア

UUIE User-to-User Information Element

V

V3PN Cisco Voice and Video Enabled Virtual Private Network; シスコの音声およびビデオに対応したバーチャル プライベート ネットワーク

VAD Voice Activity Detection; 音声アクティビティ検出

VAF Voice-Adaptive Fragmentation

VATS Voice-Adaptive Traffic Shaping

VIC Voice Interface Card; 音声インターフェイス カード

VLAN Virtual Local Area Network; バーチャル ローカル エリア ネットワーク

VMO ViewMail for Outlook

VoIP Voice over IP

VoPSTN Voice over the PSTN

VoWLAN Voice over Wireless LAN（WLAN）

VPIM Voice Profile for Internet Mail プロトコル

VPN Virtual Private Network; バーチャル プライベート ネットワーク

VRRP Virtual Router Redundancy Protocol; 仮想ルータ冗長プロトコル

VUI Voice User Interface; 音声ユーザ インターフェイス

VWIC Voice/WAN Interface Card; 音声 /WAN インターフェイス カード

W

WAN Wide Area Network; ワイド エリア ネットワーク

WebDAV Web-Based Distributed Authoring and Versioning

WEP Wired Equivalent Privacy

WFQ Weighted Fair Queuing; 重み付け均等化キューイング

WINS Windows Internet Naming Service

WLAN Wireless Local Area Network; ワイヤレス ローカル エリア ネットワーク

WLSM Cisco Wireless LAN Services Module

WMM Wi-Fi Multimedia

WMM TSPEC Wi-Fi Multimedia Traffic Specification

WPA Wi-Fi Protected Access

X

XML Extensible Markup Language

INDEX

記号

数字

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

て

と

な

に

ね

は

ひ

ふ

へ

ほ

ま

む

め

も

や

ゆ

よ

ら

り

る

れ

ろ

わ