Cisco IP テレフォニー 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 CallManager Release 4.0 および 4.1
February 2006

Text Part Number: OL-7447-03-J

CONTENTS

このマニュアルについて

このマニュアルでは、Cisco Architecture for Voice, Video, and Integrated Data（AVVID）に基づいて Cisco IP テレフォニー ソリューションを展開するための、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。

このマニュアルは、旧バージョンの『*Cisco IP Telephony Solution Reference Network Design*（SRND）』で示されている考え方や概念に基づいて作成されています（これらのマニュアルは次の URL で参照できます）。

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

このマニュアルでは、読者が、旧バージョンの『*Cisco IP Telephony SRND*』に記載されている基本用語および概念を十分理解していることを前提としています。これらの用語や概念については、上記 URL の資料を参照してください。

このリリースの新規情報または変更情報

特記のない場合、このマニュアルの情報は、Cisco CallManager Release 4.0 および 4.1 に適用されます。これらのリリース間で違いがある場合は、文章で明確に示しています。

表 1 は、このリリースで新たに追加された機能、または Cisco CallManager の以前のリリースから大幅に変更された機能に関するトピックの一覧を示しています。

表 1　　このマニュアルでの新規情報または旧リリースから変更された情報

トピック	参照
Media Convergence Server（MCS）の機能	表 8-2（P.8-15）
音声ネットワークの保護	音声セキュリティ（P.16-1）
T.38 FAX リレーの機能	表 4-10（P.4-23）

改訂の履歴

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

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

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

次の表では、このマニュアルに対する改訂の履歴をリストしています。

改訂日	備考
2006 年 2 月	音声のセキュリティに関する章が新規に追加され、その他、小規模な修正がいくつか行われました。
2005 年 8 月	Cisco CallManager Release 4.0 および 4.1 の両方に適用されるように修正されました。
2005 年 4 月	Cisco CallManager Release 4.1 を対象にしたこのマニュアルの初版です。

技術情報の入手方法

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

Cisco.com

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

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

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

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

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

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

マニュアルの発注方法（英語版）

英文マニュアルの発注方法については、次の URL にアクセスしてください。

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

シスコ製品の英文マニュアルは、次の方法で発注できます。

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

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

シスコシステムズマニュアルセンター

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

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

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

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

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

テクニカル サポート

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

Cisco Technical Support Web サイト

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

http://www.cisco.com/techsupport

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

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

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

Japan TAC Web サイト

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

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

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

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

サービス リクエストの発行

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

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

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

Cisco TAC の連絡先については、次の URL を参照してください。

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

サービス リクエストのシビラティの定義

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

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

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

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

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

補足資料および情報へのアクセス

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

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

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

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

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

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

  http://www.cisco.com/ipj

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

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

概要

IP が企業ネットワークの汎用の伝送手段になったことは、今や、通信業界や一般の業界アナリストから広く受け入れられ、そのように認められています。データ、音声、および映像アプリケーションの伝送方式としてベンダーが IP を急速に採用し、移行していることが、統合されたネットワーク方式へのこの移行をさらに裏付けています。この移行には、今まで時分割多重（TDM）インフラストラクチャを使用し、従来の方式に決めていたベンダーまでもが含まれています。こうした状況でのメッセージは明らかです。つまり、IP への移行はすでに始まっているのです。

シスコでは、オープン スタンダードに準拠したエンドツーエンド IP ネットワーク ソリューションを提供し、お客様による集中 IP ネットワークへの移行をサポートするために、確立されたアプリケーションのポートフォリオを用意し、コミュニティとしての代理店を配置しています。Cisco IP テレフォニーは、拡大を続けるこのソリューション セットの中核をなしています。このソリューション セットは、Cisco IP コミュニケーションと呼ばれています。

Cisco IP コミュニケーション ソリューションの概要

Cisco IP コミュニケーション ソリューションは、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、完全統合通信を実現します。Cisco IP コミュニケーション ソリューションは、Cisco IP ハードウェアおよびソフトウェア製品によって提供されるフレームワークを利用して、企業環境における現在および発展が予想される今後の通信ニーズに対応する、パフォーマンスと高機能をお届けします。また、このソリューションは、フィーチャ機能を最適化し、設定と保守の要件を減らし、他のさまざまなアプリケーションとの相互運用性を提供するように設計されています。さらに、このソリューションは、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、QoS（Quality Of Service）、およびセキュリティをも適正に維持します。

Cisco IP コミュニケーションには、次のソリューションが含まれます。

- 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 IP テレフォニー ソリューションには、コール処理エージェント、IP Phone、ビデオ デバイス、および特殊な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。

- ユニファイド コミュニケーション

  Cisco ユニファイド コミュニケーション ソリューションは、強力なユニファイド メッセージング（電子メール、音声、および FAX メッセージが 1 つの受信箱から管理される）、および高度ボイス メッセージ（拡張機能を提供するフル機能のボイスメール）を提供して、企業全体で通信を改善し、生産性を高め、顧客サービス機能を向上させます。また、Cisco ユニファイド コミュニケーション ソリューションを使用すると、規則ベースのコール ルーティング、簡易コンタクト管理、および音声認識などの機能を使用して、通信プロセスを合理化することができます。

- リッチメディア会議

  Cisco リッチメディア会議ソリューションは、音声、ビデオ、および Web 会議に対応した IP ベースの統合ツール セットを使用して、仮想的な会議環境を拡張します。

- ビデオ テレフォニー

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

- カスタマー コンタクト

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

- 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 テレフォニー 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。

次の項からは、Cisco IP テレフォニー ソリューションについて説明します。他の Cisco IP コミュニケーション ソリューションについては、次のサイトでオンラインで入手できるドキュメントを参照してください。

http://www.cisco.com

また、これらのソリューションに関するその他の設計ガイドについては、次のサイトを参照してください。

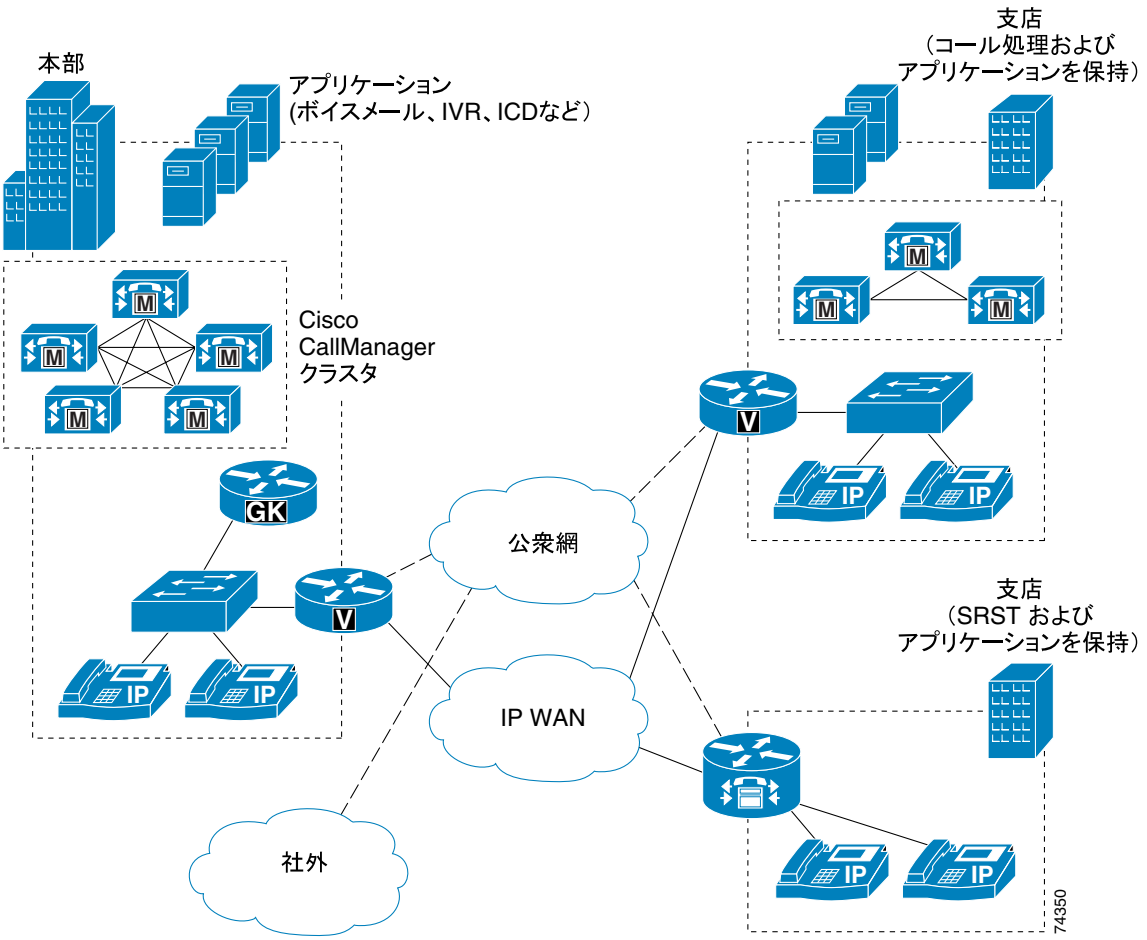
http://www.cisco.com/go/srnd

Cisco IP テレフォニー ソリューションの概要

Cisco IP テレフォニー ソリューションは、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ソリューションです。このソリューションは業界を先導するレベルのものです。Cisco IP ネットワーク インフラストラクチャの柔軟性と高度な機能性が提供するフレームワークにより新しいアプリケーションを迅速に導入することができます。それらは、デスクトップ IP テレフォニー、ユニファイド メッセージング、ビデオ テレフォニー、デスクトップ コラボレーション、エンタープライズ アプリケーションと IP Phone ディスプレイとの統合、コラボレーティブ IP コンタクト センターなどです。これらのアプリケーションにより、生産性が向上し、企業の収益が増大します。

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

図 1-1　一般的な IP テレフォニー ソリューション



Cisco IP テレフォニー ソリューション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

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。

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

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

コール処理エージェント

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

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

- 単一サイト コール処理モデル

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

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

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

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

以降の章で、Cisco IP テレフォニー ネットワークの設計にこれらの配置モデルを適用する方法について説明します。

通信エンドポイント

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

IP テレフォニー エンドポイントには、デスクトップ Cisco 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 IP Phone

  Cisco IP SoftPhone および IP 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 ダイヤルといった利点が追加されています。シスコのソフトウェアベースの IP Phone を使用すると、

ユーザは、インターネット接続が利用可能な場所であればどこでも、ポータブル オフィス IP Phone を使用できるという大きな利点が得られます。

- 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 CallManager Release 4.0 以降と完全に統合されています。また、Cisco VT Advantage では、Microsoft Windows 2000 または Windows XP パーソナル コンピュータにインストール可能な Windows ベースのアプリケーションと USB カメラが導入されています。PC が Cisco IP Phone 7940、7960、または 7970 上の PC ポートに物理的に接続されている場合、ユーザは、ネットワーク上にある別のビデオ デバイスの内線番号をダイヤルするだけで、各自の IP Phone からビデオ コールを発信できます。新しいサードパーティ製ビデオ デバイスの中にも、Cisco IP ビデオ テレフォニー ソリューションとの互換性を持つものがあります。

- 無線 IP Phone

  Cisco 7920 無線 IP Phone は、シスコの IP Phone ファミリを 10/100 イーサネットから 802.11 Wireless LAN（WLAN; 無線 LAN）へと広げます。Cisco 7920 無線 IP Phone には、既存の Cisco 7900 シリーズ IP Phone と同様の機能を持つ複数のライン アピアランスが用意されています。また、Cisco 7920 IP Phone には、802.11b ネットワークの動作に対応した拡張 WLAN セキュリティと QoS も用意されています。さらに、Cisco 7920 IP Phone は、XML ベースのデータ アクセスおよびサービスをサポートします。

アプリケーション

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

- エクステンション モビリティ

  Cisco CallManager のエクステンション モビリティ機能を使用すると、Cisco CallManager クラスタ内のユーザは、任意の Cisco IP Phone 7970、7960、または 7940 にログインすることによって、その IP Phone を一時的に自分の電話機として設定できます。ユーザがログインすると、IP Phone は、そのユーザの電話番号、短縮ダイヤル、サービス リンクなどのユーザ固有のプロパティを受け入れます。ログアウト後、IP Phone は元のユーザ プロファイルに戻ります。Cisco CallManager エクステンション モビリティを使用すると、数人の社員が、特定のオフィスを持つのではなく、交替でオフィス スペースを共有できます。

- Cisco MeetingPlace

  Cisco MeetingPlace は、音声、ビデオ、および Web 会議機能を統合した、完全なリッチメディア会議ソリューションです。これを使用すると、リモート会議が、対面式の会議と同じくらい自然で効果的なものになります。会議の主催者は、1 つのステップで、MeetingPlace Web インターフェイス、IP Phone、または Microsoft Outlook や Lotus Notes のカレンダーのいずれかを使用して、音声、ビデオ、および Web のリソースをスケジュール設定することができます。会議の招待者は、電子メールまたはカレンダーの招待状によって通知を自動的に受信し、シングルクリックでリッチメディア会議に参加することができます。職場で広く受け入れられているインスタント メッセージング アプリケーションを Cisco MeetingPlace と併用すると、ユーザは、America Online（AOL）Messenger、Lotus Sametime、MSN Messenger、および Yahoo Messenger などの一般的なインスタント メッセージング クライアントからリッチメディア会議を簡単に開催できます。

- ユニファイド メッセージング

  Cisco Unity は、強力なユニファイド メッセージング（電子メール、音声、および FAX メッセージが 1 つの受信箱に送信される）、および高度ボイス メッセージ（拡張機能を提供するフル機能のボイスメール）を提供して、企業全体で通信を改善し、生産性を高め、顧客サービス機能を向上させます。Cisco Unity ユニファイド メッセージングを使用すると、電話機を使って電子メールを音声で聞いたり、インターネット経由でボイス メッセージを確認したり、（サポートされているサード パーティ製 FAX サーバと統合する場合）FAX を任意の場所に送信することができます。

- Cisco IP Phone 用の Web サービス

  Cisco IP Phone（たとえば、Cisco IP Phone 7960 または 7940）を使用すると、キーパッドやディスプレイを介してユーザが対話できる、カスタマイズされたクライアント サービスを展開できます。eXtensible Markup Language（XML）Application Programming Interface（API; アプリケーション プログラミング インターフェイス）を使用すると、Cisco IP Phone サービス用のアプリケーションを作成できます。また、Microsoft IIS などの標準的な Web サービスから HTTP プロトコルを使用すると、そのアプリケーションを展開できます。Cisco IP Phone を通じて提供される一般的なサービスには、完全な会議インターフェイス、PC が使用不能の場合でもデータ レコードを管理できる機能、および社員の呼び出し、時刻、株式市場の情報、カスタマー コンタクト情報、日課表などを表示する機能があります。

- Cisco IP Contact Center（IPCC）Express

  Cisco IPCC Express は、強固に統合されたコンタクト センター ソリューションで、IVR（interactive voice response; 音声自動応答装置）、Automatic Call Distribution（ACD; 自動着信呼分配）、および 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）の 3 つの主要機能を備えています。IVR 機能では、IVR ポートを使用して、DTMF または音声入力を介して発信者と対話することができます。ACD 機能では、エージェントへのコールを、インテリジェントにルーティングおよびキューイングできます。CTI 機能では、コール データをエージェントのデスクトップ上に「ポップアップ表示」できます。IPCC Express ソフトウェアは、認定された Cisco MCS、Hewlett-Packard、または IBM サーバ上で動作します。動作時は、Cisco CallManager との対話が必要になります。

- Cisco IP Contact Center（IPCC）Enterprise Edition

  Cisco IPCC Enterprise Edition を使用すると、コンタクト センター エージェントは、企業内のどこからでも、インテリジェント コール ルーティング、ネットワーク デスクトップ間の CTI、およびマルチチャネル コンタクト管理を行うことができます。IPCC ソフトウェアは、ダイヤル番号と発呼回線 ID、発信者が入力した数字、Web フォームから送信されたデータ、およびカスタマー プロファイル データベースの検索から得られる情報など、コンタクト関連のデータを使用して、お客様それぞれのプロファイルを作成します。同時に、システムは、エージェントのスキルと可用性、IVR ステータス、キューの長さなど、コンタクト センターでお客様のニーズを満たすために使用できるリソースをモニタリングします。お客様のデータとコンタクト センターのデータはまとめて、企業のビジネス ルールを写実的に反映するユーザ定義のルーティング スクリプトによって処理されます。その結果、Cisco IPCC は、企業内のどこからでも、各コンタクトを最適なリソースにルーティングできます。

セキュリティ

Cisco IP テレフォニー ソリューションは、次のような主要な領域のセキュリティに対して焦点を当てます。

- 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 CallManager、エンドポイント デバイス、およびさまざまなディレクトリやデータベース用のセキュリティ対策
- さまざまなユーザ クラスの発信権限を定義するためのメカニズム
- セキュリティを向上させるための慎重なネットワーク設計と管理

ネットワーク管理ツール

Cisco IP ネットワーク インフラストラクチャには、IP テレフォニー ソリューションをサポートするネットワーク管理ツール、QoS ツール、およびセキュリティ管理ツールが多数備わっています。Cisco CallManager には、IP ネットワークの堅牢性と柔軟性を利用する拡張ソフトウェアと設定管理ツールが備わっています。Cisco CallManager ユーザ インターフェイスは、従来型のテレフォニー管理システムを基盤とし、ソフトウェアと Web ベース アプリケーションを追加することにより、最も一般的なサブスクライバとテレフォニーの設定タスクを単純化します。

また、CiscoWorks2000 には、IP テレフォニー ネットワークの操作、アドミニストレーション、および保守を管理する多数のネットワーク管理ツールが組み込まれています。特に、CiscoWorks IP Telephony Environment Monitor（ITEM）に用意されているアプリケーションおよびツールのスイートを使用すると、Cisco Architecture for Voice, Video, and Integrated Data（AVVID）や Cisco IOS ソフトウェアに基づいて、小規模と大規模の両方の IP テレフォニー導入を容易かつ効果的に管理できます。CiscoWorks ITEM には、次の主要機能があります。

- 問題に焦点を当てた障害分析：IP テレフォニー環境の健全性に関する情報をタイムリーに提供します。
- 信頼性テストとモニタリング：統合テストを使用して、通常の日常業務をエミュレートし、IP インフラストラクチャと Cisco IP テレフォニー配置に関する運用上の即用性を検証します。
- 既存の管理インフラストラクチャとのインテリジェントな統合：インテリジェントなトラップを生成します。このトラップは、ネットワークにインストールされている他のイベント管理システムへの転送、電子メールやポケットベル ゲートウェイへの送信、または Alerts and Activities Display（AAD）への表示を行うことができます。
- 評価機能と相関機能：モニタリング対象のネットワーク環境における IP テレフォニー環境の一般的な健全性を評価します。
- Alerts and Activities Display（AAD）：革新的な Web ベースの操作画面を提供し、基本 IP ネットワークおよび Cisco IP テレフォニー実装における実際の問題や疑わしい問題に関する状態や警告をリアルタイムで表示します。
- ITEM マルチビュー：大企業のお客様や管理対象サービス プロバイダーが、特定のユーザ コミュニティを分割し、そのすべてのコミュニティを単一の ITEM 実装から管理することができます。

CHAPTER 2

IP テレフォニー配置モデル

各 Cisco IP テレフォニー ソリューションは、次に説明する主要配置モデルに基づいて実現されています。

- 単一サイト（P.2-2）

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

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

- 集中型コール処理を使用するマルチサイト WAN（P.2-5）

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

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

- 分散型コール処理を使用するマルチサイト WAN（P.2-13）

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

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

- IP WAN を介したクラスタ化（P.2-17）

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

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

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

また、P.2-27 の「U. S. Section 508 準拠についての設計上の考慮事項」の項では、IP テレフォニー ネットワークを設計するときに、身体に障害のあるユーザに対して U.S. Section 508 に従ってアクセシビリティ機能を組み込む場合のガイドラインを示します。

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

単一サイト

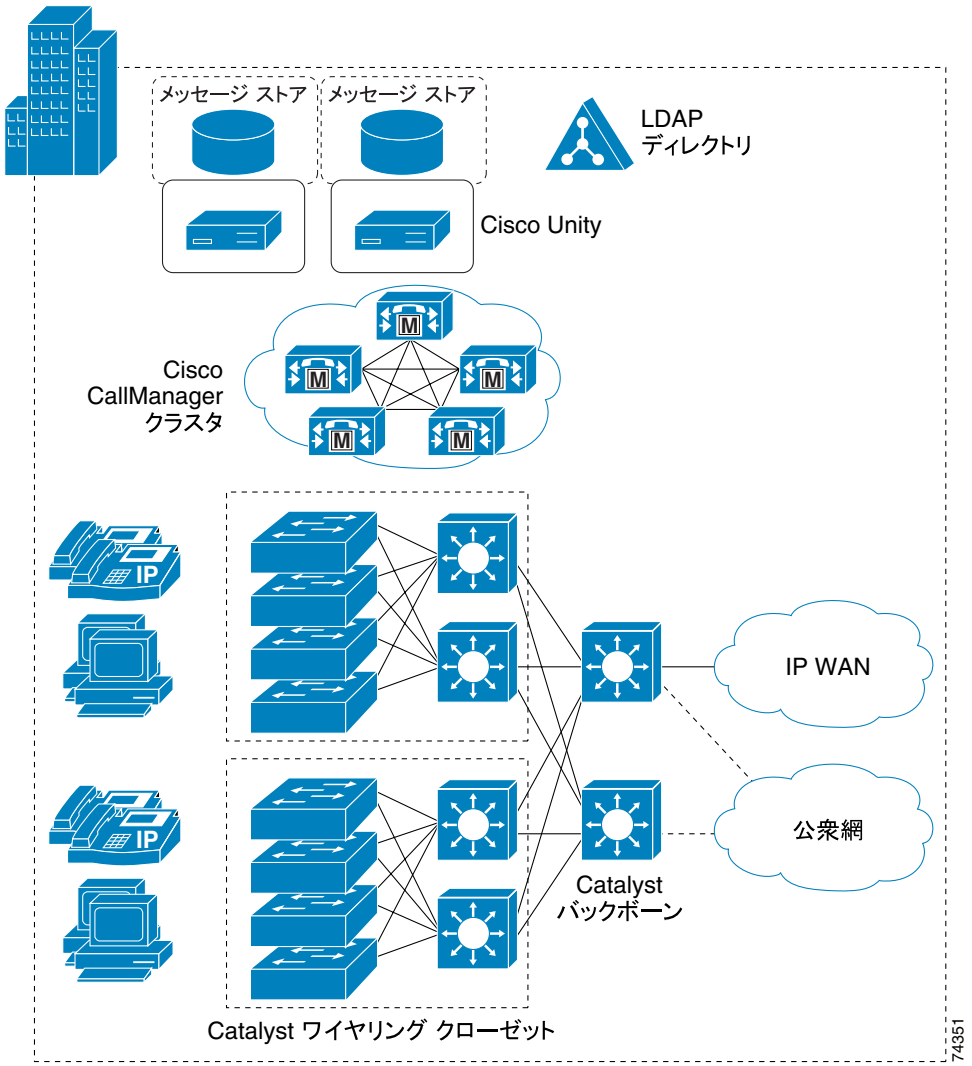
単一サイトで IP テレフォニーを実現する場合のモデルは、その単一サイト（キャンパス）に配置される 1 つのコール処理エージェントから構成されています。テレフォニー サービスは、IP WAN を使用して行われることは*ありません*。企業は、一般的に、LAN または MAN に対しては単一サイト モデルを配置して、サイト内の音声トラフィックを伝送しています。このモデルでは、コールが LAN または MAN を越えて発信される場合は、PSTN（公衆電話交換網）が使用されます。

単一サイト モデルの設計上の特長は、次のとおりです。

- 単一の Cisco CallManager または Cisco CallManager クラスタ
- クラスタごとに最大 30,000 台の IP Phone
- 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
- ボイスメールとユニファイド メッセージング コンポーネント
- すべての IP Phone コールに対して G.711 コーデックのみで対応（コールごとに 80 Kbps の IP 帯域幅、圧縮なし）
- 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

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

図 2-1　単一サイト モデル



単一サイト モデルの利点

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

要約すると、単一サイト モデルの主な利点は次のとおりです。

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

単一サイト モデルのベスト プラクティス

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

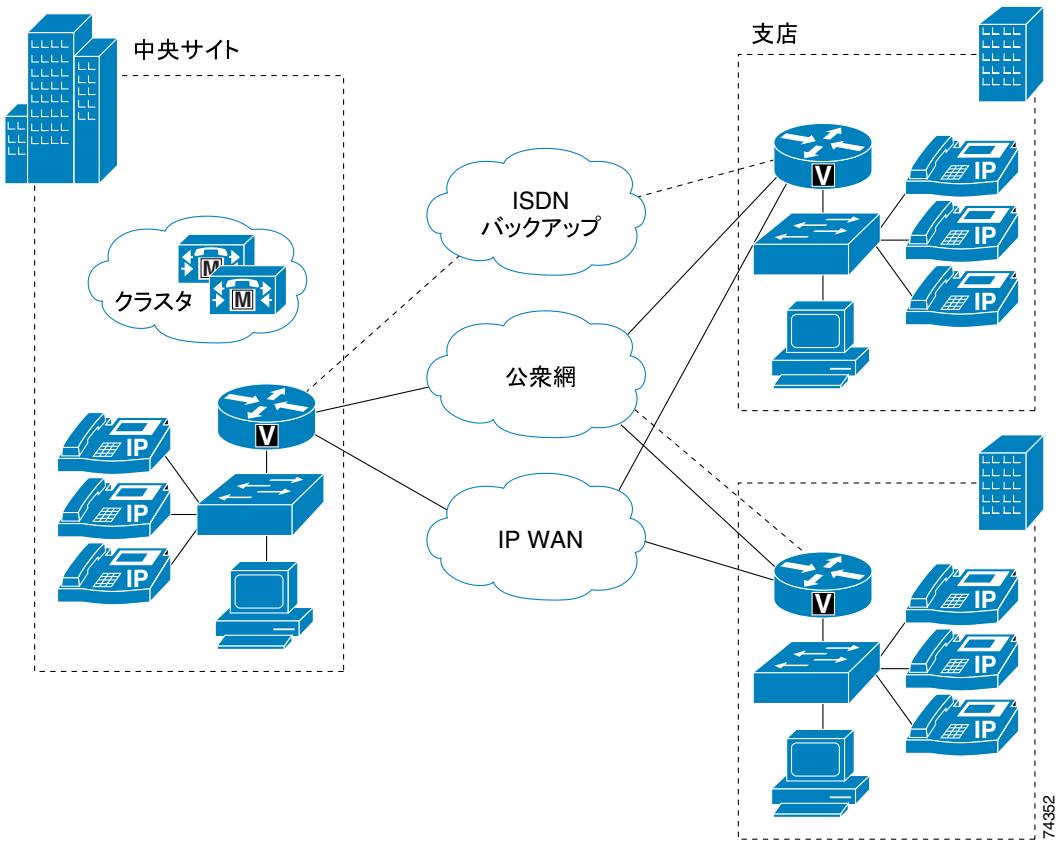
- 一般的なインフラストラクチャ 構想に基づいて可用性および耐障害性を高めます。IP テレフォニーへの迅速な移行、アプリケーションにビデオ ストリーミングやビデオ会議などを容易に統合、および IP テレフォニー配置を拡張し、WAN または複数の Cisco CallManager クラスタへのアクセスを可能にするには、インフラストラクチャを適切に構築する必要があります。
- 自社内のコール パターンを知っておく必要があります。単一サイト モデルは、大部分のコールが社内の同一サイトから発信されている場合、または社外の公衆網ユーザ宛てに発信されている場合に適用します。
- すべてのエンドポイントに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

集中型コール処理を使用するマルチサイト WAN

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

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

図 2-2　集中型コール処理配置モデル



IP WAN の接続オプションは、次のとおりです。

- 専用回線
- フレーム リレー
- 非同期転送モード（ATM）
- ATM とフレーム リレーのサービス インターワーキング（SIW）

- Multiprotocol Label Switching（MPLS）バーチャル プライベート ネットワーク（VPN）
- 音声およびビデオ対応 IP Security Protocol VPN（IPSec VPN（V3PN））

WAN エッジに置かれているルータには、プライオリティ キューイングやトラフィック シェーピングなどの QoS メカニズムが装備されていて、WAN の帯域幅が恒常的に不足している場合に、データ トラフィックから音声トラフィックを保護しています。さらに、コール アドミッション制御方式も導入されていて、音声トラフィックによる WAN リンクのオーバーサブスクリプションを防いだり、確立済みのコール品質が低下するのを防いだりしています。集中型コール処理配置の場合、Cisco CallManager 内にコール アドミッション制御を行う *ロケーション*が構築されます（ロケーションの詳細については、P.9-3 の「Cisco CallManager ロケーション」の項を参照してください）。

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

集中型コール処理モデルのベスト プラクティス

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

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

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

リモート サイトのサバイバビリティ（存続可能性）

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

表 2-1　リモート サイトの高可用性を提供する方法

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

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

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

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

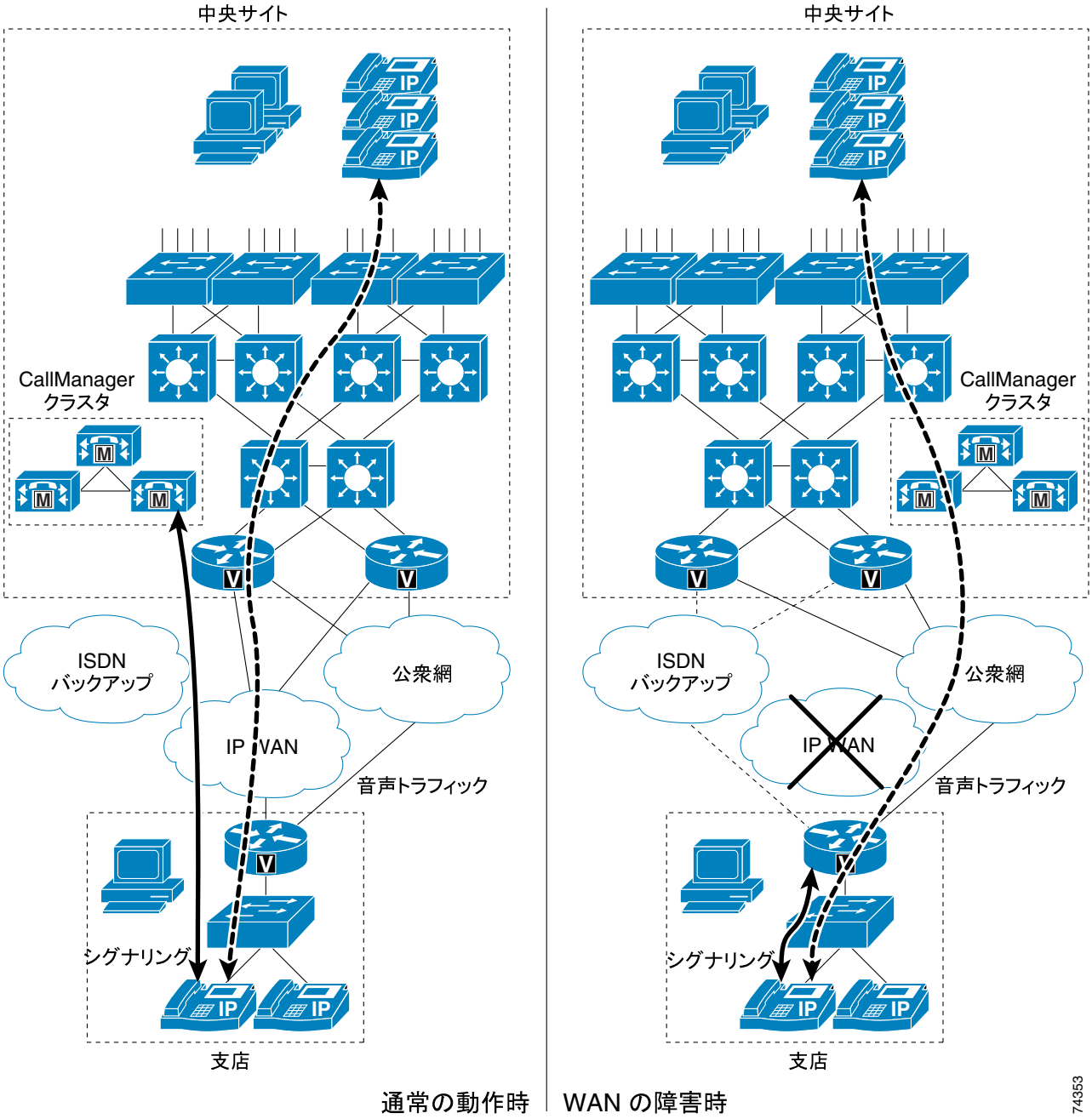


図 2-3 の左側に表示されている通常の動作では、支店は、データ トラフィック、音声トラフィック、およびコール シグナリングを伝送する IP WAN を経由して、中央サイトに接続されます。支店の IP Phone は、中央サイトの Cisco CallManager クラスタとコール信号情報を交換し、IP WAN を介してコールを発信します。支店のルータまたはゲートウェイは、両方のタイプのトラフィック（コール信号と音声）を透過的に転送し、IP Phone を認識しません。

支店との WAN リンクに障害が起きた場合、またはその他のなんらかのイベントにより、Cisco CallManager クラスタとの接続が失われた場合、支店の IP Phone は支店のルータに再登録されます。支店のルータは、設定について IP Phone に照会し、この情報を使用して独自の設定を自動的

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

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

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

- データのみの ISDN バックアップ

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

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

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

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

VoPSTN は、次のいずれかの方法で実装できます。

- Automated Alternate Routing（AAR; 自動代替ルーティング）機能を使用する（AAR の詳細については、P.10-20 の「Automated Alternate Routing」の項を参照してください）。
- Cisco CallManager と公衆網ゲートウェイの両方のダイヤル プラン構成要素を組み合せて使用する。

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

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

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

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

  これらの場合は、転送先として公衆網番号を入力するようユーザに要求することをお勧めします。

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

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

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

VoPSTN の AAR 実装方法には、次の利点があります。

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

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

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

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

ダイヤル プランを使用する VoPSTN

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

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

VoPSTN のダイヤル プラン実装方法には、次の利点があります。

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

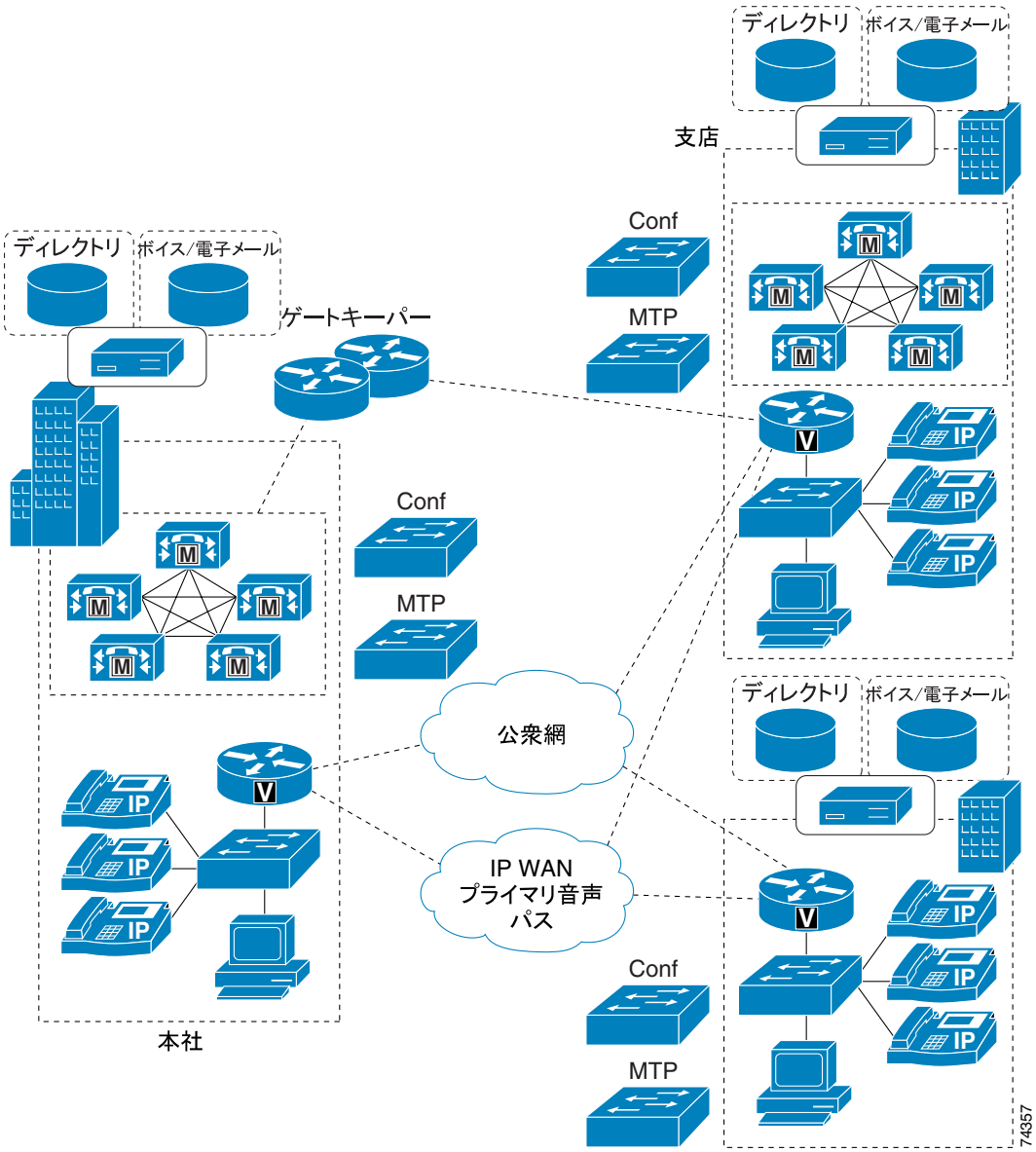
ダイヤル プラン実装方法には、VoPSTN について示した一般的な考慮事項のほかに、次の設計ガイドラインが適用されます。

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

分散型コール処理を使用するマルチサイト WAN

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

図 2-4　分散型コール処理の配置



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 CallManager
  - Cisco CallManager Express
  - その他の IP PBX

- 集中型コール処理サイトと、それに関連したすべてのリモート サイト。
- Voice over IP（VoIP）ゲートウェイを備えたレガシー PBX。

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

IP WAN の接続オプションは、次のとおりです。

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

分散型コール処理モデルの利点

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

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

分散型コール処理モデルのベスト プラクティス

分散型コール処理を使用するマルチサイト WAN 配置には、単一サイト、または集中型コール処理を使用するマルチサイト WAN 配置と同じ要件が少なからずあります。分散型コール処理モデルについては、ここでリストされているベスト プラクティスに加えて、他のモデルのベスト プラクティスにも従ってください（P.2-2 の「単一サイト」および P.2-5 の「集中型コール処理を使用するマルチサイト WAN」を参照）。

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

ゲートキーパーの使用には、次のベスト プラクティスが適用できます。

- Cisco IOS ゲートキーパーを使用して、各サイトとのコール アドミッションを制御します。
- ゲートキーパーの有効性を高めるには、HSRP（ホットスタンバイ ルータ プロトコル）ゲートキーパー ペア、ゲートキーパーのクラスタ化、および代替ゲートキーパー サポートを使用します。さらに、ネットワーク内の冗長性を確実にするために複数のゲートキーパーを使用します。
- プラットフォームの規模を適切に調整して、パフォーマンスとキャパシティの要件が満たされることを確認します。

- WAN 上のコーデックは 1 つのタイプに限定して使用します。これは、H.323 仕様では、レイヤ 2、IP、UDP（User Data Protocol）、または RTP（Real-time Transport Protocol）ヘッダーのオーバーヘッドが、帯域幅要求で許可されないからです（ヘッダーのオーバーヘッドは、パケットのペイロードまたは符号化された音声部分のみで許可されます）。WAN 上で使用するコーデックを 1 つのタイプに限定すると、最悪のシナリオに備えて IP WAN を過剰にプロビジョニングする必要がなくなるので、キャパシティ プランニングが簡単になります。
- ゲートキーパー ネットワークは、数百単位のサイトにスケーラブルです。また、設計上の制限は WAN トポロジからしか受けません。

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

- ゲートキーパーのコール アドミッション制御については、P.9-1 の「コール アドミッション制御」を参照してください。
- ゲートキーパーのスケーラビリティと冗長性については、P.8-1 の「コール処理」を参照してください。
- ゲートキーパーのダイヤル プラン解決については、P.10-1 の「ダイヤル プラン」を参照してください。

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

SIP プロキシの使用には、次のベスト プラクティスが適用できます。

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

分散型コール処理モデルのコール処理エージェント

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

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

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

表 2-2 は、推奨されるコール処理エージェントを示しています。

表 2-2　推奨されるコール処理エージェント

コール処理エージェント	推奨規模	備考
Cisco CallManager Express（CME）	最大 120 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 CallManager	50 ～ 30,000 台の電話機	• Cisco CallManager クラスタの規模に応じて、小規模から大規模までのサイト • 集中型または分散型コール処理をサポートする
VoIP ゲートウェイを備えた従来の PBX	PBX に依存する	• IP WAN コール数と機能は、PBX と VoIP ゲートウェイを接続するプロトコルおよびゲートウェイ プラットフォームによって異なる

IP WAN を介したクラスタ化

QoS 機能に対応している IP WAN によって相互接続される複数サイト間で、単一の Cisco CallManager クラスタを配置できます。ここでは、WAN を介したクラスタ化の概要を簡潔に説明します。詳細については、第 8 章「コール処理」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.2-22）

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

- リモート フェールオーバー配置モデル（P.2-25）

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

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

WAN を介したクラスタ化の主な利点は、次のとおりです。

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

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

WAN の考慮事項

WAN を介したクラスタ化が成功するには、WAN 自体のさまざまな特性を慎重に計画し、設計し、実装する必要があります。Cisco CallManager サーバ間の Intra-Cluster Communication Signaling（ICCS）は、複数のトラフィック タイプから構成されます。ICCS のトラフィック タイプは、優先またはベストエフォートのどちらかとして分類されます。優先 ICCS トラフィックには、IP Precedence 3（DSCP 26 または PHB AF31）が付けられます。ベストエフォート型 ICCS トラフィックには、IP Precedence 0（DSCP 0 または PHB BE）が付けられます。さまざまなタイプの ICCS トラフィックについては、P.2-18 の「クラスタ内通信」で説明されています。この項では、プロビジョニングについてのさらに詳しいガイドラインも記述されています。WAN の特性には、次の設計上のガイドラインが適用されます。

- 遅延

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

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

- ジッタ

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

- パケット損失とエラー

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

- 帯域幅

  予想されるコール ボリューム、デバイスのタイプ、およびデバイス数に対して、各サーバ間で適切な量の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 SQL データベースからのデータベース トラフィック。SQL データベースは、ベストエフォートを使用して、パブリッシャ サーバから、クラスタ内の他のすべてのサーバに複製されます。SQL 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、SQL 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。
- Lightweight Directory Access Protocol（LDAP）ディレクトリからのディレクトリ トラフィック。このトラフィックは、ユーザとアプリケーションを認証し、特定のユーザまたはアプリケーションの追加設定情報を提供します。デフォルトで、LDAP トラフィックはベストエフォートで送信されます。
- ICCS リアルタイム トラフィック。このトラフィックは、シグナリング、コール アドミッション制御、および開始と終了時のコールについてのその他の情報から構成されます。ICCS は、Cisco CallManager Service が使用可能になっているすべてのサーバ間で、伝送制御プロトコル（TCP）接続を使用します。この接続は、これらのサーバ間でフルメッシュです。クラスタには、

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

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

サブスクライバ サーバ間のフェールオーバー

Cisco CallManager Release 3.1 および 3.2 では、フェールオーバーの動作は、パブリッシャの到達可能性、およびサブスクライバとパブリッシャ間の遅延によって異なります。パブリッシャが通信可能である場合、サブスクライバは、デバイスの登録時に、関連したデバイス設定レコードをパブリッシャに直接要求します。ラウンドトリップ遅延、および SQL データベース トラフィックに使用可能な帯域幅は、登録の速度に影響を与えます。この結果、リモート ロケーションのデバイスから、パブリッシャへのフェールオーバーには、約 20 分の遅延が発生する場合があります。その後、フル サーバ上のすべてのデバイスは、フェールオーバー プロセスを完了します。フェールオーバー時にパブリッシャが通信不能である場合、サブスクライバは、データベースの最新のコピーを設定情報に使用します。サブスクライバが自身のデータベースにアクセスするには遅延は生じないので、この場合のフェールオーバー時間は、フル サーバの場合、約 5 分です。

Cisco CallManager Release 3.3 以降では、フェールオーバー時のパブリッシャに対する遅延の影響は最小限に抑えられます。これは、初期化時またはブートアップ時に、設定情報がキャッシュされるためです。その結果、Cisco CallManager の最初の起動時間が長くなることはありますが、それ以降は、パブリッシャ データベースへのアクセス時の遅延によってフェールオーバーとフェールバックが影響を受けることはありません。

Cisco CallManager パブリッシャ

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

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

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

- 設定の追加、変更、および削除
- エクステンション モビリティ
- ユーザ短縮ダイヤル
- データベースを必要とする Cisco CallManager User ページのオプション

- Cisco CallManager ソフトウェアのアップグレード
- 全転送の変更
- メッセージ待機インジケータ（MWI）の状態

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

コール詳細レコード（CDR）

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

遅延のテスト

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

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

```
Access_SW#ping
Protocol [ip]:
Target IP address: 10.10.10.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:y
Source address or interface:
Type of service [0]: 3
Set DF bit in IP header?[no]:
Validate reply data?[no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte 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。Cisco CallManager はランダム エラーに対する許容性がありますが、クラスタのパフォーマンス低下を避けるために、エラーを回避する必要があります。

トラブルシューティング

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

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

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

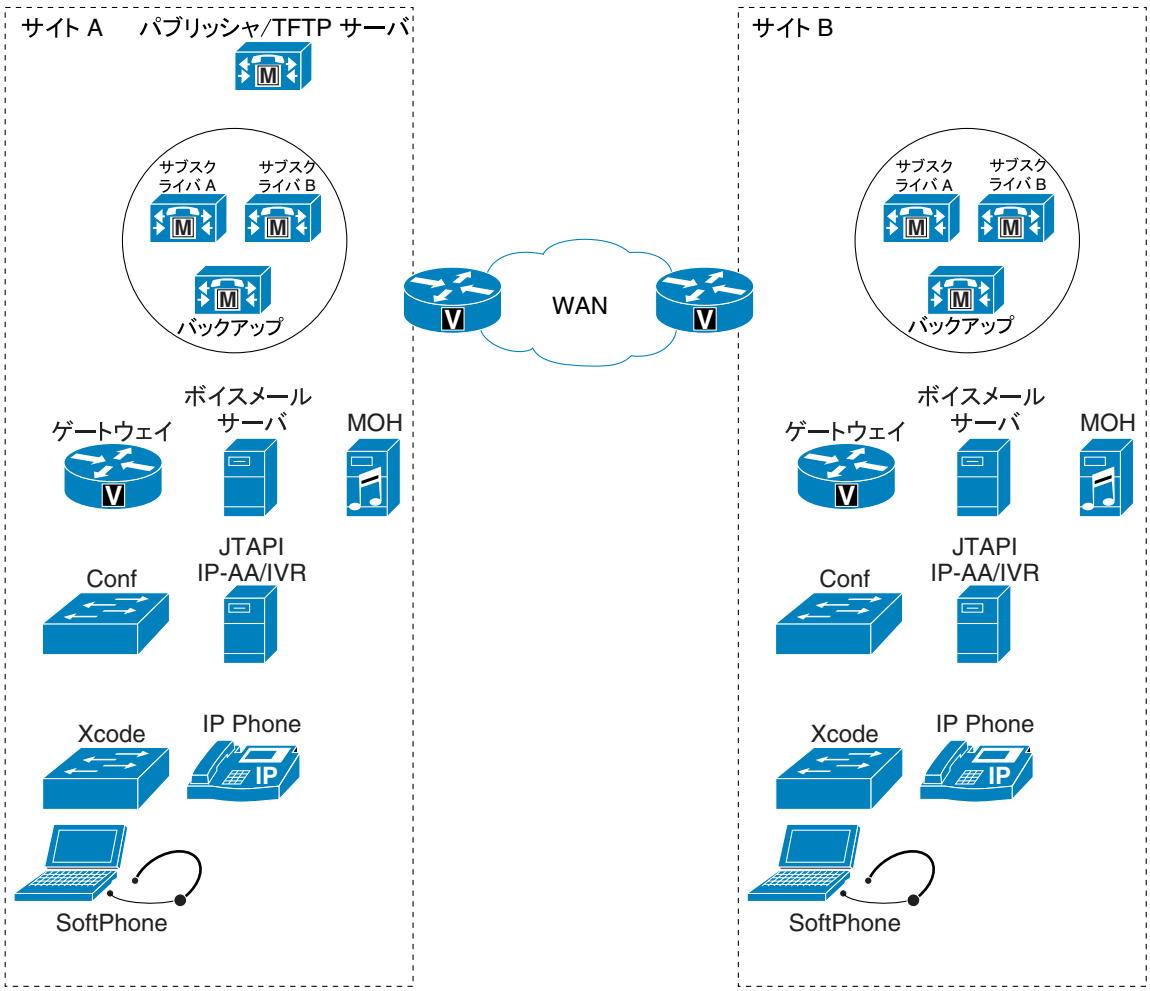
要約すると、ICCS 通信の問題のトラブルシューティングを行うには、次のタスクを実行します。

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

ローカル フェールオーバー配置モデル

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

図 2-5　ローカル フェールオーバー モデルの例



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

- 少なくとも 1 つのプライマリ Cisco CallManager サブスクライバと 1 つのバックアップ サブスクライバを含むように、各サイトを設定します。
- Cisco CallManager の *グループ*と *デバイス プール*を設定して、サイト内のデバイスが、あらゆる状況でそのサイトのサーバだけに登録されるようにします。
- 各サイトで主要なサービス（TFTP、DNS、DHCP、LDAP、および IP Phone サービス）、すべてのメディア リソース（コンファレンス ブリッジと Music On Hold）、およびゲートウェイを複製します。複製を確実に行い、最大レベルの復元性を得るよう、シスコは強くお勧めします。また、この方法を拡張して、各サイトにボイスメール システムを組み込むこともできます。

- WAN 障害が発生した場合、パブリッシャ データベースへのアクセスがないサイトでは、次に示すように、いくつかの機能を使用できないことがあります。
  - ローカル サイトのシステム管理者は、設定を一切追加、変更、または削除することができません。
  - エクステンション モビリティ ユーザは、IP Phone のログインまたはログアウトを行うことができません。
  - 全コール転送を変更することはできません。
- WAN 障害が発生した状態では、コールを発信するサブスクライバと現在通信していない電話番号にコールを発信すると、ファースト ビジー音が聞こえるか、またはコール転送されます（転送先の電話番号のロケーションによっては、ボイスメールに転送される可能性があります）。このような場合、ユーザは公衆網を介してその番号を手動でダイヤルする必要があります。
- WAN を介してクラスタ化されているサイト間で 10,000 BHCA（Busy Hour Call Attempt）が発生するたびに、Intra-Cluster Communication Signaling（ICCS）に 900 Kbps の帯域幅が必要です。これは、帯域幅の最小必要量であり、帯域幅は、900 kbps の倍数で割り当てられます。ICCS のトラフィック タイプは、優先またはベストエフォートのどちらかとして分類されます。優先 ICCS トラフィックには、IP Precedence 3（DSCP 26 または PHB AF31）が付けられます。ベストエフォート型 ICCS トラフィックには、IP Precedence 0（DSCP 0 または PHB BE）が付けられます。
- WAN を介してクラスタ化されているサイト間の推奨される最小帯域幅は、1.544 Mbps です。この量にすると、ICCS 用に最小 900 Kbps が確保され、SQL、LDAP、および他のサーバ間トラフィック用に最小 644 Kbps が確保されます。
- Cisco CallManager クラスタ内の任意の 2 つのサーバ間では、最大ラウンドトリップ時間（RTT）として 40 ms が可能です。この時間は、単方向で最大 20 ms の遅延、または理想的な条件下での約 1860 マイル（3000 km）の伝送距離に相当します。
- ローカル フェールオーバー モデルには、Cisco CallManager Release 3.1 またはそれ以降が必要です。
- 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 <None> として設定する必要があるためです。この設定が行われても、コール アドミッション制御に使用するハブアンドスポーク トポロジは保持されます。
  - Multiprotocol Label Switching（MPLS）バーチャル プライベート ネットワーク（VPN）機能を使用している場合は、Cisco CallManager ロケーションとリモート サイトにあるすべてのサイトが、メイン サイトのいずれかに登録される場合があります。
  - メイン サイト間の帯域幅が制限されている場合は、サイト間でコール アドミッション制御を使用し、ロケーションが <None> として設定されているメイン サイトにすべてのリモート サイトを登録する必要があります。このメイン サイトはハブ サイトと見なされ、それ以外のリモート サイトと、WAN を介してクラスタ化されたサイトはすべて、スポーク サイトとなります。
- ソフトウェア アップグレード時は、ソフトウェア リリース ノートで説明されている標準のアップグレード手順を使用して、クラスタ内のすべてのサーバを同じ保守期間内にアップグレードする必要があります。

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

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

冗長性とアップグレード時間を改善するために、各ロケーションの少なくとも 1 つの Cisco CallManager サーバで、Cisco TFTP サービスを使用可能にすることをお勧めします。サイトやサーバの利用可能なキャパシティに応じて、パブリッシャ サーバまたはサブスクライバ サーバのどちらかで、TFTP サービスを実行できます。TFTP サーバ オプションは、サイトごとに DHCP サーバ上で正しく設定する必要があります。DHCP を使用していないか、TFTP サーバが手動で設定される場合、ユーザが、サイトの正しいアドレスを設定する必要があります。パブリッシャから離れた TFTP サーバでは、クラスタのアップグレード時や Cisco TFTP サービスの再起動時に、すべての設定ファイルをアップグレードおよび再構築するためにより多くの時間がかかります。この時間は、TFTP サーバとパブリッシャ間の遅延や、データベースに設定されているデバイスの数によって異なります。

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

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

ローカル フェールオーバー用のゲートウェイ

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

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

ローカル フェールオーバー用のボイスメール

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

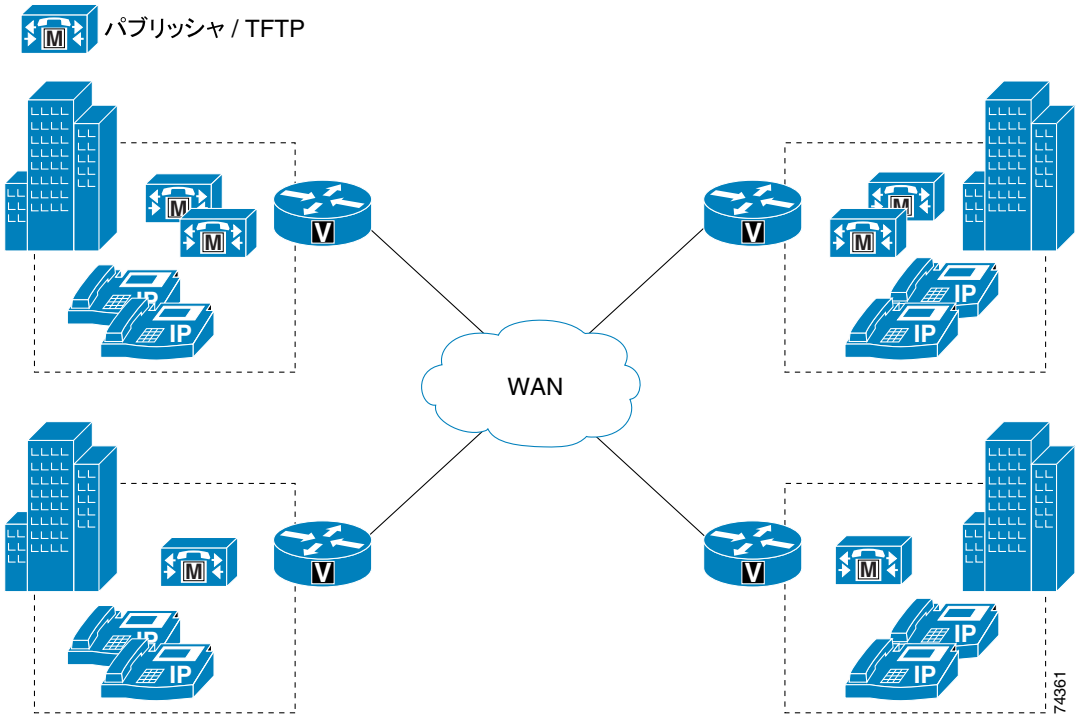
ローカル フェールオーバーに対する Music On Hold とメディア リソース

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

リモート フェールオーバー配置モデル

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

図 2-6　4 サイト構成のリモート フェールオーバー モデル



リモート フェールオーバー モデルを実装する場合は、ローカル フェールオーバー モデルのガイドライン（P.2-22 の「ローカル フェールオーバー配置モデル」を参照）と、次の変更点に従ってください。

- 少なくとも 1 つのプライマリ Cisco CallManager サブスクライバと、必要に応じてオプションのバックアップ サブスクライバを含むように、各サイトを設定します。
- Cisco CallManager の *グループ*と *デバイス プール*を設定して、WAN を介してサーバにデバイスを登録できるようにします。
- デバイスが、WAN を介して同じクラスタ内のリモート Cisco CallManager サーバに登録される場合、シグナリング トラフィックまたはコール制御トラフィックには帯域幅を追加する必要があります。この帯域幅は、ICCS トラフィックより大きくなる場合があります。また、シグナリングに関する帯域幅のプロビジョニング計算を使用して計算する必要があります（P.3-31 の「帯域幅のプロビジョニング」を参照）。

U. S. Section 508 準拠についての設計上の考慮事項

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

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

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

    RJ-11 アナログ回線用 TTY/TDD を直接 Cisco FXS ポートに接続します。FXS ポートはすべて動作します。たとえば、Cisco IP Phone 7900 シリーズ、Cisco VG248、Catalyst 6000、Cisco ATA 188 モジュール、または FXS ポートを備えている他の Cisco 音声ゲートウェイ上で動作します。シスコは、この接続方式をお勧めします。
  - アコースティック カップル

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

CHAPTER 3

ネットワーク インフラストラクチャ

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

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

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

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

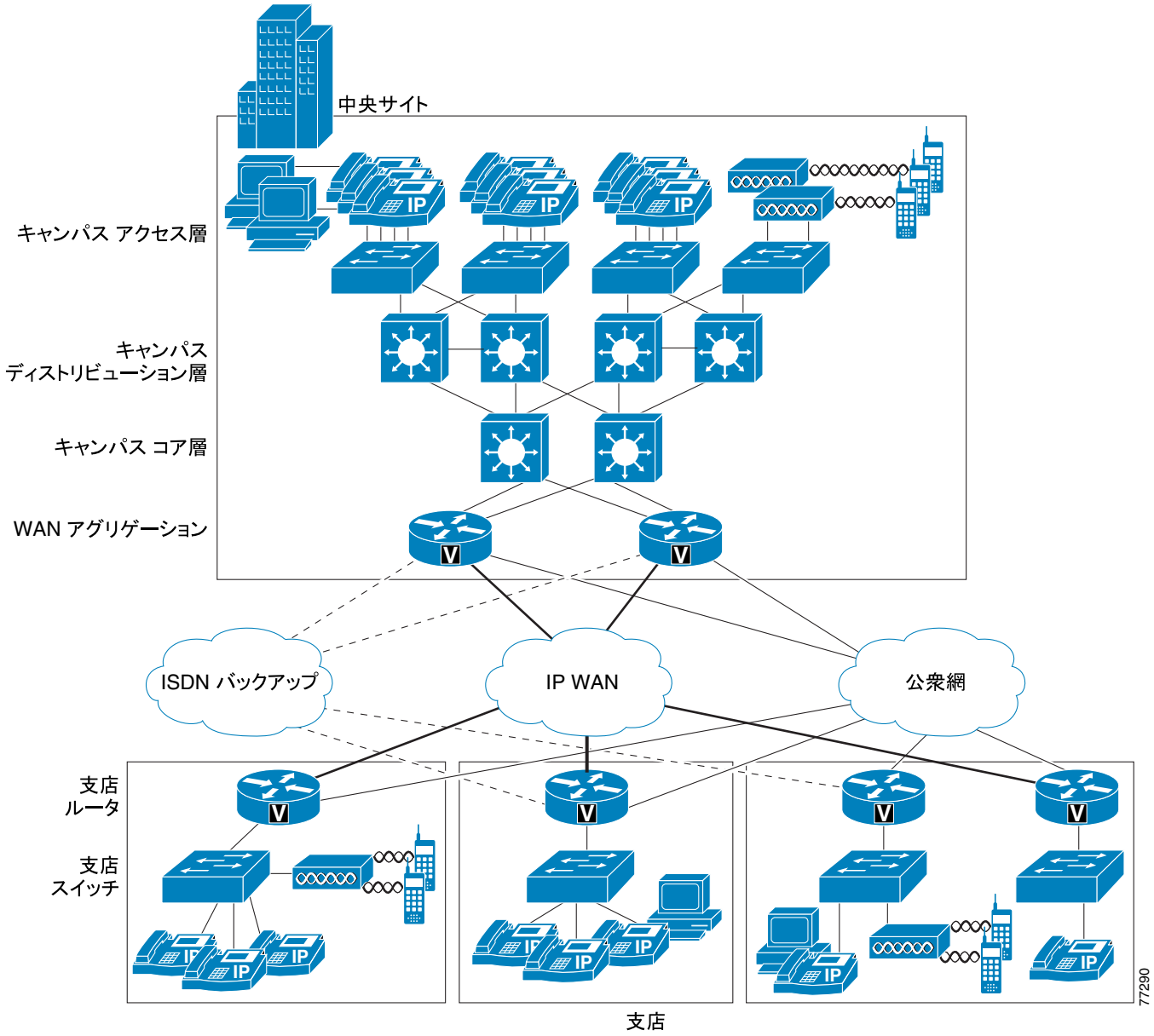


表 3-1　ネットワーク インフラストラクチャ内の役割に必要な機能

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 • トラフィック分類 • トラフィック再分類 • 802.1p および 802.1Q
支店ルータ （スポーク サイト）	• 複数キュー サポート • LFI • リンク効率 • トラフィック分類 • トラフィック再分類 • 802.1p および 802.1Q
支店または小規模サイトのスイッチ	• インライン パワー • 複数キュー サポート • 802.1p および 802.1Q

LAN インフラストラクチャ

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

- 高可用性のための LAN 設計（P.3-4）
- LAN の QoS（P.3-22）

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.3-6）
- キャンパス コア レイヤ（P.3-10）
- ネットワーク サービス（P.3-10）

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

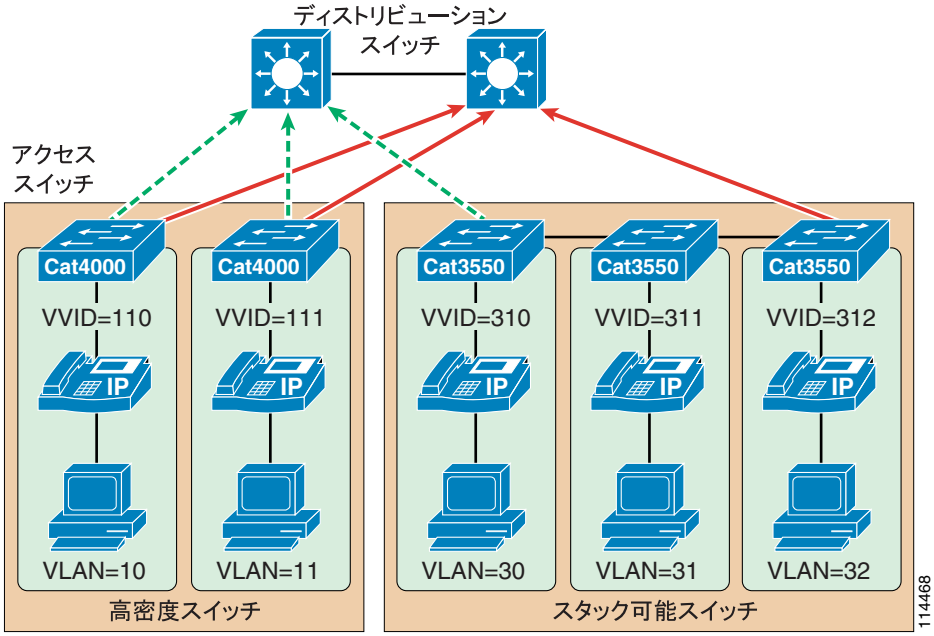
http://www.cisco.com/warp/public/cc/so/neso/lnso/cpso/gcnd_wp.pdf

キャンパス アクセス レイヤ

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

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

図 3-2　音声とデータに対応するアクセス レイヤ スイッチと VLAN



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

次の理由により、音声とデータの VLAN を分離することをお勧めします。

- アドレス スペースの確保と、外部ネットワークからの音声デバイスの保護

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

- QoS 信頼性境界の音声デバイスへの拡張

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

- 悪質なネットワーク攻撃からの保護

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

- 管理および設定の容易性

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

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

- 電話機が接続されているポート上でレイヤ 2 CoS パケット マーキングを適切に処理するための 802.1Q トランキングおよび 802.1p
- RTP 音声パケット ストリームのプライオリティ キューイングを行う複数の出力キュー

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

Spanning Tree Protocol（STP）

コンバージェンス時間を最小限に抑え、レイヤ 2 のフォールト トレランスを最大限に高めるには、次の STP 機能を有効にします。

- PortFast

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

- ルート ガードまたは BPDU ガード

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

- UplinkFast と BackboneFast

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

- 単方向リンク検出（UDLD）

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

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

キャンパス ディストリビューション レイヤ

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

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

ホットスタンバイ ルータ プロトコル（HSRP）

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

- standby track

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

- standby preempt

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

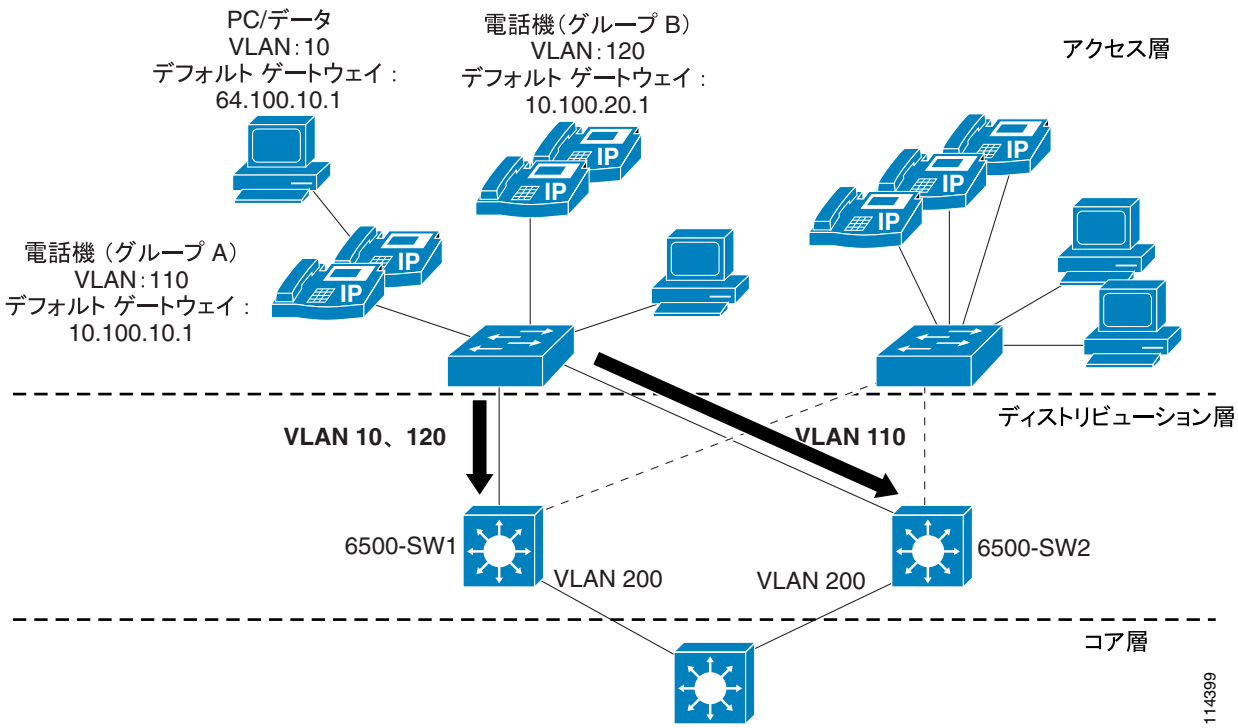
また、HSRP には、両方の HSRP ルータ間でトラフィックをロード バランシングするように設定する必要があります。ロード バランシングを行うには、アクティブ HSRP ルータである各 HSRP デバイスを 1 つの VLAN またはインターフェイス用に設定し、スタンバイ ルータを別の VLAN またはインターフェイス用に設定します。両方の HSRP デバイスにアクティブ VLAN とスタンバイ VLAN を均等に分散させると、ロード バランシングが保証されます。1 つの VLAN 上のデバイスは、アクティブ HSRP デバイスをそのデフォルト ゲートウェイとして使用し、別の VLAN 上の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

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

図 3-3 のアクセス レイヤにある PC と電話機には、各 HSRP グループの HSRP アドレスに対応したデフォルト ゲートウェイが設定されています。Voice VLAN 110 および 120 のデバイスは、デフォルト ゲートウェイとして 10.100.10.1 と 10.100.20.1 をそれぞれ指しています。これらのデフォルト ゲートウェイは、両方のスイッチにある VLAN 110 および 120 インターフェイスの HSRP アドレスに対応しています。データ VLAN 10 のデバイスは、デフォルト ゲートウェイとして 64.100.10.1 を指しています。このデフォルト ゲートウェイは、両方のスイッチにある VLAN 10 インターフェイスの HSRP アドレスに対応しています。アクセス レイヤからディストリビューション レイヤに流

れるトラフィックは 2 つのスイッチに分散されます（障害がない場合）が、リターン パスでの分散を保証するメカニズムはありません。コア レイヤから戻ってアクセス レイヤに向かうトラフィックは、最短および最小コストの、またはそのどちらかのルーテッド パスに沿って流れます。

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



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

例 3-1　6500-SW1 の設定

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

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

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

例 3-2　6500-SW2 の設定

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

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

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

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

ルーティング プロトコル

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

キャンパス コア レイヤ

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

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

- 冗長なリンクまたはケーブル パス

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

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

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

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

データ センターとサーバ ファーム

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

ネットワーク サービス

可用性が高く、耐障害性のあるマルチレイヤ キャンパス ネットワークの構築が完了したら、DNS、DHCP、TFTP、および NTP などのネットワーク サービスを配置できます。

ドメイン ネーム システム（DNS）

DNS を使用すると、ホスト名をネットワーク（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、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。

ただし、DNS を利用することは問題となる場合があります。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、Cisco CallManager と IP テレフォニー エンドポイント間の通信には DNS を利用しないでください。

ホスト名の代わりに IP アドレスを使用するように、Cisco CallManager、ゲートウェイ、およびエンドポイント デバイスを設定します。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。同様に、HOSTS ファイルを設定することもお勧めできません。これは、何千ものエンドポイントおよびサーバを含む大規模な IP テレフォニー ネットワークでは、このファイルの管理に膨大な時間がかかり、非効率的になる場合があるためです。IP テレフォニー ネットワークから DNS 設定を排除すれば、テレフォニー デバイスおよびアプリケーションは DNS サーバを利用する必要がなくなります。

ただし、LMHOSTS ファイルを設定する必要はあります。このファイルは、サーバのホスト名または NetBios 名を IP アドレスに解決またはマッピングするメカニズムを備えています。LMHOSTS ファイルには、サーバ名とそれに対応する IP アドレスのリストを含める必要があります。クラスタ内のすべてのサーバに関するエントリと、**127.0.0.1 localhost** を持つエントリ（ループバック エントリ）を含める必要があります。このファイルをクラスタ内のすべてのサーバにコピーする必要があります。LMHOSTS ファイルは、ディレクトリ パス C:\WINNT\system32\drivers\etc に配置します。例 3-3 は、6 つのサーバを含むクラスタの一般的な LMHOSTS ファイルを示しています。

例 3-3　LMHOSTS ファイル

```
127.0.0.1       localhost      !The local host entry
64.101.1.7      ccm1-hq-1
64.101.2.7      ccm1-hq-2
64.101.1.8      ccm1-hq-3
64.101.2.8      ccm1-hq-4
64.101.1.21     ccm1-moh-1
64.101.2.21     ccm1-moh-2
```

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

このどちらかの状況で DNS の設定が必要になった場合は、DNS サーバを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) クラスタ内の DNS 名が解決されるのは、システムの初期化時（つまり、サーバのブートアップ時）のみです。結果として、クラスタ内のサーバが、DNS サーバ上で変更された DNS 名を解決できるようにするには、クラスタ内のすべてのサーバ上で Cisco CallManager サービスを再起動する必要があります。

Dynamic Host Configuration Protocol（DHCP）

DHCP は、ネットワーク上のホストが、IP アドレス、サブネット マスク、デフォルト ゲートウェイ、および TFTP サーバ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 テレフォニー 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 テレフォニー ネットワーク デバイスに設定情報を提供することができます。既存のデータ専用ネットワークに IP テレフォニー デバイスを配置する場合、作業としては、この新しい音声デバイスに対応する DHCP 音声スコープを既存の DHCP サーバに追加するだけで済みます。IP テレフォニー デバイスは、DHCP サーバを利用して IP 設定情報を取得するように設定されているため、DHCP サーバは冗長な方式で配置する必要があります。テレフォニー ネットワークには、2 つ以上の DHCP サーバを配置する必要があります。この配置により、いずれかのサーバに障害が発生しても、他のサーバが引き続き DHCP クライアント要求に応答できます。また、DHCP サーバに、ネットワーク内の DHCP に依存するクライアントすべてを処理するのに十分な IP サブネット アドレスが設定されていることを確認する必要があります。

DHCP オプション 150

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

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

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

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

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

DHCP、スタンドアロン サーバと共存サーバの比較

一般に、DHCP は、スタンドアロン サーバ上で動作するように設定される必要があります。これは、多数のデバイスが DHCP 設定を要求すると、CPU とメモリの使用率が増加し、サーバのパフォーマンスに影響を及ぼす場合があるためです。したがって、Cisco CallManager サーバ上では DHCP を実行しないでください。たとえば、クラスタに登録されているデバイスが 1,000 以下の小規模な Cisco CallManager 配置であれば、Cisco CallManager サーバ上で DHCP を実行してもかまいません。ただし、サーバの CPU 負荷が高くなる場合は、DHCP をスタンドアロン サーバに移行する必要があります。クラスタに登録されているデバイスが 1,000 を超える場合、DHCP はスタンドアロン サーバ上で実行される必要があります。

DHCP のリース期間

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

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

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

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

次のいずれかの方法によって、この状況を緩和できます。

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

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

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

DHCP のネットワーク配置

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

- 中央の DHCP サーバ

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

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

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

  集中型マルチサイト Cisco CallManager 配置で使用する DHCP を設定する場合は、中央の DHCP サーバを使用して、中央にあるデバイスに DHCP サービスを提供することができます。リモート デバイスは、ローカルに設置されたサーバから、またはリモート サイトにある Cisco IOS ルータから、DHCP サービスを受信できます。このタイプの配置では、WAN に障害が発生しても、リモートのテレフォニー デバイスから DHCP サービスを使用できることが保証されます。例 3-4 は、Cisco IOS DHCP サーバの基本的な設定コマンドを示しています。

例 3-4　Cisco IOS DHCP サーバの設定コマンド

```
service dhcp                                !Activate DHCP Service on the IOS Device

ip dhcp excluded-address <ip-address>|<ip-address-low> <ip-address-high>
                                            !  Specify an IP Address or IP Address Range
to
                                            !  be excluded from the DHCP pool

ip dhcp pool <dhcp-pool name>               !Specify DHCP pool name
   network <ip-subnet> <mask>               !Specify DHCP pool IP subnet and mask
   default-router <default-gateway-ip>      !Specify the Default-gateway
   option 150 ip <tftp-server-ip-1> ...     !Specify TFTP servers (up to four) -
                                            ! IP phones use only the first two addresses
in
                                            ! the array.
```

Trivial File Transfer Protocol（TFTP）

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

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

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

たとえば、Cisco CallManager Release 3.3(3)SR1 では、電話機の設定ファイルのサイズは約 2,700 バイトで、Cisco IP Phone 7960 用のデフォルトのソフトウェア ロード（P00305000101.bin）は 396,804 バイトです。支店において 256 Kbps の WAN 帯域幅を使用してソフトウェアをダウンロードする場合、1 台の電話機でアップグレード時に新しいソフトウェアをダウンロードするには、約 12 秒かかります。その同じ支店にある 10 台の電話機で新しいソフトウェアが必要な場合、ダウンロード プロセスには約 2 分かかります。

マルチクラスタ キャンパス 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。したがって、この中央の TFTP サーバは、他のクラスタによって作成および管理されるファイルにアクセスできる必要があります。

このファイルにアクセスできるようにするには、各クラスタの TFTP サーバを、中央の TFTP サーバのドライブ上で設定ファイルを作成および管理するように設定する必要があります。設定を実行するには、各 TFTP サーバ（中央の TFTP サーバを除く）の設定で代替ファイル ロケーション エントリを使用します。

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

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

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。中央の TFTP サーバは、他のクラスタに関連付けられたサブディレクトリまで検索するように設定される必要があります。

例 3-5　代替 TFTP ファイル ロケーション

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

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

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

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

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

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

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

さらに、大規模なキャンパス配置では、Maximum Serving Count サービス パラメータを、次のように調整します。専用 TFTP サーバの推奨値は、シングル プロセッサ システムの場合が 1,500 で、デュアルプロセッサ システムの場合が 3,000 です。デュアルプロセッサ システムが Windows 2000 Advanced Server を実行している場合、サービス数は最大 5,000 にすることができます。

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。

図 3-4 に示されているように、クラスタ内に 2 つの TFTP サーバを設定できます。各サーバでは、同じ設定ファイルのリストを別々に作成および管理できます。マルチクラスタ配置では、各クラスタに、プライマリとセカンダリの 2 つの TFTP サーバを設定できます。プライマリ TFTP サーバは、中央のプライマリ TFTP サーバにファイルを書き込むように設定できます。同様に、セカンダリ TFTP サーバでは、中央のセカンダリ TFTP サーバにファイルを書き込むように設定できます。この設定により、冗長性を保証するように設定された TFTP サーバに関する 2 つの別々のグループ（プライマリとセカンダリ）が作成されます。各グループには、中央サーバとして機能するメンバーが設定されます。

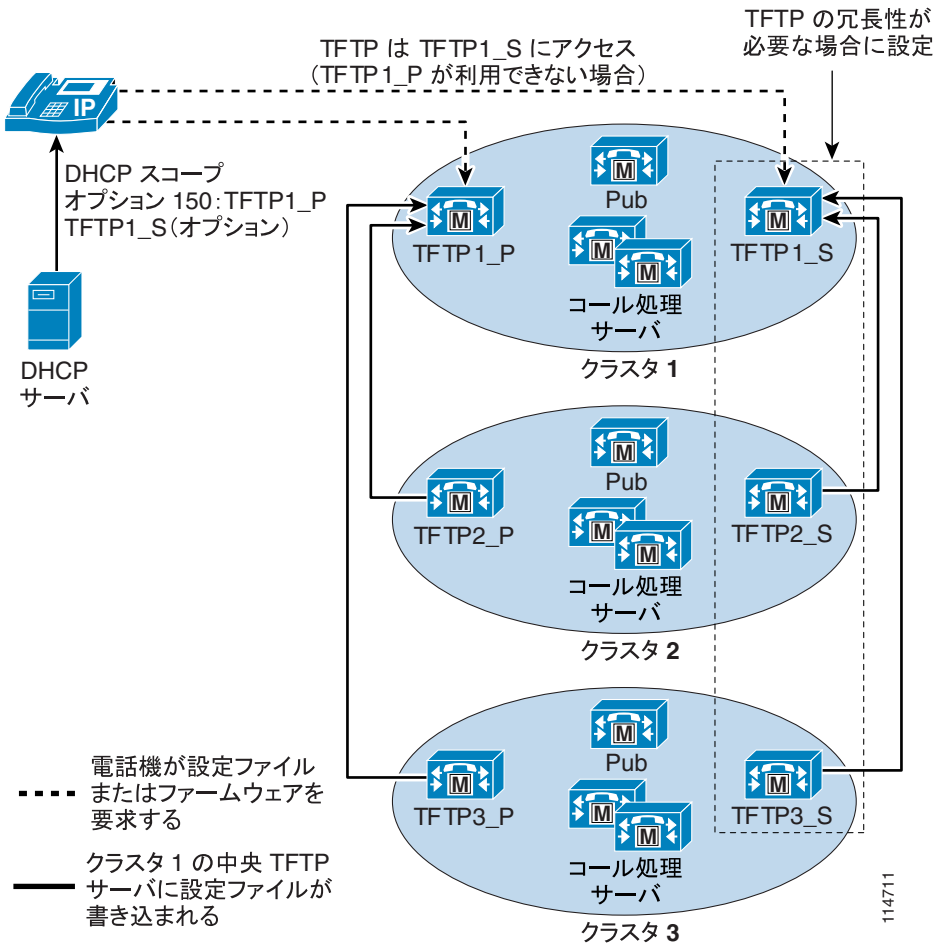
例 3-6　TFTP サーバの冗長性

例 3-5 で説明した事例に対して TFTP の冗長性を追加する場合は、各クラスタに 2 つの TFTP サーバを設定します。すべてのプライマリ TFTP サーバは、その設定ファイルを TFTP1_P に書き込むように設定し、すべてのセカンダリ TFTP サーバは、その設定ファイルを TFTP1_S に書き込むように設定します。次を参照してください。

- TFTP2_P の代替ファイル ロケーションの設定：\\TFTP1_P\Program Files\Cisco\TFTPpath\TFTP2
- TFTP3_P の代替ファイル ロケーションの設定：\\TFTP1_P\Program Files\Cisco\TFTPpath\TFTP3
- TFTP2_S の代替ファイル ロケーションの設定：\\TFTP1_S\Program Files\Cisco\TFTPpath\TFTP2
- TFTP3_S の代替ファイル ロケーションの設定：\\TFTP1_S\Program Files\Cisco\TFTPpath\TFTP3

TFTP1_P と TFTP1_S はどちらも、例 3-5 で説明したように、代替ファイル ロケーションのリストを検索するように設定する必要があります。

図 3-4　すべてのクラスタの中央 TFTP サーバに関する TFTP サーバの冗長性



TFTP のロード シェアリング

前の項では、一度に 1 つの TFTP サーバを使用して複数のクラスタの電話機にサービスを提供する方法について説明しました。ここで示すアプローチでは、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 の場合：オプション 150：TFTP1_P、TFTP1_S
- サブネット 10.1.2.0/24 の場合：オプション 150：TFTP1_S、TFTP1_P

通常動作では、サブネット 10.1.1.0/24 の電話機は TFTP1_P 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_S に TFTP サービスを要求します。TFTP1_P に障害が発生した場合、両方のサブネットの電話機は TFTP1_S に TFTP サービスを要求します。

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

ネットワーク タイム プロトコル（NTP）

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

Cisco CallManager の NTP 時刻同期

時刻同期は、Cisco CallManager サーバにおいて特に重要です。次の手順を実行して、ネットワーク内のすべての Cisco CallManager 上で自動 NTP 時刻同期を設定する必要があります。

ステップ 1　NTP.conf ファイルを設定します。

NTP.conf ファイルは C:\WINNT\ ディレクトリにあります。ファイルには、時刻について照会できる 1 つ以上の NTP タイム サーバのリストを設定する必要があります。また、ファイルは、ローカル LAN セグメントの NTP ブロードキャストを介して NTP タイム サーバのアップデートを受信するように設定する必要もあります。Cisco CallManager でブロードキャスト メッセージを介して時刻を受信するために使用できる、ブロードキャスト対応の NTP タイム サーバが必要です。例 3-7 は、NTP.conf ファイルを設定する 2 つの方法を示しています。

ステップ 2　NTP Service がブートアップ時に自動的に開始するように設定します。

各 Cisco CallManager サーバにおいて、Microsoft Windows のサービス アプリケーションで、NTP Service がシステムのブートアップ時に自動的に開始するように設定します。

ステップ 3　各 Cisco CallManager サーバにおいて、サービス アプリケーションを使用して NTP Service を開始または再開します。

（注）　NTP Service が Cisco CallManager サーバ上の Microsoft サービス コントロール パネル アプリケーションに表示されない場合は、C:\Program Files\Cisco\Xntp>**install.bat** を実行して手動でインストールします。

例 3-7　NTP.conf 設定ファイル

```
server 64.100.21.254
server 64.200.40.10
driftfile %windir%\ntp.drift
```

または

```
broadcastclient
driftfile %windir%\ntp.drift
```

例 3-7 で参照されている driftfile は、NTP タイム サーバから受信された NTP メッセージ内の情報に基づいて、NTP Service を介して自動的にアップデートされます。

(注) デフォルトでは、NTP サーバと NTP クライアント間のクロック オフセットまたは調整幅が 1,000 秒より大きい場合、NTP のアップデートは行われません。このデフォルト動作を調整するには、**tinker panic** < *秒数* > コマンドを NTP.conf ファイルに追加します。秒数には、許容できる時間差を指定します。この値を 0 に設定すると、panic 機能が無効になり、任意の値のクロック オフセットが受け入れられます。

Cisco IOS と CatOS の NTP 時刻同期

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

例 3-8 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 3-8　Cisco IOS と CatOS の NTP 設定

Cisco IOS の設定：

```
ntp server 64.100.21.254
```

CatOS の設定：

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

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

Power over Ethernet（PoE）

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

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

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

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

シスコでは現在、Cisco PoE インライン パワーのほかに、IEEE 802.3af PoE 標準をサポートしています。現時点で 802.3af に準拠しているのは、一部のアクセス スイッチおよび電話機のみです。将来的には、すべての電話機とスイッチが 802.3af PoE をサポートする予定です。Catalyst 6500、4500、および 3750 は、現在、802.3af をサポートしています。802.3af PoE 標準をサポートする Cisco IP Phone については、P.17-34 の「エンドポイント機能の要約」を参照してください。

カテゴリ 3 ケーブリング

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

- PC ポートを持ち、そのポートに PC が接続された IP Phone（Cisco 7970、7960、7940、および 7910+SW IP Phone）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 7902、7905、および 7910 IP Phone）は、10 Mb 半二重に自動ネゴシエートできるようになっている必要があります。

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

- PC ポートを持つが、そのポートに PC が接続されていない IP Phone（Cisco 7970、7960、7940、7910+SW、および 7912 IP Phone）は、10Mb 半二重にネゴシエートできるよう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 7912 IP Phone については、PC が接続されているときには、カテゴリ 3 ケーブルと共に使用しないでください。これは、この電話機のスイッチ ポートと PC ポートを 10 Mb 全二重にすることができないためです。

IBM タイプ 1A および 2A ケーブリング

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

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

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

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

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

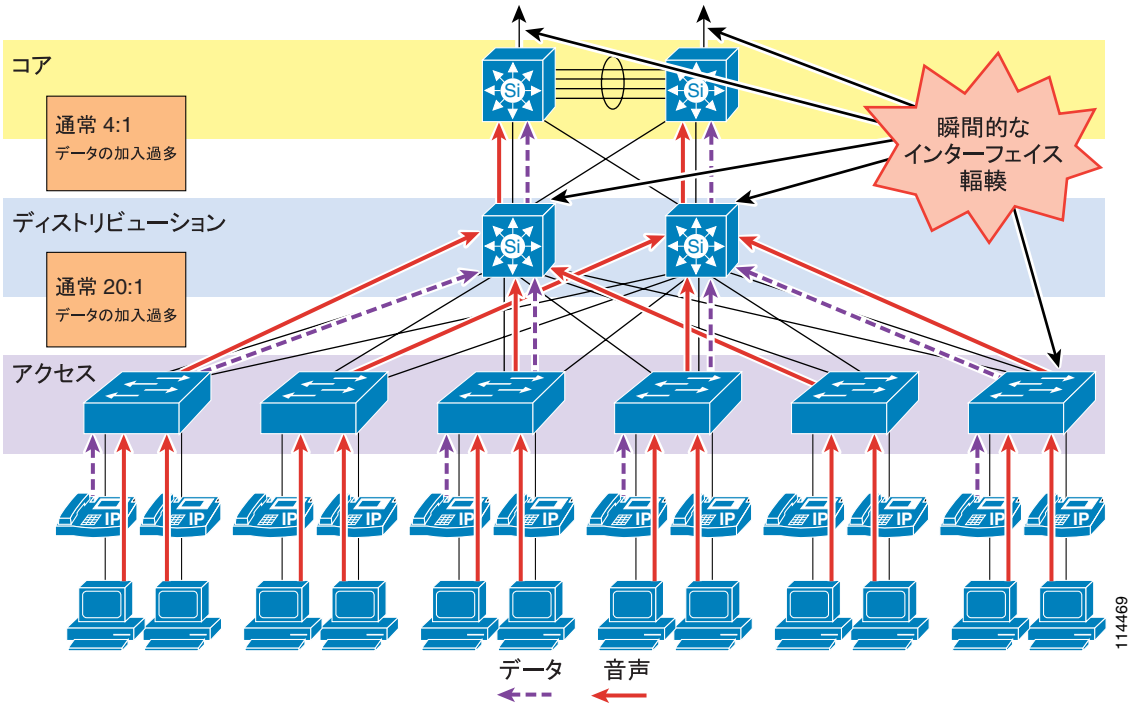
http://www.cisco.com

LAN の QoS

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

図 3-5 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 3-5　LAN におけるデータ トラフィックのオーバーサブスクリプション



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

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

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

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

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

- トラフィック分類

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

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

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

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

- トラフィック分類（P.3-24）
- インターフェイス キューイング（P.3-25）
- 帯域幅のプロビジョニング（P.3-25）
- 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.3-25）

トラフィック分類

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

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

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

トラフィックのタイプ	レイヤ 2 サービス クラス（CoS）	レイヤ 3 IP 優先順位	レイヤ 3 Differentiated Services Code Point（DSCP）	レイヤ 3 Per-Hop Behavior（PHB）
音声 Real-Time Transport Protocol（RTP）	5	5	46	EF
音声制御シグナリング[1]	3	3	24	CS3
ビデオ会議	4	4	34	AF41
データ	0、1、2	0、1、2	10 ～ 22	BE ～ AF23

1. 音声制御シグナリング 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。

インターフェイス キューイング

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

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

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

帯域幅のプロビジョニング

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

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

QoS が使用されない場合の IP コミュニケーションの障害

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

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

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

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

WAN インフラストラクチャ

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

WAN の設計と設定に関するベスト プラクティス

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

音声ネットワークに関する WAN 配置では、ハブアンドスポーク トポロジに従う必要があります。このトポロジは、中央のハブ サイトと、中央のハブ サイトに接続された複数のリモート スポーク サイトを持ちます。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。このトポロジにすると、中央サイトの Cisco CallManager 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。

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、第 2 章「IP テレフォニー配置モデル」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。

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 CallManager Express（CME）などのコール処理アプリケーションは、適宜、サイトの規模やそのサイトにおけるこれらの機能の重要性に応じて、中央以外のサイトに配置される必要があります。音声アプリケーションおよびデバイスを非集中化すると、ネットワーク配置がより複雑になり、企業全体でこれらのリソースを管理する作業もより複雑になり、さらにネットワーク ソリューションの総コストが増加する可能性があることに留意してください。ただし、WAN リンク障害の発生中にリソースが使用可能になるという事実により、これらの要因は軽減される場合もあります。

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

最後に、International Telecommunication Union（ITU; 国際電気通信連合）の G.114 勧告には、音声ネットワークにおける片方向の遅延は 150 ミリ秒以下でなければならないと明記されています。ネットワーク内に低速 WAN リンクを実装する場合は、この要件に留意することが重要です。片方向の遅延がこの 150 ミリ秒の勧告を超えないように、WAN リンクのトポロジ、テクノロジー、および物理的な距離を考慮する必要があります。

保証帯域幅

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

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

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

ベストエフォート型の帯域幅

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

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

- インターネット
- DSL
- ケーブル
- 衛星
- 無線

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

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

WAN の QoS

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

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

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

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

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

WAN テクノロジー	リンク速度 :56 kbps ～ 768 kbps	リンク速度 :768 kbps 以上
専用回線	• MLP（マルチリンク ポイントツーポイント プロトコル） • MLP LFI（Link Fragmentation and Interleaving） • LLQ（低遅延キューイング） • オプション :cRTP（Compressed Real-Time Transport Protocol）	• 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
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

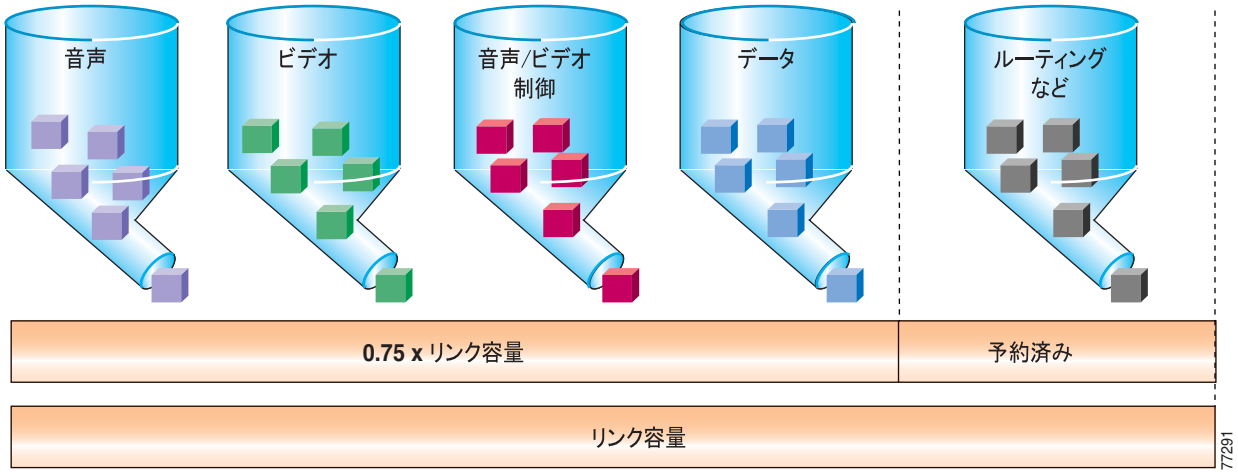
次の 4 つの項では、音声とデータの両方のトラフィックをサポートするように WAN を設計する場合に、考慮すべき最も重要な機能と手法を説明しています。

- 帯域幅のプロビジョニング（P.3-31）
- トラフィックの優先順位（P.3-37）
- リンク効率手法（P.3-39）
- トラフィック シェーピング（P.3-41）

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 3-6 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 3-6　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、音声キャリア ストリーム。
- コールに関係するエンドポイントに応じて、複数のプロトコルのいずれか（たとえば、H.323、MGCP、SCCP、または (J)TAPI）に属するパケットから構成される、コール制御信号。たとえば、コール制御機能は、コールのセットアップ、保持、終了、または転送に使用される機能です。

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

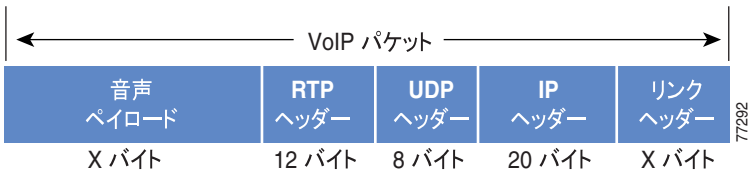
次の 3 つの項では、次のタイプのトラフィックについて、帯域幅プロビジョニングの推奨事項を説明します。

- すべてのマルチサイト WAN 配置における音声ベアラ トラフィック（P.3-32 の「音声ベアラ トラフィック用のプロビジョニング」を参照）
- 集中型コール処理を使用するマルチサイト WAN 配置におけるコール制御トラフィック（P.3-34 の「集中型コール処理を使用したコール制御トラフィック用のプロビジョニング」を参照）
- 分散型コール処理を使用するマルチサイト WAN 配置におけるコール制御トラフィック（P.3-36 の「分散型コール処理を使用したコール制御トラフィック用のプロビジョニング」を参照）

音声ベアラ トラフィック用のプロビジョニング

図 3-7 に示されているように、VoIP（Voice-over-IP）パケットは、ペイロード、IP ヘッダー、ユーザ データグラム プロトコル（UDP）ヘッダー、Real-Time Transport Protocol（RTP）ヘッダー、およびレイヤ 2 リンク ヘッダーから構成されています。デフォルトのパケット レート 20 ms では、VoIP パケットには、G.711 の場合は 160 バイトのペイロードがあり、G.729 の場合は 20 バイトのペイロードがあります。SRTP（Secure Real-Time Transport Protocol）暗号化を使用すると、各パケットのペイロードは 4 バイト増加します。デフォルトのパケット レート 20 ms では、SRTP VoIP パケットには、G.711 の場合は 164 バイトのペイロードがあり、G.729 の場合は 24 バイトのペイロードがあります。IP ヘッダーは 20 バイト、UDP ヘッダーは 8 バイト、RTP ヘッダーは 12 バイトです。リンク ヘッダーの大きさは、使用されるレイヤ 2 メディアによって異なります。

図 3-7　一般的な VoIP パケット



VoIP ストリームによって消費される帯域幅を計算するには、パケットのペイロードとすべてのヘッダーを加算し（ビット単位）、1 秒当たりのパケット レート（デフォルトでは、毎秒 50 パケット）を掛けます。表 3-4 では、デフォルトのパケット レートである毎秒 50 パケット（pps）での VoIP フロー当たりの帯域幅を詳しく記述しています。表 3-4 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、Compressed Real-Time Transport Protocol（cRTP）などの可能な圧縮方式を考慮していません。Cisco CallManager Administration の Service Parameters メニューを使用すると、パケット レートを調整できます。

表 3-4 は、音声ペイロードと IP ヘッダーのみによって消費される帯域幅を示しています。ここでは、パケット レートとして、デフォルトのパケット レートである 50 パケット / 秒（pps）と、暗号化されていないペイロードと暗号化されたペイロードの両方のレートである 33.3 pps を使用しています。

表 3-4　音声ペイロードと IP ヘッダーのみの帯域幅使用量

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

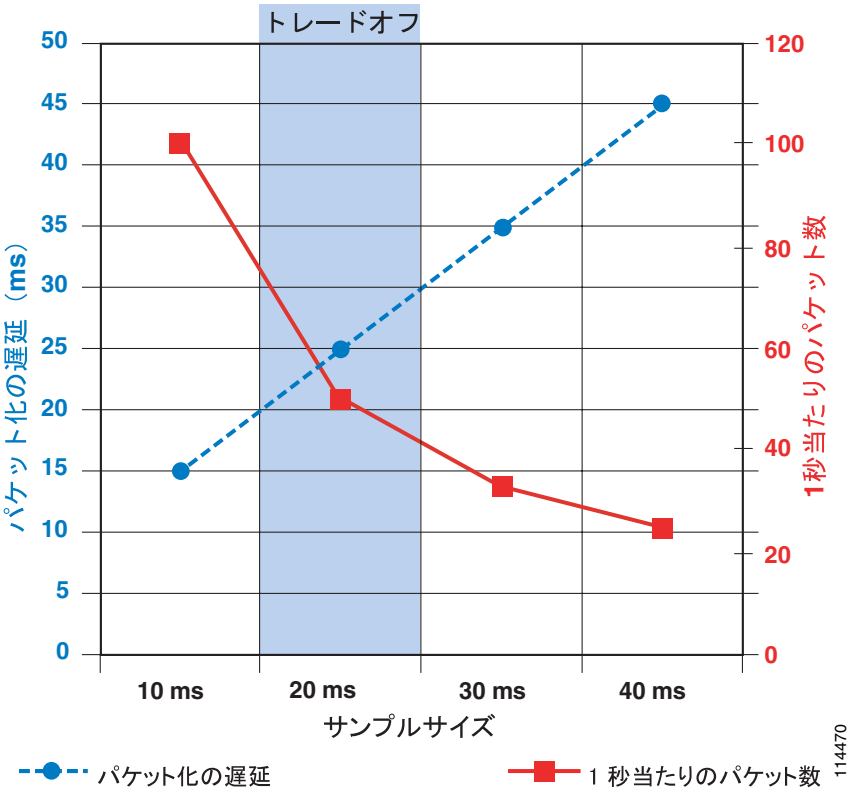
より正確な方法でプロビジョニングするには、帯域幅の計算にレイヤ 2 ヘッダーを含めます。表 3-5 は、レイヤ 2 ヘッダーを計算に含めたときの、音声トラフィックによって消費される帯域幅の量を示しています。

表 3-5　レイヤ 2 ヘッダーが含まれた帯域幅使用量

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

30 ms を超えるサンプリング レートを設定することは可能ですが、これを行うと、通常、音声品質が非常に低下します。図 3-8 に示されているように、サンプリング サイズが増加すると、1 秒当たりのパケット数が減少するため、デバイスの CPU に与える影響は小さくなります。同様に、サンプル サイズが増加すると、1 パケット当たりのペイロードが大きくなるため、IP ヘッダーのオーバーヘッドが低下します。ただし、サンプル サイズが増加すると、パケット化の遅延も増加するため、音声トラフィックのエンドツーエンドの遅延が増加します。サンプル サイズを設定する場合は、パケット化の遅延と 1 秒当たりのパケット数とのトレードオフを考慮する必要があります。このトレードオフが 20 ms で最適化されている場合、30 ms のサンプル サイズでも、1 秒当たりのパケット数に対する遅延の比率は妥当なものになります。しかし、40 ms のサンプル サイズでは、パケット化の遅延が大きくなりすぎます。

図 3-8　音声のサンプル サイズ：1 秒当たりのパケット数とパケット化の遅延との比較



集中型コール処理を使用したコール制御トラフィック用のプロビジョニング

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

この配置モデルには、次の考慮事項が適用されます。

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

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

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

- 休止トラフィック。このトラフィックは、電話機のアクティビティに関係なく、支店の IP Phone と Cisco CallManager との間で定期的に交換されるキープアライブ メッセージから構成されます。
- 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 IP Phone および / またはゲートウェイと、中央サイトの Cisco CallManager との間で交換されるシグナリング メッセージから構成されます。

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

(注)　この平均数が、特定の配置のニーズを満たさない場合、P.3-36 の「拡張公式」に記載されている拡張公式を使用して、推奨帯域幅を計算できます。

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

公式 1：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 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 パターンの変更を吸収し、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、過剰プロビジョニング係数を導入することをお勧めします。この導入は、キューのサービス レートを増やすことに相当します。

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

公式 2：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）

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 3-6 のようにまとめることができます。

表 3-6　コール制御トラフィック用の推奨帯域幅（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）	制御トラフィック用の推奨帯域幅（暗号化なし）	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
20	8 kbps	9 kbps
30	8 kbps	13 kbps
40	11 kbps	17 kbps
50	14 kbps	21 kbps
60	16 kbps	25 kbps
70	19 kbps	29 kbps
80	21 kbps	33 kbps
90	24 kbps	38 kbps

表 3-6　コール制御トラフィック用の推奨帯域幅（シグナリングの暗号化の有無別）（続き）

支店の規模（IP Phone とゲートウェイの数）	制御トラフィック用の推奨帯域幅（暗号化なし）	制御トラフィック用の推奨帯域幅（暗号化あり）
100	27 kbps	42 kbps
110	29 kbps	46 kbps
120	32 kbps	50 kbps
130	35 kbps	54 kbps
140	37 kbps	58 kbps
150	40 kbps	62 kbps

（注）　表 3-6 の値は、レイヤ 3 帯域幅を示しています。WAN リンクをプロビジョニングする場合、使用するレイヤ 2 テクノロジーに応じて、これらの数値にレイヤ 2 オーバーヘッドを加算する必要があります。

拡張公式

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

公式 3：支店の推奨帯域幅、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 4：リモート サイトの支店の推奨帯域幅、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）

分散型コール処理を使用したコール制御トラフィック用のプロビジョニング

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

この配置モデルには、次の考慮事項が適用されます。

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

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

WAN を通過する制御トラフィックは、次のカテゴリのいずれかに属します。

- 静止トラフィック。このトラフィックは、各 Cisco CallManager とゲートキーパー間で定期的に交換される登録メッセージから構成されます。

- コール関連トラフィック。このトラフィックは、次の 2 つのタイプのトラフィックから構成されます。
  - コール アドミッション制御トラフィック：コールのセットアップ前とコールの終了後に、Cisco CallManager とゲートキーパー間で交換される。
  - H.225 または H.245 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、2 つの Cisco CallManager 間で交換される。

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

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

公式 5: 仮想タイ ライン数に基づく推奨帯域幅

推奨帯域幅 (bps) = 116 ∗（仮想タイ ライン数）

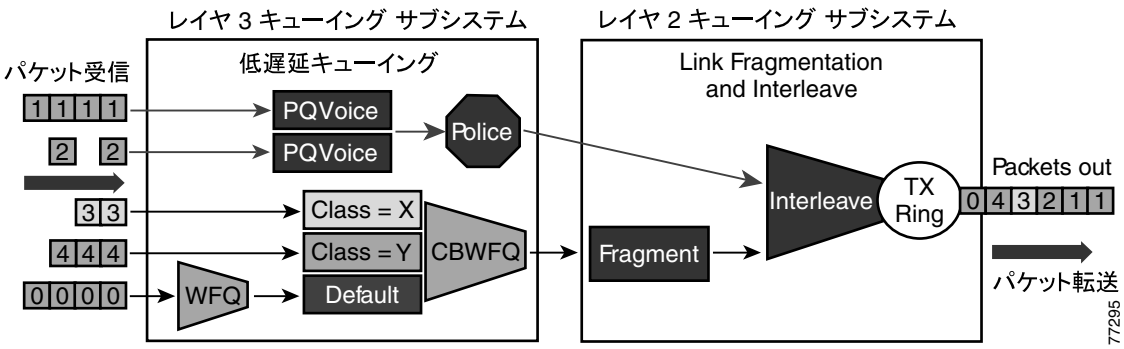
Cisco IOS ルータ上のキューに割り当て可能な最小帯域幅は、8 Kbps です。つまり 8 Kbps の最小キュー サイズは、*最大 70 の仮想タイ ライン*によって生成されるコール制御トラフィックを受け入れることができると推定できます。これは、大部分の大企業での配置に十分な量です。

トラフィックの優先順位

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

図 3-9 は、優先順位体系の例を示しています。

図 3-9　WAN を介した VoIP 用の最適化キューイング



LLQ には、次の優先順位の基準を使用することをお勧めします。

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

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

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

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

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

リンク効率手法

次のリンク効率技術によって、低速 WAN リンクの品質と効率が向上します。

Compressed Real-Time Transport Protocol（cRTP）

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

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

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

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

cRTP 圧縮は、パケットが出力インターフェイスを通過する前、つまり、LLQ クラスベース キューイングが行われた後の最終段階として行われます。Cisco IOS Release 12.(2)2T からは、cRTP により、*音声*クラスの帯域幅を圧縮パケット値に基づいて設定できる LLQ クラスベース キューイング メカニズムからフィードバック メカニズムを使用できるようになりました 12.(2)2T より前の Cisco IOS リリースでは、このメカニズムは使用されていないため、LLQ は圧縮帯域幅を認識しません。したがって、圧縮が行われないものとして、*音声*クラスの帯域幅をプロビジョニングする必要があります。表 3-7 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 3-7 では、cRTP 以外の G.729 コールの場合が 24 Kbps で、cRTP の G.729 コールの場合が 10 Kbps であることを前提としていることに注意してください。これらの帯域幅の数値は、音声ペイロードと IP/UDP/RTP ヘッダーのみに基づいています。レイヤ 2 ヘッダーの帯域幅は考慮に入れていません。ただし、実際の帯域幅プロビジョニングでは、レイヤ 2 ヘッダーの帯域幅も、WAN リンクで使用されたタイプに基づいて考慮に入れられます。

表 3-7　512 Kbps リンク帯域幅と G.729 コーデックを使用して 10 コールに対応する場合の LLQ 音声クラスの帯域幅要件

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

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

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

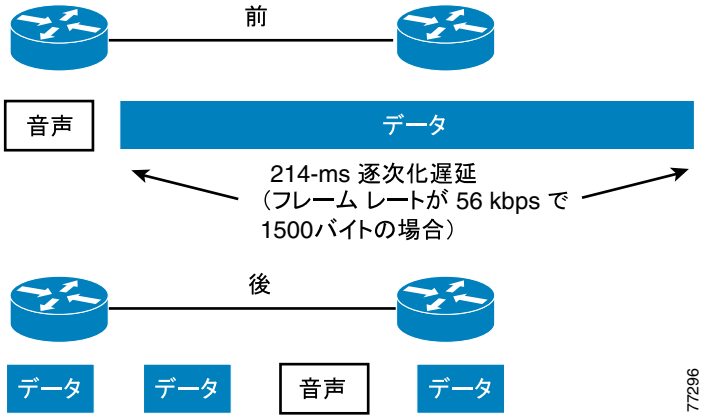
音声およびビデオに対応した IPSec VPN（V3PN）で cRTP を使用する場合の追加の推奨事項については、次の Web サイトで入手可能な V3PN 資料を参照してください。

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

LFI（Link Fragmentation and Interleaving）

低速リンク（768 Kbps 未満）の場合、許容できる音声品質を確保するには、LFI メカニズムを使用する必要があります。この手法は、図 3-10 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 3-10　LFI（Link Fragmentation and Interleaving）



Voice-Adaptive Fragmentation（VAF）

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

VAF は、一般に、Voice-Adaptive Traffic Shaping と組み合せて使用されます（P.3-42 の「Voice-Adaptive Traffic Shaping（VATS）」を参照）。VAF はオプションの LFI ツールです。VAF を有効にする場合は注意が必要です。これは、音声アクティビティが検出されるタイミングと LFI メカニズムが連動するタイミングの間に多少の遅延が生じるためです。また、最後の音声パケットが検出されてから、VAF が非アクティブになるまでの間に、設定可能な非アクティブ化タイマー（デフォルトは 30 秒）が期限切れになる必要があります。そのため、この期間は LFI が不必要に発生します。VAF は、Cisco IOS Release 12.2(15)T 以降で使用できます。

トラフィック シェーピング

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

図 3-11 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 3-11　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

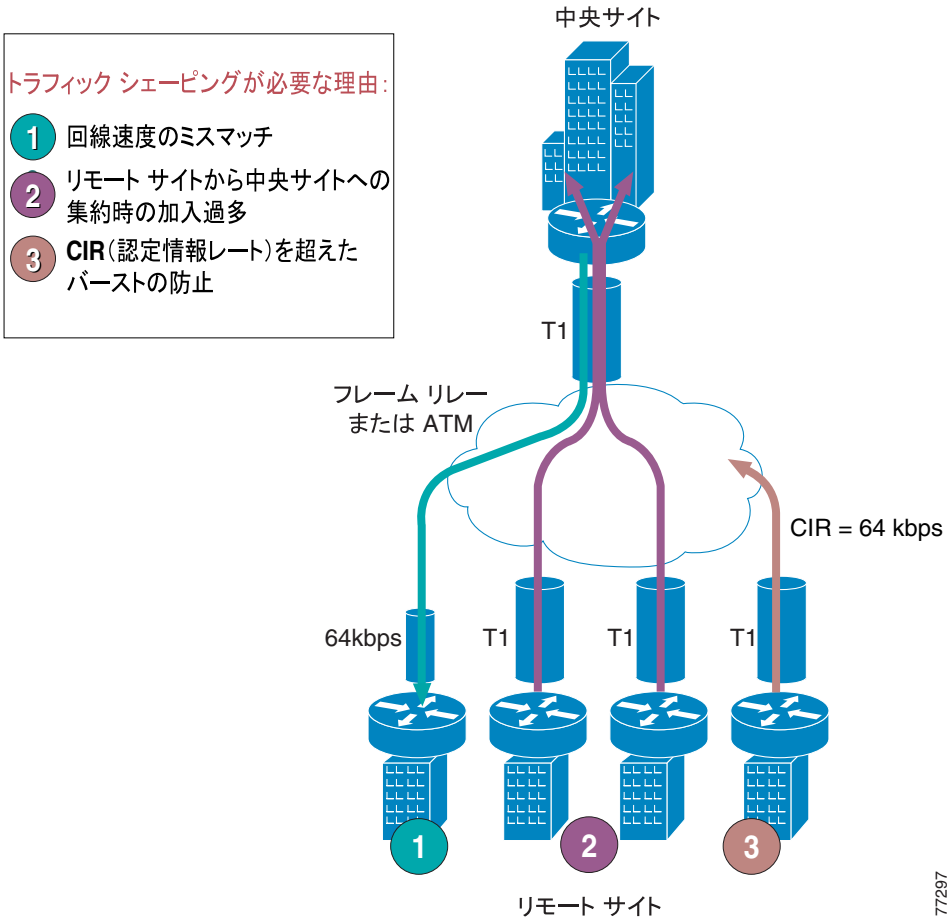


図 3-11 は、次の 3 つのシナリオを示しています。

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

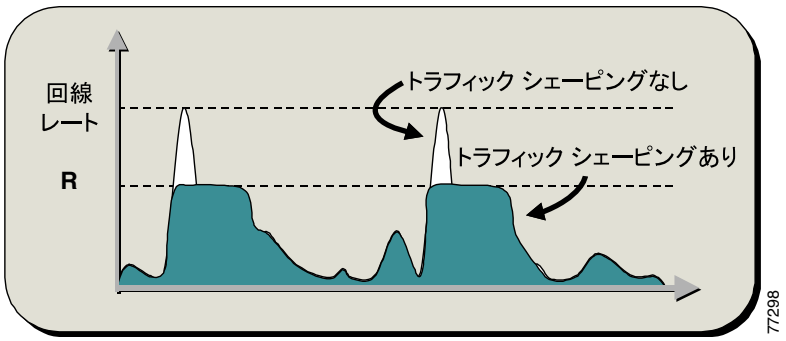
   複数のリモート サイトを 1 つの中央サイトに集約する場合、帯域幅をオーバーサブスクリプションにするのは、フレームリレーまたは ATM ネットワークでは一般的な方法です。たとえば、T1 インターフェイスで WAN に接続するリモート サイトが複数あるにもかかわらず、中央サイトには 1 つの T1 インターフェイスしかない場合があります。この設定により、配置されたネットワークは統計多重化による恩恵を受けますが、中央サイトのルータ インターフェイスが、トラフィックのバースト時に輻輳し、音声品質が低下することがあります。

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 3-12 は、このメカニズムを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 3-12　トラフィック シェーピングのメカニズム



Voice-Adaptive Traffic Shaping（VATS）

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

VATS を Voice-Adaptive Fragmentation（VAF）と組み合せて使用する場合（P.3-40 の「LFI（Link Fragmentation and Interleaving）」を参照）、インターフェイス上で音声アクティビティが検出されたときは、音声以外のトラフィックはすべてフラグメント化され、トラフィックはすべて WAN リンクの CIR に合せてシェーピングされます。

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

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

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

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 無線 IP Phone 7920 などの無線 IP テレフォニー エンドポイントが追加されている場合、音声トラフィックは WLAN 上に移動しているため、そこで既存のデータ トラフィックと共にコンバージされます。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.3-44）
- WLAN の QoS（P.3-50）

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

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

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

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

WLAN の設計と設定

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

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

- 無線インフラストラクチャに関する考慮事項（P.3-44）
- 無線 AP の設定と設計（P.3-48）
- 無線セキュリティ（P.3-49）

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.3-44）
- ローミング（P.3-45）
- 無線チャネル（P.3-45）
- 無線の干渉（P.3-47）
- WLAN 上のマルチキャスト（P.3-47）

VLAN

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

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

ローミング

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

デバイスがレイヤ 3 で移動する場合、デバイスは AP から別の AP に移動し、サブネットの境界を越えます。新しい Cisco Catalyst 6500 シリーズ ワイヤレス LAN サービス モジュール（WLSM）のリリースにより、Cisco 7920 無線 IP Phone では、スタティック WEP の使用中に、コールが存続可能なレイヤ 3 ローミングがサポートされるようになりました。Cisco Centralized Key Management（Cisco CKM）を使用すると、Cisco 7920 IP Phone は、LEAP の使用中に完全なレイヤ 3 モビリティを実現できます。Cisco WLSM の詳細については、次の Web サイトで入手可能な製品資料を参照してください。

http://www.cisco.com

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

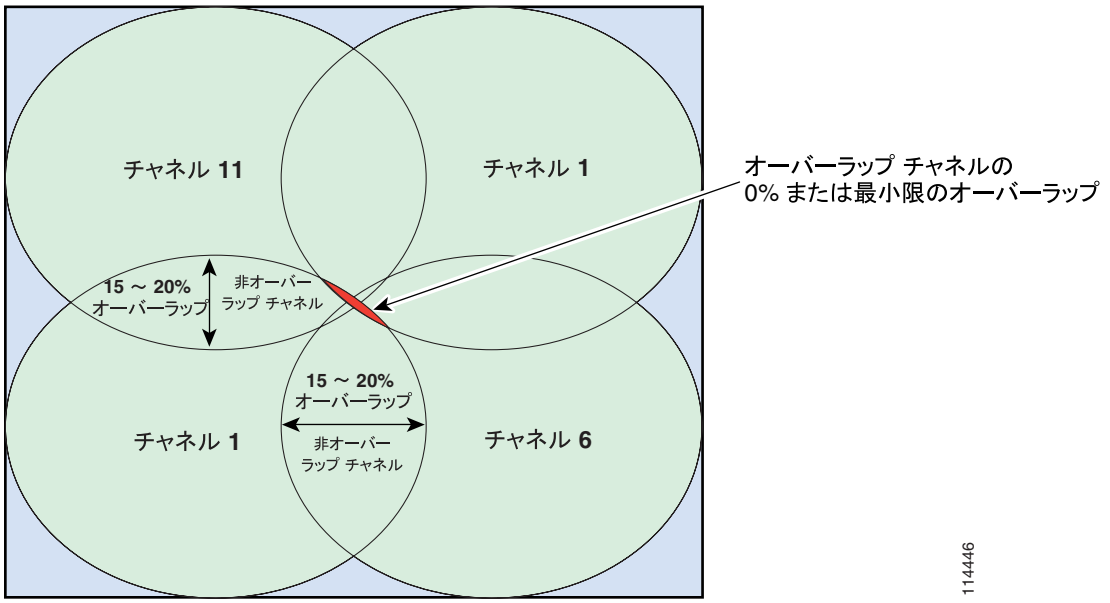
無線チャネル

無線エンドポイントと AP は、特定のチャネル上で無線を介して通信します。1 つのチャネル上で通信する場合、無線エンドポイントは、一般に、他の非オーバーラップ チャネル上で発生するトラフィックと通信を認識しません。2.4 GHz 802.11b 用のチャネル設定を最適化するには、5 チャネル広げて、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、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。欧州では、802.11b に使用可能な非オーバーラップ チャネルは、1 と 6 のほか、11、12、または 13 のいずれかです。日本では、これらのチャネルは、1 と 6 のほか、11、12、13、または 14 のいずれかです。

AP カバレッジは、同じチャネルに設定された AP 間で発生するオーバーラップが最小またはゼロになるように配置される必要があります（図 3-13 の Channel 1 を参照）。ただし、*非オーバーラップ* チャネル（北米では 1、6、および 11）上で適切な AP 配置およびカバレッジを実現するには、15 ～ 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

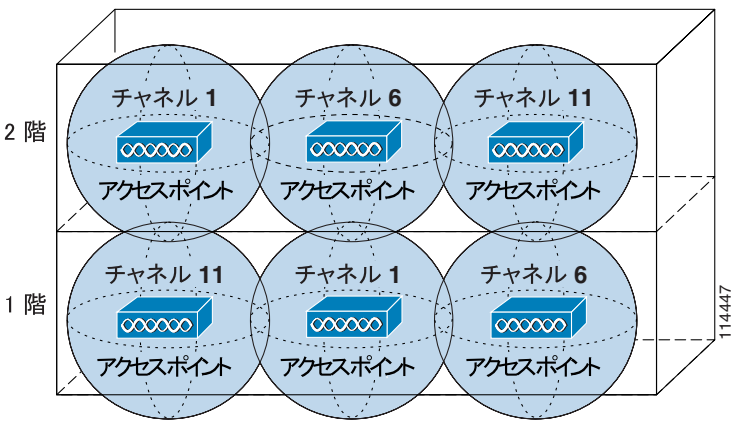
カバレッジ セルの間を移動するときにローミングが円滑に行われることが保証されます。オーバーラップが 15 ～ 20% を下回ると、ローミング時間が遅くなり、音声品質が低下する場合があります。一方、オーバーラップが 15 ～ 20% を超えると、ローミングが頻繁に、または常時行われる場合があります。図 3-13 は、オーバーラップ チャネルと非オーバーラップ チャネルの両方に適切な AP オーバーラップを示しています。

図 3-13　無線 802.11b チャネルのオーバーラップ



高層オフィスビルや病院など、多階の建物に無線デバイスを配置する場合は、無線 AP とチャネル カバレッジのプランニングに 3 つ目の次元が加わります。802.11b の 2.4 GHz 波形は、フロア、天井、および壁を通過できます。このため、同一フロア上のオーバーラップ セルまたはチャネルを考慮するだけでなく、隣接フロア間のチャネル オーバーラップを考慮する必要もあります。3 チャネルのみを使用する場合、適切なオーバーラップを実現する唯一の方法は、3 次元のプランニングを慎重に行うことです。図 3-14 は、802.11b 無線カバレッジを 3 次元の側面で考慮した場合の、チャネル オーバーラップの可能性を示しています。

図 3-14　無線 802.11b チャネルのオーバーラップに関する考慮事項（3 次元の場合）



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

無線の干渉

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

考えられる干渉源には、次のものがあります。

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

WLAN 上のマルチキャスト

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

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

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

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

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

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

無線 AP の設定と設計

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

AP の選択

無線音声を配置する場合は、次の AP を選択することをお勧めします。

- Aironet 350 シリーズ AP
- Aironet 1100 シリーズ AP
- Aironet 1200 シリーズ AP

これらの AP には、Cisco IOS Release 12.2(13)JA3 以降を使用する必要があります。無線音声を配置する場合、VxWorks オペレーティング システムを AP に使用することはお勧め*できません*。これは、VxWorks には新しい機能が追加されていませんが、音声の配置にはそれらの新しい機能の一部が必要となるためです。

AP の配置

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

AP の設定

無線音声を配置する場合は、特定の AP 設定に関する次の要件に従います。

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

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

- AP と無線音声エンドポイントの伝送パワーを一致させる

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

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

- データ レートを 11 Mbps に設定する

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

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

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

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

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

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

  この機能を使用すると、AP がビーコンで QoS Basic Service Set（QBSS）情報要素を提供することが保証されます。QBSS 要素は、AP でのチャネル使用率の推計を示します。また、QBSS 要素を使用することにより、Cisco 無線音声デバイスは、ローミングに関する決定を下し、負荷が高すぎる場合にコール試行を拒否することができます。

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

  音声ポリシーとデータ ポリシーに各 VLAN のデフォルトの分類を設定することで、音声トラフィックがプライオリティ キューイング処理されることを保証します（詳細については、P.3-51 の「インターフェイス キューイング」を参照）。

無線セキュリティ

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

- Cisco LEAP

  Cisco LEAP は、ネットワークに対して認証するためのユーザ名とパスワードを、無線エンドポイントに要求します。この認証が行われると、動的な鍵が生成され、無線デバイスとの間で送受信されるトラフィックが暗号化されます。この方法には、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、無線デバイスを認証するためのユーザ データベースにアクセスします。Cisco LEAP は、Voice VLAN へのアクセスに対して最高レベルのセキュリティを要求するため、無線音声での使用に推奨されるセキュリティ メカニズムです。

- スタティック Wire Equivalent Privacy（WEP）

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

- Open 認証

  この方法では、認証は要求されず、無線エンドポイント デバッグと無線ネットワークの間を移動するトラフィックはセキュリティで保護されません。この方法では、無線デバイスに、無線デバイスの接続先となる無線 VLAN 用の適切な SSID を設定するだけで済みます。この方法を無線音声に使用することは原則としてお勧めできません。これは、Voice VLAN へのアクセスに対して認証が要求されず、音声トラフィックが暗号化されないためです。

Cisco LEAP 認証と ACS 配置モデル

これまで説明したように、Cisco LEAP 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 Cisco LEAP を配置する場合は、ネットワーク内の ACS の配置を慎重に検討して、次の ACS 配置モデルのいずれかを選択します。

- 集中型 ACS

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

- リモート ACS

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

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

  リモート ロケーションが低速 WAN リンクを介して中央サイトから分離しているネットワークでは、ローカルの無線デバイスがローカル Cisco IOS AP に対して認証できます。Cisco IOS Release 12.2(11)JA 以降を実行する AP では、外部 ACS を利用しないでローカルに Cisco LEAP 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.3-51）
- インターフェイス キューイング（P.3-51）
- 帯域幅のプロビジョニング（P.3-52）

トラフィック分類

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

Cisco 無線 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 26（または PHB AF31）でマークします。このトラフィックをマークしたら、ネットワーク全体でプライオリティ処理およびキューイング、またはベストエフォート型よりも優れた処理およびキューイングを行うことができます。無線音声デバイスはすべて、この方法でトラフィックをマークできる必要があります。無線ネットワーク上の他のトラフィックはすべて、ベストエフォート型としてマークされるか、有線ネットワークのマーキング ガイドラインで規定されているいくつかの中間分類を使用してマークされる必要があります。

インターフェイス キューイング

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

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

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

この 2 つのキューを設定するには、AP 上に 2 つの QoS ポリシーを作成します。1 つ目のポリシーには **voice** という名前を付け、**Default Classification for all packets on the Vlan** として **Voice <10 ms Latency (6)** サービス クラスを設定します。2 つ目のポリシーには **data** という名前を付け、**Default Classification for all packets on the Vlan** として **Best Effort (0)** サービス クラスを設定します。次に、**data** ポリシーをデータ VLAN の着信および発信無線インターフェイスに割り当て、**voice** ポリシーを Voice VLAN の着信および発信無線インターフェイスに割り当てます。QoS ポリシーを VLAN レベルで適用すると、AP が着信または発信するすべてのパケットを検査して、パケットに適用する

必要があるキューイングのタイプを判別することはなくなります。この設定にすると、ダウンストリーム方向のすべての音声メディアおよびシグナリングがプライオリティ キューイング処理されることが保証されます。

帯域幅のプロビジョニング

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

トラフィック バーストによって過剰なトラフィックが AP に送信されることを許可しても、結局は AP でドロップされるため、代わりに、レート制限または規制によってこのトラフィックを無線ネットワークで処理できるレートに抑えることをお勧めします。AP で過剰なトラフィックをドロップさせると、AP での CPU 使用率と輻輳が増加します。代わりに、有線アクセス レイヤ スイッチと無線 AP 間のリンク上でトラフィック レートを 7 Mbps に制限すると、トラフィックがアクセス レイヤ スイッチでドロップされることが保証されるため、AP の負荷がなくなります。AP に送信されるトラフィックのレート制限の詳細については、P.17-31 の「Cisco 無線 IP Phone 7920」の項にある QoS の推奨事項を参照してください。無線ネットワークの配置によっては、実質的なスループットが 7 Mbps を下回ることがあります。特に、単一の AP に関連付けられたデバイスの数が推奨値より多い場合に該当します。

シスコでは、無線音声ネットワークのテストに基づいて、単一の無線 AP で最大 7 つの G.711 音声コールまたは最大 8 つの G.729 音声コールをサポートできることを確認しています。これらの制限を超えると、音声品質が低下し、場合によっては音声コールがドロップされます。音声トラフィックの無線帯域幅をプロビジョニングするのに最適なコール アドミッション制御のメカニズムまたは方式はありませんが、Cisco 7920 無線 IP Phone では、ネットワーク上の AP から受信するチャネル使用率の情報に基づいた、コール アドミッション制御または帯域幅プロビジョニングの簡易バージョンを使用できます。この情報は、QoS Basic Service Set（QBSS）を含むビーコンを介して、AP から電話機に送信できます。QBSS は、その AP による RF チャネルの使用率の推計を示します。QBSS 要素の値が大きいほど、チャネル使用率が高くなり、チャネルと AP が追加の無線音声デバイスに対して十分な帯域幅を提供できる可能性が低くなります。QBSS 要素の値が 45 以上の場合、無線 IP Phone によって試行されるコールはすべて拒否され、「Network Busy」メッセージ、ファースト ビジー音、またはその両方が示されます。また、無線 IP Phone は、そのローミング アルゴリズムで QBSS 要素を検討し、QBSS 要素が 45 以上のビーコンを送信する AP には移動しません。

（注） QBSS 値は、特定の AP におけるチャネル使用率の推計にすぎません。実際のチャネル使用率は、示された値よりもはるかに高い場合があります。このため、上限の 7 または 8 コールにすでに到達していても、引き続きその AP 上で無線音声デバイスから音声コールを発信できる場合があります。その場合は、コールがドロップされたり、音声品質が低下したりします。

QBSS 情報要素が AP から送信されるのは、AP 上で **QoS Element for Wireless Phones** が有効になっている場合のみです（P.3-48 の「無線 AP の設定と設計」を参照）。

CHAPTER 4

音声ゲートウェイ

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

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

Cisco ゲートウェイの概要

Cisco アクセス ゲートウェイにより、Cisco CallManager は IP 以外の通信デバイスと情報を交換できます。Cisco アクセス ゲートウェイには、アナログとデジタルの 2 種類があります。

Cisco アクセス アナログ ゲートウェイ

Cisco アクセス アナログ ゲートウェイには、トランク ゲートウェイとステーション ゲートウェイの 2 つのカテゴリがあります。

- アクセス アナログ ステーション ゲートウェイ

  アナログ ステーション ゲートウェイは、Cisco CallManager を POTS（Plain Old Telephone Service; 一般電話サービス）のアナログ電話機、IVR（Interactive Voice Response; 音声自動応答装置）システム、FAX マシン、およびボイスメール システムに接続します。ステーション ゲートウェイは、FXS（Foreign Exchange Station）ポートを備えています。

- アクセス アナログ トランク ゲートウェイ

  アナログ トランク ゲートウェイは、Cisco CallManager を公衆網セントラル オフィス（CO）または PBX トランクに接続します。トランク ゲートウェイは、公衆網、PBX、またはキー システムへのアクセス用の FXO（Foreign Exchange Office）ポート、および従来型の PBX とのアナログ トランク接続用の E&M（recEive and transMit、または ear and mouth）ポートを備えています。応答と接続解除の監視の問題を最小限に抑えるために、可能な限り、デジタル ゲートウェイを使用してください。アナログ Direct Inward Dialing（DID; ダイヤルイン方式）および Centralized Automatic Message Accounting（CAMA）も、公衆網接続に使用できます。

Cisco アクセス デジタル トランク ゲートウェイ

Cisco アクセス デジタル トランク ゲートウェイは、PRI（一次群速度インターフェイス）、Basic Rate Interface（BRI; 基本速度インターフェイス）、または T1 CAS（チャネル連携信号）などのデジタル トランクを経由して、Cisco CallManager を公衆網または PBX に接続します。デジタル T1 PRI トランクは、所定の従来型ボイスメール システムとの接続にも使用できます。

ゲートウェイの選択

IP テレフォニー ゲートウェイを選択する場合は、次の点を考慮してください。

コア機能要件

IP テレフォニー アプリケーションで使用するゲートウェイは、次のコア機能要件を満たす必要があります。

- DTMF（Dual tone multifrequency）リレー機能

  DTMF リレー機能、特にアウトバンド DTMF は、DTMF ディジットを音声ストリームから切り離し、音声ストリームまたはベアラ トラフィックの一部としてではなく、ゲートウェイ プロトコル（H.323、SCCP、または MGCP）シグナリング チャネルを通じて、シグナリング標識として送信します。音声圧縮に低ビット レート コーデックを使用する場合、DTMF 信号の損失また歪みの可能性があるので、アウトバンド DTMF が必要です。

- 補足サービス サポート

  補足サービスは、一般に、保留、転送、および会議などの基本的なテレフォニー機能です。

- FAX/ モデム サポート

  FAX over IP により、従来のアナログ FAX マシンと IP テレフォニー ネットワークとの相互運用性が可能になります。FAX イメージは、アナログ信号から変換され、パケット ネットワークを介してデジタル データとして伝送されます。詳細については、P.4-19 の「FAX とモデムのサポート」を参照してください。

- Cisco CallManager 冗長性サポート

  Cisco IP テレフォニーは、分散モデルに基づき、高いアベイラビリティを確保しています。Cisco CallManager クラスタには、Cisco CallManager の冗長性が用意されています。ゲートウェイは、プライマリ Cisco CallManager に障害が発生した場合に、セカンダリ Cisco CallManager に「re-home」機能をサポートする必要があります。冗長性は、Cisco CallManager またはネットワークの障害時のコール存続可能性とは異なります。

企業での配置用に選択する IP テレフォニー ゲートウェイがすべて、上記のコア要件を満たしていることを確認するには、ゲートウェイ製品の資料を参照してください。さらに、どの IP テレフォニーの実装についても、各サイト特有の機能要件（たとえば、アナログまたはデジタル アクセス、DID、およびキャパシティ要件）があります（P.4-11 の「サイト固有のゲートウェイ要件」を参照してください）。

ゲートウェイ プロトコル

Cisco CallManager（Release 3.1 およびそれ以降）では、次のゲートウェイ プロトコルがサポートされています。

- H.323
- メディア ゲートウェイ コントロール プロトコル（MGCP）

Cisco IP Phone は、超軽量プロトコルである SCCP を使用します。SCCP はマスター / スレーブ モデルを使用しますが、H.323 は、ピアツーピア モデルです。MGCP も、マスター / スレーブ モデルを使用します。

プロトコルの選択は、サイト特有の要件と機器の設置ベースによって決まります。たとえば、リモート サイトである支店の大部分のロケーションには、Cisco 2600XM または 3700 シリーズ 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 CallManager Release 3.1 以降で、H.323 と MGCP 0.1 をサポートします。ゲートウェイの設定では、MGCP が H.323 より優先されます。これは、設定が簡単であり、プライマリからセカンダリの Cisco CallManager に Cisco CallManager をフェールオーバーするときに、コールが切断されずに保持されるからです。一方、サポートされるインターフェイスの堅牢性により、H.323 が MGCP より優先される場合もあります。

SMDI（Simplified Message Desk Interface）は、ボイスメール システムを PBX または Centrex システムに統合するための標準です。SMDI を介してボイスメール システムに接続し、アナログ FXS またはデジタル T1 PRI を使用するには、SCCP または MGCP プロトコルが必要です。これは、H.323 デバイスは、ポートのグループから、使用される特定の回線を識別しないからです。この目的に H.323 ゲートウェイを使用すると、Cisco Message Interface は、着信コールに使用される実際のポートまたはチャネルと、SMDI 情報とを正常に相関させることができません。

また、使用される Cisco CallManager の配置モデルも、ゲートウェイ プロトコルの選択に影響を与える場合があります（第 2 章「IP テレフォニー配置モデル」を参照してください）。

表 4-1 では、どのゲートウェイが所定のプロトコルをサポートするかを示しています。これらのプロトコルはそれぞれ、コア ゲートウェイ要件をサポートするために多少異なる方法を使用します。P.4-6 の「ゲートウェイ プロトコルとコア機能要件」では、各プロトコルがこれらの機能要件をどのように満たしているかを説明します。

表 4-1　サポートされるゲートウェイ プロトコルと Cisco IP テレフォニー ゲートウェイ

Cisco ゲートウェイ	MGCP 0.1	H.323	SCCP
VG200[1]	あり サポート対象 : • アナログ FXS/FXO • T1 CAS（E&M Wink Start; Delay Dial のみ） • T1/E1 PRI	あり	あり（DSP ファーム）
VG224	あり、FXS のみ Cisco IOS Release 12.3(T) 以降では、VG224 の会議とトランスコーディングもサポート	あり、FXS のみ	あり、Cisco IOS Release 12.4(2)T 以降
VG248	なし	なし	あり[2]
DE-30+、DT-24+[3]	あり	なし	なし
Cisco 827-V4	なし	あり、FXS に対してサポート	なし
Cisco ATA 188	あり、FXS のみ	あり、FXS のみ	あり、FXS のみ
Cisco 1751 および 1760	あり	あり	あり、会議およびトランスコーディング

表 4-1　サポートされるゲートウェイ プロトコルと Cisco IP テレフォニー ゲートウェイ（続き）

Cisco ゲートウェイ	MGCP 0.1	H.323	SCCP
Cisco 2600 および 2600XM[4]	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
Cisco 2800	あり、Cisco IOS Release 12.3.8T4 以降	あり、Cisco IOS Release 12.3.8T4 以降	あり、Cisco IOS Release 12.3.8T4 以降
Cisco 3640 および 3660	あり サポート対象 : • アナログ FXS/FXO • T1 CAS（E&M Wink Start; Delay Dial のみ） • T1/E1 PRI	あり	Cisco IOS Release 12.2.13T の DSP ファーム
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
Cisco 3800	あり、Cisco IOS Release 12.3.11T 以降	あり、Cisco IOS Release 12.3.11T 以降	あり、Cisco IOS Release 12.3.11T 以降
Cisco 5300	なし	あり	なし
Cisco AS5350 Cisco AS5400	なし	あり	なし
Cisco AS5850	なし	あり	なし
Cisco 7200	なし	あり	なし
Catalyst 4000 WS-X4604-GWY ゲートウェイ モジュール	あり	あり	なし
Catalyst 6000 WS-X6608-x1 ゲートウェイ モジュール および FXS モジュール WS-X6624	あり サポート対象 : • T1 CAS FXS • T1/E1 PRI • FXS with WS-6624	なし	なし

表 4-1　サポートされるゲートウェイ プロトコルと Cisco IP テレフォニー ゲートウェイ（続き）

Cisco ゲートウェイ	MGCP 0.1	H.323	SCCP
Communication Media Module（CMM; コミュニケーション メディア モジュール） 24FXS	あり サポート対象 : • T1 CAS FXS • T1/E1 PRI • FXS	あり	なし
Cisco ICS7750-MRP	なし	あり	なし
Cisco ICS7750-ASI	なし	あり	なし

1. VG200 は、Cisco 2610XM ルータに置き換えられたので、販売終了になりました。VG200 の既存のモデルは、引き続き IP テレフォニー設置環境でご使用いただけます。
2. VG248 は、H.323 または MGCP ではなく、SCCP を使用するので、真のゲートウェイではありません。
3. これらのモデルは、製造中止になりました。
4. IP テレフォニー アプリケーションには、Cisco 2600XM ルータを使用してください。Cisco 2600 ルータのメモリの考慮事項については、次の Web サイトの製品情報をご覧ください。http://www.cisco.com/warp/customer/cc/pd/rt/2600/prodlit/1675_pp.htm

（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、および MGCP）が次のゲートウェイ機能要件をどのようにサポートするかについて説明します。

- DTMF リレー（P.4-6）
- 補足サービス（P.4-7）
- Cisco CallManager の冗長性（P.4-10）

DTMF リレー

DTMF（Dual-Tone Multifrequency）は、信号に音声帯域内の特定の周波数ペアを使用するシグナリング方式です。64 kbps の PCM（パルス符号変調）音声チャネルは、これらの信号を容易に伝送できます。しかし、音声圧縮に低ビット レート コーデックを使用する場合、DTMF 信号の損失または歪みの可能性があります。VoIP（Voice over IP）インフラストラクチャを介して DTMF トーンを伝送するアウトバンド シグナリング方式は、コーデックにより誘発されるこれらの症状を簡単に解決します。

SCCP ゲートウェイ

Cisco VG248 などの SCCP ゲートウェイは、伝送制御プロトコル（TCP）ポート 2002 を使用して、DTMF 信号をアウトバンドで伝送します。アウトバンド DTMF は、VG248 用のデフォルトのゲートウェイ設定モードです。

H.323 ゲートウェイ

Cisco 3700 シリーズ製品などの H.323 ゲートウェイは、DTMF 信号をアウトバンドで交換するための拡張 H.245 機能を使用して、Cisco CallManager と情報を交換できます。次の例は、Cisco IOS ゲートウェイ上のアウトバンド DTMF 設定例です。

```
dial-peer voice 100 voip
destination-pattern 555….
session target ipv4:10.1.1.1
CODEC g729ar8
dtmf-relay h245-alphanumeric
preference 0
```

MGCP ゲートウェイ

Cisco IOS ベースの VG224、2600XM、2800、3700、および 3800 プラットフォームは、Cisco CallManager との通信に MGCP を使用します。MGCP プロトコルには、パッケージの概念があります。MGCP ゲートウェイは、始動後、DTMF パッケージをロードします。MGCP ゲートウェイは、制御チャネルを介して、受信した DTMF トーンを表すシンボルを送信します。次に、Cisco CallManager は、これらの信号を解釈し、アウトバンドでシグナリング エンドポイントに DTMF 信号を渡します。DTMF リレーのグローバル設定コマンドは、次のとおりです。

```
mgcp dtmf-relay CODEC all mode out-of-band
```

Cisco CallManager MGCP ゲートウェイ設定インターフェイスで、追加の設定パラメータを入力する必要があります。

Catalyst 6000、DE-30+、および DT-24+ はすべて、Cisco CallManager Release 3.1 以降で MGCP をサポートします。デフォルトで DTMF リレーは使用可能であり、追加の設定は必要ありません。

補足サービス

補足サービスは、保留、転送、および会議などのユーザ機能を提供します。これらのサービスは、音声通信の確立の基本的な要件であると見なされます。IP テレフォニー ネットワークでの使用について評価される各ゲートウェイは、ソフトウェアの MTP（メディア ターミネーション ポイント）を使用しなくても、独自に補足サービスをサポートする必要があります。

SCCP ゲートウェイ

Cisco VG224、VG248、および ATA 188 ゲートウェイは、補足サービスを完全にサポートしています。SCCP ゲートウェイは、ゲートウェイと Cisco CallManager 間のシグナリング チャネル、および SCCP を使用して、コール制御パラメータを交換します。

H.323 ゲートウェイ

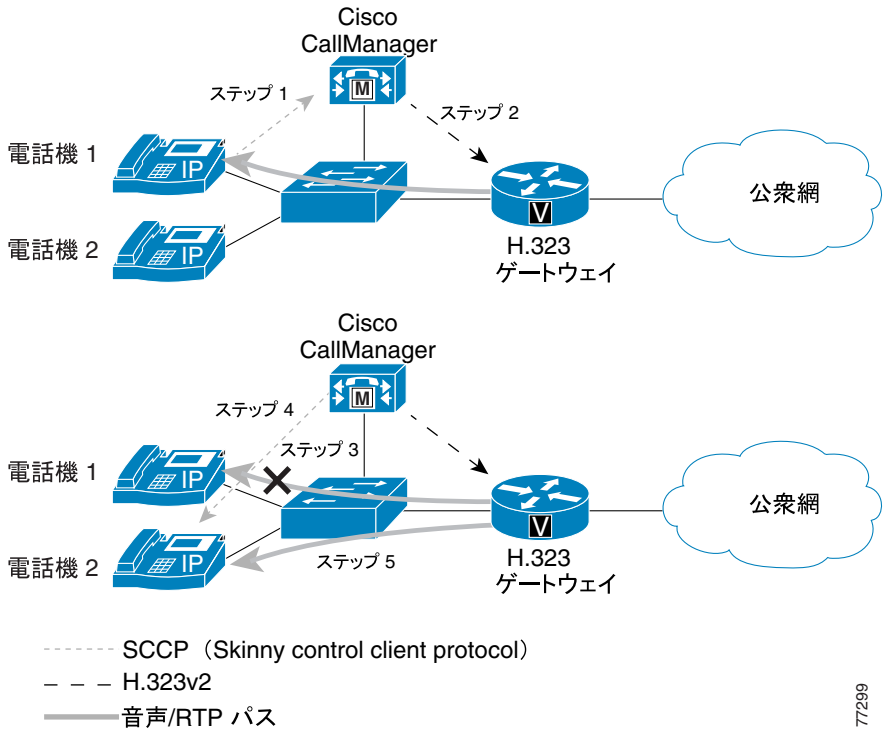
H.323v2 は、Open/Close LogicalChannel 機能と emptyCapabilitySet 機能を実行します。Cisco IOS Release 12.0(7)T および Cisco CallManager Release 3.0 以降から始まった、H.323 ゲートウェイによる H.323v2 の使用により、MTP が補足サービスを提供する必要がなくなりました。Cisco CallManager Release 3.1 以降では、トランスコーダが動的に割り当てられるのは、G.711 専用デバイスへのアクセスを提供すると同時に、WAN を介した G.729 ストリームを保持するために、コール中に必要な場合だけです。H.323v2 に対するフル サポートは、Cisco IOS Release 12.1.1T で利用可能です。

Cisco CallManager を H.323 プロキシとして使用して、Cisco IOS ゲートウェイと IP Phone 間で H.323v2 コールがセットアップされた後は、その IP Phone は、ベアラ接続の変更を要求できます。RTP（Real-Time Transport Protocol）ストリームは、Cisco IOS ゲートウェイから IP Phone に直接接続されるので、サポートされる音声コーデックをネゴシエートできます。

図 4-1 と次の手順では、2 台の IP Phone 間のコール転送を示しています。

1. IP Phone 1 が Cisco IOS ゲートウェイから Phone 2 にコールを転送しようとする場合、Phone 1 は、SCCP を使用して Cisco CallManager に転送要求を出します。
2. Cisco CallManager は、この要求を H.323v2 CloseLogicalChannel 要求に変換して、Cisco IOS ゲートウェイに送信して、適切な SessionID を求めます。
3. Cisco IOS ゲートウェイは、Phone 1 との RTP チャネルをクローズします。
4. Cisco CallManager は、SCCP を使用して、Cisco IOS ゲートウェイとの RTP 接続をセットアップする要求を、Phone 2 に出します。同時に、Cisco CallManager は、新しい宛先パラメータを指定して（ただし、同じ SessionID を使用）、Cisco IOS ゲートウェイに OpenLogicalChannel 要求を出します。
5. Cisco IOS ゲートウェイがこの要求を確認した後、RTP 音声ベアラ チャネルが、Phone 2 と Cisco IOS ゲートウェイとの間で確立されます。

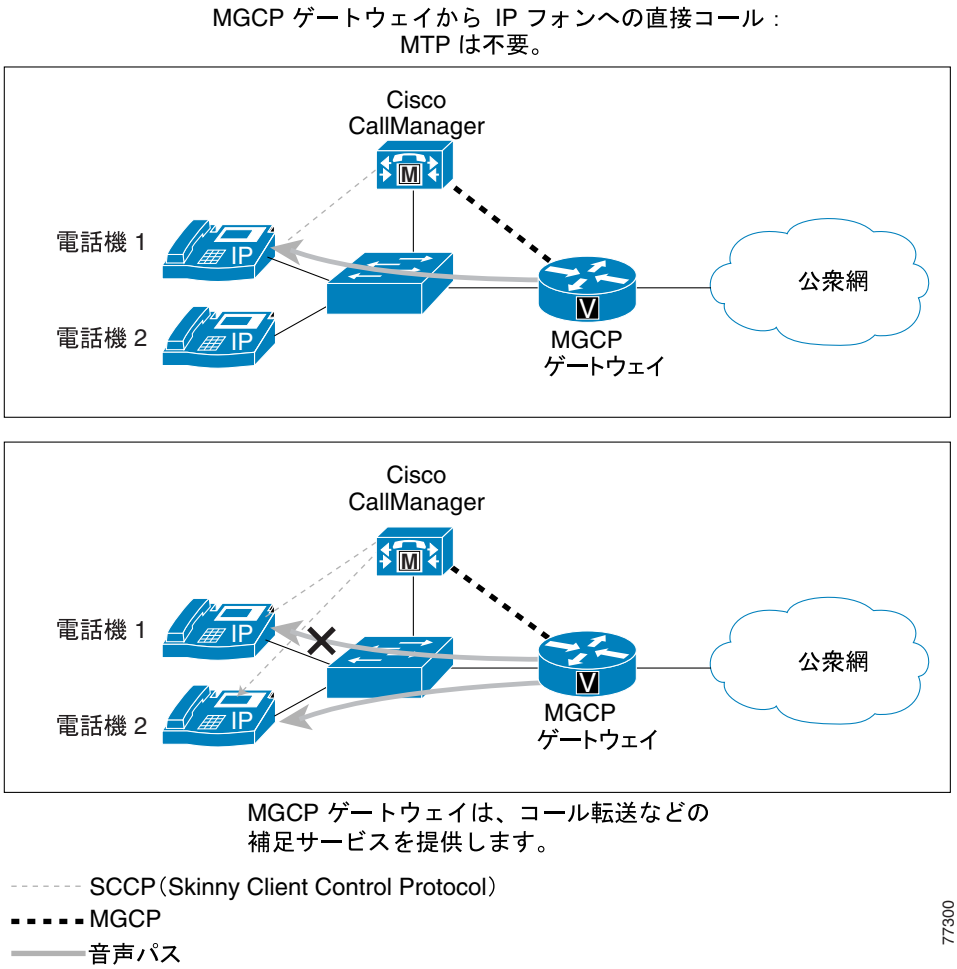
図 4-1　H.323 ゲートウェイの補足サービス サポート



MGCP ゲートウェイ

MGCP ゲートウェイは、MGCP プロトコルを使用して、保留、転送、および会議機能を完全にサポートします。MGCP プロトコルは、すべてのセッション機能を制御する、Cisco CallManager とのマスター / スレーブ プロトコルであるので、Cisco CallManager は、MGCP ゲートウェイの音声接続を容易に操作できます。IP テレフォニー エンドポイント（たとえば、IP Phone）が、セッションの変更（たとえば、コールを別のエンドポイントに転送する）を必要とする場合、そのエンドポイントは、セッションの変更を SCCP を使用して Cisco CallManager に通知します。次に、Cisco CallManager は、Session ID に関連した現在の RTP ストリームを終了し、新しいエンドポイント情報を使用して新しいメディア セッションを開始することを、MGCP UDP（ユーザ データグラム プロトコル）制御接続を使用して、MGCP ゲートウェイに通知します。図 4-2 では、プロトコルが MGCP ゲートウェイ、エンドポイント、および Cisco CallManager 間で交換される様子を示しています。

図 4-2　MGCP ゲートウェイの補足サービス サポート



Cisco CallManager の冗長性

IP テレフォニー アーキテクチャの必須部分は、高価な専有の従来型の PBX システムの代わりに、低コストの分散型 PC ベース システムを提供することです。この分散型設計は、クラスタ化された Cisco CallManager の堅固なフォールト トレラント アーキテクチャに適しています。最も単純な形式（2 システムのクラスタ）であっても、セカンダリ Cisco CallManager は、最初にプライマリ Cisco CallManager によって管理されていたすべてのゲートウェイの制御権を引き受ける必要があります。

SCCP ゲートウェイ

ブート後、Cisco VG224、VG248 および ATA 188 ゲートウェイには、Cisco CallManager サーバ情報が提供されます。これらのゲートウェイが初期設定されるときに、Cisco CallManager のリストがゲートウェイにダウンロードされます。このリストでは、プライマリ Cisco CallManager とセカンダリ Cisco CallManager に優先順位が付けられています。プライマリ Cisco CallManager が通信不能になった場合、ゲートウェイは、セカンダリ Cisco CallManager に登録されます。

H.323 ゲートウェイ

Cisco H.323 ゲートウェイは、Cisco IOS Release 12.1(2)T における **dial-peer** コマンドと **voice class** コマンドの複数の拡張機能を使用して、冗長 Cisco CallManager をサポートします。新しいコマンド **H.225 tcp timeout <seconds>** が追加されました。このコマンドは、H.323 ゲートウェイが、H.323 コール セットアップ用の H.225 制御接続の確立に要する時間をトラッキングします。H.323 ゲートウェイがプライマリ Cisco CallManager との H.225 接続を確立できない場合、別の **dial-peer** ステートメントで指定されるセカンダリ Cisco CallManager との接続を試行します。H.323 ゲートウェイは、次に高い **preference** 設定を指定する **dial-peer** ステートメントに移ります。次のコマンドを使用すると、H.323 ゲートウェイに対して Cisco CallManager の冗長性を設定できます。

```
dial-peer voice 101 voip
  destination-pattern 1111
  session target ipv4:10.1.1.101
  preference 0
  voice class h323 1
dial-peer voice 102 voip
  destination-pattern 1111
  session target ipv4:10.1.1.102
  preference 1
  voice class h323 1
voice class h323 1
  h225 tcp timeout <1-30 sec>
```

（注） Cisco CallManager　の冗長性は、コールの存続可能性を意味するものではありません。プライマリ Cisco CallManager に障害が起きると、IP Phone と、H.323 ゲートウェイを介して接続されている電話機との間のすべてのコールが終了します。

MGCP ゲートウェイ

MGCP ゲートウェイには、プライマリ Cisco CallManager との通信が失われた場合に、セカンダリ Cisco CallManager にフェールオーバーする機能もあります。フェールオーバーが起きても、アクティブ コールは保持されます。

MGCP ゲートウェイのコンフィギュレーション ファイル内で、プライマリ Cisco CallManager は、**call-agent <hostname>** コマンドを使用して指定され、セカンダリ Cisco CallManager のリストは、**ccm-manager redundant-host** コマンドを使用して追加されます。プライマリ Cisco CallManager との

キープアライブは、MGCP アプリケーション レベルのキープアライブ メカニズムを通じて行われます。このメカニズムでは、MGCP ゲートウェイは、空の MGCP notify（NTFY）メッセージを Cisco CallManager に送信し、確認応答を待ちます。バックアップ Cisco CallManager とのキープアライブは、TCP キープアライブ メカニズムを介して行われます。

プライマリ　Cisco CallManager　が後で使用可能になると、MGCP　ゲートウェイは、元の Cisco CallManager に「戻る」、つまり復帰できます。この復帰は、ただちに行われることもあれば、設定可能な時間が経過した後、または接続されているすべてのセッションが解除された後に行われることもあります。これは、次のグローバル設定コマンドを使用して使用可能になります。

```
ccm-manager redundant-host <hostname1 | ipaddress1 > <hostname2 | ipaddress2>
[no] call-manager redundancy switchback [immediate|graceful|delay <delay_time>]
```

サイト固有のゲートウェイ要件

IP テレフォニーの実装にはそれぞれ、サイト固有の要件があります。次の質問は、IP テレフォニー ゲートウェイの選択に役立ちます。

- 公衆網（または PBX）アクセスは、アナログですか、デジタルですか。
- 公衆網または PBX には、どのタイプのアナログ（FXO、FXS、E&M、DID、CAMA）インターフェイス、またはデジタル（T1、E1、CAS、CCS）インターフェイスが必要ですか。
- 公衆網アクセスがデジタルである場合、どのタイプのシグナリングが必要ですか（T1　CAS、Q.931 PRI、E1 CAS、または R2）。
- PBX は、現在どのタイプのシグナリングを使用していますか。
  - FXO または FXS: ループ スタートまたはグラウンド スタート
  - E&M: ウィンク スタート、遅延スタート、または即時スタート
  - E&M: タイプ I、II、III、IV、または V
  - T1:CAS、Q.931 PRI（ユーザ側またはネットワーク側）、QSIG、DPNSS、または Proprietary D チャネル（CCS）シグナリング
  - E1:CAS、R2、Q.931 PRI（ユーザ側またはネットワーク側）、QSIG、DPNSS、Proprietary D チャネル（CCS）シグナリング
- PBX は、現在どのタイプのフレーム同期（SF、ESF、または G.704）と回線エンコーディング（B8ZS、AMI、CRC-4、または HDB3）を使用していますか。
- PBX に、専有シグナリングを渡す必要がありますか。必要な場合、そのシグナリングはどのタイムスロットで渡されますか。それは HDLC フレームですか。
- ゲートウェイにどれくらいのキャパシティが必要ですか。つまり、チャネルがいくつ必要ですか（一般に、音声チャネルが 12 本以上必要な場合は、デジタルの方が、アナログ ソリューションより費用対効果が高くなります）。
- ダイヤルイン方式（DID）が必要ですか。必要な場合は、アナログか、デジタルかを指定してください（日本ではアナログ DID 未対応）。
- 発呼回線 ID（CLID）が必要ですか。
- 発信者名が必要ですか。
- どのタイプの FAX およびモデム サポートが必要ですか。
- どのタイプの音声圧縮が必要ですか。
- どのタイプの補足サービスが必要ですか。
- PBX はクロッキングをサポートしますか。または PBX は、Cisco ゲートウェイがクロッキングをサポートすることを期待しますか。
- 必要なすべてのゲートウェイ、ルータ、およびスイッチを収容するラック スペースがありますか。

(注)　ダイヤルイン方式（DID）とは、オペレータが介在しなくても、外部コールを直接、端末回線に着信できるようにする PBX（構内交換機）またはセントレック（Centrex）機能のことです。

(注)　発呼回線 ID（CLI、CLID、または ANI）とは、着呼側に対して発信番号を表示する、デジタル電話ネットワークで利用可能なサービスを指します。セントラル オフィス機器は、発信者の電話番号を識別し、発信者についての情報をコール自体と一緒に送信できるようにします。CLID は、ANI（Automatic Number Identification; 自動番号識別）と同義です。

Cisco IP テレフォニー ゲートウェイは、大部分の主要 PBX ベンダー製品と相互運用でき、EIA/TIA-464B に準拠しています。

可能な選択肢を絞り込むには、サイト固有およびコアのゲートウェイ要件から始めるのが適しています。必要な機能を指定した後、該当する設定ごとに、企業における規模と複雑さが異なる単一サイトの配置であるか、マルチサイトによる配置であるかに関係なく、ゲートウェイの選択を行うことができます。

次の表では、さまざまな Cisco ゲートウェイ モデルによってサポートされる機能とインターフェイス タイプをまとめています。

(注)　次の表では、Cisco IOS および Cisco CallManager のリリース番号は、リストされている機能を特定のゲートウェイ プラットフォーム上でサポートできるようになったリリースを指しています。ハードウェア プラットフォームごとの推奨ソフトウェア リリースの推奨事項については、次の Web サイトの資料を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

Cisco アナログ ゲートウェイ

表 4-2 では、H.323 または SIP（Session Initiation Protocol）を使用する Cisco アナログ ゲートウェイに対してサポートされているインターフェイス タイプをリストしています。表 4-3 では、メディア ゲートウェイ コントロール プロトコル（MGCP）を使用する Cisco アナログ ゲートウェイに対してサポートされている、インターフェイス タイプをリストしています。

表 4-2　サポートされるアナログ H.323 および SIP 機能

	インターフェイス タイプ					
Cisco ゲートウェイ	**FXS**	**FXO**	**E&M**	**FXO、バッテリ リバーサル**	**アナログ DID**	**CAMA 911**
Analog Telephone Adapter（ATA）	あり	なし	なし	なし	なし	なし
827-4V	あり	なし	なし	なし	なし	なし
1751 および 1760	あり	あり	あり	あり	あり	あり
VG200	あり	あり	あり	なし	あり	なし
VG248	なし	なし	なし	なし	なし	なし
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
2600 シリーズ	あり	あり	あり	あり	あり	12.2.11T

表 4-2　サポートされるアナログ H.323 および SIP 機能（続き）

	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**
2800 シリーズ	あり	あり	あり	あり	あり	あり
3600 シリーズ	あり	あり	あり	あり	あり	12.2.11T
3700 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
ICS 7750	あり	あり	あり	あり	あり	なし
Catalyst 4000 Access Gateway Module（AGM）	あり	あり	なし	なし	なし	なし
6608 および 6624	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
コミュニケーション メディア モジュール（CMM）24FXS	あり	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
7x00 ファミリー	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外

表 4-3　サポートされるアナログ MGCP 機能

	インターフェイス タイプ					
Cisco ゲートウェイ	**FXS**	**FXO**	**E&M**	**FXO、バッテリ リバーサル**	**アナログ DID**	**CAMA 911**
Analog Telephone Adapter（ATA）	あり	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
827-4V	なし	なし	適用対象外	適用対象外	適用対象外	適用対象外
1751 および 1760	あり	あり	なし	あり	なし	なし
VG200	あり	あり	なし	あり	なし	なし
VG248	なし	なし	なし	なし	なし	なし
VG224	あり	なし	なし	なし	なし	なし
2600 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
3600 シリーズ	あり	あり	なし	あり	なし	なし
3700 シリーズ	あり	あり	なし	あり	なし	なし
3800 シリーズ	あり	あり	なし	あり	なし	なし
ICS 7750	あり	あり	なし	なし	なし	なし
Catalyst 4000 Access Gateway Module（AGM）	あり	あり	なし	なし	なし	なし
6608 および 6624	あり	なし	なし	なし	なし	なし
コミュニケーション メディア モジュール（CMM）24FXS	あり	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
7x00 ファミリー	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外

Cisco デジタル ゲートウェイ

表 4-4 ～表 4-7 では、H.323 または SIP を使用する Cisco デジタル ゲートウェイに対してサポートされているインターフェイス タイプをリストしています。表 4-8 では、メディア ゲートウェイ コントロール プロトコル（MGCP）を使用する Cisco デジタル ゲートウェイに対してサポートされている、インターフェイス タイプをリストしています。

表 4-4　BRI、T1 CAS、T1 FGB、T1 FGD、および T1 QSIG に対してサポートされるデジタル H.323 および SIP 機能

	インターフェイス タイプ							
Cisco ゲートウェイ	BRI（TE、ユーザ側）	BRI（NT、ネットワーク側）	BRI QSIG（Net3）	BRI 電話	T1 CAS（robbed ビット）	T1 FGB	T1 FGD	T1 QSIG
Analog Telephone Adapter（ATA）	なし	なし	なし	なし	なし	なし	なし	なし
827-4V	なし	なし	なし	なし	なし	なし	なし	なし
1751 および 1760	なし	あり	あり	なし	あり	なし	なし	あり
VG200	あり	あり	なし	なし	あり	なし	あり	なし
VG248	なし	なし	なし	なし	なし	なし	なし	なし
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
2600 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
3600 シリーズ	あり	あり	あり	なし	あり	なし	あり	あり
3700 シリーズ	あり	あり	あり	なし	あり	なし	あり	あり
3800 シリーズ	あり	あり	あり	なし	あり	なし	あり	あり
ICS 7750	あり	あり	なし	なし	あり	なし	あり	なし
Catalyst 4000 Access Gateway Module（AGM）	あり	なし	あり	なし	あり	なし	あり	あり
6608 および 6624	適用対象外	適用対象外	適用対象外	適用対象外	なし	なし	なし	なし
コミュニケーション メディア モジュール（CMM）24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	適用対象外	適用対象外	適用対象外	適用対象外	あり	なし	なし	あり
7x00 ファミリー	適用対象外	適用対象外	適用対象外	適用対象外	あり	なし	あり	あり

表 4-5　T1 PRI DMS-100、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、DMS-100）**	**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）**
Analog Telephone Adapter（ATA）	なし	なし	なし	なし	なし	なし
827-4V	なし	なし	なし	なし	なし	なし
1751 および 1760	あり	将来的にサポート	あり	将来的にサポート	あり	将来的にサポート
VG200	あり	なし	あり	なし	あり	なし
VG248	なし	なし	なし	なし	なし	なし
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
2600 シリーズ	あり	将来的にサポート	あり	将来的にサポート	あり	将来的にサポート
2800 シリーズ	あり	将来的にサポート	あり	将来的にサポート	あり	将来的にサポート
3600 シリーズ	あり	将来的にサポート	あり	将来的にサポート	あり	将来的にサポート
3700 シリーズ	あり	将来的にサポート	あり	将来的にサポート	あり	将来的にサポート
3800 シリーズ	あり	将来的にサポート	あり	将来的にサポート	あり	将来的にサポート
ICS 7750	あり	なし	あり	なし	あり	なし
Catalyst 4000 Access Gateway Module（AGM）	あり	将来的にサポート	あり	将来的にサポート	あり	将来的にサポート
6608 および 6624	なし	なし	なし	なし	なし	なし
コミュニケーション メディア モジュール（CMM）24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	あり	あり	あり	あり	あり	あり
7x00 ファミリー	あり	将来的にサポート	あり	将来的にサポート	あり	将来的にサポート

表 4-6　T1 PRI NI2、NFAS、および Network Specific Facilities（NSF）サービスに対してサポートされるデジタル H.323 および SIP 機能

	インターフェイス タイプ					
Cisco ゲートウェイ	T1 PRI（ユーザ、NI2）	T1 PRI（ネットワーク、NI2）	T1 PRI NFAS（ユーザ、DMS-100）	T1 PRI NFAS（ユーザ、4ESS）	T1 PRI NFAS（ユーザ、5ESS）	T1 PRI（Megacom または SDN、4ESS）
Analog Telephone Adapter（ATA）	なし	なし	なし	なし	なし	なし
827-4V	なし	なし	なし	なし	なし	なし
1751 および 1760	あり	あり	なし	なし	なし	なし
VG200	あり	あり	なし	なし	なし	なし
VG248	なし	なし	なし	なし	なし	なし
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
2600 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
3600 シリーズ	あり	あり	あり	あり	あり	あり
3700 シリーズ	あり	あり	あり	あり	あり	あり
3800 シリーズ	あり	あり	あり	あり	あり	あり
ICS 7750	あり	あり	あり	あり	あり	なし
Catalyst 4000 Access Gateway Module（AGM）	あり	あり	将来的にサポート	将来的にサポート	将来的にサポート	将来的にサポート
6608 および 6624	なし	なし	なし	なし	なし	なし
コミュニケーション メディア モジュール（CMM）24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	あり	あり	将来的にサポート	将来的にサポート	将来的にサポート	なし
7x00 ファミリー	あり	あり	なし	なし	なし	なし

表 4-7　E1 および J1 に対してサポートされるデジタル H.323 および SIP 機能

	インターフェイス タイプ						
Cisco ゲートウェイ	E1 CAS	E1 MELCAS	E1 R2	E1 PRI（ユーザ側、Net5）	E1 PRI（ネットワーク側、Net5）	E1 QSIG	J1
Analog Telephone Adapter（ATA）	なし	なし	なし	なし	なし	なし	なし
827-4V	なし	なし	なし	なし	なし	なし	なし
1751 および 1760	なし	なし	あり	あり	あり	あり	なし
VG200	なし	あり	あり	あり	あり	なし	あり
VG248	なし	なし	なし	なし	なし	なし	なし
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
2600 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
3600 シリーズ	あり	あり	あり	あり	あり	あり	あり
3700 シリーズ	あり	あり	あり	あり	あり	あり	あり

表 4-7　E1 および J1 に対してサポートされるデジタル H.323 および SIP 機能（続き）

	インターフェイス タイプ						
Cisco ゲートウェイ	**E1 CAS**	**E1 MELCAS**	**E1 R2**	**E1 PRI（ユーザ側、Net5）**	**E1 PRI（ネットワーク側、Net5）**	**E1 QSIG**	**J1**
3800 シリーズ	あり	あり	あり	あり	あり	あり	あり
ICS 7750	なし	なし	あり	あり	あり	なし	なし
Catalyst 4000 Access Gateway Module（AGM）	なし	なし	あり	あり	あり	あり	なし
6608 および 6624	なし	なし	なし	なし	なし	なし	なし
コミュニケーション メディア モジュール（CMM）24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	なし	なし	あり	あり	あり	あり	適用対象外
7x00 ファミリー	あり	なし	あり	あり	あり	あり	なし

表 4-8　サポートされるデジタル MGCP 機能

	インターフェイス タイプ					
Cisco ゲートウェイ	**BRI**[1]	**T1 CAS（E&M）**	**T1 PRI**	**T1 QSIG**	**E1 PRI**	**E1 QSIG**
Analog Telephone Adapter（ATA）	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
827-4V	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
1751 および 1760	12.3(14)T	あり	あり	あり	あり	あり
VG200	なし	あり	あり	あり	あり	あり
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
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
2600 シリーズ	12.4(2)T	あり[2]	あり[2]	あり[2]	あり[2]	あり[2]
2800 シリーズ	12.4(2)T	あり[2]	あり[2]	あり[2]	あり[2]	あり[2]
3600 シリーズ	12.4(2)T	あり[2]	あり[2]	あり[2]	あり[2]	あり[2]
3700 シリーズ	12.4(2)T	あり[2]	あり[2]	あり[2]	あり[2]	あり[2]
3800 シリーズ	12.4(2)T	あり[2]	あり[2]	あり[2]	あり[2]	あり[2]
ICS 7750	12.3.2XA	あり	あり	あり	あり	あり
Catalyst 4000 Access Gateway Module（AGM）	なし	あり	あり	あり	あり	あり
6608	適用対象外	あり	あり	あり	あり	あり
6624	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
コミュニケーション メディア モジュール（CMM）24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	適用対象外	あり	あり	あり	あり	あり
7x00 ファミリー	適用対象外	なし	なし	なし	なし	なし

1. Cisco IOS Release 12.4(2)T は、NM-HDV2、NM-HD-XX、およびオンボード H-WIC スロットで BRI MGCP をサポートしています。BRI MGCP は、NM-1V/2V ハードウェアで旧リリースの Cisco IOS によってもサポートされています。
2. AIM-VOICE-30 モジュールは、MGCP のサポートに Cisco IOS Release 12.2.13T を必要とします。プロトコルタイプ NTT は、MGCP BRI 未対応です。

QSIG サポート

QSIG は、企業ネットワーク内で PBX 機器を柔軟に接続するために設計された、1 組の国際標準です。その他の機能の 1 つとして、QSIG には、さまざまなベンダー製の PBX 機器を相互接続するためのオープンな標準ベースの方法が用意されています。

ECMA QSIG は、PBX-to-PBX モードの H.323 ゲートウェイでサポートされています。H.323 ゲートウェイは、QSIG 情報要素に対する QSIG 機能の完全な透過性を備えています。基本的なコールのセットアップと終了は、表 4-9 に示されているように、H.323 QSIG ゲートウェイを使用してサポートされます。

表 4-9　H.323 ゲートウェイにおける QSIG サポート

プラットフォーム	メディア	必要な Cisco IOS ソフトウェア対応リリース
Cisco 1751 および 1760	BRI T1/E1 QSIG	12.2(8)YH 12.2(4)YB
Cisco 2600 および 3600 シリーズ	BRI および T1/E1 QSIG	12.1.2T
Cisco 2800 シリーズ	BRI および T1/E1 QSIG	12.3.8T4
Cisco 3700	T1/E1 QSIG	12.2.8T
Cisco 3800	BRI および T1/E1 QSIG	12.3.11T
Cisco 7200	T1/E1 QSIG	12.1.2T
Cisco 5300	T1/E1	12.0.7T
Cisco AS5350 Cisco AS5400	T1/E1	12.2.2T

Cisco IOS ゲートウェイにおける QSIG のサポートの詳細は、次の Web サイトを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_qsig.htm#xtocid116542

Cisco CallManager Release 3.3 より前のリリースでは、PBX が H.323 を介して QSIG を使用するゲートウェイに接続されている場合、PBX 上の電話機と、Cisco CallManager に接続されている IP Phone との間でコールが行われるときにサポートされているのは、基本的な PRI 機能だけです。CLID（発呼回線 ID）と DID（ダイヤルイン方式）番号だけが含まれるこの基本機能は、Cisco CallManager によってではなく、QSIG プロトコルを終端するゲートウェイによってサポートされています。

Cisco CallManager が QSIG 機能をサポートするには、QSIG を Cisco CallManager に直接バックホール（back-haul）する必要があります。このサポートは、Catalyst 6608、2600XM シリーズ、および 3640/60 シリーズなどの MGCP ゲートウェイと連携して、Cisco CallManager Release 3.3 およびそれ以降で実装されています。

FAX とモデムのサポート

ここでは、Cisco CallManager と Cisco 音声ゲートウェイで使用可能な FAX とモデムのサポートについて説明します。まず、Cisco 音声ゲートウェイ上での FAX とモデムのサポートの概要を説明した後、サポートされるプラットフォームとコンフィギュレーション ファイル例をリストします。

FAX パススルーと Cisco FAX リレーに対するゲートウェイ サポート

FAX over IP により、従来のアナログ FAX マシンと IP テレフォニー ネットワークとの相互運用性が可能になります。FAX イメージは、アナログ信号から変換され、パケット ネットワークを介してデジタル データとして伝送されます。

FAX データの元の形式は、デジタルです。しかし、従来の公衆網を経由して送信するために、データは変調され、アナログに変換されます。FAX over IP は、このアナログ変換のプロセスを逆転させて、パケット ネットワーク上でデジタル データを送信した後、受信側の FAX マシン用にそのデジタル データをアナログに再変換します。

大部分の Cisco 音声ゲートウェイは、現在、IP ネットワークを介して FAX トラフィックを送信する、次の 2 通りの方法をサポートします。

- Cisco FAX リレー：FAX リレー モードでは、ゲートウェイが T.30 FAX 信号を終端します。
- FAX パススルー：FAX パススルー モードでは、ゲートウェイは、FAX コールを音声コールと区別しません。

FAX トラフィックの送信には、Cisco FAX リレー モードをお勧めします。しかし、特定のゲートウェイが Cisco FAX リレーをサポートしない場合、そのゲートウェイは FAX パススルーをサポートします。

ベスト プラクティス

Cisco 音声ゲートウェイで FAX サポートを最大限に実装するには、次の推奨事項とガイドラインが役立ちます。

- QoS を使用する場合は、できる限り、次のパラメータが最小になる方法を採用してください。
  - パケット損失
  - 遅延
  - 遅延変動（ジッタ）

  Cisco IP テレフォニー ネットワークにおける QoS の実装についての詳細は、次の Web サイトで入手可能な『*Cisco Network Infrastructure Enterprise Quality of Service Design*』のガイドを参照してください。

  http://www.cisco.com/go/srnd
- FAX コールの完全性を確保するには、次のヒントが役立ちます。
  - コール アドミッション制御（CAC）を使用して、コールが規定の合計帯域幅限界を超えると、拒否されるようにします。
  - モデムと FAX のすべての専用ポートで、コール ウェイティングを使用不可にします。
- 最良のパフォーマンスを確保するために、起点と終端の両方のゲートウェイで、Cisco FAX リレーを有効にしていることを確認してください。2 つの Cisco IOS ゲートウェイの転送方法が異なる場合、ゲートウェイはネゴシエートして Cisco FAX リレーを使用します。

  Cisco FAX リレーをサポートしていない IOS 以外のゲートウェイは、Cisco Digital Access DT-24/DE-30+ だけです。このゲートウェイを Cisco IOS ゲートウェイに接続する場合は、FAX パススルー モードの使用を両方のゲートウェイに設定する必要があります。
- ネットワーク上の恒常的なパケット遅延が 1 秒を超えないこと、および遅延変動（ジッタ）が 240 ミリ秒を超えないことを確認してください。

- 不良パケットの着信頻度が高いネットワークで、パフォーマンスを改善するには、FAX マシンでエラー訂正モード（ECM）を無効にしてください。
- 大部分の FAX マシンは、現在の速度をスロー ダウンすることなく、0.4% ～ 0.6% の範囲内のパケット ドロップを受け入れるようです。しかし、0.8% ～ 1% の範囲内のパケット ドロップがあるネットワークでは、ECM を無効にする必要があります。
- 複数の FAX マシンで ECM を無効にするのを検討する前に、ゲートウェイ自体で ECM を無効にすることができます。しかし、パケット ドロップが発生する場合、FAX のイメージ品質が低下する恐れがあります。したがって、ECM を無効にするときには、長いコール所要時間やコールのドロップを検討する前に、イメージ品質を損なってもよいかどうかを十分に検討してください。また、パケットがドロップする原因を突き止めて、解決するために、ネットワークを監視し、評価することも必要です。

モデム パススルーに対するゲートウェイ サポート

一般に、音声ゲートウェイを使用して、IP ネットワーク上のモデム セッションをサポートするには、次の 2 通りのメカニズムがあります。

- モデム パススルー
- モデム リレー

現在、Cisco 音声ゲートウェイでサポートされているメカニズムは、モデム パススルーだけです。

モデム パススルーとは、パルス符号変調（PCM）符号化パケットと G.711 コーデックを使用して、パケット ネットワークを通じてモデム信号を転送することです。モデム パススルーでは、ゲートウェイがモデム信号と音声信号を区別し、適切なアクションを取ることができなければなりません。ゲートウェイは、モデム信号を検出すると、次のサービスを無効にします。

- エコー キャンセレーション（EC）
- 音声アクティビティ検出（VAD）

モデム パススルー モードでは、ゲートウェイは、モデム コールを音声コールと区別しません。2 台のモデム間の通信は、「音声」コールを介してインバンドにそのまま伝送されます。モデム トラフィックは、QoS 対応の IP インフラストラクチャを介して透過的に伝送され、IP ネットワーク内でデータが復調されることはありません。

モデム コールは「音声」コールを介してインバンドに伝送されるという点で、モデムのアップスピード機能は、パススルーに似ています。違いは、アップスピード機能が使用されるときに、ゲートウェイがある程度まで、モデム コールを認識する点です。リレー メカニズムは使用されませんが、ゲートウェイは、モデム トーンを認識し、「音声」コーデックを G.711（「アップスピード」部分）に自動的に変更し、コールの期間中 VAD とエコー キャンセレーション（EC）を無効にします。

現在、このアップスピード機能は、Cisco IOS Release 12.1.3T による Cisco AS5300 以外の Cisco IOS プラットフォームではサポートされていません。Cisco 2600XM、3700、VG224、および Catalyst 4000 Access Gateway Module（AGM）プラットフォームの場合、モデムのアップスピード機能は、将来の Cisco IOS リリースでサポートされる予定です。これらのプラットフォームの場合、モデムのアップスピード機能が使用可能になるまで、ダイヤルピアで **no vad** を設定できます。

モデム アップスピード機能は、Catalyst 6000 ゲートウェイ モジュールでもサポートされています。

ベスト プラクティス

IP インフラストラクチャを介して転送されるモデム トラフィックの最適なパフォーマンスを確保するには、次の推奨ベスト プラクティスを守ってください。

- IP ネットワークで QoS（Quality of Service）が使用可能になっていること、および LAN、MAN、および WAN 環境で、QoS を提供するためのすべての推奨事項に従っていることを確認します。できる限り、次のパラメータが最小になる方法を採用してください。

- パケット損失：FAX とモデムのトラフィックには、本質的に損失のない転送が必要です。パケットが 1 つでも損失すると、再送信が行われます。
- 遅延
- 遅延変動（ジッタ）

詳細は、次の Web サイトで入手可能な『*Cisco Network Infrastructure Enterprise Quality of Service Design*』のガイドを参照してください。

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

- コール アドミッション制御（CAC）を使用して、コールが規定の合計帯域幅限界を超えると、拒否されるようにします。
- モデムを使用するすべてのコールに、G.711 を使用します。ゲートウェイの 1 つがモデム リレーをサポートしていない場合、モデム パススルーがネゴシエートされます（G.711 のみ）。モデムが使用される場合、すべてのコールに G.711 を使用することが最善の方法です。
- IP ネットワークにモデムを接続して、IP ネットワークの問題のトラブルシューティングや診断をしないでください。この場合、IP インフラストラクチャを構成するデバイスのトラブルシューティングに使用されるモデムは、一般電話サービス（POTS）に接続する必要があります。
- 可能な場合、単一のシグナリング プロトコルとゲートウェイ ファミリーを使用して、相互運用性の問題を最小限にします。
- モデムと FAX のすべての専用ポートで、コール ウェイティングを使用不可にします。

V.90 サポート

現在、Cisco 機器は V.34 モデムのみをサポートします。V.90 モデムは既存のハードウェアで機能し、V.34 よりも高速ですが、V.90 の完全なサポートは保証できません。

サポートされるプラットフォームと機能

FAX とモデムの機能をサポートしている Cisco プラットフォームは、次のとおりです。

アナログ ゲートウェイ

Cisco IOS ゲートウェイ：

- 2600XM および 2691（FXS）
- 2800（FXS）
- 3725 および 3745（FXS）
- 3800（FXS）
- VG200（FXS）
- VG224
- 1751 および 1760
- コミュニケーション メディア モジュール（CMM）FXS カード

IOS 以外のゲートウェイ：

- VG248
- ATA 188
- 6624

デジタル ゲートウェイ

Cisco IOS ゲートウェイ：

- 2600XM および 2691
- 2800

- 3725 および 3745
- 3800
- VG200
- VG224
- 1751 および 1760
- 7200 および 7500
- AS5300、5350、5400、および 5850
- コミュニケーション メディア モジュール（CMM）

IOS 以外のゲートウェイ：

- 6608

（注） FAX とモデムのサポート テストは、Cisco IOS ゲートウェイ上の Cisco IOS Release 12.3(1)、および Cisco VG248 Analog Phone Gateway の Release 1.2.1 を使用して、上記のプラットフォーム上で実行されました。

プラットフォーム プロトコルのサポート

企業ソリューションで現在使用されている一般的なコール制御プロトコルには、H.323、メディア ゲートウェイ コントロール プロトコル（MGCP）、および Skinny Client Control Protocol（SCCP）があります。すべての Cisco 音声プラットフォームが、これらのプロトコル、または FAX とモデム機能をすべてサポートしているわけではないので、相互運用性の問題が発生します。また、Cisco 2600XM や Cisco 3700 シリーズなどの Cisco IOS ゲートウェイを、VG248 などの IOS 以外のゲートウェイと組み合せる場合は、さらに相互運用性の問題が発生します。ここでは、FAX、モデム、およびプロトコルの機能の相互運用性をサポートしているゲートウェイの組み合せをリストしています。

高いレベルで、Cisco IOS Release 12.3(1)（Cisco 6608 のロード 47 と Cisco 6624 のロード 41）、および VG248 の Release 1.2.1 は、Cisco FAX リレー、モデム パススルー、および音声機能の相互運用性をサポートします。Cisco IOS Release 12.2(11)T1 より前には、Cisco IOS と IOS 以外の音声プラットフォーム間では、音声と Cisco FAX リレーのみがサポートされていました。これは、パススルー ネットワーク サービス エンジン（NSE）方式の非互換性により、モデム パススルーが相互運用できなかったからです。

ネットワークにおける一般的なプロトコルの組み合せの一部には、MGCP と H.323、SCCP と H.323、および SCCP と MGCP があります。一般的な音声ゲートウェイには、Cisco VG224、VG248、2600XM、2800、3700、3800、5300、および Catalyst 6000 が含まれます。

表 4-10 では、FAX とモデムの相互運用性を現在サポートしている、プロトコルの組み合せをリストしています。

表 4-10　FAX とモデムの機能がサポートされるコール制御プロトコルの各種組み合せ

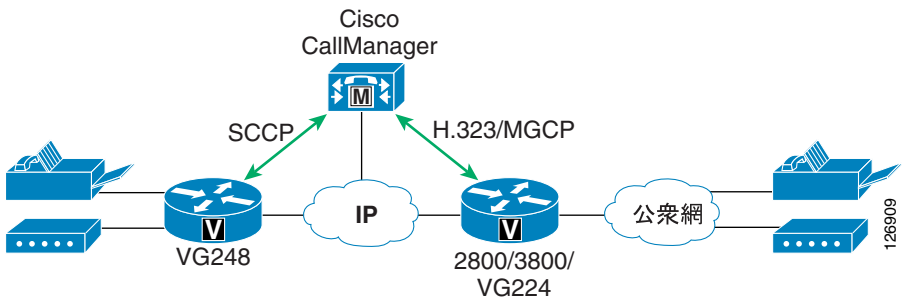
プロトコルの組み合せ	モデム リレー	モデム パススルー	T.38 FAX リレー	Cisco FAX リレー	FAX パススルー
MGCP を使用する Cisco CallManager と H.323 を使用する Cisco CallManager との組み合せ	あり	あり	なし	あり	あり
MGCP を使用する Cisco CallManager と MGCP を使用する Cisco CallManager との組み合せ	あり	あり	なし	あり	あり
SCCP と H.323 を使用する Cisco CallManager との組み合せ	あり	あり	なし	あり	あり
SCCP と MGCP を使用する Cisco CallManager との組み合せ	あり	あり	なし	あり	あり

（注）　Cisco ATA 188、VG248、および Catalyst 6000 プラットフォームは現在、T.38 FAX リレーをサポートしていません。これらのプラットフォームが Cisco AS5350 または AS5400 ゲートウェイに接続される場合、FAX アプリケーションに対して FAX パススルーのみがサポートされます。

ゲートウェイの組み合せと機能の相互運用性

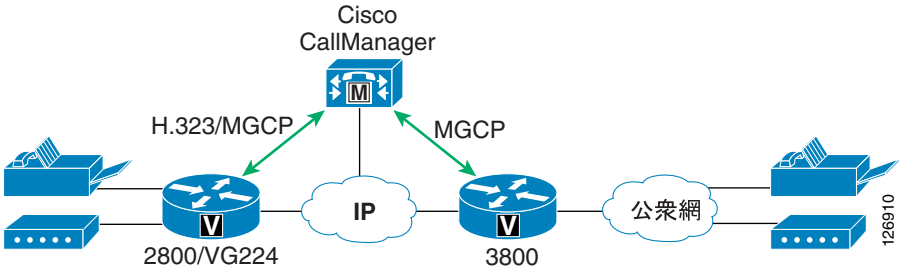
FAX とモデムの相互運用性について最も多い質問は、図 4-3 に示されているように、Cisco IOS ゲートウェイ（たとえば、Cisco 2800 や 3800）と IOS 以外のゲートウェイ（たとえば、Cisco VG248）との組み合せに関するものです。

図 4-3　Cisco IOS と IOS 以外のゲートウェイを組み合せる構成



FAX とモデムの相互運用性について次に多い質問は、図 4-4 に示されているように、Cisco IOS ゲートウェイのみを使用する構成に関するものです。

図 4-4　Cisco IOS ゲートウェイのみを使用する構成



どちらのシナリオの回答も、基本的に同じです。6608 上の Cisco IOS ロード 47、および VG248 上の Release 1.2.1 より前では、音声と Cisco FAX リレーのみがサポートされ、FAX パススルーとモデム パススルーは、NSE の非互換性によりサポートされません。6608 上の Cisco IOS ロード 47 以降、6624 上のロード 41 以降、および VG248 上の Release 1.2.1 は、この 3 つのプラットフォームはすべて、コール制御プロトコルに関係なく、音声、Cisco FAX リレー、およびモデム パススルー用に、Cisco IOS ゲートウェイと相互運用できます。NSE パススルー方式は、シグナリング パスではなく、ベアラ パスで動作するので、コール制御プロトコルとは関係しません。

類似ゲートウェイ間の機能サポート

表 4-11 では、同じ一般的なタイプのゲートウェイ間（たとえば、Cisco VG248 と 6608 間、2600XM と 3700 間、または 2600XM と AS5300 間）でサポートされる FAX とモデムの機能をリストします。両方のプラットフォームが所定の機能をサポートする限り、プラットフォームは相互運用します。

表 4-11　同じタイプのゲートウェイ上での FAX とモデム機能のサポート

ゲートウェイ タイプ	FAX パススルー	Cisco FAX リレー	T.38 FAX リレー	モデム パススルー	モデム リレー
Cisco IOS ゲートウェイ	サポートする	サポートする（5350 と 5400 を除く）	サポートする	サポートする	サポートする（NM-HDV のみ）
IOS 以外のゲートウェイ	サポートする	サポートする（ATA 188 を除く）	適用対象外	サポートする（ATA 188 を除く）	適用対象外

ゲートウェイ設定例

ここでは、FAX とモデムをサポートするためのゲートウェイ設定例を示します。

Cisco IOS ゲートウェイの設定

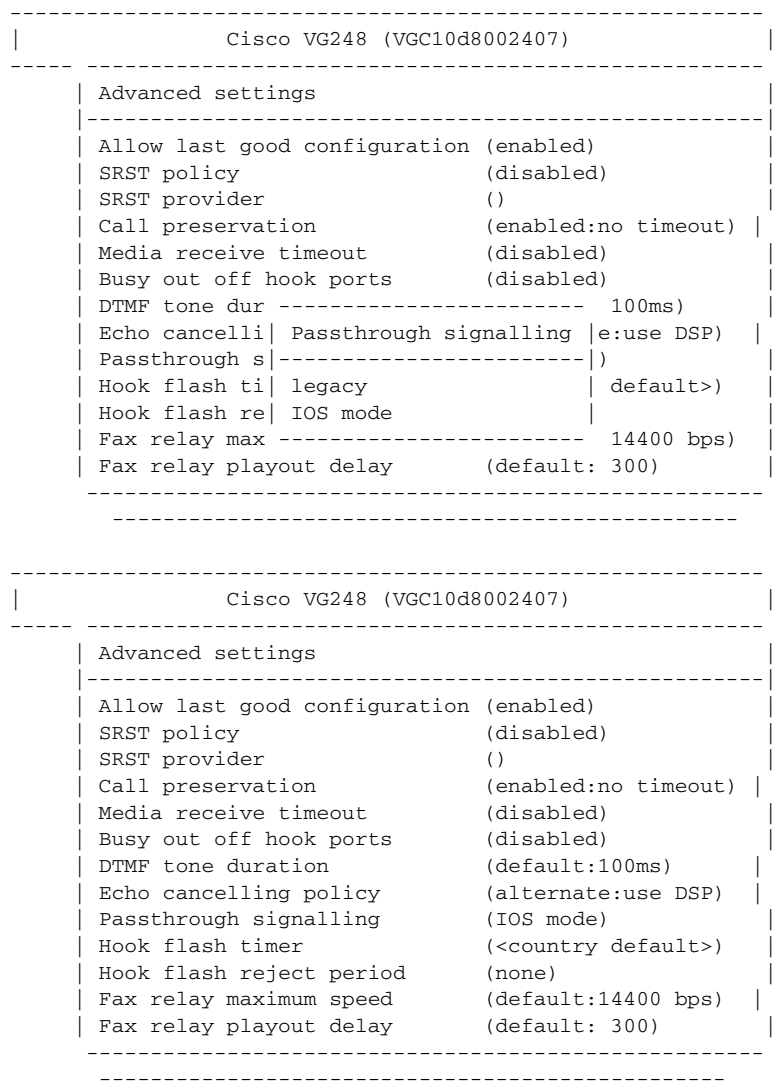
H.323

```
!
! Cisco fax relay is ON by default
!(except for 5350/5400, where Cisco fax relay is not supported)
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
!
!
```

MGCP

```
!
ccm-manage mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
mgcp modem passthrough voip mode nse
mgcp fax t38 inhibit
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
```

Cisco VG248 の設定



Cisco IOS ゲートウェイ用の Cisco CallManager 設定

Cisco IOS ゲートウェイ（たとえば、Cisco 6608 と 6624）用に Cisco CallManager を設定するには、Cisco CallManager で次の手順を実行します。また、これらの設定手順については、図 4-5 および図 4-6 も参照してください。

ステップ 1　Cisco CallManager Administration で、**Device** > **Gateway** の順に選択して、**Find/List Gateways** ウィンドウを表示します。

ステップ 2　変更するゲートウェイを検索するか（すでに存在する場合）、または **Add a New Gateway** をクリックして新しいゲートウェイを Cisco CallManager データベースに追加します。

ステップ 3　適切なタイプのゲートウェイ（たとえば、Cisco Catalyst 6000）を選択した後、**FAX Relay Enable** をクリックして Cisco FAX リレーを使用可能にします。

ステップ 4　**NSE Type** ドロップダウン リスト ボックスを使用して、モデム パススルー用に **IOS Gateways** を選択します。

ステップ 5　**Update** をクリックして変更内容を保存します。

ステップ 6　ゲートウェイをリセットして変更内容を適用します。

図 4-5　Cisco CallManager におけるゲートウェイ設定

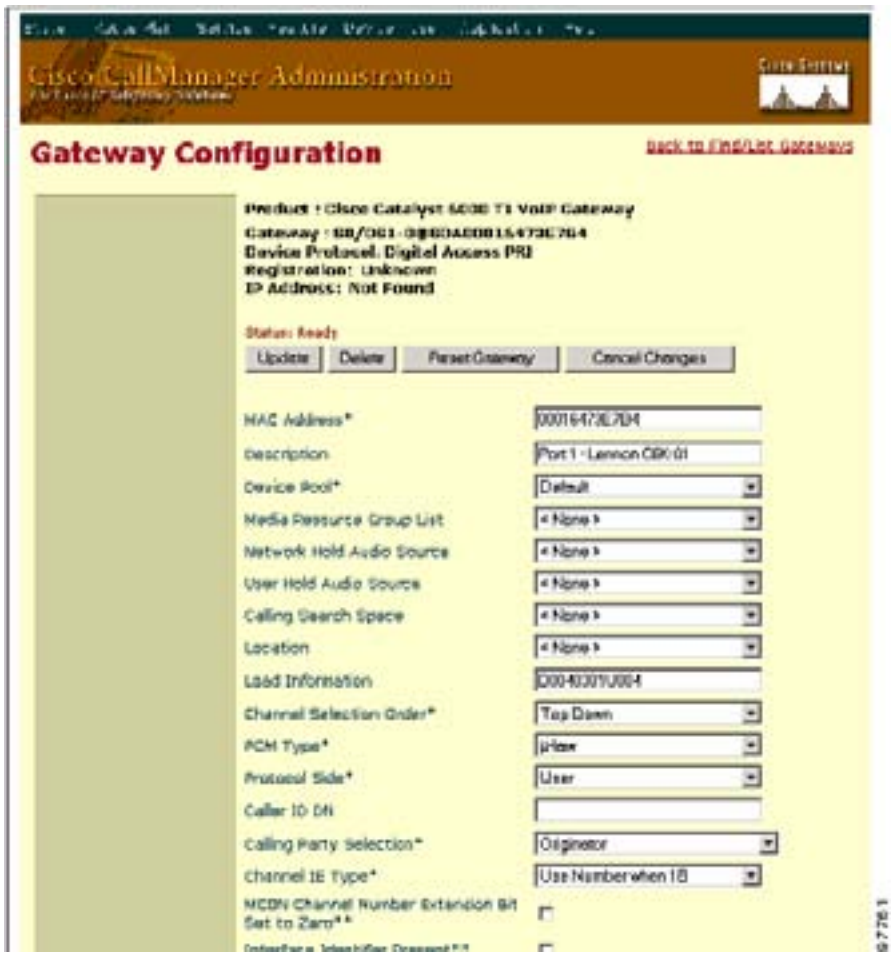


図 4-6　Cisco CallManager におけるゲートウェイ設定（続き）

この設定は、Cisco VG248、6608、6624、および IOS ゲートウェイ間での、音声、Cisco FAX リレー、およびモデム パススルーをサポートします。ただし、Cisco FAX リレーをサポートしない Cisco AS5350 および AS5400 ゲートウェイを除きます。また、この設定は、パススルー モードの V.34 モデム接続もサポートします。V.90 モデム接続は保証されていませんが、ネットワーク ジッタの量とクロック同期によっては可能です。

FAX とモデム パススルー用のクロック ソーシング

FAX とモデム パススルーを正常に機能させるには、クロック信号が重要な役割を果たします。ゲートウェイのクロックは、Stratum クロッキングが提供される公衆網クロックと同期させる必要があります。このクロック同期がないと、FAX および（特に）モデムのパススルーは機能しません。クロックを正しく同期させるには、T1 コントローラで次の設定を入力してください（この例では、T1 コントローラは、公衆網に接続している音声ゲートウェイです）。

```
!
controller T1 0
 framing esf
 linecode b8zs
 clock source line
 channel-group 1 timeslots 1-24 speed 64
 !
```

また、公衆網に接続している他のすべてのインターフェイスでも、この設定を入力してください。

T.38 FAX リレー

T.38 FAX リレーは、Cisco ATA 188、VG248、6608、および 6624 ゲートウェイではサポートされていませんが、Cisco 2800 および 3800 など、大部分の高性能 Cisco IOS 音声プラットフォームではサポートされています。

T.38 FAX リレーは、次のいずれかの方法で設定できます。

- ネットワーク サービス エンジン（NSE）を使用して制御されるルース ゲートウェイ（P.4-29）
- H.245 または SDP（Session Definition Protocol）による機能交換を使用して制御されるゲートウェイ（P.4-29）
- H.323 Annex D および MGCP を使用したコール エージェント制御の T.38（P.4-31）

ネットワーク サービス エンジン（NSE）を使用して制御されるルース ゲートウェイ

この設定では、次の Cisco IOS ゲートウェイ設定例に示されているように、ダイヤルピア上の静的 T.38 設定を使用します。

H.323

```
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
 fax protocol t38
!
!
```

MGCP

```
!
ccm-manage mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
mgcp modem passthrough voip mode nse
no mgcp fax t38 inhibit
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
!
```

H.245 または SDP（Session Definition Protocol）による機能交換を使用して制御されるゲートウェイ

この T.38 FAX リレー設定方法には、次の特性が適用されます。

- T.38 機能はゲートウェイ間で交換されます。FAX トーンの検出後に T.38 FAX リレーに切り替わることを起点側のゲートウェイに知らせるために、ネットワーク サービス エンジン（NSE）メッセージが、RTP ストリーム上で終端側のゲートウェイから送信されます。この NSE メッセージは RTP ストリーム上で送信されるので、コール制御信号に対しては透過されます。
- Cisco CallManager は、H.323 または MGCP ではこの機能交換をサポートできません。したがって、T.38 機能が交換されない場合であっても、設定コマンドを使用して強制的に T.38 FAX リレーに切り替える必要があります。
- 選択可能ならフォールバック方法は、次の 3 通りです。
  - Cisco FAX リレー（デフォルト）
  - FAX パススルー
  - なし

次に、このタイプの設定例を示します。

H.323

```
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
!
! To enable T.38 fax relay and fall back to Cisco fax relay when
! T.38 fax negotiation fails.This is the default case.
 fax protocol t38 fallback cisco
!
dial-peer voice 1001 voip
 destination-pattern 2T
 session target ipv4:10.10.10.2
 modem passthrough mode nse codec g711ulaw
!
! To enable T.38 fax relay and fall back to fax passthrough when
! T.38 fax negotiation fails.
fax protocol t38 nse fallback pass-through
!
dial-peer voice 1002 voip
 destination-pattern 3T
 session target ipv4:10.10.10.3
 modem passthrough mode nse codec g711ulaw
!
! This CLI is needed when talking to MGCP endpoint where CA/GK
! doesn't support T.38 fax relay such as CCM.
 fax protocol t38 nse force fallback none
!
!
```

MGCP

```
!
ccm-manage mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
mgcp modem passthrough voip mode nse
no mgcp fax t38 inhibit
!
! This CLI is needed when CA doesn't support T.38 fax relay
mgcp fax t38 gateway force
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
!
```

Cisco VG248 および 6608 または 6624 を使用するトポロジでは、次の Cisco IOS コマンドを使用してください。

```
fax protocol t38 [nse [force]] fallback [cisco | none]
modem passthrough nse codec {g711ulaw|g711alaw}
```

これらの 2 つのコマンドにより、Cisco IOS ゲートウェイは、T.38 FAX リレーとモデム パススルーを実行するために他の Cisco IOS ゲートウェイと相互運用するだけでなく、Cisco FAX リレーとモデム パススルーを実行するために VG248 とも相互運用できるようになります。

H.323 Annex D および MGCP を使用したコール エージェント制御の T.38

この T.38 FAX リレー設定方法には、次の特性が適用されます。

- コール制御エージェント（たとえば、Cisco CallManager）が T.38 FAX リレーを制御し、ゲートウェイはパッシブ モードで動作します。
- ゲートウェイ間で NSE メッセージは送信されません。
- このタイプの設定では、T.38 FAX リレーは、コール制御プロトコルに対して透過的ではありません。コール エージェントは、H.323 と MGCP 間のプロトコル変換を実行します。
- この方法により、T.38 FAX リレーは、Cisco IOS Release 12.3(1) で設定できます。Cisco BTS 10200 Softswitch もこの方法をサポートします。
- Cisco CallManager は、T.38 FAX リレーのコール エージェント制御をサポートしません。したがって、この T.38 FAX リレー設定方法は、Cisco CallManager の配置には適用されません。

次に、このタイプの設定例を示します。

H.323

```
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
!
! To enable T.38 fax relay.
 fax protocol t38
!
!
```

MGCP

```
!
ccm-manage mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
!
! T.38 fax relay is ON by default.HOWEVER, CCM doesn't
! support CA controlled mode.This is the configuration for
! talking to BTS.
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
```

CHAPTER 5

Cisco CallManager トランク

Cisco CallManager Release 4.0 では、Session Initiation Protocol（SIP）トランクがサポートされるようになりました。Release 4.0 より前の Cisco CallManager は、H.323 トランクのみをサポートしていました。この章では、Cisco CallManager Release 4.1 に関する設計の考慮事項について説明します。ただし、説明の多くは Release 4.0 および 3.3 にも該当します。

現在、H.323 トランクは、他の Cisco CallManager クラスタや、ゲートウェイなどの他の H.323 デバイスに対する接続性を提供します。H.323 トランクは、Cisco CallManager がクラスタ内通信用にサポートするオーディオおよびビデオ コーデックのほとんどをサポートします。ただし、ワイドバンド オーディオ、ワイドバンド ビデオ、および H.264 ビデオについてはサポートしません。

H.323 トランクは、Empty Capabilities Set（ECS）を使用して、保留 / 保留解除や転送などの補足コール サービスを提供します。この方法は、メディア ストリーム（またはチャネル）を停止または終了し、同一または別のエンドポイント アドレスに対してメディア ストリームを開始または起動するための標準の H.245 メカニズムです。この方法を使用すると、Cisco CallManager は、コールをアクティブにしたままでも、メディア ストリームの送信元および宛先を迅速に制御することができます。

たとえば、H.323 トランクを使用した 2 つのクラスタ（A と B）間のコールについて考えます。クラスタ A のユーザがクラスタ B のユーザを保留にした場合、2 人のユーザ間のメディア ストリームは終了し、クラスタ B のユーザはクラスタ A の Music On Hold（MOH）サーバに接続されます。MOH サーバは、ユーザにメディア（音楽ファイル）を送信するよう指示されます。クラスタ A のユーザがコールを保留解除すると、MOH ストリームが終了し、2 人のユーザ間で双方向メディア ストリームが再開されます（Cisco CallManager は、補足コール サービス用に H.450 をサポートしていません）。このケースでは、MOH は ECS 動作の一例です。H.323 トランクはマルチキャスト MOH をサポートしないため、H.323 トランクの Media Resource Group List（MRGL; メディア リソース グループ リスト）には、ユニキャスト MOH リソースだけを含める必要があります（詳細については、P.7-1 の「Music on Hold」を参照してください）。

H.323 トランク上のコールに使用される帯域幅を制御するには、Cisco CallManager で設定され、各トランクに割り当てられる、*リージョン*を使用します。リージョンは、そのリージョンのオーディオ コーデック タイプと帯域幅を指定することで、コールに割り当てられる帯域幅の量を制限します。そのリージョンと別のリージョン間のコールは、指定された帯域幅の制限を超えることはできません。H.323 トランク上でコールを発信するデバイスが、より限定的なリージョン内にある場合や、ビデオなどの特定のコーデックをサポートしない場合、そのデバイスはそのコールに使用可能なコーデックのサブセットになっています。H.323 トランク上のすべての DTMF（Dual Tone MultiFrequency）シグナリングは、H.245 を使用してアウトバンドで提供されます。

SIP トランクは、ゲートウェイ、プロキシ、ボイスメール システム、および他の Cisco CallManager クラスタなど、他の SIP デバイスへの接続性を提供します。SIP トランクには、H.323 トランクとは異なる次の特性があります。

- G.711 A-law および mu-law コーデックをサポートする
- ビデオをサポートしない
- コールごとにメディア ターミネーション ポイント（MTP）を必要とする（MTP も RFC 2833 DTMF をサポートする）

H.323 トランク

Cisco CallManager では、次の主要なタイプの H.323 トランクを設定できます。

- クラスタ間トランク（非ゲートキーパー制御）（P.5-2）
- クラスタ間トランク（ゲートキーパー制御）（P.5-3）
- H.225 トランク（ゲートキーパー制御）（P.5-3）

クラスタ間トランク（非ゲートキーパー制御）

このトランクは、最も単純なもので、単一のマルチクラスタ キャンパスまたは分散型コール処理配置で他の Cisco CallManager クラスタに接続するために使用されます。このトランクは、コール アドミッション制御にゲートキーパーを使用しません。ただし、帯域幅制御が必要な場合は、Cisco CallManager で設定されたロケーションを使用できます。

このタイプのトランクを定義する場合、同一の宛先クラスタに最大 3 つのリモート Cisco CallManager サーバを定義できます。トランクは、定義されているすべてのサーバに自動的にロードバランスされます。リモート クラスタでは、対応するクラスタ間トランク（非ゲートキーパー制御）を設定することが重要です。このトランクには、最初のクラスタでリモート Cisco CallManager サーバとして定義されているサーバと同じサーバを含む Cisco CallManager 冗長性グループを割り当てます。同様の設定は、クラスタ間トランクによって接続された各 Cisco CallManager クラスタでも必要です。

たとえば、クラスタ 1 にクラスタ 2 へのトランクがあり、クラスタ 2 にクラスタ 1 へのトランクがある場合は、次の設定が必要になります。

- クラスタ 1
  - サーバ B、C、および D を、クラスタ 2 へのトランクに関連付けられたデバイス プールで定義されている Cisco CallManager 冗長性グループのメンバーとして設定します。
  - 非ゲートキーパー制御トランクに、クラスタ 2 のリモート サーバ D、E、および F を設定します。
- クラスタ 2
  - サーバ D、E、および F を、クラスタ 1 へのトランクに関連付けられたデバイス プールで定義されている Cisco CallManager 冗長性グループのメンバーとして設定します。
  - 非ゲートキーパー制御トランクに、クラスタ 1 のリモート サーバ B、C、および D を設定します。

クラスタ間トランク（ゲートキーパー制御）

クラスタ数が多くなる場合は、クラスタ間非ゲートキーパー制御トランクの代わりに、クラスタ間ゲートキーパー制御トランクを使用する必要があります。ゲートキーパー制御トランクを使用する主な利点は、クラスタとフェールオーバー時間を全体的に管理できることです。非ゲートキーパー制御トランクでは、一般に、トランクのフル メッシュを設定する必要があります。ただし、この作業は、クラスタ数が増加すると管理負担になる場合があります。また、クラスタ内のサブスクライバ サーバが到達不能になった場合は、5 秒（デフォルト）でコールの試行がタイムアウトします。クラスタ全体が到達不能になった場合、コール障害または公衆網を介した再ルーティングのどちらかが発生するまでの試行回数は、トランク用に定義されたリモート サーバの数と、ルート リストまたはルート グループ内のトランクの数によって異なります。リモート サーバと非ゲートキーパー制御トランクの数が多いと、コール遅延が過剰になることがあります。

ゲートキーパー制御トランクを使用する場合は、ゲートキーパーに登録されている他のすべてのクラスタとゲートキーパーを介して通信できるトランクを 1 つだけ設定します。クラスタまたはサブスクライバが到達不能になった場合、ゲートキーパーは自動的に、コールをクラスタ内の別のサブスクライバに送信するか、または他のサブスクライバが存在しなければコールを拒否します。その結果、ほとんど遅延させることなく、公衆網を介して（必要な場合）コールを再ルーティングすることができます。単一の Cisco ゲートキーパーを使用すると、100 のクラスタすべてが、それぞれ 1 つのトランクを、相互にコールできるすべてのクラスタに登録できます。非ゲートキーパー制御トランクを使用する場合、この同じトポロジでは、各クラスタに 99 のトランクを設定する必要があります。クラスタ間ゲートキーパー制御トランクは、他の Cisco CallManager と通信する場合にのみ使用される必要があります。これは、このトランクを他の H.323 デバイスで使用すると、補足サービスに問題が発生する場合があるためです。また、Release 3.2 より前の Cisco CallManager との下位互換性を確保する場合は、クラスタ間ゲートキーパー制御トランクを使用する必要があります。

H.225 トランク（ゲートキーパー制御）

H.225 ゲートキーパー制御トランクは、本質的にはクラスタ間ゲートキーパー制御トランクと同じですが、Cisco CallManager クラスタ Release 3.2 以降のほか、ゲートウェイ、会議システム、およびクライアントなどの他の H.323 デバイスと連携動作する機能を持つ点が異なります。この機能は、コールごとに検出メカニズムを通じて実現されます（この検出プロセスの詳細については、P.5-10 の「Cisco CallManager における H.323 動作」を参照してください）。このタイプのトランクは、すべての Cisco CallManager クラスタが Release 3.2 以降の場合に推奨される H.323 トランクです。

ゲートキーパー トランクの冗長性、復元性、およびロード バランシング

冗長性は、設計の要件に応じて、複数の方法で実現できます。最も簡単に実現するには、ゲートキーパー制御トランクを設定し、そのトランクに割り当てられたデバイス プールに関連付けられている Cisco CallManager 冗長性グループに、最大 3 つのサブスクライバを割り当てます。この設定により、すべてのサーバが、同じテクノロジー プレフィックスと共に、同じゾーン内の同じゲートキーパーに登録されます。ただし、h323_id に使用される H.323 トランクの名前には、「*_n*」というサフィックスが付加されます。ここで、*n* はクラスタ内のノード番号です。この ID は自動的に生成され、変更することはできません。単一のトランクを設定しても、ゲートキーパーは、複数のトランク、つまり Cisco CallManager 冗長性グループ内のサブスクライバごとに 1 つのトランクを登録します。

追加の冗長性要件がある場合は、別のゲートキーパー制御トランクに、Cisco CallManager 冗長性グループにある別の名前と別のサブスクライバを設定できますが、それ以外のパラメータはすべて最初のトランクと同じになります。この 2 つ目のトランクによって、追加のサブスクライバがゲートキーパーに登録されます。

標準のサブスクライバ ペアを構成する 2 つのサーバから Cisco CallManager 冗長性グループを構成し、この冗長性グループを含むデバイス プールを割り当てることをお勧めします（サブスクライバの冗長性の詳細については、P.8-6 の「コール処理サブスクライバ」を参照してください）。クラスタ全体で完全な冗長性を実現するには、4 つの異なるデバイス プールを使用する 4 つのトランクが必要になります。結果的に、8 つのサブスクライバがゲートキーパーに登録されます（3 つのトランクとより大きな冗長性グループを使用しても同じ結果になる場合があります）。

登録時、Cisco CallManager とゲートキーパー間では複数のパラメータが受け渡しされます。Cisco CallManager は、リンクごとに、ゲートキーパーの Registration Admission Status（RAS）メッセージ用に、エフェメラルなユーザ データグラム プロトコル（UDP）ポートを使用します。このポートは、通常であれば、UDP 1719 です。ただし、Cisco CallManager は、特定の RAS メッセージの宛先であるトランクを判別できる必要があります。したがって、Cisco CallManager は一定範囲の UDP ポートを使用して、動的に割り当てます。

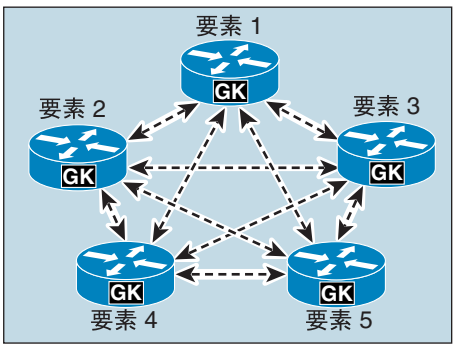
登録プロセス時、トランクは、その Cisco CallManager 冗長性グループにある他のサブスクライバに関する次の情報を登録します。

- H.225 コール シグナリング ポート
- h323_id
- CanMapAlias サポート
- テクノロジー プレフィックス
- H.225 コール シグナリング アドレス

推奨されるクラスタ化ゲートキーパーが使用されている場合、ゲートキーパーは、代替ゲートキーパー アドレスのリストを返します。このリストは、プライマリ ゲートキーパーで障害が発生した場合や使用可能なリソースが不足した場合に使用されることがあります。

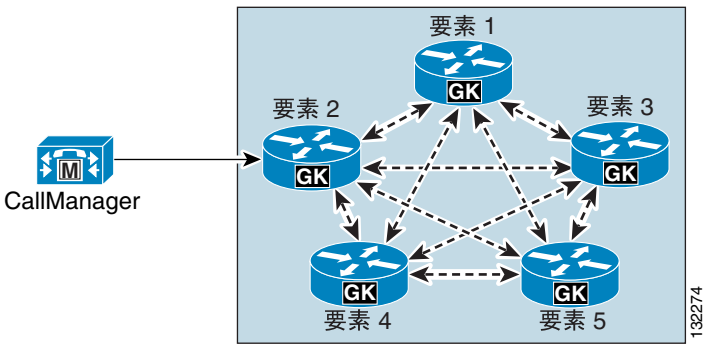
図 5-1 は、Gatekeeper Update Protocol（GUP）を使用して通信する、ゲートキーパーのクラスタを示しています（ゲートキーパーの詳細については、第 8 章「コール処理」を参照してください）。

図 5-1　ゲートキーパー クラスタ



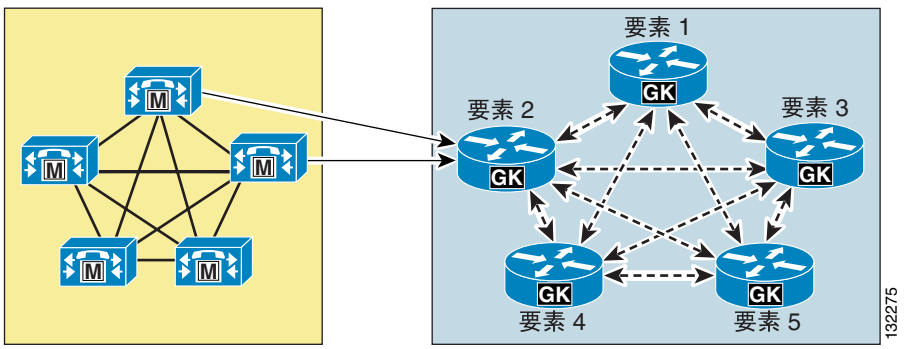
H.323 トランクの Cisco CallManager 冗長性グループにサブスクライバが 1 つだけ含まれている場合、Cisco CallManager の設定済みゲートキーパーとゲートキーパー クラスタの間の接続は 1 つのみになります（図 5-2 を参照）。

図 5-2　単一の Cisco CallManager サブスクライバに対する H.323 トランク



トランクに関連付けられた Cisco CallManager 冗長性グループに複数のサブスクライバが含まれている場合、Cisco CallManager クラスタとゲートキーパー クラスタ間には追加の接続が確立されます（図 5-3 を参照）。

図 5-3　複数の Cisco CallManager サブスクライバに対する 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に使用不能である場合や、結果的にリセットされる場合には、冗長性が確保されません。これは、代替ゲートキーパーのリストがダイナミックであり、データベースに格納されないためです。冗長性のレベルを上げたりロード バランシングを追加したりするには、ゲートキーパー クラスタにある追加のゲートキーパーを Cisco CallManager で設定します。たとえば、元のトランクが要素 2 に登録されている場合は、追加のゲートキーパーを要素 4 として設定できます（図 5-4 を参照）。

図 5-4　ロード バランシングと追加の冗長性のために設定された追加のゲートキーパー

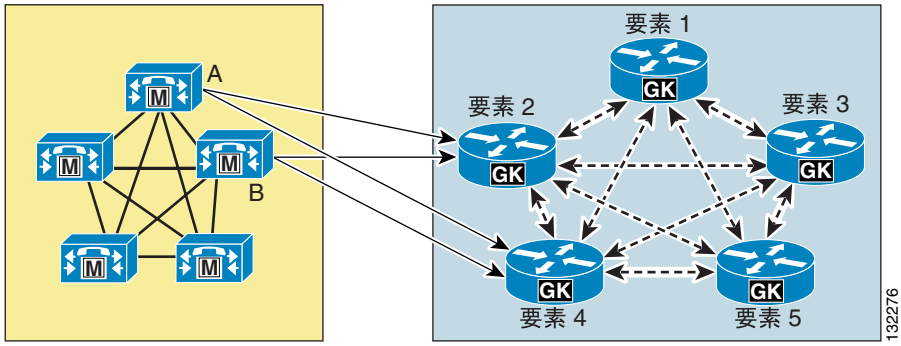


図 5-4 の例の場合、Cisco CallManager の設定には次のコンポーネントが含まれます。

- 要素 2 と要素 4 の 2 つのゲートキーパー
- サブスクライバ サーバ A および B を含む Cisco CallManager 冗長性グループに対して定義された 2 つの H.323 トランク

このアプローチを使用すると、初期設定時に要素 2 または要素 4 が到達不能であっても（つまり、起動中またはトランクのリセット中でも）、引き続き Cisco CallManager クラスタが登録できるようになります。

Cisco CallManager クラスタに着信するコールのロード バランシングは、デフォルトで自動的に行われます。これは、ゲートキーパーが、ゾーン内の登録済みサブスクライバのいずれかをランダムに選択するためです。この動作が期待と異なる場合は、ゲートキーパーで **gw-priority** 設定コマンドを使用して、このデフォルト動作を変更することができます（例 5-1 を参照）。

例 5-1　gw-priority コマンドを使用してコールを特定のトランクに送信する

```
gatekeeper
 zone local SJC cisco.com 10.0.1.10
 zone prefix SJC 1408....... gw-priority 10 sjc-trunk_2
 zone prefix SJC 1408....... gw-priority 9 sjc-trunk_3
 zone prefix SJC 1408....... gw-default-priority 0
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
 endpoint ttl 60
```

例 5-1 では、H.323 トランクは Cisco CallManager で sjc-trunk として設定されています。また、Cisco CallManager サブスクライバが、クラスタ内のサブスクライバのノード番号を示すために、「_2」と「_3」のサフィックスを自動的に付加します。したがって、この例では、最初の選択肢としてノード 2 を使用します。このノードは、このトランクの CallManager 冗長性グループにおいて最もプライオリティの高い Cisco CallManager となる必要があります。このケースでは、ノード 3 は 2 番目の選択肢となります。

gw-default-priority 0 を使用するかどうかは任意です。この例で使用したのは、このゾーンで登録するよう不用意に設定される可能性のある他のトランクが一切使用されないようにするためです。

Cisco CallManager クラスタからの発信コールは、次のいずれかの方法でロードバランスできます。

- ルート グループにある単一の H.323 トランクは、常に、Cisco CallManager 冗長性グループで使用可能な最もプライオリティの高いサブスクライバを使用します。プライオリティの低いサブスクライバが使用されるのは、プライオリティの高いサブスクライバが使用不能になった場合のみです。

- 循環ルート グループにある複数の H.323 トランクは、グループ内のすべての H.323 トランクに均等にコール負荷を分散します。

次の例は、さまざまなシナリオでロード バランシングを設定する方法を示しています。

すべてのコールをクラスタ内の単一のサブスクライバから発信する場合：

- ルート グループ内に単一の H.323 トランクを設定します。

コールをクラスタ内の 4 つのプライマリ サブスクライバに分散する場合：

- 4 つの Cisco CallManager 冗長性グループに対して 4 つの H.323 トランクを定義し、すべてのトランクを循環ルート グループに含めます。
- Cisco CallManager 冗長性グループは、次のように定義されます。
  - サブスクライバ A、サブスクライバ B
  - サブスクライバ C、サブスクライバ D
  - サブスクライバ E、サブスクライバ F
  - サブスクライバ G、サブスクライバ H

  サブスクライバ A、C、E、および G はすべてプライマリで、サブスクライバ B、D、F、および H はバックアップです。

コールをクラスタ内の 8 つのサブスクライバに分散する場合：

- 8 つの異なる Cisco CallManager 冗長性グループに対して 8 つの H.323 トランクを定義し、各グループにサブスクライバを 1 つだけ含め、すべてのトランクを循環ルート グループに含めます。
- Cisco CallManager 冗長性グループは、次のように定義されます。
  - サブスクライバ A
  - サブスクライバ B
  - サブスクライバ C
  - サブスクライバ D
  - サブスクライバ E
  - サブスクライバ F
  - サブスクライバ G
  - サブスクライバ H

メディア ターミネーション ポイントに対する H.323 トランク

メディア ターミネーション ポイント（MTP）は、一般に、H.323 トランクの通常動作には必要ありません。ただし、通信相手となるデバイスが、H.323 Version 1 である場合や、補足サービス用に Empty Capabilities Set（ECS）をサポートしていない場合には必要です。

MTP が必要かどうかをテストするには、次の簡単な手順を使用します。

1. 電話機から H.323 トランクを介して他のデバイスにコールを発信します。このコールは通常どおりに発信する必要があります。
2. コールを保留にしてから、保留解除します。コールがドロップする場合は、Cisco CallManager と他のデバイス間の相互運用性を保証するために MTP を使用することをお勧めします。

MTP は、H.323 トランク上でコールを発信する他のデバイスからのメディア ストリームを終端させる場合や、同じ音声ペイロードでメディア ストリームを再発信する場合に非常に役立ちます。ただし、そのような場合、IP アドレスは MTP のアドレスに変更されます。この事実に留意して、次のシナリオで MTP を使用します。

- 企業内の電話機、ゲートウェイ、および他のデバイスがすべて RFC 1918 プライベート アドレスを使用する場合は、すべての音声およびビデオ デバイスにネットワーク アドレス変換（NAT）を使用しなくても、引き続きパブリック ネットワーク上の他のシステムに接続できます。パブリック ネットワークと通信する Cisco CallManager サブスクライバがパブリック IP アドレスを使用している場合、シグナリングはルーティングされます。また、すべての MTP もパブリック アドレスを使用している場合、RFC 1918 アドレスを持つデバイスからのメディアは MTP で終端され、再度発信されます。ただし、今度は、パブリック ネットワーク上でルーティング可能なパブリック アドレスが割り当てられます。このアプローチを使用すると、RFC 1918 アドレスを持つ何万台ものデバイスが、パブリック ネットワークと通信できるようになります。この同じ方法を使用すると、企業ネットワークにあるデバイスが他の企業またはサービス プロバイダーと通信するときに、そのデバイスの実際の IP アドレスを隠すことができます。
- 信頼性境界を設定すると、ファイアウォールを通過させることや、アクセス コントロール リスト（ACL）を使用したアクセスを許可することができます。通常、メディアがファイアウォールを通過できるようにするには、アプリケーション レイヤ ゲートウェイ（ALG）またはフィックスアップを使用して、動的にメディア ストリームにアクセス許可を与えるか、または、ファイアウォールを越えて通信する必要のある音声デバイスすべてで使用するための広範囲のアドレスおよびポートを割り当てます。H.323 トランクを使用し、ファイルまたは ACL を通過するすべてのコールには、MTP から発信されるメディアが割り当てられます。このメディアでは、単一の IP アドレスまたは狭い範囲の IP アドレスを使用できます。

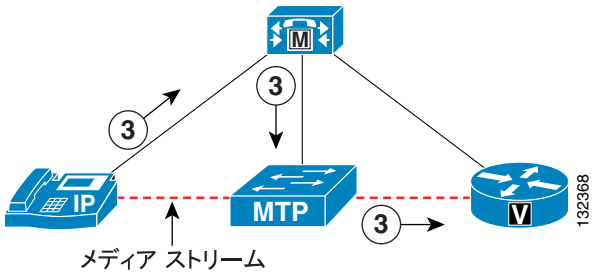
これらの方法を両方使用する場合、**MTP Required** チェックボックスをオンにすると、デフォルトで、H.323 トランク上のコールが許可されます。このことは、MTP リソースが使用不能の場合や、使い果たされた場合でも同様です。このデフォルト動作により、コールの音声パスが使用不能になる場合があります。この動作を変更するには、H.323 セクションにある Cisco CallManager サービス パラメータ **Fail Call if MTP allocation fails** を **True** に設定します。

メディア ターミネーション ポイントに対する SIP トランク

Cisco CallManager は、使用中のプロトコルによって提供されるアウトバンド シグナリング メカニズムを使用して、DTMF 信号を送受信します。メディアがエンドポイント間を直接流れる場合でも、シグナリングは常に Cisco CallManager とエンドポイント間で行われるため、この動作は Session Initiation Protocol（SIP）では多少異なります。SIP では、DTMF を送信する一般的な方法として、RFC 2833 が使用されます。RFC 2833 は、メディア ストリームにおける RTP ペイロードの特定のタイプとして DTMF ディジットを送信します。DTMF ディジットは、コーデックによって符号化されるトーンとしては送信されません。Cisco CallManager が SIP トランクを介して DTMF を検出および送信できるようにするには、SIP トランクに関連付けられた MRGL に、RFC 2833 をサポートする MTP を含める必要があります（詳細については、P.6-9 の「メディア ターミネーション ポイント（MTP）」を参照してください）。

図 5-5 は、Skinny Client Control Protocol（SCCP）を介してアウトバンドで Cisco CallManager に送信されるディジット 3 の DTMF 信号を示しています。この信号は、次に、SCCP を介してアウトバンドで MTP に送信されます。MTP は、次に、DTMF ディジットが 3 であることを示すために、RFC 2833 RTP パケットをメディア ストリームに挿入します。MTP が RFC 2833 RTP パケットを受信した場合は、同じイベントが逆の順序で発生します。この場合、パケットは、メディア ストリームから抽出され、アウトバンドで Cisco CallManager に送信されます。

図 5-5　DTMF シグナリング



Cisco CallManager における H.323 動作

この項では、H.323 プロトコルを Cisco CallManager で使用および実装する方法、および特定の機能が所定どおりに動作する仕組みとその理由について説明します。

理解する上で最も重要な点は、どのサブスクライバがコール シグナリング デーモンを実行するかということです。このデーモンは、H.323 コールを発信および受信する部分的なコードです。これは、通常、H.225 デーモン（H.225D）と呼ばれます。H.225 は、H.323 プロトコルの一部で、主にコール制御を担当します。H.245 は、H.323 のもう 1 つの主要コンポーネントで、コールのメディア制御を担当します。

特定の H.323 デバイスに対する Cisco CallManager 冗長性グループのリストに含まれているサブスクライバによって、デーモンを実行するサブスクライバと実行時期が決定されます。この点は非常に重要です。これは、不適切なサブスクライバに送信されたコールは、別の H.225D によって拒否または処理される場合があるためです。たとえば、この状況が発生するのは、Cisco IOS H.323 ゲートウェイに、Cisco CallManager クラスタ内のサブスクライバ C にコールを送信するダイヤルピアが設定されているものの、そのゲートウェイの Cisco CallManager 冗長性グループのリストにはサブスクライバ A および B しか含まれていない場合です。そのような場合、コールは失敗するか、またはデーモンがサブスクライバ上に設定されていれば H.323 トランク デーモンによって処理されます。

次のシナリオは、H.225D がサブスクライバ上に作成される仕組みとその時期について説明しています。

- H.323 クライアント

  H.225D は、H.323 クライアントに関連付けられた Cisco CallManager 冗長性グループで使用可能な、最もプライオリティの高いサブスクライバ上だけでアクティブになります。

  H.323 クライアントがゲートキーパー制御の場合、RasAggregator デバイスは、ゲートキーパー制御の H.323 クライアントに関連付けられた Cisco CallManager 冗長性グループで使用可能な、最もプライオリティの高いサブスクライバから登録されます。

  RasAggregator は、次の 2 つの特殊機能を提供するためにゲートキーパー ゾーンで登録される特殊なデバイスです。

  - H.323 クライアントが DHCP を使用している場合、Cisco CallManager が DNS を使用しているときは、Cisco CallManager でそのクライアントを使用することはできません。これは、H.323 クライアントでは、ダイナミック DNS をサポートする H.323 クライアントが必要になるためです。RasAggregator を使用すると、Cisco CallManager は、コールを発信するたびに、ゲートキーパーに登録されている特定の H.323 クライアントの IP アドレスを取得できます。ゲートキーパー登録は、H.323 クライアントの E.164 アドレスを含む標準の RAS ARQ メッセージを使用して行われます。ゲートキーパーは、E.164 アドレスを解決し、IP アドレスを ACF メッセージで Cisco CallManager に返します。
  - また、RasAggregator を使用すると、H.323 クライアントによるコールはすべて Cisco CallManager から発信されるようになり、クライアント自身の間では直接やり取りされないことが保証されます。これにより、ダイヤリング規則とコーデック制限が適用されることが保証されます。

- H.323 ゲートウェイ

  H.225D は、H.323 ゲートウェイに関連付けられた Cisco CallManager 冗長性グループにあるすべてのサブスクライバ上でアクティブになります。

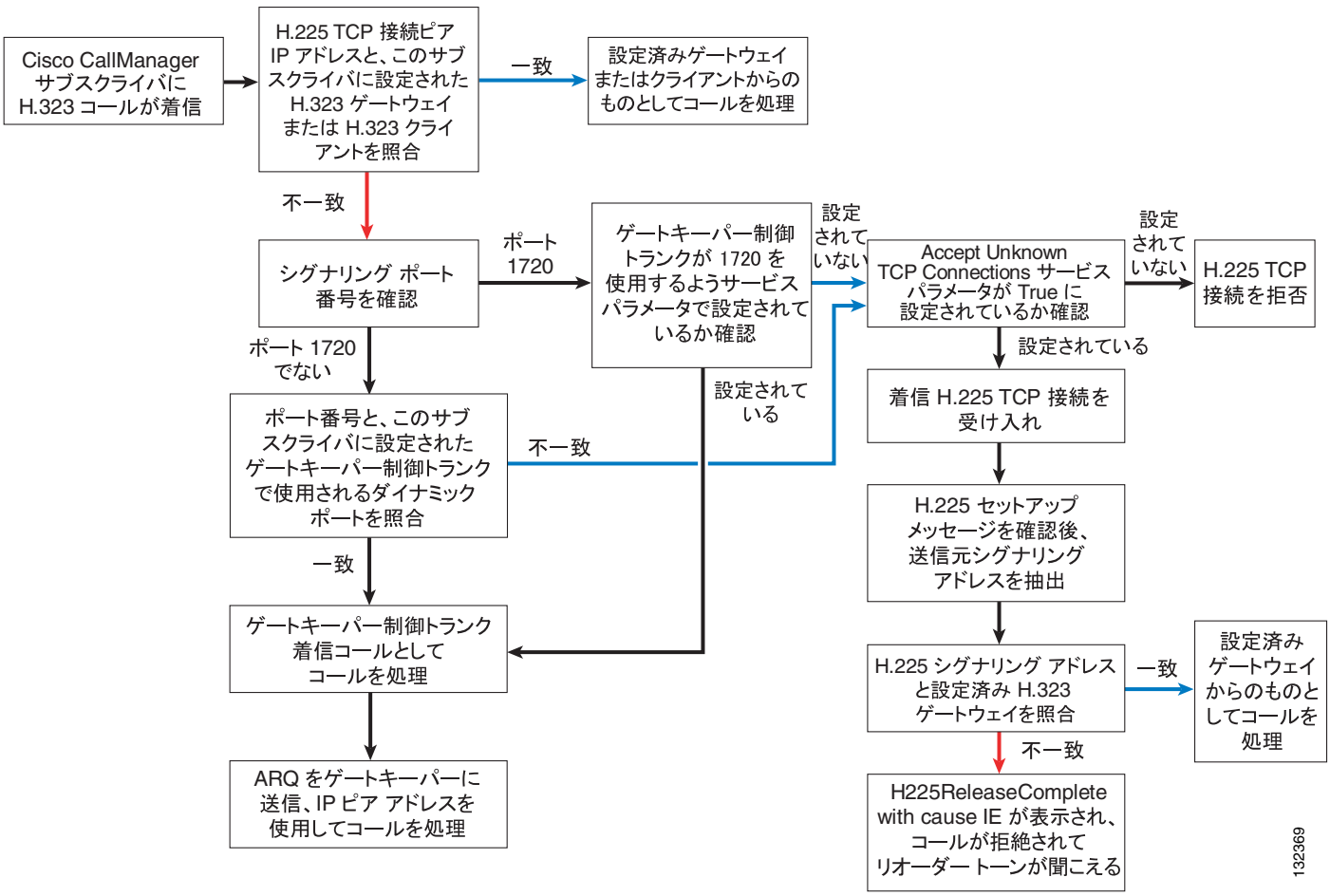
- H.323 トランク

  H.225D は、H.323 トランクに関連付けられた Cisco CallManager 冗長性グループにあるすべてのサブスクライバ上でアクティブになります。

  RAS デーモンは、関連付けられている Cisco CallManager 冗長性グループにあるすべてのサブスクライバから、トランクをゲートキーパーに登録します。

Cisco CallManager クラスタ内のサブスクライバに H.323 コールが着信すると、コールを受け入れるかまたは拒否するか、受け入れる場合はどの H.225D がコールを受信するかなど、さまざまな決定が下されます。図 5-6 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



Cisco CallManager の H.323 プロトコルには、次の追加機能が含まれています。

- Protocol Auto Detect

  この機能では、コールごとに、発信元デバイスが Cisco CallManager Release 3.2 以降を使用しているかどうかを判別できます。コールを受信するたびに、Cisco CallManager は H.225 User-to-User Information Element（UUIE）を検索します。この UUIE は、もう一方の側が別の Cisco CallManager であるかどうかを示します。UUIE が見つかった場合、Cisco CallManager は常に Intercluster Trunk Protocol を使用します。UUIE が見つからない場合は、設定済みのプロトコルをそのデバイスに対して使用します。この機能を使用すると、H.225 ゲートキーパー制御トランクは、コールごとに Intercluster Trunk Protocol と H.225 を切り替えることができます。これにより、Cisco CallManager クラスタと他の H.323 デバイスを組み合せてゲートキーパーを使用することができます。Intercluster Trunk Protocol は、H.225 と類似していますが、特定の機能を Cisco CallManager クラスタ間で正しく動作させる仕組みが異なります。

- Tunneled Q.SIG または H.323 Annex M1

  Cisco CallManager 4.1(3) のリリースから、この機能はすべての H.323 トランク上で有効にできるようになりました。これにより、特定の H.323 Annex M1 機能を、Cisco CallManager クラスタと、同じく H.323 Annex M1 をサポートする他の確認済みシステムとの間に実装することができます。これらの機能には、次のものがあります。

  — パス交換

  — メッセージ待機インジケータ（MWI）

  — コールバック

- 代替エンドポイント

  この機能をサポートするゲートキーパー（Cisco MCM Gatekeeper など）に登録する場合、Cisco CallManager はゲートキーパーに対し、H.323 トランクへのコールの代替宛先を通知できます。この代替エンドポイントまたは代替宛先は、この H.323 トランクが呼び出されたときに、ゲートキーパーによって発信元デバイスに送信されます。代替エンドポイントは、ゲートキーパーに登録されている H.323 トランクに関連付けられた Cisco CallManager 冗長性グループのリストに含まれている他のサブスクライバです。

- 代替ゲートキーパー

  この機能をサポートするゲートキーパーに H.323 トランクが登録される場合（たとえば、Cisco ゲートキーパー クラスタ）、Cisco CallManager には、このゲートキーパーが失敗した場合や独自のリソースを使い果たした場合に、登録、コール アドミッション要求、および他の RAS 機能を処理できる他のゲートキーパーに関する情報が動的に通知されます。

- CanMapAlias

  H.323 トランクは、ゲートキーパーに Admission Request（ARQ; 許可要求）を送信すると、Admission Confirmation message（ACF; アドミッション確認）で異なる E.164 番号を受信する場合があります。このことは、元の着信番号をこの新しい番号で置き換える必要があることを示しています。この機能では、Gatekeeper Transaction Message Protocol（GKTMP）を使用して Cisco ゲートキーパーと通信するルート サーバが必要になります。

  （注） CanMapAlias は、着信番号に関してのみサポートされます。

- 帯域幅要求

  H.323 トランクは、ゲートキーパーの帯域幅情報をアップデートし、特定のコールに割り当てられた帯域幅の要求量が変更されたことを示すことができます。この機能は、デフォルトでは無効になっています。この機能を制御するには、H.323 セクションにある Cisco CallManager サービス パラメータ **BRQ Enabled** を **True** に設定します。この機能は、H.323 トランク上でビデオを使用するときに特に重要です。これは、元の帯域幅要求が許容最大限の量を要求するためです。この機能を有効にすると、コール アドミッション制御が、コールのセットアップ中にネゴシエートされた実際の帯域幅を使用することが保証されます。

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。

この章では、メディア リソースに関する次のトピックについて説明します。

Music On Hold（MOH）メディア リソースの詳細については、第 7 章「Music on Hold」を参照してください。

音声インターフェイス リソース

音声インターフェイスは、時分割多重（TDM）インターフェイス上のレッグと VoIP（Voice over IP）接続上のレッグの 2 つのコール レッグを持つコールに適用されます。TDM レッグは、コーディング/デコーディングとストリームのパケット化を実行するハードウェアで終端する必要があります。この終端機能は、同じハードウェア モジュール、ブレード、またはプラットフォーム上にある Digital Signal Processor（DSP; デジタル シグナル プロセッサ）リソースによって実行されます。Cisco TDM ゲートウェイ上の DSP ハードウェアはすべて、音声ストリームを終端できます。また、特定のハードウェアは、会議やトランスコーディングなどの他のメディア リソース機能を実行することもできます（P.6-8 の「会議」および P.6-9 の「トランスコーディング」を参照）。

表 6-2 ～表 6-6 は、各ハードウェア プラットフォームでサポートできるコールの数を示しています。この数は、ハードウェア上の DSP チップセットのタイプと DSP の個数によって決まります。ハードウェアには、アップグレードおよび変更ができない固定 DSP リソース、またはアップグレード可能なモジュラ DSP リソースのどちらかが搭載されています。表 6-2 ～表 6-6 は、モジュラ（アップグレード可能な）ハードウェアに関する、ハードウェア モジュールごとの DSP の最大数も示しています。

サポートされるコールの数は、コールに使用されるコーデックの計算の複雑度や、DSP に設定された複雑度モードによって異なります。Cisco IOS を使用すると、ハードウェア モジュールの複雑度モードを設定できます。ハードウェア プラットフォームの中には、中複雑度と高複雑度の 2 つの複雑度モードを持つものがありますが、中複雑度と高複雑度のほかにフレックス モードを持つものもあります。

中複雑度モードと高複雑度モード

モジュールでサポートできるコール数を確認するには、表 6-2 ～表 6-6 でモジュールを見つけ、モジュールに搭載できる DSP の個数と、必要なコーデック タイプを確認します。たとえば、フレックス モードに設定された 3 つの C2510 DSP を持つ NM-HD-2VE モジュールは、DSP ごとに 8 つの G.729 コールをサポートできます。合計すると、フレックス モードと G.729 コーデックを使用して 24 コールをサポートできます。フレックス モードで G.711 コーデックを使用する場合は、同じハードウェアで 48 コールをサポートできます。

表 6-1 に示されているように、コーデックが中複雑度モードでサポートされている場合、そのコーデックは高複雑度モードでもサポートされます。ただし、サポートされているコール数は減少します。

各 DSP は、中複雑度モード、高複雑度モード、またはフレックス モード（C5510 のみ）のいずれかとして個別に設定できます。DSP は、コールのコーデックに関する実際の複雑度に関係なく、設定されている複雑度に応じてすべてのコールを処理します。着信コールの実際の複雑度と同じかそれ以上の複雑度が設定されたリソースが使用可能になっている必要があります。そうでない場合、コールは失敗します。たとえば、コールに高複雑度コーデックが必要な場合、DSP リソースが中複雑度モードに設定されていると、コールは失敗します。ただし、高複雑度モードに設定された DSP に対して中複雑度コールが試行された場合、コールは成功し、Cisco IOS は高複雑度モードのリソースを割り当てます。

サポートされているコールの最大数を確認するには、目的のハードウェアを含む表 6-2 ～表 6-6 で該当する行を見つけます。表 6-1 で、中複雑度と高複雑度の列を調べて、目的のコーデックを処理できる複雑度モードを確認します。次に、目的の複雑度モードの列で、DSP ごとにサポートされているコールの最大数を確認します。

フレックス モード

フレックス モードは、C5510 チップセットを使用するハードウェア プラットフォーム上のみで使用可能で、このモードでは、設定時にコーデックの複雑度を指定する必要がありません。フレックス モードの DSP は、処理能力が足りる限り、サポートされているすべてのコーデック タイプのコールを受け入れます。各コールのオーバーヘッドは、Millions of Instructions Per Second（MIPS）単位の処理能力を計算することで動的にトラッキングされます。Cisco IOS は、受信されたコールごとに MIPS の計算を実行し、新しいコールが開始されるたびにそのバジェットから MIPS クレジットを差し引きます。表 6-1 の Flex Mode 列に示されているように、1 つのコールによって消費される MIPS 数は、コールのコーデックによって異なります。着信コールに必要な MIPS 以上の MIPS クレジットが残っている限り、DSP は新しいコールを許可します。表 6-1 の Flex Mode 列は、サポートされているコーデックをコールごとの MIPS 数別に分類し（コールごとに 15、30、または 40 MIPS）、各種ハードウェアに使用可能な MIPS バジェットを示しています。

フレックス モードは、同じハードウェアで複数のコーデックのコールをサポートする必要がある場合に便利です。これは、フレックス モードでは、DSP が中複雑度または高複雑度として設定されている場合よりも多くのコールをサポートできるためです。ただし、フレックス モードではリソースのオーバーサブスクリプションが許可されています。オーバーサブスクリプションになると、すべてのリソースが使用された場合にコール障害が発生するリスクが生じます。フレックス モードを使用すると、物理 TDM インターフェイスを使用する場合よりも DSP リソースの数を削減できます。

たとえば、各 DSP のバジェットは 240 MIPS となり、バジェットの合計は NM-HD-2VE モジュールごとに 720 MIPS となります。NM-HDV2 モジュールの場合、DSP ごとのバジェットは同じく 240 MIPS ですが、使用可能な MIPS の合計数については、選択項目や PVDM の数によって異なるため、表 6-2 で確認してください。

中複雑度モードまたは高複雑度モードと比べると、フレックス モードには、DSP ごとに最も多くの G.711 コールをサポートできるという利点があります。中複雑度モードでは、DSP は 8 つの G.711 コールをサポートできますが、フレックス モードでは 16 の G.711 コールをサポートします。

（注） 製品資料では、さまざまな命名法を使用して DSP を指定しています。たとえば、C5510 は C2510 とも呼ばれます。また、C プレフィックスは、TI5510 や TI549 のように、TI で置き換えられる場合があります。

音声インターフェイスの DSP リソース

表 6-2 ～表 6-6 は、DSP チップセット別に分類されており、DSP サポートに関する情報を、プラットフォーム、DSP 密度、および DSP ごとにサポートされる音声インターフェイス（またはコール）の数別に示しています。表 6-1 は、ハードウェア モジュールでサポートされるコーデックを複雑度モードごとに示しています。

表 6-1　サポートされるコーデック（複雑度モード別）

中複雑度	高複雑度	フレックス モード
G.711（A-law、mu-law）	G.711（A-law、mu-law）	*コールごとに 15 MIPS の場合：* • G.711（A-law、mu-law） • FAX/ モデム パススルー • クリア チャネル *コールごとに 30 MIPS の場合：* • G.726（32K、24K、16K） • GSM-FR • FAX リレー • G.729 • G.729（a、b、ab） *コールごとに 40 MIPS の場合：* • G.728 • G.723.1（32K、24K、16K） • G.723.1a（5.3K、6.3K） • GSM-EFR • モデム リレー
FAX/ モデム パススルー	FAX/ モデム パススルー	
クリア チャネル	クリア チャネル	
G.726（32K、24K、16K）	G.726（32K、24K、16K）	
GSM-FR	GSM-FR	
FAX リレー	FAX リレー	
G.729（a、ab）	G.729	
	G.729（a、b、ab）	
	G.728	
	G.723.1（32K、24K、16K）	
	G.723.1a（5.3K、6.3K）	
	GSM-EFR	
	モデム リレー	

C5510 チップセットをベースとするハードウェアは、中複雑度モードと高複雑度モードのほか、フレックス モードをサポートします（表 6-2 を参照）。

表 6-2　C5510 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュールまたはシャーシ	DSP 構成	DSP およびモジュールごとの音声インターフェイス（コール）の最大数		
		中複雑度（DSP ごとに 8 コール）	高複雑度（DSP ごとに 6 コール）	フレックス モード[1]（DSP ごとに 240 MIPS）
VG-224	4 DSP で固定	適用対象外	プラットフォームごとに 24 コール サポートされるコーデック： • G.711（A-law、mu-law） • G.729a	適用対象外
NM-HD-1V[2]	1 DSP で固定	NM ごとに 4 コール	NM ごとに 4 コール	NM ごとに 240 MIPS
NM-HD-2V	1 DSP で固定	NM ごとに 8 コール	NM ごとに 6 コール	NM ごとに 240 MIPS
NM-HD-2VE	3 DSP で固定	NM ごとに 24 コール	NM ごとに 18 コール	NM ごとに 720 MIPS
NM-HDV2	次の DSP を 1 ～ 4 つ：	PVDM ごとのコール数：	PVDM ごとのコール数：	PVDM ごとの MIPS：
NM-HDV2-2T1/E1	PVDM2-8[3]（½ DSP）	4	3	120
NM-HDV2-1T1/E1	PVDM2-16（1 DSP）	8	6	240
	PVDM2-32（2 DSP）	16	12	480
	PVDM2-48（3 DSP）	24	18	720
	PVDM2-64（4 DSP）	32	24	960

表 6-2　C5510 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース（続き）

ハードウェア モジュールまたはシャーシ	DSP 構成	DSP およびモジュールごとの音声インターフェイス（コール）の最大数		
		中複雑度（DSP ごとに 8 コール）	高複雑度（DSP ごとに 6 コール）	フレックス モード[1]（DSP ごとに 240 MIPS）
2801	次の DSP を 1 ～ 2 つ：	PVDM ごとのコール数：	PVDM ごとのコール数：	PVDM ごとの MIPS：
2811	PVDM2-8[3]（½ DSP）	4	3	120
	PVDM2-16（1 DSP）	8	6	240
	PVDM2-32（2 DSP）	16	12	480
	PVDM2-48（3 DSP）	24	18	720
	PVDM2-64（4 DSP）	32	24	960
2821	次の DSP を 1 ～ 3 つ：	PVDM ごとのコール数：	PVDM ごとのコール数：	PVDM ごとの MIPS：
2851	PVDM2-8[3]（½ DSP）	4	3	120
	PVDM2-16（1 DSP）	8	6	240
	PVDM2-32（2 DSP）	16	12	480
	PVDM2-48（3 DSP）	24	18	720
	PVDM2-64（4 DSP）	32	24	960
3825	次の DSP を 1 ～ 4 つ：	PVDM ごとのコール数：	PVDM ごとのコール数：	PVDM ごとの MIPS：
3845	PVDM2-8[3]（½ DSP）	4	3	120
	PVDM2-16（1 DSP）	8	6	240
	PVDM2-32（2 DSP）	16	12	480
	PVDM2-48（3 DSP）	24	18	720
	PVDM2-64（4 DSP）	32	24	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 6-1 を参照）。
2. NM-HD-1V モジュールを使用する場合、音声インターフェイス（コール）の数は、モジュール上の物理ポートの数によって制限されます。
3. PVDM2-8 のキャパシティは C5510 の半分です。

C5421 チップセットをベースとするハードウェアでは、DSP が中複雑度または高複雑度として設定されている場合があります。表 6-3 は、DSP ごとのコール密度を、表 6-1 は、複雑度モードごとにサポートされるコーデックを示しています。

表 6-3　C5421 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュール	DSP 構成	DSP およびモジュールごとのコールの最大数	
		中複雑度（DSP ごとに 8 コール）	高複雑度（DSP ごとに 8 コール）
NM-HDA-4FXS	2 DSP で固定	NM ごとに 16 コール	NM ごとに 8 コール
	または		
	1 つの DSP-HDA-16（4 DSP）で固定	NM ごとに 16 コール	NM ごとに 16 コール
AIM-VOICE-30 AIM-ATM-VOICE-30	4 DSP で固定	AIM ごとに 30 または 60 コール	AIM ごとに 16 または 30 コール

C549 チップセットをベースとするハードウェアでは、DSP が中複雑度または高複雑度として設定されている場合があります。表 6-4 は、DSP ごとのコール密度を、表 6-1 は、複雑度モードごとにサポートされるコーデックを示しています。

表 6-4　C549 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュール	DSP 構成	DSP およびモジュールごとのコールの最大数	
		中複雑度（DSP ごとに 4 コール）	高複雑度（DSP ごとに 2 コール）
NM-HDV NM-HDV-FARM	1 ～ 5 つの PVDM-12（PVDM-12 ごとに 3 つの DSP）	NM ごとに 12、24、36、48、または 60 コール	NM ごとに 6、12、18、24、または 30 コール
1751[1]	次の DSP を 1 ～ 2 つ：	NM ごとのコール数：	NM ごとのコール数：
1760	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）	4 または 8 8 または 16 12 または 24 16 または 32 20	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）
- GSM-FR
- FAX リレー
- G.729
- G.729（a、b、ab）
- G.728
- G.723.1（32K、24K、16K）
- G.723.1a（5.3K、6.3K）
- GSM-EFR
- モデム リレー

表 6-5 は、DSP ごとのコール密度を示しています。

表 6-5　C542 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュール[1]	DSP 構成	DSP およびモジュールごとのコールの最大数
NM-1V	2 DSP で固定	DSP ごとに 1 コール NM ごとに 2 コール
NM-2V	4 DSP で固定	DSP ごとに 1 コール NM ごとに 4 コール

1. これらのモジュールは、複雑度モードを備えていませんが、すべてのコーデックを均等にサポートします。

表 6-6 は、DSP リソースに対応する非 IOS ハードウェアを示しています。すべての非 IOS ハードウェア プラットフォームでは、DSP 構成が固定されています（表 6-6 を参照）。

表 6-6　非 IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュールまたはプラットフォーム	DSP 構成	DSP およびモジュールごとのコールの最大数	サポートされるコーデック
WS-6608-T1 WS-6608-E1	64 の C549 で固定 （ポートごとに 8 つの DSP）	DSP ごとに 2 コール モジュールごとに 256 コール[1]	G.711 A-law、mu-law G.729a
WS-6624-FXS	12 の C549 で固定	DSP ごとに 2 コール モジュールごとに 24 コール	G.711 A-law、mu-law G.729a
VG-248	12 の C5409 で固定	DSP ごとに 4 コール プラットフォームごとに 48 コール	G.711 A-law、mu-law G.729a
WS-SVC-CMM-ACT	4 つの Broadcom 1500 で固定	DSP ごとに 32 コール モジュールごとに 128 コール	G.711（10-30 ms） G.729（10-60 ms） G.723（30-60 ms）
WS-SVC-CMM-6T1	12 の C5441 で固定	DSP ごとに 15 コール モジュールごとに 144 コール	G.711（10、20、30 ms） G.729（10、20、30、40、50、60 ms）
WS-SVC-CMM-6E1	12 の C5441 で固定	DSP ごとに 15 コール モジュールごとに 180 コール	G.711（10、20、30 ms） G.729（10、20、30、40、50、60 ms）
WS-SVC-CMM-24FXS	3 の C5441 で固定	DSP ごとに 15 コール モジュールごとに 24 コール	G.711 A-law、mu-law G.729 G.729a
ATA-188[2]	1 つの Komodo 3880 で固定	プラットフォームごとに 2 コール	G.711 A-law、mu-law G.729

1. 物理ポートの数に基づいて、T1 の場合は最大 192 コール、E1 の場合は最大 240 コールが可能です。T1 または E1 に対して DSP が設定されていない場合は、最大 256 の DSP リソースが使用可能です。
2. ATA モジュールには複雑度が定義されていません。このモジュールは G.711、G.729、および G.723 のみをサポートします。

会議、トランスコーディング、および MTP リソース

ここでは、次のタイプのメディア リソースについて説明します。

会議

コンファレンス ブリッジとは、複数の参加者を 1 つのコールに参加させるリソースです。そのデバイス上で 1 つの会議に許可される最大ストリーム数まで、所定の会議用に任意の数の接続を受け入れることができます。会議に接続されているメディア ストリームと、その会議に接続されている参加者との間には、1 対 1 の対応があります。コンファレンス ブリッジは、ストリームを混合し、接続されている通話者ごとに固有の出力ストリームを作成します。所定の通話者の出力ストリームは、接続されている全通話者からのストリームの合成から、当事者の入力ストリームをマイナスしたものです。一部のコンファレンス ブリッジは、会議で通話量が最も多い 3 名の通話者だけを混合し、その合成ストリーム（通話量が最も多い通話者の 1 人である場合は、当事者の入力ストリームをマイナスしたもの）を各参加者に配信します。

コンファレンス ブリッジ リソースには、次の 2 つの主要なタイプがあります。

- ソフトウェア コンファレンス ブリッジ

  ソフトウェア ユニキャスト コンファレンス ブリッジは、G.711 音声ストリームと Cisco Wideband オーディオ ストリームを混合できる標準の会議ミキサーです。Wideband または G.711 A-law および mu-law ストリームの任意の組み合せが、同じ会議に接続される場合があります。所定の会議でサポートできる通話者数は、コンファレンス ブリッジ ソフトウェアが実行されるサーバと、そのデバイスの設定によって決まります。

- ハードウェア コンファレンス ブリッジ

  ハードウェア コンファレンス ブリッジは、ソフトウェア コンファレンス ブリッジのすべての機能を備えています。さらに、一部のハードウェア コンファレンス ブリッジは、G.729、GSM、G.723 などの複数の低ビット レート（LBR）ストリーム タイプをサポートできます。この機能により、一部のハードウェア コンファレンス ブリッジが混合モードの会議を処理できるようになります。混合モードの会議では、ハードウェア コンファレンス ブリッジは、G.729、GSM、および G.723 のストリームを G.711 ストリームにトランスコードし、混合します。その後、混合したストリームを、ユーザに戻すために適切なストリーム タイプにエンコードします。一部のハードウェア コンファレンス ブリッジは、G.711 会議しかサポートしません。

Cisco CallManager の制御下にあるすべてのコンファレンス ブリッジは、Cisco CallManager との通信に Skinny Client Control Protocol（SCCP）を使用します。

Cisco CallManager は、Cisco CallManager クラスタに登録されている会議リソースから、コンファレンス ブリッジを割り当てます。ハードウェアとソフトウェアの両方の会議リソースは、同時に Cisco CallManager に登録でき、Cisco CallManager は、どちらのリソースからでも、コンファレンス ブリッジを割り当て、使用することができます。Cisco CallManager は、会議割り当て要求を処理するときに、これらのコンファレンス ブリッジのタイプを区別しません。

トランスコーディング

トランスコーダは、あるコーデックの出力ストリームを取り、別のコーデック タイプ用の入力ストリームにリアルタイムで変換する（トランスコードする）デバイスです。つまり、トランスコーダは、ある圧縮タイプのストリームを、別の圧縮タイプのストリームに変換します。

トランスコーダは、G.711 音声ストリームを、G.729a などの低ビット レート（LBR）圧縮音声ストリームに変換できます。この変換は、低速 IP WAN を介した Cisco IP Interactive Voice Response（IVR）、音声メッセージング、電話会議などのアプリケーションを使用可能にする場合に非常に重要です。さらに、トランスコーダはメディア ターミネーション ポイント（MTP）の機能を備えているので、必要に応じて H.323 エンドポイント用の補足サービスを使用可能にするのにも使用できます。

表 6-8 は、各プラットフォームでサポートされているコーデック タイプごとの MTP とトランスコーディング セッションの最大数をリストしています。

IP テレフォニー システムを大企業の環境へスケーリングするには、ハードウェア会議が必要です。表 6-7 に示されているハードウェア プラットフォームの音声モジュールの DSP リソースは、大規模システムに必要なハードウェア会議機能を提供し、次の特性をサポートします。

- MRG（メディア リソース グループ）と MRGL（メディア リソース グループ リスト）を使用して、Cisco CallManager は、クラスタ内の Cisco CallManager サーバ間でハードウェア会議ポートの共有を可能にします。
- Cisco CallManager は、Skinny Client Control Protocol（SCCP）を使用して、ハードウェア コンファレンス ブリッジと情報を交換しますが、これらのプラットフォーム上のゲートウェイ サービスはメディア ゲートウェイ コントロール プロトコル（MGCP）を使用する場合があります。

ハードウェア MTP リソースには、次のガイドラインが適用されます。

- 一部のリソース（たとえば、Cisco 会議リソース）には、G.711 音声ストリームのみを使用する機能があります。
- 音声ストリームを圧縮する場合は、G.711 以外のコーデックを使用してください。
- 圧縮された音声ストリームを、G.711 のみをサポートするデバイスに接続する場合、ハードウェア ベースの MTP とトランスコーディング サービスを使用して、圧縮された音声ストリームを G.711 に変換してください。

メディア ターミネーション ポイント（MTP）

メディア ターミネーション ポイント（MTP）は、2 つの全二重 G.711 ストリームを受け入れるエンティティです。MTP は、この 2 つのメディア ストリームをブリッジします。また、これらのメディア ストリームは、個々にセットアップと終了ができるようになります。ある接続の入力ストリームから受信されるストリーミング データは、他の接続の出力ストリームに渡され、逆も同様です。また、MTP は、A-law から mu-law への、およびその逆のトランスコーディングを行うことや、パケット化にかかる時間が異なる（使用するパケット サイズが異なる）2 つの接続をブリッジすることもできます。さらに、MTP は、RFC 2833 サポートなどのコール処理を行うこともできます。

MTP は、補足サービスに使用され、EmptyCapabilitiesSet 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。必要に応じて、MTP が割り当てられ、H.323 エンドポイントに代わってコールに接続されます。メディア ストリームは、挿入された後、MTP と H.323 デバイス間で接続され、これらの接続は、コールの期間中、存在します。MTP のもう一方の側に接続されるメディア ストリームは、保留、転送などの機能を実行するために、必要に応じて接続されたり、接続解除されたりします。

(注) Release 3.2 より前の Cisco CallManager を実装する場合は MTP を使用して H.323 エンドポイントに補足サービスを提供する必要がありますが、Cisco CallManager Release 3.2 以降を実装する場合は、MTP リソースを使用してこの機能を提供する必要はありません。

MTP には、次の 2 つの主要なタイプがあります。

- ソフトウェア MTP

  ソフトウェア MTP とは、サーバに Cisco IP Voice Media Streaming Application をインストールすることによって設定されるデバイスです。インストールされたアプリケーションが、MTP アプリケーションとして設定されると、そのアプリケーションは、Cisco CallManager ノードに登録され、サポートする MTP リソース数を Cisco CallManager に知らせます。ソフトウェア MTP デバイスは、G.711 ストリームだけをサポートします。

  Cisco IOS Enhanced ソフトウェア デバイスを Cisco IOS ルータに実装する場合、DSP ファームでソフトウェア専用の MTP を設定できます。この DSP ファームは、単純な MTP としてのみ使用でき、ルータ上のハードウェア DSP を必要としません。

- ハードウェア MTP

  ハードウェア MTP とは、Cisco CallManager の外部のハードウェア上にある DSP ベースのリソースです。トランスコーダには MTP 機能があります。実際、ハードウェア MTP は、MTP として使用されるトランスコーダです。ハードウェア デバイスは、トランスコーダとして Cisco CallManager ノードに登録され、サポートするリソース数を Cisco CallManager に知らせます。トランスコーダ機能を持つハードウェア MTP は、G.711 以外のストリームを受け入れることができます。

SIP RFC 2833 サポートに対する MTP

SIP の仕様で規定されているとおり、SIP エンドポイントには、DTMF ディジットとコール進捗音をメディア ストリームでインバンドで送信する機能があります。DTMF トーンは、修正された RTP パケットとして RTP ストリームで送信されます。Cisco CallManager Release 4.1 の時点で、Skinny Client Control Protocol（SCCP）エンドポイントにはこの機能がありません。したがって、Cisco CallManager システムと SIP システムを統合するには、メディア ストリームに MTP を挿入し、SIP インバンド シグナリングを SCCP アウトバンド シグナリングに、またはその逆に変換する必要があります。

Cisco CallManager Release 4.1 の時点で、ソフトウェアとハードウェアはどちらも RFC 2833 をサポートできます。Ad-hoc Conferencing and Transcoding（ACT）Port Adapter の最小コード バージョン 12.3(8)XY2 と Cisco IP Voice Media Streaming Application はどちらも RFC 2833 をサポートします。

SIP トランクを通過するコール用に MTP をプロビジョニングする必要があります。2 つの Cisco CallManager クラスタが SIP トランクを介して接続されている場合、各クラスタにはこの用途のための独自の MTP リソースが必要です。ソフトウェア MTP は、この用途専用のデュアル CPU サーバに実装されると、512 のストリームをサポートできます。

MTP、会議、およびトランスコーディングに対するハードウェア リソース

これらの機能を実装するためのリソースは、ハードウェアベースにすることも、ソフトウェアベースにすることもできます。ソフトウェア リソースは、Cisco CallManager サーバまたは Cisco IOS プラットフォーム上に常駐できます。また、ハードウェア プラットフォームは、Cisco IOS または Cisco Catalyst プラットフォームのどちらかになります。この項では、使用可能なすべてのリソースでサポートされるストリームのコーデック タイプと数について要約します。これらのリソースは、ゲートウェイ上で DSP ファームとして設定され、Cisco CallManager によって SCCP プロトコルを介して使用されます。ゲートウェイは、リソースの制御と割り当てを担当します。

これらの機能のサポートは、ハードウェア プラットフォーム、Cisco CallManager のバージョン、および Cisco IOS のバージョンによって異なります。表 6-7 は、モジュールおよびプラットフォームで MTP、会議、およびトランスコーディングをサポートするのに必要な最小のソフトウェア リリースを示しています。さまざまな Cisco IOS プラットフォームでサポートされるメディア リソース モジュールの数とタイプを確認する場合は、表 6-11 を使用してください。各表は、メディア リソースをサポートするモジュールのみを示しています。

（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。DSP ファームのサービスは、Cisco Survivable Remote Site Telephony（SRST）または Cisco CallManager Express ではサポートされません。

表 6-7　会議、トランスコーディング、および MTP に対する最小のソフトウェア リリース

Cisco プラットフォーム	モジュール	MTP	会議とトランスコーディング
2691 および 2600XM 2811、2821、および 2851 3640、3640A、および 3660 3725 および 3745 3825 および 3845	NM-HD-1V NM-HD-2V NM-HD-2VE	Cisco CallManager 4.0(1) Cisco IOS： • 12.3(8)T4 • 12.3(11)T（3800 シリーズの場合）	Cisco CallManager 3.3(4) または 4.0(1) Cisco IOS： • 12.3(11)T（3800 シリーズの場合） • 12.3(8)T4（それ以外のリスト項目の場合）
2691 および 2600XM 2811、2821、および 2851 3725 および 3745 3825 および 3845	NM-HDV2 NM-HDV2-1T1/E1 NM-HDV2-2T1/E1	Cisco CallManager 4.0(1) Cisco IOS： • 12.3(8)T4 • 12.3(11)T（3800 シリーズの場合）	Cisco CallManager 3.3(4) または 4.0(1) Cisco IOS： • 12.3(11)T（3800 シリーズの場合） • 12.3(8)T4（それ以外のリスト項目の場合）
VG200 2691 および 2600XM 2650 および 2651 2811、2821、および 2851 3640、3640A、および 3660 3725 および 3745 3825 および 3845	NM-HDV NM-HDV-FARM	適用対象外	Cisco CallManager 3.2(2c) Cisco IOS： • 12.1(5)YH（VG200 を HDV-FARM と併用する場合） • 12.2(13)T（リスト中の 2600 シリーズ、3600 シリーズ、および VG200 を HDV と併用する場合）

表 6-7　会議、トランスコーディング、および MTP に対する最小のソフトウェア リリース（続き）

Cisco プラットフォーム	モジュール	MTP	会議とトランスコーディング
1751、1,751V、および 1760	PVDM-256K	適用対象外	Cisco CallManager 3.3(4) Cisco IOS 12.3(2)XE
2801	PVDM2-8 PVDM2-16 PVDM2-32 PVDM2-48 PVDM2-64	Cisco CallManager 4.1 Cisco IOS 12.3(11)T	Cisco CallManager 4.1 Cisco IOS 12.3(11)T PVDM2-8 に対応する会議はなし
2811、2821、および 2851	PVDM2-8 PVDM2-16 PVDM2-32 PVDM2-48 PVDM2-64	Cisco CallManager 3.3(5) または 4.1 Cisco IOS 12.3(8)T4	Cisco CallManager 3.3(5) または 4.1 Cisco IOS 12.3(8)T4 PVDM2-8 に対応する会議はなし

次の項で説明するように、C549 プラットフォームでのリソースの割り当て処理は、C5510 プラットフォームの場合と異なります。

音声インターフェイスまたは DSP ファームへのリソースの割り当て

モジュール上の DSP リソースは、音声トランク グループの音声インターフェイスとして、または DSP ファームとして設定できます。DSP ファームでは、DSP を会議またはトランスコーディング /MTP のどちらかに割り当てることができます。表 6-8 は、各コンファレンス ブリッジでサポートできる参加者の数と、モジュールごとにサポートされる会議セッションの数を示しています。同様に、表 6-9 は、DSP およびモジュールごとにサポートされるトランスコーディング セッションの数を示しています。また、表 6-10 は、DSP およびモジュールごとにサポートされる MTP セッションの数を示しています。モジュール上で使用可能な DSP の個数を確認する場合は表 6-2 ～表 6-6 を使用し、シャーシでサポートできる NM モジュールの最大数を確認する場合は表 6-11 を使用してください。これら各種の表を使用すると、配置に必要なハードウェア構成を確認できます。

（注） モジュールでサポートできるコールまたはセッションの数は、そのモジュール上の特定の DSP 構成によって異なります。表 6-8 ～表 6-10 は、モジュール タイプごとに使用可能な多数の DSP 構成のごく一部を示しています。他の DSP 構成について調べる場合や、DSP 構成でサポートできるコールまたはセッションの数を計算する場合は、http://www.cisco.com/cgi-bin/Support/DSP/cisco_dsp_calc.pl にアクセスして、Cisco DSP Calculator を使用します（Cisco.com へのログインが必要です）。

表 6-8　DSP およびモジュールごとにサポートされる電話会議の数

ハードウェア モジュールまたはシャーシ	DSP 構成	会議	
		すべての参加者が G.711（A-law、mu-law）を使用する場合	1 名以上の参加者が G.729 または G.729a を使用する場合
NM-HDV2 （会議ごとに 8 名の参加者）	次の DSP を 1 ～ 4 つ： PVDM2-8[1]（½ DSP） PVDM2-16（1 DSP） PVDM2-32（2 DSP） PVDM2-48（3 DSP） PVDM2-64（4 DSP）	PVDM ごとの会議数： 4 8 16 24 32 NM ごとに最大 50 の会議	PVDM ごとの会議数： 1 2 4 6 8
NM-HD-1V （会議ごとに 8 名の参加者）	1 DSP で固定	NM ごとに 8 つの会議	NM ごとに 2 つの会議
NM-HD-2V （会議ごとに 8 名の参加者）	1 DSP で固定	NM ごとに 8 つの会議	NM ごとに 2 つの会議
NM-HD-2VE （会議ごとに 8 名の参加者）	3 DSP で固定	NM ごとに 24 の会議	NM ごとに 6 つの会議
NM-HDV NM-HDV-FARM （会議ごとに 6 名の参加者）	1 ～ 5 つの PVDM-12（PVDM-12 ごとに 3 つの DSP）	NM ごとに 3、6、9、12、または 15 の会議	NM ごとに 3、6、9、12、または 15 の会議
1751[2] （会議ごとに 6 名の参加者）	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）	DSP ごとに 1 つの会議 シャーシごとに最大 5 つの会議	DSP ごとに 1 つの会議 シャーシごとに最大 5 つの会議
1760 （会議ごとに 6 名の参加者）	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）	DSP ごとに 1 つの会議 シャーシごとに最大 20 の会議	DSP ごとに 1 つの会議 シャーシごとに最大 20 の会議
WS-6608-T1 および WS-6608-E1 （会議ごとに 3 ～ 32 名の参加者）	64 の C549 で固定 （ポートごとに 8 つの DSP）	ポートごとに 32 名の参加者	ポートごとに 32 名の参加者 G.729a のみ

表 6-8　DSP およびモジュールごとにサポートされる電話会議の数（続き）

ハードウェア モジュールまたはシャーシ	DSP 構成	会議	
		すべての参加者が G.711（A-law、mu-law）を使用する場合	1 名以上の参加者が G.729 または G.729a を使用する場合
WS-SVC-CMM-ACT （会議ごとに 64 名の参加者）	4 つの Broadcom 1500 で固定	モジュールごとに 128 の会議	モジュールごとに 128 の会議
Cisco IP Voice Media Streaming Application （会議ごとに 3 ～ 64 名の参加者）	適用対象外	共存サーバごとに 48 名の参加者	適用対象外

1. PVDM2-8 のキャパシティは C5510 の半分です。
2. 1751 は、最大 5 つの会議をサポートします。

表 6-9　DSP およびモジュールごとにサポートされるトランスコーディング セッションの数

ハードウェア モジュールまたはシャーシ	DSP 構成	G.711 のトランスコーディングの対象		
		G.711（A-law、mu-law）	G.729a G.729ab GSM-FR	G.729 G.729b GSM-EFR
NM-HDV2	次の DSP を 1 ～ 4 つ： PVDM2-8[1]（½ DSP） PVDM2-16（1 DSP） PVDM2-32（2 DSP） PVDM2-48（3 DSP） PVDM2-64（4 DSP）	PVDM ごとのセッション数： 32 64 128 192 256	PVDM ごとのセッション数： 4 8 16 24 32	PVDM ごとのセッション数： 3 6 12 18 24
NM-HD-1V	1 DSP で固定	NM ごとに 16 セッション	NM ごとに 8 セッション	NM ごとに 6 セッション
NM-HD-2V	1 DSP で固定	NM ごとに 16 セッション	NM ごとに 8 セッション	NM ごとに 6 セッション
NM-HD-2VE	3 DSP で固定	NM ごとに 48 セッション	NM ごとに 24 セッション	NM ごとに 18 セッション
NM-HDV NM-HDV-FARM	1 ～ 5 つの PVDM-12（PVDM-12 ごとに 3 つの DSP）	NM ごとに 12、24、36、48、または 60 セッション	NM ごとに 12、24、36、48、または 60 セッション	NM ごとに 12、24、36、48、または 60 セッション
1751[2]	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）	DSP ごとに 2 セッション シャーシごとに最大 16 セッション	DSP ごとに 2 セッション シャーシごとに最大 16 セッション	DSP ごとに 2 セッション シャーシごとに最大 16 セッション

表 6-9　DSP およびモジュールごとにサポートされるトランスコーディング セッションの数（続き）

ハードウェア モジュールまたはシャーシ	DSP 構成	G.711 のトランスコーディングの対象		
		G.711（A-law、mu-law）	G.729a G.729ab GSM-FR	G.729 G.729b GSM-EFR
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）	DSP ごとに 2 セッション シャーシごとに最大 20 セッション	DSP ごとに 2 セッション シャーシごとに最大 20 セッション	DSP ごとに 2 セッション シャーシごとに最大 20 セッション
WS-6608-T1 および WS-6608-E1	64 の C549 で固定 （ポートごとに 8 つの DSP）	ポートごとに 24 セッション	ポートごとに 24 セッション	ポートごとに 24 セッション
WS-SVC-CMM-ACT	4 つの Broadcom 1500 で固定	モジュールごとに 128 セッション	モジュールごとに 128 セッション	モジュールごとに 128 セッション

1. PVDM2-8 のキャパシティは C5510 の半分です。
2. 1751 は、最大 16 のトランスコーディング セッションをサポートします。

表 6-10　DSP およびモジュールごとにサポートされる MTP セッションの数

ハードウェア モジュールまたはシャーシ	DSP 構成	MTP G.711（A-law、mu-law）
NM-HDV2	次の DSP を 1 ～ 4 つ： PVDM2-8[1]（½ DSP） PVDM2-16（1 DSP） PVDM2-32（2 DSP） PVDM2-48（3 DSP） PVDM2-64（4 DSP）	PVDM ごとのセッション数： 8 16 32 48 64
NM-HD-1V	1 DSP で固定	NM ごとに 4 セッション
NM-HD-2V	1 DSP で固定	NM ごとに 16 セッション
NM-HD-2VE	3 DSP で固定	NM ごとに 48 セッション
WS-6608-T1 および WS-6608-E1	64 の C549 で固定 （ポートごとに 8 つの DSP）	ポートごとに 24 セッション
WS-SVC-CMM-ACT	4 つの Broadcom 1500 で固定	モジュールごとに 256 セッション

1. PVDM2-8 のキャパシティは C5510 の半分です。

NM-HDV（C549 ベースのハードウェア）におけるリソースの割り当て

各 DSP は個別に設定でき、各 DSP 機能は相互に独立して設定できます。会議、トランスコーディング、および MTP リソースは、別々の DSP に割り当てる必要があります。また、単一の DSP で一度にサポートできる DSP 機能は 1 つのみです。設定によって、各 DSP が実行する機能が指定されます。

1 つの NM-HDV モジュールに関連付けることのできる Cisco CallManager は 1 つのみです。

NM-HDV2、NM-HD-*xx*、および PVDM2（C5510 ベースのハードウェア）におけるリソースの割り当て

C5510 チップセットをベースとするハードウェア リソースは、リソース タイプを定義する DSP プロファイルを使用して割り当てられます。プロファイルには DSP ファームが関連付けられているため、DSP は特定のリソース タイプとして定義されません。

DSP ファームの DSP は、複数の Cisco CallManager によって使用される場合があります。

NM-HDV の DSP 要件の計算

音声アクティビティ検出（VAD）を有効または無効にしたサンプル レート 20、30、40、60 ms の場合（または、VAD を有効にした 10 ms の場合）、PVDM を 5 台フル装備した NM-HDV または NM-HDV-FARM を構成して、使用可能な DSP リソースを 60 得ることが可能です。

所定のアプリケーションに必要な DSP の個数を計算するには、必要な会議の数、音声インターフェイス用の DSP の個数、およびトランスコーディング セッション用の DSP の個数を加算します。トランスコーディングに必要な DSP の個数は、必要なトランスコーディング セッション数を 4 で除算して、その結果を切り上げた整数と等しくなります。

PVDM の固定構成では DSP を 3 個備えているので、必要な PVDM 数は、DSP の個数を 3 で除算して、その結果を切り上げた整数と等しくなります。

最後に、必要な NM-HDV または NM-HDV-FARM モジュールの数は、PVDM 数を 5 で除算して、その結果を切り上げた整数と等しくなります。

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

DSP リソースのプラットフォーム サポート

Cisco 2800 および 3800 シリーズ

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 によって代わりに提供されるためです。

ネットワーク モジュール

NM-HDV2、NM-HD-*xx*、および NM-HDV モジュールは、表 6-11 に示されている Cisco IOS プラットフォームに取り付けることができます。その場合の最大モジュール数は、表のとおりです。

表 6-11 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。

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 と NM-HDV-FARM モジュールを同じシャーシ内で組み合せることができますが、常にすべてのシャーシがこれらのモジュールを完全に収容できるわけではありません。表 6-11 では、各タイプのハードウェア プラットフォームがサポートする最大モジュール数を示しています。

表 6-11　Cisco IOS プラットフォームごとの最大モジュール数

Cisco IOS プラットフォーム	スロット数	プラットフォームでサポートされるモジュール		
		NM-HDV2	NM-HD-1V NM-HD-2V NM-HD-2VE	NM-HDV NM-HDV-FARM
VG200[1] 2600[2] 3620[3]	1 1 2	N	N	Y
2600XM、2691	1	Y	Y	Y
3640	3	N	N	Y
3660	6	N	Y	Y
3725	2	Y	Y	Y
3745	4	Y	Y	Y
2811	1	Y	Y	Y
2821	1	Y	Y	Y
2851	1	Y	Y	Y
3825	2	Y	Y	Y
3845	4	Y	Y	Y

1. VG200 は、Cisco 2610 ルータに置き換えられたので、販売終了になりました。VG200 の既存のモデルは、引き続き IP テレフォニー設置環境でご使用いただけます。
2. IP テレフォニー アプリケーションには、Cisco 2600XM ルータを使用してください。Cisco 2600 ルータのメモリの考慮事項については、次の Web サイトの製品情報をご覧ください。
http://www.cisco.com/warp/customer/cc/pd/rt/2600/prodlit/1675_pp.htm
3. 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 つのみです。

ソフトウェア会議

ソフトウェア会議サービスは、Cisco IP Voice Media Streaming Application です。また、これは、Cisco CallManager 用に認定された任意のプラットフォームで実行されます（認定プラットフォームのリストについては、第 8 章「コール処理」を参照してください）。このアプリケーションは、次のデバイス タイプのいずれかとして動作し、Cisco CallManager に登録されるように設定できます。デバイス タイプは、ソフトウェア コンファレンス ブリッジ、メディア ターミネーション ポイント（MTP）、Annunciator、および Music On Hold（MOH）サーバです。

Cisco IP Voice Media Streaming Application は、IP Voice Media Streaming Driver を使用して、リアルタイムの音声メディア ストリーミングを実行します。また、このアプリケーションは、アプリケーション自体と IP Voice Media Streaming Driver の両方の設定情報も取得します。ソフトウェア コンファレンス ブリッジは、G.711 コーデックだけをサポートするので、電話会議にトランスコーディングが不要の単一サイトに最も適しています。スケジューリング機能を必要としないソフトウェア会議サービスには、比較的拡張が容易なソリューションです。

ソフトウェア コンファレンス ブリッジには、次の特性があります。

- G.711（A-law または mu-law）および Cisco Wideband をサポート
- Ad Hoc 会議の参加者は最大 64 名、Meet-Me 会議の参加者は最大 128 名
- 低ビット レート（LBR）コールはすべて、電話会議に参加する前にトランスコーディングされなければならない

（注） G.711 以外のコーデックを使用するコールがソフトウェア コンファレンス ブリッジに参加する場合は、別のトランスコーダ リソースが使用可能になっている必要があります。

Annunciator

Annunciator は Cisco IP Voice Media Streaming Application のソフトウェア機能で、これを使用すると、音声メッセージや各種のコール進捗音をシステムからユーザに流すことができます。この機能は、複数の片方向 RTP ストリームを Cisco IP Phone やゲートウェイなどのデバイスに送信できます。さらに、SCCP メッセージを使用して、RTP ストリームを確立します。この機能を使用するには、デバイスが SCCP に対応している必要があります。トーンとアナウンスは、システムで事前に定義されています。アナウンスでは、ローカリゼーションがサポートされています。また、適切な .wav ファイルを置き換えて、アナウンスをカスタマイズすることもできます。Annunciator は、トランスコーディング リソースを使用しないで、G.711 A-law および mu-law、G.729、および Wideband コーデックをサポートすることができます。

次の機能には、Annunciator リソースが必要です。

- Cisco Multilevel Precedence Preemption（MLPP）

  この機能には、次のようなコール障害の状態に応じて再生されるストリーミング メッセージが用意されています。

  - 優先順位の高い既存のコールが原因で、プリエンプション処理できない。
  - 優先順位アクセス制限に到達した。
  - 試行された優先順位レベルが許可されていない。
  - 着信番号が、プリエンプション処理またはコール ウェイティングに対応していない。
- SIP トランクを介した統合

  SIP エンドポイントには、トーンを生成し、RTP ストリームでインバンドで送信する機能があります。SCCP デバイスにはこの機能がないため、SIP エンドポイントと統合した場合、DTMF トーンの生成または受け入れ時には Annunciator と MTP が併用されます。次のタイプのトーンがサポートされます。

  - コール進捗音（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、コール進捗音（リングバック トーン）のサポートが必要です。
- システム メッセージ

  次のようなコール障害の状態では、システムはエンドユーザにストリーミング メッセージを再生します。

  - ダイヤル番号をシステムが認識できない。
  - サービスが中断したためコールがルーティングされない。
  - 番号が通話中で、その番号がプリエンプション処理またはコール ウェイティング用に設定されていない。

- 会議

  電話会議の間、システムは、参加者がブリッジに参加、またはブリッジから退出したことをアナウンスするときに、割り込み音を再生します。

Cisco IP Voice Media Streaming Application をサーバ上でアクティブにすると、Annunciator がシステム内に自動的に作成されます。Media Streaming Application を非アクティブにすると、Annunciator も削除されます。単一の Annunciator インスタンスは、パフォーマンス要件を満たす場合は、Cisco CallManager クラスタ全体にサービスを提供できます（P.6-19 の「Annunciator のパフォーマンス」を参照）。そうでない場合は、追加の Annunciator をクラスタ用に設定する必要があります。追加の Annunciator を設定するには、クラスタ内の他のサーバ上で Cisco IP Voice Media Streaming Application をアクティブにします。

Annunciator は、そのデバイス プールで定義されたとおり、一度に 1 つの Cisco CallManager に登録されます。デバイス プールに対してセカンダリが設定されている場合、Annunciator は自動的にセカンダリ Cisco CallManager にフェールオーバーします。障害発生時に再生されるアナウンスはいずれも保持されません。

Annunciator はメディア デバイスと見なされるため、メディア リソース グループ（MRG）に含めて、電話機およびゲートウェイで使用される Annunciator の選択を制御することができます。

Annunciator のパフォーマンス

デフォルトでは、Annunciator は 48 のストリームを同時にサポートするように設定されています。この設定値は、Cisco CallManager サービスを含む同一のサーバ（共存）上で動作する Annunciator に推奨される最大値です。サーバの接続性が 10 Mbps しかない場合は、設定を下げて同時ストリームを 24 にします。

Cisco CallManager サービスを含まないスタンドアロン サーバでは、最大 255 のアナウンス ストリームを同時にサポートできます。デュアル CPU と高性能ディスク システムを持つ高性能サーバでは、最大 400 のストリームをサポートできます。複数のスタンドアロン サーバを追加して、必要な数のストリームをサポートすることができます。

Cisco IP Voice Media Streaming Application

Cisco IP Voice Media Streaming Application は、ソフトウェアに次のリソースを組み込みます。

- Music On Hold（MOH）
- Annunciator
- ソフトウェア コンファレンス ブリッジ
- メディア ターミネーション ポイント（MTP）

Media Streaming Application をアクティブにすると、上記の各リソースが 1 つずつ自動的に設定されます。Annunciator、ソフトウェア コンファレンス ブリッジ、または MTP が必要ない場合は、Cisco IP Voice Media Streaming Application の Run Flag サービス パラメータを無効にして、これらのリソースを無効にすることをお勧めします。

複数のリソースが必要になる状況や、それらのリソースによって Media Streaming Application にかかる負荷を慎重に検討してください。各リソースには、処理可能な接続の最大数を制御するサービス パラメータと、関連付けられたデフォルト設定があります。デフォルト設定を変更しない限り、4 つのリソースすべてを同じサーバ上で実行できます。ただし、配置においてデフォルトを超える数のリソースが 1 つでも必要になった場合は、そのリソースを独自の専用サーバ上で実行するように設定します（そのサーバ上では、その他すべてのリソースおよび Cisco CallManager サービスを実行しないでください）。

会議のガイドラインとアプリケーションのシナリオ

ここでは、次の Cisco IP テレフォニー配置モデルに関する、会議リソースのガイドラインを説明します。

すべての配置モデル用の会議ガイドライン

- ユーザ用に少なくとも次の会議リソースを用意することをお勧めします。
  - ユーザ ベースの 5% 以上に相当する Ad Hoc 会議リソース
  - ユーザ ベースの 5% 以上に相当する Meet-Me 会議リソース
- 一般に、メディア リソース グループ（MRG）とメディア リソース グループ リスト（MRGL）を使用して、複数の Cisco CallManager 間でリソースを共有し、ロード バランシングを行います。MRG と MRGL を使用しない場合、リソースは、1 つの Cisco CallManager からしか使用できません。
- また、MRG と MRGL を使用すると、地理的なロケーションに基づいてリソースを分離できます。その結果、WAN 帯域幅を節約できる場合もあります。
- 会議リソースのタイプによって、単一のブリッジにおける参加者の最大数の制限が異なります（表 6-8 を参照）。MRGL に複数のリソースが定義されている場合は、使用可能な最初のリソースが使用されます。参加者の最大数は、次の 2 つの Cisco Callmanager サービス パラメータによって制御されます。Maximum Ad Hoc Conferences の値の範囲は 3 ～ 64 で、Maximum Meet Me Conference Unicast の値の範囲は 1 ～ 128 です。デフォルト設定はどちらも 4 です。会議リソースの参加者の最大数によって、サービス パラメータの設定値が上書きされます。

  コンファレンス ブリッジのサイズを最大にするには、サービス パラメータを、MRGL 内のリソースの最小ブリッジ サイズと一致するように設定します。別の方法としては、同じ特性のリソースだけを使用してブリッジ サイズを最大にし、そのサイズと一致するようにサービス パラメータを設定します。
- CTI アプリケーションと Drop Any Party 機能では、16 を超える参加者はサポートされません。Ad Hoc 会議リソースの中には 16 を超える参加者をサポートできるものもありますが、このアプリケーションに表示される参加者は、最新の 16 名のみです。

単一サイト配置用の会議ガイドライン

単一サイト配置では、音声トラフィックは IP WAN を通過しません。1 つのタイプのコーデック（通常、G.711）だけが使用されます。したがって、このタイプの配置には、電話会議用のトランスコーディング リソースが必要ないので、ソフトウェア会議を使用できます。より多くの会議キャパシティが必要な場合は、ハードウェア会議リソースを追加できます。

単一サイト配置には、次のガイドラインが適用されます。

- このモデルでは、音声トラフィックは IP WAN を通過しません。したがって、1 つのタイプのコーデック（通常、G.711）を使用してください。トランスコーディング リソースは必要ありません。
- ソフトウェアとハードウェアのどちらの会議でも使用できます。ただしソフトウェア会議は、小規模な配置のみに使用してください。

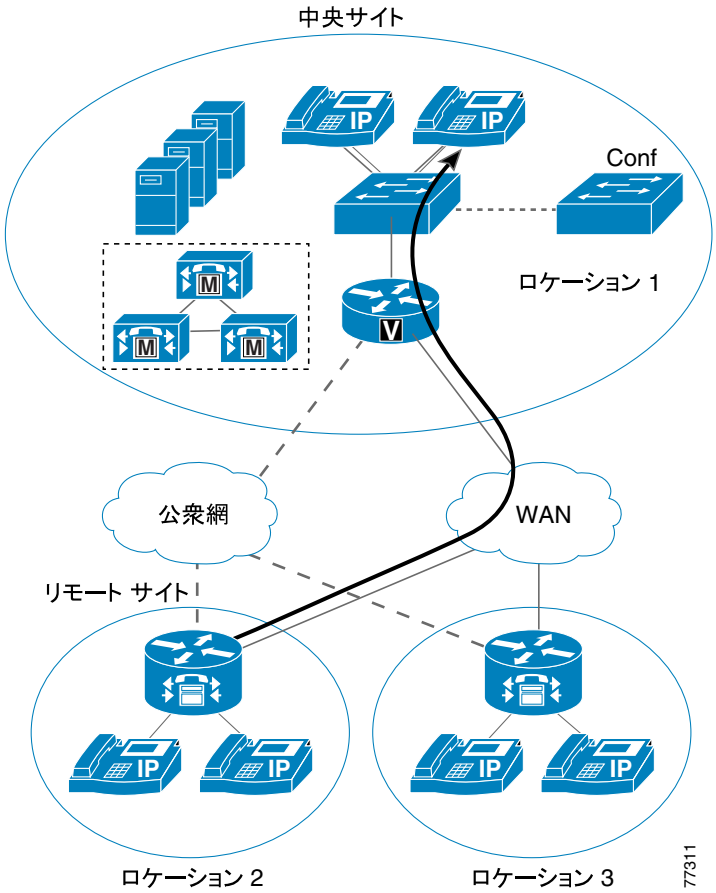
集中型コール処理を使用するマルチサイト WAN 配置用の会議ガイドライン

このモデルでは、コール処理は中央サイトでローカライズされます。MTP、トランスコーディング、および会議の各サービスは、中央で処理するか、分散させるか、または両方を組み合せることもできます。

- メディア リソースが中央に集中する場合
  - これらのリソースの 1 つを使用するすべてのコールで、WAN が使用されます。
  - リソースを中央に配置すると、ローカル コールも WAN を通過するので、帯域幅の使用量に対する影響を検討する必要があります（第 9 章「コール アドミッション制御」を参照）。
- メディア リソースが分散される場合
  - あるリモート サイトが別のリモート サイトにあるリソースを使用できないように、そのロケーションに基づいてリソースを MRGL にグループ化してください。この方法は、サイト間のコール アドミッション制御を管理するのに役立ちます。
  - 複数のタイプのコーデックと、G.729 をサポートしない任意のデバイスがクラスタに含まれている場合は、ハードウェア会議リソースを使用してください。現時点で、Cisco デバイスはすべて、両方のコーデック タイプをサポートできます。Cisco Customer Response Solution（CRS）Release 3.0 以降は、G.729 または G.711 をサポートできますが、同一のインストールで両方をサポートすることはできません。

すべての集中型コール処理配置では、Cisco CallManager のロケーション メカニズムを使用して、コール アドミッション制御を提供します。Cisco CallManager は、リージョンと連携させてロケーションを使用して、ネットワーク リンクの特性を指定します。リージョンは、リンクで使用される圧縮のタイプを定義します。ロケーションは、リンクに使用可能な帯域幅の量を定義します。図 6-1 は、音声コールに割り当てられる帯域幅の量によって制限されるロケーションを使用した、一般的な集中型コール処理モデルを示しています。帯域幅の制限があるので、この設定のリージョンは、G.729 などの低ビット レート（LBR）コーデックを使用します。各 LBR コールは、G.711 に必要な 80 kbps ではなく、約 24 kbps を使用します。

図 6-1　集中型コール処理配置用のロケーションベースのコール アドミッション制御



メディア リソース グループとメディア リソース グループ リスト

Cisco CallManager のメディア リソース グループとメディア リソース グループ リストを使用すると、リモート サイトの会議リソースを提供して、WAN 上の帯域幅使用量を最小限に抑えることができます（図 6-2 を参照）。WAN 帯域幅がオーバーサブスクリプションにならないように、ロケーションに基づくコール アドミッション制御が引き続き必要です。

図 6-2　集中型コール処理配置における会議リソースのローカライズ

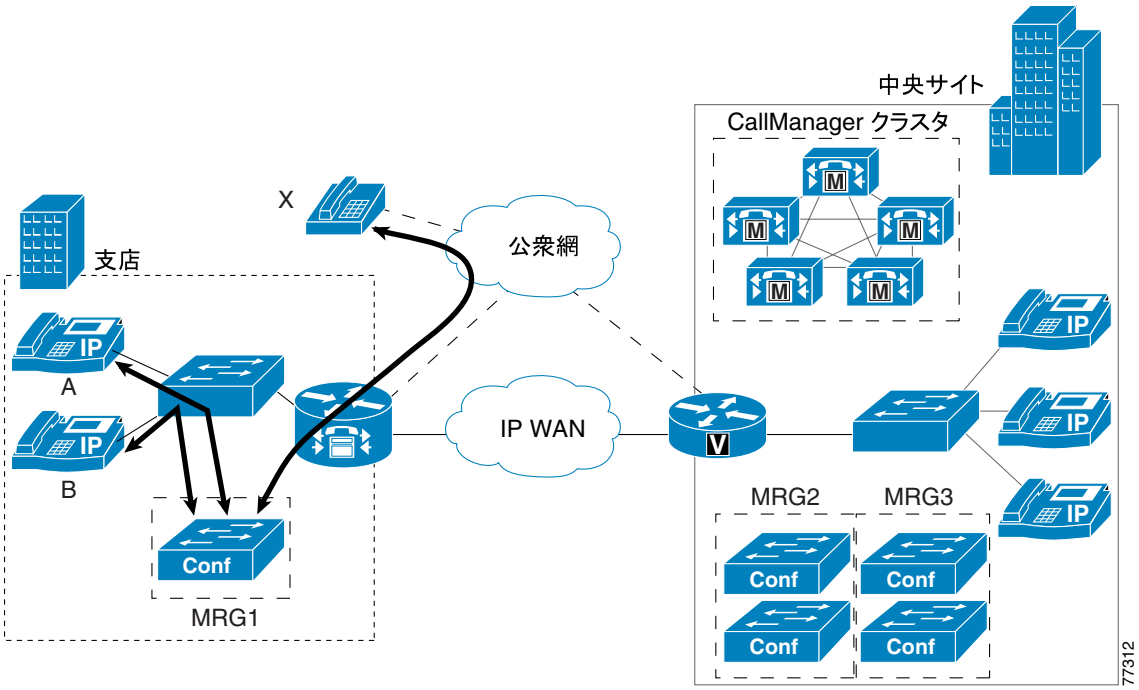


図 6-2 では、支店のリモート サイトにある電話機には、メディア リソース グループ MRG1 が登録されているメディア リソース グループ リスト（MRGL）が割り当てられています。このグループには、そのサイトのコンファレンス ブリッジ リソースが登録されています。この設定では、WAN 帯域幅を使用しないでそのサイト内で電話会議が可能になります。たとえば、Phone X が Phone A にコールし、Phone A が Phone B と電話会議を行うと想定します。この時点で、Cisco CallManager は、電話会議をホストするために、会議リソースを要求します。MRG と MRGL が設定されているので、Cisco CallManager は、この電話会議用に支店サイトのコンファレンス ブリッジを選択します。

Cisco CallManager におけるメディア リソースの割り当て

Cisco CallManager がメディア リソース グループ（MRG）内のリソースをどのように割り当てるかを理解することが、非常に重要です。上記で説明したように、MRG は、メディア リソース グループ リスト（MRGL）に含まれ、MRGL は、デバイス プールに関連付けられます。リソースを割り当てる場合、Cisco CallManager はまず、MRGL で指定されている順序に従って、適切な MRG を選択します。MRG 内のリソースは、MRG にリソースが追加された順番に関係なく、名前のアルファベット順にリストされます。Cisco CallManager は、リストされている順（つまり、アルファベット順）にリソースを MRG から割り当てます。したがって、リソースの優先順位順の割り当てが必要な場合（たとえば、ソフトウェア コンファレンス ブリッジより前に、ハードウェア コンファレンス ブリッジ）、MRG でこれらのリソースに適切な名前を付け、適切な MRGL を設定して、必要な順序を指定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 配置用の会議ガイドライン

分散型コール処理配置では、IP WAN を介して複数のサイトが接続されます。各サイトには、Cisco CallManager クラスタなどの独自のコール処理エンティティが含まれ、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。また、この場合、一般に WAN 帯域幅が制限されるので、サイト間コールは、WAN を通過するときに低ビット レート コーデック（たとえば、G.729）を使用するように設定されます。

分散型コール処理配置には、次のガイドラインが適用されます。

- このモデルでは、各サイトの Cisco CallManager クラスタに、独自の会議リソースがある場合があります。
- 各クラスタは、複数のタイプのコーデックを使用する可能性があります。一般に、クラスタ間の WAN 上では G.729、クラスタ内では G.711 です。
- 複数の Cisco CallManager クラスタ間での会議では、会議主催者の ID により、どの会議リソースが電話会議に割り当てられるかが決まります（図 6-3 を参照）。
- WAN を通過するストリームの本数は、会議の主催者、およびその他の参加者のロケーションによって異なります。主催者と別のクラスタ内にいる各参加者は、WAN 上のストリームを追加し、そのストリームは、主催者のクラスタ内のリソースで終端します。コール アドミッション制御を設定する際には、これらの要素を考慮してください（第 9 章「コール アドミッション制御」を参照）。
- 1 つのクラスタ内では、会議の参加者の最大数は、リソースのタイプと、サービス パラメータの設定値で決まります。ただし、参加者が複数のクラスタから参加する場合、電話会議では最大数を超える可能性があります。1 つのクラスタ内では、会議の主催者だけが参加者を追加できます。しかし、会議の主催者とは所属クラスタが異なる会議参加者は、自身のクラスタ内に使用可能な会議リソースがあれば、参加者を追加できます。こうした電話会議が拡張できるのは、着信コールが別のクラスタ内の既存会議の一部であることをクラスタが認識せず、各クラスタはその最大数の参加者を追加できるからです。

図 6-3 は、複数の Cisco CallManager クラスタにまたがって会議リソースが割り当てられる仕組みの例を示しています。

図 6-3　分散型コール処理配置用のリソースのローカライズ

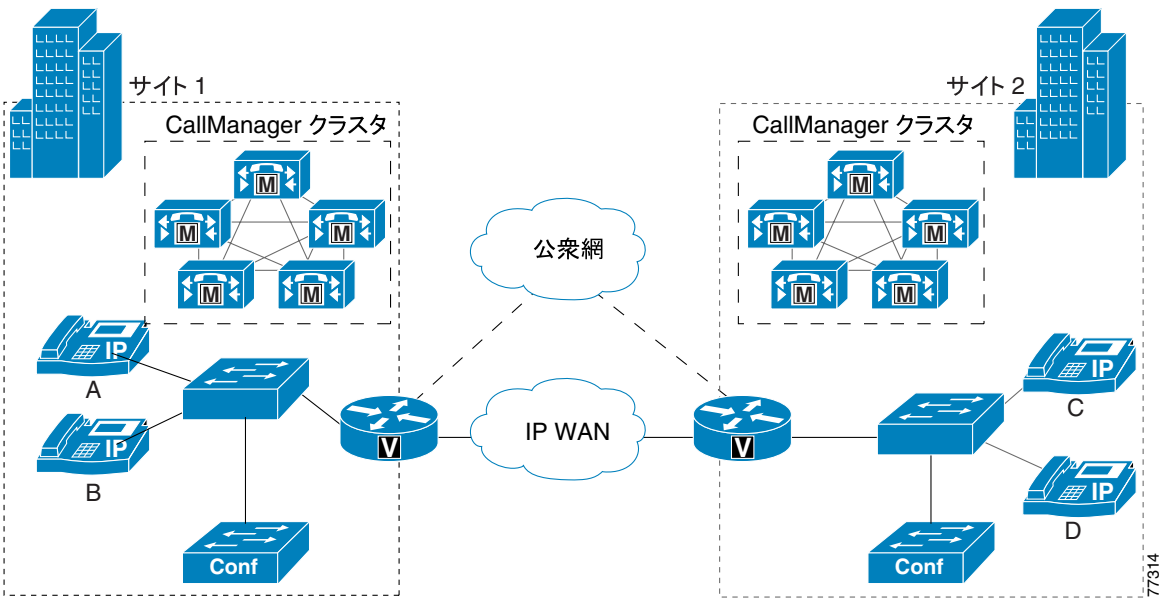


図 6-3 では、サイト 1 とサイト 2 の 2 つの Cisco CallManager クラスタが、IP WAN とクラスタ間トランクを通じて接続されます。各サイトには、MRG と MRGL を使用して個々の IP Phone に割り当てられる独自の会議リソースがあります。

サイト 1 の Phone A がサイト 2 の Phone C にコールした後、サイト 2 の Phone D に会議コールをすると想定します。会議の開始者はサイト 1 の Cisco CallManager クラスタによって制御されるので、このコールに割り当てられるコンファレンス ブリッジは、サイト 1 に置かれているコンファレンス ブリッジです。つまり、WAN を通過する 2 つのストリーム、つまり、Phone A と Phone C 間のストリームと、Phone A と Phone D 間のストリームがあります。一方、サイト 2 の Cisco CallManager クラスタによって制御される Phone C によって会議が開始された場合、そのコールには、サイト 2 に置かれているコンファレンス ブリッジが割り当てられ、（Phone C と Phone A 間の）1 つのストリームだけが、WAN を通過します。

電話会議が複数の Cisco CallManager クラスタにまたがる場合は、各クラスタで定義された参加者の最大数を超える可能性があります。図 6-3 に基づいて、次の例を検証します。

サイト 1 の Phone A が、サイト 1 にあるコンファレンス ブリッジを使用して、サイト 2 の Phone C を含む 6 名の通話者による電話会議をセットアップするとします。両方のクラスタのサービス パラメータは、会議サイズが 6 名の参加者に制限されるように設定されています。ここで、Phone C は、サイト 2 のコンファレンス ブリッジを使用して、別の 5 名の通話者用に別の電話会議をセットアップし、この 2 つの会議を「結合」することができます（すべての音声ストリームを受け入れるのに十分な帯域幅があることを前提とします）。

（注） MRGL 内のすべてのリソースが使用された場合、Cisco CallManager は、デフォルトの MRG、つまり <None> MRG 内でメディア リソースを探します。

ソフトウェア MTP リソース

ソフトウェア MTP リソースには、次のガイドラインが適用されます。

- トランスコーディングを通常必要としない単一サイト配置に適しています。
- 単一サイト配置では、ソフトウェア MTP リソースは、H.323v2 に準拠していないデバイス（たとえば、バージョン 3.1 より前の Microsoft NetMeeting）をサポートするためだけに必要です。
- IP Voice Media Streaming Application は、コール処理を担当するパブリッシャ、または任意の Cisco CallManager 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。MTP セッションによる CPU 負荷が増加すると、コール処理のパフォーマンスに悪影響が発生する可能性があります。ユーザ データグラム プロトコル（UDP）トラフィックは、Cisco CallManager サーバ上で受信されなければならないので、セキュリティ上の問題が発生する恐れがあります。

トランスコーディングのガイドラインとアプリケーションのシナリオ

ここでは、MTP リソースとトランスコーディング リソースが、どこで、いつ使用されるかを説明します。具体的には、次の 3 つの企業 IP テレフォニー配置のモデルと、4 つ目のアプリケーション シナリオで示します。

- P.6-26 の「単一サイト配置」は、1 つのサイト内の 1 つ以上のコール処理エージェントから構成され、音声トラフィックは IP WAN を介して伝送されません。
- P.6-26 の「集中型コール処理を使用するマルチサイト WAN 配置」は、IP WAN を通じて接続された複数のサイトにサービスを提供する、単一のコール処理エージェントから構成されます。
- P.6-28 の「分散型コール処理を使用するマルチサイト WAN 配置」は、IP WAN を通じて接続される複数のリモート サイトのそれぞれに置かれている、コール処理エージェントから構成されます。
- P.6-29 の「IP 公衆網アクセス」は、MTP リソースを必要とするもう 1 つのシナリオです。このアクセスは、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。MTP リソースが必要なもう一つの状況は、単一サイトが IP 公衆網プロバイダーを介して公衆網にアクセスする場合です（P.6-29 の「IP 公衆網アクセス」を参照）。

集中型コール処理を使用するマルチサイト WAN 配置

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

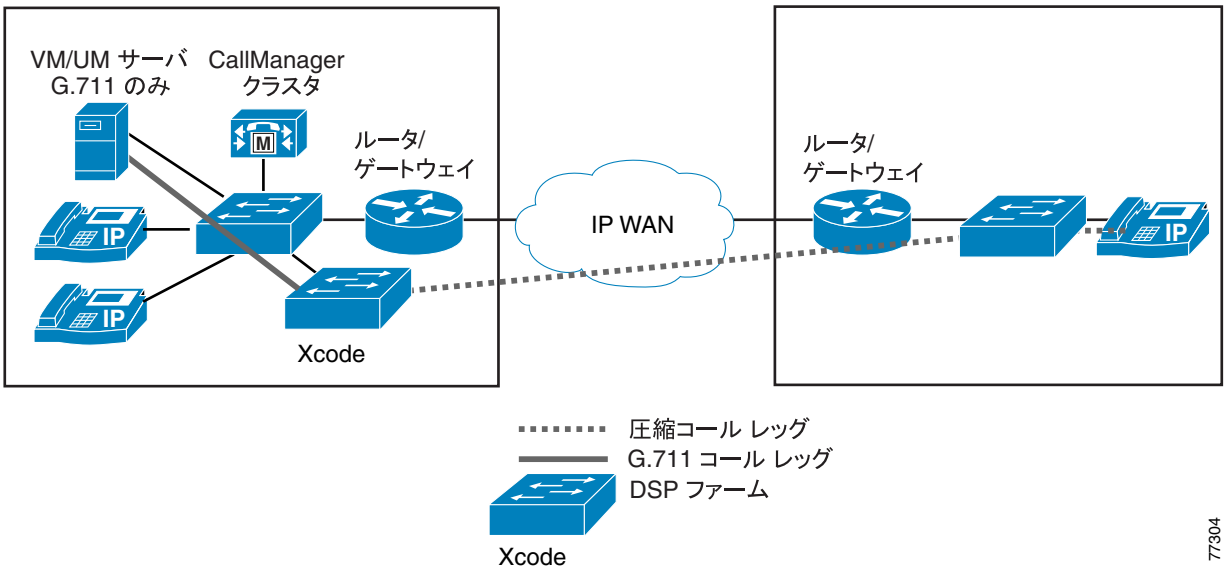
WAN 帯域幅は一般に制限されるので、WAN を通過するときは、G.729 などの低ビット レート コーデックを使用するようにコールが設定されます。図 6-4 を参照してください。

IP Phone 間の音声圧縮は、Cisco CallManager の *リージョン*と *ロケーション*を使用して簡単に設定されます。リージョンは、そのリージョン内のデバイスが使用する圧縮のタイプ（たとえば、G.711 または G.729）を指定します。ロケーションは、そのロケーションのデバイスに出入りするコールに使用可能な、合計帯域幅量を指定します。

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。Cisco CRS（Release 3.0 以降）アプリケーションは、G.711 または G.729 をサポートできますが、両方を同時にサポートすることはできません。両方のコーデックが必要な場合は、2 つの別々のサーバを使用します。単一のサーバで G.711 を使用する場合は、トランスコーディング リソースが必須となります。

Release 3.0 より前の Cisco CRS は、G.711 のみをサポートしていました。この場合、集中型コール処理配置で 2 つのコーデック タイプが使用されるときは、トランスコーディングを使用する必要があります。

図 6-4　集中型コール処理を使用する WAN のトランスコーディング



Cisco CallManager は、MRG（メディア リソース グループ）を使用して、クラスタ内の Cisco CallManager サーバ間で、MTP リソースとトランスコーディング リソースの共有を可能にします。さらに、異なるリージョンを通過するコールに LBR コーデック（たとえば、G.729）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。つまり、中央サイトの G.711 専用アプリケーションや、リモート サイトの H.323 ゲートウェイがあっても、ゲートウェイは、必ずしも、トランスコーダを実行する必要があるとは限りません。

（注） Release 3.3(2) より前の Cisco CallManager リリースの場合、MTP リソースとトランスコーディング リソースは、Cisco CallManager クラスタを備えた中央サイトに置く必要があります。この理由は、これらのリソースが、コール アドミッション制御用に*ロケーション*で設定できないからです。

要約すると、Cisco CallManager は次の機能を提供します。

- Cisco CallManager クラスタ全体でのリソース共有による、トランスコーディング リソースの最適な使用
- エンドポイントの一方または両方が必要とする場合のみ、トランスコーディング リソースを動的に割り当てることによる、リソースの効率的な使用

分散型コール処理を使用するマルチサイト WAN 配置

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

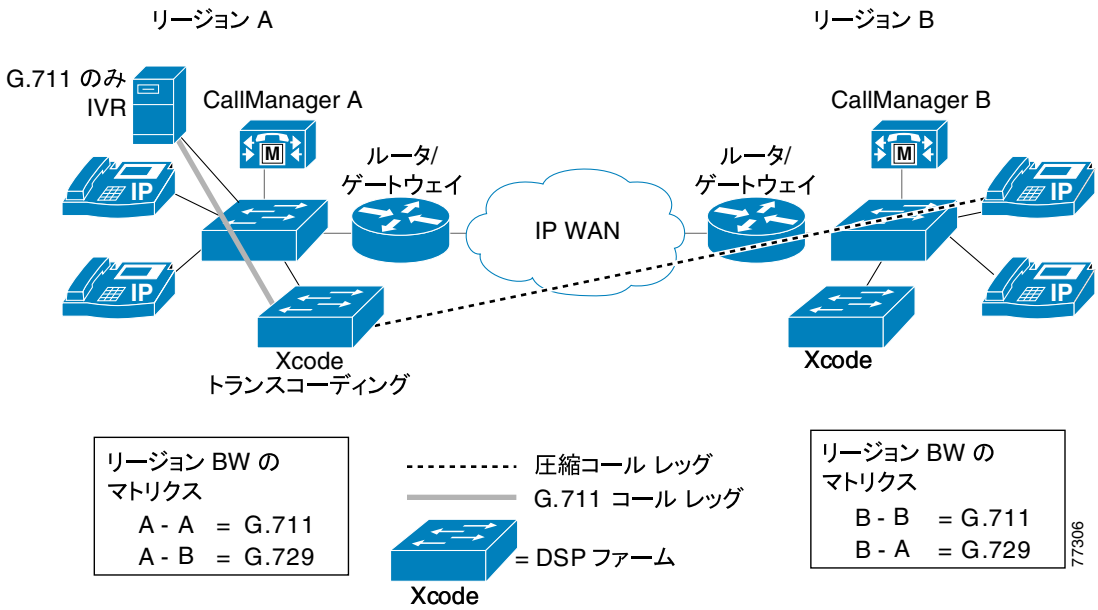
WAN 帯域幅は一般に制限されているので、WAN を通過するときは、LBR コーデック（たとえば、G.729）を使用するように、サイト間のコールが設定されます。H.323v2 クラスタ間トランクは、Cisco CallManager クラスタの接続に使用されます。Cisco CallManager は、ハードウェア MTP が使用される場合、MTP サービスを通じた圧縮音声コール接続もサポートします（図 6-5 を参照）。

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。Cisco CRS（Release 3.0 以降）アプリケーションは、G.711 または G.729 をサポートできますが、両方を同時にサポートすることはできません。両方のコーデックが必要な場合は、2 つの別々のサーバを使用します。単一のサーバで G.711 を使用する場合は、トランスコーディング リソースが必須となります。

  Release 3.0 より前の Cisco CRS は、G.711 のみをサポートしていました。この場合、分散型コール処理配置で 2 つのコーデック タイプが使用されるときは、トランスコーディングを使用する必要があります。
- 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 6-5　トランスコーディングを使用したクラスタ間コール フロー



Cisco CallManager は、MRG（メディア リソース グループ）を使用して、クラスタ内の Cisco CallManager サーバ間で、MTP リソースとトランスコーディング リソースの共有を可能にします。さらに、クラスタ間トランクを介したコールの場合、MTP リソースとトランスコーディング リソースは、必要な場合だけ使用されます。したがって、LBR コーデックをサポートしないアプリケーションに対して MTP サービスを設定する必要がなくなります。

次の特性が、分散型コール処理配置に適用されます。

- トランスコーディングを必要とするクラスタ間コールだけが、MTP サービスを使用します。たとえば、コールの両方のエンドポイントが G.729 コーデックを使用できる場合、トランスコーディング リソースは使用されません。
- クラスタ内のサーバ間で MTP リソースを共有すると、リソースの使用効率が向上します。

IP 公衆網アクセス

MTP リソースとトランスコーディング リソースの 4 つ目のアプリケーション シナリオには、従来の公衆網ではなく、IP 公衆網へのアクセスをカスタマーに提供するサービス プロバイダーが必要です。このようなシナリオでは、ゲートキーパーがサービス プロバイダーのネットワークに置かれます。ダイヤル プランを単純化するために、各カスタマーは、エンドポイントに割り当てられている個々の IP アドレスを隠せるように、MTP を使用してコールを固定する必要があります。その後、サービス プロバイダーのセントラル オフィスは、従来の公衆網を介してリレーし、他のカスタマーとの IP 接続を提供できます。図 6-6 は、この配置モデルを示しています。

図 6-6　IP 公衆網アクセスの例

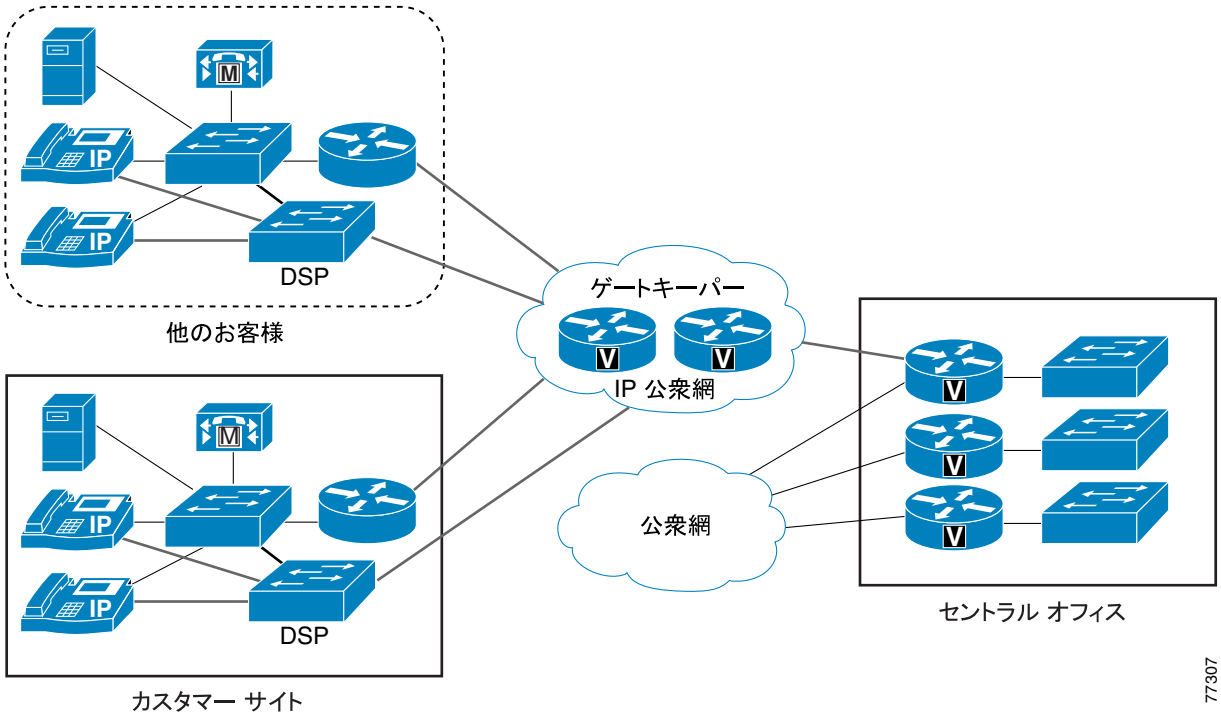


図 6-6 のカスタマー サイトは、上記の 3 つの配置モデル、つまり、単一サイト、集中型コール処理を使用するマルチサイト WAN、または分散型コール処理を使用するマルチサイト WAN のいずれのモデルでも使用できることに注意してください。

カスタマー サイトから IP 公衆網までの H.323 トランクは、エンドポイントの IP アドレスがマスクされたままであるように、MTP を使用して設定される必要があります。したがって、すべての外部コールが MTP リソースを使用します。ただし、MTP リソースは、リソースの使用効率を高めるために、Cisco CallManager クラスタ内で共有できます。

Music on Hold

Music on Hold（MoH）は、Cisco IP テレフォニー システムの統合機能です。この機能は、発信者の通話が保留、転送、一時保留（コール パーク）、または ad-hoc 会議に追加されるときに、発信者に音楽を流します。MoH の実装は、比較的簡単ですが、ユニキャストおよびマルチキャスト トラフィック、MoH コール フロー、設定オプション、サーバの動作と要件について基本的な理解が必要です。この章では、Cisco エンタープライズ IP テレフォニー配置用に MoH リソースを設計し、プロビジョニングする方法について説明します。

Cisco CallManager は、さまざまなメディア リソースにアクセスできます。メディア リソースとは、ソフトウェアベースまたはハードウェアベースのエンティティであり、接続されている音声データ ストリームに対して何らかのメディア処理を行うものです。メディア処理機能には、複数のストリームを混合して 1 つの出力ストリームを作成する機能、ある接続から別の接続にストリームを渡す機能、ある圧縮タイプから別の圧縮タイプにデータ ストリームをトランスコードする機能が含まれます。

Cisco CallManager は、次のタイプのメディア リソースを割り当て、使用します。

- メディア ターミネーション ポイント（MTP）リソース
- トランスコーディング リソース
- ユニキャスト会議リソース
- Annunciator リソース
- Music on Hold リソース

メディア リソース全般の詳細については、第 6 章「メディア リソース」を参照してください。

この章では、MoH 機能の設計について次の項目を説明します。

MoH の基本的な配置

発信者に保留音が聞こえるようにするには、Cisco CallManager の MoH 機能を有効にする必要があります。MoH 機能には、次の 2 つの主な要件があります。

- MoH オーディオ ストリーム ソースを流す MoH サーバ
- 通話を保留にするときに、MoH サーバが流す MoH ストリームを使用するように設定された Cisco CallManager

統合 MoH 機能により、ユーザは、オンネットとオフネットのユーザを保留にするときに、ストリーミング ソースから音楽を流すことができます。このソースは、保留になったオンネットまたはオフネット デバイスに音楽を流します。オンネット デバイスには、IVR（音声自動応答装置）またはコール ディストリビュータによって保留、確認保留、またはコール パーク保留にされた端末デバイスやアプリケーションが含まれます。オフネット ユーザには、メディア ゲートウェイ統合プロトコル（MGCP）、および H.323 ゲートウェイを通じて接続されたユーザが含まれます。また、MoH 機能は、Foreign Exchange Station（FXS）ポートを通じて Cisco IP ネットワークに接続された、一般電話サービス（POTS）の電話機にも使用できます。統合 MoH 機能には、メディア サーバ、データベース管理、コール制御、メディア リソース マネージャ、およびメディア制御の機能領域が含まれます。MoH サーバは、音楽リソースとストリームを提供します。

MOH 機能は、Cisco CallManager Administration インターフェイスを介して設定できます。終端装置または機能が通話を保留にすると、Cisco CallManager は、その保留デバイスを MoH メディア リソースに接続します。基本的に、Cisco CallManager は、MOH サーバとの接続を確立するように、エンド デバイスに指示します。保留にされたデバイスが復帰すると、そのデバイスは MoH リソースから切り離され、通常のアクティビティを再開します。

ユニキャストおよびマルチキャスト MoH

Cisco CallManager は、次の 2 つのタイプの MoH トランスポート メカニズムをサポートします。

- ユニキャスト
- マルチキャスト

ユニキャスト MoH は、MoH サーバから MoH オーディオ ストリームを要求するエンドポイントに直接送信されるストリームで構成されます。ユニキャスト MOH ストリームは、サーバとエンドポイント デバイス間のポイントツーポイント片方向オーディオ Real-Time Transport Protocol（RTP）ストリームです。ユニキャスト MOH は、ユーザまたは接続ごとに別々のソース ストリームを使用します。ユーザまたはネットワーク イベントを介して保留になるエンドポイント デバイスが増えるにつれて、MoH ストリームの本数も増加します。したがって、20 台のデバイスが保留になっている場合、サーバとこれらのエンドポイント デバイス間のネットワーク上で、RTP トラフィックとしてストリームが 20 本生成されます。このような MoH ストリームが生成されると、ネットワークのスループットと帯域幅に対してマイナスの影響を与える可能性があります。しかし、ユニキャスト MoH が非常に役立つのは、マルチキャストが使用可能になっていないネットワークの場合や、デバイスがマルチキャスト対応になっていないネットワークの場合です。このようなときに、管理者はユニキャスト MoH を使用することで、MoH 機能を利用できます。

マルチキャスト MoH は、MoH サーバからマルチキャスト グループ IP アドレスに送信されるストリームで構成されます。MoH オーディオ ストリームを要求するエンドポイントは、必要に応じてこの IP アドレスに加わることができます。マルチキャスト MOH ストリームは、MOH サーバとマルチキャスト グループ IP アドレス間の、ポイントツーマルチポイント片方向オーディオ RTP ストリームです。マルチキャスト Music on Hold では、複数のユーザが同じオーディオ ソース ストリームを使用して Music on Hold を提供できるようにするので、システム リソースと帯域幅を節約できます。したがって、20 台のデバイスが保留中であっても、ネットワーク上で 1 つの RTP トラフィックのストリームだけしか生成されない場合もあります。したがって、マルチキャストは、ソース デ

バイスに対する CPU の影響を大幅に削減し、共通パス上の伝送の帯域幅使用量も大幅に削減するので、MoH などのサービスの配置に非常に魅力的なテクノロジーです。しかし、ネットワークがマルチキャスト対応になっていない状況や、エンドポイント デバイスがマルチキャストを処理できない状況では、マルチキャスト MoH に問題が生じます。

IP マルチキャスト ネットワークの設計については、次の Web サイトで入手可能なオンラインの『Cisco AVVID Network Infrastructure IP Multicast Design』資料を参照してください。

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

推奨されるユニキャスト / マルチキャスト ゲートウェイ

次の推奨ゲートウェイは、ユニキャスト MOH とマルチキャスト MOH の両方をサポートします。

- Cisco 6624 および 6608 ゲートウェイ モジュールと、MGCP および Cisco CallManager Release 3.3(3) 以降の組み合せ
- Cisco Communication Media Module（CMM; コミュニケーション メディア モジュール）と、MGCP または H.323、および Cisco CallManager Release 4.0、Cisco IOS Release 12.2(13)ZP3 以降、または Catalyst OS Release 8.1(1) 以降の組み合せ
- Cisco 2600、3600、および 3700 シリーズ ルータと、MGCP または H.323、および Cisco IOS Release 12.2(8)T 以降の組み合せ

共存 MOH サーバとスタンドアロン MOH サーバ

MoH 機能を利用するには、Cisco CallManager クラスタに含まれているサーバを使用する必要があります。MoH サーバは、次のいずれかの方法で設定できます。

- 共存配置

  共存配置では、MOH 機能は Cisco CallManager ソフトウェアも実行している、クラスタ内の任意のサーバ（パブリッシャまたはサブスクライバ）で実行されます。MOH と共存している Cisco CallManager と、サーバ リソースを共有するので、このタイプの設定では、MOH サーバが送信できる同時ストリーム数が大幅に減少します。
- スタンドアロン配置

  スタンドアロン配置では、MoH 機能は Cisco CallManager クラスタ内の専用サーバに置かれます。この専用サーバの機能は、MoH ストリームをネットワーク内のデバイスに送信することだけです。スタンドアロン配置では、1 台の MoH サーバから最大数のストリームを送信できます。

MOH の固定ソースとオーディオ ファイル ソース

MoH のソースは、次のいずれかの方法で設定できます。

- Cisco CallManager または MoH サーバ上のオーディオ ファイルを使用した MoH
  - オーディオ ファイルを使用したユニキャスト MoH
  - オーディオ ファイルを使用したマルチキャスト MoH
- 固定音楽ソースを使用した MoH（サウンド カード経由）
  - 固定ソースを使用したユニキャスト MoH
  - 固定ソースを使用したマルチキャスト MoH

MOH は、MOH サーバ上に格納されているオーディオ ファイルから生成できます。オーディオ ファイルは、次の形式のいずれかでなければなりません。

- G.711 A-law または mu-law（サンプリング レート 8 KHz で録音）
- G.729 Annex A
- ワイドバンド

これらのファイルは、Cisco MoH オーディオ トランスレータ サービスを使用して作成できます。このサービスは、オーディオ ソース ファイル（たとえば、.wav または .mp3 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 サーバは、設定されたオーディオ ソースに基づいてこれらのファイルを要求し、初期化時またはオーディオ ソースの要求時に、それらのファイルをメモリにロードします。MoH イベントが発生すると、設定されたオーディオ ソース ファイルは、保留中の要求側デバイスにストリーミングされます。

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、通常、搭載しているサウンド カードにリンクしている Microsoft Windows オーディオ入力によって再生されます。

このメカニズムにより、ラジオ、CD プレーヤー、または互換性があるその他のサウンド ソースを使用できます。固定オーディオ ソースからのストリームは、リアルタイムで変換され、Cisco CallManager Administration によって設定されたコーデックに対応します。固定オーディオ ソースは、G.711（A-law または mu-law）、G.729 Annex A、およびワイドバンドに変換することができる、リアルタイムで変換可能な唯一のオーディオ ソースです。

固定またはライブ オーディオ ソースに対して、次のサウンド カードがサポートされています。

- Griffin Technologies iMic USB

  Microsoft Windows 2000（OS 2000 バージョン 2.7 以降）の Cisco CallManager Release 3.3(5) 以降でサポートされる USB サウンド デバイス。このデバイスは、3.0 GHz 以上のプロセッサを搭載したすべての Cisco MCS-78*xx*H サーバまたは MCS-78*xx*I サーバでサポートされます。

- Telex P-800 USB

  Microsoft Windows 2000（OS 2000 バージョン 2.5）の Cisco CallManager Release 3.3(3) でサポートされる USB サウンド デバイス。このデバイスは、2.2 GHz 以上のプロセッサを搭載したすべての Cisco MCS-78*xx*H サーバまたは MCS-78*xx*I サーバでサポートされます。

（注） Telex P-800 USB カードは End of Sale（EOS; 販売終了）になっているため、入手できません。既存の P-800 カードは上記のようにサポートされますが、新しい配置には Griffin iMic USB カードを使用する必要があります。

- Open AW-840（PCI）

  MCS-78*xx*-1266 までのすべての Cisco MCS-78*xx* サーバとの互換性を持つ Peripheral Component Interconnect（PCI）サウンド デバイス。

- Soundblaster PCI 16

  MCS-7835-1266 より前のすべての Cisco MCS-7835 との互換性を持つ Peripheral Component Interconnect（PCI）サウンド デバイス。

- Cisco MCS-7815 サウンド カード

  Cisco MCS-7815 サーバには、MOH サーバの固定オーディオ ソース デバイスとしてサポートされる組み込みサウンド カードが付属しています。

（注） Music On Hold を送信するときに固定オーディオ ソースを使用する場合は、事前に、著作権のあるオーディオ素材の再ブロードキャストについて、その適法性および問題を検討しておく必要があります。起こりうる問題については、貴社の法務部門に相談してください。

Cisco CallManager クラスタに含まれる MOH サーバ

MoH 機能を利用するには、各 MoH サーバが Cisco CallManager クラスタに含まれている必要があります。すべての MoH サーバは、パブリッシャ サーバと設定を共有し、SQL 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、SQL データベースを使用して、Cisco CallManager Administration を使用して設定された次の情報を共有する必要があります。

- オーディオ ソース：設定されたすべての MoH オーディオ ソースの数と ID
- マルチキャストまたはユニキャスト：これらのソースそれぞれに設定されたトランスポートの種類
- マルチキャスト アドレス：マルチキャストとしてストリーミングするように設定されたソースのマルチキャスト ベース IP アドレス

MoH サーバは、Cisco CallManager クラスタの一部になり、自動的に SQL データベースの複製に加わります。スタンドアロン MOH サーバを設定するには、最初に、そのサーバに Cisco CallManager を通常どおりにインストールします。次に、Cisco CallManager サービスを無効にし（スタンドアロン MOH サーバ上でのみ）、Cisco IP Voice Media Streaming Application を有効にします。

基本的な MoH と MoH コール フロー

ここでは、Cisco CallManager で実装される MOH の基本的な動作、および標準的なコール フローのシナリオについて説明します。

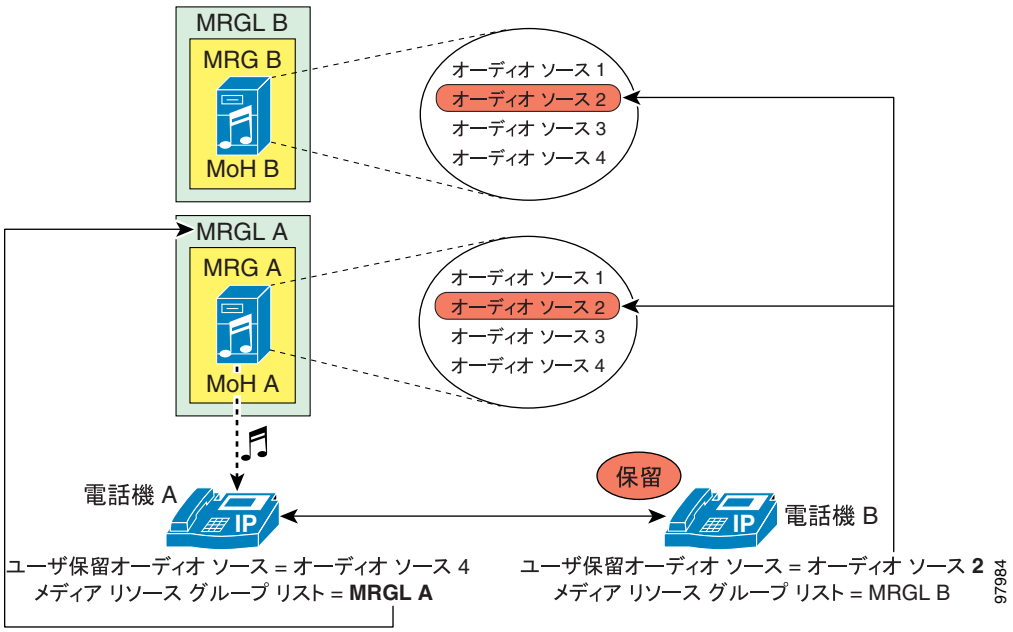
基本的な MOH

Cisco IP テレフォニー環境における基本的な MOH の動作は、保留側と被保留側から構成されます。保留側とは、通話を保留にするエンドポイント ユーザまたはネットワーク アプリケーションです。一方、被保留側とは、保留にされたエンドポイント ユーザまたはデバイスです。

エンドポイントが受信する MoH ストリームは、エンドポイントを保留にするデバイス（保留側）のユーザ保留 MoH オーディオ ソースと、保留にされたエンドポイント（被保留側）に設定されたメディア リソース グループ リスト（MRGL）との組み合せによって決まります。保留側に対して設定されたユーザ保留 MoH オーディオ ソースによって、保留側が通話を保留にしたときに流されるオーディオ ファイルが決まります。被保留側に設定された MRGL は、被保留側が MoH ストリームを受信する元のリソースまたはサーバを指定します。

簡単に言えば、保留側の設定により、再生されるオーディオ ファイルが決まり、被保留側の設定により、そのファイルを再生するリソースまたはサーバが決まります。図 7-1 の例に示すように、電話機 A および B が通話中であるときに、電話機 B（保留側）で電話機 A（被保留側）を保留にする場合、電話機 A には、電話機 B に対して設定された MOH オーディオ ソース（Audio-source2）が聞こえます。ただし、電話機 A はこの MOH オーディオ ストリームを、電話機 A に対して設定された MRGL（リソースまたはサーバ）（MRGL A）から受信します。

図 7-1　ユーザ保留オーディオ ソースとメディア リソース グループ リスト（MRGL）



MRGL により、ユニキャスト専用デバイスが MoH ストリームを受信するサーバが決まるので、ユニキャスト専用デバイスを設定する場合は、ユニキャスト MoH リソースまたはメディア リソース グループ（MRG）を指定する MRGL を使用する必要があります。同様に、マルチキャスト対応デバイスは、マルチキャスト MRG を指定する MRGL を使用して設定する必要があります。

MoH 構成の設定値

MRGL、およびユーザ保留オーディオ ソースとネットワーク保留オーディオ ソースの設定値は、Cisco CallManager Administration 内の複数の個所で指定できます。それぞれの個所で別々の（おそらく、競合する）設定値を設定できます。

個々のケースにユーザ オーディオ ソース設定値とネットワーク オーディオ ソース設定値のいずれかを適用するか決定するために、Cisco CallManager は、次の優先順位で、保留側デバイスに対するこれらの設定値を使用します。

1. ディレクトリまたは回線設定（ゲートウェイなど、回線定義のないデバイスには、このレベルはありません）
2. デバイス設定値
3. デバイス プールの設定値
4. クラスタ全体のデフォルト設定

特定の保留側のオーディオ ソースを決定しようとする場合、Cisco CallManager はまず、ディレクトリまたは回線レベルで設定されたユーザ（またはネットワーク）オーディオ ソースを調べます。このレベルが定義されていない場合、Cisco CallManager は、保留側デバイスで設定されたユーザ（またはネットワーク）オーディオ　ソースを調べます。このレベルが定義されていない場合、Cisco CallManager は、保留側デバイスのデバイス プールに対して設定されたユーザ（またはネットワーク）オーディオ ソースを調べます。このレベルが定義されていない場合、Cisco CallManager は、Cisco CallManager システム パラメータで設定された、クラスタ全体のデフォルト オーディオ ソース ID を調べます（デフォルトでは、このオーディオ ソース ID は、ユーザ保留オーディオ ソースとネットワーク保留オーディオ　ソースの両方に対して 1 に設定されています。これは、SampleAudioSource です）。

Cisco CallManager は、被保留側デバイスの MRGL 設定値も、次の優先順位で使用します。

1. デバイス設定値
2. デバイス プールの設定値
3. システムのデフォルト MoH リソース

特定の被保留側の MRGL を決定しようとする場合、Cisco CallManager は、デバイス レベルで設定された MRGL を調べます。このレベルが定義されていない場合、Cisco CallManager は、被保留側デバイスのデバイス プールに対して設定された MRGL を調べます。このレベルが定義されていない場合、Cisco CallManager は、システムのデフォルト MoH リソースを使用します。システムのデフォルト MoH リソースとは、MRG に割り当てられていないリソースであり、これらのリソースは常にユニキャストです。

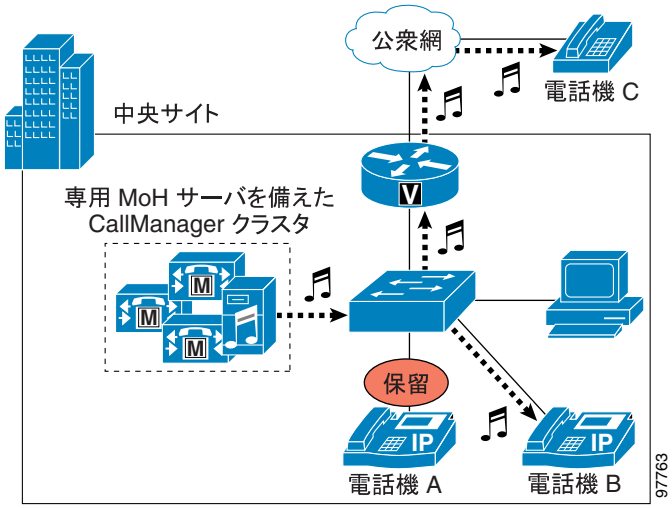
ユーザ保留とネットワーク保留

ユーザ保留には、次の 2 つの基本的なタイプがあります。

- IP Phone またはその他のエンドポイント デバイスでのユーザ保留
- MoH がゲートウェイにストリーミングされる公衆網でのユーザ保留

図 7-2 は、これらの 2 つのタイプのコール フローを示しています。電話機 A が電話機 B と通話中であるときに、電話機 A（保留側）で Hold ソフトキーを押すと、MoH サーバから電話機 B（被保留側）に音楽ストリームが送信されます。この音楽ストリームは、IP ネットワーク内の被保留側だけでなく、電話機　A が電話機　C を保留にする場合と同様に、公衆網上の被保留側にも送信できます。電話機 C の場合、MoH ストリームは音声ゲートウェイ インターフェイスに送信され、公衆網電話機に適したフォーマットに変換されます。電話機 A が Resume ソフトキーを押すと、被保留側（電話機 B または C）は、音楽ストリームから切り離され、電話機　A に再び接続されます。

図 7-2　ユーザ保留の基本的な例

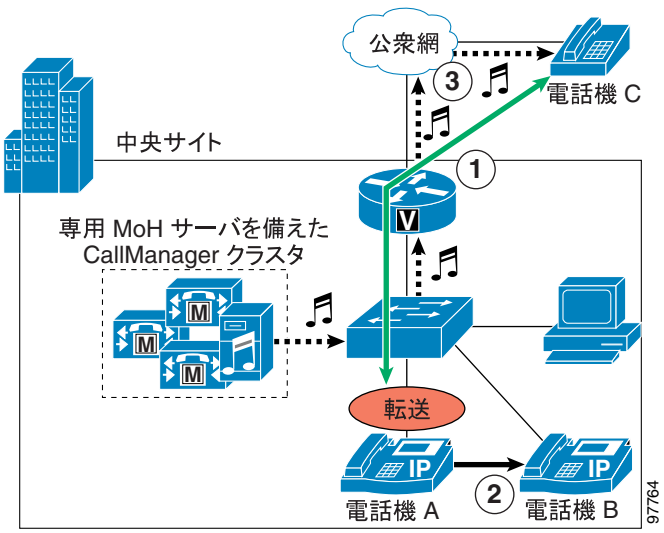


ネットワーク保留には次のタイプがあります。

- コール転送
- コール パーク
- 会議セットアップ
- アプリケーション ベースの保留

図 7-3 は、コール転送のコール フローを示しています。電話機 A が公衆網電話機 C からコールを受信する（ステップ 1）と、電話機 A はそのコールに応答し、電話機 B に転送します（ステップ 2）。転送プロセス時に、電話機 C は、ゲートウェイを介して MoH サーバから MoH ストリームを受信します（ステップ 3）。電話機 A が転送アクションを完了した後、電話機 C は音楽ストリームから切り離され、電話機 B（転送の宛先）に転送されます。このプロセスは、コール パークや会議セットアップなどの他のネットワーク保留操作の場合と同じです。

図 7-3　コール転送のネットワーク保留の基本的な例



ユニキャストとマルチキャスト MOH コール フロー

MoH 操作は、通常の電話のコール フローに非常によく似ています。MoH サーバは、被保留側デバイスが必要に応じて接続または切断される SCCP（Skinny Client Control Protocol）デバイスの役目をします。しかし、ユニキャストとマルチキャストの MoH コール フローの動作には、明らかな相違点があります。ユニキャスト MoH コール フローは、Cisco CallManager から MoH サーバへのメッセージによって初期化されます。このメッセージは、被保留側デバイスの IP アドレスにオーディオ ストリームを送信するように、MoH サーバに指示します。一方、マルチキャスト MoH コール フローは、Cisco CallManager から被保留側デバイスへのメッセージによって初期化されます。このメッセージは、設定されたマルチキャスト MoH オーディオ ストリームのマルチキャスト グループ アドレスに加わるように、エンドポイント デバイスに指示します。

MOH コール フローの詳細については、P.7-23 の「ユニキャストとマルチキャスト MoH コール フローの詳細」の項を参照してください。

MOH 設定上の考慮事項およびベスト プラクティス

ここでは、堅牢な MoH ソリューションの設計に役立つ、MoH 設定上の考慮事項とベスト プラクティスについて説明します。

コーデックの選択

MoH 配置に複数のコーデックが必要な場合、Cisco CallManager Service Parameters Configuration の IP Voice Streaming Media App サービス パラメータでコーデックを設定します。Clusterwide Parameters セクションの下の Supported MoH Codecs リストの中から、必要なコーデック タイプを選択してください。デフォルトでは、G.711 mu-law のみが選択されています。別のコーデック タイプを選択するには、リストをスクロールさせて該当するコーデックをクリックしてください。複数選択する場合は、CTRL キーを押したまま、マウスを使用して、リストをスクロールさせて複数のコーデックを選択します。選択終了後、Update ボタンをクリックしてください。

（注） MoH オーディオ ストリームに G.729 コーデックを使用する場合、このコーデックは会話用に最適化されているので、音楽用としては最低限のオーディオ品質であることに注意してください。

マルチキャスト アドレッシング

マルチキャスト MoH を設定するには、適切な IP アドレッシングが重要です。IP マルチキャストのアドレス範囲は 224.0.1.0 ～ 239.255.255.255 です。しかし、IANA（Internet Assigned Numbers Authority）は、公衆マルチキャスト アプリケーション用に 224.0.1.0 ～ 238.255.255.255 の範囲のアドレスを割り当てています。公衆マルチキャスト アドレスを MoH に使用しないことを強くお勧めします。代わりに、プライベート ネットワーク上の管理制御アプリケーション用に予約されている、239.1.1.1 ～ 239.255.255.255 の範囲内の IP アドレスを使用するように、マルチキャスト MoH オーディオ ソースを設定することをお勧めします。

さらに、次の理由で、ポート番号ではなく、IP アドレスでインクリメントするように、マルチキャスト オーディオ ソースを設定することも必要です。

- 保留にされた IP Phone は、ポート番号ではなく、マルチキャスト IP アドレスに加わる。

  Cisco IP Phone には、マルチキャスト ポート番号という概念はありません。したがって、特定のオーディオ ストリームに対して設定されているすべてのコーデックが、同じマルチキャスト IP アドレス（別々のポート番号であっても）に送信される場合、1 本のストリームしか必要ない場合であっても、すべてのストリームが IP Phone に送信されます。IP Phone は 1 本の MoH ストリームしか受信できないので、不必要なトラフィックでネットワークが飽和状態になる可能性があります。

- IP ネットワーク ルータは、ポート番号ではなく、IP アドレスに基づいて、マルチキャストをルーティングする。

  ルータには、マルチキャスト ポート番号という概念はありません。したがって、同じマルチキャスト グループ アドレス（別々のポート番号であっても）に送信される複数のストリームを検出すると、ルータは、そのマルチキャスト グループのすべてのストリームを転送します。必要なストリームは 1 本だけなので、ネットワーク帯域幅が過剰に利用され、その結果、ネットワークの輻輳が発生する可能性があります。

MOH オーディオ ソース

オーディオ ソースは、Cisco CallManager クラスタ内のすべての MOH サーバ間で共有されます。クラスタごとに最大 51 の固有オーディオ ソースを設定できます（50 のオーディオ ファイル ソースと、サウンド カードを介した 1 つの固定 / ライブ ソース）。この制限の例外については、P.7-11 の「複数の固定またはライブ オーディオ ソースの使用」および P.7-19 の「支店ルータのフラッシュからのマルチキャスト MOH」の項を参照してください。

複数の固定またはライブ オーディオ ソースの使用

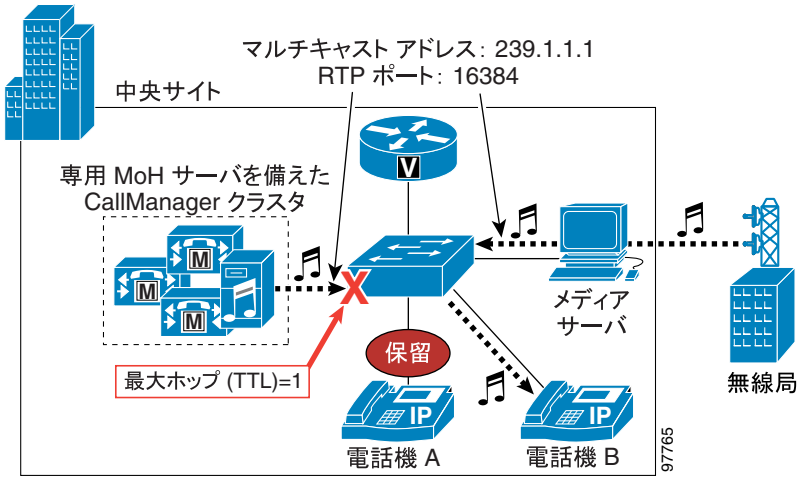
各 MoH サーバは、1 つの固定オーディオ ソースしか流すことができません。大部分の場合、複数の固定またはライブ オーディオ ソースが必要な場合は、ソースごとに別々の MoH サーバが必要です。しかし、固定またはライブ ソースからマルチキャストを流すことができる外部の非 MoH サーバまたはデバイスを使用すると、複数の固定ソース MoH オーディオ ストリームを提供することが可能です。

外部ソースごとに、外部ソース サーバまたはデバイスによってマルチキャストされるオーディオ ソース ストリームと同じマルチキャスト IP アドレス、およびポート番号を持つオーディオ ソースを使用して、MoH サーバを設定する必要があります。さらに、最大ホップ カウントを 1 に設定するか、アクセス コントロール リスト（ACL）を使用して、パケットがローカル サブネットの外に流れないようにすることによって、この設定された（非外部）オーディオ ソースが WAN を通過しないようにすることも必要です。

図 7-4 は、MOH ストリームとして使用される外部ライブ ソースの例を示しています。この図では、MOH サーバは、239.1.1.1（RTP ポート 16384 上で）にマルチキャスト オーディオ ソースを流します。このストリームは、最大ホップ カウント 1 に制限されているので、ローカル MOH サーバのサブネットから外に出ないことが保証されます。同時に、メディア サーバは、ラジオ局のライブ フィードから取得したオーディオ ストリームをマルチキャストします。このストリームも、マルチキャスト アドレスとして 239.1.1.1 を使用し、RTP ポート番号として 16384 を使用します。ただし、電話機 A で Hold ソフトキーを押したときに、このストリームが電話機 B に到達できるようにするために、このストリームのホップ カウントまたは Time to Live（TTL; 存続可能時間）は 2 以上必要です。

（注） マルチキャストの TTL の値が減少する（または満了する）のは、パケットがレイヤ 3 インターフェイスを通過するときのみです。マルチキャスト パケットがレイヤ 2 スイッチ インターフェイスを通過するときには、TTL 値は減少しません。

図 7-4　外部のライブ オーディオ ソースの例



(注)　マルチキャスト オーディオ ソースとしてラジオのライブ ブロードキャストを使用すると、法律上の問題が発生する恐れがあります。起こりうる問題については、貴社の法務部門に相談してください。

多数のストリームを、1 つまたは複数の外部メディア サーバからマルチキャストできます。これを行うには、追加のオーディオ ソースを複数の MOH サーバに設定し、MOH サーバに設定された同一のマルチキャスト グループ アドレスを使用して外部サーバからオーディオ ストリームを発信します。ただし、エンドポイント デバイスで聞こえる MOH ストリームは、保留側のユーザ / ネットワーク保留オーディオ ソースと被保留側の MRGL との組み合せによって決まるため、重複しているマルチキャスト グループ アドレスが多数存在する環境では、具体的にどのストリームをエンドポイントが受信するかを予測することは困難になる場合があります。このため、設定するマルチキャスト オーディオ ソースは MoH サーバごとに 1 つのみとすることをお勧めします。この推奨事項により、エンドポイントが受信するオーディオ ソースが、ユーザ / ネットワーク保留オーディオ ソースと MRGL の単一の組み合せによって一意に識別できることが保証されます。

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

状況に応じて、管理者は、1 つの Cisco CallManager クラスタを設定することにより、ユニキャストとマルチキャストの両方の MoH ストリームを処理できます。この設定が必要なのは、マルチキャストをサポートしないデバイス、またはエンドポイントがテレフォニー ネットワークに含まれている場合、あるいはネットワークの一部でマルチキャストが使用可能になっていない場合です。

クラスタがユニキャストとマルチキャストの両方の MoH オーディオ ストリームをサポートできるようにするには、次のいずれかの方法を使用してください。

- 別々の MoH サーバを配置します。一方のサーバをユニキャスト MoH サーバとして設定し、もう一方のサーバをマルチキャスト MoH サーバとして設定します。
- 同一 MoH サーバに対して別々のメディア リソース グループ（MRG）を設定します。オーディオ ストリームに対して、一方の MRG ではマルチキャストを使用するように設定し、もう一方の MRG ではユニキャストを使用するように設定します。

どちらの場合も、少なくとも 2 つの MRG、および少なくとも 2 つのメディア リソース グループ リスト（MRGL）を設定する必要があります。ユニキャスト MoH を必要とするエンドポイントには、1 つのユニキャスト MRG と 1 つのユニキャスト MRGL を設定します。同様に、マルチキャスト MoH を必要とするエンドポイントには、1 つのマルチキャスト MRG と 1 つのマルチキャスト MRGL を設定します。

別々の MoH サーバを配置する場合、一方のサーバをマルチキャスト無効（ユニキャスト専用）に設定し、もう一方の MoH サーバをマルチキャスト有効に設定してください。ユニキャスト専用 MoH サーバのユニキャスト オーディオ リソースをユニキャスト MRG に、マルチキャスト MoH サーバのマルチキャスト オーディオ リソースをマルチキャスト MRG に、それぞれ割り当てます。マルチキャスト MRG には **Use Multicast for MoH Audio** ボックスにチェックマークが付き、ユニキャスト MRG にはチェックマークが付いていないことを確認してください。また、これらのユニキャスト MRG とマルチキャスト MRG をそれぞれの MRGL に割り当てます。この場合、MOH ストリームを流す元のサーバ、および MRG がマルチキャストを使用するように設定されているかどうかに基づいて、MOH ストリームのユニキャストまたはマルチキャストが行われます。

単一の MOH サーバをユニキャスト MOH とマルチキャスト MOH の両方に対して配置する場合は、サーバとそのオーディオ ソースをマルチキャスト用に設定します。同じオーディオ ソースをユニキャスト MRG とマルチキャスト MRG の両方に割り当て、マルチキャスト MRG に対して **Use Multicast for MoH Audio** ボックスにチェックマークを付けます。この設定により、MRG がマルチキャストを使用するように設定されているかどうかだけに基づいて、MoH ストリームのユニキャストまたはマルチキャストが行われます。

（注） ユニキャスト MRG を設定する場合は、混乱しないようにしてください。これは、オーディオ リソースをユニキャスト MRG に追加する場合であっても、オーディオ リソース名の最後に、[Multicast] が追加されるからです。このラベルは、リソースがマルチキャスト対応であるという単なる表示です。リソースがユニキャストとして送信されるか、マルチキャストとして送信されるかを決定するのは、**Use Multicast for MoH Audio** ボックスのチェックの有無です。

さらに、適切な MRGL を使用するように、個々のデバイスまたはデバイス プールを設定する必要があります。1 つまたは複数のデバイス プールにすべてのユニキャスト デバイスを含め、ユニキャスト MRGL を使用するようにこれらのデバイス プールを設定できます。あるいは、1 つまたは複数のデバイス プールにすべてのマルチキャスト デバイスを含め、マルチキャスト MRGL を使用するようにこれらのデバイス プールを設定することもできます。オプションとして、該当するユニキャスト MRGL またはマルチキャスト MRGL を使用するように、個々のデバイスを設定できます。あるいは、デバイス プール、個々のデバイス、または（電話デバイスの場合）個々の回線かディレクトリ番号ごとに、ユーザ保留オーディオ ソースおよびネットワーク保留オーディオ ソースを設定して、適切なオーディオ ソースを決定します。

マルチキャスト MOH とユニキャスト MOH の両方を同じクラスタに配置する方法を選択する場合は、必要なサーバの数を考慮することが重要です。単一の MoH サーバをユニキャストとマルチキャストの両方に使用すると、クラスタ全体に必要な MOH サーバの数が減ります。マルチキャスト MOH サーバとユニキャスト MOH サーバを別々に配置すると、クラスタ内に必要なサーバの数が明らかに増えます。

冗長性

完全な冗長性のある MoH 動作を確保するために複数の MoH サーバを設定し、配置することをお勧めします。最初の MoH サーバに障害が発生したり、要求を処理するために必要なリソースがなくなったために使用不能になると、2 番目のサーバが自動的に MoH 機能を引き継ぎ、要求に応答します。適切な冗長構成のために、クラスタ内の 2 つ以上の MoH サーバから各 MRG にリソースを割り当ててください。

MRG 内のリソースは、リストされている順に使用されます。デバイスが MoH オーディオ リソースを要求すると、Cisco CallManager は、MRG 内の最初の MoH リソースをそのデバイスに送信しようとします。最初のリソースがサーバ障害またはリソースの不足により使用不能である場合、Cisco CallManager は、MRG 内の次の MoH リソースを使用しようとします。

マルチキャストとユニキャストの両方の MoH が必要な環境では、ネットワーク内のすべてのエンドポイントの MoH 冗長性が確保されるように、必ず両方のトランスポート タイプに冗長性をもたせてください。

QoS

時間に依存する重要なリアルタイム アプリケーション（音声など）に遅延または損失がないように、1 つのネットワーク上のデータと音声のコンバージェンスには、適切な QoS が必要です。音声トラフィック用の適切な QoS を確保するには、ストリームがネットワークに入り、通過するときに、ストリームのマーク付け、分類、およびキューイングを行って、音声ストリームを重要度の低いトラフィックよりも優先的に処理する必要があります。MoH サーバは、オーディオ ストリーム トラフィックに、音声ベアラ トラフィックと同じマークを自動的に付けて、DSCP（Differentiated Services Code Point）を EF（ToS を 0xB8）にします。したがって、ネットワーク上で QoS が適切に設定されている限り、MoH ストリームは、音声 RTP メディア トラフィックとして分類され、プライオリティ キューイングとして扱われます。

MOH リソース用のハードウェアとキャパシティ プランニング

MoH リソースも、他のすべてのメディア リソースと同じように、ハードウェアを配置し、設定した後、予想されたネットワークのコール量を確実にサポートするために、キャパシティ プランニングが非常に重要です。このため、MoH リソースのハードウェア キャパシティを認識し、このキャパシティとの関連からマルチキャストとユニキャストの MoH の役割りを考慮することが重要です。

サーバ プラットフォームの最大同時セッション数

表 7-1 は、サーバ プラットフォームと、そのプラットフォームがサポートできる最大同時 MOH セッション数をリストしています。MoH セッションがこの最大同時セッション数を超えてから、さらに負荷が増えると、MoH 品質の低下、不規則な MoH 動作、または MoH 機能の喪失までも発生する恐れがあるので、ネットワークのコール量が最大同時セッション数を超えないようにしてください。

表 7-1　サーバ プラットフォーム タイプごとの最大 MoH セッション数

サーバ プラットフォーム	サポートされるコーデック	サポートされる MoH セッション数
MCS 7815 MCS 782*x*（全モデル） MCS 7830（全モデル） SPE-310 HP DL320 IBM xSeries 33x（全モデル）	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：40 MoH セッション スタンドアロン MoH サーバ：200 MoH セッション
MCS 7835（全モデル） MCS 7845（全モデル） HP DL380 IBM xSeries 34x（全モデル）	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：100 MoH セッション スタンドアロン MoH サーバ：250 MOH セッション[1]

1. Cisco CallManager クラスタごとに最大 51 の固有オーディオ ソースを設定できます。

MoH Server 設定ページの Maximum Half Duplex Streams フィールドと Maximum Multicast Connections フィールドを、表 7-1 に示されているキャパシティと一致するように設定する必要があります。これらのフィールドは、デフォルトで 250 と 30 にそれぞれ設定されていますが、表に示されているサーバ プラットフォームのタイプとサーバ配置のタイプ（共存またはスタンドアロン）に応じて設定変更する必要があります。推奨されるキャパシティの数値に一致させないと、サーバ リソースが十分に使用されない、またはサーバがネットワーク負荷を処理できないといった問題が発生する可能性があります。

（注） 表 7-1 にリストされている最大セッションの上限は、ユニキャスト、マルチキャスト、またはユニキャストとマルチキャストの同時セッションに適用されます。この上限は、トランスポート メカニズムに関係なく、プラットフォームがサポートできる推奨最大セッション数を示しています。

リソースのプロビジョニングとキャパシティ プランニング

共存またはスタンドアロンの MOH サーバ設定のプロビジョニングを行う場合、ネットワーク管理者は、MOH オーディオ ストリームに使用されるトランスポート メカニズムのタイプを考慮する必要があります。ユニキャスト MoH を使用する場合、保留される各デバイスには、別々の MoH ストリームが必要です。しかし、マルチキャスト MOH と単一のオーディオ ソースのみを使用する場合、保留にするタイプのデバイス数に関係なく、設定されているコーデック タイプごとに必要な MOH ストリームは 1 つだけです。

たとえば、30,000 台の電話機のあるクラスタがあり、保留率が 2% である（すべてのエンドポイント デバイスの 2% だけが、常に保留になる）場合、600 の MoH ストリームまたはセッションが必要です。ユニキャスト専用の MOH 環境の場合、次の計算で示されているように、この負荷を処理するには、2 つのスタンドアロン MOH サーバ（MCS 7835 または 7845）と 1 つの共存 MOH サーバ（MCS 7835 または 7845）が必要です。

［（MCS 7835 または 7845 スタンドアロン サーバごとに 250 セッション）＊（スタンドアロン サーバ 2 台）］+［（MCS 7835 または 7845 共存サーバごとに 100 セッション）＊（共存サーバ 1 台）］= 600 セッション

一方、たとえば、36 の固有 MOH オーディオ ストリームがあるマルチキャスト専用 MOH 環境には、次の計算で示されているように、1 つの共存 MOH サーバ（MCS 7815、782*x*、または 7830）だけが必要です。

（MCS 7815、782*x*、または 7830 共存サーバごとに 40 セッション）＊（共存サーバ 1 台）> 36 セッション

36 の固有マルチキャスト ストリームは、次のいずれかの方法でプロビジョニングできます。

- 単一のコーデックを使用して 36 の固有オーディオ ソースをストリーミングする
- 2 つのコーデックだけを使用して 18 の固有オーディオ ソースをストリーミングする
- 3 つのコーデックだけを使用して 12 の固有オーディオ ソースをストリーミングする
- 4 つのコーデックすべてを使用して 9 つの固有オーディオ ソースをストリーミングする

上記の例で示されているように、マルチキャスト MoH は、ユニキャスト MoH よりも、サーバ リソースを大幅に節約できます。

上記の例では、2% の保留率は、30,000 台の電話機に基づくものであり、保留になる可能性があるネットワーク内のゲートウェイまたはその他のエンドポイント デバイスを考慮していません。こうしたその他のデバイスは、電話機と同じように保留になる可能性があるので、保留率を計算するときは、これらのデバイスも考慮する必要があります。

上記の計算では、MoH サーバの冗長性を見込んでいません。MoH サーバに障害が発生する場合、またはユーザの 2% 以上が同時に保留になる場合、このシナリオでは、オーバーフローが発生したり負荷が増えたときに処理するための MoH リソースがありません。MoH リソースの計算には、冗長性に配慮して十分に余裕のあるキャパシティを含める必要があります。

（注） Cisco CallManager クラスタごとに設定できる固有オーディオ ソースの上限は 51 で、MOH ストリームに使用可能なコーデックの上限は 4 つであるため、MOH サーバごとのマルチキャスト ストリームの最大数は 204 です。

MoH に対する IP テレフォニー配置モデルの影響

各種 IP テレフォニー配置モデルにより、MoH の構成設計にはさらに考慮事項が発生します。配置モデルの選択が、MoH のトランスポート メカニズム（ユニキャストまたはマルチキャスト）、リソースのプロビジョニング、およびコーデックの決定に影響を与える場合があります。ここでは、各種配置モデルに関連した問題について説明します。

配置モデルの詳細については、第 2 章「IP テレフォニー配置モデル」を参照してください。

単一サイト キャンパス（すべての配置に関連）

単一サイト キャンパス配置は、通常、LAN インフラストラクチャに基づくものであり、大量のトラフィックに対して十分な帯域幅が用意されています。LAN インフラストラクチャでは一般に帯域幅が制限されないので、単一サイト配置内のすべての MoH オーディオ ストリームには、G.711（A-law または mu-law）コーデックの使用をお勧めします。G.711 は、IP テレフォニー環境に、最適な音声と音楽のストリーミング品質を提供します。

MoH サーバの冗長性も考慮する必要があります。MoH サーバが過負荷になるか、使用不能になった場合でも、複数の MoH サーバを設定し、それらのサーバを優先順に MRG に割り当てておくと、別のサーバが制御を引き継いで、MoH ストリームを流すことができます。

ネットワーク テクノロジーの多様性が増すにつれて、大規模な単一サイト キャンパスでは、一部のエンドポイント デバイスがマルチキャストをサポートできなくなる可能性があります。このため、ユニキャストとマルチキャストの両方の MoH リソースを配置する必要があります。たとえば、無線 IP Phone は、無線テクノロジーの動作により、マルチキャストをサポートしません。したがって、無線 IP Phone を配置する場合は、マルチキャストとユニキャストの両方の MoH を設定する必要があります。

オフネット コールとアプリケーション処理コールが、保留時に期待された MOH ストリームを受け取るには、適切な MRGL とオーディオ ソースを使用してすべてのゲートウェイとその他のデバイスを設定するか、それらを適切なデバイス プールに割り当ててください。

集中型マルチサイト配置

集中型コール処理を使用するマルチサイト IP テレフォニー配置には、一般的に、中央以外の複数のサイトとの WAN 接続が含まれます。これらの WAN リンクは、通常、帯域幅とスループットの障害になります。これらのリンク上での帯域幅使用量を最小限にするには、WAN を通過するすべての MoH オーディオ ストリームとして G.729 コーデックを使用することをお勧めします。G.729 コーデックは、音楽アプリケーションではなく、音声用に最適化されています。したがって、MoH トランスポートに G.729 がもたらす品質の低下よりも、帯域幅の節約がはるかに重要な問題である WAN 上でのみ、G.729 を使用してください。さらに、マルチキャスト トラフィックにより、帯域幅を大幅に節約できるので、WAN を介してエンドポイントにオーディオを流す場合は、常にマルチキャスト MoH を使用する必要があります。

WAN を介して G.729 を使用するときに MOH ストリームの音声品質が問題になる場合は、WAN を介した MOH オーディオ ストリームに G.711 コーデックを使用し、音声コールには引き続き G.729 を使用します。WAN を介した MOH ストリームの送信に G.711 コーデックを使用し、WAN を介した音声コールの送信に G.729 コーデックを使用するには、Cisco CallManager リージョンにすべての MOH サーバだけを配置し、そのリージョンが他のリージョンとの間で G.711 を使用するように設定します。この設定により、WAN の一方の側にある 2 つの電話機間でコールを発信するときは、それぞれのリージョンの間で G.729 コーデックが使用されます。ただし、一方の通話者がコールを

保留にした場合、MOH オーディオ ストリームは G.711 を使用して符号化されます。これは、G.711 が、MOH サーバのリージョンと、保留にされた電話機のリージョンとの間で使用するコーデックとして設定されているためです。

コール アドミッション制御と MOH

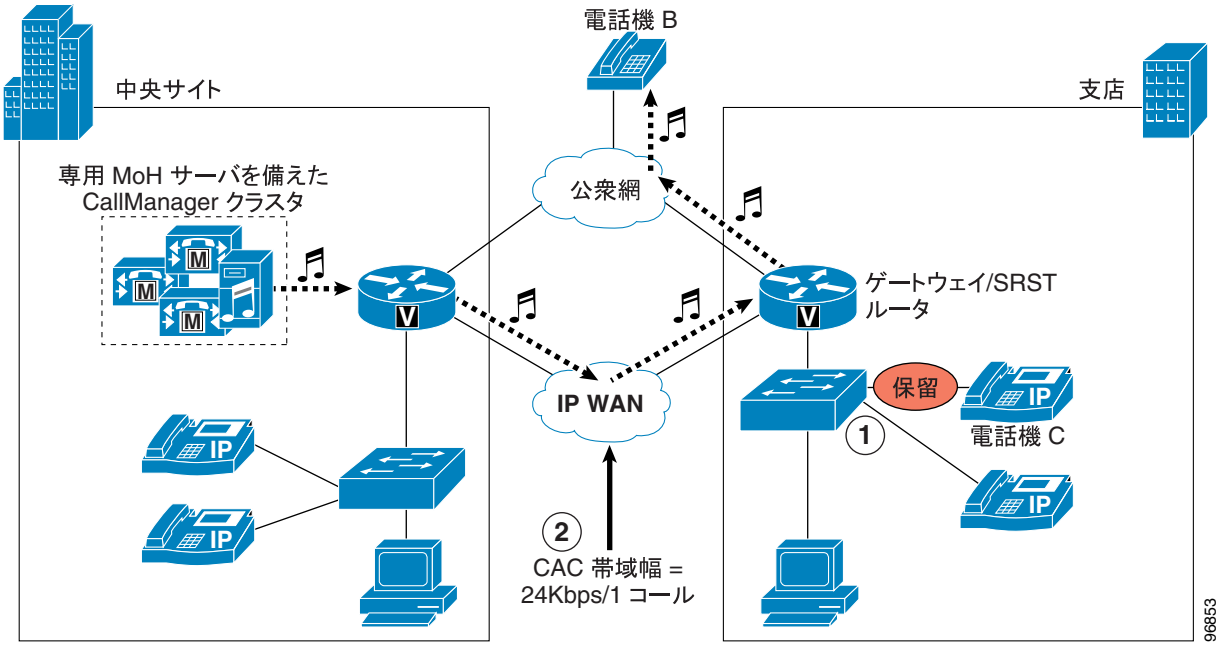
IP テレフォニー トラフィックが WAN リンク上を流れる場合は、コール アドミッション制御（CAC）が必要です。このようなリンク上では使用可能な帯域幅が制限されているので、音声メディア トラフィックの遅延または損失が起きる可能性が高くなります。Cisco CallManager ロケーション ベースのコール アドミッション制御メカニズムを使用すると、他のロケーションとの WAN リンクを介した決まった数のコールだけを受け入れるか、許可して、WAN 帯域幅のオーバーサブスクリプション、または音声パケットの遅延や損失を防ぐように、IP テレフォニー環境内の各ロケーションを設定することができます。WAN リンクに帯域幅値を指定すると、リンクの速度に基づいてコール数を制限できます。コール数が決められていた数に達するか、その数を超えると、Cisco CallManager は、そのリンクを介して処理されようとするその他のコールをすべて拒否します。

Cisco CallManager ロケーション ベースのコール 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分かりやすく示すための例に過ぎません。また、この設定の推奨または保証を意味するものではありません。前述のように、WAN を介した MoH オーディオ ストリームの送信用のトランスポート メカニズムには、マルチキャスト MoH をお勧めします。

図 7-5　ロケーションベースのコール アドミッション制御と MOH



支店ルータのフラッシュからのマルチキャスト MOH

Cisco IOS Release 12.2(15)ZJ および SRST Release 3.0 から、MoH は支店のルータのフラッシュを介して、リモートまたは支店のサイト内でマルチキャストできるようになりました。Cisco IOS ルータのフラッシュからのマルチキャスト MoH は、次の理由で MoH 機能を向上させます。

- 支店のゲートウェイまたはルータが SRST モードのときに、支店のデバイスが中央サイトの Cisco CallManager との接続を失った場合、支店のゲートウェイまたはルータが MoH をマルチキャストします。
- この設定により、WAN を介してリモート支店サイトに MOH を転送する必要がなくなります。ただし、そのためには、WAN が稼働中で、電話機が Cisco CallManager で制御されている場合でも、ローカルに発信される MOH を提供する必要があります。

例 7-1 は、ルータのフラッシュからのマルチキャスト MOH を可能にするために、Cisco IOS ルータ設定（SRST セクションの下）で使用するコマンドを示しています。

例 7-1　支店ルータのフラッシュからのマルチキャスト MOH を有効にする

```
SRST-router(config)#call-manager-fallback
SRST-router(config-cm-fallback)#ip source-address 10.1.1.1
SRST-router(config-cm-fallback)#moh music-on-hold.au
SRST-router(config-cm-fallback)#multicast moh 239.192.240.1 port 16384 route
10.1.1.254
```

例 7-1 では、ルータのフラッシュ上のオーディオ ファイルの名前は music-on-hold.au です。設定されたマルチキャスト アドレスとポート番号は、それぞれ 239.192.240.1 と 16384 です。オプションの **route** コマンドは、マルチキャスト ストリーム用のソース インターフェイス アドレスを指定します。route オプションを指定しない場合、マルチキャスト ストリームは、設定されている SRST のデフォルト アドレスから発信されます。このアドレスは、SRST 設定モードで **ip source-address** コマンドによって指定されたものです。フラッシュから流すことのできるオーディオ ファイルは 1 つのみで、ルータごとに使用可能なマルチキャスト アドレスとポート番号は 1 つのみです。

支店ルータが SRST モードで動作している場合、シャーシ内のすべてのアナログ ポートとデジタル ポートに、マルチキャスト MOH を流すことができます。これによりアナログ電話機および公衆網電話機に MOH を流すことができます。このとき、SRST モードの IP Phone は、SRST ルータのフラッシュからマルチキャスト MoH を受信できないので、代わりに保留音を受け取ります。

（注） SRST 機能が実際に使用されるかどうかに関係なく、SRST ライセンスが必要です。ライセンスが必要なのは、支店ルータのフラッシュから MOH を流すための設定が SRST 設定モードで行われるため、および SRST 機能が使用されない場合でも少なくとも 1 つの **max-ephones** と 1 つの **max-dn** を設定する必要があるためです。これらの設定コマンドのほか、例 7-1 に示されているコマンドが必要です。

設定後、ルータは、SRST モードでないときでも継続的にフラッシュから MOH ストリームを流します。支店のルータが SRST モードで動作していない場合でも、フラッシュからすべてのローカル デバイス（IP Phone を含む）に MOH をマルチキャストできます。支店のルータに対して、フラッシュからの非 SRST マルチキャスト MoH を設定する方法は、SRST モードでの設定と同じです（例 7-1 を参照）。ただし、ルータに対して設定するマルチキャスト アドレスは、目的の動作によって異なります。フラッシュからのマルチキャスト MOH が SRST モードのみで必要な場合（たとえば、SRST モードでないときに、リモート デバイスで受信する MOH が中央の MOH サーバから発信される場合）は、ルータに対して設定するマルチキャスト アドレスとポート番号が、中央サイトの MOH サーバのオーディオ ソースと重複しないようにする必要があります。重複していると、リモート デバイスは、設定されているユーザ / ネットワーク保留オーディオ ソースに応じて、ローカル ルータのフラッシュから MOH を継続的に受信することがあります。

支店ルータのフラッシュからのマルチキャスト MOH が常に必要になる場合は、支店ルータ上で設定された内容と同じマルチキャスト IP アドレスとポート番号をもつオーディオ ソースを使用して、中央サイトのサーバを設定する必要があります。このシナリオでは、マルチキャスト MoH オーディオ ストリームが、常にルータのフラッシュから発信されるので、中央サイトの MOH サーバのオーディオ ソースが WAN を通過する必要はありません。

中央サイトのオーディオ ストリームが WAN を通過しないようにするには、次のいずれかの方法を使用してください。

- 最大のホップ カウントを設定する

  中央サイトの MoH オーディオ ソースが、中央サイトの LAN より先に流れないように、最大ホップ カウントまたは TTL を十分に小さく設定します。

  （注） マルチキャストの TTL の値が減少する（または満了する）のは、パケットがレイヤ 3 インターフェイスを通過するときのみです。

- WAN インターフェイス上でアクセス コントロール リスト（ACL）を設定する

  中央サイトの WAN インターフェイス上で ACL を設定して、マルチキャスト グループ アドレス宛のパケットがインターフェイスから発信されないようにします。

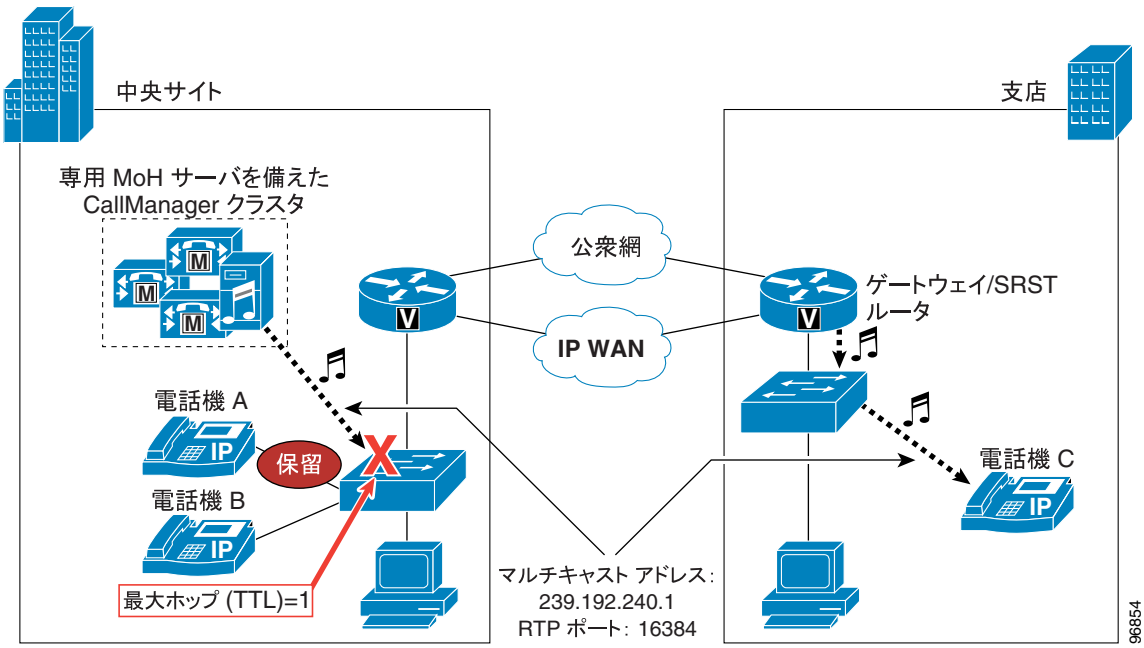
- WAN インターフェイス上でマルチキャスト ルーティングを無効にする

  WAN インターフェイス上ではマルチキャスト ルーティングを設定しないでください。設定しなければ、マルチキャスト ストリームが WAN に転送されないことが保証されます。

図 7-6 は、SRST モードでないときにリモート ルータのフラッシュからマルチキャスト MOH を流す仕組みを示しています。電話機 A で電話機 C を保留にすると、電話機 C は、ローカル SRST ルータからマルチキャスト MoH を受信します。この図では、MoH サーバは、（RTP ポート 16384 上で）

239.192.240.1 にマルチキャスト オーディオ ソースを流します。しかし、最大ホップ数が 1 に制限されているので、このストリームは、ローカル MoH サーバのサブネットから WAN を通過して外に出ないことが保証されています。同時に、支店の SRST ルータまたはゲートウェイは、フラッシュからオーディオ ストリームをマルチキャストします。このストリームも、マルチキャスト アドレスとして 239.192.240.1 を使用し、RTP ポート番号として 16384 を使用します。電話機 A で Hold ソフトキーを押すと、電話機 C は、SRST ルータから発信された MOH オーディオ ストリームを受信します。

図 7-6　支店ルータのフラッシュからのマルチキャスト MOH



この方法を使用してマルチキャスト MOH を配信する場合は、Cisco CallManager クラスタ内のすべてのデバイスが、同じユーザ保留およびネットワーク保留オーディオ ソースを使用するように設定し、すべての支店ルータに同じマルチキャスト グループ アドレスとポート番号を設定します。保留側のユーザまたはネットワーク保留オーディオ ソースは、オーディオ ソースを特定するときに使用されるため、クラスタ内に複数のユーザまたはネットワーク保留オーディオ ソースを設定する場合、リモートの被保留側が常にローカルの MOH ストリームを受信することを保証する手段はありません。たとえば、中央サイトの電話機に設定されているオーディオ ソースが、そのユーザおよびネットワーク保留オーディオ ソースとして、グループ アドレス 239.192.254.1 を使用するものとします。この電話機がリモート デバイスを保留にすると、ローカル ルータのフラッシュの MoH ストリームがマルチキャスト グループ アドレス 239.192.240.1 に送信される場合でも、リモート デバイスは 239.192.254.1 に加わろうとします。代わりに、ネットワーク内のすべてのデバイスがマルチキャスト グループ アドレス 239.192.240.1 でユーザ / ネットワーク保留オーディオ ソースを使用するように設定し、すべての支店ルータが 239.192.240.1 でフラッシュからマルチキャストするように設定すると、リモート デバイスはすべて、そのローカル ルータのフラッシュから MOH を受信します。

フラッシュからマルチキャスト MOH を流すように設定された複数の支店ルータを含むネットワークでは、クラスタ内に 51 を超える固有 MOH オーディオ ソースを含めることができます。支店サイトの各ルータは、フラッシュから固有オーディオ ソースをマルチキャストできます。ただし、すべてのルータが同じマルチキャスト グループ アドレス上でこのオーディオをマルチキャストする必要があります。また、中央サイトの MOH サーバは、この同じマルチキャスト グループ アドレス上で MOH ストリームをマルチキャストできます。したがって、100 の支店サイトそれぞれがフラッ

シュからオーディオ ファイルをマルチキャストする場合、クラスタには 101 の固有 MOH オーディオ ソース（100 の支店ストリームと 1 つの中央サイト ストリーム）を含めることができます。中央サイトで複数の固有オーディオ ストリームが必要な場合は、追加の MOH サーバまたは外部メディア サーバから固定 / ライブ ソースを流すことができます（P.7-11 の「複数の固定またはライブ オーディオ ソースの使用」を参照）。ただし、サーバごとに複数のオーディオ ソースを設定しないでください。

分散型マルチサイト配置

分散型コール処理を使用するマルチサイト IP テレフォニー配置には、通常、サイト間の WAN または MAN 接続が含まれます。これらの低速リンクは、通常、帯域幅とスループットの障害になります。リンク上での帯域幅使用量を最小限にするには、リンクを通過するすべての MOH オーディオ ストリームとして G.729 コーデックを使用することをお勧めします。ただし G.729 コーデックは、音楽用ではなく、音声用に最適化されているので、MoH トランスポートに G.729 がもたらす品質の低下よりも、帯域幅の節約がはるかに重要な問題である WAN/MAN 上でのみ、G.729 を使用してください。

集中型マルチサイト配置の場合とは異なり、WAN を介して移動する MOH オーディオ ストリーム用に G.711 が必要になる可能性がある状況では、分散型マルチサイト環境で MOH オーディオ ストリームが G.711 を使用するように強制することはできません。MOH サーバが別の Cisco CallManager リージョンに配置されている状況で、このリージョンとクラスタ間トランクのリージョンとの間で G.711 コーデックが設定されている場合でも、2 つのクラスタ間のコールが一方の電話機によって保留にされたときは、元の音声コールのコーデックが保持されます。これらのクラスタ間コールは、一般に、帯域幅の節約のために G.729 を使用して符号化されるため、一方のクラスタからの MOH ストリームも G.729 を使用して符号化されます。

さらに、Cisco CallManager クラスタ間のコール（クラスタ間コール）では、マルチキャスト MOH はサポートされません。したがって、クラスタ間トランク（ICT）上で MoH が必要な場合は、各 Cisco CallManager クラスタで少なくとも 1 つのユニキャスト MoH リソースを設定する必要があります。

分散型クラスタ間環境では、適切なマルチキャスト アドレス管理も、設計上の重要な考慮事項です。分散型ネットワーク全体で流れるリソースの重複を防止するために、いかなる MoH オーディオ ソース マルチキャスト アドレスも、配置内のすべての Cisco CallManager クラスタに対して固有でなければなりません。

WAN を介したクラスタ化

その名前が示すように、WAN を介したクラスタ配置には、他のマルチサイト配置と同様、低速 WAN リンクを含みます。したがって、これらの配置にも、G.729 コーデック、マルチキャスト トランスポート メカニズム、および低速 WAN リンクを介した MOH トラフィックに対して欠かせない安定した QoS の、3 つの要件が必要です。

さらに、このタイプの設定では、WAN の各端部に MoH サーバ リソースを配置することも必要です。WAN に障害が発生した場合には、WAN の各端部のデバイスは、ローカルに配置された MoH サーバから、引き続き MoH オーディオ ストリームを受信できます。さらに、適切な MoH 冗長設定がきわめて重要です。WAN の各端部のデバイスには、MRGL を指定する必要があります。この MRGL の MRG には、少なくとも 1 つのローカル リソースが最優先になった MoH リソースの優先順位リストが必要です。プライマリ サーバが使用不能になるか、要求を処理できない場合に備えて、この MRG に対して、MoH リソースを追加設定しておく必要があります。WAN のローカル側のリソースは使用不能になった場合に備えて、リスト内で他に少なくとも 1 つの MoH リソースは、リモート側の MoH リソースを指定しておく必要があります。

ユニキャストとマルチキャスト MoH コール フローの詳細

図 7-7 は、標準的なマルチキャスト コール フローを示しています。この図に示されているように、電話機 A で Hold ソフトキーが押されると、Cisco CallManager は、Close Receive Channel（受信チャネルのクローズ）と Stop Media Transmission（メディア送信の停止）を電話機 A と電話機 B の両方に指示します。このアクションは、実質的に、RTP 双方向オーディオ ストリームを停止させます。次に、Cisco CallManager は、マルチキャスト グループ アドレス 239.192.240.1 から、Start Multicast Media Reception（マルチキャスト メディア受信の開始）を電話機 B（非保留側）に指示します。電話機 B は、このグループに加わることを示す、インターネット グループ管理プロトコル（IGMP）メンバーシップ レポートを発行します。

一方、MoH サーバがこのマルチキャスト グループ アドレスに RTP オーディオを発信したので、電話機 B はそのマルチキャスト グループに加わった後、MoH ストリームの受信を開始します。電話機 A で Resume ソフトキーが押されると、Cisco CallManager は、電話機 B に Stop Multicast Media Reception（マルチキャスト メディア受信の停止）を指示し、実質的に MoH セッションを終了させます。次に、Cisco CallManager は、電話機 A と電話機 B 間の通話の開始時に送信するように、両方の電話機に一連の Open Receive Channel（受信チャネルのオープン）メッセージを送信します。その後すぐに、Cisco CallManager は、互いの IP アドレス（この場合、10.96.200.12 と 10.96.200.13）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分かりやすいように、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。

図 7-7　マルチキャスト MOH コール フローの詳細

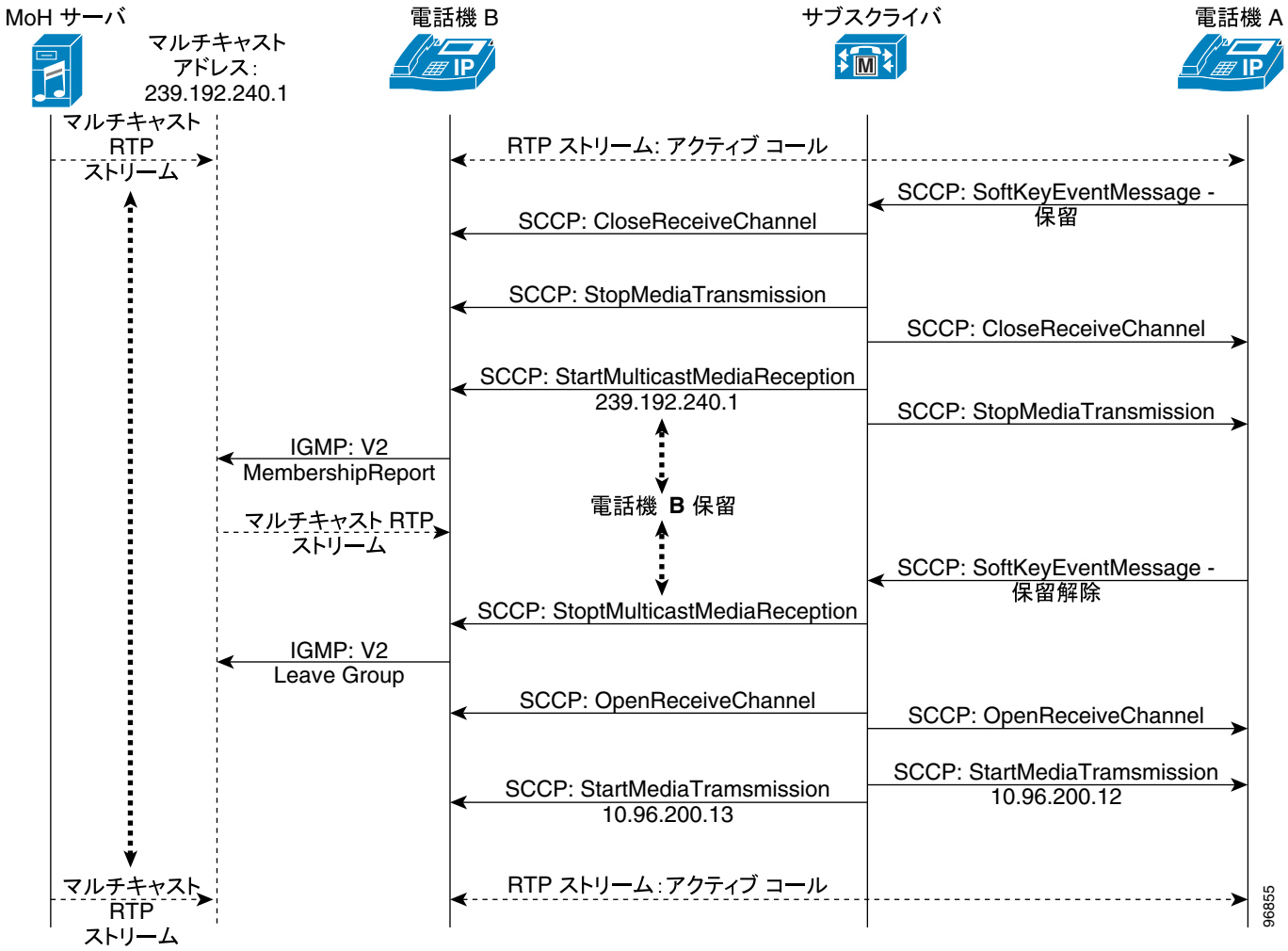
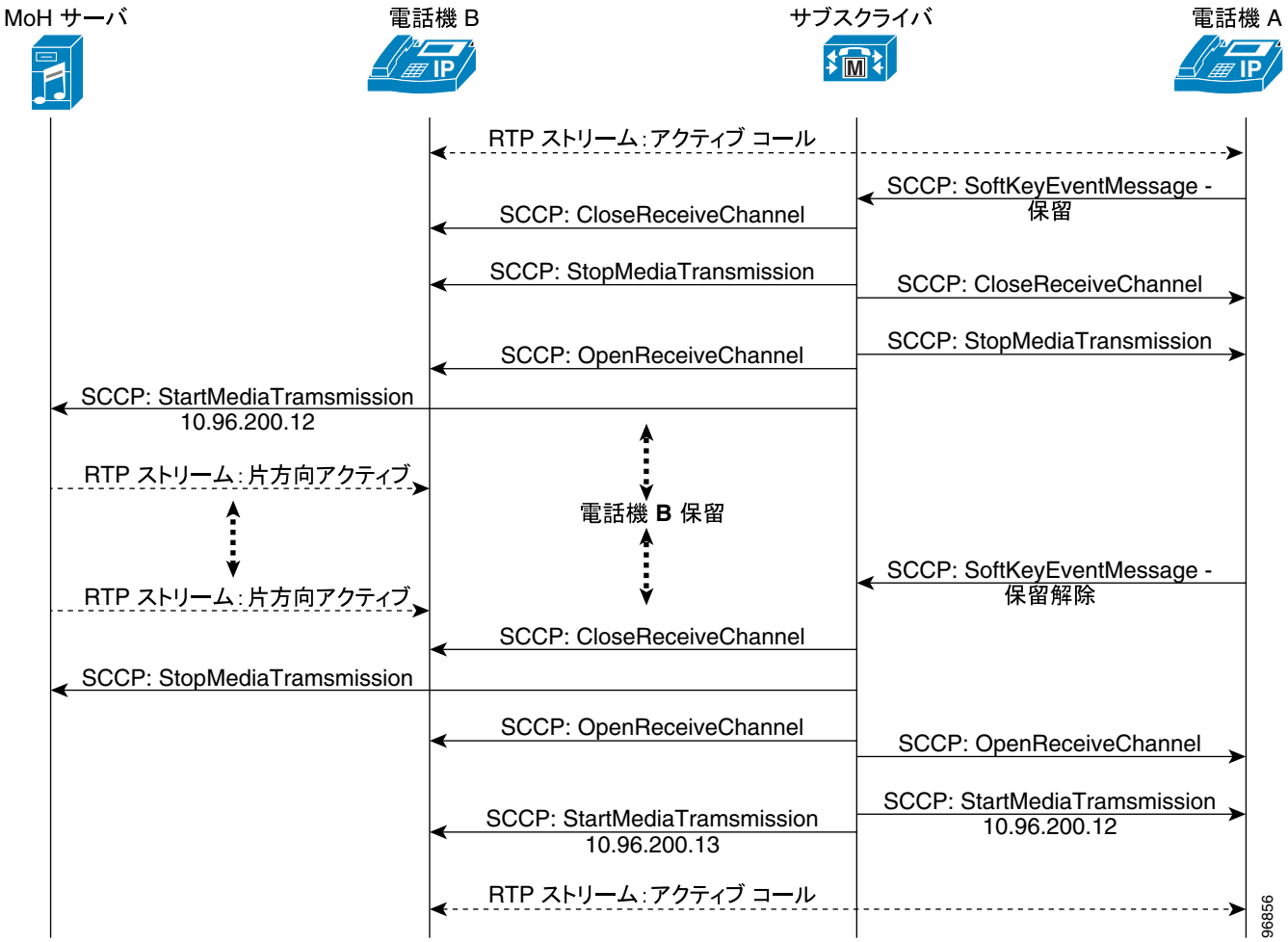


図 7-8 は、ユニキャスト MOH コール フローを示しています。このコール フロー図では、電話機 A で Hold ソフトキーが押されると、Cisco CallManager は、Close Receive Channel（受信チャネルのクローズ）と Stop Media Transmission（メディア送信の停止）を電話機 A と電話機 B の両方に指示します。このアクションは、実質的に、RTP 双方向オーディオ ストリームを停止させます。この時点まで、ユニキャストとマルチキャストの MOH コール フローは、まったく同じように動作します。

次に、Cisco CallManager は、Open Receive Channel（受信チャネルのオープン）を電話機 B（被保留側）に指示します。これは、マルチキャストの場合とまったく異なっています。マルチキャストでは、Cisco CallManager は、Start Multicast Media Reception（マルチキャスト メディア受信の開始）を被保留側に指示します。次に、Cisco CallManager は、MoH サーバに、電話機 B の IP アドレスへの Start Media Transmission（メディア送信の開始）を指示します。これも、マルチキャスト MoH コール フローとはまったく異なる動作です。マルチキャストの場合、マルチキャスト グループ アドレスに加わるように、電話機に指示します。この時点で、MoH サーバは、片方向ユニキャスト RTP 音楽ストリームを電話機 B に送信します。電話機 A で Resume ソフトキーが押されると、Cisco CallManager は、Stop Media Transmission（メディア送信の停止）を MoH サーバに指示し、Close Receive Channel（受信チャネルのクローズ）を電話機 B に指示して、実質的に MoH セッションを終了させます。マルチキャスト シナリオの場合と同じように、Cisco CallManager は、一連の Open

Receive Channel（受信チャネルのオープン）メッセージ、および Start Media Transmissions（メディア送信の開始）メッセージを電話機 A と電話機 B に相互の IP アドレスを使用して送信します。電話機は、RTP 双方向オーディオ ストリームを介して再び接続されます。

図 7-8　ユニキャスト MOH コール フローの詳細



CHAPTER 8

コール処理

この章では、スケーラブルで復元性のあるコール処理システムの設計ガイドラインを示し、Cisco CallManager と H.323 ゲートキーパーの設計を中心に説明します。

Cisco CallManager アーキテクチャでは、複数の物理サーバを 1 つの IP PBX システムとして連携させることができます。このサーバ グループを「クラスタ」と呼びます。Cisco CallManager サーバのクラスタは、設計上の制限事項を遵守している限り、IP ネットワークを介して分散していてもかまいません。クラスタを使用することで、空間的な冗長性、およびそれに伴う復元性を IP Communications システムの設計にもたらすことができます。

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。

ここでは、次に示す個々の要件に基づいて、適切なハードウェアおよび配置シナリオを選択する方法についても説明します。

- 規模：ユーザ、ゲートウェイ、アプリケーションなどの数
- パフォーマンス：コールのレート
- 復元性：冗長性の規模

Cisco CallManager クラスタのガイドライン

ここでは、Cisco CallManager クラスタを形成しているサーバが実行する各種の機能について説明し、必要な規模、パフォーマンス、および復元性を達成するようにサーバを配置する方法について、ガイドラインを示します。

ハードウェア プラットフォーム

Cisco CallManager クラスタでは、必要となる規模、パフォーマンス、および冗長性に応じて、さまざまなタイプのサーバを利用します。利用するサーバの範囲は、冗長性のないシングル プロセッサのサーバから、冗長性の高いマルチプロセッサ ユニットにまで及びます。

Cisco CallManager は、特定のハードウェア プラットフォーム上でのみサポートされます。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 プラットフォームには、それぞれ固有のメモリ要件があります。この要件については、次の Web サイトにある製品情報 2864『*Physical Memory Recommendations For Cisco CallManager Version 4.0 and Later*』で説明しています。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_bulletin0900aecd80284099.html

表 8-1 では、クラスタ内で使用できる一般的なサーバのタイプとその主な特性を一緒にリストしています。

表 8-1　Cisco CallManager サーバのタイプ

サーバ タイプ	特性
標準サーバ（高可用性でない）	• 単一プロセッサ • 単一電源装置 • 非 RAID ハードディスク
高可用性標準サーバ	• 単一プロセッサ • 複数の電源装置 • 単一 SCSI RAID ハードディスク アレイ
高性能サーバ	• 複数のプロセッサ • 複数の電源装置 • 複数の SCSI RAID ハードディスク アレイ

サーバは、IP ネットワークに加えて電源と冷却についても可用性の高い環境に配置する必要があります。建物の電力が必要な可用性を備えていない場合は、サーバの電力を無停電電源装置（UPS）から供給する必要があります。二重化電源を備えたサーバについても、それぞれの電源を 2 つの異なる電力源に接続しておくと、1 つの電源回路が故障しただけでサーバに障害が発生することを回避できます。

IP ネットワークへの接続性によっても、最大限のパフォーマンスと可用性が保証されます。Cisco CallManager サーバは、イーサネットに 100 Mbps 全二重で接続する必要があります。小規模な配置で 100 Mbps が使用可能でない場合、10 Mbps 全二重を使用してください。比較的新しいサーバでは、多くの場合 1000 Mbps 全二重も選択肢の 1 つになります。この設定を行うには、ネットワーク インターフェイス カード（NIC）を 100 Mbps または 10 Mbps のデュプレックス モードに設定し、イーサネット スイッチ ポートも手動で調整します。

(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。最善の方法は、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。

2 枚のイーサネット NIC を備えたサーバ プラットフォームでは、NIC チーミングをサポートできます。この機能は、使用できるかどうかは製造業者によって異なりますが、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。この機能を利用すると冗長性が向上するため、特定の状況下では有益です。ただし、正しく配置するには、事前に IP インフラストラクチャを慎重に設計する必要があります。シスコおよび Hewlett-Packard（HP）のサーバ プラットフォームにチーミング ドライバをインストールする方法の詳細については、次の Web サイトにあるドキュメントを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/driver/hp_team7.htm

すべての Cisco CallManager クラスタに次のガイドラインが適用されます。

(注) 1 つのクラスタに複数のサーバ プラットフォームを組み合せることができますが、クラスタ内のすべてのサーバでは、同じ Cisco CallManager ソフトウェア リリースを実行する必要があります。

- 通常の環境では、同一 LAN または MAN 内にクラスタのすべてのメンバーを入れます。クラスタのすべてのメンバーを同一の VLAN またはスイッチに配置することは、お勧めしません。
- 冗長性を持たせるには、クラスタのメンバーを次のように配置して、インフラストラクチャや建物で発生した障害によって受ける影響を最小限に抑える必要があります。
  - 同じディストリビューション スイッチまたはコア スイッチに、複数のアクセス スイッチが接続されている
  - 複数のディストリビューション スイッチまたはコア スイッチに、複数のアクセス スイッチが接続されている
  - 同じ LAN または MAN の中に複数の建物がある
- クラスタが IP WAN にわたって構築されている場合、P.2-17 の「IP WAN を介したクラスタ化」の項を参照して、IP WAN を介したクラスタリングのガイドラインに従ってください。

Cisco CallManager クラスタのサービス

Cisco CallManager クラスタの内部には、それぞれ固有のサービスを提供する複数のサーバが存在します。これらの各サービスは、同じ物理サーバ上で他のサービスと共存できます。たとえば、小規模なシステムでは、1 台のサーバがパブリッシャ、バックアップ サブスクライバ、Music On Hold（MOH）サーバ、TFTP サーバ、CTI Manager、およびコンファレンス ブリッジを兼ねることができます。クラスタの規模とパフォーマンスを強化する必要が高まった場合は、これらのサービスの多くを 1 台の専用物理サーバに移行する必要があります。

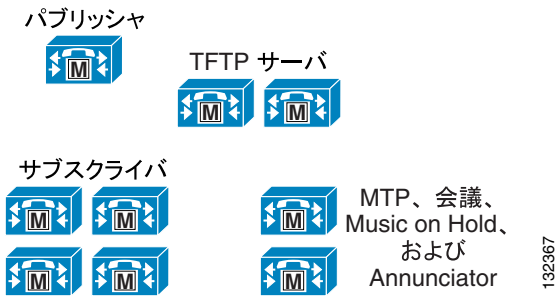
Cisco CallManager 3.3 および 4.*x* からは、1 つのクラスタに、20 のサーバを組み込めるようになりました。20 のサーバのうち、最大 8 つのサーバが、コール処理を提供する Cisco CallManager サービスを実行できます。残りのサーバは、専用データベース パブリッシャ、トリビアル ファイル転送プロトコル（TFTP）専用サーバ、または Music On Hold（MOH）サーバとして設定できます。メディア ストリーミング アプリケーション（コンファレンス ブリッジやメディア ターミネーション ポイント）も、クラスタに登録される別個のサーバにインストールできます。

Cisco MCS 7815 または同等のサーバを含んだクラスタを配置するときは、クラスタ内の 2 つのサーバに関して制限事項があります。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。この構成では、サポートされるユーザの最大数は 300 です。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、専用のパブリッシャを配置することをお勧めします。

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、クラスタのユーザ数が 1,000 を超えないようにする必要があります。シングル サーバ構成では、Survivable Remote Site Telephony（SRST）も配置して、Cisco CallManager が使用不可になっている間にサービスが提供されるようにしない限り、冗長性はありません。シスコでは、実稼働環境でシングル サーバ配置を採用することはお勧めしません。ロード バランシングは、パブリッシャがバックアップ コール処理サブスクライバである場合には実装できません。

図 8-1 では、一般的な Cisco CallManager クラスタを示しています。

図 8-1　一般的な Cisco CallManager クラスタ



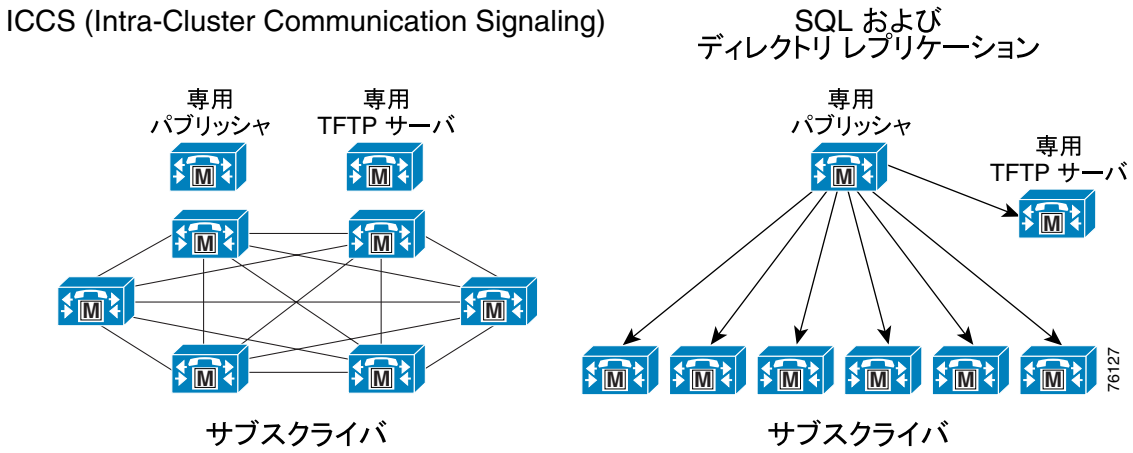
クラスタ内通信

Cisco CallManager クラスタ内の通信（クラスタ内通信）には、2 種類あります（図 8-2 を参照）。1 つは、すべてのデバイス設定情報を含んでいるデータベースを配布するためのメカニズムです。コンフィギュレーション データベースは、パブリッシャ サーバに保存され、読み取り専用のコピーがクラスタのサブスクライバ メンバーに複製されます。パブリッシャで加えられた変更は、サブスクライバ データベースに伝達され、クラスタのメンバー全体で設定を一貫させると共に、データベースの空間的な冗長性を実行します。

2 タイプ目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。この情報は、Cisco CallManager Service を実行している、クラスタのすべてのメンバー全体で共有されます。クラスタのメンバーと関連ゲートウェイとの間で、コールの最適なルーティングが確保されます。

Lightweight Directory Access Protocol（LDAP）ディレクトリ情報も、クラスタ内のすべてのサーバ間で複製されます。LDAP ディレクトリは、パブリッシャによって他のすべてのサーバに複製されます。Cisco CallManager は、Microsoft の Active Directory や Netscape Directory などの、企業の LDAP ディレクトリに統合できます。この複製は、配置される統合方式によって異なり、このマニュアルでは説明していません。ディレクトリ統合の詳細については、第 14 章「ディレクトリ アクセスとディレクトリ統合」を参照してください。

図 8-2　クラスタ内通信



パブリッシャ

「パブリッシャ」はすべてのクラスタに必要で、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 サービスとディレクトリ サービスを提供します。パブリッシャ サーバは、コンフィギュレーション データベースに読み取りと書き込みのアクセスができる唯一のサーバです。設定が変更されたとき、クラスタの他のメンバーは、データベースの読み取り専用コピーを保持します。1,250 ユーザを超える大規模なシステムの場合、パブリッシャ サーバ上ではコール処理を実行しないことをお勧めします。実行しないことで、管理操作がテレフォニー ユーザからの影響を受けなくなります。

クラスタ内のサーバは、初期化時にパブリッシャのデータベースを使用しようとします。パブリッシャが使用不可になっている場合は、自身のハード ドライブにあるローカルの読み取り専用コピーを使用します。

システムが動作していても、パブリッシャが使用不可になっている場合は、次の操作を実行できません。

- 設定の変更
- 自動転送の変更
- エクステンション モビリティのログイン操作およびログアウト操作

エクステンション モビリティは、データベースに読み取りと書き込みのアクセスを行う必要があるため、パブリッシャなしでは機能しません。したがって、このサービスはパブリッシャ上でのみ実行することをお勧めします。

パブリッシャ用のハードウェア プラットフォームは、クラスタの規模とパフォーマンスを基準として選択します。パブリッシャは、コール処理サブスクライバと同等のパフォーマンスを持つものにすることをお勧めします。可能な場合には、パブリッシャを高可用性サーバにして、ハードウェアの障害による影響を最小限に抑えるようにします。

コール処理サブスクライバ

Cisco CallManager ソフトウェアをインストールするときに、パブリッシャとサブスクライバという 2 タイプのサーバを定義できます。これらの用語は、データベース間の関係をインストール時に定義するために使用されています。ソフトウェアをインストールしたときに使用可能になる唯一のサービスが、データベース サービスです。すべてのサブスクライバは、パブリッシャをサブスクライブして、データベースとディレクトリの情報の読み取り専用コピーを取得します。

コール処理サブスクライバは、Cisco CallManager サービスが使用可能になっているサーバです。このサービスが使用可能になった時点で、このサーバはコール処理機能を実行できるようになります。電話、ゲートウェイ、メディア リソースなどのデバイスが登録やコール発信を実行できるのは、このサービスが使用可能になっているサーバに対してのみです。Cisco CallManager Release 3.3 より前では、このサービスを使用可能にできるのはクラスタ内の 6 つのサーバのみでした。これ以降のリリースでは、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（P.8-6 の「コール処理の冗長性」を参照）、コール処理サブスクライバは、プライマリ（アクティブ）サブスクライバまたはバックアップ（スタンバイ）サブスクライバのどちらかになります。ロード バランシングを実装する場合は、サブスクライバがプライマリ サブスクライバとバックアップ サブスクライバの両方を兼ねることもあります。クラスタの設計を計画するときは、通常はコール処理サブスクライバにこの機能を割り当てます。大規模なクラスタや高性能クラスタでは、パブリッシャおよび TFTP の機能をコール処理サーバ上で使用可能にしないでください。コール処理サブスクライバは、採用する冗長性方式に応じて、通常は専用ペアまたは共有ペアのどちらかで運用します。1：1 冗長性では、専用ペアを使用します。2：1 冗長性では、各ペアに含まれるサーバ 1 台（バックアップ サーバ）を共有する、2 組のサーバを使用します。

ハードウェア プラットフォームは、サーバの規模、パフォーマンス、冗長性、およびコストに応じて選択します。規模とパフォーマンスについては、P.8-13 の「Cisco CallManager プラットフォームのキャパシティ プランニング」の項で説明しています。冗長性については、P.8-6 の「コール処理の冗長性」の項で説明しています。

コール処理の冗長性

すべてのバージョンの Cisco CallManager で、次の冗長性設定の中から選択できます。

- 2:1 冗長性方式：プライマリ サブスクライバ 2 台ごとに、1 つの共用バックアップ サブスクライバを設置します。
- 1:1 冗長性方式：プライマリ サブスクライバごとに、1 つのバックアップ サブスクライバを設置します。

1:1 冗長性方式では、フェールオーバー期間だけがクラスタに影響を与えるアップグレードが可能です。このフェールオーバー メカニズムは、IP Phone のフェールオーバー レート、毎秒約 100 台の登録を実現できるように拡張されました。

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　パブリッシャ サーバをアップグレードします。

ステップ 2　TFTP 専用サーバを 1 台ずつアップグレードします。クラスタ内の他のサーバをアップグレードする前に、このサーバをリブートし、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機します。

ステップ 3　Music On Hold（MOH）専用サーバおよびその他のメディア リソース サーバを 1 台ずつアップグレードします。

ステップ 4　バックアップ サブスクライバを 1 台ずつアップグレードします。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ます。

ステップ 5　プライマリ サブスクライバをバックアップ サブスクライバにフェールオーバーし、プライマリ サブスクライバ上の Cisco CallManager サービスを停止します。

ステップ 6　プライマリ サブスクライバを 1 台ずつアップグレードしてから、Cisco CallManager サービスを再び使用可能にします。

このアップグレード方法では、異なるバージョンの Cisco CallManager ソフトウェアを実行しているサブスクライバ サーバにデバイスが登録される期間（フェールオーバー期間を除く）がありません。サブスクライバ間で通信する ICCS（Intra-Cluster Communication Signaling）プロトコルは、異なるソフトウェア バージョンを検出し、そのサブスクライバとの通信をシャットダウンする可能性があるので注意が必要です。

2:1 冗長性方式では、クラスタ内のサーバ数を減らすことができますが、その結果、アップグレード時に障害が発生する可能性があります。

（注）　10,000 台以上の IP Phone が 2 つのプライマリ サブスクライバに登録される場合は、1:1 冗長性を使用する必要があります。これは、1 つのバックアップ サブスクライバで 10,000 台以上のバックアップ登録はできないからです。

コール処理サブスクライバの冗長性

次の図では、Cisco CallManager でコール処理の冗長性を実現するための一般的なクラスタ構成を示しています。

図 8-3　基本的な冗長性方式

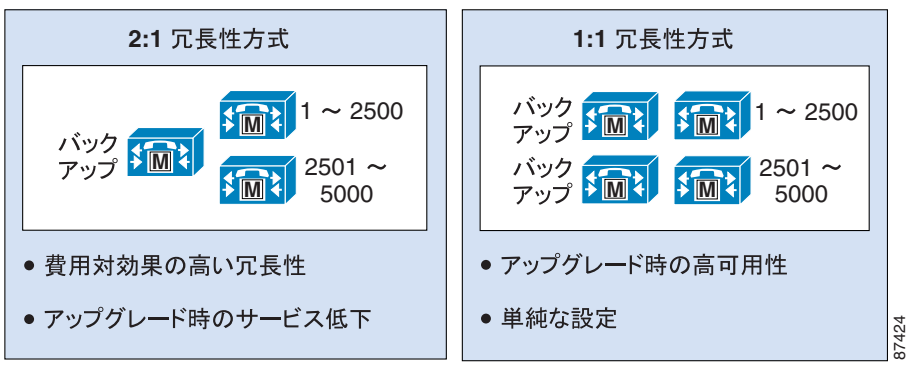


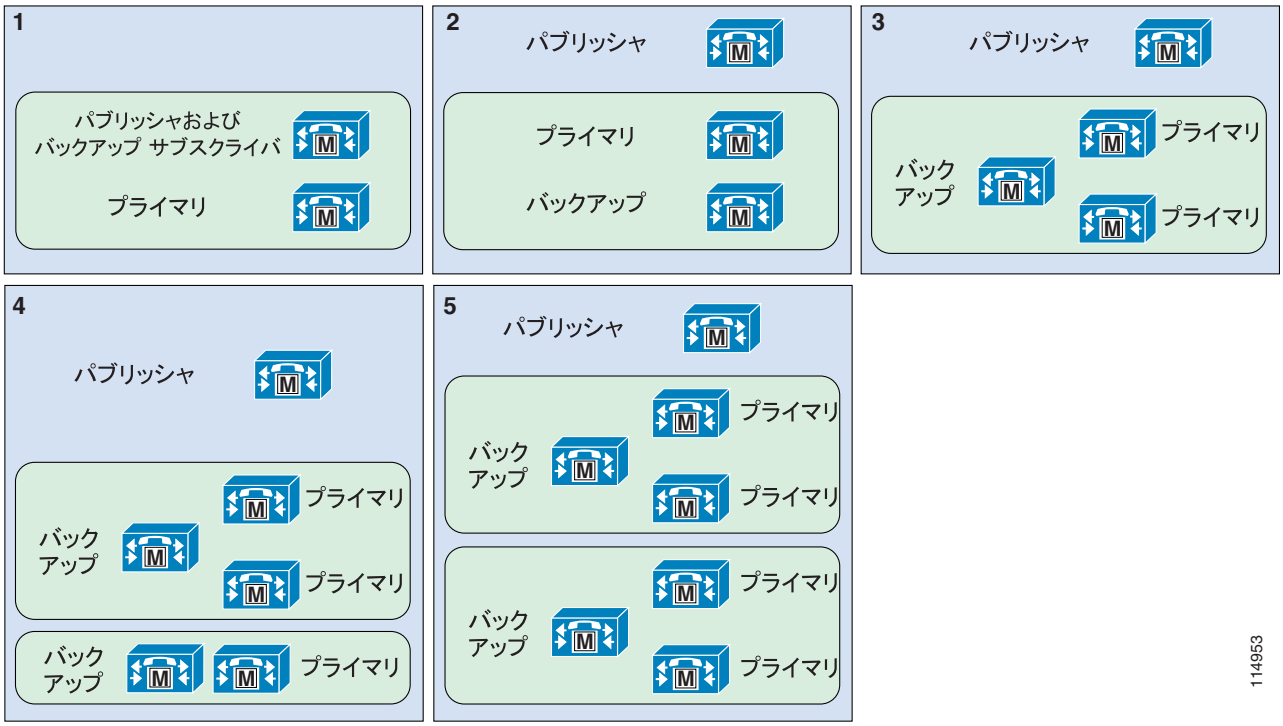
図 8-3 では、利用できる 2 つの基本的な冗長性方式を示しています。どちらの場合でも、バックアップ サーバは、障害の発生するプライマリコール処理サーバ 1 台分以上の処理能力を備えている必要があります。2：1 冗長性方式の場合、バックアップ サーバは、個々の配置の要件に応じて、障害の発生するコール処理サーバ 1 台分、または両方のプライマリ コール処理サーバに相当する処理能力を備えている必要があります。サーバのキャパシティの選定およびハードウェア プラットフォームの選択については、P.8-13 の「Cisco CallManager プラットフォームのキャパシティ プランニング」の項で説明しています。

図 8-4　1：1 冗長構成のオプション

図 8-4 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 8-5　2：1 冗長構成のオプション



ロード バランシング

1:1 冗長性方式を使用するもう 1 つの利点は、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のバランスを取ることができる点です。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。

ロード バランシングを使用すると、Cisco CallManager の冗長性グループとデバイス プールの設定値を使用して、デバイスにかかる負荷の半分までをプライマリ サブスクライバからセカンダリ サブスクライバに移すことができます。この方法で、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 サブスクライバやバックアップ サブスクライ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 1 台分の負荷を超えないようにします。

すべてのアクティブ サブスクライバにわたって、デバイスとコールの量をできる限り等しく分散することをお勧めします。たとえば、ゲートウェイ、トランク、ボイスメール ポート、ユーザをすべてのサブスクライバに等しく分散すると、障害による影響が最も小さくなります。

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。クラスタのサイズが大きくなった場合や、冗長性を強化する必要がある場合は、ロード バランシングおよび冗長性のために TFTP サーバを 2 台配置することをお勧めします。DHCP を使用して、または静的に TFTP オプションを設定するときは、TFTP サーバの IP アドレス アレイを定義するようにします。つまり、TFTP サーバのアドレスを複数定義します。このように定義すると、半数のデバイスでは TFTP サーバ A をプライマリとして使用し、TFTP サーバ B をバックアップとして使用するように割り当てて、他の半数のデバイスでは、TFTP サーバ B をプライマリとして使用し、TFTP サーバ A をバックアップとして使用するように割り当てることができます。TFTP 専用サーバのパフォーマンスを向上させるには、サービス パラメータを設定して、サーバ上で許容する同時 TFTP セッションの数を増やします。

Cisco CallManager クラスタをアップグレードするときは、パブリッシャの後に TFTP サーバをアップグレードし、次にその他のサーバをアップグレードすることを強くお勧めします。また、TFTP サーバをアップグレードした後は、すべてのコンフィギュレーション ファイルが再作成されるように十分な間隔を空けます。一般的な Cisco TFTP の BuildDuration 時間を使用するか、パフォーマンス モニタを使用して Cisco TFTP の DeviceBuildCount を監視して、これらの増加が止まるまで監視します。このアップグレード順序に従うと、新しいバイナリと設定変更が、クラスタ内の他のサービスをアップグレードする前に有効になります。電話やゲートウェイの個々のバイナリまたはファームウェア ロードを手動で追加する場合は、ファイルを必ずクラスタ内の各 TFTP サーバにコピーしてください。

Cisco CallManager Release 3.3 以降では、電話機のコンフィギュレーション ファイルは、旧バージョンの Cisco CallManager のように、TFTP サーバのハード ドライブにデフォルトで保存されることはありません。デフォルトでは、電話機のすべてのコンフィギュレーション ファイルは作成されると、TFTP サーバ上の RAM に置かれます。このデフォルト設定を変更して、電話機のコンフィギュレーション ファイルを TFTP サーバのハード ドライブに入れることができますが、これを行うと、TFTP のパフォーマンスに影響があります。したがって、このデフォルト設定を変更しないことをお勧めします。

TFTP サーバのハードウェア プラットフォームには、コール処理サブスクライバと同じものを使用することをお勧めします。

CTI Manager

CTI Manager は、クラスタ上で 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（Cisco CallManager Release 3.3 より前のリリースでは 6 つ）。復元性、パフォーマンス、および冗長性を最大限まで高めるには、CTI アプリケーションの負荷をクラスタ内の複数の CTI Manager に分散することをお勧めします。

一般に、アプリケーションによって制御または監視されるデバイスは、CTI Manager に使用するものと同じサーバ ペアに関連付けることをお勧めします。たとえば、IVR（interactive voice response; 音声自動応答装置）アプリケーションでは 4 つの CTI ポートが必要になります。1：1 冗長性と 50/50 ロード バランシングを使用する場合は、これらを次のように設定します。

- 2 つの CTI ポートは、サーバ A をプライマリ、サーバ B をバックアップ（セカンダリ）とする Cisco CallManager 冗長性グループを持っています。他の 2 つの CTI ポートは、サーバ B をプライマリ、サーバ A をバックアップとする Cisco CallManager 冗長性グループを持っています。
- 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、CTI Manager 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。

メディア リソース

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、ソフトウェア サービスによって提供されます。

メディア リソースには、次のものがあります。

- Music On Hold（MOH）：保留状態になっているデバイス、会議に転送または追加されるデバイスに対して、マルチキャストまたはユニキャストの保留音を提供できます（P.7-1 の「Music on Hold」を参照）。
- Annunciator サービス：電話番号を間違えていることや、コール ルーティングが使用不可になっていることを伝える場合に、トーンの代わりに音声アナウンスを流します（P.6-18 の「Annunciator」を参照）。
- コンファレンス ブリッジ：Ad Hoc 会議と Meet-Me 会議のための、ソフトウェア ベースの会議を提供します（P.6-8 の「会議」を参照）。
- メディア ターミネーション ポイント（MTP）サービス：H.323 クライアント、H.323 トランク、および Session Initiation Protocol（SIP）トランク用の機能を提供します（P.6-9 の「メディア ターミネーション ポイント（MTP）」を参照）。

クラスタ内でメディア リソースを実行する場合は、メディアの処理とネットワークに関する要件が追加される場合に備えて、すべてのガイドラインに準拠することが重要です。一般に、マルチキャスト MOH と Annunciator には専用サーバを使用せず、ソフトウェア ベースの大規模な会議と MTP に専用サーバを使用することをお勧めします（これらのサービスが、第 6 章「メディア リソース」、第 7 章「Music on Hold」で説明している設計ガイドラインの範囲内にない場合は除きます）。

音声アクティビティ検出

クラスタ内で音声アクティビティ検出（VAD）も使用不可にしておくことをお勧めします。デフォルトでは、Cisco CallManager サービス パラメータで VAD は使用不可になっています。H.323 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。

エクステンション モビリティ

クラスタ内でエクステンション モビリティを使用する場合は、必要となるキャパシティおよびパフォーマンスに応じて、選択するパブリッシャ ハードウェア プラットフォームが異なってきます。ユーザが電話でログインまたはログアウトしたときに、コンフィギュレーション データベースに含まれているコンフィギュレーションをアップデートし、TFTP サービスでコンフィギュレーション ファイルを再生成し、次にデバイスをリセットして、変更内容を有効にする必要があります。これらの処理のほとんどは、パブリッシャ上で発生します。

エクステンション モビリティでサポートサポートされている、現時点での上限は次のとおりです。

- Cisco CallManager Release 3.3
  - 1 時間あたりの順次ログインまたはログアウト：2,000 回
- Cisco CallManager Release 4.0
  - 1 時間あたりの順次ログインまたはログアウト：2,000 回
- Cisco CallManager Release 4.1
  - 1 時間あたりの順次ログインまたはログアウト：2,000 回
  - MCS 7845 パブリッシャは、1 時間あたり 4,500 回の順次ログインまたはログアウトをサポートします。

Cisco CallManager プラットフォームのキャパシティ プランニング

Cisco CallManager には、タイプの異なるデバイスを登録できます。たとえば、IP Phone、ボイスメール ポート、CTI（TAPI または JTAPI）デバイス、ゲートウェイ、および DSP リソース（トランスコーディングや会議）などです。これらの各デバイスは、登録先となるサーバ プラットフォームのリソースを必要とします。必要なリソースには、メモリ、プロセッサ使用、およびディスク I/O が含まれます。各デバイスは、トランザクション（通常、コールの形式）中に、追加のサーバ リソースを消費します。たとえば、1 時間当たり 6 回のコールだけを行うデバイスが消費するリソースは、1 時間当たり 12 回のコールを行うデバイスより少なくなります。

この項で示す推奨事項は、Cisco CallManager Capacity Calculator を、デフォルトのトレース レベルと CDR を有効にして使用し、その結果として得た計算に基づいています。コール処理に直接関係しない他の機能を使用不可にしたり、縮小したり、再設定したりすると、より高いレベルのパフォーマンスが得られます。こうした機能の一部を増やすと、システムのコール処理機能に影響を与える可能性があります。これらの機能には、トレース、コール詳細レコード、複雑なダイヤル プラン、およびサーバ上に共存するその他のサービスが含まれます。複雑なダイヤル プランには、複数のライン アピアランス、多くのパーティション、コーリング サーチ スペース、ルート パターン、変換、ルート グループ、ハント グループ、ピックアップ グループ、ルート リスト、自動転送の拡張使用、共存サービス、およびその他の共存アプリケーションが含まれています。こうした機能はすべて、Cisco CallManager サーバ内の追加リソースを消費します。

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にサポートされている最大量まで、サーバに追加の保証メモリを取り付ける。MCS 7825 および MCS 7835、または同等のサーバ クラスの大規模構成では、これらのサーバの RAM を倍に増やすことをお勧めします。このメモリ アップグレードが必要かどうかは、パフォーマンス モニタを使用して検証することでわかります。サーバが物理メモリを最大量近くまで使用すると、オペレーティング システムは、ディスクへのスワップを開始します。このスワッピングが発生した場合は、追加の物理メモリを取り付ける必要があることを示しています。個々のサーバのメモリに関する推奨事項については、次の Web サイトにある製品情報 2864『*Physical Memory Recommendations For Cisco CallManager Version 4.0 and Later*』を参照してください。

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_bulletin0900aecd80284099.html
- サポートされているハードウェア上で、書き込みキャパシティ 50% のバッテリ バックアップ付き書き込みキャッシュ（BBWC）を使用可能にする。この機能を使用する場合は、Small Computer System Interface（SCSI）コントローラ カードにバッテリを追加する必要が生じることがあります。
- MCS 7845 または同等のサーバ上で、トレース ファイルの位置を F: ドライブに設定する。この設定は、Cisco CallManager のサービス パラメータです。
- トレース ファイルのパーティションを再フォーマットして、小さなブロック サイズを使用するようにする（インストール済みオペレーティング システムのリリース ノートを参照）。この目的のためのユーティリティが提供されています。

多数のゲートウェイ、ルート パターン、トランスレーション パターン、およびパーティションを含む非常に大きなダイヤル プランをもつ Cisco CallManager クラスタでは、Cisco CallManager Service の初回始動時に、初期化に長い時間がかかる場合があります。デフォルトの時間内にシステムが初期化されない場合、サービス パラメータを変更して、設定の初期化時間を延長してください。サービス パラメータの詳細については、Cisco CallManager Administration オンライン ヘルプの「*Service Parameters*」を参照してください。

Cisco CallManager Release 3.1 および 3.2 を使用したコール処理

Cisco CallManager Release 3.1 および 3.2 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 Service を使用して最大 6 台のサーバ（4 台のプライマリ サーバと 2 台のバックアップ 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（Trivial File Transfer Protocol）、データベース パブリッシャ、Music on Hold などの専用機能に使用できます。
- サーバごとにコンピュータ / テレフォニー インテグレーション（CTI）接続またはアソシエーションを最大 800 設定できます。サーバ間で均等にバランスが取られる場合は、クラスタごとに最大 3,200 を設定できます。
- 各 H.323 デバイスは、Cisco CallManager Release 3.1 では H.323 コールを最大 500 件、Cisco CallManager Release 3.2 では H.323 コールを最大 1,000 件までサポートできます。
- 各クラスタは、最大 600 台の H.323（ゲートウェイとクライアント）デバイス、およびデジタル MGCP デバイスをサポートできます。

Cisco CallManager Release 3.3 以降を使用したコール処理

Cisco CallManager Release 3.3 以降には、次のガイドラインが適用されます。

- クラスタ内では、Cisco CallManager Service を使用して最大 8 台のサーバを使用可能にすることができます。それ以外のサーバは、TFTP、パブリッシャ、Music on Hold などの専用機能に使用できます。
- 標準サーバごとに CTI 接続またはアソシエーションを最大 800 設定できます。サーバ間で均等にバランスが取られる場合は、クラスタごとに最大 3200 設定できます。
- 高性能サーバごとに CTI 接続またはアソシエーションを最大 2,500 設定できます。サーバ間で均等にバランスが取られる場合は、クラスタごとに最大 10,000 設定できます。
- 各クラスタは、最大 30,000 台の IP Phone をサポートできます。
- 各クラスタは、最大 600 台の H.323（ゲートウェイとクライアント）デバイス、およびデジタル MGCP デバイスをサポートできます。

キャパシティの計算

以前のソフトウェア リリースでは、システムのキャパシティを計算するために、デバイスの重み、BHCA 係数、ダイヤル プランの重みを使用した、各種の方式を使用していました。Cisco CallManager Release 4.*x* では、この単純な方式がキャパシティ ツールで置き換えられ、より正確なシステム プランニングを実現しました（P.8-15 の「Cisco CallManager キャパシティ ツール」を参照）。キャパシティ プランニング ツールを使用できるのは、現時点ではシスコの従業員とシスコ代理店のみです。システムが次のガイドラインを満たしていない場合や、システムをさらに複雑にするためにキャパシティを確認する必要がある場合は、シスコのシステム エンジニアまたは Cisco Technical Assistance Center（TAC）にお問い合せください。

システムが次の要件を満たしている場合は、コンフィギュレーションを Cisco CallManager キャパシティ ツールで確認する必要はありません。

- システムに含まれているユーザ数が、サーバ プラットフォームの最大ユーザ数の 25% 未満である。
- 電話機ごとの平均の回線数が、1.1 を超えていない。
- ユーザごとの平均の Busy Hour Call Attempt（BHCA）が、1 時間あたり 6 コール未満である。
- ゲートウェイまたはトランクのどちらかを経由するトランキングが、20%（1 トランクあたり 5 ユーザ）以下である。
- ボイスメール ポートが 5%（1 ボイスメール ポートあたり 20 ユーザ）以下である。
- サーバ 1 台あたりの MOH ストリームが 20 以下である。

- CTI、JTAPI、および TAPI のデバイスがない。
- コンファレンス ブリッジが 5%（ブリッジ上の 1 ポートあたり 20 ユーザ）以下である。
- トランスコーダがない。
- トランキングに必要な最大コールをサポートする目的では、MTP のみ使用する。
- ロケーションが 20 未満である。
- システムには、上に定義されていないもの以外は、IP Phone、IP Communicator、ゲートウェイ、メディア リソース、ボイスメール ポート、トランクしか含まれていない。

Cisco CallManager がサポートできるユーザの最大数は、サーバ プラットフォームによって異なります（表 8-2 を参照）。

表 8-2　サーバ プラットフォームごとの最大デバイス数

サーバ プラットフォームの特性	サーバ 1 台あたりの最大ユーザ数[1]	高可用性サーバ[2]	高性能サーバ
Cisco MCS-7845（全モデル）[3]	7,500	あり	あり
Cisco MCS-7835（全モデル）	2,500	あり	なし
Cisco MCS-7825（全モデル）	1,000	なし	なし
Cisco MCS-7815（全モデル）[4]	300	なし	なし

1. 高可用性サーバでないプラットフォームは、非冗長インストレーションで最大 500 ユーザ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-7845-1400 サーバは、4 GB RAM へのメモリ アップグレードが必要です。また、Microsoft Windows 2000 Advanced Server を実行している必要があります。OS 2000.2.4 からロードされる MCS-7845-1400 サーバは Microsoft Windows 2000 Advanced Server がインストールされていますが、これより前の OS リリースでは、Microsoft Windows 2000 Server がインストールされています。アップグレードしない MCS-7845-1400 サーバでは、サーバ 1 台あたり 2,500 の IP Phone しかサポートされません。
4. MCS-7815 サーバは N+1 冗長性のみサポートし、クラスタのメンバーになることはできません。

サポートされるプラットフォーム、サードパーティ プラットフォーム、個々のハードウェア設定の最新情報については、次の Web サイトにあるオンライン資料を参照してください。

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

（注） 高可用性に対応していないプラットフォームの場合は、非冗長インストレーションとして、サポートされる IP Phone の最大数は、500 台になります。

Cisco CallManager キャパシティ ツール

Cisco CallManager キャパシティ ツールは、さまざまな情報を要求して、システムに必要となるサーバの最小限のサイズとタイプについて、見積もりを提示します。要求される情報には、IP Phone、ゲートウェイ、メディア リソースなどのデバイスの、タイプと数が含まれています。キャパシティ ツールは、デバイス タイプごとに 平均 BHCA と平均利用時間も要求します。たとえば、IP Phone で 1 時間あたり平均 5 件のコールが発生し、コールの平均持続時間が 3 分である場合、BHCA は 5 で、利用時間は 0.25 です（電話機上で 3 分間のコールが 5 件発生しているため、1 時間あたり 15 分、つまり 0.25 時間に相当します）。

デバイス情報に加えて、ルート パターンやトランスレーション パターンなどの、ダイヤル プランに関する情報も要求します。詳細をすべて入力すると、目的のサーバ タイプのプライマリ サーバがいくつ必要になるかについて、キャパシティ ツールが計算します。必要なキャパシティがクラスタ 1 つ分のキャパシティを超える場合は、クラスタの数も計算します。

キャパシティ ツールは、以前にデバイスの重み、BHCA 係数、コール タイプ係数、ダイヤル プランの重みと呼ばれていたメカニズムを置き換えるものです。

情報をキャパシティ カルキュレータに入力する場合は、次の項のガイドラインを使用してください。

電話機に関する計算

数

この値は、クラスタ内に設定する Skinny Client Control Protocol（SCCP）電話の合計数です。この数には、Cisco 7900 シリーズのすべての IP Phone、VG248 ポート、IP Communicator、およびその他のサードパーティ SCCP エンドポイント デバイスを含めます。この数には、アクティブになっていないものも含めて、設定済みのすべての電話を含める必要があります。

BHCA

この値は、すべての電話の平均 BHCA です。複数の電話で共用している回線がある場合、BHCA には、回線を共用しているそれぞれの電話のコールを 1 つとして含める必要があります。つまり、共用回線への 1 つのコールは、複数のコールとして計算します。それぞれ別の BHCA を生成する複数の電話グループがある場合、Cisco CallManager キャパシティ ツールで使用する BHCA 値は、次の方法で指定します。

たとえば、次の 2 クラスのユーザがいるとします。

- 20 BHCA の電話 100 台 = 合計 2,000 BHCA
- 4 BHCA の電話 5,000 台 = 合計 20,000 BHCA

すべての電話デバイスの合計 BHCA は、この場合 22,000 です。

この合計 BHCA を電話デバイスの合計数で除算して、次の値を算出します。

電話デバイス 1 台あたりの平均 BHCA = 22,000/5,100 = 4.31 BHCA

使用率

この値は、電話ごとの平均コール使用率です。コールが電話上に存在した、すべての時間を含めます。電話の実際の使用率は、100% を超えることがあります。これは、電話が 1 回線あたり複数のコールを許可しているか、頻繁に使用される複数のライン アピアランスを備えている場合です。使用率は、1 時間における百分率で測定します。たとえば、最も混雑している時間に 3 分間のコールが発生した電話は、5% 使用されたものと見なします。BHCA の計算と同じ方法を、複数の電話グループがある場合の平均使用率の計算にも使用することができます。電話に共用回線がある場合は、その電話の予想使用率のみ計算し、共用されている回線の実際の使用率は計算しません。Cisco CallManager キャパシティ ツールで使用できるのは、現時点では、すべての電話の平均使用率です。

ライン アピアランス

この値は、すべての電話の平均回線数です。同じ DN を持つ電話が複数のパーティション内に出現している場合は、複数のライン アピアランスと見なします。共用回線は 1 つの回線としてカウントしますが、BHCA と使用率が正しく計算されていることを確認してください。回線ごとに複数のコールが発生した場合、ライン アピアランスの数は増加しませんが、BHCA と使用率の計算には影響します。

ゲートウェイ

ゲートウェイの数

ゲートウェイの数は、ゲートウェイのタイプに応じて異なるため、次のいくつかのエントリに分けられています。

- MGCP T1/E1 ゲートウェイ

  この値は、Cisco CallManager データベース内に設定する必要のあるゲートウェイの合計数です。たとえば、Cisco IOS MGCP ゲートウェイは複数の T1 または E1 を保持できますが、単一のゲートウェイとして追加します。Cisco WS-6608 モジュールは、T1 または E1 ゲートウェイとして設定されているポートごとに、1 モジュールあたり最大で 8 つまで、ゲートウェイとして追加します。
- MGCP アナログ ゲートウェイ

  この値は、Cisco CallManager データベースに追加するアナログ ゲートウェイの合計数です。通常は、モジュール全体（WS-6624 または Cisco CallManager）またはハードウェア プラットフォーム（Cisco IOS ルータ プラットフォーム）を 1 つのゲートウェイとして追加します。
- H.323 ゲートウェイ

  モジュール全体またはハードウェア プラットフォームを、1 つのゲートウェイとして追加します。この数には、Cisco CallManager に定義されていないものの、H.323 トランク経由で使用される H.323 ゲートウェイは含みません。

DS0 の数

この値は、各タイプのゲートウェイがサポートする DS0 またはアナログ ポートの合計数です。DS0 の数は、次のように、ゲートウェイのタイプによって分かれています。

- T1 CAS

  24 *（T1 CAS スパンの数）
- T1（E1）PRI

  （23 または 30）*（PRI の合計数）
- H.323 ゲートウェイ

  （DS0 の合計数）/（すべてのデジタル、アナログ、IP インターフェイス上でサポートされるコールの数）

BHCA

この BHCA は、最も混雑している時間における、ゲートウェイ上のすべての DS0 またはアナログ ポートの平均値です。この平均値を計算する方法は、電話の BHCA に使用する方法と同じです。

使用率

この値は、最も混雑している時間における、すべての DS0 またはアナログ ポートの平均使用率です。

EM プロファイル

エクステンション モビリティ（EM）プロファイルには、電話の計算でも含めている、ライン アピアランスを含めます。エクステンション モビリティは、デバイスの数には影響しませんが、電話ごとのライン アピアランスの平均数が増加します。EM ユーザの BHCA および使用率は、ユーザのログイン先となる電話について、すでに計算したものです。

H.323 と SIP のトランク

トランクの数

この値は、Cisco CallManager データベース内に設定されるトランクの合計数です。ゲートキーパーが制御するトランクは、宛先の数の影響を受けません。このため、設定済みのゲートキーパー制御トランクごとに 1 つとしてカウントします。これは、Session Initiation Protocol（SIP）プロキシを使用する SIP トランクにも当てはまります。

コールの数

この値は、すべてのトランク上で許容できる同時発生コールの合計数です。許容されるコールの数は、通常はロケーションまたはゲートキーパーのコール アドミッション制御によって制御されます。許容されるコールの数には、リージョンとコーデックも影響することに注意してください。

使用率

この値は、すべてのトランクにわたる、すべてのコールの平均使用率です。これは、最も混雑している時間における百分率（%）です。使用率が 75% の場合は、コールが 1 時間あたり 45 分アクティブであることを意味します。

MTP の要件

MTP の要件についても、カルキュレータで別個に検討する必要があります。H.323 トランク上で MTP が必要となる場合（SIP トランクでは必須）、そのトランク上でのすべての同時発生コールで、MTP リソースが必要になります。

ゲートキーパーの考慮事項

1 台の Cisco IOS ゲートキーパーで、分散型コール処理環境で最大 100 の Cisco CallManager クラスタに対してコール ルーティングとコール アドミッション制御をサポートできます。複数のゲートキーパーを設定すると、数千の Cisco CallManager クラスタをサポートできます。Cisco IOS ゲートキーパーを使用して、H.323 ゲートウェイと Cisco CallManager 間の通信とコール アドミッション制御をサポートすることによって、ハイブリッド Cisco CallManager とトール バイパス ネットワークを実装することもできます。

ゲートキーパーのコール アドミッション制御は、ポリシーベースの方式であり、使用可能なリソースの静的設定を必要とします。ゲートキーパーは、ネットワーク トポロジを認識しないので、ハブアンドスポーク トポロジに制限されます。

Cisco 2600、2800、3600、3700、3800、および 7200 シリーズのルータはすべて、ゲートキーパー機能をサポートします。冗長性、ロード バランシング、および階層コール ルーティング用に、さまざまな方法で Cisco IOS ゲートキーパーを設定できます。この項では、ゲートキーパー ネットワークを構築するための設計要件について検討します。ただし、コール アドミッション制御やダイヤル プラン解決については扱いません。これらについては、第 9 章「コール アドミッション制御」と第 10 章「ダイヤル プラン」でそれぞれ説明しています。

ゲートキーパーの詳細については、次の Web サイトで入手可能な『*Cisco IOS H.323 Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_book09186a00801fcee1.html

ハードウェア プラットフォームの選択

ゲートキーパーのプラットフォームは、1 秒間あたりのコール数、および同時発生コール数に基づいて選択します。1 秒間あたりのコール数が多いほど、Cisco 3700、3800、7200 シリーズ ルータなどの高性能な CPU が必要になります。同時発生コールの数が大きいほど、より多くのメモリが必要になります。プラットフォームの選択に関する最新情報については、シスコ代理店またはシスコのシステム エンジニア（SE）にお問い合せください。

ゲートキーパーの冗長性

ゲートキーパーが、クラスタ間通信にすべてのコール ルーティングとアドミッション制御機能をサポートする場合は、冗長性が必要です。Cisco CallManager Release 3.3 より前では、ゲートキーパーの冗長性をサポートする方法は、ホットスタンバイ ルータ プロトコル（HSRP）だけでした。Cisco CallManager Release 3.3 以降、ゲートキーパーの冗長性をサポートする方法として、ゲートキーパー クラスタリングと冗長ゲートキーパー トランクも使用できるようになりました。次の項では、これらの方法について説明します。

（注） 可能な場合、ゲートキーパーの冗長性をサポートするには、ゲートキーパー　クラスタリングを使用することをお勧めします。冗長性に HSRP を使用するのは、ソフトウェア機能セットでゲートキーパー クラスタリングが利用できない場合だけにしてください。

ホットスタンバイ ルータ プロトコル（HSRP）

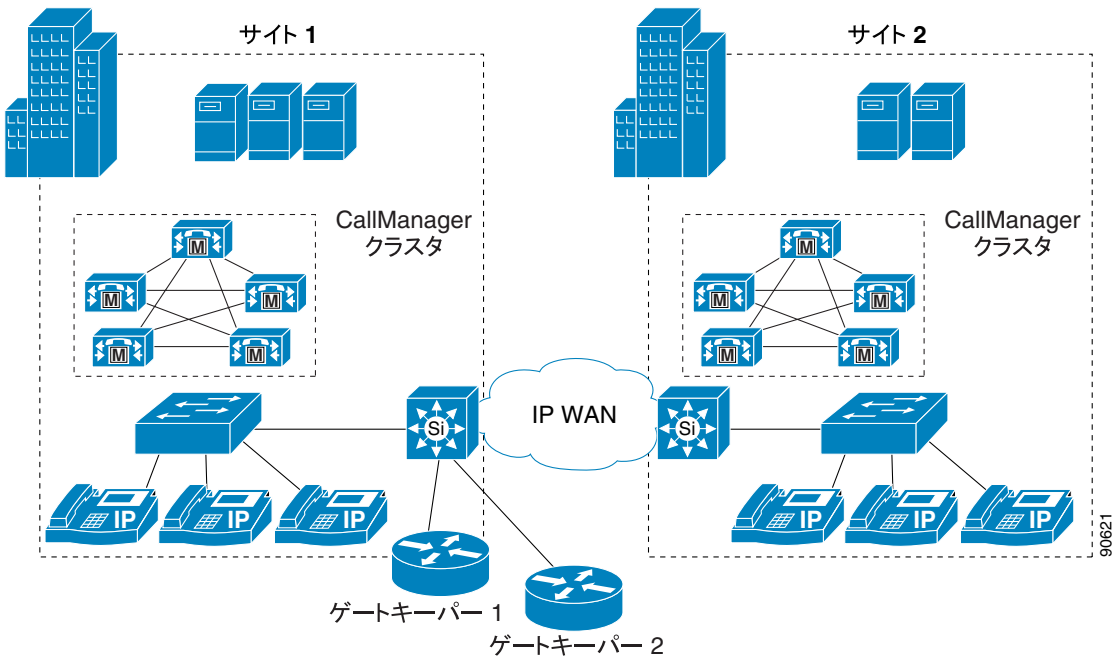
Release 3.3 より前の Cisco CallManager では、ゲートキーパーの冗長性には、ホットスタンバイ ルータ プロトコル（HSRP）しか選択できませんでした。HSRP は、冗長かつスケーラブルなゲートキーパー ネットワークの構築に必要な機能をサポートしないので、Release 3.3 より前の Cisco CallManager 環境でのみ使用してください。

HSRP には、次のガイドラインが適用されます。

- 一度に 1 つのゲートキーパーしかアクティブになりません。
  - スタンバイ ゲートキーパーは、プライマリに障害が発生した場合でなければ、コールを処理しません。
  - ロード バランシング機能は使用できません。
- すべてのゲートキーパーが同じサブネットまたはロケーションに存在しなければなりません。
- フェールオーバー後に以前の状態情報が使用できません。
- フェールオーバー後、スタンバイ ゲートキーパーは、すでにアクティブになっているコールを認識しないので、帯域幅のオーバーサブスクリプションが発生する可能性があります。
- コールの発信前に、HSRP スタンバイ ゲートキーパーにエンドポイントを再登録する必要があるので、フェールオーバーには相応の時間がかかることがあります。フェールオーバー時間は、登録タイマーの設定に依存します。

図 8-6 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 8-6　HSRP を使用するゲートキーパー冗長性



例 8-1 では、図 8-6 のゲートキーパー 1 の設定を示しています。例 8-2 では、ゲートキーパー 2 の設定を示しています。イーサネット インターフェイス上の HSRP 設定を除いて、両方の設定は同一です。

例 8-1　ゲートキーパー 1 の設定

```
interface Ethernet0/0
 ip address 10.1.10.2 255.255.255.0
  standby ip 10.1.10.1
  standby priority 110

gatekeeper
 zone local GK-Site1 customer.com 10.1.10.1
 zone local GK-Site2 customer.com
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth interzone default 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

例 8-2　ゲートキーパー 2 の設定

```
interface Ethernet0/0
 ip address 10.1.10.3 255.255.255.0
 standby ip 10.1.10.1

gatekeeper
 zone local GK-Site1 customer.com 10.1.10.1
 zone local GK-Site2 customer.com
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth interzone default 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 8-1 と例 8-2 について説明します。

- 各ルータには、それぞれが共有する仮想 IP アドレスを識別するために、HSRP 用に **standby** コマンドが設定されます。ゲートキーパー 1 は、コマンド **standby priority 110** を使用して、プライマリとして設定されています。
- Cisco CallManager トランク登録をサポートするために、各 Cisco CallManager クラスタには、各ルータ上でローカル ゾーンが設定されます。最初のゾーンに定義されている IP アドレスは、HSRP の使用する仮想 IP アドレスと一致する必要があることに注意してください。
- ゾーン間とクラスタ間のコール ルーティングを可能にするために、両方のルータでゾーンごとにゾーン プレフィックスが設定されます。
- 各ルータで、両方のサイトの帯域幅ステートメントが設定されます。シスコでは、**bandwidth interzone** コマンドを使用することをお勧めします。**bandwidth total** コマンドは、設定内容によっては機能しないことがあるためです。
- ローカルで解決されないすべてのコールを、ローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できるように、**gw-type-prefix 1# default-technology** コマンドが両方のルータで設定されます。この例では、すべての Cisco CallManager トランクは、1# プレフィックスに登録されるように設定されています。
- 冗長 Cisco CallManager トランク上にできるコール ルーティング ループを回避するために、**arq reject-unknown-prefix** コマンドが両方のルータで設定されます。

HSRP に関するこの他の高度な情報については、次の Web サイトにあるオンライン ドキュメントを参照してください。

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs009.htm
- http://www.cisco.com/warp/public/619/3.html
- http://www.cisco.com/warp/public/473/62.shtml

ゲートキーパー クラスタリング（代替ゲートキーパー）

ゲートキーパー クラスタリング（代替ゲートキーパー）により、「ローカル」ゲートキーパー クラスタの設定が可能になります。各ゲートキーパーは、一部の Cisco CallManager トランクのプライマリ、およびその他のトランクの代替として機能します。GUP（Gatekeeper Update Protocol）は、ローカル クラスタ内のゲートキーパー間で状態情報を交換するために使用されます。GUP は、クラスタ内のゲートキーパーごとに CPU 使用率、メモリ使用率、アクティブ コール数、および登録されたエンドポイント数をトラッキングし、報告します。GUP メッセージングで次のパラメータにしきい値を設定すると、ロード バランシングがサポートされます。

- CPU 使用率
- メモリ使用率
- アクティブ コール数
- 登録されたエンドポイント数

ゲートキーパー クラスタリング（代替ゲートキーパー）と Cisco CallManager Release 3.3 以降のサポートにより、ステートフル冗長性とロード バランシングが使用可能になります。ゲートキーパー クラスタリングは、次の機能を提供します。

- ローカルとリモートのクラスタ
- ローカル クラスタ内の最大 5 つのゲートキーパー
- ローカル クラスタ内のゲートキーパーを、別々のサブネットまたはロケーションに配置可能
- フェールオーバーの遅延なし（代替ゲートキーパーはすでにエンドポイントを認識しているので、完全な登録プロセスを実行する必要はありません）
- クラスタ内のゲートキーパーは、状態情報を渡し、ロード バランシングを行う

図 8-7 では、Cisco CallManager 分散型コール処理を行う 3 つのサイト、およびローカル クラスタで設定された 3 つの分散型ゲートキーパーを示しています。

図 8-7　ゲートキーパー クラスタリング

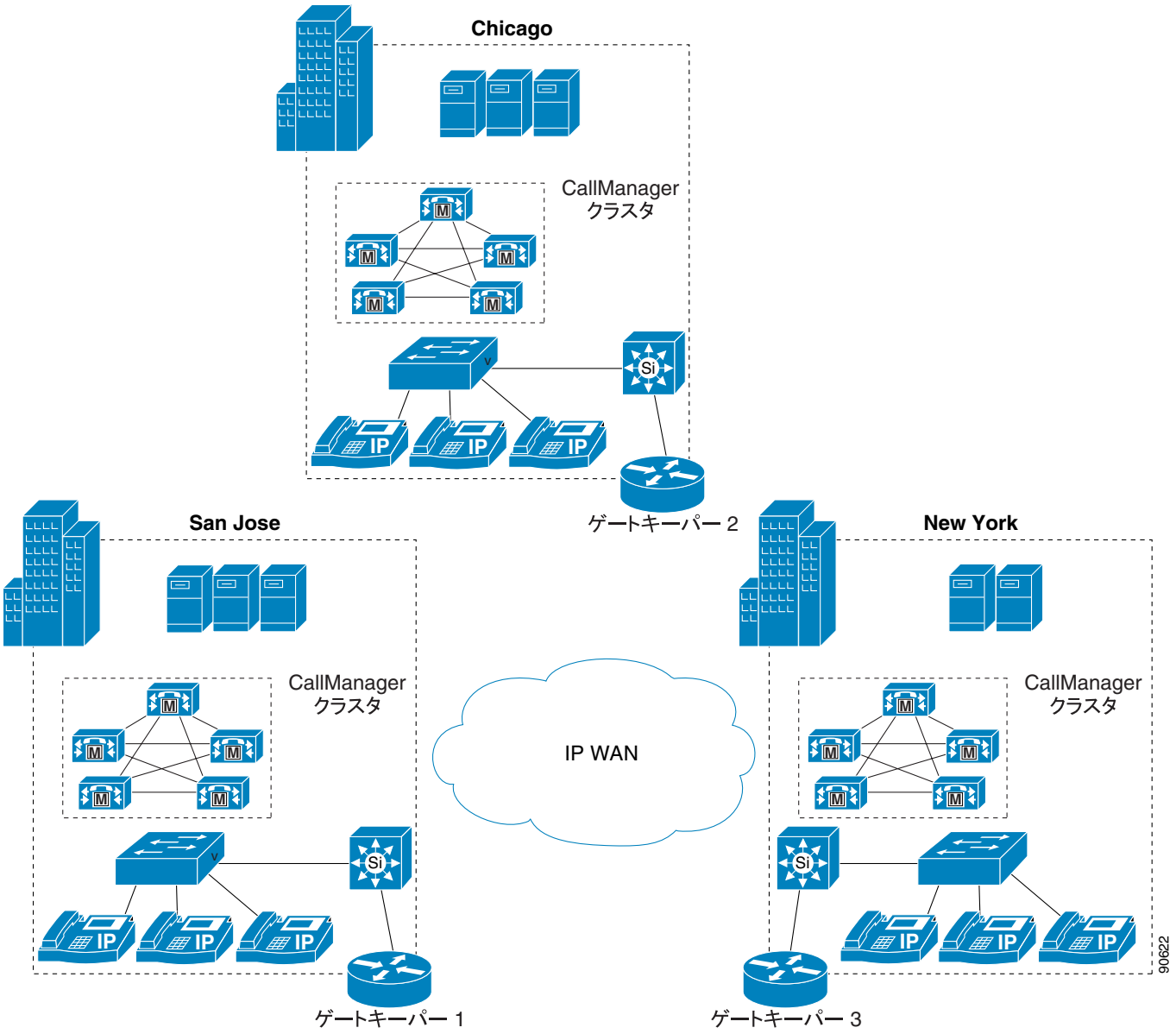


図 8-7 では、ゲートキーパー 2 はゲートキーパー 1 のバックアップ、ゲートキーパー 3 はゲートキーパー 2 のバックアップ、ゲートキーパー 1 はゲートキーパー 3 のバックアップです。

例 8-3 では、ゲートキーパー 1（SJC）の設定を示し、例 8-4 は、ゲートキーパー 2（CHC）の設定を示しています。ゲートキーパー 3（NYC）の設定は、他の 2 つの例を参照してください。

例 8-3　ゲートキーパー 1 のゲートキーパー クラスタリング設定

```
gatekeeper
 zone local SJC cisco.com 10.1.1.1
 zone local CHC_GK1 cisco.com
 zone local NYC_GK1 cisco.com
!
 zone cluster local SJC_Cluster SJC
  element SJC_GK2 10.1.2.1 1719
  element SJC_GK3 10.1.3.1 1719
 !
 zone cluster local CHC_Cluster CHC_GK1
  element CHC 10.1.2.1 1719
  element CHC_GK3 10.1.3.1 1719
 !
 zone cluster local NYC_Cluster NYC_GK1
  element NYC 10.1.3.1 1719
  element NYC_GK2 10.1.2.1 1719
 !
 zone prefix SJC 40852.....
 zone prefix NYC_GK1 21251.....
 zone prefix CHC_GK1 72067.....
 gw-type-prefix 1#* default-technology
 load-balance cpu 80 memory 80
 bandwidth interzone SJC 192
 bandwidth interzone NYC_GK1 160
 bandwidth interzone CHC_GK1 160
 arq reject-unknown-prefix
 no shutdown
```

例 8-4　ゲートキーパー 2 のゲートキーパー クラスタリング設定

```
gatekeeper
 zone local CHC cisco.com 10.1.2.1
 zone local SJC_GK2 cisco.com
 zone local NYC_GK2 cisco.com
!
 zone cluster local CHC_Cluster CHC
  element CHC_GK3 10.1.3.1 1719
  element CHC_GK1 10.1.1.1 1719
!
 zone cluster local SJC_Cluster SJC_GK2
  element SJC  10.1.1.1 1719
  element SJC_GK3 10.1.3.1 1719
 !
  zone cluster local NYC_Cluster NYC_GK2
  element NYC_GK1 10.1.1.1 1719
  element NYC 10.1.3.1 1719
 !
 zone prefix SJC_GK2 40852.....
 zone prefix NYC_GK2 21251.....
 zone prefix CHC 72067.....
 gw-type-prefix 1#* default-technology
 load-balance cpu 80 memory 80
 bandwidth interzone CHC_Voice 160
 bandwidth interzone SJC_Voice2 192
 bandwidth interzone NYC_Voice3 160
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 8-3 と例 8-4 について説明します。

- Cisco CallManager トランク登録をサポートするために、各 Cisco CallManager クラスタにはローカル ゾーンが設定されます。

- ローカル ゾーンごとにクラスタが定義され、他のゲートキーパー上のバックアップ ゾーンはエレメントとしてリストされます。エレメントは、バックアップが使用される順にリストされます。
- ゾーン間とクラスタ間のコール ルーティングを可能にするために、ゾーンごとにゾーン プレフィックスが設定されます。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Cisco CallManager トランクは、1# プレフィックスに登録されるように設定されています。
- **load-balance cpu 80 memory 80** コマンドは、CPU とメモリの使用率を制限します。ルータがどちらかの制限に達すると、新しい要求はすべて拒否され、使用率がしきい値以下に下がるまで、リスト内の最初のバックアップが使用されます。
- サイトごとに帯域幅ステートメントが設定されます。シスコでは、**bandwidth interzone** コマンドを使用することをお勧めします。**bandwidth total** コマンドは、設定内容によっては機能しないことがあるためです。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco CallManager トランク上にできるコール ルーティング ループを回避します。

クラスタ内のすべてのゲートキーパーは、すべての Cisco CallManager トランク登録を表示しています。ゲートキーパーをプライマリ リソースとして使用するトランクの場合、フラグ フィールドはブランクです。クラスタ内の別のゲートキーパーをプライマリ ゲートキーパーとして使用するトランクの場合、フラグ フィールドは A（代替）に設定されます。すべてのエンドポイントをプライマリまたは代替として登録すると、すべてのコールをローカル側で解決できるようになり、別のゲートキーパーにロケーション要求（LRQ）を送信する必要はありません。

例 8-5 では、ゲートキーパー 1（SJC）での **show gatekeeper endpoints** コマンドからの出力を示します。

例 8-5　ゲートキーパー エンドポイントの出力

```
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type        Flags
--------------- ----- --------------- ----- ---------         ----        -----
10.1.1.12       1307  10.1.1.12       1254  SJC               VOIP-GW
    H323-ID:SJC-to-GK-trunk_1
10.1.1.12       4422  10.1.1.12       4330  SJC               VOIP-GW
    H323-ID:SJC-to-GK-trunk_2
10.1.2.12       4587  10.1.2.12       4330  CHC_GK1           VOIP-GW     A
    H323-ID:CHC-to-GK-trunk_1
10.1.3.21       2249  10.1.3.21       1245  NYC_GK1           VOIP-GW     A
    H323-ID:NYC-to-GK-trunk_1
Total number of active registrations = 4
```

ディレクトリ ゲートキーパーの冗長性

HSRP を使用するか、複数の同じディレクトリ ゲートキーパーを設定すると、ディレクトリ ゲートキーパーの冗長性を実装できます。同じゾーン プレフィックスを使用して、複数のリモート ゾーンをもつゲートキーパーを設定するとき、このゲートキーパーには、次のいずれかの方法が使用できます。

- 順次 LRQ（デフォルト）

  冗長リモート ゾーン（ゾーン プレフィックスが一致）にコストが割り当てられ、LRQ は、コスト値に基づいた順序で、一致するゾーンに送信されます。順次 LRQ を使用すると、一致するすべてのゲートキーパーに LRQ を送信しないので、WAN 帯域幅の節約になります。

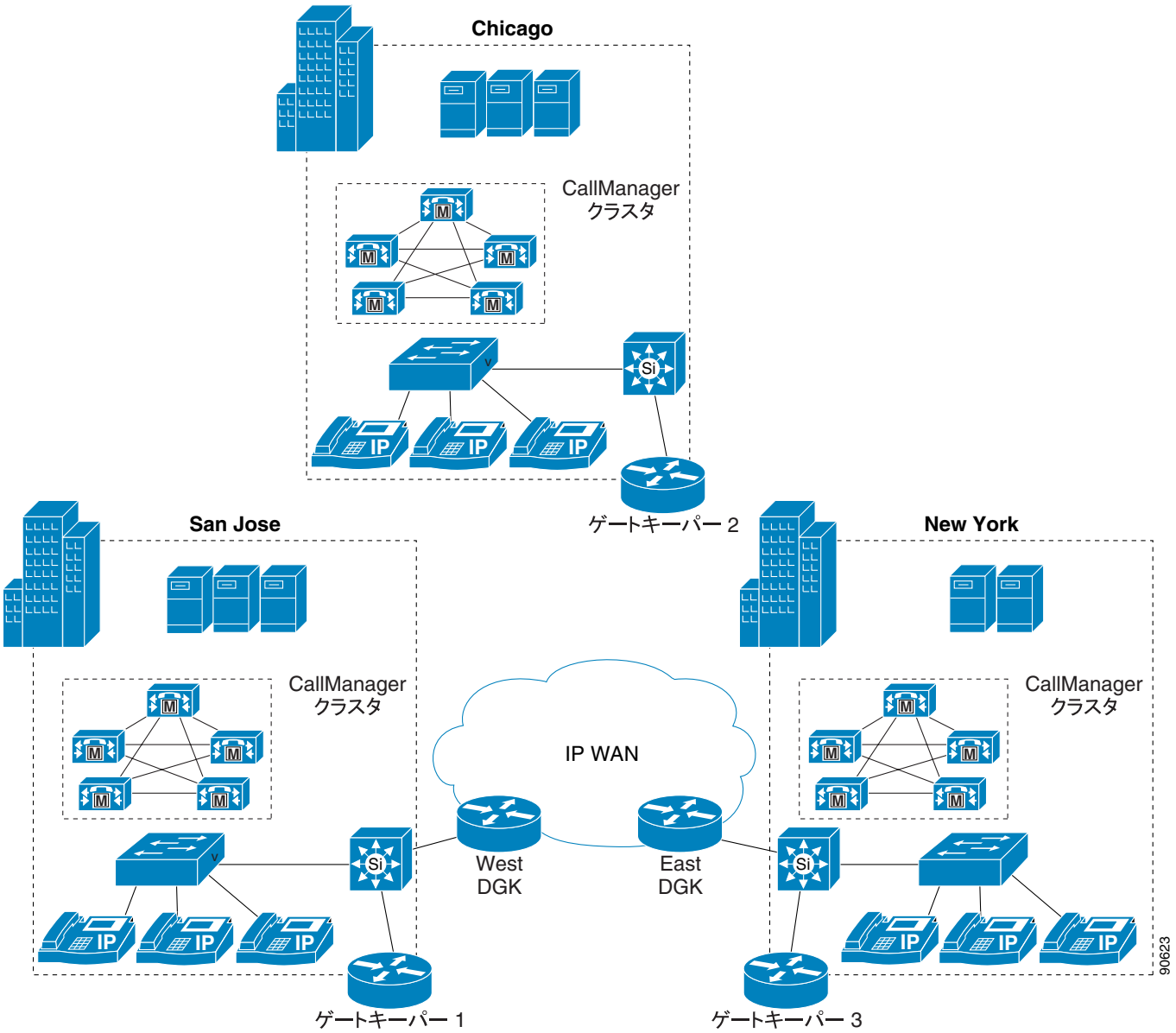
- LRQ ブラスト

  LRQ は、冗長ゾーン（ゾーン プレフィックスが一致）に同時に送信されます。ロケーション確認（LCF）で応答する最初のゲートキーパーが、使用されます。

順次 LRQ を使用して複数のアクティブ ディレクトリ ゲートキーパーを使用することをお勧めします。これによって、ディレクトリ ゲートキーパーを別々のロケーションに配置することができます。HSRP を使用するには、両方のディレクトリ ゲートキーパーを同じサブネットに置く必要があります。この場合常に 1 つのゲートキーパーしかアクティブにすることができません。

図 8-8 では、2 つのアクティブ ディレクトリ ゲートキーパーを備えた Cisco CallManager 分散型コール処理環境を示しています。

図 8-8　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 8-8 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 8-8 のゲートキーパー 1 ～ 3 の設定を示しています。

例 8-8　ゲートキーパー 1（SJC）の設定

```
zone local SJC customer.com 10.1.1.1
 zone remote DGKW customer.com 10.1.10.1
 zone remote DGKE customer.com 10.1.12.1
 zone prefix SJC 408.......
 zone prefix DGKW ..........
 zone prefix DGKE ..........
 bandwidth remote 192
 gw-type-prefix 1# default-technology
 arq reject-unknown-prefix
 no shutdown
```

例 8-9　ゲートキーパー 2（CHC）の設定

```
gatekeeper
 zone local GK-CHC customer.com 10.1.2.1
 zone remote DGKE customer.com 10.1.12.1
 zone remote DGKW customer.com 10.1.10.1
 zone prefix CHC 720.......
 zone prefix DGKE ..........
 zone prefix DGKW ..........
 bandwidth remote 160
 gw-type-prefix 1# default-technology
 arq reject-unknown-prefix
 no shutdown
```

例 8-10　ゲートキーパー 3（NYC）の設定

```
gatekeeper
 zone local NYC customer.com 10.1.3.1
 zone remote DGKE customer.com 10.1.12.1
 zone remote DGKW customer.com 10.1.10.1
 zone prefix NYC 212.......
 zone prefix DGKE ..........
 zone prefix DGKW ..........
 bandwidth remote 160
 gw-type-prefix 1# default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 8-8、例 8-9、および例 8-10 について説明します。

- Cisco CallManager トランク登録をサポートするために、各 Cisco CallManager クラスタにはローカル ゾーンが設定されます。
- ディレクトリ ゲートキーパーごとに、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、ローカル ゾーンと両方のリモート ゾーンにゾーン プレフィックスが設定されます。両方のディレクトリ ゲートキーパー プレフィックスは、10 個のドットです。一致するゾーン プレフィックスが設定されるとき、デフォルトで順次 LRQ が使用されます。ゲートキーパーは、コストが最低のディレクトリ ゲートキーパーに LRQ を送信します。応答がない場合、ゲートキーパーは、2 番目のディレクトリ ゲートキーパーに LRQ の送信を試みます。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Cisco CallManager トランクは、1# プレフィックスに登録されるように設定されています。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco CallManager トランク上にできるコール ルーティング ループを回避します。

Cisco CallManager と CallManager Express の相互運用性

この項では、H.323 プロトコルを使用している Cisco CallManager と Cisco CallManager Express（CME。以前に Cisco IOS Telephony Services（ITS）と呼ばれていた製品）に関して、マルチサイト IP テレフォニー配置における相互運用性、およびインターネットワーキングの要件について説明します。ここでは、Cisco CallManager の制御する電話と CME の制御する電話間でのコール転送や自動転送など、補足サービスを中心に説明します。

Cisco CallManager と CME を相互運用するには、少なくとも次のソフトウェア リリースが必要です。

- Cisco CallManager Express Release 3.1 以降、Cisco IOS Release 12.3(7)T 以降、および IP VOICE 機能セット
- Cisco CallManager Release 3.3(3) 以降

Cisco CME 3.1 には、次の 2 つの機能が追加されています。

- Cisco CallManager 自動検出

  この機能は、リモートの Cisco CallManager エンドポイントを自動的に検出し、Cisco CallManager エンドポイントが宛先または発信元となって転送または自動転送されるコールに対して、H.323-to-H.323 ヘアピンを確立します。また、この自動検出機能は、Cisco CallManager および CME の制御する IP Phone 間でのリングバックの生成など、シグナリングの決定を処理します。
- H.323-to-H.323 コール ヘアピンのサポート

  Cisco CallManager は H.450 仕様をサポートしていないため、H.323-to-H.323 ヘアピンが必要になります。

(注) Cisco CME 3.0、および ITS の以前のバージョンは、H.323 コール ヘアピンを使用する Cisco CallManager との相互運用をサポートしていません。これらの旧バージョンでは、ループバック DN ポートを使用して Cisco CallManager との相互運用を実現していました。

次の各項では、Cisco CallManager と CME の相互運用を実現するためのガイドラインを示します。

- Cisco CallManager および CME を使用したマルチサイト IP テレフォニー配置（P.8-30）
- Cisco CallManager、CME、および H.450 タンデム ゲートウェイを使用したマルチサイト IP テレフォニー配置（P.8-31）

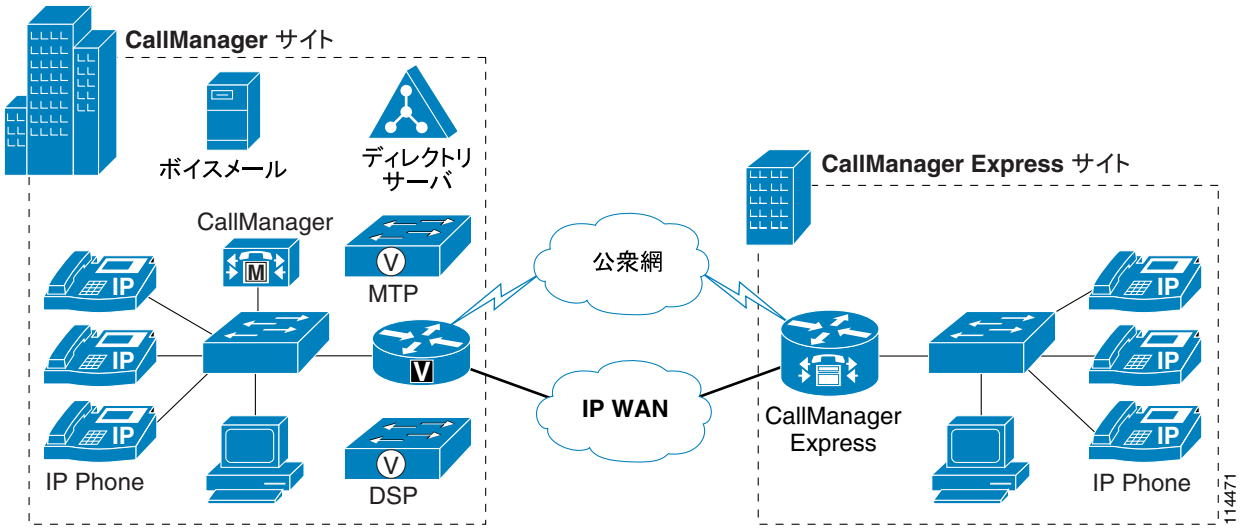
CME の詳細については、次の Web サイトで入手可能な Cisco CallManager Express 製品マニュアルを参照してください。

http://www.cisco.com

Cisco CallManager および CME を使用したマルチサイト IP テレフォニー配置

Cisco CallManager は、H.323 インターフェイスを使用する CME と直接通信することができます。図 8-9 では、Cisco CME と直接にネットワーク接続された Cisco CallManager を使用する IP テレフォニー配置を示しています。

図 8-9　Cisco CallManager および CME を使用したマルチサイト IP テレフォニー配置



ベスト プラクティス

図 8-9 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。

- Cisco CallManager 上に、ゲートキーパー制御のクラスタ間トランク（ICT）を設定する。Cisco CallManager は、ICT を通じてゲートキーパーに登録し、CME は H.323 ゲートウェイとしてゲートキーパーに登録します。
- クラスタ間トランクを使用する場合は、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。Cisco CME が、端末機能セット（TCS）シグナリングを開始することはありません。また、MTP を使用すると、Cisco CallManager と CME の間で TCS 交換ができなくなります。
- Cisco CallManager で、サービス パラメータ **Send H225 user info message** を **H225 info for Ringback** に設定する。
- Cisco CallManager ダイヤル プランの設定（ルート パターン、ルート リスト、およびルート グループ）を使用して、CME に接続しているクラスタ間トランクにコールを送信する。
- Cisco CallManager のデバイス プールとリージョンを使用して、サイト内では G.711 コーデックを設定し、リモートの CME サイトに対しては G.729 コーデックを設定する。
- CME 上で **allow-connection h323 to h323** コマンドを設定して、H.323-to-H.323 コール ヘアピン接続を許可する。CME 3.1 の Cisco CallManager 自動検出機能を使用すると、Cisco CallManager に接続されているインターフェイス上での H.450 ベースの通信が、すべて無効になります。Cisco CallManager　電話と　CME　電話間でコール転送または自動転送を確立するには、H.323-to-H.323 接続が必要です。
- VoIP ダイヤル ピアを定義して、Cisco CallManager エンドポイントを宛先とするコールをゲートキーパーに転送する。
- コールをリモート サイトにルーティングする VoIP ダイヤル ピアに対しては、G.729 コーデックを設定する。

例 8-11 に、この配置モデルでの CME の設定例を示します。

例 8-11　Cisco CME 3.1 の設定

```
voice service voip
    allow-connections h323 to h323
    h323
dial-peer voice 1 voip       /* To Cisco CallManager endpoints */
    destination-pattern xxxx
    session target ras       /* "ras" if gatekeeper is used, otherwise "ipv4:y.y.y.y"
*/
    dtmf-relay h245-alphanumeric
    codec g729r8             /* Voice class can also be used */
    no vad
```

ここで示したガイドラインに従うと、Cisco CallManager 電話および CME 電話間で基本的なコールを使用できるようになります。ただし、この配置モデルでは、Cisco CallManager 電話が宛先または発信元となって転送または自動転送されるすべてのコールが、ヘアピンされます。ヘアピンでは、コール フローに関係するすべてのデバイス間で、エンドツーエンドのシグナリングが必要です。したがって、コールがジッタ、遅延、ネットワーク障害の影響を受けやすくなります。また、コールが WAN を経由する場合には、不要な帯域幅を消費します。これらの問題が発生することを避けるために、次の項の説明に従って、Cisco CallManager クラスタのフロントエンドに H.450 タンデム ゲートウェイを配置することをお勧めします。

Cisco CallManager、CME、および H.450 タンデム ゲートウェイを使用したマルチサイト IP テレフォニー配置

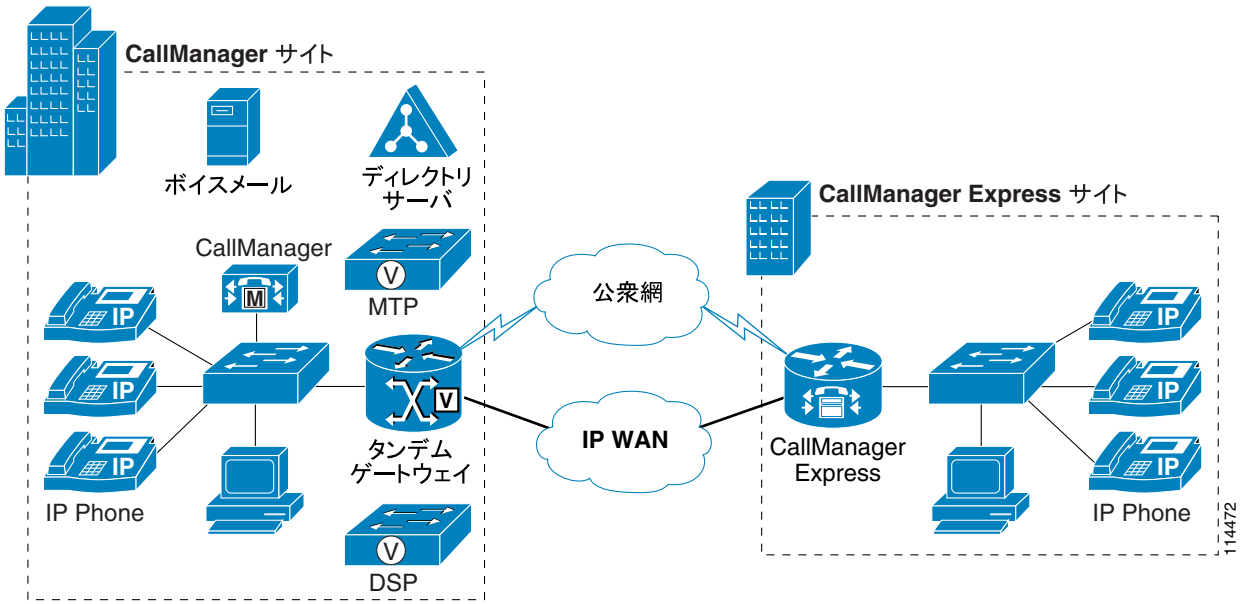
タンデム ゲートウェイは、Cisco CallManager など、H.450 をサポートしないシステムのためにプロキシ（フロントエンド）を提供する独立ルータです。タンデム ゲートウェイは、Cisco CallManager と CME ルータの中間に配置できます。H.450 をサポートしないエンドポイントに転送または自動転送するコールを終端し、再発信するための H.323-to-H.323 コール接続を提供します。

また、H.450 タンデム ゲートウェイは、Cisco CallManager やリモート Cisco CME システム用の公衆網ゲートウェイとしても動作できます。この場合は、公衆網ゲートウェイを別に用意する必要がありません。

H.450 タンデム ゲートウェイは、Cisco CME 3.1 と互換性があり、かつ H.450 をサポートしている Cisco IOS リリースを実行している必要があります。たとえば、IP VOICE 機能セットを備えた Cisco IOS Release 12.3(7)T 以降などです。

図 8-10 では、H.450 タンデム ゲートウェイを通じて Cisco CME に接続されている Cisco CallManager を使用した、IP テレフォニー配置を示しています。

図 8-10　Cisco CallManager、CME、および H.450 タンデム ゲートウェイを使用したマルチサイト IP テレフォニー配置



ベスト プラクティス

図 8-10 に示した配置モデルを使用する場合は、次のガイドラインに従い、ベスト プラクティスを参考にしてください。

- Cisco CallManager と H.450 タンデム ゲートウェイの間に、ゲートキーパーの制御しないクラスタ間トランク（ICT）を設定する。
- クラスタ間トランクを使用する場合は、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。Cisco CME が、端末機能セット（TCS）シグナリングを開始することはありません。また、MTP を使用すると、Cisco CallManager と CME の間で TCS 交換ができなくなります。
- Cisco CallManager で、サービス パラメータ **Send H225 user info message** を **H225 info for Ringback** に設定する。
- Cisco CallManager ダイヤル プランの設定（ルート パターン、ルート リスト、およびルート グループ）を使用して、H.450 タンデム ゲートウェイに接続しているクラスタ間トランクにコールを送信する。
- ゲートキーパー上に、Cisco CME と H.450 タンデム ゲートウェイを H.323 ゲートウェイとして登録する。
- H.450 タンデム ゲートウェイ上で **allow-connection h323 to h323** コマンドを設定して、H.323-to-H.323 コール ヘアピン接続を許可する。リモート CME ルータについては、このコマンドを有効にする必要はありません。
- H.450 タンデム ゲートウェイ上で VoIP ダイヤル ピアを定義して、コールを Cisco CallManager および CME のエンドポイントにルーティングする。
- CME 上で VoIP ダイヤル ピアを定義して、Cisco CallManager エンドポイントを宛先とするコールを H.450 タンデム ゲートウェイに転送する。
- コールを Cisco CallManager および CME との間でルーティングする H.450 タンデム ゲートウェイ上で、すべてのダイヤル ピアに同じ音声コーデックを使用する。コーデックの再ネゴシエーションはサポートされません。このため、WAN 経由で G.729 を使用する場合は、コールをリモート サイトにルーティングするすべての VoIP ダイヤル ピアで、G.729 コーデックを設定します。また、Cisco CallManager のデバイス プールとリージョンを使用して、Cisco CallManager IP Phone と H.450 タンデム ゲートウェイ間に G.729 コーデックを設定します。

- H.450 タンデム ゲートウェイを公衆網接続用の MGCP ゲートウェイとして使用できる。公衆網接続で H.323 ゲートウェイが必要な場合は、別個のゲートウェイを使用する必要があります。

例 8-12 に、H.450 タンデム ゲートウェイの設定例を示します。

例 8-12　H.450 タンデム ゲートウェイの設定

```
voice service voip
    allow-connections h323 to h323
    supplementary-service h450.12
    h323
dial-peer voice 1 voip        /* To Cisco CallManager endpoints */
    destination-pattern xxxx
    session target ipv4:y.y.y.y
    dtmf-relay h245-alphanumeric
    codec g729r8
    no vad
dial-peer voice 1 voip        /* To Cisco CallManager endpoints */
    destination-pattern zzzz
    session target ras        /* "ras" if gatekeeper is used, otherwise "ipv4:a.b.c.d"
*/
    dtmf-relay h245-alphanumeric
    codec g729r8
    no vad
```

コール アドミッション制御

コール アドミッション制御機能は、IP WAN 経由で接続された複数のサイトで構成されるすべての Cisco IP Communications 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

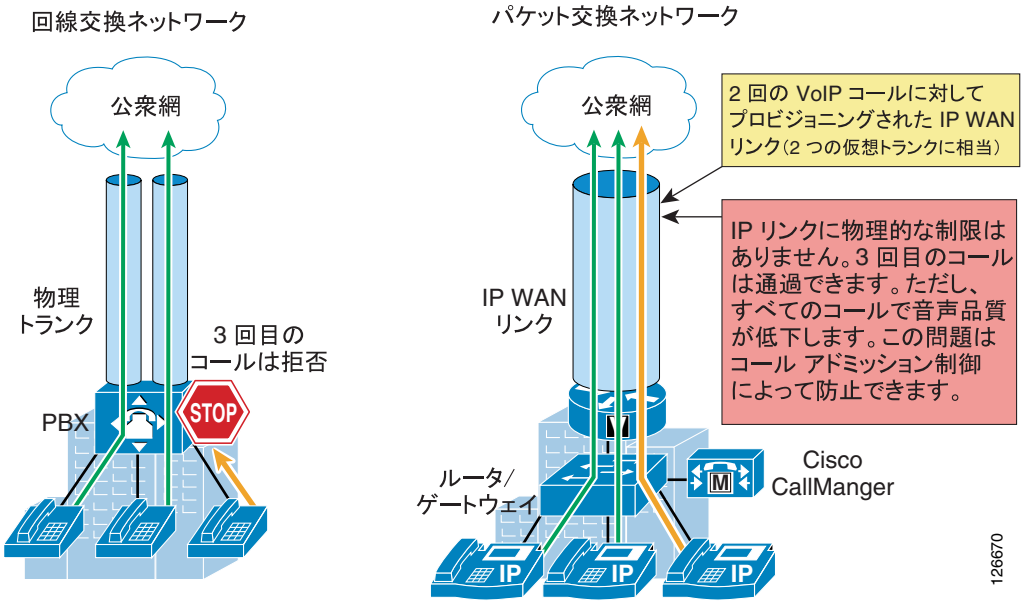


図 9-1 の左側で示すように、従来の TDM ベースの PBX は、回線交換ネットワークの一部として動作します。このネットワークでは、回線はコールがセットアップされるたびに確立されます。このため、レガシー PBX が公衆網または他の PBX に接続されている場合は、一定数の物理トランクを設定する必要があります。公衆網または他の PBX 宛てのコールをセットアップする必要があるとき、PBX は、使用可能なトランクの中からトランクを選択します。使用可能なトランクがない場合、コールは PBX によって拒否され、発信者にはネットワーク ビジー信号が聞こえます。

次に、図 9-1 の右側に示している Cisco IP Communications 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 Communications 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、Cisco IP Communications 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、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。

この章では、コール アドミッション制御の主な側面について、次の項目を説明します。

- コール アドミッション制御の要素（P.9-3）

  ここでは、Cisco IP Communications システムのさまざまなコンポーネント、たとえば Cisco CallManager ロケーション、Cisco IOS ゲートキーパー、RSVP、IP-to-IP ゲートウェイなどで使用できる、各種のコール 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.9-22）

  ここでは、上の項で説明したメカニズムを適用し、組み合せる方法について、IP WAN のトポロジ（単純なハブアンドスポーク、2 層ハブアンドスポーク、MPLS、複合トポロジ）に基づいて、および採用する Cisco CallManager 配置モデル（集中型、分散型、集中型および分散型複合）に基づいて示します。

コール アドミッション制御の要素

この項では、Cisco IP Communications システムに含まれている次のコール アドミッション制御要素について、設計と設定のガイドラインを示します。

Cisco CallManager ロケーション

Cisco CallManager では、集中型コール処理配置において、コール アドミッション制御を実装するために、「ロケーション（location）」と呼ばれている単純なメカニズムを取り入れています。Cisco CallManager でデバイスを設定するときは、デバイスをロケーションに割り当てて、各ロケーションが宛先または発信元となるコールに一定量の帯域幅を割り当てます（図 9-2 を参照）。Cisco CallManager で設定するロケーションは、仮想ロケーションであり、実際の物理ロケーションではありません。Cisco CallManager は、デバイスの物理的なロケーションを認識しません。このため、デバイスをある物理ロケーションから別のロケーションに移動する場合は、システム管理者がロケーション情報を手動でアップデートして、Cisco CallManager がそのデバイスの帯域幅割り当てを正しく計算できるようにする必要があります。各デバイスは、デフォルトでは <None> ロケーションに配置されます。ロケーション <None> は、無限の音声帯域幅とビデオ帯域幅を持った、特殊な名称未設定ロケーションです。支店サイトにあるデバイスが <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メカニズムによって受け付けられます。

Cisco CallManager は、ロケーションで使用可能になっている音声帯域幅とビデオ帯域幅を使用して、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 コールの数を制御します。ロケーションの音声帯域幅とビデオ帯域幅が **Unlimited** に設定されている場合、そのロケーションでは帯域幅を無限に使用できるため、そのロケーションが宛先または発信元となる音声コールとビデオ コールは、Cisco CallManager ではすべて許可されます。帯域幅の値が特定のキロビット / 秒（Kbps）に設定されている場合は、アクティブになっているすべてのコールで使用されている合計帯域幅が、その設定値以下になっている場合に限り、Cisco CallManager は、そのロケーションで入出力されるコールを許可します。ロケーションのビデオ帯域幅を **None** に設定して、このロケーションが宛先または発信元となるビデオ コールをすべて拒否することもできます。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。つまり、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 ベースのコール アドミッション制御メカニズムでは、通話中のコール タイプ変更も考慮に入れる必要があります。たとえば、サイト間でビデオ コールを確立する場合、Cisco CallManager は、それぞれのロケーションから適切な量の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コールに変更された場合、Cisco CallManager は割り当てた帯域幅をビデオ プールに戻し、適切な量の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。

(注) Cisco CallManager Release 3.1 より前は、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する場合、クラスタ内には 1 つのプライマリ（アクティブ）CiscoCallManager サーバしかありませんでした。Cisco CallManager Release 3.1 以降では、ロケーションの帯域幅は、クラスタ内のすべての Cisco CallManager サブスクライバ間で共有されるので、任意のサイズのクラスタでロケーション メカニズムを使用できるようになりました。

図 9-2　Cisco CallManager におけるロケーションの定義

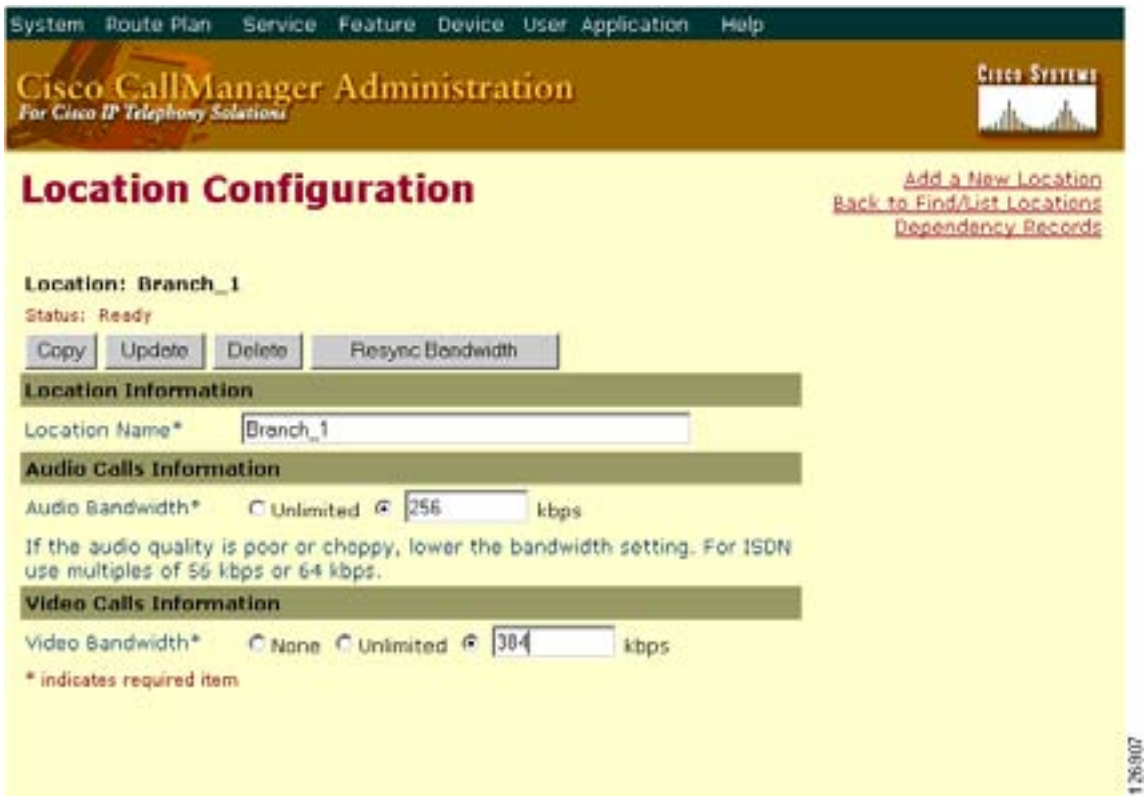


図 9-2 では、使用可能な音声帯域幅 256 Kbps およびビデオ帯域幅 384 Kbps を指定した、ロケーション Branch_1 の設定を示しています。このロケーションは、最高 3 つの G.711 音声コール（コールごとに 80 Kbps）、または 10 個の G.729 音声コール（コールごとに 24 Kbps）、または両方のコールの組み合せ（256 Kbps を超えないこと）をサポートできます。このロケーションでは、使用されているビデオ コーデックおよび音声コーデックに応じて、さまざまな数のビデオ コールをサポートすることもきます。たとえば、G.711 音声コーデックと H.261 または H.263 ビデオ コーデックを使用する 1 つのビデオ コールで 320 Kbps のレートが必要な場合は、帯域幅を 384 Kbps 消費します。G.729 音声コーデックと H.261 または H.263 ビデオ コーデックを使用する 3 つのコールで 120 Kbps のレートが必要な場合も、同じ帯域幅を消費します。

(注) Cisco CallManager Release 4.0 以降では、Cisco IP Phone で暗号化電話コールを発信できます。暗号化コールのペイロードは、暗号化されていないコールのペイロードよりもわずかに大きくなります。このため、ネットワーク経由での暗号化コールの送信を計画している場合は、この追加の帯域幅に対応するように IP WAN ルータの帯域幅設定を調整する必要があります。IP WAN ルータのキューを設定するときに考慮するその他の要素は、レイヤ 2 ヘッダーによって発生するオーバーヘッドです。暗号化コールの帯域幅の計算、およびさまざまなレイヤ 2 テクノロジーの詳細については、P.3-25 の「帯域幅のプロビジョニング」を参照してください。

ロケーションに配置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（メディアを終端する場合）
- コンファレンス ブリッジ
- Music On Hold（MOH）サーバ
- ゲートウェイ
- トランク

CTI ルート ポイントに対して設定されているロケーションが Cisco CallManager で考慮されるのは、そのルート ポイントにメディアを処理するアプリケーションが登録されている場合のみです。CTI ルート ポイントがコールのルーティングにのみ使用されていて、メディアの終端とならない場合、設定されているロケーションは、Cisco CallManager では無視されます。

（注） トランスコーダと MTP は、ロケーションに割り当てることはできません。したがって、これらは通常は中央サイトに配置します。ただし、Cisco CallManager Release 3.2(3)、3.3(3)、4.0(1) 以降では、G.711 専用デバイスとともに配置される場合に限り、トランスコーダをリモート サイトに配置することもできます。基本的には、Cisco CallManager はトランスコーダに関係するコールは常に G.729 コールであると見なし、24 Kbps の帯域幅を関連ロケーションから差し引きます。

コール アドミッション制御は、同じロケーション内にあるデバイス間でのコールには適用されません。Cisco CallManager は、これらのデバイスが同一 LAN 上にあり、使用可能な帯域幅が無限にあると見なすためです。

あるロケーションから別のロケーションにコールが発信されると、Cisco CallManager は、両方のロケーションで適切な量の帯域幅を差し引きます。たとえば、Branch_1 内のデバイスが、Branch_2 内のデバイスに G.711 コールを発信する場合、Cisco CallManager は、両方のロケーションの使用可能な帯域幅から 80 Kbps を差し引きます。コールが完了すると、Cisco CallManager は、帯域幅を差し引かれたロケーションに帯域幅を戻します。Branch_1 ロケーションまたは Branch_2 ロケーションのいずれかで十分な帯域幅がない場合、コールは Cisco CallManager によって拒否され、発信者にはネットワーク ビジー トーンが聞こえます。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。

Cisco CallManager Release 3.3 以降では、発信者または着信側のどちらかで帯域幅が不足しているためにクラスタ内コールが拒否された場合、Cisco CallManager は Automated Alternate Routing（AAR）機能を使用して、コールを公衆網を通じて自動的に宛先に再ルーティングできます。Cisco CallManager は、着信番号および着信側の外線電話番号マスクを使用して、完全な E.164 宛先番号を取得します。発信者の回線に設定されている AAR グループによって、E.164 番号の前に付けられるアクセス コードが決定し、発信デバイスの AAR コーリング サーチ スペースによって、ローカル出口公衆網ゲートウェイを選択する方法が決定します。

（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のみです。IP WAN が使用不可の場合や、接続に関するその他の問題によって着信側デバイスが Cisco CallManager に登録されない状態になった場合には、AAR は呼び出されません。このような場合、コールは着信側デバイスの Call Forward Busy フィールドで指定されている宛先に転送されます。AAR の詳細については、P.2-1 の「IP テレフォニー配置モデル」および P.10-20 の「Automated Alternate Routing」を参照してください。

Cisco CallManager クラスタ内で、あるロケーションが宛先または発信元となって外部コールが発生すると、Cisco CallManager はロケーション ベースのコール アドミッション制御計算も実行します。コールをサポートするための帯域幅が十分にある場合、Cisco CallManager はコールを許可して、ロケーションにある適切な量の帯域幅を割り当てます。ロケーションに十分な帯域幅がない場合、コールは Cisco CallManager によって拒否されます。

図 9-3 では、ロケーション Branch_1 に割り当てられた IP Phone の設定を示しています。Cisco CallManager は、コールをサポートする十分な帯域幅が Branch_1 にある場合、この IP Phone に出入りする各コールを受け入れます。IP Phone が発信コールを実行したときに Branch_1 に十分な帯域幅がない場合、Cisco CallManager は、AAR を通じてコールを再ルーティングし、Branch_1 の公衆網ゲートウェイに発信します。

図 9-3　ロケーションへのデバイスの割り当て

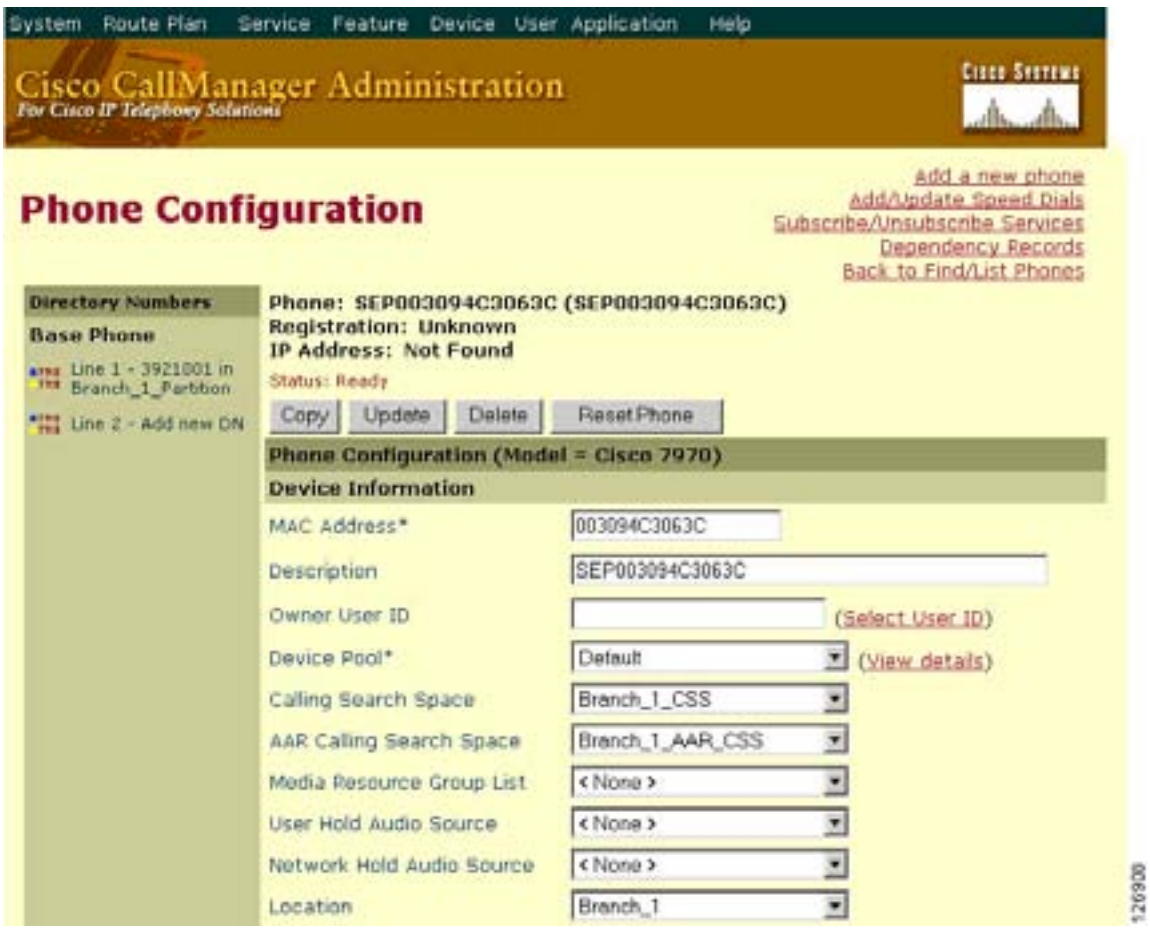


表 9-1 に、さまざまなコール速度において Cisco CallManager ロケーション アルゴリズムが要求する帯域幅の量を示します。

表 9-1　ロケーション アルゴリズムが要求する帯域幅の量

コールの速度	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

ゲートキーパー

Cisco IOS ゲートキーパーは、Cisco CallManager、Cisco CallManager Express、レガシー PBX に接続されている H.323 ゲートウェイなどのデバイス間で、コール ルーティングとコール アドミッション制御を提供できます。H.323 Registration Admission Status（RAS）プロトコルを使用してこれらのデバイスと通信し、コールをネットワークにルーティングします。

ゲートキーパーのコール アドミッション制御は、ポリシーベースの方式であり、使用可能なリソースの静的設定を必要とします。ゲートキーパーは、ネットワーク トポロジを認識しないので、単純なハブアンドスポーク トポロジに制限されます。複数のゲートキーパーを配置している場合は、2 層ハブアンドスポーク トポロジをサポートできることもあります。トポロジの詳細な例については、P.9-22 の「コール アドミッション制御の設計」の項を参照してください。

Cisco 2600、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、「コール処理」の章の「ゲートキーパー」の項を参照してください。コール ルーティングに関する考慮事項については、P.10-33 の「ゲートキーパーを使用する Cisco IOS でのコール ルーティング」を参照してください。

Cisco IOS ゲートキーパーのコール アドミッション制御機能について理解するには、ゲートキーパーの「ゾーン」の概念を再確認すると役立ちます。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。
- **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。

たとえば、ネットワーク上に、DS-3 WAN リンクを通じて本社に接続されている 2 つの Cisco CallManager クラスタがあるとします。また、リンクごとに 20 の G.711 音声コールと 5 つの 384 Kbps ビデオ コールを許可し、どのビデオ コールの帯域幅も 384 Kbps に制限するとします。この場合は、**bandwidth interzone** コマンドを使用して、各ゾーンの帯域幅を 20 の G.711 コールと 5 つの 384 Kbps ビデオ コールの合計値に制限し、**bandwidth session** コマンドを使用して、各コールの最大帯域幅を 384 Kbps に制限します。次に例を示します。

```
gatekeeper
 zone local ccm-1 customer.com 10.10.10.10
 zone local ccm-2
 bandwidth interzone ccm-1 6400
 bandwidth session ccm-1 768
 bandwidth interzone ccm-2 6400
 bandwidth session ccm-2 768
```

ゲートキーパーの使用する帯域幅の値は、レイヤ 2、IP、および RTP のオーバーヘッドを除いた、コールのビットレートの倍です。たとえば、64 Kbps を使用する G.711 音声コールは、ゲートキーパーでは 128 Kbps と認識され、384 Kbps のビデオ コールは 768 Kbps と認識されます。表 9-2 に、一般に利用されているいくつかのコール速度において、ゲートキーパーが使用する帯域幅の値を示します。

表 9-2　さまざまなコール速度におけるゲートキーパーの帯域幅設定

コールの速度	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

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、アプリケーションがネットワーク帯域幅を動的に予約することを可能にします。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、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。

Cisco IOS ルータのほとんどは RSVP をサポートしており、P.9-15 の「IP-to-IP ゲートウェイ」の項で説明する Cisco マルチサービス IP-to-IP ゲートウェイ機能を使用すると、Cisco IP Communications ネットワークに RSVP を導入することができます。

RSVP のプロトコルについて詳細に説明することは、このマニュアルの対象範囲外です。詳細については、インターネット技術特別調査委員会（IETF）が発行する関連 Request For Comments（RFC）ドキュメントを参照してください。このドキュメントは、次の Web サイトにあります。

http://www.ietf.org

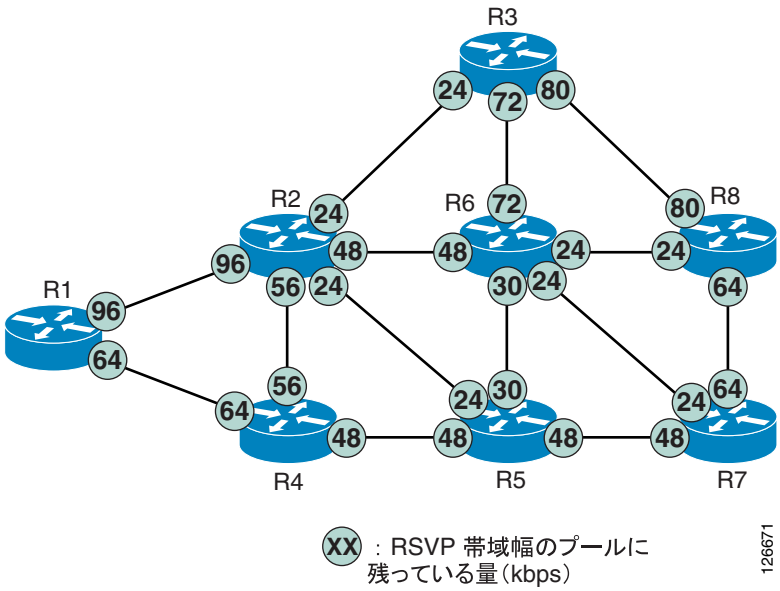
ここでは、RSVP の全般的な動作原理、Cisco IOS におけるさまざまな RSVP 運用モデル、企業ネットワークにおいて音声とビデオのアプリケーションに RSVP を使用する場合の設計上のベスト プラクティスを中心に説明します。

RSVP の原理

RSVP がネットワークでコール アドミッション制御と帯域幅予約を実行する方法について、基本的な原理を理解するために、図 9-4 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。

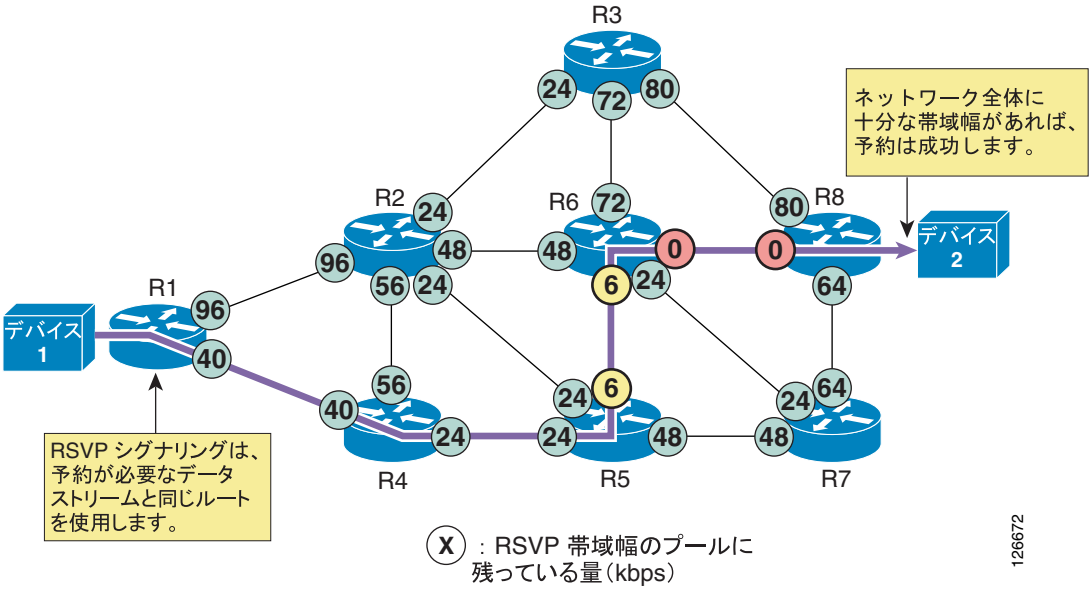
図 9-4 に示すネットワークの各ルータ インターフェイスで、RSVP が有効になっているとします。円で囲まれた数値は、各インターフェイス上に残っている使用可能な RSVP 帯域幅の量を表しています。

図 9-4　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量の帯域幅を予約するとします。このシナリオを図 9-5 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 9-5　予約が成功する RSVP シグナリング

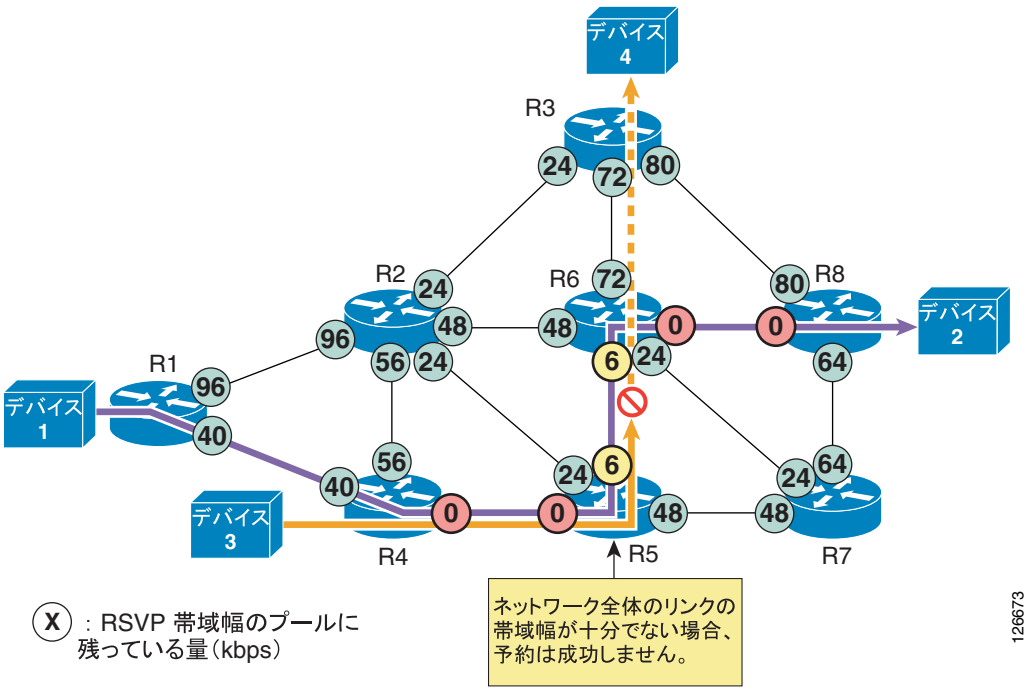


ここでは、図 9-5 について説明します。

- RSVP は、自身ではルーティングを実行しません。代わりに、下層で機能しているルーティング プロトコルを使用して、予約要求の宛先を決定します。トポロジの変更に対応するためにルーティングのパスが変化すると、RSVP は、自身の予約を予約が存在する新しいパスに合せて調整します。
- RSVP プロトコルは、デバイス 1 からデバイス 2 へのパスにあるすべての RSVP 対応ルータ上で、使用可能な帯域幅リソースを確認することによって、エンドツーエンドの予約を確立しようとします。図 9-5 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、関係するルータ 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 メッセージを無視するだけであり、予約を確立することは可能です。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 を要求したとします（図 9-6 を参照）。

図 9-6　予約が成功しない RSVP シグナリング



ここでは、図 9-6 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 9-6 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、関係するルータ 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、ルータ R5 と R6 の間にあるリンク上に、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。

RSVP 運用モデル

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

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

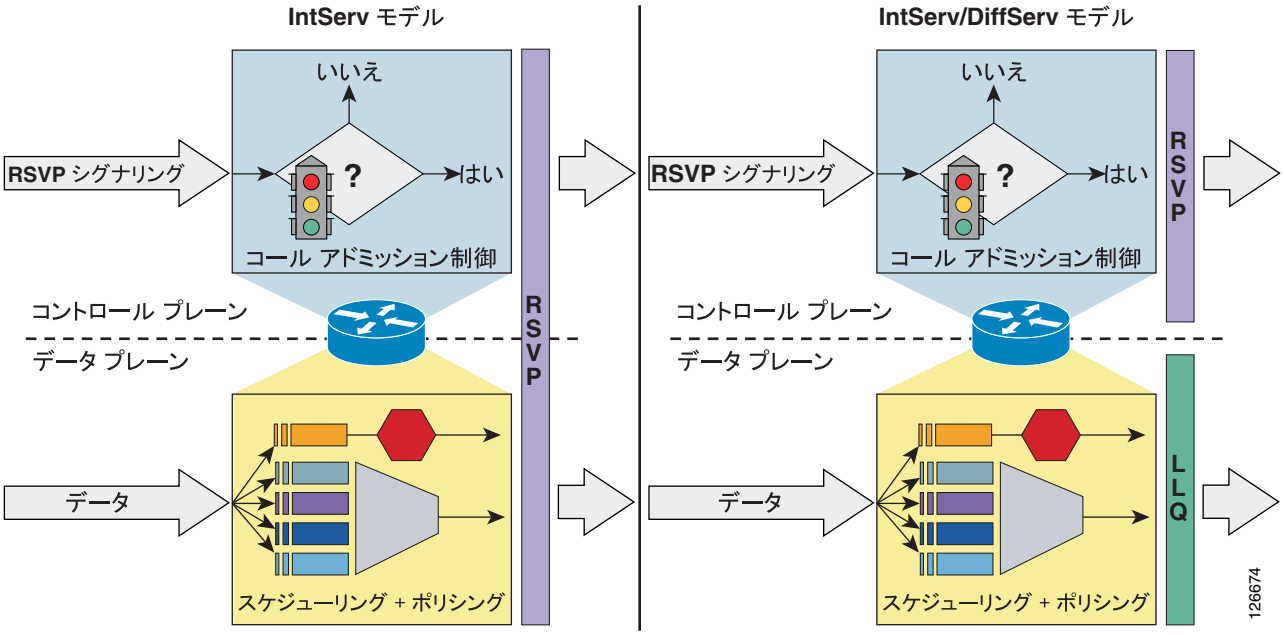
interface-kbps パラメータには、RSVP が所定のインターフェイス上で予約できる帯域幅の上限を指定します。*single-flow-kbps* パラメータには、予約 1 つあたりの帯域幅の上限を指定します（要求している帯域幅がこれより大きいフローは、インターフェイス上に使用可能な帯域幅がある場合でも拒否されます）。

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 9-7 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 9-7　2 つの RSVP 運用モデル：IntServ と IntServ/DiffServ



IntServ モデル

図 9-7 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。

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

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

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

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

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

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

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

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

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

IntServ/DiffServ モデル

図 9-7 の右側に示すように、IntServ/DiffServ モデルの RSVP では、アドミッション制御を実行するコントロール プレーンのみが関係し、データ プレーンは関係しません。つまり、コール アドミッション制御機能は、スケジューリング機能およびポリシング機能とは独立しています。スケジューリングとポリシングは、事前定義済みのクラス マップ、ポリシー マップ、およびサービス ポリシーに従って、低遅延キュー（LLQ）アルゴリズムによって実行できます。

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

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

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

これらのコマンドがアクティブになっている場合、RSVP は、**ip rsvp bandwidth** コマンドで定義された帯域幅上限のみに基づいて新しい予約を許可または拒否します。インターフェイス上で使用可能な実際の帯域幅リソースは考慮されません。許可された RSVP フローは、RSVP 以外の他のすべてのトラフィックと同じスケジューリング規則（たとえば、LLQ クラスとポリシー マップ）に従

います。このため、RSVP 対応トラフィックを適切な DSCP 値を使用してマーキングし、対応する PQ または CBWFQ キューの帯域幅は、RSVP 対応トラフィックと他のすべてのトラフィックの両方に対応できるように設定することが重要です。

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

設計上のベスト プラクティス

Cisco IP Communications ネットワークでは、すべてのデバイスが適切な DSCP 値を使用して自身のベアラ トラフィックとシグナリング トラフィックをマーキングし、QoS アプローチは、現時点では ディファレンシエーテッド サービス モデルに基づいています。このため、RSVP を IP WAN に追加するときは、IntServ モデルと IntServ/DiffServ モデルという 2 つの設計方式を選択できます。

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 キューに入るトラフィックは、RSVP 対応トラフィックのみである。
- プライオリティ キューに入る RSVP 未使用トラフィックは、アウトバンドのコール アドミッション制御メカニズム（Cisco CallManager ロケーションや Cisco IOS ゲートキーパーなど）によって、すべて確定的に一定量に制限される。

このような条件下では、ルータを設定するときに、LLQ の priority コマンドで指定した帯域幅値を超えないようにし、プライオリティ キューがオーバーサブスクリプションにならないようにする必要があります。

すべての PQ トラフィックが RSVP 対応の場合は、単に **ip rsvp bandwidth** コマンドと **priority** コマンドに同じ値を指定するだけで済みます。一部の PQ トラフィックが RSVP 非対応の場合は、**ip rsvp bandwidth** コマンドとアウトバンド コール アドミッション制御メカニズムで指定した値の合計が、**priority** コマンドで指定した帯域幅値を超えないようにする必要があります。

一方、この他のタイプのトラフィックは、自身の DSCP 値に基づいて引き続きクラスベース WFQ（CBWFQ）にアクセスできます。このアプローチでは、RSVP によって発生する処理オーバーヘッドが最も小さくなります。RSVP シグナリング メッセージを分析するだけで済み、データ パケットのスケジューリングが関係しないためです。ただし、PQ を宛先とする RSVP 未使用トラフィックが、事前設定済みの帯域幅値を超えないようにすることが重要です。トラフィックが過剰になると、不正なアプリケーションと RSVP 対応アプリケーションの両方に影響があります。

IP WAN インターフェイスのプライオリティ キューで、RSVP トラフィックと RSVP 未使用トラフィックの両方に対応する必要がある場合、RSVP 未使用トラフィックの最大量を見極めることが難しい場合は、IntServ モデルを採用することをお勧めします。

この場合、RSVP 未使用トラフィックは、**priority** キーワードによって、LLQ クラスを通じて一定量の PQ 帯域幅を与えられます。また、インターフェイス上で十分な帯域幅を未割り当てのまま残して、RSVP がその帯域幅をフローに使用できるようにしておく必要があります。さらに、**ip rsvp pq-profile** コマンドも使用して、どの RSVP フローを PQ に割り当てるかを定義する必要があります。このアプローチでは、すべてのデータ パケットを個々に分析する必要があるため、IP WAN ルータ上で RSVP によって発生する処理オーバーヘッドが大きくなります。ただし、RSVP 未使用 PQ トラフィックが不正な状態になって、LLQ に設定されている帯域幅値を超えた場合に、LLQ プライオリティ クラスに対して実行されるポリシングの影響を RSVP トラフィックが受けないという利点があります。

どのアプローチを選択したかにかかわらず、次のコマンドを使用して、シスコのベースライン QoS 推奨事項に従って RSVP シグナリング パケットをマーキングすること、およびこれらのパケットが他のタイプのシグナリング トラフィックと同様に扱われるようにすることが必要です。

```
ip rsvp signalling dscp 24
```

各種のトラフィックに対する推奨 DSCP 値の詳細については、第 3 章「ネットワーク インフラストラクチャ」を参照してください。

IP-to-IP ゲートウェイ

シスコのマルチサービス IP-to-IP ゲートウェイ（IP-IP ゲートウェイまたは IPIPGW とも呼ばれます）を使用すると、Cisco CallManager クラスタ間、H.323 ゲートウェイ間、またはこれらの 2 者間の IP WAN 接続に関して、ハブアンドスポーク トポロジにおける制約を緩和できます。

Cisco IOS 機能が、IP ネットワーク間で H.323 Voice over IP（VoIP）コールおよびビデオ会議コールを使用するためのメカニズムを提供します。IP-IP ゲートウェイの主な目的は、管理ドメインを通過する VoIP コールとビデオ コールにコントロール ポイントと境界を提供することです。このゲートウェイは、PSTN-to-IP ゲートウェイとほぼ同じ機能を実行しますが、公衆網レッグと IP コール レッグの代わりに、通常は 2 つの IP コール レッグに加入します。

企業の IP Communications 環境において、IP-IP ゲートウェイが備える最も興味深い機能は、このゲートウェイを通過する各コールのための RSVP 予約を生成できることです。P.9-8 の「RSVP」の項で説明しているように、RSVP は、トポロジ対応型のコール アドミッション制御メカニズムを提供するためのネットワーク ベース シグナリング プロトコルです。トポロジがハブアンドスポークである必要はなく、任意のネットワーク トポロジで機能します。

結果として、コール フローに 2 つの IP-IP ゲートウェイを挿入し、両者間で RSVP を有効にすることで、任意の IP WAN トポロジ上でコール アドミッション制御を実行できます。図 9-8 に、2 つのサイト A と B による基本的な例を示します。それぞれ Cisco CallManager クラスタがあり、任意のトポロジを持つ IP WAN を通じて接続されています。各サイトには IP-IP ゲートウェイも配置されており、2 つの Cisco CallManager クラスタは、すべてのサイト間コールを、ローカル IP-IP ゲートウェイを指しているトランクを通じてルーティングするように設定されています。サイト A とサイト B の間でコールがセットアップされると、次のイベントが発生します。

- サイト A の Cisco CallManager が、サイト A の IP-IP ゲートウェイに向かう H.323 トランク（図中のコール レッグ 1）を通じてコールをセットアップします。
- サイト A の IP-IP ゲートウェイが、サイト B の IP-IP ゲートウェイに向かう別のコールを確立しようとしますが、まず RSVP を使用して、IP WAN パスに沿って帯域幅リソースを確保します。
- RSVP 予約が成功すると、2 つの IP-IP ゲートウェイ間にコール レッグ 2 が確立されます。
- サイト B の IP-IP ゲートウェイが、サイト B の Cisco CallManager クラスタに向かう別のコール（図中のコール レッグ 3）を生成します。

図 9-8　RSVP コール アドミッション制御のための IP-to-IP ゲートウェイの簡単な例

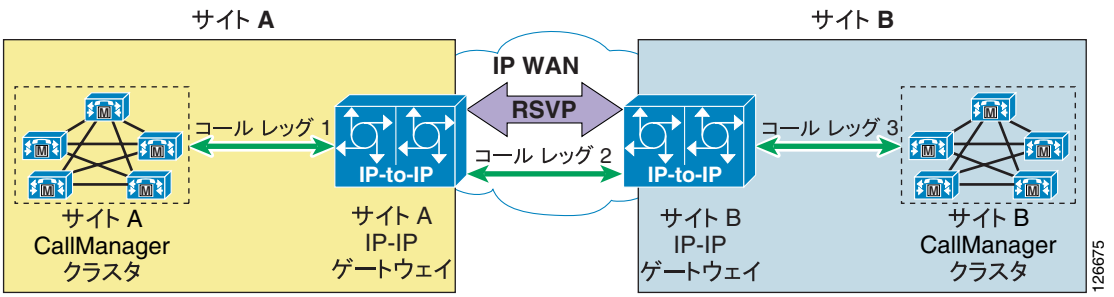


図 9-8 の例は、Cisco CallManager クラスタ間のすべてのコールが、IP-IP ゲートウェイ ペアを通じてルーティングされる単純なシナリオです。しかし、多くの実稼働環境では、このアプローチは十分にスケーラブルで柔軟なものとは言えません。これらの場合は、Cisco IOS ゲートキーパーを使用することで、Cisco CallManager クラスタ、H.323 ゲートウェイ、H.323 ビデオ会議エンドポイント、IP-IP ゲートウェイの間に幅広い通信オプションを配置できるようになります。

次の各項では、IP-IP ゲートウェイを中継ゾーン ゲートキーパーと連携して使用する方法について詳しく説明し、設計上のベスト プラクティス、スケーラビリティと冗長性に関する考慮事項、および設定ガイドラインも示します。

(注)　この項で説明した IP-IP ゲートウェイ関係のシナリオは、すべて複数の Cisco CallManager クラスタ間のコールに関するものです。同じ Cisco CallManager クラスタに登録されているエンドポイント間で、コールに IP-IP ゲートウェイを挿入することはお勧めしません。

中継ゾーン（Via-Zone）ゲートキーパー

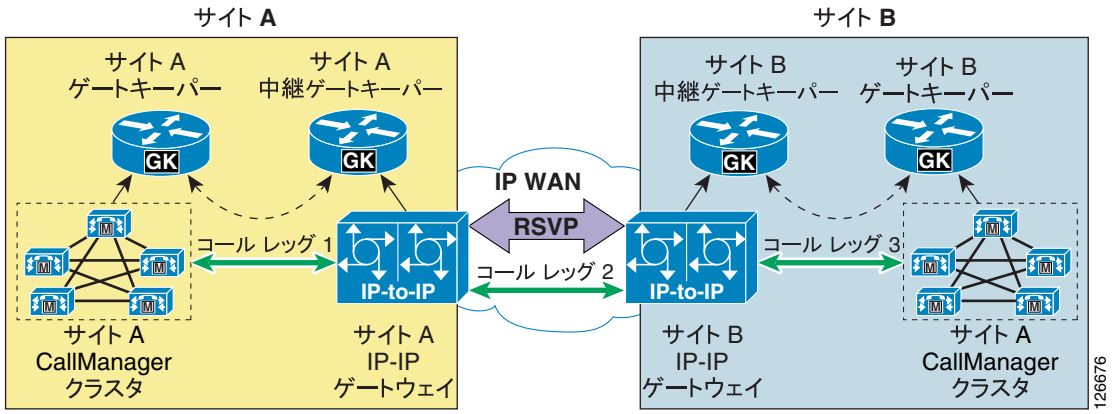
従来の Cisco IOS ゲートキーパー機能は、「中継ゾーン」ゲートキーパーという概念を通じて、IP-IP ゲートウェイに対応するように拡張されました。中継ゾーン ゲートキーパーがレガシー ゲートキーパーと異なっている点は、コール ルーティングでの LRQ メッセージと ARQ メッセージの使用方法です。中継ゾーン ゲートキーパーを使用しても、通常のクラスタおよび機能はそのまま使用できます。レガシー ゲートキーパーは、着信する LRQ を着信番号に基づいて検査します。具体的には、LRQ の destinationInfo 部分にある dialedDigits フィールドを検査します。中継ゾーン 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。設定にこれらのキーワードが含まれている場合、ゲートキーパーは新しい中継ゾーン処理を使用します。含まれていない場合は、従来の処理を使用します。

ARQ メッセージの場合、ゲートキーパーは宛先ゾーンに **outvia** キーワードが設定されているかどうかを調べます。**outvia** キーワードが設定されていて、**outvia** キーワードを使用して命名されているゾーンがゲートキーパーに対してローカルである場合は、そのゾーンの IP-IP ゲートウェイに ACF ポインティングが返され、コールが IP-IP ゲートウェイに転送されます。**outvia** キーワードを使用して命名されているゾーンがリモートである場合、ゲートキーパーは、ロケーション要求をリモート ゾーンのゲートキーパーではなく outvia ゲートキーパーに送信します。**invia** キーワードは、ARQ の処理では使用されません。

図 9-9 に、IP-IP ゲートウェイと中継ゾーン ゲートキーパーを Cisco CallManager クラスタおよびレガシー ゲートキーパーと連携するように使用して、コール ルーティングとコール アドミッション制御を提供する方法の例を示します。このシナリオには、次の考慮事項が適用されます。

- サイト A の Cisco CallManager クラスタは、サイト A のゲートキーパーを使用して、コールをクラスタ間で直接ルーティングする。
- サイト A のゲートキーパーは、サイト B の E.164 番号に転送されるすべてのコールを、サイト A の中継ゾーン ゲートキーパーに送信する。
- サイト A の中継ゾーン ゲートキーパーは、サイト A のゲートキーパーを発信元または宛先とするすべてのコールに対して、IP-IP ゲートウェイを挿入する。
- サイト A の IP-IP ゲートウェイは、コールをサイト B の IP-IP ゲートウェイに送信する前に、RSVP 予約を試行する。
- サイト B の Cisco CallManager クラスタ、ゲートキーパー、および IP-IP ゲートウェイは、サイト A のそれぞれと同様の方法で設定されている。

図 9-9　中継ゾーン ゲートキーパーを使用した RSVP のための IP-to-IP ゲートウェイ



設計上のベスト プラクティス

IP-IP ゲートウェイを Cisco CallManager と連携するように配置して、IP WAN で RSVP コール アドミッション制御を使用できるようにする場合は、次に示す設計上のベスト プラクティスに従ってください。

- 1 つまたはそれ以上の IP-IP ゲートウェイを通じて他の Cisco CallManager クラスタと音声専用通信を行うために、Cisco CallManager にトランクを設定する場合は、クラスタ間トランクを使用し、トランク設定ページの Media Termination Point required チェックボックスをオンにして、IP-IP ゲートウェイを介して補足サービスを使用できるようにします。
- クラスタ間トランクを介してコールするときに IP WAN 帯域幅の使用が増大するのを避けるために、IP-IP ゲートウェイと同じサイトに MTP リソースを配置することをお勧めします。これらの MTP リソースは、ソフトウェア ベース（Cisco MCS サーバや Cisco IOS ルータなど）でも、ハードウェア ベース（Cisco コミュニケーション メディア モジュールを備えた Catalyst 6500 や、NM-HDV ネットワーク モジュールを備えた Cisco IOS ルータなど）でもかまいません。使用できる MTP リソースの完全なリストについては、第 6 章「メディア リソース」を参照してください。
- 保留と保留解除、転送、会議などの Cisco CallManager 補足サービスは、IP-IP ゲートウェイを介してサポートされます。ただし、MTP を使用するため、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。
- クラスタ間に IP-IP ゲートウェイを通じてビデオ コールを確立する必要がある場合は、ビデオ コール専用のクラスタ間トランクを定義します。このとき、Media Termination Point required チェックボックスはオフにします（これは、MTP がビデオ コールをサポートしていないためです）。これらのトランクでは、補足サービスは一切使用できません。
- すべてのクラスタ間コールで IP-IP ゲートウェイを使用する場合に限り、Cisco CallManager から IP-IP ゲートウェイに向かう直接クラスタ間トランク（ゲートキーパーが制御しないトランク）を設定します。この場合でも、IP-IP ゲートウェイはゲートキーパーを使用してリモートの宛先を解決することができます。
- クラスタ間コールの解決、およびクラスタ間コールを IP-IP ゲートウェイを通じてルーティングするか、直接ルーティングするかの判定にゲートキーパーを使用する場合は、Cisco CallManager にゲートキーパー制御のクラスタ間トランクを設定します。このアプローチでは、より柔軟でスケーラビリティのある配置になります。
- IP-IP ゲートウェイ上の Cisco CallManager との互換性があるのは、Cisco IOS Release 12.3(1) 以降です。Cisco IOS Release 12.3(7)T 以降を使用することをお勧めします。

- ゲートキーパーと中継ゾーン ゲートキーパーの機能は、それぞれ別のルータ プラットフォーム上で実行して、分離します。各 IP-IP ゲートウェイに対して、専用の中継ゾーン ゲートキーパーを配置する必要があります。
- IP-IP ゲートウェイは、遅延保証付きの RSVP 予約を要求するように設定します。また、コールを正常に運用するために、予約を必須にします（詳細については、P.9-18 の「設定のガイドライン」の項を参照）。
- 中継ゾーン ゲートキーパー機能と IP-IP ゲートウェイ機能は、同じルータ プラットフォーム上で実行（共存）することができます。ただし、P.9-18 の「冗長性」の項で説明しているスケーラビリティの要件に注意してください。
- 同じ Cisco CallManager クラスタに制御されているエンドポイント間では、コールに IP-IP ゲートウェイを使用しないでください。

冗長性

冗長性とスケーラビリティを実現するには、複数の IP-IP ゲートウェイを同じ中継ゾーン ゲートキーパーおよび同じ中継ゾーンに登録します。中継ゾーン ゲートキーパーは、ラウンドロビン アルゴリズムを使用して、同じ中継ゾーンに含まれているすべての IP-IP ゲートウェイに着信コールを自動的に分配します。

IP-IP ゲートウェイに障害が発生すると、そのゲートウェイは中継ゾーン ゲートキーパーへの登録を失います。ゲートキーパーは、使用可能リソースのリストからそのゲートウェイを削除します。

IP-IP ゲートウェイに対して、最大負荷しきい値を手動で設定することもできます。ある IP-IP ゲートウェイで回線の使用率が一定の割合を超えると、そのゲートウェイは新しいコールの処理用としては選択されなくなり、回線の使用率が一定の割合を下回ると、再び使用可能になります。このように設定するには、次の Cisco IOS コマンドを使用します。

- IP-IP ゲートウェイ上：

```
ip circuit max-calls max-call-number
```

- ゲートキーパー上：

```
endpoint resource-threshold onset onset-threshold abatement abatement-threshold
```

これらのコマンドの詳細については、次の Web サイトで入手できる Cisco IOS コマンド解説資料を参照してください。

http://www.cisco.com

設定のガイドライン

ここでは、図 9-10 に示したネットワーク ダイアグラムに基づく簡単な設定例を示します。この項は、詳細なコマンド リファレンス ガイドを意図したものではなく、一般的な配置シナリオに役立つガイドラインをまとめたものです。IP-IP ゲートウェイおよび中継ゾーン ゲートキーパーを設定する方法の詳細については、次の Web サイトで入手可能な、シスコ マルチサービス IP-to-IP ゲートウェイのオンライン ドキュメントで説明しています。

http://www.cisco.com

図 9-10　中継ゾーン ゲートキーパーを使用した IP-IP ゲートウェイの設定例

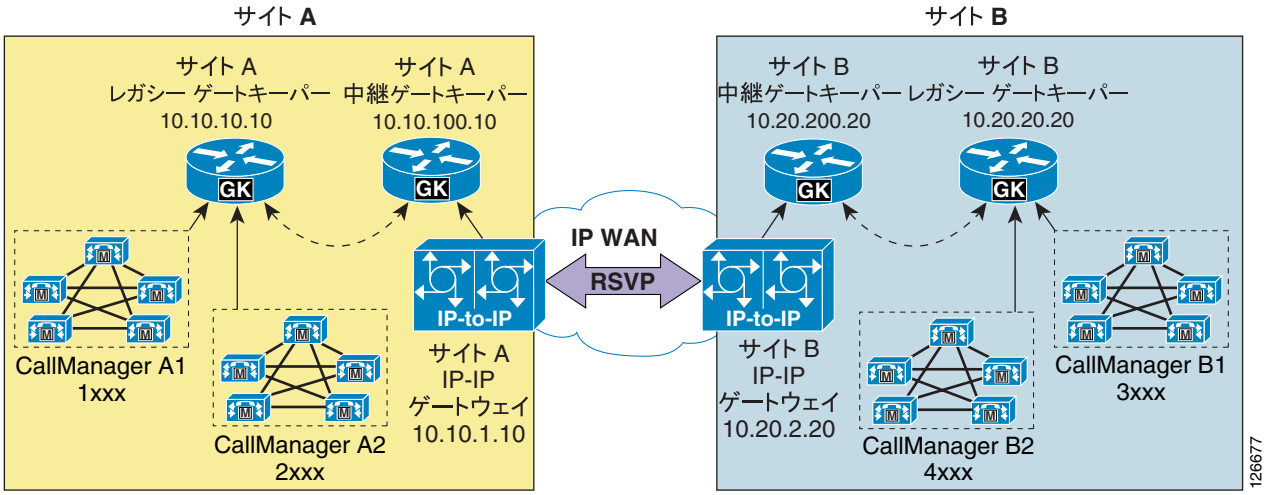


図 9-10 に示すネットワークで、サイト A に、電話内線番号 1*xxx* を持つクラスタ A1、および電話内線番号 2*xxx* を持つクラスタ A2 という 2 つの Cisco CallManager クラスタがあるとします。サイト B にも、電話内線番号 3*xxx* を持つクラスタ B1、および電話内線番号 4*xxx* を持つクラスタ B2 という 2 つの Cisco CallManager クラスタがあります。

次の各項に、サイト A にあるデバイスに関連する設定を示します。サイト A の内部でやり取りされるコールは、（サイト A のレガシー ゲートキーパーを使用して）Cisco CallManager クラスタ間で直接ルーティングされるのに対して、サイト B に向かうコールは、2 つの IP-IP ゲートウェイを通じて（それぞれのレガシー ゲートキーパーと中継ゾーン ゲートキーパーを使用して）ルーティングされます。

Cisco CallManager

クラスタ A1 とクラスタ A2 は、ゲートキーパー制御の 2 つのクラスタ間トランクを使用します。最初のトランク T1 は、必要となる MTP を使用して設定され、サイト A のレガシー ゲートキーパーを指しています。2 番目のトランク T2 もサイト A のレガシー ゲートキーパーを指していますが、MTP を必要としません。

[34]XXX ルート パターンは、ゲートキーパーおよび IP-IP ゲートウェイを通じてサイト B のクラスタに到達するために、ルート リストおよびルート グループを通じてトランク T1 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 トランク T2 を指すことで、クラスタ A1 と A2 がゲートキーパーを通じて互いに通信できるようにしています。

レガシー ゲートキーパー

サイト A のレガシー ゲートキーパーは、クラスタ A1 と A2 の間ではコールを直接ルーティングし、サイト B に向かうコール（内線番号 3*xxx* と 4*xxx*）については、すべてサイト A の中継ゾーン ゲートキーパーに送信します。例 9-1 に、関連する設定を示します。

例 9-1　サイト A のレガシー ゲートキーパー設定

```
gatekeeper
 zone local CCM-A1 customer.com 10.10.10.10
 zone local CCM-A2 customer.com
 zone remote A-VIAGK customer.com 10.10.100.10
 zone prefix CCM-A1 1...
 zone prefix CCM-A2 2...
 zone prefix A-VIAGK 3...
 zone prefix A-VIAGK 4...
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

中継ゾーン ゲートキーパー

サイト A の中継ゾーン ゲートキーパーは、サイト B の Cisco CallManager クラスタ（内線番号 3*xxx* と 4*xxx*）に向かうコールをサイト B の中継ゾーン ゲートキーパーに送信し、サイト B で発着信されるコールに使用される IP-IP ゲートウェイを呼び出します。サイト A のクラスタに向かうコールは、サイト A のレガシー ゲートキーパーにルーティングされ、IP-IP ゲートウェイは呼び出されません。例 9-2 に、関連する設定を示します。

例 9-2　サイト A の中継ゾーン ゲートキーパー設定

```
gatekeeper
 zone local A-VIAGK customer.com 10.10.100.10
 zone remote CCM-A1 customer.com 10.10.10.10
 zone remote CCM-A2 customer.com 10.10.10.10
 zone remote B-VIAGK customer.com 10.20.200.20 invia A-VIAGK outvia A-VIAGK
 zone prefix B-VIAGK 3...
 zone prefix B-VIAGK 4...
 zone prefix CCM-A1 1...
 zone prefix CCM-A2 2...
 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に **invia** キーワードと **outvia** キーワードが存在しているため、このゾーンの中継ゾーン ゲートキーパーの処理がアクティブになります。つまり、B-VIAGK リモート ゾーンが宛先また発信元となるすべてのコールについて、中継ゾーン ゲートキーパーは、A-VIAGK ローカル ゾーンに登録されている IP-IP ゲートウェイ リソースを呼び出します。
- CCM-A1 リモート ゾーンおよび CCM-A2 リモート ゾーンに関連するコマンドラインには、**invia** キーワードと **outvia** キーワードがありません。このため、標準のゲートキーパー処理が適用され、これらのゾーンで発着信されるコールに対しては、IP-IP ゲートウェイは呼び出されません。

IP-IP ゲートウェイ

サイト A の IP-IP ゲートウェイは、サイト B の Cisco CallManager クラスタ（内線番号 3*xxx* と 4*xxx*）に向かう音声コールとビデオ コールについては、RSVP 予約を要求します。一方で、サイト A の Cisco CallManager クラスタ（内線番号 1*xxx* と 2*xxx*）に向かうコールについては要求しません。例 9-3 に、関連する設定を示します。

例 9-3　サイト A の IP-IP ゲートウェイ設定

```
voice service voip
 allow-connections h323 to h323
 h323
   h225 h245-address
   ccm-compatible
   call sync-rsvp slow-start
!
gateway
!
interface FastEthernet0/1
 ip address 10.10.1.10 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id A-VIAGK ipaddr 10.10.100.10
 h323-gateway voip h323-id A-IPIPGW
 h323-gateway voip bind srcaddr 10.10.1.10
!
dial-peer voice 10 voip
 destination-pattern [3-4]...
 session target ras
 req-qos guaranteed-delay audio
 req-qos guaranteed-delay video
 acc-qos guaranteed-delay audio
 acc-qos guaranteed-delay video
 codec transparent
!
dial-peer voice 11 voip
 destination-pattern [1-2]...
 session target ras
 codec transparent
```

例 9-3 に示す設定には、次の考慮事項が適用されます。

- Cisco IOS Release 12.3(7)T 以降では、IP-IP ゲートウェイ上で、Cisco CallManager 互換モードがデフォルトでは有効になっていません。このため、**h225 h245-address** コマンドと **ccm-compatible** コマンドが必要になります。
- **call sync-rsvp slow-start** コマンドで、H.323 スロースタート音声コールおよびビデオ コールと RSVP シグナリングの同期を有効にします。この機能は、通常はデフォルトで有効になっています。音声コールとビデオ コールで RSVP 予約を必須にする場合は、このコマンドが無効になっていないことを確認してください。
- **req-qos guaranteed-delay** [**audio** | **video**] コマンドで、ダイヤルピア 10（サイト B の内線に到達するためのダイヤルピア）を使用する音声コールとビデオ コールについて、IP-IP ゲートウェイが遅延保証付きの RSVP 予約を要求することを指定します。
- **acc-qos guaranteed-delay** [**audio** | **video**] コマンドで、音声コールとビデオ コールに関して許容可能な最小限の QoS レベルも、遅延保証付き RSVP 予約であることを指定します。これは、RSVP 要求が失敗した場合はコールも失敗するので、RSVP 予約を必須にすることを意味します。RSVP 予約がオプションになるように（予約が失敗した場合でもコールが通過できるように）IP-IP ゲートウェイを設定するには、代わりに **acc-qos best-effort** [**audio** | **video**] コマンドを使用します。

コール アドミッション制御の設計

ここでは、各種の Cisco CallManager 配置モデルおよび次の IP WAN トポロジに対して、コール アドミッション制御メカニズムを適用する方法について説明します。

- 単純なハブアンドスポーク トポロジ（P.9-22）
- 2 層ハブアンドスポーク トポロジ（P.9-27）
- MPLS ベースのトポロジ（P.9-34）
- 複合トポロジ（P.9-41）

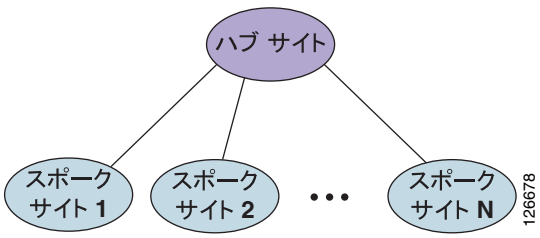
採用する Cisco CallManager 配置モデルに基づいて、トポロジごとにそれぞれ別の設計考慮事項を示します。

(注)　この項で説明するコール アドミッション制御ソリューションは、RSVP に基づくものを除いて、すべて各サイトの使用可能帯域幅を静的に設定することで成り立っています。このコール アドミッション制御メカニズムは、トポロジの変更やリンク障害に動的に対応することはできません。サイトが IP WAN に 2 系統で接続している場合、計算時には帯域幅が最も小さいリンクを選択して、最悪のシナリオを見越しておく必要があります。

単純なハブアンドスポーク トポロジ

図 9-11 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 9-11　単純なハブアンドスポーク トポロジ



単純なハブアンドスポーク トポロジに関する設計上の考慮事項は、次のような従来のレイヤ 2 IP WAN テクノロジーに適用されます。

- フレーム リレー
- ATM
- フレーム リレー /ATM 間サービス インターワーキング
- 専用回線

MPLS テクノロジーに基づいた IP WAN 配置については、P.9-34 の「MPLS ベースのトポロジ」の項を参照してください。

以降では、採用する Cisco CallManager 配置モデルごとに、単純なハブアンドスポーク トポロジに関する設計上のベスト プラクティスを示します。

- 単純集中型配置（P.9-23）

  1 つまたはそれ以上の Cisco CallManager クラスタをハブ サイトに配置し、スポーク サイトには電話とゲートウェイのみを配置します。
- 単純分散型配置（P.9-23）

  Cisco CallManager クラスタを各サイトに配置します。
- 集中型および分散型複合配置（P.9-26）

  Cisco CallManager クラスタをハブ サイトと一部のスポーク サイトに配置し、それ以外のスポーク サイトには電話とゲートウェイのみを配置します。

単純集中型配置

単純なハブアンドスポーク トポロジ上にあり、集中型コール処理を使用するマルチサイト WAN 配置では、Cisco CallManager の「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。コール アドミッション制御に対してロケーションを使用する場合は、次のガイドラインに従ってください。

- 各スポーク サイトの Cisco CallManager に対しては、個別にロケーション設定が必要です。
- 各サイトの帯域幅の上限を、そのサイトに使用されているコーデックのタイプに応じて、適切に設定します（帯域幅の推奨設定については、表 9-1 を参照してください）。
- 各スポーク サイトのすべてのデバイスを適切なロケーションに割り当てます。
- ハブ サイトのデバイスは、<None> ロケーションのままにします。
- あるデバイスを別のロケーションに移した場合、ロケーションの設定も変更します。
- Cisco CallManager は、ロケーションを 500 個所までサポートします。
- WAN の帯域幅が十分にない場合に、公衆網を介した自動ルーティングを実行する必要があるときは、Cisco CallManager 上で Automated Alternate Routing（AAR）機能を設定します（P.10-20 の「Automated Alternate Routing」を参照）。
- 中央サイトに複数の Cisco CallManager クラスタを配置する場合は、クラスタ間トランク デバイスを <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。

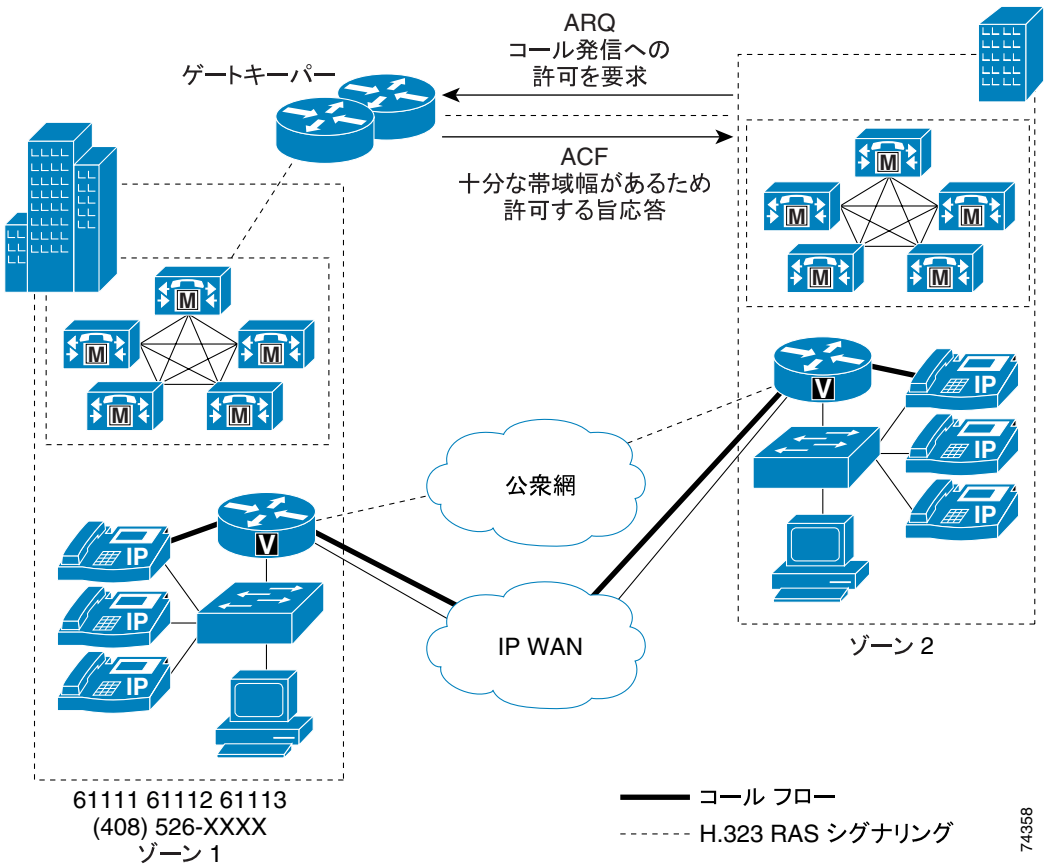
（注） Cisco CallManager Release 3.1 以前のリリースでは、コール アドミッション制御用にロケーションを使用する場合には、クラスタはプライマリ（アクティブ）Cisco CallManager サーバを 1 つのみサポートしていました。Cisco CallManager Release 3.1 およびそれ以降では、ロケーションの帯域幅は、クラスタ内のすべての Cisco CallManager サブスクライバ サーバ間で共有されるので、ロケーション メカニズムには任意のサイズのクラスタを使用できるようになりました。

単純分散型配置

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は Cisco IOS ゲートキーパーに登録し、IP WAN コールを発信しようとするたびに、エージェントがゲートキーパーに照会します。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 9-12 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。この設計は、本来、アドミッション制御を提供するためのコール アカウンティング方式から構成されます。この方式では、ゲートキーパーは、IP WAN コールによって消費される帯域幅をトラッキングします。ゾーンに最大帯域幅を設定する場合は、音声トラフィックの消費量が通常は WAN リンクの 33% を超えてはならないという制限事項を考慮してください。

図 9-12　ゲートキーパーを使用したコール アドミッション制御



要約すると、ゲートキーパーによるコール アドミッション制御の主な設計上の意味は、次のとおりです。

- ゲートキーパーは、マルチサイト分散型コール処理環境で数百のサイトをサポートする。
- ゲートキーパーは、ゾーンに出入りする使用済み帯域幅をトラッキングする。各コールによって消費される帯域幅量は、コール処理エージェントからのコール要求の総数、およびコールに使用されるコーデックのタイプに依存します。
- コール　ARQ（アドミッション要求）に対する帯域幅計算には、cRTP（Compressed　Real-time Transport Protocol）やその他のトランスポートのオーバーヘッドは含まれない。
- トポロジは、ゲートキーパーのゾーン概念に基づいた、論理ハブアンドスポークである。

H.225 ゲートキーパー制御トランクは、Cisco CallManager が Cisco CallManager クラスタおよび H.323 ゲートキーパーに登録済みの他の H.323 デバイスと通信できるようにします。H.225 ゲートキーパー制御トランクは、Cisco CallManager のみの環境ではお勧めしませんが、Cisco CallManager と Cisco CallManager Express（または H.323 ゲートウェイ）の混合環境では必要です。H.225 トランクは、コールごとに他の H.323 デバイスを検出しようとします。クラスタ間トランク プロトコルを認識できるデバイスを検出した場合は、自動的にそのプロトコルを使用します。トランクが他のデバイスを検出できない場合、Cisco CallManager は標準の H.225 プロトコルを使用します。

クラスタ間トランク プロトコルの検出は、Cisco CallManager Release 3.2 で追加された機能です。これより前のリリースと併用する場合は、Cisco CallManager クラスタと通信するために、クラスタ間トランクを使用する必要があります。使用しない場合は、すべてのクラスタを Release 3.2 以降にアップグレードして、H.225 トランクと H.323 トランクを正しく操作できるようにします。クラスタ間トランクと H.225 トランクのどちらか一方でも使用しない場合、H.323 デバイスと Cisco CallManager の両方をすべてゲートキーパーに登録して、正常に運用することはできません。

コール アドミッション制御に H.225 ゲートキーパー制御トランクを使用する場合は、次に示すガイドラインに従ってください。

- 各 Cisco CallManager クラスタのゲートウェイは、同じ方法で設定します。
- Cisco CallManager クラスタに H.225 ゲートキーパー制御トランクを設定して、ゾーンをサイトの適切なゲートキーパー ゾーンに対応付けます。
- デバイス プールの Cisco CallManager 冗長性グループにリストされている各 Cisco CallManager サブスクライバは、H.225 ゲートキーパー制御トランクをゲートキーパーに登録します（最大で 3 つまで）。
- コールは、Cisco CallManager クラスタ内に登録済みのトランク間にロードバランスされます。
- Cisco CallManager は、複数のゲートキーパーおよびトランクをサポートします。
- トランクをルート グループとルート リスト コンストラクトに配置すると、自動公衆網フェールオーバーを提供できます。詳細については、P.10-1 の「ダイヤル プラン」を参照してください。
- Cisco CallManager、Cisco CallManager Express、または音声ゲートウェイをサポートしている各サイトに対するゲートキーパーのゾーンは、個別に設定します。
- **bandwidth interzone** コマンドをゲートキーパーに使用して、そのゲートキーパーに直接登録済みの Cisco CallManager クラスタ、Cisco CallManager Express サーバ、および H.323 デバイス間の帯域幅の制御を行います（コーデック タイプ別の帯域幅の設定については、表 9-2 を参照してください）。
- 1 つの Cisco IOS ゲートキーパーで、100 までのゾーンまたはサイトをサポートできます。例 9-4 では、一般的なゲートキーパー設定を示しています。
- 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 クラスタリングが利用可能ではない場合に限り使用します。

例 9-4　H.225 ゲートキーパー制御トランクに対する一般的なゲートウェイ設定

```
gatekeeper
 zone local GK-Headquarters customer.com 10.1.10.100
 zone local GK-BranchA  customer.com
 zone local GK-BranchB customer.com
 zone prefix GK-Headquarters 408…….
 zone prefix GK-BranchA 212…….
 zone prefix GK-BranchB 818…….
 bandwidth interzone GK-Headquarters 200
 bandwidth interzone GK-BranchA 200
 bandwidth interzone GK-BranchB 200
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 9-4 について説明します。

- **zone local** コマンドを使用して、ゲートキーパー ゾーンを作成しています。設定済みのゾーンには、各 Cisco CallManager およびゲートウェイが登録されます。
- ゾーン間のコール ルーティングには、**zone prefix** が使用されています。
- **bandwidth interzone** コマンドは、ゾーン間で利用できる帯域幅の量を割り当てます。
- **gw-type-prefix 1# default technology** コマンドは、ゾーン内で解決されないコールを登録済みテクノロジー プレフィックス 1# を持つデバイスにルーティングします。この設定例では、Cisco CallManager トランクが該当します。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco CallManager トランク上にできるコール ルーティング ループを回避します。

（注） クラスタ間ゲートキーパー制御トランクは、Cisco CallManager が H.323 ゲートキーパーに登録済みの他の Cisco CallManager クラスタとの通信を行えるようにします。ゲートキーパー制御のクラスタ間トランクは、全面的に Cisco CallManager を基盤としている配置でのみ使用することをお勧めします。

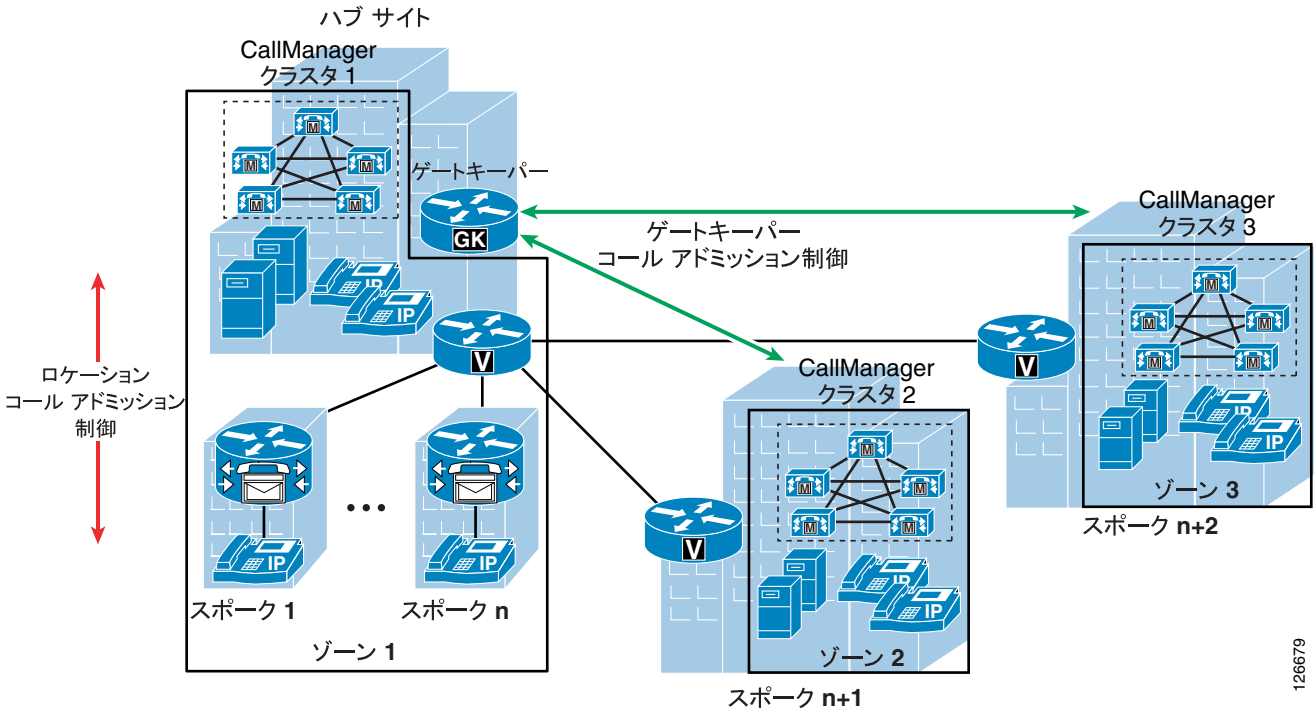
集中型および分散型複合配置

集中型および分散型のコール処理を単純なハブアンドスポーク トポロジ上で組み合せた複合配置では、Cisco IOS ゲートキーパーと Cisco CallManager ロケーションの両方を使用してコール アドミッション制御を提供できます。図 9-13 では、スポーク サイト 1 ～ n がハブ サイトの Cisco CallManager クラスタ 1 によって集中制御されるトポロジを示しています。スポーク サイト (n+1) と (n+2) は、それぞれが専用のオンサイト Cisco CallManager クラスタ（クラスタ 2 と 3）を持っています。

このタイプの配置には、次の考慮事項が適用されます。

- スポーク サイト 1 ～ n にコール アドミッション制御を提供するには、Cisco CallManager ロケーションを使用します。各スポーク サイトは、それぞれ別のロケーションに割り当てます。この他の考慮事項については、P.9-23 の「単純集中型配置」の項を参照してください。
- スポーク サイト (n+1) と (n+2) にコール アドミッション制御を提供するには、ハブ サイトにある Cisco IOS ゲートキーパーを使用します。各 Cisco CallManager クラスタは、それぞれ別のゲートキーパー ゾーンに割り当てます。この他の考慮事項については、P.9-23 の「単純分散型配置」の項を参照してください。
- ゲートキーパー制御のクラスタ間トランク（または H.225 トランク）は、<None> ロケーションのままにします。これは、クラスタ間のコール アドミッション制御はゲートキーパーが実行するためです。

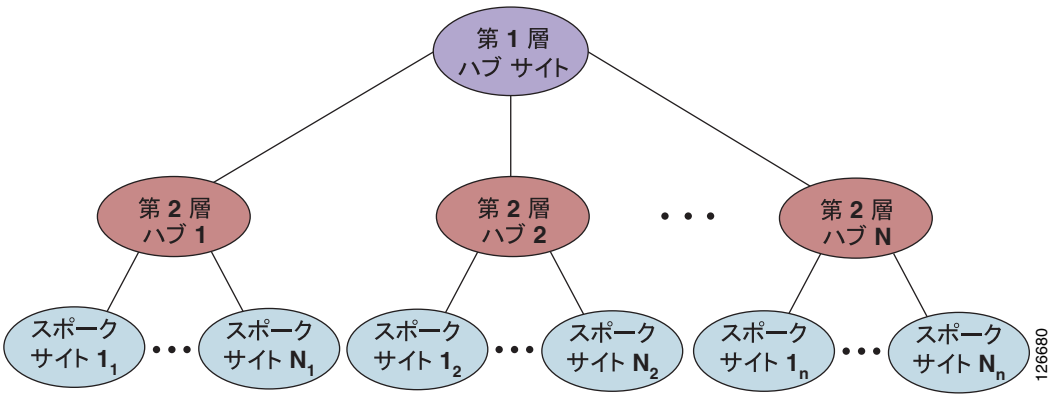
図 9-13　単純なハブアンドスポーク トポロジの集中型および分散型複合配置



2 層ハブアンドスポーク トポロジ

図 9-14 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、ハブアンドスポーク トポロジを「2 乗」したものと見なすことができ、3 階層のサイトで構成されています。第 1 層ハブ サイト、第 2 層ハブサイト、およびスポーク サイトです。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 9-14　2 層ハブアンドスポーク トポロジ



2 層ハブアンドスポーク トポロジに関する設計上の考慮事項は、次のような従来のレイヤ 2 IP WAN テクノロジーに適用されます。

- フレーム リレー
- ATM
- フレーム リレー /ATM 間サービス インターワーキング
- 専用回線

MPLS テクノロジーに基づいた IP WAN 配置については、P.9-34 の「MPLS ベースのトポロジ」の項を参照してください。

以降では、採用する Cisco CallManager 配置モデルごとに、2 層ハブアンドスポーク トポロジに関する設計上のベスト プラクティスを示します。

- 単純集中型配置（P.9-28）

  1 つまたはそれ以上の Cisco CallManager クラスタを第 1 層ハブ サイトに配置し、第 2 層ハブ サイトとスポーク サイトには電話とゲートウェイのみを配置します。
- 単純分散型配置（P.9-31）

  Cisco CallManager クラスタを各サイトに配置します。
- 集中型および分散型複合配置（P.9-33）

  Cisco CallManager クラスタを第 1 層ハブ サイトと第 2 層ハブ サイトに配置し、スポーク サイトには電話とゲートウェイのみを配置します。

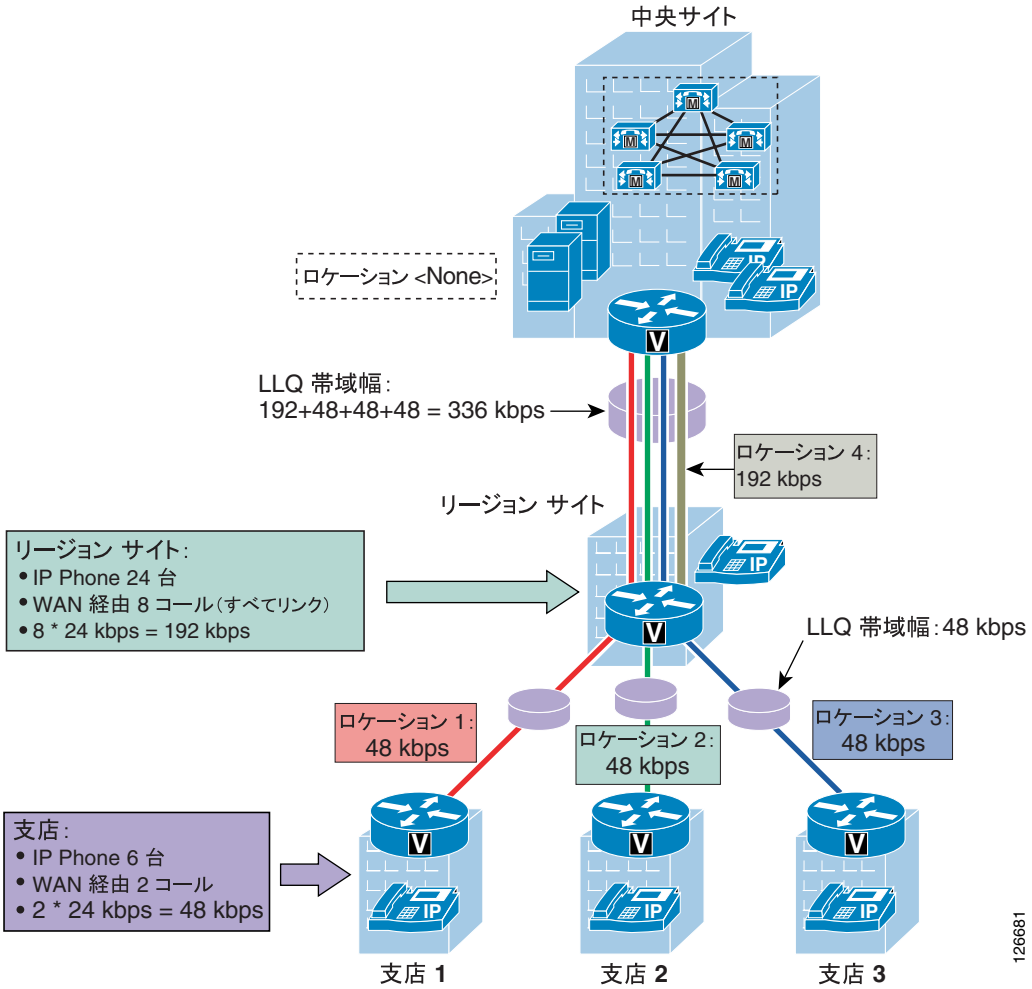
単純集中型配置

2 層ハブアンドスポーク トポロジを使用する集中型コール処理配置は、コール アドミッション制御に関しては問題が生じます。Cisco CallManager の「ロケーション」アルゴリズムは、集中型コール処理配置でコール アドミッション制御に使用できる唯一のメカニズムであり、単純なハブアンドスポーク トポロジで機能するように設計されています。

ここでは、このようなトポロジで生じる問題点を緩和する方法について説明します。ただし、この回避策には制約があるため、この問題を解決するには、Cisco CallManager クラスタの分布を変更するか、トポロジを単純なハブアンドスポークに変更する方法をお勧めします。この方法については、この項の最後で説明します。

図 9-15 では、集中型コール処理配置の Cisco CallManager クラスタで 2 層ハブアンドスポーク トポロジをサポートする方法を示しています。

図 9-15　単純集中型配置の 2 層ハブアンドスポーク



この方法を使用する場合は、次のガイドラインに従ってください。

- 第 1 層ハブ サイト（中央サイト）のデバイスは、<None> ロケーションのままにします。
- 各スポーク　サイトのデバイスは、独自のロケーションに配置します。ロケーションの帯域幅は、それぞれのサイトで発着信を許可するコール数に従って定義します。図 9-15 の例では、3 つのスポーク サイト（支店 1、2、3）のロケーションの帯域幅を 48 Kbps に設定しています。これは、G.729 コーデックを使用するコール 2 つに対応できる値です。
- 第 2 層ハブ サイトとスポーク サイト間のリンクについて、プライオリティ キューの帯域幅を LLQ 設定で設定します。この帯域幅が、スポーク サイトのロケーションの帯域幅と一致するようにします。ここでは、この帯域幅設定は 48 Kbps です。
- 各第 2 層ハブ サイトのデバイスは、独自のロケーションに配置します。ロケーションの帯域幅は、それぞれのサイトで発着信を許可するコール数に従って定義します。この帯域幅については、第 2 層ハブ サイトで発着信されるすべてのコールを考慮に入れてください。第 1 層ハブ サイトに向かうコールに加えて、下位のスポーク サイトに向かうコールも含めます。図 9-15 の例では、第 2 層ハブ サイト（リージョン サイト）のロケーションの帯域幅を 192 Kbps に設定しています。これは、G.729 コーデックを使用するコール 8 つに対応できる値です。
- 第 1 層ハブ サイトと各第 2 層ハブ サイト間のリンクについて、プライオリティ キューの帯域幅を LLQ 設定で設定します。この帯域幅が、第 2 層ハブ サイト自体のロケーション帯域幅と、その第 2 層ハブ サイトに接続されているスポーク サイトのすべてのロケーション帯域幅を合計した値と一致するようにします。ここでは、この帯域幅設定は 192 + 48 + 48 + 48 = 336 Kbps です。

(注) この例では、説明を簡潔にするために、レイヤ 3 の値（つまり、G.729 コールの 24 Kpbs）に基づいた LLQ 帯域幅設定を示しています。LLQ キューを設定するときは、実際にはレイヤ 2 オーバーヘッドも考慮する必要があります。各種のレイヤ 2 WAN テクノロジーの帯域幅値の完全なリストについては、P.3-31 の「帯域幅のプロビジョニング」の項の表 3-5 を参照してください。

図 9-15 の例に示したように、この方法は、第 1 層ハブと第 2 層ハブ間のプライオリティ キュー帯域幅を多めに設定することで成り立っています。この設定によって、Cisco CallManager ロケーションが、一連のスポーク サイトが実際には特定の第 2 層ハブ サイトを通じて接続されているという事実を認識しない点を補っています。したがって、設定では、任意の 2 サイトが通信するときは必ず第 1 層ハブ サイトを経由する、と見なして帯域幅を考慮する必要があります。

この方法では、どのような状況でも音声品質が維持されますが、次の設計上の考慮事項と警告事項も適用されるようになります。

- 第 2 層ハブ サイト 1 つあたりのスポーク サイト数が大きくなると、第 2 層サイトと第 1 層ハブ サイトの間に設定する必要のあるプライオリティ キュー帯域幅の量も大幅に増加します。
- 計算は最悪のシナリオに基づいて行うため、帯域幅の使用率は、限界値よりは低くなります。たとえば、図 9-15 の 3 つの支店それぞれで、リージョン サイトに向かう 2 つのアクティブなコールが発生しているとします。この場合、プライオリティ キューで実際に使用可能な帯域幅を見ると、さらに 14 のコールを許可できますが、Cisco CallManager は、これ以上はリージョン サイトから中央サイトに向かう 2 つのコールしか許可しません。
- IP WAN を介してコールを確立できるかどうかは、実際の帯域幅リソースに余裕がある場合でも保証されません。たとえば、図 9-15 のリージョン サイトで、中央サイトに向かう 8 つのアクティブなコールが発生しているとします。この場合、使用可能な実際の帯域幅を見ると、各支店からの 2 つのコールを許可できますが、Cisco CallManager は支店がリージョン サイトにコールすることを許可しません。一方、同じ状況で支店が中央サイトにコールすることは許可されます。

(注) 第 2 層ハブ サイトに接続されているスポーク サイトを、その第 2 層ハブ サイトと同じロケーションにすべて配置することはお勧めしません。このようなソリューションは、すべてのシナリオで音声品質を保証できるとは限らず、シスコではサポートしません。

この項で今までに説明したように、この項で示した回避策にはいくつかの制約があります。これよりも優れたソリューションとしては、次のいずれかの変更を実施して、配置の特性を変更することをお勧めします。

- 第 2 層ハブ サイトとスポーク サイトにある電話の数に基づいて、第 2 層ハブ サイトと第 1 層ハブ サイト間のリンク速度およびプライオリティ キュー帯域幅を十分に増強し、オーバーサブスクリプションの状態にならないようにします。この状況では、第 2 層ハブ サイトは第 1 層ハブ サイトと論理上同じ場所にあるものと見なすことができ、第 2 層ハブ サイトのデバイスを <None> ロケーションのままにすることができます。したがって、ロケーションを、スポーク サイトと第 2 層ハブ サイト間にあるリンクの帯域幅使用を制御するためにのみ使用できます。
- すべてのスポーク サイトを第 1 層ハブ サイトに直接接続して、ネットワーク トポロジを単純なハブアンドスポークに変更します。P.9-22 の「単純なハブアンドスポーク トポロジ」の項の説明に従って、Cisco CallManager 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行します。
- ネットワーク トポロジを MPLS ベース ネットワークに変更します。P.9-34 の「MPLS ベースのトポロジ」の項の説明に従って、Cisco CallManager 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行します。

- 第 1 層ハブ サイトに加えて、第 2 層ハブ サイトにも Cisco CallManager クラスタを配置して、集中型および分散型複合 Cisco CallManager 配置にします。第 1 層ハブ サイトと第 2 層ハブ サイトの間にあるリンクに対してコール アドミッション制御を実行するには、Cisco IOS ゲートキーパーを使用します。第 2 層ハブ サイトとスポーク サイト間のリンクに対しては、Cisco CallManager ロケーションを使用します。詳細については、P.9-33 の「集中型および分散型複合配置」の項を参照してください。

単純分散型配置

2 層ハブアンドスポーク トポロジを使用する分散型のコール処理配置では、Cisco IOS ゲートキーパーを使用することで、すべての IP WAN リンクに対してコール アドミッション制御を実行できます。図 9-16 では、このような配置の例を示しています。Cisco CallManager を各サイトに配置し、Cisco IOS ゲートキーパーを第 1 層ハブ サイトと第 2 層ハブ サイトに配置し、ディレクトリ ゲートキーパーを第 1 層ハブ サイトに配置しています。

図 9-16　単純分散型配置の 2 層ハブアンドスポーク

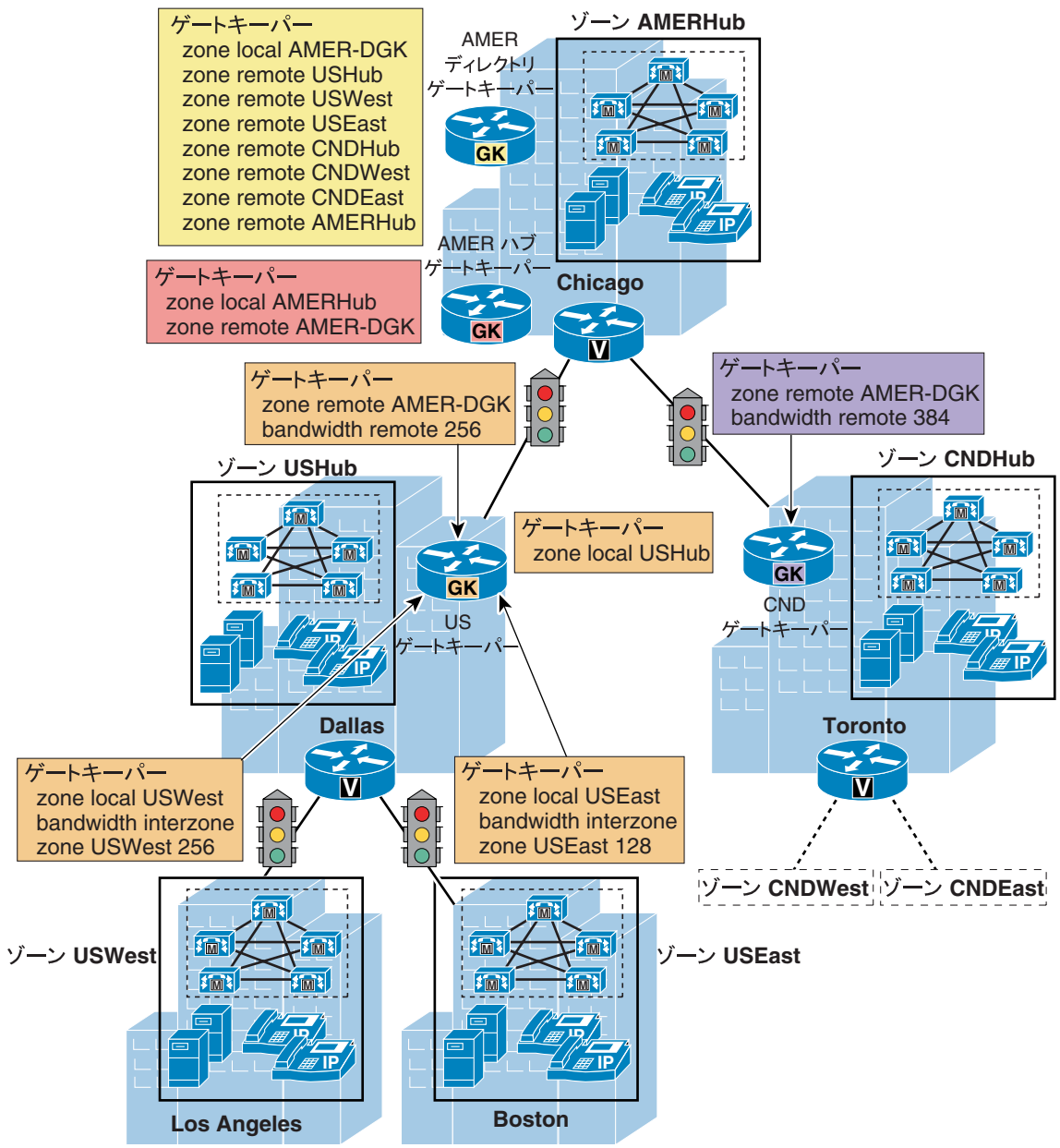


図 9-16 の例には、次の設計上の推奨事項が適用されます。

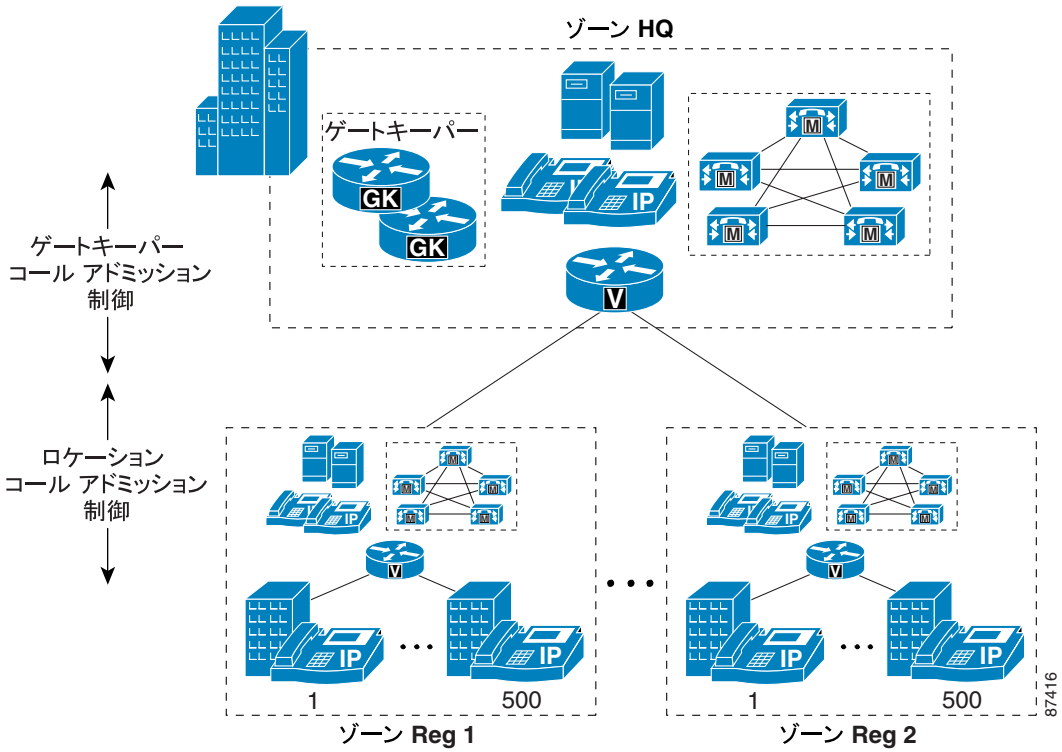
- 第 2 層ハブ サイトにあるゲートキーパー上で、第 2 層ハブ サイト自体のローカル ゾーンとともに、各スポーク サイトのローカル ゾーンも定義します。スポーク サイトと第 2 層ハブ サイトの間にあるリンクに対してコール アドミッション制御を実行するには、このゲートキーパー上で **bandwidth interzone** コマンドを使用します。この例では、Dallas にある US ゲートキーパーに 3 つのローカル ゾーンが設定されています。Dallas サイトの USHub、Los Angeles サイトの USWest、Boston サイトの USEast です。**bandwidth interzone** コマンドは、スポーク サイト（USWest と USEast）に割り当てられているゾーンに適用されます。
- 第 2 層ハブ サイトにあるゲートキーパー上で、第 1 層ハブ サイトにあるディレクトリ ゲートキーパーを指すリモート ゾーンを定義します。コール ルーティングは、ローカル ゾーンで処理できないすべてのコールがこのリモート ゾーンに送信されるように設定します。第 1 層ハブ サイトに向かうリンクに対してコール アドミッション制御を実行するには、各第 2 層ハブ サイトのゲートキーパー上で、**bandwidth remote** コマンドを使用します。この例では、Dallas にある US ゲートキーパー上に、ディレクトリ ゲートキーパー（AMER-DGK）に接続するためのリモート ゾーンが設定されています。このゲートキーパーでは、**bandwidth remote** コマンドを使用して、Chicago に向かうリンクで使用される帯域幅の量を制限しています。
- 第 1 層ハブ サイトにあるゲートキーパー上で、同じ場所にある Cisco CallManager クラスタのローカル ゾーンを定義し、同じ場所にあるディレクトリ ゲートキーパーのリモート ゾーンを定義します。このゲートキーパー上では、コール アドミッション制御は必要ありません。
- 第 1 層ハブ サイトにあるディレクトリ ゲートキーパー上で、ディレクトリ ゲートキーパー自体のローカル ゾーンを定義し、各 Cisco CallManager クラスタ（つまり、このトポロジに含まれている各サイト）のリモート ゾーンを定義します。コール ルーティングは、コールが着信番号に従って適切なゲートキーパーに送信されるように設定します。

（注） この配置モデルでは、**bandwidth remote** コマンドを使用できます。第 2 層ハブ サイトの各ゲートキーパーで、トポロジの性質上、宛先がいずれかのローカル ゾーンではないコールは、すべて第 1 層ハブ サイトに向かうリンクを通過することが保証されるためです。第 2 層ハブ サイト間にピアツーピアのリンクがある場合では、第 1 層ハブ サイトに向かうリンクと同様に、それらのリンク上の帯域幅を制御することはできません。これは、**bandwidth remote** コマンドは 1 つの帯域幅値しか受け付けないためです。

集中型および分散型複合配置

2 層ハブアンドスポーク トポロジを採用していて、第 1 層ハブ サイトと第 2 層ハブ サイトに Cisco CallManager がある配置にコール アドミッション制御を提供するには、図 9-17 に示されているようにロケーションとゲートキーパー メカニズムを組み合せて対応します。

図 9-17　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



H.323 トランクをロケーションと組み合せてコール アドミッション制御を実行する場合は、次の推奨事項に従ってください。

- ローカル Cisco CallManager を使用していないサイト（つまり、スポーク サイト）には、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します。
- Cisco CallManager クラスタ間（つまり、第 1 層ハブ サイトと第 2 層ハブ サイト間）には、ゲートキーパー ベースのコール アドミッション制御を使用します。
- ローカル Cisco CallManager を使用していない各サイトには、そのサイトをサポートしている Cisco CallManager クラスタ内にロケーションを設定します。
- 各サイトの帯域幅の上限を、そのサイトに使用されているコーデックのタイプに応じて、適切に設定します（帯域幅の設定については、表 9-1 と表 9-2 を参照してください）。
- Cisco CallManager に設定された各デバイスをロケーションに割り当てます。あるデバイスを別のロケーションに移した場合、ロケーションの設定も変更します。
- Cisco CallManager は、ロケーションを 500 個所までサポートします。
- 各 Cisco CallManager クラスタは、ゲートキーパー制御の H.323 トランクをゲートキーパーに登録します。
- ゾーン間の帯域幅を設定して、クラスタ間のコールの数を制御します。

例 9-5 では、一般的なゲートキーパーの設定を示しています。

例 9-5　ロケーションを使用するゲートキーパー制御クラスタ間トランクに対する一般的なゲートキーパー設定

```
gatekeeper
 zone local GK-HQ customer.com 10.1.10.100
 zone local GK-Reg1  customer.com
 zone local GK-Reg2 customer.com
 zone prefix GK-HQ 408*
 zone prefix GK-Reg1 718*
 zone prefix GK-Reg1 212*
 zone prefix GK-Reg2 818*
 zone prefix GK-Reg2 602
 bandwidth interzone GK-HQ 768
 bandwidth interzone GK-Reg1 768
 bandwidth interzone GK-Reg2 768
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 9-5 について説明します。

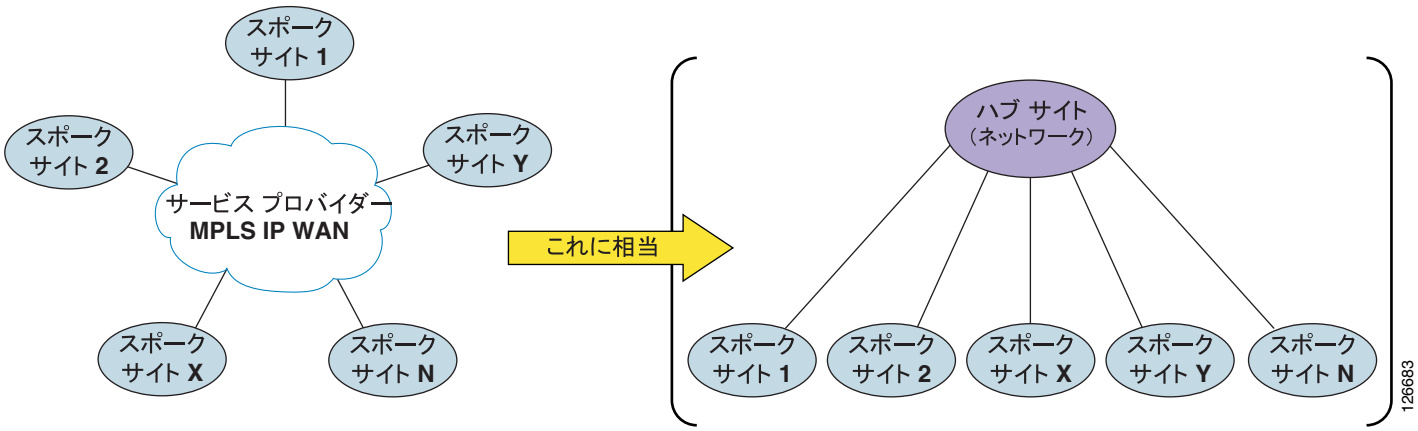
- **zone local** コマンドを使用して、ゲートキーパー ゾーンを作成しています。各 Cisco CallManager は、ゲートキーパー制御のクラスタ間トランクをその設定済みゾーンに登録しています。
- ゾーン間のコール ルーティングには、**zone prefix** が使用されています。必要な場合は、同一ゾーンに対して複数のゾーン プレフィックスを設定します。
- **bandwidth interzone** コマンドは、ゾーン間で利用できる帯域幅の量を割り当てます。
- **gw-type-prefix 1# default technology** コマンドは、ゾーン内で解決されないコールを登録済みテクノロジー プレフィックス 1# を持つデバイスにルーティングします。この設定例では、Cisco CallManager トランクが該当します。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco CallManager トランク上にできるコール ルーティング ループを回避します。

MPLS ベースのトポロジ

図 9-18 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 9-18　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



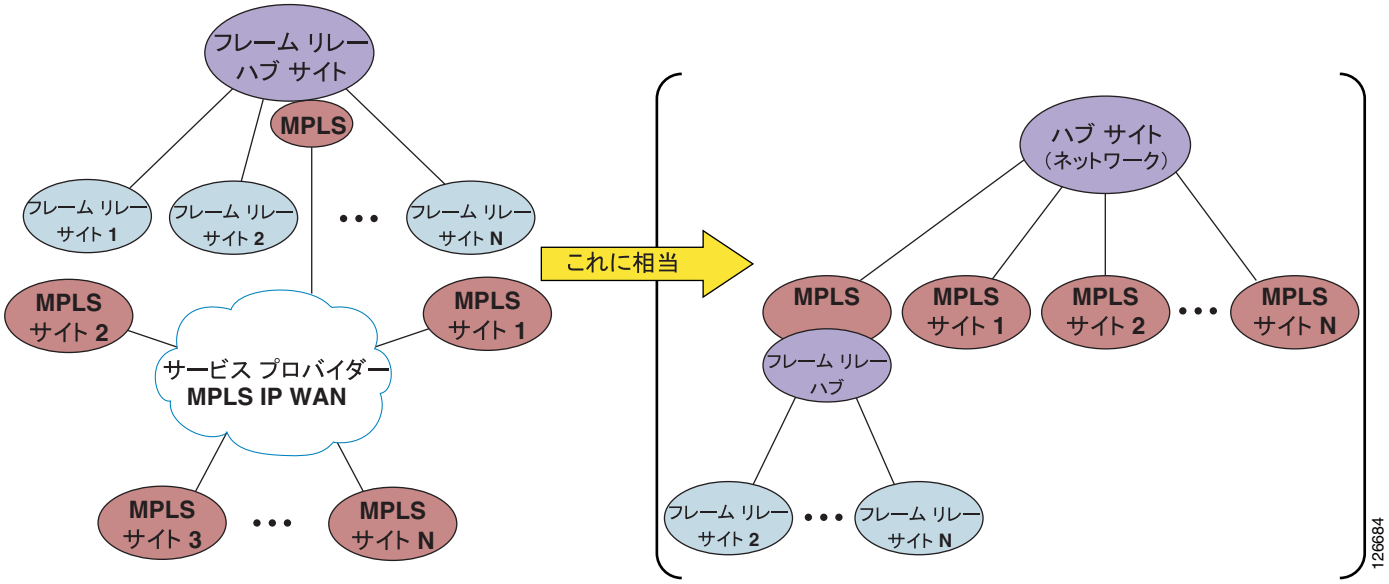
これまでに検討した内容に基づくと、コール アドミッション制御という観点から見たとき、MPLS に基づくサービス プロバイダー IP WAN サービスは、実質的には、ハブ サイトのないハブアンドスポーク トポロジに相当することが簡単にわかります（図 9-18 を参照）。事実上、ネットワーク自体をハブ サイトと見なすことができます。企業サイトは、いずれも（本社、つまり中央サイトを含めて）スポーク サイトに相当します。このように見方を変えると、コール アドミッション制御の実行方法も異なってきます。この方法については、以降で説明します。

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 9-19 に示すように、従来のレイヤ 2 テクノロジー（フレーム リレーなど）ベースのハブアンドスポーク IP WAN を MPLS ベースの IP WAN と統合すると、ネットワーク トポロジは単純なハブアンドスポークやフルメッシュではなく、2 層ハブアンドスポークになります。

この場合、MPLS ネットワークが第 1 層ハブ サイトを表し、MPLS 対応のフレーム リレー ハブ サイト、および MPLS ベースのサイトが第 2 層ハブ サイトを表し、フレーム リレー スポーク サイトがスポーク サイトを表します。したがって、このような配置での設計上の考慮事項については、P.9-27 の「2 層ハブアンドスポーク トポロジ」の項を参照してください。

図 9-19　MPLS サイトとフレーム リレー サイトの共存、およびこれに相当するトポロジ



以降では、採用する Cisco CallManager 配置モデルごとに、MPLS ベースのトポロジに関する設計上のベスト プラクティスを示します。

- 単純集中型配置（P.9-37）

  1 つのサイトに Cisco CallManager クラスタを 1 つのみ配置し、それ以外のすべてのサイトには、電話とゲートウェイのみを配置します。
- 単純分散型配置（P.9-39）

  Cisco CallManager クラスタを各サイトに配置します。
- 集中型および分散型複合配置（P.9-40）

  Cisco CallManager クラスタを一部のサイトに配置し、それ以外のサイトには、電話とゲートウェイのみを配置します。

（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 ネットワークを企業が独自に配置している場合は、ある 2 つの条件のうちいずれかを満たしていると、実質的にコール アドミッション制御を実行できます。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。

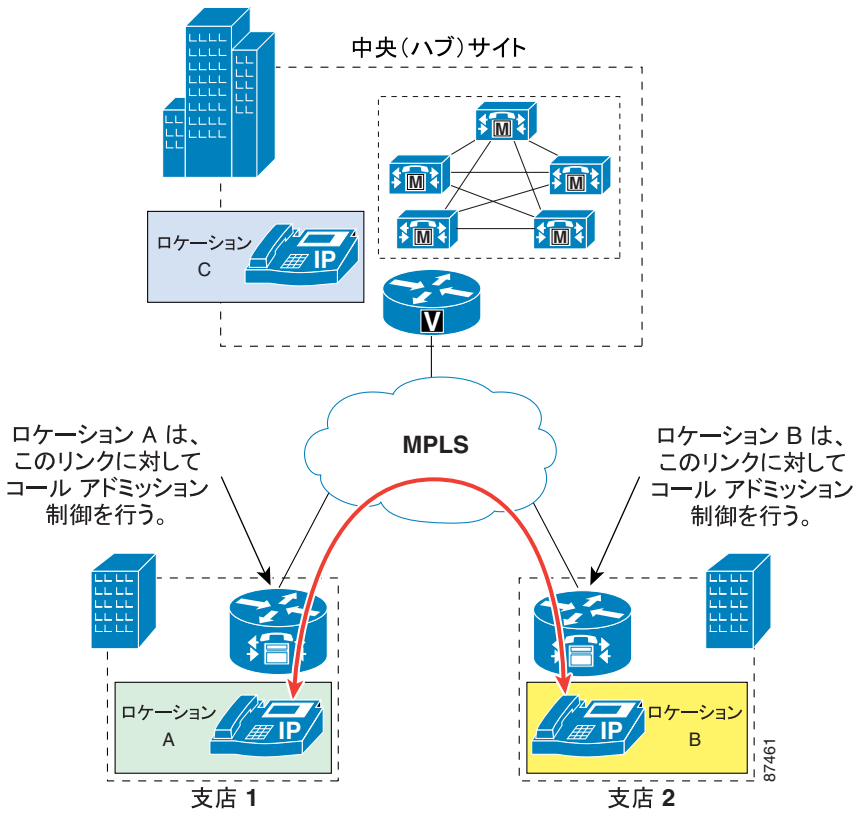
単純集中型配置

単一クラスタ集中コール処理配置では、コール アドミッション制御機能は Cisco CallManager 内のロケーション構成により実行されます。

ハブアンドスポーク WAN トポロジ（フレーム リレー、ATM など）では、支店サイトとのリンクはすべて、中央サイトで終端します。フレーム リレーを例にすると、支店ルータからのすべての PVC（Permanent Virtual Circuits; 相手先固定接続）は、中央サイトのヘッドエンド ルータに集約されています。この例では、帯域幅に対する課金は WAN リンクの支店エンドで行われているので、中央サイドではデバイスにコール アドミッション制御を適用する必要はありません。したがって、Cisco CallManager ロケーションの設定では中央サイトのデバイスのロケーションは <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。

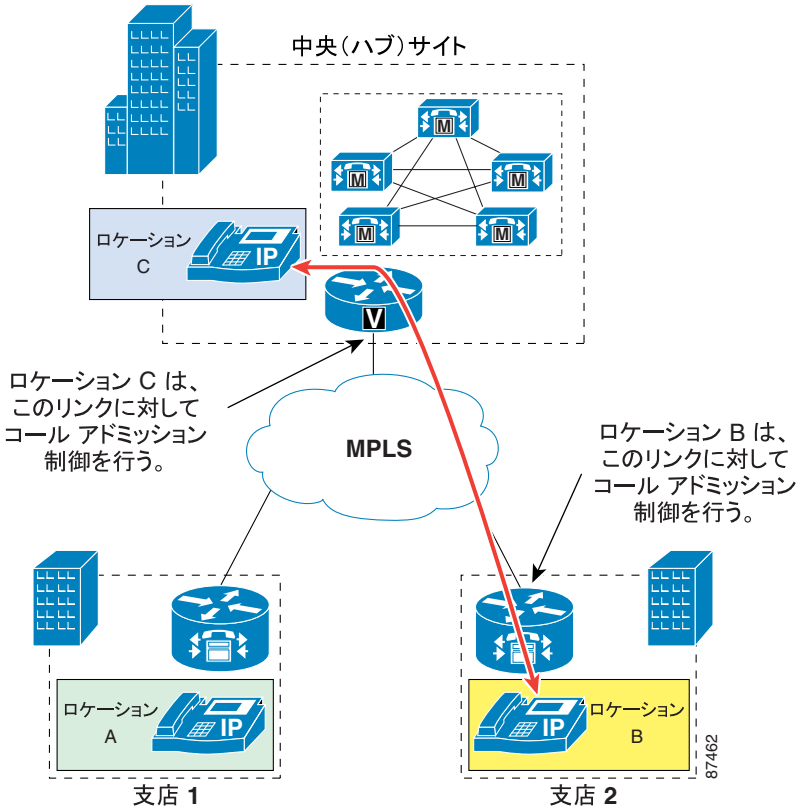
MPLS WAN ネットワークでは、すべての支店はレイヤ 3 で隣接していると見なされるため、中央サイトに接続する必要はありません。図 9-20 では、スポークツースポーク配置による 2 つの支店間のコールを説明しています。

図 9-20　MPLS 配置におけるスポークツースポーク コール



また、MPLS WAN では、中央サイト WAN に接続しているリンクは支店の WAN リンクに集約していません。中央サイトに存在するすべてのデバイスは、個々のデバイスに対応するコール アドミッション制御ロケーション（したがって、<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 9-21 を参照）。

図 9-21　MPLS 配置におけるハブとのコール

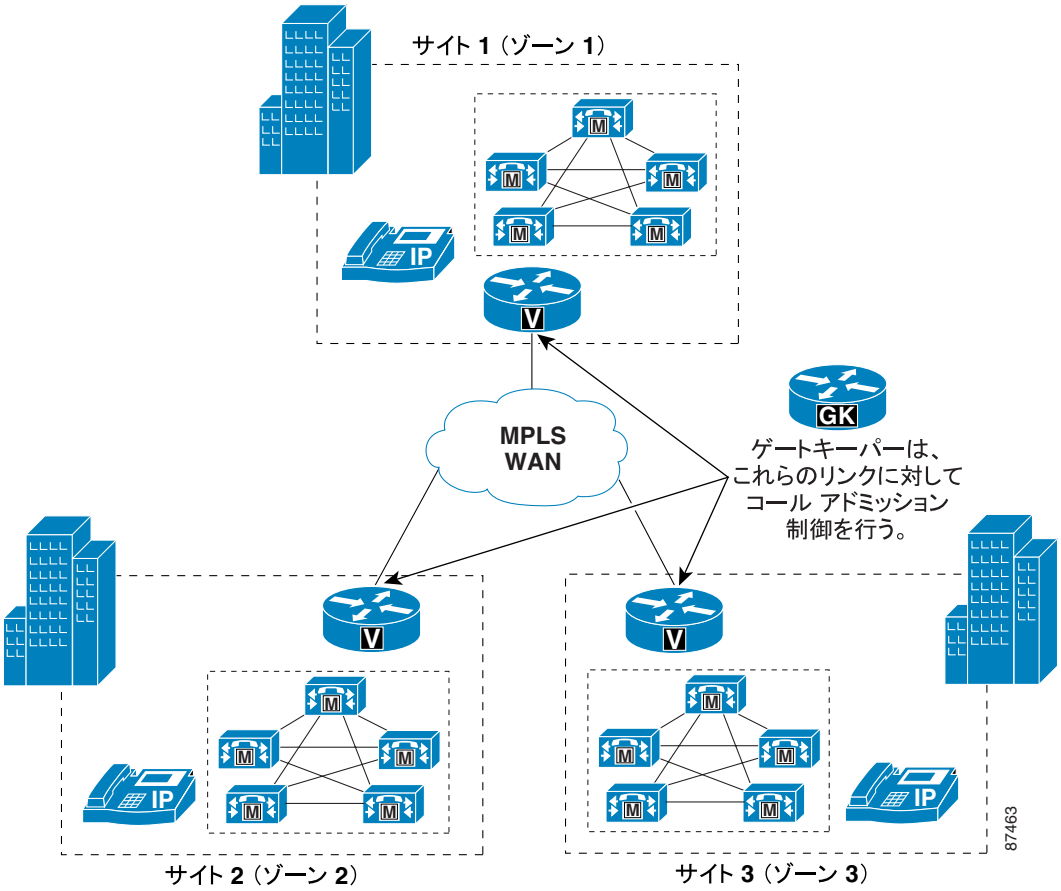


特定サイトに許されている帯域幅がすべて消費されてしまっている場合は、Cisco CallManager が備えている Automated Alternate Routing（AAR）機能を使用して、公衆網へ自動的にフェールオーバーさせることができます。AAR の詳細については、P.10-20 の「Automated Alternate Routing」を参照してください。

単純分散型配置

各サイトに Cisco CallManager クラスタが設定されていて、どのサイト間も MPLS WAN でリンクされているマルチ サイト配置の場合は、ゲートキーパーがサイト間のコール 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 9-22 を参照）。

図 9-22　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

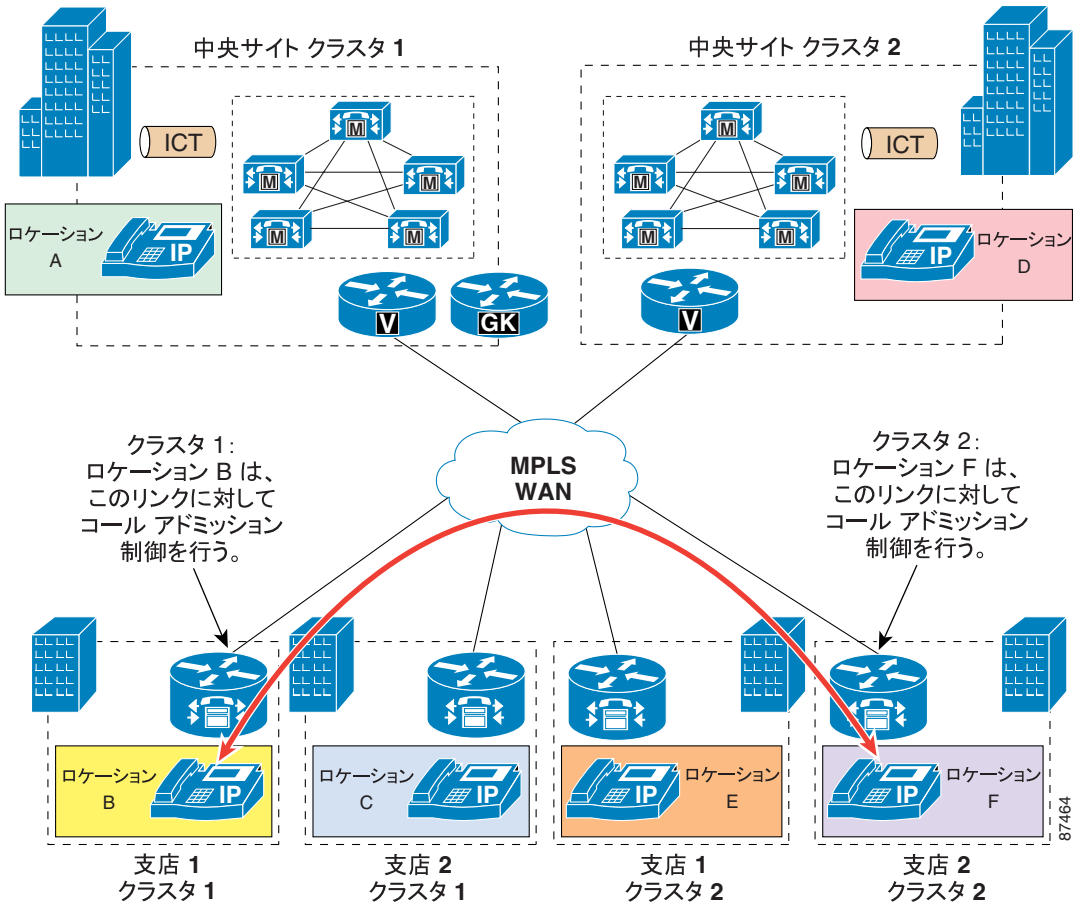


特定サイトに許されている帯域幅がすべて消費されてしまっている場合は、各クラスタからゲートキーパーへ接続する際のルート パターンが指定されているルート リストおよびルート グループを使用して、公衆網へ自動的にフェールオーバーさせることができます。

集中型および分散型複合配置

集中型および分散型コール処理を複合的に配置しているマルチ サイト モデルでは、MPLS WAN はクラスタ間のコールに対して新しい展開を意味します。異なるクラスタに属している支店間にコールが発生した場合は、音声パスはその支店間で直接確立できるので、支店のクラスタから中央サイトへメディアを転送する必要はありません。したがって、コール アドミッション制御は各支店の WAN リンクに必要なだけです（図 9-23 を参照）。

図 9-23　クラスタ間トランク（ICT）によるマルチ クラスタ接続



単純集中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、<None> のままにしておきます。

この方式の配置では、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。

特定のサイトに許されている帯域幅を消費してしまっている場合は、次の 2 つの方式を組み合せて、公衆網へ自動的にフェールオーバーすることができます。

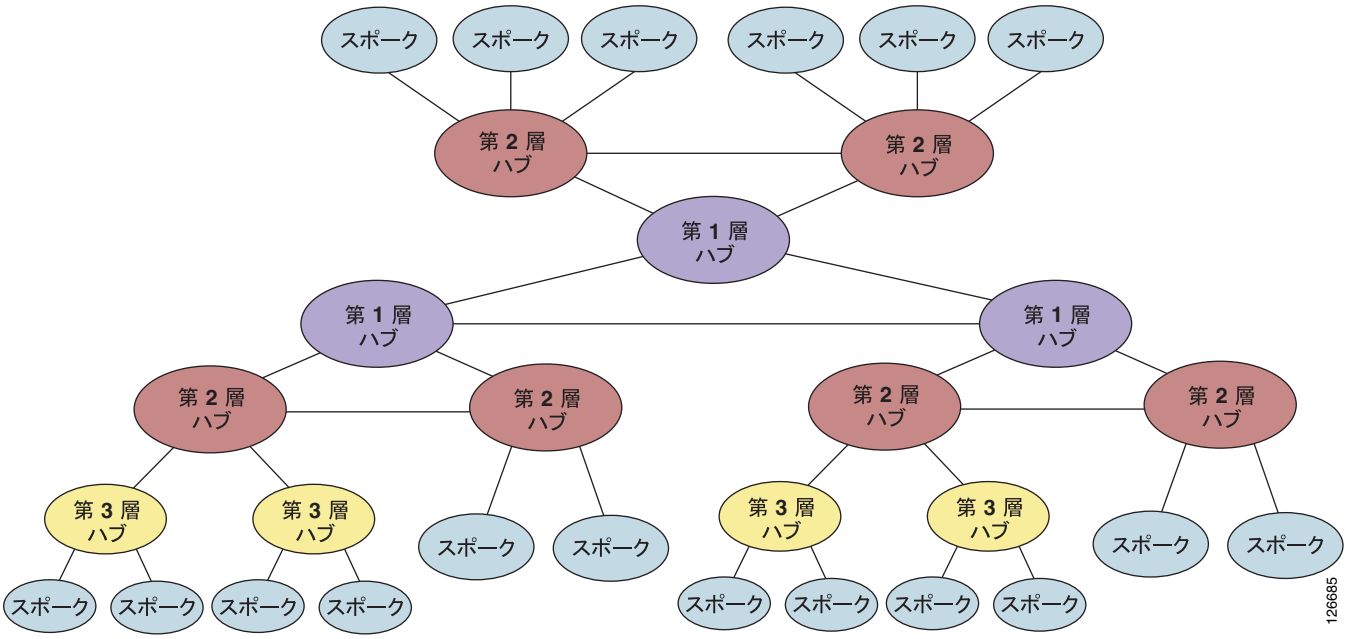
- マルチ Cisco CallManager クラスタに対するコールには、ルート リストおよびルート グループで対応
- Cisco CallManager クラスタ内のコールには、Automated Alternate Routing（AAR）機能で対応（AAR の詳細については、P.10-20 の「Automated Alternate Routing」を参照）

複合トポロジ

このドキュメントにおける「複合トポロジ」とは、この章でこれまでに説明した、どのトポロジ タイプにも単純化できないネットワーク トポロジです。

図 9-24 の例に示すように、複合ネットワーク 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。

図 9-24　複合トポロジの例



一般的に言うと、あらゆるトポロジをサポートできる唯一のコール アドミッション制御メカニズムは、RSVP です。RSVP は、ネットワーク トポロジとは完全に独立した、動的な分散型シグナリング プロトコルです。このため、ハブアンドスポークへと論理的に単純化できないトポロジで利用するのに最適です。

RSVP ベースのコール アドミッション制御サポートを Cisco IP Communications ネットワークに追加するには、P.9-15 の「IP-to-IP ゲートウェイ」の項で説明しているように、中継ゾーン ゲートキーパーと Cisco IP-to-IP ゲートウェイを使用します。

ただし、IP-IP ゲートウェイ機能を大規模ネットワークのすべてのサイトに追加することは、不可能な場合もあります。（ネットワーク接続を変更するか、使用可能な帯域幅に基づいて仮定することで）ネットワークの特定の部分をハブアンドスポーク トポロジへと単純化できる場合には、Cisco CallManager ロケーションや Cisco IOS ゲートキーパーなどの「静的な」コール アドミッション制御メカニズムを、RSVP の提供する動的なコール アドミッション制御と同一ネットワーク内で組み合せることができます。

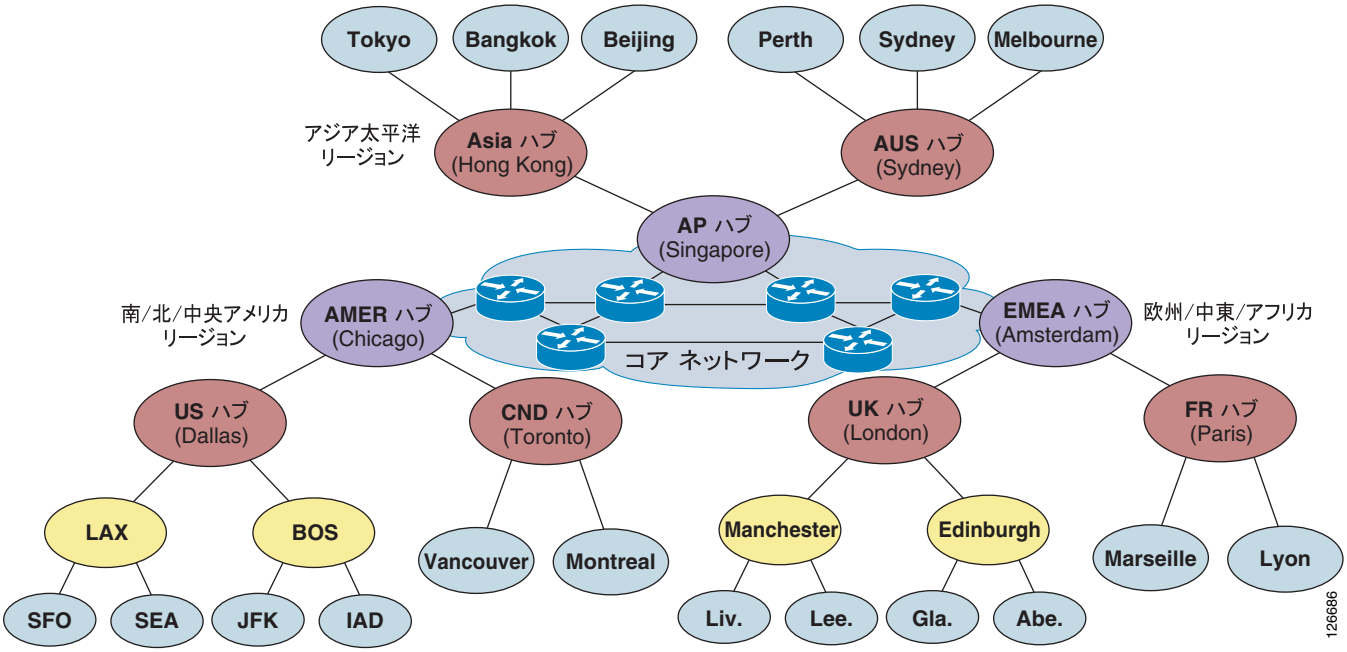
以降では、ハブアンドスポークへと単純化できない架空の大規模顧客ネットワークに基づいて、詳細なケース スタディを示します。この例では、次のコール アドミッション制御メカニズムを組み合せて、エンドツーエンドのソリューションを提供します。

- Cisco CallManager ロケーション
- Cisco IOS ゲートキーパー
- RSVP（Cisco IP-to-IP ゲートウェイを使用）

ケース スタディ

図 9-25 では、架空の大規模顧客ネットワークの概略的なトポロジを示しています。この顧客サイトは、3 つの主要リージョンに分かれています。南 / 北 / 中央アメリカ（AMER）、欧州 / 中東 / アフリカ（EMEA）、およびアジア太平洋（AP）です。これらの各リージョンの内部では、ネットワーク トポロジは 3 層のハブアンドスポークです。リージョン ハブといくつかの国ハブがあり、それぞれは 1 つまたは 2 つの小さな下位サイトを保持していることがあります。コア ネットワークによって、3 つのリージョンが任意のネットワーク トポロジで相互接続され、どの 2 つの宛先間にも、等コストのパスが複数用意されています。

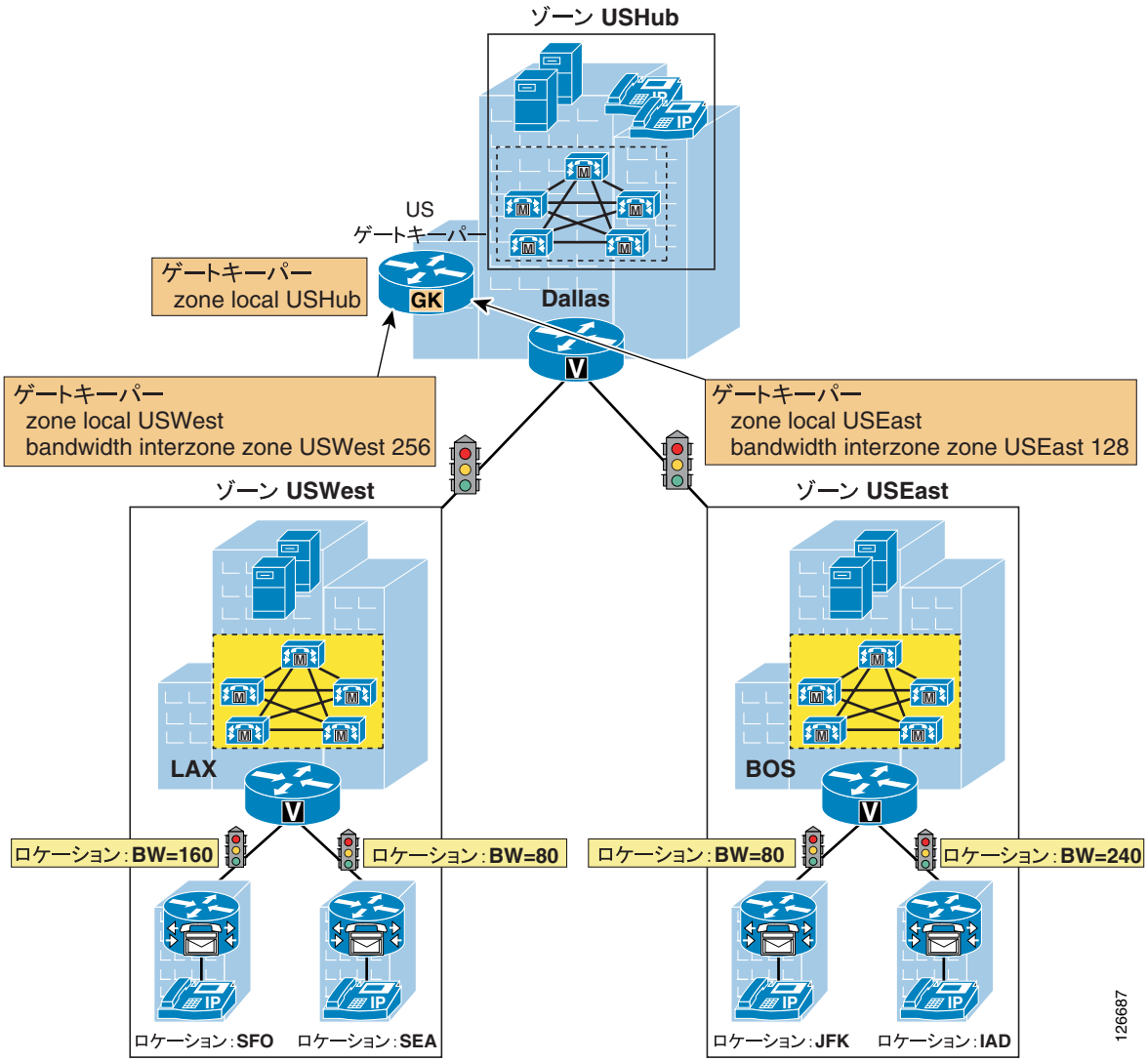
図 9-25　架空の顧客ネットワーク



この複合トポロジは、各種のコール アドミッション制御メカニズムをどこに適用するか、およびどのように組み合せるかを示しています。ソリューション全体をわかりやすく説明するために、ここではネットワークの各部分を個別に分析していきます。

まず、AMER リージョンについて検討します。図 9-25 に示すように、リージョン ハブに接続されている 2 つの国ハブがあります。Dallas にある US ハブ サイトと、Toronto にある CND ハブ サイトです。図 9-26 では、ネットワークの US 部分にコール アドミッション制御を実装する方法を示しています。

図 9-26　顧客ネットワークの最初の 2 レベルに対するコール アドミッション制御（米国）



Cisco IOS ゲートキーパーが、Dallas の US ハブ サイトに配置されています。このハブ サイトには、数多くの第 1 レベル スポーク サイト（ゲートキーパーごとに 100 まで）を接続できます。図 9-26 の例では、第 1 レベル スポーク サイトは Los Angeles（LAX）と Boston（BOS）です。各サイトのローカル ゾーン（この例では、USHub、USWest、USEast）をゲートキーパー内に定義すると、第 1 レベル スポーク サイトと US ハブ サイトの間にあるリンクに対してコール アドミッション制御を実行できます。このためには、Cisco IOS ゲートキーパー コマンドの **bandwidth interzone zone** *zone-name bandwidth-value* を使用します。このコマンドによって、各ゾーンで発着信される音声コールとビデオ コールの使用する帯域幅が、設定した値を超えないことが保証されます。

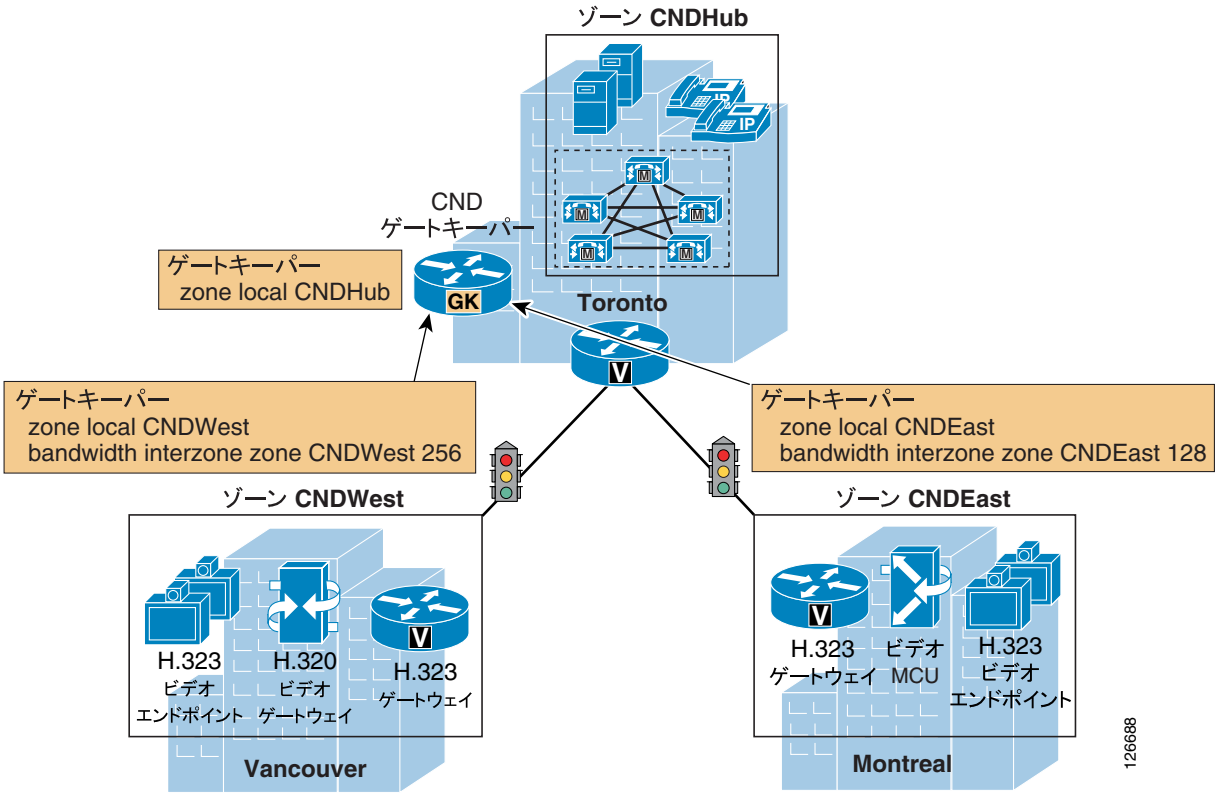
この図にある第 1 レベル スポーク サイト（LAX と BOS）は、それぞれ Cisco CallManager クラスタをホストしています。Cisco CallManager は、独自にコール アドミッション制御メカニズム（ロケーション制御による）を使用しているため、数多くの第 2 レベル スポーク サイト（クラスタごとに 500 まで）をそれぞれの第 1 レベル スポーク サイトに追加することができます。この例では、各 Cisco CallManager クラスタがそれぞれ 2 つの追加サイトを制御しています。Los Angeles クラスタの San Francisco（SFO）と Seattle（SEA）、Boston クラスタの New York（JFK）と Washington D.C.（IAD）です。したがって、これらの第 2 レベル スポーク サイトとそれぞれの第 1 レベル サイト間にあるリンクの帯域幅は、Cisco CallManager ロケーションによって制御されます。

(注)

ゲートキーパーに関しては、第 2 レベル スポーク サイトは「親」である第 1 レベル スポーク サイトと同じ Cisco CallManager クラスタによって制御されるため、第 1 レベル スポーク サイトと同じゾーンに属するものと見なされます。Cisco CallManager によって制御されないオンネット宛先に向かうコールが、いずれかの第 2 レベル スポーク サイトから発信された場合、そのコールは、「親」である第 1 レベル スポーク サイトと国ハブ サイト間にあるリンクを経由する必要があるため、この分析は適切です。

図 9-27 では、カナダ（CND）サイトを示しています。このサイトは、ネットワークのこのレベルにコール アドミッション制御を実装する方法のもう 1 つの例です。

図 9-27　顧客ネットワークの第 1 レベルに対するコール アドミッション制御（カナダ）



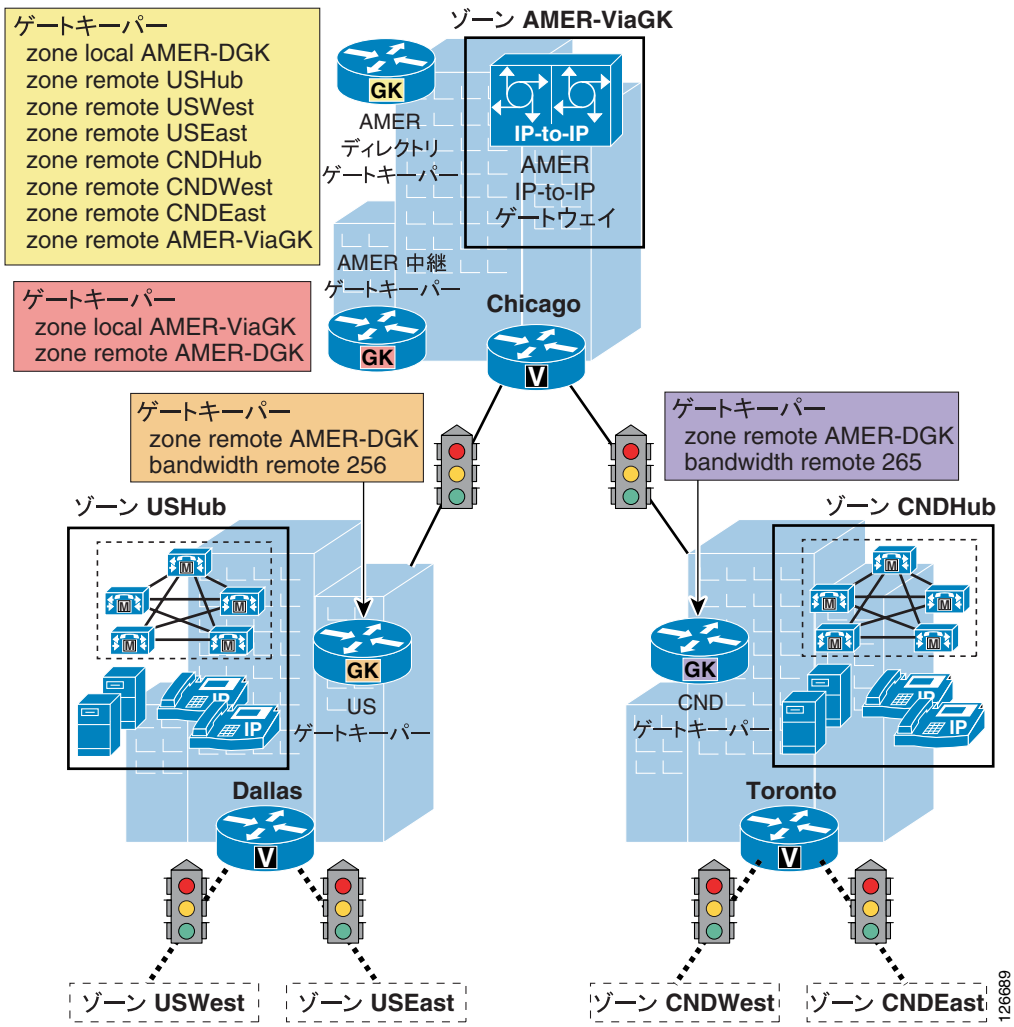
Toronto にあるカナダ ハブ サイトには、もう 1 つの Cisco IOS ゲートキーパーが配置され、多数のスポーク サイトがこのハブ サイトに接続されています。この例では、2 つのスポーク サイトが Vancouver と Montreal にあります。これらのスポーク サイトには、Cisco CallManager クラスタは含まれていませんが、音声ゲートウェイ、ビデオ エンドポイント、マルチポイント コントロール ユニット（MCU）、H.320 ビデオ ゲートウェイなど、H.323 ベースのさまざまなデバイスが含まれています。サイトごとに、ゲートキーパー内にローカル ゾーンが定義されています（この例では、CNDHub、CNDWest、CNDEast）。カナダ ハブ サイトとスポーク サイトの間にあるリンクの帯域幅も、Cisco IOS のゲートキーパー コマンド **bandwidth interzone zone** *zone-name bandwidth-value* を使用して制御することができます。このコマンドによって、各ゾーンで発着信される音声コールとビデオ コールの使用する帯域幅が、設定した値を超えないことが保証されます。

スポーク サイトにある H.323 デバイスは、コール アドミッション制御を実行できません。したがって、ここに第 2 レベルのスポーク サイトを追加することはできません。ただし、これらのどのデバイスも Cisco CallManager で制御できるため、Cisco CallManager クラスタを第 1 レベル スポーク サイトに追加して、これらの H.323 デバイスを複数の第 2 レベル スポーク サイトに分散させることは可能です。

また、同じゲートキーパーの制御する複数のサイト内で、Cisco CallManager スポーク サイトと H.323 スポーク サイトを混在させることはできます。

ここで、ネットワーク階層の 1 つ上のレベルについて考えます。図 9-28 では、Chicago にある AMER リージョン ハブ サイトと、Dallas および Toronto にある 2 つの国ハブ サイト（米国とカナダ）の間でそれぞれ使用されているコール アドミッション制御メカニズムを示しています。

図 9-28　顧客ネットワークの第 2 レベル（リージョン ハブ）に対するコール アドミッション制御



ネットワークのこの部分もハブアンドスポークですが、ここでは、コール アドミッション制御の実行に使用されるアプローチが、国ハブ サイトと第 1 レベル スポーク サイト間で使用されるものとは異なります。

これまでに説明したように、国ハブ サイトには Cisco IOS ゲートキーパーが含まれています。このゲートキーパーが、ローカル ゲートキーパー ゾーンと **bandwidth interzone** Cisco IOS コマンドを使用して、第 1 レベル スポーク サイトに向かう帯域幅を制御しています。AMER リージョン ハブ サイトには、ディレクトリ ゲートキーパーとして使用されるゲートキーパーが含まれています。このゲートキーパーの主な目的は、国ゲートキーパー間のコール ルーティングを処理することです。

国ハブ サイトとリージョン ハブ サイトの間にあるリンクの帯域幅使用を制御するには、国ハブ サイトにある 2 つのゲートキーパー上で、**bandwidth remote** *bandwidth-value* Cisco IOS コマンドを使用します。このコマンドによって、すべてのローカル ゾーンとすべての非ローカル ゾーン間で発着信される音声コールとビデオ コールの使用する帯域幅が、設定した値を超えないことが保証されます。ローカル ゾーンに属していない宛先へのコールは、すべて国ハブ サイトとリージョン ハブ サイトの間にあるリンクを通過する必要があります。このため、**bandwidth remote** コマンドを使用することで、実質上このリンクに対してコール アドミッション制御を実行できます。

図 9-28 で、AMER リージョン ハブ サイトに中継ゾーン ゲートキーパーがあることにも注目してください。他のリージョン（AP や EMEA など）内の宛先へのコールを AMER 中継ゾーン ゲートキーパーにルーティングするために、ディレクトリ ゲートキーパーが設定されています（この設定は、図 9-28 には示していません）。

次に、ネットワークのコア セクションについて考えます。このセクションは、3 つのリージョン ハブ サイトを接続しています。図 9-29 と図 9-30 では、コール ルーティングとコール アドミッション制御がコア ネットワークにわたってどのように実行されるかを示しています。

図 9-29　中継ゾーン ゲートキーパーを使用した顧客ネットワークのコア部分でのコール ルーティング

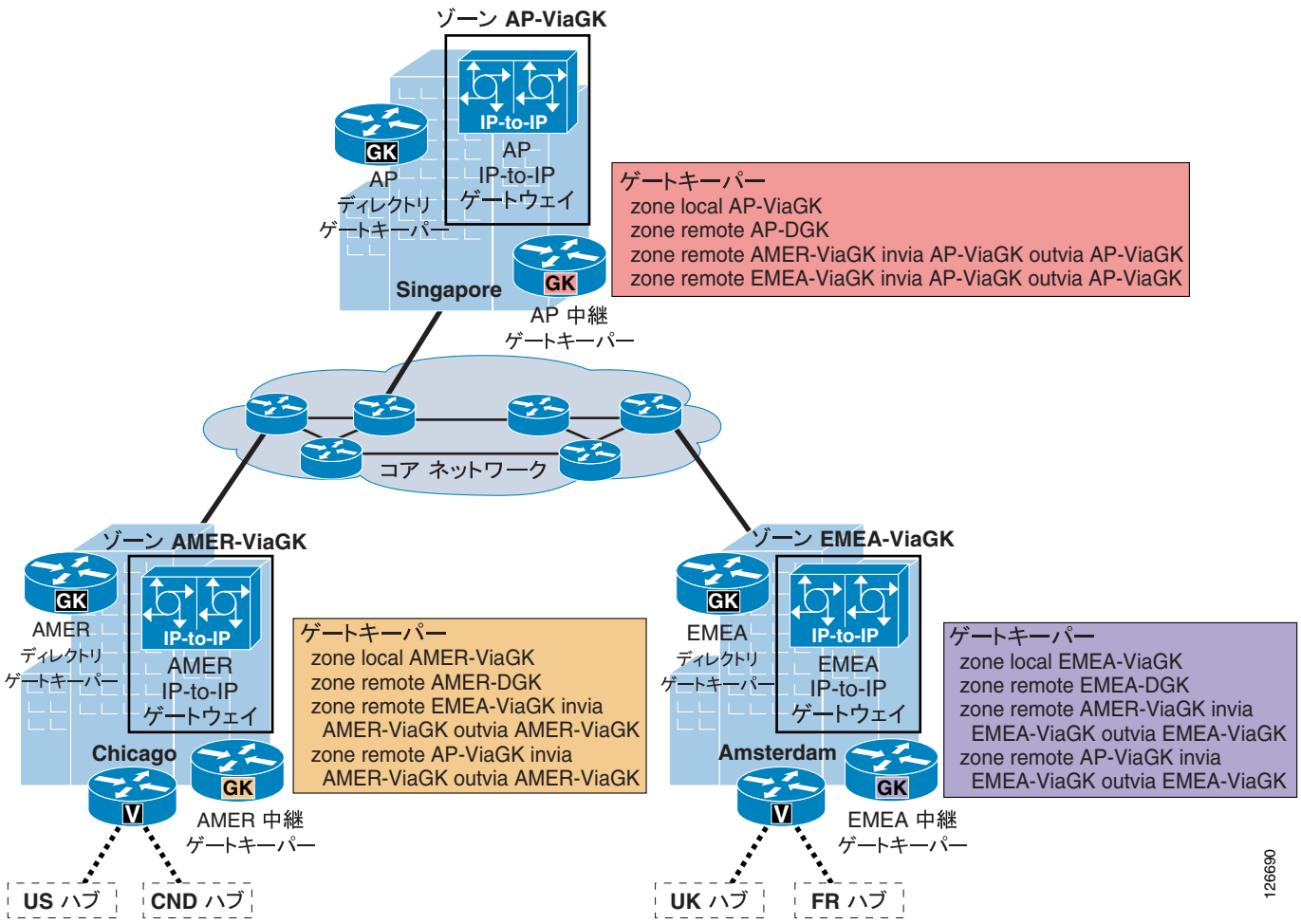


図 9-29 では、3 つのリージョン ハブ サイトそれぞれにある 3 つの中継ゾーン ゲートキーパーの設定の抜粋を示しています。各リージョンの中継ゾーン ゲートキーパーは、他の 2 つのリージョンが宛先または発信元となるコールが発生すると、コールに IP-to-IP ゲートウェイを挿入するように設定されています。

たとえば、AMER リージョンの中継ゾーン ゲートキーパーの設定では、次のゾーンが定義されています。

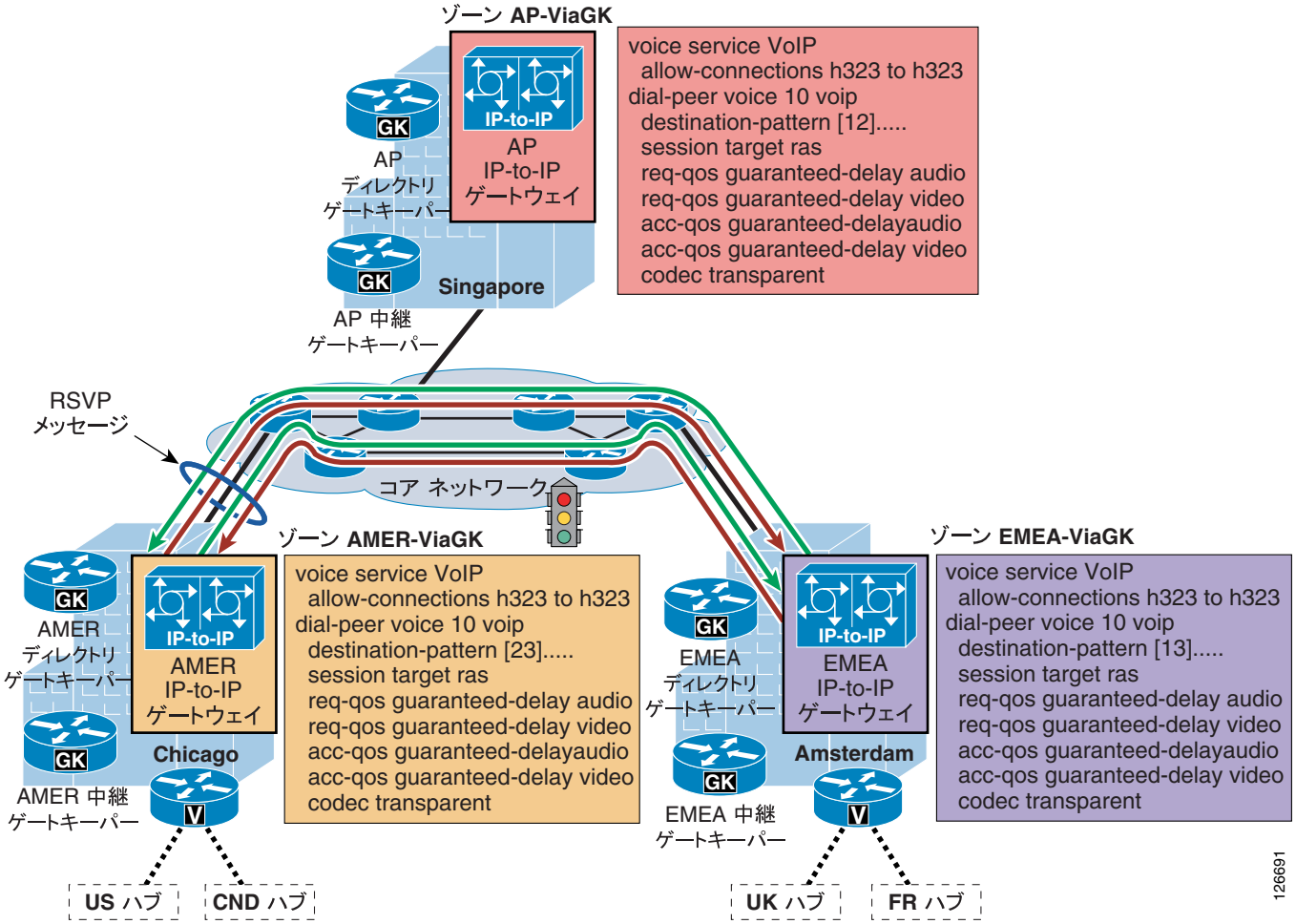
- 1 つのローカル ゾーン（AMER-ViaGK）
- AMER ディレクトリ ゲートキーパーに（つまり、AMER リージョン内のすべての宛先に）到達するためのリモート ゾーン AMER-DGK
- EMEA リージョン内の宛先に到達するためのリモート ゾーン EMEA-DGK
- AP リージョン内の宛先に到達するためのリモート ゾーン AP-DGK

EMEA-DGK リモート ゾーンと AP-DGK リモート ゾーンの定義では、ローカル ゾーン AMER-ViaGK が、これらの宛先に到達するための **invia** ゾーンおよび **outvia** ゾーンとして使用されることも指定しています。つまり、これらのリモート ゾーンが宛先または発信元となるコールが発生すると、AMER 中継ゾーン ゲートキーパーがコールに IP-to-IP ゲートウェイを挿入します。ローカル ゾーン AMER-ViaGK のゲートキーパーに登録されているすべての IP-to-IP ゲートウェイ リソースの中から、特定の IP-to-IP ゲートウェイ リソースが選択されます。

（注） IP-to-IP ゲートウェイをコールに挿入すると、コールは実質上 2 つのコール レッグに分割されます。この例では、IP-to-IP ゲートウェイが各リージョン ハブ サイトに挿入されるため、AMER リージョンのエンドポイントと EMEA リージョンのエンドポイント間のコールは、3 つのコール レッグで構成されることになります。最初のレッグは AMER エンドポイントから AMER IP-to-IP ゲートウェイまで、2 番目のレッグは AMER IP-to-IP ゲートウェイから EMEA IP-to-IP ゲートウェイの間、3 番目のレッグは EMEA IP-to-IP ゲートウェイと EMEA エンドポイントの間です。

図 9-30 では、コア ネットワークで使用されるコール アドミッション制御メカニズムを示しています。

図 9-30　顧客ネットワークのコア部分にわたる RSVP ベース コール アドミッション制御



コールがコア ネットワークを通過する必要がある場合は、中継ゾーン ゲートキーパーによって、コール フローに IP-to-IP ゲートウェイが挿入されます。各 IP-to-IP ゲートウェイも、コールのルーティングに中継ゾーン ゲートキーパーを使用し、コア ネットワークにわたって自身が発信または終端するコールに RSVP コール アドミッション制御を使用するように設定されています。RSVP 予約は単方向であるため、音声コールごとに、それぞれの方向に 1 つずつ、2 つの RSVP 予約が生成されます。

図 9-30 では、AMER IP-to-IP ゲートウェイと EMEA IP-to-IP ゲートウェイ間のコールを示しています。コア ネットワークの 2 つのリージョン ハブの間には、複数のパスがあるものとします。取得したルートが非対称である場合は、2 つの RSVP 予約がそれぞれ別のパスに沿って流れていきます。ただし、個々の予約に注目すると、RSVP メッセージは常に同じパスに沿って流れます。これは、RSVP ではリバース ホップバイホップ ルーティングを使用して予約を確立しているためです。RSVP によって、コア ネットワークで音声コールとビデオ コールの使用する帯域幅が、各ルータ インターフェイス上で設定されている値を超えないことが保証されます。

要約すると、エンドツーエンドのコール アドミッション制御は、ネットワークの各部分でそれぞれ別の手法を組み合せて達成されています。

図 9-25 に示したネットワークについて説明すると、たとえば、米国の San Francisco と英国の Liverpool にある 2 つの IP Phone 間のコールでは、次のメカニズムが使用されます。

- San Francisco と Los Angeles 間にあるリンクでは、Cisco CallManager ロケーション
- Los Angeles と Dallas 間にあるリンクでは、Cisco IOS ゲートキーパーの **bandwidth inter-zone** コマンド
- Dallas と Chicago 間にあるリンクでは、Cisco IOS ゲートキーパーの **bandwidth remote** コマンド
- Chicago と Amsterdam（2 つのリージョン ハブ サイト）間では、RSVP
- Amsterdam と London（英国の国ハブ サイト）間では、Cisco IOS ゲートキーパーの **bandwidth remote** コマンド
- London と Manchester（英国のハブ サイト）間では、Cisco IOS ゲートキーパーの **bandwidth inter-zone** コマンド
- Manchester と Liverpool 間にあるリンクでは、Cisco CallManager ロケーション

CHAPTER 10

ダイヤル プラン

ダイヤル プランは、IP テレフォニー システムの重要な要素の 1 つ であり、すべてのコール処理エージェントにとって不可欠となる部分です。概説すると、ダイヤル プランは、コールをどのようにルーティングするかをコール処理エージェントに指示する役割を果たします。具体的には、ダイヤル プランは次の機能を実行します。

- エンドポイントのアドレッシング

  システム内部の宛先への到達は、すべてのエンドポイント（IP Phone、FAX マシン、アナログ電話機など）とアプリケーション（ボイスメール システム、自動アテンダント、会議システムなど）にディレクトリ番号（DN）を割り当てることで実現しています。

- パスの選択

  発信側のデバイスによっては、同じ宛先に到達する場合でも、複数のパスから選択することができます。また、プライマリ パスが使用不可になっている場合にはセカンダリ パスを使用できます。たとえば、IP WAN に障害が発生した場合は、コールを公衆網を介して透過的に再ルーティングできます。

- コール特権

  特定の宛先へのアクセスを許可または拒否することによって、複数のデバイス グループにそれぞれ別のサービス クラスを割り当てることができます。たとえば、ロビーにある電話からはシステム内部および市内の公衆網宛先にしか到達できないようにし、その一方で、幹部社員の電話からは無制限に公衆網アクセスできるようにします。

- 番号操作

  特定の状況では、ダイヤルされたストリングをコールのルーティング前に操作する必要があります。たとえば、オンネットのアクセス コードを使用してダイヤルされたコールを公衆網を通じて再ルーティングするときや、省略コード（オペレータにつなぐ場合の 0 など）を内線番号に展開するときです。

- コールのカバレッジ

  特殊なデバイス グループを作成して、特定サービスの着信コールを別の規則（トップダウン、循環ハント、最長アイドル時間、またはブロードキャスト）に従って処理することができます。

この章では、ダイヤル プランの主な側面について、次の項目を説明します。

- プランニングの考慮事項（P.10-3）

  この項では、IP テレフォニー ダイヤル プランのプランニングに関係するプロセスを詳しく説明します。取り扱う範囲は、内線番号に使用される桁数から、企業内部のダイヤル プラン アーキテクチャ全般までです（前提条件：ダイヤル プラン一般について、ある程度の知識があること）。

- ダイヤル プランの要素（P.10-8）

  この項では、Cisco IP テレフォニー 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 CallManager および Cisco IOS の操作知識があることを推奨）。

- 設計上の考慮事項（P.10-47）

  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 CallManager および Cisco IOS の操作知識があることを推奨）。

詳細については、次の Web サイトから入手可能な『*Cisco CallManager System Guide*』、『*Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*』、およびその他の製品マニュアルを参照してください。

http://www.cisco.com

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。

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。最初に A 社のネットワーク、次に公衆網、最後に B 社のネットワークです。発信者から見ると、コールはオフネットワーク（オフネット）でルーティングされています。着信側から見ると、コールはオフネットで発生しています。

TDM システムでは、PBX または Centrex システムがテレフォニー システムのオンネット境界になります。TDM システムは、通常は 1 つのサイトの外側まで伸びていることはありません。伸びている場合も、その TDM システムは、大規模なシステム ハブの外周上に配置されていないサイトを含んでいないのが普通です。

IP テレフォニーの重要な特性の 1 つは、オンネットと見なすことのできるコール境界を拡張する機能です。たとえば、6 つの支店を保有している企業に所属するテレフォニー ユーザが、着信側が同じサイトにいる場合は省略ダイヤリング（4 桁の内線番号など）を使用して同僚に到達し、他のサイトにいる別の同僚に到達するときは、完全な公衆網番号をダイヤルしているとします。IP ベース システムを使用すると、すべてのユーザが同じ IP ネットワークによって処理されるため、6 つの支店を 4 桁の省略ダイヤリング プランによって経済的に結ぶことが可能になります。IP ネットワークを優先パスとして使用し、IP ネットワークが輻輳した場合のセカンダリ パスとして、公衆網への自動オーバーフローを使用します。

省略ダイヤリング

公衆網から直接到達可能な、ダイヤルイン（DID）機能を使用した内線番号があるとします。オフネットの公衆網発信者が DID 内線番号に到達するには、完全修飾公衆網番号（たとえば、1 415 555 1234）をダイヤルする必要があります。しかし、オンネットの発信者については、DID 番号の最後のいくつかの桁をダイヤルするだけでこの内線番号に到達する機能を利用することを考えています。4 桁の省略ダイヤル プランを使用すると、この例のオンネットの発信者は、1234 のみダイヤルすればこの内線番号に到達します。

内線ダイヤリングの重複の防止

テレフォニー システムは、どの内線番号にも明確な方法で到達できるように設定する必要があります。この目標を達成するには、ダイヤル プランが次の要件を満たす必要があります。

- すべてのオンネット内線ダイヤリングを、グローバルに一意なものにする。たとえば、4 桁の省略オンネット ダイヤル プランを使用するシステムで、サイト A とサイト B のどちらの内線番号についても、サイト C から 4 桁のみダイヤルして到達することが要件である場合、サイト A に内線番号 1000 があり、サイト B の別の内線番号も 1000 である状態は許されません。
- 個々のダイヤルストリングは、部分的にも重複していない。
  - たとえば、4 桁の省略ダイヤル プランにおいて、9 をオフネット アクセス コードとして使用する場合（公衆網コールを発信する場合など）、内線番号を 9XXX にすることはできません。このように設定すると、コールがすぐにはルーティングされない状況が発生します。たとえば、ユーザが 9141 をダイヤルしたとします。システムは、追加の数字が入力されるか（ユーザが 9 1 415 555 1234 をダイヤルしようとしている場合など）、桁間タイムアウトに達するまで待機し、その後でコールを内線番号 9141 にルーティングします。同様に、オペレータ コード（たとえば 0）を使用する場合にも、0XXX の内線番号範囲全体を 4 桁の定型ダイヤル プランから除外する必要があります。
  - 長さが異なっていても、ストリングが重複していることは許されません。たとえば、システムで内線番号 1000 と 10000 を使用すると、1000 にダイヤルする場合、ユーザは桁間タイムアウトに達するまで待機する必要があります。

ダイヤリング ストリングの長さ

内線番号にダイヤルするときの必要桁数は、ダイヤル可能な内線番号の数によって決まります。たとえば、4 桁の省略ダイヤル プランでは、内線番号が 10,000 個（0000 ～ 9999）を超える場合には対応できません。0 と 9 をオペレータ コードおよびオフネット アクセス コードとしてそれぞれ予約する場合、この番号範囲は、さらに 8,000 個（1000 ～ 8999）まで減ります。

定型オンネット ダイヤル プラン

ダイヤル プランは、システム内のすべての内線番号に一定の方法で到達するように設計できます。つまり、任意のオンネット発信地点から、特定の内線番号に一定の桁数で到達することができます。ユーザにとって簡潔であるため、定型ダイヤリングを使用することをお勧めします。各種のオンネット ロケーションから発信するときに、番号をダイヤルするための方法をユーザがいくつも覚えておく必要がありません。

たとえば、任意のオンネット ロケーションから 1234 をダイヤルすると電話 A に到達するとします。この場合、発信側の電話が同じオフィスまたは別のサイトのどちらにあっても、企業のダイヤル プランは定型と見なすことができます。

企業のサイト数が少ない場合は、このアプローチを容易に採用できます。企業の内線番号とサイトの数が多くなるほど、定型ダイヤル プランを設計するときに次の点が問題になってきます。

- 内線番号の数は、ダイヤル　プラン用に予定した桁数で対応できる範囲を超える場合もあります。たとえば、8,000 個（内線番号 0XXX と 9XXX を除外するものと想定）を超える内線番号が必要になった場合は、5 桁以上使用する省略ダイヤル プランが必要になります。
- オンネット省略内線番号を DID 番号と同じものにする場合、地域通信事業者から新しい DID 範囲を取得するときに、その範囲が既存のオンネット省略ダイヤルの範囲と競合することが許されなくなります。たとえば、4 桁の定型省略ダイヤル プランを使用しているシステムに、DID 範囲 415 555 1XXX があるとします。DID 範囲 650 556 1XXX の取得も検討している場合は、オンネット ダイヤリングの桁数を 5 に増やすことが望ましくなります。この例では、5 桁のオンネット範囲 51XXX と 61XXX は重複することがありません。
- ほとんどのシステムでは、一定の範囲をオフネット アクセス コードとオペレータ ダイヤリング用に除外する必要があります。9 と 0 が予約コードになっているシステムで、9 または 0 で始まるオンネット内線番号ダイヤリングに対応できるダイヤル プランは、（定型もそれ以外も）存在しません。つまり、ダイヤル プランで最初の数字として 9 または 0 を使用する必要がある場合は、最初の数字が 9 または 0 である DID 範囲を使用できません。たとえば、5 桁の省略ダイヤル プランを使用する場合、DID 範囲 415 559 XXXX（およびこのサブセット）は使用できません。この例では、代替策として、省略ダイヤリングの長さを 6 桁以上に増やすか、末尾の 5 桁が 9 で始まる DID 範囲を使用しないようにするという方法があります。

桁数を選定し、必要な範囲（たとえば、9 または 0 で始まる範囲）を除外したら、残りのダイヤリング スペースをすべてのサイトに分配する必要があります。

ほとんどのシステムでは、2 つの範囲を除外する必要があります。このため、ダイヤル範囲の先頭となる可能性が残っている数字は、8 つです。表 10-1 では、一般的な 4 桁の定型ダイヤル プランにおける、ダイヤリング スペースの分配例を示しています。

表 10-1　一般的な 4 桁定型ダイヤル プランでの番号の分配

範囲	用途	DID 範囲	DID 以外の範囲
0XXX	除外（0 はオフネット アクセス コードとして使用される）		
1XXX	サイト A の内線番号	418 555 1XXX	適用対象外
2XXX	サイト B の内線番号	919 555 2XXX	適用対象外
3XXX	サイト C の内線番号	415 555 30XX	3[1-9]XX
4[0-4]XX	サイト D の内線番号	613 555 4[0-4]XX	適用対象外
4[5-9]XX	サイト E の内線番号	450 555 4[5-9]XX	適用対象外
5XXX	サイト A の内線番号	418 555 5XXX	適用対象外
6XXX	サイト F の内線番号	514 555 6[0-8]XX	69XX
7XXX	将来的にサポート	XXX XXX 7XXX	7XXX
8XXX	将来的にサポート	XXX XXX 8XXX	8XXX
9XXX	除外（9 はオフネット アクセス コードとして使用される）		

表 10-1 の例では、さまざまなサイトが次の方法に従って番号を割り当てられています。

- サイト A（企業の本社）では、必要な内線番号が 1,000 個を超えるため、2 つの番号範囲（1XXX と 5XXX）全体を確保しています。対応する DID 範囲も、このサイトの地域通信事業者から取得する必要があります。
- サイト B は、1 つの範囲全体（2XXX）を割り当てられているため、内線番号を 1,000 個まで使用できます。
- サイト C も 1 つの範囲全体を割り当てられていますが、100 個の DID 内線番号（415 555 30XX）と 900 個の DID 以外の内線番号に分割されています。DID 内線番号がさらに必要になった場合は、DID 以外の範囲にある、まだ割り当てられていない番号を使用することができます。

- サイト D と E は、4XXX 範囲からそれぞれ 500 個ずつ番号を割り当てられています。対応する DID 範囲は、それぞれのサイトの 4XXX 範囲の部分と一致している必要があります。DID 範囲がサイトごとに異なっているため（おそらく、別の公衆網サービス プロバイダーから取得したことが原因）、サイト間で範囲を分割するには、密接な連携作業が必要です。特定の範囲内で割り当てられるサイトの数が多くなるほど、範囲全体をすべて使用することは困難になり、場合によっては不可能になります。
- サイト F の範囲は、900 個の DID 番号（6[0-8]XX）と 100 個の DID 以外の番号（69XX）に分割されています。
- 範囲 7XXX と 8XXX は、将来の使用に備えて予約されています。

新しいダイヤル プランを実装する場合、プラン立案者の主な目標の 1 つは、電話番号の変更が必要になるのを避けることです。また、既存の電話システムで内線番号範囲が重複している場合、過去に問題がなくても、定型ダイヤル プランでは許容されない場合があります。

可変長のオンネット ダイヤル プラン

サイトの数が多いシステムや、サイトの内線番号範囲が重複しているシステムでは、次の特性を備えた可変長ダイヤル プランを使用すると効果的です。

- サイトの内部では、オンネット内線番号へのコールに対して、省略ダイヤリング（4 桁の内線番号など）を引き続き使用できる。
- サイト間では、ユーザはアクセス コードをダイヤルし、次にサイト コードと宛先のオンネット内線番号をダイヤルする。
- オフネット コールの場合は、アクセス コードの次に公衆網番号をダイヤルする必要がある。

アクセス コードとダイヤル コードを使用すると（表 10-2 を参照）、定型省略ダイヤル プランであれば重複となる内線番号を、オンネット ダイヤル プランで区別できるようになります。

表 10-2　サイト コードの一般的な使用方法

サイト コード	範囲	用途	DID 範囲	DID 以外の範囲
1	1XXX	サイト A の内線番号	418 555 10XX	1[1-9]XX
2	1XXX	サイト B の内線番号	919 555 1XXX	適用対象外
3	1XXX	サイト C の内線番号	907 555 1XXX	適用対象外

表 10-2 では、サイト A、B、C はそれぞれ独自に 4 桁範囲 1XXX を割り当てられています。従来のテレフォニー システムでは、サイト A からサイト B へのコールはオフネット コールとしてルーティングする必要がありました。新しいシステムでは、これらのコールをオンネット コールとしてダイヤルできます。

サイト A からは、ユーザは 1234 をダイヤルするだけで内線番号 1234 に到達できます。一方で、サイト B からサイト A の内線番号 1234 に対して、サイト B にある内線番号 1234 と競合することなく到達するには、ダイヤル プラン側で対応する必要があります。このため、各サイトにサイト コードが割り当てられています。

サイト B から、単にサイト A のコードを目的の内線番号と組み合せてダイヤルすることだけでは不十分です。この場合、11234 はサイト B の内線番号 1123 と部分的に重複しているため、桁間タイムアウトの問題が発生します。代わりに、サイト間オンネット アクセス コードとして 8 を割り当てると、サイト B から 81234 をダイヤルしてサイト A の内線番号 1234 に到達できるようになります。

オンネットのオフサイト内線番号にダイヤルするために必要な桁数は、次の要素によって決まります。

- サイト間アクセス コードに使用する 1 桁
- サイト コードに使用する N 桁（N は、必要となるサイト コードの数に見合う数値。たとえば、システムに 13 のサイトがある場合、サイト コードには少なくとも 2 桁が必要）
- 宛先サイトのローカル ダイヤル プランで必要となる桁数

たとえば、システムに 75 のサイトがあり、各サイトが 4 桁の省略ダイヤリングを使用している場合は、8 + SS + XXXX という形式が必要になります。8 はオンネット アクセス コード、SS は 2 桁のサイト コード、XXXX は 4 桁の内線番号で、合計 7 桁です。

オンネットとオフネットのアクセス コード

ほとんどの企業のテレフォニー システムでは、オフネットの宛先にコールを振り分けるためのオフネット アクセス コード専用として、1 つの数字（たとえば 9）を割り当てることが一般的です。可変長のオンネット ダイヤル プランでは、他のサイトにあるオンネット内線番号宛てのコールをダイヤルするために、オンネット アクセス コードとして、振り分け用の数字（たとえば 8）がもう 1 つ必要です。これらの 2 つのアクセス コードをオペレータ アクセス コード（たとえば 0）とともに使用するので、ダイヤル ストリングの先頭の数字となる可能性のある 10 個の数字からは、3 つが暗黙的に除外されます。この制限事項は、次の両方の理由から、好ましいものとは言えません。

- ユーザは、オンネットとオフネットの違いを理解し、適切なアクセス コードを選択する必要がある。
- 3 つのダイヤリング範囲全体を除外することによって、著しい制約や、一部の割り当て済み内線番号範囲との競合が生じる恐れがある。たとえば、サイトですでに 8 で始まる省略ダイヤリング範囲を使用している場合、この数字をアクセス コードとして使用するには、変更作業が必要になります。

定型オフネット アクセス コード（たとえば 9）をすでにすべてのサイトで使用しているシステムでは、同じコードをオフネットとオンネットの両方のオフサイト宛先に使用することをお勧めします。このアプローチには、主に次の 2 つの暗黙的要件があります。

- 部分的な重複や待ちが発生することを避けるには、アクセス コードの後に続く桁数を一定にする必要がある。
- テレフォニー システムは、ダイヤルされるすべてのオンネット番号をオフネット番号として認識し、IP ネットワーク経由でルーティングできる必要がある。このタスクは、Cisco CallManager クラスタが 1 つしかない小規模システムの場合は単純ですが、複数の Cisco CallManager クラスタがある大規模なシステムでは複雑なものになります。

事前の計画

IP ベースのシステムを実装するときは、ユーザの普段の操作手順を変更する必要が生じる場合もあります。新しいシステムのプランニングでは、この実装をできる限りユーザから見えないようにすることが望ましいのですが、それぞれ別のテレフォニー システム上にあった複数のサイトの統合に対応するには、ダイヤリング手順の調整が必要になることもあります。たとえば、企業全体にわたる新しいグローバルなダイヤル プランに対応するには、ユーザが他のサイトにいる別のユーザに到達する方法、サイト内コールに使用している桁数、ときには内線番号までも変更することが必要な場合もあります。ユーザが何度もダイヤル プラン変更を経験することを避けるには、企業規模の拡大を見越しておくようにします。企業が成長すると、複数のダイヤリング リージョンへのサイトの追加、オンネット内線番号の必要数の増加、公衆網番号の再割り当て（たとえば、エリア コードの分割など）、他国への事業展開が発生する可能性があります。

ダイヤル プランの要素

この項では、Cisco IP テレフォニー 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。

Cisco CallManager におけるコール ルーティング

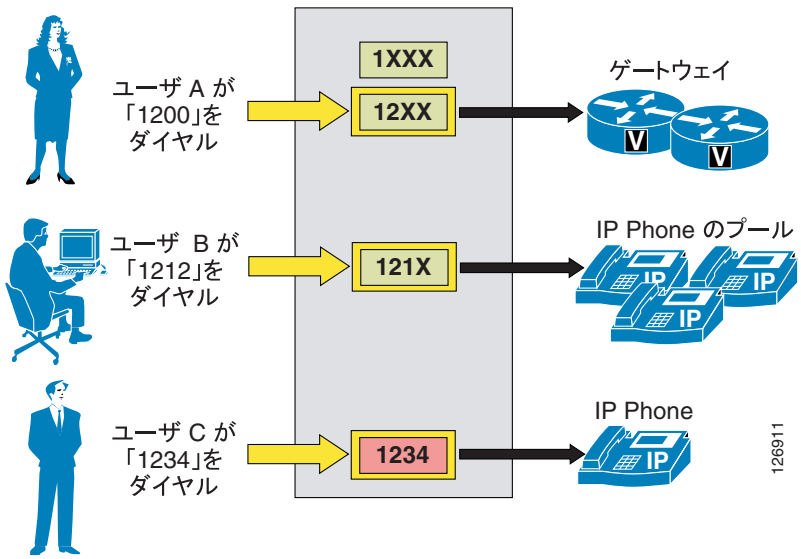
Cisco CallManager 内に設定されるダイヤリング宛先は、すべて内部のコール ルーティング テーブルにパターンとして追加されます。このような宛先としては、IP Phone 回線、ボイスメール ポート、ルート パターン、トランスレーション パターン、および CTI ルート ポイントがあります。

番号がダイヤルされると、Cisco CallManager は closest-match ロジックを使用し、コール ルーティング テーブルにあるすべてのパターンの中から一致パターンを選択します。一致している可能性のあるパターンが複数ある場合は、次の基準に基づいて宛先パターンを選択します。

- ダイヤルされたストリングに一致する。また、
- 一致する可能性のあるすべてのパターンの中から、ダイヤルされたストリングを除くストリング数が最も少ないパターンに一致する。

たとえば、図 10-1 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 10-1　Cisco CallManager のコール ルーティング ロジックの例



ユーザ A がストリング 1200 をダイヤルすると、Cisco CallManager は、この番号をコール ルーティング テーブル内のパターンと比較します。この場合は、一致する可能性のあるパターンが 2 つあります（1XXX と 12XX）。両方ともダイヤル ストリングに一致していますが、1XXX は合計 1,000 個のストリングに一致する一方で（1000 ～ 1999）、12XX は 100 個のストリングに一致します（1200 ～ 1299）。したがって、12XX がこのコールの宛先として選択されます。

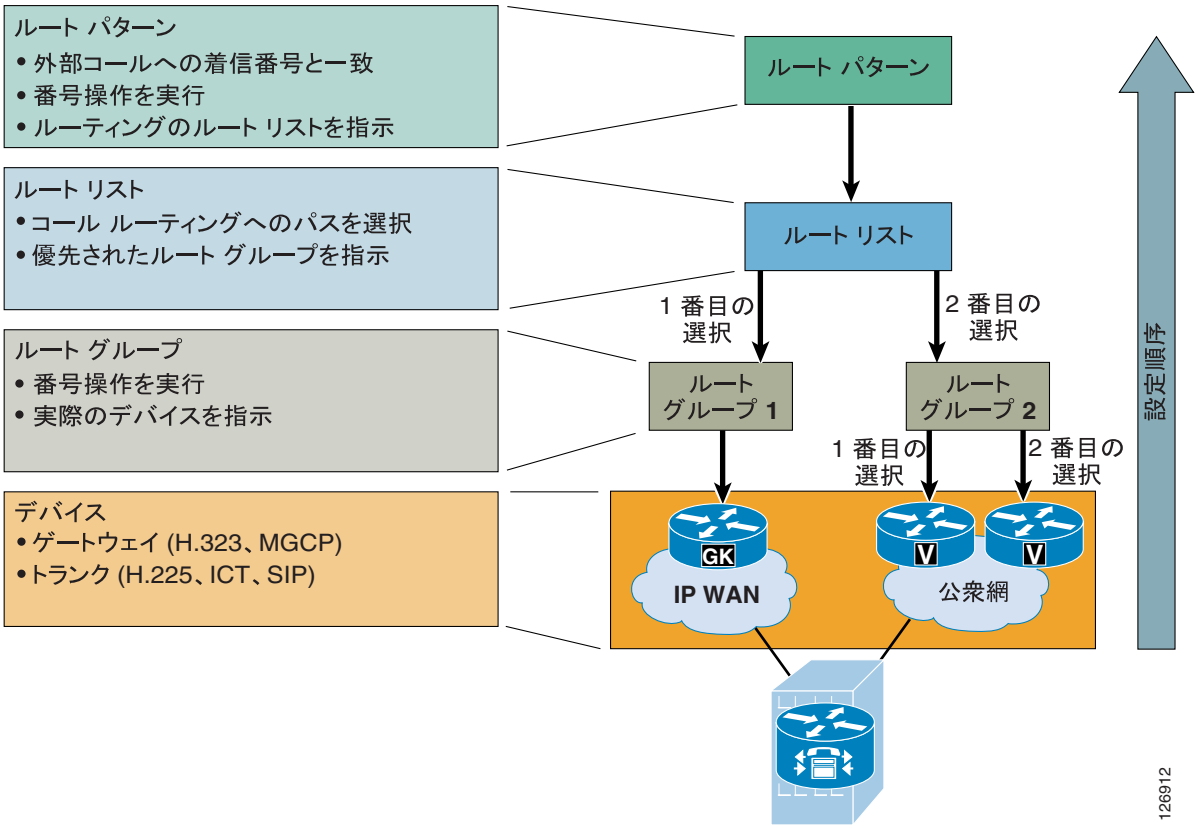
ユーザ B がストリング 1212 をダイヤルした場合、一致する可能性のあるパターンは 3 つあります。上で説明したように、1XXX に一致するストリングは 1,000 個あり、12XX に一致するストリングは 100 個あります。しかし、121X に一致するストリングは 10 個しかありません。したがって、このパターンがコールの宛先として選択されます。

ユーザ C がストリング 1234 をダイヤルした場合、一致する可能性のあるパターンは 3 つあります（1XXX、12XX、1234）。上で説明したように、1XXX に一致するストリングは 1,000 個あり、12XX に一致するストリングは 100 個あります。しかし、1234 に一致するストリングは 1 個しかありません（ダイヤルされたストリング）。したがって、このパターンがコールの宛先として選択されます。

（注） Cisco CallManager Release 4.0 以降でディレクトリ番号（DN）を設定すると、それぞれのデバイス（IP Phone など）が登録済みかどうかにかかわらず、その番号はコール ルーティング テーブルに配置されます。この動作は、これより前の Cisco CallManager バージョンとは異なります。旧バージョンでは、パターンがコール ルーティング テーブルに追加されるのは、それぞれのデバイスが登録済みの場合のみでした。この仕様変更によって、アプリケーション（およびそのプライマリ パターン）が未登録である場合、セカンダリの一致パターンを利用してフェールオーバー機能を提供することができなくなりました。プライマリ パターンがコール ルーティング テーブルに必ず存在するため、セカンダリ パターンに一致するかどうかは検索されません。ただし、CTI ルート ポイントなどのプライマリ パターンの Forward Busy フィールドを使用して、フェールオーバーと同じ効果を得ることは可能です。Cisco CallManager Release 4.0 以降では、このフィールドでワイルドカードを使用できるためです。

Cisco CallManager は、同じクラスタ内の宛先にコールをルーティングする方法を自動的に「習得」します。公衆網ゲートウェイ、H.323 ゲートキーパー、またはその他の Cisco CallManager クラスタなどの外部宛先の場合、外部ルート コンストラクト（次の項で説明）を使用して、明示的にルーティングを設定する必要があります。このコンストラクトは、3 層式のアーキテクチャに基づいています。このアーキテクチャでは、複数層のコール ルーティングと共に、番号操作も可能です。Cisco CallManager は、外部ダイヤル ストリングと一致する設定済みルート パターンを検索し、それを使用して、対応するルート リストを選択します。ルート リストには、コールに使用可能なパスが優先順位順に並べられています。これらのパスは、ルート グループと呼ばれ、従来の PBX でトランク グループと呼ばれていたものに非常によく似ています。図 10-2 では、Cisco CallManager 外部ルート コンストラクトの 3 層アーキテクチャを示しています。

図 10-2　外部ルート パターンのアーキテクチャ



次の各項では、Cisco CallManager の外部ルート コンストラクトの個々の要素について説明します。

- ルート パターン（P.10-10）
- ルート リスト（P.10-13）
- ルート グループ（P.10-14）
- ルート グループ デバイス（P.10-14）

ルート パターン

ルート パターンは、コールを外部エンティティにルーティングするために Cisco CallManager で設定された、数字とワイルドカードを組み合せたストリング（たとえば、9.[2-9]XXXXXX）です。ルート パターンでは、コールをルーティングするゲートウェイを直接指すことも、ルート リストを指すこともできます。ルート リストはルート グループを指しており、最終的にゲートウェイを指します。

ルート パターン、ルート リスト、およびルート グループ コンストラクトとを完全パスで指定するようにシスコは強くお勧めします。その理由は、この構造を使用するとコール ルーティング、番号操作、および将来のダイヤル プランの拡張を最も柔軟に行うことができるからです。

@ ワイルドカード

- @ ワイルドカードは、特殊なマクロ関数であり、特定の国の番号計画全体を表す一連のパターンに拡張されます。たとえば、フィルタ処理されていない単一のルート パターン（たとえば、9.@）を北米番号計画を使用して設定すると、実際には、Cisco CallManager 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。

- Cisco.com で公開されている International Dial Plan Tool で作成したファイルを使用すると、北米以外の番号計画を受け付けるように Cisco CallManager を拡張できます。この作業が完了すると、Route Pattern 設定ページの Numbering Plan フィールドで選択した値に応じて、同じ Cisco CallManager クラスタ内で、複数の番号計画に対して @ ワイルドカードを使用できるようになります。現時点で使用可能な番号計画の詳細については、Cisco アカウント チームにお問い合せください。
- @ ワイルドカードは、いくつかの中小規模の配置では十分に実務で使用できますが、大規模な配置では、管理とトラブルシューティングが困難になる可能性があります。これは、@ ワイルドカードを利用する場合、ルート フィルタを使用して、管理者が特定のパターンをブロックする必要があるためです（P.10-11 の「ルート フィルタ」を参照してください）。

ルート フィルタ

- ルート フィルタは、@ ワイルドカードによって作成されるルート パターン数を減らすために、@ ルート パターンと一緒にのみ使用します。
- ルート フィルタと一緒に入力する論理式は、NOT-SELECTED フィールドを除いて、最大 1024 文字にすることができます。
- ルート フィルタ内の論理文節数が増えるにつれて、設定ページのリフレッシュ時間も増え、容認できないほど長くなる場合があります。
- 大規模な配置の場合、@ ワイルドカードとルート フィルタではなく、明示ルート パターンを使用してください。この方法を利用すると、管理とトラブルシューティングも容易になります。これは、Cisco CallManager で設定されているすべてのパターンが、Route Pattern コンフィギュレーション ページから簡単に参照できるからです。

国際および可変長のルート パターン

- 国際間の宛先は、通常、任意の桁数を表す ! ワイルドカードを使用して設定されます。たとえば、北米では通常、国際コール用にルート パターン 9.011! が設定されています。欧州諸国のほとんどでは、0.00! ルート パターンを使用することで同じ結果が得られます。
- ! ワイルドカードは、ダイヤルされる番号の長さが変化する国では配置にも使用されます。このような場合、Cisco CallManager は、ダイヤルがいつ完了するか分からないので、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。
  - 2 番目のルート パターンの後に # ワイルドカードを続けて設定し（たとえば、北米の場合 9.011!#、欧州の場合 0.00!#）、ダイヤルの終わりを示すために # をダイヤルするようにユーザに指示します。この処置は、携帯電話で送信ボタンを押すことに相当します。

重複送信と重複受信

国内の番号計画をスタティック ルート パターンで定義することが難しい国では、Cisco CallManager に重複送信および重複受信を設定することができます。

重複送信とは、エンドユーザのダイヤルする数字を Cisco CallManager で収集しながら、数字がダイヤルされると同時に公衆網に渡すことを意味します。Cisco CallManager Release 4.0 以降で重複送信を使用可能にするには、Route Pattern Configuration ページの Allow Overlap Sending チェックボックスをオンにします。これより前の Cisco CallManager リリースで重複送信を使用可能にするには、SendingCompleteIndicator サービス パラメータを False に設定します。ルート パターンが必要になるのは、公衆網アクセス コード（たとえば、北米では 9、欧州諸国の多くでは 0）を含める場合のみです。

重複受信とは、ダイヤルされる数字を PRI 公衆網ゲートウェイから Cisco CallManager で 1 つずつ受信し、ストリングのダイヤルが完了するまで待機し、その後でコールを内部宛先にルーティングすることを意味します。Cisco CallManager Release 3.3(3) 以降で重複受信を使用可能にするには、OverlapReceivingFlagForPRI サービス パラメータを Trule に設定します。これより前の Cisco CallManager リリースでは、パラメータ名は OverlapReceivingForPriFlag です。

ルート パターンにおける番号操作

- 番号操作は、ルート パターンではなく、ルート グループのみで設定してください。
- ルート グループでの番号操作は、ルート パターンで行われた番号操作を完全に上書きします。
- ルート パターンで番号操作を設定する場合、コール詳細レコード（CDR）は、番号操作が行われた後のダイヤル番号を記録します。ルート グループだけで番号操作を設定する場合、CDR は、番号操作が行われる前の実際のダイヤル番号を記録します。
- 同様に、ルート パターンでの番号操作を設定すると、発信側の IP Phone ディスプレイおよび Placed Calls レジスタには、操作後の番号が示されます。ルート グループのみで番号操作を設定する場合、この操作はエンドユーザには見えなくなります。

発呼回線 ID

- 発呼回線 ID の表示は、ゲートウェイで使用可能または使用不可にすることができます。また、サイトの要件に基づいて、ルート パターンで操作することもできます。
- Use Calling Party's External Phone Number Mask オプションを選択する場合、外部コールは、コールを発信する IP Phone に指定された発呼回線 ID を使用します。このオプションを選択しない場合、Calling Party Transform Mask フィールドに指定されたマスクが、発信者番号識別の生成に使用されます。

緊急プライオリティ

- Urgent Priority チェックボックスは、一般に、パターンに一致したコールを T302 タイマーの満了を待たずにすぐルーティングする目的で使用されます。たとえば、北米でパターン 9.911 と 9.[2-9]XXXXXX が設定されている場合、ユーザが 9911 をダイヤルすると、Cisco CallManager は T302 タイマーが満了するまで待機し、その後でコールをルーティングします。これは、9911 の後に数字が入力されて、9.[2-9]XXXXXX に一致する可能性があるためです。9.911 ルート パターンについて緊急プライオリティを有効にすると、Cisco CallManager はユーザが 9911 とダイヤルした直後にルーティング処理を実行し、T302 タイマーの満了までは待機しません。
- Urgent Priority チェックボックスをオンにした場合に実行されるのは、設定済みのパターンがダイヤルされた番号と一致する可能性があるとき、その直後に T302 を満了させることだけです。つまり、緊急パターンが他のパターンよりも高い優先順位を持っているわけではありません。P.10-8 の「Cisco CallManager におけるコール ルーティング」の項で説明した closest-match ロジックは、依然として有効です。たとえば、ルート パターン 1XX が緊急パターンとして設定され、パターン 12! が通常のルート パターンとして設定されているとします。ユーザが 123 とダイヤルした場合、1XX が緊急パターンであるため、Cisco CallManager は 3 番目の数字を受信した直後にルーティング処理を実行しますが、この場合はパターン 12! が選択されます。これは、一致確率が大きいためです（12! が合計 10 パターンに一致するのに対して、1XX は 100 パターンに一致）。

コール分類

- このルート パターンを使用しているコールは、オンネットまたはオフネットのコールとして分類することができます。このルート パターンを使用すると、オフネット間でのコール転送を禁止したり、オンネット通話者がいないコンファレンス ブリッジを終了したりすることによって、料金詐欺を防止できます（これらの機能は、どちらも Cisco CallManager Administration の Service Parameters を使用して制御します）。
- Allow device override チェックボックスをオンにすると、コールは、関連するゲートウェイまたはトランク上で、コール分類設定に基づいて分類されるようになります。

強制アカウント コード（FAC）

- Forced Account Codes（FAC）チェックボックスを使用すると、個々のルート パターンを使用して発信コールが制限されます。ルート パターンに対して FAC を有効にすると、ユーザは、目的のコール受信者に到達するための許可コードを入力するように要求されます。

- ユーザのダイヤルした番号が、FAC が有効になったルート パターンを通じてルーティングされるものである場合、システムは許可コードの入力を求めるトーンを再生します。コールを確立するには、ユーザ許可コードが、ダイヤルされた番号のルーティングに必要となる許可レベルにを満たしているか、そのレベルを超えている必要があります。
- コール詳細レコード（CDR）に表示されるのは、許可名のみです。許可コードは CDR には表示されません。
- FAC 機能は、Allow overlap sending チェックボックスがオンの場合は使用できません。

クライアント証明書コード（CMC）

- Client Matter Code（CMC）チェックボックスを使用すると、個々のルート パターンを使用して特定番号へのコールがトラッキングされます。たとえば、企業で使用すると、特定のクライアントへのコールをトラッキングできます。
- ルート パターンに対して CMC を有効にすると、ユーザは目的の宛先に到達するためのコードを入力するように要求されます。
- ユーザのダイヤルした番号が、CMC が有効になったルート パターンを通じてルーティングされるものである場合、システムはコードの入力を求めるトーンを再生します。コールを確立するには、ユーザが正しいコードを入力する必要があります。
- クライアント証明書コードは、コール詳細レコードに表示されます。これは、クライアントの課金およびアカウンティングに関するレポートを生成するための、CDR の分析およびレポート ツールで使用できるようにするためです。
- CMC 機能は、Allow overlap sending チェックボックスがオンの場合は使用できません。
- CMC と FAC を両方とも有効にすると、ユーザは番号をダイヤルするとき、FAC の入力を求められたら入力し、次のプロンプトで CMC を入力します。

ルート リスト

ルート リストは、発信コールに使用できるパス（ルート グループ）が優先順位順に並べられたリストです。一般に、1 つのルート リストは、1 つのリモート ロケーションに関連付けられ、複数のルート パターンがそのルート リストを指定することができます。ルート リストの標準的な用途は、リモートの宛先に 2 つのパスを指定することです。この場合、第一選択のパスは、IP WAN を介したパスであり、第二選択のパスは、ローカル公衆網ゲートウェイを介したパスです。

ルート リストには次の特性があります。

- 複数のルート パターンが同一ルート リストを指すことができます。
- ルート リストは、所定の宛先への代替パスの役目をするルート グループが、優先順位順に並べられたリストです。たとえば、ルート リストを使用して最低料金選択機能をサポートすることができます。この場合、リスト内のプライマリ ルート グループが、コール当たりのコストがより低くなるようにします。プライマリ ルート グループが「all trunks busy（全トランク使用中）」状態、または IP WAN リソースの不足により使用できない場合だけ、セカンダリ ルート グループが使用されます。
- ルート リスト内の各ルート グループは、独自の番号操作を行うことができます。たとえば、ルート パターンが 9.@ であるときに、ユーザが 91 408 555 4000 をダイヤルした場合、IP WAN ルート グループは 9 1 を削除し、公衆網ルート グループは 9 だけを削除することが可能です。
- 複数のルート リストに、同じルート グループを含むことができます。ルート グループの番号操作は、そのルート グループを指定する特定のルート リストに関連しています。
- ルート パターンまたはルート グループ内で複数の番号操作を実行しようとする場合、変換が実行される順序が、変換結果の E.164 アドレスに影響を与える可能性があります。Cisco CallManager は、次に示す主要なタイプの番号操作を表示されている順に実行します。
  1. 数字を破棄する
  2. 着信側変換
  3. 数字をプレフィックスとして付加する

ルート グループ

ルート グループは、一般にゲートキーパーまたはリモート Cisco CallManager クラスタとのゲートウェイ（MGCP または H.323）、H.323 トランク、または SIP プロキシへの SIP トランクである特定のデバイスを制御し、それを指定します（Cisco CallManager Release 3.2 以前では、H.323 トランクの役割は、「Anonymous Device」ゲートウェイ、および Intercluster Trunk プロトコルを使用して設定された H.323 ゲートウェイによって実行されていました）。

Cisco CallManager は、割り当てられている分配アルゴリズムに従ってコールをデバイスに送信します。Cisco CallManager では、トップダウン アルゴリズムと循環アルゴリズムをサポートしています。

ルート グループ デバイス

ルート グループ デバイスは、ルート グループによってアクセスされるエンドポイントであり、一般に、ゲートキーパーまたはリモート Cisco CallManager とのゲートウェイまたは H.323 トランクで構成されます。次のタイプのデバイスは、Cisco CallManager で設定できます。

- メディア ゲートウェイ コントロール プロトコル（MGCP）ゲートウェイ
- H.323 ゲートウェイ
- H.225 トランク、ゲートキーパー制御：ゲートキーパーを介した標準 H.323 ゲートウェイとのトランク
- クラスタ間トランク、非ゲートキーパー制御：別の Cisco CallManager クラスタとの直接トランク
- クラスタ間トランク、ゲートキーパー制御：ゲートキーパーを介した他の Cisco CallManager クラスタまたは H.323 ゲートウェイとのトランク
- SIP トランク：SIP プロキシへのトランク（Cisco CallManager Release 4.0 以降で使用可能）

（注） H.225 トランクとクラスタ間トランク（ゲートキーパー制御）はどちらも、相手方エンドポイントが標準 H.323 ゲートウェイであるか、Cisco CallManager であるかを自動的に検出し、それに応じて H.225 または Intercluster Trunk プロトコルを選択します（この自動検出メカニズムは、Cisco CallManager Release 3.2 用にクラスタ間プロトコルを使用して設定される「Anonymous Device」ゲートウェイにも適用されます）。Cisco CallManager Release 3.1 より前のリリースで、クラスタとの直接トランクをセットアップしようとする場合は、Intercluster Trunk プロトコルを選択してください。

Cisco CallManager におけるコール特権

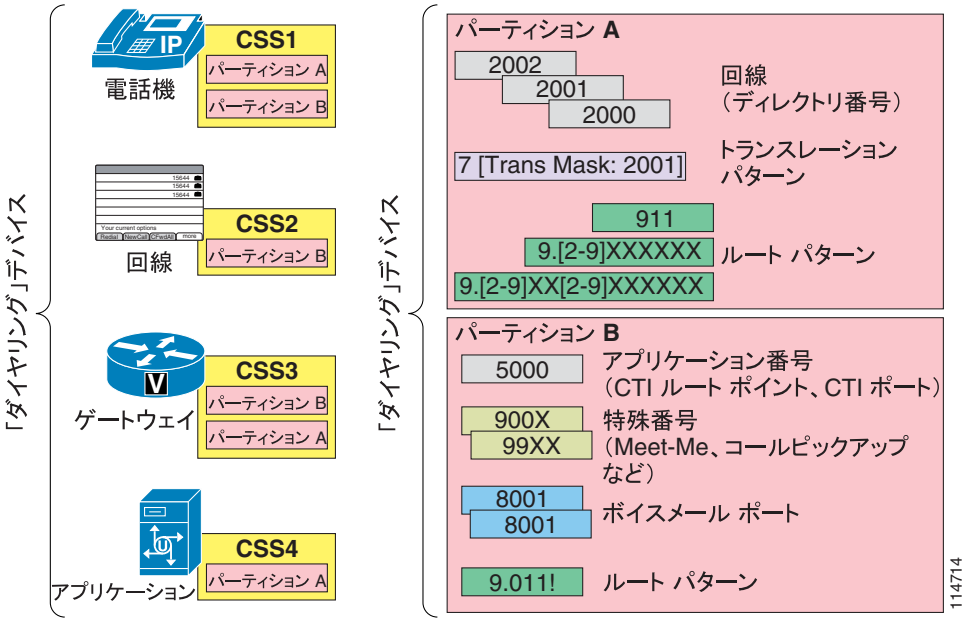
コール特権を実装するには、Cisco CallManager で次の要素を設定します。

- パーティション（P.10-15）
- コーリング サーチ スペース（P.10-16）

パーティションは、ほぼ同じアクセス可能性を持つディレクトリ番号のグループです。コーリング サーチ スペースは、特定のデバイスからどのパーティションがアクセス可能であるかを指定します。デバイスは、コーリング サーチ スペースに含まれているパーティション内の DN だけを呼び出すことができます。

図 10-3 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 10-3　パーティションとコーリング サーチ スペース

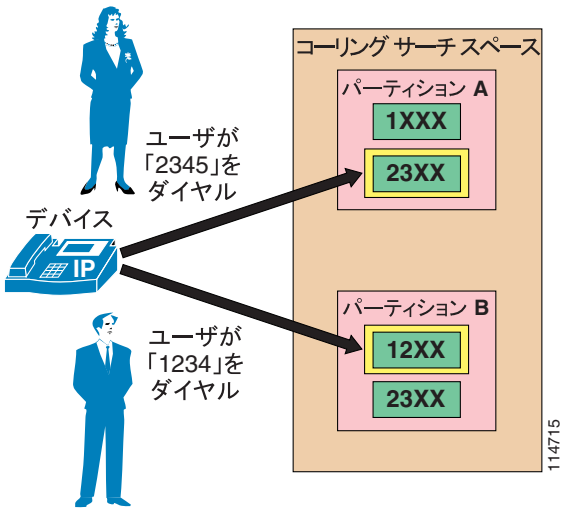


パーティション

パーティションに含めることができるダイヤル プラン項目には、IP Phone のディレクトリ番号、トランスレーション パターン、ルート パターン、CTI ルート ポイント、およびボイスメール ポートがあります。P.10-8 の「Cisco CallManager におけるコール ルーティング」で説明するように、複数のダイヤル プラン項目（ディレクトリ番号、ルート パターンなど）が重複する場合、Cisco CallManager は、ダイヤルされた番号と一致するか、または最も近い（最も固有性の高い一致）項目を選択します。2 つのダイヤル プラン項目が、ダイヤルされたパターンに等しく一致した場合、Cisco CallManager は、コールを発信するデバイスのコーリング サーチ スペース内で最初に表示されているダイヤル プラン項目を選択します。

たとえば、図 10-4 について考えます。ルート パターン 1XXX と 23XX はパーティション A の一部であり、ルート パターン 12XX と 23XX はパーティション B の一部です。発信デバイスのコーリング サーチ スペースには、パーティション A: パーティション B の順にパーティションがリストされています。このデバイスのユーザが 2345 をダイヤルすると、Cisco CallManager は、パーティション A のルート パターン 23XX を一致項目として選択します。これは、このパターンが発信デバイスのコーリング サーチ スペースで最初に示されているためです。ただし、ユーザが 1234 をダイヤルした場合には、Cisco CallManager はパーティション B のルート パターン 12XX を一致項目として選択します。これは、パーティション A の 1XXX よりも一致率が大きいためです。コーリング サーチ スペースに含まれているパーティションの順序は、closest-match ロジックに基づいて均等一致項目が複数あった場合に、競合を解消する要素としてのみ使用されます。

図 10-4　マッチング ロジックにおけるパーティション順序の影響



（注） 均等一致項目が同じパーティションに複数ある場合、Cisco CallManager は、ローカルのダイヤル プラン データベース内で最初にリストされている項目を選択します。ダイヤル プラン データベース内でダイヤル プラン項目がリストされる順序は、設定することができません。したがって、同じパーティション内で均等一致項目が共存しないようにすることを強くお勧めします。これはこのような場合に発生するダイヤル プラン ロジックが予測できないからです。

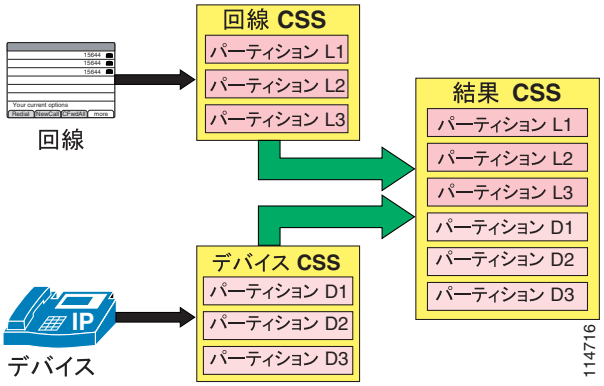
Cisco CallManager Release 4.1 以降では、日時に基づいてパーティションをアクティブまたは非アクティブにすることができます。パーティションをアクティブまたは非アクティブにするには、まず、Cisco CallManager Administration で期間とスケジュールを設定し、次に個々のタイム スケジュールを各パーティションに割り当てます。スケジュールに指定した日時の範囲外では、このパーティションは非アクティブになります。このパーティションに含まれているパターンは、Cisco CallManager コール ルーティング エンジンによってすべて無視されます。この機能の詳細については、P.10-29 の「時間帯ルーティング」を参照してください。

コーリング サーチ スペース

コーリング サーチ スペースは、特定のデバイスからどのパーティションがアクセス可能であるかを指定します。所定のコーリング サーチ スペースが割り当てられるデバイスは、そのコーリング サーチ スペースにリストされているパーティションだけにアクセスできます。そのコーリング サーチ スペース以外のパーティションの DN へのダイヤルは失敗します。発信者にはビジー信号が聞こえます。

IP Phone 回線とデバイス（電話機）自体の両方でコーリング サーチ スペースを設定する場合、Cisco CallManager は、この 2 つのコーリング サーチ スペースを図 10-5 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 10-5　IP Phone の回線とデバイスのコーリング サーチ スペース（CCS）の連結



同じルート パターンが、2 つのパーティション（回線のコーリング サーチ スペースに含まれているパーティションとデバイスのコーリング サーチ スペースに含まれているパーティション）に指定されている場合、Cisco CallManager は、P.10-15 の「パーティション」の項で説明している規則に従って、パーティションの連結リスト内で最初にリストされているルート パターン（この場合、回線のコーリング サーチ スペースに関連したルート パターン）を選択します。

回線とデバイスのコーリング サーチ スペースを設定する方法に関する推奨事項については、P.10-66 の「従来のアプローチによる Cisco CallManager のサービス クラスの構築」とP.10-69 の「回線 / デバイス アプローチによる Cisco CallManager のサービス クラスの構築」の項を参照してください。

（注） Cisco CallManager Release 3.1 より前のリリースでは、連結は逆順に行われていました。つまり、デバイスのコーリング サーチ スペースが先で、その後に回線のコーリング サーチ スペースが続きました。この逆順動作は、CTI ポートと CTI ルート グループにはまだ採用されています。

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 CallManager Administration Guide*』を参照してください。

http://www.cisco.com

パーティションまたはコーリング サーチ スペースを設定する前に、すべての DN は、<None> という名前が付いた特別なパーティションに置かれ、すべてのデバイスには、<None> という名前が付いたコーリング サーチ スペースが割り当てられます。カスタム パーティションとコーリング サーチ スペースを作成する場合は、作成するどのコーリング サーチ スペースにも、<None> パーティションが含まれています。一方、<None> コーリング サーチ スペースには、<None> パーティションだけが入っています。

（注） <None> パーティションに残っているどのダイヤル プラン項目も、コールを発信する任意のデバイスから暗黙的に到達可能です。したがって、予期しない結果を避けるために、<None> パーティションにダイヤル プラン項目を残さないように強くお勧めします。

自動転送コーリング サーチ スペース

回線に対して設定されているメインのコーリング サーチ スペースは、デバイスのコーリング サーチ スペースと連結されます。一方、3 タイプの自動転送（Forward All、Forward Busy、Forward No Answer）に対して設定されているコーリング サーチ スペースは、他のどのコーリング サーチ スペースとも連結されないスタンドアロン値です。Forward All コーリング サーチ スペースが <None> のままになっている場合、処理の結果は Cisco CallManager のリリースによって異なり、予想することは困難です。このため、自動転送のコーリング サーチ スペースを設定する場合は、次のベストプラクティスに従うことをお勧めします。

- 自動転送コーリング サーチ スペースは、常に <None> 以外の値を使用して設定する。この設定により混乱を避けることができ、トラブルシューティングが容易になります。転送されるコールにどのコーリング サーチ スペースが使用されるかについて、ネットワーク管理者が正確に把握できるためです。
- Call Forward Busy コーリング サーチ スペースと Call Forward No Answer コーリング サーチ スペースは、ボイスメール パイロットおよびボイスメール ポートの DN に到達可能で、かつ外部公衆網番号以外の値を使用して設定する。
- Call Forward All コーリング サーチ スペースは、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、私用電話に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 番号を公衆網からダイヤルしたりすることを防止します。

Call Forward All コーリング サーチ スペースを <None> のままにすると、次の処理が適用されます。

- Call Forward All が IP Phone から呼び出された場合、自動転送のコーリング サーチ スペースは、その IP Phone の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になります。
- Call Forward All が User Options ページから呼び出された場合、動作は Cisco CallManager リリースによって異なります。
  - Cisco CallManager Release 3.3(3) 以前では、自動転送のコーリング サーチ スペースは回線のコーリング サーチ スペースのみからコピーされます。
  - Cisco CallManager Release 3.3(4) および 4.0(2) 以降では、自動転送のコーリング サーチ スペースは、回線のコーリング サーチ スペースと「best-guess（最良の推論）」デバイス（つまり、ユーザが最後に Call Forward All を呼び出したときのデバイス）のコーリング サーチ スペースを連結したものになります。

（注） Cisco CallManager Release 4.0(1) では、Call Forward All コーリング サーチ スペースが <None> のままである場合、Cisco CallManager は、Forward All を呼び出した回線の回線またはデバイスのコーリング サーチ スペースを使用しません。代わりに、転送される発信デバイスのコーリング サーチ スペースを使用します。

Cisco CallManager における番号操作

Cisco CallManager の番号操作機能は、次のツールが提供しています。

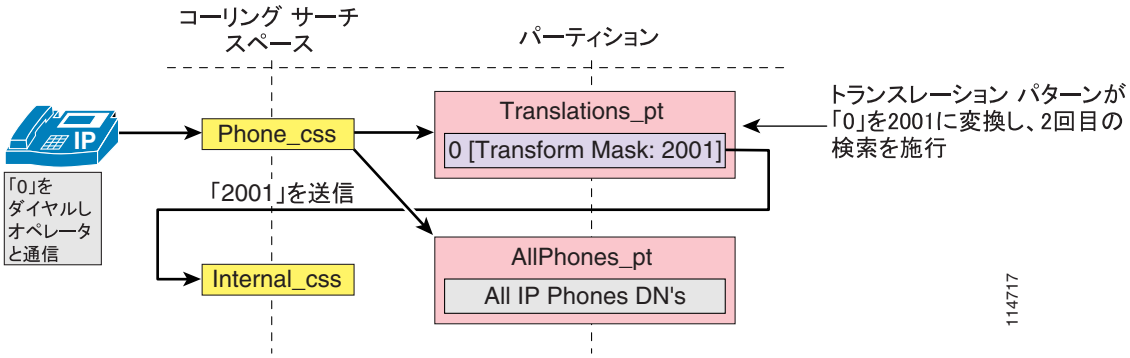
- 外部ルート コンストラクト（ルート パターン、ルート リスト、ルート グループ）
- トランスレーション パターン

外部ルート コンストラクトを使用すると、コールを外部デバイスにルーティングしながら一部の番号操作を実行できます。この機能については、P.10-8 の「Cisco CallManager におけるコール ルーティング」の項で説明しています。

トランスレーション パターンは、Cisco CallManager で最も強力な番号操作ツールであり、あらゆるタイプのコールに対して使用できます。トランスレーション パターンは、ルート パターンと同じ一般規則に従い、同じワイルドカードを使用します。ルート パターンと同じように、トランスレーション パターンをパーティションに割り当てます。しかし、ダイヤルされた数字がトランスレーション パターンと一致する場合、Cisco CallManager は、ゲートウェイなどの外部エンティティにコールをルーティングしません。代わりに、まず変換を実行した後、トランスレーション パターン内で設定されたコーリング サーチ スペースを使用して、コールを再度ルーティングします。

トランスレーション パターンは、図 10-6 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 10-6　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、パターントランスレーション パターン 0 が定義されています。設定済みの Called Party Transform Mask によって、ダイヤル ストリング（0）を新しいストリング 2001 で置き換えるように Cisco CallManager に指示しています。2001 は、オペレータの電話の DN に対応しています。2 回目の（この場合は 2001 の）ルックアップが、Internal_css コーリング サーチ スペースを使用して、コール ルーティング エンジンを通じて強制的に実行されます。この時点で、AllPhones_pt パーティションに含まれている実際のオペレータ DN（2001）までコールを伸ばすことができます。

（注） ダイヤルされた番号をトランスレーション パターンを使用して操作すると、その変換後の番号が、コール詳細レコード（CDR）と IP Phone の Placed Calls ディレクトリに記録されます。ただし、番号操作がルート リスト内で発生した場合、CDR と IP Phone の Placed Calls ディレクトリには、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。

Automated Alternate Routing

Automated Alternate Routing（AAR）機能を使用すると、Cisco CallManager で音声メディア用の代替パスを確立することができます。このパスが確立されるのは、2 つのクラスタ内エンドポイント間にある優先パスで、コール アドミッション制御用のロケーション メカニズムによって決定される使用可能帯域幅が使い果たされたときです。

AAR 機能の主な適用対象は、集中型コール処理配置です。たとえば、支店 A の電話から支店 B の電話にコールする場合、支店間の WAN リンクで使用可能な帯域幅（ロケーション メカニズムによって計算）が不足しているときは、AAR によって公衆網経由でコールを再ルーティングできます。コールの音声パスは、発信元の電話からローカルの（支店 A の）公衆網ゲートウェイまでは IP ベース、このゲートウェイから公衆網を経由して支店 B のゲートウェイまでは TDM ベース、支店 B のゲートウェイから宛先の IP Phone までは IP ベースです。

AAR による処理は、ユーザには見えません。ユーザが着信側電話のオンネット（たとえば 4 桁の）ディレクトリ番号にしかダイヤルできないように AAR を設定すると、公衆網などの代替ネットワーク経由で宛先に到達するときに、ユーザによる追加入力が不要になります。

（注） AAR では、CTI ルート ポイントがコールの発信元や宛先になることはサポートしていません。また、ユーザが複数のサイトにわたってローミングする場合、AAR はエクステンション モビリティ機能と共存できません。詳細については、P.10-23 の「エクステンション モビリティ」を参照してください。

AAR を正常に動作させるには、AAR の次の主要要素を指定する必要があります。

- 宛先公衆網番号の確立（P.10-20）
- 必要なアクセス コードの付加（P.10-21）
- 適切なダイヤル プランおよびルートの選択（P.10-22）

（注） Cisco CallManager Release 4.1.3 以降では、Automated Alternate Routing（AAR）をボイスメール ハント グループのメンバーに適用することができます。

宛先公衆網番号の確立

コールを再ルーティングするには、公衆網などの代替ネットワーク経由でルーティングできる宛先ディレクトリ番号（DN）を使用する必要があります。AAR は、ダイヤルされた番号を使用してコールのクラスタ上での宛先を特定し、この番号を着信側の外部電話番号マスクと結合します。この 2 つの要素を結合することで、代替ネットワークによってルーティング可能な、完全修飾番号（Fully Qualified Number) が生成される必要があります。

たとえば、San Francisco にある電話 A（DN = 2345）から、New York の電話 B 上に設定されているオンネット DN（1234）にダイヤルするとします。ロケーション ベースのコール アドミッション制御によってコールが拒否された場合、AAR は New York の電話の外部電話番号マスク（212555XXXX）を取得して使用し、公衆網上でルーティング可能な完全修飾番号（2125551234）を導出します。

San Francisco から New York へのコールを公衆網でルーティングするには、電話番号のプレフィックスとして「1」が必要です。このプレフィックスは、電話の外部電話番号マスクには含めないことをお勧めします。この電話からオフネットの宛先に発信されるコールでは、このプレフィックスが Calling Party Identification（CallerID）の一部として表示されるためです。代わりに、AAR グループ設定の一部として「1」を追加することをお勧めします。

同じ Cisco CallManager クラスタの内部で複数の国にわたる配置を実現するには、外部電話番号マスクを設定するときに、プレフィックス番号を付けるだけで同じ国または別の国から宛先電話に到達できるようにする必要があります。つまり、国内であることを示すプレフィックス（多くの国では 0）は、それらが E.164 アドレスの一部でない場合、外部電話番号マスクには含めないでください。

この状況を十分に理解するために、London（英国）、Paris（フランス）、Nice（フランス）にサイトがある Cisco CallManager クラスタの例を考えます。Paris の DID 範囲の E.164 アドレスは、+33145678XXX です。ただし、フランスの公衆網内からコールする場合、これらの内線には、通常は 0145678XXX として到達します。

London のオフィスにいる人物が Paris のオフィスに公衆網経由でダイヤルする場合、ダイヤル ストリングは 90033145678XXX です。一方で、Nice のオフィスにいる人物が Paris のオフィスに公衆網経由でダイヤルする場合、ダイヤル ストリングは 00145678XXX です。したがって、Paris のオフィスにある電話の外部電話番号マスクは、通常のフランス国内番号 0145678XXX ではなく、この場合 145678XXX に設定する必要があります。このマスクに 0 を含めた場合、単に追加番号をプレフィックスとして付加するだけでは、ストリング 90033145678XXX を取得できなくなります。

必要なアクセス コードの付加

宛先番号が元の支店のダイヤル プランによって正常にルーティングされるためには、オフネット アクセス コードのプレフィックス（たとえば 9）が必要になる場合もあります。また、発信地点が別のエリア コード（番号計画エリア（NPA）とも呼ばれます）内に配置されている場合、ダイヤル ストリングの一部として、プレフィックス「1」が必要になります。AAR を設定する場合は、DN を AAR グループ内に配置します。AAR グループのペアごとに、同じ AAR グループ内で発信または終端するコールのプレフィックス番号も含めて、その 2 グループ間のコールで DN に追加するプレフィックス番号を設定できます。

一般的な規則として、複数の DN が次の特性をすべて共有している場合は、それらを同じ AAR グループに配置します。

- 共通のオフネット アクセス コード（たとえば 9）
- エリア間コールにおける共通の公衆網ダイヤリング構造（たとえば、北米では 1-NPA-NXX-XXXX）
- 共通の外部電話番号マスク形式

たとえば、San Francisco と New York の両方のサイトで、上の特性がすべて共通しているとします。San Francisco と New York の DN を 1 つの AAR グループに配置して、この AAR グループ内で発生した AAR コールにプレフィックス 91 を付けるようにこのグループを設定します。San Francisco の電話 A が New York の電話 B（212 555 1212）に到達するには、ダイヤル ストリングにプレフィックス 91 を付けるように AAR グループを設定して、全体で 91 212 555 1212 というストリングが完成されるようにします。

複数の国にわたる配置では、通常は国ごとに少なくとも 1 つの AAR グループが必要です。前の項で示した例について考えると、2 つの AAR グループを定義することができます。（London にあるすべての DN に割り当てられる）UK AAR グループと、（Paris と Nice にあるすべての DN に割り当てられる）France AAR グループです。UK AAR グループは、France AAR グループに向かうコールにプレフィックス 90033 を付加するように設定します。一方、France AAR グループは、同じ AAR グループ内でのコールに対して 00 のみをプレフィックスとして付加するようにします。

適切なダイヤル プランおよびルートの選択

AAR コールは、発信元の電話と同じロケーションにあるゲートウェイを通じて出力する必要があります。これによって、完成されたダイヤル ストリングが、発信元サイトのダイヤル プランを通じて送信されます。このように設定するには、Cisco CallManager Administration のデバイス設定ページで、適切な AAR コーリング サーチ スペースを選択します。AAR コーリング サーチ スペース内で、オフネット ダイヤル プラン項目（たとえば、ルート パターン）を、同じ場所にあるゲートウェイを指し、公衆網にコールを転送する前にアクセス コードを削除するように設定します。

たとえば、San Francisco サイトの電話を設定する場合は、91-NPA-NXX-XXXX としてダイヤルされた長距離電話を許可し、アクセス コード（9）を削除して San Francisco のゲートウェイに送信する AAR コーリング サーチ スペースを使用します。

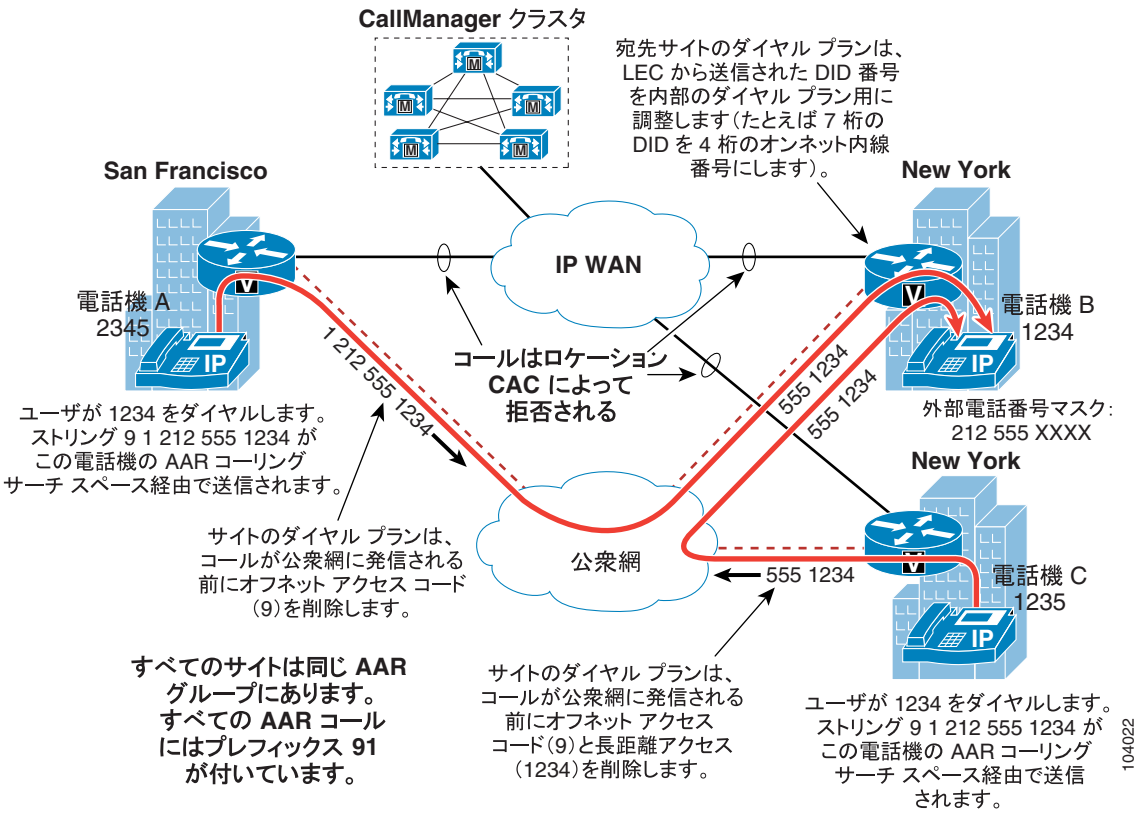
（注） オンネット社内コールを強制的に公衆網コールとしてダイヤルする追加のルート　パターンを設定した場合は、それらのパターンが AAR 機能のものと一致しないことを確認します。詳細については、P.10-47 の「マルチサイト配置用の設計ガイドライン」を参照してください。

同じローカル ダイヤリング エリアに複数のサイトがある場合の特別な考慮事項

場合によっては、ローカルエリア ダイヤリングを使用できるように AAR ダイヤル ストリングをローカルに修正する必要があります。たとえば、New York にある 2 つのサイトが、同じエリア コード 212 を共有しているとします（図 10-7 を参照）。この場合は、91 212 555 1234 としてダイヤルされた番号を 9 555 1234 に変換する必要があります。

この変換を実行する最良の方法は、サイト固有のトランスレーション パターン 91212.555XXXX を設定することです（ドットの前の番号を削除して、先頭に 9 を付加します）。このトランスレーション パターンは、New York サイトの AAR コーリング サーチ スペースのメンバー パーティションにのみ配置します。San Francisco サイトからは、この同じ宛先に 91 212 555 1234 として到達する必要があります。また、New York サイトのダイヤル プランにもこのトランスレーション パターンを配置して、長距離電話としてダイヤルされたローカルに到達可能な番号を適切にルーティングできるようにする必要があります。New York サイトのダイヤル プランでは、9 555 1234 を有効なストリングとして受け付け、このコールを公衆網に送信する前に、ストリングを 555 1234 に変換するようにします。

図 10-7　サイト間 AAR コールにおけるダイヤル番号の変換



（注） AAR 機能は、宛先の電話が到達不能であることが検出されても起動しません。したがって、WAN の障害によって AAR 機能が起動することはありません。

エクステンション モビリティ

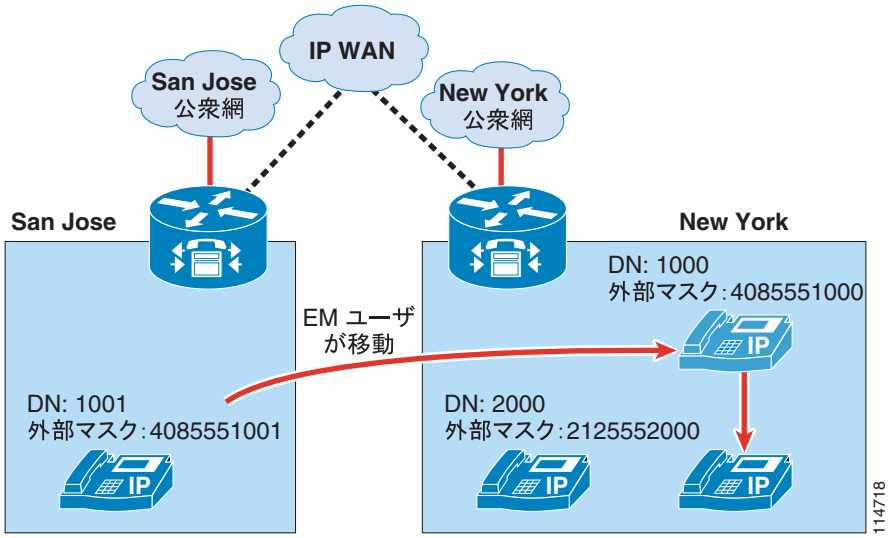
エクステンション モビリティ機能を使用すると、ユーザが IP Phone にログインしたとき、内線番号、短縮ダイヤル、コール特権を含めて、そのユーザのプロファイルが自動的にその電話に適用されるようになります。このメカニズムは、それぞれのエクステンション モビリティ ユーザに関連付けられる、デバイス プロファイルを作成することで成り立っています。デバイス プロファイルは、実質的には仮想 IP Phone であり、1 つまたはそれ以上の回線を設定したり、コール特権や短縮ダイヤルなどを定義したりできます。

IP Phone がログアウト状態になっている（つまり、エクステンション モビリティ ユーザがログインしていない）とき、この IP Phone の特性は、デバイス設定ページと回線設定ページによって決まります。ユーザが IP Phone にログインすると、デバイス設定は変更されませんが、既存の回線設定は Cisco CallManager データベースに保存され、ユーザのデバイス プロファイルの回線設定によって置き換えられます。

エクステンション モビリティの重要な利点の 1 つは、ユーザがどこにいるかにかかわらず、同じ Cisco CallManager クラスタによって制御されている IP Phone にユーザがログインできれば、そのユーザに対して、そのユーザ固有の内線番号で到達できることです。集中型コール処理を使用しているマルチサイト配置に対してエクステンション モビリティを適用すると、地理的に互いに分離している複数のサイトに対して、この機能を展開することができます。

ただし、エクステンション モビリティ機能を P.10-20 の「Automated Alternate Routing」の項で説明している AAR 機能と組み合せる場合は、一定の制限事項があります。図 10-8 に示した例について考えます。エクステンション モビリティと AAR を集中型コール処理の Cisco CallManager クラスタに配置していて、San Jose と New York にそれぞれ 1 つのサイトがあります。

図 10-8　エクステンション モビリティと AAR



この例では、通常 San Jose を拠点としているエクステンション モビリティ ユーザが、DN 1000 と DID 番号 (408) 555-1000 を持っているとします。このユーザの外部電話番号マスクは、4085551000 と設定されています。このユーザが New York サイトに移動し、ログインします。さらに、San Jose と New York 間の IP WAN 帯域幅がすべて使用されているとします。

San Jose にいる内線番号 1001 のユーザが 1000 にコールすると、AAR が呼び出され、発信側の AAR コーリング サーチ スペースと着信側の AAR グループに基づいて、914085551000 への新しいコールが、San Jose の電話によって試行されます。このコールは、San Jose のゲートウェイを使用して公衆網にアクセスしますが、DID (408) 555-1000 が同じゲートウェイによって所有されているため、公衆網はコールをこのゲートウェイに戻します。San Jose のゲートウェイは、内線番号 1000 を持つ電話へのコールを確立しようとしますが、この電話は現在 New York にあります。New York にアクセスするための帯域幅を使用できないため、AAR 機能がもう一度呼び出され、次の 2 つのうち、いずれかのシナリオが発生します。

- ゲートウェイの AAR コーリング サーチ スペースに外部公衆網ルート パターンが含まれている場合、ループが開始され、San Jose サイトにあるすべての公衆網トランクが使い果たされる。
- 逆に、ゲートウェイの AAR コーリング サーチ スペースに内部の番号のみが含まれている場合は、コールが失敗し、発信者にはファースト ビジー トーンが聞こえる。この場合は、1 つの公衆網コールが発生して 1 つが受信されるため、コールのセットアップ中、San Jose のゲートウェイでは 2 つの公衆網トランクが使用されます。

ヒント　ここで説明したようなルーティング ループを阻止するには、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、外部ルート 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 IP Communications の動的な側面を利用しているため、サイト間のコール ルーティングで IP ネットワークを使用する必要があることを中心に説明しています。公衆網に定義されている E.164 番号は静的なものであり、公衆網ネットワークはエクステンション モビリティ ユーザの移動を認識しません。AAR 機能は、コール ルーティングを公衆網に依存しているため、ホーム サイト以外のサイトに移動したエクステンション モビリティ ユーザに対して、この機能を使用して到達することはできません。

（注） ただし、エクステンション モビリティ ユーザが自分のホーム サイトと同じ AAR グループに属するリモート サイトに移動した場合には、使用可能な IP WAN 帯域幅が十分にないとき、そのユーザは AAR 機能を使用して他のサイトへのコールを発信することができます。

ハント リストと回線グループ

「ハント パイロット」は、通常はコール カバレッジや、Skinny Client Control Protocol（SCCP）エンドポイントを通じたコール分配に使用されます。コールの分配には、ハント コンストラクトを使用できます。このハント コンストラクトは、3 層式のアーキテクチャに基づいています。外部コールのルーティングに使用されるアーキテクチャに似たこのアーキテクチャでは、複数層のコール ルーティングと共に、番号操作も可能です。

Cisco CallManager は、着信番号と一致する設定済みハント パイロットを検索し、それを使用して、対応するハント リストを選択します。ハント リストには、コールに使用可能なパスが優先順位順に並べられています。これらのパスは、「回線グループ」と呼ばれます。図 10-9 では、Cisco CallManager Release 4.1 のハント コンストラクトの 3 層式アーキテクチャを示しています。

（注） Cisco CallManager Release 3.3 以前では、コール カバレッジ機能はハント グループによって提供されていました。このグループは、Telephony Call Dispatcher（TCD）サービスによって制御され、Cisco Attendant Console によっても使用されます。Cisco CallManager Release 4.0 では、ハント パイロット、ハント リスト、および回線グループが導入されました。ただし、このリリースでは、ハント パイロット構造はルート パターン構造と組み合せられ、ハント リストはルート リストと組み合せられていました。Cisco CallManager Release 4.1 では、これらの構造は独立しています。表 10-3 では、Cisco CallManager Release 4.0 と 4.1 のハント リストと回線グループ、および Cisco CallManager Release 3.3 以前で Attendant Console を使用したハント グループの機能比較を示しています。

表 10-3　ルート リスト、ハント リスト、ハント パイロット、ハント グループの機能比較

機能	Cisco CallManager Release 3.3 以前のハント グループ	Cisco CallManager Release 4.0 のルート リストとハント リスト	Cisco CallManager Release 4.1 のハント パイロット
Skinny Client Control Protocol（SCCP）エンドポイント	あり	あり（回線グループ）	あり
ゲートウェイとトランク（オフネットの宛先）	なし	あり（ルート グループ）	なし
トップダウン アルゴリズム	あり	あり	あり
循環アルゴリズム	あり	あり	あり
最長アイドル時間アルゴリズム	あり	あり	あり
ブロードキャスト アルゴリズム	あり	あり	あり

表 10-3　ルート リスト、ハント リスト、ハント パイロット、ハント グループの機能比較（続き）

機能	Cisco CallManager Release 3.3 以前のハント グループ	Cisco CallManager Release 4.0 のルート リストとハント リスト	Cisco CallManager Release 4.1 のハント パイロット
ハント オプション	なし	あり	あり
無応答時の復帰	なし	あり	あり
パフォーマンスの監視（PerfMon）	なし	あり	あり
SCCP ボイスメール ポート（Cisco Unity）	なし	あり（回線グループ）	あり
Simplified Message Desk Interface（SMDI）ボイスメール システム	あり	あり	あり
キューイング	あり	なし	なし
ハント グループとハント パイロットのリンク	あり	なし	あり

比較のために、図 10-9 に Cisco CallManager 4.1 のハント パイロットのアーキテクチャを示し、図 10-10 に Cisco CallManager 4.0 のハント パイロットのアーキテクチャを示します。

図 10-9　Cisco CallManager Release 4.1 のハント アーキテクチャ

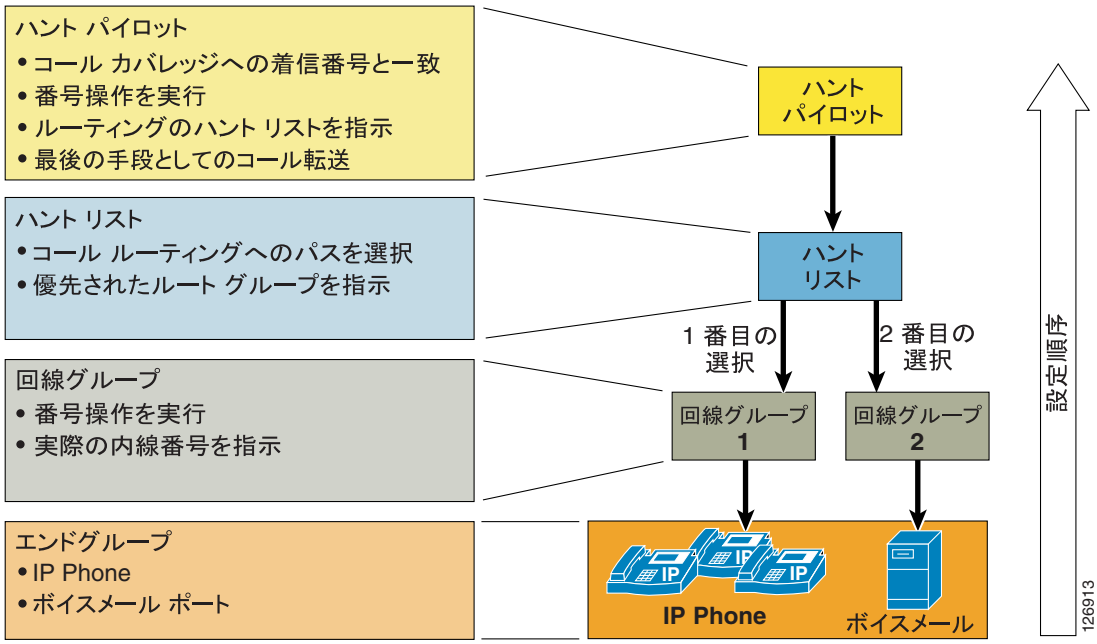
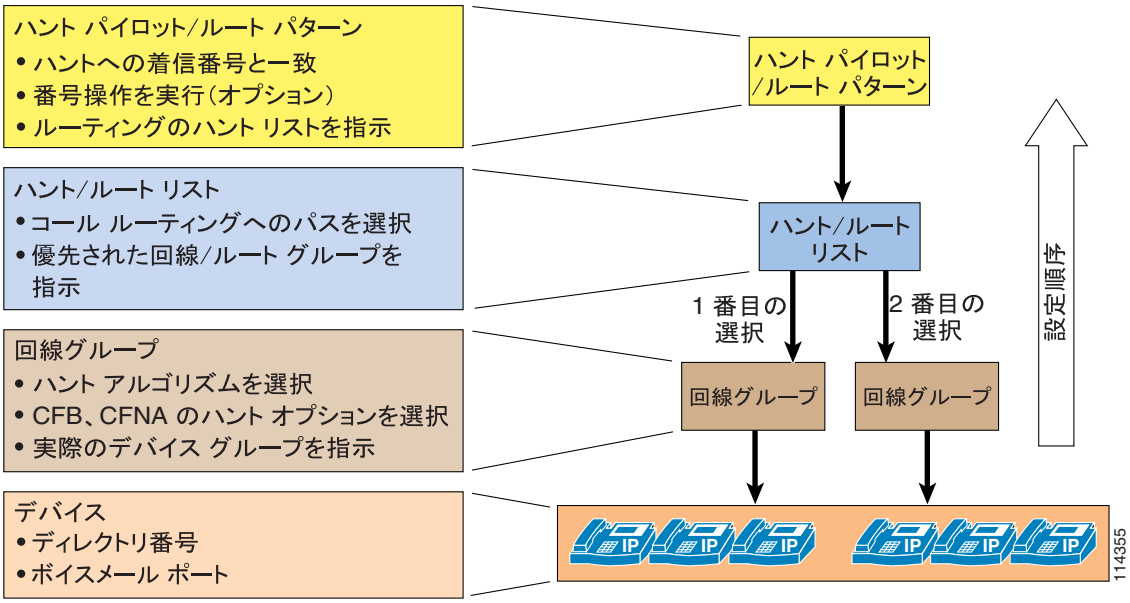


図 10-10　Cisco CallManager Release 4.0 のハント アーキテクチャ



ハント パイロット

ハント パイロットは、コールをディレクトリ番号にルーティングするために Cisco CallManager で設定された、ルート パターンのように数字とワイルドカードを組み合せたストリング（たとえば、9.[2-9]XXXXXX）です。ハント パイロットは、ハント リストを直接指しています。ハント リストは回線グループを指しており、回線グループは、最終的に SCCP エンドポイントを指しています。

Cisco CallManager Release 4.1 以降では、ハンティングが次のいずれかまたは両方の理由で失敗した場合、コールを最終的な宛先に転送することができます。

- すべてのハンティング オプションを使い果たしても、コールはまだ応答されていない。
- タイムアウト期間が満了した。

このコール転送は、Hunt Pilot 設定ページの Hunt Forward Settings セクションで設定します。この転送の宛先は、次のいずれかから選択できます。

- Cisco CallManager の内部コール ルーティング テーブルに含まれている、特定のパターン。
- 個人用プリファレンス。このプリファレンスは、元々の着信番号の Call Forward No Coverage 設定を指しています。

たとえば、個人用プリファレンス オプションを実装するには、Forward No Answer フィールドに従ってコールをハント パイロットへ転送するようにユーザの電話を設定して、コールに応答できるユーザが他にいないかどうか検索できるようにします。すべてのハンティング オプションが使い果たされたか、タイムアウト期間が満了したためにコール ハンティングが失敗した場合、コールを当初の宛先ユーザの個人設定宛先に転送することができます。たとえば、ユーザの DN 設定ページにある Forward No Coverage フィールドにボイスメール番号を設定すると、ハンティングが失敗した場合、コールはそのユーザのボイスメール ボックスに送信されます。

（注） Cisco CallManager Release 4.0 では、コール転送をサポートしていません。

ハント パイロットの処理するコールには、次の考慮事項が適用されます。

- コール ピックアップとグループ コール ピックアップは、ハント パイロットが分配するコールではサポートされません。回線グループのメンバーは、回線グループの他のメンバーに提供されたハント パイロット コールについては、メンバー同士が同じコール ピックアップ グループに属している場合でもピックアップできません。
- ハント パイロット番号に基づいて分配されるコールは、回線グループ内のディレクトリ番号に対して設定される、個別の自動転送処理をサポートしていません。このため、Immediate Divert（iDivert）ソフトキーや、ディレクトリ番号に対して設定されている自動転送は、ハント パイロットが分配するコールに対しては機能しません。回線グループの設定でハント オプションとして使用できる自動転送条件のみが、ハント パイロット コールに適用されます。ただし、iDivert ソフトキーや自動転送設定は、ハント パイロットが分配したコールを除く、すべての着信コールで機能します。
- ハント パイロットは、自身の回線グループのメンバーとハント パイロットが別のパーティションに配置されている場合でも、コールを自身の回線グループのいずれかのメンバーに分配できます。ハント パイロットが分配するコールは、すべてのパーティションおよびコーリング サーチ スペース制限を上書きします。

ハント リスト

ハント リストは、コール カバレッジに使用できるパス（回線グループ）が優先順位順に並べられたリストです。ハント リストには次の特性があります。

- 複数のハント パイロットが同一ハント リストを指すことができます。
- ハント リストは、所定の宛先への代替パスの役目を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。ハント リストを使用すると、たとえば、コールを特定サイト内や一部の他のリモート サイトで分配することができます。
- ハント リストは、番号操作は一切実行しません。
- 複数のハント リストに、同じ回線グループを含めることができます。

回線グループ

回線グループのメンバーは、Cisco CallManager が制御しているユーザ内線番号です。このため、コールを回線グループのメンバー間に分配するときは、Cisco CallManager がコールを制御します。コールが応答されなかった場合や、内線番号が使用中または未登録の場合は、ハント オプションをコールに適用できます。

回線グループは、コールが分配される順序を制御し、次の特性を持っています。

- 回線グループは、特定の内線番号（通常は、IP Phone 内線番号またはボイスメール ポート）を指しています。
- 1 つの内線番号が複数の回線グループに含まれていることがあります。
- コンピュータ / テレフォニー インテグレーション（CTI）ポートと CTI ルート ポイントは、回線グループに追加できません。したがって、CTI アプリケーション（Cisco Customer Response Solutions（CRS）や IP 音声自動応答装置（IP IVR）など）を通じて制御されるエンドポイントには、コールを分配できません。
- Cisco CallManager は、割り当てられている分配アルゴリズムに従ってコールをデバイスに分配します。Cisco CallManager では、次のアルゴリズムをサポートしています。
  - トップダウン
  - 循環
  - 最長アイドル時間
  - ブロードキャスト

- No-Answer、Busy、Not-Available のいずれかのイベントが発生すると、分配されたコールを回線グループがハント オプションに基づいて内線番号に転送します。Cisco CallManager では、次のハント オプションをサポートしています。
  - 次のメンバーにアクセスし、その後はハント リスト内の次のグループにアクセスする。
  - 次のメンバーにアクセスするが、次のグループにはアクセスしない。
  - 残りのメンバーをスキップして、次のグループに直接アクセスする。
  - ハンティングを停止する。

ハント アルゴリズムとハント オプションの詳細については、次の Web サイトで入手可能な『*Cisco CallManager Administration Guide*』を参照してください。

http://www.cisco.com

回線グループ デバイス

回線グループ デバイスは、回線グループがアクセスするエンドポイントであり、次のいずれかのタイプに該当します。

- Skinny Client Control Protocol（SCCP）エンドポイント（Cisco IP Phone、VG248、ATA 188 など）
- ボイスメール ポート（Cisco Unity）
- H.323 クライアント
- MGCP ゲートウェイに接続されている FXS

時間帯ルーティング

Cisco CallManager Release 4.1 では、Time-of-Day（ToD）ルーティング機能が導入されました。この機能を使用するには、次の要素を設定します。

- 期間
- タイム スケジュール

期間を利用すると、営業開始時刻と終了時刻を設定できます。この開始時刻と終了時刻は、コールをルーティングできる期間を示しています。これらの時刻に加えて、毎週または毎年発生するイベントを設定することもできます。さらに、Start Time オプションと End Time オプションにある No business hours を選択して、休業時間を設定することもできます。このオプションを選択した場合は、すべての着信コールがブロックされます。

タイム スケジュールは、パーティションに割り当てられている特定の期間をグループにまとめたものです。このタイム スケジュールによって、指定した期間中にパーティションがアクティブまたは非アクティブのどちらになっているかが判断されます。一致したパターンやダイヤリング パターンには、そのダイヤリング パターンの配置されているパーティションがアクティブになっている場合のみ到達できます。

図 10-11 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 10-11　時間帯ルーティング

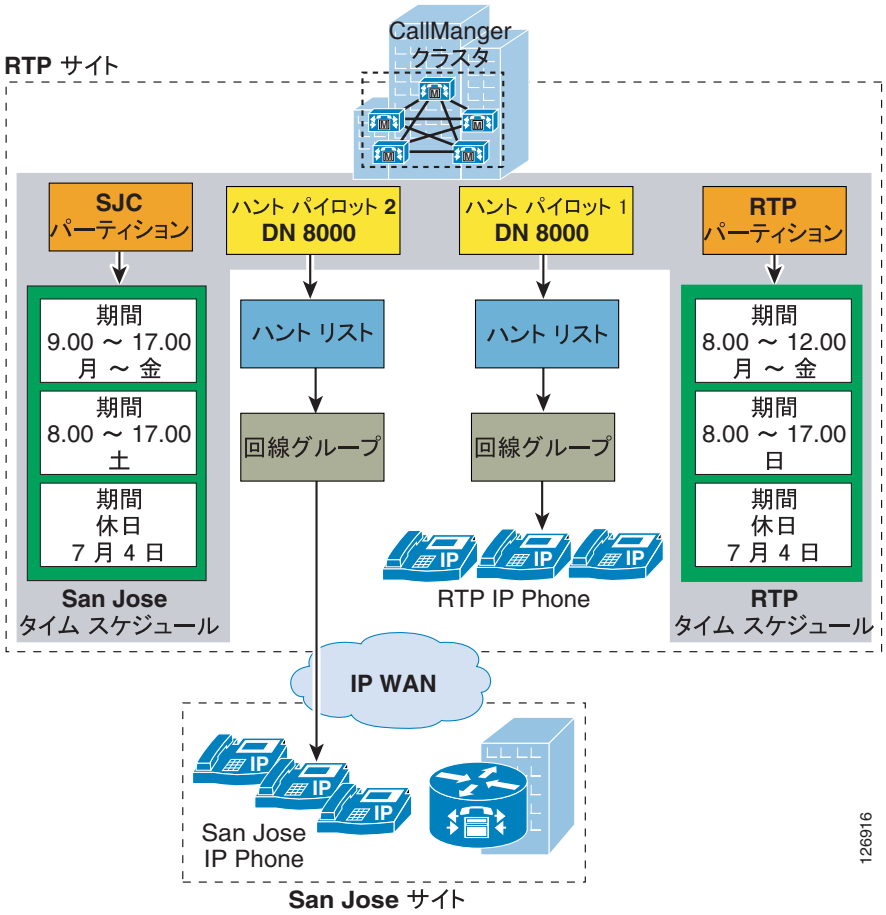


図 10-11 の例では、水曜日の午後 3 時にハント パイロット（8000）に着信したコールは、SJC の電話に転送されます。一方、このハント パイロットに 7 月 4 日にコールした人は、別のパターンが 8000 に一致しない限り、ファースト ビジー トーンを受信します。

H.323 ダイヤル ピアを使用する Cisco IOS でのコール ルーティング

H.323 プロトコルを使用する Cisco IOS ルータ上でのコール ルーティング ロジックは、ダイヤル ピア コンストラクトに依存しています。ダイヤル ピアは、スタティック ルートに似たものです。コールの発信地点と終端地点、およびコールがネットワークで通過するパスを定義しています。ダイヤル ピアは、コールの発信元と宛先のエンドポイントを指定するため、およびコール接続の各コール レッグに適用される特性を定義するために使用します。ダイヤル ピアに含まれている属性によって、ダイヤルされるどの番号をルータが収集し、テレフォニー デバイスに転送するかが決まります。

ダイヤル ピアおよびその設定の詳細については、次の Web サイトで入手可能な『*Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*』の「Configuring Dial Plans, Dial Peers, and Digit Manipulation」を参照してください。

http://www.cisco.com

ダイヤル ピアを使用したコール ルーティングを理解するための鍵の 1 つは、着信コール レッグと発信コール レッグ、つまり着信ダイヤル ピアと発信ダイヤル ピアという概念です。Cisco IOS ルータを経由する各コールは、2 つのコール レッグを持っていると見なされます。1 つはルータに入るもので、1 つはルータから出るものです。ルータに入るコール レッグが「着信コール レッグ」であり、ルータから出るコール レッグが「発信コール レッグ」です。

コール レッグには、主に次の 2 つのタイプがあります。

- ルータを公衆網、アナログ電話機、または PBX に接続する、従来の TDM テレフォニー コール レッグ
- ルータを他のゲートウェイ、ゲートキーパー、または Cisco CallManager に接続する、IP コール レッグ

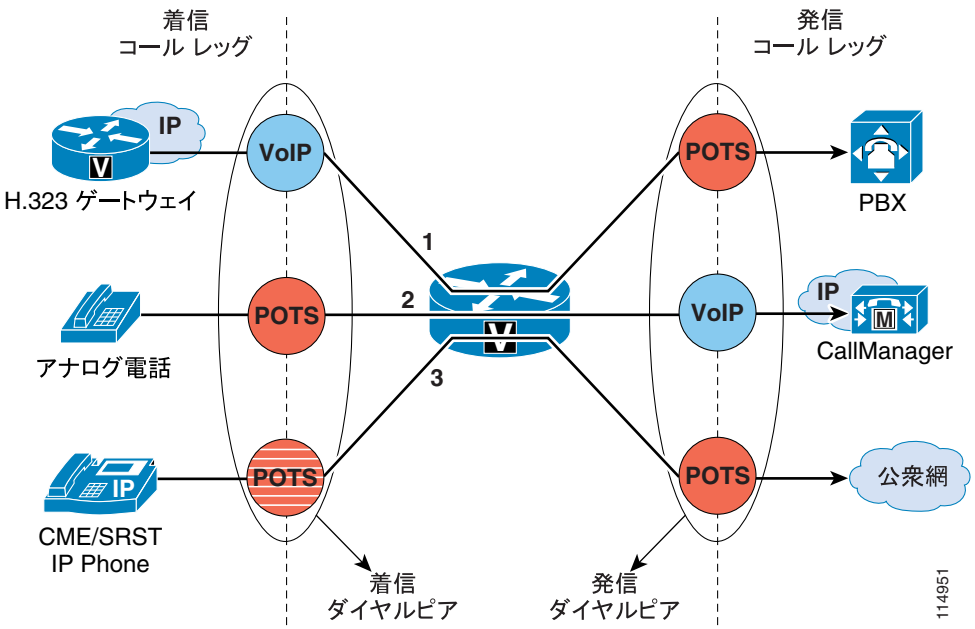
Cisco IOS は、ルータを通過するすべてのコールについて、1 つのダイヤル ピアを各コール レッグに関連付けます。ダイヤル ピアにも、関連付け先となるコール レッグのタイプに応じて、次に示す主に 2 つのタイプがあります。

- 従来の TDM テレフォニー コール レッグに関連付けられる、POTS ダイヤル ピア
- IP コール レッグに関連付けられる、VoIP ダイヤル ピア

図 10-12 では、Cisco IOS ルータを通過する、次の各種コールの例を示しています。

- コール 1 は、IP ネットワークにある別の H.323 ゲートウェイから、ルータに接続されている従来の（たとえば、PRI インターフェイス経由の）PBX までです。このコールに対しては、着信 VoIP ダイヤル ピアと発信 POTS ダイヤル ピアが選択されます。
- コール 2 は、ルータの FXS ポートに接続されているアナログ電話機から、IP ネットワークにある Cisco CallManager クラスタまでです。このコールに対しては、着信 POTS ダイヤル ピアと発信 VoIP ダイヤル ピアがルータによって選択されます。
- コール 3 は、Cisco CallManager Express または SRST の制御する IP Phone から、ルータ上の公衆網インターフェイス（たとえば、PRI インターフェイス）までです。このコールに対しては、自動生成の POTS ダイヤル ピア（ルータ上に設定されている **ephone** に対応します）と発信 POTS ダイヤル ピアが選択されます。

図 10-12　着信ダイヤル ピアと発信ダイヤル ピア



着信コール レッグを着信ダイヤル ピアと対応付けるために、ルータは、セットアップ メッセージ内の情報要素（着信番号 /DNIS と発信番号 /ANI）が 4 つの設定可能ダイヤル ピア属性と一致するかどうか調べることによって、ダイヤル ピアを選択します。ルータは、これらの項目が一致するかどうかを次の順序で調べます。

1. 着信番号と **incoming called-number**
2. 発信番号と **answer-address**
3. 着信番号と **destination-pattern**
4. 着信音声ポートと設定済み音声ポート

ルータで必要となるのは、これらの条件のいずれか 1 つのみ一致することです。すべての属性をダイヤル ピア内に設定する必要はなく、すべての属性がコール セットアップ情報に一致している必要はありません。ルータがダイヤル ピアを選択するために必要な条件は 1 つのみです。ルータは、1 つのダイヤル ピアが一致するとすぐに検索を停止し、コールは設定済みのダイヤル ピア属性に従ってルーティングされます。一致するダイヤル ピアが他にある場合でも、最初に一致したピアのみが使用されます。

ルータが発信ダイヤル ピアを選択する方法は、着信 POTS ダイヤル ピアに **direct-inward-dial**（DID）が設定されているかどうかによって異なります。

- 着信 POTS ダイヤル ピアに DID が設定されていない場合、ルータは 2 段階ダイヤリングを実行し、着信ダイヤル ストリングを 1 桁ずつ収集します。1 つのダイヤル ピアが宛先パターンに一致すると、ルータは一致したダイヤル ピアの設定済み属性を使用して、コールをただちに発信します。
- 着信 POTS ダイヤル ピアに DID が設定されている場合、ルータは着信番号全体を使用して、発信ダイヤル ピアに含まれている宛先パターンに一致するかどうかを調べます。DID を使用する場合は、コールのルーティングに必要な番号がセットアップ メッセージにすべて含まれているため、番号をそれ以上収集する必要がありません。複数のダイヤル ピアがダイヤル ストリングに一致した場合、一致するすべてのダイヤル ピアが「ハント グループ」の形成に使用されます。ルータは、発信コール レッグを確立できるまで、ハント グループに含まれているすべてのダイヤル ピアを使用して確立を試行します。

デフォルトでは、ハント グループ内のダイヤル ピアは、次の基準を使用して、この順序に従って選択されます。

1. 電話番号の最長一致

   この方法では、ダイヤルされた番号と一致している部分が最も長い宛先パターンが選択されます。たとえば、あるダイヤル ピアがダイヤル ストリング 345.... を使用して設定され、2 番目のダイヤル ピアが 3456789 を使用して設定されている場合、ルータはまず 3456789 を選択します。2 つのダイヤル ピアのうち、正確に一致している部分が最も長いためです。

2. 明示的プリファレンス

   この方法では、**preference** ダイヤル ピア コマンドで設定した優先順位を使用します。プリファレンスの数値が小さくなるほど、優先順位が高くなります。最高の優先順位は、プリファレンス順位 0 のダイヤル ピアに与えられます。同じ宛先パターンを持つ複数のダイヤル ピアに対して同じ優先順位が定義されている場合、ダイヤル ピアはランダムに選択されます。

3. ランダム選択

   この方法では、すべての宛先パターンが同等の重みになります。

このデフォルト選択順序を変更することも、**dial-peer hunt** グローバル設定コマンドを使用して、別のダイヤル ピア ハンティング方法を選択することもできます。この他の選択基準は、「最長待機時間」です。最後に選択された時点から、最も長く待機している宛先パターンを選択します（Cisco CallManager 回線グループの「最長アイドル時間」に相当します）。

Cisco IOS ルータ上で H.323 ダイヤル ピアを設定するときは、次のベスト プラクティスに従ってください。

- 着信公衆網コールが　DNIS　情報に基づいて宛先に直接ルーティングされるようにするには、**direct-inward-dial** 属性を使用して、次のようにデフォルト POTS ダイヤル ピアを作成します。

```
dial-peer voice 999 pots
  incoming called-number .
  direct-inward-dial
  port 1/0:23
```

- ルータを Cisco CallManager クラスタに接続されている H.323 ゲートウェイとして使用する場合は、同じ宛先パターンを持ち、2 つの異なる Cisco CallManager サーバを指す VoIP ダイヤル ピアを少なくとも 2 つ設定して、冗長性を実装します。プライマリとセカンダリの Cisco CallManager サーバ間での優先順位を選択するには、**preference** 属性を使用します。

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 CallManager Express および Cisco CallManager のクラスタ、H.323 端末、ゲートウェイ、マルチポイント コントロール ユニット（MCU）など）を管理するためのオプション ノードです。これらのエンドポイントに対して、コール ルーティング機能とコール アドミッション制御機能を提供します。エンドポイントは、H.323 Registration Admission Status（RAS）プロトコルを使用してゲートキーパーと通信します。

エンドポイントは、起動するとゲートキーパーへの登録を試行します。他のエンドポイントとの通信が必要な場合は、E.164 アドレスや電子メール アドレスなど、自身のシンボリック エイリアスを使用して、コールを開始するための許可を要求します。ゲートキーパーは、そのコールを許可してもよいと判断した場合、宛先の IP アドレスを発信元エンドポイントに返します。この IP アドレスは、宛先エンドポイントの実際の IP アドレスではなく、中継アドレスである場合もあります。たとえば、IP-to-IP ゲートウェイや、コール シグナリングをルーティングするゲートキーパーのアドレスです。

H.323 プロトコル、および H.323 エンドポイントとゲートキーパーとのメッセージ交換の詳細については、次の Web サイトで入手可能な『*Cisco IOS H.323 Configuration Guide*』を参照してください。

http://www.cisco.com

Cisco 2600、3600、3700、2800、3800、および 7200 シリーズのルータはすべて、ゲートキーパー機能をサポートします。冗長性、ロード バランシング、および階層コール ルーティング用に、さまざまな方法で Cisco IOS ゲートキーパーを設定できます。ここでは、ゲートキーパー機能のコール ルーティング機能を中心に説明します。冗長性とスケーラビリティに関する考慮事項については、P.8-19 の「ゲートキーパーの冗長性」を参照してください。コール アドミッション制御に関する考慮事項については、P.9-7 の「ゲートキーパー」を参照してください。

Cisco IOS ゲートキーパーのコール ルーティングは、次のタイプの情報に基づいています。

- 静的に設定されている情報（ゾーン プレフィックスや、デフォルト テクノロジー プレフィックスなど）
- 動的な情報（登録フェーズで H.323 デバイスが提供した E.164 アドレスやテクノロジー プレフィックスなど）
- コールごとの情報（着信番号やテクノロジー プレフィックスなど）

ゾーンは、エンドポイント、ゲートウェイ、MCU などの、ゲートキーパーに登録される H.323 デバイスの集合です。アクティブになることができるゲートキーパーは、ゾーンごとに 1 つのみです。1 つのゲートキーパーには、ローカル ゾーンを 100 個まで定義できます。

H.323 エンドポイントがゲートキーパーに登録すると、エンドポイントはゾーンに割り当てられます。また、処理できるコールの種類（音声、ビデオ、ファックスなど）を指定するテクノロジー プレフィックスとともに、処理を担当している 1 つまたはそれ以上の E.164 アドレスを登録することもできます。

ゾーンごとに、ゲートキーパー上で 1 つまたはそれ以上の「ゾーン プレフィックス」を設定できます。ゾーン プレフィックスは、番号とワイルドカードを含んだストリングであり、ゲートキーパーがコール ルーティングの判断に使用します。ゾーン プレフィックス ストリングでは、次の文字を使用できます。

- 0 ～ 9 までのすべての数字。それぞれが特定の 1 桁に対応
- ドット（.）ワイルドカード。いずれかの 1 桁の 0 ～ 9 までの数字に対応
- * ワイルドカード。1 またはそれ以上の桁の 0 ～ 9 までの数字に対応

ゲートキーパーのコール ルーティング動作を理解するには、メッセージ解析ロジックについて考えると役立ちます。図 10-13 では、アドミッション要求（ARQ）の解析ロジックを示しています。エンドポイントは、コールを初期化するために、ARQ（Admission Request ; アドミッション要求）をゲートキーパーに送信します。ARQ には、宛先つまり着信側の H.323 ID または E.164 アドレスのどちらか、および送信元つまり発信側の E.164 アドレスまたは H.323 ID が含まれています。

ARQ に E.164 アドレスが入っている（Cisco CallManager では、ARQ には常に E.164 アドレスが入っています）場合、ARQ にはテクノロジー プレフィックスが含まれている場合と、含まれていない場合があります。ARQ にテクノロジー プレフィックスが含まれている場合、ゲートキーパーはテクノロジー プレフィックスを着信番号から削除します。ARQ にテクノロジー プレフィックスが含まれていない場合、ゲートキーパーは、デフォルトのテクノロジー プレフィックスが設定されていれば、それを使用します（P.10-37 の「集中型ゲートキーパー設定」の項の **gw-type-prefix** コマンドを参照）。このように取得したテクノロジー プレフィックスは、メモリに格納され、ゲートキーパーはコール ルーティング アルゴリズムに基づく処理を続行します。

次に、ゲートキーパーは、着信番号が設定済みのいずれかのゾーン プレフィックスに一致しないかどうかを調べます。一致する可能性のあるエントリが複数ある場合は、一致する部分の最も長いものが使用されます。一致するゾーン プレフィックスがない場合、未知のプレフィックスを持つコールを受け付けるようにゲートキーパーが設定されているときは、ゲートキーパーは宛先ゾーンが発信元ゾーンと同じであると想定します。

この時点で、ゲートキーパーは選択された宛先ゾーン内を検索して、着信番号に一致する登録済み E.164 アドレスがあるかどうかを調べます。一致が見つかると、コールに関して要求した帯域幅が使用可能になっていて、着信側エンドポイントがゲートキーパーに登録されている場合、ゲートキーパーはアドミッション確認（ACF）を送信します。ACF には、宛先エンドポイントの IP アドレスが入っています。帯域幅が使用不能であるか、着信側エンドポイントが登録されない場合、ゲートキーパーは、発信側エンドポイントに ARJ（Admission Reject ; アドミッション拒否）を戻します。

一致する E.164 アドレスが宛先ゾーン内に登録されていない場合、ゲートキーパーは、以前に格納したテクノロジー プレフィックスを使用して、そのゾーンに登録されているゲートウェイをコールの宛先として選択します。ゲートキーパーが ACF または ARJ のどちらを発信元エンドポイントに送信するかは、帯域幅の可用性とエンドポイントの登録に関する、上と同じ考慮事項に基づいて決まります。

送信元エンドポイントは、ゲートキーパーから ACF を受信した後、ACF で戻された IP アドレスを使用して、直接セットアップ メッセージを宛先エンドポイントに送信できます。

図 10-13　ARQ のゲートキーパー アドレス解決

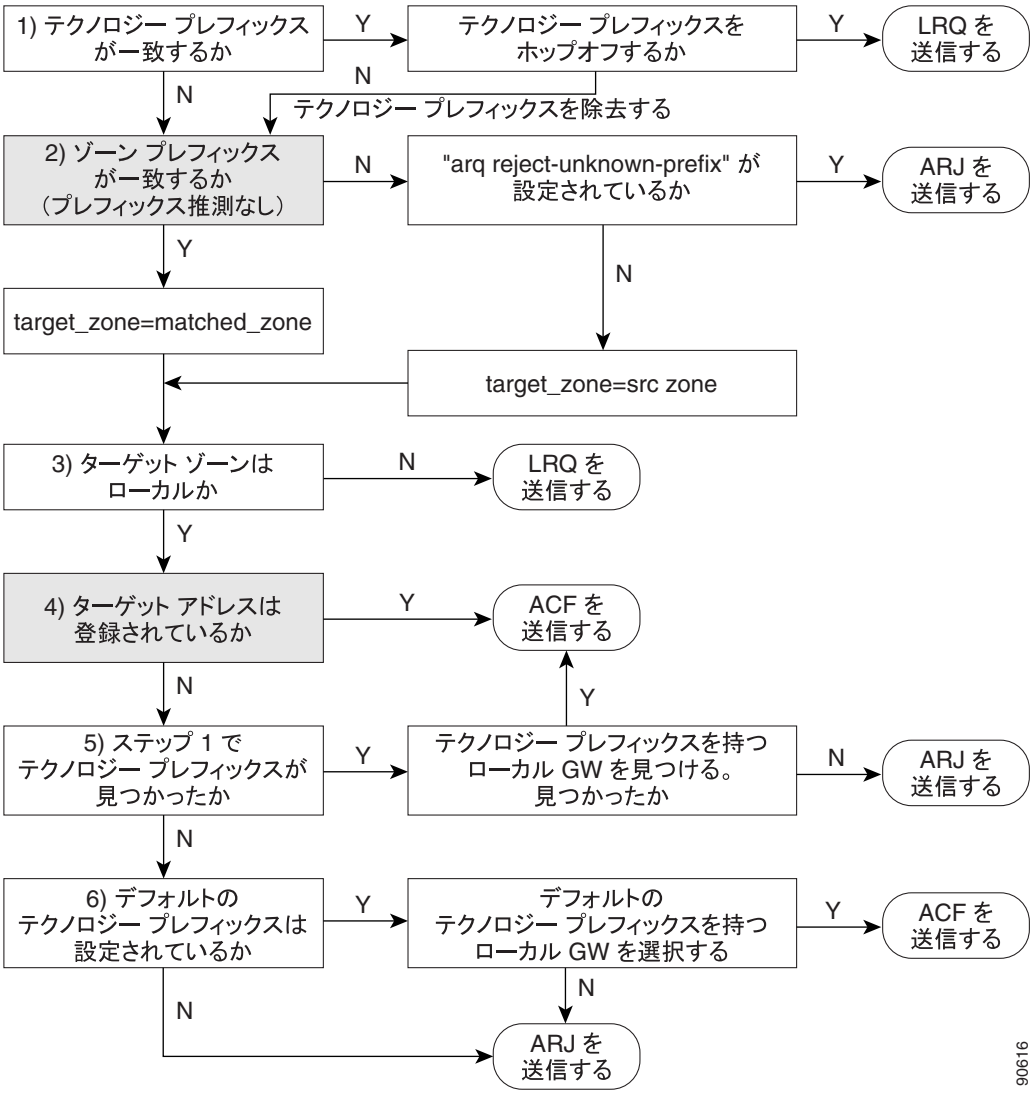
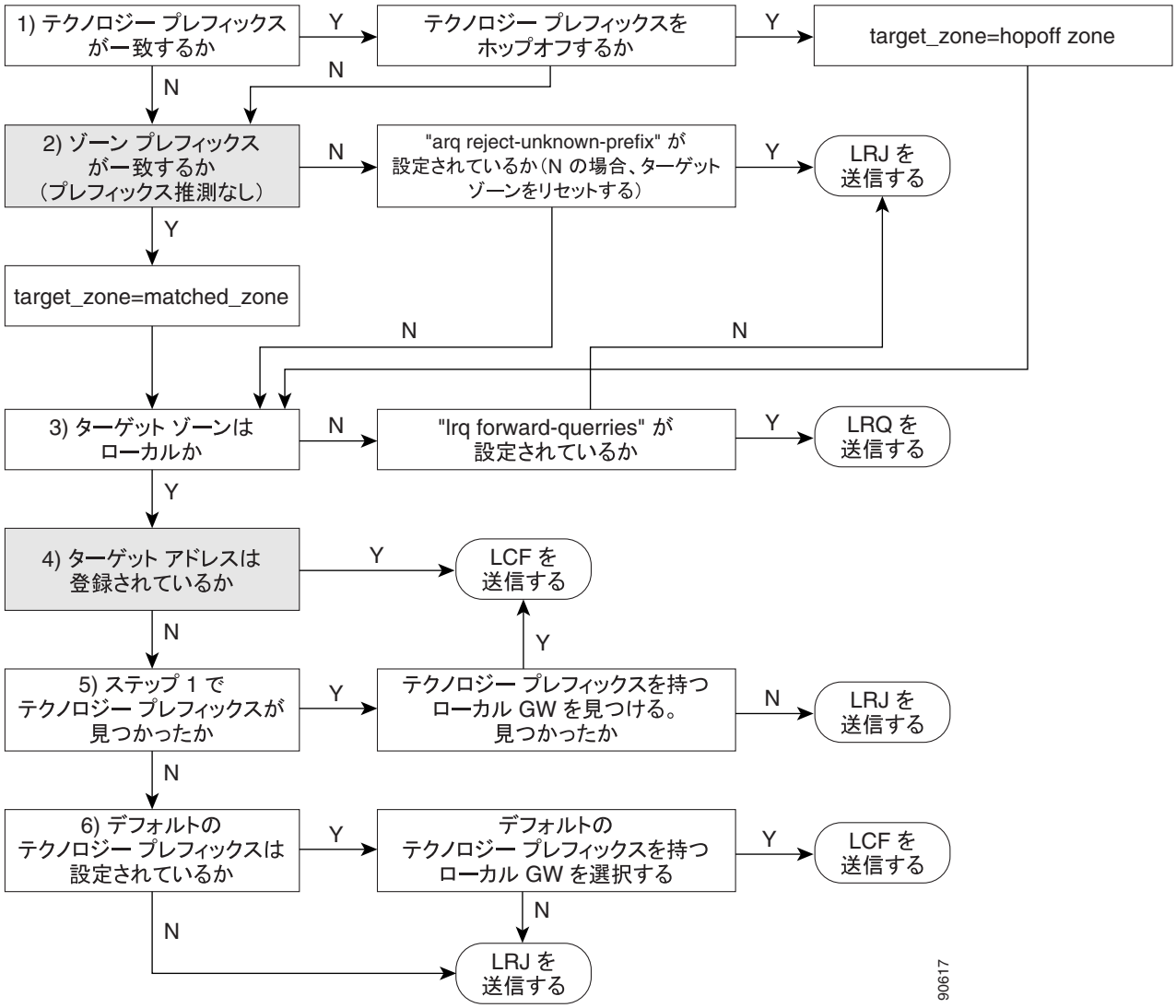


図 10-14 では、ロケーション要求（LRQ）の解析ロジックを示しています。LRQ メッセージは、ゲートキーパー間で交換され、ゾーン（リモート ゾーン）間のコールに使用されます。たとえば、ゲートキーパー A が ARQ をローカル ゾーンのゲートウェイから受信し、その ARQ は、リモート ゾーンのデバイスに対するコール アドミッションを要求しているとします。ゲートキーパー A は、ゲートキーパー B に LRQ メッセージを送信します。ゲートキーパー B は、自身がゾーン間コール要求を許可するように設定されているかどうか、および要求されたリソースが登録されているかどうかに応じて、この LRQ メッセージにロケーション確認（LCF）メッセージまたはロケーション拒否（LRJ）メッセージで応答します。

図 10-14　LRQ のゲートキーパー アドレス解決



従来の Cisco IOS ゲートキーパー機能は、「中継ゾーン」ゲートキーパーという概念を通じて、IP-to-IP ゲートウェイに対応するように拡張されました。配置の例については、P.9-15 の「IP-to-IP ゲートウェイ」を参照してください。

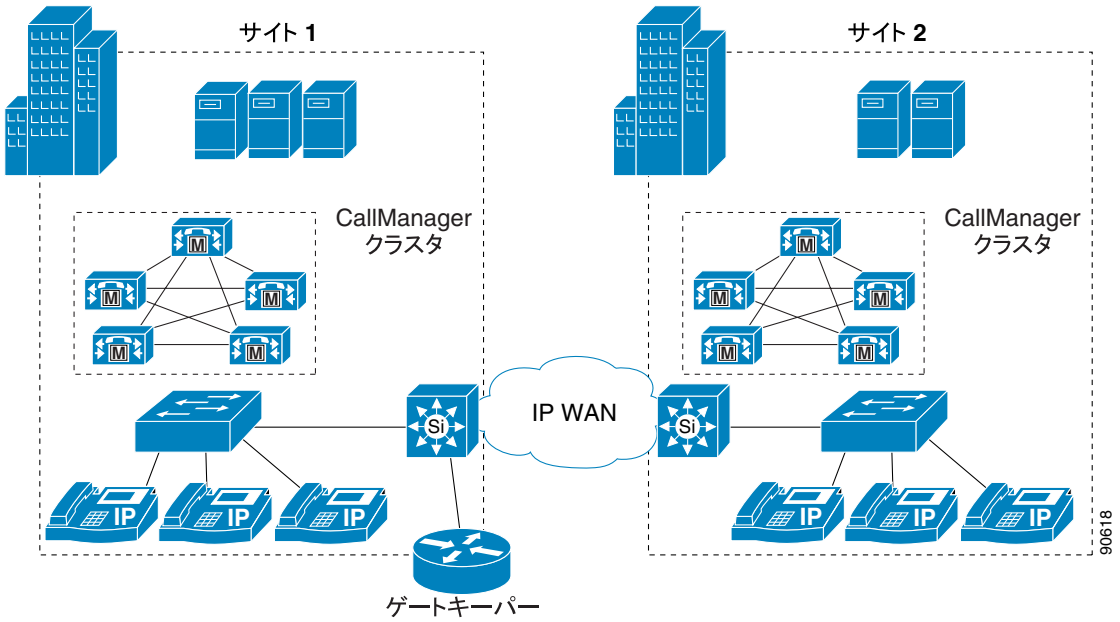
中継ゾーン ゲートキーパーがレガシー ゲートキーパーと異なっている点は、コール ルーティングでの LRQ メッセージと ARQ メッセージの使用方法です。中継ゾーン ゲートキーパーを使用しても、通常のクラスタおよび機能はそのまま使用できます。レガシー ゲートキーパーは、着信する LRQ を着信番号に基づいて検査します。具体的には、LRQ の destinationInfo 部分にある dialedDigits フィールドを検査します。中継ゾーン ゲートキーパーは、着信番号を検査する前に LRQ の発信地点を検査します。LRQ が、中継ゾーン ゲートキーパーのリモート ゾーン設定にリストされているゲートキーパーから送信されている場合、ゲートキーパーは、ゾーンのリモート設定に **invia** キーワードまたは **outvia** キーワードが含まれているかどうかを確認します。設定にこれらのいずれかのキーワードが含まれている場合、ゲートキーパーは中継処理をします。含まれていない場合は、従来の処理をします。

ARQ メッセージの場合、ゲートキーパーは宛先ゾーンに **outvia** キーワードが設定されているかどうかを調べます。**outvia** キーワードが設定されていて、**outvia** キーワードを使用して命名されているゾーンがゲートキーパーに対してローカルである場合は、そのゾーンの IP-IP ゲートウェイに ACF ポインティングが返され、コールは IP-IP ゲートウェイに転送されます。**outvia** キーワードを使用して命名されているゾーンがリモートである場合、ゲートキーパーは、ロケーション要求（LRQ）をリモート ゾーンのゲートキーパーではなく **outvia** ゲートキーパーに送信します。**invia** キーワードは、ARQ の処理では使用されません。

集中型ゲートキーパー設定

単一のゲートキーパーは、クラスタ間のコール ルーティング、および最大 100 の Cisco CallManager クラスタに対するコール アドミッション制御をサポートできます。図 10-15 では、2 つの Cisco CallManager クラスタと単一の集中型ゲートキーパーを備えた分散型コール処理環境を示しています。

図 10-15　2 つのクラスタをサポートする集中型ゲートキーパー



例 10-1 では、図 10-15 のゲートキーパー設定を示しています。

例 10-1　集中型ゲートキーパーの設定

```
gatekeeper
 zone local GK-Site1 customer.com 10.1.10.100
 zone local GK-Site2 customer.com
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth interzone GK-Site1 160
 bandwidth interzone GK-Site2 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、図 10-15 について説明します。

- Cisco CallManager トランク登録をサポートするために、各 Cisco CallManager クラスタにはローカル ゾーンが設定されます。
- ゾーン間とクラスタ間のコール ルーティングを可能にするために、ゾーンごとにゾーン プレフィックスが設定されます。
- サイトごとに帯域幅ステートメントが設定されます。シスコでは、**bandwidth interzone** コマンドを使用することをお勧めします。**bandwidth total** コマンドを使用すると、設定内容によっては問題が発生することがあるためです。帯域幅はキロビット / 秒 (kbps) 単位で測定されます。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Cisco CallManager トランクは、1# プレフィックスに登録されるように設定されています。

  テクノロジー プレフィックスは、発信されているコールのタイプを示しています。テクノロジー プレフィックスとして使用される個々の値は任意のものであり、ネットワーク管理者が定義します。配置全体で常に同じ値を使用する必要があります。

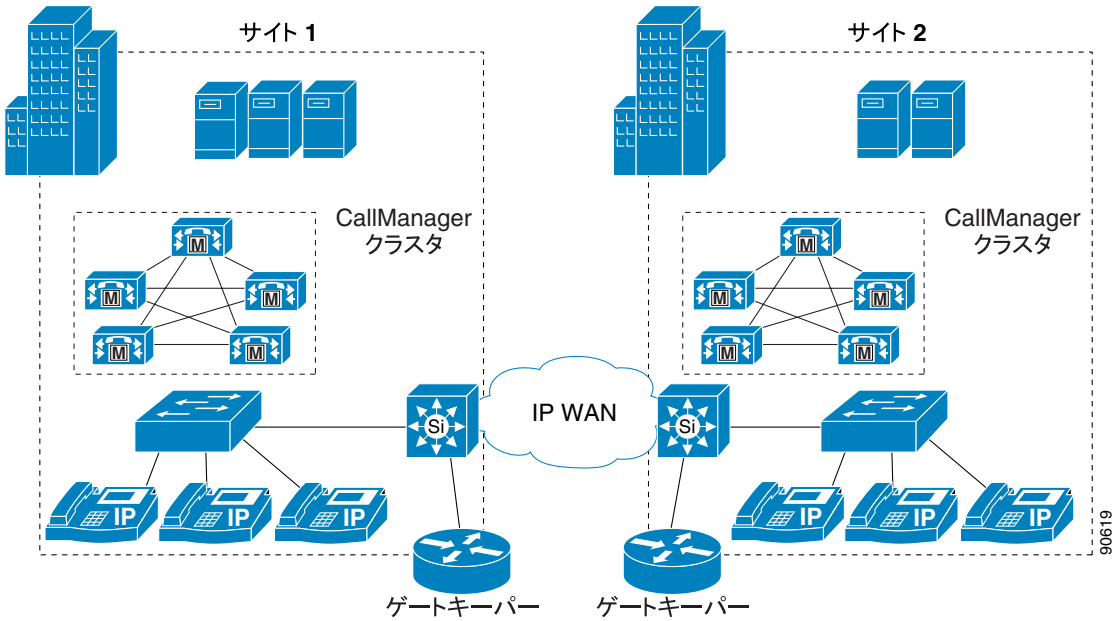
  テクノロジー プレフィックスは、E.164 アドレス（電話番号）のプレフィックスとして送信され、コールが音声であるか、ビデオであるか、その他のタイプであるかを示します。# シンボルは、一般に、プレフィックスと E.164 番号を区別するために使用します。プレフィックスが含まれていない場合、コールのルーティングにはデフォルトのテクノロジー プレフィックスが使用されます。配置全体で 1 つのデフォルト テクノロジー プレフィックスだけが使用される場合があります。

  Cisco IOS ゲートウェイは、プレフィックスが設定されていれば、自動的に発信コールにテクノロジー プレフィックスを追加します。ゲートウェイは、自動的に着信 H.323 コールからプレフィックスを除去します。Cisco CallManager は、ゲートキーパー制御 H.323 トランクの設定ページで指定されているテクノロジー プレフィックスを使用して、ゲートキーパーに登録することができます。ただし、このテクノロジー プレフィックスは、ゲートキーパーに向かう発信コールに自動的に追加されることはありません。また、Cisco CallManager に向かう着信コールから自動的に除去されることもありません。トランスレーション パターンとゲートウェイコンフィグレーションを使用して着信番号を操作すると、テクノロジー プレフィックスを必要に応じて追加または除去できます。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco CallManager トランク上にできるコール ルーティング ループを回避します。

分散型ゲートキーパー設定

帯域幅を節約するため、または WAN 障害時に H.323 ゲートウェイにローカル コール ルーティングをサポートするために、ゲートキーパーを分散させることができます。図 10-16 では、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 10-16　2 つのクラスタをサポートする分散型ゲートキーパー



例 10-2 では、図 10-16 のサイト 1 に対するゲートキーパー設定を示しています。

例 10-2　サイト 1 のゲートキーパー設定

```
gatekeeper
 zone local GK-Site1 customer.com 10.1.10.100
 zone remote GK-Site2 customer.com 10.1.11.100
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth remote 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 10-2 について説明します。

- ローカル Cisco CallManager クラスタ トランクの登録用に、ローカル ゾーンが設定されます。
- サイト 2 のゲートキーパーへのコール ルーティング用に、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のゾーンにゾーン プレフィックスが設定されます。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Cisco CallManager トランクは、1# プレフィックスに登録されるように設定されています。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco CallManager トランク上にできるコール ルーティング ループを回避します。

例 10-3 では、図 10-16 のサイト 2 に対するゲートキーパー設定を示しています。

例 10-3　サイト 2 のゲートキーパー設定

```
gatekeeper
 zone local GK-Site2 customer.com 10.1.11.100
 zone remote GK-Site1 customer.com 10.1.10.100
 zone prefix GK-Site2 212.......
 zone prefix GK-Site1 408.......
 bandwidth remote 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 10-3 について説明します。

- ローカル Cisco CallManager クラスタ トランクの登録用に、ローカル ゾーンが設定されます。
- サイト 1 のゲートキーパーへのコール ルーティング用に、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のゾーンにゾーン プレフィックスが設定されます。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Cisco CallManager トランクは、1# プレフィックスに登録されるように設定されています。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco CallManager トランク上にできるコール ルーティング ループを回避します。

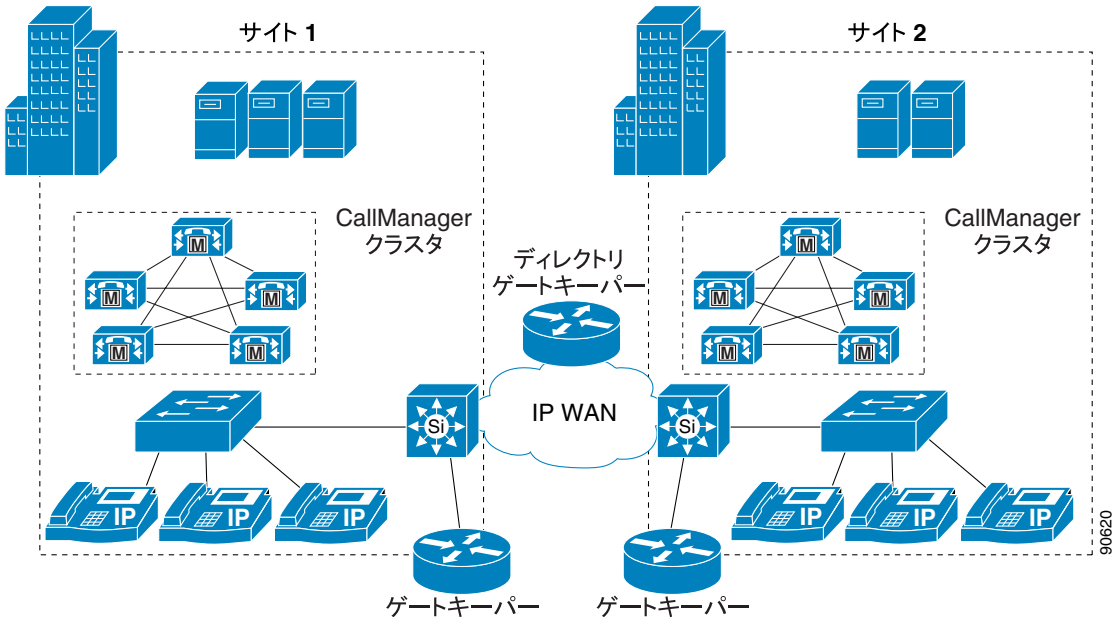
ディレクトリ ゲートキーパーを使用した分散型ゲートキーパー設定

ゲートキーパー ルーティング テーブルを更新するために使用できるゲートキーパー プロトコルがないので、ディレクトリ ゲートキーパーを使用すると、分散型ゲートキーパー設定のスケーラビリティとマネージャビリティの向上に役立ちます。ディレクトリ ゲートキーパーを実装すると、各サイトのゲートキーパー設定が簡単になり、ゾーン間通信の大部分の設定をディレクトリ ゲートキーパーでできるようになります。

ディレクトリ ゲートキーパーがない場合、ゲートキーパーに新しいゾーンを追加するたびに、ネットワーク上のすべてのゲートキーパーに項目を追加する必要があります。しかし、ディレクトリ ゲートキーパーを使用すると、ローカル ゲートキーパーとディレクトリ ゲートキーパーのみで新しいゾーンを追加できます。ローカル ゲートキーパーは、コール要求をローカル側で解決できない場合、ゾーン プレフィックスが一致するディレクトリ ゲートキーパーにその要求を転送します。

図 10-17 では、ローカル コール ルーティング用の分散型ゲートキーパー、およびゲートキーパー間のコール ルーティングをサポートするディレクトリ ゲートキーパーを備えた、Cisco CallManager 分散型コール処理環境を示しています。

図 10-17　ディレクトリ ゲートキーパーを備えた分散ゲートキーパー



例 10-4 では、図 10-17 のサイト 1 に対するゲートキーパー設定を示しています。この例では、サイト 1 とサイト 2 のゲートキーパー設定がほぼ同じなので、ここでは、サイト 1 だけについて説明します。

例 10-4　ディレクトリ ゲートキーパーを使用したサイト 1 のゲートキーパー設定

```
gatekeeper
 zone local GK-Site1 customer.com 10.1.10.100
 zone remote DGK  customer.com 10.1.10.101
 zone prefix GK-Site1 408.......
 zone prefix DGK ..........
 bandwidth remote 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 10-4 について説明します。

- ローカル Cisco CallManager クラスタ トランクの登録用に、ローカル ゾーンが設定されます。
- ディレクトリ ゲートキーパー用にリモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のゾーンにゾーン プレフィックスが設定されます。
- ディレクトリ ゲートキーパーのゾーン プレフィックスは、10 個のドットを使用して設定されます。このパターンは、未解決の任意の 10 桁のダイヤル ストリングと一致します。1 つのゾーンに複数のゾーン プレフィックスを設定して、異なる長さのダイヤル ストリングを一致させることができます。ディレクトリ ゲートキーパーのゾーン プレフィックスにもワイルドカード (*) を使用できますが、この方法はコール ルーティングの問題が発生する場合があります。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Cisco CallManager トランクは、1# プレフィックスに登録されるように設定されています。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco CallManager トランク上にできるコール ルーティング ループを回避します。

例 10-5 では、図 10-17 の例のディレクトリ ゲートキーパー設定を示しています。

例 10-5　ディレクトリ ゲートキーパー設定

```
gatekeeper
 zone local DGK customer.com 10.1.10.101
 zone remote GK-Site1 customer.com 10.1.10.100
 zone remote GK-Site2 customer.com 10.1.11.100
 zone prefix GK-Site1 408*
 zone prefix GK-Site2 212*
 lrq forward-queries
 no shutdown
```

ここでは、例 10-5 について説明します。

- ディレクトリ ゲートキーパー用にローカル ゾーンが設定されます。
- リモート ゲートキーパーごとに、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のリモート ゾーンにゾーン プレフィックスが設定されます。設定を簡単にするために、ゾーン プレフィックスでワイルドカード (*) が使用されます。コールは DGK ゾーンにルーティングされないので、DGK ゾーンにはプレフィックスが必要ありません。
- **lrq forward-queries** コマンドは、ディレクトリ ゲートキーパーが、別のゲートキーパーから受信した LRQ を転送できるようにします。

H.323 ダイヤル ピアを使用する Cisco IOS のコール特権

H.323 を使用する Cisco IOS ベースのシステム（H.323 ゲートウェイ、SRST、および Cisco CallManager Express を含む）にコール特権を実装するには、クラス制限（COR）機能を使用します。この機能は、ネットワークの設計に柔軟性をもたらし、管理者は、すべてのユーザに関して任意のコールをブロックできるようになります（たとえば、米国では 900 番号へのコール）。また、個々の発信者のコール試行に対して、それぞれ別のコール特権を適用できます（一部のユーザには国際通話を許可し、他のユーザには許可しない、など）。

COR 機能の中心となる基本的メカニズムは、着信と発信の「COR リスト」を定義することで成立しています。このリストは既存のダイヤル ピアに関連付けるもので、着信および発信という概念は、Cisco IOS ルータに対してのものです（ダイヤル ピアの場合と同様）。各 COR リストは、メンバーの番号を含めることで定義します。この番号は、Cisco IOS 内に定義済みの単純なタグです。

コールがルータを通過するときには、Cisco IOS ダイヤル ピア ルーティング ロジックに基づいて、着信ダイヤル ピアと発信ダイヤル ピアが選択されます。選択されたダイヤル ピアに COR リストが関連付けられている場合は、コールをルーティングする前に、さらに次のチェックが実行されます。

- 発信ダイヤル ピアに関連付けられている発信 COR リストのメンバーが、着信ダイヤル ピアに関連付けられている着信 COR リストのメンバーのサブセットである場合、コールは許可されます。
- 発信ダイヤル ピアに関連付けられている発信 COR リストのメンバーが、着信ダイヤル ピアに関連付けられている着信 COR リストのメンバーのサブセットではない場合、コールは拒否されます。

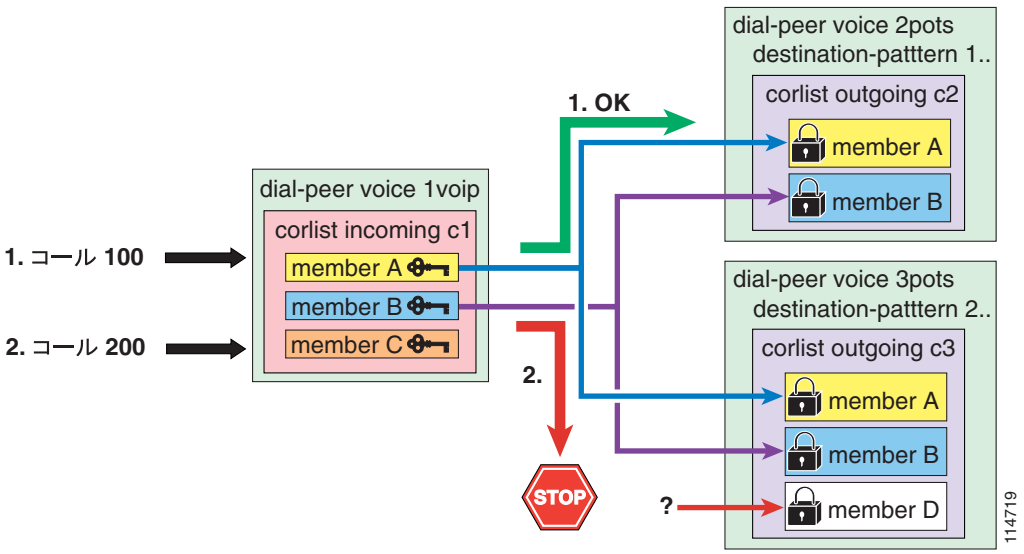
COR リスト ステートメントが一切適用されていないダイヤル ピアが存在する場合は、次のプロパティが適用されます。

- ダイヤル ピア上に着信 COR リストが設定されていない場合は、デフォルトの着信 COR リストが使用されます。デフォルト着信 COR リストは最高の優先順位を持っているため、発信 COR リストの内容にかかわらず、このダイヤル ピアは他のすべてのダイヤル ピアにアクセスできます。

- ダイヤル ピア上に発信 COR リストが設定されていない場合は、デフォルトの発信 COR リストが使用されます。デフォルト発信 COR リストは優先順位が最も低いため、着信 COR リストの内容にかかわらず、他のすべてのダイヤル ピアがこのダイヤル ピアにアクセスできます。

この動作の内容を最もよく表しているのが、図 10-18 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 10-18　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 10-18 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 CallManager クラスタへの接続を失うときまで、個々の IP Phone について事前には一切把握していません。したがって、COR 機能の SRST 用の設定は、電話の DN に基づいています。SRST ルータに登録するとき、IP Phone は自身の DN をルータに通知して、SRST ルータが IP Phone を適切な COR リストに割り当てられるようにします。

SRST によって制御される IP Phone のための COR を設定するには、コマンド **cor** {**incoming** | **outgoing**} *corlist-name* {*corlist-number starting-number – ending-number* | **default**} を **call-manager-fallback** 設定モードで使用します。

このコマンドには、次の制限事項があります。

- Cisco IOS Release 12.2(8)T 以降で使用可能な SRST バージョン 2.0 では、**call-manager-fallback** で許容される **cor** {**incoming** | **outgoing**} ステートメントの数は、最大で 5（デフォルト ステートメント含まず）です。
- Cisco IOS Release 12.3(4)T 以降で使用可能な SRST バージョン 3.0 では、**call-manager-fallback** で許容される **cor** {**incoming** | **outgoing**} ステートメントの数は、最大で 20（デフォルト ステートメント含まず）です。

COR 機能は、Cisco IOS Release 12.2(8)T 以降を使用する Cisco CallManager Express にも配置できます。個々の IP Phone は、Cisco CallManager Express で個別に設定されます。したがって、COR リストを IP Phone 自体に直接適用することができます。このためには、コマンド **cor** {**incoming** | **outgoing**} *corlist-name* を各 IP Phone の **ephone-dn** *dn-tag* 設定モードで使用します。

これらの概念を実際に適用する方法の例については、P.10-77 の「H.323 を使用している Cisco IOS でのサービス クラスの構築」の項を参照してください。

Cisco SRST と Cisco CallManager Express の設定の詳細については、次の Web サイトで入手可能な『*Cisco SRST 3.0 System Administrator Guide*』および『*Cisco CallManager Express 3.1 System Administrator Guide*』を参照してください。

http://www.cisco.com

H.323 ダイヤル ピアを使用する Cisco IOS での番号操作

H.323 を実行している Cisco IOS ルータでは、番号操作は音声トランスレーション プロファイルを通じて実行されます。このプロファイルは、音声コールの発信番号（ANI）または着信番号（DNIS）の番号を操作するために、またはコールの番号タイプを変更するために使用されるものです。

音声トランスレーション プロファイルは、Cisco IOS Release 12.2(11)T 以降で使用できます。このプロファイルは、コールが着信ダイヤル ピアに対応付けられる前、またはコールが発信ダイヤル ピアによって転送される前に、電話番号を別の番号に変換するために使用します。たとえば、社内で 5 桁の内線番号をダイヤルすると、別のサイトにいる従業員に到達できるとします。コールが他の

サイトに公衆網を通じてルーティングされ、到達する場合は、発信側のゲートウェイで音声トランスレーション プロファイルを使用する必要があります。これによって、5 桁の内線番号が公衆網で認識される 10 桁の形式に変換されます。

音声トランスレーション プロファイルを設定するには、**voice translation-rule** および **voice translation-profile** Cisco IOS コマンドを使用します。これらのコマンドでは、変換の対象となる番号ストリングを正規表現を使用して定義します。次に、この操作を発信番号、着信番号、転送先着信番号のいずれに関連付けるのかを指定します。音声トランスレーション プロファイルを定義したら、次の任意の要素に適用することができます。

- 特定の音声ポート上で終端する、すべての着信 POTS コール レッグ
- ルータに入るすべての着信 VoIP コール レッグ
- 特定の VoIP ダイヤル ピアまたは POTS ダイヤル ピアに関連付けられている発信コール レッグ
- SRST 制御の IP Phone 上で終端する、すべての着信または発信コール レッグ
- SRST 制御のすべての IP Phone によって発信されるコールのための着信コール レッグ

（注） **voice translation-rule** コマンドを使用する音声トランスレーション プロファイルは、以前に **translation-rule** コマンドで提供されていた機能を置き換え、拡張するものです。この新しいコマンドの構文は、以前のコマンドで使用されていた構文とは異なります。詳細については、http://www.cisco.com で入手可能な『*Cisco IOS Voice Command Reference*』（Release 12.2(11)T 以降）の **voice translation-rule** を参照してください。

音声トランスレーション プロファイルの一般的な用途は、IP WAN が使用不可になっていてルータが SRST モードで動作している場合でも、支店サイトからのオンネット サイト間ダイヤリング手順をそのまま維持できるようにすることです。たとえば、中央サイトが San Jose にあり、3 つのリモート サイトが San Francisco、New York、Dallas にある単純な配置について考えます。表 10-4 では、この例の DID 範囲と内部サイト コードを示しています。

表 10-4　変換規則応用例の DID 範囲とサイト コード

	San Jose	San Francisco	New York	Dallas
DID 範囲	(408) 555-1XXX	(415) 555-1XXX	(212) 555-1XXX	(972) 555-1XXX
サイト コード	1	2	3	4

サイト間のコールは、オンネット アクセス コード 8 の次に 1 桁のサイト コードと着信側の 4 桁内線番号をダイヤルすることによって、通常は IP WAN 経由で発生します。IP WAN がダウンしていて Cisco SRST がアクティブな場合にも、これらのダイヤル手順を維持できるようにするには、内部の番号を E.164 番号に再変換してから公衆網に送信する必要があります。次に、San Francisco ルータの設定例を示します。

```
voice translation-rule 1
  rule 1 /^81/ /91408555/
  rule 2 /^83/ /91212555/
  rule 3 /^84/ /91972555/

voice translation-profile on-net-xlate
  translate called 1

call-manager-fallback
  translation-profile outgoing on-net-xlate

dial-peer voice 2 pots
  destination-pattern 91[2-9]..[2-9].....
port 1/0:0
  direct-inward-dial
  forward-digits 11
```

この設定では、San Francisco サイトが SRST モードになっているときにユーザが 831000 をダイヤルすると、ルータは **voice translation-rule 1** の **rule 2** と一致するものと判定し、着信番号を 912125551000 に変換します。この新しい番号が使用され、発信ダイヤル ピア（**dial-peer voice 2**）と一致するものと判定されます。

ダイヤル ピアおよびその設定の詳細については、次の Web サイトで入手可能な『*Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*』の「Configuring Dial Plans, Dial Peers, and Digit Manipulation」を参照してください。

http://www.cisco.com

Cisco IOS の正規表現構文の詳細については、次の Web サイトで入手可能な『*Regular Expressions*』ドキュメントを参照してください。

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7e6.html

設計上の考慮事項

この項では、マルチサイト配置について、ダイヤル プランの設計上の次の考慮事項について説明します。

- P.10-47 の「マルチサイト配置用の設計ガイドライン」では、すべてのマルチサイト配置モデルに当てはまるガイドラインとベスト プラクティスを示します。
- P.10-49 の「ダイヤル プラン アプローチの選択」では、定型オンネット ダイヤリングおよび可変長オンネット ダイヤリングのダイヤル プランを作成するためのさまざまなアプローチを紹介し、この 2 番目のオプションについては、分割アドレッシングとフラット アドレッシングを紹介します。
- 次の各項では、3 つのダイヤル プラン アプローチについて詳しく分析し、それぞれの設定ガイドラインを示します。
  - 定型オンネット ダイヤル プランの配置（P.10-51）
  - 分割アドレッシングを使用する可変長オンネット ダイヤル プランの配置（P.10-53）
  - 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.10-58）
- 次の各項では、Cisco CallManager でサービス クラスを設定する方法について、2 つの代替的な方法を示します。
  - 従来のアプローチによる Cisco CallManager のサービス クラスの構築（P.10-66）
  - 回線 / デバイス アプローチによる Cisco CallManager のサービス クラスの構築（P.10-69）
- P.10-77 の「H.323 を使用している Cisco IOS でのサービス クラスの構築」では、H.323 プロトコルを実行している Cisco IOS ルータにサービス クラスを実装する方法を説明します。
- P.10-80 の「コール カバレッジの配置」では、ハント リストと回線グループを使用して Cisco CallManager にコール カバレッジ機能を実装する場合の、ガイドラインとベスト プラクティスを示します。

マルチサイト配置用の設計ガイドライン

あらゆるマルチサイト IP テレフォニー配置に対して、次のガイドラインとベスト プラクティスが共通して適用されます。複数の Cisco CallManager クラスタが関係する配置については、P.10-48 の「分散型コール処理配置に関する追加の考慮事項」の項も参照してください。

- ルーティング ループを防止するには、どの公衆網ゲートウェイのコーリング サーチ スペースにも、外部ルート パターンを含むパーティションが含まれていないことを確認してください。
- 地域通信事業者（LEC）との間で DID 範囲を取り決めるときは、サイト内で重複が発生しない DID 範囲を選択するようにしてください。たとえば、サイト内で 4 桁ダイヤリングを使用していて、1,000 個の DID ブロックが 2 つ必要な場合、ブロック (408)555-1XXX と (408)999-1XXX は 4 桁番号に短縮すると重複し、着信変換と発信変換が実行されるとさらに複雑な状態になります。
- 緊急番号をダイヤルする方法は、複数用意します。たとえば、北米の場合には、911 と 9.911 の両方を Cisco CallManager で緊急ルート パターンとして設定します。
- Automated Alternate Routing（AAR）を配置する場合は、IP Phone 上に設定されている外部電話番号マスクが、各種 AAR グループによって付加されるどのプレフィックスとも競合しないようにする必要があります。たとえば、複数の国にわたる配置の場合、0 などの国内アクセス コードは、それらがグローバル E.164 アドレスの一部でない限り、マスクに含めないでください。
- クラスタ内の宛先に対するオンネット コールを、強制的に公衆網としてダイヤルさせることができます。このためには、各サイトの E.164 DID 範囲に一致するトランスレーション パターンを追加し、このパターンによって、宛先内線番号に一致するように番号を操作します。ただし、適切な AAR を必ず設定してください。次のいずれかの方法を使用して、IP WAN が使用不可になったときに公衆網フェールオーバーができるようにします。

— 「オンネット強制」トランスレーション パターンを含んだパーティションを除外し、公衆網を指す標準ルート パターンを含んだパーティションを含むように、AAR コーリング サーチ スペースを設定します。

— * などの特殊文字をプレフィックスとして番号に付加する AAR グループを設定し、*9.! や *9.!#（または *0.! や *0.!#）などの追加ルート パターンを標準パーティション内に設定します。

2 番目の方法を使用することをお勧めします。この方法では、AAR 用の追加コーリング サーチ スペースを定義する必要がなく、また、追加の * ルート パターンによって、AAR を呼び出さなくても「オンネット強制」設定を上書きして公衆網経由でコールを発信できる、AAR 用の優れたトラブルシューティング ツールおよびテスト ツールが提供されるためです。

- N 個のサイトがある集中型コール処理クラスタでは、次のいずれかの方法を使用することで、テールエンド ホップオフ（TEHO）を実装できます。

  — 集中型フェールオーバーを使用する TEHO

  この方法では、N 個のルート パターンをグローバル パーティション内に設定します。各パターンが、適切なリモート サイト ルート グループを最初の選択肢として保持し、中央サイト ルート グループを 2 番目の選択肢として保持しているルート リストを指すようにします。

  — ローカル フェールオーバーを使用する TEHO

  この方法では、N 個のルート パターンを N セット、サイト固有のパーティション内に設定します。各パターンが、適切なリモート サイト ルート グループを最初の選択肢として保持し、ローカル サイト ルート グループを 2 番目の選択肢として保持しているルート リストを指すようにします。

  2 番目の方法では、リモート ゲートウェイや IP WAN が使用不可になった場合に、最も優れたフェールオーバー シナリオを実現できる一方で、ダイヤル プランが非常に複雑になります。最初の方法では、必要になるのは N 個のルート パターンと N 個のルート リストであるのに対して、少なくとも N^2 個のルート パターンと N^2 個のルート リストが必要になるためです。

- 国内の番号計画で許容される場合は、長距離電話としてダイヤルされたローカル公衆網コールを捕捉し、適切な省略形式に変換するための追加トランスレーション パターンを各サイトに設定することをお勧めします。このトランスレーション パターンには、サイト内の電話からのみアクセスできるようにします。このように設定することで、AAR 設定も簡潔化できます（P.10-22 の「同じローカル ダイヤリング エリアに複数のサイトがある場合の特別な考慮事項」を参照）。
- Multilevel Precedence and Preemption（MLPP）機能を使用して、緊急コールに高い優先順位を割り当てないでください。緊急時のコールは、IP テレフォニー システムに緊急コールとして表示されない場合もあります。また、メインの緊急サービス ルーティング番号に新たにコールが発信された場合、既存の緊急コールが終了する恐れがあります。

（注） 多数のゲートウェイ、ルート パターン、トランスレーション パターン、およびパーティションを含む非常に大きなダイヤル プランをもつ Cisco CallManager クラスタでは、Cisco CallManager Service の初回始動時に、初期化に長い時間がかかる場合があります。デフォルトの時間内にシステムが初期化されない場合、サービス パラメータを変更して、設定の初期化時間を延長してください。サービス パラメータの詳細については、Cisco CallManager Administration オンライン ヘルプの「Service Parameters」を参照してください。

分散型コール処理配置に関する追加の考慮事項

分散型コール処理配置（つまり、複数の Cisco CallManager クラスタが複数のサイトに配置）のダイヤルプランを設計する場合は、前の項で説明した考慮事項に加えて、次のベスト プラクティスに従ってください。

- DID 範囲を複数の Cisco CallManager クラスタにわたって分割することは避けます。分割した場合、経路の集約が不可能になり、クラスタ間ルーティングが非常に困難になります。各 DID 範囲は、それぞれ単一の Cisco CallManager クラスタに配置してください。
- リモート サイト内のデバイスを複数の Cisco CallManager クラスタに分割することは避けます。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パーティションで区切る必要があるため、IP WAN 帯域幅が効率よく使用されなくなります。各リモート サイトは、それぞれ単一の Cisco CallManager クラスタに配置してください。
- Cisco CallManager クラスタ間でのコール ルーティングには、ゲートキーパー制御クラスタ間トランクを使用します。このようにすると、ネットワーク内でクラスタを簡単に追加および修正できるようになり、他のクラスタをすべて再設定しなくても済みます。
- Cisco CallManager とゲートキーパー間の接続には、冗長性を持たせます。このためには、ゲートキーパー クラスタを使用するか、複数のサーバが設定された Cisco CallManager グループを使用しているデバイス プールに対して、クラスタ間トランクを割り当てます。
- コールをゲートキーパーに送信するときは、着信番号を完全な E.164 アドレスへと展開します。このようにすると、IP WAN が使用不可になった場合の公衆網フェールオーバーが簡単になります。これは、コールを公衆網ゲートウェイ経由で再ルーティングするための追加の番号操作が必要ないためです。また、リモート サイトごとのダイヤル長情報を使用してローカル（発信側）Cisco CallManager を設定する必要がなくなります。
- ゲートキーパー内に、Cisco CallManager クラスタごとにゾーンを 1 つ設定します。クラスタ（ゾーン）ごとに、そのクラスタの所有するすべての DN 範囲に一致するゾーン プレフィックス ステートメントを追加します。
- 次のガイドラインに従うと、複数の Cisco CallManager クラスタにわたってテールエンド ホップオフ（TEHO）を実装することができます。
  - 関係する E.164 範囲の個々のルート パターンを、送信元（発信元）Cisco CallManager クラスタに追加します。これらのパターンでは、IP WAN ルート グループを最初の選択肢として保持し、ローカル公衆網ルート グループを 2 番目の選択肢として保持するルート リストを指すようにします。
  - Cisco IOS ゲートキーパー設定に、関係するすべての E.164 範囲のゾーン プレフィックス ステートメントを追加します。これらのステートメントでは、適切な Cisco CallManager クラスタを指すようにします。
  - 宛先 Cisco CallManager クラスタに含まれているクラスタ間トランク コーリング サーチ スペースに、ローカル公衆網番号に一致するルート パターンを備えたパーティションを含めます。また、必要に応じて番号操作を適用します（たとえば、コールを公衆網に送信する前にエリア コードを除去します）。

分散型コール処理配置の Cisco IOS ゲートキーパーを設定する方法の詳細については、P.8-19 の「ゲートキーパーの考慮事項」を参照してください。

ダイヤル プラン アプローチの選択

P.10-3 の「プランニングの考慮事項」で紹介したように、IP テレフォニー システムの内部宛先用のダイヤル プランには、主に次の 2 つのアプローチがあります。

- 定型オンネット ダイヤル プラン：個々の内部宛先には、発信者が同じサイトにいるか、別のサイトにいるかにかかわらず、同じ方法でダイヤルします。
- 可変長オンネット ダイヤル プラン：内部宛先がサイト内にある場合、複数のサイトにわたっている場合とは別の方法でダイヤルします。通常、サイトの内部でやり取りされるコールの場合は 4 桁または 5 桁の省略ダイヤリングを使用し、複数サイトにわたるコールの場合は、完全な E.164 アドレスを使用するか、オンネット アクセス コード、サイト コード、内線番号をこの順序で使用します。

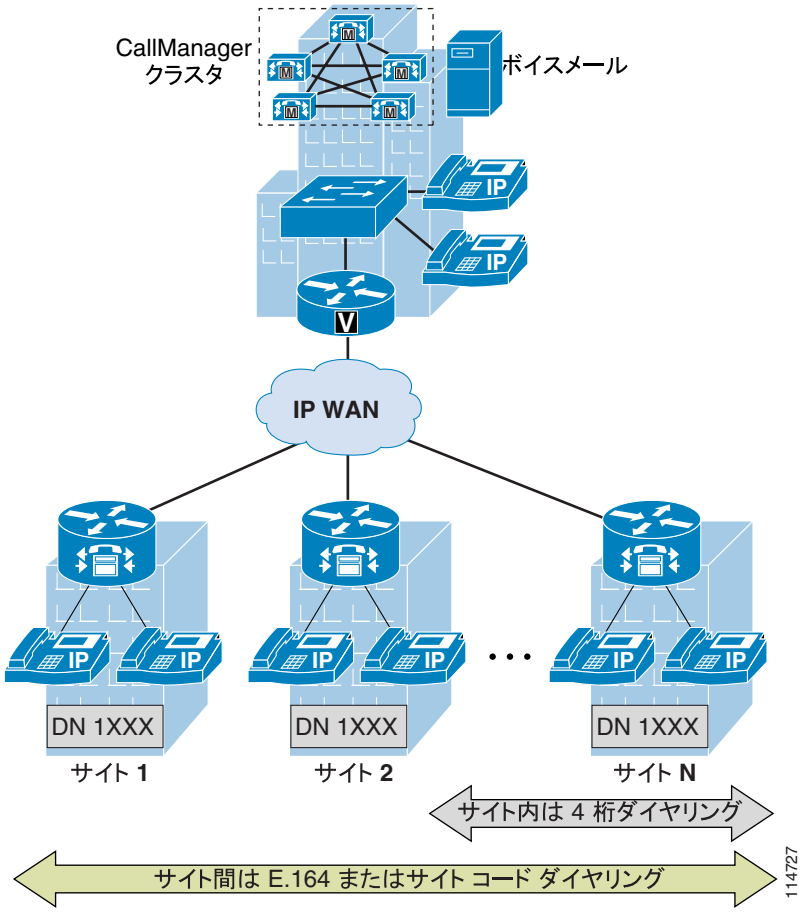
どちらのアプローチが最適かを判断するには、次の基本的な設計上の質問について検討すると役立ちます。

- IP テレフォニー システムによってサービスされるサイトは、最終的にいくつあるか。
- サイト間または支店間の発信パターンは何か。
- サイト内で、および別のサイトに到達するために、ユーザは何をダイヤルするか。
- オンネットサイト間コールに適用されるコール制限はあるか。
- ほとんどのサイト間コールで使用される転送ネットワークは何か（公衆網または IP WAN）。
- CTI アプリケーションが使用されている場合、それは何か。
- サイト コードを使用して、オンネット ダイヤリング構造を標準化する予定はあるか。

定型オンネット ダイヤル プランは、設計と設定が最も簡単です。ただし、このプランが最も適しているのは中小規模の配置であり、サイトおよびユーザの数が大きくなるほど、実用には適さなくなります。このプランについては、P.10-51 の「定型オンネット ダイヤル プランの配置」の項で詳しく説明および分析しています。

可変長オンネット ダイヤル プランは、スケーラビリティが優れていますが、設計と設定も複雑になります。図 10-19 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 10-19　大規模マルチサイト配置の一般的なダイヤリング要件



Cisco CallManager で可変長オンネット ダイヤル プランを実装する方法には、主に次の 2 つがあります。

- 分割アドレッシング

  内部の内線番号は、配置されているサイトに応じて、複数のパーティションに配置します。この方法は、通常はサイト間コールの E.164 アドレスに基づいています。詳細については、P.10-53 の「分割アドレッシングを使用する可変長オンネット ダイヤル プランの配置」の項を参照してください。
- フラット アドレッシング

  内部の内線番号を、すべて同じパーティションに配置します。この方法は、通常はサイト間コールのオンネット サイト コードに基づいています。詳細については、P.10-58 の「フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置」の項を参照してください。このアプローチは、サイト間コールに完全な E.164 アドレスを使用している場合でも使用できることがあります。P.10-64 の「サイト コードを使用しない配置に関する特別な考慮事項」の項を参照してください。

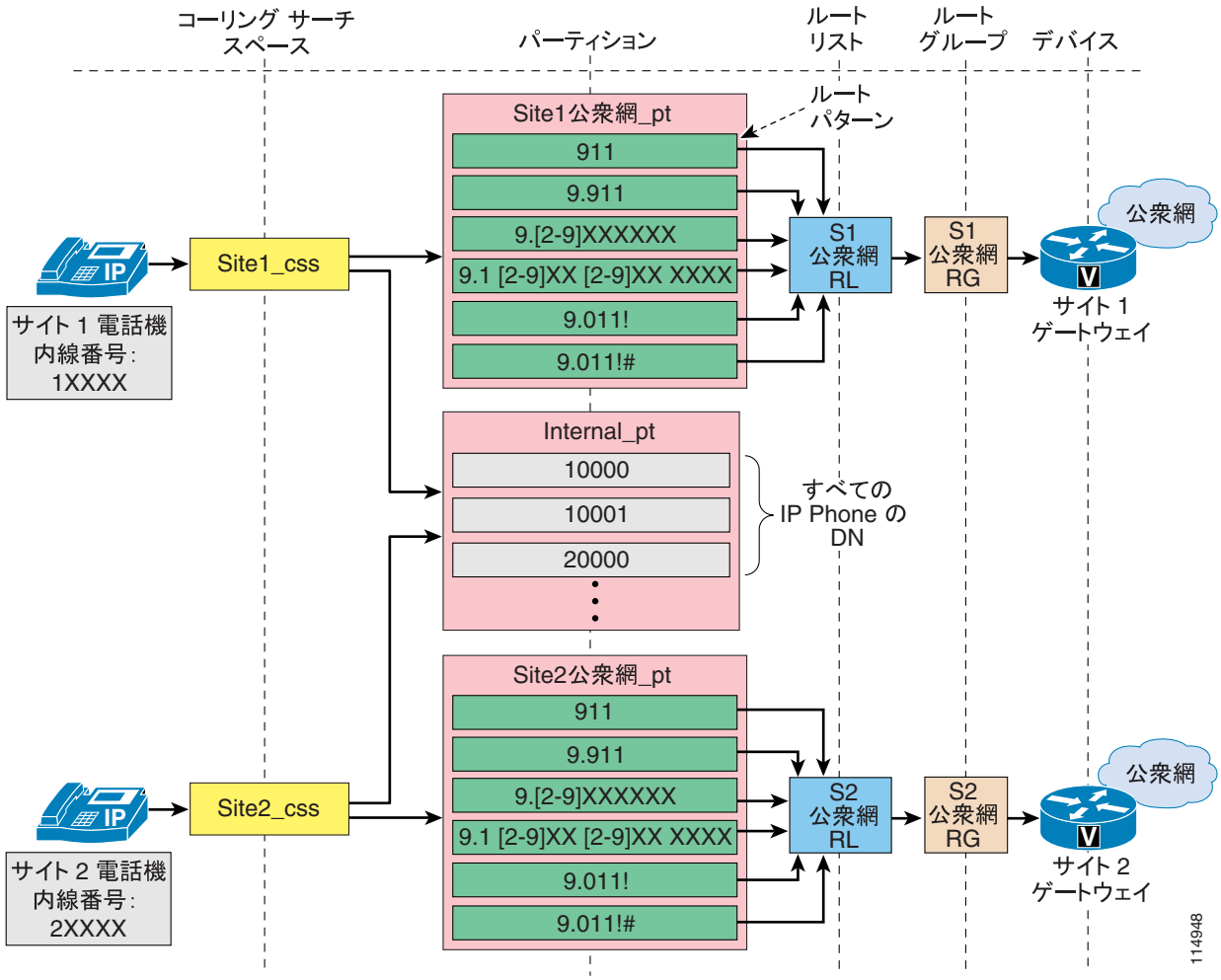
定型オンネット ダイヤル プランの配置

定型オンネット ダイヤル プランを実装するには、次のガイドラインに従います。

- 省略ダイヤルを使用して、すべての電話を一意に識別する。
- すべての電話 DN を単一のパーティションに配置する。
- 各サイトで、選択したサービス クラス アプローチに従って、公衆網ルート パターンを 1 つまたはそれ以上のサイト固有パーティションに配置する。

図 10-20 では、単一 Cisco CallManager クラスタ配置での実装例を示しています。

図 10-20　定型オンネット ダイヤル プランの配置の例



次の両方の条件に当てはまる場合は、このアプローチを使用します。

- 内部内線番号の識別用に選択した桁数を考慮したとき、使用可能な DID 範囲どうしが重複していない。
- IP テレフォニー システムによって処理されるサイトの数は、長期的に見て大幅に増加することがない。

次の各項では、定型オンネット ダイヤル プランのフレームワークで使用される各種のコールについて、実装の詳細およびベスト プラクティスを分析します。

- クラスタ内でのサイト間コール（P.10-52）
- 発信公衆網コールと IP WAN コール（P.10-53）
- 着信コール（P.10-53）
- ボイスメール コール（P.10-53）

クラスタ内でのサイト間コール

すべての内部 DN に対して、あらゆるデバイスのコーリング サーチ スペースから直接到達することができるため、すべてのオンネット コール（サイト内およびサイト間）が自動的に使用可能になります。Cisco CallManager で特に設定する必要はありません。

発信公衆網コールと IP WAN コール

公衆網コールは、サイト固有のパーティションとルート パターンを使用することで可能になります。このため、緊急コールと市内電話は、ローカルの支店ゲートウェイを通じてルーティングすることができます。長距離電話と国際コールは、企業のポリシーに応じて、同じ支店ゲートウェイを通じてルーティングすることも（図 10-20 を参照）、中央ゲートウェイを通じてルーティングすることもできます。この 2 番目の方法で必要になるのは、サイトごとの追加ルート リストのみです。このリストには、中央サイト ゲートウェイを指す第 1 位ルート グループ、およびローカル支店ゲートウェイを指す第 2 位ルート グループ（省略可）を含めます。

別の Cisco CallManager クラスタや Cisco CallManager Express への省略ダイヤリングも、ゲートキーパーを通じて使用できます。これらの IP WAN コールについては、ゲートキーパーに送信する前に、トランスレーション パターンを通じて省略ストリングを完全な E.164 に展開することをお勧めします。

着信コール

着信公衆網コールで必要となるのは、Cisco CallManager に設定されている内線番号の長さに合せて、余分な桁を除去することのみです。この操作は、ゲートウェイの設定によって、またはゲートウェイのコーリング サーチ スペースに含まれているトランスレーション パターンを通じて実行できます。

ボイスメール コール

各内線番号は、いずれもシステム内部では一意です。したがって、この内線番号を使用してボイスメール システム内にボイスメール ボックスを設定することができます。ボイスメール システムにコールを送信するために、または Cisco CallManager 内のメッセージ待機インジケータ（MWI）をオンにするために、変換を実行する必要はありません。

ただし、ユーザが公衆網からボイスメール システムにアクセスする場合は、ユーザを訓練して、ボイスメール ボックスにアクセスするときに 8 桁の内線番号を入力してもらうようにする必要があります。

分割アドレッシングを使用する可変長オンネット ダイヤル プランの配置

分割アドレッシングを使用する可変長オンネット ダイヤル プランを実装するには、複数のパーティション（サイトごとに 1 パーティション）に分かれている各サイトの電話に対して省略 DN を定義し、グローバル パーティションに含まれている一連のトランスレーション パターン（サイトごとに 1 トランスレーション パターン）を利用して、サイト間コール ルーティングを実行します。

この方法を使用すると、サイトの内部では省略ダイヤリング（通常は 4 桁または 5 桁）をサポートし、サイト間では完全な E.164 ダイヤリングをサポートするという重要な要件を満たすことができます。ただし、ダイヤル プランが複雑になるという代償もあります。

（注） これらの配置は、「重複ダイヤル プラン」または「重複内線番号のあるダイヤル プラン」とも呼ばれます。それぞれのサイトで定義した省略 DN が、通常は互いに重複しているためです。

表 10-5 では、各サイトでのコーリング サーチ スペースとパーティションの基本的な関係を示しています。ただし、サービス クラスの実装に必要となる追加の要素は考慮に入れていません。

表 10-5　分割アドレッシングを使用する可変長ダイヤル プランのコーリング サーチ スペースとパーティション

コーリング サーチ スペース	パーティション	パーティションの内容
Site1_css	Site1Phones_pt	サイト 1 の電話 DN（省略形式）
	Site1PSTN_pt	サイト 1 の公衆網ルート パターン（サービス クラスに基づいて、他にもパーティションが必要）
	Translations_pt	クラスタ内でのサイト間コールのためのトランスレーション パターン
…	…	…
SiteN_css	SiteNPhones_pt	サイト N の電話 DN（省略形式）
	SiteNPSTN_pt	サイト N の公衆網ルート パターン（サービス クラスに基づいて、他にもパーティションが必要）
	Translations_pt	クラスタ内でのサイト間コールのためのトランスレーション パターン

次の条件に 1 つ以上当てはまる場合は、このアプローチを使用します。

- サイト コードを使用するグローバル オンネット番号計画を使用する予定がない。

（注）　このアプローチは、サイト コードを使用するオンネットの内部内線番号計画がある場合にも使用できますが、そのようなシナリオでは、P.10-58 の「フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置」の項で説明しているフラット アドレッシング アプローチに従うことをお勧めします。ダイヤル プランの構造を大幅に簡素化でき、システムの管理とトラブルシューティングが容易になるためです。

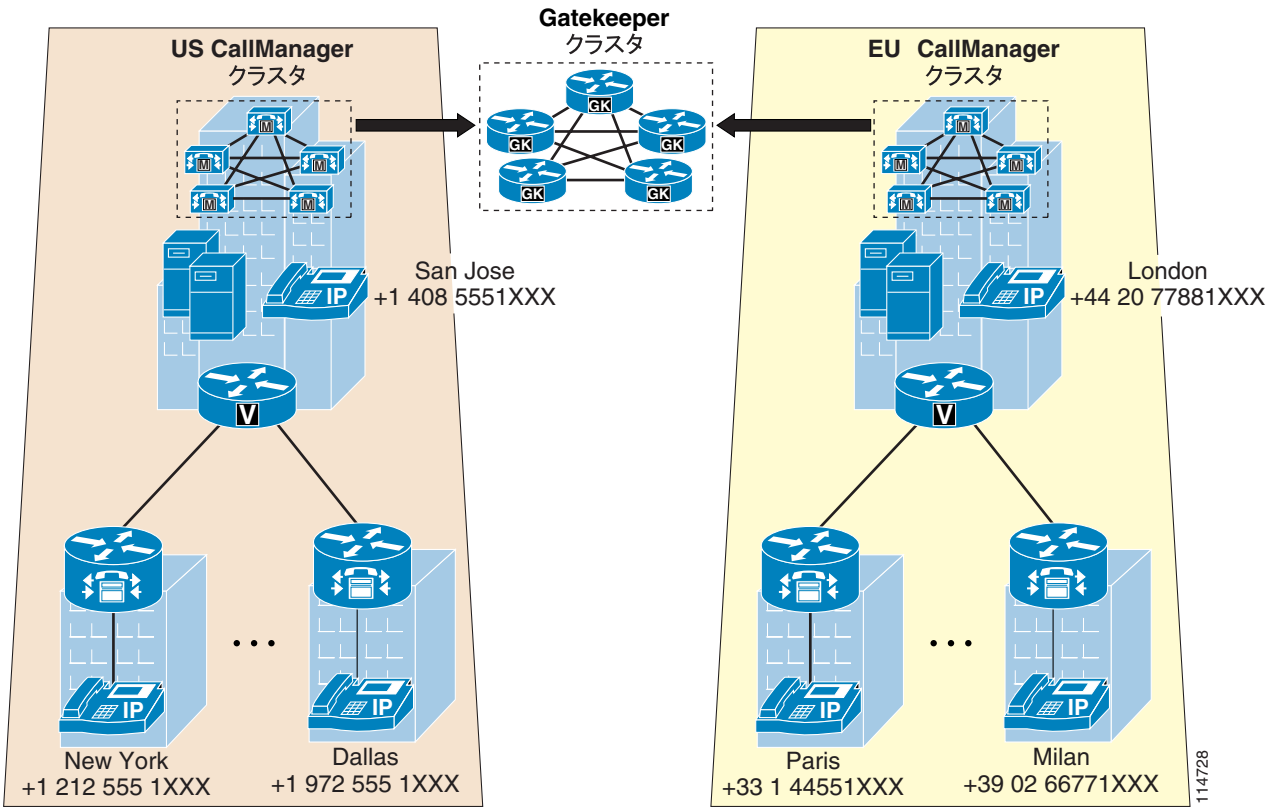
- オンネットのサイト間コールに対して、ポリシーによる制約を適用する必要がある（つまり、一部またはすべてのユーザが他のオンネット サイトにダイヤルすることを不許可にする）。
- サイト間コールは、常に公衆網を介してルーティングされる（P.2-9 の「集中型コール処理のバリエーションとしての Voice Over the PSTN」の項を参照）。
- CTI ベースのアプリケーションは、サイト間では使用しない。

（注）　CTI ベースの一部のアプリケーションは、Cisco Attendant Console と同様に重複内線番号をサポートしていないため、分割アドレッシング アプローチを使用して配置することができません。Cisco Personal Assistant や Cisco IP Manager Assistant（IPMA）など、その他のアプリケーションは追加のダイヤル プラン設定を必要とします。重複内線番号が存在している場合、このダイヤル プラン設定は複雑なものになり、場合によっては正常に機能しない可能性があります。これらのアプリケーションを配置する予定がある場合は、次の項で説明するフラット アドレッシング アプローチを選択することをお勧めします。

分割アドレッシング アプローチを配置する方法をわかりやすくするために、図 10-21 に示す架空の顧客ネットワークについて考えます。このネットワークは、米国内にメイン サイト（San Jose）と多くの小規模支店サイト（New York と Dallas）があり、トポロジは、欧州のメイン サイト（London）と小規模支店サイト（Paris と Milan）に類似しています。ユーザ数、管理上の必要性、およびネットワーク トポロジに基づいて、集中型コール処理を使用する Cisco CallManager クラスタが 2 つ配

置されています。1 つは米国で、1 つは欧州です。Cisco IOS ゲートキーパー クラスタを使用して、2 つのクラスタ間での E.164 アドレス解決とコール アドミッション制御を提供しています。可変長オンネット ダイヤル プランが必要なことも決定していて、各サイトの内部では 4 桁ダイヤリングを使用し（各サイトで 1XXX 内線番号範囲を利用）、サイト間では完全な E.164 ダイヤリングを使用します。

図 10-21　大規模なマルチサイト配置の例



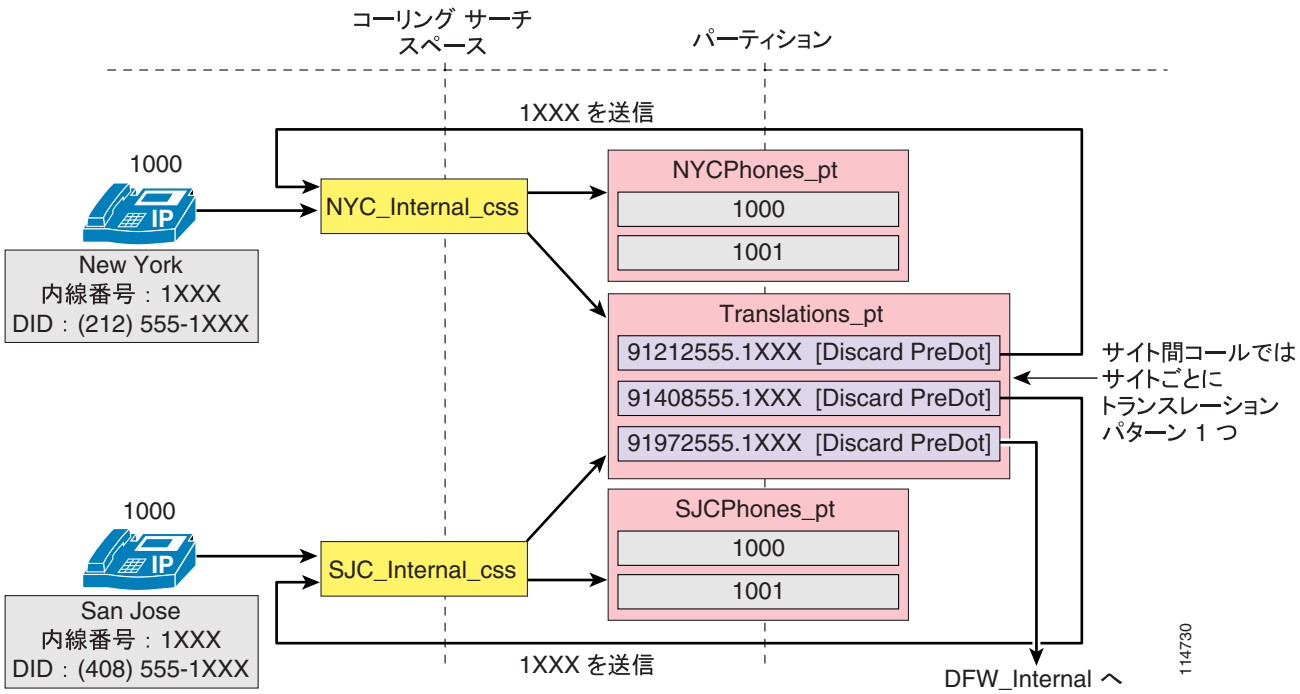
次の各項では、図 10-21 の米国（US）クラスタを例にとって、分割アドレッシング アプローチのフレームワークで使用される各種のコールについて、実装の詳細とベスト プラクティスを分析します。

- クラスタ内でのサイト間コール（P.10-56）
- 発信公衆網コールと IP WAN コール（P.10-56）
- 着信コール（P.10-58）
- ボイスメール コール（P.10-58）

クラスタ内でのサイト間コール

図 10-22 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 10-22　分割アドレッシング法におけるクラスタ内部のサイト間コール



サイトとパーティション間の接続性をサポートするために、次のガイドラインに従ってトランスレーション パターンを使用してください。

- サイトごとに 1 つのトランスレーション パターンを定義し、すべてのトランスレーション パターンを Translations_pt パーティションに入れる。
- 各パーティションは、公衆網サイト コード（この例では 9）を含めて、サイトの E.164 アドレス範囲と一致する必要がある。
- 変換後に得られる着信番号は、サイトの内線番号（この例では 1XXX）と一致する必要がある。
- 変換後にコールが送信されるコーリング サーチ スペースには、宛先サイトの IP Phone の DN が入っているパーティションが含まれている必要があります。

発信公衆網コールと IP WAN コール

各種の公衆網コールをどのようにルーティングするかに応じて（集中型ゲートウェイと分散型ゲートウェイ）、設定が異なります。図 10-23 の例では、国内公衆網コールはすべてローカル支店ゲートウェイを通じてルーティングされます。国際コールは、欧州クラスタの制御するサイトへのコールを代行受信するために、まずゲートキーパーを通じてルーティングされ、次にローカル公衆網ゲートウェイを通じてルーティングされます。

図 10-23　分割アドレッシング法における発信の公衆網コールと IP WAN コール

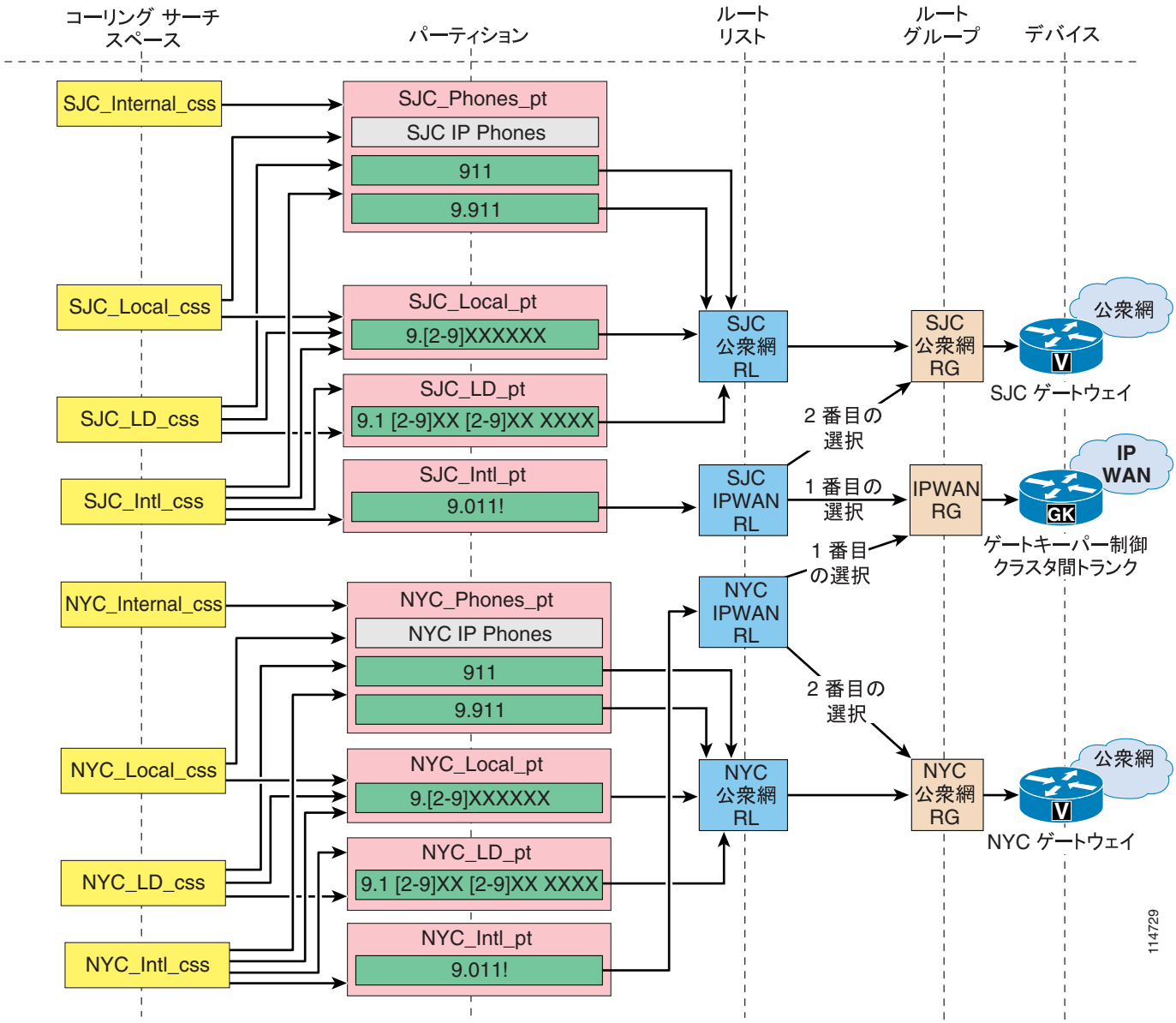


図 10-23 に示すように、発信の公衆網コールと IP WAN コールについては、内部アドレッシングが分割されていても特に考慮事項はありません。

（注） 図 10-23 では、従来のアプローチに従ってサービス クラスを構築しています。ただし、回線 / デバイス アプローチを分割アドレッシング アプローチと組み合せることもできます。サービス クラス アプローチとエンドポイント アドレッシング アプローチはそれぞれ独立しており、互いを置き換えることはできません。

着信コール

着信の公衆網コールまたは IP WAN コールを適切な内線に送信するには、上記で説明されている Translations_pt パーティション内のトランスレーション パターンを再使用できます。Translations_pt パーティションだけが入っているコーリング サーチ スペースに、すべての公衆網ゲートウェイを割り当て、すでに定義されているトランスレーション パターンと一致させるために、ゲートウェイが、ダイヤル番号の前に 9 または 91 をプレフィックスとして付けることを確認するだけで十分です。

ボイスメール コール

ボイスメール統合では、分割アドレッシング アプローチに関する次の要件に特に注意する必要があります。

- ボイスメール ボックスに固有の ID が必要です。つまり、IP Phone の内線番号はボイスメール ボックスとして使用できません。固有の番号を取得するには、番号操作が必要です。
- ボイスメール システムからの MWI（メッセージ待機インジケータ）メッセージは、固有でない内線番号がある場合でも、適切な IP Phone に到達できなければなりません。

最初の項目は、Voice Mail Profile Configuration ページの Voice Mail Box Mask フィールドを使用して、Cisco CallManager で処理されます。このパラメータを設定すると、ボイスメール システムと情報を交換し、ユーザを固有に識別できます。たとえば、Voice Mail Box Mask パラメータをユーザに関連した完全な E.164 番号に設定できます。

2 番目の項目は、オンクラスタ パーティション内のトランスレーション パターンを再使用することによって処理されます。ボイスメール システムが完全な E.164 番号を使用して設定されている場合、以前に定義されたトランスレーション パターンと一致させ、適切なサイト間通信を確保するために、E.164 番号の前に 9 を付けることができます。このように、完全な E.164 番号をもつボイスメール システムからの MWI メッセージは、特定のパーティション内の適切な内線番号に変換されます。たとえば、ボイスメール ポートを設定するときに、ボイスメール システムによってダイヤルされる E.164 番号に 9 をプレフィックスとして付加するトランスレーション パターンのみが入った VM_Translations_pt パーティションを含んでいるコーリング サーチ スペースを使用します。このトランスレーション パターンのコーリング サーチ スペースには、Translations_pt パーティションが含まれています。このパーティションによって、定義済みのトランスレーション パターンを通じて、すべての内線番号へのアクセスが提供されます。

（注） このアプローチには、Cisco CallManager 内の 2 つのサービス パラメータの設定が必要です。Cisco CallManager サービス内の MultiTenantMwiMode パラメータを True に設定し、CMI（Cisco Messaging Interface）サービス内の ValidateDNs パラメータを False に設定する必要があります。

フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置

フラット アドレッシングを使用する可変長オンネット ダイヤル プランを実装するには、電話の DN を、オンネット アクセス コード、サイト コード、および内線番号を含んだ一意のストリング（たとえば、8-123-1000）として定義します。これらの DN を同じグローバル パーティションに配置すると、サイト コードを使用したサイト間コールを使用できるようになり、サイト固有のパーティション内にトランスレーション パターンを定義すると（サイトごとに 1 トランスレーション パターンと 1 パーティション）、サイトの内部では省略ダイヤリングを使用できるようになります。

サイト内でユーザが通常ダイヤルしている 4 桁または 5 桁の番号を使用して、Directory Number 設定ページの Line Text Label パラメータを設定すると、この内部構造をエンドユーザから見えないようにすることができます。AAR を使用可能にし、ユーザが自分の DID 番号を IP Phone のディスプレイで見られるようにするには、外部電話番号マスクについても、対応する公衆網番号を使用して設定する必要があります。

表 10-6 では、各サイトでのコーリング サーチ スペースとパーティションの基本的な関係を示しています。ただし、サービス クラスの実装に必要となる追加の要素は考慮に入れていません。

表 10-6　フラット アドレッシングを使用する可変長ダイヤル プランのコーリング サーチ スペースとパーティション

コーリング サーチ スペース	パーティション	パーティションの内容
Site1_css	Site1Translations_pt	サイト 1 の省略ダイヤリングのためのトランスレーション パターン
	Site1PSTN_pt	サイト 1 の公衆網ルート パターン（サービス クラスに基づいて、他にもパーティションが必要）
	Internal_pt	すべての IP Phone の DN（一意形式）
…	…	…
SiteN_css	SiteNTranslations_pt	サイト N の省略ダイヤリングのためのトランスレーション パターン
	SiteNPSTN_pt	サイト N の公衆網ルート パターン（サービス クラスに基づいて、他にもパーティションが必要）
	Internal_pt	すべての IP Phone の DN（一意形式）

次の条件に 1 つ以上当てはまる場合は、このアプローチを使用します。

- オンネットのサイト間コールで、ダイヤリング制限が必要ない。
- サイト コードを使用するグローバル オンネット番号計画を使用する予定がある。
- サイト間コールは、通常は IP WAN を通じてルーティングされる。
- CTI ベースのアプリケーションをサイト間で使用する。

（注） オンネットのサイト間コールにダイヤリング制限を適用する必要がある場合や、サイト コードを使用するオンネット番号計画を使用する予定がない場合は、それらのニーズに対応可能なこのアプローチの変型について、P.10-64 の「サイト コードを使用しない配置に関する特別な考慮事項」の項を参照してください。

このアプローチには、次の考慮事項が適用されます。

- ローカルの 4 桁コールの宛先番号は、IP Phone のディスプレイおよび Placed Calls ディレクトリでは一意の内部 DN へと展開されます。
- 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。

分割アドレッシング アプローチを配置する方法をわかりやすくするために、図 10-21 に示す架空の顧客ネットワークについてもう一度考えます。この場合、可変長オンネット ダイヤル プランが必要になることは決定していて、各サイトの内部では 4 桁ダイヤリングを使用し（各サイトで 1XXX 内線番号範囲を利用）、サイト間のダイヤリングでは、オンネット アクセス コード（この例では 8）、3 桁のサイト コード、および 4 桁の内線番号で構成される 8 桁のストリングを使用します。3 桁のサイト コードは、米国にあるサイトの場合は NANP エリア コードから生成され、欧州にあるサイトの場合は E.164 国コードとサイト識別子から生成されます。表 10-7 では、選択されたサイト コードを示しています。

表 10-7　図 10-21 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

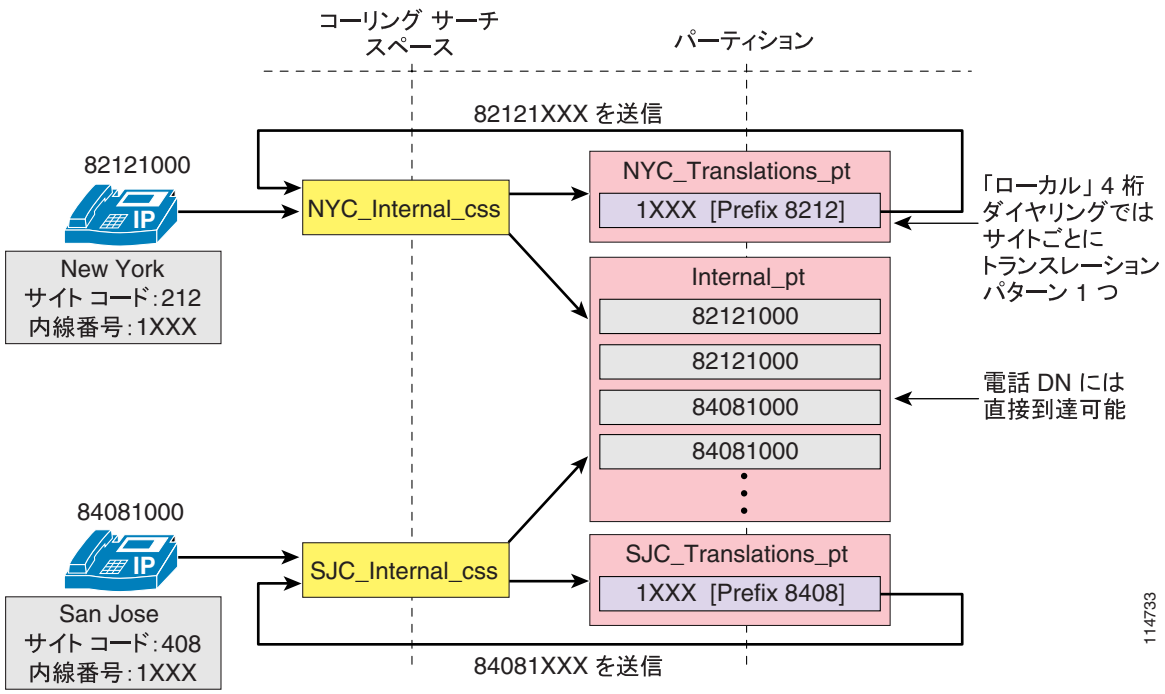
次の各項では、この例の US クラスタを使用して、フラット アドレッシング アプローチのフレームワークで使用される各種のコールについて、実装の詳細とベスト プラクティスを分析します。

- クラスタ内でのサイト間コール（P.10-60）
- 発信公衆網コールと IP WAN コール（P.10-61）
- 着信コール（P.10-64）
- ボイスメール コール（P.10-64）
- 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.10-64）

クラスタ内でのサイト間コール

図 10-24 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 10-24　フラット アドレッシング法におけるクラスタ内部のサイト間コール



サイトとパーティション間の接続性をサポートするために、次のガイドラインに従ってください。

- オンネット アクセス コード 8 を含めて、一意の DN をすべてグローバル パーティション（この例では Internal_pt）に配置します。
- サイトごとにパーティションを 1 つ作成し、それぞれのパーティションの中に、4 桁番号をそのサイトの完全修飾 8 桁番号に展開するトランスレーション パターンを配置して、サイト内部で省略ダイヤリングを使用できるようにします。
- 各サイトで、Internal_pt パーティションとローカル トランスレーション パーティションの両方を電話のコーリング サーチ スペースに含めます。

Cisco CallManager に設定されている DN にオンネット アクセス コードを含めると、すべての電話から直接アクセスできるパーティションの中にすべての内部内線番号を配置できるようになり、同時に、IP Phone 上のすべてのコール ディレクトリの中に、直接にリダイヤル可能な番号が確実に入力されます。

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

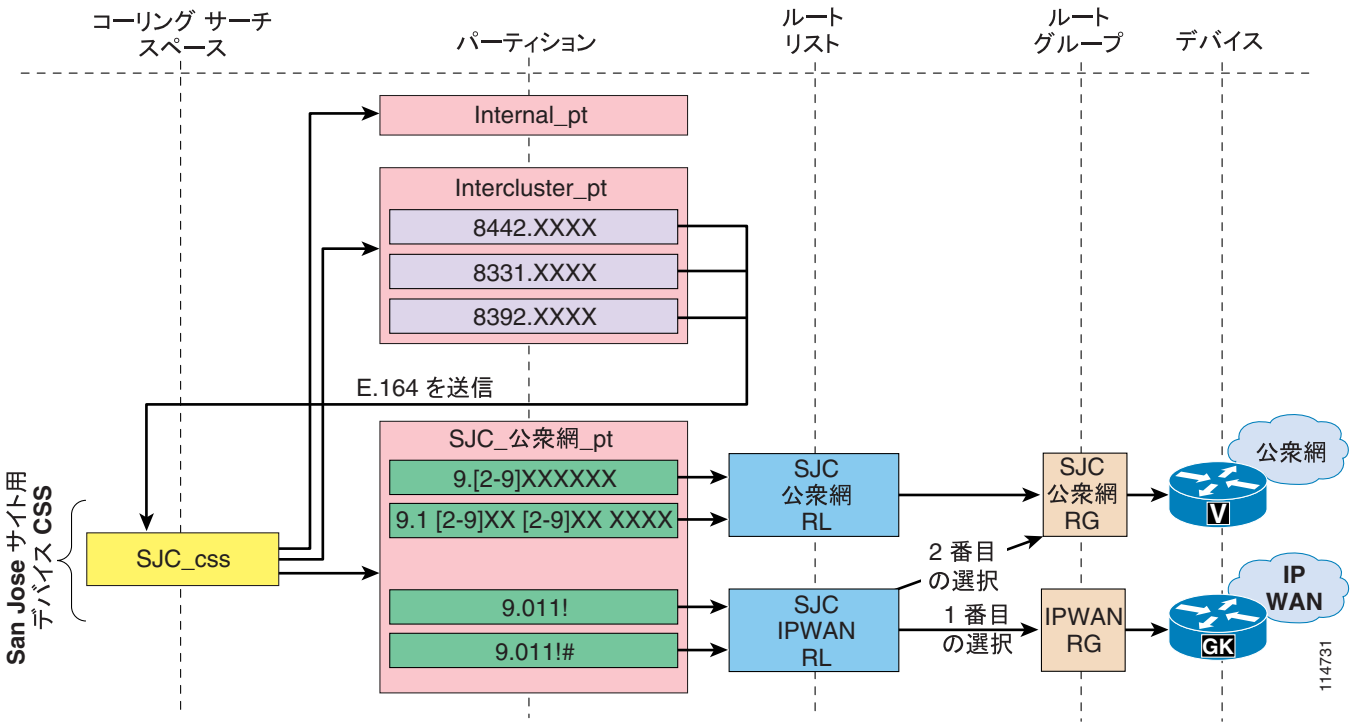
このオプションでは、単一のルート パターンを利用します。このパターンはすべての 8 桁範囲（8XXXXXXX）に一致し、ゲートキーパー制御クラスタ間トランクのみを含んだルート リストまたはルート グループを指しています。ゲートキーパーは、サイト コードをゾーン プレフィックスとして使用するように設定します。

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 10-25 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 10-25　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 10-25 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。

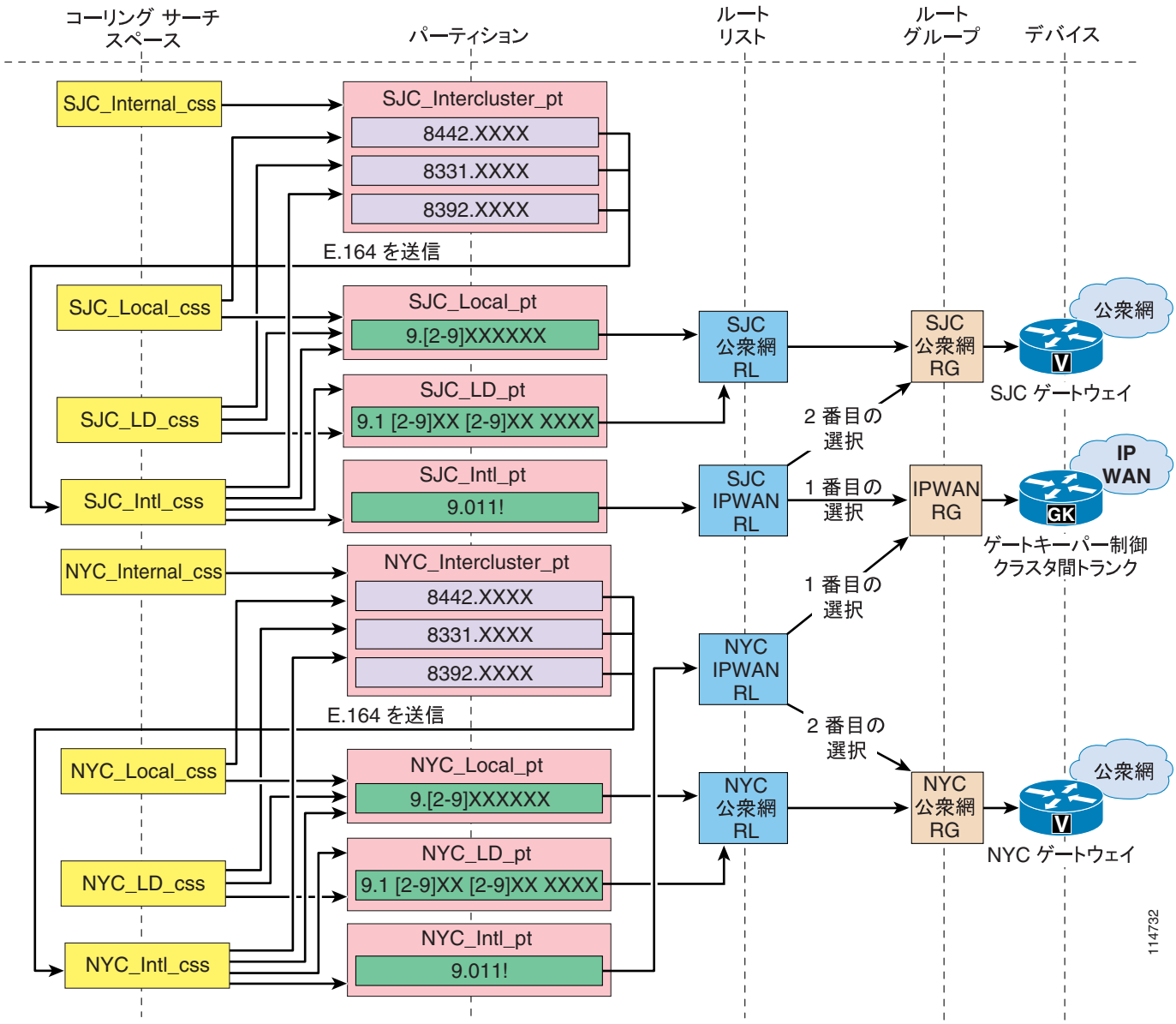
このソリューションは、オプション 1 で説明したソリューションよりもわずかに設定および保守作業が増えます。これは、他のクラスタのサイト コードと E.164 範囲に関する情報を設定し、保守する必要があるためです。その一方で、IP WAN が使用不可になった場合には、自動公衆網フェールオーバーが提供されます。公衆網フェールオーバーは、中央サイトのゲートウェイのみを使用して提供されます。このため、IP WAN 帯域幅の使用効率は最適なものにはなりません。

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 10-26 に示すように、サイトごとに一連のトランスレーション パターンを使用します。各セットは、欧州の 8 桁範囲に一致し、それらを対応する E.164 番号に変換します。これらのトランスレーション パターンでは、発信元サイトのコーリング サーチ スペースを使用するので、コールは発信元サイトの公衆網パーティションにある国際公衆網ルート パターンに一致します。各サイトの国際公衆網ルート パターンは、IP WAN ルート グループを最初の選択肢として保持し、ローカル公衆網ルート グループを 2 番目の選択肢として保持しているルート リストを指しています。ゲートキーパーは、E.164 アドレスをゾーン プレフィックスとして使用するように設定します。

図 10-26　IP WAN コールに分散型公衆網フェールオーバーを使用する、フラット アドレッシング法における発信の公衆網コールと IP WAN コール



このソリューションは、オプション 2 で説明したソリューションよりも設定および保守作業がかなり増えます。これは、他のクラスタのサイト コードと E.164 範囲に関する情報を設定し、保守して、クラスタ内の各リモート サイトでこの設定作業を繰り返す必要があるためです。その一方で、IP WAN が使用不可になった場合には、ローカル サイトのゲートウェイを使用して自動公衆網フェールオーバーが提供されるため、IP WAN 帯域幅の使用効率は最適なものになります。

このソリューションでも、公衆網コールとしてダイヤルされた欧州サイトへのコールは、IP WAN が使用可能な場合、ローカル ゲートウェイを使用する自動公衆網フェールオーバーによって、オプション 2 と同様に自動的にオンネットになります。

着信コール

着信公衆網コールでは、8 桁の内部番号を取得して宛先の電話に到達するには、E.164 番号を操作する必要があります。この要件は、次の方法のいずれかで満たすことができます。

- Cisco CallManager の Gateway Configuration ページにある Num Digits フィールドと Prefix Digits フィールドを設定して、必要な番号を除去してプレフィックスを付加するようにします。
- クラスタ内でオンネット サイト間コールを強制するトランスレーション パターンを設定した場合は、公衆網アクセス コードをゲートウェイ上の着信番号にプレフィックスとして付加するだけで、それらのパターンを再利用することができます。
- H.323 ゲートウェイを使用している場合は、コールを Cisco CallManager に送信する前に、ゲートウェイ内の変換規則を使用して番号を操作できます。

3 番目のアプローチは、支店が SRST モードになっている場合、設定済みの変換規則を再利用して IP Phone に着信公衆網接続を提供できる利点があります。

ボイスメール コール

8 桁の各内線番号は、いずれもシステム内部では一意です。したがって、この内線番号を使用してボイスメール システム内にボイスメール ボックスを設定することができます。ボイスメール システムにコールを送信するために、または Cisco CallManager 内のメッセージ待機インジケータ（MWI）をオンにするために、変換を実行する必要はありません。

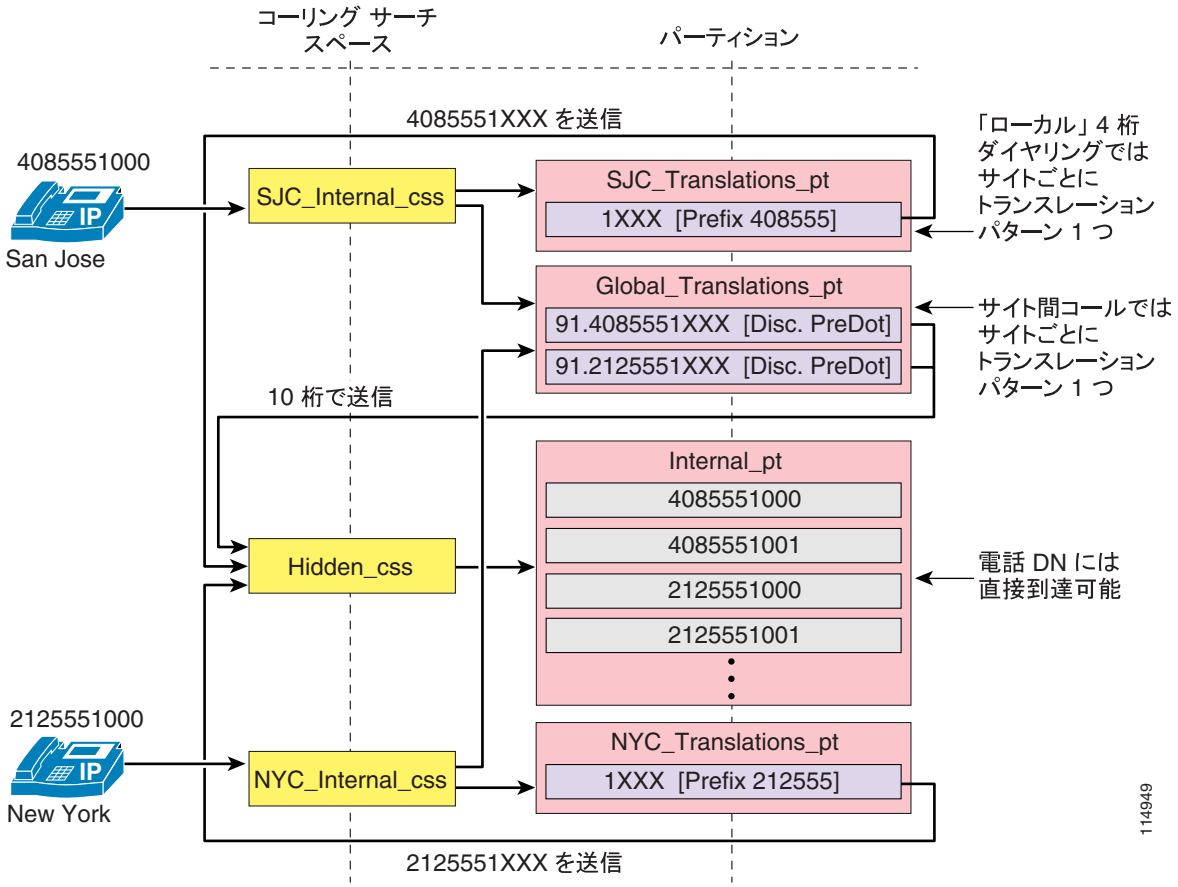
サイト コードを使用しない配置に関する特別な考慮事項

このシナリオは、フラット アドレッシング アプローチの変型であり、サイト コードに基づいてオンネット番号計画を定義することに依存しません。このシナリオでは、サイト内コールは 4 桁番号としてダイヤルします。その一方で、サイト間コールは通常の公衆網コールとしてダイヤルするため、コールは Cisco CallManager によって代行受信され、IP WAN を通じてルーティングされます。

このメカニズムを実装するには、図 10-27 に示すように、次のガイドラインに従います。

- 電話 DN は、完全な E.164 アドレスとして定義し、すべて同じパーティション（この例では Internal_pt）に配置します。
- 電話のコーリング サーチ スペースは、Internal_pt パーティションに直接アクセスできないように設定します。代わりに、Global_Translation_pt というグローバル パーティションを指すようにします。このパーティションには、サイトごとに 1 パーティション、または DID 範囲を含めます。
- 公衆網アクセス コード（たとえば 9）を除去するトランスレーション パターンを設定し、コールを Hidden_css コーリング サーチ スペースを通じて Internal_pt パーティションに送信します。
- 各サイトの内部では、トランスレーション パターン（サイトごとに 1 パーティションと 1 トランスレーション パターン、または DID 範囲）を含んだサイト固有のパーティションを通じて、省略 4 桁ダイヤリングを提供できます。

図 10-27　サイト コードを使用せずにフラット アドレッシングを使用する可変長ダイヤル プラン



この応用設定では、サイト間コールにダイヤリング制限を課すことができます。たとえば、あるユーザ グループが他のサイトにコールすることを禁止する必要がある場合は、そのグループのコーリング サーチ スペースに Global_Translation_pt パーティションを含めないようにします。ただし、このアプローチを選択する場合は次の要素に注意してください。

- トランスレーション パターンの形式が、さらに複雑になります。
- 実質上オンネット公衆網コールを強制することになるため、AAR を設定して、IP WAN の帯域幅が十分にない場合でも公衆網経由でコールを発信できるようにしてください。詳細については、P.10-47 の「マルチサイト配置用の設計ガイドライン」を参照してください。
- 発信されたコール、受信されなかったコール、および受信されたコールのディレクトリには、一意の電話 DN が表示されます。これらの DN に直接到達することはできないため、ユーザは、これらのディレクトリから番号を直接ダイヤルすることはできません。
- 図 10-27 に示した設定では、公衆網コールがすべてのサイトで同じ方法によってダイヤルされることを前提としています。単一の国内で閉じている配置は、通常はこの条件を満たしています。複数の国にわたる配置では、サイト間コールを代行受信するために、国ごとに一連の追加トランスレーション パターンが必要です。
- 複数の国にわたる配置では、可変長の内部 DN を取り扱うという複雑さもあります。E.164 アドレスは、国によって（場合によっては、1 つの国の中でも）長さが異なるためです。

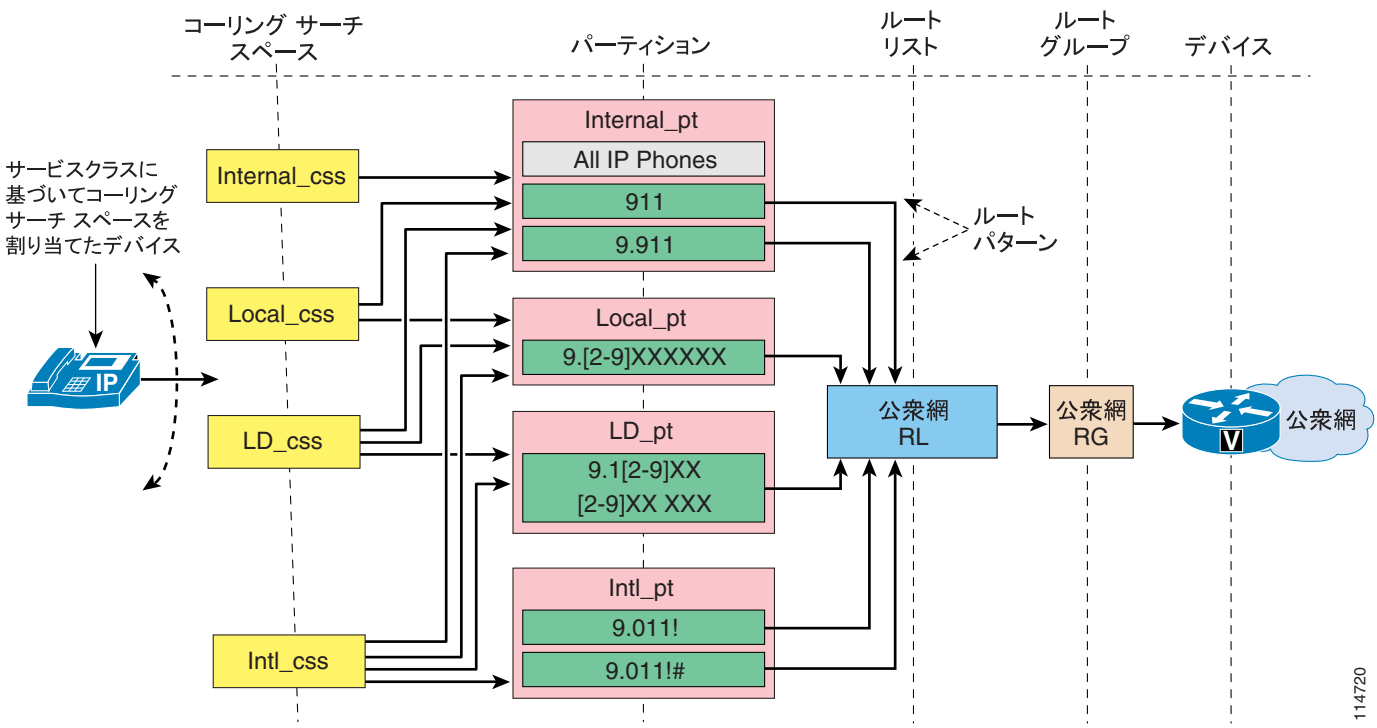
従来のアプローチによる Cisco CallManager のサービス クラスの構築

Cisco CallManager では、次のようにパーティションおよびデバイス コーリング サーチ スペースを外部ルート パターンと組み合せると、IP テレフォニー ユーザにサービス クラスを定義することができます。

- 外部ルート　パターンをコール可能な宛先に関連したパーティションに置きます。1 つのパーティションにすべてのルート パターンを含めることができますが、コール可能な宛先に応じてルート パターンをパーティションに関連付けると、より高度なコール制限ポリシーを実現できます。たとえば、同じパーティションにローカル ルート パターンと国際ルート パターンを入れる場合、すべてのユーザは、ローカルの宛先と海外の宛先の両方と通信できます。ただし、これは好ましくない場合があります。ルート パターンは、さまざまなサービス クラスの到達可能性ポリシーに従って、それぞれのパーティションに分類することをお勧めします。
- 各コーリング サーチ スペースがそのコール制限ポリシーに関連したパーティションのみに到達できるように設定します。たとえば、ローカル コーリング サーチ スペースが内部パーティションとローカル パーティションを指定するように設定します。その結果、このコーリング サーチ スペースに割り当てられるユーザは、内部コールおよびローカル コールしか発信できません。
- Cisco CallManager のデバイス ページで電話を設定して、これらのコーリング サーチ スペースを電話に割り当てます。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 10-28 では、単純な単一サイト配置の例を示しています。

図 10-28　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

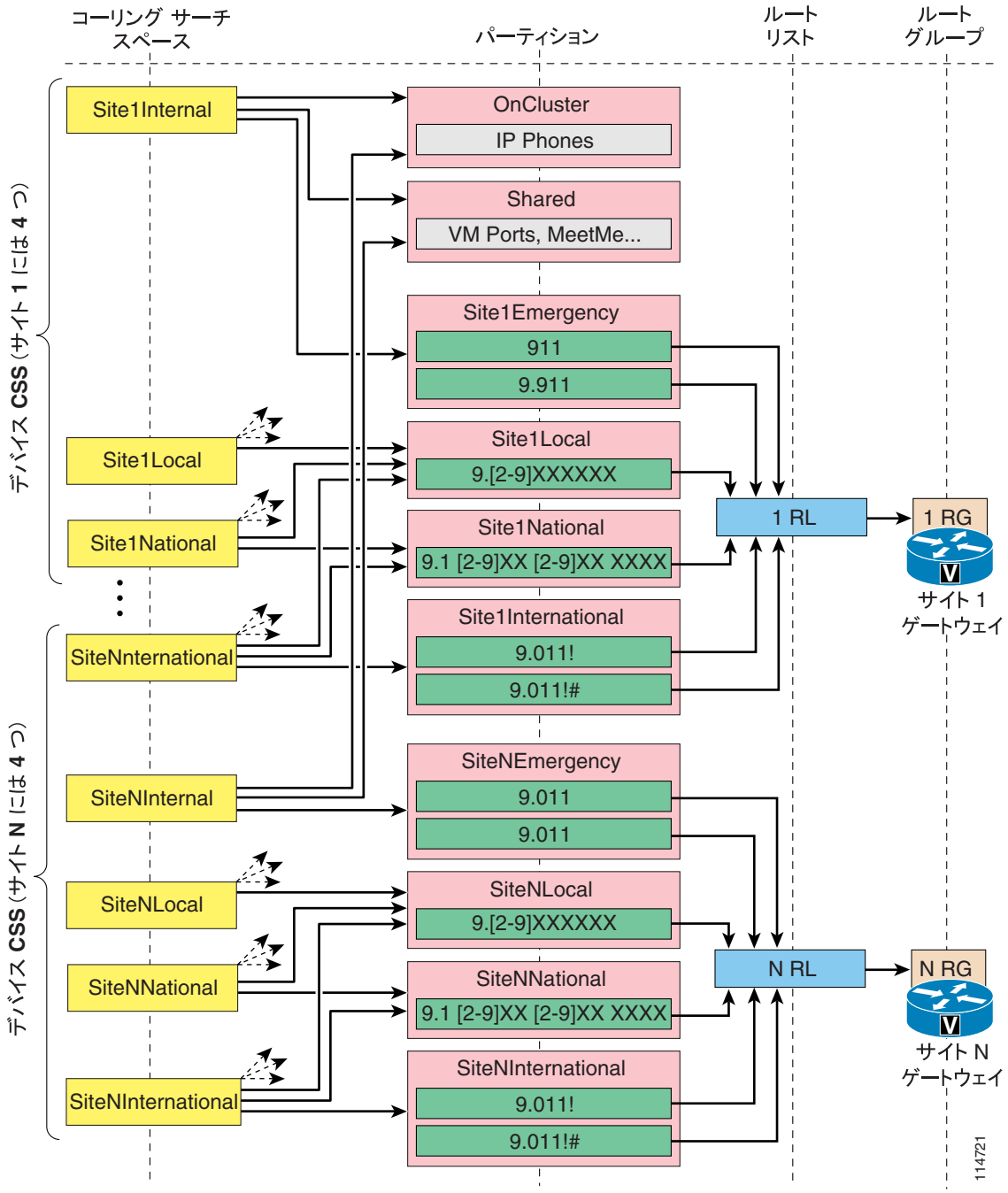
  コーリング サーチ スペースは、特定のパーティションを含んでいます。このパーティションは、特定の公衆網ゲートウェイを指している特定のルート パターンを含んでいます。

- 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 10-29 に示すように、サイトごとにサービス クラスを作成し、同時に、ローカル支店ゲートウェイから発信される公衆網コールをルーティングする必要があるためです。

図 10-29　従来のアプローチで必要となるコーリング サーチ スペースとパーティション



集中型コール処理を使用するマルチサイト配置に対してこのダイヤル プラン アプローチを適用する場合は、さらに次のガイドラインに従ってください。

- サイト間のオンネット ダイヤリングを構成するために、すべての IP Phone の DN をすべてのサイトのコーリング サーチ スペースからアクセス可能なオンクラスタまたは内部のパーティションに置きます。これは、IP Phone の DN が重複している場合は不可能であることに注意してください。重複内線番号を使用するダイヤル プランの詳細については、P.10-53 の「分割アドレッシングを使用する可変長オンネット ダイヤル プランの配置」を参照してください。
- 各リモート サイトに、独自のパーティションとルート パターンのセットを指定します。リモート サイトごとのパーティション数は、ルート パターンに関連したコール制限ポリシー数によって異なります。
- 各サイトに、そのサイトの IP Phone 用に独自のコーリング サーチ スペースのセットを指定します。このコーリング サーチ スペースは、適切なローカル ルート パターン パーティションと共に、オンクラスタ パーティションも指定します。
- 企業の自動転送制限ポリシーによっては、サイト固有のデバイス コーリング サーチ スペースの 1 つを Forward All コーリング サーチ スペースに再利用することができます。

必要なコーリング サーチ スペースの合計数とパーティションの合計数を計算するには、通常は次の公式を使用してください。

合計パーティション数 =（サービス クラス数）*（サイト数）+（すべての IP Phone の DN 用に 1 パーティション）

合計コーリング サーチ スペース数 =（サービス クラス数）*（サイト数）

（注） これらの値は、最低限必要となるパーティション数とコーリング サーチ スペース数を表しています。特殊なデバイスやアプリケーションには、他のコール処理エージェント用のオンネット パターンと同様に、追加のパーティションやコーリング サーチ スペースが必要になることがあります。

従来のアプローチにおけるエクステンション モビリティの考慮事項

エクステンション モビリティ機能を使用する場合、電話機のダイヤル制限は、その電話機へのログイン（またはログアウト）中の機能の 1 つになります。ログアウトされた電話機は、他の電話機やサービス（たとえば、米国では 911）のコールを制限する必要があります。一般に、公衆網を通じた市内または市外通話へのアクセスは制限されます。逆に、ユーザがログインしている電話機は、そのユーザのダイヤリング権限に応じてコールを許可し、それらのコールを適切なゲートウェイ（たとえば、同じ場所に配置されているローカル コール用の支店ゲートウェイ）にルーティングする必要があります。

エクステンション モビリティを使用する場合、サービス クラスを構築するための従来のアプローチでコール制限を適用するには、次のガイドラインを考慮してください。

- 各サイトで、すべての IP Phone のデバイス コーリング サーチ スペースを、公衆網緊急サービスのみを（ローカル ゲートウェイを使用して）指すように設定します。
- エクステンション モビリティに使用される IP Phone がログアウト状態になっている場合の回線コーリング サーチ スペースを、内部番号のみを指すように設定します。
- 各エクステンション モビリティ ユーザについて、デバイス プロファイル内の回線コーリング サーチ スペースを、個々のユーザのサービス クラスで許可されている内部番号と追加公衆網ルート パターンを（ここでも、企業ポリシーに従って適切なゲートウェイを使用して）指すように設定します。

通常はサイト 1 を拠点としているエクステンション モビリティ ユーザが、サイト 2 の IP Phone にログインすると、公衆網コールのパス選択が次のように変更されます。

- 緊急コールは、サイト 2 の公衆網ゲートウェイを使用して正しくルーティングされます。緊急サービスは、サイト 2 にある IP Phone のデバイス コーリング サーチ スペースによって提供されるためです。
- この他のすべての公衆網コールは、エクステンション モビリティ ユーザのプロファイル（具体的には、デバイス プロファイル内に設定されている回線コーリング サーチ スペース）に従ってルーティングされます。これは、通常、これらの公衆網コールが 2 つの WAN リンクを通過し、サイト 1 のゲートウェイを使用して公衆網にアクセスすることを意味します。

この動作を修正し、エクステンション モビリティ ユーザが別のサイトにローミングしている場合でも、公衆網コールが常にローカル公衆網ゲートウェイを通じてルーティングされるようにするには、次のいずれかの方法を使用します。

- ローカル公衆網ルート パターンは、デバイス コーリング サーチ スペースに含めて、デバイス プロファイル内の回線コーリング サーチ スペースからは削除します。この方法によって、ローカルの公衆網コールは、同じ場所にある支店ゲートウェイを通じてルーティングされるようになります。ただし、同時に、ユーザは IP Phone にログインしなくてもこれらのコールをダイヤルできるようになります。長距離電話と国際コールについては、エクステンション モビリティ ユーザのデバイス プロファイルに従ってルーティングされます。したがって、このソリューションが適しているのは、通常これらのコールが中央ゲートウェイを通じてルーティングされている場合のみです。
- 各ユーザに対して、ユーザがローミングするサイトごとに 1 つずつ、複数のデバイス プロファイルを定義します。各デバイス プロファイルの設定では、回線コーリング サーチ スペースが、そのサイトのローカル ゲートウェイを使用する公衆網ルート パターンを指すようにします。ローミングするユーザおよびローミング先となるサイトが非常に多い場合、この方法は設定と管理の負荷が大きくなります。
- 次の項（P.10-69 の「回線 / デバイス アプローチによる Cisco CallManager のサービス クラスの構築」）で説明する回線 / デバイス アプローチを実装します。

回線 / デバイス アプローチによる Cisco CallManager のサービス クラスの構築

前の項で説明した従来のアプローチは、集中型コール処理を使用した大規模なマルチサイト配置に適用する場合、結果的にパーティションとコーリング サーチ スペースの数が非常に多くなることがあります。このような構成にする必要があるのは、デバイス コーリング サーチ スペースを使用して、パス選択（外部コールにどの公衆網ゲートウェイを使用するか）とサービス クラスの両方を決定しているためです。

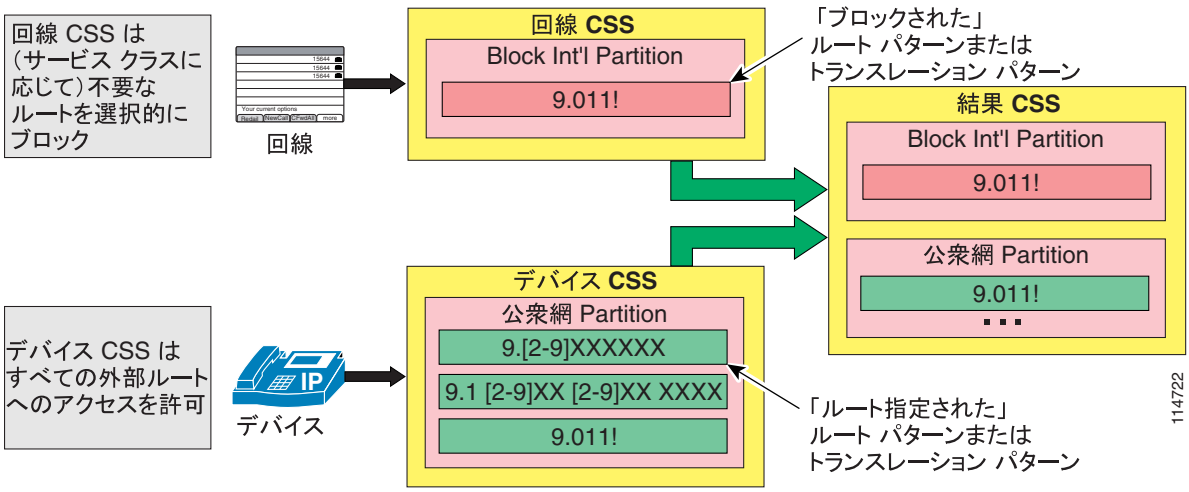
これらの 2 つの機能を回線コーリング サーチ スペースとデバイス コーリング サーチ スペースに分配すると、必要となるパーティションとコーリング サーチ スペースの総数を大幅に減らすことができます。この手法を「回線 / デバイス アプローチ」と呼びます。

所定の各 IP Phone の回線コーリング サーチ スペースとデバイス コーリング サーチ スペースが Cisco CallManager でどのように組み合されているか、および回線コーリング サーチ スペースのパーティションが、結果のコーリング サーチ スペースでどのようにして最初に表示されるのか（P.10-14 の「Cisco CallManager におけるコール特権」を参照）に注目すると、回線 / デバイス アプローチでは、一般に次の規則を適用できます。

- デバイス コーリング サーチ スペースは、コール ルーティング情報（たとえば、どのゲートウェイを公衆網コール用に選択するか）を提供するために使用します。
- 回線コーリング サーチ スペースは、サービス クラス情報（たとえば、どのコールを許可するか）を提供するために使用します。

これらの規則がどのように適用されるのかをわかりやすくするために、図 10-30 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 10-30　回線 / デバイス アプローチにおける重要な概念



同時に、回線コーリング サーチ スペースは、トランスレーション パターンが 1 つのみ入ったパーティションを保持しています。このパターンは国際番号に一致し、ブロック パターンとして設定されています。

したがって、結果のコーリング サーチ スペースには、国際番号に一致する 2 つの同一パターンが保持されています。最初に表示されるのは、回線コーリング サーチ スペースに含まれているブロック パターンです。結果として、この回線からの国際通話はブロックされます。

回線コーリング サーチ スペースでは、トランスレーション パターンの代わりに、ルート パターンを使用してコールをブロックすることもできます。ブロック ルート パターンを設定するには、まず、使用されていない IP アドレスを使用して「ダミー」ゲートウェイを作成し、そのゲートウェイを「ダミー」ルート リストおよびルート グループに配置します。次に、ダミー ルート リストを指すようにルート パターンを設定します。コールをブロックするルート パターンとトランスレーション パターンの主な違いは、ブロックされている番号をエンドユーザがダイヤルしようとしたときの対応です。次に例を示します。

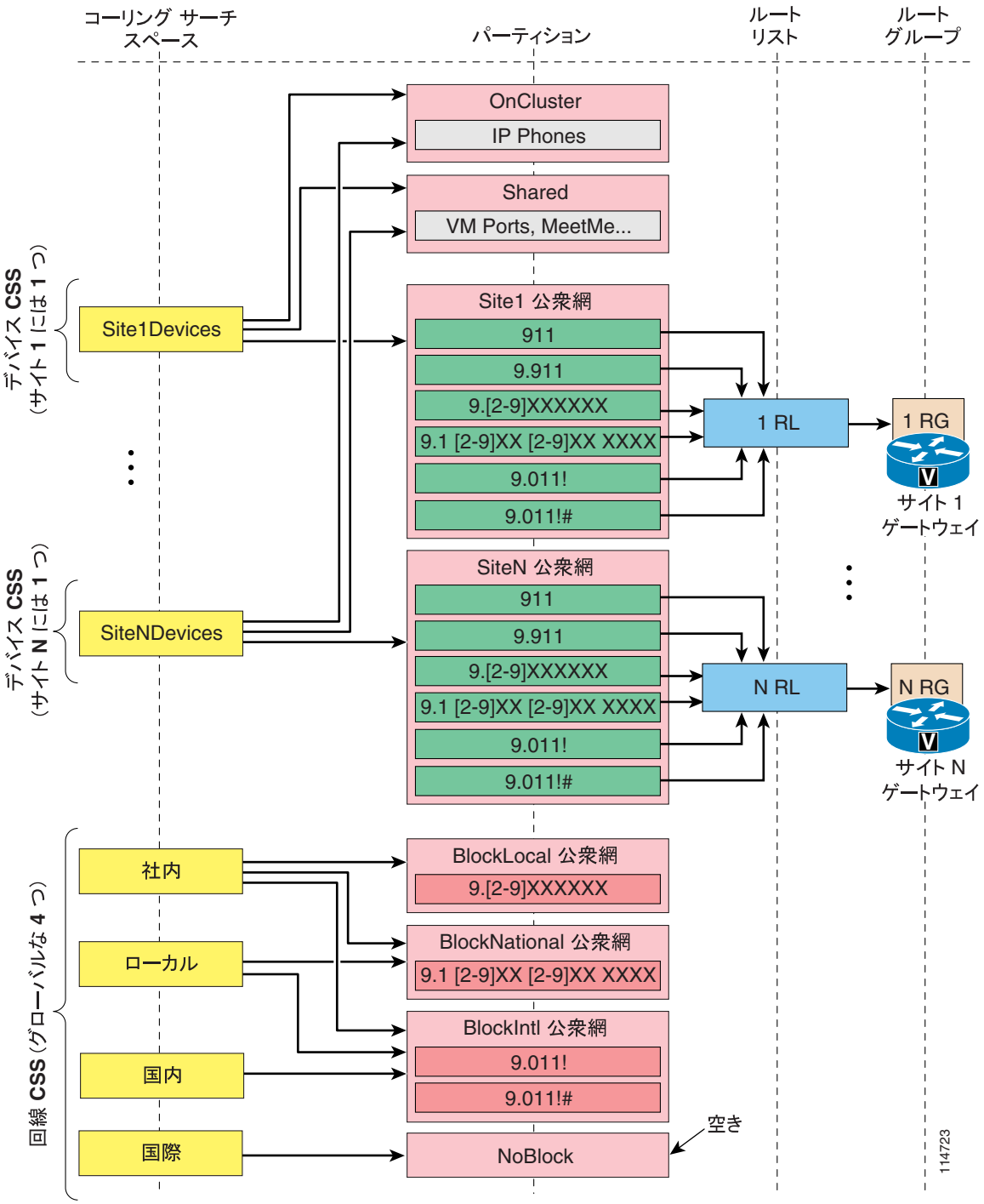
- トランスレーション パターンを使用した場合、エンドユーザは番号を最後までダイヤルできます。ダイヤルが完了した時点でのみ、ユーザにファースト ビジー トーンが再生されます。
- ルート パターンを使用した場合は、エンドユーザのダイヤルしている番号が許可パターンに一致する可能性がなくなると、その時点ですぐにファースト ビジー トーンが再生されます。

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 10-31 では、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 10-31　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。

サイトの数が多い集中型コール処理配置に対して回線 / デバイス アプローチを適用すると、必要となるパーティションとコーリング サーチ スペースの数が大幅に減少します。たとえば、100 のリモート サイトと 4 つのサービス クラスがある配置の場合、従来のアプローチでは、少なくとも 401 のパーティションと 400 のコーリング サーチ スペースが必要です。回線 / デバイス アプローチでは、105 のパーティションと 104 のコーリング サーチ スペースしか必要ありません。

ただし、回線 / デバイス アプローチが成立するのは、特定サービス クラスの使用を制限する必要のある公衆網コールのタイプ（たとえば、市内電話、長距離電話、国際コール）を、グローバルに識別できる場合です。使用している国の国内番号計画が原因で、コール タイプをグローバルに識別することができない場合、このアプローチの効果は、（設定の省力化に関しては）上の公式に示したものよりも小さくなります。

たとえば、フランスでは、番号計画は 5 桁のエリア コード（01 ～ 05、および携帯電話の 06 エリア コード）に基づいており、この後に 8 桁の加入者番号が続きます。ここで重要となる特徴は、各公衆網宛先に到達するとき、同じローカルエリアからコールするときも、別のエリアからコールするときも、必ず同じ番号（たとえば、Paris の番号は 01XXXXXXXX、Nice の番号は 02XXXXXXXX など）をダイヤルすることです。つまり、「長距離電話」であるかどうかは、発信者がどのエリアにいるかに応じて変化します。このため、1 つのパーティションと 1 つのルート パターンでは、長距離電話へのアクセスをブロックできません。たとえば、発信者が Paris にいる場合、014455667788 へのコールは市内電話ですが、発信者が Nice や Lyon にいる場合は長距離電話です。

このような場合は、市内電話と長距離電話が同じ方法でダイヤルされるエリアごとに 1 つずつ、一連のブロック用コーリング サーチ スペースとパーティションを追加設定する必要があります。フランスの例では、表 10-8 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!#
Local03_css	BlockLD03_pt	0.0[124-6]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
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。

- 自動転送のコーリング サーチ スペース（Forward Busy、Forward No Answer、および Forward All）は、回線またはデバイスのコーリング サーチ スペースとは連結されません。
- Forward Busy および Forward No Answer コーリング サーチ スペースは、ボイスメール パイロット番号およびポートに到達できる、グローバル コーリング サーチ スペースに設定します。
- Forward All コーリング サーチ スペースは、企業のポリシーに従って設定します。
  - 転送コールが無制限の特権を持つ必要がある場合は、サイト固有のデバイス　コーリング サーチ スペースに一致するように Forward All コーリング サーチ スペースを設定します（エクステンション モビリティを使用する場合の追加の考慮事項については、P.10-74 の「回線 / デバイス アプローチにおけるエクステンション モビリティの考慮事項」を参照）。
  - 転送コールを内部番号のみに制限する必要がある場合は、Forward All コーリング サーチ スペースを、内部番号にのみ到達可能なグローバル コーリング サーチ スペースに設定します。
  - 転送コールに中間的な制限を適用する必要がある場合は（ローカル公衆網番号へのアクセスに適用し、国際番号には適用しないなど）、サイト固有の追加のコーリング サーチ スペースが必要になるため、回線 / デバイス アプローチの効果は小さくなります。このような場合は、従来のアプローチを選択することをお勧めします。
- このアプローチが機能するには、回線コーリング　サーチ　スペース内に設定するブロック　パターンの詳細度が、デバイス コーリング サーチ スペース内に設定したルート パターンと少なくとも同等になっている必要があります。エラーが発生することを避けるために、ブロックの対象となるパターンは、可能な場合にはルーティングを許可するパターンよりも詳細に設定することをお勧めします。@ ワイルドカード内に定義されるパターンは非常に詳細なものになるため、このワイルドカードの取り扱いには十分に注意してください。
- オンネット DN がダイヤルされると、AAR が呼び出されます。これらの DN へのアクセスは、上で説明したものと同じプロセスで制御できます。AAR は、再ルーティングされるコールには別のコーリング サーチ スペースを使用します。ほとんどの場合、AAR コーリング サーチ スペースは、サイト固有の無制限デバイス コーリング サーチ スペースと同じものでかまいません。このコーリング サーチ スペースは、エンドユーザによって直接ダイヤルされることがないためです。

（注） 回線とデバイスの優先順位は、CTI デバイス（CTI ルート ポイントと CTI ポート）に関しては逆になります。これらのデバイスの場合、結果のコーリング サーチ スペースでは、デバイス コーリング サーチ スペースに含まれているパーティションが、回線コーリング サーチ スペースよりも前に配置されます。したがって、回線 / デバイス アプローチを Cisco IP SoftPhone などの CTI デバイスに適用することはできません。

回線 / デバイス アプローチにおけるエクステンション モビリティの考慮事項

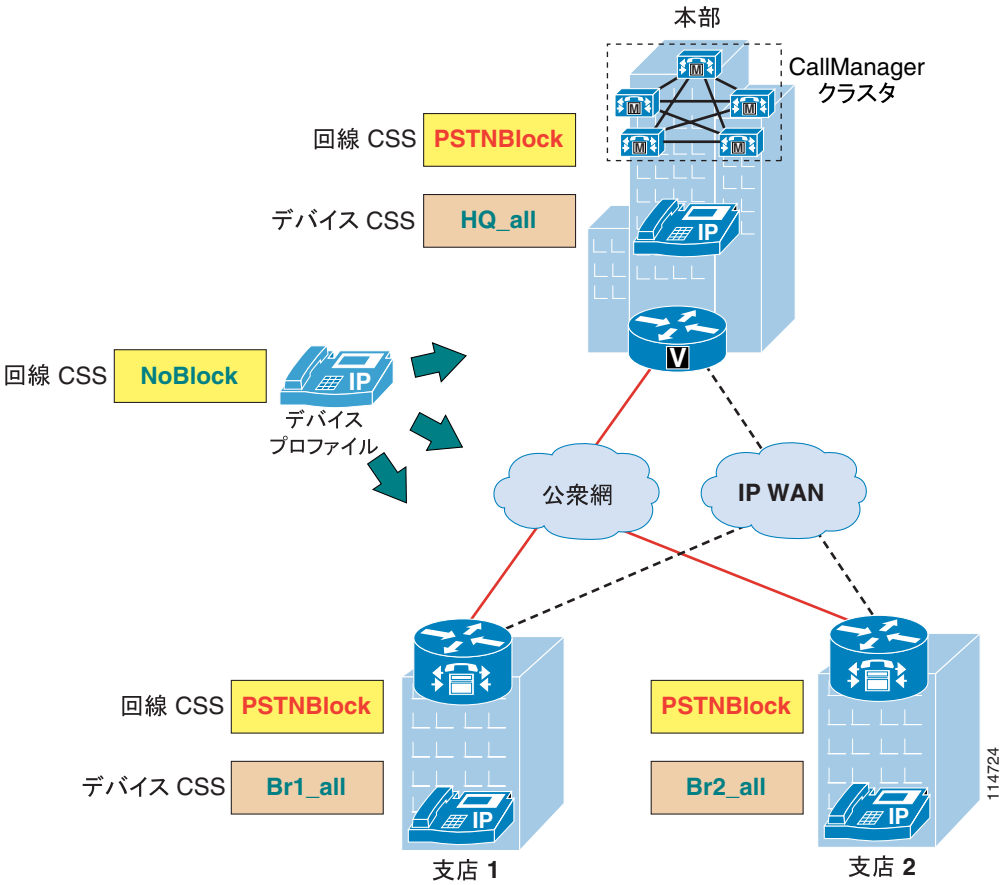
エクステンション モビリティ機能を使用する場合、電話機のダイヤル制限は、回線 / デバイス アプローチを使用することによって、その電話機へのログイン（またはログアウト）中の機能の 1 つとして自然な方法で実装できます。ログアウトされた電話機は、他の電話機やサービス（たとえば、米国では 911）のコールを制限する必要があります。一般に、公衆網を通じた市内または市外通話へのアクセスは制限されます。逆に、ユーザがログインしている電話機は、そのユーザのダイヤリング権限に応じてコールを許可し、それらのコールを適切なゲートウェイ（たとえば、同じ場所に配置されているローカル コール用の支店ゲートウェイ）にルーティングする必要があります。

サービス クラスの構築に回線 / デバイス アプローチを使用する場合は、前の項で説明したものと同じ規則を、エクステンション モビリティのデバイス プロファイル コンストラクトに適用するだけで済みます。エクステンション モビリティ使用時にコール制限を適用するには、次のガイドラインを考慮してください。

- 一致する可能性のあるすべての公衆網ルート パターンが入っていて、それらのパターンを適切にルーティングする（たとえば、緊急コールと市内電話にはローカル ゲートウェイを使用し、長距離電話には中央ゲートウェイを使用する）サイト固有のパーティションを指すように、各サイトのすべての IP Phone のデバイス コーリング サーチ スペースを設定します。
- ユーザがログインしていないときでも許可されるコール（たとえば、内部内線番号と緊急サービス）以外のコールをすべてブロックするブロック トランスレーション / ルート パターンを備えたグローバル コーリング サーチ スペースを指すように、すべての IP Phone の回線コーリング サーチ デバイス（または、デフォルト ログアウト デバイス プロファイルの回線コーリング サーチ スペース）を設定します。
- エクステンション モビリティ ユーザごとに、特定のサービス クラスに対して許可しない公衆網コールを選択してブロックする（たとえば、国際コールのみをブロックする）ブロック トランスレーション / ルート パターンを備えたグローバル コーリング サーチ スペースを指すように、回線コーリング サーチ スペースをデバイス プロファイル内に設定します。一部のユーザに無制限のコール特権を与える必要がある場合は、それらのユーザを空のパーティションを備えた回線コーリング サーチ スペースに割り当てます。

エクステンション モビリティに回線 / デバイス アプローチを使用することの主な利点は、図 10-32 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 10-32　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。

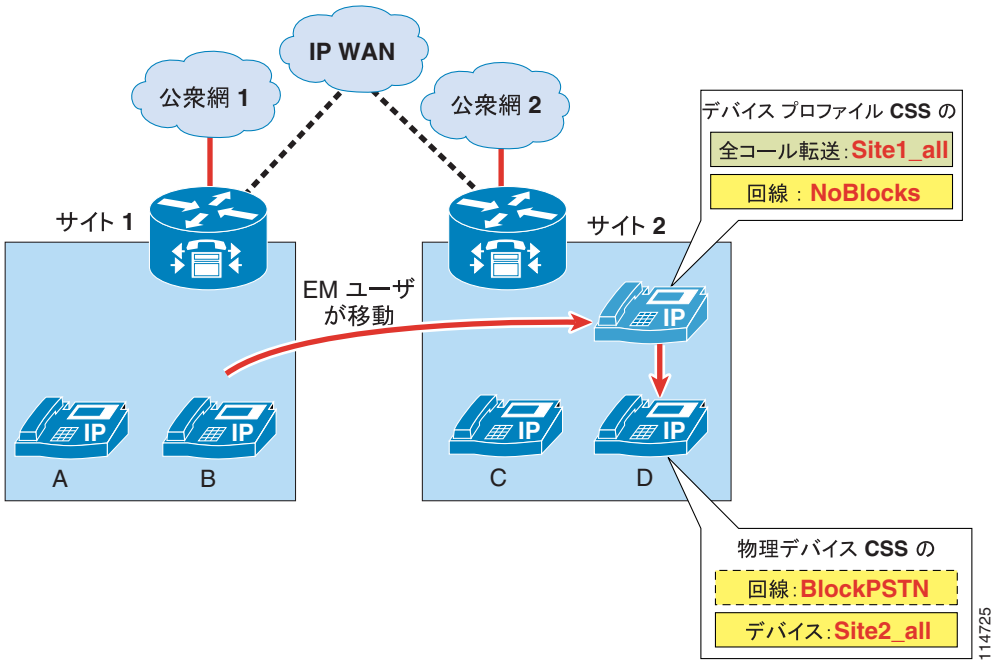
つまり、回線 / デバイス アプローチをエクステンション モビリティに使用する場合は、エンドユーザがログイン先サイトのダイヤリング手順に従う必要があります。

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 10-33 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 10-33　回線 / デバイス アプローチを使用したエクステンション モビリティにおける自動転送の考慮事項



P.10-18 の「自動転送コーリング サーチ スペース」の項で説明したように、Forward All コーリング サーチ スペースは、回線およびデバイスのコーリング サーチ スペースとは連結されないため、Site1_all に設定する必要があります。Site1_all は、サイト 1 のゲートウェイを使用するすべての公衆網ルートを含んでいます。

このユーザがサイト 2 に移動して電話 D にログインすると、ユーザのデバイス プロファイルに従って、このプロファイルの回線コーリング サーチ スペースと Forward All コーリング サーチ スペースが物理デバイスに適用されます。直接公衆網コールの場合、使用されるコーリング サーチ スペースは、回線とデバイスのコーリング サーチ スペースを連結したものです。電話 D のデバイス コーリング サーチ スペース（Site2_all）は、サイト 2 のゲートウェイを正しく指しています。

このユーザが、すべてのコールを公衆網番号に転送するように電話を設定すると、転送されるすべてのコールは、Site1_all コーリング サーチ スペースを使用します。Site1_all は、サイト 1 のゲートウェイを指したままです。この状態になると、次のような動作が発生します。

- 着信公衆網コールは、サイト 1 のゲートウェイで IP ネットワークに入り、同じゲートウェイ内で公衆網にヘアピンされます。
- サイト 1 の電話（電話 A など）から発信されるコールは、サイト 1 のゲートウェイを通じて公衆網に正しく転送されます。

- サイト 2 の電話（電話 C など）から発信されるコールは、WAN を経由してサイト 1 に到達し、サイト 1 のゲートウェイを通じて公衆網にアクセスします。同じ Cisco CallManager クラスタ内の他のサイトから発信されるコールに対しても、同じ動作が適用されます。

ネットワークを設計し、ユーザをトレーニングするときは、この動作に注意してください。

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 CallManager マルチサイト配置
- Cisco CallManager Express 配置

集中型コール処理を使用する Cisco CallManager マルチサイト配置では、通常、サービス クラスは Cisco CallManager でパーティションとコーリング サーチ スペースを使用して実装します。ただし、支店サイトと中央サイト間の IP WAN 接続が失われた場合は、Cisco SRST が支店 IP Phone の制御を取得し、パーティションとコーリング サーチ スペースに関する設定は、IP WAN 接続が復旧するまですべて使用できなくなります。したがって、SRST モードで動作している支店ルータ内にサービス クラスを実装することが望ましくなります。

同様に、Cisco CallManager Express 配置の場合も、ルータには IP Phone 用のサービス クラスを実装するメカニズムが必要です。

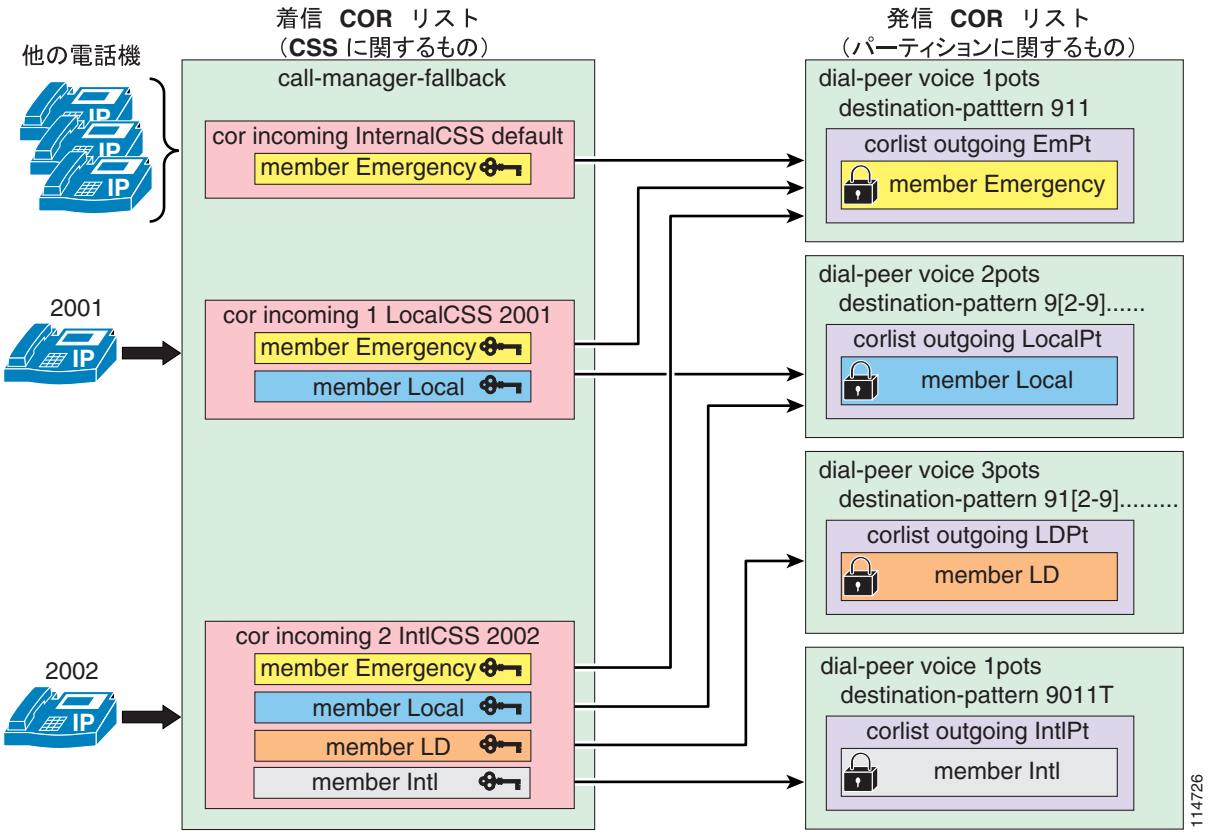
どちらの事例でも、制限クラス（COR）機能を使用して、サービス クラスを Cisco IOS ルータ内に定義します（COR の詳細については、P.10-42 の「H.323 ダイヤル ピアを使用する Cisco IOS のコール特権」を参照）。

次の主要ガイドラインに従うと、COR 機能を調整して、Cisco CallManager のパーティションとコーリング サーチ スペースという概念を再現することができます。

- 区別する必要のあるコールのタイプごとに、タグを定義する。
- 各コール タイプをルーティングするそれぞれの POTS ダイヤル ピアに対して、メンバー タグを 1 つだけ含んだ、「基本的な」発信 COR リスト（パーティションに相当）を割り当てる。
- 各種のサービス クラスに属している IP Phone に対して、メンバー タグのサブセットを含んだ、「複雑な」着信 COR リスト（コーリング サーチ スペースに相当）を割り当てる。

図 10-34 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 10-34　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 10-34 のような Cisco IOS ソリューションの実装例とガイドラインを示します。

ステップ 1　**dial-peer cor custom** コマンドを使用して、各種コールの内容をわかりやすく表しているタグを定義します（この例では、Emergency、VMail、Local、LD、Intl）。

```
dial-peer cor custom
  name Emergency
  name VMail
  name Local
  name LD
  name Intl
```

ステップ 2　**dial-peer cor list** コマンドを使用して、パーティションとして使用される基本的な COR リストを定義します。各リストには、タグを 1 つのみメンバーとして含めます。

```
dial-peer cor list EmPt
  member Emergency

dial-peer cor list VMailPt
  member VMail

dial-peer cor list LocalPt
  member Local

dial-peer cor list LDPt
  member LD

dial-peer cor list IntlPt
  member Intl
```

ステップ 3　**dial-peer cor list** コマンドを使用して、コーリング サーチ スペースとして使用される比較的複雑な COR リストを定義します。各リストには、必要となるサービス クラスに従って、タグのサブセットをメンバーとして含めます。

```
dial-peer cor list InternalCSS
  member Emergency
  member VMail

dial-peer cor list LocalCSS
  member Emergency
  member VMail
  member Local

dial-peer cor list LDCSS
  member Emergency
  member VMail
  member Local
  member LD

dial-peer cor list IntlCSS
  member Emergency
  member VMail
  member Local
  member LD
  member Intl
```

ステップ 4　**corlist outgoing** *corlist-name* コマンドを使用して、基本的な「パーティション」COR リストを、対応する POTS ダイヤル ピアに割り当てる発信 COR リストとして設定します。

```
dial-peer voice 100 pots
  corlist outgoing EmPt
  destination-pattern 911
  no digit-strip
  direct-inward-dial
  port 1/0:23

dial-peer voice 101 pots
  corlist outgoing VMailPt
  destination-pattern 914085551234
  forward-digits 11
  direct-inward-dial
  port 1/0:23

dial-peer voice 102 pots
  corlist outgoing LocalPt
  destination-pattern 9[2-9].....
  forward-digits 7
  direct-inward-dial
  port 1/0:23

dial-peer voice 103 pots
  corlist outgoing LDPt
  destination-pattern 91[2-9]..[2-9].....
  forward-digits 11
  direct-inward-dial
  port 1/0:23

dial-peer voice 104 pots
  corlist outgoing IntlPt
  destination-pattern 9011T
  prefix-digits 011
  direct-inward-dial
  port 1/0:23
```

ステップ 5　**cor incoming** コマンドを **call-manager-fallback** 設定モードで使用して、「コーリング サーチ スペース」として機能する複雑な COR リストを、各種の電話 DN に割り当てる着信 COR リストとして設定します。

```
call-manager-fallback
  cor incoming InternalCSS default
  cor incoming LocalCSS 1 3001 - 3003
  cor incoming LDCSS 2 3004
  cor incoming IntlCSS 3 3010
```

SRST 用の COR を配置する場合は、次の制限事項に注意してください。

- Cisco IOS Release 12.2(8)T 以降で使用可能な SRST バージョン 2.0 では、**call-manager-fallback** で許容される **cor incoming** ステートメントの数は、最大で 5（デフォルト ステートメント含まず）です。
- Cisco IOS Release 12.3(4)T 以降で使用可能な SRST バージョン 3.0 では、**call-manager-fallback** で許容される **cor incoming** ステートメントの数は、最大で 20（デフォルト ステートメント含まず）です。

したがって、デフォルト以外の特権を持つユーザの電話 DN が連続しておらず、SRST サイトが比較的大きい場合は、SRST モードのサービス クラスの数を減らして、これらの制限値を超えずにすべての DN に対応できるようにする必要があります。

上の例は Cisco SRST に基づいていますが、Cisco CallManager Express 配置にも同じ概念を適用することができます。ただし、次の考慮事項があります。

- Cisco CallManager Express を使用している場合は、サービス クラスを表現している COR リスト（コーリング サーチ スペースに相当するもの）を個々の IP Phone に直接割り当てることができます。割り当てるには、**cor** {**incoming** | **outgoing**} *corlist-name* コマンドを **ephone-dn** *dn-tag* 設定モードで使用します。
- COR リストの設定されていない IP Phone は、COR の一般規則に従って、発信 COR リストの内容に関係なくすべてのダイヤル ピアに無制限にアクセスできます。Cisco CallManager Express は、すべての電話にデフォルトの制限を適用する、**cor incoming** *corlist-name* **default** コマンドに相当するメカニズムを備えていません。

コール カバレッジの配置

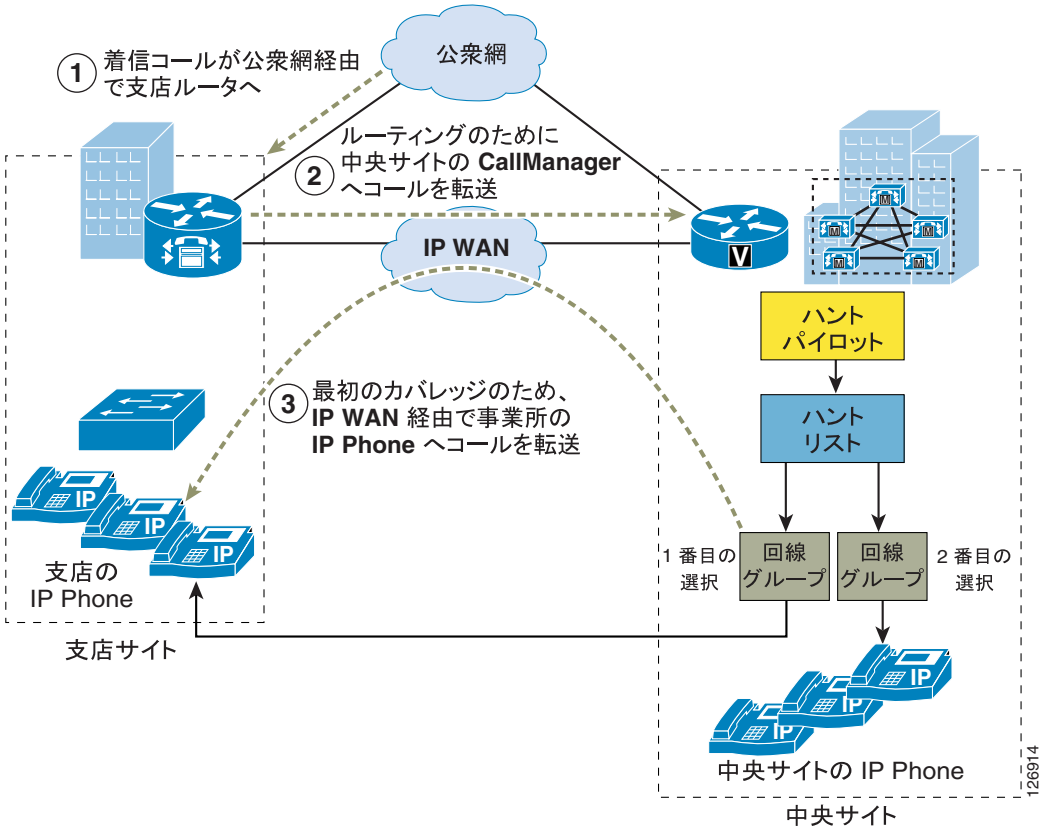
コール カバレッジ機能は、多くの IP テレフォニー配置で重要となる機能です。顧客サービスを重視する多くの企業では、顧客のコールを適切なサービス部門に迅速にルーティングすることが必須になります。この項では、ハント パイロット、ハント リスト、および回線グループに基づいたハンティング メカニズムを使用して、Cisco CallManager 4.1 でコールを分配する場合の設計ガイドラインを中心に説明します。ここでは、次のトピックを主に扱います。

- 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.10-81）
- Cisco CallManager 4.1 を使用する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.10-82）

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 10-35 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 10-35　集中型コール処理配置における複数のサイト間でのコール カバレッジ



集中型の IP テレフォニー システムでは、Automated Alternate Routing（AAR）や Survivable Remote Site Telephony（SRST）などの機能を有効にすることで、高い可用性を実現できます。AAR 機能や SRST 機能を有効にした上でコール カバレッジ機能を配置する場合は、次のガイドラインを考慮してください。

- 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、ロケーションの帯域幅が不足していたためにいずれかの回線グループ メンバーへのコールが Cisco CallManager によってブロックされた場合には、AAR を使用して再ルーティングされることはありません。代わりに、Cisco CallManager はコールを使用可能な次のメンバーまたは回線グループに分配します。

（注） ハント パイロットによって分配されるコールは、Cisco CallManager 4.1(3) の AAR を使用することができます。ただし、AAR を使用するのは、回線グループ内でボイスメール ポートを使用している場合のみにすることを強くお勧めします。

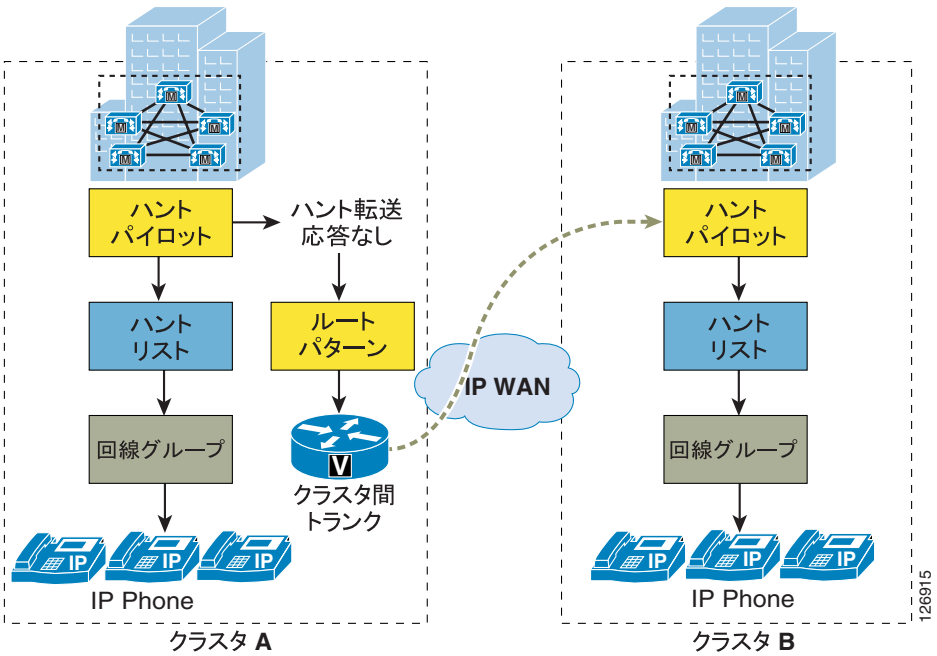
- Survivable Remote Site Telephony（SRST）
  - Cisco CallManager がハント パイロットのコールを受信したとき、その回線グループ メンバーの一部が、SRST モードで動作しているリモート サイトにある場合、Cisco CallManager はそれらのメンバーをスキップし、使用可能な次の回線グループ メンバーにコールを分配します。Cisco CallManager から見ると、SRST モードで動作しているメンバーは未登録であり、ハント パイロットのコールは未登録メンバーには転送されません。
  - SRST モードで動作しているルータがハント パイロットのコールを受信したときは、コール カバレッジ機能を使用できません。このコールは、使用可能な登録済み内線番号にコールを再ルーティングする設定が追加されていない場合、失敗します。**alias** コマンドまたは **default-destination** コマンドを Cisco IOS の **call-manager-fallback** モードで使用すると、ハント パイロットを宛先とするコールをオペレータ内線またはボイスメールに再ルーティングすることができます。

Cisco CallManager 4.1 を使用する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 CallManager Release 4.1 以降では、ルート グループをハント リストに追加することができなくなりました。このため、ハント リストを使用して、コールを他のクラスタまたはリモート ゲートウェイに送信することはできません。ただし、Cisco CallManager 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 10-36 では、クラスタ間トランクを使用する分散型コール処理配置における、ハント リストの設定例を示しています。この例では、ハント パイロットのコールが最初にクラスタ A の内部に分配されることを前提としています。コールに対する応答がない場合は、ルート パターンに一致する Forward Hunt No Answer 設定を使用して、コールがコール分配のためにクラスタ B に再ルーティングされます。このルート パターンは、クラスタ B に向かうクラスタ間トランクを指しています。

図 10-36　Cisco CallManager 4.1 分散型コール処理配置におけるクラスタ間でのコール カバレッジ

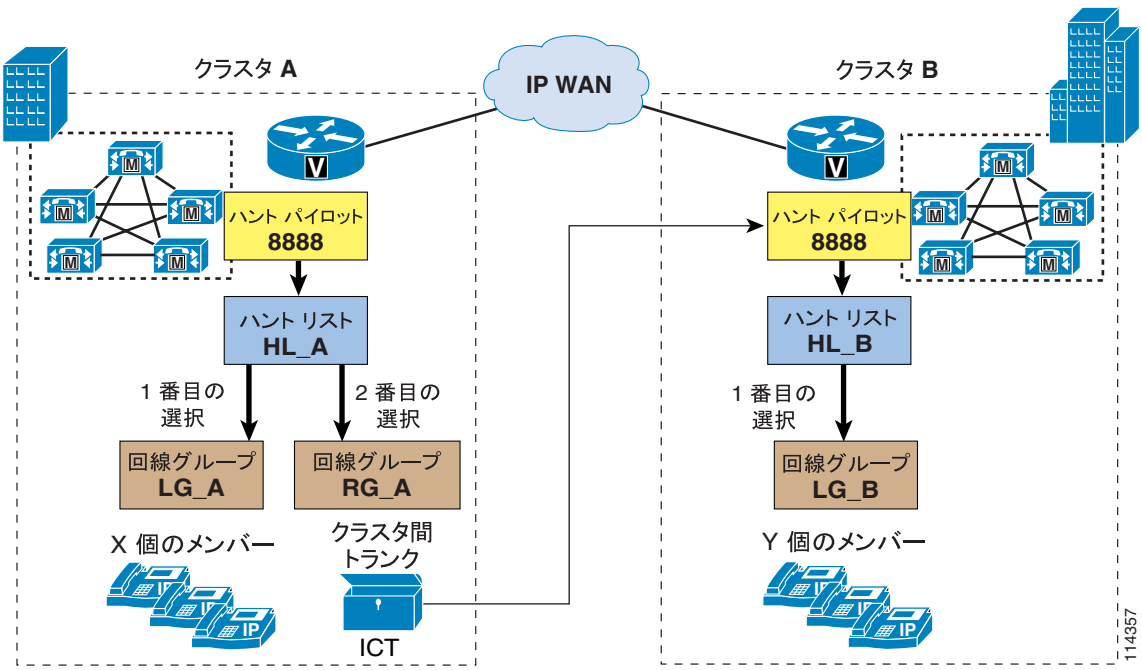


ヒント　分散型コール処理配置では、Cisco VoIP ゲートウェイとゲートキーパーを使用して、着信するハント パイロット コールの負荷共有を管理できます。あるクラスタ内でコールに応答がなかった場合は、そのコールを別のクラスタにオーバーフローしてサービスを提供できます。コールは、ゲートウェイまたはトランクを通じて IVR 処理に送信することもできます。Tool Command Language（TCL）IVR アプリケーションは、Cisco IOS ゲートウェイ上に実装できます。

Cisco CallManager 4.0 を使用する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

図 10-37 では、クラスタ間トランクを使用する分散型コール処理配置における、ハント リストの設定例を示しています。この例では、ハント パイロットのコールが最初にクラスタ A の内部に分配されることを前提としています。コールに対する応答がない場合は、コールがクラスタ B に再ルーティングされ、メンバーを通じて分配されます。

図 10-37　Cisco CallManager 4.0 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



次の各項では、クラスタ間トランクを使用して複数のクラスタを横断するコールのルーティングについて説明します。このコール フローは、他のゲートウェイ デバイスやトランク デバイスの場合と類似しています。

構成

図 10-37 では、A と B という 2 つのクラスタを示しています。クラスタは両方ともルート パターンとハント パイロット 8888 を保持していて、それぞれのクラスタは、ハント リスト HL_A と HL_B に関連付けられています。クラスタ A のハント リスト HL_A は、X 個のメンバーが入った回線グループ LG_A、およびルート グループ RG_A を保持しており、クラスタ A とクラスタ B の間には、クラスタ間トランクが定義されています。クラスタ B のハント リスト HL_B は、Y 個のメンバーが入った回線グループ LG_B を保持しています。

コール フロー

図 10-37 のコール フローには、次の一連のイベントが関係しています。

1. クラスタ A がハント パイロット 8888 のコールを受信し、このコールが、まず LG_A のメンバーを通じて分配されます。
2. コールが LG_A のメンバーによって応答されず、ルート グループ RG_A を使用してクラスタ B に転送されます（番号変換は発生していないものとし、コールの宛先はまだ 8888 です）。

   コール アドミッション制御によって、または宛先デバイスが未登録であるためにコールが拒否された場合、そのコールは、HL_A に含まれている次のルート グループ メンバー宛てに再ルーティングされます（メンバーが存在する場合）。コールを HL_A に含まれている他のルート グループ メンバーに再ルーティングすることができるのは、クラスタ間トランク上で H.225 シグナリングが完了しておらず、クラスタ A もまだハント パイロット コールの制御権を持っているためです。

   使用可能な HL_A ルート グループ デバイスがない場合、コールは切断されます。
3. コールがクラスタ B に進み、クラスタ B はコールを受け付けて、着信番号の宛先をルート パターンを使用して検索します。着信番号 8888 は、LG_B のメンバーを宛先として保持しています。

   a. 回線グループ LG_B の Y 個のメンバーがすべて使用不可または通話中の場合、クラスタ A の Cisco CallManager は、HL_A に含まれている次のルート グループ メンバーにコールを再ルーティングします（メンバーが存在する場合）。コールをクラスタ A の他のルート グループ メンバーに転送することができるのは、クラスタ A がまだハント パイロット コールの制御権を持っているためです。クラスタ間トランク上の H.225 コール セットアップ シグナリングは、この場合は失敗します。

      使用可能な HL_A ルート グループ デバイスがない場合、コールは切断されます。

   b. 回線グループ LG_B の Y 個のメンバーのうち、いずれか 1 つでも使用可能な場合、コールはそのメンバーに転送されます。この時点で、クラスタ A はコールの制御権を失います。コールがクラスタ B のどのメンバーにも応答されない場合、そのコールを HL_A の次のルート グループ メンバーに転送することはできません。クラスタ間トランク上で H.225 シグナリングが完了しており、クラスタ B がハント パイロット コールの制御権を持っているためです。

ガイドライン

分散型コール処理モデルにコール カバレッジ機能を配置する場合は、次のガイドラインを考慮してください。

- コールが複数のクラスタにわたって分配される場合は、発信または着信のルート グループ デバイス上で実行される番号変換を考慮に入れて、ルート パターンを適切に設定する必要があります。番号変換が実行されない場合、設定するルート パターンとハント パイロットは、すべてのクラスタ上で同一にする必要があります。同一でない場合は、コールが適切に分配されません。
- 分散型コール処理配置では、Cisco VoIP ゲートウェイを使用して、着信ハント パイロット コールの負荷共有を管理できます。あるクラスタ内で着信コールに応答がなかった場合は、そのコールを別のクラスタにオーバーフローしてサービスを提供できます。

ヒント　コールは、ゲートウェイまたはトランクを通じて IVR 処理に送信することができます。Tool Command Language（TCL）IVR アプリケーションは、Cisco IOS ゲートウェイ上に実装できます。

ハント パイロットのスケーラビリティ

トップダウン、循環、および最長アイドル時間の各アルゴリズムを使用してコール カバレッジを配置する場合は、次のガイドラインを参考にすることをお勧めします。

- Cisco CallManager クラスタは、最大で 15,000 のハント リスト デバイスをサポートします。
- ハント リスト デバイスは、1,500 個のハント リストそれぞれに 10 台の IP Phone を入れた組み合せにすることも、750 個のハント リストそれぞれに 20 台の IP Phone を入れた組み合せにすることもできます。ただし、ハント リストの数が多い場合は、その数に応じて、Cisco CallManager のサービス パラメータで指定するダイヤル プラン初期化タイマーの値を大きくする必要があります。ダイヤル プラン初期化タイマーは、ハント リストを 1,500 個設定する場合、600 秒に設定することをお勧めします。

（注） コール カバレッジにブロードキャスト アルゴリズムを使用する場合、ハント リスト デバイスの数は、Busy Hour Call Completion（BHCC）の数によって制限されます。

- 1 つの回線グループ内に、コールをすべての DN に同時に送信することを目的として設定するディレクトリ番号の数は、最大で 35 までにすることをお勧めします。また、ブロードキャスト回線グループの数は、BHCC によって決まります。Cisco CallManager システム内に複数のブロードキャスト回線グループがある場合、回線グループ内のディレクトリ番号の数は、35 よりも少なくする必要があります。すべてのブロードキャスト回線グループの Busy Hour Call Attempt（BHCA）の数が、1 秒あたり 35 コール セットアップを超えないようにします。

CHAPTER 11

緊急サービス

音声システムの適切な配置には、緊急サービスが非常に重要です。この章では、緊急コールのために不可欠な、次の設計上の主な考慮事項について説明しています。

- 911 機能の計画（P.11-2）
- ゲートウェイの考慮事項（P.11-11）
- Cisco Emergency Responder の考慮事項（P.11-13）

この章では、カナダと米国で配置されている 911 緊急ネットワークに固有の情報について、説明します。ここで説明されている概念の多くは、他の地域にも適応できます。緊急コール機能の適切な実装については、ローカル テレフォニー ネットワーク プロバイダーに問い合せてください。

米国の一部の州では、MLTS（Multi-Line Telephone System）のユーザに必要な 911 機能を対象とする法律がすでに制定されています。National Emergency Number Association（NENA）が作成した、『*Technical Information Document on Model Legislation Enhanced 911 for Multi-Line Telephone Systems*』は、次の Web サイトで入手可能です。

http://www.nena9-1-1.org/9-1-1TechStandards/TechInfoDocs/MLTS_ModLeg_Nov2000.PDF

米国連邦通信委員会（FCC）も、タイトル 47、パート 68、セクション 319 に新しいセクション案を作成しました。これは次の Web サイトで入手可能です。

http://www.apcointl.org/about/pbx/worddocs/mltspart68.doc

この章では、読者が北米在住の公衆網ユーザに使用可能な汎用 911 機能を十分理解していることを前提としています。この件の詳細については、次の URL で、北米の E911 サービスの現況の説明を参照してください。

http://www.nena.org/florida/Directory/911Tutorial%20Study%20Guide.pdf

911 機能の計画

ここでは、MLTS（Multi-Line Telephone Systems）におけるライフライン コールの機能要件の一部を説明しています。ライフライン コールとは、北米の公衆電話交換網（PSTN）によって処理される 911 コールのことです。

MLTS 配置を計画する場合は、まず、電話サービスに必要なすべての物理ロケーションを確立してください。これらのロケーションは、次のように分類できます。

- 単一の建物配置。すべてのユーザは同じ建物に住んでいます。
- 単一のキャンパス配置。ユーザは近くにある建物のグループに住んでいます。
- マルチサイト配置。ユーザは地理的に広い範囲に分散しており、WAN 接続を介してテレフォニー コール処理サイトにリンクされています。

これらのロケーション、つまり配置のタイプは、911 サービスの設計と実装に使用される基準に影響を与えます。次の項では、主な基準と、それぞれの標準的な状況および例外的な状況を共に説明します。これらの基準を分析し、適用する際には、ネットワーク内の電話ロケーションによって受ける影響を考慮してください。

Public Safety Answering Point（PSAP）

PSAP は、911 コールに応答して、適切な緊急対応（警察、消防署、または救急チームの派遣など）を手配する機関です。911 コールを発信する電話機の物理的なロケーションは、そのコールに応答する適切な PSAP を決定する基本要素です。一般に、建物ごとに、1 つのローカル PSAP が担当します。

所定のロケーションを担当する PSAP を確認するには、地域の防火管理者または警察署などの地域の公衆安全情報サービス機関に問い合せてください。また、通常、地域通信事業者のディレクトリにも、所定地域内の 911 コールを処理する機関がリストされています。

標準的な状況

- 1 つの番地に対して、1 つの PSAP だけが指定されます。
- 1 つの番地の 911 コールはすべて、同じ PSAP にルーティングされます。

例外的な状況

- キャンパスの物理的な規模により、一部の建物が別の PSAP の管轄になります。
- 一部の 911 コールをオンネット ロケーション（キャンパスのセキュリティ、建物のセキュリティ）にルーティングする必要があります。

911 ネットワーク サービス プロバイダー

担当 PSAP を確認した後、各 PSAP が接続されている 911 ネットワーク サービス プロバイダーも特定する必要があります。通常、PSAP は公衆網から 911 電話コールを受信すると想定されますが、そうとは限りません。911 コールは、地域の重要な専用ネットワーク上で伝送され、各 PSAP は 1 つ以上のこうした地域ネットワークに接続されます。大部分の場合、既存 Local Exchange Carrier（LEC; 地域通信事業者）が PSAP の 911 ネットワーク サービス プロバイダーです。例外には、軍事施設、大学構内、国立または州立の公園、もしくは公衆安全の責任が地方自治体の管轄外であるロケーション、もしくは公共の地域通信事業者以外のエンティティによってプライベート ネットワークが運営されているロケーションがあります。

所定の PSAP の 911 ネットワーク サービス プロバイダーについて疑問がある場合は、その PSAP に直接連絡して、情報を確認してください。

標準的な状況

- 所定の番地の 911 ネットワーク サービス プロバイダーは、既存地域通信事業者（LEC）です。電話会社 X がサービスを提供するロケーションの場合、対応する PSAP も、電話会社 X からサービスを提供されます。
- すべての 911 コールは、オフネット ロケーションに直接ルーティングされるか、オンネット ロケーションに直接ルーティングされます。

例外的な状況

- MLTS インターフェイスから公衆網へ接続するために使用する地域通信事業者（LEC）と、PSAP に対して 911 ネットワーク サービス プロバイダーの役目をする LEC が異なる場合があります（たとえば、電話システムは電話会社 X からサービスを受け、PSAP は電話会社 Y に接続されている場合です）。この状況では、LEC 間の特別な調整、または電話システムと PSAP の 911 ネットワーク サービス プロバイダー間に特別な専用トランクが必要な場合があります。
- 一部の LEC は、ネットワーク上で 911 コールを受け入れることができません。この場合、LEC を変更するか、911 コールを適切な PSAP にルーティングできる LEC に接続されたトランク（911 コール ルーティング専用）を確立するかの 2 つのオプションしかありません。
- 一部（またはすべて）の 911 コールをオンネット ロケーション（キャンパスのセキュリティや建物のセキュリティ）にルーティングする必要があります。この状況は、設計および実装の段階で簡単に対応できますが、電話機ごとの 911 コールの宛先が、正しく計画され、文書化されている必要があります。

該当する 911 ネットワークへのインターフェイス ポイント

大規模なテレフォニー システムでは、911 接続に多数のインターフェイス ポイントが必要になる場合があります。一般に、複数の E911 選択ルータが LEC の管轄地区内で使用され、これらのルータは、通常、相互接続されません。

たとえば、大規模なキャンパスを備えた企業に、次の状況があるとします。

- 建物 A は San Francisco にある
- 建物 B は San Jose にある
- San Francisco 警察と San Jose 警察が、該当する PSAP である
- San Francisco 警察と San Jose 警察は、同じ 911 ネットワーク サービス プロバイダーのサービスを利用している
- しかし、San Francisco 警察と San Jose 警察は、同じ 911 ネットワーク サービス プロバイダーが運営する異なる 911 選択ルータのサービスを受けている

このタイプの状況では、2 つの別々のインターフェイス ポイント（E911 選択ルータごとに 1 つずつ）が必要です。E911 選択ルータの管轄地区に関する情報は、一般に、担当 LEC が保持しており、その LEC の地域アカウント担当者が、企業カスタマーに関連情報を提供できます。多くの LEC は、911 問題の専門家のサービスも用意しています。この専門家は、911 アクセス サービスの適切なマッピングについてアカウント担当者と協議できます。

標準的な状況

- 単一サイト配置またはキャンパス配置では、通常、911 コール用に 1 つだけの PSAP があります。
- 1 つの PSAP のみへのアクセスが必要な場合は、1 つのインターフェイス ポイントだけが必要です。複数の PSAP へのアクセスが必要な場合でも、同じ集中インターフェイスを介して、同じ E911 選択ルータから到達可能です。企業の支店サイトが WAN を介してリンクされている場合（集中型コール処理）、Survivable Remote Site Telephony（SRST）操作がアクティブであるときに WAN 障害が発生した場合の 911 分離を防止するため、911 へのローカル（つまり、各支店内の）アクセスを各ロケーションに指定することをお勧めします。

例外的な状況

- キャンパスの物理的な規模により、一部の建物が別の PSAP 管轄になり、かつ
- 一部の 911 コールは、異なるインターフェイス ポイントを通じて、異なる E911 選択ルータにルーティングされる必要があります。

（注） PSAP と E911 選択ルータの地理的な管轄地区の設定に必要な情報は、オンライン、または各種の競合地域通信事業者（CLEC）の Web サイトから部分的に情報を入手できます。たとえば、https://clec.sbc.com/clec/hb/shell.cfm?section=782 では、SBC/Pacific Bell がカバーする管轄地区についての貴重なデータが提供されています。しかし、911 コール ルーティングを設計および実装する前に、該当するインターフェイス ポイントの適切な情報を LEC から入手しておくことを強くお勧めします。

インターフェイス タイプ

音声通信の提供に加えて、ネットワークへの 911 コールの発信に使用されるインターフェイスは、発信者についての識別データも提供する必要があります。

自動番号識別（ANI）は、ネットワークが適切な宛先へ 911 コールをルーティングするために使用する、発信者の E.164 番号を参照します。この番号は、PSAP がコールの ALI（Automatic Location Identification; 自動ロケーション識別）を検索するためにも使用されます。

911 コールは、ソースルートされます。つまり、911 コールは発信番号に応じてルーティングされます。別々のロケーションからすべて同じ番号（911）をダイヤルする場合でも、ANI によって表される起点ロケーションに基づいて、別々の PSAP に到達します。

次のインターフェイス タイプのどちらかを使用して、911 コール機能を実装できます。

- 動的 ANI 割り当て
- 静的 ANI 割り当て

動的 ANI 割り当ては、（複数の ANI をサポートするので）スケーラビリティに優れていますが、小規模のシステム配置には適していません。静的 ANI 割り込みは、最小のシステムから最大のシステムまで、より広範囲にわたる環境で使用できます。

動的 ANI（トランク接続）

動的 ANI では、システムの 1 つのインターフェイスを、911 ネットワークにアクセスする多数の電話機が共用します。また、ネットワークに送信される ANI がコールごとに異なっていることが必要な場合があります。

動的 ANI インターフェイスには、次の 2 つの主なタイプがあります。

- ISDN-PRI（Integrated Services Digital Network-Primary Rate Interface）または単に PRI
- CAMA（Centralized Automatic Message Accounting）

PRI

このタイプのインターフェイスは、通常、テレフォニー システムを公衆網 Class 5 スイッチに接続します。発番号（CPN）は、発信者の E.164 番号を識別するためにコールのセットアップ時に使用されます。

911 にコールする場合、LEC によって CPN を扱う方法が異なります。Class 5 スイッチ機能の制限、または LEC もしくは地方自治体の方針によっては、CPN が 911 コール ルーティング用の ANI として使用されない場合があります。この場合、CPN の代わりに LDN（Listed Directory Number）、または請求先番号（BTN）を ANI の目的で使用するように、ネットワークをプログラムすることができます。

CPN が ANI に使用されない場合、PRI インターフェイスから発信する 911 コールはすべて、911 ネットワークには同じように見えます。これらの 911 コールはすべて、同じ ANI をもち、同じ宛先（適切な宛先でない場合があります）にルーティングされるからです。

一部の LEC は、911 コールの CPN が PRI インターフェイスを通過するようにする機能を備えています。この機能を使用すると、コールのセットアップ時に Class 5 スイッチに提示された CPN は、コールをルーティングするために ANI として使用されます。この機能の名称は、LEC によって異なります（たとえば、SBC はカリフォルニアでこの機能を Inform 911 と呼びます）。

（注） CPN は、ルーティング可能な E.164 番号でなければなりません。つまり、CPN は、関連した E911 選択ルータのルーティング データベースに入力されている必要があります。

（注） ダイヤルイン方式（DID）の電話機の場合、DID 番号は、911 の目的で ANI として使用できますが、これは、911 サービス プロバイダーのネットワーク内で、緊急サービス番号に適切に関連付けられている場合だけです。DID 以外の電話機の場合は、別の番号を使用してください（詳細については、P.11-7 の「緊急ロケーション識別番号のマッピング」を参照してください）。

多くの Class 5 スイッチは、複数のエリア コードをサポートしないトランクを通じて、E911 選択ルータに接続されています。このような場合、PRI が 911 コールの伝送に使用される場合、適切にルーティングされる 911 コールだけが、Class 5 スイッチと同じ Numbering Plan Area（NPA）のある CPN（または ANI）を持ちます。

例

MLTS は、エリア コード 514（NPA = 514）の Class 5 スイッチに接続されるとします。MLTS が PRI トランク上で 911 コールを送信し、CPN が **450**.555.1212 である場合、Class 5 スイッチは、（正しい **450**.555.1212 ではなく）ANI **514**.555.1212 として E911 選択ルータにそのコールを送信するので、不適切なルーティングが実行され、ALI を取り出すための検索が発生します。

PRI を 911 インターフェイスとして適切に使用するには、システム計画者は、CPN が ANI に使用されることを確認し、リンク上で受け入れ可能な番号の範囲（NPA NXX TNTN の形式）を適切に識別する必要があります。たとえば、PRI リンクが、範囲 514 XXX XXXX 内の ANI 番号を受け入れるように指定されている場合、NPA = 514 の発番号を持つコールだけが適切にルーティングされます。

CAMA

CAMA（Centralized Automatic Message Accounting）トランクも、MLTS がコールを 911 ネットワークに送信することを可能にします。ただし、PRI 方式とは次の相違点があります。

- CAMA トランクは、E911 選択ルータに直接接続されます。E911 選択ルータと MLTS ゲートウェイ ポイント間の距離をカバーするために、マイレージ追加料金が適用される場合があります。

- CAMA トランクは、911 コールのみをサポートします。CAMA トランクの設置と操作に関連した資産コストと運営コストは、911 トラフィックのサポートのみに使用されます。
- MLTS 業界の CAMA トランクは、固定エリア コードに制限され、このエリア コードは、一般に、リンク プロトコルで黙示されます（つまり、明示的に送信されません）。接続には、すべてのコールが同じ固定エリア コードを共用するので、7 桁または 8 桁のみが ANI として送信されます。

（注） シスコは、VIC-2CAMA、VIC-2FXO、および VIC-4FXO トランク カードを介した CAMA ベースの 911 機能をサポートしています。

静的 ANI（回線接続）

静的 ANI は、公衆網との回線（トランクではなく）接続をサポートし、発信側の電話機の CPN に関係なく、回線の ANI が、その回線で発信されるすべての 911 コールに関連付けられます。一般電話サービス（POTS）が、この目的に使用されます。

POTS 回線は、最も単純かつ、最も広くサポートされている公衆網インターフェイスの 1 つです。POTS 回線は、通常、911 コールを受け入れるように設定されています。さらに、既存の E911 インフラストラクチャは、POTS 回線からの 911 コールを非常によくサポートします。

POTS には、次のような特徴があります。

- POTS 回線に関連した運用コストを低減できます。
- POTS 回線に、電源障害に備えたバックアップ回線の役割をもたせることができます。
- POTS 回線番号を、ALI データベースに入力されるコールバック番号として使用できます。
- POTS 回線は、公衆網へのローカル PRI、または CAMA アクセスに見合うユーザ密度をもたないロケーションに対して、最低コストで最適な 911 サポートを実現します。
- 公衆網の敷設に伴い、POTS 回線は広く普及しています。

このタイプのインターフェイスを介した発信 911 コールはすべて、E911 ネットワークによって同じものとして扱われます。ANI は POTS 回線番号に過ぎないので、E911 ネットワークに提示される ANI を Cisco CallManager が制御できるようにするツール（たとえば、発信者番号変換マスク）は、無意味です。

緊急応答ロケーションのマッピング

National Emergency Number Association（NENA）は、最近、企業テレフォニー システムで 911 を規定する規則を制定する際に、州および国の機関が使用する法律モデルを提案しました。NENA 提案の概念の 1 つは、次のように定義される緊急応答ロケーション（ERL）です。

> *911 緊急応答チームの派遣先ロケーション：このロケーションは、緊急応答チームがそのロケーション内で発信者の位置をすばやく確認するための妥当な機会を提供できる、明確なものでなければならない。*

この要件は、各電話機のロケーションを個々に識別するのではなく、電話機を「ゾーン」（ERL）にグループ化することを見込んでいます。ERL の最大サイズは、この法律の地域ごとの実施に応じて異なる可能性がありますが、ここでは説明の基準として 7000 平方フィートを使用します（ここで説明する概念は、任意の州または地域で許可される最大 ERL サイズとは無関係です）。

緊急ロケーション識別番号（ELIN）が各 ERL に関連付けられます。ELIN は、E911 ネットワーク内でコールのルーティングに使用される完全修飾 E.164 番号です。関連した ERL から発信するすべての 911 コールで、ELIN が E911 ネットワークに送信されます。このプロセスは、911 の目的で、複数の電話機を同じ完全修飾 E.164 番号に関連付けることを可能にし、DID 電話機と非 DID 電話機にも同様に適用できます。

(注)　このマニュアルは、法律の実際の要件を提示しようとするものではありません。ここで提示する情報や例は、説明のためだけのものです。システム計画者の責任において、適用されるローカル要件を確認してください。

たとえば、ある建物の床面積が 70,000 平方フィートであり、100 台の電話機があるとします。911 機能を計画する際に、この建物を 7000 平方フィートごとの 10 個のゾーン（ERL）に分割し、各電話機を、それが置かれている ERL に関連付けることができます。911 コールが発信されると、関連した ELIN を PSAP に送信することによって、ERL（複数の電話機に対して同一）が識別されます。この例のように、電話機が均等に分散されている場合、10 台の電話機を持つ各グループには、同じ ERL があり、したがって同じ ELIN をもちます。

各種法律により、最小台数の電話機（たとえば 49）と最低床面積（たとえば、40,000 平方フィート）が定義されます。この数を下回ると、MLTS 911 の要件は適用されません。しかし、法律が企業の 911 機能を要求しない場合であっても、911 機能をプロビジョニングすることが常に最善の方法です。

緊急ロケーション識別番号のマッピング

一般に、緊急ロケーション識別番号（ELIN）と呼ばれる 1 つの完全修飾 E.164 番号を、各 ERL に関連付ける必要があります（ただし、Cisco Emergency Responder を使用する場合は、ERL ごとに複数の ELIN を設定できます）。ELIN は、E911 インフラストラクチャ全体でコールをルーティングするために使用され、ALI データベースへのインデックスとして PSAP が使用します。

ELIN は次の要件を満たす必要があります。

- ELIN は、E911 インフラストラクチャ全体でルーティング可能でなければなりません（P.11-4 の「インターフェイス タイプ」の項の例を参照してください）。ELIN がルーティング不能である場合、関連した ERL からの 911 コールは、E911 選択ルータでプログラムされたデフォルト ルーティングに応じて処理されます。
- 企業の ERL-to-ELIN マッピングが定義された後、LEC を使用して、対応する ALI レコードを設定する必要があります。その結果、PSAP にサービスを提供する ANI と ALI データベース レコードを正確に更新することができます。

ELIN マッピング プロセスは、所定の ERL に対する E911 インフラストラクチャとのインターフェイスのタイプに応じて、次のどちらかを選択できます。

- 動的 ANI インターフェイス

  このタイプのインターフェイスを使用すると、ネットワークに渡される発番号識別は MLTS によって制御されます。MLTS のテレフォニー ルーティング テーブルは、発信側電話機の ERL に基づいて、正しい ELIN をコールに関連付けます。Cisco CallManager では、変換マスクを使用して、911 へのコールの発番号を変更できます。たとえば、所定の ERL 内にあるすべての電話機が、トランスレーション パターン（911）を含み、かつ電話機の CPN をそのロケーションの ELIN に置き換える発信者番号変換マスクも含むパーティションをリストする同じコーリング サーチ スペースを共有できます。

- 静的 ANI インターフェイス

  このタイプのインターフェイスを使用すると、ネットワークに渡される発番号識別は公衆網によって制御されます。これは、インターフェイスが POTS 回線である場合に該当します。ELIN は POTS 回線の電話番号であり、電話機の発信者識別番号に追加操作はできません。

PSAP コールバック

PSAP は、最初の会話の完了後、発信者に到達できることが必要な場合があります。PSAP がコールバックできるかどうかは、PSAP が最初の着信コールと共に受信する情報によって決まります。

この情報は、次の 2 つの部分から成るプロセスによって、PSAP に送信されます。

1. まず、自動番号識別（ANI）が PSAP に送信されます。ANI は、コールをルーティングするために使用される E.164 番号です。この説明では、PSAP で受信された ANI は、MLTS が送信した ELIN を指しています。
2. PSAP は ANI を使用して、データベースを照会し、自動ロケーション識別（ALI）を抽出します。ALI は、次のような情報を PSAP 係員に知らせます。
   - 発信者の名前
   - 住所
   - 該当する公衆安全機関
   - コールバック情報を組み込むことができる、その他のオプション情報。たとえば、救援活動の調整に役立てるために、企業のセキュリティ サービスの電話番号がリストされています。

標準的な状況

- ANI 情報が PSAP コールバックに使用されます。ここでは、ELIN がダイヤル可能番号であると想定します。
- ELIN は、MLTS に関連した公衆網番号です。公衆網から ELIN にコールすると、そのコールは、MLTS によって制御されるインターフェイス上で終端します。
- システム内の任意の ELIN に発信されたコールが、関連した ERL のすぐ近くにある電話機（または複数の電話機）を鳴らすように、コール ルーティングをプログラムするのは、MLTS システム管理者の責任です。
- ERL-to-ELIN マッピングが設定された後、修正が必要なのは、企業の物理的な状況に変更があった場合だけです。電話機が単に追加、移動、またはシステムから削除された場合、ERL-to-ELIN マッピングと、それに関連した ANI/ALI データベース レコードは変更する必要はありません。

例外的な状況

- 発信 ERL のすぐ近くへのコールバックを、オンサイト緊急デスクへのコールバックのルーティングと組み合せる（もしくは、置き換える）ことができます。これは、PSAP が最初の発信者を呼び出し、緊急事態に対してただちに支援を要請するときに役立ちます。
- たとえば、エリア コードの分割、公衆安全業務の新しい配分を必要とする地方自治体業務の変更、新しい建物の追加、または 911 の目的でコールの望ましいルーティングに影響を与えるその他の変更により、企業の状況が変わる場合があります。こうした状況では、企業の ERL-to-ELIN マッピングおよび ANI/ALI データベース レコードの変更が必要です。

非固定電話機の考慮事項

この章のここまでの説明はすべて、電話機のロケーションが静的（固定）であることを前提としていました。しかし、電話機が ERL 境界を越えて移動する場合、新しい場所に移動した電話機からの 911 コールは、正しくルーティングされません。別の ERL に物理的に配置されるので、電話機は現在の ERL の ELIN を使用する必要があります。Cisco CallManager データベースで設定が変更されない場合、次のイベントが発生します。

- 旧 ERL の ELIN が、E911 インフラストラクチャ上のコールのルーティングに使用されます。
- IP ネットワークから E911 インフラストラクチャへの出口点が正しくない可能性があります。
- PSAP に提供されるコールバック機能により、誤った宛先に到達する可能性があります。
- ALI 情報が PSAP に提供されると、緊急応答担当者を誤ったロケーションに派遣する可能性があります。
- 電話機に対するロケーション ベースのコール アドミッション制御は、電話機の WAN 帯域幅使用量を正しく把握できず、WAN 帯域幅リソースのオーバーサブスクリプションや加入過少が発生する可能性があります。

この状況を修復する方法は、Cisco CallManager における電話機の設定（コーリング サーチ スペースやロケーション情報など）を手動で更新して、新しい物理ロケーションを反映することだけです。

Cisco Emergency Responder

移動、追加、および変更の管理が容易であることが、IP テレフォニー テクノロジーの主な利点の 1 つです。ユーザが介入することなく自動的に 911 情報を更新する移動、追加、および変更をサポートするために、シスコは、Cisco Emergency Responder（Cisco ER）と呼ばれる製品を開発しました。

Cisco ER は、次の主な機能を備えています。

- 検出された電話機の物理ロケーションに基づいて、電話機を ERL に動的に関連付けます。
- コールバックのために、ELIN を発信側電話機に動的に関連付けます。上記の項で説明されている ER 以外のシナリオと異なり、Cisco ER は、911 コールを発信した電話機にコールバックできるようにします。
- 緊急コールが進行中であることを知らせるために、指定された通話者へのオンサイト通知が可能です（ポケットベル、電子メール、または電話による）。この通知には、発信者の名前と電話番号、ERL、およびそのコールに関連した日付と時刻の詳細が含まれます。

Cisco ER の詳細は、P.11-13 の「Cisco Emergency Responder の考慮事項」の項、および次の Web サイトで入手可能な Cisco ER 製品資料を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/respond/index.htm

Cisco ER の主な機能は、電話機が 911 コールを発信したネットワーク ポート（ファースト イーサネット スイッチ ポートなどのレイヤ 2 ポート）の検出による、電話機のロケーションの検出に依存します。この検出メカニズムは、主に次の 2 つの前提事項に依存します。

- 企業のワイヤード インフラストラクチャが十分に確立され、散発的な変更が行われないこと。
- Cisco ER が、このインフラストラクチャをブラウズできること。つまり、Cisco ER は、敷設されたネットワーク インフラストラクチャとの簡易ネットワーク管理プロトコル（SNMP）セッションを確立することができ、接続された電話機を検出するためにネットワーク ポートをスキャンできること。

Cisco ER はコールの発信ポートを検出した後、そのコールを、そのポートのロケーション用にあらかじめ設定された ERL に関連付けます。このプロセスは、ロケーションにあらかじめ設定された ELIN との関連付け、および発信 ERL に基づく、E911 インフラストラクチャとの適切な出口点の選択も行います。

Cisco ER では、上記の項で説明されている ERL-to-ELIN マッピング プロセスが適用されますが、相違点が 1 つあります。つまり、Cisco ER を使用しない場合、各 ERL は 1 つの ELIN だけに関連付けられますが、Cisco ER を使用すると、ERL ごとに複数の ELIN を使用できます。この機能拡張の目的は、次の例に示されているように、同じ期間内に 1 つの ERL から複数の 911 コールが発信される特定のケースに対応するためです。

例 1

- 電話機 A と電話機 B はどちらも、ERL X 内に置かれ、ERL X は ELIN X に関連付けられています。
- 電話機 A は 13:00 に 911 にコールします。ELIN X は、そのコールを PSAP X にルーティングするために使用され、PSAP X はそのコールに応答し、解除します。その後、13:15 に電話機 B が 911 にコールします。再び ELIN X が、コールを PSAP X にルーティングするために使用されます。
- PSAP X は、電話機 B からコールを解除した後、電話機 A の最初のコールに関連した詳細情報を取得するために、電話機 A にコールバックすることを決定します。PSAP は ELIN X にダイヤルしますが、（目的の電話機 A ではなく）電話機 B につながります。

この状況を回避するために、Cisco ER では、ERL ごとに ELIN のプールを定義できます。このプールにより、後続のコールごとに別個の ELIN をラウンドロビン方式で使用できます。この例で ERL X に対して 2 つの ELIN を定義すると、例 2 で説明する状況になります。

例 2

- 電話機 A と電話機 B はどちらも、ERL X 内に置かれ、ERL X は ELIN X1 と ELIN X2 の両方に関連付けられます。
- 電話機 A は 13:00 に 911 にコールします。ELIN X1 は、そのコールを PSAP X にルーティングするために使用され、PSAP X はそのコールに応答し、解除します。その後、13:15 に電話機 B が 911 にコールし、このコールを PSAP X にルーティングするのに ELIN X2 が使用されます。
- PSAP X は、電話機 B からコールを解除した後、電話機 A の最初のコールに関連した詳細情報を取得するために、電話機 A にコールバックすることを決定します。PSAP は ELIN X1 にダイヤルし、電話機 A につながります。

もちろん、3 番目の 911 コールが発信されたが ERL に 2 つの ELIN しかない場合、コールバック機能では、最後の 2 人の発信者にしか正しく到達できません。

緊急コール ストリング

アクセス コード（たとえば、9）を使用するかどうかにかかわらず、システムが緊急コールを認識しやすいように、ダイヤル プランを設定することが望まれます。北米の緊急ストリングは、通常、911 です。ストリング 911 と 9911 の両方を認識するように、システムを設定することを強くお勧めします。

緊急ルート パターンに Urgent Priority のマークを明示的に付けて、Cisco CallManager が、コールのルーティング前に、番号間タイムアウト（Timer T.302）を待機しないようにすることも強くお勧めします。

これ以外の緊急コール ストリングを、システム上で並行してサポートすることができます。選択した緊急コール ストリング使用を想定した訓練をテレフォニー システム ユーザに行うことをお勧めします。

また、ユーザが誤って緊急ストリングをダイヤルした場合に適切な対応ができるように訓練することも望まれます。北米では、アクセス コード 9 を使用して長距離番号にアクセスしようとするユーザが、誤って 911 をダイヤルする可能性があります。このような場合、ユーザは、緊急事態ではないので、緊急隊員を派遣する必要がないことを確認するために、回線を保持する必要があります。Cisco ER のオンサイト通知機能では、誤って発信されたコールを含め、911 に発信されたすべてのコールの詳細なアカウントを提供することによって、そのような疑わしい 911 コールの起点にある電話機を識別できます。

ゲートウェイの考慮事項

システムの緊急コールを処理するゲートウェイを選択する際には、次の要素を考慮してください。

ゲートウェイの配置

地域通信事業者（LEC）ネットワーク内で、911 コールは、コールの起点に基づいて、ローカル側で有効なインフラストラクチャ上でルーティングされます。サービスを提供する Class 5 スイッチは、ロケーションに関連した PSAP に直接接続されるか、E911 選択ルータに接続されます。この選択ルータ自体は、その地域に有効な PSAP 群に接続されます。

シスコの IP ベースの企業テレフォニー アーキテクチャでは、リモート側に置かれているゲートウェイに、オンネットでコールをルーティングすることが可能です。たとえば、San Francisco に置かれている電話機は、IP ネットワークを介して、San Jose にあるゲートウェイにコールを伝送してから、LEC のネットワークに送信することができます。

911 コールの場合、緊急コールが適切なローカル PSAP にルーティングされるように、LEC ネットワークへの出口点を選択することが重要です。上記の例では、San Francisco の電話機からの 911 コールが、San Jose のゲートウェイにルーティングされてしまうと、San Francisco の PSAP に到達できません。これは、そのコールを受信する San Jose の LEC スイッチには、San Francisco PSAP にサービスを提供する E911 選択ルータへのリンクがないからです。さらに、San Jose 地域の 911 インフラストラクチャは、San Francisco の発番号に基づいてコールをルーティングすることができません。

大まかに言えば、発信側電話機と物理的に同じ場所にあるゲートウェイに、911 コールをルーティングしてください。共通ゲートウェイを使用して、複数のロケーションからの 911 コールを集約できるかどうかは、LEC に問い合せてください。所定の地域の 911 ネットワークが、911 コールに中央ゲートウェイを使用しやすい場合でも、911 コール ルーティングが WAN 障害中の影響を受けないように、発信側電話機と同じ場所にあるゲートウェイを使用することが望ましいことに注意してください。

ゲートウェイのブロック

911 コールが「全トランク使用中」状況にならないようにすることが望まれます。911 コールを接続する必要がある場合、トランキング リソースの不足により他のタイプのコールがブロックされる場合でも、911 コールは処理可能にしておく必要があります。このような状況に備えて、明示トランク グループを 911 コール専用にすることができます。

緊急コールを独占的に緊急トランク グループにルーティングするのが、好ましい方法です。もう 1 つの方法は、通常の公衆網コールと同じトランク グループに緊急コールを送信し（インターフェイスが許可する場合）、専用緊急トランク グループへの代替パスを用意するものです。後者の方法では、最大限の柔軟性が得られます。

たとえば、緊急コールを PRI トランク グループに向け、オーバーフロー状態になったときに備えて POTS 回線への代替パス（緊急コール専用に予約済み）を指定することができます。代替トランク グループに 2 つの POTS 回線を入れる場合、メインのトランク グループで許可されたすべてのコールの他に、少なくとも 2 つの 911 コールを同時にルーティングできることを保証します。

優先ゲートウェイが使用不能になる場合、緊急コールを代替番号にオーバーフローさせて、代替ゲートウェイが使用されるようにすることができます。たとえば、北米で 911 にダイヤルされたコールは、E.164（911 以外）ローカル緊急番号にオーバーフローすることができます。この方法は、北米の 911 ネットワーク インフラストラクチャを利用しません（つまり、選択ルーティング、ANI、または ALI サービスを使用しません）。この方法は、該当する公衆安全機関によって受け入れられる場合に限り、ネットワーク リソースの不足による緊急コールのブロックを回避する最後の手段としてのみ使用してください。

応答監視

通常の状態では、緊急番号に発信されたコールは、PSAP との接続後、応答監視を戻します。応答監視は、他のコールと同じように、オンネット発信者と、LEC ネットワークへの出口インターフェイスとの間の全二重音声接続をトリガできます。

一部の北米 LEC では、「無料」コールを行う場合、応答監視は戻されません。これは、一部のフリーダイヤル番号（たとえば、800 番）にも該当します。例外的な状況では、緊急コールは「無料」コールと見なされるので、PSAP との接続後、応答監視は戻されません。この状況は、911 テストコールを発信するだけで検出できます。PSAP との接続後、音声が存在する場合、コール タイマーが発信コールの所要時間を記録します。コール タイマーがない場合は、応答監視が戻されなかった可能性があります。応答監視が戻されない場合、LEC に連絡して、この状況を報告することをお勧めします。おそらく、望ましい機能ではありません。

この状況が地域通信事業者によって修正できない場合、LEC ネットワークにコールが発信されるときに応答監視を必要としないように出口ゲートウェイを設定することをお勧めします。また、応答監視が戻されない場合でも、進行標識音、代行受信メッセージ、および PSAP との通信が可能であるように、両方向で音声をカットスルーすることもお勧めします。

デフォルトでは、Cisco IOS ベースの H.323 ゲートウェイは、両方向で音声を接続するために、応答監視を受信する必要があります。これらのゲートウェイ上で応答監視の必要をなくすには、次のコマンドを使用してください。

- **progress_ind alert enable 8**

  このコマンドは、アラートの受信時に進行標識値 8（インバンド情報が使用可能）を受信することに相当します。このコマンドを使用すると、ゲートウェイの POTS 側が、コールの起点方向の音声を接続できます。

- **voice rtp send-recv**

  このコマンドは、宛先スイッチから Connect メッセージを受信する前に、逆方向と順方向の両方の音声カットスルーを可能にします。このコマンドは、すべての Voice over IP（VoIP）コール（使用可能である場合）に影響を与えます。

応答監視が提供されない場合は、Call Detail Record（CDR; コール詳細レコード）が 911 コールの接続時間または期間を正確に反映しません。その結果、コール レポーティング システムが、911 コール関連の統計情報を正しく表すことができない場合があります。

いかなる場合でも、すべてのコール パスからの 911 コール機能をテストし、PSAP との接続後、応答監視が戻されることを確認することをお勧めします。

Cisco Emergency Responder の考慮事項

デバイス モビリティにより、緊急コールに特別な設計上の考慮事項が生じます。Cisco Emergency Responder（Cisco ER）は、デバイスの動的な物理ロケーションに基づいて、デバイス モビリティをトラッキングし、システムによる緊急コールのルーティングを適合させるために使用できます。

コール アドミッション制御ロケーションを超えたデバイス モビリティ

集中型コール処理配置では、Cisco ER は、複数のコール アドミッション制御ロケーションにわたるデバイスの移動を完全にサポートすることはできません。これは、Cisco CallManager が、デバイスの移動を認識しないからです。たとえば、電話機を支店 A から支店 B に物理的に移動したにもかかわらず、電話機のコール アドミッション制御ロケーションが同じままである（たとえば、Location_A）場合、Location_A に使用可能な帯域幅がすべて、他のコールで使用中であれば、その電話機から 911 に発信するコールは、コール アドミッション制御拒否によりブロックされる可能性があります。現在、ロケーション B にある電話機が、ロケーション B の PSAP との接続に使用されるゲートウェイと物理的に同じ場所にある場合でも、このコール ブロックは発生します。

同じ理由で、Cisco ER は、ゲートキーパーによって制御されるコール アドミッション制御ゾーン間のデバイス移動をサポートできません。ただし、Cisco ER は、コール アドミッション制御ロケーション内でのデバイスの移動を完全にサポートできます。

集中型コール処理配置では、Cisco ER は、支店内のデバイス移動を自動的にサポートします。ただし、デバイスが支店間を移動する場合、Cisco ER が 911 コールを完全にサポートできるようにするには、デバイスのロケーションとリージョンのパラメータを手動で調整する必要があります。

デフォルトの緊急応答ロケーション

Cisco ER が、電話機の物理的なロケーションを直接判別できない場合、コールにデフォルトの緊急応答ロケーション（ERL）を割り当てます。デフォルトの ERL は、こうしたすべてのコールを、特定の PSAP に導きます。この状態が発生した場合、コールの送信先について共通の推奨事項はありませんが、通常、中央に置かれ、最大の公衆安全管轄権を提示する PSAP を選択するのが望ましい方法です。また、デフォルト ERL の緊急ロケーション識別番号（ELIN）の ALI レコードに、企業の緊急番号の連絡先情報を取り込み、発信者のロケーションの不確実さについての情報を提供することも、お勧めします。さらに、緊急コールのデフォルト ルーティングが発生したという注記を、ALI レコードに付けることもお勧めします。

ソフト クライアント

Cisco IP Communicator などのソフト クライアントが企業内で使用される場合、Cisco ER は、デバイス モビリティをサポートできます。しかし、企業の境界外でソフト クライアントが使用される場合（たとえば、ホーム オフィスやホテルからの VPN アクセス）、Cisco ER は、発信者のロケーションを判別できません。さらに、Cisco システムで、発信者のロケーションに該当する PSAP にコールを送信できるように、適切な位置にゲートウェイが配置されている可能性はほとんどありません。

ソフト クライアントに 911 コールの使用を許可するか、許可しないかは、企業ポリシーの問題です。インターネット上でローミングする可能性があるソフト クライアントに対して、企業のポリシーとして 911 コールを許可しないことをお勧めします。それにもかかわらず、このようなユーザが 911 をコールした場合、ベスト エフォート型のシステム応答では、オンサイト保安部隊、またはシステムのメイン サイトに近い大規模 PSAP のどちらかに、コールをルーティングします。

次のパラグラフは、ソフト クライアント ユーザに対して緊急コール機能が保証されていないことを警告するために、ユーザに発行される通知の例を示しています。

> 緊急コールは、設定されているサイト（たとえば、オフィス）に設置されている電話機から発信してください。地域保安当局は、設定されたサイトから移動された電話機からの緊急コールに応答しない可能性があります。設定済みのサイトから離れているときに、この電話機を緊急コールに使用する必要がある場合は、公共安全応答機関に、ロケーションについての特定情報を伝えてください。旅行または在宅勤務時の緊急コールには、サイトに対してローカル側で設定されている電話機（たとえば、ホテルの電話機や自宅の電話機）を使用してください。

テスト コール

企業テレフォニー システムの場合、911 コール機能のテストは、初期インストール後だけでなく、予防手段として定期的に実施することをお勧めします。

テストの実行には、次の項目を参考にしてください。

- PSAP に連絡して、テスト前に許可を要請し、テストを実施する人物の連絡先情報を伝えます。
- 各コール発信時に、実際の緊急事態ではなく、単なるテストであることを伝えます。
- 通話者の画面上に表示される ANI と ALI を確認します。
- コールがルーティングされた先の PSAP を確認します。
- IP Phone 上のコール所要時間タイマーを調べることによって、応答監視が受信されたことを確認します。アクティブ コール タイマーは、応答監視が正しく機能していることを示します。

共用ディレクトリ番号への PSAP コールバック

Cisco ER は、緊急ロケーション識別番号（ELIN）に対する着信コールのルーティングを処理します。911 コールの発信元の回線が、共用ディレクトリ番号である場合、PSAP コールバックにより、すべての共用ディレクトリ番号アピアランスが鳴ります。その後、共用アピアランスのいずれかがコールに応答します。これは、911 コールが発信された電話機ではない可能性があります。

マルチクラスタの考慮事項

複数の Cisco CallManager クラスタに基づく企業テレフォニー システムは、Cisco Emergency Responder（Cisco ER）の機能から利点を得ることができます。

ここで使用する用語の詳細、および次の説明を理解するために必要な背景情報については、『*Cisco Emergency Responder Administration Guide*』を参照してください。「Planning for Cisco Emergency Responder」の章は特に重要です。このマニュアルは、次の Web サイトで入手できます。

http://www.cisco.com

単一の Cisco ER グループ

単一の Emergency Responder グループを配置して、複数の Cisco CallManager クラスタからの緊急コールを処理できます。この設計の目的は、どの電話機の緊急コールも、その Cisco ER グループにルーティングされることを保証することです。その Cisco ER グループが、ELIN を割り当て、電話機のロケーションに基づいてコールを適切なゲートウェイにルーティングします。

単一の Cisco ER グループを使用する 1 つの利点は、すべての ERL と ELIN が単一のシステムに設定されることです。単一の Cisco ER グループがシステムのすべてのアクセス スイッチのポーリングを担当しているため、どのクラスタに登録されている電話機でも、そのグループによって位置が確認されます。図 11-1 では、2 つの Cisco CallManager クラスタとインターフェイスする単一の Cisco ER グループを示しています。

図 11-1　2 つの Cisco CallManager クラスタに接続されている単一の Cisco ER グループ

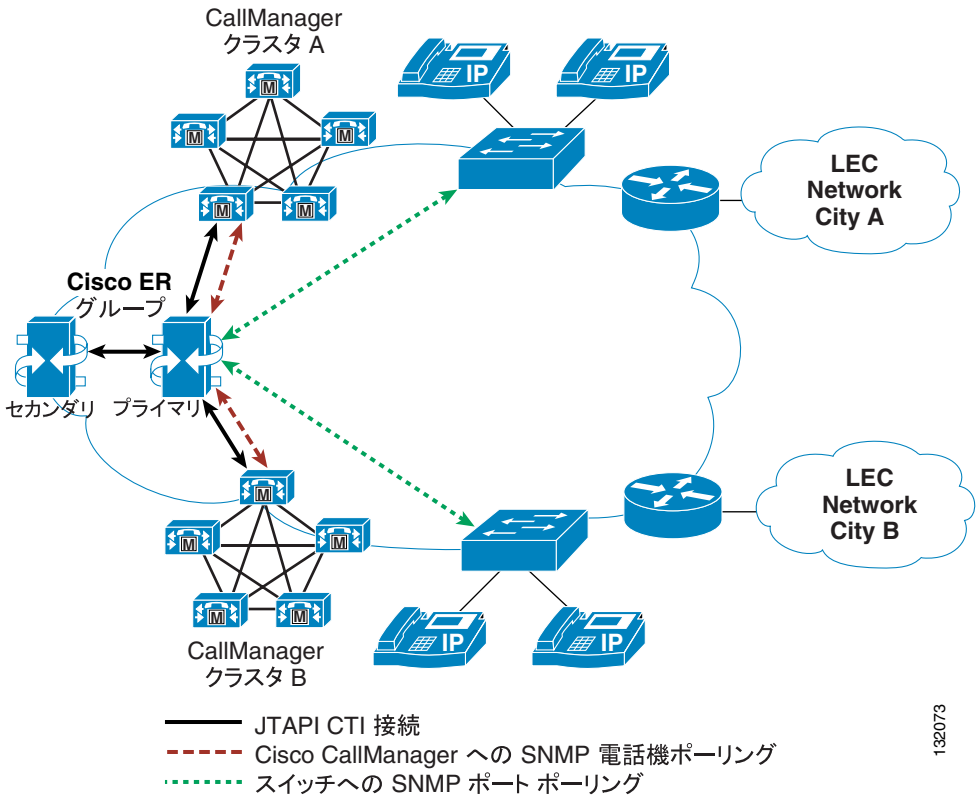


図 11-1 の単一の Cisco ER グループは、次のコンポーネントとインターフェイスします。

- SNMP を介して各 Cisco CallManager クラスタとインターフェイスし、それぞれに設定されている電話機に関する情報を収集する。
- SNMP を介して企業のすべてのスイッチとインターフェイスし、どのスイッチに接続されているどのクラスタの電話機でも、その位置を確認できるようにする。電話機のロケーションが IP サブネットに基づいて識別される場合、この接続は不要です。IP サブネットベースの ERL を設定する方法の詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「Configuring Cisco Emergency Responder」の章を参照してください。

  http://www.cisco.com
- JTAPI を介して各 Cisco CallManager クラスタとインターフェイスし、911 をダイヤルするどの電話機にも必要なコール処理を可能にする。そのコール処理とは、発信側電話機の ERL の識別、ELIN の割り当て、（発信側電話機のロケーションに基づく）適切なゲートウェイへのコール リダイレクション、PSAP コールバック機能の処理などです。

Cisco Emergency Responder によって使用される JTAPI インターフェイスのバージョンは、Cisco Emergency Responder が接続される Cisco CallManager ソフトウェアのバージョンによって決まります。システムの初期化時に、Cisco ER は Cisco CallManager クラスタに問い合せ、適切な JTAPI Telephony Service Provider（TSP）をロードします。Cisco ER サーバ上には 1 つのバージョンの JTAPI

TSP しか存在できないため、単一の Cisco ER グループがインターフェイスするすべての Cisco CallManager クラスタが、同じバージョンの Cisco CallManager ソフトウェアを実行する必要があります。

配置によっては、このソフトウェア バージョン要件によって問題が生じる場合があります。たとえば、Cisco CallManager のアップグレード中は、クラスタが異なると、実行されているソフトウェアのバージョンが異なり、一部のクラスタが、Cisco ER サーバ上で実行されているバージョンと互換性のないバージョンの JTAPI を実行していることがあります。このような場合、Cisco ER グループの JTAPI バージョンとは異なるバージョンを実行しているクラスタからの緊急コールは、緊急番号の CTI ルート ポイントの Call Forward Busy 設定によって提供されるコール処理を受けることができます。

複数の Cisco CallManager クラスタに対して単一の Cisco ER グループが適切であるかどうかを検討する場合は、次のガイドラインを適用してください。

- 緊急コールの数ができるだけ少ない許容可能なメンテナンス時間帯に（たとえば、営業時間後や、システムの使用量が最小限のとき）、Cisco CallManager をアップグレードする。
- クラスタの数とサイズから判断して、ソフトウェアのアップグレード中に異なるバージョンの JTAPI が使用される時間を最小限に抑えることができると思われる場合にだけ、単一の Cisco ER グループを使用する。

たとえば、8 台のサーバで構成される 1 つの大規模なクラスタと、2 台のサーバで構成される 1 つの小規模なクラスタを同時に配置し、単一の Cisco ER グループと共に使用するとします。この場合、大規模なクラスタを最初にアップグレードすることをお勧めします。これにより、アップグレードのメンテナンス時間帯に Cisco ER サービスを使用できないユーザ（小規模なクラスタからサービスを受けるユーザ）の数を最小限に抑えることができます。さらに、小規模なクラスタのユーザは、Cisco ER に到達できない間、実際には、緊急コールの一時スタティック ルーティングによって適切にサービスを受けることができます。これは、そのユーザが、その時間中に発信されるすべての非 ER コールに割り当てられている単一の ERL/ELIN によって識別されることが可能なためです。

複数の Cisco ER グループ

マルチクラスタ システムをサポートするために、複数の Cisco ER グループを配置することもできます。この場合は、各 ER グループが次のコンポーネントとインターフェイスします。

- Cisco CallManager クラスタ。次の方式を使用します。
  - SNMP：クラスタに設定されている電話機に関する情報を収集します。
  - JTAPI：適切なゲートウェイへの、またはローミング電話機の場合は適切な Cisco CallManager クラスタへの、コール リダイレクションに関連するコール処理を可能にします。
- その Cisco ER グループの Cisco CallManager に関連付けられているほとんどの電話機の接続先となるアクセス スイッチ（SNMP を使用）。

この方法を使用すると、Cisco CallManager クラスタが、異なるバージョンのソフトウェアを実行できます。これは、各クラスタが、別の Cisco ER グループとインターフェイスするためです。

電話機がネットワーク上のさまざまな場所をローミングし、Cisco ER がその電話機をトラッキングできるようにするには、Cisco ER グループを 1 つの Cisco ER クラスタに設定する必要があります。Cisco ER のクラスタとグループの詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「Planning for Cisco Emergency Responder」の章を参照してください。

http://www.cisco.com

図 11-2 では、Cisco ER クラスタリングの背後にある基本的な概念を表すトポロジの例を示しています。

図 11-2　複数の Cisco ER グループ

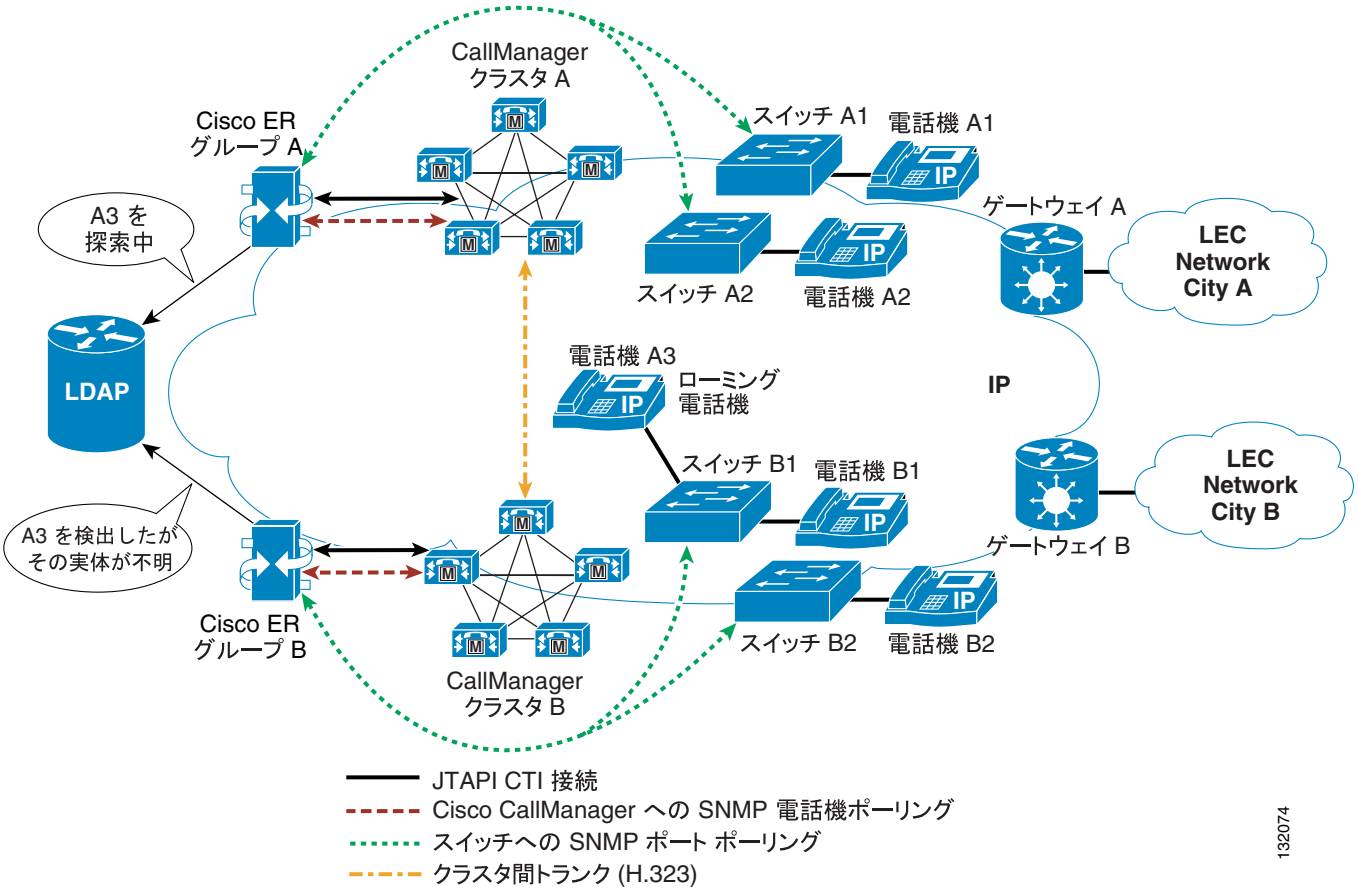


図 11-2 では、次のトポロジを示しています。

- Cisco ER グループ A は、Cisco CallManager クラスタ A とインターフェイスして、スイッチ A1 および A2 にアクセスする。このグループは、Cisco CallManager クラスタ A に登録されているすべての電話機のホーム Cisco ER グループであると見なされます。
- 同様に、Cisco ER グループ B は、Cisco CallManager クラスタ B とインターフェイスして、スイッチ B1 および B2 にアクセスする。このグループは、Cisco CallManager クラスタ B に登録されているすべての電話機のホーム Cisco ER グループであると見なされます。

Cisco ER グループのトラッキング ドメイン内の電話機移動

電話機が、同じホーム Cisco ER グループによって制御されるアクセス スイッチ間を移動する場合、その電話機の緊急コール処理は、単一の Cisco CallManager クラスタを使用する配置で行われる処理と同じです。たとえば、アクセス スイッチ A1 と A2 の間を移動する電話機は、Cisco CallManager クラスタ A に登録されたままで、移動前も移動後もその電話機のロケーションは Cisco ER グループ A によって特定されます。Cisco CallManager クラスタ A による電話機検出と、スイッチ A2 による電話機のロケーション特定の両方で、電話機は引き続き Cisco ER グループ A の完全な制御下にあります。したがって、電話機は位置未確認の電話機と見なされません。

Cisco ER クラスタのさまざまなトラッキング ドメイン間の電話機移動

Cisco ER クラスタは、基本的に、Lightweight Directory Access Protocol（LDAP）データベースを介してロケーション情報を共有する Cisco ER グループの集まりです。各グループは、アクセス スイッチ上または IP サブネット内で検出するすべての電話機のロケーションを共有します。ただし、Cisco ER グループ独自の Cisco CallManager クラスタ内で検出される電話機は*不明*であると見なされ、その情報は共有されません。

Cisco ER グループは、Cisco ER グループのトラッキング ドメイン内（スイッチまたは IP サブネット内）で位置を確認できないが、そのグループに関連付けられている Cisco CallManager クラスタに登録されていることがわかっている電話機に関する情報も共有します。このような電話機は、*位置未確認*と見なされます。

異なる Cisco ER グループによって監視されるアクセス スイッチ間を電話機がローミングする場合、それらのグループは、電話機のロケーションに関する情報を交換できるように、1 つの Cisco ER クラスタに設定される必要があります。たとえば、Cisco CallManager クラスタ A に登録されている電話機 A3 が、Cisco ER グループ B によって制御されるアクセス スイッチに接続されているとします。Cisco ER グループ A は、電話機 A3 が Cisco CallManager クラスタ A に登録されていることを認識しますが、サイト A のどのスイッチでも電話機 A3 の位置を確認できません。したがって、電話機 A3 は Cisco ER グループ A によって*位置未確認*と見なされます。

これに反して、Cisco ER グループ B は、監視対象のスイッチの 1 つで、電話機 A3 の存在を検出します。電話機 A3 は、Cisco CallManager クラスタ B に登録されていないため、*不明*な電話機として Cisco ER LDAP データベースを介してアドバタイズされます。

2 つの Cisco ER グループは、LDAP データベースを介して通信しているため、Cisco ER グループ B の*不明*な電話機 A3 が Cisco ER グループ A の*位置未確認*の電話機 A3 と同じであることがわかります。

Cisco ER グループ A の Unlocated Phone ページには、この電話機のホスト名が、リモート Cisco ER グループ（この場合は Cisco ER グループ B）と共に表示されます。

Cisco ER クラスタ内の緊急コール ルーティング

Cisco ER クラスタリングは、1 つの Cisco CallManager クラスタと 1 つの Cisco ER で構成されるペア間で緊急コールをリダイレクトできるようにするルート パターンにも依存します。詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「Creating Route Patterns for Inter-Cisco Emergency Responder-Group Communications」の項を参照してください。

http://www.cisco.com

電話機 A3 が緊急コールを発信した場合、コール シグナリング フローは次のようになります。

1. 電話機 A3 が、処理のために緊急コール ストリングを Cisco CallManager クラスタ A に送信する。
2. Cisco CallManager クラスタ A が、リダイレクションのためにコールを Cisco ER グループ A に送信する。
3. Cisco ER グループ A が、電話機 A3 の位置を Cisco ER グループ B のトラッキング ドメイン内であると確認し、Cisco CallManager クラスタ B を指すルート パターンにコールをリダイレクトする。
4. Cisco CallManager クラスタ A がコールを Cisco CallManager クラスタ B に送信する。
5. Cisco CallManager クラスタ B が、リダイレクションのためにコールを Cisco ER グループ B に送信する。

6. Cisco ER グループ B が、電話機 A3 のロケーションに関連付けられている ERL と ELIN を識別し、コールを Cisco CallManager クラスタ B にリダイレクトする。発信番号は、電話機 A3 の ERL に関連付けられている ELIN に変換されます。着信番号は、コールを適切なゲートウェイにルーティングするように変更されます。
7. Cisco CallManager クラスタ B が、Cisco ER グループ B から入手した新しい着信番号情報に従ってコールをルーティングする。
8. Cisco CallManager クラスタ B が、ゲートウェイを通じてコールを緊急公衆網ネットワークに送信する。

Cisco ER クラスタリングのスケーラビリティの考慮事項

Cisco ER クラスタでは、ホーム Cisco ER グループのトラッキング ドメイン外をローミングする電話機の数が、スケーラビリティ ファクタとなります。このような電話機の数は、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide 1.2(3)*』の「Network Hardware and Software Requirements」の項に記載されている制限内に収める必要があります。

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

Cisco MCS 7845 サーバ プラットフォームおよび Cisco ER ソフトウェアのバージョン 1.2(3) では、Cisco ER クラスタは最大 3000 台のローミング電話機をサポートできます。この制限を超える必要のある配置（たとえば、複数の Cisco CallManager クラスタを含む大規模なキャンパス配置）では、IP サブネットによって電話機の移動をトラッキングできます。各 Cisco ER グループに IP サブネットを定義し、Cisco ER グループごとに各 ERL を 1 つの ELIN に割り当てることによって、事実上、ローミング電話機をなくすことができます。これは、キャンパス内のすべての電話機が、それぞれの Cisco ER グループのトラッキング ドメインに含まれるためです。

ALI フォーマット

マルチクラスタ構成では、単一の Cisco ER グループに定義されている ERL と ELIN の物理ロケーションが、複数の電話会社の管轄地区にまたがることがあります。これにより、複数の LEC 用のレコードを含む共通ファイルから、さまざまな電話会社用のレコードを抽出する必要が生じることがあります。

Cisco ER は、この情報を、National Emergency Number Association（NENA）2.0、2.1、および 3.0 フォーマットに準拠する ALI レコードとしてエクスポートします。ただし、数多くのサービス プロバイダーが NENA 規格を使用しません。そのような場合は、Cisco ER によって生成された ALI レコードが、サービス プロバイダーによって指定されたフォーマットに準拠するように、ALI Formatting Tool（AFT）を使用してそのレコードを変更できます。これにより、サービス プロバイダーは、フォーマットし直されたファイルを使用して、ALI データベースを更新できます。

ALI Formatting Tool（AFT）では、次の機能を実行できます。

- レコードを選択し、ALI フィールドの値を更新する。AFT では、ALI フィールドを編集し、さまざまなサービス プロバイダーの要件を満たすようにカスタマイズできます。これにより、サービス プロバイダーは、フォーマットし直された ALI ファイルを読み取り、そのファイルを使用して ELIN レコードを更新できます。
- 複数の ALI レコードに対するバルク更新を実行する。バルク更新機能を使用すると、選択したすべてのレコード、1 つのエリア コード、または 1 つのエリア コードと 1 つのシティ コードに対して共通の変更を適用できます。
- エリア コード、シティ コード、または 4 桁のディレクトリ番号に基づいて ALI レコードを選択してエクスポートする。たとえば、あるエリア コードのすべての ALI レコードを選択してエクスポートすることにより、各サービス プロバイダーのすべての ELIN レコードに素早くアクセスできるため、複数のサービス プロバイダーを簡単にサポートできます。

AFT の柔軟性を利用して、単一の Cisco ER グループが、複数の ALI データベース フォーマットで ALI レコードをエクスポートできます。Cisco ER グループがサービスを提供する Cisco CallManager クラスタが 2 つの LEC の管轄地区内にあるサイトを持つ場合、基本的な方法は次のとおりです。

1. Cisco Emergency Responder からの ALI レコード ファイル出力を標準の NENA フォーマットで入手します。このファイルには、複数の LEC 用のレコードが含まれています。
2. 必要な ALI フォーマットごとに元のファイルの 1 つのコピーを作成します（LEC ごとに 1 つのコピー）。
3. 最初の LEC（たとえば、LEC-A）の AFT を使用して、NENA フォーマットのファイルのコピーをロードし、他の LEC に関連付けられているすべての ELIN のレコードを削除します。削除する情報は、通常、NPA（またはエリア コード）によって識別できます。
4. 結果として生成されたファイルを、LEC-A に必要な ALI フォーマットで保存し、適宜ファイル名を付けます。
5. LEC ごとにステップ 3 ～ 4 を繰り返します。

ALI Formatting Tool は、次の Web サイトで入手できます。

http://cco/en/US/products/sw/voicesw/ps842/products_administration_guides_list.html

この URL にリストされていない LEC の場合、スプレッドシート プログラムや標準のテキスト エディタなど、標準のテキスト ファイル編集ツールを使用して Cisco CallManager からの出力をフォーマットできます。

CHAPTER 12

ボイスメール設計

この章では、Cisco CallManager と共にボイスメール システムを配置するための次のオプションについて説明します。

（注） この章では、ポートやストレージに関して、ボイスメール　システムをサイジングする方法については説明しません。このような情報については、ボイスメール ベンダーに問い合せてください。特定のトラフィック パターンに基づき、ベンダー独自のシステムの個々の要件について詳細な説明を受けることができます。

Cisco Unity

Cisco Unity は先進的なユニファイド メッセージング ソリューションであり、バックエンド メッセージ ストアとして Microsoft Exchange または IBM（Lotus）Domino をサポートしています。Unity は、ローカル メッセージ ストアとして Microsoft Exchange だけを使用するスタンドアロン ボイスメール システムとしても提供されます。Cisco Unity でのさまざまな配置オプションについては、第 13 章「Cisco Unity」を参照してください。

Cisco Unity の詳細については、次の Web サイトで入手可能な Cisco Unity の製品資料を参照してください。

http://www.cisco.com

Cisco Unity Express

ここでは、Cisco CallManager のボイスメールおよび Automated Attendant（AA; 自動応答機能）の分散ソリューションとして Cisco Unity Express を紹介します。Cisco Unity Express は、最大 100 人（100 個のメールボックス）のオフィスに向けたエントリレベルのボイスメール システムであり、ブレードとして各サイトの支店ルータに物理的に統合されます。

Cisco CallManager ネットワーク配置に次のいずれかの条件があてはまる場合は、分散ボイスメール ソリューションとして Cisco Unity Express を使用してください。

- WAN のアベイラビリティに関係なく、ボイスメールおよび AA アクセスの存続可能性を保証する必要がある。
- 使用可能な WAN 帯域幅が十分でなく、WAN を介して中央のボイスメール サーバに送信されるボイスメール コールをサポートできない。
- ローカル コミュニティに発行される AA または支店サイト公衆網電話番号の地理的カバレッジに制限があり、これらの電話番号をダイヤルして中央の AA サーバに到達するには、必ず通話料金が発生する。
- 支店への外線コールが、支店 AA から同じオフィスのローカル内線番号に転送される可能性が高い。
- 管理方針によって、リモート ロケーションが独自のボイスメールおよび AA テクノロジーを選択することが許可されている。

（注） Cisco CallManager との相互運用性を実現するには、最低でも、Cisco Unity Express Release 1.1 と Cisco CallManager Release 3.3.3 以降の 3.3 ベースのリリースが必要です。Cisco Unity Express 2.0 は Cisco CallManager Release 4.0 との相互運用性を実現し、Cisco Unity Express 2.1 は Cisco CallManager Release 4.1 との相互運用性を実現します。

Cisco Unity Express の詳細については、次の Web サイトで入手可能な製品資料を参照してください。

http://www.cisco.com

Cisco Unity Express の配置モデル

Cisco Unity Express は、すべての Cisco CallManager 配置モデル（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、分散型コール処理を使用するマルチサイト WAN など）でサポートされています。図 12-1 では Cisco Unity Express を組み込んだ集中型コール処理配置を示し、図 12-2 では分散型コール処理配置を示しています。

図 12-1　集中型コール処理配置における Cisco Unity Express

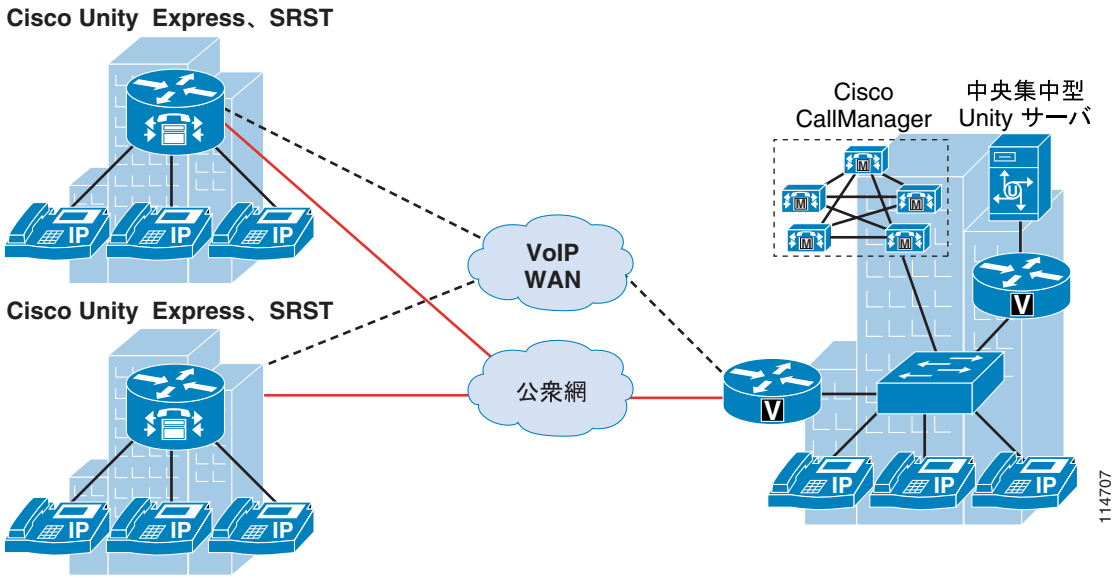
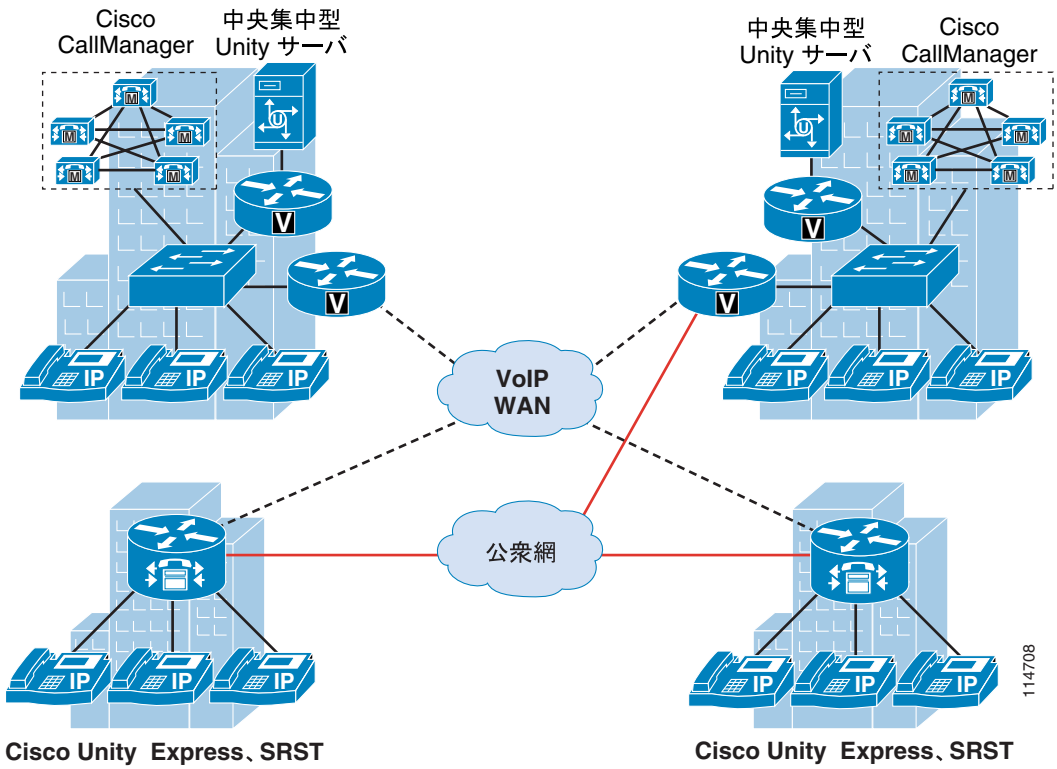


図 12-2　分散型コール処理配置における Cisco Unity Express



Cisco Unity Express を使用する最も一般的な配置モデルは、集中型コール処理を使用するマルチサイト WAN です。この配置モデルでは、Cisco Unity Express が小規模なリモート オフィスに分散ボイスメールを提供し、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を提供します。

Cisco Unity Express は、Cisco CallManager Express とプラットフォームを共有する構成のボイスメール ソリューションとしても配置できます。Cisco CallManager Express によって制御される Cisco Unity Express サイト、および Cisco CallManager によって制御される他のサイトは、同じネットワークで相互接続できます。Cisco Unity Express は Cisco CallManager または Cisco CallManager Express と統合できますが、両方と同時に統合することはできません。

集中型または分散型 Cisco CallManager 配置の Cisco Unity Express に関する特性とガイドラインは、次のとおりです。

- 単一の Cisco Unity Express を単一の Cisco CallManager クラスタと統合できる。
- Cisco Unity Express は、JTAPI アプリケーションおよび 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）Quick Buffer Encoding（QBE）プロトコルを使用して、Cisco CallManager と統合する。CTI ポートおよび CTI ルート ポイントは、Cisco Unity Express のボイスメールおよび自動応答アプリケーションを制御します。
- Cisco Unity Express は、Skinny Client Control Protocol（SCCP）の Cisco IP Phone にボイスメール機能を提供する。将来のリリースでは、Session Initiation Protocol（SIP）IP Phone をサポートする予定です。
- Cisco CallManager では、Cisco Unity Express 用に次の CTI ルート ポイントが定義される。
  - 自動応答エントリ ポイント（Cisco Unity Express は最大 5 つの別個の AA を含むことができるため、最大 5 つの異なるルート ポイントが必要です）。
  - ボイスメール パイロット番号。
  - Greeting Management System（GMS）パイロット番号（オプション。GMS を使用しない場合、このルート ポイントを定義する必要はありません）。
- Cisco CallManager では、Cisco Unity Express 用に次の CTI ポートが定義される。
  - 12 個または 25 個のメールボックスのシステム（4 つのポート）
  - 50 個のメールボックスの AIM-CUE システム（4 つのポート）
  - 50 個のメールボックスの NM-CUE システム（8 つのポート）
  - 100 個のメールボックスのシステム（8 つのポート）
- 各 Cisco Unity Express サイトは、100 個以下のメールボックスを持つ。100 個を超えるメールボックスを必要とする配置では、Cisco Unity または他のボイスメール 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 つの異なる内線番号と関連付けることができる。
- Cisco Unity Express を使用して配置される任意のオフィスの自動応答機能は、そのオフィスに対してローカルにすることも（Cisco Unity Express で AA アプリケーションを使用）、中央集中型にすることも（ボイスメールだけに Cisco Unity Express を使用）できる。
- Cisco Unity Express Release 2.0 以降では、単一の Cisco Unity Express が他の Cisco Unity Express または Cisco Unity に限ってネットワーク接続できる。これにより、Cisco Unity Express 加入者が別のリモートの Cisco Unity Express 加入者または Cisco Unity 加入者にメッセージを転送または送信できます。
- Cisco Unity Express では、フェールオーバー用に最大 3 つの Cisco CallManager を指定できる。3 つすべての Cisco CallManager への IP 接続が失われた場合、Cisco Unity Express は Survivable Remote Site Telephony（SRST）コール制御に切り替えます。したがって、AA コール応答サービスおよび IP Phone からメールボックスへのアクセスの提供、および支店への外線からの着信呼もボイスメールにメッセージを残すことができます。

- Cisco Unity Express の自動応答機能は、内線番号によるダイヤル機能と名前によるダイヤル機能をサポートする。内線番号によるダイヤル操作では、発信者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 の内部にあるディレクトリ データベースを使用し、外部の LDAP データベースとも Active Directory データベースとも対話しません。

図 12-3 では、Cisco CallManager と Cisco Unity Express 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 12-3　Cisco Unity Express と Cisco CallManager の間で使用されるプロトコル

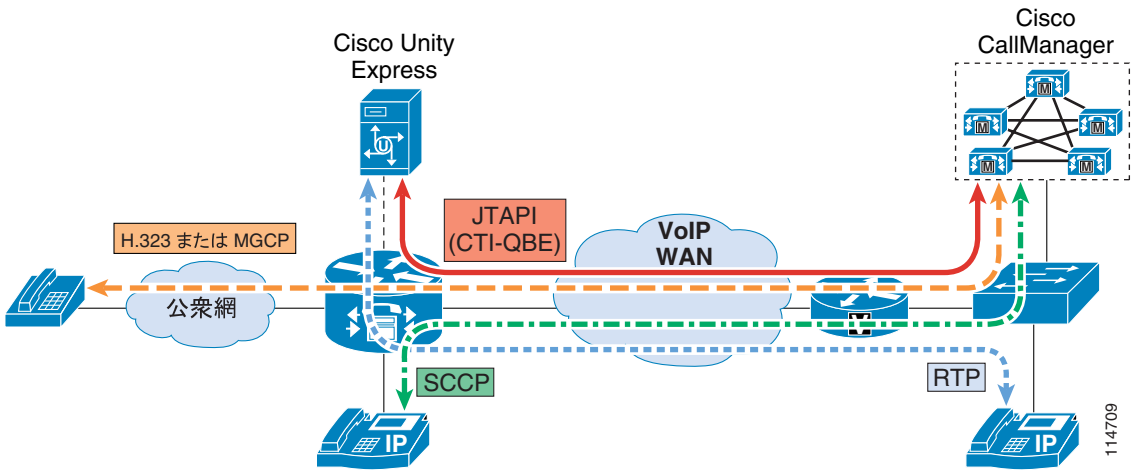


図 12-3 では、次のシグナリング フローおよびメディア フローを示しています。

- 電話機は、Cisco CallManager から SCCP を介して制御される。
- Cisco Unity Express は、Cisco CallManager から JTAPI（CTI-QBE）を介して制御される。
- 電話機の Message Waiting Indicator（MWI; メッセージ待機インジケータ）は、CTI-QBE を介して Cisco CallManager にメールボックスの内容の変更を伝える Cisco Unity Express によって変わり、さらにランプの状態を変えるよう電話機に MWI メッセージを送信する Cisco CallManager によって変わる。
- 音声ゲートウェイは、H.323 または MGCP を介して Cisco CallManager と通信する。
- 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伝送する。

図 12-4 では、WAN リンクがダウンした場合の SRST ルータと Cisco Unity Express 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 12-4　Cisco Unity Express と SRST ルータの間で使用されるプロトコル

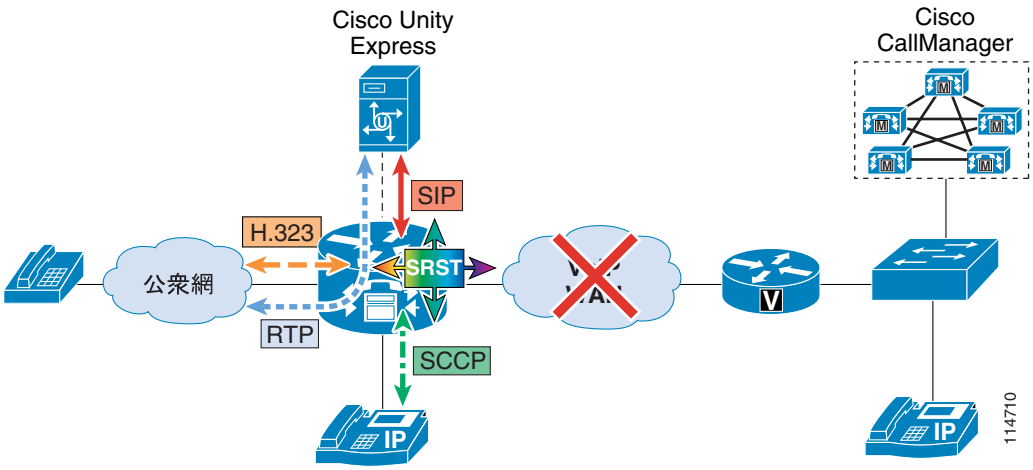


図 12-4 では、次のシグナリング フローおよびメディア フローを示しています。

- 電話機は、SRST ルータから SCCP を介して制御される。
- Cisco Unity Express は、内部 SIP インターフェイスを介して SRST ルータと通信する。
- 現在、SRST モードにおいて MWI の変更はサポートされていない。正常な動作時と同様に、音声メッセージを送信したり取り出したりできますが、電話機が Cisco CallManager に再び登録されるまで、電話機の MWI ランプの状態は変わらないままです。登録された時点で、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と自動的に再同期されます。
- 音声ゲートウェイは、H.323 を介して SRST ルータと通信する。
- 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伝送する。

Cisco Unity Express を配置するためのベスト 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。

- Cisco Unity Express をボイスメールの宛先とする IP Phone は、Cisco Unity Express をホスティングするルータと同じ LAN セグメント上に置く。Cisco Unity Express は、それ自身と同じ場所にない電話機にメールボックスを提供できません。
- Cisco Unity Express を使用して配置するサイトで、中断されない AA およびボイスメール アクセスが必要な場合は、Cisco Unity Express ブレード、SRST、および公衆網音声ゲートウェイ インターフェイスのすべてを同じ物理ルータに統合する。Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）または他の冗長ルータ構成は、現在 Cisco Unity Express でサポートされていません。
- 各メールボックスを、プライマリ内線番号およびプライマリ E.164 番号と関連付けることができる。通常、プライマリ E.164 番号は、外線からの発信者が使用する Direct-Inward-Dial（DID; ダイヤルイン）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は、Cisco IOS トランスレーション 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 番号のいずれかに一致させ、SRST モード中に正しいメールボックスに到達できるようにします。
- 各 Cisco Unity Express サイトは、少なくとも 2 つの CTI ルート ポイントおよび 4 つの CTI ポートに関連付けられる必要がある。Cisco Unity Express を使用するサイトの数が、第 8 章「コール処理」に記載されている CTI スケーラビリティのガイドラインを超えないようにします。

- Cisco Unity Express を、Cisco CallManager 上の JTAPI ユーザと関連付ける。1 人の JTAPI ユーザをシステム内の複数の Cisco Unity Expresse と関連付けることができますが、Cisco CallManager 上の各専用 JTAPI ユーザを単一の Cisco Unity Express に関連付けることをお勧めします。
- Cisco Unity Express へのコールは G.711 だけを使用する。ローカル 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。リージョン内コールには G.711 音声コーデックを使用し、リージョン間コールには G.729 音声コーデックを使用するように Cisco CallManager リージョンを設定できます。
- Cisco Unity Express サイトでトランスコーディング ファシリティを使用できない場合は、WAN を介した G.711 ボイスメール コールの必要数に合せて十分な帯域幅をプロビジョニングする。IP Phone と Cisco Unity Express デバイス（CTI ポートおよび 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 Cisco CallManager リージョンを設定します。
- CTI ポートおよび CTI ルート ポイントは、特定のロケーションに定義できる。Cisco CallManager と Cisco Unity Express の間では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。
- Cisco Unity Express と Cisco CallManager の間の WAN を通過するシグナリング トラフィックに対して、適切な QoS（Quality of Service）と帯域幅を確保する。各 Cisco Unity Express サイトの CTI-QBE シグナリングに対して 20 kbps の帯域幅をプロビジョニングします。詳細については、第 3 章「ネットワーク インフラストラクチャ」を参照してください。
- Cisco CallManager から Cisco Unity Express への CTI-QBE シグナリング パケットは、AF31 の DSCP 値（0x68）でマーキングされる。ただし、Cisco Unity Express から Cisco CallManager への CTI-QBE シグナリング パケットはマーキングされません。Access Control List（ACL; アクセス コントロール リスト）を使用してこのような CTI-QBE パケットをマーキングし、適切な QoS を確保することをお勧めします。例 12-1 では、CTI-QBE シグナリング パケットに対して適切な QoS を実現するための設定例を示しています。Cisco CallManager は、CTI-QBE シグナリングに TCP ポート 2748 を使用します。

例 12-1　CTI-QBE シグナリング パケット用の QoS 設定

```
access-list 101 permit tcp host a.b.c.d any eq 2748
!
class-map match-all cti-qbe
 match access-group 101
!
policy-map cti-qbe
 class cti-qbe
 set dscp af31
 bandwidth 20
!
interface Serial0/1
 service-policy output cti-qbe
```

サードパーティ製のボイスメール システム

数多くのボイスメール ベンダーが存在します。お客様が Cisco CallManager を配置するときに、既存のボイスメール システムを引き続き使用するよう希望するのは、珍しいことではありません。このような要求を念頭において、シスコは、Simplified Message Desk Interface（SMDI）と呼ばれる業界標準のボイスメール プロトコルをサポートしています。SMDI はシリアル プロトコルであり、ボイスメール システムが適切にコールに応答するために必要なすべてのコール情報を提供します。

この他にも、Digital Set Emulation、Microsoft TAPI、QSIG など、Cisco CallManager をボイスメール システムに統合するためのオプションがあります。各方法にはそれぞれ長所と短所があり、採用する方法は、ボイスメール システムがどのように現在の PBX に統合されているかに大きく左右されます。

ここでは、サードパーティ製のボイスメール システムと Cisco CallManager の統合について、次の項目を説明します。

SMDI

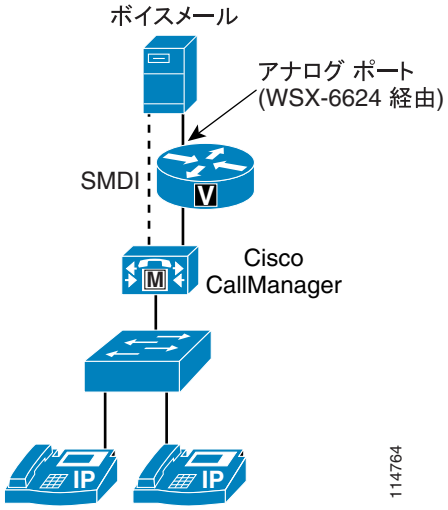
Cisco CallManager では、次のいずれかの方法で SMDI を使用できます。

Cisco Messaging Interface

Cisco Messaging Interface（CMI）は、パブリッシャ サーバ上だけで実行する必要のある Cisco CallManager サービスです。このサービスは、ボイスメール用のコールを代行受信して、適切な SMDI メッセージを生成します。その後、この SMDI メッセージはサーバの Component Object Model（COM; コンポーネント オブジェクト モデル）ポートの 1 つに送信されます。CMI は、アナログ FXS ポートまたは T1 CAS E&M をサポートするどの MGCP ゲートウェイにも対応しています。ただし、WS-X6624 モジュールは、確実な接続解除監視（P.12-16 の「確実な接続解除監視」を参照）をサポートする 2 つしかないゲートウェイの 1 つであるため、現在 CMI と共に使用することが推奨される唯一のゲートウェイです。

図 12-5 では、Cisco CallManager 内の CMI を介して SMDI を使用する方法を示しています。

図 12-5　Cisco CallManager を介した SMDI



Cisco CallManager は、CMI を介して、事実上、アナログ FXS ポートを備えた SMDI を提供できるどのボイスメール システムとの統合もサポートしています。このボイスメール システムには、次のようなものがあります。

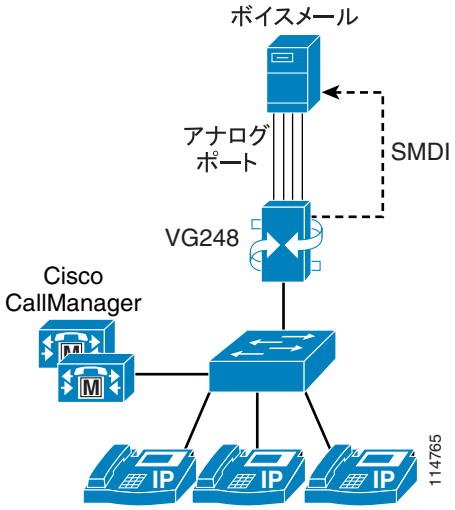
- Octel 100、200/300、および 250/350
- Intuity Audix
- Siemens PhoneMail
- Centigram/BayPoint（OnePoint Messenger および NuPoint Messenger）
- Lyrix ECS
- IBM Message Center

Cisco VG248

Cisco VG248 は SCCP ゲートウェイであり、48 個のアナログ FXS ポートをサポートし、ローカルで SMDI を生成します（つまり、CMI サービスとは関係なく動作します）。WS-X6624 モジュールと同様に、VG248 も確実な接続解除監視をサポートしています。

図 12-6 では、VG248 によって SMDI を使用する方法を示しています。

図 12-6　VG248 を介した SMDI



VG248 を介したボイスメール統合では、次の機能および利点が提供されます。

- Cisco CallManager ごとに複数の SMDI リンク
- SMDI フェールオーバー機能
- ボイスメール システムのロケーションからの独立性

VG248 は、ボイスメール統合に使用されることのある他の 2 つのシリアル プロトコルもサポートできます。そのプロトコルとは、NEC Message Center Interface（MCI）および Ericsson MD110 専用プロトコルです。

FXS ポートを使用する場合の考慮事項

ボイスメール システムにアナログ FXS ポートが装備されている場合は、次の Cisco ゲートウェイを使用してボイスメール システムと統合します。

- WS-X6624

  Catalyst 6500 シャーシ内にこのモジュールに使用できるスロットがある場合は、このモジュールを使用します。

- VG248

  シリアル ポートおよび音声ポートに完全なフェールオーバーが必要な場合、SMDI 以外のシリアル プロトコル（たとえば、NEC MCI や Ericsson MD110）が必要な場合、または Catalyst 6500 シャーシのスロットが使用できない場合は、このゲートウェイを使用します。

Digital Set Emulation

Digital Set Emulation（DSE）は、PBX をボイスメール システムに統合するもう 1 つの方法です。このモードでは、ボイスメール ポートが PBX にとって専用デジタル受話器のように見えます。この統合方法は、アナログ FXS ポートを備えた SMDI を使用する場合よりも次の点で優れています。

- 音声パスとコール情報のシグナリングの両方で、回線が完全にデジタルである。
- 音声とシグナリングの両方が同じ物理回線を介して転送されるため、アウトバンド シグナリングがない。
- 一般に、コールの全体的な品質が高い。

Digital PBX Adapter（DPA）

シスコは、特に、Digital Set Emulation を介して Cisco CallManager をサードパーティ製のボイスメール システムと統合するために、Digital PBX Adapter（DPA）を開発しました。DPA は、基本的に、一方の側で IP 接続を持ちながら、もう一方の側で複数のデジタル PBX 内線として機能します。DPA を使用すると、既存のボイスメール　　システムとそのインターフェイスを保持しながら、Cisco CallManager に接続できます。

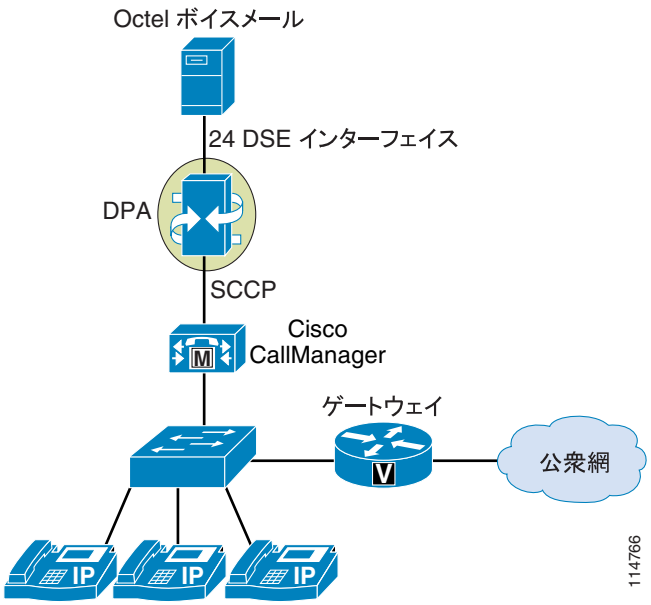
これら 2 種類の DPA があります。

- Avaya Definity G3 7400 シリーズのデジタル電話セットをエミュレートするための DPA 7630
- Nortel Meridian 1 2616 デジタル電話セットをエミュレートするための DPA 7610

（注）　DPA は、Lucent/Avaya または Nortel の Digital Set Emulation を使用する場合に限り、Octel Aria 250/350 または Serenade 200/300 のボイスメール システムと連携します。

図 12-7 では、Octel ボイスメール システムを Cisco CallManager と統合している DPA を示しています。

図 12-7　Octel ボイスメールを Cisco CallManager と統合している DPA



二重 PBX 統合

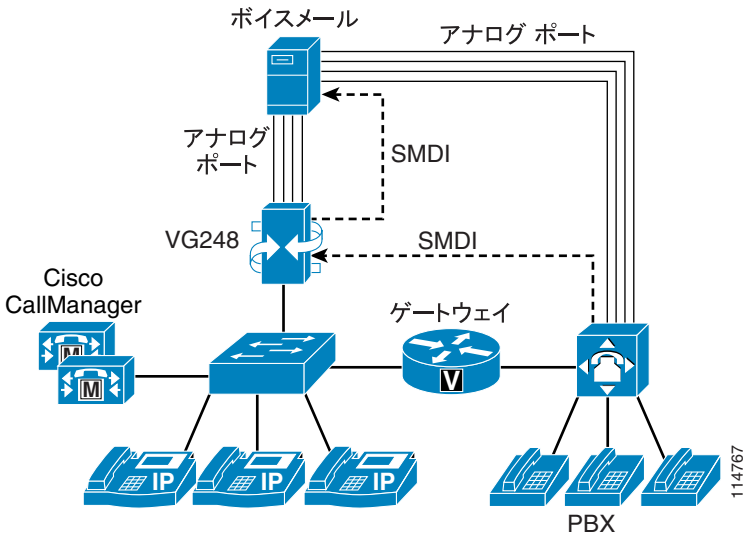
二重 PBX 統合は、既存のボイスメール サービスを保持しながら、現在の PBX から IP テレフォニーに移行する企業にとって便利なオプションです。

(注)

このシナリオは複雑であるため、ほとんどのボイスメール　ベンダーはこのシナリオをサポートしていませんが、必要に応じて「サイト固有に」サポートするベンダーもあります。このソリューションを実装するには、事前にボイスメール ベンダーに問い合せてください。

Cisco VG248 には、二重統合を提供できるようにする固有の多重化機能が備わっています。VG248 は、既存のシリアル リンクからの情報を独自のリンクと結合してから、単一のシリアル ストリームをボイスメール システムに提供できます（図 12-8 を参照してください）。

図 12-8　VG248 と SMDI を介した二重統合

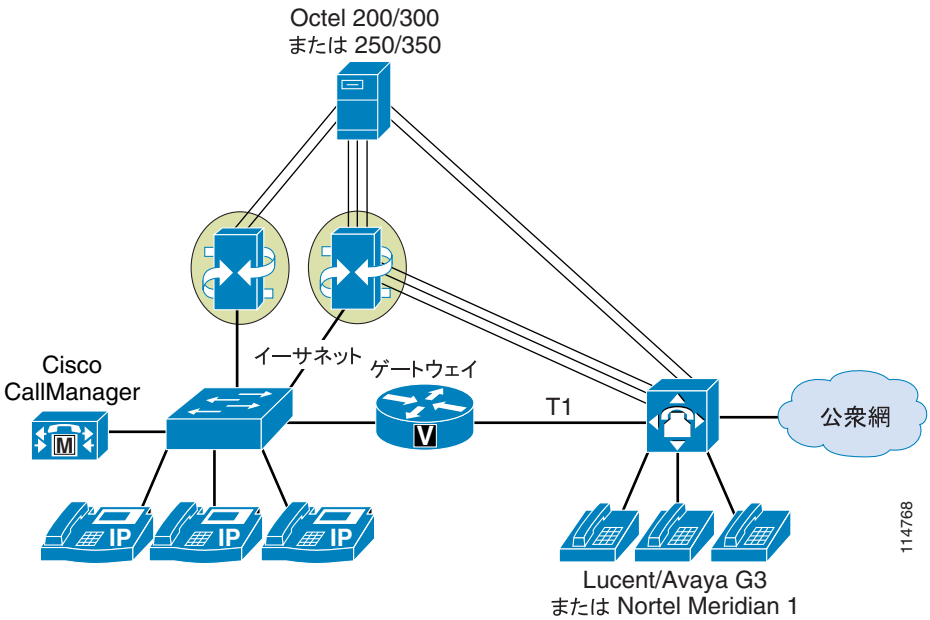


VG248 は、SMDI 機能とアナログ FXS ポートを備えた任意のボイスメール システムと連携します。二重統合が必要である場合は、実装する前に次の前提条件が必要となります。

- 統一されたダイヤル プラン
- 転送および再接続のシーケンス
- PBX と Cisco CallManager の間の接続

図 12-9 に示しているように、Cisco DPA にも Digital Set Emulation を介して二重統合を実現する機能が備わっています。

図 12-9　DPA を介した二重統合



DPA は、Octel の Digital Set Emulation と連携します。二重統合が必要である場合は、実装する前に次の前提条件が必要となります。

- 統一されたダイヤル プラン
- 転送および再接続のシーケンス
- PBX と Cisco CallManager の間の接続

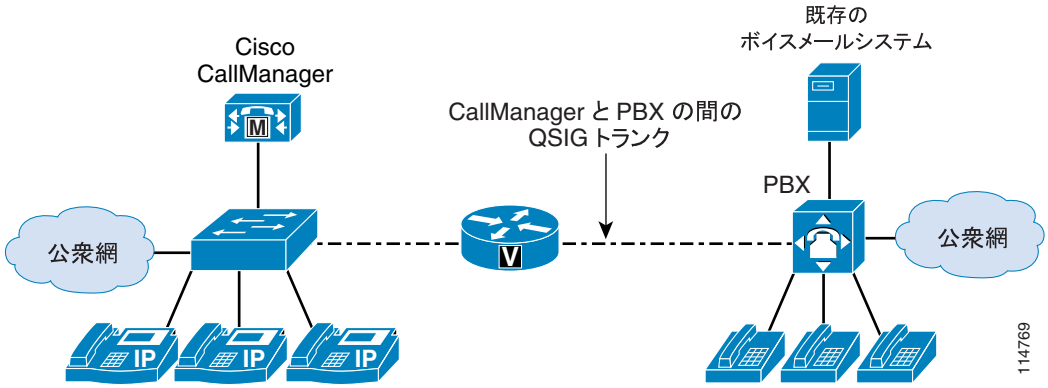
集中型ボイスメール

集中型ボイスメール配置では、複数の PBX が単一のボイスメール システムを共有します。この共有は、ボイスメール システムを 1 つの PBX だけに統合してから、PBX 間のプライベート ネットワーキング プロトコルを利用して、ボイスメール サービスをリモート加入者まで拡張することによって実現されます。ネットワーク接続された PBX は、ボイスメール システムにとって、1 つの大規模な PBX のように見え、そのように機能します。さまざまな PBX 製造業者が、大規模なネットワーク全体の加入者に対する機能透過性を実現しながらそのようなサービスの提供を可能にする専用プロトコル（たとえば、Avaya DCS、Nortel MCDN、Siemens CorNet、Alcatel ABC、NEC CCIS、Fujitsu FIPN）を開発しました。

集中型ボイスメール システムを使用するための主な動機付けは、既存のボイスメール システムから IP テレフォニー加入者にボイスメール サービスを提供することで、加入者が新しい Telephony User Interface（TUI; 電話ユーザ インターフェイス）を学習する必要がないようにするという目的から来ています。

一部のボイスメール システムは、Simple Messaging Desktop Interface（SMDI）などのプロトコルを介して複数の PBX をサポートできます（二重 PBX 統合）。Cisco Digital PBX Adapter（DPA）など、二重統合を可能にする他のソリューションも導入されています。状況によっては、ボイスメール ベンダーがこの構成をサポートしないと決めたため、このようなソリューションを実現できないことがあります。また、ボイスメール システムが、異なる PBX 統合を同時にサポートできないため、二重統合が単に技術的に不可能な場合もあります。そのような場合は、集中型ボイスメール配置が、二重統合に代わるソリューションを提供します（図 12-10 を参照してください）。

図 12-10　Cisco CallManager と QSIG による集中型ボイスメール



「集中型ボイスメール」という用語は、ボイスメール システム自体を意味しているのではないことに注意してください。集中型ボイスメールは、ボイスメール機能の提供に必要な、PBX の PBX 間ネットワーキング プロトコル（Avaya DCS、Nortel MCDN、Siemens CorNet などの専用プロトコル、または QSIG や DPNSS などの規格ベース プロトコル）の機能です。

集中型ボイスメールには、次の重要な用語および概念が適用されます。

- メッセージ センター Private Integrated Services Network Exchange（PINX）：これは、ボイスメール システムを「ホスティング」する PBX です（ボイスメール システムに直接接続されている PBX）。
- サブスクライバ PINX：これは、ボイスメール システムから「リモート」である PBX です（ボイスメール システムに直接接続されていない PBX）。

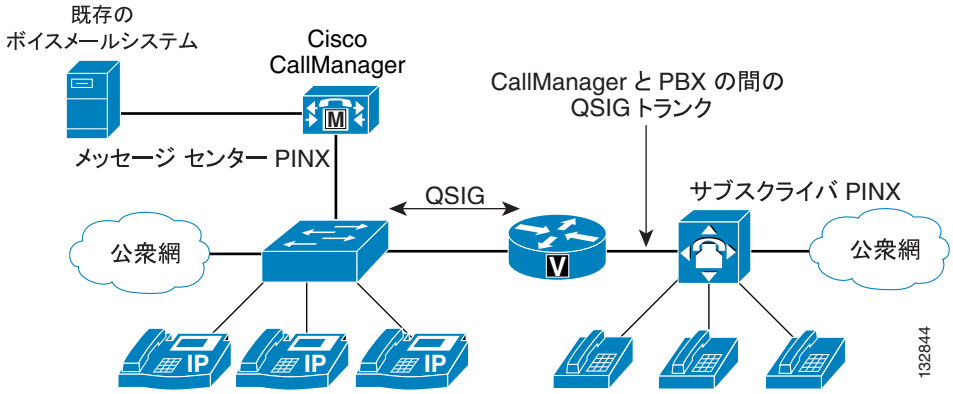
集中型ボイスメール構成では、QSIG などの適切な PBX 間ネットワーキング プロトコルが必要です。このプロトコルは、次のような最小限の機能サポートも提供する必要があります。

- Message Waiting Indicator（MWI; メッセージ待機インジケータ）
- 転送：正しい発信者 ID と着信者 ID がボイスメール システムに送信されることを保証するために必要です。
- 宛先変更：正しい発信者 ID と着信者 ID がボイスメール システムに送信されることを保証するために必要です。

ボイスメール システムがどのように使用されるかに応じて、他の機能が必要になる場合もあります。たとえば、ボイスメール システムが自動応答機能も提供する場合は、ヘアピンコールを防ぐために、パス置換機能が必要となります。

すべての PBX がメッセージ センター PINX として機能できるわけではありません。PBX がメッセージ センター PINX として機能できない場合は、ボイスメール システムを Cisco CallManager の方に移動して、Cisco CallManager をメッセージ センター PINX として機能させ、PBX をサブスクライバ PINX として機能させることを検討します（図 12-11 を参照してください）。

図 12-11　Cisco CallManager がメッセージ センター PINX として機能する集中型ボイスメール



サポート

シスコは、他のベンダーの製品が特定の方法で動作することを保証できません。また、他のベンダーの製品に対する設定変更またはアップグレードに関して、何が必要であるかを指示できません。各製品のサプライヤやベンダーに直接質問をしたり確認を求めたりするのは、お客様の責任です。

シスコは、お客様がサプライヤやベンダーに尋ねるべき質問を決める際に、お役に立つことができます。たとえば、「QSIG を介して接続されるリモート PBX ユーザが、メールボックスを持ち、かつすべてのボイスメール機能（MWI など）にフル アクセスできるようにするには、PBX に対して何を行う必要がありますか」などの質問です。

PBX の相互運用性を支援するために、シスコはさまざまな PBX を Cisco CallManager とテストし、これらのテストをアプリケーション ノートという形で文書化しています。これらの文書は、成功を保証するものではありませんが、サポートされている機能および Cisco CallManager と PBX の両方の設定詳細に関して、ある程度のガイダンスを提供します。主な PBX に関して Cisco CallManager のアプリケーション ノートがすでに記述されており、その中で Cisco CallManager がメッセージ センター PINX として機能する集中型ボイスメールのシナリオが扱われています。アプリケーション ノートは、次の Web サイトで入手できます。

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

（注） シスコは、メッセージ センター PINX として機能する他のベンダーの PBX をテストすることはできません。シスコには、このようなシステムを構成するファシリティも専門知識もありません。したがって、お客様がこれらの情報をサプライヤやベンダーに直接要求する必要があります。

要約

- 集中型ボイスメールは、ボイスメール システム自体ではなく、PBX 間ネットワーキング プロトコルの機能である。
- すべての PBX がメッセージ センター PINX として機能できるわけではない。お客様が PBX のサプライヤやベンダーにこの機能を確認する必要があります。シスコは、PBX のこの機能を提供することもサポートすることもできません。
- Cisco CallManager はメッセージ センター PINX として機能できるため、PBX がこの機能を実行できない場合、お客様に代替を提供できる。
- パス置換が必要であるかを確認する必要がある。Cisco CallManager Release 4.1 以降は、この機能をサポートしています。

確実な接続解除監視

確実な接続解除監視は、遠端のデバイスがオンフックになったことを示すために PBX ポートからボイスメール システムに送信される信号です。この信号は、通常、約 600 ms のループ電流切断という形を取ることによって、ボイスメール システムにセッションを終了させます。

この信号がないと、ボイスメール システムは遠端のデバイスがオンフックになったことを認識せず、この状況で PBX が提供するどのような監視トーンでも録音し続けます（たとえば、ダイヤルトーンを再生する PBX も、ビジー トーンを再生する PBX もあります）。ボイスメール システムは、メッセージの最大時間に達するまで、このようなトーンを録音し続けます（たとえば、メールボックスでメッセージごとの制限が 3 分であり、発信者が 30 秒後に電話を切った場合、確実な接続解除監視がないと、ボイスメール システムはその後 2 分 30 秒間このようなトーンを録音し続けます）。この不必要な録音によって、加入者がいらいらすることがあります。また、ディスク使用率が上がり、ポート使用時間が増えるため、システムのパフォーマンスが低下することもあります。ボイスメール システムの中には、既知のトーンを監視して、その後削除することにより、このシナリオに対処できるものもありますが、その場合でもシステム パフォーマンスへの影響は避けられません。

加入者がメールボックスにコールしてメッセージがないか調べる場合にも、同様の問題が発生します。接続解除監視がない場合にユーザが単に電話を切ると、ボイスメール システムは、アクティビティ タイマーが期限切れになるまで、セッションを終了させずに有効な応答を待ち続けます。このシナリオの場合、主な影響は追加のポート使用時間が発生することからもたらされます。

これらの理由から、ボイスメール システムに接続されているアナログ ポートが、確実な接続解除監視を提供する必要があります。

サードパーティ製ボイスメール統合の要約

ボイスメール システムを Cisco CallManager に接続する方法は他にもありますが（SMDI と併用する Microsoft TAPI および PRI ISDN トランクなど）、これらの方法は一般的ではありません。サードパーティ製ボイスメール統合の大部分は、Cisco VG248 を使用します。これがお勧めのソリューションです。

Cisco CallManager をボイスメール システムに統合する方法は、ボイスメール システムが現在どのように PBX に統合されているかによって異なります。現在アナログ ポートが使用されている場合、Cisco VG248 は優れた統合方法を提供します。ただし、Avaya または Nortel の Digital Set Emulation が使用されている場合は、Cisco DPA を導入すると、現在のボイスメール システムをアナログ FXS ポート用に設計し直さずに統合を行うことができるため、低コストでソリューションを実現できます。

（注） シスコは、サードバーティ製のボイスメール システムのテストおよび認定を行いません。一般に、業界では、このような製品をさまざまな PBX システムに対してテストしたり認定したりするのは、ボイスメール ベンダーの責任であると考えられています。もちろん、シスコは、接続されるサードバーティ製のボイスメール システムに関係なく、PBX システムに対してシスコのインターフェイスをテストし、そのインターフェイスをサポートします。

CHAPTER 13

Cisco Unity

この章では、Cisco Unity と Cisco CallManager の統合について、設計上の側面を中心に説明します。この章で扱う設計に関するトピックは、ボイスメール配置とユニファイド メッセージング配置の両方に適用されます。

さらに、この章では、Microsoft Exchange 2000 または 2003 メッセージ ストアあるいは Lotus Notes Domino メッセージ ストアおよび Microsoft Windows 2000 または 2003 と共に Cisco Unity を配置する場合の設計上の問題についても説明します。この章では、Microsoft NT 4.0 や Exchange 5.5 による配置、および Microsoft NT 4.0 や Exchange 5.5 からのアップグレードは扱いません。

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 に関するその他の設計情報については、次の Web サイトで入手可能な『*Cisco Unity Design Guide*』を参照してください。

http://www.cisco.com

この章では、Cisco Unity の設計に関する次のトピックについて取り上げます。

Cisco CallManager Release 4.0 では、回線グループ、ハント リスト、およびハント パイロットが導入されています。これらは、既存の音声ポートの動作に影響を及ぼすことができます。旧バージョンの Cisco CallManager から Cisco CallManager Release 4.0 以降にアップグレードする前に、該当する 4.*x* リリースの『*Cisco CallManager Administration Guide*』を参照してください。このマニュアルは、次の Web サイトで入手できます。

http://www.cisco.com

この章で説明する配置モデルおよび設計上の考慮事項はすべて、Cisco CallManager Release 3.1 以降によって完全にサポートされています。

メッセージング配置モデル

Cisco Unity は、次の 3 つの主なメッセージング配置モデルをサポートしています。

- 単一サイト メッセージング（P.13-2）
- 集中型メッセージング（P.13-2）を使用するマルチサイト WAN 配置
- 分散型メッセージング（P.13-3）を使用するマルチサイト WAN 配置

Cisco CallManager と Cisco Unity の両方を含む配置では、Cisco CallManager に 1 つのコール処理モデルを使用し、Cisco Unity に 1 つのメッセージング モデルを使用します。メッセージング配置モデルは、配置されるコール処理モデルのタイプに依存しません。

3 つのメッセージング配置モデルに加えて、Cisco Unity はメッセージング フェールオーバーもサポートしています（P.13-3 の「メッセージング フェールオーバー」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、ボイスメールとユニファイド メッセージングの両方のインストールをサポートしています。

単一サイト メッセージング

このモデルでは、メッセージング システムとメッセージング インフラストラクチャ コンポーネントがすべて、アベイラビリティの高い同じ LAN 上の同じサイトに置かれます。サイトは、単一サイトである場合も、高速 Metropolitan Area Network（MAN; メトロポリタン エリア ネットワーク）を介して相互接続されたキャンパス サイトである場合もあります。メッセージング システムのクライアントもすべて、単一（またはキャンパス）サイトに置かれます。このモデルの際立った特徴は、リモート クライアントが存在しないことです。

集中型メッセージング

このモデルでは、単一サイト モデルと同様に、メッセージング システムとメッセージング インフラストラクチャ コンポーネントがすべて、同じサイトに置かれます。サイトは、1 つの物理的なサイトである場合も、高速 MAN を介して相互接続されたキャンパス サイトである場合もあります。ただし、単一サイト モデルとは異なり、集中型メッセージング クライアントをローカルとリモートの両方に置くことができます。

メッセージング クライアントがメッセージング システムに対してローカルでもリモートでもかまわないため、特別な設計上の考慮事項が、次の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）クライアントに対して適用されます。そのクライアントとは、Microsoft Exchange を使用する ViewMail for Outlook（VMO）クライアント、Lotus Domino を使用する Domino Unified Communications Services（DUC）クライアント、および Telephone Record and Playback（TRaP; 電話での録音および再生）機能とメッセージ ストリーミング機能を使用するクライアントです。リモート クライアントは、TRaP を使用できません。また、リモート クライアントは、再生前にメッセージをダウンロードするように設定する必要があります。ローカル クライアントとリモート クライアントで機能や操作が異なるとユーザが混乱する恐れがあるため、クライアントがローカルであるかリモートであるかに関係なく、音声ポートで TRaP を無効にし、メッセージをダウンロードするように、および TRaP を使用しないように GUI クライアントを設定する必要があります。Cisco Unity Personal Assistant（CPCA）を介してアクセスされる Cisco Unity Inbox は、ローカル クライアントに

対してだけ許可される必要があります。Cisco Unity Telephone User Interface（TUI; 電話ユーザ インターフェイス）は、ローカル クライアントとリモート クライアントの両方に対して同様に動作します。

分散型メッセージング

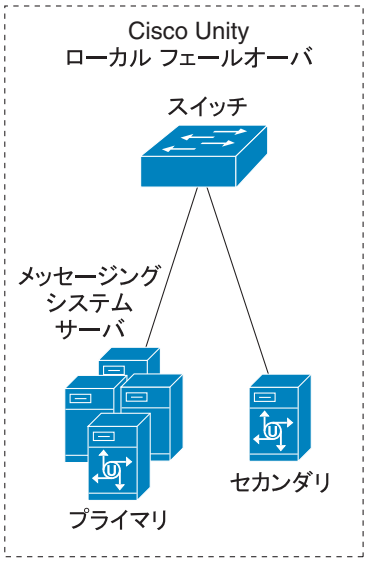
分散型メッセージングでは、メッセージング システムとメッセージング インフラストラクチャ コンポーネントが分散方式で同じ場所に置かれます。複数のロケーションを持つことができ、各ロケーションに独自のメッセージング システムとメッセージング インフラストラクチャ コンポーネントが置かれます。すべてのクライアント アクセスが各メッセージング システムに対してローカルであり、メッセージング システムは、すべてのロケーションにまたがるメッセージング バックボーンを共有します。分散型メッセージング システムからのメッセージ送信は、ハブアンドスポーク タイプのメッセージ ルーティング インフラストラクチャによって、メッセージング バックボーンを介して行われます。WAN によって、メッセージング インフラストラクチャ コンポーネントを、サービス提供先のメッセージング システムから切り離すことはできません。分散型メッセージングは、基本的に、共通のメッセージング バックボーンを持つ複数の単一サイト メッセージング モデルです。

分散型メッセージング モデルは、ローカルおよびリモートの GUI クライアント、TRaP、およびメッセージのダウンロードに関して、集中型メッセージングと同じ設計基準を持っています。

メッセージング フェールオーバー

3 つのメッセージング配置モデルはすべて、メッセージング フェールオーバーをサポートしています。図 13-1 に示しているように、ローカル メッセージング フェールオーバーを実装できます。ローカル フェールオーバーでは、プライマリ Cisco Unity サーバとセカンダリ Cisco Unity サーバの両方が、アベイラビリティの高い同じ LAN 上の同じサイトに置かれます。

図 13-1　Cisco Unity メッセージングのローカル フェールオーバー



Cisco Unity および Cisco CallManager は、メッセージング配置モデルとコール処理配置モデルの次の組み合せをサポートしています。

- 単一サイト メッセージングと単一サイト コール処理
- 集中型メッセージングと集中型コール処理
- 分散型メッセージングと集中型コール処理
- 集中型メッセージングと分散型コール処理
- 分散型メッセージングと分散型コール処理

サイト分類の詳細、およびメッセージング配置モデルとコール処理配置モデルのサポートされている組み合せの詳細な分析については、http://www.cisco.com で入手可能な『*Cisco Unity Design Guide*』を参照してください。

メッセージング システム インフラストラクチャ コンポーネント

Cisco Unity は、Dynamic Domain Name Server（DDNS）、ディレクトリ サーバ、メッセージ ストアなど、さまざまなネットワーク リソースと対話します（図 13-2 を参照してください）。Cisco Unity は、単一の一体型デバイスではなく、相互依存コンポーネントのシステムと見なす方が適しています。正常に動作するには、Cisco Unity メッセージング システムの各メッセージング システム インフラストラクチャ コンポーネントが必要であり、これらすべてのコンポーネントがアベイラビリティの高い同じ LAN 上に存在することが重要です（ほとんどの場合、これらのコンポーネントは物理的に同じ場所に置かれます）。これらのコンポーネント間に WAN リンクがある場合は、どのような WAN リンクでも、Cisco Unity の動作に影響を及ぼす遅延を引き起こす可能性があります。このような遅延は、TUI 操作中の長い遅延や無音期間となって表れます。詳細については、http://www.cisco.com から入手可能な『*Cisco Unity Design Guide*』の「Network and Infrastructure Considerations」の章を参照してください。

図 13-2　Cisco Unity メッセージング システム インフラストラクチャ コンポーネント

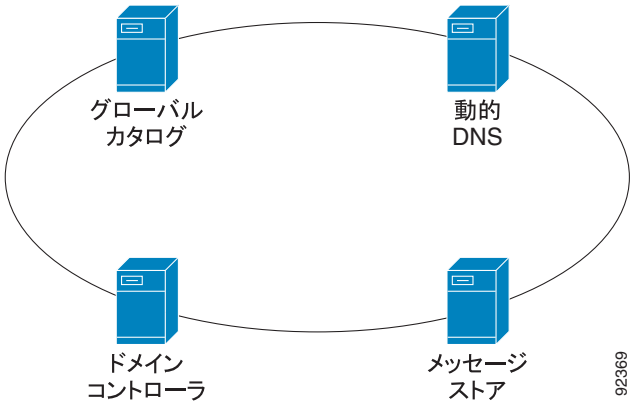


図 13-2 は、メッセージ システム インフラストラクチャ コンポーネントを論理的に表現したものです。これらのコンポーネントのいくつかは、同じサーバ上に置くことができます。Domino Lotus Notes の場合、メッセージ ストアとディレクトリ（Names.nsf）が同じサーバ上に置かれます。Microsoft Windows、グローバル カタログ サーバ、およびドメイン コントローラも同じサーバ上に置くことができます。メッセージ ストア クラスタリングの場合と同様に、Cisco Unity が Microsoft Exchange 2000 または 2003 および Lotus Domino に対してサポートする各コンポーネントの複数のインスタンスを使用することもできます。すべてのメッセージング システム インフラストラクチャ コンポーネントは、サービス提供先の Cisco Unity サーバと同じ、アベイラビリティの高い LAN 上に置く必要があります。分散型メッセージングを使用して Cisco Unity を配置する場合は、各サイト（ロケーション）がメッセージング システム コンポーネントの独自の完全なセットを持っている必要があります。

帯域幅の管理

Cisco CallManager は、帯域幅を管理するためのさまざまな機能を備えています。リージョン、ロケーション、およびゲートキーパーさえも使用して、Cisco CallManager は、WAN リンクを介して伝送される音声コールの数によって既存の帯域幅がオーバーサブスクリプションの状態になることがなく、音声品質が低下しないことを保証できます。Cisco Unity は、帯域幅の管理とコールのルーティングを Cisco CallManager に依存しています。コール（音声ポート）が WAN リンクを通過することのある環境に Cisco Unity 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 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 Cisco CallManager がリモートに置かれている場合（分散型メッセージングまたは集中型コール処理）、いつでも発生します。ゲートキーパーベースのコール アドミッション制御に代わる唯一の方法は、Cisco CallManager のリージョンとロケーションの使用です。

図 13-3 では、集中型メッセージングと集中型コール処理を使用する小規模なサイトで、リージョンとロケーションを連携させて使用可能な帯域幅を管理する方法を示しています。リージョンとロケーションの詳細については、第 9 章「コール アドミッション制御」を参照してください。

図 13-3　ロケーションとリージョン

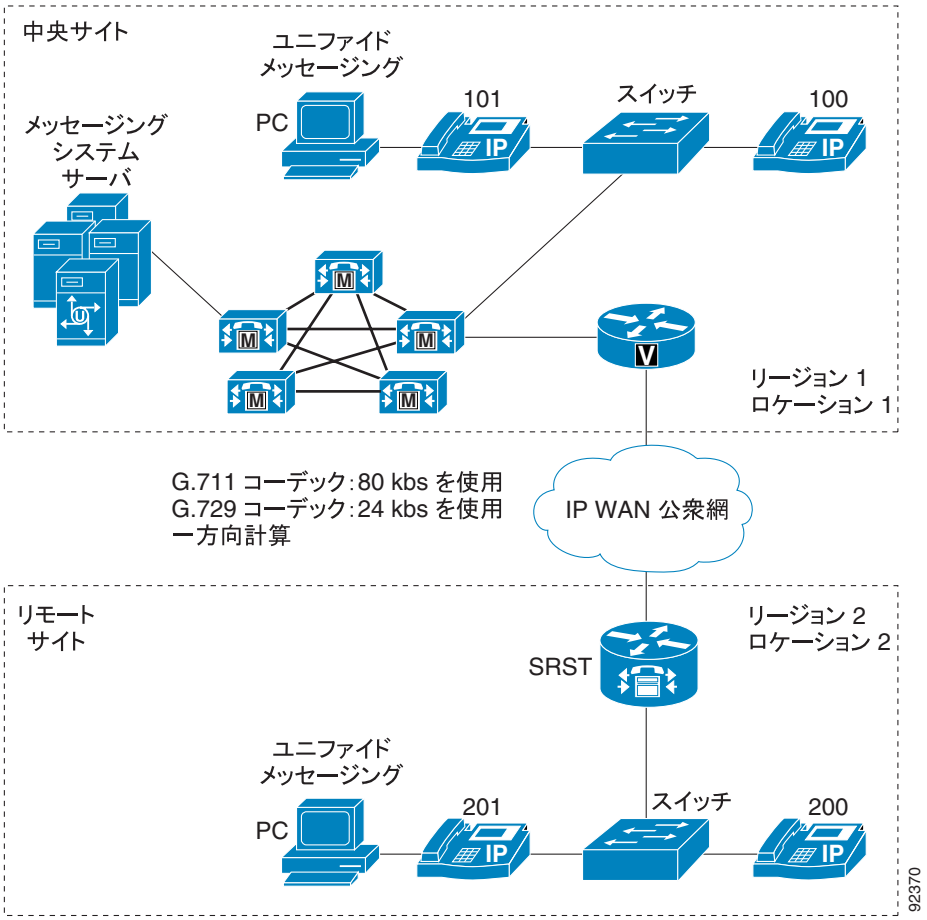


図 13-3 では、リージョン 1 と 2 が、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。ロケーション 1 と 2 は、両方 24 kbps に設定されています。ロケーションの帯域幅は、ロケーション間コールの場合にだけ配分されます。

リージョン内（G.711）コールは、ロケーションの使用可能な帯域幅に対して配分されません。たとえば、内線番号 100 が内線番号 101 をコールする場合、このコールはロケーション 1 の使用可能帯域幅 24 kbps に対して配分されません。ただし、G.729 を使用するリージョン間コールは、ロケーション 1 とロケーション 2 の両方の帯域幅割り当て 24 kbps に対して配分されます。たとえば、内線番号 100 が内線番号 200 をコールすると、このコールは接続されますが、追加の（同時）リージョン間コールでは、リオーダー（ビジー）トーンが聞こえます。

AAR によってルーティングされるボイスメール コールで RDNIS が送信されないことによる影響

Cisco CallManager の機能である Automated Alternate Routing（AAR; 自動代替ルーティング）では、WAN がオーバーサブスクリプションの状態になった場合に、公衆網を介してコールをルーティングできます。ただし、公衆網を介してコールが再ルーティングされる場合、Redirected Dialed Number Information Service（RDNIS）が損なわれることがあります。Cisco Unity がメッセージング クライアントに対してリモートである場合は、正しくない RDNIS 情報によって、AAR が外線を介して再ルーティングするボイスメール コールに影響が及ぼされることがあります。RDNIS 情報が正しくない場合、コールはダイヤル先のユーザのボイスメール ボックスに到達せず、自動アテンダント プロンプトを受信します。発信者は、到達を試みているユーザの内線番号を再入力するように要求されることがあります。この動作は、主に、電話通信事業者がネットワークを介した RDNIS を保証できない場合の問題です。通信事業者が RDNIS の正常な送信を保証できない理由は数多くあります。通信事業者に問い合せて、回線のエンドツーエンドで RDNIS の送信を保証しているかどうかを確認してください。オーバーサブスクリプションの状態になった WAN に対して AAR を使用する代わりの方法は、単に、オーバーサブスクリプションの状況で発信者にリオーダー トーンが聞こえるようにすることです。

Cisco Unity のネイティブ トランスコーディング動作

デフォルトでは、Cisco Unity サーバは自動的にトランスコーディングを実行します。現在、Cisco CallManager および Cisco Unity は、SCCP TAPI Service Provider（TSP）音声ポートに対して G.729 と G.711 だけをサポートしています。他のコーデックは、Intel または Dialogic の音声ボードを使用する従来型の統合でサポートされています。Cisco Unity のネイティブ トランスコーディングは、外部ハードウェア トランスコーダを使用せず、サーバのメイン CPU を使用します。Cisco CallManager がハードウェア トランスコーダを音声ポート コールに割り当てるようにするには、レジストリ設定によって、Cisco Unity サーバ上でネイティブ トランスコーディングを無効（オフ）にする必要があります。このレジストリ設定は「Audio - Enable G.729a codec support」と呼ばれます。これを設定するためのツールは、http://www.CiscoUnityTools.com で入手可能な *Advanced Settings Tool* です。デフォルトでは、コーデック レジストリ キーが存在しないため、ネイティブ トランスコーディングは有効（オン）です。Advanced Settings Tool により、使用可能な 2 つのコーデックのうちのどちらか 1 つを選択できる新しいレジストリ キーが追加されます。その後、Cisco Unity は、1 つのコーデックだけをサポートすることを Cisco CallManager に「アドバタイズ」します。音声ポートを終端または起点とするコールが、Cisco Unity サーバに設定されているタイプと異なるコーデックを使用している場合、Cisco CallManager はそのコールに外部トランスコーディング リソースを割り当てます。Cisco CallManager 上でトランスコーディング リソースを設定する方法の詳細については、第 6 章「メディア リソース」を参照してください。

Advanced Settings Tool を使用して 1 つのコーデックだけを有効にする場合は、Cisco Unity サーバのシステム プロンプトが、使用されるコーデックと同じである必要があります。デフォルトでは、システム プロンプトは G.711 です。コーデックが G.711 に設定されている場合、システム プロンプトは正常に機能します。ただし、G.729 が選択されている場合は、システム プロンプトを変更する必要があります。システム プロンプトを変更する方法の詳細については、http://www.cisco.com で入手可能な『*Cisco Unity Administration Guide*』を参照してください。システム プロンプトが、レジストリで選択されているコーデックと同じでない場合は、エンド ユーザに、理解不能なシステム プロンプトが聞こえます。

Cisco CallManager クラスタとの音声ポート統合

単一サイト メッセージング環境に Cisco Unity を配置する場合、Cisco CallManager クラスタとの統合は SCCP 音声ポートを介して行われます。Cisco CallManager サブスクライバに障害が発生した場合でも（Cisco CallManager フェールオーバー）、ユーザおよび外部コールが引き続き音声メッセージングにアクセスできるように、設計上の考慮事項には、Cisco CallManager サブスクライバ間の音声ポートの適切な配置が含まれる必要があります（図 13-4 を参照してください）。

図 13-4　Cisco CallManager クラスタと統合された Cisco Unity サーバ（専用バックアップ サーバなし）

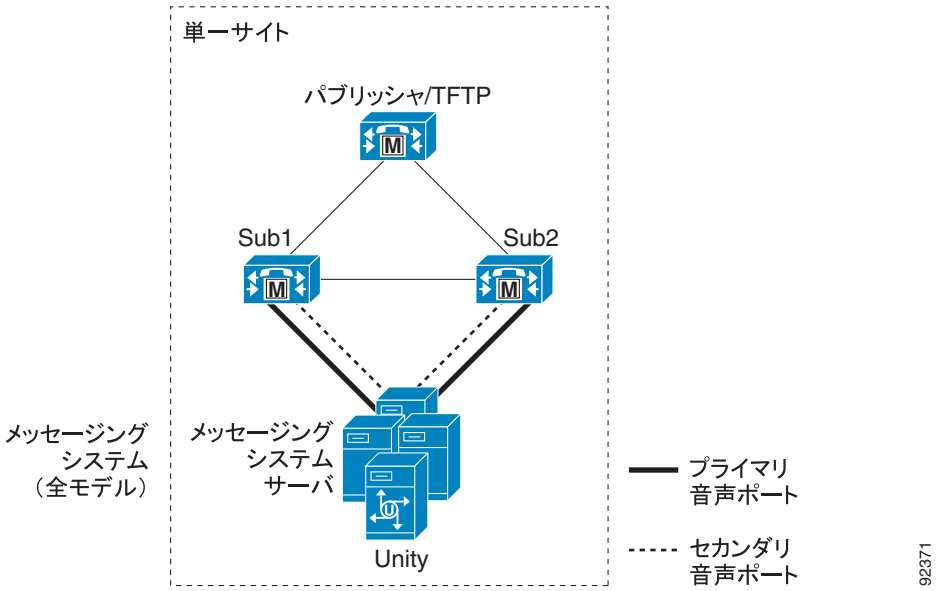


図 13-4 の Cisco CallManager クラスタは、1 対 1 のサーバ冗長性および 50/50 のロード バランシングを採用しています。正常な動作時には、各サブスクライバ サーバがアクティブで、サーバの全コール処理負荷の 50% を処理します。1 台のサブスクライバ サーバに障害が発生すると、残りのサブスクライバ サーバが、障害の発生したサーバの負荷を担います。

図 13-5 と図 13-6 では、Cisco Unity Telephone Integration Manager（UTIM）でのボイスメール ポート設定を示しています。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（図 13-5 を参照してください）。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（図 13-6 を参照してください）。

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 UTIM ユーティリティでポートの 2 つのグループを設定する場合は、必ずデバイス名プレフィックスがグループごとに固有となるようにし、Cisco CallManager Administration でボイスメール ポートを設定するときと同じデバイス名を使用します。図 13-5 および図 13-6 で示しているように、この例で、デバイス名プレフィックスがポートのグループごとに固有になっています。グループ SUB1 ではデバイス名プレフィックスとして CiscoUM1 が使用され、SUB2 では CiscoUM2 が使用されています。

着信ボイスメール ポートと発信ボイスメール ポート（MWI、メッセージ通知、および TRaP 用）の比率に関する設計上の詳細情報については、http://www.cisco.com で入手可能な『*Cisco Unity Design Guide*』を参照してください。

図 13-5　サブスクライバ 1 の音声ポートに関する Cisco Unity の設定

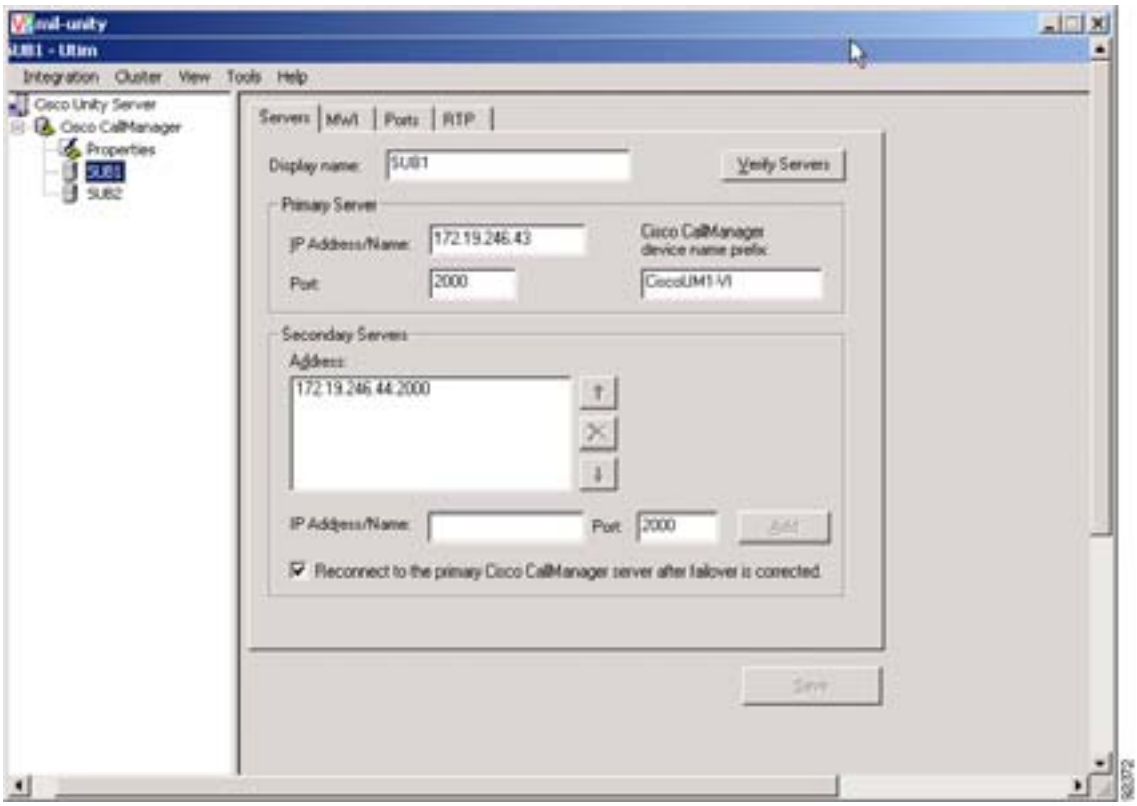
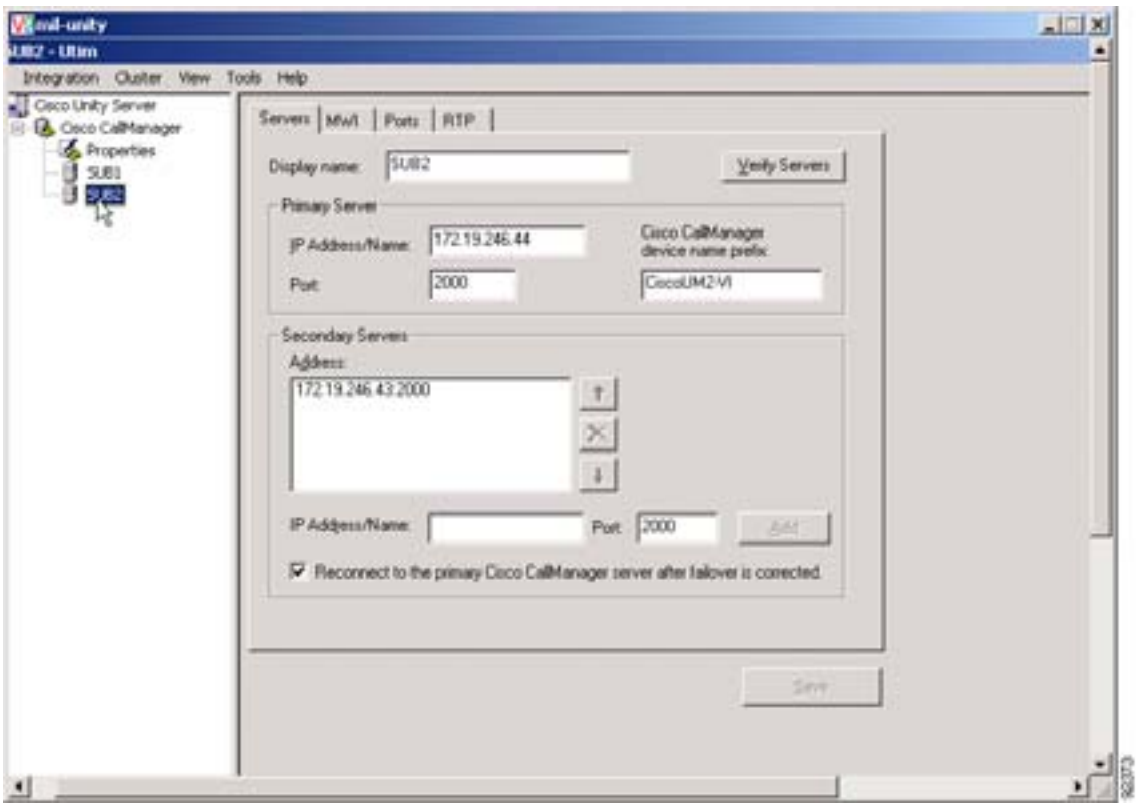


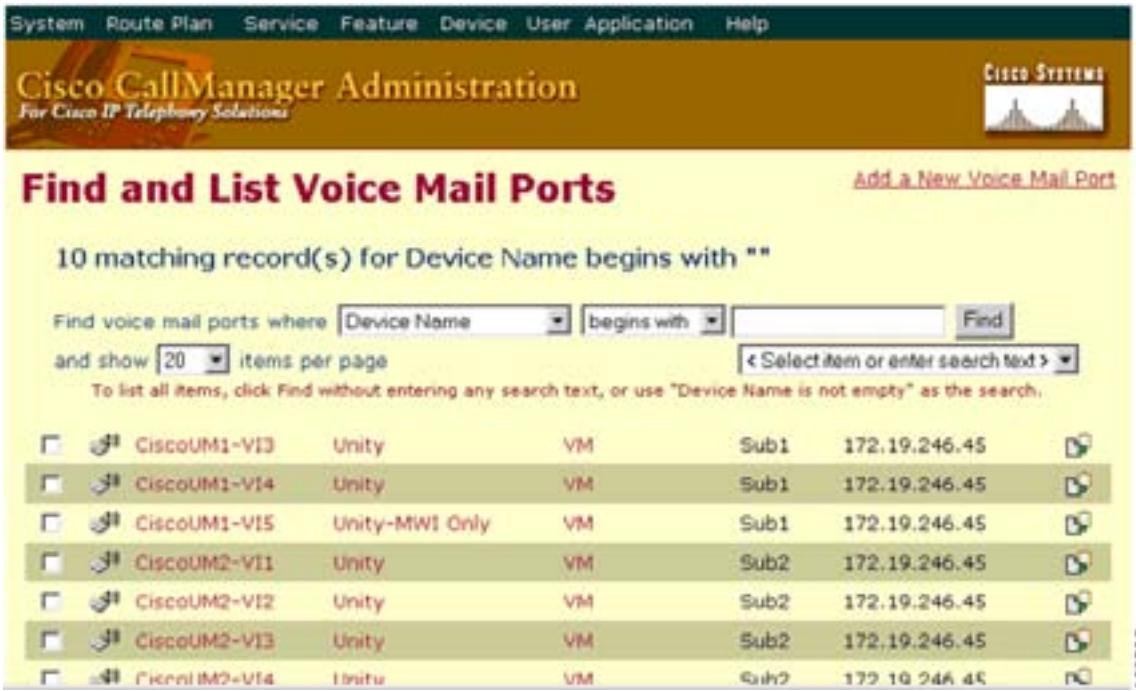
図 13-6　サブスクライバ 2 の音声ポートに関する Cisco Unity の設定



(注)　デバイス名プレフィックスは、ポートのグループごとに固有で、Cisco CallManager Administration に設定されているボイスメール ポートの命名規則と一致する必要があります。

Cisco CallManager Administration では、この例のポートの半分が固有なデバイス名プレフィックス CiscoUM1 を使用して登録されるよう設定され、残りの半分が CiscoUM2 を使用して登録されるよう設定されています（図 13-7 を参照してください）。ポートが Cisco CallManager に登録される場合、半分がサブスクライバ Sub1（図 13-4 を参照）に登録され、残りの半分が Sub2 に登録されます。

図 13-7　Cisco CallManager Release 3.3 以前の Cisco CallManager Administration でのボイスメール ポート設定



(注)　Cisco CallManager Administration でボイスメール ポートに使用される命名規則は、Cisco UTIM で使用されるデバイス名プレフィックスと一致する必要があります。一致しないと、ポートの登録に失敗します。

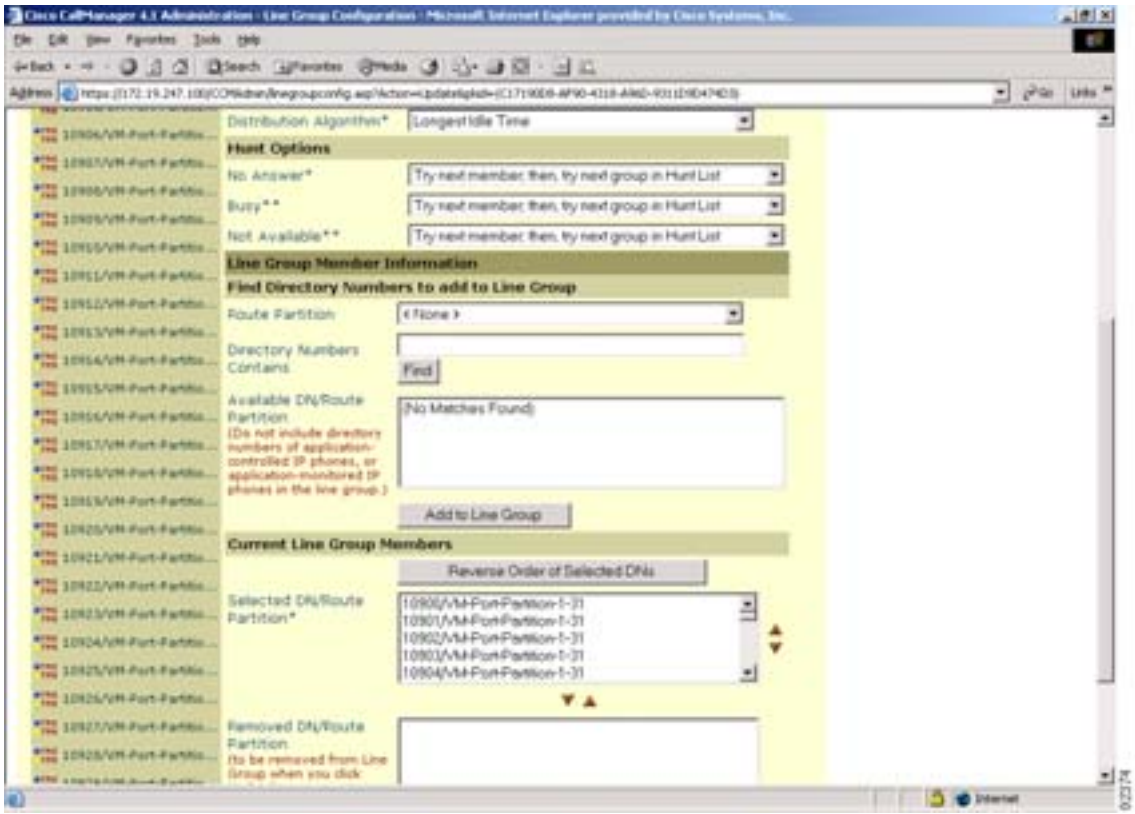
Cisco CallManager の正常な動作時、ボイスメール ポートはビジーである場合も、応答しない場合もあります（たとえば、ボイスメールのメンテナンス中）。Cisco CallManager Release 3.3 以前では、話中転送や無応答時転送などの場合のポートの動作を設定する必要があります。通常は、各ポートが順番に次のポートに転送されます（表 13-1 を参照してください）。この一般的な規則の例外は、MWI 専用ポートの直前のポートです。このポートは次のポート（MWI 専用ポート）を飛ばして、その後のポートに転送されます。たとえば、表 13-1 では、CiscoUM1-VI4（DN 1003）が CiscoUM2-VI1（DN 1005）に転送されることを示しています。MWI 専用ポートでない最後のポートは、最初のポートに戻って転送されるため、循環が完成します。最適なパフォーマンスを得るため、MWI 専用ポートの数を音声ポートの合計数の 25% 以下に制限し、他のすべてのポート上で MWI 機能を無効にしてください。

表 13-1　Cisco CallManager Release 3.3 以前での話中転送状態と無応答時転送状態に対する一般的なボイスメール ポート設定

音声ポート名	ディレクトリ番号	話中転送	無応答時転送
CiscoUM1-VI1	1000	1001	1001
CiscoUM1-VI2	1001	1002	1002
CiscoUM1-VI3	1002	1003	1003
CiscoUM1-VI4	1003	1005	1005
CiscoUM1-VI5	1004	MWI 専用ポート	
CiscoUM2-VI1	1005	1006	1006
CiscoUM2-VI2	1006	1007	1007
CiscoUM2-VI3	1007	1008	1008
CiscoUM2-VI4	1008	1001	1001
CiscoUM2-VI5	1009	MWI 専用ポート	

Cisco CallManager Release 4.0 では、ボイスメール ポートの設定方法と動作方法を大きく変える新機能が導入されました。Release 4.0 以降では、回線グループ、ハント リスト、およびハント パイロットを使用して、ボイスメール ポートがアベイラビリティ、使用状況、および状態に基づいて相互に転送を行う方法を指定します。ボイスメール ポートのハント方法を設定する場合は、Current Line Group Members リストから MWI ポートをすべて削除します（図 13-8 を参照してください）。これにより、これらのポートがコール応答用のハント グループから外れて、MWI アクティビティのために確保されることが保証されます。さらに、Cisco UTIM ユーティリティを使用して MWI ポートがコールに応答しないように設定する必要があるため、回線グループからこれらのポートを削除すると、ボイスメールにアクセスするユーザが ring-no-answer 状態を受信しないことが保証されます。回線グループ、ハント リスト、およびハント パイロットの詳細については、http://www.cisco.com で入手可能な Release 4.0 以降の『*Cisco CallManager Administration Guide*』を参照してください。

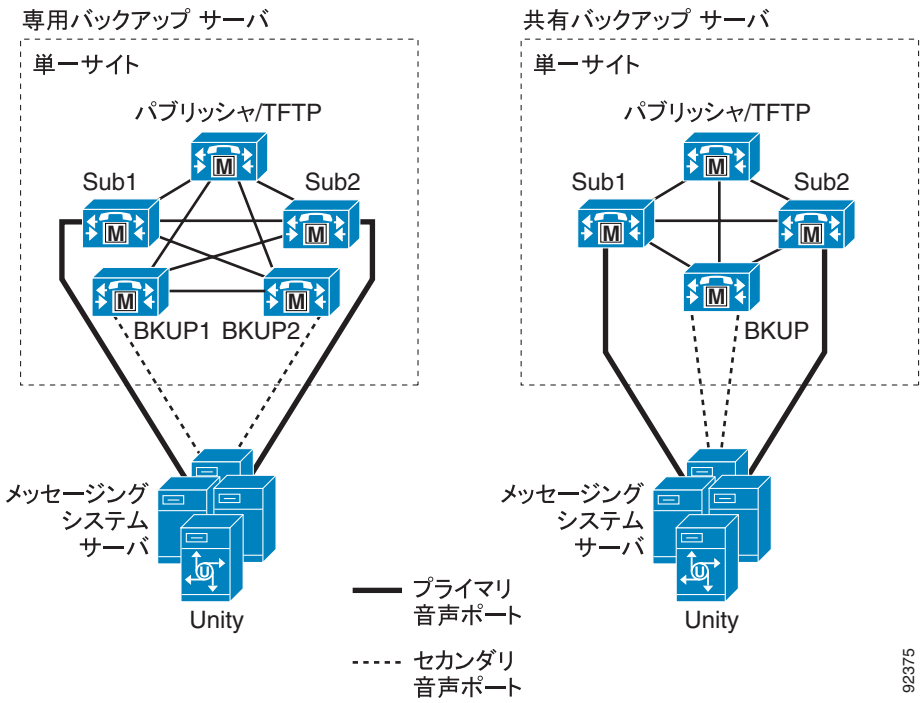
図 13-8　Cisco CallManager Release 4.0 以降の Cisco CallManager Administration での回線グループ設定



専用 Cisco CallManager バックアップ サーバを使用する音声ポート統合

この Cisco CallManager クラスタ構成では、各サブスクライバ サーバが 50% を超えるコール処理負荷で動作できます。各プライマリ サブスクライバ サーバは、専用バックアップ サーバまたは共有バックアップ サーバを持ちます（図 13-9 を参照してください）。正常な動作時、バックアップ サーバはコールを処理しません。サブスクライバ サーバの障害時またはメンテナンス時に、バックアップ サーバはそのサブスクライバ サーバのすべての負荷を担います。

図 13-9　単一の Cisco CallManager クラスタと統合された Cisco Unity サーバ（バックアップ サブスクライバ サーバを使用）

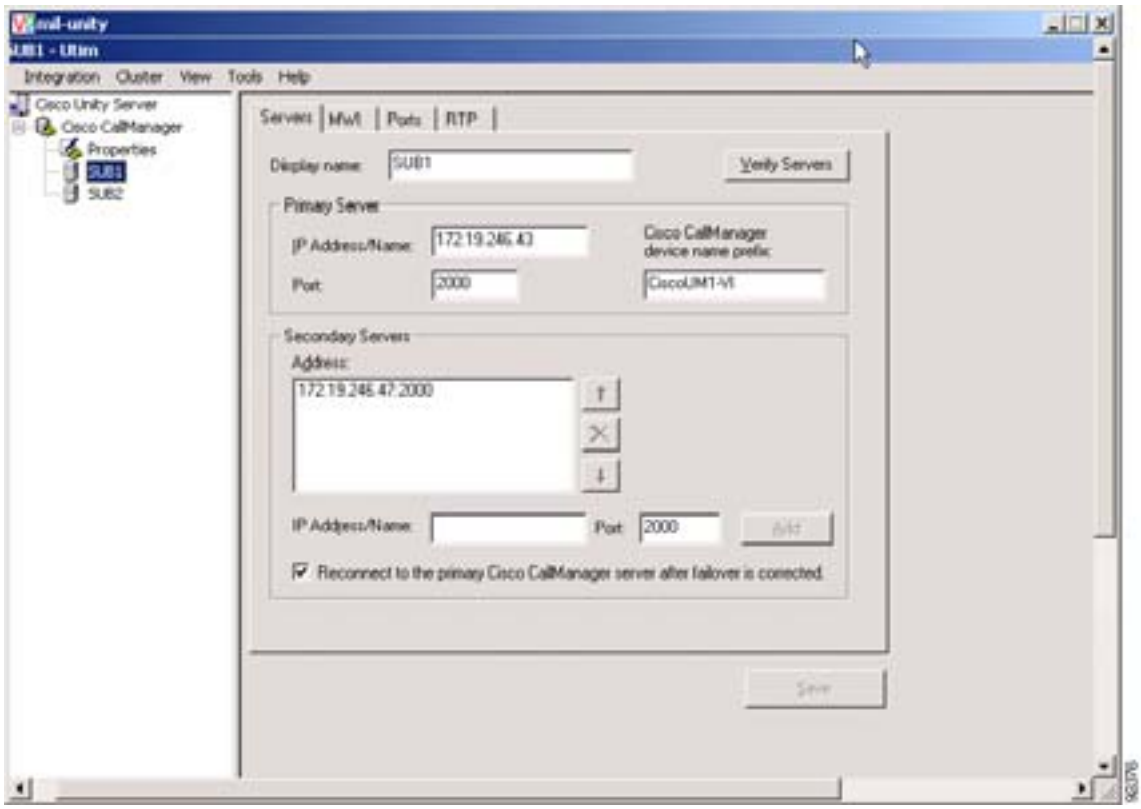


この場合のボイスメール ポートの設定は、50/50 のロードバランシング クラスタに似ています。ただし、もう 1 台のサブスクライバ サーバをセカンダリ サーバとして使用するように音声ポートを設定せず、個別の共有バックアップ サーバまたは専用バックアップ サーバを使用します。共有バックアップ サーバと共にクラスタ化された Cisco CallManager では、両方のサブスクライバ サーバのセカンダリ ポートが、単一のバックアップ サーバを使用するように設定されます。

音声ポート名（デバイス名プレフィックス）は、Cisco UTIM グループごとに固有で、Cisco CallManager サーバ上で使用されるデバイス名と同じである必要があります。

この例の設定では、Cisco UTIM ユーティリティでボイスメール ポートの 2 つのグループを設定します。Secondary Servers ボックスには、バックアップ サーバの IP アドレスまたは DNS 名を指定します（図 13-10 を参照してください）。クラスタが共有バックアップ サーバを持つ場合は、両方のグループで同じサーバが使用されます。音声ポートを設定する場合は、両方のポート グループに、同じ数の MWI 専用ポートとフル機能の音声ポートが存在するようにしてください。また、Audio Messaging Interchange Specification（AMIS）および TRaP の音声ポートを 2 つのグループに等しく分散させることも必要です。表 13-1 に示しているように、話中転送および無応答時転送用のポートを設定します。

図 13-10　バックアップ サーバ（Bkup1）をセカンダリとするサブスクライバ サーバ（Sub1）の音声ポートに関する Cisco UTIM 設定画面



サービスの復元後に音声ポートがサブスクライバ サーバに再接続されるようにするには、「Reconnect to the primary Cisco CallManager server after failover is corrected.」というラベルのボックスをオンにします。

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、Cisco Unity サーバが Cisco CallManager クラスタと同じ場所に置かれますが、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とリモートの両方にあります（図 13-11 を参照してください）。リモート ユーザが中央のサイトのリソース（Tail-End Hop-Off（TEHO; テールエンド ホップオフ）の場合と同様に、音声ポート、IP Phone、公衆網ゲートウェイなど）にアクセスする場合、そのコールはゲートキーパー コール アドミッション制御にとって透過的になります。したがって、Cisco CallManager でリージョンとロケーションを設定して、コール アドミッション制御を提供する必要があります。（P.13-6 の「帯域幅の管理」を参照してください）。IP Phone または MGCP ゲートウェイにリージョン間コールを発信する場合、IP Phone は設定済みのリージョン間コーデックを自動的に選択します。ネイティブ トランスコーディングが無効である場合、Cisco Unity 音声ポートは、WAN を通過する（リージョン間）コールのために Cisco CallManager トランスコーディング リソースを要求します。

図 13-11　集中型メッセージングと集中型コール処理

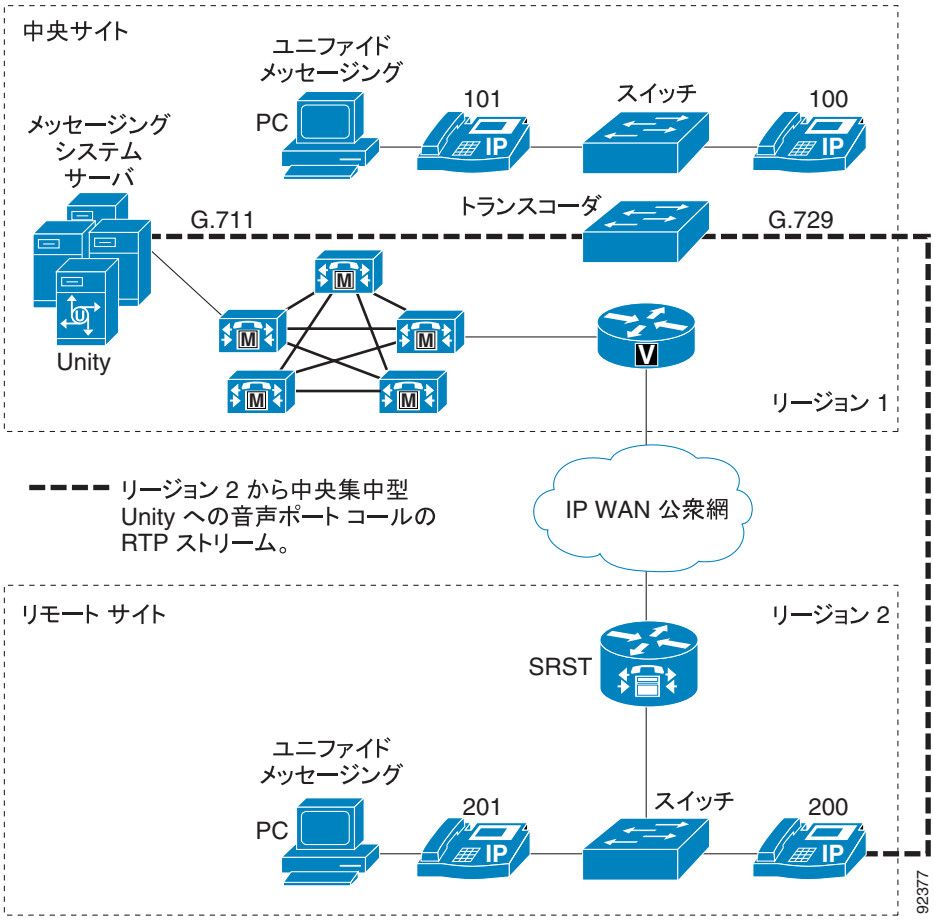


図 13-11 では、リージョン 1 と 2 が、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。Cisco Unity サーバ上でネイティブ トランスコーディングは無効になっています。

図 13-11 で示しているように、内線番号 200 からリージョン 1 のボイスメール ポートにコールが発信されると、エンドポイントではリージョン間の G.729 コーデックが使用されますが、RTP ストリームがトランスコードされ、音声ポート上では G.711 が使用されます。この例では、Cisco Unity サーバ上のネイティブ トランスコーディングが無効になっています。Cisco CallManager トランスコーディング リソースは、ボイスメール システムと同じサイトに置く必要があります。

ヘアピン

考慮する必要のあるもう 1 つの問題は、複数の Cisco Unity 音声ポートを介する音声コールのヘアピン（トロンボーニング）です。ヘアピンは、SCCP TSP 音声ポートだけを使用する環境では問題ではありませんが、二重統合環境では問題になります。二重統合環境では、従来型のシステムの音声ポートと SCCP TSP 音声ポートの間でヘアピンが発生する可能性があります。

二重統合の詳細については、次の Web サイトで入手可能な『*Cisco Unity Administration Guide*』を参照してください。

http://www.cisco.com

分散型メッセージングと集中型コール処理

分散型メッセージングは、テレフォニー環境内に複数のメッセージング システムが分散されており、各メッセージング システムがローカル メッセージング クライアントだけにサービスを提供することを意味します。このモデルは集中型メッセージングとは異なります。集中型メッセージングでは、メッセージング システムに対してローカルなクライアントとリモートのクライアントの両方が存在します。図 13-12 では、集中型コール処理を使用する分散型メッセージング モデルを示しています。他のマルチサイト コール処理モデルと同様に、WAN 帯域幅を管理するためにリージョンとロケーションを使用する必要があります。このモデルでは、Cisco Unity ネイティブ トランスコーディングを無効にすることも必要です。

図 13-12　分散型メッセージングと集中型コール処理

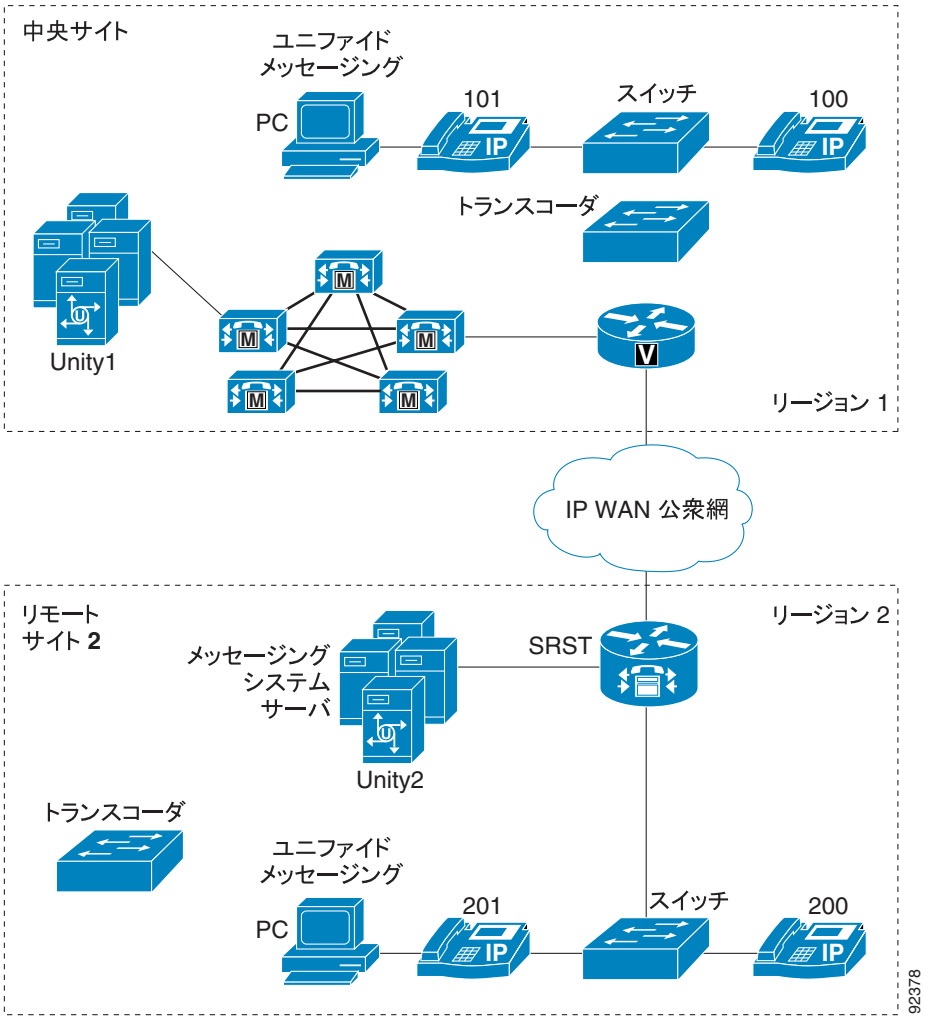


図 13-12 の構成では、トランスコーダ リソースが各 Cisco Unity メッセージ システム サイトに対してローカルである必要があります。リージョン 1 と 2 は、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。Cisco Unity サーバ上でネイティブ トランスコーディングは無効になっています。

Cisco CallManager サーバに設定されているコーリング サーチ スペースとデバイス プールによって、両方の Cisco Unity サーバの音声メッセージング ポートに、適切なリージョンとロケーションが割り当てられる必要があります。さらに、テレフォニー ユーザをボイスメール ポートの特定のグループに関連付けるために、Cisco CallManager ボイスメール プロファイルを設定する必要があります。コーリング サーチ スペース、デバイス プール、およびボイスメール プロファイルを設定する方法の詳細については、次の Web サイトで入手可能な、該当するバージョンの『*Cisco CallManager Administration Guide*』を参照してください。

http://www.cisco.com

メッセージング システムは相互に「ネットワーク接続」され、内部ユーザと外部ユーザの両方に単一のメッセージング システムを提供します。分散 Unity サーバ向けの Cisco Unity ネットワーク機能については、次の Web サイトで入手可能な『*Networking in Cisco Unity Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html

結合されたメッセージング配置モデル

複数のメッセージング モデルを同じ配置で組み合わ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 13-13 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 13-13　結合された配置モデル

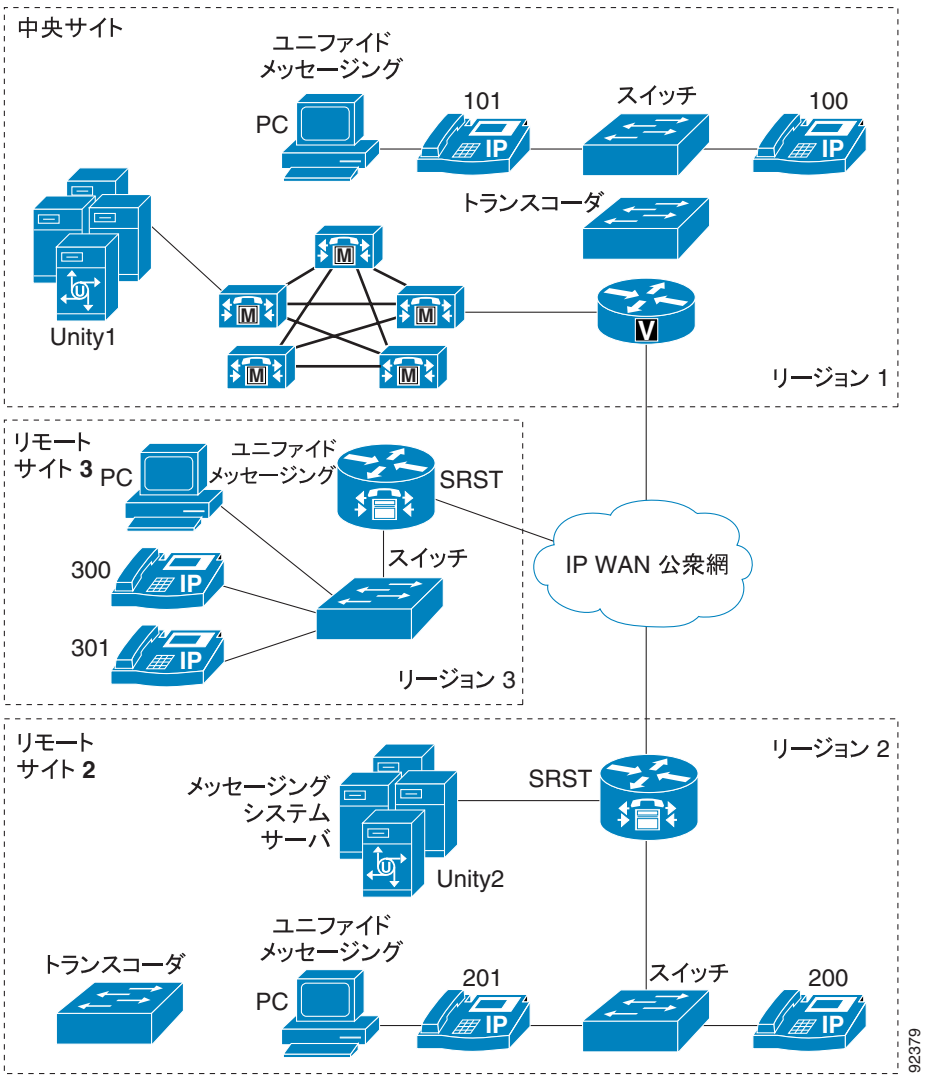


図 13-13 では、2 つのメッセージング モデルの結合を示しています。リージョン 1 と 3 は集中型メッセージングと集中型コール処理を使用し、リージョン 2 は分散型メッセージングと集中型コール処理を使用しています。すべてのリージョンが、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。

図 13-13 では、中央サイトとサイト 3 の間で、集中型メッセージングと集中型コール制御が使用されています。中央サイトのメッセージング システムは、中央サイトとサイト 3 の両方のクライアントにメッセージング サービスを提供します。サイト 2 は、集中型コール処理を使用する分散型メッセージング モデルを使用しています。サイト 2 に置かれているメッセージング システム（Unity2）は、サイト 2 の中にいるユーザだけにメッセージング サービスを提供します。この配置では、両方

のモデルが、この章に記載されているそれぞれの設計上のガイドラインに従っています。トランスコーディング リソースは各メッセージング システム サイトに対してローカルに置かれ、サイト 2 のユーザが中央サイトのユーザにメッセージを残す場合のように、（メッセージング システムに対して）リモートのサイトからメッセージング サービスにアクセスするクライアントをサポートします。

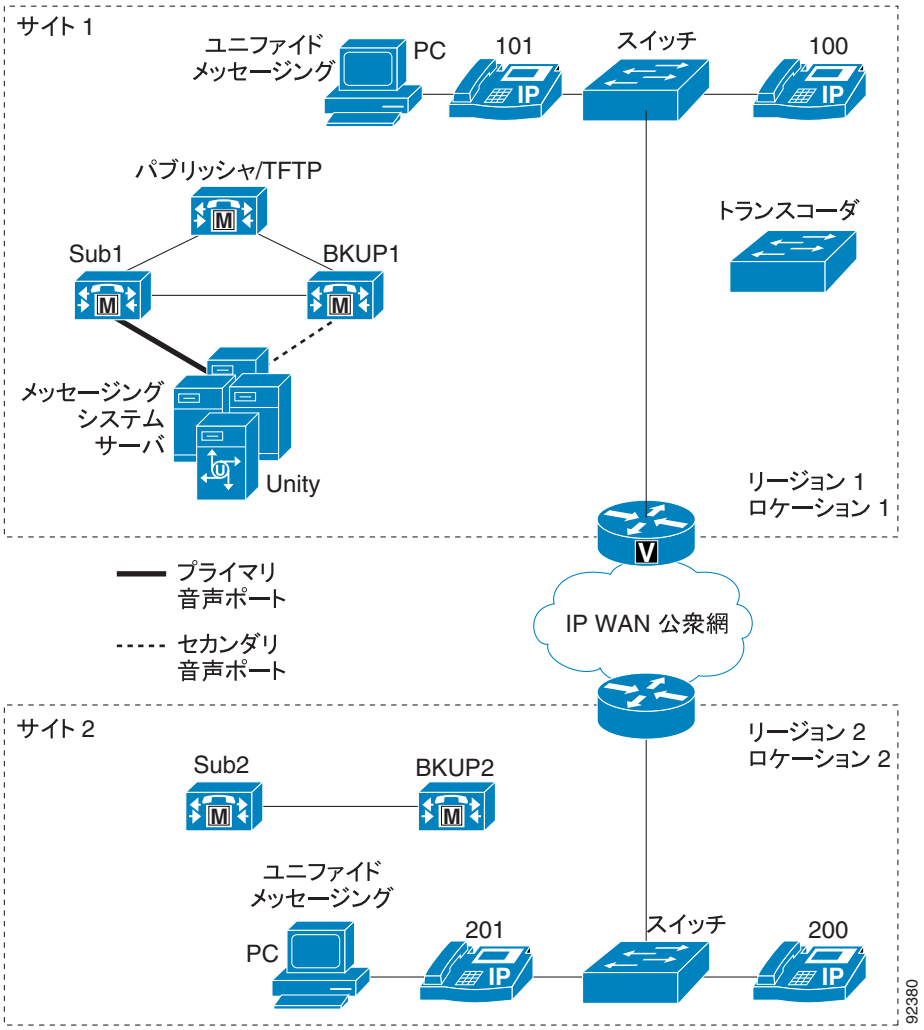
集中型メッセージングと WAN を介したクラスタ化

ここでは、集中型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介した Cisco CallManager クラスタ化を一緒に配置する場合の Cisco Unity の設計上の問題について説明します。このモデルで WAN に障害が発生した場合は、WAN が復元されるまで、すべてのリモート メッセージング サイトがボイスメール機能を失います（図 13-14 を参照してください）。

WAN を介したクラスタ化は、ローカル フェールオーバーをサポートしています。ローカル フェールオーバーでは、各サイトが、物理的にそのサイトに置かれているバックアップ サブスクライバ サーバを持ちます。ここでは、Cisco Unity 集中型メッセージングと、WAN を介したクラスタ化のローカル フェールオーバーを一緒に配置する方法を中心に説明します。

詳細については、P.2-17 の「IP WAN を介したクラスタ化」の項を参照してください。

図 13-14　Cisco Unity 集中型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介したクラスタ化



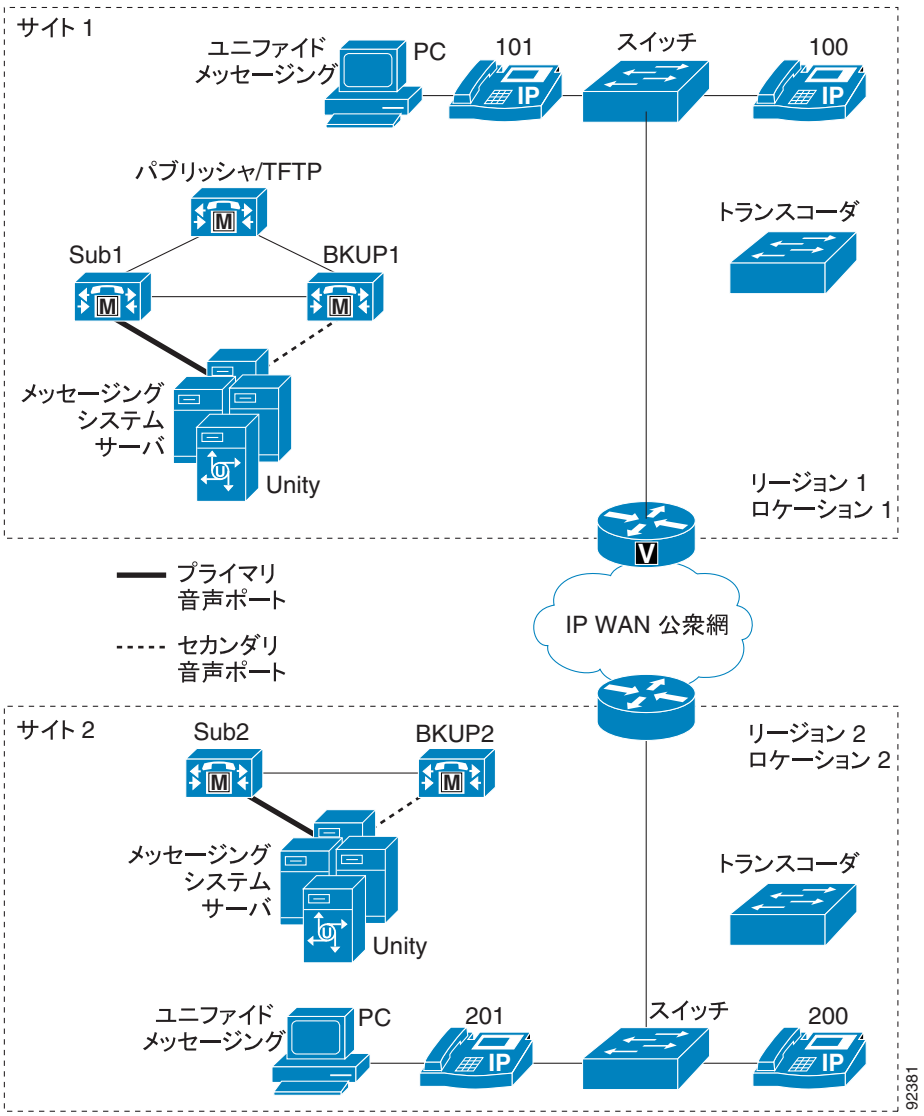
クラスタ サイト間で必要な最小帯域幅は T1 回線（1,544 MHz）です。この量の帯域幅で、最大 10,000 の Busy Hour Call Attempts（BHCA: 混雑時発呼）に対してシグナリング トラフィックおよびデータベース トラフィックをサポートできます。ただし、これには、必要なメディア帯域幅が含まれていません。

Cisco CallManager Release 3.3(3) 以前を使用する WAN を介したクラスタ化では、クラスタごとに最大 4 つのサイトをサポートしますが、Cisco CallManager Release 4.1 以上では最大 8 つのサイトをサポートします。Cisco Unity は、どちらの場合でもその最大数までサイトをサポートします。ボイスメール ポートは、Cisco Unity メッセージング システムが置かれているサイトだけに設定されます（図 13-14 を参照してください）。ボイスメール ポートは、WAN を介してリモート サイトに登録されません。他のサイトのメッセージング クライアントは、プライマリ サイトのすべてのボイスメール リソースにアクセスします。WAN に障害が発生すると、リモート サイトは集中型メッセージング システムにアクセスできなくなるため、WAN を介してリモート サイトに音声ポートを設定してもメリットがありません。帯域幅を考慮して、ボイスメール ポートで TRaP を無効にし、すべてのメッセージング クライアントがそのローカル PC（ユニファイド メッセージング専用）にボイスメール メッセージをダウンロードするようにする必要があります。

分散型メッセージングと WAN を介したクラスタ化

Cisco Unity メッセージング サーバも配置されたローカル フェールオーバー サイトでは、集中型メッセージング モデルと同様に、音声ポートがローカル Cisco CallManager サブスクライバ サーバに登録されます。音声ポートの設定については、P.13-9 の「Cisco CallManager クラスタとの音声ポート統合」および P.13-15 の「専用 Cisco CallManager バックアップ サーバを使用する音声ポート統合」を参照してください。

図 13-15　Cisco Unity 分散型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介したクラスタ化



WAN を介したクラスタ化を含む単純分散型メッセージング実装では、クラスタ内の各サイトに、独自の Cisco Unity メッセージング サーバとメッセージング インフラストラクチャ コンポーネントが置かれます。すべてのサイトにローカル Cisco Unity メッセージング システムが置かれるわけではなく、一部のサイトで、ローカル メッセージング クライアントがリモート メッセージング サーバを使用する場合、その配置は分散型メッセージングと集中型メッセージングの結合モデルとなり

ます（P.13-21 の「結合されたメッセージング配置モデル」を参照してください）。このモデルで WAN に障害が発生した場合は、WAN が復元されるまで、集中型メッセージングを使用するすべてのリモート サイトがボイスメール機能を失います。

ローカル メッセージング サーバを持たない各サイトは、そのすべてのメッセージング クライアントに対して単一のメッセージング サーバを使用する必要がありますが、そのようなサイトのすべてが同じメッセージング サーバを使用する必要はありません。たとえば、サイト 1 とサイト 2 のそれぞれがローカル メッセージング サーバを持っているとします。その場合、サイト 3 のすべてのクライアントがサイト 2 のメッセージング サーバを使用し（そのメッセージング サーバに登録し）、サイト 4 のすべてのクライアントがサイト 1 のメッセージング サーバを使用するようにすることができます。ローカル Cisco Unity メッセージング サーバを持つサイトには、トランスコーダ リソースが必要です。

他の分散型コール処理配置と同様に、これらのサイト間のコールはゲートキーパー コール アドミッション制御にとって透過的です。したがって、Cisco CallManager でリージョンとロケーションを設定してコール アドミッション制御を提供する必要があります（P.13-6 の「帯域幅の管理」を参照してください）。

分散 Cisco Unity サーバは、デジタルでネットワーク接続することもできます。このトピックの詳細については、http://www.cisco.com で入手可能な『*Cisco Unity Networking Guide*』を参照してください。配置される特定のメッセージング ストアに固有の Networking Guide が用意されています。

Cisco Unity メッセージング フェールオーバー

Cisco Unity フェールオーバーにより、Cisco Unity サーバに障害が発生した場合のボイスメール存続可能性が確保されます（図 13-1 を参照してください）。Cisco Unity ローカル フェールオーバーでは、プライマリとセカンダリの両方の Unity メッセージング サーバが同じ物理ロケーションに存在し、メッセージング インフラストラクチャ コンポーネントがプライマリ サーバと同じ場所に置かれます。メッセージング インフラストラクチャ コンポーネント（メッセージング ストア サーバ、Domain Controller/Global Catalog（DC/GC; ドメイン コントローラ / グローバル カタログ）サーバ、DNS サーバなど）は、オプションで、冗長コンポーネントを持つこともできます。これらは、Cisco Unity セカンダリ サーバと物理的に同じ場所に置くことができます。

Cisco Unity フェールオーバーは、すべてのメッセージング配置モデルでサポートされています。

Cisco Unity フェールオーバーの設定については、次の Web サイトで入手可能な『*Cisco Unity Failover Configuration and Administration Guide*』を参照してください。

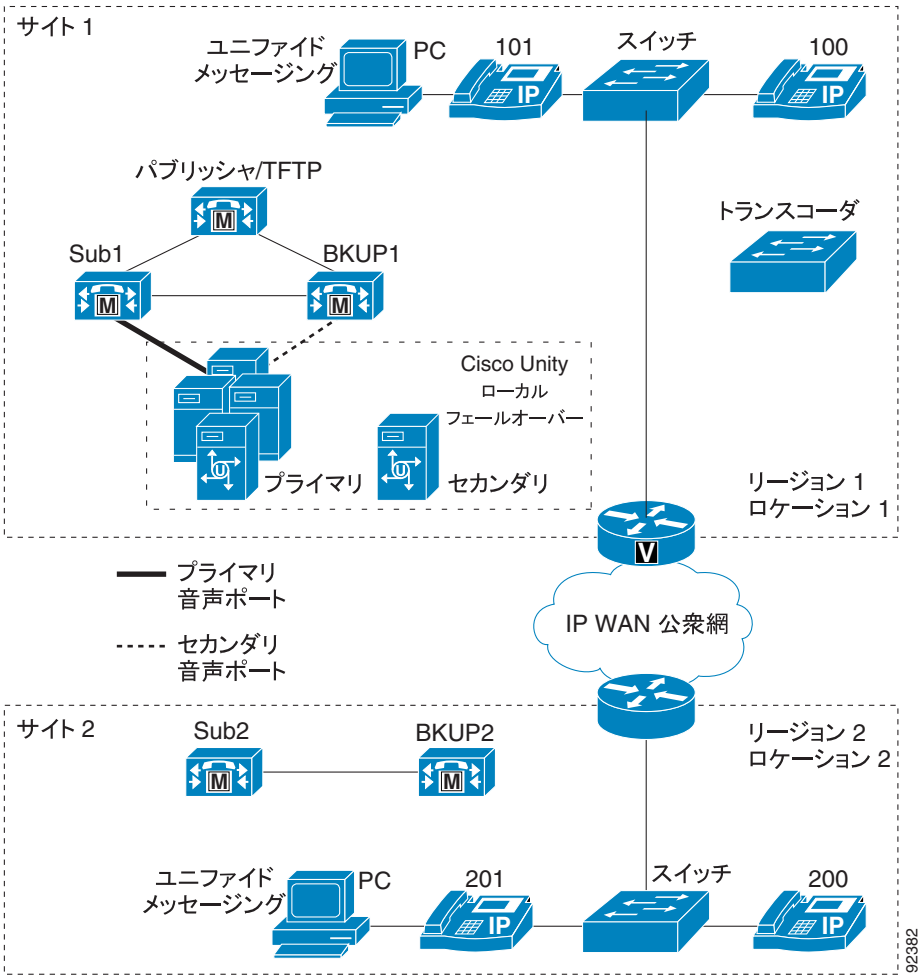
http://www.cisco.com

Cisco Unity フェールオーバーと WAN を介したクラスタ化

Cisco Unity ローカル フェールオーバーと WAN を介したクラスタ化を配置する場合は、P.13-23 の「集中型メッセージングと WAN を介したクラスタ化」および P.13-25 の「分散型メッセージングと WAN を介したクラスタ化」で説明している設計プラクティスを適用します。正常な動作時、プライマリ Cisco Unity サーバからの音声ポートは WAN を通過しません。

図 13-16 では、Cisco Unity ローカル フェールオーバーを示しています。プライマリ Cisco Unity サーバとセカンダリ Cisco Unity サーバの両方が物理的に同じサイトに置かれていることに注意してください。Cisco Unity フェールオーバーは、Cisco CallManager の WAN を介したクラスタ化で使用可能な最大数までリモート サイトをサポートします。

図 13-16　Cisco Unity ローカル フェールオーバーと WAN を介したクラスタ化



Cisco Unity フェールオーバーの設定については、次の Web サイトで入手可能な『*Cisco Unity Failover Configuration and Administration Guide*』を参照してください。

http://www.cisco.com

集中型メッセージングと複数の Cisco CallManager サーバ

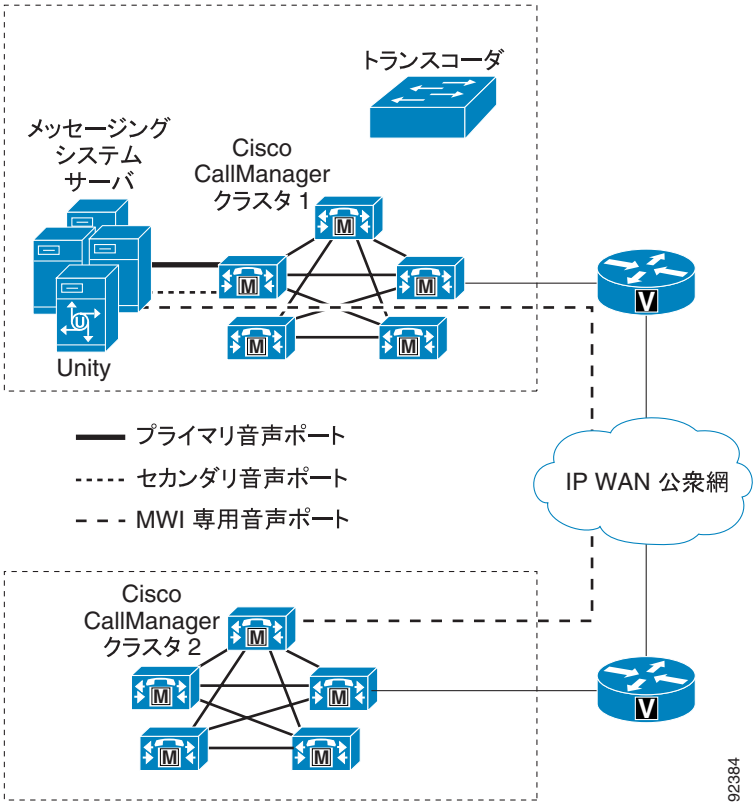
このモデルでは、Cisco Unity メッセージング サーバと同じ場所にある Cisco CallManager クラスタ（図 13-17 ではクラスタ 1）にフル機能の音声ポートと MWI ポートを設定し、リモート Cisco CallManager クラスタ（図 13-17 ではクラスタ 2）に MWI 専用ポートを割り当てます。ボイスメール コールがクラスタ 1 とクラスタ 2 の間の WAN を通過する場合は、必ずトランスコーディング リソースが必要になります。このリソースは、Cisco Unity メッセージング サーバと同じ場所に置く必要があります。Cisco CallManager のトランスコーディング リソースを使用するために、Cisco Unity サーバのネイティブ トランスコーディングを無効にする必要があります。

図 13-17 では、Cisco CallManager クラスタ 2 に MWI 専用のボイスメール ポートが設定されています。テレフォニー加入者が Cisco CallManager クラスタ 1 のボイスメール ポートにアクセスするようにするには、パイロット番号を DN 以外にして、その番号がルート パターンによってルーティングされるようにする必要があります。2 つのクラスタ間でクラスタ間トランクが設定されると、そのクラスタ間トランクを介してボイスメール パイロットをルーティングできます。ルート パターンが使用されるため、ゲートキーパーのコール アドミッション制御を使用でき、WAN 帯域幅を適切に管理できます。

図 13-17 には、次の設定情報が適用されます。

クラスタ 1	クラスタ 2
内線番号：2000 ～ 2999	内線番号：12000 ～ 12999
ボイスメール ポート：4	ボイスメール ポートなし
MWI 専用ポート：1	MWI 専用ポート 1
ポート DN：2200 ～ 2205	ポート DN：14000
MWI オン / オフ DN：それぞれ 2249 と 2250	MWI オン / オフ DN：それぞれ 2249 と 2250
シスコ ポート：1 ～ 5	シスコ ポート：6
ボイスメール パイロット：2200	ボイスメール パイロット：82000（ルート パターンは 8 を削除し、G.729 でゲートキーパー制御トランクを介してパイロット番号を送信）

図 13-17　複数のクラスタにサービスを提供する単一の Cisco Unity サーバ



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 メッセージング インフラストラクチャを使用します。

単一の Cisco Unity を複数の Cisco CallManager クラスタと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 White Paper『*Cisco Unity Integration with Multiple Clusters of Cisco CallManager 3.1 and Later*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/whitpapr/clust_31.htm

CHAPTER 14

ディレクトリ アクセスとディレクトリ統合

ディレクトリ（電話帳）は、多数の読み取りや検索、および随時の書き込みや更新用に最適化される特殊なデータベースです。ディレクトリには、一般に、社員の情報、企業ネットワークでのユーザ特権など、頻繁に変更されないデータが保存されます。

ディレクトリのもう 1 つの面は、拡張可能であることです。つまり、ディレクトリに保存される情報のタイプを変更し、拡大することが可能です。ディレクトリ スキーマという語は、保存されている情報のタイプ、および情報の規則を指します。多くのディレクトリは、さまざまなアプリケーションによって定義される情報タイプに対応するために、ディレクトリ スキーマを拡張する方法を備えています。この機能により、企業は、ディレクトリをユーザ情報の中央リポジトリとして使用できます。

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、複数のアプリケーションから利用できるすべてのユーザ情報を、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 CallManager と社内 LDAP ディレクトリを統合する場合の、設計上の主な原則について説明しています。また、Cisco IP Phone や Cisco IP SoftPhone などの Cisco IP テレフォニー エンドポイントに、社内 LDAP ディレクトリへのアクセスを提供する場合の、設計上の考慮事項についても説明しています。この章の構成は、次のとおりです。

この章で説明する考慮事項は、Cisco CallManager、および Cisco CallManager にバンドルされているエクステンション モビリティ、IP Management Assistant、Web Dialer、Bulk Administration Tool、Real-Time Monitoring Tool、およびマルチレベル管理という各アプリケーションに適用されます。

その他のシスコ音声アプリケーションについては、次の Web サイトで入手可能なそれぞれの製品資料を参照してください。

http://www.cisco.com

特に、Cisco Unity については、『*Cisco Unity Design Guide*』、および『*Cisco Unity Data and the Directory*』、『*Active Directory Capacity Planning*』、『*Cisco Unity Data Architecture and How Cisco Unity Works*』の各 White Paper を参照してください。

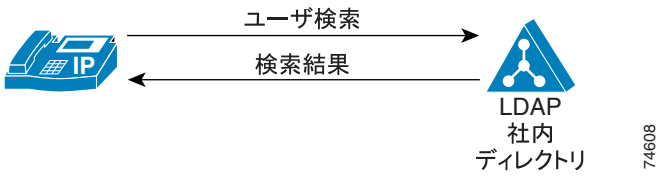
ディレクトリ アクセスとディレクトリ統合との比較

この項では、次の定義が適用されます。

- ディレクトリ アクセスとは、Cisco IP Phone や Cisco IP SoftPhone などの Cisco IP テレフォニー エンドポイントが、社内 LDAP ディレクトリにアクセスする機能のことです。
- ディレクトリ統合とは、Cisco CallManager などのアプリケーションが、独自の組み込みデータベースの替わりに、中央の社内 LDAP ディレクトリに、ユーザ関連情報を保存する機能のことです。

図14-1 では、この章で定義されるディレクトリ アクセスを示しています。この例では、Cisco IP Phone からアクセスしています。クライアント アプリケーションは、企業の社内ディレクトリなどの LDAP ディレクトリに対してユーザ検索を実行し、一致するエントリを受け取ります。ユーザ検索に対して 1 つのエントリが選択され、エントリは Cisco IP Phone から検索されたユーザにダイヤルするために使用されます。

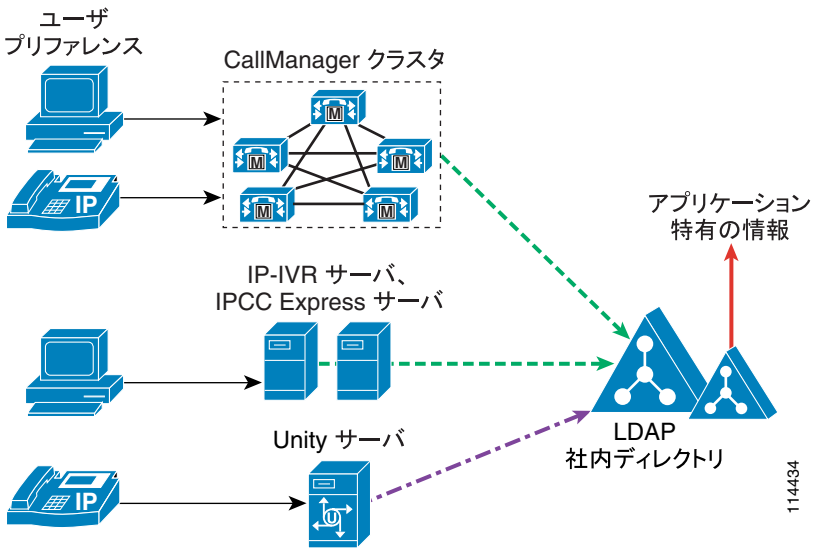
図 14-1　Cisco IP テレフォニー エンドポイントのディレクトリ アクセス



ここで定義しているディレクトリ アクセスには、ディレクトリに対する読み取り操作だけが含まれるため、ディレクトリ スキーマの拡張や他の設定変更は不要であることに注意してください。

一方、複数のアプリケーションと 1 つの社内ディレクトリを統合するディレクトリ統合は、これらのアプリケーションが、独自の個別の組み込みデータベースを使用するのではなく、中央ディレクトリにユーザ関連情報を保存することを意味します。図 14-2 では、この章で定義されるディレクトリ統合の例を示しています。

図 14-2　Cisco IP テレフォニー アプリケーションのディレクトリ統合



ディレクトリ統合には、ディレクトリに対する読み取り操作と書き込み操作が含まれるため、社内 LDAP ディレクトリに対するスキーマの拡張や他の設定変更が必要になることに注意してください。

デフォルトでは、Cisco CallManager は、組み込み LDAP ディレクトリに、ユーザ情報（たとえば、ユーザが制御するデバイス、個人用アドレス帳のエントリなど）を保存します。しかし、通常、電子メール アドレス、オフィスの住所、および役職などの一般的な社員情報を保存するために使用される社内 LDAP ディレクトリに、Cisco CallManager を統合することもできます。この場合、Cisco CallManager は、独自の組み込みディレクトリを使用しなくなり、社内ディレクトリにアプリケーション特有のユーザ情報を保存します。

（注） Cisco CallManager Release 3.1 では、ディレクトリ統合は、Microsoft Active Directory（AD）2000 および Netscape Directory Server Release 4.*x* でサポートされています。Cisco CallManager Release 3.3(2) で iPlanet/Sun Directory Server 5.1 のサポートが追加され、Cisco CallManager Releases 3.3(3) および 4.0(1)sr2 で Microsoft Active Directory（AD）2003 のサポートが追加されました。

Cisco CallManager などのアプリケーションと社内ディレクトリを統合することには、単にエンドポイントにディレクトリ アクセスを提供すること以外に、次のような意味もあります。

- 社内ディレクトリにアプリケーション固有のユーザ属性を保存するには、ディレクトリ スキーマを拡張する必要があります。この操作は複雑なので、操作の際には、ディレクトリ構造を十分に理解している必要があります。
- アプリケーションはいつでもディレクトリと交信できる必要があり、ディレクトリは適切な応答時間を実現する必要があります。ディレクトリ サービスのアベイラビリティは、アプリケーションの機能に影響を与える場合があります。
- データ保存と、読み取りと書き込み照会によって、ディレクトリに不必要な負荷がかかります。新しいサービスまたはアプリケーションを導入する場合は、サーバのオーバーサブスクリプションを避けるために、慎重な計画とサイジングをお勧めします。

複数のアプリケーションにわたるディレクトリ統合には多くの利点がありますが、ディレクトリ統合が及ぼす影響をすべて理解し、個々の配置ごとにビジネスのニーズを確認することが重要です。

Cisco 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

Cisco CallManager やその他の IP テレフォニー アプリケーションが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。どちらの場合も、エンドユーザからは同じように見えます。これは、相違点によって影響を受けるのは、アプリケーションがユーザ情報を保存する方法と、ネットワーク上でこの情報の一貫性が保持される方法だけであるためです。

次の各項では、XML 対応電話機（Cisco IP Phone モデル 7940、7960 など）に対して、任意の LDAPv3 準拠ディレクトリ 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概説します。

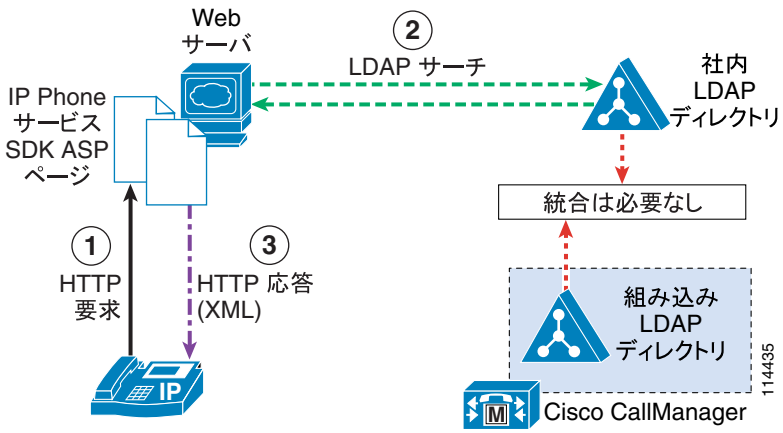
（注）　Cisco IP SoftPhone Release 1.2 以降には、Cisco IP Communicator と同様、LDAP ディレクトリにアクセスして検索するメカニズムが組み込まれています。この機能の設定方法の詳細は、製品資料を参照してください。

Cisco IP Phone のディレクトリ アクセス

XML 対応の Cisco IP Phone（モデル 7940 や 7960 など）は、ユーザが電話機の Directories ボタンを押すと、社内 LDAP ディレクトリを検索できます。IP Phone は、Hyper-Text Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）を使用して、要求を Web サーバに送信します。Web サーバからの応答には、電話機が解釈して表示できる特定の Extensible Markup Language（XML）オブジェクトが含まれている必要があります。社内ディレクトリを検索する場合、Web サーバは、プロキシとして動作します。電話機から要求を受け取り、その要求を LDAP 要求に変換します。LDAP 要求は、社内ディレクトリ サーバに送信されます。応答は適切な XML オブジェクトにカプセル化された後、解釈され電話機に戻されます。

図 14-3 では、Cisco CallManager が社内ディレクトリに統合されていない配置における、このメカニズムを示しています。このシナリオでは、Cisco CallManager はメッセージ交換に関わっていないことに注意してください。

図 14-3　ディレクトリ統合が行われていない場合の Cisco IP Phone 社内ディレクトリ アクセスのメッセージ交換



Web サーバのプロキシ機能は、Cisco LDAP Search Component Object Model（COM; コンポーネント オブジェクト モデル）サーバが組み込まれている Cisco IP Phone Services Software Development Kit（SDK; ソフトウェア開発キット）バージョン 2.0 以降を使用して設定できます。次の Web サイトの Developer Support Central から最新の Cisco IP Phone Services SDK をダウンロードできます。

http://www.cisco.com/pcgi-bin/dev_support/access_level/product_support

Log in now リンクをクリックしてログインし、**Voice Technology/AVVID** リスト ボックスから **CallManager - IP phone Services SDK** を選択します。

Cisco IP Phone のディレクトリ アクセスを設定するには、次の手順に従います。

ステップ 1　Microsoft Internet Information Server（IIS）を実行している Web サーバに Cisco IP Phone Services SDK をインストールします。このサーバは Cisco CallManager サーバとは異なるサーバである必要がありますが、企業ネットワーク上の既存の Web サーバでもかまいません（インストレーション手順の詳細は、SDK 製品資料を参照）。

ステップ 2　SDK に付属のマニュアルを使用して、LDAP Search COM オブジェクトとインターフェイスするための Active Server Page（ASP）を作成します。SDK にはサンプルの ASP が用意されていますが、高レベルのカスタマイゼーションが必要な場合は、独自の ASP を記述できます。IP Phone Services SDK Release 3.3 を使用している場合は、サンプルの ldapsearch.asp ページを IIS 仮想ディレクトリに置いてから、次のパラメータを設定して、社内 LDAP ディレクトリ サーバを指すようこのファイルを編集します。

- s.server

  このパラメータを LDAP サーバの名前または IP アドレスに設定します（たとえば、ldap.vse.lab）。
- s.port

  このパラメータを、LDAP サーバ上で LDAP 要求に使用するポートに設定します（標準のポートは 389 です）。
- s.base

  このパラメータを、LDAP ルックアップの検索ベースに設定します。この検索ベースには、ルックアップから返されるすべてのユーザが含まれている必要があります（たとえば、cn=Users, dc=vse, dc=lab）。
- s.AuthName

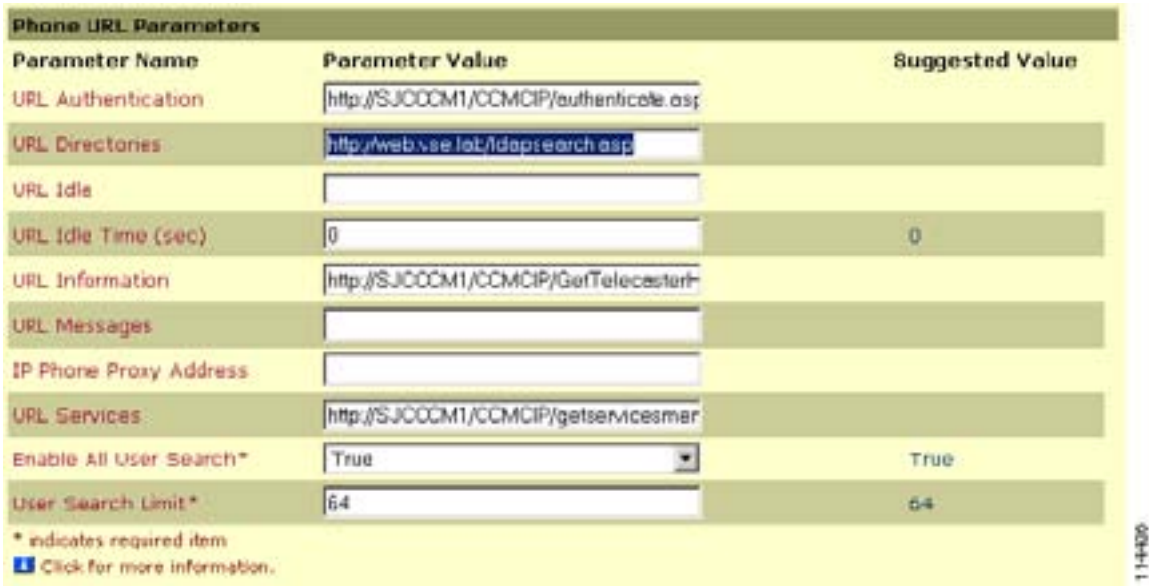
  LDAP サーバがルックアップで認証を要求する場合は、このパラメータを、検索ベースで指定したサブツリーを検索する権限を持つユーザの認定者名に設定します（たとえば、cn=CCMDirMgr, ou=System Accounts, cn=Users, dc=vse, dc=lab）。
- s.AuthPasswd

  LDAP サーバがルックアップで認証を要求する場合は、このパラメータを、検索ベースで指定したサブツリーを検索する権限を持つユーザのパスワードに設定します。

ステップ 3　図 14-4 に示しているように、Cisco CallManager Administration の Enterprise Parameter Configuration ページ（**System** > **Enterprise Parameters**）で、**URL Directories** フィールドを編集します。このフィールドを、前の手順で設定した、Web サーバ上の ldapsearch.asp ファイルへの URL に設定します。

ステップ 4　変更を有効にするために IP Phone をリセットします。

図 14-4　ディレクトリ アクセスを有効にするための Cisco CallManager におけるエンタープライズ パラメータの設定



さらに、Cisco IP Phone のディレクトリ アクセスには、次の特性があります。

- LDAPv3 準拠ディレクトリがすべてサポートされている。
- Cisco CallManager ユーザ プリファレンス（短縮ダイヤル、不在転送、個人用アドレス帳）は、社内 LDAP ディレクトリと統合されない。したがって、ユーザは、Cisco CallManager User Options Web ページにアクセスするために、別のログイン名とパスワードを持ちます。

Cisco CallManager とのディレクトリ統合

CallManager は、組み込み Microsoft SQL データベースを使用して、システムとデバイスの設定データ（たとえば、ダイヤル プラン情報、電話機とゲートウェイの設定、メディア リソースの使用率）を保存します。また、組み込み LDAP ディレクトリを使用して、ユーザとアプリケーションのプロファイル（たとえば、ユーザが制御するデバイス、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）ユーザ パラメータ、個人用アドレス帳のエントリ）を保存します。

SQL データベースと LDAP ディレクトリはどちらも、クラスタ内の各 Cisco CallManager サーバで実行され、サーバ間で複製アグリーメントが自動的にセットアップされます。パブリッシャ サーバには、SQL データベースと LDAP ディレクトリの両方のマスター コピーが入っています。パブリッシャ サーバは、すべてのサブスクライバ サーバへの複写を処理します。サブスクライバ サーバには、両方のリポジトリの読み取り専用コピーが入っています。

（注） この章の例と推奨事項は、いくつかの新機能と機能拡張が導入された Cisco CallManager Releases 4.0 および 4.1 に基づいています。旧バージョンの Cisco CallManager を実行している場合は、一部の動作が異なっていたり、一部の機能が使用できなかったりする場合があります。

アプリケーション固有の情報を LDAP ディレクトリに保存するために、Cisco CallManager は、組み込みディレクトリの使用時と、社内ディレクトリとの統合時の両方で有効な方法を採用します。

通常は、ディレクトリ ベンダーが異なると、異なる User オブジェクト モデルが使用され、各モデルが複数の標準外の追加属性を持っています。このため、Cisco CallManager は、User オブジェクトの標準 LDAPv3 コア属性だけを使用します。User オブジェクトは、次の属性が入っている補助クラス ciscoocUser で拡張されます。

- ciscoatGUID

  この属性は、ディレクトリ内のユーザを固有に識別します。

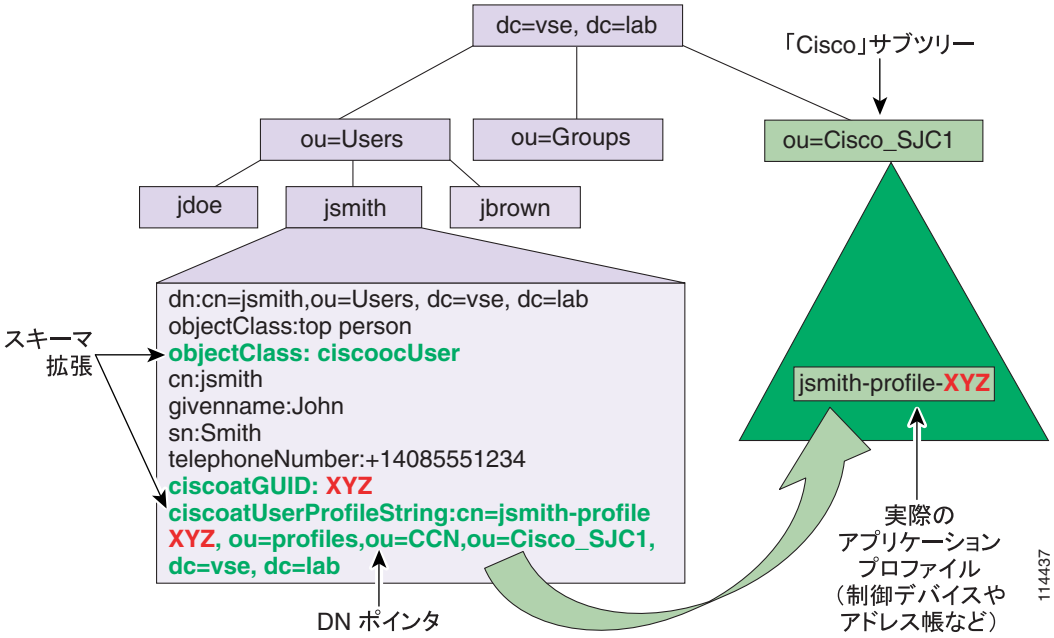
- ciscoatUserProfile

  この属性は、以前のバージョンの Cisco CallManager および他のアプリケーションによって使用されます。この属性は下位互換性のために残っています。

- ciscoatUserProfileString

  この属性は、ユーザのアプリケーション固有のプロファイルが入っている、ディレクトリ内の別のオブジェクトを指す認定者名ポインタです。この方法により、コア User オブジェクトに対する影響が最小限に抑えられ、アプリケーション特有のすべての情報を、通常 Cisco サブツリー、CISCOBASE、または Cisco Directory Information Tree（DIT; ディレクトリ インフォメーション ツリー）と呼ばれる、ディレクトリ内の別個の Organizational Unit（OU; 組織ユニット）に保存できます。図 14-5 では、このプロセスを示しています。

図 14-5　アプリケーション特有のユーザ情報をディレクトリに保存するための Cisco CallManager の方法



ciscoatUserProfileString 属性が指すオブジェクトは、ciscoocUserProfile と呼ばれる構造型オブジェクト クラスに属しています。このオブジェクトの主な目的は、ユーザのロケール、ユーザの Cisco IP Manager Assistant（IPMA）アシスタント、ディレクトリと統合されているすべてのシスコ アプリケーションのさまざまな固有プロファイル オブジェクトへのポインタなど、ユーザに固有のいくつかの詳細を保存することです。Cisco CallManager が使用するアプリケーション プロファイルは ciscoCCNocAppProfile と呼ばれる補助クラスに属し、Cisco CallManager はここにユーザのエクステンション モビリティ PIN、ユーザが制御するデバイスのリスト、ユーザが CTI アプリケーションの使用を許可されているかどうかなどの情報を保存します。Cisco CallManager は「Cisco」サブツリーの下にこれらのプロファイル オブジェクトの両方を作成します。

（注） ユーザに関連付けられるデバイスのリストは、多値属性としてディレクトリに保存されます。組み込み Cisco CallManager ディレクトリを使用している場合は、ユーザに関連付けることのできるデバイスの最大数は 2,000（クラスタ内のすべてのサブスクライバがデュアル CPU サーバである場合は 2,500）です。ただし、Microsoft Active Directory では、多値属性の値の数が 850 に制限されます。したがって、CallManager を Microsoft Active Directory と統合する場合、ユーザに関連付けることのできるデバイスの最大数は 850 になります。

Cisco Customer Directory Configuration Plugin

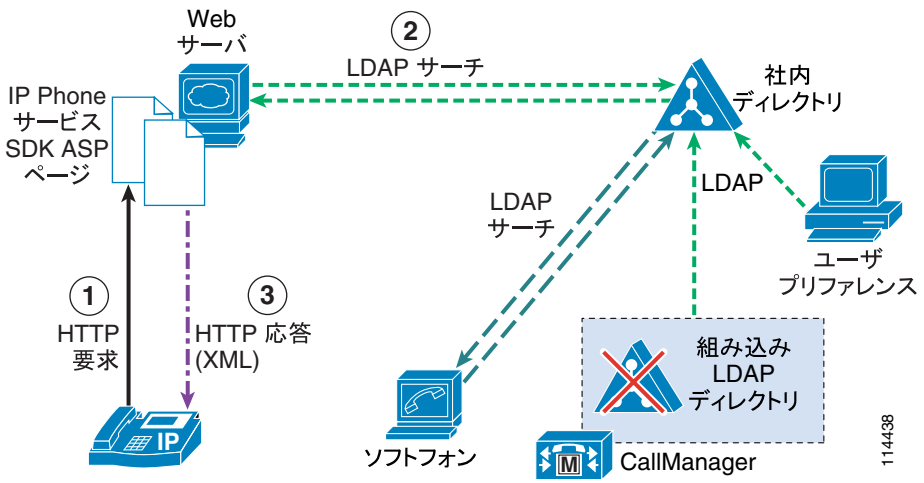
Cisco CallManager を外部 LDAP ディレクトリと統合するには、Cisco CallManager にバンドルされている Cisco Customer Directory Configuration Plugin を実行します（**Applications** > **Install Plugins**）。このプラグインを利用する主な目的は、次の 3 点です。

- 社内ディレクトリ スキーマを拡張して、アプリケーション固有のオブジェクトと属性に対応すること。
- 「Cisco」サブツリーに、Cisco CallManager が必要とする設定オブジェクトを取り込むこと。
- 社内ディレクトリを使用するように Cisco CallManager を設定し、その組み込みディレクトリを使用不可にすること。

通常、このプラグインを Cisco CallManager 上でローカルに実行すると、スキーマの更新が行われます。ただし、Cisco CallManager Release 4.0 以降では、LDAP Data Interchange Format（LDIF）ファイルを別個に作成する新しいオプションが用意されています。このため、LDIF ファイルを使用して、社内ディレクトリのスキーマ マスター サーバ上で直接スキーマの更新を行うことができます。このオプションを使用すると、さまざまなグループのユーザがその作業の関連部分を実行でき、Cisco CallManager がスキーマ マスター サーバに対してローカルでない場合に、ネットワークを介して更新する必要性が低くなります。

プラグインの実行後、Cisco CallManager は、社内ディレクトリを効果的に使用して、ユーザ プリファレンスを保存します。前の項で説明しているように、Cisco IP テレフォニー エンドポイントもこの社内ディレクトリにアクセスできる場合は、図 14-6 に示すようなシナリオになります。

図 14-6　Cisco CallManager が社内ディレクトリと統合されている場合の Cisco IP Phone 社内ディレクトリ アクセスのメッセージ交換



セキュリティの考慮事項

Cisco CallManager Release 4.1 以降では、Cisco CallManager と組み込みディレクトリの間の通信が、デフォルトで、LDAPS とも呼ばれる LDAP over Secure Socket Layer（SSL）を使用するように設定されています。

社内ディレクトリと統合する場合も、LDAP over SSL を有効にすることができます。これにより、すべての機密 LDAP データが保護接続を介して伝送されることが保証されます。LDAP over SSL オプションは、Cisco Customer Directory Plugin の一部として設定できます。このオプションでは、社内ディレクトリと共有され、同じ認証局によって発行された証明書が必要となります。

Cisco CallManager で LDAP over SSL が有効である場合は、次に示す Cisco IP Communications アプリケーションもこのセキュア チャネルを介してディレクトリと通信します。

- Cisco CallManager Administration 内のユーザ ページ
- Cisco Multi-Level Administration（MLA; マルチレベル管理）
- Cisco IP Phone Options ページ
- エクステンション モビリティ アプリケーション：Cisco CallManager サーバ上で実行されているエクステンション モビリティ アプリケーションと、社内ディレクトリの間の通信に SSL が使用されます。ただし、IP Phone とエクステンション モビリティ アプリケーションの間の通信には SSL が使用されず、HTTP が使用されます。

- Cisco CTI Manager
- Serviceability および Cisco Real-Time Monitoring Tool（RTMT）
- Cisco CDR Analysis and Reporting（CAR）
- Cisco IP Manager Assistant（IPMA）サービス
- Cisco Bulk Administration Tool（BAT）

ドメインへの Cisco CallManager サーバの追加

Microsoft Windows ドメインへの Cisco CallManager サーバの追加は、Cisco CallManager と外部ディレクトリの統合とは大きく異なります。これらの操作は相互排他的ではありませんが、異なる意味を持つ完全に独立した操作です。

- Cisco CallManager サーバを Microsoft Windows Active Directory（AD）ドメインに追加すると、ドメイン ポリシーが Windows 2000 Server オペレーティング システムに適用されることがあります。また、このような追加は Cisco CallManager サーバ自体の管理だけに影響を及ぼします。
- Cisco CallManager を外部ディレクトリ（Microsoft Active Directory や Netscape Directory Server など）と統合すると、Cisco CallManager がすべてのユーザ情報およびプリファレンスをそのディレクトリに保存します。ただし、このような統合は、Cisco CallManager サーバ自体の管理に影響を及ぼしません。

Cisco CallManager サーバをワークグループ サーバとして保持することをお勧めします。ただし、サーバをドメインに追加する場合は、サーバの正常な動作を妨げる可能性のあるドメイン ポリシーをサーバに適用することは避けてください。

サーバをドメインに追加する場合のその他の推奨事項については、次の Web サイトで入手可能な最新の Cisco CallManager 製品資料を参照してください。

http://www.cisco.com

ディレクトリ統合のベスト プラクティス

ディレクトリ統合プロセスには、ネットワーク内の複数のコンポーネントおよびサービスが関連します。したがって、ディレクトリ統合プロセスは、慎重に計画して実装する必要があります。この項では、次のトピックを扱います。

（注） 既知の Cisco CallManager 統合の大部分は、Microsoft Active Directory（AD）との間で行われているため、ここでは AD に対するベスト プラクティスを中心に説明します。ただし、この項で述べる推奨事項やベスト プラクティスのほとんどは、Cisco CallManager によってサポートされているもう 1 つのディレクトリ製品 Sun/iPlanet Netscape Directory Server にも適用されます。

ディレクトリ統合の計画

ディレクトリは、企業全体のリソースであり、多数のアプリケーションおよびエンド ユーザによって使用される可能性があるため、統合を慎重に計画して、他のすべてのアプリケーションへの影響を最小限に抑えることが重要です。

ヒント 統合を開始する前に、社内のディレクトリ チームが計画、設計、および実装の各段階に携わっていることを確認してください。

この章で前述したように、Cisco CallManager および他のアプリケーションを外部ディレクトリと統合する場合は、ディレクトリ スキーマを拡張する必要があります。スキーマの拡張は、細心の注意を要する操作です。たとえば、Microsoft Windows 2000 Active Directory の場合、スキーマの変更を取り消すことはできません。ディレクトリの損傷を避けるために、次の予防措置を講じる必要があります。

- 計画したスキーマ変更を社内のディレクトリ チームと共に再検討する。この作業は、社内の変更制御手順の一部である必要があります。
- 実験用設備で実稼働ディレクトリのレプリカを作成し、そのレプリカに対して統合をテストする。
- 統合前に実稼働ディレクトリ（データとスキーマの両方）をバックアップし、復元が必要となったときにデータとスキーマを正常に復元するための有効なバックアウト計画を用意しておく。
- 他のアプリケーションおよびエンド ユーザへの影響を最小限に抑えるため、オフピーク時にスキーマの拡張を計画して実行する。

上記の予防措置リストを見て不安になったとしても、実際は、スキーマの拡張によって、バックアウトを必要とするような問題が発生することはほとんどありません。ただし、操作がいかに安全であると認識されていても、予期せぬ問題から回復できるようにするための予防措置を怠ってリスクを高めることのないよう注意してください。

もう 1 つの重要な考慮事項は、音声アプリケーションはディレクトリと統合するとすぐに、そのディレクトリに依存して正常な動作を行うため、ディレクトリ サーバに到達できないと音声システムに悪影響が及ぶ可能性があるということです。

たとえば、ディレクトリが突然使用できなくなると、エンド ユーザが Cisco CallManager User Options Web ページにログインして自分のプリファレンスを設定できなくなったり、エクステンション モビリティ ユーザ、Attendant Console オペレータ、および IPCC Express エージェントがログインもログアウトもできなくなったり、名前によるダイヤル機能が使用できなくなったりします。

このような問題を避けるため、すべてのシスコ音声アプリケーションに高いアベイラビリティを提供できるようにディレクトリ インフラストラクチャを設計する必要があります。次のいずれかの方法で、このような高いアベイラビリティを実現できます。

- ディレクトリ複製メカニズムを活用して、ディレクトリ サーバをシスコ音声アプリケーションと同じロケーションに置く。
- Cisco IOS ソフトウェアの Server Load Balancing（SLB）などのサーバ ロードバランシング メカニズムを使用して、特定のキャンパスまたはデータ センタ内でサーバの冗長性を実現し、できる限りローカル サーバへのアクセスが行われるようにする。
- ディレクトリ プラグインを設定する場合は、特定のドメイン コントローラ ホスト名ではなく、Domain Name System（DNS; ドメイン ネーム システム）ドメイン名を使用する。

冗長サーバがある場合は、DNS によって最初に返される名前のサーバが、後の応答で返される名前のサーバほど、Cisco CallManager に対してローカルでないことがあります。また、DNS サーバでラウンドロビン機能が有効である場合、DNS サーバは応答で意図的に複数のアドレスを 1 つずつ順番に返します。クライアント側の DNS キャッシュ タイムアウトなどのメカニズム、およびその間に同じドメインに対して照会する他のクライアントによっては、Cisco CallManager が 2 つの連続した操作を 2 つの異なる Domain Controller（DC; ドメイン コントローラ）に対して行うことがあります。前述のローカル性の問題の他に、DNS 冗長性を使用すると、最初の操作とその後の照会の間にディレクトリが複製されなかった場合、最初の操作で作成したオブジェクトを、その後の照会で別の DC に対して検索しても見つけることができないという問題もあります。したがって、DNS を使用して実装を冗長にすることを決定する前に、これらの問題が配置に影響を及ぼさないことを確認してください。

また、正しい LDAP 照会には DNS が必要であることにも注意してください。Cisco CallManager は、LDAP 照会で返されるどの DC のホスト名も解決できる必要があります。

（注） Microsoft Windows 2000 DNS には最初にローカル リソースを返す機能（LocalNetPriority）が備わっていますが、この機能は要求側クライアントのクラスフル IP アドレスの調査に基づいています。したがって、この機能はサブネット化されたネットワークではあまり役に立ちません。この機能については、Microsoft Knowledge Base 記事 177883 で説明されています（http://support.microsoft.com/ を参照してください）。Windows 2000 DNS を使用しない場合は、選択した実装のどの機能でこれらの問題を軽減できるかを調べる必要があります。これらの推奨事項は、Cisco CallManager が DNS を使用するように設定され、その DNS が Active Directory によって使用される DNS インフラストラクチャと同じであるという前提に基づいています。

統合のためのディレクトリの準備

Microsoft Windows 2000 Active Directory では、スキーマ変更を許可するようにドメイン コントローラを設定する必要があります。この要件は、スキーマ マスター（変更が行われるロケーション）として機能するドメイン コントローラだけに適用され、次の Web サイトで入手可能な Microsoft Knowledge Base 記事 285172 で詳しく説明されています。

http://support.microsoft.com

Cisco CallManager を Microsoft Windows 2000 Active Directory と統合し、Microsoft Exchange 2000 が同じフォレスト内に共存する必要がある場合は、追加の準備手順が必要になります。Cisco CallManager は、RFC 2798 で定義されている iNetOrgPerson クラスによって指定された

labeledURI 属性を使用します。Microsoft は、現在、Exchange 2000 に対して別の方法でこの属性を定義しています。これにより、Cisco CallManager スキーマとの間で名前の衝突が発生します。この問題については、Microsoft Knowledge Base 記事 314649（http://support.microsoft.com から入手可能）で説明されています。次の Web サイトから iNetOrgPerson キットを入手できます。

http://msdn.microsoft.com/library/en-us/dnactdir/html/inetopkit.asp

注意　スキーマを拡張する前に、必ずディレクトリをバックアップしてください。復元メカニズムが必要となる前に、使用する予定の復元メカニズムを必ずテストしてください。

Cisco CallManager のディレクトリ スキーマを拡張するには、クラスタのパブリッシャ サーバから Cisco Customer Directory Configuration Plugin を実行し、次のベスト プラクティスに従います。

- プラグインを実行する場合は、セットアップ タイプとして必ず **Custom** を使用する。Express セットアップ タイプは、Cisco CallManager や他のシスコ音声アプリケーション専用のスタンドアロン ドメインとの統合だけに適しています。既存のドメインと統合する場合は、Express セットアップを使用しないでください。
- プラグイン設定画面では、**Install Schema on the Schema Master** オプションだけを選択する。
- スキーマ マスター サーバが Cisco CallManager に対してローカルであるか、またはスキーマ マスター サーバと Cisco CallManager の間に高速接続が存在することを確認する。どちらも実現できない場合は、プラグインで LDIF ファイルの作成だけを行い、そのファイルを使用してスキーマ マスター上で直接スキーマを更新することを検討します。
- この段階で、プラグインに、Active Directory の Schema Admins グループのメンバーであるユーザのクレデンシャル（認定者名とパスワード）を入力する。このクレデンシャルは、通常の Cisco CallManager 動作ではなく、スキーマの拡張だけに使用されます。

（注）　大規模な AD フォレストまたは複雑なトポロジがある場合は、スキーマの変更がフォレスト内のすべてのドメインおよびすべてのドメイン コントローラに伝搬されるまで、しばらく時間がかかることがあります。この伝搬のために十分な時間をとってから準備プロセスを続行するか、または必要に応じて強制的に複製を行ってください。

スキーマが拡張されるとすぐに、Cisco CallManager クラスタおよび他のシスコ音声アプリケーションによって使用される「Cisco」OU（サブツリー）を作成する場所を決めることができます。統合される Cisco CallManager クラスタごとに 1 つの組織ユニット（OU）が必要です。

単一ドメインの AD または Netscape Directory Server を使用する配置では、位置は重要ではありません。ツリー内のどこにでも、OU を効果的に配置できます。

マルチドメイン AD フォレストでは、多くの場合、ルート ドメインはユーザもリソースも含まず、プレースホルダ ドメインとして使用されるため、通常、「Cisco」サブツリーは子ドメイン内に存在します。このタイプのマルチドメイン トポロジでは、地理的な境界に基づいてドメインを作成できます。したがって、各ロケーションが各ドメインのローカル ドメイン コントローラを持つ可能性が低くなります。ネットワークを介した複製トラフィックを減らすため、ドメイン コントローラは、通常、必要な場所だけに配置されます。この点を念頭に置いて、所定のクラスタの Cisco OU を、そのクラスタによってサービスを提供されるユーザの大部分を含むドメイン内に置くことをお勧めします。

図 14-7 では、マルチドメイン単一ツリー AD フォレストを示しています。このフォレストでは、2 つの CallManager クラスタの「Cisco」OU が、2 つの個別の子ドメイン emea.vse.lab と amer.vse.lab の中に作成されています。

図 14-7　マルチドメイン単一ツリー AD フォレスト

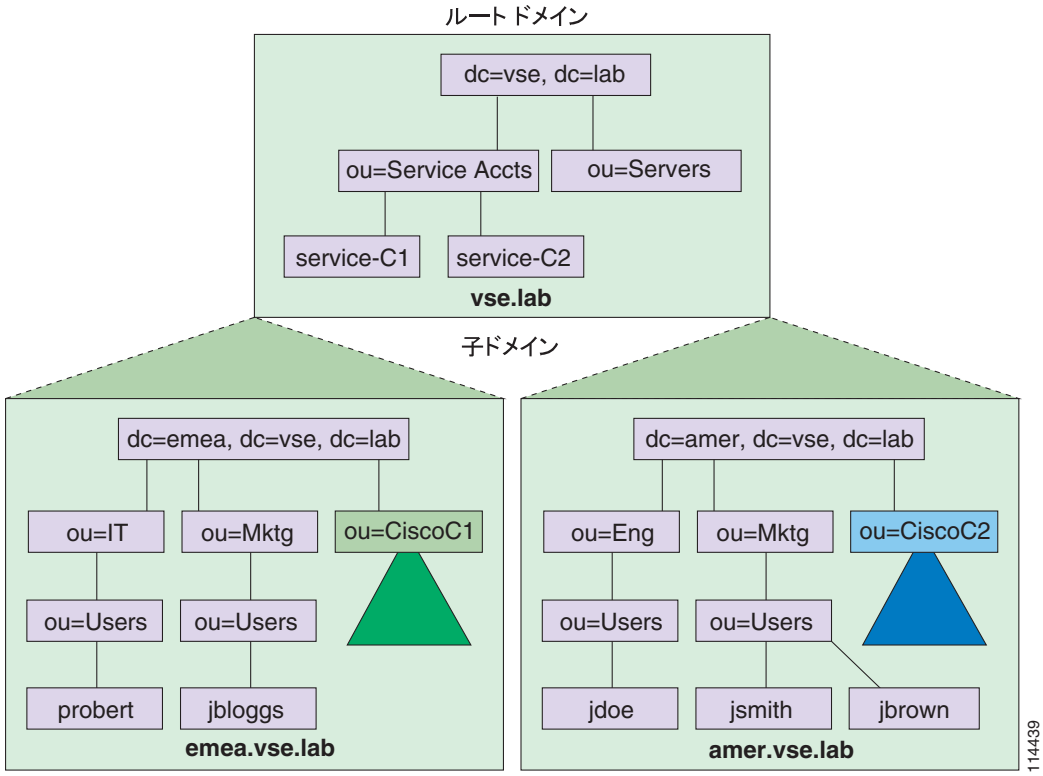
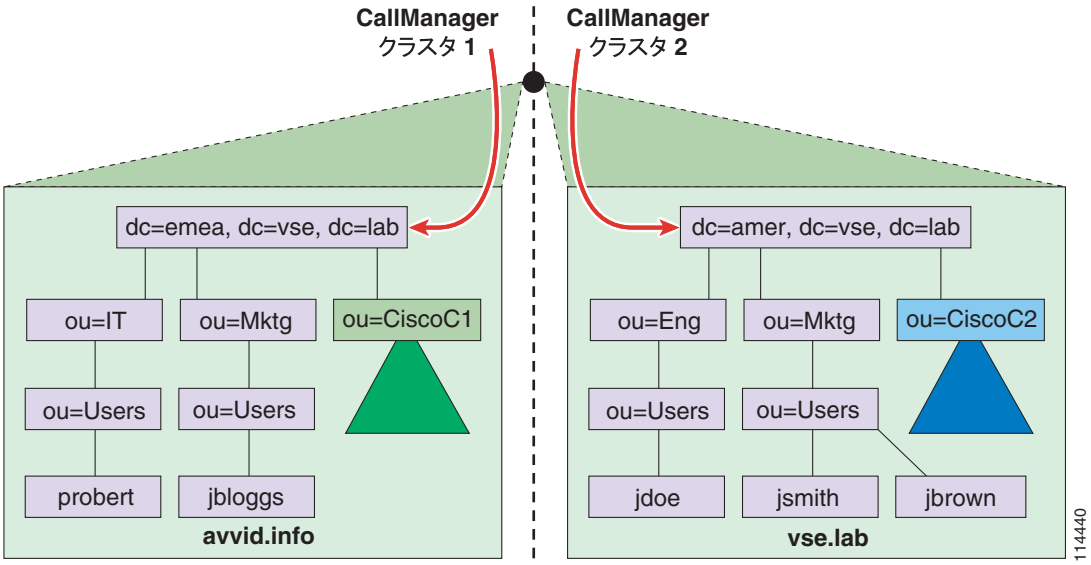


図 14-7 では、各クラスタが、集中型コール処理モデルで、地理的に対応する場所にサービスを提供します。したがって、AD に保存されているユーザ データもローカルであることが保証されます。この設計により、ローカルでない DC から情報を取り出す必要がなくなり、検索で関連情報を見つけるために必要な LDAP 照会の数が減ります。

Cisco CallManager クラスタが、異なるドメインのユーザにサービスを提供するようにすることはお勧めしません。なぜなら、ドメイン コントローラがローカルでないドメインが含まれている場合、ユーザ データ取得中の応答時間が最適ではなくなる可能性があるためです。ただし、マルチドメイン AD を作成する理由（つまり、地理、帯域幅、または組織構造）は、通常、複数のクラスタを必要とする理由と同じであるため、このシナリオは一般的ではありません。

現在、クラスタは AD フォレスト内の複数のツリーにまたがることはできません。なぜなら、ツリーは、LDAP 照会の要件である連続したネームスペースを持たないためです。クラスタは 1 つのドメインまたは単一のツリー内に存在でき、（前述のように）マルチツリー フォレスト内に存在することもできます。ただし、図 14-8 に示しているように、特定のクラスタのすべてのユーザが同じネームスペースに含まれている必要があります。

図 14-8　Cisco CallManager クラスタは単一ツリー（連続したネームスペース）に含まれる必要がある



User Search Base は、ディレクトリと統合する場合に Cisco CallManager によって使用されるもう 1 つの重要な要素です。User Search Base は、クラスタ内のデバイスと関連付けることができるユーザを検索するために Cisco CallManager によって使用されるサブツリーのルートを示します（このパラメータを設定する方法については、P.14-17 の「Cisco CallManager とディレクトリの統合」の項を参照してください）。

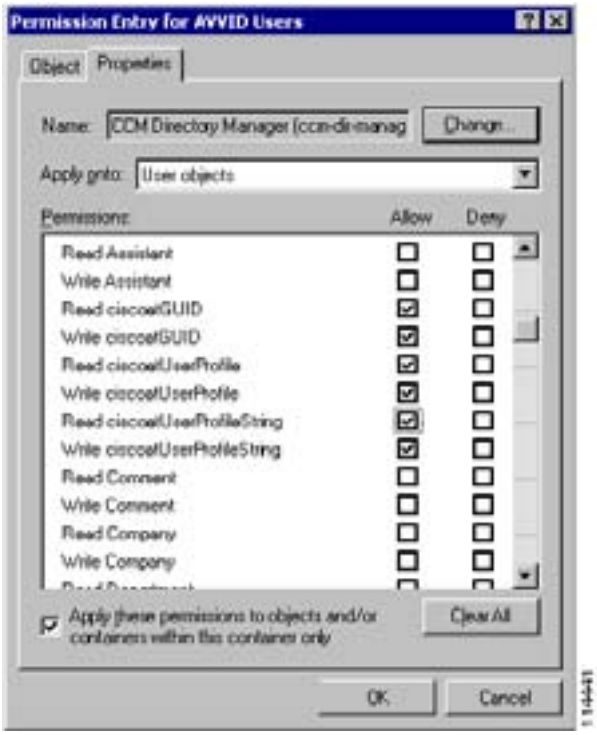
Cisco CallManager や他のシスコ音声アプリケーションがディレクトリに対するアクセスおよび管理に使用できる、特別なユーザ アカウントを作成する必要があります。Cisco CallManager クラスタごとに 1 つのアカウントが必要です。なぜなら、これにより、必要な場合にだけ各アカウントに特定の権限を付与し、企業の他の部門に影響を与えることなく、クラスタごとの簡単な管理を行うことができるためです。この章の例では、このアカウントの名前を CCM Directory Manager としていますが、このユーザ アカウントに異なる名前を付けてもかまいません。

各 CCM Directory Manager アカウントには、ディレクトリ内で少なくとも次の権限を付与する必要があります。

- それぞれの「Cisco」OU サブツリーに対する **Read/Write/Create all child objects/Delete all child objects** 特権。これらの権利は、オブジェクトとプロパティの両方で **This object and all child objects** に適用されるように設定する必要があります。AD では、Active Directory Users and Computers（ADUC）内のセキュリティの詳細オプションを使用して、この特権を設定できます。デフォルトでは、そのオブジェクトだけに適用するように設定されているため、権利を変更する必要があります。
- User Search Base およびその下に含まれているすべての OU に対する **Read** 特権。ツリーの下部で継承がブロックされていない限り、User Search Base レベルだけでこの特権を設定できます。
- User Search Base の下に含まれているすべての User オブジェクトの ciscoatGUID、ciscoatUserProfile、および ciscoatUserProfileString 属性に対する **Read/Write** 特権。AD では、ADUC 内のセキュリティの詳細オプションを使用して、この特権を設定できます。

ヒント AD では、User Search Base 内のすべての User オブジェクトの ciscoatGUID、ciscoatUserProfile、および ciscoatUserProfileString 属性に対する権限を設定するには、User Search Base のルートで組織単位（OU）の Advanced security ウィンドウから CCM Directory Manager ユーザを選択します（この章では、このユーザの名前を CCM Directory Manager としていますが、ユーザ名は異なっていてもかまいません）。その後、**View/Edit** をクリックし、図 14-9 に示しているような、新しいウィンドウの **Properties** タブに移動します。**Apply onto** ドロップダウン メニューから **User objects** を選択し、下にスクロールして ciscoatGUID、ciscoatUserProfile、および ciscoatProfileString 属性まで移動します。これらすべてに対して **Write** 権限を許可します。

図 14-9　Active Directory でのユーザ アカウントに対する権限の設定



ヒント CCM Directory Manager アカウントを作成する場合は、**Password never expires** オプションを設定してください。パスワードを変更する場合は、Cisco CallManager から CCMPwdChanger ユーティリティを実行します。この方法により、AD でパスワードが更新され、Cisco CallManager でレジストリが更新されて、ディレクトリ初期化ファイルが更新されます。

Cisco CallManager とディレクトリの統合

前項の説明に従ってディレクトリを準備した後、Cisco Customer Directory Configuration Plugin を再び実行して統合を行うことができます。この時点で考慮する必要のある 2 つの主な概念は、User Search Base と User Creation Base です。

(注)　User Creation Base は、Cisco CallManager Release 4.0 で導入されました。以前のバージョンの Cisco CallManager では、ユーザの作成にも User Search Base が使用されます。

前項で述べたように、User Search Base パラメータは、Cisco CallManager によってすべてのユーザ検索に使用されるサブツリーのルートを示します。

User Creation Base パラメータは、次のようなシステム アカウントを作成する場所を Cisco CallManager に指示します。これらのアカウントは、いくつかのアプリケーションおよびそのアプリケーションにバンドルされている機能で必要となります。

- CCM Administrator：Cisco CallManager Multilevel Administration Access（MLA）によって使用されます。
- CCM SysUser：コールバックおよびエクステンション モビリティによって使用されます。
- IPMA SysUser：Cisco IP Manager Assistant によって使用されます。

Cisco CallManager はシステム アカウント ユーザを認証する前に検索できる必要があるため、User Creation Base は User Search Base 内に含まれている必要があります。

User Search Base を設定するには、クラスタによってサービスを提供されるユーザが置かれている場所を参照し、そのようなユーザをすべて含む第 1 レベルに User Search Base を設定します。User Search Base を低いレベルに設定するほど、応答時間やパフォーマンスが向上します。なぜなら、検索で多くの照会を行ったり、低速 WAN リンク通過してリモート ドメイン コントローラに到達したりする必要がなくなるためです。また、クラスタが必要としないユーザ データを検索で解析する必要もありません。

単一ドメイン AD フォレスト（またはスタンドアロン Netscape Directory）では、User Search Base を、Cisco CallManager クラスタのすべてのユーザを含む最下位レベルの組織ユニット（OU）（たとえば、ou=AVVID Users, dc=vse, dc=lab）に設定します。この OU は、ドメインのルート（たとえば、dc=vse, dc=lab、または o=avvid.lab）になる場合もあります。それは、ユーザがその OU の直下の複数の OU に散在している場合です。

マルチドメイン AD フォレストでは、特定の Cisco CallManager クラスタのユーザを単一のドメイン内に保持するようにし、前述のガイドラインに従います。ユーザが複数のドメインに散在しているため、単一のドメイン内に保持できない場合は、Cisco CallManager クラスタによってサービスを提供されるユーザのドメインをすべて含むツリー内の最下位ポイントに User Search Base を設定します。サービスを提供される複数の子ドメインが最上位レベル ドメインの直下にある構造では、User Search Base を AD フォレスト全体のルートに設定する必要があります。ただし、どのような場合でも、サービスを提供される各ドメインのドメイン コントローラを Cisco CallManager と同じ場所に置くか、またはネットワークの回復力と高速性を十分高くして、ローカル検索に比べてリモート検索でパフォーマンスが大きく低下しないようにする必要があります。

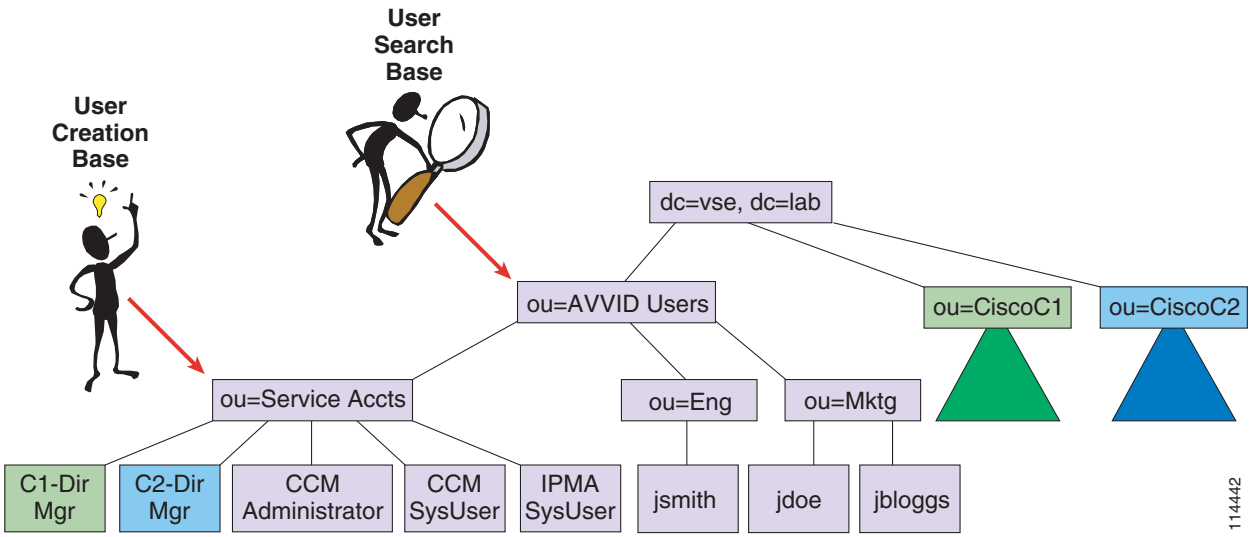
(注)

User Creation Base は User Search Base 内に存在する必要がありますが、User Creation Base 内に作成されるシステム アカウントに既存の Active Directory ユーザ ポリシーが適用されないように注意してください。システム アカウントにユーザ ポリシーが適用されないようにする簡単な方法は、アカウントをサブ OU 内に入れ、その OU に Group Policy Object（GPO）が継承されないようにすることです。

複数の Cisco CallManager クラスタを同じ AD フォレストと統合できます。ただし、お客様の AD 構成と、Cisco CallManager と共に配置されてディレクトリを使用できるシスコ音声アプリケーションの組み合せが多数である可能性があるため、マルチクラスタ統合を進める前に、シスコのエンジニアリング チームに特別なサポートを要請する必要があります。お近くのシスコの代理店に連絡して、サポートを要請してください。Cisco CallManager 以外のシスコ音声アプリケーション（CDR Analysis and Reporting ツール、Multilevel Administration Access、IP Contact Center、IPCC Express など）を配置する場合は、追加の制限が適用されることがあります。このような他製品の詳細については、それぞれのオンライン マニュアルおよびリリース ノートを参照してください。

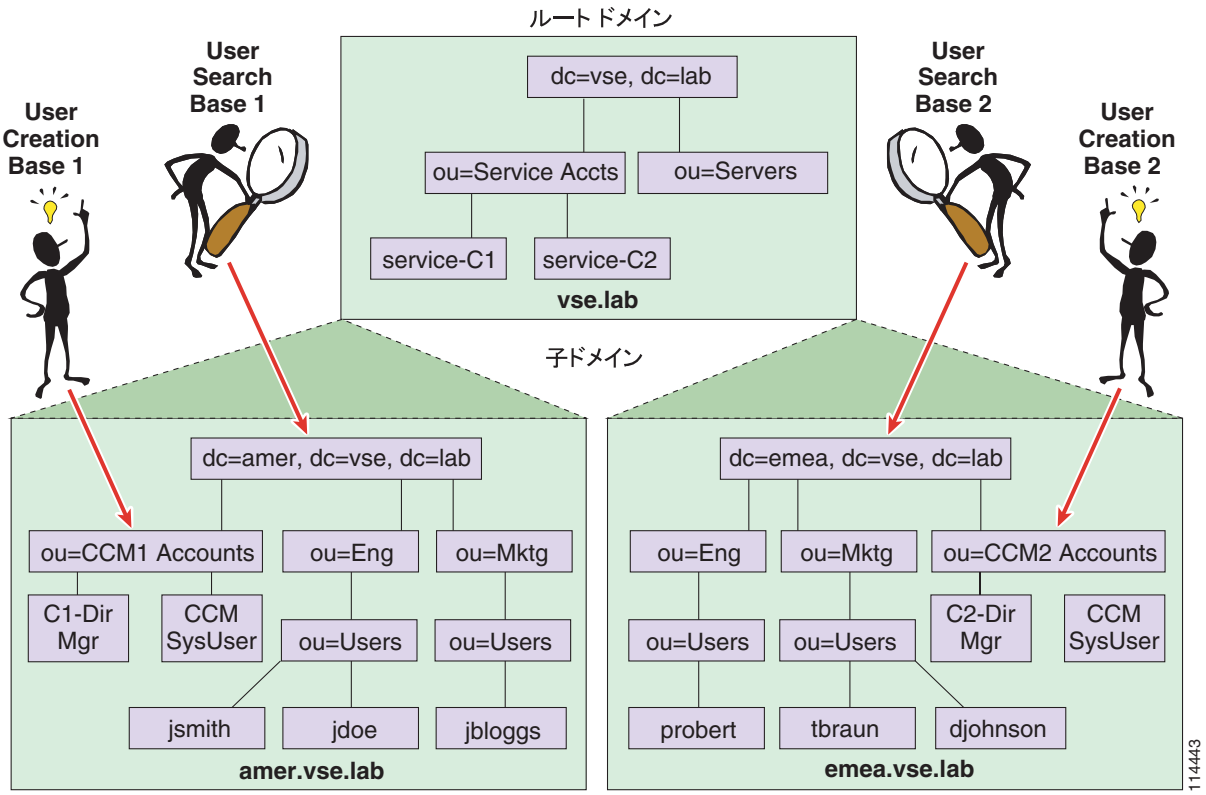
複数の Cisco CallManager クラスタを同じ AD ドメイン（またはスタンドアロン Netscape Directory）と統合する場合は、図 14-10 で示しているように、同じ User Creation Base を指定することによって、クラスタ間でシステム アカウントを共有できます。

図 14-10　単一 AD ドメイン内の User Search Base と User Creation Base の設定



複数の Cisco CallManager クラスタをフォレスト内の異なる AD ドメインと統合する場合は、図 14-11 で示しているように、User Creation Base を関連ドメイン内の OU に設定して、クラスタごとに異なる User Creation Base を定義することをお勧めします。

図 14-11　マルチクラスタ マルチドメイン フォレスト内の User Search Base と User Creation Base の設定



ヒント

システム アカウントおよびサービス アカウントが Cisco CallManager Administration に表示されないようにするには、ユーザの Description フィールドに **CiscoPrivateUser** という文字列を追加します。CCM Administrator、CCM SysUser、および IPMA SysUser の各アカウントの場合は、このフィールドがデフォルトで設定されていますが、CCM Directory Manager アカウントにも問題なくこの Description を追加できます。Description フィールドを更新するには、Microsoft ADSIEdit（Windows 2000 Support Tools の一部として使用できる Active Directory Service Interfaces）または他の LDAP ツールを使用してください。

User Search Base および User Creation Base をどのように設定するか決めた後、クラスタ内の Cisco CallManager パブリッシャ サーバ上で Cisco Customer Directory Configuration Plugin を再び実行できます。この手順を実行する場合は、次のベスト プラクティスに従ってください。

- **Custom** プラグイン セットアップ タイプを選択し、**Configure Active Directory** オプションと **Enable CallManager Integration with Active Directory** オプションだけを選択する。
- Cisco CallManager と同じ LAN に置かれているドメイン コントローラのホスト名を指定する。または、DNS を使用しており、このドメインのすべてのドメイン コントローラが Cisco CallManager と同じ LAN に置かれている場合は、ドメイン名を使用します。ディレクトリ統合で高いアベイラビリティを実現する方法の詳細については、P.14-11 の「ディレクトリ統合の計画」を参照してください。

パブリッシャ サーバ上でこれらの手順を完了した後、3 つのシステム アカウントのパスワードを設定します。これを行うには、Cisco CallManager にバンドルされている CCMPwdChanger ツールを使用するか（**Start** > **Run** を選択し、**cmd** と入力して DOS ウィンドウを開き、**CCMPwdChanger** と入力して **Enter** キーを押します）、または社内ディレクトリのインターフェイス（たとえば、Active Directory の場合は ADUC）を使用します。パスワードが期限切れになったり、最初のログインで変

更するよう設定されたりしないように、これらのユーザのパスワード ポリシーを設定することをお勧めします。このパスワード ポリシーを使用することで、これらのアカウントに GPO が適用されないようにすることもできます。

有効期限ポリシーを適用すると、パスワードが期限切れになったときに Cisco CallManager が動作を停止しますが、期限切れのパスワードが問題であることを知らせる警告は表示されません。たとえば、3　か月ごとにパスワードの変更を必要とするポリシーがある場合は、3　か月ごとに CCMPwdChanger ツールを実行する必要があります。

前述の手順をすべて完了した後、Cisco CallManager クラスタ内のサブスクライバ サーバごとに Cisco Customer Directory Configuration Plugin を実行できます。

（注） 統合を行う場合、Cisco CallManager 組み込みディレクトリと社内ディレクトリの間のデータ移行は行われません。組み込みディレクトリに設定したユーザとプロファイルを移行する場合のために、シスコはこのタスクに役立ついくつかの移行スクリプトを開発しました。これらのスクリプトを入手するには、シスコのアカウント チームまたは販売代理店に問い合せてください。これらのスクリプトは、現状のまま、サポートなしで提供されることに注意してください。

ディレクトリ統合の管理

Cisco CallManager を外部ディレクトリと統合した後、ユーザとパスワードの管理手順およびポリシーを適宜設定する必要があります。

次の管理操作には、社内ディレクトリのインターフェイス（またはサポートされている API）を使用します。

- ユーザの追加
- ユーザの削除
- コア ユーザ属性（表示名、部門、アドレス、パスワードなど）の設定および変更

また、次の管理操作には、Cisco CallManager Administration を使用します。

- CallManager 固有のユーザ属性（PIN やユーザ ロケールなど）の設定
- ユーザとデバイス（IP Phone や CTI ポートなど）の関連付け

デフォルトでは、Cisco CallManager Administration を使用してユーザを追加することも削除することもできません。また、名前や電話番号など、コア ユーザ属性を変更することもできません。Cisco CallManager Administration でユーザを追加および削除できるようにするには、次の Web サイトで入手可能な『*Installing the Cisco Customer Directory Configuration Plugin for Cisco CallManager Release 4.0(1)*』の説明に従って、Cisco CallManager サーバ上の UMDirectoryConfiguration.ini ファイルを修正します。

http://www.cisco.com

この機能は便宜的に提供しているもので、既存のユーザ管理ツールやディレクトリ管理ツールに取って代わるものではありません。この機能は限定的であることに注意してください。通常は、他の使用可能なツールでユーザを追加または削除することをお勧めします。

Active Directory ではパスワードをクリアテキスト LDAP で設定できないため、Cisco CallManager が Microsoft Active Directory と統合されている場合でも、Cisco CallManager Administration でユーザ パスワードを設定することも変更することもできません。ディレクトリ パスワードを安全な方法で変更するには、Cisco CallManager にバンドルされている CCMPwdChanger ツール、またはディレクトリ ベンダーによって提供される管理インターフェイスを使用できます。

Cisco CallManager 上の UMDirectoryConfiguration.ini ファイルを修正した後でも、AD 内のユーザを作成および削除するための十分な権限を CCM Directory Manager アカウントに与える必要があります。

複数の Cisco CallManager クラスタを同じディレクトリと統合する場合は、同じユーザを異なるクラスタ内のデバイスに関連付けることはできないことに注意してください。各ユーザは、どの時点でも、単一の特定の Cisco CallManager クラスタと関連付ける必要があります（もちろん、あるクラスタから別のクラスタにユーザを移動できます。これを行うには、単に、最初のクラスタでユーザとデバイスの関連付けを解除し、2 番目のクラスタでユーザをデバイスに関連付けます）。

ユーザがパスワードを変更したりプリファレンスを設定したりする場合は、次の方法で行うようユーザに指示してください。

- パスワードを変更する場合は、ディレクトリ　アプリケーションのインターフェイスを使用する。Microsoft Active Directory の場合、パスワードの変更は、ユーザの Windows ワークステーションから、または管理ツールを使用する管理者によって行われます。
- PIN または Cisco CallManager プリファレンス（短縮ダイヤルや不在転送番号など）を変更する場合は、Cisco CallManager User Options Web ページを使用する。

（注） ユーザは AD との統合後でも Cisco CallManager User Options Web ページを使用してパスワードを変更できますが、各ユーザが Windows のパスワードを同時に変更していることに気付かない可能性があるため、この操作はお勧めしません。また、クライアント ワークステーションと Cisco CallManager サーバの間の通信では HTTP が使用されるため、パスワードがクリア テキストでネットワークを通過します。Active Server Page（ASP）から関連コードを削除するだけで、Cisco CallManager User Options Web ページから **Change your Password** オプションを削除できます。

追加、削除、および変更という点では、Cisco CallManager がディレクトリと統合されている場合、次の操作がサポートされないことに注意してください。

- ユーザ名（AD の場合、sAMAccountName）の変更
- ある OU から別の OU へのユーザの移動
- 「Cisco」OU の移動または名前変更

ただし、これらの制限に対処するために、ユーザの CallManager 固有属性（該当するユーザの「Cisco」OU 内のプロファイルや、ciscoatGUID 属性、ciscoatUserProfile 属性、および ciscoatUserProfileString 属性内のデータなど）を手動で削除できます。その後、ディレクトリ管理ツールを使用してユーザ名の変更またはユーザの移動を行ってから、ユーザを Cisco CallManager 加入者として再び追加できます。これは煩雑な手順ですが、この手順によってディレクトリ アプリケーション内でユーザのファイル所有権およびセキュリティ方針が維持されます。

Cisco CallManager のアップグレード

Cisco CallManager のメジャー リリースごとにスキーマが変更される可能性があるため、アップグレード後には必ず Cisco Customer Directory Integration Plugin を実行する必要があります。

複数の Cisco CallManager クラスタを同じディレクトリと統合した場合は、スキーマを 1 回だけ拡張する必要があります。クラスタが、異なる Cisco CallManager リリースを実行している場合は、最新のリリースを実行しているクラスタ内からスキーマを拡張する必要があります。

CHAPTER 15

IP テレフォニー移行オプション

この章では、IP テレフォニー システム（または他の電話システム）に移行するための、次の主な方法について説明します。

- 段階的な移行（P.15-2）
- フラッシュ カットオーバー（ビッグバン移行）（P.15-3）

どちら方法が正しいというわけではありません。お客様の状況や好みに応じて、どちらのオプションを使用するかを決めてください。

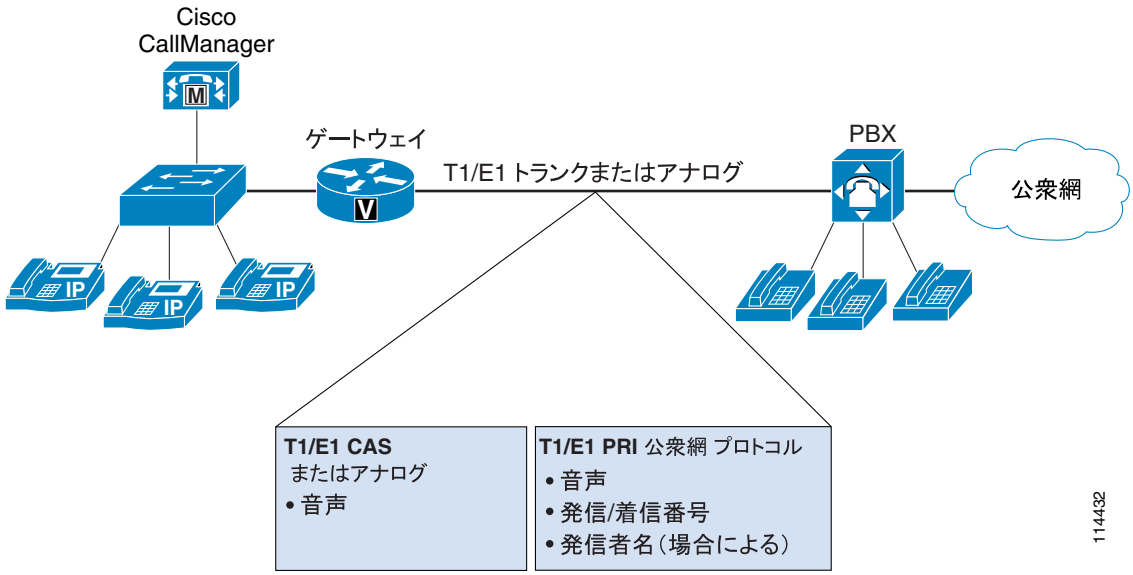
この章では、P.15-4 の「マルチサイト企業における QSIG の必要性」についても説明します。

段階的な移行

この方法では、通常、メインの社内 PBX に接続されている小規模な初期 IP テレフォニー配置が実現されます。どのシグナリング プロトコルを選択するかは、必要な機能および実装コストによって決まります。Cisco CallManager は、一般的な公衆網タイプの PRI または QSIG PRI を提供できます。

公衆網タイプの PRI は、基本的なコール接続および Automatic Number Identification（ANI; 自動番号識別）を提供します。場合によっては、図 15-1 に示しているように、このプロトコルが発信者名情報をサポートすることもあります。

図 15-1　シグナリング プロトコルによってサポートされる機能



このレベルの接続は、すべての PBX に使用できます。つまり、Cisco CallManager を接続の「ネットワーク」側として設定できるため、PRI を介してパブリック ネットワークに接続できる PBX は Cisco CallManager に接続できます。

Cisco CallManager Release 3.3 以降では、International Standards Organization（ISO; 国際標準化機構）バリアントの QSIG が組み込まれています。QSIG プロトコルを使用すると、公衆網タイプの PRI から得られる機能に加えて、異なるベンダーの PBX 間の機能透過性を実現できます。したがって、このプロトコルは、すでに複雑なネットワークを稼働している大規模な企業に適しています（P.15-4 の「マルチサイト企業における QSIG の必要性」を参照してください）。

公衆網タイプの PRI や QSIG でも、段階的な移行のプロセスはほぼ同じです。移行が完了するまで、加入者を一度に 1 グループずつ、グループ単位で PBX から Cisco CallManager に移動します。

約 60 個のビルディングに約 23,000 人の加入者が収容されているシスコの San Jose キャンパスでは、開始から終了まで 1 年以上かかって、この方法で IP テレフォニーに移行しました。週末ごとに 1 つのビルディングを変換しました。選択したビルディング内のすべての加入者を識別し、金曜日の晩にその内線番号を PBX から削除しました。同時に、その内線番号をダイヤルした人が正しい PRI トランクを介してルーティングされ、Cisco CallManager に転送されるように、PBX ルーティング テーブルに追加の設定を加えました。週末の間、Cisco CallManager に加入者の新しい内線番号を作成し、新しい IP Phone を適切なロケーションに配置して、月曜日の朝までに使用できるよう準備しました。すべての加入者を移行するまで、このプロセスを各ビルディングに対して繰り返しました。

フラッシュ カットオーバー（ビッグバン移行）

この方法は、完全な IP テレフォニー インフラストラクチャの実装から開始されます。完全な IP テレフォニー インフラストラクチャとは、冗長で、アベイラビリティが高く、QoS 対応のインフラストラクチャであり、インライン パワーが供給されるイーサネット ポートを装備しています。インフラストラクチャの完成後、IP テレフォニー アプリケーションを配置できます。加入者が自分のデスクに 2 台の電話機（IP Phone と PBX 電話機）を同時に置くことができるように、すべての IP Phone とゲートウェイを完全に設定および配置できます。この方法を使用すると、システムをテストする機会が得られ、加入者には新しい IP Phone に慣れるための時間が与えられます。発信専用トランクを IP テレフォニー システムに接続することもできます。これにより、加入者は、新しい IP Phone で内部コールだけではなく外部コールも発信できます。

IP テレフォニー システムを完全に配置した後、着信公衆網トランクを PBX から IP テレフォニー ゲートウェイに移動して新しいシステムの完全な運用を開始するための時間枠を選択できます。IP テレフォニー システムが正常に動作することを確信するまで PBX をそのまま残し、確信した時点で PBX を撤去することもできます。

フラッシュ カットオーバーは、段階的な移行に比べて次のような利点があります。

- 予期せぬ事態が発生した場合のために、フラッシュ カットオーバーでは、着信公衆網トランクを IP テレフォニー ゲートウェイから PBX に戻すだけで PBX システムに戻ることができるバックアウト計画が提供される。段階的な移行が 50% 進んでいる場合は、段階的な移行で同様の処置を試すよう検討することもできます。
- フラッシュ カットオーバーでは、システムによって実際の公衆網トラフィックが伝送される前に、IP テレフォニー データベースの設定を確認できる。このシナリオは、着信公衆網トランクを PBX から IP テレフォニー ゲートウェイに移動するカットオーバー前のどれだけの期間でも実行できるため、加入者情報、電話機、ゲートウェイ、ダイヤル プランなどすべての設定が正しいことを確認できます。
- 着信公衆網トランクのカットオーバー前の都合のよいときに、加入者が IP テレフォニー システムを調べたり使用したりできるようにして、ゆったりとしたペースでトレーニングを実施できる。
- システム管理者が「対象となるコミュニティ」に対して特別な準備をする必要がない。段階的な移行方法では、コール ピックアップ グループ、ハント グループ、シェアドラインなどの整合性を保つことを考慮する必要があります。フラッシュ カットオーバーでサイト全体を移行する場合は、これらのアソシエーションを簡単に保持できます。

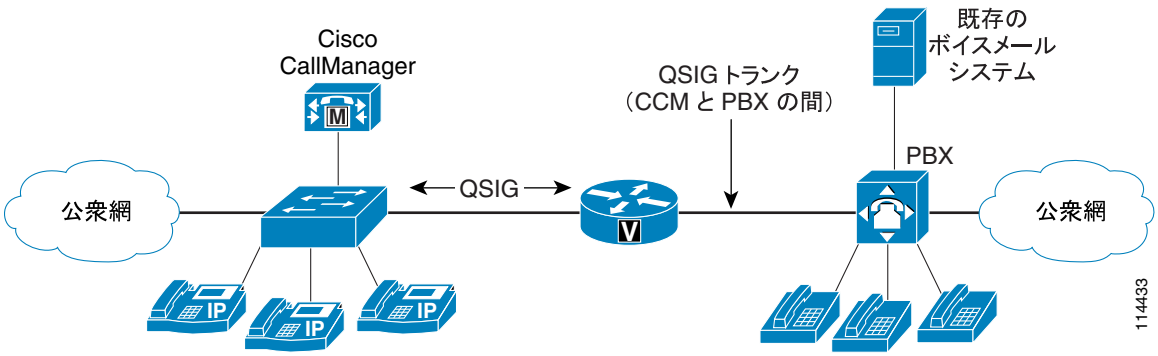
フラッシュ カットオーバーの 1 つの欠点は、システムの運用開始前にシステム全体を準備しておく必要があるため、最初から IP テレフォニー ソリューションに対する完全な資金供給が必要であるということです。これに対して、段階的な移行では、必要に応じてシステムの個々のコンポーネントを購入でき、完全な配置に移行する前に、小規模な試行システムから始めることができます。

マルチサイト企業における QSIG の必要性

1 つのロケーションだけで構成されている企業もありますが、多数のサイトで構成され、その一部のサイトが遠方に散在している企業もあります。マルチサイト企業の PBX ネットワークは、通常、Avaya DCS、Nortel MCDN、Siemens CorNet、NEC CCIS、Fujitsu FIPN、Alcatel ABC などの専用プロトコルを実行している T1 トランクまたは E1 PRI トランク（ロケーションに応じて異なる）を使用して接続されています。これらの専用ネットワーキング プロトコルによって、PBX は加入者間の高レベルの機能透過性を提供できます。

QSIG は異なるベンダーの PBX の相互接続を可能にするために開発されたため、同様のレベルの機能透過性を実現できます。シスコは、まず、Cisco CallManager Release 3.3 に QSIG を追加して、Cisco CallManager を大規模企業ネットワークに導入できるようにしました（図 15-2 を参照してください）。

図 15-2　Cisco CallManager と PBX の間で使用される QSIG



Cisco CallManager Release 4.0(1) で実装された QSIG に適用される特記事項は、次のとおりです。

- Cisco CallManager は、現在、エンドポイント Private Integrated Network eXchange（PINX）としてだけサポートされている。つまり、中継機能およびタンデム機能を持ちません。
- Cisco CallManager Release 4.0(1) は、宛先変更、転送、および Message Waiting Indicator（MWI; メッセージ待機インジケータ）機能のサポートを追加して、以前のリリースに基づいて作成されているため、集中ボイスメール配置が可能である。
- Cisco CallManager Release 4.0(1) の QSIG は、次の機能をサポートしている。
  - 基本的なコール
  - Direct Inward Dialing（DID; ダイヤルイン方式）
  - 発信番号
  - 着信番号
  - 接続名
  - 転送（参加による）
  - メッセージ待機表示（MWI）
  - 宛先変更（転送切り替えによる）
  - 発信者名の制限
  - 発信番号の制限

Cisco CallManager によって QSIG がサポートされるため、加入者間の機能透過性を保持しながら、Cisco CallManager を大規模な企業ネットワークに導入できます。いつでも都合のよいときに、PBX ロケーションを IP テレフォニーに変換できます。

ただし、PBX でまだ QSIG を有効にしていない場合、または QSIG の追加機能が特に必要でない場合は、短期間で PBX を撤廃すると、PBX のアップグレードのコストが正当化されにくくなることがあります。たとえば、2、3 か月で PBX を撤廃することを計画している場合に、PBX で QSIG を有効にするために 30,000 ドルを費やす理由はありません。

要約

どちらの移行方法も正常に機能するので、どちらの方法が正しいということはありませんが、ほとんどの場合はフラッシュ カットオーバー方法の方がうまくいきます。さらに、大規模な企業では、QSIG を使用して Cisco CallManager を企業ネットワークに導入することにより、どちらの移行方法も改良できます。

要約

CHAPTER 16

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。この章の目的は、テクノロジーに伴うリスクや利点について情報に基づいた選択ができるように、十分な情報を提供することです。リスク、利点、およびコストを慎重に考慮してから、任意のテクノロジーを配置してください。適切なセキュリティを達成するには、適切なセキュリティ ポリシーを確立し、そのセキュリティ ポリシーを適用する必要があります。また、ハッカーおよびセキュリティ コミュニティでの最新の動向を常に把握し、信頼性の高いシステム管理プラクティスによりすべてのシステムを保守および監視する必要があります。

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

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

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

セキュリティ 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。

Voice over IP（VoIP）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。

適切なセキュリティ 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。

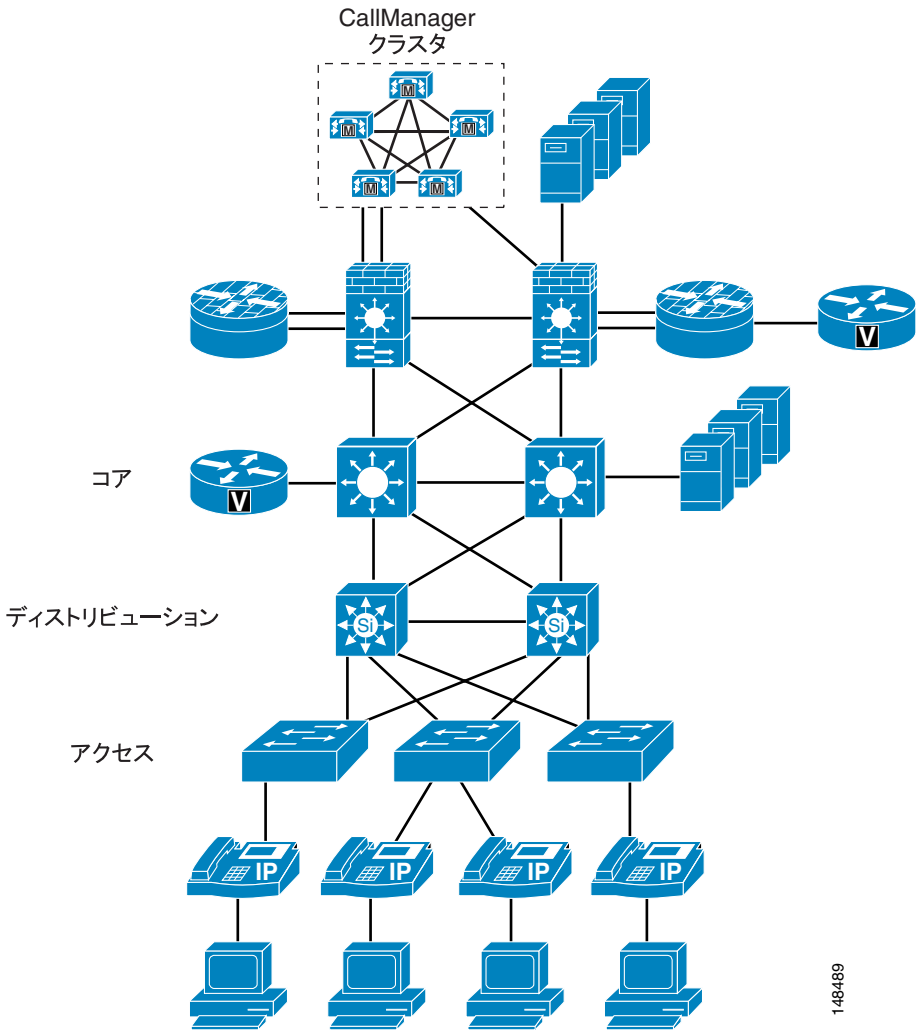
- ネットワーク上のデータを定義する。
- データの重要性を定義する。
- データの重要性に基づいてセキュリティを適用する。

セキュリティ レイヤ

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 16-1 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 16-1 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、VoIP アプリケーションを配置するのが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、VoIP デバイスを配置できるからです。

図 16-1　セキュリティ レイヤ



IP アドレッシング

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

このマニュアルの他の項で説明されているとおり（P.3-4 の「キャンパス アクセス レイヤ」を参照）、RFC 1918 に基づいた IP アドレッシングを使用する必要があります。このアドレッシング方式では、ネットワークの IP アドレッシングをやり直すことなく、IP テレフォニー システムをネットワークに配置できます。音声エンドポイントの IP アドレスは適切に定義されていて理解しやすいので、RFC 1918 を使用すると、ネットワーク内の制御をより適切に実行できます。すべての音声エンドポイントが 10.x.x.x. のネットワーク内でアドレッシングされていると、アクセス コントロール リスト（ACL）、およびこれらのデバイスが受信または送信するデータのトラックは単純になります。

利点

音声配置のために適切に定義された IP アドレッシング プランがあると、VoIP 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。

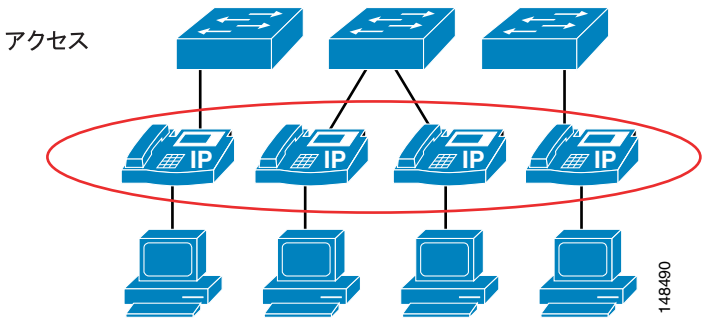
欠点

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 IP Phone には、VoIP 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、VoIP 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 16-2 を参照）。

図 16-2　電話機レベルでのセキュリティ



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

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuphne.htm

電話機の PC ポート

電話機には、通常、PC を接続するための電話機の背面のポートを、オンまたはオフにする機能があります。この機能は、そのタイプの制御が必要な場合に、ネットワークにアクセスするためのコントロール ポイントとして使用できます。

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

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

利点

電話機の PC ポートを無効にすると、電話機からネットワークへのアクセスを禁止する必要があるエリアに電話機を配置できます。これにより、電話機の背面の PC ポートが有効であればアクセス可能だったはずのネットワークへのアクセスが制御されます。

欠点

電話機の PC ポートが無効な場合、ネットワーク アクセスを必要としているユーザで、アクセスのための承認を得ているユーザごとに、ネットワーク アクセスを提供する個別のイーサネット ポートを追加する必要があります。ユーザは、イーサネット ジャックを電話機から切断し、別のデバイスに接続することを試行できます。

Gratuitous ARP

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

Gratuitous ARP は、攻撃者がネットワークの音声セグメントにアクセスできた場合に、攻撃者が電話機からのシグナリングや RTP 音声ストリームを取り込むことから電話機を保護するのに役立ちます。この機能で保護されるのは電話機だけです。インフラストラクチャの残りの部分は、Gratuitous ARP 攻撃から保護されません。スイッチ ポートには電話機とネットワーク デバイスの両方を保護する機能があるので、Cisco インフラストラクチャを実行している場合、この機能はそれほど重要ではありません。これらのスイッチ ポートの機能の説明については、P.16-12 の「スイッチ ポート」を参照してください。

利点

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

欠点

別の電話機から発信されたかネットワークを経由して到達するダウンストリーム シグナリングおよび RTP 音声ストリームは、電話機のこの機能では保護されません。保護されるのは、この機能が有効になっている電話機からのデータのみです（図 16-3 を参照）。

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

図 16-3　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

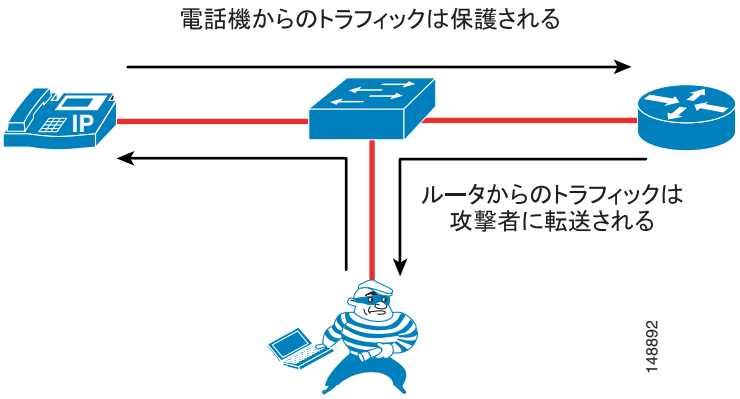


図 16-3 が示しているとおり、Gratuitous ARP 機能を持つ電話機からのトラフィックは保護されますが、エンドポイントに、データ フローを保護する機能がない可能性があるので、攻撃者が別のエンドポイントからのトラフィックを見ることができる場合があります。

PC Voice VLAN へのアクセス

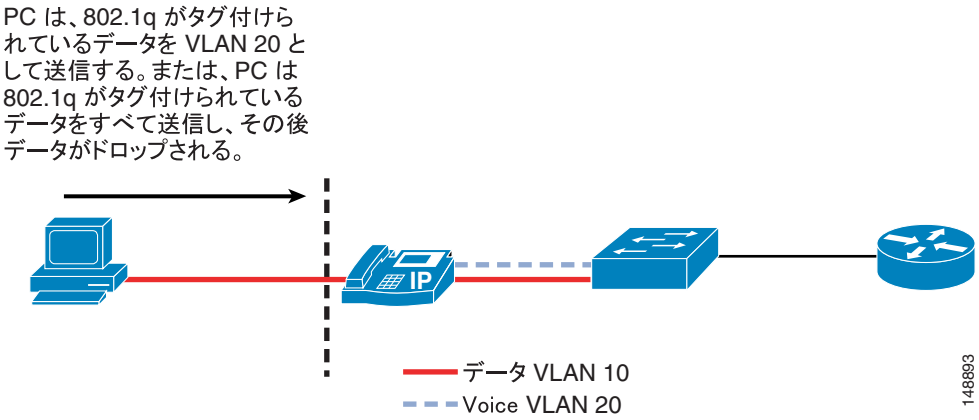
スイッチから電話機までに 2 つの VLAN が存在するので、電話機は、望まないアクセスから Voice VLAN を保護する必要があります。電話機では、電話機の背面から Voice VLAN に入り込む、望まないアクセスを防止できます。PC Voice VLAN Access 機能は、電話機の背面にある PC ポートから Voice VLAN への任意のアクセスを防止します。この機能を無効にすると、電話機の PC ポートに接続されたデバイスが、電話機の背面の PC ポートに到達する Voice VLAN を宛先とした 802.1q タグ付き情報を送信することにより、VLAN を「ジャンプ」して 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 16-4 に示す例の場合、PC が、電話機の PC ポートに対して Voice VLAN トラフィック（このケースでは 200 の 802.1q タグ付き）の送信を試行すると、そのトラフィックはブロックされます。この機能が動作する他の方法は、電話機の PC ポートに着信する、802.1q タグ付きのすべてのトラフィック（Voice VLAN トラフィックに限らない）をブロックする方法です。

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

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

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

図 16-4　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 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 CallManager から電話機にプッシュされたアプリケーションを受信するのを可能にします。この Web サーバへのアクセスは、Cisco CallManager 設定の Web Access 機能を使用して、電話機で有効または無効にできます。この設定は、グローバルで行うことも、電話機ごとに有効または無効にすることもできます。

利点

電話機の Web アクセスを有効にすると、電話機やネットワークの問題をデバッグするときにその電話機を使用できます。電話機からの Web アクセスを無効にすると、ユーザまたは攻撃者は、VoIP 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 VoIP の問題をデバッグするのがより困難になります。Web サーバがグローバルで無効だが、デバッグの参考として必要な場合、Cisco CallManager の管理者は、電話機のこの機能を有効にする必要があります。この Web ページにアクセスする機能は、ネットワークの ACL で制御できます。ネットワーク オペレータは、この機能を使用して、必要なときに Web ページにアクセスできます。

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

アクセス設定

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

このアクセスを電話機ごとに無効にすることにより（図 16-5 を参照）、エンド ユーザまたは攻撃者が、Cisco CallManager IP アドレスや TFTP サーバ情報などの追加情報を取得するのを防止できます。

電話機の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 IP Phone Authentication and Encryption for Cisco CallManager』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/ae/index.htm

図 16-5　Cisco CallManager の Phone Configuration ページ

利点

電話機設定ページへのアクセスを無効にすると、エンド ユーザおよび攻撃を仕掛けようとしている人が、ネットワークに関する詳細情報や音声システムで使用される VoIP 情報を見ることはできません。この機能を無効にしたときに保護される情報には、電話機の IP アドレス、電話機の登録先の Cisco CallManager、および電話機が最後に呼び出したデバイス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。

Voice VLAN および CDP

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。

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 が有効ではない場合、電話機のロケーションを判別するのは特に困難です。その場合、Cisco ER は 911 コールで電話機のロケーションを判別できません。

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。

電話機の認証および暗号化

Cisco CallManager では、音声システム内の電話機に対して複数のレベルのセキュリティを適用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 IP Phone モデルのサポート状況の詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/

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

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/

利点

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

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

欠点

Cisco CallManager は、メディア サービスが使用されていない単一クラスタにおける、2 つの Cisco IP Phone の間のコールの、認証、完全性、および暗号化をサポートしています。ただし、すべてのデバイスまたは電話機の認証、完全性、または暗号化を提供しているわけではありません。ご使用のデバイスがこれらの機能をサポートしているかどうかを判別するには、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/

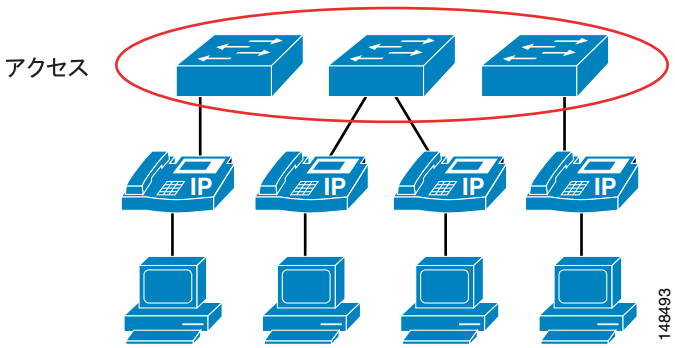
クラスタを混合モードで設定すると、自動登録は動作しません。混合モードは、デバイス認証に必要なモードです。クラスタにデバイス認証が存在しない場合、つまり、Cisco Certificate Trust List（CTL）クライアントがインストールおよび設定されていない場合、シグナリングまたはメディア暗号化を実装することはできません。VoIP がファイアウォールおよびネットワーク アドレス変換（NAT）を通過するのを可能にするアプリケーション レイヤ ゲートウェイ（ALG）も、シグナリング暗号化では動作しません。暗号化されたメディアでは、一部のゲートウェイ、電話機、または会議はサポートされません。

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。ここでは、ネットワーク内の VoIP 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 16-6 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 16-6　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 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 アドレスを 2 に設定できます（1 つは IP Phone 用、1 つは電話機の背後にあるワークステーション用）。以前であれば、トランク モードでポートを設定する旧来の方法により、この場合の設定は 3 つの MAC アドレスになります。電話機ポートの設定でマルチ VLAN アクセス モードを使用する場合、この場合の設定は 2 つの MAC アドレスになります。1 つは電話機用、1 つは電話機に接続された PC 用です。PC ポートに接続するワークステーションがない場合、そのポートの MAC アドレスの数は 1 に設定する必要があります。これらの設定は、スイッチ上のマルチ VLAN アクセス ポート用です。トランク モードに設定されているポート（電話機と PC が接続されているアクセス ポートでは推奨されていない配置）では、設定が異なる場合があります。

ポート セキュリティ：ポート アクセスの防止

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

この期間は、固定タイマーまたは非活動タイマー（非持続アクセス）のいずれかで決定するか、永続的に割り当てることができます。永続的に MAC アドレスを割り当てる機能は、Cisco 6000 スイッチでは*自動設定*と呼ばれ、Cisco Catalyst 4500、2550、2750、または 2950 スイッチでは*スティッキ*と呼ばれます。どちらの場合も、スイッチのリロードまたはリブートが発生しても、取得された MAC アドレスはポートで保持されます。

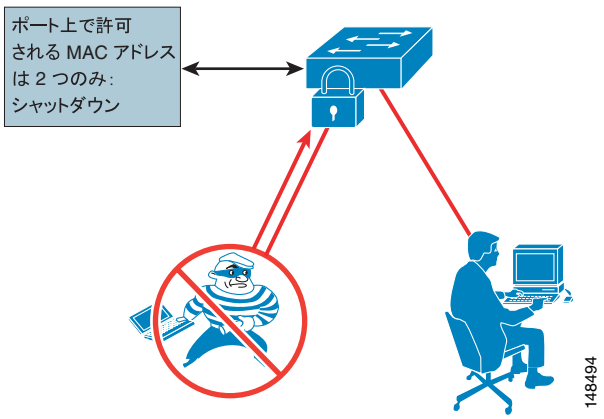
自動設定またはスティッキを使用した MAC アドレスの持続割り当ては、コマンドを使用してのみクリアできます。現在、Cisco Catalyst スイッチング プラットフォーム全体で最も一般的なデフォルト動作は、非持続動作です。この動作は、Cisco CatOS Release 7.6（1）が持続的になる前に、唯一有効だった動作です。デバイス モビリティに対し、静的ポート セキュリティまたは持続性のある動的ポート セキュリティによるプロビジョニングは行われません。最重要の要件ではありませんが、MAC フラッディング攻撃は、特定の MAC アドレスへのアクセスを制限することを目的としているポート セキュリティにより暗黙的に防止されます。

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

ポート セキュリティ：不良ネットワーク拡張の防止

ハブまたは無線アクセス ポイント（AP）を経由する不良なネットワーク拡張を防止します。ポート セキュリティは 1 つのポートでの MAC アドレスの数を制限するので、ポート セキュリティを、IT で作成されたネットワークへのユーザ拡張を抑制するためのメカニズムとして使用することもできます。たとえば、ユーザ方向のポート、または単一の MAC アドレス用にポート セキュリティが定義された電話機のデータ ポートに、ユーザが無線 AP を接続した場合、無線 AP 自体がその MAC アドレスを占有し、背後にあるデバイスはネットワークにアクセスできません。（図 16-7 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 16-7　MAC アドレス数の制限による不良ネットワーク拡張の防止



利点

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

欠点

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

設定例

（注） この設定例は、これらの機能をサポートするために適切なコード レベルを実行しているスイッチに基づいています。電話機へのトランク モードは実行されません。

次の例は、データ ポートにデバイスが接続されている電話機に対して、ダイナミック ポート セキュリティを使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

```
switchport access vlan 10
switchport mode access
switchport voice vlan 20
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

上記の例のコマンドは、次の機能を実行します。

- **switchport port-security** *x/x* **enable**
  このコマンドは、指定したモジュール / ポートでポート セキュリティを有効にします。

- **switchport port-security violation restrict**

  このコマンドが、推奨されている設定です。デフォルトでは、ポートを無効にします。ポートを **restrict** すると、ポートは、MAC アドレスの最大数に達するまで MAC アドレスを取得し、その後は新しい MAC アドレスの取得を停止します。ポートの設定がデフォルトの **disable** の場合、MAC アドレスの最大数に達すると、ポートはエラーを無効化し、電話機の電源を切ります。ポートを再有効化するデフォルト タイマーは、5 分です。導入済みのセキュリティ ポリシーによっては、ポートを無効にすることにより電話機をシャットダウンせずに、ポートを制限した方が適切な場合があります。

- **switchport port-security aging time 2**

  このコマンドは、MAC アドレスからのトラフィックがない状態で、その MAC アドレスをポートで保持する時間を設定します。一部のスイッチと電話機の間の CDP 通信を考慮に入れると、推奨されている最小時間は 2 分です。

- **switchport port-security aging type inactivity**

  このコマンドは、取得した MAC アドレスをタイムアウトするために、ポートで使用されるエージングのタイプを定義します。

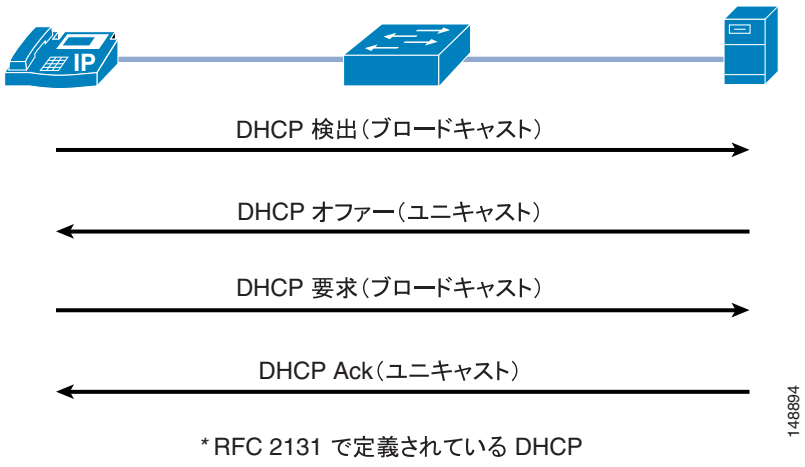
DHCP スヌーピング：不正な DHCP サーバ攻撃の防止

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

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

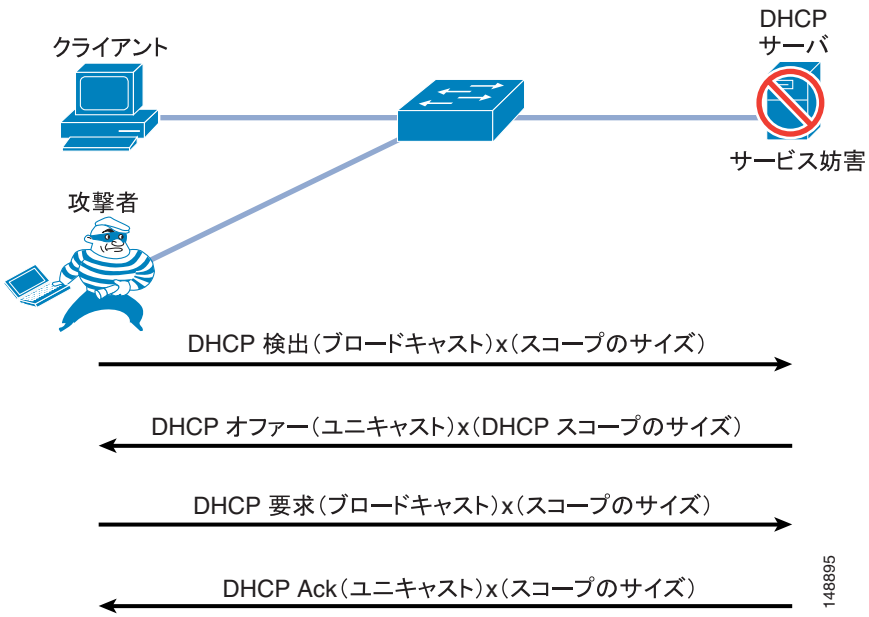
図 16-8 は、DHCP サーバから IP アドレスを要求するネットワーク接続デバイスの通常の操作を示しています。

図 16-8　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 16-9 を参照）。これは、ネットワークへのアクセスを試みている正当なデバイスのための IP アドレスが存在しないことを意味します。IP アドレスがないと、電話機は Cisco CallManager に接続できません。

図 16-9　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。

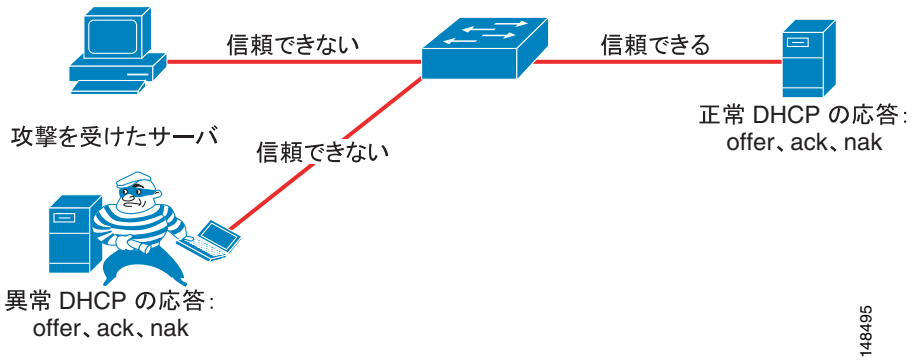
欠点

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 16-10 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 16-10　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 サーバが判断するかぎり、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 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。

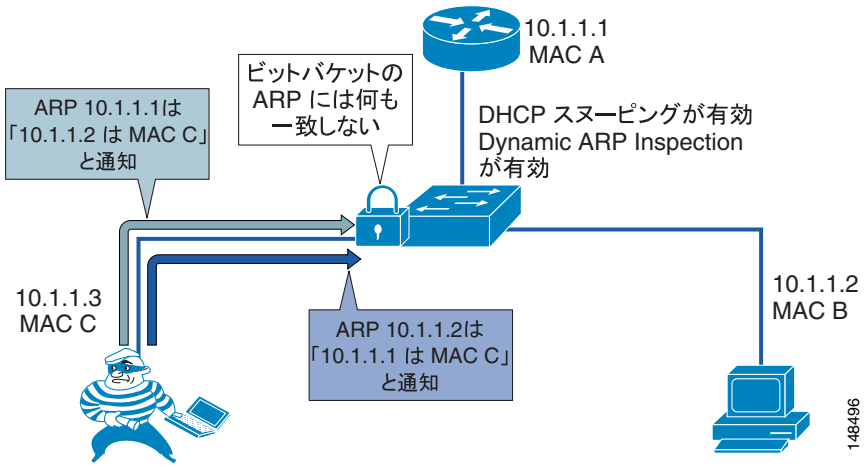
ただし、Gratuitous ARP は、別のステーションの身分を不正にかたること目的とした悪質なプログラムにより悪用される可能性もあります。悪質なステーションが、相互に通信しているその他の 2 つのステーションのトラフィックを自らにリダイレクトすると、GARP メッセージを送信したハッカーが中間者になります。ettercap などのハッカー プログラムは、このことを精密に行うため、GARP メッセージをブロードキャストするのではなく、「プライベートな」GARP メッセージを特定の MAC アドレスに発行します。これにより、攻撃の犠牲者は、自分のアドレスに対する GARP パケットを見ることができません。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 16-11 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 16-11　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 IP Phone でデフォルト ゲートウェイとのアクセス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、回線電源の代わりに電源アダプタを使用して Cisco IP Phone を使用している場合を想定します。この場合、リブートの後にスイッチがバックアップされると、電話機用の DHCP スヌーピング バインディング テーブル エントリが存在しないので、電話機はデフォルト ゲートウェイと通信できません。これを回避するには、DHCP スヌーピング バインディング テーブルのバックアップを取り、電話機からトラフィックが流れ始める前に古い情報をロードする必要があります。

利点

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

欠点

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

設定例

次の例は、DHCP スヌーピングおよび Dynamic ARP Inspection を使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

- グローバル コマンド

```
ip dhcp snooping vlan 10,20 (required)
no ip dhcp snooping information option (required without option 82 dhcp server)
ip dhcp snooping (required)
ip arp inspection vlan 10,20
ip dhcp snooping database tftp://172.26.168.10/tftpboot/cisco/ngcs-dhcpdb
```

- インターフェイス コマンド

```
ip dhcp snooping trust
ip arp inspection trust
no ip arp inspection trust (default)
ip arp inspection limit rate 15 (pps)
```

上記の例のグローバル コマンドは、次の機能を実行します。

- **ip arp inspection vlan 10,20**

  このコマンドは、Dynamic ARP Inspection（DAI）が有効になっている VLAN を特定します。

- **ip arp inspection trust**

  ip dhcp snooping trust と同様、このコマンドは、ルータなどの信頼済みデバイスが ARP メッセージに応答するのを許可します。このコマンドは、使用するルータ用のポートで設定する必要があります。そのように設定しないと、ルータは DHCP スヌーピング バインディング テーブルに含まれないので、ルータはいずれの ARP 要求にも応答できません。

- **no ip arp inspection trust**

  この設定は、VLAN 上のすべてのポートのデフォルト設定です。信頼を有効にする必要があります。

- **ip arp inspection limit rate 15 (pps)**

  このコマンドは、インターフェイス上の ARP メッセージで許可されている、1 秒当たりのパケット数の最大数のグローバル デフォルト値を設定します。この値を超えると、インターフェイスは有効になります。この動作が問題になる場合は、制限を増加または減少させるか、**none** に設定することができます。

- **ip dhcp snooping database tftp://172.26.168.10/tftpboot/cisco/ngcs-dhcpdb**

  このコマンドは、DHCP スヌーピング バインディング テーブルのバックアップを TFTP サーバに作成します。DHCP スヌーピング バインディング テーブルは、ブートフラッシュ、FTP、RCP、スロット 0、および TFTP にバックアップできます。

上記の例のインターフェイス コマンドは、次の機能を実行します。

- **no ip arp inspection trust**

  このコマンドは、ポート上で DAI を有効にし、DHCP スヌーピング バインディング テーブルを基にすべての ARP をチェックします。

- **ip arp inspection limit rate 15 (pps)**

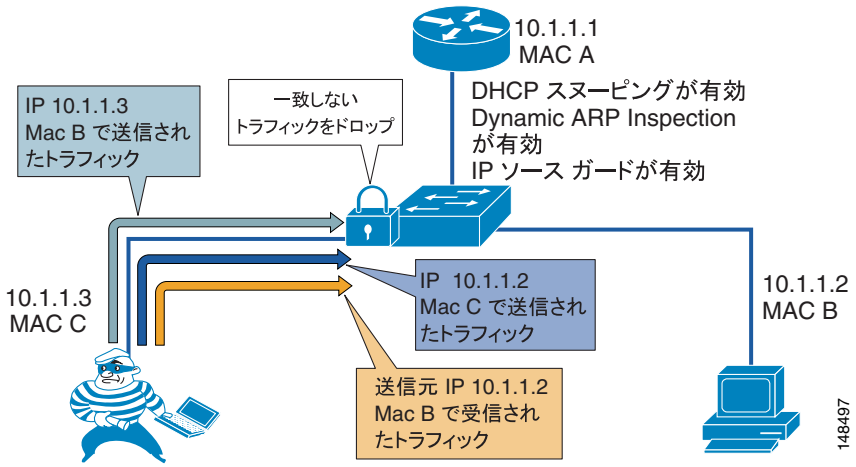
  このコマンドは、インターフェイス上の ARP メッセージで許可されている、1 秒当たりのパケット数の最大数を指定します。インターフェイスが、指定された数を超える ARP メッセージを 1 秒間に受信する場合、ポートは無効化されます。導入済みのセキュリティ ポリシーによっては、デフォルト値（15 pps）が最適な設定の場合があります。1 秒間に 15 個を超える ARP メッセージをポートが受信するときに電話機を無効化しない場合は、レート制限を **none** に設定できます。この設定では、電話機は有効なままです。

IP ソース ガード

ARP スプーフィングに加えて、攻撃者は IP アドレス スプーフィングも仕掛ける場合があります。この方法は、第二の当事者に対して DoS 攻撃を行うときに一般的に使用されます。この方法では第三の当事者を介してパケットが送信されるため、攻撃システムの ID がマスクされます。単純な例として、攻撃者は、攻撃先の第二の当事者の IP アドレスを送信元にしながら、サードパーティ システムに ping することがあります。ping の応答は、サードパーティ システムから第二の当事者に転送されます。スプーフィングされた IP アドレスを基にしたアグレッシブ SYN フラッディングは、サーバを TCP ハーフセッションで氾濫させる別の一般的なタイプの攻撃です。

IP ソース ガード（IPSG）機能を呼び出すと、DHCP スヌーピング バインディング テーブルの内容に基づいて ACL が動的に作成されます。この ACL は、トラフィックの送信元が DHCP バインディング時に発行された IP アドレスであることを保証し、スプーフィングされた他のアドレスによりトラフィックが転送されるのを防止します。DHCP スヌーピングは IP ソース ガードの前提条件ですが、DAI は前提条件ではありません。ただし、IP アドレス スプーフィングに加えて ARP ポイズニングおよび中間者攻撃を防止するため、IP ソース ガードだけでなく DAI も有効にすることをお勧めします（図 16-12 を参照）。

図 16-12　IP ソース ガードを使用したアドレス スプーフィングの防止



IP アドレス スプーフィングを使用すると、攻撃者は、アドレスを手動で変更するか、アドレス スプーフィングを行うように設計された hping2 などのプログラムを実行することにより、有効なアドレスになりすますことができます。インターネット ワームは、送信元を偽装するためスプーフィング技法を使用する場合があります。

設定例

次の例は、IP ソース ガードを使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

- IP ソース ガードを有効にする前に有効にする必要があるコマンド

```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
```

- インターフェイス コマンド：このコマンドは、DHCP Option 82 を指定せずに IP ソース ガードを有効にします。

```
ip verify source vlan dhcp-snooping
```

追加情報

ネットワーク セキュリティに関する追加情報については、次の Web サイトで入手可能な Cisco マニュアルを参照してください。

- http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper0900aecd8015f0ae.shtml
- http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008014870f.shtml

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。VoIP 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、第 3 章「ネットワーク インフラストラクチャ」、および次の Web サイトで入手可能な『*Enterprise QoS Solution Reference Network Design（SRND）Guide*』を参照してください。

http://cisco.com/go/srnd

利点

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

欠点

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

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、VoIP ネットワーク内で使用される各アプリケーションで電話機が正しく動作するようにするにはどのポートが必要かを検証する必要があります。通常、任意の VLAN ACL は、電話機が使用する VLAN に適用されます。これにより、アクセス ポートでのコントロールを、アクセス ポートに接続されているデバイスに近づけることができます。

必要なポートを判別するには、次の製品マニュアルを参照してください。

- Cisco Catalyst 3750 スイッチ
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225sed/scg/swacl.htm
- Cisco Catalyst 4500 シリーズ スイッチ
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_2_25s/conf/secure.htm
- Cisco Catalyst 6500 シリーズ スイッチ（Cisco IOS を実行）
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/acl.htm
- Cisco 6500 シリーズ スイッチ（Cisco CatOS を実行）
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_5/confg_gd/acc_list.htm

次の例は、Cisco 7960 IP Phone のトラフィックだけが VLAN でブートおよび機能するのを許可する、VLAN ACL を示しています（インライン コメントは、ACL の各行の目的を示しています）。この例の VLAN ACL は、Cisco CallManager Release 4.1 で使用するポート用です。この例では、次の IP アドレス範囲を使用します。

- 電話機の範囲は 10.0.20.*
- サーバの範囲は 10.0.10.*
- ゲートウェイの範囲は 10.0.30.*
- デフォルト ゲートウェイは 10.0.10.2 および 10.0.10.3
- DNS サーバの IP アドレスは 10.0.40.3

（注） 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。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 VoIP デバイスに適用されます。

```
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 49152 65535 10.0.20.0 0.0.0.255 eq tftp
70 permit udp 10.0.20.0  0.0.0.255 range 1024 5000 10.0.10.0 0.0.0.255 range 49152 65535
80 permit udp 10.0.10.0 0.0.0.255 range 49152 65535 10.0.20.0  0.0.0.255 range 1024 5000
!permit the tftp traffic from the tftp server and phone
90 permit udp 10.0.10.0 0.0.0.255 range 49152 65535 host 10.0.40.3 eq domain
100 permit udp host 172.19.244.2 eq domain 10.0.10.0 0.0.0.255 range 49152 65535
!permit DNS to and from the phone
110 permit tcp 10.0.10.0 0.0.0.255 range 49152 65535 10.0.20.0  0.0.0.255 eq 2000
120 permit tcp 10.0.20.0  0.0.0.255 eq 2000 10.0.10.0 0.0.0.255 range 49152 65535
!permit signaling to and from the phone.
130 permit udp 10.0.10.0 0.0.0.255 range 16384 32767 10.0.10.0 0.0.0.255 range 16384 32767
140 permit udp 10.0.0.0 0.0.255.255 range 16384 32767 10.0.10.0 0.0.0.255 range 16384 32767
150 permit udp 10.0.10.0 0.0.0.255 range 16384 32767 10.0.0.0 0.0.255.255 range 16384 43767
!permit all phones to send udp to each other
160 permit tcp 10.0.10.0 0.0.0.255 range 49152 65535 10.0.20.0  0.0.0.255 eq www
170 permit tcp 10.0.20.0  0.0.0.255 eq www 10.0.10.0 0.0.0.255 range 49152 65535
180 permit tcp 10.0.20.0  0.0.0.255 range 49152 65535 10.0.10.0 0.0.0.255 eq www
190 permit tcp 10.0.10.0 0.0.0.255 eq www 10.0.20.0  0.0.0.255 range 49152 65535
!permit web access to and from the phone
200 permit ICMP any any
!allow all icmp - phone to phone, gateway to phone, and NMS to phone
220 permit udp 10.0.30.0 0.0.0.255 rang 16384 327676 10.0.10.0 0.0.0.255 rang 16384 32767
!permit udp to the gateways in the network for pstn access
```

この ACL の例が示しているとおり、ネットワーク内で IP アドレスが適切に定義されているほど、ACL を書き出して配置するのが簡単になります。

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

- Cisco Catalyst 3750 スイッチ

  http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_guide_book09186a0080464bdc.html

- Cisco Catalyst 4500 シリーズ スイッチ

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_book09186a008011c8a5.html

- Cisco Catalyst 6500 シリーズ スイッチ（Cisco CatOS 対応）

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_5/confg_gd/

- Cisco Catalyst 6500 シリーズ スイッチ（Cisco IOS 対応）

  http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_book09186a00801609ea.html

利点

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

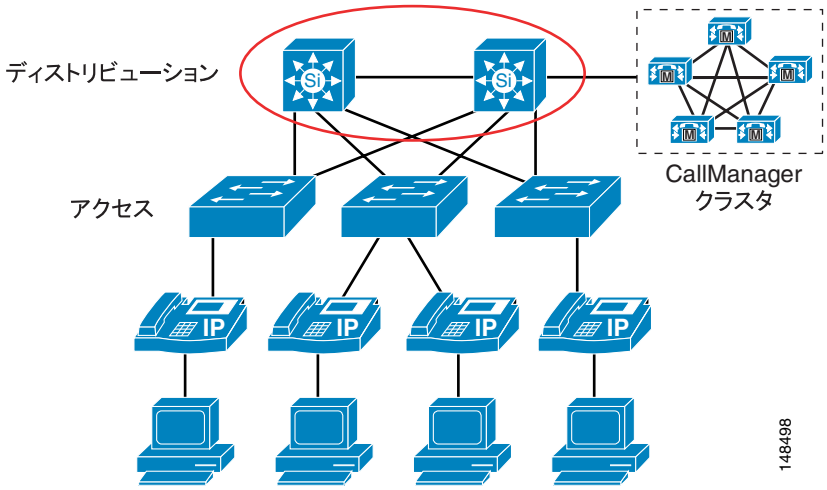
欠点

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

ルータのアクセス コントロール リスト

VLAN ACL と同様、ルータにも、ポートごとにインバウンド ACL およびアウトバウンド ACL の両方を処理する機能があります。最初のレイヤ 3 デバイスは、音声およびデータ VLAN を使用するときの音声データと別タイプのデータとの間の境界ポイントです。境界ポイントでは、2 つのタイプのデータが、相互にトラフィックを送信することが許可されます。VLAN ACL とは異なり、ルータ ACL は、ネットワーク内のすべてのアクセス デバイスには配置されません。その代わり、ネットワーク全体にルーティングするすべてのデータを準備する場所である、エッジ ルータで適用されます。これは、各 VLAN のデバイスがネットワーク内でアクセス可能なエリアを制御するために、レイヤ 3 ACL を適用するのに最適な場所です。レイヤ 3 ACL をネットワーク全体に配置することにより、トラフィックが収束する場所で、デバイスを相互に保護できます（図 16-13 を参照）。

図 16-13　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 VoIP 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を制御するという詳細な設定にもできます。ソフトフォンが導入されていないと仮定すると、Cisco CallManager 、音声ゲートウェイ、電話機、および音声専用サービスで使用される他の任意の音声アプリケーションに対する、すべてのトラフィック（IP アドレス別、または IP 範囲別）をブロックするための ACL を書き込むことができます。この方法により、レイヤ 3 ACL を、レイヤ 2 または VLAN ACL よりも簡素化できます。

この例では、次の IP アドレス範囲を使用します。

- 電話機の範囲は 10.0.20.*
- VoIP 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。

インフラストラクチャの保護

VoIP 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、VoIP 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。

次のリンクは、Cisco.com で入手可能なセキュリティ関連マニュアルをリストしています。

- Best Practices for Cisco Switches（ログイン認証が必要）

  http://cisco.com/en/US/partner/products/hw/switches/ps663/products_tech_note09186a0080094713.shtml
- SAFE：A Security Blueprint for Enterprise Networks

  http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b6.shtml

セキュリティの概要

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

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

- http://www.cisco.com/go/safe/
- http://www.cisco.com/web/about/ac123/iqmagazine/archives/q2_2005/addressing_network_security.html

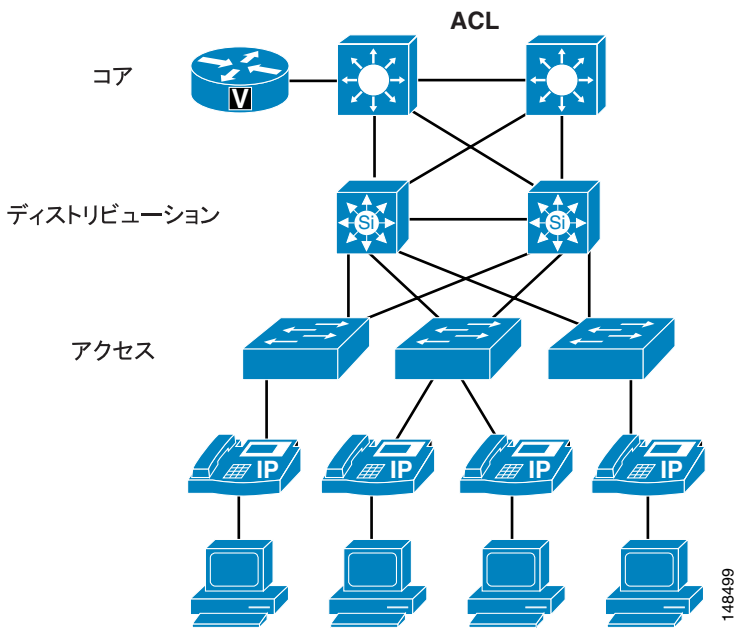
ゲートウェイおよびメディア リソース

ゲートウェイおよびメディア リソースは、VoIP コールを公衆網コールに変換するデバイスです。外部コールが配置された場合、ゲートウェイまたはメディア リソースは、VoIP 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。

VoIP 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、VoIP ゲートウェイまたはメディア リソースを保護することが、他のデバイスを保護することより難しいと見なされる場合があります。しかし、ネットワーク内のどこで信頼が確立されているかによりますが、ゲートウェイおよびメディア リソースを簡単に保護できる場合もあります。ゲートウェイおよびメディア リソースが Cisco CallManager により制御される方法が関係していますが、シグナリングがゲートウェイまたはメディア リソースに到達するために通るパスがネットワーク内で安全と見なされている部分にある場合、単純な ACL を使用して、ゲートウェイまたはメディア リソースに送る、またはそこから戻るシグナリングを制御することができます。ゲートウェイ（またはメディア リソース）と Cisco CallManager のロケーションの間のネットワークが安全と見なされない場合は（ゲートウェイがリモートの支店に置かれている場合など）、インフラストラクチャを使用してゲートウェイおよびメディア リソースへの IPSec トンネルを構築することにより、シグナリングを保護できます。ほとんどのネットワークでは、通常、2 つの方式（ACL および IPSec）の組み合せにより、これらのデバイスが保護されています。

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 16-14 を参照）。

図 16-14　IPSec、ACL、および QoS を使用したゲートウェイおよびメディア リソースの保護



電話機で SRTP が有効な場合、一部のゲートウェイおよびメディア リソースでは、ゲートウェイに対する Secure RTP（SRTP）および電話機からのメディア リソースがサポートされます。ゲートウェイまたはメディア リソースが SRTP をサポートしているかどうかを判別するには、次の Web サイトで入手可能な適切な製品マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_access/index.htm

IPSec トンネルの詳細については、次の Web サイトで入手可能な『*Site-to-Site IPSec VPN Solution Reference Network Design（SRND）*』を参照してください。

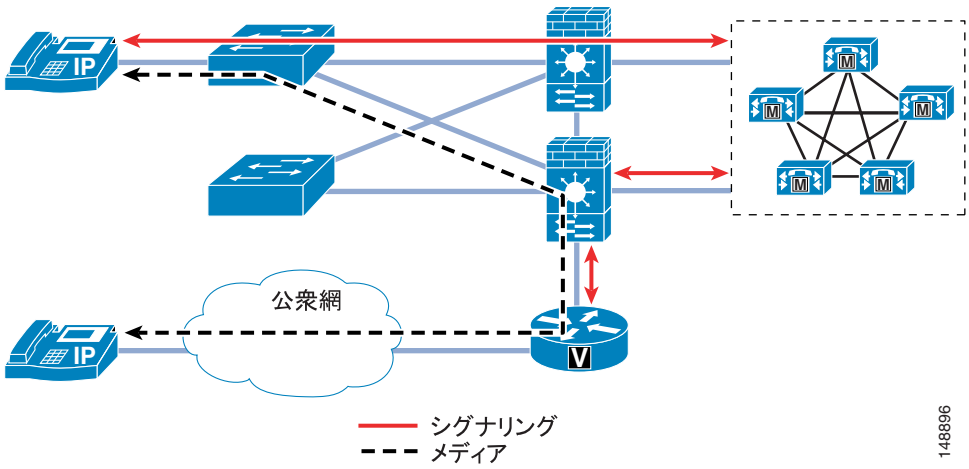
http://www.cisco.com/go/srnd

ゲートウェイの周囲へのファイアウォールの配置

コールの送信元である電話機と、公衆網ネットワークへのゲートウェイとの間にファイアウォールを配置する場合、注意が必要な問題が生じます。ステートフル ファイアウォールは、Cisco CallManager、ゲートウェイ、および電話機の間のシグナリング メッセージの内容を参照し、コールの実行を許可するための RTP ストリーム用のピンホールを開けます。通常の ACL で同じことを行うには、RTP ストリームで使用されるポート範囲全体を、ゲートウェイに対して開放する必要があります。

ネットワーク内にゲートウェイを配置する方法は 2 つあります。つまり、ファイアウォールの背後に配置する方法と、ファイアウォールの前面に配置する方法です。ゲートウェイをファイアウォールの背後に配置する場合、そのゲートウェイを使用している電話機からのすべてのメディアは、ファイアウォールを通過する必要があります。また、これらのストリームがファイアウォールを通過するようにするには、追加の CPU リソースが必要です。次に、ファイアウォールでは、これらのストリームの制御が追加され、ゲートウェイが DoS 攻撃から保護されます（図 16-15 を参照）。

図 16-15　ファイアウォールの背後に配置されたゲートウェイ



ゲートウェイを配置する 2 番目の方法は、ファイアウォールの外側に配置する方法です。電話機からゲートウェイに送信される唯一のデータ タイプは RTP ストリームなので、そのゲートウェイに送信可能な RTP トラフィックの量は、アクセス スイッチの QoS 機能により制御されます。Cisco CallManager からゲートウェイに送信されるのは、コールをセットアップするためのシグナリングだけです。ネットワーク内で、信頼できるエリアにゲートウェイが配置されている場合、Cisco CallManager とゲートウェイの間で許可する必要がある唯一の通信は、そのシグナリングです（図 16-15 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かぎり、Cisco CallManager が電話機とゲートウェイに対して、それらの 2 つのデバイスの間で使用するように指示している RTP ストリーム ポートだけが開放されます。また、ファイアウォールには、DoS 攻撃用の追加機能や、対象トラフィックを参照して、攻撃者が禁止動作を行っていないかどうかを判別するための Cisco Intrusion Detection System（IDS）シグニチャがあります。

欠点

P.16-33 の「ファイアウォール」の項で説明したとおり、ファイアウォールが、すべてのシグナリング、および電話機からゲートウェイへの RTP ストリームを参照する場合、キャパシティが問題になることがあります。また、音声データ以外のデータがファイアウォールを通過する場合、ファイアウォールを通過するコールがファイアウォールにより影響されないように、CPU 使用率を監視する必要があります。

アクティブまたはスタンバイ モードでは、Cisco Adaptive Security Appliance（ASA）および Cisco Private Internet Exchange（PIX）のフェールオーバー時間の最小設定は 3 秒です。Cisco Firewall Services Modules（FWSM）の最小タイマー設定も、3 秒です。引き継ぐ必要があるとスタンバイ ユニットが判別した場合、ファイアウォールでは、すぐにフェールオーバーが発生します。ステートフル フェールオーバーが設定されている場合、プライマリ ファイアウォールを通過するデータの状態は、フェールオーバー ユニットに渡されます。このようにして、フェールオーバーの前に実行されていたすべてのことが保持されます。しかし、プライマリ ユニットまたはそのユニットに対する接続性に全面的な障害が発生した場合、ゲートウェイにトラフィックが渡されない時間が、ASA または PIX の場合は 3 秒以上、FWSM の場合は 3 秒間発生します。つまり、ファイアウォールでのフェールオーバーを強要する、ある種類の障害が発生した場合、RTP ストリームは最低 3 秒間停止します。

ファイアウォール

ファイアウォールを ACL と組み合せて使用すると、VoIP 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。VoIP 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、VoIP 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。

VoIP ネットワークには、固有のデータ フローがあります。電話機はクライアント / サーバ モデルを使用してコール セットアップ用のシグナリングを生成し、Cisco CallManager はそのシグナリングを使用して電話機を制御します。VoIP 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。VoIP 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、VoIP 電話機、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 VoIP 電話機は影響を受け、進行中のコールの品質は低下し、新しいコールのコール セットアップは問題を抱えます。CPU 使用率が 60% を超えた状態が続くと、最悪の場合、電話機の登録解除が始まります。このことが発生すると、電話機は Cisco CallManager への再登録を試みるようになり、ファイアウォールの負荷はさらに増大します。この状態が発生すると、結果的に、登録解除と Cisco CallManager への再登録の試行を繰り返す電話機の連続ブラックアウトが発生します。ファイアウォールの CPU 使用率が継続的に 60% 未満に落ち着くまで、この連続ブラックアウトは続き、すべてまたはほとんどの電話機が影響を受けます。現在、ネットワーク内で Cisco ファイアウォールを使用している場合、ネットワークに VoIP トラフィックを追加するときは、トラフィックが悪影響を受けないように、CPU 使用率を注意深く監視してください。

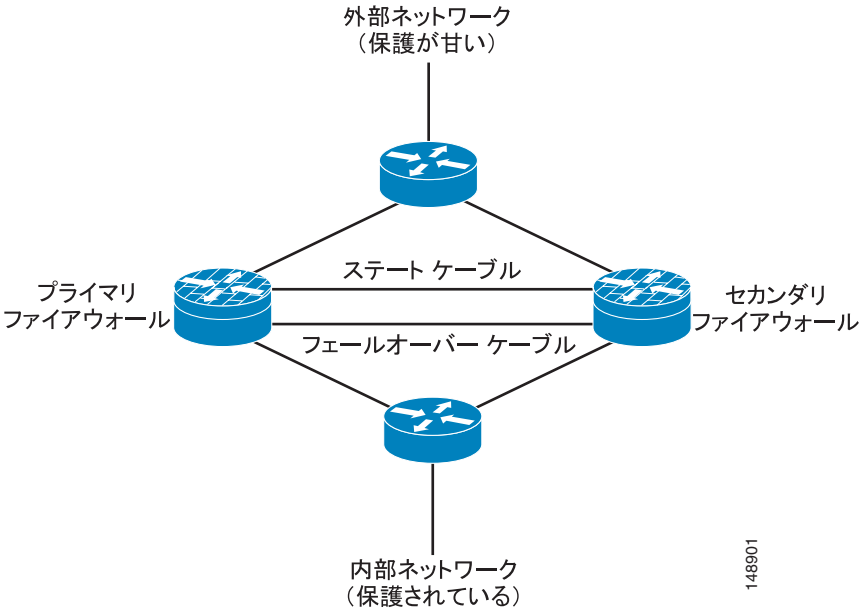
ファイアウォールを配置する方法はいくつもあります。この項では、ルーテッドおよび透過の両方のシナリオにおける、アクティブ / スタンバイ モードの ASA、PIX、および FWSM について集中的に説明します。この項で説明する各設定は、ファイアウォール設定の音声セクション内で、シングル コンテキスト モードで設定されたものです。

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

ASA または PIX と FWSM の機能性の相違点

図 16-16 は、ネットワーク内の冗長ファイアウォールを論理的に表現しています。配置方法は、ルーテッド設定と透過設定で同じです。

図 16-16　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 がないかぎり、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 16-17 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 16-18 を参照）。

図 16-17　Cisco ASA または PIX の機能

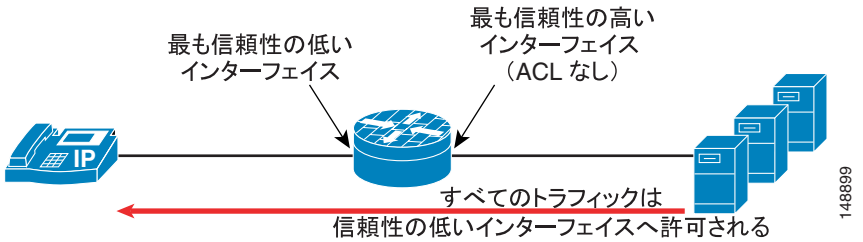
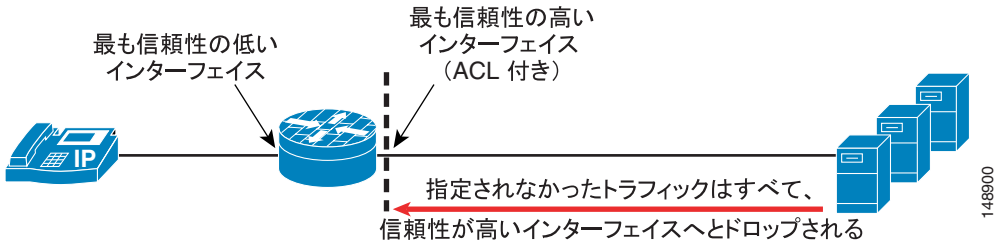


図 16-18　Cisco FWSM の機能



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、VoIP 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 VoIP 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、IPCC Enterprise、および IPCC 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。

バージョン 3.0 より前の Cisco FWSM では、SCCP フラグメンテーションがサポートされていません。電話機、Cisco CallManager、またはゲートウェイから別の VoIP デバイスに送信される SCCP パケットが断片化されている場合、断片化されたパケットが FWSM を通過するのは許可されません。断片化が、バージョン 2.*x* のコードを実行する FWSM で発生した場合、シグナリング トラフィック用のファイアウォールの ALG 機能を使用せずに、ACL を使用する必要があります。この設定では、FWSM を通過するシグナリング トラフィックが許可されますが、シグナリングがファイアウォールを通過するときにパケットの検査は実行されません。

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

http://www.cisco.com/univercd/cc/td/doc/product/ipcvoice.htm

ルーテッド ASA および PIX

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

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_70/config/index.htm

利点

ルーテッド ASA または PIX ファイアウォールは、QoS、NAT、およびボックスへの VPN 終端をサポートしています。これらの機能は、トランスペアレント モードではサポートされていません（P.16-36 の「トランスペアレント ASA および PIX」を参照）。

図 16-16 は、アクティブ スタンバイ モードのルーテッド設定と透過設定の両方における、ファイアウォールの論理配置を示しています。ルーテッド設定では、ASA または PIX 上の各インターフェイスに IP アドレスが与えられます。トランスペアレント モードでは、ASA または PIX をリモートで管理するための IP アドレスの他には、インターフェイス上に IP アドレスは与えられません。

欠点

トランスペアレント モードとは異なり、デバイスはネットワークで参照することができ、それが原因で攻撃ポイントになる場合があります。ルーティングの一部はファイアウォールで実行可能なため、ルーテッド ASA または PIX ファイアウォールをネットワークに配置すると、ネットワークのルーティングが変更されます。ファイアウォールに存在する、使用する予定のすべてのインターフェイスでは、IP アドレスも使用可能でなければなりません。そのため、ネットワーク内のルータの IP アドレスを変更する必要が生じる場合もあります。ASA または PIX ファイアウォールを経由してルーティング プロトコルまたは RSVP を許可する場合、トラフィックが外側（または信頼性の低い）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（または最も信頼性の高い）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かぎり、セキュリティ アプライアンスを通過できません。アクセス リストなしで許可されるトラフィックは、Address Resolution Protocol（ARP）トラフィックだけです。

利点

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

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

欠点

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

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

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

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_70/config/index.htm

ASA および PIX の設定例

次の設定例は、ファイアウォールが ASA および PIX ソフトウェア Release 7.04 の音声に対して動作するように設定するための、ポートおよび **inspect** コマンドをリストしています。これはあくまでも例にすぎません。任意のファイアウォールを配置する前に、ネットワーク内で使用されているすべてのアプリケーションから取得したポート リストを確認する必要があります。この設定例は、音声セクションのみを示しています。

```
!
!
object-group service remote-access tcp
 description remote access
 !Windows terminal
 port-object range 3389 3389
 !VNC
 port-object range 5800 5800
 !VNC
 port-object range 5900 5900
 port-object range 8080 8080
 port-object eq ssh
 !SSH
 port-object eq ftp-data
 !FTP data transport
  port-object eq www
 !HTTP Access
 port-object eq ftp
 !FTP
 port-object eq https
 !HTTPS Access
object-group service voice-protocols-tcp tcp
 description TCP voice protocols
 CTI/QBE
 port-object range 2428 2428
 !SIP communication
 port-object eq ctiqbe
 !SCCP
 port-object range 2000 2000
 !Secure SCCP
 port-object range 2443 2443
object-group service voice-protocols-udp udp
 !TFTP
 port-object eq tftp
 !MGCP Signaling
 port-object range 2427 2427
 !DNS
 port-object eq domain
 !RAS
 port-object range 1719 1719
 !SIP

!Object Group applied for remote-access
access-list OUTSIDE extended permit tcp any any object-group remote-access
!Object Group applied for voice-protocols-tcp
access-list OUTSIDE extended permit tcp any any object-group voice-protocols-tcp
!Object Group applied for voice-protocols-udp
access-list OUTSIDE extended permit udp any any object-group voice-protocols-udp
! Object Group applied for remote-access
access-list inside_access_in extended permit tcp any any object-group remote-access
! Object Group applied for voice-protocols-tcp
access-list inside_access_in extended permit tcp any any object-group
voice-protocols-tcp
! Object Group applied for voice-protocols-udp
access-list inside_access_in extended permit udp any any object-group
voice-protocols-udp

!Failover config
ip address 172.19.245.3 255.255.255.248 standby 172.19.245.4
failover
```

```
failover lan unit primary
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
!Lowest and fastest setting for failover
failover polltime interface 3
failover link failover_state GigabitEthernet0/2
failover interface ip failover 192.168.1.1 255.255.255.0 standby 192.168.1.2
failover interface ip failover_state 192.168.0.1 255.255.255.0 standby 192.168.0.2

!
!Default inspection with inspects enabled
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect h323 h225
  inspect h323 ras
  inspect skinny
  inspect sip
  inspect tftp
  inspect mgcp
```

FWSM ルーテッド モード

ルーテッド モードでは、FWSM がネットワークのルータ ホップと見なされます。このモードでは、接続されているネットワークの間で NAT が実行されます。また、OSPF またはパッシブ RIP（シングル コンテキスト モード）を使用できます。ルーテッド モードでは、コンテキストあたり最大 256 個のインターフェイスがサポートされています。シングル モードでは、すべてのコンテキストに分割された最大 1,000 個のインターフェイスがサポートされています。

利点

ネットワーク内のルーテッド デバイスとして、FWSM は、ルーティング機能、およびトランスペアレント モードで使用可能でない他のすべての機能をサポートしています。

欠点

トランスペアレント モードとは異なり、ルーテッド デバイスはネットワーク上で参照することができ、それが原因で攻撃ポイントになる場合があります。ネットワークにデバイスを配置するには、IP アドレッシングとルーティングの設定を変更する必要があります。

FWSM トランスペアレント モード

トランスペアレント モードでは、FWSM は「Bump In The Wire」または「ステルス ファイアウォール」として動作し、ルータ ホップではありません。FWSM はインターフェイスの内側と外側で同じネットワークに接続しますが、各インターフェイスは異なる VLAN に置かれている必要があります。ダイナミック ルーティング プロトコルまたは NAT は必要ありません。ただし、ルーテッド モードと同様、トランスペアレント モードでも、トラフィックの通過を許可する ACL が必要です。トランスペアレント モードでは、オプションで EtherType ACL を使用して、非 IP トラフィックを許可することもできます。トランスペアレント モードでは、内側インターフェイスと外側インターフェイスの 2 つのインターフェイスのみがサポートされています。

透過ファイアウォールを使用すると、ネットワーク設定を簡素化できます。トランスペアレント モードは、ファイアウォールを攻撃者から見えないようにするためにも便利です。ルーテッド モードではブロックされるトラフィックのために、透過ファイアウォールを使用することもできます。たとえば、透過ファイアウォールで、EtherType ACL を使用したマルチキャスト ストリームを許可できます。

利点

この設定には、ファイアウォールがルーティングを一切行わないため、攻撃者がファイアウォールを見つけることができないという利点があります。この設定では、ファイアウォールに合せてルーティングを変更する必要がないので、より簡単に既存のネットワークにファイアウォールを配置できます。またこの設定は、ファイアウォール内でいずれのルーティングも行わないため、ファイアウォールの管理やデバッグも簡単に実行できます。また、非 IP トラフィックと IP マルチキャスト トラフィック、静的 ARP インスペクション、および MAC 移動検出と静的 MAC をブリッジできます。

欠点

トランスペアレント モードでフェールオーバーを使用するときにループを回避するには、Bridge Port Data Unit（BPDU）転送をサポートしているスイッチ ソフトウェアを使用し、BPDU を許可するように FWSM を設定する必要があります。トランスペアレント モードでは、NAT、ダイナミック ルーティング、またはユニキャストのリバース パス フォワーディング（RPF）チェックはサポートされていません。トランスペアレント モードの FWSM に NAT 0 はありません。

FWSM の設定例

次の設定例では、ファイアウォールを FWSM ソフトウェア ReleaseRelease 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 CCM 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、セキュリティ ポリシーを使用して、VoIP アプリケーション サーバで必要なセキュリティを定義する必要があります。Cisco VoIP サーバは IP に基づいているので、データ センター内で、他にある時間に敏感なデータに適用するセキュリティを、これらのサーバに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セキュリティ ポリシーに、Cisco VoIP 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 アプリケーション用に適切なデータ センター セキュリティを設計するには、次の Web サイトで入手可能な『*Data Center Networking:Server Farm Security SRND*』（『*Server Farm Security in the Business Ready Data Center Architecture*』）のガイドラインに従うことをお勧めします。

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

アプリケーション サーバ

Cisco CallManager セキュリティ機能のリスト、および有効にする方法については、次の Web サイトで入手可能な『*Cisco CallManager Security Guide*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/ipp7960/sec_vir/sec413/index.htm

任意の Cisco CallManager セキュリティ機能を有効にする前に、それらの機能が、ネットワーク内のこれらのタイプのデバイスに関する企業セキュリティ ポリシーで指定されている、セキュリティ要件を満たしていることを確認してください。

Cisco CallManager およびアプリケーション サーバ上の Cisco Security Agent

Cisco Security Agent は、VoIP および VoIP サービスを提供するのにシスコが使用する、ほとんどのアプリケーション サーバで使用されています。Cisco Security Agent ソフトウェアは、サーバとの間のトラフィックの動作と、サーバ上でアプリケーションが実行される方法を調べて、すべてが正常かどうかを判別する、ホスト侵入防御ソフトウェアです。異常と見なされるものが見つかった場合、Cisco Security Agent ソフトウェアはそのアクティビティが発生するのを阻止します。たとえば、Cisco CallManager にソフトウェア パッケージをインストールすることを試みるウイルスがあり、そのような事態が以前発生したことがない場合でも、ウイルスがインストールを実行することは阻止されます。ただし、Cisco Security Agent は感染を防止するだけで、一度感染したサーバをクリーンにすることはできないので、サーバにはアンチウイルス ソフトウェアが引き続き必要です。

Cisco CallManager サーバでの Cisco Security Agent の実行に関する追加情報は、次の Web サイトで入手可能です。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/index.htm

マネージドではない Cisco Security Agent

シスコは、自社サーバ用のデフォルト Cisco Security Agent ポリシーを開発しました。このポリシーにより、VoIP 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 VoIP サーバに影響することは防止されます。最低でも、このマネージドではないバージョンの Cisco Security Agent をインストールおよび実行する必要があります。このソフトウェアは、アプリケーションとオペレーティング システムを、ウイルスやワーム攻撃から保護します。これらのタイプの侵入からの最大限の保護を得るには、常に最新バージョンの Cisco Security Agent ソフトウェアがサーバにインストールされていることを確認してください。マネージドではないエージェントがサーバにインストールされていると、攻撃のログは、エージェントがインストールされているシステムでのみ参照できます。特定のタイプのアラームが発生したので書き込まれた可能性があるログ ファイルをチェックするには、各システムにログインする必要があります。

利点

マネージドではない Cisco Security Agent は、既知および不明の攻撃、ワーム、およびウイルスから各システムを保護します。

欠点

Cisco Security Agent を管理対象外モードで実行すると、アラームは相関されません。システムのログ ファイルを参照するには、各システムに個別にアクセスする必要があります。マネージドではない Cisco Security Agent をアップグレードする場合、新しいクライアントをインストールした後、通常は、クライアント設定を有効にするためシステムをリブートする必要があります。何らかの理由によりシステムが感染した場合、Cisco Security Agent は、そのシステムをクリーンにすることはできません。セキュリティを保持し、システムを保護するには、システムでアンチウイルス ソフトウェアも実行する必要があります。

マネージド Cisco Security Agent

マネージド Cisco Security Agent は、管理対象外バージョンと同じように動作しますが、管理コンソールに、追加の利点がいくつかあります。管理対象システムを実行すると、すべてのシステムからのすべてのアラームを 1 つのコンソールで受信できます。また、この機能では、異常な状態が重大なレベルに達したときに、そのことを電子メールまたはポケットベルで通知するように設定できます。

利点

マネージド Cisco Security Agent では、マネージドではないシステムと同じ保護が提供されるだけでなく、エージェントの制御も行うことができます。この制御により、アップデート時にシステムに負荷をかけることなく、イベントの相関、管理コンソールへのグローバル レポートの返信、エージェントの Cisco Security Agent 設定のアップグレードを実行できます。

欠点

別個のサーバに、管理対象エージェントのグローバル モニタリングと設定用の別々のソフトウェアが必要です。何らかの理由によりシステムが感染した場合、Cisco Security Agent は、そのシステムをクリーンにすることはできません。セキュリティを保持し、システムを保護するには、システムでアンチウイルス ソフトウェアも実行する必要があります。

アンチウイルス

ソフトウェアを実行することが承認されているすべての IP テレフォニー サーバおよび VoIP アプリケーション サーバで、承認済みのアンチウイルス ソフトウェアを実行する必要があります。ネットワーク内の他のサーバと同様、アンチウイルス ソフトウェアは、コールの処理に影響するワームやウイルスの感染から、Cisco CallManager サーバを保護します。Cisco Security Agent はシステムの感染をクリーンにできないので、Cisco Security Agent 以外の防御ソフトウェアもシステムにインストールする必要があります。感染したシステムをクリーンにできるのはアンチウイルス ソフトウェアのみです。

Cisco CallManager サーバでのアンチウイルス ソフトウェアの実行に関する追加情報は、次の Web サイトで入手可能です。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/index.htm

利点

アンチウイルス ソフトウェアは、アプリケーション サーバが感染して、パフォーマンスが低下するのを防止するのに役立ちます。

欠点

アンチウイルス ソフトウェアの管理には、いくらかのオーバーヘッドが含まれます。さらに、Cisco CallManager および VoIP アプリケーション サーバへのインストールで、ソフトウェアのバージョンが承認されていることを確認する必要があります。

サーバに関する一般的なガイドライン

Cisco CallManager およびその他の VoIP アプリケーション サーバは、通常のサーバとして扱わないでください。システムの設定時に行う任意の操作が、開始を試みているコール、または進行中のコールに影響する場合があります。他のビジネスクラス アプリケーションと同様、大規模な設定の変更は、電話の会話を遮断することがないようメンテナンス ウィンドウで行う必要があります。

アプリケーション サーバ用の標準的なセキュリティ ポリシーは、VoIP 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。VoIP 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、VoIP 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、VoIP サーバで行うことはできません。

また、シスコは VoIP サーバ用に適切に定義されたパッチ システムを提供しています。IT 組織内のパッチ ポリシーに基づいて、このパッチ システムを適用する必要があります。シスコシステムズにより承認されている場合を除き、OS ベンダーのパッチ システムを使用する通常の方法でシステムにパッチを適用しないでください。すべてのパッチは、シスコシステムズの指示に従ってシスコまたは OS ベンダーからダウンロードし、パッチ インストール プロセスに応じて適用する必要があります。

Cisco CallManager 用に OS を強化する方法の詳細は、Cisco CallManager サーバの C:\Utils\SecurityTemplates ディレクトリにリストされています。導入済みのセキュリティ ポリシーで、デフォルト インストールで提供された以上の OS のロック ダウンが要求されている場合は、OS の強化手法を使用する必要があります。

さまざまなソフトウェア パッチが、次の Web サイトで入手可能です。

http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

(注)　このリンクにアクセスするには、Cisco.com ログイン アカウントが必要です。

上記のサイトには、VoIP サーバに重要なパッチを適用する必要が生じたときに電子メールで通知する通知ツールも含まれています。

利点

アプリケーション サーバを他のアプリケーション サーバのようではなく PBX のように扱う場合、一般的なサーバ セキュリティ プラクティスを実施すると、ウイルスやワームを減らすのに役立ちます。

欠点

追加のセキュリティ機能を設定すると、一部の Cisco CallManager 機能が低下する場合があります。また、アップグレードを正常に実行するには、追加のセキュリティで無効になっている一部のサービスを有効にする必要があるため、アップグレード中は特に注意が必要です。

ロビーに設置された電話機の例

この項の例は、物理的なセキュリティが低いロビー エリアのようなエリアで使用する、電話機およびネットワークを設定する 1 つの方法を示しています。この例に出てくる機能は、いずれもロビーに設置する電話機で要求されている機能ではありませんが、導入済みのセキュリティ ポリシーで、より強固なセキュリティが必要とされている場合は、この例でリストされている機能を使用できます。

いずれのユーザも電話機の PC ポートからネットワークにアクセスできないようにするため、電話機の背面の PC ポートを無効にして、ネットワーク アクセスを制限する必要があります（P.16-5 の「電話機の PC ポート」を参照）。また、攻撃を仕掛けようとしている人が、ロビーに設置された電話の接続先ネットワークの IP アドレスを参照できないように、電話機の設定ページも無効にする必要があります（P.16-9 の「アクセス設定」を参照）。電話機の設定を変更できないという欠点は、通常、ロビーに設置された電話機では問題になりません。

ロビーに設置された電話機が移動される可能性は非常に低いため、電話機には固定 IP アドレスを使用できます。固定 IP アドレスを使用すると、攻撃者が電話機を切断して接続することにより新しい IP アドレスを取得するのを防止できます（P.16-4 の「IP アドレッシング」を参照）。また、電話機を切断すると、ポートの状態が変化し、電話機は Cisco CallManager から登録解除されます。ロビーに設置された電話機のポートでこのイベントをトラッキングするだけで、だれかがネットワークへの接続を試行しているかどうかを判別できます。

電話機の静的ポート セキュリティを使用し、MAC アドレスを取得することを許可しない場合、攻撃者は、そのアドレスを発見できたときに、自らの MAC アドレスをその電話機の MAC アドレスに変更しなければなりません。動的ポート セキュリティを無制限タイマーと共に使用して、MAC アドレスを取得する（取得したアドレスは解除しない）場合、MAC アドレスを追加する必要はありません。これにより、電話機を交換しないかぎり、MAC アドレスをクリアするためにスイッチ ポートを変更せずにすみます。MAC アドレスは、電話機の底面のラベルにリストされています。MAC アドレスをリストすることがセキュリティの問題と見なされる場合は、ラベルを除去し、デバイスを識別するための「ロビー用」というラベルに置き換えることができます（P.16-12 の「スイッチ ポート」を参照）。

ポートまたはポートが接続されているスイッチに関する情報を攻撃者がイーサネット ポートから参照できないように、単一の VLAN を使用し、ポートで Cisco Discovery Protocol（CDP）を無効にできます。この場合、電話機の E911 緊急コール用のスイッチに CDP エントリは与えられません。緊急番号をダイヤルするときは、ロビーに設置された各電話機に、ラベル、またはローカル セキュリティ用の情報メッセージのいずれかが必要です。

ポート上に DHCP は存在しないため、DHCP スヌーピング バインディング テーブルに静的エントリを定義できます（P.16-15 の「DHCP スヌーピング：不正な DHCP サーバ攻撃の防止」を参照）。DHCP スヌーピング バインディング テーブルに静的エントリを定義すると、VLAN で Dynamic ARP Inspection を有効にして、攻撃者が、ネットワーク上のレイヤ 2 ネイバーの 1 つに関する他の情報を取得するのを防止できます（P.16-19 の「Dynamic ARP Inspection の要件」を参照）。

DHCP スヌーピング バインディング テーブルに静的エントリが定義されていると、IP ソース ガードを使用できます（P.16-22 の「IP ソース ガード」を参照）。攻撃者が MAC アドレスと IP アドレスを取得でき、パケットの送信を開始した場合、正しい IP アドレスが設定されたパケットだけを送信できます。

電話機が動作するのに必要なポートと IP アドレスのみを許可する、VLAN ACL を書き込むことができます（P.16-25 の「VLAN アクセス コントロール リスト」を参照）。次の例には、ネットワークへのアクセスを制御するための、レイヤ 2 または最初のレイヤ 3 デバイスのポートに適用可能な非常に小規模な ACL が含まれています（P.16-27 の「ルータのアクセス コントロール リスト」を参照）。この例は、ロビー エリアで使用されている Cisco 7960 IP Phone に基づいています。電話機への Music on Hold または電話機からの HTTP アクセスは使用しません。

この例では、次の IP アドレス範囲を使用します。

- ロビーに設置された電話機の IP アドレスは 10.0.40.5
- Cisco CallManager クラスタのアドレス範囲は 10.0.20.*
- DNS サーバの IP アドレスは 10.0.30.2
- HSRP ルータの IP アドレスは 10.0.10.2 および 10.0.10.3
- ネットワーク内の他の電話機の IP アドレスの範囲は 10.0.*.*

```
10 permit icmp any any
! Allow all icmp - phone to phone, gateway to phone and NMS to phone

20 permit udp host 10.0.10.2 eq 1985 any
!Allow HSRP information in, do not allow out

30 permit udp host 10.0.10.3 eq 1985 any
! Allow in from HSRP neighbor

40 permit udp host 10.0.40.5 range 49152 65535 10.0.20.0 0.0.0.255 eq tftp
! Using ip host from ephemeral port range from phone to the TFPT server  port 69
(start of tftp)

50 permit udp 10.0.20.0 0.0.0.255 range 1024 5000 host 10.0.40.5 range 49152 65535
!Using IP subnet from TFTP server with ephemeral port range to ip host and ephemeral
port range for phone

60 permit udp host 10.0.40.5 range 49152 65535 10.0.20.0 0.0.0.255 range 1024 5000
! Using host from phone to TFTP server with ephemeral port range to ip range and
ephemeral port range for TFTP (continue the TFTP conversation)

70 permit udp host 10.0.40.5 range 49152 65535 host 10.0.30.2 eq domain
! Using IP host and ephemeral port range from phone to DNS server host

80 permit udp host 10.0.30.2 eq domain host 10.0.40.5 range 49152 65535
! Using IP from DNS server to phone host ip and ephemeral port range

90 permit tcp 10.0.40.5 range 49152 65535 10.0.20.0 0.0.0.255 eq 2000
! Using IP host and ephemeral port range from phone to CCM cluster for SCCP


100 permit tcp 10.0.20.0 0.0.0.255 eq 2000 host 10.0.40.5 range 49152 65535
! Using IP range and SCCP port to phone IP host and ephemeral port range


110 permit udp 10.0.0.0 0.0.255.255 range 16384 32767 host 10.0.40.5 range 16384 32767
! Using IP range and ephemeral port range from all phones or gateways outside a vlan
to the IP host to phone

120 permit udp host 10.0.40.5 range 16384 32767 10.0.0.0 0.0.255.255 range 16384 43767
! Using IP host and ephemeral port range from vlan to all other phones or gateways

130 permit udp host 172.19.244.3 range 1024 5000 host 10.0.40.5 eq snmp
!From IP host of NMS server and ephemeral port range (Different for Windows vs Sun) to
IP host of phones and SNMP port (161)

140 permit udp host 10.0.40.5 eq snmp host 172.19.244.3 range 1024 5000
! From IP host of phone with SNMP port (161) to IP host of NMS server and ephemeral
port range
```

ロビーに設置された電話機用の基本的な QoS の例

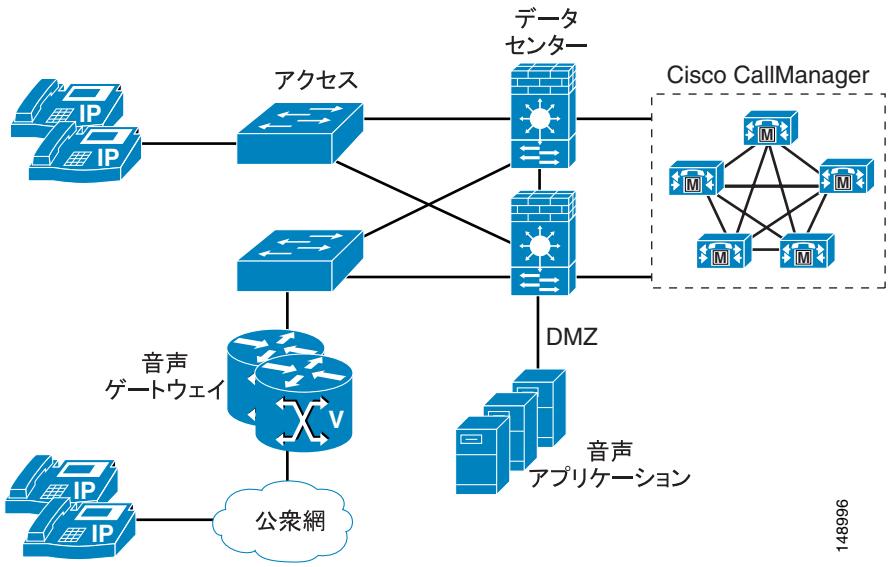
音声ストリームを G.729 に設定し、ポートに送信可能なトラフィックの量を、QoS を使用して制限します（P.16-24 の「QoS」を参照）。QoS 最大値を超えても、トラフィックは、一般的な企業ネットワークで優先度が最低のトラフィックである CS1 つまり Scavenger Class にリセットされます。

```
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、Cisco CallManager が背後に配置されているデータ センター内に、ファイアウォールを配置する 1 つの方法を示しています（図 16-19）。この例では、Cisco CallManager は、ファイアウォールの外側のすべての電話機が 1 つのクラスタに含まれる集中型配置に置かれています。この配置内のネットワークには、社内データ センター内でルーテッド モードで設定されたファイアウォールがすでに含まれているので、ゲートウェイの配置を決定する前に負荷が確認されます。ファイアウォールの平均的な負荷を確認した後、CPU に対するファイアウォールの負荷を 60% 未満に保つため、すべての RTP ストリームがファイアウォールを横断しないようにすることが決定されました（P.16-31 の「ゲートウェイの周囲へのファイアウォールの配置」を参照）。ゲートウェイはファイアウォールの外側に配置されています。Cisco CallManager とゲートウェイの間の TCP データ フローを制御するため、ネットワーク内の ACL を使用します。電話機の IP アドレスは適切に定義されているので、ACL は、電話機からの RTP ストリームを制御するためネットワークにも書き込まれます（P.16-4 の「IP アドレッシング」を参照）。音声アプリケーション サーバは非武装地帯（DMZ）に配置されています。Cisco CallManager との間のアクセス、およびネットワーク上のユーザへのアクセスを制御するため、ファイアウォールで ACL を使用します。この設定では、インスペクションを使用してファイアウォールを通過する RTP ストリームの量を制限します。これにより、既存のネットワークに新しい音声アプリケーションを追加したときの、ファイアウォールに対する影響を最小に抑えられます。

図 16-19　ファイアウォールの配置例



まとめ

この章では、ネットワーク内の音声データを保護するために有効にできるセキュリティのうち、一部のみを取り上げました。ここで取り上げた手法は、ネットワーク内のすべてのデータを保護するためにネットワーク管理者が使用できる、すべてのツールのサブセットにすぎません。逆に、ネットワーク全体のデータで必要なセキュリティのレベルによっては、これらのツールでさえ、ネットワークで有効にする必要がない場合もあります。セキュリティの方法は、注意深く選択してください。ネットワーク内のセキュリティが高くなると、それに応じて、複雑度や問題のトラブルシューティングも増加します。各企業の責任で、リスクと組織の要件の両方を定義し、ネットワークとネットワークに接続されたデバイスに適切なセキュリティを適用する必要があります。

まとめ

CHAPTER 17

IP テレフォニー エンドポイント

この章では、さまざまなタイプの Cisco IP テレフォニー エンドポイントとその機能、関連する設計上の考慮事項、および QoS 推奨事項について要約します。Cisco IP テレフォニー エンドポイントは、次の主要なタイプに分類できます。

- アナログ ゲートウェイ（P.17-2）
- Cisco デスクトップ IP Phone（P.17-6）
- ソフトウェアベースのエンドポイント（P.17-11）
- 特殊な用途の Cisco IP Phone。次のものが含まれます。
  - 無線エンドポイント（P.17-16）
  - Cisco IP Conference Station（P.17-21）

加えて、P.17-21 の「QoS の推奨事項」の項では QoS 設定のリストを示し、P.17-34 の「エンドポイント機能の要約」の項ではエンドポイントの全機能のリストを示します。

ビデオ対応のエンドポイントの詳細については、次の Web サイトで入手可能な『*Cisco IP Video Telephony Solution Reference Network Design（SRND）*』を参照してください。

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

アナログ ゲートウェイ

アナログ ゲートウェイには、アナログ ネットワーク モジュール、24-FXS ポート アダプタ搭載の Cisco Communication Media Module（CMM）、Catalyst 6500 24-FXS アナログ インターフェイス モジュール、Cisco VG224、Cisco VG248、および Cisco Analog Telephone Adaptor（ATA）186 および 188 があります。通常、アナログ ゲートウェイは、FAX、モデム、TDD/TTY、およびアナログ電話機などのアナログ デバイスを VoIP ネットワークに接続するために使用します。これにより、アナログ信号を IP ネットワーク上でパケット化して送信できるようになります。

アナログ ネットワーク モジュール

Cisco アナログ ネットワーク モジュールには、低密度音声 /FAX ネットワーク モジュール（NM-1V および NM-2V）、高密度音声 /FAX ネットワーク モジュール（NM-HDA-4FXS）、および Cisco IP Communication 音声 /FAX モジュール（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。Cisco アナログ ネットワーク 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 ネットワーク 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。

低密度音声 /FAX ネットワーク モジュール

低密度音声 /FAX ネットワーク モジュールには、NM-1V および NM-2V があります。これらのモジュールには、音声 /FAX インターフェイス カード（VIC）が 1 つまたは 2 つ含まれています。音声 /FAX 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、VIC-2FO-M2、VIC-2FXO-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。

高密度音声 /FAX ネットワーク モジュール

高密度音声 /FAX ネットワーク モジュールである NM-HDA-4FXS には、4 つのオンボード FXS ポートと、2 つの拡張モジュール（EM-HDA-8FXS または EM-HDA-4FXO）用のスペースがあります。これにより、最大で 12 個のアナログ ポート（4 FXS + 8 FXO）または 16 個のアナログ ポート（12 FXS + 4 FXO）を提供します。2 つの 8 ポート FXS EM を使用する設定は、現在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ます。

Cisco IP Communications 音声 /FAX ネットワーク モジュール

Cisco IP Communications 音声 /FAX ネットワーク モジュールには、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-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 接続を処理するデジタルまたはアナログの BRI 音声カードまたは WAN 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 つのネットワーク 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 /FAX 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 Multiflex Trunk（MFT）T1 VWIC（VWIC-1MFT-T1、VWIC-2MFT-T1、および VWIC-2MFT-T1-DI）、1 ポートおよび 2 ポート RJ-4 および VWIC-2MFT-E1-D1）、および WAN 接続専用の 1 ポートおよび 2 ポート RJ-48 G703 VWIC（VWIC-1MFT-G703 および VWIC-2MFT-G703）があります。

アナログ ネットワーク 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 ネットワーク モジュール用にサポートされているプラットフォームは、Cisco 2600XM、Cisco 2691、Cisco 3640 および 3660、および Cisco 3725 および 3745 です。表 17-1 は、各プラットフォームでサポートされているネットワーク モジュールの最大数と、必要な Cisco IOS ソフトウェアの最小バージョンをリストしています。

表 17-1　アナログ ネットワーク 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

	サポートされているネットワーク モジュールの最大数				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	NM-HD-1V、-2V、-2VE	NM-HDV2、-1T1/E1、-2T1/E1	NM-1V、-2V	NM-HDA-4FXS	NM-HD-1V、-2V、-2VE	NM-HDV2、-1T1/E1、-2T1/E1
Cisco2600XM	1	1	1	1	12.2(8)T 以降	12.2(8)T 以降	12.2(15)ZJ "Plus" イメージ	12.3(7)T 12.3(11)T
Cisco 2691	1	1	1	1	12.2(8)T 以降	12.2(8)T 以降	12.2(15)ZJ "Plus" イメージ	12.3(7)T 12.3(11)T
Cisco 3640	3	3	3	サポートされない	11.3(1)T 以降 12.0(1)T 以降	12.2(2)XT 以降 12.2(8)T 以降	12.2(15)ZJ "Plus" イメージ	適用対象外
Cisco 3660	6	6	6	サポートされない	11.3(1)T 以降 12.0(1)T 以降	12.2(2)XT 以降 12.2(8)T 以降	12.2(15)ZJ "Plus" イメージ	適用対象外
Cisco 3725	2	2	2	2	12.2(8)T 以降	12.2(8)T 以降	12.2(15)ZJ "Plus" イメージ	12.3(7)T 12.3(11)T
Cisco 3745	4	4	4	4	12.2(8)T 以降	12.2(8)T 以降	12.2(15)ZJ "Plus" イメージ	12.3(7)T 12.3(11)T

Cisco コミュニケーション メディア モジュール（CMM）

Cisco CMM は、Catalyst 6000 および Cisco 7600 シリーズ スイッチに、高密度アナログ、T1、および E1 ゲートウェイ接続を提供するライン カードです。Cisco CMM は、最大 72 個の 72 FXS 接続を処理できます。CMM は MGCP または H.323 ゲートウェイとして動作し、最大 480 個の IP Phone に Survivable Remote Site Telephony（SRST）サービスを提供します。

Cisco CMM に含まれるインターフェイス ポート アダプタは、24 ポート FXS アナログ ポート アダプタ（WS-SVC-CMM-24FXS）、6 ポート T1 インターフェイス ポート アダプタ（WS-SVC-CMM-6T1）、6 ポート E1 インターフェイス ポート アダプタ（WS-SVC-CMM-6E1）、および会議 / トランスコーディング ポート アダプタ（WS-SVC-CMM-ACT）です。表 17-2 は、互換性のあるポート アダプタの最小ソフトウェア要件をリストしています。

表 17-2　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	12.2(13)ZP	12.2(2)YK	12.2(2)YK	12.2(13)ZP
CatOS リリース	8.1(1)	7.3(1)	7.3(1)	8.1(1)
Native IOS リリース	12.1(15)E	12.1(14)E	12.1(14)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。

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 ベースの高密度 24 ポート ゲートウェイです。Cisco IOS Release 12.3.4-XD をサポートしています。Cisco VG224 は、MGCP を使用して Cisco CallManager に接続します。SRST ルータへの H.323 接続に対する、組み込み MGCP フェールオーバーを提供します。Cisco VG224 は、H.323 または SIP のいずれかを使用して Cisco CallManager Express と統合します。Cisco VG224 は、Cisco CallManager Release 3.3（3）SR2 以降をサポートしています。Cisco VG224 は、高密度アナログ 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、Cisco VG248 を使用して 24 個のアナログ ポートを配置する場合よりコスト的に効率的です。

Cisco VG248 ゲートウェイ

Cisco VG248 アナログ ゲートウェイは、アナログ デバイスを企業音声ネットワークに接続するための高密度 SCCP（Skinny Client Control Protocol）ゲートウェイで、48 個のアナログ ポートを提供します。

Cisco VG248 には、Release 1.2 の SRST 機能があります。デフォルトでは、VG248 は付随のゲートウェイを SRST ルータとして使用します。Cisco VG248 で SRST ルータの IP アドレスが設定されている場合、VG248 は特定の SRST ルータを使用することができます。Cisco VG248 は、強力なコール機能を備えた高密度アナログ デバイスを使用する場合に最適です。

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るアナログ テレフォニー アダプタです。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 または 188 は、ユニキャスト Music on Hold（MoH）のみをサポートしています。

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。Cisco ATA 186 または 188 は、Cisco CallManager に対する H.323 クライアント、または H.323 ゲートキーパーに対する H.323 ターミナルとして設定することができます。Cisco ATA を、H.323 ターミナルとしてゲートキーパーに登録する場合、ATA が配置されているゾーンでは、H.323 プロキシを無効にする必要があります。

別のエンドポイントから電話をかけられるよう、Cisco ATA 186 または 188 を、SIP 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もできます。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 ATA 186 および 188 は、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。H.323 モードの場合、デフォルトでは、Cisco ATA 186 および 188 は音声ベアラ パケットを正しくマーキングできません。Differentiated Services Code Point（DSCP）の値を EF に設定して音声ベアラ トラフィックをマーキングするように ATA を手動で設定する必要があります。そのためには、タイプ オブ サービス（ToS）フィールドを、デフォルト値から 0x000000B8 に変更します。この設定の変更は、Cisco ATA Release 3.1 以降では必要ありません。

Cisco デスクトップ IP Phone

Cisco デスクトップ IP Phone には、ローエンド、ミッドレンジ、およびハイエンドの IP Phone があります。

ローエンドの Cisco デスクトップ IP Phone

ローエンドの Cisco デスクトップ 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。ローエンドの Cisco デスクトップ IP Phone には、Cisco IP Phone 7902G、7905G、7910G、7910G+SW、および 7912G があります。

Cisco IP Phone 7902G

Cisco IP Phone 7902G は単一回線をサポートしており、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 IP Phone 7902G に液晶（LCD）画面はありません。

Cisco IP Phone 7905G

Cisco IP Phone 7905G は単一回線をサポートしており、電話機の背面に 1 つの 10 Base-T イーサネット ポートを備えています。スピーカーは、一方向のリッスン モードでのみ動作します。Cisco IP Phone 7905G は、C 割り込み機能（P.17-8 の「C 割り込み」を参照）もサポートしています。

Cisco IP Phone 7910G および 7910G+SW

Cisco IP Phone 7910G は単一回線をサポートしており、スピーカーは一方向のリッスン モードでのみ動作します。Cisco IP Phone 7910G には、機能が固定された 6 つのアクセス キーがあります。これらのアクセス キーは、管理者がカスタマイズする電話機ボタン テンプレートで設定可能で、さまざまなエンドユーザ コール機能を提供できます。機能が固定されたキーは 6 つしかないので、モデル 7910G では、1 つの電話機ボタン テンプレートですべてのコール機能をエンド ユーザに提供することはできません。

Cisco IP Phone 7910G と 7910G+SW の唯一の違いは、前者が 10 Base-T イーサネット ポートを 1 つ備えているのに対し、後者は 10/100 Base-T イーサネット ポートを 2 つ備えている点です。

Cisco IP Phone 7912G

Cisco IP Phone 7912G は単一回線をサポートしており、2 つの 10/100 Base-T イーサネット接続を備えています。スピーカーは、一方向のリッスン モードでのみ動作します。Cisco IP Phone 7912G は、C 割り込み機能（P.17-8 の「C 割り込み」を参照）もサポートしています。

ミッドレンジの Cisco デスクトップ IP Phone

ミッドレンジの Cisco デスクトップ 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する、トラフィック量の多いユーザに最適です。ミッドレンジの Cisco デスクトップ IP Phone には、Cisco IP Phone 7940G および 7960G があります。Cisco IP Phone 7940G では最大 2 つのディレクトリ番号を設定でき、Cisco IP Phone 7960G では合計 6 つのディレクトリ番号を設定できます。どちらの電話機モデルも割り込みおよび C 割り込みの機能をサポートしており、どちらも Cisco VT Advantage ビデオ対応エンドポイントでのビデオ コールと互換性があります。

割り込み

割り込みは、Cisco IP Phone 7940G または 7960G で使用可能な組み込み型のコンファレンス ブリッジ機能を使用します。割り込みが動作するのは、回線が、割り込み機能をサポートしている別の電話機と共に共有されている場合に限られます。シェアドライン型の IP Phone は、回線を共有している IP Phone と別の電話機の間で確立されているコールに、参加する（割り込む）ことができます。コールで最初のシェアドライン型電話がコンファレンス ブリッジになり、他の 2 つの音声ストリームを終端します。

電話機設定ページの Built-In-Bridge フィールドは、On モード、Default モード、または Off モードに設定できます。Default に設定する場合、電話機の設定は、企業サービス パラメータ "Built In Bridge - Enable" の設定から継承されます。割り込み機能を有効にするには、仮想コンファレンス ブリッジになる電話機で、Built-In-Bridge フィールドを On モードに設定する必要があります。また、シェアドライン型の IP Phone が割り込みを開始できるように、プライバシ設定を Off モードに設定する必要があります。

図 17-1 は、A、B、C の 3 つの IP Phone が配置されている状況で割り込みがどのように動作するかを示しています。この例では、電話機 B と C が 1 つの回線を相互に共有しており、どちらの電話機も Built-In-Bridge 機能を備えています。電話機 B が仮想コンファレンス ブリッジであるため、割り込みが動作するには、Built-In-Bridge フィールドを On モードに設定する必要があります。

図 17-1　割り込みの例

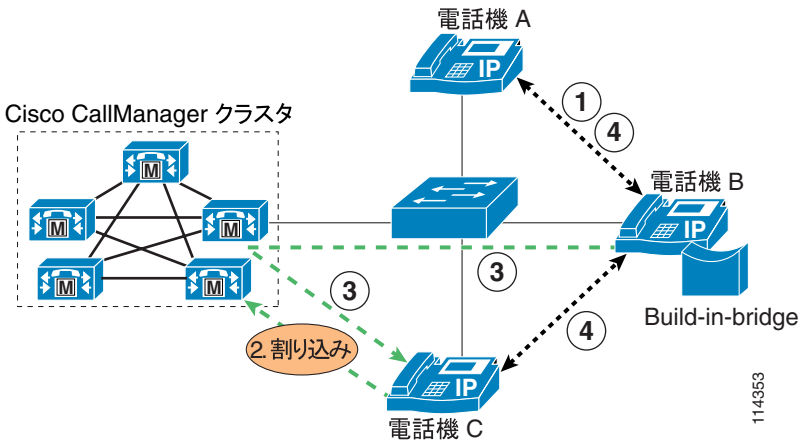


図 17-1 は、次の連続したイベントを示しています。

1. 電話機 A と電話機 B の間でコールが確立されます。
2. 電話機 C が、Cisco CallManager に要求を送信することにより、既存のコールに対する割り込みを試行します。
3. Cisco CallManager が、電話機 A と電話機 C に対して、相互のメディア ストリームを受信し、メディア ストリームを相互に送信することを開始するように指示します。
4. 電話機 B がコンファレンス ブリッジになり、電話機 A と電話機 C のメディア ストリームを終端します。電話機 C が会議から退出すると、Cisco CallManager は、電話機 C 用のメディア受信チャネルを閉じるように電話機 B に指示します。

電話機 A が会議から退出すると、コールは終端されます。電話機 B が会議から退出すると、Cisco CallManager は、3 つの電話機すべてに、メディアの送信を停止し、メディア受信チャネルを閉じるように指示します。また電話機 A と電話機 C に、ポイントツーポイント コールをセットアップするように指示します。電話機 B が EndCall ソフトキーをアクティブにしてから電話機 A と電話機 C の両方が双方向の RTP ストリームをセットアップするまで、約 400 ms かかります。

(注)　現在、割り込みは G.711 コールでのみサポートされています。WAN 上での会議コールでは、C 割り込み機能を使用してください。

C 割り込み

C 割り込みもシェアドライン型の電話機で動作しますが、他のシェアドライン型電話機が同時に C 割り込み機能をサポートしていることは要求されていません。C 割り込みは、ソフトウェアまたはハードウェアのいずれかのコンファレンス ブリッジ リソースを使用するという点で、通常の会議に似ています。C 割り込みは、コールで最初のシェアドライン型電話機のメディア リソース グループ リスト（MRGL）で指定されている共有コンファレンス ブリッジ リソースを使用します。C 割り込みが動作するには、シェアドライン型の他の IP Phone が C 割り込みを開始できるように、プライバシ設定を Off モードに設定する必要があります。

図 17-2 は、A、B、C の 3 つの IP Phone が配置されていて、IP Phone B と C が 1 つの回線を相互で共有している状況で C 割り込みがどのように動作するかを示しています。

図 17-2　C 割り込みの例

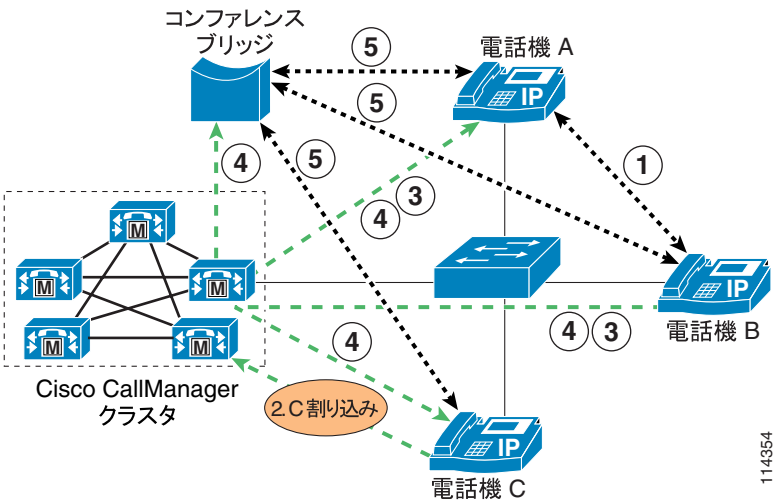


図 17-2 は、次の連続したイベントを示しています。

1. 電話機 A と電話機 B の間でコールが確立されます。
2. 電話機 C が、Cisco CallManager に要求を送信することにより、既存のコールに対する C 割り込みを試行します。
3. Cisco CallManager が、電話機 A と電話機 B の両方に対して、メディア受信チャネルを閉じ、メディア ストリームの送信を停止するように指示します。
4. Cisco CallManager は、3 つのすべての IP Phone に、着信メディア ストリームを受信できるように準備し、独自のメディア ストリームを共有コンファレンス ブリッジに送信するように指示します。ここで言う共有コンファレンス ブリッジは、Cisco CallManager 上のソフトウェア ブリッジか、会議デバイスで設定されているハードウェア コンファレンス ブリッジのいずれかです。また Cisco CallManager は、IP Phone からの着信メディア ストリームを受信できるように準備し、これらのメディア ストリームを IP Phone にもリレーするよう、共有コンファレンス ブリッジに指示します。

5. 3 つのすべての IP Phone からのメディア ストリームは共有コンファレンス ブリッジで終端され、各 IP Phone は、共有コンファレンス ブリッジからの着信メディア ストリームを受信します。

いずれかの電話機が会議から退出すると、Cisco CallManager は、3 つのすべての電話機に、メディア受信チャネルを閉じてメディア送信を停止するように指示します。次に Cisco CallManager は、残りの 2 つの電話機に、ポイントツーポイント コールをセットアップするように指示します。いずれかの電話機が EndCall ソフトキーをアクティブにしてから残りの 2 つの電話機が双方向の RTP ストリームをセットアップするまで、約 400 ms かかります。

(注) 割り込みおよび C 割り込みのどちらにおいても、電話機 A と電話機 B の間でコールが開始されたときに電話機 C が切断状態またはリブート中の場合、または電話機 A と電話機 B の間でコールがセットアップされた後に電話機 C が切断またはリブートされた場合、電話機 C は、電話機 A と電話機 B の間の既存のコールに対する割り込みまたは C 割り込みを実行できません。

セキュリティ

Cisco 7940G および 7960G IP Phone は、ローカルで重要な証明書を使用して、認証トランスポート レイヤ セキュリティ（TLS）を実行します。IP Phone は、ローカルで重要な証明書を Certificate Authority Proxy Function（CAPF）から取得します。CAPF は、Cisco CallManager パブリッシャで実行するアプリケーションです。証明書とは、認証機関（CA）でハッシュ暗号化されるデジタル識別文書で、デバイスの ID を認証するためのものです。

Cisco 7940G および 7960G IP Phone には、認証モードと暗号化モードという 2 つのセキュア モードがあります。認証モードでは、認証 TLS はラベル スイッチ コントローラ（LSC）を使用して実行され、IP Phone は TCP ポート 2443 で Cisco CallManager に登録されます。暗号化モードでは、IP Phone は認証 TLS を実行するだけでなく、シグナリングとメディア パケットの両方を暗号化します。Cisco CallManager が使用不可になると、Cisco 7940G または 7960G IP Phone は、TCP ポート 2443 上の SRST デバイスに対してセキュア（TLS）なシグナリング接続を開始できます。

Cisco 7940G または 7960G IP Phone が暗号化モードで、ワイドバンド コーデック リージョンに関連付けられている場合、Cisco CallManager は暗号化コールの間、ワイドバンド コーデックを無視し、その代わりに、リージョンのコーデック リストから、サポートされている別のコーデックを選択します。ただし、保護されていないコールまたは認証済みコールの場合、Cisco CallManager はワイドバンド コーデックを使用してコールをセットアップします。暗号化モードの Cisco 7940G または 7960G IP Phone は、既存の暗号化コールだけでなく、保護されていないコールや認証済みコールにも割り込みできますが、これらの電話機が、暗号化された割り込みコールの仮想ブリッジとして動作することはできません。

Cisco 7940G または 7960G IP Phone には、コールおよび Cisco CallManager との接続の両方についてセキュリティ モードを示す、2 つのアイコンが表示されます。コールまたは接続が、認証されているが暗号化されていない場合、盾のアイコンが電話機の画面に表示されます。コールが暗号化されている場合、錠のアイコンが表示されます。IP Phone で暗号化されたコールをセットアップし、次にコールを保留するか別の IP Phone に転送すると、錠のアイコンはオフフック電話アイコンに置き換わります。このアイコンは、これらのタスクに関連付けられたメディア ストリームが暗号化されていないことを示しています。

現在、暗号化されたコンファレンス ブリッジおよび C 割り込みはサポートされていません。3 台の Cisco 7940G または 7960G IP Phone が暗号化モードで会議をセットアップしている場合、これらの 3 つの参加者からのメディア ストリームは暗号化されません。いずれかの参加者が会議から退出すると、残りの 2 つの参加者は、暗号化されたポイントツーポイント コールをセットアップします。暗号化されたビデオ コールはサポートされていません。1 台の IP Phone が暗号化モードでビデオ コールを開始した場合、ビデオ RTP メディア トラフィックは暗号化されませんが、オーディオ メディア パケットは暗号化されます。

ハイエンドの Cisco デスクトップ IP Phone

ハイエンドの Cisco デスクトップ IP Phone である Cisco IP Phone 7970G は、拡張コール機能を使用する、トラフィック量の多いユーザに最適です。Cisco IP Phone 7970G は高解像度のカラー表示のタッチスクリーンを備えており、ミッドレンジの Cisco IP Phone よりも多くの機能キーとセキュリティ機能を利用できます。Cisco IP Phone 7970G には、最大で 8 個のディレクトリ番号を設定できます。

現在の電話ソフトウェア ロード（TERM70.5-0-1-4DEV）では、Cisco IP Phone 7970G は割り込みおよび C 割り込み機能をサポートしています。Cisco IP Phone 7970G は、ビデオ コールの使用について、Cisco VT Advantage ビデオ対応エンドポイントとも互換性があります。現在、Cisco IP Phone 7970G は、Cisco プレスタンダードの Power-over-Ethernet（PoE）と IEEE 802.3af PoE の両方をサポートしている唯一の Cisco IP Phone です。Cisco IP Phone 7970G で画面の明るさを最大にするには、インライン パワーと 802.3af PoE の両方を備えた外部電源アダプタ（CP-PWR-CUBE2）を使用する必要があります。

セキュリティ

Cisco IP Phone 7970G には、Manufacturing Installed Certificate（MIC; 製造元でインストールされる証明書）があります。これは、フラッシュに書き込まれ、ハードウェアのリセット時に消去されません。Cisco IP Phone 7970G には、認証モードと暗号化モードという 2 つのセキュア モードがあります。認証モードでは、電話機は MIC を介して認証 TLS を実行し、TCP ポート 2443 で Cisco CallManager に登録されます。暗号化モードでは、電話機は認証 TLS を実行するだけでなく、シグナリングとメディア パケットの両方を暗号化します。Cisco CallManager が使用不可になると、Cisco IP Phone 7970G は、TCP ポート 2443 上の SRST デバイスに対してセキュア（TLS）なシグナリング接続を開始できます。暗号化モードの Cisco IP Phone 7970G は、既存の暗号化コールだけでなく、保護されていないコールや認証済みのコールにも割り込みできます。Cisco 7940G または 7960G とは異なり、Cisco 7970G IP Phone は、暗号化された割り込みコールの仮想ブリッジとして動作できます。

Cisco IP Phone 7970G には、コールおよび Cisco CallManager との接続の両方についてセキュリティ モードを示す、2 つのアイコンが表示されます。コールまたは接続が認証されているが暗号化されていない場合、盾のアイコンが電話機の画面に表示されます。コールまたは接続が認証され、かつ暗号化されている場合、錠のアイコンが表示されます。オフフック電話アイコンは、保護されていないコールを表しています。Cisco IP Phone 7970G で暗号化された電話コールをセットアップし、次にコールを保留するか別の IP Phone に転送すると、錠のアイコンはオフフック電話アイコンに置き換わります。このアイコンは、これらのタスクに関連付けられたメディア ストリームが暗号化されていないことを示しています。

現在、暗号化されたコンファレンス ブリッジおよび C 割り込みはサポートされていません。3 台の Cisco 7970G IP Phone が暗号化モードで会議をセットアップしている場合、これらの 3 つの参加者からのメディア ストリームは暗号化されません。いずれかの参加者が会議から退出すると、残りの 2 つの参加者は、暗号化されたポイントツーポイント コールをセットアップします。暗号化されたビデオ コールはサポートされていません。1 台の IP Phone が暗号化モードでビデオ コールを開始した場合、ビデオ RTP メディア トラフィックは暗号化されませんが、オーディオ メディア パケットは暗号化されます。

ソフトウェアベースのエンドポイント

ソフトウェアベースのエンドポイントには、Cisco IP SoftPhone 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、登録と制御は Cisco CallManager で行います。

Cisco IP SoftPhone

この項では、CiscoCallManager と一緒に Cisco IP SoftPhone を使用する場合に適用される、次の設計上の考慮事項について説明します。

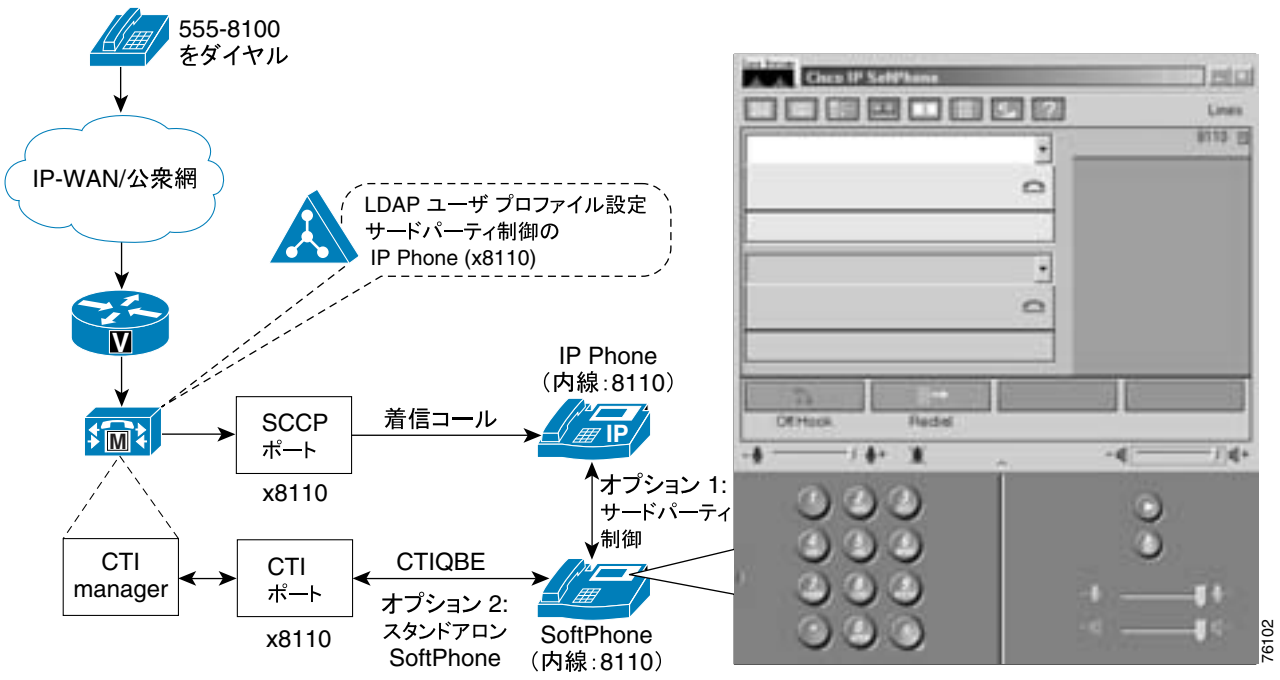
- Cisco IP SoftPhone の最大設定の制限（P.17-12）
- コーデックの選択（P.17-12）
- コール アドミッション制御（P.17-13）

この項の情報は、Cisco IP SoftPhone Release 1.3 に明示的に適用されます。Cisco IP SoftPhone の設定と機能の詳細は、次の Web サイトでオンラインで入手可能な『Cisco IP Softphone Administrator Guide (1.3)』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/softphon/index.htm

図 17-3 では、Cisco IP SoftPhone アプリケーションが、関連付けられたハードウェア IP Phone をモニタまたは制御できることを示しています。サードパーティ制御の電話機の場合、Cisco IP SoftPhone は、デスクトップ IP Phone の仮想内線電話の役目をします。Cisco IP SoftPhone アプリケーションは、ハードウェア電話機の着信コールと発信コールを表示し、処理できます。デバイスと CTI リソースのプロビジョニングの観点から見ると、この設定を使用する各ユーザは、サードパーティ制御の IP Phone として設定されます。CTI ポートとしての Cisco IP SoftPhone は、デスクトップ電話機で追加の制御やモニタリングをすることなく、クライアント マシンへのコールを直接処理する専用回線です。

図 17-3　Cisco IP SoftPhone のデバイスの関連付けオプション



Cisco IP SoftPhone は、CTI ポートとサードパーティ制御の電話機を、同じディレクトリ番号（DN）で同時に実行することはできません。図 17-3 に示されているように、ユーザは、CTI ポート、またはデスクトップ電話機の制御として、x8110 を使用できます。

デバイスおよびリソース プロビジョニングの詳細については、第 8 章「コール処理」を参照してください。

Cisco IP SoftPhone の最大設定の制限

サーバごとに許可されるデバイスの制限とは関係なく、Cisco CallManager で設定できる最大 CTI デバイス数に制限があります。Cisco IP SoftPhone に適用される CTI デバイスの制限は、次のとおりです。

- Cisco Media Convergence Server（MCS）7825 または 7835 の場合、1 台あたり最大 800 台の Cisco IP SoftPhone。MCS 7825s または 7835s の場合、1 台あたり最大 3,200 台の Cisco IP SoftPhone。
- MCS 7845 の場合、1 台あたり最大 2,500 台の Cisco IP SoftPhone。MCS 7845s の場合、1 台あたり最大 10,000 台の Cisco IP SoftPhone。

上記の Cisco IP SoftPhone の最大限度には、次の前提が適用されます。

- 各 Cisco IP SoftPhone は、1 つのライン アピアランスで設定されます。
- 各 Cisco IP SoftPhone は、見積もりで 6 コール以下の Busy Hour Call Attempt（BHCA）を処理します。
- CTI デバイスを必要とする他の CTI アプリケーションが、その Cisco CallManager クラスタで設定されていません。

コーデックの選択

Cisco IP SoftPhone は、G.711 および G.729a コーデックをサポートします。G.729a 低帯域幅コーデック設定は、Cisco IP SoftPhone を WAN 経由で接続する在宅勤務者の環境に配置することをお勧めします。

Cisco CallManager が G.723 コーデックをサポートしていないため、Cisco IP Softphone には、使用可能な帯域幅コーデック設定が 2 つあります。G.711 がデフォルト設定で、TAPI Service Provider（TSP）クライアント上で低帯域幅コーデック設定 G.729 を選択するためにユーザが設定可能なオプションがあります（図 17-4 を参照）。ネットワーク帯域幅のプロビジョニングの詳細については、第 3 章「ネットワーク インフラストラクチャ」を参照してください。

図 17-4　Cisco IP Softphone のオーディオ設定

WAN を介した低帯域幅の接続を使用する Cisco IP SoftPhone のユーザは、この低帯域幅の G.729 コーデック設定の選択を検討する必要があります。

コール アドミッション制御

コール アドミッション制御により、ネットワークを介した IP Phone コールの処理に使用可能な帯域幅が十分確保されます。コール アドミッション制御の実装には複数のメカニズムがありますが、Cisco IP SoftPhone は、Cisco CallManager で設定されるロケーション メカニズムだけを使用します。Cisco CallManager のロケーションを使用したコール アドミッション制御の詳細については、第 2 章「IP テレフォニー配置モデル」を参照してください。

ロケーションベースのコール アドミッション制御は、Cisco IP SoftPhone が単一の Cisco CallManager ロケーション内でモバイルとして使用されているかぎり、コール帯域幅の管理で有効です。ただし、Cisco IP SoftPhone が複数の Cisco CallManager ロケーション間を移動すると、コール アドミッション制御が問題の原因になる場合があります。モビリティの詳細については、P.17-19 の「デバイス モビリティおよび Cisco CallManager」を参照してください。

Cisco IP Communicator

Cisco IP Communicator は Cisco IP SoftPhone と似ており、リモート ユーザと在宅勤務者にとっては理想的なソリューションです。Cisco IP Communicator は、SCCP ベースのスタンドアロン デバイスです。クライアントの PC 画面では、Cisco IP Phone 7970G のように表示されます。この項では、Cisco CallManager と一緒に Cisco IP Communicator を使用する場合に適用される、次の設計上の考慮事項について説明します。

- IP Communicator の最大設定の制限（P.17-14）
- コーデックの選択（P.17-14）
- コール アドミッション制御（P.17-15）

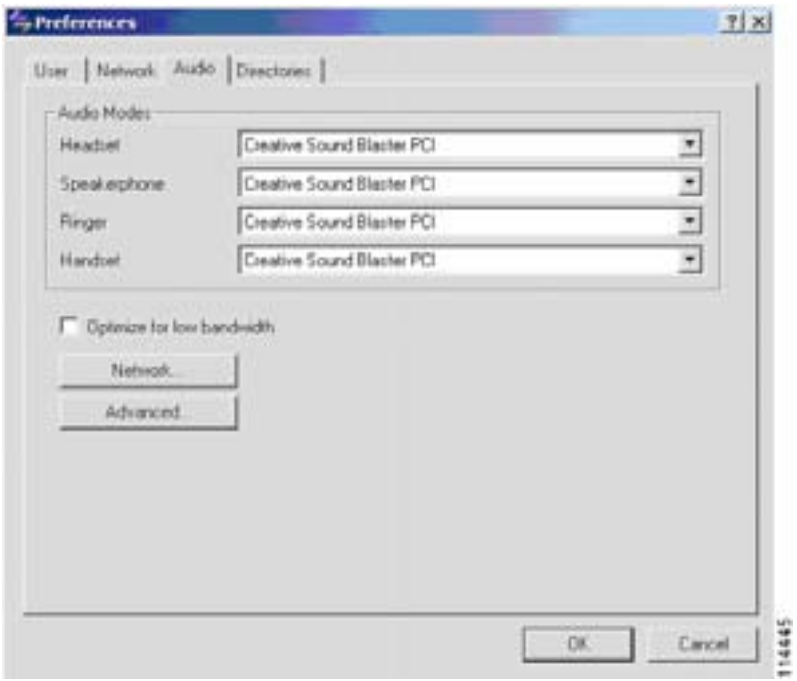
IP Communicator の最大設定の制限

Cisco IP Communicator は SCCP スタンドアロン デバイスであるため、さまざまな IP テレフォニー配置モデルに含まれる IP Phone の設計に関するガイドラインは、Cisco IP Communicator にも当てはまります。詳細については、第 2 章「IP テレフォニー配置モデル」を参照してください。

コーデックの選択

Cisco IP Communicator は、G.711 および G.729a コーデックをサポートします。コーデックを選択するには、Cisco IP Communicator が配置されているリージョンを設定します。G.729a 低帯域幅コーデック設定は、WAN 経由で Cisco IP Communicator を接続する在宅勤務者の環境に配置することをお勧めします。Cisco IP Communicator にも、G.711 リージョン内の低帯域幅コーデックを上書きする機能があります。この機能を有効にするには、Audio 設定ウィンドウの Optimize for Low Bandwidth オプション チェックボックスをオンにします（図 17-5 を参照）。ここでは、Cisco IP Communicator は、G.729 コーデックを使用して、同じリージョン内の別の電話機とのコールをセットアップします。

図 17-5　Cisco IP Communicator のオーディオ設定



コール アドミッション制御

コール アドミッション制御により、ネットワークを介した IP Phone コールの処理に使用可能な帯域幅が十分確保されます。コール アドミッション制御の実装には複数のメカニズムがありますが、Cisco IP Communicator は、Cisco CallManager で設定されるロケーション メカニズムだけを使用します。Cisco CallManager のロケーションを使用したコール アドミッション制御の詳細については、第 2 章「IP テレフォニー配置モデル」を参照してください。

ロケーションベースのコール アドミッション制御は、Cisco IP SoftPhone が単一の Cisco CallManager ロケーション内でモバイルとして使用されているかぎり、コール帯域幅の管理で有効です。ただし、Cisco IP Communicator が複数の Cisco CallManager ロケーション間を移動すると、コール アドミッション制御が問題の原因になる場合があります。詳細については、P.17-19 の「デバイス モビリティおよび Cisco CallManager」を参照してください。

無線エンドポイント

Cisco 無線エンドポイントは、無線アクセス ポイント（AP）経由で無線 LAN（WLAN）インフラストラクチャを使用して、テレフォニー機能を提供します。このタイプのエンドポイントは、エリア内でモバイル ユーザの必要性がある環境で、従来の有線電話では不適切であったり問題が生じたりする場合に理想的です（無線ネットワークの設計の詳細については、P.3-43 の「無線 LAN インフラストラクチャ」を参照してください）。

Cisco 無線 IP Phone 7920 は、ネットワークへの 802.1b 無線 LAN 接続を可能にする組み込み型の無線アンテナを備えた、ハードウェアベースの電話機です。これらの電話機は、他のハードウェアベースの電話機や Cisco IP Communicator と同様、Skinny Client Control Protocol（SCCP）を使用して Cisco CallManager に登録されます。詳細については、次の Web サイトで入手可能な『*Cisco Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。

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

サイト調査

Cisco 無線 IP Phone 7920 を配置する前に、完全なサイト調査を実行して、無線周波数（RF）カバレッジを提供するのに最適な AP の数と場所を判別する必要があります。サイト調査では、最適なカバレッジを提供するアンテナ タイプや RF 干渉の送信元が存在している可能性がある場所を考慮する必要があります。サイト調査では、Cisco 無線 IP Phone 7920 の Site Survey ツール（**Menu** > **Network Config** > **Site Survey** からアクセス）、およびラップトップまたは PC の Cisco Aironet NIC カードと共に使用する Aironet Client Utility Site Survey ツールを使用する必要があります。追加のサードパーティ ツールもサイト調査で使用できますが、アンテナの感度と調査アプリケーションの制限によって各エンドポイントまたはクライアント無線の動作が異なるため、Cisco 無線 IP Phone 7920 を使用して最終サイト調査を実行することを強くお勧めします。

認証

Cisco 無線 IP Phone 7920 を無線ネットワークに接続するには、最初に次のいずれかの認証方法を使用して、AP に関連付けて通信する必要があります。

- Cisco LEAP

  この方法では、ユーザ名とパスワードに基づいて、Cisco 無線 IP Phone 7920 と AP を相互に認証できます。認証時に動的な鍵が生成され、Cisco 無線 IP Phone 7920 と AP の間のトラフィックの暗号化に使用されます。ユーザ データベースへのアクセスを提供するため、Cisco Secure Access Control Server（ACS）などの、LEAP 準拠の Radius 認証サーバが必要です。

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

  この方法では、Cisco 無線 IP Phone 7920 と AP に、静的な 10 文字（40 ビット）または 26 文字（128 ビット）の鍵を設定します。この方法は AP ベースの認証方法で、一致する鍵がデバイスに存在する場合にネットワークへのアクセスが許可されます。

- Open 認証

  この方法では、Cisco 無線 IP Phone 7920 と AP の間で、識別情報を交換する必要はありません。この方法では音声またはシグナリングの安全な交換が提供されず、偽装したデバイスを AP に関連付けることができるため、この方法はお勧めしません。

キャパシティ

各 AP は、最大で 7 つのアクティブな G.711 音声コールまたは 8 つの G.729 コール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。

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 無線 7920G IP Phone の数を計算できます。たとえば、標準的なユーザ対コールのキャパシティ比率を 3:1 と想定すると、使用するコーデックが G.711 か G.729 かに応じて、1 つの AP で 21 ～ 24 台の Cisco 無線 7920G IP Phone をサポートできます。ただし、この数には、他の Cisco 無線 7920G IP Phone がこの AP にローミングする可能性は加味されていません。現実的には、AP あたりの電話機の数は上記の数より少なくなります。

VLAN またはレイヤ 2 サブネットあたりの AP の数も考慮する必要があります。AP のメモリおよびパフォーマンスを最適化するには、1 つの VLAN またはサブネットに、30 を超える数の AP を配置しないことをお勧めします。標準的なユーザ対コールのキャパシティ比率を適用すると、レイヤ 2 サブネットあたりの Cisco 無線 7920G IP Phone の数は、概算で 500（または AP あたり 15 ～ 17 の Cisco 無線 7920G IP Phone）に制限されます。

これらのキャパシティは、音声アクティビティ検出（VAD）が無効で、パケット化のサンプル サイズが 20 ミリ秒（ms）であると想定して計算されました。VAD とは、コール中に音声が発生しないときに RTP パケットを送信しないことにより、帯域幅を節約するメカニズムです。しかし、VAD の有効化または無効化は、Cisco CallManager で、クラスタ全体のグローバル設定パラメータで設定します（Cisco CallManager では無音圧縮と呼ばれます）。このため、Cisco 無線 IP Phone 7920 で VAD を有効にすると、VAD は Cisco CallManager クラスタ内のすべてのデバイスで有効になります。全体の音声品質を良好に保つため、VAD（無音圧縮）を *disabled* のままにすることをお勧めします。

サンプリング レートを 20 ms に設定すると、片方向の音声コールで 50 パケット / 秒（pps）が生成されます。通常は、サンプル レートを 20 ms に設定するようにお勧めします。それより大きいサンプル サイズ（30 または 40 ms）を使用すると、AP あたりの同時コールの数を増分できますが、エンドツーエンドの遅延も大きくなります。また、サンプル サイズを大きくすると、1 つのパケットが失われたときに欠落する会話の量が大きくなるので、無線環境で許容される音声パケットの損失率は大幅に減少します。音声サンプリング サイズの詳細については、P.3-31 の「帯域幅のプロビジョニング」を参照してください。

電話機設定

Cisco 無線 IP Phone 7920 は、電話機のキーパッド、または USB ケーブルで電話機に接続された PC で実行する 7920 設定ユーティリティのいずれかを使用して設定できます。いずれの場合も、次のパラメータを設定する必要があります。

- ネットワーク設定

  ネットワークの必要に応じて、DHCP サーバ アドレスを指定するか、IP アドレス、サブネット マスク、デフォルト ゲートウェイ、TFTP サーバ、DNS サーバなどの静的設定を設定します。これらの設定は、Cisco 無線 IP Phone 7920 では **Menu** > **Network Config** > **Current Config** から参照できます。

- 無線設定

  Voice VLAN の Service Set Identifier（SSID）および認証タイプを設定します。必要に応じて、WEP 鍵、LEAP ユーザ名、およびパスワードを設定してください。これらの設定は、Cisco 無線 IP Phone 7920 では **Menu** > **Network Config** > **802.11b Configuration** から参照できます。

ローミング

現在、Cisco 無線 IP Phone 7920 は、レイヤ 2（同一の VLAN またはサブネット内）にローミングし、引き続きアクティブなコールを保持できます。

レイヤ 2 ローミングは、次の状況で発生します。

- Cisco 無線 IP Phone 7920 の初期ブートアップ中に、電話機は初めて新しい AP にローミングします。
- Cisco 無線 IP Phone 7920 が、現在関連付けられている AP からビーコンまたは応答を受信しない場合、電話機は現在の AP が使用不可であると想定し、新しい AP へのローミングと関連付けを試行します。
- Cisco 無線 IP Phone 7920 は、適格な AP ローミング ターゲットのリストを保持します。現在の AP の状態が変更されると、電話機は、使用可能な AP ローミング ターゲットのリストを参照します。ローミング ターゲットの 1 つが、より適切な選択肢であると判別された場合、電話機はその新しい AP にローミングします。
- Cisco 無線 IP Phone 7920 の設定済みの SSID または認証タイプが変更された場合、電話機は AP にローミングして再度関連付けする必要があります。

レイヤ 2 ローミングで適格な AP ローミング ターゲットの判別を試行するとき、無線 IP Phone は、次の変数を使用して、関連付ける最適な AP を判別します。

- Relative Signal Strength Indicator（RSSI）

  無線 IP Phone が、シグナルの長さと、RF カバレッジ エリア内で使用可能な AP の品質を判別するときに使用されます。電話機は、RSSI 値が最高で、認証 / 暗号化タイプが一致する AP との関連付けを試行します。
- QoS Basis Service Set（QBSS）

  AP が、チャネル利用率情報を無線電話機に通信するのを可能にします。チャネル利用率が高い AP は VoIP トラフィックを効率的に処理できない場合があるので、電話機は、QBSS 値を使用して、別の AP へのローミングを試行する必要があるかどうかを判別します。
- RSSI 差分しきい値

  次の AP RSSI が現在の AP RSSI よりも高く、その差分がこのしきい値以上である場合、無線 IP Phone はローミングします。デフォルトのしきい値は 15 です。
- QBSS 差分しきい値

  次の AP QBSS が現在の QBSS よりも低く、その差分がこのしきい値以上である場合、無線 IP Phone はローミングします。デフォルトのしきい値は 15 です。

無線 IP Phone は、次のステップを使用して、ローミング先として適切な AP を判別します。

1. ビーコン内で QBSS をアドバタイズしている AP を検出します。いずれかの AP が、QBSS 差分しきい値基準を満たしている場合、それらの AP の 1 つに対するローミング プロセスを開始します。
2. QBSS をアドバタイズしている AP がない場合、またはアドバタイズしている AP が差分しきい値基準を満たしていない場合は、QBSS をアドバタイズしていない AP で、RSSI が許容レベルの AP を検索し、それらの AP の 1 つへのローミング プロセスを開始します。

無線 IP Phone のレイヤ 2 ローミング時間は、使用される認証タイプによって異なります。電話機と AP の間の認証で静的な WEP 鍵が使用されている場合、レイヤ 2 ローミングは、100 ms 未満で実行されます。LEAP（ローカルの Cisco Secure ACS 認証を使用）が使用されている場合、レイヤ 2 ローミングは 200 ～ 400 ms で実行されます。高速セキュア ローミングを使用すると、レイヤ 2 ローミングの LEAP 認証時間を 150 ms 未満に短縮できます。

レイヤ 3 ローミングは、Cisco 7920 無線 IP Phone が 1 つの AP から別の AP に移動し、サブネットの境界を横切ったときに実行されます。Cisco Catalyst 6500 シリーズ ワイヤレス LAN サービス モジュール（WLSM）が新たにリリースされたことにより、Cisco 7920 無線 IP Phone は、スタティック WEP を使用しながら、存続可能なコールを使用するレイヤ 3 モビリティをサポートできるよう

になりました。Cisco Centralized Key Management（Cisco CKM）を使用すると、Cisco 7920 無線 IP Phone は、LEAP を使用しながら、完全なレイヤ 3 モビリティを達成できます。Cisco WLSM の詳細については、次の Web サイトで入手可能な製品資料を参照してください。

http://www.cisco.com

AP コール アドミッション制御

Cisco CallManager またはゲートキーパー内のコール アドミッション制御メカニズムは、WAN 帯域幅の利用率を制御し、既存のコールの QoS を提供できますが、どちらのメカニズムも、コールの開始時にしか適用されません。静的なデバイス間のコールでは、このタイプのコール アドミッション制御で十分です。しかし、Cisco 無線 IP Phone 7920 などの 2 つのモバイル無線デバイス間のコールの場合、無線デバイスが 1 つの AP から別の AP へと順にローミングする可能性があるので、AP レベルにもコール アドミッション制御メカニズムが必要です。

コール アドミッション制御用の AP メカニズムは QBSS です。AP は、このビーコン情報エレメントを使用して、チャネル利用率情報を無線 IP Phone に通信できます。前述のとおり、電話機はこの QBSS 値を使用して、別の AP にローミングする必要があるかどうかを判別します。QBSS 値が低いと、その AP がローミング先として適切な候補であることを示し、QBSS 値が高いと、電話機がその AP にローミングするべきでないことを示しています。

この QBSS 情報は便利ですが、ローミング中、コールが適切な QoS を保持することを 100% 保証するものではありません。Cisco 無線 7920 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。

デバイス モビリティおよび Cisco CallManager

無線 IP Phone をモバイル デバイスとして使用し、1 つのロケーションから別のロケーションに移動する場合、次の問題が発生することがあります。

- Cisco CallManager ロケーションベースのコール アドミッション制御用の不正確な帯域幅計算

  無線 IP Phone が 1 つのロケーションから別のロケーションに順にローミングする場合、現在、Cisco CallManager には、コール アドミッション制御のために電話機のロケーションを動的に更新するメカニズムはありません。そのため、実際には帯域幅を使用していないロケーションから帯域幅が差し引かれ、他のロケーションで使用可能な帯域幅がロケーションベースのコール アドミッション制御の計算に含まれない事態が生じ、WAN 帯域幅のオーバーサブスクリプションが発生する場合があります。

- 不適切なコーデックの選択

  無線 IP Phone が 1 つのロケーションから別のロケーションに順にローミングする場合、現在、Cisco CallManager には、コーデック タイプを判別するためにリージョンまたはデバイス プールを動的に更新するメカニズムはありません。そのため、不正なコーデックがテレフォニー ネットワーク全体で使用される場合があります。

- 不適切な公衆網ゲートウェイの選択

  無線 IP Phone が 1 つのロケーションから別のロケーションに順にローミングする場合、現在、Cisco CallManager には、ローカル公衆網ゲートウェイを指定するためにダイヤル プランを動的に更新するメカニズムはありません。そのため、無線 IP Phone が、公衆網アクセス用のリモート公衆網ゲートウェイを使用する場合があります。無線 IP Phone がこのリモート公衆網ゲート

ウェイを使用して緊急の 911 コールをかける場合、緊急サービスは、リモート公衆網ゲートウェイのロケーションに転送され、コールを開始した無線 IP Phone のロケーションには転送されません。

（注） Cisco Emergency Responder（ER）が配置されている場合、911 コールは、ローカル公衆網ゲートウェイ、および適切な Public Safety Answering Point（PSAP）に転送されます。ただし、コール アドミッション制御は依然としてこのコールで使用される帯域幅を把握しておらず、不正なコーデックが選択される場合があります。

これらのデバイス モビリティ問題を防止するには、電話機が 1 つのロケーションから別のロケーションに物理的に移動するたびに、Cisco CallManager で、次の無線 IP Phone のパラメータを手動で再設定する必要があります。

- コール アドミッション制御のロケーション
- デバイス プールおよびリージョン
- コーリング サーチ スペース

これらのパラメータは、無線 IP Phone の移動先のロケーションごとに適切に調整する必要があります。拡張機能や非標準の機能が必要な場合、状況によっては、他のパラメータを手動で再設定する必要があります。たとえば、ローカル メディア リソースが使用されており、各ロケーションで自動代替コール ルーティングが適切であることを確認するため、メディア リソース グループ リスト（会議、トランスコーディング、および Music-on-Hold リソース用）、および Automated Alternate Routing（AAR）コーリング サーチ スペースおよびグループ（AAR が設定されている場合）を再設定する必要があります。

デバイス モビリティに関するこれらの問題は、無線 IP Phone だけではなく、ロケーション間を移動するすべてのデバイスに当てはまります。これらのデバイスには、Cisco IP SoftPhone、Cisco IP Communicator、および 1 つの場所から別の場所に物理的に移動するすべての Cisco ハードウェア IP Phone が含まれます。

最後に、デバイス モビリティに関するこれらの問題は、集中型と分散型の両方のコール処理配置に影響します。

Cisco IP Conference Station

Cisco IP Conference Station は、会議室のスピーカーフォン テクノロジーと、Cisco IP Communications テクノロジーを結合します。Cisco IP Conference Station は、360 度の室内カバレッジを提供する会議環境に最適です。

Cisco IP Conference Station 7935 および 7936 は、どちらも外部スピーカー 1 つと組み込み型のマイク 3 つを備えています。Cisco IP Conference Station 7936 には、Cisco CallManager Release 3.3（3）SR3 以降が必要です。Cisco IP Conference Station 7936 は、バックライト付きのピクセルベース LCD 画面も備えています。大きな部屋でマイクのカバレッジを拡張するため、オプションの拡張マイクも接続できます。

QoS の推奨事項

この項では、IP テレフォニー エンドポイントで配置される一般的な Cisco Catalyst スイッチでの、基本的な QoS ガイドラインおよび設定について説明します。詳細については、次の Web サイトで入手可能な『*Quality of Service*』を参照してください。

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

Cisco VG224 および VG248

アナログ ゲートウェイは、信頼できるエンドポイントです。Cisco VG224 および VG248 ゲートウェイの場合、VG248 パケットの DSCP 値を信頼するようにスイッチを設定します。ここでは、Cisco VG224 および VG248 アナログ ゲートウェイで配置される一般的な Cisco Catalyst スイッチを設定するためのコマンドをリストします。

（注） 次の項では、*vvlan_id* は Voice VLAN ID を表し、*dvlan_id* はデータ VLAN ID を表します。

Cisco 2950

```
CAT2950(config)#interface interface-id
CAT2950(config-if)#mls qos trust dscp
CAT2950(config-if)#switchport mode access
CAT2950(config-if)#switchport access vlan vvlan_id
```

（注） **mls qos trust dscp** コマンドは、Enhanced Image（EI）でのみ使用できます。

Cisco 2970 または 3750

```
CAT2970(config)#mls qos
CAT2970(config)interface interface-id
CAT2970(config-if)#mls qos trust dscp
CAT2970(config-if)#switchport mode access
CAT2970(config-if)#switchport access vlan vvlan_id
```

Cisco 3550

```
CAT3550(config)#mls qos
CAT3550(config)interface interface-id
CAT3550(config-if)#mls qos trust dscp
CAT3550(config-if)#switchport mode access
Cat3550(config-if)#switchport access vlan vvlan_id
```

Cisco 4500（SUPIII、IV、または V 使用）

```
CAT4500(config)#qos
CAT4500(config)interface interface-id
CAT4500(config-if)#qos trust dscp
CAT4500(config-if)#switchport mode access
CAT4500(config-if)#switchport access vlan vvlan_id
```

Cisco 6500

```
CAT6500>(enable)set qos enable
CAT6500>(enable)set port qos 2/1 vlan-based
CAT6500>(enable)set vlan vvlan_id mod/port
CAT6500>(enable)set port qos mod/port  trust trust-dscp
```

Cisco ATA 186 および Conference Station

Cisco Analog Telephone Adaptor（ATA）186 および IP Conference Station は、信頼されているエンドポイントであるため、それらの QoS 設定は、P.17-21 の「Cisco VG224 および VG248」の項で説明されている設定とまったく同じです。

Cisco ATA 188 および IP Phone

Cisco Analog Telephone Adaptor（ATA）188 および IP Phone の場合、Voice VLAN をデータ VLAN から分離することをお勧めします。Cisco ATA 186、7902、7905、7910、および IP Conference Station の場合は、従来どおり、Voice VLAN とデータ VLAN を分離することと、Auxiliary VLAN を設定することをお勧めします。これにより、同じアクセスレイヤの設定を、異なる IP Phone モデルや ATA に使用できます。またエンド ユーザは、IP Phone または ATA を、スイッチ上の異なるアクセス ポートに接続して、同じ処理を受けることができます。Cisco ATA 186、7902、7905、7910、および IP Conference Station の場合、これらのデバイスは PC に接続されていないので、接続された PC からのフレームの CoS 値を上書きするためのコマンドは何の効果もありません。

次の項では、一般的に配置されている Cisco Catalyst スイッチ上の IP Phone に対して実行できる設定コマンドをリストします。

Cisco 2950

```
CAT2950(config)#
CAT2950(config)#class-map VVLAN
CAT2950(config-cmap)# match access-group name VVLAN
CAT2950(config-cmap)#class-map VLAN
CAT2950(config-cmap)# match access-group name DVLAN
CAT2950(config-cmap)#exit
CAT2950(config)#
CAT2950(config)#policy-map IPPHONE-PC
CAT2950(config-pmap)# class VVLAN
CAT2950(config-pmap-c0#  set ip dscp 46
CAT2950(config-pmap-c)#  police 1000000 8192 exceed-action-drop
CAT2950(config-pmap)# class DVLAN
CAT2950(config-pmap-c0#  set ip dscp 0
CAT2950(config-pmap-c)#  police 5000000 8192 exceed-action-drop
CAT2950(config-pmap-c)#exit
CAT2950(config-pmap)#exit
CAT2950(config)#
CAT2950(config)#interface interface-id
CAT2950(config-if)#mls qos trust device cisco-phone
CAT2950(config-if)#mls qos trust cos
CAT2950(config-if)#switchport mode access
CAT2950(config-if)#switchport voice vlan vvlan_id
CAT2950(config-if)#switchport access vlan dvlan_id
CAT2950(config-if)#service-policy input IPPHONE-PC
CAT2950(config-if)#exit
CAT2950(config)#
CAT2950(config)#ip access-list standard VVLAN
CAT2950(config-std-nacl)# permit voice_IP_subnet wild_card_mask
CAT2950(config-std-nacl)#exit
CAT2950(config)#ip access-list standard DVLAN
CAT2950(config-std-nacl)# permit data_IP_subnet wild_card_mask
CAT2950(config-std-nacl)#end
```

（注） **mls qos map cos-dscp** コマンドは、Enhanced Image（EI）でのみ使用できます。Standard Image（SI）では、このコマンドを使用できません。CoS から DSCP へのデフォルトのマッピングは、次のとおりです。

Cos 値	0	1	2	3	4	5	6	7
DSCP 値	0	8	16	24	32	40	48	56

Cisco 2970 または 3750

```
CAT2970(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT2970(config)# mls qos map policed-dscp 0 24 to 8
CAT2970(config)#
CAT2970(config)#class-map match-all VVLAN-VOICE
CAT2970(config-cmap)# match access-group name VVLAN-VOICE
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT2970(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-ANY
CAT2970(config-cmap)# match access-group name VVLAN-ANY
CAT2970(config-cmap)#
CAT2970(config-cmap)# policy-map IPPHONE-PC
CAT2970(config-pmap)#class VVLAN-VOICE
CAT2970(config-pmap-c)# set ip dscp 46
CAT2970(config-pmap-c)# police 128000 8000 exceed-action drop
CAT2970(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-ANY
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)# exit
CAT2970(config)#
CAT2970(config)#
CAT2970(config)#interface interface-id
CAT2970(config-if)# switchport voice vlan vvlan_id
CAT2970(config-if)# switchport access vlan dvlan_id
CAT2970(config-if)# mls qos trust device cisco-phone
CAT2970(config-if)# service-policy input IPPHONE-PC
CAT2970(config-if)# exit
CAT2970(config)#
CAT2970(confiig)#ip access list extended VVLAN-VOICE
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384
32767 dscp ef
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-CALL-SIGNALING
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 2000 2002
dscp cs3
CAT2970(config-ext-nacl)# 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 to 8
CAT3550(config)#class-map match-all VOICE
CAT3550(config-cmap)# match ip dscp 46
CAT3550(config-cmap)#class-map match-any CALL SIGNALING
CAT3550(config-cmap)# match ip dscp 26
CAT3550(config-cmap)# match ip dscp 24
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VVLAN-VOICE
CAT3550(config-cmap)# match vlan vvlan_id
CAT3550(config-cmap)# match class-map VOICE
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT3550(config-cmap)# match vlan vvlan_id
CAT3550(config-cmap)# match class-map CALL SIGNALING
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all ANY
CAT3550(config-cmap)# match access-group name ACL_Name
CAT3550(config-cmap)#
CAT3550(config-cmap)# class-map match-all VVLAN-ANY
CAT3550(config-cmap)# match vlan vvlan_id
CAT3550(config-cmap)# match class-map ANY
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all DVLAN-ANY
CAT3550(config-cmap)# match vlan dvlan_id
CAT3550(config-cmap)# match class-map ANY
CAT3550(config-cmap)#
CAT3550(config-cmap)#policy-map IPPHONE-PC
CAT3550(config-pmap)# class VVLAN-VOICE
CAT3550(config-pmap-c)# set ip dscp 46
CAT3550(config-pmap-c)# police 128000 8000 exceed-action drop
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class VVLAN-CALL-SIGNALING
CAT3550(config-pmap-c)# set ip dscp 24
CAT3550(config-pmap-c)# police 32000 8000 exceed-action drop
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 drop
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class DVLAN-VOICE
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 5000000 8000 exceed-action drop
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 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)# 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, 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 0 aggregate VVLAN-ANY Voice_IP_Subnet
Subnet_Mask any
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 0 aggregate PC-DATA any
CAT6500> (enable) commit qos acl IPPHONE-PC
CAT6500> (enable) set vlan vvlan_id mod/port
CAT6500> (enable) set port qos mod/port trust-device ciscoipphone
CAT6500> (enable) set qos acl map IPPHONE-PC mod/port
CAT6500> (enable)
```

ソフトウェアベースのエンドポイント

Cisco IP SoftPhone および IP Communicator は、それぞれシグナリング パケットおよびメディア パケットをマーキングしますが、Cisco IP SoftPhone または IP Communicator を実行している PC から、パケットの DSCP 値を再度マーキングするようにお勧めします。その PC は、ネットワーク上で信頼されているデバイスではないからです。メディア パケット用の UDP（ユーザ データグラム プロトコル）ポート（16384 ～ 32767）の全範囲を使用する代わりに、特定の UDP ポートを使用するように Cisco IP Softphone と Communicator を設定できます。

Cisco IP SoftPhone の場合、**Network Audio Settings** > **Audio Output Port** で UDP ポートとポート範囲を指定できます。Cisco IP Communicator の場合、次のいずれかのオプションを使用して UDP ポートを指定できます。

- IP Communicator 設定ページの製品固有のセクションで、**RTP Port Range Start** および **RTP Port Range End** を指定します。
- **Preferences** > **Audio Settings** > **Network** > **Port Range** を選択し、ポート範囲を指定します。

両方のオプションを使用して UDP ポートおよびポート範囲を設定する場合、2 番目のオプションでの設定値の方が 1 番目のオプションより優先されます。

次の項では、一般的に配置されている Cisco Catalyst スイッチ上の Cisco IP SoftPhone および IP Communicator に対して実行できる QoS 設定コマンドをリストします。

Cisco 2950（Enhanced Image 対応）

Cisco Catalyst 2950 シリーズ スイッチを、ソフトウェアベースのエンドポイント QoS の実装で使用することは推奨されていません。原因は、次の 2 つの制限です。

- Cisco 2950 では、**range** キーワードを使用して ACL 設定内で UDP ポート範囲を指定することはサポートされていません。この制限の回避策は、前の項で説明した方法で、使用する Cisco IP SoftPhone 用の単一の静的 UDP ポートを設定することです。
- Cisco 2950 は、FastEthernet ポートで 1 Mbps の増分のみサポートしています。これにより、許可されていないネットワーク トラフィックにかなり大きなホールが発生し、コール シグナリングまたはメディアの模倣が発生することがあります。

Cisco 2970 または 3750

```
CAT2970 (config) #mls qos
CAT2970 (config) #mls qos map policed-dscp 0 24 46 to 8
CAT2970 (config) #
CAT2970 (config) #class-map match-all SOFTPHONE-VOICE
CAT2970 (config-cmap) #  match access-group name SOFTPHONE-VOICE
CAT2970 (config-cmap) #class-map match-all SOFTPHONE-SIGNALING
CAT2970 (config-cmap) #  match access-group name SOFTPHONE-SIGNALING
CAT2970 (config-cmap) #exit
CAT2970 (config) #
CAT2970 (config) #policy-map SOFTPHONE-PC
CAT2970 (config-pmap-c) #class SOFTPHONE-VOICE
CAT2970 (config-pmap-c) # set ip dscp 46
CAT2970 (config-pmap-c) # police 128000 8000 exceed-action policed-dscp-transmit
CAT2970 (config-pmap-c) #class SOFTPHONE-SIGNALING
CAT2970 (config-pmap-c) # set ip dscp 24
CAT2970 (config-pmap-c) # police 32000 8000 exceed-action policed-dscp-transmit
CAT2970 (config-pmap-c) #class class-default
CAT2970 (config-pmap-c) # set ip dscp 0
CAT2970 (config-pmap-c) # police 5000000 8000 exceed-action policed-dscp transmit
CAT2970 (config-pmap-c) # exit
CAT2970 (config-pmap) #exit
CAT2970 (config) #
CAT2970 (config) #interface FastEthernet interface-id
CAT2970 (config-if) # switchport access vlan vvlan_id
CAT2970 (config-if) # switchport mode access
CAT2970 (config-if) # service-policy input SOFTPHONE-PC
CAT2970 (config-if) # exit
CAT2970 (config) #ip access list extended SOFTPHONE-VOICE
CAT2970 (config-ext-nacl) #  permit udp host PC_IP_address eq fixed_port_number any
CAT2970 (config-ext-nacl) # exit
CAT2970(config)#ip access-list extended SOFTPHONE-SIGNALING
CAT2970(config-ext-nacl)# permit tcp host PC_IP_address host CallManager_IP_address eq
2748 or 2000
CAT2970(config-ext-nacl)# exit
```

Cisco 3550

```
CAT3550 (config) #mls qos
CAT3550 (config) #mls qos map policed-dscp 0 24 46 to 8
CAT3550 (config) #
CAT3550 (config) #class-map match-all SOFTPHONE-VOICE
CAT3550 (config-cmap) #  match access-group name SOFTPHONE-VOICE
CAT3550 (config-cmap) #class-map match-all SOFTPHONE-SIGNALING
CAT3550 (config-cmap) #  match access-group name SOFTPHONE-SIGNALING
CAT3550 (config-cmap) #exit
CAT3550 (config) #
CAT3550 (config) #policy-map SOFTPHONE-PC
CAT3550 (config-pmap-c) #class SOFTPHONE-VOICE
CAT3550 (config-pmap-c) # set ip dscp 46
CAT3550 (config-pmap-c) # police 128000 8000 exceed-action policed-dscp-transmit
CAT3550 (config-pmap-c) #class SOFTPHONE-SIGNALING
CAT3550 (config-pmap-c) # set ip dscp 24
CAT3550 (config-pmap-c) # police 32000 8000 exceed-action policed-dscp-transmit
CAT3550 (config-pmap-c) #class class-default
CAT3550 (config-pmap-c) # set ip dscp 0
CAT3550 (config-pmap-c) # police 5000000 8000 exceed-action policed-dscp transmit
CAT3550 (config-pmap-c) # exit
CAT3550 (config-pmap) #exit
CAT3550 (config) #
CAT3550 (config) #interface FastEthernet interface-id
CAT3550 (config-if) # switchport access vlan vvlan_id
CAT3550 (config-if) # switchport mode access
CAT3550 (config-if) # service-policy input SOFTPHONE-PC
CAT3550 (config-if) # exit
CAT3550 (config) #ip access list extended SOFTPHONE-VOICE
CAT3550 (config-ext-nacl) #  permit udp host PC_IP_address eq fixed_port_number any
CAT3550 (config-ext-nacl) # exit
CAT3550(config)#ip access-list extended SOFTPHONE-SIGNALING
CAT3550(config-ext-nacl)# permit tcp host PC_IP_address host CallManager_IP_address eq
2748 or 2000
CAT3550(config-ext-nacl)# exit
```

Cisco 4500（SUPIII、IV、または V 使用）

```
CAT4500(config) #qos
CAT4500(config) #qos map policed-dscp 0 24 46 to 8
CAT4500(config) #
CAT4500(config) #class-map match-all SOFTPHONE-VOICE
CAT4500(config-cmap) #  match access-group name SOFTPHONE-VOICE
CAT4500(config-cmap) #class-map match-all SOFTPHONE-SIGNALING
CAT4500(config-cmap) #  match access-group name SOFTPHONE-SIGNALING
CAT4500(config-cmap) #exit
CAT4500(config) #
CAT4500(config) #policy-map SOFTPHONE-PC
CAT4500(config-pmap-c) #class SOFTPHONE-VOICE
CAT4500(config-pmap-c) # set ip dscp EF
CAT4500(config-pmap-c) # police 128 kps 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c) #class SOFTPHONE-SIGNALING
CAT4500(config-pmap-c) # set ip dscp CS3
CAT4500(config-pmap-c) # police 32000 kps 8000 byte exceed-action
policed-dscp-transmit
CAT4500(config-pmap-c) #class class-default
CAT4500(config-pmap-c) # set ip dscp default
CAT4500(config-pmap-c) # police 5 mpbs 8000 byte exceed-action policed-dscp transmit
CAT4500(config-pmap-c) # exit
CAT4500(config-pmap) #exit
CAT4500(config) #
CAT4500(config) #interface FastEthernet interface-id
CAT4500(config-if) # switchport access vlan vvlan_id
CAT4500(config-if) # switchport mode access
CAT4500(config-if) # service-policy input SOFTPHONE-PC
CAT4500(config-if) # exit
CAT4500(config) #ip access list extended SOFTPHONE-VOICE
CAT4500(config-ext-nacl) #  permit udp host PC_IP_address eq fixed_port_number any
CAT4500(config-ext-nacl) # exit
CAT4500(config)#ip access-list extended SOFTPHONE-SIGNALING
CAT4500(config-ext-nacl)# permit tcp host PC_IP_address host CallManager_IP_address eq
2748 or 2000
CAT4500(config-ext-nacl)# exit
```

Cisco 6500

```
CAT6500> (enable) set qos enable
CAT6500> (enable) set qos policed-dscp-map 0, 24, 46:8
CAT6500> (enable)
CAT6500> (enable) set qos policer aggregate SOFTPHONE-VOICE rate 128 burst 8000
policed-dscp
CAT6500> (enable) set qos policer aggregate SOFTPHONE-SIGNALING rate 32 burst 8000
policed-dscp
CAT6500> (enable) set qos policer aggregate PC-DATA rate 5000 burst 8000 policed-dscp
CAT6500> (enable)
CAT6500> (enable) set qos acl ip SOFTPHONE-PC dscp 46 aggregate SOFTPHONE-VOICE udp
host PC_IP_address eq fixed_port_number any
CAT6500> (enable) set qos acl ip SOFTPHONE-PC dscp 24 aggregate SOFTPHONE-SIGNALING
tcp host PC_IP_address host CallManager_IP_address eq 2748 or 2000
CAT6500> (enable) set qos acl ip SOFTPHONE-PC dscp 0 aggregate PC-DATA any
CAT6500> (enable) commit qos acl SOFTPHONE-PC
CAT6500> (enable) set vlan vvlan_id mod/port
CAT6500> (enable) set port qos mod/port trust untrusted
CAT6500> (enable) set qos acl map SOFTPHONE-PC mod/port
CAT6500> (enable)
```

（注） DSCP の再マーキングは、レイヤ 3 対応のスイッチが行う必要があります。アクセス レイヤ スイッチ（Cisco Catalyst 2950 with Standard Image または Cisco 3524XL など）にこの機能がない場合、DSCP の再マーキングは分散レイヤ スイッチで行う必要があります。

Cisco 無線 IP Phone 7920

デフォルトでは、Cisco 無線 IP Phone 7920 は、Per-Hop Behavior（PHB）値 AF31、または Differentiated Services Code Point（DSCP）値 26（ToS 値 0x68 に相当）を使用して SCCP シグナリング メッセージをマーキングし、PHB 値 EF、または DSCP 値 46（ToS 値 0xB8 に相当）を使用して RTP 音声パケットをマーキングします。AP でキューイングが正しく設定されており、アップストリームの最初のホップのスイッチが AP のポートを信頼するように設定されている場合、無線 IP Phone のトラフィックは、有線 IP Phone のトラフィックと同じように処理されます。この方法により、LAN と WLAN 環境で QoS 設定の一貫性を保つことができます。

さらに、Cisco 無線 IP Phone 7920 は、Cisco Discovery Protocol（CDP）を使用して、その存在を AP に自動的に伝えます。CDP パケットは無線 IP Phone から AP に送信され、これらのパケットにより電話機が特定されます。これにより、AP は、その IP Phone へのすべてのトラフィックを高プライオリティ キューに入れることができます。

通常、イーサネット スイッチ ポートは 100 Mbps での送受信が可能ですが、802.11b AP ではスループット レートがより低く、可能なデータ レートは最大で 11 Mbps です。さらに、無線 LAN は共有メディアであり、このメディアで発生するコンテンションが原因で、実際のスループットは大幅に低くなります。スループットにミスマッチがあることは、トラフィックのバースト時に AP でパケットがドロップされ、それが原因でプロセッサに過剰な負荷がかかりパフォーマンスが低下する可能性を示しています。

Cisco Catalyst 3550 および 6500 シリーズ スイッチのポリシングおよびレート制限を活用すると、AP へのトラフィックをレート制限またはポリシングするようにアップストリーム スイッチ ポートを設定することにより、AP が過剰なパケットをドロップする必要性をなくすことができます。次の項のスイッチ ポート設定は、ポートでの 802.11b のスループットを現実的な 7 Mbps にレート制限し、高優先度の音声および制御トラフィックのために 1 Mbps を確保します。また、設定例が示しているとおり、AP から送られるパケットは信頼されている必要があり、各パケットの VLAN タグに基づいて DSCP マーキングを保持またはダウンとマーキングする必要があります。このように、Voice VLAN 上の Cisco 7920 無線 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)#mls qos map policed-dscp  24 26 46 to 8
CAT3550(config)#mls qos aggregate-policer AGG-POL-1M-VOICE-OUT 1000000 8000
exceed-action policed-dscp-transmit
CAT3550(config)#mls qos aggregate-policer AGG-POL-6M-DEFAULT-OUT 6000000 8000
exceed-action drop
CAT3550(config)#
CAT3550(config)#class-map match-all EGRESS-DSCP-0
CAT3550(config-cmap)#match ip dscp 0
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all EGRESS-DSCP-8
CAT3550(config-cmap)#match ip dscp 8
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all EGRESS-DSCP-16
CAT3550(config-cmap)#match ip dscp 16
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all EGRESS-DSCP-32
CAT3550(config-cmap)#match ip dscp 32
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all EGRESS-DSCP-48
CAT3550(config-cmap)#match ip dscp 48
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all EGRESS-DSCP-56
CAT3550(config-cmap)#match ip dscp 56
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-any VOICE-SIGNALING
CAT3550(config-cmap)#match ip dscp 24
CAT3550(config-cmap)#match ip dscp 26
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VOICE
CAT3550(config-cmap)#match ip dscp 46
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-DATA
CAT3550(config-cmap)#match any
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-VVLAN-VOICE
CAT3550(config-cmap)#match vlan vvlan-id
CAT3550(config-cmap)#match class-map VOICE
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-VVLAN-VOICE-SIGNALING
CAT3550(config-cmap)#match vlan vvlan-id
CAT3550(config-cmap)#match class-map VOICE-SIGNALING
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-DVLAN
CAT3550(config-cmap)#match vlan dvlan-id
CAT3550(config-cmap)#match class-map INGRESS-DATA
CAT3550(config-cmap)#
CAT3550(config-cmap)#policy-map EGRESS-RATE-LIMITER
CAT3550(config-pmap)#class EGRESS-DSCP-0
CAT3550(config-pmap-c)#police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class EGRESS-DSCP-8
CAT3550(config-pmap-c)#police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class EGRESS-DSCP-16
CAT3550(config-pmap-c)#police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class EGRESS-DSCP-32
CAT3550(config-pmap-c)#police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class EGRESS-DSCP-48
CAT3550(config-pmap-c)#police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3550(config-pmap-c)#class EGRESS-DSCP-56
CAT3550(config-pmap-c)#police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class EGRESS-VOICE
CAT3550(config-pmap-c)#police aggregate AGG-POL-1M-VOICE-OUT
```

```
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class EGRESS-VOICE-SIGNALING
CAT3550(config-pmap-c)#police aggregate AGG-POL-1M-VOICE-OUT
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#policy-map INGRESS-QOS
CAT3550(config-pmap)#class INGRESS-VVLAN-VOICE
CAT3550(config-pmap-c)#set ip dscp 46
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class INGRESS-VVLAN-CALL-SIGNALING
CAT3550(config-pmap-c)#set ip dscp 24
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class INGRESS-DVLAN
CAT3550(config-pmap-c)#set ip dscp 0
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class class-default
CAT3550(config-pmap-c)#set ip dscp 0
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#interface interface id
CAT3550(config-if)#description 11Mb towards Wireless Access Point
CAT3550(config-if)#switchport access dvlan-id
CAT3550(config-if)#switchport voice vvlan-id
CAT3550(config-if)#mls qos trust dscp
CAT3550(config-if)#service-policy output EGRESS-RATE-LIMITER
CAT3550(config-if)#service-policy input INGRESS-QOS
```

Cisco 6500

```
CAT6500> (enable) set qos enable
CAT6500> (enable) set qos cos-dscp-map 0 8 16 24 32 46 48 56
CAT6500> (enable) set qos policed-dscp-map 24,26,46:0
CAT6500> (enable)
CAT6500> (enable) set qos policer microflow VOICE-OUT rate 1000 burst 32 policed-dscp
CAT6500> (enable) set qos policer microflow DATA-OUT rate 6000 burst 32 drop
CAT6500> (enable)
CAT6500> (enable) set qos acl ip AP-VOICE-EGRESS dscp 24 microflow VOICE-OUT ip any
any dscp-field 24
CAT6500> (enable) set qos acl ip AP-VOICE-EGRESS dscp 24 microflow VOICE-OUT ip any
any dscp-field 26
CAT6500> (enable) set qos acl ip AP-VOICE-EGRESS dscp 46 microflow VOICE-OUT ip any
any dscp-field 46
CAT6500> (enable) set qos acl ip AP-DATA-EGRESS dscp 0 microflow DATA-OUT ip any any
CAT6500> (enable)
CAT6500> (enable) set qos acl ip AP-VOICE-INGRESS dscp 24 ip any any dscp-field 26
CAT6500> (enable) set qos acl ip AP-VOICE-INGRESS trust-dscp ip any any
CAT6500> (enable) set qos acl ip AP-DATA-INGRESS dscp 0 ip any any
CAT6500> (enable)
CAT6500> (enable) set qos acl map AP-VOICE-EGRESS vvlan-id output
CAT6500> (enable) set qos acl map AP-DATA-EGRESS dvlan-id output
CAT6500> (enable) set qos acl map AP-VOICE-INGRESS vvlan-id input
CAT6500> (enable) set qos acl map AP-DATA-INGRESS dvlan-id input
CAT6500> (enable)
CAT6500> (enable) set port qos mod/port vlan-based
CAT6500> (enable)
CAT6500> (enable) set port qos mod/port trust trust-dscp
CAT6500> (enable)
```

エンドポイント機能の要約

表 17-3 は Cisco アナログ ゲートウェイ用の Cisco IP テレフォニー機能、表 17-4 は Cisco IP Phone 用の機能、表 17-5 は Cisco IP ソフトウェア デバイス用の機能をそれぞれ要約したものです。

表 17-3　アナログ ゲートウェイの機能

機能	アナログ NM	Ws-svc-cmm-24fxs	Ws-x6624-fxs	VG224	VG248	ATA 186 および 188
イーサネット接続	N	N	N	Y[1]	Y[2]	Y[3]
アナログ ポートの最大数	16	72	24	24	48	2
発信者 ID	Y	N	N	Y	Y	N
コール ウェイティング	N	N	N	N	Y	Y
コール ウェイティング時の発信者 ID	N	N	N	N	Y	N
保留	N	N	N	Y[4]	N	Y
コール転送	N	N	N	Y[4]	Y	Y
自動転送	N	N	N	N	Y[5]	Y
Ad Hoc 会議	N	N	N	N	Y	Y
Meet-Me 会議	N	N	N	N	N	Y
コール ピックアップ	N	N	N	N	N	Y
グループ ピックアップ	N	N	N	N	N	Y
リダイヤル	N	N	N	N	Y[6]	Y[6]
短縮ダイヤル	N	N	N	N	Y	Y
ボイスメールへのアクセス	Y	Y	Y	Y	Y	Y[7]
メッセージ待機インジケータ（MWI）	N	N	N	N	Y	Y[7]
Survivable Remote Site Telephony（SRST）サポート	N	N	N	Y	Y	Y
Music on Hold（MoH）	Y	Y	Y	N	Y	Y[8]
消音	N	N	N	N	N	N
Multilevel Precedence and Preemption（MLPP）	N	N	N	N	N	N
コール保持	N	N	N	N	Y[9]	N
コール アドミッション制御	Y	N	N	N	N	N
ローカル ボイス ビジーアウト	Y	N	N	N	N	N
PLAR（Private Line Automatic Ringdown）	Y	N	N	N	N	N
グループのハント	Y	N	N	N	N	N
ダイヤル プランのマッピング	Y	N	N	N	N	N
監視切断	Y	N	N	N	N	N
シグナリング パケット ToS 値のマーキング	0x68	0x68[10]	0x68	0x68	0x68	0x68
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xA0
FAX パススルー	Y[11]	Y	Y[12]	Y	Y[11]	Y
FAX リレー	Y	Y	N	Y	Y	N
SCCP（Skinny Client Control Protocol）	N	N	N	N	Y	Y
Session Initiation Protocol（SIP）	N	N	N	Y	N	Y
H.323	Y	Y	N	Y	N	Y

表 17-3　アナログ ゲートウェイの機能（続き）

機能	アナログ NM	Ws-svc-cmm-24fxs	Ws-x6624-fxs	VG224	VG248	ATA 186 および 188
メディア ゲートウェイ コントロール プロトコル（MGCP）	Y	Y	Y	Y	N	Y[13]
G.711	Y	Y	Y	Y	Y	Y
G.723	Y	N	N	N	N	Y
G.726	Y	N	N	N	N	N
G.729	Y	Y	Y	Y	Y	Y
音声アクティビティ検出（VAD）	Y	Y	N	Y	N	Y
コンフォート ノイズ生成（CNG）	Y	Y	N	Y	N	Y

1. 2 つの 10/100 Base-T
2. 1 つの 10/100 Base-T
3. ATA 188 では 2 つの 10/100 Base-T、ATA 186 では 1 つの 10 Base-T
4. H.323 および SIP でのコール制御
5. Call Forward All
6. リダイヤル
7. SCCP および SIP バージョンのみ
8. ユニキャスト MoH のみサポート
9. VG248 バージョン 1.2 以降でサポート
10. UDP ポート 2427 では MGCP シグナリングをマーキングしますが、TCP ポート 2428 ではベストエフォート型の MGCP キープアライブ パケットをマーキングします。
11. FAX パススルーおよび FAX リレー
12. FAX パススルー
13. Cisco CallManager は、ATA を使用する MGCP をサポートしていません。

表 17-4　IP Phone の機能

機能	7902G	7905G	7910G	7910 +SW	7912G	7920G	7935G、7936G	7940G	7960G	7970G
イーサネット接続	Y[1]	Y[1]	Y[1]	Y[2]	Y[2]	N	Y[3]	Y[2]	Y[2]	Y[2]
イーサネット スイッチ	N	N	N	Y	Y	N	N	Y	Y	Y
Cisco Power-Over-Ethernet（PoE）	Y	Y	Y	Y	Y	N	N	Y	Y	Y
IEEE 802.3af Power-Over-Ethernet（PoE）	N	N	N	N	N	N	N	N	N	Y
ローカリゼーション	N	Y	N	N	Y	N	N	Y	Y	Y
ディレクトリ番号	1	1	1	1	1	6	1	2	6	8
液晶ディスプレイ	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
発信者 ID	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
コール ウェイティング	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
コール ウェイティング時の発信者 ID	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
保留	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
コール転送	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
自動転送	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
自動応答	Y	Y	N	N	Y	Y	N	Y	Y	Y
Ad Hoc 会議	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Meet-Me 会議	N	Y	Y	Y	Y	Y	Y	Y	Y	Y

表 17-4　IP Phone の機能（続き）

機能	7902G	7905G	7910G	7910 +SW	7912G	7920G	7935G、7936G	7940G	7960G	7970G
コール ピックアップ	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
グループ ピックアップ	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
リダイヤル	[4] Y	Y[4]	Y[4]	Y[4]	Y[4]	Y	Y	Y	Y	Y
短縮ダイヤル	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
オンフック ダイヤル	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
ボイスメールへのアクセス	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
メッセージ待機インジケータ（MWI）	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
ビデオ コール	N	N	N	N	N	N	N	Y	Y	Y
Survivable Remote Site Telephony（SRST）サポート	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Music on Hold（MoH）	Y	Y	Y	Y	Y	Y[5]	Y	Y	Y	Y
スピーカー	N	Y[6]	Y[6]	Y[6]	Y[6]	N	Y	Y	Y	Y
ヘッドセット ジャック	N	N	N	N	N	Y[7]	N	Y	Y	Y
消音	N	N	Y	Y	N	Y	Y	Y	Y	Y
Multilevel Precedence and Preemption（MLPP）	Y	Y	Y	Y	Y	N	N	Y	Y	Y
割り込み	N	N	N	N	N	N	N	Y	Y	Y
C 割り込み	N	Y	N	N	Y	N	N	Y	Y	N
General Attribute Registration Protocol（GARP）の無効化	Y	Y	Y	Y	Y	N	N	Y	Y	Y
シグナリングおよびメディア暗号化	N	N	N	N	N	Y[8]	N	Y	Y	Y
シグナリングの完全性	N	N	N	N	N	N	N	Y	Y	Y
製造元でインストールされる証明書（X.509v3）	N	N	N	N	N	N	N	N	N	Y
現場でインストールされる証明書	N	N	N	N	N	N	N	Y	Y	N
サードパーティの XML サービス	N	Y	N	N	Y	N	N	Y	Y	Y
外部マイクおよびスピーカー	N	N	N	N	N	N	N	N	N	Y
ダイヤル プランのマッピング	N	N	N	N	N	N	N	N	N	N
シグナリング パケット ToS 値のマーキング	0x60	0x68	0x68	0x68	0x60	0x68	0x68	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
SCCP（Skinny Client Control Protocol）	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
Session Initiation Protocol（SIP）	N	Y	N	N	Y	N	N	Y	Y	N
H.323	N	Y	N	N	N	N	Y	N	N	N
メディア ゲートウェイ コントロール プロトコル（MGCP）	N	N	N	N	N	N	N	Y	Y	N
G.711	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
G.723	N	Y	N	N	N	N	N	N	N	N
G.726	N	Y	N	N	N	N	N	N	N	N
G.729	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

表 17-4　IP Phone の機能（続き）

機能	7902G	7905G	7910G	7910 +SW	7912G	7920G	7935G、7936G	7940G	7960G	7970G
音声アクティビティ検出（VAD）	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
コンフォート ノイズ生成（CNG）	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

1. 1 つの 10 Base-T
2. 2 つの 10/100 Base-T
3. 1 つの 10/100 Base-T
4. リダイヤル
5. ユニキャスト MoH のみサポート
6. 一方向のリッスン モード
7. Cisco IP Phone 7920 でサポートされている唯一のヘッドセットは、2.5 mm ジャックです。http://www.cisco.getheadsets.com で入手可能です。
8. シグナリングおよびメディア暗号化は、静的 WEP および LEAP セキュリティ設定でのみ使用できます。

表 17-5　ソフトウェア デバイスの機能

機能	IP Communicator	IP SoftPhone
ディレクトリ番号	8	6[1]
発信者 ID	Y	Y
コール ウェイティング	Y	Y
コール ウェイティング時の発信者 ID	Y	Y
保留	Y	Y
コール転送	Y	Y
自動転送	Y	Y
自動応答	Y	Y
Ad Hoc 会議	Y	Y
Meet-Me 会議	Y	N
コール ピックアップ	Y	N
グループ ピックアップ	Y	N
リダイヤル	Y	Y
短縮ダイヤル	Y	N
オンフック ダイヤル	Y	Y
ボイスメールへのアクセス	Y	Y
メッセージ待機インジケータ（MWI）	Y	Y
ビデオ コール	N	N
Survivable Remote Site Telephony（SRST）サポート	Y	N
Music on Hold（MoH）	Y	Y
スピーカー	Y	Y
消音	Y	Y
Multilevel Precedence and Preemption（MLPP）	Y	Y
割り込み	Y	N
C 割り込み	N	N
General Attribute Registration Protocol（GARP）の無効化	Y	N
シグナリングおよびメディア暗号化	N	N

表 17-5　ソフトウェア デバイスの機能（続き）

機能	IP Communicator	IP SoftPhone
シグナリングの完全性	N	N
製造元でインストールされる証明書（X.509v3）	N	N
現場でインストールされる証明書	N	N
サードパーティの XML サービス	Y	N
シグナリング パケット ToS 値のマーキング	0x60	0x68
メディア パケット ToS 値のマーキング	0xB8	0xB8
SCCP（Skinny Client Control Protocol）	Y	N
Session Initiation Protocol（SIP）	N	N
H.323	N	Y
メディア ゲートウェイ コントロール プロトコル（MGCP）	N	N
Telephony Application Programming Interface（TAPI）	N	Y
G.711	Y	Y
G.723	N	Y
G.726	N	N
G.729	Y	Y
音声アクティビティ検出（VAD）	Y	N
コンフォート ノイズ生成（CNG）	Y	N

1. スタンドアロン CTI デバイスとして

推奨されるハードウェアとソフトウェアの組み合せ

Cisco CallManager Release 4.1 ベースの Cisco IP Communications ソリューションで推奨されるハードウェア プラットフォーム、ソフトウェア リリース、およびファームウェア バージョンの最新情報については、次の Web サイトにある最新のリリース ノートおよびその他のドキュメントを定期的に確認してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/gblink/system/gbtst4x/index.htm

(注) 『Cisco IP Communications Systems Release Notes』で推奨されているプラットフォームとソフトウェア バージョンが、サポートされる唯一の配置オプションとなるわけではありません。この表のオプションは、シスコによる広範囲にわたるシステム レベルのテストに対応するハードウェアとソフトウェアの組み合せを表しています。十分な検証を重ねてきましたが、その検証には、さまざまな配置モデル、複数のエンド ステーション サイズのカテゴリ、および実際のコール フロー、トラフィック パターン、導入事例が使用されています。Cisco IP Telephony ソリューションで使用できるハードウェアとソフトウェアのその他のオプションの詳細については、製品を購入された代理店にお問い合せください。

A

AA	自動応答機能
AAD	警告とアクティビティの表示
AAR	Automated Alternate Routing
ACD	自動着信呼分配
ACF	アドミッション確認
ACL	アクセス コントロール リスト
ACS	アクセス コントロール サーバ
AD	Microsoft Active Directory
ADUC	Active Directory ユーザーとコンピュータ
AFT	ALI フォーマット ツール
AGM	Cisco アクセス ゲートウェイ モジュール
ALG	アプリケーション レイヤ ゲートウェイ
ALI	自動ロケーション識別
AMI	交互マーク反転
AMIS	Audio Messaging Interchange Specification
ANI	自動番号識別
AP	アクセス ポイント
API	アプリケーション プログラミング インターフェイス
ARJ	アドミッション拒否
ARP	アドレス解決プロトコル
ARQ	アドミッション要求
ASA	適応型セキュリティ アプライアンス
ASP	Active Server Pages
ASR	自動音声認識

ATA Cisco Analog Telephone Adapter

ATM 非同期転送モード

AVVID Cisco Architecture for Voice, Video, and Integrated Data

B

BAT Cisco Bulk Administration Tool

BBWC バッテリ バックアップ付き書き込みキャッシュ

BHCA Busy Hour Call Attempts

BHCC Busy Hour Call Completions

BPDU ブリッジ プロトコル データ ユニット

bps ビット / 秒

BRI 基本速度インターフェイス

BTN 請求先番号

C

CA 認証機関

CAC コール アドミッション制御

CAM 連想メモリ

CAMA Centralized Automatic Message Accounting

CAPF 認証機関プロキシ機能

CAR Cisco CDR 分析とレポート

CAS 個別線信号方式

CBWFQ クラスベース WFQ

CCS 共通線信号方式

CDP シスコ検出プロトコル

CDR コール詳細レコード

CIR 認定情報レート

CKM Cisco Centralized Key Management

CLEC 競争的地域通信事業者

CLID 発呼回線 ID

CMC クライアント証明書コード

CME Cisco CallManager Express

CMI Cisco Messaging Interface

CMM Cisco コミュニケーション メディア モジュール

CNG コンフォート ノイズ生成

CO セントラル オフィス

COM コンポーネント オブジェクト モデル

COR 制限クラス

CoS サービス クラス

CPCA Cisco Unity Personal Assistant

CPI Cisco Product Identification ツール

CPN 発番号

CRS Cisco Customer Response Solutions

cRTP Compressed Real-Time Transport Protocol

CSUF クロススタック UplinkFast

CTI コンピュータ / テレフォニー インテグレーション

CUE Cisco Unity Express

D

DC ドメイン コントローラ

DDNS ダイナミック ドメイン ネーム サーバ

DHCP ダイナミック ホスト コンフィギュレーション プロトコル

DID ダイヤルイン方式

DIT ディレクトリ インフォメーション ツリー

DMZ 非武装地帯

DN ディレクトリ番号

DNIS 着信番号識別サービス

DNS ドメイン ネーム システム

DoS サービス拒絶

DPA Digital PBX Adapter

DSCP DiffServ コード ポイント

DSE Digital Set Emulation

DSP デジタル信号プロセッサ

DTMF Dual Tone Multifrequency

DTPC ダイナミック伝送パワー コントロール

DUC Domino Unified Communications Services

E

E&M 受信と伝送（Ear and Mouth）

EAP 拡張可能認証プロトコル

EC エコー キャンセレーション

ECM エラー訂正モード

ECS Empty Capabilities Set

EI Enhanced Image

EIGRP Enhanced IGRP

ELIN 緊急ロケーション識別番号

EM エクステンション モビリティ

ER Cisco Emergency Responder

ERL 緊急応答ロケーション

ESF 拡張スーパ フレーム

F

FAC 強制アカウント コード

FCC 米国連邦通信委員会

FIFO ファーストイン ファーストアウト

FR フレーム リレー

FWSM ファイアウォール サービス モジュール

FXO Foreign Exchange Office

FXS Foreign Exchange Station

G

GARP 一般属性登録プロトコル

GC グローバル カタログ

GKTMP ゲートキーパー トランザクション メッセージ プロトコル

GMS グリーティング管理システム

GPO グループ ポリシー オブジェクト

GUI グラフィカル ユーザ インターフェイス

GUP Gatekeeper Update Protocol

H

H.225D H.225 デーモン

HP Hewlett-Packard

HSRP ホットスタンバイ ルータ プロトコル

HTTP ハイパーテキスト転送プロトコル

Hz ヘルツ

I

IANA Internet Assigned Numbers Authority（インターネット割り当て番号局）

IAPP アクセス ポイント間プロトコル

ICCS Intra-Cluster Communication Signaling

ICS IBM 配線システム

ICT クラスタ間トランク

IETF Internet Engineering Task Force（インターネット技術特別調査委員会）

IGMP インターネット グループ管理プロトコル

IIS Microsoft Internet Information Server

IntServ 統合サービス

IntServ/DiffServ 統合サービス / ディファレンシエーテッド サービス

IP インターネット プロトコル

IPCC Cisco IP コンタクト センター

IPIPGW IP-to-IP ゲートウェイ

IPMA Cisco IP Manager Assistant

IPSec IP Security

ISO 国際標準化機構

ITEM CiscoWorks IP Telephony Environment Monitor

ITU 国際電気通信連合

IVR 音声自動応答装置

J

JTAPI Java Telephony Application Programming Interface

K

Kbps キロビット / 秒

L

LAN ローカルエリア ネットワーク

LBR 低ビット レート

LCD 液晶ディスプレイ

LCF ロケーション確認

LDAP Lightweight Directory Access Protocol

LDIF LDAP Data Interchange Format

LDN Listed Directory Number

LEAP 簡易拡張可能認証プロトコル

LEC 地域通信事業者

LFI Link Fragmentation and Interleaving

LLQ 低遅延キューイング

LRJ ロケーション拒否

LRQ ロケーション要求

LSC ラベル スイッチ コントローラ

M

MAC メディア アクセス制御

MAN メトロポリタン エリア ネットワーク

Mbps メガビット / 秒

MCS Cisco Media Convergence Server

MCU マルチポイント コントロール ユニット

MFT Multiflex Trunk

MGCP メディア ゲートウェイ コントロール プロトコル

MIC 製造元でインストールされる証明書

MIPS 100 万命令 / 秒

MISTP マルチインスタンス スパニング ツリー プロトコル

MITM 中間者

MLA Cisco マルチレベル管理

MLP マルチリンク ポイントツーポイント プロトコル

MLPP Multilevel Precedence and Preemption

MLTS Multi-Line Telephone System

MoH Music on Hold

MPLS Multiprotocol Label Switching

MRG メディア リソース グループ

MRGL メディア リソース グループ リスト

ms ミリ秒

MTP メディア ターミネーション ポイント

mW ミリワット

MWI メッセージ待機インジケータ

N

NAT ネットワーク アドレス変換

NENA National Emergency Number Association

NFAS ノンファシリティ アソシエーテッド シグナリング

NIC ネットワーク インターフェイス カード

NPA 番号計画エリア

NSE ネットワーク サービス エンジン

NSF Network Specific Facilities

NTP ネットワーク タイム プロトコル

O

OSPF Open Shortest Path First

OU 組織ユニット

P

PBX 構内交換機

PC パーソナル コンピュータ

PCI Peripheral Component Interconnect

PCM パルス符号変調

PD 受電装置

PHB Per-Hop Behavior

PINX Private Integrated Services Network Exchange

PIX プライベート インターネット エクスチェンジ

PLAR Private Line Automatic Ringdown

PoE Power over Ethernet

POTS 一般電話サービス

pps 1 秒当たりのパケット数

PQ プライオリティ キュー

PRI Primary Rate Interface

PSAP Public Safety Answering Point

PSE 電源機器

PSTN 公衆電話交換網

PVC 相手先固定接続

Q

QBE Quick Buffer Encoding

QBSS QoS 基本サービス セット

QoS Quality of Service

QSIG Q シグナリング

R

RADIUS	Remote Authentication Dial-In User Service
RAS	登録アドミッション ステータス
RCP	リモート コピー プロトコル
RDNIS	Redirected Dialed Number Information Service
RF	無線周波数
RFC	Request for Comments
RIP	Routing Information Protocol
RSSI	相対信号強度インジケータ
RSTP	敏速スパニング ツリー プロトコル
RSVP	リソース予約プロトコル
RTMT	Cisco Real-Time Monitoring Tool
RTP	Real-Time Transport Protocol
RTT	ラウンドトリップ時間

S

S1、S2、S3、および S4	サービス リクエストのための重大度のレベル
SCCP	Skinny Client Control Protocol
SCSI	Small Computer System Interface
SDK	ソフトウェア開発キット
SDL	信号配信レイヤ
SDP	Session Definition Protocol
SE	シスコ システム エンジニア
SF	スーパー フレーム
SI	Standard Image
SIP	Session Initiation Protocol
SIW	サービス インターワーキング
SLB	サーバ ロード バランシング
SMDI	Simplified Message Desk Interface

SNMP 簡易ネットワーク管理プロトコル

SQL 構造化照会言語

SRND ソリューション リファレンス ネットワーク デザイン

SRST Survivable Remote Site Telephony

SRTP Secure Real-Time Transport Protocol

SS7 No.7 共通線信号方式

SSID サービス セット識別子

SSL Secure Sockets Layer

STP スパニング ツリー プロトコル

SUP1 Cisco スーパーバイザ エンジン 1

SUP2 Cisco スーパーバイザ エンジン 2

SUP2+ Cisco スーパーバイザ エンジン 2+

SUP3 Cisco スーパーバイザ エンジン 3

T

TAC Cisco Technical Assistance Center

TAPI テレフォニー アプリケーション プログラミング インターフェイス

TCD Telephony Call Dispatcher

TCER Total Character Error Rate

TCL Tool Command Language

TCP 伝送制御プロトコル

TCS 端末機能セット

TDD Telephone Device for the Deaf

TDM 時分割多重

TEHO テールエンド ホップオフ

TFTP Trivial File Transfer Protocol

TLS トランスポート レイヤ セキュリティ

ToD 時間帯

ToS タイプ オブ サービス

TRaP 電話機による録音と再生

TSP テレフォニー サービス プロバイダー

TTL 存続可能時間

TTS テキストと音声間の変換

TTY ターミナル テレタイプ

TUI テレフォニー ユーザ インターフェイス

U

UAC ユーザ エージェント クライアント

UAS ユーザ エージェント サーバ

UDC ユニバーサル データ コネクタ

UDLD 単方向リンク検出

UDP ユーザ データグラム プロトコル

UNC 汎用命名規則

UPS 無停電電源装置

URI ユニフォーム リソース識別子

USB ユニバーサル シリアル バス

UTIM Cisco Unity Telephone Integration Manager

UTP シールドなしツイストペア

UUIE ユーザ間情報要素

V

V3PN シスコの音声およびビデオ対応バーチャル プライベート ネットワーク

VAD 音声アクティビティ検出

VAF ボイス適応型フラグメンテーション

VATS ボイス適応型トラフィック シェーピング

VIC 音声インターフェイス カード

VLAN バーチャル LAN

VMO ViewMail for Outlook

VoIP Voice over IP

VoPSTN Voice over the PSTN

VPN バーチャル プライベート ネットワーク

VWIC 音声 /WAN インターフェイス カード

W

WAN	ワイドエリア ネットワーク
WEP	Wired Equivalent Privacy
WFQ	重み付け均等化キューイング
WLAN	無線 LAN
WLSM	Cisco 無線 LAN サービス モジュール

X

XML	eXtensible Markup Language

Symbols

Numerics

A

B

C

D

E

F

G

H

I

J

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

つ

て

と

ひ

ふ

へ

ほ

ま

む

め

も

ゆ

よ

ら

り

る

れ

ろ

わ