CHAPTER 5

# Unified Communications の配置モデル

この章では、Cisco Unified Communications システムの配置モデルについて説明します。

この章の旧版では、Cisco Unified Communications Manager（Unified CM）向けのコール処理配置モデルに基づいて、配置モデルを説明しました。これに対して、この章の最新版では、Cisco Unified Communications システムの構成技術に関する設計ガイドラインについてサイトベースで説明します。その目的は、Cisco Unified Communications システム全体の設計ガイドラインを示し、コール処理サービスにとどまらず豊富な情報を提供することです。

以前のリリースの Cisco Unified Communications での設計ガイドラインについては、次の Web サイトで入手可能な Cisco Unified Communications ソリューション リファレンス ネットワーク デザイン（SRND）のマニュアルを参照してください。

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

## この章の新規情報

表 5-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

**表 5-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報**

| 新規トピックまたは改訂されたトピック | 説明箇所 | 改訂日 |
|---|---|---|
| Cisco UCS C シリーズ ラックマウント | 「Cisco UCS C シリーズ ラックマウント」（P.5-53）<br>「C シリーズ ラックマウント サーバ上で仮想 Unified Communications アプリケーションを実行する場合の設計上の考慮事項」（P.5-55） | 2010 年 7 月 23 日 |
| Cisco Unified Communications Manager Session Management Edition | 「Session Management Edition を配置する場合の設計上の考慮事項」（P.5-27） | 2010 年 7 月 23 日 |
| Cisco Intercompany Media Engine | 「Cisco Intercompany Media Engine」（P.5-30） | 2010 年 4 月 2 日 |
| Cisco IOS Service Advertisement Framework（SAF） | 「Service Advertisement Framework のコール制御ディスカバリを使用したコール ルーティングおよびダイヤル プラン配信」（P.5-57） | 2010 年 4 月 2 日 |
| サイトベースの設計ガイドライン | 「サイトベースの設計」（P.5-2） | 2010 年 4 月 2 日 |
| 仮想サーバでの Unified Communications アプリケーション | 「仮想サーバでの Unified Communications の配置」（P.5-51） | 2010 年 4 月 2 日 |

# 配置モデル アーキテクチャ

一般に、配置モデル アーキテクチャは、サービスを提供する企業のアーキテクチャに従います。配置モデルは、企業の代表的なトポロジにおける Unified Communications ニーズを満たす参照アーキテクチャを記述します。たとえば、集中型コール処理配置モデルは、1 箇所または数箇所の中央集中型の本社に接続された多数のサイトで業務の大部分が行われる企業に向いたモデルです。

場合によっては、技術的制約のために技術の配置モデルが企業の配置モデルから逸脱することがあります。たとえば、企業に 1 つあるキャンパスのスケールが 1 つのサービス インスタンス（Cisco Unified Communications Manager が提供するコール処理サービスなど）のスケールを超えている場合、1 つのキャンパスに複数のコール処理クラスタ インスタンスまたは複数のメッセージング製品が必要になることがあります。

## 配置モデルの高可用性

Unified Communications サービスは、高可用性を実現するための機能を数多く備えています。その実装には、次のようにさまざまな方法があります。

- フェールオーバー冗長性

  不可欠なサービスの場合、設計に単一障害点が存在しないように冗長な要素を配置します。2 つ（またはそれ以上）の要素間の冗長性が自動的に確保されます。たとえば、Cisco Unified Communications Manager（Unified CM）に使用されているクラスタ化技術では、最大 3 台のサーバがお互いをバックアップできます。このタイプの冗長性は、技術的境界を越えて実現される場合もあります。たとえば、1 台の電話機に対して、優先順位 3 番目までの呼制御エージェントとして、同じコール処理クラスタに属する 3 台の独立した Unified CM サーバを設定できます。そして 4 番目の選択肢として、Cisco IOS ルータを利用してコール処理サービスを提供するように電話機を設定することもできます。

- リンクの冗長性

  1 つの WAN リンクでの障害に対処するために、IP WAN リンクなどの冗長な IP リンクを配置すると有益な場合があります。

- 地理的多様性

  一部の製品は、冗長なサービス ノードを WAN リンク越しに分散させて、（あらかじめ設定しておいた UPS および発電バックアップ システムの機能を超えて長時間停電が発生するなど）サイト全体がオフラインになっても、別の場所にある別のサイトで事業を継続できるようにしています。

## 配置モデルのキャパシティ プランニング

さまざまな配置モデルのキャパシティは、一般にその基となる製品のキャパシティと切り離すことができません。この章では、適宜キャパシティについて説明します。サービスをサポートしている製品をこのドキュメントの他の項で詳しく取り上げている場合、その項でその製品のキャパシティについて説明します。

# サイトベースの設計

Cisco Unified Communications システムを構成するどの技術でも、設計時に検討する基準として次のものがあります。

### サイズ

このコンテキストでのサイズとは一般にユーザ数を指し、これが IP 電話、ボイスメールボックス、プレゼンス ウォッチャなどの数量に読み換えられます。また、データセンターなど、ユーザがほとんど（あるいはまったく）存在しないサイトでは、処理キャパシティの点からサイズを考えることもできます。

### ネットワーク接続

サイトをシステムの他の部分への接続を設計する際に考慮が必要な主な要素が 3 つあります。

- Quality of Service（QoS; サービス品質）を確保できる帯域幅
- 遅延
- 信頼性

多くの場合、Local Area Network（LAN; ローカル エリア ネットワーク）ではこれらの要素は十分達成されています。すべての LAN 機器で QoS が達成されており、帯域幅は一般にギガビット範囲、遅延は最小限（数ミリ秒程度）で、優れた信頼性が標準で確保されています。

Metropolitan Area Network（MAN; メトロポリタン エリア ネットワーク）では、3 つの要素とも LAN に近いものとなっています。帯域幅は一般にまだ数メガビット範囲、遅延は一般に数十ミリ秒で、優れた信頼性が確保されています。一般にパケット処理ポリシーが MAN プロバイダーから提供されるため、エンドツーエンドの QoS を実現できます。

Wide Area Network（WAN; ワイド エリア ネットワーク）では、これらの要素に特に注意する必要があります。帯域幅はコストが何よりも重視され、遅延は実効的な送出速度だけでなく物理的な距離にかかわる実際の伝搬遅延にも左右されることがあり、信頼性はさまざまな要因の影響を受けます。また、QoS 実現のために、余分な運用コストと設定作業が必要になることもあります。

帯域幅は、サイトで利用できる Unified Communications サービスのタイプおよびサービスの提供方法に大きな影響を与えます。たとえば、20 人のユーザにサービスを提供するサイトがシステムの他の部分に 1.5 Mbps の帯域幅で接続している場合、サイトの音声、プレゼンス、インスタント メッセージング、電子メール、およびビデオ サービスをリモートのデータセンター サイトに問題なくホストできます。その同じサイトが 1000 人のユーザをホストしている場合、比較的限られた帯域幅がシグナリングおよびメディア フローで飽和状態になるのを避けるために、サービスの一部をローカルにホストするのが最善です。これ以外にもう 1 つ、リモートのデータセンター サイトから WAN 全体にサービスを配信できるよう帯域幅を拡大する方法もあります。

遅延が設計に与える影響は、リモートに配置する Unified Communications サービスのタイプに応じて異なります。たとえば、片方向の遅延が 200 ms である WAN 全体に音声サービスを提供する場合、ダイヤルトーン遅延やメディア カットスルー遅延増大などの問題が発生することがあります。プレゼンスなど他のサービスでは、200 ms の遅延があっても問題が発生しない可能性があります。

サイトからネットワークの他の部分への接続の信頼性は、技術に適した配置モデルを決定する際の基本的な考慮事項です。信頼性が高い場合は、ほとんどの Unified Communications コンポーネントではリモート サイトからホストされるサービスを配置できます。信頼性が安定しない場合、一部の Unified Communications コンポーネントはリモートからホストされる際に正しく実行されないことがあります。信頼性が低いと、サイトに Unified Communications サービスのコロケーションが必要になることがあります。

### 高可用性要件

サービスの高可用性は常に設計の目標となるものです。信頼性の必要性とその実現に伴うコストとのバランスを保つには、実際的な設計の判断が必要です。次のいずれの要素も、設計が高可用性を実現できるかどうかに影響を与えます。

- 帯域幅の信頼性。Unified Communications サービスの配置モデルに直接影響を与えます。
- 電源の可用性

停電は、どんなシステムでも極めて破壊的な事象です。停電中はサービスが利用できなくなるだけでなく、電力復旧によってリプル効果がもたらされるためです。電力の可用性が高いサイト（たとえば、Uninterruptible Power Supply [UPS; 無停電電源装置 ] および発電装置によるバックアップを備えて、電力グリッド接続が安定しているサイト）は、一般に Unified Communications サービスのホストに選択できます。サイトの電力可用性に一貫性がない場合、そのサイトをホスト用のサイトとして使用するのは賢明な判断ではありません。

- 熱、湿度、振動などの環境要因
- 能力ある人材の確保

  一部の Unified Communications サービスは、サーバなど定期的な保守を必要とする機器を使用して配信されます。Unified Communications コール エージェント サーバのホストなど、一部の Unified Communications 機能は、能力ある人材が配属されているサイトに配置するのが最善です。

# サイトベースの設計ガイドライン

このドキュメント全体を通して、さまざまな Unified Communications サービスおよび技術の系列に沿って設計ガイドラインを編成しています。たとえば、コール処理の章では、コール処理サービスを実際に説明するだけでなく、サイトのサイズ、ネットワーク接続、および高可用性の要件に基づいて IP Phone および Cisco Unified Communications サーバを配置するための設計ガイドラインも示します。同様に、コール アドミッション制御の章では、技術自体の説明に焦点を当てるだけでなく、サイトベースの設計考慮事項も示します。

一般に、特定の Unified Communications サービスまたは技術のほとんどの側面が、サイトのサイズまたはネットワーク接続とは関係なく、すべての配置に関係しています。必要に応じて、サイトベースの設計考慮事項について説明します。サービスは集中化、分散化、インターネットワーク化、および地理的多様化が可能です。

# サービスの集中化

企業の支店サイトが地理的に分散し、ワイド エリア ネットワークで相互接続されている用途では、Cisco Unified Communications サービスを中央に配置しつつ、WAN 接続でエンドポイントにサービスを提供できます。たとえば、コール処理サービスを集中的に配置できます。テレフォニー サービスの配信に必要なのは、リモート サイトとの IP 接続だけです。同様に、Cisco Unity Connection プラットフォームから提供されるようなボイス メッセージ サービスも中央にプロビジョニングして、IP WAN で接続されたリモートからサービスをエンドポイントに配信できます。

中央にプロビジョニングした Unified Communications サービスは、WAN 接続中断の影響を受けます。そのため、サービスごとに、ローカル サバイバビリティ オプションを計画すべきです。たとえば、Cisco Unified CM から提供されるようなコール処理サービスには、SRST や Cisco Unified Communications Manager Express（Unified CME）などのローカル サバイバビリティ機能を設定できます。同様に、Cisco Unity Connection のような集中型ボイス メッセージ サービスは、SRST または Unified CME で運用するリモート サイトから中央サイトのボイス メッセージ サービスへは公衆網経由でアクセスできるようにプロビジョニングできます。

すべての Unified Communications サービスでサービスの集中化を統一する必要はありません。たとえば、複数のサイトが 1 つの集中型コール処理サービスを利用する場所にシステムを配置し、一方で Cisco Unity Express などの非集中型（分散型）ボイス メッセージ サービスでそのシステムをプロビジョニングすることもできます。同様に、Cisco Unity Connection などの集中型ボイス メッセージ サービスとともに、Cisco Unified Communications Manager Express を使用してコール処理が各サイトでローカルにプロビジョニングされる形態で Unified Communications システムを配置することもできます。

多くの場合、各サービスの設計時に考慮すべき主要な基準は、サイト間の IP ネットワークの可用性と品質です。サイト間の IP 接続が次の特性を備えている場合、Unified Communications サービスの集中化は、機器のホストと運用に伴う資本費用と運用費用のどちらの面でもスケールメリットが得られます。

- 予想されるトラフィック負荷に十分対応できる帯域幅。ボイスメールへのアクセス、集中型の公衆網接続へのアクセス、音声やビデオを含むサイト間オンネット通信などによって発生する、ピーク時のアクセス負荷も含めます。
- 高可用性。WAN サービス プロバイダーがサービス レベル契約に従って接続を迅速に保守および復旧することによりもたらされます。
- 低遅延。主要な中央サイトへのラウンドトリップ時間のためにシステムの応答時間に遅延が発生しても、リモート サイトのローカルなイベントは損害を受けません。

また、特定のサービスを中央に配置して複数のサイトのエンドポイントにサービスを提供した場合、複数のサイトでユーザに同じ処理リソースを使用することから、機能の透過性という利点が得られます。たとえば、2 つのサイトに同じ集中型 Cisco Unified Communications Manager クラスタからサービスを提供する場合、ユーザは 2 つのサイト間でライン アピアランスを共有できます。各サイトに異なる（分散した）コール処理システムからサービスを提供する場合には、この利点は得られません。

機能の透過性およびスケール メリットという利点は、Unified Communications トラフィックの需要に応えるために WAN ネットワークを構築および運用する際の相対的コストに照らして評価する必要があります。

## サービスの分散化

Unified Communications サービスは、複数のサイトに分散させて個別に配置することもできます。たとえば、2 つ（またはそれ以上の）のサイトを独立したコール処理 Cisco Unified CME ノードでプロビジョニングできます。同じ場所にあるエンドポイントに対するサービスの可用性を確保するために WAN を利用する必要はありません。同様に、サイトを Cisco Unity Express などの独立したボイス メッセージ システムでプロビジョニングできます。

Unified Communications サービスを分散させた場合の主な利点は、配置方法が WAN 接続の相対的な可用性およびコストに依存しないことです。たとえば、WAN 接続が使用できないか、極めて費用がかかるか、または信頼性が高くないリモートの場所でサイトを運用している場合、そのリモート サイト内で Cisco Unified Communications Manager Express などの独立したコール処理ノードをプロビジョニングすると、WAN がダウンしてもコール処理の中断が回避されます。

## サービスのインターネットワーク化

2 つのサイトを独立したサービスでプロビジョニングした場合でも、両サイトを相互接続してサイト間で機能の透過性をある程度実現できます。たとえば、Cisco Unified Communications Manager Express でプロビジョニングした分散コール処理サービスを H.323 トランクまたは SIP トランクでインターネットワーク化して、サイト間で IP コールを許可できます。同様に、Cisco Unity Connection または Cisco Unity Express の独立したインスタンスを同じメッセージング ネットワークに参加させることによって、ユニファイド メッセージ ネットワーク内でメッセージをルーティングしたり、サブスクライバ情報およびディレクトリ情報を交換したりできます。

# Unified Communications サービスの地理的多様性

一部のサービスを IP WAN 越しで複数の冗長なノードにプロビジョニングすると、停電やネットワーク障害でサイトが中断したり、火事や地震などの災害でサイトの物理的な整合性が損なわれたりしても、サービスを継続できます。

このような地理的多様性を実現するには、個々のサービスが冗長なノードをサポートするだけでなく、IP WAN の遅延と帯域幅の制約を越えてこれらのノードを配置できる必要があります。たとえば、ノード間のエンドツーエンドの合計ラウンドトリップ時間が 80 ms を超えず、適度な容量の QoS 対応帯域幅をプロビジョニングしている限り、Unified CM のコール処理サービスは単一クラスタのコール処理ノードを IP WAN 越しに配置できます。これに対して、Unified CME は冗長性を備えていないため、地理的に多様な構成に配置できません。

表 5-2 に、各 Cisco Unified Communications サービスを上記の方法で配置できるかどうかをまとめます。

**表 5-2　Cisco Unified Communications サービスに使用可能な配置オプション**

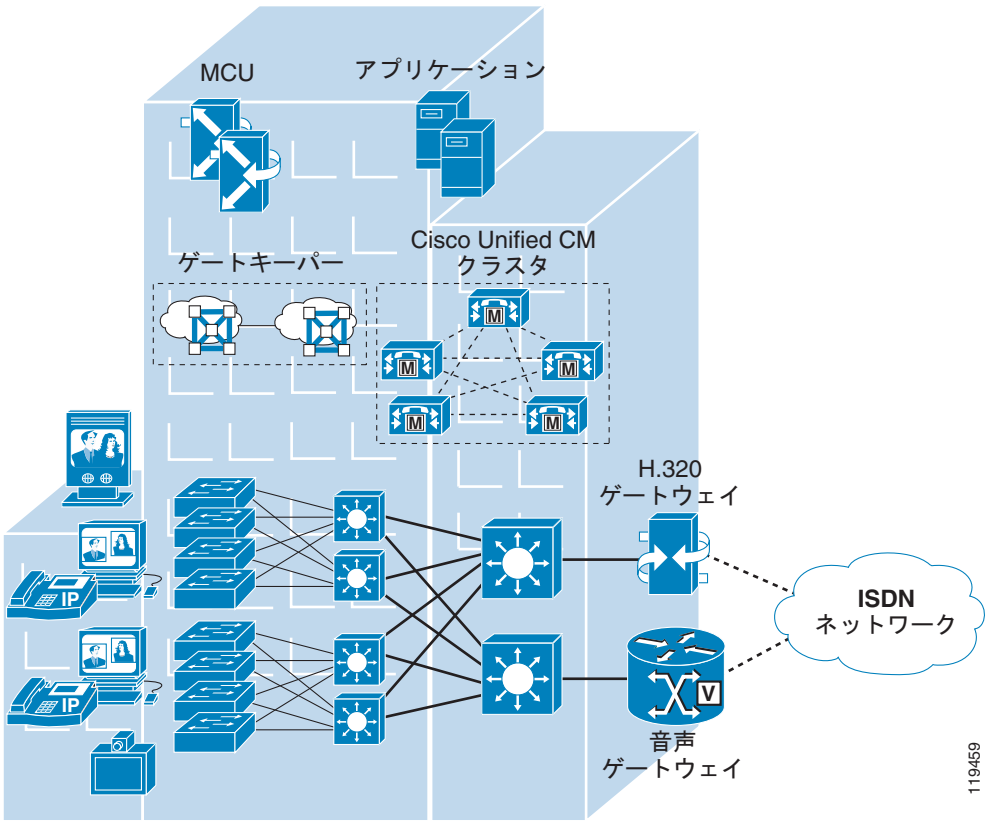
| サービス | 集中型 | 分散型 | インターネットワーク化 | 地理的多様性 |
|---|---|---|---|---|
| Cisco Unified CM | 可 | 可 | 可 | 可 |
| Cisco Unified CME | 不可 | 可 | 可 | 不可 |
| Cisco Unified CMBE | 可 | 可 | 可 | 不可 |
| Cisco Unity Express | 不可 | 可 | 可（Cisco Unified Messaging Gateway を使用） | 不可 |
| Cisco Unity | 可 | 可（サイトごとに 1 つの Cisco Unity） | 可（Cisco Unified Messaging Gateway を使用） | 可 |
| Cisco Unity Connection | 可 | 可（サイトごとに 1 つの Cisco Unity Connection） | 可（Cisco Unified Messaging Gateway を使用） | 可 |
| Cisco Emergency Responder | 可 | 可（サイトごとに 1 つの Emergency Responder グループ） | 可（Emergency Responder クラスタ化を使用） | 可 |
| Cisco Unified Presence | 可 | 可（サイトごとに 1 つの Cisco Unified プレゼンス） | 可（ドメイン間フェデレーションを使用） | 不可 |
| Cisco Unified Mobility | 可 | 可（Unified CM シングル ナンバー リーチとして） | 不可 | 可 |

コール処理は基本的なサービスであるため、この章では基本コール処理配置モデルについて説明します。Cisco Unified Communications Manager コール処理の技術的詳細については、「コール処理」（P.8-1）の章を参照してください。

# キャンパス

このコール処理配置モデルでは、Unified Communications サービスとエンドポイントはキャンパスの同じ場所にあります。サービス ノード、エンドポイント、およびアプリケーション間の QoS 対応ネットワークは高い可用性を実現しており、帯域幅は事実上無制限で、エンドツーエンドの遅延は 15 ms 未満です。同様に、電源の品質および可用性は極めて高く、サービスは適切なデータセンター環境にホストされます。エンドポイント間の通信は、LAN または MAN を通過し、企業外部の通信は公衆網などの外部ネットワークを経由します。企業は、一般に LAN または MAN で接続された 1 つまたは複数のまとまったビルにキャンパス モデルを配置します。

図 5-1　キャンパス配置の例




キャンパス モデルの設計上の特長は、次のとおりです。

- 単一の Cisco Unified CM クラスタ。一部のキャンパス コール処理配置では、複数の Unified CM クラスタが必要になる場合があります。たとえば、コールの対象となるエンドポイントの数が多すぎて単一のクラスタでは対応できない場合や、クラスタをコール センターなどの用途に限る必要がある場合などです。
- Unified CM クラスタあたり最大 30,000 の設定済みおよび登録済み Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone または SCCP ビデオ エンドポイント。
- Unified CM クラスタごとに最大 2,100 のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H.323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）。
- キャンパスの外部にある宛先へ向かうすべてのコール用のトランクやゲートウェイ（IP または公衆網）。
- 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）に対応する、同じ場所のデジタル シグナル プロセッサ（DSP）リソース。
- メッセージング（ボイスメール）、プレゼンス、モビリティなどその他の Unified Communications サービスも一般に同じ場所に設置されます。
- PBX やボイスメール システムなど従来の音声サービスへのインターフェイスがキャンパス内に接続されるため、帯域幅または接続に運用コストがかかりません。
- マルチポイント ビデオ会議には、Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）リソースが必要です。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。

- 公衆 ISDN 網上で H.320 ビデオ会議デバイスと通信するために H.323 および H.320 ビデオ ゲートウェイが必要です。
- サイト内のデバイス間では、広帯域オーディオ（G.722 や Cisco Wideband Audio など）が使用できます。
- サイト内のデバイス間では、広帯域ビデオ（384 kbps 以上など）が使用できます。7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec もサポートされます。

## キャンパス 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。

- インフラストラクチャが高可用性で、QoS に対応し、復元性、高速コンバージェンス、およびインライン パワーを備えていることを確認します。
- 自社内のコール パターンを知っておく必要があります。キャンパス 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 Media Termination Point（MTP; メディア ターミネーション ポイント）などの他の機能に割り当てることができます。
- 高可用性、電話機用の接続オプション（インライン パワー）、Quality of Service（QoS）メカニズム、およびセキュリティ用の推奨ネットワーク インフラストラクチャを実装しています （「ネットワーク インフラストラクチャ」（P.3-1）を参照）。
- 「コール処理」（P.8-1）の章にリストされているプロビジョニングの推奨事項を実行します。

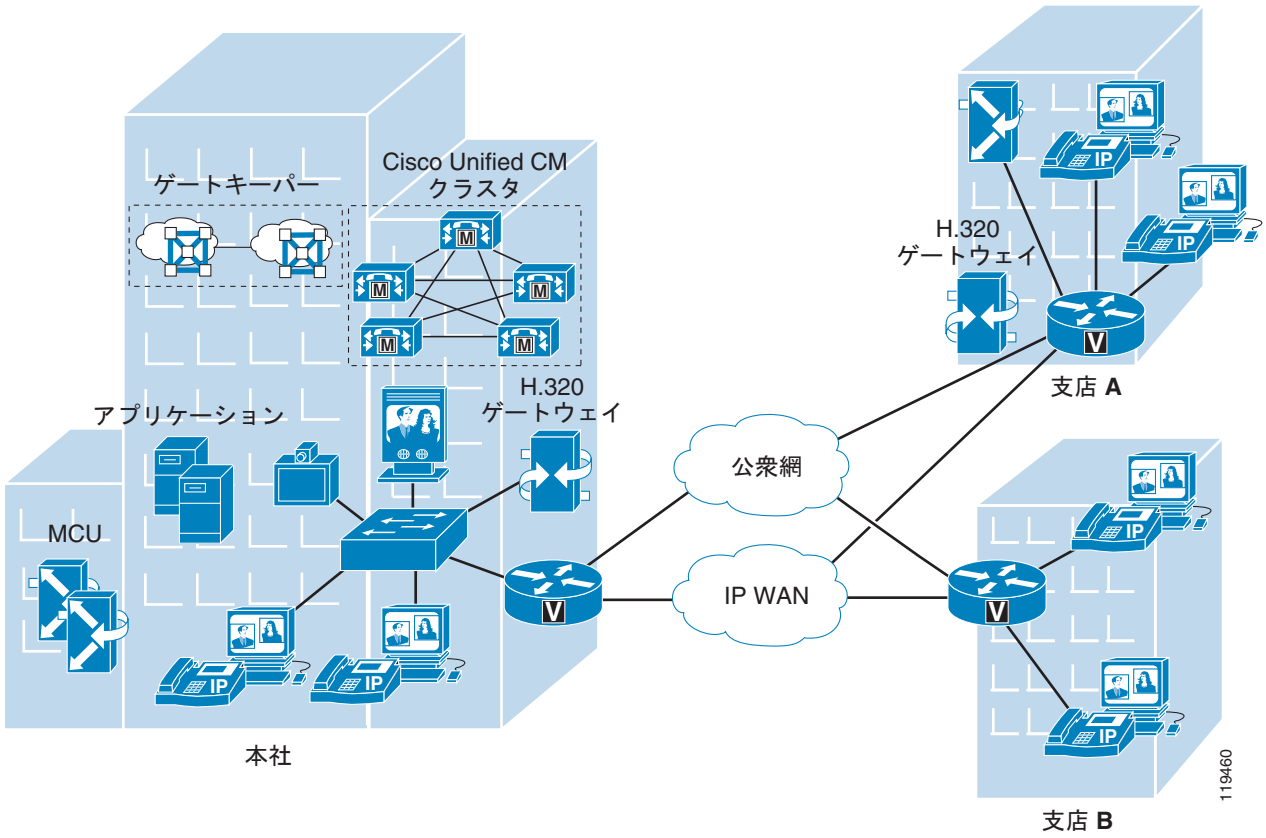
# 集中型コール処理を使用するマルチサイト

このコール処理配置モデルでは、エンドポイントは QoS 対応のワイド エリア ネットワークを越えてコール処理サービスとは離れた場所に置かれます。WAN 全体で利用できる帯域幅の容量が限られているため、特定の WAN リンクで認められるコールの数を管理して、負荷を使用可能な帯域幅の制限内に収めるには、コール アドミッション制御メカニズムが必要です。エンドポイント間のオンネット通信は、LAN/MAN（エンドポイントが同じサイトにある場合）または WAN（エンドポイントが異なるサイトにある場合）のいずれかを通過します。企業外部の通信は、エンドポイントと同じ場所または別の場所（たとえば、メイン サイトで集中型ゲートウェイを使用している場合や、企業ネットワーク全体で Tail End Hop Off [TEHO; テールエンド ホップオフ ] を行っている場合）に配置できるゲートウェイを介して、公衆網などの外部ネットワークを経由します。

IP WAN は、中央サイトとリモート サイト間の呼制御シグナリングも伝送します。図 5-2 は、一般的な集中型コール処理配置を示しています。この配置では、中央サイトのコール処理エージェントとして Unified CM クラスタを使用し、すべてのサイトを接続するために、QoS 対応の IP WAN を使用します。この配置モデルでは、管理と保守全体のコストを削減するために、ボイス メッセージ、プレゼンス、モビリティなど他の Unified Communications サービスも中央サイトにホストすることがよくあります。WAN の信用性が低い場合や、WAN 帯域幅のコストが高い場合には、サービスの可用性が WAN の障害の影響を受けないように、ボイス メッセージ（ボイスメール）など一部の Unified Communications サービスを分散させることができます。

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

**図 5-2　集中型コール処理を使用するマルチサイト配置**




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

- 単一の Unified CM クラスタ。一部の集中型コール処理配置では、複数の Unified CM クラスタが必要になる場合があります。たとえば、コールの対象となるエンドポイントの数が多すぎて単一のクラスタでは対応できない場合や、クラスタをコール センターなどの用途に限る必要がある場合などです。
- クラスタあたり最大 30,000 の設定済みおよび登録済み Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone または SCCP ビデオ エンドポイント。
- Unified CM クラスタあたり最大 2,000 のロケーションまたは支店サイト。
- Unified CM クラスタごとに最大 2,100 のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H.323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）。
- すべてのオフネット コールのための公衆網接続。
- 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）用のデジタル シグナル プロセッサ（DSP）リソースを各サイトにローカルに分散させて、DSP を必要とするコールが消費する WAN 帯域幅の容量を削減します。

- 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。PBX やボイスメール システムなど従来の音声サービスへのインターフェイスを中央サイト内に接続できるため、帯域幅または接続に運用コストがかかりません。リモート サイトにある従来のシステムに接続するには、余分な WAN 帯域幅のプロビジョニングに伴う運用費が必要になる場合があります。
- コールを発信するためにゲートキーパーを必要とする H.323 クライアント、MCU、および H.323/H.320 ゲートウェイを、Cisco IOS ゲートキーパーに登録することが必要です。Unified CM は H.323 トランクを使用してゲートキーパーと統合し、そこに登録された H.323 デバイスのコール ルーティングと帯域幅管理サービスを提供します。複数の Cisco IOS ゲートキーパーを使用して、冗長性を提供することもできます。
- マルチポイント ビデオ会議には MCU リソースが必要です。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。すべてのリソースが中央サイトに存在していても、ローカル会議リソースが必要な場合はリモート サイトに分散していてもかまいません。
- 公衆 ISDN 網上で H.320 ビデオ会議デバイスと通信するために H.323/H.320 ビデオ ゲートウェイが必要です。これらのゲートウェイは中央サイトにあっても、ローカル ISDN アクセスが必要な場合はリモート サイトに分散していてもかまいません。
- サイト内のデバイス間では広帯域オーディオ（G.711、G.722、Cisco Wideband Audio など）を自動的に選択し、一方異なるサイトのデバイス間では狭帯域オーディオ（G.729 や G.728 など）を選択できます。
- 同じサイト内のデバイス間では広帯域ビデオ（384 kbps 以上など）、異なるサイトのデバイス間では狭帯域ビデオ（128 kbps など）を自動的に選択できます。同じサイト内のデバイス間のコールに限っては、7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec を推奨します。
- WAN でビデオを発信するときには、WAN リンク速度を最低でも 768kbps 以上にする必要があります。
- Unified CM ロケーション（静的または RSVP 対応）では、コール アドミッション制御を提供します。
- 音声コールおよびビデオ コールの場合、帯域幅不足のためにコール アドミッション制御がコールを拒否したときには、Automated Alternate Routing（AAR; 自動代替ルーティング）により、公衆網を介して自動的にコールを再ルーティングできます。AAR は、ゲートウェイを利用して発信側電話機から公衆網へ向かうコールをルーティングし、着信側電話機に接続される別のゲートウェイを利用してリモート サイトで公衆網からのコールを受け付けます。
- リモート WAN リンク障害のためにエンドポイントが未登録であると見なされたときには、Call Forward Unregistered（CFUR）機能により、公衆網経由で自動的にコールを再ルーティングできます。CFUR は、ゲートウェイを利用して呼び出し元の電話機から公衆網へ向かうコールをルーティングし、呼び出し先の電話機に接続される別のゲートウェイを利用してリモート サイトで公衆網からのコールを受け付けます。
- ビデオ用 Survivable Remote Site Telephony（SRST）。WAN 接続で障害が発生すると、リモート サイトにある SCCP ビデオ エンドポイントが音声だけのデバイスになります。
- SRST ルータの代わりに Cisco Unified Communications Manager Express（Unified CME）を使用して、リモート サイトのサバイバビリティ（コール処理の継続）を確保することもできます。
- Cisco Unified Communications Manager Express（Unified CME）は、支店またはリモート サイトで Cisco Unity サーバと統合可能。Cisco Unity サーバは、中央サイトの Unified CM に通常モードで登録され、Unified CM が到達不能の場合や WAN の障害時は、Unified CME に SRST モードでフォール バックできます。これにより支店のユーザは、MWI を使用してボイスメールにアクセスできます。

IP WAN の接続オプションは、次のとおりです。

- 専用回線
- フレーム リレー

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

WAN エッジに置かれているルータには、プライオリティ キューイングやトラフィック シェーピングなどの QoS メカニズムが装備されていて、WAN の帯域幅が恒常的に不足している場合に、データ トラフィックから音声トラフィックを保護しています。加えて、音声トラフィックによる WAN リンクのオーバーサブスクリプションや確立されたコールの品質低下を防止するために、コール アドミッション制御方式が必要です。集中型コール処理配置の場合は、Unified CM 内に設定された *ロケーション*（静的または RSVP 対応）でコール アドミッション制御が行われます （ロケーションの詳細については、「コール アドミッション制御」（P.11-1）の章を参照してください）。

リモート サイトでは、さまざまな Cisco ゲートウェイにより、公衆網を介したアクセスが可能です。IP WAN で障害が発生した場合や、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 サイトのユーザからのコールは、公衆網経由で再ルーティングできます。Cisco Unified Survivable Remote Site Telephony（SRST）機能は、SCCP および SIP 電話機の両方で使用可能です。Cisco Unified IP Phone が、リモートの 1 次、2 次、および 3 次 Unified CM への接続を失った場合、または WAN 接続がダウンした場合に、支店でのコール処理を提供します。Cisco Unified SRST 機能は、SRST 機能を実行する Cisco IOS ゲートウェイ、または SRST モードで動作する Cisco Unified CME で使用できます。SRST モードで動作する Unified CME では、Cisco IOS ゲートウェイの SRST よりも多くの機能が電話機に提供されます。

# 集中型コール処理モデルのベスト プラクティス

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

- 音声のカットスルー遅延（クリッピングとも呼ばれます）を減らすために、Unified CM とリモート ロケーション間の遅延を最小限に抑えます。
- Unified CM 内のロケーション（静的または RSVP 対応）でリモート支店との間のコール アドミッション制御が行われるように設定する。このメカニズムをさまざまな WAN トポロジに適用する方法については、「コール アドミッション制御」（P.11-1）の章を参照してください。
- 各リモート サイトでの Survivable Remote Site Telephony（SRST）モードでサポートされている IP Phone およびライン アピアランスの数は、その支店内にあるルータのプラットフォーム、取り付け済みメモリ容量、および Cisco IOS リリースにより異なります。Cisco IOS ゲートウェイの SRST では最大 1,500 台の電話機がサポートされますが、SRST モードで動作する Unified CME の場合は、最大 350 台です （SRST または Unified CME プラットフォームおよびコード仕様に関する詳細は、http://www.cisco.com から入手できる SRST および Unified CME の文書を参照してください）。一般的には、特定サイトに対して集中型コール処理か、分散コール処理かを決定するには、次に示す種々の要素によります。
  - IP WAN 帯域幅、または遅延制限
  - 音声ネットワークに関する臨界状況
  - 機能セットの必要性
  - スケーラビリティ
  - 管理の容易性
  - コスト

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

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

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

# リモート サイトのサバイバビリティ（呼処理の継続）

集中型コール処理モデルで WAN を介した Cisco Unified Communications を配置する場合、リモート サイトのデータ サービスと音声サービスの高可用性を確保するために、追加の処置が必要です。表 5-3 では、リモート サイトでの高可用性を提供するためのさまざまな方法をまとめています。これらの方法のいずれを選択するかは、ビジネスまたはアプリケーションの特殊な要件、可用性が高いデータ サービスと音声サービスに関連した優先順位、コストの考慮事項などの複数の要素によって異なります。

**表 5-3　リモート サイトの高可用性を提供する方法**

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

表 5-3 にリストされている最初の 2 つのソリューションは、IP WAN アクセス ポイントに冗長性を追加して、リモート IP Phone と中央の Unified CM との間の IP 接続を常に保持することによって、ネットワーク インフラストラクチャ層に高い可用性を提供します。これらのソリューションは、データ サービスと音声サービスの両方に適用され、コール処理層からはまったく見えません。このオプションは、支店ルータでの冗長 IP WAN リンクの追加から、冗長 IP WAN リンクを備えた 2 つ目の支店ルータ プラットフォームの追加までにわたります。

表 5-3 の 3 番目と 4 番目のソリューションでは、ISDN バックアップ リンクを使用して、WAN 障害時の存続可能性を提供します。ISDN バックアップ用には、次の 2 つの配置オプションがあります。

- データのみの ISDN バックアップ

  このオプションでは、ISDN はデータのみの存続可能性の確保に使用され、一方 SRST または SRST モードの Unified CME は音声のサバイバビリティの確保に使用されます。Skinny Client Control Protocol（SCCP）、H.323、Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）、Session Initiation Protocol（SIP）などのテレフォニー シグナ

リング プロトコルからのトラフィックが ISDN インターフェイスに入らないように支店ルータにアクセス制御リストを設定して、IP Phone からの信号が中央サイトの Unified CM に到達しないようにする必要があることに注意してください。これにより、支店にあるテレフォニー エンドポイントは WAN の障害を検出し、ローカル SRST リソースを利用するようになります。

- データと音声の ISDN バックアップ

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

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

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

図 5-3　Survivable Remote Site Telephony（SRST）または SRST モードの Unified CME

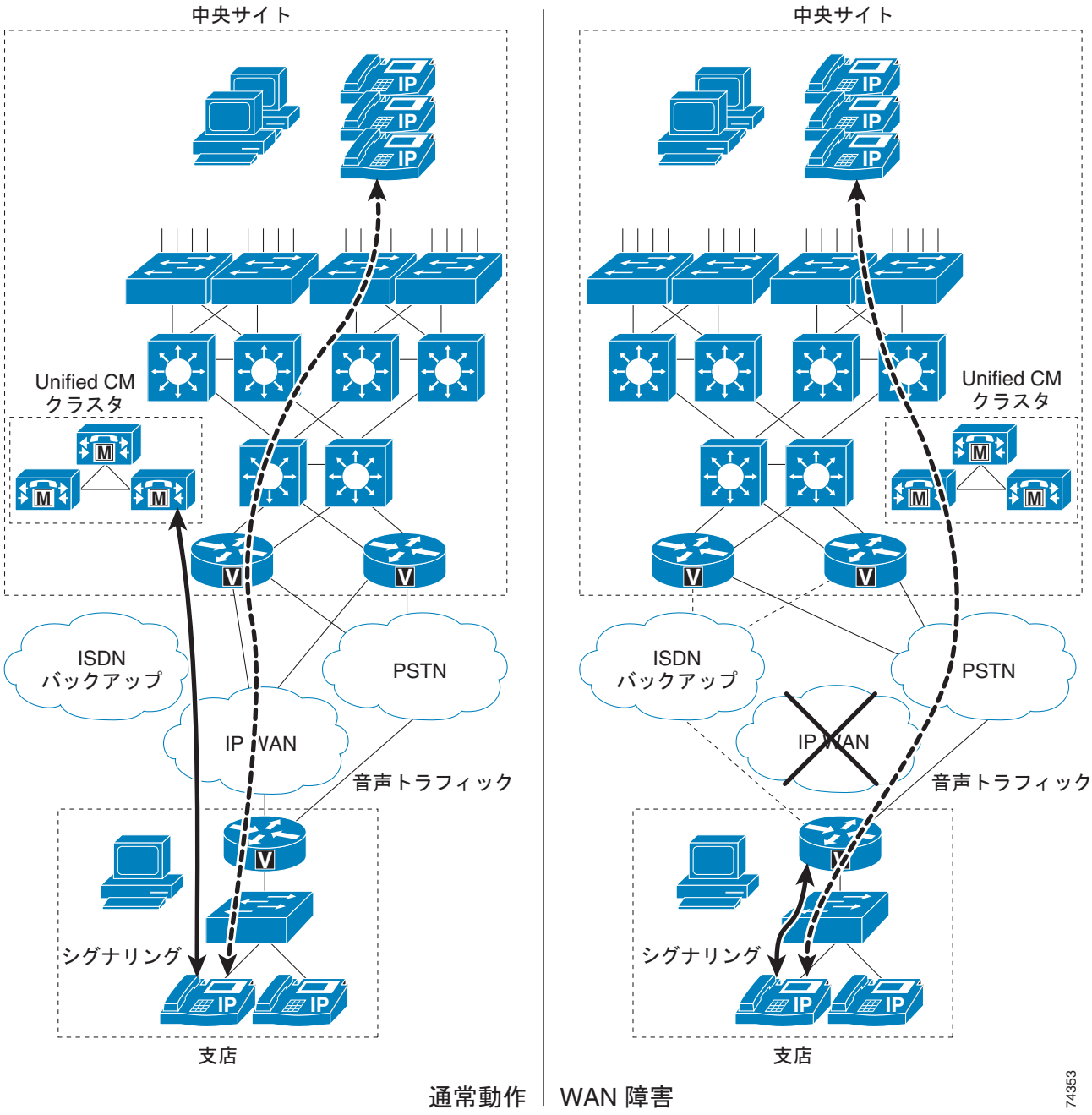



図 5-3 の左側に表示されている通常の動作では、支店は、データ トラフィック、音声トラフィック、およびコール シグナリングを伝送する IP WAN を経由して、中央サイトに接続されます。支店の IP Phone は、中央サイトの Unified CM クラスタとコール シグナリング情報を交換し、IP WAN を介してコールを発信します。支店のルータまたはゲートウェイは、両方のタイプのトラフィック（コール シグナリングと音声）を透過的に転送し、IP Phone を認識しません。

支店との WAN リンクに障害が起きた場合、またはその他の何らかのイベントにより、Unified CM クラスタとの接続が失われた場合、支店の IP Phone は支店のルータに SRST モードで再登録されます。支店のルータ、SRST、または SRST モードで動作する Unified CME は、設定について IP Phone に照会し、この情報を使用して独自の設定を自動的に作成します。支店の IP Phone は、支店のネットワー

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

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

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

### SRST モードの Unified CME

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

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

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

### SRST モードの Unified CME のベスト プラクティス

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

り、電話機が SRST ルータと Unified CM の間で登録と再登録を繰り返すことがなくなります。電話機が長期間にわたって SRST から Unified CM にフォールバックしなくなるため、この値を極端に長い期間に設定しないでください。

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

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

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

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

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

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

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

### SRST ルータのベスト プラクティス

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

- 1 台の SRST ルータで、最大 1,500 台の電話機をサポートする場合。
- 最大 3,000 台の電話機をサポートする場合は、2 台の SRST ルータを使用します。各 SRST ルータ間でコールが相互にルーティングされるように、ダイヤル プランを正しく設定する必要があります。
- 基本的な SRST 機能の、単純な 1 回限りの設定を行う場合。
- Cisco Unified SRST（セキュア SRST）でのみ使用可能な SRTP メディア暗号化を使用する場合。
- Cisco VG248 音声ゲートウェイをサポートする場合。

到達不能または SRST ルータに登録されていない電話機のコールをルーティングする場合は、**alias** コマンドを使用。

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

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

VoPSTN は、次のいずれかの方法で実装できます。

- Automated Alternate Routing（AAR; 自動代替ルーティング）機能を使用する （AAR の詳細については、「Automated Alternate Routing」（P.9-100）の項を参照してください）。
- Unified CM と公衆網ゲートウェイの両方のダイヤル プラン構成要素を組み合せて使用する。

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

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

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

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

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

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

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

- 「AAR を使用する VoPSTN」（P.5-18）
- 「ダイヤル プランを使用する VoPSTN」（P.5-19）

## AAR を使用する VoPSTN

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

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

VoPSTN の AAR 実装方法には、次の利点があります。

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

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

- AAR 機能を正しく設定する必要があります。
- 一般に、サポートされているデバイスには、IP Phone、ゲートウェイ、およびアナログ電話機を収容するゲートウェイがあります。
- 支店間コールが AAR を使用できるのは、宛先デバイスが IP Phone または Cisco Unity ポートの場合のみです。
- 他のエンドポイントに対する支店間コールは、完全修飾 E.164 番号を使用する必要があります。
- すべてのオンネット支店間コールでは、「Network congestion, rerouting」というメッセージが表示されます。
- 宛先の電話機が（WAN 接続の通信断などのため）登録から外れている場合、AAR 機能が呼び出されないため、省略ダイヤリングは Call Forward Unregistered（CFUR）が設定されている場合にだけ使用できます。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、宛先に到達することもできます。
- 発信側の電話機が（WAN 接続の通信断などのため）登録から外れている場合、その電話機は SRST（または SRST として機能する Unified CME）モードに移行します。このような条件の下でも省略ダイヤリングを機能させるには、SRST（または SRST として機能する Unified CME）ルータに、宛先の省略ダイヤル形式を照合して公衆網が宛先へコールをルーティングするのに必要な形式に変換するという変換規則を設定します。
- 同じ支店内のシェアドラインは、その支店のコーリング サーチ スペースのみに含まれているパーティション内に設定される必要があります。シェアドラインへのサイト間アクセスには、次のどちらかの操作が必要です。
  - 発信側サイトでシェアドラインの DID 番号をダイヤルします。
  - シェアドラインへのサイト間省略ダイヤリングが必要な場合は、ユーザがダイヤルした省略ストリングをシェアドラインの DID 番号へと変換するトランスレーション パターンを使用します。

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

## ダイヤル プランを使用する VoPSTN

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

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

VoPSTN のダイヤル プラン実装方法には、次の利点があります。

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

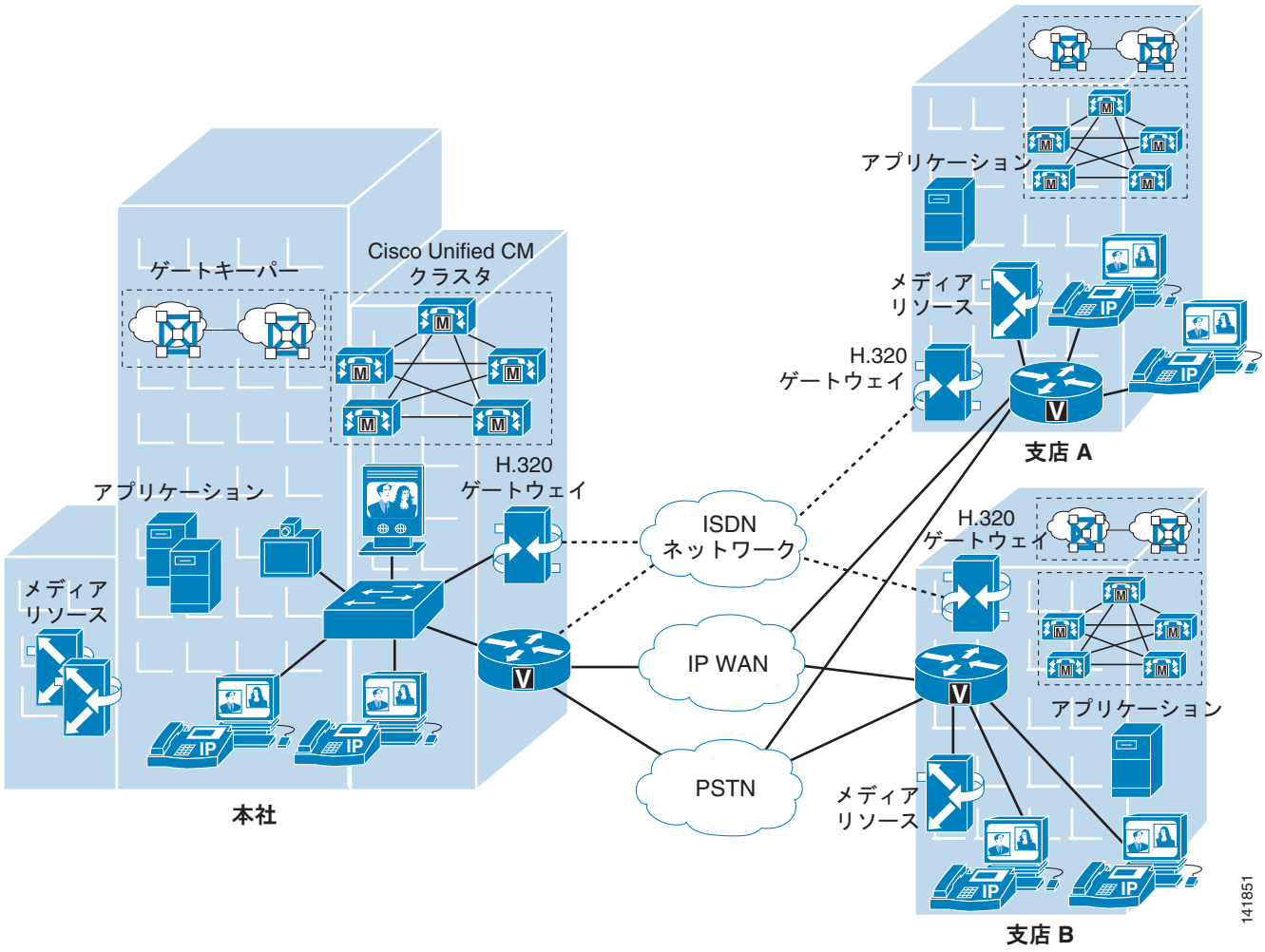
ダイヤル プラン実装方法には、VoPSTN について示した一般的な考慮事項のほかに、次の設計ガイドラインが適用されます。

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

# 分散型コール処理を使用するマルチサイト

分散型コール処理を使用するマルチサイト配置のモデルは、複数の独立したサイトから構成されています。各サイトには独自のコール処理エージェント クラスタがあり、そのエージェント クラスタは、分散されたサイト間の音声トラフィックを伝送する IP WAN に接続されます。図 5-4 は、標準的な分散型コール処理配置を示しています。

**図 5-4　　分散型コール処理を使用するマルチサイト配置**



分散型コール処理モデルの各サイトは、次のいずれかになります。

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

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

- クラスタあたり最大 30,000 の設定済みおよび登録済み Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone または SCCP ビデオ エンドポイント。
- Unified CM クラスタごとに最大 2,100 のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H.323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）。
- すべての外部コールに対して公衆網で対応。
- 会議、トランスコーディング、および Media Termination Point（MTP; メディア ターミネーション ポイント）用のデジタル シグナル プロセッサ（DSP）リソースを各サイトにローカルに分散させて、DSP を必要とするコールが消費する WAN 帯域幅の容量を削減します。
- ボイスメール、ユニファイド メッセージング、および Cisco Unified Presence の各コンポーネント。
- レガシー Private Branch Exchange（PBX; 構内交換機）システムおよびボイスメール システムとの統合機能。
- コールを発信するためにゲートキーパーを必要とする H.323 クライアント、MCU、および H.323/H.320 ゲートウェイを、Cisco IOS ゲートキーパーに登録することが必要です。Unified CM は H.323 トランクを使用してゲートキーパーと統合し、そこに登録された H.323 デバイスのコール ルーティングと帯域幅管理サービスを提供します。複数の Cisco IOS ゲートキーパーを使用して、冗長性を提供することもできます。Cisco IOS ゲートキーパーを使用して、分散した Unified CM クラスタ間でコール ルーティングおよび帯域幅管理を提供することもできます。多くの場合、Unified CM クラスタごとに専用のエンドポイント ゲートキーパーを持ち、それとは別のゲートキーパーを使用してクラスタ間コールを管理することを推奨します。状況によっては、ネットワークのサイズやダイヤル プランの複雑さに応じて、同じゲートキーパーを両方の機能に使用することもできます（詳細については、「ゲートキーパー」（P.12-22）を参照してください）。
- マルチポイント ビデオ会議のクラスタごとに MCU リソースが必要。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。すべてのリソースがリージョン サイトに存在していても、ローカル会議リソースが必要な場合は各クラスタのリモート サイトに分散していてもかまいません。
- 公衆 ISDN 網上で H.320 ビデオ会議デバイスと通信するために H.323/H.320 ビデオ ゲートウェイが必要です。これらのゲートウェイはリージョン サイトにあっても、ローカル ISDN アクセスが必要な場合は各クラスタのリモート サイトに分散していてもかまいません。
- 同じサイト内のデバイス間の広帯域オーディオ（G.711、G.722、Cisco Wideband Audio など）、異なるサイトのデバイス間の狭帯域オーディオ（G.729、G.728 など）。
- 同じサイト内のデバイス間の広帯域ビデオ（384 kbps 以上など）、異なるサイトのデバイス間の狭帯域ビデオ（128 kbps など）。同じサイト内のデバイス間のコールに限っては、7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec を推奨します。ただし、Cisco VT Camera Wideband Video Codec はクラスタ間トランクでサポートされていません。
- 最大 768 kbps 以上の WAN リンク速度。速度が 768 kbps 未満の WAN 接続ではビデオを*推奨しません*。

- コール アドミッション制御は、同じ Unified CM クラスタで制御されるサイト間のコールに対しては Unified CM のロケーションから提供。Unified CM クラスタ間のコールに対しては Cisco IOS ゲートキーパーから提供されます（クラスタ間トランク）。

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 （「キャンパス」（P.5-6）を参照）。

IP WAN の接続オプションは、次のとおりです。

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

# 分散型コール処理モデルのベスト プラクティス

分散型コール処理を使用するマルチサイト配置には、単一サイトと同じ、または集中型コール処理を使用するマルチサイト配置と同じ要件が少なからずあります。分散型コール処理モデルについては、ここでリストされているベスト プラクティスに加えて、他のモデルのベスト プラクティスにも従ってください （「キャンパス」（P.5-6）および「集中型コール処理を使用するマルチサイト」（P.5-8）を参照）。

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

ゲートキーパーの使用には、次のベスト プラクティスが適用できます。

- Cisco IOS ゲートキーパーを使用して、各サイトとのコール アドミッションを制御します。
- ゲートキーパーの有効性を高めるには、HSRP（ホットスタンバイ ルータ プロトコル）ゲートキーパー ペア、ゲートキーパーのクラスタ化、および代替ゲートキーパー サポートを使用します。さらに、ネットワーク内の冗長性を確実にするために複数のゲートキーパーを使用します （「ゲートキーパーの設計上の考慮事項」（P.8-40）を参照）。
- プラットフォームの規模を適切に調整して、パフォーマンスとキャパシティの要件が満たされることを確認します。
- WAN 上のコーデックは 1 つのタイプに限定して使用します。これは、H.323 仕様では、レイヤ 2、IP、UDP（User Data Protocol）、または RTP（Real-time Transport Protocol）ヘッダーのオーバーヘッドが、帯域幅要求で許可されないからです （ヘッダーのオーバーヘッドは、パケットのペイロードまたは符号化された音声部分のみで許可されます）。WAN 上で使用するコーデックを 1 つのタイプに限定すると、最悪のシナリオに備えて IP WAN を過剰にプロビジョニングする必要がなくなるので、キャパシティ プランニングが簡単になります。
- ゲートキーパー ネットワークは、数百単位のサイトにスケーラブルです。また、設計上の制限は WAN トポロジからしか受けません。

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

- ゲートキーパーのコール アドミッション制御については、「コール アドミッション制御」（P.11-1）を参照してください。

- ゲートキーパーのスケーラビリティと冗長性については、「コール処理」（P.8-1）を参照してください。
- ゲートキーパーのダイヤル プラン解決については、「ダイヤル プラン」（P.9-1）を参照してください。

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

SIP プロキシの使用には、次のベスト プラクティスが適用できます。

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

# 分散型コール処理モデルのコール処理エージェント

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

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

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

表 5-4 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 5-4　推奨されるコール処理エージェント**

| コール処理エージェント | 推奨規模 | 備考 |
|---|---|---|
| Cisco Unified Communications Manager Express（Unified CME） | 最大 350 台の電話機 | • 小規模なリモート サイト用<br>• キャパシティは Cisco IOS プラットフォームに依存する |
| Cisco Unified Communications Manager Business Edition（Unified CMBE） | 最大 575 台の電話機 | • 小規模なサイト用<br>• 集中型または分散型コール処理をサポートする |
| Cisco Unified Communications Manager（Unified CM） | 50 ～ 30,000 台の電話機 | • Unified CM クラスタの規模に応じて、小規模から大規模までのサイト<br>• 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 |

同じシステムに複数のコール処理エージェントが存在する場合は、他のエージェントを認識するように各エージェントを手動で設定できます。また、Cisco Service Advertisement Framework（SAF）を使用して、コール エージェント間でコール ルーティングおよびダイヤル プラン情報を自動的に共有することもできます。SAF の詳細については、「Service Advertisement Framework のコール制御ディスカバリを使用したコール ルーティングおよびダイヤル プラン配信」（P.5-57）を参照してください。

# Unified CM Session Management Edition

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

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

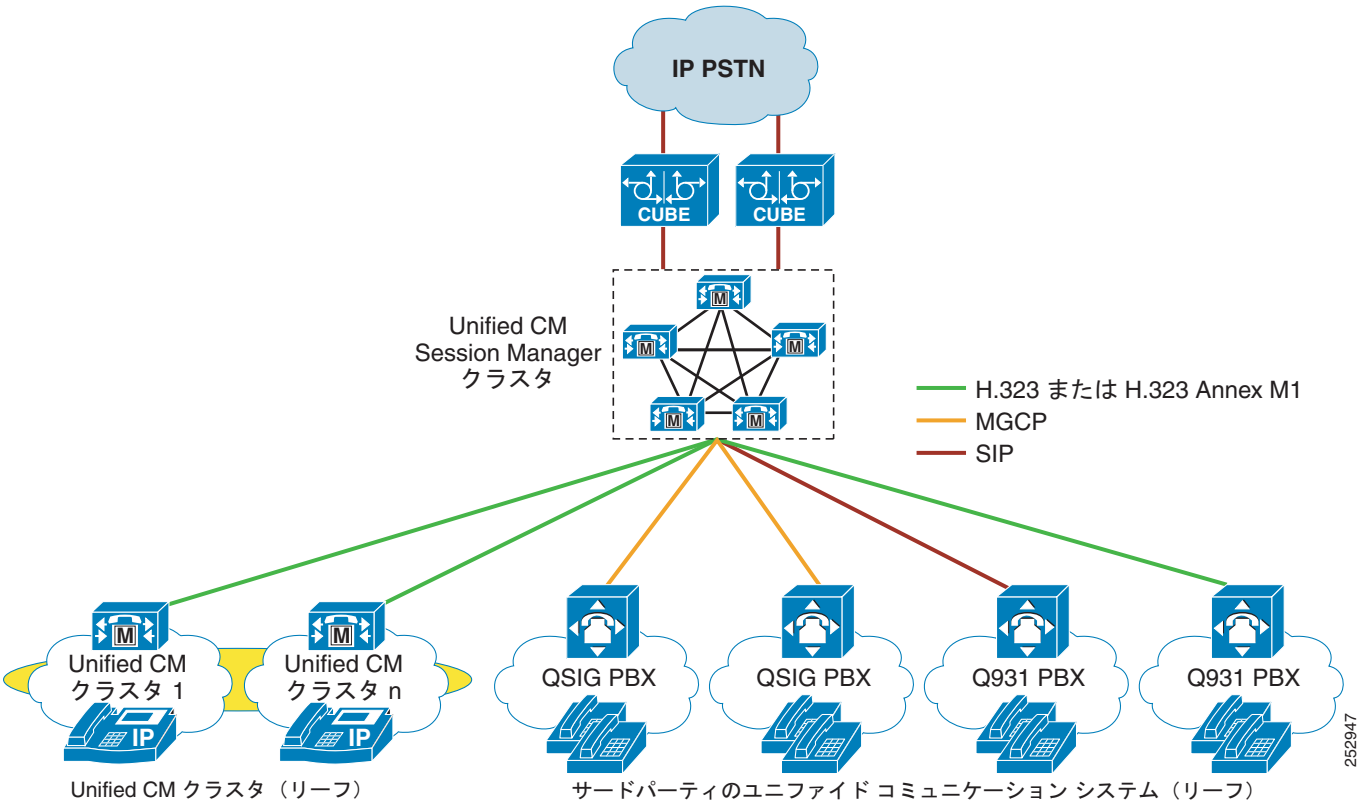
Session Management Edition の配置は、複数の PBX 配置とそれに関連する電話を、IP 電話があり比較的少数のトランクを持つ Unified CM クラスタに移行するために使用できます。Session Management Edition クラスタをサードパーティの PBX を相互接続する多数のトランクで開始し、何千もの IP 電話を持つ Unified CM クラスタ配置に徐々に移行することも可能です。

Cisco Unified CM 8.0 以降のリリースでは、Unified CM Session Management Edition で次の機能がサポートされています。

- H.323 Annex M1 クラスタ間トランク
- SIP クラスタ間トランク
- SIP トランク
- H.323 トランク
- MGCP トランク
- 音声コール
- ビデオ コール
- 暗号化されたコール
- FAX コール

また、Unified CM Session Management Edition を使用して、IP 公衆網接続、PBX、集中型のユニファイド コミュニケーション アプリケーションなど、サードパーティのユニファイド コミュニケーション システムに接続できます （図 5-5 を参照）。ただし、標準の Unified CM クラスタと同様に、サードパーティ デバイスからの Unified CM Session Management Edition への接続は、実稼動環境で使用する前に相互運用性をテストしたシステムである必要があります。

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




## Unified CM Session Management Edition を配置する状況

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

- 集中型ダイヤル プランを作成および管理

  他のすべてのユニファイド コミュニケーション システムに接続するために各ユニファイド コミュニケーション システムに別個のダイヤル プランおよびトランクを設定するのではなく、Unified CM Session Management Edition を使用すると、Session Management クラスタを指す簡潔なダイヤル プランおよびトランクをリーフのユニファイド コミュニケーション システムに設定できます。Unified CM Session Management Edition には、集中型ダイヤル プランと、他のすべてのユニファイド コミュニケーション システムに到達するためのこのプランに対応する情報が含まれています。

- 集中型公衆網アクセスを提供

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

- アプリケーションを集中化

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

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

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

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

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

- キャパシティ

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

- トランク

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

- Unified CM バージョン

  Unified CM Session Management Edition と Unified CM リーフ クラスタの両方とも、Cisco Unified CM 7.1(2) 以降のリリースと一緒に配置する必要があります。それよりも前のバージョンの Unified CM も配置できますが、クラスタを Unified CM 7.1(2) 以降のリリースにアップグレードしないと解決できない問題が発生する可能性があります。

- 相互運用性

  ほとんどのベンダーが標準に準拠していますが、各ベンダーによるプロトコルの実装には相違があります。標準の Unified CM クラスタの場合と同様に、実稼動環境にシステムを配置する前に、サードパーティの未検証のユニファイド コミュニケーション システムとのエンドツーエンドの相互運用性テストを実施することを強くお勧めします。相互運用性テストでは、Unified CM Session Management クラスタを介したシスコおよびサードパーティのリーフ システムからのコール フローと機能を検証します。シスコの相互運用性チームによってテストされたサードパーティのユニファイド コミュニケーション システムの情報を得るには、www.cisco.com/go/interoperability にアクセスして、[Cisco Unified Communications Manager] > [Session Management Edition] のリンクを選択してください。

- 着信コールと発信コールのロード バランシング

  Session Management クラスタ内の Unified CM サーバ間に着信コールと発信コールが均等に分散されるよう、Unified CM Session Management Edition およびリーフのユニファイド コミュニケーション システムのトランクを設定します。トランク コールのロード バランシングの詳細については、「Cisco Unified CM トランク」（P.14-1）の章を参照してください。

- 設計のサポート

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

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

## Session Management Edition を配置する場合の設計上の考慮事項

ここで示す設計上の考慮事項とガイドラインは、Cisco Unified CM Session Management Edition の配置に当てはまるものです。

### Session Management Edition と SAF CCD Deployments

Session Management Edition の配置は、内部ダイヤル プランの集約を提供します。Cisco Service Advertisement Framework（SAF）Call Control Discovery（CCD; コール制御ディスカバリ）の配置は、内部ダイヤル プランと対応する外部「To PSTN」ダイヤル プランの両方を、参加している SAF CCD Unified Communications システムに分散させます。Session Management Edition と SAF CCD を組み合せることにより、Session Management Edition がすべてのリーフ Unified Communications システムに対して中央のセッション マネージャとして機能する中で、SAF CCD を使用して内部ダイヤル プランと外部「To PSTN」ダイヤル プランの両方を SAF CCD に参加しているすべての Unified CM リーフ クラスタに分散させることが可能になります。

Session Management Edition と SAF のハイブリッド配置では、リーフ クラスタ間のすべてのコールが Session Management Edition クラスタを通じてだけルーティングできるようにするために、SAF CCD の特定の設定を使用します。この SAF 設定は、次の 2 つの部分から成ります。

- Session Management Edition からまたはそれを通じた SAF CCD ルートのリーフ クラスタへのアドバタイジング
- SAF CCD ルートのリーフ クラスタから Session Management Edition へのアドバタイジング

（注）　ここの説明では、Unified CM 上ですでに Cisco IOS SAF フォワーダと基本的な SAF CCD 設定（アドバタイズ サービス、要求サービス、SAF 対応トランク など）が設定されていることを前提としています。この設計は、単一の SAF Autonomous System（AS; 自律システム）を使用します。

#### Session Management Edition からまたはそれを通じた SAF CCD ルートのリーフ クラスタへのアドバタイジング

Session Management Edition クラスタ上で、各 SAF 対応リーフ クラスタでホストされる内部の番号範囲および外部「To PSTN」番号のための DN パターン、DN グループ、および対応する「to DID」ルールを作成します。これらの DN パターンを 1 つまたは複数の SAF 対応トランクおよびアドバタイジング サービスに関連付けることにより、SAF AS にパブリッシュします。これらの DN パターンと、Session Management Edition への対応するルートが、すべての SAF 対応リーフ クラスタによって学習されます。Session Management Edition が IP WAN を介して到達可能な間は、すべてのクラスタ間コールが Session Management Edition を通じてルーティングされます。Session Management Edition が到達不能なときは、クラスタ間コールは、学習済みの DN パターンの「to DID」規則を使用して着信番号が修正された後に、リーフ クラスタのローカル PSTN ゲートウェイを通じてルーティングされます。

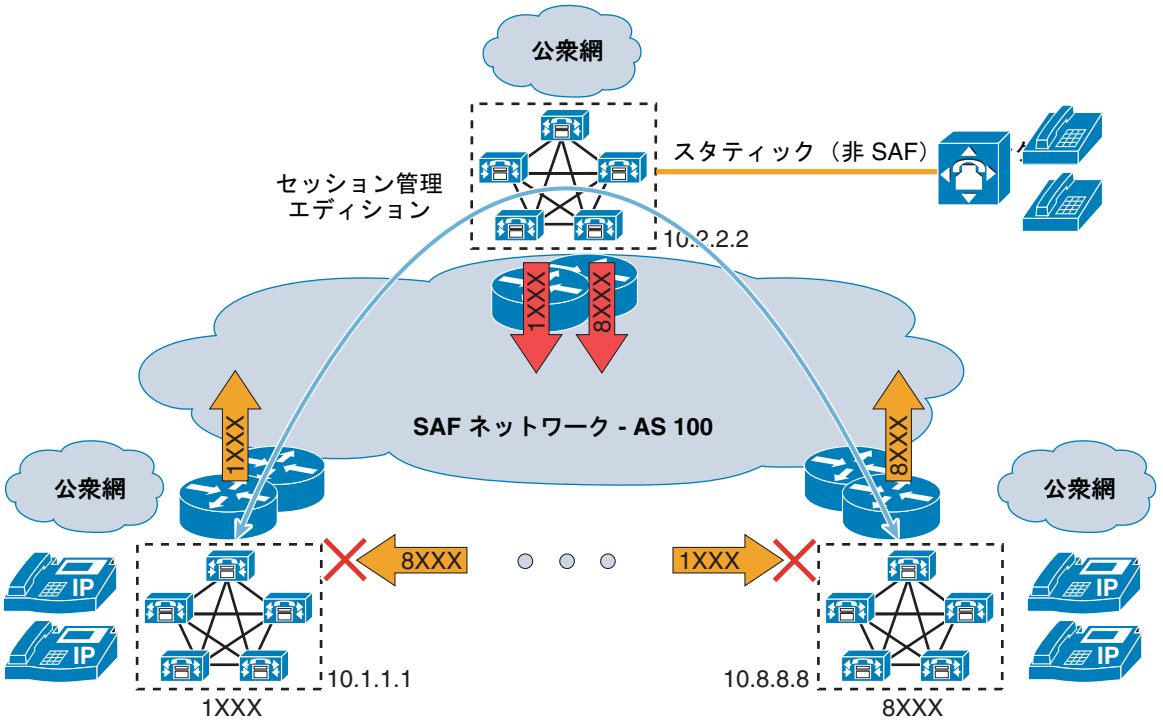
## SAF CCD ルートのリーフ クラスタから Session Management Edition へのアドバタイジング

各リーフ クラスタのホストされている DN 範囲を SAF AS にアドバタイズすることの目的は、Session Management Edition クラスタにこれらの DN 範囲およびリーフ クラスタの到達可能性について学習させることです。これらの番号範囲は、その他のすべてのリーフ クラスタにも学習されます （図 5-6 を参照）。リーフ間の直接ルートが使用されるのを避けるために、各リーフ クラスタ内で、他のすべてのリーフ クラスタから学習されたルートをブロックします。ルートは、それがリーフ クラスタ内の SAF ノードの IP アドレスか、または（可能であれば）各リーフ クラスタの Remote Call Control Entity Name に一致するかどうかに基づいてブロックできます （後者、Unified CM の [Enterprise Parameters] メニューの [Unified CM Cluster ID] です）。

**図 5-6　Session Management Edition の配置での SAF CCD ルートのアドバタイジング**

**セッション管理エディション SAF CCD ルーティング テーブル**

| DN パターン | 「to DID」規則 | IP アドレス | プロトコル |
|---|---|---|---|
| 1XXX | 0:+1212444 | 10.1.1.1 | SIP |
| 8XXX | 0:+1408902 | 10.8.8.8 | SIP |




**リーフ 1 SAF CCD ルーティング テーブル**

| DN パターン | 「to DID」規則 | IP アドレス | プロトコル |
|---|---|---|---|
| 1XXX | 0:+1212444 | 10.2.2.2 | SIP |
| 8XXX | 0:+1408902 | 10.2.2.2 | SIP |
| ~~8XXX~~ | ~~0:+1408902~~ | ~~10.8.8.8~~ | ~~SIP~~ |

**リーフ 8 SAF CCD ルーティング テーブル**

| DN パターン | 「to DID」規則 | IP アドレス | プロトコル |
|---|---|---|---|
| 1XXX | 0:+1212444 | 10.2.2.2 | SIP |
| ~~1XXX~~ | ~~0:+1212444~~ | ~~10.1.1.1~~ | ~~SIP~~ |
| 8XXX | 0:+1408902 | 10.2.2.2 | SIP |

## Session Management Edition と SAF CCD の配置の運用上の考慮事項

ここで示す運用上の考慮事項は、Service Advertisement Framework（SAF）Call Control Discovery（CCD）を備えた Cisco Unified CM Session Management Edition の配置に当てはまるものです。

### リーフ クラスタによる自身の DN 範囲の Session Management Edition からの学習

図 5-6 の SAF CCD ルーティング テーブルからわかるように、リーフ クラスタは、自身の DN 範囲の到達可能性について Session Management Edition から学習します。これらの DN 範囲は、クラスタ間の DN 範囲およびルートをブロックするのと同じ方法でブロックできます。これらの Session Management Edition SAF CCD ルートがブロックされていない場合、発信デバイスのコーリング サーチ スペースが内部 DN のパーティションの上に順序付けられた、SAF CCD で学習されたルート パーティションを持っていれば、これらはクラスタ内コールにだけ選択されます。ほとんどの場合、内部 DN パーティションが SAF CCD パーティションの上に順序付けられるため、内部クラスタ コールは Session Management Edition を通じてはルーティングされません。

### Session Management Edition からのリーフ クラスタへの IP ルートが使用できない場合の公衆網へのルーティング コール

コールを公衆網に再ルーティングする場合に、次の 2 つの設定オプションが使用できます。

- Session Management Edition に関連付けられた公衆網ゲートウェイを通じての公衆網へのコールの再ルーティング

  Session Management Edition クラスタが公衆網アクセスを持っており、Session Management Edition からの IP パスを通じてでは接続先リーフ クラスタに到達しないコールを再ルーティングしたい場合は、各リーフ クラスタが、アドバタイズされる各 DN 範囲またはグループについて、必ず「to DID」規則を Session Management Edition にアドバタイズするようにしてください。この「to DID」規則は、Session Management Edition が着信番号に変更を加え、インバウンド トランクの Automated Alternate Routing（AAR; 自動代替ルーティング）コーリング サーチ スペース（CSS）を通じてコールをルーティングするために使用されます。

- 発信側リーフ クラスタから公衆網へのコールの再ルーティング

  Session Management Edition クラスタが公衆網アクセスを持っておらず、Session Management Edition から接続先リーフ クラスタに到達できないコールを発信側リーフ クラスタでの公衆網を通じて再ルーティングしたい場合は、各リーフ クラスタが、アドバタイズされる各 DN 範囲またはグループの「to DID」規則を決して Session Management Edition にアドバタイズしないようにしてください。この場合、Session Management Edition から接続先リーフ クラスタへのシグナリング パスが確立できないと、Session Management Edition は、コールが失敗したことを発信側リーフ クラスタに通知します。これを受けて、発信側リーフ クラスタはその「to DID」規則（Session Management Edition から学習したもの）を使用して、着信番号を修正し、発信側デバイスの自動代替ルーティング（AAR）コーリング サーチ スペース（CSS）を通じてコールをルーティングします。

### Static Session Management Edition トランクを介した非 SAF ユニファイド コミュニケーション システムへのコール

Session Management Edition は、SAF CCD を使用して、非 SAF ユニファイド コミュニケーション システムの DN 範囲をすべての SAF 対応リーフ クラスタにアドバタイズできます。リーフ クラスタから非 SAF ユニファイド コミュニケーション システムへの Session Management Edition クラスタを介したコールは、Session Management Edition に到達するために SAF トランクを使用します。次に、Session Management Edition は、設定されているルート パターンと対応するスタティック（標準）トランクを使用して、非 SAF ユニファイド コミュニケーション システムに到達します。

### 非 SAF ユニファイド コミュニケーション システムへのコールの公衆網フォールバック

非 SAF ユニファイド コミュニケーション システムが Session Management Edition からのスタティック トランクを通じて到達できない場合の公衆網フォールバックには、次の 2 つのオプションがあります。

- 発信側リーフ クラスタから公衆網へコールを再ルーティングします。

  このオプションでは、Session Management Edition から接続先ユニファイド コミュニケーション システムへの単一のトランクが設定されます。Session Management Edition から接続先のユニファイド コミュニケーション システムへのシグナリング パスが確立できないと、Session Management Edition は、コールが失敗したことを発信側リーフ クラスタに通知します。これを受けて、発信側リーフ クラスタはその「to DID」規則（Session Management Edition から学習したもの）を使用して、着信番号を修正し、発信側デバイスの自動代替ルーティング（AAR）コーリング サーチ スペース（CSS）を通じてコールをルーティングします。

- Session Management Edition から公衆網へコールを再ルーティングします。

  このオプションでは、ルート リストとルート グループの一部として 2 つのトランクが作成されます。最初に選択されるトランクは、Session Management Edition から接続先ユニファイド コミュニケーション システムへと設定し、2 つ目に選択されるトランクは、Session Management Edition からそのローカル公衆網ゲートウェイへと設定します。Session Management Edition から接続先ユニファイド コミュニケーション システムへのシグナリング パスが確立できない場合、Session Management Edition は公衆網への 2 つ目のトランクを選択します。公衆網トランクを含むルート グループを使用して、内部着信番号をその公衆網での相当する番号に変更できます。

# Cisco Intercompany Media Engine

Cisco Unified Communications システム Release 8.0(2) とともに導入された Cisco Intercompany Media Engine（IME）は、分散型コール処理でマルチサイト配置を実現するもう 1 つの方法です。ただし、IME ではサイトは独立した企業組織となります。Unified Communications では、この技術を説明するために*境界なし*という用語が使用されます。高忠実度のコーデック、拡張発信者 ID、企業ネットワーク外部のビデオ テレフォニーなどの Unified Communications 機能を企業間に広げていくことができるためです。ソリューションは、動的かつ安全な方法でルートを学習し、インターネットを介して組織同士が安全に通信できるようにします。他の組織と密接に連携し、高度な企業間通信を備えた組織であれば、IME が提供する拡張通信の恩恵を最大限に享受できます。ここでは、ソリューションのコンポーネントと高度なアーキテクチャについて説明し、あわせて IME を配置するための設計上の考慮事項も示します。

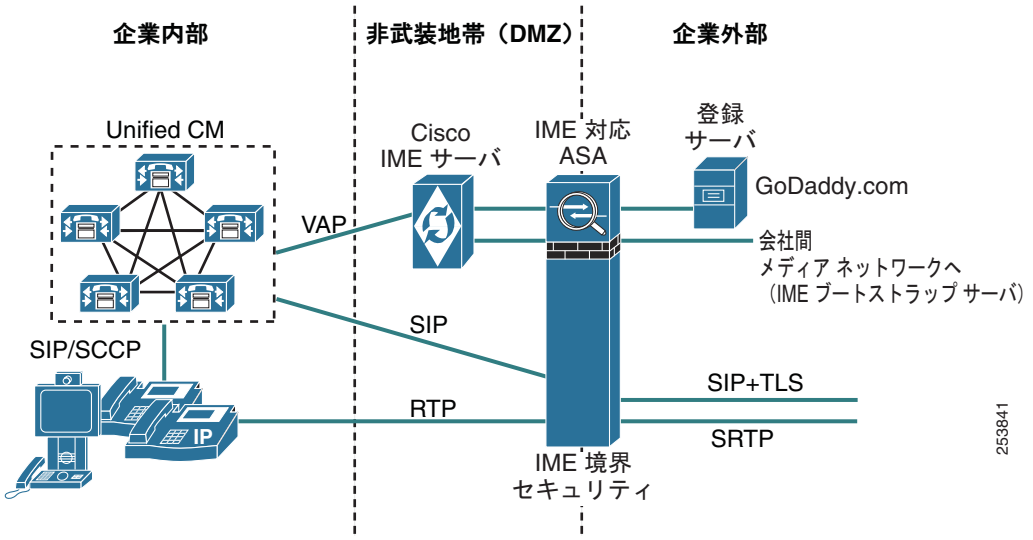
## IME のコンポーネント

IME ソリューションは、IME ルートの動的学習と、組織間でのコール シグナリングおよびメディアの安全な暗号化を実現する複数のコンポーネントで構成されています。このうち 2 つの要素はインターネットにホストされます。GoDaddy.com 登録サーバと Intercompany Media Engine Bootstrap サーバで、GoDaddy.com と Cisco がそれぞれホストします。これ以外に次の必須コンポーネントがオンプレミスで配置されます。

- Cisco Intercompany Media Engine サーバ
- Cisco Unified Communications Manager（Unified CM）
- Cisco Adaptive Security Appliance（ASA）

図 5-7 に、配置したコンポーネントの概要図を示します。

図 5-7　Cisco Intercompany Media Engine コンポーネント




## GoDaddy.com 登録サーバ

GoDaddy.com 登録サーバは、IME サーバを必ず検証してから、インターネットに形成された IME サーバのリングに加えます。適切な GoDaddy.com 証明書とともにインストールして登録した IME サーバだけがそのリングに参加することができます。この登録サーバにアクセスするのは、リングに参加させる前と、または証明書が期限切れになって IME サーバを再登録する必要があるときだけです。

## Intercompany Media Engine ブートストラップ サーバ

IME ブートストラップ サーバはグローバルにアクセスしやすいひとまとまりの IME サーバで、Cisco が所有し、運用しています。（分散型キャッシュ リングとも呼ばれる）リングに参加している各 IME サーバは、IME ブートストラップ サーバにまず接続してネットワークに参加します。登録プロセスで取得したピアツーピア証明書は、ブートストラップ サーバへの初めての接続を含め、すべてのピアツーピア TLS 接続に使用されます。

## Intercompany Media Engine サーバ

各組織が、それぞれのネットワークで 1 つ以上の IME サーバを所有および運用します。IME サーバは、組織が所有するディレクトリ番号を分散型キャッシュ リングに公開し、コール レコードを検証し、リモートの企業へのルートを学習して、IME 学習ルートを Unified CM にプッシュします。このような役割は、ソリューションの IME 学習サイクルにだけかかわるもので、リアルタイム シグナリング通信およびメディア通信では機能しません。

## Unified Communications Manager および Session Management Edition

組織が IME に参加するには、Cisco Unified CM 8.*x* または Unified CM Session Management Edition 8.*x* が必要です。Unified CM は、IME サーバと通信して IME 指定のディレクトリ番号を分散型キャッシュ リングにアップロードし、そのディレクトリ番号から発信された公衆網コールのコール レコードを IME に送信します。また、Unified CM は IME サーバが検証した IME 学習ルートを受信し、その IME 学習ルートでリモートのディレクトリ番号への動的 SIP トランク コールを開始します。SIP トランク シグナリングは、常に IME 対応の Adaptive Security Appliance（ASA）を経由します。

## Adaptive Security Appliance

IME コールは常に IME 対応の Adaptive Security Appliance（ASA）を経由する必要があります。これで、境界のセキュリティが確保されます。IME 対応の ASA は、SIP シグナリング通信（Unified CM からの発信またはリモートの企業からの着信）を受信し、IME チケットを検証し、アドレス変換を実行して、インターネット経由での安全なシグナリングのために SIP と SIP+TLS との変換を提供します。組織間のオーディオおよびビデオ メディアも、IME 対応の ASA を経由します。その際、RTP-to-Secure RTP（sRTP）変換と、インターネットから着信したオーディオ ストリームの音声品質モニタリングが行われます。配置オプションには、オフ パスと基本（インライン）があります。このような配置オプションの詳細については、「ASA Intercompany Media Engine プロキシ」（P.4-30）を参照してください。

# IME のアーキテクチャ

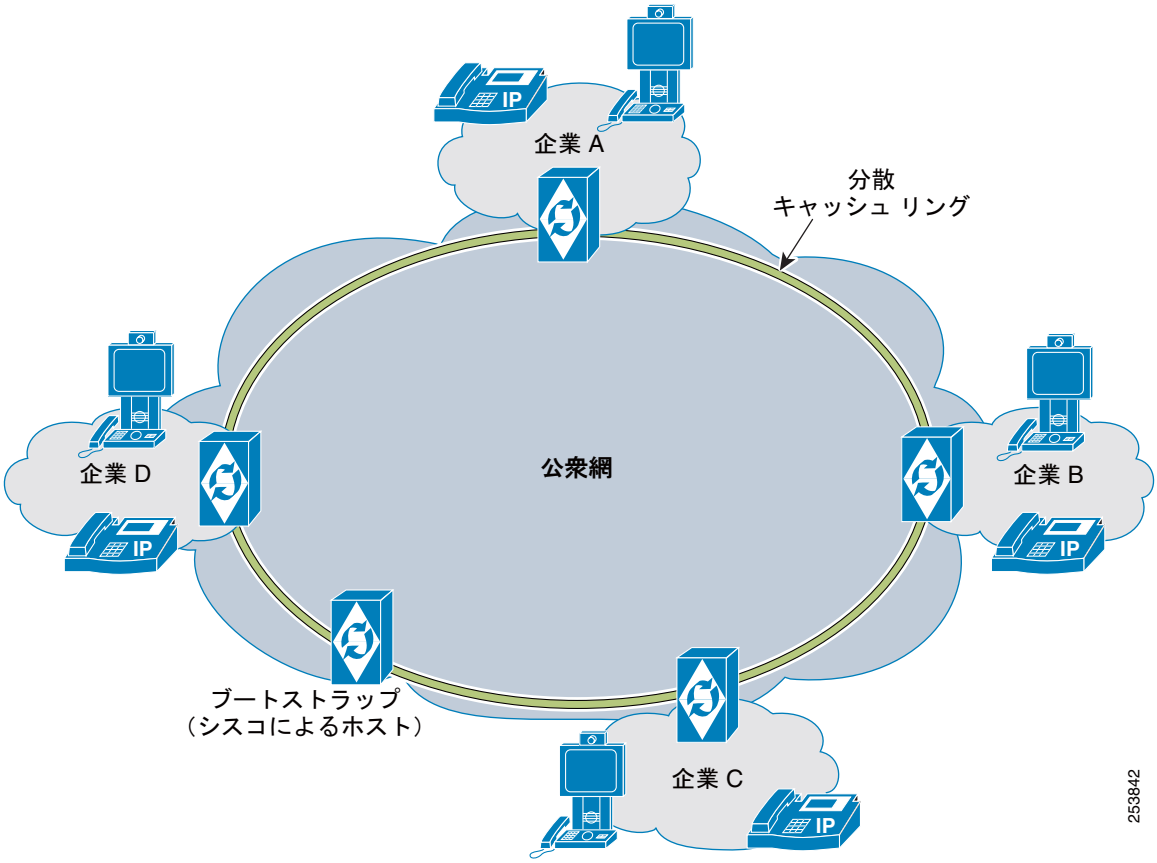
IME のアーキテクチャは、IME の運用方法に反映されます。IME の動作は、次の上位段階にかかわってきます。

- 「IME 学習ルート」（P.5-32）
- 「IME コール処理」（P.5-35）

## IME 学習ルート

GoDaddy.com 登録サーバに登録し、IME ブートストラップ サーバによる検証が完了すると、IME サーバがピアツーピア リングでアクティブなサーバになります。IME に参加しているすべての組織の IME サーバが、インターネット上のリングに加わり、Resource Location And Discovery（RELOAD）プロトコルに基づく安全なピアツーピア技術を使用して通信します。IME サーバは、IME 固有の情報を 1 つ格納する分散ハッシュ テーブルを作成します。公開済みのすべての +E.164 ディレクトリ番号と、その番号を所有する IME サーバ ピア ID を収めた一方向ハッシュです。この情報はすべての IME サーバに分散され、ピアツーピア技術のアーキテクチャは IME サーバがリングの機能を低下させることなくリングへの参加または脱退を動的に行えるようになっています。IME サーバをリング上に確立し、企業が IME に登録したディレクトリ番号を公開することが、IME ルートの学習に向けた最初の手順となります。図 5-8 に、Distributed Cache Ring（DCR; 分散キャッシュ リング）の論理構成図を示します。

図 5-8　Intercompany Media Engine 分散キャッシュ リング

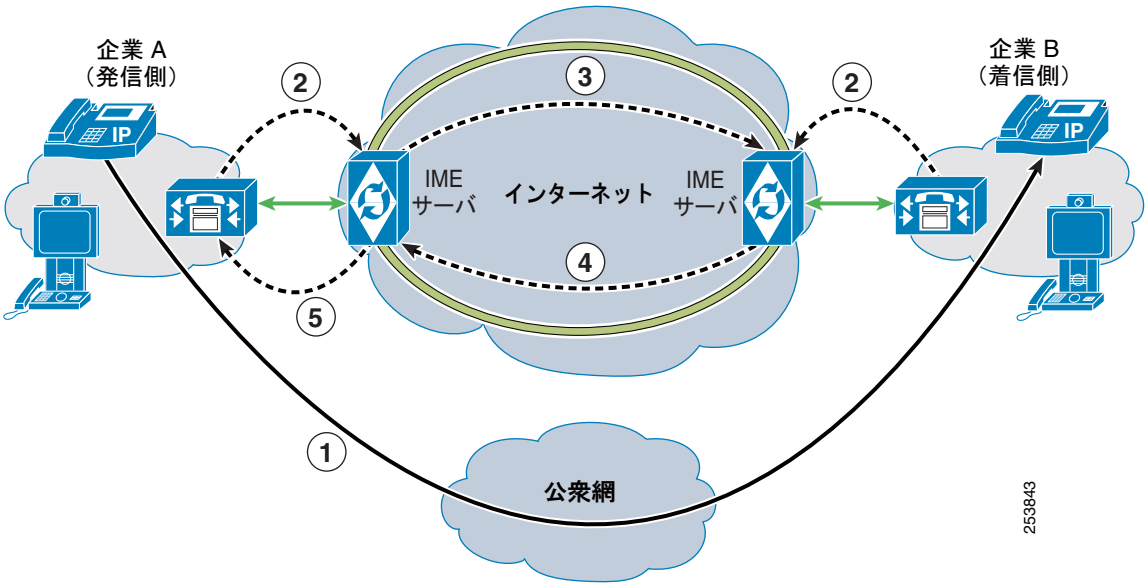



（注）　IME サーバ ピアツーピア プロトコルの標準化を目指して、IETF 機関にドラフトが提出されています。詳細は、http://www.ietf.org/id/draft-rosenberg-dispatch-vipr-reload-usage-01.txt から入手できます。

（注）　IME では、国際番号に付く + プレフィックス（+14085551212 など）を含め、Intercompany Media Network に関連付けられたすべてのディレクトリ番号を E.164 形式にする必要があります。このドキュメントでは、これを +E.164 形式と呼びます。

図 5-9 に、IME 学習ルート プロセスを示します。

図 5-9　Intercompany Media Engine 学習ルート プロセス




組織に IME ソリューションを配置した後、選択したディレクトリ番号を登録して IME で管理できます。このように登録した +E.164 番号は、分散型キャッシュ リングに公開されます。IME ディレクトリ番号からの最初のコールは、事前に定めたとおりに公衆網を使用します（図 5-9 のステップ 1）。コール元が IME ディレクトリ番号であるため、コールが完了すると、そのコールに関する情報が Voice Call Record（VCR; 音声コール レコード）という IME に固有の CDR のようなレコードで作成され、Validation Access Protocol（VAP）によって IME サーバにアップロードされます（図 5-9 のステップ 2）。

音声コール レコードには、+E.164 形式の発着信番号やコールの開始時間と終了時間などの情報が含まれています。（リアルタイムではなく）その後のある時点で、コールの発信側の企業の IME サーバはこの +E.164 着信番号を所有する企業を見つけるために、DCR 上のピアに問い合せます（図 5-9 のステップ 3）。この着信番号のオーナーが検出されると（このディレクトリ番号は別の企業によって IME にすでに登録されているものとします）、検証プロセスが始まります。IME サーバ間のすべての通信が 128 ビット AES TLS で行われます。着信側 IME サーバは、発信側 IME サーバの VCR に記載された着信側 / 発信側番号および開始 / 終了時間が着信側の対応する VCR のものと一致することを確認します。一致を確認すると、着信側 IME サーバが、正常完了の返信を発信側 IME サーバに送信します（図 5-9 のステップ 4）。返信には、「チケット」（着信側の ASA だけが「IME コール処理」（P.5-35）の要領で解読できるセキュリティ ハッシュ）と、この +E.164 番号に対応する IME SIP トランク コールの送信先の外部 IP アドレスが含まれています。これが、IME 学習ルートとなります。発信側 IME サーバはこの学習ルートを受信し、その後のある時点で VAP を使用して Unified CM に公開します（図 5-9 のステップ 5）。Unified CM は、この IME 学習ルートを受信すると、そのルートを Unified CM データベースに挿入します。この時点で、発信側の企業にある IME 対応のディレクトリ番号が IME 学習ルート リストにある番号にコールを発信すると、そのコールは IME コールになります。IME ルートの学習にはリアルタイムの通信は関与しないことに留意してください。学習ルートの詳細な例については、次の URL で入手可能な『*Cisco Intercompany Media Engine Installation and Configuration Guide*』を参照してください。

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

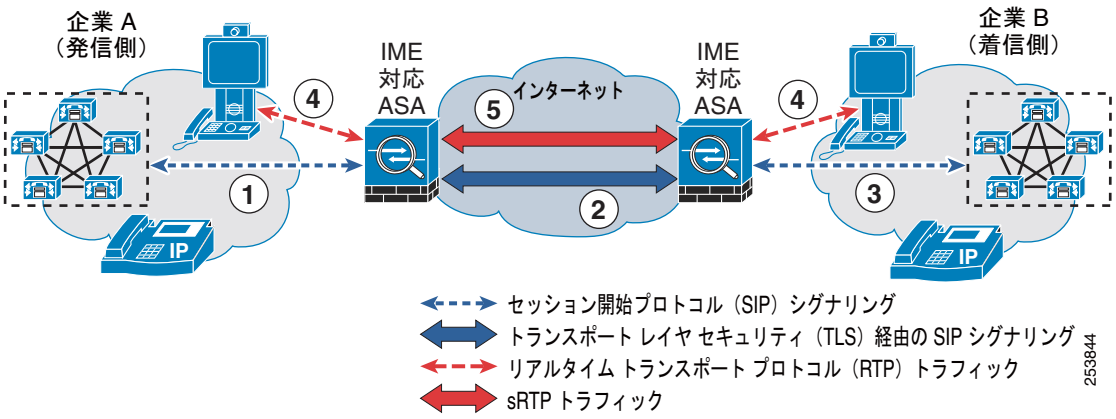
（注）　Unified CM には、定義済みのプレフィックスまたはドメインについては IME 学習ルートを Unified CM データベースに挿入しないようにする機能があります。

（注）　Unified CM には、グローバル化されたダイヤル プランが実装されていない場合でも、発着信の番号を IME VCR に固有のグローバル化された +E.164 形式に変換する方法が用意されています。VCR のための +E.164 変換の詳細については、「Intercompany Media Engine のダイヤル プランに関する考慮事項」（P.9-33）を参照してください。

## IME コール処理

IME 学習ルートが Unified CM データベースに存在していると、IME コールをセットアップするときにルートの情報が使用されます。ただし、IME サーバ自体はコール処理段階に関与しません。図 5-10 に、IME コール処理の概要図を示します。

**図 5-10　Intercompany Media Engine のコール処理**




（注）　IME では、IME 対応の ASA と Unified CM との間で TLS 経由で安全な SIP シグナリングも使用できます。

IME コールを開始するには、着信番号がデータベース内の IME 学習ルート パターンに一致し、発信側のエンドポイントのディレクトリ番号が IME に登録されている必要があります。これらの基準が満たされた場合、Unified CM は IME 学習ルートに含まれていた着信側の企業の外部 IP アドレスまたは Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）宛ての IME SIP トランクを動的に呼び出します。IME 学習ルート パターンは +E.164 形式です。ただし、グローバル化された Unified CM ダイヤル プランが配置されていない場合でも、IME 固有の VCR 用に着信番号を +E.164 形式に変換する場合と同じプロセスを使用して、IME 固有の分析用にゲートウェイで着信番号が分析されて +E.164 形式に変換されます。E.164 変換プロファイルの詳細については、「Intercompany Media Engine のダイヤル プランに関する考慮事項」（P.9-33）を参照してください。

IME 対応の ASA は、リモートの組織との間で行われるすべての IME 通信のプロキシとして機能します。ASA は、Network Address Translation（NAT; ネットワーク アドレス変換）および SIP Application Layer Gateway（ALG; アプリケーション レイヤ ゲートウェイ）機能を備えており、SIP メッセージング自体の内部でアドレッシングを変換できます。IME 対応の ASA 向けの配置オプションが 2 つあります。基本（インライン）とオフパスです。オフパスが推奨のオプションで、Unified CM が IME トラフィックを DMZ 内の IME 対応の ASA に送信できるようになります。このオプションでは、ネットワークにすでに配置されている既存の ASA を使用して、インターネットへ向かうすべての Unified CM トラフィックがこの ASA を経由するように構成できます。基本とオフパスによる ASA 配置の詳細については、「ASA Intercompany Media Engine プロキシ」（P.4-30）を参照してください。

発信側の Unified CM が、IME 対応の ASA に到達する SIP INVITE を開始します（図 5-10 のステップ 1）。この SIP INVITE の SIP ヘッダーには、学習ルートから取得したセキュリティ ハッシュ チケットが属性として含まれています。ASA は、SIP レベルでパケットを整えます。INVITE の送信元として外向きの IP アドレスが表示され、安全な（256 ビット AES）TLS 接続上でリモートの企業の外部 IP アドレスへ送信されます（図 5-10 のステップ 2）。IME 学習ルートに記載されている外部 IP アドレスは、Unified CM クラスタに代わって着信 SIP シグナリングを受信する IME 対応 ASA の外部アドレスと関連付けられています。着信側の ASA は、SIP INVITE を受信して解読し、チケットを検証します。有効なチケットがない要求はブロックされます。チケットの検証が完了すると、ASA は NAT 機能および ALG 機能を実行してから、チケットを着信側の Unified CM に転送します（図 5-10 のステップ 3）。

（注）　IME サーバおよび IME 対応 ASA は直接には通信しませんが、どちらも同じ**エポック チケットパスワード**で設定されており、チケットの検証を正常に完了できます。

SIP シグナリングのネゴシエートが正常に完了すると、各 IME 対応 ASA はそれぞれの Unified CM に指示し、エンドポイントが RTP メディアを内部メディア ターミネーション アドレスに直接ストリーミングするようにします（図 5-10 のステップ 4）。ASA は、この RTP ストリームを取得して暗号化し、NAT を実行して、オーディオ メディアやビデオ メディアなどの外部メディア ターミネーション アドレスから発生した sRTP としてストリームをリモート ASA に送信します（図 5-10 のステップ 5）。この時点で、2 つのエンドポイントにアクティブな IME コールができあがります。

IME ソリューションには、オーディオ ストリームの音声品質が許容レベルを下回った場合に、コールを公衆網にフォールバックするためのメカニズムもあります。ビデオなどの高度な機能は失われますが、コールの音声部分は元の状態のままであるため、ユーザには変更が明示されません。

IME フォールバック機能および IME 対応 ASA の設定の詳細については、次の URL で入手可能な『*Cisco ASA 5500 Series Configuration Guide using the CLI, 8.3*』にある、Cisco Intercompany Media Engine プロキシの設定に関する説明を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/config.html

# キャパシティ プランニング

IME サーバの規模は、サーバに公開する登録済み DID の数に従って調整します。表 5-5 に、プラットフォームごとの現在サポートされているキャパシティ制限を示します。

**表 5-5　IME サーバでサポートしているキャパシティ**

| プラットフォーム | 登録 DID の最大数 |
|---|---|
| Cisco MCS 7825-H2/I2 と 7825-H4/I4 | 20,000 |
| Cisco MCS 7845-H2/I2 と 7845-I3 | 40,000 |

すべての IME コール メディア（オーディオおよびビデオ）が IME 対応の ASA を経由するため、キャパシティは ASA を経由するコールのタイプおよび数によって異なります。IME 対応の ASA は、音声品質確保のためインターネットから着信したオーディオ ストリームだけを監視します。ビデオ メディアは音声品質確保の目的で監視されることはありませんが、RTP と sRTP 間の変換のため IME 対応の ASA を経由します。そのため、ビデオの帯域幅は処理できるセッションの数に直接影響を与えます。表 5-6 に、ASA-5550 および ASA-5580 のキャパシティ制限を示します。その他の ASA モジュールのパフォーマンス制限は、まだ検証されていません。

表 5-6　タイプおよび ASA モデルごとのコールの最大数

| ASA モデル | Voice G.711 | Video 300 kbps | Video 800 kbps | Video 1 Mbps |
|---|---|---|---|---|
| ASA-5550 4 GB | 480 コール | 240 コール | 120 コール | 80 コール |
| ASA-5580-20 4 GB | 900 コール | 600 コール | 300 コール | 200 コール |

Unified CM では、処理できる IME コールの数に制限はありませんが、クラスタが提供するコール キャパシティに対する IME コールの影響を考慮する必要があります。シスコ代理店またはシスコのシステム エンジニアが、Cisco Unified Communications Sizing Tool（http://tools.cisco.com/cucst）を使用して、大量のコール トラフィックを処理する設計をすべて検証する必要があります。サイジング ツールでは、設計基準を満たすために必要なサーバまたはクラスタの正確な台数を決定できます。

# ハイ アベイラビリティ

IME ルート学習段階には、高可用性の側面がいくつか含まれています。Distributed Cache Ring（DCR; 分散型キャッシュ リング）自体にはピアツーピア技術による高度な冗長性があり、IME サーバがリングに加入したりリングから脱退したりすると、DCR ピアに保存される情報が調整されます。また、有効な IME サーバがいつでもリングに参加できるようにするために、Cisco では複数の IME ブートストラップ サーバをホストしています。これらの側面は、このソリューションが本質的に備えているものです。

Unified CM では、（一連の登録済み DID、除外済み DID、および IME サーバなどのパラメータを定義する）各 IME サービスはプライマリ IME サーバとセカンダリ IME サーバからなります。どちらのサーバも稼動しており、Unified CM は登録済み DID および着信側コール VCR を両サーバにアップロードします。ただし、発信側コール VCR はプライマリ IME サーバにだけアップロードされます。このため、プライマリだけが検証要求を開始しますが、どちらのサーバも着信側コール VCR があるため他の企業から受信した検証要求を処理できます。VCR に関してプライマリとセカンダリの IME サーバとが直接通信することはないため、停電になると、検証のためにプライマリに格納した発信側コール VCR が失われます。推奨するオプションは、登録済み DID を 2 つの範囲に分割し、2 つの IME サービスを作成して、サービス A のプライマリ IME サーバがサービス B のセカンダリ IME サーバになったり、あるいはその逆になったりできるようにすることです。これにより、発信側コール検証負荷が IME サーバ全体にバランスよく配分されるほか、停電時に失われる発信側 VCR の数を最小限に抑えることができます。

Unified CM 側では、IME サービスを設定した後に、IME サービスに関連付けられた IME SIP トランクのデバイス プールによって、プライマリ IME サーバとの VAP 通信を開始する Unified CM が決まります。デバイス プールに関連付けられた Unified CM Group 属性によって、サービスを担当する 1 次、2 次、および 3 次の Unified CM が決まります。1 次 Unified CM がダウンした場合には、2 次 Unified CM がアクティブな IME サーバとの VAP 通信を引き継ぎます。

コール処理については、IME サービスの IME SIP トランクに関連付けられた Unified CM Group によって、どの Unified CM サブスクライバが IME コールを開始するかが決まります。このため、IME SIP トランクの 1 次 Unified CM がオフラインであっても、IME コールは続行します。コールを受信する場合、各 IME サービスはクラスタ内の Unified CM コール処理サブスクライバに対して外部 IP アドレスとポートのペアを設定できます。各外部 IP アドレスとポートのペアは、実際には IME 対応の ASA 上に設定された IP アドレスとポートであり、Unified CM コール処理ノードと 1:1 で対応しています。IME ルートに複数の外部 IP アドレスおよびポートがあるときは、Unified CM はこの IME ルートへのコールを順繰りに送信して、コールの負荷がリモートの企業の Unified CM サーバにバランスよく配分されるようにします。リモートの Unified CM がオフラインの場合、発信側 Unified CM はリストの次に掲載されている外部 IP アドレスおよびポートを試します。応答がなく、このリストの末尾に達した場合、コールは IME がない場合と同じように公衆網に送信されます。

2 台の IME 対応の ASA をアクティブ スタンバイ モードで配置できます。ただし、ステートフル フェールオーバーは提供されません。フェールオーバーの場合には、アクティブ コールは切断されますが、後続の IME コールはスタンバイ（今はアクティブな）ASA によって接続されます。オフパス IME 対応 ASA を使用した配置の場合、Unified CM での IME サービス設定によって、1 つの IME ファイアウォールを関連付けることができます。異なる登録済み DID 範囲ごとにいくつか IME 対応の ASA を配置して、IME コールを処理できます。このため、キャパシティの増大に加え、IME コールの負荷をバランスよく配分するメカニズムを実現できます。

（注）　IME 対応の ASA では、アクティブ/アクティブ フェールオーバー モードはサポートされません。

IME コールが接続されている間、IME 対応の ASA はコールの品質を監視できます。品質が特定の感度レベルを下回ると、コールは公衆網に戻されます。詳細については、「ASA Intercompany Media Engine プロキシ」（P.4-30）を参照してください。

# 設計上の考慮事項

IME ソリューションでは、IME サーバと IME 対応の ASA にパブリックに到達可能な IP アドレスが付与されている必要があります。このため、どちらも組織の DMZ に配置する例が最も多く見られます。そのために、組織内でセキュリティを担当するグループと Unified Communications を担当するグループとが緊密に連携することが必要になる場合があります。セキュリティと Unified Communications の両チームが IME プロジェクトの早期設計段階からかかわることが重要です。また、自社の IME ソリューションを設計するときは、次のガイドラインおよび考慮事項に従ってください。

- すべての Unified CM サーバ、IME サーバ、および IME 対応の ASA にネットワーク タイム プロトコルを使用する必要があります。いずれも、信頼できる上位層のクロック ソースに同期する必要があります。IME ルート学習段階では、そのようなクロック ソースが音声コール レコードの開始時間と終了時間に不可欠です。
- ホスト型 IME ソリューション配置モデルもサポートされます。ホスト型 IME 配置では、IME サーバが複数の Unified CM または Unified CM Session Management Edition クラスタに代わって、登録済みディレクトリ番号を公開し、VCR を検証します。詳細については、http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html で入手可能な『*Cisco Intercompany Media Engine Installation and Configuration Guide*』で、ホスト型 IME ソリューションに関する説明を参照してください。

### IME サーバ

- デフォルトでは、Unified CM と IME サーバとの VAP 通信では認証だけが行われます。DMZ に IME サーバを配置する場合は、VAP 通信を認証および暗号化の対象として設定することをお勧めします。このように設定すると、通信が強制的に TLS 経由で行われます。そのためには、セキュリティ証明書を共有するための追加の設定が必要です。

### Unified CM および Unified CM Session Management Edition

- Intercompany Media Network では、公開するすべての番号を +E.164 形式にして、グローバルな一意性を確保する必要があります。発信側と着信側の番号は、IME 固有の Voice Call Record（VCR; 音声コール レコード）が IME サーバにアップロードされたときに正しい形式になるように、+E.164 形式に変換する必要があります。Unified CM には、IME だけのために発信側と着信側の番号を +E.164 形式に変換する機能が用意されています。これは通常のダイヤル プラン番号分析には影響を与えません。詳細については、http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html で入手可能な『*Cisco Intercompany Media Engine Installation and Configuration Guide*』で、E.164 変換プロファイルに関する説明を参照してください。

- 公衆網接続に使用されるゲートウェイまたはトランクでは、[PSTN Access] チェックボックスをオンにして、IME 参加のために発信側と着信側の番号を分析する必要があります。Unified CM 8.*x* へのアップグレード時に、このパラメータはすべてのゲートウェイおよびトランクでデフォルトで有効になります。このチェックボックスが必要ない場合にはオフにできます。
- 内部エンドポイントと IME SIP トランク間のリージョンで Unified CM をどのように設定するかによって、IME コールに許可されるオーディオとビデオの機能が決まります。
- IME 対応の ASA でキャパシティを制限するために、Unified CM ロケーション ベースのコール アドミッション制御を IME SIP トランクに適用して、ASA 経由で送信されるオーディオ コールおよびビデオ コールの数を制御することをお勧めします。帯域幅の制限に達すると、後続のコールは IME を配置する前と同じように公衆網でルーティングされます。
- IME で通信しようとしているリモートの企業のドメインを明示的に信頼することをお勧めします。信頼グループを設定すると、VCR を検証しようとする他のすべてのドメインはデフォルトで拒否となります。
- ユーザが開始した保留および転送シナリオでは、ユニキャスト Music On Hold（MoH; 保留音）がサポートされます。ファイアウォールを正しく機能させるには、MoH full-duplex streaming サービス パラメータを有効にする必要があります。
- IME サーバの登録済み DID グループからアナログおよび FAX ステーションのディレクトリ番号を除外することをお勧めします。そのようなディレクトリ番号は拡張 Unified Communications のメリットを受けず、IME では FAX コールがサポートされていないためです。

### IME 対応の ASA

- 基本およびオフパスの ASA 配置の詳細と、ネットワーク内にある他のファイアウォールのセキュリティを確保するための考慮事項については、「ASA Intercompany Media Engine プロキシ」（P.4-30）を参照してください。
- （384 kbps 以上の）高帯域幅ビデオがサポートされます。ただし、IME 対応の ASA を経由するコールのキャパシティに直接影響を与えます。
- フォールバック感度レベルは、初期 IME 配置のデフォルト設定のままにしてください。フォールバックは使用し始めてから数か月間監視し、その結果に応じて調整します。コール詳細レコードを表示して、IME またはフォールバックのために生成されたコールを探すことをお勧めします。適切なフォールバック感度レベルは、企業によって異なります。
- IME 登録済み DID があるエンドポイントをリモートに配置して企業へ VPN 接続している場合、そのようなエンドポイントではコールの遅延およびジッタ特性が増幅され、その結果 IME 対応の ASA が公衆網にトリガーするフォールバックの頻度が高くなることがあります。特定のエンドポイントにおいてフォールバックが頻繁に発生する場合、このようなデバイスにデバイス プールを設定してそのフォールバック プロファイルでフォールバックを無効にするか、フォールバック感度レベルを下げるか、または IME から登録済み DID を削除することが必要になる場合があります。

# IP WAN を介したクラスタ化

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

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

- 「ローカル フェールオーバー配置モデル」（P.5-44）

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

- 「リモート フェールオーバー配置モデル」（P.5-50）

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

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

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

WAN を介したクラスタ化の主な利点として、次のようなものが挙げられます。

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

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

# WAN の考慮事項

WAN を介したクラスタ化が成功するには、WAN 自体のさまざまな特性を慎重に計画し、設計し、実装する必要があります。Unified CM サーバ間の Intra-Cluster Communication Signaling（ICCS）は、複数のトラフィック タイプから構成されます。ICCS のトラフィック タイプは、優先またはベストエフォートのどちらかとして分類されます。優先 ICCS トラフィックには、IP Precedence 3（DSCP 24 または PHB CS3）が付けられます。ベストエフォート型 ICCS トラフィックには、IP Precedence 0（DSCP 0 または PHB BE）が付けられます。さまざまなタイプの ICCS トラフィックについては、「クラスタ内通信」（P.5-41）で説明されています。この項では、プロビジョニングについてのさらに詳しいガイドラインも記述されています。WAN の特性には、次の設計上のガイドラインが適用されます。

- 遅延

  任意の 2 台の Unified CM サーバ間の片方向の最大遅延は 40 msec、つまり 80 msec Round-Trip Time（RTT; ラウンドトリップ時間）以下でなければなりません。遅延の測定については、「遅延のテスト」（P.5-43）を参照してください。2 つのサイト間の伝搬遅延は、他のネットワーク遅延を考慮しない場合、1 キロメートルあたり 6 マイクロ秒になります。これは、20 ms 遅延に対して理論的な最大距離約 3000 km、つまり約 1860 マイルに相当します。この距離は、相対的なガイドラインとしてのみ記載されています。実際には、ネットワーク内の他の遅延により、これより短くなります。

- ジッタ

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

- パケット損失とエラー

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

- 帯域幅

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

- QoS

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

# クラスタ内通信

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

サーバ間のクラスタ内トラフィックは、次のものから構成されます。

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

（TCP）接続を使用します。この接続は、これらのサーバ間でフルメッシュです。クラスタには、Cisco CallManager Service が使用可能になっているサーバが 8 つしかないので、各サーバには最大 7 つの接続が可能です。このトラフィックは、優先 ICCS トラフィックであり、Cisco CallManager リリースおよびサービス パラメータ設定に応じてマークされます。

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

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

## Unified CM パブリッシャ

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

- Call Forward All（CFA; 全コール転送）
- Message Waiting Indication（MWI; メッセージ待機インジケータ）
- プライバシーの有効 / 無効
- Do Not Disturb（DND）の有効 / 無効
- Extension Mobility（EM; エクステンション モビリティ）のログイン
- モニタ（将来的に使用、現在ユーザ レベルの更新はありません）
- ハント グループのログアウト
- デバイス モビリティ
- エンド ユーザおよびアプリケーション ユーザの CTI Certificate Authority Proxy Function（CAPF）ステータス
- クレデンシャルのハッキングと認証

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

- コール処理
- フェールオーバー
- 設定済みデバイスの登録

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

## コール詳細レコード（CDR）およびコール管理レコード（CMR）

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

## 遅延のテスト

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

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

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

## エラー率

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

## トラブルシューティング

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

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

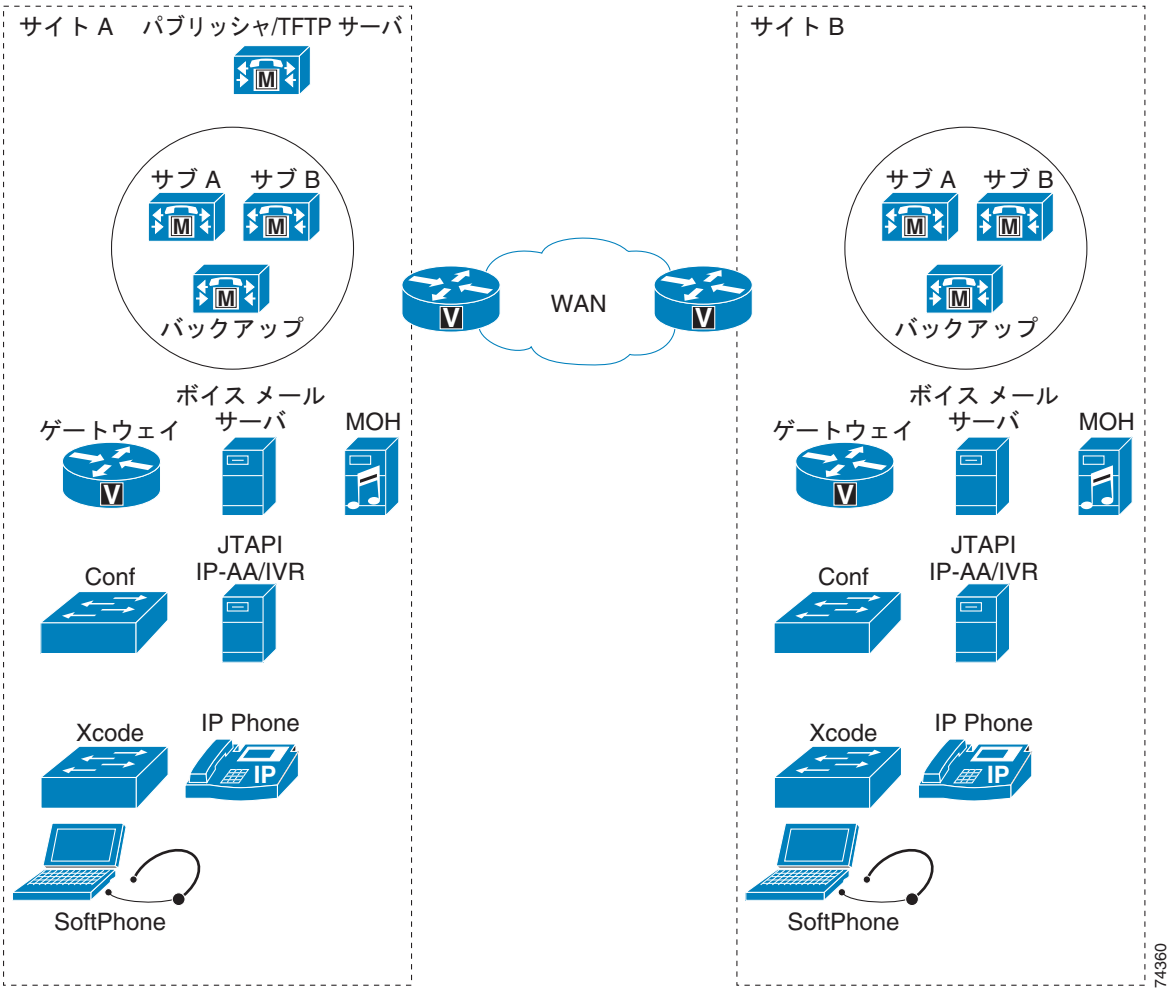
要約すると、ICCS 通信の問題のトラブルシューティングを行うには、次のタスクを実行します。

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

# ローカル フェールオーバー配置モデル

ローカル フェールオーバー配置モデルは、WAN を介したクラスタ化に対する最大の復元性があります。このモデルの各サイトには、少なくとも 1 つのプライマリ Unified CM サブスクライバと 1 つのバックアップ サブスクライバがあります。この設定では、最大 4 つのサイトをサポートできます。電話機および他のデバイスの最大数は、配置されているサーバの数とタイプによって異なります。全サイトの IP Phone の最大総数は 30,000 です （図 5-11 を参照）。

図 5-11　ローカル フェールオーバー モデルの例




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

- 少なくとも 1 つのプライマリ Unified CM サブスクライバと 1 つのバックアップ サブスクライバを含むように、各サイトを設定します。
- Unified CM の *グループ*と *デバイス プール*を設定して、サイト内のデバイスが、あらゆる状況でそのサイトのサーバだけに登録されるようにします。
- 各サイトで主要なサービス（TFTP、DNS、DHCP、LDAP、および IP Phone サービス）、すべてのメディア リソース（カンファレンス ブリッジと Music On Hold）、およびゲートウェイを複製します。複製を確実に行い、最大レベルの復元性を得るよう、シスコは強くお勧めします。また、この方法を拡張して、各サイトにボイスメール システムを組み込むこともできます。
- WAN 障害が発生した場合、パブリッシャ データベースへのアクセスがないサイトでは、いくつかの機能を使用できないことがあります。たとえば、リモート サイトのシステム管理者は、設定を一切追加、変更、または削除することができません。ただし、ユーザは、「Unified CM パブリッシャ」（P.5-42）の項にリストされているユーザ方向の機能に、引き続きアクセスできます。
- WAN 障害が発生した状態では、コールを発信するサブスクライバと現在通信していない電話番号にコールを発信すると、ファーストビジー トーンが聞こえるか、またはコール転送されます（ボイスメールまたは Call Forward Unregistered で設定された宛先に転送される可能性があります）。

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

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

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

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

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

- Intra-Cluster Communication Signaling（ICCS）トラフィックに必要な帯域幅に加え、リモートからパブリッシャとなるあらゆるサブスクライバ サーバに対するデータベースおよびその他のサーバ間トラフィック用に、最低でも 1.544 Mbps（T1）の帯域幅が必要になります。
- WAN を介した CTI Manager も配置する場合は、次の公式を使用して CTI 帯域幅（Mbps）を計算できます。

  （合計 BHCA/10,000）× 1.25

**例 5-1　　2 つのサイトの帯域幅の計算**

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

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

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

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

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

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

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

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

  遅延 = IP WAN を介した RTT 遅延（ms 単位）

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

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

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

  遅延 = RTT 遅延（ms 単位）

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

**例 5-2　　ディレクトリ番号を共有する 2 つのサイトの帯域幅の計算**

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

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

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

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

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

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

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

- クラスタ内のサブスクライバ サーバは、ローカル データベースを読み取ります。データベースの変更は、変更のタイプに応じて、ローカル データベースとパブリッシャのデータベースの両方で発生する可能性があります。クラスタ内のさまざまなサーバの同期には、Informix Dynamic Server（IDS）のデータベース複製が使用されます。そのため、長期間にわたる WAN 接続の喪失など、障害状態から回復する場合は、障害時に行われた可能性があるあらゆる変更と Unified CM

データベースを同期する必要があります。このプロセスは、パブリッシャとクラスタ内のその他のサーバへのデータベース接続が復元されると、自動的に実行されます。低帯域幅のリンクや遅延が大きいリンクでは、このプロセスに時間がかかる場合があります。また、まれなケースですが、手動によるリセットやサーバ間でのデータベース複製の修復が必要になる場合もあります。この操作は、Command Line Interface（CLI; コマンドライン インターフェイス）で **utils dbreplication repair all** や **utils dbreplication reset all** などのコマンドを使用して実行します。WAN を経由して、リモートのサブスクライバでデータベース複製の修復またはリセットを実行すると、クラスタ内のすべての Unified CM データベースが再同期されます。この場合、1.544 Mbps を超える帯域幅が必要になる場合があります。低帯域幅の場合、データベース複製の修復またはリセットが完了するまでに、時間がかかる場合があります。

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

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

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

ローカル フェールオーバー モデルに対する Unified CM クラスタのプロビジョニングは、「コール処理」（P.8-1）の章で説明されているキャパシティについての設計上のガイドラインに従う必要があります。WAN を介してサイト間の音声コールまたはビデオ コールが可能である場合、サイト間のコール アドミッション制御を提供するために、他のサイトのデフォルト ロケーションに加えて、Unified CM の *ロケーション*も設定する必要があります。デバイス数に対して帯域幅が余分にプロビジョニングされ

る場合でも、ロケーションに基づくコール アドミッション制御を設定するのが最良の方法です。ロケーションベースのコール アドミッション制御によってコールが拒否された場合は、自動代替ルーティング（AAR）機能によって公衆網への自動フェールオーバーを行うことができます。

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

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

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

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

## ローカル フェールオーバー用のゲートウェイ

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

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

## ローカル フェールオーバー用のボイスメール

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

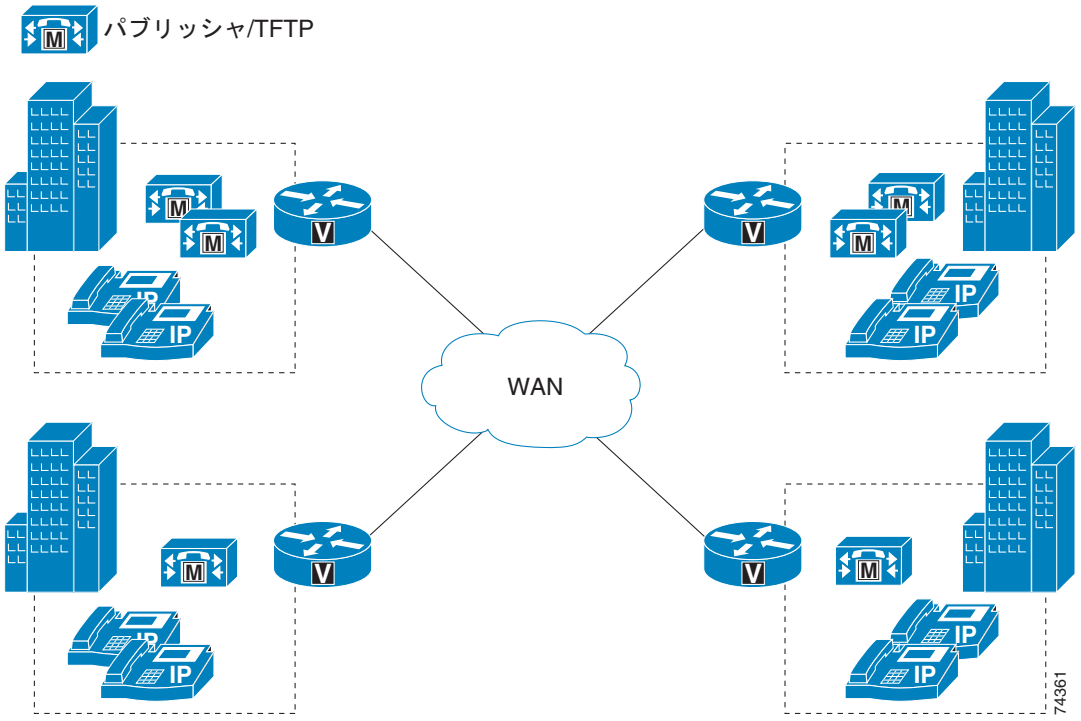
## ローカル フェールオーバーに対する Music On Hold とメディア リソース

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

# リモート フェールオーバー配置モデル

リモート フェールオーバー配置モデルでは、バックアップ サーバを柔軟に配置できます。各サイトには、少なくとも 1 つのプライマリ Unified CM サブスクライバを含め、バックアップ サブスクライバを必要に応じて配置します。このモデルでは、最大 8 つのサイトを配置できます。また、「コール処理」（P.8-1）の章で説明されている 1:1 冗長性と 50/50 ロードバランシング オプションを使用すると、IP Phone やその他のデバイスは、通常、ローカル サブスクライバに登録されます。バックアップ サブスクライバは、他の 1 つ以上のサイトで、WAN を介して配置されます （図 5-12 を参照）。

**図 5-12　　4 サイト構成のリモート フェールオーバー モデル**




リモート フェールオーバー モデルを実装する場合は、ローカル フェールオーバー モデルのガイドライン（「ローカル フェールオーバー配置モデル」（P.5-44）を参照）と、次の変更点に従ってください。

- 少なくとも 1 つのプライマリ Unified CM サブスクライバと、必要に応じてオプションのバックアップ サブスクライバを含むように、各サイトを設定します。IP WAN を経由したバックアップ サブスクライバを設定しない場合は、Survivable Remote Site Telephony（SRST）ルータをバックアップのコール処理エージェントとして使用できます。
- Unified CM の *グループ*と *デバイス プール*を設定して、デバイスが第 2 または第 3 の選択肢として WAN を越えたサーバに登録できるようにします。

- デバイスが、WAN を介して同じクラスタ内のリモート Unified CM サーバに登録される場合、シグナリング トラフィックまたは呼制御トラフィックのために帯域幅を追加する必要があります。この帯域幅は、ICCS トラフィックより大きくなる場合があります。また、シグナリングに関する帯域幅のプロビジョニング計算を使用して計算する必要があります（「帯域幅のプロビジョニング」（P.3-46）を参照）。

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

# 仮想サーバでの Unified Communications の配置

Cisco Unified Communications 製品は、サポートされているバーチャライゼーション サーバ テクノロジーを組み合せて仮想マシンとして実行できます。仮想サーバの主要コンポーネントは、Cisco Unified Computing System（UCS）プラットフォームと、そのハイパーバイザ バーチャライゼーション テクノロジーです。

ここでは、Cisco Unified Computing System（UCS）アーキテクチャ、アプリケーション バーチャライゼーションのためのハイパーバイザ テクノロジー、および Storage Area Networking（SAN; ストレージ エリア ネットワーキング）の概念について説明し、あわせて各製品が企業向け Cisco Virtualized Unified Communications ソリューションのどの位置に納まるかを示します。また、仮想サーバで Unified Communications アプリケーションを配置するための設計考慮事項も示します。

ここでの説明は、http://www.cisco.com/en/US/products/ps10265/index.html から入手できる製品固有の詳細な設計ガイドラインに置き換わるものではありません。

仮想サーバでの Unified Communications システムのサイジングについては、Cisco Unified Communications Sizing Tool を使用してください。このツールは、（有効なログイン認証を持つ）Cisco パートナーおよび従業員が http://tools.cisco.com/cucst から入手できます。

## Cisco Unified Computing System

Unified Computing は、コンピューティング リソース（CPU、メモリ、および I/O）、IP ネットワーキング、ネットワークベースのストレージ、およびバーチャライゼーションを単一の高可用性システムに統合するアーキテクチャです。このレベルの統合により、電力および冷却の費用を節約し、ネットワークへのサーバ接続を簡易化し、物理ホスト間でアプリケーション インスタンスを動的に再配置し、ディスク ストレージ容量をプールできます。

Cisco Unified Computing System は、多くのコンポーネントで構築されています が、サーバの観点からすると、UCS アーキテクチャは次の 2 つのカテゴリに分割されます。

- 「Cisco UCS B シリーズ ブレード サーバ」（P.5-52）
- 「Cisco UCS C シリーズ ラックマウント」（P.5-53）

Cisco Unified Computing System アーキテクチャの詳細については、次の URL から入手可能な資料を参照してください。

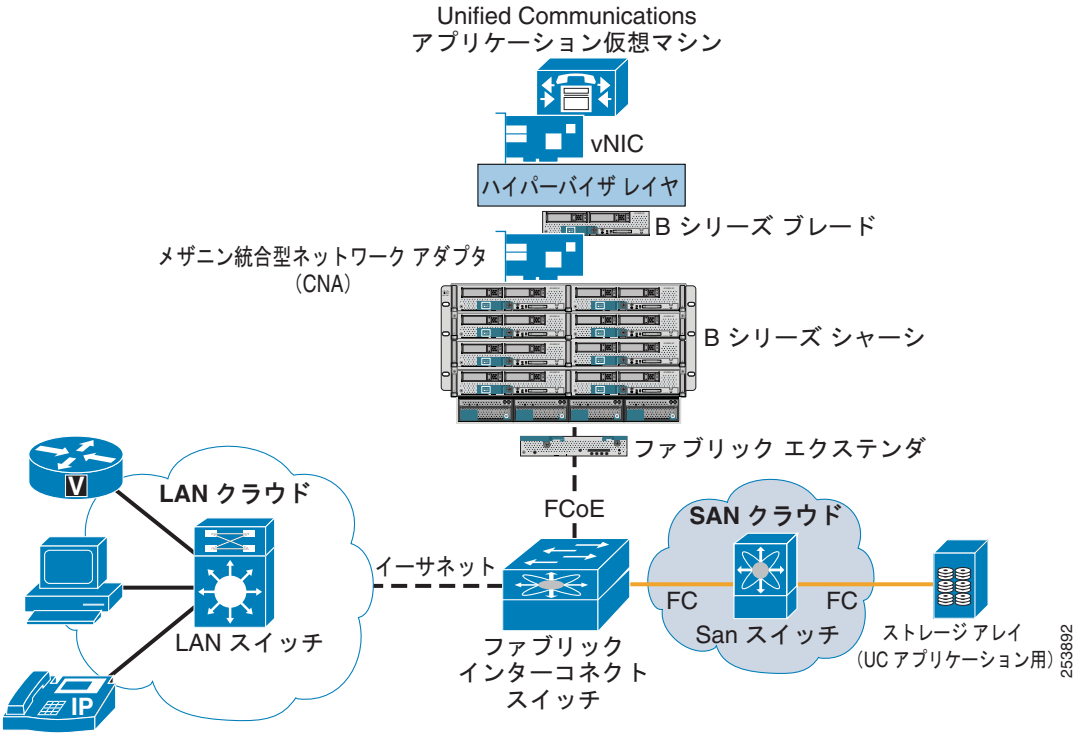
http://www.cisco.com/en/US/netsol/ns944/index.html

# Cisco UCS B シリーズ ブレード サーバ

Cisco Unified Computing System（UCS）機能ブレード サーバは、x86 アーキテクチャに基づいています。ブレード サーバは、コンピューティング リソース（メモリ、CPU、および I/O）をオペレーティング システムおよびアプリケーションに提供します。ブレード サーバは、メザニン フォーム ファクタの Converged Network Adapter（CNA; 統合型ネットワーク アダプタ）を介して統合ファブリックにアクセスできます。

このアーキテクチャでは、Fiber Channel over Ethernet（FCoE）などの技術を利用して、単一のインフラストラクチャで LAN、ストレージ、および高性能コンピューティング トラフィックを転送する統合ファブリックを採用しています （図 5-13 を参照）。Cisco の統合ファブリック技術は 10 Gbps イーサネットを基盤とするため、LAN、SAN、および高性能コンピューティング ネットワークのためにアダプタ、ケーブル、およびスイッチをいくつも用意する必要がありません。

**図 5-13　Cisco UCS B シリーズ ブレード サーバでのユニファイド コミュニケーションの基本的なアーキテクチャ**




ここでは、プライマリ UCS コンポーネントと、そのコンポーネントが Unified Communications ソリューションで機能する方法について簡単に説明します。Cisco UCS B シリーズ ブレード サーバの詳細については、次の URL で入手可能なモデル比較を参照してください。

http://www.cisco.com/en/US/products/ps10280/prod_models_comparison.html

## Cisco UCS 5100 シリーズ ブレード サーバ シャーシ

Cisco UCS 5100 シリーズ ブレード サーバ シャーシは、B シリーズ ブレード サーバをホストするだけでなく、Cisco UCS 2100 シリーズ ファブリック エクステンダによってアップリンクのファブリック インターコネクト スイッチ（Cisco UCS 6100 シリーズ スイッチ）への接続も提供します。

### Cisco UCS 2100 シリーズ ファブリック エクステンダ

Cisco UCS 2100 シリーズ ファブリック エクステンダは、B シリーズ シャーシに挿入され、Cisco UCS 5100 シリーズ ブレード サーバ シャーシを Cisco UCS 6100 シリーズ ファブリック インターコネクト スイッチに接続します。ファブリック エクステンダは、Fiber Channel over Ethernet（FCoE）プロトコルを使用して、ブレード サーバの FCoE 対応 CNA 間のトラフィックをファブリック インターコネクト スイッチ（Cisco UCS 6100 シリーズ）に渡すことができます。

### Cisco UCS 6100 シリーズ ファブリック インターコネクト スイッチ

Cisco UCS 6100 シリーズ ファブリック インターコネクト スイッチは、10 ギガビット FCoE 対応スイッチです。B シリーズ シャーシ（およびブレード サーバ）はファブリック インターコネクトに接続し、ファブリック インターコネクトはデータセンター内の LAN または SAN スイッチング要素に接続します。

### Cisco UCS Manager

管理がシステムのすべてのコンポーネントに統合されるため、Cisco UCS Manager を使用して UCS システム全体を単一のエンティティとして管理できます。Cisco UCS Manager では、直観的なユーザ インターフェイスを使用して、すべてのシステム設定操作を管理できます。

### ハイパーバイザ

ハイパーバイザはサーバ ハードウェアで直接動作してハードウェアを制御するシン ソフトウェア システムであり、複数のオペレーティング システム（ゲスト）がサーバ（ホスト コンピュータ）で同時に動作できます。このため、ゲスト オペレーティング システム（Cisco Unified CM のオペレーティング システムなど）はハイパーバイザとは別の上のレベルで動作します。ハイパーバイザはクラウド コンピューティングおよびバーチャライゼーション テクノロジーの基盤要素のいずれかであり、アプリケーションを統合するサーバの数が少なくて済みます。

### ストレージ エリア ネットワーキング

Storage Area Networking（SAN; ストレージ エリア ネットワーキング）を使用すると、リモート ストレージ デバイスまたはストレージ アレイをサーバに接続して、ストレージがサーバにローカルに接続されているようにオペレーティング システムに認識させるようにすることができます。SAN ストレージは、複数のサーバ間で共有できます。

## Cisco UCS C シリーズ ラックマウント

B シリーズ ブレード サーバだけでなく、Cisco Unified Computing System（UCS）も、x86 アーキテクチャに基づいた汎用ラックマウント サーバを特徴としています。C シリーズ ラックマウント サーバは、コンピューティング リソース（メモリ、CPU、I/O）およびローカル ストレージをオペレーティング システムとアプリケーションに提供します。C シリーズ サーバの詳細については、次の Web サイトにある資料を参照してください。

http://www.cisco.com/en/US/products/ps10493/index.html

# B シリーズ ブレード サーバ上で仮想 Unified Communications アプリケーションを実行する場合の設計上の考慮事項

ここでは、仮想サーバで Unified Communications サービスを実行する場合に従う必要がある設計規則および考慮事項を示します。次の Cisco Unified Communications アプリケーションが、仮想サーバをサポートしています。

- Cisco Unified Communications Manager
- Cisco Unity
- Cisco Unity Connection
- Cisco Unified Presence
- Cisco Unified Contact Center Express
- Cisco Unified Contact Center Enterprise 製品
- Cisco Unified Customer Voice Portal 製品

## ブレード サーバ

仮想 Cisco Unified Communications アプリケーションは、統合型ネットワーク アダプタを備えた Cisco B シリーズ ハーフ幅ブレード サーバ（B200 M1）で実行する必要があります。1 つの B200 M1 ブレードが 2 つのクアッドコア CPU をホストできます。このため、計 8 個の CPU コアをアプリケーションに使用できます。

Cisco Unified Communications アプリケーションは、Unified Communications 以外のアプリケーションは実行しない専用のブレードで実行する必要があります。各 Unified Communications アプリケーションは、専用の CUP およびメモリ リソースに割り当てて、リソース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。

## ハイパーバイザ

仮想 Unified Communications アプリケーションを実行するには、VMware ESXi 4.0（またはそれ以降の）ハイパーバイザが必要です。ブレード サーバに接続されているローカル ハード ドライブは、仮想マシンの格納には使用できません。これらは、ESXi ハイパーバイザ ソフトウェアのインストールにだけ使用できます。Unified Communications アプリケーションは、仮想マシンのテンプレートおよび設定についてそれぞれのガイドラインに従う必要があります。

VMware vCenter は必須ではありませんが、配置の規模が大きく複数の ESXi ホストを管理するときにお勧めします。

仮想マシンの具体的な設定要件とサイジング要件については、http://www.cisco.com から入手できるそれぞれの製品マニュアルを参照してください。

## SAN およびストレージ アレイ

Unified Communications アプリケーションは、Fiber Channel（FC; ファイバ チャネル）経由でリモート ストレージ アレイにアクセスできる必要があります。仮想サーバでの Unified Communications アプリケーションの実行にあたって、iSCSI、NAS、DAS の各プロトコルはサポートされません。ストレージ アレイは、VMware ハードウェア互換性リストに準拠している必要があります。SAN から ESXi を起動するオプションもサポートされません。

（注）　Cisco は、業界標準に基づき、EMC や NetApp などのストレージ アレイ プロバイダーと連携するストレージ ネットワーキング製品およびスイッチング製品を提供します。Virtualized Unified Communications は、Cisco UCS および VMware がサポートするストレージ アクセス製品およびストレージ アレイ製品でサポートされます。ストレージ ネットワーキングの詳細については、http://www.cisco.com/en/US/netsol/ns747/networking_solutions_sub_program_home.html で入手できるドキュメントを参照してください。

## C シリーズ ラックマウント サーバ上で仮想 Unified Communications アプリケーションを実行する場合の設計上の考慮事項

UCS C シリーズ ラックマウント サーバ上で Cisco Unified Communications アプリケーションを仮想サーバとして実行するには、満たしておかなければならない特定の要件があります。これらの要件については、次の資料を参照してください。

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/solution_overview_c22-597556.html

次の Cisco Unified Communications アプリケーションが、C シリーズ ラックマウント サーバ上で仮想サーバ サポートを提供します。

- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco Unified Contact Center Express

## 仮想サーバが配置モデルに及ぼす影響

仮想サーバでの Cisco Unified Communications アプリケーションの配置では、物理サーバを使用するときと同じ配置モデルがサポートされます。「ネットワーク インフラストラクチャ」（P.3-1）の章では、Cisco UCS B ブレード仮想サーバの QoS 機能をネットワークに統合する方法に関する設計ガイドラインを示します。また、多くの場合、物理サーバ（Cisco MCS サーバなど）と Cisco UCS 仮想サーバの統合もサポートされます。たとえば、Music On Hold（MoH; 保留音）サーバは、Cisco MCS サーバ プラットフォームで実行できるほか、他のメンバー サーバが Cisco UCS 仮想サーバで実行されるクラスタのメンバーになることもできます。

この章で説明するすべてのコール処理配置モデルが、Cisco UCS 仮想サーバ プラットフォームでサポートされます。

# U. S. Section 508 準拠についての設計上の考慮事項

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

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

- ネットワーク上の Quality of Service（QoS）を使用可能にします。

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

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

    IP Phone のハンドセットを TTY/TDD に接続しているカップリング機器に置きます。アコースティック カップルは、RJ-11 接続に比較すると信頼性が劣ります。カップリング方式は部屋の周囲の雑音やその他の要素で、一般的に通信エラーを起こしやすい方式です。
- stutter ダイヤルトーンをサポートする必要がある場合は、アナログ電話を Cisco VG248 または ATA 188 上に備えている FXS ポートに接続します。また、ほとんどの Cisco IP Phone では、スタッター ダイヤル トーンをサポートしています。この機能は、Audible Message Waiting Indication（AMWI; 音声メッセージ待機インジケータ）と呼ばれることもあります。この機能をサポートする具体的な Cisco IP Phone のモデルについては、「エンドポイント機能の要約」（P.19-51）を参照してください。

# Service Advertisement Framework のコール制御ディスカバリを使用したコール ルーティングおよびダイヤル プラン配信

複数のコール処理エージェントが同じシステムに存在する場合、相互に認識するようにそれぞれを手動で設定できます。この設定には時間がかかることがあり、エラーも発生しやすくなっています。さまざまなコール処理エージェント間でコール ルーティングを実現するには、コール エージェントでスタティック ルートを設定し、変更のたびに更新する必要があります。

代わりに、Cisco Service Advertisement Framework（SAF）を使用すると、コール エージェント間でコール ルーティングおよびダイヤル プラン情報を自動的に共有できます。SAF を使用すると、Cisco 以外のコール エージェント（TDM PBX など）も Cisco IOS ゲートウェイを介して相互接続して Service Advertisement Framework に参加させることができます。

Service Advertisement Framework（SAF）を使用すると、ネットワーク アプリケーションで IP ネットワーク内のネットワーク サービスに関する情報をアドバタイズしたり検出したりできます。SAF は、次の機能コンポーネントおよびプロトコルで構成されています。

- SAF クライアント：サービスに関する情報をアドバタイズしたり消費したりします。
- SAF フォワーダ：SAF サービスの可用性情報を配布したり維持したりします。
- SAF クライアント プロトコル：SAF クライアントと SAF フォワーダ間で使用されます。
- SAF フォワーダ プロトコル：SAF フォワーダ間で使用されます。

アドバタイズされたサービスの特性は、SAF フォワーダのネットワークにとって重要ではありません。SAF フォワーダ プロトコルは、サービスの可用性に関する情報を、SAF ネットワークに登録されている SAF クライアント アプリケーションに動的に配布するように設計されています。

## SAF でアドバタイズできるサービス

理論上は、どのサービスでも SAF を介してアドバタイズできます。SAF を使用する最も重要なサービスは、Cisco Unified Communications の Call Control Discovery（CCD; コール制御ディスカバリ）です。CCD は SAF を使用して、Cisco Unified CM、Unified CME などの呼制御エージェントによってホストされる内部 Directory Number（DN; ディレクトリ番号）の可用性に関する情報を配布および維持します。また、CCD は、これらの内部ディレクトリ番号に公衆網から到達できるようにする対応した番号プレフィックスも配布します（「To PSTN」プレフィックス）。

SAF の動的な特性、およびコール エージェントがホストする DN 範囲と To PSTN プレフィックスの可用性を SAF ネットワーク内の他のコール エージェントにアドバタイズできることにより、静的でより労働集約的な他のダイヤル プラン配布方式を大幅に上回るメリットを提供します。

この章では、SAF 対応 Unified Communications ネットワークでの Call Control Discovery（CCD; コール制御ディスカバリ）の配置について説明します。SAF 自体の詳細については、「Service Advertisement Framework（SAF）」（P.3-63）を参照してください。

次の Cisco 製品が、SAF に対応した Call Control Discovery（CCD; コール制御ディスカバリ）サービスをサポートしています。

- Cisco Unified Communications Manager（Unified CM）Release 8.0(1) 以降
- Cisco Integrated Services Router（ISR; サービス統合型ルータ）上の Cisco Unified Communications Manager Express（Unified CME）
- Cisco ISR プラットフォーム上の Survivable Remote Site Telephony（SRST）

- Cisco ISR プラットフォーム上の Cisco Unified Border Element
- Cisco ISR プラットフォーム上の Cisco IOS ゲートウェイ

CCD は、Cisco IOS Release 15.0(1)M 以降で動作する Cisco ISR プラットフォームでサポートされます。Cisco IOS Release 15.0(1)M の詳細については、次の Web サイトを参照してください。

- http://wwwin.cisco.com/ios/release/15mt
- http://www.cisco.com/en/US/products/ps10621/index.html

Unified CM での CCD の使用の詳細については、次の URL で入手可能な『*Cisco Unified Communications Manager Features and Services Guide*』を参照してください。

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

## SAF サービス ID

CCD が最初の SAF サービスです。SAF サービスは、SAF フォワーダと SAF クライアントからなるネットワークでそれぞれの SAF サービス ID によって識別されます。Unified Communications の CCD は、101:2:*x.x.x.x* という SAF サービス ID を使用します。その意味は次のとおりです。

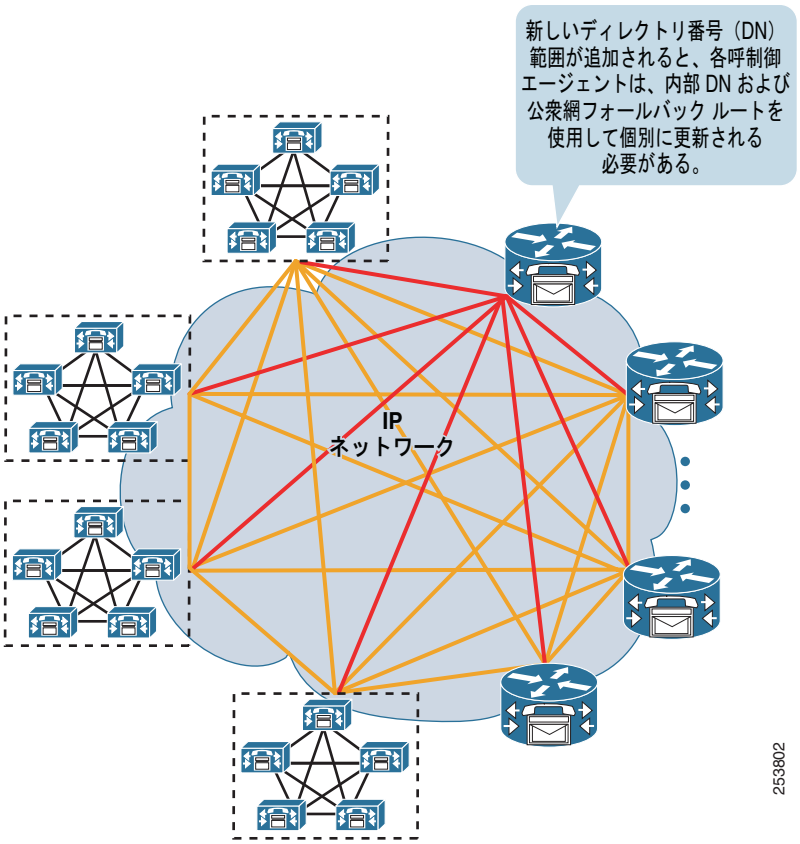
- サービス ID 101 = Unified Communications
- サブサービス ID 2 = CCD
- インスタンス ID *x.x.x.x* = Unified CM クラスタ（PKID）または Cisco IOS デバイスの ID

## ネットワーク内での SAF CCD の配置

SAF CCD サービスを使用すると、Unified CM や Unified CME などの呼制御エージェントがホストするディレクトリ番号範囲の場所および可用性に関する情報を SAF 対応 Unified Communications ネットワーク内で動的に伝達できます。

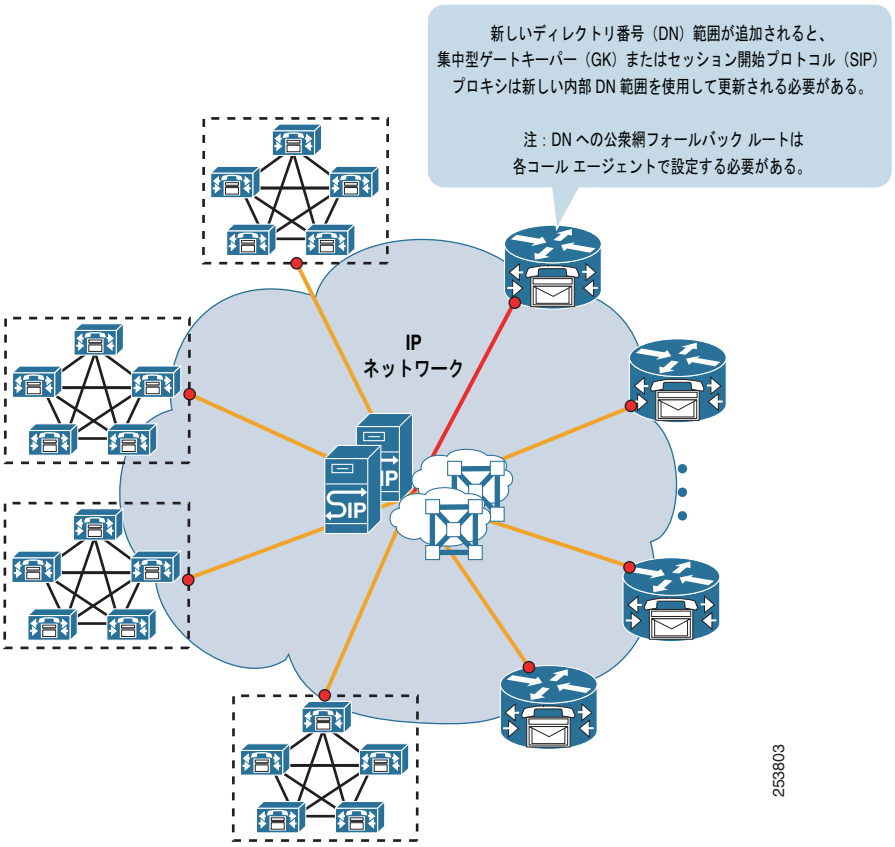
SAF を配置して DN 情報を配布および保守する利点は、4 個の Unified CM クラスタと 40 個の Unified CME で構成される Unified Communications ネットワークでダイヤル プランを管理する場合を考えてみると理解できます。静的に設定したネットワークでは、Unified Communications システム内に新しいディレクトリ番号範囲が導入された場合、その新しい番号範囲に到達する方法の詳細を、Unified Communications ネットワーク内の他のすべての呼制御アプリケーションが入手できるようにする必要があります。最悪の場合、すべての呼制御アプリケーション間に接続のフル メッシュを構築し、新しい番号範囲とその到達方法に関する情報で各呼制御アプリケーションを更新する必要があります（図 5-14 を参照）。この設定変更の連鎖は時間がかかってエラーが発生しやすいため、多大な管理作業が必要になります。

図 5-14　呼制御アプリケーション間の接続のフル メッシュ



ダイヤル プランは、ゲートキーパーまたは SIP プロキシに集中化できます（図 5-15 を参照）。これにより、設定オーバーヘッドは削減されますが、集中化できるのが内部ダイヤル プランに限られます。集中型ダイヤル プランへのアクセスが使用できなくなった場合、公衆網ルートなどの代替ルートを使用できるのは、そのルートが各呼制御アプリケーションでバックアップ ルートとして設定されている場合に限られます。

**図 5-15　　集中型内部ダイヤル プラン**




SAF CCD を使用すると、各呼制御アプリケーションがディレクトリ番号範囲とその対応する「To PSTN」プレフィックスを SAF ネットワーク内の他のすべての呼制御アプリケーションにアドバタイズできます （図 5-16 および図 5-17 を参照）。そのために、SAF CCD は次の制限を解除します。

- 内部システム全体のダイヤル プランをホストする集中型アプリケーションの必要性。
- 新しい DN 範囲およびその対応する「To PSTN」プレフィックスが Unified Communications ネットワークに追加された場合、各呼制御アプリケーションを個別に設定するという要件。

また、SAF CCD には静的な性質ではなく動的な性質があります。DN 範囲を削除するか、または呼制御アプリケーションへの IP 接続を失うと、SAF ネットワークは、使用できない DN へのルートを取り消して他のすべての呼制御アプリケーションを自動的に更新します。同様に、接続を再確立すると（または DN 範囲を再設定すると）、SAF ネットワークは他のすべての呼制御アプリケーションを更新して、DN 範囲を復元します。

図 5-16　Unified CM 内部 DN 範囲および対応する「To PSTN」プレフィックスの SAF ネットワークへのアドバタイズ

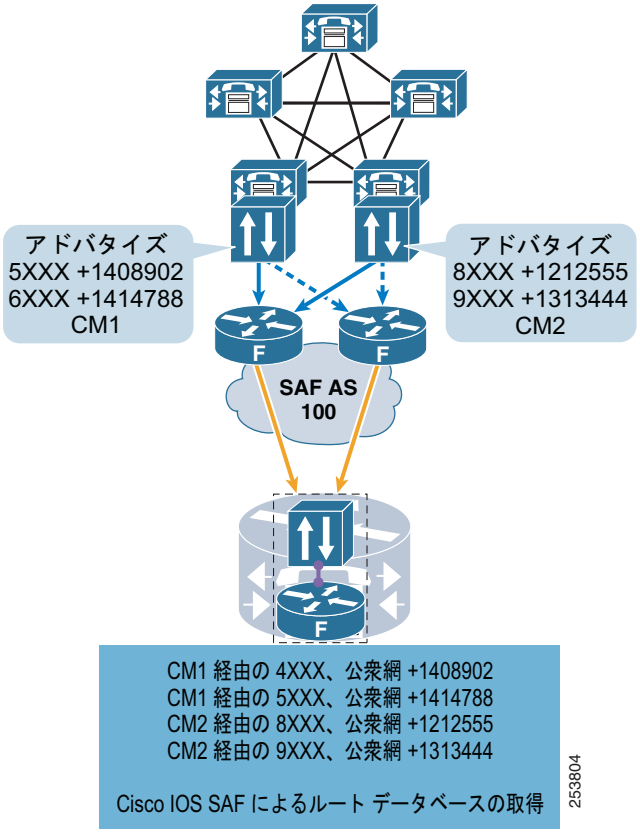
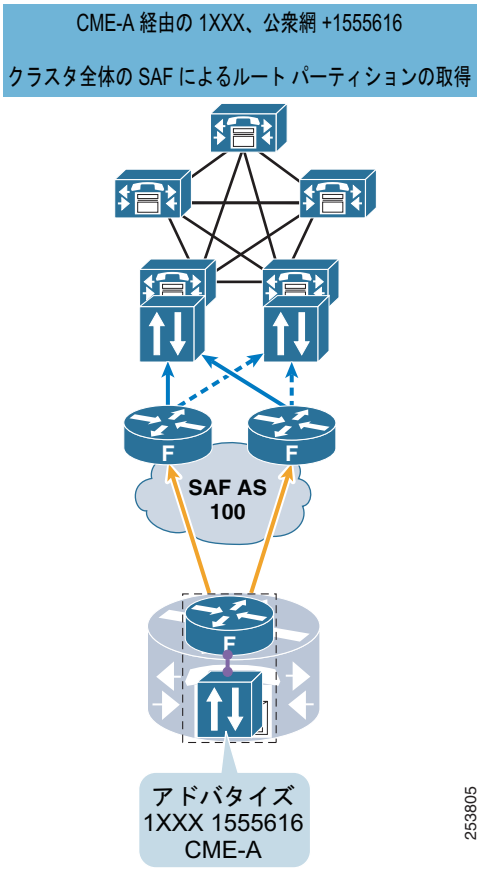


図 5-17　Unified CME 内部 DN 範囲および対応する「To PSTN」プレフィックスの SAF ネットワークへのアドバタイズ




# SAF CCD 操作と標準の Unified CM コール ルーティングの比較

SAF CCD を使用したコール ルーティングは、標準の Unified CM コール ルーティングとは根本的に異なります。標準の Unified CM コール ルーティングではルート パターン、ルート リスト、およびルート グループを使用しますが、これらは SAF CCD では使用しません。代わりに、ディレクトリ番号、ディレクトリ番号範囲、およびリモート エンドポイントへの「To PSTN」プレフィックスが、静的に設定されるのではなく、SAF CCD 対応クラスタによって動的に学習されます（図 5-18 を参照）。SAF CCD では、各 Unified CM クラスタ（または他の SAF 対応呼制御アプリケーション）が、SAF ネットワークにアドバタイズするディレクトリ番号や DN 範囲などを設定します。SAF CCD は、クラスタ内の SAF 対応 SIP トランクまたは H.323 トランクの IP アドレスおよびポート番号をアドバタイズして、これらの番号に到達する方法もアドバタイズします。

また、各 SAF 対応クラスタは、DN、DN 範囲、関連付けられた「To PSTN」プレフィックス、およびトランク情報に関する他のクラスタからのアドバタイズメントを監視します。このような SAF 学習ルートは、単一のパーティションに配置されます。このパーティションへのアクセス権があるデバイスであれば、SAF 内でアドバタイズされるデバイスに到達できます。SAF CCD では、内部 DN 範囲とその To PSTN ルートだけを配布することをお勧めします。

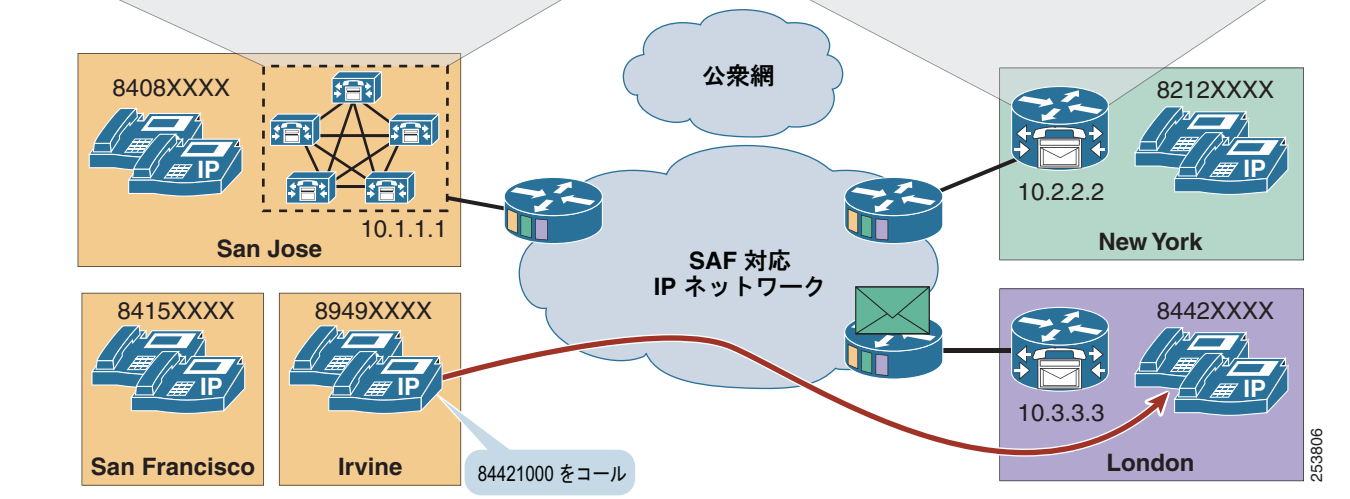
図 5-18　SAF CCD での動的コール ルーティング

**New York Unified CME ルーティング テーブル**

| DN パターン | 「対 DID」規則 | IP アドレス | プロトコル |
|---|---|---|---|
| 8408XXXX | +1408555 /4 | 10.1.1.1 | SIP |
| 8415XXXX | +1415777 /4 | 10.1.1.1 | SIP |
| 8949XXXX | +1949222 /4 | 10.1.1.1 | SIP |
| **8442XXXX** | **4:+442077111** | **10.3.3.3** | **H.323** |
| | | | |

**San Jose Unified CM ルーティング テーブル**

| DN パターン | 「対ダイヤルイン方式（DID）」規則 | IP アドレス | プロトコル |
|---|---|---|---|
| 8212XXXX | 4:+1212444 | 10.2.2.2 | SIP |
| **8442XXXX** | **4:+442077111** | **10.3.3.3** | **H.323** |
| | | | |




SAF 学習ルートを使用して発信されたコールは、着信側番号への IP パスが使用できない場合、自動的に公衆網にフェールオーバーされます（図 5-19 を参照）。コールは、次の順序に従ってルーティングされます。

- 選択した IP パスを取得して、着信番号に到達します。
- IP パスが使用できない場合は、公衆網プレフィックスを使用して、着信番号を変更し、コールを公衆網経由でルーティングします。

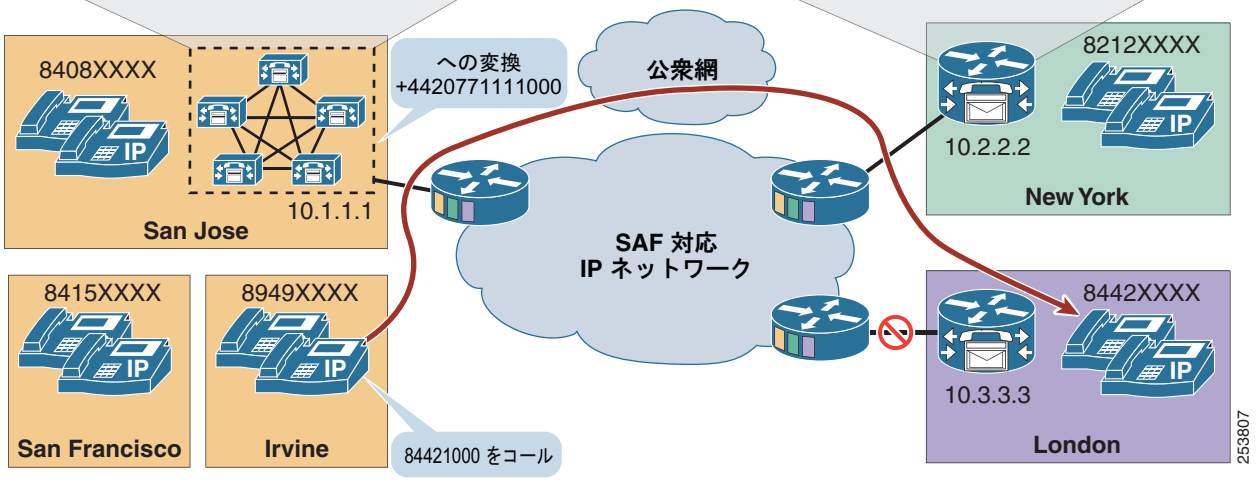
図 5-19　SAF CCD での自動公衆網フェールオーバー

San Jose Unified CM ルーティング テーブル

| DN パターン | 「対ダイヤルイン方式（DID）」規則 | IP アドレス | プロトコル |
|---|---|---|---|
| 8212XXXX | 4:+1212444 | 10.2.2.2 | SIP |
| **8442XXXX** | **4:+442077111** | **10.3.3.3** | **H.323** |
| | | | |

New York Unified CME ルーティング テーブル

| DN パターン | 「対 DID」規則 | IP アドレス | プロトコル |
|---|---|---|---|
| 8408XXXX | +1408555 /4 | 10.1.1.1 | SIP |
| 8415XXXX | +1415777 /4 | 10.1.1.1 | SIP |
| 8949XXXX | +1949222 /4 | 10.1.1.1 | SIP |
| **8442XXXX** | **4:+442077111** | **10.3.3.3** | **H.323** |
| | | | |




SAF CCD は、特定の SIP コールまたは H.323 コールに対して IP ルートを 1 つだけ選択できるという点で、標準のコール ルーティングとは異なります。一方、標準のコール ルーティングでは、ルート リストおよびルート グループを使用して、単一のコールに複数の IP パスを定義し、連続して試行できます。

# CCD および Unified CM

CCD を使用すると、Unified CM は複数のディレクトリ番号、ディレクトリ番号範囲、および対応する「To PSTN」プレフィックスを SAF 対応ネットワークにアドバタイズできます。CCD は、Unified CM に新たに複数の設定可能なコンポーネントを導入します。

- SAF フォワーダ設定（Unified CM 上の外部 SAF クライアント）
- SAF 対応トランク
- ホスト DN パターン
- ホスト DN グループ
- CCD アドバタイズ サービス
- CCD 要求サービス

## SAF フォワーダ設定（Unified CM 上の外部 SAF クライアント）

Unified CM 上の SAF フォワーダ設定は、Unified Communications ネットワークで SAF フォワーダに対する外部 SAF クライアントの設定を表します。Unified CM SAF フォワーダ設定では、次の項目を定義します。

- リモート SAF フォワーダの宛先 IP アドレスおよびポート番号
- SAF フォワーダでの認証に使用するセキュリティ プロファイル（ユーザ名およびパスワード）
- クライアント ラベル

  これは、SAF フォワーダが Unified CM 外部クライアントを特定の SAF 自律システムにマッピングするときに使用する文字列です。Cisco IOS はクライアント ラベルのバルク プロビジョニングをサポートしており、@ で終わるクライアント ラベル文字列は基本名または基本ラベルであると見なされます。ルータに設定された基本ラベルは、基本名で @ に続く文字を有効なクライアント ラベルとして受け付け、外部クライアントが送信した REGISTER メッセージに含まれるクライアントを識別します。

たとえば、Unified CM クラスタ A は、CUCM-A をクラスタの基本名として使用でき、設定された各 SAF フォワーダ（Unified CM 上の外部 SAF クライアント）の基本名に続く @ の後に番号を付加できます。Cisco IOS で外部クライアント CUCM-A を基本名として定義すると、Cisco IOS フォワーダは、次のような CUCM-A@ で始まるクライアント ラベルを受け付けます。

- CUCM-A@Client-1
- CUCM-A@Client-2
- CUCM-A@Client-3
- CUCM-A@Client-4

これで、SAF クライアント 1 ～ 4 は、同じ SAF フォワーダおよび SAF Autonomous System（AS; 自律システム）に登録できます。

## Unified CM クラスタ内での外部 SAF クライアント インスタンスの作成とアクティブ化

デフォルトでは、Unified CM の [SAF Forwarder Configuration] ページで設定した外部 SAF クライアントのインスタンスが、クラスタ内のどのコール処理ノードにも作成されます（図 5-20 を参照）。外部 SAF クライアントがアクティブになるのは、コール処理ノードで CCD アドバタイズ サービスまたは CCD 要求サービスのインスタンスもアクティブになっている場合だけです。コール処理ノードでのアドバタイズ サービスおよび要求サービスのアクティブ化は、各サービスに関連付けられた SAF トランクによって決まります （詳細については、「CCD アドバタイズ サービスおよび要求サービス」（P.5-69）を参照してください）。

図 5-20　Unified CM での単一の SAF フォワーダの定義

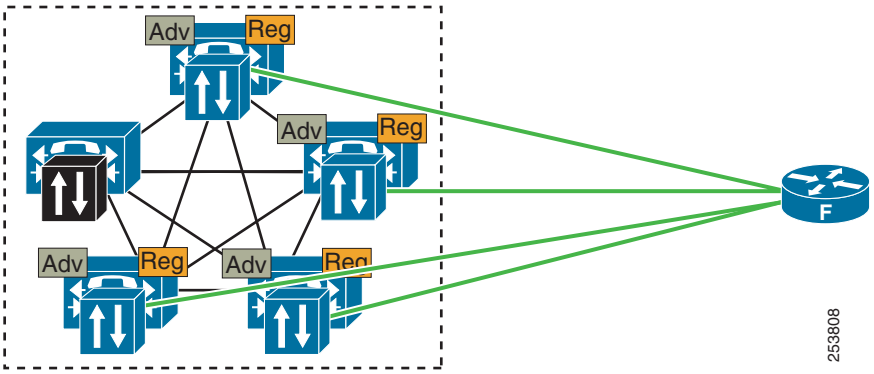
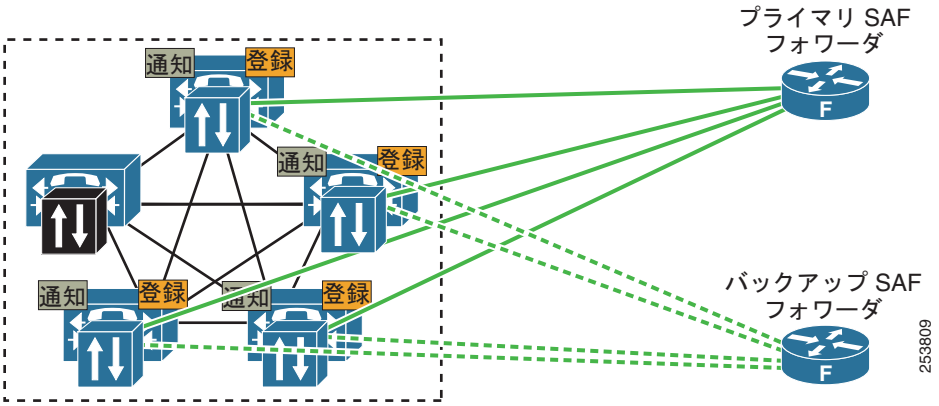



図 5-20 に、単一の SAF フォワーダにアクティブな 4 つの外部 SAF クライアントが接続されている様子を示します（灰色表示の SAF クライアントはアクティブではありません。アクティブなアドバタイズ サービスまたは要求サービスが Unified CM ノードに関連付けられていないためです）。アクティブな各外部 SAF クライアントが、SAF フォワーダへの接続を確立し、SAF ネットワークに登録し、関連付けられているサービスを公開し、SAF AS でアクティブな SAF CCD サービスをサブスクライブします。このような重複は復元力および冗長性の確保に役立ちますが、その一方でクラスタと SAF フォワーダ内にオーバーヘッドが発生します。クラスタ内でのアドバタイズ サービスおよび要求サービスの実行場所を慎重に選択することによって、このような重複および冗長性を微調整できます。詳細については、「CCD アドバタイズ サービスおよび要求サービス」（P.5-69）を参照してください。

## 複数の SAF フォワーダ

冗長性を確保するために、クラスタ内に複数の SAF フォワーダを設定できます。SAF クライアントは、プライマリとバックアップの SAF フォワーダへのセキュアな接続を確立し、SAF フォワーダに登録し、HostedDN サービスの公開要求をプライマリ SAF フォワーダに送信します。SAF クライアントは、クライアントからの登録要求に最初に応答した SAF フォワーダを選び、システム起動時に 1 つの SAF フォワーダをプライマリとして選択し、別の SAF フォワーダをバックアップとして選択します。SAF クライアントは、プライマリ SAF フォワーダだけを対象とするサービスを公開し、サブスクライブします。SAF クライアントは、通常の間隔でキープアライブを SAF フォワーダに送信して、SAF フォワーダへの接続を保持します。プライマリ SAF フォワーダへの接続が失敗した場合、SAF クライアントはバックアップ SAF フォワーダに切り替えて、それまでプライマリ SAF フォワーダに送信されたすべての公開要求およびサブスクライブ要求をバックアップ SAF フォワーダに送信します。

図 5-21　Unified CM での 2 つの SAF フォワーダの定義



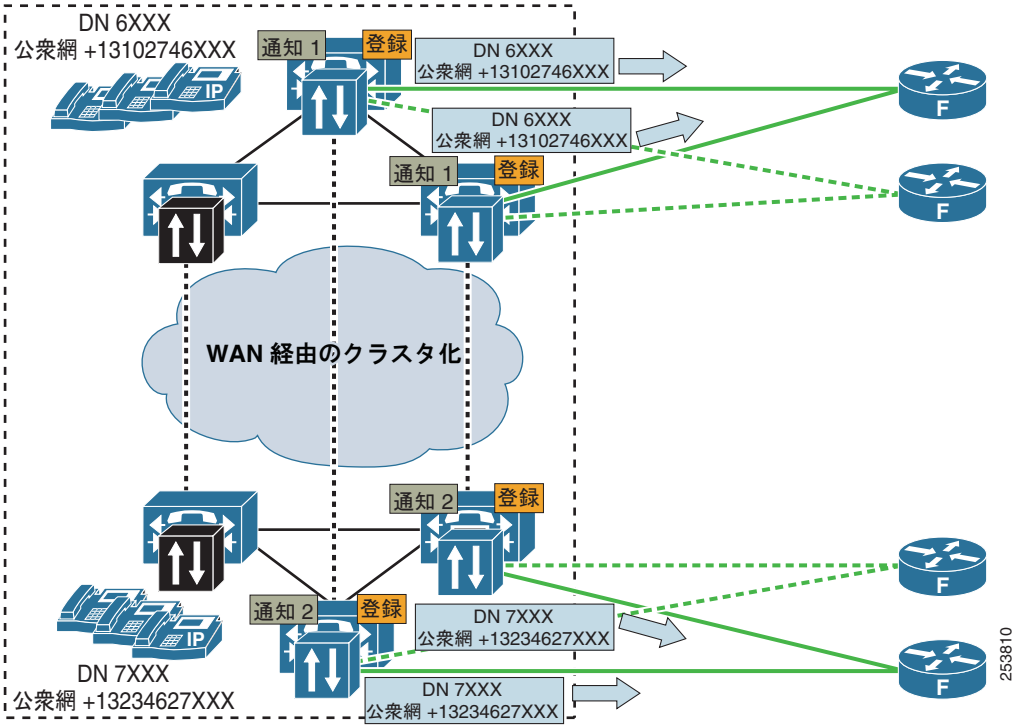
# 高度な SAF クライアント設定

デフォルトでは、SAF クライアントのインスタンスが、Unified CM クラスタ内のすべてのコール処理ノードに作成されます。高度な SAF フォワーダ設定オプションを使用すると、管理者はクラスタ内の特定のコール処理ノードのみに SAF クライアントを作成できます。この設定オプションでは、管理者はクラスタ内の特定のノードに SAF クライアントを作成できるほか、WAN を介したクラスタ化を採用するシステム向けに CCD サービスを広域に分散するように SAF CCD を設定できます。

## SAF CCD および WAN を介したクラスタ化

WAN を介したクラスタ化を採用するクラスタ内では、複数の SAF クライアント インスタンスおよび複数のアドバタイズ サービスを作成して、特定の Unified CM ノードに関連付けることによって、クラスタ内のローカルな Unified CM トランクおよびノードの地理的な関連付けとともに、CCD ホスト ディレクトリ番号範囲を SAF ネットワークにアドバタイズできます。

**図 5-22　　WAN を介したクラスタ化において、SAF CCD により SAF クライアントを選択する設定**




## SAF 対応トランク

SAF 対応トランクは、SAF 対応呼制御アプリケーション間でコールをルーティングするためにだけ使用されます。標準のルート パターン、ルート リスト、およびルート グループとは併用できません。SAF 対応トランクの宛先アドレスは、SAF を介して学習されるため設定できません。それ以外のトランク パラメータは設定できます。

次のトランク タイプで SAF を有効にできます。

- SIP トランク : SIP トランクの新規作成時に [Trunk Service Type] として [Call Control Discovery] を選択すると、有効になります。
- H.323 非ゲートキーパー制御クラスタ間トランク : [Trunk] 設定ページで [Enable SAF] チェックボックスをオンにすると、有効になります。

このどちらのトランク タイプも、Unified CM クラスタ間および Unified CM と Cisco IOS ゲートウェイ間で使用できます。

CCD は、SAF 対応トランクを次の 2 つの目的で使用します。

- コールの発信：このような SAF 対応トランクは、CCD 要求サービスに関連付けられます。
- 着信コールの受け付け：このような SAF 対応トランクは、CCD アドバタイズ サービスに関連付けられます。このような SAF 対応トランクの IP アドレスおよびポート番号は、アドバタイズ サービスに関連付けられた DN 範囲とともに公開されます。

アドバタイズ サービスと要求サービスのどちらも、SAF 対応トランクを使用できます。

CCD アドバタイズ サービスは、ホスト DN 範囲のトランクの詳細を公開するとき、SAF トランクの Cisco Unified Communications Manager グループに属する各 Unified CM ノードの IP アドレスおよびポート番号を個別の SAF アドバタイズメントで送信します。たとえば、Cisco Unified Communications Manager グループに CUCM1 および CUCM2 がある SIP トランク A からホスト DN 範囲 5*XXX* をアドバタイズする場合、CCD アドバタイズ サービスは次の 2 つのアドバタイズメントを公開します。

- SIP トランク IP アドレス（CUCM1）ポート番号 5060 を経由する 5XXX
- SIP トランク IP アドレス（CUCM2）ポート番号 5060 を経由する 5XXX

このアドバタイズメントを受信するクラスタの要求サービスは、5XXX への 2 つのルートを SAF 学習ルート パーティションに配置します。

- SIP トランク IP アドレス（CUCM1）ポート番号 5060 を経由する 5XXX
- SIP トランク IP アドレス（CUCM2）ポート番号 5060 を経由する 5XXX

このクラスタから 5XXX へのコールが、2 つの使用可能な SIP トランク宛先をラウンドロビン順に選択します。

SAF トランクは、TCP または UDP 転送プロトコルをサポートします。SAF トランクが複数の呼制御アプリケーションから着信コールを受け付けることができるため、SAF 対応トランクでは TLS ベースのシグナリング認証と暗号化がサポートされません。

### ホスト DN パターンおよびホスト DN グループ

ホスト DN グループとは、ホスト DN パターンのグループのことです。ホスト DN グループのホスト DN パターンは、一般に物理的なサイトに関連付けられたディレクトリ番号の範囲のことです。ホスト DN グループごとに「To PSTN」フェールオーバー ルーティング用の番号削除および先頭付加情報を設定できます。同じ DN パターンを複数のホスト DN グループに関連付けることはできません。

ホスト DN パターンには、1 つのディレクトリ番号（たとえば、5000）も、広範囲のディレクトリ番号（たとえば、5*XXX*）も定義できます。どの DN パターンも一意である必要があります。各ホスト DN パターンは、公衆網フェールオーバー ルーティングに対応するための番号削除および先頭付加情報とともに設定できます。ホスト DN パターンでの公衆網フェールオーバー設定は、ホスト DN グループ レベルの公衆網フェールオーバー設定よりも優先されます。

## CCD アドバタイズ サービスおよび要求サービス

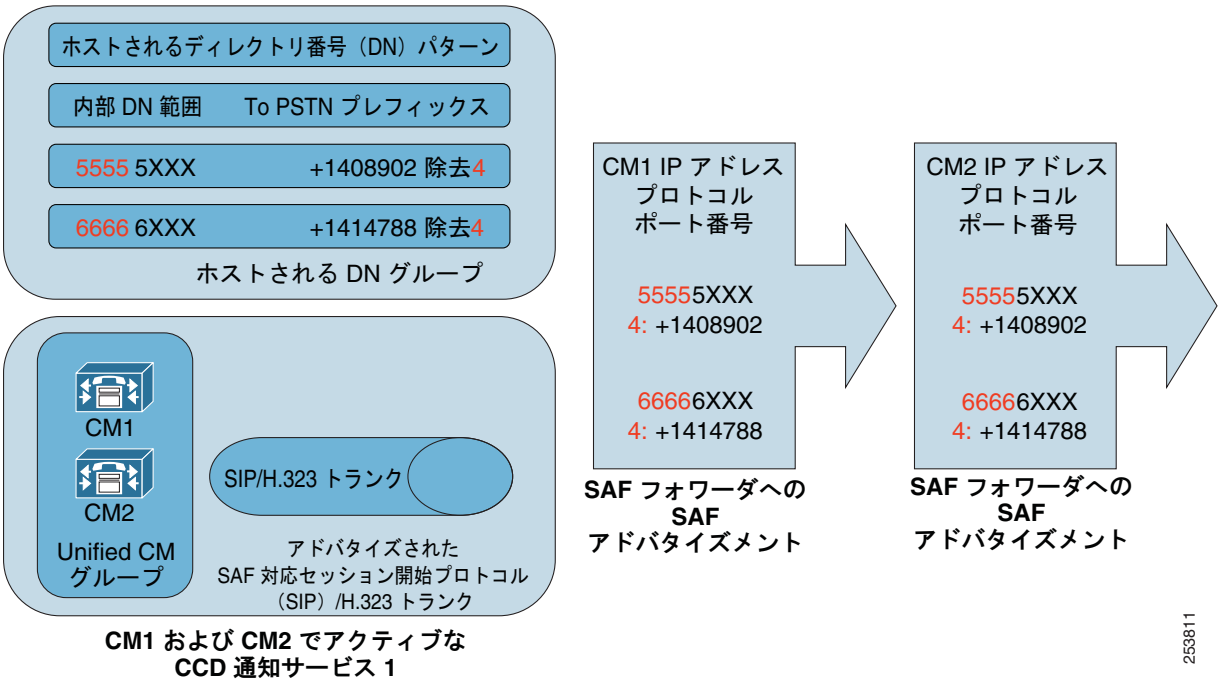
CCD は、2 つの Unified CM サービスを使用して、SAF ネットワークと通信します。アドバタイズ サービスは DN 範囲およびその関連するトランクを SAF ネットワークに公開するために使用し、要求サービスは SAF ネットワーク内の他のコール エージェントから DN 範囲への到達可能性を学習するために使用します。以降の項では、この 2 つのサービスについて説明します。

### CCD アドバタイズ サービス

CCD アドバタイズ サービスは、1 つのホスト DN グループを SAF 対応 SIP トランクや H.323 トランクに関連付けます。アドバタイズ サービスは、関連付けられた SAF 対応トランクの属する Cisco Unified Communications Manager グループ（Unified CM Group）内のそれぞれのサーバで作成されてアクティブ化されます。アドバタイズ サービスは、各トランクのある Unified CM Group 内のそれぞれのサーバ上にある SAF クライアントを使用して、ホスト DN グループおよび関連付けられたトランク ノードに関する情報をクライアントの SAF フォワーダに公開します （図 5-23 を参照）。

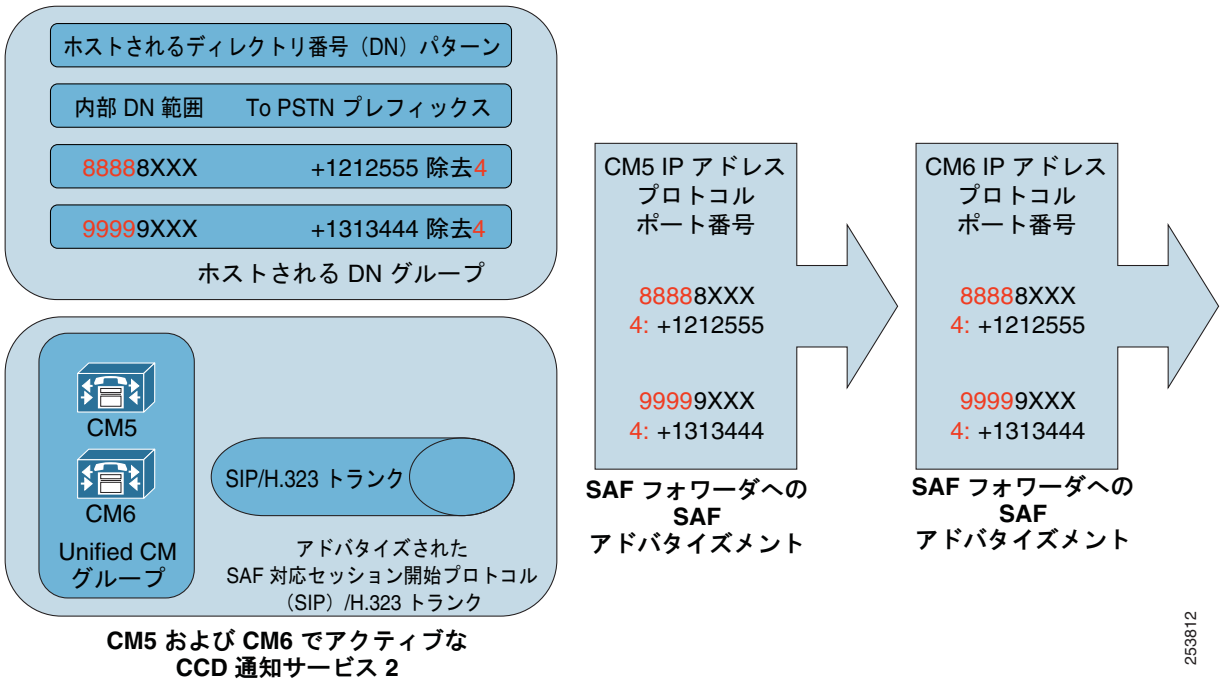
SIP トランクおよび H.323 トランクがそれぞれ異なる機能セットをサポートするため（たとえば、H.323 トランクは Annex M1 を介した QSIG をサポートします）、アドバタイズ サービスごとにトランク タイプを 1 つだけ選択するのが一般的です。H.323 トランクと SIP トランクの両方を選択すると、このアドバタイズ サービスに関連付けられたホスト DN 範囲へのコールがラウンドロビン方式で SIP トランクと H.323 トランクの両方に分散されます。

**図 5-23　CM1 と CM2 でアクティブな CCD アドバタイズ サービス 1**




Unified CM クラスタ内に複数のアドバタイズ サービスを作成できます。アドバタイズ サービスは、他のアドバタイズ サービスと同じ（か異なる）SAF 対応トランクを使用できます。ただし、各アドバタイズ サービスを一意のホスト DN グループに関連付ける必要があり、クラスタ内の複数のアドバタイズ サービスで同じホスト DN パターンをアドバタイズすることはできません。複数のアドバタイズ サービスを作成すると、着信コールを DN 範囲に従ってクラスタ内の複数のトランク サーバに分散させることができます （図 5-24 を参照）。

図 5-24　CM5 と CM6 でアクティブな CCD アドバタイズ サービス 2



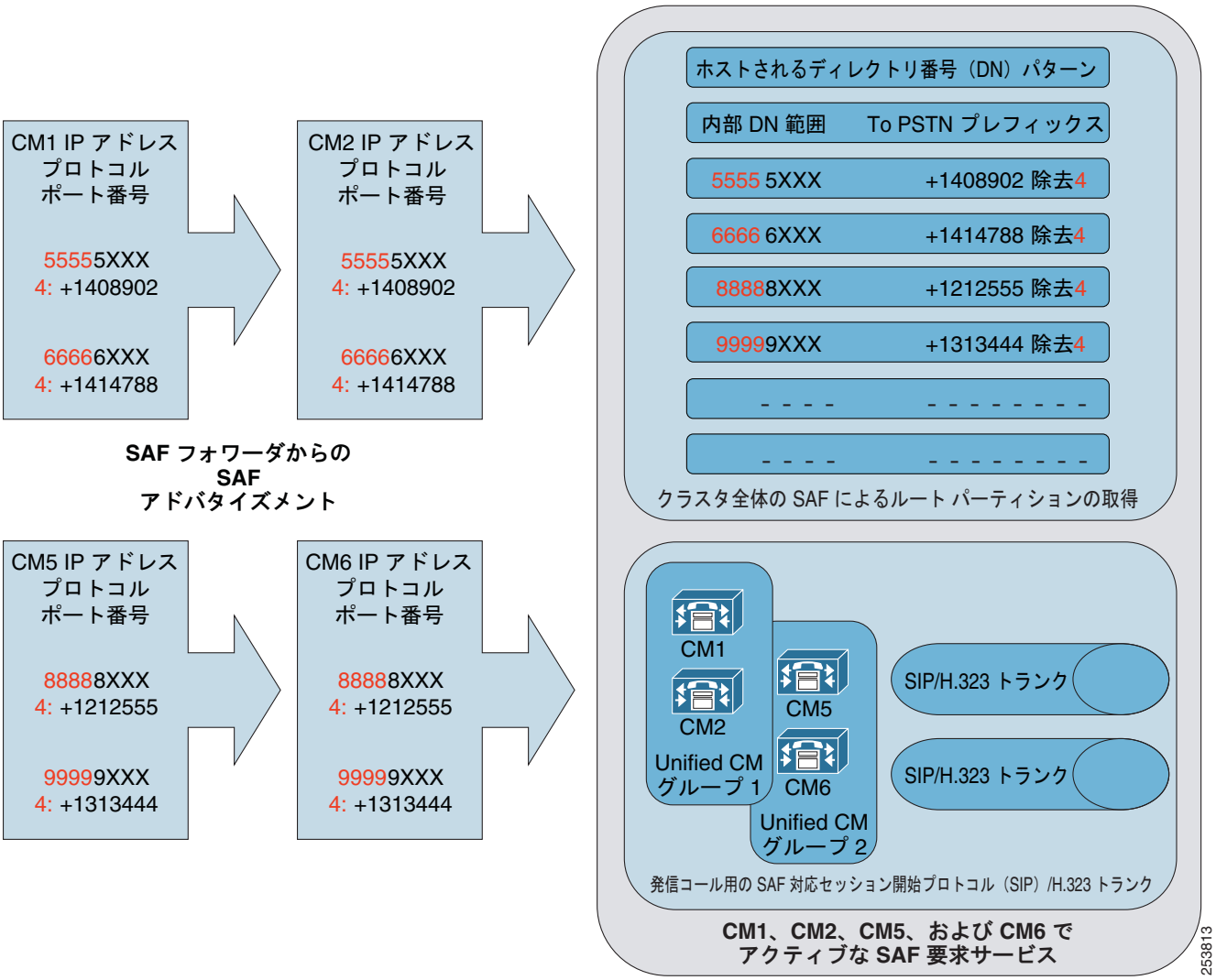

CM5 および CM6 でアクティブな CCD 通知サービス 2

### CCD 要求サービス

CCD 要求サービスは、SAF AS でアドバタイズされるホスト DN ルートに関する情報を収集して、SAF 学習ルート用のパーティションに配置します（図 5-25 を参照）。要求サービスは、発信 SAF コールを開始するのに使用する SAF トランクを選択するときにも使用されます。複数の SAF 対応トランクを選択できます。複数のトランクを選択した場合、発信コールに使用する SAF トランクとその対応する Unified CM Group サーバ ノードがラウンドロビン方式で選択されます。アドバタイズ サービスと同様に、要求サービスには通常同じプロトコル タイプのトランクを関連付けます。また、要求サービスは、学習した DN パターンや学習した「To PSTN」パターンに数字をプレフィックスとして付加できます。

Unified CM クラスタに要求サービスを 1 つだけ設定でき、その要求サービスは関連付けられた SAF トランクの Unified CM Group のすべてのノードでアクティブになります。

図 5-25　Unified CM CCD 要求サービス




## CCD 学習パターンのブロック

Unified CM を使用すると、SAF CCD 管理者は SAF CCD 学習ルート パーティションから学習ルート情報を消去およびブロックできます。次のエントリの 1 つ以上に一致するかどうかに基づいて、ルートをブロックできます。

- Learned Pattern（たとえば、500*X*）
- Learned Pattern Prefix（たとえば、+1408）
- Remote Call Control Entity Name（エンタープライズ パラメータでは、これは Unified CM クラスタ ID です）
- Remote Call Control IP Address（これは、Cisco IOS SAF CCD ルータまたは Unified CM クラスタ内の 1 つ以上の Unified CM サーバのアドレスです）

ここに挙げたエントリは、必要に応じて次のように論理 AND を組み合せて使用できます。

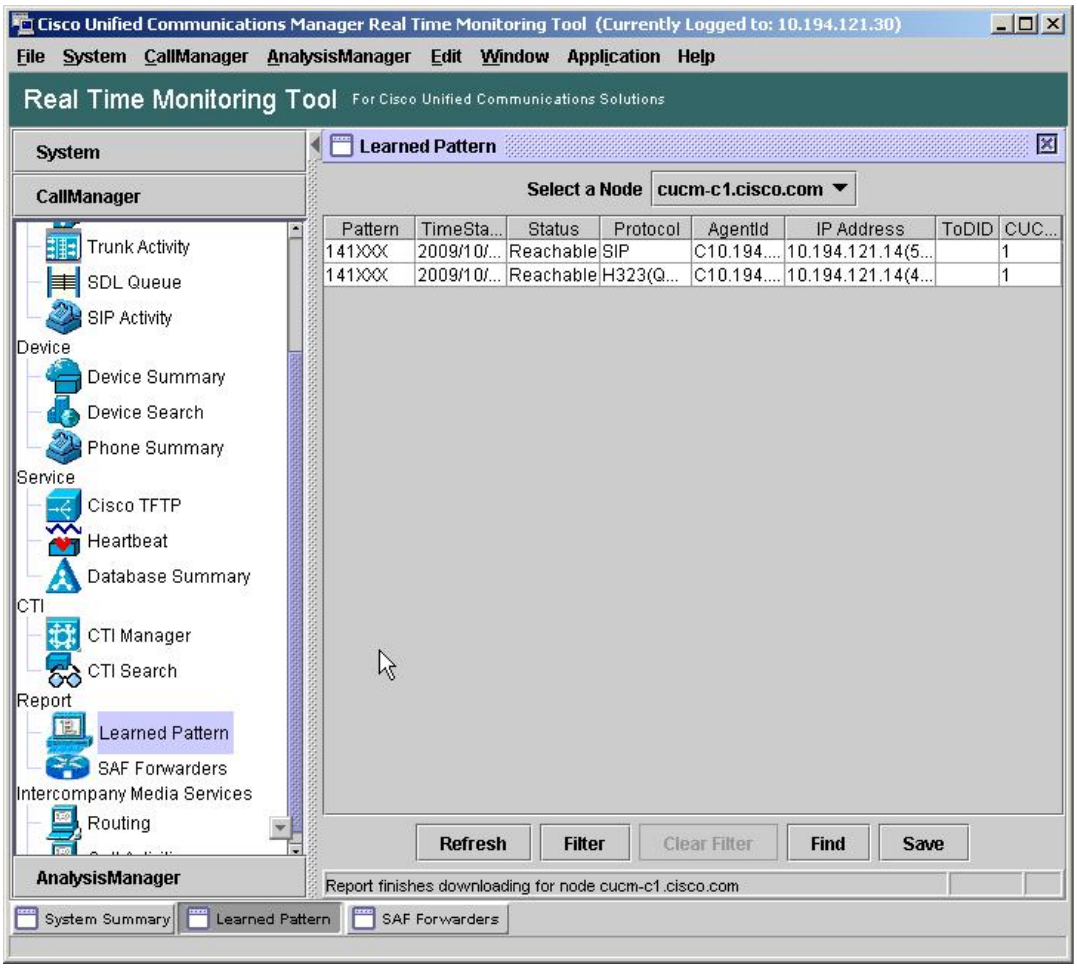
Pattern = "5XXX" AND Prefix = "+1408" AND Remote Call Control Address = "10.10.1.1"

CCD 学習パターンのブロックが特に有益なのは、SAF CCD 配置のうち、Unified CM クラスタが複数の SAF AS に接続していて、DN ルート情報を AS にアドバタイズしながら、その AS から送信される DN ルート情報の一部または全部を受信しないようにしたい場合です。

## Unified CM での SAF 学習ルートの表示

SAF 学習ルートは動的な性質があるため、Unified CM データベースには保持されませんが、メモリに格納されます。SAF 学習ルートを表示し、SAF フォワーダを監視するには、Cisco Unified Communications Manager Real-Time Monitoring Tool（RTMT）を使用します（図 5-26 を参照）。

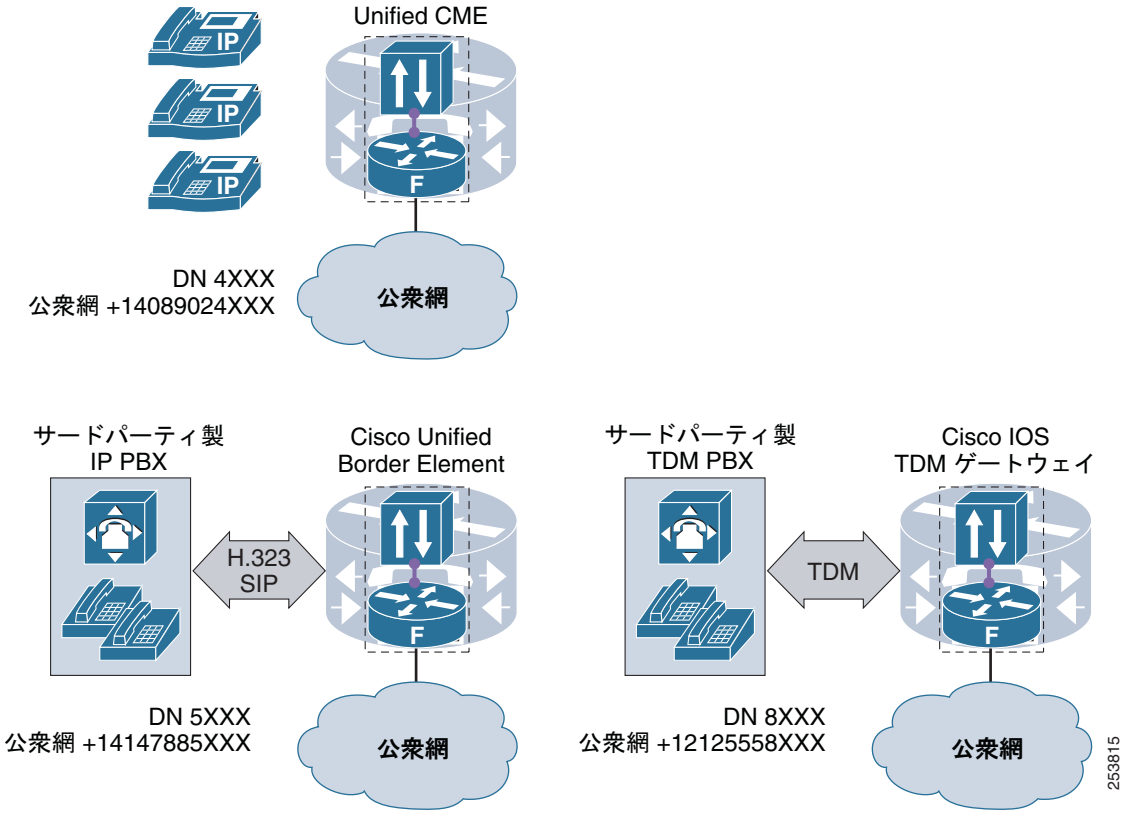
**図 5-26　SAF CCD 用 Real-Time Monitoring Tool（RTMT）**




## Cisco IOS-Based SAF CCD

Cisco IOS ベースの SAF CCD は、Cisco IOS Release 15.0(1)M を搭載した Integrated Services Router（ISR; サービス統合型ルータ）プラットフォーム上の Unified CME、SRST、Cisco Unified Border Element、および Cisco IOS ゲートウェイでサポートされます（図 5-27 を参照）。Cisco IOS SAF CCD の設定は、ここに挙げたどの製品でも同じです。ただし、SRST は CCD の特殊な事例であり、「SAF CCD と SRST」（P.5-76）の項で説明します。

図 5-27　Cisco IOS ベースの SAF CCD コール エージェント




Unified CME、Cisco IOS TDM ゲートウェイ、および Cisco Unified Border Element の場合、SAF CCD を使用すると、この各製品に関連付けられたエンドポイントの内部ディレクトリ番号範囲および「To PSTN」プレフィックスをアドバタイズできます。また、他の SAF CCD 対応呼制御アプリケーションから SAF アドバタイズメントをサブスクライブできます。

Cisco IOS と Unified CM のどちらの場合でも、SAF CCD を使用して外部公衆網の番号範囲（テールエンド ホップオフなど）をアドバタイズすることはお勧め *しません*。その主な理由は次のとおりです。

- SAF CCD は、IP、公衆網、または TDM トランクのキャパシティに関する情報を提供しません（たとえば、SAF CCD では、2 DS0 の ISDN BRI と 24 DS0 の T1 TDM インターフェイスが等しく重み付けされます）。
- すべての SAF CCD ルートが、単一のパーティションに配置されます。つまり、どの SAF CCD ユーザもすべての SAF CCD 学習ルートにアクセスでき、SAF CCD サービス クラスを作成することはできません。

Cisco IOS SAF CCD 設定の原則は Unified CM のものと同じですが、命名規則およびコマンドは異なります。

### 内部 SAF クライアント

Cisco IOS ベースの SAF CCD アプリケーションの場合、SAF クライアントおよびフォワーダは Cisco IOS 内に共存します。内部 SAF クライアントと内部 SAF フォワーダとの間で、設定および認証は必要ありません。

### 外部 SAF クライアント

Cisco IOS SAF フォワーダに対して外部 SAF クライアントの認証を有効にするには、**external-client** Cisco IOS コマンドを使用して、外部クライアントのラベルまたは基本名、ユーザ名、パスワード、およびキープアライブ タイマーを定義します。

## SAF 対応トランク

SAF トランクを定義するには、**profile trunk-route** Cisco IOS コマンドを使用します。トランクルート プロファイルでは、SAF トランクの IP アドレス、ポート番号、プロトコル（SIP または H.323）、および転送プロトコル（UDP または TCP）を定義します。

## DN パターン、DN ブロック、および DN サービス

Cisco IOS では、ディレクトリ番号、DN 範囲、および「To PSTN」プレフィックスの定義および設定が、Unified CM 設定と比較すると若干異なります。Cisco IOS は、DN ブロックという概念を採用して、DN 番号および DN 範囲をグループ化します。DN ブロックには、複数の DN パターンを含めることができます。番号の削除および先頭付加に関する「To PSTN」フェールオーバー規則も、DN ブロック コマンドラインで定義します。公衆網フェールオーバー規則は、Cisco IOS では **alias** と呼ばれます（公衆網フェールオーバー規則は、サイト コードおよび拡張 DN パターンを連結したものに適用されます）。DN ブロックの Cisco IOS 設定の例を次に示します。

```
profile dn-block 1 alias 1408902 strip 3
    pattern 1 extension 5xxx
    pattern 2 extension 6xxx
```

## 呼制御プロファイル、DN サービス、およびサイト コード

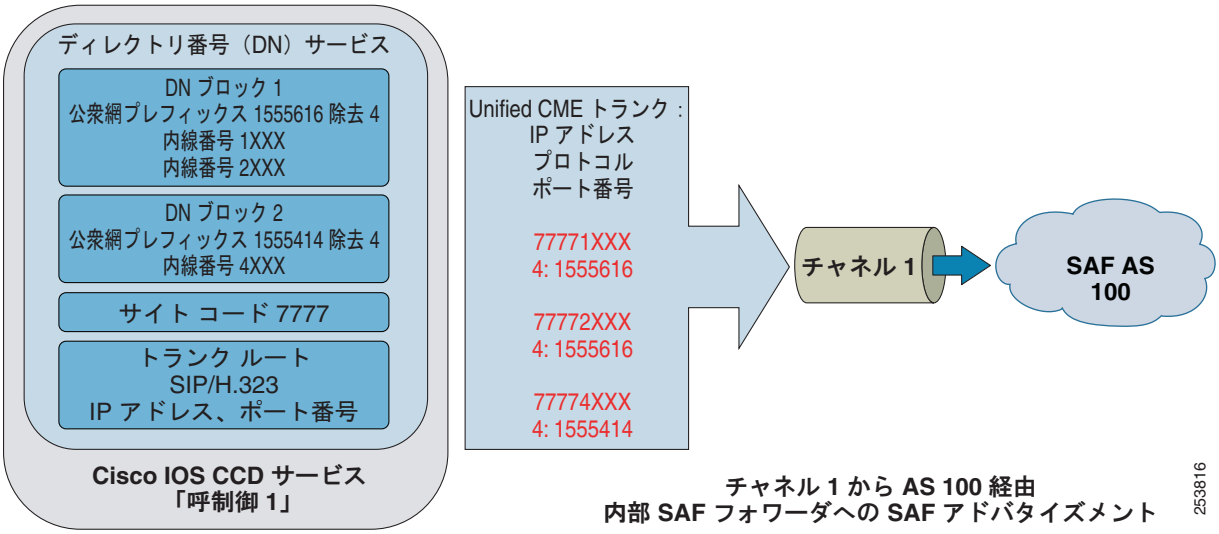
CCD 呼制御プロファイルは、DN サービスに関連付けられます。Cisco IOS の DN サービスは、Unified CM のアドバタイズ サービスと同等であると考えることができます。DN サービスは、1 つ以上の DN ブロック、1 つのトランク ルート、および 1 つのサイト コードをグループ化するために使用します。サイト コードが存在する場合、アドバタイズする拡張 DN パターンの先頭に付加される 1 つ以上の数字で構成されます。

複数の呼制御プロファイルを作成できます。同じ DN ブロック、トランク ルート、およびサイト コードを複数の呼制御プロファイルで再利用できますが、SAF AS に関連付けることができるプロファイルは 1 つだけです。

## SAF AS 内の SAF サービスの公開とサブスクライブ

呼制御プロファイルは、設定された SAF「チャネル」を利用して、自身に関連付けられた DN 範囲、「To PSTN」フェールオーバー規則、およびトランク ルートを 1 つの SAF AS にアドバタイズします。SAF チャネルは、1 つの呼制御プロファイルだけに含まれる CCD サービス情報を 1 つの SAF AS に公開できます （図 5-28 を参照）。

**図 5-28　チャネル 1 を介して SAF AS 100 にアドバタイズする Cisco IOS CCD サービス呼制御 1**




SAF チャネルは、ワイルドカード サービス ID を使用して、SAF AS 内のすべての CCD サービスをサブスクライブできます。また、SAF サービス ID のインスタンス値で特定した SAF CCD サービスを最大 2 つまでサブスクライブできます （Unified CM のインスタンス値はクラスタ PKID です）。次に例を示します。

ワイルドカード SAF サービス ID =

| サービス： | サブサービス： | インスタンス． | インスタンス． | インスタンス． | インスタンス． |
|---|---|---|---|---|---|
| 101: | 2: | FFFFFFFF. | FFFFFFFF. | FFFFFFFF. | FFFFFFFF. |

**ヒント**　ルータ上の Cisco IOS SAF CCD サービスのサービス ID を表示するには、Cisco IOS コマンド **show eigrp service-family ipv4** [*AS number*] **events** を使用します。サービス ID が「connected」（たとえば、101:2:59F8412.0.0.6F0100）と表示されます。

## Cisco IOS での発信 SAF CCD コール

Cisco IOS は、SAF を設定可能なセッション ターゲットとして標準の Cisco IOS 音声ダイヤル ピアに追加します。ダイヤル ピアには、標準と SAF のダイヤル ピアを選択する順序を制御するために、プリファレンス設定を割り当てることもできます。

## SAF CCD と SRST

SRST CCD は、SAF 配置の特殊なタイプです。SRST CCD は、番号範囲を SAF にアドバタイズしません。Unified CM や Unified CME など他の SAF CCD サービスからのアドバタイズメントを監視するだけです。SRST CCD は、SAF 学習 IP ルートを使用しません。公衆網ルートだけを使用し、ルータおよび関連付けられた電話機が SRST モードのときにだけ機能します。

SAF for SRST CCD を使用すると、新たに SRST ルータを Unified Communications ネットワークに追加するたびに、すべての SRST ルータを新しい番号拡張規則で更新するという非常に手間のかかるタスクを回避できます。

（SAF ではなく）標準の SRST の動作では、Unified CM が使用できなくなると、電話機が内線番号を SRST リファレンス ルータに登録します（図 5-29 を参照）。SRST モードでは、通常どおり内線番号をダイヤルして、SRST ルータに登録されている他の電話機にコールを発信できます。SRST モードの電話機を使用して別のサイトの電話機をコールするときは、着信側電話機の公衆網番号をダイヤルする必要があります（図 5-30 を参照）。Cisco IOS の番号拡張コマンドは SAF CCD の公衆網フェールオーバー規則とよく似ており、このコマンドを使用すると、ダイヤルした内線番号を SRST モードの完全な公衆網番号に拡張できます。

SRST ルータの数が多い Unified Communications 配置では、新たに SRST ルータを Unified Communications ネットワークに追加すると、すべての SRST ルータがこの新規 SRST サイトの公衆網アクセス プレフィックスに対応する番号拡張規則を追加する必要があります。

SAF for SRST CCD を使用すると、すべての SRST サイトの公衆網フェールオーバー規則を SAF AS 内のすべての SRST ルータに分散させることができます。

**図 5-29　SAF SRST CCD のある Unified CM 配置の通常の（Unified CM）動作**

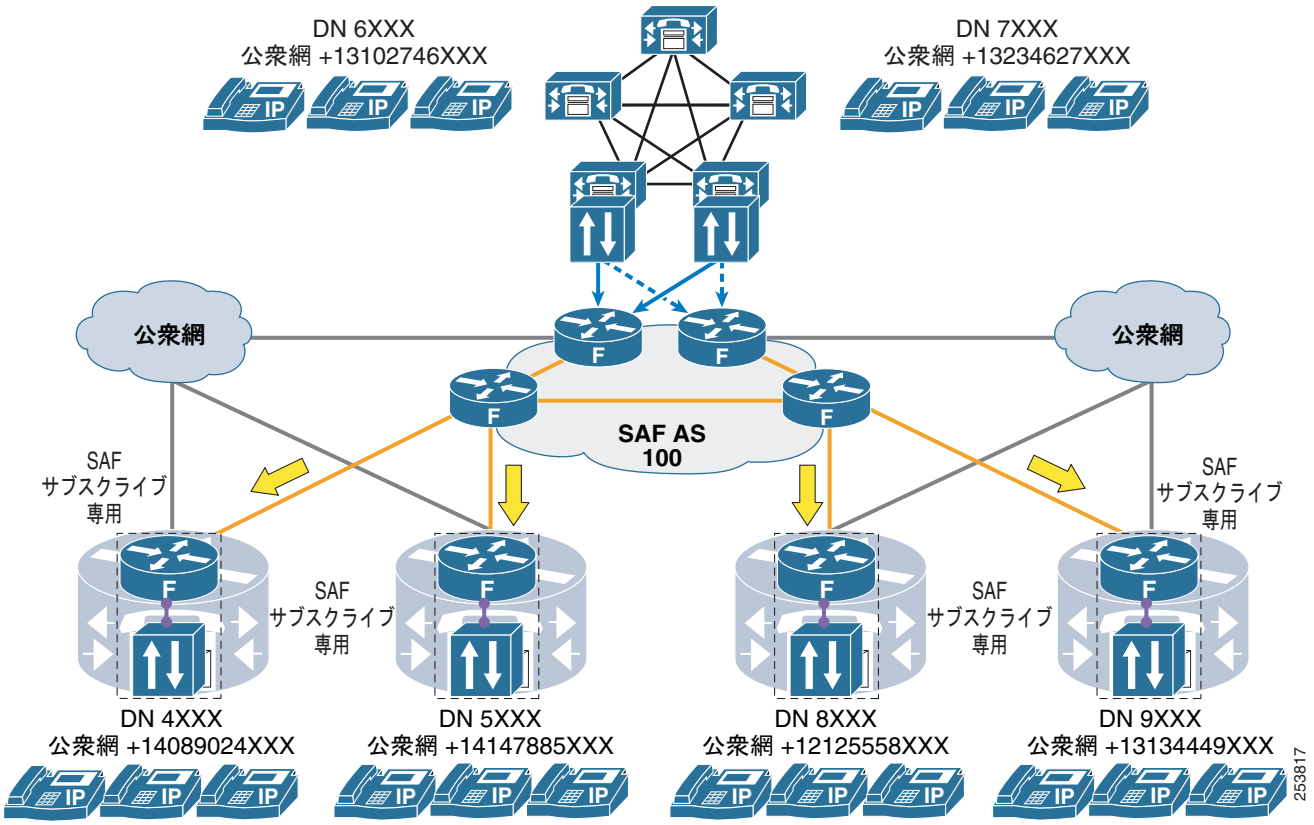
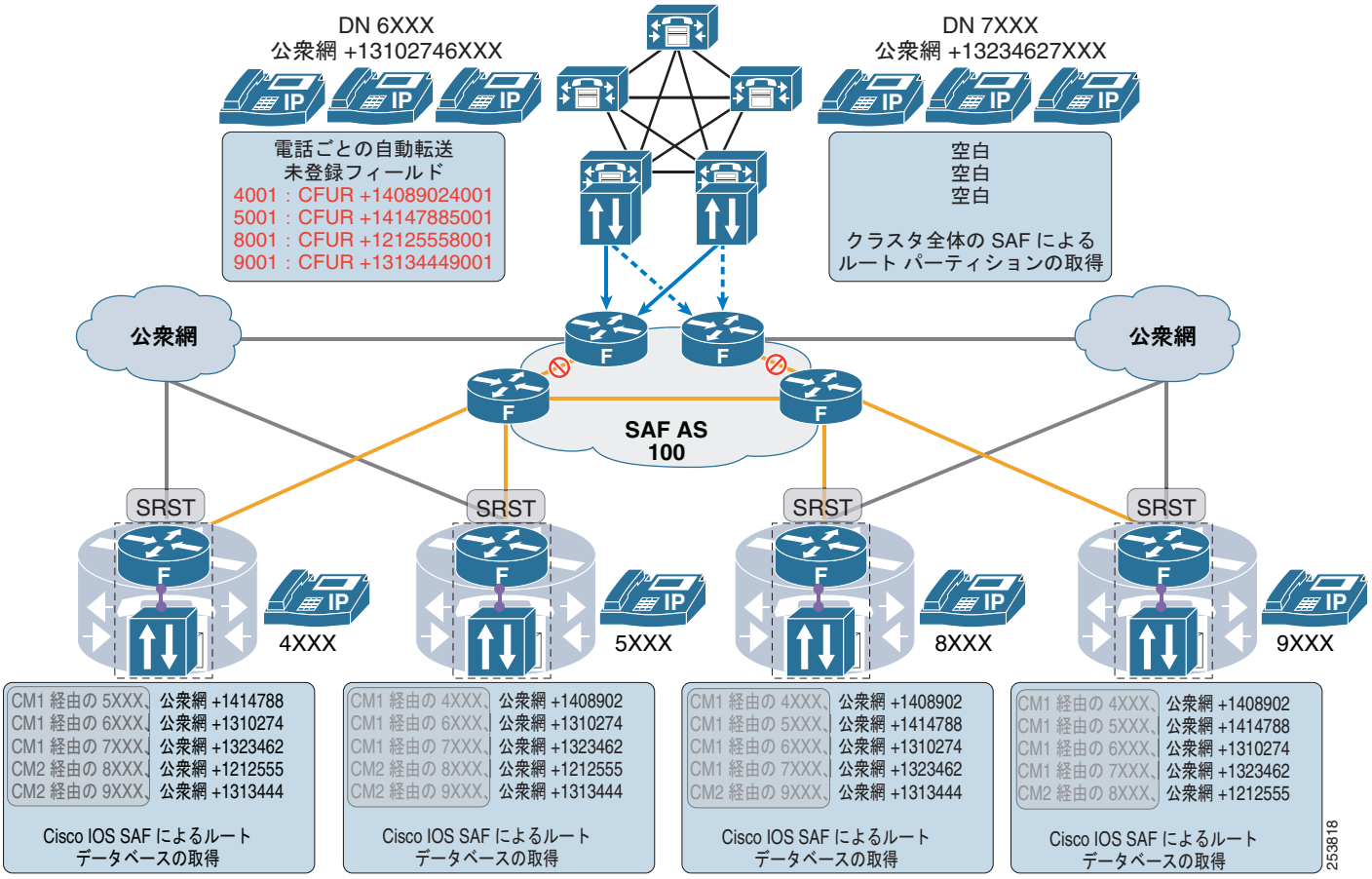


図 5-30　SAF SRST CCD のある Unified CM 配置の SRST 動作



## 代表的な SAF CCD ベースの Unified Communications 配置

図 5-31 に、代表的な SAF CCD ネットワーク配置を示します。

**図 5-31　リージョン コール エージェント、SAF クライアント、および SAF フォワーダのあるグローバル SAF ネットワーク**

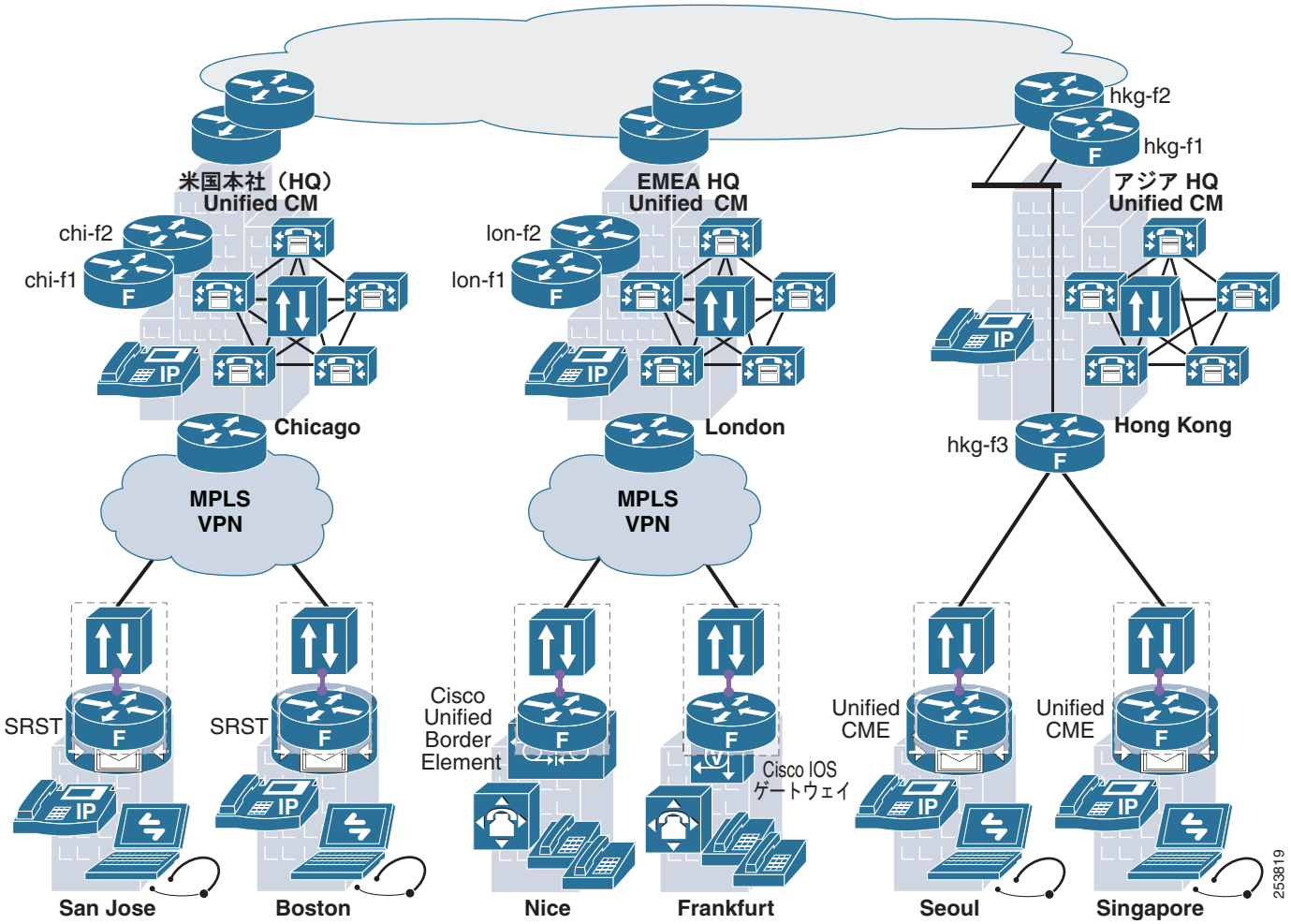
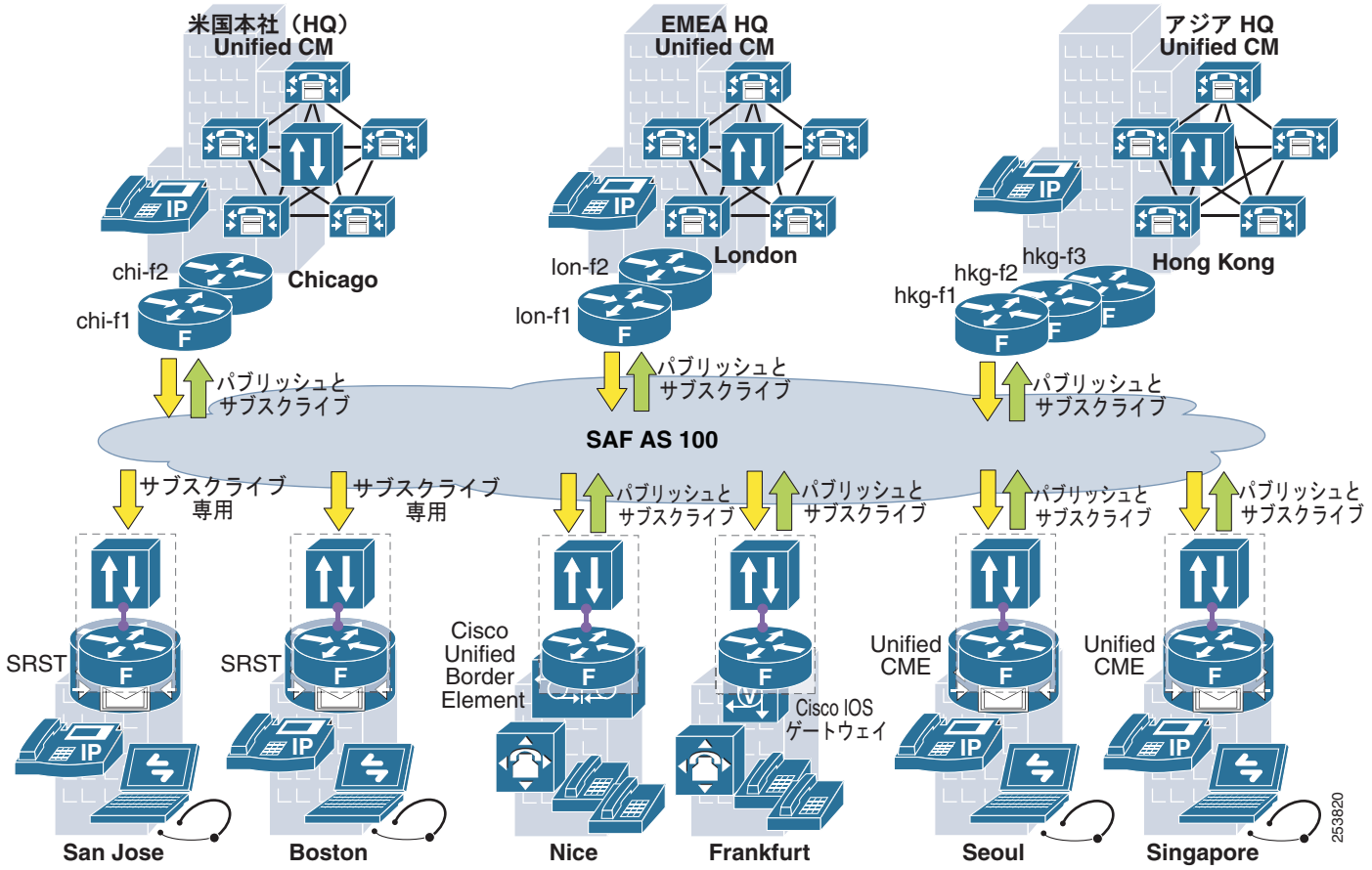



図 5-32 に、リージョン コール エージェント、SAF クライアント、および SAF フォワーダのある同じグローバル SAF ネットワークの論理図を示します。

図 5-32　リージョン コール エージェント、SAF クライアント、および SAF フォワーダのあるグローバル SAF ネットワークの論理図




# SAF CCD 配置の考慮事項

SAF CCD への移行は比較的リスクがありません。SAF を使用するデバイスをネットワークで有効にする前に、SAF CCD ネットワークを構築して基本的な動作およびスケーラビリティをテストできます。Unified CM ユーザは、SAF 学習ルート パーティションを自身のデバイスまたはプロファイルに追加することによって、SAF CCD ネットワークを使用できます。Cisco IOS では、標準のダイヤル ピアよりも SAF ダイヤル ピアのプリファレンスを優先させることができます。これにより、SAF をネットワーク全体で段階的に有効にできます。

次のスケーラビリティ制限が、Unified CM および Cisco IOS SAF CCD 製品に適用されます。

- アドバタイズする DN パターンは Unified CM クラスタあたり最大 2,000
- 学習する DN パターンは Unified CM クラスタあたり最大 20,000
- アドバタイズする DN パターンは Unified CME、Cisco Unified Border Element、または Cisco IOS ゲートウェイあたり最大 125
- 学習する DN パターンは Unified CME、Cisco Unified Border Element、Cisco IOS ゲートウェイ、または SRST あたり最大 6,000（プラットフォーム依存）

極めて大規模な SAF CCD ネットワークでは、複数の SAF AS を使用して、SAF がアドバタイズする DN パターンの配布を制限できます。Unified CM や Cisco Unified Border Element では、1 つの SAF AS からの SAF アドバタイズメントを手動で集約して、別の SAF AS に静的にアドバタイズすることもできます。

### SAF CCD ポート番号

SAF CCD は、次のポート番号を使用します。

- SAF EIGRP：IP プロトコル 88
- Unified CM SAF クライアントから Cisco IOS SAF フォワーダへの間 ：TCP ポート 5050（設定可能）
- アドバタイズする SIP トランク：ポート 5060
- アドバタイズする H.323：エフェメラル ポート番号

（注） Cisco Adaptive Security Appliance（ASA）ファイアウォールは、標準の SIP 検査およびフィックスアップを使用して、SAF 対応 SIP トランク コールの RTP メディア ストリームのためにファイアウォールのピンホールを開きます。SAF 対応 H.323 トランク コールの H.323 検査およびフィックスアップはサポートされません。