オンプレミス導入環境での Cisco Collaboration 12.0 エンタープライズ向け Cisco Collaboration 12.*x* Enterprise オンプレミス展開

シスコ検証済み（CVD）デザイン ガイド

改訂日：2019 年 2 月 19 日

Cisco Systems, Inc.
http://www.cisco.com/jp

Cisco は世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は
当社の Web サイトをご覧ください。
www.cisco.com/go/offices をご覧ください。

初版発行日：2014 年 10 月 28 日

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付されたインフォーメーション パケットに記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムに適応したものですここに掲載されているコンテンツの全ては、カ二フォル二ア大学に著作権がある。

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルに適用できるまたは適用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らせられても、それらに対する責任を一切負わないものとします。

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、www.cisco.com/go/trademarks でご確認いただけます。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」などの用語はシスコと他社とのパートナーシップという関係の意味ではありません。(1721R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジー図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2014-2019 Cisco Systems, Inc. 全著作権所有。

はじめに

改訂日：2019 年 2 月 19 日

Cisco Validated Design（CVD）は、一般的な使用事例や現在のシステム リリースに基づき、設計と導入に関する重要な決定事項について説明しています。CVD には、お客様のニーズに応えるための幅広いテクノロジー、機能、アプリケーションが組み込まれています。より迅速で信頼性が高く、完全に予測可能な導入を実現するために、シスコのエンジニアは CVD に含まれるガイドラインを包括的にテストした後、文書化しています。シスコのパートナーやお客様は CVD のテスト済みの成果を活用して、独自の設定と構成でシステムの設計 / 導入を開始できます。

エンタープライズ コラボレーションに関するドキュメント

『Cisco Preferred Architecture（PA）Design Overview』を活用すると、お客様およびセールス チームは組織のビジネス要件に基づいて適切なアーキテクチャを選択し、アーキテクチャ内で使用される製品について理解し、設計上の一般的なベスト プラクティスを習得することができます。これらの資料はセールス プロセスを支援します。

『Cisco Validated Design（CVD）』資料は、シスコ推奨アーキテクチャを導入する手順について詳しく説明しています。これらの資料はプリファード アーキテクチャの計画、設計、および実装を支援します。

『Cisco Collaboration System Solution Reference Network Design（SRND）』資料は、Cisco Collaboration の設計上のオプションについて詳しく説明しています。設計上の要件がシスコ推奨アーキテクチャの適用範囲を超える場合には、SRND を参考にしてください。

このマニュアルについて

企業のコラボレーション向けシスコ プリファード アーキテクチャに関するこの『Cisco Validated Design』の対象読者は次のとおりです。

- コラボレーション ソリューションの販売、設計、導入に携わるセールス チーム
- Cisco Collaboration を導入するための設計上のベスト プラクティスと適切な手順について詳しい情報を必要とされているお客様とセールス チーム

このガイドは、読者の皆様がシスコの音声、ビデオ、コラボレーション製品に関する一般的な知識があり、それらの製品の導入方法の基本を理解していることを前提としています。この CVD 資料をお読みになる前に、Preferred Architecture for Cisco Collaboration（Cisco が推奨するコラボレーション用アーキテクチャ）12.*x* オンプレミス導入、設計概要を参照してください。

この CVD に掲載されている設計上の決定事項は、『Cisco Collaboration SRND』の最新版に記載されたフレームワークに沿ったものです。SRND には設計上および導入上のさまざまなオプションが提示されていますが、本資料では、プリファード アーキテクチャ デザインの基本想定に基づいて 1 つの推奨導入が選択されています。想定が異なると、設計上の決定も異なる可能性があり、その場合は SRND に照らして確認する必要があります。独特の要件と高度なカスタマイズを備えた大規模な導入環境では、シスコ アカウント マネージャと連絡を取り、この CVD および SRND の適用範囲を超えるガイドラインを得ることをお勧めします。

本資料は、次のような方法で設計および販売のプロセスをシンプルにします。

- 『 Preferred Architecture for Cisco Collaboration 12.*x* On-Premises Deployments, Design Overview』にある製品および設計に関する推奨事項に基づく
- 『Cisco Preferred Architecture Design Overview』
- コラボレーション アーキテクチャについて詳しく説明し、ベスト プラクティスを明示し、これらの推奨事項の根拠を示します

この CVD ガイドは次に示す個別のモジュールで編成され、これらが総合的にコラボレーション ソリューションを構成します。

- コール制御 — ダイヤル プラン設計、コンピュータ テレフォニー インテグレーション（CTI）、Survivable Remote Site Telephony（SRST）、IM and Presence、LDAP ディレクトリ統合、SIP トランク、その他のコール制御機能の概念を示します。また、この章では、企業のコラボレーション向けのプリファード アーキテクチャでコール制御を導入するうえでのベスト プラクティスも紹介します。
- 会議 — 企業のコラボレーション向けのプリファード アーキテクチャで使用可能なさまざまな種類の会議と、会議機能を導入する方法について説明します。
- コラボレーション エッジ — リモート登録サービス、外部通信、および相互運用性を提供する Cisco Collaboration Edge コンポーネントの導入方法を説明します。
- ボイス メッセージング — 企業のコラボレーション向けのプリファード アーキテクチャで使用可能なさまざまなアプリケーションと導入ツールについて紹介し、ユニファイド メッセージングおよび会議スケジュール用の 2 つのコア アプリケーションについて詳しく説明します。
- サイジング — お客様の導入環境の要件に合わせて企業のコラボレーション向けのプリファード アーキテクチャ コンポーネントの規模を決定するための簡単な例を示します。

マニュアルの変更履歴

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

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

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

C：表 1は、このマニュアルの改訂履歴を示しています。

C：表 1　　このCVDガイドの改訂履歴

改訂日	説明
2019年1月23日	このドキュメントは、Cisco Collaboration System Release（CSR）12.5向けに更新されました。詳細については、各章の「*この章の新規情報とは*」*を参照*してください。
2017年8月30日	Cisco Collaboration System Release（CSR）12.0向けにこのマニュアルが更新されました。詳細については、各章の「*この章の新規情報とは*」*を参照*してください。

マニュアルの入手方法およびテクニカルサポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html から入手できます。

「*What's New in Cisco Product Documentation*」に配信登録すると、新しい（または改訂された）シスコ技術情報のリストがRSSフィードとして提供され、リーダーアプリケーションを使ってコンテンツがデスクトップに直接配信されるようにすることができます。RSSフィードは無料のサービスです。

表記法

このマニュアルでは、次の表記法を使用しています。

太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。

string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

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

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

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

ワンポイント アドバイス　「*時間の節約に役立つ操作*」です。記述されている操作を実行すると時間を節約できます。

警告　**安全上の重要な注意事項**

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

これらの注意事項を保存しておいてください

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

はじめに

改訂日：2019 年 2 月 19 日

このわずか数年の間に、ビジネスの境界を超えてコミュニケーションの強化とコラボレーションの拡大を実現する多くの新しいコラボレーション ツールが市場に投入されました。組織がコラボレーション アプリケーションから得ているビジネスの付加価値は、従業員の生産性向上とお客様との関係強化です。コラボレーション分野の著しい進化により、導入の簡素化、相互運用性の向上、ユーザ エクスペリエンスの全体的な改善が実現しました。

現在のコラボレーション ソリューションでは、ビデオ、音声、そして Web による参加者を一元的な会議環境に統合することが可能になっています。この Cisco Validated Design（CVD）ガイドに含まれるガイドラインは、コラボレーション アーキテクチャ全体を考慮して記載されています。内容をより適切に編成する目的で、サブシステムが使用されています。また、サブシステムの推奨事項をテストし、これらのサブシステムの推奨事項が、関連サブシステムの推奨事項と一致していることを確認しています。

この章の新規情報とは

C：表 1-1 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。

C：表 1-1　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 Prime License Manager を Cisco Smart Software Manager に置き換える	C：表 1-2	2017 年 8 月 30 日
追加した Cisco Webex Room シリーズ エンドポイント	C：表 1-3	2017 年 8 月 30 日

アーキテクチャの概要

このエンタープライズ コラボレーション向けプリファード アーキテクチャの CVD は、Cisco Collaboration ポートフォリオの全製品のうち、エンタープライズ市場セグメントに最適な製品で構成されます。このプリファード アーキテクチャ導入モデルはすぐに使える規範的な導入モデルで、組織とそのビジネス ニーズの変化に対応できる拡張性を備えています。この規範的なアプローチでは、複数のシステムレベルのコンポーネントを簡単に統合でき、組織がそれぞれのビジネス ニーズに最適な機能、サービス、キャパシティを選択できます。

このエンタープライズ コラボレーション向けプリファード アーキテクチャの CVD は、ユーザ数が 1,000 人を超える導入環境に対応したエンドツーエンドのコラボレーションを実現します。これよりも小規模な導入環境の場合は、『Preferred Architecture Design Overview and CVDs for Midmarket Collaboration』を参照してください。

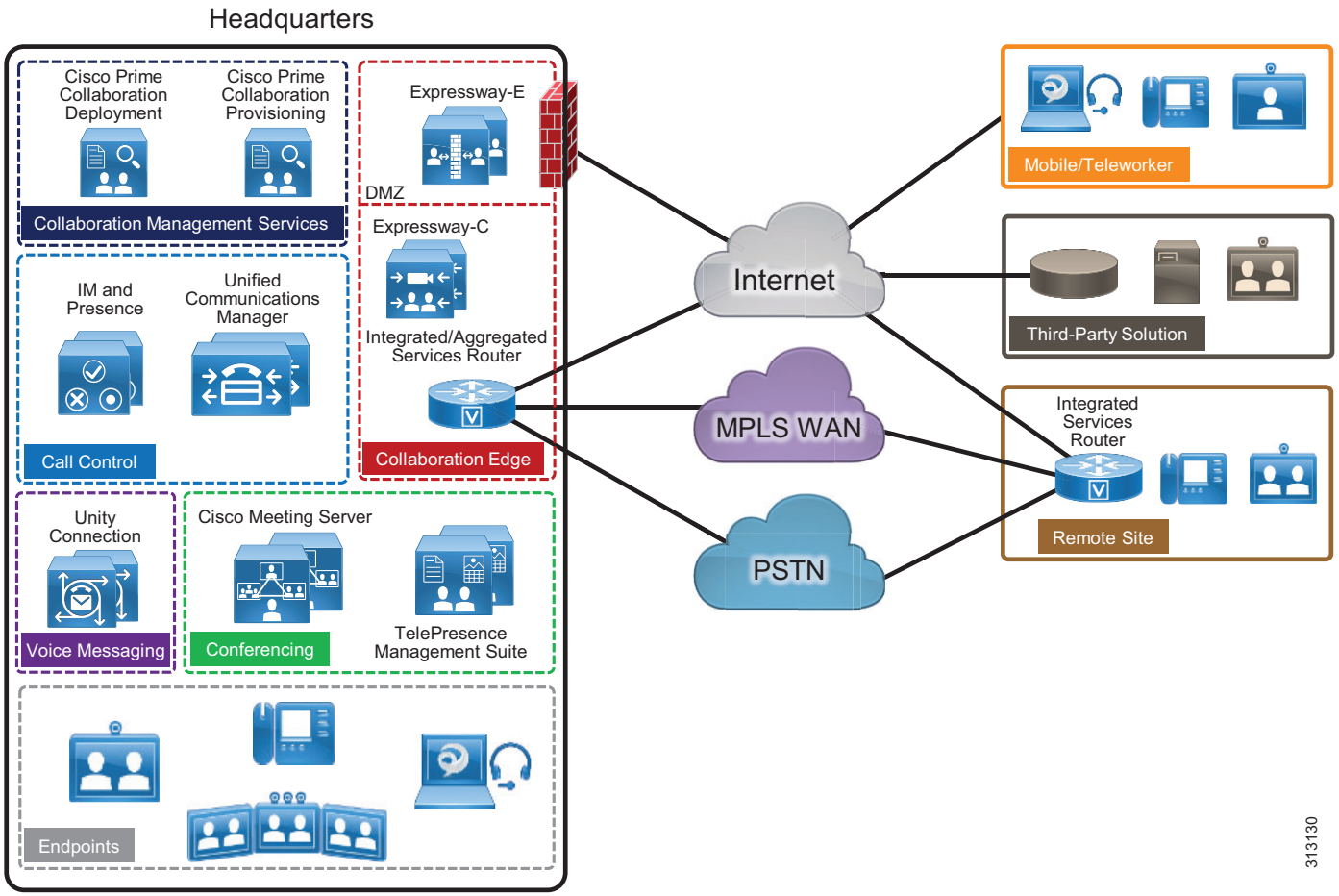
このエンタープライズ コラボレーション向け推奨アーキテクチャの CVD では、重要なアプリケーションの高可用性を実現します。このアーキテクチャは次の主要なサービスを通じてモバイル ワーカー、パートナー、お客様に拡張できる、高度なコラボレーション サービスをサポートします。

- 音声コミュニケーション
- インスタント メッセージおよびプレゼンス
- 高精細度ビデオおよびコンテンツ共有
- リッチ メディア会議機能
- モバイル ワーカーやリモート ワーカーへの対応
- 企業間（B2B）音声 / ビデオ通信
- ユニファイド ボイス メッセージング

シスコのエンドポイントは適応性が高く、IP ネットワークをサポートしているため、このアーキテクチャを導入すれば、組織が現行データ ネットワークを使用して音声通話とビデオ通話の両方に対応できます。このプリファード アーキテクチャでは、帯域幅管理についての包括的なアプローチを採用しています。ここにはエンドツーエンドの QoS アーキテクチャ、コール アドミッション制御、ビデオ レート アダプテーション メカニズム、および復元力メカニズムが組み込まれており、マネージド ネットワークでもアンマネージド ネットワークでもパーベイシブ ビデオの展開に最適なユーザ エクスペリエンスを提供します。

エンタープライズ コラボレーション向けシスコ プリファード アーキテクチャは、C：図 1-1 に示すように、可用性とセキュリティを備えた集中管理型のサービスを提供します。これらのサービスはリモート オフィスや移動の多い社員に容易に拡張でき、本社との通信が失われた場合でも重要なサービスの可用性を提供できます。これは、新たな導入環境を設計する場合や既存の導入環境を拡大する場合のベースとなる基本アーキテクチャとして理解しておく必要があります。推奨アーキテクチャの進展に伴い、製品やソリューションが追加され、このアーキテクチャは拡大します。

C：図 1-1　エンタープライズ コラボレーション向けシスコ推奨アーキテクチャ



C：表 1-2 に、このアーキテクチャで使用されている製品を示します。製品の分類と役割定義がしやすいように製品をモジュールに分けて記載しています。この CVD の内容はこのモジュールと同じ構成になっています。

C：表 1-2　エンタープライズ コラボレーション向けシスコ推奨アーキテクチャのコンポーネント

モジュール	コンポーネント	目的
コール制御	Cisco Unified Communications Manager（Unified CM） Cisco Unified Communications Manager IM and Presence Service Cisco Integrated Services Router（ISR）	コール制御は、ユーザとエンドポイントに対し、登録、呼処理、リソース管理、およびインスタント メッセージおよびプレゼンスの機能を提供します。また、リモート オフィスのリモート サイト耐障害性も備えています。
会議	Cisco Meeting Server Cisco TelePresence Management Suite（TMS） Cisco Webex Software as a Service（クラウド）	会議では、3 者以上が音声、ビデオ、およびコンテンツ共有によりリアルタイムで通信できます。リソースをオンプレミスに配置することも、クラウドでホストすることもできます。

C：表 1-2　エンタープライズ コラボレーション向けシスコ推奨アーキテクチャのコンポーネント（続き）

モジュール	コンポーネント	目的
コラボレーション エッジ	Cisco Expressway-C Cisco Expressway-E Cisco Integrated Services Router（ISR） Cisco Aggregation Services Routers (ASR)	コラボレーション エッジは、リモート登録サービス、外部通信、相互運用性を提供します。
ボイス メッセージング	Cisco Unity Connection	Cisco Unity Connection は、ユニファイド メッセージングとボイスメール サービスを提供します。
コラボレーション管理サービス	Cisco Prime Collaboration Deployment	Cisco Prime Collaboration Deployment は、ユニファイド コミュニケーション アプリケーションの管理を支援します。以前のバージョンのクラスタ ソフトウェアから新しい仮想マシンへの移行、新規インストール、既存のクラスタでのアップグレードなどのタスクを実行できます。
	Cisco Smart Software Manager	簡略化された全社的なライセンス管理を提供するインター ネット ベースの Web ポータルです。Cisco Smart Software Manager を使用すると、管理者は展開内の Cisco Unified CM ライセンスと Cisco Unity Connection ライセンスを一括管理できます。
	Cisco Prime Collaboration Provisioning	Cisco Prime Collaboration プロビジョニングは、システム設定、ユーザとデバイスのプロビジョニング、および簡略化された移動 / 追加 / 変更を行うためのテンプレート ベースの集中型コンソールを備えており、コラボレーション システムの迅速な設定を可能にします。
セキュリティー	すべてのコンポーネント	セキュリティ：デフォルトで有効になるセキュリティ機能から、展開で推奨されるセキュリティ機能に至るまで、さまざまな機能が組み込まれています。セキュリティ機能の例には、このソリューション内のすべてのコンポーネントに関する不正アクセス防止、料金詐欺行為防止、証明書の生成と管理、および暗号化のプロビジョニングと有効化が含まれます。

C：表 1-2 エンタープライズ コラボレーション向けシスコ推奨アーキテクチャのコンポーネント（続き）

モジュール	コンポーネント	目的
帯域幅管理	このドキュメントのすべての章に記載されているネットワーク インフラストラクチャと製品	帯域幅管理には、エンドツーエンドの QoS アーキテクチャ、コール アドミッション制御、ビデオ レート アダプテーション メカニズム、および復元力メカニズムが組み込まれており、マネージド ネットワークでもアンマネージド ネットワークでもパーベイシブ ビデオの展開に最適なユーザ エクスペリエンスを提供します。
サイジング	このマニュアルのすべての章に記載されている製品 仮想マシン配置ツール（VMPT）	このマニュアルで説明するすべてのモジュールのサイジングと、仮想マシンの配置の例。

ネットワーク サービス

エンタープライズ コラボレーション向けプリファード アーキテクチャでは、構造化されて可用性と回復力が高いネットワーク インフラストラクチャ、およびドメイン ネーム システム（DNS）、DHCP（Dynamic Host Configuration Protocol）、TFTP（Trivial File Transfer Protocol）、ネットワーク タイム プロトコル（NTP）を含むネットワーク サービスの統合セットが必要です。シスコのアプリケーションおよびエンドポイントでこれらの基本ネットワーク サービスがどのように使用されるかについて、詳しくは『Cisco Collaboration SRND』の「*Network Services*」の項を参照してください。

仮想化

複数のアプリケーションを仮想化して物理サーバ上で統合することで、コストを節約し、ラック スペースを最小限に抑え、所要電力量を削減し、導入と管理を簡素化できます。仮想化は、組織で変更が必要になる際のハードウェアの再導入とソフトウェア アプリケーションのスケーリングにも対応します。

Cisco Unified Computing System（UCS）上の Cisco Unified Communications

Cisco UCS サーバは、ユニファイド コミュニケーション（UC）コア アプリケーションを使用して十分なテストが行われており、仮想環境で信頼性と一貫したパフォーマンスを実現することが確認されています。UC アプリケーションを UCS サーバに導入するには 2 つのオプションがあります。

- UCS テスト済みリファレンス構成（TRC）の UC

  UCS TRC は、UCS サーバ コンポーネントの特定のハードウェア構成です。これらのコンポーネントには、CPU、メモリ、ハード ディスク（ローカル ストレージの場合）、RAID コントローラ、および電源などがあります。特定の TRC については、『Collaboration Virtualization Hardware』の Web サイトを参照してください。

- UCS ベースの UC

  UCS ベースのハードウェア構成では、UC アプリケーションの検証は明示的に実施されていません。したがって、UC アプリケーションが UCS ベースのハードウェアにインストールされる場合に、UC アプリケーション仮想マシンのパフォーマンスの予測や保証は行わ

れません。この場合、シスコはガイダンスのみを提供します。プリセールスでのハードウェア設計によって、UC アプリケーションが必要とするパフォーマンスを実現できるかどうかの確認は、お客様の責任で行っていただきます。

『Cisco Collaboration Virtualization』のすべてのルールに準拠している限り、このどちらのオプションも Cisco Technical Assistance Center（TAC）で完全にサポートされます。

Cisco Business Edition 7000（BE7000）

Cisco BE7000 は、仮想ハイパーバイザとアプリケーション インストール ファイルがプリインストールされており、すぐに利用できる状態で出荷される仮想化 UCS 上に構築されています。BE7000 は、UCS TRC であり、UC アプリケーションが特定の UCS 設定で明示的にテストされています。Cisco BE7000 ソリューションは、1 つの統合プラットフォーム上で、高度な音声、ビデオ、メッセージ、インスタント メッセージおよびプレゼンス、およびコンタクト センターの各機能を提供します。Cisco BE7000 について詳しくは、『Cisco Business Edition 7000 Solutions Data Sheet』を参照してください。

コア アプリケーション

エンタープライズ コラボレーション向け推奨アーキテクチャでは、ハードウェアとソフトウェアの冗長性を提供するため、次の仮想化アプリケーションが複数の Cisco UCS サーバに導入されます。

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager IM and Presence Service
- Cisco Unity Connection
- Cisco Expressway（Expressway-C および Expressway-E で構成）
- Cisco Meeting Server
- Cisco TelePresence Management Suite

重要なビジネス アプリケーションの可用性を最大限に引き出すため、常に冗長構成で導入することを推奨します。

コラボレーション エンドポイント

この CVD ガイドでの推奨事項は、シスコの音声 & ビデオ エンドポイント（Cisco Jabber などのソフト クライアントを含む）を前提としています。これらのエンドポイントは SIP を使用して Cisco Unified Communications Manager（Unified CM）に登録します。C：表 1-3 に、最適な機能とユーザエクスペリエンスを実現するための推奨エンドポイントを示します。

C：表 1-3　　Cisco Collaboration Endpoints

製品	説明
モバイル： • Android 向けの Jabber • iPhone/iPad 向けの Jabber **デスクトップ：** • Mac 向けの Jabber • Windows 向けの Jabber	音声、ビデオ、ボイスメール、インスタント メッセージ、およびプレゼンス機能を統合し、モバイル デバイスとパーソナル コンピュータのためのセキュア エッジ トラバーサルを備えたソフト クライアント。
Cisco IP Phone 8800 シリーズ	パブリック スペース、一般オフィスでの使用、単一回線と複数回線、および音声 / ビデオ電話機
Cisco IP Phone 8832	IP 会議用電話
Cisco Webex DX 80	デスクトップ向けパーソナル TelePresence エンドポイント
Cisco MX シリーズ	多目的ルーム向け TelePresence エンドポイント
Cisco SX シリーズ	インテグレータシリーズテレプレゼンスエンドポイント
Cisco Webex Room シリーズ	コラボレーション統合機能および多目的ルーム エンドポイント

コール制御

改訂日：2019 年 2 月 19 日

この章では、Enterprise Collaboration 向けの Cisco Preferred Architecture（PA）のコール制御機能について説明します。

展開に際して、PA 設計ガイドラインおよび推奨事項以外の特定の要件が課せられることがあります。その場合は *Cisco Collaboration SRND* や関連する製品のマニュアルなど、他のマニュアルを使用しなければならない場合があります。

この章の最初の部分では、アーキテクチャについて概説し、いくつかの基本的な設計概念を紹介します。2 番目の部分では、展開に関する考慮事項についてより詳しく説明します。アーキテクチャの項では、冗長の概念、高可用性、コンピュータ / テレフォニー インテグレーション（CTI）、IM and Presence のアーキテクチャなどのトピックについて解説し、本書の例で使用される架空のカスタマー トポロジを紹介します。この章の中心となるのは 展開の概要 の項です。概念の抽象的な説明よりも、このセクションで紹介されている展開例を見れば、特定の設計に関する決定の背景について、より明確に理解できるようになります。展開の概要 の項で取り上げているトピックとしては、DNS 要件、クラスタ プロビジョニング、証明書の管理、ダイヤル プラン設定、LDAP を使用したユーザ プロビジョニング、メディア リソース、SIP トランクの考慮事項、エンドポイント プロビジョニング、マルチクラスタの考慮事項などがあります。展開の概要 の項でのトピックの順番は、推奨される設定順になっています。

この章の新規情報とは

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

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

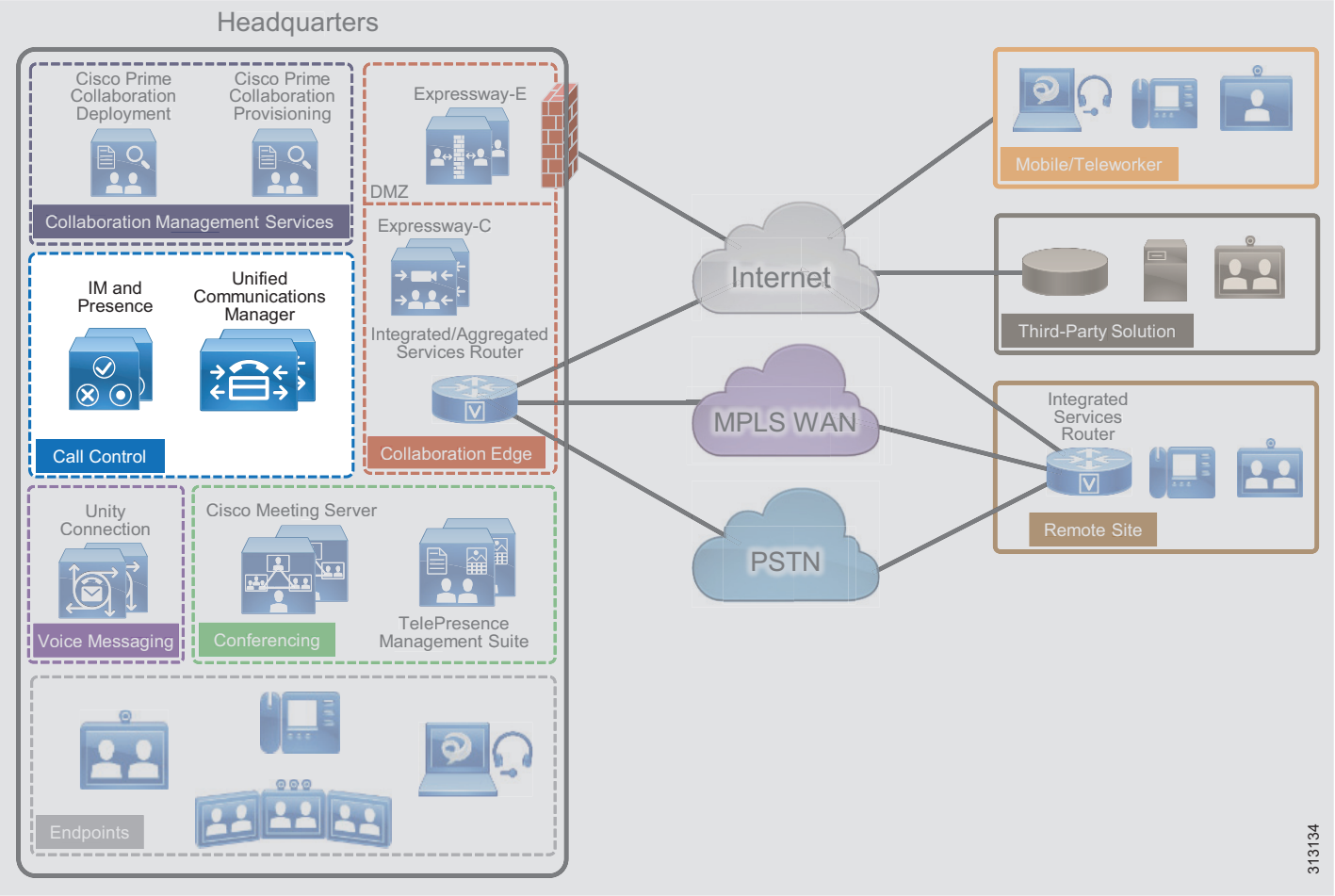
新規トピックまたは改訂されたトピック	説明箇所	改訂日
Apple Push Notification Service（APN）に関する情報を追加	アップル　プッシュ　ノーティフィケーション サービス（APN）との統合（C：2-10 ページ） Apple Push Notification Service（APN）経由のプッシュ通知のオンボーディング（C：2-26 ページ） その他の IM とプレゼンス設定（C：2-27 ページ）	2017 年 8 月 30 日
更新ログイン フローを使用した OAuth	その他の IM とプレゼンス設定（C：2-27 ページ） C：表 2-2	2017 年 8 月 30 日

コア コンポーネント

コア アーキテクチャには次の重要な要素が含まれています（C：図 2-1）

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager IM and Presence Service
- Cisco Integrated Services Router（ISR）

C：図 2-1　　プリファード アーキテクチャの概要



主なメリット

- コール制御が 1 か所で集中管理され、そこから複数のリモート サイトが制御されます。
- 操作と管理が一元化されます。
- 一般的なテレフォニー機能がどの音声エンドポイント、ビデオ エンドポイントでも使用できます。
- 音声エンドポイントおよびビデオ エンドポイントのために単一のコール制御および統合されたダイヤル プランが提供されます。
- 重要なビジネス アプリケーションの可用性が高くなり、冗長化されます。

アーキテクチャ

音声コールとビデオ コールの処理は、企業のコミュニケーション システムによって提供される重要な機能です。この機能は、特定のタイプの呼処理エンティティまたは呼処理エージェントによって処理されます。呼処理の操作は重要であるため、ユニファイド コミュニケーションの配置を設計して、呼処理システムが、必要なユーザ数およびデバイス数を処理するのに十分なスケーラビリティと、ネットワークおよびアプリケーションのさまざまな異常または障害を処理するのに十分な復元性を持つようにすることが重要です。

この章では Cisco Unified Communications Manager（Unified CM）および Survivable Remote Site Telephony（SRST）を使った、スケーラブルで復元性の高い呼処理システムを設計するためのガイダンスを行います。集中型 Unified CM クラスタはすべてのカスタマー サイトに対して呼処理サービスを実装します。集中型 Unified CM クラスタの一部である Unified CM IM and Presences Service はエンタープライズに対してインスタント メッセージとプレゼンス サービスを実装します。Cisco Survivable Remote Site Telephony（SRST）は、企業 WAN の信頼性が音声サービスの可用性要件を満たさない場合に、リモート サイトに対してバックアップ サービスを実装するために使用されます。

Cisco Unified CM は、小規模～非常に大規模な単一サイト配置、マルチサイト集中型呼処理配置、およびマルチサイト分散呼処理配置に、呼処理サービスを提供します。Unified CM は Cisco Collaboration ソリューションの中核をなし、音声、ビデオ、IM and Presence、メッセージング、モビリティ、Web 会議、およびセキュリティを提供する基盤として機能します。

VPN や Cisco Expressway などのさまざまなコラボレーション エッジ ソリューションを通して、インターネットから Enterprise Collaboration ネットワークおよび Unified CM にアクセスして、リモート アクセスおよび business-to-business のセキュアなビデオ コミュニケーションを可能にすることもできます。

Unified CM の役割

Cisco Unified CM はすべての Cisco Collaboration 展開における中央のコール制御コンポーネントです。Unified CM は、コール制御、エンドポイントの登録、エンドポイントの設定、コール アドミッション制御、コーデック ネゴシエーション、トランク プロトコル変換、CTI などの基盤サービスを提供します。Unified CM は、管理とプロビジョニングの中心です。会議メディア リソース、ゲートウェイ、およびその他のコンポーネントを含む、すべてのコンポーネントへのアクセスを Unified CM が調整できるように、これらのコンポーネントに対するすべての SIP トランクは Unified CM で終端します。コール ルーティングは Unified CM に適用されるダイヤル プラン設定により制御されます。

IM と Presence Service の役割

Cisco Unified CM IM and Presence Service はオンプレミスのインスタント メッセージおよびプレゼンスを提供します。各種標準に基づく XMPP を使用するほか、SIP IM プロバイダとの相互運用のために SIP もサポートしています。Cisco Unified CM IM and Presence Service はオンプレミス ソリューションです。もう 1 つの Cisco インスタント メッセージおよびプレゼンス サービスである Cisco Webex Messenger はクラウドベースのサービスであり、このマニュアルでは取り上げません。

SRST の役割

低速な、または信頼できない WAN リンクにより集中型呼処理プラットフォームから隔てられた支社のロケーションに Cisco デスク フォンを展開する場合、ローカル呼処理の冗長化を検討することが重要です。各支社のロケーションで集中型呼処理プラットフォームへの接続が失われた場合は、そこにある Cisco IOS ルータで Survivable Remote Site Telephony（SRST）を利用することにより、デスク フォンの基本的な IP テレフォニー サービスを維持できます。ただし、デバイスが SRST に登録された場合に使用可能な一連の対ユーザ機能は、電話が Unified CM に登録された場合よりもずっと少なくなります。

存続可能リモートサイトテレフォニー（SRST）を使用した統一された CM の冗長性

Cisco IOS SRST は、Unified CM クラスタから離れたロケーションにあるエンドポイントに、可用性の高い呼処理サービスを提供します。Unified CM クラスタリングの冗長性方式は、LAN または MAN 環境内の呼処理などのアプリケーション サービスには高レベルの冗長性をもたらします。一方で、WAN などの低速リンクによって中央の Unified CM クラスタから分離されたリモート ロケーションの場合、冗長性方式として SRST を使用することにより、リモート サイトと中央サイトの間でネットワーク接続が失われたときに、基本的な呼処理サービスをこれらのリモート ロケーションに提供できます。呼処理サービスが重要であり、Unified CM クラスタへの接続が失われた場合にも呼処理サービスを維持する必要がある各リモート サイトには、SRST 対応の Cisco IOS ルータを配置することを推奨します。これらのリモート ロケーションのエンドポイントは、Unified CM 内の適切な SRST リファレンスとともに設定する必要があります。Unified CM サブスクライバへの接続を使用できない場合に、呼処理サービス用にどのアドレスを使用して SRST ルータに接続するかをエンドポイントが認識するようにするためです。

統一された CM と IM とプレゼンスサービスのクラスタリング

Unified CM はクラスタリングの概念をサポートしています。Unified CM アーキテクチャにより、サーバ ノード グループは単一の呼処理エンティティとして連携できるようになります。このサーバ ノード グループをクラスタと呼びます。

Cisco Unified CM にはパブリッシャとサブスクライバの 2 種類のノードがあります。

- Unified CM パブリッシャ

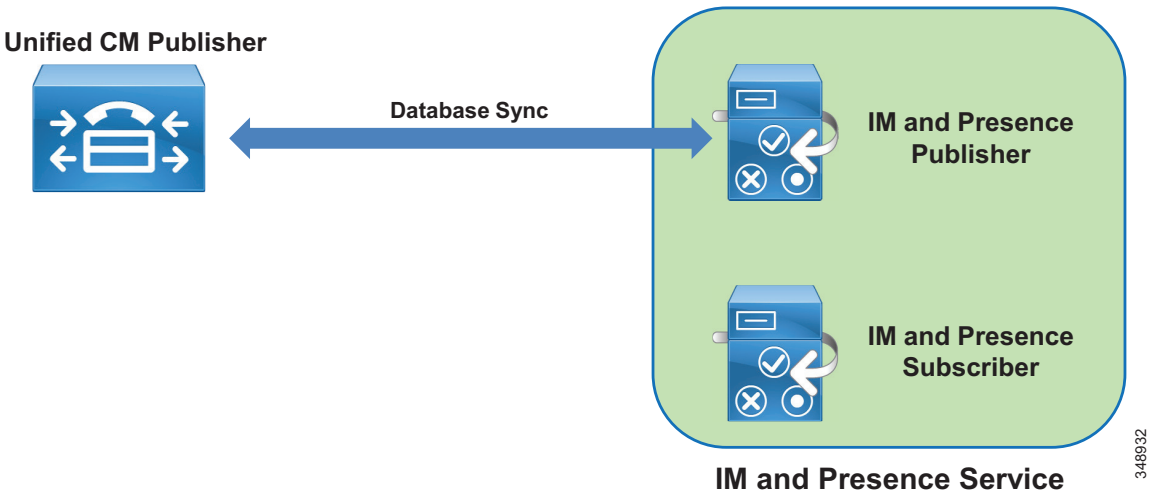
  パブリッシャはすべてのクラスタの必須サーバ ノードです。各クラスタにパブリッシャは 1 つだけ存在できます。このサーバ ノードにはクラスタ設定が含まれており、クラスタ内の他のすべてのサブスクライバにデータベース サービスを提供します。この設計では Unified CM パブリッシャは専用ノードなので TFTP 要求やエンドポイントの登録、呼処理は扱いません。

- Unified CM サブスクライバ

  サブスクライバ ノードは、パブリッシャにサブスクライブして、データベース情報のコピーを取得します。たとえば、サブスクライバ ノードには Unified CM TFTP ノードや Unified CM 呼処理サブスクライバ ノードなどがあります。

Cisco IM and Presence ノードには同じクラスタリングの概念があります。最初の IM and Presence ノードは IM and Presence パブリッシャです。その他の IM and Presence ノードは IM and Presence サブスクライバで、IM and Presence パブリッシャからデータベースのコピーを取得します。IM and Presence パブリッシャは Unified CM パブリッシャと通信を行い、大半の IM and Presence 設定は実際には Unified CM パブリッシャにより行われます（Unified CM ユーザ、プレゼンス ユーザが利用できる UC サービス、サービスのアクティブ化など）。このため、IM and Presence パブリッシャをはじめとするすべての IM and Presence ノードは、より大きな Unified CM and IM and Presence Service クラスタのサブスクライバであると見なされます。C：図 2-2 に Unified CM パブリッシャと 2 つのノードを持つ IM and Presence クラスタの関係を示します。

C：図 2-2　　Unified CM と 2 つのノードを持つ IM and Presence クラスタとの関係



高適用性

Unified CM および IM and Presence ノードは高可用性インフラストラクチャで展開する必要があります。たとえば、二重化電源の使用と無停電電源（UPS）の使用を組み合わせると、電力の可用性が最大になります。ネットワーク面から見ると、プラットフォーム サーバは複数の上流側のスイッチに接続する必要があります。

また、Unified CM システムおよび IM and Presence システムは、アプリケーション レベルでも高可用性処理を行います。

この設計の Unified CM では、冗長化のために 2 つの TFTP サーバを配置する必要があります。呼処理ノードは一対一（1:1）の冗長性をもって配置する必要があります。つまり、それぞれのプライマリ呼処理サブスクライバについてバックアップ呼処理サブスクライバがあります。この 100%:0% 冗長化設計は 50%:50% 冗長化設計に比べ、Unified CM グループおよびデバイス プールが少なくてすむ、冗長化オプションが少ないのでデバイス設定と配布が簡素化されるなど、多くの利点があります。

Cisco IOS Survivable Remote Site Telephony（SRST）は Unified CM クラスタから離れたロケーションにあるエンドポイントに対して、WAN リンクがダウンしたときに高可用性のある呼処理を提供します。

個々の Cisco IM and Presence ノードはサブクラスタでグループ化されます。1 つのサブクラスタは 1 つないし 2 つのノードを持つことができます。サブクラスタで 2 番目のノードを追加すると、高可用性が提供されます。高可用性が推奨されるため、この設計では各サブクラスタが 2 つのノードで構成されています。2 つのノードを持つサブクラスタでは、サブクラスタの 1 つのサーバに関連付けられたユーザは、フェイルオーバー イベントが発生した場合に、そのサブクラスタのもう一方のサーバを自動的に使えるようになります。各ノード ペアで 2 つのノード間のユーザ割り当てのバランスをとることが推奨されます。IM and Presence パブリッシャは、他の IM and Presence サブスクライバとまったく同じように、プレゼンス クライアントからの IM and Presence 情報を処理し、IM and Presence サブクラスタの 2 つのノードの 1 つとして配置されます。

コンピュータ テレフォニー インテグレーション（CTI）

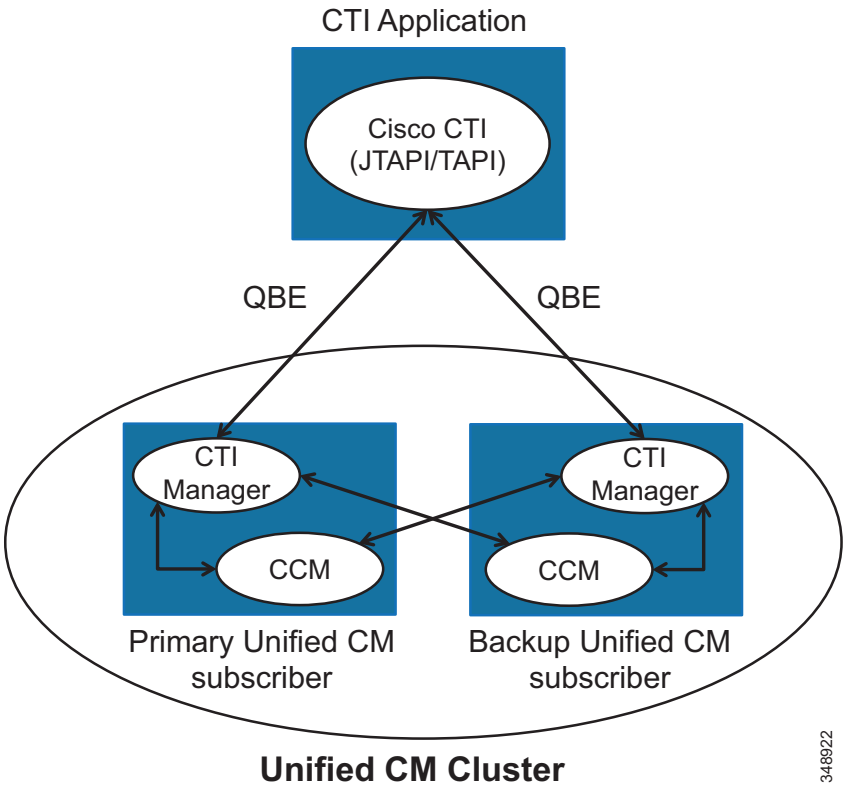
Cisco コンピュータ テレフォニー インテグレーション（CTI）を利用すると、Cisco Unified CM で使用可能な豊富なフィーチャ セットを、サードパーティ製のアプリケーションでも使用できるようになります。

CTI のアーキテクチャー

Cisco CTI は、次のコンポーネントで構成されます（C：図 2-3 を参照）。これらは互いに対話し、Cisco Unified CM で使用可能なテレフォニーフィーチャ セットを各アプリケーションで利用できるようにします。

- CTI アプリケーション：特定のテレフォニー機能を提供するために作成されたシスコまたはサードパーティのアプリケーション。このアプリケーションは JTAPI または TAPI インターフェイスを使用できます。CTI アプリケーションと Unified CM との間のプロトコルは Quick Buffer Encoding（QBE）です。
- 次のサービスを持つ Unified CM サブスクライバ：
  - CCM：Cisco CallManager サービス。テレフォニー処理エンジンです。
  - CTI Manager（CTIM）：プライマリまたはセカンダリ モードで動作する 1 つ以上の Unified CM サブスクライバで実行され、Cisco IP デバイスを制御およびモニタできるようにテレフォニー アプリケーションを認証および許可するサービス。

C：図 2-3　　CTI のアーキテクチャ



高適用性

CTI Manager の高可用性は、プライマリ CTI Manager に障害が発生した場合にバックアップ CTI Manager Service に接続することができる、CTI アプリケーションに依存します。プライマリ Unified CM サブスクライバの CTI Manager と CCM サービスの両方に障害が発生した場合（プライマリ Unified CM サブスクライバ全体に障害が発生した場合など）、バックアップ Unified CM サブスクライバで実行されている CCM と CTI Manager サービスの両方がアクティブ化され、CTI Manager サービスは同じバックアップ Unified CM サブスクライバ上にある CCM サービスに登録されている各デバイスを監視し、制御します。プライマリ CTI Manager Service に障害が発生したものの、プライマリ CCM Service はまだ実行中の場合（1:1 冗長化がプライマリ / バックアップ Unified CM サブスクライバの 100 %/0 % 分散で実現されている場合）、すべてのデバイスはそのままプライマリ Unified CM サブスクライバ上で実行されている CCM Service に登録されたままになり、バックアップ Unified CM サブスクライバで実行されている CTI Manager がアクティブ化されて、別のノード（この場合はプライマリ Unified CM サブスクライバ）で実行中の CCM サービスに登録されている CTI デバイスであってもそれらを監視し、制御します。

CTI のキャパシティー　プランニング

3 種類の CTI リソースについての次のキャパシティの上限を超えないようにしてください。

- 所定の CTI Manager インスタンス（CTI Manager サービスを実行している Unified CM ノード）に接続される CTI アプリケーションの最大数。CTI サーバベースのアプリケーションではこの数は通常少ないのですが、デスクフォン モードの Jabber クライアントなど、CTI クライアントベースのアプリケーション（この場合は各 Jabber クライアントが CTI アプリケーションと見なされます）では、多数の Jabber クライアントを展開する場合にこの上限を超えないようにすることが重要です。
- 所定の Unified CM 呼処理サブスクライバに登録される CTI 対応エンドポイントの最大数。
- 1 つの CTI Manager インスタンスによって監視され、制御される CTI 対応エンドポイントの最大数。Unified CM ノードで実行される CTI Manager サービスは、その Unified CM ノードに登録されたエンドポイントだけを監視するのが理想的です。しかし CTI Manager サービスが他の Unified CM ノードに登録されたエンドポイントを監視することも可能です。

CTI の上限は上記の 3 つの CTI リソースすべてで同じです。CTI のキャパシティの上限は OVA テンプレートの種類によって異なります。CTI の上限に達したら、CTI Manager サービスを実行する別の Unified CM 呼処理ノードのペアを配置します。

IM とプレゼンスのアーキテクチャー

Cisco Unified CM IM and Presence Service はオンプレミスのインスタント メッセージおよびプレゼンスを提供します。このソリューションの主要なプレゼンス コンポーネントは IM and Presence Service です。これには Extensible Communications Platform（XCP）が組み込まれ、ユーザの在籍ステータスとコミュニケーション手段に関する情報を収集する SIP/SIMPLE および Extensible Messaging and Presence Protocol（XMPP）をサポートしています。ユーザの在籍ステータスは、ユーザが電話機などの通信デバイスをアクティブに使用しているかどうかを示します。

アプリケーション（シスコ製またはサードパーティ製）にプレゼンスを統合することによって、エンド ユーザ エクスペリエンスと効率性を向上させるサービスを提供できます。さらに、Cisco Jabber はインスタント メッセージングとプレゼンス ステータスも統合した IM and Presence Service の対応クライアントです。

IM and Presence Service は Cisco Unified Computing System（UCS）プラットフォーム上の Unified CM で使用されるのと同じ基本アプライアンス モデルおよびハードウェアを使用します。

IM and Presence Service は IM and Presence クラスタとして展開されます。IM and Presence クラスタは最大 6 つのノードで構成されます。1 つのノードはパブリッシャとして指定され、最大 5 つのノードがサブスクライバ ノードになります。統一された CM と IM とプレゼンスサービスのクラスタリングおよび高適用性の項で説明されているように、IM and Presence ノードはサブクラスタでグループ化され、各サブクラスタは高可用性を得るために 2 つのノードで構成されます。サイジングの項で説明されているように、1 つのサブクラスタを展開すると、最大 15,000 人のユーザをサポートできます。IM and Presence パブリッシャは IM and Presence サブスクライバとまったく同じように IM and Presence 要求を処理するので、最初のサブクラスタは IM and Presence パブリッシャと 1 つの IM and Presence サブスクライバで構成されます。

統一された CM と IM とプレゼンスサービスのクラスタリングの項で説明されているように、IM and Presence ノードはより大きな Unified CM and IM and Presence Service クラスタの一部と見なされます。

統一された CM と IM とプレゼンスサービスラスターの展開

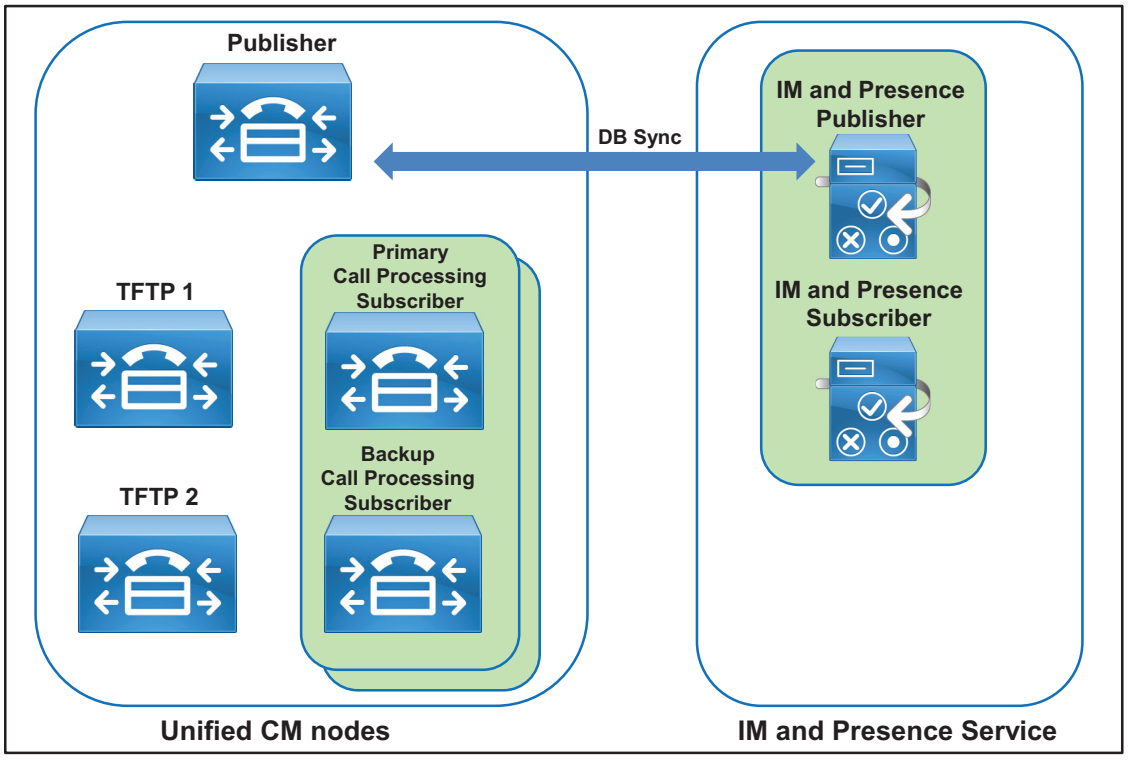
Cisco Unified CM and IM and Presence Service クラスタは次のノードで構成されます。

- 1x Cisco Unified CM パブリッシャ
- 2x（1 ペア）Cisco Unified CM TFTP サーバ サブスクライバ
- 2x（1 ペア）Cisco Unified CM 呼処理サブスクライバ（拡張のためにペアを追加）
- 2x（1 ペア）Cisco Unified IM and Presence ノード（拡張のためにペアまたはサブクラスタを追加）

拡張のために追加する Unified CM 呼処理および IM and Presence のペア数については、サイジングの章で説明します。

C : 図 2-4 は、最大 10,000 台のデバイスおよび 10,000 人のユーザを持つ Unified CM and IM and Presence Service クラスタ展開の例です。サイジング情報の詳細については、サイジングの章を参照してください。

C : 図 2-4　　Unified CM and IM and Presence Service クラスタの展開



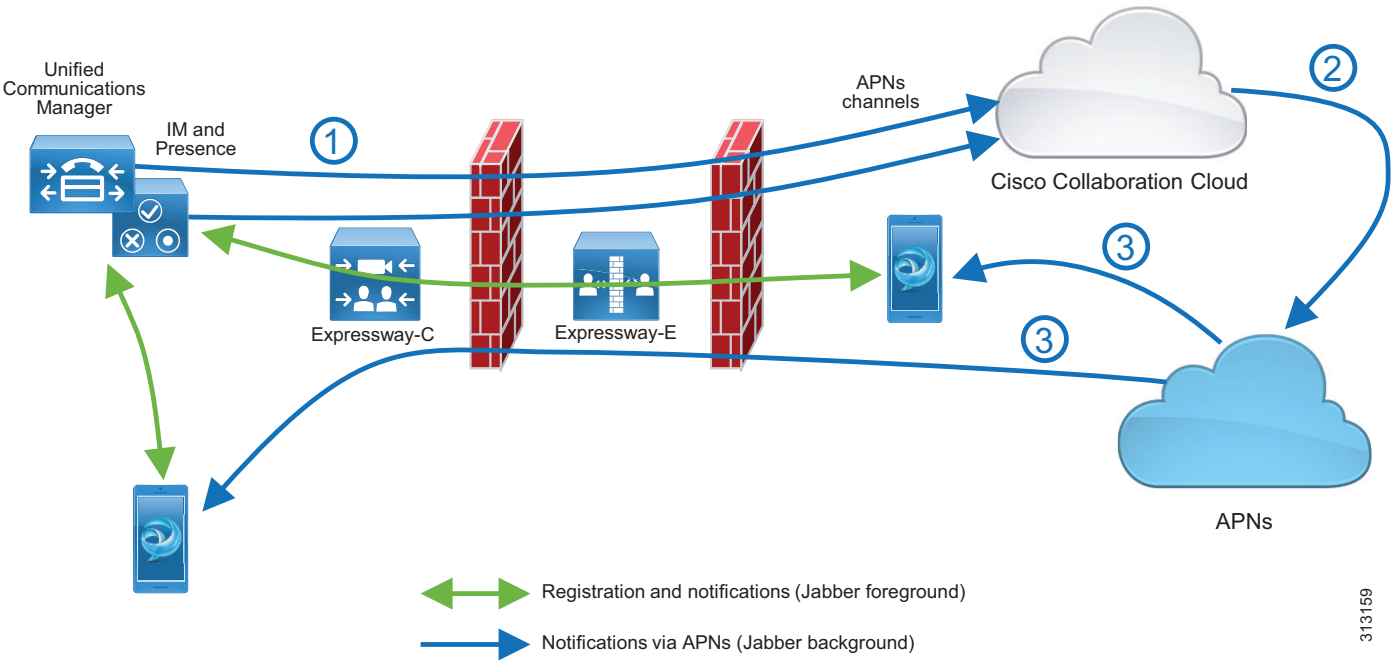
Unified CM with IM and Presence Service

アップル　プッシュ　ノーティフィケーション　サービス（APN）との統合

Unified CM および Unified CM IM and Presence Service の展開を Apple Push Notification Service（APN）に統合すると、Apple のクラウドベースのプッシュ通知サービスを使用して、音声 / ビデオ コールに関する通知とインスタント メッセージを、バックグラウンドで動作する Cisco Jabber for iPad and iPhone クライアントに配信することができます。Cisco Jabber クライアントは起動時に、社内ネットワーク上に存在する場合は Unified CM に直接登録し、社内ネットワークの外部から接続する場合はモバイルおよびリモート アクセス（MRA）を使って Cisco Expressway 経由で Unified CM に登録します。Cisco Jabber クライアントがフォアグラウンド モードで動作している限り、コールと IM 通知が Unified CM または Unified CM IM and Presence Service から直接受信されます。Cisco Jabber クライアントが中断モード (バックグラウンド) に移行するとすぐに、通知を直接受け取るこの方式から Apple Push Notification に移行します。バックグラウンドの Cisco Jabber クライアントは、Apple Push Notification が Apple iOS で受信されるとすぐにアクティブになります。その後、Cisco Jabber が Unified CM および Unified CM IM and Presence Service との直接通信を再度アクティブにします。このメカニズムでは、Cisco Jabber が着信 IM メッセージやコール イベントなどのイベントを常にポーリングする必要がありません。これより、バッテリの寿命が延び、ユーザ エクスペリエンスが向上します。

C：図 2-5 は、APN との統合の全体的なアーキテクチャを示しています。Apple iOS プラットフォーム上で動作する各アプリケーションは、APN 経由で通知を受け取るために APN に登録し、デバイスとアプリケーションに固有のデバイス トークンを受け取ります。APN 経由で通知を送信する通知プロバイダーは、APN に登録します。また、通知をデバイスに送信するときに、ターゲット デバイスとアプリケーションを一意に識別するデバイス トークンを提示する必要があります。

C：図 2-5　　APN との統合のためのアーキテクチャ



C：図 2-5 に示すアーキテクチャでは、単一の APN プロバイダーがすべての統合に使用され、この APN プロバイダー（Push REST サービス）は Cisco Collaboration Cloud でホストされます。特定の Unified CM and IM and Presence Service クラスタの APN 統合を有効にするには、最初に、クラウドベースの Push REST サービスにクラスタをオンボードする必要があります。このオンボーディング プロセス中に、Cisco Collaboration Cloud 内の特定のクラスタ用のマシン アカウントが作成され、そのクラスタの OAuth 更新トークンが発行されます。この情報を使用すれば、クラスタのすべての IM and Presence ノードと呼処理ノードは Push REST サービスへの接続を構築して、特定の Jabber クライアントを対象とする通知要求を発行することができます（ステップ 1）。これらの要求は、オンボーディング プロセス中に取得される OAuth 更新トークンを使って生成された OAuth アクセス トークンを使用して認証されます。

Jabber クライアントは、APN への登録中に APN からデバイス トークンを受け取ります。このデバイス トークンは元の Unified CM クラスタに報告された後、Push REST サービス宛てのアウトバウンド通知要求内で IM and Presence ノードと呼処理ノードによって使用されます。

Push REST サービスは、IM and Presence ノードと呼処理ノードから送られるすべての通知要求を APN に中継します（ステップ 2）。その後、通知は、Apple iOS デバイスと APN の間の永続的接続を介して個別のデバイスに転送されます（ステップ 3）。

Apple Push Notification を受信すると、Apple iOS はその通知をターゲット アプリケーションにディスパッチします。これにより、Cisco Jabber が起動してフォアグラウンド モードに移行し、Unified CM および Unified CM IM and Presence Service との間で通常のコールと IM のやり取りを再開します。

Apple iOS 上で動作する Jabber クライアントが APN との接続を作成して APN から通知を受け取るためには、社内からポート 443/TCP を介して Apple クラウド内の APN に接続できる必要があります。

エンドポイント

Jabber

Cisco Jabber クライアントは、音声、ビデオ、およびインスタント メッセージのためのコア コラボレーション機能をユーザに提供します。Cisco Jabber は Windows、Mac、およびスマートフォンやタブレットなどのモバイル デバイスを含む幅広いプラットフォームで利用できます。

Cisco Jabber は次の 2 つのモードのいずれかで展開できます。

- フル UC と Cisco Jabber for Everyone（IM のみ）モード

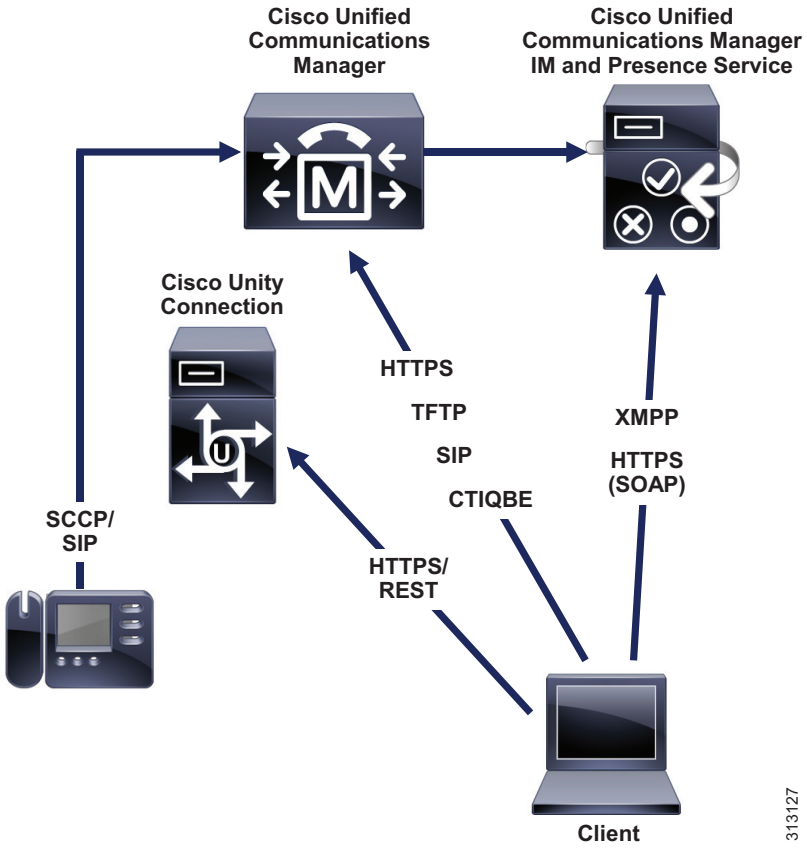
  これはデフォルト モードです。ユーザのプライマリ認証は IM and Presence サーバに対して行われます。これは、このプリファード アーキテクチャ設計で使用されるモードであり、本マニュアルで取り上げられています。

- 電話モード

  電話モードでは IM と Presence サービスは必要ありません。

C：図 2-6 は Cisco Unified Communications Manager IM and Presence が含まれたオンプレミス展開のアーキテクチャを示しています。

C：図 2-6　Cisco Unified Communications IM and Presence のアーキテクチャ



Cisco Jabber は、サービスに接続するために次の情報を必要とします。

- ユーザがクライアントにサインインできる認証のソース

  フル UC および IM のみモードでは、認証のソースは IM and Presence サービスです。電話のみモードでは、Unified CM です。

- サービスのロケーション

  サービスには IM and Presence、ディレクトリ、CTI、ボイスメール、会議が含まれます。

この情報をクライアントに提供するには、Manual Connection メソッドよりも Service Discovery メソッドの使用を推奨します。Service Discovery メソッドを使うと、クライアントが自動的に配置され、サービスに接続します。

この設計では、ユーザが最初に Jabber クライアントで電子メール アドレスを入力したときに取得される SRV レコード _cisco-uds を使って、クライアントが自動的にサービスと設定を検出します。

Jabber Contact Source として、Cisco Directory Integration（CDI）を伴う LDAP 連絡先ソースを使用できます。別の連絡先ソースとして Unified CM ユーザ データ サービス（UDS）を使用することもできますが、オンプレミス展開用の連絡先ソースとしては CDI が推奨されます。

マルチクラスターに関する考慮事項

マルチクラスタ展開では、SIP トランクを介して個々の Unified CM クラスタすべてを相互接続します。個々のクラスタ間のセッション トラバーサルを防ぐには、フルメッシュの SIP トランクを展開します。4 つ以上のクラスタでは、Cisco Unified CM Session Management Edition（SME）を展開してダイヤル プランとトランキングを一元化し、フルメッシュ SIP トランク トポロジの複雑さを回避します。Cisco Unified CM SME については、このマニュアルでは取り上げません。SME の詳細については、『*Cisco Collaboration SRND*』を参照してください。

マルチクラスタ展開では、グローバル ダイヤル プラン レプリケーション（GDPR）を使用して、クラスタ間でダイヤル プラン情報を複製します。GDPR はディレクトリ番号ごとに 1 つの +E.164 番号、1 つの Enterprise Significant Number（ESN）、そして最大 5 個の英数字 URI をアドバタイズできます。ESN はディレクトリ番号に相当する、サイト内の短縮ダイヤルです。GDPR を通じてアドバタイズされ、学習された情報により、次のようなダイヤル手順での決定論的なクラスタ内ルーティングが可能になります。

- アドバタイズされた +E.164 番号に基づく +E.164 ダイヤリング
- アドバタイズされた ESN に基づくエンタープライズのサイト内短縮ダイヤリング
- アドバタイズされた URI に基づく英数字 URI ダイヤリング

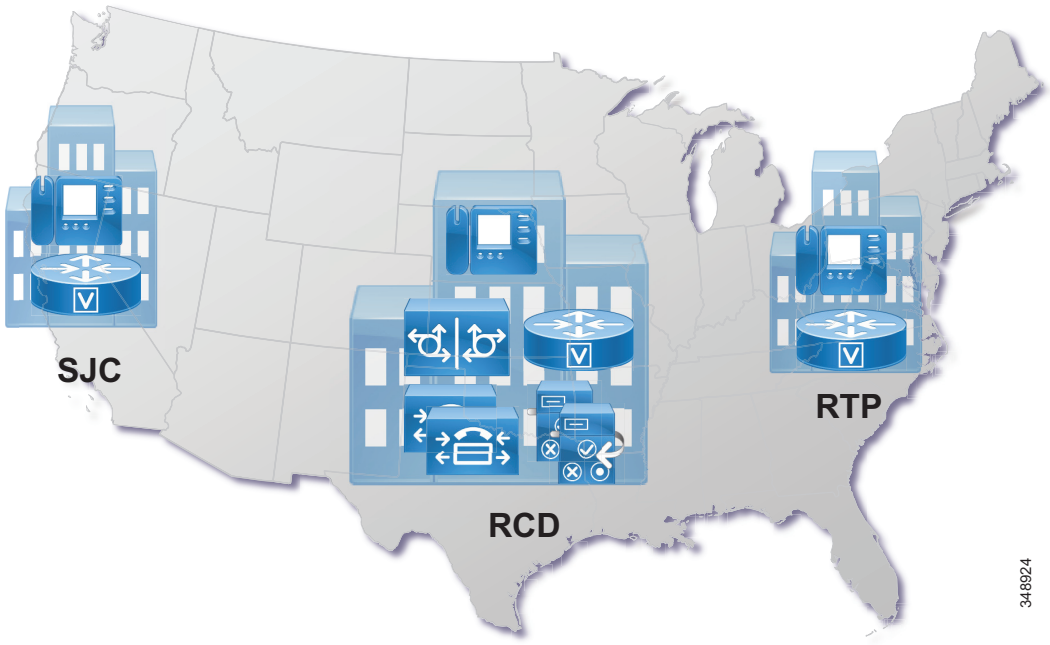
GDPR はトランスポート媒体としてクラスタ間検索サービス（ILS）を利用するので、マルチクラスタ展開の場合は、すべての Unified CM クラスタ間で ILS をセットアップする必要があります。GDPR に加えて、Jabber によって使われる UDS ベースのサービス検出でも ILS 交換を利用し、非ローカル ユーザの /cucm-uds/homeCluster 要求の転送先として可能なリモート クラスタ上の UDS ノードの存在を検出し、Jabber にログイン試行するユーザのホーム クラスタを特定します。

IM and Presence 機能は、単一クラスタ内での通信により制限されます。プレゼンスとインスタント メッセージングの能力と機能を拡張するには、これらのスタンドアロンのクラスタにピア関係を設定することで、同じドメイン内の複数のクラスタ間で通信できるようになります。この機能により、1 つのクラスタ内のユーザが、同じドメイン内の異なるクラスタにいるユーザと通信したり、プレゼンスをサブスクライブしたりできます。フルメッシュのプレゼンス トポロジを作成するには、それぞれの Cisco IM and Presence クラスタと、同じドメイン内の他のそれぞれの Cisco IM and Presence クラスタとの間に、個別のピア関係が設定されている必要があります。クラスタ間のピアはリモートの Unified CM cluster IM and Presence パブリッシャ ノードの IP アドレスとして設定されます。

トポロジーの例

このマニュアルでは、米国の 3 つのサイト（SJC、RCD、RTP）にサービスを提供する集中型の呼処理展開を想定しています。Unified CM および IM and Presence Service の各サーバは集中的に RCD に配置されます。中央の PSTN アクセスは RCD でも同様に行われます。SJC と RTP は、ローカルで Survivable Remote Site Telephony (SRST) を設定され、RCD サイトへの WAN 接続がダウンした場合のローカル PSTN アクセスを備えた小さなサイトであると想定します。C：図 2-7 はこのトポロジの例を示しています。

C：図 2-7　　トポロジの例



マルチクラスタに関する考慮事項のために、このマニュアルでは、2 つのクラスタ（C：図 2-7 で示されている米国のクラスタと、ヨーロッパ、中東、アフリカ（EMEA）を対象とした 2 つ目のクラスタ）による展開がトポロジの例として使用されます。

証明書に関する考慮事項

証明書に関する考慮事項（一般的な概念や展開に関する推奨事項など）については、セキュリティーの章を参照してください。

DNS に関する考慮事項

前のセクションで説明したように、接続のセットアップ中に提出されるサーバ証明書のアイデンティティが検証されます。つまり、クライアントの接続先となるアイデンティティに対して、提出された証明書のサブジェクトが実際に検査されるようにするには、完全修飾ドメイン名（FQDN）に基づいてクライアントが接続を開始する必要があります。接続の開始で FQDN を使用するということは、DNS が基本要件であることを意味します。ネットワーク内のすべて

のクライアントとサーバで名前解決を確実に利用できるように、エンタープライズ DNS がセットアップされる必要があります。信頼できる FQDN-IP アドレス解決（およびその逆の解決）を提供することに加えて、Jabber クライアントで使用される自動サービス検出プロセスにも DNS が必要とされます。

起動中に Jabber クライアントは、DNS を使用して _cisco-uds._tcp SRV を解決することにより、UDS ベースのサービス検出に必要な UDS サービスを特定します。最適な冗長性とロード バランシングを実現するには、Unified CM パブリッシャ ノードと TFTP ノードに等しい優先順位と重要度を使用して DNS SRV レコードをプロビジョニングすることをお勧めします。

エンドポイントのアドレッシング

DID アドレスを持つエンドポイント上のすべてのディレクトリ番号が +E.164 番号としてプロビジョニングされます。このアプローチのメリットは次のとおりです。

- +E.164 ディレクトリ番号は、一意として定義されます。
- +E.164 ディレクトリ番号は、それ以上のダイヤル プラン設定を必要とせず、直接的に 1 つのダイヤル手順（+ E.164）を有効にします。
- +E.164 ディレクトリ番号は、ネット上の強制的なルーティングの実装を簡略化します。
- 自動代替ルーティング（AAR）の設定が大幅に簡略化されます。ターゲットのネット上宛先を代替 PSTN アドレス（+E.164 番号）として直接使用できるので、複数の AAR グループと AAR PSTN プレフィックスをプロビジョニングする必要がありません。
- すべてのコール フロー（直接、転送、ネット上、およびネット外）で、正しい発信者 ID が自動的に生成されます。

DID が関連付けられていないエンドポイント（ロビーの電話機など）およびエンタープライズ サービス（コール ピックアップやコール パークなど）にも、一意のアドレスが必要です。それらの +E.164 番号は存在しないため、代替のエンタープライズ固有番号計画（ESN）スキーマを使ってこれらを処理することをお勧めします。推奨される ESN スキーマ形式は、ESN ダイヤルと他のダイヤル手順が重複しないようにアクセス コードを選択した後、サイト コードとサイト内拡張番号を続けることです。サイト コードと拡張番号の長さでは、十分に大きな番号スペースを確保するか、それとも ESN ダイヤリングをできるだけ短くするかのトレードオフが存在します。

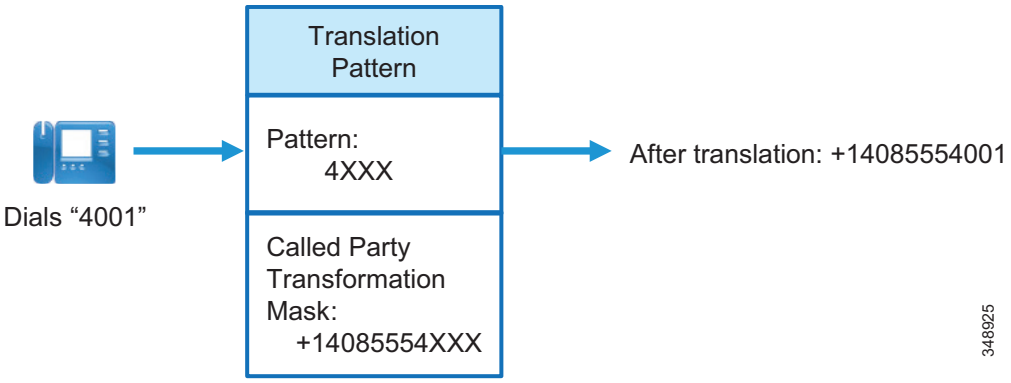
+E.164 ルーティングおよびダイヤリングの正規化

意図した通りのオンネットの強制的なルーティング（サポートされている数字でのダイヤル手順のどれを使って任意のオンネットの接続先にダイヤルしても、オンネットでルーティングされなければならない）を実現するために、推奨されるダイヤル プランの設計では 2 段階のルーティング方法が使用されます。第 1 段階で、ダイヤルされる数字列は可能であれば +E.164 で正規化されます（非 DID への発信は明らかに +E.164 で正規化されません）。次に第 2 段階で、正規化された +E.164 数字列が、電話番号およびルート パターンを含む +E.164 番号計画に対して照合されます。

ダイヤリングの正規化は、非 +E.164 ダイヤル列での照合を行うトランスレーション パターンをプロビジョニングし、その後に、そのトランスレーション パターンに基づいた発信側トランスフォーメーションにより、ダイヤルした番号が +E.164 に変換されることで実現されます。

C：図 2-8 に、SJC のサイト内短縮ダイヤルをダイヤル先の +E.164 フル番号に正規化するために使用できる、ダイヤリング正規化トランスレーション パターンの例を示します。サイト SJC のユーザ to ユーザーが 4001 にダイヤルすると、その数字列がトランスレーション パターン 4XXX; とそのトランスレーション パターン上で設定された着信側トランスフォメーション マスクによって照合され、4001 に適用されたときに、結果の数字列 +14085554001 が生成され、その後で、+E.164 ルーティング方式でルーティングできます。

C：図 2-8　　ダイヤリング正規化トランスレーション パターンの例



トランスレーション パターンに基づいて定義された着信側トランスフォーメーションを適用した後に、Unified CM はそのトランスレーション パターンに基づいて定義されたコーリング サーチ スペース（CSS）を使用して数字列に対する 2 回目の検索を実行します。Unified CM は、この 2 回目の検索のために、発信元の CSS と使用するトランスレーション パターンの定義を有効にします。これにより、複数のコンテキストで再利用できるダイヤリング正規化トランスレーション パターンの定義が可能になります。ダイヤリング正規化を適用した後に、単一の固定された CSS に基づくのではなく、そのトランスレーション パターンが用意されたときに有効だった CSS に基づいて、正規化された数字列の 2 回目の検索が実行されるからです。

Tip

2 回目の検索で使用される CSS が最初の検索で使用される CSS と同一であるようにするために、ダイヤリング正規化トランスレーション パターンでオプション [発信側コーリングサーチスペースを使用 （Use Originator's Calling Search Space）] を設定します。

Tip

（可変長ワイルドカードで終わらない）固定長のダイヤリング正規化トランスレーション パターンでは、[後続のホップで番号間タイムアウトを待機しない（Do Not Wait For Interdigit Timeout On Subsequent Hops）] オプションも設定します。これにより、2 次的な検索で可変長ルート パターンと一致した場合でも、番号間タイムアウトなしでコールが引き続きルーティングされます。

サービス クラスとコーリング サーチ スペース（CSS）

パーティションと CSS はサービス クラスを構築するために Unified CM で使用される基本的なコンポーネントです。ダイヤル可能なパターンは、同じクラスに属するパターンを同じパーティションに入れることにより、等価クラスにグループ化されます。このときの各 CSS は、その CSS を使用する発呼側エンティティがどのパーティションおよびパターンにアクセスできるかを定義するパーティションのリストです。CSS は、その CSS を使用するデバイスから到達可能な宛先を決定することにより、サービス クラスを効率的に適用します。

ダイヤル プランを複雑にする主な要因は定義されたサービス クラスの数であるため、必要なサービス クラスの数をできるだけ少なくする必要があります。適切に設計されたエンタープライズ ダイヤル プランでは、サービス クラス間でパターンとパーティションを再利用することにより、ダイヤル プラン展開が簡略化されます。

ローカル ルート グループを使用したアウトバウンド ゲートウェイ選択

ダイヤル プラン内の重複をできるだけ回避および排除するための根本原理に従って、イーグレス ゲートウェイの定義にローカル ルート グループ（LRG）の概念が使用されます。

ローカル ルート グループを使用したルート パターンには固有の特性があります。つまり、コールの発信元デバイスに基づいて出口ゲートウェイを動的に選択できます。それに対し、スタティック ルート グループを使用したルート パターンによってルーティングされるコールでは、コールの発信元デバイスに関係なく、コールが同じゲートウェイにルーティングされます。LRG を使用するルート リストを参照するよう設定されたルート パターンは、発信側のデバイス プールで LRG として設定された実際のルート グループに解決されます。

これにより、各サイトに固有ではないルート パターンの再利用が可能になります。各サイトのイングレス ゲートウェイに直接関連付けられたサイト固有のルート パターンをプロビジョニングする必要はありません。

アウトバウンド コール：着信者番号と発信者番号のローカリゼーション

このマニュアルで説明するダイヤル プランの設計では、ローカル ルート グループを使用して、発信側デバイスに基づく出力ゲートウェイを選択します。したがって、サービス プロバイダの要件に適応するために必要な発信側および着信側トランスフォーメーションは、ルート パターンまたはルート リストのレベルで行うことができません。その場合、これらのトランスフォーメーションは、すべてのゲートウェイ間で共有されることになります。代わりに、発信者情報と着信者情報をローカライズするためのこれらのサービス プロバイダ固有のトランスフォーメーションが、Cisco IOS Voice トランスレーション ルールを使用してゲートウェイに設定されるか、発信側または着信側トランスフォーメーション パターン（ゲートウェイまたはゲートウェイのデバイス プールに設定された発信側または着信側トランスフォーメーション CSS によって対処するパターン）を使用して Unified CM に設定されます。

インバウンド コール：着信者番号と発信者番号のグローバリゼーション

Unified CM 上のすべてのコール ルーティングは、Unified CM に到着するすべての着信コールの +E.164 番号に基づくため、プロバイダからリンク経由で受信された着信側情報の形式から +E.164 に確実にグローバル化する必要があります。これを実現するには、SIP ゲートウェイ上の Cisco IOS トランスレーション（SIP 経由で Unified CM に要求を送るときに ISDN ネットワークから受信される番号タイプの消失を防ぐために必要）、Unified CM 上で設定されたプレフィックス、および場合によっては着信番号変換と発信番号変換を組み合わせます。

LDAP 同期によるユーザー　プロビジョニング

Unified CM を社内 LDAP ディレクトリに同期すると、管理者は Unified CM データ フィールドをディレクトリ属性にマッピングすることにより、ユーザを容易にプロビジョニングできるようになります。LDAP ストアに保持されている重要なユーザ データは、スケジュール ベースで Unified CM データベース内の対応する適切なフィールドにコピーされます。社内 LDAP ディレクトリのステータスは、中央リポジトリのままとなります。Unified CM は、ユーザ データを保存するための統合データベースを備え、またユーザ アカウントおよびデータを作成して管理するための Web インターフェイスを、Unified CM Administration 内に備えています。LDAP 同期を有効にすると、ローカル Unified CM データベースを引き続き使用しながら、追加のローカル エンドユーザ アカウントを作成できます。その後、LDAP ディレクトリと Unified CM Administration のインターフェイスを通してエンドユーザ アカウントを管理できます。

LDAP によるユーザー認証

LDAP 認証機能により、Unified CM が LDAP で同期されたユーザを社内 LDAP ディレクトリに対して認証できます。ローカルに設定されたユーザは、常にローカル データベースに対して認証されます。また、すべてのエンドユーザの PIN も、常にローカル データベースで確認されます。

認証を有効にするには、クラスタ全体に単一の認証アグリーメントを定義します。

認証を有効にした場合の Unified CM の動作説明を、次に示します。

- LDAP からインポートされたユーザのエンド ユーザ パスワードは、シンプル バインド操作によって社内ディレクトリに対して認証される。
- ローカル ユーザのエンド ユーザ パスワードは、Unified CM データベースに対して認証される。
- アプリケーション ユーザ パスワードは、Unified CM データベースに対して認証される。
- エンド ユーザ PIN は、Unified CM データベースに対して認証される。

複数のドメイン コントローラを地理的に分散させた分散型 Active Directory トポロジを採用している環境では、認証速度が許容されない可能性があります。認証アグリーメント用のドメイン コントローラにユーザ アカウントが保持されていない場合、他のドメイン コントローラでそのユーザの検索が実行される必要があります。この設定が当てはまる展開においてログイン速度が過度に遅い場合は、グローバル カタログ サーバを使用するように認証設定を構成できます。

ただし、重要な制限があります。グローバル カタログは employeeNumber 属性をデフォルトで伝送しません。この場合は、認証（上記に示す制限に注意）用のドメイン コントローラを使用するか、employeeNumber 属性を含めるようにグローバル カタログを更新します。詳細については、Microsoft Active Directory のマニュアルを参照してください。

グローバル カタログに対する照会を有効にするには、グローバル カタログの役割が有効になっているドメイン コントローラの IP アドレスまたはホスト名を指すように [LDAP 認証（LDAP Authentication）] ページの [LDAP サーバ情報（LDAP Server Information）] を設定し、LDAP ポートを 3268 として設定します。

展開の概要

展開は集中型の Cisco Unified CM クラスタのプロビジョニングで始まり、さらに設定タスクとプロビジョニング タスクが続きます。次の項では、このマニュアルのプリファード アーキテクチャ設計に従って、コール制御をセットアップし、設定する方法について説明します。

- DNS 要件
- Cisco Unified CM と IM とプレゼンスサービスクラスタのプロビジョニング
- Cisco Unified CM と IM とプレゼンスサービスの証明書管理
- Cisco Unified CM の初期設定
- その他の IM とプレゼンス設定
- ダイヤル プラン設定
- LDAP システムの設定
- Cisco Unified CM グループ設定
- 電話用 NTP リファレンス
- 日付および時刻グループ
- メディア リソース
- デバイス プール
- SIP トランク
- エンドポイントのプロビジョニング
- マルチクラスター展開向けの ILS 設定
- GDPR の設定マルチクラスターのみ
- Survivable Remote Site Telephony（SRST）展開
- 拡張モビリティー
- ビジー回線フィールド（BLF）のプレゼンス
- コンピュータ テレフォニー インテグレーション（CTI）の展開

DNS 要件

ソリューションを展開する前に、展開するすべてのサーバで DNS 解決が使用できることを確認します。エンタープライズ DNS では、正引き（DNS 名から IP アドレス）と逆引き（IP アドレスから DNS 名）の両方のルックアップを設定する必要があります。

また、Unified CM IM and Presence Service ノードと Unified CM 呼処理ノードで設定された DNS リゾルバが、外部ルーティング可能なアドレスの解決を許可する必要があります。APN 経由のプッシュ通知では、これが必須です。

Jabber クライアント用の UDS ベースのサービス検出を有効にするのに加えて、すべての Unified CM パブリッシャ ノードおよび TFTP サブスクライバ ノードについて、DNS SRV レコードをプロビジョニングし、これらを _cisco-uds のサービス ロケーションとして定義します。C：例 2-1 は、いくつかの Unified CM ノードを _cisco-uds のサービス ロケーションとして定義した DNS SRV レコードの例です。

C：例 2-1　UDS ベースのサービス検出のための DNS SRV レコード

```
_cisco-uds._tcp.ent-pa.com     SRV service location:
          priority       = 10
          weight         = 10
          port           = 8443
          srv hostname   = us-cm-pub.ent-pa.com
_cisco-uds._tcp.ent-pa.com     SRV service location:
          priority       = 10
          weight         = 10
          port           = 8443
          srv hostname   = us-cm-tftp1.ent-pa.com
_cisco-uds._tcp.ent-pa.com     SRV service location:
          priority       = 10
          weight         = 10
          port           = 8443
          srv hostname   = us-cm-tftp2.ent-pa.com
```

C：例 2-1 では、3 つの Unified CM ノード（1 つのパブリッシャ ノードと 2 つの TFTP サブスクライバ ノード）が UDS サービス検出のサービス ロケーションとして定義され、UDS サービス検出を利用する Jabber クライアントからの最初の UDS 要求の負荷が、アクティブなすべての Unified CM ノード間で均等に分散されます。

UDS サービス検出処理の一部として /cucm-uds/clusterUser リソースを使用してホーム クラスタを探した後に、Jabber クライアントは /cucm-uds/servers リソースを使用して、ユーザのホーム クラスタ内のすべての UDS ノードのリストを取得します。これにより、SRV レコードでパブリッシャだけをサービス ロケーションとして定義した場合でも、登録処理中の実際の UDS 要求は、すべての UDS ノード間でロード バランシングされます。

Cisco Unified CM と IM とプレゼンスサービスクラスタのプロビジョニング

Unified CM and IM and Presence Service クラスタを展開するには、次のタスクを実行します。

1. 対象となるユーザ数とデバイス数に基づいて、必要な呼処理サブスクライバのペア数を決定します。
2. 対象となるユーザ数に基づいて、必要な IM と Presence ノード数を決定します。
3. 必要なすべてのクラスタ メンバーのネットワーク パラメータ（DNS 名、IP アドレスなど）を決定します。TFTP サーバも同様に考慮します。
4. Cisco が提供する適切な OVA テンプレート ファイルを使用して、必要な数の仮想マシンを計算インフラストラクチャに展開します。これらの OVA ファイルの取得方法について詳しくは、次の場所にあるマニュアルを参照してください。

   https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html
5. Cisco Prime Collaboration 展開で、すべてのメンバを含む Unified CM クラスタを定義し、タスク 4 で作成した仮想マシンにノードをマップします。
6. Cisco Prime Collaboration 展開を使用してすべてのノードを展開します。

Cisco Prime Collaboration Deployment を使用してクラスタをプロビジョニングする方法の詳細については、以下の場所にある『*Cisco Prime Collaboration Deployment Administration Guide*』の最新版を参照してください。

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

Cisco Unified CM と IM とプレゼンスサービスの証明書管理

セキュリティーの章の、サーバー証明書の生成と管理に関するセクションに記載されている手順に従います。エンドポイント上で暗号化を設定する予定がない場合でも、Cisco Unified CM and IM and Presence Service と Cisco Unity Connection の Tomcat 証明書の署名を外部 CA に依頼することをお勧めします。

CA により発行された証明書が、必要な鍵の用途と拡張鍵の用途を備えているかどうか、確認することが重要です。提供された CSR に基づいて証明書を発行する CA が、単にその CSR から鍵の用途と拡張鍵の用途をコピーして証明書を発行するのではなく、証明書を発行するために選択したテンプレートの設定に基づいて、発行される証明書の鍵の用途と拡張鍵の用途を設定することが、多くの場合に問題となります。たとえば、一般的な Web サーバ テンプレートに基づいて発行される証明書には、TLS Web クライアント認証の拡張鍵の用途が含まれていません。このために、TLS 接続を開始する側の Tomcat 証明書がクライアント証明書としても使用されるサーバ間通信（クラスタ間検索サービス（ILS）やユーザ データ ストア（UDS）など）において問題が生じ、鍵の用途が正しくないことが原因で TLS 接続のセットアップが失敗します（UDS 証明書要件の検討事項を参照）。

Cisco Unified CM の初期設定

Unified CM クラスタをインストールした後すぐに、次の基本的な設定タスクを実行します。

- ノード名設定
- エンタープライズ パラメーター設定
- サービスのアクティベーション
- サービス パラメーターの設定

ノード名設定

正しい証明書検証を許可し、Unified CM クラスタ メンバーへの参照が常に正しく解決できるようにするには、Unified CM 管理 GUI のシステム / サーバで、すべてのクラスタ メンバーに対してノード名に完全修飾ドメイン名（FQDN）を設定します。これを実現するには、Cisco Unified CM 管理 GUI でシステム / サーバに移動し、最初の列に表示されているすべてのサーバが FQDN であることを確認します。DNS ドメインが付いていない、ホスト名だけで表示されているサーバのエントリを FQDN に変更します。

エンタープライズ パラメーター設定

C：表 2-2 にリストされているエンタープライズ パラメータを確認し、更新します。

C：表 2-2　エンタープライズ パラメータ

エンタープライズ パラメータ	説明	値
[クラスタ ID（Cluster ID）]	クラスタ間検索サービス（ILS）およびクラスタ間コール アドミッション制御をはじめとする多くのクラスタ間機能において、Unified CM クラスタを一意に識別するために使用される	例：USCluster
[自動登録フォンプロトコル（Auto Registration Phone Protocol）]	自動登録フォン用にプロビジョニングされるシグナリング プロトコル	[SIP]
[コールリストの BLF（BLF For Call Lists）]	この機能をサポートしている電話のコール リストがプレゼンスを表示するかどうかを指定します	[有効（Enabled）]
[URI 検索ポリシー（URI Lookup Policy）]	RFC 3261 に従い、SIP URI に相当するものを確定する際に、URI の左側（ユーザ部分）のチェックで大文字小文字を区別する必要があります。Unified CM のデフォルトの動作はこの標準に従いますが、大文字小文字が混合している URI で発生する潜在的な問題を回避するには、通常、このデフォルト設定を変更する方が望ましいです。	[大文字小文字の区別なし（Case Insensitive）]
[依存性レコードを有効化（Enable Dependency Records）]	依存性レコードは Unified CM の管理を簡素化します。	[はい（True）]
[すべてのパーティションで DN を自動選択（Auto Select DN on Any Partition）]	管理を簡素化します。有効にした場合、ディレクトリ番号設定ページには、最初に一致したディレクトリ番号が自動的に入力されます。	[はい（True）]
[CDR ファイルの時間間隔（CDR File Time Interval）]	呼詳細レコード（CDR）ファイル更新の時間間隔を決定する	[10]
[URL 認証（URL Authentication）] [URL ディレクトリ（URL Directories）] [URL 情報（URL Information）] [URL サービス（URL Services）] [保護された認証 URL（Secured Authentication URL）] [保護されたディレクトリ URL（Secured Directory URL）] [保護された情報 URL（Secured Information URL）] [保護されたサービス URL（Secured Services URL）]	さまざまな目的のためのエンドポイントで使用される URL	これらの URL が Unified CM パブリッシャ ノードの FQDN を参照することを確認します
[組織の最上位ドメイン（Organization Top Level Domain）]		例：ent-pa.com

C：表 2-2 エンタープライズ パラメータ（続き）

エンタープライズ パラメータ	説明	値
[クラスタの完全修飾ドメイン名（Cluster Fully Qualified Domain Name）]	数値 SIP URI をルーティングする際に、Unified CM は URI の右側（ホスト部分）が、設定したクラスタの完全修飾ドメイン名（CFQDN）に一致する SIP URI を、設定したローカル数値ダイヤル プランに従ってルーティングされる宛先と見なします。設定された数値ダイヤル プランに URI の左側の数値に一致するものが見つからない場合、Unified CM はコールを拒否します。詳細については、最新版『*Cisco Collaboration System SRND*』の「*Dial Plan*」の章の「*Routing of SIP Requests in Unified CM*」に関するセクションを参照してください。	クラスタ内の Unified CM のすべての呼処理ノードのスペース区切りリスト。 例： us-cm-sub1.ent-pa.com us-cm-sub2.ent-pa.com
[更新ログイン フローを使用した OAuth（OAuth with Refresh Login Flow）]	これにより、OAuth 付与フロー認証が可能になります。これは、APN を介したプッシュ通知を使用する展開で強く推奨されます。OAuth 付与フロー認証では、着信 APN を受信する Jabber クライアントをフォアグラウンドに配置し、ユーザが着信コールにタイムリーに応答できるように迅速に再認証することができます。また、ローカルで有効な証明書 (LSC) が Jabber にインストールされていない場合は、暗号化されたメディアと Jabber でのシグナリングを有効にする必要があります。	有効（Enabled）

サービスのアクティベーション

C：表 2-3 に、Unified CM パブリッシャ ノード、専用の Unified CM TFTP サーバ サブスクライバ ノード、および Unified CM 呼処理サブスクライバ ノードでアクティブ化されるサービスをまとめます。

C：表 2-3 Unified CM ノードのサービスのアクティブ化

サービス	パブリッシャ	専用 TFTP サブスクライバ	呼処理サブスクライバ
CM サービス			
Cisco CallManager			はい
Cisco IP Voice Media Streaming App			はい
Cisco CTIManager			はい
Cisco Intercluster Lookup Service	はい		
Cisco Location Bandwidth Manager			はい
Cisco Dialed Number Analyzer Server	はい		
Cisco Dialed Number Analyzer	はい		
Cisco Tftp		はい	
CTI サービス			

C：表 2-3 Unified CM ノードのサービスのアクティブ化（続き）

サービス	パブリッシャ	専用 TFTP サブスクライバ	呼処理サブスクライバ
Cisco WebDialer Web Service			はい
データベースおよび管理者サービス			
Cisco Bulk Provisioning サービス	はい		
Cisco AXL Web Service	はい		
パフォーマンスおよびモニタリング サービス			
Cisco Serviceability Reporter	はい		
Cisco CallManager SNMP サービス	はい	はい	はい
セキュリティ サービス			
Cisco CTL Provider	はい	はい	はい
Cisco Certificate Authority Proxy Function	はい		
ディレクトリ サービス			
Cisco DirSync	はい		

C：表 2-4 に、Cisco Unified CM IM and Presence パブリッシャおよびサブスクライバ ノードでアクティブ化すべきサービスをリストします。

C：表 2-4 Unified CM IM and Presence ノード サービスのアクティブ化

サービス	パブリッシャ	サブスクライバ
Cisco AXL Web Service	はい	はい
Cisco Bulk Provisioning Service	はい	
Cisco Serviceability Reporter	はい	
Cisco SIP Proxy	はい	はい
Cisco Presence Engine	はい	はい
Cisco XCP Connection Manager	はい	はい
Cisco XCP Authentication Service	はい	はい

サービス パラメーターの設定

Cisco CallManager サービスの一部のサービス パラメータはグローバルであり、Unified CM Administration で 1 度だけ設定する必要があります。Cisco CallManager サービスのグローバル サービス パラメータ設定は、C：表 2-5 のリストに記載されています。

注 このマニュアルでは、デフォルト以外のサービス パラメータおよびその他の設定フィールドの値だけを示しています。フィールド設定値が示されていない場合は、デフォルト値が想定されます。

注 列挙したサービス パラメータの一部は、高度なサービス パラメータです。

C：表 2-5　グローバル サービス パラメータ

サービス パラメータ	値	説明
[コール診断有効（Call Diagnostics Enabled）]	[CDR 有効フラグが True の場合にのみ有効（Enable Only When CDR Enabled Flag is True）]	このパラメータは、コール管理レコード（CMR）（コール診断レコードとも呼ばれる）を生成するかどうかを決定します。
[T302 タイマー（T302 Timer）]	[5000]	接続先へのダイヤリングが Unified CM にプロビジョニングされている数値ダイヤル プランに基づいており、1 桁ずつ行われる場合は常に、プロビジョニングされているどのパターンをダイヤル先で検討する必要があるかに関して、即時の決定論的な意思決定を行うことはできません。マッチングが長くなる（可変長の場合も考えられる）可能性があるため、Unified CM が最適ルートを選択し、コールをルーティングする前に、T302 インターディジット タイムアウトの期限が切れる必要があります。デフォルト値の 15,000 ミリ秒（ms）は、通常は長すぎます。
[リモート番号に変換を適用（Apply Transformations On Remote Number）]	[はい（True）]	コール側の変換がミッドコールにも適用されることを確認します。たとえば、ある関係者から別の関係者へコールが転送される場合などです。
DN への未登録ホップの最大転送数	2	たとえば、電話機の登録が解除されているもの、サイトのゲートウェイが依然として統一された CM に登録されている場合は、CFUR ループが発生しないように制限します。
[Q.931 接続解除原因コード時のルーティングの中止（Stop Routing on Q.931 Disconnect Cause Code）]	[3 21 27 28 38 42 63]	特定の Q.850 原因コード受信時に、設定済みのハント リストの追跡を Unified CM がやめることを許可します。
[G.722 コーデック有効（G.722 Codec Enabled）]	録音を有効化したデバイス以外のすべてのデバイスで有効	レコーダーによってサポートされていない G.722 での問題を回避するため、録音を有効化したデバイスでは G.722 を無効化します。
[自動代替ルーティングの有効化（Automated Alternate Routing Enable）]	True	このサービス パラメータは、自動代替ルーティング（AAR）をグローバルに有効にします。

Cisco CallManager サービスの他のサービス パラメータは、C：表 2-6 に示すように、各 Unified CM 呼処理ノードについて明示的に設定する必要があります。

C：表 2-6　ノードごとのサービス パラメータ

サービス パラメータ	値	説明
[CDR 有効フラグ（CDR Enabled Flag）]	[はい（True）]	このパラメータは、コール詳細レコード（CDR）の生成を有効にします。
[接続時間がゼロのコールを CDR に記録するフラグ（CDR Log Calls With Zero Duration Flag）]	[はい（True）]	このパラメータは、接続されなかった、または接続時間が 1 秒未満だったコールのコール詳細レコード（CDR）のロギングを有効または無効にします。
[ディジット分析の複雑性（Digit Analysis Complexity）]	[TranslationAndAlternatePatternAnalysis]	このパラメータは、CCM トレース ファイルが提供するディジット分析情報の量を指定します。

Apple Push Notification Service（APN）経由のプッシュ通知のオンボーディング

次で入手可能な *Cisco Unified Communications Manager を使用した iPhone および iPad での Cisco Jabber のプッシュ通知の展開*の最新バージョンで説明されている *プッシュ通知設定タスク フロー*に従います。

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

要約すると、オンボーディングでは次の手順が必要です。

- スマート ライセンスの登録
  - [ライセンス管理（license management）] ページで Unified CM クラスタを登録する
- バウチャーの生成
  - [拡張機能（Advanced Features）] > [シスコ クラウド オンボーディング（Cisco Cloud Onboarding）] で、[バウチャーの生成（Generate Voucher）] をクリックする
- オンボーディング
  - [拡張機能（Advanced Features）] > [シスコ クラウド オンボーディング（Cisco Cloud Onboarding）] で、

    [プッシュ通知の有効化（Enable Push Notifications）] を選択します。

    [シスコ クラウドにトラブルシューティング情報を送信する（Send Troubleshooting information to the Cisco Cloud）] を選択します。

    [この信頼に必要なシスコ クラウド サービス CA 証明書をシスコが管理する（I want Cisco to manage the Cisco Cloud Service CA Certificates required for this trust）] を選択します。

    C：表 2-7 の接続要件でフォワード プロキシを使用する必要がある場合は、[HTTP プロキシの有効化（Enable HTTP Proxy）] を選択して、プロキシの詳細を入力します。

    [保存（Save）] をクリックします。
- Unified CM IM and Presence ノードで **XCP ルータ サービス**を再起動します。
  - クラスタのオンボーディングが成功したら、クラスタ内のすべての Unified CM IM and Presence ノードで XCP ルータ サービスを再起動する必要があります。このサービスをメンテナンス期間に再起動することをお勧めします。

C：表 2-7 に、さまざまな Unified CM ノードの接続要件を示します。既存のネットワーキング ポリシーのために直接アクセスが不可能な場合は、フォワード プロキシ経由で、C：表 2-7 の宛先へのアクセスを可能にする必要があります。

C：表 2-7　APN 経由のプッシュ通知のクラウド接続要件

遷移元	目的	ポート	使用方法
Unified CM パブリッシャ	Cisco cloud	443/TCP	オンボーディング プロセス中の Unified CM パブリッシャは、**fos-a.wbx2.com** でホストされるオンボーディング サービスへのアクセス権を必要とします。
Unified CM IM and Presence と呼処理	Cisco cloud	443/TCP	すべての呼処理サブスクライバ ノードと IM and Presence ノードは、OAuth アクセス トークンを取得する目的で、**idbroker.webex.com** における共通 ID サービスへのアクセスを必要とします。また、**push.webexconnect.com** における Push REST サービスにアクセスできる必要もあります。

その他の IM とプレゼンス設定

これまでの項では、IM and Presence サービスのアクティブ化、証明書管理、および IM and Presence SIP トランク設定について説明しました。それらに加えて、IM and Presence サーバの次の設定を行います。

- [IM&P Cisco SIP Proxy] サービス パラメータでの Unified CM ドメインの設定。
- [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）] :
  - クラスタ ID の値を設定します。
  - 可用性の共有を有効にします。これを有効にしない場合、ユーザは自分の可用性ステータスしか表示できません。
  - [アドホックプレゼンスサブスクリプションを有効にする（Enable ad-hoc presence subscriptions）] チェックボックスを選択し、Cisco Jabber ユーザのアドホック プレゼンス サブスクリプションをオンにします。
- [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [ルーティング（Routing）] > [設定（Settings）] :
  - [プロキシサーバの設定（Proxy Server Settings）] : **[メソッド / イベントルーティングのステータス（Method/Event Routing Status）] を [有効（Enable）] に設定します**
- [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [メッセージング（Messaging）] > [設定（Settings）] :
  - インスタント メッセージを有効にします。
- OAuth 付与フロー認証を有効にします。
  - エンタープライズ パラメータ [更新ログイン フローを使用した OAuth（OAuth with Refresh Login Flow）] を [有効（Enabled）] に設定します。
- マルチ デバイス メッセージングを有効にします。
  - Cisco Unified CM IM and Presence Administration で、[システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。
  - [サーバ（Server）] ドロップダウン リストから、[IM and Presence サービス パブリッシャ（IM and Presence Service Publisher）] ノードを選択します。
  - [サービス（Service）] ドロップダウン リストから、[Cisco XCP ルータ（アクティブ）（Cisco XCP Router (Active)）] を選択します。
  - [マルチ デバイス メッセージングの有効化（Enable Multi-Device Messaging）] ドロップダウン リストから、[有効（Enable）] を選択します。
  - [保存（Save）] をクリックします。
- プッシュ通知高可用性の有効化
  - Cisco Unified CM IM and Presence Administration で、[システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。
  - [サーバ（Server）] ドロップダウン リストから、[IM and Presence サービス パブリッシャ（IM and Presence Service Publisher）] ノードを選択します。
  - [サービス（Service）] ドロップダウン リストから、[Cisco XCP ルータ（アクティブ）（Cisco XCP Router (Active)）] を選択します。
  - [プッシュ通知高可用性（Push Notifications High Availability）] ドロップダウン リストから、[有効（Enabled）] を選択します。
  - [保存（Save）] をクリックします。

- XCP ルータ サービスを再起動します。
  - マルチ デバイス メッセージングとプッシュ通知高可用性を有効にする 2 つのサービス パラメータを変更するには、メンテナンス期間中にすべての Unified CM IM and Presence ノードで **Cisco XCP ルータ**を再起動する必要があります。

さらに、Jabber プロビジョニング で説明されているように、Jabber クライアント用の UC サービスを設定します。

ダイヤル プラン設定

すべてのコール制御システムを思い通りに展開するために、構造化され、適切に設計されたダイヤル プランは必要不可欠です。エンタープライズ ダイヤル プランの設計では、次の主要な領域を対象とする必要があります。

- エンドポイントのアドレッシング
- 一般的な番号計画
- ダイヤル手順
- ルーティング
- サービス クラス

推奨されているダイヤル プランの設計は、最新版『*Cisco Collaboration System SRND*』の「*Dial Plan*」の章に記載されている設計アプローチに従っています。

トポロジーの例

このマニュアルでは、米国の 3 つのサイト（SJC、RCD、RTP）にサービスを提供する集中型の呼処理展開を想定しています。C : 表 2-8 に、これらのサイトの DID（ダイレクト イン ダイヤル）の範囲を示します。

C : 表 2-8　　サイトの例の DID 範囲

サイト	DID 範囲
SJC	+1 408 555 4XXX
RCD	+1 972 555 5XXX
RTP	+1 919 555 1XXX

エンドポイントのアドレッシング

DID アドレスを持つエンドポイントの場合、電話番号は +E.164 のフル番号でプロビジョニングされます。この場合、+E.164 は最初の「+」に続いてグローバルな E.164 フル電話番号を表します。Unified CM で +E.164 電話番号をプロビジョニングするには、最初の「+」をエスケープする必要があります。たとえば、SJC の内線 4001 は \+14085554001 としなければなりません。

プロバイダから十分な DID が入手できない、あるいは関連付けられたデバイスに PSTN から電話をかける必要がない（内線電話など）などの理由から、一部のエンドポイントは DID を持ちません。こうしたエンドポイントには DID（E.164 番号）が存在せず、そのためこれらのエンドポイントには +E.164 以外のアドレス形式が必要です。このアドレス形式については、一般的な番号計画に関するセクションで説明します。

外部アクセス用エンタープライズ サービスのアドレッシング

一部のサービスには割り当てられた PSTN 番号があります。こうした例として、ユーザが PSTN からボイスメールに電話をかけられるように、外部から到達可能でなければならないボイスメールの代表番号が考えられます。こうしたサービスの PSTN の E.164 番号は、PSTN プロバイダによって割り当てられる DID の範囲から予約しておく必要があります。

一般的な番号計画

+E.164 アドレスが使用できる DID に関連付けられたエンドポイントに加えて、DID がない、以下のような接続先も数多く存在します。

- 内線電話
- プロバイダが DID を割り当てることができなかった正規のエンドポイント
- 各種サービス（コール ピックアップ番号、コールパーク番号、会議など）

このマニュアルではこれらのタイプの接続先のことを*非 DID* と呼びます。

これら非 DID のアドレスは +E.164 アドレス同様、非 DID のサイト固有パーティションを回避するためにシステム全体で一意でなければなりません。推奨されるソリューションは、すべての非 DID に関してエンタープライズ固有の番号計画（ESN）を導入することです。この ESN 方式は一般的なサイト間短縮ダイヤルの構造に従います。

- アクセスコード

  サイト間短縮ダイヤルの 1 桁のアクセスコード。設計段階において、ほかのどのエンタープライズ ダイヤル手順とも重複しないようにアクセスコードを選択します（下記参照）。
- サイトコード

  ネットワーク内のサイトを一意に識別するための一連の番号。設計段階において、すべての既存のサイトを対象とするだけではなく、規模が拡大した場合も考慮したサイト コードの長さを選択します。
- 内線番号

  サイト内で各エンティティを一意に識別するための一連の番号。

このマニュアルでは、サイト間短縮ダイヤルのアクセスコードに 8 を使います。したがって、すべての ESN は 8 で始まります。また、サイト コードには 3 桁、内線番号には 4 桁を使用します。C：表 2-9 では、本書の例にある各サイトの DID 番号および非 DID 番号の ESN 範囲を示しています。

C：表 2-9　DID および非 DID の ESN 範囲

サイト	+E.164 範囲	サイト コード	DID の ESN 範囲	非 DID の ESN 範囲
SJC	+1 408 555 4XXX	140	8-140-4XXX	8-140-5XXX
RCD	+1 972 555 5XXX	197	8-197-5XXX	8-197-6XXX
RTP	+1 919 555 1XXX	191	8-191-1XXX	8-191-2XXX

このプランでは DID と非 DID について同じサイト コードを使用しますが、非 DID の内線番号の最初の数字は DID 内線番号の最初の数字とは異なります。これにより、非 DID 番号および DID 番号への 4 桁のサイト内短縮ダイヤルも可能になります。

C：表 2-9 の ESN 範囲ではサイト固有番号に対して ESN 計画に余地を残していますが、スケジュール済み会議などのサイト固有以外のサービスについても番号を割り当てる必要があります。C：表 2-10 に、専用のサイト コード（この場合は 099）を予約しておくことにより、この要件に対処する方法の例を示します。

C：表 2-10　会議用の ESN 範囲

ESN 範囲	使用方法
8099[12]XXX	スケジュール済み会議

ダイヤル手順

ダイヤル手順では、エンド ユーザがさまざまな種類の接続先に電話をかけるためにどのようにダイヤルする必要があるかを記述します。ダイヤル手順はまず、数字でダイヤルするか（914085550123 など）、または英数字でダイヤルするか（ bob@ent-pa.com）などで分類されます。

この設計では、英文字の URI でダイヤルする方法に加えて C：表 2-11 に示すように数字でのダイヤル手順もサポートされています。

C：表 2-11　サポートされている数字でのダイヤル手順

ダイヤル パターン	例（サイト SJC）	接続先のタイプ
XXXX	4001（DID） 5001（非 DID）	接続先に同時にダイヤルするためのサイト内短縮ダイヤル。 発信先は DID 番号、非 DID 番号、またはサービス番号であることが可能です。
+E.164	+14085554001（ネット上、SJC） +19195551001（ネット上、RTP） +1212551001（ネット外）	ディレクトリなどからの +E.164 フル番号ダイヤル。ダイヤル先はネット上であることもネット外であることも可能です。実装されたダイヤル プランによって、+E.164 でダイヤルされるネット上の接続先へのコールが、確実にネット上にルーティングされます。明らかなこととして、非 DID を +E.164 でコールすることはできません。
アクセス コード – サイト コード – 内線番号	8-140-4001（DID、SJC） 8-140-5001（非 DID、SJC） 8-191-1001（DID、RTP） 8-191-2001（非 DID、RTP）	同じサイトまたは別のサイトの接続先にダイヤルするためのサイト間短縮ダイヤル。発信先は DID 番号、非 DID 番号、またはサービス番号であることが可能です。アクセス コード（この例では 8）は、他のダイヤル手順（サイト内短縮ダイヤルなど）と重複しないように選択する必要があります。サイト間ダイヤルにアクセス コード 8 を使うことで、8 で始まる 4 桁のサイト内ダイヤルができなくなります。
*E.164	*12125551567	専用のビデオ ISDN ゲートウェイによるビデオ コールのダイヤル。アスタリスク（*）を使用して、数字（!）による他のダイヤル手順とは重複しない、特定のダイヤル手順を作成します。アスタリスク（*）の使用を避けるために、サイト間短縮アクセス コード 8 で始まる数字領域（8000-<E.164> など）を使用することもできます。

C：表 2-11　サポートされている数字でのダイヤル手順（続き）

ダイヤル パターン	例（サイト SJC）	接続先のタイプ
91-<10 digits>	914085554001（ネット上、SJC） 919195551001（ネット上、RTP） 912125551001（ネット外）	国内の接続先にダイヤルするための米国固有の PSTN ダイヤル手順。実装されたダイヤル プランにより、ダイヤル先がネット上の場合は、確実にそのコールがネット上にルーティングされます。ここで、先行する 9 は、米国で通常使用されている PSTN アクセス コードです。
9011-<E.164 number>	90114961007739764	海外の接続先にダイヤルするための米国特有の PSTN ダイヤル手順。実装されたダイヤル プランにより、ダイヤル先がネット上の場合は、確実にそのコールがネット上にルーティングされます。

一般的に、サポートされるダイヤル手順が少ないほど設計は簡易になります。設計プロセスの開始時にすべてのダイヤル手順を考慮することで、番号間タイムアウトにつながる任意の 2 種類のダイヤル手順の重複を確実に見つけて、ダイヤル プランの展開前にそれを解決できます。PSTN アクセス コード（上記のように米国では 9 が標準）を使用する主な理由は、他の (通常はネット上の) ダイヤル手順との重複を避けることです。

パーティション

エンタープライズ ダイヤル プランを作成するためにプロビジョニングされるパーティションおよび CSS を定義するときの目標の 1 つは、できるだけ重複設定を防ぐことです。この原則に従い、C：表 2-12 では、必要とされるグローバル パーティション（サイト別、国別ではない）を示します。

C：表 2-12　グローバル パーティション

パーティション	説明
DN	+E.164 電話番号すべてと、その他のローカルのオンネットの +E.164 接続先（PSTN から接続可能な代表番号など）を保持します。すべての +E.164 パターンは緊急パターンとしてプロビジョニングされます。
ESN	すべてのエンタープライズ固有番号（ESN）を保持します。これには ESN 電話番号（非 DID 電話など）と、DID のサイト間短縮ダイヤルから +E.164 へ変換するダイヤリング正規化トランスレーション パターンが含まれます。
PSTNInternational	海外の接続先への PSTN アクセスを提供するために必要な +E.164 ルート パターンを保持します。
URI	手動でプロビジョニングした URI を保持します。
onNetRemote	リモートのネット上の接続先のすべてのパターンを保持します。複数の Unified CM クラスタが存在する環境では、グローバル ダイヤル プラン レプリケーション（GDPR）を介して通知されるすべてのリモート番号の範囲が含まれます。

C：表 2-12　グローバル パーティション（続き）

パーティション	説明
B2B_URI	インターネットを使った business-to-business（B2B）の URI ダイヤルに必要な SIP ルート パターンを保持します。
Directory URI	自動生成されたすべての URI が置かれるシステム パーティション。このパーティションは作成不要です。ここでは、このパーティションの紹介をするために参考としてリストしています。このパーティションについては、このマニュアルの後半で再度使用します。

Directory URI 以外の C：表 2-12 にリストされたすべてのパーティションを作成する必要があります。これらのグローバル パーティションで表すパターン クラスに加えて、C：表 2-13 に示すような複数のサイト、国、またはサービス クラス固有のパターン クラスが必要です。

C：表 2-13　国またはサイト固有のパーティション

パーティション	説明
USPSTNNational	米国国内の接続先への PSTN アクセスを提供するために必要な +E.164 ルート パターンを保持します。他の国をサポートし、さらには他の国固有のダイヤル手順をサポートするには、当該国の xxPSTNNational パーティション（xx は国を表します。たとえば、DEPSTNNational、UKPSTNNational、ITPSTNNational などです）もプロビジョニングする必要があります。そのパーティションは、その国の国内接続先への PSTN アクセスを提供するために必要な +E.164 ルート パターンを保持します。 海外 PSTN アクセス（C：表 2-12 を参照）と国内 PSTN アクセスを区別する理由は、国内接続先だけを対象としたコールを許可するサービス クラスや、国内と海外の接続先を対象としたコールを許可するサービス クラスを区別して作成できなければならないからです。
USToE164	米国固有の PSTN ダイヤル手順（91-<*10 digits*> など）を +E.164 へ変換するためのダイヤリング正規化トランスレーション パターンを保持します他の国をサポートし、さらには他の国固有のダイヤル手順をサポートするには、当該国の xxToE164 パーティション（xx は国を表します。たとえば、DEToE164、UKToE164、ITToE164 などです）もプロビジョニングする必要があります。そのパーティションはその国固有の PSTN ダイヤル手順を +E.164 に変換するために必要なダイヤリング正規化トランスレーション パターンを保持します。
USEmergency	米国固有の緊急ダイヤル手順を使用する緊急コールへのアクセスを提供するために必要なルート パターンを保持します。
USPhLocalize	米国内で電話で +E.164 発呼側番号を短縮表示にローカライズするための発呼側トランスフォーメーション パターンを保持します。
<site>Intra	サイト固有のサイト内ダイヤリング。たとえば、SJCIntra などです。サイト固有のサイト内短縮ダイヤルを DID に、または非 DID を +E164 または ESN にそれぞれ変換するためのダイヤリング正規化パターンを保持します。
<site>PhLocalize	サイト固有です。たとえば、SJCPhLocalize などです。所定のサイトの電話で +E.164 発呼側番号を短縮表示にローカライズするための発呼側トランスフォーメーション パターンを保持します

緊急コールは国固有のダイヤル手順を使用して行われるため、緊急コールの米国のダイヤル手順を可能にするルート パターンを持つパーティション USEmergency も、国固有です。他のダイヤリング ドメイン（国）もサポートするには、それらの他のダイヤリング ドメインに相当するパーティション（DEEmergency：ドイツ、ITEmergency：イタリア、DEPhLocalize：ドイツ、ITPHLocalize：イタリアなど）を作成する必要があります。

ダイヤリング正規化トランスレーション パターン

C：表 2-14 は、前の項で説明したパーティションを使用してどのダイヤリング正規化トランスレーション パターンをプロビジョニングする必要があるかをまとめています。すべてのダイヤリング正規化トランスレーション パターンは、緊急パターンとしてプロビジョニングされ、[発信側コーリングサーチスペースを使用（Originator's Calling Search Space）] が設定されています（パーティション項を参照）。これにより、ダイヤリング正規化トランスレーション パターンで定義された着信側トランスフォーメーションを適用した後に、元の CSS を使用してダイヤル先の最終的な一致を検出できます。

C：表 2-14　ダイヤリング正規化トランスレーション パターンの概要

パーティション	パターン	着信側トランスフォーメーション マスク	注
ESN	81404XXX	+14085554XXX	サイト SJC のサイト間短縮ダイヤル
ESN	81975XXX	+19725555XXX	サイト RCD のサイト間短縮ダイヤル
ESN	81911XXX	+19195551XXX	サイト RTP のサイト間短縮ダイヤル
SJCIntra	4XXX	+14085554XXX	SJC でのサイト SJC から DID へのサイト内短縮ダイヤル
SJCIntra	5XXX	81405XXX	SJC でのサイト SJC から非 DID へのサイト内短縮ダイヤル
RCDIntra	5XXX	+19725554XXX	RCD でのサイト RCD から DID へのサイト内短縮ダイヤル
RCDIntra	6XXX	81976XXX	RCD でのサイト RCD から非 DID へのサイト内短縮ダイヤル
RTPIntra	1XXX	+19195551XXX	RTP でのサイト RTP から DID へのサイト内短縮ダイヤル
RTPIntra	2XXX	81912XXX	RTP でのサイト RTP から非 DID へのサイト内短縮ダイヤル
UStoE164	9.1 [2-9]XX [2-9]XX XXXX	マスクなし、ドットの前の番号を削除して、先頭に + を付加	米国内の接続先の米国固有の PSTN ダイヤル手順
UStoE164	9011.!#	マスクなし、ドットの前の番号を削除して、先頭に + を付加	米国内の接続先の米国固有の PSTN ダイヤル手順。
UStoE164	9011.!	マスクなし、ドットの前の番号を削除して、先頭に + を付加	米国内の接続先の米国固有の PSTN ダイヤル手順 注　これは、[後続のホップで番号間タイムアウトを待機しない（Do Not Wait For Interdigit Timeout On Subsequent Hops）] が設定されない唯一のパターンです。

米国以外のダイヤリング ドメインの場合、インストールでそうした国固有のダイヤル手順をサポートする必要があるなら、他の国固有のダイヤリング正規化トランスレーション パターンを定義しなければなりません。C：表 2-15 に、例としてドイツ（DE）とイタリア（IT）に必要なダイヤリング正規化を示します。

C：表 2-15　ドイツとイタリアのダイヤリング正規化

パーティション	パターン	着信側トランスフォーメーション	注
DEtoE164	000.!	ドットの前の番号を削除して、先頭に + を付加	ドイツ：国際コール（000-E.164）。 注　[後続のホップで番号間タイムアウトを待機しない（Do Not Wait For Interdigit Timeout On Subsequent Hops）] が設定されません。
DEtoE164	000.!#	ドットの前の番号と後続 # を削除して、先頭に + を付加	ドイツ：国際コール（000-E.164）。
DEtoE164	00.[^0]!	ドットの前の番号を削除して、先頭に +49 を付加	ドイツ：国内コール（00- 国内番号）。 注　ドイツの番号計画は可変長であり、このパターンはこれを対象にする必要があります。 注　[後続のホップで番号間タイムアウトを待機しない（Do Not Wait For Interdigit Timeout On Subsequent Hops）] が設定されません。
DEtoE164	00.[^0]!#	ドットの前の番号と後続 # を削除して、先頭に +49 を付加	ドイツ：国内コール（00- 国内番号）。
ITtoE164	000.!	ドットの前の番号を削除して、先頭に + を付加	イタリア：国際コール（000-E.164）。 注　[後続のホップで番号間タイムアウトを待機しない（Do Not Wait For Interdigit Timeout On Subsequent Hops）] が設定されません。
ITtoE164	000.!#	ドットの前の番号と後続 # を削除して、先頭に + を付加	イタリア：国際コール（000-E.164）
ITtoE164	0.0[^0]!	ドットの前の番号を削除して、先頭に +39 を付加	イタリア：国内コール（0- 国内番号（NSN）、NSN は 0 で始まる）。 注　イタリアの番号計画は可変長であり、このパターンはこれを対象にする必要があります。 注　[後続のホップで番号間タイムアウトを待機しない（Do Not Wait For Interdigit Timeout On Subsequent Hops）] が設定されません。
ITtoE164	0.0[^0]!#	ドットの前の番号と後続 # を削除して、先頭に +39 を付加	イタリア：国内コール（0-NSN、NSN は 0 で始まる）。

C：表 2-15　ドイツとイタリアのダイヤリング正規化（続き）

パーティション	パターン	着信側トランスフォーメーション	注
ITtoE164	0.[^0]!	ドットの前の番号を削除して、先頭に +39 を付加	イタリア：国内コール（0-NSN、NSN は 0 で始まらない）。 注　イタリアの番号計画は可変長であり、このパターンはこれを対象にする必要があります。 注　[後続のホップで番号間タイムアウトを待機しない（Do Not Wait For Interdigit Timeout On Subsequent Hops）] が設定されません。
ITtoE164	0.[^0]!#	ドットの前の番号と後続 # を削除して、先頭に +39 を付加	イタリア：国内コール（0-NSN、NSN は 0 で始まらない）。

C：表 2-15 の例は、イタリアとドイツではエンタープライズ内部からトランクにアクセスするのに ITU が推奨する 0 が使用され、次に国内および国際アクセスに 0 および 00 が使用されていることを示しています。1998 以降、イタリアの地域番号は 0 で始まり、1 から 9 の数字が国内番号の最初の数字として、番号のさまざまな種類を示します。したがって、2 個のゼロ（00）で始まるダイヤル番号は、ドイツとイタリアでは異なる処理をする必要があります。イタリアでは 2 番目のゼロは NSN の一部であると見なさなければならず、したがって +E.164 数字列に残しておく必要がありますが、ドイツでは地域番号がゼロで始まらないため、ドイツの 2 番目のゼロは削除する必要があります。

これら 2 つの国に必要なダイヤリング正規化の例は、提示する設計方法で国固有のダイヤル手順をどのようにモデル化できるかを示しています。

国際番号計画の詳細については、ITU-T の「*International Numbering Resources*」ページ（https://www.itu.int/en/ITU-T/inr/Pages/default.aspx）を参照してください。このページには、E.164 国コードおよび国内番号計画を含むさまざまなリソースへのリンクがあります。さまざまな国で使用されているダイヤル手順の概要は、「*Operational Bulletin No.994 (15.XII.2011) and Annexed List: Dialling procedures (international prefix, national (trunk) prefix and national (significant) number) (in accordance with ITU-T Recommendation E.164 (11/2010)) (Position on 15 December 2011)*」（https://www.itu.int/pub/T-SP-OB.994-2011）にあります。実際のダイヤル手順のリストはその文書の 25 ページから始まっています。また、https://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-E.164C-2011-PDF-E.pdf からもダウンロード可能です。

サービス クラスとコーリング サーチ スペース（CSS）

前述のように、CSS は、CSS を使用する発呼側エンティティがアクセスできるパーティションやパターンを定義するパーティションのリストです。このマニュアルでは、サービス クラスを定義する回線 CSS だけを使用するダイヤル プラン方法を使います。

C：表 2-16 に、この設計で検討するサービス クラスをリストします。この設計のために選択したサービス クラスは例にすぎません。さらにサービス クラスが必要な場合は、同じように定義できます。

Tip

サービス クラスの数は、エンタープライズ ダイヤル プランの設計の複雑さを決める重要なパラメータの 1 つです。したがって、ダイヤル プランに定義するサービス クラスの数をできる限り少なくすることが肝要です。

推奨される設計では、サービス クラスを定義するために、回線にプロビジョニングされる CSS のみを利用し、デバイス CSS を使用しません。デバイス CSS は、誰にでも利用できることが必要な一般的なダイヤル手順を実装するために使用できます。この例として緊急コールがあります。デバイス CSS を使用して緊急コールを実装する場合の詳細については、多国間環境における緊急コールの考慮事項を参照してください。

C：表 2-16　サービス クラス

サービス クラス	アクセス先
国際	すべてのネット上の接続先 国内の PSTN 接続先 国際 PSTN 接続先 Business-to-business URI ダイヤリング 緊急コール
国内	すべてのネット上の接続先 国内の PSTN 接続先 緊急コール
内線	すべてのネット上の接続先 緊急コール

International サービス クラスだけに business-to-business URI ダイヤリングを追加することは、business-to-business（B2B）コールが限られたエッジ リソースを消費するという前提に基づいた例です。また、International、InternationalB2B、National、NationalB2B、Internal、および InternalB2B のサービス クラスを導入することによって、サービス クラスの数の倍増を避けようとしています。

所定の発信者が利用できるサービス クラスとダイヤル手順セットの両方を定義するために回線 CSS だけを使用するため、サイトごと、サービス クラスごとに、CSS をプロビジョニングする必要があります。

C：表 2-17 に、以前に定義したパーティション セット（C：表 2-12 および C：表 2-13 を参照）に基づいてサービス クラス International をサイト SJC のユーザに対して定義する方法を示します。

C：表 2-17　SJC ユーザ用のサービス クラス International

CSS 名	パーティション
SJCInternational	DN Directory URI URI ESN onNetRemote SJCIntra UStoE164 USPSTNNational PSTNInternational B2B_URI USEmergency

C：表 2-18 に示すように、残りのサービス クラスは B2B URI ダイヤリング、国際、および国内 PSTN 接続先へのアクセスを選択的に削除することにより、同じように作成できます。

C：表 2-18　SJC ユーザ用のサービス クラス National および Internal

CSS 名	パーティション
SJCNational	DN Directory URI URI ESN onNetRemote SJCIntra UStoE164 USPSTNNational USEmergency

CSS 名	パーティション
SJCInternal	DN Directory URI URI ESN onNetRemote SJCIntra UStoE164 USEmergency

他のサイトのユーザ用のサービス クラスの CSS は上述の CSS と同様に作成しますが、サイト固有のダイヤリング正規化パターンと共に使用するパーティションが異なる点だけが違います。C：表 2-19 に、RTP サイトの National および Internal サービス クラスの例を示します。

C：表 2-19　RTP ユーザ用のサービス クラス National および Internal

CSS 名	パーティション
RTPNational	DN Directory URI URI ESN onNetRemote RTPIntra UStoE164 USPSTNNational USEmergency

CSS 名	パーティション
RTPInternal	DN Directory URI URI ESN onNetRemote RTPIntra UStoE164 USEmergency

これらの例は、選択したパーティション方式により、複数サイトのサービス クラスを実装する CSS を作成する際に、パターンとパーティションの理想的な再利用が可能になることをはっきり示しています。

他のダイヤリング ドメイン（国）の場合、上記に示すのと同じ CSS とパーティション方式を利用できますが、上記で使用される米国パーティションの代わりに、特定のダイヤリング ドメインのダイヤリング正規化パーティションおよび国内の PSTN 接続先への国固有のルートを使用する点のみが違います。たとえば、C：表 2-20 はドイツ（DE）のサイト FRA のサービス クラス International の CSS を示しています。

C：表 2-20　ドイツ（DE）のサイト FRA のユーザ用のサービス クラス International

CSS 名	パーティション
FRAInternational	DN Directory URI URI ESN onNetRemote FRAIntra DEtoE164 DEPSTNNational PSTNInternational B2B_URI DEEmergency

特殊な CSS

ユーザ向けサービス クラスのほかに、コーリング サーチ スペース（CSS）は Cisco Unity Connection など、トランクを通じて接続されるアプリケーションのサービス クラスの定義にも使用されます。Unity Connection がネット上の接続先にのみアクセスでき、ESN および +E.164 ダイヤリング以外に Unity Connection からの米国ダイヤル手順もサポートされることを前提として、C：表 2-21 は、このサービス クラスを実装する CSS を示しています。

C：表 2-21　ボイスメールのサービス クラス

CSS 名	パーティション
VoiceMail	DN ESN URI onNetRemote Directory URI UStoE164

Cisco Unity Connection が複数の国で提供される必要があるシナリオでは、上記の例のパーティション UStoE164 で定義された国固有のダイヤリング正規化の実装はオプションではありません。この場合にサポートできるダイヤル手順は、グローバルで有効なダイヤル手順である ESN と +E.164 だけです。

Unified CM プレゼンスを使用するには、プレゼンス ユーザのサブスクライブ先のすべてのプレゼンティティへのアクセスができるように、何よりもサブスクライブ CSS をプロビジョニングする必要があります。プレゼンス アクセスのさらなる差別化をせずに Unified CM プレゼンスのプロビジョニングを簡素化ができるようにするには、考えられるすべてのネット上の接続先へのアクセスが可能な単一の CSS をプロビジョニングする必要があります。C：表 2-22 は、このデフォルトのサブスクライブ CSS の設定を示しています。

C：表 2-22　デフォルトのサブスクライブ CSS

CSS 名	パーティション
DefaultSubscribe	DN ESN URI onNetRemote Directory URI

このサブスクライブ CSS は、すべてのタイプのネット上の接続先へのアクセスを保証します。

C：表 2-23 に、PSTN トランクでの着信 CSS として使用される（平易な）CSS「DN」を示します。ループを回避するため、PSTN トランクは +E.164 電話番号だけに接続できます。PSTN がサポートする番号方式は 1 つだけで、それが着信時に +E.164 に正規化されるため、PSTN トランクは ESN パターン、ダイヤリング正規化パターン、または URI にアクセスする必要がなくなります。

C：表 2-23　PSTN ゲートウェイ用の着信 CSS

CSS 名	パーティション
DN	DN

C：表 2-24 に、他の Unified CM クラスタへのトランクの着信 CSS として使用される CSS ICTInbound を示します。ループを回避するため、これらのクラスタ間トランクの着信 CSS は、リモートのネット上接続先（パーティション onNetRemote）へのアクセスを提供すべきではありませんが、トランク（着信 CSS）はネット上のすべての有効なアドレッシング モード（+E.164、ESN、URI）をサポートする必要があります。ダイヤリング正規化は、この CSS の一部ではありません。コールが着信クラスタ間トランクに着信する前に、+E.164 および ESN 以外のダイヤル手順はリモートの Unified CM クラスタで +E.164 または ESN に正規化されているはずだからです。

C：表 2-24　他の Unified CM クラスタへのトランク用の着信 CSS

CSS 名	パーティション
ICTInbound	DN ESN URI Directory URI

コール タイプ固有の発信ゲートウェイを選択するためのローカル ルート グループ

発信側デバイスに基づいて柔軟な出口ゲートウェイ選択ができるように、ローカル ルート グループ（LRG）の使用が推奨されます。出口ゲートウェイの選択に LRG を使用すると、サイト固有のルート パターンが不要になります。

異なるコール タイプについて別々の LRG を選択できるようにするには、C：表 2-25 に示すように複数の LRG 名を設定します。

C：表 2-25　ローカル ルート グループ名

ローカル ルート グループ名	説明
LRG_PSTN_1	PSTN コールに使用されるプライマリ PSTN リソースを参照するローカル ルート グループ
LRG_PSTN_2	PSTN コールに使用されるセカンダリ PSTN リソースを参照するローカル ルート グループ
LRG_VIDEO_1	PSTN ビデオ コールに使用されるプライマリ PSTN リソースを参照するローカル ルート グループ
LRG_VIDEO_2	PSTN ビデオ コールに使用されるセカンダリ PSTN リソースを参照するローカル ルート グループ

C：表 2-25　ローカル ルート グループ名（続き）

ローカル ルート グループ名	説明
LRG_Emergency_1	緊急コールに使用されるプライマリ PSTN リソースを参照するローカル ルート グループ
LRG_Emergency_2	緊急コールに使用されるセカンダリ PSTN リソースを参照するローカル ルート グループ

これらの LRG 定義により、緊急コールと通常の PSTN コールに別々の PSTN リソース（ゲートウェイ）を使用できるように、「通常の」PSTN コールと緊急コールの両方についてそれぞれ専用のルート リストを作成できます。これは、一元化された PSTN リソースが通常の PSTN コールのためにプロビジョニングされているものの、適切な Public Safety Answering Point（PSAP）へローカルの緊急コールをルーティングできるように、緊急コールがローカル サイトの小さな専用ゲートウェイを依然として使用する必要があるような状況で役立ちます。

ビデオ LRG はビデオ対応の ISDN ゲートウェイ用にプロビジョニングされ、別のリソースとして扱われます。

ローカル ルート グループを使用するルート リスト

前の項で定義した LRG を使用して、C：表 2-26 に示すようにルート リストを作成する必要があります。

C：表 2-26　ルート リストの定義

ルート リスト	メンバー	説明
RL_PSTN	LRG_PSTN_1 LRG_PSTN_1 標準ローカル ルート グループ	通常の PSTN コールは、通常の PSTN コール用に定義されたサイト固有のプライマリおよびセカンダリ PSTN リソースを使用しなければなりません。最後のメンバーである標準ローカル ルート グループは、コール タイプ固有ではない PSTN リソースへのフォールバックが可能です。
RL_Emergency	LRG_Emergency_1 LRG_Emergency_2 LRG_PSTN_1 LRG_PSTN_1 標準ローカル ルート グループ	緊急コールの場合、緊急コール用の最初のコール固有リソースを使用し、次に 2 番目の固有リソースを、その後に通常の PSTN コールに定義された PSTN リソースを、最後に固有ではない PSTN リソースを使用する必要があります。
RL_VIDEO	LRG_VIDEO_1 LRG_VIDEO_2 LRG_PSTN_1 LRG_PSTN_2 標準ローカル ルート グループ	ビデオ コールの場合、最初にビデオ固有のゲートウェイ リソースを使用し、次の正規の PSTN リソースをフォールバック（音声のみ）として検討し、最後に、他のリソースが失敗した場合に標準ローカル ルート グループが使用されます。

各デバイス プールの上記の LRG およびルート リスト定義により、定義済みの LRG 対して最大 7 つのルート グループを選択でき、非常に限定した発信ゲートウェイ選択が可能になります。あるコール タイプに使用される実際の PSTN リソースは、デバイス プールのプロビジョニング

中に定義されます。所定のデバイス セットについてコール タイプに基づく異なる発信 PSTN リソースの選択が不要で、すべてのコール タイプについて PSTN リソースが 1 つしか必要ではない場合、それぞれのデバイス プールに標準ローカル ルート グループの実際のルート グループだけを定義し、そのデバイス プール セットの他のすべての LRG は <None> に設定されたままにしておくだけで十分です。　すべてのルート リストで [標準ローカルルートグループ（Standard Local Route Group）] を最後のエントリにすることでできます。

PSTN アクセスと緊急コールのルート パターン

PSTN アクセスは PSTN ルート パターンにより実現します。サービス クラスとコーリング サーチ スペース（CSS）で説明したように、PSTNInternational パーティションでは国際接続先へのルートをプロビジョニングする必要がある一方で、ダイヤリング ドメイン固有パーティション xxPSTNNational（xx は、USPSTNNational のように、ダイヤリング ドメインを表します）では国内 PSTN ルートがプロビジョニングされます。C：表 2-27 に、設定済みの PSTN ルート パターンを示します。

C：表 2-27　PSTN ルート パターン

パターン	パーティション	ゲートウェイまたはルート リスト	説明
\+!	PSTNInternational	RL_PSTN	任意の国際接続先にダイヤルできる可変長番号。
\+!#	PSTNInternational	RL_PSTN	可変長のダイヤルを # で終わらせることができるようにするための、国際接続先の代替パターン。 [番号の削除（Discard Digits）] を [末尾番号（Trailing-#）] **に設定。**
\+1.[2-9]XX[2-9]XX XXXX	USPSTNNational	RL_PSTN	米国の国内接続先用の明示的なパターン。 国際接続先用に定義された可変長の PSTN ルート パターン \+! との重複を避けるために、[緊急優先（Urgent Priority）] がオンになります。
911	USEmergency	RL_Emergency	米国の緊急コール [緊急優先（Urgent Priority）] をチェックします
9911	USEmergency	RL_Emergency	米国の緊急コール [緊急優先（Urgent Priority）] をチェックします

C：表 2-27 に明示的に示したルート パターン設定以外のすべてのその他の設定は、C：表 2-28 に示すデフォルト値のまま残します。これには特に、空白のまま残す発呼側、接続先、着信側のトランスフォーメーションが含まれます（前述の末尾番号の削除を除く）。PSTN 要件に合致することが必要な発呼側および着信側のトランスフォーメーションは、明示的な発呼側および着信側トランスフォーメーションとして設定されるからです。これは、アウトバウンド コール：ISDN ゲートウェイでの着信者番号と発信者番号のトランスフォーメーションおよびアウトバウンド コール：SIP トランクでの着信者番号および発信者番号のトランスフォーメーションで説明されています。

C：表 2-28　ルート パターンのデフォルト設定

設定	値
[パターン定義（Pattern Definition）]	
[番号計画（Numbering Plan）]	-- 選択しない --
[ルートフィルタ（Route Filter）]	< なし >
[MLPP 優先度（MLPP Precedence）]	[デフォルト（Default）]
[ブロックコール率の適用（Apply Call Blocking Percentage）]	オフ
[リソースプライオリティネームスペース ネットワークドメイン（Resource Priority Namespace Network Domain）]	< なし >
[ルートクラス（Route Class）]	[デフォルト（Default）]
[ルートオプション（Route Option）]	[このパターンをルーティング（Route this pattern）]
[コールの分類（Call Classification）]	[オフネット（OffNet）]
[外部コール制御プロファイル（External Call Control Profile）]	< なし >
[デバイスの上書きを許可（Allow Device Override）]	オフ
[外部ダイヤルトーンの提供（Provide Outside Dial Tone）]	オン
[オーバーラップ送信を許可（Allow Overlap Sending）]	オフ
[強制承認コードが必須（Require Forced Authorization Code）]	オフ
[承認レベル（Authorization Level）]	[0]
[クライアント識別コードの要求（Require Client Matter Code）]	オフ
[発呼側トランスフォーメーション（Calling Party Transformations）]	
[発呼側の外線電話番号マスクを使用（Use Calling Party's External Phone Number Mask）]	オフ
[発呼側トランスフォーメーション マスク（Calling Party Transform Mask）]	空白のままにします。値は何も入力しないでください。
[プレフィックス番号（発信コール）（Prefix Digits (Outgoing Calls)）]	空白のままにします。値は何も入力しないでください。
[発呼者回線 ID の表示（Calling Line ID Presentation）]	デフォルト（Default）
発呼者名の表示（Calling Name Presentation）	[デフォルト（Default）]
[発呼側番号タイプ（Calling Party Number Type）]	[Cisco CallManager]
[発呼側番号計画（Calling Party Numbering Plan）]	[Cisco CallManager]

C：表 2-28　ルート パターンのデフォルト設定（続き）

設定	値
[接続側トランスフォーメーション（Connected Party Transformations）]	
[接続側回線 ID の表示（Connected Line ID Presentation）]	デフォルト（Default）
接続先名の表示（Connected Name Presentation）	[デフォルト（Default）]
[着信側トランスフォーメーション（Called Party Transformations）]	
[番号の削除（Discard Digits）]	< なし >
[着信側トランスフォーメーションマスク（Called Party Transform Mask）]	空白のままにします。値は何も入力しないでください。
[プレフィックス番号（発信コール）（Prefix Digits (Outgoing Calls)）]	空白のままにします。値は何も入力しないでください。
[着信側番号タイプ（Called Party Number Type）]	[Cisco CallManager]
[着信側番号計画（Called Party Numbering Plan）]	[Cisco CallManager]
[ISDN ネットワーク固有ファシリティの情報要素（ISDN Network-Specific Facilities Information Element）]	
[ネットワークサービスプロトコル（Network Service Protocol）]	-- 選択しない --
[通信事業者識別コード（Carrier Identification Code）]	空白のままにします。値は何も入力しないでください。
[ネットワーク サービス（Network Service）]	-- 選択しない --

パーティション PSTNInternational の PSTN 国際ルート パターンはダイヤリング ドメイン（国）固有ではありませんが、パーティション USPSTNNational および USEmergency のルート パターンは国固有です。ダイヤル プランで他の国をサポートしなければならない場合は、C：表 2-29 に示すように、それらの国のルート パターンを作成する必要があります。

C：表 2-29　国内接続先用の米国以外のルート パターン

パターン	パーティション	ゲートウェイまたはルート リスト	説明
\+49!	DEPSTNNational	RL_PSTN	国コード 49 を持つドイツの番号計画が可変長のため、可変長。
\+49!#	DEPSTNNational	RL_PSTN	可変長のダイヤルを # で終わらせることができるようにするための、国内接続先の代替パターン。 [番号の削除（Discard Digits）] を [末尾番号（Trailing-#）] に設定。
\+33XXXXXXXXX	FRPSTNNational	RL_PSTN	フランスの国内接続先用の明示的パターン。 国際接続先用に定義された可変長の PSTN ルート パターン \+! との重複を避けるために、[緊急優先（Urgent Priority）] がオンになります。
112	DEEmergency	RL_Emergency	ドイツの緊急コール [緊急優先（Urgent Priority）] をチェックした
0112	DEEmergency	RL_Emergency	ドイツの緊急コール [緊急優先（Urgent Priority）] をチェックした
112	FREmergency	RL_Emergency	フランスの緊急コール [緊急優先（Urgent Priority）] をチェックした
0112	FREmergency	RL_Emergency	フランスの緊急コール [緊急優先（Urgent Priority）] をチェックした

C：表 2-29 に、固定長と可変長の番号計画の違いを示します。ドイツの国内番号計画は可変長なので、ドイツの国内接続先に一致させるルート パターンは可変長の数字列に一致する必要があります。また、ユーザが電話番号を明示的に # で終わらせることができるように、# で終わる代替ルート パターンをプロビジョニングして、国内接続先にダイヤルする際の番号間タイムアウトを回避する必要もあります。これとは対照的に、フランスの国内番号計画は固定長（米国と同じ）なので、1 つの固定長の緊急用ルート パターンでフランスの全国内番号をカバーできます。

ドイツとフランスは同じ緊急ダイヤル手順を使用するため、緊急用パーティション DEEmergency および FREmergency の両方を組み合わせて 1 つのパーティション 112Emergency とし、CSS 定義で代わりにそのパーティションを使用することにより、緊急用ルーティングを簡素化することができます。

多国間環境における緊急コールの考慮事項

個々のサービス クラスとは独立して、全エンドポイントから常時緊急番号へアクセスできることが必要です。前述のように、これは緊急コール ルート パターンを持つパーティションをすべての CSS に追加することで、簡単に実現します。この方法で問題が生じるのは、複数の国をサポートしなければならず、それらの国で異なる緊急ダイヤル手順が必要であり、エクステンション モビリティやデバイス モビリティなどのモビリティ機能が使用される場合です。

そのような場合、異なる緊急ダイヤル手順のある複数の国の間でユーザがローミングを行うと、このユーザが使用しているデバイスはアクセス中のユーザが使用する緊急ダイヤル手順を継承します。たとえば、ドイツのユーザがアメリカの電話にログインすると、ドイツ人ユーザのエクステンション モビリティ プロファイルで定義された回線 CSS が、アクセス先であるアメリカの電話に割り当てられ、この電話で緊急コールを発信するにはドイツの緊急電話番号 112 を使用しなければならず、米国の緊急コールのダイヤル手順 911 はサポートされなくなれます。

外国人ユーザが電話にログインするかどうかに関わらず、任意の国の電話が常にその国の国内緊急コールのダイヤル手順をサポートするように、緊急コール用に異なる方式を実装できます。USEmergency をすべての CSS に追加する代わりに、専用の USEmergency CSS を作成し、その CSS を米国のすべてのデバイスにデバイス CSS として割り当てます。こうすると、外国人ユーザが米国の電話にログインした場合に、回線 CSS により定義されたアクセス中のユーザの「ホーム」ダイヤル手順が、アクセス先の国の緊急ダイヤル手順と結びつきます。ドイツ人ユーザが米国の電話にログインする上記のケースでは、そのユーザのドイツ式 PSTN ダイヤル手順は、米国固有の緊急ダイヤル手順 911 と一緒にサポートされるようになります。異なる国間でのこうしたダイヤル手順の組み合わせにより、アクセス先の緊急ダイヤル手順とアクセス中のユーザの通常のダイヤル手順との間に重複が生じる可能性があることを念頭に置く必要があります。たとえば、ドイツのサイトが 9 で始まる 4 桁の内線番号を持つ場合（+E.164 範囲が +49 6100 773 9XXX など）、そのドイツのサイトのユーザが米国の電話にログインすると、9XXX ダイヤリング正規化トランスレーション パターンによりそのサイトに定義された 4 桁のサイト内短縮ダイヤルが、米国緊急ダイヤル 911 と重複してしまいます。緊急ダイヤル手順がより固有である限り、緊急パターンとして緊急コール ルート パターンを作成することにより、緊急コールをかけるときに遅滞が生じないことが保証されます。一方で、911 の米国緊急パターンは 911 で始まるすべての 4 桁のダイヤルを「ブロック」する可能性があり、これにより、例えば +49 6100 773 911X などの電話番号への 4 桁のサイト内のダイヤルに影響を与えることがあります。

緊急ダイヤルを回線 CSS からデバイス CSS に移動すると、アクセス中のユーザの緊急ダイヤル手順（ドイツ人ユーザの場合は 112）をアクセス先の国の緊急ダイヤル手順（米国の場合は 911）に変換しなければならないという問題も回避できます。

ビデオ PSTN（ISDN）コールのルート パターン

コスト面から見て、通常のボイスコールに ISDN ビデオ ゲートウェイを使用することは実現不可能なため、ダイヤル プランの観点からビデオ用の ISDN ゲートウェイに特別の処理が必要です。この設計では、ビデオ ISDN ゲートウェイの選択を、特別なビデオ PSTN ダイヤル手順に明示的に結びつけます（C：表 2-11 を参照）。C：表 2-30 に、このダイヤル手順を有効にするために必要なルート パターンを記載します。

C：表 2-30　ビデオ PSTN（ISDN）コールのルート パターン

パターン	パーティション	ゲートウェイまたはルート リスト	説明
*!	PSTNInternational	RL_VIDEO	* で表された E.164 をサポートする必要があるため、可変長。
*!#	PSTNInternational	RL_VIDEO	# を使用した可変長のダイヤルを終了できるようにするための代替パターン。 [番号の削除（Discard Digits）] を [末尾番号（Trailing-#）] **に設定。**
*1XXXXXXXXXX	PSTNInternational	RL_VIDEO	番号間タイムアウトを発生させずに米国の着信先（固定長）にダイヤルできるようにするための補足ルート パターン。 [緊急優先（Urgent Priority）] をオンに設定。

ビデオ ISDN ルート パターンをパーティション PSTNInternational に含めると、実質的に「国際」サービス クラスにビデオ ダイヤル機能が追加されます。

アウトバウンド コール：ISDN ゲートウェイでの着信者番号と発信者番号のトランスフォーメーション

ISDN トランクでは、発信側番号および着信側番号の情報が、発信側および着信側の情報要素で送受信されます。これらの情報要素は、番号計画、番号タイプ、および番号の 3 つで構成されます。これらのフィールドをどのように設定しなければならないかは、プロバイダのトランク サービス定義に依存します。一例として、ドイツ国内の同じ市外局番 6100 内のトランクにある E.164 着信番号 4961007739764 へのコールの場合、発信 ISDN SETUP メッセージに含まれる着信側番号は、（番号計画 / タイプ / 番号の形式で）「ISDN/national/61007739764」、「ISDN/subscriber/7739764」、または「unknown/unknown/061007739764」として送信される場合があります。

ISDN トランクの終端となるゲートウェイが SIP を使用して Unified CM に接続されている場合、SIP は番号タイプの概念を把握しないため、番号タイプを Unified CM からゲートウェイに送信することはできません。コールのタイプによって異なる ISDN 番号タイプをサポートする必要があるかどうかは、プロバイダの SIP トランク サービス定義によって決まります。ISDN トランクでは、一部のプロバイダは常に、着信先にかかわらず、同じ ISDN 計画およびタイプのインジケータを使用した着信側番号と発信側番号の送信を許可します。

C：表 2-31 に、米国の ISDN プロバイダが許容する可能性のある代替着信側番号形式の例を記載します。

C：表 2-31　米国 ISDN トランクでのコールの代替 ISDN 番号形式

コールのタイプ	接続先	PSTN に送信される着信側の番号計画 / タイプ / 番号	ゲートウェイに送信される数字列
国内	+12125551234	unknown/unknown/12125551234	*12125551234
国際	+4961007739764	unknown/unknown/0114961007739764	*0114961007739764

ゲートウェイに送信される数字列の先頭には、ゲートウェイでのダイヤルピア定義を簡略化したプレフィックス「*」が付加されます。PSTN から受信する着信側番号が「*」で始まることは決してありません。したがって、ゲートウェイに送信する着信側番号にプレフィックス「*」を使用することで、インバウンド コールとアウトバウンド コールに関して、簡単で競合のない宛先パターンに基づいたアウトバウンド ダイヤルピアの選択がゲートウェイで可能です。コールを PSTN に送信する前に、Unified CM によって先頭に付加された「*」をゲートウェイで削除する必要があります。Unified CM からゲートウェイに送信されるすべての着信側番号で、先頭に「*」を使用すると、ゲートウェイで POTS ダイヤルピアに対して「宛先パターン *」を使用することが可能になります。この場合、先頭の「*」は、Cisco IOS のデフォルトでの桁削除動作により自動的に削除されます。

着呼側の +E.164 着信番号から PSTN に送信される数字列へのトランスフォーメーションは、Unified CM で行うことができます。ゲートウェイでは、C：例 2-2 に記載する Cisco IOS Voice トランスレーション ルールを使用して、簡単に ISDN 計画およびタイプを適用できます。

C：例 2-2　単一の ISDN 計画およびタイプを適用する Cisco IOS Voice トランスレーション

```
voice translation-rule 1
    rule 1 /^\*/ // type any unknown plan any unknown
    rule 2 // // type any unknown plan any unknown
voice translation-profile ISDNunknown
    translate called 1
    translate calling 1
dial-peer voice 1 pots
    translation-profile outgoing ISDNunknown
```

C：例 2-2 に記載されている、Cisco IOS 設定の抜粋には、特定の POTS ダイヤルピアから PSTN に送信される発信側と着信側の情報に単一の ISDN 計画およびタイプを適用する方法が示されています。voice-translation-rule 1 のルール 1 は、「*」で始まるすべての番号に一致し、この先頭の「*」を除去します。voice translation-rule 1 のルール 2 は、任意の計画およびタイプのすべての番号に一致し、計画とタイプの両方を「unknown」に強制する一方で、番号の実際の数字列は変更しません。ISDN を指す POTS ダイヤルピアに、この Cisco IOS Voice トランスレーション ルールを適用することで、計画とタイプが「unknown」に強制された上で、Unified CM からゲートウェイに送信されるすべての着信側番号と発信側番号が変更されずに PSTN に転送されます。

このトランスレーション ロジックをゲートウェイに設定した場合、Unified CM 側では、+E.164 着信側情報を C：表 2-31 に従った数字列に変換してから PSTN に送信するようにプロビジョニングする必要があります。表 24 に、ISDN ダイヤル用に +E.164 をローカライズするために必要な着信側トランスフォーメーション パターンを記載します。

C：表 2-32　SIP を使用した ISDN 用に +E.164 をローカライズするための着信側トランスフォーメーション パターン

パターン	パーティション	トランスフォーメーション	説明
\+.1!	USGWLocalizeCd	ドットの前の番号を削除して、先頭に * を付加	+12125551234 –> *12125551234
\+.!	USGWLocalizeCd	ドットの前の番号を削除して、先頭に *011 を付加	+4961007739764 –> *0114961007739764

C：表 2-32 に記載されている着信側トランスフォーメーション パターンで定義された着信側トランスフォーメーションをゲートウェイに適用するには、まず、USGWLocalizeCd パーティションだけを設定した CSS USGWLocalizeCd を定義します。そして、ゲートウェイのデバイス プールの [デバイスモビリティ関連情報（Device Mobility Related Information）] セクションで、その CSS を [着信側トランスフォーメーション CSS（Called Party Transformation CSS）] として設定します。これらのトランスフォーメーションをデバイス プールに設定すれば、同じ着信側トランスフォーメーション要件を共有する同じサイト内の複数のゲートウェイで、これらの同じ設定を共有することができます。それには、ゲートウェイ設定ページの [アウトバウンドコール（Outbound Calls）] セクションで、[デバイスプールの着信側トランスフォーメーション CSS を使用（Use Device Pool Called Party Transformation CSS）] オプションをオンにする必要があります。

また、必要なプロビジョニングとして、+E.164 からサービス プロバイダへ送信しなければならない形式への発信側番号のトランスフォーメーションを行います。ここで、非 DID から発信されるコール、または特定のゲートウェイに関連付けられた DID 範囲に含まれない DN から発信されるコールの発信側情報を処理する方法を検討する必要があります。最も一般的な選択肢は、発信者 ID をサイト固有の主要な内線番号に設定することです。このサイトでは特に、C：表 2-33 に記載するサイト固有の発信側トランスフォオーメーションを作成する必要があります。

C：表 2-33　SIP を使用した ISDN 用に +E.164 をローカライズするための発信側トランスフォーメーション パターン

パターン	パーティション	トランスフォーメーション	説明
\+.19195551XXX	RTPGWLocalizeCn	ドットの前の番号を削除	+19195551001 –> 19195551001 ゲートウェイに関連付けられた DID 範囲の発信者 ID を転送。ただし、発信側番号を 1 プラス 10 桁の数字で送信できることを前提に、先頭のプラス（+）を削除
\+!	RTPGWLocalizeCn	マスク 19195551888	すべてを 19195551888 に強制
!	RTPGWLocalizeCn	マスク 19195551888	すべてを 19195551888 に強制

C：表 2-33 に記載されている発信側トランスフォーメーション パターンは、+E.164 形式の番号であるか、トランクの DN 範囲に一致しない企業固有の番号であるかにかかわらず、すべての発信側番号が主要な番号（19195551888）に強制されるようにするために必要なトランスフォーメーションを行います。

前述のアウトバウンド着信側トランスフォーメーションに適用する手法に相当する、これらのトランスフォーメーションを可能にするには、まず、パーティション RTPGWLocalizeCn だけを使用した CSS RTPGWLocalizeCn を作成します。そして、ゲートウェイ設定ページの [アウトバウンドコール（Outbound Calls）] セクションまたはゲートウェイのデバイス プールの [デバイスモビリティ関連情報（Device Mobility Related Information）] セクションで、その CSS を発信側トランスフォーメーション CSS として適用します。

ゲートウェイごとに特定の着信側または発信側トランスフォーメーションが必要な場合、着信側トランスフォーメーションにデバイス プール レベルの設定を使用すると、複雑になりすぎます。その場合には、ゲートウェイ設定ページの [アウトバウンドコール（Outbound Calls）] セクションで、[デバイスプールの着信側 / 発信側トランスフォーメーション CSS を使用（Use Device Pool Called/Calling Party Transformation CSS）] オプションをオフにして、着信側または発信側トランスフォーメーション CSS を設定します。

アウトバウンド コール：SIP トランクでの着信者番号および発信者番号のトランスフォーメーション

前述のように、SIP には、番号の「タイプ」という概念がありません。通常、SIP トランクでは、着信先のタイプにかかわらず、すべての着信者番号と発信者番号を単一の形式で送信する必要があります。最も一般的な選択肢は、+E.164 または E.164 です。インバウンド コールおよびアウトバウンド コールの宛先パターンを重複させることなく、より簡単なダイヤルピア設定を行うには、SIP トランクの終端となる Cisco Unified Border Element に送信されるすべての E.164 着信側情報に、プレフィックス「*」を付加する必要があります。

（+ を含まない）E.164 を送信する必要がある場合は、着信側トランスフォーメーション パターンを使用した前述の手法を使用できます。C：表 2-34 に記載されている着信側トランスフォーメーションを 1 回行えば、すべての +E.164 番号から先頭の + を除去できます。この場合も、パーティション GWNoPlus だけに対応する CSS（例えば、GWNoPlus）を作成してから、ゲートウェイまたはゲートウェイのデバイス プールのいずれかに対し、この着信側トランスフォーメーション パターンを [着信側トランスフォーメーション CSS（Called Party Transformation CSS）] として適用する必要があります。

*C：表 2-34　SIP 用に +E.164 を *E.164 へローカライズするための着信側トランスフォーメーション パターン*

パターン	パーティション	トランスフォーメーション	説明
\+.!	GWNoPlus	ドットの前の番号を削除して、先頭に * を付加	+4961007739764 –> *4961007739764 +12125551234 –> *12125551234

送信される着信側情報の形式を SIP トランクで変換する必要がないとしても、有効な番号だけがプロバイダに送信されるようにするには、何らかのフィルタリングを着信側情報に適用する必要があります。アウトバウンド コール：ISDN ゲートウェイでの着信者番号と発信者番号のトランスフォーメーションの項で説明し、C：表 2-33 に要約した発信側トランスフォーメーションと同じものを使用できます。さらに、Cisco Unified Border Element の Cisco IOS Voice トランスレーションにより、確実に、プロバイダの形式要件に従って発信側情報がプロバイダに送信されます。C：例 2-3 に、プロバイダを指す Cisco Unified Border Element（CUBE）上で VoIP ダイヤルピアに適用される Cisco IOS Voice トランスレーションを記載します。これらのトランスレーションにより、着信側情報が *E.164 から +E.164 に変換され、発信側情報が E.164 から +E.164 に変換されます。

C：例 2-3　CUBE で +E.164 発信側番号と着信側番号に強制される Cisco IOS Voice トランスレーション

```
voice translation-rule 2
    ルール 1 /^\*/ /+/
    ルール 2 // /+/
voice translation-profile SIPtoE164
    translate called 2
    translate calling 2
dial-peer voice 2 voip
    translation-profile outgoing SIPtoE164
```

C：例 2-3 のルール 1 は先頭の「*」を「+」に置き換え、ルール 2 はすべての番号の先頭にプレフィックス「+」を付加します。

インバウンド コール：ISDN ゲートウェイでの着信者番号および発信者番号のトランスフォーメーション

Unified CM にルーティングされるコールはすべて、Unified CM に到着するすべての着信コールの +E.164 に基づくため、リンクで受信されたプロバイダからの着信側情報の形式が確実に +E.164 に変換されなければなりません。アウトバウンド コール：ISDN ゲートウェイでの着信者番号と発信者番号のトランスフォーメーションの項で説明したように、ISDN トランクで送受信する発信側情報と着信者情報は、番号計画、番号タイプ、および番号の 3 つで構成されています。SIP では番号タイプをサポートしていないため、実際の番号だけがゲートウェイから SIP トランク経由で Unified CM に転送されるとしたら、プロバイダから受信した番号タイプの意味が失われてしまいます。この状況を回避するためには、ゲートウェイに Cisco IOS Voice トランスレーションを導入し、受信した番号計画、番号タイプ、番号に基づく +E.164 数字列を作成して Unified CM に送信する必要があります。C：例 2-4 に、この目的を果たすための Cisco IOS Voice トランスレーションの設定を記載します。

C：例 2-4　ISDN を +E.164 にマッピングする Cisco IOS Voice トランスレーション

```
voice translation-rule 3
    rule 1 /^\(.+\)$/ /+1\1/ type national unknown plan any unknown
    rule 2 /^\(.+\)$/ /+\1/ type international unknown plan any unknown
voice translation-profile ISDNtoE164
    translate called 3
    translate calling 3
dial-peer voice 1 pots
    translation-profile incoming ISDNtoE164
```

C：例 2-4 に記載されている Cisco IOS トランスレーションは、受信する着信側情報のタイプが「national」であること、したがって番号が 10 桁のみであることを前提とします。ルール 1（/^\(.+\)$/）は、タイプが「international」に設定されたすべての番号にプレフィックス「+1」を付加し（/+\1/）、計画およびタイプを「unknown」に強制します。SIP トランクで Unified CM に転送する場合、計画とタイプは両方とも無関係であるためです。この同じトランスレーション ルールが、トランスレーション プロファイル ISDNtoE164 で発信側情報と着信側情報の両方に適用されます。したがって、タイプが「national」に設定された 10 桁の番号である発信側情報は、ルール 1 によって適切に +E.164 に変換されます。ルール 2 は、実際には着信側情報に適用されません。プロバイダは一般に、単一の形式だけを使用して着信側情報を送信するためです。したがって、ルール 2 が関係してくるのは、国外から受信したコールに限られます。この場合、受信する発信側情報は「international」タイプであり、番号は発信側の完全な E.164 番号に設定されていることになります。

プロバイダによって使用される番号形式は異なる場合があるため、ゲートウェイまたは Unified CM で異なる複数のトランスフォーメーションを使用する必要が生じてきます。音声トランスレーション ルールの詳細については、『*Number Translation using Voice Translation Profiles*』を参照してください。このドキュメントには、以下の URL でアクセスできます。

https://www.cisco.com/c/en/us/support/docs/voice/call-routing-dial-plans/64020-number-voice-translation-profiles.html

何らかの理由で発信側情報と着信側情報の両方に同じ音声トランスレーション ルールを使用できない場合、発信側情報と着信側情報にそれぞれ個別の音声トランスレーション ルールをプロビジョニングして、1 つのトランスレーション プロファイルで発信側トランスレーションと着信側トランスレーションを関連付ける必要があります。

インバウンド Cisco IOS Voice トランスレーション ルールを使用する必要があるのは、プロバイダから複数の異なる番号タイプが送信される場合のみです。たとえば、発信側情報または着信側情報の番号タイプが常に不明である場合は、Unified CM で数字をグローバル化された +E.164 に変換するために、発信側情報と着信側情報にインバウンド プレフィックスを使用するか、発信側および着信側トランスフォーメーション CSS を使用することができます。プレフィックスと発信側および着信側トランスフォーメーションの両方を、トランク レベルまたはデバイス プール レベルで定義することもできます。ただし、SIP では異なる番号タイプをサポートしていないため、デバイス プール レベルで定義する場合は、インバウンド プレフィックスまたは発信側および着信側 CSS を番号タイプ **unknown** に設定する必要があります。

インバウンド コール：SIP トランクでの着信者番号と発信者番号のトランスフォーメーション

一般に、PSTN SIP トランクでのインバウンド コール番号情報の処理は、前述の ISDN の場合の番号処理よりも単純です。その主な理由は、SIP トランクでの番号情報にはタイプが設定されていないためです。したがって、トランスフォーメーションの複雑さは軽減され、考慮しなければならないのは受信した数字列だけとなります。通常、SIP トランクでの発信側情報と着信側情報はすでに +E.164 形式になっているため、トランスフォーメーションは不要です。

E.164 形式で受信した発信側情報と着信側情報を +E.164 形式に変換する最も簡単な方法は、Unified CM の SIP トランクまたはトランクのデバイス プールでプレフィックス「+」を付加するように設定することです。このプレフィックスは、トランクまたはトランクのデバイス プールの [着信の発呼側設定（Incoming Calling Party Settings）] または [着信の着呼側設定（Incoming Called Party Settings）] に設定できます。SIP トランクの場合、[不明な番号（Unknown Number）] の設定は、デバイス プール レベルに適用されることに注意してください。

電話上での発信側情報の表示

+E.164 電話番号から発信されるコールの場合、すべての電話番号は +E.164 番号としてプロビジョニングされるため、発信側情報は自動的に +E.164 形式になります。考えられるあらゆるコール フローでの発信側情報の表示を単純化して一貫性を持たせるために、PSTN などの外部ネットワークから受信するすべての発信側情報は、前述のように +E.164 に正規化されます。電話や外部ネットワークにコールを表示する際には、そのコールに関して表示される発信側情報を、外部ネットワークが必要とする形式（そのコールがゲートウェイに送信される場合）またはユーザが必要とする形式（電話に送信される場合）に変換しなければならないことがあります。

非 DID を使用した電話から発信されるコールには、特殊な考慮事項があります。この場合、使用可能な発信側情報は、ESN（Enterprise Specific Number）形式でプロビジョニングされた非 DID と同一です。C：表 2-9 に、サンプル トポロジーで使用されている ESN 範囲を要約します。

電話の場合、優先される発信側の表示情報が +E.164 形式ではない場合もありますが、この情報を +E.164 として保持すると、展開が簡素化されるため、この方法が推奨されます。その場合の望ましい形式は、通常、発信側エンティティと着信側エンティティの両方に依存します。C：表 2-35 に、サイト SJC の電話で、各種のソースからのコールで必要とされる発信側情報表示の例を記載します。

C：表 2-35　SJC 電話で必要とされる発信側情報表示

発信側エンティティの「ネイティブ」発信側情報	期待される表示	コメント
+12125551234+12125551234	912125551234	米国からのコール。PSTN ダイヤル手順に従った表示。
+14085554001	4001	SJC DID 範囲の +E.164 DN からのコール。サイト内短縮ダイヤル手順に従った表示。
81405001	5001	SJC ESN 範囲の非 DID からのコール（C：表 2-9 を参照）。サイト SJC 内の非 DID への 4 桁のサイト内短縮ダイヤル手順に従った表示。
+4961007739764	90114961007739764	国際 PSTN 接続先からのコール。国際コール着信先に対する米国 PSTN ダイヤル手順に従った表示。

C：表 2-35 に記載されている表示形式を実現するには、発信側トランスフォーメーション パターンを適切なパーティションにプロビジョニングし、それらのパーティションに基づく発信側トランスレーション CSS を電話に設定して、トランスフォーメーションを有効にする必要があります。

表 28 に、C：表 2-9 に記載された番号範囲に基づき、米国のすべてのサイトに関して、C：表 2-35 に記載された短縮発信側番号を表示するためにプロビジョニングする必要がある、すべての発信側トランスフォーメーション パターンを記載します。

C：表 2-36　電話ローカリゼーション発信側トランスフォーメーション パターン

パターン	パーティション	トランスフォーメーション	説明
\+.1!	USPhLocalize	ドットの前の番号を削除して、先頭に 9 を付加	米国のすべての着信先：+12125551234 –> 912125551234
\+.!	USPhLocalize	ドットの前の番号を削除して、先頭に 9011 を付加	すべての国際コール着信先：+4961007739764 –> 90114961007739764
\+14085554XXX	SJCPhLocalize	4XXX をマスク	ローカル DN 範囲からのコール：+14085554001 –> 4001
81405XXX	SJCPhLocalize	5XXX をマスク	ローカル非 DID 範囲からのコール：81405001 –> 5001
\+19725555XXX	RCDPhLocalize	5XXX をマスク	ローカル DN 範囲からのコール：+19725555001 –> 5001
81976XXX	RCDPhLocalize	6XXX をマスク	ローカル非 DID 範囲からのコール：81976001 –> 6001

C：表 2-36　電話ローカリゼーション発信側トランスフォーメーション パターン（続き）

パターン	パーティション	トランスフォーメーション	説明
\+19195551XXX	RTPPhLocalize	1XXX をマスク	ローカル DN 範囲からのコール： +19195551001 –> 1001
81912XXX	RTPPhLocalize	2XXX をマスク	ローカル非 DID 範囲からのコール： 81912001 –> 2001

C：表 2-37 に、米国の全サイトの電話の発信側ローカリゼーションを有効にするための発信側トランスフォーメーション CSS を記載します。このスキーマを使用すると、ダイヤル発信ドメイン（国）に固有の発信側ローカリゼーション トランスフォーメーション パターンを、そのダイヤル発信ドメイン（国）内のすべてのサイトに再利用できます。国固有の発信側ローカリゼーション パターンは、基本的に、国番号と国際番号をその国に固有の国内および国際ダイヤル手順にマッピングします。

C：表 2-37　米国のサイトの電話ローカリゼーション発信側トランスフォーメーション CSS

CSS	パーティション
SJCPhLocalize	SJCPhLocalize USPhLocalize
RCDPhLocalize	RCDPhLocalize USPhLocalize
RTPPhLocalize	RTPPhLocalize USPhLocalize

C：表 2-38 に、国固有の電話ローカリゼーション発信側トランスフォーメーション パターンの例を記載します。これは、イタリアおよびドイツに対してプロビジョニングする必要があるパターンの例です。

C：表 2-38　イタリアおよびドイツの電話ローカリゼーション発信側トランスフォーメーション パターン

パターン	パーティション	トランスフォーメーション	説明
\+49.!	DEPhLocalize	ドットの前の番号を削除して、先頭に 00 を付加	ドイツのすべての着信先： +4941001234 –> 0041001234
\+.!	DEPhLocalize	ドットの前の番号を削除して、先頭に 000 を付加	すべての国際コール着信先： +14085551234 –> 00014085551234
\+39.!	ITPhLocalize	ドットの前の番号を削除して、先頭に 0 を付加	イタリアのすべての着信先： +390730123456 –> 00730123456 +393012345678 –> 03012345678
\+.!	ITPhLocalize	ドットの前の番号を削除して、先頭に 000 を付加	すべての国際コール着信先： +14085551234+14085551234 –> 00014085551234

自動代替ルーティング

自動代替ルーティング（AAR）は、発信元のエンドポイント、ゲートウェイ、またはトランクと発信先のエンドポイント間で十分な帯域幅がない（コール アドミッション制御がコールを許可しない）場合に、PSTN 経由の代替ルートを介して登録済みエンドポイントへのコールを再ルーティングするメカニズムです。AAR は、エンドポイントへのコールにのみ適用されます。

ゲートウェイやトランクなどの他の宛先へのコール用の帯域幅が不十分な場合は、AAR がトリガーされません。このような場合の代替ルーティング メカニズムは、ルート リストとルート グループに基づいています。AAR をアクティブにするには、次の手順が必要です。

- [自動代替ルーティングの有効化（Automated Alternate Routing Enable）] サービス パラメータを設定します（サービス パラメーターの設定の項を参照）。
- [ダイヤルプレフィックス（Dial Prefix）]（デフォルト）を設定せずに、Default という単一の AAR グループを設定します。
- +E.164 PSTN ルート パターンへのアクセスだけを設定した CSS PSTNReroute を設定します。この設計例に基づく CSS には、パーティション PSTNInternational だけを含める必要があります。
- AAR の対象となる可能性があるコールを開始するエンドポイント、トランク、およびその他のデバイスのすべてで、以下を設定します。
  - [AAR コーリングサーチスペース（AAR Calling Search Space）] を PSTNReroute に設定します。
  - [AAR グループ（AAR Group）] を Default に設定します。
- すべてのデバイス ポートで、[AAR コーリングサーチスペース（AAR Calling Search Space）] を PSTNReroute に設定します。
- [AAR グループ（AAR Group）] を Default に設定します。
- +E.164 電話番号に AAR マスクを設定し、その電話番号が +E.164 番号になるようにします。固定長の番号計画を使用する国では、すべての電話番号でマスクを同じ値に設定できます（たとえば米国では、+1XXXXXXXXXX など）。可変長の電話番号に対応する必要がある場合、単一のサイトをカバーする具体的なマスクをプロビジョニングします。あるいは最悪の場合、それぞれの電話番号と同じ完全修飾子を付けた +E.164 AAR マスクをプロビジョニングする必要があります。非 DID の場合、AAR マスクは空のままにします。これにより実質的に、非 DID が呼び出された場合は AAR が無効になります。非 DID には同等の E.164 アドレスがなく、PSTN を介してアクセスできないため、これは理にかなっています。

上記のリストでは、+E.164 電話番号を使用したダイヤル プランの利点の 1 つが示されています。この場合、他に変更を加えることなく、着信側 +E.164 アドレスを PSTN 経由の代替ダイヤルに直接再使用できるためです。

未登録エンドポイントの代替ルーティング

コール処理を一元化したマルチサイト展開環境で WAN に障害が発生した場合、その障害によって中央の Unified CM との接続を失ったエンドポイントは、代わりにローカル SRST ゲートウェイに登録します（Survivable Remote Site Telephony（SRST）展開の項を参照）。これにより、影響を受けた電話をそのまま配置して、受信したコールを同じサイト内の電話と PSTN との間で受け渡すことができます。ただし、中央の Unified CM の観点からは着信デバイスは登録されていないため、そのデバイスには到達できません。したがって、中央の Unified CM に登録された電話からのコールは失敗します。PSTN を介した未登録エンドポイントへのコールの自動再ルーティングを有効にするには、自動再ルーティングが必要な電話番号のそれぞれに対して、以下のタスクを実行します。

- 「未登録内線の不在転送」および「未登録外線の不在転送」の宛先を、+E.164 電話番号と同じ値に設定します。
- [未登録内線の不在転送の CSS（Forward Unregistered Internal CSS）] および [未登録外線の不在転送の CSS（Forward Unregistered External CSS）] を、PSTNReroute に設定します。これは、自動代替ルーティングの項で定義したのと同じ CSS です。これにより、PSTN ルート パターンにアクセスできるようになります。

- サイトのゲートウェイがまだ統一された CM に接続中に電話機が登録解除された際（たとえば、接続されていない場合など）に発生する可能性があるルーティングループの影響を確実に制限するには、**DN への未登録ホップの最大転送数**サービスパラメータをゼロ以外の値に設定します。

未登録エンドポイントに対する PSTN を介した代替ルーティングが意味を持つのは、+E.164 電話番号のみです。DID を使用しないエンドポイント（電話番号として ESN を使用するエンドポイント）の場合、未登録エンドポイントに対して意味を持つ再ルーティングは、着信コールをボイスメールに転送するというルーティングだけです。未登録エンドポイントへのコールをボイスメールに転送するには、以下のタスクを実行します。

- [未登録内線の不在転送（Forward Unregistered Internal）] および [未登録外線の不在転送（Forward Unregistered External）] に [ボイスメールオプション（Voicemail options）] を選択します。
- [未登録内線の不在転送の CSS（Forward Unregistered Internal CSS）] および [未登録外線の不在転送の CSS（Forward Unregistered External CSS）] を、「国内」サービス クラスを実装する CSS（たとえば、SJCInternal）に設定します。実質的に、この CSS ではボイスメールパイロット番号にのみアクセスできます。

LDAP システムの設定

実際の同期アグリーメントを定義する前に、LDAP システムを有効にする必要があります。[LDAP システムの設定（LDAP System Configuration）] メニューでは、次の操作を実行できます。

- [LDAP サーバからの同期を有効にする（Enable Synchronizing from LDAP Server）] オプションを選択する（チェックボックスをオンにする）。
- 展開環境に適切な [LDAP サーバタイプ（LDAP Server Type）] を選択します。
- 展開環境に適切な [ユーザ ID の LDAP 属性（LDAP Attribute for User ID）] を選択します。

Microsoft Active Directory からユーザが同期される環境では、C：表 2-39 に記載する設定を使用します。

C：表 2-39　Microsoft Active Directory の場合の LDAP システム設定

設定	値
[LDAP サーバタイプ（LDAP Server Type）]	Microsoft Active Directory
[ユーザ ID の LDAP 属性（LDAP Attribute for User ID）]	sAMAccountName

LDAP　カスタムフィルター

Unified CM ベースのディレクトリ検索が電話で使用されている場合は、社内 LDAP ディレクトリ全体を Unified CM に同期することが理にかなっています。その場合、実際にローカル クラスタの UC サービスを使用するユーザと、完全な社内 LDAP ディレクトリを Unified CM に反映するためだけに同期されるユーザとを区別可能にする必要があります。

この目標を達成するには、カスタム LDAP フィルタを使用して、ローカル ユーザ グループとリモート ユーザ グループの 2 つを定義できます。ここで言うリモート ユーザとは、ローカル Unified CM クラスタの UC サービスを一切使用しないユーザを意味します。C：表 2-40 に、2 つのカスタム LDAP フィルタを記載します。ここでは、展開環境のユーザが米国と欧州に存在し、米国のユーザのみがローカル ユーザであることを前提としています。

C：表 2-40　カスタム LDAP フィルタ設定

LDAP フィルタ名	フィルタ
[ローカル（Local）]	(& (objectclass=user) (!(objectclass=Computer)) (!(UserAccountControl:1.2.840.113556.1.4.803:=2)) (telephoneNumber=+1*))
[リモート（Remote）]	(& (objectclass=user) (!(objectclass=Computer)) (!(UserAccountControl:1.2.840.113556.1.4.803:=2)) (| (telephoneNumber=+3*) (telephoneNumber=+4*)))

読みやすくするために、C：表 2-40 では、インデント レベルに LDAP フィルタ文字列の構造を反映して、LDAP フィルタ文字列を複数の行に分けて記載しています。これらの LDAP フィルタを Unified CM にプロビジョニングするには、特定のフィルタのすべての行を 1 行に連結する必要があります。

上記の LDAP フィルタは、どちらも Microsoft Active Directory のデフォルト LDAP フィルタを拡張したものです。他のディレクトリ タイプのデフォルト LDAP フィルタは、『*Cisco Collaboration System SRND*』最新版の「*Directory Integration and Identity Management*」に関する章と、LDAP ディレクトリの設定に関する Unified CM オンライン ヘルプに記載されています。

C：表 2-40 に記載されている LDAP フィルタでは、電話番号の開始部分を基準として、個々のユーザがローカル ユーザまたはリモート ユーザのどちらであるかを判別します。

複数の LDAP 同期アグリーメントを使用する場合は、それらの同期アグリメーメントで使用される LDAP フィルタを分離して、同じユーザが複数のフィルタに一致しないようにしてください。

機能グループ テンプレート

LDAP からユーザを同期する機能は、機能グループ グループ テンプレート（FGT）に定義されています。C：表 2-41 に、Unified CM クラスタのアクティブ デバイスでのユーザの機能を定義する FGT の設定を要約します。

C：表 2-41　ローカル ユーザの機能グループ テンプレート

設定	値	コメント
名前	FGTlocal	名前でローカル ユーザ用の FGT であることを示す必要があります。
[説明（Description）]	ローカルユーザ用の FGT	
[ホームクラスタ（Home Cluster）]	オン	このユーザの UDS ベースのサービス検出がローカル Unified CM クラスタに解決されるようにします。
[Unified CM IM and Presence のユーザを有効化（Enable User for Unified CM IM and Presence）]	オン	IM and Presence のユーザを有効にします。
[BLF プレゼンスグループ（BLF Presence Group）]	標準のプレゼンス グループ	展開を簡素化するために、すべてのユーザを単一の BLF プレゼンス グループに割り当てます。
[SUBSCRIBE コーリング サーチ（SUBSCRIBE Calling Search）]	DefaultSubscribe	特殊な CSS の項で説明している、デフォルトのサブスクライブ CSS を使用します。

その他すべての設定には、デフォルト値をそのまま使用できます。

リモート ユーザも LDAP から同期されるため（LDAP　カスタムフィルターの項を参照）、リモート ユーザ用の FGT もプロビジョニングする必要があります。主な違いは、リモート ユーザ用の FGT では、[ホームクラスタ（Home Cluster）] および [Unified CM IM and Presence のユーザを有効化（Enable User for Unified CM IM and Presence）] オプションをオンにしないことです。C：表 2-42 に、これらの設定を要約します。

C：表 2-42　リモート ユーザの機能グループ テンプレート

設定	値	コメント
名前	FGTremote	名前にリモート ユーザ用の FGT であることを示す必要があります。
[説明（Description）]	リモート ユーザ用の FGT	
[ホームクラスタ（Home Cluster）]	オフ	このユーザの UDS ベースのサービス検出がローカル Unified CM クラスタに解決されないようにします。
[Unified CM IM and Presence のユーザを有効化（Enable User for Unified CM IM and Presence）]	オフ	IM and Presence のユーザは有効にしません。

その他すべての設定には、デフォルト値をそのまま使用できます。

LDAP 同期アグリーメント

すべてのローカル ユーザを Unified CM に同期させるには、LDAP 同期アグリーメントを構成する必要があります。C：表 2-43 に、[システム /LDAP/LDAP ディレクトリ（System/LDAP/LDAP Directory）] に構成する必要がある設定を記載します。

C：表 2-43　ローカル ユーザの LDAP 同期アグリーメント

設定	値	コメント
[LDAP 設定名（LDAP Configuration Name）]	[ローカル（Local）]	ローカル ユーザを同期する LDAP 同期アグリーメントであることを示します。
[LDAP マネージャの識別名（LDAP Manager Distinguished Name）]	管理ユーザの名前	ldapaccess@ent-pa.com または cn=ldapaccess,cn=users,dc=ent-pa,dc=com の形式で指定できます。
[LDAP パスワード（LDAP Password）]	LDAP 管理者のパスワード	
[LDAP ユーザ検索ベース（LDAP User Search Base）]	LDAP 検索ベース	例：dc=ent-pa,dc=com
LDAP カスタムフィルタ	[ローカル（Local）]	LDAP　カスタムフィルターの項で説明しているカスタム LDAP フィルタを参照してください。
[同期を 1 回だけ実行する（Perform Sync Just Once）]	オフ	LDAP 同期を定期的に実行します。
[再同期の実行間隔（Perform a Re-sync Every)]	妥当な間隔	社内ディレクトの変更内容が妥当な間隔で反映されるように、小さな値を設定します。ただし、LDAP 同期を実行すると、Unified CM パブリッシャにかなりの負荷がかかることに注意してください。おそらく、デフォルトの 24 時間間隔で同期を行うのが妥当です。
[Directory URI]	メール アドレス	通常、ユーザのディレクトリ URI は、ユーザの電子メール アドレスと同じです。
[アクセスコントロールグループ（Access Control Groups）]	[標準 CCM エンドユーザ（Standard CCM End Users）] [標準 CTI を有効にする（Standard CTI Enabled）]	必要に応じて、その他のアクセス コントロール グループを追加または削除します。ただし、標準 CCM エンドユーザが設定されていないと、ユーザはセルフサービス ポータルにログインできません。
[機能グループテンプレート（Feature Group Template）]	[ローカル（Local）]	機能グループ テンプレートの項で説明している FGT を参照してください。
[LDAP サーバ情報（LDAP Server Information）]	ソースとして使用する社内 LDAP サーバを参照	可能な場合は、冗長サーバをプロビジョニングするようにしてください。

C：表 2-43 に記載されている LDAP 同期アグリーメントは、前に定義した FGT とカスタム LDAP フィルタを関連付けます。これにより、カスタム LDAP フィルタに一致する社内ディレクトリ内のすべてのユーザについて、Unified CM に、FGT に定義された機能が割り当てられたユーザが作成されます。

ローカル Unified CM クラスタで UC サービスを使用しないリモート ユーザを同期するための専用の LDAP 同期アグリーメントも必要です。C：表 2-44 に、この LDAP 同期アグリーメントを要約します。

C：表 2-44　リモート ユーザの LDAP 同期アグリーメント

設定	値	コメント
[LDAP 設定名（LDAP Configuration Name）]	[リモート（Remote）]	これがリモート ユーザを同期する LDAP 同期アグリーメントであることを示します。
[LDAP マネージャの識別名（LDAP Manager Distinguished Name）]	管理ユーザの名前	ldapaccess@ent-pa.com または cn=ldapaccess,cn=users,dc=ent-pa,dc=com の形式で指定できます。
[LDAP パスワード（LDAP Password）]	LDAP 管理者のパスワード	
[LDAP ユーザ検索ベース（LDAP User Search Base）]	LDAP 検索ベース	例：dc=ent-pa,dc=com
LDAP カスタムフィルタ	[リモート（Remote）]	LDAP　カスタムフィルターの項で説明しているカスタム LDAP フィルタを参照してください。
[同期を 1 回だけ実行する（Perform Sync Just Once）]	オフ	LDAP 同期を定期的に実行します。
[再同期の実行間隔（Perform a Re-sync Every)]	妥当な間隔	社内ディレクトの変更内容が妥当な間隔で反映されるように、小さな値を設定します。ただし、LDAP 同期を実行すると、Unified CM パブリッシャにかなりの負荷がかかることに注意してください。おそらく、デフォルトの 24 時間間隔で同期を行うのが妥当です。
[Directory URI]	メール アドレス	通常、ユーザのディレクトリ URI は、ユーザの電子メール アドレスと同じです。
[アクセスコントロールグループ（Access Control Groups）]	アクセス コントロール グループの選択なし	リモート ユーザは、どのアクセス コントロール グループにも属しません。
[機能グループテンプレート（Feature Group Template）]	[リモート（Remote）]	機能グループ テンプレートの項で説明している FGT を参照してください。
[LDAP サーバ情報（LDAP Server Information）]	ソースとして使用する社内 LDAP サーバを参照	可能な場合は、冗長サーバをプロビジョニングするようにしてください。

上記の LDAP 同期アグリーメントを使用すると、すべてのユーザを社内ディレクトリから識別できるようになり、LDAP 同期アグリーメントに関連付けられた FGT によって確実に、すべてのユーザに適切な機能が設定されます。

LDAP によるユーザ認証

C：表 2-45 に、LDAP 認証設定の例を記載します。

C：表 2-45　LDAP 認証設定

設定	例	コメント
[エンドユーザ用 LDAP 認証（LDAP Authentication for End Users）]		
[エンドユーザに LDAP 認証を使用する（Use LDAP Authentication for End Users）]	オン	Unified CM クラスタの LDAP 認証を有効にします。
[LDAP マネージャの識別名（LDAP Manager Distinguished Name）]	cn=ldapmanager,dc=ent pa,dc=com	目的のユーザ検索ベース内のすべてユーザ オブジェクトに対する読み取りアクセス権限が割り当てられた AD アカウントの識別名。
[LDAP パスワード（LDAP Password）]	何らかのパスワード	
[パスワードの確認（Confirm Password）]	同上	
[LDAP ユーザ検索ベース（LDAP User Search Base）]	ou=enterprise,dc=ent-pa,dc=com	
[LDAP サーバ情報（LDAP Server Information）]		
[サーバのホスト名または IP アドレス（Host Name or IP Address for Server）]	ent-dc1.ent-pa.com	グローバル カタログ ロールが割り当てられたサーバ
[LDAP ポート（LDAP Port）]	3268	グローバル カタログにアクセスするためのポート（推奨）

Cisco Unified CM グループ設定

Cisco Unified CM グループを使用して、クラスタ内に Unified CM インスタンスのグループを定義し、デバイスが Unified CM クラスタに登録するために使用する Unified CM インスタンスを指定することができます。単一の Unified CM コール処理ペアだけが展開されている場合（詳細については、Cisco Unified CM と IM とプレゼンスサービスクラスタのプロビジョニングの項を参照）、Default という名前の単一の Unified CM グループも導入し、クラスタ内の単一の Unified CM コール処理サブスクライバ ペアで実行する両方の Unified CM インスタンスを、この単一の Unified CM グループのメンバにする必要があります。

複数の Unified CM コール処理サブスクライバ ペアが存在する場合、追加の Unified CM グループ（各 Unified CM コール処理サブスクライバ ペアごとに 1 つのグループ）をプロビジョニングして、各 Unified CM グループに、その特定のペアで実行する 2 つの Unified CM インスタンスを追加する必要があります。

最初のペアに ucm1a.ent-pa.com および ucm1b.ent-pa.com という名前の 2 つの Unified CM コール処理サブスクライバがあり、2 番目のペアに ucm2a.ent-pa.com および ucm2b.ent-pa.com という名前の 2 つの Unified CM コール処理サブスクライバがあり、それぞれのペアで ucm1a、ucm2a がプライマリ Unified CM コール処理サブスクライバとなっている Unified CM クラスタの場合、C：表 2-46 にリストされているように Unified CM グループをプロビジョニングします。

C：表 2-46 Unified CM グループ定義の例

Unified CM グループ	Unified CM グループ メンバ
CM_1	CM_ucm1a.ent-pa.com CM_ucm1b.ent-pa.com
CM_2	CM_ucm2a.ent-pa.com CM_ucm2b.ent-pa.com

Unified CM グループ間ですべての登録のバランスを取る必要があります。それには、デバイス プールの項で説明しているデバイス プール設定を使用して、デバイスを Unified CM グループに割り当てます。

電話用 NTP リファレンス

必要に応じて、SIP を実行している電話が NTP サーバから日時を取得するように、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で電話用 Network Time Protocol（NTP）を設定することができます。すべての NTP サーバが応答しない場合、SIP を実行している電話は、REGISTER メッセージに対する 200 OK 応答の日付ヘッダーを日時に使用します。

電話用 NTP を Cisco Unified CM の管理に追加した後は、日付 / 時刻グループにその電話用 NTP を追加する必要があります。

電話用 NTP を定義するには、使用する予定の NTP サーバの IP アドレスを取得し、C：表 2-47 に従って設定を行います。

C：表 2-47 電話用 NTP リファレンス の設定

設定	例	コメント
[IP アドレス（IP Address）]	66.228.35.252	使用する NTP サーバの IP アドレス
[説明（Description）]	0.pool.ntp.org	入力した IP アドレスのホスト名を参照する必要があります。
[モード（Mode）]	[ユニキャスト（Unicast）]	ユニキャストを設定すると、デバイスはリストされたサーバからの NTP 応答のみを使用するように制限されます。

冗長性をもたらすためには、複数の電話用 NTP をプロビジョニングする必要があります。

日付および時刻グループ

日付および時刻グループを使用して、Unified CM に登録する一連のデバイスに使用するタイムゾーンおよび日付と時刻の形式を定義できます。日付および時刻グループはデバイス プールに設定し、デバイス プールは電話ページで指定します。デバイス プールの詳細については、デバイス プールのセクションを参照してください。

SIP 電話で NTP サーバから日付と時間を取得したい場合は、電話用 NTP の優先順位を設定している日時グループで、電話を接続する最初のサーバを最も高い優先順位にします。

エンドポイントを展開するそれぞれのタイム ゾーンに対して、C：表 2-48 に示すように 1 つの日時グループを作成します。

C：表 2-48　日時グループの定義例

日時グループ	タイム ゾーン
RCD_Time	America/North_Dakota/New_Salem
RTP_Time	America/New_York
SJC_Time	America/Los_Angeles

メディア リソース

メディア リソースとは、ソフトウェア ベースまたはハードウェア ベースのエンティティであり、接続中のデータ ストリームに対してメディア処理を行うものです。メディア処理機能には、複数のストリームを混合して 1 つの出力ストリームを作成する機能（会議）、ある接続から別の接続にストリームを渡す機能（メディア ターミネーション ポイント）、ある圧縮タイプから別の圧縮タイプにデータ ストリームを変換する機能（トランスコーディング）、保留中の発信者への音楽のストリーミング（保留音）、エコー キャンセレーション、シグナリング、TDM 回線からの音声インターフェイス（コーディング / デコーディング）、ストリームのパケット化、オーディオのストリーミング（Annunciator）などが含まれます。ソフトウェアベースのリソースは、Cisco Unified CM IP Voice Media Streaming アプリケーションによって提供されます。

メディア　リソース　マネージャー

Unified CM のソフトウェア コンポーネントであるメディア リソース マネージャ（MRM）は、メディア リソースの割り当ておよびメディア パスの挿入が必要であるかどうかを判別します。MRM は、メディア リソースのタイプを判別および特定すると、当該デバイスに関連付けられているメディア リソース グループ リスト（MRGL）およびメディア リソース グループ（MRG）の構成の設定値に応じて、使用可能なリソース全体を検索します。MRGL および MRG は、割り当ての目的のためにメディア リソースの関連グループをまとめて保持している構成体です。

メディア リソースの選択とデフォルト MRG の回避

メディア リソース グループ（MRG）とメディア リソース グループ リスト（MRGL）は、リソースの割り当て方法を制御する方式を提供するもので、リソースに対するアクセス権、リソースの場所、特定のアプリケーションのリソース タイプが含まれます。MRG の使用により、類似の特性を持つメディア リソースがまとめてグループ化されます。MRGL は、セッションのために必要なメディア リソースを選択するときに考慮される MRG のセットを定義します。メディア リソース マネージャが設定されている MRGL を検索しても必要なリソースが見つからない場合は、すべてのメディア リソースがリストの MRG のメンバーであると見なして、メディア リソース マネージャがデフォルトのメディア リソース グループでメディア リソースをチェックします。特定の MRG のメンバーであることが明示的に設定されている場合を除き、デフォルトではすべてのメディア リソースはこのデフォルトの MRG のメンバーです。

この設計では、メディア リソース選択のトラブルシューティングがより複雑になってしまうため、デフォルトの MRG は使用しません。デフォルトの MRG が確実に空になるようにするには、すべてのメディア リソースを少なくとも 1 つの MRG に割り当てる必要があります。

Cisco IP Voice Media Streaming Application

Cisco IP Voice Media Streaming Application は、ソフトウェアベースの次のメディア リソースを提供します。

- 会議ブリッジ
- 保留音（MoH）
- アナンシエータ
- メディア ターミネーション ポイント（MTP）

Unified CM クラスタのノードで IP Voice Media Streaming Application が アクティブになると、上記ースの 1 つが自動的に設定されます。サービスのアクティブ化についての推奨事項は、C：表 2-3 を参照してください。

この設計では、ユニキャスト MoH のみが使用され、Unified CM クラスタのサブスクライバ ノード上で稼働している Cisco IP Voice Media Streaming Application からメディアが流されます。

アナンシエータは Cisco IP Voice Media Streaming Application のソフトウェア機能で、これを使用すると、音声メッセージや各種コール プログレス トーンをシステムからユーザに流すことができます。

Unified CM 上で実行されている Cisco IP Voice Media Streaming Application によって作成されたすべての MOH およびアナンシエータ メディア リソースは、以下のタスクを実行することにより 1 つの MRG に組み込まれます。

- Software という名前の MRG を作成する。
- Cisco IP Voice Media Streaming Application で作成したすべてのアナンシエータ リソースを MRG Software に割り当てる。
- Cisco IP Voice Media Streaming Application で作成したすべての MoH リソースを MRG Software に割り当てる。

Cisco IP Voice Media Streaming Application で作成されたソフトウェアベースの会議およびメディア ターミネーション ポイントは、この設計では使用されません。これらのものを無効にするには、次のタスクを実行します。

- Unused という名前の MRG を作成する。
- Cisco IP Voice Media Streaming Application で作成されたソフトウェアベースの会議ブリッジを MRG Unused に割り当てる。
- Cisco IP Voice Media Streaming Application で作成されたソフトウェアベースのメディア ターミネーション ポイントを MRG Unused に割り当てる。

このようにすると、これらのリソースはデフォルトの MRG に属さないため、メディア リソース マネージャのメディア リソース選択プロセスでは考慮されなくなります。

MRG および MRGL の定義

プロビジョニングされた MRGL の数を最小に保持しておくことは重要なポイントです。必要な MRGL の数に影響を与える要因には、次のものがあります。

- サイトの特異性

  サイト固有のメディア リソースが存在する場合は、それらのリソースに対してサイト固有の MRG を設定する必要があります。また一般的には、サイト固有のメディア リソースの選択（通常はローカル）を可能にするには、サイト固有の MRGL も必要になります。

- 同じクラスにおける異なるタイプのメディア リソース

  Unified CM は音声のみの会議リソースと、音声 / ビデオの会議リソースを区別しません。音声のみと音声 / ビデオの両方の会議メディア リソースがプロビジョニングされている場合、これらのリソースに対して異なるアクセス ポリシーを設定できるようにするには、メディア リソースのタイプごとに MRG（および MRGL）が必要になります。会議リソースの詳細については、会議 の章を参照してください。

サイト固有のメディア リソースがなく、メディア リソースのタイプを区別する必要がない場合は、Standard という名前の MRGL を少なくとも 1 つ設定する必要があります。

サイトの特異性およびメディア リソース タイプのプロビジョニングに基づいて必要なそれぞれの MRGL に対して、次のタスクを実行して MRGL を作成します。

- サイトの特異性、および MRGL のメディア リソース タイプを反映するように、MRGL に名前を付けます。
- MRGL に対して適切な MRG を選択します。MoH およびアナンシエータに対するアクセスが保証されるよう、Software MRG は必ず含めるようにします。

C：表 2-49 は、音声会議とビデオ会議について処理が異なる MRGL の定義例を示しています。MRGL Video ではビデオ会議リソースへアクセスすることができますが、MRGL Audio は、音声会議メディア リソースへのアクセスのみが必要なデバイスへ割り当てる必要があります。

C：表 2-49　音声会議とビデオ会議の MRGL の定義例

MRGL 名	MRG	コメント
[音声（Audio）]	[音声（Audio）] [ソフトウェア（Software）]	MRG Audio の音声会議メディア リソースへのアクセス権を持っている MRGL。 MRG Software は MoH およびアナンシエータへのアクセスを提供するために追加されました。
[ビデオ（Video）]	[ビデオ（Video）] [ソフトウェア（Software）]	MRG Video のビデオ会議メディア リソースへのアクセス権を持っている MRGL。 MRG Software は MoH およびアナンシエータへのアクセスを提供するために追加されました。

デバイス プール

デバイス プールはデバイスの共通の特性セットを定義します。デバイス プールで定義されている特性には、C：表 2-50 に示されている設定が含まれています。

C：表 2-50　デバイス プールの設定

設定	説明
[Cisco Unified CM グループ（Cisco Unified Communications Manager Group）]	Unified CM グループは、Unified CM の呼処理サブスクライバのペア間で登録を均等に分配する必要があります（Cisco Unified CM グループ設定のセクションを参照してください）。デバイス プール上にプロビジョニングされている Unified CM グループは Unified CM の呼処理サブスクライバを決定します。特定のデバイス プールに関連付けられているデバイスは、このサブスクライバに対して登録を試行します。
[ローカルルートグループ（Local Route Groups）]	コール タイプ固有の発信ゲートウェイを選択するためのローカル ルート グループのセクションに説明されているように、LRG に基づいてコール タイプ特有の出口ゲートウェイを選択できるように、複数の LRG が定義されています。定義されている各 LRG 名では、LRG 名に対して選択されたルート グループによって、選択されたタイプのコールについてどのデバイスが考慮されるかが定義されます（着信番号と特定の LRG を参照しているルート リストへのポインティングについてのルート パターン マッチングによって定義されます）。ルート リストに有効な PSTN リソースが含まれていないために通話が失敗することを回避するためには、定義されているすべての LRG 名に対してルート グループを設定することが重要です。

C：表 2-50　デバイス プールの設定（続き）

設定	説明
[ローミングに合わせて変化する設定（Roaming Sensitive Settings）]	
[日時グループ（Date/Time Group）]	日付と時間の形式、および電話用 NTP を定義します。電話用 NTP リファレンスのセクションを参照してください。
[メディアリソースグループリスト（Media Resource Group List）]	デバイスのグループで使用できるメディア リソースを定義する MRGL。MRG および MRGL の定義のセクションを参照してください。
[デバイスモビリティ関連情報（Device Mobility Related Information）]	
[AAR コーリングサーチスペース（AAR Calling Search Space）]	PSTN の他の通知先へコールをルートするために使用する CSS。このドキュメントのダイヤル プラン設計では、どのような場合でも同じ AAR CSS（PSTNReroute）を使用することができます（自動代替ルーティングのセクションを参照してください）。
[AAR グループ（AAR Group）]	AAR を有効にするには、AAR グループを定義する必要があります。+E.164 の電話番号を使用すると、1 つの AAR グループ Default を使用して AAR を展開することができます（自動代替ルーティングのセクションを参照してください）。
[発呼側トランスフォーメーション CSS（Calling Party Transformation CSS）]	この CSS は、影響を受けるデバイスの方向へ送信される発呼側情報に適用される、発呼側のトランスフォーメーションを定義します。 ゲートウェイの場合、この CSS は、ゲートウェイの設定ページの [アウトバウンド コール（Outbound Calls）] セクションで定義された発呼側トランスフォーメーション CSS に関連付けられています。 電話の場合、この CSS は、電話の設定ページの [リモート番号（Remote Number）] セクションで定義された発呼側トランスフォーメーション CSS に関連付けられています。
[着信側トランスフォーメーション CSS（Called Party Transformation CSS）]	この CSS は、影響を受けるデバイスの方向へ送信される着信側情報に適用される、着信側のトランスフォーメーションを定義します。 ゲートウェイの場合、この CSS は、ゲートウェイの設定ページの [アウトバウンド コール（Outbound Calls）] セクションで定義された着信側トランスフォーメーション CSS に関連付けられています。 電話の場合、この CSS は電話の設定ページに相当する機能がなく、電話で使用されるデバイス プール上で設定しても何も影響を与えません。
[コールルーティング情報（Call Routing Information）]	この設定により、着信の発呼側および着呼側の番号タイプごとのトランスフォーメーションを、ゲートウェイ上の着信コールに適用するように定義できます。ゲートウェイ固有の個別の設定が必要な場合は、同じ設定をゲートウェイの設定ページで行うこともできます。

デバイス プールのその他のレベルの設定はすべて、この設計では使用されません。

デバイスのグループに対して、C：表 2-50 に記載されている設定オプションで同じ設定を適用する必要がある場合は、これらの設定を持つデバイス プールを作成し、このデバイス プールにすべてのデバイスを割り当てることを推奨しています。すべてのデバイスに対して 1 つの設定を変更する必要がある場合は、デバイス プールのレベル設定を使用して、すべてのデバイスに対してその部分だけを変更することができます。

デバイス プールの数を最小にするには、複数のデバイスで同じ特性を共有している場合のみデバイス プールを作成します。次に、同じサイト内の電話の例を示します。C：表 2-51 は、RTP サイト内でビデオ会議機能を使用している電話に対するデバイス プールの設定例です。

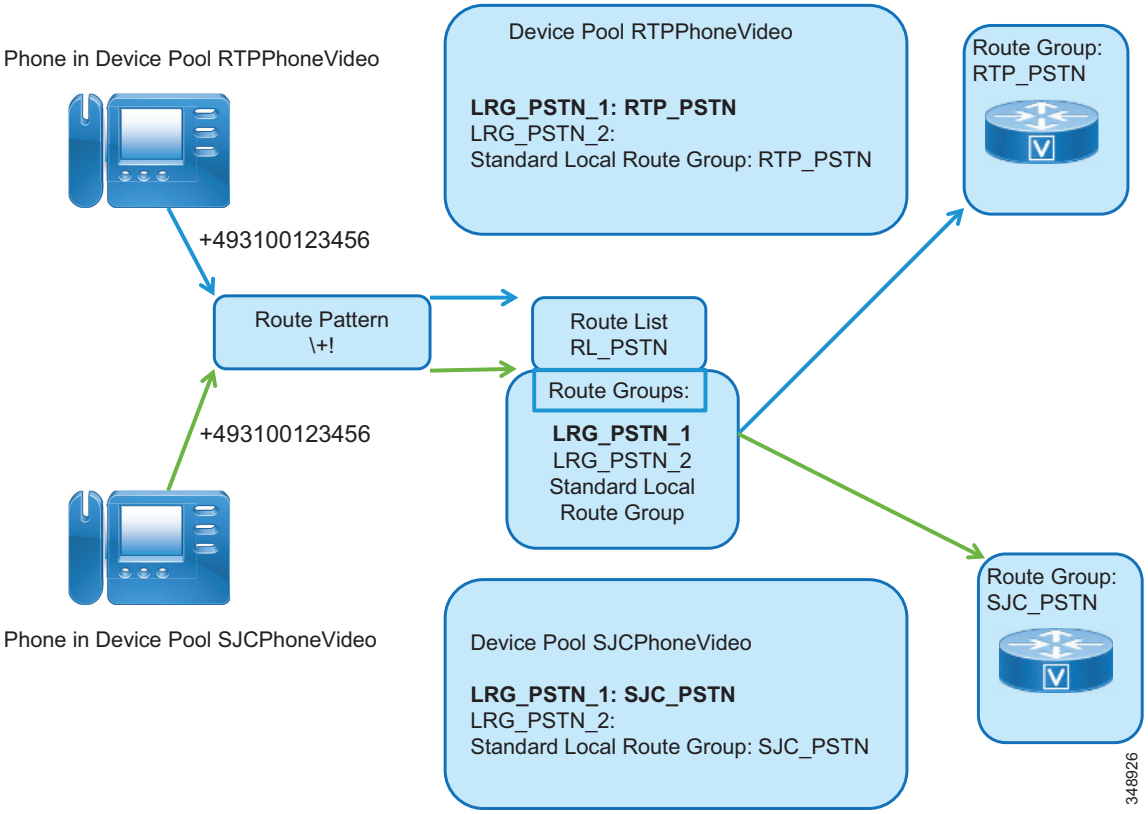
C：表 2-51　RTP サイト内でビデオ会議機能を使用している電話のデバイス プール設定

設定	値	コメント
[デバイスプール名（Device Pool Name）]	[RTPPhoneVideo]	名前は、このデバイス プールを使用するデバイスを一意に識別できるようなものにします（タイプや詳細な分類など）。この場合はこのデバイス プールを、ビデオ会議機能を使用している RTP サイト内の電話に対して使用します。
[Cisco Unified CM グループ（Cisco Unified Communications Manager Group）]	[CM_1]	
[ローカルルートグループの設定（Local Route Group Settings）]		
[標準ローカル ルート グループ（Standard Local Route Group）]	[RTP_PSTN]	すべてのルート リストは最後のオプションとして [標準ローカルルートグループ（Standard Local Route Group）] を使用します。[標準ローカルルートグループ（Standard Local Route Group）] は必ずローカル PSTN ゲートウェイのルート グループに設定します。
[LRG_PSTN_1]	[RTP_PSTN]	PSTN コールの最初のオプションは、ローカル RTP ゲートウェイを使用することです。
[LRG_PSTN_2]	[SJC_PSTN]	フォールバックとして HQ ゲートウェイを使用します。
[LRG_VIDEO_1]	[SJC_VIDEO]	サイト固有のビデオ ゲートウェイはありません。サイト SJC のビデオ ゲートウェイを使用します。
[LRG_VIDEO_2]	< なし >	
[LRG_EMERGENCY_1]	< なし >	設定なし：[標準ローカルルートグループ（Standard Local Route Group）] にフォールバックします。
[LRG_EMERGENCY_2]	< なし >	設定なし：[標準ローカルルートグループ（Standard Local Route Group）] にフォールバックします。
[ローミングに合わせて変化する設定（Roaming Sensitive Settings）]		
[日時グループ（Date/Time Group）]	[RTP_Time]	日付および時刻グループのセクションを参照してください。
[メディアリソースグループ リスト（Media Resource Group List）]	[ビデオ（Video）]	ビデオ会議メディア リソースへのアクセスを提供します（C：表 2-49 を参照）。
[デバイスモビリティ関連情報（Device Mobility Related Information）]		
[AAR コーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	すべてのデバイスおよびデバイス プールで同じです。
[AAR グループ（AAR Group）]	[デフォルト（Default）]	すべてのデバイスおよびデバイス プールで同じです。
[発呼側トランスフォーメーション CSS（Calling Party Transformation CSS）]	[RTPPhLocalize]	サイト固有の発呼側トランスフォーメーション（C：表 2-36 および C：表 2-37 を参照）。
[着信側トランスフォーメーション CSS（Called Party Transformation CSS）]	< なし >	電話には適用されません。

C：表 2-51 は、実際のサイト固有の PSTN ゲートウェイがどのように LRG 名に割り当てられて、異なるサイトの電話に関して、サイト固有の出口ゲートウェイの選択を実現しているかを示しています。

C：図 2-9 は、サイト RTP および SJC の電話のデバイス プールで、同じ LRG 名（LRG_PSTN_1）に対して異なる LRG を選択することにより、サイト RTP および SJC で同じルート パターンおよびルート リストが使用されている場合でも、それぞれの電話からの PSTN コールを、異なるゲートウェイを介してどのように PSTN へストリームするかを示しています。

C：図 2-9　　サイト固有の出力ゲートウェイの選択



C：表 2-51 の例と同じスキーマで考えると、1 つのサイトについて 2 つのデバイス プールをプロビジョニングして、ビデオ会議の機能を備えたデバイスと、備えていないデバイスを区別できるようにする必要があります。ビデオ会議機能が例外になっている場合は、デバイス設定で MRGL を Audio（音声）に設定して、1 つのサイトにつき 1 つのデバイス プールのみを使用し、ビデオ対応の少数のデバイスで MRGL を Video（ビデオ）に設定するように決定できます。

C：表 2-52 は、特定のサイトのゲートウェイで使用されるデバイス プールの設定についてまとめています。ここでは、例としてサイト RTP を使用します。

C：表 2-52　サイト RTP の PSTN ゲートウェイに関するデバイス プールの設定

設定	値	コメント
[デバイスプール名（Device Pool Name）]	[RTP_PSTN]	名前は、このデバイス プールを使用するデバイスを一意に識別できるようなものにします（タイプや詳細な分類など）。この場合は、このデバイス プールをサイト RTP の PSTN ゲートウェイ用に使用します。
[Cisco Unified CM グループ（Cisco Unified Communications Manager Group）]	[CM_1]	
[ローカルルートグループの設定（Local Route Group Settings）]		
[標準ローカル ルート グループ（Standard Local Route Group）]	[RTP_PSTN]	実際には、PSTN トランクで PSTN リソースを必要とするコール フローはありません。ルート グループのセクションの設定順序の注意についても参照してください。デバイス プールを作成する時点では、必要なルート グループはまだ存在していません。したがって、デバイス プールを設定し、LRG マッピングを < なし（None）> に設定しておく必要があります。SIP トランクとルート グループが設定できたら、戻って LRG マッピングを設定することができます。
[LRG_PSTN_1]	< なし >	
[LRG_PSTN_2]	< なし >	
[LRG_VIDEO_1]	< なし >	
[LRG_VIDEO_2]	< なし >	
[LRG_EMERGENCY_1]	< なし >	
[LRG_EMERGENCY_2]	< なし >	
[ローミングに合わせて変化する設定（Roaming Sensitive Settings）]		
[日時グループ（Date/Time Group）]	[RTP_Time]	日付および時刻グループのセクションを参照してください。
[メディアリソースグループリスト（Media Resource Group List）]	[音声（Audio）]	PSTN から着信するコールは、ビデオ会議リソースへアクセスする必要はありません。
[デバイスモビリティ関連情報（Device Mobility Related Information）]		
[AAR コーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	実際には PSTN トランクではほとんど必要ではありませんが、すべてのデバイスおよびデバイス プールで同じにします。
[AAR グループ（AAR Group）]	[デフォルト（Default）]	実際には PSTN トランクではほとんど必要ではありませんが、すべてのデバイスおよびデバイス プールで同じにします。
[発呼側トランスフォーメーション CSS（Calling Party Transformation CSS）]	[RTPGWLocalizeCn]	正当な発呼側情報のみが確実に送信されるようにするためのサイト固有の発呼側トランスフォーメーション（RTP DID の範囲外の番号はすべてマスクされます）。また、番号の文字列が ISDN ゲートウェイに適した形式に設定されます（C：表 2-33 を参照してください）。
[着信側トランスフォーメーション CSS（Called Party Transformation CSS）]	[USGWLocalizeCd]	C：表 2-32 を参照してください。このトランスフォーメーションにより、着呼側の番号が、+E.164 から、プラン **unknown** およびタイプ **unknown** として送信できるような形式に変換されることが保証されます。

C：表 2-52　サイト RTP の PSTN ゲートウェイに関するデバイス プールの設定（続き）

設定	値	コメント
[コールルーティング情報（Call Routing Information）]		
[着信の発呼側設定（Incoming Calling Party Settings）]	ここでは何も設定されません。ISDN の番号形式から +E.164 へのトランスフォーメーションは、ゲートウェイ上で Cisco IOS の音声変換ルールを使用して行われることを前提としています（インバウンド コール：ISDN ゲートウェイでの着信者番号および発信者番号のトランスフォーメーションのセクションを参照してください）。	
[着信の着呼側設定（Incoming Called Party Settings）]		

C：表 2-53 は、他の Unified CM クラスタおよびアプリケーション サーバへの、SIP トランクに関するデバイス プールの設定についてまとめています。他の Unified CM クラスタへの SIP トランクでは、発呼側および着呼側の情報について変換は必要ありません。着呼側の番号は、ダイヤル プランでプロビジョニングされているダイヤル正規化変換パターンによってすでに +E.164 にグローバル化されているため、およびプロビジョニングされているダイヤル プランに基づいた Unified CM 内部の発呼側の情報は +E.164 または ESN であり、どちらの形式もネット上のクラスタ間コールの状態で有効になるためです。

C：表 2-53　セントラル トランクおよびアプリケーションに関するデバイス プールの設定

設定	値	コメント
[デバイスプール名（Device Pool Name）]	[Trunks_and_Apps]	名前は、このデバイス プールを使用するデバイスを一意に識別できるようなものにします（タイプや詳細な分類など）。
[Cisco Unified CM グループ（Cisco Unified Communications Manager Group）]	[CM_1]	
[ローカルルートグループの設定（Local Route Group Settings）]		
[標準ローカル ルート グループ（Standard Local Route Group）]	[RTP_PSTN]	実際にはトランクで PSTN へのアクセスは必要ありませんが、アプリケーションでは PSTN へのアクセスが必要になる場合があります。そのため、1 つのサイトの PSTN リソースは、[標準ローカルルートグループ（Standard Local Route Group）] の設定を介して選択します。他のサイトの PSTN リソースはフェールオーバーとして使用できます。
[LRG_PSTN_1]	[RTP_PSTN]	
[LRG_PSTN_2]	[SJC_PSTN]	
[LRG_VIDEO_1]	< なし >	
[LRG_VIDEO_2]	< なし >	
[LRG_EMERGENCY_1]	< なし >	
[LRG_EMERGENCY_2]	< なし >	
[ローミングに合わせて変化する設定（Roaming Sensitive Settings）]		
[日時グループ（Date/Time Group）]	[RTP_Time]	日付および時刻グループのセクションを参照してください。
[メディアリソースグループ リスト（Media Resource Group List）]	[ビデオ（Video）]	クラスタ間コールでは、ビデオ メディア リソースが必要になる可能性があります。

C：表 2-53　セントラル トランクおよびアプリケーションに関するデバイス プールの設定（続き）

設定	値	コメント
[デバイスモビリティ関連情報（Device Mobility Related Information）]		
[AAR コーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	すべてのデバイスおよびデバイス プールで同じです。
[AAR グループ（AAR Group）]	[デフォルト（Default）]	すべてのデバイスおよびデバイス プールで同じです。
[発呼側トランスフォーメーション CSS（Calling Party Transformation CSS）]	< なし >	クラスタ間のトランクと、アプリケーション サーバに対するトランクで変換はありません。
[着信側トランスフォーメーション CSS（Called Party Transformation CSS）]	[USGWLocalizeCd]	クラスタ間のトランクと、アプリケーション サーバに対するトランクで変換はありません。
[コールルーティング情報（Call Routing Information）]		
[着信の発呼側設定（Incoming Calling Party Settings）]	設定はありません。発呼側および着呼側の番号はすでに正規化されていると仮定しています。	
[着信の着呼側設定（Incoming Called Party Settings）]		

SIP トランク

コール制御、アプリケーション、会議リソースなどの他のエンティティへのすべての接続は SIP トランクを使用します。

SIP プロファイル

SIP プロファイルは、SIP トランクおよび SIP エンドポイントに関連付けられている一連の SIP 属性で構成されています。SIP プロファイルの数を最小に保持するには、次のルールに従います。

- 最初にデフォルトのプロファイルを考慮します。
- 次に、すでに定義されているデフォルト以外のプロファイルを考慮します。
- デフォルトのプロファイルが一致しなかった場合のみ、新しい SIP プロファイルを作成します。
- トランクごとにプロファイルを定義しないようにします。

C：表 2-54 は、他の Unified CM クラスタまたは SIP ゲートウェイへのすべての SIP IP 電話および SIP トランクで使用する SIP プロファイルについての設定を示しています。

C：表 2-54　SIP 電話および標準トランク向けの SIP プロファイル

設定	値	コメント
[標準 SIP プロファイルのコピー（Copy of Standard SIP Profile）]		
[名前（Name）]	[FQDN]	

C：表 2-54　SIP 電話および標準トランク向けの SIP プロファイル（続き）

設定	値	コメント
[SIP 要求で完全修飾ドメイン名を使用（Use Fully Qualified Domain Name in SIP Requests）]	オン	Unified CM サーバの IP アドレスが、Unified CM によって送信される SIP の発呼側情報に表示されないようにします。
[音声コールとビデオコールに対する早期オファーサポート（Early Offer support for voice and video calls）]	[ベストエフォート（MTP の挿入なし）]	これは、すべての Unified CM トランクに対して推奨される設定です。ベスト エフォート早期オファー トランクは早期オファーを作成するために MTP を使用することはありませんが、発信側デバイスによっては早期オファーまたは遅延オファーのいずれかを使用して、送信 SIP トランクを開始することができます。この設計では、発信コールは常に早期オファーを使用します。
[サービスタイプ " なし（デフォルト）" のトランクの接続先ステータスをモニタするために OPTIONS Ping を有効にする（Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"）]	オン	SIP トランク ピアの到達性の監視を可能にします（SIP トランクのみに適用されます）。
[インサービスおよび一部インサービスのトランクの Ping 間隔（秒）（Ping Interval for In-service and Partially In-service Trunks (seconds)）]	[10]	再試行回数 6 回で 10 秒ごとに ping を実行し、SIP トランクが使用不可能な状態が 1 分以内に確実に検出されるようにします。
[アウトオブサービスのトランクの Ping 間隔（秒）（Ping Interval for Out-of-service Trunks (seconds)）]	[60]	トランクが停止または使用不可の場合は、ここで設定した秒数を経過するまでピアへの到達を試行する必要はありません。
[Ping 再試行タイマー（ミリ秒）（Ping Retry Timer（milliseconds））]	[500]	
[Ping 再試行数（Ping Retry Count）]	[6]	

SIP トランク セキュリティー　プロファイル

Cisco CallManager Administration は SIP トランク セキュリティ関係の設定（デバイス セキュリティ モード、ダイジェスト認証、着信 / 発信転送タイプの設定など）をグループ化して、[SIP トランクの設定（SIP Trunk Configuration）] ウィンドウでプロファイルを選択するときに、設定したすべての内容を 1 つの SIP トランクに適用することができます。

C：表 2-55 は、SIP トランクのセキュリティ プロファイルである非セキュア SIP トランク プロファイル（Non Secure SIP Trunk Profile）で生成された、システム上のデフォルト設定について示しています。この SIP トランク セキュリティ プロファイルは、ISDN PSTN ゲートウェイ向けの SIP トランクなどで使用されます。

C：表 2-55　SIP トランク セキュリティ プロファイル（非セキュア SIP トランク プロファイル）の設定

設定	値
名前（Name）	非セキュア SIP トランクプロファイル（Non Secure SIP Trunk Profile）
デバイスセキュリティモード（Device Security Mode）	非セキュア（Non Secure）
着信転送タイプ（Incoming Transport Type）	TCP+UDP
発信転送タイプ（Outgoing Transport Type）	[TCP]
[ダイジェスト認証を有効化（Enable Digest Authentication）]	オフ
[着信ポート（Incoming Port）]	[5060]
[アプリケーションレベル認証を有効化（Enable Application Level Authorization）]	オフ
[プレゼンスの SUBSCRIBE の許可（Accept Presence Subscription）]	オフ
[Out-of-Dialog REFER の許可（Accept Out-of-Dialog REFER）]	オフ
[Unsolicited NOTIFY の許可（Accept unsolicited notification）]	オフ
[Replaces ヘッダーの許可（Accept replaces header）]	オフ
[セキュリティステータスの送信（Transmit security status）]	オフ
[Charging ヘッダーの許可（Allow charging header）]	オフ
[SIP V.150 アウトバウンド SDP オファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）]	[デフォルトのフィルタを使用（Use Default Filter）]

C：表 2-56 は、IM and Presence ノード向けの SIP トランクで使用される SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）の設定について示しています。これは、C：表 2-55 のデフォルトの設定とは異なります。

C：表 2-56　IM と Presence トランク向けの SIP トランク セキュリティ プロファイル

設定	値	コメント
名前	[IM と Presence]	SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）の用途を説明するためのわかりやすい名前。
[プレゼンスの SUBSCRIBE の許可（Accept Presence Subscription）]	オン	

C：表 2-56　IM と Presence トランク向けの SIP トランク セキュリティ プロファイル

設定	値	コメント
[Out-of-Dialog REFER の許可（Accept Out-of-Dialog REFER）]	オン	
[Unsolicited NOTIFY の許可（Accept unsolicited notification）]	オン	
[Replaces ヘッダーの許可（Accept replaces header）]	オン	

C：表 2-57 は、他の Unified CM クラスタへのクラスタ間トランクで使用する SIP トランク セキュリティ プロファイルの設定について示しています。これらのトランクでは、プレゼンスの SUBSCRIBE を許可して、クラスタ間のビジー ランプ フィールド（BLF）プレゼンスを有効にするとよいでしょう。

C：表 2-57　クラスタ間トランクの SIP トランク セキュリティ プロファイル

設定	値	コメント
名前	[ICT]	SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）の用途を説明するための名前。
[プレゼンスの SUBSCRIBE の許可（Accept Presence Subscription）]	オン	
[セキュリティステータスの送信（Transmit security status）]	オン	

SIP トランク接続

SIP トランクは、Unified CM のクラスタ間、および Unified CM と（ゲートウェイ、アプリケーション、メディア リソースなどの）他のシステム間での接続を設定する場合に推奨される方法です。接続するシステムのタイプによって、各 SIP トランクで設定されるパラメータは少し異なります。C：表 2-58 は、サイト RTP における、PSTN ゲートウェイ向けの SIP トランクについての設定をまとめて示しています。

C：表 2-58　サイト RTP での ISDN ゲートウェイ向けトランクの SIP トランク設定

設定	値	コメント
名前	[ST_RTP_PSTN_1]	同じテーブルに内部で格納されている他のデバイスとの名前のコリジョン（衝突）を回避するためのプレフィックス ST_。名前の残りの部分はゲートウェイの場所を特定するもので、複数のゲートウェイに対して数字を割り当てることができます。
[説明（Description）]		わかりやすい説明

C：表 2-58　サイト RTP での ISDN ゲートウェイ向けトランクの SIP トランク設定（続き）

設定	値	コメント
[デバイスプール（Device Pool）]	[RTP_PSTN]	すべての RTP PSTN ゲートウェイに対する共通のデバイス プール。すべての RTP ゲートウェイ間でサイト特定の設定を共有できるようにします。
[メディアリソースグループリスト（Media Resource Group List）]	< なし >	デバイス プールで定義されている MRGL を使用します。
[AAR グループ（AAR Group）]	[デフォルト（Default）]	すべての場所で同じ
[PSTN アクセス（PSTN Access）]	オン	
[すべてのアクティブな Unified CM ノードで実行（Run on All Active Unified CM Nodes）]	オン	この設定は、すべての SIP トランクで推奨されます。この設定により、SIP への発信コールで、Unified CM コールを処理するサブスクライバ間でのクラスタ間のシグナリング制御が不要になります。
[着信コール（Inbound Calls）]		
[コーリングサーチスペース（Calling Search Space）]	[DN]	着信コールには +E.164 の着呼側の番号が定義されているため、PSTN からコールできるのはローカルな通知先のみになります。したがって、ESN 番号およびクラスタ間の通知先へはアクセスする必要はありません。
[AAR コーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	
[アウトバウンドコール（Outbound Calls）]		
[デバイスプールの着信側トランスフォーメーション CSS を使用（Use Device Pool Called Party Transformation CSS）]	オン	
[デバイスプールの発呼側トランスフォーメーション CSS を使用（Use Device Pool Calling Party Transformation CSS）]	オン	
[SIP 情報（SIP Information）]		
接続先	[X.X.X.X]	ISDN ゲートウェイの IP アドレス
[SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）]	[非セキュア SIP トランクプロファイル（Non Secure SIP Trunk Profile）]	デフォルトの SIP トランク セキュリティ プロファイル
[SIP プロファイル（SIP Profile）]	[FQDN]	

ここでは、着信 CSS はローカルな +E.164 の通知先のみにアクセスを提供することがポイントです。これらの通信先には、ボイスメール パイロットや、PSTN から到達可能であることが必要な他のサービスが含まれますが、PSTN のルート パターン、ダイヤル正規化変換パターン、ESN、URI、およびクラスタ間の通知先へのアクセスは必要ありません。

他の Unified CM クラスタへの SIP トランクの設定は、ISDN ゲートウェイへの SIP トランクの設定とは少し異なります。C：表 2-59 に、これらの設定を要約します。

C：表 2-59　他の Unified CM クラスタ向けクラスタ間トランクについての SIP トランクの設定

設定	値	コメント
名前	[ST_UCM_EMEA]	同じテーブルに内部で格納されている他のデバイスとの名前のコリジョン（衝突）を回避するためのプレフィックス ST_。名前の残りの部分は、トランクの目的を表します。
[説明（Description）]		わかりやすい説明
[デバイスプール（Device Pool）]	[Trunks_and_Apps]	セントラル トランクに対する共通のデバイス プール（C：表 2-53 を参照してください）。
[メディアリソースグループリスト（Media Resource Group List）]	< なし >	デバイス プールで定義されている MRGL を使用します。
[AAR グループ（AAR Group）]	[デフォルト（Default）]	すべての場所で同じ
[PSTN アクセス（PSTN Access）]	オフ	
[すべてのアクティブな Unified CM ノードで実行（Run on All Active Unified CM Nodes）]	オン	この設定は、すべての SIP トランクで推奨されます。この設定により、SIP への発信コールで、Unified CM コールを処理するサブスクライバ間でのクラスタ間のシグナリング制御が不要になります。
[着信コール（Inbound Calls）]		
[コーリングサーチスペース（Calling Search Space）]	[ICTInbound]	トランク上の着信コールは +E.164、ESN、および URI ダイヤルをサポートしている必要があります。この特別な CSS は、3 つのダイヤリング手順をすべてサポートしていますが、PSTN またはリモートのネット上での通知先へのアクセスは提供していません（特殊な CSS のセクションの C：表 2-24 を参照してください）。 PSTN へのアクセスが必要なアプリケーションについては、PSTN アクセス ルート パターンを使用してパーティションへアクセスするために、もうひとつの特別なサービス クラス（CSS）が必要になります（PSTN アクセスと緊急コールのルート パターンのセクションの C：表 2-27 を参照してください）。
[AAR コーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	すべての場所で同じ CSS
[アウトバウンドコール（Outbound Calls）]		
[デバイスプールの着信側トランスフォーメーション CSS を使用（Use Device Pool Called Party Transformation CSS）]	オン	
[デバイスプールの発呼側トランスフォーメーション CSS を使用（Use Device Pool Calling Party Transformation CSS）]	オン	

C：表 2-59　他の Unified CM クラスタ向けクラスタ間トランクについての SIP トランクの設定（続き）

設定	値	コメント
[発呼側および接続側情報形式（Calling and Connected Party Info Format）]	[接続側にのみ URI および DN を配信（使用可能な場合）（Deliver URI and DN in connected party, if available）]	他の Unified CM クラスタ向けのクラスタ間トランクで、数値の ID と URI 情報の ID の 2 つが混在している場合は、リモート クラスタに配信する必要があります。2 つのタイプの ID が存在する場合は、着呼側のエンドポイント機能に基づいて、コールを終了するクラスタが ID 情報のどの部分を最終的な着信側に表示するかを決定することができます。
[SIP 情報（SIP Information）]		
接続先	[X.X.X.X]	リモートの Unified CM クラスタのサブスクライバを処理する、すべての Unified CM コールの IP アドレスがリストされます。発信コールは、定義された通知先の中でランダムに配信されるため、IP アドレスの順序は関連していません。
[SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）]	[ICT]	C：表 2-57 を参照してください
[SUBSCRIBE コーリングサーチスペース（AAR Calling Search Space）]	[ICTInbound]	+E.164、ESN、および URI のサブスクリプションを許可する必要があります。CSS の定義については、特殊な CSS のセクションを参照してください。
[SIP プロファイル（SIP Profile）]	[FQDN]	C：表 2-54 を参照してください

PSTN ISDN ゲートウェイ向けの SIP トランクとは異なり、+E.164 番号だけでなく他の Unified CM クラスタからの着信コールも ESN と URI へのアクセスが必要です。ただし、ルーティングのループやトランジット ルーティングを回避するために、クラスタ間のトランクはクラスタ間の通知先（パーティション onNetRemote、C：表 2-12 を参照）へのアクセス権を持っていません。

IM と Presence ノードへの SIP トランクについては、Unified CM と IM と Presence 間の SIP トランクを設定します。SIP トランクについては、IM と Presence のすべてのノードの通知先 IP アドレスを設定します。IM と Presence サービスに対して自身が設定した SIP トランク セキュリティ プロファイルを選択します。標準の SIP プロファイルも選択します。

ルート グループ

すべての SIP トランクはルート グループに割り当てられます。ルート グループは、トランクと、共通の特性を組み合わせます。C：表 2-60 は、サイト RTP における PSTN ゲートウェイに対するルート グループの定義を示しています。

C：表 2-60　RTP PSTN ゲートウェイに対するルート グループ

設定	値	コメント
[ルートグループ名（Route Group Name）]	[RTP_PSTN]	わかりやすい名前
[分配アルゴリズム（Distribution Algorithm）]	[ラウンドロビン（Circular）]	ゲートウェイ全体で確実に負荷を均等化できるようにします。
[ルートグループメンバ（Route Group Members）]	[ST_RTP_PSTN_1] [ST_RTP_PSTN_2] [ST_RTP_PSTN_3]	サイト RRP のすべての SIP ゲートウェイにすべての SIP トランクを追加します。

注　ルート グループは、SIP トランクが作成された後でのみ設定することが可能で、SIP トランクは、それぞれのデバイス プールが設定された後でのみ追加することが可能です。これは、PSTN ゲートウェイに対してデバイス プールを作成するときには、ルート グループはまだ存在していないことを意味しています。したがって、設定の順序は次のようになります。

1. デバイス プールで LRG マッピングを定義せずに、PSTN ゲートウェイに対するデバイス プールを設定します。
2. SIP トランクを設定します。
3. ルート グループを作成します。
4. デバイス プールに戻り、（必要に応じて）LRG マッピングを追加します。

他の Unified CM クラスタ向けのクラスタ間トランクでは、1 つのトランクにつき 1 つのルート グループを定義する必要があります。C：表 2-61 は、リモート Unified CM クラスタ向けのクラスタ間トランクに対するルート グループの例を示しています。

C：表 2-61　他の Unified CM クラスタ向けのクラスタ間トランクのルート グループ

設定	値	コメント
[ルートグループ名（Route Group Name）]	[UCM_EMEA]	わかりやすい名前。この場合は、EMEA Unified CM クラスタ向けのクラスタ間トランクのみを保持しているルート グループの名前。
[分配アルゴリズム（Distribution Algorithm）]	[ラウンドロビン（Circular）]	ルート グループ メンバーが 1 つだけ存在する場合は不適切。
[ルートグループメンバ（Route Group Members）]	[ST_UCM_EMEA]	リモート Unified CM クラスタ向けの SIP トランク。

Unified CM にプロビジョニングされているそれぞれの非 PSTN SIP トランクに対しては、簡単な類似のルート グループを作成する必要があります。

特定の非 LRG ルート リスト

ローカル ルート グループを使用するルート リストのセクションでは、ローカル ルート グループのみを使用した PSTN アクセスのルート リストについて概要を説明します。非 PSTN トランクでは、特定のルート リストは、これらの非 PSTN トランクを参照するルート グループを使用して作成する必要があります。1 つのメンバーのみを持つ簡単なルート グループと、メンバーとして 1 つの非 LRG ルート グループのみを持つ簡単なルート リストを定義する理由は、Unified CM のルート パターンはトランクを直接指定しないためです。具体的には、Unified CM でルート パターンが変更されるたびに、ルート パターンが指定しているデバイスがリセットされます。（トランクの代わりに）ルート リストに対してルート パターンを指定すると、ルート パターンの編集によってトランク自身はリセットされずに、ルート リストがリセットされます。このようなトランクの例として、他の Unified CM クラスタおよびアプリケーション向けのトランクが含まれます。

C：表 2-62 は、他の Unified CM クラスタ向けのクラスタ間トランクの簡単なルート リストを示しています。

C：表 2-62　他の Unified CM クラスタ向けのクラスタ間トランクのルート リスト

ルート リスト	メンバー	説明
[RL_UCM_EMEA]	[UCM_EMEA]	1 つのメンバーのみ（リモート Unified CM クラスタ向けの実際のトランク）。先頭の RL により、トランクと命名のコリジョンが発生しないことが保証されます。内部ではルート リストはデバイスとして扱われ、ルート リストの名前は SIP トランクなどの名前と同じにすることはできません。

Unified CM にプロビジョニングされているそれぞれの非 PSTN SIP トランクに対しては、簡単な類似のルート リストを作成する必要があります。

エンドポイントのプロビジョニング

新しいエンドポイントをプロビジョニングする場合には、次の最小限のタスクが必要です。

- デバイスの設定
- 回線の設定
- ユーザーが制御するデバイスへデバイスを追加する
- プレゼンスに対する回線の関連付けの設定

デバイスの設定

Unified CM に新しいエンドポイントを追加する場合は、このドキュメントで説明している設計では、C：表 2-63 に要約されている設定が必要です。ここに記載されていない設定はデフォルトのままにしておくか、または、デバイス特有の要件に従って設定する必要があります。

C：表 2-63　エンドポイントのデバイス設定

定設	値	説明
[デバイス情報（Device Information）]		
[デバイスプール（Device Pool）]	[RTPPhoneVideo]	エンドポイントに対するサイト固有のデバイス プール（C：表 2-51 を参照してください）。この場合には、ビデオ会議メディア リソースへのアクセス権を持つサイト RTP 内のエンドポイントに対するデバイス プールになります。
[コーリングサーチスペース（Calling Search Space）]	[USEmergency]	多国籍環境でのイマージェンシー ルーティングへのアクセスは、デバイス レベルで実現されます（多国間環境における緊急コールの考慮事項を参照してください）。US などの 1 つの国（ダイヤル ドメイン）をサポートする必要がある場合は、この CSS は < なし（None）> のままにすることもできます。
[AAR コーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	すべての場所で同じ（自動代替ルーティングのセクションを参照してください）。
[メディアリソースグループリスト（Media Resource Group List）]	< なし >	デバイス プール レベルの設定を使用します。
[AAR_Group]	デフォルト	すべての場所で同じ（自動代替ルーティングのセクションを参照してください）。
[オーナー（Owner）]	" ユーザ " の選択	デバイスが、ユーザが関連付けされていない電話（ロビーにある電話など）である場合は、[匿名（公共 / 共有スペース）（Anonymous（Public/Shared Space））] を選択し、[オーナーのユーザ ID（Owner User ID）] は選択しません。
[オーナーのユーザ ID（Owner User ID）]	この電話の所有者のユーザ ID を選択します。	
[CTI からのデバイスの制御を許可（Allow Control of Device from CTI）]	オン	
[番号表示トランスフォーメーション（Number Presentation Transformation）]		
[この電話からのコールの発信者 ID（Caller ID For Calls From This Phone）]	[デバイス プールの発呼側トランスフォーメーション CSS を使用（この電話からのコールの発信者 ID）（Device Pool Calling Party Transformation CSS (Caller ID For Calls From This Phone)）] をオンにする	
[リモート番号（Remote Number）]	[デバイス プールの発呼側トランスフォーメーション CSS を使用（デバイス モビリティ関連情報）（Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)）] をオンにする	
[プロトコル固有情報（Protocol Specific Information）]		

C：表 2-63　エンドポイントのデバイス設定（続き）

定設	値	説明
[SIP プロファイル（SIP Profile）]	[FQDN]	C：表 2-54 を参照してください

回線の設定

各エンドポイントで、少なくとも最初の回線をプロビジョニングする必要があります。C：表 2-64 は、このドキュメントに記載されている設計固有の回線設定について説明しています。

C：表 2-64　回線の設定

設定	値	説明
[電話番号情報（Directory Number Information）]		
[電話番号（Directory Number）]	[\+14085554146]	この DN がプロビジョニングされているユーザの電話番号と一致する、完全な +E.164 の電話番号。先頭の + はスラッシュ（\）でエスケープする必要があります。非 DID がプロビジョニングされている場合、電話番号は（81405001 などのように）ESN に設定されます。
[ルートパターン（Route Pattern）]	[DN]	非 DID がプロビジョニングされている場合、この部分は ESN になります。
[呼び出し表示（Alerting Name）]	[Aristotle Boyle]	この番号に関連付けられているユーザのフル ネーム。番号がユーザに関連付けられていない場合、わかりやすい名前をプロビジョニングします（たとえば「Bldg. 31 Lobby」つまり第 31 ビルのロビー）。
[CTI からのデバイスの制御を許可（Allow Control of Device from CTI）]	オン	
[電話番号の設定（Directory Number Settings）]		
[コーリングサーチスペース（Calling Search Space）]	[SJCInternational]	この回線からのコールに対する実際のサービス クラスを定義している CSS。CSS はサイトおよびサービス クラス固有のものです（他の CSS についてはサービス クラスとコーリング サーチ スペース（CSS）を参照してください）。
[BLF プレゼンスグループ（BLF Presence Group）]	標準のプレゼンス グループ	すべての回線について同じ
[+E.164 代替番号（+E.164 Alternate Number）]		
[番号マスク（Number Mask）]	マスクを空のままにしておく	マスクを空にしておくと、上記で設定された電話番号と同じ +E.164 代替番号が作成されます。非 DID がプロビジョニングされている場合は、非 DID には定義により PSTN アドレスが存在しないため、+E.164 代替番号が追加されます。

C：表 2-64　回線の設定（続き）

設定	値	説明
[ローカルルートパーティションに追加（Add to Local Route Partition）]	オフ	電話番号にはすでに +E.164 の番号が存在するため、+E.164 代替番号はローカル ルート パーティションには追加されません。
[ILS を介してグローバルにアドバタイズ（Advertise Globally via ILS）]	オフ	+E.164 代替番号は ILS を介してアドバタイズされません。代わりに、各 DID 範囲に対するサマリ ルートがアドバタイズされます（C：表 2-68 を参照してください）。+E.164 代替番号を作成する唯一の理由は、この +E.164 代替番号を、この電話番号に関連付けられている URI の GDPR PSTN フェールオーバー番号としてアドバタイズできることです。
[エンタープライズ代替番号、+E.164 代替番号、および URI ダイヤリングの PSTN フェールオーバー（PSTN Failover for Enterprise Alternate Number, +E.164 Alternate Number, and URI Dialing）]		
[アドバタイズされたフェールオーバー番号（Advertised Failover Number）]	[+E.164 番号（Advertised Failover Number）]	+E.164 番号は GDPR PSTN としてアドバタイズされます。非 DID がプロビジョニングされている場合は、< なし（None）> に設定します。
[AAR 設定（AAR Settings）]		
[ボイスメール（Voicemail）]	オフ	非 DID がプロビジョニングされている場合は、このオプションをオンにします。
[AAR 接続先マスク（AAR Destination Mask）]	+14085554XXX	この DID 範囲マスクにより、AAR に対する代わりの PSTN 通知先が電話番号と同じであることが保証されます。非 DID がプロビジョニングされている場合は、このマスクを空のままにします。
[AAR グループ（AAR Group）]	[デフォルト（Default）]	すべての場所で同じ
[コール転送とコールピックアップの設定（Call Forward and Call Pickup Settings）]		
Calling Search Space Activation Policy	[システムデフォルトの使用（Use System Default）]	
[不在転送（Forward All）]	[ボイスメール（Voicemail）] をオフに設定する [コーリングサーチスペース（Calling Search Space）]：SJCInternational	より限定的な CSS に設定される可能性があります。
[未登録内線の不在転送（Forward Unregistered Internal）] および [未登録外線の不在転送（Forward Unregistered External）] 以外のすべての転送の設定	[ボイスメール（Voicemail）] をオフに設定する [コーリングサーチスペース（Calling Search Space）]：SJCInternational	より限定的な CSS に設定される可能性があります。

C：表 2-64　回線の設定（続き）

設定	値	説明
[未登録内線の不在転送（Forward Unregistered Internal）] および [未登録外線の不在転送（Forward Unregistered External）]	[通知先（Destination）]：+14085554146 [コーリングサーチスペース（Calling Search Space）]：PSTNReroute	エンドポイントが未登録の場合、未登録転送は PSTN を介して代替ルートを実装します。これは、PSTN を介して代替ルートが確立できるローカル PSTN へのアクセスを持つ、リモート サイトのエンドポイントでのみ有効です。 非 DID がプロビジョニングされている場合、または PSTN がリルートする DN が有効ではない場合は、[ボイスメール（Voicemail）] をオンにして、CSS を SJCInternational、またはボイスメール パイロットに到達可能な他の CSS に設定します。
[デバイスの回線 1（Line 1 on Device）]		
[表示（発信者 ID）（Display (Caller ID)）]	[Aristotle Boyle]	この番号に関連付けられているユーザのフル ネーム。番号がユーザに関連付けられていない場合は、わかりやすい名前をプロビジョニングします（たとえば「Bldg. 31 Lobby」つまり第 31 ビルのロビー）。
[回線のテキストラベル（Line Text Label）]	4146	電話の回線ボタンの隣に、電話番号の最後の 4 桁が表示されるようになります。この設定は、回線テキスト ラベルをサポートしているデバイス上の回線にのみ存在します。
[外線電話番号マスク（External Phone Number Mask）]	+14085554XXX	外線電話番号のマスクは、プロビジョニングされているダイヤル プランの中では参照されず、任意に設定することができます。外線電話番号のマスクが、電話表示における最初の回線のテキストを決定する電話の場合は、マスクを、意味のあるラベルを作成するものに設定することができます。

ユーザーが制御するデバイスへデバイスを追加する

ユーザに関連付けられているデバイスでは、Unified CM Administration の [デバイス情報（Device Information）] セクションにおいて各ユーザの [エンドユーザの設定（End User Configuration）] でデバイスをプロビジョニングした後で、デバイスがユーザに関連付けられていることを確認します。これを実行するための推奨される方法は、[デバイスの割り当て（Device Association）] を選択し、ユーザの電話番号と一致する電話番号を持つデバイスを検索することです。

プレゼンスに対する回線の関連付けの設定

ユーザのプレゼンス状態を決定するために、プレゼンスに明示的に関連付けられている（DN およびデバイスごとの）ライン アピアランスのみが考慮されます。ユーザの電話番号のすべてのライン アピアランスがプレゼンスに対して考慮されることを確認するには、Unified CM Administration の [デバイス情報（Device Information）] のセクションで各ユーザの [エンドユーザの設定（End User Configuration）] で、[プレゼンスのラインアピアランス関連付け（Line Appearance Association for Presence）] を選択し、すべてのライン アピアランスを関連付けます。

ユーザーのプライマリー内線の確認

LDAP から同期されているユーザのディレクトリ URI が電話番号へ反映されていることを確認するには、Unified CM Administration で各ユーザの [エンドユーザの設定（End User Configuration）] の [電話番号の割り当て（Directory Number Associations）] セクションにおいて、[プライマリ内線（Primary Extension）] を選択します。

Jabber プロビジョニング

Service Discovery により、Jabber が自動的に設定を確立することができます。Jabber クライアントは Unified CM User Discovery Service（UDS）を介して自身の設定を取得します。これは推奨される設定で、以前の手動による設定よりも優先されます。

サービスは UC サービスを介して設定されます。サービス プロファイルは、どの UC サービスを使用するかを指定します。各ユーザは、1 つのサービス プロファイルに関連付けられています。

C：表 2-65 は、Jabber クライアントで使用することができる UC サービスを示しています。これらのサービスは [ユーザ（User）] > [ユーザ設定（User Settings）] > [UC サービス（UC service）] で設定されます。

C：表 2-65　UC サービス

UC サービスのタイプ	コメント
[IM と Presence]	各 IM と Presence ノードに対して IM と Presence サービスを作成します。
[ディレクトリ（Directory）]	アクティブなディレクトリ サーバについてそれぞれディレクトリ サービスを作成します。LDAP ディレクトリと統合する場合は、[連絡先の解決に UDS を使用する（Use UDS for Contact Resolution）] を選択しないでください。オンプレミス展開で推奨されている連絡先ソースは CDI です。
[CTI]	CTI Manager サービスを実行している各 Unified CM に対して CTI サービスを作成します。これは、デスク電話の制御モードで使用されます。Unified CM のすべてのコール処理ノードで、CTI の負荷を均衡にします。
[ボイスメール（Voicemail）]	各 Unity Connection ノードに対してボイスメール サービスを作成します。

UC サービスをサービス プロファイルに関連付けます。次に、サービス プロファイルを各ユーザに関連付けます。複数の Unified CM 呼処理サブスクライバを備えている展開では、Unified CM のすべての呼処理サブスクライバに対して CTI の負荷を均等に分散させて、CTI の拡張性制限が、CTI Manager サービスを実行している単一の Unified CM の呼処理サブスクライバを超えないようにします。Jabber クライアントを、CTI Manager サービスを実行しているもう 1 つの Unified CM の呼処理に関連付けるには、関連する CTI UC サービスの設定を使用してもう 1 つのサービス プロファイルを設定します。

（Cisco Collaboration Edge を使用せずに）内部のエンタープライズ ネットワークに接続しているユーザに対しては、UDS または LDAP を介してディレクトリ検索 Contact Sources を提供することができます。LDAP では、Cisco Directory Integration（CDI）を使用できます。Contact Source またはディレクトリは、jabber-config.xml ファイルまたは UC サービスを介して設定することができます（UC サービスが優先されます）。この場合には、Unified CM TFTP サーバへアップロードされている jabber-config.xml ファイルを設定することが推奨されます。jabber-config.xml ファイルは、Jabber クライアント用の URI ダイヤルを有効にする場合にも使

用します。C：例 2-5 は、jabber-config.xml ファイルによる Jabber クライアント用の URI ダイヤルの有効化について示しています。これは最小限の推奨事項です。これ以外の設定オプションを追加することもできます。

C：例 2-5　jabber-config.xml ファイルによる URI ダイヤルの有効化

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
    <Policies>
        <EnableSIPURIDialling>true</EnableSIPURIDialling>
    </Policies>
</config>
```

詳しくは、次のドキュメントの最新版を参照してください。

- *Cisco Unified Communications Manager での IM と Presence の設定と管理*

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

- Cisco Jabber Install and Upgrade Guides

  https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

マルチクラスター展開向けの ILS 設定

複数のクラスタ上にクラスタ間検索サービス（ILS）を設定した場合、ILS は、ILS ネットワーク内のリモート クラスタの現在のステータスで Unified CM を更新します。

ILS のクラスタ検出サービスを使用すると、管理者が各クラスタ間の接続を手動で設定しなくても Unified CM はリモート クラスタの詳細を知ることができます。

ILS クラスタ検出サービスにより、マルチクラスタ環境の Jabber クライアントに対して UDS ベースのサービス検出を実現できます。また、ILS はグローバル ダイヤル プラン レプリケーションのベースとなるもので、これにより Unified CM クラスタ間の英数字 URI と数字の通知先の両方について、到達性の情報のやりとりを可能にします。

複数の Unified CM クラスタの ILS ネットワークを作成するには、次のタスクを実行します。

- ネットワーク内の各 United CM クラスターに対いて一意のクラスター ID を割り当てる
- ネットワーク内の最初の ILS ハブ クラスターで ILS をアクティブにする
- ネットワーク内の残りの ILS クラスターで ILS をアクティブにする
- UDS 証明書要件の検討事項

ネットワーク内の各 United CM クラスターに対いて一意のクラスター ID を割り当てる

Unified CM クラスタのエンタープライズ パラメータに定義されているクラスタ ID は一意である必要があります。詳細については、C：表 2-2 を参照してください。

ネットワーク内の最初の ILS ハブ クラスターで ILS をアクティブにする

ILS ネットワークの構築は、最初の Unified CM クラスタ上で ILS をアクティブにすることから始めます。アクティブにするには、最初に Unified CM Administration の [ILS 設定（ILS Configuration）] メニューで、役割を [スタンドアロンクラスタ（Standalone Cluster）] から [ハブクラスタ（Hub Cluster）] へ変更します。

C：表 2-66 は、最初の Unified CM クラスタで ILS をアクティブにするときに適用される設定を示しています。

C：表 2-66　最初の Unified CM クラスタでの ILS のアクティベーション

設定	値	コメント
[役割（Role）]	[ハブクラスタ（Hub Cluster）]	役割を [スタンドアロンクラスタ（Standalone Cluster）] から [ハブクラスタ（Hub Cluster）] へ変更して、ILS をアクティブにします。
[リモートクラスタとのグローバルダイヤルプランのレプリケーションデータの交換（Exchange Global Dial Plan Replication Data with Remote Clusters）]	オン	URI および数字の到達性情報が、リモート クラスタとやりとりされることを確認します。
[アドバタイズされたルート文字列（Advertised Route String）]	us.route	アドバタイズされたルート文字は、この Unified CM クラスタにアドバタイズされるすべての URI および数字の到達性情報に関連付けられているロケーション属性です。このクラスタによってアドバタイズされるいずれかの通知先に到達しようとするリモート クラスタは、学習した SIP ルート文字列をリモート クラスタ上でプロビジョニングされた SIP ルート パターンに照合して、この通知先へのルートを確立しようとします。
[クラスタ同期間隔（Synchronize Clusters Every）]	2	同期間隔を適度に小さく設定すると、リモート クラスタによって短期間で変更が取得されることが保証されます。GDPR は差分更新のアルゴリズムを使用しており、これは最後の更新後に何らかの変更が生じた場合に、差分の情報のみをやりとりするため、間隔を短期間にすることのオーバーヘッドは制限定されます。
[ILS 認証（ILS Authentication）]		
TLS 証明書の使用	オン	証明書に基づく ILS TLS 接続の認証。
[パスワードの使用（Use Password）]	オン	パスワードに基づく承認。
[パスワード（Password）]	パスワード文字列	安全なパスワードを選択します。このパスワードは、ILS ネットワークに属しているすべての Unified CM クラスタ間で共有します。

Unified CM Administration で、役割を [スタンドアロン クラスタ（Standalone Cluster）] から [ハブ クラスタ（Hub Cluster）] に変更することによって ILS をアクティブにすると、[ILS クラスタ登録（ILS Cluster Registration）] ポップアップが表示され、登録サーバを入力するよう要求されます。最初の Unified CM クラスタで ILS をアクティブにするときには、登録サーバの情報を使用できないため、ポップアップの入力は空白のままにしておきます。

[TLS 証明書の使用（Use TLS Certificates）] と [パスワードの使用（Use Password）] の両方を同時にアクティブにした場合、TLS 接続のセットアップ時にリモート エンドから提出される TLS 証明書は通常の TLS 証明書妥当性チェック（同一性、妥当性、および信頼性）に合格するだけでよく、リモート ピアが ILS 通信の信頼されたピアであるかどうかの決定は、共有秘密（パスワード）の検査に基づいて行われます。共有秘密（パスワード）認証を使用しない場合は、ILS 交換に関与するすべてのクラスタのすべての Tomcat 証明書をすべてのクラスタ間で交換する必要があります。共有秘密（パスワード）認証を使用すると、ILS および CA 署名付き証明書の展開が大幅に簡略化されます。

ネットワーク内の残りの ILS クラスターで ILS をアクティブにする

ILS ネットワークへ Unified CM クラスタを追加するには、最初の Unified CM クラスタで ILS をアクティブにするのと同じプロセスが必要です。つまり、Unified CM Administration の [ILS 設定（ILS Configuration）] メニューで、[スタンドアロンクラスタ（Standalone Cluster）] から [ハブクラスタ（Hub Cluster）] へ役割を変更します。

C：表 2-67 は、残りの Unified CM クラスタ上で ILS をアクティブにするときに適用される設定を示しています。

C：表 2-67　残りの Unified CM クラスタでの ILS のアクティベーション

設定	値	コメント
[役割（Role）]	[ハブクラスタ（Hub Cluster）]	役割を [スタンドアロンクラスタ（Standalone Cluster）] から [ハブクラスタ（Hub Cluster）] へ変更して、ILS をアクティブにします。
[リモートクラスタとのグローバルダイヤルプランのレプリケーションデータの交換（Exchange Global Dial Plan Replication Data with Remote Clusters）]	オン	URI および数字の到達性情報が、リモート クラスタとやりとりされることを確認します。
[アドバタイズされたルート文字列（Advertised Route String）]	emea.route	これらのルート文字列に基づいて決定論的ルーティングを可能にするには、各クラスタに対する SIP ルート文字列が一意になるようにします。 この例は、EMEA の通知先として機能する Unified CM クラスタを示しています。
[クラスタ同期間隔（Synchronize Clusters Every）]	2	整合性を保証するために、すべてのクラスタで同じ同期間隔を使用するようにします。
[ILS 認証（ILS Authentication）]		
TLS 証明書の使用	オン	証明書に基づく ILS TLS 接続の認証。
[パスワードの使用（Use Password）]	オン	パスワードに基づく認証が選択されます。
[パスワード（Password）]	パスワード文字列	安全なパスワードを選択します。このパスワードは、ILS ネットワークに属しているすべての Unified CM クラスタ間で共有します。

UDS 証明書要件の検討事項

UDS ベースの検出を可能にするために、それぞれの Unified CM クラスタ上の UDS プロセスは、リモート Unified CM クラスタ上で実行中の UDS プロセスとの接続を確立して、リモート クラスタの UDS ノードについて情報を取得しようとします。このサーバ間通信では、Unified CM クラスタのノード間で TLS 接続が確立され、TLS 接続のセットアップ中にリモート ピアの証明書が検証されます。この検証に失敗しないためには、Unified CM パブリッシャ ノードと呼処理サブスクライバ ノードの Tomcat 証明書に、信頼できる CA が署名する必要があります。

また、外部 CA で Tomcat 証明書を発行するときに X.509 拡張鍵の用途に **TLS Web クライアント認証**を含める必要がある理由の 1 つは、このサーバ間通信です。

GDPR の設定マルチクラスターのみ

ILS ネットワークでグローバル ダイヤル プラン レプリケーション（GDPR）を有効にすると、ILS ネットワーク内のリモート クラスタで、次のようなグローバル ダイヤル プラン データを共有します。

- ディレクトリ URI
- +E.164 および ESN パターン
- PSTN フェールオーバー番号

GDPR では、ILS ネットワーク全体を対象としてディレクトリ URI のクラスタ間ダイヤルや代替番号などのグローバル ダイヤル プランを作成することができます。GDPR を使用すると、各クラスタに対して個別にダイヤル プラン コンポーネントを設定する必要がなく、ILS ネットワーク全体にグローバル ダイヤル プランをすばやく設定できます。

GDPR の設定には、前のセクションで説明した ILS のアクティベーションの他に、次の手順が必要です。

- URI のアドバタイズ
- アドバタイズされたパターンの設定
- 学習番号およびパターンに対するパーティションの設定
- クラスター間のトランクの設定
- SIP ルート パターンの設定

URI のアドバタイズ

このドキュメントでは、ユーザの URI は、社内ディレクトリの電子メール属性から、各ユーザに同期されているディレクトリ URI に基づいて（C：表 2-43 を参照）、および各ユーザに設定されているプライマリ内線に基づいて自動的にプロビジョニングされると仮定しています。デフォルトでは、[ILS を介してグローバルにアドバタイズ（Advertise Globally via ILS）] オプションは、パーティション ディレクトリ URI で自動的に作成された URI に対して設定されています。また、自動的に作成された URI だけでなく、プロビジョニングしたすべての URI について [ILS を介してグローバルにアドバタイズ（Advertise Globally via ILS）] オプションを設定するようにします。

アドバタイズされたパターンの設定

リモート クラスタ上でルート プランを小規模に保持するために、この設計では、各クラスタにホストされている +.164 および ESN 範囲に対してサマリー パターンのみがアドバタイズされます。たとえば、サイト RTP、RCD、および SJC にホストしているクラスタについては、C：表 2-68 で示されているパターンは、GDPR アドバタイズ パターンとして設定する必要があります。この例で使用されている DID 範囲および ESN 範囲の詳細については、C：表 2-9 および C：表 2-10 を参照してください。

C：表 2-68　GDPR を介してアドバタイズされるパターン

パターン	パターン タイプ	PSTN フェールオーバー設定	コメント
+14085554XXX	[+E.164 番号（Advertised Failover Number）]	[パターンを PSTN フェールオーバー番号として使用する（Use Pattern as PSTN Failover Number）]	サイト SJC の DID 範囲
81404XXX	[エンタープライズ番号（Enterprise Number）]	[パターンに削除桁数と付加番号を適用し、PSTN フェールオーバーに使用する（Apply Strip Digits and Prepend Digits to Pattern and Use for PSTN Failover）] [PSTN フェールオーバー削除桁数（PSTN Failover Strip Digits）]：4 [PSTN フェールオーバー付加番号（PSTN Failover Prepend Digits）]：+1408555	SJC DID の ESN 範囲 ESN から PSTN フェールオーバー番号へ変換するための削除桁数とプレフィックス。
81405XXX	[エンタープライズ番号（Enterprise Number）]	[PSTN フェールオーバーを使用しない（Don't use PSTN Failover）]	SJC 非 DID の ESN 範囲 PSTN フェールオーバーは不可
+19195551XXX	[+E.164 番号（Advertised Failover Number）]	[パターンを PSTN フェールオーバー番号として使用する（Use Pattern as PSTN Failover Number）]	サイト RTP の DID 範囲
81911XXX	[エンタープライズ番号（Enterprise Number）]	[パターンに削除桁数と付加番号を適用し、PSTN フェールオーバーに使用する（Apply Strip Digits and Prepend Digits to Pattern and Use for PSTN Failover）] [PSTN フェールオーバー削除桁数（PSTN Failover Strip Digits）]：4 [PSTN フェールオーバー付加番号（PSTN Failover Prepend Digits）]：+1919555	RTP DID の ESN 範囲 ESN から PSTN フェールオーバー番号へ変換するための削除桁数とプレフィックス。
81912XXX	[エンタープライズ番号（Enterprise Number）]	[PSTN フェールオーバーを使用しない（Don't use PSTN Failover）]	SJC 非 DID の ESN 範囲 PSTN フェールオーバーは不可
+19725555XXX	[+E.164 番号（Advertised Failover Number）]	[パターンを PSTN フェールオーバー番号として使用する（Use Pattern as PSTN Failover Number）]	サイト RCD の DID 範囲

C：表 2-68　GDPR を介してアドバタイズされるパターン（続き）

パターン	パターン タイプ	PSTN フェールオーバー設定	コメント
81975XXX	[エンタープライズ番号（Enterprise Number）]	[パターンに削除桁数と付加番号を適用し、PSTN フェールオーバーに使用する（Apply Strip Digits and Prepend Digits to Pattern and Use for PSTN Failover）] [PSTN フェールオーバー削除桁数（PSTN Failover Strip Digits）]：4 [PSTN フェールオーバー付加番号（PSTN Failover Prepend Digits）]：+1972555	RCD DID の ESN 範囲 ESN から PSTN フェールオーバー番号へ変換するための削除桁数とプレフィックス。
81976XXX	[エンタープライズ番号（Enterprise Number）]	[PSTN フェールオーバーを使用しない（Don't use PSTN Failover）]	RCD 非 DID の ESN 範囲 PSTN フェールオーバーは不可
8099XXXX	[エンタープライズ番号（Enterprise Number）]	[PSTN フェールオーバーを使用しない（Don't use PSTN Failover）]	このクラスタの会議用の ESN 範囲（C：表 2-10 を参照）

各サイトに対して +E.164 範囲と ESN 範囲の両方をアドバタイズすることにより、この情報を学習するリモート クラスタ上のクラスタ間ダイヤリング手順として両方の形式を使用することができます。

学習番号およびパターンに対するパーティションの設定

リモート クラスタから学習した番号パターン（+E.164 および ESN）は、事前定義のパーティションのローカル ルート プランに追加されます。Unified CM Administration の [学習番号とパターンのパーティション（Partitions for Learned Numbers and Patterns）] メニューでは、学習した情報のそれぞれのタイプについて、異なるパーティションを定義することができます。この設計では、1 つのパーティション、onNetRemote のすべてのリモート数値パターンを学習するために、この区別および簡単な設定 GDPR を行う必要はありません（C：表 2-12 を参照してください）。

C：表 2-69 は、GDPR パーティションの設定をまとめています。

C：表 2-69　GDPR パーティションの設定

設定	値	コメント
[エンタープライズ代替番号のパーティション（Partition for Enterprise Alternate Numbers）]	onNetRemote [学習番号を緊急とする（Mark Learned Numbers as Urgent）] をオンにする	
[+E.164 代替番号のパーティション（Partition for +E.164 Alternate Numbers）]	onNetRemote [学習番号を緊急とする（Mark Learned Numbers as Urgent）] をオンにする	+E.164 ネット上クラスタ間コールに対する番号間タイムアウトを回避するために、緊急としてマークされる。

C：表 2-69　GDPR パーティションの設定（続き）

設定	値	コメント
[エンタープライズパターンのパーティション（Partition for Enterprise Patterns）]	onNetRemote [固定長パターンを緊急とする（Mark Fixed Length Patterns as Urgent）] をオンにする [可変長パターンを緊急とする（Mark Variable Length Patterns as Urgent）] をオンにする	
[+E.164 パターンのパーティション（Partition for +E.164 Patterns）]	onNetRemote [固定長パターンを緊急とする（Mark Fixed Length Patterns as Urgent）] をオンにする [可変長パターンを緊急とする（Mark Variable Length Patterns as Urgent）] をオンにする	+E.164 ネット上クラスタ間コールに対する番号間タイムアウトを回避するために、緊急としてマークされる。

クラスター間のトランクの設定

GDPR 交換では、すべての URI および数値の到達性情報が Unified CM クラスタ間で交換され、SIP ルート文字列にロケーション属性として関連付けられることを保証するだけです。クラスタ間のセッションは、SIP トランクを確立する必要があります。この設計では、すべての Unified CM クラスタ間において、最大 3 つの Unified CM クラスタを備えたフルメッシュ SIP トランクを仮定しています。最大 3 つの Unified CM クラスタにより、SIP トランクのフルメッシュのトポロジが管理可能であることが保証されます。4 つ以上の Unified CM クラスタが必要な場合は、Unified CM Session Management Edition（SME）を追加し、SME をハブとして、その他すべての Unified CM クラスタをスポークスまたはリーフ クラスタとするハブアンドスポーク トポロジになるように簡素化することが推奨されます。

標準の SIP クラスタ間トランクは GDPR ルーティングとして使用されます。C：表 2-59 に示されている設定と同様に、SIP トランク ST_UCM_EMEA は、GDPR 用にプロビジョニングされたクラスタ間トランクの例です。

SIP ルート パターンの設定

SIP ルート パターンは、GDPR を介して学習した SIP ルート文字列と SIP トランク トポロジを関連付けます。GDPR のルート文字列が、学習した URI 又は数値パターンが見つかった「場所」を教えてくれると考えると、この通知先に到達する方法を教えるには、これらのルート文字列上でルート パターン マッチングが必要になります。

GDPR の完全な到達性を実現するには、GDPR を介してアドバタイズされる各 SIP ルート文字列が、プロビジョニングされている SIP ルート パターンに従ってルートできることを確実にする必要があります。C：表 2-70 は、2 つの Unified CM 間で完全なクラスタ間 GDPR ルーティングを実現するためにプロビジョニングする必要があるトランク、ルート、グループ、ルートリスト、および SIP ルート パターンについて概要を示しています。

C：表 2-70　2 つの Unified CM クラスタを備えた GDPR ルーティング

コンポーネント	US クラスタ	EMEA クラスタ	コメント
SIP トランク	[ST_UCM_EMEA]	ST_UCM_US	他の Unified CM クラスタに向けた、各クラスタ上の SIP トランク（C：表 2-59 を参照）
上記の SIP トランクをメンバーとするルート グループ	[UCM_EMEA]	UCM_US	クラスタ間トランクに対する専用のルート グループ（C：表 2-61 を参照）
上記のルート グループをメンバーとするルート リスト	[RL_UCM_EMEA]	RL_UCM_US	クラスタ間トランクに対する専用の非 LRG ルート リスト（C：表 2-62 を参照）
SIP ルート文字列	us.route	emea.route	Unified CM クラスタによってアドバタイズされた SIP ルート文字列
上記のルート リストをポイントする SIP ルート パターン	パーティション onNetRemote の emea.route	パーティション onNetRemote の us.route	他の Unified CM クラスタによってアドバタイズされた SIP ルート文字列上での、プロビジョニングされた SIP ルート パターン マッチ

GDPR コール フローの例

このセクションでは、上記の設定例で EMEA クラスタに登録されている "international" サービス クラスのエンドポイントで +14085554001 がダイヤルされた場合に、コールがどのようにルートされるかについて説明しています。

1. ダイヤルされた番号（+14085554001）は、発信側デバイスの CSS XXXInternational を使用して、EMEA クラスタ上のダイヤル プランに対して照合されます。ここで XXX は、EMEA クラスタ上でプロビジョニングされているサイトのサイト コードを表します。実際のサイト特定のダイヤル正規化は、ここでは関係ありません。

   CSS XXXInternational には少なくとも次のパーティションが含まれていることが重要なポイントです（C：表 2-17 を参照。XXX はサイトのコードを、XX はダイヤル ドメイン識別子を表します）。

   - DN
   - Directory URI
   - URI
   - ESN
   - onNetRemote
   - XXXIntra
   - XXtoE164
   - XXPSTNNational
   - PSTNInternational
   - B2B_URI
   - USEmergency

これらのパーティション ダイヤル番号（+14085554001）は、次の 3 つのものと一致します。

- SIP ルート文字列が us.route である US クラスタから学習したパーティション onNetRemote の +14085554XXX（C：表 2-68 を参照）
- パーティション PSTNInternational の \+!（C：表 2-27 を参照）
- パーティション PSTNInternational の \+!#（C：表 2-27 を参照）

2。 パーティション onNetRemote の +14085554XXX は緊急パターンとしてルートに挿入され（C：表 2-69 を参照）、この段階ではこのパターンがベスト マッチであるため、番号の収集はすぐに停止し、このベスト マッチに基づいてルートされます。

3。 パーティション onNetRemote の +14085554XXX は GDPR の学習パターンで、SIP ルート文字列 us.route に関連付けられます。したがって、us.route は EMEA クラスタ上に設定された SIP ルート パターンに対して、発信側デバイスの CSS XXXInternational を使用して照合されます。

唯一のマッチは、パーティション onNetRemote における SIP ルート パターンです。

4。 EMEA クラスタのコールは SIP トランク ST_UCM_EMEA に拡張され、マッチした SIP ルート パターン us.route がポイントしているルート リスト RL_UCM_EMEA への参照、および RG_UCM_EMEA への参照は解除されます（C：表 2-70 を参照してください）。

5。 US クラスタでは、SIP トランク ST_UCM_EMEA の着信側 CSS ICTInbound（C：表 2-59 を参照）を使用して、着信コールが通知先 +14085554001 へルートされます。

6。 CSS ICTInbound には次のパーティションがあります。

- DN
- ESN
- URI
- Directory URI

これらのパーティションの唯一の（潜在的な）マッチは、パーティション DN における +E.164 電話番号 \+14085554001（緊急としてマークされている）です。この電話番号が存在する場合は、コールは、関連付けられているすべてのデバイスに拡張されます。

リモートでダイヤルされた ESN 通知先のルーティングは同じフローに従いますが、ここでは CSS ICTInbound を使用した US クラスタ上の最後のルックアップで、パーティション ESN の ESN を見つけることだけが異なります。

IM とプレゼンスクラスター間

フルメッシュのプレゼンス トポロジを作成するには、それぞれの Cisco IM and Presence クラスタと、同じドメイン内の他のそれぞれの Cisco IM and Presence クラスタとの間に、個別のピア関係が設定されている必要があります。このクラスタ間ピアに設定されているアドレスは、リモート Unified CM クラスタ IM and Presence のパブリッシャ ノードの IP アドレスです。

各 Cisco IM and Presence クラスタ間のインターフェイスには、AXL/SOAP インターフェイスとシグナリング プロトコル インターフェイス（SIP または XMPP）の 2 つが使用されます。IM and Presence クラスタのパブリッシャのみのサーバ間の AXL/SOAP インターフェイスはホーム クラスタ アソシエーションの同期を処理しますが、これは完全なユーザ同期ではありません。シグナリング プロトコル インターフェイス（SIP または XMPP）はフルメッシュで、展開内のすべてのサーバを対象としています。これは、サブスクリプション トラフィックと通知トラフィックを処理します。また、同じドメイン内のリモートの Cisco IM and Presence クラスタにユーザが存在することが検出された場合、SIP インターフェイスが URI のホスト部分を書き換えた後でユーザを転送します。

Cisco IM and Presence がクラスタ間環境に展開されている場合、プレゼンス ユーザを決定する必要があります。プレゼンス ユーザ プロファイルは、マルチクラスタ プレゼンスの展開の規模とパフォーマンス、およびサポート可能なユーザ数の決定に役立ちます。プレゼンス ユーザ プロファイルによって、一般的なユーザの連絡先（バディ）の数、およびそれらの連絡先の多くがローカル クラスタのユーザか、リモート クラスタのユーザかが確定します。

Survivable Remote Site Telephony（SRST）展開

リモート サイトへの WAN に障害が発生した場合に呼処理が存続するようにするために、各リモート サイトで SRST を設定します。SRST では WAN に障害が発生しても、リモート サイトまたは PSTN 内で電話のコールを作成することができます。

展開

SRST に対応させる各リモート サイトに 1 つの Cisco Integrated Services Router（ISR）を展開します。

プロビジョニング

SRST を設定するには、Unified CM と SRST ルータの両方で設定を行う必要があります。

Unified CM での設定

- 各リモート サイトに対して SRST 参照先を設定し、リモート電話のデバイス プール内の SRST 参照先に関連付けます。
- 電話機の +E.164 番号および AAR CSS を使用するには、リモート電話の DN で [未登録時コール転送（CFUR）] を設定します。WAN に障害が発生して電話機が登録解除された場合、統一された CM はこの情報を使用して、未登録の電話を宛先とする着信コールを PSTN 経由でサイトのゲートウェイにルーティングします。
- サイトのゲートウェイがまだ Unified CM に接続中に電話機が登録解除された際（たとえば、接続されていない場合など）に発生する可能性があるルーティング ループの影響 を確実に制限するには、**DN への未登録ホップの最大転送数**サービス パラメータをゼロ以外の値に設定します。

SRST ルータでの設定

- 各リモート ブランチ ルータで SRST を設定します。ここでは、SIP 電話の使用が推奨されるため、**voice register global** および **voice register pool** コマンドを使用します。**voice service voip/sip** コマンドを使用してソース インターフェイスの IP アドレスをバインドし、レジスタの容量を有効にします。リモート ブランチの電話に DHCP を設定します。DHCP サーバは、SRST ルータ、または他のネットワーク サービス リソース上に設定することができます。
- WAN が失敗した場合、SIP phone は自身の +E.164 内線番号で登録します。4 桁の内線番号を使用して他のローカル ユーザへ通話できるようにするには、音声レジスタ プールの設定で着信プロファイルとして参照される音声変換プロファイルを設定します。この音声変換プロファイルは、着信番号を 4 桁から +E.164 の完全な番号へ変換します。
- POTS ダイヤルピアを設定して、WAN が停止している場合の PSTN へのローカル アクセスを可能にします。サービス プロバイダの PSTN ダイヤル要件に準拠するために、変換音声プロファイルを設定します。ダイヤルピア設定の詳細については、Cisco Unified Border Element を展開するの方法について説明しているセクションを参照してください。

C：例 2-6 の SRST 設定は、前の段落で説明したいくつかの概念を説明するための、部分的なものです。SRST の完全な設定について記載しているわけではありません。たとえば、メインサイトの Cisco Unity Connection サーバへ到達するための設定については、ボイス メッセージングの章で説明しています。

C：例 2-6　　SRST 設定（一部）

```
voice service voip
 allow-connections sip to sip
sip
  bind control source-interface GigabitEthernet0/0.241
  bind media source-interface GigabitEthernet0/0.241
  registrar server
!
voice register global
 mode srst
 max-dn 100
 max-pool 100
!
voice register pool 1
 translation-profile incoming 4-digit-rtp
 id network 10.0.94.0 mask 255.255.255.0
 !
voice translation-rule 1
 ルール 1 /\(^1...\)$/ /+1919555\1/
!
voice translation-profile 4-digit-rtp
 translate called 1
!
```

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

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide.html

拡張モビリティー

Cisco Extension Mobility では、Cisco Unified IP Phone の設定（ライン アピアランス、サービス、短縮ダイヤルなど）に他の Cisco Unified IP Phone から一時的にアクセスすることができます。

1 つまたは 2 つの Unified CM コール処理ノードは、Extension Mobility の要求をアクティブに処理することができます。Extension Mobility に対して 2 つ目の Unified CM コール処理ノードを追加すると、レジリエンスおよびキャパシティが増加するという利点があります。このシナリオでは、2 つの Unified CM ノードへ要求を送信するために 1 つのロード バランサが必要です。Cisco IOS Server Load Balancing などを使用することができます。

Extension Mobility Cross Cluster（EMCC）を使用すると、社内のクラスタ間でエクステンション モビリティのログインを実行することができます。この機能については、このガイドでは説明していません。EMCC の詳細については、『*Cisco Collaboration System SRND*』の最新版と EMCC 製品のドキュメントを参照してください。

拡張モビリティーの展開

エクステンション モビリティを展開するには、次のタスクを実行します。

- 1 つまたは 2 つの Unified CM 呼処理サーバで Cisco Extension Mobility サービスがアクティブになっていることを確認します。
- エクステンション モビリティ向けの IP Phone サービスを追加します。非セキュアな URL の他に、HTTPS を使用したセキュアな IP Phone サービスの URL を設定できます。非セキュア URL は次のとおりです。

  http://<*IPAddress*>:8080/emapp/ EMAppServlet?device=#DEVICENAME#

  ユーザは、[エンタープライズ登録（Enterprise Subscription）] を選択してクラスタ内のすべての電話でサービスを使用できるようにするか、またはこれらの電話をこのサービスに登録し、選択した電話で使用できるようにするか、いずれかを選択することができます。
- エクステンション モビリティを使用する各ユーザについて、少なくとも 1 つのデバイス プロファイルを作成します。デバイス プロファイルは特定のユーザに関連付けられているため、デバイス プロファイルは通常、ユーザ デバイス プロファイルとして参照されます。あるユーザに対してデバイス プロファイルが作成されていない場合、ユーザはエクステンション モビリティにログインできません。
- デバイス プロファイルを、エクステンション モビリティのユーザに関連付けます。CTI が必要な場合は、CTI コントロールのデバイス プロファイルとなるプロファイルを関連付けます。
- ユーザのログインで使用できるそれぞれの電話について、エクステンション モビリティを有効にします。
- DN の設定で、対象ユーザの関連付けを回線へ設定します。これにより、電話回線が使用中の場合でも、DN で対象ユーザのプレゼンス情報を送信することができます。次に例を示します。

  ユーザ B は Jabber を使用し、ユーザ A を監視しています。ユーザ A は Extension Mobility を使って電話機にログインし、DN が自身に関連付けられたユーザ デバイス プロファイルを持っています。ユーザ A がオフフック状態になると、このプレゼンス情報はユーザ B の Jabber クライアントでレポートされます。

Extension Mobility の詳細については、次の場所にある『*Feature Configuration Guide for Cisco Unified Communications Manager*』の最新版を参照してください。

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

ビジー回線フィールド（BLF）のプレゼンス

BLF プレゼンス機能により、ユーザ（ウォッチャ）は、ある電話番号または SIP URI における他のユーザのリアルタイムのステータスを、ウォッチャのデバイスから監視することができます。ウォッチャは、次のオプションを使用してユーザのステータスを監視することができます。

- BLF/ スピードダイヤル ボタン
- ディレクトリ ウィンドウの不在着信、発信履歴、または着信履歴のリスト
- 共有ディレクトリ（社内ディレクトリなど）

BLF プレゼンスは Cisco Unified IM and Presence をベースにしているわけではありません。

BLF プレゼンスの展開

- **コール リストの BLF** エンタープライズ パラメータを有効にします（C：表 2-2 を参照してください）。
- BLF プレゼンスに対してクラスタ全体のサービス パラメータを設定します。
- BLF プレゼンス グループの認証を使用するには、BLF プレゼンス グループおよび権限を設定します。
- Cisco Unified Communications Manager Administration で、電話番号、SIP トランク、SIP を実行している電話、SCCP を実行している電話、エンド ユーザ、およびアプリケーション ユーザ（SIP トランクを介して BLF プレゼンス要求を送信しているアプリケーション ユーザ）に対して BLF プレゼンス グループを適用します。
- SIP トランクから BLF プレゼンス要求を可能にするには、[SIP トランクセキュリティプロファイルの設定（SIP Trunk Security Profile Configuration）] ウィンドウの [プレゼンスの SUBSCRIBE の許可（Accept Presence Subscription）] オプションを選択します（C：表 2-57 を参照してください）。
- SUBSCRIBE コーリング サーチ スペースを設定し、必要に応じて電話、トランク、またはエンド ユーザにコーリング サーチ スペースを適用します。
- 電話の BLF/ スピードダイヤル ボタンでは、BLF/ スピードダイヤル ボタンのボタン テンプレートをカスタマイズしたり、電話へ直接追加したりできます。

コンピュータ テレフォニー インテグレーション（CTI）の展開

- CTI Manager サービスを必要とする Unified CM 呼処理ノード上で、CTI Manager サービスをアクティブにします。
- 冗長性を実現するために、CTI のアプリケーション管理全体で、CTI Manager サービスを実行しているプライマリおよびバックアップの Unified CM ノードを選択します。
- TAPI を使用するアプリケーションについて、TAPI クライアント ソフトウェアをダウンロードします。
- 可能な場合は、CTI に対応している特定のエンドポイントについて、CCM 登録および CTI Manager 監視および制御について同じ Unified CM 呼処理ノードを設定します。
- CTI Manager を実行しているすべての Unified CM ノードで CTI の負荷が分散されており、CTI の容量制限を超えていないことを確認します。たとえば、Jabber クライアントで 2 つの Unified CM 呼処理ペアが必要な場合、登録を 2 つのペアで分散させます。また、Jabber クライアントがデスク電話モードでの機能で設定されている場合は、2 つのペアで CTI Manager の接続性を分散させます。これは、複数のサービス プロファイルに複数の CTI プロファイルを関連付けることによって実現されます。CTI Manager サービスを実行している各 Unified CM で監視および制御されているデスク電話モードの Jabber クライアントの数が、CTI の容量制限を超えていないことを確認します。

会議

改訂日：2019 年 2 月 19 日

この章では、企業展開におけるビデオおよび音声会議のコンポーネントと導入方法について説明します。また、会議のアーキテクチャーについて説明し、会議の導入プロセスに含まれる主なタスクについて概要を示します。

会議の導入プロセスの主なタスクはそれぞれ、そのタスクに必要な手順をリストする「*概要*」セクションから始まり、そのタスクの重要な「*導入上の考慮事項*」を扱うセクションが続きます。その後、「*概要*」セクションでリストされた導入タスク（展開タスク）の詳細を示すセクションが続きます。

この章の新規情報とは

C：表 3-1 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。

C：表 3-1　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 Meeting 管理	この章の各項で説明	2019 年 1 月 23 日
会議参加者の最大数	会議ソリューションのスケーリング（C：3-15 ページ）	2017 年 8 月 30 日

コア コンポーネント

コア アーキテクチャには、以下の主要な会議要素が含まれます。

- 音声 / ビデオ会議と会議リソース管理用の Cisco Meeting Server
- 会議のプロビジョニング、モニタリング、およびスケジューリング用の Cisco TelePresence Management Suite（TMS）
- Microsoft Exchange のルームおよびリソース カレンダーとインターフェイスするための Cisco TelePresence Management Suite Extension for Microsoft Exchange（TMSXE）
- Cisco Meeting Management の会議のモニタリングと管理

加えて、Cisco TMS アーキテクチャには、次のシスコ以外のコンポーネントが含まれています。

- Microsoft SQL データベース
- Microsoft Active Directory
- Microsoft Exchange or Microsoft Office 365
- ネットワーク ロードバランサ

主なメリット

- すべてのデバイス タイプでの会議ユーザ エクスペリエンスが簡略化および最適化されました
- 無期限、スケジュール、インスタントのいずれかまたはすべての会議の 1 つ以上のリソースの導入をサポートする柔軟性と拡張性のあるアーキテクチャ
- 会議リソースとプロセスの高可用性
- ビデオ ネットワークでの復元性
- ホストで会議の参加者と会議室をスケジュールするための単一のツール
- マルチパーティ ライセンスは、ブリッジ上のすべての会議リソースへのフル アクセスを可能にします
- 1 つのインターフェイスで会議をモニタおよび管理する White Glove サービス

会議タイプ

会議ソリューションは、C：表 3-2 に示す会議タイプと会議機能をサポートします。

C：表 3-2　　会議の種類

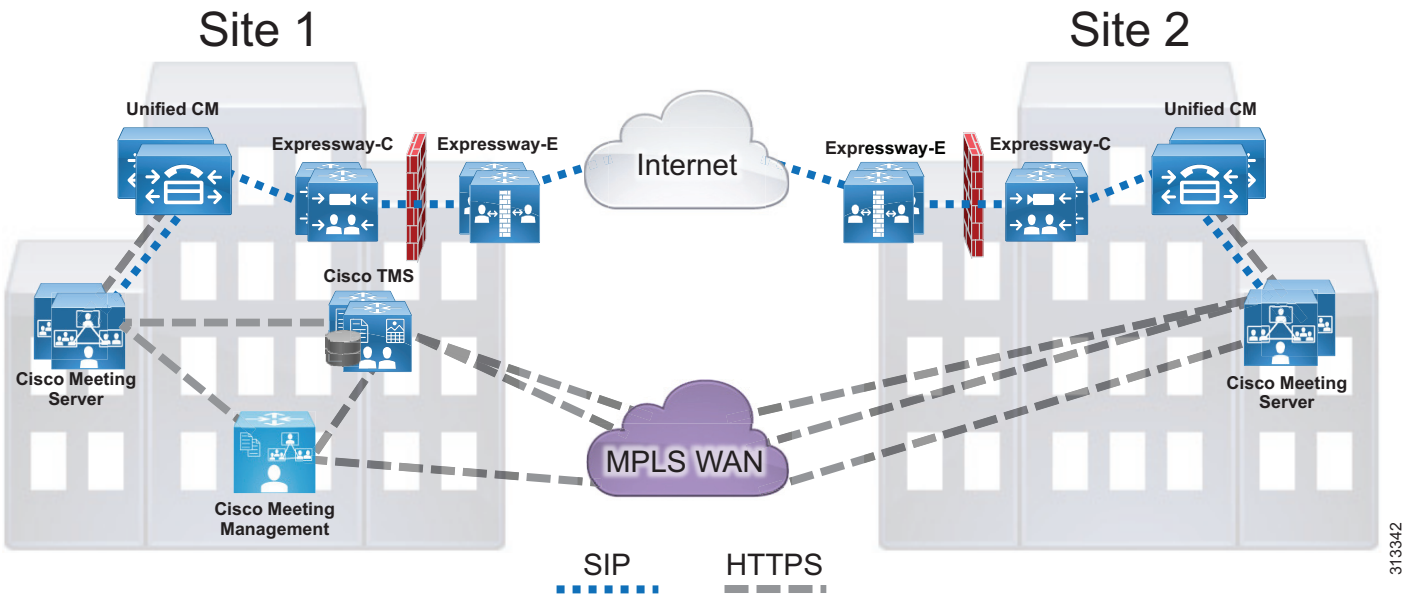
会議タイプ	説明
[インスタント会議（Instant conferences）]	Unified CM でホストされたポイントツーポイント コールから、会議ブリッジにホストされた三者コールへのエスカレートは手動で行います（アドホック会議とも呼ばれます）。インスタント会議は、会議前にスケジュールまたは用意されません。
[無期限の会議（Permanent conferences）]	事前のスケジュールなしで会議を行えるようにする、事前定義されたアドレス。会議ホストはその他のユーザとアドレスを共有します。それらのユーザは、いつでもそのアドレスにコールインできます（ミートミー会議、スタティック会議、または、ランデブー会議とも呼ばれます）。この章で説明する無期限会議では、Cisco Meeting Server スペースが使用されます。スペースをユーザ ベースにすることができ、会議名、レイアウト、PIN などの項目に関して Cisco Meeting Server からスペースがプロビジョニングされます。スペースを作成する方法として、ユーザのインポート、API、または手動作成が可能です。
スケジュール済み会議	開始および終了時間のある（オプションで一連の参加者を事前定義する）、Cisco TMS を介して、または Cisco TMS を使用した統合、あるいはその両方を使用して予約する会議。

アーキテクチャー

会議アーキテクチャは、ブリッジ リソース用およびリソース管理用の Cisco Meeting Server、リソースのプロビジョニング、スケジューリング用の Cisco TelePresence Management Suite（TMS）、会議モニタリング用の Cisco Meeting Management、およびコール処理用の Cisco Unified Communications Manager（Unified CM）で構成されます。このアーキテクチャでは SIP コール制御が排他的に使用されます。すべての会議タイプ用の会議ブリッジとして Cisco Meeting Server を使用し、SIP トランクを使用して Cisco Meeting Server を Unified CM に接続します（C：図 3-1）。

Unified CM は、HTTPS 経由で XML-RPC を使用して Cisco Meeting Server と通信し、インスタント会議用の会議ブリッジを制御します。Cisco TMS は REST API 接続を使用して Cisco Meeting Server にリンクし、会議リソースのプロビジョニングとスケジューリングを行います。Cisco Meeting Management および Cisco Meeting Server は、REST API、イベント サブスクリプション、およびコール詳細レコード (CDR) インターフェイスを介して接続されて、会議管理機能を実行します。また、Cisco Meeting Management は、TMS Booking API を使用して Cisco TMS に接続し、スケジュールされた会議を管理します。（C：図 3-1）。

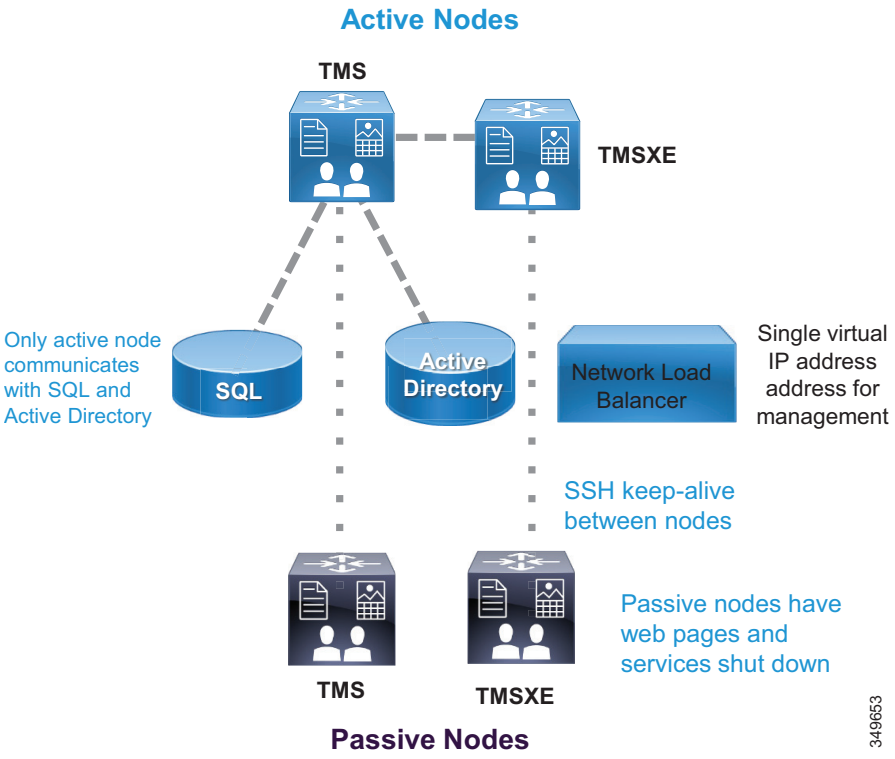
C：図 3-1　　アーキテクチャの概要



ライセンスに関しては、各 Cisco Meeting Server にマルチパーティ ライセンスをインストールして、他の機能ライセンスと一緒に使用します。デフォルトで、システム内のすべてのユーザが Shared Multiparty Plus（SMP+）を使用します。また、Personal Multiparty Plus（PMP）が必要な場合は、Cisco Meeting Server API 経由で PMP+ をユーザに割り当てる必要があります。

スケジューリング アーキテクチャは、Cisco TMS および TMSXE 両方のアクティブ ノードとパッシブ ノードで構成されています。これらは、ネットワーク ロード バランサの後ろに導入されています。アクティブ ノードは着信要求を処理します。一方、パッシブ ノードはスタンバイ モードで動作し、その Web ページとサービスがロック ダウン状態になってすべての着信トラフィックを拒否します。大規模な Cisco TMS 展開 (サイジングの章を参照）では、C：図 3-2 に示すように、Cisco TMS と TMSXE を別々の仮想マシンにインストールする必要があります。TMS サーバは顧客データ センターに設置され、そこでは組織の SQL 展開もホストされます。すべてのサーバ ノードが、外部の Microsoft SQL データベースから機能します。加えて、会議を適切にスケジュールするにはエンドポイント、Cisco Meeting Server、および Unified CM が使用されます。（C：図 3-2）。

C：図 3-2　スケジューリング アーキテクチャの概要



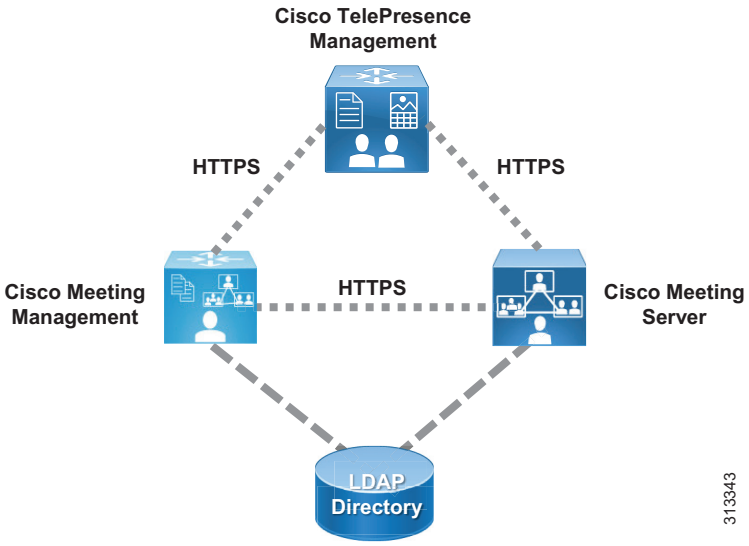
Cisco Meeting Management は Cisco Meeting Server の外部にある別個のサーバ上で、Cisco Meeting Server 導入環境専用として稼働します。Cisco Meeting Management ユーザは、ユーザ認証とユーザ ロールの判別に使用される LDAP ディレクトリ内にあります。Cisco Meeting Management は、イベント サブスクリプション インターフェイスと REST API を使用して、Cisco Meeting Server で会議管理機能を実行します。Cisco Meeting Management は Cisco Meeting Server 上の CDR 受信者として自己設定して、コール関連のイベントを受信します。これにより、会議がいつ開始したか、または終了したのかという情報や、その他のコール アクティビティが認識されます。Cisco Meeting Management は、Cisco TMS 用 Booking API を使用して、Cisco TMS から今後予定されている会議の情報を取得します。（C：図 3-3）。

Cisco Meeting Server と TMS の互換性のあるバージョンについては、以下で入手できる最新バージョンの *Cisco Meeting Management インストレーションおよび設定ガイド*を参照してください。

https://www.cisco.com/c/en/us/support/conferencing/meeting-management/products-installation-guides-list.html

注　Cisco Meeting Management には、適切なライセンスを持つ Cisco Meeting Server インスタンス以外の追加ライセンスは必要ありません。

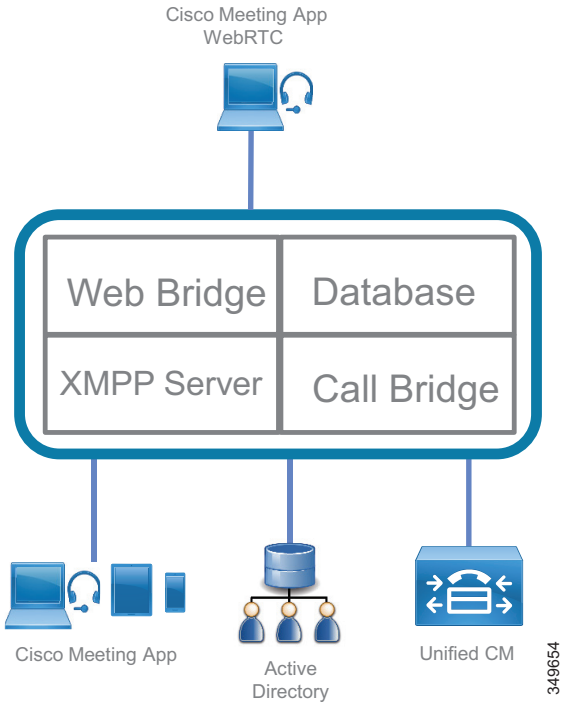
C：図 3-3　　Cisco Meeting Management のアーキテクチャ



Cisco Meeting Server の役割

Cisco Meeting Server は、ビデオ会議機能（C：図 3-4）を提供してすべてのタイプの会議を処理できる複数のコンポーネントで構成されます。Call Bridge コンポーネントは、コール制御用の Unified CM と統合し、会議機能を実行するためのリソースを提供します。すべての Cisco Meeting Server 会議がスペース上でホストされます。スペースは、音声、ビデオ、コンテンツ共有機能を備えた、スペース URI またはディレクトリ番号を使ってアクセス可能な仮想会議室です。Cisco Meeting Server は、ユーザをシステムにインポートするために Microsoft Active Directory などのディレクトリ サーバと統合する必要があります。インポート プロセス中に、フィールド マッピング表現設定を使用してスペースが作成されます。ユーザとスペースに関するすべての情報がデータベースに保存されます。参加者は、シスコまたはサードパーティ製の標準的なビデオ エンドポイント、Cisco Jabber クライアント、または Cisco ミーティング アプリを使用して会議に参加できます。XMPP サーバは、Cisco ミーティング アプリ経由でログインするユーザを認証します。ログイン後に、Web Bridge が WebRTC クライアント ユーザを Call Bridge に接続します。

C：図 3-4 Cisco Meeting Server 内部のコンポーネント



注 すべての Cisco Meeting Server コンポーネントが C：図 3-4 に表示されているわけではなく、エンタープライズ コラボレーション プリファード アーキテクチャに関連したコンポーネントのみが表示されています。

Cisco ミーティング アプリは Cisco Meeting Server のクライアントであり、ネイティブ デスクトップまたはモバイル アプリケーションとして、あるいは WebRTC ブラウザ アプリケーションとして使用可能です。Cisco ミーティング アプリを使用すれば、ユーザは音声、ビデオ、およびコンテンツ共有を使用する会議にログインし、参加することができます。WebRTC クライアントを使用すれば、Cisco Meeting Server アカウントを持っていないユーザがゲストとして会議に参加することができます。加えて、Cisco ミーティング アプリを使用するとユーザは会議を開催したり、参加者の表示 / ミュート / 削除などの操作を実行したり、録音を開始 / 停止したり、独自のスペースを作成して編集することができます。

注 Cisco ミーティング アプリをエンタープライズ ネットワークの内側と外側のどちらにも展開して会議に参加させることができますが、このエンタープライズ コラボレーション プリファード アーキテクチャではエンタープライズ ネットワーク内部の展開のみを扱います。エンタープライズ ネットワークの外部の展開については、https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html にある Cisco Meeting Server 構成ガイドの最新版を参照してください。

会議用の Cisco Meeting Server を使用すると、次のようなメリットがあります。

- 小規模な展開と大規模な展開のどちらにも簡単にスケーリングし、必要に応じてキャパシティを段階的に追加できる
- すべてのデバイス タイプで簡略化された、直感的かつ最適な会議エクスペリエンス
- マルチパーティ ライセンスを使用すると、利用可能な基盤ハードウェアの上限に達するまで会議の参加人数を増やすことができる
- 1 つの展開モデルですべての会議タイプに対応

Cisco TMS の役割

Cisco TMS は、会議スケジューリングと会議室システム予約を提供します。Unified CM はエンドポイントの設定管理を維持し、TMS はカレンダー情報をこれらのエンドポイントに配信できます。管理者は、組織のデフォルト会議のパラメータを設定できます。パラメータの設定後に、このテンプレートに基づいて個々の会議が作成されます。

TMS 機能の一部（電話帳、ソフトウェア管理、レポート機能など）はプリファード アーキテクチャで使用されません。

Microsoft Exchange に対する Cisco TMS Extension の役割

エンドユーザが複数の会議室リソースを使用する会議を Microsoft Outlook でスケジュールすると、Exchange の Exchange Web Service（EWS）機能により、そのイベントが TMS にスケジュール済み会議として同期されます。この同期は双方向であるため、管理者またはサポート担当員が、会議主催者の Outlook イベントにアクセスせずに、会議を更新できます。組織内で会議に使用する予定のすべてのエンドポイント リソースが、1 つの Exchange 会議要求にリストされている必要があります。

Cisco Meeting Management の役割

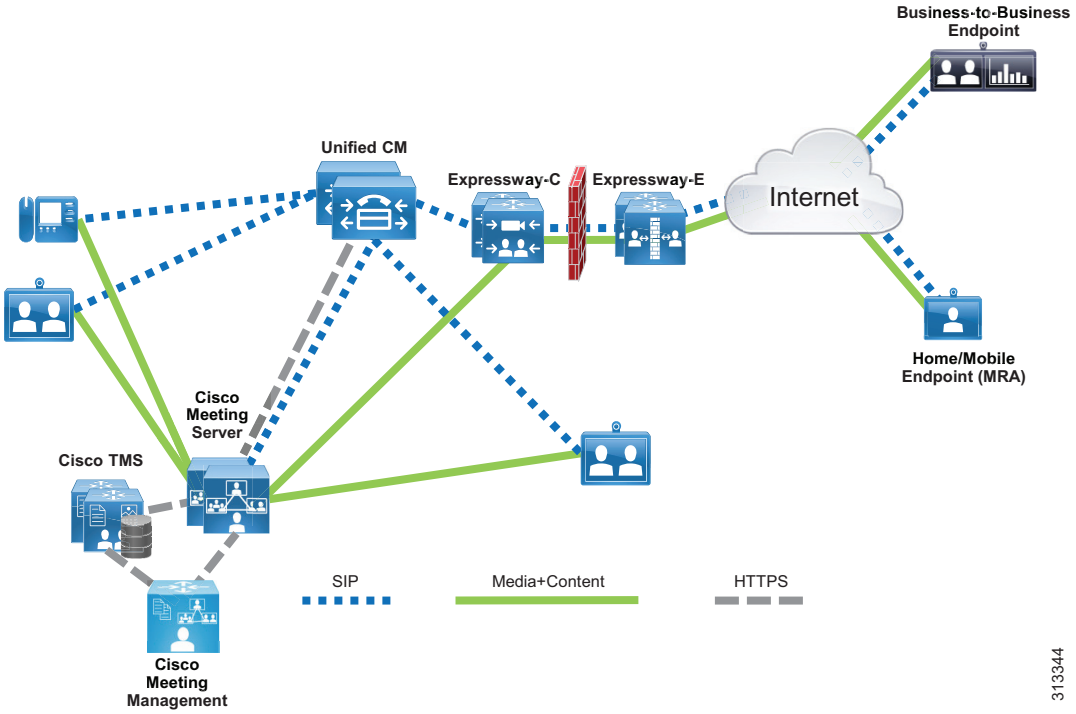
Cisco Meeting Management は Cisco TMS と併せて使用することで、Cisco Meeting Sever に完全な管理機能を提供します。Meeting Management では、顧客に White Glove サービスを提供することができます。また、オペレータに、アクティブな会議、過去の会議 (最長 7 日前)、または今後の会議 (最長 24 時間前) の一覧を表示します。さらに、オペレータは、参加者、会議の期間、会議の開始時刻など、個々の会議に関する詳細情報を表示することができます。会議中、オペレータは、録音またはストリーミングの開始または停止、レイアウトの変更、参加者の追加またはドロップ、会議の終了などの会議管理機能を実行し、アクティブな発言者を確認することができます。個々の参加者レベルでは、オペレータは音声またはビデオのミュート・ミュート解除、レイアウトの変更、重要度の設定・設定解除、あるいは参加者の通話統計を確認することができます。

Cisco Meeting Management のユーザは、管理者、またはビデオ オペレータのいずれかのユーザグループに属します。各ユーザグループは、ユーザが割り当てられているディレクトリ内で定義される LDAP グループにマッピングされます。ユーザがポータルにログインすると、会議管理はディレクトリを使用してユーザを認証し、グループのメンバーシップを判断します。管理者は、Cisco Meeting Management ポータルのすべての機能へのフル アクセス権を持っています。ビデオ オペレータは、Cisco Meeting Management のポータルの会議のモニタリングと管理、システムのステータスチェック機能にのみにアクセスすることができます。

展開の概要

標準的な展開では、複数の Unified CM ノードがコール制御に使用されます。Cisco Meeting Server は SIP トランクを使って Unified CM に接続し、会議リソースを管理したり、コールをブリッジしたりします。（C：図 3-5）Cisco TMS および Cisco Meeting Management は、会議管理ファシリティとスケジューリングを提供します。同じインフラストラクチャが、非スケジュール済み会議とスケジュール済み会議の両方に使用されます。Cisco Expressway は、ローカル エンタープライズへの Business-to-Business（B2B）コールとモバイルおよびリモート アクセス（MRA）コールを可能にするためのファイアウォール トラバーサル機能を提供します。これらの要素は一緒に、ローカル エンタープライズに音声およびビデオ会議を提供します。

C：図 3-5　　標準的な展開



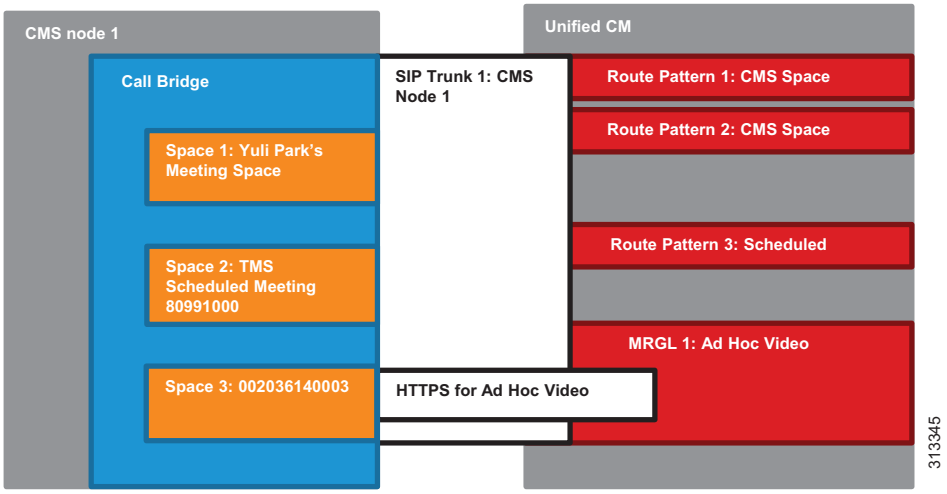
要件と推奨事項

- TelePresence コールを伝達する Unified CM に接続されたすべての SIP トランクで、早期オファー メッセージングを推奨します。
- Cisco Meeting Server ではすべての会議タイプ（インスタント、無期限、およびスケジュール済み）用に 1 つの SIP トランクを使用します。
- Cisco Meeting Server で会議をホストするためのマルチパーティ ランセンスを設定します。

会議のコール フロー

Unified CM で、接続されたエンドポイント間の音声およびビデオ コールのデバイス登録およびルーティングを行います。無期限、インスタント、およびスケジュール済み会議のコールはすべて、単一の SIP トランクを介して Cisco Meeting Server 上の Call Bridge にルーティングされます。Call Bridge ごとに個別の SIP トランクが必要です。インスタント会議用に Cisco Meeting Server ノード宛てに XML-RPC 要求を伝送する Unified CM ノードで、HTTPS 接続が設定されます（C : 図 3-6 を参照）。ユーザがデバイス上の会議ソフトキーを押して二者通話を三者通話にエスカレートすると、Unified CM が Cisco Meeting Server に API 要求を送信し、この HTTPS 接続を介して会議をホストするための一時スペースが作成されます。さまざまなコンポーネントによって作成されるスペース上で、インスタント、無期限、およびスケジュール済み会議がホストされます。スペースの詳細については、5. Cisco Meeting Server スペースを展開するのセクションを参照してください。

C : 図 3-6　　Unified CM と Cisco Meeting Server SIP トランク



Unified CM によって管理されるインスタント コール フローは、スケジュール会議など、その他の方法で作成された会議への参加者を追加するために使用できません。その他のコール フローを使用して、インスタント会議への参加者を追加することはできません。インスタント コール エスカレーション方式は、その方法で作成されたインスタント会議でのみサポートされます。その他の方法で生成された会議をインスタント メカニズムで拡張することはできません。これにより、チェーン会議の可能性を回避できます。

インスタント会議

インスタント会議では、Unified CM と Cisco Meeting Server 上の Call Bridge の間で SIP トランクに関連付けられた HTTPS XML-RPC 接続が使用されます。ユーザが会議ソフトキーを押してインスタント会議を開始すると、Unified CM が HTTPS 接続を介して API 要求を発行し、Cisco Meeting Server 上で一時スペースが作成されます。その後、Unified CM は SIP トランクを介してすべての参加者をそのスペースにルーティングします。会議が終わると、Unified CM は別の API 要求を発行して、Cisco Meeting Server からそのスペースを削除します。

Cisco Meeting Server スペースを使用した常設会議

無期限会議は、Cisco Meeting Server スペースを使用して展開されます。スペースは、無期限タイプの会議を提供し、LDAP からのユーザ インポート プロセスの一部として作成されます。ユーザは、いつでもスペース URI をダイヤルして会議を開始できます。管理者はフィールド マッピングを通してスペースの属性（名前、ユーザ名、URI など）を指定できます。これにより、これらのマッピングを使ってスペースを作成できるようになります。ユーザはその後、Cisco ミーティング アプリを使ってログインし、自分のスペースにメンバーを追加できます。Unified CM と、この会議タイプ用の Cisco Meeting Server 上の Call Bridge の間で SIP トランクを接続します。同じ SIP トランクが、他の会議タイプで会議参加者をスペースにルーティングするために使用されます。

スケジュール済み会議

このソリューションは Cisco Meeting Server 上の会議のスケジューリングをサポートし、スケジューリングは Cisco TMS を使用して実行されます。スケジュール済み会議では、Unified CM と、Cisco Meeting Server 上の Call Bridge の間に SIP トランクが必要です。ここでも、他の会議タイプの場合と同じ SIP トランクが使用され、Unified CM はスケジュール済み会議の参加者を SIP トランクの宛先にルーティングします。HTTPS 接続を介して Cisco Meeting Server 上で REST API 要求を発行できるようにするには、Cisco TMS に Cisco Meeting Server を追加します。スケジュール済み会議用の数値 ID 範囲を設定した後、Cisco TMS は API リンクを介して数値 ID ごとに Cisco Meeting Server 上に非アクティブなスペースを作成します。その後、Cisco TMS は、主催者が会議をスケジュールしたときにダイヤルイン番号をこの範囲からランダムに選択します。スケジュール済み会議を開始する時間になると、Cisco TMS は API を使用してスペースをアクティブにし、参加者がコールインを開始できるようになります。

サイドパーティー　エンドポイント

他の機器プロバイダ製のエンドポイントは、標準的な SIP を使用して会議に参加できます。インスタント会議を開始できるのは、会議ボタンをサポートする Unified CM に登録されたエンドポイントだけです。SIP への H.323 コールをインターワーキングさせるために Cisco Expressway または Cisco VCS を使用できます。これにより、H.323 エンドポイントは会議に参加できるようになります。

ハイアベイラビリティー

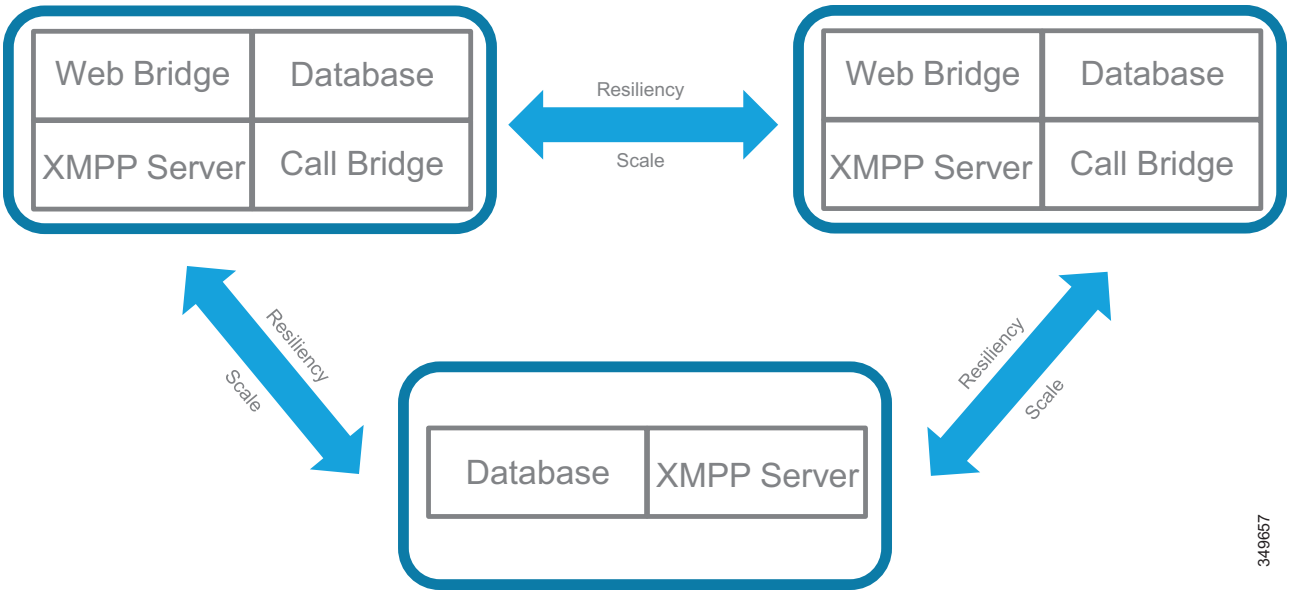
会議ソリューションについていくつかのレベルで、ハイ アベイラビリティを考慮する必要があります。また、ハイ アベイラビリティは、考慮するサービスに応じて異なる方法で実現されます。

スケジュール済み会議と非スケジュール済み会議の両方で、高可用性のために Cisco Unified CM、Cisco Meeting Server、および Cisco TMS が必要です。

Ciso Meeting Server の高適用性

追加のコンポーネント インスタンスを 1 つ以上のサーバに展開すると、Cisco Meeting Server の復元力が強化され、複数コンポーネント インスタンスで負荷を共有することができ、それらの 1 つで障害が発生してもバックアップ インスタンスが負荷を処理します。加えて、XMPP サーバ、Call Bridge、およびデータベースをまとめてクラスタ化して単一のインスタンスとして動作させることができます。C：図 3-7 を参照してください。

C：図 3-7　　高可用性を備えた Cisco Meeting Server クラスタの最小構成



標準的な 1 つの Cisco Meeting Server クラスタは、Call Bridge サービスが有効になっている 2 つ以上（8 つ以下）のノードで構成されます。コールブリッジ間の最大ラウンドトリップ時間（RTT）は 300 ms です。Call Bridge クラスタ ピアは、分配リンクを介してフル メッシュ内で相互に接続されます。このリンクは、コールブリッジ間でコール信号と制御ステータスメッセージを渡すために使用される HTTPS 接続です。コールは、クラスタ内の任意のコールブリッジに送信することができます。1 つのコールブリッジがダウンした場合、統一された CM は残りの Call Bridge にコールをルーティングして会議に参加できるようにします。ライブ会議中に 1 つの Call Bridge で障害が発生した場合、それらのコールがドロップされ、参加者は同じ番号をダイヤルして新しい Call Bridge 上の会議に参加する必要があります。Unified CM ルート グループとルート リスト構造を使用すると、SIP トランクを介してコールを Cisco Meeting Server に分配できます。

1 つのクラスタとして構成された複数の Call Bridge を、1 つ以上の Call Bridge グループに分けることができます。グループ内の Call Bridge では、Cisco Meeting Server がそれらのブリッジ間でコールをインテリジェントに負荷分散して、可能な場合には同じ会議のすべてのコールを同じ Call Bridge に送信することができます。コールが Call Bridge に送信されると、Cisco Meeting Server は Call Bridge 内の現在の負荷に基づいてコールの拒否または受け入れを決定します。現在の負荷がプリセットしきい値を下回っている場合は、コールが受け入れられます。そうでない場合はコールが拒否され、Unified CM はダイヤル プラン設定を使用してそのコールを Call Bridge グループ内の別 Call Bridge に再ルーティングします。コールを受け入れる Call Bridge が Unified CM で見つからない場合は、コール全体が拒否されます。Cisco Meeting Server がコールを受け入れた後、コールをその Cisco Meeting Server の Call Bridge 上でホストすることも、会議の内部順序付きリストに従って優先順位が最も高い別の Call Bridge に移動することもできます。コールを移動した場合は、Call Bridge が有効になっているターゲット Cisco Meeting Server が Replaces を伴う INVITE を Unified CM に送ってコールを引き継ぎます。デフォルトで、Call Bridge グループ内の Call Bridge は、負荷が 80% になった時点で新しい参加者のコールをすべて拒否し、新しい分配コールだけが許可されます。コールブリッジ間のネットワーク要件としては、グループ内部のコールブリッジ間の RTT を 100 ms 以下に、同じクラスタ内の 2 つのコールブリッジ間の RTT を 300 ms 以下にする必要があります。

注　Call Bridge グループとロード バランシングが使用されない場合は、コールが拒否されませんが、負荷制限に到達したときにすべてのコールの品質が低下します。この現象が頻繁に起きる場合は、追加のハードウェアを配置することをお勧めします。

データベース クラスタは、1 つのマスターと複数のスレーブで構成されます。最大データベース数は 5 で、ノード間の最大 RTT は 200 ms です。データベース マスターは読み取り操作と書き込み操作の両方を実行できますが、スレーブは読み取り操作だけを実行できます。Call Bridge は常にデータベース マスターに接続して読み取りと書き込みを行い、マスターでのすべての変更内容がスレーブに複製されます。ローカル データベースを備えた Call Bridge は自動的にローカル データベース クラスタのマスターに接続しますが、ローカル データベースを備えていない Call Bridge は手動でデータベース クラスタに接続される必要があります。マスターで障害が発生すると、スレーブの 1 つが新しいマスターになり、他のスレーブがこの新しいマスターに対して再登録します。障害が修復されると、古いマスターがスレーブになり、新しいマスターに対して登録します。ネットワーク分割が発生した場合は、クラスタ メンバーの過半数を認識できるデータベース ノードのみが、マスターへの昇格対象と見なされます。同様に、クラスタ メンバーの過半数を認識できない既存のマスターはスレーブに降格されます。これにより、複数のマスターが作成されないことが保証されます。ここで、データベース クラスタが偶数（2 つまたは 4 つ）のノードで構成され、等しいノード数の 2 つのセグメントにネットワークが分割された場合、一方の側のマスターが過半数の（つまり半数を超える）クラスタ メンバーを認識できないため、スレーブに降格されます。この場合、クラスタ内にマスターが存在しなくなり、Call Bridge は引き続きコールを引き受けますが、データベースの書き込み操作が不可能になります。このような理由で、マスターが常に選択されるようにするには、データベース クラスタのノード数を奇数にすることをお勧めします。その結果、クラスタ内のデータベース ノードの最小数は 3 になります。

XMPP の復元力により、特定の XMPP サーバに到達できないクライアント向けのフェールオーバー保護が提供されます。3 つ以上の奇数の XMPP サーバ ノードを使用して XMPP サーバ クラスタを設定する必要があります。これは、Cisco Meeting Server が XMPP サーバ マスターを選択するために過半数のクラスタ ノードが使用可能であるというマスター選択アルゴリズム要件があるためです。クラスタで XMPP サーバ マスターが使用可能でない場合、Cisco ミーティング アプリ ユーザはログインできません。各 XMPP サーバは、リンクが確立されている他のサーバの場所を認識しています。サーバはキープアライブ メッセージを使用して互いをモニタし、マスターを選出します。XMPP メッセージは任意のサーバに送られる可能性があり、マスター XMPP サーバに転送されます。マスターで障害が発生した場合は、新しいマスターが選択され、他の XMPP サーバは新しいマスターにメッセージを転送します。Call Bridge は DNS SRV レコード（_xmpp-component）を使用して、SRV レコードで設定された優先順位と重要度に基づいて利用可能な XMPP サーバと接続します。Call Bridge は、一度に 1 つの XMPP サーバに接続します。ネットワークの問題によって Call Bridge と XMPP サーバとの接続が失われた場合、Call Bridge は別の XMPP サーバに再接続しようとします。すべての Call Bridge をそれぞれの XMPP サーバ内で設定する必要があります。

C：図 3-7 は、高可用性を備えた Cisco Meeting Server クラスタの最小設定を示しています。この構成では、データベースおよび XMPP サーバの 3 つのインスタンスをホストするために、最低 3 台のサーバが必要です。別個のサーバで各コンポーネント サービス（Web Bridge と Call Bridge）の少なくとも 2 つのインスタンスを有効にし、Call Bridge を 1 つのグループに配置します。各サーバ内のすべてのサービスを有効にする必要はありません。必要なものだけを有効にします。2 つの Call Bridge で処理できる以上のキャパシティが展開に必要な場合は、追加の Call Bridge を 3 番目のサーバでセットアップすることができます（Call Bridge 専用の 4 番目のサーバを調達する必要はありません）。C：表 3-3 は、単一の Unified CM クラスタ用のさまざまな数の Call Bridge に必要な Cisco Meeting Server クラスタ最小構成を示しています。

C：表 3-3　単一の Unified CM クラスタ用のさまざまな数の Call Bridge に必要な Cisco Meeting Server クラスタ最小構成

Call Bridge グループ	コール ブリッジの数	Cisco Meeting Server クラスタ構成
A	2	ノード A1：Web Bridge、Call Bridge、データベース、XMPP ノード A2：Web Bridge、Call Bridge、データベース、XMPP ノード A3：XMPP、データベース
	3	ノード A1：Web Bridge、Call Bridge、データベース、XMPP ノード A2：Web Bridge、Call Bridge、データベース、XMPP ノード A3：Call Bridge、データベース、XMPP
	4	ノード A1：Web Bridge、Call Bridge、データベース、XMPP ノード A2：Web Bridge、Call Bridge、データベース、XMPP ノード A3：Call Bridge、データベース、XMPP ノード A4：Call Bridge
	5	ノード A1：Web Bridge、Call Bridge、データベース、XMPP ノード A2：Web Bridge、Call Bridge、データベース、XMPP ノード A3：Call Bridge、データベース、XMPP ノード A4：Call Bridge ノード A5：Call Bridge

TMS ハイ アベイラビリティー

大規模な Cisco TMS 展開の高可用性には、2 つの TMS フロントエンド サーバ、TMSXE を実行する 2 つのサーバ、ネットワーク ロード バランサ、および外部 Microsoft SQL データベースが含まれます（C：図 3-2 を参照）。TMS 復元性では、2 つのサーバ（1 つのアクティブ ノードと 1 つの パッシブ ノード）だけがサポートされており、またこのモデルでは、TMS 導入環境のキャパシティを増減することはできません。ネットワーク ロード バランサ（NLB）は、TMS サーバの前面に展開されます。TMS への着信トラフィックは、NLB を通過してアクティブ ノードに転送されます。TMS からの送信トラフィックは、NLB を通過せず直接、宛先に送信されます。NLB は既存のアクティブ ノードで障害を検出すると、ユーザによる介入なしで、自動的に新しいアクティブ ノードに切り替えます。

Cisco Meeting Management のハイ アベイラビリティー

Cisco Meeting Management には、復元力のためのクラスタ機能は組み込まれていません。高可用性のために、お客様は同一の設定で、2 つの独立した Cisco Meeting Management インスタンスを設定できます。この場合、両方のインスタンスを同じ Cisco Meeting Servers と Cisco TMS に接続する必要があります。次に、ネットワークロードバランサーを Cisco Meeting Management インスタンスの前に配置すると、ユーザはロード バランサを介して Cisco Meeting Management ポータルに接続することができます。Cisco Meeting Management サーバのロード バランサの設定と可用性により、どの Cisco Meeting Management サーバにユーザが接続するかが判断されます。

会議のセキュリティー

プリファード アーキテクチャは、メディアとシグナリングの暗号化を完全にサポートします。ただし、このドキュメントで紹介するソリューションでは、簡略化のために、すべての会議用に Cisco Meeting Server と Unified CM の間に非セキュア SIP トランクを実装します。例外として、Unified CM と Cisco Meeting Server の間の API 通信を暗号化するというソリューション要件があるので、この場合は HTTPS を使用する必要があります。

Cisco Meeting Server は外部コンポーネントとの通信および内部コンポーネント間の通信にセキュア接続を使用するため、証明書が必要です。コンポーネント間の接続を保護するには、認証局（CA）署名付き証明書を使用します。詳細については、セキュリティーの章を参照してください。

PIN やパスワードを使用して会議へのアクセスを制限するため、別レベルのセキュリティを追加できます。接続が許可される前にすべての参加者に PIN の入力を求めるように、すべてのスケジュール済み会議または無期限会議で PIN を設定できます。

会議ソリューションのスケーリング

会議ソリューションを拡張する主な方法は、標準的な Cisco Meeting Server クラスタに（最大 8 つまで）Call Bridge を追加することです。

この展開では、Unified CM 内の SIP トランクを使用したダイヤル プラン、ルート グループ、およびルート リスト設定に基づいて、クラスタ内の任意の Call Bridge にコールをルーティングできます。同じ会議に対する複数コールが別々の Call Bridge にルーティングされる場合は、最後の 4 人のアクティブ スピーカー（話者）の音声とビデオが Call Bridge 間で交換され、1 つのブリッジ上の参加者が別のブリッジ上のアクティブ スピーカーを認識できます。

注　Cisco Meeting Server は、8 つを超える Call Bridge を使用したクラスタリングをサポートしますが、その展開にはシスコの事前承認が必要です。詳細については、地域のシスコ アカウント チームにお問い合わせください。

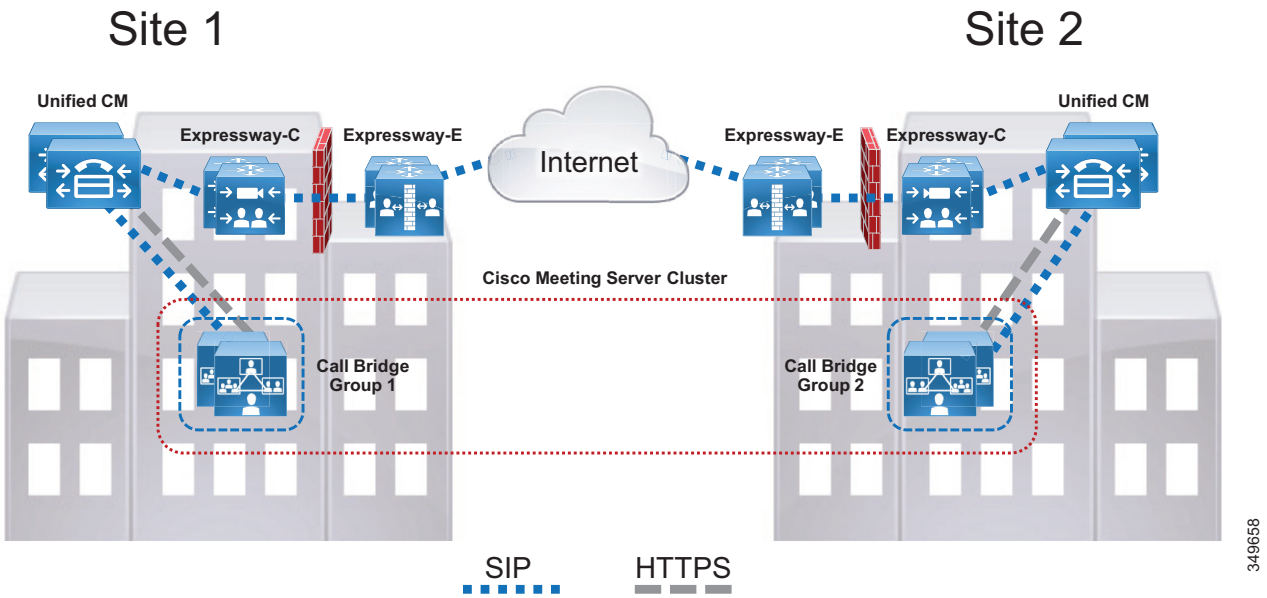
Call Bridge ごとに 450 人の参加者をサポートできます。そのため、会議ごとの参加者の最大数は単一のサーバで 450 人、1 つのクラスタ内の複数サーバでは最大 2,600 人の参加者をサポートできます。

複数の Unified CM クラスターに関する考慮事項

複数の Unified CM クラスタを含む大規模展開では、複数の Call Bridge グループを使って設定された 1 つの Cisco Meeting Server クラスタを使用し、Unified CM クラスタごとに 1 つのグループを割り当てます。

たとえば、展開に 3 つの Unified CM クラスタがある場合は、各 Unified CM クラスタに 1 つずつ、合計 3 つの Call Bridge グループを使用して 1 つの Cisco Meeting Server クラスタを展開する必要があります。各 Unified CM クラスタにおいて、ローカル Call Bridge グループ内の Call Bridge ごとに 1 つの SIP トランクが必要です。Unified CM クラスタへのすべての着信会議コールが、ローカル Call Bridge グループによって処理されます。Call Bridge には、フル メッシュ内のグループ内部および外部のピアに接続された分配リンクが必要です。同じ会議では、ユーザが Unified CM クラスタからダイヤルインしてローカル Call Bridge グループに到達できます。別々のグループ内の Call Bridge は、参加者がブリッジを超えて互いに認識できるように、最後の 4 人のアクティブ スピーカーの音声とビデオをピアと交換します。（C：図 3-8）。

C：図 3-8　　複数の Unified CM クラスタを使用した Cisco Meeting Server の展開



最初の Unified CM クラスタの設計については、Ciso Meeting Server の高適用性に関するセクションと C：表 3-3 を参照してください。

2 番目の Unified CM クラスタでは、Cisco Meeting Server クラスタを拡張して 2 つの新しいサーバを追加します。それぞれのサーバで Web Bridge と Call Bridge を有効にします。この Unified CM クラスタでは、余分なデータベースや XMPP サービスは必要ありません。Call Bridge を既存のデータベース クラスタに接続し、すべての新しい Call Bridge を XMPP クラスタに追加します。この 2 番目の Unified CM クラスタで使用される新しい Call Bridge グループに Call Bridge を配置し、Web Bridge をこの Call Bridge グループに関連付けます。追加のキャパシティが必要な場合は、Call Bridge をホストする 1 つのサーバを追加して、その Call Bridge をこの 2 番目の Unified CM クラスタの Call Bridge グループに配置します。C：表 3-4 は、必要な新しい Call Bridge の数に基づいて、2 番目の Unified CM クラスタに必要な追加の Cisco Meeting Server クラスタ構成を示しています。

C：表 3-4　2 番目の Unified CM クラスタ用の追加の Cisco Meeting Server ノード構成

Call Bridge グループ	追加のコール ブリッジの数	追加の Cisco Meeting Server ノード構成
B	2	ノード B1：Web Bridge、Call Bridge ノード B2：Web Bridge、Call Bridge
	3	ノード B1：Web Bridge、Call Bridge ノード B2：Web Bridge、Call Bridge ノード B3：Call Bridge
	4	ノード B1：Web Bridge、Call Bridge ノード B2：Web Bridge、Call Bridge ノード B3：Call Bridge ノード B4：Call Bridge

3 番目の Unified CM クラスタでは、Cisco Meeting Server クラスタを拡張して 2 つのサーバを追加します。それぞれのサーバで Web Bridge と Call Bridge を有効にします。Call Bridge を既存のデータベース クラスタに接続し、すべての新しい Call Bridge を XMPP クラスタに追加します。この 3 番目の Unified CM クラスタで使用される新しい Call Bridge グループに Call Bridge を配置し、Web Bridge をこの Call Bridge グループに関連付けます。追加のキャパシティが必要な場合は、Call Bridge をホストする 1 つのサーバを追加して、その Call Bridge をこの 3 番目の Unified CM クラスタの Call Bridge グループに配置します。C：表 3-5 は、必要な新しい Call Bridge の数に基づいて、3 番目の Unified CM クラスタに必要な追加の Cisco Meeting Server ノード構成を示しています。

C：表 3-5　3 番目の Unified CM クラスタ用の追加の Cisco Meeting Server ノード構成

Call Bridge グループ	追加のコール ブリッジの数	追加の Cisco Meeting Server ノード構成
C	2	ノード C1：Web Bridge、Call Bridge ノード C2：Web Bridge、Call Bridge
	3	ノード C1：Web Bridge、Call Bridge ノード C2：Web Bridge、Call Bridge ノード C3：Call Bridge
	4	ノード C1：Web Bridge、Call Bridge ノード C2：Web Bridge、Call Bridge ノード C3：Call Bridge ノード C4：Call Bridge

3 つの Unified CM クラスタと 3 つの別々の Call Bridge グループを使用すれば、最初の Call Bridge グループに対してローカルな 3 つの XMPP およびデータベース クラスタ ノードを Call Bridge グループ間で分散できるため、Call Bridge グループごとに 1 つのローカル XMPP およびデータベース クラスタ ノードが割り当てられます。最初の Call Bridge グループに対してローカルな XMPP およびデータベース クラスタ ノードのうち 2 つをそれぞれ 2 番目と 3 番目の Call Bridge グループに移行することにより、すべての Call Bridge グループで XMPP および

データベース サービスの冗長性が確保されます。C：表 3-6 は、この新しい Cisco Meeting Server クラスタ設定を示しています。

C：表 3-6　　2 番目と 3 番目の Call Bridge グループに XMPP およびデータベース サービスを移行する

Call Bridge グループ	Cisco Meeting Server クラスタ構成
A（Unified CM クラスタ 1）	ノード A1：Web Bridge、Call Bridge、データベース、XMPP ノード A2：Web Bridge、Call Bridge
B（Unified CM クラスタ 2）	ノード B1：Web Bridge、Call Bridge、データベース、XMPP ノード B2：Web Bridge、Call Bridge
C（Unified CM クラスタ 3）	ノード C1：Web Bridge、Call Bridge、データベース、XMPP ノード C2：Web Bridge、Call Bridge

展開に 4 番目の Unified CM クラスタが必要な場合は、Cisco Unified CM Session Management Edition 設計に移行することをお勧めします。ただし、このドキュメントではこれについて説明しません。

以降のガイドラインは、複数の Unified CM クラスタ用の別々のリージョンに Cisco Meeting Server クラスタを拡張する場合に当てはまります。

- 1 つの Cisco Meeting Server クラスタを 1 つ以上の Unified CM クラスタの展開に使用する必要があります。
- 標準的な Cisco Meeting Server クラスタに、最大 8 つの Call Bridge を展開することができます。8 つを超える Call Bridge をクラスタに展開する場合は、事前にシスコ アカウント チームの承認を得てください。
- Cisco Meeting Server クラスタに、最大 5 つのデータベースと奇数のノードを展開します。
- Cisco Meeting Server クラスタに、奇数の XMPP サービス ノードを展開します。
- ラウンド トリップ時間（RTT）ネットワーク要件：
  - Cisco Meeting Server クラスタ内の Call Bridge 間で最大 300 ms、データベース間で最大 200 ms
  - グループ内部の Call Bridge 間で最大 100 ms

会議の導入プロセス

会議ソリューションを導入するには、以下の主要なタスクをリストの順に実行します。

1. 会議の導入を計画する
2. Cisco Meeting Server を展開する
3. 会議用の Unified CM を有効にする
4. Cisco TelePresence Management Suite を展開する
5. Cisco Meeting Server スペースを展開する
6. Cisco Meeting Management の展開

1. 会議の導入を計画する

会議ソリューションを導入する前に、以下の項目について計画します。

要件

- 複数の DNS SRV レコードと A レコードが必要な Cisco Meeting Server の DNS を設定します。たとえば、Cisco ミーティング アプリは _xmpp-client SRV レコードを使用してユーザ認証用の XMPP サービスを検索します。
- Cisco Meeting Server では、導入を完了するために API を使用する必要があります。更新用の REST API コマンドを発行するために使用できるツール（Postman（ https://www.getpostman.com/）など）を入手します。

ライセンス

さまざまな製品にライセンスをインストールする必要があります。

- Cisco TMS では、展開に十分なデバイス ライセンスをインストールする必要があります。
- Cisco Meeting Server では、Call Bridge を実行する各ノードに十分なマルチパーティ ライセンスをインストールする必要があります。

マルチパーティは、Cisco Meeting Server の展開に推奨されているユーザ ベースのライセンス モデルであす。Call Bridge サービスが有効になっているすべてのノードにこれを適用する必要があります。Personal と Shared の 2 つのバリエーションがあります。Personal Multiparty Plus（PMP+）は特定のネームド ホスト用であり、Shared Multiparty Plus（SMP+）は会議室システム用またはユーザ間での共有用です。各ライセンスでは、ユーザは、参加者数無制限、ビデオの最大解像度 1080p の会議をホストできます。C：表 3-7 で、Personal Multiparty および Shared Multiparty の各ライセンスに含まれる機能を要約します。

C：表 3-7　　Cisco Personal および Shared Multiparty Plus ライセンスの機能

機能	Personal Multiparty Plus	Shared Multiparty Plus
ネームド ホストとの関連付け	はい	いいえ（No）
アベイラビリティ	Cisco UWL Meetings に付属	個別に購入するか、またはルーム システムと共に割引価格で購入

C：表 3-7　Cisco Personal および Shared Multiparty Plus ライセンスの機能（続き）

機能	Personal Multiparty Plus	Shared Multiparty Plus
最小発注数	25	1
会議の最大参加者数	無制限（利用可能なハードウェア キャパシティの制限内）	
最大解像度	ビデオ用の 1080p60（フル HD）とコンテンツ用の 1080p30 シングル スクリーンまたはマルチ スクリーン エンドポイント	
Business-to-Business（B2B）または Business-to-Customer（B2C）用のリッチ メディア セッション	同梱	同梱
Cisco TMS、TMSXE、および Skype for Business/Lync 相互運用ライセンス	同梱	新規顧客は Starter Pack を購入[1]
インスタント会議、無期限会議、およびスケジュール済み会議のサポート	はい	はい

1. TMS と関連製品のライセンスだけが必要な場合は、TMS Starter Pack をご購入いただけます。

マルチパーティ ランセンスは、プリファード アーキテクチャで使用されるライセンス モデルです。マルチパーティ ライセンスの詳細については、次の Web サイトで入手可能な『*Cisco Multiparty Licensing At-a-Glance*』を参照してください。

https://www.cisco.com/c/dam/en/us/solutions/collateral/collaboration/pervasive-conferencing/at-a-glance-c45-729835.pdf

Cisco TelePresence Management Suite

インストールと設定のプロセスを開始する前に、組織固有の構造と設定に合わせて各種アイテムを決定する必要があります。設定プロセス中にいくつかの設定値を使用する必要があるため、インストール プロセスの開始前にそれらの情報を収集してください。

Microsoft SQL

Cisco TMS は、会議、ユーザ、システムに関するすべてのデータを外部 Microsoft SQL データベースを使用して保存します。インストール プロセスでは、TMS と関連ソフトウェア拡張機能によって特定のデータベースがいくつか作成されます。TMS アプリケーションでは、tmsng データベースとの通信がアクティブでない場合には、ユーザは Web ページにログインできません。このように SQL データベースとの継続的な通信に依存しているため、SQL データベースでは、Microsoft によるデータベースの復元性を実現する手法も使用する必要があります。データベースのサイズは、導入の規模とスケジューリング イベントの数に応じて異なりますが、一般的な指針として、ほとんどの組織では初期ストレージとして 1 GB あれば十分です。

C：表 3-8 に、Cisco TMS と TMSXE をサポートするために必要な Microsoft SQL 2012 の仕様を示します。

C：表 3-8　Cisco TMS と TMSXE のサポートに必要な Microsoft SQL 2012 の仕様

要件	パラメータ
TMS が使用するアカウントの SQL ユーザ アカウント権限	**dbcreator** ロールと **security admin** ロール
認証	SQL Server および Windows 認証（混合モード）
デフォルト言語	英語
タイム ゾーン	TMS サーバのタイム ゾーンに一致している必要があります
作成されるデータベース	tmsng（CiscoTMS）
復元性モデル	Windows Server フェールオーバー クラスタ（WSFC）による **AlwaysOn フェールオーバー クラスタ** インスタンス

注　その他の SQL 復元性モードが TMS でサポートされていますが、**AlwaysOn フェールオーバー クラスタ**以外の方法では、SQL の停止中に TMS 管理者が手動で調整を行う必要があります。

Active Directory

Cisco TMS は、Microsoft Active Directory のさまざまな側面と統合するので、サーバを組織のドメインに追加する必要があります。すべての TMS ユーザは Active Directory からインポートされ、Active Directory に対して認証されます。

設定プロセスでは、TMS がユーザをインポートできるようにするため、**AD サービス アカウントのユーザ名とパスワード**を入力する必要があります。これは読み取り専用アカウントであり、TMS が Active Directory の情報を変更することはありません。このアカウントには、AD 構造の最上位レベルへのアクセス権限が必要です。このアクセス権限により、後続のすべてのエンドユーザがその機能にアクセスできるようになります。複数ドメインを使用する組織では、TMS ユーザ アカウントに最上位ドメインを関連付ける必要があります。エンドユーザが Exchange リソースを予約できるようにするため、TMSXE アプリケーションには追加のサービス アカウントが必要です。これも読み取り専用サービス アカウントである必要があります。また、実際のイベント予約にはエンドユーザのクレデンシャルが使用されます。TMSXE ユーザ アカウントでは、TMSXE アプリケーションだけが Exchange Web Service を介して Exchange Server で認証および Exchange Server と通信できます。

また、AD で、TMS のスケジュール機能へのアクセス権限を持つエンドユーザと TMS 管理者の同期に使用する既存のグループを指定するか、または新規のグループを作成します。

注　TMS サーバのローカル マシン アカウントは、フロントエンド サーバ間で複製されないため、使用しないでください。また他のノードがアクティブになるとユーザ クレデンシャルが使用できなくなります。

電子メールの統合

ユーザが会議をスケジュールすると、TMS は参加者のすべての接続情報を記載した自動メールをユーザに送信します。インストール プロセスで、この自動メールの送信元としてエンドユーザに対して表示される「from」アドレスを入力する必要があります。このため、collabconferencing@ent-pa.com のようなアドレス、または現在組織内で使用していない類似アドレスを選択します。

また、送信メール サーバの SMTP アドレスも入力する必要があります。

エンドポイントの命名規則

エンドポイントが Cisco TMS に追加される理由として、次の 2 つの理由があります。

- 会議リソースの割り当てのために Exchange リソースを関連付ける
- TMS がワンボタン機能の接続情報をエンドポイント ユーザ インターフェイスに提供できるようにする

TMS にエンドポイントが追加されると、Exchange でルーム名またはリソース名として同じ文字列が使用されます。これにより、エンドユーザに対して、コール履歴にシステム名が表示されるときに統一がとられます。また、画面上のラベルのテキストが会議リソースから取り込まれます。

TMS Systems Navigator のフォルダ構造の使用法について系統立った計画を立てることで、管理者が簡素化されたインターフェイスを使用できるようになります。

組織のデフォルト会議パラメータ

これは組織別にカスタマイズ可能な設定であり、各自のネットワークに関する考慮事項、会議の流れ、企業風土に基づいて使用する必要があります。エンドユーザが Outlook 経由でスケジュールしたすべての会議に、デフォルトの会議設定が使用されます。デフォルトの会議のさまざまな設定については、次の場所にある『*Cisco TelePresence Management Suite Administrator Guide*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html

Cisco Meeting Server スペースのプロビジョニング

組織で Cisco Meeting Server スペースをどのように利用すべきかを理解するには、エンドユーザたちが会議で想定するワークフローについて理解する必要があります。組織によっては、特にスタッフが別々の場所にいて共通の会議室に集合できないような場合に、特定の会議タイプにスケジュール済みリソースの代わりにスペースを活用することができます。

サーバのロケーション

冗長 TMS 導入環境のアクティブ ノードとパッシブ ノードの両方に対し、サーバ オペレーティング システムで同一タイム ゾーンを設定する必要があります。また、これは SQL サーバと同じタイム ゾーンである必要もあります。冗長 TMS のサポートは、アクティブ ノードとパッシブ ノードの両方と SQL サーバが同じローカル ネットワーク上に存在する場合に限定されています。

2. Cisco Meeting Server を展開する

このセクションでは、Cisco Meeting Server を展開してスケジュール済み会議と非スケジュール済み会議用にそれらを準備するのに必要な主なタスクについて説明します。

概要

Cisco Meeting Server の展開タスク：

1。 Cisco Meeting Server 機能ライセンス キーをインストールします。

2。 エンタープライズ CA 署名付き証明書を生成します。

3。 Web 管理、XMPP、Call Bridge、および Web Bridge サービスを設定します。

4。 冗長性のために追加のノードをセットアップし、XMPP、データベース、および Call Bridge のクラスタリングを設定します。

5。 分散会議用の Call Bridge クラスタ ピアにコールを送信するアウトバウンド ダイヤル プランをセットアップします。

6。 Call Bridge グループを 1 つ作成し、Unified CM クラスタ用にすべての Call Bridge をそのグループに追加します。

7。 コール設定のパラメータを更新します。

展開の考慮事項

メディア トラフィックが Cisco Meeting Server と会議の各参加者との間を流れるので、Cisco Meeting Server の物理的な場所を考慮することが重要です。参加者に最高のエクスペリエンスを提供するには、Call Bridge を使用する Cisco Meeting Server の場所を集中させ、それらのブリッジを各リージョンの Unified CM クラスタ用の 1 つのグループに配置します。

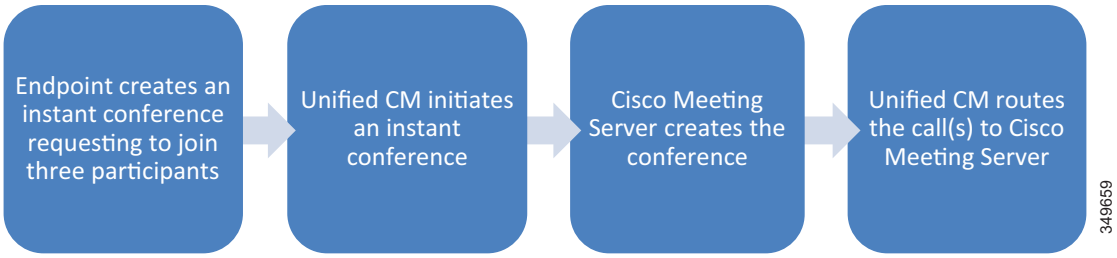
展開に Cisco Meeting アプリあるいは Web Bridge が含まれている場合は、XMPP サーバを有効にして、ユーザ認証用の XMPP ドメインを使ってそれを設定する必要があります。親ドメイン（ent-pa.com など）を XMPP ドメインとして使用することを避けてください。これは、そのドメインが Cisco Unified CM IM and Presence Service などの他のコンポーネントですでに使用されている可能性があり、その場合には全体の設計が複雑になるためです。Cisco Meeting Server 用の XMPP ドメインとしてサブドメイン（cms.ent pa.com など）を使用することをお勧めします。

XMPP サーバ / データベース用の 3 ノード クラスタを展開します。これにより、ほとんどの展開シナリオで復元力と高可用性が提供されるはずです。

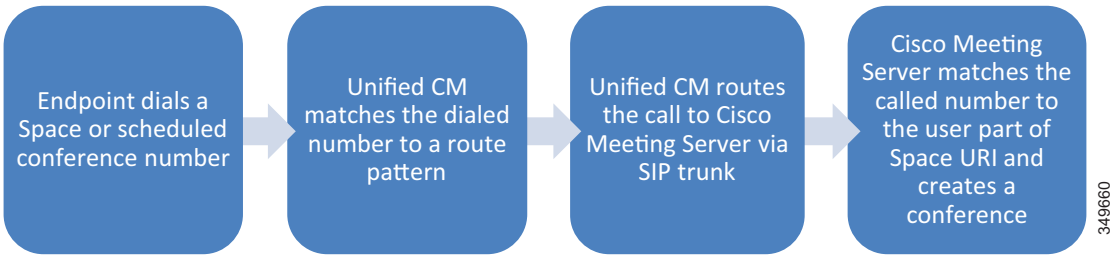
各 Web Bridge に同じ名前（join.ent pa.com など）を使用して DNS A レコードを作成します。そうすれば、会議に参加するために使用する Web Bridge URL（たとえば https://join.ent-pa.com）を参加者が覚えやすくなります。

インスタント、無期限、およびスケジュール会議

C : 図 3-9　　インスタント会議のコール フロー



C : 図 3-10　　無期限またはスケジュール会議のコール フロー



Cisco Meeting Server の展開タスク

Cisco Meeting Server は、Call Bridge ライセンスなしでコールを受け取ることができません。Call Bridge、マルチパーティ ランセンス、その他の機能ライセンスが **cms.lic** という名前の単一のライセンス ファイルにバンドルされています。SFTP クライアント ソフトウェアを使用して、ライセンス ファイルをそれぞれの Cisco Meeting Server にアップロードします。ライセンス ファイルは Cisco Meeting Server の MAC アドレスに対応付けられます。このため、正しいファイルを対応するサーバにアップロードする必要があることに注意してください。

エンタープライズ CA 署名付き証明書の生成方法の詳細については、セキュリティーの章の Cisco Meeting Server のセクションを参照してください。これにより、2 つの証明書が生成されます。1 つは、任意のノード内の Web 管理、XMPP、Call Bridge、Web Bridge、およびデータベース クラスタ用に共有される証明書で、もう 1 つは、データベース クラスタへの接続用にローカル データベースを備えていない Call Bridge によって使用される証明書です。

これが **Call Bridge** ノードでない場合は、省略してください。

Web 管理では、メインボード管理プロセッサ（MMP）コマンドを使用してリスニング インターフェイスとポートを指定し、共有 CA 署名付き証明書をインストールして、サービスを有効にします。これにより、管理者は、指定されたリスニング インターフェイスおよびポートを使用して Web インターフェイスにアクセスすることができます。デフォルトでは、Web 管理と Web Bridge の両方がポート 443 を使用します。この両方がポート 443 を使用する場合は、別々のネットワーク インターフェイスを使用する必要があります。しかし、同じインターフェイスを使用する場合は、どちらかのサービスが別のデフォルト ポートを使用する必要があります。その場合、Web 管理のデフォルト ポートを、他の使用されているポート（ポート 445 など）に変更することをお勧めします。

Call Bridge では、MMP コマンドを使用してリスニング インターフェイスを指定し、共有 CA 署名付き証明書をインストールして、サービスを再起動します。

XMPP サーバでは、MMP コマンドを使用してリスニング インターフェイスと XMPP ドメイン（cms.ent-pa.com など）を指定し、共有 CA 署名付き証明書をインストールして、サービスを有効にします。最初の XMPP サーバでは、必要な数の Call Bridge を追加し、各 Call Bridge に一意の名前を割り当て、生成された名前と秘密文字列を書き留めます。後続の XMPP サーバでは、最初の XMPP サーバで生成された Call Bridge 名と秘密文字列を使用して、必要な数の Call Bridge を追加します。

これが Call Bridge ノードでない場合は、省略してください。

Web インターフェイス（[設定（Configuration）] -> [全般（General）]）に移動し、C：表 3-9 の値を使用して XMPP サーバ設定を構成します。

C：表 3-9　　最初の Call Bridge 用の XMPP サーバ設定

フィールド名	値
一意の Call Bridge 名（Unique Call Bridge name）	< *一意の Call Bridge 名* >
ドメイン（Domain）	cms.ent-pa.com
サーバ アドレス（Server address）	空白のまま
共有秘密（Shared secret）	<*Call Bridge の秘密文字列*>

Web Bridge では、MMP コマンドを使用してリスニング インターフェイスを指定し、共有 CA 署名付き証明書をインストールし、上記でインストールした Call Bridge 証明書に対する信頼を有効にして、サービスを有効にします。Web Bridge は、WebRTC クライアントからの接続を受け入れた後で Call Bridge に接続するので、Call Bridge からの証明書を信頼する必要があります。

クラスタ内のすべてのノードに対して上記の手順を繰り返します。

データベース クラスタをセットアップします。

各データベース ノードで MMP コマンドを使用して、データベースによって使用されるネットワーク インターフェイスを指定し、共有 CA 署名付き証明書をインストールします。1 つのノードをマスターとして選択し、MMP コマンドを実行してデータベースを初期化します。各データベース スレーブ ノードに移動し、MMP コマンドを実行してデータベースとクラスタを接続します。ローカル データベースを備えていない Call Bridge が配置されたすべてのノードで、2 番目の証明書をインストールし、MMP コマンドを実行してクラスタに接続します。次のコマンドに移る前に、コマンドの実行ステータスが「成功」になっていることを確認してください。これで、データベース クラスタのセットアップが完了しました。

警告　スレーブ データベース内のデータは、スレーブがクラスタに参加した後、マスターによって上書きされます。

Call Bridge クラスタをセットアップします。

各 Call Bridge ノードで、Web インターフェイス（[設定（Configuration）] -> [クラスタ（Cluster）]) に移動して、Call Bridge の [ID（Call Bridge identity）] の下で一意の名前（callbridge1 など）を設定します。その後、いずれかの Call Bridge ノードでクラスタの設定（[設定（Configuration）] -> [クラスタ（Cluster）]）に戻り、C：表 3-10 の例を参考にして [クラスタ化された Call Bridges（Clustered Call Bridges）] にすべての Call Bridge に関する情報を入力し、その他のフィールドを空白またはデフォルトのままにします。

C：表 3-10　クラスタ化された Call Bridge の設定例

一意の名前	アドレス	コメント
callbridge1	https://10.x.x.60:445	[アドレス（Address）] 列は、Web インターフェイスにアクセスするために使用される URL とポート番号です。
callbridge2	https://10.x.x.61:445	
callbridge3	https://10.x.x.62:445	

[クラスタ化された Call Bridge（Clustered Call Bridges）] の設定は、Web インターフェイスからすべての Call Bridge ノードに表示されます。これらは、分散会議用にピア間でコール信号とステータス メッセージを渡すために Call Bridge で使われる分配リンクです。

API を使用して、分散会議用のコールブリッジクラスタピアにコールを送信するためのアウトバウンドダイヤルプランルールをセットアップします。各コールブリッジには、コール制御ではなく直接ピアにコールをルーティングするように、各ピアに対して設定された発信ダイヤルプランルールを設定する必要があります。クラスタ内に 3 つの Call Bridge が存在する場合は、Call Bridge ごとに 2 つのアウトバウンド ダイヤル プラン ルールを設定する必要があります。クラスタ内で設定されるアウトバウンド ダイヤル プラン ルールは全部で 6 つになります。/callBridges ノードで GET メソッドを使用して、Cisco Meeting Server クラスタ内のすべての Call Bridge の ID を取得します。C：表 3-10 の [クラスタ化された Call Bridge（Clustered Call Bridges）] の設定例を参考にして、C：表 3-11 の各行をパラメータ設定として使用し、/outboundDialPlanRules ノードで POST メソッドを実行します。

C：表 3-11　アウトバウンド ダイヤル プラン ルールのパラメータの例

ドメイン	プライオリティ	スコープ	trunkType	callBridge
10.x.x.61	100	callBridge	sip	*<callbridge1 ID>*
10.x.x.62	100	callBridge	sip	*<callbridge1 ID>*
10.x.x.60	100	callBridge	sip	*<callbridge2 ID>*
10.x.x.62	100	callBridge	sip	*<callbridge2 ID>*
10.x.x.60	100	callBridge	sip	*<callbridge3 ID>*
10.x.x.61	100	callBridge	sip	*<callbridge3 ID>*

展開された Web Bridge ごとに、Call Bridge は Web Bridge にアクセスするための URL を認識する必要があります。C：表 3-12 の各行の URL パラメータを使用して、/webBridges ノードで POST メソッドを実行します。

C：表 3-12　Web Bridge の設定例

Web Bridge の IP アドレス	URL
10.x.x.60	https://10.x.x.60
10.x.x.61	https://10.x.x.61

XMPP サーバ クラスタをセットアップします。

1 つのノードをマスターとして選択し、MMP コマンドを実行してクラスタを有効化および初期化し、共有 CA 署名付き証明書を信頼するようにクラスタをセットアップします。残りの XMPP サーバで、MMP コマンドを実行してクラスタリングを有効にし、クラスタに参加させて、共有 CA 署名付き証明書を信頼するようにクラスタをセットアップします。次のコマンドに移る前に、各コマンドが正常に実行されたことを確認してください。

C：表 3-13 に示すように、XMPP サーバ ノードごとに DNS SRV レコードを作成します。

C：表 3-13　　XMPP サーバ用の DNS SRV レコード

名前	解決先	ポート	説明
_xmpp-client._tcp.<*XMPPDomain*>	XMPP サーバの FQDN	5222	ログイン認証用の XMPP サーバを検索するために Cisco ミーティング アプリで使用される
_xmpp-component._tcp.<*XMPPDomain*>	XMPP サーバの FQDN	5223	使用可能な XMPP サーバを検索するために Call Bridge で使用される

各 Web Bridge で同じ名前（join.ent pa.com など）を使用して、Web Bridge によって使用されるインターフェイスの IP アドレスに解決される DNS A レコードを作成します。

パラメータ **loadBalancingEnabled** を **true** に設定した API（POST/callBridgeGroups）を使用して、ロード バランシング オプションが有効化された Call Bridge グループを作成し、返された Call Bridge グループの GUID を書き留めます。各 Call Bridge で API（PUT/callBridges）を使用して、Call Bridge をグループに追加するために **callBridgeGroup** パラメータを <*callBridgeGroup GUID*> に設定します。API（PUT/system/configuration/cluster）を使用して、サーバ プラットフォームの最大負荷に関する **loadLimit** パラメータ値を設定します。その際、次の場所にある『*Load Balancing Calls Across Cisco Meeting Servers*』に関するホワイト ペーパーの最新版で指定されているプラットフォーム依存値を使用してください。

https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html

各 Web Bridge で、API（PUT/webBridges）を使用して **callBridgeGroup** パラメータを <*callBridgeGroup GUID*> に設定することで、グループ内の Call Bridge のみが Web Bridge への接続を試みるように Web Bridge と Call Bridge グループを関連付けます。

この時点で、完全な Cisco Meeting Server クラスタが設定されるはずです。いずれかの Web 管理ページを参照し、C：表 3-14 の値を使用して、Web インターフェイス（[設定（Configuration）] -> [全般（General）]）でコール設定パラメータを更新します。

C：表 3-14　　コール設定の構成例

フィールド名	値	コメント
SIP メディア暗号化	[許可（allowed）]	RTP と SRTP の両方を許可する
SIP コール参加者ラベル	[有効（enabled）]	表示名を表示する（レイアウトでサポートされている場合）
TIP コール	[有効（enabled）]	TIP の使用を許可する

要約

上記のタスクが完了したら、Cisco Meeting Server を Unified CM に追加する準備が整います。

3. 会議用の Unified CM を有効にする

このセクションでは、Cisco Meeting Server クラスタを使用した会議用に Unified CM を有効にするために必要な主なタスクを説明します。

概要

インスタント会議用に Unified CM を有効にするための展開タスク：

1. 「**Standard SIP Profile for CMS**」という名前の新しい SIP プロファイルと、「**Security SIP Trunk Profile for CMS**」という名前の SIP トランク セキュリティ プロファイルを作成します。
2. Cisco Meeting Server の Call Bridge ノードを指し示す SIP トランク（SIP_TRUNK_CMS1）を作成します。この手順を、Cisco Meeting Server クラスタ ノード内の各 Call Bridge に対して繰り返す必要があります。たとえば、クラスタ内に 3 つの Call Bridge が存在する場合は、設定された 3 つの SIP トランクが存在する必要があります。
3. 1 つの会議ブリッジを作成し、SIP トランク（タスク 2 で設定済み）をそれに追加します。各会議ブリッジに、いずれかの Call Bridge クラスタ ピアへの SIP トランクが含まれている必要があります。

   API 特権を持つ Cisco Meeting Server 上で作成されたユーザ名とパスワードを使って各会議ブリッジを設定します。

   この手順を、Cisco Meeting Server クラスタで有効になっている各 Call Bridge で繰り返す必要があります。たとえば、クラスタ内に 3 つの Call Bridge が存在する場合は、設定された 3 つの会議ブリッジが存在する必要があります。
4. **Video** という名前のメディア リソース グループ（MRG）を作成します。すべての会議ブリッジを MRG に追加します。クラスタ内に 3 つの Call Bridge が存在する場合は、MRG 内に 3 つの会議ブリッジが存在する必要があります。
5. **Video** という名前のメディア リソース グループ リスト（MRGL）を作成して、MRG（タスク 4 で設定済み）をそれに追加します。エンドポイントによるインスタント会議の使用を許可するには、MRGL をデバイス プールまたはデバイス自体に割り当てます。

無期限会議とスケジュール済み会議用に Unified CM を有効にするための展開タスク：

6. 無期限会議とスケジュール済み会議用のルート グループ（RG_SPACE_SCHED）を作成します。すべての SIP トランク（タスク 2 で設定済み）をルート グループに追加します。クラスタ内に 3 つの Call Bridge ノードが存在する場合は、ルート グループ内に、それぞれ Call Bridge ノードのいずれかを指し示す 3 つの SIP トランクが存在する必要があります。
7. ルート リスト（RL_SPACE_SCHED）を作成し、それにルート グループを追加します。
8. 4. Cisco TelePresence Management Suite を展開する のセクションで設定するスケジュール済み会議の数字エイリアスと一致するルート パターン（8099[12]XXX）を作成します。スペースを設定する場合には、さらに追加のルート パターンが必要になります。それらについては、5. Cisco Meeting Server スペースを展開する のセクションで説明します。

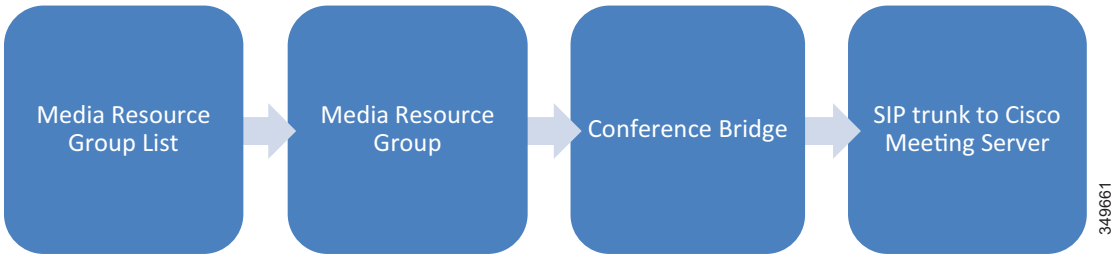
展開の考慮事項

Unified CM は、会議を開始するために Cisco Meeting Server へのコールをどのようにルーティングするかを記述する最初の論理点です。Unified CM でのインスタント会議と無期限 / スケジュール済み会議の設定手順は異なります。これは、それぞれのタイプの会議に参加するためのメカニズムが異なるためです。

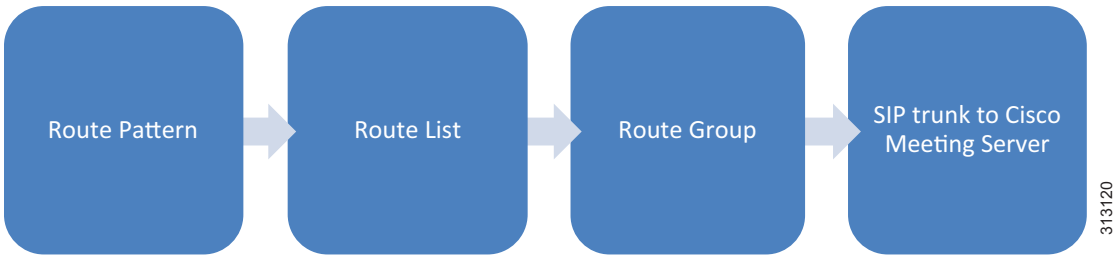
注　インスタント会議を開始するために使用するエンドポイントには、会議ボタンが必要になります。会議ボタンがないエンドポイントもインスタント会議に参加することはできますが、会議ボタンがあるエンドポイントに、会議に追加してもらう必要があります。

インスタントおよび無期限の会議

C：図 3-11　インスタント会議用の Unified CM の内部設定フロー



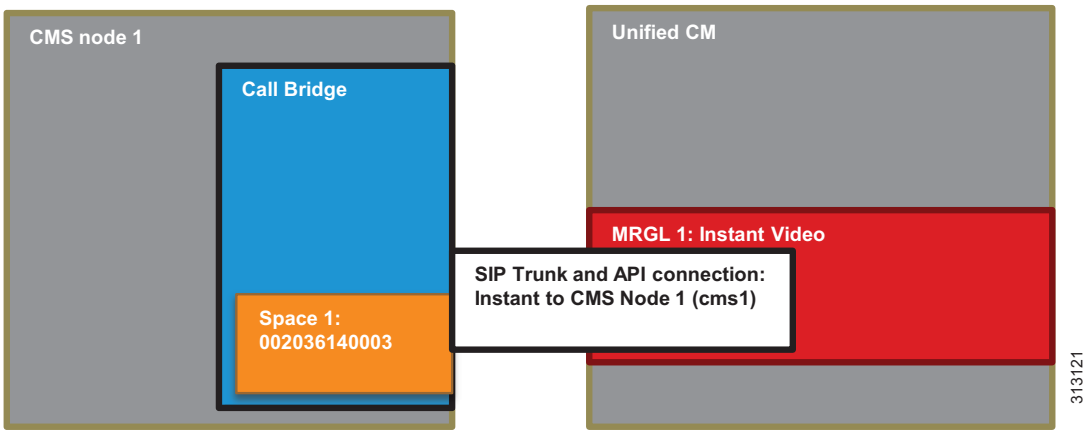
C：図 3-12　無期限会議とスケジュール済み会議用の Unified CM の内部設定フロー



インスタント会議用に Unified CM を有効にするための展開タスク

Unified CM 内の SIP トランクは Cisco Meeting Server 内の Call Bridge を指し示す必要がありますが、API 接続は Web 管理インターフェイスとポートを指し示す必要があることを理解することが重要です。HTTPS を使用して API 接続を保護する必要があります。すべての会議タイプに対して同じ SIP トランクを使用することができます。Cisco Meeting Server クラスタ内の各 Call Bridge ノードには、SIP トランクと Unified CM 内の会議ブリッジからの API 接続で構成される一意のセットが必要です（C：図 3-13）。

C：図 3-13　Cisco Unified CM と Cisco Meeting Server のインスタント関係



Cisco Meeting Server への SIP トランクですべてのシナリオのコールをサポートするには、カスタマイズされた SIP プロファイルと SIP トランク セキュリティ プロファイルが必要です。SIP プロファイルを作成するには、**Standard SIP Profile for TelePresence Conferencing** をコピーして、そのコピーに「**Standard SIP Profile for CMS**」という名前を付け、C：表 3-15 に示されているように設定を変更します。

C：表 3-15　SIP プロファイルの設定

設定	値	コメント
[音声コールとビデオコールに対する早期オファーサポート（Early Offer support for voice and video calls）]	[ベストエフォート（MTP の挿入なし）]	これは、すべての Unified CM トランクに対して推奨される設定です。ベスト エフォートの早期オファー トランクでは、早期オファーを作成するために MTP を使用しません。コールに使用するデバイスに応じて、早期オファーか遅延オファーのいずれかを使用して発信 SIP トランク コールを開始します。この設計では、発信コールは常に早期オファーを使用します。

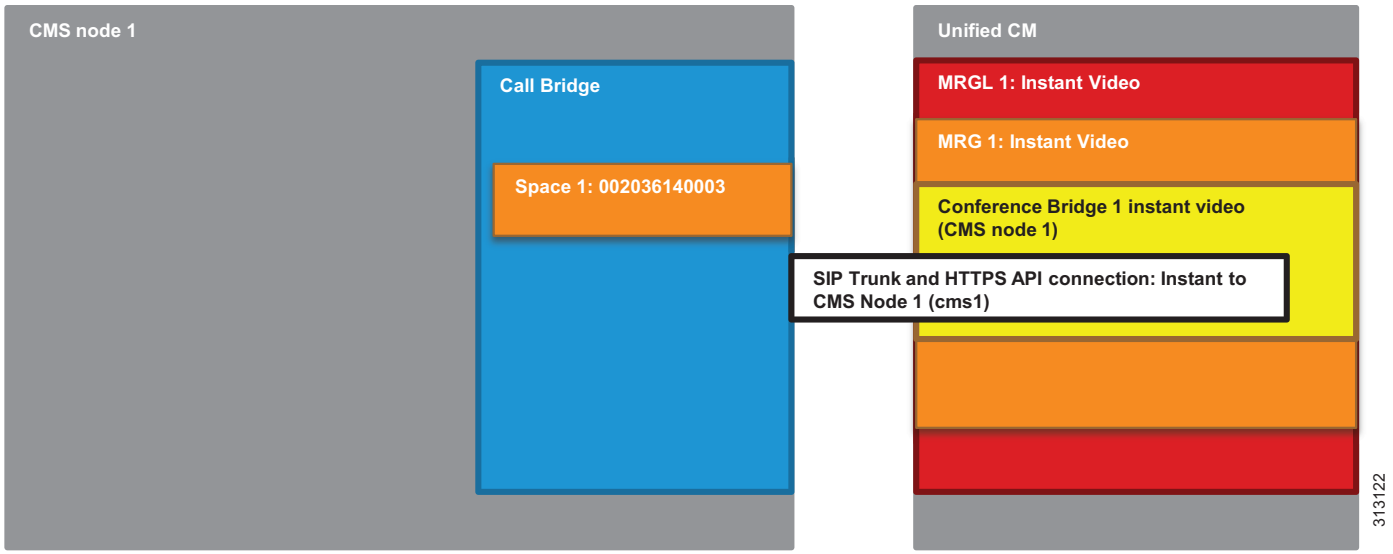
SIP トランク セキュリティ プロファイルを作成するには、**Non Secure SIP Trunk Profile** をコピーして、そのコピーに「**Security SIP Trunk Profile for CMS**」という名前を付け、C：表 3-16 に示すように設定を変更します。

C：表 3-16　SIP トランク セキュリティ プロファイルの設定

設定	値	コメント
[Replaces ヘッダーの許可（Accept replaces header）]	オン	Call Bridge グループ内の該当する Cisco Meeting Server にコールを再ルーティングするための Replaces ヘッダーを伴う INVITE を Unified CM で受け入れるには、このオプションを有効にします。

SIP トランクは、Unified CM に SIP トラフィックをルーティングする場所を伝達します。インスタント会議の場合、SIP トランクは Unified CM に API 要求の宛先も伝達し、それらは会議ブリッジ設定（C：図 3-14）で使用されます。Cisco Meeting Server 内の Call Bridge に接続される SIP トランクを、セキュリティで保護するように設定できますが、このガイドでは、セキュリティで保護しない設定を想定しています。

C：図 3-14　Cisco Unified CM のインスタント設定



会議ブリッジ設定によって、2 つの重要な情報（Cisco Meeting Server と通信するための API クレデンシャルと、その通信用の宛先アドレス）が Unified CM に通知されます（C：図 3-14）。ユーザ名とパスワードが、Cisco Meeting Server で設定された API ユーザのものと一致する必要があります。会議ブリッジで設定された SIP トランクは、HTTPS API トラフィックの送信先を Unified CM に示します。各 SIP トランクは、C：表 3-17 に示す設定で設定します。加えて、各 Unified CM クラスタには、会議ブリッジで設定された一意の会議ブリッジ プレフィックスが必要です。このプレフィックスは単一 Unified CM クラスタの操作には影響を与えませんが、マルチクラスタ Unified CM 展開では、このプレフィックスにより、2 つの Unified CM クラスタが同じミーティング番号を同時に別々のインスタント会議に割り当てることが防止されます。

C：表 3-17　インスタント会議用の SIP トランク設定

設定	値	コメント
名前	SIP_TRUNK_CMS1	Call Bridge が有効になっている Cisco Meeting Server ノード 1 を指し示す SIP トランクの名前
[説明（Description）]		わかりやすい説明
[デバイスプール（Device Pool）]	[Trunks_and_Apps]	中央トランクの共通デバイス プール
[メディアリソースグループリスト（Media Resource Group List）]	< なし >	デバイス プールで定義された MRGL を使用する
[AAR グループ（AAR Group）]	[デフォルト（Default）]	すべての場所で同じ
[発呼側名に UTF-8 を転送（Transmit UTF-8 for Calling Party Name）]	オン	この設定によって、ASCII 呼び出し表示を、UTF-8 文字をサポートするデバイスに転送できます。
[PSTN アクセス（PSTN Access）]	オフ	
[すべてのアクティブな Unified CM ノードで実行（Run on All Active Unified CM Nodes）]	オン	すべての SIP トランクで、この設定が推奨されています。この設定によって、SIP への発信コールは、Unified CM コール処理サブスクライバ間のクラスタ内制御シグナリングを必要としなくなります。

C：表 3-17　インスタント会議用の SIP トランク設定（続き）

設定	値	コメント
着信コール		
[コーリングサーチスペース（Calling Search Space）]	[TelePresenceConferencing]	コール制御の章で定義されているとおり
[AAR コーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	
[アウトバウンドコール（Outbound Calls）]		
[デバイスプールの着信側トランスフォーメーション CSS を使用（Use Device Pool Called Party Transformation CSS）]	オン	
[デバイスプールの発呼側トランスフォーメーション CSS を使用（Use Device Pool Calling Party Transformation CSS）]	オン	
[SIP 情報（SIP Information）]		
接続先	us-cms1.ent-pa.com	Cisco Meeting Server ノード 1 の FQDN
[SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）]	CMS のセキュリティ SIP トランク プロファイル	上記で作成した SIP トランク セキュリティ プロファイルを使用します。
再ルーティング用コーリング サーチスペース（Rerouting Calling Search Space）	TelePresenceConferencing	上記で着信コールに関して設定したものと同じコーリング サーチ スペースを使用します。
[SIP プロファイル（SIP Profile）]	CMS の標準 SIP プロファイル	上記で作成した SIP プロファイルを使用します。

すべての会議ブリッジを設定したら、それらをメディア リソース グループ（MRG）に追加できます。各メディア リソース グループでは、1 つの Call Bridge ノードが通信不能になった場合にコールを別のノードにルーティングできるように、Cisco Meeting Server ノード内の各 Call Bridge から 1 つの会議ブリッジを含める必要があります。

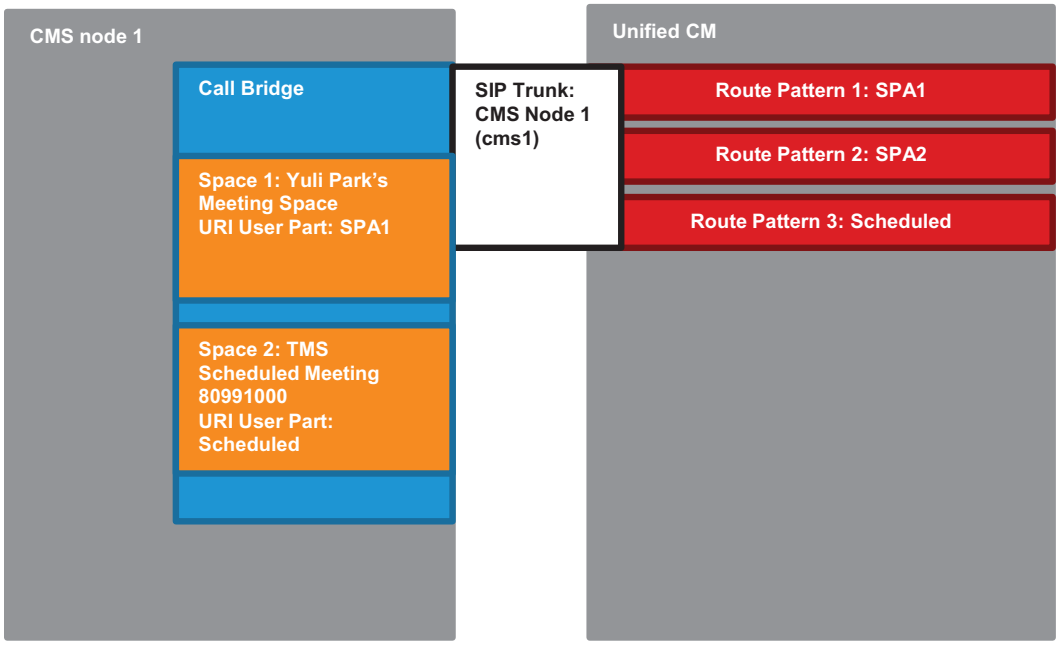
各メディア リソース グループは、独自のメディア リソース グループ リスト（MRGL）に追加できます。メディア リソース グループ リストは、Unified CM 内のデバイスまたはデバイス プールに割り当てることができます。また、会議ボタンを使用して、ポイントツーポイント コールから会議コールにそれらのデバイスをエスカレートするときに使用できます。

Cisco Meeting Server 内部では、ユーザがデバイスで会議ボタンを押してエスカレーションを開始したときに、インスタント会議によって使用されるスペースが HTTPS API 接続を介して動的に作成されます。このスペースは、会議の終了後に、API 接続を介して削除されます。

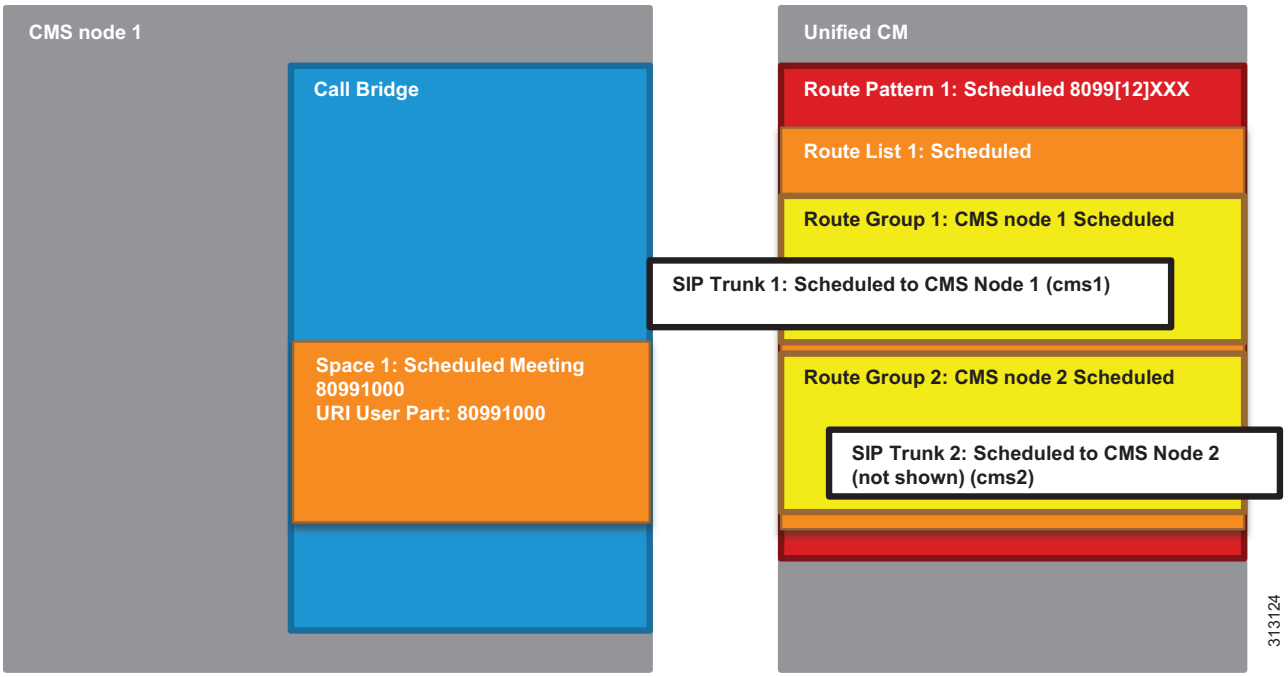
無期限会議とスケジュール済み会議用に Unified CM を有効にするための展開タスク

無期限会議とスケジュール済み会議は、インスタント会議と同様の方法で Unified CM で設定されますが、メディア リソースではなくダイヤル プランを設定する必要があります（C：図 3-15）。無期限会議およびスケジュール済み会議には、インスタント会議用に作成したものと同じ SIP トランクと SIP プロファイルを使用しますが、C：表 3-17 に示す設定値を使用します。

C：図 3-15　　Cisco Unified CM と Cisco Meeting Server スペースのスケジュール済み関係



C：図 3-16　無期限会議とスケジュール済み会議用の Cisco Unified CM の設定



インスタント会議用に作成されたすべての SIP トランク用のルート グループを作成します。ルート グループをルート リストの中に追加します。コールがそのルートを指すルート パターンに一致する場合に、ルート リストが選択されます。

SIP トランクを介して Cisco Meeting Server にコールをルーティングするには、ルート リスト用のルート パターンを設定します。ルート パターンは、C：表 3-18 に示すように、スケジュール済み会議用に設定されたエイリアス範囲と一致する必要があります。管理者が Cisco TMS でスケジュール済み会議の数値 ID 範囲を作成すると、スケジュール済み会議用のスペースが作成され、数値 ID ごとに 1 つのスペースが作成されます。詳細については、4. Cisco TelePresence Management Suite を展開するのセクションを参照してください。

C：表 3-18　スケジュール会議ルート リストのルート パターン

パターン	パーティション	ゲートウェイまたはルート リスト	説明
8099[12]XXX	ESN	RL_SPACE_SCHED	スケジュール済みエイリアス範囲と一致するパターン

Cisco Meeting Server の無期限会議用の展開とルート パターン設定の詳細については、5. Cisco Meeting Server スペースを展開するのセクションを参照してください。

概要

上記の展開タスクを完了すると、Unified CM が Cisco Meeting Server と通信できるようになります。

4. Cisco TelePresence Management Suite を展開する

このセクションでは、Cisco Meeting Server を使用したスケジュール済み会議用の Cisco TMS の展開タスクについて説明します。

概要

Cisco TMS の高適用性のための展開タスク：

1。 アクティブ ノードとパッシブ ノードで Cisco TMS をインストールして設定します。

2。 ネットワーク ロード バランサ（NLB）をインストールして設定します。

3。 アクティブ ノード サーバとパッシブ ノード サーバの間のファイル共有を設定します。

Cisco TMS の基本設定のための展開タスク：

4。 Active Directory 統合、グループ構造、およびユーザを設定します。

5。 TMS システム ナビゲータのフォルダ構造を作成します。

6。 デフォルトの会議設定を行います。

スケジュール済み会議用の Cisco TMS の展開タスク：

7。 Cisco Meeting Server と TMS を統合します。

8。 Unified CM と TMS を統合します。

9。 会議室エンドポイントを TMS に追加します。

10。TMS Extension for Microsoft Exchange（TMSXE）をインストールして設定します。

Cisco TMS の高適用性のための展開タスク

このセクションでは、高可用性を備えた Cisco TMS を展開するために必要なタスクについて説明します。

アクティブ ノードとパッシブ ノードでの Cisco TMS のインストールと設定

次の場所にある最新版『*Cisco TelePresence Management Suite Installation and Upgrade Guide*』のガイドラインに従って、冗長展開用に Cisco TelePresence Management Suite（TMS）をインストールする必要があります。

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-guides-list.html

- プライマリ サーバにこのアプリケーションをインストールします。
- 計画段階で設定した外部 SQL リソースを指し示します。
- 暗号化キーをメモしておきます。
- Web ポータルにログインして TMS 冗長性を有効にし、基本的な操作を検証します。
- 1 番目のサーバの暗号化キーを使用し、1 番目のサーバと同じ SQL クレデンシャルを使用して、2 番目のサーバにアプリケーションをインストールします。

両方のサーバが、すべての会議データと設定データが保存されている 1 つの SQL データベースにアクセスします。アクティブ ノード設定とパッシブ ノード設定で、1 つの暗号化キーと証明書が両方のサーバに対して使用されます。この暗号化キーと証明書をそれぞれのサーバに配置しておくと、エンドユーザから TMS への通信と、TMS から管理対象デバイスへの通信に、セキュア プロトコルを使用できるようになります。

ネットワーク ロード バランサ（NLB）のインストールと設定

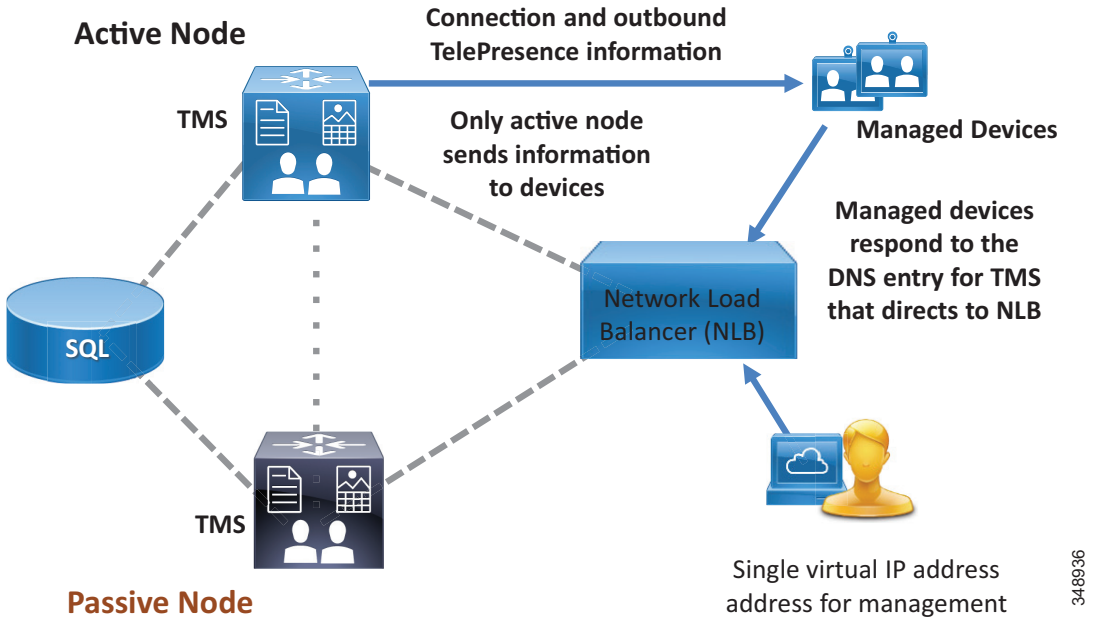
ネットワーク ロード負荷分散設定の詳細は、お客様が選ぶロード バランサの指示に応じて異なります。以下は、設定する必要がある機能要件です。

- HTTP、HTTPS、および SNMP トラフィックをアクティブ ノードに転送します。
- Cisco TMS 内で Probe URL へのネットワーク ロード バランサ プローブを設定します。
- すべてのトラフィックをアクティブ ノードにプッシュします。

Cisco TMS サーバは発信通信を管理対象デバイスに直接送信し、トラフィックを NLB 経由でルーティングしません。ただし、管理対象デバイスからのすべての戻り通信とすべての Web ポータル要求は、NLB 経由でルーティングされる必要があります。通信パスにより、エンドユーザとエンドポイントは、どの TMS サーバ ノードがアクティブ モードであるかに関係なく、1 つのアドレスを使用できます。

TMS ネットワーク設定を、ネットワーク ロード バランサで設定されている TMS アドレスの FQDN に設定します。TMS 内のこの設定によって、管理対象デバイスが TMS との通信を開始するときに使用するアドレスが生成されます。ロード バランサに解決される tms.ent-pa.com の FQDN を使用することで、エンドポイントまたはエンドユーザ Web クライアントからのすべての着信トラフィックが NLB を経由して送信され、アクティブ ノードに解決されます（C：図 3-17 を参照）。

C：図 3-17　　NLB による管理対象デバイスからアクティブ TMS ノードへの通信の指示



アクティブ ノード サーバとパッシブ ノード サーバの間のファイル共有の設定

すべての運用データは SQL データベースに保管されますが、一部のアプリケーション固有ファイルはホスト サーバのファイル ストラクチャ内に保存されます。これらのカスタマイズ可能なファイルは TMS アプリケーションにより追加され、冗長環境を使用する場合は 2 つのサーバ間でこれらのファイルを同期する必要があります。このようなファイルには、Cisco TMS にアップロード可能なソフトウェアおよびイメージ、Cisco TMS により作成されたイメージなどが含まれます。

デフォルトのインストール環境では、ファイルの場所は次のとおりです。

C:\Program Files\TANDBERG\TMS\Config\System\

C:\Program Files\TANDBERG\TMS\Data\GenericEndpoint\

C:\Program Files\TANDBERG\TMS\Data\SystemTemplate\

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\CompanyLogo\

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles\

C:\Program Files\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware\

Windows Server オペレーティング システムの分散ファイル システム（DFS）を使用して、2 つのサーバ間のレプリケーション プロセスを実行します。「フル メッシュ」設定が使用されている場合、DFS は 2 つのサーバ間でこれらのファイルを同期した状態で維持します。

Cisco TMS の基本設定のための展開タスク

プリファード アーキテクチャで意図されているとおりに導入環境が機能するようにするには、Cisco TMS のインストール中に次の追加設定タスクを実行します。

- Active Directory の統合、グループ構造、ユーザ
- システム ナビゲータ フォルダの構造
- デフォルトの会議設定
- デフォルトの会議設定
- TMS 内での電子メール テンプレートの変更

Active Directory の統合、グループ構造、ユーザ

Active Directory サービス アカウントのすべての情報が正しく入力されていることを確認します。

注　AD 接続のすべての設定が正しいことを確認し、接続をテストします。AD 同期が機能していない場合でも、TMS 内でその他の AD インターフェイス コマンドを実行すると、エラーが表示されないことがあります。

Active Directory Group を使用して、組織のニーズに対応するグループ構造を作成します。

デフォルトでは、TMS のインストール中に 3 種類のグループが作成されます。

- Users
- Video Unit Administrator
- Site Administrator

顧客のニーズに対応するようにこれらのグループを変更できますが、削除はできません。デフォルトでは、すべてのグループに Site Administrator と同じアクセス権限が付与されます。

これらのデフォルト グループでのユーザ エントリは手動入力に限定されているため、グループを Active Directory からインポートし、既存の Active Directory グループを使用して TMS 機能へのエンドユーザ アクセスを管理する必要があります。会議をスケジュールするエンドユーザ用のグループに加えて、サポート デスク担当者や技術管理者用のグループも必ず考慮してください。

グループに関する追加情報については、次の場所にある『*Cisco TelePresence Management Suite Administrator Guide*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html

[AD からインポート（Import from AD）] 機能を使用すると、エンドユーザの職務を一元的に管理できます。従業員を追加または削除するか、あるいは職務を変更して、組織的な Active Directory グループを変更すると、TMS 権限が自動的に更新されます。

Active Directory からグループをインポートしたら、各グループに適切な権限を割り当てます。表示される画面で、グループに設定しない権限をすべてオフにします。これらの権限を制限しないと、意図しない設定変更が発生する可能性があります。

また、すべてのユーザに対して適切なデフォルト グループを選択してください。

注　Cisco CMS にアクセスできるすべてのユーザは自動的に Users グループに追加されます。このグループをオフにすることはできません。管理者が組織内のすべてのユーザに対して付与しない権限があれば、それらをすべて選択解除します。

ユーザのインポート

グループの権限が設定されたら、[すべてのユーザを AD と同期する（Synchronize All Users with AD）] 機能を使用してユーザをインポートします。組織の規模と関連するグループの数に応じて、同期が完了するまでに長時間かかることがあります。

注　ユーザは、初めて TMS にログインするまではユーザ リストに表示されません。

システム ナビゲータ フォルダの構造

TMS システム ナビゲータは、フォルダ構造を使用して管理者のためにデバイスを論理的にグループ化します。組織の物理的な環境に対応したフォルダ構造を作成します。これらのフォルダは管理者に対してだけ表示され、エンドユーザに対しては表示されません。組織の論理フローに基づいてフォルダを配置します。たとえば、地域ごとに 1 つのフォルダを作成し、続いてインフラスストラクチャのサブフォルダと会議室エンドポイントのための別のフォルダを作成します。システム ナビゲータ内のフォルダには、TMS から接続の指示を受信するインフラストラクチャ デバイスまたはエンドポイント、あるいはこの両方を含めることができます。

デフォルトの会議設定

会議をスケジュールする前に、管理者はエンドユーザ コミュニティの使用モデルと、エンドポイントの制限について理解しておく必要があります。検討すべき重要な Cisco TMS 設定には、次のものがあります。

- ワンボタン機能
- 帯域幅
- 参加者に対し 5 分前の接続を許可する

ワンボタン機能

ワンボタン機能により、エンドユーザは特定のルームで開催される当日の会議をカレンダーで確認し、会議への接続を開始できます。Cisco TMS はユーザに対し、1 要求あたり 72 時間分のカレンダー情報を提供します。

帯域幅

この設定はエンドポイントごとに行います。ネットワークに必要な設定にあわせて帯域幅を調整してください。コンテンツの HD メインチャネルと最大解像度を可能にするには、非ルームシステムのビデオデバイスのデフォルト帯域幅を 2048 kbps に設定する必要があります。最大帯域幅にこれよりも低い値が設定されているエンドポイントはすべて、その最大帯域幅で接続します。

参加者に対し 5 分前の接続を許可する

エンドユーザの時間インターフェイスで多少の差異を許可するには、この設定を選択します。TMS サーバでの正確な時刻よりも前にユーザが接続できるようにすることで、より一貫性のあるエンドユーザ エクスペリエンスを提供し、また会議開始時刻の数分前にエンドユーザが会議に接続しようとしたときに「接続できない」というメッセージが表示されなくなります。

TMS 内での電子メール テンプレートの変更

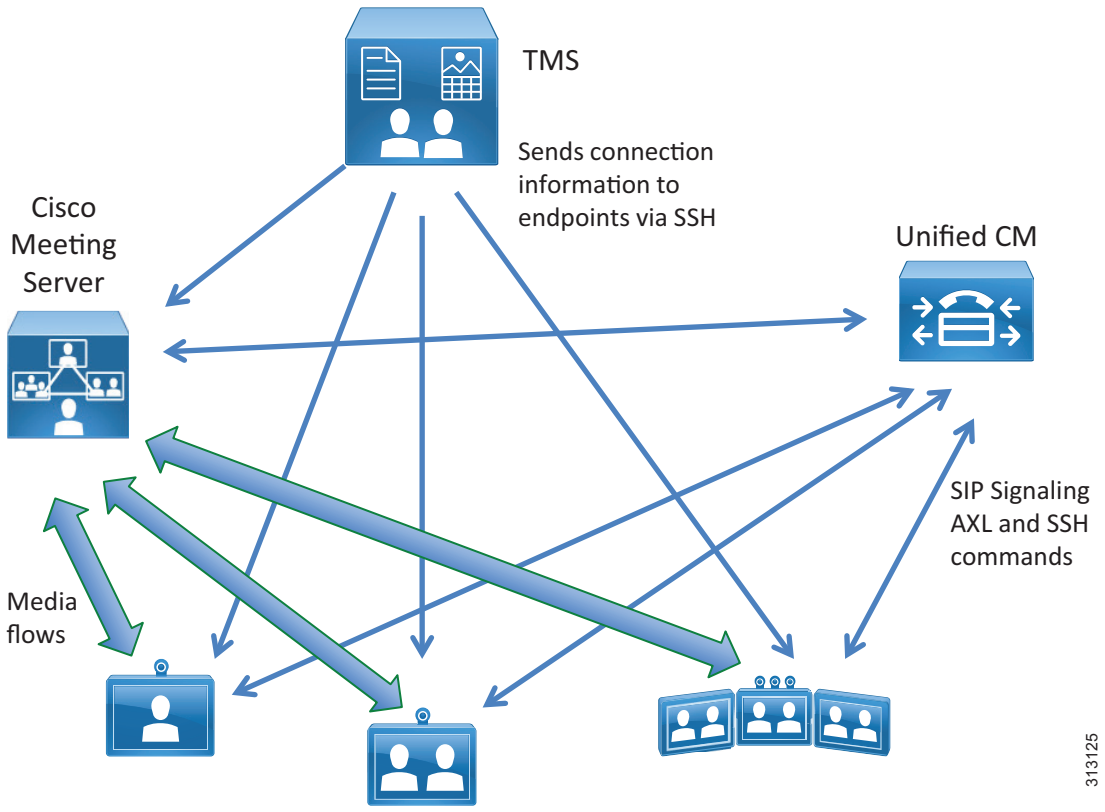
Cisco TMS には、会議主催者への通知に使用できるテンプレートがあります。ただし Cisco TMSXE では、Cisco TMS が送信する電子メールのメッセージにエラー、警告、および情報テキストが挿入されることがあります。管理者はこれらのメッセージを変更できます。{MEETING_TITLE}、{CONTACT_HOST} のように中カッコで囲まれたテキストは、スケジュール済みイベントの特定のコンテンツを組み込む変数であるため、これらのテキストを削除または変更しないようにしてください。

すべての電子メール テンプレートで、TMS により自動生成される通信内容が目的の手続きに対応していることを確認します。多くのテンプレートはシンプルに作られており、各組織がテンプレートを拡張することを前提としています。また、テンプレートは標準 HTML エディタを使用して変更できます。

スケジュール済み会議用の Cisco TMS の展開タスク

Cisco TMS がスケジュール済み会議を作成できるようにするため、必要なコンポーネントを TMS にシステムとして追加する必要があります。TMS スケジューリング メカニズムがすべてのデバイスのコール制御エンティティを認識できるようにするため、Unified CM が TMS に追加されます。TMS は Unified CM の設定を制御しませんが、Unified CM が管理する会議室のエンドポイントと直接通信します。（C：図 3-18 を参照）。

C：図 3-18　　Cisco TMS と Unified CM 管理対象エンドポイントの直接通信



Cisco Meeting Server と Cisco TMS の統合

Cisco TMS でスケジュール済み会議のスケジューリングと会議制御を可能にするには、各 Cisco Meeting Server クラスタから 1 つの Cisco Meeting Server ノードを追加します。

特定の範囲の数値 ID を使って Cisco TMS を設定する必要があります。これらの ID は、スケジュール済みコールの配置場所を決定するために Cisco TMS で使用されます。

各 Cisco Meeting Server クラスタから 1 つの Cisco Meeting Server を Cisco TMS に追加します。それらを該当するフォルダに追加します。その際、Cisco Meeting Server で設定された管理者アカウントを使用します。Cisco TMS で設定された TelePresence Conductor ごとに、C：表 3-19 に示すパラメータを設定します。

C：表 3-19　Cisco Meeting Server 用の Cisco TMS パラメータの設定

設定	値	コメント
[IP アドレス（IP Address）]	10.X.X.2:445	Cisco Meeting Server Web 管理インターフェイスの IP アドレスとポート番号
[ユーザ名（Username）]	[TMSadmin]	この設定は、Cisco Meeting Server で設定されたユーザ名と一致する必要がある
[パスワード（Password）]	< パスワード >	
[使用タイプ（Usage Type）]	[その他（Other）]	

Cisco Meeting Server を追加した後、C：表 3-20 に示すように、Cisco Meeting Server 設定の中で代替 IP ネットワーク設定を指定します。最初の Cisco Meeting Server で障害が発生すると、代替 IP Cisco Meeting Server が操作を引き継ぎます。

C：表 3-20　Cisco Meeting Server 用の代替 IP ネットワーク設定

設定	値	コメント
[代替 IP（Alternate IP）]	< *ドロップダウンで 1 つ選択* >	Call Bridge が有効になっている Cisco Meeting Server クラスタ ノード
[代替 IP ユーザ名（Alternate IP Username）]	[TMSadmin]	代替 IP アドレスで指定された IP アドレスを持つ Cisco Meeting Server で設定されたユーザ
[パスワード（Password）]	< *パスワード* >	

会議エイリアスを設定し、ダイヤル プランの一環として Cisco Meeting Server で使用する、SIP トランクで指定される数値範囲を特定します。C：表 3-21 は、スケジュールされたコール用の数値 ID 範囲を指定するための Cisco Meeting Server の拡張設定を示しています。

C：表 3-21　Cisco Meeting Server の拡張設定

パラメータ	値
[ドメイン（Domain）]	Cisco Meeting Server に関連付けられたドメイン。
[数字 ID ベース（Numeric ID Base）]	これは、ダイヤル プランのスケジュール会議範囲の 1 番目の数字です。
[数字 ID の桁数（Numeric ID Quantity）]	スケジュール済み会議に必要な数値 ID の数を指定します。

Cisco Meeting Server を追加するための設定を保存します。数値 ID ごとに、Cisco TMS は、Cisco Meeting Server 上の URI ユーザ部分として数値 ID を使って非アクティブ スペースを作成します。これらのスペースは、Cisco TMS で作成されるスケジュール済み会議をホストするために使用されます。スケジュール済み会議を開始する時間になると、Cisco TMS は Cisco Meeting Server 上のスペースをアクティブにして、参加者がコールインを開始できるようになります。

Cisco TMS は、E.164 エイリアスと SIP URI の両方に、前述のステップで指定したダイヤル プランの数値を取り込みます。ただし TMS 内での E.164 ロジックの実装は、プリファード アーキテクチャのその他の場所での E.164 の使用方法とは異なります。TMS は E.164 エイリアスを H.323 通信だけに関連付けます。したがって、Cisco Meeting Server の特定の警告を無視するように TMS の統合チケット システムを調整する必要があります。

Cisco Meeting Server が TMS に追加されたら、[ゲートキーパーモードオフ（Gatekeeper Mode Off）] 用のフィルタを追加することにより、このエントリのチケット フィルタを調整します。

スケジュールされたコールに Cisco Meeting Server を使用するには、Cisco TMS 内の Cisco Meeting Server 設定を編集する必要があります。H.323 ダイヤルは両方向で無効、[予約の許可（Allow booking）] は有効、SIP ダイヤルは両方向で有効にする必要があります。

使用する数値 ID 範囲を設定する際には、スケジュール済み会議の番号範囲が Unified CM で設定されたものと一致するようにする必要があります。C：表 3-22 に示すように、Cisco TMS 内で Cisco Meeting Server の拡張設定を編集します。ドメインは、Cisco Meeting Server で設定された XMPP ドメインと一致する必要があります。数値 ID は、Unified CM から Cisco Meeting Server へのトランク用に設定されたルート パターンと一致する必要があります。

C：表 3-22　Cisco Meeting Server の拡張設定

設定	値	コメント
ドメイン（Domain）	cms.ent-pa.com	スケジュール済み会議の SIP URI ドメイン
[数字 ID ベース（Numeric ID Base）]	80991000	スケジュール済み会議にダイヤルインする参加者によって使われるダイヤル文字列を形成するために Cisco TMS で使用する最初の番号（80991000 など）。
[数字 ID の桁数（Numeric ID Quantity）]	1999	Cisco TMS が [数字 ID ベース（Numeric ID Base）] からの数値を増やす回数。この数値は、最大値がスケジュールに割り当てられた範囲を超えないように設定する必要があります（80991000 ～ 80992999）。

スケジューリングに Cisco Meeting Server を使用するように Cisco TMS を設定することが重要です。そうしなければ、スケジューリングが失敗します。[管理ツール（Administrative Tools）] > [設定（Configuration）] > [会議設定（Conference Settings）] で、C：表 3-23 に示されているように設定を編集します。

C：表 3-23　Cisco TMS Conference 設定

設定	値	コメント
[ルーティングの優先 MCU タイプ（Preferred MCU Type in Routing）]	Cisco Meeting Server	スケジューリングに関して、他のデバイスより Cisco Meeting Server を優先する

Unified CM と TMS の統合

Unified CM はその他のすべての設定および管理の面で会議室のエンドポイントを管理しますが、予約と接続開始を実行できるようにするため、Unified CM クラスタを TMS に追加する必要があります。Unified CM を TMS に追加するには、次のタスクを実行します。

- Unified CM 内での Cisco TMS のアプリケーション ユーザの作成
- ご使用の環境での各 Unified CM クラスタのパブリッシャの追加

複数の Unified CM クラスタを追加する場合は、コール制御の章で説明するダイヤル プラン設定に準拠する必要があります。

Unified CM 内での Cisco TMS のアプリケーション ユーザの作成

このアプリケーション ユーザにより、Unified CM が制御するエンドポイントと TMS が通信できるようになります。このユーザには、Unified CM 内のスケジュール対象の会議室デバイスすべてを割り当てる必要があります。また、次のロールが設定されている Cisco TMS 専用のユーザ グループにこのユーザを追加する必要もあります。

- Standard AXL API Access
- Standard CTI Enabled
- Standard SERVICEABILITY
- Standard CCM Admin Users
- 標準 RealtimeAndTraceCollection

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

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

ご使用の環境での各 Unified CM クラスタのパブリッシャの追加

Unified CM パブリッシャを TMS に追加すると、TMS はそのエンドポイントのコール制御権限を認識します。Unified CM を認識しない場合、TMS スケジューリング エンジンは導入環境の全機能を利用できず、接続が失敗することがあります。

他のデバイスの場合と同じ方法でパブリッシャを追加します。TMS から入力を求められたときのユーザ名およびパスワードとして、上記ステップで作成したアプリケーション ユーザを使用します。

TMS への会議室エンドポイントの追加

IP アドレスまたは DNS 名でデバイスを追加する代わりに、[リストから（From List）] タブを使用して、Unified CM を選択します。TMS のスケジューリング インターフェイスから使用できるようにする会議室の TelePresence デバイスをすべて選択します。Unified CM の各エンドポイントの DN が、コール制御 の章に記載されている E.164 ガイドラインに準拠していることを確認します。

TMS Extension for Microsoft Exchange のインストールと設定

Cisco TelePresence Management Suite Extension for Microsoft Exchange（Cisco TMSXE）は、Microsoft Outlook からビデオ会議のスケジュールを可能にする Cisco TelePresence Management Suite の拡張機能であり、Cisco TMS 会議を Outlook の会議室予定表にレプリケートします。

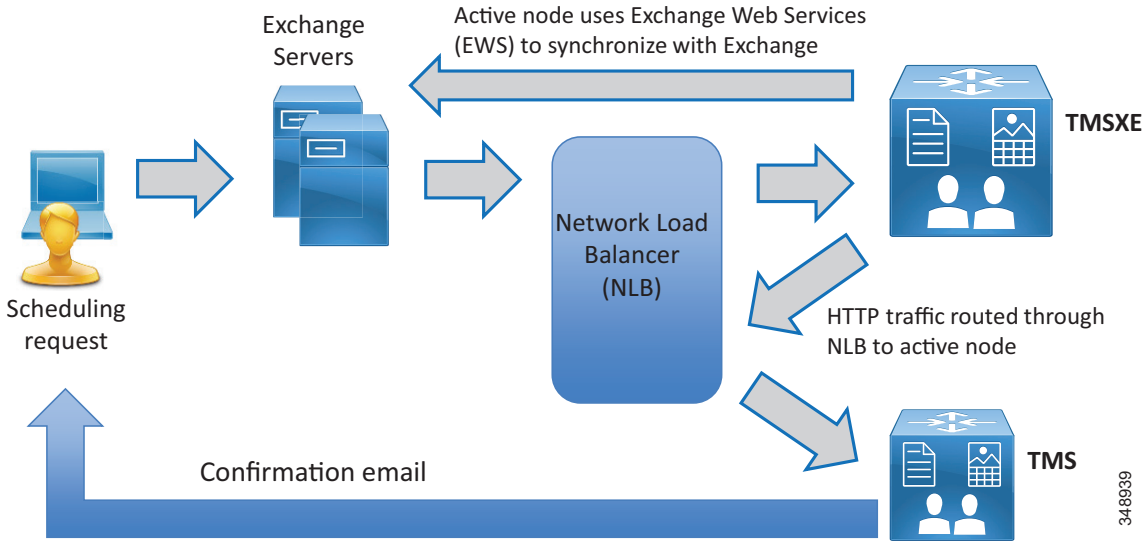
この TMS ソフトウェア拡張機能を使用するには、TMS 内で機能を有効にするためのライセンス キーが必要です。TMSXE ソフトウェアのインストール前に、このキーを TMS にインストールしておく必要があります。スケジュールされるエンドポイントの数が 50 を超える導入環境では、TMSXE を専用のサーバまたは仮想マシン インスタンスにインストールする必要があります。

前提条件

Cisco TMSXE をインストールする前に、Outlook と Exchange がすでにセットアップされており、ユーザがルーム メールボックスを含む会議を予約できることを確認してください（C：図 3-19 を参照）。この統合は、エンドポイント グループによりライセンスされるか、または Application Integration ライセンス キーとしてライセンスされます。インストールを続行する前に、正しいキーを作成し、TMS に入力する必要があります。両方のオプション キーを追加した場合、Cisco TMS は Application Integration Package オプションのみを使用します。

Cisco TMSXE が使用できる Microsoft Exchange リソースは、オンプレミス、Office 365 ホスティング導入環境、または顧客のハイブリッド導入環境のいずれかです。お客様の特定の環境に適用される可能性のある推奨事項またはガイドラインについては、Microsoft Exchange の管理と導入に関する資料を参照してください。

C：図 3-19　　エンドユーザによる会議のスケジュール フローの例



システム別のオプション キーを Cisco TMS で有効化したら、[リモート予約を許可する（Allow Remote Bookings）] 設定により、各システムがライセンスを使用するかどうかが決定します。この設定により、エンドユーザが予約でき、個別のエンドポイント ライセンスの 1 つを使用できるエンドポイントを管理者が選択できます。Application Integration Package オプションを使用する場合は、この設定は無効であり非表示になります。

Cisco TMSXE にエンドポイントを追加するには、その前に、Exchange でこれらのエンドポイントがルーム メールボックスによって示されている必要があります。TMSXE のセットアップを簡素化するため、エンドポイントの Cisco TMS 表示名をメールボックス名として使用することを推奨します（スペースはすべて削除してください）。これにより、エンドユーザに対するシステム名の表示方法すべてで統一が図られます。

Exchange のプライバシー機能に関する特別な注意事項

Cisco TMSXE に追加されるすべてのルーム メールボックスが、予約件名とプライバシー設定を同一の方法で処理するように設定されている必要があります。つまり、以下の設定をすべてのメールボックスに適用するか、またはどのメールボックスにも適用しないかのいずれかになります。

- [件名の削除（Delete the subject）]

  サポート担当者が会議制御センターで特定の会議を識別できるようにするため、この機能を使用しないことを推奨します。また、これにより会議のタイトルが対応エンドポイントの One Button to Push インターフェイスに表示されるようになります。

- [開催者名を件名に追加する（Add the organizer's name to the subject）]

  この設定を使用する際には十分に注意し、組織の慣習に基づいて使用してください。あるユーザが複数グループの会議をスケジュールすると、スケジュールされた会議は会議の件名ではなくそのスケジュール担当者のユーザ名でリストされることに注意してください。会議

の件名の方が便利である可能性があります。一方、会議がそれぞれ該当する主催者によってスケジュールされる場合、特定の会議の件名を覚えておくよりも、「ボブの会議」と確認できる方が容易なことがあります。ほとんどの組織ではこの設定を使用しないことを推奨します。

- [承諾した会議に設定されたプライベートフラグを削除する（Remove the private flag on an accepted meeting）]

  「プライベート」フラグは Outlook クライアント内では反映されますが、Cisco TMS ではサポートされていないため、会議の議題は以下の場所で制限なしで表示されます。

  - Cisco TMS 内
  - 組織内で件名を公開すべきではない会議に使用する会議室を、他の担当者も使用している場合は、会議室予定表をサポートしているエンドポイント。（たとえば、最高責任者による「合併会議」がスケジュールされている会議室を使用する、保留中の合併について知る必要がない下位レベルの従業員に対し、会議室システム予定表にこの会議が表示されることがあります。）
  - Exchange で「プライベート」フラグが設定されている予約の参加者または定例会議パターンが Cisco TMS で変更されると、この変更が Exchange にレプリケートされる時点で「プライベート」フラグが削除されます。

TMSXE ユーザの作成

- Active Directory で TMSXE ユーザを作成し、TMS にインポートします。
- TMS では、[予約（Booking）] の下で次の権限が有効な既存のグループまたは新規のグループにこのユーザが属している必要があります。
  - [読み取り（Read）]
  - [更新（Update）]
  - [代理予約（Book on Behalf of）]
  - [会議承認（Approve Meeting）]

証明書のインストール

Cisco TMSXE と TMS の通信には HTTPS が使用されます。TMSXE サーバと Exchange 環境間のセキュア通信は証明書でも可能です。TMS アプリケーション サーバと同様に、TMSXE のアクティブ ノードとパッシブ ノードの両方に同じ証明書がロードされ、証明書の DNS 項目は TMSXE に使用されるネットワーク ロード バランサのアドレスの項目を指し示します。

ソフトウェア インストーラの実行

- TMS Booking Service を選択します。
- アクティブ ノードまたはパッシブ ノードに適切な冗長性オプションを選択します。
- アクティブ ノードとパッシブ ノードの両方でソフトウェア インストールを実行します。

アクティブ ノードとパッシブ ノードの両方でインストールが完了したら、各ノードのプローブ URL を使用してネットワーク ロード バランサを設定します。

Cisco TMSXE の設定

- Cisco TMS 接続情報

  TMSXE アプリケーションが TMS アプリケーションと通信できるようにするため、Active Directory で作成した TMSXE アカウントを使用して TMS 接続情報を設定します。

- Exchange Web Services の設定

  ユーザとリソース メールボックスのために TMSXE が Exchange サーバと通信できるように Exchange Web Services（EWS）を設定します。この接続に使用するクレデンシャルは、他の場所で使用されるものと同じ TMSXE クレデンシャルです。

- Exchange と TMS リソースの調整

  TMS システム ID に合わせて Exchange リソースを調整します。この操作を個別に行うことも、あるいは次の場所にある『*Cisco TelePresence Management Suite Extension for Microsoft Exchange Deployment Guide*』の最新版に記載されている .csv ファイルを使用することもできます。

  https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/products-installation-guides-list.html

概要

上記の展開タスクを完了すると、スケジュール済み会議用の Cisco Meeting Server と通信するように Cisco TMS が設定されます。

5. Cisco Meeting Server スペースを展開する

このセクションでは、Cisco Collaboration Meeting スペースを展開するために必要な主なタスクについて説明します。

概要

Cisco Meeting Server 常設会議用の統一された CM の展開タスク：

1. Unified CM と Cisco Meeting Server の間の Early Offer SIP トランクを設定します。以前に設定した SIP トランク SIP_TRUNK_CMS1 をここで使用することができます。
2. 関連するトランクを含むルート リストを指し示すスペース数字エイリアス用の新しいルート パターンをセットアップします。以前に設定したルート リスト RL_SPACE_SCHED をここで使用することができます。
3. タスク 2 で使用したルート リスト（RL_SPACE_SCHED）を指し示すスペース URI 用の SIP ルート パターンを作成します。

スペースを作成するための Cisco Meeting Server の展開タスク：

4. ユーザ プロファイルを作成し、マルチパーティ ランセンスをユーザに割り当てます。
5. LDAP からユーザをインポートし、スペースを作成します。
6. 着信コールを処理するダイヤル プラン ルールを作成します。

展開の考慮事項

Cisco Meeting Server スペースは、企業のデータセンターに配置された TelePresence インフラストラクチャで作成される無期限会議に似ています。各スペースには、会議を開始するためにユーザがいつでも発信できるビデオ アドレスの固有のセットが存在します。これらのビデオ アドレスは、数字エイリアスまたは SIP URI の形式で指定できます。各スペースを個別ユーザに関連付け、LDAP ユーザ同期を介して作成することができます。

Cisco Meeting Server スペースは、居場所に関係なく、参加者が会議に参加するための簡単な方法を提供します。すべてのユーザは、ラップトップ、テレプレゼンス会議室、デスクトップ エンドポイント、またはモバイルデバイスから同じ仮想会議室にダイヤルします。

スペースを展開するには、Unified CM と Cisco Meeting Server の展開が必要です。以降のセクションでは、スペースの各コンポーネントの展開に関するプロセスの概要を説明します。

Tip　スペースを展開する前に、会議エイリアスの形式（数字または SIP URI）を決定します。

Cisco Meeting Server 常設会議用の統一された CM の展開タスク

Unified CM の主な機能は、Cisco Meeting Server との間のコール ルーティングを処理することです。Early Offer 用に有効にされた SIP トランクを使用して、Unified CM を Cisco Meeting Server に接続します（以前にスケジュール済み会議用に設定したものと同じトランク SIP_TRUNK_CMS1 を使用します）。ユーザがスペース エイリアスにダイヤルすると、コールは SIP トランクを介して Cisco Meeting Server 上の Call Bridge に送信されます。同様に、Cisco Meeting Server は、自動ダイヤル参加者用の SIP トランクを介して Unified CM にコールを送信できます。会議エイリアスには、2 つの形式（SIP URI と数字）があります。ダイヤル プラン設計には、スペースの数字エイリアスと SIP URI の両方のコール ルーティングを含める必要があります。ダイヤル プラン設計の詳細については、コール制御の章を参照してください。

Cisco Meeting Server スペースを個別のユーザごとに作成でき、ユーザの DID 番号に基づくスペース数字エイリアスにすることができます。C：表 3-24 は、コール制御の章のダイヤル プラン例を使用した展開用のスペース数字エイリアス範囲を示しています。

C：表 3-24　スペース数字エイリアスの範囲

サイト	+E.164 DID 範囲	スペース数字エイリアスの範囲
SJC	+1 408 555 4XXX	8-004-4XXX
RTP	+1 919-555 1XXX	8-005-1XXX
RCD	+1 972 555 5XXX	8-006-5XXX

数字エイリアスでは、C：表 3-25 に示すように、無期限会議用の Cisco Meeting Server ルート リストにルーティングする各サイトのルート パターンを設定します。

C：表 3-25　スペース数字エイリアスのルート パターン設定

パターン	パーティション	ゲートウェイまたは ルート リスト	説明
80044XXX	ESN	RL_SPACE_SCHED	SJC DID 範囲に一致するパターン
80051XXX	ESN	RL_SPACE_SCHED	RTP DID 範囲に一致するパターン
80065XXX	ESN	RL_SPACE_SCHED	RCD DID 範囲に一致するパターン

SIP URI では、ドメイン部分として XMPP ドメインを使用します。このドキュメントで設定する XMPP ドメインは cms.ent-pa.com です。たとえば、参加者は **<*username*>.space@cms.ent-pa.com** にダイヤルして Cisco Meeting Server 上の会議に参加することができます。また、Cisco Meeting アプリのユーザは、統一された CM 登録デバイスなどから、たとえば **<** *ユーザ名* **>@cms.ent-pa.com** にダイヤルすることによっても到達できます。

Unified CM は、XMPP ドメインに関するすべてのコールを Cisco Meeting Server に送ります。C：表 3-26 に示すように、無期限会議用の Cisco Meeting Server ルート リストにコールをルーティングする Cisco Meeting Server XMPP ドメインを含むドメイン ルーティング SIP ルート パターンを設定します。

C：表 3-26　スペース URI 用の SIP ルート パターンの設定

パターン	パーティション	ゲートウェイまたはルート リスト
cms.ent-pa.com	URI	RL_SPACE_SCHED

スペースを作成するための Cisco Meeting Server の展開タスク

注　このセクション内のタスクは、REST API を実行するためのツール（Postman など）と Cisco Meeting Server API を使用して展開されます。API の詳細については、https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html にある『*Cisco Meeting Server API Reference Guide*』の最新版を参照してください。

Cisco Meeting Server で会議をホストするには、その前にマルチパーティ ランセンスを適用する必要があります。Personal Multiparty Plus（PMP+）が必要な場合は、ユーザごとにライセンスを付与する必要があります。PMP+ を割り当てるには、hasLicense フィールドが **true** に設定されたユーザ プロファイル オブジェクトにユーザを関連付ける必要があります。HasLicense フィールドが **false** の場合またはユーザ プロファイル オブジェクト内に存在しない場合は、ユーザがライセンスを持っていないため、Shared Multiparty Plus（SMP+）が使用されます。ユーザ プロファイルは、ユーザの機能を指定します。API を使用して、C：表 3-27 に示すパラメータを使って userProfile オブジェクト（POST /userProfiles）を作成し、hasLicense フィールドを **true** に設定します。

C：表 3-27　userProfile オブジェクトのパラメータ

パラメータ	値	説明
hasLicense	true	Personal Multiparty ライセンスを使用する
canReceiveCall	true	Cisco ミーティング アプリのユーザにコールの受信を許可する

Cisco Meeting Server 内のすべてのユーザは LDAP ディレクトリに存在します。（以前に作成した）ユーザ プロファイル オブジェクトをパラメータの 1 つとして使用し、ディレクトリから Cisco Meeting Server にユーザを同期する必要があり、インポートされたすべてのユーザはそのユーザ プロファイルに関連付けられます。ユーザ同期プロセスを作成するには ldapServers、ldapMappings、および ldapSources オブジェクトが必要です。

ldapServers は、サーバにアクセスするための場所、クレデンシャル、その他の属性を指定します。C：表 3-28 に示すパラメータを使用して、ldapServers オブジェクト（POST /ldapServers）を作成します。

C：表 3-28　ldapServers オブジェクトのパラメーター

パラメータ	値の例	説明
address	10.192.168.10	ディレクトリの IP アドレスまたは FQDN
portNumber	636	ディレクトリによって使用されるポート番号
username	ent-pa\tmssvc	ディレクトリにアクセスするためのユーザ名

C：表 3-28　ldapServers オブジェクトのパラメーター（続き）

パラメータ	値の例	説明
password	< パスワード>	ユーザ名に関連付けられたアカウントのパスワード
secure	true	ディレクトリ アクセスにセキュア接続を使用する

ldapMappings ではスペースに関する属性（名前、ユーザ名、URI など）を指定できます。これらの属性は、Microsoft Active Directory からの属性に基づいて作成できます（C：表 3-29 を参照）。C：表 3-29 に示すパラメータを使用して、ldapMappings オブジェクト（POST /ldapMappings）を作成します。

C：表 3-29　ldapMappings オブジェクトのパラメータ

パラメータ	値の例	説明
nameMapping	$displayName$	表示名
jidMapping	$sAMAccountName$@cms.ent-pa.com	XMPP ユーザ名
coSpaceNameMapping	$displayName$ のミーティング スペース	スペース名
coSpaceUriMapping	$sAMAccount$.space	スペース プライマリ URI
coSpaceSecondaryUriMapping	80044 $ telephoneNumber | '/. * ([[:d igit:]] {3}) $/\ 1/' $	スペース セカンダリ URI

スペース セカンダリ URI のプレフィックスはサイトによって異なり、最後の 3 桁がユーザの DID 番号から抽出されることに注意してください。コール制御 の章のダイヤル プラン例に従うと、SJC サイトにはプレフィックス 80044、RTP サイトにはプレフィックス 80051、RCD サイトにはプレフィックス 80065 がそれぞれ付加されます。したがって、ldapMappings オブジェクトはサイトごとに 1 回ずつ、合計 3 回作成されます。

C：表 3-29 のマッピングを使用してユーザをインポートすると、ユーザに *<username>***@cms.ent-pa.com** というユーザ名が付きます。Cisco ミーティング アプリにサインインするときにこれを使用できます。ユーザに、プライマリ URI *<username>***.space@***<domain>* とセカンダリ URI **80044XXX@***<domain>* に関連付けられたスペースが割り当てられます。ドメインは、Cisco Meeting Server 内の着信コール用の呼一致表で設定されたドメイン名に基づきます（C：表 3-31 を参照）。

特定のユーザ グループを Cisco Meeting Server にインポートできるように、LDAP ソースを使用して LDAP サーバ、LDAP マッピング、ユーザ プロファイル、および LDAP フィルタが単一のソースに結合されます。C：表 3-30 に示すパラメータを使用して、ldapSources オブジェクト（POST /ldapSources）を作成します。

C：表 3-30　ldapSources オブジェクトのパラメータ

パラメータ	値の例	説明
server	*<ldapServers id>*	ldapServers オブジェクト ID
mapping	*<ldapMappings id>*	ldapMappings オブジェクト ID
userProfile	*<userProfile id>*	userProfile オブジェクト ID
baseDn	ou=enterprise,dc=ent-pa,dc=com	トップ レベル検索ベース
filter	memberof=cn=sjcgroup,ou,ou=enterprise,dc=ent-pa,dc=com	LDAP フィルタ

GET 操作を使用してオブジェクトの ID を取得できることに注意してください。たとえば、ldapMapping オブジェクトの ID を取得するには GET /ldapMappings を使用します。また、ユーザが属する Active Directory グループに基づいて各サイトのユーザがインポートされるように、サイトごとに異なるフィルタが存在します。たとえば、SJC ユーザは **sjcgroup** Active Directory グループに、RTP ユーザは **rtpgroup** Active Directory グループに、RCD ユーザは **rcdgroup** Active Directory グループに属する必要があります。そのため、サイト固有の ldapMapping とフィルタを使用して 3 つの ldapSource オブジェクトが作成されます。

すべての LDAP ソースが作成された後、ldapSyncs オブジェクト（POST /ldaySyncs）を使用して、ただちにユーザ同期を開始します。同期が完了したら、すべてのサイトのユーザと、インポートされたユーザごとのスペースが Cisco Meeting Server に作成されるはずです。

注　Cisco ミーティング アプリでユーザが手動でスペースを作成することも、API を使ってスペースを作成することもできます。

次に、Cisco Meeting Server で着信コールを処理するダイヤル プラン ルールを作成します。いずれかの Web 管理インターフェイスを参照し、C：表 3-31 の値を使用して、Web インターフェイス（[設定（Configuration）] -> [着信コール（Incoming Calls）]）で設定された着信コールの呼一致表にドメインを追加します。ドメインは、XMPP ドメイン（cms.ent-pa.com）、トップ レベル ドメイン（ent pa.com）、およびすべての Call Bridge の FQDN および IP アドレス（us-cms1.ent-pa.com と cms2.ent-pa.com）です。

C：表 3-31　着信コール処理の設定

ドメイン名	プライオリティ	スペースを対象とする	ユーザを対象とする	IVR を対象とする	Lync を対象とする
cms.ent-pa.com	100	はい	はい	はい	いいえ（No）
ent-pa.com	100	はい	いいえ（No）	はい	いいえ（No）
us-cms1.ent-pa.com	100	はい	いいえ（No）	いいえ（No）	いいえ（No）
us-cms2.ent-pa.com	100	はい	いいえ（No）	いいえ（No）	いいえ（No）
10.x.x.60	100	はい	いいえ（No）	はい	いいえ（No）
10.x.x.61	100	はい	いいえ（No）	はい	いいえ（No）

XMPP ドメイン（cms.ent pa.com）にダイヤルされるすべての SIP URI コールは、スペース宛てまたは Cisco ミーティング アプリ ユーザ宛てです。数字ダイヤリングを使用してスペースを呼び出すユーザは、トップレベルドメインまたはコールブリッジ FQDN あるいは IP アドレスのルールにヒットします。数字ダイヤリングを使用した場合、Cisco ミーティング アプリのユーザには到達できません。

概要

上記の展開タスクを完了すると、ユーザは Cisco ミーティング アプリを使用してスペースにサインインし、PIN を指定したり、メンバーを追加したり、その他の環境設定をカスタマイズしたりできます。ユーザは SIP URI または数字エイリアスをダイヤルして会議を開始できます。

6. Cisco Meeting Management の展開

このセクションでは、Cisco Meeting Management スペースを展開するために主な展開タスクについて説明します。

概要

Cisco Meeting Management の展開タスク：

1。 ワンタイムパスワードを使用して、初回セットアップを実行し、Cisco Meeting 管理ポータルにログインします。

2。 ユーザ認証とグループ マッピングの LDAP セットアップを続行します。Cisco Meeting Server と同じディレクトリを使用します。

3。 CDR 受信者、Cisco TMS、および NTP アドレスを設定します。Cisco Meeting Server と TMS に同じ NTP を使用して、すべてのタイムスタンプが同期していることを確認します。

4。 Cisco Meeting Management に call bridge を追加します。

展開の考慮事項

Cisco Meeting Management は、ユーザ認証に LDAP ディレクトリを使用し、LDAP ディレクトリを通じてユーザ ロールを判別するユーザ グループをマッピングします。導入には少なくとも 2 つの LDAP ディレクトリグループが必要です。管理者用に 1 つのグループ（CMMAdmin など）と、ビデオオペレータ用に別のグループ（CMMOperator など）を作成します。次に、初期セットアップに進む前に、どのユーザがどのグループに所属するかを決定し、対応するグループにユーザを割り当てる必要があります。

Cisco Meeting Management の展開タスク

初期セットアップを開始し、ワンタイムパスワードを使用して初めて Cisco Meeting Management ポータルにログインするステップまで、続行します。初期セットアップの詳細については、以下で提供される最新バージョンの *Cisco Meeting Management インストレーションおよび設定ガイド*を参照してください。

https://www.cisco.com/c/en/us/support/conferencing/meeting-management/products-installation-guides-list.html

Cisco Meeting Management のすべてのユーザは、会議管理がユーザ認証の判別に使用する LDAP ディレクトリに所属します。したがって、ポータルに初めてログインした後、C：表 3-32 の値を使用して LDAP サーバ、ユーザ検索ベース、および認証情報を設定します。

C：表 3-32　　サーバの初回設定

パラメータ	値の例	説明
LDAP サーバ：		
プロトコル	LDAPS	ディレクトリへのアクセスに使用するプロトコル
Server Address	10.192.168.10	ディレクトリの IP アドレスまたは FQDN
ポート	636	ディレクトリによって使用されるポート番号
検索ベース：		

C：表 3-32　サーバの初回設定（続き）

パラメータ	値の例	説明
Base DN	OU = Enterprise、DC = ent-pa、DC = com	トップ レベルのユーザ検索ベース
属性の検索	sAMAccountName	ユーザの識別に使用される属性
Authorization:		
Bind DN	CN = tmssvc、OU = Enterprise、DC = ent-pa、DC = com	ディレクトリへのアクセスに使用するサービス アカウント
[パスワード（Password）]	< パスワード >	サービス アカウントのパスワード

Cisco Meeting Management では、LDAP グループを使用してユーザ グループをマッピングするため、ポータルでユーザアクセス権限を決定します。この時点で、管理者に対して以前に作成した LDAP グループ (CMMGroup) をマッピングして、ユーザがログインしてセットアップを続行できるようにします。C：表 3-33 に示される値を使用して、グループ マッピングを設定します。

C：表 3-33　グループ マッピングの設定

パラメータ	値の例	説明
Group DN	CN = CMMAdmin、OU = Enterprise, DC = ent-pa、DC = com	管理者用の LDAP グループ

初期セットアップが完了したら、管理者 (CMMAdmin LDAP グループのユーザ) のいずれかの管理者の承認情報を使用して、Cisco Meeting Management ポータルにログインします。ログインしたら、**設定** -> **CDR** に移動して、Cisco Meeting Management サーバ の IP アドレスまたは FQDN (たとえば、https://10.x.x.68) を使用して CDR 受信者アドレスを設定します。Cisco Meeting Management は、このアドレスを使用して、コールブリッジに CDR 受信者 URI 文字列を作成して、コールに関連するイベントを受信します。次に、**設定** -> **TMS** に移動し、TMS との Booking API 接続を設定して、今後予定されている会議に関する情報を取得します。設定には、C：表 3-34 に示される値を使用します。

C：表 3-34　TMS の設定

パラメータ	値の例	説明
ミーティング管理で TMS を使用する		TMS 統合を有効にする
TMS アドレス	10.x.x.75	TMS の IP アドレスまたは FQDN
プロトコル	HTTPS	TMS との接続に使用するプロトコル
ユーザ名	*<username>*	TMS サイト管理者のユーザ アカウント
[パスワード（Password）]	*< パスワード >*	ユーザのパスワード

設定 -> **NTP** に移動して、NTP サーバを追加します。3 つのコンポーネント間で時刻を同期させるために、同じ NTP サーバを Cisco Meeting Server と TMS に使用する必要があります。

前述のとおり、Cisco Meeting Management には、管理者およびビデオ オペレータのユーザグループがあります。管理者グループは、初期セットアップ手順で追加されます。ビデオ オペレータはここで追加する必要があります。**ユーザ -> ユーザ グループ** に移動し、C：表 3-35 に示される値を使用して設定を行います。

C：表 3-35　　ビデオグループの設定

パラメータ	値の例	説明
LDAP パス	CN = CMMOperator、OU = Enterprise、DC = ent-pa、DC = com	ビデオ オペレータの LDAP グループ
ロール	ビデオ オペレータ	ユーザ グループのロール

次に、モニタリングおよび管理のために、クラスタ内のすべてのコールブリッジを Cisco Meeting Management に追加します。**サーバ** ページに移動し、設定のための C：表 3-36 の値を使用して、コールブリッジ（クラスタ内のすべてのユーザ）を追加します。

C：表 3-36　　コールブリッジの設定を追加する

パラメータ	値の例	説明
サーバーアドレス	10.x.x.60	コールブリッジの IP アドレスまたは FQDN
ポート	445	Cisco Meeting Server で webadmin が使用するポート
表示名	US-CMS1	コールブリッジを表す意味のある名前
ユーザ名	<*user*>	API アクセス権を持つローカル Cisco Meeting Server ユーザ
[パスワード（Password）]	< *パスワード*>	ユーザ パスワード

自動検出されたコールブリッジオプションを使用して、クラスタ内の他のコールブリッジを Cisco Meeting Management に追加します。Cisco Meeting Management では、スケジュールされた会議を表示するために、TMS に追加されたコールブリッジを把握しておく必要があります。そのためには、管理者が Cisco Meeting Server クラスタを TMS に関連付ける必要があります。クラスタ テーブルの上部に表示される**クラスタと TMS 設定の関連付け** リンクをクリックし、C：表 3-37 の値を使用して設定を行います。

C：表 3-37　　クラスタと TMS 設定の関連付け

パラメータ	値の例	説明
接続されているコールブリッジ	US-CMS1	TMS に追加されたコールブリッジの名前
TMS システム ID（TMS System ID）	<*id*>	TMS 内のコールブリッジの設定ページに表示される TMS ID

Cisco Meeting Management の 2 つ目のインスタンスで高可用性を実現する必要がある場合は、このセクションの作業を繰り返します。次に、ネットワークロードバランサーを 2 つの Cisco Meeting Management インスタンスの前に配置するように設定します。

概要

上記の設定作業が完了したら、ビデオ オペレータは Cisco Meeting Management ポータルにログインして、Cisco Meeting Server の会議をモニタおよび管理することができます。

関連資料

Cisco Meeting Server の追加情報については、下記リンクから入手可能な次のドキュメントの最新版を参照してください。

- Cisco Multiparty Licensing At-A-Glance

  https://www.cisco.com/c/dam/en/us/solutions/collateral/collaboration/pervasive-conferencing/at-a-glance-c45-729835.pdf

- Cisco Meeting Server の導入ガイドと証明書のガイドライン ドキュメント

  https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html

- Cisco Meeting Server API Reference Guide

  https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html

- Cisco Meeting Server リリース ノート

  https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-release-notes-list.html

コラボレーション エッジ

改訂日：2019 年 2 月 19 日

この章では、コラボレーション ネットワーク境界におけるサービスへのアクセスを定義する一連のサーバとゲートウェイを含むコラボレーション エッジ推奨アーキテクチャについて説明します。コラボレーション エッジ推奨アーキテクチャは、インターネットや PSTN などのパブリック ネットワークへのアクセスを提供します。

コラボレーション エッジの詳細なアーキテクチャーの説明のあとに、インターネット アクセス用の Cisco Expressway と PSTN アクセス用の Cisco Unified Border Element の展開方法に関する展開の概要セクションが続きます。また、コラボレーション エッジのハイ アベイラビリティー、コラボレーション エッジのセキュリティー、およびコラボレーション エッジ ソリューションのスケーリングについても取り上げます。さらに、コラボレーション エッジの展開プロセスに関するセクションでは、Cisco Expressway、Cisco Unified Border Element、および Cisco 音声ゲートウェイの展開方法に関する詳細情報を提供します。

この章の新規情報とは

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

C：表 4-1　　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
細部の訂正および変更	この章の各項で説明	2019 年 1 月 23 日
モバイルおよびリモート アクセス制御	モバイルおよびリモート アクセス（C：4-28 ページ） モバイルおよびリモート アクセスを展開する（C：4-45 ページ）	2017 年 8 月 30 日

コア コンポーネント

コラボレーション エッジ アーキテクチャのコア コンポーネントを以下に示します。

- Cisco Expressway-C と Expressway-E：音声とビデオのインターネット接続とファイアウォール トラバーサル用
- Cisco Unified Border Element：IP トランク経由の音声 PSTN 接続用
- PSTN 音声ゲートウェイ：直接音声 PSTN 接続用

主なメリット

- 実装されているテクノロジーや使用されているパブリック ネットワークに関係なく、顧客やパートナーに接続します。
- 回復力のある、柔軟で拡張可能なアーキテクチャを提供します。
- ハードウェア クライアントとソフトウェア クライアントがパブリック ネットワーク（インターネットや PSTN）にアクセスできるようにします。
- Cisco Mobile クライアント、リモート クライアント、およびエンドポイントにコラボレーション サービスへのセキュアな VPN レス アクセスを提供します。

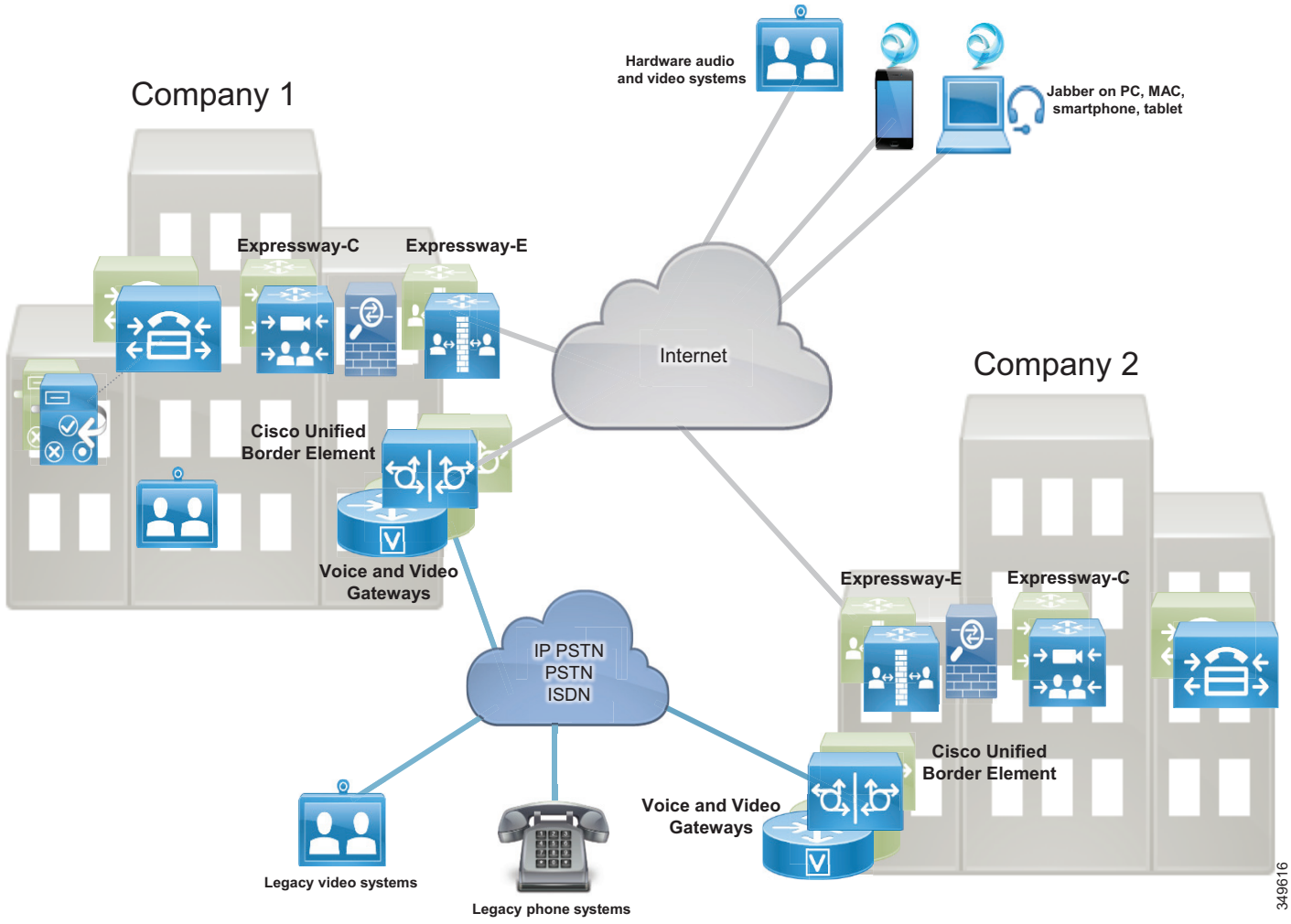
アーキテクチャー

コラボレーション エッジのアーキテクチャは、2 つの主要なネットワーク（インターネットと PSTN）とインターフェイス接続します。

インターネット接続は、VPN レス モバイル & リモート アクセス（MRA）と Business-to-Business（B2B）コミュニケーションを可能にします。これらのサービスを使用すれば、Jabber ユーザとハードウェア エンドポイントは、組織のネットワーク境界の外側にある企業コラボレーション サービスに安全にアクセスして、外部組織との Business-to-Business（B2B）音声およびビデオ通信を実現できます。

Cisco Expressway-C と Expressway-E は、ファイアウォール境界を横断しなければならないほとんどのケースでペアとして展開する必要があります。Expressway-C を内部ネットワークに、Expressway-E を緩衝地帯（DMZ）に配置することによって、ファイアウォールの両側でファイアウォール トラバーサル機能を有効にします。加えて、Expressway-C と Expressway-E をそれぞれクラスタ化することができます（C：図 4-1 を参照）。ほとんどの場合、横断するファイアウォール境界はインターネット接続ですが、個人所有デバイス持ち込み（BYOD）接続用の別個の企業 WiFi ネットワークである場合もあります。

C：図 4-1　　アーキテクチャの概要



PSTN 接続は、通信事業者ネットワークとの音声およびビデオ通信を可能にします。また、PSTN 接続は次のような方法で実現できます。

- 通信事業者への IP トランク経由。通常は音声専用サービス用。この接続は、Cisco Integrated Services Router（ISR）または Cisco Aggregation Services Router（ASR）上の Cisco Unified Border Element（CUBE）によって提供されます。Cisco Unified Border Element は、通信事業者のネットワークが企業ネットワークと通信するセントラル サイトに展開する必要があります。
- 音声ゲートウェイ経由。ゲートウェイには、Cisco Integrated Services Routers（ISR）などのさまざまなルータプラットフォーム上のアナログインターフェイスと ISDN インターフェイスが含まれます。このマニュアルでは、ISDN 音声インターフェイスのみを取り上げます。音声ゲートウェイは、PSTN 接続が必要なサイトでローカルに展開する必要があります。

ビデオ コール用のインターネット通信（Expressway）と音声専用コール用の IP PSTN 接続（CUBE）の展開に関連したコストを削減できます。ただし、IP ネットワークの信頼性は徐々に向上していますが、ネットワークの接続性の問題でリモート サイトから集中型 IP PSTN サービスにアクセスできない場合があることに注意する必要があります。このようなサイトで日常業務が PSTN 接続に大きく依存している場合は、集中型アクセス用のバックアップとしてローカル PSTN 接続の使用をお勧めします。

PSTN に関する推奨事項を以下に示します。

- PSTN を一元管理します。これにより、運用コストと経費が削減されます。
- 日常業務の実行を PSTN に大きく依存しているサイト専用のローカル PSTN 接続を設置します。このような場合は、ISDN チャネル数を削減する必要があります。これは、中央の PSTN アクセスが使用できない状況でしか ISDN チャネルが使用されないためです。これにより、ハードウェア コストが削減され、管理が簡素化され、資金の節約につながります。

上記の考察に基づくと、音声用に PSTN への IP トランク接続、ビデオ用にローカル PSTN ブレークアウトをバックアップとして使用したインターネットを使用することにより、大半の接続要件を満たすことになります。

Cisco Collaboration エッジには、ユーザが次のオプションにアクセスできるシナリオが含まれます。

- テレワーカやモバイル接続用のモバイル & リモート アクセス（MRA）
- 組織間の Business-to-Business（B2B）ビデオ通信
- 携帯電話用と固定電話へのアクセス用の PSTN

これらのシナリオでは、会社にいるユーザもインターネット上の社内ユーザも、まるで会社の中にいるかのように PSTN 音声コールと Business-to-Business（B2B）コミュニケーションにアクセスできます。ほとんどのケースで、保留、転送、会議などのサービスも使用できます。誰が誰に電話するかに関係なく、コラボレーション エッジ ソリューションは、モバイル & リモート アクセス、Business-to-Business（B2B）、PSTN 音声、およびビデオ サービス間の相互接続を可能にします。

インターネット アクセスに関する Expressway-C と Expressway-E の役割

インターネットを使用したコラボレーション サービスは、人気が高く、既存のレガシー ISDN ビデオ システムがどんどん置き換えられています。インターネット ベースのコラボレーション サービスに使用されている 2 つの主なプロトコルは SIP と H.323 です。

また、インターネットは、リモート ユーザとモバイル ユーザを、バーチャル プライベート ネットワーク（VPN）を使用せずに、音声、ビデオ、IM と Presence、およびコンテンツ共有サービスに接続するためにも使用されます。

モバイル & リモート アクセスだけでなく、Business-to-Business（B2B）サービスも、同じ Expressway-C と Expressway-E のソリューション ペアの一部として有効にできます。Expressway-C は社内ネットワーク内に展開されるのに対して、Expressway-E は DMZ 内に展開されます。

Expressway-C と Expressway-E のペアは次の機能を実行します。

- インターワーキング：音声、ビデオ、およびコンテンツ共有用の H.323 / SIP 間コールを相互接続する機能。
- 境界通信サービス：Expressway-C は社内ネットワーク内に配置されますが、Expressway-E はエンタープライズ DMZ 内に配置され、企業ネットワークとインターネット間の通信サービス専用の接続点を提供します。
- セキュリティ：モバイル & リモート アクセスと Business-to-Business（B2B）コミュニケーションの両方に認証と暗号化を提供する機能。

モバイル & リモート アクセス、および Business-to-Business（B2B）コールは Expressway-E と Expressway-C をフロースルーして、コール シグナリングとメディアの両方だけでなく、その他のコラボレーション データ フロー（XMPP や HTTP を含む）も処理されます。

モバイルおよびリモート アクセス

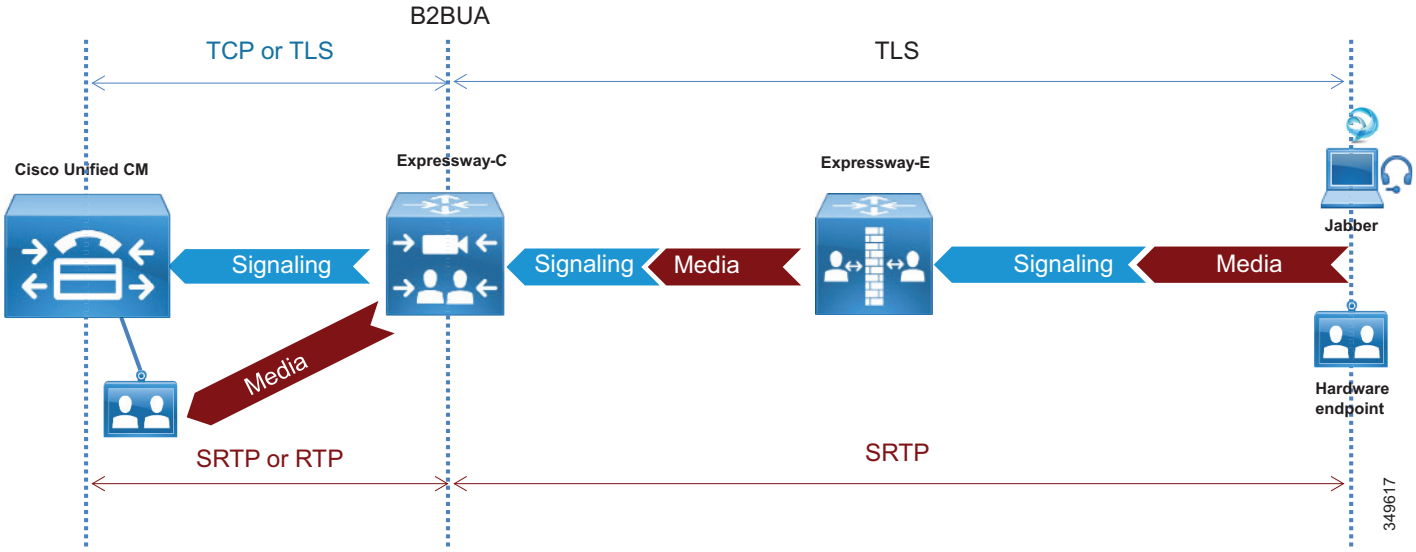
Cisco Expressway ソリューションのモバイル & リモート アクセス機能は、逆プロキシ ファイアウォール トラバーサル接続を提供します。これにより、リモート ユーザとそのデバイスが企業のコラボレーション アプリケーションおよびサービスにアクセスして利用できます。

C：図 4-2 に示すように、Cisco Expressway ソリューションには、2 つの主なコンポーネント（Expressway-E ノードと Expressway-C ノード）が含まれています。この 2 つのコンポーネントは、Cisco Unified Communications Manager（Unified CM）と連携して、セキュアなモバイル & リモート アクセスを可能にします。Expressway-E ノードは、モバイル & リモート デバイスにセキュアなエッジ インターフェイスを提供します。

Expressway-C は、Expressway-E ノードとのセキュアな接続を構築します。Expressway-C ノードは、Unified CM へのプロキシ登録を提供し、リモート セキュア エンドポイント登録を可能にします。Expressway-C ノードには、メディア終端機能を提供するバックツーバック ユーザ エージェント（B2BUA）が含まれます。

C：図 4-2 に、すべてのモバイル & リモート アクセス コールのシグナリングとメディアの両方が Expressway-C と Expressway-E を行き来する様子を示します。

C：図 4-2　　Expressway 上の B2BUA とコール レッグ

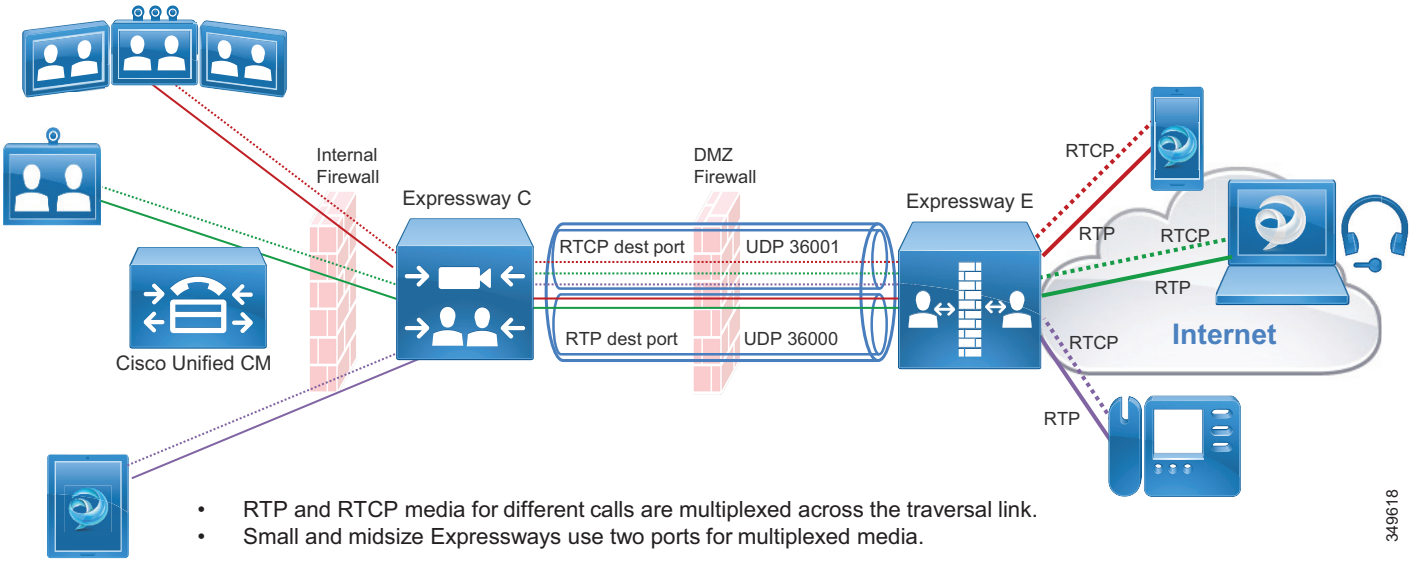


Business-to-Business（B2B）コミュニケーション

Expressway-C と Expressway-E は、連携してインターネット経由の Business-to-Business（B2B）コミュニケーション用のコア コンポーネントであるファイアウォール トラバーサル ソリューションを形成するように設計されています。

Expressway-C は、企業ネットワークの内部（信頼された側）に配置され、Expressway-E へのセキュアで信頼できる各種の標準規格に準拠した接続手段を提供する役割を果たします。また、その背後にあるすべてのデバイスへのトラバーサル クライアントとしての機能を果たします。このソリューションは、アウトバウンド通信用に開かれた少数のポートにすべてのメディアを多重化することによって、大量のメディア ポートを使用するデバイスの問題を解決します。また、Expressway-C から Expressway-E までのトラバーサル ゾーンに関するキープアライブを送信することによって、社内から社外への認証された信頼できる接続を実現します。また、すべてのインターネット通信に対して一括窓口を提供することで、セキュリティ リスクを最小化します。（C：図 4-3 を参照）。

C：図 4-3　　Expressway-C の多重化とキープアライブ



SIP、H.323、XMPP などのリアルタイムや準リアルタイムの通信プロトコルでは、ファイアウォールの背後に設置されたデバイスとの通信ニーズは解決されません。このようなプロトコルを使用した典型的な通信には、シグナリングとメディア内にデバイス IP アドレスが含まれており、それぞれが TCP パケットと UDP パケットのペイロードになります。これらのデバイスが、内部的にルーティング可能な同じネットワーク上に存在する場合は、相互に直接通信することができます。TCP パケットのペイロードで伝送されるシグナリング IP アドレスは送信デバイスに戻すルーティングが可能であり、その逆もできます。ただし、送信デバイスがパブリックまたはネットワーク エッジ ファイアウォールの背後の別のネットワーク上に存在する場合は、2 つの問題が発生します。1 つ目の問題は、受信デバイスが、パケットの復号化後に、ペイロードで伝送された内部 IP アドレスに応答することです。この IP アドレスは、通常、ルーティング不可能な RFC 1918 アドレスであり、絶対に返信先に到達しません。発生する 2 つ目の問題は、返信先 IP アドレスがルーティング可能であっても、メディア（RTP/UDP）が外部ファイアウォールによってブロックされることです。このことは、Business-to-Business（B2B）コミュニケーションと、モバイル & リモート アクセスの通信の両方に当てはまります。

Expressway-E は DMZ 内のネットワーク エッジに配置されます。これは、標準の相互運用性を維持しながら、SIP、H323、および XMPP に関するシグナリングとメディアの両方のルーティング問題を解決する役割を果たします。さらに、ネットワーク内部のエンドポイント、デバイス、およびアプリケーション サーバの代わりにメディアとシグナリングを処理するために該当するヘッダーと IP アドレスを変更します。

インスタント メッセージおよびプレゼンス フェデレーション

インスタント メッセージおよびプレゼンス フェデレーションは、ある組織のユーザがチャットやプレゼンス ステータス情報に関する XMPP トラフィックをその組織の外部ファイアウォール経由で別の組織のユーザとやり取りできるようにします。

以前のシスコ アーキテクチャでは、シスコ適応型セキュリティ アプライアンス（ASA）ファイアウォールを使用して、外部ファイアウォール経由で内部の IM and Presence サーバに直接アクセスするために受信ポートを開くことができました。SIP フェデレーションでは、引き続きこのソリューションが推奨されています。

XMPP フェデレーションでは、XMPP トラフィックを外部の宛先とやり取りするための信頼できるセキュアなファイアウォール トラバーサル ソリューションとして同じ Expressway-C と Expressway-E のペア アーキテクチャを使用します。Expressway-E は、XMPP 用のセキュアな DMZ ベースのターミネーション ポイントをインターネットに提供します。Expressway-C は、ファイアウォール トラバーサル用に Expressway-E への TLS ベースの認証されたセキュア接続を提供するので、ファイアウォール上でポートを開く必要がありません。

また、Expressway-C は、IM と Presence サーバへの AXL API 接続も提供します。AXL API は、Expressway-E から収集された XMPP サーバ間情報を IM と Presence データベースに送信します。これにより、ファイアウォール上で他のポートを開くことなく、Expressway-E 経由で他の組織へのフェデレーション接続を開始するのに必要な接続情報が IM と Presence サーバに提供されます。XMPP フェデレーションでは、音声とビデオのエスカレーションが可能です。同じ組織で、XMPP フェデレーションと SIP フェデレーションの両方を同時に実装することができます。

PSTN アクセス

ここでは、Cisco Unified Border Element をセッション ボーダー コントローラ（SBC）として使用した PSTN アクセス用のアーキテクチャについて説明します。

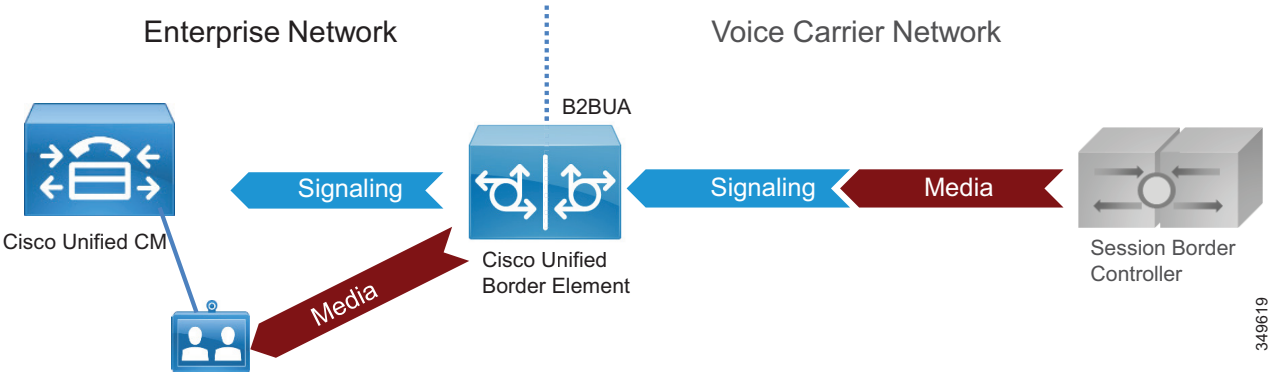
Cisco Unified Border Element の役割

従来の PSTN 接続の代わりに通信事業者への IP トランクを使用した音声接続は人気が高まっており、徐々に既存の TDM ベースの PSTN アクセスに取って代わろうとしています。SIP はプロバイダー ネットワークに接続するためのアクセス プロトコルとして広く使用されており、今日では、多くの通信事業者が音声専用サービスを Cisco Unified Border Element などのセッション ボーダー コントローラ経由で PSTN に提供しています。セッション ボーダー コントローラは、SIP バックツーバック ユーザ エージェント（B2BUA）であり、各コールの音声メディアと SIP シグナリングの両方が Cisco Unified Border Element を通過するフロースルー モードでよく使用されます（C：図 4-4 を参照）。

Cisco Unified Border Element は、さまざまな Cisco ルータおよびゲートウェイ上で利用可能なライセンス供与された Cisco IOS アプリケーションであり、通信事業者のボーダー エレメントへの SIP トランク経由で PSTN に接続するための推奨プラットフォームです。

また、Cisco Unified Border Element は、Cisco Unified Communications Manager（Unified CM）に基づくエンタープライズ音声ネットワークを SIP トランク サービス経由で通信事業者に接続して相互運用できるようにします。さらに、Cisco Unified Border Element は、シグナリング ストリームとメディア ストリームの両方を終端処理して再発信することにより、IP ネットワーク間のセキュアなボーダー相互接続サービスを提供します。Cisco Unified Border Element を使用しているお客様は、現在のネットワーク サービスを縮小して、ネットワーク アーキテクチャを簡略化し、機能強化中のネットワークをコラボレーション サービスに位置付けることができます。

C：図 4-4　　B2BUA としての Cisco Unified Border Element



Cisco Unified Border Element は、エンタープライズ ネットワークと通信事業者ネットワークの間で次の機能を実行します。

- セッション制御：SIP セッションに対して、柔軟なトランク ルーティング、コール アドミッション制御、復元力、およびコール アカウンティングを提供する機能。
- インターワーキング：音声用のメディア トランスコーディング サービスと、SIP の遅延オファーと早期オファー間の相互運用性を提供する機能。
- 境界設定：2 つのネットワーク間のアドレス変換用とポート変換用に別々の境界ポイントとして機能し、トラブルシューティングを容易にする機能。
- セキュリティ：ネットワーク間のリアルタイム トラフィックをインテリジェントに許可または禁止し、アプリケーションの必要に応じてリアルタイム トラフィックを暗号化する機能。

音声ゲートウェイの役割

集中型 PSTN アクセスが使用できない場合は、TDM ゲートウェイを使用して PSTN に接続することをお勧めします。Cisco では、適切なインターフェイスカード（低密度デジタル（BRI）、高密度デジタル（T1、E1、および T3）、およびアナログ（FXS、FXO、および E&M）の各インターフェイス）が有効になっているサービス統合型ルータ（ISR）上で PSTN へのアナログ接続とデジタル接続を可能にするさまざまな TDM ゲートウェイを提供しています。

音声ゲートウェイの詳細については、次に提供される Cisco サービス統合型ルータのドキュメンテーションを参照してください。

https://www.cisco.com/c/en/us/products/routers/branch-routers/index.html

展開の概要

ここでは、インターネット接続用の Cisco Expressway と PSTN アクセス用の Cisco Unified Border Element の展開方法について説明します。

インタネット接続用の Expressway の展開

Cisco Collaboration エッジ アーキテクチャの標準展開には、企業のコラボレーション サービスに対するセキュアなモバイルデバイスおよびリモート VPN レス アクセス用の 1 つ以上の Expressway-C と Expressway-E のペアの展開が含まれます。

復元力を高めるためには、Expressway-C と Expressway-E の両方をクラスタ内に展開する必要があります。クラスタごとのサーバ数は、Unified CM に対する同時プロキシ化登録の数と同時コールの数によって異なります。前者の数には Expressway 経由で Unified CM に登録するモバイル ユーザとリモート ユーザの数が数えられるのに対して、後者の数には Business-to-Business（B2B）とモバイル & リモート アクセス（MRA）の同時コールの数が数えられます（詳細については、サイジングの章を参照してください）。

このサービスは、Jabber クライアント、特定の IP フォン モデル、および TC または CE ソフトウェアを実行している Cisco TelePresence System エンドポイントに提供されます。しばしば、地理的範囲とスケーリングのために複数のペアの Expressway-C と Expressway-E が展開され、これにより、コラボレーション サービスの複数のインスタンスへのアクセスが可能になります。インターネット サービス プロバイダーからのさまざまなメトリックに基づいてリモート クライアントおよびエンドポイント アクセスのバランスを取るため、GeoDNS を使用する必要があります。

この同じ Expressway を Business-to-Business（B2B）コミュニケーションに利用することもできます。コールの量が Expressway クラスタの容量を超える場合は、Business-to-Business（B2B）サービスと MRA サービスを別々のボックスに分割する必要があります（詳細については、サイジングの章を参照してください）。

Expressway が両方のサービスに使用されている場合は、Unified CM がインターネット上のユニファイド ビジネス コミュニケーション アクセス用の SIP トランク経由で Expressway-C に接続されます。Expressway-C は、ネットワークの信頼された側に配置され、セキュアなファイアウォール トラバーサル サービスを Expressway-E に提供します。

エンタープライズ セキュリティ ポリシーに基づいて、さまざまな展開モデルを実装できます。このマニュアルでは、デュアル インターフェイスを備えた DMZ 展開を中心に説明します。これは、この展開が最も一般的でセキュアな展開モデルだからです。その他の展開モデルについては、『*Cisco Expressway Basic Configuration Deployment Guide*』の最新版を参照してください。

Expressway-C と Expressway-E は、ファイアウォール トラバーサル機能を提供します。ファイアウォール トラバーサルは次のように動作します。

1. Expressway-E はエンタープライズ DMZ 内に設置されたトラバーサル サーバです。Expressway-C は企業ネットワーク内部に設置されたトラバーサル クライアントです。
2. Expressway-C は、セキュアなログイン クレデンシャルを使用して、ファイアウォールを通って Expressway-E 上の特定のポートに至るトラバーサル アウトバウンド接続を開始します。ファイアウォールがほとんどの場合の動作と同様にアウトバウンド接続を許可している場合は、企業のファイアウォールで追加のポートを開く必要はありません。ポートの詳細については、『*Cisco Expressway IP Port Usage for Firewall Traversal*』に関するドキュメントの最新版を参照してください。

   モバイル & リモート アクセスには、Unified Communications トラバーサル ゾーンと呼ばれる別のトラバーサル ゾーンが必要です。Unified Communications トラバーサル ゾーンは SIP と連動し、TLS およびメディア暗号化を必要とします。一方、Business-to-Business（B2B）トラバーサル ゾーンは SIP と H.323 を音声とビデオのシグナリング プロトコルとして許可します。Unified Communications トラバーサル ゾーンは、IM and Presence サーバへの接続とプロビジョニング目的で使用される XMPP と HTTPs も許可します。

3。 接続が確立されると、Expressway-C がキープアライブ パケットを定期的に Expressway-E に送信して接続を維持します。

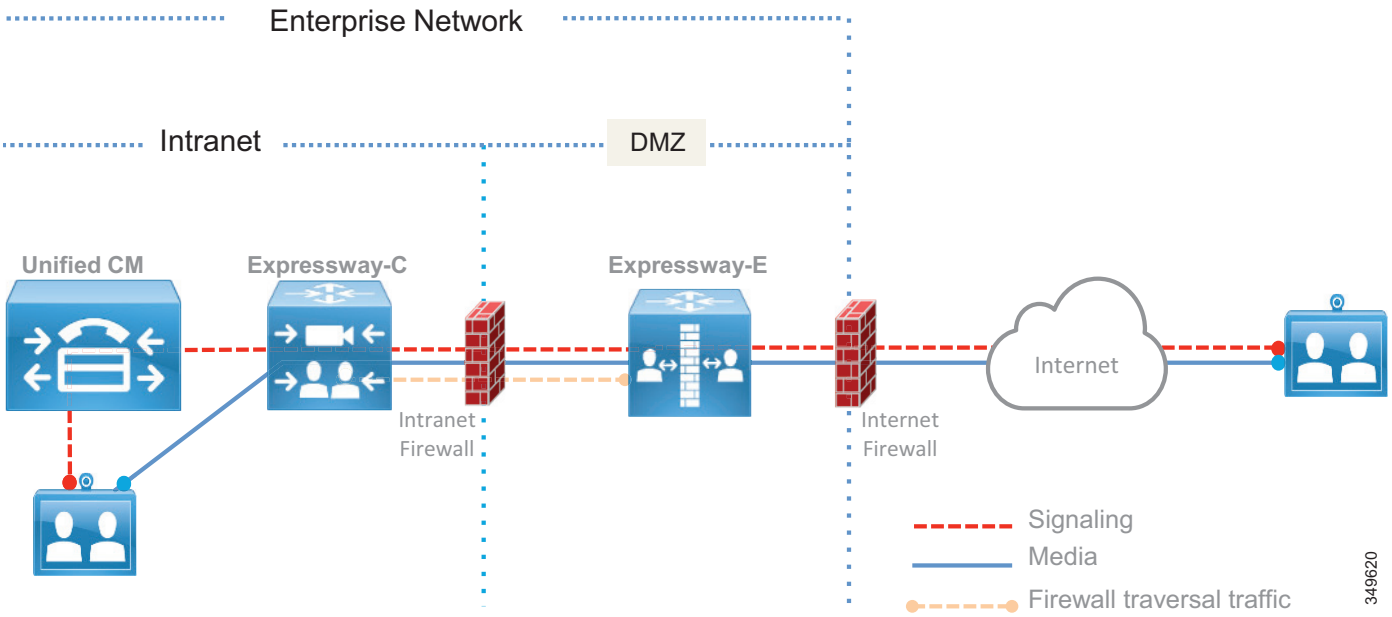
4。 Expressway-E がコールやその他のコラボレーション サービス要求を受け取ると、着信要求を Expressway-C に発行します。

5。 その後で、Expressway-C がその要求を Unified CM またはその他のコラボレーション サービス アプリケーションにルーティングします。

6。 接続が確立され、アプリケーション トラフィック（音声メディアとビデオ メディアを含む）が既存のトラバーサル接続経由で安全にファイアウォールを通過します。

ファイアウォール トラバーサルが機能するためには、Expressway-C 上でトラバーサル クライアント ゾーンを設定し、Expressway-E 上でトラバーサル サーバ ゾーンを設定する必要があります。C：図 4-5 に、ファイアウォール トラバーサル プロセスの概要を示します。

C：図 4-5　　Expressway-C と Expressway-E のファイアウォール トラバーサル プロセス



Expressway-E の展開ではシングル LAN インターフェイスまたはデュアル LAN インターフェイスのどちらも使用できますが、デュアル インターフェイスの使用をお勧めします。デュアルインターフェイス展開シナリオでは、Expressway-E が次の 2 つのファイアウォール間の DMZ 内に配置されます。インターネット ファイアウォールはインターネット向けの NAT サービスを提供し、イントラネット ファイアウォールは企業信頼ネットワークへのアクセスを提供します。

Expressway-E は次の 2 つの LAN インターフェイスを備えています。1 つはインターネット ファイアウォール向け（*外部インターフェイス*とも呼ばれる）で、もう 1 つはイントラネット ファイアウォール向け（*内部インターフェイス*とも呼ばれる）です。

外部インターフェイスにパブリック IP アドレスを割り当てる必要はありません。これは、NAT によってアドレスを静的に変換できるためです。この場合は、NAT で使用されるパブリック IP アドレスを Expressway-E 上の「静的 NAT アドレス」として設定する必要があります。

Expressway-C には、モバイル / リモート アクセスおよび Business-to-Business（B2B）コールを終端する B2BUA が組み込まれています。それぞれのモバイル / リモート アクセス コールに B2BUA のインスタンスが 1 つ必要です。暗号化の設定に応じて、それぞれの Business-to-Business（B2B）コールに B2BUA のインスタンスが 1 つ必要な場合があります。Expressway-E には、Business-to-Business（B2B）コールを終端する B2BUA が組み込まれています。Expressway-C と Expressway-E には、Microsoft や H.323/SIP プロトコル インターワーキングなどのさまざまなサービスに専用の B2BUA も組み込まれています。

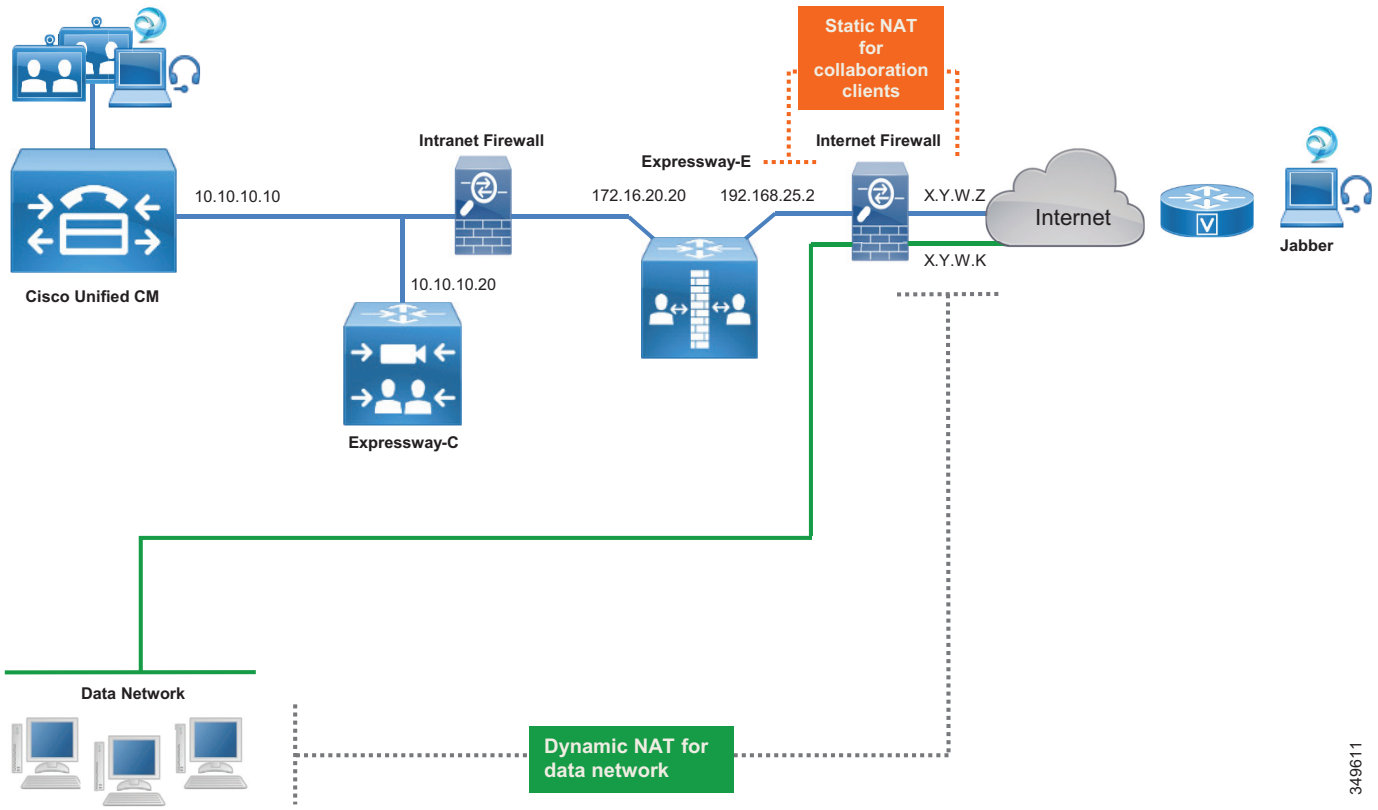
B2BUA は、コラボレーション アプリケーション トラフィックを終端します。インターネットから Expressway-E 経由の Expressway-C への接続はモバイルおよびリモート アクセス用に常に暗号化されますが、Expressway-C と Unified Communications Manager エンドポイントの間の接続は設定に応じて暗号化できる場合とできない場合があります。Business-to-Business（B2B）コミュニケーション用のインターネットからの接続は、設定および会社の方針に従って暗号化される場合とされない場合があります。このマニュアルでは、インターネットと Expressway-C の間でモバイルおよびリモート アクセス用の暗号化が実行されるが、Expressway-C と内部バックエンド サーバおよびクライアントの間の通信は暗号化されずに送信されるシナリオを中心に説明します。これは単なる 1 つのオプションです。Cisco Unified Communications Manager が混在モード用に設定されている場合は、Expressway-C と Cisco Unified Communications Manager の間でもモバイルおよびリモート アクセス接続を暗号化するように設定できます。Business-to-Business（B2B）暗号化機能については、後述のコラボレーション エッジのセキュリティーに関するセクションで説明します。

Expressway-C は、モバイルおよびリモート アクセス クライアントまたはデバイスの Unified CM への登録をプロキシします。Unified CM では、それらが Expressway-C の IP アドレスで登録されたデバイスとして一覧表示されます。

C：図 4-6 に、前述した展開を示します。関連する IP アドレスが図に示されています。場所やインターネット サービス プロバイダーによって異なるパブリック IP アドレスが数字ではなく文字で表現されています。

Expressway-E は 2 つのインターフェイスを備えています。内部インターフェイスの IP アドレスは 172.16.20.20 で、外部インターフェイスの IP アドレスは 192.168.25.2 です。外部インターフェイスの IP アドレスは静的に X.Y.W.Z に変換されます。このアドレスは Expressway-E 上でも設定されます。Expressway-E が INVITE を送信すると、独自のアドレスを使用するのではなく、変換されたインターフェイス アドレスに設定された IP アドレスを使用して Session Description Protocol（SDP）メッセージが作成されるため、着信側はプライベート アドレスではなくルーティング可能なパブリック アドレスを使用できます。

C：図 4-6　　インターネット ファイアウォール上の NAT インターフェイス



インターネット上のエンドポイントが Expressway 経由で Unified CM やその他のコラボレーション アプリケーションに接続すると、ローカル顧客宅内機器（CPE）によってその IP アドレスが最初にパブリック IP アドレスに変換されます。Expressway-E では、ソース IP アドレスが Expressway-E の内部 IP LAN インターフェイスのアドレスに置き換えられます。パケットが Expressway-C に到着すると、Expressway-C はパケットをコラボレーション サービス アプリケーションに転送する前に、パケットのソース IP アドレスを独自の IP アドレスに置き換えます。

もう一方の方向では、内部エンドポイントからのトラフィックが Expressway を通ってインターネットに入ると、その送信元 IP アドレスが Expressway-E 外部 LAN インターフェイス アドレスに置き換えられ、その後、インターネット ファイアウォール上の NAT によって静的に変換されます。データ デバイスの送信元 IP アドレスは、インターネット ファイアウォールの別のインターフェイスを使用して X.Y.W.K に動的に変換されます。

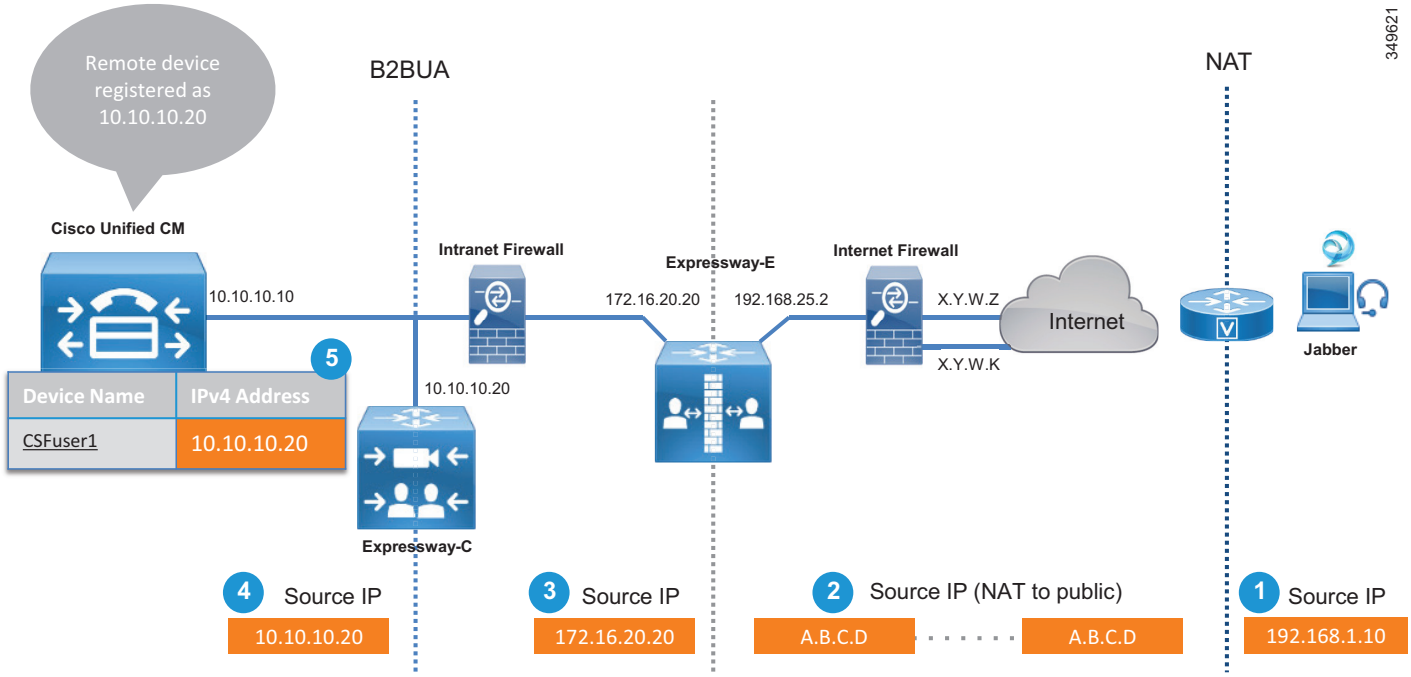
データと Jabber やブラウザなどの通信アプリケーションを使用する PC では、Jabber アプリケーション アドレスは NAT によって静的に変換され、ブラウザ アプリケーション アドレスは NAT によって動的に変換されます。

ファイアウォール内でスタティック NAT 変換が実行される場合でも、パケットの送信元 IP アドレスは転送中に次のように変換されます。パケットが Expressway-C から Expressway-E に到達すると Expressway-C の IP アドレスに変換され、パケットが Expressway-E からファイアウォールに到達すると Expressway-E の IP アドレスに変換されます。ファイアウォールでは、パケットが NAT によって静的に変換されてからインターネットに送信されます。

モバイルおよびリモート アクセス

コール制御サービスの場合は、C：図 4-7 に示すように、Expressway-C プロキシが独自の IP アドレスを使用してエンドポイントを Unified CM に登録します。この動作は、共有回線や複数回線などのサービスがモバイルおよびリモート アクセスで設定されている場合には変化することがあります。

C：図 4-7　　パケットの性質から見た NAT



C：図 4-7 に示すアドレス変換プロセスは次のステップで構成されます。

1. エンドポイントにパブリック IP アドレスが割り当てられていない場合は、インターネットへのアクセスを提供するルータでエンドポイントの送信元 IP アドレスが NAT によって（192.168.1.10 から A.B.C.D に）変換されます。
2. パケットが Expressway-E に到着します。
3. Expressway-E が独自の内部 LAN インターフェイス アドレスを使用して Expressway-C にパケットを送信します（A.B.C.D から 172.16.20.20 に）。
4. Expressway-C がそのパケットを受け取って、接続を終了します。また、独自の IP アドレスを使用して、Unified CM 向けの別の接続を再発信します（172.16.20.20 から 10.10.10.20 に）。
5. エンドポイントが Expressway-C の IP アドレス（10.10.10.20）を使用して Unified CM に登録されます。

Expressway-C の IP アドレスを使用してデバイスを Unified CM に登録する場合は、次のような固有のメリットが得られます。たとえば、リモート デバイスが企業ネットワークに直接接続されていない場合にビデオ帯域幅を制限し、リモート デバイスがオンプレミスの場合にはビデオ帯域幅に別の値を割り当てたりできます。ここでは説明しませんが、この方法は Unified CM 上のモビリティ機能を使用して簡単に実現できます。このモビリティ機能は、IP アドレス範囲に基づく特定のポリシーの定義を可能にします。

エンドポイントがインターネット経由で登録された場合は、Cisco Collaboration アーキテクチャでリモートから管理することはできません。これは、エンドポイントの IP アドレスが動的に変換され、ファイアウォールの背後に配置されるためです。リモート管理が必要な場合は、エンドポイントを VPN 経由で展開してください。ただしエンドポイント アップグレードは例外で、エンドポイントがファイアウォールの背後にある場合でも、リモートでこれを実施できます。

VPN Technologies はこのアーキテクチャの一部ではありませんが、必要に応じて追加することができます。

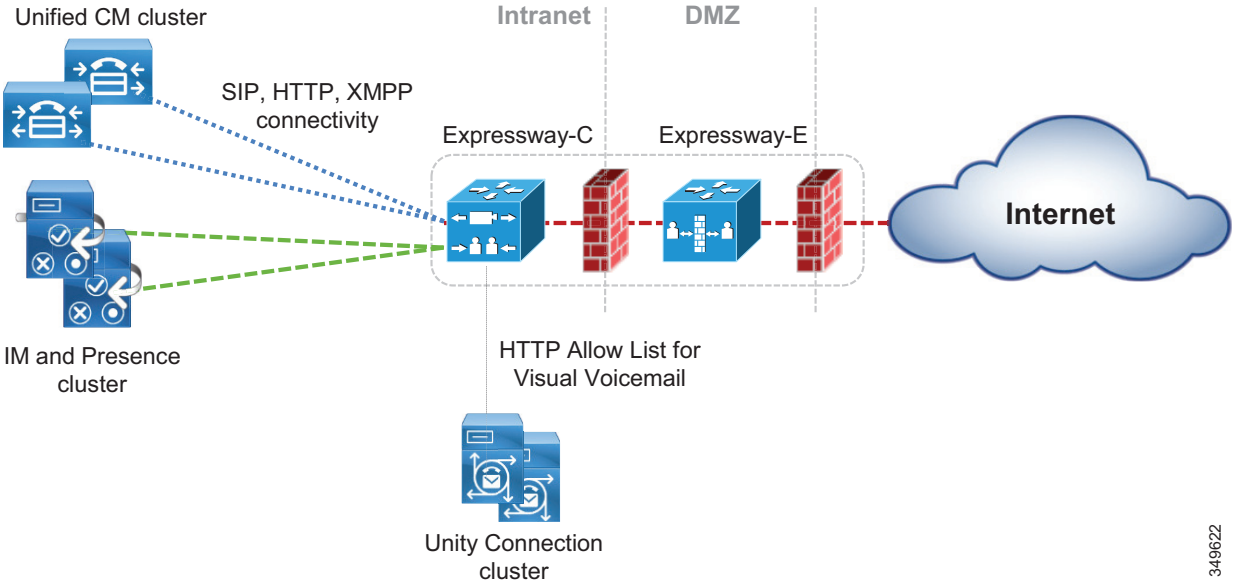
Expressway-E と Expressway-C 上でモバイルおよびリモート アクセスを有効にする必要があります。そうすれば、Unified CM and IM and Presence パブリッシャ ノードの DNS 名を指定することによって、Unified CM and IM and Presence クラスタを検出するように Expressway-C を設定できます。

DMZ 内に展開された Expressway-E は、モバイル & リモート アクセス サービスを使用する Jabber クライアントと TelePresence エンドポイントに信頼できるエントリ ポイントを提供します。

Expressway-C は、HTTPs、SIP、および XMPP を使用して、Unified CM クラスタ、IM と Presence クラスタ、および Cisco Unity Connection に接続します（C：図 4-8 を参照）。

さらに、Jabber が HTTP 経由で特定のサーバに接続しなければならない場合が数多くあります。たとえば、ビジュアル ボイスメール、Jabber 更新サーバ、カスタム HTML タブおよびアイコン、ディレクトリ フォト ホストなどです。このようなケースでは、Jabber が Unified CM を経由せずに直接これらのサーバに接続します。Expressway-C は Jabber クライアントが接続を許可されたサーバを示す HTTP 許可リストを必要とします。

C：図 4-8　　Unified CM、IM と Presence サービス、および Unity Connection への Expressway 接続



C：表 4-2 に、モバイル & リモート アクセスのために Expressway によって使用されるプロトコルの概要を示します。

C：表 4-2　モバイル & リモート アクセス用の Expressway プロトコル

プロトコル	セキュリティ	サービス
SIP	TLS	セッションの確立：登録や招待など
HTTPS	TLS	ログイン、プロビジョニング、設定、連絡先検索、ビジュアル ボイスメール
XMPP	TLS	インスタント メッセージ、プレゼンス
RTP	SRTP	音声、ビデオ、コンテンツ共有、高度なコントロール

Jabber または TelePresence エンドポイント ユーザがログインするときには、完全修飾名（user1@ent-pa.com など）を指定します。クライアントが次の特定の SRV レコードをパブリック DNS サーバにクエリします。

- _cisco-uds._tcp.ent-pa.com：企業 DNS サーバ上でのみ設定されます。
- _collab-edge._tls.ent-pa.com：パブリック DNS サーバ上でのみ設定され、Expressway-E クラスタのパブリック インターフェイスに解決されます。このレコードは常に TLS を示していることに注意してください。

クライアントがインターネット経由で接続されている場合は、パブリック DNS サーバから _cisco-uds に関する応答が返されませんが、クライアントは _collab-edge SRV レコードに関する応答を受け取ります。

その後で、DNS サーバが Expressway-E に関する A レコード（または Expressway-E がクラスタ化されている場合は複数のレコード）をクライアントに送信します。クライアントが Expressway-E の DNS 名を認識したら、プロビジョニングと登録の手順を開始できます。

プロビジョニングは HTTPs を使用して実行されるのに対して、登録では SIP と XMPP が使用されます。

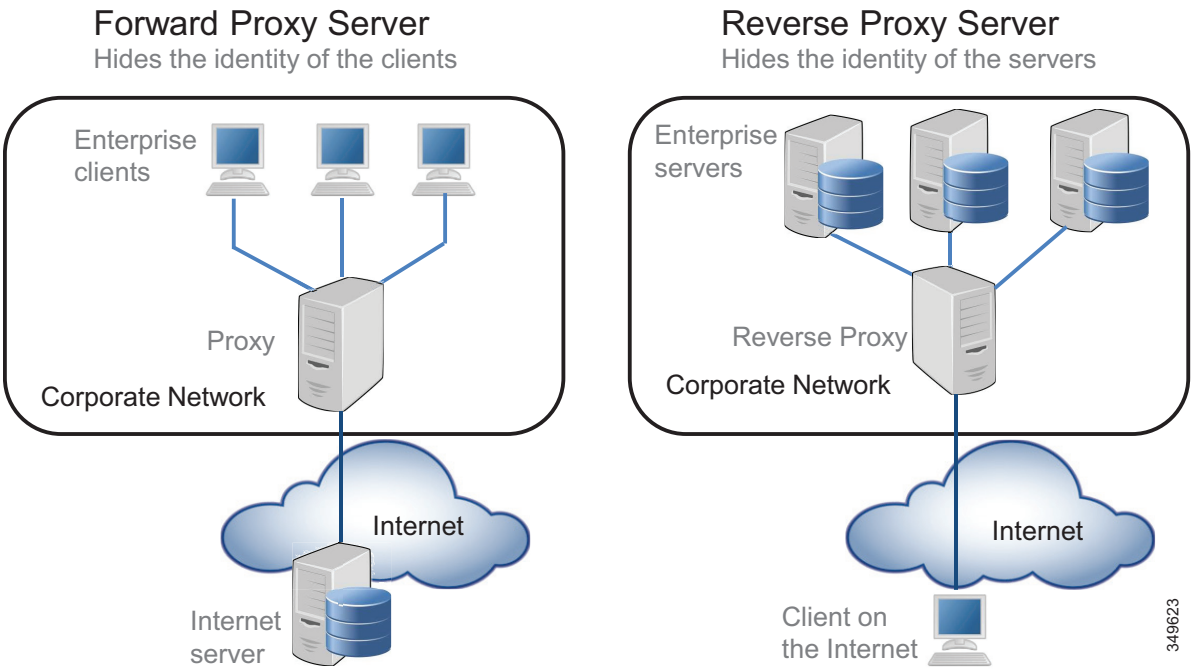
Expressway-C は、プロビジョニング プロセスを管理するための HTTPs 逆プロキシ サーバ機能を備えています。逆プロキシは、*プロキシ サーバ*とも呼ばれる最も一般的な転送プロキシ サーバの逆です。

C：図 4-9 に示すように、転送プロキシ サーバはインターネット サーバへの接続時にクライアント詳細を隠すことによってオンプレミス クライアントに関するサービス情報を提供するのに対して、逆プロキシ サーバはオンプレミス サーバ情報を隠すことによってオフプレミス クライアントに関する情報を提供します。転送プロキシ経由でインターネット サーバに接続している社内ネットワーク内のクライアントは接続先のサーバの ID は知っていますが、サーバはクライアントの ID を知りません。

一方、逆プロキシ経由で接続しているインターネット上のクライアントは、逆プロキシ サーバ経由で接続しているためオンプレミス サーバの ID を知りませんが、オンプレミス サーバは接続先のクライアントの ID を知っています。その後、この情報は、オンプレミス サーバから発信されたかのようにクライアントに戻されます。

Expressway-C は、Cisco Unified CM、IM と Presence、Unity Connection などのコラボレーション アプリケーション サーバの代わりに、プロビジョニング、登録、およびサービスの詳細をインターネット上のクライアントに提供する逆プロキシ機能を備えています。

C：図 4-9　　フォワード プロキシ サーバとリバース プロキシ サーバ



ビジュアル ボイスメール、Jabber 更新サーバ、カスタム HTML タブおよびアイコン、ディレクトリ フォト ホストなどのサービスに対して、Expressway-C は HTTP サービス用のアクセス リストの一種である *HTTP 許可リスト*でこれらのサービスが指定されている場合にこれらの接続を許可することにも留意してください。

プロビジョニングと登録は、クライアント、Expressway-C、Expressway-E、Unified CM、および IM と Presence サーバが関与する多段階プロセスです。

クライアントがコラボレーション エッジ経由で登録する場合に関係する主なステップの概要を以下に示します。

1. プロビジョニングは、クライアントから発行された **get_edge_config** 要求で開始されます。次に例を示します。

   https://expressway_e.ent-pa.com:8443/ZeW50LXBhLmNvbQ/get_edge_config?service_name=_cisco-uds&service_name=_cuplogin

   この要求と一緒に、クライアントはユーザのクレデンシャル（たとえば、ユーザ名「user1」とパスワード「user1」）を送信します。クエリは Expressway-E に送信されてから、Expressway-C に転送されます。

2. Expressway-C が Unified CM に対する UDS クエリを実行して user1 のホーム クラスタを特定します。これはマルチクラスタ シナリオでは必須です。

   GET cucm.ent-pa.com:8443/cucm-uds/clusterUser?username=user1

3. ホーム クラスタが見つかると、Expressway-C に応答が送信されます。この応答には、クラスタ内のすべてのサーバが含まれています。

4。 Expressway-C がクライアントの代わりに user1 に関する次のクエリを発行することによって、ホーム クラスタにプロビジョニング情報を問い合わせます。

GET /cucm-uds/user/user1/devices はデバイス割り当てリストを取得します。

GET /cucm-uds/servers はクラスタのサーバ リストを取得します。

GET /cucm-uds/user/user1 は user1 のユーザ設定と回線設定を取得します。

クエリに対する応答で、TFTP サーバも返されます。

以降のクエリ（**http://us_cucm1.ent-pa.com:6972/SPDefault.cnf.xml** など）は HTTP 経由の TFTP クエリです。こうして、プロビジョニング プロセスが UDS と TFTP サーバに対するクエリによって実行されます。これらのクエリの結果として、プロビジョニング情報がクライアントに転送され、クライアントは登録プロセスを開始することができます。

登録プロセスは次の 2 つのアクションで構成されます。

1。 Expressway-C 上の XCP ルータ機能を介して実行される IM と Presence ログイン。XCP ルータは Expressway-C 上の IM と Presence クラスタに問い合わせて、ユーザの設定場所である IM と Presence クラスタを見つけ、Jabber クライアントが IM と Presence サービスにログインできます。

2。 SIP REGISTER メッセージを使用した Unified CM 登録：Expressway SIP プロキシ機能によってプロキシされます。

Business-to-Business（B2B）コミュニケーション

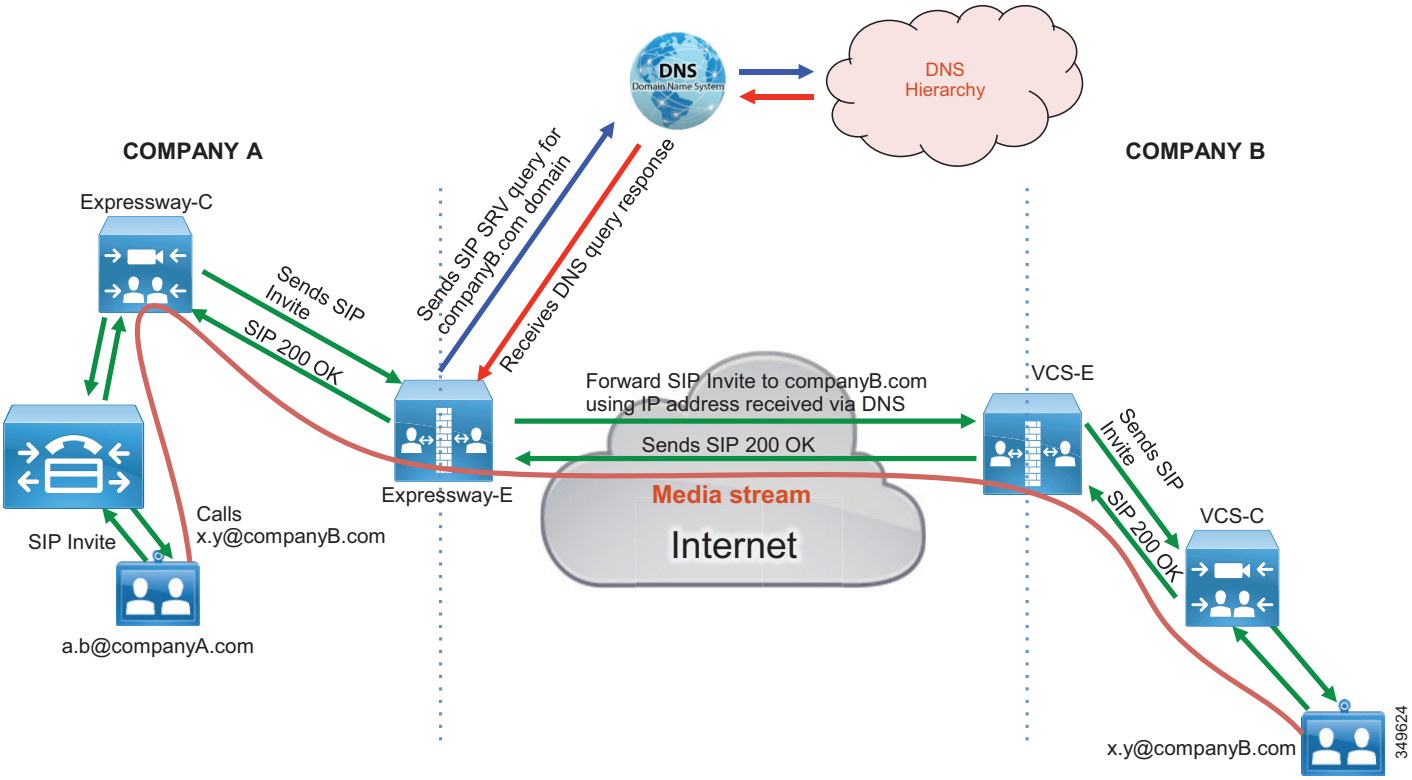
Business-to-Business（B2B）コミュニケーションには、URI ルーティングの目的でリモート組織のドメインを検索できる機能が必要です。これは、Expressway-E 上で DNS ゾーンを作成することによって実行されます。SIP と H.323 の両方がデフォルトで設定されます。これにより、Expressway-E は、自動的に、開始コールで使用されていない別のプロトコルを使用して DNS クエリを再発行できます。そのため、このコールは成功する可能性が高くなります。Expressway-C と Expressway-E は、コールを開始するために使用されたプロトコルを使用しますが、Expressway 上で SIP/H.323 間ゲートウェイ インターワーキングが有効になっている場合は自動的に別のプロトコルを使用しようとします。

Expressway-E の場合、SIP/H.323 間のインターワーキングは [オン（On）] に設定する必要があります。これにより、コールが H.323 コールとして受信された場合に、Expressway-E がそのコールを SIP に接続し、Unified CM への残りのコール レッグにネイティブ SIP を使用できます。同様に、H.323 システムへの発信コールは、Expressway-E に到達して H.323 に接続されるまで SIP コールを維持します。

インターネット経由で Business-to-Business（B2B）コミュニケーションを受信するには、外部 SIP レコードと H.323 DNS レコードが必要です。これらのレコードを使用すれば、他の組織は URI のドメインをそのコール サービスを提供している Expressway-E に解決できます。シスコの検証済みデザインには、Business-to-Business（B2B）コミュニケーション用の SIP レコード、SIPS SRV レコード、および H.323/H.225 SRV レコードが含まれています。RAS に使用される SRV レコードは、登録用のゲートキーパーを見つけるためにエンドポイントで使用されるレコードであり、Expressway-E ではこれが必要ありません。

C：図 4-10 は URI のドメインを解決する DNS プロセスを示し、C：例 4-1 は SRV 検索の例を示し、C：表 4-3 は Business-to-Business（B2B）コール シナリオに使用される DNS SRV レコードを示しています。

C：図 4-10　　DNS を使用した URI ダイヤリング



C：例 4-1　　ent-pa.com ドメインの SRV レコードの例

```
>nslookup
set type=srv
_sips._tcp.ent-pa.com

Non-authoritative answer:
_sips._tcp.ent-pa.com  SRV service location
    priority = 1
    weight   = 10
    port     = 5061
    srv hostname = expe.ent-pa.com.
```

C：表 4-3　　Business-to-Business（B2B）DSN SRV レコード

コール タイプ	SRV レコード	ポート	プロトコル
SIP Business-to-Business（B2B）	_sips._tcp.ent-pa.com	5061	TLS
	_sip._tcp.ent-pa.com	5060	TCP
	_sip._udp.ent-pa.com	5060	UDP
H.323 Business-to-Business（B2B）	_h323ls._udp.ent-pa.com	1719	RAS
	_h323cs._tcp.ent-pa.com	1720	H.225

Expressway-E 上の DNS ゾーンの設定方法については、『*Cisco Expressway Basic Configuration Deployment Guide*』の最新版を参照してください。

Business-to-Business（B2B）コールの IP ベース ダイヤリング

IP ベース ダイヤリングは、H.323 エンドポイントを使ってダイヤルする場合のほとんどのシナリオで使用されるよく知られた機能です。Cisco Collaboration Architecture では、SIP URI を使用するため、IP ベース ダイヤリングは必要ありません。ただし、コールの発着信に IP アドレスしか使用できない他の組織のエンドポイントと対話する場合は、Cisco Collaboration Architecture で着信コールと発信コールの両方に IP ベース ダイヤリングを使用できます。

アウトバウンド コール

アウトバウンド IP ダイヤリングは Expressway-E と Expressway-C ではサポートされますが、Cisco Unified Communications Manager では完全なネイティブ サポートはありません。ただし、後述するように、IP ベース ダイヤリングを使用するように Unified CM をセットアップすることができます。

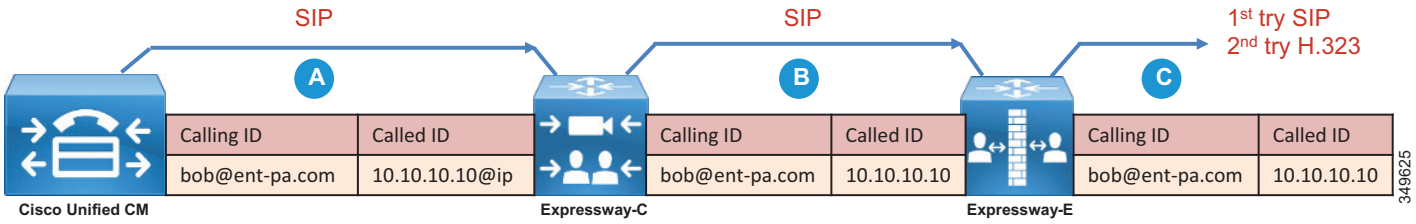
IP アドレス単独でダイヤルする代わりに、Cisco Unified CM 上のユーザは、10.10.10.10@ip のように SIP URI ベースの IP アドレスにダイヤルすることができます。ここで、「@ip」は、リテラルで、「external」、「offsite」、またはその他の意味のある単語に置き換えることができます。

Unified CM は、「ip」架空ドメインを Expressway-C にルーティングするように設定された SIP ルート パターンに一致します。Expressway-C はドメイン「@ip」を除外して、そのコールを（IP アドレス ダイヤリング用に設定されている）Expressway-E に送信します。

Expressway -E 上の不明な IP アドレス宛てのコールは [直接（Direct）] に設定する必要があります。コール制御が展開されていない場合は IP ベース アドレス ダイヤリングのほとんどが H.323 エンドポイントで設定されるため、Expressway-E は H.323 コールをパブリック IP アドレスにあるエンドポイントに直接送信できます。C：図 4-11 に示すように、コールは Expressway-E 上で接続されるまで SIP コールを維持します。

IP アドレス ダイヤリングを提供するための他のオプションがあります。1 つのオプションは、IP アドレス フィールドに使用される "." を記号 "*" に置き換えることです（例：
"10*10*10*10"）。Cisco Unified Communications Manager がそれをルート パターンに照らして照合し、Expressway が正規表現（regex）検索ルールを使用して "*" を "." に置き換えます。

C：図 4-11　　アウトバウンド IP ベース ダイヤリングの例



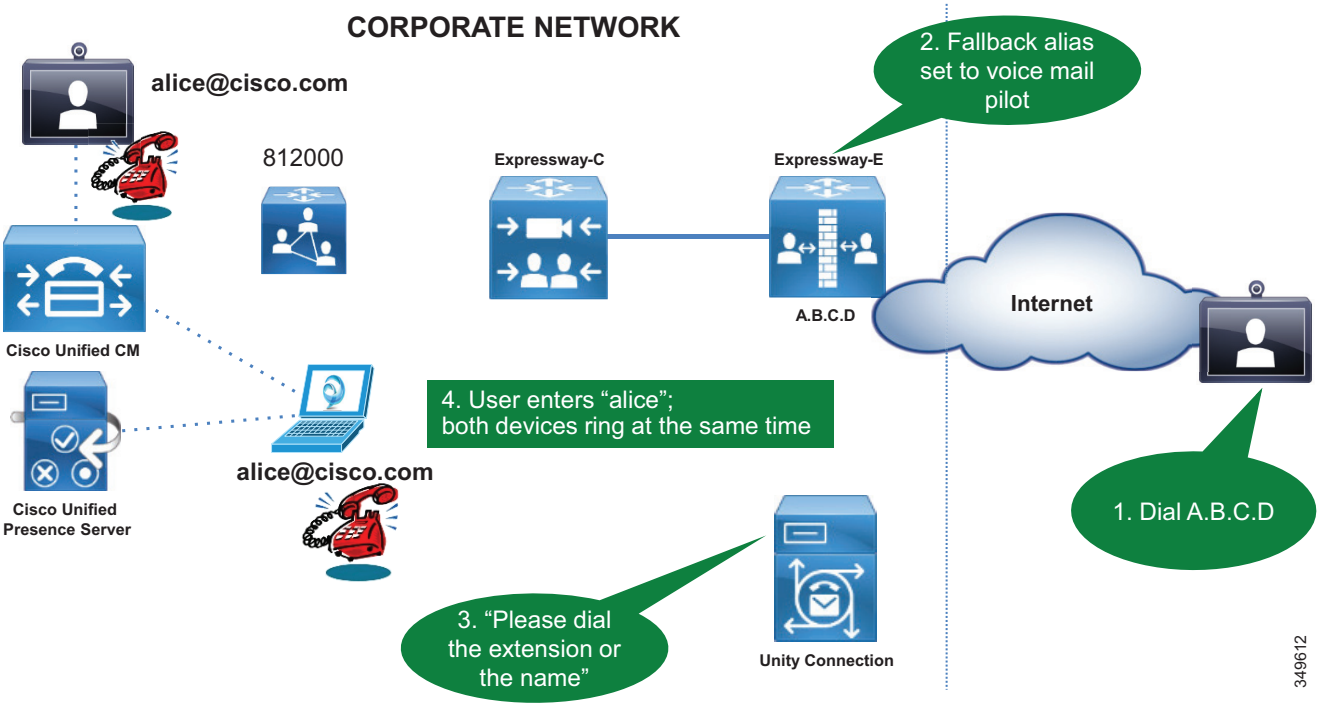
着信コール

IP ベースの着信コールは、Expressway-E で設定されたフォールバック エイリアスを使用します。インターネット上のユーザが Expressway-E 外部 LAN インターフェイスの IP アドレスにダイヤルすると、Expressway-E がそのコールを受信して、フォールバック エイリアスで設定されたエイリアスにコールを送ります。たとえば、コールを会議番号 80044123 または会議エイリアス meet@ent-pa.com に送信するようフォールバック エイリアスが設定されている場合、着信コールはそのような会議を担当する Cisco Meeting Server に送信されます。

IP アドレスとフォールバック エイリアス間の静的マッピングが制限されている場合は、フォールバック エイリアスを Cisco Unity Connection のパイロット番号に設定できます。この方法では、Unity Connection 自動応答機能を使用して、DTMF 経由で、または、Unity Connection でサポート可能な場合は音声認識によって、最終宛先を指定できます。

Unity Connection が Expressway-E の IP アドレスにダイヤルする外部エンドポイントの自動応答機能として使用されている場合は、Unity Connection の Unified CM トランク設定で [再ルーティング用コーリングサーチスペース（Rerouting Calling Search Space）] に設定することを忘れないでください。C：図 4-12 に、セットアップを示します。

C：図 4-12　　インバウンド IP ベース ダイヤリングの例



Expressway 経由の外部 XMPP フェデレーションの展開

XMPP フェデレーションは、モバイル & リモート アクセスと同じタイプのトラバーサル接続（Unified Communications トラバーサル）を利用します。XMPP フェデレーションはスタンドアロン サービスとして展開できます。また、同じ Unified Communications トラバーサル リンクを利用するモバイル & リモート アクセスと一緒に、同じ Expressway-C と Expressway-E のペア上に展開することもできます。

インスタント メッセージおよびプレゼンス フェデレーションを展開するには、次の標準作業を実行します。

1。 フェデレーション用のメールアドレスを検証します。

Expressway 経由の XMPP フェデレーションは、メールアドレスから XMPP アドレスへの変換をサポートしていません。メールアドレスから Jabber ID への変換は、IM と Presence サーバ フェデレーション モデルの機能です。この機能は、ユーザ エクスペリエンスを向上させ、電子メール URI 表記と JID URI 表記が異なる場合に XMPP フェデレーションに関する通信を簡

略化するためによく使用されます。Expressway 経由で XMPP フェデレーションを展開する場合は、ユーザ エクスペリエンスの向上と通信の簡略化という同じ目的が適用されます。IM と Presence ドメインは電子メール ドメインと同じドメインに設定することをお勧めします。また、UserID、メールアドレス表記、および Jabber ID に対して LDAP sAMaccount 名を使用することもお勧めします。コラボレーション アーキテクチャ全体では、反復可能でスケーラブルな URI 表記に関する包括的で一貫した戦略を策定することをお勧めします。

2. IM と Presence サービスが稼働可能で、XMPP フェデレーションがオフになっていることを確認してください。

   IM と Presence サーバ上の XMPP フェデレーションは、Expressway 上で設定されたフェデレーションと競合しないようにするため、オフにする必要があります。

3. サーバ証明書要件を解決します。

   Expressway-C および Expressway-E 用の証明書をセットアップする時期を事前に計画します。XMPP フェデレーションの一部としてチャット ノード エイリアスを使用する予定の場合は、チャット ノード エイリアス FQDN を証明書のサブジェクト代替名（SAN）フィールドに含める必要があります。これを事前に行うことによって、新しい証明書を生成する必要がなくなるだけでなく、Expressway-E 上での公開証明書に対する経費の増加が抑えられます。Expressway のセキュリティと証明書の詳細については、セキュリティーの章を参照してください。

4. Expressway-C 上で XMPP フェデレーション用のローカル ドメインを設定します。

5. Expressway-E を XMPP フェデレーションとセキュリティ用に設定します。

   このステップによって、フェデレーションと、外部フェデレーションに必要なセキュリティ レベルが有効になります。認証は必須であり、ダイヤルバック シークレット経由でセットアップされます。TLS 経由の通信保護が推奨設定です。許可または拒否する外部ドメインと外部チャット ノード エイリアスの承認もこのセクションで設定されます。

6. フェデレーテッド ドメインとチャット ノード エイリアス用の XMPP サーバを DNS ルックアップまたは静的ルートを使用してどのように配置するかを設定します。

   Expressway シリーズは、DNS SRV レコード経由のフェデレーションと静的ルート経由のフェデレーションをサポートしています。静的ルートは、DNS クエリを実行せずに外部ドメインに到達するパスを定義します。パブリック XMPP SRV レコードは、フェデレーションをサポートする外部ドメインを解決するために使用されます。これらのレコードは、オープン フェデレーション モデルを展開するときに、他の組織があなたの組織に到達するために必要です。

7. 正しいファイアウォール ポートが開いていることを確認します。

8. XMPP フェデレーションのステータスをチェックします。

SIP トランク経由の PSTN 音声接続用の Cisco Unified Border Element の展開

Cisco Unified Border Element は、PSTN 集中型アクセスに推奨されているセッション ボーダー コントローラです。これは、企業ネットワークと通信事業者ネットワークの間に境界ポイントとして展開されます。外部インターフェース経由の IP PSTN へのアクセスと、内部インターフェイス経由の企業ネットワークへのアクセスを提供します。集中型 PSTN サービスを有効にするため、企業ネットワークが通信事業者のネットワークに接続されている場所に展開する必要があります。

すべてのリモート サイトが中央の PSTN 接続を利用するため、Cisco Unified Border Element は高い冗長性を備えている必要があります。PSTN 中央サービスが使用できない場合は、ローカル PSTN アクセスを備えたオフィスだけが外部コールを発信できます。そのため、Cisco Unified Border Element をペアで展開して冗長性を確保することをお勧めします。

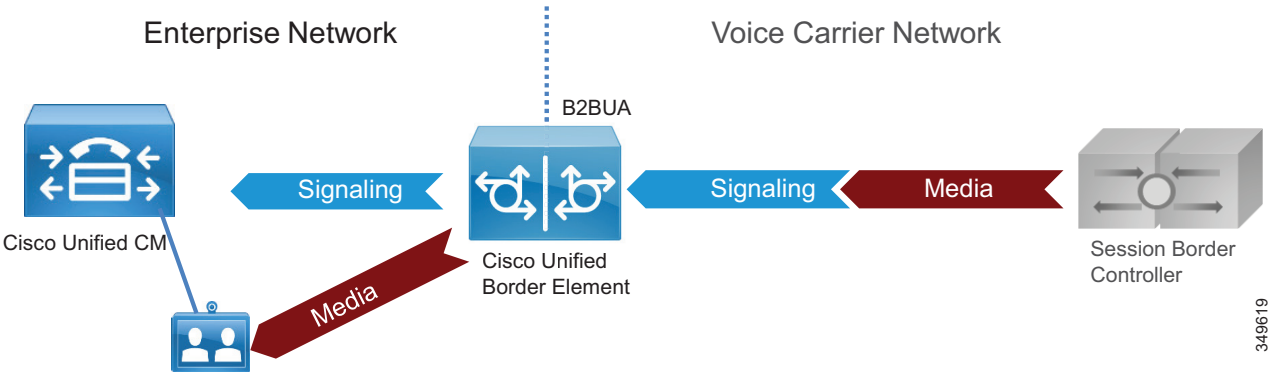
Unified Border Element は、Cisco IOS サービス統合型ルータ（ISR）プラットフォームとアグリゲーション サービス ルータ（ASR）プラットフォーム上でサポートされる Cisco IOS フィーチャ セットです。正しいプラットフォームの選択方法については、サイジング の章を参照してください。

Cisco Unified Border Element は、Unified CM からのセッションを終了して通信事業者ネットワークに向けて再発信する、または、その逆を実行するセッション ボーダー コントローラです。インターネット上で公開される Expressway-E とは対照的に、Cisco Unified Border Element はプライベート ネットワーク（社内ネットワークと通信事業者のネットワーク）間に展開されることに注意してください。通信事業者の視点では、集中型 PSTN へのトラフィックが Cisco Unified Border Element の外部インターフェイスから開始されます。企業の視点では、通信事業者からのトラフィックが Cisco Unified Border Element の内部インターフェイスから開始されます。この意味で、Cisco Unified Border Element はトポロジ隠蔽を実行しています。

Cisco Unified Border Element の展開は Expressway のそれとは異なります。前者は通信事業者ネットワーク（プライベートな管理および保護されたネットワーク）へのアクセスを提供するのに対して、後者はインターネットへのアクセスを提供します。そのため、Cisco Unified Border Element の展開では DMZ が必要ありません。

C：図 4-13 に示すように、この推奨アーキテクチャでは、Unified Border Element が、通信事業者ネットワークに対する WAN インターフェイスと企業ネットワークに対する LAN インターフェイスを備えています。

C：図 4-13　　IP PSTN アーキテクチャ

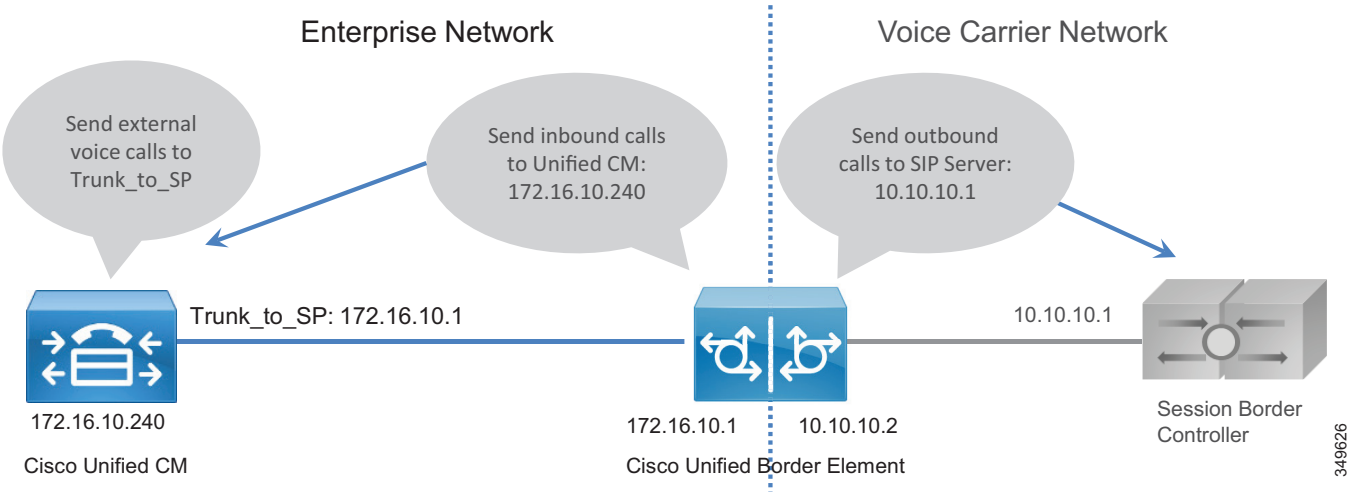


Cisco Unified Border Element は次の機能を実行します。

- C：図 4-14 に示すアドレス変換とポート変換を含むトポロジ隠蔽。Unified CM からのすべてのトラフィックが Unified Border Element 内部インターフェイスに送信され、通信事業者ソフトスイッチからのすべてのトラフィックが Unified Border Element 外部インターフェイスに送信されます。これらの間の直接接続は存在しません。C：図 4-14 に、Cisco Unified CM 上のトランキング設定と Unified Border Element 上の音声ルートの詳細を示します。
- 遅延オファーから早期オファーへの変換とその逆変換
- メディア インターワーキング：インバンドおよびアウトオブバンド DTMF サポート、DTMF 変換、FAX パススルーおよび T.38 FAX リレー、音量およびゲイン制御
- コール アドミッション制御（CAC）：CAC は、CPU、メモリ、コール到着スパイク検出などのリソース消費に基づいて Unified Border Element によって実行できます。CAC はインターフェイス レベルでまたはグローバルに実装できます。Unified CM 上で設定される CAC はロケーションベースですが、Unified Border Element 上で設定される CAC はリソースベースです。Unified Border Element のオーバーサブスクリプションを避ける目的、およびセキュリティ上の理由から、リソースベースの CAC を推奨します（コラボレーション エッジのセキュリティーに関するセクションを参照）。

- RTP/SRTP 間インターワーキング、SIP 不正パケットの検出、非ダイアログ RTP パケットの破棄、SIP リスニング ポートの設定、ダイジェスト認証、同時コール数制限、コール レート制限、電話料金の詐欺行為からの保護、および複数のシグナリングとメディアの暗号化オプションを含むセキュリティ機能
- 保留、転送、および会議を含む通話中補足サービス
- PPI/PAI/ プライバシーおよび RPID：通信事業者との ID ヘッダー インターワーキング
- 複数の通信事業者からの SIP トランクに対する同時接続
- マルチキャスト保留音（MoH）からユニキャスト MoH への変換
- 課金統計情報と呼詳細レコード（CDR）の収集

C：図 4-14　　Cisco Unified Border Element のトランキングに関する留意点



PSTN ゲートウェイ

レガシー PSTN ゲートウェイは、サイトごとに独自の PSTN 接続が割り当てられる分散アーキテクチャで展開されます。集中型 PSTN アクセスには Cisco Unified Border Element の使用をお勧めしますが、日常業務の実行を外部コールに大きく依存しているサイトのバックアップとして PSTN ゲートウェイを使用することもできます。

この場合は、同時 ISDN チャネル数が集中型 PSTN への同時コール数を大きく下回る可能性があります。これは、それらがバックアップ シナリオでしか使用されないためです。たとえば、通常の状況で集中型 PSTN への 30 本の同時コールが許容される場合は、バックアップ シナリオでしか使用されないバックアップ ISDN ゲートウェイを 2 つの BRI チャネルだけをサポートする規模に設定できます。

シスコ音声ゲートウェイは以下をサポートしています。

- DTMF リレー機能
- 補足サービス サポート：補足サービスは、保留、転送、会議などの基本的なテレフォニー機能です。
- FAX パススルーと T.38 FAX リレー

PSTN ゲートウェイはさまざまなプロトコル（SCCP、MGCP、H.323、SIP）をサポートしています。SIP は、Cisco Collaboration ソリューション全体と調和しているうえ、新しい音声製品やビデオ製品に選択されたプロトコルであるため、お勧めのプロトコルです。

音声ゲートウェイ機能は、適切な PVDM とサービス モジュールまたはカードが実装されたすべての Cisco ISR 上で有効になっています。

コラボレーション エッジのハイ アベイラビリティー

ハイ アベイラビリティは、コラボレーション システムの設計と展開における重要な側面です。コラボレーション エッジによって、冗長性、ロード シェアリング、およびコール ライセンス共有が実現されます。

Expressway-C と Expressway-E のハイ アベイラビリティ

Expressway-C と Expressway-E はクラスタで展開することをお勧めします。クラスタごとに最大 6 つの Expressway ノードと最大 N+2 の物理冗長性を設定できます。クラスタ内のすべてのノードがアクティブです。クラスタ設定の詳細については、『*Cisco Expressway Cluster Creation and Maintenance Deployment Guide*』の最新版を参照してください。

Expressway クラスタは設定の冗長性を提供します。クラスタ内で設定される最初のノードは*パブリッシャ*で、その他のすべてのノードは*サブスクライバ*です。設定はパブリッシャ内で実行され、自動的に他のノードにレプリケートされます。

Expressway クラスタは、コール ライセンス共有と回復力を提供します。すべてのリッチ メディア セッションがクラスタ内のノード間で等しく共有されます。コール ライセンスはノードごとに設定されたライセンスによって供与されます。

次のルールが Expressway クラスタリングに適用されます。

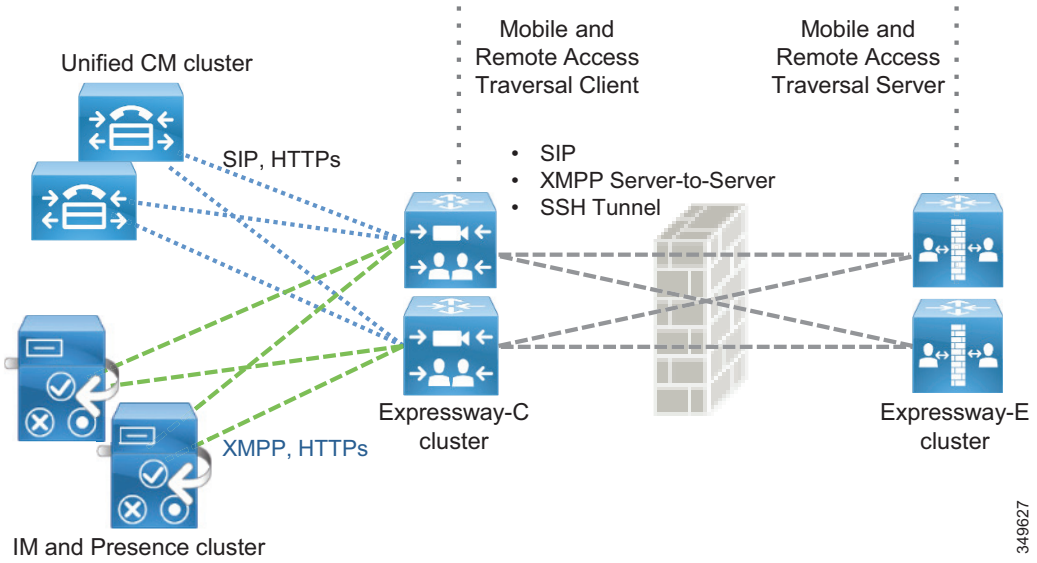
- Expressway-C ノード タイプと Expressway-E ノード タイプを同じクラスタ内に混在させることはできません。
- クラスタ内のすべてのノードで、ゾーン、認証、およびコール ポリシーの設定を同じにする必要があります。
- 設定の変更はマスター ノードでのみ行う必要があり、この変更によってレプリケーション時にクラスタ内の他のピア上の設定が上書きされます。
- あるノードが使用できなくなった場合は、そのノードがクラスタに供与していたライセンスが 2 週間後に使用できなくなります。
- Expressway-C クラスタと Expressway-E クラスタには同じ数のノードを展開します。
- クラスタ全体に同じ OVA テンプレートを展開します。
- クラスタ内のすべてのノードは、他のすべてのクラスタ ノードへの最大ラウンドトリップ時間を 30 ms 以内にする必要があります。したがって、WAN 経由のクラスタリングは遅延の制約があるためお勧めできません。
- 同じクラスタ内のすべてのノードに対して同じクラスタ事前共有キーを使用する必要があります。
- データベース レプリケーションのために、クラスタ内のすべてのノードで H.323 を有効にする必要があります。同時に、インターネットから送られてくる H.323 コールもブロックする必要がある場合は、外部 LAN インターフェイス上の H.323 トラフィックをドロップするファイアウォール ルールを使って Expressway-E を設定できます。

- 同じ Expressway-C と Expressway-E のペアでモバイル & リモート アクセスと Business-to-Business（B2B）コミュニケーションが有効になっている場合は、Unified CM と Expressway-C 間の SIP トランク上で使用されている SIP ポート番号をデフォルトの 5060 または 5061 から変更する必要があります。
- DNS SRV レコードは、クラスタに対して使用可能にする必要があり、クラスタのノードごとに A レコードまたは AAAA レコードを含む必要があります。

Expressway-C は内部ネットワークに、Expressway-E は DMZ にそれぞれ展開されるため、モバイルおよびリモート アクセス用のユニファイド コミュニケーション トラバーサル ゾーンを介して Expressway-C と Expressway-E を接続する必要があります。Business-to-Business（B2B）コールには別個のトラバーサル ゾーンが必要です。このゾーンでは Expressway-C 用のトラバーサル クライアント ゾーンと Expressway-E 用のトラバーサル サーバ ゾーンの名前が保持されます。トラバーサル サーバ、トラバーサル クライアント、およびユニファイド コミュニケーション トラバーサル ゾーンには、Expressway-C と Expressway-E のすべてのノードが含まれているので、いずれかのノードに到達できない場合は代わりにクラスタの別のノードに到達します。

C：図 4-15 に示すように、Expressway-C が Cisco Unified CM、IM and Presence、および Unity Connection の各クラスタのすべてのサーバに接続するため、接続パス全体でハイ アベイラビリティと冗長性が確保されます。

C：図 4-15　　Expressway サービス接続



C：図 4-15 に、Unified Communications トラバーサル ゾーンとモバイル & リモート アクセスに組み込まれているハイ アベイラビリティを示します。ただし、次の説明は、Unified Communications トラバーサル ゾーンと標準の（クライアントとサーバ）トラバーサル ゾーンの両方に適用されます。

Expressway-C 上に設定されたトラバーサル クライアント ゾーンには、対応する Expressway-E クラスタのすべてのクラスタ ノードの完全修飾ドメイン名を含める必要があります。同様に、トラバーサル サーバ ゾーンはすべての Expressway-C クラスタ ノードに接続する必要があります。これは、Expressway-C 証明書のサブジェクトの別名に Expressway-C クラスタ ノードの FQDN を含め、**TLS 検証サブジェクト名**を Expressway-C クラスタの FQDN と同一に設定することによって実現されます。これにより、トラバーサル ゾーン全体にクラスタ ノードのメッシュ構成が形成され、最後のクラスタ ノードが使用不能になるまでトラバーサル ゾーンのハイ アベイラビリティが維持されます。

Expressway-C はトランク経由で Unified CM に接続して、Business-to-Business（B2B）の着信コールと発信コールをルーティングします。Unified CM は Expressway-C へのトランキングも行います。ハイ アベイラビリティを維持するために、各 Expressway-C クラスタ ノードの完全修飾ドメイン名を Unified CM 上のトランク設定に列挙する必要があります。逆に、Unified CM クラスタの各メンバーの完全修飾ドメイン名（FQDN）を Expressway-C のネイバー ゾーン プロファイルに列挙する必要があります。

ここでも、メッシュ状のトランク構成が形成されます。Unified CM は、SIP Options Ping 経由でトランク設定内のノードのステータスをチェックします。あるノードが使用できなくなると、Unified CM はそのノードを運用停止にして、そのノードに対するコールをルーティングしなくなります。Expressway-C も SIP OPTIONS Ping 経由で Unified CM からのトランクのステータスをチェックします。コールは、アクティブかつ使用可能として示されているノードにのみルーティングされます。これにより、トランク設定の両側にハイ アベイラビリティが提供されます。

DNS SRV レコードは、インバウンド Business-to-Business（B2B）トラフィックに対する Expressway-E の可用性を高めることができます。高可用性を確保するためには、クラスタ内のすべてのノードを SRV レコード内に同じ優先度と同じ重要度で列挙する必要があります。これにより、すべてのノードを DNS クエリで返すことができます。DNS SRV レコードは、クライアントがルックアップに費やす時間を最小にするために役立ちます。これは、SRV レコード内に列挙されたすべてのノードを DNS 応答に含めることができるためです。通常は、遠端サーバまたは遠端エンドポイントが DNS 応答をキャッシュし、応答が受信されるまで DNS クエリで返されたすべてのノードを試します。これにより、コールが成功する確率が高まります。

さらに、Expressway クラスタは、クラスタ全体でのリッチ メディア ライセンス共有をサポートします。クラスタからノードが削除された場合は、そのコール ライセンスの共有が次の 2 週間だけ継続されます。どの Expressway も、その物理能力を上回るライセンスを保持することはできても、その物理能力を上回る Rich Media ライセンスを処理することはできません。

Cisco Unified Border Element のハイ アベイラビリティ

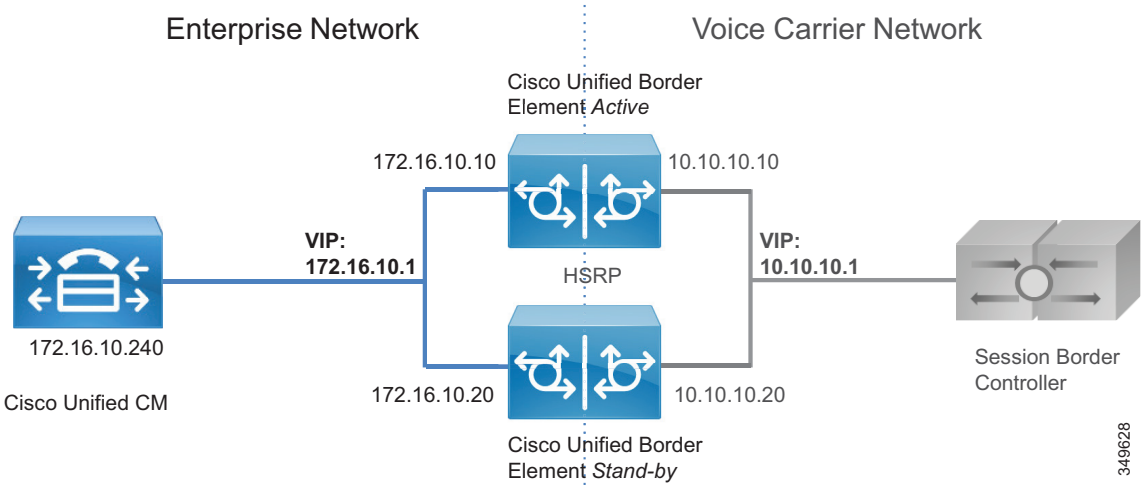
Cisco Unified Border Element のハイ アベイラビリティは複数の方法で実現できます。推奨アーキテクチャでは、コールの保存によるボックスツーボックス冗長性をお勧めします。これは、Unified Border Element で障害が発生した場合にシグナリングとメディアの両方のコールの保存が実施されるためです。

Unified Border Element サーバは、次のアクティブ / スタンバイ モデルのペアで展開されます。アクティブ Unified Border Element がダウンすると、スタンバイ Unified Border Element が起動され、すべてのアクティブ セッションが移行されます。これにより、シグナリングとメディアの両方のハイ アベイラビリティが提供されます（C：図 4-16 を参照）。

Hot Standby Routing Protocol（HSRP）テクノロジーは、1 つのルータの可用性に頼らずに、ネットワーク上のホストからの IP トラフィックをルーティングすることによって、ネットワークのハイ アベイラビリティを実現します。ルータのグループで HSRP を使用して、アクティブ ルータとスタンバイ ルータを選択します HSRP は内部と外部の両方のインターフェイスをモニタします。インターフェイスのいずれかがダウンした場合は、デバイス全体がダウンしたと見なされ、スタンバイ デバイスがアクティブになってアクティブ ルータの役割を引き継ぎます。

ボックスツーボックス冗長性は、HSRP プロトコルを使用してルータの HSRP アクティブ / スタンバイ ペアを形成します。アクティブ サーバとスタンバイ サーバは、同じ仮想 IP アドレスを共有し、ステータス メッセージを継続的に交換します。C：図 4-16 に示すように、Unified Border Element セッション情報がルータのアクティブ / スタンバイ ペア全体で共有されます。ここで、172.16.0.1 と 10.10.10.10 は Cisco Unified Border Element ペアの仮想 IP アドレスです。これにより、アクティブ ルータが予定どおりにまたは予定外の理由で稼働停止状態になった場合に、すぐにスタンバイ ルータがすべての Unified Border Element コール処理の役割を引き継ぐことができます。

C：図 4-16　Cisco Unified Border Element のボックスツーボックス冗長性



音声ゲートウェイのハイ アベイラビリティー

PSTN ゲートウェイは、物理インターフェイスを介して直接 PSTN ネットワークに接続します。ゲートウェイがダウンすると、PSTN とのすべての通信がクリアされます。HSRP などのメカニズムは、このケースではメリットがありませんが、通信事業者向けの IP トランク経由の PSTN アクセスのケースではメリットがあります。ゲートウェイ相互接続を使用した集中型 PSTN が展開される場合もありますが、Unified Border Element と違って、TDM ベースの PSTN ゲートウェイ展開は基本的に分散型です。また、PSTN 音声ゲートウェイは Unified Border Element ほど多くのコール量を管理できません。PSTN の特性上、このシナリオではメディア保存ができません。

ただし、同じ Unified CM ルート グループ内の複数のゲートウェイをコールがロード バランシングされるように設定することによって、シグナリング回復力を提供できます。グループ内のゲートウェイのいずれかがダウンすると、すべてのコールが破棄されますが、残りの使用可能なゲートウェイのいずれかを使用して新しいコールが確立されます。

コラボレーション エッジのセキュリティー

ここでは、コラボレーション エッジでのセキュリティの実装方法について説明します。

Expressway-C と Expressway-E のセキュリティー

Expressway-C と Expressway-E 上のセキュリティは、ネットワーク レベルとアプリケーション レベルでさらに分割することができます。ネットワーク レベルのセキュリティにはファイア ウォール ルールや侵入からの保護などの機能が含まれるのに対して、アプリケーション レベルのセキュリティには認可、認証、および暗号化が含まれます。

ネットワーク レベル保護

Expressway-C と Expressway-E のネットワーク レベル保護は、2 つの主なコンポーネント（ファイアウォール ルールと侵入防御）で構成されます。

ファイアウォール ルールは次の機能を有効にします。

- トラフィックを許可または拒否する送信元 IP アドレスのサブネットを指定します。
- 拒否対象のトラフィックを破棄または拒否するかを選択します。
- SSH や HTTP/HTTPS などの既知のサービスを設定する、または、トランスポート プロトコルとポート範囲に基づいてカスタマイズされたルールを指定します。
- Expressway-E 上の LAN 1 インターフェイスと LAN 2 インターフェイスで別々のルールを設定します。

悪意のあるトラフィックを検出およびブロックし、辞書ベースでの不正ログイン攻撃から Expressway を保護するためには、自動侵入保護機能を使用する必要があります。

自動化された侵入保護は、システム ログ ファイルを解析して、SIP、SSH、Web/HTTPS などの特定のサービス カテゴリへのアクセスの連続的な失敗を検出することによって機能します。指定された時間内の失敗回数が設定されたしきい値を超えた場合は、送信元ホスト IP アドレス（侵入者）と宛先ポートが、指定された期間ブロックされます。その期間が過ぎると、自動的にホスト アドレスのブロックが解除されるため、一時的に設定が間違っていた正規のホストがロックアウトされなくなります。

モバイルおよびリモート アクセス

モバイルおよびリモート アクセスでは、インターネット上のクライアントと Expressway-C の間の設定オプションは TLS、SRTP、HTTPS、および XMPP だけです。クライアントと Expressway-C の間のすべてのトラフィックが常に暗号化されます。

Unified CM と Expressway-C の間の接続は設定に応じて、暗号化と認証が行われます。Unified CM が混合モードの場合は、メディアとシグナリングのエンドツーエンド暗号化をお勧めします。

Cisco Unified CM と Expressway-C の間のセキュアな通信にはセキュリティ証明書が必要です。証明書はサーバとクライアントのアイデンティティを提供し、Expressway-C、Expressway-E、Unified CM、および Unified CM IM and Presence Service に証明書を展開する必要があります。推奨される設定は、認証局（CA）を使用して証明書に署名することです。

CA はプライベートにもパブリックにもできます。プライベート CA 展開にはコスト効率が高いというメリットがありますが、この証明書は組織内部でしか有効ではありません。パブリック CA はセキュリティを向上させ、すべての組織から信頼されます。そのため、異なる組織間の通信に広く利用されています。

コストを削減するために、Expressway-C 証明書が社外で認定されていない内部 CA によって署名されている場合があります。この場合は、Expressway-C と Expressway-E の接続を確立するために、内部 CA 証明書を Expressway-E の信頼された CA 証明書リストに含めることが重要です。Expressway-E 証明書は、パブリック CA によって署名される必要があります。

C：表 4-4 に、証明書展開に対するパブリック アプローチとプライベート アプローチの概要を示します。証明書の詳細については、セキュリティーの章を参照してください。

C：表 4-4　　パブリック証明機関、プライベート証明機関、および証明書

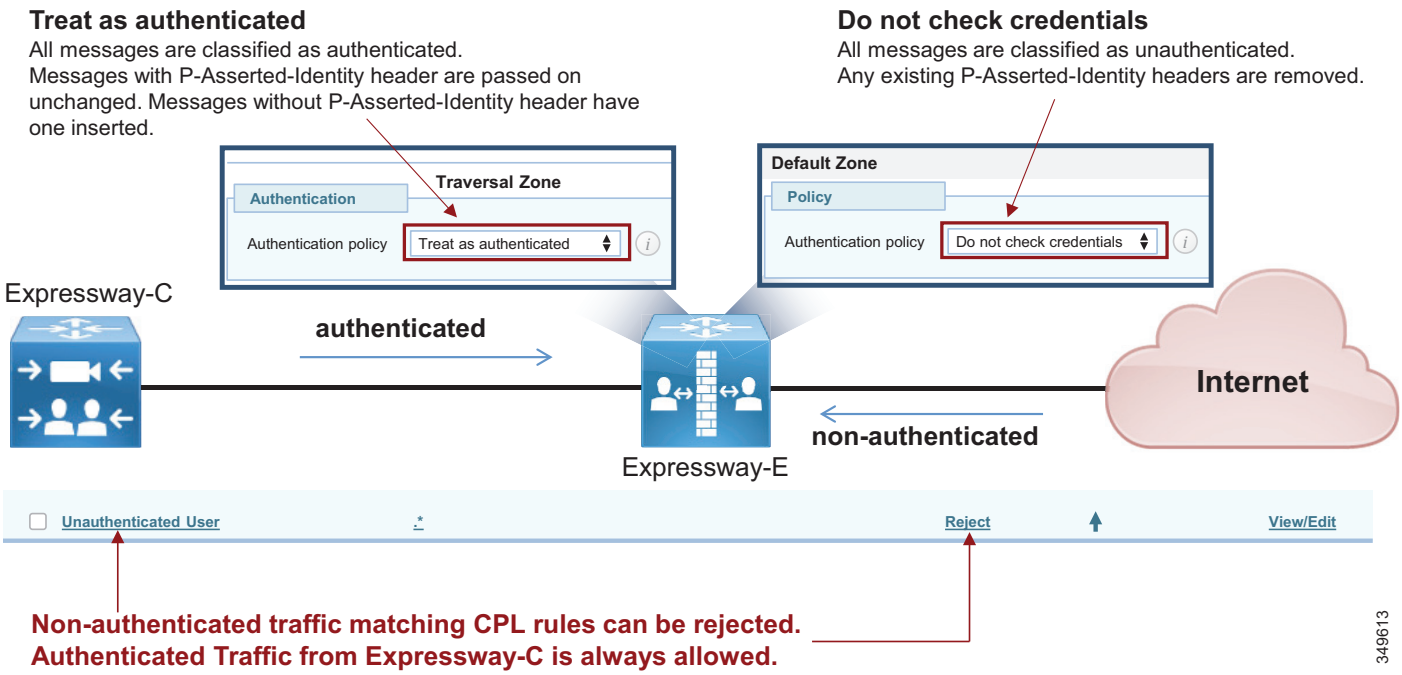
	Unified CM	IM and Presence Service	Expressway-C	Expressway-E
証明書の署名者	内部 CA	内部 CA	内部 CA	パブリック CA
信頼リストへの掲載	内部 CA 証明書	内部 CA 証明書	内部 CA 証明書とパブリック CA 証明書	内部 CA 証明書とパブリック CA 証明書

Business-to-Business（B2B）コミュニケーション

Business-to-Business（B2B）コミュニケーションの保護には、認証、暗号化、および認可が含まれます。Business-to-Business（B2B）コミュニケーションでは、デフォルトで、認証されたトラバーサル リンクが使用されます。また、トラバーサル リンクは、Expressway-C と Expressway-E の間の相互認証される Transport Layer Security（MTLS）接続によって検証される公開キー インフラストラクチャ（PKI）の利点を活用できます。Business-to-Business（B2B）トラバーサル リンクがモバイルおよびリモート アクセスと同じ Expressway-C および Expressway-E インフラストラクチャに展開される場合は、トラバーサル ゾーンが Expressway-C クラスタ ノードと Expressway-E クラスタ ノードの IP アドレスではなく FQDN を使用することを確認してください。これにより、各サーバの証明書を使用して、提示された証明書をトラバーサル接続に対して信頼された証明書に照らして検証するのが容易になります。

着信コールは認証済みか未認証かによって区別できます。この区別は、保護されたリソースへのアクセスの承認に使用できます。コール認証の設定は、ゾーン設定レベルで実施されます。例として、Expressway-E デフォルト ゾーン認証ポリシーを「クレデンシャルを確認しない」に設定できます。これにより、C：図 4-17 に示すように、不明なリモート Business-to-Business（B2B）コールが未認証としてマークされます。

C：図 4-17　　コール認証



これらのコールでは、PSTN などの保護されたリソースへのアクセスを制限する必要があります。これは、Call Processing Language（CPL）ルールをゲートウェイ アクセスに使用されるプレフィクスへのアクセスをブロックする正規表現を使用して設定することによって実現されます

例として、範囲 80XXXXXX の一連のデバイスだけにコールが許可され、外部のインターネット宛先からの +E.164 番号、ゲートウェイ アクセス、その他のサービス（ここでは 0 と 9 で示す）が禁止されている企業を想定します。この場合、ルールは C：表 4-5 に示すように設定できます。

C：表 4-5　　拒否ベースのポリシーの例

ソース タイプ	[接続先（Destination）]	アクション
デフォルト ゾーン	8 [1-9] \ d{6} @ent-pa¥ com	却下
デフォルト ゾーン	[09]\d*@ent-pa\.com	却下
デフォルト ゾーン	\+\d*@ent-pa\.com	却下
デフォルト ゾーン	.*@ent-pa\.com	許可
デフォルト ゾーン	.*	却下

ルールは、トップダウンで照合されます。C：表 4-5 のルールの例では、次の場合にコールが拒否されます。

- 宛先が 8 で始まり、その後に 1 ～ 9 の 1 桁の数字、さらに 6 桁、さらに会社のドメインが続く。
- 宛先が 0 または 9 で始まり、その後に任意の桁数、さらに会社のドメインが続く。
- 宛先が +E.164 番号に一致し、その後に会社のドメインが続く。

C：表 4-5 の最初の 3 つのルールによって拒否されなかったコールは、宛先に会社のドメインが含まれていれば、4 番目のルールによって許可されます。

その他の宛先は、C：表 4-5 の最後のルール（"deny all"）によって拒否されます。これには、ドメインが指定されていないコールが含まれます。

要件と推奨事項

- Business-to-Business（B2B）トラバーサル クライアント ゾーンとトラバーサル サーバ ゾーンで H.323 をオフにします。これにより、Expressway-C と Expressway-E の間のすべてのトラフィックが確実に暗号化されます。コールがトラバーサル サーバ ゾーンに送信される前（インバウンド コールの場合）およびインターネットに送信される前（アウト バウンド コールの場合）に、H.323 インターワーキングが Expressway-E 上で実行されます。
- Business-to-Business（B2B）トラバーサル ゾーンのトラバーサル クライアント側（Expressway-C）のメディア暗号化を**ベスト エフォート**に設定します。Expressway-E Business-to-Business（B2B）トラバーサル サーバ、デフォルト ゾーン、および Business-to-Business（B2B）DNS ゾーンに、同じメディア暗号化設定（**ベスト エフォート**）を使用します。これは、SIP コールの暗号化が常に Expressway-C 上で実施されることを意味します。リモート システムで暗号化がサポートされない場合は、Expressway-C が非暗号化コールをセットアップします。強力な暗号化ポリシーが必要な場合は、メディア暗号化を**強制暗号化**に設定します。この場合、ベスト エフォートの場合と同様にコールが暗号化されます。違いは、リモート システムで暗号化がサポートされない場合に、非暗号化フォールバックなしでコールが終了することです。
- Unified CM と Expressway-C 間の SIP トランクのシグナリング暗号化には TLS を使用します。

モバイルおよびリモート アクセス シナリオと Business-to-Business（B2B）コール シナリオでの証明書の設定：

- 証明書に関する一般的な要件として、Expressway-C と Expressway-E の完全修飾 DNS 名（FQDN）が証明書のホスト名と一致する必要があります。
- Business-to-Business（B2B）コミュニケーションには、証明書に関する他の要件はありませんが、モバイル / リモート アクセス（MRA）には追加の要件があります。Expressway でのモバイルおよびリモート アクセス用の証明書のセットアップ方法について、詳しくはセキュリティーの章を参照してください。

Cisco Unified Border Element のセキュリティー

インターネット接続とは異なり、IP トランク経由の PSTN 接続は、通信事業者から提供されたプライベート ネットワークを介して配信されます。つまり、この接続は制御されたネットワークです。したがって、インターネット エッジ用に展開されたセキュリティは、IP PSTN アクセス用に展開されたセキュリティとは異なります。Cisco Unified Border Element と通信事業者間にはファイアウォールが存在しません。ただし、特定のケースでは、企業と電気通信プロバイダーでエンタープライズ DMZ を使用する必要があります。

通信事業者と企業ネットワークの間では、通常、トラフィックが暗号化されずに送信されます。会社のポリシーによって、内部のエンタープライズ トラフィックを暗号化できる場合とできない場合があります。このようなケースでは、Unified Border Element で TLS/TCP 変換と SRTP/RTP 変換を実行できます。複数のゲートウェイが展開されている場合は、内部 CA を使用して Unified Border Element 証明書に署名することをお勧めします。

Unified Border Element はファイアウォールなしで展開されるため、さまざまなレイヤで保護されます。たとえば、通信事業者のセッション ボーダー コントロールのみに PSTN 側からのコールの開始を許可し、Unified CM のみに内部ネットワーク側からのコールの開始を許可するアクセス コントロール リストを作成できます。

Unified Border Element は、電話料金の詐欺行為やテレフォニー サービス拒否（TDoS）攻撃からも保護されます。ラージ パケット到着率は、CPU、メモリ、帯域利用率、およびコール到着スパイク検出に基づくコール アドミッション制御メカニズムを通して削減することもできます。

音声ゲートウェイのセキュリティ

PSTN ゲートウェイは、顧客ネットワークに 1 つのインターフェイス、PSTN 上に 2 つ目のインターフェイスを備えています。これらのインターフェイスは社内ネットワーク内に展開され、インターネットからは到達できません。PSTN は本質的にセキュアなので、ゲートウェイを保護するための特定のツールは存在しません。ただし、インターネットにアクセス可能なルータ上にゲートウェイが展開されている場合は例外です。この場合は、ゲートウェイ上の Cisco IOS 機能を使用してファイアウォールと侵入防御を実行できます。その他の場合は、ゲートウェイを保護するために必要な特定のツール（サービス拒否（DoS）攻撃からの保護など）はありません。

ただし、エンドポイントからゲートウェイへのメディアを常に暗号化することをお勧めします。このようなケースでは、ゲートウェイで TLS と SRTP が使用されます。この場合は、CA 署名証明書を使用することをお勧めします。

コラボレーション エッジ ソリューションのスケーリング

展開されたコラボレーション エッジ クラスタの数は、コール制御クラスタの数ではなく、インターネットへの接続ポイントの数に左右されます。複数の Unified CM および IM and Presence クラスタと、複数の TelePresence Conductor クラスタを使用しているお客様は、単一のインターネット接続ポイントが設置されていれば、単一のインターネット エッジを所有していることになります。通信事業者が PSTN ネットワークへの接続ポイントを複数提供している場合は、同じ環境に複数の PSTN 外線が設置されている可能性があります。

インターネット エッジ ソリューションのスケーリング

複数のインターネット エッジが展開されている場合は、コラボレーション トラフィックを最も近いインターネット エッジに送信するためのルーティング ルールを正しく設定することが重要です。

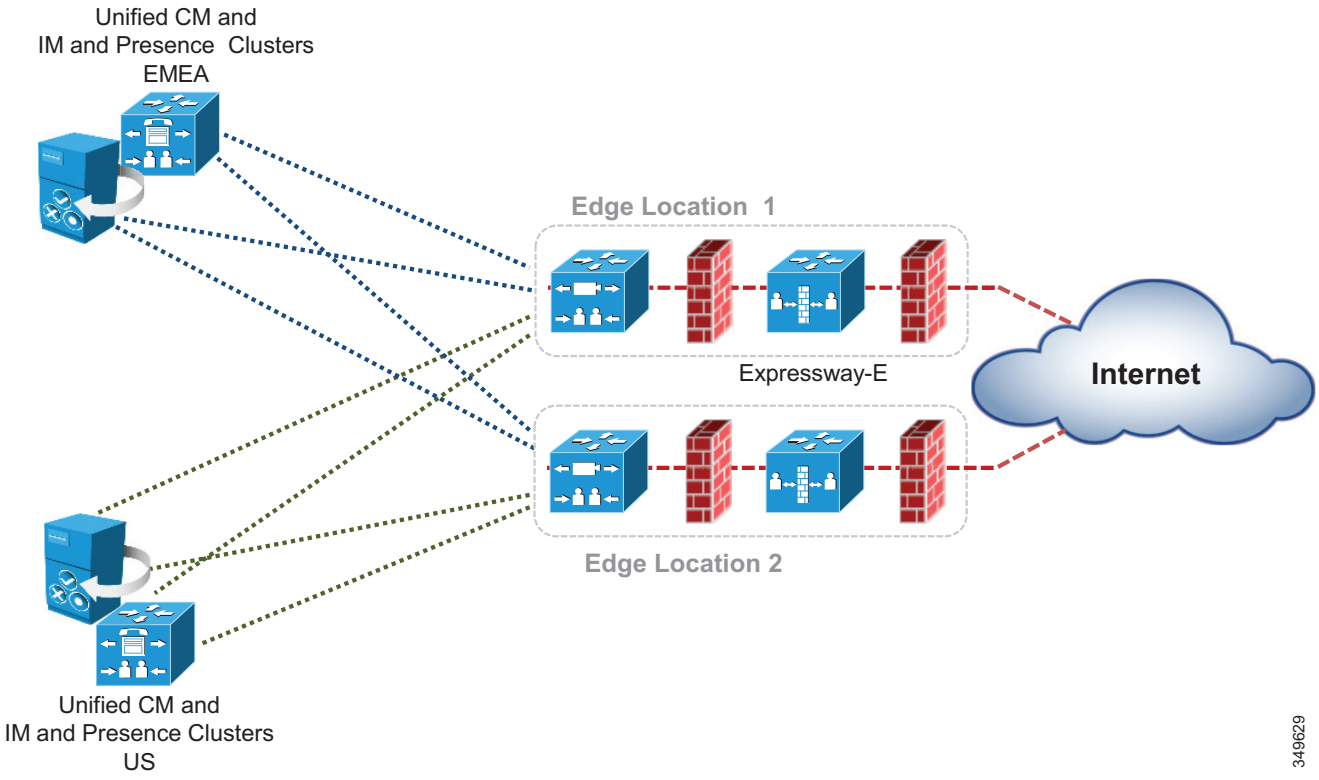
モバイルおよびリモート アクセス

複数の Unified CM および IM and Presence クラスタが展開されている場合は、すべての Expressway-C がすべての Unified CM クラスタを検出する必要があります。Expressway-C が一部のクラスタしか検出しない場合は、検出されたクラスタに属しているユーザに関する登録しかプロキシできません。

Expressway-C でまだ未検出の Unified CM and IM and Presence クラスタに属するクライアントから登録要求が発行された場合、そのクライアントはログインできません。この理由で、C：図 4-18 に示すように、ユーザのモビリティが有効になっている場合に各 Expressway-C がすべての Unified CM and IM and Presence クラスタを検出することが重要です。

加えて、いくつかの Unified CM and IM and Presence クラスタが同じ SIP ドメインを共有している場合は、Unified CM クラスタで ILS を有効にすることが重要です。ILS 機能は、各 Unified CM クラスタに同じネットワーク内の他のクラスタを認識させ、特定のユーザがどのクラスタ（つまりホーム）に属するかを Expressway-C に示すことができます。そのためには、Unified CM ユーザ ページ設定で [ホーム クラスタ（home cluster）] 設定が有効になっている（チェックボックスがオンになっている）必要があります。

C：図 4-18　　複数の Unified CM および IM and Presence クラスタのサービス検出



複数のインターネット エッジが展開されている場合は、着信要求の負荷がそれらの間でどのように分散されるかを理解することが重要です。インターネット エッジが同じデータセンターまたは同じエリアに展開されている場合は、DNS SRV レベルでロード バランシングを実行できます。たとえば、企業ネットワークにモバイル & リモート アクセス用の 3 つのインターネット エッジが含まれており、それぞれが 2 つの Expressway-E ノードと Expressway-C ノードのクラスタで構成されている場合は、**_collab-edge._tls.ent-pa.com** に 6 つすべての Expressway-E レコードが同じ優先度と重要度で追加されます。これにより、登録とコールがさまざまな Expressway-E クラスタと Expressway-C クラスタに均等に分配されます。

モバイル & リモート アクセス接続エンドポイントが特定の Expressway クラスタ ペアを介して登録されると、クライアントが切断されるか、クライアントのスイッチがオフにされるまで接続されたままになります。

ただし、Expressway クラスタが地理的地域全体に展開されている場合は、エンドポイントが確実に最も近い Expressway-E クラスタを使用するようにするため、DNS SRV の優先度と重要度のレコードに加えて何らかのインテリジェント メカニズムが必要になります。

たとえば、ある企業が 2 つの Expressway クラスタを使用しており、1 つは米国（US）に、もう 1 つはヨーロッパ（EMEA）に設置されている場合、US に住んでいるユーザは US 内の Expressway-E クラスタに転送され、ヨーロッパに住んでいるユーザはヨーロッパ内の Expressway-E クラスタに転送されるのが理想的です。これは、GeoDNS サービスを実装することによって容易に実現できます。GeoDNS サービスはコスト効率が高く、設定が簡単です。GeoDNS を使用すれば、位置（IP アドレス ルーティング）や最小遅延などの複数のポリシーに基づいてトラフィックをルーティングできます。

次に、GeoDNS サービス用の DNS を設定する例を示します。

- DNS SRV レコード用の GeoDNS 設定
- CNAME エイリアス用の GeoDNS の設定

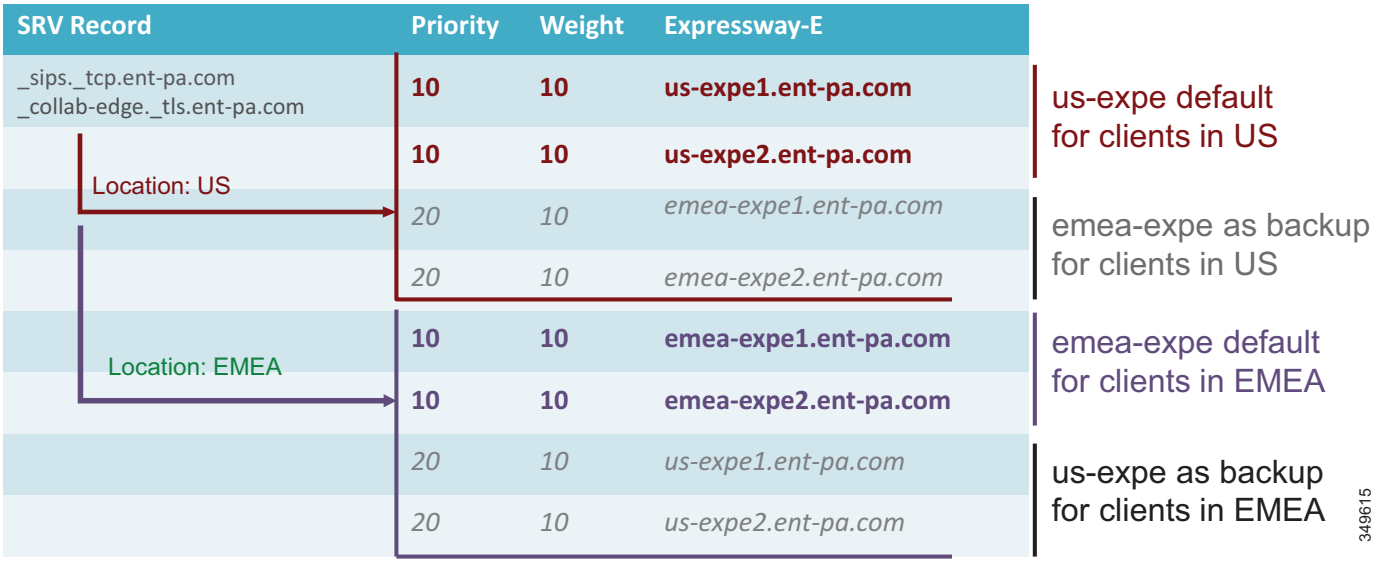
DNS SRV レコード用の GeoDNS 設定

最初のシナリオ例では、2 つのインターネット エッジ Expressway クラスタが米国と欧州に 1 つずつ展開され、それぞれが 2 つの Expressway-C および Expressway-E サーバで構成されます。発信側エンドポイントとヨーロッパ エッジの間で測定された遅延が、エンドポイントと米国エッジの間の遅延を下回っている場合、またはエンドポイント IP アドレスが欧州の範囲に一致する場合、設定されたポリシー（遅延または IP アドレス）に基づいてエンドポイントがヨーロッパ エッジに転送されて登録されます。

一部の GeoDNS プロバイダーは、SRV レコードで GeoDNS サービスをサポートしていますが、多くのプロバイダーは CNAME または A レコードに対してのみ GeoDNS を許可しています。設定をシンプルにしてトラブルシューティングを容易にするために、SRV レコードで GeoDNS サービスを実装することをお勧めします。SRV レコードの GeoDNS 設定を C：図 4-19 に示します。

発信者が米国にいる場合は、コールが米国クラスタに送信されますが、米国クラスタがダウンしている場合はコールが EMEA クラスタに送信されます。この設定は任意の DNS SRV レコードに対して機能するので、Business-to-Business（B2B）シナリオだけでなく、モバイルおよびリモート アクセス シナリオにも対応できます。また、これにより、C：図 4-19 に示すように地理的冗長性も確保されます。

C：図 4-19　　DNS SRV レコード用の GeoDNS 設定例



このシナリオでは、モバイルおよびリモート アクセス (または Business-to-Business コール) の SRV レコードに、特定の場所に対応するタグが付加されます。この SRV レコードはその場所の Expressway-E ピアに解決され、さらに低い優先度でバックアップ場所の Expressway-E ピアに解決されます。これにより、何らかの理由で米国エンドポイントが米国 Expressway クラスタを使用できない場合は、EMEA 内の Expressway-E クラスタにリダイレクトされます。逆もまた同じです。

地理的冗長性は Jabber クライアントとハードウェア クライアントの両方で機能します。ただし、Jabber ユーザがほぼ毎日ログオンとログオフを行うのに対して、ハードウェア クライアントは同じエッジに接続されることが多い点に注意してください。この設定がハードウェア エン

ドポイントにも提供される場合、地理的バックアップの発生後に一旦オフにしてオンに戻さない限り、元の Expressway-E クラスタをホームとして再設定できません。Jabber ではログアウトがより頻繁に発生するため、これは問題とはなりません。

CNAME エイリアス用の GeoDNS の設定

一部の Geo DNS プロバイダーは、DNS SRV レコードに適用される GeoDNS サービスをサポートしませんが、代わりに CNAME または A レコードに適用される GeoDNS サービスをサポートする場合があります。CNAME はそのリソースの実際の A レコードに解決されるエイリアスで、これは DNS SRV 実装において最も一般的な DNS レコードです。すべてのケースで機能する普遍的な設定を提供することはできませんが、この特定のシナリオに対処するための推奨事項をいくつか紹介します。

SRV レコードではなく CNAME レコードに関してのみ GeoDNS サービスを指定することを GeoDNS プロバイダーが許可している場合、以下の例は、CNAME のみが GeoDNS サービスでサポートされる場合の GeoDNS の設定方法を示しています。このシナリオでは、DNS SRV レコードが CNAME レコードに解決され、さらに A レコードに解決されます。CNAME レコードに地理的場所を割り当てることができます。たとえば、米国の Expressway-E クラスタと EMEA における別の Expressway-E クラスタを考えてください。Business-to-Business コール用に SIP TLS の SRV レコード **_sips._tcp.ent pa.com** または **_sip._tcp.ent pa.com** が設定されています。このレコードは、CNAME レコード **alias1.ent pa.com** に解決されます。

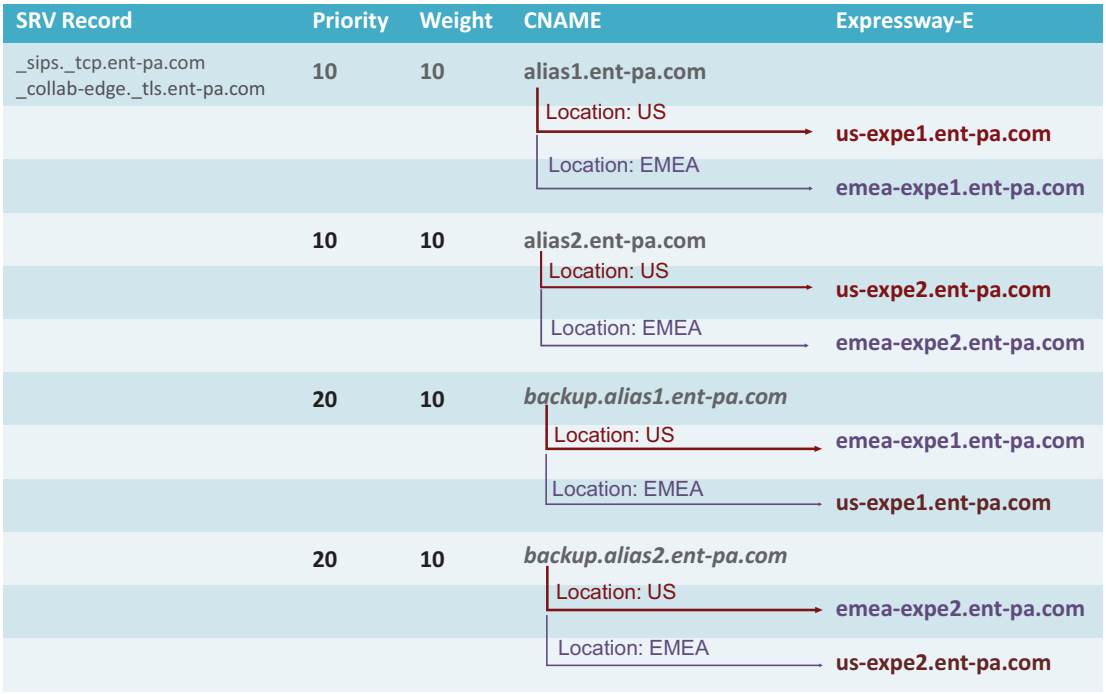
GeoDNS 設定に基づいて、レコードがアクティブになっているリージョンを識別するラベルが CNAME レコードに適用されます。この場合の CNAME 解決は、最も高い優先度（この例では 10）を持つ米国用の A レコード 1 つと EMEA 用の別の A レコードになります。これにより、両方のリージョンのクラスタの最初のピアが解決されます。

2 番目の CNAME レコードは、優先度が最も高い米国および EMEA クラスタの 2 番目のピアに解決されます。クラスタのすべてのピアが含まれるようになるまで、これを繰り返す必要があります。

地理的冗長性を確保するには、バックアップ CNAME エイリアスを作成する必要があります。C：図 4-20 の例では、**backup-alias1.ent-pa.com** が米国ユーザ用の最初の EMEA Expressway ピアと EMEA ユーザ用の米国 Expressway ピアに解決されるため、両方のリージョンの地理的冗長性が確保されます。クラスタのすべてのピアが含まれるようになるまで、このバックアップ エイリアス プロセスを繰り返す必要があります。これらのバックアップ レコードは、DSN SRV が低優先度（この例では 20）に設定されているので、最初のものが応答しない場合にのみ使用されます。

C：図 4-20 は、CNAME レコードに適用される GeoDNS サービスの DNS レコード構造を示しています。

C：図 4-20　　CNAME と地理的冗長性を伴う Geo DNS の DNS レコード構造



Business-to-Business（B2B）コミュニケーション

Business-to-Business（B2B）コミュニケーションの拡張性は、複数の Expressway-C クラスタと Expressway-E クラスタを同じ物理位置にまたは地理的に分散して追加することによって解決できます。

複数の Expressway-C と Expressway-E のペアが展開されている場合は、Unified CM が発信コールを発信側エンドポイントに最も近いエッジ サーバに転送できるため、内部 WAN トラフィックが最低限に抑えられます。加えて、複数のエッジ クライアントが利用されている場合は、Expressway-C が Unified CM クラスタを使用してメッシュ状のトランク構成を形成する必要があります。これにより、地理的に見つけたトラバーサルがいっぱいになった場合または使用できない場合に、追加のアウトバウンド トラバーサル パスを許可することで拡張性と復元力が高まります。

大規模展開では、モバイル & リモート アクセスから分離した Expressway-C と Expressway-E のペア上で Business-to-Business（B2B）コミュニケーションをホストした方が適切な場合があります。これにより、サーバ リソースを外部インターネット通信専用にすることができます。

着信コールに関する留意点

DNS SRV レコードは、SIP と H.323 ent-pa.com ドメインに対して承認された Expressway-E クラスタを特定するために使用されます。重要度と優先度が同じ SRV レコードは、Expressway-E クラスタ ノード全体でコールのバランスを取るために使用されます。

地理的に分散した複数の Expressway-E クラスタ全体で着信コールをスケーリングする場合は、トラフィックのロード バランシングが主要課題になります。Expressway-C と Expressway-E は SIP または H.323 トラフィックのロード バランシングをサポートしません。そのため、DNS クエリに対する応答のロード バランシングがソリューションの重要なスケーリング手段になります。

モバイル & リモート アクセス サービスと同様に、GeoDNS は同じクエリに対する別々の DNS 応答を送信するために使用されます。ネットワーク遅延や地理的位置などのさまざまなメトリックを使用して、DNS 応答で正しい Expressway-E クラスタを指定する必要があります。

GeoDNS は、お客様が選択したメトリックに基づいて、接続先の他のサーバまたはエンドポイントに最適なエッジ Expressway-E を提供する非常に優れた手段です。この場合の応答は、通常、クエリの発行元のサーバに物理的に最も近いエッジに基づいて行われます。このメカニズムは、SRV レコードが異なることを除いて、前述したメカニズムと同じです。たとえば、SIP TLS の SRV レコードは _sips._tcp.ent-pa.com になります。C：図 4-20 は、GeoDNS サービスのセットアップに使用できます。ここで、_collab-edge._tls.ent-pa.com は _sips._tcp.ent-pa.com に置き換えられます。

別のソリューションとしては、宛先のエンドポイントまたはデバイスに最も近いエッジを返すように設計します。この場合は、宛先エンドポイントの位置を検索または確認して、該当するエッジを返す必要があります。このソリューションのメリットは、最短の内部パスをエンドポイントに提供することによって顧客ネットワーク上の帯域幅の使用が最小限に抑えられることです。

これを実現するには、着信側エンドポイントが別のリージョンに属している場合にそのリージョンの Expressway-E にコールを転送するよう Expressway-E を設定できます。

たとえば、EMEA 内の 2 つの Expressway-C クラスタと Expressway-E クラスタと、APJC 内の別の 2 つの Expressway-C クラスタと Expressway-E クラスタについて考えます。EMEA 内の Expressway-C トランク上の Unified CM インバウンド コーリング サーチ スペースには、EMEA 電話機のパーティションは含まれますが、APJC 電話機のパーティションは含まれません。同様に、APJC 内の Expressway-C トランク上のインバウンド コーリング サーチ スペースには、APJC 電話機のパーティションは含まれますが、EMEA 電話機のパーティションは含まれません。EMEA 内のインターネット上のユーザが APJC にある企業エンドポイントにコールした場合は、そのコールが DNS から EMEA Expressway-E クラスタ（Business-to-Business コールのデフォルト）に送信されます。EMEA Expressway-E と Expressway-C はそのコールを宛先に送信しようとしますが、Expressway-C トランクのインバウンド コーリング サーチ スペースがそのコールをブロックします。次に EMEA Expressway-E はそのコールを APJC Expressway E に転送します。今回はコールが宛先に配信されます。これは、APJC Expressway-C のインバウンド コーリング サーチ スペースに APJC エンドポイントのパーティションが含まれているためです。

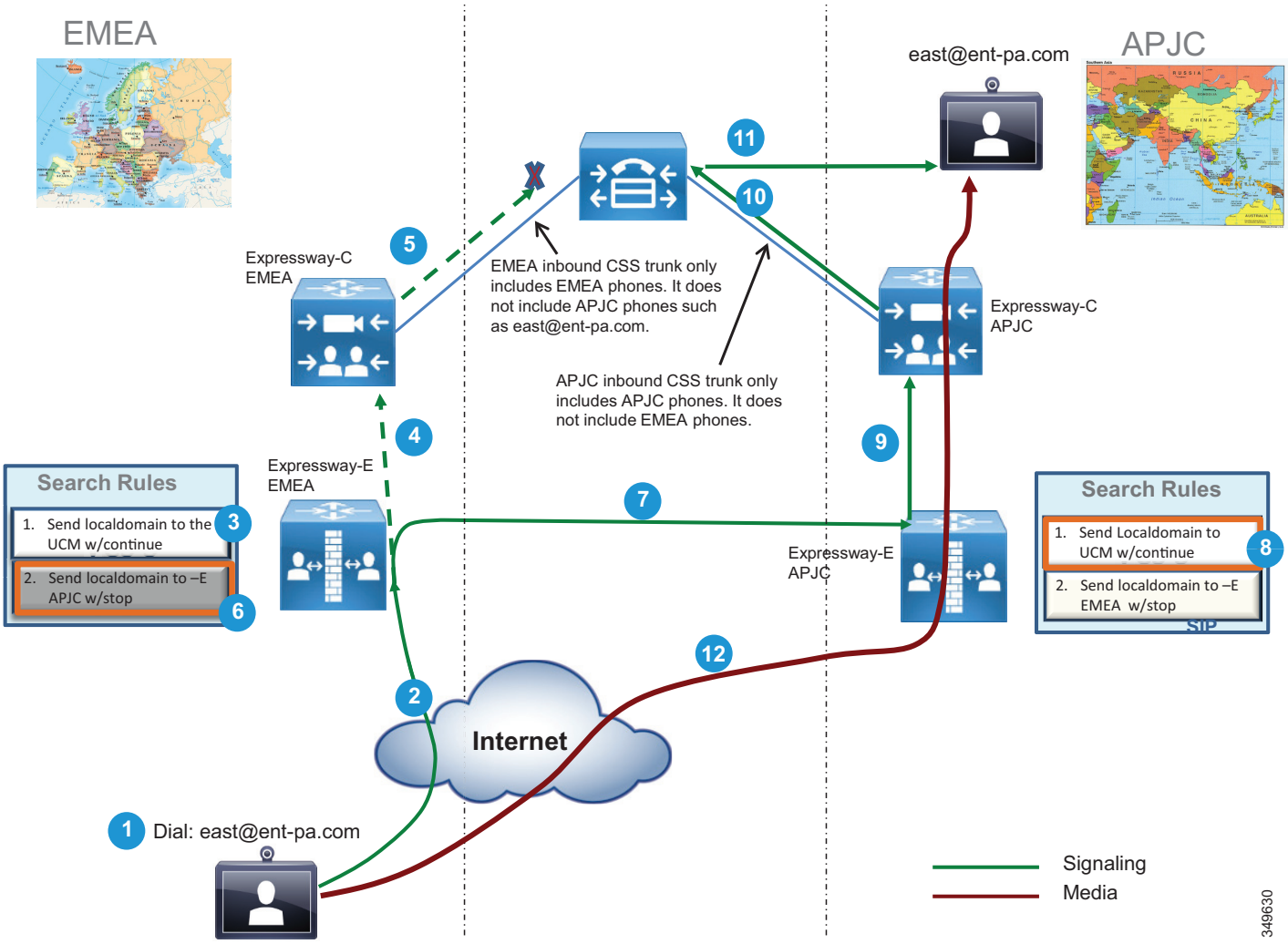
EMEA 内の Expressway-E がシグナリングとメディアのパスからそれ自体を削除できるようにするには、Expressway-E EMEA クラスタ上に TCP/TLS 変換または RTP/SRTP 変換が確実に存在しないようにし、すべての Expressway-C と Expressway-E でコール シグナリング最適化パラメータが確実に [オン（on）] に設定することが重要です。

これは確定的プロセスではないため、Expressway エッジが 3 つ以上の場合は、検索メカニズムに時間がかかりすぎることがあります。したがって、この設定は Expressway エッジが 2 つ以下の場合にお勧めします。

3 つ以上のエッジにスケールするには、Directory Expressway と呼ばれる別のアーキテクチャを展開できます。Directory Expressway アーキテクチャは、プリファード アーキテクチャに含まれません。

C：図 4-21 に、宛先エンドポイントに最も近いエッジの選択を可能にする Expressway エッジ設計を示します。

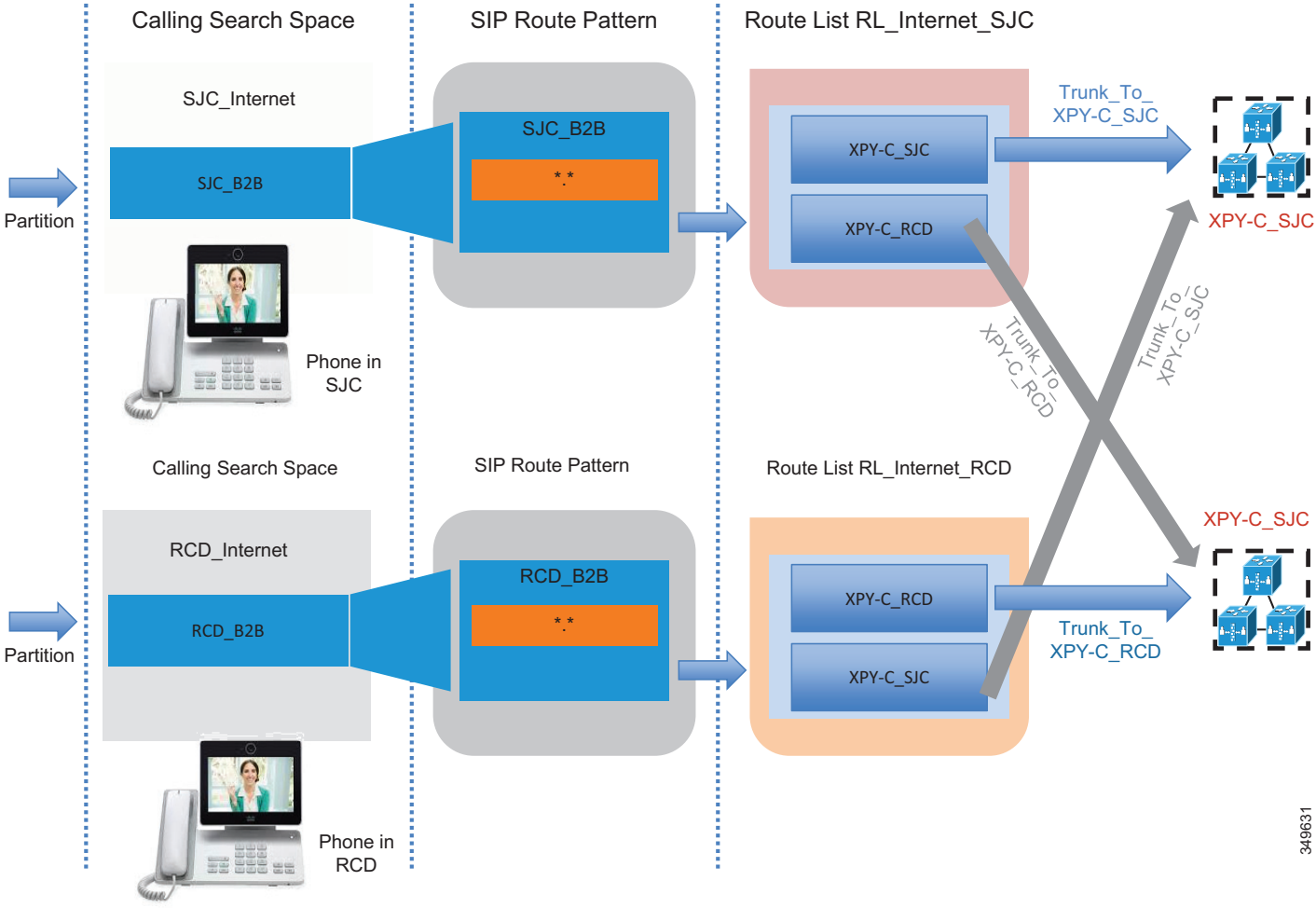
C：図 4-21　　宛先に最も近い Expressway クラスタの選択



発信コールに関する留意点

発信コールは発信側のエンドポイントに最も近い Expressway-C に転送する必要があります。これは、コーリング サーチ スペースやパーティションなどの Cisco Unified CM メカニズムを使用して実現できます。C：図 4-22 に、Unified CM の設定を示します。

C：図 4-22　Unified CM で設定するパーティションとコーリング サーチ スペース



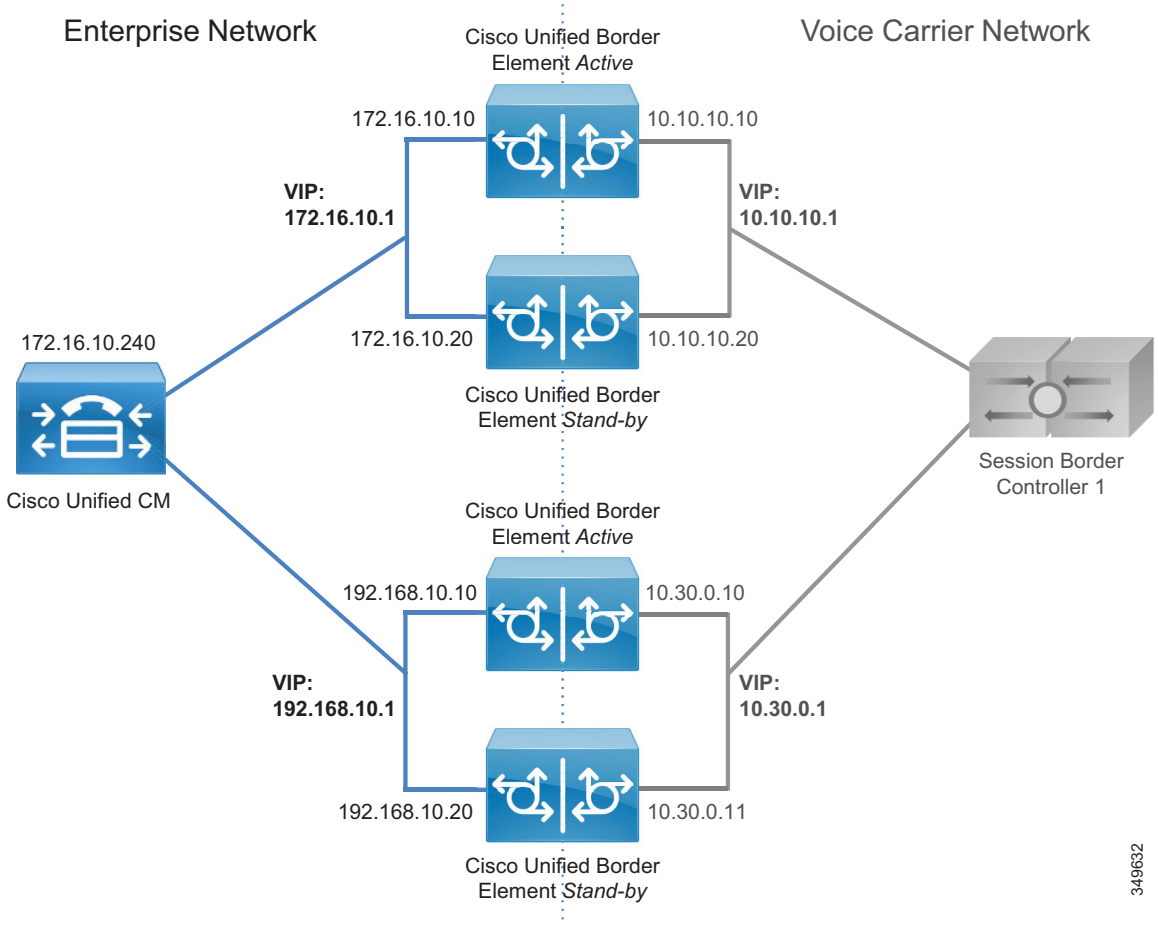
Unified CM ローカル ルート グループ機能は、複数のサイトが複数の Expressway-C クラスタにアクセスする場合にこのソリューションのスケーリングに役立ちます。このメカニズムは、ISDN ゲートウェイや Cisco Unified Border Element 上でも適用されます。詳細については、次のセクションで説明します。設定の詳細は、Cisco Unified Border Element や音声ゲートウェイにも当てはまるため、次の 2 つのセクションで説明します。

Cisco Unified Border Element のスケーリング

プラットフォームあたりのセッション容量については、サイジングの章を参照してください。

複数のデータセンターを展開している場合は、それぞれのデータセンターに Cisco Unified Border Element を展開することができます。この構成はさまざまな用途に使用されます。たとえば、C：図 4-23 に示すようなディザスタ リカバリ アーキテクチャが必要な場合があります。

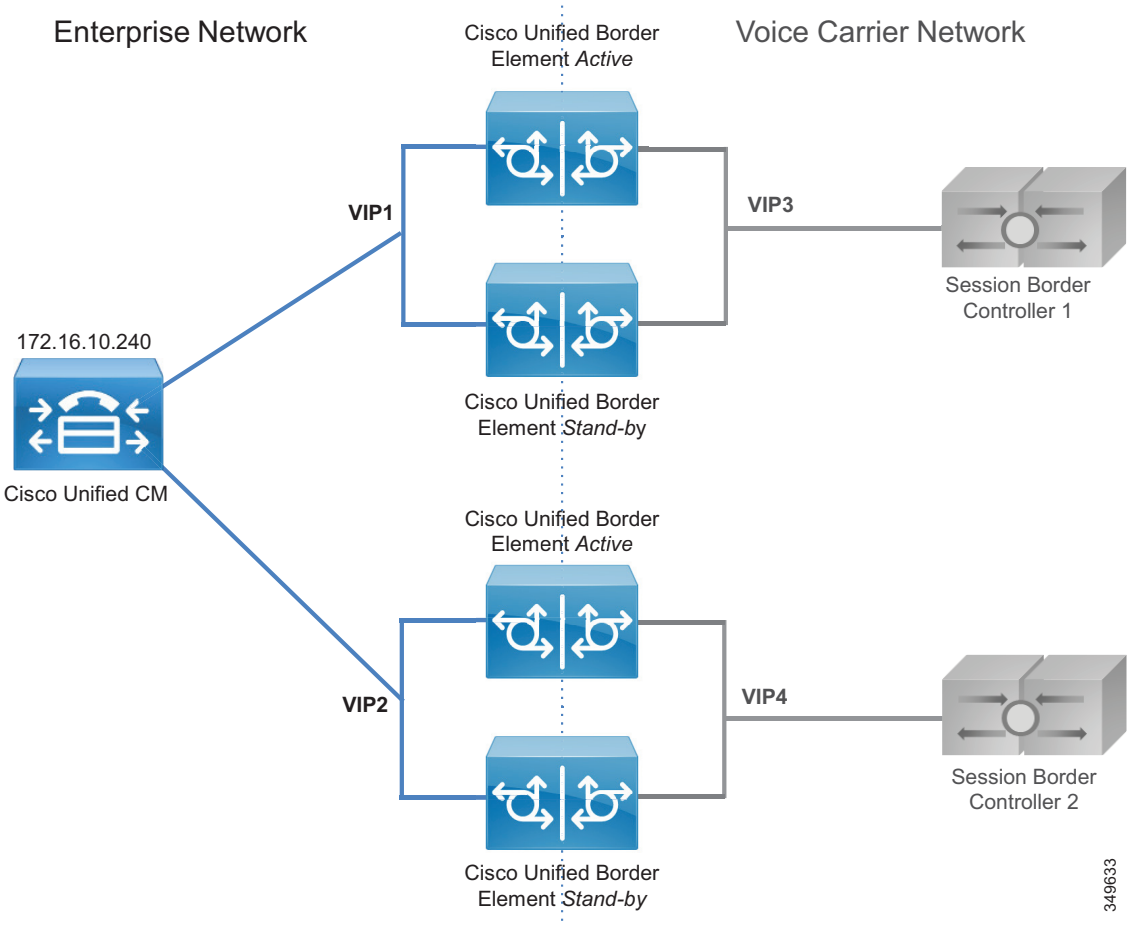
C：図 4-23　　複数の Cisco Unified Border Element



Unified Border Element へのすべてのトランクを同じルート グループ内に含めることができます。これにより、データセンター間にロード バランシングが実現します。データセンター内のアクティブ ルータが故障した場合は、アクティブ コールが保存されます。あるデータセンターが到達不能になった場合、コール要求は残りのデータセンターに送信されます。この場合は、アクティブ コールが破棄されるため、ユーザは手動で回復する必要があります。

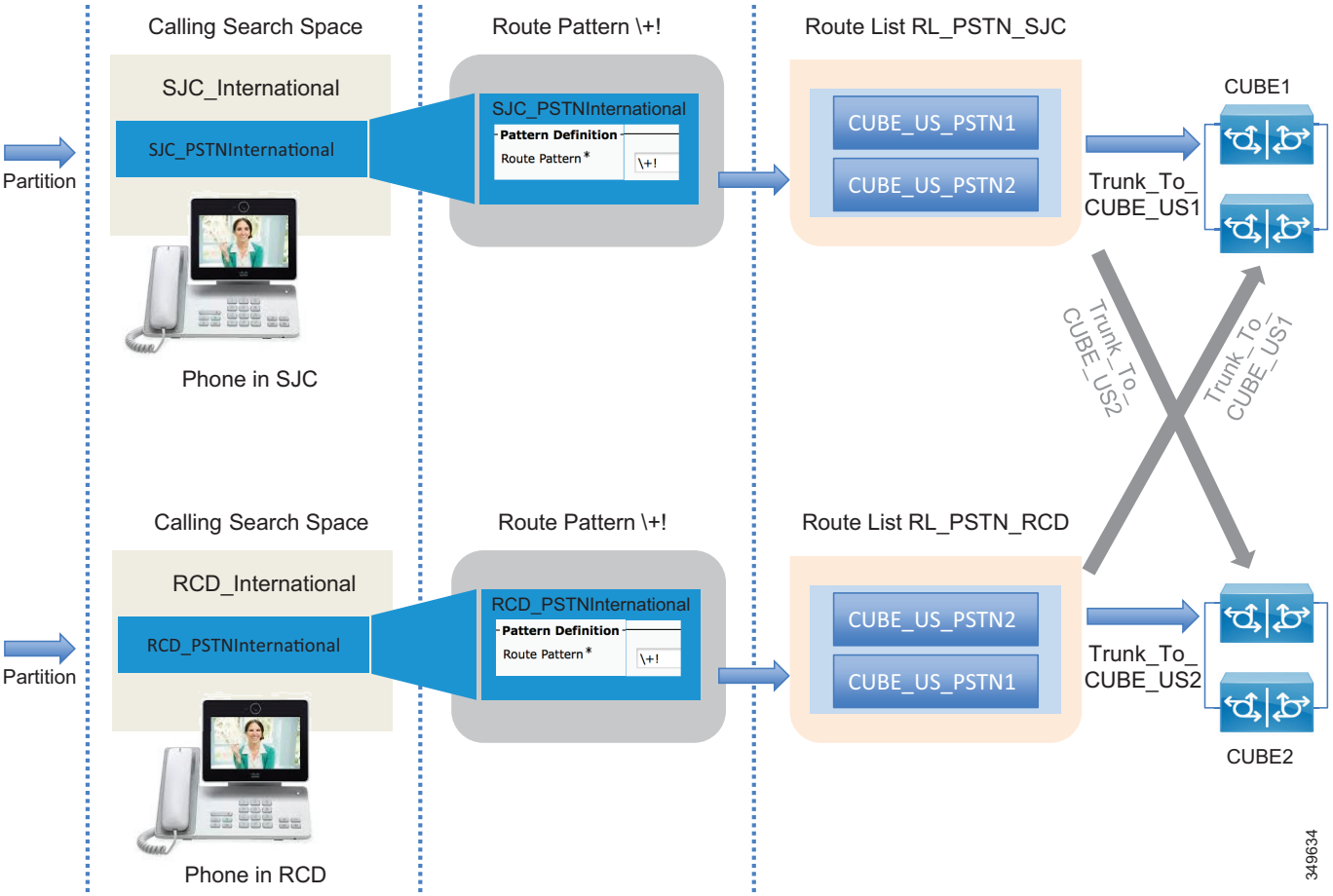
C：図 4-24 に示すように、企業音声ネットワークが広範囲に広がっている場合は、通信事業者からの複数のセッション ボーダー コントローラ（SBC）が使用されます。通信事業者の推奨事項に基づいて、SBC ごとに Cisco Unified Border Element が展開される場合があります。

C：図 4-24　　別々の SBC に接続された複数の Cisco Unified Border Element



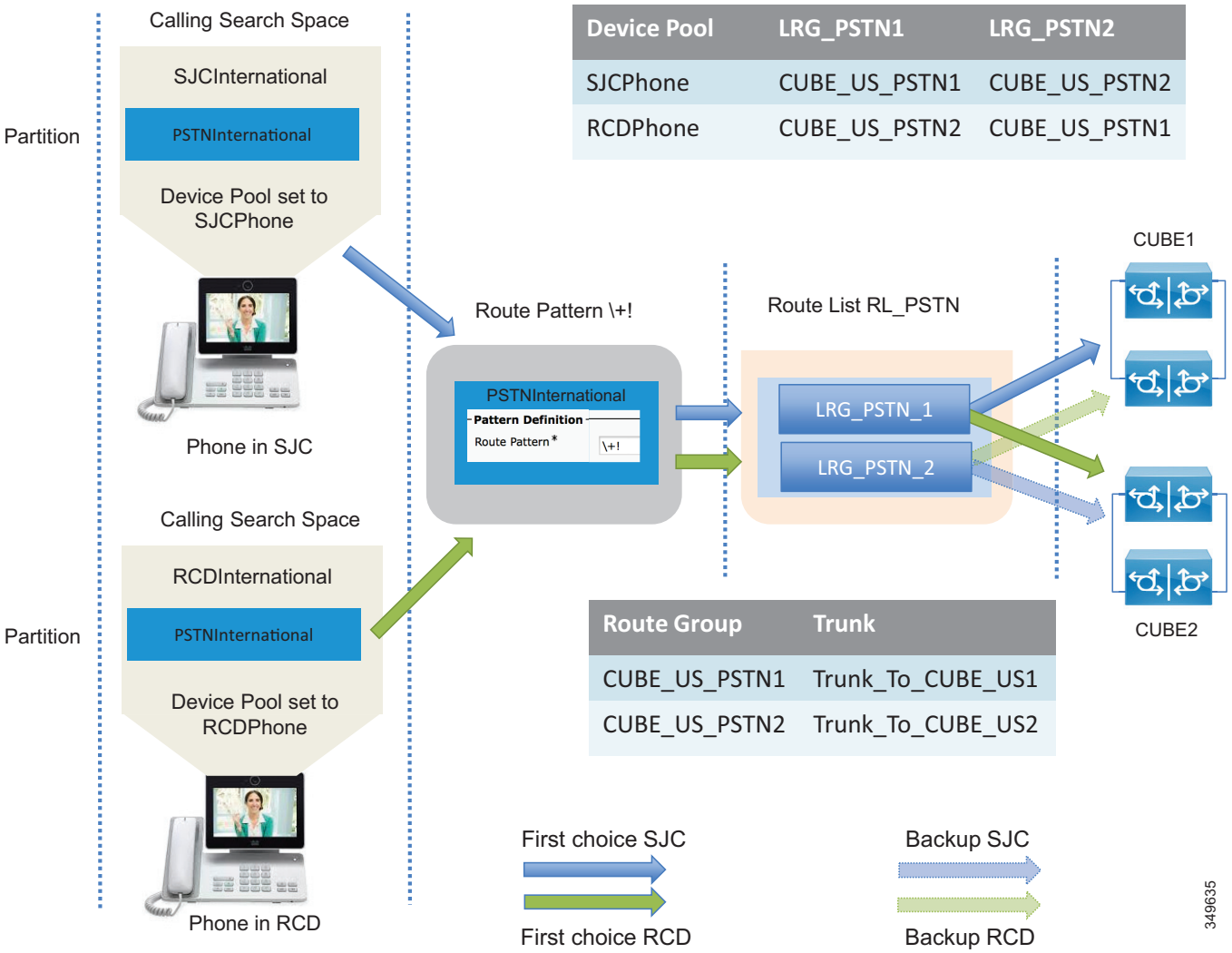
たとえば、US ですでに展開済みのものに加えて、別の Unified Border Element が必要になったとします。Trunk_to_CUBE_US2 という名前の新しいトランクを追加します。C：図 4-25 に、コーリング サーチ スペースとルート パターン間の標準の一対一マッピングに基づく設定を示します。この設定は、Unified Border Elements の数が増えるにつれて、Unified CM リソースに対する影響が大きくなるため、いくつかの制限があります。この設定を C：図 4-25 に示します。C：図 4-26 に示すローカル ルート グループ アプローチと比較してみてください。

C：図 4-25　Cisco Unified Border Element 接続用の Unified CM の設定



同じルート パターン \+! がすべての物理宛先分繰り返され、別々のパーティションに配置されます。元のパーティション PSTNInternational を SJC_PSTNInternational と RCD_PSTNInternational の 2 つに分割する必要があります。ルート パターン \+! を削除して、新しく作成された 2 つのパーティションに移動する必要があります。このアプローチは、サイト数があまり多くない（3 つ以下の）場合に機能します。さらに優れたアプローチは、C：図 4-26 に示すローカル ルート グループの概念を使用したアプローチです。

C：図 4-26　ローカル ルート グループ アプローチを使用した Cisco Unified Border Element 接続用の Unified CM の設定



この場合、デバイス プール SCJPhone の LRG_PSTN1 はルート グループ CUBE_US_PSTN1 と同じに設定されるのに対して、デバイス プール RCDPhone の LRG_PSTN1 はルート グループ CUBE_US_PSTN2 と同一に設定されます。LRG_PSTN2 は、SJC 電話機では CUBE_US_PSTN2 と同じに設定され、RCD 電話機では CUBE_US_PSTN1 と同一に設定されます。このアプローチをお勧めする理由は、新しいパーティションやルート パターンが必要ないうえ、C：図 4-25 に示すアプローチよりはるかにスケーラブルなことです。

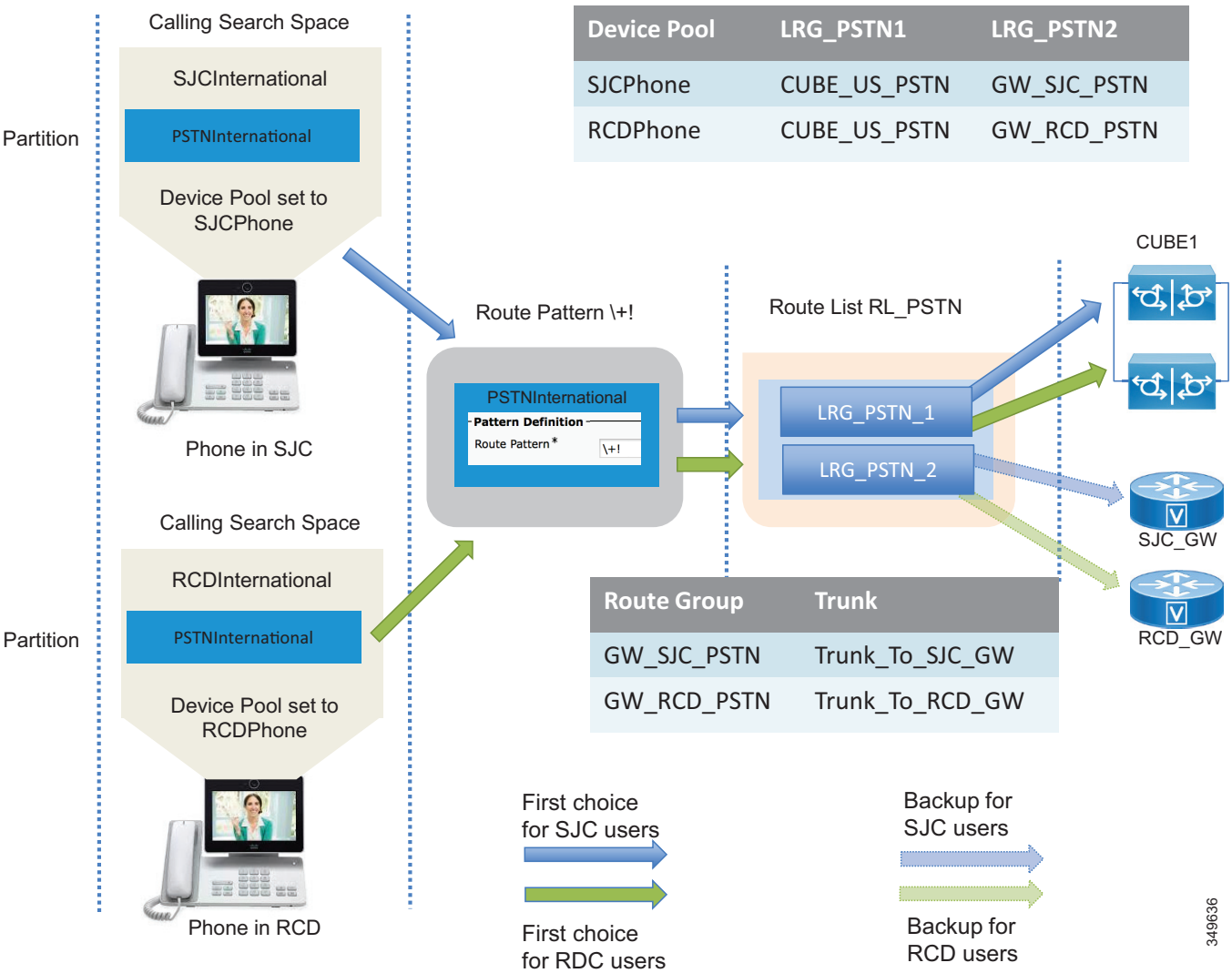
PSTN ソリューションのスケーリング

ローカル PSTN アクセスを提供する分散ゲートウェイは、支店に展開され、バックアップ サービスとして使用されます。

支店の数が多い場合は、Unified CM 内のルート グループとルート リスト設定の構造がうまくスケーリングしません。この展開では、PSTN へのルート パターンをサイトごとにレプリケートする必要のないローカル ルート グループ機能の使用をお勧めします。

以前のセクションで説明した設定は、このシナリオをカバーするため容易に対応できます。必要なことは、C：図 4-27 に示すように、デバイス プロファイル LRG_PSTN1 をルート グループ CUBE_US_PSTN に割り当て、LRG_PSTN2 をそのデバイス プール用のローカル ゲートウェイに対応するルート グループに割り当てることです。

C：図 4-27　ローカル ゲートウェイを使用した集中型 PSTN アクセスに関する設定



コラボレーション エッジの展開プロセス

ここでは、コラボレーション エッジの展開プロセスの概要について説明します。すべての展開ですべてのアクセス手段が必要なわけではないため、コラボレーション エッジの各コンポーネントは個別に取り扱われます。たとえば、ある会社は PSTN しか所有していないが、別の会社が、特定のローカル サイトで IP PSTN のローカル バックアップとして PSTN を使用し、インターネット エッジを展開している場合があります。

コラボレーション エッジ コンポーネントは次の順序で展開する必要があります。

- Expressway-C と Expressway-E を展開する
- Cisco Unified Border Element を展開する
- Cisco Voice Gateway を展開する

Expressway-C と Expressway-E を展開する

このセクションでは、Expressway-C と Expressway-E をインストールして展開するのに必要なタスクの概要を示します。このタスクを次の順序で実行する必要があります。

1. Expressway-C と Expressway-E の OVA テンプレートをダウンロードして展開し、Expressway ソフトウェアをインストールします。アプライアンス モデルが使用されている場合、OVA テンプレートと Expressway ソフトウェアをダウンロードしてインストールする必要はありません。
2. DNS と NTP を含むネットワークのインターフェイスと設定、およびシステムのホスト名とドメイン名を構成します。Expressway-E は 2 つの LAN インターフェイスを備えています。外部インターフェイスの IP アドレスを静的に変換しなければならない場合は、変換後のインターフェイスの IP アドレスを設定する必要があります。Expressway-E はペイロード参照内のパブリック IP アドレスを使用します。2 つの LAN インターフェイスを備えた Expressway-E 用のスタティック ルーティングを設定します。Expressway-C インタ フェースが Expressway-E とは別のネットワーク上に存在し、Expressway-C インターフェイスが NAT によって変換されない場合は、スタティック ルーティングが必要です。これにより、Expressway-C が Expressway-E と同じネットワークに存在するかのように表されます。単一の Expressway-E インターフェイスもサポートされますが、このプリファード アーキテクチャのドキュメントでは説明しません。
3. クラスタリングを設定します。

モバイルおよびリモート アクセスを展開する

1. Unified Communications モードを [モバイルおよびリモート アクセス（Mobile and remote access）] に設定することによって、モバイルおよびリモート アクセスを有効にします。
2. ユニファイド コミュニケーション モードを [モバイルおよびリモート アクセス（Mobile and remote access）] に設定した後、Expressway-C 上で、C：表 4-6 に示すように [MRA アクセス制御（MRA Access Control）] 設定を指定します。

C：表 4-6　Expressway-C モバイルおよびリモート アクセス（MRA）のアクセス制御設定

パラメータ	設定	説明
認証パス（Authentication path）	UCM/LDAP 基本認証	MRA 接続エンドポイントの認証パスを決定します。SSO を使用している場合は、他の設定のいずれかを選択します。
OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）	オン	Jabber MRA 接続に関する OAuth 2 認証フローを有効にします。
ユーザ クレデンシャルによる承認（Authorize by user credential）	オン	ハードウェア エンドポイント MRA 接続の認証を有効にします。
内部認証の可用性の確認（Check for internal authentication availability）	いいえ（No）	ホーム クラスタ認証モードを問い合わせないようにシステムを設定します。この展開内のすべてのクラスタが同じ認証方式を使用します。

3。 モバイルおよびリモート アクセスが有効にするドメインを選択します。[Unified CM 上の SIP 登録およびプロビジョニング（SIP registration and provisioning on Unified CM）]、[Unified CM 上の IM and Presence サービス（IM and Presence service on Unified CM）]、および [会社間フェデレーションの場合の XMPP フェデレーション（XMPP federation if inter-company federation）] をオンにします。

4。 Expressway-C と Expressway-E に CA 証明書をアップロードします。[TLS 検証モード（TLS verify mode）] が [オン（on）]（推奨）になっている場合は、Unified CM クラスタと IM and Presence クラスタを検出するためにこの証明書が必要です。このように、Expressway-C は、証明書をチェックすることによって、クラスタ サーバのアイデンティティを検証します。

5。 各クラスタのパブリッシャを設定することによって、Unified CM サーバと IM and Presence サーバを検出します。

6。 Expressway-C と Expressway-E の両方に証明書をインストールします。どちらのタイプの Expressway ノードも、その後 CA によって署名される、証明書署名要求（CSR）を生成できます。内部 CA を使用している場合は、CSR をその CA で署名する必要があります。Expressway-C 証明書を内部 CA によって署名することができますが、Expressway-E ではパブリック CA によって署名される証明書が必要です。その後で、署名した証明書を Expressway-C と Expressway-E にアップロードする必要があります。

7。 Expressway-C と Expressway-E の間の Unified Communication トラバーサル ゾーンを設定して、Cisco Unified CM へのプロキシ登録を許可します。

8。 すべてが正しくセットアップされていることを確認するために、Unified Communications のステータスをチェックします。

注
- この設定によって、モバイルおよびリモート アクセスが有効になります。Business-to-Business（B2B）では追加の設定が必要です。
- 上記設定は、Expressway-C と Expressway-E 上だけで完結します。
- これらのステップは、Unified CM への TCP/RTP 接続（TLS/SRTP は表示されていない）の場合に必要です

Business-to-Business（B2B）コミュニケーションを展開する

ここでは、Business-to-Business（B2B）コミュニケーションのセットアップに必要な追加のステップの概要について説明します。

1. Expressway-C と Expressway-E の両方で NTP、DNS、およびシステム名を含む基本的なレイヤ 3 設定を構成します。
2. Expressway-E 上でトラフィック ルーティングに必要な IP ルートを含む NAT 設定をセットアップします。
3. Expressway-E を DMZ に配置する前に、外部ファイアウォールが Expressway-E 宛てのすべてのトラフィックをブロックするように設定されていることを確認します。
4. Expressway-C と Expressway-E の両方のローカルまたはリモート認証を含む管理アクセス ポリシーを設定します。
5. 該当する DNS サーバ内の DNS A レコードを各サーバの FQDN が解決できるように設定します。
6. Expressway-C からのトラバーサル クライアント接続を認証する目的で Expressway-E 内のローカル認証クレデンシャルをセットアップします。
7. Expressway-E 上で SIP 専用のトラバーサル サーバ ゾーンをセットアップします。
8. Expressway-E 上のインターワーキングを [オン（On）] に設定します。これにより、Expressway-E で H.323 コールを送受信して、それらをネットワークのエッジで SIP に接続できるようになるため、企業内部で単一のプロトコルが維持されます。
9. Expressway-C 上で SIP 専用のトラバーサル クライアント ゾーンをセットアップします。
10. Expressway-E の FQDN を使用してトラバーサル リンクを有効にして PKI の使用を可能にします。
11. 外部 DNS ゾーンを Business-to-Business（B2B）コミュニケーションのアウトバウンド ドメイン解決用に設定します。
12. Expressway-E 上でビデオ、音声、IP PSTN ゲートウェイなどの保護されたリソースへのアクセスを制限する基本的な CPL ルールを導入します。
13. Expressway-C と Expressway-E が権限を与えられたドメインをセットアップします。
14. Expressway-C と Expressway-E 上で事前検索変換、検索ルール、DNS 検索ルール、および外部 IP アドレス ルーティングを使用してダイヤル プランをセットアップします。
15. Expressway-C 上で Unified CM までの SIP ネイバー ゾーンを設定します。
16. Unified CM 上の SIP トランクが Expressway-C と通信するように設定します。

Cisco Unified Border Element を展開する

ここでは、ボックスツーボックス冗長性を備えた Cisco Unified Border Element を展開するためのプロセスの概要について説明します。ボックスツーボックス冗長性は両方の Unified Border Element ルータ上で設定する必要があり、設定内容は両方とも同じです。アクティブ Unified Border Element から スタンバイ Unified Border Element に設定をコピーして貼り付けることができます。

1. ネットワーク設定（アクティブ Unified Border Element とスタンバイ Unified Border Element の両方の 2 つのイーサネット インターフェイス（LAN 向けと WAN 向け）と IP ルーティング）を構成します。

2。 両方のルータ上の Unified Border Element を SIP 間コール、FAX のリレーまたはパススルー、プライバシー ヘッダーとしての発信元 ID 処理、およびアーリーオファーの強制に対して有効にします。Unified CM がベスト エフォートアーリーオファー専用に設定されているため、Unified Border Element 上でこの機能を有効にすることをお勧めします。新しい展開ではアーリーオファーのみがエンドポイントから送信されますが、代わりにディレイドオファーが送信される旧式のシスコ デバイスが関与している場合もあります。このマニュアルではこのようなケースを取り上げませんが、Cisco Unified Border Element 上でアーリーオファーを強制することをお勧めします。

3。 ボックスツーボックス冗長性を有効にして、アクティブ ルータとスタンバイ ルータの LAN インターフェイスと WAN インターフェイスの両方で HSRP をグローバルに設定します。

4。 音声コーデック優先順位を設定します（音声コーデックがネゴシエート可能であり、Unified CM または通信事業者ソフト スイッチによって強制されない場合）。

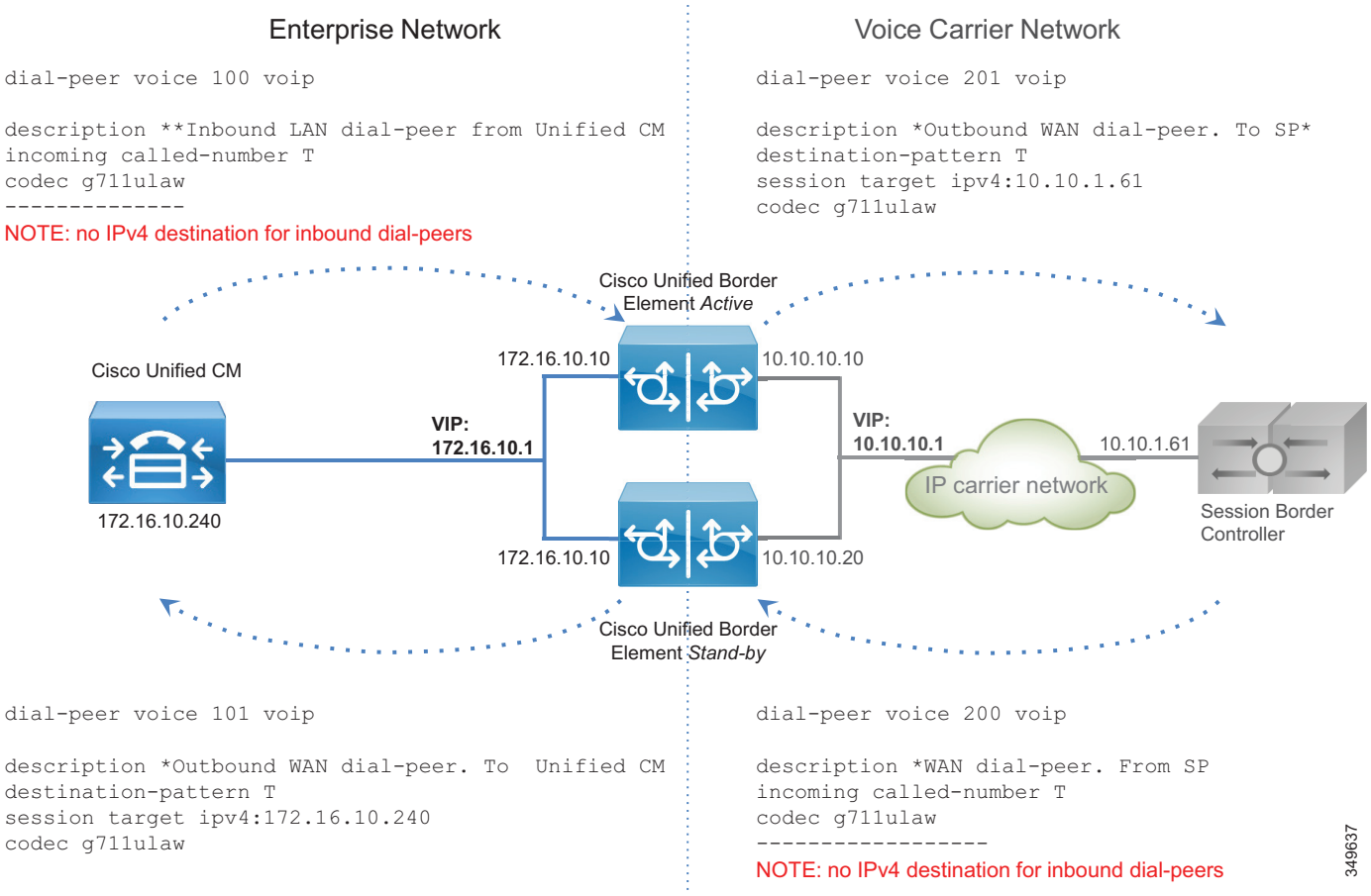
5。 保留音を設定します。

6。 ダイヤルピアを設定します。ダイヤルピアはコール レッグに関連付けられており、インバウンドまたはアウトバウンドで照合できます。たとえば、Unified CM からの着信コールはインバウンド ダイヤルピア（着信コール レッグに対応する）によって照合されます。別のコール レッグが電気通信業者のセッション ボーダー コントローラ（SBC）宛てに Cisco Unified Border Element（CUBE）によって生成され、別のダイヤル ピアに対して照合されます。同じダイヤル ピアでインバウンド コールまたはアウトバウンド コールを照合できますが、各ダイヤル ピアで特定のコール レッグを照合することをお勧めします。この提案に従うと、次の 4 種類のダイヤルピアが用意されます。Unified CM から CUBE へのインバウンド ダイヤルピア、CUBE から SBC へのアウトバウンド ダイヤルピア、SBC から CUBE へのインバウンド ダイヤルピア、および CUBE から Unified CM へのアウトバウンド ダイヤルピア。ダイヤルピアは、発信側または着信側の番号またはパターンに照らして照合できます。また、ダイヤルピアは、単一のコーデックを強制することも、ステップ 4 で設定したコーデックのリストをネゴシエートすることもできます。**incoming called-number** コマンドはダイヤルピア インバウンドのみを作成します。

   インバウンド ダイヤルピアにはターゲットが関連付けられませんが、アウトバウンド ダイヤルピアには Unified CM または通信事業者の SBC がターゲットとして定義されます。

   外部宛先へのコールは汎用パターンと一致するため、Unified Border Element 上のダイヤルピア設定がエラーの原因になる場合があります。たとえば、C：図 4-28 では、発信コールがダイヤルピア 201 と 101 の両方と一致するため、ルーティングが正しく機能しません。

C：図 4-28　Cisco Unified Border Element 上でのインバウンド ダイヤルピアとアウトバウンド ダイヤルピアの設定



C：図 4-29 の変数 T は任意の長さの任意の数値文字列を表します。これは、Unified CM からのコールが世界中の任意の宛先に送信される可能性があるためです。最も近い一致が役に立つ場合もありますが、Unified Border Element が一元管理されており、複数の場所にサービスを提供している場合は、「宛先パターン」設定内で可能性のあるすべての宛先を列挙するのは実用的ではありません。この制限を克服し、ルーティング プロセスを簡略化して応答性を高めるために、次の追加の設定を実行します。

a。 アウトバウンド ダイヤルピア内のサーバ グループ：サーバ グループがダイヤルピア内の宛先として設定され、ラウンドロビン アルゴリズムが選択されている場合は、Unified Border Element は複数のサーバで負荷を共有します。

```
voice class server-group 1
    ipv4 172.16.10.240
    ipv4 172.16.10.241
    ipv4 172.16.10.242
    ipv4 172.16.10.243
    ipv4 172.16.10.244
    hunt-scheme round-robin
```

b。 SIP Out-of-Dialog OPTIONS Ping：サーバが稼働中の ping 間隔やサーバがダウン中の間隔（この例ではそれぞれ 30 秒と 60 秒に設定）などのさまざまなパラメータを設定できます。

```
voice class sip-options-keepalive 171
    transport tcp
    sip-profile 100
    down-interval 30
    up-interval 60
    retry 5
    description Target Unified CM
```

この方法では、Unified CM へのアウトバウンド ダイヤルピアが次のようになります。

```
dial-peer voice 101 voip
    description *Outbound WAN dial-peer. ToUnified CM
    destination-pattern T
    session protocol sipv2
    session server-group 1
    voice-class sip options-keepalive profile 171
    codec g711ulaw
```

c。 通信事業者への発信コール レッグがアウトバウンド ダイヤルピアによって照合されます。

```
dial-peer voice 201 voip
description *Outbound WAN dial-peer. To SP*
destination-pattern T
session target ipv4:10.10.1.61
 codec g711ulaw
```

d。 先行する「*」は、発信コール（Unified Border Element から見れば着信コール）で Unified CM から送信されます。これにより、ルータはコールの方向を識別できます。この記号はコールが IP PSTN に到達する前に除去する必要があります。また、設定されたダイヤル プランに基づいて、発信者番号を 「+」を使って正規化する必要があります。ルール 2 は「+」を前に付加し、発信者番号に適用されますが、ルール 1 は先行する「*」を「+」に置き換えます。これらのルールは着信者番号にも適用されます。そのため、着信者番号用と発信者番号用の 2 つのルールを作成できます。ただし、着信者番号は常に最初のルールと照合され、発信者番号は常に 2 つ目のルールと照合されるため、単一の音声トランスレーション ルールを使用できます。これは、インバウンド ダイヤルピア上で設定されます。

発信コール レッグ（ダイヤルピア）は **dpg** コマンド経由でインバウンド ダイヤルピアにバインドされるため、「*」が先行するコールが受信された場合は、SBC に対向しているダイヤルピアに送信され、Cisco Unified CM 向けのダイヤルピアには送信されません。

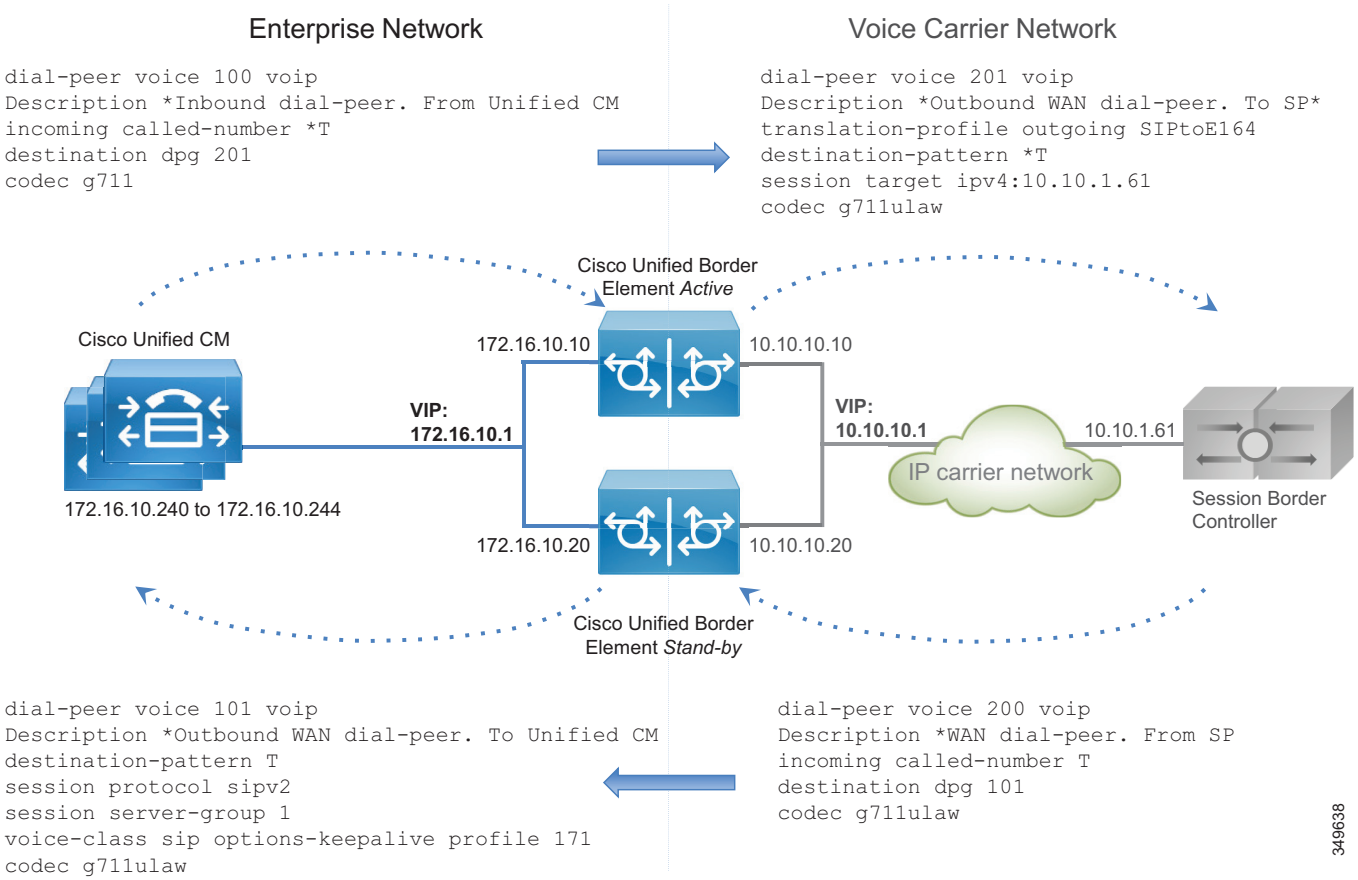
```
voice class dpg 201
    dial-peer 201

voice translation-rule 2
    ??? 1 /^\*/ /+/
    ???2 // /+/
voice translation-profile SIPtoE164
    translate called 2
    translate calling 2
dial-peer voice 100 voip
    translation-profile outgoing SIPtoE164
    incoming called-number *T
destination dpg 201
    codec g711
```

ダイヤルピア 200 はダイヤルピア 101 にもバインドする必要があります。

```
voice class dpg 101
    dial-peer 101

dial-peer voice 200 voip
    description *WAN dial-peer. From SP
    incoming called-number T
    destination dpg 101
    codec g711ulaw
```

C：図 4-29 でこれについて説明します。

C：図 4-29　　Cisco Unified Border Element のダイヤルピア設定



コール レッグが Unified CM から到着した場合は、「*」が先行する Unified Border Element にヒットするため、ダイヤルピア 100 と一致します。その後で、このコールは、インバウンド ダイヤルピア宛先としてアウトバウンド ダイヤルピア グループを使用してダイヤルピア 200 に送信されます。ダイヤルピア 200 は先行する「*」を除外し、そのコールを PSTN に送信します。この機能を使用しない場合は、ダイヤルピア 201 も一致するため、ルーティング エラーが発生することに注意してください。

コール レッグが SBC から到着した場合は、ダイヤルピア 201、101、および 200 と一致する可能性があります。ただし、「着信者番号」の方が「宛先パターン」より優先されるため、ダイヤルピア 200 が一致します。また、ダイヤルピア 200 がダイヤルピア 101 にリンクされているため、コールは正しく宛先にルーティングされます。

7。 必要に応じて、トランスコーディングを設定します。トランスコーディングには専用のハードウェア リソース（DSP）が必要なことを覚えておいてください。

Unified CM 上で次の設定作業を実行します。

1。 コール制御の章で指定されているように、各 Unified Border Element にベスト エフォート早期オファー トランクを設定します。

2。 ルート グループ CUBE_US_PSTN を設定し、メンバーとして Unified Border Element トランクを追加します。

3。 ローカル ルート グループ LRG_PSTN1 を設定します。

4。 デフォルト ローカル ルート グループとルート グループ LRG_PSTN1 を含むルート リストを設定します。

5。 デバイス プールごとに、LRG_PSTN1 を CUBE_US_PSTN に設定します。

Cisco Voice Gateway を展開する

PSTN インターフェイスは Cisco ISR ルータや ASR ルータなどのさまざまなルータで使用できます。PSTN インターフェイスには、アナログ、BRI、および PRI ISDN 音声カードが含まれます。アナログ インターフェイスは、ほとんど、FAX マシンとアナログ電話機に接続するために使用されます。

ISDN 音声インターフェイスを備えた PSTN ゲートウェイを設定するには、次の作業を実行します。

1。 ルータ上でネットワーク設定とルーティングを構成します。

2。 ISDN インターフェイスをアクティブ化します。

3。 通信事業者の要件に基づいて、ユーザ側の ISDN パラメータ、スイッチタイプ、フレーミング、および回線コードを設定します。

4。 ダイヤルピアを設定します。

ダイヤルピア ロジックは IP PSTN や Unified Border Element 用のものと同じですが、この場合は、「voip」ダイヤルピアに加えて、音声ゲートウェイには PSTN 向けの「pots」ダイヤルピアもあります。

FAX マシンなどのアナログ装置が存在する場合は、アナログ インターフェイスを介してルータに接続できます。

ルータがアナログ FAX 相互接続専用に使用されていて、PSTN インターフェイスが別のルータに接続されている場合は、T.38 FAX リレーを設定できます。これは、特に PSTN ゲートウェイへのパスが WAN をトラバースする場合に、このリレーがより高い復元力を示すためです。

ダイヤルピア設定は IP PSTN や Unified Border Element の設定と異なります。ゲートウェイは特定の場所に展開され、その場所の電話機を制御するため、パターン宛先は +14085554XXX のようによく見る形式になります。

一方、着信 PSTN コールのアドレスはプラン、タイプ、および番号で構成されます。プランとタイプは SIP でサポートされておらず、通信事業者に基づくため、コールは別のプランとタイプを使用してゲートウェイに到達する可能性があります。たとえば、ドイツの同じエリア コード 6100 内のトランク上の E.164 宛先 4961007739764 へのコールの場合は、出力 ISDN SETUP メッセージ内の着信者番号（プラン / タイプ / 番号）が ISDN/national/61007739764、ISDN/subscriber/7739764、または unknown/unknown/061007739764 として送信されます。

プラン / タイプに基づいて番号が変化するため、ダイヤルピアが一致しない場合があります。そのため、プラン / タイプを unknown/unknown に強制する必要があります。この方法では、完全な E164 番号が宛先に開示されます。ダイヤルピア構造は、コール制御の章で詳しく説明されており、ここでは一貫性を保つために参照されています。

アウトバウンド ダイヤルピアの場合は、次のルールによって、発信者番号がプラン「unknown」とタイプ「unknown」に変換され、着信者番号が先行する「*」を使って +E.164 番号に変換されます。

```
voice translation-rule 1
       rule 1 /^\*/ // type any unknown plan any unknown
       rule 2 // // type any unknown plan any unknown
voice translation-profile ISDNunknown
       translate called 1
translate calling 1
dial-peer voice 1 pots
       translation-profile outgoing ISDNunknown
```

インバウンド ダイヤルピアの場合は、発信者情報にタイプが 「national」の 10 桁の数字が含まれていれば（および米国を示す国番号「1」が含まれていなければ）、コールは「+1」が先行する +E.164 番号に正しく変換されます。「unknown」の場合は、以降のルールが一致しません。

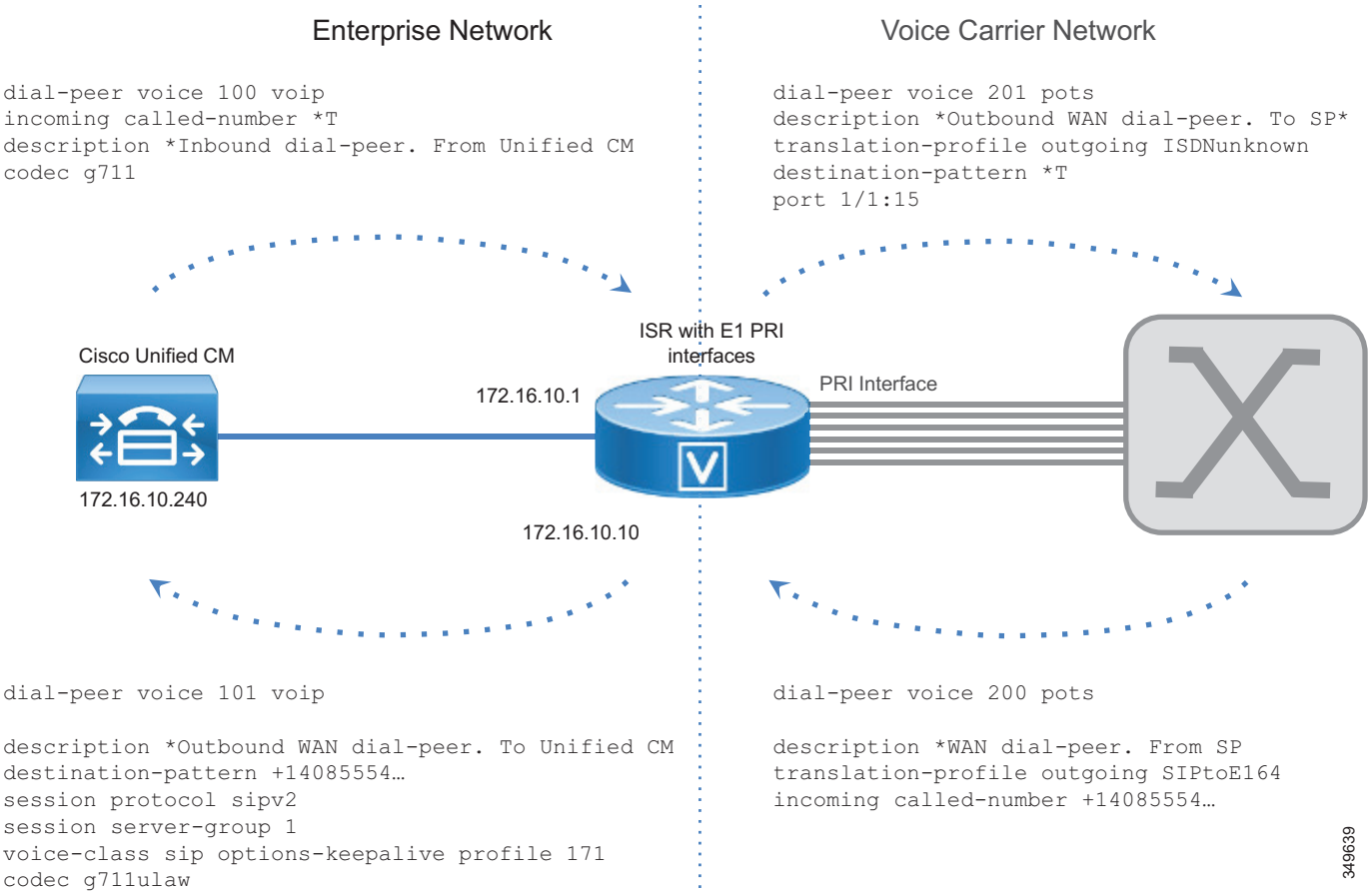
着信者番号が海外の宛先から送られてきたため国番号が含まれており、E.164 形式だった場合は、ルール 2 によって先行する「+」が付加されます。

ただし、ISDN セットアップはホップバイホップのため、タイプが「national」のコールはそれほど多くないことが予想されます。これは、最近のスイッチが強制的にタイプを「national」にしているためです。いずれの場合も、次のルールによって、発信者番号と着信者番号が正しく正規化されます。

```
voice translation-rule 3
    rule 1 /^\(.+\)$/ /+1\1/ type national unknown plan any unknown
    rule 2 /^\(.+\)$/ /+\1/ type international unknown plan any unknown
voice translation-profile ISDNtoE164
    translate called 3
    translate calling 3

dial-peer voice 1 pots
    translation-profile incoming ISDNtoE164
```

C：図 4-30 に、G.711 のダイヤルピア設定と E1 PRI インターフェイスを示します。

C：図 4-30　　音声ゲートウェイのダイヤルピア設定



Unified CM 上で次の設定作業を実行します。

1. 各ゲートウェイのベスト エフォート早期オファー トランク（Trunk_to_SiteID_GW、SiteID は場所を識別する変数）を設定します。
2. ルート グループ LRG_PSTN1 を設定して、メンバーとしてゲートウェイ トランクを含めます。
3. ローカル ルート グループ LRG_PSTN1 を設定します。
4. デフォルト ローカル ルート グループと LRG_PSTN1 を含むルート リストを設定します。
5. デバイス プールごとに、LRG_PSTN1 を Trunk_to_SiteID_GW に設定します。この設定では、推奨されているように、サイトごとにデバイス プール SiteIDPhone が存在することを想定しています。

ローカル ルート グループ設定を使用することによって、PSTN アクセスの認識が容易になります。たとえば、Unified Border Element を PSTN への集中型アクセスに使用し、ローカル PSTN 接続をバックアップとして使用することができます。この場合は、デバイス プールによって Unified Border Element ルート グループが LRG_PSTN1 に指定され、LRG_PSTN2 にローカル ゲートウェイへのトランク（Trunk_to_SiteID_GW）が含まれます。

ボイス メッセージング

改訂日：2019 年 2 月 19 日

この章では、エンタープライズ コラボレーションのプリファード アーキテクチャに含まれるボイス メッセージング サービスについて説明します。この章では Cisco Unity Connection によるユニファイド メッセージング の実装方法について説明します。コア アーキテクチャの説明に加えて、展開プロセスの詳細も含まれています。

この章の新規情報とは

C：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。

C：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
コラボレーションシステム リリース（CSR）12.5 の一部の内容のマイナー 修正およびアップデート。	この章の各項で説明	2019 年 1 月 23 日
Cisco Smart Software Manager を介した Unity Connection ライセンス供与	ライセンスの要件（C：5-6 ページ）	2017 年 8 月 30 日
更新トークンを使用した OAuth サポートの有効化	3. ユニティコネクションの基本設定（C：5-17 ページ）	2017 年 8 月 30 日

前提条件

コア アプリケーションをプリファード アーキテクチャに導入する前に、以下の点を確認してください。

- Cisco Unified Communications Manager（Unified CM）が導入されており、機能している。
- Microsoft Active Directory がインストールされており、各アプリケーションの統合について理解している。
- このマニュアルのコール制御の章の内容を理解しており、この機能を実装している。

Cisco Unity Connection によるユニファイド メッセージング

Cisco Unity Connection により、エンタープライズ コラボレーション向けシスコ プリファード アーキテクチャのユニファイド メッセージングが有効になります。この項では、ボイス メッセージングとユニファイド メッセージングのための Unity Connection と、シングル インボックスおよびビジュアル ボイスメールなどの機能の導入に関する情報と手順を説明します。この項では、2 つの Unity Connection クラスタ間のネットワークについても説明します。

コア コンポーネント

コア アーキテクチャに含まれている要素を次に示します。

- Cisco Unified Communications Manager（Unified CM）
- Cisco Unity Connection
- Microsoft Exchange
- Microsoft Active Directory

主なメリット

- ユーザは次のいずれかを使用してボイスメール システムにアクセスし、ボイス メッセージを取得できます。
  - Cisco Unified IP Phone、TelePresence エンドポイント、Jabber、およびモバイル デバイス
  - PC または Mac の Web インターフェイス
  - 電子メール クライアント アプリケーション（Microsoft Outlook など）
- ビジュアル ボイスメールにより、Jabber クライアントのボイス メッセージのビジュアル表示にアクセスできます。この表示には、送信者の名前、日付、メッセージの長さも示されます。

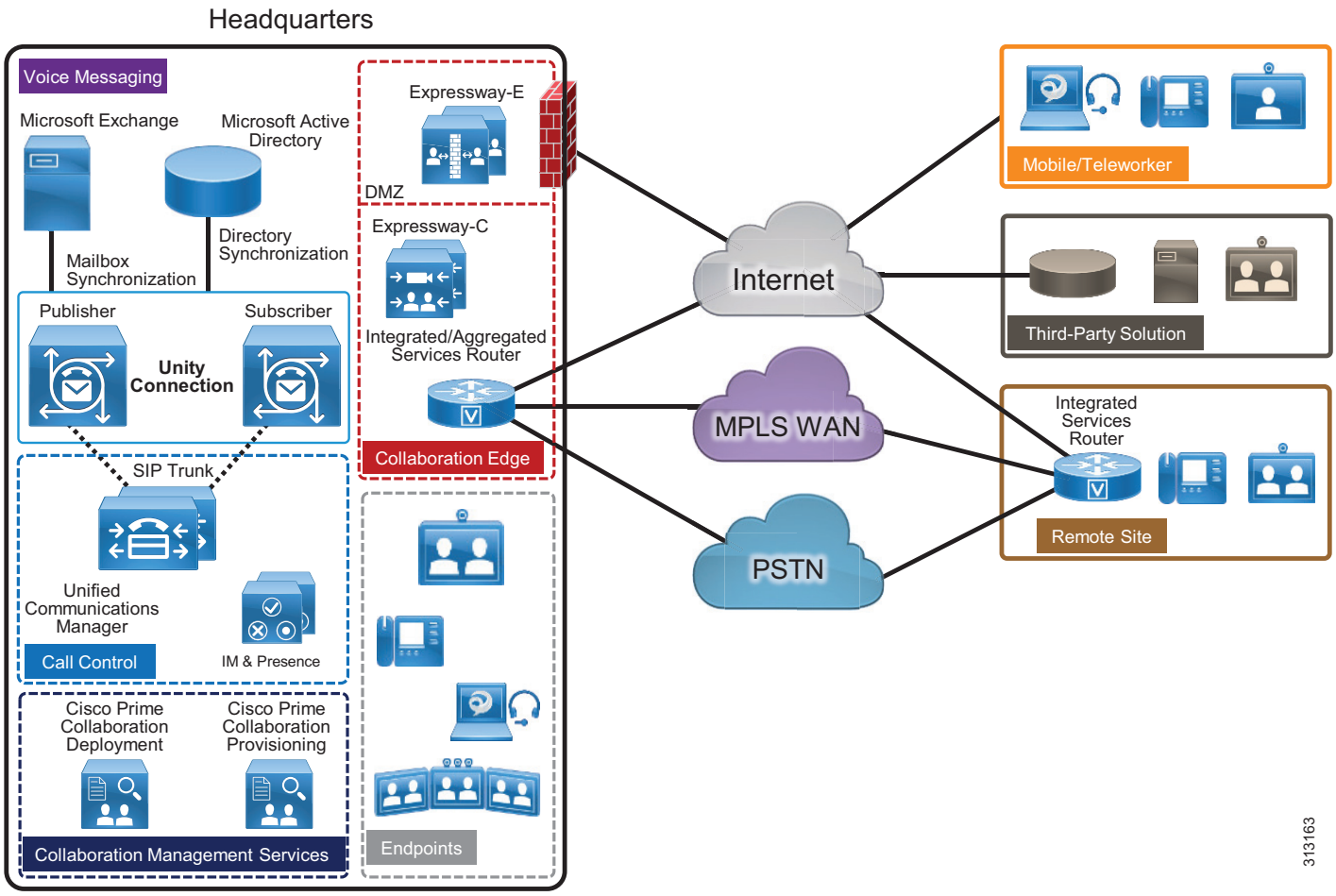
アーキテクチャー

プリファード アーキテクチャでは、このセクションで説明する、ボイス メッセージング用および呼処理用の集中型展開モデルが使用されます。

集中型メッセージングと集中型コール プロセッシング

C：図 5-1 に示すように、集中型メッセージングでは、Unity Connection が Unified Communications Manager（Unified CM）クラスタと同じサイトに配置されます。中央サイトから WAN 経由で接続しているリモート ブランチ サイトは、ユニファイド メッセージング サービスについて集中型 Unity Connection に依存しています。Unity Connection は、コール制御に SIP を使用し、メディア パスに RTP を使用して、Unified CM と統合しています。各 Unity Connection クラスタは 2 つのサーバ ノードで構成されており、高可用性と冗長性を備えています。

C：図 5-1　　アーキテクチャの概要



リモート ブランチ サイトでは、Cisco Unified Survivable Remote Site Telephony（SRST）がバックアップ コール エージェントとしてインストールされており、これは中央の Unity Connection サーバと統合しています。IP WAN の停止時には、リモート ブランチのすべての電話が SRST に登録されます。SRST は、無応答コールと話中コールを PSTN 経由で中央の Unity Connection サーバに送信するように事前に設定されています。

Unified CM の役割

Unified CM は、コール制御機能を備えており、着信側電話が話中または無応答の場合にコールを Unity Connection に転送します。ユーザが電話のメッセージ ボタンを押すか、または外部ネットワークからボイスメール パイロット番号にダイヤルすると、Unified CM はそのコールを Unity Connection にルーティングします。

Unity Connection の役割

集中型メッセージング環境では、Unity Connection によりユーザがボイスメールを保存および取得できます。一般に、Unity Connection に転送されるコールは直接コールであるか、または話中または無応答であった内線コールによるものです。ユーザに対し新しいメッセージが保存されている場合は、エンドポイントにメッセージ受信インジケータ（MWI）が表示されます。通常、電話システムと Unity Connection の間でコールごとに次のコール情報が渡されます。

- 着信側の内線番号
- 発信側の内線番号（内線の場合）、または発信側の電話番号（外線であり、電話システムが発信者 ID をサポートしている場合）
- 転送の理由（内線が通話中である、応答しない、またはすべてのコールを転送するように設定されている）

着信側が応答しないためにコールが転送された場合、Unity Connection は着信側ユーザの標準グリーティングを再生します。着信側電話が通話中であるためにコールが転送された場合、Unity Connection は着信側ユーザの通話中グリーティングを再生します。

Unity Connection は、直接コールと転送コールを異なる方法で処理します。Unity Connection は、コールを受信すると最初に発信者がユーザであるかどうかを判別します。このために、発信者 ID がユーザのプライマリ内線番号または代行内線番号に一致するかどうかを特定します。Unity Connection は一致を検出すると、ユーザが発信していると想定し、そのユーザのボイスメール PIN を入力するよう求めます。発信者 ID がユーザに関連付けられていないと Unity Connection が判断した場合、コールはガイダンスに送信されます。ガイダンスとは、外部の発信者が Unity Connection 自動応答に接続すると再生されるメイン グリーティングです。

Microsoft Exchange の役割

シングル インボックス機能を有効にするため、Unity Connection は Microsoft Exchange と統合されています。Unity Connection のシングル インボックスは、ユニファイド メッセージングを可能にし、Unity Connection と Microsoft Exchange の間でボイス メッセージを同期します。これにより、ユーザは電子メール クライアントを使用してボイスメールを受け取ることができます。

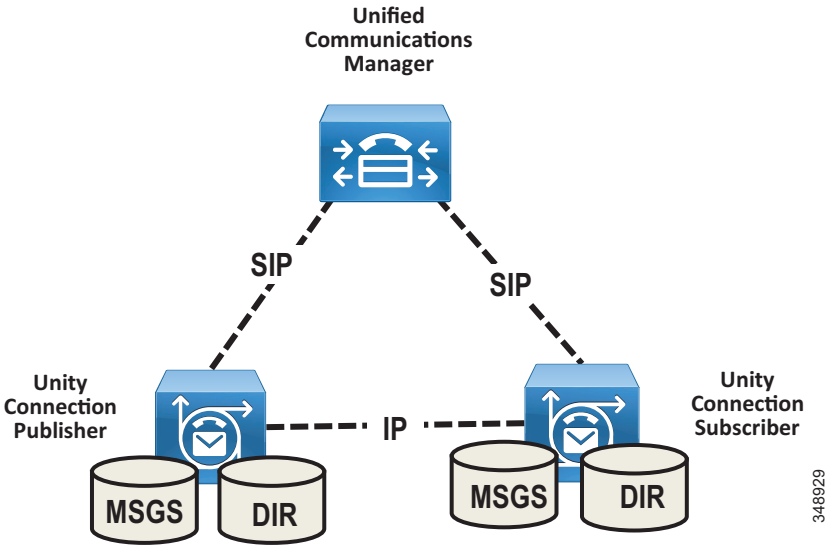
この章では、Microsoft Exchange が統合されている Unified Messaging を中心に説明します。Unity Connection は IBM Lotus Sametime インスタント メッセージング アプリケーションとも統合できます。この統合では、ユーザが Lotus Sametime を使用してボイス メッセージを再生できます。このトピックの詳細については、次の URL から入手可能な Unity Connection のマニュアルを参照してください。

https://www.cisco.com/en/US/products/ps6509/index.html

ユニファイド メッセージングの高適用性

C：図 5-2 に、アクティブ / アクティブ ペアの Unity Connection を示します。この場合、Unity Connection サーバを同じ建物または異なる建物に設置でき、高可用性と冗長性が実現します。アクティブ / アクティブ ペアの両方のサーバで Unity Connection が稼働しており、この両方のサーバでコールと HTTPS 要求が受け入れられ、ユーザ情報とメッセージが保存されます。クラスタ ペアの 1 つのサーバだけがアクティブな場合、Unity Connection は完全なエンドユーザ機能（ボイス コールと HTTPS 要求を含む）を維持します。ただし、コールに対する Unity Connection ポート キャパシティは半減し、単一サーバのキャパシティと同様になります。

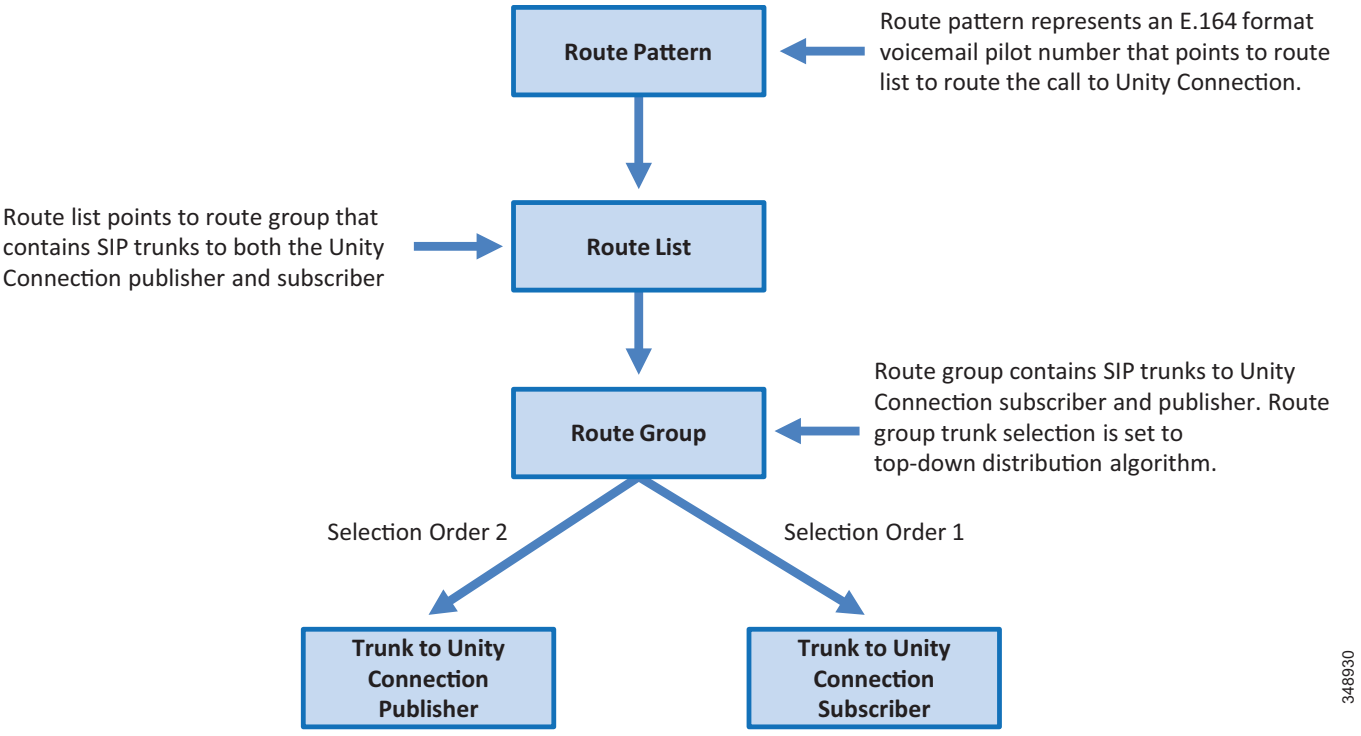
C：図 5-2　Unity Connection クラスタ



すべてのユーザ クライアント セッションおよび管理者セッション（IMAP および Cisco Personal Communications Assistant など）と管理トラフィック（Cisco Unity Connection の管理、一括管理ツール、バックアップ操作など）は、Unity Connection パブリッシャ サーバに接続します。パブリッシャ サーバが機能しなくなった場合、ユーザ クライアント セッションと管理者セッションは、Unity Connection サブスクライバ サーバに接続できます。

このトポロジでは、クラスタ内の各 Unity Connection サーバ ノードを指し示す 2 つの個別の Unified CM SIP トランクが必要です。この構成では、高可用性と冗長性の両方が実現します。すべてのコールを最初に Unity Connection サブスクライバ ノードにルーティングするように Unified CM を設定する必要があります。サブスクライバ サーバが使用不可であるか、またはサブスクライバのすべてのポートが使用中の場合、コールはパブリッシャ ノードにルーティングされます。Unified CM と Unity Connection 間で SIP が統合されている場合、トランクの選択は Unified CM ルート パターン、ルート リスト、およびルート グループ構成によって決まります。（C：図 5-3 を参照）。両方のトランクは同じルート グループに属し、同じルート リストに割り当てられています。ルート グループ内のトランクは、優先度順のトランク分配アルゴリズムを使用して並べ替えられます。この方法では、通常の運用時とフェールオーバー時の Unity Connection サーバ ノードの選択設定を Unified CM が制御できます。

C：図 5-3 Unity Connection SIP トランクの選択



Unity Connection では、高可用性のために Microsoft Exchange Database Availability Group（DAG）でのシングル インボックスの使用がサポートされています。DAG は、Microsoft の推奨事項に基づいて導入されます。高可用性を実現するため、Unity Connection ではクライアント アクセス サーバ（CAS）アレイへの接続もサポートされています。この項では、Microsoft Exchange の高可用性展開については説明しません。Exchange の高可用性展開の詳細については、http://www.microsoft.com/ で入手可能な Microsoft Exchange 製品情報を参照してください。

ライセンスの要件

Unity Connection のライセンスは Cisco Smart Software Manager によって管理されます。ライセンスされた機能を Unity Connection で使用するには、有効な機能ライセンスがお客様の Cisco Smart Software Manager ライセンス アカウントで使用可能になっている必要があり、Unity Connection はライセンスにアクセスして使用する目的で Cisco Smart Software Manager サービスと通信する必要があります。Cisco Smart Software Manager は、ユーザ ベースでライセンスを管理するための、Web に基づく集中型で全社規模のシンプルな管理機能を提供します。

ユニファイド メッセージングの要件

- Unity Connection は、Microsoft Exchange、Microsoft Business Productivity Online Suite（BPOS）専用サービス、および Microsoft Office 365 クラウドベース Exchange for Single Inbox をサポートします。
- Exchange サーバと Active Directory ドメイン コントローラ / グローバル カタログ サーバ（DC/GC）は、Microsoft がサポートする任意のハードウェア仮想環境にインストールできます。サポートされているハードウェア プラットフォームの詳細については、http://www.microsoft.com/ で入手可能な Microsoft Exchange の製品情報を参照してください。
- Microsoft Exchange メッセージ ストアは、Microsoft がサポートする任意のストレージ エリア ネットワーク コンフィギュレーションに格納できます。サポートされているストレージ エリア ネットワークの詳細については、http://www.microsoft.com/ で入手可能な Microsoft Exchange の製品情報を参照してください。
- 各サーバで 50 個のボイス メッセージング ポートごとに、Unity Connection と Microsoft Exchange の間でメッセージ同期のために 7 Mbps の帯域幅が必要となります。
- Unity Connection のデフォルト設定は、最大 2,000 ユーザと、Unity Connection と Microsoft Exchange サーバの間での最大 80 ミリ秒のラウンドトリップ遅延に十分に対応できます。2,000 を超えるユーザや 80 ミリ秒を超える遅延に対応する場合は、デフォルト設定を変更できます。詳細については、次の場所にある最新版『*Design Guide for Cisco Unity Connection*』で遅延に関する情報を参照してください。

  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

Unity Connection のスケーリング

Unity Connection クラスタは、最大 2 つのノード（アクティブ / アクティブ展開の 1 つのパブリッシャと 1 つのサブスクライバ）で構成されます。通常の運用時には、アクティブ / アクティブ展開では呼処理負荷分散は発生しません。Unified CM は、すべてのコールを最初に Unity Connection サブスクライバ サーバにルーティングするように設定されています。すべてのポートが使用中であるか、またはサブスクライバ サーバが使用不可の場合、コールはパブリッシャにルーティングされます。Unity Connection のサイジングでは、次の点を考慮してください。

- 現在と将来のユーザの総数
- ボイス メッセージングに必要なストレージ容量
- 各プラットフォームでサポートされるボイスメール ポートの数
- 暗号化が有効化されるかどうか

Unity Connection のスケーリングの詳細については、サイジング の章を参照してください。

Cisco Unity Connection 導入プロセス

このセクションでは、プリファード アーキテクチャでの Cisco Unity Connection の展開方法について説明します。

前提条件

ユニファイド メッセージング アーキテクチャを導入する前に、次の点を確認してください。

- Cisco Unified CM がインストールされ、コール制御用に設定されている（コール制御 の章を参照）。
- Microsoft Exchange がインストールされており、電子メール サーバとして設定されている。

展開の概要

このプリファード アーキテクチャの目的上、米国内の 3 か所のサイト（SJC、RCD、RTP）に対応する集中型メッセージング導入モデルを想定します。集中型メッセージングの導入では最初に、Unity Connection クラスタをインストールし、続いてプロビジョニングと設定を行います。Cisco Unity Connection で集中型メッセージングを導入するには、次のタスクを記載の順に行います。

1. Unity Connection クラスターのプロビジョニング
2. Unity Connection 統合のための Unified CM の設定
3. ユニティコネクションの基本設定
4. シングル インボックスの有効化
5. ビジュアル ボイスメールの有効化
6. SRST モードでのボイスメール
7. 2 つのユニティコネクションクラスタの HTTPS インターネットワーキング

注 このマニュアルでは、非デフォルト値およびその他の設定フィールド値だけが示されています。フィールド設定値が示されていない場合は、デフォルト値が想定されます。

1. Unity Connection クラスターのプロビジョニング

Unity Connection サーバ ノードをクラスタリングする場合、サーバ ペアの 1 方がパブリッシャ サーバ、もう 1 方がサブスクライバ サーバとして指定されます。

パブリッシャー

Unity Connection では、アクティブ / アクティブの高可用性を実現するために 2 つのサーバのみがクラスタでサポートされています。パブリッシャ サーバは最初にインストールするサーバであり、データベースとメッセージ ストアをパブリッシュし、クラスタ内のもう一方のサブスクライバ サーバにこの情報をレプリケートします。

サブスクライバー

ソフトウェアをインストールしたら、サブスクライバ サーバ ノードをパブリッシャに登録して、データベースとメッセージ ストアのコピーを取得します。

Unity Connection メールボックス ストア

インストール時に、Unity Connection により次のものが自動的に作成されます。

- ディレクトリ データベース：システム設定情報（ユーザ データ、テンプレート、サービス クラスなど）に使用されます。
- メールボックス ストア データベース：ボイス メッセージに関する情報（メッセージの送信先、送信時刻、ハードディスク上の WAV ファイルの場所など）に使用されます。
- オペレーティング システム ディレクトリ：ボイス メッセージの WAV ファイルに使用されます。

サーバを同じ建物に設置する場合の Unity Connection クラスタ導入の前提条件

- Unity Connection に対する着信コールと発信コールのためには、次の場所にある『*Security Guide for Cisco Unity Connection*』の最新版の「*IP Communications Required by Cisco Unity Connection*」に関する章に記載されているように、ファイアウォールの TCP ポートと UDP ポートが開いている必要があります。

  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html
- 2 つの仮想マシンが含まれているクラスタでは、この両方のマシンが同一の仮想プラットフォーム オーバーレイに属している必要があります。
- サーバはファイアウォールによって隔離されてはなりません。
- 両方の Unity Connection サーバが同一のタイム ゾーンに位置している必要があります。
- 両方の Unity Connection サーバ ノードは同一の電話システムに統合されている必要があります。
- 両方の Unity Connection サーバで、同じ機能と構成が有効である必要があります。

サーバを異なる建物に設置する場合の Unity Connection クラスタ導入の前提条件

- Unity Connection に対する着信コールと発信コールのためには、次の場所にある『*Security Guide for Cisco Unity Connection*』の最新版の「*IP Communications Required by Cisco Unity Connection*」に関する章に記載されているように、ファイアウォールの TCP ポートと UDP ポートが開いている必要があります。

  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html
- 2 つの仮想マシンが含まれているクラスタでは、この両方のマシンが同一の仮想プラットフォーム オーバーレイに属している必要があります。
- 両方の Unity Connection サーバ ノードは同一の電話システムに統合されている必要があります。
- 両方の Unity Connection サーバで、同じ機能と構成が有効である必要があります。
- 各 Unity Connection サーバ ノードのボイス メッセージング ポートの数に応じて、サーバ ノード間の接続に、次に示す定常輻輳のない保証帯域幅が必要です。
  - 各サーバで 50 個のボイス メッセージング ポートごとに、7 Mbps の帯域幅が必要となります。
  - 最大往復遅延は、150 ミリ秒（ms）以下でなければなりません。

Unity Connection クラスターを導入する

- ポートの最大数とユーザの最大数に基づいて、Unity Connection ノードに導入する VMware Open Virtual Archive（OVA）テンプレートを決定します。Unity Connection のスケーリングの項を参照してください。
- 両方の Unity Connection ノードをホスト A レコードとして企業のドメイン ネーム サービス（DNS）サーバに追加します。たとえば、パブリッシャ Unity Connection ホスト名を US-CUC1.ent-pa.com と設定し、サブスクライバ ホスト名を US-CUC2.ent-pa.com と設定します。
- インストールに必要なネットワーク パラメータを判別します。
  - サーバのタイム ゾーン
  - ホスト名、IP アドレス、ネットワーク マスク、およびデフォルト ゲートウェイ。ホスト名と IP アドレスが前の DNS 設定に一致していることを確認します。
  - DNS IP アドレス
  - ネットワーク タイム プロトコル（NTP）サーバの IP アドレス
- 該当する OVA ファイルを Cisco Web サイトからダウンロードします。
- VMware vSphere Client を使用して Unity Connection のパブリッシャ サーバ ノードとサブスクライバ サーバ ノードを展開します。
- Cisco Prime Collaboration Deployment を使用して、Unity Connection のパブリッシャ ノードとサブスクライバ ノードをインストールします。

詳細については、コラボレーション管理サービスの章の Cisco Prime Collaboration Deployment に関するセクションを参照してください。

注 必要に応じて、Unity Connection クラスタを手動で展開することもできます。その場合は、まず、VMWare ホスト上で推奨される OVA を使って Unity Connection パブリッシャ ノードを展開した後、そのパブリッシャ ノードに Unity Connection パッケージを手動でインストールします。パブリッシャ ノードのインストールが完了したら、サブスクライバ ノード向けのプロセスを繰り返します (VMWare ホスト上で OVA を展開し、Unity Connection パッケージを手動でインストールします)。

2. Unity Connection 統合のための Unified CM の設定

Unity Connection が Unified CM と通信する前に、Unified CM で実行する必要があるタスクがあります。Unity Connection は SIP トランクを介して Unified CM と通信します。この項では、Unified CM を Unity Connection と統合するために必要なタスクの概要を説明します。

エンドユーザ PIN 同期のための Unity Connection アプリケーションのユーザー名とサーバー

エンドユーザ PIN 管理を簡略化するには、Unified CM と Unity Connection の間の PIN 同期を有効にします。PIN 同期を使用すれば、エンドユーザは、ボイス メール アクセス、Extension Mobility、および Conference Now などの複数の目的に同じ PIN を使用できます。ユーザが PIN 番号を変更するのに Unified CM セルフケア ポータルを使用するか、それとも Cisco Unity Connection Personal Communications Assistant (PCA) を使用するかに関係なく、PIN が同期されます。

最初に、Unity Connection システム管理者アカウントのユーザ名とパスワードに一致する 1 人のアプリケーション ユーザが設定されていることを確認します（たとえば **administrator**）。Unified CM と Unity Connection でシステム管理者アカウントの名前とパスワードが同じであれば、このアカウントはすでに設定済みです。

次に、C：表 5-2 に示すように、パブリッシャ ノードとサブスクライバ ノードの両方の新しい Unity Connection アプリケーション サーバを追加します。

C：表 5-2　Unity Connection アプリケーション サーバの定義

パラメータ	値	注
[名前（Name）]	**US-CUC1**	Unity Connection サーバの名前を入力します。
[IP アドレス（IP Address）]	*<IP_Address_US-CUC1>*	Unity Connection サーバの IP アドレスを入力します。
選択されたアプリケーション ユーザ	**管理者**	Unity Connection システム管理者アカウントに一致するアプリケーション ユーザを選択します。
エンド ユーザ PIN 同期を有効化	オン	Unified CM（Extension Mobility 用など）と Unity Connection（ボイス メッセージ アクセス用）の間のエンド ユーザ PIN 同期を有効にするには、オンにします。

注　Unified CM と Unity Connection の間のエンドユーザ PIN 同期を有効にする際には、Unified CM で割り当てられる PIN 認証ルールと Unity Connection で割り当てられるボイスメール認証ルールが、最小クレデンシャル長および有効期限の点で必ず一致することが重要です。これらの認証ルールが一致するよう調整しない場合、PIN 同期エラーやログイン障害が発生する可能性があり、管理者の介入が必要になることもあります。

注　PIN 同期が機能するためには、Unity Connection と Unified CM の両方に、**tomcat-trust** に読み込まれる遠端サーバまたはルート CA 証明書が含まれている必要があります。証明書管理の詳細については、セキュリティーの章を参照してください。

SIP トランク セキュリティー プロファイル

メディアおよびシグナリングの暗号化に関して、このマニュアルではこれらの暗号化は使用されず、代わりに Unified CM と Unity Connection サーバ ノードの間には非セキュアな SIP トランクが実装されていることを前提としています。デバイス セキュリティ モードが [非セキュア（Non Secure）] に設定された状態で、Unity Connection に新規 SIP トランク セキュリティ プロファイルを作成します。C：表 5-3 に、SIP トランク セキュリティ プロファイルの設定を示します。

C：表 5-3　SIP トランク セキュリティ プロファイルの設定

パラメータ	値	注
[名前（Name）]	Unit Connection SIP トランク セキュリティ プロファイル	セキュリティ プロファイルの名前を入力します。
[説明（Description）]	Unit Connection SIP トランク セキュリティ プロファイル	プロファイルの説明を入力します。
[デバイスセキュリティモード（Device Security Mode）]	非セキュア（Non Secure）	SIP トランクのセキュリティ モード。
[ダイアログ外 REFER の許可（Accept Out-of-Dialog refer）]	オン	Unified CM が、SIP トランク経由で着信する非インバイトの ダイアログ外 REFER メッセージを受け入れることを指定します。
[未承諾 NOTIFY の許可（Accept unsolicited notification）]	オン	Unified CM が、SIP トランク経由で着信する非インバイトの未承諾 NOTIFY メッセージを受け入れることを指定します。Unity Connection から MWI メッセージを受け入れるには、このパラメータをオンにする必要があります。
[REPLACE ヘッダの許可（Accept replaces header）]	オン	Unified CM が、既存の SIP ダイアログを置き換える新しい SIP ダイアログを受け入れることを指定します。これにより、Cisco Unity Connection が開始する監視転送に使用される "REFER w/replaces" を渡すことができるようになります。

SIP プロファイル

Unity Connection への SIP トランクの SIP プロファイルを設定します。標準 SIP プロファイルをコピーし、その名前を **Unity Connection SIP Profile** に変更します。Unified CM サーバの IP アドレスが、Unified CM により送信される SIP 発呼側情報に含まれないようにするには、[SIP 要求で完全修飾ドメイン名を使用（Use Fully Qualified Domain Name in SIP Requests）] チェックボックスをオンにします。[サービスタイプ " なし (デフォルト)" のトランクの接続先ステータスをモニタするために OPTIONS Ping を有効にする（Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"）] チェックボックスがオンになっていることを確認します。これにより、システムが Unity Connection ノードへの接続の状況を追跡できます。

OPTIONS Ping が有効な場合、トランクの SIP デーモンを実行する各ノードは、トランクの各宛先 IP アドレスに対して OPTIONS 要求を定期的に送信して到達可能性を判断し、到達可能なノードにのみコールを送信します。宛先アドレスが OPTIONS 要求に応答しない場合、Service Unavailable（503）応答または Request Timeout（408）応答を送信する場合、または TCP 接続を確立できない場合、そのアドレスは「アウト オブ サービス」と見なされます。1 つ以上のノードが、1 つ以上の宛先アドレスから（408 または 503 以外の）応答を受信した場合、トランク全体の状態は「イン サービス」と見なされます。SIP トランク ノードは、トランクの設定済み宛先 IP アドレス、またはトランクの DNS SRV エントリの解決済み IP アドレスに対して OPTIONS 要求を送信できます。すべての SIP トランクで SIP OPTIONS Ping を有効にすることを推奨します。有効にすることで、Unified CM は、コールごとの状態、ノードごとの状態、およびタイムアウトに基づいて判別するのではなく、動的にトランクの状態を追跡することができるためです。

SIP トランク

クラスタ内の Unity Connection サーバ ノードごとに 1 つずつ、合計で 2 つの個別 SIP トランクを作成します。C：表 5-4 に SIP トランクの設定を示します。

C：表 5-4　Unity Connection サーバへの SIP トランクのパラメータ設定

パラメータ	値	説明
名前（Name）	US_CUC1_SIP_Trunk	Unity Connection への SIP トランクの固有名を入力します。
[説明（Description）]	Unity Connection パブリッシャ	SIP トランクの説明を入力します。
[デバイスプール（Device Pool）]	Trunks_and_Apps	Unity Connection のデバイス プールを入力します。（コール制御の章を参照。）
[すべてのアクティブな Unified CM ノードで実行（Run on All Active Unified CM Nodes）]	オン	SIP トランクを使用した発信コールでは、Unified CM 呼処理サブスクライバ間のクラスタ内制御シグナリングが必要ではないことを指定します。
[コールルーティング情報 - インバウンドコール（Call Routing Information - Inbound Calls）]		
[コーリングサーチスペース（CSS）（Calling Search Space (CSS)）]	ボイスメール（CSS 設定の詳細については、コール制御の章を参照してください。）	割り当てられる CSS には、DID、DID 以外の番号、URI パーティションなどのすべてのネットワーク上の宛先が含まれています。CSS にこれらのすべてのパーティションが含まれていないと、Unity Connection からの MWI 未承認 NOTIFY メッセージがユーザの電話に到達しません。
[Diversion ヘッダー配信のリダイレクト - インバウンド（Redirecting Diversion Header Delivery - Inbound）]	オン	リダイレクト情報要素、最初のリダイレクト番号、およびコール転送理由が着信メッセージの一部として送信され、受け入れられることを指定します。Unity Connection は最初のリダイレクト番号を使用してコールに応答します。

C：表 5-4　Unity Connection サーバへの SIP トランクのパラメータ設定（続き）

パラメータ	値	説明
[コールルーティング情報 - アウトバウンドコール（Call Routing Information - Outbound Calls）]		
[発呼側および接続側情報形式（Calling and Connected Party Info Format）]	[接続側にのみ URI および DN を配信 (使用可能な場合) （Deliver URI and DN in connected party, if available）]	このオプションは、Unified CM がディレクトリ番号、ディレクトリ URI、またはディレクトリ番号とディレクトリ URI の両方を含むアドレスを、発信 SIP メッセージの SIP ID ヘッダーに挿入するかどうかを決定します。
[Diversion ヘッダー配信のリダイレクト - アウトバウンド（Redirecting Diversion Header Delivery - Outbound）]	オン	リダイレクト情報要素、最初のリダイレクト番号、およびコール転送理由が発信メッセージの一部として送信され、受け入れられることを指定します。Unity Connection は最初のリダイレクト番号を使用してコールに応答します。
[SIP 宛先情報（SIP Destination Information）]		
[宛先アドレス（Destination Address）]	us-cuc1.ent-pa.com	Unity Connection サーバの完全修飾ドメイン名（FQDN）を入力します。
[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]	Unit Connection SIP トランク セキュリティ プロファイル	C：表 5-3 を参照してください。
[SIP プロファイル（SIP Profile）]	Unity Connection SIP プロファイル	SIP プロファイルを参照してください。

ルート グループ

Unity Connection クラスタに対し、別のルート グループ RG_CUC を作成します。このルート グループには、Unity Connection サブスクライバ ノードとパブリッシャ ノードへの SIP トランクが含まれています。リストに、サブスクライバ ノードに接続する SIP トランク（US_CUC2_SIP_Trunk）が最初に示され、続いてパブリッシャ ノードに接続する SIP トランク（US_CUC1_SIP_Trunk）が示されていることを確認してください。ルート グループ分配アルゴリズムとして、[優先度順（Top Down）] トランク選択方式を設定する必要があります。[優先度順（Top Down）] 分配アルゴリズムが設定されているルート グループでは常に、コールが最初に Unity Connection サブスクライバ サーバ ノード（US-CUC2）に送信されます。Unity Connection サブスクライバ サーバ ノードがビジーまたは使用不可の場合、コールはパブリッシャ サーバ ノード（US-CUC1）に送信されます。

ルート リスト

Unity Connection クラスタに対し、別のルート リスト RL_CUC を作成します。このルート リストには、前述の説明で作成した Unity Connection ルート グループ（RG_CUC）だけが含まれている必要があります。[このルートリストを有効にする（Enable this Route List）] と [すべてのアクティブな Unified CM ノードで実行（Run on all Active Unified CM Nodes）] オプションが選択されていることを確認してください。

ルート パターン

前述の説明で作成した Unity Connection ルート リストを指し示すボイスメール パイロット番号の別のルート パターンを作成します。この番号はボイスメール パイロット番号に一致している必要があります。C：表 5-5 に、ルート パターンの設定例を示します。

C：表 5-5　Unity Connection パイロット番号：ルート パターンの例

パラメータ	値
[ルートパターン（Route Pattern）]	+14085554999
[ルートパーティション（Route Partition）]	DN
[ゲートウェイ / ルートリスト（Gateway/Route List）]	RL_CUC
[コールの分類（Call Classification）]	オンネット（OnNet）
[外部ダイヤルトーンの提供（Provide Outside Dial Tone）]	オフ

ボイスメールパイロット

ボイスメール パイロット番号は、ユーザがボイス メッセージにアクセスするための電話番号を指定します。Unified CM は、ユーザが IP エンドポイントの [メッセージ（Messages）] ボタンを押すと、自動的にボイスメール パイロット番号にダイヤルします。3 つのサイトすべてに対して 1 つのボイスメール パイロット番号が作成されます。C：表 5-6 に、ボイスメール パイロットの設定例を示します。

C：表 5-6　ボイスメール パイロットの例

パラメータ	値
[ボイスメールパイロット番号（Voice Mail Pilot Number）]	+14085554999
[コーリングサーチスペース（Calling Search Space）]	DN
[説明（Description）]	VM Pilot
[システムのデフォルトボイスメールパイロットに設定（Make this the default Voice Mail Pilot for the system）]	オン

リモート サイトのボイスメール ユーザは、各自の DID 範囲からボイスメール アクセス番号にダイヤルして、PSTN からメッセージを確認できます。ボイスメール PSTN アクセス番号をボイスメール パイロット番号に変換するためのトランスレーション パターンが個別に作成されます。表 6 に、ボイスメール パイロットのトランスレーション パターンの設定を示します。

C：表 5-7　ボイスメール パイロットのトランスレーション パターンの例

パラメータ	値
[トランスレーションパターン（Translation Pattern）]	+19195551999
[パーティション（Partition）]	DN
[発信側コーリングサーチスペースを使用（Use Originators Calling Search Space）]	オン
[ルートオプション（Route Option）]	[このパターンをルーティング（Route this pattern）]
[着信側トランスフォーメーション（Called Party Transformations）]	
[着信側トランスフォーメーションマスク（Called Party Transform Mask）]	+14085554999

他のリモート サイト向けに追加のトランスレーション パターンが作成されます。

ボイスメール プロファイル

すべてのエンドポイント デバイスとエクステンション モビリティ プロファイルで、各ユーザの電話回線に対してボイスメール プロファイルが割り当てられます。このプロファイルにより、ユーザはエンドポイントの [メッセージ（Messages）] ボタンを押すだけで、ボイスメール システムにワンタッチでアクセスできます。Unity Connection が単一電話システムに統合されている場合は、デフォルトのボイスメール プロフィルを使用することを推奨します。エンドポイント デバイスでの回線の初期プロビジョニング時に、デフォルトのボイスメール プロファイル（[なし（None）]）が電話番号に割り当てられます。ボイスメールにアクセスする必要がないユーザの場合、そのエンドポイント回線にボイスメール プロファイルが割り当てられません。C：表 5-8 に、ボイスメール プロファイルの設定例を示します。

C：表 5-8　ボイスメール プロファイルの例

パラメータ	値
[ボイスメールプロファイル名（Voice Mail Profile Name）]	デフォルト
説明	VM プロファイル
[ボイスメールパイロット（Voice Mail Pilot）]	+14085554999/DN
[ボイスメールマスク（Voice Mail Mask）]	空欄
[システムのデフォルトボイスメール プロファイルとして使用する（Make this the default Voice Mail Profile for the System）]	オン

3. ユニティコネクションの基本設定

サービスのアクティベーション

- Unity Connection のインストールが完了したら、Cisco Unified Serviceability にログインし、パブリッシャ サーバ ノードの **DirSync** サービスをアクティブにします。
- [ユニファイドサービスアビリティ（Unified Serviceability）] で [ツール（Tools）] –> [コントロールセンターの機能サービス（Control Centre-Feature Services）] に移動します。パブリッシャ サーバ ノードで Cisco DirSync サービスが開始していることを確認します。
- [Unity Connection のサービスアビリティ（Unity Connection Serviceability）] で [ツール（Tools）] –> [サービス管理（Service Management）] に移動します。パブリッシャおよびサブスクライバ Unity Connection サーバ ノードでサービスのステータスを確認します。C：表 5-9 に、この導入環境のサービス ステータスを示します。

C：表 5-9　Unity Connection サービス ステータス

サービス	Unity Connection パブリッシャ（プライマリ）	Unity Connection サブスクライバ (セカンダリ)
ステータスのみのサービス（OS コマンド ライン インターフェイスから非アクティブにできます）		
このカテゴリのすべてのサービス	はい	はい
重要なサービス		
接続会話マネージャ	はい	はい
接続メールボックスの同期	はい	いいえ（No）
接続メッセージ転送エージェント	はい	いいえ（No）
接続ミキサー	はい	はい
接続通知	はい	いいえ（No）
基本サービス		
このカテゴリのすべてのサービス	はい	はい
オプション サービス		
接続ブランチ同期サービス	いいえ（No）	いいえ（No）
コネクション デジタル ネットワーク レプリケーションエージェント	いいえ（No）	いいえ（No）
このカテゴリに含まれるその他の残りのすべてのサービス (Connection Jetty と Connection REST サービスを含む)	はい	はい

データベースのリプリケーション

パブリッシャとサブスクライバの両方の Unity Connection サーバ ノードでサービスをアクティブにした後、サブスクライバ ノードからパブリッシャ ノードに接続できることを確認します。また、両方のノードで OS コマンド ライン インターフェイス（CLI）のコマンド **show perf query class "Number of Replicates Created and State of Replication"** を使用して、データベース レプリケーションのステータスを確認します。

Unified CM の統合

各 Unity Connection クラスタは、同じ場所に配置されている Unified CM クラスタと統合されます。これにより、Unified CM クラスタ専用の各 Unity Connection クラスタによる単純な統合モデルが実現します。Unified CM では Unity Connection クラスタとの相互接続のために SIP トランクが設定されますが、Unity Connection システムではキャパシティとライセンスの目的で、ボイスメール ポートが使用されます。この項では、設計時の考慮事項、キャパシティ プランニング、ボイスメール ポートの設定について説明します。

ボイスメール ポートのオーディオ コーデック設定

Unity Connection では、Unity Connection SIP シグナリングでサポートされるオーディオ コーデック形式のコールは常に PCM リニアにトランスコードされます。PCM リニアから、Unity Connection Administration のシステムレベル録音オーディオ コーデック システム全体設定で録音がエンコードされます。デフォルトは G.711 mu-law です。

この項では、発信側デバイスと Unity Connection の間でネゴシエートされるオーディオ コーデックを*回線コーデック*と呼び、システムレベルの録音用オーディオ コーデックとして設定されたオーディオ コーデックを*録音コーデック*と呼びます。

サポートされる回線コーデック（公表コーデック）

- G.711 mu-law
- G.711 a-law
- G.722
- G.729
- iLBC

サポートされる録音コーデック（システムレベルの録音オーディオ コーデック）

- PCM リニア
- G.711 mu-law（デフォルト）
- G.711 a-law
- G.729a
- G.726
- GSM 6.10

トランスコーディングは、本来すべての接続で発生するので、ライン コーデックと録音コーデックが違っても、システムへの影響にほとんど違いはありません。たとえば、G.729a を回線コーデックとして、G.711 mu-law を録音コーデックとして使用しても、Unity Connection サーバにはトランスコーディングに伴う大きな追加負荷はかかりません。しかし、iLBC コーデックまたは G.722 コーデックはトランスコーディングにより多くの計算を必要とするので、Unity Connection サーバに大きな追加負荷がかかります。そのため、Unity Connection サーバがサポートできる G.722 または iLBC 接続の数は、G.711 mu-law 接続の数の半分のみです。

このトポロジの例では、システム録音コーデックはデフォルト（G.711 mu-law）のままです。サポートされる回線コーデックは G.729 および G.711 mu-law に設定されます。このデフォルト設定を使用する場合、同一の Unity Connection サイトのユーザは G711 mu-law を使用します。中央の Unity Connection サーバに WAN 経由で接続するユーザの場合、選択される回線コーデックは G.729 です。

G.722 コーデックまたは iLBC コーデックを回線コーデック（アドバタイズされているコーデック）として使用すると、Cisco Unity Connection サーバでプロビジョニング可能なボイス ポートの数が減少します。G.722 または iLBC コーデックを使用する場合に各プラットフォーム オーバレイでサポートされるボイス ポートの数の詳細については、『Virtualization for Cisco Unity Connection』を参照してください。

システム設定（System Settings）

Unified CM コール制御システムの場合と同様に、Unity Connection ボイスメール システムでは更新トークンを使用した OAuth が必要です。更新トークンを使用した OAuth をシステムで有効にして、Unified CM パブリッシャ ノードを承認 (Authz) サーバとして設定する必要があります。

[Cisco Unity Connection Administration] > [システム設定（System Settings）] > [エンタープライズ パラメータ（Enterprise Parameters）] に移動して、[SSO と OAuth の設定（SSO and OAuth Configuration）] セクションで、[更新ログイン フローを使用した OAuth（OAuth with Refresh Login Flow）] を [有効（Enabled）] に設定します。

次に、[システム設定（System Settings）] > [Authz サーバ（Authz Servers）] に移動して、[新規追加（Add New）] ボタンをクリックし、Authz サーバを追加します。C：表 5-10 に、Unified CM パブリッシャを追加して AuthZ サーバとして設定するための Authz サーバ設定を示します。

C：表 5-10　Authz サーバ設定

パラメータ	値	説明
Display Name	Authz サーバ（us-cm-pub）	この設定は、Authz サーバの表示名を定義します。
[認証サーバ（Authz Server）]	us-cm-pub.ent-pa.com	この設定は、Unified CM パブリッシャ ノードである Authz サーバの FQDN を指定します。
[ポート（Port）]	8443（デフォルト）	この設定は、Authz サーバとの通信に使われるポートを決定します。
[ユーザ名（Username）]	管理者	これは、Unity Connection が Authz サーバへのサインインに使用するユーザ名です。
[パスワード（Password）]	*<password>*	これは、Unity Connection が Authz サーバへのサインインに使用するパスワードです。
[証明書エラーを無視する（Ignore Certificate Errors）]	オフ（デフォルト）	この設定は、Unity Connection が Authz サーバから受信した証明書を検証するかどうかを決定します。

[保存（Save）] をクリックして、Authz サーバを作成し、キーを同期します。

電話システムの設定

電話システムの統合により、Unity Connection と Unified CM の間の通信が実現します。Unity Connection が 1 つの Unified CM クラスタと統合している場合は、デフォルトの **PhoneSystem** を使用することを推奨します。C：表 5-11 に、電話システムの設定を示します。

C：表 5-11　電話システムの設定

パラメータ	値	説明
[電話システムの名前（Phone System Name）]	PhoneSystem	電話システム
[デフォルト TRAP 電話システム（Default TRAP Phone System）]	オン	電話システムにより TRAP 接続が有効になるので、ボイス メール ボックスを使用していない管理者とユーザが、Unity Connection Web アプリケーションで電話から録音、再生できます。
[内線番号を使用したコールループの検出（Call Loop Detection by Using Extension）]		
[転送メッセージ通知コールに対して有効にする (内線番号を使用)（Enable for Forwarded Message Notification Calls (by Using Extension)）]	オン	（携帯電話などの）デバイスに送信される新規メッセージ通知、およびデバイスが応答しなかったために Unity Connection にデバイスが再転送した新規メッセージ通知を Unity Connection で内線番号を使用し検出して拒否します。コールループが検出されず拒否されない場合、コールによってユーザ宛ての新しいボイス メッセージが作成され、Unity Connection が新規メッセージ通知のコールをデバイスに送信します。
[発信コール規制（Outgoing Call Restrictions）]		
[発信コールを有効にする（Enable outgoing calls）]	オン	Unity Connection は、必要に応じて電話システムを通じて発信コール（MWI の設定など）をかけます。
[AXL サーバ（AXL Servers）]（[編集（Edit）] > [Cisco Unified Communications Manager AXL サーバ（Cisco Unified Communications Manager AXL Servers）] の下)		
[順序 0（Order 0）]	*<IP_Address_US-CM-PUB>*	Unified CM AXL サーバ ノード（パブリッシャ）の IP アドレスを入力します。
[ポート（Port）]	8443	Unity Connection が AXL 通信に使用する Unified CM サーバの TCP ポートを入力します。
[ユーザ名 / パスワード（Username/Password）]	管理者	「標準 AXL API アクセス」の役割を持つ Unified CM アプリケーション ユーザのユーザ名とパスワードを入力します。
[Cisco Unified Communications Manager のバージョン（Cisco Unified Communications Manager Version）]	5.0 以降（SSL 対応）	Unified CM 5.0 以降のバージョンの SSL を指定します。
[プライマリ AXL サーバのエンドユーザ暗証番号同期を有効にする（Enable End User PIN Synchronization for Primary AXL Server）]	オン	Unity Connection（ボイス メッセージ アクセス用）と Unified CM（Extension Mobility 用など）の間でエンドユーザ PIN 同期を有効にするには、オンにします。
[証明書エラーを無視する（Ignore Certificate Errors）]	オフ	Unity Connection が Unified CM Tomcat 証明書を必ず検証するようにするには、オフにします。

注　Unified CM と Unity Connection の間のエンドユーザ PIN 同期を有効にする際には、Unified CM で割り当てられる PIN 認証ルールと Unity Connection で割り当てられるボイスメール認証ルールが、最小クレデンシャル長および有効期限の点で必ず一致することが重要です。これらの認証ルールが一致するよう調整しない場合、PIN 同期エラーやログイン障害が発生する可能性があり、管理者の介入が必要になることもあります。

ポート グループの設定

ポート グループを使用して、Unified CM クラスタと Unity Connection クラスタの間の SIP 通信を制御します。ポート グループを使用することで、システムは Unity Connection サーバが受け入れる SIP メッセージの送信元 Unified CM と、Unity Connection サーバが発信コールを Unified CM サーバにルーティングするときに使用する設定と順序を制限および指定できます。Unity Connection サーバは、Unity Connection 向けの Unified CM SIP ルーティング設計をミラーするように設定されているため、Unity Connection サーバで発信ルーティングが 1 番目に使用可能な Unified CM サブスクライバ ノードを選択するように設定する必要があります。C：表 5-12 に、ポート グループの設定を示します。

C：表 5-12　ポート グループの設定

パラメータ	値	説明
[表示名（Display Name）]	PhoneSystem-1	電話システムの記述名
[連動方法（Integration Method）]	SIP	Unity Connection と Unified CM の接続に使用する連動方法。
[セッション開始プロトコル (SIP) の設定（Session Initiation Protocol (SIP) Settings）]		
[SIP サーバで登録する（Register with SIP Server）]	オン	これにより、Cisco Unity Connection が SIP サーバに登録されます。
[SIP サーバ（SIP Servers）]（[編集（Edit）] > [サーバ（Servers）] の下）		
[順序 0（Order 0）]	*<IP_Address_US-CM-SUB1>*	順序 0 に設定されている SIP サーバには高い優先度が設定されます。プライマリ Unified CM 呼処理ノードの IP アドレスを入力します。
[順序 1（Order 1）]	*<IP_Address_US-CM-SUB2>*	順序 1 に設定されている SIP サーバには低い優先度が設定されます。セカンダリ Unified CM 呼処理ノードの IP アドレスを入力します。
[ポート（Port）]	5060	Unity Connection が SIP 通信に使用する Unified CM サーバの TCP ポートを入力します。
[TLS ポート（TLS Port）]	5061	Unity Connection がセキュア SIP 通信に使用する Unified CM サーバの TCP TLS ポートを入力します。
[TFTP サーバ（TFTP Servers）]（[編集（Edit）] > [サーバ（Servers）] の下）		

C：表 5-12　ポート グループの設定（続き）

パラメータ	値	説明
[順序 0（Order 0）]	*<IP_Address_US-CM-TFTP1>*	順序 0 に設定されている TFTP サーバには、より高い優先度が与えられます。プライマリ Unified CM TFTP ノードの IP アドレスを入力します。
[順序 1（Order 1）]	*<IP_Address_US-CM-TFTP2>*	順序 1 に設定されている TFTP サーバには、より低い優先度が与えられます。バックアップ Unified CM TFTP ノードの IP アドレスを入力します。

ボイス メッセージング ポートのサイジングに関する考慮事項

クラスタ内の各 Unity Connection サーバでは、いずれかのサーバが停止した場合のために、次のダイヤルイン機能用のボイス メッセージング ポートが指定されている必要があります。

- コールへの応答

各 Unity Connection サーバではさらに、次の発信機能用のボイス メッセージング ポートが指定されている必要があります。

- メッセージ受信インジケータ（MWI）の送信
- メッセージ到着通知の実行
- 電話での録音および再生（TRAP）接続の許可

システムのボイスメール ポートの合計数の 20% を、メッセージ通知、MWI の発信、および TRAP 用に確保しておくことを推奨します。これにより、コールへの応答とポートでの発信のためにポートでコール ブロッキングが発生する可能性が低減します。

ポート設定

前述の項で説明したように、ポートは着信ポートまたは発信ポートのいずれかになります。C：表 5-13 に、ボイスメール ポート割り当ての設定例を示し、C：表 5-14 に、応答ポートの設定のための設定テンプレートを示します。

C：表 5-13　ボイスメール ポート割り当ての設定例

Cisco Unity Connection のサーバ	ポート範囲	機能
US-CUC1	1 ～ 80	応答
US-CUC2	1 ～ 80	応答
US-CUC1	81 ～ 100	発信
US-CUC2	81 ～ 100	発信

C：表 5-14　ボイスメール応答ポートの設定例

パラメータ	値	説明
[有効（Enabled）]	オン	電話システム ポートを有効にするには、このボックスをオンにします。
[電話システムポート（Phone System Port）]		
[ポート名（Port Name）]	自動作成	Unity Connection によりポート名が自動的に作成されます。
[電話システム（Phone System）]	電話システム	適切な電話システムを選択します。
[ポートグループ（Port Group）]	PhoneSystem-1	適切なポート グループを選択します。
[サーバ（Server）]	US-CUC2/US-CUC1	最初に Cisco Unity Connection サブスクライバ ノードを選択し、同様に Unity Connection パブリッシャ ノードのポートを追加します。
[電話の動作（Phone behavior）]		
[呼び出しに応答（Answer Call）]	オン	この設定により、コールに応答するポートが指定されます。
[メッセージ通知を実行する（Perform Message Notification）]	オフ	この設定により、メッセージをユーザに通知するためのポートが指定されます。
[MWI 要求を送信する（Send MWI Requests）]	オフ	この設定により、MWI オン / オフ要求を送信するためのポートが指定されます。
[TRAP 接続を許可する（Allow TRAP Connections）]	オフ	この設定により、Telephony Recording and Playback（TRAP）接続のポートが指定されます。

C：表 5-14 に示す設定は、ボイスメールの発信ポートを作成するときにも使用する必要があります。ただし発信ポートの場合は、[呼び出しに応答（Answer Call）] パラメータをオフにし、[メッセージ通知を実行する（Perform Message Notification）]、[MWI 要求を送信する（Send MWI Requests）]、および [TRAP 接続を許可する（Allow TRAP Connections）] パラメータをオンにします。

アクティブ ディレクトリーの統合

Unity Connection は、Active Directory に対する認証を使用する Unity Connection Web アプリケーション（エンドユーザ向けの Cisco Personal Communications Assistant（PCA）など）の Microsoft Active Directory 同期および認証をサポートします。同様に、Unity Connection ボイス メッセージへにアクセスするために使用する IMAP 電子メール アプリケーションは、Active Directory に対して認証されます。電話ユーザ インターフェイスまたはボイス ユーザ インターフェイスによる Unity Connection ボイス メッセージへのアクセスでは、引き続き Unity Connection データベースに対して数値パスワード（PIN）による認証が行われます。Unity Connection と Unified CM の間で PIN 同期が有効になっている場合、これらの PIN は Unified CM システム PIN と同期されます。

Active Directory で、Unity Connection がユーザ検索ベースに指定されているサブツリーにアクセスするときに使用する管理者アカウントを作成する必要があります。検索ベースのすべてのユーザ オブジェクトを「読み取る」ための最小限の権限が設定されており、また、有効期限のないパスワードが設定されている Unity Connection 専用アカウントを使用することを推奨します。

Unified CM の [メール ID（Mail ID）] フィールドが、Active Directory のメール フィールドと同期されます。統合プロセスでは、これにより LDAP のメール フィールドが Unity Connection の [社内電子メールアドレス（Corporate Email Address）] フィールドに表示されます。Unity Connection は Unified Messaging アカウントの [社内電子メールアドレス（Corporate Email Address）] を使用してシングル インボックスを有効にします。

Unity Connection と Active Directory の統合により、ユーザ情報のインポートが可能になります。Unity Connection と Active Directory の統合にはさまざまなメリットがあります。

- ユーザの作成：Active Directory からデータをインポートして Unity Connection ユーザを作成できます。
- データの同期：Unity Connection は、Unity Connection データベースのユーザ データと Active Directory のデータを自動的に同期するように設定されています。
- 1 つのクレデンシャル セット：Unity Connection Web アプリケーションのユーザ名とパスワードを Active Directory に対して認証するように Unity Connection を設定します。これにより、ユーザが複数のアプリケーション パスワードを管理する必要がなくなります。

Active Directory の設定については、コール制御の章を参照してください。

ユニティコネクションのパーティションと CSS

この導入環境のすべてのユーザは、デフォルトのコーリング サーチ スペース（US-CUC1 サーチ スペース）で設定されています。このサーチ スペースにはデフォルトのパーティション（US-CUC1 パーティション）が含まれています。

規制テーブル

Unity Connection は、ボイスメール システムが未承認の電話番号を呼び出すことがないようにするため、規制テーブルを使用します。通常、これらのルールは許可されている番号またはブロックされている番号のいずれかに完全一致するように設定されています。この展開では、Unity Connection システムがボイスメール システムでのコール ブロッキングの規制ルールを使用せず、代わりに SIP トランク着信コーリング サーチ スペース（CSS）を使用して、Unity Connection からの不正なコールを阻止します。Unity Connection がネット上の宛先のみをダイヤルできるように、SIP トランク CSS を設定します。C：表 5-15 に、デフォルトの転送規制テーブルの設定を示します。

C：表 5-15　Unity Connection の規制テーブル

順序	ブロック	パターン
0	このチェックボックスをオフにします。	+*
1	このチェックボックスをオフにします。	9+*
2	このチェックボックスをオフにします。	91???????*
3	このチェックボックスをオフにします。	9011???????*

C：表 5-15　Unity Connection の規制テーブル（続き）

順序	ブロック	パターン
4	このチェックボックスをオフにします。	9???????????*
5	このチェックボックスをオフにします。	900
6	このチェックボックスをオフにします。	*

Unity Connection には、この他に、デフォルトのファクス、デフォルトの発信ダイヤル、デフォルトのシステム転送、およびユーザ定義および自動追加の代行内線番号用の 4 つの規制テーブルがあります。これらの規制テーブルも、C：表 5-15 で説明する設定を使用して無効にすることができます。

サービス クラス

サービス クラス（CoS）は、Unity Connection ボイスメールのユーザに対する制限と機能を定義します。サービス クラスは一般にユーザ テンプレートで定義され、このテンプレートがユーザ アカウントの作成時にアカウントに適用されます。この導入環境では、デフォルトのボイスメール ユーザ の COS がすべてのユーザに関連付けられています。

ユーザー プロビジョニング

ユーザを Unity Connection にインポートするには、Active Directory サーバのユーザ テンプレートを使用します。このユーザ テンプレートには、特定のユーザのグループに共通する設定が含まれています。ユーザ アカウントの作成時に、ユーザ テンプレートの共通設定がユーザに継承されます。ローカル タイム ゾーンの各サイトに個別のユーザ テンプレートを作成する必要があります。C：表 5-16 に、ユーザ テンプレートの設定を示します。

C：表 5-16　ボイスメール ユーザ テンプレート

セクション	フィールド	値
[基本設定（Basics）]	[エイリアス（Alias）]	SJC_User_Template
	[表示名（Display Name）]	SJC_User_Template
	[表示名の生成（Display Name Generation）]	[名、姓の順（First name, then last name）]
	[電話システム（Phone System）]	電話システム
	[サービスクラス（Class of Service）]	[ボイスメールユーザの COS（Voice Mail User COS）]
	[次回ログイン時に自己登録を設定する（Set for Self-enrollment at Next Login）]	オン
	[ディレクトリに登録（List in Directory）]	オン
	[タイムゾーン（Time Zone）]	[(GMT-08:00) アメリカ / ロサンゼルス ((GMT-8:00) America/Los_Angeles）]
	[言語（Language）]	[英語 (アメリカ合衆国) （English(United States)）]
	[社内電子メールアドレスから SMTP プロキシアドレスを生成（Generate SMTP Proxy Address from the Corporate Email Address）]	オン
[パスワード設定 - VM（Password Settings - VM）]	[次回サインイン時に、ユーザによる変更が必要（User Must Change at Next Sign-In）]	オン
	[期限切れなし（Does Not Expire）]	オン
	[認証規則（Authentication Rule）]	[ボイスメール認証規則 (推奨)（Recommended Voice Mail Authentication Rule）]
[パスワードの変更 - ボイスメール（Change Password-Voicemail）]	[PIN]	*<PIN>*

テンプレートに基づいて新規ユーザ設定を行うことで、個々のユーザ アカウントで変更する必要がある設定の数を最小限に抑えるとともにユーザ追加作業にかかる時間も短縮され、エラーが発生しにくくなります。

これ以降（テンプレートを使用してユーザ アカウントを作成した後）に行うすべてのユーザ テンプレート変更は、既存のユーザ アカウントには適用されません。つまり、共通設定はユーザ アカウント作成時点でのみテンプレートから取得されます。テンプレートを使用して Unity Connection アカウントを作成した後で、テンプレートまたは他のユーザに影響を及ぼさずに個々のユーザの設定を変更できます。

ここでは Web アプリケーション パスワードを変更しないでください。これは、Unity Connection は LDAP と統合されており、Active Directory からユーザが認証されるためです。これらの PIN とパスワードをユーザに指定する必要があります。これにより、ユーザは Unity Connection システム電話ユーザ インターフェイス（TUI）と Cisco Personal Communications Assistant（PCA）にサインインできます。

[ボイスメールユーザ COS サービスクラス（Voice Mail User COS class of Service）] 下の [Messaging Assistant の使用をユーザに許可する（Allow Users to Use the Messaging Assistant）] オプションと [Web Inbox と RSS フィードの使用をユーザに許可する（Allow Users to Use the Web Inbox and RSS Feeds）] オプションを選択して、ユーザが Cisco PCA を使用して Web Inbox にアクセスできるようにします。

前述の説明で作成したテンプレートを使用して LDAP からユーザをインポートします。

ユニティコネクションユーザー自己登録

エンドユーザを Unity Connection ユーザとして登録する必要があります。Unity Connection 管理者は各ユーザの ID（通常はユーザのデスク電話の内線番号）と一時 PIN（ユーザー プロビジョニングで設定）を指定する必要があります。初回登録ガイダンスは、あらかじめ録音された一連のプロンプトであり、ユーザはこのガイダンスに従って次のタスクを実行します。

- ユーザ名を録音します。
- ユーザが電話に応答しないときに外部発信者に対して再生されるグリーティングを録音します。
- ユーザ PIN を変更します。（ユーザの新しい PIN が PIN 同期を使用して Unified CM に伝播されます）。
- 電話帳に登録するかどうかを選択します（ユーザが電話帳に登録されていると、発信者はユーザの内線番号を知らない場合でも、ユーザの名前のスペルを言うか、ユーザ名を言うことでユーザに電話をかけられます。）

Unity Connection ユーザは組織内の IP エンドポイントまたは外部ネットワークから、自己登録プロセスのためにボイスメール パイロット番号をダイヤルできます。ユーザは、組織内または外部の不明な内線番号から Unity Connection に発信している場合、Unity Connection が自己登録プロセスを続行するよう応答したら、*（スターキー）を押す必要があります。登録が完了する前にユーザが通話を切断すると、次回ユーザが Unity Connection にサインインしたときに、初回登録ガイダンスが再び再生されます。

4. シングル インボックスの有効化

シングル インボックスは、Unity Connection のユニファイド メッセージング機能の 1 つであり、Unity Connection のボイス メッセージと Microsoft Exchange メールボックスを同期します。ユーザがシングル インボックスを使用可能な場合、ユーザに送信されるすべての Unity Connection ボイス メッセージ（Unity Connection ViewMail for Microsoft Outlook から送信されたメッセージを含む）は、最初に Unity Connection に保存され、直ちにユーザの Exchange メールボックスにレプリケートされます。このセクションでは、Unity Connection を Microsoft Exchange と統合してシングル インボックスを有効にするために必要な設定タスクについて説明します。

ユニティコネクションでのシングルインボックス有効化の前提条件

- シングル インボックス機能を有効にする前に、Microsoft Exchange が設定されており、ユーザが電子メールを送受信できることを確認してください。
- Unified Messaging サービス アカウント認証には Microsoft Active Directory が必要です。
- Unity Connection ユーザがインポートされ、基本ボイス メッセージング用に設定されます。ユーザー プロビジョニングを参照してください。

ユニティコネクション証明書管理

Cisco Unity Connection をインストールすると、Cisco PCA と Unity Connection 間の通信、および IMAP 電子メール クライアントと Unity Connection 間の通信を保護するため、ローカル自己署名証明書が自動的に作成およびインストールされます。つまり、Cisco PCA と Unity Connection 間でのすべてのネットワーク トラフィック（ユーザ名、パスワード、その他のテキスト データ、ボイス メッセージを含む）は自動的に暗号化され、IMAP クライアントで暗号化を有効化している場合には IMAP 電子メール クライアントと Unity Connection 間のネットワーク トラフィックは自動的に暗号化されます。

認証局（CA）から発行された証明書を使用することをお勧めします。この場合は、Unity Connection 自己署名 Tomcat 証明書が、エンタープライズ CA によって発行および署名されたマルチサーバ証明書に置き換えられます。このプロセスの詳細については、セキュリティーの章を参照してください。

ユニティコネクションの交換認証および SSL 設定の確認

Exchange サーバが適切な Web ベース認証モード（NT LAN Manager つまり NTLM を推奨）および Web ベースのプロトコル（HTTPS を推奨）で設定されていることを確認します。認証モードは、互いに通信する Exchange と Unity Connection の両方で一致する必要があります。

Exchange サーバと Active Directory ドメイン コントローラ用に外部 CA によって署名された証明書を検証するためのオプションを選択します。エンタープライズ CA ルート証明書を入手して、Exchange サーバとドメイン コントローラ サーバの両方にインストールします。

ユニティコネクションでの SMTP プロキシアドレスの設定

シングル ボックスを設定すると、Unity Connection は SMTP プロキシ アドレスを使用して、Unity Connection ViewMail for Microsoft Outlook から送信されたメッセージの送信者を適切な Unity Connection ユーザにマップし、受信者を Unity Connection ユーザにマップします。

たとえば、電子メール クライアントが電子メール アドレス aross@ent-pa.com を使用して Unity Connection にアクセスするように設定されているとします。このユーザが Outlook 向けの ViewMail でボイス メッセージを録音し、そのメッセージをユーザ ahall@ent-pa.com に送信します。Unity Connection は SMTP プロキシ アドレスのリストで aross@ent-pa.com と ahall@ent-pa.com を検索します。これらのアドレスがそれぞれ Unity Connection ユーザである ahall および aross の SMTP プロキシ アドレスとして定義されている場合、Unity Connection はメッセージを Unity Connection ユーザ aross からのボイス メッセージとして Unity Connection ユーザ ahall に送信します。

ユーザ テンプレートを使用してユーザをインポートする場合、ユーザの SMTP プロキシ アドレスが自動的に作成されます。ユーザ テンプレートでは、SMTP プロキシ アドレスを作成するために [社内電子メールアドレスから SMTP プロキシアドレスを生成（Generate SMTP Proxy Address from the Corporate Email Address）] オプションを選択します。詳細については、ユーザー プロビジョニングを参照してください。

アクティブ　ディレクトリー での統一されたメッセージングサービスアカウントの作成およびユニティコネクションの権限の付与

シングル インボックスを使用するには、Active Directory のアカウント（ユニファイド メッセージング サービス アカウント）が必要です。このアカウントには、Unity Connection がユーザの代わりに操作を実行するために必要な権限が付与されている必要があります。Unity Connection は ユニファイド メッセージング サービス アカウントを使用して Exchange メールボックスにアクセスします。ユニファイド メッセージング サービス アカウントを作成する際には、次のガイドラインに従ってください。

- アカウントには Exchange メールボックスを作成しません。
- 管理者グループにはアカウントを追加しません。
- アカウントを無効にしないでください。無効にすると、Unity Connection がアカウントを使用して Exchange メールボックスにアクセスできなくなります。

Exchange Management Shell がインストールされているサーバにサインインし、次のコマンドを使用して、[アプリケーション偽装管理（ApplicationImpersonation Management）] の役割を Unity Connection のユニファイド メッセージング サービス アカウントに割り当てます。

new-ManagementRoleAssignment -Name: *RoleName* **-Role:ApplicationImpersonation -User:'** *Account* **'**

ここで、

- *RoleName* は、割り当てるロールの名前です（Unity ConnectionUMServicesAcct など）。**get-ManagementRoleAssignment** コマンドを実行すると、RoleName に入力する名前が表示されます。
- *Account* は、domain\alias 形式のユニファイド メッセージング サービス アカウントの名前です。

SMTP スマート ホスト

Unity Connection は、SMTP スマート ホストを使用してメッセージをユーザの電子メール アドレスにリ レーします。Unity Connection ユーザが新しいメッセージを受け取ると、Unity Connection がテキスト形式の到着通知を電子メール アドレスに送信できますこのタイプの通知では、Cisco PCA へのリンクを電子メール メッセージの本文に組み込むように Unity Connection を設定できます。ユーザ設定で、ユーザの [通知デバイスの編集（Edit Notification Device）] ページに移動し、[メッセージテキストに Cisco Unity Connection Web Inbox へのリンクを含める（Include a Link to the Cisco Unity Connection Web Inbox in Message Text）] オプションを選択します。C：表 5-17 に、SMTP スマート ホストの設定を示します。

C：表 5-17　SMTP スマート ホストの詳細（[システム設定（System Settings）] > [SMTP の設定（SMTP Configuration）] > [スマートホスト（Smart Host）]）

パラメータ	値
SmartHost	US-EXCH1.ent-pa.com

ユニファイド メッセージング サービス

Cisco Unity Connection Administration で、[ユニファイドメッセージング（Unified Messaging）] を展開し、[ユニファイドメッセージングサービス（Unified Messaging Services）] を選択します。

- ユニファイド メッセージング サービスは、Unity Connection が Microsoft Exchange と通信するために使用する認証方式と Microsoft Exchange のタイプを定義します。
- FQDN を使用して特定の Exchange サーバと通信するようにユニファイド メッセージング サービスを設定します。
- Unity Connection ユニファイド メッセージング サービスを、Microsoft Exchange で設定されているものと同じ Web ベース認証モード（NTLM を推奨）および Web ベース プロトコル（HTTPS を推奨）で設定します。
- アクティブ　ディレクトリー での統一されたメッセージングサービスアカウントの作成およびユニティコネクションの権限の付与の項で作成した Active Directory アカウントのクレデンシャルを入力します。
- [Exchange の予定表および連絡先にアクセス（Access Exchange Calendar and Contacts）] オプションと [Connection と Exchange のメールボックスを同期する (シングル インボックス) （Synchronize Connection and Exchange Mailboxes (Single Inbox)）] オプションを選択し、ユニファイド メッセージング機能を有効にします。
- Exchange サーバ証明書がエンタープライズ CA によって署名されている場合は、Unity Connection が自動的に Exchange からの SSL 証明書を検証します。これは、エンタープライズ CA ルート証明書が信頼ストアにインストールされるためです。

ユニファイド メッセージング アカウント

Unity Connection Administration で、[ユーザ（Users）] を展開し、次に [ユーザ（Users）] を選択します。[ユーザの基本設定の編集（Edit User Basics）] ページの [編集（Edit）] メニューで、[ユニファイドメッセージングアカウント（Unified Messaging Accounts）] を選択します。

- ユーザ アカウントを作成する際、Unity Connection はそのユーザのユニファイド メッセージング アカウントを自動的には作成しません。ユニファイド メッセージング アカウントは、1 人のユーザまたは複数のユーザに対して作成できます。多数のユーザを対象にユニファイド メッセージング アカウントを作成するには、一括管理ツール（BAT）を使用します。
- ユニファイド メッセージングでは、各 Unity Connection ユーザの Exchange メール アドレスを入力する必要があります。[ユニファイドメッセージングアカウント（Unified Messaging Account）] ページで、[社内電子メールアドレスを使用 : 指定なし（Use Corporate Email Address: None Specified）] を選択します。これにより、Unity Connection は [ユーザの基本設定の編集（Edit User Basics）] ページで指定した社内電子メール アドレスを Exchange 電子メール アドレスとして使用します。
- Active Directory 統合では、Unified CM の [メール ID（Mail ID）] フィールドが、Active Directory のメール フィールドと同期されます。これにより、LDAP メール フィールドが Unity Connection の [社内電子メールアドレス（Corporate Email Address）] フィールドに表示されます。

一括管理ツールを使用して複数ユーザのユニファイド メッセージング アカウントを作成する方法については、次の場所にある『*System Administration Guide for Unity Connection*』の最新版を参照してください。

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

ボイスメールユーザーの COS

ユーザがシングル インボックスを使用できるようにするため、ボイスメール ユーザのサービス クラスを編集します（[サービスクラス（Class of Service）] –> [ボイスメールユーザの COS（Voice Mail User COS）] ）。[ライセンス済み機能（Licensed Features）] で [IMAP クライアントやシングルインボックスを使用したボイスメールへのアクセスをユーザに許可する（Allow Users to Access Voicemail Using an IMAP Client and/or Single Inbox）] オプションを選択します。また、[メッセージ本文へのアクセスを IMAP ユーザに許可する（Allow IMAP Users to Access Message Bodies）] オプションも選択します。

ユーザ ワークステーションへの Outlook 向けの ViewMail のインストール

Cisco ViewMail for Microsoft Outlook のビジュアル インターフェイスにより、ユーザは Outlook 内で各自の Unity Connection ボイス メッセージを送信、再生、管理できます。シスコの Web サイトから Unity Connection ViewMail for Microsoft Outlook をダウンロードして、各ユーザ ワークステーションにインストールします。ViewMail のインストールが完了したら、ViewMail の設定または [オプション（Options）] タブを開き、Unity Connection サーバに電子メール アカウントを関連付けます。ユーザ情報と Unity Connection サーバの詳細情報を入力します。

他の電子メール クライアントを使用して Exchange の Unity Connection ボイス メッセージにアクセスする場合、または Outlook 向けの ViewMail がインストールされていない場合は、次の点に注意してください。

- メール クライアントは、Unity Connection ボイス メッセージを .wav ファイルが添付された電子メールとして処理します。
- ユーザが Unity Connection ボイス メッセージに返信またはボイス メッセージを転送すると、ユーザが .wav ファイルを添付した場合でも、返答または転送は電子メールとして処理されます。メッセージ ルーティングは、Unity Connection ではなく Exchange によって処理されます。したがって、メッセージは受信者の Unity Connection メールボックスに送信されません。

5. ビジュアル ボイスメールの有効化

ビジュアル ボイスメールにより、Jabber クライアントのボイスメール タブから Unity Connection に直接アクセスできます。ユーザは Jabber からボイス メッセージのリストを確認し、メッセージを再生できます。ユーザは、ボイス メッセージを削除することもできます。

ユニティコネクションの設定

- Unity Connection ユーザがインポートされ、基本ボイス メッセージング向けに設定されていることを確認します。ユーザー プロビジョニングの項を参照してください。
- Unity Connection の **Connection Jetty** サービスと **Connection REST Service** が稼働していることを確認します。これらのサービスはいずれもサービスのアクティベーションで [オプションサービス（Optional Services）] の下でアクティブ化されます。
- IMAP クライアントからボイスメールにアクセスできるように、[サービスクラス（Class of Service）] が有効になっていることを確認してください。ボイスメールユーザーの COS の項を参照してください。
- Unity Connection ボイスメール サービス クラス（CoS）を編集し、ユーザが Web インボックスを使用できるようにします。[機能（Features）] タブで [Unified Personal Communicator を使用したボイスメールへのアクセスをユーザに許可する（Allow Users to Use Unified Client to Access Voicemail）] オプションを選択します。

- [API 設定（API settings）]（[システム設定（System Settings）] > [詳細設定（Advanced）]）で、次のオプションを選択します。
  - [Cisco Unity Connection Messaging Interface（CUMI）経由でセキュアなメッセージ録音へのアクセスを許可する（Allow Access to Secure Message Recordings through Cisco Unity Connection Messaging Interface (CUMI)）]
  - CUMI を介してセキュア メッセージのメッセージ ヘッダー情報を表示する（Display Message Header Information of Secure Messages through CUMI）
  - [CUMI 経由のメッセージ添付ファイルを許可する（Allow Message Attachments through CUMI）]

統一された CM の設定

各 Unity Connection サーバ ノードに**ボイスメール** UC サービスを追加します。C：表 5-18 に、ボイスメール UC サービスの設定を示します。

C：表 5-18　ボイスメール サービスの設定（[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）]）

パラメータ	値	注
[製品のタイプ（Product Type）]	Unity Connection	ボイスメール システムの製品名を入力します。
[名前（Name）]	us-cuc1	ボイスメール サービスの名前を入力します。パブリッシャ ボイスメール サービスとサブスクライバ ボイスメール サービスを区別できる表示名を選択します。
[説明（Description）]	us-cuc1	パブリッシャ ボイスメール サービスとサブスクライバ ボイスメール サービスを区別できる表示名を入力します。
[ホスト名 /IP アドレス（Host Name/IP address）]	us-cuc1.ent.pa.com	ボイスメール サービスの FQDN を入力します。
ポート	443	ボイスメール サービスに接続するポートを入力します。
[プロトコル（Protocol）]	HTTPS	ボイス メッセージを安全にルーティングするためのプロトコルを選択します。

以前に作成した**ボイスメール** UC サービスを**標準**サービス プロファイル（[ユーザ管理（User Management）] –> [ユーザ設定（User Settings）] –> [サービスプロファイル（Service Profile）]）に適用します。Unity Connection パブリッシャ（us-cuc1.ent.pa.com）に対して作成したボイスメール UC サービスがプライマリ プロファイルに設定されており、Unity Connection サブスクライバ（us-cuc2.ent.pa.com）に対して作成したボイスメール UC サービスがセカンダリ プロファイルに設定されていることを確認してください。ボイスメール サービスのクレデンシャルを同期する場合は、[ボイスメールサービスのクレデンシャルソース（Credentials source for voicemail service）] ドロップダウン リストから [Unified CM - IM/Presence（Unified CM - IM and Presence）] を選択します。

6. SRST モードでのボイスメール

集中型メッセージング導入モデルでは、WAN の停止中にブランチ サイトの Survivable Remote Site Telephony（SRST）が無応答コールおよび話中コールを中央の Unity Connection にルーティングします。ビジー信号を受けた着信コール、無応答コール、およびメッセージ ボタンを押して開始されたコールは、Unity Connection に転送されます。この設定では、電話のメッセージ ボタンをアクティブなままにできます。この機能を有効にするには、PRI を介した Unity Connection への POTS ダイヤル ピア アクセスを設定します。

コールが PSTN 経由で Unity Connection にルーティングされる場合は、Redirected Dialed Number Information Service（RDNIS）が非常に重要です。RDNIS 情報が誤っている場合、PSTN 経由で再ルーティングされるボイスメールへのコールに影響が及ぶ可能性があります。RDNIS 情報が誤っている場合、通話はダイヤル先のユーザのボイスメール ボックスに到達せず、代わりに自動受付のプロンプトを受信します。その場合、発信者は、到達先の内線番号を再入力するように要求されることがあります。この動作は、主に、電話通信事業者がネットワークを介した RDNIS を保証できない場合の問題です。通信事業者が RDNIS の正常な送信を保証できない理由は数多くあります。通信事業者に問い合わせて、回線のエンドツーエンドで RDNIS の送信を保証しているかどうかを確認してください。

統一された CM の設定

C：表 5-19 で説明する設定が、中央サイトの PSTN ゲートウェイへの SIP トランクの Unified CM 設定で有効になっていることを確認します。

C：表 5-19　SRST モードでのボイスメール向け PSTN ゲートウェイへの SIP トランクの設定

パラメータ	値	注
[コールルーティング情報 - インバウンドコール（Call Routing Information - Inbound Calls）]		
[Diversion ヘッダー配信のリダイレクト - インバウンド（Redirecting Diversion Header Delivery - Inbound）]	オン	リダイレクト情報要素、最初のリダイレクト番号、およびコール転送理由が着信メッセージの一部として送信され、受け入れられることを指定します。Unity Connection は最初のリダイレクト番号を使用してコールに応答します。
[コールルーティング情報 - アウトバウンドコール（Call Routing Information - Outbound Calls）]		
[Diversion ヘッダー配信のリダイレクト - アウトバウンド（Redirecting Diversion Header Delivery - Outbound）]	オン	リダイレクト情報要素、最初のリダイレクト番号、およびコール転送理由が発信メッセージの一部として送信され、受け入れられることを指定します。Unity Connection は最初のリダイレクト番号を使用してコールに応答します。

ブランチ SRST ルータの設定

ブランチ サイトの SRST ルータで、PRI を介したボイスメール アクセスを有効にするため次のコマンドを設定します。

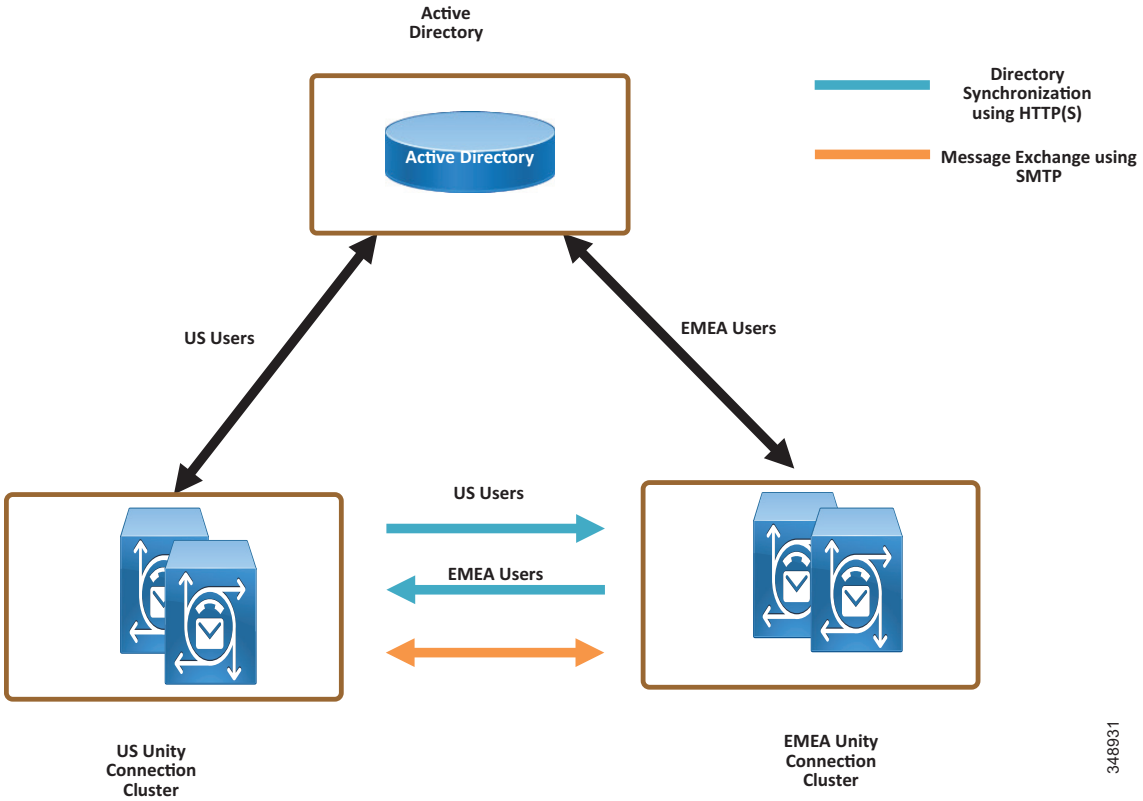
```
!
!
dial-peer voice 10 pots
destination-pattern +14085554999
direct-inward-dial
port 1/0:15
!
!
voice register pool 1
call-forward b2bua busy +14085554999
call-forward b2bua noan +14085554999 timeout 12
!
!
```

7. 2 つのユニティコネクションクラスタの HTTPS インターネットワーキング

C：図 5-4 に、2 つの Unity Connection クラスタの HTTPS インターネットワーキングを示します。HTTPS ネットワーキングにより複数の Unity Connection クラスタが接続されます。これにより、接続されたこれらのクラスタ間でディレクトリ情報を共有し、ボイス メッセージを交換できます。複数の Unity Connection サーバまたはクラスタを接続して、Unity Connection サイトと呼ばれる適切に接続されたネットワークを形成できます。サイトに接続するサーバは、*ロケーション*と呼ばれます。サイト内の各ロケーション間のディレクトリ情報の交換には HTTPS プロトコルが使用され、ボイス メッセージの交換には SMTP プロトコルが使用されます。

サイト内の Unity Connection ロケーションはディレクトリ情報を自動的に交換するため、受信側 / 送信先ユーザが発信側 / 送信元ユーザの検索範囲内で到達できる場合は、あるロケーションの受信側 / 送信先ユーザが別のシステムの発信側 / 送信元ユーザに対し、名前または内線番号を使用して発信するか、またはメッセージを送信できます。ネットワーク接続されたシステムは、1 つのディレクトリを共有しているかのように機能します。

C：図 5-4　　2 つの Unity Connection クラスタの HTTPS インターネットワーキング



HTTPS ネットワーキングでは、ハブアンドスポーク トポロジを使用して Unity Connection クラスタが相互に接続します。このトポロジでは、スポーク間のすべてのディレクトリ情報が、スポークに接続するハブを介して共有されます。HTTPS ネットワークで接続できる Unity Connection ロケーションの数と、HTTPS ネットワーキングの最大ユーザ数は、導入されている OVA テンプレートに応じて異なります。サポートされているロケーション最大数とディレクトリ最大サイズの詳細については、『*System Requirements for Cisco Unity Connection*』の最新版でディレクトリ オブジェクト制限に関する情報を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-guides-list.html

HTTPS ネットワーキングでは、ネットワーク内の各ロケーションで稼働しているリーダー サービスとフィーダー サービスによって、ディレクトリ レプリケーションが行われます。リーダー サービスは、リモート ロケーションを定期的にポーリングして、前回のポーリング間隔以降に行われたディレクトリ変更情報を収集します。フィーダー サービスは、変更トラッキング データベースを調べてディレクトリ変更が行われたかどうかを確認し、必要な情報を使用してポーリング要求に応答します。

HTTPS ネットワーキングでは、クラスタ ロケーションのパブリッシャ サーバが稼働している場合、このサーバがディレクトリ情報の同期化を行います。ただしパブリッシャ サーバがダウンしている場合は、サブスクライバ サーバがディレクトリ情報を同期します。

ディレクトリ同期が実行されるクラスタのサーバ（パブリッシャまたはサブスクライバ）に応じて、ディレクトリ同期は次のいずれかのタイプになります。

- [標準（Standard）] : ディレクトリ同期が、パブリッシャ サーバにより接続ロケーションとの間で実行されることを示します。
- [アラート（Alert）] : パブリッシャ サーバに接続できず、サブスクライバ サーバが接続ロケーションにディレクトリ情報を提供することを示します。ただし、サブスクライバ サーバに格納されているディレクトリ情報は、パブリッシャ サーバの稼働時にパブリッシャ サーバとの間で最後に同期されたディレクトリ情報です。

パブリッシャで障害が発生すると、ディレクトリ同期はアラート モードで実行されます。アラート モードでは、HTTPS ネットワーク上の接続ノードに対し、サブスクライバとのディレクトリ同期へのアクセスが制限されます。制限付きアクセスとは、接続ノードが、パブリッシャの稼働時にパブリッシャとの間で最後に同期されたディレクトリ情報のみを取得できることを意味します。パブリッシャが復旧すると、パブリッシャに直接接続しているノードはパブリッシャを介して最新のディレクトリ情報を同期します。したがって、アラート モードの主要なメリットとしては、パブリッシャがダウンした場合でも接続ノードが引き続きサブスクライバ サーバと同期する点が挙げられます。

相互にネットワーク接続されたクラスタには、TCP/IP ポート 25（SMTP）を介して直接アクセスできます。加えて、両方のロケーションはポート 8444 上で HTTPS を介して相互にルーティングできる必要があります。

展開の解説という本書の目的に沿って、米国と EMEA の Unity Connection クラスタ間で HTTPS インターネットワーキングが設定されると想定します。C：表 5-20 に、HTTPS ネットワークにより接続されるこの 2 つのクラスタのサーバ ノード情報を示します。

C：表 5-20　HTTPS ネットワークでの Unity Connection クラスタの詳細

	US Unity Connection クラスタ		EMEA Unity Connection クラスタ	
サーバ	**ホスト名**	**IP アドレス**	**ホスト名**	**IP アドレス**
パブリッシャ	US-CUC1	*<IP_Address_US_CUC1>*	EMEA-CUC1	*<IP_Address_EMEA_CUC1>*
サブスクライバ	US-CUC2	*<IP_Address_US_CUC2>*	EMEA-CUC2	*<IP_Address_EMEA_CUC2>*

2 つの Unity Connection クラスタ間で HTTPS ネットワーキングをセットアップするには、次のタスクを実行します。

各ユニティコネクションサーバの表示名および SMTP ドメインの確認

- HTTPS ネットワークに接続する Unity Connection サーバには、一意の表示名と SMTP ドメインが設定されている必要があります。
- HTTPS ネットワークを有効にする前に、[ネットワーク（Networking）] –> [ロケーション（Locations）] の設定で、Unity Connection パブリッシャ サーバの表示名と SMTP ドメインを確認します。

ユニティコネクションクラスタ間の HTTPS ネットワークの作成

- Unity Connection サーバの HTTPS ネットワークを作成するには、最初に HTTPS リンクを作成して 2 つのクラスタをリンクし、その後各クラスタのサブスクライバが SMTP アクセスのために追加されていることを確認します。
- 各 Unity Connection パブリッシャで、新しい HTTPS リンクを追加します。C：表 5-21 に、HTTPS リンクの設定を示します。

C：表 5-21　HTTPS リンクの設定（[ネットワーク（Networking）] > [HTTP(S) リンク（HTTP(s) Links）]）

パラメータ	値	注
[Cisco Unity Connection のリモートロケーションへのリンク（Link to Cisco Unity Connection Remote Location）]		
[パブリッシャ（IP アドレス /FQDN/ ホスト名）（Publisher (IP address/FQDN/ Hostname)）]	emea-cuc1.ent-pa.com	リモート Unity Connection パブリッシャ ノードの FQDN を入力します。
[ユーザ名（Username）]	管理ユーザの名前	上記のパブリッシャ フィールドに指定したロケーションの管理者のユーザ名を入力します。管理者のユーザ アカウントには、システム管理者ロールを割り当てておく必要があります。
[パスワード（Password）]	管理ユーザのパスワード	[ユーザ名（Username）] フィールドに指定された管理者のパスワードを入力します。
[転送プロトコル（Transfer Protocol）]		
[Secure Sockets Layer(SSL) を使用する（Use Secure Sockets Layer (SSL)）]	オン	このオプションは、さまざまな HTTPS ロケーション間のディレクトリ同期トラフィックを SSL により暗号化できるようにします。

クラスター　サブスクライバーサーバーの ＳＭＴＰ アクセスの設定

Unity Connection クラスタ サーバ ペアを含む HTTPS ネットワークでは、ペアのパブリッシャ サーバだけをネットワークに接続できます。クラスタのサブスクライバがプライマリ サーバである場合に、ネットワーク上のすべてのロケーションがクラスタ サブスクライバ サーバ ノードと直接通信できるようにするには、すべてのネットワーク ロケーションで、サブスクライバ サーバからの SMTP 接続を許可するように設定する必要があります。

この例では、EMEA サブスクライバを US パブリッシャの SMTP 設定に追加し、US サブスクライバを EMEA パブリッシャの SMTP 設定に追加します。

- US パブリッシャの US クラスタで、EMEA サブスクライバを SMTP 設定（[システム設定（System Settings）]）に追加します。[編集（Edit）] メニューで [IP アドレスアクセスリストの検索（Search IP Address Access List）] を選択します。[IP アドレスの新規作成（New IP Address）] ページで、EMEA サブスクライバ サーバの IP アドレス（*<IP_Address_EMEA_CUC2>*）を入力します。[接続を許可する（Allow Connection）] オプションが選択されていることを確認します。
- EMEA クラスタのパブリッシャ（emea-cuc1.ent-pa.com）で上記の手順を繰り返し、US クラスタ サブスクライバの IP アドレスを追加します。

ロケーション間でのレプリケーション

HTTPS ネットワークの作成後に、ネットワークに追加された 2 つのロケーション間でデータベース全体がレプリケートされることを確認します。初回のレプリケーションが開始されると、データが全ロケーション間で完全にレプリケートされるまでには、ディレクトリのサイズによって数分間から数時間かかることがあります。

前述のステップで作成した **HTTP（S）リンク**を開き、次の値を確認します。

- [前回の同期時刻（Time of Last Synchronization）]

  ローカルのリーダー サービスが前回、リモート ロケーションのフィーダー サービスにポーリングしてリモート ロケーションのディレクトリ変更の確認を試みた時刻（応答の有無にかかわらず）のタイムスタンプを示します。

- [前回のエラー時刻（Time of Last Failure）]

  ローカルのリーダー サービスが前回リモート ロケーションのフィーダー サービスのポーリングを試行中にエラーが発生した時点のタイムスタンプを示します。このフィールドの値が 0 の場合、または [前回の同期時刻（Time of Last Synchronization）] の値が [前回のエラーの時刻（Time of Last Error）] の値よりも遅い場合、レプリケーションは問題なく進行している可能性が高くなります。

- [オブジェクト数（Object Count）]

  ローカル Unity Connection ロケーションが同期したリモート ロケーションのユーザの数を示します。

ローカルユニティコネクション CSS へのリモートロケーションパーティションの追加

ロケーション間のネットワークを初めてセットアップする場合、US クラスタでプロビジョニングされたユーザは、EMEA クラスタのユーザにボイス メッセージを送信できません。これは、各ロケーションのユーザは個別のパーティションに属しており、個々のユーザ検索スペースには他のロケーションのユーザのパーティションが含まれていないためです。

- US Unity Connection サーバの us-cuc1 コーリング サーチ スペース（CSS）を編集して、EMEA ロケーションの Unity Connection サーバ パーティション emea-cuc1 を追加します。
- EMEA Unity Connection サーバの emea-cuc1 コーリング サーチ スペース（CSS）を編集して、US ロケーションの Unity Connection サーバ パーティション us-cuc1 を追加します。

関連資料

ボイス メッセージングと Cisco Unity Connection に関する追加情報については、下記リンクから入手可能な次のドキュメントの最新版を参照してください。

- 『*Cisco Collaboration System SRND*』の「*Voice Messaging*」の章

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

- 『*Design Guide for Cisco Unity Connection*』

  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

- 『*HTTPS Networking Guide for Cisco Unity Connection*』

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

- 『*Unified Messaging Guide for Cisco Unity Connection*』

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

コラボレーション管理サービス

改訂日：2019 年 2 月 19 日

この章では、Enterprise Collaboration 向けプリファード アーキテクチャに組み込まれるコラボレーション管理サービスについて説明します。この章で重点を置くのは、ほとんどのコラボレーション環境に必要となる、コア アプリケーションのサブセットです。このプリファード アーキテクチャは、アプリケーションの導入を簡素化し、不必要な設定の変更を防ぐために、利用可能なすべてのアプリケーションを考慮して構築されています。

この章の最初の 2 つのセクションでは、Cisco Unified Communications Manager（Unified CM）、Cisco Unified CM IM and Presence サービス、Cisco Unity Connection を導入するためのツールについて説明します。これらのツールは、具体的には Cisco Prime Collaboration Deployment と Web ベースの Cisco Smart Software Manager ポータルです。この章の 3 番目のセクションでは、Unified CM を設定するために使用する Cisco Prime Collaboration プロビジョニングの最適な実装について説明します。

コラボレーション管理サービスには、以下のものがあります。

- Cisco Prime Collaboration Deployment
- Cisco Smart Software Manager
- Cisco Prime Collaboration Provisioning

コラボレーション管理サービスの主な利点

- 新規インフラストラクチャ コンポーネントの導入を簡素化します。
- 一元化された単一の Web ベースのツールを使用して、各種製品のライセンス、ソフトウェア、権限付与を管理できます。
- 自動化されたプロビジョニング、モニタリング、傾向レポートによって製品の導入と管理を簡素化し、統合します。
- ワークフロー ポリシーの制御下で移動、追加、変更を迅速に行うことで、生産性と一貫性を向上させます。

この章の新規情報とは

C：表 6-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

C：表 6-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
代替ライセンス方式としての登録トークンと特定のライセンスの予約の有効期間に関連するスマートライセンスの更新	Cisco Smart Software Manager（C：6-6 ページ）	2019 年 1 月 23 日
その他の小さな修正および更新	この章の各項で説明	2019 年 1 月 23 日
Cisco Smart Software Manager が Cisco Prime License Manager に置き換えられました。	Cisco Smart Software Manager（C：6-6 ページ）	2017 年 8 月 30 日

Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment は、Cisco Unified Communications Manager（Unified CM）、Cisco Unified CM IM and Presence サービス、Cisco Unity Connection などのコラボレーション アプリケーション ノードの導入を簡素化するためのソリューションです。Cisco Prime Collaboration Deployment は、Unified CM、Unified CM IM and Presence サービス、および Unity Connection クラスタをインストールするために必要なステップの多くを自動化することによって、管理者を支援します。

コア コンポーネント

Cisco Prime Collaboration Deployment アーキテクチャのコア コンポーネントは次のとおりです。

- Cisco Prime Collaboration Deployment。Cisco ISO インストール ファイルを使用して、コラボレーション アプリケーション ノードを VMware ESXi サーバに導入します。
- VMware ESXi サーバ。Unified CM と Unity Connection を含め、コラボレーション アプリケーション ノードの仮想マシン（VM）をホストします。

利点

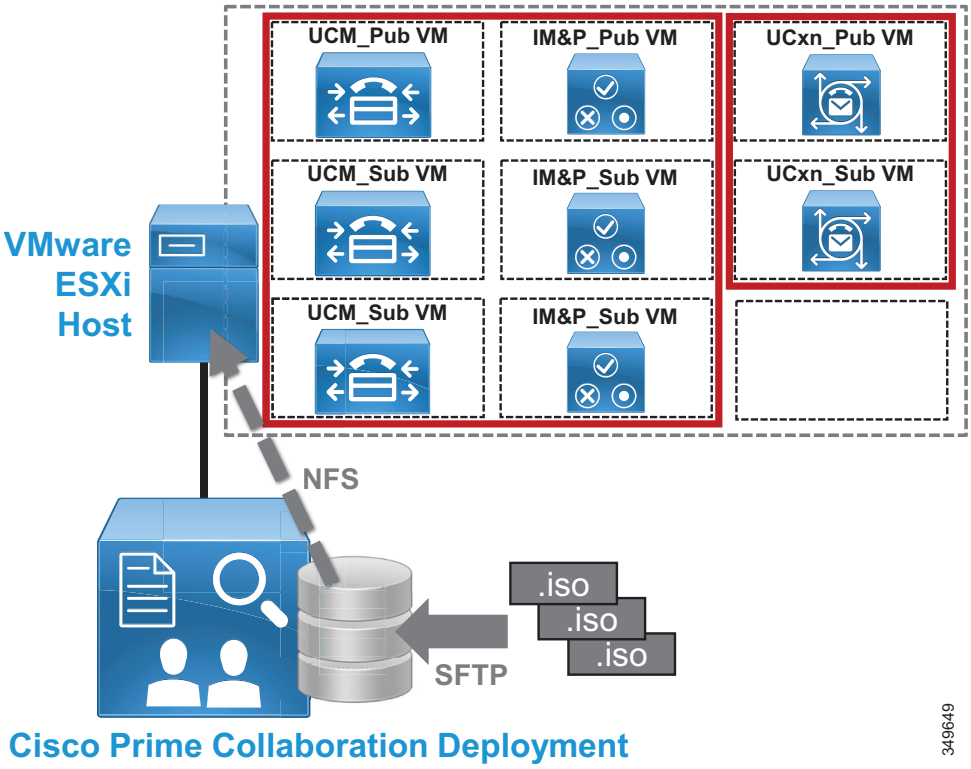
Cisco Prime Collaboration Deployment を使用して Enterprise Collaboration 向けプリファード アーキテクチャのコール制御およびボイス メッセージング アプリケーション ノードを導入することには、次の利点があります。

- コラボレーション アプリケーションの Cisco ISO ファイルのストレージを一元化できます。
- Unified CM、Unified CM IM and Presence サービス、Unity Connection の各コラボレーション アプリケーションのインストールが自動化されます。
- 複数のコラボレーション アプリケーション サーバ ノード VM にわたり、ネットワーク コンポーネント（NTP、DNS）、管理アカウントとパスワード、証明書の基本情報などといった一連の共通の設定を適用できます。

アーキテクチャー

Cisco Prime Collaboration Deployment アーキテクチャは Cisco Prime Collaboration Deployment サーバ ノードからなり、このノードにインストール対象のコラボレーション アプリケーション Cisco ISO ファイルが保管されます。これらのファイルは、セキュア FTP（SFTP）を使用して Cisco Prime Collaboration Deployment 上に配置されます。Cisco Prime Collaboration Deployment で ESXi ホストが設定されると、その ESXi ホストに応じてネットワーク ファイル システム（NFS）マウントが作成されます。この NFS マウントを使用して、該当するコラボレーション アプリケーション Cisco ISO ファイルを ESXi ホスト サーバ ノード VM にインストールできます（C：図 6-1）。

C：図 6-1　　Cisco Prime Collaboration Deployment アーキテクチャ



複数の ESXi ホスト サーバにまたがる大規模な導入環境では、必要な数だけの ESXi ホストを Cisco Prime Collaboration Deployment に導入できます。

Cisco Prime Collaboration Deployment の役割

Cisco Prime Collaboration Deployment は、コラボレーション アプリケーションの Cisco ISO ストアとして機能します。さらに、1 つ以上の VMware ESXi ホストにコラボレーション アプリケーション ノードを導入して設定するための管理インターフェイスとしての役割も果たします。

ESXi ホストの役割

1 つ以上の ESXi ホスト サーバに、Cisco Prime Collaboration Deployment によってインストールされた Unified CM、Unified CM IM and Presence サービス、および Unity Connection クラスタ用のアプリケーション ノード VM が収容されます。

Cisco Prime Collaboration Deployment の高適用性

Cisco Prime Collaboration Deployment アプリケーションでは高可用性をサポートしていませんが、Cisco Prime Collaboration Deployment は初期導入と基本設定のために使用するので、冗長性は要件となりません。コラボレーション アプリケーション ノードを導入して基本設定を行うためには、Cisco Prime Collaboration Deployment アプリケーション ノードが運用中であり、コラボレーション アプリケーション サーバ ノードの導入先とする 1 つ以上の ESXi サーバ ホストにアクセス可能でなければなりません。Cisco Prime Collaboration Deployment が運用可能な状態になっていない場合は、ネットワーク接続を有効にして ESXi サーバへの NFS マウントが稼働中になるよう、Cisco Prime Collaboration Deployment を運用中の状態に戻す必要があります。

他のコラボレーションおよび管理アプリケーションの場合と同様、Cisco Prime Collaboration Deployment アプリケーション サーバはディザスタ リカバリ システム（DRS）を使用して定期的にバックアップしてください。DRS デバイスの設定、バックアップのスケジュール、バックアップおよび復元操作は、Cisco Prime Collaboration Deployment アプリケーション サーバのコマンド ライン インターフェイス（CLI）を使用して行います。

Cisco Prime Collaboration Deployment のスケーリング

Cisco Prime Collaboration Deployment にはリリースごとに OVA テンプレート ファイルが 1 つのみであることから、Cisco Prime Collaboration Deployment の容量に関する考慮事項は Cisco Prime Collaboration Deployment VM のディスクのストレージ容量に限られます。導入される各種のコラボレーション アプリケーションの Cisco ISO ファイルは Cisco Prime Collaboration Deployment 上に保管されるため、ディスク容量は重要です。このことから、Cisco ISO ファイルを管理することが非常に重要となります。不要になった Cisco ISO ファイルを削除して、新しい Cisco ISO ファイルを保管するためのスペースをあけてください。

Cisco Prime Collaboration Deployment のプロセス

Cisco Prime Collaboration Deployment では、導入に関して考慮しなければならない 2 つの側面があります。

- Cisco Prime Collaboration Deployment アプリケーションサーバーの展開
- Cisco Prime Collaboration Deployment を使用した Cisco Collaboration アプリケーション サーバー クラスターの導入

Cisco Prime Collaboration Deployment アプリケーションサーバーの展開

Cisco Prime Collaboration Deployment アプリケーションは、単一のスタンドアロン ノードとして導入されます。Cisco 提供の Cisco Prime Collaboration Deployment の OVA テンプレート ファイルは、計算インフラストラクチャに導入してください。

OVA を導入した後、Cisco Prime Collaboration Deployment の Cisco ISO ファイルをマウントした上で、Cisco Prime Collaboration Deployment をインストールするために Cisco Prime Collaboration Deployment VM の電源を入れます。アカウント情報（管理者アカウント名とパスワード）、ネットワーク情報（IP アドレス、ホスト名、DNS、NTP など）、Web セキュリティ情報（場所、組織などの自己署名証明書情報）を含む適切な情報を入力すると、インストールが完了します。

OVA テンプレートと Cisco ISO ファイルの取得方法について詳しくは、次のリンク先にあるマニュアルを参照してください。

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-prime-collaboration-deployment.html

OVA テンプレートが導入されて、Cisco Prime Collaboration Deployment の Cisco ISO ファイルがインストールされた後は、Web ベースのグラフィカル ユーザ インターフェイス（GUI）を使用して Cisco Prime Collaboration Deployment を管理し、コラボレーション アプリケーション サーバ ノードおよびクラスタを導入します。Cisco Prime Collaboration Deployment のアップグレードとバックアップは、CLI を使用して行います。

Cisco Prime Collaboration Deployment を使用した Cisco Collaboration アプリケーション サーバー クラスターの導入

Cisco Prime Collaboration Deployment を使用してコラボレーション アプリケーションのノードとクラスタを導入するには、次の手順に従う必要があります。

1。 コラボレーション アプリケーションの導入環境を準備します。

ターゲット コラボレーション アプリケーション（Unified CM、Unified CM IM and Presence サービス、Unity Connection）に必要な OVA テンプレートとブート可能 Cisco ISO イメージをダウンロードします。次に、SFTP を使用して、コラボレーション アプリケーションのインストール .iso イメージを Cisco Prime Collaboration Deployment 上の '/fresh_install' ディレクトリに転送します。

注　Cisco Prime Collaboration Deployment では、上述した以外の PA コラボレーション アプリケーション（Cisco Expressway、Cisco Meeting Server、Cisco TelePresence Management Suite など）をサポートしていません。

2。 OVA テンプレートと仮想マシン（VM）を計算インフラストラクチャの ESXi ホストに導入します。

導入サイズに基づく適切なアプリケーション OVA テンプレートを使用して、必要なコラボレーション アプリケーション ノードごとに 1 つの VM を作成します。たとえば、Unified CM パブリッシャ、専用 Unified CM TFTP サブスクライバ、Unified CM コール処理サブスクライバの各ノードの VM を作成します。Unified CM IM and Presence サービス ノードと Unity Connection ノードについて、このプロセスを繰り返します。すべての VM を電源オフの状態にままにしておきます。

3。 計算インフラストラクチャの ESXi ホストを Cisco Prime Collaboration Deployment インベントリに追加します。

Cisco Prime Collaboration Deployment の管理 GUI を使用して、コラボレーション アプリケーション VM の導入先とする 1 つ以上の ESXi ホストを追加します。各ホストに応じた適切な ESXi ホスト名、ユーザ名、パスワードを入力します。

4。 Cisco Prime Collaboration Deployment インベントリ内で新しい Unified Communications クラスタを定義します。

Cisco Prime Collaboration Deployment の管理 GUI を使用して、Unified CM、IM and Presence Service、Unity Connection のクラスタごとに Unified Communications クラスタを定義します。それぞれのクラスには一意の名前を指定する必要があります。次に、適切なコラボレーション アプリケーション ノード VM（ステップ 1 で作成したもの）を、それぞれ対応するクラスタに追加します。最後に、クラスタごとに、クラスタ全体の設定（資格情報とパスワード、証明書情報、DNS、NTP、タイム ゾーン）を構成します。

5。 各クラスタでのインストール タスクを追加します。

Cisco Prime Collaboration Deployment の管理 GUI で、Unified Communications クラスタの中からインストール対象とするクラスタを 1 つ選び、そのクラスタのノードに適切なインストール ファイル（Cisco ISO ファイル）を選択します。次に、開始時間（即時、または将来の特定の時間）を指定します。各クラスタについて、以上の手順を繰り返します。手動による開始を選択した場合は、各インストール タスクを手動で開始します。インストール タスクをモニタリングし、各インストールが正常に完了したことを確認します。

6。 インストールされたクラスタを、アプリケーション サーバの GUI を使用して設定します。

Cisco Prime Collaboration Deployment のインストール タスクが正常に完了すると、すべてのクラスタ ノードの基本設定が導入されます。次に、「コール制御」の章（Unified CM クラスタ、IM and Presence Service クラスタの場合）または「ボイス メッセージング」の章（Unity Connection クラスタの場合）に記載されている情報を使用して手動でクラスタを構成します。クラスタの設定が完了した後は、Cisco Prime Collaboration プロビジョニングを使用して移動、追加、変更、削除（MACD）の操作を行います（「Cisco Prime Collaboration Provisioning」を参照）。

Cisco Smart Software Manager

Cisco Smart Software Manager を使用すると、Cisco Unified CM、IM and Presence Service、Unity Connection ならびに他の Cisco 製品のライセンスの適用、追跡、管理を 1 か所で行うことができます。Cisco Smart Software Manager は、アプリケーション サーバの使用をユーザに許可するために必要なステップの多くを自動化することにより、管理者を支援します。

コア コンポーネント

Smart Software Manager アーキテクチャのコア コンポーネントは、Web でホストされる Cisco Smart Software Manager ポータルです。このポータルを使用して、企業の導入環境内にあるすべての Unified CM および Unity Connection クラスタについて、ユーザ ライセンスを取得、適用、追跡します。

利点

Enterprise Collaboration 向けプリファード アーキテクチャのコール制御およびボイス メッセージング クラスタの使用を許可するには、Cisco Smart Software Manager を使用する必要があります。シスコ スマート ソフトウェア ライセンシングには、次の利点があります。

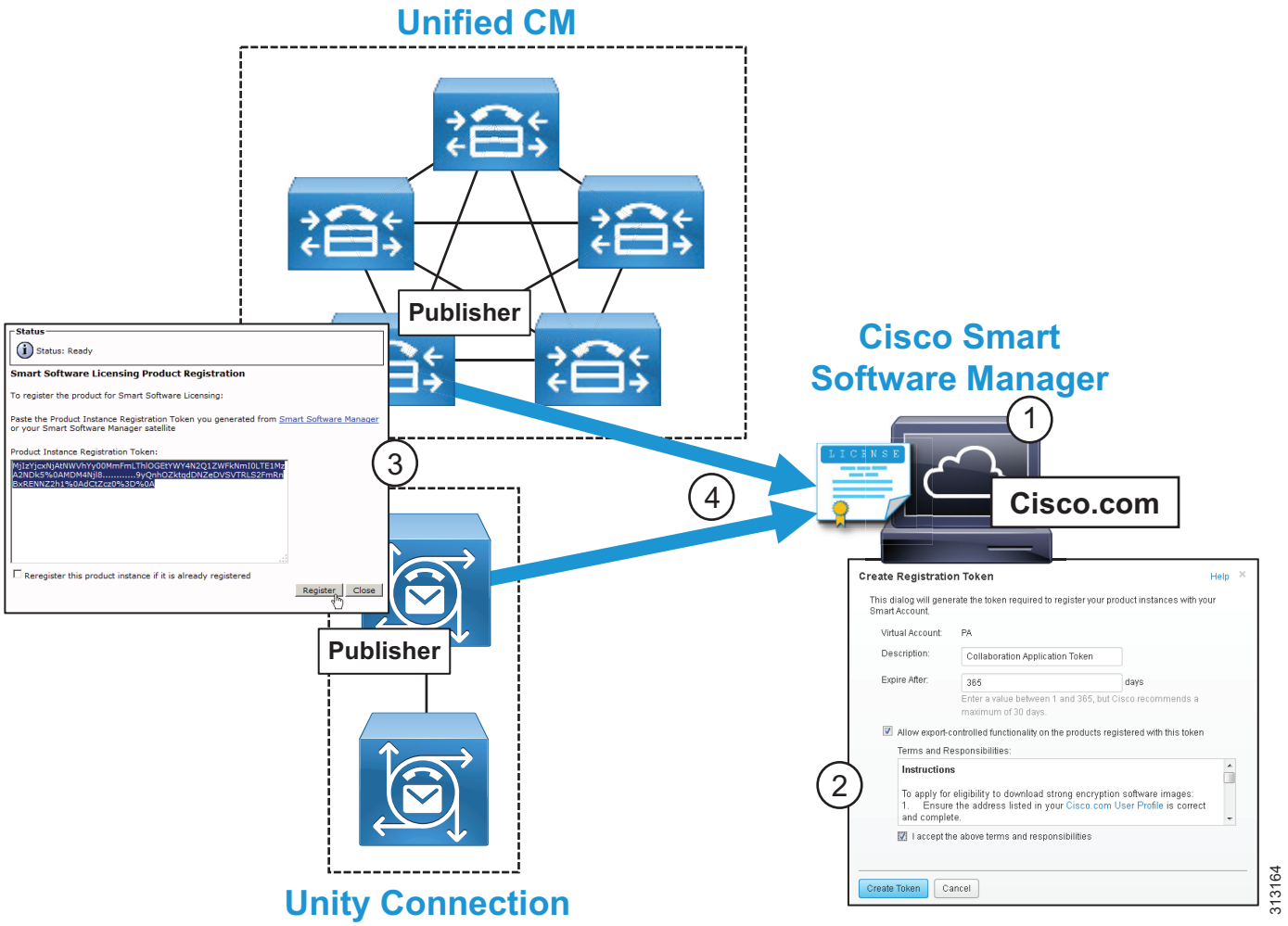
- Unified CM、Unified CM IM and Presence Service、Unity Connection でのユーザ ライセンスと機能ライセンスの管理、割り当て、権限付与、調整が一元化されます。
- 企業のすべてのクラスタでライセンス プールを共有できます。
- 企業全体での使用状況と権限付与に関するレポートを取得できます。
- 将来のライセンス計画、および導入環境内のユーザ数の増加に応じた追加ライセンスの調達を簡素化できます。

アーキテクチャー

Cisco Smart Software Manager アーキテクチャはシスコでホストする Cisco Smart Software Manager Web ポータルからなります。このポータルで、組織のコラボレーション アプリケーションに対する権限付与とライセンスを追跡し、コール制御およびボイス メッセージング コンポーネントを同期します。Cisco Smart Software Manager では、Cisco Unified CM と Unity Connection のユーザおよび機能ライセンスを管理し、モニタリングします。

Cisco Smart Software Manager ポータルを使用してソフトウェアと権限付与を管理する際は、まず、C：図 6-2 に示されているように適切なライセンスを取得して Cisco スマート アカウントに適用する必要があります（ステップ 1）。次に、管理者が Cisco Smart Software Manager ポータル（https://software.cisco.com）で製品インスタンスの登録トークンを生成します（ステップ 2）。管理者はその登録トークンを Cisco Smart Software Manager ポータルからコピーし、コラボレーション アプリケーション パブリッシャ製品インスタンス（Unified CM および Unity Connection）を登録します（ステップ 3）。登録されたパブリッシャは、Cisco Smart Software Manager と同期して、ユーザおよび機能ライセンス資格の情報を受信するようになります（ステップ 4）。

C：図 6-2　　Cisco Smart Software Manager アーキテクチャ



Cisco Unified CM クラスタと Unity Connection クラスタのパブリッシャ ノードでは、初期インストール時に自動的に Cisco Smart Licensing Manager サービスが有効にされます。Unified CM/Unity Connection パブリッシャと Cisco Smart Software Manager 間での登録と同期は、パブリッシャからインターネットでホストされた Cisco.com Cisco Smart Software Manager サービスへのアウトバウンド HTTPS 接続を使用して直接行われます。

Cisco Smart Software Manager の詳細については、次のリンク先を参照してください。

https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html

Cisco Smart Software Manager の役割

Cisco Smart Software Manager は、エンタープライズ コラボレーション アプリケーションの導入環境全体にわたり、ユーザベースのコール制御およびボイス メッセージングのライセンスと権限付与の管理を一元化します。Cisco Smart Software Manager を使用することで、ライセンス計画、ライセンスの権限付与と配布、使用状況の追跡を行うことが可能になります。Cisco Smart Software Manager はインターネットでホストされるため、ライセンスとソフトウェア権限付与の管理は Web ブラウザを使用して行います。

Cisco Smart Software Manager の代替アーキテクチャ

組織のネットワーク可用性に関する考慮事項、あるいはセキュリティ ポリシーにより、Cisco Unified CM クラスタや Unity Connection クラスタのパブリッシャ ノードから直接インターネットにアクセスできない場合は、以下のオプションがあります。

- HTTPS プロキシ

  組織にすでに HTTPS プロキシが導入されている場合、その HTTPS プロキシを使用して Cisco Smart Software Manager と通信することができます。

- オンプレミスの Cisco Smart Software Manager サテライト システム

  Cisco Unified CM と Unity Connection のパブリッシャがオンライン Cisco Smart Software Manager サービスではなく、Cisco Smart Software Manager サテライト オンプレミス サーバに登録して、ライセンスの使用状況をレポートします。このサテライト システムは、定期的にオンライン Cisco Smart Software Manager に接続して同期する必要があります。オンライン Cisco Smart Software Manager に接続されていない場合は、システムから提供されたレポート ファイルを、手動でこのオンライン サービスにアップロードする必要があります。

  Cisco Smart Software Manager サテライトについて詳しくは、次のリンク先を参照してください。

  https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html

- 特定のライセンスの予約

  Cisco Unified CM および Unity Connection は、Cisco Smart Software Manager サービスを使用した情報を始めに手動で交換すること (カットアンドペースト) によってライセンス供与されます。製品の設定と認証が完了したら、Cisco Smart Software Manager サービスとのやり取りは必要ありません。この設定では、予約が更新または削除されるまで、ライセンス予約が Cisco Smart Software Manager 内のシステムに永続的に割り当てられます。予約を更新するには、Cisco Smart Software Manager サービスと、ユニ統一された　CM とユニティコネクションシステム間で情報を手動で交換する必要があります。

Cisco Smart Software Manager の高適用性

オンライン Cisco Smart Software Manager アプリケーションには高可用性が備わっていますが、インターネット接続に問題が発生した場合、コラボレーション アプリケーション システムが動作を継続するのは問題発生後の 90 日間となります。システムが完全に要件に準拠しない状態になると、ユーザとデバイスをプロビジョニングすることができなくなります。システムを運用状態に維持するためには、オンライン Cisco Smart Software Manager に常にアクセス可能でなければなりません。

Cisco Smart Software Manager のスケーリング

Cisco Smart Software Manager はインターネットでホストされたオンライン サービスであるため、スケーラビリティに関する考慮事項はほとんど、あるいはまったくありません。企業の視点から見たサイジングに関する主な考慮事項は、インターネット接続帯域幅とネットワーク可用性です。

Cisco Smart Software Manager Deployment のプロセス

Cisco Smart Software Manager では、導入に関して考慮しなければならない 2 つの側面があります。

- Cisco Smart Account と Smart Software Manager を使用したライセンスと権限付与の管理
- コラボレーション製品インスタンスの承認および登録とライセンスの適用

Cisco Smart Account と Smart Software Manager を使用したライセンスと権限付与の管理

コラボレーション アプリケーションの使用に対するライセンスを付与するには、まず、適切なコラボレーション ユーザ ライセンスおよび機能ライセンスを調達する必要があります。これによって、コラボレーション アプリケーション システムを承認できるようになります。適切なライセンスを購入した後、それらのライセンスを Cisco スマート アカウントに適用できます。

次に、Cisco スマート アカウントを使用して Cisco Smart Software Manager（https://software.cisco.com）にアクセスします。Cisco Smart Software Manager にログインし、該当するバーチャル アカウント（組織に依存）を選択（または作成）します。このバーチャル アカウントを使用して、コラボレーション ライセンスの管理、ライセンスとライセンス使用状況の表示、製品インスタンスの登録を行うことができます。

Cisco スマート アカウントについては、次のリンク先を参照してください。

https://www.cisco.com/c/en/us/buy/smart-accounts.html

コラボレーション製品インスタンスの承認および登録とライセンスの適用

Cisco Unified CM および Unity Connection パブリッシャでは、デフォルトで自動的にスマート ライセンスが有効にされます。ただし、製品を Cisco Smart Software Manager に登録して、ライセンスをシステムに適用するまでは、システムはコンプライアンス違反の状態です。そのままの状態で猶予期間が経過すると、使用できる機能が大幅に削減されます。

Cisco Smart Software Manager を使用してコール制御およびボイス メッセージング クラスタのユーザ ライセンスを管理するためには、次の手順に従う必要があります。

1。 製品インスタンスの登録トークンを作成します。

スマート ライセンスをセットアップするために、Smart Software Manager に移動し、[新しいトークン ...（New Token...）] ボタンをクリックして、バーチャル アカウントを適用した新しい製品インスタンスの登録トークンを作成します。後続のダイアログボックスで、登録トークンが有効となる少ない日数を指定します（**有効期限**：）。**輸出規制による機能限定 ...** をオンにします。**上記利用条件と責任に同意する**というチェックボックス、およびチェックボックスをオンにして、**トークンの作成**をクリックします。

注　登録トークンの有効期間 (日数) は、低い値 (たとえば、3) に設定する必要があります。トークンは、スマート ライセンス登録プロセスの初期段階でのみ有効である必要があります。その期間を過ぎると、トークンは無効あるいは削除され、再度の使用が不可能となる場合があります。

2。 製品インスタンスを登録します。

次に、Unified CM および Unity Connection パブリッシャを登録するために、製品インスタンスの登録トークンを Smart Software Manager ポータルからコピーし、そのトークンをデバイス / 製品ラインセンス ウィンドウに入力します。Unified CM と Unity Connection のライセンス ページで、[登録（Register）] ボタンをクリックします。ポップアップ表示されるスマート ソフトウェア ライセンシングの製品登録ウィンドウで、製品インスタンスの登録トークンを入力し、[登録（Register）] ボタンをクリックして登録を完了します。

Unified CM パブリッシャと Unity Connections パブリッシャが登録されると、これらのパブリッシャは Cisco Smart Software Manager と同期して現在のユーザおよび機能のライセンスを受け取り、承認されるようになります。

上記の登録および承認の操作には、シスコ ソフトウェアおよびライセンスを管理するための有効なスマート アカウントと、適切な製品ライセンス資格が必要です。

Cisco Prime Collaboration Provisioning

Cisco Prime Collaboration プロビジョニングは、管理者が IP テレフォニー、ビデオ、ボイスメール、ユニファイド メッセージが統合された環境でのプロビジョニングのニーズを管理するために利用できる、スケーラブルな Web ベースのソリューションです。Cisco Prime Collaboration プロビジョニングを使用して、移動、追加、変更、削除（MACD）などの日常的な設定更新を行うことができます。

Enterprise Collaboration 向けプリファード アーキテクチャの場合、「コール制御」の章（Unified CM クラスタ、IM and Presence Service クラスタの場合）または「ボイス メッセージング」の章（Unity Connection クラスタの場合）に記載されている情報を使用して、手動で初期設定を行うことをお勧めします。クラスタを設定した後、Unified CM、IM and Presence Service、Unity Connection の運用上の設定更新（MACD）が必要になった場合は、Cisco Prime Collaboration プロビジョニングを使用して更新できます。

利点

Cisco Prime Collaboration プロビジョニングを使用して移動、追加、変更、削除（MACD）を行う場合は、次の特長と利点があります。

- Cisco Prime Collaboration プロビジョニングでは、組織全体およびクラスタ全体にわたるユーザを単一の統合ビューで表示することができます。
- 各 MACD 要求に割り当てられた注文番号を使用して、MACD を追跡および監査できます。
- MACD を一度に 1 つずつ手動で実行する代わりに、バッチ ファイルとして同時にまとめて実行できます。
- サービス テンプレートにより、MACD が高速化されるとともに、手動による設定で発生しがちな設定エラーが少なくなります。
- 最繁時以外の時間帯にバッチ ファイルを実行することで、起こり得るユーザ サービスの中断を回避できます。

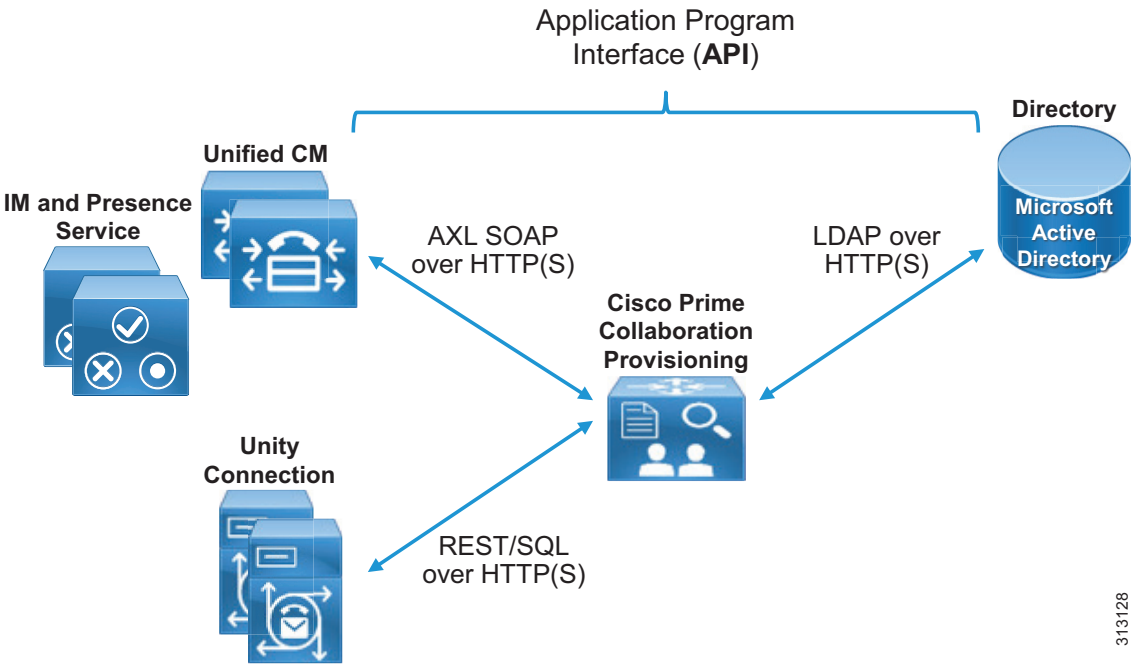
アーキテクチャー

Cisco Prime Collaboration プロビジョニングのアーキテクチャは、Cisco Prime Collaboration プロビジョニング サーバ ノード、Cisco Unified CM、IM and Presence Service、Unity Connection からなります。Cisco Prime Collaboration プロビジョニングでは各種の API を使用してコラボレーション アプリケーション サーバに接続し、これらのサーバを設定します。

Cisco Prime Collaboration Provisioning の役割

Cisco Prime Collaboration プロビジョニングは、Cisco Unified Communications Manager と Cisco Unity Connection が組み込まれ、IP テレフォニー、ビデオ、ボイスメール、ユニファイド メッセージングが統合された環境で、IP 通信のエンドポイントとサービスの設定変更を管理します。C：図 6-3 に、これらのコンポーネントと API を示します。

C：図 6-3　Cisco Prime Collaboration プロビジョニング アーキテクチャ



統一されたコミュニケーションアプリケーションとの通信に使用されるプロトコル

Cisco Prime Collaboration プロビジョニングでは、管理対象のアプリケーションと通信するために、次のプロトコルを使用します（C：表 6-2 を参照）。

- Cisco Unified CM と Cisco Unified CM IM and Presence Service

  Cisco Prime Collaboration プロビジョニングでは、AXL SOAP over an HTTPS API を使用して Unified CM と IM and Presence Service と通信するため、Unified CM と IM and Presence Service のリモート プロビジョニングが可能です。

- Cisco Unity Connection

  Cisco Prime Collaboration プロビジョニングでは、REST および SQL over HTTPS を使用して Cisco Unity Connection をプロビジョニングします。

- ディレクトリ サーバ（Microsoft Active Directory）

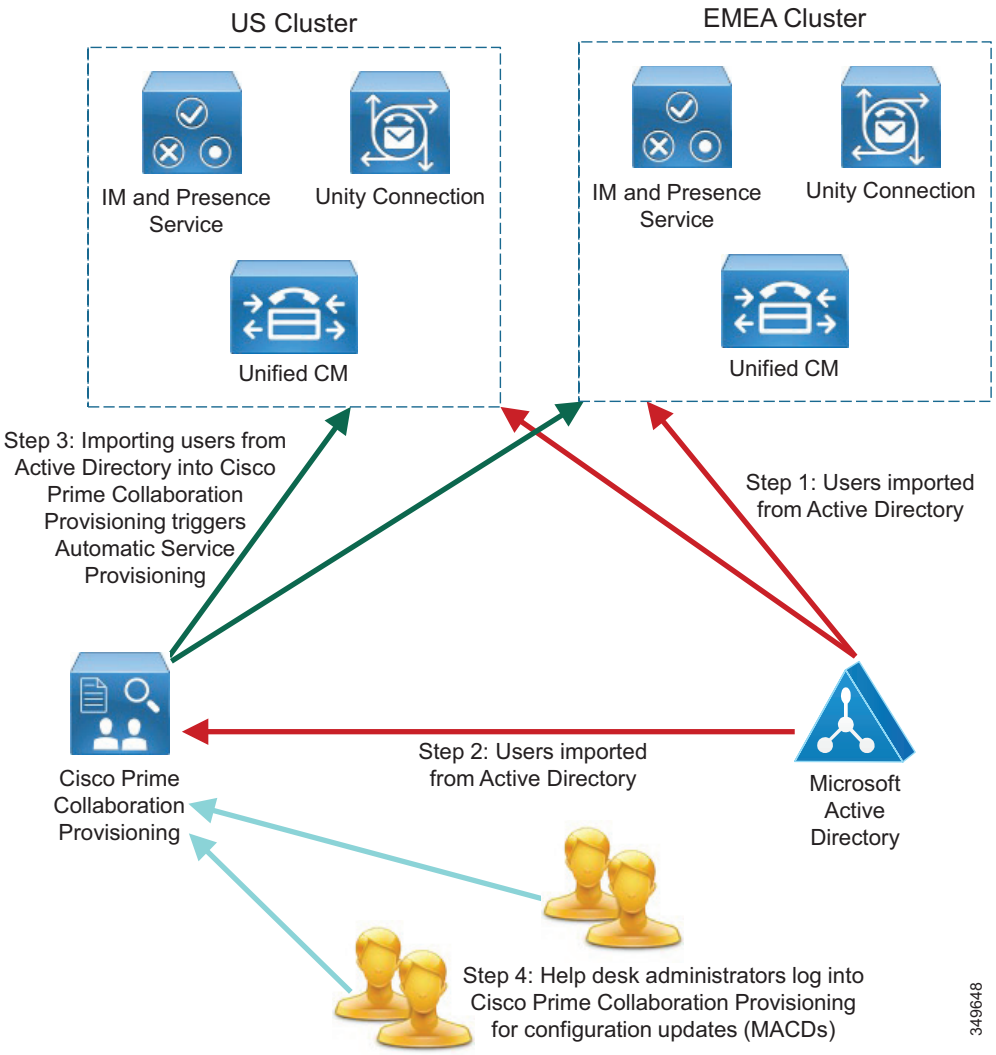
  Cisco Prime Collaboration プロビジョニングは、Microsoft Active Directory サーバとの通信には LDAP を使用します。この通信が LDAP over HTTPS になるよう、SSL を有効にすることをお勧めします。SSL が有効でない場合、Cisco Prime Collaboration プロビジョニングは HTTP を介した LDAP を使用します。

C：表 6-2　Cisco Prime Collaboration プロビジョニングで使用するプロトコルの要約

Unified Communications Manager	Cisco Prime Collaboration プロビジョニングで使用するプロトコル
Cisco Unified CM、IM および Presence Service	AXL SOAP over HTTPS API
Cisco Unity Connection	HTTPS を介した REST と SQL
ディレクトリ サーバ（Microsoft Active Directory）	LDAP over HTTPS（推奨）または LDAP over HTTP

移動、追加、変更、削除（MACD）などの日常的な運用上のプロビジョニングを行えるようにするには、管理者は Cisco Prime Collaboration プロビジョニング上にユーザ アカウントを作成する必要があります。それには、Cisco Prime Collaboration プロビジョニングに Microsoft Active Directory サーバを統合するという方法、または Cisco Unified CM のユーザを同期するという方法があります（C：図 6-4 を参照）。あるいは、バッチまたはグラフィカル ユーザ インターフェイスを使用して、手動でユーザを Cisco Prime Collaboration プロビジョニングに追加することもできます。Enterprise Collaboration 向けプリファード アーキテクチャの場合、ユーザ オンボードおよびオフボードに対する自動サービス プロビジョニングをサポートするために、Unified CM と Cisco Prime Collaboration プロビジョニングの両方で LDAP 同期を有効にすることをお勧めします。LDAP 同期を有効にすることで、ユーザがディレクトリ サーバに追加されると自動的にサービスがプロビジョニングされ、ユーザがディレクトリ サーバから削除されると、そのユーザに対するすべてのサービスが削除されるようになります。ただし、Cisco Prime Collaboration プロビジョニングとすべての Unified Communications アプリケーションはディレクトリ サーバと同期するため、どのアプリケーションが最初にディレクトリ サービスと同期するかが問題になります。Cisco Prime Collaboration プロビジョニングが最初に同期して新しいユーザをダウンロードした場合、そのユーザが Unified Communications アプリケーションで見つからなければ、Cisco Prime Collaboration プロビジョニングはそのユーザが Unified Communications アプリケーションで見つかるまで待機します。そのユーザ ロールに対して自動サービス プロビジョニング（ASP）が有効にされている場合、ユーザが見つかった時点で ASP がトリガーされます。したがって、Cisco Prime Collaboration プロビジョニングよりも先に Unified Communications アプリケーションが同期するよう、Active Directory サーバの同期機能を使用して同期をスケジュールすることをお勧めします。この章の残りの部分では、この推奨に従っていることを前提とします。

C：図 6-4　Cisco Prime Collaboration の Microsoft Active Directory とのプロビジョニング同期



Cisco Prime Collaboration Provisioning の用語

ここでは、Cisco Prime Collaboration プロビジョニングの最も重要な概念と主要な機能を説明する用語について説明します。ここで説明する用語は、この章全体を通して使用されています。

- ドメイン：ドメインとは、1 人以上の管理者によって管理されるユーザのグループを指します。ドメイン管理者は、そのドメインのすべてのユーザの移動、追加、変更、および削除（MACD）を処理します。
- サービス エリア：サービス エリアは、ドメイン内でのグループ化であり、通常はロケーションまたはサイトを表します。設定更新（MACD）の操作を行う際は、サービス エリアが、使用するプロビジョニング属性の値を決定するテンプレート メカニズムになります。

- ユーザ ロール：ユーザ ロールは、ユーザのさまざまなクラスに対して使用を許可する Unified Communications の機能と、自動サービス プロビジョニング プロセスで特定のユーザ タイプに適用するサービス テンプレートを制御することにより、ポリシーを適用します。管理者はさまざまなサービス レベルを定義するために、多数のユーザ ロールを作成できます。デフォルトのユーザ ロールは、従業員、役員、およびルームです。
- サービス テンプレート：サービス テンプレートを使用することで、量の多少にかかわらず、複数の設定を 1 つのテンプレートにまとめ、エンドポイントまたはサービスに適用することができます。このため、多数の属性を個々に設定する場合と比べて時間が節約され、属性の不足または属性フィールドの入力ミスを防止して正確な処理が可能です。サービス テンプレートはキーワードとキーワード切り捨てを活用して、エンドポイントに表示される行のテキストをカスタマイズできます。
- ビジネス ルール：ドメインには、ビジネス ルールまたはポリシーを設定できます。これらのルールとポリシーは、そのドメイン内のユーザに対するサービスに適用されます。
- インフラストラクチャ同期：これは、Cisco Unified CM や Cisco Unity Connection から Cisco Prime Collaboration プロビジョニングに、個々のユーザに固有ではないオブジェクトのみをダウンロードするプロセスです。
- ユーザ同期：Cisco Unified CM や Cisco Unity Connection から Cisco Prime Collaboration プロビジョニングへのこのダウンロード プロセスにより、個々のユーザに関連するすべてのユーザ アカウントとすべてのオブジェクトが検出されます。
- ドメイン同期：これは、ユーザ同期の実行中にすべての Unified Communications クラスタから検出された既存のユーザを、それぞれに対応するドメインに関連付けるプロセスです。
- バッチ エンジン：Cisco Prime Collaboration プロビジョニングのバッチ エンジンを使用して、多数のユーザとそれらのユーザのサービスに対して一括処理を実行することができます。Cisco Unified Communications Manager（Unified CM）でのみ実行される Cisco Unified CM BAT ファイルとは異なり、Cisco Prime Collaboration プロビジョニングのバッチ ファイルでは、複数の Unified Communications アプリケーションに対してコマンドを実行できます。

Cisco Prime Collaboration Provisioning の展開プロセス

Cisco Prime Collaboration プロビジョニングをインストールするには、Cisco Prime Collaboration プロビジョニング メディア OVA テンプレート（最大 20,000 のエンドポイントに対応）をダウンロードします。このテンプレートは、Enterprise Collaboration 向けプリファード アーキテクチャで使用するためのものです。

OVA テンプレート ファイルの名前は、**cpc-provisioning-<***version number***>-<***build number***>-<***deployment size***>.ova** の形式になっています。ここで、バージョン番号は Cisco Prime Collaboration プロビジョニングのリリース番号です。Enterprise Collaboration 向けプリファード アーキテクチャの場合、次の名前の OVA テンプレート ファイルをダウンロードしてください。

cpc-provisioning-12.2.0.659-medium_SIGNED.ova

OVA テンプレートのインストールが完了したら、システムの電源を入れて、ネットワークの詳細（IP アドレス、ネットマスク、ゲートウェイ、DNS、NTP）を設定できます。インストールの手順についての詳細は、以下で入手できる最新バージョンの *Cisco Prime Collaboration Provisioning Install and Upgrade Guide* を参照してください。

https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.html

Cisco Prime Collaboration Provisioning を使用した設定更新

ここでは、Cisco Prime Collaboration プロビジョニングを使用して、Enterprise Collaboration 向けプリファード アーキテクチャに含まれる Unified Communications アプリケーションの設定更新（移動、追加、変更、削除）を行う方法を説明します。

次の手順に従って、Cisco Prime Collaboration プロビジョニングを導入し、Unified Communications アプリケーションの設定更新（MACD）に使用します。この手順を順番どおりに実行することで、依存関係への影響を最小限に抑えるとともに、最も効率的な方法で Cisco Prime Collaboration プロビジョニングを導入できます。

1。 Cisco Prime Collaboration プロビジョニングに Unified Communications アプリケーションを接続します。

Unified Communications アプリケーションを Cisco Prime Collaboration プロビジョニングに追加するには、Cisco Prime Collaboration プロビジョニングがそれらのアプリケーションに接続するために必要な資格情報を入力します。この操作は、[デバイスの設定（Device Setup）] メニューから行うことができます。ここで追加する必要があるのは、Unified CM と Unity Connection のパブリッシャ ノードのみであることに注意してください。

2。 ドメインを作成します。ドメインとは、さまざまなサイトを管理するユーザおよび管理者のグループを指します。

組織内の管理者の数に応じた数のドメインを作成することをお勧めします。たとえば、2 つのクラスタ（US と EMEA）があり、管理者のグループが 2 つある場合（米国のユーザの MACD を処理するグループと、EMEA のユーザの MACD を処理するグループ）、2 つのドメインを作成します。ただし、組織でユーザ数の少ない小規模な管理グループを作成する必要がある場合、それ以上のドメインを作成することもできます。たとえば、米国内の州または EMEA 内の国ごとにドメインを作成できます。

3。 ユーザ ロールを追加 / 編集します。

ドメインを作成すると、作成された各ドメイン内にユーザ ロールが作成されているはずです。Cisco Prime Collaboration プロビジョニングでは、自動的にいくつかのデフォルト ユーザ ロールが作成されます。これらのロールは、管理者が変更できます。また、必要に応じて追加のロールを作成することもできます。さらに、必要な場合はユーザ ロールに対して自動サービス プロビジョニングを有効にすることもできます。この場合、ユーザのオンボーディング（ユーザが Active Directory に追加されて、Active Directory との同期後に Cisco Prime Collaboration プロビジョニングに取り込まれた時点で、自動的にサービスがプロビジョニングされます）、オフボーディング（ユーザが Active Directory から削除されると、そのユーザに対するサービスが自動的に削除されます）が可能になります。

4。 インフラストラクチャのコンポーネントを同期します。

Cisco Prime Collaboration プロビジョニングは Unified Communications アプリケーションと同期されなければなりません。この同期のステップで、Cisco Prime Collaboration プロビジョニングが Unified CM、Unity Connection、Unified CM IM and Presence Service から設定をダウンロードします。次のステップでサービス エリアを作成する際には、Unified CM からダウンロードしたデバイス プール、ロケーション、パーティションと、Unity Connection からダウンロードしたボイスメール テンプレートが必要になります。

5。 サービス エリアを作成します。

サービス エリアには、デバイス プール、ロケーション、ボイスメール テンプレート、ディレクトリ番号（DN）ブロックをはじめとする一連のサービス パラメータが格納されます。サービス エリアはサイトまたは物理的な場所にマッピングすることをお勧めします。これらのサービス エリアはドメインの中にあり、そのドメイン内のユーザにのみ適用されます。各サービス エリアは特定のデバイス プールとロケーションに接続されることから、必須の属性のさまざまな組み合わせによって、サービス エリアの数がかなり多くなる可能性があります。したがって、未使用のデバイス プールをクリーンアップするか、未使用のデバイス プールに対してはサービス エリアを作成しないようにしてください。サービス エリアが管理しきれないほどの数になった場合は、各ドメイン内のサービス エリアの数を減らすためにドメインの数を増やすことをお勧めします。

6。 電話、回線、ボイスメールなどを対象にしたサービス テンプレートを作成します。

これらのサービス テンプレートは、人為的なミスを最小限に抑えて設定エラーを削減するために、注文時にすぐに適用できるものです。最もよく使用されるエンドポイント モデル、回線、およびボイスメール サービス用のサービス テンプレートと、必要に応じて Extension Mobility およびモート接続先プロファイル用のサービス テンプレートを作成することをお勧めします。

7。 LDAP、ユーザ、ドメインの同期を設定します。

テンプレートを作成してサービス テンプレート セクションのユーザ ロールとサービス エリアに割り当てた後は、LDAP 同期を実行して Microsoft Active Directory サーバから Cisco Prime Collaboration プロビジョニングにユーザを取り込むことができます。ドメイン LDAP フィルタ、サービス エリア LDAP フィルタ、ユーザ ロール LDAP フィルタとして拡張クエリを作成できるので、特定の属性に基づいてユーザを除外することを強く推奨します。Active Directory からユーザをインポートすると、自動サービス プロビジョニング（ASP）がトリガーされます。これにより Cisco Prime Collaboration プロビジョニングは、ビジネス ルール セクションに指定されているデフォルト ユーザ ロールに属する、ASP セクションに指定されているサービスを設定します。Cisco Prime Collaboration プロビジョニングが Active Directory サーバと同期する前に、Active Directory サーバが Unified CM および Unity Connection に同期するようにしてください。Unified CM と Unity Connection には Active Directory サーバが統合されていることから、これらのアプリケーションは両方とも、Cisco Prime Collaboration プロビジョニングの [デバイスの設定（Device Setup）] で [LDAP 統合（LDAP integrated）] としてマーキングされます。このため、Cisco Prime Collaboration プロビジョニングはユーザがこれらのアプリケーションに取り込まれてから、サービスをプロビジョニングします。インフラストラクチャ同期とユーザ同期が完了した後は、ドメイン同期が必要です。

8。 [アクセス制御（Access Control）] メニューを使用して、プロビジョニング権限、ドメイン管理者、その他の管理者を割り当てます。

9。 プロビジョニング サービスの受注を開始します。

10。頻繁に実行される操作のバッチ ファイルを作成します。

Cisco Prime Collaboration Provisioning を使用した設定更新のトラブルシューティング

Cisco Prime Collaboration プロビジョニングは、トレース メッセージを調べたり、ログ ファイルを収集したりするための便利な手段になります。Cisco Prime Collaboration プロビジョニングによって、Service Enabling Platform（SEP）モジュール（sep.log）および Network Interface and Configuration Engine（NICE）サービス（nice.01.log）のアプリケーション ログ ファイルが作成されます。ログ ファイルは、/opt/cupm/sep/logs フォルダにあります。これらのログには、[管理（Administration）] メニューの [ロギング（Logging）] および [ShowTech] メニュー オプションからアクセスすることもできます。トラブルシューティングの前に、アプリケーション レベルと NICE レベルのログを [詳細（DETAILED）] に設定すると、Unity Connection、Unified CM、Unified CM IM and Presence Service との間で交換されたメッセージをログに記録できます。トレースを収集するには、[ShowTech の生成（Generate ShowTech）] を使用します。管理者は [ログの参照（Browse Logs）] > [アプリケーション ログと NICE ログ（Application and NICE logs）] オプションを選択して、ユーザ インターフェイスでログを表示できます。この場合、管理者はブラウザ ウィンドウでログを表示することも、ローカル コンピュータにログをダウンロードすることもできます。これらのログには、日常的な設定更新（MACD）で発生する可能性のある問題をトラブルシューティングするのに非常に役立つ多数のメッセージが記録されます。

Cisco Prime Collaboration Provisioning の冗長性とバックアップ

Cisco Prime Collaboration プロビジョニングは、設定およびとデータのバックアップと復元をサポートします。Cisco Prime Collaboration プロビジョニングを使用して、設定とデータを FTP または SFTP 経由で外部サーバにバックアップすることを強くお勧めします。バックアップと復元を実行する手順について詳しくは、次のリンク先にある Cisco Prime Collaboration プロビジョニングの製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-user-guide-list.html

セキュリティー

改訂日：2019 年 2 月 19 日

この章では、企業のコラボレーション向けシスコ プリファード アーキテクチャ（PA）のネットワーク アクセス セキュリティ、電話料金の詐欺行為に関するアクセス保護、証明書の管理、および暗号化について説明します。

この章の前半ではアーキテクチャの概要を示し、後半では導入手順を説明します。「アーキテクチャー」では、セキュリティのさまざまな側面について説明します。最初に、階層型セキュリティ アプローチ、不正アクセスからの保護、電話料金の詐欺行為からの保護について概説します。その後、証明書の管理と暗号化について説明します。次の項は「展開」です。この項では、証明書を生成および管理する手順と、このソリューションのすべてのコンポーネントに対して暗号化を有効化およびプロビジョニングする手順について説明します。

注　この章の情報は、製品がソフトウェアバージョン 12.5 以降を実行していることを前提としています。

この章の新規情報とは

C：表 7-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

C：表 7-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
ローカルで有効な証明書（LSC）のインスタレーション	この章の各項で説明	2019 年 1 月 23 日
ローカルで有効な証明書（LSC）をインストールするための Jabber 用の SIP OAuth モードと要件の削除	この章の各項で説明	2019 年 1 月 23 日
Cisco Meeting Management	この章の各項で説明	2019 年 1 月 23 日
CAPF オンライン CA モード	CAPF オンライン CA モード（C：7-41 ページ）	2019 年 1 月 23 日
CE エンドポイントでの MIC のサポート	この章の各項で説明	2019 年 1 月 23 日

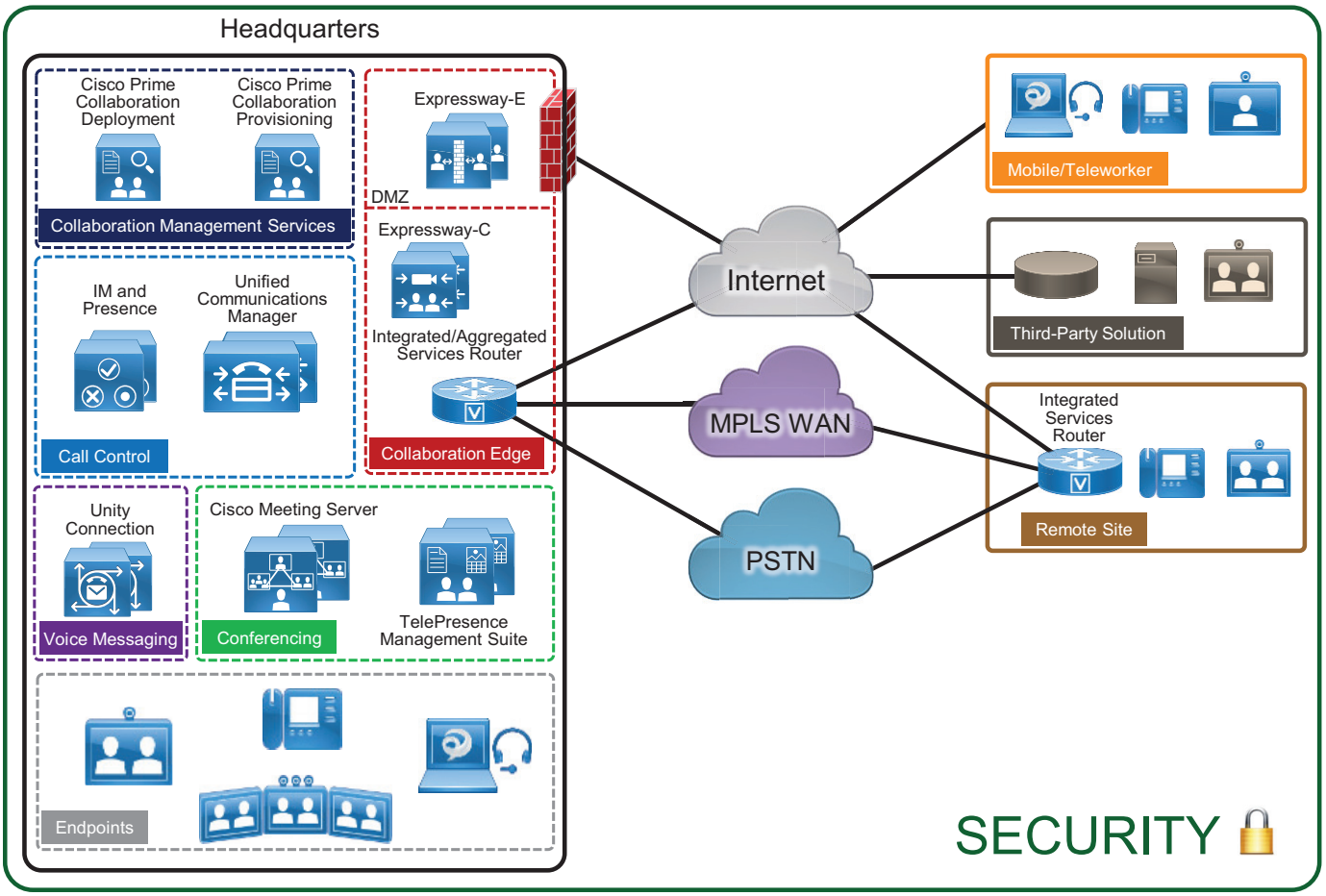
C：表 7-1 新規情報、またはこのマニュアルの以前のリリースからの変更情報（続き）

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 Prime License Manager はこのアーキテクチャから除外されたため、この章から削除されました。	この章のすべての項	2017 年 8 月 30 日
初期信頼リスト（ITL）とトークンレス型証明書信頼リスト（CTL）	この章の各項で説明	2017 年 8 月 30 日

コア コンポーネント

Cisco Collaboration ソリューションのすべてのコンポーネントにセキュリティが適用されます（C：図 7-1 を参照）。ソリューション全体でセキュリティを実装することが重要です。実際には、階層型アプローチでセキュリティを実装することが重要です。1 つのコンポーネントに頼ってセキュリティを提供するのではなく、多層型防御を計画します。

C：図 7-1 企業のコラボレーション向けプリファード アーキテクチャのすべてのコンポーネントのセキュリティ保護



主なメリット

この展開には次の利点があります。

- 階層型アプローチを導入することで、多層型防御が実現します。
- ネットワークとシステムへのアクセスを保護することで、サーバ、コラボレーション ソリューション、組織のその他の部分への侵害が困難になります。
- 電話料金の詐欺行為からの保護メカニズムを導入することで、不正請求の原因となるテレフォニー システム、データ ネットワーク、および PSTN 回線への不正アクセスを防止できます。
- さまざまな通信で暗号化と証明書を使用することで、盗聴、改ざん、セッション リプレイからの保護を実現できます。
- 適切な証明書管理計画を実施することで、適切なレベルの保護を実現し、かつ複雑さを軽減できます。

アーキテクチャー

はじめに、Cisco Collaboration のセキュリティ メカニズムの概要について説明します。次に、電話料金の詐欺行為の緩和と、証明書の管理および暗号化について説明します。

レイヤ化したセキュリティー

さまざまな脅威が存在し、これらの脅威に対処できるさまざまなメカニズムがあります。一般的なベスト プラクティスとして、コラボレーション導入を保護する多層セキュリティ アプローチを使用します。施設への物理アクセスと、ネットワーク、サーバ、エンドポイント、およびシステムへのアクセスを保護し、安全にする必要があります。通信を暗号化し、適切な証明書管理システムを導入する必要があります。可能な限り多くのコンポーネントおよび層を保護することでセキュリティが強化されます。特定の層またはコンポーネントが侵害を受けても、他のセキュリティ層およびセキュリティ メカニズムによりシステムは引き続き保護されます。

C：表 7-2 に、コラボレーションにおける脅威と対策の例を示します。それぞれの脅威に対して複数の対策を導入してください。

C：表 7-2　　コラボレーションの脅威とその対策の例

脅威	対策
サービス拒否（DoS）	物理的セキュリティ、ネットワーク セキュリティ、ファイアウォールおよび侵入防御システム（IPS）、QoS
スパムおよびインターネット テレフォニーでのスパム	ファイアウォールおよび高度なマルウェア防御（AMP）、Cisco Collaboration エッジ セキュリティ、Cisco Unified Communications Manager（Unified CM）ダイヤルプラン
ウイルス	ホストベースのファイアウォール、IPS、ウイルス対策ソフトウェア
電話料金の詐欺行為	Cisco Unified CM コーリング サーチ スペース（CSS）およびパーティション、電話料金の詐欺行為の防止およびアクセス保護、Cisco Collaboration エッジ セキュリティ

C：表 7-2　コラボレーションの脅威とその対策の例（続き）

脅威	対策
個人情報の入手	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ
中間者攻撃	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ
盗聴	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ
なりすまし	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ
メディア改ざん	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ
データ変更	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ
セッション リプレイ	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ

物理的なセキュリティー

最初の防御策は、物理的なセキュリティです。施設、ネットワーク アクセス、あるいはさらに重要なコア ネットワークインフラストラクチャおよびサーバに対する物理的セキュリティを導入することが重要です。物理的セキュリティが侵害されると、施設やサーバへの電源遮断によるサービスの中断などの単純な攻撃が可能になります。物理的にアクセスできるようになった攻撃者は、サーバ デバイスにアクセスし、パスワードをリセットしてサーバへのアクセスを可能にします。物理的にアクセスできることで、中間者攻撃などの高度な攻撃も可能になるため、2 番目のセキュリティ層であるネットワーク セキュリティが重要になります。

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

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

https://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html

ネットワーク セキュリティー

次の防御策はネットワーク セキュリティです。次の項では、いくつかのネットワーク セキュリティ メカニズムの例を紹介します。この項では、ネットワーク セキュリティについて簡単に説明します。このガイドの展開では、ネットワーク セキュリティについては説明しません。ネットワーク セキュリティの詳細については、次のリンク先にあるネットワーク セキュリティ設計ガイドを参照してください。

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

音声 / ビデオ VLAN

次の理由により、音声 / ビデオ VLAN とデータ VLAN を分離することを推奨します。

- 悪質なネットワーク攻撃からの保護

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

- 管理および設定の容易性

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

音声 / ビデオ VLAN には、卓上電話（ハードウェア）とビデオ システムが含まれます。データ VLAN には、エンドユーザのデスクトップおよびラップトップ、Jabber などのソフトウェア クライアントが含まれます。アクセス リスト（ACL）、VLAN アクセス リスト（VACL）、またはファイアウォールを使用して、VLAN 間のトラフィックを制限できます。

ワイヤレス アクセスの場合は、追加の考慮事項があります。詳細については、https://www.cisco.com/go/ucsrnd から入手可能な『*Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide*』および『*Cisco Collaboration System Solution Reference Network Design (SRND)*』を参照してください。

レイヤ 2 およびレイヤ 3 セキュリティ

レイヤ 2 およびレイヤ 3 で使用可能な標準セキュリティ機能を使用します。

ポート セキュリティ

スイッチ ネットワークに対する典型的な攻撃は、MAC 連想メモリ（CAM）フラッディング攻撃です。このタイプの攻撃では、スイッチに対して大量の MAC アドレスによるフラッディングが実行されることで、スイッチは、エンド ステーションまたはデバイスが接続されているポートを判別できなくなります。デバイスが接続されているポートを判別できない場合、スイッチは、そのデバイスが宛先になっているトラフィックを VLAN 全体にブロードキャストします。これにより、攻撃者は、VLAN 内のすべてのユーザに到達するすべてのトラフィックを見ることができます。MAC フラッディング攻撃を抑制するには、ポート セキュリティまたはダイナミック ポート セキュリティのいずれかを使用できます。承認メカニズムとしてポート セキュリティを使用する必要がない場合、特定のポートに接続する機器分の MAC アドレスの数を設定するダイナミック ポート セキュリティを使用できます。たとえば、1 台のワークステーションが接続されているポートの場合、取得する MAC アドレスの数を 1 に制限できます。1 台の Cisco Unified IP Phone と、その背後に 1 台のワークステーションが接続されているポートの場合、電話機の PC ポートに 1 台のワークステーションを接続するには、取得する MAC アドレスの数を 2 に設定できます（1 つは IP Phone 用、1 つは電話機の背後にあるワークステーション用）。ポート セキュリティでは、エンドポイントの MAC アドレスを確認する一種のデバイスレベル セキュリティ認証も実現します。

DHCP スヌーピング

Dynamic Host Configuration Protocol（DHCP）スヌーピングは、承認されていない DHCP または不正な DHCP サーバがネットワーク上で IP アドレスを配布するのを防止します。具体的には、信頼されていないポートからの DHCP 要求へのすべての応答をブロックします。電話機を設置する際に、そのほとんどが DHCP を使用して複数の電話機に IP アドレスを配布しており、スイッチで DHCP スヌーピング機能を使用し DHCP メッセージングを保護する必要があります。DHCP スヌーピングでは、DHCP サービス妨害（DoS）攻撃に使用される DHCP アドレス範囲枯渇攻撃からの保護も促進されます。DHCP スヌーピングを有効にすると、信頼されていない

ポートで、送信元 MAC アドレスと DHCP ペイロード情報が比較され、それらが一致しない場合は要求が失敗します。DHCP スヌーピングにより、任意の単一デバイスが特定範囲内のすべての IP アドレスをキャプチャすることを防止できますが、この機能が正しく設定されていないと、認定ユーザの IP アドレスが拒否される場合があります。

ダイナミック ARP インスペクション

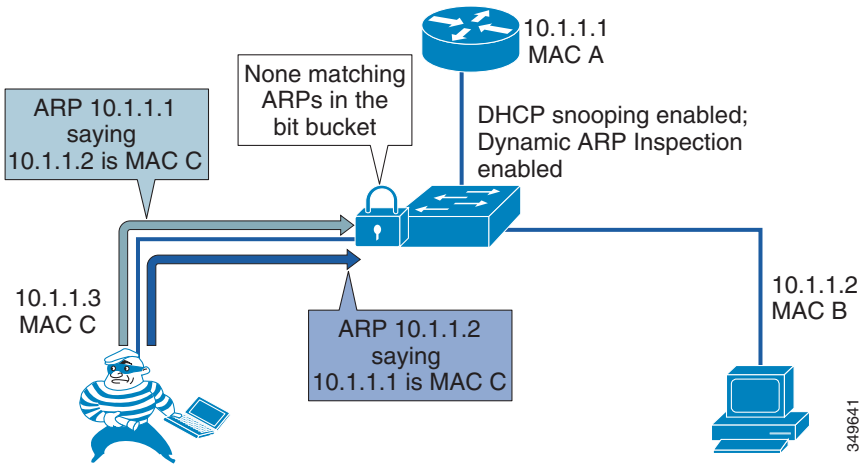
ダイナミック アドレス解決プロトコル（ARP）インスペクション（DAI）は、ルータのスイッチに接続されたデバイスに対する Gratuitous ARP 攻撃を防止するために、スイッチで使用される機能です。

Gratuitous ARP（GARP）は、要求がなくても送信される ARP 応答です。通常の使用法では、MAC ブロードキャストとして送信されます。GARP メッセージを受信する、LAN セグメント上のすべてのステーションは、この非請求 ARP 応答をキャッシュに入れます。この非請求 ARP 応答により、送信者が、GARP メッセージに含まれる IP アドレスのオーナーであることが認定されます。Gratuitous ARP には、障害時に別のステーションのアドレスを引き継ぐ必要があるステーションを正当に使用します。ただし、Gratuitous ARP は、別のステーションの身分を不正にかたること目的とした悪質なプログラムにより悪用される可能性もあります。悪質なステーションが、相互に通信しているその他の 2 つのステーションのトラフィックを自らにリダイレクトすると、GARP メッセージを送信したハッカーが中間者になります。

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

ダイナミック ARP インスペクション（DAI）では、ARP 応答または Gratuitous ARP メッセージを正当化するために、DHCP バインディングが存在している必要があります。ホストで、アドレスを取得するための DHCP が使用されていない場合、そのホストを信頼するか、ホストの IP アドレスと MAC アドレスを対応付けるために ARP インスペクション用のアクセス コントロール リスト（ACL）を作成する必要があります（C：図 7-2 を参照）。DHCP スヌーピングと同様に、DAI は VLAN ごとに有効化されます。すべてのポートは、デフォルトで、信頼できないポートとして定義されます。DAI で DHCP スヌーピングからのバインディング情報を活用するには、DAI を有効化する前に、VLAN で DHCP スヌーピングを有効化する必要があります。

C：図 7-2　　DHCP スヌーピングおよび DAI を使用した ARP 攻撃の防止



IP ソース ガード

IP ソース ガードは、レイヤ 2 ポートで送信元 IP アドレス フィルタリングを提供して、悪意のあるホストが正規のホストの IP アドレスを装うことで正規のホストを偽装することを防ぎます。この機能では、ダイナミックな Dynamic Host Configuration Protocol（DHCP）スヌーピングおよびスタティックな IP ソース バインディングを使用して、IP アドレスと信頼できないレイヤ 2 アクセス ポート上のホストを照合します。

まず、DHCP パケットを除く、保護済みポート上の全 IP トラフィックがブロックされます。クライアントが DHCP サーバから IP アドレスを受信したあと、またスタティック IP ソース バインディングが管理者によって設定されたあと、その IP 送信元アドレスのある全トラフィックがそのクライアントから許可されます。他のホストからのトラフィックは拒否されます。このフィルタリングは、隣接ホストの IP アドレスを要求することによって、ホストのネットワーク攻撃を制限します。IP ソース ガードは、暗黙的なポート アクセス コントロール リスト（PACL）を自動的に作成するポートベースの機能です。

802.1X

802.1X は、エンドユーザまたはデバイスのアイデンティティに基づいてネットワーク接続を許可または拒否する IEEE 規格です。802.1X 認証機能は、シスコ エンドポイントのデバイス クレデンシャルの、ネットワークへのアクセス権を与える前に行う識別と検証に使用できます。802.1X は、エンド デバイスと RADIUS サーバ（Cisco Identity Service Engine（ISE）など）間で機能する MAC レイヤ プロトコルです。このプロトコルは、Extensible Authentication Protocol（EAP）over LAN（EAPOL）をカプセル化し、エンド デバイスとスイッチの間での認証メッセージの転送を行います。802.1X 認証プロセスでは、シスコのエンドポイントが 802.1X サプリカントとして動作し、ネットワーク アクセス要求を開始し、証明書（ローカルで有効な証明書を推奨）を提供します。オーセンティケータとして機能する Cisco Catalyst スイッチは、その要求を認証サーバに渡し、その電話にネットワークへのアクセスを許可するかまたはその電話からのアクセスを制限するかのいずれかを行います。

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

ファイアウォール、IPS、および AMP

ファイアウォールをアクセス コントロール リスト（ACL）と組み合わせて使用すると、コラボレーション サーバやゲートウェイを、これらとの通信が許可されていないデバイスから保護できます。Cisco 適応型セキュリティ アプライアンス（ASA）と FirePOWER サービスを導入できます。これにより、ASA ファイアウォール機能、次世代侵入防御システム（NGIPS）、マルウェア対策保護（AMP）の組み合わせが実現します。

Cisco Collaboration システムで使用される UDP ポートと TCP ポートの中には、ファイアウォールで開く必要があるものがあります。使用するポートを決定する際には、次のガイドを参照してください。

- Cisco Unified CM および IM と Presence については、次のリンク先にある『*System Configuration Guide for Cisco Unified Communications Manager*』の最新版を参照してください。
  https://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html
- Cisco Unity Connection については、次のリンク先にある『*Security Guide for Cisco Unity Connection*,』の最新版を参照してください。
  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

- Cisco Expressway については、次のリンク先にある『*Cisco Expressway IP Port Usage for Firewall Traversal Deployment Guide*』の最新版を参照してください。
  https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html
- Cisco Jabber については、次のリンク先にある『*Planning Guide for Cisco Jabber*』の最新版を参照してください。
  https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

QoS

ネットワークにおいてコラボレーション トラフィックが他のトラフィックよりも適切に優先され、ネットワーク フラッド攻撃（DoS 攻撃の一種）から保護されるようにするため、Quality of Service（QoS）を使用できます。QoS 自体はセキュリティ機能ではありませんが、適切に実装することで、適切な QoS レベルが設定されたパケットが優先されるようになります。これは、インターフェイス バッファに圧倒的な負担をかけるためにネットワークにパケットの大量送信を試行するパケット フラッド攻撃に対して有効です。QoS により、マークされていないパケットは削除され、適切にマークされているパケットが許可されるため、バッファが保護されます。

コラボレーション QoS ポリシーの詳細については、帯域幅管理を参照してください。

不正アクセスの防止

Cisco Collaboration ン製品のほとんどでは、プラットフォームが強化されています。たとえば、Cisco Unified CM、IM and Presence Service、および Unity Connection が使用するプラットフォームのロックダウン、root アカウントの無効化、サードパーティ製ソフトウェアのインストール禁止、ホストベースの侵入保護（SELinux）およびホストベースのファイアウォール（iptables）のインストールとデフォルトでの有効化、管理アカウントへの複雑なパスワード ポリシーの適用、セキュア管理インターフェイス（HTTPS、SSH、SFTP）の適用などです。さらに、ユーザをアクセス コントロール グループ、つまり特定のロールに割り当てることができるため、管理者、エンドユーザ、アプリケーション ユーザに対し、それぞれに必要な権限だけを付与できます。すべてのインストール パッケージは署名付きであり、OS とアプリケーションの両方が含まれています。システム監査ロギングを使用できます。このログは、問題発生時の状況を確認する上で重要です。

エッジに導入されるサーバは、インターネットへの露出が高いため、保護する必要があります。Cisco IOS Gateway または Cisco Unified Border Element では、アクセス コントロール リスト（ACL）、IP 信頼リスト、コールしきい値、コール スパイク保護、帯域幅ベースのコール アドミッション制御（CAC）、メディア ポリシング、NBAR ポリシング、音声ポリシーなど、多数のセキュリティ機能を利用できます。Cisco Expressway では、システムを保護するため、Call Processing Language（CPL）ルール、ホストベースのファイアウォール（動的システム ルール、設定不可のアプリケーション ルール、およびユーザが設定可能なルール）、自動侵入保護を設定できます。

エンドポイントの保護は、サーバの保護ほど重要ではないように思われますが、エンドポイントも保護する必要があります。エンド ユーザがエンドポイントにアクセスでき、またエンドポイントはデータ センター内ではロックダウンされていないことから、通常、エンドポイントには簡単にアクセスできます。また、エンドポイントが侵害されると被害が発生する可能性があります。エンドポイントと、エンドポイントが登録されているシステムに関する重要な情報は、電話画面と電話の Web インターフェイスで確認できます。ログをダウンロードできます。Cisco TelePresence エンドポイントなどの一部のエンドポイントには、エンドポイントのコール制御やパケット キャプチャなど、エンドポイント管理者ユーザ向けの高度な機能が多数用意されています。このようなエンドポイントでは、デフォルトのパスワード（空白）をそのままにせずに、強力なパスワードを設定してください。一般に、Web アクセス、Web 管理画面、コン

ソール アクセス、Telnet アクセス、SSH アクセスがエンドポイントで使用可能な場合は、これらを無効にすることが推奨されます。これらの機能は、必要な場合（エンドポイントのトラブルシューティング時など）に限り有効にしてください。管理ステーションや、管理者がアクセスできるステーションへのインターフェイスへのアクセスを制限するため、アクセス コントロール リストを設定してください。エンドポイントで Web アクセスを有効にする場合は、（HTTP ではなく）HTTPS のみを許可します。

Unified CM 管理電話ページの [設定へのアクセス（Settings Access）] パラメータにより、ユーザは [設定（Settings）] ボタンを押すとデバイス設定にアクセスできます。このパラメータが使用可能な場合には、無効にするかまたは [制限（Restricted）] に設定することをお勧めします（管理タスクへのアクセスが無効になります）。エンドポイントと Unified CM 間の信頼関係が失われる可能性のある操作を実行する場合（たとえば Unified CM クラスタ間でエンドポイントを移行し、すべての Unified CM クラスタに 1 つの ITLRecovery 証明書と秘密キーを配布しない場合など）は、[設定へのアクセス（Settings Access ）] を一時的に有効にできます。また、Unified CM 証明書はアップグレード中に変更してはなりませんが、Unified CM のアップグレードのために予防措置として [設定へのアクセス（Settings Access ）] を一時的に有効にすることもできます。エンドポイントと Unified CM 間の信頼関係が失われた場合は、[設定へのアクセス（Settings Access ）] を一時的に有効にすると、ユーザが各自の電話機でメニューに進み、セキュリティ設定をリセットすることで、信頼を回復できます。この操作により、初期信頼リスト（ITL）または証明書信頼リスト（CTL）が削除されます。あるいは、信頼関係が失われた場合には ITL リカバリ キーを使用して回復することもできます（詳細については「CTL および ITL」を参照）。

複雑なパスワードおよび PIN のポリシー（許容可能なログイン失敗回数、ログイン失敗によるアカウントのロックアウト期間、クレデンシャルの最小長など）がデフォルトでまだ適用されていない場合には、すべての Cisco Collaboration 製品で、管理者とユーザに対してこのポリシーが設定されていることを確認してください。

電話料金詐欺行為の削減

Cisco Unified CM

Cisco Unified CM には、電話料金の詐欺行為を防止するためのさまざまなメカニズムがあります。パーティションとコーリング サーチ スペース（CSS）により、コール可能な電話番号、ルート パターン、ディレクトリ URI、および SIP ルート パターン、またはコール発信可能なデバイスや回線へのアクセス制御とセグメンテーションが実現します。ベスト プラクティスは、パーティションとコーリング サーチ スペースに基づき、可能な限り限定的なサービス クラスを適用することです。たとえば、PSTN ゲートウェイと Expressway に接続する SIP トランクの場合は、PSTN ゲートウェイ パーティションへのアクセスを許可しないインバウンド コーリング サーチ スペースを作成します。オフネット間の転送をすべて防止するには、[コール分類（Call Classification）] エンタープライズ パラメータを使用して PSTN ゲートウェイへの SIP トランクを [オフネット（Offnet）] として分類し、[オフネット間転送のブロック（Block OffNet to OffNet Transfer）] CallManager サービス パラメータを [はい（True）] に設定します。時刻のルーティング、強制承認コード（FAC）、[アドホック会議の削除（Drop Ad hoc Conferences）] CallManager サービス パラメータの使用（[会議に OnNet 参加者がいない場合（When No OnNet Parties Remain in the Conference）] に設定）など、その他のメカニズムも使用できます。自動登録が有効な場合は、制限付きコーリング サーチ スペースを使用してデバイス プールを作成します。また、システム コール詳細レコード（CDR）をプロアクティブにモニタリングすることが推奨されます。

Cisco Unity Connection

不正ユーザが Cisco Unity Connection の転送機能を使用して不正なコールを発信する可能性があります。Unity Connection では、主に 2 通りの方法で電話料金の詐欺行為を防止します。

- Unity Connection：規制テーブルにより、着信転送、メッセージ通知、および Unity Connection のその他の機能に使用できる電話番号が制御されます。各サービス クラスにいくつかの規制テーブルが関連付けられており、必要に応じて規制テーブルを追加することもできます。詳細と例については、「ボイス メッセージング」の章を参照してください。
- Unified CM：コーリング サーチ スペースおよびコーリング サーチ スペースの再ルーティングのため、必要なパーティションのみを含めます。「ボイスメールのサービス クラス」の C：表 2-21 を参照してください。

詳細については、次のリンク先にある『*Unified Messaging Guide for Cisco Unity Connection*』の最新版を参照してください。

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

次のリンク先にある『*Troubleshoot Toll Fraud via Unity Connection*』も参照してください。

https://www.cisco.com/c/en/us/support/docs/unified-communications/unity-connection/119337-technote-cuc-00.html

Cisco Expressway

Expressway の Business-to-Business 導入では、Call Processing Language（CPL）ルールを使用してデフォルト ゾーンからのコールを許可または拒否します。たとえば、（PSTN への不正コールを防止するため）プレフィックスとして 9 を使用する Business-to-Business（B2B）コールをすべて拒否する場合には、C：表 7-3 に示す設定を使用して CPL ルールを作成できます。

C：表 7-3　Business-to-Business（B2B）コールの CPL 設定

ソース タイプ	ゾーン
発信側ゾーン	DefaultZone
宛先パターン	9.*
操作	却下

Cisco IOS Gateway と Cisco Unified Border Element

テレフォニー サービス妨害（TDoS）攻撃緩和機能により、Cisco IOS Gateway と Cisco Unified Border Element が、信頼されない IP アドレスからの Session Initiation Protocol（SIP）要求に応答することが防止されます。これにより、電話料金詐欺行為を防止し、パフォーマンスが向上します。SIP スタックにより、着信 SIP 要求の送信元 IP アドレスが認証され、送信元 IP アドレスが信頼できる IP アドレス リストの IP アドレスに一致しない場合には応答がブロックされます。ダイヤルピア セッション ターゲットまたは音声クラス サーバ グループで設定されている IP アドレスは、信頼される IP アドレスのリストに自動的に追加されます。信頼される IP アドレスを追加するには、**ip address trusted list** コマンドを使用します。

この TDoS 機能を設定するには、次のコマンドを使用します。

```
voice service voip
  ip address trusted authenticate
```

Cisco Unified Border Element がレジストラ サーバとして導入されていない場合は、不要なリソースの消費を防止するためレジストラ サービスを無効にします。

証明書の管理

証明書は、Cisco Collaboration 導入において重要です。証明書により、ネットワーク上の個人ユーザ、コンピュータ、その他のサービスを認証できます。また、セキュアな接続を確立する際には証明書が必要です。適切な証明書管理を実施することで、適切なレベルの保護を実現し、かつ複雑さを軽減できます。

この項では最初に Public Key Infrastructure（PKI）を簡単に説明します。続いて一般的なガイダンスを示します。最後に、さまざまな Cisco Collaboration 製品のアーキテクチャについて詳しく説明します。

PKI の概要

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

公開 / 秘密キー ペア

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

証明書

デジタル証明書は、ネットワーク上の個人ユーザ、コンピュータ、その他のサービスのアイデンティティを証明する電子クレデンシャルです。これは公開キーのラッパーです。公開キーの所有者に関する情報が含まれています。たとえば、もう一方の側を認証するため TLS ハンドシェイクで使用され、またファイルのデジタル署名に使用されます。Cisco Collaboration 製品とともに導入される証明書は、X.509 標準に基づいています。証明書に含まれている情報には、次のものがあります。

- 公開キー
- 一般名（CN）
- 組織名 (O)
- 発行元名
- 有効期間（それ以前でもそれ以後でもない）
- 拡張（オプション）：サブジェクト代替名（SAN）など

証明書は、自己署名するか、認証局（CA）の署名を受けることができます。

TLS ハンドシェイクでの証明書の検証

クライアントがサーバとの TLS 接続を開始すると、TLS ハンドシェイク中にサーバからその証明書が送信されます。これにより、クライアントはサーバを認証できます。たとえば、管理者またはエンドユーザが Unified CM のページに接続する場合や、Jabber クライアントが起動し Unified CM UDS サーバ、IM and Presence サーバ、Unity Connection サーバに接続する場合などに実行されます。

場合によっては、サーバがクライアントを認証し、クライアントに対して証明書の送信を要求することもあります。これは相互認証（相互 TLS（MTLS））であり、暗号化モード（メディアおよびシグナリング暗号化で設定）での Unified CM と Cisco エンドポイント間、2 つの Unified CM クラスタを接続する SIP トランク、または Unified CM を Unity Connection、Cisco IOS Gateway、または Expressway（TLS 検証が Expressway で設定されている場合）に接続する SIP トランクで使用されます。

証明書を受信すると、検証で次の項目がチェックされます。

- ID — 証明書が発行される対象や ID は、セッションのイニシエータが意図した接続先の ID に一致しなければなりません。ホスト名（FQDN）は、コモン ネーム（CN）またはサブジェクト代替名（SAN）拡張と突き合わせてチェックされます。
- 有効期間 — 現在の時刻と日付が証明書の有効範囲内になければなりません。
- 証明書の失効状況
- 信頼性 — 証明書が信頼できるものでなければなりません。署名（発行）側を信頼できる場合、証明書は信頼できるものであると見なされます。一般的に、署名側による信頼は、署名側の証明書を信頼された証明書ストア（信頼ストア）にインポートすることにより確立されます。詳細については、自己署名証明書の代わりの CA 署名付き証明書を参照してください。

証明書に関する一般的なガイダンス

一部のサーバ（Cisco Unified CM や IM and Presence Service など）は、システム サービスに応じて異なる証明書を使用できます。Cisco Expressway などのサーバは、サーバが提供するサービスで 1 つの証明書だけを使用します。C：表 7-4 に、このプリファード アーキテクチャのサーバ証明書を示します。次の項で説明するように、ECDSA 証明書についてはこのドキュメントでは扱いません。

C：表 7-4　Cisco Collaboration 向けプリファード アーキテクチャのサーバ証明書

サービス	証明書	説明
Cisco Unified CM	tomcat	セキュアな Web 接続のために使用されます。LDAP、ILS、LBM などのサービスにも使用されます。
Cisco Unified CM	CallManager	CallManager サービスによるセキュア シグナリングと、TFTP 設定ファイルの署名に使用されます。
Cisco Unified CM	CAPF	認証局プロキシ機能（CAPF）サービスへの接続時にエンドポイントに必要です。
Cisco Unified CM	TVS	Trust Validation Service（TVS）への接続時に必要です。
Cisco Unified CM	ITLRecovery	ITL とトークンレス型 CTL ファイルの署名に使用されます。
Cisco Unified CM	ipsec	IPSec 接続に使用されます。IPSec を有効にできますが、これについてはこのドキュメントでは扱いません。IPSec 証明書は、ディザスタ リカバリ システムでも使用されます。
Cisco Unified CM	authz	OAuth に使用されます。
IM and Presence Service	tomcat	SIP クライアント（Unified CM）、Web サービス、SOAP、LDAP に使用されます。
IM and Presence Service	cup	SIP プロキシ、プレゼンス エンジン、SIP フェデレーションに使用されます。
IM and Presence Service	cup-xmpp	セキュア XMPP（IM）に使用されます。
IM and Presence Service	cup-xmpp-s2s	セキュア XMPP フェデレーションに使用されます。
IM and Presence Service	ipsec	IPSec に使用されます。
Cisco Unity Connection	tomcat	Unity Connection の Web サービス証明書。ボイス メール ポートへのメディアおよびシグナリング暗号化に使用されます。
Cisco Unity Connection	ipsec	IPSec に使用されます。

C：表 7-4　Cisco Collaboration 向けプリファード アーキテクチャのサーバ証明書（続き）

サービス	証明書	説明
Cisco Expressway-C	サーバ	Expressway-C とのすべてのセキュアな接続に使用されます。
Cisco Expressway-E	サーバ	Expressway-E とのすべてのセキュアな接続に使用されます。
Cisco Meeting Server	データベース クライアント	データベースがなく Call Bridge サービスを使用する Cisco Meeting Server が、データベースがある Cisco Meeting Server ノードと安全に接続するために使用されます。
Cisco Meeting Server	Web 管理画面、Call Bridge、XMPP、Web ブリッジ、およびデータベース サーバに使用される共有証明書	わかりやすくするため、データベース クライアントを除き、すべての Cisco Meeting Server ノードとサービスに同じ証明書を使用します。
Cisco Meeting Management	Server	Web 接続とコールブリッジ接続の場合
Survivable Remote Site Telephony（SRST）、Cisco IOS Gateway、Cisco Unified Border Element	Cisco IOS 証明書	SRST の場合、各エンドポイントの設定ファイルに SRST 証明書が含まれています。
Cisco Prime Collaboration Deployment	tomcat	Web サービスに使用されます。
Cisco Prime Collaboration Provisioning	プロビジョニング	Web アクセスのプロビジョニングに使用されます。

その他の ECDSA 証明書もありますが、この章の「RSA および ECDSA」で説明したように、この章の導入ガイダンスでは使用されないため、これらの証明書は C：表 7-4 には含まれていません。

一般に、デフォルトでは Cisco Collaboration サーバは自己署名証明書とともにインストールされます。ただし、証明書がデフォルトでインストールされない Cisco Meeting Server は例外です。

ITLRecovery 証明書以外の Cisco Unified CM の自己署名証明書の有効期間は 5 年間です。ITLRecovery 証明書の有効期間は 20 年です。証明書がシステム全体のトラスト アンカーとして使用される場合は、証明書の有効期間はさらに長くなります。

RSA および ECDSA

Cisco Collaboration 製品の証明書は通常、公開キー / 秘密キーとデジタル署名については RSA（Rivest, Shamir, and Adelman）に基づいています。一部の製品では楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）（ECDSA）証明書がサポートされていますが、簡素化するために、RSA ベースの証明書を使用することが一般に推奨されます。このドキュメントでは RSA ベースの証明書の使用について説明します。

エンドポイントについて、RSA ベースのローカルで有効な証明書 (LSC) を使用することを推奨します。Unified CM SIP TLS では、ECDSA と RSA は常に有効ですが、デフォルトでは RSA が ECDSA よりも優先されるため、RSA 証明書がネゴシエートされます。これが推奨されている設定です。HTTPS の場合、Unified CM、IM and Presence Service、Unity Connection では ECDSA はデフォルトで無効になっています。有効にするには [HTTPS 暗号方式（HTTPS Ciphers）] エンタープライズ パラメータを変更します。ただし、デフォルト設定（ECDSA 無効）を使用することが推奨されます。

注　ECDHE に基づく暗号化アルゴリズム スイートでは、ECDSA に基づく証明書は不要です。このようなスイートは RSA に基づく証明書とネゴシエートできます。

自己署名証明書の代わりの CA 署名付き証明書

デフォルトでは、ここで説明するシスコ製品のサーバのインストール時には、自己署名証明書がインストールされます（デフォルトで証明書がインストールされない Cisco Meeting Server を除く）。自己署名証明書に基づいてサービスへの信頼を確立するには、サービス（クライアント）へのセキュアな接続を必要とするすべてのエンティティの信頼された証明書ストア（または信頼ストア）に、サーバの自己署名証明書をインポートする必要があります。このようにしないと、サーバが接続を開始するときに（Unified CM SIP トランクへの接続など）、接続が失敗します。Jabber と Web ブラウザでは、ユーザに対し警告メッセージが表示されます。ユーザが証明書を受け入れると、通常その証明書は信頼された証明書ストアに追加されます。クライアントの起動中に多くの証明書を受け入れるよう何度もプロンプトが出されることは最良のユーザ エクスペリエンスとは言えないため、これは避けるべきです。より重要なこととして、ほとんどのユーザは、提示された証明書のフィンガープリントを確認してその証明書が正しいものであるかどうかを実際には検証せずに、どの証明書もそのまま受け入れてしまいます。これでは、セキュアなセッションを確立するための証明書ベースの認証のセキュリティの概念が成り立たなくなってしまいます。

自己署名証明書のインポートは、通信ピアが少ない場合は対処可能ですが、通信ピアの数が多い場合には実用的ではなくなります。これが、ほとんどのデフォルトの自己署名証明書を CA 署名付き証明書に置き換えることが推奨される主な理由です。これにより証明書の管理が簡素化されます。CA 署名付き証明書の場合、各サーバ証明書をクライアントの信頼ストアにインポートする必要はありません。ルート CA 証明書をクライアントの信頼ストアにインポートするだけで十分です。サーバ側では一般に、ルート CA 証明書をサーバの信頼ストアにインポートする必要もあります。また中間 CA を使用する場合は、証明書チェーンのすべての証明書をサーバの信頼ストアにインポートする必要もあります。CA 署名付き証明書を使用することで、署名側 CA のルート証明書がすべてのクライアントの信頼された証明書ストアにすでに追加されている限り、すべてのクライアントまたはサーバの信頼された証明書ストアを更新しなくても、新たなサービス証明書を発行できます。CA 署名付き証明書は、マルチサーバ証明書を使用する場合の要件でもあります。

CA 署名付き証明書を利用するメリットの例としては、自己署名証明書を Jabber クライアントで使用した場合は、Unified CM の tomcat 証明書 証明書（UDS および TFTP 設定ファイルのダウンロード用）、IM and Presence の tomcat および cup-xmpp 証明書（ログインおよびセキュアチャット用）、および Unity Connection の tomcat 証明書（ビジュアル ボイス メール用）は、Jabber を実行する各クライアントの信頼ストアにインポートする必要があることがあります。CA 署名付き証明書でインポートする必要があるのは、署名 CA のルート証明書のみです。

一般に、tomcat 証明書で CA 署名付き証明書を使用する場合が最も有用性が高くなります。これは、tomcat 証明書は広く使用されており、またユーザに表示される証明書であるためです。CallManager 証明書に CA 署名付き証明書を使用する場合も有用性が高くなります。これは、マルチサーバ証明書を使用でき（詳細については「マルチサーバ証明書」を参照）、SIP トランク経由で Unified CM サブスクライバに接続するすべてのエンティティの CallManager 証明書をインポートすることが回避されるためです。

ただし、1 つのエンタープライズ CA ですべての証明書を署名する必要はありません。一部の証明書は内部操作専用であり、これらの証明書を必要とするエンティティに対し、ユーザによる操作なしで提供されます。たとえば、信頼検証サービス（TVS）証明書は初期信頼リスト（ITL）ファイルに含まれており、エンドポイントの起動、再起動、またはリセット時にこの ITL ファイルがエンドポイントにより自動的にダウンロードされます。同様に、ITLRecovery 証明書は証明書信頼リスト（CTL）と初期信頼リスト（ITL）に含まれています。したがって、外部 CA でこれらの証明書に署名するメリットはありません。また、外部 CA で CAPF 証明書

に署名する実質的なメリットもありません。認証局プロキシ機能（CAPF）証明書またはエンドポイントのローカルで有効な証明書（LSC）の失効はサポートされていません。また、電話の VPN または 802.1x を設定するときには、ルート CA 証明書を ASA 信頼ストアにインポートするだけでは十分ではありません。TLS ハンドシェイク中にエンドポイントから証明書チェーンが送信されないため（したがって CAPF 証明書が送信されないため）、CAPF 証明書をインポートする必要があります。

C：表 7-5 に、CA による署名が推奨される証明書を示します。

C：表 7-5　　CA による署名が推奨される証明書

製品	証明書	注記
Cisco Unified CM、IM および Presence Service	tomcat	管理者やユーザが Web インターフェイスにアクセスする場合や、Jabber が UDS にアクセスしてログインする場合など、さまざまな用途に使用されます。
Cisco Unified CM	CallManager	SIP トランクなどさまざまな用途に使用されます。
Cisco Unified CM	ipsec	IPsec を使用する場合にのみ使用されます。
IM and Presence Service	xmpp	
IM and Presence Service	xmpp-s2s	
Cisco Unity Connection	tomcat	管理者やユーザが Web インターフェイスにアクセスする場合や、Jabber がビジュアル ボイス メールにアクセスする場合など、さまざまな用途に使用されます。
Cisco Expressway-C	サーバ	
Cisco Expressway-E	サーバ	パブリック CA を使用します。
Survivable Remote Site Telephony（SRST）と Cisco IOS Gateway	SRST と Cisco IOS ゲートウェイ	
Cisco Unified Border Element	Cisco IOS	一般にエンタープライズ CA を使用します。SIP サービス プロバイダーで暗号化がサポートされている場合は、パブリック CA を使用します。
Cisco Meeting Server	サーバ	すべての Cisco Meeting Server サービス用の共有証明書
Cisco Meeting Server	データベース クライアント	
Cisco Meeting Management	Server	
Cisco TelePresence Management Suite（TMS）	サーバ	
Cisco Prime Collaboration Deployment	tomcat	
Cisco Prime Collaboration Provisioning	プロビジョニング	

マルチサーバ証明書

証明書の管理をさらに簡素化するには、マルチサーバ証明書を使用できます。ノードごとに証明書を作成する代わりに、1 つの CA 署名付き証明書をクラスタ内のすべてのノードに使用できます。1 つの対応する秘密キーがすべてのノードで使用され、すべてのノードに自動的に反映されます。マルチサーバ証明書が使用可能な場合は常にマルチサーバ証明書を使用すること

が推奨されます。C：表 7-6 でこれを説明します。

C：表 7-6　マルチサーバ証明書のサポート

製品	証明書	注記
Unified CM and IM and Presence Service	tomcat	クラスタ内のすべての Unified CM ノードと IM and Presence ノードに対する 1 つの tomcat 証明書。証明書署名要求（CSR）を生成し、CA 発行の証明書を Unified CM パブリッシャ ノードにアップロードします。
Unified CM	CallManager	
IM and Presence Service	xmpp	
IM and Presence Service	xmpp-s2s	
Unity Connection	tomcat	

Cisco Meeting Server では、（データベース クライアント用の証明書の他に）Cisco Meeting Server クラスタ内のすべてのノードで共有される 1 つの証明書と 1 つの秘密キーを発行することもできます。ただし、秘密キーは自動的には反映されません。各 Cisco Meeting Server ノードに手動でインポートする必要があります。

注　この章で説明する Cisco Meeting Server 以外の Cisco Collaboration 製品では、ワイルドカード証明書はサポートされていません。Cisco Meeting Server では、（ワイルドカード以外の）標準証明書を発行し、その証明書をすべての Cisco Meeting Server サービスとノードに使用することが推奨されます（データベース クライアントの 2 番目の証明書を生成する必要があります）。

パブリック CA とプライベート CA

Expressway-E 証明書にはパブリック CA を使用するという要件の他に、このドキュメントで説明する Cisco Collaboration 製品のさまざまな証明書の署名に、パブリック CA またはエンタープライズ CA（プライベートまたは内部 CA）のいずれかを使用できます。パブリック CA を利用するメリットには、一部のクライアントとサーバではすでにデフォルトで主要なパブリック CA が信頼されているため、これらのデバイスとパブリック CA 間で信頼を確立する（CA 証明書をクライアントの信頼ストアにインポートする）必要がないことなどがあります。パブリック CA を使用する場合、IT 部門が内部 CA サーバをインストールして保守する必要がありません。ただし主要な短所として、証明書の発行にかかるコストと、一部のパブリック CA の制限事項があります。

CA での署名が推奨される証明書にはエンタープライズ CA を使用することが推奨され、このドキュメントでもこの点について説明しています。ただし、パブリック CA により署名する必要がある Expressway-E 証明書と、SIP サービス プロバイダーで暗号化がサポートされている場合の Cisco Unified Border Element 証明書は除きます。

Cisco Unified CM および IM と Presence

ここでは、Cisco Unified CM および IM と Presence の証明書の管理について説明します。

Unified CM 混合モード

メディアおよびシグナリング暗号化のための Unified CM 混合モード で後述するように、統一された CM 混合モードにより、電話機と TelePresence のエンドポイントでメディアおよびシグナリング暗号化が有効になります。トークンレス方式で混合モードを有効にすることが推奨されており、このドキュメントで説明しています。

CTL および ITL

証明書信頼リスト（CTL）と初期信頼リスト（ITL）は、Unified CM 証明書が含まれているファイルです。これらのファイルはシスコ エンドポイントによりダウンロードされます。これらの信頼リストにより、エンドポイントは Unified CM サービスへの信頼を確立するための最小限の Unified CM 証明書を取得します。Unified CM クラスタのモード（非セキュア モードまたは混合モード）に関係なく、ITL ファイルは常に Unified CM クラスタに存在しています。CTL ファイルは、Unified CM が混合モードの場合にのみ存在および適用されます。

CTL ファイルと ITL ファイルは、System Administrator Security Token（SAST、C：表 7-7 を参照）を使用して署名され、一連のレコードが含まれています。各レコードには、証明書、証明書のロールまたは機能、エンドポイントによる検索を容易にするために事前に抽出された証明書のフィールドが含まれています。C：表 7-7 に、証明書のロールを示します。

C：表 7-7　CTL ファイルと ITL ファイルでの証明書のロール

証明書のロール	証明書	説明
TFTP	CallManager	Unified CM TFTP サーバを認証します。たとえば、TFTP 設定ファイルの署名の検証に使用されます。この証明書ロールのレコードは、Unified CM が混合モードではない場合に ITL ファイルに含まれています。
CCM+TFTP	CallManager	暗号化シグナリングを使用して CallManager サービスを認証し、TFTP 設定ファイルの署名の検証時に Unified CM TFTP サーバを認証します。この証明書ロールのレコードは、Unified CM が混合モードである場合に ITL ファイルと CTL ファイルに含まれています。
System Administrator Security Token（SAST）	トークンレス型 CTL： パブリッシャの ITLRecovery 証明書および CallManager 証明書 ITL： TFTP サーバの ITLRecovery 証明書および CallManager 証明書	SAST（CTL、ITL、または TFTP 設定ファイルを署名するエンティティ）を認証します。 このタイプのレコードは ITL ファイルと CTL ファイルに含まれています。 ITL ファイルとトークンレス CTL ファイルは、ITL リカバリ キーを使用して署名されます。TFTP 設定ファイルは、TFTP サーバの CallManager 秘密キーを使用して署名されます。
Certificate Authority Proxy Function（CAPF）	CAPF	CAPF とのセキュア通信中に CAPF サービスを認証します。この証明書ロールのレコードは、CAPF サービスが Unified CM パブリッシャで有効化されている場合に、ITL ファイルと CTL ファイルに含まれています。
信頼検証サービス（TVS）	TVS	TVS への接続時に TVS サービスを認証します。ITL ファイルにのみ含まれています。

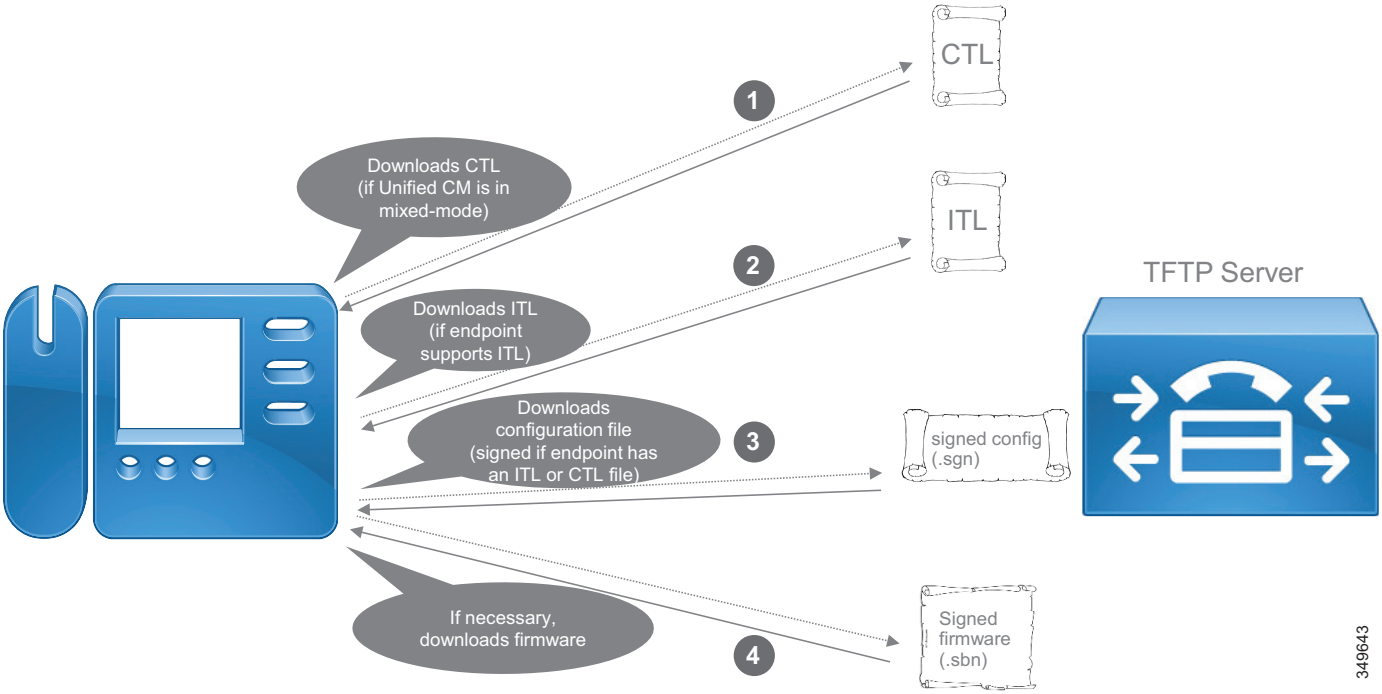
ITL は ITLRecovery 秘密キーを使用して署名されます。TFTP サービスを実行している各 Unified CM ノードには独自の ITL ファイルがあり、この ITL ファイルがエンドポイントに提供されます。

CTL ファイルは、System Administrator Security Token（SAST）の秘密キーを使用して署名されます。トークンレス CTL の場合、SAST は ITLRecovery 秘密キーです。Unified CM クラスタ全体で共有される CTL ファイルは 1 つだけです。

Unified CM が混合モードの場合、エンドポイントの起動またはリセット時に、エンドポイントの設定ファイルをダウンロードする前に証明書信頼リスト（CTL）が TFTP サーバからダウンロードされます。初期信頼リスト（ITL）がエンドポイントでサポートされている場合は、その後 TFTP サーバの ITL がダウンロードされます。ITL は Jabber ではサポートされていませんが、このプリファード アーキテクチャのその他のエンドポイントではサポートされています。エンドポイントを新規に導入し、エンドポイントが初めて Unified CM へ接続するときには、既存の CTL ファイルまたは ITL ファイルがないので、CTL または ITL 署名の検証に使用できる一連の証明書がありません。この場合、エンドポイントは 1 回限りで無条件に CTL/ITL ファイルを受け入れ、それらのファイルに含まれている証明書を保存します。エンドポイントに一連の信頼できる証明書が保存されたら、それ以降の CTL ファイルおよび ITL ファイルの署名の検証にはそれらの証明書を使用できます。

エンドポイントで ITL がサポートされている場合、または統一された CM が混合モードである（CTL ファイルがエンドポイントによりダウンロードされる）場合、エンドポイントは ITL/CTL ファイルに含まれている ITLRecovery 証明書を処理し、統一された CM TFTP サーバの CallManager 秘密キーを使用して署名されている設定ファイルを要求します。それ以外の場合（Jabber や、Unified CM が混合モードではない場合など）は、未署名の設定ファイルを要求します。エンドポイントは、設定ファイルのダウンロード後に、設定ファイルに正しいファームウェアが含まれていることを検証します。含まれていない場合は、該当するファームウェアをダウンロードし、そのファームウェアの署名を検証して、ファームウェアが改ざんされていないことを確認します。C：図 7-3 に、エンドポイントの起動中にエンドポイントによりダウンロードされるファイルの要約を示します。

C：図 7-3　　起動中にエンドポイントがダウンロードするファイル



エンドポイント証明書

エンドポイント証明書は主に、セキュア モードのエンドポイント、つまりエンドポイントでのメディアおよびシグナリング暗号化の実行時に使用されます。この証明書は、暗号化 TFTP 設定ファイル、802.1x 認証、電話の VPN、またはエンドポイントの Web サーバに HTTPS を介してアクセスする場合などにも使用できます。

シスコのエンドポイントの証明書には 2 種類あります。

- 製造元でインストールされる証明書（MIC）
- ローカルで有効な証明書（LSC）

MIC は、製造工程でエンドポイントに事前にインストールされており、Cisco Manufacturing CA により署名されています。その有効期間は 10 年であり、証明書失効はサポートされていません。MIC はメディアおよびシグナリング暗号化に使用できますが、MIC の代わりに LSC を生成することが推奨されます（これについては後述します）。Cisco IP Phone 7800 シリーズおよび 8800 シリーズ（Cisco Unified IP Conference Phone 8831 を含む）、Cisco TelePresence IX5000 シリーズのエンドポイント（Cisco MX、SX、Webex DX、および Webex Room シリーズ）、および Cisco TelePresence IX5000 シリーズエンドポイントにはすべて MIC があります。Jabber には MIC がありません。

LSC は、独自の展開にインストールする証明書です。統一された CM パブリッシャノードで実行される認証局プロキシ機能（CAPF）サービス、あるいは外部 CA によって署名されます。このプリファード アーキテクチャのすべてのシスコ エンドポイントでは LSC がサポートされます。LSC の有効期間は 5 年間であり、[Unified CM の管理（Unified CM Administration）] ページを使用するか、または有効期限に近くなると電子メールの通知が送信されるため、LSC の有効性を簡単に確認できます。このガイドに記載されているすべてのエンドポイントでは、LSC は SHA2 に基づいています。また、Jabber エンドポイントと Cisco IP Phone 7800 シリーズおよび 8800 シリーズのエンドポイントでは、2048 ビットまたは最大 4096 ビットのキー長に基づくことができます。LSC のインストールが完了すると、MIC は使用されなくなります。

MIC は、電話機がシスコの純正電話機であることを証明する目的で使用され、Cisco Manufacturing CA による署名を受けています。MIC を使用するメリットの 1 つに、Unified CM クラスタで設定されている正当な MAC アドレスが、不正なクライアントによりスプーフィングされることを防止することがあります。ただし MIC では、エンドポイントが Unified CM クラスタの一部であることは証明されません。したがって、802.1x または VPN には MIC に基づく認証を使用しないでください。このような認証を使用すると、あらゆるシスコ エンドポイント（組織外のエンドポイントを含む）が認証可能になります。通常、最初の CAPF 登録時に MIC を使用してエンドポイントの最初の LSC を生成することが推奨されます。エンドポイントで LSC が生成された後は、認証には、常に MIC ではなく LSC を使用することが推奨されます。MIC がないか、または MIC を公開するエンドポイント（たとえば、Jabber など）では、CAPF 登録認証は認証文字列またはヌル ストリングに基づいて実行できます。認証文字列に基づく認証は安全ですが、ユーザがエンドポイントで文字列を手動で入力する必要があります。この操作が現実的ではない場合は、ヌル ストリングに基づく認証を選択できますが、この認証では、最初の CAPF 登録時にすべてのエンドポイント認証が実質的に迂回されます。Jabber で LSC が生成されたら、その他のエンドポイントと同様に、LSC の更新に基づく認証が推奨されます。

電話機で LSC を発行するには、次の 3 つの方法があります。

- 最初の方法は、Cisco Unified CM の CAPF サービスに lSC に署名させる方法です。これが最も簡単な方法です。
- 2 番目の方法は、CAPF 登録を開始する際に、CAPF サービスを介して電話機に LSC を発行するオンライン外部 CA (Microsoft CA) を使用する方法です。この方法の主な利点は、LSC が独自の CA によって署名される点です。
- 3 番目の方法は、2 番目の方法に類似した方法です。LSC は外部 CA によって発行されますが、オフラインの方法では、エンドポイントの証明書署名要求 (CSR) ファイルを統一された CM から手動でエクスポートし、外部 CA によって署名してから、統一された CM にインポートし直す必要があります。この方法は手動の手順であるため、この推奨アーキテクチャでは説明されていません。

注　ワイヤレス接続を使用するエンドポイントと Jabber エンドポイントでは、CAPF が発行する LSC は Unified CM でのみ使用され、802.1X または EAP に拡張することはできません。

Jabber に関する考慮事項

暗号化されたメディアとシグナリングを実行するために、Jabber に証明書をインストールする必要はありません。Cisco Expressway のセクションで説明したように、Jabber が Mobile & Remote Access (MRA) 経由で接続している場合、他のエンドポイントと同様に、エンドポイント証明書をインストールする必要はありません。Jabber がエンタープライズ ネットワーク内にある場合、この推奨アーキテクチャでは、OAuth と SIP OAuth モードが有効であるため、LSC のインストールは必要ありません。

Survivable Remote Site Telephony（SRST）

セキュア SRST がサポートされています。Unified CM サーバが到達不能になると、エンドポイントはローカル SRST ルータに登録されます。Unified CM で暗号化モードで設定されているエンドポイントは、SRST ルータへの登録時にも、メディアとシグナリングが暗号化されたままになります。

セキュア SRST のプロビジョニング方法をまとめると、次のようになります。

1。 最初に、SRST ルータの証明書を生成します。ほとんどの証明書では、CA 署名付き証明書を使用することで証明書の管理が容易になります。

2。 [セキュア SRST（Is SRST Secure）] 設定を有効にして（チェックボックスがオン）設定されている Unified CM は、SRST ルータで実行されている証明書サーバの SRST 証明書を要求し、SRST を使用して設定されているエンドポイントの設定ファイルに SRST 証明書を挿入します。

3。 エンドポイント LSC に署名したエンティティに対応する信頼証明書を SRST ルータに手動でインポートします。CAPF を使用して LSC を発行する場合、これが CAPF 証明書となります。外部 CA を使用して lSC を発行する場合、これが CA 証明書 (または信頼チェーン証明書) となります。

4。 WAN がダウンするか、または Unified CM サーバが到達不能になると、エンドポイントは SRST と安全に通信します。エンドポイントは TFTP 設定ファイル内の SRST 証明書を使用して SRST を認証し、SRST は前の手順でインポートした LSC を発行したエンティティに対応する証明書（CAPF または外部 CA 証明書）を認証します。

Cisco Unity Connection

このドキュメントでは、次世代暗号化（NGE）を使用した Cisco Unity Connection のメディアおよびシグナリング暗号化について説明します。この構成では、Unity Connection のルート証明書および SIP 証明書の代わりに、tomcat 証明書が使用されます。Unified CM と Unity Connection の間で SIP トランクが設定されています。この SIP トランクはセキュアであり、Unified CM と Unity Connection は相互に認証します。Unified CM の認証には CallManager 証明書が使用され、Unity Connection の認証には tomcat 証明書が使用されます。前述したように、Unity CM と Unity Connection の間での証明書交換が不要になるように、エンタープライズ CA でこれらの証明書を署名することが推奨されます。ルート CA 証明書を Unified CM CallManager 信頼ストアと Unity Connection tomcat 信頼ストアにインポートする必要があります。また Unity Connection は、Unified CM TFTP サーバから tomcat 信頼ストアに Unified CM CallManager 証明書を自動的にダウンロードします。

Cisco Expressway

Cisco Expressway ソフトウェアの新規インストールには、一時的に信頼された CA と、その一時 CA が発行するサーバ証明書が付属しています。サーバ証明書を CA 署名付き証明書に置き換え、信頼する機関のルート CA 証明書または証明書チェーンをインストールすることが推奨されます。

Expressway-C 証明書は、エンタープライズ CA またはパブリック CA により署名できます。前述したように、このドキュメントではエンタープライズ CA が使用されていることを前提としています。Expressway-E では、サーバ証明書をパブリック CA で署名するという要件があります。この要件には次の 2 つの理由があります。

- モバイルおよびリモート アクセス（MRA）可能なハードウェア エンドポイントには、エンドポイントのファームウェアに含まれており信頼されるパブリック ルート CA 証明書が 100 以上含まれています。ルート CA 証明書を追加するメカニズムはないので、これらのパブリック CA のいずれかで Expressway-E 証明書を署名する必要があります。サポートされているパブリック CA の一覧は、https://www.cisco.com のエンドポイント ドキュメント（https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html など）に記載されています。
- Cisco Expressway-E は、エンドポイント、その他の組織、さらには Cisco Collaboration Cloud とも通信するインターネットに公開されているコンポーネントです。このため、最小限の労力で最大限のセキュリティと信頼性を実現するには、パブリック CA の信頼性の基盤となる Public Key Infrastructure（PKI）が必要です。

エンドポイントがモバイルおよびリモート アクセス（MRA）経由で企業に接続している場合、CAPF 登録はサポートされません。つまり、エンドポイントが MRA 経由で接続されている場合には LSC をインストールできません。ただし、エンドポイントに MIC がない場合でも、これによってエンドポイントがエンドツーエンドの暗号化（すべてのコール レッグの暗号化）を使用できなくなることはありません。実際には、MRA 経由での接続時には MIC と LSC は不要であるかまたは使用されません。

注　（**デバイス セキュリティ モード** が **暗号化**に設定されている電話セキュリティ プロファイルを使用して）エンドポイントが暗号化モードで設定されており、MIC または LSC がエンドポイントにない場合、エンドポイントは MRA 経由で接続する際に、継続して正常に接続されます。ただし、エンドポイントが企業（オンプレミス）に直接接続する場合、エンドポイントには証明書が必要です。証明書がないとエンドポイントは登録されません。これは、OAuth トークンを使用する Jabber には適用されません。

MRA では CAPF 登録がサポートされていないため、MRA エンドポイントでの TFTP 設定ファイルの暗号化に関する考慮事項があります。詳細については、「TFTP 設定ファイルの暗号化」を参照してください。

「コラボレーション エッジ」の章でも、Cisco Expressway に関するセキュリティ上の考慮事項について説明しています。詳細についてはこの章を参照してください。

Cisco Meeting Server

デフォルトでは、Cisco Meeting Server には証明書がありません。Cisco Meeting Server では、証明書に関して複数のオプションがサポートされていますが、このドキュメントでは、データベース クライアント用に 1 つの CA 署名付き証明書を発行し、その他のサービス用にもう 1 つの CA 署名付き証明書を発行し、Cisco Meeting Server クラスタ内のすべてのノードにこれらの証明書とそれに対応する秘密キーをコピーすることを推奨しています。

Cisco Meeting Management

Cisco Meeting Management は、証明書を使用してブラウザとコールブリッジに対して自己識別します。セットアップ中に、Meeting Management が自己署名証明書を生成します。これを CA 署名付き証明書に置き換える必要があります。

Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment は Unified CM と同じプラットフォームを使用しますが、証明書管理用のグラフィカル ユーザ インターフェイスがありません。HTTPS の場合 ECDSA が無効になるため、tomcat 証明書だけを CA で署名する必要があります。プラットフォームの CLI（コマンド ライン インターフェイス）を使用して、証明書署名要求（CSR）を生成し、CA 署名付き tomcat 証明書をアップロードします。

Cisco Prime Collaboration Deployment は、HTTPS に基づいて SOAP サービスを使用して Cisco Collaboration 製品に接続し、Cisco Prime Collaboration Deployment タスクの実行中にデータをインポートまたはエクスポートします。

Cisco Prime Collaboration Provisioning

Cisco Prime Collaboration プロビジョニングには、デフォルトで署名付き証明書があります。この証明書を、エンタープライズ CA によって署名された証明書に置き換えることが推奨されます。Cisco Prime Collaboration プロビジョニングでは証明書チェーンはサポートされていません。プロビジョニングを実行するため、Cisco Prime Collaboration プロビジョニングは暗号化接続を介してさまざまな Cisco Collaboration サーバに接続します。

暗号化

内部ネットワークを超えて拡張するするサービスが増加し、内部ネットワークが内部攻撃の対象となる可能性があることから、暗号化と認証の重要性が増しています。

暗号化により、盗聴、改ざん、セッション リプレイなどの攻撃から保護されます。不正ユーザは、トラフィックをキャプチャできても、暗号キーなしでは通信内容を復号化または変更することはできません。暗号化では、暗号化通信の設定時にデジタル証明書による認証も実現できます。

通常、TLS の概要のセクション項で説明したように、さまざまなサーバ接続で暗号化を有効にすることをお勧めします。Jabber では、暗号化メディアとシグナリングを有効にすることを推奨します。Jabber は OAuth トークンを使用して暗号化メディアおよびシグナリングを実行することができ、LSC を必要としないため、プロビジョニングおよび管理が容易です。電話機とテレプレゼンス エンドポイントでは、可能な場合は暗号化メディアとシグナリングを有効にすることを推奨します。ただし、混合モードを有効にして、LSC をインストールする必要があるため、より多くの設定が必要になります (MIC でなく、LSC を使用することを推奨します)。

認証が一方向の認証であることがあります。たとえば、管理者またはエンド ユーザが Web ブラウザを使用して Web サービスにアクセスする場合などです。この場合、クライアント（ブラウザ）が Web サーバを認証しますが、サーバはクライアント（ブラウザ）を認証しません。認証が、相互 TLS（MTLS）を使用した双方向認証であることもあります。この場合、サーバもクライアントを認証します。たとえば、エンドポイントと、エンドポイントが登録している Unified CM サーバ間のシグナリング、または Unified CM SIP トランクに、MTLS が使用されます。

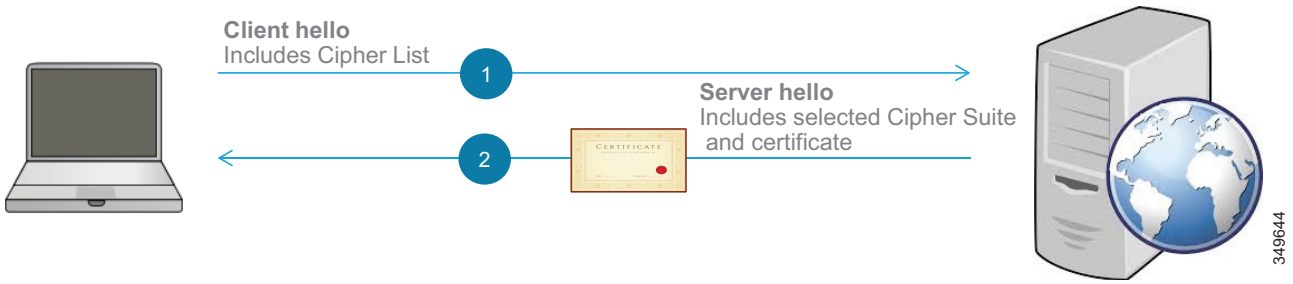
TLS の概要

Transport Layer Security（TLS）は、TCP トラフィックを暗号化する手法であり、一般に Web サービス トラフィックと SIP シグナリングに使用されます。TLS セッションの確立の全体的な流れを次に示します。

1. TLS クライアントにより TLS 接続が開始されます。このクライアントは TLS サーバに接続します。クライアントはまず、乱数とクライアントの機能を含む Client Hello を送信して、サーバとの TCP 接続を確立します。これらの機能には、クライアントでサポートされている暗号スイートのリストなどが含まれています。
2. TLS サーバは、通常はクライアントで優先される暗号スイートに基づいて暗号スイートの 1 つを選択し、Server Hello で応答します。このメッセージには、別の乱数とサーバ証明書も含まれているため、クライアントがこの証明書を認証できます。

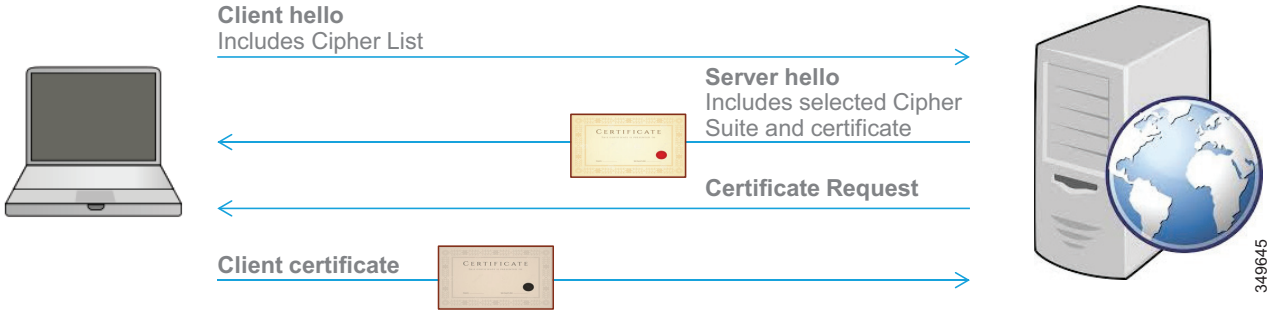
C：図 7-4 に、この 2 段階の TLS セッション確立手順を示します。便宜上、この図には TLS ハンドシェイクでのすべてのメッセージとバリエーションは含まれていません。サーバ証明書は Server Hello メッセージで送信されるか、または個別に送信されます。

C：図 7-4　TLS ハンドシェイク



認証が一方向の認証であることがあります。たとえば、管理者またはエンド ユーザが Web ブラウザを使用して Web サービスにアクセスする場合などです。この場合、クライアント（ブラウザ）が Web サーバを認証しますが、サーバはクライアント（ブラウザ）を認証しません。認証が、相互 TLS（MTLS）を使用した双方向認証であることもあります。この場合、サーバもクライアントを認証します。たとえば、エンドポイントと、エンドポイントが登録している Unified CM サーバ間のシグナリング、または Unified CM SIP トランクに、MTLS が使用されます。相互 TLS（MTLS）では、サーバもクライアントを認証します。サーバから CertificateRequest がクライアントに送信され、クライアントからそのクライアント証明書が送信されます。C：図 7-5 に全体的な流れを示します。

C：図 7-5　MTLS ハンドシェイク



RSA では、クライアントがサーバの公開キーを使用してプリマスター シークレットを暗号化し、サーバに送信します。Diffie-Hellman（DH）キー アグリーメント アルゴリズムでは、プリマスター シークレットはネットワーク経由では送信されず、クライアントとサーバが（乱数から計算され、認証のために秘密キーで署名された）データを交換します。これにより、クライアントとサーバは各自でプリマスター シークレットを導出できます。DH と変化する乱数の組み合わせ（Diffie-Hellman Ephemeral）により、Perfect Forward Secrecy（PFS）が実現します。

マスター シークレットが導出され、マスター シークレットからセッション キーが計算されます。この時点でクライアントとサーバは公開キー / 秘密キー ペア（非対称暗号化）の使用を停止し、暗号化に共有セッション キー（対称暗号化）を使用し始めます。

一般に、Cisco Collaboration 製品では TLS 1.2 がサポートされています。ただし、一部の製品ではこの TLS はまだサポートされていない可能性があり、一部の古い製品では一切サポートされていません。相互運用性を最大に引き出すため、デフォルト設定を使用し、特に無効にする必要がある場合を除き TLS 1.0 または TLS 1.1 を明示的に無効にしないでおくことをお勧めします。デフォルト設定では、クライアント インターフェイスとサーバ インターフェイスの両方で TLS 1.2 がサポートされている一般的なケースの場合、TLS 1.2 がネゴシエートされます。Cisco Collaboration 製品での TLS 1.2 のサポートと、TLS の古いバージョンを無効にする機能の詳細については、次で提供される *TLS Compatibility Matrix for Cisco Collaboration Products* の最新版を参照してください。

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

Cisco Unified CM および IM と Presence とエンドポイント

暗号化する主な 3 種類の接続を次に示します。

- HTTPS および管理インターフェイスまたはユーザ インターフェイス

  これらのインターフェイスのほとんどでは、デフォルトで暗号化が使用されます。たとえば、Unified CM 管理 Web インターフェイスと Unified CM エンドユーザ ポータルでは HTTPS が使用されます。パスワードまたはその他の機密情報が接続で送信される場合は、その接続を暗号化します。たとえば、LDAP と統合された Unified CM の場合は、LDAP over SSL を使用します。あるいはエンドポイントでは、エクステンション モビリティなどの Web サービスに対して HTTPS を設定します。

- シグナリング

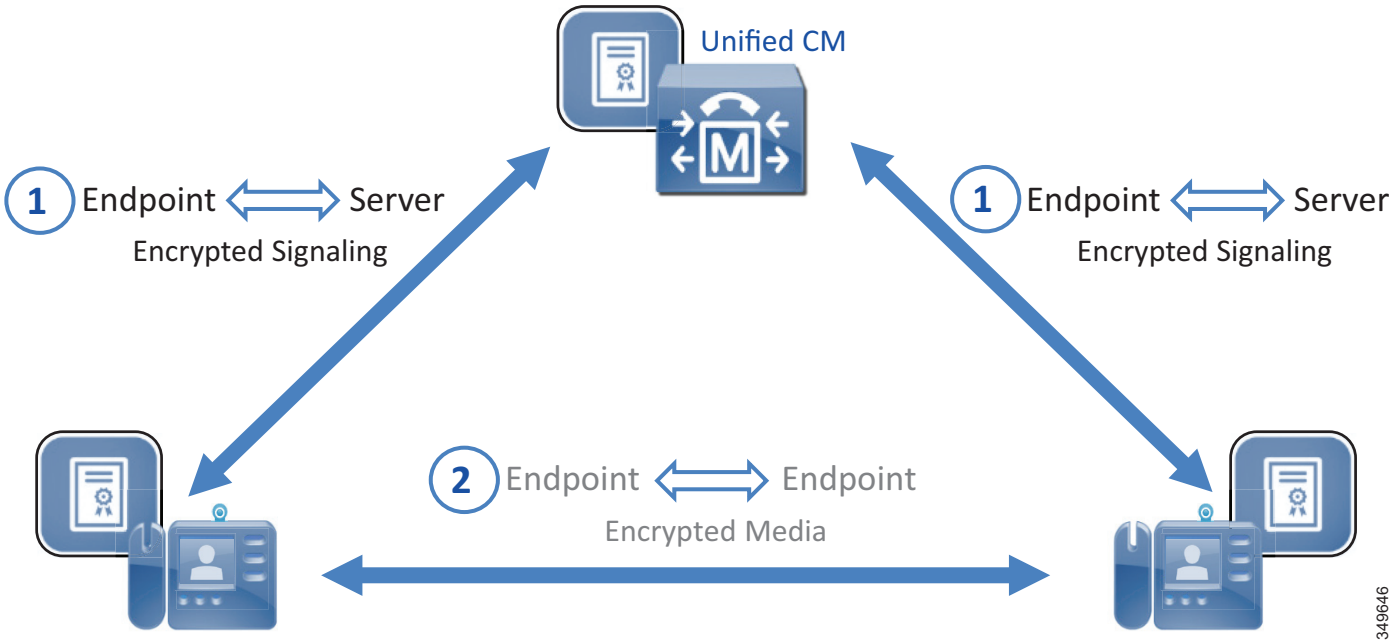
  TLS は主に、コール制御シグナリングの暗号化に使用されます。たとえば、エンドポイントと Unified CM サーバ間の SIP シグナリングまたは SIP トランクでの SIP シグナリングなどです。TLS は、XMPP など他の TCP 通信にも使用されます。

- メディア

  メディア トラフィックは、Secure RTP（SRTP）で暗号化できます。シグナリングも暗号化する必要があります。これは、（SDES を使用した）Unified CM へのシグナリングでは、メディア暗号化キーがエンドポイント間で交換されるためです。

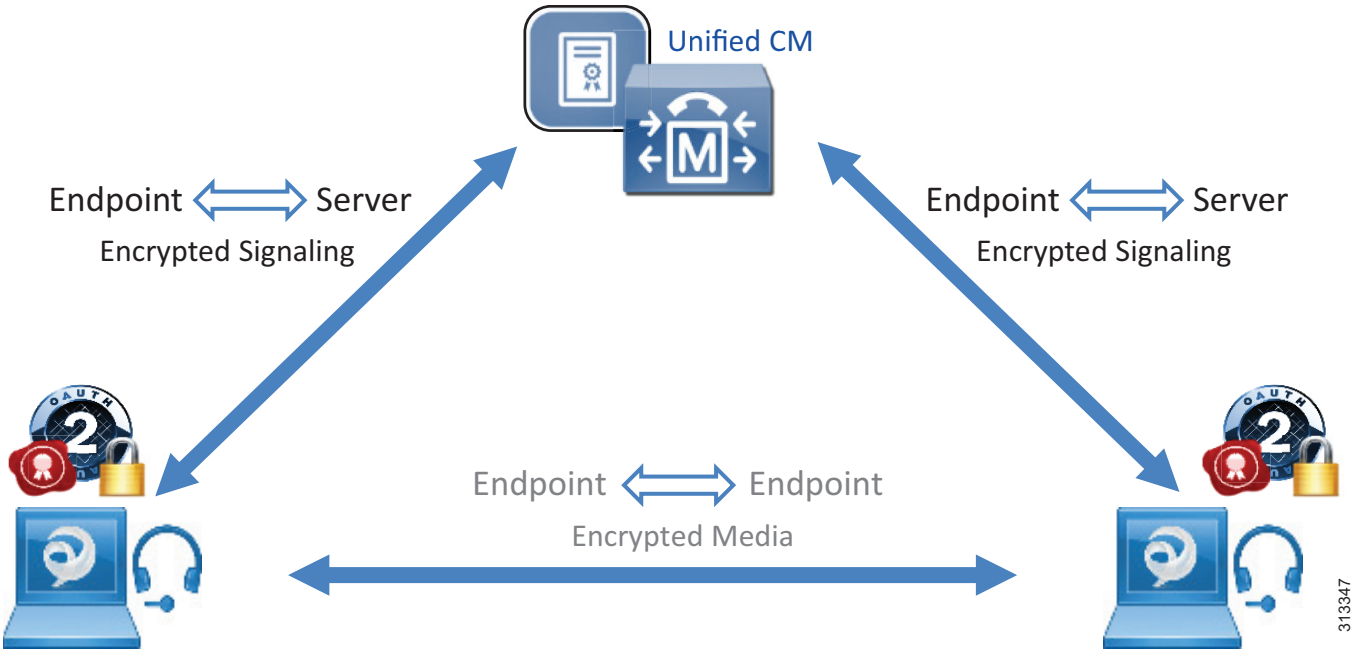
C：図 7-6 に、エンドポイントでのシグナリングとメディアの暗号化の全体像を示します。図のステップ 1 で示されるように、まず、エンドポイントと Unified CM の間の SIP シグナリングのために TLS が設定されます（エンドポイント登録）。図のステップ 2 で示されるように、エンドポイントからコールが発信されると、メディア暗号化キーが生成され、SIP TLS チャネルで送信されます。メディアは SRTP を使用して暗号化されます。C：図 7-6 で示されるように、電話機と TelePresence エンドポイントでは、シグナリング用の TLS ハンドシェイク認証は、統一された CM とエンドポイントの証明書に基づいています。

C：図 7-6　電話またはテレプレゼンスエンドポイントでのシグナリングおよびメディア暗号化



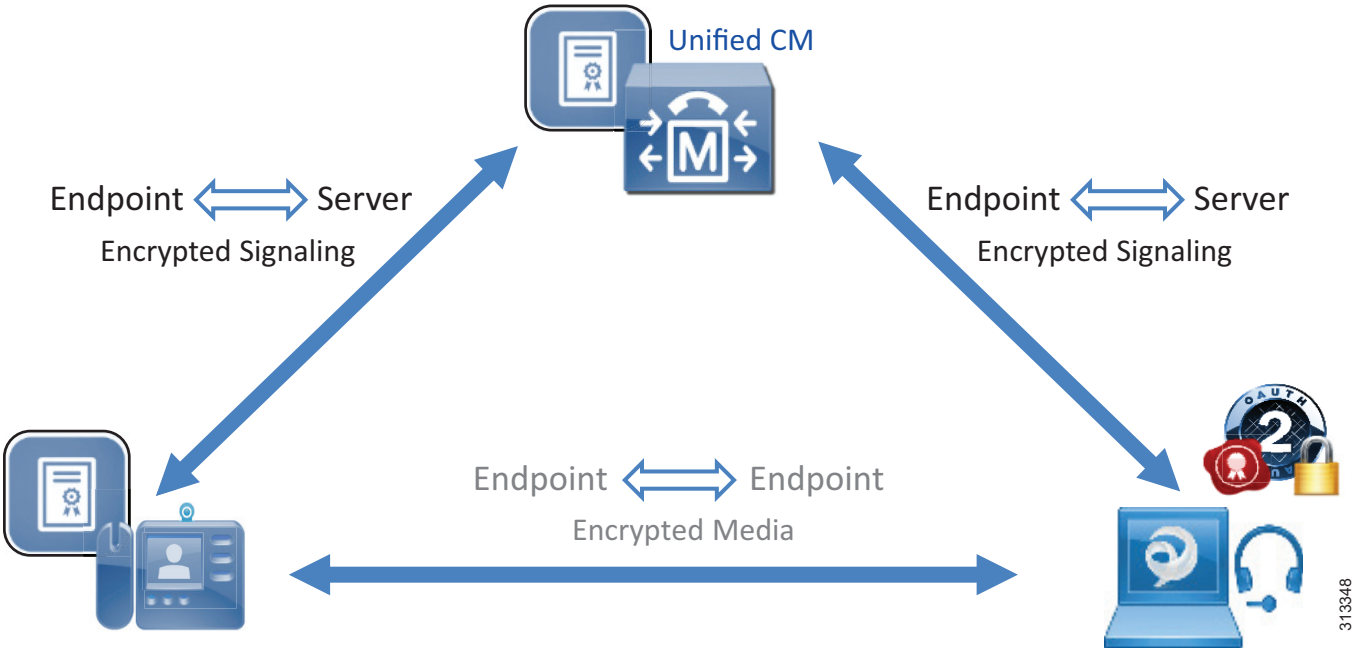
メディアとシグナリングの暗号化を実行するには、この推奨アーキテクチャの Jabber クライアントは、C：図 7-7 に示すように、TLS 認証に OAuth トークンを使用します。

C：図 7-7 Jabber を使用したシグナリングおよびメディア暗号化



LSC を使用してメディアおよびシグナリングを暗号化する電話機および TelePresence エンドポイントは、C：図 7-8 に示すように、OAuth トークンを使用する Jabber クライアントに対して暗号化されたコールを発信および受信することができます。

C：図 7-8 電話またはテレプレゼンス エンドポイントと Jabber を使用したシグナリングとメディアの暗号化



注　IM and Presence が導入されている Unified CM クラスタ内のノード間の通信（Intra-Cluster Communication Signaling（ICCS）など）を暗号化するには、IPSec を導入する必要があります。ただし、IPSec の設定と運用によって複雑さが大幅に増し、システムのスケーラビリティに影響すること、および Unified CM および IM and Presence ノードは通常、保護されており信頼できるデータ センター内に配置されていることから、IPSec の導入はほとんどの導入では通常は必要ではないため、このドキュメントでは説明しません。

暗号スイートのサポート

暗号スイートは、TLS セッションの確立に使用する暗号化アルゴリズムの組み合わせです。通信リンクの暗号化に使用できる暗号スイートは、Cisco Collaboration 製品に応じて異なります。標準的な暗号スイートは、Cisco Collaboration ソリューション全体でサポートされます。Cisco Unified CM、IM and Presence、Unity Connection などの一部の製品と、このガイドに示されているほとんどのエンドポイント（Cisco Jabber、Cisco IP Phone 7800 シリーズおよび 8800 シリーズ、Cisco Webex DX シリーズなど）では、次世代暗号化（NGE）と呼ばれる強力な新しい暗号スイートがサポートされています。これらの強力な暗号スイートは、新しいアルゴリズムをベースにしているか、またはより長い暗号キーを使用しているため、侵害が困難です。一般に、クライアントとサーバの両方でサポートされている最も強力な暗号スイートがネゴシエートされます。クライアントで弱い暗号スイートだけがサポートされている場合は、弱い暗号がネゴシエートされる可能性があります。弱すぎる暗号スイートにネゴシエートすることを回避するには、通常、ネゴシエート可能な暗号スイートを制限できます。たとえば統一された CM では、TLS 暗号スイートネゴシエーションを最も強力な暗号スイート（AES 256 と SHA 384 のみ）に制限する設定、強力な暗号スイートおよび中程度の強度の暗号スイート（AES 128 と SHA 256）を許可する設定、およびサポートされているすべての暗号スイートを許可する設定があります。より詳細な方法として、許可できる暗号スイートのリストを設定することも可能です。Cisco Collaboration ソリューション全体では、TLS 接続の設定に使用するデジタル署名アルゴリズムとして RSA がサポートされています。使用可能なもう 1 つのデジタル署名アルゴリズムとして、楕円曲線デジタル署名アルゴリズム（ECDSA）があります。ECDSA は、RSA と同レベルのセキュリティを提供しますが、キーのサイズが RSA よりも小さくなっています。ただし、すべての統一された CM サービス、すべての Cisco Collaboration 製品、またはエンドポイントでサポートされているわけではありません。また、それはサーバおよびクライアントが ECDSA ベースの証明書を持つことを必要としする場合があります。RSA と ECDSA の詳細については、「証明書の管理」を参照してください。

注　ECDHE に基づく暗号化アルゴリズム スイートでは、ECDSA に基づく証明書は不要です。このようなスイートは RSA に基づく証明書とネゴシエートできます。

次に、各種接続の暗号スイートと推奨事項を説明します。

- HTTPS 接続

  Unified CM および IM and Presence の場合、HTTPS 暗号スイートを対象としたエンタープライズ パラメータ設定が 1 つあります。このパラメータにより、RSA 専用暗号スイートが許可されるのか、またはすべての暗号スイート（RSA および ECDSA）が許可されるのかが決まります。デフォルト値（RSA 専用暗号スイートの許可）を使用することが推奨されます（詳細については「RSA および ECDSA」を参照）。

  ネゴシエートされる一般的な暗号スイートは、TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 または TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 です。これらの暗号スイートでは、ECDHE（Elliptical Curve Diffie Hellman Ephemeral）と RSA は、デジタル署名アルゴリズムとキー アグリーメントに使用される暗号を示します。AES（Advanced Encryption Standard）、GCM（Gallois Counter Mode）、および SHA（Secure Hash Algorithm）は、暗号化パケットの実際の暗号化と認証に使用されます。

- SIP TLS (シグナリング)

  Unified CM ではデフォルトで、RSA に基づく暗号スイートが ECDSA に基づく暗号スイートよりも優先されます。ECDSA はすべてのエンドポイントでサポートされているわけではなく、またすべての Cisco Collaboration サーバでサポートされているわけではないため、これは推奨される設定です。

  デフォルトでは、サポートされているすべての暗号スイートが有効になります。前述したように、より強力な暗号スイートが最初にネゴシエートされます。通常は TLS_ECDHE_RSA および AES256_GCM_SHA384 がネゴシエートされます。ただし、場合によってはこの暗号化がいずれの側でもサポートされていないため、これよりも弱い暗号をネゴシエートする必要があります。ソリューション内の各種コンポーネントでの暗号スイートの互換性を最大限に引き出すため、デフォルト設定（すべての暗号スイートを許可し、RSA を優先する）を使用することが推奨されます。

- SRTP（メディア）

  Unified CM では、デフォルトですべての暗号化が有効になっています。前述したように、強力な暗号スイートが最初に試行されます。通常、最も強力な暗号化である AEAD AES-256 GCM（Authenticated Encryption with Associated Data、Advanced Encryption Standard、256 キー サイズ、Galois Counter Mode）がネゴシエートされます。ただし Cisco IOS Gateway、一部のエンドポイント、および一部のサーバではこの暗号スイートがサポートされていないことがあります。このため、デフォルト設定を使用し、弱い暗号スイートへのフォールバックを許容することが推奨されます。シスコ エンドポイントでサポートされている暗号スイートを確認するには、Unified CM の [Cisco Unified Reporting] ページに移動します（[システム レポート（System Reports）] > [Unified CM Phone の機能リスト（Unified CM Phone Feature List）]）。

メディアおよびシグナリング暗号化のための Unified CM 混合モード

Unified CM を初めてインストールする場合、いわゆる「非セキュア モード」でインストールされますが、実際にはこのモードではほとんどのセキュリティ機能が使用可能です。たとえば、非セキュア モードの Unified CM では、署名付き TFTP 設定ファイル、暗号化 TFTP 設定ファイル、署名付き電話ファームウェア、Web サービスへの HTTPS アクセス、ローカルで有効な証明書（LSC）をインストールするための CAPF 登録、SIP トランク暗号化、電話の VPN、802.1x はすべてデフォルトで使用可能になっています。Jabber でのメディアおよびシグナリングの暗号化は、SIP OAuth モードが有効になっている場合にも可能です (詳細については、Jabber を使用した SIP OAuth の項を参照してください)。非セキュアモードで欠落しているセキュリティ機能は、電話機および TelePresence エンドポイントのメディアおよびシグナリング暗号化です。この機能を有効にするには、スマートライセンスで輸出規制機能が許可されており、統一された CM を混合モードで設定する必要があり、また統一された CM ソフトウェアの制限付きバージョンが必要です。（メディアおよびシグナリング暗号化は、無制限バージョンの Unified CM では使用できません。）

混合モードと暗号化に関する重要な考慮事項として、電話および TelePresence エンドポイントでの証明書の管理があります。エンドポイントで MIC の代わりに LSC を使用することが推奨されるため、電話機と TelePresence エンドポイントでの CAPF 登録 (LSC インストール) は、メディアとシグナリングの暗号化が有効になっている電話機と TelePresence エンドポイントで実行する必要があります。管理者は LSC の有効期間をモニタし、有効期限切れになる前に証明書を交換する必要があります。エンドポイントは、現在有効なサーバ証明書を保持する必要もあります。たとえば、現在の CallManager 証明書がなく、メディアおよびシグナリング暗号化を使用して設定されている場合は、統一された CM に登録されません。（詳細については、「CTL および ITL」を参照。）

混合モードを有効にする方法は 2 通りあります。

- ハードウェア USB eToken

  混合モードを有効にする従来の方法です。2 つ以上のハードウェア USB eToken（KEY-CCM-ADMIN-K9= または新しい KEY-CCM-ADMIN2-K9=）が必要です。証明書信頼リスト（CTL）ファイルの署名に 1 つの eToken が使用されます。もう 1 つの eToken を用意することで、1 番目の eToken が紛失した場合または使用できない状態になった場合に備えた冗長性が実現します。混合モードを有効にするには、CTL クライアント ソフトウェアを Microsoft Windows デスクトップにインストールする必要があります。この CTL クライアント ソフトウェアの実行中に、USB eToken をデスクトップに挿入する必要があります。混合モードの設定後に、Unified CM クラスタの CTL ファイルを作成し、USB eToken を取り外し、オフラインにします。

- トークンレス（ソフトウェア eToken）

  この方法では、USB トークンと Microsoft Windows デスクトップは不要です。単に CLI コマンド **utils ctl set-cluster mixed-mode** を使用して混合モードを有効にします。CTL ファイルは、ハードウェア USB eToken ではなく ITLRecovery 秘密キーによって署名されます。

トークンレス方式が推奨されます。このドキュメントではこの方式について説明します。トークンレス方式では、混合モードを有効にする方法と CTL ファイルを更新する方法がシンプルです。混合モードを有効化するときと CTL ファイルを更新するときに、USB eToken を取得し、CTL クライアントを Microsoft Windows デスクトップにインストールし、CTL クライアントを実行する必要はありません。実行する必要がある CLI コマンドは 1 つだけです。CTL の署名には、長い秘密キー（ITLRecovery 秘密キー）が使用されます。また、Cisco Unified CM 12.0 以降では、ITL ファイルとトークンレス CTL ファイルは ITLRecovery 秘密キーにより署名されるため、Trust Verification Service（TVS）に問題がある場合、CallManager 証明書の更新に関する懸念が解消され、またこの更新が原因でエンドポイントと Unified CM 間の信頼関係が失われることがなくなりました。

Jabber を使用した SIP OAuth

Jabber でメディアおよびシグナリングの暗号化を有効にするには、混合モードを有効にして、Jabber に LSC をインストールします。このアプローチの欠点は、LSC をインストールして維持するため、Jabber による追加の管理上のオーバーヘッドが必要になる場合があることです。たとえば、Jabber エンドポイントがリセットされた場合、新たな LSC をインストールする必要があります。Jabber に LSC をインストールする代わりに、SIP の OAuth トークンを有効にすることを推奨します。このモードでは、Jabber は LSC なしで、また、統一された CM で混合モードを有効にする必要なく、メディアおよびシグナリングの暗号化を実行できます。

OAuth トークンを SIP で使えるように、スマートライセンスで輸出規制機能が許可されており、統一された CM ソフトウェアの制限付きバージョンが必要です。（メディアおよびシグナリング暗号化は、無制限バージョンの Unified CM では使用できません。）

注　Jabber 以外のエンドポイントに対して暗号化メディアとシグナリングを有効にする場合も、統一された CM で混合モードを有効にする必要があります。

TFTP 設定ファイルの暗号化

TFTP 設定ファイルを暗号化しないと、すべての Unified CM TFTP サーバで TFTP 設定ファイルがプレーンテキスト形式で使用可能になります。TFTP 設定ファイルには、電話ファームウェアの情報や Unified CM クラスタの情報などが含まれています。さらに、ユーザ名とパスワードが Unified CM 管理電話ページでプロビジョニングされている場合、このユーザ名とパスワードが TFTP 設定ファイルにプレーンテキスト形式で保存されています。したがって、オンプレミスのエンドポイント（モバイルおよびリモート アクセス（MRA）経由で接続していないエンドポイント）で電話と TelePresence 用の TFTP 設定ファイルの暗号化を有効にすることが推奨されます。これは、Unified CM 管理電話ページでユーザ名、パスワード、または機密情報が設定されている場合に特に重要です。

MRA 電話および MRA TelePresence エンドポイントでは、TFTP 設定ファイル暗号化が設定されている場合、MIC が含まれていても、最初に MRA エンドポイントをオンプレミスに導入してから、統一された CM に直接登録し、その後インターネットに導入して MRA 経由で接続する必要があります。さらに、MRA 経由で接続するエンドポイントに LSC をインストールまたは更新することはできません。したがって、LSC の有効期限が切れると、エンドポイントは社内ネットワークに戻す必要があります。このような理由から、MRA 経由で接続しているエンドポイント（特に Jabber エンドポイント）では、TFTP 設定ファイルの暗号化を有効にしないでおく方が簡単です。ただし、これらのエンドポイントの機密情報（たとえばパスワード）が設定されていないことを確認してください。

Jabber クライアントは、この推奨アーキテクチャでは SIP OAuth モードに対して有効になっており、暗号化メディアおよびシグナリングには LSC は必要ありませんが、TFTP 設定ファイルの暗号化には 1 つ必要となります。Jabber クライアントで LSC を管理するには、追加の管理オーバーヘッドが必要です (たとえば、Jabber をリセットすると、LSC が削除されるので、新しい LSC をインストールする必要があります)。また、LSC は暗号化メディアおよびシグナリングには不要です。通常、Jabber クライアントに LSC をインストールしないことを推奨します。つまり、Jabber クライアントがオンプレミスであるか、MRA 経由で接続されているかにかかわらず、TFTP 設定ファイルの暗号化を採用しないことになります。ただし、Jabber クライアント用に、これらのエンドポイントの機密情報が設定されていないことを確認してください。

セキュア SRST

Cisco 4000 シリーズ サービス統合型ルータに基づく Survivable Remote Site Telephony（SRST）ルータは、セキュア SRST を使用して設定することもできます。エンドポイントは、Unified CM コール処理サーバとの通信を確立できないと SRST にフェールオーバーし、メディアおよびシグナリングは引き続きセキュア SRST で暗号化されます。エンドポイントの TFTP 設定ファイルに SRST 証明書が含まれており、SRST ルータの信頼ストアに LSC に署名した CA の証明書が含まれているため（管理者により手動でインポートされた CAPF 証明書あるいは外部 CA 証明書）、エンドポイントと SRST ルータはセキュアな認証済みセッションを確立することができます。

Cisco Meeting Server

Cisco Meeting Server ノード間の内部通信には暗号化（TLS）が使用されます。Cisco Meeting Server とその他のサーバまたはデバイス間の外部通信では、通信のタイプに応じて暗号化は強制またはオプションです。たとえば、Unified CM と Cisco Meeting Server 間の RESTful API 通信は常に暗号化されます。ただし、Cisco Meeting Server と Unified CM またはエンドポイント間の SIP シグナリングおよびメディアの設定時には、暗号化を使用してもしなくてもかまいません（暗号化が推奨されます）。会議では、すべての参加エンドポイントが暗号化されている場合（暗号化メディアおよびシグナリング）、会議ロックをサポートするすべてのエンドポイントにロック アイコンが表示されます。参加エンドポイントのいずれかがセキュアではない場合、会議ロックをサポートするすべてのエンドポイントにロック解除アイコンが表示されます。

Cisco Unity Connection

このドキュメントでは、次世代暗号化（NGE）を使用した Cisco Unity Connection のメディアおよびシグナリング暗号化について説明します。暗号化により、Unity Connection との間でのシグナリングと、エンドポイントと Unity Connection ボイスメール ポート間でのメディアが暗号化されます。デフォルトでは、Unified CM と Unity Connection 間のシグナリングでは TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 暗号スイートがネゴシエートされます。

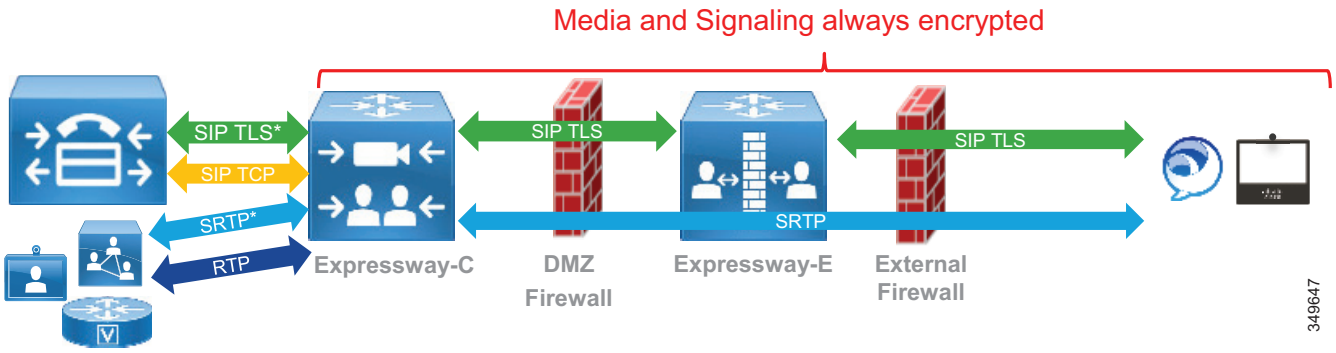
Cisco Expressway

Cisco Expressway とのモバイルおよびリモート アクセス（MRA）コミュニケーションおよび Business-to-Business（B2B）コミュニケーションについて説明します。

モバイル&リモートアクセス（MRA）

MRA エンドポイントと Expressway-C 間のメディアおよびシグナリングは常に暗号化されます。MRA エンドポイントが社内ネットワーク内部のエンドポイントをコールする場合、社内ネットワーク内のコール レッグ（Expressway-C と Unified CM 間のシグナリングおよび Expressway-C と内部エンドポイント間のメディア）は設定に基づいて暗号化できます。非暗号化モードで電話セキュリティ プロファイルを使用して MRA エンドポイントが設定されている場合、この内部コール レッグは暗号化されません。Unified CM が混合モードであり、暗号化モードで電話セキュリティ プロファイルを使用して MRA エンドポイントが設定されている場合、Expressway-C と Unified CM 間の SIP シグナリングは暗号化されます。さらに、内部エンドポイントも暗号化モードで設定されている場合、Expressway-C と内部エンドポイント間のメディアは暗号化されるため（SRTP）、メディアおよびシグナリングはエンドツーエンドで暗号化されます（厳密にはすべてのコール レッグが暗号化されます）。C：図 7-9 を参照してください。

C：図 7-9　MRA エンドポイントのメディアおよびシグナリング暗号化



MRA での SIP TLS 認証に使用される証明書は、オンプレミス コールとは異なります。エンドポイントが MRA 経由で企業に接続している場合、エンドポイントは Expressway-E サーバの証明書を検証しますが、サーバではエンドポイントの証明書は確認されません。この TLS 接続では相互認証は使用されません。MRA クライアントの MIC 証明書または LSC は、存在しているかどうかに関係なく、検証されません。MRA クライアントのユーザのユーザ名とパスワードが、Cisco Unified CM ユーザ データベースまたは統合 LDAP サーバ（Jabber がシングル サインオンを使用して導入されている場合は IdP）と照合され、ユーザが認証されます。Expressway-C と Unified CM 間のコール レッグの場合、MRA エンドポイントが暗号化モードで設定されていると、Expressway-C は Unified CM との SIP TLS 接続を確立し、MRA エンドポイ

ントの代わりにそれ自体の証明書を送信します。Unified CM はこの証明書を受信すると、その MRA エンドポイントに対して設定されている電話セキュリティ プロファイルの名前が、Expressway-C 証明書の SAN 拡張の一部であるかどうかを確認します。

Business-to-Business（B2B）コミュニケーション

Business-to-Business（B2B）コミュニケーションでは、Expressway ともう一方の側の間の接続を暗号化する必要はありません。これは、Expressway ゾーン設定の [トランスポート（Transport）] パラメータに基づきます。[トランスポート（Transport）] が [TLS] に設定されている場合、証明書の検証は不要です。管理者は証明書の検証を無効にできます。無効にするには、Expressway ゾーン設定の [TLS 検証（TLS verify）] パラメータを [オフ（Off）] に設定します。

Cisco IOS Gateway と Cisco Unified Border Element

Cisco IOS Gateways と Cisco Unified Border Element では TLS と SRTP がサポートされています。SRTP の場合、デフォルトでは暗号スイート AES_CM_128_HMAC_SHA1_32 がネゴシエートされます。暗号スイート AES_CM_128_HMAC_SHA1_80 も設定できます。NGE 暗号スイートをサポートするには、SRTP パススルーを設定する必要があります。SRTP パススルーの主なデメリットは、RTP と SRTP 間のメディア インターワーキング（RTP と SRTP をそれぞれ別のコール レッグで処理）がサポートされていない点です。

デフォルトでは、Cisco IOS Gateway または Cisco Unified Border Element からコールが発信され、SRTP が要求されるが、着信側エンドポイントでは SRTP がサポートされていない場合、コールはドロップされます。相互運用性を最大限に引き出すには、**srtp fallback** と **srtp negotiate** を設定します。これらが設定されている場合、デフォルトでは、Cisco IOS Gateway または Cisco Unified Border Element はコールをドロップしませんが、代わりに SRTP から RTP にフォールバックします。

SRTP コマンドの詳細については、次のリンク先にある『*Cisco IOS Voice Command Reference*』を参照してください。
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/vcr4/vcr4-cr-book/vcr-s11.html

マルチクラスターに関する考慮事項

マルチクラスタ導入環境では、クラスタが同じデータセンター内にある場合、クラスタ間の暗号化は重要ではありません。ただし、クラスタが異なるデータセンターに分散しており、サービス プロバイダー リンクにより接続されている場合には、次のクラスタ間リンクで暗号化を有効にすることが推奨されます。

- SIP トランク

  クラスタ間の SIP トランクを暗号化します。CA により署名された CallManager 証明書と CA 証明書（またはルート CA 証明書）がすでに CallManager 信頼ストアに格納されている場合、クラスタ間 SIP トランク暗号化のために追加の証明書関連操作を行う必要はありません。

- クラスタ間検索サービス（ILS）接続

  クラスタ間検索サービス（ILS）接続を暗号化します。ILS 暗号化を有効にするには、認証に TLS 証明書（tomcat 証明書）を使用し、承認にすべてのクラスタで共有パスワードを使用することが推奨されます。CA により署名された tomcat 証明書と CA 証明書（またはルート CA 証明書）がすでに tomcat 信頼ストアに格納されている場合、ILS 暗号化を有効にするために追加の証明書関連操作を行う必要はありません。

- Location Bandwidth Manager（LBM）リンク

  コール アドミッション制御（CAC）が設定されている場合、クラスタ間 LBM リンクも暗号化する必要があります。LBM 暗号化も tomcat 証明書に基づいており、CA により署名された tomcat 証明書と CA 証明書がすでに tomcat 信頼ストアに格納されている場合、LBM 暗号化を有効にするために追加の証明書関連操作を行う必要はありません。

コラボレーション セキュリティーのハイ アベイラビリティーに関する考慮事項

統一された CM の信頼検証サービス（TVS）には高可用性が備わっています。TVS はすべての統一された CM ノードでネットワークサービスとして動作します。エンドポイントは、Cisco Unified CM グループで設定されている Unified CM コール処理ノードと同じ TVS ノードを使用します。そのプライマリ TVS サーバはプライマリ コール処理サブスクライバであり、そのバックアップ TVS サーバはバックアップ コール処理サブスクライバです。

Unified CM パブリッシャには、セキュリティ コンポーネントに関する重要な役割があります。パブリッシャは、電話が接続する CAPF サービスを実行します。したがって、パブリッシャがダウンすると、CAPF 操作が不可能になります。たとえば、ローカルで有効な証明書（LSC）をインストールできなくなります。マルチサーバ証明書を生成し、混合モードを有効 / 無効にする操作もパブリッシャで実行され、このためにはパブリッシャが稼働している必要があります。

コラボレーション セキュリティ キャパシティ プランニング

暗号化を有効にすると、サーバの CPU およびメモリの使用率が多少増加します。ただし Cisco Unified Border Element を除き、「サイジング」で説明する簡易サイジング導入は、暗号化を有効にする操作の影響を受けません。

展開

ここでは、証明書の管理と暗号化機能の導入について説明します。まず、最初に実行する必要がある証明書の管理について説明します。すべての証明書が用意されたら、暗号化を有効化および設定できます。

ここでは、企業のコラボレーション向けプリファード アーキテクチャの次のコンポーネントの導入について説明します。

- Cisco Unified CM および IM と Presence とエンドポイント
- Cisco Unity Connection
- コラボレーション エッジ（Cisco Expressway、Cisco IOS Gateway、および Cisco Unified Border Element）
- 会議
- コラボレーション管理サービス

Cisco Unified CM および IM と Presence とエンドポイント

Cisco Unified CM および IM と Presence とエンドポイントで行う設定の概要を次に示します。

- 暗号スイートの設定
- サーバー証明書の生成と管理
- 証明書のモニタリング
- LDAP over SSL の設定
- SIP トランクの暗号化

エンドポイントでのメディアおよびシグナリング暗号化のため、次の設定を行います。

- 混合モードの設定
- エンドポイントのメディアおよびシグナリング暗号化のための CAPF 登録と設定
- セキュア SRST の設定

暗号スイートの設定

主要なセキュア接続は 3 種類あり、接続ごとに暗号エンタープライズ パラメータがあります。

- HTTPS

  「暗号スイートのサポート」で説明したように、[HTTPS 暗号（HTTPS Ciphers）] エンタープライズ パラメータではデフォルト値の [RSA 暗号のみ（RSA Ciphers only）] を使用することが推奨されます。ECDSA 暗号を有効にするには、この設定を [サポートされているすべての EC および RSA 暗号（All Supported EC and RSA Ciphers）] に変更します。

- TLS（シグナリング）

  「暗号スイートのサポート」で説明したように、[TLS 暗号（TLS Ciphers）] エンタープライズ パラメータにはデフォルト値の [すべての RSA 暗号を優先（All Ciphers RSA Preferred）] を使用することが推奨されます。ただし特定の要件がある場合、たとえば弱い暗号スイートのネゴシエーションを無効にする必要がある場合や、RSA 暗号スイートよりも ECDSA を優先してネゴシエートしたい場合などには、[TLS 暗号（TLS Ciphers）] エンタープライズ パラメータを変更できます。

- SRTP（メディア）

  「暗号スイートのサポート」で説明したように、[SRTP 暗号（SRTP Ciphers）] エンタープライズ パラメータではデフォルト値の [サポートされているすべての暗号（All Supported Ciphers）] を使用することが推奨されます。ただし特定の要件がある場合、たとえば弱い暗号スイートのネゴシエーションを無効にする必要がある場合などには [SRTP 暗号（SRTP Ciphers）] エンタープライズ パラメータを変更し、[最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] または [中程度 - AEAD AES-256 GCM、AEAD AES-128 GCM 暗号のみ（Medium - AEAD AES-256 GCM, AEAD AES-128 GCM ciphers only）] に設定できますが、一部のエンドポイントとサーバではこれらの暗号スイートがサポートされていないことに注意してください。詳細については、暗号スイートのサポートを参照してください。

サーバー証明書の生成と管理

「自己署名証明書の代わりの CA 署名付き証明書」で説明したように、ほとんどの証明書には CA 署名付き証明書を使用することが推奨されます。CA により署名される証明書のリストについては、C：表 7-5 を参照してください。CA の署名が不要な証明書は、変更または再生成する必要はありません。

CA 署名付き証明書を発行する全体的な手順を次に示します。

1．ルート CA 証明書をアップロードするまたは証明書チェーンを対応するサーバの信頼ストアにアップロードします。

2．証明書署名要求（CSR）を生成する希望する証明書の証明書署名要求（CSR）を生成します。

3．CSR をダウンロードする。

4．署名 CA に CSR を送信する。

5．適切なタイプを使用して新しい CA 署名付き証明書をアップロードする。

Unified CM、IM and Presence Service、および Unity Connection では、これらの操作はシステムの OS 管理 Web インターフェイスから実行します。

手順の詳細については、次のリンク先にある『*Security Guide for Cisco Unified Communications Manager*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

1. ルート CA 証明書をアップロードする

最初に、ルート CA 証明書（パブリック CA を使用する場合は証明書チェーン）をインポートします。Unified CM と IM and Presence Service では、この操作をパブリッシャでのみ実行する必要があります。これにより、証明書はクラスタ内の他のノードの信頼ストアに自動的に配布されます。

[OS の管理（OS Administration）] ページに移動し、[セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [証明書 / 証明書チェーンのアップロード（Upload Certificate/Certificate chain）] を選択して、CA 署名付き証明書を発行するサービスの信頼ストアにルート CA 証明書（または証明書チェーン）をアップロードします。RSA 証明書と ECDSA 証明書は同じ信頼ストアを共有します。C：表 7-8 に、CA 証明書をインポートする必要がある信頼ストアを示します。

C：表 7-8　Unified CM および IM and Presence Service の CA 証明書をインポートする信頼ストア

製品	CA 証明書をアップロードする必要があるノード
Unified CM	tomcat-trust
Unified CM	callManager-trust
IM and Presence Service	tomcat-trust
IM and Presence Service	cup-xmpp-trust

2. 証明書署名要求（CSR）を生成する

証明書署名要求（CSR）を生成するには、[OS の管理（OS Administration）] ページに進み、[セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [CSR の生成（Generate CSR）] を選択します。

一部の証明書ではマルチサーバ機能がサポートされています。リストについては C：表 7-6 を参照してください。これらの証明書の場合、パブリッシャで CSR を生成し、[CSR] ページの [配布（Distribution）] フィールドで [マルチサーバ（SAN）（Multi-Server (SAN)）] を選択します。マルチサーバ証明書の CSR を生成する場所については、C：表 7-9 を参照してください。その他の証明書の場合、各ノードで CSR を発行し、[配布（Distribution）] フィールドではデフォルト値を使用します。

C：表 7-9　マルチサーバ証明書の CSR

製品	証明書	CSR を生成する場所
Unified CM and IM and Presence Service	tomcat	Unified CM パブリッシャ
Unified CM	CallManager	Unified CM パブリッシャ
IM and Presence Service	xmpp	IM and Presence Service パブリッシャ
IM and Presence Service	xmpp-s2s	IM and Presence Service パブリッシャ

通常は、[コモンネーム（Common Name）] フィールドのデフォルト値を変更する必要はありません。デフォルトでは、このフィールドには CSR を生成するノードの FQDN が設定されています。マルチサーバ証明書では、FQDN のホスト名部分の後に「-ms」が付加されます。

通常は、[キー長（Key Length）] に 2048 ビット以上、[ハッシュ アルゴリズム (Hash Algorithm)] に [SHA256] を使用することが推奨されます。したがってこれらのフィールドではデフォルト値を使用できます。

3. CSR をダウンロードする

4. 署名 CA に CSR を送信する

CA が対応する証明書を生成します。

キー使用法拡張機能と拡張キー使用法拡張機能により、キーの使用目的が限定されます。発行された証明書での X.509 キー使用法と X.509 拡張キー使用法が CSR の要求に一致していることを確認します。一般的な問題として、証明書を発行および署名するエンタープライズ CA が、適切な証明書テンプレートを使用して設定されておらず、適切なキー使用法拡張機能を含む証明書を発行しないことがあります。たとえば、Unified CM tomcat 証明書には「TLS Web クライアント認証」拡張キー使用法（EKU）が含まれている必要があります。TLS Web クライアント EKU が含まれているテンプレートを使用しないと、キー使用法が正しくないことが原因で、クラスタ間検索サービス（ILS）やユーザ データ ストア（UDS）などのサーバ間通信のための TLS 接続の設定が失敗します。C：表 7-10 に、キー使用法の要件を示します。原則として、CSR を生成し、CSR に指定されているキー使用法と拡張キー使用法を確認して、エンタープライズ CA に、正しいキー使用法と拡張キー使用法が含まれている証明書テンプレートがあるかどうかを確認し、ない場合には新しい証明書テンプレートを作成します。CSR を CA に送信し、証明書に戻ったら、キー使用法と拡張キー使用法が証明書に含まれていることを確認します。

C：表 7-10　キー使用法と拡張キー使用法の要件

製品	証明書	X509v3 キー使用法	X509v3 拡張キー使用法
Unified CM and IM and Presence Service	tomcat	デジタル署名、 キーの暗号化、 データの暗号化	TLS Web サーバ認証、 TLS Web クライアント認証
Unified CM	CallManager	デジタル署名、 キーの暗号化、 データの暗号化	TLS Web サーバ認証、 TLS Web クライアント認証
Unified CM	CAPF	デジタル署名、 証明書の署名、	TLS Web サーバ認証
IM and Presence Service	cup-xmpp	デジタル署名、 キーの暗号化、 データの暗号化	TLS Web サーバ認証、 TLS Web クライアント認証
IM and Presence Service	cup-xmpp-s2s	デジタル署名、 キーの暗号化、 データの暗号化	TLS Web サーバ認証、 TLS Web クライアント認証

5. 適切なタイプを使用して新しい CA 署名付き証明書をアップロードする

証明書をアップロードし、[証明書の目的（Certificate Purpose）] フィールドで対応する値を選択します。たとえば、tomcat 証明書をアップロードする場合は、[証明書の目的（Certificate Purpose）] フィールドで [tomcat] を選択します。

マルチサーバ証明書の場合、サブスクライバ ノードではなくパブリッシャ ノードでアップロード操作を実行します。

証明書のアップロードが完了したら、サービスを再起動する必要があります。GUI で、再起動するサービスが示されます。たとえば CallManager 証明書の場合、Cisco Tftp、Cisco CallManager、および Cisco CTIManager サービスを再起動する必要があります。

証明書のモニタリング

証明書の有効性のモニタリング

Unified CM で、サーバ証明書と LSC の有効性のモニタリングを有効にします。

[Cisco Unified CM OS の管理（Cisco Unified CM OS Administration）] > [セキュリティ（Security）] > [証明書モニタ（Certificate Monitor）] に移動し、通知を開始する有効期限前の日数と、通知頻度を入力します。電子メール通知を有効にします。サーバ証明書と LSC の両方がモニタされるようにするため、[LSC モニタリングの有効化（Enable LSC monitoring）] を選択します。

長期セッションの証明書有効性チェック

Unified CM は、長期接続で証明書の失効状況と有効期限状況を定期的に確認します。JTAPI/TAPI アプリケーションとの CTI 接続と LDAP 接続（および IPSec、ただし IPSec についてはこのドキュメントでは説明しません）についてこの確認を行います。

長期接続での証明書有効性チェック（有効期限および失効状況のチェック）を有効にするには、Unified CM エンタープライズ パラメータ [証明書有効性チェック（Certificate Validity Check）] をオンにします。

証明書の失効状況の検証の場合、[Cisco Unified CM OS の管理（Cisco Unified CM OS Administration）] > [セキュリティ（Security）] > [失効（Revocation）] で Online Certificate Status Protocol（OCSP）も設定します。

LDAP over SSL の設定

Microsoft Active Directory への接続に LDAP over SSL を設定します。

Unified CM で次の手順を実行します。

- LDAP 証明書が自己署名証明書の場合は、その証明書を Unified CM tomcat-trust ストアにインポートします。

  LDAP 証明書が CA 署名付き証明書の場合は、ルート CA 証明書を Unified CM tomcat-trust ストアにインポートします。LDAP 証明書の失効状況をモニタするために Online Certificate Status Protocol（OCSP）を設定している場合は、LDAP 証明書自体もインポートしてください。

- **Cisco Unified CM の管理** で、> **システム** > **LDAP** > **LDAP ディレクトリ**、また、**Cisco Unified CM の管理** > **システム** > **LDAP** > **認証**で、**LDAP ポート** を安全なポートに変更し、**TLS を使用** のオプションを有効（チェックボックスをオン）にします。通常、LDAP セキュアポートは、グローバルカタログ（GC）に対して同期する場合は「3268」、Windows Microsoft Active Directory ドメインコントローラ（DC）に対して同期する場合は「636」です。DC および GC の動作とポート番号に関する詳細については、Microsoft のドキュメンテーション https://technet.microsoft.com/en-us/library/cc978012.aspx[英語] を参照してください。

SIP トランクの暗号化

ここでは、Unified CM SIP トランクの暗号化を設定する方法を説明します。

既存のすべての SIP トランク セキュリティ プロファイルの [Unified CM の管理（Unified CM Administration）] インターフェイス（[システム（System）] > [セキュリティ（Security）] の下）で、SIP トランクのタイプ別にセキュア SIP トランク セキュリティ プロファイルを作成します。既存の SIP トランク セキュリティ プロファイルと同じパラメータ（「コール制御」の章を参照）を使用します（ただし C：表 7-11 にリストされているパラメータを除きます）。

C：表 7-11　セキュア SIP トランクの SIP トランク セキュリティ プロファイル パラメータ

パラメータ	値
[デバイスセキュリティ モード（Device Security Mode）]	暗号化
[着信転送タイプ（Incoming Transport Type）]	TLS
[発信転送タイプ（Outgoing Transport Type）]	TLS
[X.509 のサブジェクト名（X.509 Subject Name）]	リモート パーティのコモンネーム（CN）。次に例を示します。 • Unity Connection：us-cuc-ms.ent-pa.com（マルチサーバ証明書） • Cisco Meeting Server：cms.ent-pa.com（Cisco Meeting Server xmpp ドメイン名） • Expressway-C（Business-to-Business）：Expressway-C クラスタの CN • Cisco IOS Gateway および Cisco Unified Border Element：Cisco IOS Gateway と Cisco Unified Border Element により使用される CN のリスト • その他の Unified CM クラスタ：emea-cm-pub-ms.ent-pa.com（CallManager マルチサーバ証明書）
[着信ポート（Incoming Port）]	通常、5061 を入力します。Expressway への SIP トランクの場合、このプリファード アーキテクチャでは同一 Expressway クラスタでモバイルおよびリモート アクセス（MRA）と Business-to-Business（B2B）が有効であるため、Business-to-Business には異なるポートを使用します（ポート 5561 など）。

各 SIP トランクの設定では、C：表 7-12 に示す設定を使用します。

C：表 7-12　セキュア SIP トランクの SIP トランク設定

パラメータ	値
[SRTP を許可（SRTP Allowed）] このオプションが有効な場合、エンドツーエンド セキュリティを提供するため、ネットワークで暗号化 TLS を設定する必要があります。IPSec が設定されない場合、キーやその他の情報が公開されることになります。	選択（ボックスをオンにする）
[SIP 情報（SIP Information）] > [宛先（Destination）] - > [宛先ポート（Destination port）]	5061
[SIP トランク セキュリティ プロファイル（SIP Trunk security profile）]	前述の手順で作成した SIP トランク セキュリティ プロファイルを選択します。
[発信転送タイプ（Outgoing Transport Type）]	TLS

注　すべてのメッセージが暗号化されているわけではないため、Unified CM ノードと IM and Presence ノード間の Presence SIP トランクは、暗号化しないでください。

エンドポイントでのメディアおよびシグナリング暗号化

エンドポイントでメディアおよびシグナリング暗号化を設定するには、次の手順を実行します。

- SIP の OAuth トークンを有効にします (Jabber 用)。
- 混合モードを有効にします。
- メディアおよびシグナリング暗号化を有効にするため、暗号化モードで電話セキュリティ プロファイルを作成します。
- 電話セキュリティ プロファイルをエンドポイントに関連付け、MRA を介してのみ接続するエンドポイントを除き、電話機および TelePresence エンドポイントにローカルで有効な証明書 (LSC) をインストールします。

各手順の詳細については、以降の項で説明します。

SIP の OAuth トークンを有効にします

SIP に対して OAuth トークンを有効にすると、Jabber は LSC をインストールしたり、混合モードを有効にしたりせずに、メディアおよびシグナリングの暗号化を実行することができます。

SIP OAuth モードを有効にするには、次の CLI コマンドを入力します。

```
ユーティリティ sipOAuth モードの有効化
```

CallManager サービスを実行しているすべての統一された CM ノードで、このサービスを再起動します。混合モードを有効にする予定がある場合は、混合モードを有効にするまで、CallManager サービスの再起動を待っても構いません。

Jabber 使用する電話セキュリティ プロファイル

Unified CM クラスタの SIP OAuth モードを有効にした後、Jabber エンドポイントの電話セキュリティ プロファイルを作成します。

混合モードの有効化

混合モードを有効にする前に、Unified CM パブリッシャで CAPF サービスを有効にしておきます。混合モードを有効にした後で CAPF サービスを有効にする場合は、証明書信頼リスト（CTL）ファイルを更新する必要があります。

このドキュメントでは、CLI（コマンド ライン インターフェイス）（トークンレス）を使用して混合モードを有効にする方法を説明します。混合モードを有効にするには、次の手順を実行します。

- Unified CM パブリッシャに SSH で接続します。
- **utils ctl set-cluster mixed-mode** CLI コマンドを入力します。
- TFTP、CallManager、および CTIManager サービスを実行しているすべての Unified CM ノードで、これらのサービスを再起動します。

詳細については、次のリンク先にある『*Security Guide for Cisco Unified Communications Manager*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

CAPF オンライン CA モード

LSC エンドポイント証明書が外部 CA によって署名される CAPF オンライン CA モードを選択した場合は、次の手順を実行します。

1。 CA 証明書 (またはトラストチェーン) を、統一された CM CAPF トラストにインポートします。

2。 まだ実行していない場合は、CA サーバの IIS 証明書またはその CA 証明書 (または信頼チェーン) を統一された CM tomcat-trust にインポートします。

3。 一部の電話機または TelePresence エンドポイントが暗号化モードで設定されている場合は、CA 証明書 (または信頼チェーン) を Unified CM CallManager-trust にインポートします (まだ実行していない場合)。

4。 統一された CM パブリッシャで CAPF サービスパラメータを設定します。次の設定を使用します。

フィールド	設定
エンドポイントへの証明書発行者	オンライン CA
オンライン CA ホスト名	Microsoft IIS サービスによって使用される証明書内の共通名 (CN)。通常、これは FQDN です。
オンライン CA ポート	通常は 443
オンライン CA テンプレート	Microsoft CA で定義された証明書テンプレート名
オンライン CA タイプ	**Microsoft CA**
オンライン CA ユーザ名	上記で指定した証明書テンプレートを使用して証明書を発行するための適切な権限を持つユーザのユーザ名
オンライン CA パスワード	上記で指定した証明書テンプレートを使用して証明書を発行するための適切な権限を持つユーザのパスワード

5。 統一された CM パブリッシャで Cisco Certificate Enrollment Service をアクティブにします (まだ未設定の場合)。

6。 CAPF サービスを再起動します。

電話セキュリティ プロファイルと LSC のインストール

設定プロセスのこの時点で、サーバ証明書が生成され、Unified CM が混合モードになっています。

次に、エンドポイントでのメディアおよびシグナリング暗号化を有効にするため、[デバイス セキュリティ モード（Device Security Mode）] を [暗号化（Encrypted）] に設定して電話セキュリティ プロファイルを作成します。電話セキュリティ プロファイルには次の考慮事項が適用されます。

- 電話セキュリティ プロファイルの作成時には、[電話セキュリティ プロファイルのタイプ (Phone Security Profile Type)] として [ユニバーサル デバイス テンプレート（Universal Device Template）] を使用します。このタイプの電話セキュリティ プロファイルは特定の電話モデルに固有ではなく、すべての電話モデルに適用できます。これにより、設定と証明書管理がシンプルになります。電話モデルに固有の電話セキュリティ プロファイルの場合、新しいタイプの電話の追加時に、新しい電話セキュリティ プロファイルを作成する必要があります。また、MRA エンドポイントが新しい電話セキュリティ デバイス プロファイルを使用している場合は、この新しい電話セキュリティ デバイス プロファイル名を SAN として追加して、Expressway-C 証明書を再生成する必要があります。汎用電話セキュリティ プロファイルの場合、新しいデバイス タイプが追加されるたびに新しい電話セキュリティ プロファイルを作成することや、新しい Expressway-C 証明書を再生成することは不要です。

- 電話セキュリティ プロファイルは、MRA エンドポイントと非 MRA エンドポイントの両方に関連付けることができます。ただし、電話セキュリティ プロファイルが MRA エンドポイントに関連付けられている場合は、そのプロファイル名が FQDN 形式であることを確認してください。
- メディアおよびシグナリングの暗号化の使用が推奨されるため、[デバイス セキュリティ モード（Device Security Mode）] の設定を [暗号化（Encrypted）] に設定してください。
- TFTP 設定ファイルの暗号化を有効にするには、[TFTP 暗号化設定（TFTP Encrypted Config）] オプションを選択します（ボックスをオンにします）。「アーキテクチャー」で説明したように、オンプレミス エンドポイントに対し暗号化 TFTP 設定を有効にし、MRA 経由で接続するエンドポイントに対し暗号化 TFTP 設定を無効にすること（および機密情報が電話のページに入力されていないことを確認すること）が推奨されます。また、**TFTP 暗号化設定**では、エンドポイントに証明書がインストールされている必要があります (MIC または LSC)。
- Jabber エンドポイントで使用される電話セキュリティプロファイルの **OAuth 認証の有効化（Enable OAuth Authentication**）チェックボックスをオンにします (C：表 7-14 を参照)。
- 電話セキュリティ プロファイルは、エンドポイントが CAPF に接続するときに使用される認証モードも指定します。通常、認証モードとして [既存の証明書 (LSC を優先)（By Existing Certificate (precedence to LSC)）] を使用することが推奨されます。この設定では、エンドポイントに MIC のみが含まれている場合には既存の MIC が CAPF への認証に使用されます。エンドポイントに LSC が含まれている場合は、（MIC 証明書の有無にかかわらず）LSC が使用されます。したがって、これは MIC または LSC のいずれかが含まれているエンドポイントでは適切に機能します。

  エンドポイントに MIC と LSC が含まれていない場合、LSC がインストールされるまでは認証モードを使用できません。代わりに、最初の LSC インストールでは認証文字列またはヌル ストリングに基づく認証を使用する必要があります。認証文字列に基づく認証のほうが安全ですが、管理者が認証文字列をデバイス設定ページに入力し、ユーザがエンドポイントに認証文字列を手動で入力する必要があります。この操作が現実的ではない場合は、ヌル ストリングに基づく認証を選択できますが、この認証では、最初の CAPF 登録時にすべてのエンドポイント認証が実質的に迂回されます。LSC のインストールが完了したら、認証モードが [既存の証明書 (LSC を優先)（By Existing Certificate (precedence to LSC)）] の電話セキュリティ プロファイルを割り当てる必要があります。
- 電話セキュリティ プロファイルの [キー順序（Key Order）] 設定で [RSA のみ（RSA Only）] を選択し、[RSA キー サイズ（RSA Key Size）] 設定で [2048] 以上を選択します。

上記の事項を考慮して、3 つの電話セキュリティ プロファイルを作成します。C：表 7-13 に、各プロファイルの相違点を示します。その他の設定には、前述の値を使用します。

C：表 7-13　　設定する電話セキュリティ プロファイル

電話セキュリティ プロファイル名の例	認証モード（CAPF 登録）	TFTP 暗号化設定ファイル	OAuth 認証
UDT-Encrypted-LSC-TFTPenc.ent-pa.comf	既存の証明書（LSC の優先）	イネーブル	無効
UDT-Encrypted-LSC.ent-pa.com	既存の証明書（LSC の優先）	無効	ディセーブル
UDT-Encrypted-NullString.ent-pa.com	Null 文字列または 認証ストリング	無効	ディセーブル
UDT-Jabber-SIPOAuth	Null 文字列または 認証ストリング	無効	イネーブル

3 つの電話セキュリティ プロファイルの設定が完了したら、**Cisco Unified CM の管理 > デバイス > 電話**に移動し、これらのプロファイルをエンドポイントに関連付け、エンドポイントのタイプに応じて LSC のインストールに進みます。C：表 7-14 に、エンドポイントのタイプ別の実行アクションを示します。

C：表 7-14　電話セキュリティ プロファイルの関連付けと LSC のインストール

エンドポイントのタイプ	手順（電話セキュリティ プロファイルの関連付けと LSC のインストール）
Cisco IP Phone および Cisco TelePresence エンドポイント (MIC 対応)	• **UDT-Encrypted-LSC-TFTPenc.ent-pa.com**（TFTP 設定ファイルの暗号化用）または **UDT-Encrypted-LSC.ent-pa.com**（TFTP 設定ファイルの暗号化なしの場合）をエンドポイントに関連付けます。 • LSC をインストールします。
Jabber クライアント (オンプレミスまたは MRA)	• **UDT-Jabber-SIPOAuth の関連付け**
MRA ハードウェア エンドポイント	• **UDT-Encrypted-NullString.ent-pa.com の関連付け**

電話セキュリティ プロファイルを電話に関連付けるには、電話の設定ページに移動し、[デバイス セキュリティ プロファイル（Device security profile）] 設定で必要なセキュリティ プロファイルを選択します。

LSC のインストールを設定するには、電話の設定ページの [証明書の操作（Certificate Operation）] フィールドで [インストール / アップグレード（Install/Upgrade）] を選択します。電話の設定ページの [Certification Authority Proxy Function（CAPF）の情報（Certification Authority Proxy Function (CAPF) Information）] セクションには、電話セキュリティ プロファイルの CAPF 情報が自動的に取り込まれます。[操作の完了期限 (Operation Completes By)] フィールドがまだ設定されていない場合には、このフィールドを将来の日付に更新する必要があります。

電話セキュリティ プロファイルの関連付けと LSC インストールの設定（オプション）が完了したら、設定を保存します。設定を適用するか、またはエンドポイントをリセットします。この時点で、電話セキュリティ プロファイルが適用されます。LSC インストールを設定した場合、エンドポイントが LSC を取得します。（認証文字列を使用する場合は、LSC インストールを続行するためにユーザが [更新（Update）] ボタンを押す必要があることがあります。）また、エンドポイントでメディアおよびシグナリング暗号化も設定する必要があります。

Tip　電話セキュリティ プロファイルの割り当てと CAPF 登録の実行には、Cisco Unified Communications Manager 一括管理ツール（BAT）または Cisco Prime Collaboration プロビジョニングを使用できます。

通常、Jabber エンドポイントに LSC をインストールする必要はありません。SIP OAuth モードが有効になっている場合、暗号化されたメディアとシグナリングを実行するために、Jabber は LSC を必要としません。TFTP 設定ファイルの暗号化をサポートするために、Jabber は引き続き LSC を必要とします。ただし Jabber で LSC 証明書を管理するには、追加の管理オーバーヘッドが必要になるため、通常は Jabber エンドポイントで TFTP 設定ファイルの暗号化を展開することは推奨されません。したがって、Jabber に LSC 証明書をインストールする必要はありません。

Survivable Remote Site Telephony（SRST）の有効化

Survivable Remote Site Telephony（SRST）では、次の手順を使用します。

- エンタープライズ CA を使用して、SRST ルータの証明書に署名します。Cisco IOS ルータでの証明書の管理の詳細については、「Cisco IOS Gateway と Cisco Unified Border Element」を参照してください。
- SRST が LSC を認証できるように、エンドポイント LSC に署名したエンティティに対応する信頼証明書を SRST ルータにインポートします。CAPF を使用して LSC を発行する場合、これが CAPF 証明書となります。外部 CA を使用して LSCs を発行する場合、これが CA 証明書 (または信頼チェーン証明書) となります。
- **SRST はセキュアか？**をオンにする（チェックボックスをオンにする）ことで、セキュア SRST が有効になったことを確認します。**Cisco Unified CM の管理 > システム > SRST** の SRST リファレンス設定で、

詳細については、次のリンク先にある『*Security Guide for Cisco Unified Communications Manager*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Cisco Unity Connection

ここでは次世代暗号化（NGE）を使用した Cisco Unity Connection のメディアおよびシグナリング暗号化について説明します。この暗号化では、Unity Connection のルート証明書および SIP 証明書の代わりに Unity Connection tomcat 証明書が使用されます。

Unity Connection でメディアおよびシグナリングのために NGE を有効にする全体的な手順は次のとおりです。

- Unity Connection で証明書を管理します。
- Unity Connection でテレフォニー統合のために暗号化を設定します。
- Unified CM で、Unity Connection への SIP トランクの暗号化を有効にします。

最初に Unity Connection で証明書を管理します。Unity Connection で次の手順を実行します。

- Unity Connection パブリッシャ ノードで、ルート CA 証明書（または証明書チェーン）を Unity Connection tomcat-trust ストアにアップロードします。同様に、ルート CA 証明書を CallManager-trust ストアにアップロードします（CA 署名付き CallManager 証明書に必要です）。これらの証明書は、Unity Connection サブスクライバ ノードの信頼ストアに自動的に反映されます。
- Unity Connection パブリッシャ ノードで、マルチサーバ tomcat 証明書を取得してエンタープライズ CA により署名するため、CSR を発行します。たとえば、コモンネームが us-cuc-ms.ent-pa.com であるとします。X509v3 キー使用法拡張機能は、デジタル署名、キーの暗号化、およびデータの暗号化です。X509v3 拡張キー使用法拡張機能は、TLS Web サーバ認証および TLS Web クライアント認証です。これはマルチサーバ証明書であるため、この証明書を Unity Connection パブリッシャにインストールすると、自動的に Unity Connection サブスクライバにもインストールされます。この新しい tomcat 証明書のインストールが完了したら、両方の Unity Connection ノードで Tomcat Service を再起動します。

CA 証明書のアップロードまたは CA 署名付き tomcat 証明書の発行の詳細については、「Cisco Unified CM および IM と Presence」を参照してください。手順は Unity Connection の場合と同じです。

Cisco Unified CM と Unity Connection で同じ CA を使用することを前提としているため、Unified CM tomcat-trust ストアに CA 証明書をインポートする必要はありません。この証明書はすでにこの信頼ストアに格納されているはずです。

次に、Unity Connection で暗号化を設定にします。

- **Cisco Unity Connection 管理 > テレフォニー統合 > セキュリティ > SIP セキュリティ プロファイル**で、次の設定を使用して新しい SIP セキュリティ プロファイルを作成します。

フィールド	設定
ポート	5061
TLS を実行（Do TLS）	チェックボックスをオンにする

  この SIP セキュリティ プロファイルには、表示名 **5061/TLS** が自動的に割り当てられます。

- **テレフォニー統合 > ポート グループ**から、ポート グループ **PhoneSystem-1** を選択し、次の設定を使用してポート グループを変更します。

フィールド	設定
SIP セキュリティ プロファイル（SIP Security Profile）	前の手順で作成した SIP セキュリティ プロファイル（**5061/TLS**）を選択する
次世代暗号化の有効化（Enable Next Generation Encryption）	チェックボックスをオンにする
セキュア RTP（Secure RTP）	チェックボックスをオンにする

- [ポート グループ（Port Group）] ページで [編集（Edit）] > [サーバ（Servers）] に移動します。SIP サーバの設定で、TLS ポートとして 5061 が設定されていることを確認します。TFTP サーバの設定で、Unified CM TFTP サーバが設定されていることを確認します。このようにして、ポート グループがリセットされると、Unity Connection の CallManager-trust ストアに CallManager 証明書が自動的にダウンロードされます。

次に、Unity Connection への Unified CM SIP トランクで暗号化を有効にします。

- 暗号化と適切な X.509 サブジェクト名が設定された SIP トランク セキュリティ プロファイルがすでに作成されている必要があります（C：表 7-11 を参照）。Unity Connection への SIP トランクに対しこの SIP トランク セキュリティ プロファイルを選択します。

この時点で、Unified CM では暗号化 SIP トランクが完全に動作するはずです。電話からボイスメール ポートへの接続時には、メディアおよびシグナリングも暗号化される必要があります。LDAP over SSL も設定する必要があります。[Cisco Unity Connection の管理（Cisco Unity Connection Administration）] > [システム設定（System Settings）] > [LDAP] に移動し、[LDAP ディレクトリの設定（LDAP Directory Configuration）] ページと [LDAP 認証（LDAP Authentication）] ページで、[TLS を使用（Use TLS）] を選択し、ポート 636 を設定します（Unified CM での LDAP over SSL の設定と同様）。

コラボレーション エッジ

ここでは、Cisco Expressway、Cisco IOS Gateway、および Cisco Unified Border Element での証明書の管理と暗号化の導入の概要を説明します。

Cisco Expressway

ここでは、0、次に暗号化に使用する設定について説明します。

Cisco Expressway 証明書の管理

「アーキテクチャー」で説明したように、Cisco Expressway ソフトウェアの新規インストールには、信頼された一時 CA と、その一時 CA が発行するサーバ証明書が付属しています。一時 CA 証明書を、信頼する CA 証明書に置き換え、Expressway の CA 署名付き証明書を生成します。「アーキテクチャー」で説明したように、Expressway-C 証明書経の署名にはエンタープライズ CA を使用し、Expressway-E 証明書への署名にはパブリック CA を使用します。Expressway-E でサポートされているパブリック CA のリストについては、cisco.com にあるエンドポイントに関するドキュメントを参照してください。たとえば、次の Web サイトから入手できる『*Certificate Authority Trust List*』を参照してください。
https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html.

Cisco Expressway の証明書の管理を導入するには、以降の項で説明する手順を使用します。

CA ルート証明書をアップロードする。

[信頼された CA 証明書（Trusted CA certificate）] ページに移動します（[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼された CA 証明書（Trusted CA certificate）]）。このページで、既存の証明書を新しいルート CA 証明書または証明書チェーンに置き換えます。これ以降の CA 証明書は、既存の CA 証明書リストに追加されます。C：表 7-15 に示されている CA 証明書をアップロードします。この操作は、Expressway-C クラスタと Expressway-E クラスタの両方の各 Expressway ノードで行う必要があります。

C：表 7-15　Cisco Expressway 信頼ストア

Expressway-C 信頼ストア	Expressway-E 信頼ストア
• Expressway-E 証明書を署名したパブリック CA からのルート CA 証明書 • Unified CM CallManager 証明書と Expressway-C 証明書に署名するエンタープライズ CA からのルート CA 証明書（または証明書チェーン）	• Expressway-E 証明書を署名したパブリック CA からのルート CA 証明書（または証明書チェーン） • Unified CM CallManager 証明書と Expressway-C 証明書に署名するエンタープライズ CA からのルート CA 証明書 • Business-to-Business（B2B）コミュニケーションまたはクラウド コミュニケーションでは、他のビジネスのルート CA 証明書

各 Expressway ノードの証明書署名要求（CSR）を生成する。

1。 **メンテナンス > セキュリティ > サーバ証明書**に移動します。

2。 CSR を作成します。

IM and Presence のチャット ノード エリアスのサブジェクト代替名（SAN）拡張は自動的に追加されます。Expressway ノードが Expressway-C ノードまたは Expressway-E ノードのいずれであるかと、導入されている機能によっては、SAN 拡張の追加が必要となることがあります。詳細については、C：表 7-16 を参照してください。

C：表 7-16　CSR に追加するサブジェクト代替名（SAN）

サブジェクト代替名（SAN）として追加する項目	次の目的で CSR を生成する場合に追加する：		
	モバイル & リモート アクセス	**XMPP フェデレーション**	**Business-to-Business（B2B）コール**
Expressway-C クラスタ名	Expressway-C でのみ	Expressway-C でのみ	Expressway-C でのみ
Unified CM 登録ドメイン[1]	Expressway-E でのみ必要	–	–
XMPP フェデレーション ドメイン	–	Expressway-E でのみ必要	–
IM and Presence のチャット ノード エイリアス（フェデレーテッド グループ チャット）	–	Expressway-C と Expressway-E の両方で必要	–
Unified CM 電話セキュリティ プロファイル名（FQDN 形式）[2]	Expressway-C でのみ必要	–	–

1. Expressway 設定と Expressway-E 証明書で使用されている Unified CM 登録ドメインは、サービス検出中に MRA クライアントが _collab-edge DNS SRV レコードを検索するときに使用するドメインです。Unified CM 登録ドメインにより、Unified CM での MRA 登録が有効になります。この例では、これらのドメインは Unified CM で SIP URI に使用されているドメインと一致します。ただしこれらのドメインは主にサービス検出用であるため、Unified CM で使用される SIP ドメインと一致する必要はありません。
2. SIP OAuth が使用されるため、SAN の Jabber に使用される電話セキュリティプロファイル名を、Expressway-C 証明書に追加する必要はありません（C：表 7-14 を参照）。

詳細については、次のリンク先にある『*Cisco Expressway Certificate Creation and Use Deployment Guide*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

前述したように、操作を簡単にするため、ユニバーサル デバイス テンプレート（UDT）の使用が推奨されます。これにより、Expressway-C SAN で電話セキュリティ プロファイル名の長いリストを入力する必要がなくなります。この章の例では、CSR の [Unified CM Phone セキュリティ プロファイル名（Unified CM phone security profile names）] フィールドに、UDT-Encrypted-LSC-TFTPenc.ent-pa.com、UDT-Encrypted-RSA-LSC.ent-pa.com、および UDT-Encrypted-AuthString.ent-pa.com（または UDT-Encrypted-NullString.ent-pa.com）を入力します。

3。 CSR をダウンロードして CA に送信します。これにより、CA 署名付き証明書を発行できるようになります。Base 64 形式を使用します。C：表 7-17 に示すように、CSR の X509v3 キー使用法と X509v3 拡張キー使用法が CA から発行される証明書に含まれています。

C：表 7-17　Cisco Expressway のキー使用法と拡張キー使用法

証明書	X509v3 キー使用法	X509v3 拡張キー使用法
Expressway-C および Expressway-E	デジタル署名、キーの暗号化	TLS Web サーバー認証、TLS Web クライアント認証

4。 新規証明書のアップロード

Cisco Expressway の暗号化設定

MRA および XMPP フェデレーション

Expressway-C の Unified Communications ゾーンには TLS が使用されます。すべての Unified Communications サービス（Unified CM サーバ、IM and Presence Service ノード、Unity Connection）の [TLS 検証（TLS Verify）] が [オン（On）] に設定されていることを確認します。Unified Communications サービス ノードの検出を実行するときにこの設定を行います（[設定（Configuration）] > [Unified Communications]）。これにより、Expressway-C ノードが Unified Communications ノードの証明書を検証します。

Expressway-C と Expressway-E の間の Unified Communications トラバーサル ゾーンは、TLS 証明書検証を有効にし、メディア暗号化を設定して暗黙に設定されます。Expressway-C MRA トラバーサル ゾーンで [認証ポリシー（Authentication policy）] を [クレデンシャルを確認しない（Do not check credentials）] に設定します。Expressway-E MRA トラバーサル ゾーンで [認証ポリシー（Authentication policy）] を [クレデンシャルを確認しない（Do not check credentials）] に設定し、Expressway-C 証明書のクラスタ名（Expressway-C 証明書に SAN として追加）と一致する TLS 検証サブジェクト名を入力します。

MRA エンドポイントと Expressway-C 間のメディアおよびシグナリング トラフィックは常に暗号化されます。社内ネットワーク内部のコール レッグ（Expressway-C と Unified CM の間のシグナリングと、Expressway-C と内部エンドポイント間のメディア）を暗号化するため、暗号化モードの電話セキュリティ プロファイルを使用して MRA エンドポイントとネットワーク内部のエンドポイントを設定します。このようにすると、メディアとシグナリングがエンドツーエンドで暗号化されます（すべてのコール レッグが暗号化されます）。

XMPP フェデレーションでは、[セキュリティ モード（Security mode）] を [TLS（必須）（TLS Required）] に設定することが推奨されます。ただし、[TLS（オプション）（TLS optional）] に設定する必要があるケースがあります。たとえば [TLS（必須）（TLS Required）] は Cisco Webex Messenger でサポートされていないため、Cisco Webex Messenger を使用する企業との XMPP フェデレーションがある場合は [TLS（オプション）（TLS Optional）] を使用する必要があります。このシナリオでは、[クライアント側のセキュリティ証明書が必要（Require Client-side security certificates）] を [オフ（Off）] に設定する必要もあります。

Business-to-Business（B2B）コミュニケーション

「アーキテクチャー」で説明したように、Call Processing Language（CPL）ルールを設定します。

また、Expressway-C の Unified CM ネイバー ゾーンには C：表 7-18 に示す推奨設定を使用します。

C：表 7-18　Expressway-C Business-to-Business（B2B）Unified CM ネイバー ゾーンの設定

フィールド	設定
ポート	MRA と Business-to-Business（B2B）が同一 Expressway クラスタで有効になっている場合は、5061 以外のポート（ポート 5561 など）を使用します。
トランスポート（Transport）	TLS
TLS 検証（TLS Verify）	オン
メディア暗号化（Media Encryption）	ベストエフォート型

Expressway-C のトラバーサル ゾーンには、C：表 7-19 に示す推奨設定を使用します。

C：表 7-19　Expressway-C Business-to-Business（B2B）トラバーサル ゾーンの設定

フィールド	設定
ポート	5060、5061、およびその他のトラバーサル ゾーンで使用されているポート以外のポートを設定する必要があります。たとえば範囲 7*xxx* のポートを使用します。
トランスポート（Transport）	TLS
TLS 検証（TLS Verify）	オン
メディア暗号化（Media Encryption）	Auto

Expressway-E のトラバーサル ゾーンには、C：表 7-20 に示す推奨設定を使用します。

C：表 7-20　Expressway-E Business-to-Business（B2B）トラバーサル ゾーンの設定

フィールド	設定
ポート	Expressway-C でのトラバーサル ゾーンのポートと同じポート
トランスポート（Transport）	TLS
TLS 検証（TLS Verify）	オン
TLS 検証サブジェクト名（TLS Verify subject name）	Expressway-C クラスタ名の SAN
メディア暗号化（Media Encryption）	ベストエフォート型

Expressway-E のデフォルト ゾーン（着信コール）には、C：表 7-21 に示す推奨設定を使用します。

C：表 7-21　Expressway-E デフォルト ゾーンの設定

フィールド	設定
デフォルト ゾーンで相互 TLS を有効にする（Enable Mutual TLS on Default Zone）	オフ
認証ポリシー（Authentication policy）	クレデンシャルを確認しない
メディア暗号化（Media Encryption）	ベストエフォート型

Expressway-E の DNS ゾーン（発信コール）には、C：表 7-22 に示す推奨設定を使用します。

C：表 7-22　Expressway-E DNS ゾーンの設定

フィールド	設定
TLS 検証（TLS Verify）	オフ
メディア暗号化（Media Encryption）	ベストエフォート型

この時点で、Unified CM に SIP トランク セキュリティ プロファイルがすでに作成されている必要があります。詳細については、C：表 7-11 を参照してください。

Cisco IOS Gateway と Cisco Unified Border Element

ここでは最初に証明書の管理について説明し、続いて暗号化の設定について説明します。

証明書の管理

Cisco IOS Gateway と Cisco Unified Border Element（CUBE）でも、CA 署名付き証明書の使用が推奨されます。

証明書はさまざまな方法でアップロードできます。次の手順は、端末を使用した手動での証明書の登録に基づいています。証明書は PEM（Base 64）形式です。

1。 RSA キーペアを作成します。

例：**crypto key generate rsa general-keys label CUBE modulus 2048**

2。 Cisco Unified Border Element（CUBE）の PKI トラストポイントを作成します。

たとえば、端末を使用した手動での登録の場合は次のようにします。

```
crypto pki trustpoint CUBE-Certificate
 enrollment terminal pem
 subject-name CN=US-CUBE1.ent-pa.com
 revocation-check none
 rsakeypair CUBE
 hash sha256
```

3。 CA を使用してトラストポイントを認証し、CA 証明書を受け入れます。

基本的には、これによりそのトラストポイントの CA 証明書がアップロードされます。

例：**crypto pki authenticate CUBE-Certificate**

次に PEM 形式の CA 証明書を貼り付けます。

4。 CA サーバにトラストポイントを登録します。基本的には、これにより証明書署名要求（CSR）が作成されます。

例：**crypto pki enroll CUBE-Certificate**

この手順では、ルータのシリアル番号または IP アドレスをサブジェクト名に追加する必要はありません。

5。 この CSR に CA で署名します。

クライアントおよびサーバ Web 認証（X509v3 拡張キー使用法の TLS Web クライアント認証と TLS Web サーバ認証）のための CA テンプレートを使用します。

6。 生成された証明書を Cisco ゲートウェイにインポートします。

たとえば、端末を使用して PEM 形式の証明書を手動でインポートする場合は次のようにします。**crypto pki import CUBE-Certificate certificate**

Unified CM 証明書に CA による署名が付いていない場合、新しいトラストポイントを使用して、すべての Unified CM コール処理サブスクライバ ノードの Unified CM CallManager 証明書を、Cisco IOS Gateway および Cisco Unified Border Element（CUBE）にインポートする必要があります。

証明書の管理が完了したら、暗号化の設定に進みます。

暗号化設定

次の手順に従ってください。

1。 トラストポイントを Cisco IOS 音声プロセスに関連付けます。

次に例を示します。

```
sip-ua
 crypto signaling remote-addr [UnifiedCMIPaddress1] [mask] trustpoint
 CUBE-Certificate
 crypto signaling remote-addr [UnifiedCMIPaddress2] [mask] trustpoint
 CUBE-Certificate
```

2。 ダイヤルピアに対して TLS トランスポートを有効にします。

次に例を示します。

```
dial-peer voice 300 voip
 session protocol sipv2
 session transport tcp tls
```

3。 セキュア シグナリングを有効にします。

たとえば特定のデバイスとの間でのセキュア シグナリングを有効にするには、次のように設定します。

```
sip-ua
 crypto signaling remote-addr [UnifiedCMIPaddress1] [mask] trustpoint CUBE-Certificate
 crypto signaling remote-addr [UnifiedCMIPaddress2] [mask] trustpoint CUBE-Certificate
```

4。 SRTP を有効にします。

Cisco IOS Gateway と Cisco Unified Border Element（CUBE）では、AES_CM_128_HMAC_SHA1_80 と AES_CM_128_HMAC_SHA1_32（デフォルト）がサポートされています。AES_CM_128_HMAC_SHA1_80 を有効にするには、次のように設定します。

```
voice service voip
  sip
    srtp-auth sha1-80
```

SRTP パススルーでは、送信元デバイスと宛先デバイスの間でより強力な暗号を使用でき、Cisco Unified Border Element はパケットを転送するだけで処理は行いません。**srtp passthru** を設定するには、次のように設定します。

```
voice service voip
  srtp pass-thru
```

会議

ここでは、Cisco Meeting Server と Cisco TelePresence Management Suite（TMS）を会議サービス用に展開する方法を説明します。

Cisco Meeting Server

Cisco Meeting Server には、証明書管理用の Web インターフェイスがありません。証明書の管理には、メインボード管理プロセッサ（MMP）コマンドを使用します。

次に、Cisco Meeting Server 証明書を生成およびインストールする全体的な手順を示します。

- すべてのサービスを対象とする 1 つの CSR（および秘密キー）を生成します。この CSR で、SAN 拡張の CN フィールドに XMPP ドメインを指定します。また、SAN 拡張ですべての Cisco Meeting Server ノードの FQDN を指定します。SFTP 経由で秘密キーをダウンロードします。エンタープライズ CA で CSR を署名します。拡張キー使用法 [サーバ認証（Server Authentication）] と [クライアント認証（Client Authentication）] が存在していることを確認します。このドキュメントでは、この証明書を*共有証明書*と呼びます。
- ローカル データベースなしで Call Bridge サービスを実行する Cisco Meeting Server を導入するには、**CN=postgres** を使用してデータベース クライアントに CSR（および秘密キー）を生成します。SFTP 経由で秘密キーをダウンロードします。エンタープライズ CA で CSR を署名します。拡張キー使用法 [クライアント認証（Client Authentication）] が存在していることを確認します。
- 新しい共有 CA 署名付き証明書（および関連付けられている秘密キー）と CA 証明書を SFTP 経由ですべての Cisco Meeting Server ノードにアップロードします。また、新しいデータベース クライアント CA 署名付き証明書（および関連付けられている秘密キー）を、ローカル データベースなしで Call Bridge サービスを実行している Cisco Meeting Server ノードにアップロードします。
- 証明書をインストールします。
  - Web 管理画面：このサービスを実行する各ノードで、このサービスを無効にし、共有証明書と関連秘密キーをインストールし、サービスを有効にします。
  - Call Bridge：このサービスを実行する各ノードで、共有証明書と関連秘密キーをインストールし、サービスを再始動します。
  - XMPP：このサービスを実行する各ノードで、このサービスを無効にし、共有証明書と関連秘密キーをインストールし、サービスを有効にします。
  - Web Bridge：このサービスを実行する各ノードで、共有証明書、関連秘密キー、および CA 証明書をインストールし、サービスを再始動します。
  - データベース サーバ：ローカル データベースが存在する各ノードで、データベース クラスタリングが有効になっていないことを確認してから、共有証明書と関連秘密キーをインストールします。この操作が完了したら、ノード間のクラスタリング構成を有効にできます。
  - データベース クライアント：Call Bridge サービスを実行し、ローカル データベースがない各ノードで、データベース クラスタリングが有効になっていないことを確認してから、データベース クライアント証明書と関連秘密キーをインストールします。この操作が完了したら、ノード間のクラスタリング構成を有効にできます。

以降の項では、上記の手順の例を示します。これらの例では、エンタープライズ CA により署名された共有 Cisco Meeting Server 証明書が CAsignedCluster.cer、これに対応する秘密キーが CAsignedCluster.key、ルート CA 証明書が rootCAcert.cer です。

CSR を生成する。

データベース クライアント証明書：

```
pki csr dbclusterclient CN:postgres
```

共有証明書：

```
pki csr CAsignedCluster CN:cms.ent-pa.com OU:"TME" O:"Cisco" L:"San Jose"
ST:CaliforniaC:USsubjectAltName:us-acano1.ent-pa.com,us-acano2.ent-pa.com,us-cmsdb.ent
-pa.com,us-cmscb.ent-pa.com, cms.ent-pa.com
```

さまざまなサービスと Cisco Meeting Server ノードの証明書をインストールする。

Web 管理画面サービスを実行する各ノードで次のようにします。

```
webadmin disable
webadmin certs CAsignedCluster.key CAsignedCluster.cer
webadmin enable
```

Call Bridge サービスを実行する各ノードで次のようにします。

```
callbridge certs CAsignedCluster.key CAsignedCluster.cer
callbridge restart
```

XMPP サービスを実行する各ノードで次のようにします。

```
xmpp disable
xmpp certs none
xmpp certs CAsignedCluster.key CAsignedCluster.cer
xmpp enable
```

Web Bridge サービスを実行する各ノードで次のようにします。

```
webbridge disable
webbridge certs CAsignedCluster.key CAsignedCluster.cer
webbridge trust rootCAcert.cer
webbridge enable
```

ローカル データベースが存在している各ノードで次のようにします。

```
database cluster certs CAsignedCluster.key CAsignedCluster.cer dbclusterclient.key
dbclusterclient.cer rootCAcert.cer
```

Call Bridge サービスを実行しているがローカル データベースがない各ノードで次のようにします。

```
database cluster certs dbclusterclient.key dbclusterclient.cer rootCAcert.cer
```

詳細については、次のリンク先にある『*Cisco Meeting Server, Certificate Guidelines for Scalable and Resilient Server Deployments*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html

Unified CM で、X.509 サブジェクト名の Cisco Meeting Server XMPP ドメイン名、TLS、および暗号化を使用して、SIP トランク セキュリティ プロファイルが設定されていることを確認します。詳細については「SIP トランクの暗号化」を参照してください。この SIP トランク セキュリティ プロファイルを、Call Bridge サービスを実行している CMS ノードへのすべての SIP トランクに関連付けます。

Cisco Meeting Management

Cisco Meeting Management は、デフォルトで自己署名証明書を使用してインストールされます。

DRreceiveraddress と、ユーザがブラウザインターフェイスに使用するアドレスを使用して、CA 署名付き証明書を生成します。

秘密キーと証明書は、次の手順を実行して、Cisco Meeting Management の外部で作成されます。

1。 次のコマンドを使用して秘密キーを生成します。

```
openssl genrsa -out privatekey.pem 2048
```

2。 step 1 の秘密キーを使用して、証明書署名要求（CSR）を生成します。

```
openssl req -new -key us-cmm-privatekey.pem -out us-cmm-certcsr.pem
```

3。 要求されたデータ（国、都道府県または地域、組織名など）を入力します。

4。 社内の認証局（CA）による署名を受けるため、Cisco Meeting Management 証明書署名要求ファイル **us-cmm-certcsr.pem** を送信します。CA から署名付き証明書 **us-cmm.cer** を受け取ります。

5。 秘密キーと証明書をアップロードします。

6。 Cisco Meeting Management を再起動します。

Cisco TelePresence Management Suite

秘密キーと証明書は、Cisco TelePresence Management Suite（TMS）外部で作成されます。この操作は、たとえば次のハイレベルな手順に従って、OpenSSL で実行することができます。

1。 次のコマンドを使用して秘密キーを生成します。

```
openssl genrsa -out us-tms1-privatekey.pem 2048
```

2。 上記の秘密キーを使用して、証明書署名要求（CSR）を生成します。

```
openssl req -new -key us-tms1-privatekey.pem -out us-tms1-certcsr.pem
```

3。 要求されたデータ（国、都道府県または地域、組織名など）を入力します。

4。 社内の認証局（CA）による署名を受けるため、TMS 証明書署名要求ファイル us-tms1-certcsr.pem を送信します。CA から署名付き証明書 us-tms1.cer を受け取ります。

5。 署名付き証明書を秘密キーと結合します。

```
openssl pkcs12 -export -inkey us-tms1-privatekey.pem -in us-tms1.cer -out
us-tms1-cert-key.p12 -name us-tms1-cert-key
```

6。 TMS でルート CA 証明書を証明機関の信頼ストアにインポートします。また、新しい TMS 証明書とその関連秘密キーをパーソナル信頼ストアにインポートします。

7。 Microsoft 管理コンソール（MMC）と証明書スナップインで、インポートした証明書を選択し、右クリックして [すべてのタスク（All Tasks）] > [秘密キーの管理（Manage Private Keys）] を選択します。TMS により使用されるユーザに、読み取り権限および完全アクセス権限を付与します（ほとんどの場合、これは SERVICE ユーザと NETWORK SERVICE ユーザです）。

8。 TMS ツールに移動し、[セキュリティ設定（Security Settings）] > [TLS 証明書（TLS Certificates）] で新しい証明書を選択します。

9。 IIS に移動し、新しい証明書へのバインドを設定します。

10。IIS サービスと TMS サービスを再起動します。

詳細については、次のリンク先にある『*Cisco TelePresence Management Suite Administrator Guide*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html

また、次のリンク先にある『*TMS Certificates with TMS Tools for TLS Communication Configuration Example*』も参照してください。
https://www.cisco.com/c/en/us/support/docs/conferencing/telepresence-management-suite-tms/118723-configure-tms-00.html.

コラボレーション管理サービス

Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment には、プラットフォームを管理するためのグラフィカル ユーザ インターフェイス（GUI）がありません。CA 署名付き証明書を発行するには、CLI（コマンド ライン インターフェイス）に移動して CSR を発行します。CSR を生成するには CLI コマンド **set csr gen tomcat** を使用し、PEM 形式で CSR を表示するには **show csr own tomcat /tomcat.csr** を使用します。CA 証明書または下位 CA 証明書をインポートするには **set cert import trust tomcat** を使用し、tomcat 証明書をインポートするには **set cert import own tomcat tomcat-trust/**<*tomcat-certificate-name*> を使用します。

Tomcat Service を再起動するには、**utils service restart Cisco Tomcat** というコマンドを入力します。

Cisco Prime Collaboration Provisioning

証明書の操作は、[管理（Administration）] > [更新（Updates）] > [SSL 証明書（SSL Certificates）] で実行できます。[CSR の生成（Generate CSR）] をクリックして CSR を生成します。

使用するパラメータは、[キータイプ（Key Type）] が [RSA]、[キー長（Key length）] が [2048]、[ハッシュ アルゴリズム（Hash Algorithm）] が [SHA-256] です。エンタープライズ ルート CA で CSR に署名します。

[アップロード（Upload）] をクリックして CA 署名付き PCP 証明書と LDAP 証明書をアップロードします。

その後、GUI または CLI で Apache を再起動します。

詳細については、次のリンク先にある『*Cisco Prime Collaboration Provisioning Guide - Standard and Advanced*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-user-guide-list.html

マルチクラスタに関する考慮事項

マルチクラスタ導入では、すべてのクラスタが同一データセンター内にない場合、クラスタ間リンクの暗号化を有効にします。

SIP トランクについては、CallManager に CA 署名付き証明書を使用することが推奨されており、また複数のクラスタに同一 CA が使用されていることを前提としていることから、クラスタ間で CallManager 証明書または CA 証明書を交換する必要はありません。

ILS 暗号化を有効にするには、認証に TLS 証明書を使用し、承認にパスワードを使用することが推奨されます。Unified CM ILS 設定ページで、[TLS 証明書の使用（Use TLS Certificates）] オプションを選択し（チェックボックスをオン）、[パスワードの使用（Use Password）] オプションを選択して（チェックボックスをオン）、Unified CM クラスタ間で共有するパスワードを入力します。エンタープライズ CA により署名された tomcat s 証明書と、すでに tomcat 信頼ストアに格納されているエンタープライズ ルート CA 証明書（または証明書チェーン）では、証明書の ILS 暗号化を有効にするために追加の操作を行う必要はありません。

LBM 暗号化を有効にするには、単に Unified CM エンタープライズ パラメータ [LBM セキュリティ モード（LBM Security Mode）] を [セキュア（Secure）] に設定します。ここでもまた、エンタープライズ CA により署名された tomcat 証明書と、すでに tomcat 信頼ストアに格納されているエンタープライズ ルート CA 証明書では、証明書の LBM 暗号化を有効にするために追加の操作を行う必要はありません。

帯域幅管理

改訂日：2019 年 2 月 19 日

この章では、Cisco Enterprise Collaboration 向けプリファード アーキテクチャ（PA）での帯域幅管理戦略について説明します。

導入に際して、PA 設計ガイドラインおよび推奨事項以外の特定の要件が課せられることがあります。その場合は、それらの要件に応じてアーキテクチャをカスタマイズするために、Cisco Collaboration SRND や関連する製品のマニュアルなど、他のマニュアルを使用しなければならない場合があります。

この章の前半では、アーキテクチャについて概説し、いくつかの基本的な設計概念を紹介します。後半では、導入手順を説明します。「アーキテクチャー」では、識別と分類、キューイングとスケジューリング、プロビジョニングとアドミッション制御などのトピックについて、本書で一貫して使用している架空のカスタマー トポロジの例に基づいて説明します。次の項は「帯域幅管理の導入」です。特定の設計に関する決定の背景について、概念の抽象的な説明よりも明確に理解できるよう、具体的な導入例を紹介します。「帯域幅管理の導入」でのトピックの順番は、推奨される設定順に対応しています。

この章の新規情報とは

C：表 8-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

C：表 8-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
ビデオ トラフィックのマーキング。優先順位付けされたビデオの場合は AF41 として、状況対応型ビデオの場合は AF42 としてマーキングします。	この章の各項で説明	2017 年 8 月 30 日

コア コンポーネント

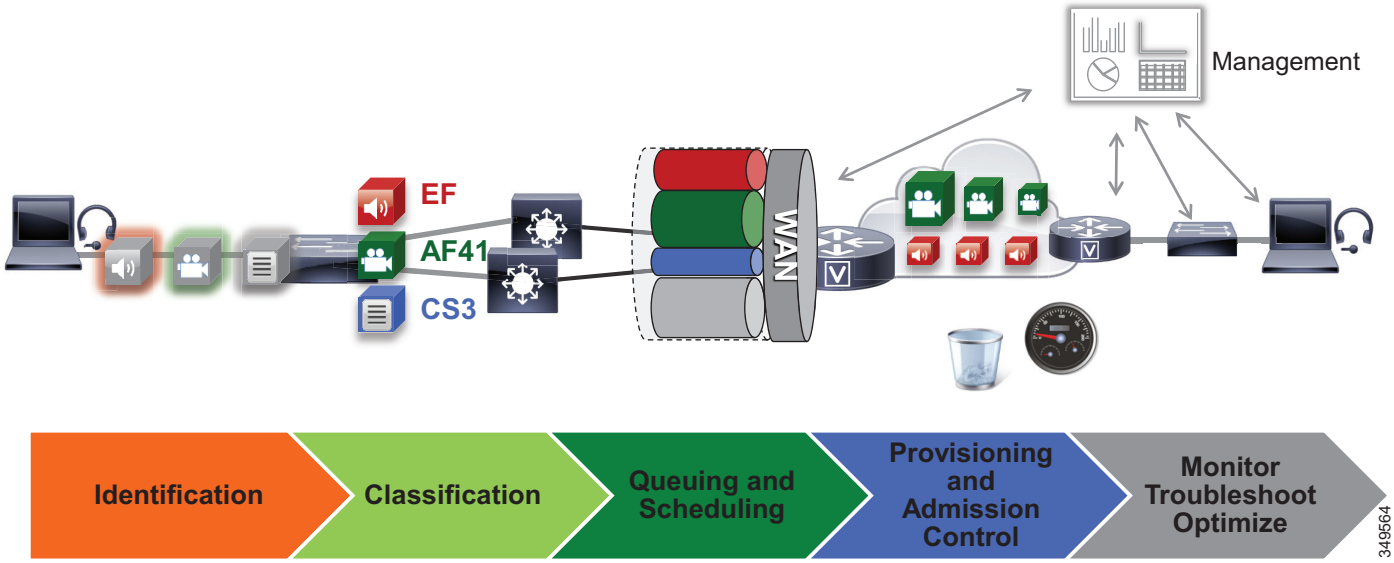
Quality of Service（QoS）アーキテクチャを構成する主要なコンポーネントは次のとおりです。

- Cisco Unified Communications Manager
- Cisco エンドポイント
- Cisco Expressway
- Cisco Unity Connection
- Cisco Meeting Server
- ネットワーク インフラストラクチャ：
  - Cisco ルータ
  - Cisco スイッチ

C：図 8-1 に、Enterprise Collaboration 向け Cisco PA での QoS 設計アプローチを示します。このアプローチは、次のフェーズからなります。

- **識別と分類：**エンドポイントやアプリケーションのメディアとコール シグナリングの識別に対する信頼の概念および手法のことを指します。このフェーズには、ネットワーク全体にわたり、エンドツーエンドの適切な Per-Hop Behavior を使用してメディアとシグナリングを提供するために、識別したトラフィックを適切な DSCP にマッピングするプロセスも含まれます。
- **キューイングとスケジューリング：**このフェーズは、一般的な WAN キューイングとスケジューリング、各種キューイング、ならびに WAN への出力時にコラボレーション メディアとシグナリングが正しくキューイングされるようにするための推奨事項からなります。
- **プロビジョニングとアドミッション制御：**これは、ネットワーク内の帯域幅をプロビジョニングして、エンドポイント グループが使用する最大ビット レートを決定することを意味します。また、コール アドミッション制御を必要なネットワーク領域に実装することもできます。
- **モニタリング、トラブルシューティング、および最適化：**ネットワーク全体で音声とビデオが適切に運用および管理されるようにします。Cisco Prime Collaboration には、これらの機能を実行するための一連のツールが揃っています。モニタリング、トラブルシューティング、最適化は、プリファード アーキテクチャではカバーされていませんが、全体的なアプローチの一部となります。

C：図 8-1 帯域幅管理のアーキテクチャ



推奨される展開

- エンドポイントからのメディアと SIP シグナリング トラフィックを識別します。
- アクセス スイッチのエッジでトラフィックを分類し、マーキングします。
  - すべてのオーディオ（音声のみのコールのオーディオとビデオ コールのオーディオの両方を含む）は、完全優先転送（Expedited Forwarding）クラス EF としてマーキングします。
  - デスクトップおよびルーム システムの重要なすべてのビデオは、優先順位付けされたビデオの相対的優先転送（Assured Forwarding）クラス AF41 としてマーキングします。
  - Jabber ビデオ、モバイルおよびリモート アクセス（MRA）ビデオ、エッジ ビデオは、いずれも状況対応型ビデオの相対的優先転送（Assured Forwarding）クラス AF42 としてマーキングします。企業で状況対応型ビデオを使用できない場合は、AF41 としてマーキングします。
  - すべてのコール シグナリングは、CS3 としてマーキングします。
  - ソリューション全体にわたり、メディアを発信および終端するアプリケーションと MCU のすべてに、QoS を設定します。
- コラボレーション トラフィックの識別、分類、マーキング、キューイングには、次の簡素化した WAN エッジ ポリシーを適用します。
  - WAN エッジ入力時の再マーキング ポリシー
  - WAN エッジ出力キューイングおよびスケジューリング ポリシー
- ビデオの最大ビット レートに基づいてビデオ エンドポイントをクラス別にグループ化し、エンドポイントのタイプおよびソリューションでの用途に応じて帯域幅使用量を制限します。
- Enhanced Locations Call Admission Control を導入し、ネットワーク内で帯域幅リソースが限られているエリアでのみ、ビデオ コールを制限します。

主なメリット

この帯域幅管理の導入には、次の利点があります。

- 簡素化された QoS アーキテクチャによって導入環境を簡素化する際の規範的な推奨事項に従うことができます。
- ネットワーク リソースの使用効率が高くなります。
- モバイルおよびマルチメディア対応のコラボレーション デバイスがサポートされます。
- 「アンマネージド」ネットワーク セグメント（インターネット）が考慮されます。
- 新しいサービス、機能、エンドポイントを簡単に導入できるため、将来の変更に対応できます。

アーキテクチャー

帯域幅管理の目的は、コラボレーション ソリューションを構成する音声 / ビデオ エンドポイント、クライアント、アプリケーションのすべてで、エンドツーエンドの最高のユーザ エクスペリエンスを実現することです。この章では帯域幅管理の全体的アプローチについて説明します。この全体的アプローチには、マネージドおよびアンマネージド ネットワークでパーベイシブ ビデオを導入する際に最高のユーザ エクスペリエンスを実現することを目的に、エンドツーエンドの Quality of Service（QoS）アーキテクチャ、コール アドミッション制御、ビデオ レート アダプテーション、復元力メカニズムも組み込まれています。

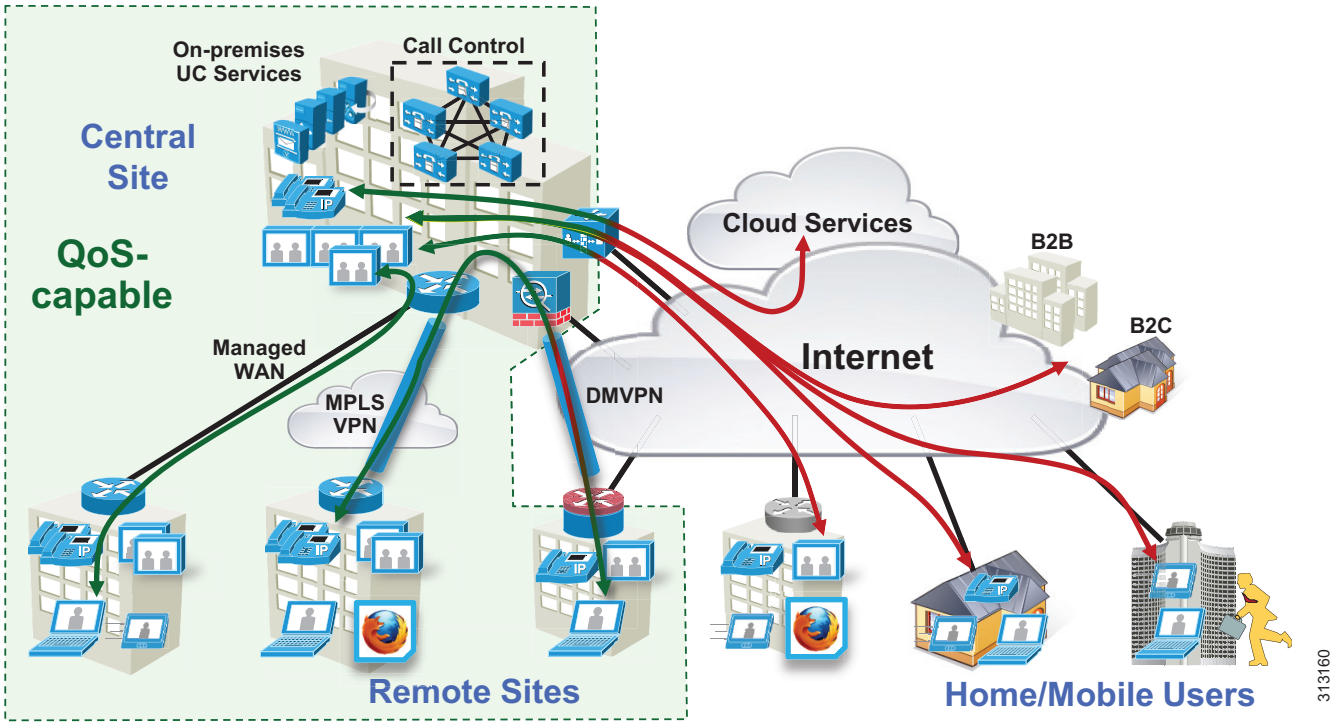
ここではまず、コラボレーション メディアの説明、音声とビデオの違いと、その違いがネットワークに与える影響について説明します。次に、エンドポイント、クライアント、アプリケーションで使用するコラボレーション メディアと SIP シグナリングの識別と分類、WAN キューイングとスケジュール、帯域幅プロビジョニングとアドミッション制御を含む、エンドツーエンドのコラボレーションに対応する QoS アーキテクチャの概要を説明します。これに続き、「帯域幅管理の導入」ではこのアーキテクチャをコラボレーションとネットワーク両方のアーキテクチャで実装するために必要な手順を説明します。

注 LAN と WAN で QoS の基盤については、最新バージョンの Cisco Collaboration SRND に記載されている「*Network Infrastructure*」の章で説明されています。QoS の概念に不慣れな場合は、この章を読んで、そこで説明されている概念を十分に理解してください。本章では、読者が QoS を理解していることを前提としています。

はじめに

このプリファード アーキテクチャでは、インターネットとクラウドベース サービス（Webex など）を利用することが、ソリューションの重要な側面となっています。つまり、コラボレーション インフラストラクチャの一部は、マネージド エンタープライズ ネットワーク外部のクラウド内に置かれることになります。企業のオフィスを接続するためのオプションも多岐にわたり、リモート サイトとモバイル ユーザがマネージド専用回線で直接 MPLS に接続するという選択肢から、たとえば Dynamic Multipoint VPN（DMVPN）などのテクノロジーを使用してインターネット経由で接続するという選択肢まであります。C：図 8-2 では、クラウド サービスを使用するマネージド（QoS 対応）ネットワーク内の従来のオンプレミス コラボレーション ソリューションと、インターネットなどのアンマネージド（QoS 非対応）ネットワーク上に配置されたサイトをまとめています。オンプレミス リモート サイトは、管理者が QoS でコラボレーション メディアとシグナリングの優先順位を設定できるマネージド ネットワークを経由して接続されます。他のリモート サイトとブランチは、インターネットを経由して企業に接続します。この場合、コラボレーション メディアとシグナリングの優先順位を設定することはできないか、サイトからの発信に対してのみ優先順位を設定できます。また、多くのさまざまなモバイル ユーザとテレワーカーも、インターネットを経由してオンプレミス ソリューションに接続します。このように、企業をリモート サイト、家庭、モバイル ユーザならびに他のビジネスや消費者を結ぶソースとしてインターネットを統合する場合、帯域幅管理とユーザ エクスペリエンスに大きな影響が及びます。

C：図 8-2　マネージド ネットワークとアンマネージド ネットワーク



ここでは、Cisco ビデオ エンドポイントでスマート メディア手法を利用し、エンドツーエンドの QoS アーキテクチャを構築し、帯域幅を管理するための最新の設計と導入推奨事項とベスト プラクティスに従って、利用可能なネットワーク リソースとコラボレーション メディアが経由する各種のネットワークに基づいて最高のユーザ エクスペリエンスを実現するための戦略を紹介します。

コラボレーション メディア

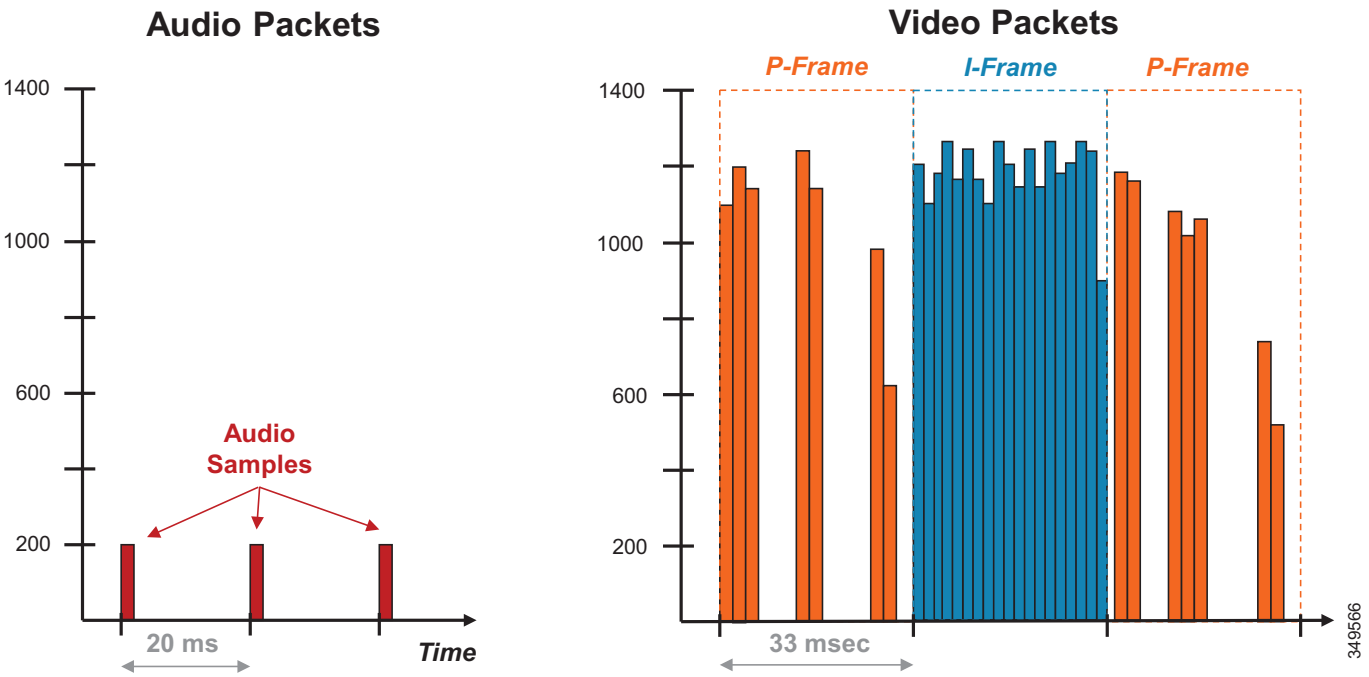
ここでは、音声ストリームとビデオ ストリームの特性と、パケットの損失、遅延、ジッターが発生したとしても高品質のビデオを実現できるよう Cisco ビデオ エンドポイントで採用しているリアルタイム メディア手法とスマート メディア手法について説明します。

音声とビデオの違い

音声とビデオは同様のものとして見なされることがよくあります。どちらもリアルタイム プロトコル（PTP）アプリケーションではあるものの、それ以上の類似点はありません。通常、各パケットのサイズとレートは固定されているため、音声は適切に動作すると考えられています。ビデオ フレームは複数のパケットに広がり、グループとして移動します。1 つのパケットが失われると、P フレームが無駄になり、1 つの P フレームが無駄になると、永続的なアーティファクトが生成されるため、通常、ビデオには音声よりも厳密な損失要件があります。ビデオは非対称です。音声も非対称ですが、通常は対称です。ミュートの場合でも、IP Phone は同じサイズのフローを送受信します。

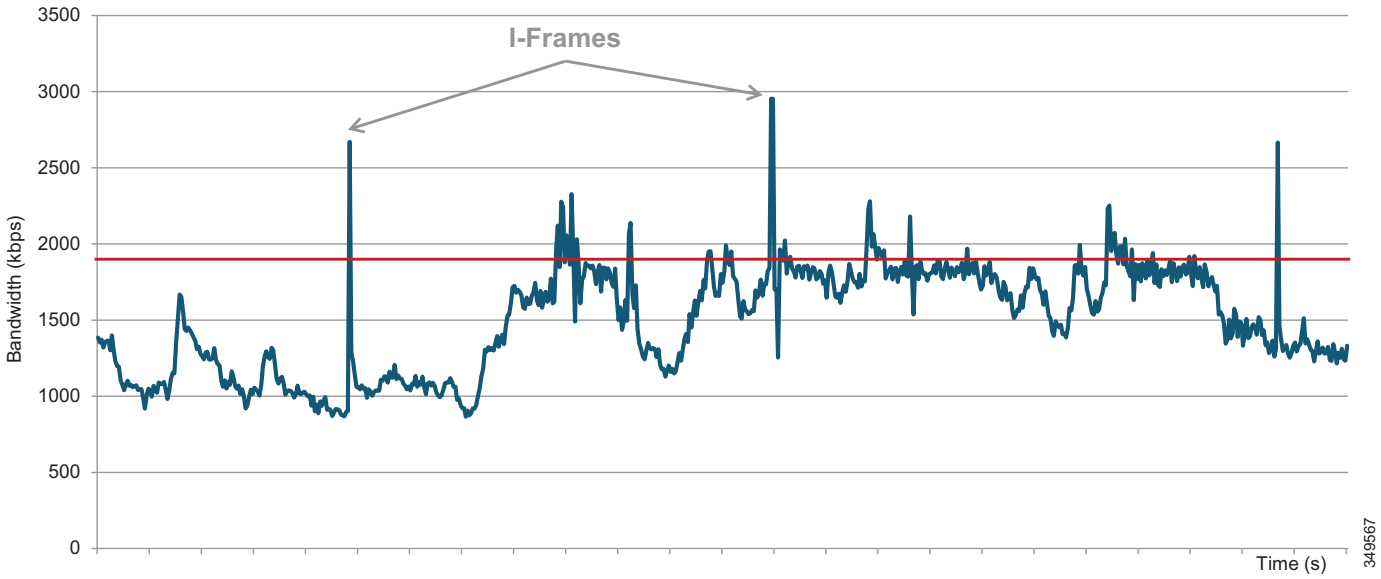
ビデオでは、平均リアルタイム パケット サイズが増え、ネットワークのトラフィック プロファイルを素早く変更する可能性があります。計画的に行わないと、ネットワーク パフォーマンスに悪影響を与える可能性があります。C：図 8-3 に、一定期間中に送信された一連の音声パケットとビデオ パケットの違いを示します。

C：図 8-3　　音声とビデオの違い



C：図 8-3 に示されているように、オーディオ パケットはすべて同じサイズで、まったく同じ間隔で送信されることから、非常にスムーズなストリームになっています。一方、ビデオは一定の間隔で大量のパケットを送信し、フレームごとに大きく異なります。C：図 8-3 に、I フレームと P フレームを比較した場合の、パケット数とパケット サイズの違いを示します。音声と比較すると、非常にバースト性のあるメディア ストリームに変換されます。C：図 8-4 に示されているバースト性は、HD ビデオ ストリームの一定期間にわたる帯域幅プロファイルを表しています。I フレームの送信時にはバーストが大きくなることに注目してください。

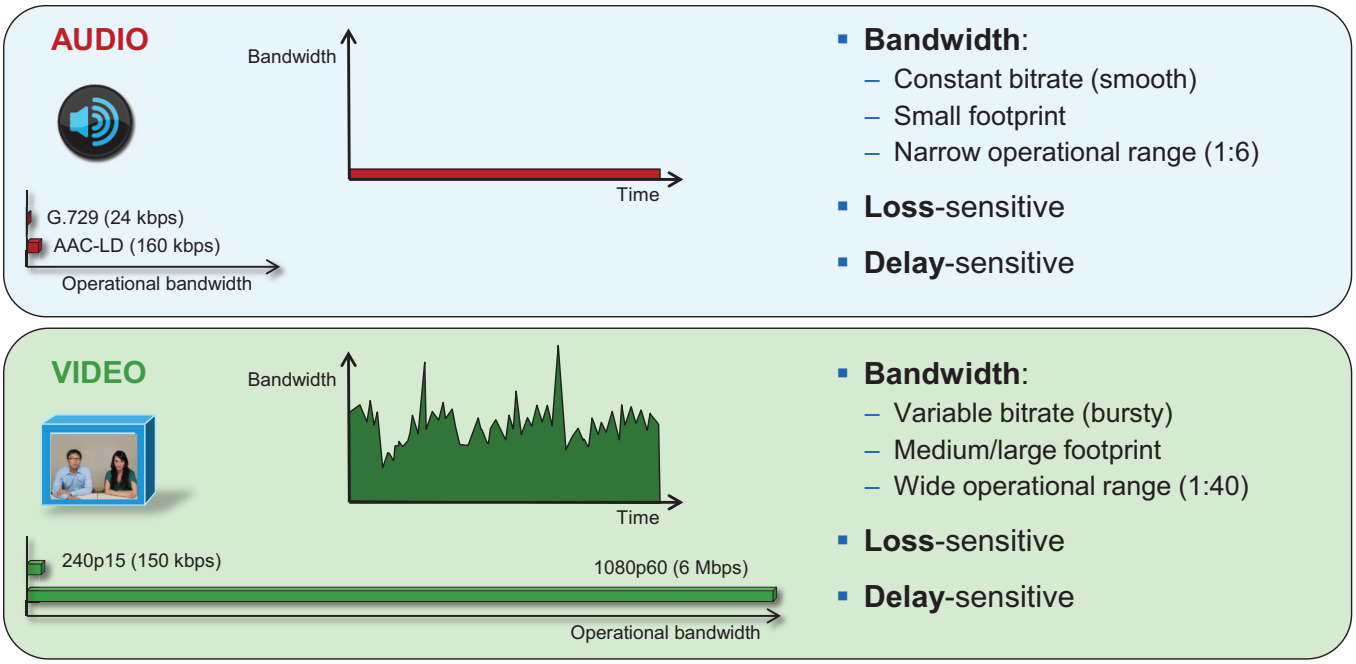
C：図 8-4　　帯域幅の使用：高解像度ビデオ コール



C：図 8-4 に、720p、30 fps、および 1920 kbps（1792 kbps ビデオ + 128 kbps のオーディオ）で転送された HD ビデオ コールを示します。赤い線は、通話期間中の平均ビット レートを示します。

オーディオとビデオは両方とも UDP で転送され、パケット損失と遅延の影響を受けやすくなっているという点では同様ですが、ネットワーク要件とプロファイルについてかなりの違いがあります。C：図 8-5 に示されているように、オーディオのビット レートは一定であり、ビデオと比べると密度が低くなっています。また、最小ビット レート オーディオ コーデックと最大ビット レート コーデックの 1 つを比較しても、運用範囲の比率は 1:6 と狭くなっています。一方、ビデオのビット レートは可変（バースト性がある）であり、オーディオと比べると高密度です。また、運用範囲も 1:40 と広くなっています（15 fps で 250p、最大 60 fps で 1080p）。

C：図 8-5　　ビデオ トラフィック要件とプロファイル



ここでの要点は、オーディオとビデオは、転送およびパケット損失と遅延による影響という点では似ていますが、ネットワークで帯域幅要件を管理するために採用する手法は大きく異なることです。また、ビデオはコラボレーション エクスペリエンス全体に関連しますが、オーディオが重要です。たとえば、ビデオ通話中にネットワークの停止や他のネットワーク関連のイベントによってビデオが失われたり、ビデオ品質が損なわれたりしたとしても、オーディオが失われていない限り通信を継続できます。これは、PA での帯域幅管理に極めて重要な概念です。

「スマート」メディア テクニック（メディアの復元力とレート調整）

管理者が組織全体にパーベイシブ ビデオを導入する際に必然的に直面する問題は、ワイドエリア ネットワーク（WAN）のボトルネック エリアでは、最繁時にビデオのロードを処理するために必要な帯域幅が不足することです。この問題を踏まえると、ビデオに正しく優先順位を付けることが重要となります。優先順位付けで目的とするのは、ビデオのパケット損失によってオーディオが影響されないようにすること、そして輻輳中に帯域幅の使用量を管理できるよう、特定のタイプのビデオでビデオ レート アダプテーションを利用できるようにすることです。メディアの復元力およびレート アダプテーション手法を使用すれば、マネージド ネットワークおよびアンマネージド ネットワークで輻輳やパケット損失が発生したとしても、最適化されたビデオ エクスペリエンスを実現できます。ただし、それだけではありません。これらの手法を QoS と組み合わせた戦略として使用することで、エンドポイントでは、輻輳またはパケット損失の発生時にはビット レートを下げて帯域幅の使用量を削減できるとともに、最繁時以外の時間帯には最大限のビデオ品質を達成するためにビット レートを上げて帯域幅の使用量を増やすことができます。したがって、この方法を取ることによって、組織はパーベイシブ ビデオを導入することが可能になります。

あらゆる Cisco ビデオ エンドポイントには、ネットワークの輻輳の回避、パケット損失からの回復、ネットワーク リソースの最適化に対応するさまざまなスマート メディア手法が使用されています。Cisco ビデオ エンドポイントで使用されているスマート メディア手法には、具体的には以下のものがあります。

- メディア復元力手法
  - エンコーダ ペーシング
  - 段階的なデコーダの更新（GDR）
  - 修復機能を備えた長時間参照フレーム（LTRF）
  - 前方誤り訂正（FEC）
- レート アダプテーション

メディア復元力手法

このプリファード アーキテクチャでは、Cisco ビデオ エンドポイントに対して次のメディア復元力手法をサポートしています。

- エンコーダ ペーシング

  エンコーダ ペーシングは、パケットを可能な限り均等に分散して帯域幅のバーストのピークを抑制するために使用される単純な手法です。

- 段階的なデコーダの更新（GDR）

  GDR は、多数のフレームで画像を徐々にリフレッシュして、よりスムーズでバースト性の低いビット ストリームを提供する手法です。

- 長時間参照フレーム（LTRF）

  長時間参照フレーム（LTRF）とは、エンコードとデコーダに保管される参照フレームのことです。この参照フレームを使用することで、ビデオ エンドポイントはパケット損失の際に、ネットワーク パスでより少ない帯域幅を使用して、損失したフレームをより効率的に再送信できるようになります。

- 前方誤り訂正（FEC）

  前方誤り訂正（FEC）では、所定のアルゴリズムを使用して、転送される情報に冗長性を与えます。この冗長性により、受信側では、メッセージのいずれかの箇所でエラーが発生した場合でもそれが一定数であれば、送信側に追加データを要求することなく、そのエラーを検出し訂正することができます。FEC では、受信側でエラーを訂正する場合、データの再送信を要求するためのリバース チャネル（RTCP など）は必要ありませんが、その代わりとして、より高い転送チャネル帯域幅（より多くのパケットの送信）が常に必要となります。FEC では最も重要なデータ（通常は修正 P フレーム）が保護されます。これにより、それらのフレームは受信側で確実に受信されます。エンドポイントでは、帯域幅が 768 kbps を下回る場合 FEC は使用されません。また、1.5% 以上のパケット損失が発生していない場合も FEC は適用されません。通常、FEC の有効性はエンドポイントによりモニタリングされます。FEC が有効でない場合は、エンドポイントにより FEC の実行が中止されます。

レート アダプテーション

レート アダプテーション（別名、ダイナミック ビット レート調整）は、使用できる可変帯域幅に合わせてコール レートを調整します。これにより、パケット損失の状況に基づいてビデオ ビット レートの速度が上下します。エンドポイントは、受信側から受け取ったメッセージにパケット損失が発生したことが示されているとビット レートを下げ、パケット損失が減少すると、ビット レートを上げます。

自動調整ビデオ ネットワーク、優先順位付けされたオーディオ、状況対応型ビデオ

自動調整ビデオ ネットワーク、優先順位付けされたオーディオ、状況対応型ビデオは、いずれも QoS の概念であり、QoS 戦略でもあります。自動調整ビデオ ネットワークでは、適切なプロビジョニングおよび QoS と併せ、前述のスマート メディア手法とレート アダプテーションを利用します。これにより、ネットワーク内のビデオ帯域幅が十分に利用されていない間は、ビデオ エンドポイントでビデオ解像度が最大化されるようにするとともに、最繁時にはビット レートのアダプテーションまたはスロットリングを行って、より多くのビデオ フローに対応できるようにします。

音声のみのコールのオーディオとビデオ コールに含まれるオーディオの両方に対してオーディオ優先順位付けを適用すると、ネットワーク内のすべてのオーディオに優先順位が付けられることになります。したがって、ビデオ キューでパケット損失が発生したとしても、その影響は及びません。あらゆるタイプのコラボレーション メディアに含まれる音声に優先順位を付けると、重度の輻輳が発生している間にビデオでパケット損失が発生し、その損失に応じて調整する場合でも、オーディオ ストリームにはパケット損失の影響が及ぶことなく、ユーザのオーディオが中断されません。音声のみのコールのオーディオとビデオ コールに含まれるオーディオの両方に優先順位付けるという手法は、音声コールとビデオ コールを常に同じ QoS でマーキングしていた従来のモデルからのパラダイム シフトです。

状況対応型ビデオを使用すると、ビデオ エンドポイントのグループをマーキングするビデオ クラスを戦略的に低くして、これらのビデオ エンドポイントが使用可能な帯域幅を状況に応じて使用できるようになります。つまり、ネットワークがアイドル状態で、より多くの帯域幅を使用できる場合は、ビデオ解像度を最適化し、逆にネットワークの最繁時に輻輳が発生している間は、優先順位が高いビデオ クラスよりも積極的にビデオ速度を下げるということです。この状況対応型ビデオの概念を優先順位付けされたオーディオと組み合わせることで、許容可能なビデオ エクスペリエンスが維持され、状況対応型ビデオ コールの音声メディアの品質が低下しないようになります。インターネットなどのアンマネージド ネットワークは QoS 対応ではなく、パケット損失に関して何の保証もないことから、この手法が適用されるのは当然、マネージド ネットワークです。それでも、メディア復元力とレート アダプテーションのメカニズムでは、アンマネージド ネットワークで配信されるメディアもパケット損失、遅延、ジッターに際して最大限の品質を保てるよう試みます。

状況対応型ビデオは、優先順位付けオーディオによって自動調整ビデオ ネットワークに付加価値を与える最適な導入オプションですが、自動調整ビデオ ネッワークの機能には必須ではありません。

コラボレーション用の QoS アーキテクチャ

サービス品質（QoS）により、メディア エンドポイントおよびアプリケーションの遅延、パケット損失、ジッターの削減し、信頼性のある高品質な音声とビデオを実現します。QoS は、音声、ビデオ、データ ネットワークの透過的なコンバージェンスをサポートするのに必要な基本的ネットワーク インフラストラクチャ テクノロジーを提供します。インタラクティブ アプリケーション（特に音声およびビデオ アプリケーション）の増加に伴い、多くの場合、ネットワークのリアルタイム サービスが求められます。これらのリソースは限られているため、効率的かつ効果的に管理する必要があります。優先リソースのフロー数に制限がない場合は、これらのリソースがオーバーサブスクライブされるため、すべてのリアルタイム トラフィック フローの品質が低下し、最終的には役に立たなくなります。「スマート」メディアの手法、QoS、およびアドミッション制御により、リアルタイム アプリケーションとその関連メディアが、これらのアプリケーションにプロビジョニングされたネットワークおよび帯域幅をオーバーサブスクライブしないようにします。QoS に関連するこれらのスマート メディアの手法と、必要に応じたアドミッション制御は、リアルタイム メディアを非リアルタイム ネットワーク トラフィックから保護し、ネットワークをオーバーサブスクリプションから保護して、音声とビデオのアプリケーションのエンド ユーザ エクスペリエンスの潜在的な品質低下を回避するための強力なツール セットです。

識別と分類

QoS の信頼と適用

QoS の適用は、リアルタイムの音声またはビデオ エクスペリエンスに必要不可欠です。ネットワークで QoS（分類、優先順位付け、およびキューイング）を適切に処理しないと、リアルタイム メディアに過度の遅延またはパケット損失が発生する可能性があり、リアルタイム メディア フローの品質が低下します。QoS の適用のパラダイムでは、信頼の問題と信頼境界が同様に重要です。信頼とは、エンドポイントまたはデバイスがトラフィックに QoS マーキング（レイヤ 2 CoS またはレイヤ 3 IP DSCP）を適用してネットワークを引き続き通過できるようにすることを許容すること、またはこのマーキングを「信頼」することです。信頼境界は信頼するネットワーク内の場所です。これはネットワーク内のあらゆる場所で設定できますが、LAN アクセス入力や WAN エッジ、または必要に応じてその両方など、ネットワーク エッジで信頼を適用することをお勧めします。

信頼には主に 3 つのカテゴリがあります。

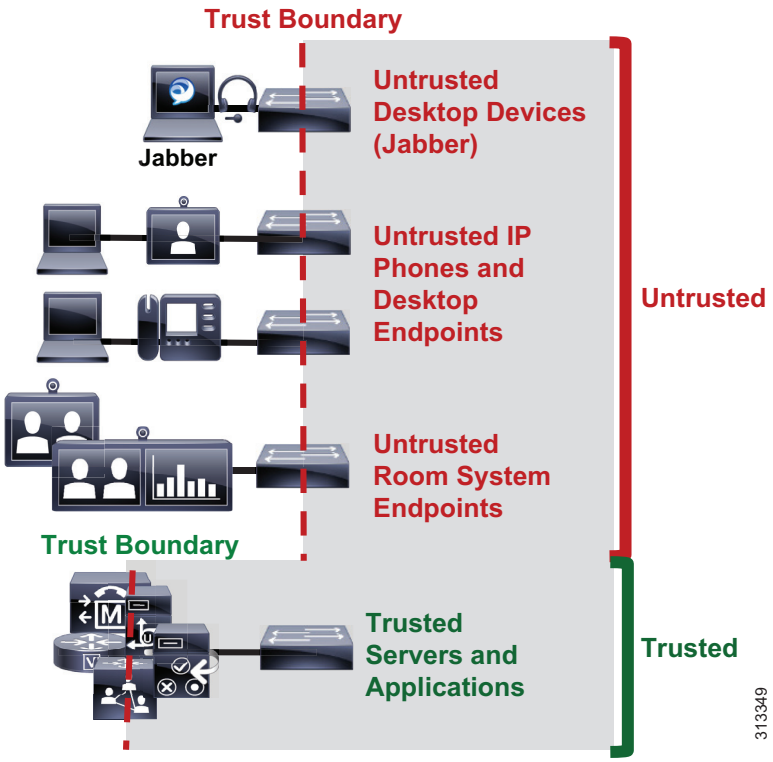
- **信頼できないデバイス** — 安全でない PC、Mac、あるいは Jabber クライアント、IP 電話、およびデスクトップエンドポイントを実行する携帯モバイル。
- **信頼されている**：信頼されているデバイスとしては、セキュアな PC およびサーバ、ビデオ会議エンドポイント、アナログ / ビデオ会議ゲートウェイ、PSTN ゲートウェイ、Cisco Unified Border Element、信頼されているアプリケーション サーバ、および他の同様のデバイスが挙げられます。
- **条件付きで信頼できる**：条件付きで信頼できるデバイスには、一般に、Cisco Discovery Protocol（CDP）をサポートするエンドポイントが含まれます。Cisco Room システム、IP 電話、デスクトップ フォンは CDP をサポートしていますが、PA では、これらのデバイスを条件付きで信頼できるデバイスとして扱いません。

PA では、信頼されているスイッチ ポートと信頼されていないスイッチ ポートが使用されますが、条件付きで信頼できるポートは使用されません。PA では次の理由により、条件付きの信頼は推奨されません。

- スイッチの多様性による複雑さ：さまざまなスイッチ タイプで条件付きの信頼を有効にすると、アーキテクチャが複雑化することになります。古いタイプのスイッチの中にはデフォルトで信頼しないものがある一方、新しいタイプのスイッチはデフォルトで信頼するためです。しかも、信頼を有効にするコマンドと、信頼を適用するプロセスは、プラットフォームによって異なります。
- さらに重要な点として、IP フォンとデスクトップ エンドポイントの PC ポートでは、レイヤ 3 DSCP 再マーキングを使用できません。これらのエンドポイントはレイヤ 2 CoS 再マーキングのみに対応します。この点に加え、DSCP レベルでは PC トラフィックを正しく再マーキングできないことから、PA ではアクセス リストを使用して IP フォンとデスクトップ エンドポイントを再マーキングすることが推奨される手法となります。
- 限られた数のポートを信頼されているポートとして指定するよりも、すべてのスイッチ ポートに直接マッピングする単一の ACL を使用したほうが管理が容易になります。

C：図 8-6 に、PA で使用する信頼のタイプと、信頼されているデバイスおよび信頼されていないデバイスを示します。

C：図 8-6　　プリファード アーキテクチャでの信頼境界



分類とマーキング

ここでは、エンドポイントの分類とマーキングについて説明します。

すべての Cisco エンドポイントは、Unified CM から DSCP マーキングを取得します。Unified CM では、CallManager サービスのサービス パラメータ（[クラスタ全体のパラメータ（システム - QoS）（Clusterwide Parameters (System - QOS)）]）と SIP デバイスにのみ適用される SIP プロファイルの 2 つの場所にエンドポイントの QoS 設定が保存されます。QoS 設定の SIP プロファイル設定は、サービス パラメータ設定を上書きします。これにより、Unified CM の管理者はエンドポイント グループの異なる QoS ポリシーを設定することができます。エンドポイント登録時に、Unified CM は、この QoS 設定を TFTP 経由で設定ファイルとしてエンドポイントに転送します。この設定ファイルには、QoS パラメータと、他の多くのエンドポイント固有のパラメータが含まれます。ビデオのエンドポイントには、QoS の観点から 2 つのカテゴリが提供されています。*ルーム システム エンドポイント*（電話名でテレプレゼンスがあるエンドポイント、通常はルームシステムまたは Webex Room シリーズ、また Webex DX80 等の大規模なデスクトップ ビデオ エンドポイント）、そしてルームシステム以外のビデオ エンドポイント（以下*デスクトップ エンドポイント*）があります。

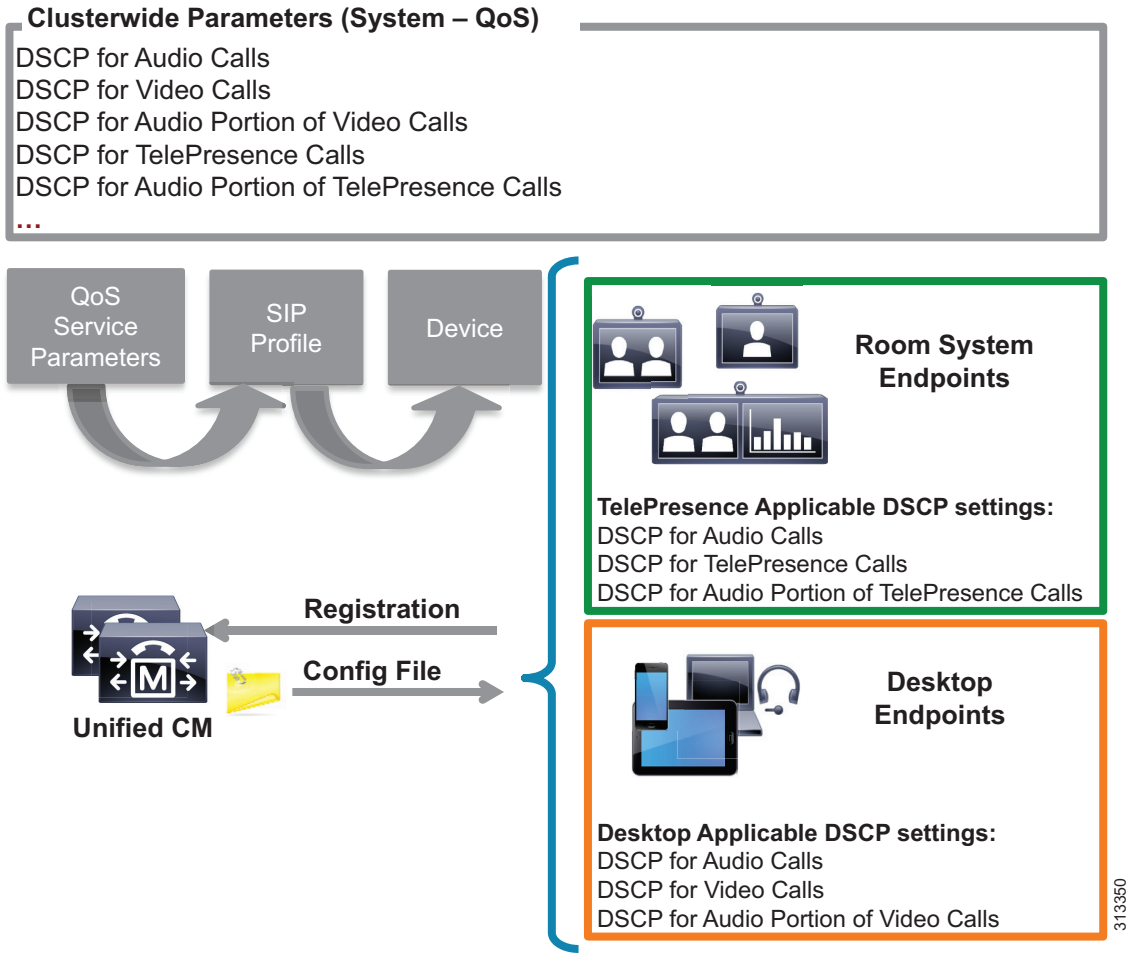
C：表 8-2 に、プリファード アーキテクチャのエンドポイントとその分類を記載します。

C：表 8-2　PA ビデオ エンドポイント

エンドポイント	ルームシステム エンドポイント	デスクトップ エンドポイント
Cisco IP Phone 8800 シリーズ		X
Cisco Jabber		X
Cisco Webex DX80	X	
Cisco MX シリーズ	×	
Cisco SX シリーズ	×	
Cisco Webex Room シリーズ	×	

C：図 8-7 では、シスコのビデオ エンドポイントの 2 つのカテゴリが DSCP を取得する方法について示します。これらのカテゴリは、QoS とコール アドミッション制御（CAC）にのみ適用されます。

C：図 8-7　シスコのエンドポイントによる DSCP の取得方法



設定ファイルは、設定時に CallManager サービス パラメータまたは SIP プロファイルの QoS パラメータと統合され、登録時にエンドポイントに送信されます。次に、エンドポイントは、エンドポイントのカテゴリに応じて、メディア ストリームの各タイプに正しい DSCP パラメータを使用します。C：表 8-3 に、DSCP パラメータ、エンドポイントのタイプ、ストリームの DSCP マーキングを決定するコール フローのタイプを記載します。

C：表 8-3　基本的なコール フローの DSCP

DSCP パラメータ	ルームシステム エンドポイント	デスクトップ エンドポイント	コール フロー
音声コールの DSCP（DSCP for Audio Calls）	×	×	Voice-only
ビデオ コールの DSCP（DSCP for Audio Calls）		X	ビデオ：ビデオ コールの音声とビデオ ストリーム。ただし、エンドポイントは [ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）] パラメータをサポートします（C：表 8-4 を参照）。
ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）		X	ビデオ コールのオーディオ ストリーム：このパラメータをサポートするエンドポイントのみに適用される
TelePresence コールの DSCP（DSCP for TelePresence Calls）	X		ビデオ：ビデオコールの音声とビデオストリーム。エンドポイントは [テレプレゼンスコールの音声部分の DSCP（DSCP for Audio Portion of TelePresence Calls）] パラメータをサポートしていない場合（C：表 8-4 を参照）。
TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）	X		ビデオ コールのオーディオ ストリーム：このパラメータをサポートするエンドポイントのみに適用される

C：表 8-4　ビデオと TelePresence コールのオーディオ部分の DSCP に対するエンドポイント サポート

ビデオ エンドポイント	ビデオ コールのオーディオ部分の **DSCP**	**TelePresence** コールのオーディオ部分の **DSCP**
IP Phone 8845 および 8865 シリーズ	はい	いいえ（No）
Webex DX80[1]	いいえ（No）	はい
SX および MX シリーズ[1]	いいえ（No）	はい
Cisco Webex Room シリーズ[1]	いいえ（No）	はい

1. CE ソフトウェア

信頼されているコア デバイスおよびアプリケーション

エンドポイントと同じく、コラボレーション ポートフォリオに含まれるデバイスとアプリケーションは、メディア ストリームとシグナリング ストリームを発信および終端します。これらの信頼されているアプリケーションがメディアとシグナリングの QoS マーキングを透過的に渡すには、アプリケーション自体だけでなく、アプリケーションが接続先とするスイッチにも適切な設定が必要になります。

信頼されているコア デバイスおよびアプリケーションは次のとおりです。

- Cisco Unified Communications Manager と IM and Presence サービス
- Cisco Expressway
- Cisco Unity Connection
- Cisco Meeting Server
- Cisco IOS SIP ゲートウェイと Cisco Unified Border Element

これらのエンドポイントとアプリケーション サーバを接続するスイッチ ポート上で、DSCP 信頼が有効であることを必ず確認してください。通常、新しい Cisco スイッチのすべてで、デフォルトで QoS DSCP 信頼が有効になっていますが、一部のスイッチ プラットフォームではデフォルトで DSCP を信頼しないため、各スイッチ プラットフォームを確認して、この QoS 信頼が有効かどうかを確認してください。

エンドポイントとクライアント

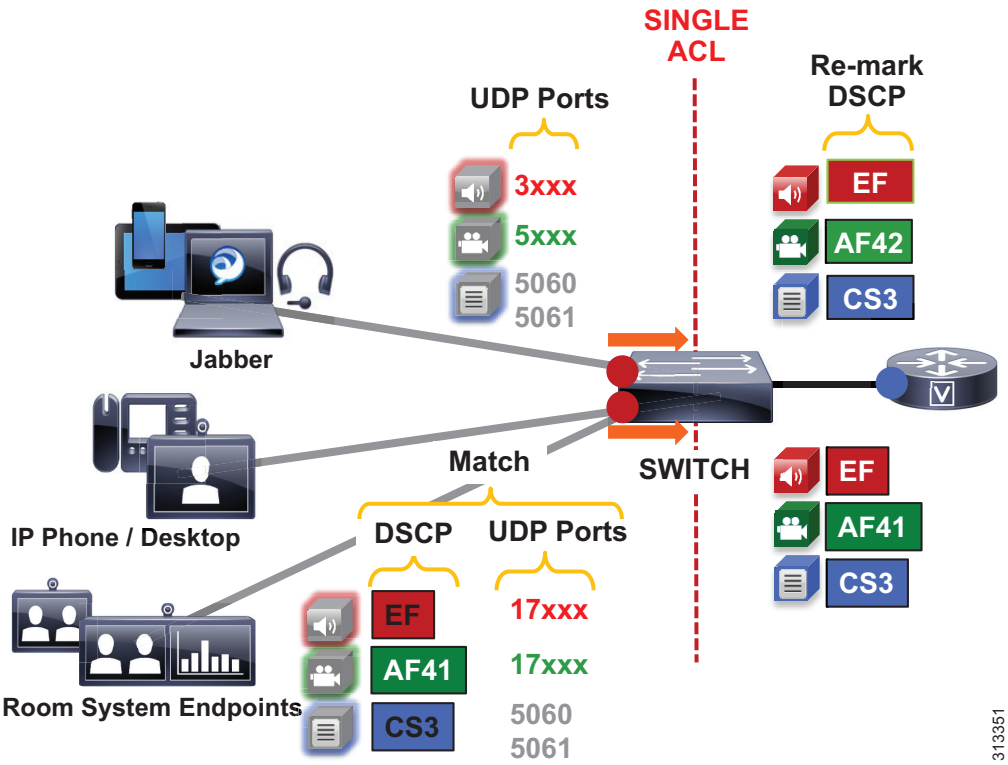
エンドポイントでは、パケットのスイッチ入力時の DSCO マーキングを、ネットワーク アクセス コントロール リスト（ACL）を使用して再マーキングする必要があります。これは、コラボレーション メディアと SIP シグナリングが適切にマーキングされること、そして他の PC データ トラフィックがベスト エフォートの DSCP（DSCP 0）としてマーキングされるか、または企業で規定する QoS データ ポリシーに応じてマーキングされることを確実にするためです。

この場合に使用する手法では、UDP と TCP ポートなどの特定のプロトコル ポートに応じて識別可能なメディアとシグナリング ストリームをマッピングし、ネットワーク アクセス リストを使用して、そのプロトコル ポート範囲に応じたシグナリングとメディア ストリームの QoS を再マーキングします。Cisco Jabber クライアント（Cisco Jabber for Windows、Cisco Jabber for Mac OS、Cisco Jabber for iPhone、Cisco Jabber for iPad、Cisco Jabber for Android）はメディアとシグナリングにポート範囲を割り当てる際に、すべて同じように動作することから、この手法はすべての Cisco Jabber クライアントに適用されます。Cisco Jabber クライアントとは異なり、IP フォン、8800 シリーズの IP およびビデオ フォン、そして PC ポートを搭載した DX シリーズには、DSCP ならびに UDP ポートに対する追加のマッチング手段が必要となります。その理由は、IP フォンとビデオ エンドポイントはオーディオとビデオの両方に同じ UDP ポート範囲を使用するため、オーディオとビデオを区別するには、UDP ポート範囲と DSCP の両方に対するマッチングを行い、メディア トラフィックを適切に識別できるようにしなければならないためです。

この概念はシンプルです。ネットワーク アクセス レイヤの装置（スイッチ）内でアクセス リストを使用して、UDP ポート範囲と DSCP のマッチングを基にメディア ストリームとシグナリング ストリームを識別した上で、適切な DSCP 値に再マーキングするようにスイッチを設定します。この手法は簡単に実装でき、広範に導入することができます。ただし、これは 100% セキュアな手段ではないことに注意してください。この PA では、ネットワークへの適切なアクセスを確保するとともに、オペレーティング システム（OS）関連の QoS 設定をユーザが改ざんできないよう、Jabber に使用する PC や Mac 上の OS をセキュリティで保護するために、他のセキュリティ対策を実装することを前提としています。

C：図 8-8 に、ネットワーク アクセス コントロール リスト（ACL）を使用して、識別可能なメディアとシグナリング ストリームを Jabber クライアントの DSCP にマッピングする方法を示します。

C：図 8-8 エンドポイントのマーキング



C：例 8-1 C：図 8-8 に示されている信頼されていないエンドポイントに対する ACL ベースの QoS ポリシー切り替え

- Jabber クライアント
  - UDP ポート範囲 3xxx に一致 –> DSCP EF として再マーキング
  - UDP ポート範囲 5xxx に一致 –> DSCP AF42 として再マーキング
  - TCP ポート 5060 または 5061 に一致 –> DSCP CS3 として再マーキング
- IP フォンとビデオ エンドポイント
  - UDP ポート範囲 17xxx と DSCP EF に一致 –> DSCP EF として再マーキング
  - UDP ポート範囲 17xxx と DSCP AF41 に一致 –> DSCP AF41 として再マーキング
  - TCP ポート 5060 または 5061 に一致 –> DSCP CS3 として再マーキング
- 汎用マッチング
  - 残りのトラフィックをマッチングし、デフォルトのクラス マップを使用して DSCP を 0（ベスト エフォート（BE））として設定

エンドポイントが送受信するデータとシグナリングは他にもあります（ICMP、DHCP、TFTP、BFCP、LDAP、XMPP、FECC、CTI など）。このようなトラフィックの QoS 値は、トラフィックのタイプに応じた企業のベスト プラクティスに従う必要があります。この手順を行わないと、メディアと SIP シグナリング以外のすべてのトラフィックの DSCP は、この設定でのクラスのデフォルトによって BE（DSCP 0）に設定されます。DSCP に基づくマッチングでマーキングしたトラフィックを通過させてから、DSCP を同じ値に再マーキングするか、エンドポイントが通信に使用するプロトコルごとに TCP および UDP ポートを使用することを推奨します。

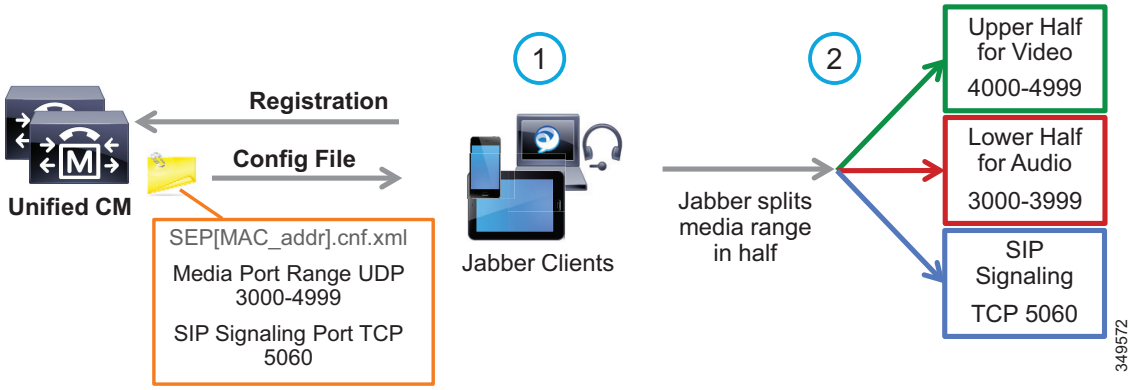
Cisco Jabber クライアントの QoS

前述したように、この方法では、IP アドレス、プロトコル、プロトコル ポート範囲に応じて Jabber クライアントからのさまざまなストリームを特定することで、メディアとシグナリングを分類します。いったん特定されると、シグナリングとメディア ストリームは、対応する DSCP で分類および再マーキングできます。プロトコル ポート範囲は Unified CM で設定し、デバイス登録時に使用するエンドポイントに転送されます。次にネットワークをアクセス コントロール リスト（ACL）経由で設定し、IP アドレス、プロトコル、プロトコル ポート範囲に応じてトラフィックを分類し、前のセクションで説明したように、適切な DSCP で分類したトラフィックを再マーキングできます。

Cisco Jabber は、UDP プロトコル ポート範囲に応じて識別可能なメディア ストリームおよび TCP プロトコル ポート範囲に応じて識別可能なシグナリング ストリームを提供します。Unified CM では、エンドポイントのシグナリング ポートは SIP セキュリティ プロファイルで設定しますが、メディア ポート範囲は Unified CM の管理ページの SIP プロファイルで設定します。

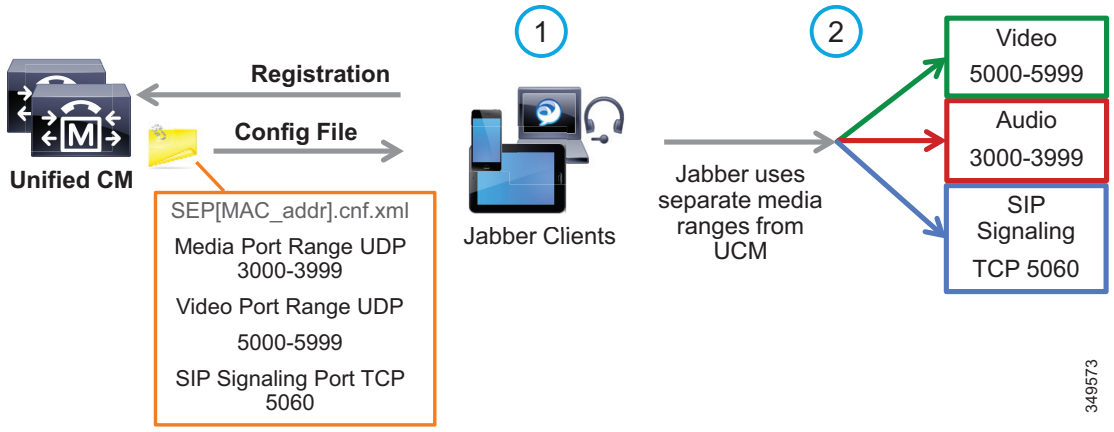
メディア ポート範囲の場合、すべてのエンドポイントおよびクライアントは、SIP プロファイル パラメータの [メディア ポートの範囲（Media Port Ranges）] を使用して、メディアで使用される UDP ポートを取得します。デフォルトでは、メディア ポート範囲は [オーディオおよびビデオ用コモンポートの範囲（Common Port Range for Audio and Video）] で設定します。設定ファイルで Jabber クライアントにこのポート範囲が割り当てられると、Jabber クライアントはポート範囲を半分に分割し、オーディオとビデオの両方のコールのオーディオ ストリームに前半の範囲を使用し、ビデオ コールのビデオ ストリームに後半の範囲を使用します。C：図 8-9 でこれについて説明します。

C：図 8-9　　メディアとシグナリングのポート範囲：共通



Jabber では、[メディアポートの範囲（Media Port Ranges）] > [オーディオとビデオのポート範囲の分割（Separate Port Range for Audio and Video）] の設定も使用できます。この設定では、Unified CM の管理者は、C：図 8-10 に示すように連続しないオーディオとビデオ ポートの範囲を指定できます。

C：図 8-10　メディアとシグナリングのポート範囲：分割

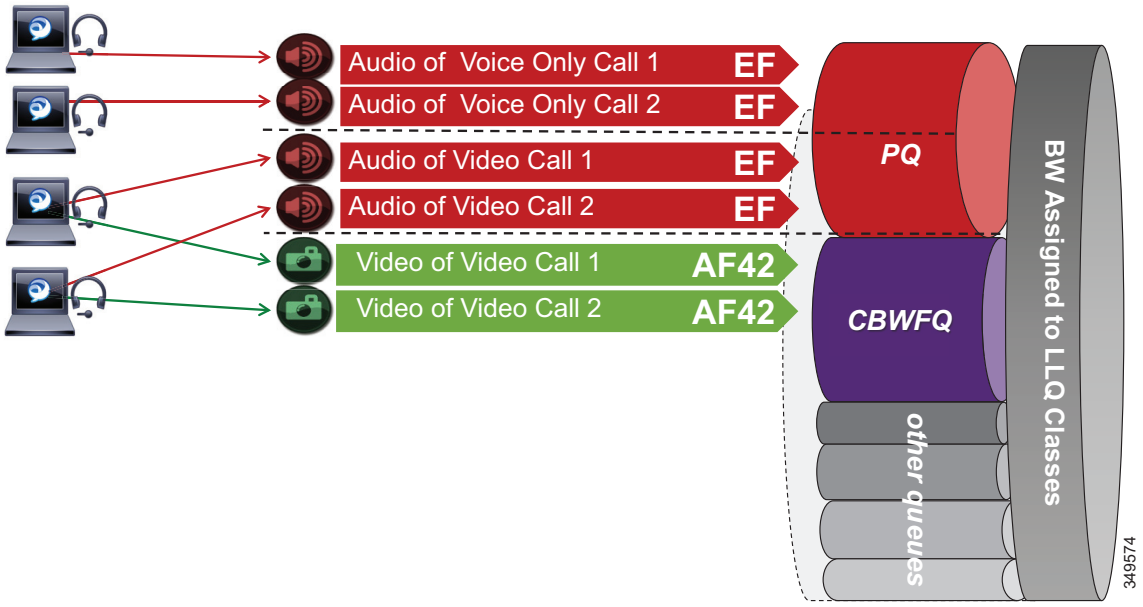


注意

セキュリティ警告：ネットワーク レベルで QoS 分類に識別可能なメディア ストリームを使用すると、信頼モデルがアプリケーション自体に拡張されることは*ありません*。目的のアプリケーションのストリームに優先順位を付けること以外に、同じ識別基準（メディア ポート範囲）を使用するように他のアプリケーションを潜在的に設定できるため、ネットワークの優先順位付けを実現できる*可能性*があります。この目的外のトラフィックはコール アドミッション制御やネットワークのプロビジョニングで考慮されないため、リアルタイムの会話全体に深刻な影響を与える可能性があります。このことから、メディア ストリームを識別するには、できるだけ限られたポート範囲を使用することが推奨されます。

この手法を使用する場合、オーディオ トラフィック クラス（EF）として再マーキングされるこれらのビデオ コールのオーディオ部分、およびビデオ トラフィック クラス（AF4）に再マーキングされるビデオ部分が、状況に応じてネットワーク内でプロビジョニングされるようにすることが重要です。C：図 8-11 に、オーディオ トラフィックをプライオリティ キュー（PQ）に入れ、ビデオ トラフィックをクラスベースの重み付け均等化キュー（CBWFQ）に入れる例を示します。PQ と CBWFQ の組み合わせは、低遅延キューイング（LLQ）とも呼ばれます。Cisco Jabber エンドポイントでは、ポート範囲を使用して音声のみのコールのオーディオとビデオ コールに含まれるオーディオを区別することはできないため、この手法を使用するすべてのオーディオは EF として再マーキングされることに注意してください。音声のみのコールのオーディオとビデオ コールに含まれるオーディオをサポートするには、PQ を適切にプロビジョニングすることが重要です。C：図 8-11 に、このプロビジョニングの例を示します。ネットワーク内でキューイングとスケジューリングをプロビジョニングする際の設計および導入に関する推奨事項については、「WAN キューイングとスケジューリング」を参照してください。

C：図 8-11　ネットワークでの Jabber QoS のプロビジョニング



RFC 3551 に準拠して、RTCP がエンドポイントで有効な場合は、次に大きな奇数のポートが使用されます。たとえば、ポート 3500 で RTP ストリームを確立するデバイスは、ポート 3501 で同じストリームの RTCP を送信します。RTCP のこの機能は、すべての Jabber クライアントにも当てはまります。RTCP はほとんどのコール フローに共通しており、ストリームの統計情報用として一般的に使用され、ビデオ コールのオーディオとビデオを同期して適切なリップシンクを実現します。ほとんどの場合、ビデオおよび RTCP は、エンドポイント自体または電話の共通プロファイル設定で有効または無効にできます。

分類とマーキングでのネットワークの活用

エンドポイントで作成された識別可能なメディアおよびシグナリング ストリームに基づいて、トラフィック クラスを作成し、それらのクラスに応じてパケットを再マーキングするには、共通ネットワーク QoS ツールを使用できます。

これらの QoS メカニズムは、アクセス レイヤ（アクセス スイッチ）などの異なるレイヤで適用できます。これは、ディストリビューション、コア、またはサービスの WAN エッジのエンドポイントおよびルータ レベルに最も近いレイヤです。分類および再マーキングの実行場所に関係なく、エンドツーエンドの Per-Hop Behavior を実現するために DSCP を使用することをお勧めします。

前述したように、Cisco Unified CM により、SIP エンドポイントで利用されるポート範囲は、SIP プロファイルで設定できます。一般的なルールとして、少なくとも 100 ポート（たとえば、3000 ～ 3099）のポート範囲であれば、ほとんどのシナリオには十分です。各種の音声ポート、ビデオ ポート、および関連する RTCP ポート（RTCP はポート範囲の奇数のポートで動作します）に対応できるだけのポート数があり、それらのポートを使用するデバイスのオペレーティング システムで、ポート コリジョンの原因となるような他のアプリケーションとのポート競合がない限り、これよりも小さいポート範囲を設定することもできます。

アクセス レイヤ（レイヤ 2 定義）

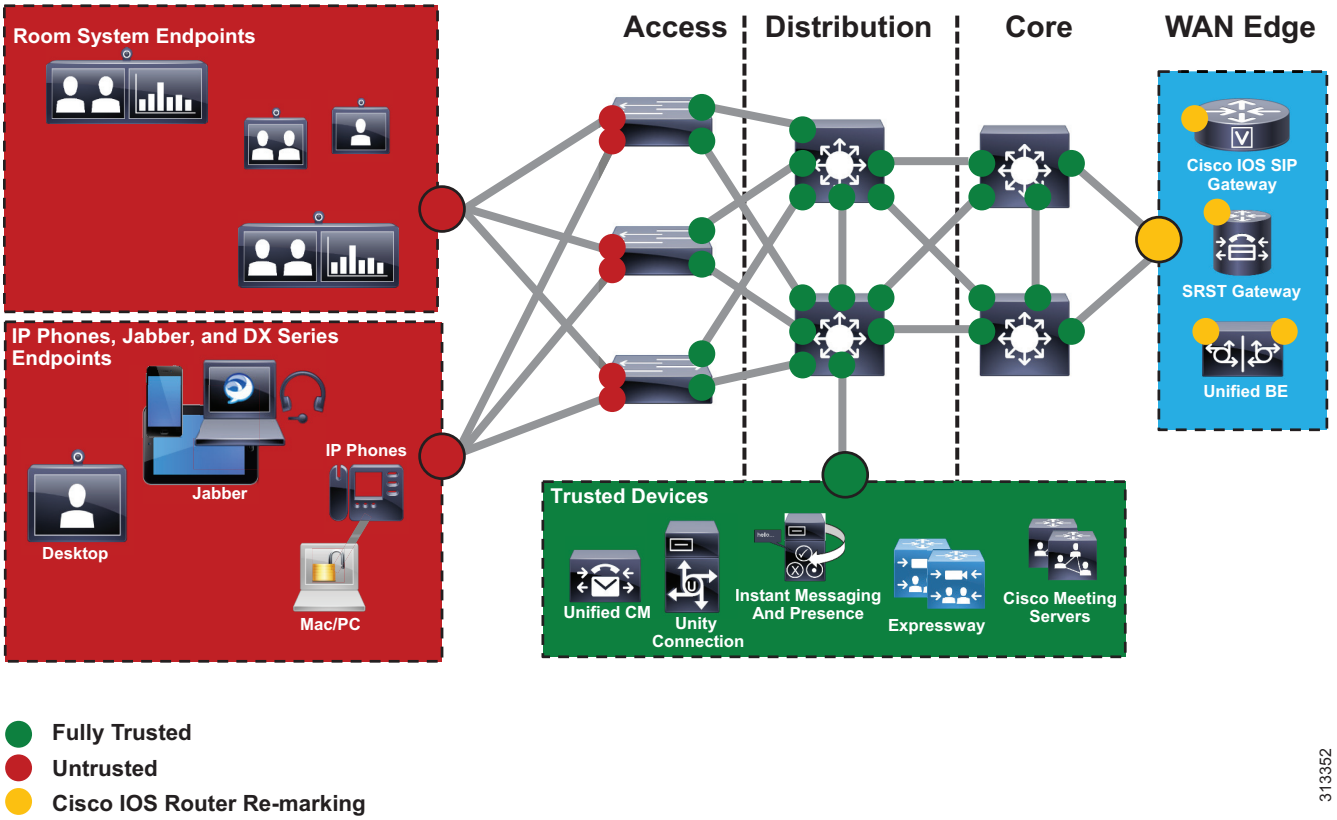
トラフィックの分類にアクセス レイヤを使用する場合、ネットワークへのトラフィックの入力時に分類が行われるため、入力に合わせてフローが識別されます。QoS ポリシーが WAN と LAN 内にも適用される環境では、すべてのアップストリーム コンポーネントが、処理時にトラフィック マーキングを使用できます。入力時の分類により、各種エンドポイントに応じてさまざまな方法を使用できます。

ネットワークのアクセス レイヤで QoS ポリシーを設定すると、大量のデバイスの設定が必要になる場合があるため、新たな運用上のオーバーヘッドが発生する可能性があります。QoS ポリシー設定は、テンプレートを通じてアクセス レイヤの各種スイッチ全体で標準化する必要があります。設定導入ツールを使用すると、手動設定の負担を軽減できます。PA ではこのプロセスを簡素化するために、各種のスイッチング プラットフォームで単一の ACL グループを使用できるようになっています。

ディストリビューション / コア / サービスの WAN エッジ（レイヤ 3 定義）

QoS マーキングが行われる場所は、レイヤ 3 のルート設定済み境界にあります。キャンパス ネットワークでは、レイヤ 3 は、アクセス、ディストリビューション、コア、またはサービス WAN エッジ レイヤでもかまいません。推奨される手法は、アクセス レイヤで分類して再マーキングを適用した上で、ネットワークのディストリビューションとコアを介して信頼し、最後に必要に応じて WAN エッジで再分類して再マーキングすることです。小規模なネットワーク（レイヤ 3 スイッチング コンポーネントを導入していない支店など）の場合、QoS マーキングは WAN エッジ ルータで適用できます。レイヤ 3 では、QoS ポリシーがレイヤ 3 ルーティング インターフェイスに適用されます。ほとんどのキャンパス ネットワークでは、VLAN インターフェイスですが、ファスト イーサネットまたはギガビット イーサネット インターフェイスの場合もあります。C：図 8-12 に、ネットワーク内の場所（アクセス、ディストリビューション、コア、または WAN エッジ）に応じて、さまざまなタイプの信頼が適用されるネットワークの領域を示します。

C：図 8-12　　信頼と適用：ネットワーク内の場所



エンドポイントの識別と分類の考慮事項と推奨事項

以下に、設計と導入に関する考慮事項と推奨事項をまとめます。

- DSCP マーキングは IP レイヤにエンドツーエンドで適用され、レイヤ 2 マーキングよりも詳細で拡張性に優れているため、可能な限り DSCP マーキングを使用してください。
- できるだけエンドポイントの近くにマーキングします。LAN スイッチ レベルがお勧めです。
- Cisco Jabber クライアントで使用するメディア ポート数を最小限に抑える場合、最小範囲として 100 個のポートを使用することが推奨されます。これは、RTCP、オーディオとビデオ用の RTP、BFCP、デスクトップ共有セッションのセカンダリ ビデオ用の RTP など、すべてのストリームに十分なポートを割り当て、同一コンピュータ上の他のアプリケーションと重複しないようにするためです。
- QoS ポリシーに、他の関連するコラボレーション トラフィックが再マーキング対象として含まれるようにします。再マーキング対象になっていないと、これらすべてのトラフィックに値 0（ベスト エフォート（BE））が設定されます。

WAN キューイングとスケジューリング

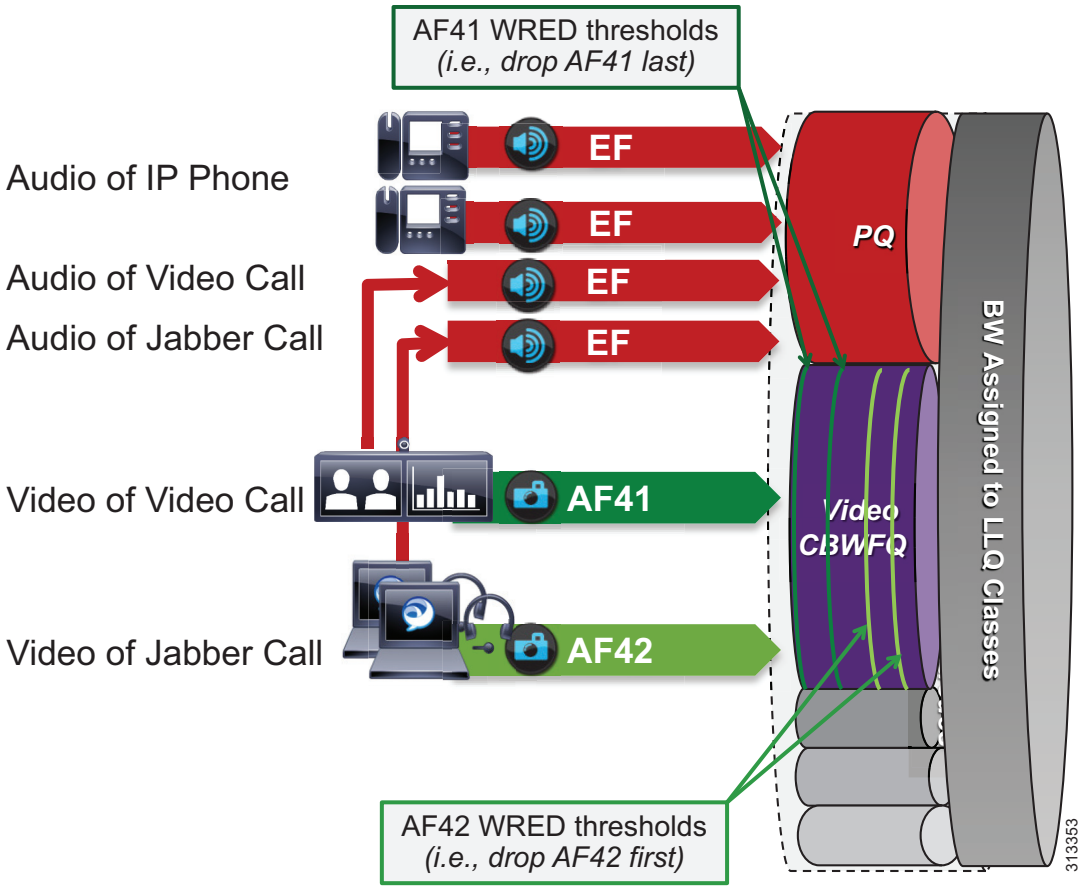
「識別と分類」で説明したように、Unified CM ではビデオ エンドポイントのタイプと、それぞれのメディア ストリームを区別することができます。このため、ネットワーク管理者はネットワーク内で、エンドポイントのタイプによってビデオを異なる方法で処理できます。PA で推奨される方法は、Jabber クライアントには AF 42 DSCP マーキングを使用し、すべてのデスクトップおよびルームシステムのビデオエンドポイントには AF 41 を使用することです。これらの値は、RFC 4594 に準拠しています。別の方法として、すべてのビデオ エンドポイントで AF41 を使用することもできます。ただし、この方法を取ると、ビデオ エンドポイントの状況対応型クラスによってもたらされる利点がなくなり、同じクラスが設定されたすべてのビデオ エンドポイントが平等にビデオ帯域幅を取得しようと争うことになります。

PA のキューイングおよびスケジューリング手法（単一のビデオ キュー）

PA では、統合コラボレーション メディアおよびデータ ネットワーク全体で各種のビデオを管理するために、ドロップ確率が異なる複数の DSCP で単一のレートベースのキューを使用します。このアプローチでは、WAN のビデオ トラフィックのスケジューリングに対して単一のビデオ キューを設定し、そこに AF41 と AF42 を使用して 2 つの AF4 ドロップ確率を設定します。この場合、AF42 のドロップが優先され、AF41 よりも高い確率でドロップされます。階層型廃棄優先のこのサービス クラスを使用する単一のビデオ キューでは、あるクラスのビデオがキュー内の帯域幅を使用していない場合、キューの残りの帯域幅を他のビデオ クラスで使用できることが前提となります。このアプローチでは、輻輳が発生している間、ビデオ専用に予約された帯域幅をビデオ キューだけが使用できるようになります。デュアル レートベースのビデオ キューといった他のアプローチは、あるキューからの余剰ビデオ帯域幅をインターフェイス上のすべてのキューに均等に割り当てるという、準最適な方法です。

最適化されたビデオ帯域幅使用率に関する多くの異なる戦略は、階層型 DSCP 廃棄率を使用するこの単一ビデオ キューに基づいて設計することができます。ただし、PA のアプローチは、C：図 8-13 に示すとおりです。

C：図 8-13　　単一ビデオ キュー手法



C：図 8-13 では、音声コールのオーディオは EF とマーキングされ、PQ がこのトラフィックに割り当てる帯域幅に関する厳格なポリサーを使用して、プライオリティ キュー（PQ）に配置されます。ビデオ コールは、優先順位付けされたビデオの AF41 と、状況対応型または Jabber ビデオの AF42 という 2 つのクラスに分けられます。重み付けランダム早期検出（WRED）で CBWFQ を使用すると、管理者は、AF41 に対して AF42 の廃棄優先度を調整できるため、キューがいっぱいになって輻輳が発生したとき、AF42 パケットが AF41 よりも高い確率でキューから廃棄されます。WRED の機能について詳しくは、最新バージョンの Cisco Collaboration SRND に記載されている「*Network Infrastructure*」のセクション「*WAN Quality of Service*」を参照してください。

上記の例には、管理者が、すべてのビデオに対して DSCP ベースの WRED と単一 CBWFQ を使用し、輻輳時のパケット損失から、特定のタイプのビデオ（優先ビデオ）を別の種類のビデオ（状況対応型ビデオ（C：8-23 ページ）を参照）に優先して保護する方法が示されています。この *単一ビデオ キュー手法*では、*デュアル ビデオ キュー手法*とは異なり、ある種類のビデオがキューの帯域幅を使用していない場合、他の種類のビデオが、必要に応じてキューの帯域幅全体の完全なアクセス権を得ることになります。パーベイシブ ビデオを導入する場合、この手法は顕著な改善をもたらします。

ソリューション全体でこの手法を実現するためには、いくつかの条件があります。すべてのオーディオの DSCP を EF としてマーキングするために必要な条件は、次のとおりです。

- 顧客機器（CE）またはサービス プロバイダー（SP）所有の WAN 機器で、AF41 と AF42 両方の QoS マーキングを含む AF4 QoS と、重み付けランダム早期検出（WRED）をサポートしている必要があります。
- すべてのオーディオの EF マーキングと併せ、Enhanced Locations Call Admission Control（ELCAC）を実装できなければなりません。ELCAC は適切な DSCP 設定に依存して、音声およびビデオ CAC プールが表すキューが保護されるようにします。ビデオ コールのオーディオ ストリームの DSCP を変更するには、ELCAC がビデオ コールの帯域幅を差し引く方法を更新する必要があります。それには、CallManager サービスのコール アドミッション制御セクションで、サービス パラメータ [ビデオ コールのオーディオ プールからオーディオ帯域幅を差し引く（Deduct Audio Bandwidth from Audio Pool for Video Call）] を [はい（True）] に設定します。このパラメータは、[はい（True）] または [いいえ（False）] に設定できます。
  - [はい（True）]（推奨）：Cisco Unified CM は、ビデオ コールのオーディオとビデオの帯域幅割り当てを個別のプールに分けます。ビデオ コールのオーディオ部分の帯域幅割り当てはオーディオ プールから差し引かれ、ビデオ コールのビデオ部分はビデオ プールから差し引かれます。
  - [いいえ（False）]（デフォルト）：Cisco Unified CM は従来の動作を適用します。ビデオ コールのオーディオとビデオの帯域幅割り当てをビデオ プールから差し引きます。これがデフォルトの設定です。

状況対応型ビデオ

組織全体で広範囲にビデオを導入する場合、帯域幅の一般的な制約により、利用可能な帯域幅および最繁時のビデオ コールの数に基づいて、一日の最繁時に実現できるビデオ解像度が決まります。PA ではこの課題に対処するために、ネットワークで状況に応じてビデオが処理されるエンドポイントのグループを対象に、DSCP ベースの WRED に Jabber クライアントのコラボレーション メディアの識別および分類戦略を組み合わせた単一のビデオ キューを使用します。

状況対応型ビデオは、任意の時点で利用可能な WAN 帯域幅リソースに応じて、最善のビデオ品質を実現します。これを実現するには、いくつかの要件を満たす必要があります。

- 状況対応型ビデオ エンドポイント グループを選択します。PA では、状況対応型ビデオ エンドポイントとして Jabber クライアントを使用します。
- WAN に、ドロップ優先度が AF41 および AF42 の AF4 DSCP クラス サービスで DSCP ベースの WRED を使用する単一のビデオ キューを設定するようにしてください (AF43 を使用することもできますが、PA で必要な DSCP の値は 2 つだけです)。
- AF42 を使用する状況対応型エンドポイントのビデオを識別して分類します。
- AF41 を使用する他のすべてのビデオ エンドポイントも識別して分類します。

注 エンタープライズ WAN エッジで AF42 マーキングとスケジューリングを使用できない場合は、すべてのビデオに AF41 を使用できます。その場合、この文書で AF42 に設定されている値をすべて AF41 に変更すると、状況対応型ビデオのメリットが最小限になります。AF41 マーキングだけを使用する場合、すべてのビデオが同じようにリソースを取得しようと争い、自動調整ビデオ ネットワークの使用状況に基づいて、同じようにレートを調整します。これにより、設定が簡素化されることにもなります。ただし、このドキュメントでは、Jabber を状況対応型ビデオ エンドポイントとして AF42 でマーキングするために必要な導入手順を説明します。

プロビジョニングとアドミッション制御

帯域幅をプロビジョニングし、適切なビット レートがさまざまなエンドポイント グループ間でネゴシエートされるようにすることは、帯域幅管理の重要な側面です。Unified CM 環境では、ビット レートは Unified CM を介してネゴシエートされます。Unified CM ではリージョンの概念を使用し、特定のコール フローの最大オーディオ ビット レートおよび最大ビデオ ビット レートを設定します。ここでは、ビデオ コールの最大ビット レートに注目します。

Unified CM のロケーション（拡張ロケーションのコールアドミッション制御 を参照）は、リージョンとの組み合わせで、コール フローの特性を定義します。リージョンは、2 つのデバイス間で使用される圧縮とビット レートの種類（8 kbps または G.729、64 kbps または G.722/G.711 など）を定義します。ロケーション リンクは、デバイス間のパスで利用可能な帯域幅の容量を定義します。システム内の各デバイスおよびトランクを（デバイス プールを使用して）リージョンに割り当て、（デバイス プールまたはデバイス自体に直接設定した値を使用して）ロケーションに割り当てます。

- リージョンにより、ビデオ コールの帯域幅を設定できます。リージョンのオーディオ制限により、高いビット レートのコーデックが除外される可能性があります。ただしビデオ コールでは、ビデオの制限により、ビデオの品質（解像度と転送速度）が抑制されます。
- ロケーションは、対象のリンクのすべてのコールで利用可能な総帯域幅の容量を定義します。リンク上でコールが確立すると、そのリンクで許可された総帯域幅からそのコールのリージョンの値を差し引く必要があります。

デバイス グループの最大ビデオ ビット レート（ビデオ解像度）を管理するリージョン マトリックスを作成すると、特定のデバイス グループがネットワーク帯域幅を過剰に使用しないようにすることができます。リージョン マトリックスを作成する際は、次のガイドラインが適用されます。

- 最大ビデオ ビット レート カテゴリにデバイスをまとめます。
- グループの数が少ないほど、帯域幅要件の計算が簡単になります。
- デフォルトのリージョン設定を検討し、マトリックスを簡単にして、リージョン内およびリージョン間のデフォルト値を入力します。
- 組織全体（LAN と WAN の両方）で単一のオーディオ コーデックを使用して、リージョン マトリックスを簡素化します。

リージョン設定の詳細については、「拡張ロケーションのコールアドミッション制御」を参照してください。

C：表 8-5 に、3 つのデバイス グループでのビデオ セッションの最大ビット レート リージョン マトリックスの例を示します。

注　C：表 8-5 は、デバイスのグループ化方法と、デバイス グループ間の通常の解像度に適した最大ビット レートのほんの一例です。

C：表 8-5　3 つのデバイス グループのリージョン マトリックスの例

エンドポイント グループ	Video_1.5MB	Video_2.5MB	Video_20MB
Video_1.5MB	1,500 kbps	1,500 kbps	1,500 kbps
Video_2.5MB	1,500 kbps	2,500 kbps	2,500 kbps
Video_20MB	1,500 kbps	2,500 kbps	20,000 kbps

C：表 8-5 の例で使用されている 3 つのグループは次のとおりです。

- Video_1.5MB

  これらのクライアントは、一般に、導入済みビデオ対応エンドポイントの最大規模のグループになるため、状況対応型ビデオの手法によるメリットがもたらされます。状況対応型ビデオとして分類されると、レートが最大 1,500 kbps（720p @ 30 fps）まで上がり、パケット損失に応じてレートが下方調整されます。

- Video_2.5MB

  これらのデバイスは、Cisco TelePresence MX または SX シリーズなどのルーム システム、あるいは Cisco DX シリーズなどのデスクトップ エンドポイントとなります。これらのエンドポイントは、2,500 kbps の最大ビデオ ビット レートで、通常は 720p @ 30 fps に対応可能です。

- Video_20MB

  このクラスは、Webex Room シリーズ、Cisco Meeting Server、MCU 等の大規模なルームシステム エンドポイント向けに、エンドポイントが最高解像度とフレーム / 秒 (FPS) で実行できるように、最大 20 Mbps に設定されています。マルチスクリーン システムではより多くの帯域幅を使用し、単一画面システムで使用される帯域幅は遥かに少なくなりますが、このグループは、最大ビット レート容量を使用するデバイスに適用されます。

リージョンの設定を簡素化するには、組織全体にわたって使用する 1 つのオーディオ コーデックを基準に標準化することが重要となります。最初の考慮事項は、サイト間のオーディオ コールに低いビット レートのコーデックを使用するかどうかを決定することです。従来、企業では帯域幅管理の一環として、WAN では G.729 などの低いビット レートのコーデックを使用し、LAN や MAN 内でのコールには、ビット レートが高く、バンドの範囲がより広い G.722 などのコーデックを使用していました。通常、コールあたり 2.5 MB でビデオを導入する場合、（コールあたり 80 kbps でも）オーディオが消費する帯域幅はかなり少ないため、企業は組織全体（LAN および WAN）で、ビット レートが高く、より品質に優れたコーデック（G.722 など）を使用する傾向にあります。この決定は、リージョン マトリックスと、サイトごとのリージョンが必要であるかどうかに影響します。ここでの考え方として、リージョン内のオーディオまたはビデオのに異なるビット レートを設定する場合は、サイトごとにリージョンを設定する必要があります。このため、リージョンの設定は、次のようにサイトの数（N）にビデオ グループの数（X）を掛けた値まで増えます。

必要な平均リージョン数 = N*X

WAN と LAN でオーディオ ビット レートを同じにする場合は、ビデオ グループのリージョンのみが必要となります（X）。

拡張ロケーションのコールアドミッション制御

コール アドミッション制御機能は、特に複数のサイトが IP WAN 経由で接続され、オーディオ コールとビデオ コールで使用可能な帯域幅リソースが制限されている場合、コラボレーション システムの重要なコンポーネントとなります。

コール アドミッション制御のアーキテクチャ

Unified CM の Enhanced Locations Call Admission Control

Cisco Unified CM では、Enhanced Locations Call Admission Control（ELCAC）を提供し、複数のクラスタが同じ物理サイトのデバイスを同じ WAN アップリンクを使用して管理している、複雑な WAN トポロジと、Unified CM の分散型配置でのコール アドミッション制御をサポートします。

より複雑な WAN トポロジをサポートするために、Unified CM はロケーション ベースのネットワーク モデリング機能を実装しています。これは、発信側と着信側の間のマルチ ホップ WAN 接続をサポートする機能を Unified CM に提供します。このネットワーク モデリング機能は、段階的にマルチ クラスタの分散型 Unified CM 配置をサポートするように強化されました。これにより、クラスタ全体で同じロケーションに割り当てられた帯域幅を予約、解放、および調整するためにクラスタが相互に通信できるようにすることで、各クラスタがロケーションを「共有」することが可能になります。

ロケーション、リンク、および重みによるネットワーク モデリング

Enhanced Locations CAC はモデル ベースのスタティック CAC メカニズムです。ELCAC では、「ルーテッド WAN ネットワーク」をモデリングするロケーションとリンクを設定するのに、Unified CM で管理インターフェイスを使用する必要があります。このモデルは、WAN ネットワーク トポロジがエンドツーエンドの音声コールとビデオ コールに対し、エンドポイント グループ間のメディアをどのようにルーティングするのかを表します。ネットワークをモデル化するために Unified CM は設定インターフェイスおよびサービスアビリティ インターフェイスを提供しますが、まだ再ルーティングしているネットワーク障害とネットワーク プロトコルを考慮しない「静的」CAC メカニズムです。したがって、WAN ネットワーク トポロジが変更された場合や、WAN での帯域幅割り当てが増減された場合は、このモデルを更新する必要があります。Enhanced Locations CAC もコール指向であり、帯域幅の差し引きはストリームごとではなくコールごとであるため、片方向のストリームのビットレートが反対方向のビットレートよりも高いようなメディア フローの場合、必ず高い方のビットレートに対して双方向で差し引かれます。また、単方向メディア フロー アラウンドは双方向メディア フローであるかのように差し引かれます。

管理者がロケーションとリンクを使用してネットワーク モデルを構築できるように、拡張 CAC は次の設定コンポーネントを組み込みます。

- ロケーション：ロケーションは LAN を表します。これは、エンドポイントを含み、または単に WAN ネットワークのモデル化に対してリンク間の中継場所として機能します。たとえば、MPLS プロバイダーはロケーションで表される可能性があります。
- リンク：リンクはロケーションを相互接続し、ロケーション間で利用可能な帯域幅を定義するために使用されます。リンクは論理的に WAN リンクを表し、ロケーションのユーザ インターフェイス（UI）に設定されます。
- 重み：重みは、ロケーションのペア間に有効なパスを構成するリンクの相対的なプライオリティを与えます。有効なパスは、帯域幅の計算に Unified CM で使用するパスであり、すべての可能なパスにある最小の累積重みが設定されます。重みは、「有効なパス」に「コスト」を提供するためにリンクで使用され、任意の 2 地点間に複数のパスがある場合にだけ該当します。
- パス：パスはロケーション ペアを接続するリンクおよび中間場所のシーケンスです。Unified CM では、各ロケーションから他のすべてのロケーションへの最小コスト パス（最も小さい累積的な重み）をパス計算し、さまざまなパスへのマップを構築します。1 つの「有効なパス」だけがロケーションの任意のペア間で使用されます。
- 有効パス：有効パスは、累積的な重みが最も小さいパスであり、任意の 2 つのロケーション間で常に使用される、帯域幅を考慮したパスです。
- 帯域割り当て：オーディオ、ビデオの各トラフィック タイプ用のモデルで割り当てられる帯域幅。
- Location Bandwidth Manager（LBM）：1 つ以上のクラスタで設定されているロケーションとリンク データからネットワーク モデルを組み立てる、Unified CM でのアクティブなサービス。このサービスでは、2 つのロケーション間の有効なパスを決定し、コールのタイプごとの帯域幅の可用性に基づいて 2 つのロケーション間のコールを許可するかどうかを決定し、許可された各コールの実行期間の帯域幅を差し引きます（予約します）。
- Location Bandwidth Manager ハブ：固定ロケーション、リンクのデータおよびダイナミック帯域幅割り当てのデータのクラスタ間のレプリケーションに直接参加するように指定された Location Bandwidth Manager（LBM）サービス。LBM のハブ グループに割り当てられている複数の LBM は、共通の接続を介して互いに探索し、フル メッシュ構造のクラスタ間のレプリケーション ネットワークを形成します。LBM ハブを持つクラスタ内の他の LBM サービスはクラスタの LBM のハブを介してクラスタ間のレプリケーションに間接的に参加します。

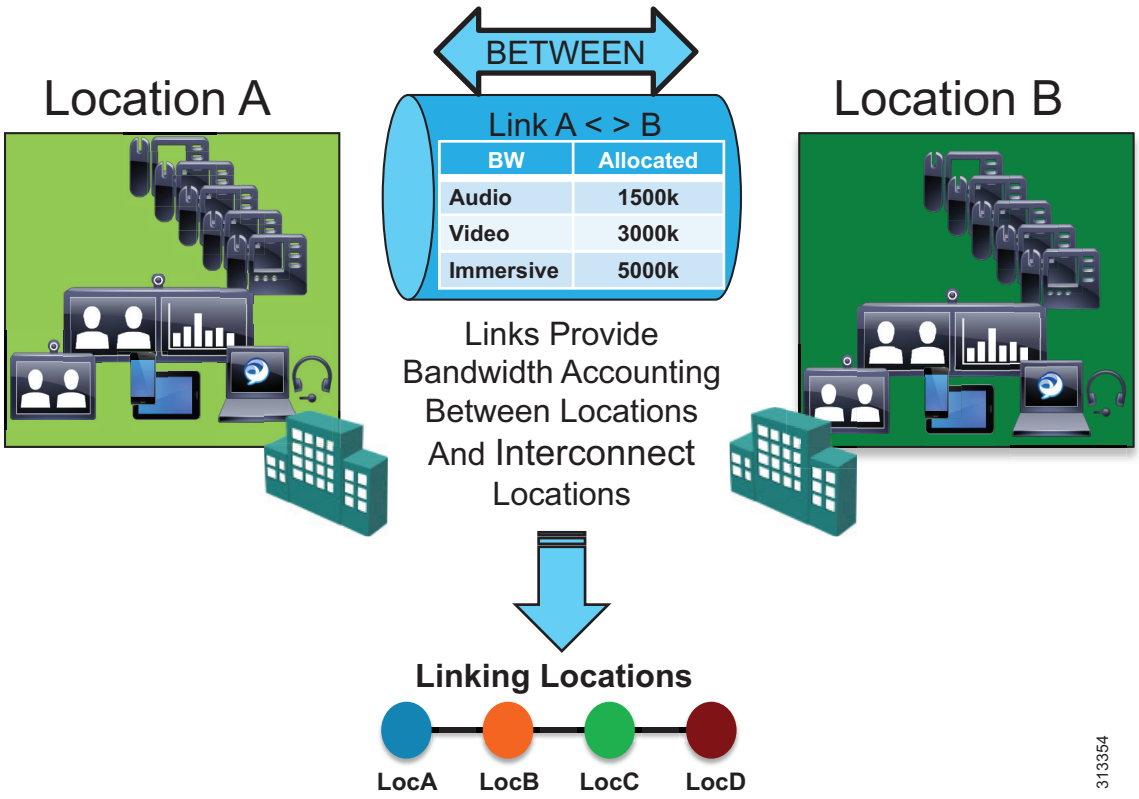
ロケーション、リンク、重み

Unified CM は、ロケーションの概念を使用して物理的なサイトを表し、エンドポイント、ボイス メッセージ ポート、トランク、ゲートウェイなどのメディア デバイスとの関連付けを作成します。これは、デバイス自体に直接設定した値、デバイス プール、またはデバイス モビリティを通じて行われます。ロケーションは、ローカル エリア ネットワーク（LAN）を論理的に表します。Unified CM では、ロケーションを相互接続するため、そしてロケーション間で使用可能な帯域幅を定義するために、リンクと呼ばれる設定パラメータも使用します。リンクは、ワイド エリア ネットワーク（WAN）を論理的に表すものです。ここでは、ロケーションおよびリンクおよびその使用方法について説明します（C：図 8-14 を参照）。

ロケーション設定自体は、リンク、ロケーション間の帯域幅パラメータ、および RSVP ロケーションの設定の 3 つの主要部分で構成されます。ロケーション内の帯域幅パラメータは、デフォルトでは無制限に設定されます。ロケーション（LAN）内で帯域幅を制限する理由はほとんど、あるいはまったくないため、この設定はそのままにしておいてください。Enhanced Location CAC に対する RSVP ロケーションの設定は、RSVP 実装にのみ適用されるため、ここでは考慮されません。

リンク帯域幅パラメータは、管理者が「隣接ロケーション」（つまり、その間で設定されたリンクがあるロケーション）間の音声、ビデオ、およびイマーシブ コール用にプロビジョニングされた帯域幅を特徴付けることができます。この機能により管理者にマルチ ホップ WAN ネットワークをモデル化するロケーションの組み合わせのストリングを作成する機能を提供します。

C：図 8-14　　ロケーションおよびリンク



2 つのロケーション間で複数のパスを使用できる場合、リンクに重みを設定して、特定のパスが強制的に選択されるようにすることができます。複数のパスが設定されている場合、累積重みに基づいて 1 つだけが選択され、このパスが*有効なパス*と呼ばれます。この重みはスタティックであり、有効なパスを動的に変更されません。2 つの重みが同じである場合は、どちらか一方のパスがランダムに選択されます。したがって、1 つのパスだけが存在するようにするか、あるいは 1 つのパスだけに Location Bandwidth Manager（LBM）の有効パスになるような累計的な重みを持たせることが重要です。これは、マルチ クラスター環境では特に重要性が大きくなります。ほとんどの場合、デフォルトの重みを変更する必要はありませんが、2 つのロケーション間に同じ重みを持つ複数のパスが存在する場合、いずれかのパスの重みを変更して、そのパスが有効パスとして選択されるようにする必要があります。

Unified CM でデバイスを設定するときは、そのデバイスをロケーションに割り当てることができます。ロケーションは、トポロジを構築するために他のロケーションへのリンクで設定できます。Unified CM で設定するロケーションは、仮想ロケーションであり、実際の物理ロケーションではありません。前述のように、Unified CM は、ネットワーク内の実際の物理トポロジを認識しません。したがって Unified CM ロケーション モデルの実際の基本ネットワーク トポロジをマッピングするには、Unified CM の物理ネットワークに対する変更は手動で加える必要があります。デバイスが 1 つの物理ロケーションから他のロケーションに移動されると、システム管理者は、Unified CM がそのデバイスとの間で正しくコールの帯域幅割り当てを計算できるように、ロケーション設定の手動アップデートを実行するかデバイス モビリティ機能を実装する必要があります。各デバイスは、デフォルトでは **Hub_None** ロケーションに配置されます。ロケーション Hub_None は、通常、複数のロケーションをリンクするハブとして動作し、音声およびビデオ帯域幅の無制限のロケーション内帯域幅割り当てがデフォルトで設定されるロケーションの例です。

統一された CM では管理者が、ロケーション間のリンクごとに別の音声およびビデオの帯域幅プールを定義することができます。PA では、音声およびビデオ帯域幅プールのみを使用します。通常、ロケーション間のリンクは、物理サイト間の WAN リンクにプロビジョニングされた、オーディオとビデオに使用可能な帯域幅の量に対応する、有限数のキロ ビット / 秒（kbps）に設定されます。一部の WAN では、予期されるトラフィック量以上の量がプロビジョニングされているため、制限は不要です。帯域幅の値が有限数のキロ ビット / 秒（kbps）に設定されている場合、Unified CM はロケーション内のすべてのコール、および中継ロケーション（計算パス内にあるが、パス内の発信または着信ロケーションではないロケーション）としてロケーションを使用するすべてのコールをトラッキングします。

ロケーションには、次のデバイスを設定する必要があります。

- エンドポイント
- カンファレンス ブリッジ
- ゲートウェイ
- SIP トランク
- 保留音（MoH）サーバ
- アナンシエータ（デバイス プールを使用）

C：表 8-6 に、さまざまなコール速度で必要となる帯域幅の量を記載します。すべてのオーディオ（音声のみのコールのオーディオとビデオ コールに含まれるオーディオの両方）については、Unified CM はメディア ビット レートに加え、IP と UDP のオーバーヘッドを考慮します。たとえば、G.711 または G.722 の音声コールでは、ロケーションとリンクのオーディオ帯域幅の割り当てから差し引かれた 80 kbps（64 kbps ビット レート + IP/UDP ヘッダー用の 16 kbps）が消費されます。ビデオ コールについては、Unified CM はビデオ ストリームのペイロードしか考慮しませんが（IP/UDP ヘッダーのオーバーヘッドは考慮されません）、オーディオ部分は IP および UDP オーバーヘッドを使用して計算されます。たとえば、ビット レート 384 kbps のビデオ コールで、オーディオには ビット レート 64 kbps を使用するように設定されている場合、Unified CM はビデオ帯域幅割り当てから 320 kbps を割り当て、そこからオーディオ用に 64 kbps を使用し、IP/UDP ヘッダー用の 16 kbps を加算してオーディオ プールから 80 kbps を差し引きます。同じビデオ コールで、オーディオには ビット レート 8 kbps を使用するように設定されている場合、Unified CM はビデオ帯域幅割り当てから 376 kbps を割り当て、そこからオーディオ用に 8 kbps を使用し、IP/UDP ヘッダー用の 16 kbps を加算してオーディオ プールから 24 kbps を差し引きます。

C：表 8-6　PA 設定でのロケーションおよびリンクの帯域幅の差し引きアルゴリズムによって要求される帯域幅の量[1]

コール速度（セッション ビット レート）	オーディオ プール帯域幅	ビデオ プール帯域幅
G.711 または G.722 音声コール（64 kbps）	80 kbps	該当なし
G.729 音声コール（8 kbps）	24 kbps	該当なし
G.729 オーディオ（8 kbps）を使用した 512 kbps のビデオ コール	24 kbps	504 kbps
G.711 または G.722 オーディオ（64 kbps）を使用した 512 kbps のビデオ コール	80 kbps	448 kbps
G.729 オーディオ（8 kbps）を使用した 768 kbps のビデオ コール	24 kbps	760 kbps
G.711 または G.722 オーディオ（64 kbps）を使用した 768 kbps のビデオ コール	80 kbps	704 kbps
G.729 オーディオ（8 kbps）を使用した 1,024 kbps のビデオ コール	24 kbps	1,016 kbps
G.711 または G.722 オーディオ（64 kbps）を使用した 1,024 kbps のビデオ コール	80 kbps	960 kbps

1. この例で使用されているのは 8 kbps と 64 kbps だけですが、他のオーディオ ビット レートのコーデックにも同じ原理が適用されます。ビデオ ビット レートの値を調整するために、ビデオ ビット レートからオーディオ ビット レート（ペイロードのみ）が差し引かれます。

たとえば Hub_None への支社 1 のロケーションのリンク設定が使用可能なビデオ帯域幅 256 kbps および音声帯域幅 1,024 kbps を割り当てるとします。この場合支社 1 から Hub_None へのパスは、最高 3 つの G.711 音声コール（コールごとに 80 kbps）、または 10 の G.729 音声コール（コールごとに 24 kbps）、または 256 kbps を超えない両方の組み合わせをサポートできます。このロケーション間のリンクでは、使用されているビデオ コーデックおよびオーディオ コーデックに応じて、さまざまな数のビデオ コールをサポートすることもできます（たとえば、1,024 kbps の帯域幅を要求する 1 つのビデオ コール、またはそれぞれ 512 kbps の帯域幅を要求する 2 つのビデオ コールをサポートできます）。

あるロケーションから他のロケーションにコールが発信されると、Unified CM は、ロケーションおよびあるロケーションから他のロケーションへのリンクの有効なパスから適切な帯域幅を差し引きます。コールが完了すると、Unified CM は有効なパス上でこれらの同じリンクに帯域幅を返却します。十分な帯域幅がパス上のリンクのいずれかにない場合、コールは Unified CM によって拒否され、発信者はネットワーク ビジー トーンを受信します。発信側デバイスが、ディスプレイを備えた IP Phone である場合、そのデバイスには、「Not Enough Bandwidth」というメッセージも表示されます。

ロケーション間コールがコール アドミッション制御によって拒否された場合、Unified CM は自動代替ルーティング（AAR）機能を使用して、PSTN 接続を通じて宛先にコールを自動的に再ルーティングできます（自動代替ルーティング（C：2-52 ページ）を参照）。

注　AAR は、有効なパスに沿ってネットワーク帯域幅が不足しているために、Enhanced Locations Call Admission Control によってコールが拒否される場合のみ、呼び出されます。このような場合、コールは着信側デバイスの [Call Forward No Answer] フィールドで指定されている宛先に転送されます。IP WAN が使用不可の場合や、接続に関するその他の問題によって着信側デバイスが Unified CM に登録されない状態になった場合には、AAR は呼び出されません。

また、AAR はクラスタ内のエンドポイント間コールにのみ適用されます。CAC に失敗したクラスタ間のすべてのコールには、別の SIP ルーティング パスを試すためにルート グループが使用されます。

デバイス間のビデオ コールが CAC に失敗した場合、ビデオ デバイスで [ビデオ コールをオーディオとして再試行（Retry Video Call as Audio）] を有効にすることもできます。このオプションは、Unified CM のビデオ エンドポイントまたは SIP トランクの設定ページで設定され、コールを発信するビデオ エンドポイントまたはトランクに適用できます。一部のビデオ エンドポイントでは、デフォルトで [ビデオコールをオーディオとして再試行（Retry Video Call as Audio）] が有効にされて、エンドポイント上で設定可能になっていません。

ロケーション、リンク、リージョンの設定

ロケーション リンクは、リージョンとの組み合わせで、ロケーションおよびリンクに有効なパス上でコールの特性を定義します。リージョンはデバイス間で使用される圧縮のタイプまたはビット レート（G.729 では 8 kbps、G.722/G.711 では 64 kbps など）を定義し、ロケーション リンクはデバイス間の有効なパスで使用可能な帯域幅の量を定義します。システム内の各デバイスを（デバイス プールを使用して）リージョンに割り当て、（デバイス プールまたはデバイス自体に直接設定した値を使用して）ロケーションに割り当てます。

Unified CM では、ロケーションを設定することにより、次の要素を定義できます。

- 物理的なサイト（たとえば、ブランチ オフィス）または中継サイト（たとえば、MPLS クラウド）：場所は LAN を表します。これは、エンドポイントを含み、または単に WAN ネットワークのモデル化に対してリンク間の中継場所として機能します。
- 隣接するロケーション間のリンク帯域幅：リンクはロケーションを相互接続し、ロケーション間で利用可能な帯域幅を定義するために使用されます。リンクは物理的なサイト間の WAN リンクを論理的に表します。
  - 音声帯域幅：ロケーション デバイスから設定された隣接した場所に行われる音声および FAX コールの WAN リンクで使用可能な帯域幅の量。Unified CM は、Enhanced Locations Call Admission Control にこの帯域幅値を使用します。
  - ビデオ帯域幅：ロケーション デバイスから設定された隣接した場所に行われたビデオ コール用の WAN リンクで使用可能なビデオ帯域幅の量。Unified CM は、Enhanced Locations Call Admission Control にこの帯域幅値を使用します。
  - イマーシブ ビデオ帯域幅：PA 構成では使用されません。

  Unified CM では、リージョンを設定することにより、次の要素を定義できます。
- 最大オーディオ ビット レート
- ビデオ コール（オーディオを含む）の最大セッション ビット レート
- イマーシブ ビデオ コール（オーディオを含む）の最大セッション ビット レート：PA 構成では使用されません。
- オーディオ コーデック プリファレンス リスト

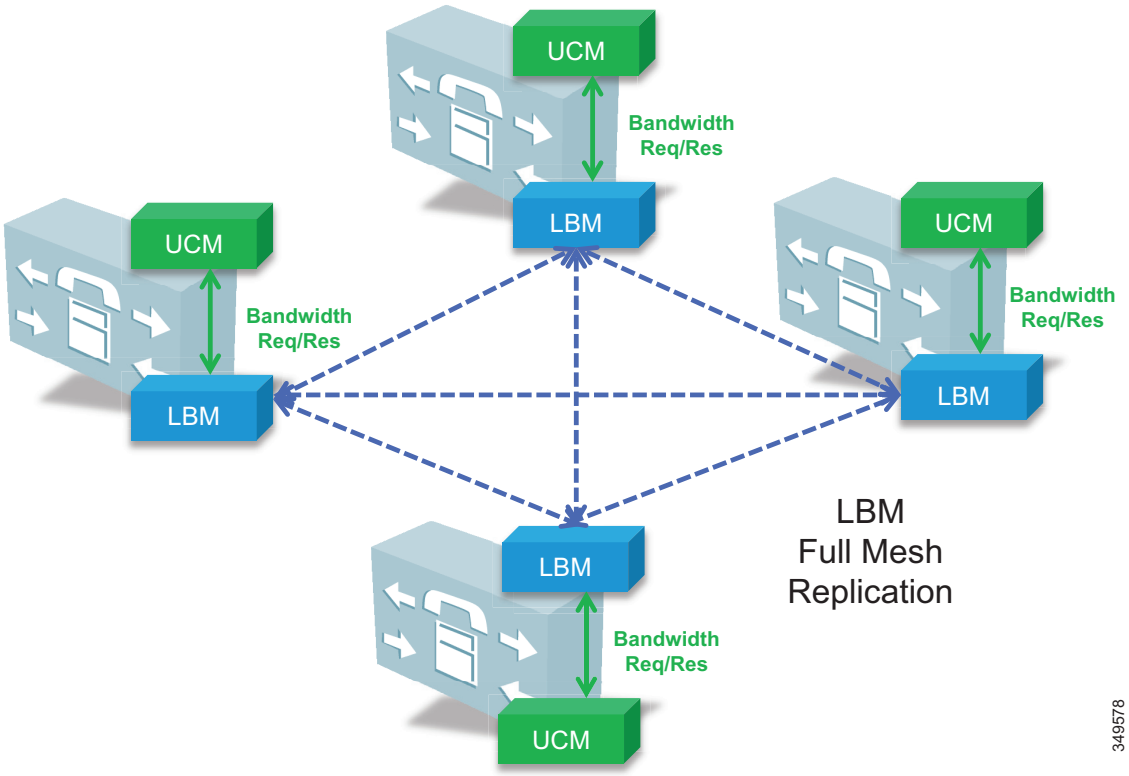
Location Bandwidth Manager

Location Bandwidth Manager（LBM）は、サービスアビリティ Web ページから管理し、Enhanced Locations CAC 帯域幅の機能すべてを担当する Unified CM 機能サービスです。Cisco CallManager サービスも実行しているクラスタ内の各サブスクライバ ノード上で動作するように LBM を設定してください。

LBM では次の機能が実行されます。

- ロケーションおよびリンク パスのトポロジを組み合わせる
- トポロジにわたる有効なパスの計算
- Cisco CallManager サービス（Unified CM 呼制御）からのサービスの帯域幅要求
- 他の LBM への帯域幅情報の複製（C：図 8-15 を参照）
- 設定済みのダイナミック情報をサービスアビリティに提供
- Location Real-Time Monitoring Tool（RTMT）カウンタの更新

C：図 8-15　LBM のローカル レプリケーション ネットワーク



デフォルトでは、CallManager サービスは、ローカル LBM サービスと通信します。

音声プールからのすべてのオーディオの差し引き

この PA では、管理者がビデオ コールのオーディオ帯域幅を音声プールから差し引くために使用できる、新しい Unified CM 11.*x* 機能を使用しています。ELCAC は音声とビデオ CAC プールが表示するキューを確実に保護するために適切な DSCP 設定を使用するため、Unified CM がビデオ プールから帯域幅を差し引く方法を変更するには、ビデオ コールのオーディオ ストリームの DSCP をオーディオ専用コールのオーディオ ストリームと同じようにマーキングする必要があります。

Unified CM でこの機能をイネーブルにするには、CallManager サービスのコール アドミッション制御セクションで、サービス パラメータ [ビデオ コールのオーディオ プールからオーディオ帯域幅を差し引く（Deduct Audio Bandwidth from Audio Pool for Video Call）] を [はい（True）] に設定します。デフォルト設定は [いいえ（False）] であり、デフォルトでは、Unified CM はビデオ プールからビデオ コールのオーディオとビデオの両方のストリームを差し引きます。

マルチクラスターに関する考慮事項

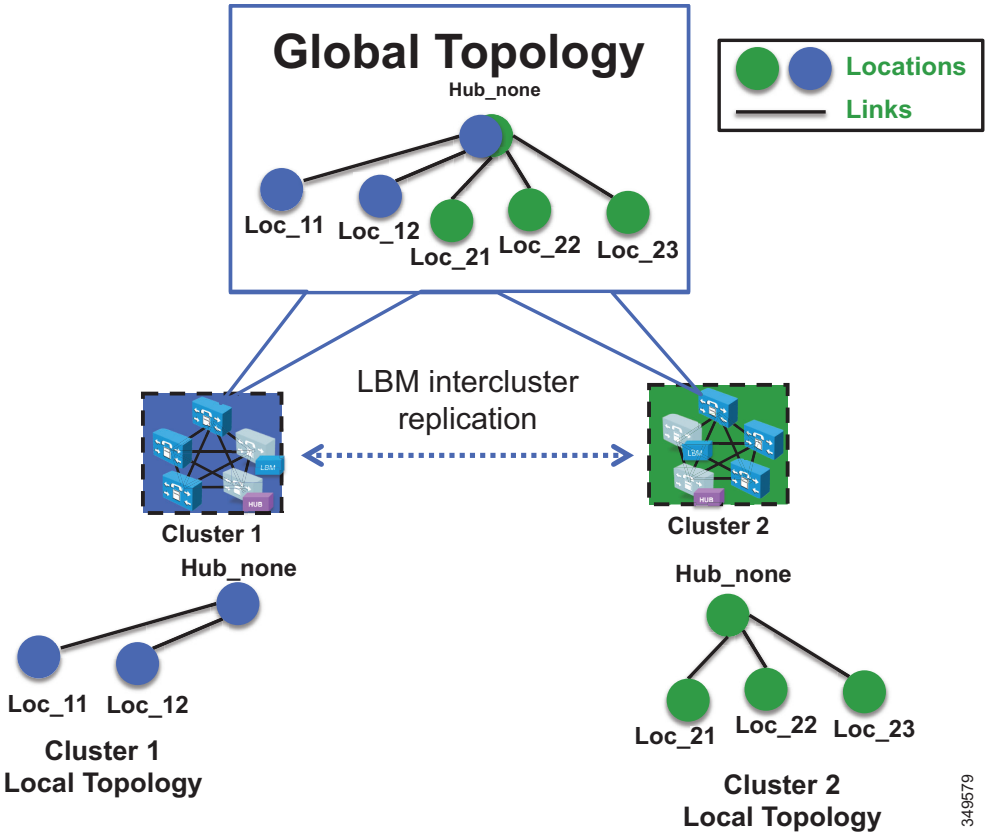
この項では、次の項目について説明します。

- クラスタ内 ELCAC
- LBM のハブのレプリケーション ネットワーク
- 共通ロケーション（共有ロケーション）およびリンク
- シャドウ ロケーション
- ロケーションおよびリンク管理クラスタ

クラスタ内 ELCAC

クラスタ間の Enhanced Locations CAC は、複数のクラスタにわたるネットワーク モデリングの概念を拡張します。クラスタ間の Enhanced Locations CAC では、各クラスタは、ロケーションとリンク上でローカルに設定されたトポロジを管理し、LBM クラスタ間のレプリケーション ネットワーク内にある他のリモート クラスタにこのローカル トポロジを伝播します。リモート クラスタのトポロジを受け取ると、LBM は独自のローカル トポロジにこれを再構成し、グローバル トポロジを作成します。このプロセスによって、グローバル トポロジはすべてのクラスタ間で同じになり、エンドツーエンド CAC に対する企業ネットワーク トポロジの全体的視野を各クラスタに提供します。C：図 8-16 は、単純なハブアンドスポーク ネットワーク トポロジを持つグローバル トポロジの概念を例として示します。

C：図 8-16　　単純なハブアンドスポーク ネットワークのグローバル トポロジの例



C：図 8-16 に示されているクラスタ 1 とクラスタ 2 の 2 つのクラスタには、それぞれローカルにハブアンドスポーク ネットワーク トポロジが設定されています。クラスタ 1 の Hub_None には Loc_11 と Loc_12 へのリンクが設定され、クラスタ 2 の Hub_None には Loc_21、Loc_22、Loc_23 へのリンクが設定されています。クラスタ間の Enhanced Locations CAC が有効にされていると、クラスタ 1 はそのローカル トポロジをクラスタ 2 に送信し、クラスタ 2 もそのローカル トポロジをクラスタ 1 に送信します。各クラスタはリモート クラスタのトポロジのコピーを取得した後、各クラスタはオーバーレイ独自上のリモート クラスタのトポロジを自身のトポロジ上にオーバーレイします。オーバーレイは、同じ名前で設定されたロケーションの一般的な場所によって実現されます。クラスタ 1、クラスタ 2 の両方に同じ名前の共通のロケーション Hub_None があるため、各クラスタは、共通の場所として Hub_None により他方のネットワーク トポロジをオーバーレイし、Hub_None がハブで Loc_11、Loc_12、Loc_21、Loc_22、および Loc_23 がすべてスポーク ロケーションであるグローバル トポロジを作成します。これは単純なネットワーク トポロジの例ですが、より複雑なトポロジは同じ方法で処理されます。

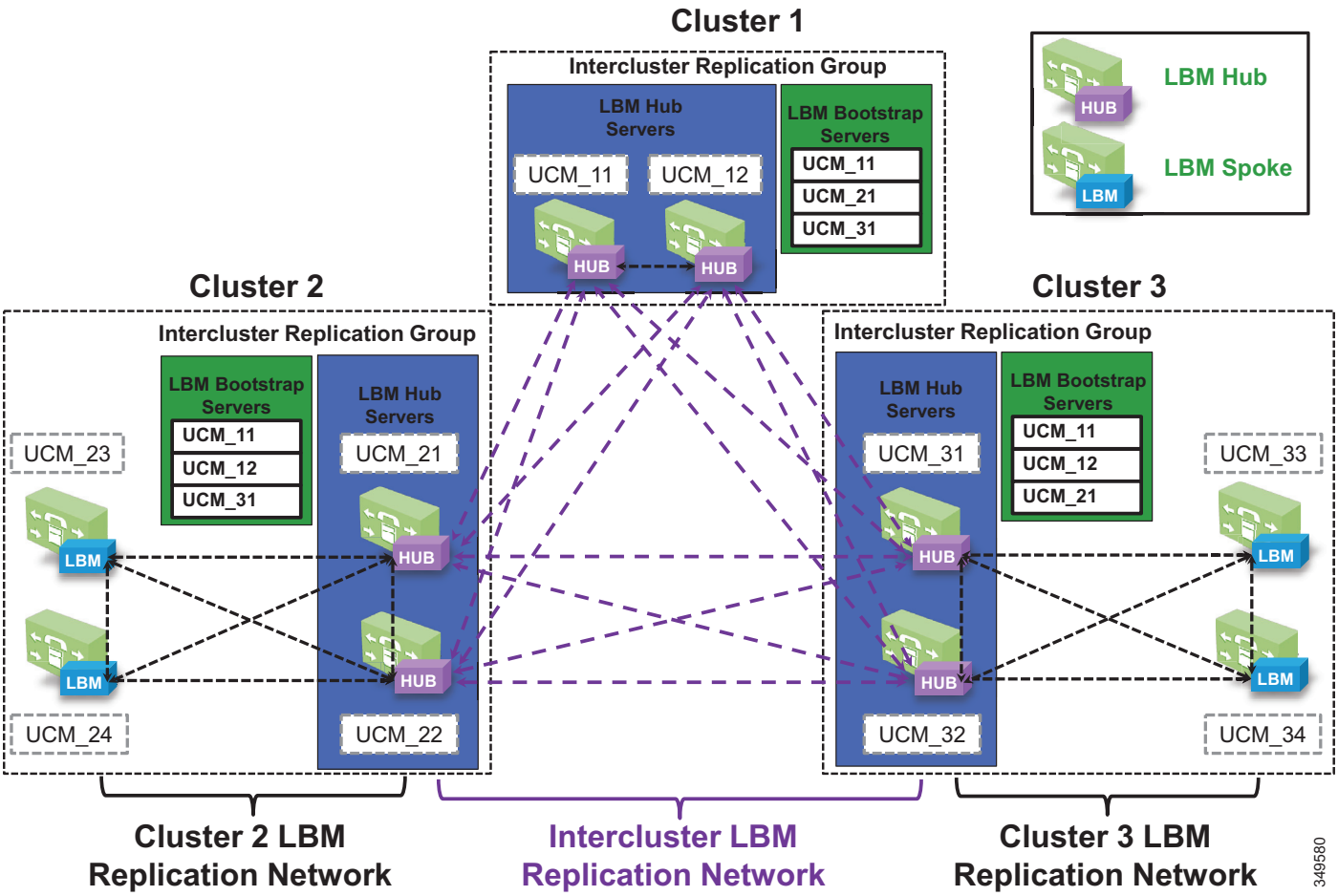
LBM のハブのレプリケーション ネットワーク

クラスタ間 LBM のレプリケーション ネットワークは、LBM ハブと呼ばれる指定 LBM の個別のレプリケーション ネットワークです。LBM ハブは、個別のフル メッシュを相互に作成し、ローカル クラスタのトポロジを他のリモート クラスタに複製します。各クラスタは、グローバル トポロジを作成するために、他のすべてのリモート クラスタからトポロジを効果的に受信します。クラスタ間のレプリケーション ネットワークの指定 LBM は、*LBM ハブ*と呼ばれます。クラスタ内でだけ複製する LBM は *LBM スポーク*と呼ばれます。LBM のハブは、LBM **クラスタ間のレプリケーション グループ**による設定で指定されます。クラスタ内のいずれの LBM でも、その LBM ロールの割り当てを、クラスタ間レプリケーション グループの設定で、ハブまたはスポークのロールに変更することができます（LBM ハブ グループの設定について詳しくは、Cisco Unified Communications Manager 製品マニュアル（https://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html）を参照してください）。

LBM クラスタ間のレプリケーション グループでは、ブートストラップ LBM の概念もあります。ブートストラップ LBM は、他のすべての LBM ハブに、フル メッシュのハブ レプリケーション ネットワークを作成するために必要な接続の詳細を提供する LBM ハブです。ブートストラップ LBM は、すべての LBM ハブが持つことができるロールです。すべての LBM ハブが 1 つの LBM ハブを指す場合、その 1 つの LBM ハブが他のすべての LBM ハブに相互に接続する方法を伝えます。各レプリケーション グループは、最大 3 つのブートストラップ LBM を参照できます。

LBM のハブ グループが各クラスタに設定されると、指定 LBM ハブはフル メッシュのクラスタ間のレプリケーション ネットワークを作成します。C：図 8-17 に示すクラスタ間レプリケーション ネットワークの設定では、3 つのクラスタ（クラスタ 1、クラスタ 2、クラスタ 3）の間に LBM ハブ グループを設定してクラスタ間レプリケーション ネットワークを形成しています。

C：図 8-17　　3 つのクラスタのクラスタ間レプリケーション ネットワークの例



C：図 8-17 では、各クラスタから 2 つの LBM がクラスタの LBM のハブとして指定されます。これにより、LBM ハブのロールに冗長性がもたらされます。これらの LBM ハブは、クラスタ間の LBM レプリケーション ネットワークを形成します。各 LBM クラスタ間のレプリケーション グループに設定されたブートストラップ LBM は、UCM_11、UCM_12 として指定されています。クラスタ 1 のこれら 2 つの LBM ハブは、クラスタ間 LBM のレプリケーション ネットワーク全体の窓口またはブートストラップ LBM として機能します。クラスタ 2 の UCM_21 とクラスタ 3 の UCM_31 はそれぞれ、プライマリが使用可能でない場合（つまり、クラスタ 1 が使用可能でない場合）、バックアップ ルートストラップ LBM ハブとして機能します。クラスタ間 LBM のレプリケーション ネットワークを確立するということは、各クラスタ内のそれぞれの LBM ハブが UCM_11 に接続して、そのローカル トポロジを複製し、リモート トポロジを取得することを意味します。また、UCM_11 から他のクラスタの接続情報を取得し、他のリモート クラスタに接続して、それぞれのトポロジを複製します。これは、フル メッシュのレプリケーション ネットワークを作成します。UCM_11 が使用できない場合、LBM ハブは UCM_12 に接続します。クラスタ 2 の LBM ハブが使用できない場合、クラスタ 2 とクラスタ 3 の LBM ハブは UCM_31 に接続し、クラスタ 3 の LBM ハブは UCM_21 に接続します。

LBM には、LBM クラスタ間のレプリケーション ネットワークに関する次の役割があります。

- LBM ハブ（ローカル LBM）
  - クラスタ間 LBM のレプリケーション ネットワークの一部として他のリモート ハブと直接通信する
- LBM スポーク（ローカル LBM）
  - クラスタのローカル LBM のハブと直接通信し、ローカル LBM のハブを介してリモート LBM のハブと間接的に通信する
- ブートストラップ LBM
  - レプリケーション ネットワーク内のすべてのクラスタの LBM ハブを相互接続する LBM ハブ
  - ネットワーク内の任意の LBM ハブを使用できる
  - LBM クラスタ間のレプリケーション グループごとに最大 3 つのブートストラップ LBM ハブを表示できる
- LBM のハブのレプリケーション ネットワーク：帯域幅の差し引きと調整メッセージ
  - LBM は各クラスタから送信元および受信者を選択して、LBM メッセージを最適化する

LBM ハブは、通信を暗号化するように設定することもできます。これは、クラスタ間のリンクが保護されていないネットワークに存在する可能性があるためにクラスタ間のトラフィックの暗号化が欠かせない環境に、クラスタ間 ELCAC を配置することを可能にします。暗号化されたシグナリングを LBM ハブ間に設定する方法の詳細については、次の Web サイトで入手可能な Cisco Unified Communications Manager の製品マニュアルを参照してください。

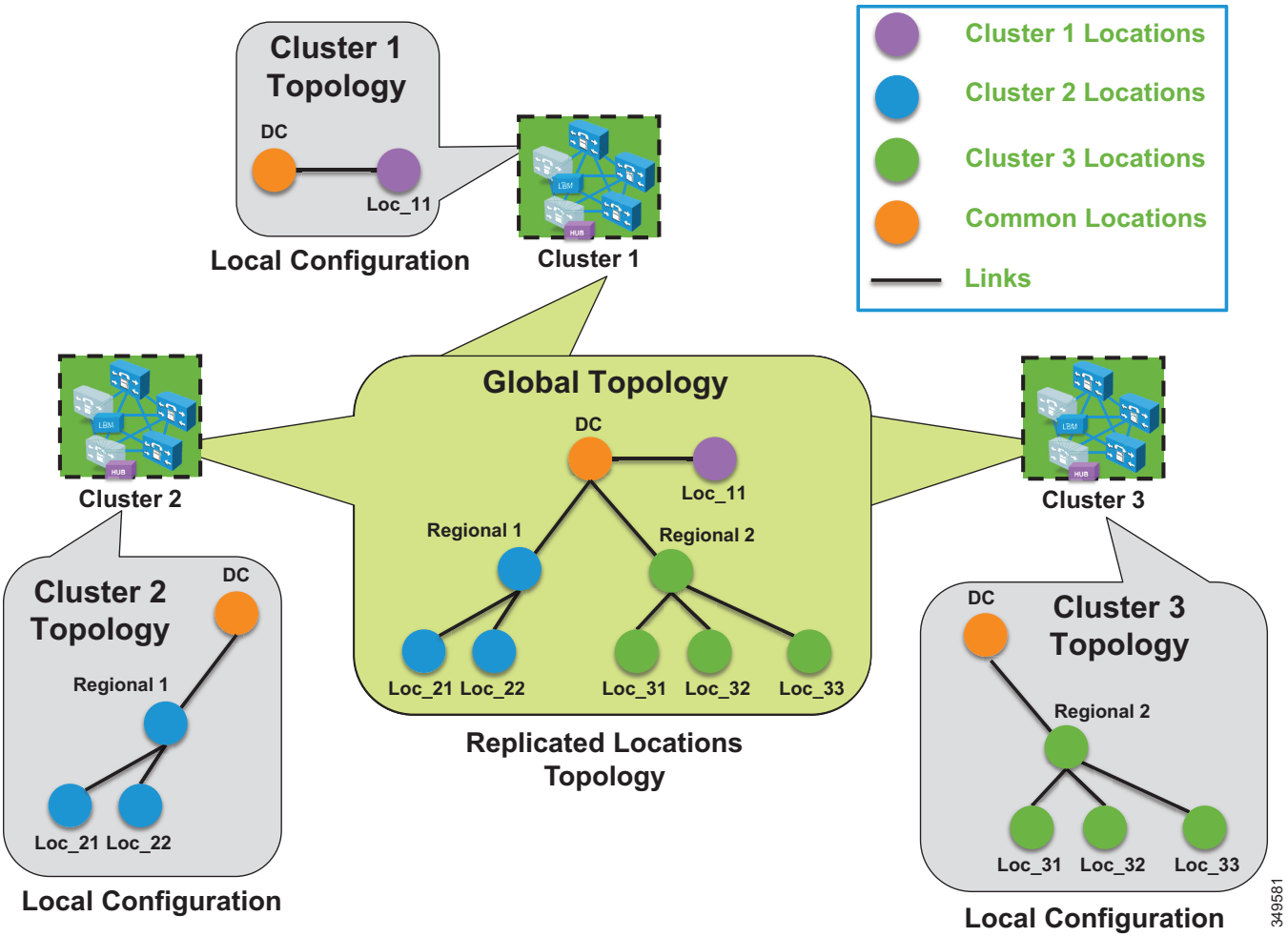
https://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

共通ロケーション（共有ロケーション）およびリンク

共通ロケーションとは、すべてのクラスタで同じ名前が付けられたロケーションのことです。共通ロケーションは、LBM がグローバル トポロジを作成する方法、および複数のクラスタ間で 1 つのロケーションを関連付ける方法において重要な役割を果たします。複数のクラスタ間で名前が共通するロケーションは同じロケーションと見なされるため、これらのクラスタ間での共有ロケーションとなります。あるロケーションが複数のクラスタ間で共有されるようにするには、名前がまったく同じである必要があります。複製後も、LBM は、ロケーションとリンクでの設定の矛盾点について確認します。帯域幅値の不一致、または共通ロケーションとリンク間の重みはサービスアビリティで表示でき LBM は、重みの帯域幅と最小値（最低コスト）の最も厳しい値のロケーションおよびリンク パスを計算します。

共通のロケーションとリンクは、いくつかの異なる理由でクラスタ全体に対して設定できます。同じ物理サイトのデバイスを管理し、同じ WAN アップリンクを使用するいくつかのクラスタを使用することがあるため、同じロケーションは、各クラスタのローカル デバイスにそのロケーションを関連付けるために各クラスタに設定する必要があります。独自のトポロジを管理するクラスタがある場合もありますが、これらのトポロジは、特定のロケーションにおいて相互接続されるため、これらのロケーションを各クラスタ間の共通ロケーションとして設定する必要が生じます。そうすることで、グローバル トポロジが作成されている際に、クラスタでは、各クラスタで共通の相互接続ロケーションとリンクを持ち、各リモート トポロジをともに効果的にリンクさせることができるようになります。C：図 8-18 はトポロジをリンクすることを示し、各クラスタが共有する共通トポロジを示します。

C：図 8-18　グローバル トポロジを作成する共通のロケーションとリンクの使用



C：図 8-18 に示されているクラスタ 2 には、リージョン 1 のロケーション Loc_11 と Loc_12 にデバイスがありますが、グローバル トポロジの他の部分にリンクするためには、DC と、リージョン 1 から DC へのリンクを設定する必要があります。クラスタ 3 も同様に、リージョン 2 の Loc_31、Loc_32、Loc_33 にデバイスがありますが、グローバル トポロジにマッピングするために、DC と、DC からリージョン 2 へのリンクを設定する必要があります。クラスタ 1 には Loc_11 にしかデバイスがないため、DC と、DC から Loc_11 へのリンクを設定して、クラスタ 2 とクラスタ 3 のトポロジにマッピングする必要があります。

クラスタからクラスタへのトポロジ マッピングのキーは、トポロジを相応に相互接続するように少なくとも 1 つのクラスタに別のクラスタの共通ロケーションがあることを確認します。

シャドウ ロケーション

シャドウ ロケーションを使用して、Enhanced Locations CAC がクラスタ間で機能するために必要となる、ロケーションの名前をはじめとする Enhanced Locations CAC 情報を SIP トランクが渡せるようにします。クラスタ全体でこのロケーション情報を渡すためには、SIP クラスタ間トランク（ICT）を「シャドウ」ロケーションに割り当てる必要があります。シャドウ ロケーションは他の場所へのリンクを持つことができないため、帯域幅はシャドウ ロケーションと別のロケーションの間で予約できません。Hub_None に関連付けられたように、シャドウ ロケーションに割り当てられた SIP ICT 以外のいずれかのデバイスが処理されます。

ロケーションおよびリンク管理クラスタ

設定のオーバーヘッドを防ぐため、そして多数のロケーションを共有するクラスタで設定が重複しないようにするために、グローバル トポロジに含まれるすべてのロケーションとリンクを管理するロケーションおよびリンク管理クラスタを設定できます。他のすべてのクラスタはロケーションからデバイスへの関連付けに必要なロケーションを一意に設定し、無制限以外のリンクまたは帯域幅値を設定しません。ロケーションおよびリンク管理クラスタは設計概念です。LBM のレプリケーション ネットワーク上の他のすべてのクラスタは、帯域幅の値を無制限に設定したロケーションだけで構成され、リンクは設定されないのに対し、ロケーションおよびリンク管理クラスタはロケーションとリンクのグローバル トポロジ全体を設定したクラスタに過ぎません。クラスタ間の Enhanced Locations CAC がイネーブルになり、LBM のレプリケーション ネットワークが設定されている場合、すべてのクラスタがネットワーク ビューを複製します。指定したロケーションおよびリンク管理のクラスタには、ロケーション、リンクおよび帯域幅の値を持つグローバル トポロジ全体があります。これらの値は、複製されると最も制限的になるため、すべてのクラスタで使用されます。この設計によって、多数の共通のロケーションが複数のクラスタ間で必要な配置の設定オーバーヘッドが軽減されます。

推奨事項

ロケーションおよびリンク管理クラスタ：

- 1 つのクラスタを管理クラスタ（ロケーションとリンクを管理するために選択したクラスタ）として選択する必要があります。
- クラスタ管理は次のように設定する必要があります。
  - 企業内のすべてのロケーションは、このクラスタに設定されます。
  - すべてのロケーションとリンクの帯域幅値と重みは、このクラスタで管理されます。

企業内の他のすべてのクラスタ：

- 企業内の他のすべてのクラスタは、デバイスへの関連付けに必要なロケーションのみを設定する必要があります。ロケーション間のリンクを設定してはなりません。このリンク情報は、クラスタ間の Enhanced Locations CAC が有効な場合に管理クラスタから取得されます。デフォルトでは、新しく追加されるロケーションと hub_none の間には、常に 1 つのリンクが設定されます。hub_none を使用しない場合、あるいは構築しているトポロジに hub_none が適切でない場合は、このリンクを削除してください。
- クラスタ間 Enhanced Locations CAC を有効にすると、管理クラスタからすべてのロケーションとリンクが複製されます。

これらが複製された後、LBM は常に、最も小さく最も限定的な帯域幅と、最も小さい重みの値を使用します。

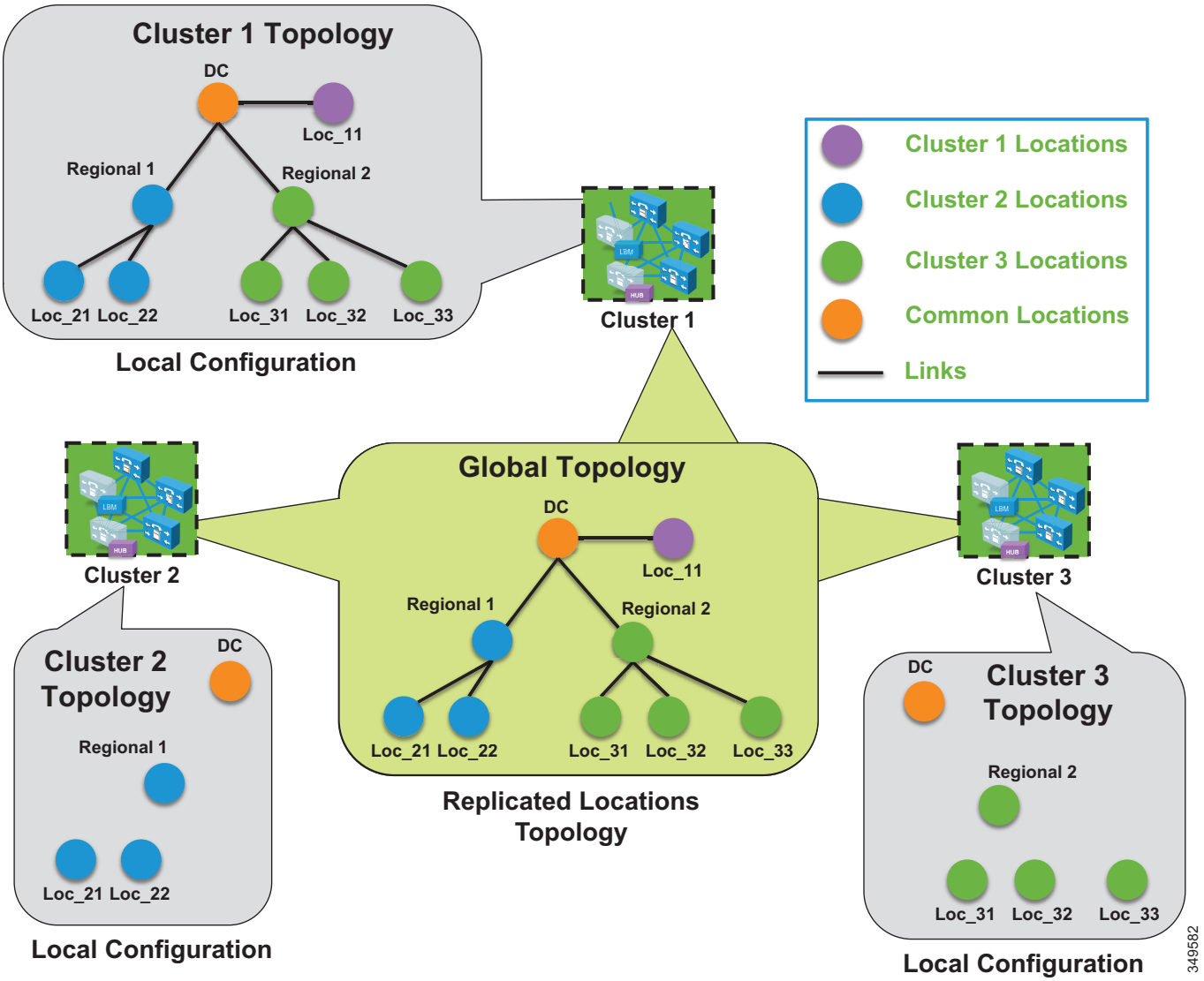
利点

- 単一クラスタから企業 CAC トポロジを管理します。
- クラスタが複数の共通のロケーションを共有する場合のロケーションとリンク設定のオーバーヘッドを軽減します。
- クラスタ間でロケーションおよびリンクの設定の誤りを軽減します。
- 企業の他のクラスタは、ロケーションからデバイスやエンドポイントへの関連付けに必要なロケーションにだけ設定を必要とします。
- グローバル ロケーション トポロジのモニタリングに単一のクラスタを提供します。

C：図 8-19 に、3 つのクラスタを対象としたロケーションおよびリンク管理クラスタを示します。

注　前述のように、任意のクラスタがロケーションおよびリンク管理クラスタとして機能することができます。C：図 8-19 では、クラスタ 1 がロケーションおよびリンク管理クラスタとなっています。

C：図 8-19　ロケーションおよびリンク管理クラスタとしてのクラスタ 1 の例



C：図 8-19 に示されている 3 つのクラスタでは、それぞれリージョン ロケーションとリモート ロケーションだけにデバイスがあります。クラスタ 1 にはロケーションおよびリンクが設定されているグローバル トポロジ全体があり、クラスタ間 LBM の複製は 3 つのすべてのクラスタの間で有効です。この例でロケーションを共有するクラスタはありませんが、クラスタ 1 でロケーションとリンク トポロジ全体が設定されているため、すべてのロケーションが共通ロケーションとなります。クラスタ 2 とクラスタ 3 では、デバイスとエンドポイントを関連付けるために必要なロケーションだけを設定している一方、クラスタ 1 にはグローバル トポロジ全体が設定されていることに注意してください。クラスタ間レプリケーション後に、すべてのクラスタはロケーションとリンクからなるグローバル トポロジを使用できるようになります。

コール アドミッション制御の設計上の考慮事項

この項では、さまざまな IP WAN トポロジに対して、コール アドミッション制御メカニズムを適用する方法について説明します。Unified CM の Enhanced Locations CAC ネットワーク モデリング サポートをクラスタ間の拡張ロケーションと組み合わせることで、あらゆる Unified CM 導入モデルでほとんどのネットワーク トポロジをサポートできます。Enhanced Locations CAC は依然としてネットワークを参照しない静的に定義されたメカニズムであるため、ネットワークの変更がアドミッション制御に影響するたびに、管理者は適宜 Unified CM をプロビジョニングする必要があります。これは、ネットワーク障害が発生し、メディア ストリームがネットワークの異なるパスを取る場合などに RSVP などのネットワーク対応のメカニズムが、その間隔を埋めてネットワークの動的変化をサポートできる場合です。これは、ロード バランシングされた二重またはマルチホーム WAN アップリンク、あるいは不等サイズのプライマリおよびバックアップ WAN アップリンクがある設計の場合がよくあります。

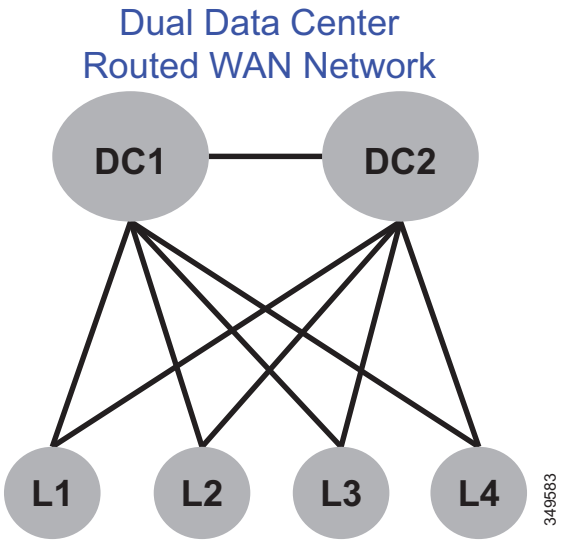
Enhanced Locations CAC の仕組みと、Enhanced Locations CAC の設計および導入の詳細については、最新バージョンの Cisco Collaboration SRND に記載されている「*Bandwidth Management*」の Enhanced Locations Call Admission Control に関する情報を参照してください。

ここでは、いくつかの一般的なトポロジを調べ、それらのトポロジを管理するために Enhanced Locations CAC を設計する方法について説明します。

デュアル データセンター設計

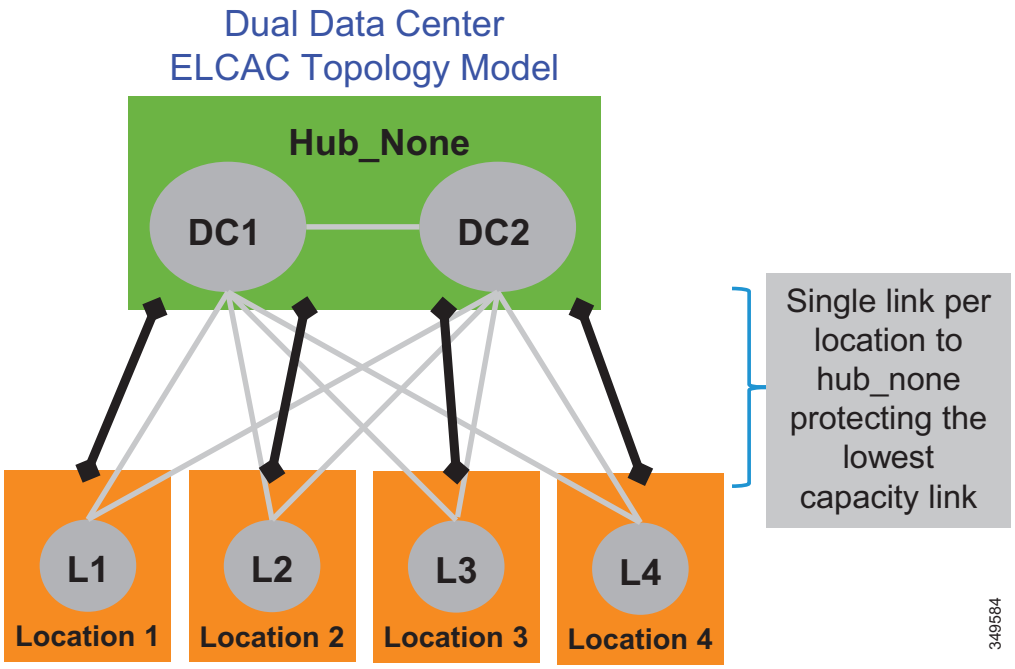
C：図 8-20 に、各リモート サイトに単一の WAN アップリンクがある単純なデュアル データセンター WAN ネットワーク設計を示します。データセンターは、データ トラフィック用に余裕を持ってプロビジョニングされた高速 WAN 接続を介して相互接続します。

C：図 8-20　　デュアル データセンター WAN ネットワーク



通常、リモート サイトからデータセンターへのこれらの WAN アップリンクは、ロードバランシングされているかプライマリ / バックアップ設定にあり、これらのシナリオを処理するスタティック CAC メカニズム用の制限方法があります。Enhanced Locations CAC のこのマルチパス トポロジを設定できますが、重みのメトリックが変更されるまで 1 つのパスだけが有効なパスとして計算されてスタティックのままになります。このタイプのネットワーク トポロジをサポートする、よりよい方法は、2 つのデータセンターを Enhanced Locations CAC の 1 つのデータセンターまたはハブ ロケーションとして設定し、各リモート サイト ロケーションに対して単一リンクを設定することです。C：図 8-21 に、Enhanced Locations CAC のロケーションとリンクのオーバーレイを示します。

C：図 8-21　デュアル データセンターの Enhanced Locations CAC のトポロジのモデル



設計に関する推奨事項

リモート ロケーションへのリモート デュアルまたはより多くのリンクを持つリモートのデュアル データセンターに関する次の設計上の推奨事項は、ロードバランシング WAN 設計、プライマリ / バックアップ WAN 設計の両方に適用されます。

- 1 つのロケーション（Hub_None）は、両方のデータセンターを表します。
- リモート ロケーションと Hub_None 間の単一リンクは、通常の状態または最高帯域幅容量のリンクの障害時にリモート サイトのアップリンクをオーバーサブスクリプションから保護します。
- リモート サイトと Hub_None 間のリンク帯域幅割り当て容量は、単一リンクの適切な Unified Communications メディア用の最低帯域幅容量と同じです。たとえば、各 WAN アップリンクが音声トラフィックによってマークされた EF の 2 Mbps をサポートできる場合、障害状態または等コスト パスのルーティングをサポートするために、リンクの音声帯域幅値は 2 Mbps 以下である必要があります。

MPLS クラウド

Enhanced Locations CAC ネットワークのモデルでマルチ プロトコル ラベル スイッチング（MPLS）の Any-to-Any 接続タイプのクラウドを設計する場合、1 つのロケーションは MPLS クラウドとして動作できます。このロケーションに関連付けられているデバイスはありませんが、このクラウドにアップリンクを持つすべてのロケーションには、クラウドを表すロケーションへのリンクが設定されます。このように、MPLS クラウドは、他のリモート ロケーションに複数の可変サイズの帯域幅 WAN アップリンクを相互接続するための中継ロケーションとして機能します。

設計に関する推奨事項

- MPLS クラウドは、エンドポイントを含まなくてもロケーションを相互接続するハブとして使用されるロケーションとして設定する必要があります。
- MPLS クラウドは、他のリモート ロケーションに複数の可変サイズの帯域幅 WAN アップリンクを相互接続するための中継場所として機能します。
- デュアル MPLS クラウドへの接続を持つリモート サイトは、その接続を単一リンクとして扱い、ネットワーク障害状態時のオーバーサブスクリプションを回避するためにリンクの最低容量までサイジングする必要があります。

ビデオの導入に関するコール アドミッション制御の設計上の推奨事項

アドミッション制御と QoS は相互に補完し、多くの場合は共存します。オーディオとビデオのエンドポイント、音声とビデオのゲートウェイ、音声メッセージ、会議など、最新のシスコ製品サービスは、IP DiffServ コード ポイント（IP DSCP）に基づいてネイティブ QoS パケット マーキングをすべてサポートします。ただし、Jabber for Windows クライアントは、Windows オペレーティング システムが、アプリケーション、IP アドレス、および UDP/TCP ポート範囲を使用するグループ ポリシー オブジェクト（GPO）を使用してオペレーティング システム自体からの DSCP のトラフィックをマーキングする必要があるため、他のクライアントと同じようにネイティブ マーキング機能に厳密に従うことはありません。グループ ポリシー オブジェクトは、トラフィックをマーキングする機能という点で、ネットワーク アクセス リストと非常に類似した機能です。

QoS を使用しないと、許可されたトラフィックが許可されていないトラフィックまたは他のトラフィックの分類よりも上位を求めるネットワーク リソースを使用できるように、ネットワークがメディアの優先順位を付けられないため、QoS はアドミッション制御に必要不可欠です。エンドポイント メディア分類に適用される 5 つの主要な QoS 設定は、Unified CM の QoS 関連の CallManager サービス パラメータならびに SIP プロファイル設定で行います。C：表 8-7 に、主な 5 つの DSCP パラメータとそれぞれのデフォルト値と推奨値、および対応する Per-Hop Behavior（PHB）のデフォルト値と推奨値を記載します。

C：表 8-7　エンドポイント メディア分類の QoS 設定

Cisco CallManager サービス パラメータ クラスタ全体のパラメータ（システム - QoS）（Clusterwide Parameters (System - QoS)）	デフォルト値		推奨値	
	DSCP	PHB	DSCP	PHB
音声コールの DSCP（DSCP for Audio Calls）	46	EF	46	EF
ビデオ コールの DSCP（DSCP for Audio Calls）	34	AF41	34	AF41
ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）	34	AF41	46	EF
TelePresence コールの DSCP（DSCP for TelePresence Calls）	32	CS4	34	AF41
TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）	32	CS4	46	EF

[音声コールの DSCP（DSCP for Audio Calls）] 設定は、オーディオ専用コールを発信するデバイスに使用されます。[ビデオ コールの DSCP（DSCP for Audio Calls）] 設定は、「デスクトップ」に分類されるデバイスのオーディオとビデオのトラフィックに使用されます。**テレプレゼンスコールの DSCP（DSCP for TelePresence Calls）**が、「ルームシステム」に分類されるデバイスのオーディオとビデオのトラフィックに使用されます。分類されたビデオ コールに依存する [ビデオ コールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）] と [TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）] は、ビデオ コールのオーディオ部分だけを区別します。

Enhanced Locations CAC の設計上の考慮事項と推奨事項

次の設計上の推奨事項は、Enhanced Locations CAC を使用するビデオ ソリューションに適用されます。

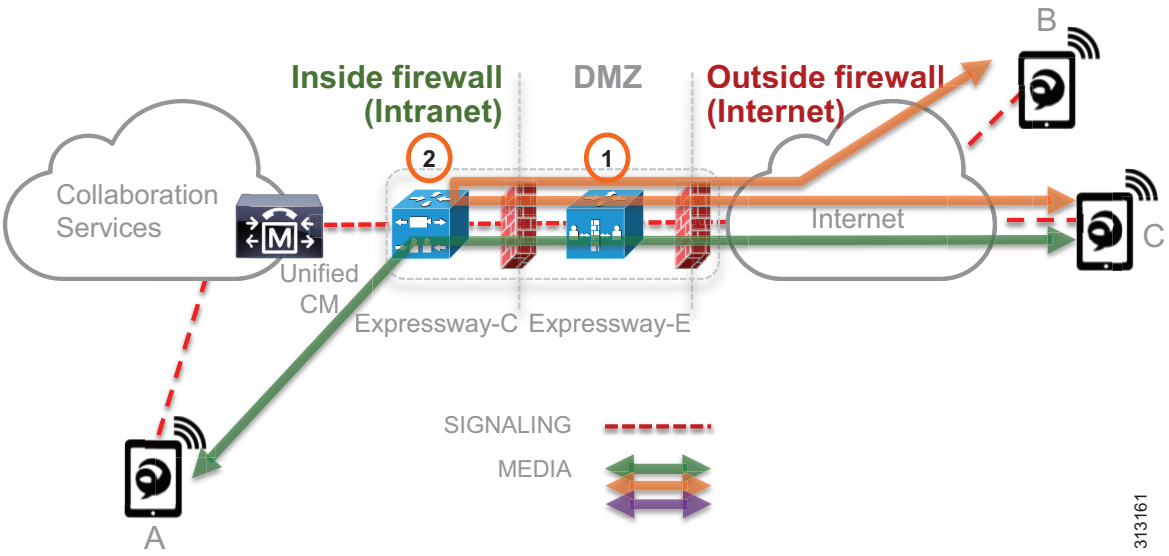
- クラスタ間 SIP トランクはシャドウ ロケーションに関連付けられている必要があります。

Enhanced Locations CAC を使用する Cisco Expressway の導入に関する設計上の推奨事項

Cisco Expressway のモバイルおよびリモート アクセス（MRA）ソリューションでは、この機能をサポートするエンドポイントは、VPN を使用せずに Cisco Expressway 配置を介して Unified CM に登録できます。Cisco Expressway-C サーバと Expressway-E サーバは、それぞれがハイ アベイラビリティの冗長性を備えて導入されます。Expressway-E はファイアウォールからインターネット（外側）とファイアウォールから企業（内側）間の DMZ に導入される一方、Expressway-C は企業内に導入されます。C：図 8-22 に、この配置を示します。また、次のメディア フローを示しています。

- お互いをコールするインターネットベースのエンドポイントでは、C：図 8-22 のエンドポイント B と C の間に示されるように、メディアは Expressway E と Expressway C を経由してルーティングされ、インターネットに戻されます。
- 内部エンドポイントをコールするインターネットベースのエンドポイントでは、C：図 8-22 のエンドポイント A と C の間に示されるように、メディアは Expressway-E と Expressway-C を経由します。

C：図 8-22　　Cisco Expressway モバイルおよびリモート アクセス (MRA) の導入



Cisco Expressway 導入環境での Enhanced Locations CAC では、デバイス モビリティと呼ばれる Unified CM の機能を使用する必要があります。エンドポイントでデバイス モビリティを有効にすると、Unified CM は、デバイスが Cisco Expressway を介して登録された時点、あるいは企業内で登録された時点でそれを認識できるようになります。またデバイス モビリティを使用すると、企業とインターネット間をローミングするときに、Unified CM がアドミッション制御をデバイスに適用できるようになります。エンドポイントが Expressway-C の IP アドレスを使用して Unified CM に登録された場合、デバイス モビリティでは、Unified CM が該当するインター

ネット ロケーションを関連付けることを認識することで、アドミッション制御を適用することもできます。ただし、エンドポイントが他の IP アドレスで登録されている場合、Unified CM は、デバイスに直接設定されている（またはデバイスに直接設定されたデバイス プールから）企業ロケーションを使用します。企業全体にわたってデバイス モビリティを導入しなくても、この機能は有効であることに注意してください。Unified CM のデバイス モビリティ設定は Expressway の IP アドレスでのみ必要となり、この機能を必要とするデバイス（つまり、インターネット経由で登録するデバイス）上だけでこの機能が有効にされます。

帯域幅管理の導入

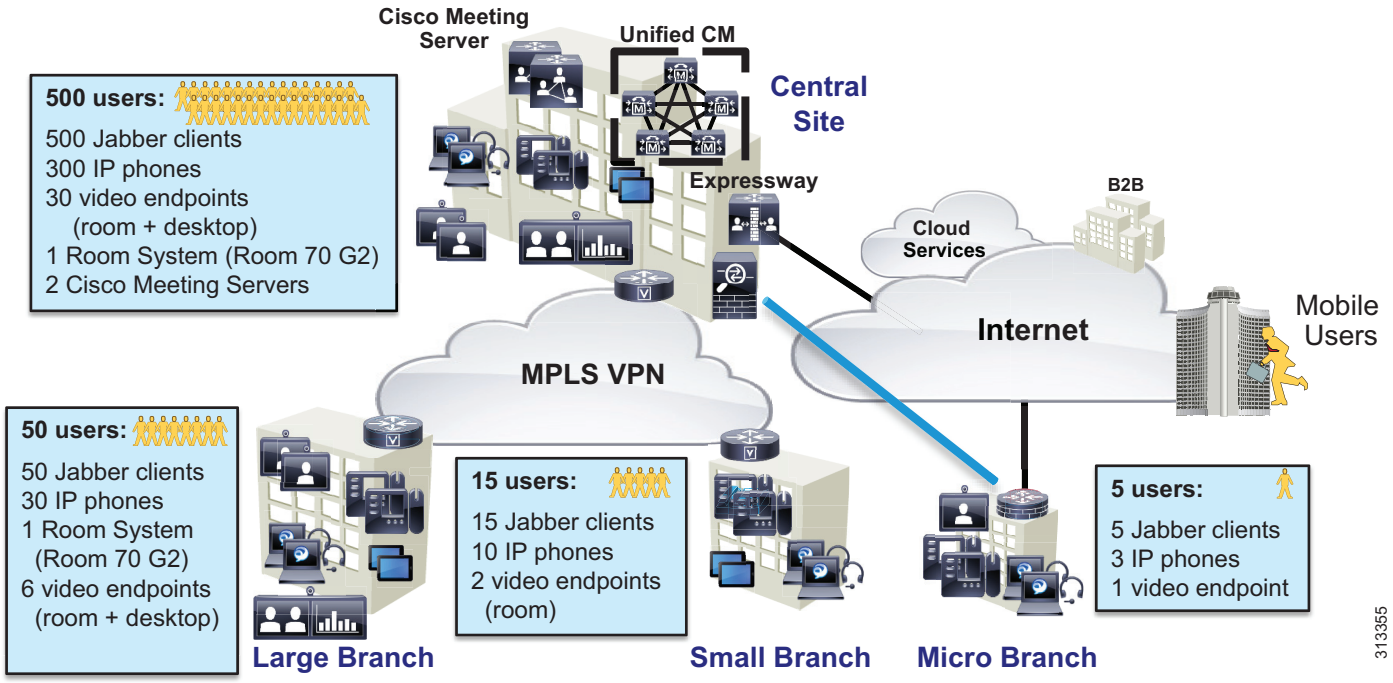
ここでは、PA の帯域幅管理の導入方法を説明します。また、サイトのタイプごとに、本章でこれまでに取り上げたすべての側面（識別と分類、WAN キューリングとスケジューリング、プロビジョニング、リソース管理、帯域幅割り当て）に関するガイドラインを詳しく示します。

展開の概要

ここではプリファード アーキテクチャの例として、広範な地理的エリアにユーザが存在する大企業を取り上げます。この企業には、データ センターが設置された本社と、大規模、小規模、および非常に小規模の支社があります。本社にはおよそ 500 人、各支社にはそれぞれ 50 人、15 人、5 人のユーザがいます。ネットワーク図を簡略化するため、これらのサイトのカテゴリ（本社、大規模支社、小規模支社、営業所）をテンプレートとして使用し、同様のユーザ数とエンドポイントの密度を持つ各サイトに応じた帯域幅の考慮事項を決定します。C：図 8-23 に、サイトのタイプごとのユーザ数とエンドポイントの数が示されています。この例での企業は、ビデオ機能を備えた Jabber を導入し、ユーザが会議でビデオ端末にアクセスできるようにしています。ビデオ会議のリソースは、中央サイト（本部）のデータセンターにあります。IP フォンは、音声のみの通信に使用します。ビデオ エンドポイントは、Jabber クライアント、コラボレーション デスクトップ エンドポイント（DX シリーズ）、ルームベースのエンドポイント（MX シリーズおよび SX シリーズ）です。セントラルサイトと大規模ブランチには、Webex Room 70 G2 も導入されています。

サイトの各タイプに応じた WAN エッジでの帯域幅要件の決定は、IT 部門に任されています。以降の各セクションでは、この要件を示し、QoS を適用し、帯域幅とキューイング要件、アドミッション制御要件を決定するための方法を説明します。

C：図 8-23　Enterprise Collaboration 向けプリファード アーキテクチャ



Enterprise Collaboration 向けプリファード アーキテクチャでの帯域幅管理の導入に伴う主要なタスクは次のとおりです。

- 識別と分類
  - アクセス レイヤ エンドポイントの識別と分類
  - アプリケーション サーバーの QoS
  - WAN エッジの識別と分類
  - WAN エッジでのキューイングとスケジューリング
- プロビジョニングとアドミッション制御
  - 拡張ロケーション CAC
  - モバイルおよびリモート アクセス（MRA）を対象としたデバイス モビリ ティーの導入
  - 帯域幅割り当てのガイドライン

識別と分類

ここでは、企業全体の QoS 要件を確立します。この項では、次の項目について説明します。

- アクセス レイヤ エンドポイントの識別と分類
  - エンドポイント：Jabber
  - エンドポイント：デスクトップおよびルーム システム
- アプリケーション サーバーの QoS
- WAN エッジの識別と分類
- WAN エッジでのキューイングとスケジューリング

導入のこのフェーズでは、大まかに次のステップが必要になります。

1。 Jabber クライアントおよびデスクトップおよびルームシステムエンドポイントの QoS を使用して、統一された CM のエンドポイントを設定します。

2。 信頼されないエンドポイントの識別と分類に適用するアクセス レイヤ ポリシーを導入します。

3。 メディアおよび SIP シグナリングを対象としたアプリケーション サーバ QoS を設定します。

4。 コラボレーション メディアと SIP シグナリングを対象とした WAN エッジ入力時のマーキング ポリシーを導入します。

5。 コラボレーション メディアと SIP シグナリングを対象とした WAN エッジ出力キューイング ポリシーを導入します。

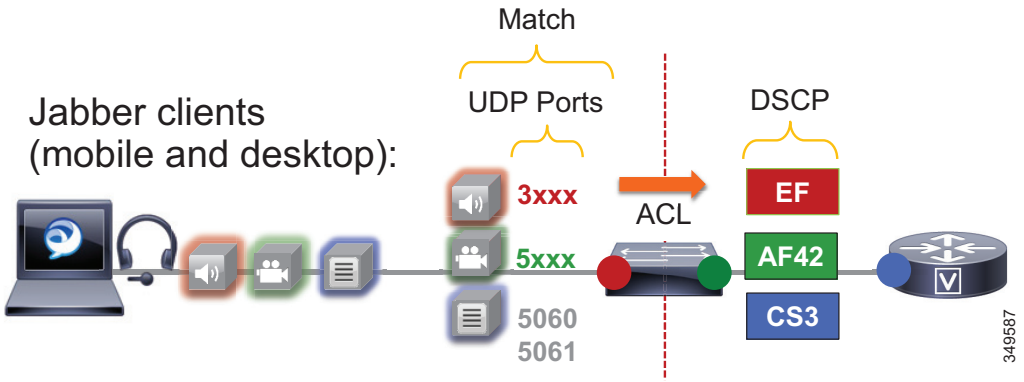
アクセス レイヤ エンドポイントの識別と分類

ここでは、ネットワークおよび Unified CM で、エンドポイントの QoS とメディア ポート範囲を設定します。

エンドポイント：Jabber

Jabber エンドポイントは信頼されていないエンドポイントであり、通常はデータ VLAN 内に置かれます。アクセス レイヤ スイッチでシグナリングおよびメディアの再マーキングを適用するには、特定の UDP ポート範囲を使用します。この場合、Unified CM で SIP プロファイルを設定し、すべての Jabber クライアントが [メディアとシグナリングのポート範囲：分割（Separate Media and Signaling Port Range）] の値 3000 ～ 3999（オーディオの場合）と 5000 ～ 5999（ビデオの場合）を使用するよう明示的に指定します。SIP シグナリングには SIP シグナリング ポート 5060 を使用し、セキュアな SIP シグナリングには SIP シグナリング ポート 5061 を使用します。SIP シグナリング ポートは、Unified CM の [SIP セキュリティ プロファイル（SIP Security Profile）] で設定します。C：図 8-24 に、この設定を示します。

C：図 8-24　　Jabber エンドポイントの QoS



管理者は、次の DSCP 値に UDP ポートを再マーキングするデータ VLAN にアクセス スイッチの ACL を作成します。

- オーディオ：UDP ポート 3000 ～ 3999 を EF として再マーキング
- ビデオ：UDP ポート 5000 ～ 5999 を AF42 として再マーキング
- シグナリング：TCP ポート 5060 ～ 5061 を CS3 として再マーキング

Jabber の分類概要：

- すべての Jabber コールのオーディオ ストリーム（音声専用とビデオ）は EF としてマーキングされます。
- Jabber ビデオ コールのビデオ ストリームは AF42 としてマーキングされます。

Jabber エンドポイントについては、Jabber SIP プロファイルでデフォルトの QoS 値を変更することもお勧めします。これは、何らかの理由でワイヤレス ルータまたは他のネットワーク コンポーネントにより QoS が「信頼される」場合、適切な「信頼される」値が再マーキング値と同じになるようにするためです。したがって、SIP プロファイル内の QoS パラメータを C：表 8-8 に記載するように設定し、UDP ポート範囲を C：表 8-9 に記載するように設定してください。

C：表 8-8　SIP プロファイルでの Jabber エンドポイントの QoS パラメータの設定

QoS サービス パラメータ名（SIP プロファイル）	デフォルト値	変更値
音声コールの DSCP（DSCP for Audio Calls）	EF	変更なし
ビデオ コールの DSCP（DSCP for Audio Calls）	AF41	AF42
ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）	AF41	EF
TelePresence コールの DSCP（DSCP for TelePresence Calls）	CS4	AF41
TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）	CS4	EF

C：表 8-9　Jabber エンドポイントの UDP ポートの設定

[メディアポートの範囲（Media Port Range）] > [オーディオとビデオのポート範囲の分割（Separate Port Range for Audio and Video）]	値
オーディオ ポートの開始値	3000
オーディオ ポートの終了値	3999
ビデオ ポートの開始値	5000
ビデオ ポートの終了値	5999

C：表 8-8 の設定により、何らかの理由で Jabber クライアントのオーディオとビデオが信頼され、アクセス スイッチで UDP ポート範囲によって再マーキングされない場合、Jabber クライアントのオーディオは EF に設定され、ビデオは AF42 に設定されます。これは単に、Jabber エンドポイント間で設定の一貫性を確保するためです。

注　Jabber ビデオに AF42 を使用しない場合は、QoS のデフォルト システム パラメータを使用して、SIP プロファイルの QoS パラメータを [システムデフォルトの使用（Use System Default）] に設定できます。

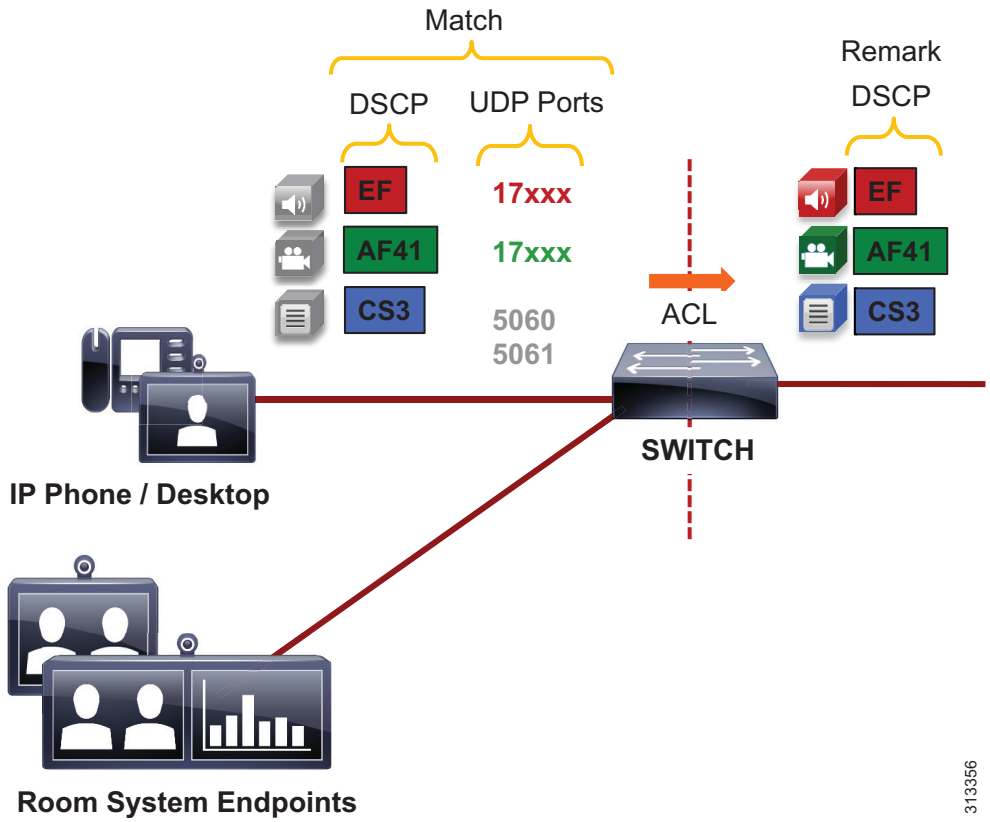
モバイル デバイス上の Jabber については、それらのデバイス用に新しい SIP プロファイルを作成する際に、**モバイル デバイス用の標準 SIP プロファイル**をコピーすることをお勧めします。モバイル デバイス用のデフォルトの標準 SIP プロファイルには、Android デバイスや Apple iOS デバイスで Jabber 登録を維持する際に推奨されるタイマー値が含まれているためです。これらのタイマーは、デュアルモードおよびタブレット Jabber クライアント デバイスに割り当てられているすべての SIP プロファイルに必要です。

注 Mac/iPad/iPhone/Android 向けの Jabber は、いずれも OS によってネイティブに DSCP でマーキングされます。ただし、Windows 向けの Jabber には、OS による DSCP 再マーキングのためにグループ ポリシー オブジェクトが必要になります。グループ ポリシー オブジェクトを使わなければ、Windows 向けの Jabber はすべてのトラフィックの DSCP を 0 としてマーキングします。このことから、Jabber には特定のポート範囲が使用され、DSCP に基づくマッチングは行われません。

エンドポイント：デスクトップおよびルーム システム

IP フォン、デスクトップ、および ルーム システム エンドポイントも、トラフィックを再マーキングする際にアクセス レイヤ スイッチ ACL に依存します。アクセス レイヤ スイッチでシグナリングおよびメディアを再マーキングするには、特定の UDP ポート範囲と DSCP を使用します。統一された CM で SIP プロファイルを設定し、すべての IP フォン、デスクトップ、および ルームシステムエンドポイントがオーディオとビデオに対して共通のメディアとシグナリングのポート範囲の値 17000 ～ 17999 を使用するように明示的に指定します。SIP シグナリングには SIP シグナリング ポート 5060 を使用し、セキュアな SIP シグナリングには SIP シグナリング ポート 5061 を使用します。SIP シグナリング ポートは、Unified CM の [SIP セキュリティ プロファイル（SIP Security Profile）] で設定します。C：図 8-25 でこれについて説明します。

C：図 8-25　デスクトップおよびルーム システム エンドポイント QoS



管理者は、アクセス スイッチ ポートで UDP ポートが次の DSCP 値に再マーキングされるようにするための ACL を作成します。

- オーディオ：UDP ポート 17000 ～ 17999 では DSCP が EF となっているオーディオを EF として再マーキング
- ビデオ：UDP ポート 17000 ～ 17999 では DSCP が AF41 となっているビデオを AF41 として再マーキング
- シグナリング：TCP ポート 5060 ～ 5061 を CS3 として再マーキング

デスクトップおよびルーム システム エンドポイントの分類の要約：

- すべてのデスクトップおよび ルーム システム エンドポイント コールのオーディオ ストリーム（音声専用とビデオ）は EF としてマーキングされます。
- デスクトップおよび ルーム システム エンドポイント ビデオ コールのビデオ ストリームは AF41 としてマーキングされます。

デスクトップおよび ルーム システム エンドポイントについては、SIP プロファイルでデフォルトの QoS 値を変更して C：表 8-10 に記載するように設定し、UDP ポート範囲を C：表 8-11 に記載するように設定してください。

C：表 8-10　SIP プロファイルでのデスクトップおよびルーム システムのエンドポイントの QoS パラメータ

QoS サービス パラメータ名（SIP プロファイル）	デフォルト値	変更値
音声コールの DSCP（DSCP for Audio Calls）	EF	変更なし
ビデオ コールの DSCP（DSCP for Audio Calls）	AF41	変更なし
ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）	AF41	EF
TelePresence コールの DSCP（DSCP for TelePresence Calls）	CS4	AF41
TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）	CS4	EF

C：表 8-11　デスクトップおよびルーム システムのエンドポイントの UDP ポートの設定

[メディアポートの範囲（Media Port Range）] > [オーディオおよびビデオ用コモンポートの範囲（Common Port Range for Audio and Video）]	値
メディア ポートの開始値	17000
メディア ポートの終了値	17999

エンドポイント スイッチ ポート用のスイッチ ACL ベース QoS ポリシーの例

デスクトップおよびルーム システムのエンドポイント：

- UDP ポート範囲 17xxx と DSCP EF に一致 –> DSCP EF として再マーキング
- UDP ポート範囲 17xxx と DSCP AF41 に一致 –> DSCP AF41 として再マーキング
- TCP ポート 5060 または 5061 に一致 –> DSCP CS3 として再マーキング

Jabber クライアント

- UDP ポート範囲 3xxx に一致 –> DSCP EF として再マーキング
- UDP ポート範囲 5xxx に一致 –> DSCP AF42 として再マーキング
- TCP ポート 5060 または 5061 に一致 –> DSCP CS3 として再マーキング

汎用マッチング

- 残りのトラフィックをマッチングし、デフォルトのクラス マップを使用して DSCP を 0（ベスト エフォート（BE））として設定

注 以下に、Cisco Common Classification Policy Language（C3PL）に基づくアクセス コントロール リストの例を記載します。

```
! This section configures the ACLs to match the UDP port ranges and DSCP.
ip access-list extended QOS_VOICE
    permit udp any range 17000 17999 any dscp ef
    permit udp any range 3000 3999 any
ip access-list extended QOS_PRIORITIZED_VIDEO
    permit udp any range 17000 17999 any dscp af41
ip access-list extended QOS_JABBER_VIDEO
    permit udp any range 5000 5999 any
ip access-list extended QOS_SIGNALING
    permit tcp any any range 5060 5061
    permit tcp any range 5060 5061 any

! This section configures the classes that match on the ACLs above.
class-map match-any VOICE
   match access-group name QOS_VOICE
class-map match-any PRIORITIZED_VIDEO
   match access-group name QOS_PRIORITIZED_VIDEO
class-map match-any JABBER_VIDEO
   match access-group name QOS_JABBER_VIDEO
class-map match-any SIGNALING
   match access-group name QOS_SIGNALING

! This section configures the policy-map matching the classes configured above and sets
DSCP for voice, video, and SIP signaling on ingress. Note that the class-default sets
everything that does not match the above to a DSCP of 0 (BE).
policy-map INGRESS_MARKING
  class VOICE
    set dscp ef
  class PRIORITIZED_VIDEO
    set dscp af41
  class JABBER_VIDEO
    set dscp af42
  class SIGNALING
    set dscp cs3
  class class-default
    set dscp 0

! This section applies the policy-map to the interface.
Switch (config-if)# service-policy input INGRESS-MARKING
```

前にも説明したように、エンドポイントが送受信するデータとシグナリングは他にもあります（ICMP、DHCP、TFTP、BFCP、LDAP、XMPP、FECC、CTI など）。このようなトラフィックの QoS 値は、トラフィックのタイプに応じた企業のベスト プラクティスに従う必要があります。この手順を行わないと、メディアと SIP シグナリング以外のすべてのトラフィックの DSCP は、この設定でのクラスのデフォルトによって BE（DSCP 0）に設定されることになり

ます。DSCP に基づくマッチングでマーキングしたトラフィックを通過させてから、DSCP を同じ値に再マーキングするか、エンドポイントが通信に使用するプロトコルごとに TCP および UDP ポートを使用することを推奨します。

それには、以下の例に示されているように、AF21（トランザクション データ）である DSCP に対するマッチングを行うようにクラス マップを作成し、そのデータを AF21 に設定するようにポリシーを設定して、実質的に DSCP を同じ値で再マーキングします。これは、DSCP に対するマッチングを行って、同じ DSCP に再マーキングする一例にすぎません。

```
class-map match-any TRANSACTIONAL-DATA
  match dscp af21

policy-map INGRESS_MARKING
....
class TRANSACTIONAL-DATA
  set dscp af21
```

TCP ポート範囲と UDP ポート範囲を使用することもできます。エンドポイントと Unified CM 間の通信に使用する TCP ポートと UDP ポートについて詳しくは、次の URL でアクセスできる最新バージョンの『*System Configuration Guide for Cisco Unified Communications Manager*』に記載されている「*Cisco Unified Communications Manager TCP and UDP Port Usage*」を参照してください。

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

また、他のエンドポイント トラフィックに使用されるさまざまなプロトコルとポートを確認するには、エンドポイントの管理ガイドまたは Jabber の計画ガイドを参照してください。これらのドキュメントの例としては、以下が挙げられます。

- 『*Cisco DX Series Administration Guide*』（次の URL でアクセス）

  https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html

- 『*Planning Guide for Cisco Jabber*』（次の URL でアクセス）

  https://www.cisco.com/c/en/us/support/unified-communications/jabber-android/products-installation-guides-list.html

アプリケーション サーバーの QoS

ソリューション全体にわたり、メディアを発信および終端するアプリケーションと MCU のすべてに、QoS を設定します。ここでは、PA に含まれるすべてのアプリケーション サーバでのデフォルト以外の設定を取り上げます。また、同じく重要な点として、アプリケーション サーバが接続するスイッチ ポートが、サーバによって設定された QoS を信頼するようにしてください。一部のスイッチ（Cisco Catalyst 3850 シリーズなど）は、デフォルトで QoS を信頼するため、スイッチの設定を調べて、スイッチ ポートがデフォルトで信頼されるかどうかを確認し、信頼されない場合は、QoS 信頼を有効にしてください。

各種アプリケーション サーバでの QoS 設定：

- Cisco Unified CM（エンドポイト）

  [システム（System）] > [サービス パラメータ（Service Parameters）] > [パブリッシャの選択（Select Publisher）] > [Cisco CallManager サービスの選択（Select Cisco CallManager Service）] > [クラスタ全体のパラメータ（システム - QoS）（Clusterwide Parameters (System - QOS)）] に移動し、QoS のデフォルト値を変更して、C：表 8-12 に記載されている値に設定します。

C：表 8-12　Unified CM エンドポイントの QoS パラメータの設定

QoS サービス パラメータ名（SIP プロファイル）	デフォルト値	変更値
音声コールの DSCP（DSCP for Audio Calls）	EF	変更なし
ビデオ コールの DSCP（DSCP for Audio Calls）	AF41	変更なし
ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）	AF41	EF
TelePresence コールの DSCP（DSCP for TelePresence Calls）	CS4	AF41
TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）	CS4	EF

- Cisco Unity Connection

  [システム設定（System settings）] > [詳細設定（Advanced）] > [Telephony]

  - デフォルトでは、オーディオは 46 / EF、ビデオは 46 / EF、シグナリングは 24 / CS3 に設定されています。
  - ビデオを 34 / AF41 に変更します。
- Cisco Meeting Server
  - Cisco Meeting Server の DSCP 設定は、コマンド ライン インターフェイス（CLI）を使用して行います。会議（C：3-1 ページ）の章で説明しているように、DSCP の設定は、Cisco Meeting Server を設定した後に行ってください。すべての値はデフォルトで DSCP 0 に設定されるため、すべての DSCP 値を設定する必要があります。*これらの変更を適用するには、サーバの再起動が必要になります。*
  - コマンド ラインの値：

```
dscp 4 signaling 24
dscp 4 voice 46
dscp 4 multimedia 34
dscp 4 oa&m 24
```

- Cisco Expressway

  ビデオの Expressway DSCP 値は、値 AF42（DSCP 36）を使用して状況対応型ビデオとして設定されます。ソリューションで状況対応型ビデオを使用していない場合（したがって AF42 を使用していない場合）は、AF41 を代わりに使用することもできます。その他すべての値（オーディオ、シグナリング、XMPP）は、デフォルト値に設定されます。

  [システム（System）] > [QoS（Quality of Service）]

  - DSCP シグナリングの値：24（デフォルト）
  - DSCP オーディオの値：46（デフォルト）
  - DSCP ビデオの値：36 または 34（デフォルト）
  - DSCP XMPP の値：24（デフォルト）

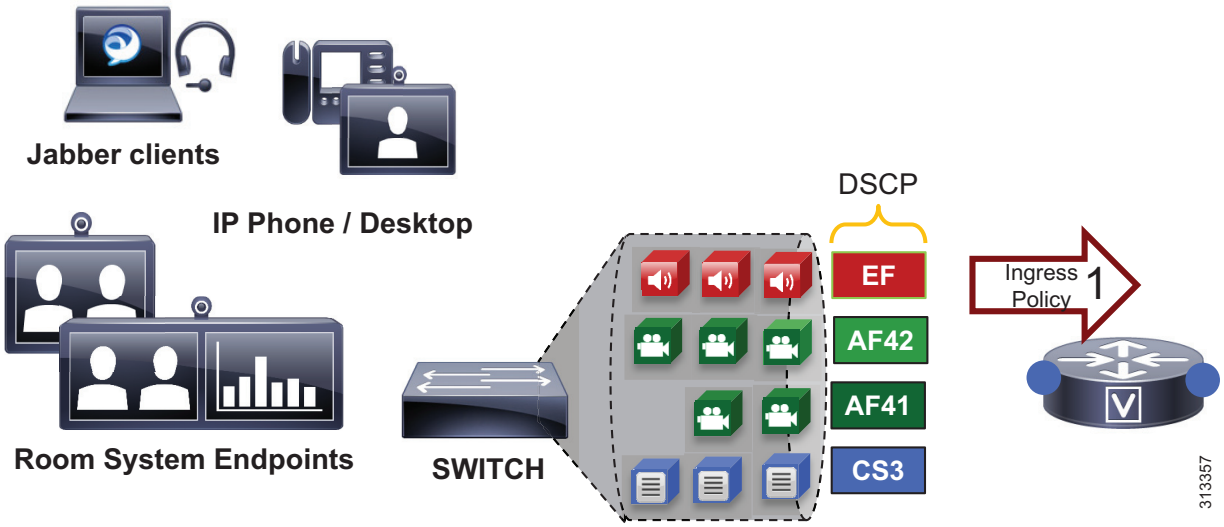
WAN エッジの識別と分類

WAN エッジでの企業からサービス プロバイダーへの出力時には、コラボレーション トラフィックにはアクセス レイヤ スイッチですでに再マーキングが適用されていることから、パケットが特定の DSCP 値で到達することが前提とされます。入力時には、アクセス スイッチからのいずれかのトラフィックが LAN 経由で信頼された場合のフェールセーフとして、アクセス レイヤで再マーキングできなかった WAN エッジのすべてのトラフィックを再マーキングするこ

とが重要です。QoS は LAN で重要ですが、WAN では最も重要です。ルータは入力トラフィックが信頼されていると見なすため、ビジネス要件およびユーザ エクスペリエンスに応じた適切な QoS ポリシーを設定することが重要です。WAN エッジの再マーキングは、ルータへの入力インターフェイスで常に実行されます。キューイングおよびスケジューリングは出力インターフェイスで実行されます。次に、WAN 入力 QoS ポリシーと出力キューイング ポリシーの例を示します。C：図 8-26 から C：図 8-31 に、設定および再マーキング プロセスを示します。

C：図 8-26 では、エンドポイントからのパケットが識別され、信頼されているポートまたは ACL によって適切な DSCP マーキングで分類されます。スイッチド アクセス ネットワークには一般に、適切な QoS ポリシーを設定できないエリアや、コラボレーション トラフィックをベスト エフォート DSCP（BE）として再マーキングできないエリアがあります。そのため、アクセス レイヤで見逃されたトラフィックが WAN に向かう前に、キャッチオール ポリシーで対処するには、WAN 入力ポリシーが絶好の場所となります。

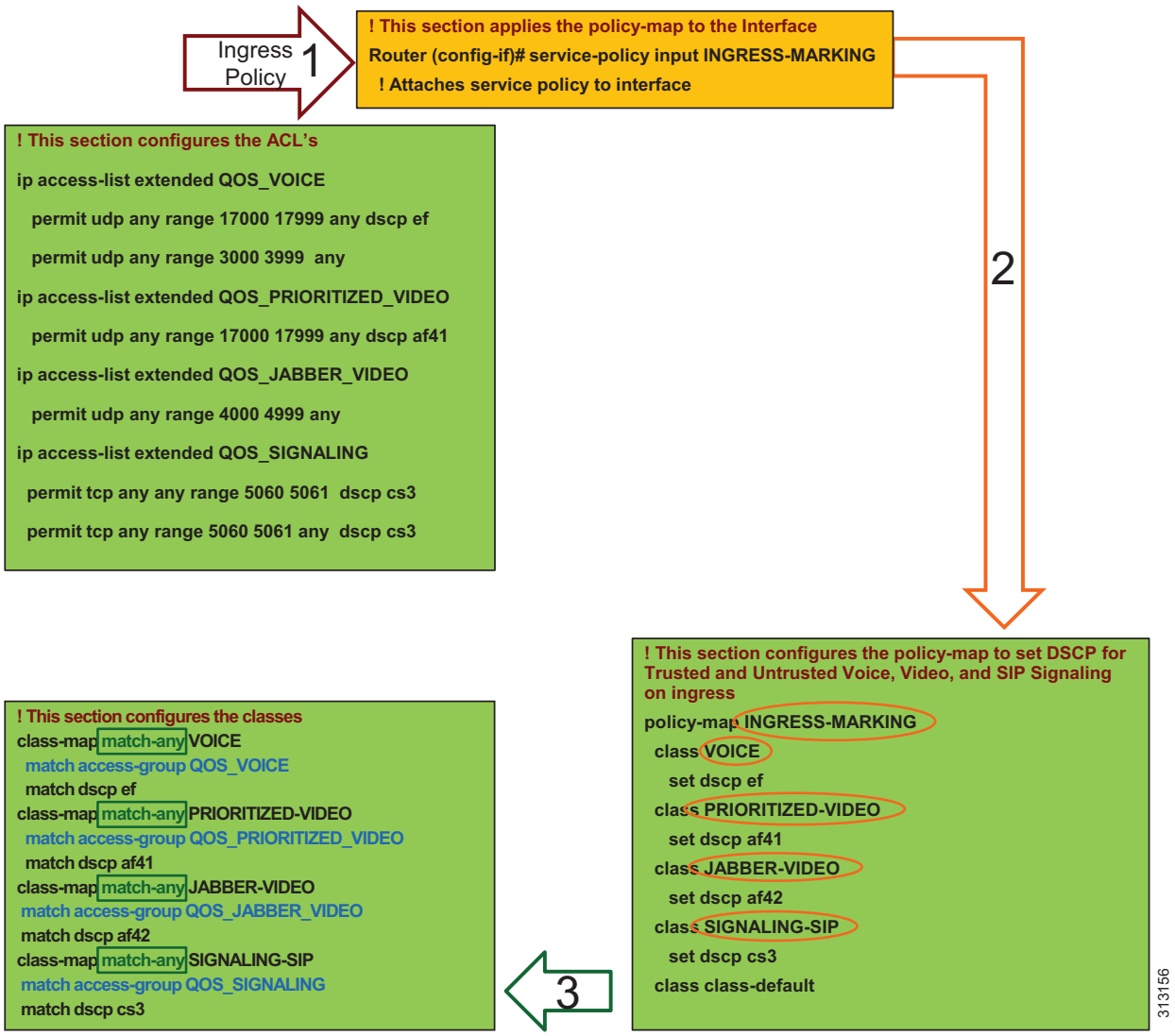
C：図 8-26　ルータ入力 QoS ポリシー プロセスの例：ステップ 1



C：図 8-26 から C：図 8-31 に、ポリシー一致基準および DSCP 再マーキングを示します。これらの図では、次のステップが説明されています。

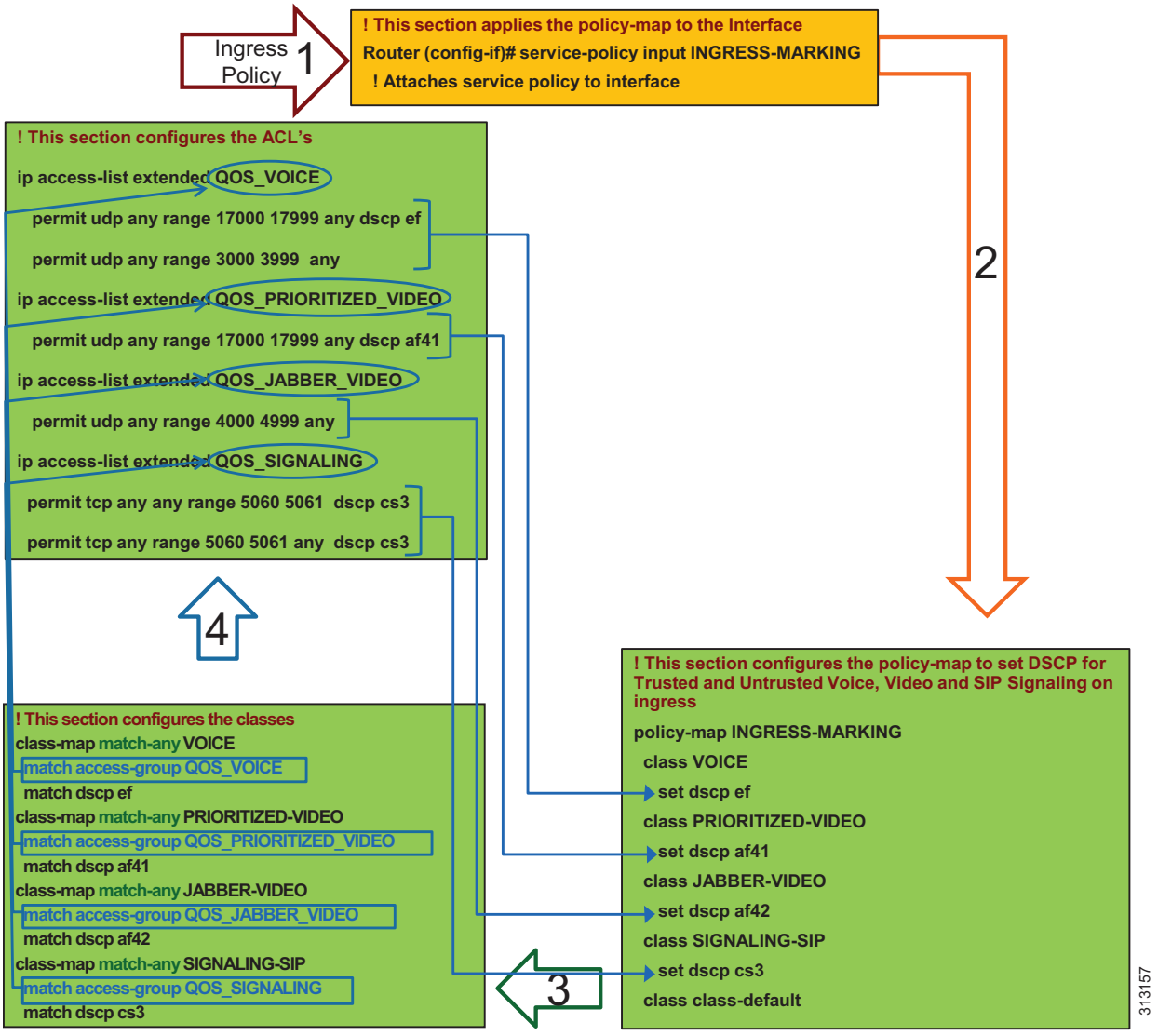
1. ステップ 1 では、入力サービス ポリシーが設定されたルータ入力インターフェイスにパケットが到着します。
2. ステップ 2 では、4 つのトラフィック クラスが設定されたポリシー マップにより、適切な DSCP（音声 = EF、優先順位付けされたビデオ = AF41、Jabber ビデオ = AF42、シグナリング = CS3）が設定されます。
3. ステップ 3 では、これらのクラスのそれぞれで、match-any 基準が設定された同じ名前のクラス マップをマッチングします。この match-any 基準は、プロセスがトップダウン方式で始まり、最初に一致した基準がポリシー マップ ステートメントの各クラスに応じて実行されることを意味します。

C：図 8-27 ルータ入力 QoS ポリシー プロセスの例：ステップ 1 ～ 3



4。 ステップ 4 では、クラス マップ ステートメントの最初の行が解析されます。この行は、識別と分類のセクションで Unified CM に設定された UDP ポートを（場合によっては、DSCP 値も）マッチングする ACL です。（プロトコル、ポート範囲、DSCP が）ACL 基準に一致すると、そのトラフィックは、対応するポリシー マップ ステートメントでの設定に従ってマーキングされます。

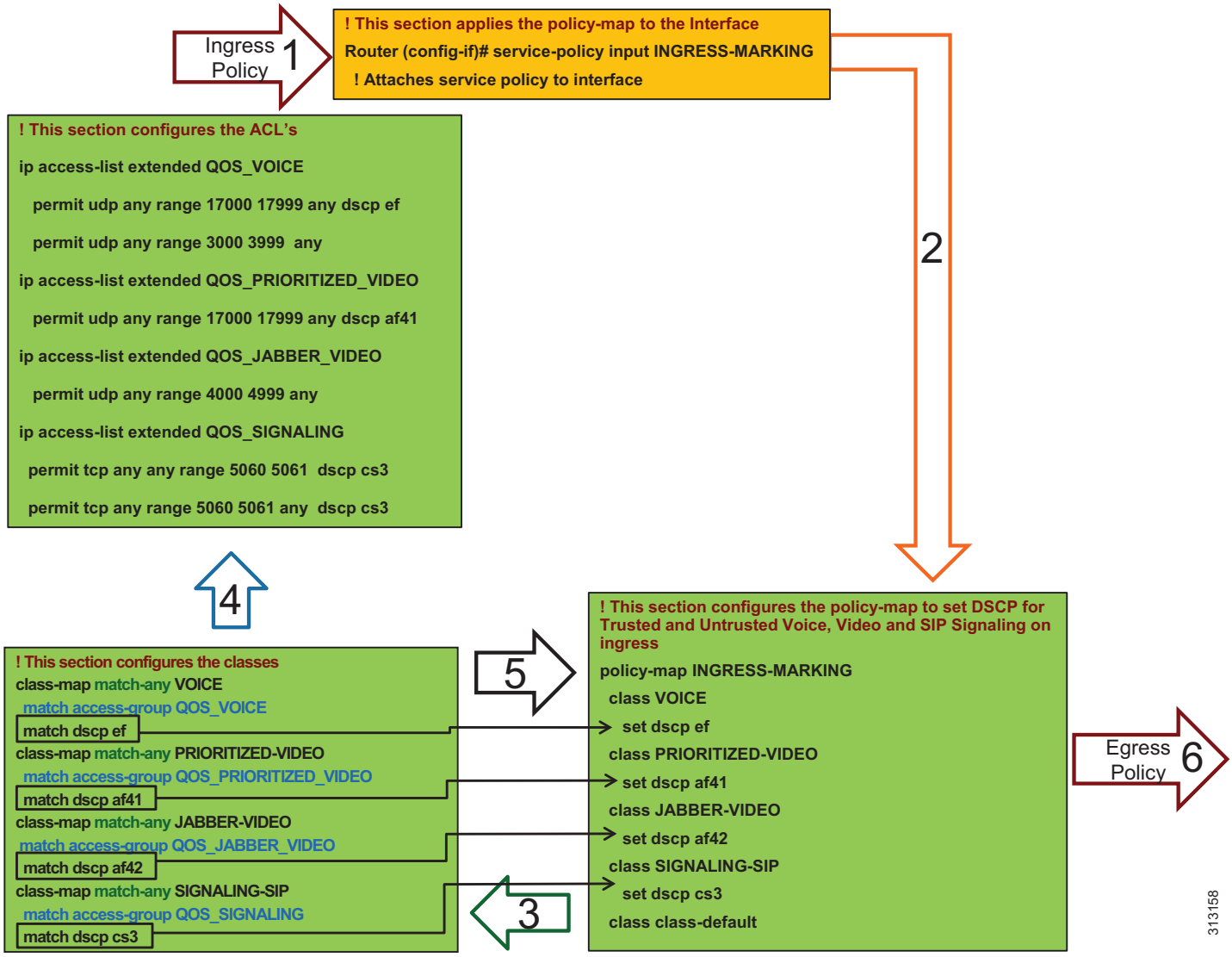
C：図 8-28　ルータ入力 QoS ポリシー プロセスの例：ステップ 4



5。 ステップ 5 では、最初のステートメントに一致しなかったトラフィックにクラス マップの次のマッチング ステートメント **match dscp** が適用されます。トラフィックが DSCP にだけ一致する場合、DSCP は再び、マッチングされた、ポリシー マップ ステートメントに設定

されている同じ値に設定されます。この場合、ルータは単純に DSCP に一致し、DSCP を同じ値にリセットします。これはサーバおよびアプリケーションから WAN ルータに入ってくる信頼された DSCP の catch-all 設定です。

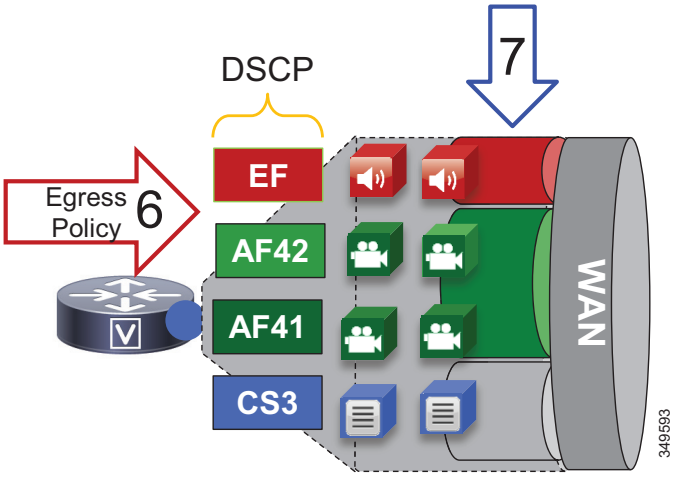
C：図 8-29　ルータ入力 QoS ポリシー プロセス例：ステップ 5



注　これは、Cisco Common Classification Policy Language（C3PL）に基づいた QoS 入力マーキング ポリシー例です。使用している特定のルータの設定ガイドを参照して、更新された C3PL コマンドがないかどうかを確認し、C3PL をサポートする Cisco ルータで同様のポリシーを設定する方法を調べてください。

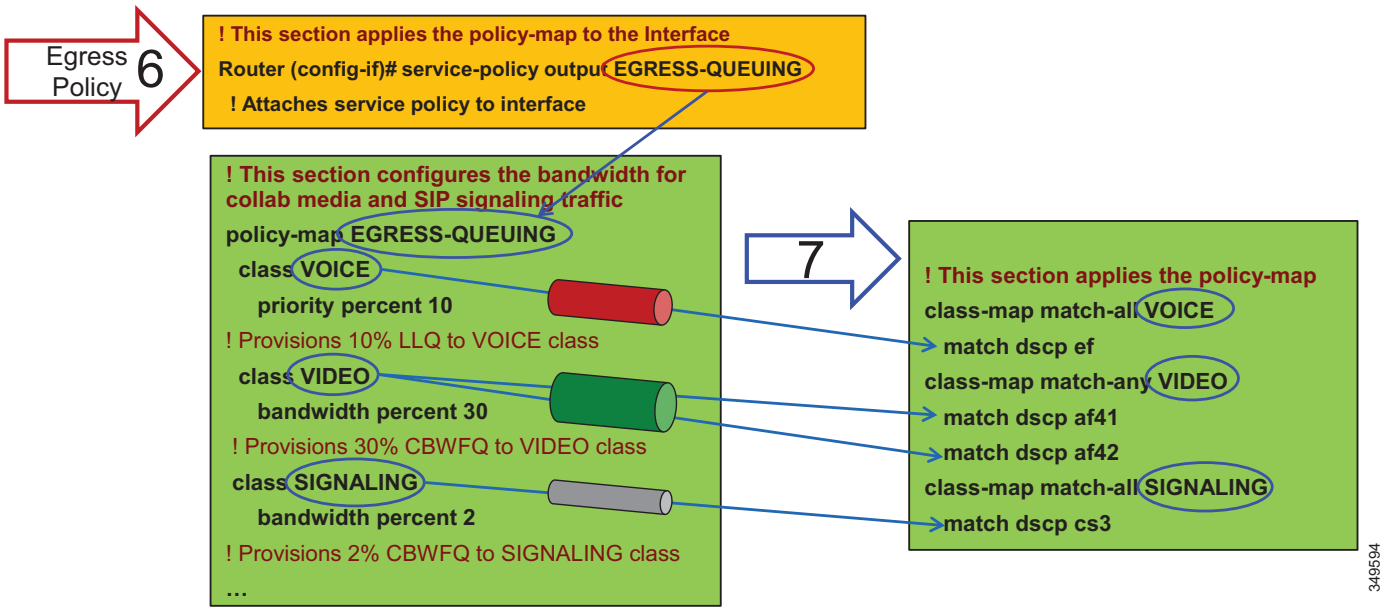
6。 ステップ 6 では、トラフィックがアウトバウンド インターフェイスに到達し、そこで 3 つのキュー（VOICE という名前のプライオリティ キュー、VIDEO という名前の CBWFQ、SIGNALING という名前の CBWFQ）が作成されている出力サービス ポリシーにより、キューに入れられてスケジュールされます。C：図 8-30 から C：図 8-31 に、この仕組みが示されています。ここでは、この出力キューイング ポリシーが、アクセス スイッチや WAN ルータ入力インターフェイスへの入力で発生するネットワーク マーキングとして DSCP のみに基づいている点が強調されています。これは一致基準とキューを説明する単なる例に過ぎないため、WRED 機能は含まれていません。WRED の詳細については、「WAN エッジでのキューイングとスケジューリング」を参照してください。

C：図 8-30　ルータ出力キューイング ポリシー プロセスの例：ステップ 6



7。 ステップ 7 では、トラフィックがクラス マップのマッチング ステートメントと照合されます。EF としてマーキングされたトラフィックはすべて VOICE PQ に送られ、AF41 および AF42 としてマーキングされたトラフィックは VIDEO CBWFQ に、CS3 としてマーキングされたトラフィックは SIGNALING CBWFQ に送られます。

C：図 8-31 ルータ出力キューイング ポリシー プロセス例：ステップ 7



注 これは、Cisco Common Classification Policy Language（C3PL）に基づいた出力キューイング ポリシー例です。使用している特定のルータの設定ガイドを参照して、更新された C3PL コマンドがないかどうかを確認し、C3PL をサポートする Cisco ルータで同様のポリシーを設定する方法を調べてください。

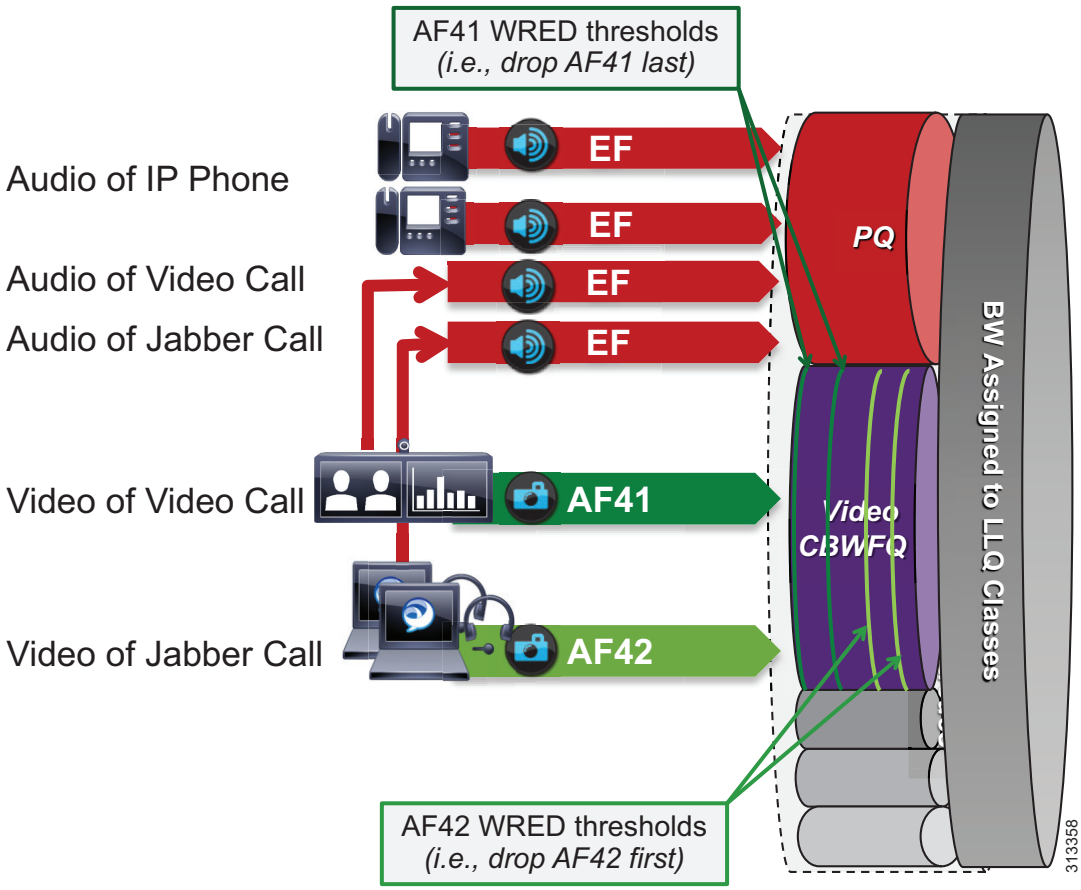
出力キューの設定例

```
! This section applies the policy-map classes to match media and signaling QoS.
class-map match-any VIDEO
 match dscp af41
 match dscp af42
class-map match-any VOICE
 match dscp ef
class-map match-any SIGNALING
 match dscp cs3

! This section configures the bandwidth for Collaboration media and SIP signaling traffic.
policy-map EGRESS-QUEUING
 class VOICE
  priority percent 10
 class VIDEO
  bandwidth percent 30
  fair-queue
 class SIGNALING
  bandwidth percent 2
...

! This section applies the policy-map to the interface.
Router (config-if)# service-policy output EGRESS-QUEUING
! Attaches service policy to interface
```

WAN エッジでのキューイングとスケジューリング

ここでは、インターフェイス キューイングについて説明します。C：図 8-32 に、CBWFQ で使用される音声 PQ、ビデオ CBWFQ、および WRED のしきい値を示します。

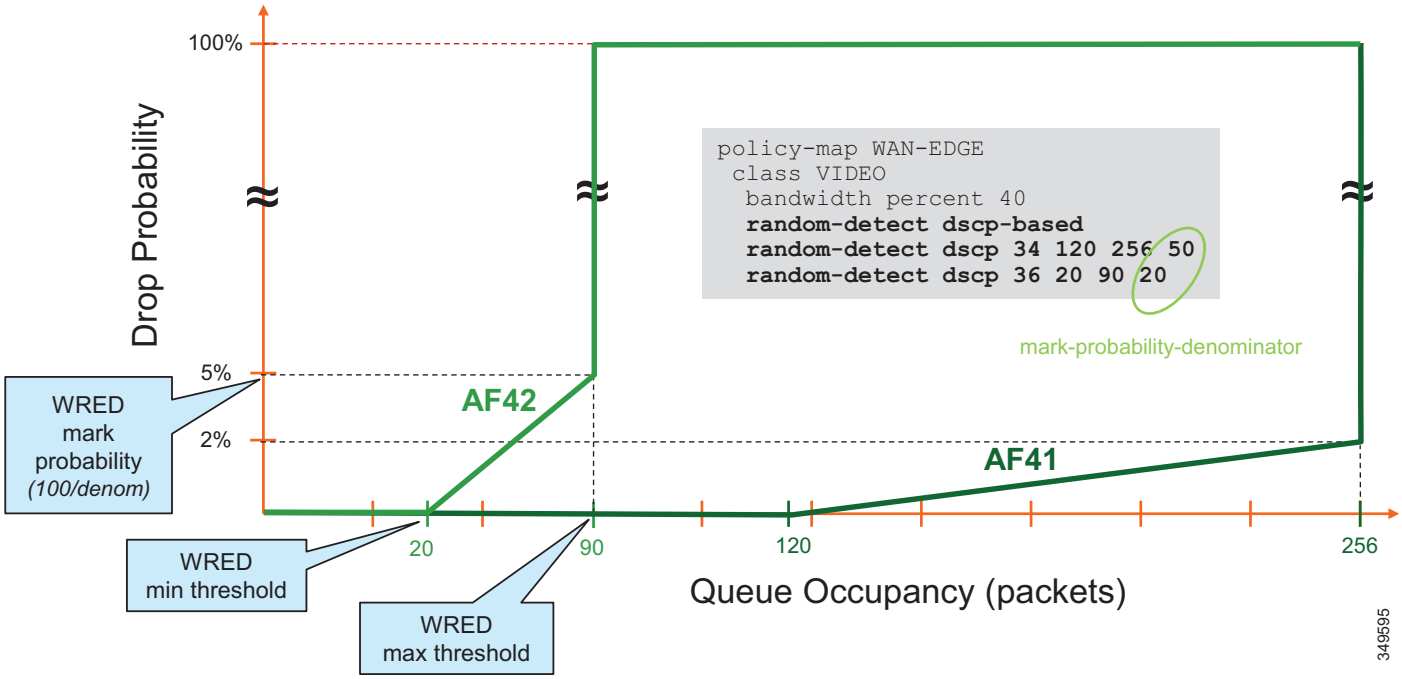
C：図 8-32　　キューイングとスケジューリングのコラボレーション メディア



- EF とマーキングされたすべてのエンドポイントからのオーディオはすべて、PQ にマッピングされます。
- ビデオ コールおよび Jabber は同じ CBWFQ を共有します。
  - エンドポイントからのビデオ コールのオーディオ ストリームには EF
  - エンドポイントからのビデオ コールのビデオ ストリームには AF41
  - Jabber クライアントからのすべてのコールのオーディオ ストリームには EF
  - Jabber クライアントからビデオ コールのビデオ ストリームには AF42
- WRED はビデオ キューで設定されます。
  - AF42 の最小しきい値と最大しきい値の範囲：キュー制限の約 10% ～ 30%
  - AF41 の最小しきい値と最大しきい値の範囲：キュー制限の約 45% ～ 100%

重み付けランダム早期検出（WRED）の最小しきい値と最大しきい値は、ビデオ CBWFQ でも設定されます。WRED のしきい値の設定方法の説明として、インターフェイスはキューの深さが 256 パケットで設定されているとします。次に、上述のガイドラインに従って、AF42 および AF41 の WRED の最小しきい値および最大しきい値を C：図 8-33 で説明されているとおりに設定します。

C：図 8-33　WRED を使用したビデオ CBWFQ のしきい値の例



推奨される WRED しきい値

C：図 8-34 に、各トラフィック クラス（AF41 および AF42）の WRED しきい値と、各種のリンク速度に対してテスト済みである、推奨されるマーキング確率基準の一覧を示します。これらの値は例に過ぎないため、各トラフィック クラスのトラフィック量および最繁時の WRED ドロップ確率で必要となる積極性に基づいてテストし、カスタマイズしてください。

注　ソリューションで AF41 のみを使用する場合でも、同じ WRED の値が推奨されます。この場合、AF41 ではキューの深さの約半分で WRED を使用するようになり、キューがフルになるとテール ドロップを開始します。

C：図 8-34　　リンク速度ごとの推奨 WRED しきい値

WAN Link Speed / WRED Values		622 Mbps (OC12)	155 Mbps (OC3)	34-44 Mbps (E3/DS3)	10 Mbps	5 Mbps
AF41	min-threshold	240	180	120	60	60
	max-threshold	512	384	256	128	128
	mark-probability-denominator	50	50	50	50	50
AF42	min-threshold	40	30	20	15	15
	max-threshold	180	135	90	40	40
	mark-probability-denominator	20	20	20	20	20
Video queue bandwidth %		43	53	55	40	30

349596

次の設定例では、DS3 リンク（44 Mbps）のビデオに対するクラスベースの重み付け均等化キュー（CBWFQ）に WRED を設定します。

```
policy-map EGRESS-QUEUING
 class VOICE
  priority percent 10
 class VIDEO
  bandwidth percent 30
  random-detect dscp-based
  random-detect dscp 34 120 256 50
  random-detect dscp 36 20 90 20
fair-queue
 class SIGNALING
  bandwidth percent 2
```

注　特定の環境に応じて WRED 値をカスタマイズしなければならない場合があります。たとえば、AF42 トラフィックの量が AF41 トラフィックの量より大幅に多い場合は、それぞれのクラスに応じて WRED しきい値変数を調整するのが妥当な方法です。望ましい結果を得るためには、ドロップの変数とモニタリング レベルを微調整することが常に最善の方法となります。

プロビジョニングとアドミッション制御

ここでは、各サイト タイプのキューに対してアドミッション制御およびプロビジョニング帯域幅を指定します。内容は次のとおりです。

- 拡張ロケーション CAC
  - リージョンの設定
  - Enhanced Locations Call Admission Control の導入

- モバイルおよびリモート アクセス（MRA）を対象としたデバイス モビリ ティーの導入
- 帯域幅割り当てのガイドライン

導入のこのフェーズでは、大まかに次のステップが必要になります。

1。 Enhanced Locations CAC を設定します。

2。 最大ビデオ ビット レート グループのリージョン マトリックスを設定します。

3。 モバイルおよびリモート アクセス（MRA）エンドポイントのデバイス モビリティを導入します。

4。 帯域幅割り当てに関するガイドラインに従います。

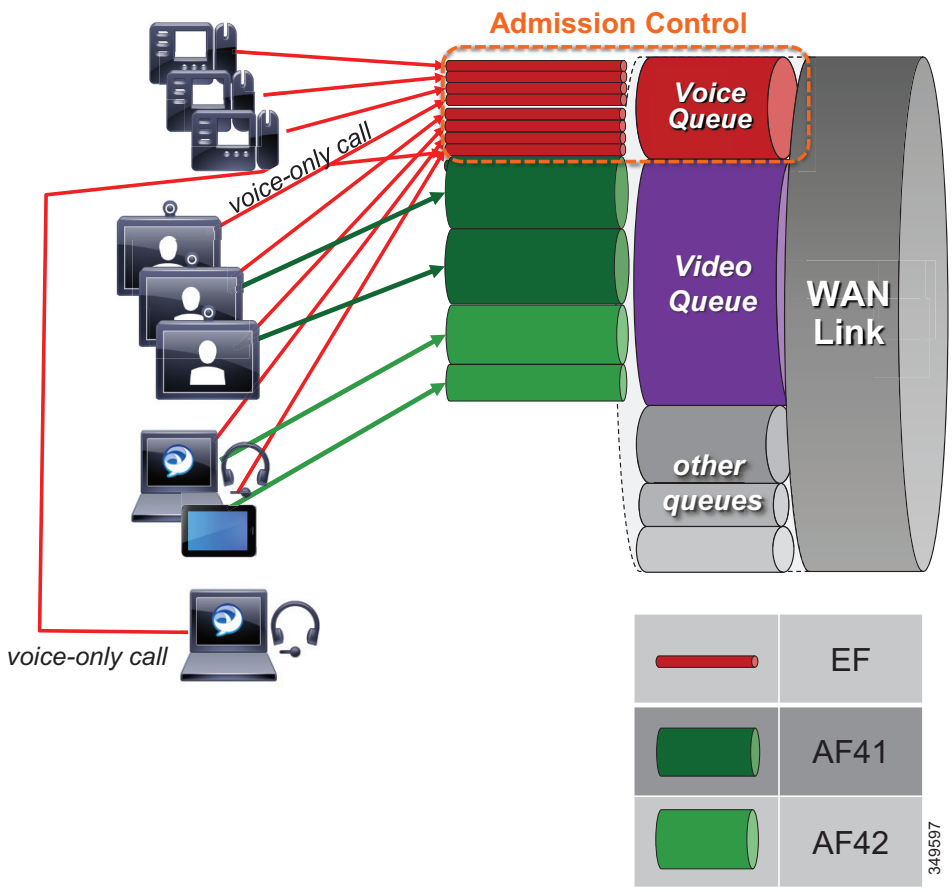
拡張ロケーション CAC

この例ではビデオ帯域幅の管理にアドミッション制御を使用しませんが、代わりに、プライオリティ キュー（PQ）がオーバーサブスクライブされないようにするために、アドミッション制御を使用してオーディオ トラフィックを管理します。この特定の例での Enhanced Locations CAC の音声プールでは、音声のみのコールおよびビデオ コール両方の音声を許可します。

Unified CM でこの機能をイネーブルにするには、CallManager サービスのコール アドミッション制御セクションで、サービス パラメータ [ビデオ コールのオーディオ プールからオーディオ帯域幅を差し引く（Deduct Audio Bandwidth from Audio Pool for Video Call）] を [はい（True）] に設定します。デフォルト設定は [いいえ（False）] であり、デフォルトでは、Unified CM はビデオ プールからビデオ コールのオーディオとビデオの両方のストリームを差し引きます。このパラメータはその動作を変更するため、プリファード アーキテクチャでの QoS の変更に不可欠です。

C：図 8-35 に、各種のコール フローとそれぞれに対応するオーディオ ストリームとビデオ ストリーム、そしてそれらのストリームが転送されるキューを示します。

C：図 8-35　　プロビジョニングとアドミッション制御



C：図 8-35 に示されている例には、次の条件が適用されます。

- プライオリティ キューはエンドポイントからのすべてのコールを対象にプロビジョニングされ、アドミッション制御（*E-LCAC 音声 BW プール*）によって保護されます。
- ビデオ キューは、ルームベースのビデオ システムにオーバープロビジョニングされます。
  - 比率は、デスクトップ ビデオ エンドポイントの使用に適用されます。
  - Jabber ビデオ コールは、ビデオ ルーム システムで使用されていない帯域幅を使用できます。
  - 輻輳の発生時、Jabber コールのビデオ ストリームでは、WRED が低下するため、ビデオ ビット レートが動的に下がります。

リージョンの設定

ビデオ エンドポイントを最大ビデオ ビット レート別のクラスにグループ化し、エンドポイントのタイプとソリューション内での用途に応じて帯域幅使用量を制限します。必要となるリージョンは合計 3 つであり（C：表 8-13 を参照）、サイトごとに 3 つのデバイス プールが必要になります。この要件が適用されるのは、組織全体（LAN と WAN の両方）で G.722 を単一オーディオ コーデックとして使用する場合の設定です。それ以外の場合、サイトごとに 3 つのリージョンも必要になります。リージョンに関する考慮事項については、「アーキテクチャー」を参照してください。

C：表 8-13　3 つのグループのリージョン マトリックスの例

エンドポイント グループ	Video_1.5MB	Video_2.5MB	Video_20MB
Video_1.5MB	1,500 kbps	1,500 kbps	1,500 kbps
Video_2.5MB	1,500 kbps	2,500 kbps	2,500 kbps
Video_20MB	1,500 kbps	2,500 kbps	20,000 kbps

Enhanced Locations Call Admission Control の導入

ネットワーク内で帯域幅リソースが限定されており、AF41 としてマーキングされたトラフィックに対応できないエリアでのみ、ビデオ コールを制限します。それ以外のエリアでは、ロケーション リンクでの帯域幅を無制限にします。

- Cisco CallManager サービスが有効になっているすべてのノードで、LBM サービスを有効にします。
- ロケーションを設定します。
  - ロケーションおよびリンク管理クラスタで、組織内のすべてのロケーションとリンクを設定します。
  - その他すべてのクラスタ（ロケーションおよびリンク管理クラスタに従属するクラスタ）では、ロケーションのみを設定し、それらのロケーションのリンクを削除します。
- 各デバイス プールにロケーションを追加します。ロケーションには、直接、またはデバイス プールを介して以下のデバイスを設定する必要があります。
  - IP フォン（デバイス プールを介して設定）
  - 会議ブリッジ（デバイス プールを介して設定）
  - ゲートウェイ（デバイス プールを介して設定）
  - SIP トランク（デバイス プールを介して設定）
  - 保留音（MoH）サーバ（直接設定）
  - アナンシエータ（デバイス プールを使用）

クラスタ間の設定

- LBM ハブ グループを設定します。
  - LBM をハブ ロールに割り当てるため使用する
  - LBM のハブのレプリケーション ネットワークの全ハブのハブ連絡先情報を複製する 3 つのリモート ハブのメンバーを定義するために使用される

    LBM は、LBM のハブのグループに割り当てられる場合のハブです。

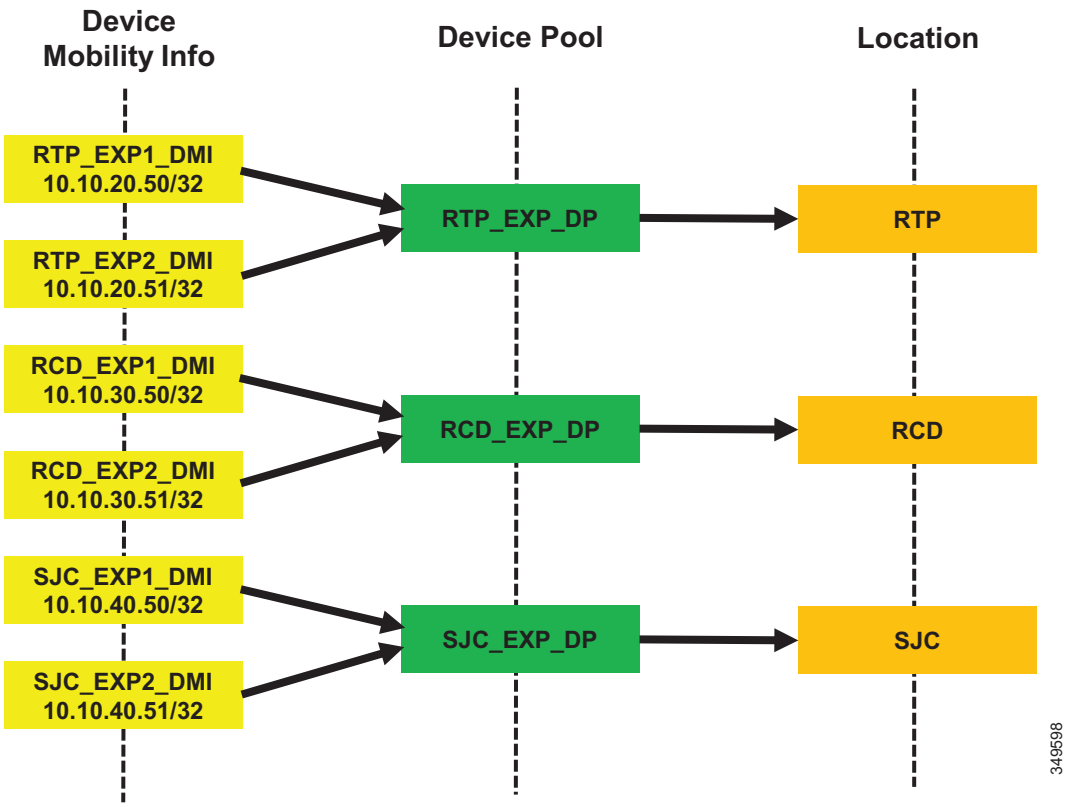
    LBM は LBM のハブのグループに割り当てられていない場合、スポークになります。
  - 名前：Cluster1_LBM_Hub_1
  - ブートストラップ サーバ：*<names or IP addresses of bootstrap servers>*（「LBM のハブのレプリケーション ネットワーク」を参照）
  - クラスタ内でハブとして機能する最大 2 つの LBM を選択します。
- クラスタ間 ELCAC が実装されている場合のロケーション設定に関する推奨事項：
  - クラスタでは、ロケーションからデバイス プールへの関連付けで、ローカルにロケーションが設定されていなければなりません。
  - 各クラスタのロケーションには、他のクラスタの直接隣接するロケーション を設定して、各クラスタのトポロジが相互接続して単一のグローバル トポロジを形成できるようにします。これは、ロケーションとリンクの管理クラスタの配置には適用されません。
  - 共通のロケーションとリンクの帯域幅制限および重みの不一致は、帯域幅および重みの最小値を使用して解決されます。
  - クラスタ全体でのロケーションの一貫した命名は重要です。「同じロケーション、同じ名前、および、異なるロケーション、異なる名前」の方法に従ってください。
  - Hub_none ロケーションの名前を変更し、各クラスタで一意の名前になるようにします。Hub_none がすべてのクラスタでデフォルトのままになっていると、同じロケーションとして扱われることになります。このようにするのが望ましいかどうかは、設定するロケーション設計に依存します（「拡張ロケーションのコールアドミッション制御」を参照）。
  - クラスタ ID は、サービスアビリティ レポートを使用できるよう、各クラスタで一意になるように設定する必要があります。

モバイルおよびリモート アクセス（MRA）を対象としたデバイス モビリ ティーの導入

デバイス モビリティ情報の設定

C：図 8-36 に、デバイス モビリティ設定の概要を示します。この図に示されているのは ELCAC がインターネットベースのデバイスで機能するためのデバイス モビリティの最小設定要件ですが、企業内の同一のエンドポイントのモビリティをサポートするために、デバイス モビリティを設定することができます企業内のデバイスを対象としたデバイス モビリティの詳細については、最新バージョンの Cisco Collaboration SRND を参照してください。

C：図 8-36　　デバイスのモビリティ設定とロケーションの関連付け

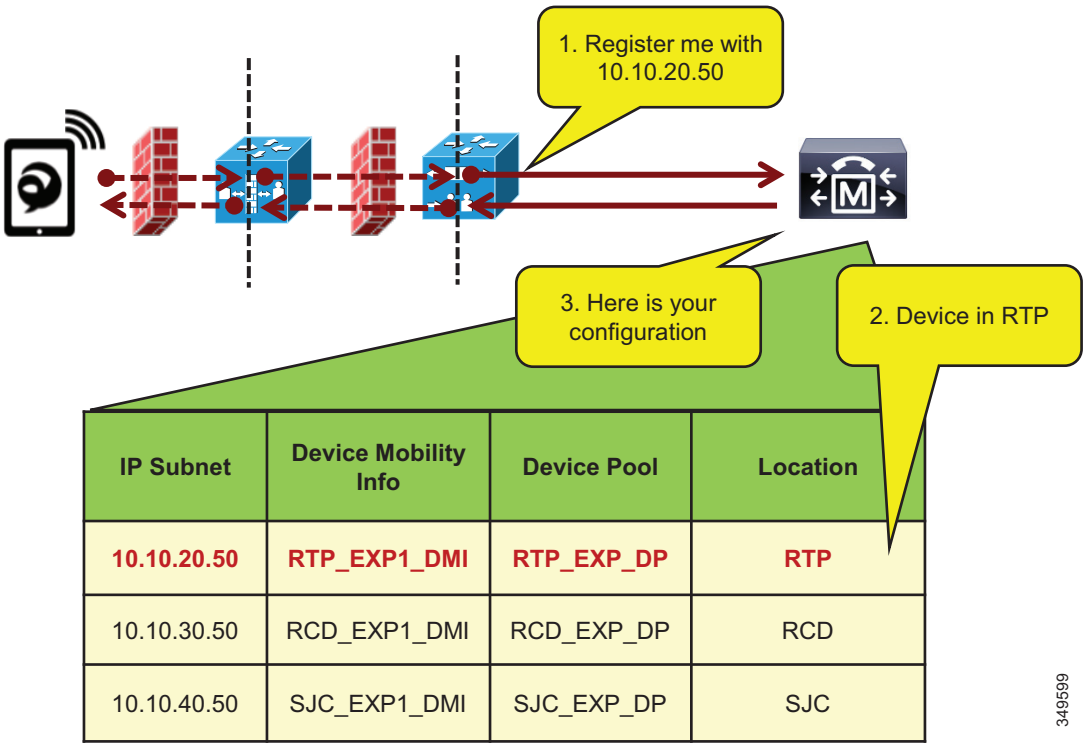


C：図 8-36 には、ELCAC の導入例でのデバイス モビリティの概略が示されています。Expressway-C サーバの IP アドレスは、デバイス モビリティ情報に設定されています。この例では、3 つのサイト（RTP、BLD、および SJC）のそれぞれに Expressway-C サーバの冗長ペアがあります。RTP_EXP1_DMI および RTP_EXP2_DMI にはそれぞれ、RTP Expressway-C サーバのサーバ IP アドレスが設定されています。この 2 つは、ロケーション RTP が設定されている RTP_EXP_DP と呼ばれる新しいデバイス プールに関連付けられます。各サイトが同様に設定されます。この設定では、任意のデバイスが RTP_EXP1_DMI または RTP_EXP2_DMI のデバイス モビリティ情報に対応する IP アドレスで Unified CM に登録されるデバイス モビリティで有効にされている場合、RTP_EXP_DP デバイス プール、そして RTP ロケーションに関連付けられます。

上記の設定では、インターネット ベースのデバイスが Expressway を介して Unified CM に登録される場合は、Expressway-C の IP アドレスを使用して登録されます。次に、Unified CM は、デバイス モビリティ情報に設定された IP アドレスを使用して、デバイス プールとこのデバイ

ス プールに関連するインターネット ロケーションを関連付けます。C：図 8-37 に、このプロセスを示します。

C：図 8-37　Expressway IP アドレスに基づいたデバイス プールとロケーションの関連付け



C：図 8-37 では、クライアントが RTP の Expressway を介して Unified CM に登録されます。シグナリングは RTP の Expressway-C で変換されるため、デバイスはその Expressway-C の IP アドレスを使用して登録されます。デバイス プール RTP_EXP_DP は、この IP アドレスに基づいてデバイスに関連付けられます。RTP_EXP_DP プールは RTP ロケーションで設定されているため、そのロケーションがデバイスに関連付けられます。そのため、デバイスが Expressway に登録されると、デバイス モビリティを介して正しいロケーションの関連付けを取得します。エンドポイントが企業に移動する場合、静的ロケーションの設定に戻ります。また、たとえばエンドポイントが SJC の別の Expressway に移動する場合、デバイス モビリティを介して正しいロケーションの関連付けを取得します。

次のようにして、Expressway-C のデバイス モビリティ情報（DMI）を設定します。

- Expressway-C グループ（ペアにされている 2 つの Expressway-C ノード）ごとに 2 つの DMI を作成します。
- サブネットに Expressway-C ノードの IP アドレスを追加し、32 ビットのマスクを適用します（これは、IP アドレスと完全に一致します）。
- サイトのデバイス プールをそれぞれの DMI に追加します。これは、Expressway ペアが位置するサイトのデバイス プールであり、適切なロージョンとロケーションが含まれている必要があります。

  一方の DMI の例：

  名前：SJC_EXP1_DMI

  サブネット：10.10.40.50

  マスク：32

  選択されているデバイス プール：SJC_Video_1.5MB

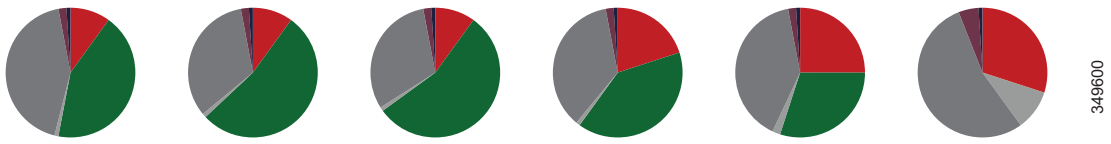
デバイス モビリティに対してデバイスを有効にします。この手順を簡単に実行するための一括管理ツール（BAT）が用意されているため、これを使用してください。

帯域幅割り当てのガイドライン

C：図 8-38 に記載する帯域幅割り当ては、この企業の例に基づく固有のガイドラインです。ここには、コラボレーション トラフィックのさまざまな共通クラスで利用可能な帯域幅の割合が示されています。

C：図 8-38　帯域幅割り当てのガイドライン

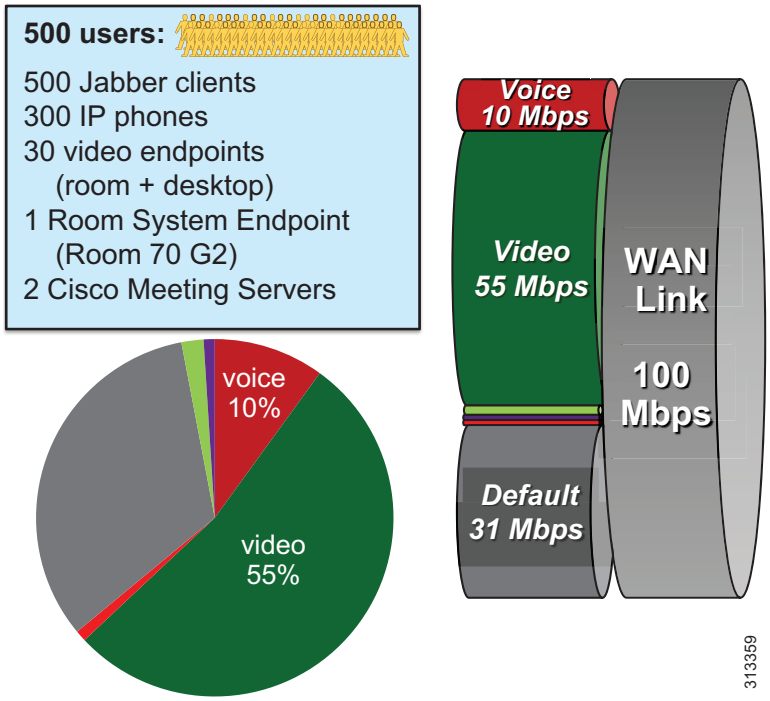
WAN Link Speed / Class	622 Mbps (OC12)	155 Mbps (OC3)	34-44 Mbps (E3/DS3)	10 Mbps	5 Mbps	<2 Mbps (T1/E1)
Control (%)	1	1	1	1	2	10
Voice (%)	10	10	10	20	25	30
Video (%)	43	53	55	40	30	--
Signalling (%)	2	2	2	2	2	5
Scavenger (%)	1	1	1	1	1	1
Default (%)	43	33	31	36	40	54



C：図 8-39 から C：図 8-42 に、各サイト（本社、大規模支社、小規模支社、営業所）と、各クラスのユーザ数と利用可能な帯域幅に基づいてクラスごとにプロビジョニングされたリンク帯域幅を示します。これらの値は、レイヤ 3 以上用に計算された帯域幅に基づいていることに注意してください。そのため、これら値にはリンク タイプ（イーサネット、フレーム リレー、MPLS など）に依存するレイヤ 2 のオーバーヘッドは含まれていません。L2 のオーバーヘッドについて詳しくは、最新バージョンの Cisco Collaboration SRND に記載されている「*Network Infrastructure*」の章を参照してください。また、ビデオ コールのオーディオ部分の帯域幅はボイス プールから差し引かれるため、音声のみのコールとビデオ コール両方のオーディオ帯域幅が含まれるように音声キューがプロビジョニングされていることにも注意してください。

注 次の計算では、エンドポイントの数に対する最大帯域幅を使用し、その値を、アクティブなコールを考慮するためのパーセンテージで乗算しています。たとえば、30 のビデオ エンドポイントがあり（30 のコールに対応可能）、アクティブなビデオ コールの割合が 20% である場合、1.2 Mbps * 30 コール * 0.2 = 7.2 Mbps という計算になります。

C：図 8-39　中央サイト



中央サイト リンク（100 Mbps）帯域幅の計算

C：図 8-39 で示すように、中央サイトには次の帯域幅要件があります。

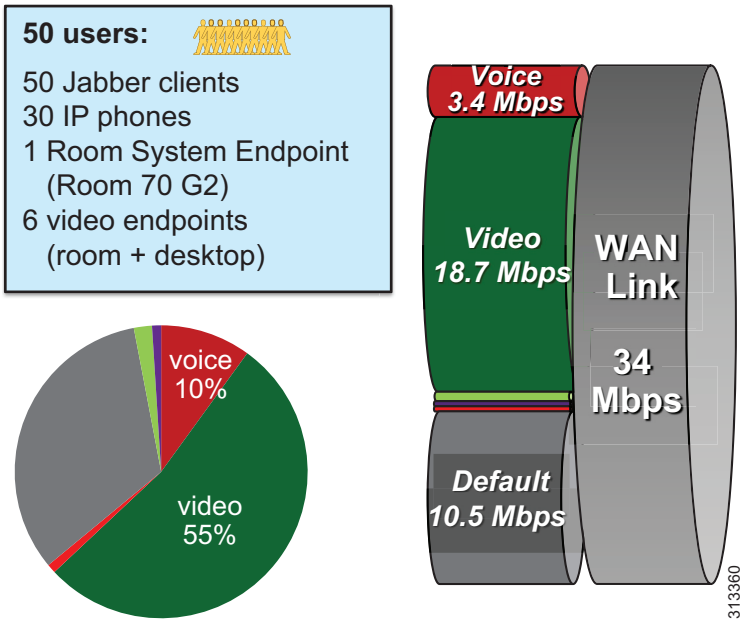
- 音声キュー（PQ）：10 Mbps（L3 帯域幅）

  G.711/G.722 での 125 のコール
- 音声プール用の Unified CM ロケーション リンク帯域幅：

  125 * 80 kbps = 10 Mbps

- ビデオ キュー：55 Mbps（L3 帯域幅）
  - ルーム システム ビデオ エンドポイント（Webex Room 70 G2）：6 Mbps ＊ 1 call = 6 Mbps
  - ビデオ エンドポイント：1.2 Mbps ＊ 30 コール ＊ 0.2 = 7.2 Mbps
  - Cisco Meeting Server: 1.5 Mbps ＊ 40 コール ＊ 0.5 = 30 Mbps
  - 55 Mbps – (6 Mbps + 7.2 Mbps + 30 Mbps) = Jabber メディア用 11.8 Mbps
    9（720p の場合）、13（576p の場合）、36（288p の場合）の Jabber ビデオ コール（さらに残りの帯域幅）

C：図 8-40　　大規模支店

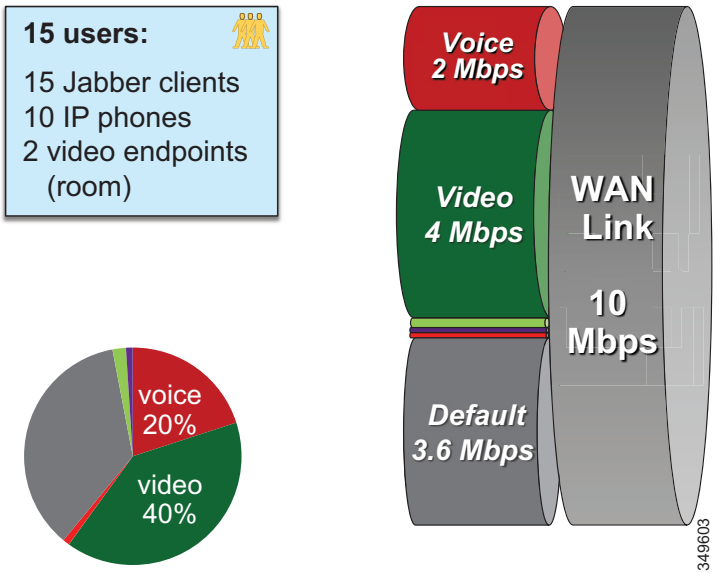


大規模支店リンク（34 Mbps）帯域幅の計算

C：図 8-40 で示すように、大規模支店サイトには次の帯域幅要件があります。

- 音声キュー（PQ）：3.4 Mbps（L3 帯域幅）
  G.711/G.722 での 42 のコール
- 音声プール用の Unified CM ロケーション リンク帯域幅：
  42 ＊ 80 kbps = 3.360 Mbps
- ビデオ キュー：18.7 Mbps（L3 帯域幅）
  - ルーム システム ビデオ エンドポイント（Webex Room 70 G2）：6 Mbps ＊ 1 call = 6 Mbps
  - ビデオ エンドポイント：1.2 Mbps ＊ 6 コール = 7.2 Mbps
  - 18.7 Mbps –（6 Mbps + 7.2 Mbps）= Jabber メディア用 5.5 Mbps
    4（720p の場合）、6（576p の場合）、17（288p の場合）の Jabber ビデオ コール（さらに残りの帯域幅）

C：図 8-41　　小規模支店



小規模支店リンク（10 Mbps）帯域幅の計算

C：図 8-41 で示すように、小規模支店サイトには次の帯域幅要件があります。

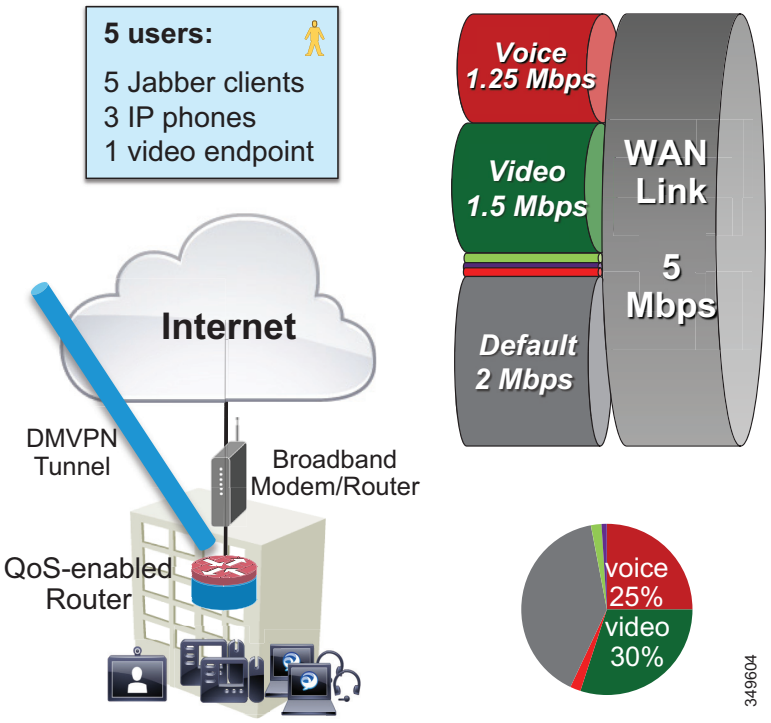
- 音声キュー（PQ）：2 Mbps（L3 帯域幅）

  G.711/G.722 での 25 のコール
- 音声プール用の Unified CM ロケーション リンク帯域幅：

  25 * 80 kbps = 2 Mbps
- ビデオ キュー：4 Mbps（L3 帯域幅）
  - ビデオ エンドポイント：1.2 Mbps * 2 コール = 2.4 Mbps
  - 4 Mbps – 2.4 Mbps = 1.6 Mbps（Jabber メディア用）

    1（720p の場合）、2（576p の場合）、5（288p の場合）の Jabber ビデオ コール（さらに残りの帯域幅）

C：図 8-42 営業所



営業所ブロードバンド インターネット接続（5 Mbps）帯域幅の計算

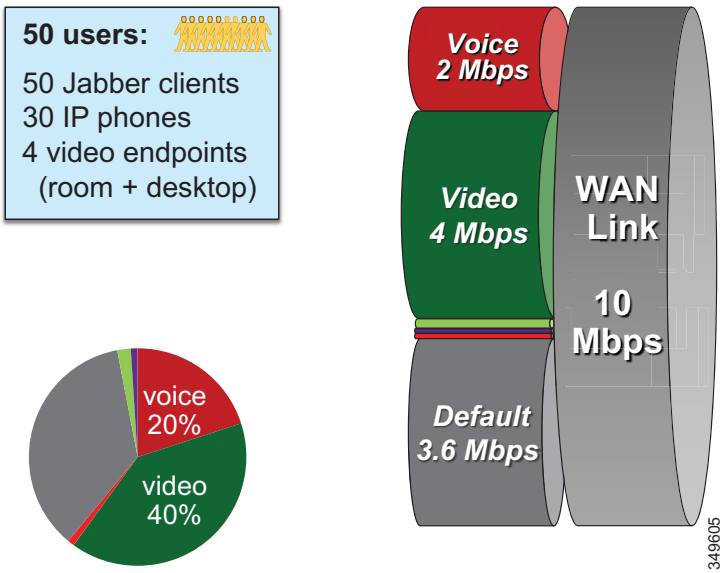
C：図 8-42 で示すように、営業所サイトには次の帯域幅要件があります。

- ブロードバンド インターネット接続 + 中央サイトへの DMVPN
- ブロードバンド アップリンク速度に対応するように VPN ルータのインターフェイスを設定する
- TCP フローの bufferbloat を回避するために VPN ルータで QoS を有効にする
- 非対称ダウンロード / アップロードのブロードバンド：ビデオ エンドポイントでのビットレートの制限を検討する
- 帯域幅の計算は、最終的には使用可能なブロードバンド帯域幅に依存するため、小規模支店サイトのリンクをプロビジョニングする場合と同じ推奨事項に従ってください。

制限付き WAN リンクを使用する大規模支店（ビデオに対応する Enhanced Locations CAC）

低速 WAN リンクを持つ特定の支店サイトでは、ビデオ キューのオーバープロビジョニングは実現不可能です。ビデオ コールがリンク帯域幅をオーバーサブスクライブしないようにするために、ビデオのこれらのロケーション リンクに、ELCAC を適用できます。このテンプレートでは、サイト固有のリージョン設定を使用して、ビデオ エンドポイントおよび Jabber クライアントで使用される最大帯域幅を制限する必要があります。また、Jabber ユーザがサイト間でローミングする場合には、デバイス モビリティも必要になることに注意してください。

C：図 8-43　制限付き WAN リンクを使用する大規模支店（ビデオに対応する Enhanced Locations CAC）



C：図 8-43 の説明のとおり、制限付き WAN リンク（10 Mbps）の大規模支店サイトには次の帯域幅要件があります。

- 音声キュー（PQ）：2 Mbps（L3 帯域幅）

  G.711/G.722 での 25 のコール
- 音声プール用の Unified CM ロケーション リンク帯域幅：

  25 * 80 kbps = 2 Mbps
- ビデオ キュー：4 Mbps（L3 帯域幅）
  - 有効な使用方法：

    720p（1,220 kbps）で 1 コール + 576p（810 kbps）で 3 コール = 3,650 kbps

    または、576p（768 kbps）で 2 コール + 288p（320 kbps）で 5 コール = 3136 kbps
  - ビデオ コールの Unified CM ロケーション リンク帯域幅：3.7 Mbps（L3 帯域幅）
  - L2 オーバーヘッドに対応できるだけの余地を残しておきます。

サイジング

改訂日：2019 年 2 月 19 日

エンタープライズ コラボレーション向けプリファード アーキテクチャ ソリューションのコンポーネントのサイジングは、ソリューション設計全体の重要な部分です。

特定の展開におけるサイジング プロセスの目標は、以下の項目を決定することです。

- 使用するプラットフォーム タイプ。
- 各 Cisco Collaboration 製品に関して展開されるインスタンスの仕様と数。

  仮想化を使用して展開される製品では、これは Open Virtual Archive（OVA）テンプレートで定義される仮想マシンのハードウェア仕様と仮想マシンの数に相当します。仮想化を使用せずに展開される製品では、これはアプライアンスまたはブレードのタイプと数に相当します。

サイジングは、考慮すべきパラメータの数が多いため、複雑な作業になる可能性があります。サイジングの作業を簡略化するため、この章ではサイジングの例を対応する仮定条件とともにいくつか紹介します。ここでは、これらのサイジング例を*簡易サイジング展開*と呼びます。個々の展開の要件がこれらの仮定条件の範囲内である場合は、このマニュアルの簡易サイジング展開を参考として使用できます。それ以外の場合は、https://www.cisco.com/go/srnd で提供される *Cisco Collaboration SRND* の最新版の*サイジング*に関する章および製品ドキュメントの記載内容に従って、通常のサイジング計算を行う必要があります。

仮想化を使用して展開された製品のサイジングを行った後は、仮想マシンを Cisco Unified Computing System（UCS）サーバに配置する方法を決定し、共存のルールを検討します。最終的には、この仮想マシンの配置プロセスによってソリューションに必要な UCS サーバの数が決まります。

この章では、このマニュアルで扱っているすべてのモジュール（つまり、コール制御、会議、コラボレーション エッジ、およびボイス メッセージング）のサイジングについて説明します。この章では、仮想マシンの配置とプラットフォームについても説明します。

このマニュアルでは、仮想マシンとして展開される製品の仮想マシン OVA テンプレートの詳しい仕様については説明しません。詳細については、次のリンク先にある *Cisco Collaboration Virtualization* に関するドキュメントを参照してください。
https://www.cisco.com/go/virtualized-collaboration.

この章の新規情報とは

C：表 9-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

C：表 9-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Meeting Management Suite	Cisco Meeting Management Suite（C：9-8 ページ）	2019 年 1 月 23 日
その他マイナー更新および修正	この章の各項で説明	2019 年 1 月 23 日
Cisco Prime License Manager の後継として Cisco Smart Software Manager が導入されました。Cisco Prime License Manager についてはこの章では説明していません。	Cisco Smart Software Manager の詳細については、「コラボレーション管理サービス」の章を参照してください。	2017 年 8 月 30 日
Cisco Unified Border Element のサイジング	Cisco Unified Border Element のサイジング（C：9-11 ページ）	2017 年 8 月 30 日

コール制御

コール制御の章で説明したように、Cisco Unified Communications Manager（Unified CM）および IM and Presence サービスは Unified CM クラスタおよび IM and Presence クラスタを通じて提供されます。

Cisco Unified CM クラスタは、1 つのパブリッシャ ノード、2 つの専用 TFTP サーバ、および 1 つまたは複数のコール処理ノード ペアで構成されます。コール処理ペアの数は展開のサイズによって異なるため、後で説明します。コール処理ノードは、1:1 の冗長性を確保するためにペアで展開されます。

IM and Presence ノードもペアで展開されます。IM and Presence ペアの数も展開のサイズによって異なるため、後で説明します。IM and Presence ノードは、1:1 の冗長性を確保するためにペアで展開されます。

Unified CM のサイジング

Unified CM については、簡易サイジングのガイダンスで最大 10,000 ユーザおよび 10,000 デバイスの展開に対応できます。Unified CM は、異なる仮定条件やコール処理ペアの追加によってより多くのユーザおよびデバイスをサポートしますが、これはこの章で示す簡易サイジングのガイダンスの範囲外です。C：表 9-2 に、簡易サイジング展開を示します。これらの展開に対して行われた仮定については、この表の後で説明します。展開環境内のユーザまたはエンドポイントの数が C：表 9-2 示す値の範囲外である場合や、個々の展開の要件が仮定条件の範囲外である場合は、これらの簡易サイジング展開を使用せずに、https://www.cisco.com/go/srnd で提供される *Cisco Collaboration SRND* の最新版の *サイジング* に関する章と、次で提供される Unified CM 製品ドキュメントに記載されている通常のサイジング手順を実行してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

C：表 9-2　　Unified CM の簡易サイジング展開

展開サイズ	展開される Unified CM ノード（各 Unified CM ノードで 7,500 ユーザの OVA テンプレートを使用）
5,000 までのユーザまたはデバイス	**5 ノード：** 1 つのパブリッシャ、2 つの TFTP、1 つのコール処理ペア（2 つのコール処理サブスクライバ）
5,000 ～ 10,000 のユーザまたはデバイス	**7 ノード：** 1 つのパブリッシャ、2 つの TFTP、2 つのコール処理ペア（4 つのコール処理サブスクライバ）

C：表 9-2 では、ユーザとデバイス（のどちらか大きい方）の最大数に基づいてサイジングしています。たとえば、5,000 人のユーザと 1 ユーザあたり平均 2 個のデバイス（ユーザごとにデスクの電話とソフトフォン モードの Jabber クライアントがある場合など）を含む展開では、合計で 10,000 個のデバイスがあるため、7 ノードの展開が必要です。

これらの簡易サイジング展開では、UCS サーバで消費されるリソース全体を最適化するため、7,500 ユーザの仮想マシン設定（OVA テンプレート）が使用されます。この OVA テンプレートには、UC のパフォーマンスを最大限に引き出す CPU プラットフォーム（Cisco Business Edition 7000 など）が必要です。このテンプレートは Business Edition 6000 などではサポートされません。これらの OVA 仮想マシン構成テンプレートおよびプラットフォーム要件の詳細については、https://www.cisco.com/go/virtualized-collaboration のドキュメントを参照してください。

7,500 ユーザの OVA テンプレートを使用して展開された Unified CM コール処理ペアは、一定の条件下で最大 7,500 人のユーザをサポートできます。しかし、この設計では Unified CM に追加の負荷がかかる仮定条件を使用します。たとえば、シングル ナンバー リーチ用のリモート接続先プロファイルを使って各ユーザを構成できること、各ユーザがエクステンション モビリティを使用できること、各エンドポイントを CTI で制御できること、いくつかの共有回線が構成されていること、モバイル アクセスやリモート アクセスが有効であることなどを仮定します。したがって、C：表 9-2 に示したように、Unified CM コール処理ペアあたりの容量は減少します。次に、簡易サイジング モデルで使用される仮定条件について詳しく説明します。

Unified CM の仮定条件

C：表 9-2 に示した 2 つの簡易サイジング展開には、次の仮定条件が適用されます。

- ユーザあたりの最繁時呼数（BHCA）が平均 4 個以下。BHCA とは、最繁時のコール試行の数です。
- デバイスあたりの DN が平均 2 個以下です。
- メディアおよび SIP シグナリング暗号化は、この Unified CM の簡易サイジングを変更せずに有効にできます。
- コール処理サブスクライバ ペアあたりの共有回線が最大 500 回線で、各回線が平均 3 個以下のデバイスによって共有されます。
- Unified CM（ソフトフォン モード）に登録される Jabber クライアントの数をデバイスの制限に照らしてカウントする必要があります。
- パーティションが最大 3,000 個、コーリング サーチ スペース（CSS）が最大 6,000 個、クラスタあたりのトランスレーション パターンが最大 12,000 個です。

- Unified CM クラスタごとに、ルート パターンが最大 1,000 個、ルート リストが最大 1,000 個、ルート グループが最大 2,100 個。Unified CM コール処理ペアごとに、ハント パイロットが最大 100 個、ハント リストが最大 100 個、サーキュラーおよびシーケンシャル回線グループが最大 50 個（回線グループあたりのメンバー数は平均 5）、ブロードキャスト回線グループが最大 50 個（回線グループあたりのメンバー数は平均 10）です。
- Unified CM コール処理ペアごとに、CTI ポートが最大 500 個、CTI ルート ポイントが最大 100 個です。
- 複数の Unified CM クラスタを展開するときは、GDPR/ILS が有効になっています。
- エクステンション モビリティ（EM）：すべてのユーザが EM を使用できますが、クラスタ間のエクステンション モビリティ（EMCC）ユーザは存在しません。1 分あたり最大 250 回の EM ログイン / ログアウトがサポートされています。（この簡易サイジングでは、EM サービスが 1 つの Unified CM ノードで有効になっていることを前提としています。）
- Unified CM のメディア リソース：この設計では、Unified CM ソフトウェア会議ブリッジ（ソフトウェア CFB）と Unified CM メディア ターミネーション ポイント（MTP）は使用できません。代わりに、Cisco Meeting Server と Cisco IOS ベースの MTP を使用します。
- モビリティ ユーザあたりのリモート接続先またはモビリティ ID が平均 1 個以下。たとえば、5,000 ユーザを含む展開では、最大 5,000 個のリモート接続先またはモビリティ ID が存在します。
- Active Directory と同期するユーザが最大 40,000 人（ただし、コールの発着信を行うアクティブ ユーザは、C：表 9-2 から選択する簡易サイジング展開に応じて最大 5,000 人または 10,000 人）です。
- Unified CM コール処理ペアあたりの同時アクティブ コール（会議セッションと会議以外のセッション）が最大 1,500 個。たとえば、すべてのコールが会議コールで、1 つの会議の平均参加者数が 10 人の場合、この設計では Unified CM コール処理ペアあたり最大 150 個の会議コールがあると仮定します。
- Unified CM コール処理ペアあたりのコール数 / 秒（CPS）が最大 15 個です。

この他、Cisco Collaboration ソリューションに適用可能な容量制限や、『*Cisco Collaboration SRND*』の最新版および製品ドキュメントに記載されている容量制限も適用されます。次に例を示します。

- コンピュータ テレフォニー インテグレーション（CTI）：すべてのデバイスを CTI で使用できます（デバイスあたり最大 5 回線、同じ CTI デバイスを監視する J/TAPI アプリケーションが最大 5 個）。
- アナンシエータ：Unified CM コール処理ペアあたり 48 個。保留音（MoH）：コール処理ペアあたりの同時 MoH セッションが 250 個です。アナンシエータや同時 MoH セッションの数が多い場合は、スタンドアロンの Unified CM サブスクライバを MoH サーバとして展開します。
- ゲートウェイ：クラスタあたり最大 2,100 個です。
- ロケーションとリージョン：リージョンを追加するときには、[オーディオコーデック設定リスト（Audio Codec Preference List）] と [音声およびセッション ビットレート（Audio and Session Bit Rate）] の値として [システム デフォルトの使用（Use System Default）] を選択します。個々のリージョンについてこれらの値をデフォルトから変更すると、サーバの初期化とパブリッシャのアップグレードにかかる時間に影響します。合計 2,000 のリージョンを使用する場合、最大 200 リージョンでデフォルト以外の値を使用するように変更できます。合計 1,000 以下のリージョンを使用する場合、そのうち最大 500 のリージョンでデフォルト以外の値を使用するように変更できます。最大 2,000 のロケーションがサポートされており、ロケーションにはリージョンのような使用制限はありません。

IM と Presence のサイジング

IM and Presence については、簡易サイジングのガイダンスで最大 15,000 ユーザまたは 15,000 のログイン Jabber エンドポイントの展開に対応できます。C：表 9-3 に、簡易サイジング展開を示します。展開環境内のユーザ数またはログイン Jabber エンドポイントの数が C：表 9-3 に示す値の範囲外である場合は、これらの簡易サイジング展開を使用せずに、『*Cisco Collaboration SRND*』の最新版の *サイジング*に関する章および製品ドキュメントに記載されている通常のサイジング手順を実行してください。

C：表 9-3　　IM and Presence の簡易サイジング展開

展開サイズ	展開する IM and Presence ノード
5,000 未満のユーザまたはログイン Jabber エンドポイント	5,000 ユーザの OVA テンプレートを使用する 1 つの IM and Presence ペア
5,000 ～ 15,000 のユーザまたはログイン Jabber エンドポイント	15,000 ユーザの OVA テンプレートを使用する 1 つの IM and Presence ペア

たとえば、展開環境のユーザ数が 5,000 であり、各ユーザが平均して 2 つの Jabber エンドポイントに同時にログオンする場合、キャパシティは 10,000 ログイン Jabber エンドポイントで制限されます。したがって、この展開環境では 15,000 ユーザの OVA テンプレートを使用する 1 つの IM and Presence ペアが必要です。C：表 9-3 に示す 2 つの OVA 仮想マシン設定テンプレートには、Unified Communications のパフォーマンスを最大限に引き出す CPU プラットフォーム（Cisco Business Edition 7000 など）が必要です。これらの OVA 仮想マシン設定テンプレートおよびプラットフォーム要件の詳細については、https://www.cisco.com/go/virtualized-collaboration で入手可能なドキュメントを参照してください。

2 つの IM and Presence ノードは、一方のノードに障害が発生した場合に冗長性を提供するため、ペアとして展開されます。

SRST のサイジング

Survivable Remote Site Telephony（SRST）モードの Cisco サービス統合型ルータ（ISR）でサポートされる電話機および DN の数は、プラットフォームによって異なります。C：表 9-4 キャパシティの例が提供されます。その他の SRST プラットフォームに関する情報（必要な DRAM とフラッシュ メモリの量を含む）については、次のリンク先にある Cisco Unified SRST のドキュメントを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html

C：表 9-4　　SRST のサイジング例

プラットフォーム	電話機の最大数	DN の最大数
Cisco 4451-X サービス統合型ルータ	1,500	2,500

会議

会議展開のサイジングは、主に Cisco Meeting Server で必要となる同時接続の数を決定する作業です。次のような検討事項があります。

- 地理的なロケーション：Unified CM のサービスを提供する地域ごとに、会議専用のリソースを確保する必要があります。たとえば、Unified CM、Cisco Meeting Server、およびその他のサーバをインストールする中央のロケーションを米国向けに 1 か所、EMEA 向けに 1 か所、それぞれ設置できます。
- Cisco Meeting Server プラットフォームの容量
- 会議のタイプ：音声またはビデオ（あるいはその両方）。スケジュールされた会議またはスケジュールされていない会議（あるいはその両方）
- 会議のビデオ解像度：高品質の会議ほど多くのリソースを消費します。
- 大規模な会議の要件：オールハンズ ミーティングなど

地域ネットワークの会議メディアをできるだけ多く維持するため、会議リソースは一般に 1 つの地域でのみ使用されます。したがって、サイジングは地域単位で検討することができます。

会議ポートの使用ガイドライン

音声およびビデオ会議のサイジングは、お客様、お客様のユーザ ベース、およびお客様の会議手順に関する個別の詳細に大きく依存します。この項のガイドラインを会議展開のサイジングの基本として使用できますが、ユーザとポートの比率は展開環境と組織の要件によって大きく異なります。

C：表 9-5 に、会議リソース要件を計画する最初の段階で推奨される比率を示します。これらの数は、展開されるエンドポイントの機能、代替の音声会議（Cisco Webex など）の可用性、および会議の作成と参加におけるユーザの快適度によって大きく変化します。最初に、次の式を使ってポートの要件を計算します。

- 音声ポート = 50 + (<number of users> / 9)
- ビデオ ポート = 8 + (<number of users> / 15)

C：表 9-5　　推奨される会議ポートの数

ユーザ数	音声ポートの数	ビデオ ポートの数
1,000	161	75
1,750	244	125
3,000	383	208
5,000	605	342
10,000	1,161	675

C：表 9-5 に示した数は、スケジュールされた会議とスケジュールされていない会議のどちらにも使用できます。スケジュールされた会議については、お客様が既存の使用状況データを使って、同時会議の使用量についてより明確な結論を出すことが期待されます。

お客様が行う会議のタイプを理解することで、必要なポートの数をより正確に特定できます。ポートの総数は次の式で計算できます。

ポートの総数 = <Average number of participants in a meeting> X <Concurrent meetings>

たとえば、ユーザが 3,000 人の場合、C：表 9-5 では 208 ポートを推奨しています。これにより、たとえば、会議あたり平均 3 人の参加者と 69 個の同時会議、または会議あたり平均 6 人の参加者と 34 個の同時会議に対応できます。推奨されるポート数をこのように評価することで、ポートの総数が展開環境に対して十分なものかどうかを簡単に判定できます。

検討すべきもう 1 つの重要な点は、予想される最大の会議サイズです。ほとんどの場合、最大の会議はオールハンズ ミーティング タイプです。たとえば、お客様のユーザ数が 1,000 人でも、全員参加のテレプレゼンス会議で 96 個のシステムを結合する必要がある場合は、推奨値の 75 ポートでは間に合いません。

Cisco Meeting Server プラットフォームのサイジング

Cisco Meeting Server は、会議のサポートや拡張性が異なる複数のモデルおよびプラットフォームで使用可能です。C：表 9-6 に、企業展開で推奨される Cisco Meeting Server プラットフォームと、関連するノードあたりのポート容量を示します。この数値は、非暗号化および暗号化メディアおよびシグナリングで有効です。Cisco Meeting Server のクラスタリング、その他の Cisco Meeting Server プラットフォーム、またはその他のビデオおよびデータ チャネル解像度の詳細については、次のリンク先にある『*Cisco Meeting Server and Cisco Meeting App Data Sheet*』を参照してください。

https://www.cisco.com/c/en/us/products/conferencing/meeting-server/datasheet-listing.html

C：表 9-6　　Cisco Meeting Server プラットフォームと容量

Cisco Meeting Server プラットフォーム[1]	Full HD 1080p30 ポート容量[2]	HD 720p30 ポート容量[2]	SD 480p30 ポート容量[2]
Cisco Meeting Server 1000	48	96	192
Cisco Meeting Server 2000	350	700	1,000

1. Cisco Meeting Server は、任意の音声コーデックを使用するスタンドアロン展開またはクラスタの音声接続を最大 3,000 個サポートします。
2. 解像度 720p および 5 フレーム / 秒（fps）でコンテンツを共有すると仮定します。

他にも留意すべき事項があります。たとえば、Cisco Meeting Server ではノードあたり各会議で最大 450 の参加者をサポートしています。この容量を増加するには、Cisco Meeting Server ノードを追加します。

Cisco TelePresence Management Suite（TMS）

Cisco TMS については、C：表 9-7 に示す 2 つの簡易サイジング展開をお勧めします。TMS には他にも可能な展開がありますが、このガイドでは説明しません。たとえば、TMS、TMSXE、および Microsoft SQL のすべてのコンポーネントを同じ仮想マシンに配置する単一サーバ展開については、冗長性が提供されないため、ここでは説明しません。

C：表 9-7 に示した 2 つの展開では、高可用性が提供されます。冗長ノードは、拡張性ではなく回復力を確保するために展開されます。プライマリ ノードとバックアップ ノードに単一の仮想 IP アドレスを提供するロード バランサも必要です。

C：表 9-7　　Cisco TMS の簡易展開と容量

展開モデル	展開	Cisco TMS	Cisco TMSXE
通常の展開	合計 2 ノード： 各ノードで実行されている TMS および TMSXE の両方 Microsoft SQL 用のサーバを追加する	制御対象システム（TMS に追加されるスケジューリング用のエンドポイント）が最大 200 個 同時参加者が最大 100 人 同時進行するスケジュール済み会議が最大 50 個	Microsoft Exchange で予約可能なエンドポイントが最大 50 個
大規模な展開	合計 4 ノード： TMS がある 2 つのノードと TMSXE がある 2 つのノード Microsoft SQL 用のサーバを追加する	制御対象システム（TMS に追加されるスケジューリング用のエンドポイント）が最大 5,000 個 同時参加者が最大 1,800 人 同時進行するスケジュール済み会議が最大 250 個	Microsoft Exchange で予約可能なエンドポイント数：1,800 未満 または Office 365（またはオンプレミスの Exchange と Office 365 の組み合わせ）で予約可能なエンドポイント数：1,000 未満

Cisco TMS のパフォーマンスとスケーリングに影響を与えるその他の要因として、次が挙げられます。

- Cisco TMS Web インターフェイスにアクセスするユーザの数。
- スケジュールまたは監視されている会議の同時開催。
- 複数の拡張機能またはカスタム クライアントによる Cisco TMS Booking API（TMSBA）の同時使用。ブッキングのスループットは、Cisco TMS の [新しい会議（New Conference）] ページを含むすべてのスケジューリング インターフェイスで共有されます。

Cisco TMS のサイジングの詳細については、次の場所にある『*Cisco TelePresence Management Suite Installation and Upgrade Guide*』を参照してください。

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-guides-list.html

Cisco Meeting Management Suite

Cisco Meeting Management Suite には、Cisco Meeting Server の Call Bridge 数、すべての Call Bridge のピーク時に開始されたコール レッグの数、および会議管理にログインしているユーザ数に応じて、2 つの VM 設定が同時に提供されます。詳細については、以下で提供される最新バージョンの *Cisco Meeting Management インストレーションおよび設定ガイド*を参照してください。

https://www.cisco.com/c/en/us/support/conferencing/meeting-management/products-installation-guides-list.html

コラボレーション エッジ

この項では、コラボレーション エッジの 2 つの主要コンポーネントである Cisco Expressway と Cisco Unified Border Element のサイジングについて説明します。

Cisco Expressway のサイジング

C：表 9-8 中規模 OVA テンプレートを使用する際、特定の時点で 1 つの Expressway ノードで処理可能な最大容量が表示されます。

Expressway ノードはクラスタに編成されており、冗長性と高いスケーラビリティを提供します。このドキュメントで説明する推奨クラスタ構成は、2、3、または 6 ノードのクラスタからなります。C：表 9-9 に、推奨される展開のクラスタ容量を示しますすべての展開モデルが冗長性に対応していることに注意してください。2 ノードまたは 3 ノードのクラスタでは、1 つのノードに障害が発生してもクラスタ容量に影響しません（N+1 冗長性）。6 ノードのフル クラスタでは、2 つのノードに障害が発生してもクラスタ容量に影響しません（N+2 冗長性）。

クラスタ容量と冗長性レベルの関係をさらに理解するため、次の例では、中規模 OVA テンプレートを使用して通常動作中およびフェールオーバー後のビデオ容量を分析します。

ノードあたりの最大ビデオ コール容量は 100 セッションです。回復力のない展開における 3 ノードのクラスタでは、クラスタのビデオ コール容量は 300 ですが、1 つのノードに障害が発生した場合はその 1/3 に減少します。推奨される高可用性の 3 ノード クラスタでは、3 ノードのいずれかに障害が発生した場合に回復力を提供し、クラスタ容量を維持するため、ビデオ セッション容量が 200 に制限されます。通常の操作では、ビデオ コールの負荷がクラスタ全体で分散され、各ノードが約 66 のビデオ コールを処理します。1 つのノードで障害が発生すると、残りのノードで 200 ビデオ セッションすべてを処理でき（各ノードで 100 のビデオ セッションを処理できるため）、クラスタ容量が維持されます。

C：表 9-8　　Expressway ノードの容量

OVA テンプレート	ノードあたりのモバイルおよびリモート アクセスのプロキシ登録数[1]	ノードあたりのビデオ コール容量	ノードあたりの音声専用コール容量
中規模 OVA テンプレートによる仮想マシン	2,500	100	200

1. プロキシ登録に関する考慮事項は、モバイルおよびリモート アクセスにのみ適用され、Business-to-Business（B2B）コミュニケーションには適用されません。

C：表 9-9　　Cisco Expressway の簡易サイジング展開と関連するクラスタ容量

展開モデル	Expressway クラスタの展開	冗長性モデル	クラスタあたりのモバイルおよびリモート アクセスのプロキシ登録数[1]	クラスタあたりのビデオ コール容量	クラスタあたりの音声専用コール容量
中規模 OVA テンプレートによる仮想マシン					
展開 1	2 ノード	N+1	2,500	100	200
展開 2	3 ノード	N+1	5,000	200	400
展開 3	6 ノード	N+2	10,000	400	800

1. プロキシ登録に関する考慮事項は、モバイルおよびリモート アクセスにのみ適用され、Business-to-Business（B2B）コミュニケーションには適用されません。

注　その他、2 つの OVA テンプレート、小規模 OVA テンプレートおよび 大規模 OVA テンプレートが提供されます。小規模 OVA テンプレートは、Cisco Business Edition 6000M または 6000H で実行される設計です。大規模 OVA テンプレートは Cisco Business Edition 7000 ではサポートされておらじ、特定のハードウェアでのみで限定して提供されています。また、Cisco Expressway CE1200 のハードウェア アプライアンスを使用するオプションもあります。詳細については、https://www.cisco.com/go/virtualized-collaboration のドキュメントを参照してください。

C：表 9-9 に示した Expressway の簡易サイジング展開には、次の仮定条件が適用されます。

- すべてのビデオ コールが暗号化されています。すべてのビデオ コールの平均コール レートは 768 kbps です。たとえば、ビデオ コールの半分が 384 kbps で、残りの半分が 1152 kbps です。
- すべての音声コールが暗号化され、すべての音声コールの平均帯域幅は 64 kbps です。
- 中規模 OVA テンプレートを使った仮想マシンでは、コール レートはノードあたり最大 5 コール / 秒（cps）です。

Cisco Expressway をクラスタ化する場合は、次のガイドラインが適用されます。

- Expressway クラスタは最大 6 ノードをサポートします（クラスタ容量はノード容量の最大 4 倍）。
- Expressway-E ノードと Expressway-C ノードは別個にクラスタ化されます。Expressway-E クラスタは Expressway-E ノードのみで構成され、Expressway-C クラスタは Expressway-C ノードのみで構成されます。
- Expressway のピアは、Expressway-E クラスタと Expressway-C クラスタで同じ数だけ展開する必要があります。たとえば、3 ノードの Expressway-E クラスタは、3 ノードの Expressway-C クラスタとともに展開する必要があります。
- Expressway-E クラスタと Expressway-C クラスタの各ペア間およびペア内のすべてのノードの容量は、同じである必要があります。たとえば、Expressway-E クラスタ内または対応する Expressway-C クラスタ内の他のノードが中規模 OVA テンプレートを使用している場合は、小規模 OVA テンプレートを使用する Expressway-E ノードを展開してはいけません。
- Expressway-E クラスタと Expressway-C クラスタのペアは、ノード容量がすべてのノードで同じであるかぎり、アプライアンスで実行されるノードまたは仮想マシンとして実行されるノードを組み合わせて構成できます。
- 複数の Expressway-E および Expressway-C クラスタを展開して、容量を増やすことができます。

Expressway に詳細については、次の場所にある『*Cisco Expressway Administrator Guide*』を参照してください。

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

Cisco Expressway のサイジング例

ある企業では、6,000 人のユーザがいて、平均 1,000 人のユーザが常に出張しています。常にモバイル ユーザの 80% がモバイルおよびリモート アクセスを必要としています。このケースでは、800 人（1,000 人の 80%）が同時登録できるように Expressway をサイジングする必要があります。

さらに、モバイル ユーザの 10% が同時にコールを行います。これらのユーザの 5% が Expressway 経由でコールし、残りの 5% が携帯電話ネットワーク経由でコールするため、Expressway に対する同時コール数は 40（800 の 5%）です。

社内ネットワークでは、ユーザの 1% が同時に Business-to-Business（B2B）コールを行います。これによって、50 個（(6,000 - 1,000）の 1%）のコールが追加されます。

このケースでは、800 個の同時登録と 90 個の同時コール（40 + +50）をサポートするようにクラスタをサイジングする必要があります。

C：表 9-8 に示すように、中規模 OVA テンプレートは最大 100 個の同時コールと 2,500 個の同時登録をサポートします。したがって、中規模 OVA テンプレートを使用する 2 ノードで構成される Expressway-C クラスタと、やはり中規模 OVA テンプレートを使用する 2 ノードで構成される Expressway-E クラスタを展開することができます。C：表 9-9 の展開 1 で示したように、各 Expressway サーバ ノードは 800 個の登録と 90 個のコールをすべて同時に管理できます。クラスタ化が必要とされる理由は、2 つの Expressway ノードのいずれかが停止した場合に、もう一方のノードがすべてのトラフィックを処理できるためです。通常の状況では、Expressway-C クラスタと Expressway-E クラスタの 2 つのノード間でコールと登録の負荷が分散されます。

この例では、しばらくすると Business-to-Business（B2B）コールが 1% から 3% に増加します。そこで、90 個ではなく 190 個（40 + +150）の同時コールに対応する必要があります。中規模 OVA テンプレートの最大処理量は 100 コールなので、この場合は大規模なクラスタを展開する必要があります。C：表 9-9 に示すように、展開 2 によって、1 つのサーバに障害が発生しても 200 個の同時コールに対応できます。したがって、この例の管理者は、Expressway-C および Expressway-E クラスタにもう 1 つの中規模 OVA ノードを追加して、クラスタあたり合計 3 ノードを展開します。

Cisco Unified Border Element のサイジング

Cisco Unified Border Element は広範囲のシスコ ルーティング プラットフォームでサポートされます。これには、Cisco 4400 シリーズのサービス統合型ルータ（ISR）や Cisco 1000 シリーズのアグリゲーション サービス ルータ（ASR）が含まれます。また、Cisco Unified Border Element は、次のプラットフォームで冗長性を提供します。

- Cisco ISR プラットフォームでは、アクティブ コールのシグナリングとメディアの両方の保護を含むボックスツーボックス冗長性を提供できます。
- Cisco ASR プラットフォームでは、アクティブ コールのメディアとシグナリングの保護（ステートフル フェールオーバー）を含むインボックス冗長性またはボックスツーボックス冗長性を提供できます。

C：表 9-10 では、いくつかのプラットフォームについて容量の例を示します。この表には、エンドツーエンド PSTN SIP 間コールの最大数に対応する SIP トランク セッションの最大数を示します。これにより、メディアおよびシグナリングを暗号化しない場合の制限と、RTP/SRTP インターワーキング（トラフィックが社内ネットワーク内部で暗号化され、SIP サービス プロバイダーへの接続では暗号化されない）の制限が決定します。その他のプラットフォームや、必要な DRAM とフラッシュ メモリの量などの詳細については、次の場所にある『*Cisco Unified Border Element Data Sheet*』および『*Cisco Unified Border Element and Gatekeeper Ordering Guide*』を参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/unified-border-element/datasheet-listing.html

C：表 9-10　Cisco Unified Border Element の容量の例

プラットフォーム	非暗号化メディアおよびシグナリングでの最大 SIP トランク セッション数	暗号化メディアおよびシグナリングでの最大 SIP トランク セッション数
Cisco 4451-X サービス統合型ルータ	6,000	1,400
Cisco 1004 および 1006 アグリゲーション サービス ルータ	16,000	5,000

Cisco Unified Border Element のサイジング例

企業に 10,000 のユーザが存在し、社内ネットワークでメディアおよびシグナリング暗号化が有効になっています。最繁時にはユーザの 10% が同時にコールを行います。ユーザの 8% は外部の接続先にコールし、残りのユーザは内線コールに関与しています。電気通信業者とこの企業はすべてのコールに G.711 を使用できることで合意しているため、トランスコードは必要ありません。この展開では、800 個の SIP セッション（10,000 人の 8%）が必要です。C：表 9-10 に示すように、Cisco 4451-X ISR では暗号化により最大 1,400 個のセッションをサポートできます。したがって、この例では 2 つの Cisco 4451-X ISR を展開でき、1 つをアクティブ、もう 1 つをスタンバイとして使用することで冗長性を確保できます。

ボイス メッセージング

ここでは、Cisco Unity Connection のサイジングについて説明します。

Cisco Unity Connection 導入プロセスの項で説明したように、この設計で推奨される Unity Connection の展開は、アクティブ / アクティブ モードのパブリッシャ 1 台とサブスクライバ 1 台で構成されます。

このガイドでは、Unity Connection のユーザ数と Jabber エンドポイント数に応じた 3 つの簡易サイジング展開について説明します。これらの展開を C：表 9-11 に示します。たとえば、展開に 10,000 のユーザと 1,000 の Jabber エンドポイントが含まれている場合、少なくとも 10,000 ユーザの OVA テンプレートを展開する必要があります。あるいは、展開に 6,000 のユーザと 2,000 の Jabber エンドポイントが含まれている場合、少なくとも 10,000 ユーザ OVA テンプレートを展開する必要があります。Unity Connection には他にも可能な展開がありますが、このガイドでは説明しません。その他の可能な展開については、『*Cisco Collaboration SRND*』の最新版および製品ドキュメントを参照してください。

C：表 9-11　Cisco Unity Connection の簡易サイジング展開

展開サイズ	アクティブ / アクティブで展開する Unity Connection ノード
最大 5,000 ユーザまたは最大 1,000 Jabber エンドポイント	5,000 ユーザの OVA テンプレートを使用する 1 つの Unity Connection ペア
5,000 ～ 10,000 ユーザまたは最大 2,000 Jabber エンドポイント	10,000 ユーザの OVA テンプレートを使用する 1 つの Unity Connection ペア
10,000 ～ 20,000 ユーザまたは最大 5,000 Jabber エンドポイント	20,000 ユーザの OVA テンプレートを使用する 1 つの Unity Connection ペア

Cisco Unity Connection の仮定条件

- すべての Cisco エンドポイント（Jabber エンドポイントを含む）にハイ アベイラビリティが実装されています。
- メディアおよび SIP シグナリング暗号化は、この Unity Connection の簡易サイジングを変更せずに有効にできます。
- すべてのユーザに対し 1 つの受信トレイが存在します（ユニファイド メッセージング）。
- ボイス メッセージの通知（新着メッセージ、メッセージの更新、メッセージの削除）では（HTTPS ではなく）HTTP が使用されます。

OVA テンプレートの制限を超えないようにする必要があります。たとえば、5,000 ユーザの OVA テンプレートには、G.711 で 200 ポート、G.722 で 50 ポートの制限があります。OVA テンプレートの制限の詳細については、次を参照してください。

- 次の場所にある Cisco Unity Connection の仮想化に関する情報 https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unity-connection.html
- 次の場所にある『*Cisco Unity Connection Supported Platforms List*』 https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-guides-list.html

ボイスメールの保存に必要なストレージ量を検討することも重要です。メッセージ ストレージは、仮想ディスクのサイズによって異なります。たとえば、G.711 コーデックを使用するメッセージのストレージは 5,000 ユーザの OVA テンプレートでおよそ 137,000 分であり、これは 200 GB の vDisk 1 台で定義されます。10,000 ユーザの OVA テンプレートを使用する場合は、異なるメッセージ ストレージ要件に対応するために別の vDisk サイズを使用できます。詳細については、『*Cisco Unity Connection Supported Platforms List*』の最新版を参照してください。

コラボレーション管理サービス

ここでは、企業のコラボレーションのプリファード アーキテクチャで使用される次の管理サービスのサイジングについて説明します。

- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Provisioning

この設計における Cisco Prime Collaboration プロビジョニングの推奨される展開は、1 つのノードで構成されています。この展開には冗長ノードはありません。代わりに、Cisco Prime Collaboration プロビジョニング仮想マシンをバックアップします。

このガイドには、エンドポイントの数に基づく Cisco Prime Collaboration プロビジョニングの 2 種類のサイジング展開が記載されています。これらの展開を C：表 9-12 に示します。Cisco Prime Collaboration プロビジョニングには他にも可能な展開がありますが、このガイドでは説明しません。その他の可能な展開については、『*Cisco Collaboration System 11.x SRND*』の最新版および Cisco Prime Collaboration プロビジョニング製品ドキュメントを参照してください。

C：表 9-12　　Cisco Prime Collaboration プロビジョニングの展開サイジング

展開サイズ	展開する Cisco Prime Collaboration プロビジョニング ノード
最大 3,000 デバイス	小規模（3,000 デバイス）OVA テンプレートを使用する 1 つのノード
最大 20,000 デバイス	中規模（20,000 デバイス）OVA テンプレートを使用する 1 つのノード

Cisco Prime Collaboration Deployment

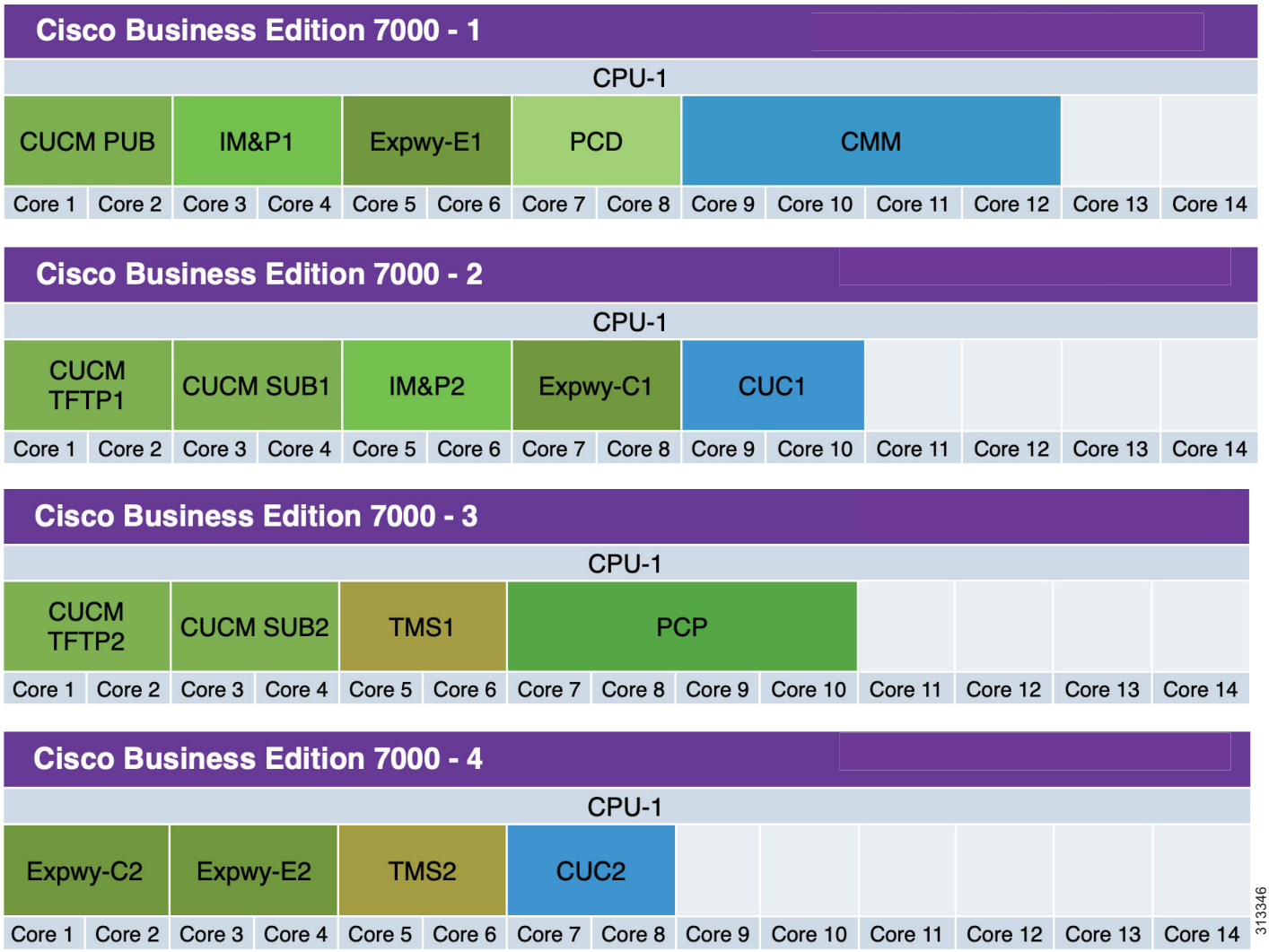
Cisco Prime Collaboration Deployment は 1 つのノードとして展開されます。この展開には冗長ノードはありません。代わりに、Prime Collaboration Deployment 仮想マシンをバックアップします。1 つの Cisco Prime Collaboration Deployment ノードでサポートできる展開のサイズに制限はありません。

仮想マシンの配置とプラットフォーム

仮想化を使用して展開される Cisco Collaboration 製品については、展開をサイジングした後の次のステップとして、Cisco Unified Computing System（UCS）サーバに仮想マシンをまとめて配置する方法を決定します。これにより、ソリューションに必要な UCS サーバの数が最終的に決定します。このプロセスは、Collaboration Virtual Machine Placement Tool（VMPT）を使用して実行します。このツールを使用するには cisco.com へのログインが必要です。このツールは https://www.cisco.com/go/vmpt から入手できます。

C：図 9-1 に、5,000 ユーザと 5,000 の合計エンドポイント（1,000 の Jabber エンドポイントを含む）の展開に VMPT を使用する例を示します。この例は、Cisco Business Edition 7000M が展開されていることを前提としています。Cisco Meeting Server は含まれていません。Cisco Meeting Server は Cisco Meeting Server 1000 プラットフォームに展開されていることを前提としています。

C：図 9-1　　VMPT を使った仮想マシンの配置例



通常は、VMPT を使用するのに加えて、仮想マシンの配置を検証するため、展開環境が次のドキュメントに記載されている共存要件をすべて満たしているかどうか確認することをお勧めします。

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html

主な配置と共存のルールは次のとおりです。

- オーバーサブスクリプションをしない：すべての仮想マシンの仮想ハードウェアと物理ハードウェアが 1 対 1 でマッピングされている必要があります。たとえば、CPU については、ハイパースレッディングが有効になっている場合でも、仮想ハードウェアと物理ハードウェアが 1 対 1 でマッピングされている必要があります。
- vSphere 5.5 以降で使用可能な VMware 遅延感度は、Unity Connection 仮想マシンでは [高（High）] に設定する必要があります。このように設定しない場合は、Unity Connection がインストールされている各 ESXi ホスト上の ESXi スケジューラ用に予備の 1 つの物理コアを予約する必要があります。
- このガイドで説明しているほとんどのアプリケーションは、サードパーティ製アプリケーションとの共存をサポートしているため、同じ UCS サーバにインストールできます。ただし、サードパーティ製アプリケーションとの共存では、サードパーティ製アプリケーションが Cisco Collaboration アプリケーションと同じルールに従う必要があります。たとえば、サードパーティ製アプリケーションを Cisco Collaboration アプリケーションと同じホストにインストールした後は、そのサードパーティ製アプリケーションで CPU のオーバーサブスクリプションがサポートされない、Unity Connection の展開時に ESXi スケジューラ用に物理コアを予約する必要がある、などです。Cisco Business Edition プラットフォームでは、共存オプションの一部が ESXi ライセンスで指定されます。たとえば、Cisco UC Virtualization Hypervisor および Foundation では、共存できるサードパーティ製アプリケーションの数に制限があります。

冗長性の考慮

ハードウェア プラットフォームに高い冗長性がある場合でも、ハードウェアの冗長性を考慮することをお勧めします。たとえば、C：図 9-1 の例で示すように、プライマリ アプリケーションとバックアップ アプリケーションの仮想マシンを同じ UCS サーバに展開しないでください。代わりに、ホストの障害発生時に冗長性を提供するため、プライマリとバックアップの仮想マシンを異なるサーバに展開してください。

プラットフォーム

仮想化を使用して展開される製品には、Cisco Business Edition 7000 が最適なソリューションとして考えられます。このソリューションは、簡単に発注して展開することができ、VMware vSphere Hypervisor (ESXi) が事前にインストールされています。Business Edition 7000 には Cisco Collaboration ソフトウェア セットが事前にロードされており、また Cisco Collaboration アプリケーションの一部も事前にインストールされています。

製品リスト

改訂日：2019 年 2 月 19 日

この製品リストには、エンタープライズ コラボレーション向けプリファード アーキテクチャのシスコ製品と、推奨されるソフトウェア バージョンを記載しています。

C：表 A-1　　Enterprise Collaboration 12.x 向けプリファード アーキテクチャの製品およびソフトウェア バージョン

製品	製品の説明	推奨されるソフトウェア バージョン
Cisco Unified Communications Manager IM と Presence サービス	コール制御、インスタント メッセージ、プレゼンス サービス	12.5(1)
Cisco Unity Connection	ボイスメール サービス	12.5(1)
Cisco Expressway-C および Expressway-E	モバイルおよびリモート アクセス、企業間コミュニケーション	X12.5
Cisco Prime Collaboration Deployment	IM and Presence サービスを使用した Unified CM クラスタ、Unity Connection クラスタをインストールする	12.5(1)
Cisco Prime Collaboration Provisioning	Unified CM とその他のアプリケーションの設定、ユーザとデバイスのプロビジョニング（移動、追加、変更の処理）を行う	12.6 以降
Cisco Meeting Server	音声会議とビデオ会議およびリソースの管理	2.5 以降
Cisco ISR および ASR	PSTN ゲートウェイ、SRST、インターネットとの外部接続	IOS XE 16.10 (2)
Cisco IP Phone 8800 シリーズ	一般的なオフィス用および IP 会議用電話	12.5
Cisco Unified IP Conference Phone 8832	IP 会議用電話	12.5
Cisco Jabber	音声、ビデオ、ボイスメール、インスタント メッセージ、プレゼンス機能が統合された、モバイル デバイスおよびパーソナル コンピュータ用のソフト クライアント	Jabber 12.5
Cisco Webex DX シリーズ	デスクトップ向けパーソナル TelePresence エンドポイント	CE 9.5 以降
Cisco TelePresence MX シリーズ	多目的ルーム向け TelePresence エンドポイント	CE 9.5 以降

C：表 A-1　Enterprise Collaboration 12.x 向けプリファード アーキテクチャの製品およびソフトウェア バージョン（続き）

製品	製品の説明	推奨されるソフトウェア バージョン
Cisco TelePresence SX シリーズ	インテグレータシリーズテレプレゼンスエンドポイント	CE 9.5 以降
Cisco Webex Room シリーズ	コラボレーション統合機能および多目的ルーム エンドポイント	CE 9.5 以降
Cisco TelePresence Management Suite（TMS）	スケジューリング、Web 会議統合、およびその他の高度なビデオ機能	15.8