



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

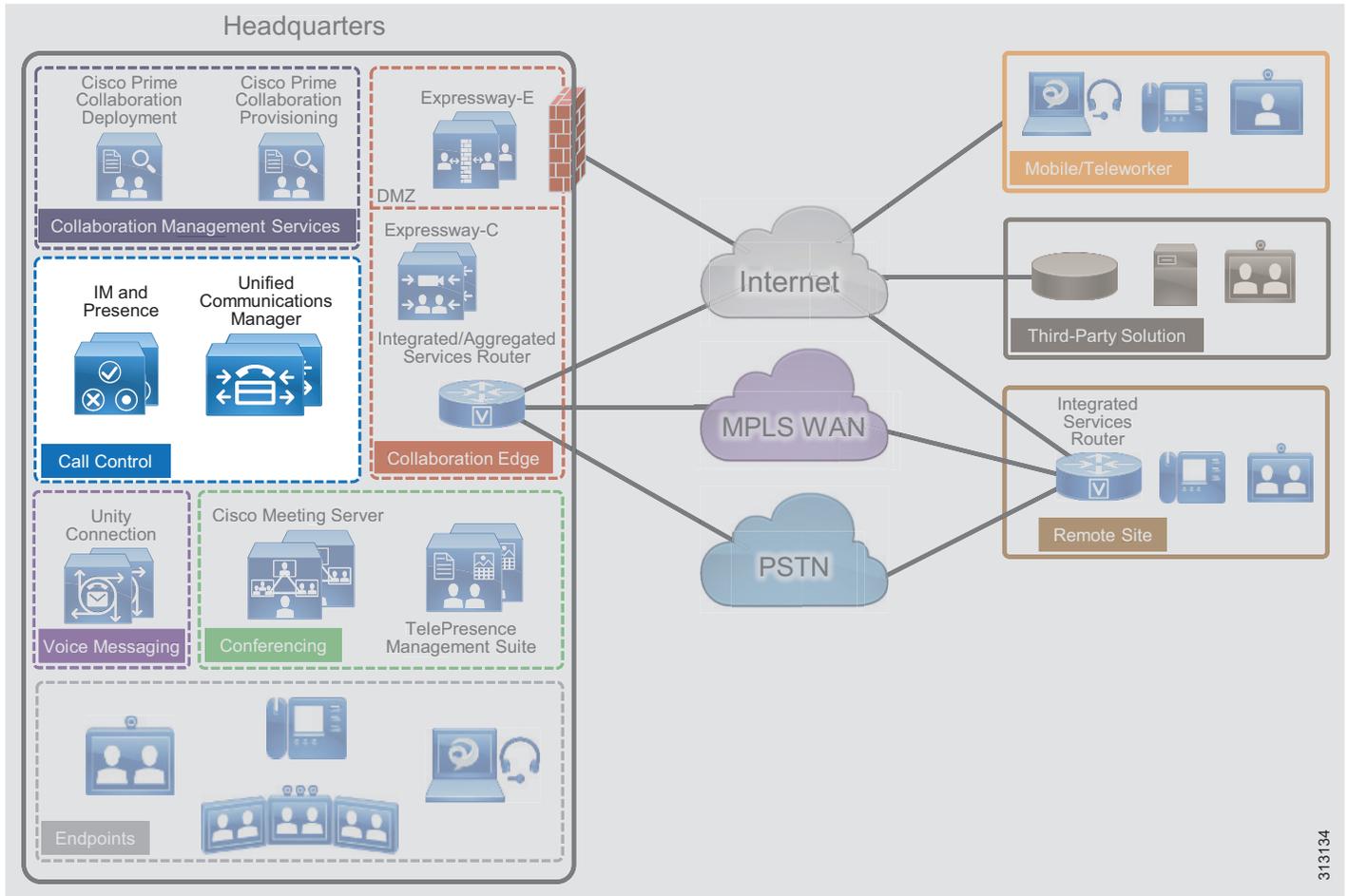
新規トピックまたは改訂されたトピック	説明箇所	改訂日
Apple Push Notification Service (APN) に関する情報を追加	アップル プッシュ ノートフィケーション サービス (APN) との統合 (C : 2-10 ページ) Apple Push Notification Service (APN) 経由のプッシュ通知のオンボーディング (C : 2-26 ページ) その他の IM とプレゼンス設定 (C : 2-27 ページ)	2017年8月30日
更新ログイン フローを使用した OAuth	その他の IM とプレゼンス設定 (C : 2-27 ページ) C :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



313134

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性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

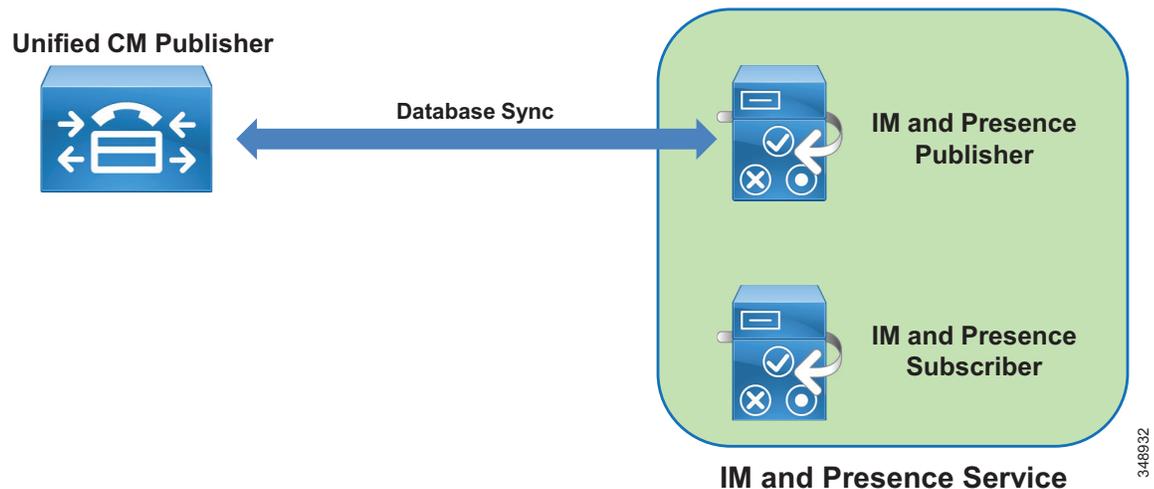
パブリッシャはすべてのクラスタの必須サーバノードです。各クラスタにパブリッシャは 1 つだけ存在できます。このサーバノードにはクラスタ設定が含まれており、クラスタ内の他のすべてのサブスクライバにデータベース サービスを提供します。この設計では Unified CM パブリッシャは専用ノードなので TFTP 要求やエンドポイントの登録、呼処理は扱いません。

- 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 サブスクリバで、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リ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リバについてバックアップ呼処理サブスクリバがあります。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 パブリッシュャは、他の IM and Presence サブスクリ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)

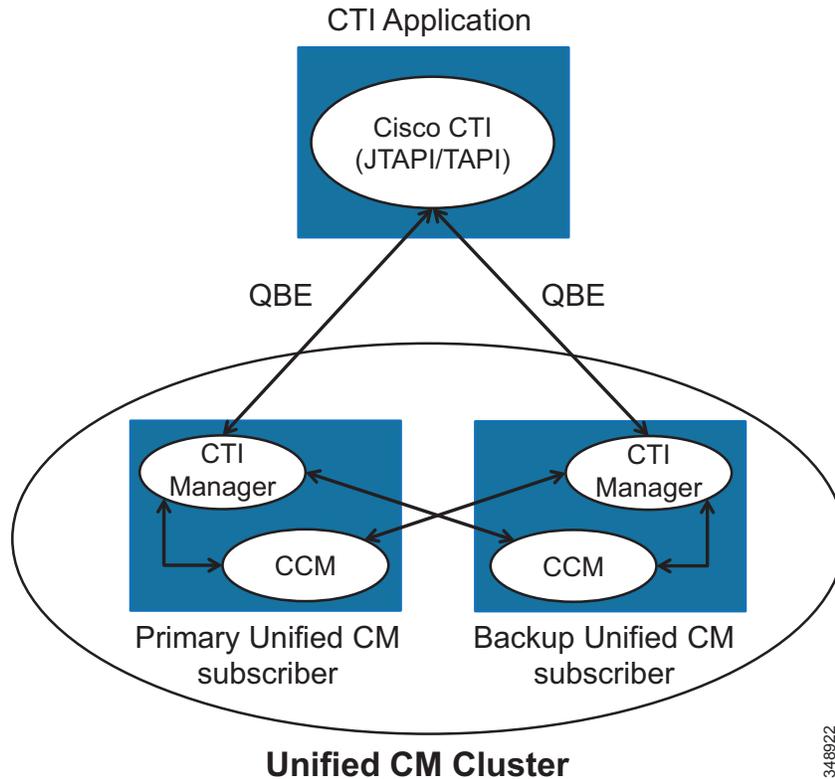
Cisco コンピュータ テレフォニー インテグレーション (CTI) を利用すると、Cisco Unified CM で使用可能な豊富なフィーチャ セットを、サードパーティ製のアプリケーションでも使用できるようになります。

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 サブスクリバ：
 - 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 サブスクリバで実行され、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 サブスクリバの 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 サブスクリバ全体に障害が発生した場合など）、バックアップ Unified CM サブスクリ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 サブスクリバ上にある 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 サブスクリバの 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 サブスクリ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 サブスクリ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 サブスクリバ）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 呼処理サブスクリバに登録される 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リ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 サブスクリ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 サブスクリバで構成されます。

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

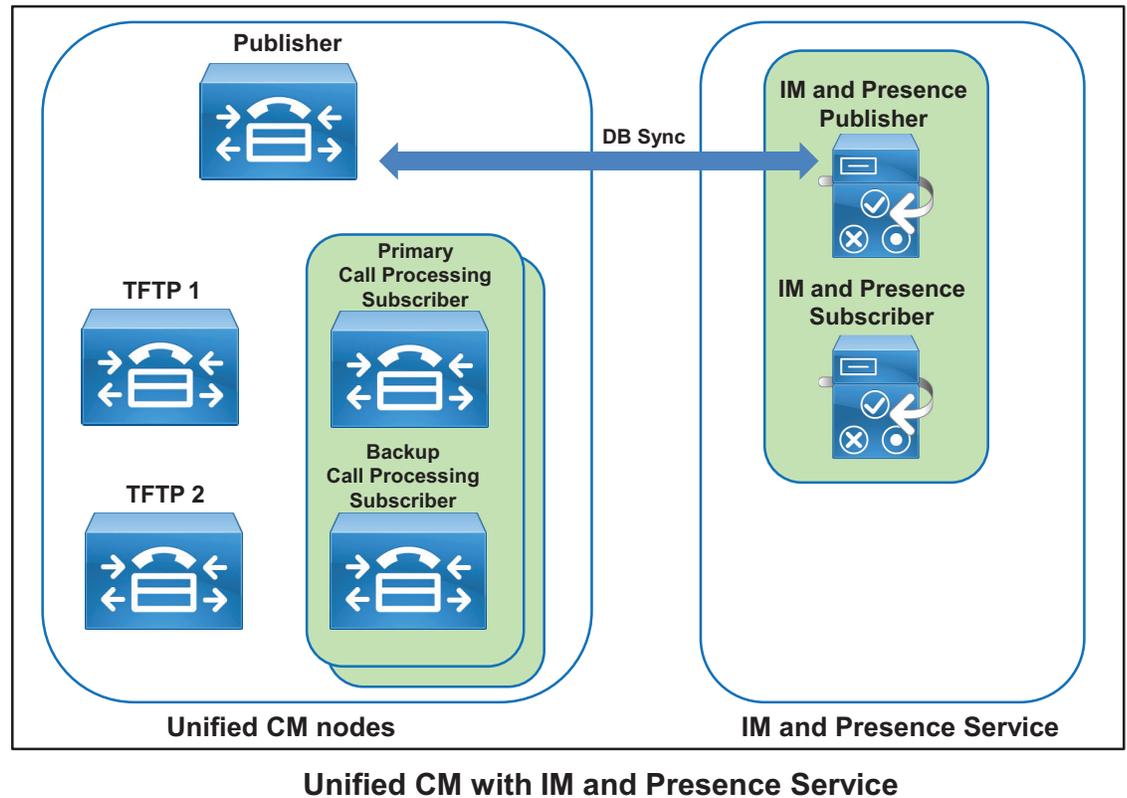
Cisco Unified CM and IM and Presence Service クラスタは次のノードで構成されます。

- 1x Cisco Unified CM パブリッシャ
- 2x (1 ペア) Cisco Unified CM TFTP サーバ サブスクリバ
- 2x (1 ペア) Cisco Unified CM 呼処理サブスクリバ (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



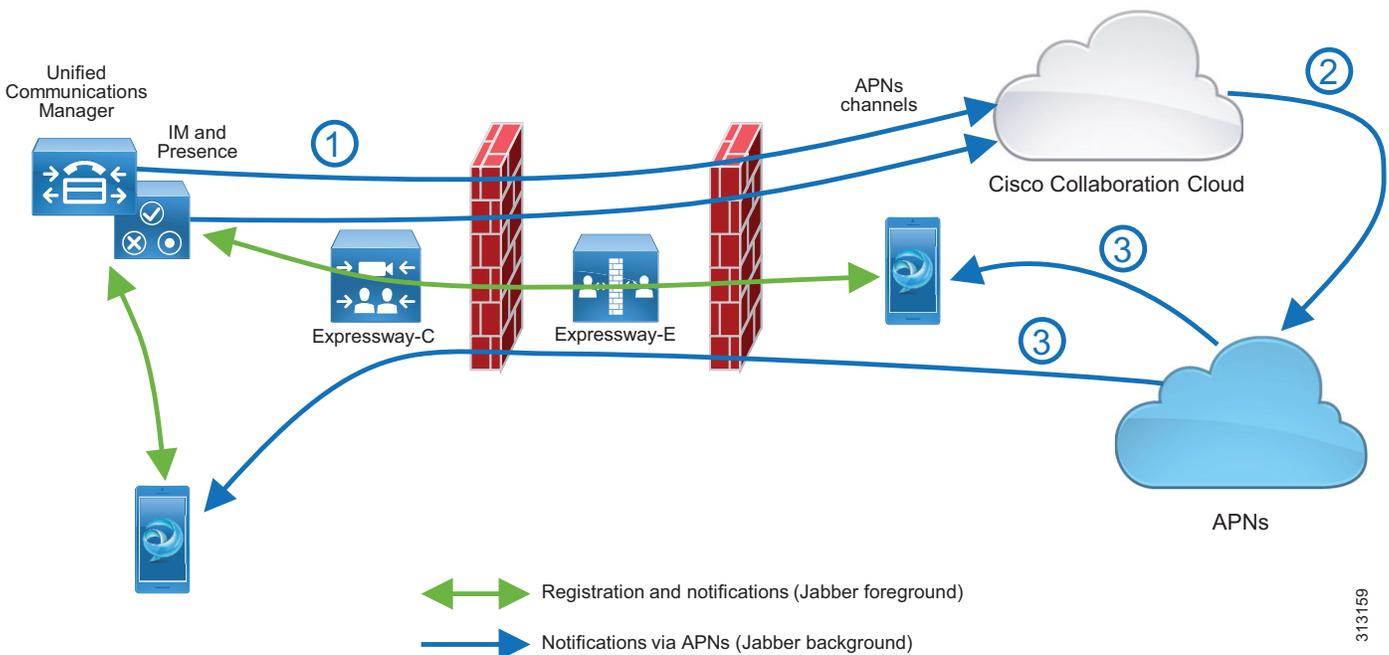
348923

アップル プッシュ ノートフィケーション 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、バッテリーの寿命が延び、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



313159

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 クラスターの 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ー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ー用のマシンアカウントが作成され、そのクラスターの OAuth 更新トークンが発行されます。この情報を使用すれば、クラスターのすべての 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 クラスターに報告された後、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 に接続する必要があります。

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

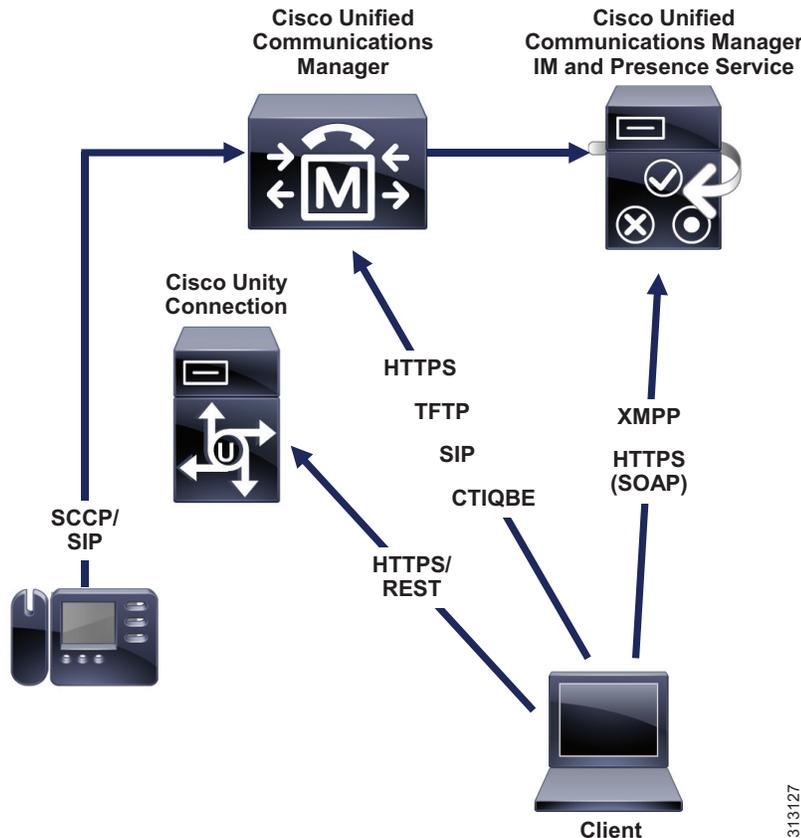
これはデフォルト モードです。ユーザのプライマリ認証は IM and Presence サーバに対して行われます。これは、このプリファード アーキテクチャ設計で使用されるモードであり、本マニュアルで取り上げられています。

- 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

マルチクラスター展開では、SIP トランクを介して個々の Unified CM クラスターすべてを相互接続します。個々のクラスター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 つ以上のクラスターでは、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。

マルチクラスター展開では、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、クラスター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ー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ー間検索サービス (ILS) を利用するので、マルチクラスター展開の場合は、すべての Unified CM クラスター間で 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ー上の 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ーを特定します。

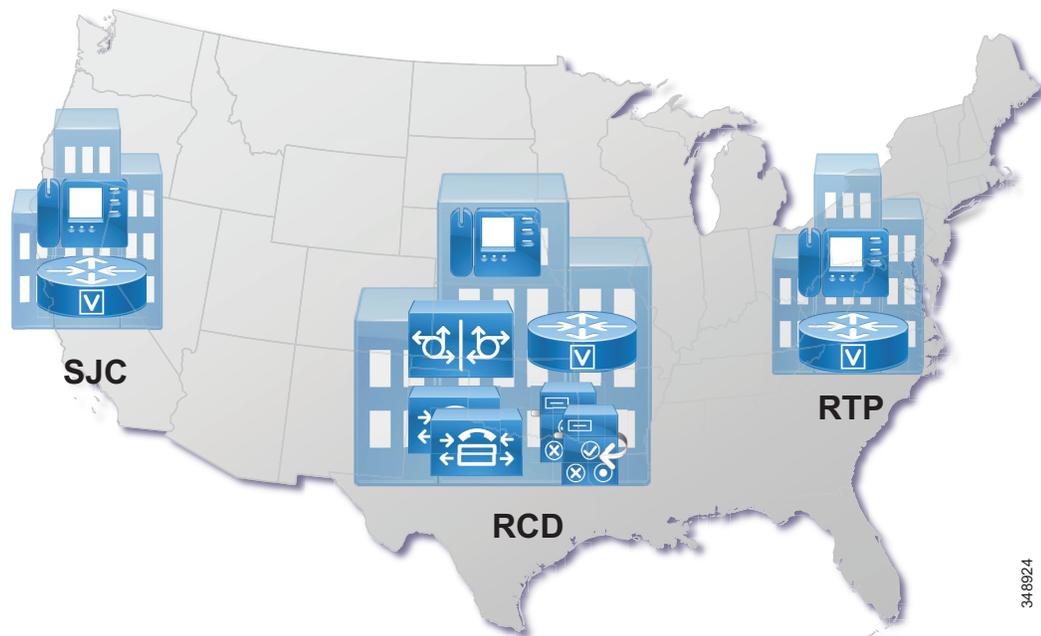
IM and Presence 機能は、単一クラスター内での通信により制限されます。プレゼンスとインスタントメッセージングの能力と機能を拡張するには、これらのスタンドアロンのクラスターにピア関係を設定することで、同じドメイン内の複数のクラスター間で通信できるようになります。この機能により、1 つのクラスター内のユーザが、同じドメイン内の異なるクラスターにいるユーザと通信したり、プレゼンスをサブスクライブしたりできます。フルメッシュのプレゼンス トポロジを作成するには、それぞれの Cisco IM and Presence クラスターと、同じドメイン内の他のそれぞれの Cisco IM and Presence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

C : 図 2-7 トポロジーの例



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ー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 を使用するという事は、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进行处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。

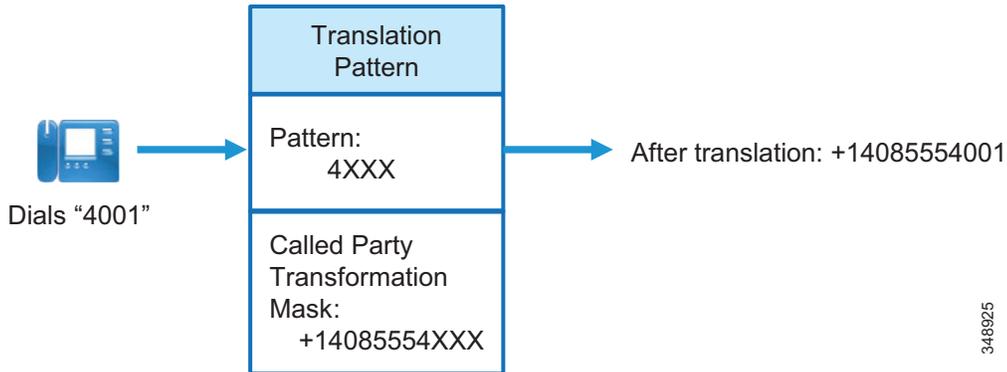
+E.164 ルーティングおよびダイヤリングの正規化

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、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ー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、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、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せん。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。各サイトのイーグレス 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となります。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ル化

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](#)
- [ビジ回線フィールド \(BLF\) 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リ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rotocol (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 パブリック 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 サブスクリバ ノード、および Unified CM 呼処理サブスクリバ 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 サブスクリバ	呼処理サブスクリバ
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 サブスクリバ	呼処理サブスクリバ
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リバ 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	サブスクリバ
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、設定済みのハンドリストの追跡を 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。
[デジタル分析の複雑性 (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ジタル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。既存のネットワーク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リバ 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。しがたって、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 ダイアルに必要な 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) 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 ダイアル手順 (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) 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 ダイアル手順を +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 の一部であると思わなければならない、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	CSS 名	パーティション
SJCNational	DN Directory URI URI ESN onNetRemote SJCIntra UStoE164 USPSTNNational USEmergency	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	CSS 名	パーティション
RTPNational	DN Directory URI URI ESN onNetRemote RTPIntra UStoE164 USPSTNNational USEmergency	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

このサブスクリプト 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 に対して最大 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 クラスとコーディング 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ります。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ない、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ない、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、簡単に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 ダイアルピアから 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 ダイアルピアに、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 ダイアル用に +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 [デバイスマビリティ関連情報 (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となります。

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あります。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 ダイア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。サイト内短縮ダイア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ア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 ダイア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通じ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せん。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)]	<pre>(& (objectclass=user) (! (objectclass=Computer)) (!(UserAccountControl:1.2.840.113556.1.4.803:=2)) (telephoneNumber=+1*))</pre>
[リモート (Remote)]	<pre>(& (objectclass=user) (! (objectclass=Computer)) (!(UserAccountControl:1.2.840.113556.1.4.803:=2)) ((telephoneNumber=+3*) (telephoneNumber=+4*)))</pre>

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	名前がローカル 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	名前がリモート 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 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 同期を定期的に行います。
[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 パブリッシュ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 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 同期を定期的に行います。
[再同期の実行間隔 (Perform a Re-sync Every)]	妥当な間隔	社内ディレクトリ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 パブリッシング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リバ 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リバ 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リバ 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リバがあり、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リバがあり、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リバとなっている 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

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、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)
- アナウンサータ
- 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リバ 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。

アナウンサータは 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 およびアナウンサータ 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ウンサータ 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 およびアナウンサー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 およびアナウンサー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 およびアナウンサー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 の呼処理サブスクリ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 の呼処理サブスクリバを決定します。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、このサブスクリ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。

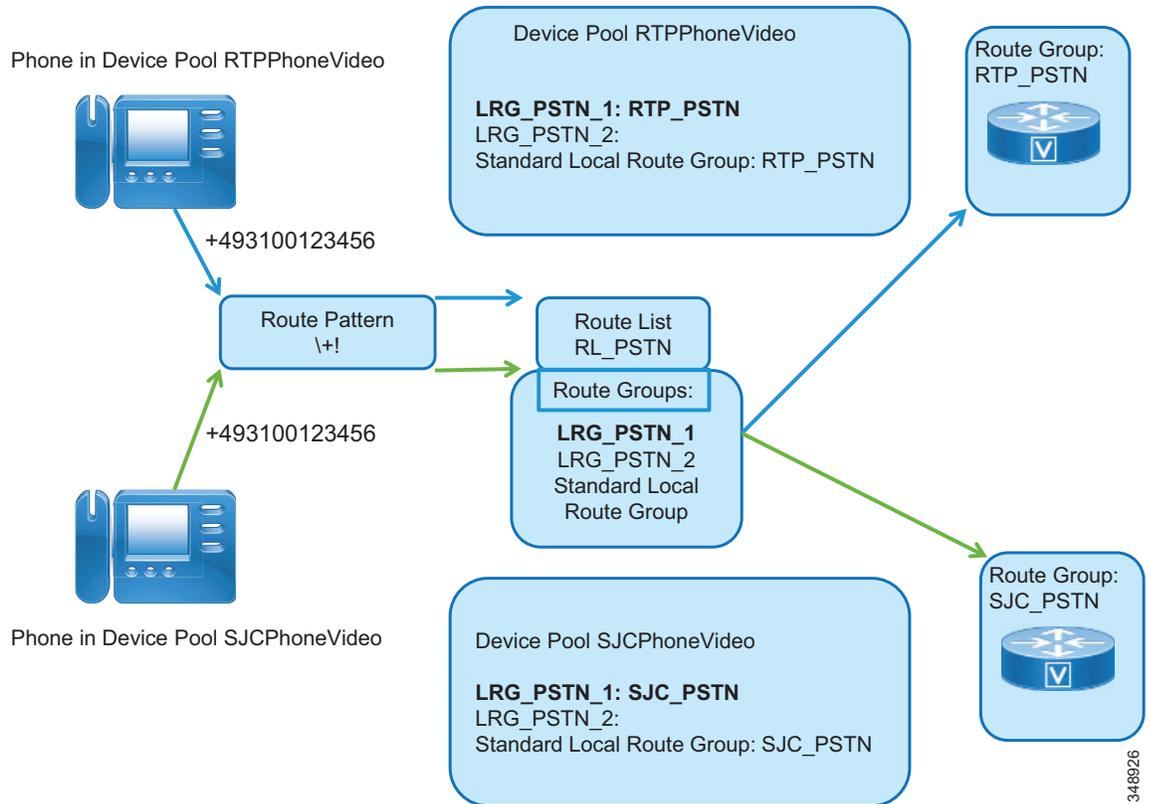
C : 表 2-51 RTP サイト内でビデオ会議機能を使用している電話のデバイス プール設定

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)。
[デバイスマビリティ関連情報 (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 ヘ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。
[デバイスマビリティ関連情報 (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も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
[デバイスマビリティ関連情報 (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 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
[デバイスポール (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 ダイアルをサポートする必要があります。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)]		
[デバイスポ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	
[デバイスポ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 (多国籍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)

設定	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 (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、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 に対する代替の 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 呼処理サブスクリ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リバに対して 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 の呼処理サブスクリ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 ダイア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

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

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

ILS クラスター検出サービスにより、マルチクラスター環境の 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 クラスター間の英数字 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 クラスターの 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 **Unified CM** クラスターに対し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 **Unified CM** クラスターに対して一意のクラスター ID を割り当てる

Unified CM クラスター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ー 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認しようとしています。
[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) に合格するだけでなく、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リバノードの 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
+1408554XXX	[+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ダプタイズされた 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ダプタイズされた 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 ダイアルピアを設定して、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 ダイア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。ダイア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

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/ EAppServlet?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ィールを関連付けます。
- 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>

ビジョー回線フィールド (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。