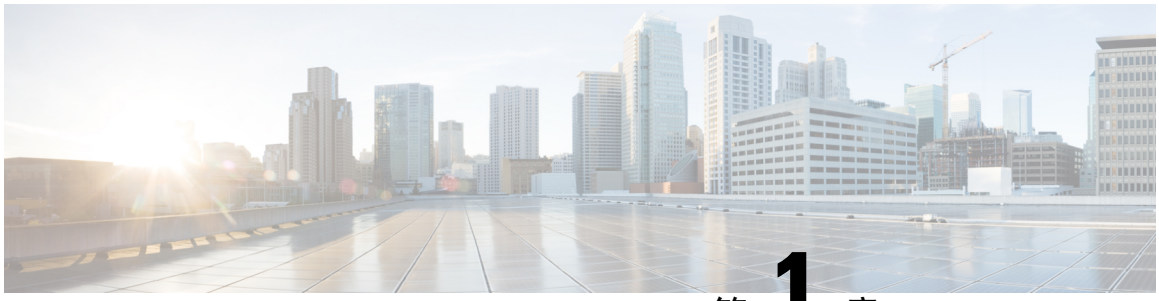
Cisco Unified Communications Manager リリース 15 システム設定ガイド

First Published: 2023-12-18

Last Modified: 2024-01-25

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



第 1 章

新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

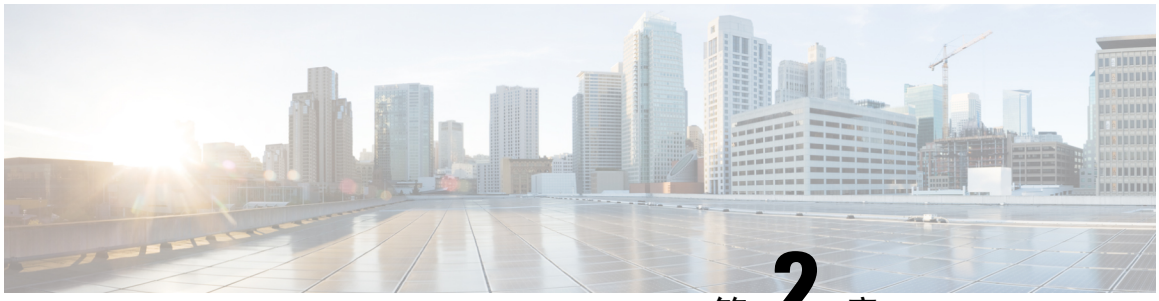
次の表は、この最新リリースまでのガイドでの機能の主な変更点の概要を示したものです。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Unified Communications Manager* と *IM and Presence* サービスの新機能と変更された動作

日付	説明	参照先
2023 年 12 月 18 日	SRTP DTMF インターワークのサポートに関する情報を提供するセクションを追加。	SRTP DTMF インターワーキング（139 ページ）
2023 年 12 月 18 日	ローカルプッシュ通知サービス（LPNS）機能に関連するポート情報を追加。	• 共通サービス ポート （466 ページ） • 電話機と Cisco Unified Communications Manager の間のシグナリング、メディア、およびその他の通信 （471 ページ）
2023 年 12 月 18 日	H.323 ゲートキーパーのサポートの削除に関する情報を追加。	H.323 トランクの概要 （106 ページ）
2023 年 12 月 18 日	Webex アプリと Cisco Jabber デバイスの自動プロビジョニングに関する情報を追加。	LDAP ディレクトリの同期の設定 （353 ページ）
2023 年 12 月 18 日	「Cisco Smart Software Manager」および「Cisco Smart Software Manager Satellite」セクションを更新して、アップグレード条件に関する注記を追加。	• スマート ソフトウェア ライセンシングの概要 （7 ページ） • 永久ライセンス予約対応システムのバージョン 15 へのアップグレード （33 ページ）

新機能および変更された機能に関する情報

日付	説明	参照先
2023 年 12 月 18 日	「SSO および OAuth 設定」セクションを更新：CUCM パブリッシャに対する更新トークンの依存関係を排除	よくある企業パラメータ （39 ページ）
2023 年 12 月 18 日	更新トークンを自動的に更新するために、サポートの「SSO および OAuth 設定」セクションを更新	よくある企業パラメータ （39 ページ）



第 2 章

はじめに

システム設定の概要

このドキュメントでは、コール制御システムのインストール後のセットアップに関する基本的な設定作業について説明します。このドキュメントでは、システムパラメータ、ダイヤルプランとコールルーティング、メディアリソースの設定、アプリケーションの統合、エンドユーザとエンドポイントのプロビジョニングを行うことができます。このドキュメントを完了する際には、設定されたダイヤルプラン、コールルーティング、メディアリソース、帯域幅管理リソース、および基本セキュリティを含む基本的な condiguration が必要です。さらに、ユーザとエンドポイントがプロビジョニングされます。

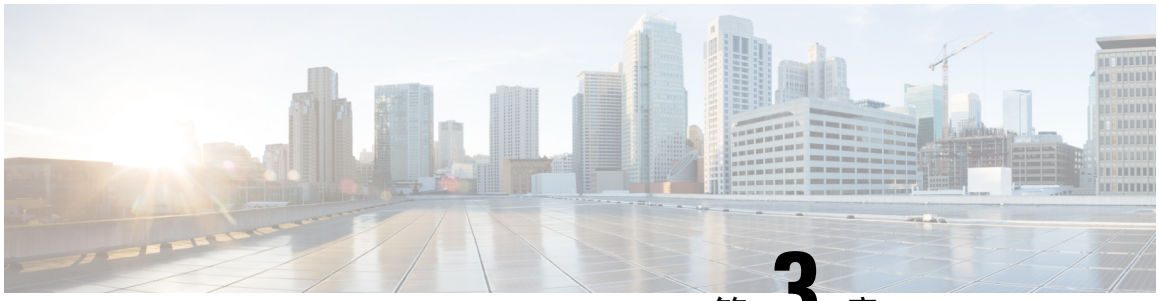
このマニュアルの構成は、次のとおりです。

- システムコンポーネント:システムライセンス、基本セキュリティ、SSO、デバイスプール、トランク、ゲートウェイ、メディアリソース、およびコールの許可制御などの項目を設定します。
- ダイヤルプラン: ダイヤルプランとコールルーティング要素を設定します。
- アプリケーションの統合: Cisco 緊急応答側、Cisco Unity Connection、Cisco Expressway などのアプリケーションを統合します。
- ユーザのプロビジョニング: システムにユーザを追加します。
- デバイスのプロビジョニング: ユーザのデバイスを登録します。

このガイドのタスクが完了すると、システムはユーザ、デバイス、基本セキュリティ、およびSSOを使用してセットアップされます。その後、シスコのソリューションの設定に進むことができます。

第 部

システム コンポーネント



第 3 章

スマート ソフトウェア ライセンシング

スマート ソフトウェア ライセンシングの概要

シスコスマートソフトウェアライセンシングは、ライセンスに関する新しい考え方を提供しています。ライセンスの柔軟性が増し、企業全体のライセンスがシンプルになります。また、ライセンスの所有権および消費が可視化されます。

Ciscoスマート ソフトウェア ライセンシングを使用すると、デバイスが自己登録し、ライセンス消費を報告し、製品アクティベーション キー（PAK）が必要なくなり、ライセンスの調達、展開、管理が簡単にできるようになります。ライセンス資格を単一のアカウントにプールして、必要に応じてネットワーク経由でライセンスを自由に移動することができます。Cisco製品全体で有効化され、直接クラウドベースまたは間接導入モデルによって管理されます。

Cisco スマート ソフトウェア ライセンシング サービスでは、製品インスタンスを登録し、ライセンスの使用状況を報告し、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから必要な認証を取得します。

スマート ライセンシングでは次のことを実行できます。

- ライセンスの使用状況とライセンス数の表示
- 各ライセンス タイプのステータスの表示
- Cisco Smart Software Manager または Cisco Smart Software Manager サテライトによる利用可能な製品ライセンスの表示

- Cisco Smart Software Manager または Cisco Smart Software Manager サテライトによるライセンス認証の更新
- ライセンス登録の更新
- Cisco Smart Software Manager または Cisco Smart Software Manager サテライトによる登録解除

（注） ライセンス承認は、30 日間に少なくとも 1 回更新することで 90 日間有効になります。Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに接続しないと、90 日後に承認の期限が切れます。

Cisco Smart Software Manager サテライトのオプションを選択する場合、このサテライトが認証を行うために、Cisco Smart Software Manager へのインターネット接続が必要になります。Cisco Smart Software Manager サテライトは、接続時間が設定可能な接続済みモードと、手動同期が必要な切断モードの 2 つのモードで動作できます。

スマート ライセンシングの導入オプションには、主に次の 2 つがあります。

- Cisco Smart Software Manager
- Cisco Smart Software Manager サテライト

Cisco Smart Software Manager

Cisco Smart Software Manager は、システムのライセンスを処理するクラウドベースのサービスです。Unified Communications Manager が直接またはプロキシ サーバ経由で、cisco.com に接続できる場合に、このオプションを使用します。Cisco Smart Software Manager によって、次のことを行うことができます。

- ライセンスの管理およびトラック
- バーチャル アカウント間でのライセンスの移動
- 登録済みの製品インスタンスの削除

オプションで、Unified Communications Manager が直接 Cisco Smart Software Manager に接続できない場合、接続を管理するプロキシ サーバを導入することができます。

（注） Cisco Smart Software Manager に登録されている Unified Communications Manager を 15 より前のリリースからリリース 15 以降にアップグレードする場合、Cisco Unified Communications Manager は、製品インスタンスの Cisco Smart Software Manager UI で製品バージョンを 15 に更新しません。詳細については、CSCwf94088 を参照してください。

Cisco Smart Software Manager の詳細については、https://software.cisco.com に進みます。

Cisco Smart Software Manager サテライト

Cisco Smart Software Manager サテライトは、セキュリティ上または可用性上の理由で、Unified Communications Manager が直接 cisco.com に接続できない場合に、ライセンスのニーズを処理できるオンプレミス導入です。このオプションを導入すると、Unified Communications Manager は、ライセンスの使用を登録し、サテライトに報告します。この際、cisco.com でホストされているバックエンドの Cisco Smart Software Managerとそのデータベースを定期的に同期します。

サテライトが cisco.com に直接接続できるかどうかに応じて、Cisco Smart Software Manager サテライトを接続または切断のいずれかのモードで導入できます。

- 接続（Connected）：Smart Software Manager サテライトから cisco.com への直接の接続がある場合に使用されます。スマート アカウントの同期が自動的に実行されます。
- 切断（Disconnected）：Smart Software Manager サテライトから cisco.com への接続がない場合に使用されます。Smart Account の同期を手動でアップロードおよびダウンロードする必要があります。

（注） デュアルスタックモードで実行される Unified CM は、IPv4 アドレスと IPv6 アドレスを使用して構成されたサテライトをサポートします。

（注） Cisco Smart Software Manager Satellite に登録されている Unified Communications Manager を 15 より前のリリースからリリース 15 以降にアップグレードする場合、Cisco Unified Communications Manager は、製品インスタンスの Cisco Smart Software Manager UI で製品バージョンを 15 に更新しません。詳細については、CSCwf94088 を参照してください。

Cisco Smart Software Manager サテライトの情報およびドキュメントについては、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html に進みます。

ライセンスタイプ

ニーズをカバーするために、次のライセンスタイプを使用できます。

Cisco Unified Workspace Licensing

Cisco Unified Workspace Licensing（UWL）は、シスコ コラボレーション アプリケーションおよびサービスの最も一般的なバンドルをコスト効率の高いシンプルなパッケージで提供します。このパッケージには、ソフト クライアント、アプリケーション サーバ ソフトウェア、およびユーザごとのライセンスが含まれています。

Cisco User Connect Licensing

User Connect Licensing（UCL）は、個々の Cisco Unified Communications アプリケーションに対するユーザベースのライセンスで、アプリケーション サーバ ソフトウェア、ユーザ ライセンス、ソフトクライアントが含まれています。UCLは、必要なデバイスのタイプとデバイ

スの数に応じて、Essential、Basic、Enhanced、Enhanced Plus の各バージョンから選択できます。

これらのライセンス タイプと使用可能なバージョンの詳細については、http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html を参照してください。

Session Management Edition

Session Management Edition は、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトのいずれかに登録できます。Session Management Edition の登録には、Unified Communications Manager と同じプロセスを使用できます。Cisco Unified Communications Manager が登録されているバーチャルアカウントまたは別のバーチャルアカウントに登録し、最小のライセンス要件を満たします。

（注） 特定ライセンス予約（SLR）に登録された SME では、SLR 承認コードの生成時に最小セットのライセンスが CSSM に予約されている必要があります。

製品インスタンスの評価モード

Unified Communications Manager は、インストール後 90 日間は評価期間として実行されます。評価期間が終了すると、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されるまで、Unified Communications Manager で新規ユーザや新規端末の追加ができなくなります。

（注） 製品が登録されると評価期間は終了します。

（注） 90 日の評価期間を使用して実行している間、セキュア SIP トランクを導入することはできません。セキュア SIP トランクを導入するには、製品登録トークンで [エクスポート管理された機能を許可（Allow export-controlled functionality）] を選択した Smart Software Manager アカウントにシステムを登録してある必要があり ます。

システム ライセンスの前提条件

システムのライセンスプランの策定

Unified Communications（UC）のライセンス構造を確認し、把握します。詳細については、http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html を参照してください。

Unified Communications Manager を Smart Software Manager サービスに接続する方法を計画します。

- cisco.com の Cisco Smart Software Manager への直接接続：Unified Communications Manager は、cisco.com の Cisco Smart Software Manager に直接接続します。このオプションでは、`tools.cisco.com` を解決するように Unified Communications Manager で DNS を設定する必要があります。
- プロキシ サーバ経由で Smart Software Manager への接続：Unified Communications Manager はプロキシ サーバまたはトランスポート ゲートウェイに接続し、そこから cisco.com の Cisco Smart Software Manager サービスに接続します。Unified Communications Manager では DNS は必要ありませんが、プロキシ サーバで `tools.cisco.com` を解決できるように DNS を設定する必要があります。
- オンプレミスの Cisco Smart Software Manager サテライトへの接続：Unified Communications Manager は、オンプレミスの Smart Software Manager サテライトに接続します。Unified Communications Manager では DNS は必要ありません。接続モードを展開する場合は、サテライトサーバ上に `tools.cisco.com` を解決できる DNS が必要です。非接続モード展開の場合は、サテライトサーバで DNS を使用する必要はありません。

スマートライセンスの登録

スマートアカウントおよびバーチャル アカウントを設定します。詳細については、https://software.cisco.com/ を参照してください。

（オプション）Cisco Smart Software Manager サテライトを導入する場合は、サテライトをインストールしてセットアップします。『*Smart Software Manager* サテライト設置ガイド』などのドキュメントを参照してください。ドキュメントは https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html で入手できます。

スマート ソフトウェア ライセンシングのタスクフロー

このタスクを完了して、Unified Communication Manager のシステムライセンスを設定します。

手順

	コマンドまたはアクション	目的
Step 1	製品インスタンスの登録トークンの取得（12 ページ）。	仮想アカウントでの製品インスタンス登録トークンの生成は、この手順を使用します。
Step 2	スマート ソフトウェア ライセンシング への接続の設定（13 ページ）	Unified Communcations Manager がスマート ソフトウェア ライセンシング サービスに接続するトランスポート設定を選択します。デフォルトでは [直接（Direct）] オプションが選択されており、製品がシスコ ライセンシング サーバに直接接続します。

	コマンドまたはアクション	目的
Step 3	Cisco Smart Software Manager への登録（14 ページ）。	次の手順を実行して、Unified Communications Manager を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録します。

製品インスタンスの登録トークンの取得

始める前に

製品インスタンスを登録するには、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから製品インスタンス登録トークンを取得します。トークンは、エクスポート管理された機能が有効か無効かに関係なく生成できます。

手順

Step 1 Cisco Smart Software Manager または Cisco Smart Software Manager サテライトのいずれかでスマート アカウントにログインします。

Step 2 Unified Communications Manager クラスタを関連付けるバーチャル アカウントに移動します。

Step 3 「製品インスタンス登録トークン」を生成します。

（注） [このトークンで登録されている製品でエクスポート管理された機能を許可（Allow export-controlled functionality on the products registered with this token）] チェックボックスを選択して、このスマート アカウントで使用する製品インスタンスのトークンに対して、エクスポート管理された機能を有効にします。このチェックボックスをオンにして条件に同意して、この登録トークンに登録されている製品の高度な暗号化を有効にします。デフォルトでは、このチェックボックスはオンです。エクスポート管理された機能をこのトークンで使用できなくするには、このチェックボックスをオフにします。

注意 このオプションは、エクスポート管理された機能を準拠している場合のみ使用します。

（注） [このトークンで登録されている製品でエクスポート管理された機能を許可（Allow export-controlled functionality on the products registered with this token）] チェックボックスは、エクスポート管理された機能の使用が許可されていないスマート アカウントでは表示されません。

Step 4 トークンをコピーするか、別の場所に保存します。

詳細については、https://software.cisco.com/ を参照してください。

スマート ソフトウェア ライセンシング への接続の設定

この作業を完了して、Smart Software Licensing サービスに Unified Communications Manager を接続します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [ライセンス（Licensing）] > [ライセンス管理（License Management）]** を選択します。
[ライセンス管理（LicenseManagement）] ウィンドウが表示されます。

Step 2 [スマートソフトウェアライセンシング（Smart Software Licensing）] セクションから、[ライセンスSmart Call Home設定の表示/編集（View/Edit the Licensing Smart Call Home settings）] リンクをクリックします。
[転送設定（Transport Settings）] ダイアログ ボックスが表示されます。

Step 3 Smart Licensing サービスに Unified Communications Manager を接続する方法を選択します。

- [直接（Direct）]：Unified Communications Manager が cisco.com の Smart Software Manager に直接接続します。これがデフォルトのオプションです。このオプションでは、`tools.cisco.com` を解決できる Unified Communications Manager で DNS を導入する必要があります。
- [トランスポートゲートウェイ（Transport Gateway）]：Unified Communications Manager がオンプレミスの Cisco Smart Software Manager サテライトまたはシステム ラインセンシング用のトランスポート ゲートウェイに接続します。[URL] テキスト ボックスに、Smart Software Manager サテライトまたはトランスポート ゲートウェイのアドレスとポートを入力します。`fqdn_of_smart_software_manager:port_number` が一例になります。HTTPS の場合は、port 443 を使用します。
- [HTTP/HTTPSプロキシ（HTTP/HTTPS Proxy）]：Unified Communications Manager はプロキシ サーバに接続します。プロキシ サーバは、Cisco Smart Software Manager サービスと併せて、cisco.com のサテライトおよびトランスポート ゲートウェイと接続します。プロキシ サーバの IP アドレス、ホスト名、およびポートを入力します。
  - HTTP または HTTPS プロキシで必要な認証: 認証ベースのプロキシサーバを使用して Cisco Smart Software Manager に登録する場合は、このチェックボックスをオンにします。
  - IPアドレス/ホスト名
  - [ポート（Port）]：HTTPS の場合、port 443 を使用します。
  - [ユーザ名（User Name）]
  - [パスワード（Password）]

Step 4 Unified Communications Manager が IP アドレスとホスト名を共有しないように制限するには、スマートライセンシング登録中に [自分のホスト名またはIPアドレスをシスコと共有しません（Do not share my hostname or IP address with Cisco）] チェックボックスをオンにします。

Step 5 [保存（Save）] をクリックします。

Cisco Smart Software Manager への登録

製品を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録するには、この手順を使用します。登録するまで、製品は評価モードになっています。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [ライセンス（Licensing）] > [ライセンス管理（License Management）]** を選択します。
[ライセンス管理（LicenseManagement）] ウィンドウが表示されます。

Step 2 [スマートソフトウェアライセンシング（Smart Software Licensing）]セクションで、[登録（Register）] ボタンをクリックします。
[登録（Registration）] ウィンドウが表示されます。

Step 3 [製品インスタンス登録トークン（Product Instance Registration Token）]セクションで、Smart Software Manager または Smart Software Manager サテライトを使用して生成し、コピーまたは保存した「登録トークン キー」を貼り付けます。

Step 4 [登録（Register）] をクリックして、登録プロセスを完了します。

Step 5 [閉じる（Close）]をクリックします。詳細については、オンライン ヘルプを参照してください。

Step 6 [ライセンスの使用状況レポート（License Usage Report）] セクションで、[使用状況の詳細の更新（Update Usage Details）] をクリックして、システムのライセンスの使用状況の情報を手動で更新します。

（注） 使用状況の情報は、24 時間ごとに自動的に更新されます。詳細については、オンライン ヘルプを参照してください。

スマート ソフトウェア ライセンシングでの追加タスク

Unified Communications Manager とスマート ソフトウェア ライセンシングでは、次のオプションのタスクを実行できます。

手順

	コマンドまたはアクション	目的
Step 1	認証を更新 （16 ページ）	ライセンスタイプの下に表示されるすべてのライセンスのライセンス認証ステータス

	コマンドまたはアクション	目的
		を手動で更新するにはこの手順を実行します。 （注） ライセンス認証は30日ごとに自動的に更新されます。Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに接続しないと、認証ステータスの期限は90日後に切れます。 Cisco Smart Software Manager サテライトのオプションを選択する場合、このサテライトが認証を行うために、Cisco Smart Software Manager へのインターネット接続が必要になります。Cisco Smart Software Manager サテライトは、接続時間が設定可能な接続済みモードと、手動同期が必要な切断モードの 2 つのモードで動作できます。
Step 2	登録の更新 （17 ページ）	登録情報を手動で更新するには、以下手順を実行します。 （注） 初回登録の有効期間は 1 年です。登録の更新は、製品を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに接続すると、6か月ごとに自動的に行われます。
Step 3	登録解除 （18 ページ）	Cisco Smart Software Manager または Smart Software Manager サテライトから Unified Communications Manager クラスタを切断するには、このタスクを実行します。製品は、評価期間の終了まで評価モードに戻ります。製品で使用されているすべてのライセンス権限は、バーチャル アカウントにすぐにリリースされ、他の製品インスタンスで使用できるようになります。

	コマンドまたはアクション	目的
Step 4	Cisco Smart Software Manager でのライセンスの再登録 （19 ページ）	Unified Communications Manager を Cisco Smart Software Manager またはCisco Smart Software Manager サテライトに再登録するには、このタスクを実行します。 （注） 新しいバーチャル アカウントのトークンを使用して再登録すると、製品が異なるバーチャル アカウントに移行される場合があります。

認証を更新

この手順を使用すると、ライセンスタイプの下に表示されるすべてのライセンスのライセンス認証ステータスを手動で更新できます。

（注） ライセンス認証は 30 日ごとに自動的に更新されます。Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに接続しないと、認証ステータスの期限は 90 日後に切れます。

Cisco Smart Software Manager サテライトのオプションを選択する場合、このサテライトが認証を行うために、Cisco Smart Software Manager へのインターネット接続が必要になります。Cisco Smart Software Manager サテライトは、接続時間が設定可能な接続済みモードと、手動同期が必要な切断モードの 2 つのモードで動作できます。

始める前に

製品は Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録する必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [ライセンス（Licensing）] > [ライセンス管理（License Management）]** を選択します。
[ライセンス管理（LicenseManagement）] ウィンドウが表示されます。

Step 2 [スマートソフトウェアライセンシング（Smart Software Licensing）] セクションで、[アクション（Actions）] ドロップダウンリストをクリックします。

Step 3 [認証を今すぐ更新（Renew Authorization Now）] を選択します。
[認証の更新（Renew Authorization）] ウィンドウが表示されます。

Step 4 [OK] をクリックします。

Unified Communications Manager は、「ライセンス承認ステータス」を確認するために Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに要求を送信し、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトが Unified Communications Manager にステータスを返します。詳細については、オンライン ヘルプを参照してください。

Step 5 [ライセンスの使用状況レポート（License Usage Report）] セクションで、[使用状況の詳細の更新（Update Usage Details）] をクリックして、システムのライセンスの使用状況の情報を手動で更新します。

（注） 使用状況の情報は、24 時間ごとに自動的に更新されます。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

登録の更新

製品を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録する間、製品の識別にはセキュリティ アソシエーションが使用され、登録証明によってアンカーが設定されます。この有効期限（登録期間）は 1 年間です。これは登録トークン ID の有効期限とは異なり、トークンの時間制限が有効になります。この登録期間は6か月ごとに自動的に更新されます。ただし、問題がある場合は、この登録期間を手動で更新できます。

始める前に

製品は Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録する必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [ライセンス（Licensing）] > [ライセンス管理（License Management）]** を選択します。
[ライセンス管理（LicenseManagement）] ウィンドウが表示されます。

Step 2 [スマートソフトウェアライセンシング（Smart Software Licensing）] セクションで、[アクション（Actions）] ドロップダウンリストをクリックします。

Step 3 [登録を今すぐ更新（Renew Registration Now）] を選択します。
[登録の更新（Renew Registration）] ウィンドウが表示されます。

Step 4 [OK] をクリックします。

Unified Communications Manager は、「登録ステータス」 を確認するために Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに要求を送信し、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトが Unified Communications Manager にステータスを返します。

Step 5 [ライセンスの使用状況レポート（License Usage Report）] セクションで、[使用状況の詳細の更新（Update Usage Details）] をクリックして、システムのライセンスの使用状況の情報を手動で更新します。

（注） 使用状況の情報は、24 時間ごとに自動的に更新されます。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

登録解除

この手順を使用すると、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから登録を解除して、現在のバーチャル アカウントからすべてのライセンスをリリースします。この手順を実行すると、Unified Communications Manager クラスタが Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから切断されます。製品で使用されているすべてのライセンス権限は、バーチャル アカウントにリリースされ、他の製品インスタンスで使用できるようになります。

（注） Unified Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに接続できず、製品がまだ登録されていない場合は、警告メッセージが表示されます。このメッセージでは、製品を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから手動で削除してライセンスを解放する通知が表示されています。

始める前に

製品は Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録する必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [ライセンス（Licensing）] > [ライセンス管理（License Management）]** を選択します。
[ライセンス管理（LicenseManagement）] ウィンドウが表示されます。

Step 2 [スマートソフトウェアライセンシング（Smart Software Licensing）] セクションで、[アクション（Actions）] ドロップダウンリストをクリックします。

Step 3 [登録解除（Deregister）] を選択します。
登録解除 ウィンドウが表示されます。

Step 4 [OK] をクリックします。

Step 5 [ライセンスの使用状況レポート（License Usage Report）] セクションで、[使用状況の詳細の更新（Update Usage Details）] をクリックして、システムのライセンスの使用状況の情報を手動で更新します。

（注） 使用状況の情報は、24 時間ごとに自動的に更新されます。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

（注）
- Cisco Smart Software Manager または Cisco Smart Software Manager サテライトへの登録後にデータ プレーン暗号化（混合モードの Unified Communications Manager クラスタ）が有効化され、製品が後で登録解除された場合、混合モードでは引き続き有効となります。

  Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから製品が登録解除されると、SmartLicenseExportControlNotAllowedという名前の警告が管理者に送信され、クラスタが非セキュアモードに設定されます。混在モードは、再起動後も引き続き有効となります。

- この登録解除後の動作は、製品の将来のバージョンでは変更される可能性があります。CTL クライアントのセットアップに関する詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-maintenance-guides-list.html にある「『Cisco Unified Communications Manager セキュリティガイド』」の「*Cisco CTL* クライアントの設定」の章を参照してください。

  トークンレス CTL の混合モードに関する詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-tech-notes-list.html にある「「Tokenless CTL との CUCM 混合モード」」セクションを参照してください。

Cisco Smart Software Manager でのライセンスの再登録

この手順を使用すると、Cisco Unified Communications Manager を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに再登録できます。

始める前に

製品インスタンスの登録トークンの取得 （12 ページ）。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [ライセンス（Licensing）] > [ライセンス管理（License Management）]** を選択します。
[ライセンス管理（LicenseManagement）] ウィンドウが表示されます。

Step 2 [スマートソフトウェアライセンシング（Smart Software Licensing）] セクションで、[登録（Register）] ボタンをクリックします。
[登録（Registration）] ウィンドウが表示されます。

Step 3 [スマートソフトウェアライセンシング（Smart Software Licensing）] セクションで、[アクション（Actions）] ドロップダウンリストをクリックします。

Step 4 [登録（Reregister）] を選択します。
[登録（Reregister）] ウィンドウが表示されます。

Step 5 [OK] をクリックします。

Step 6 [製品インスタンス登録トークン（Product Instance Registration Token）] セクションで、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトを使用して生成し、コピーまたは保存した「登録トークン キー」を貼り付けます。

Step 7 [登録（Register）] をクリックして、登録プロセスを完了します。

Step 8 [閉じる（Close）] をクリックします。詳細については、オンラインヘルプを参照してください。

Step 9 [ライセンスの使用状況レポート（License Usage Report）] セクションで、[使用状況の詳細の更新（Update Usage Details）] をクリックして、システムのライセンスの使用状況の情報を手動で更新します。

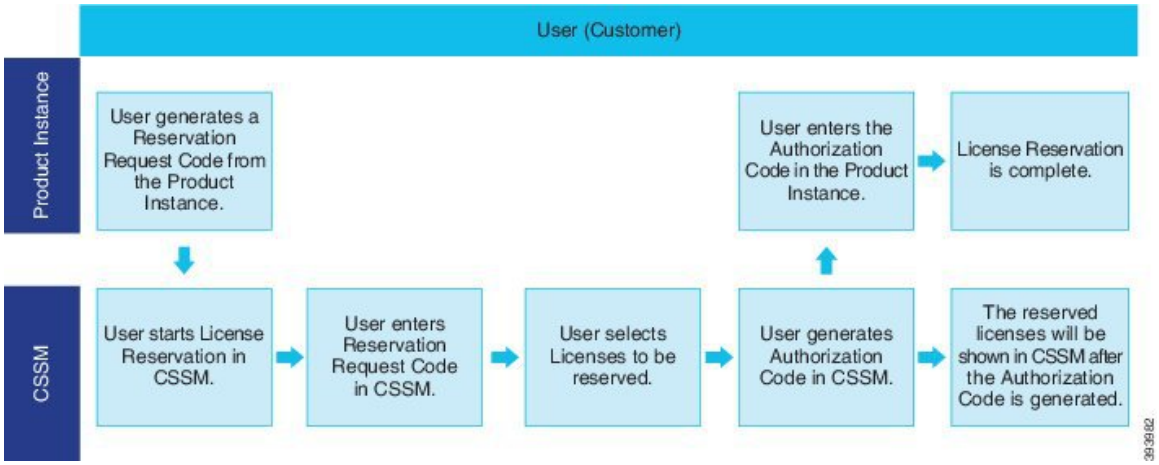
（注） 使用状況の情報は、24 時間ごとに自動的に更新されます。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

特定ライセンス予約

特定ライセンス予約は、非常にセキュリティの高いネットワークで使用される機能です。特定ライセンス予約は、使用情報を通信せずに、デバイス（製品インスタンス、Unified Communications Manager）にソフトウェアライセンスを展開する方法を提供します。

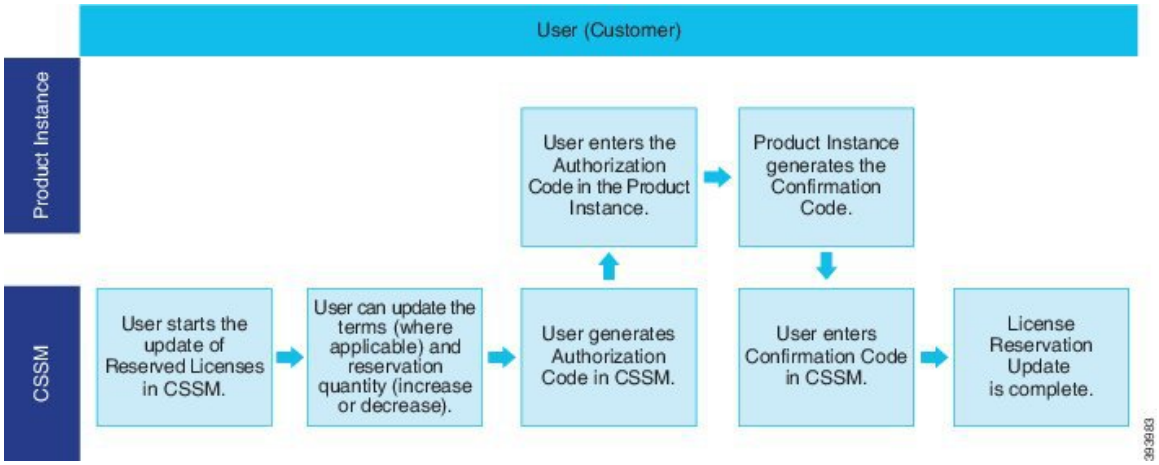
Unified Communications Manager 製品では、永久ライセンスまたは期間ベースのライセンスを指定して予約することができます。認証コードが交換された後は、予約に変更があるまで定期的な製品の同期は必要ありません。予約済みライセンスは、リターンコードを使用して製品からリリースされてない限り、Cisco Smart Software Manager でブロックされたままになります。

図 *1:* ライセンスの予約



予約済みライセンスの更新または変更 (増減) は、Cisco Smart Software Manager で以前に予約されたライセンスに実行できます。新しい認証コードの製品へのインストールおよび確認コードの取得が可能です。製品からの確認コードが Cisco Smart Software Manager にインストールされていない限り、新しい変更は送信中の状態のままになります。

図 *2:* ライセンス予約のアップデート

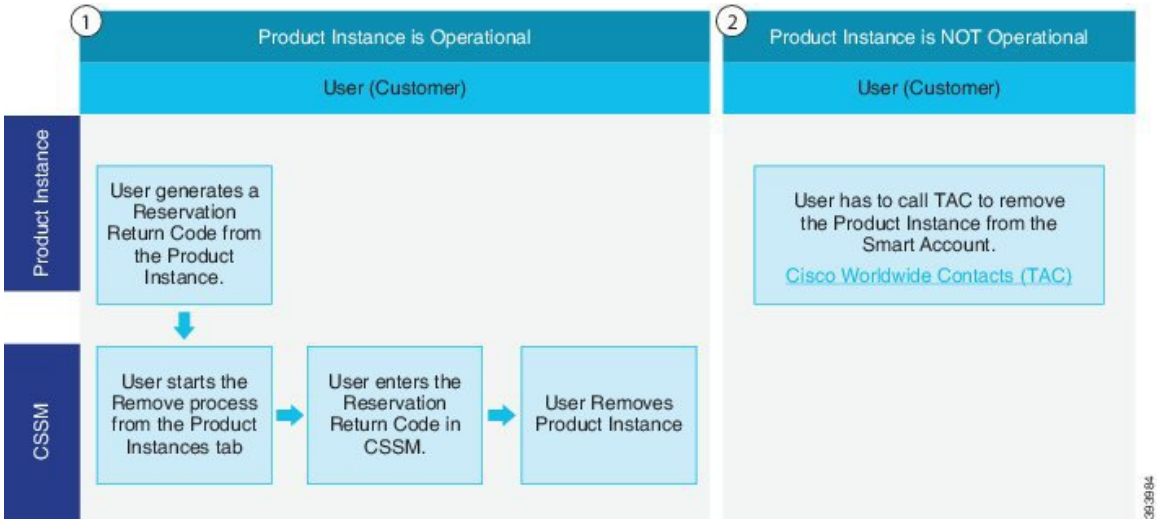


ライセンスが製品インスタンス（Unified Communications Manager）で予約されている場合、スマートアカウントから製品インスタンスを削除して、スマートアカウントからその製品インスタンス（Unified Communications Manager）に予約されているすべてのライセンスをすべてリリースするには、2 つの方法があります。

製品インスタンスは動作可能 (グレースフル削除): 製品インスタンスで（認証コードの削除）予約戻りコードを作成して、特定のライセンス予約認証をリリースすることができます。その後、CiscoSmart Software Manager に予約戻りコードを入力します。

製品インスタンスは動作不可能 (失敗または RMA による場合、または VM またはコンテナを破棄する場合): ユーザは TAC に連絡する必要があります。スマートアカウントからの製品インスタンスの削除は、TACが行います。

図 *3 :* 製品インスタンスの削除*: Unified Communications Manager*



（注） ユーザが特定のライセンス予約を有効にするには、CLI 設定のみが使用可能です。

（注） 特定ライセンス予約が Unified Communications Manager で有効化されている場合、クラウド オンボーディング用のバウチャー生成はサポートされません。

スマートアカウントでライセンス予約機能を使用できるお客様は、自身のバーチャルアカウントからライセンスを予約し、そのライセンスをデバイス UDI に関連付けて、接続していない状態で予約済みライセンスを使用してデバイスを使用することができます。この場合、バーチャル アカウントから UDI 用の特定ライセンスと数量を予約します。以下のオプションは、特定のライセンス予約向けの新機能および設計要素の説明です。

- license smart reservation enable
- license smart reservation disable
- license smart reservation request
- license smart reservation cancel
- update license reservation
- license smart reservation install "<authorization-code>"
- license smart reservation install-file <url>
- license smart reservation return
- license smart reservation return-authorization "<authorization-code>"

特定ライセンス予約のタスクフロー

これらのタスクを完了して、Unified Communications Manager の特定のライセンスを予約します。

license smart reservation enable

特定のライセンスの予約を有効化するには、この手順を使用します。

始める前に

Unified Communications Manager が Cisco Smart Software Manager またはサテライトから登録解除されます。

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart reservation enable

license smart reservation request

Unified Communications Manager 製品から予約要求コードを生成するには、次の手順を実行します。

始める前に

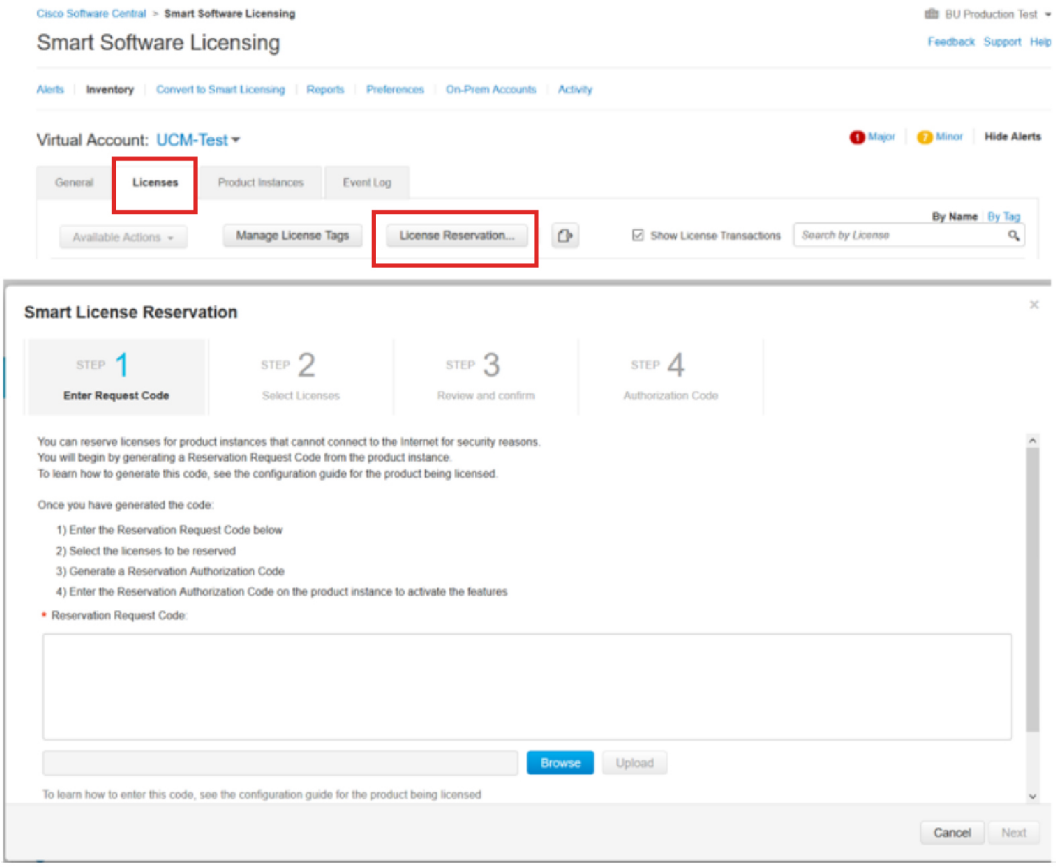
license smart reservation enable を実行して、Unified Communications Manager の登録ステータスが [予約を実行中（Reservation in progress）] になっていることを確認します。

。

手順

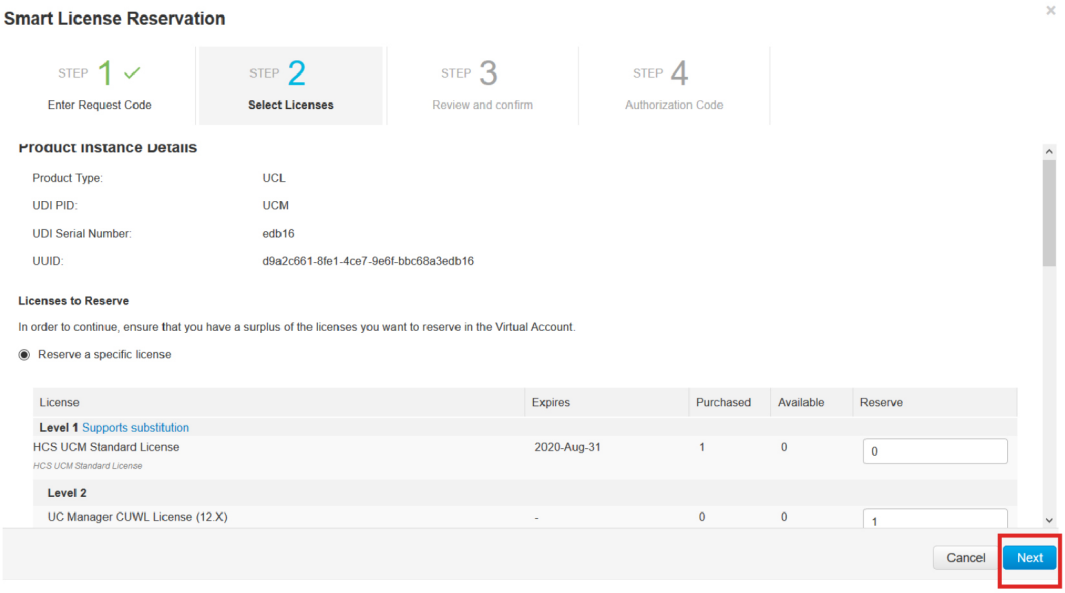
Step 1 Cisco Unified CM 管理コンソールから、*license smart reservation request* コマンドを実行します。

Step 2 CSSM（Cisco Smart Software Manager）にログインし、予約要求コードを入力します。



450364

Step 3 このデバイス用に予約するライセンスを選択し、承認コードを生成します。



450365

Step 4 承認コードを製品インスタンスにコピーし、**license smart reservation install "<authorization-code>"** コマンドを実行してインストールします。

450366

license smart reservation install "<authorization-code>"

Cisco Smart Software Manager から生成された予約承認コードをインストールするには、この手順を使用します。

始める前に

次の順序でコマンドを実行して、Unified Communications Manager の登録ステータスが [進行中の予約（Reservation In Progress）] であることを確認します。

- **license smart reservation enable**
- **license smart reservation request**

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart reservation install "<authorization-code>"

license smart reservation install-file <url>

Cisco Smart Software Manager で生成されたライセンス予約承認コード ファイルをインストールするには、この手順を使用します。

始める前に

次の順序でコマンドを実行して、Unified Communications Manager の登録ステータスが [進行中の予約（Reservation In Progress）] であることを確認します。

- **license smart reservation enable**
- **license smart reservation request**

（注） URL は、SFTP サーバ上の承認コード ファイルへの必須のパスであり、次の形式で表されます。

sftp://<HostName/IP>:<port>/<Path to Authorization-Code file>

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart reservation install-file <url>

特定のライセンス予約に関する追加タスク

特定ライセンス予約については、Unified Communications Manager で次の追加タスクを使用できます。

license smart reservation disable

このプロセスで特定のライセンスの保留を無効にします。

始める前に

特定ライセンス予約は、Unified Communications Manager で有効化します。

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart reservation disable

ライセンス予約の更新

製品インスタンスのライセンス予約を更新し、新しい承認コードを取得するには、次の手順を実行します。

始める前に

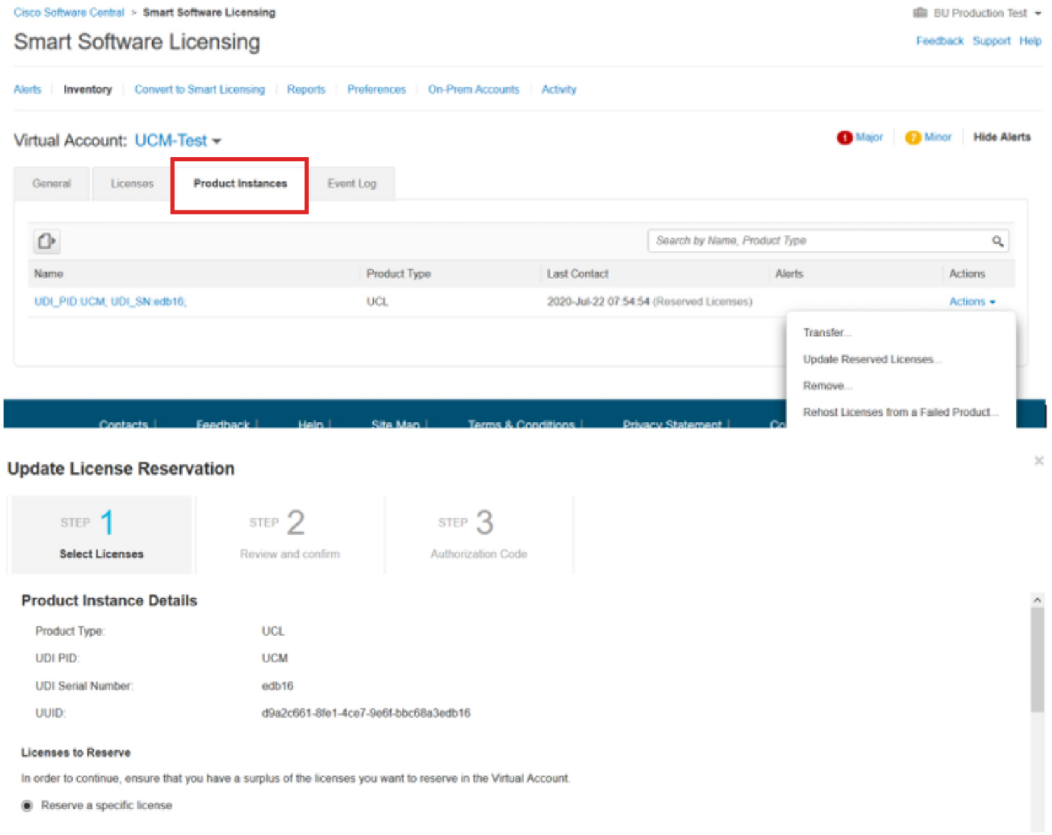
次の順序でコマンドを実行して、Unified Communications Manager の登録ステータスが [登録済み-特定ライセンス予約（Registered - Specific License Reservation）] になっていることを確認します。

- license smart reservation enable
- license smart reservation request
- license smart reservation install "<authorization-code>"

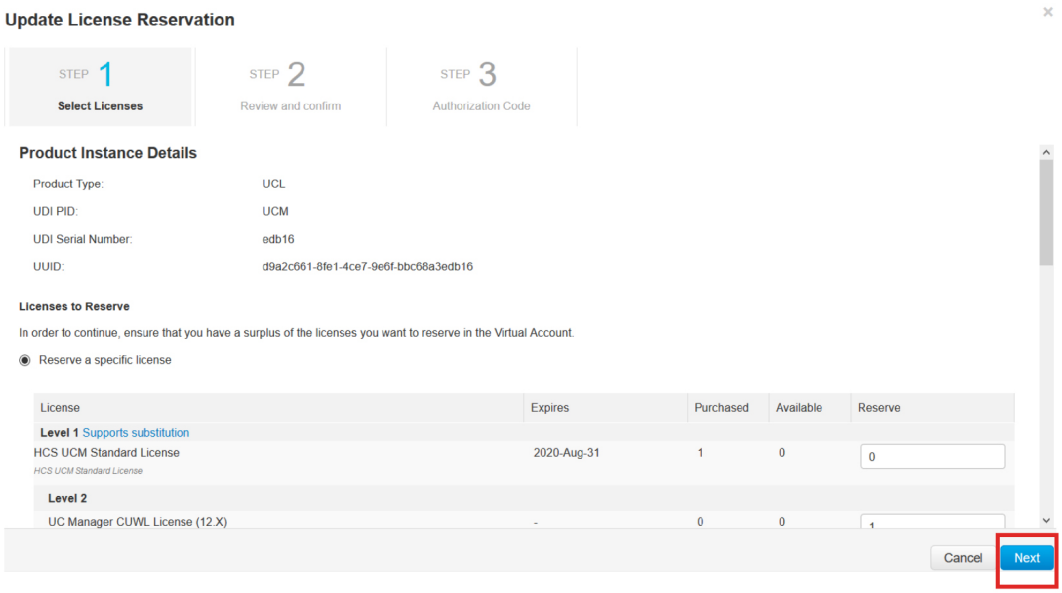
（注） Unified Communications Manager で特定ライセンス予約が有効になっている場合、上位層からのライセンスの借用は自動的には行われません。ライセンス予約は、Unified Communications Manager でのライセンスの消費/使用に合わせて手動で更新する必要があります。

手順

Step 1 CSSM で予約を更新する製品インスタンスの横にある [アクション（Actions）] ドロップダウンリストから、[予約済みライセンスの更新（Update Reserved Licenses）] を選択します。

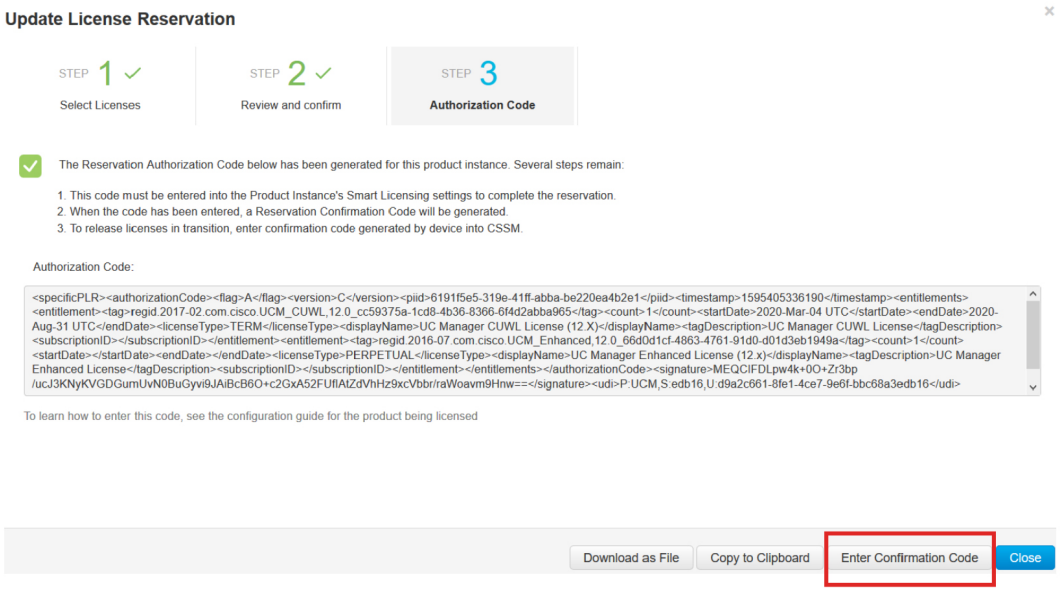


Step 2 予約を更新（この製品インスタンスに対するライセンスを追加、削除、更新）し、承認コードを生成します。



450367

Step 3 承認コードを製品インスタンスにコピーし、**license smart reservation install "<authorization-code>"** コマンドを実行してインストールします。

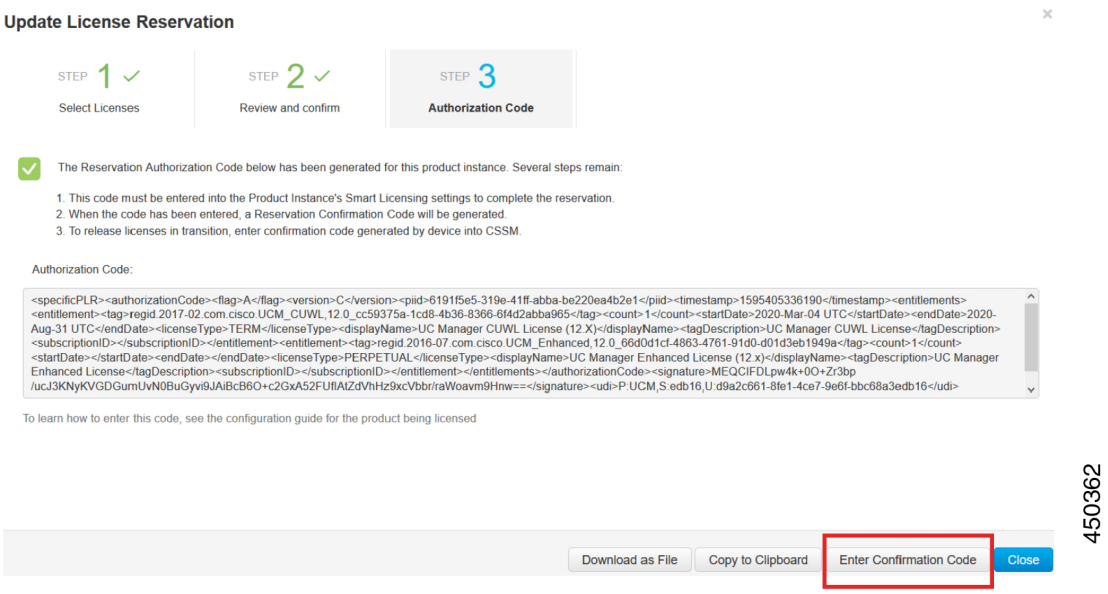


450362

Step 4 承認コードが正しくインストールされると、製品で確認コードが生成されます。

450368

Step 5 確認コードをコピーして CSSM に入力し、予約の更新を完了します。



license smart reservation cancel

次の手順を使用して、CUCM 要求コードに対する Cisco Smart Software Manager からの認証コードがインストールされる前に、予約プロセスをキャンセルします。

始める前に

次の順序でコマンドを実行して、Unified Communications Manager の登録ステータスが [進行中の予約（Reservation In Progress）] であることを確認します。

- **license smart reservation enable**
- **license smart reservation request**

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart reservation cancel

license smart reservation return

ライセンスをバーチャルアカウントプールに返却し、CSSM から製品インスタンスを削除するには、Cisco Smart Software Manager に返却コードを入力する必要があります。返却コードを生成するには、次の手順を実行します。

始める前に

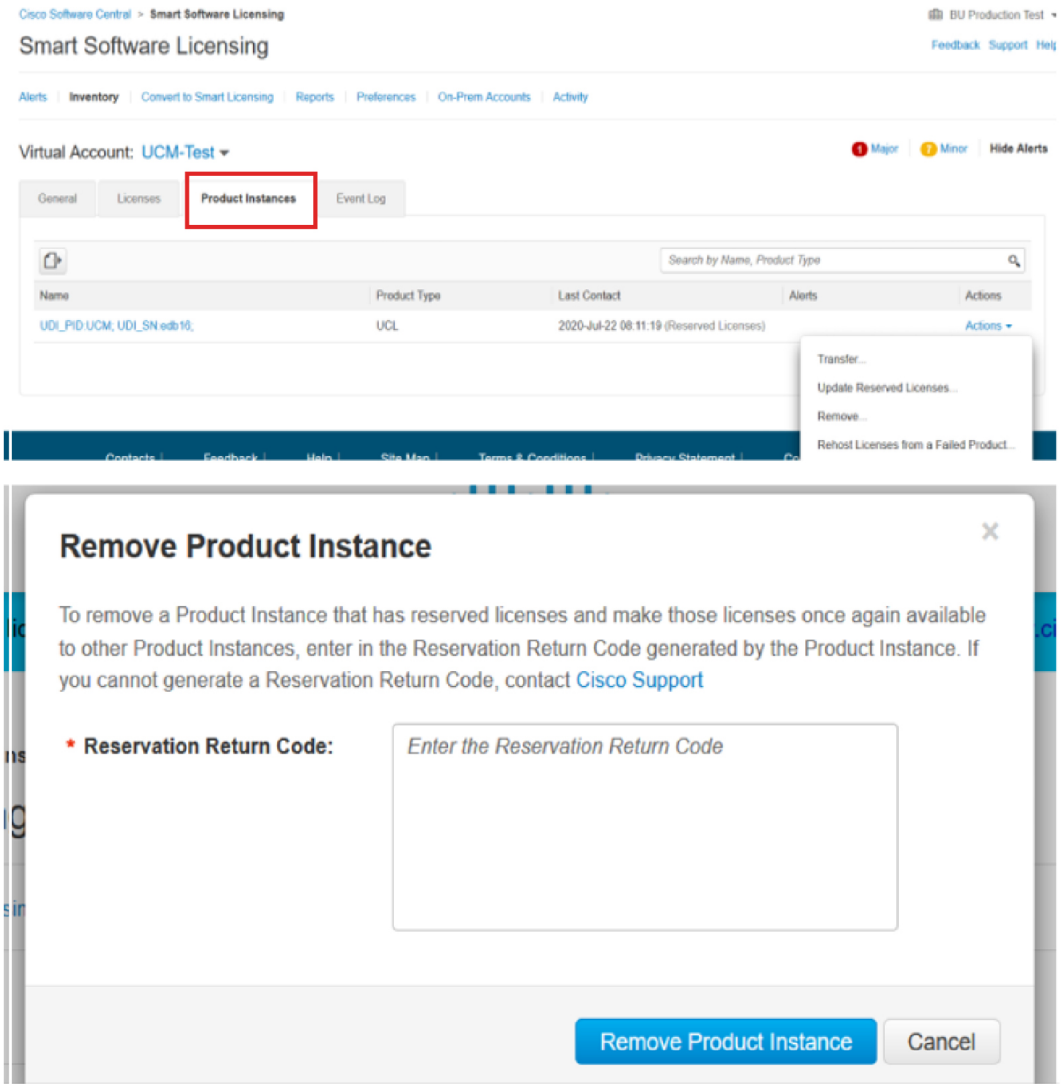
次の順序でコマンドを実行して、Unified Communcations Manger の登録ステータスが [登録済み-特定ライセンス予約（Registered - Specific License Reservation）] であることを確認します。

- **license smart reservation enable**
- **license smart reservation request**
- **license smart reservation install "<authorization-code>"**

手順

Step 1 Cisco Unified CM 管理コンソールから、license smart reservation return コマンドを実行します。

Step 2 予約返却コードを CSSM にコピーし、製品インスタンスを削除します。



license smart reservation return-authorization "<authorization-code>"

まだインストールされていない認証コードのリターンコードを生成するには、次の手順を使用します。ライセンスをバーチャルアカウントプールに返却し、CSSM から製品インスタンスを削除するには、Cisco Smart Software Manager に返却コードを入力する必要があります。

始める前に

次の手順でコマンドを実行して、Unified Communcations Manager の登録ステータスが [進行中の予約（Reservation In Progress）] であることを確認します。

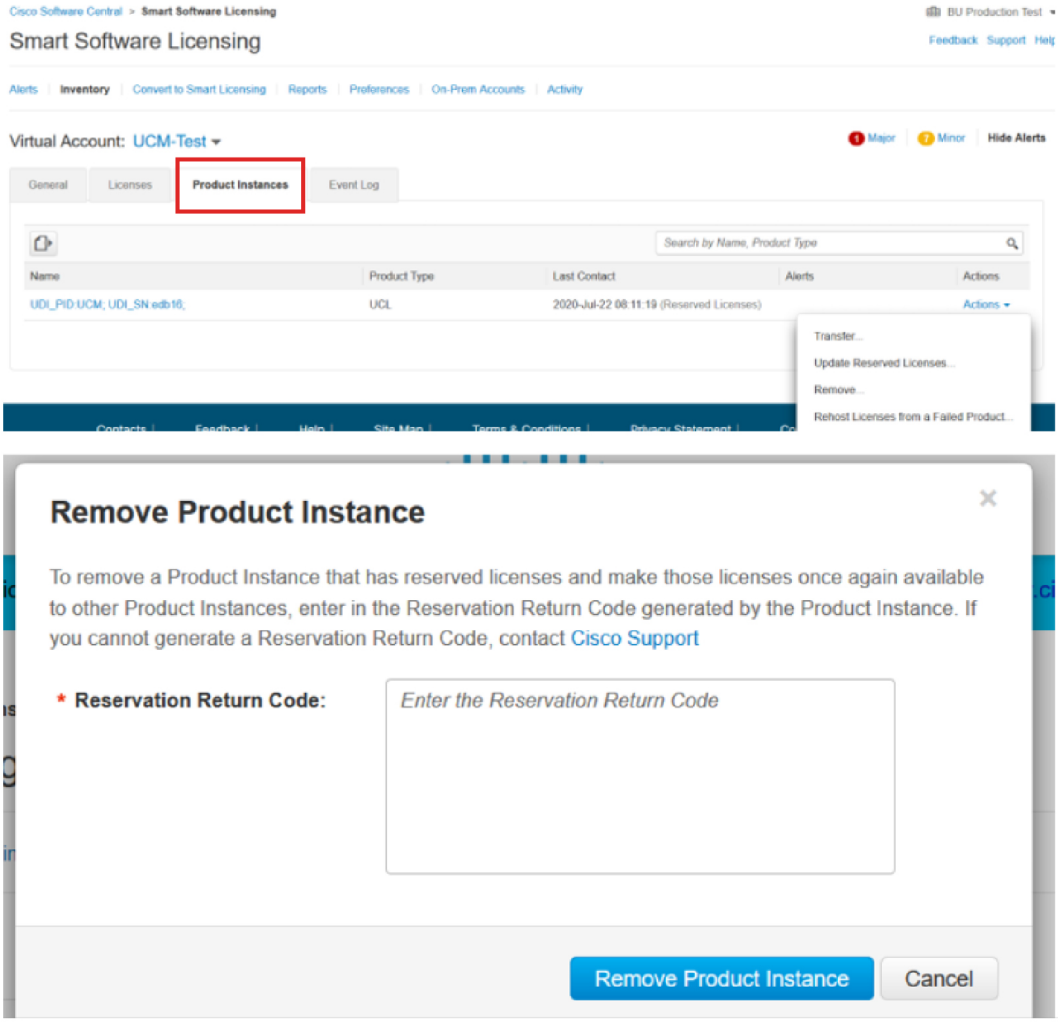
- **license smart reservation enable**

- **license smart reservation request**

手順

Step 1 Cisco Unified CM 管理コンソールから、license smart reservation return-authorization "<authorization-code>" コマンドを実行します。

Step 2 予約返却コードを CSSM にコピーし、製品インスタンスを削除します。



450361

特定ライセンス予約対応システムのバージョン14へのアップグレード

ライセンス予約が有効になっている Unified Communications Manager 12.5 システムをバージョン 14 にアップグレードする場合は、次のシナリオを考慮する必要があります。

1. バージョン 14 にアップグレードする前に、"license smart reservation return" コマンドを使用して 12.x のライセンスを返却します（推奨）。

   または

   バージョン 14 にアップグレードした後で、"license smart reservation return" コマンドを使用して 12.x のライセンスを返却します。

2. "license smart reservation request" コマンドを使用して要求コードを作成します。Cisco Smart Software Manager で、バージョンのないライセンスを使用して承認コードを生成します。
3. Cisco Unified Communications Manager で、"license smart reservation install <auth-code>" コマンドを使用して承認コードをインストールします。

永久ライセンス予約対応システムのバージョン 15 へのアップグレード

永久ライセンス予約（PLR）が有効になっている Unified Communications Manager 14 SU2 以降のシステムをバージョン15にアップグレードする場合は、次のシナリオを考慮する必要があります。

1. バージョン 15 にアップグレードした後で、"license smart reservation return" コマンドを使用してライセンスを返却します。
2. アップグレード後、"license smart reservation request" コマンドを使用してリクエストコードを作成します。Cisco Smart Software Manager で、PLR ライセンスを使用して承認コードを生成します。
3. Unified Communications Manager で、"license smart reservation install <auth-code>" コマンドを使用して承認コードをインストールします。

バージョンに依存しないライセンス

重要 このセクションは、リリース 14 以降に適用されます。

Unified Communications Manager は、バージョンに依存しないユーザライセンスをサポートしています。ライセンスは、年間契約で、サブスクリプション期間に対して発行されます。これらのV14ライセンスは、Flex EA（エンタープライズ アグリーメント）または Flex NU（名前付き—プロフェッショナル、拡張、アクセス）からご注文いただけます。詳細については、『注文ガイド』を参照してください。

Unified Communications Manager は、引き続きバージョン 12.X ライセンスを使用します。

ライセンスは CSSM（Cisco Smart Software Manager）で管理されます。詳細については、「スマート ソフトウェア ライセンシング （7 ページ）」を参照してください。

スマートライセンシングのエクスポートに関するコンプライアンス

スマートライセンシングは、エクスポート制限機能をユーザが使用できるようにする手段を提供します。接続された状態では、登録プロセスを使用して、エクスポート制限機能を使用します。接続されていない状態では、スマート ライセンス予約を使用してエクスポート制限機能を使用します。

このエクスポート制限機能は、スマート アカウントを使用している、エクスポート制限が適用されるお客様向けのソリューションです。この機能によってユーザは、Cisco Smart Software Manager またはサテライトで付与される規制上のエクスポート許可を要求し、エクスポート制限されている機能を Cisco Unified Communications Manager で有効化することができます。

以下のオプションでは、エクスポート制限機能に関する新しい機能と設計要素について説明しています。

- license smart export request local <exportfeaturename>
- license smart export return local <exportfeaturename>
- license smart export cancel

エクスポート制御のタスクフロー

次のタスクを実行して、Cisco Unified Communications Manager のエクスポート制限ライセンスを取得します。

license smart export request local <exportfeaturename>

このコマンドを使用すると、スマート アカウントを使用している、エクスポート制限の対象となるユーザは、Cisco Smart Software Manager またはサテライトから規制対象となるエクスポート ライセンスを要求することができます。

Cisco Smart Software Manager またはサテライトで規制対象となるエクスポート ライセンスが利用可能になると、このコマンドはエクスポート承認キーを返し、エクスポート制限の対象となる機能を製品上で有効化します。

始める前に

Cisco Unified Communications Manager は、Cisco Smart Software Manager またはサテライトを使用して登録されます。<CUCM の輸出制限の対象となる承認キー> ライセンスが利用可能であることを Cisco Smart Software Manager で確認してください。

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart export request local <exportfeaturename>

license smart export return local <exportfeaturename>

このコマンドは、以前に要求されたエクスポート制限付きライセンスを Cisco Smart Software Manager またはサテライトに返すことを許可します。エクスポート制限機能のエクスポート認証キーがシステムから削除されます。

始める前に

機能に対してエクスポート認証キーが生成されます。

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart export return local <exportfeaturename>

license smart export cancel

このコマンドを使用すると、エクスポート制限の対象となっている Smart アカウントを持つユーザは、Cisco Smart Software Manager またはサテライトからのエクスポート要求またはリターンの自動再試行のキャンセルを取り消すことができます。

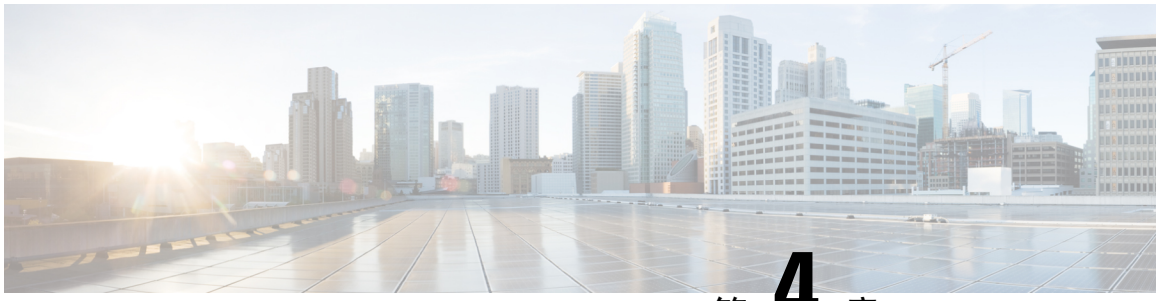
始める前に

Cisco Unified Communications Manager は、Cisco Smart Software Manager またはサテライトを使用して登録されます。

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart export cancel



第 4 章

エンタープライズパラメータおよびサービスの設定

エンタープライズ パラメータの概要

エンタープライズパラメータは、同一クラスタに存在するすべてのデバイスやサービスに適用されるデフォルト設定を提供します。クラスタは、同じデータベースを共有する Cisco Unified Communications Manager のセットで構成されます。Cisco Unified Communications Manager の新規インストール時には、エンタープライズパラメータを使用して、デバイスのデフォルトの初期値が設定されます。

エンタープライズパラメータの多くは、ほとんど変更の必要がありません。変更しようとしている機能を完全に理解している場合、または Cisco Technical Assistance Center（TAC）から変更を指示された場合を除き、エンタープライズパラメータを変更しないでください。

ほとんどの場合、推奨されるデフォルト設定が機能するはずです。

- IP 電話のフォールバック接続モニタ期間を設定します。
- すべてのユーザに対して社内ディレクトリの検索を許可します。
- クラスタの完全修飾電話番号（FQDN）と組織のトップレベル ドメインを設定します。
- ビデオ対応の Cisco Jabber 開始条件を設定します。
- （オプション）ネットワークが IPv6 を使用している場合は、IPv6 を有効にします。
- （オプション）リモート syslog サーバ名前を入力します。
- （オプション）導入をトラブルシューティングするためのコール トレース ログを設定します。
- （オプション）依存関係レコードを有効にします。

サービスパラメータの概要

サービスパラメータを使用すると、選択した Unified Communications Manager サーバでさまざまなサービスを設定できます。すべてのサービスに適用されるエンタープライズパラメータとは異なり、各サービスは個別のサービスパラメータのセットで設定されます。

サービスパラメータでは、次の 2 種類のサービスを設定できます。これらはいずれも Cisco Unified Serviceability 内で有効化できます。

- **機能サービス**：この種類のサービスは、特定のシステム機能を実行するのに使用されます。それらを使用するためには、機能サービスをに対してオンにする必要があります。
- **ネットワーク サービス**：ネットワーク サービスはデフォルトでオンになっていますが、トラブルシューティングの目的でネット ワークサービスの停止と開始（または再起動）を選択できます。この種類のサービスには、データベースやプラットフォームなどのシステム コンポーネントが正常に機能できるようにするサービスが含まれます。

サービスパラメータの [サービスパラメータ（service parameter）] フィールドの説明を表示するには、[サービスパラメータの設定（Service Parameter Configuration）] ウィンドウで [?] アイコンをクリックするか、パラメータの名前をクリックします。

（注） サービスを非アクティブ化すると、更新されたサービスパラメータ値は Unified Communications Manager に保持されます。サービスを再開すると、Unified Communications Manager はサービスパラメータを変更後の値に設定します。

システム パラメータのタスクフロー

始める前に

Unified Communications Manager ノードとポート設定をセットアップします。

手順

	コマンドまたはアクション	目的
Step 1	エンタープライズパラメータを設定する（39 ページ）。	ユニファイド コミュニケーション マネージャノードの初期セットアップに必要なシステム全体のパラメータを設定します。
Step 2	基本サービスのアクティブ化（45 ページ）。	Cisco Unified Serviceability を使用するノードで、サービスをアクティブ化することができます。

	コマンドまたはアクション	目的
Step 3	サービスパラメータの設定 （48 ページ）。	クラスタ内のパブリッシャノードとサブスクライバ ノードのサービスパラメータを設定します。

エンタープライズパラメータを設定する

導入のエンタープライズレベルのパラメータを編集するには、次の手順を実行します。これを使用して、組織の最上位ドメインまたはクラスタの完全修飾ドメイン名などのエンタープライズレベルの設定を設定できます。

（注） Cisco ユニファイド CM Administration でパラメータを編集すると、新しい設定も Cisco ユニファイド CM、IM およびプレゼンスの管理に反映されます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

[エンタープライズパラメータ (Enterprise parameters)] ウィンドウに、エンタープライズパラメータのリストが表示されます。

Step 2 パラメータ設定を編集します。

パラメータに関する説明を参照するには、GUI でパラメータ名をクリックします。一般的なエンタープライズパラメータの詳細については、「よくある企業パラメータ （39 ページ）」を参照してください。

Step 3 [保存（Save）] をクリックします。

Step 4 **[リセット(reset)]** をクリックし、**[OK]** をクリックしてすべてのデバイスをリセットします。

（注） ほとんどのパラメータでは、設定を保存した後にデバイスをリセットする必要があります。デバイスを登録している場合は、デバイスをリセットする前に、すべての設定変更を完了することをお勧めします。

システム内のすべてのデバイスプールをリセットすることで、すべてのデバイスをリセットできます。

よくある企業パラメータ

次の表に、組織のトップレベル ドメインまたはクラスタの完全修飾ドメイン名など、エンタープライズ設定に使用される共通のエンタープライズパラメータを示します。詳細なリストを見るに

は、Cisco Unified CM Administration の **[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** メニューを使用します。

表 *2 : Unified Communications Manager* の初期設定用の共通エンタープライズパラメータ

パラメータ名	説明
エンタープライズパラメータ	
接続モニタ間隔（Connection Monitor Duration）	クラスタ内の IP 電話がセカンダリ ノードに登録された場合に、このパラメータを使用して、プライマリ ノードが使用可能になった後、それがフォールバックして再登録される前に、IP 電話が待機する時間を設定します。このパラメータは、特定のセキュア Survivable Remote Site Telephony（SRST）ルータに対応するすべてのセキュアなデバイスに影響します。 詳細については、『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。 デフォルトは 120 秒です。 変更内容を反映するには、すべてのサービスを再起動してください。
CCMAdmin パラメータ	
依存性レコードを有効化（Enable Dependency Records）	このパラメータはトラブルシューティングに必要な依存関係の記録を表示します。初期システム設定の間、依存記録を表示することは有益であるかもしれない。 依存関係記録の表示は、高いCPU使用率のピークをもたらし、コール処理に影響を与える可能性がある。考えられるパフォーマンス問題を回避するために、システム設定の完了後は、このパラメータを無効にします。負荷の低い時間帯またはメンテナンス ウィンドウの間のみに依存関係レコードを表示することを推奨します。 有効にすると、Unified Communications Manager を使用してほとんどの設定画面からアクセスできる [関連リンク（Related Links）] ドロップダウンリストで、[依存関係レコード（Dependency Records）] を選択できるようになります。 デフォルト：False
ユーザ データ サービスパラメータ	
すべてのユーザ検索を有効にする（Enable All User Search）	名前、名前、またはディレクトリ番号が指定されていない場合、このパラメータは会社のディレクトリのすべてのユーザを検索することができます。このパラメータは、[Cisco CallManager セルフ ケア（Cisco CallManager Self Care）]（CCMUser）ウィンドウでのディレクトリ検索にも適用されます。 デフォルト：True
クラスタ全体のドメイン設定	

パラメータ名	説明
組織の最上位ドメイン（Organization Top Level Domain）	このパラメータは、組織のトップレベルのドメインを定義します。例：cisco.com 最大長：255 文字 許可された値は、大文字と小文字、数字（0-9）、ハイフンとポイント（ドメインラベル区切り記号として）の有効領域を使用します。ドメインラベルの先頭文字をハイフンにすることはできません。最後のラベルの先頭文字を数字にすることはできません。たとえば、cisco.1om といったドメインは無効です。
クラスタの完全修飾ドメイン名（Cluster Fully Qualified Domain Name）	このパラメータに、このクラスタの 1 つまたは複数の完全修飾ドメイン名（FQDN）を定義します。複数の FQDN はスペースで区切る必要があります。アスタリスク（*）を使用して、FQDN 内でワイルドカードを指定することができます。例：`cluster-1.cisco.com *.cisco.com` このパラメータのいずれかの FQDN に一致するホスト部分がある URL を含む要求（SIP コールなど）は、クラスタと接続されたデバイスにルーティングされます。 最大長：255 文字 有効な値：FQDN または * ワイルドカードを使用した部分的な FQDN。大文字と小文字、数字（0-9）、ハイフンとポイント（ドメインラベル区切り記号として）。ドメインラベルの先頭文字をハイフンにすることはできません。最後のラベルの先頭文字を数字にすることはできません。たとえば、cisco.1om といったドメインは無効です。
IPv6	

パラメータ名	説明
IPv6 の有効化（Enable IPv6）	このパラメータは、Unified Communications Manager が Internet Protocol Version 6（IPv6）をネゴシエートできるかどうか、および電話で IPv6 機能をアドバタイズできるかどうかを決定します。 このパラメータを有効化する前に、すべてのノードのプラットフォームも含め、他のすべてのネットワーク コンポーネントで IPv 6を有効にする必要があります。それ以外の場合、システムは引き続き IPv4 専用モードで稼動します。 必須フィールドです。 デフォルト：False（IPv6 は無効です） IPv6パラメータの変更を有効にするには、以下のサービスと、IM and Presence Service クラスタ内の影響を受けるサービスを再起動する必要があります。 • Cisco CallManager • Cisco IP Voice Media Streaming App • Cisco CTIManager • Cisco Certificate Authority Proxy Function
Cisco Syslog Agent	
リモート Syslog サーバ名 1（Remote Syslog Server Name 1）	リモート Syslog サーバの名前または IP アドレスを入力します。サーバ名が指定されていない場合、Cisco Unified Serviceability は Syslog メッセージを送信しません。このパラメータは、ログ用に Syslog サーバを使用している場合にのみ必須です。 最大長：255 文字 許可された値:文字の大きさ、数字(0-9)、ハイフン、ポイントの有効なリモートSylogサーバ名を使用します。 別の Unified Communications Manager ノードを宛先として指定することはできません。
Cisco Jabber	
ビデオとともにコールを開始しない（Never Start Call with Video）	このパラメータは、ビデオコールの開始時に、ビデオを送信するかどうかを決定します。すぐにビデオを送信せずにビデオ コールを開始するには、[True] を選択します。ビデオ コール中はいつでも、ビデオの送信開始を選択できます。 このパラメータは、IM and Presence Service のどの設定よりも優先されます。False に設定すると、ビデオコールは IM and Presence Service で指定された設定に従って開始されます。 デフォルト：False

パラメータ名	説明
SSO および OAuth の設定	
IOS の SSO ログイン動作（SSO Login Behavior for iOS）	このパラメータは、制御された Mobile Device Manager（MDM）導入環境で Cisco Jabber が IdP に対して証明書ベースの認証を実行できるようにする場合に必要です。 [iOS向けSSOログイン動作（SSO Login Behavior for iOS）] パラメータには次のオプションが含まれます。 • [組み込みブラウザの使用（Use Embedded Browser）]：このオプションを有効化すると、Cisco Jabber は SSO 認証に組み込みブラウザを使用します。このオプションにより、バージョン 9 より前の iOS デバイスのネイティブ Apple Safari ブラウザで、クロス起動なしの SSO を使用できるようになります。 • [ネイティブブラウザの使用（Use Native Browser）]：このオプションを有効化すると、Cisco Jabber は、MDM 導入環境でアイデンティティ プロバイダー（IdP）に対して証明書ベースの認証を実行するために、iOS デバイスで Apple Safari フレームワークを使用します。 （注） 制御された MDM 導入環境である場合を除き、ネイティブブラウザの使用は組み込みブラウザを使用する場合ほどセキュアではないため、このオプションの設定は推奨しません。 必須フィールドです。 [デフォルト（Default）]：組み込みブラウザ（WebView）を使用します。

パラメータ名	説明
更新ログインフローを使用した OAuth（OAuth with Refresh Login Flow）	このパラメータは、Unified Communications Manager に接続するときに、Cisco Jabber などのクライアントによって使用されるログインフローを制御します。 • [有効（Enabled）]：このオプションを有効にすると、クライアントで oAuth ベースの高速なログイン フローを使用してすばやく効率的にログインできるようになり、たとえばネットワークの変更などによってログインし直す際にユーザが入力する必要がなくなります。このオプションを使用するためには、Expressway や Unity Connection（更新ログイン フローが有効化されている互換性のあるバージョン）など、Unified Communications ソリューションのその他のコンポーネントからのサポートが必要です。 • [無効（Disabled）]：このオプションを有効化する場合、従来の動作のままとなり、旧バージョンの他のシステム コンポーネントとの互換性が保たれます。 （注） Cisco Jabber を使用したモバイルおよびリモート アクセスの導入環境では、更新ログイン フローで oAuth をサポートする、互換性のある Expressway バージョンでのみ、このパラメータを有効化することを推奨します。互換性のないバージョンは、Cisco Jabber の機能に影響する場合があります。サポートされているバージョンおよび設定要件については、特定の製品のドキュメントを参照してください。 **重要** この機能は、リリース 12.5(1)SU7 および 14SU3 以降で適用されます。 パブリッシャとともに、サブスクライバノードもリクエスト送信者ノードのデータベースの更新トークンを更新するためのアクセス権を持ち、同じものがクラスタ全体にレプリケートされます。 必須フィールドです。 デフォルトでは無効になっています。
更新トークンの自動更新	このパラメータを使用すると、管理者は更新トークンの自動更新を有効または無効にできます。デフォルトでは、このパラメータはイネーブルです。無効になっている場合、Unified Communications Manager は更新トークンを自動延長しないことで、以前の動作を保持します。 **重要** この機能は、リリース 15 以降で適用されます。 必須フィールドです。 デフォルトは Enabled です。

パラメータ名	説明
RTMT での SSO の使用（Use SSO for RTMT）	このパラメータは、Real-Time Monitoring Tool（RTMT）用に SAML SSO を有効化するために設定します。 [RTMTでのSSOの使用（Use SSO for RTMT）] パラメータには、次のオプションが含まれます。 • [True]：このオプションを選択すると、RTMT は、SAML SSO ベースの IdP ログイン ウィンドウを表示します。 （注） 新規インストール時には、[RTMTでのSSOの使用（Use SSO for RTMT）] パラメータのデフォルト値は **True** になっています。 • [False]：このオプションを選択すると、RTMT は、基本認証のログイン ウィンドウを表示します。 （注） [RTMT での SSO の使用（Use SSO for RTMT）] パラメータがない Cisco Unified Communications Manager のバージョンからアップグレードする場合、新しいバージョンに表示されるこのパラメータのデフォルト値は False です。 必須フィールドです。 デフォルト：True。

基本サービスのアクティブ化

クラスタ全体でサービスをアクティブ化するには、この手順を使用します。

パブリッシャノードとサブスクライバ ノードで推奨されるサービスの一覧については、次のトピックを参照してください。

- パブリッシャノードに推奨するサービス（46 ページ）
- サブスクライバーノード用の推奨サービス（47 ページ）

手順

Step 1 Cisco Unified Serviceability から、**[ツール（Tools）]>[サービスのアクティブ化（Service Activation）]** を選択します。

Step 2 ドロップダウン メニューから [サーバ（Server）] を選択して、[移動（Go）] をクリックします。

サービスと現在のステータスが表示されます。

Step 3 必要なサービスをアクティブ化または非アクティブ化します。

- サービスをアクティブ化するには、アクティブ化するサービスの横にあるチェックボックスをオンにします。
- サービスを非アクティブ化するには、非アクティブ化するサービスの横にあるチェックボックスをオフにします。

Step 4 [保存（Save）] をクリックします。
サービスのアクティブ化が完了するには数分かかることがあります。ステータスの変更を確認するには、ページを更新します。

パブリッシャノードに推奨するサービス

次の表に、専用でない TFTP サーバを使用している場合に Unified Communications Manager パブリッシャノードに推奨されるサービスを示します。

表 *3 :* 専用ではない *TFTP* サーバの導入環境に推奨するパブリッシャノードサービス

タイプ	サービス名
CM サービス	Cisco CallManager
	Cisco Unified Mobile Voice Access Service
	Cisco IP Voice Media Streaming App
	Cisco CTIManager
	Cisco Extended Functions
	シスコ クラスタ間検索サービス
	シスコ ロケーション帯域幅マネージャ
	Cisco TFTP
CTI サービス	Cisco IP Manager Assistant
	Cisco WebDialer Web Service
CDR サービス	Cisco SOAP - CDRonDemand Service
	Cisco CAR Web Service
データベースおよび管理者サービス	Cisco Bulk Provisioning サービス
	AXL Web サービス
	Cisco URL Web Service
パフォーマンスおよびモニタリングサービス	Cisco Serviceability Reporter
	Cisco Certificate Authority Proxy Function

タイプ	サービス名
ディレクトリサービス	Cisco DirSync

ヒント　以下のサービスを使用しない場合、安全にそれらを無効にできます。

- Cisco Messaging Interface
- Cisco DHCP Monitor サービス
- Cisco TAPS サービス
- Cisco Directory Number Alias Sync
- Cisco Dialed Number Analyzer Server
- Cisco Dialed Number Analyzer
- Self Provisioning IVR

サブスクライバーノード用の推奨サービス

次の表に、専用でない TFTP サーバを使用している場合に、Unified Communications Manager サブスクライバノードに推奨されるサービスを示します。

ヒント　他のサービスを使用する予定がない場合は、そのサービスを安全に無効にすることができます。

表 *4:* 専用の *TFTP* サーバ導入に推奨されるサブスクライバーノードサービス

タイプ	サービス名
CM サービス	Cisco CallManager
	Cisco IP Voice Media Streaming App
	Cisco CTIManager
	Cisco Extension Mobility
	Cisco Extended Functions
	Cisco TFTP

クラスタ内の各 IM and Presence Service ノードで、次のサービスをアクティブ化する必要があります。

- Cisco SIP Proxy
- Cisco Presence Engine

- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

サービスパラメータの設定

ノードのサービスパラメータは、 Cisco Unified Communications Manager Administration を使用して設定できます。クラスタ全体としてマークされているサービスパラメータは、クラスタ内の全ノードに影響を及ぼします。

注意 サービスパラメータの一部の変更は、システム障害の原因になることがあります。変更しようとしている機能を完全に理解している場合と、Cisco Technical Assistance Center（TAC）から変更の指定があった場合を除いて、サービスパラメータに変更を加えないようにしてください。

始める前に

- Unified Communications Manager ノードが設定されていることを確認します。
- サービスがアクティブであることを確認します。詳細については、「基本サービスのアクティブ化 （45 ページ）」を参照してください。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。

Step 2 [サーバ（Server）] ドロップダウンリストのノードを選択します。

Step 3 [サービス（Service）] ドロップダウンリストのサービスを選択します。

ヒント [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウ の？アイコンをクリックして、サービスパラメータのリストと説明を表示します。

Step 4 [詳細設定（Advanced）] をクリックして、すべてのパラメータのリストを表示します。

Step 5 サービスパラメータを変更し、[保存（Save）] をクリックします。

ウィンドウが更新され、サービスパラメータ値が更新されます。

[デフォルトに設定（Set to Default）] ボタンをクリックすると、すべてのパラメータが、[パラメータ値（Parameter Value）] フィールドの後に表示される推奨値に更新されます。パラメータに提案値が設定されていない場合は、[デフォルトに設定（Set to Default）] ボタンをクリックしてもサービスパラメータ値は変更されません。

クラスタ全体のサービスパラメータ設定の表示

Cisco Unified Communications Manager Assistant および Cisco Unified Serviceability を使用して、クラスタ内のノードのサービス ステータスを表示できます。サービスパラメータの設定とパラメータの説明を表示するには、Cisco Unified Communications Manager Assistant を使用します。

手順

Step 1 Cisco Unified Communications Manager Assistant を使用してノードのサービスを表示し、サービスパラメータ設定を確認するには、次の手順を実行します。

a) **[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。

b) [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウで、[サーバ（Server）] ドロップダウンリスト ボックスのノードを選択します。

c) [サービス（Service）] ドロップダウン ボックスのサービスを選択します。

選択したノードに適用されるすべてのパラメータが表示されます。[クラスタ全体のパラメータ（一般）（Clusterwide Parameters（General））] セクションに表示されるパラメータは、クラスタ内の全ノードに適用されます。

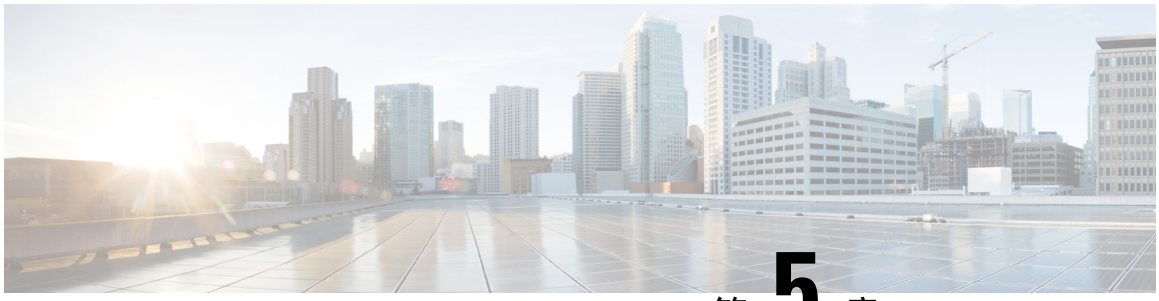
d) [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウの（? ）アイコンをクリックし、サービスパラメータと説明のリストを表示します。

Step 2 クラスタ内の全ノードに関する特定のサービスのサービスパラメータを表示するには、[サービスパラメータ設定（Service Parameter Configuration）] ウィンドウの [関連リンク（Related Links）] ドロップダウン ボックスの [すべてのサーバに対するパラメータ（Parameters for All Servers）] を選択し、[Go] をクリックします。

[すべてのサーバに対するパラメータ（Parameters for All Servers）] ウィンドウが表示されます。表示されているサーバ名またはパラメータ値をクリックして、関連する [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウを開くことができます。

Step 3 クラスタ内の全ノードに関する特定のサービスの同期外れサービスパラメータを表示するには、[すべてのサーバに対するパラメータ（Parameters for All Servers）] ウィンドウの [関連リンク（Related Links）] ドロップダウン ボックスの [すべてのサーバに対する同期外れパラメータ（Out of Sync Parameters for All Servers）] を選択し、[Go] をクリックします。

[すべてのサーバに対する同期外れパラメータ（Out of Sync Parameters for All Servers）] ウィンドウが表示されます。表示されているサーバ名またはパラメータ値をクリックして、関連する [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウを開くことができます。



第 5 章

IPv6 スタックの設定

IPv6 スタックの概要

IPv6 は、IPv4 アドレスが使用する 32 ビットの代わりに 128 ビットを使用する拡張 IP アドレス指定プロトコルです。IPv6 は IPv4 よりもはるかに広い範囲の IP アドレスを提供しています。これにより、IP アドレスが枯渇するリスクが大幅に軽減されます。これは IPv4 アドレスを使用する主な懸念事項の中にあります。

デフォルトでは、Cisco Unified Communications Manager は IPv4 アドレス指定を使用するように設定されています。ただし、IPv6 スタックをサポートするようにシステムを構成して、IPv6 のみのエンドポイントを使用して SIP ネットワークを展開できるようにすることもできます。IP アドレスが枯渇するリスクを減らすことに加えて、IPv6 は次の利点をいくつか提供しています。

- 状態なしアドレス自動設定
- 単純化されたマルチキャスト機能
- ルーティングの簡素化とルーティングテーブルの必要性の最小化
- サービスの最適化
- モビリティの適切な処理
- より優れたプライバシーと安全性

システムレベルIPv 6

IPv6 ネットワークを展開していても、Cisco Unified Communications Manager サーバは内部通信で IPv4 を使用することがあります。これは、内部のシステムコンポーネントとアプリケーションの一部が IPv4 のみをサポートしているためです。その結果、すべてのデバイスが IPv6 専用モードで動作しても、Cisco Unified Communications Manager サーバはいくつかの内部通信で IPv4 を使用する必要があるため、IPv4 と IPv6 の両方のアドレスが指定されます。

（注） SIP デバイスを IPv4 と IPv6 の両方のネットワークで動作させる必要がある場合は、2 つのスタックを設定する必要があります。この章のタスクを実行して Cisco Unified Communications Manager で IPv6 スタックを有効にする場合、2 つのスタックの SIP ネットワークも有効にする必要があります。「2 つのスタック (IPv4 および IPv6) の概要 （59 ページ）」を参照してください。

デュアル スタック IPv6 の前提条件

デュアルスタックCisco Unified Communications Manager を設定する前に、IPv6 をサポートするように次のネットワークサーバとデバイスを設定する必要があります。詳細については、デバイスのユーザ ドキュメントを参照してください。

- IPv6 がサポートされている DHCP サーバと DNS サーバをプロビジョニングします。シスコネットワーク登録サーバは、DHCPとDNSに対するIPv 6をサポートする。
- IPv6 がサポートされている場合は、ゲートウェイ、ルータ、MTP などのネットワークデバイス用の IOS を設定します。
- IPv6 を実行するように TFTP サーバを設定します。

IPv6 の設定タスクフロー

システムのデュアル スタック IPv6 を設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
Step 1	オペレーティング システムの IPv6 の設定 （53 ページ）	IPv6アドレスをサポートするオペレーティング システムを設定します。
Step 2	IPv6 向けのサーバ設定 （54 ページ）	IPv6アドレスを使用して、クラスタのサーバを設定します。
Step 3	IPv6 の有効化 （54 ページ）	IPv6 のシステムを有効にするエンタープライズパラメータを設定します。
Step 4	次のいずれかの操作を行います。 • クラスタの IP アドレッシング優先順位の設定 （55 ページ） • デバイス用 IP アドレッシング モードの優先順位の設定 （55 ページ）	クラスタ全体の IP アドレッシング設定を割り当てるために、エンタプライズ パラメータを設定することができます。 エンドポイントのグループごとに異なる設定を割り当てる必要がある場合は、共通デ

	コマンドまたはアクション	目的
		バイス設定でアドレッシング設定を入力します。 IP アドレッシング方式が推奨されるクラスタ設定を設定します。
Step 5	サービスの再起動 （57 ページ）	次のネットワーク サービスを再起動します。 • Cisco CallManager • Cisco CTIManager • Cisco IP Voice Media Streaming App • Cisco Certificate Authority Proxy Function

次のタスク

デュアル スタックのトランクを設定する方法については、SIP トランクの設定の章を参照してください。

SIP デバイスのデュアル スタックを設定する方法については、設定する SIP デバイスのセクションを参照してください。

オペレーティング システムの IPv6 の設定

Cisco Unified OS の管理でイーサネット IPv6 を設定するには、以下の手順を実行します。

（注） IPv6 DHCP サーバの設定は Windows でサポートされていないため、Cisco IOS IPv6 DHCP サーバを使用します。

手順

Step 1 Cisco Unified OS の管理で **設定** > **IPv6** > **イーサネット**を選択します。

Step 2 [Enable IPv6] チェックボックスをオンにします。

Step 3 **アドレス送信元** ドロップダウンリスト ボックスで、システムの IPv6 アドレス取得方法を設定します。

- **ルーターアドバタイズ**: システムは、ステートレス自動構成を使用して IPv6 アドレスを取得します。
- **DHCP**: システムは、DHCP サーバから IPv6 アドレスを取得します。
- **手動入力**: IPv6 アドレスを手動で入力する場合は、このオプションを選択します。

Step 4 IPv6 アドレスの取得方法に手動入力を設定する場合は、以下のフィールドに入力します。

- **IPv6 アドレス**を入力します。たとえば、 **fd62:6:96:2le:bff:fecc:2e3a**と入力します。
- **IPv6 マスク**を入力します。たとえば、**64** と入力します。

Step 5 **再起動して更新する** チェックボックスをオンにして、保存後に確実にシステムが再起動するようにします。

Step 6 [保存（Save）] をクリックします。

IPv6 向けのサーバ設定

IPv6 アドレスを使用して、クラスタのサーバを設定します。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [サーバ（Server）]** の順に選択します。

Step 2 **[IPv6 アドレス（デュアル IPv4/IPv6 の場合）（IPv6 Address (for dual IPv4/IPv6)）]** フィールドに、次のいずれかの値を入力します。

- DNS 設定済みで、DNS サーバが IPv6 対応の場合は、サーバのホスト名を入力します。
- それ以外の場合は、非リンク ローカル IPv6 アドレスを入力します。

Step 3 [保存（Save）] をクリックします。

Step 4 各クラスタ ノードで上記の手順を繰り返します。

IPv6 の有効化

システムで IPv6 サポートを設定する場合、システムで IPv6 デバイスをサポートできるようにする必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

Step 2 [IPv6 を有効化（Enable IPv6）] エンタープライズパラメータの値を [True（True）] に設定します。

Step 3 [保存（Save）] をクリックします。

次のタスク

クラスタ内デバイス用のIPアドレッシング設定を指定します。クラスタ全体のエンタープライズパラメータを使用して設定を適用するか、共通デバイス設定を使用して、その設定を使用するデバイスのグループに設定を適用することができます。

- クラスタの IP アドレッシング優先順位の設定 （55 ページ）
- デバイス用 IP アドレッシング モードの優先順位の設定 （55 ページ）

クラスタの IP アドレッシング優先順位の設定

デュアル スタック IPv6 でクラスタ全体の IP アドレッシング優先順位を設定するには、この手順でエンタープライズパラメータを使用します。これらの設定は、これよりも優先される共通デバイス設定が特定のトランクまたはデバイスに対して適用される場合を除き、すべての SIP トランクおよびデバイスに適用されます。

（注） 共通デバイス設定でのIPアドレス優先順位は、共通デバイス設定を使用するデバイスに対するクラスタ全体のエンタープライズパラメータの設定よりも優先されます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

Step 2 [メディア用のIPアドレッシングモード設定（IP Addressing Mode Preference for Media）] のエンタープライズパラメータの値を [IPv4（IPv4）] または [IPv6（IPv6）] に設定します。

Step 3 [シグナリング用のIPアドレッシングモード設定（IP Addressing Mode Preference for Media）] のエンタープライズパラメータの値を [IPv4（IPv4）] または [IPv6（IPv6）] に設定します。

Step 4 [保存（Save）] をクリックします。

デバイス用 IP アドレッシング モードの優先順位の設定

共通デバイス設定で優先順位を設定することで、個々のデバイスにIPアドレッシングモードの優先順位を設定できます。トランク、電話、会議ブリッジ、トランスコーダなど、IPv6 アドレッシングをサポートするSIPデバイスおよびSCCPデバイスには、共通デバイス設定を適用できます。

（注） 共通デバイス設定でのIPアドレス優先順位は、共通デバイス設定を使用するデバイスに対するクラスタ全体のエンタープライズパラメータの設定よりも優先されます。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]**>**[デバイスの設定（Device Settings）]**>**[共通デバイス設定（Common Device Configuration）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 SIP トランク、SIP 電話または SCCP 電話の場合、[IPアドレッシングモード（IP Addressing Mode）] ドロップダウンリストの値を選択します。

- [IPv4 のみ（IPv4 Only）]—デバイスはメディアやシグナリングに IPv4 アドレスだけを使用します。
- [IPv6 のみ（IPv6 Only）]—デバイスはメディアやシグナリングに IPv6 アドレスだけを使用します。
- [IPv4 および IPv6（IPv4 and IPv6）]—（デフォルト）デバイスはデュアルスタック デバイスで、利用できる IP アドレスのタイプを使用します。両方の IP アドレスのタイプがデバイスに設定されている場合、デバイスのシグナリングには、[シグナリグ用IPアドレッシングモード優先設定（IP Addressing Mode Preference for Signaling）] 設定を使用し、メディア デバイスには、[メディア用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Media）] エンタープライズパラメータの設定を使用します。

Step 4 前のステップで IPv6 を設定した場合は、[シグナリング用のIPアドレッシングモード（IP Addressing Mode for Signaling）] ドロップダウンリストで IP アドレッシング設定を指定します。

- [IPv4（IPv4）]—デュアル スタック デバイスでシグナリングに IPv4 アドレスを優先して使用します。
- [IPv6（IPv6）]—デュアル スタック デバイスでシグナリングに IPv6 アドレスを優先して使用します。
- [システム デフォルトを使用（Use System Default）]—デバイスは、[シグナリグ用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）] エンタープライズパラメータの設定を使用します。

Step 5 [共通デバイス設定（Common Device Configuration）] ウィンドウで、残りのフィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 6 [保存（Save）] をクリックします。

次のタスク

IPv6 設定が完了したら、「サービスの再起動 （57 ページ）」を実行します。

SIP デバイスが IPv4 と IPv6 の両方のネットワークを同時にサポートするには、デバイスレベルで両方のスタックをサポートするようにシステムを設定する必要があります。詳細については、「2 つのスタック (IPv4 および IPv6) の概要 （59 ページ）」を参照してください。

サービスの再起動

システムの IPv6 設定したら、基本的なサービスを再起動します。

手順

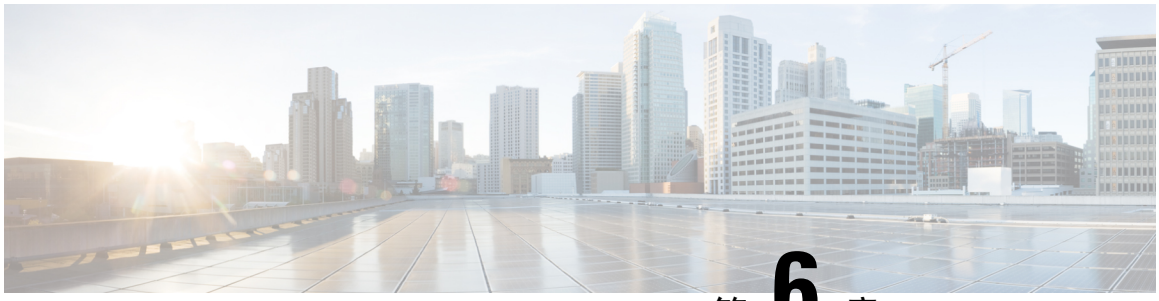
Step 1 Cisco Unified Serviceability にログインして、**[ツール（Tools）]>[コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択します。

Step 2 次のそれぞれのサービスに対応するチェックボックスをオンにします。

- Cisco CallManager
- Cisco CTIManager
- Cisco Certificate Authority Proxy Function
- Cisco IP Voice Media Streaming App

Step 3 [再起動（Restart）] をクリックします。

Step 4 **[OK]** をクリックします。



第 6 章

2 つのスタック（IPv4 と IPv6）の設定

2 つのスタック (IPv4 および IPv6) の概要

SIP ネットワークが IPv4 と IPv6 の両方のスタックに設定されている場合、SIP デバイスは次の各シナリオのコールを処理できます。

- コール内のすべてのデバイスが IPv4 のみをサポートします。
- コールに含まれるすべてのデバイスは IPv6 のみに対応しています。
- コール内のすべてのデバイスは、IPv4 と IPv6 の両方のスタックをサポートしています。このシナリオでは、システムはシグナリング イベントの [シグナリングのIPアドレッシングモード設定（IP Addressing Mode Preference for Signaling）] 設定とメディア イベントの [メディアのIPアドレッシングモード設定（IP Addressing Mode Preference for Media）] エンタープライズパラメータを設定することで、IP アドレスのタイプを判別します。
- 1 つのデバイスで IPv4 のみをサポートし、他のデバイスで IPv6 のみをサポートしている。このシナリオでは、Unified Communications Manager は、2 つのアドレッシング タイプ間でシグナリングを変換するために、コール パスに MTP を挿入します。

SIP デバイスとトランクの場合は、代替ネットワーク アドレス タイプ（ANAT）を設定すると、2 つのスタック サポートを有効にできます。ANAT が SIP デバイスまたはトランクに適用されると、IPv4 と IPv6 の両方のアドレスが使用可能な場合は、デバイスまたはトランクが送信する SIP シグナリングに両方のアドレスが含まれます。ANAT により、エンドポイントは IPv4 専用と IPv6 専用の両方のネットワークでシームレスに相互運用できます。

2 つのスタック（IPv4 と IPv6）の前提条件

IPv6 スタックをサポートするには、まず Cisco Unified Communications Manager を設定する必要があります (デフォルトでは IPv4 が有効になっています)。これには、メディアとシグナリングの IP アドレッシング設定の設定も含まれます。設定の詳細については、「IPv6 の設定タスクフロー（52 ページ）」を参照してください。

2 つのスタック（IPv4 と IPv6）の設定タスクフロー

IPv4 と IPv6 の両方のアドレス指定を同時にサポートするように SIP デバイスとトランクを設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
Step 1	SIP プロファイル用 ANAT の設定 （60 ページ）	IPv4 と IPv6 の両方のスタックを同時にサポートする SIP プロファイルを設定します。
Step 2	SIP 電話への ANAT の適用 （61 ページ）	ANAT 対応 SIP プロファイルを SIP 電話に適用します。これにより、SIP phone は IPv4 と IPv6 の両方のスタックを同時にサポートできます。
Step 3	SIP トランクへの ANAT の適用 （61 ページ）	ANAT 対応 SIP プロファイルを SIP トランクに適用します。これにより、トランクが IPv4 と IPv6 の両方のスタックを同時にサポートできるようになります。
Step 4	サービスの再起動 （62 ページ）	IPv4 と IPv6 の両方のスタックを同時にサポートするようにシステムを設定した後、重要なサービスを再起動します。

SIP プロファイル用 ANAT の設定

この手順を使用すると、代替ネットワーク アドレス タイプ（ANAT）をサポートする SIP プロファイルを設定できます。このプロファイルを使用する SIP デバイスおよびトランクは、IPv4 専用と IPv6 専用のネットワーク間でシームレスに相互運用できます。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[SIPプロファイル（SIP Profile）]** を選択します。

Step 2 次のいずれかを実行します。

a) 新しい SIP プロファイルを作成するには、[新規追加（Add New）] をクリックします。

b) **[検索（Find）]** をクリックし、既存の SIP プロファイルを選択します。

Step 3 [ANATの有効化（Enable ANAT）] チェックボックスを選択します。

Step 4 [SIPプロファイルの設定（SIP Profile Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 5 [保存（Save）] をクリックします。

SIP プロファイル SIP 電話または SIP トランクに適用して、これらのデバイスが IPv4 と IPv6 の両方のスタックを同時にサポートできるようにする必要があります。

SIP 電話への ANAT の適用

この手順を使用すると、SIP 電話に代替ネットワーク アドレス タイプ（ANAT）設定を適用できます。ANAT が有効な場合は、電話は IPv4 専用と IPv6 専用の両方のネットワークと通信できます。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

Step 2 既存の電話機を選択するには、[検索（Find）] をクリックします。

Step 3 [SIPプロファイル（SIP Profile）] ドロップダウンリスト ボックスから、ANAT を有効にした SIP プロファイルを選択します。

Step 4 [電話の設定（Phone Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 5 [保存（Save）] をクリックします。

SIP トランクへの ANAT の適用

次の手順を使用して、オルタネートネットワークアドレスタイプ設定を SIP トランクに適用します。これにより、 SIP トランクが IPv4 と IPv6 の両方のスタックを同時にサポートできるようになります。

（注） SIP トランク設定オプションの詳細については、「SIP トランクの設定（104 ページ）」を参照してください。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]>[トランク（Trunk）]** を選択します。

Step 2 [検索（Find）] をクリックして、既存の SIP トランクを選択します。

Step 3 [SIPプロファイル（SIP Profile）] ドロップダウンリスト ボックスから、ANAT を有効にした SIP プロファイルを選択します。

Step 4 **トランク設定**ウィンドウの残りのフィールドをすべて入力します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 5 [保存（Save）] をクリックします。

サービスの再起動

IPv4 と IPv6 の両方のスタックを同時にサポートするようにシステムを設定した後、重要なサービスを再起動します。

手順

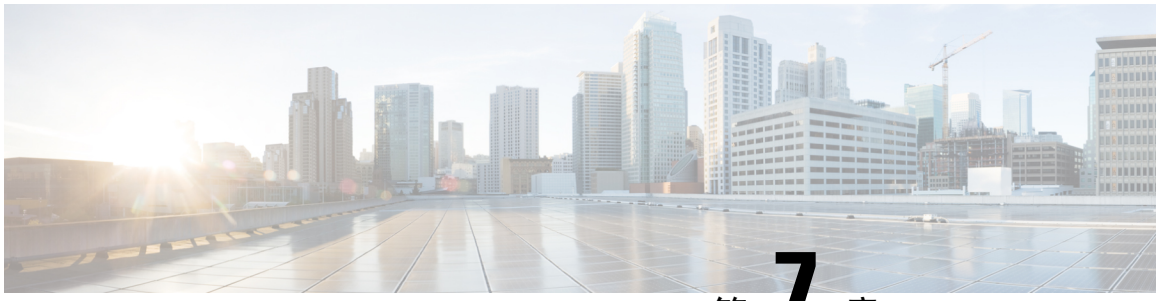
Step 1 Cisco Unified Serviceability にログインして、**[ツール（Tools）]>[コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択します。

Step 2 次のそれぞれのサービスに対応するチェックボックスをオンにします。

- Cisco CallManager
- Cisco CTIManager
- Cisco Certificate Authority Proxy Function
- Cisco IP Voice Media Streaming App

Step 3 [再起動（Restart）] をクリックします。

Step 4 **[OK]** をクリックします。



第 7 章

基本的なセキュリティの設定

セキュリティの設定について

ここでは、Cisco Unified Communications Manager を設定するために実行する必要がある基本的なセキュリティ設定タスクについて説明します。

セキュリティ設定のタスク

基本的なセキュリティ設定をセットアップするには、次のタスクを実行します。

クラスタの混合モードの有効化

クラスタ内で混合モードを有効にするには、次の手順を実行します。

手順

Step 1 パブリッシャノードでコマンドライン インターフェイスにログインします。

Step 2 **utils ctl set-cluster mixed-mode** CLI コマンドを実行します。

（注） Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Managerサテライトに登録されていること、およびスマートアカウントまたはバーチャル アカウントから受信した登録トークンで輸出制御機能の許可が有効になっており、そのトークンがこのクラスタに登録されていることを確認します。

証明書のダウンロード

CSR要求を送信する場合は、ダウンロード証明書タスクを使用して証明書のコピーを作成するか、証明書をアップロードします。

手順

Step 1 [Cisco Unified OS Administration] から **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

Step 2 検索情報を指定し、[検索（Find）] をクリックします。

Step 3 必要なファイル名を選択し、[ダウンロード（Download）] をクリックします。

証明書署名要求の生成

証明書署名要求（CSR）を生成します。これは、公開キー、組織名、共通名、地域、および国などの証明書申請情報を含む暗号化されたテキストのブロックです。認証局はこの CSR を使用して、ご使用のシステムの信頼できる証明書を生成します。

（注） 新しい CSR を生成すると、既存の CSR は上書きされます。

手順

Step 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

Step 2 [CSR の作成（Generate CSR）] をクリックします。

Step 3 [証明書署名要求の作成（Generate Certificate Signing Request）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 4 [生成（Generate）] をクリックします。

証明書署名要求のダウンロード

CSR を生成した後にダウンロードし、認証局に提出する準備をします。

手順

Step 1 [Cisco Unified OS Administration] から **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

Step 2 [CSR のダウンロード（Download CSR）] をクリックします。

Step 3 [証明書の用途（Certificate Purpose）] ドロップダウン リストで、証明書名を選択します。

Step 4 [CSR のダウンロード（Download CSR）] をクリックします。

Step 5 （任意） プロンプトが表示されたら、[保存（Save）] をクリックします。

サードパーティの認証局のルート証明書のアップロード

CA ルート証明書を CAPF 信頼ストアと Unified Communications Manager 信頼ストアにアップロードし、外部 CA を使用して LSC 証明書に署名します。

（注） LSC の署名にサードパーティ CA を使用しない場合は、このタスクをスキップします。

手順

Step 1 [Cisco Unified OS Administration] から **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

Step 2 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

Step 3 **[証明書の目的（Certificate Purpose）]** ドロップダウンリストで、**[CAPF 信頼（CAPF-trust）]** を選択します。

Step 4 証明書の説明を [説明（Description）] に入力します。たとえば、**外部 LSC 署名 CA の証明書**のように指定します。

Step 5 [参照（Browse）] をクリックしてファイルに移動してから、[開く（Open）] をクリックします。

Step 6 [アップロード（Upload）] をクリックします。

Step 7 このタスクを繰り返し、[証明書の用途（Certificate Purpose）] を [CallManager 信頼（callmanager-trust）] として証明書をアップロードします。

TLS の前提条件

最低 TLS バージョンを設定する前に、ネットワーク デバイスとアプリケーションの両方でその TLS バージョンがサポートされていることを確認します。また、それらが、ユニファイド コミュニケーション マネージャIM およびプレゼンスサービス で設定する TLS で有効になっていることを確認します。次の製品のいずれかが展開されているなら、最低限の TLS 要件を満たしていることを確認します。この要件を満たしていない場合は、それらの製品をアップグレードします。

- Skinny Client Control Protocol（SCCP）Conference Bridge
- トランスコーダ（Transcoder）
- ハードウェア メディア ターミネーション ポイント（MTP）
- SIP ゲートウェイ
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment
- Cisco Unified Border Element（CUBE）
- Cisco Expressway
- Cisco TelePresence Conductor

会議ブリッジ、メディア ターミネーション ポイント（MTP）、Xcoder、Prime Collaboration Assurance および Prime Collaboration Provisioning をアップグレードすることはできません。

（注） ユニファイドコミュニケーションマネージャの旧リリースからアップグレードする場合は、上位のバージョンの TLS を設定する前に、すべてのデバイスとアプリケーションでそのバージョンがサポートされていることを確認します。たとえば、ユニファイドコミュニケーションマネージャ IM およびプレゼンスサービス のリリース 9.x でサポートされるのは、TLS 1.0 のみです。

最小 TLS バージョンの設定

デフォルトでは、Unified Communications Manager において、最小 TLS バージョンとして 1.0 がサポートされています。Unified Communications Manager および IM and Presence Service の最低サポート TLS バージョンを 1.1 または 1.2 などの上位バージョンにリセットするには、次の手順を使用します。

設定対象の TLS バージョンが、ネットワーク内のデバイスとアプリケーションでサポートされていることを確認します。詳細については、「TLS の前提条件 （66 ページ）」を参照してください。

手順

Step 1 コマンド ライン インターフェイスにログインします。

Step 2 既存の TLS のバージョンを確認するには、**show tls min-version** CLI コマンドを実行します。

Step 3 **set tls min-version** <*minimum*> CLI コマンドを実行します。ここで、<*minimum*> は TLS のバージョンを示します。

たとえば、最低 TLS バージョンを 1.2 に設定するには、**set tls min-version 1.2** を実行します。

Step 4 すべての Unified Communications Manager と IM and Presence Service クラスタノードで、手順 3 を実行します。

TLS 暗号化の設定

SIP インターフェイスで使用可能な最強の暗号方式を選択することで、弱い暗号を無効にすることができます。TLS 接続を確立するために Unified Communications Manager でサポートされる暗号化を設定するには、この手順を使用します。

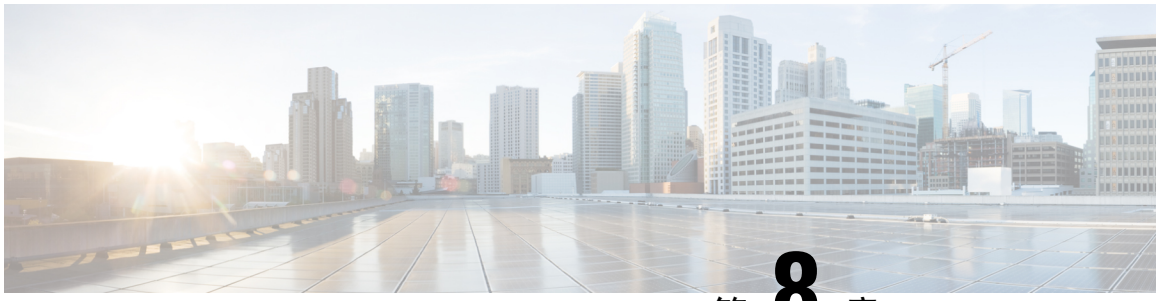
手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

Step 2 [セキュリティ パラメータ（Security Parameters）] で、[TLS 暗号化（TLS Ciphers）] エンタープライズパラメータの値を設定します。使用可能なオプションについては、エンタープライズパラメータのオンラインヘルプを参照してください。

Step 3 [保存（Save）] をクリックします。

（注） すべての TLS 暗号は、クライアントの暗号設定に基づいてネゴシエートされます。



第 8 章

シングルサインオンの設定

SAML SSO ソリューションについて

重要 Cisco Jabber を Cisco Webex Meeting Server と共に展開する場合、Unified Communications Manager と Webex Meeting Server は同じドメインに存在している必要があります。

SAML は XML ベースのオープン規格のデータ形式であり、いずれかのアプリケーションにサインインした後に、管理者は定義された一連のシスコのコラボレーション アプリケーションにシームレスにアクセスできます。SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。これは、サービス プロバイダ（例：Unified Communications Manager）がユーザの認証に使用する認証プロトコルです。SAML により、ID プロバイダー（IdP）とサービス プロバイダーの間で、セキュリティ認証情報を交換できます。

SAML SSO は SAML 2.0 プロトコルを使用して、シスコのコラボレーション ソリューションのドメイン間と製品間で、シングル サインオンを実現しています。SAML 2.0 は、Cisco アプリケーション全体で SSO を有効にし、Cisco アプリケーションと IdP 間でフェデレーションを有効にします。SAML 2.0 では、高度なセキュリティ レベルを維持しながら、シスコの管理ユーザが安全なウェブ ドメインにアクセスして、IdP とサービス プロバイダーの間でユーザ認証と承認データを交換できます。この機能が安全なメカニズムを提供していることで、さまざまなアプリケーションにわたり、共通の資格情報や関連情報を使用します。

SAML SSO の管理者権限は、シスコのコラボレーション アプリケーションでローカルに設定されたロールベース アクセス コントロール（RBAC）に基づき認証されます。

SAML SSO は、IdP とサービス プロバイダーの間のプロビジョニング プロセスの一部として、メタデータと証明書を交換することで信頼の輪（CoT）を確立します。サービス プロバイダーは IdP のユーザ情報を信頼しており、さまざまなサービスやアプリケーションにアクセスできるようにします。

重要　サービス プロバイダーが認証にかかわることはありません。SAML 2.0 では、サービス プロバイダーではなく、IdP に認証を委任します。

クライアントは IdP に対する認証を行い、IdP はクライアントにアサーションを与えます。クライアントはサービス プロバイダーにアサーションを示します。CoT が確立されているため、サービス プロバイダーはアサーションを信頼し、クライアントにアクセス権を与えます。

SAML SSO 設定タスクフロー

SAML SSO 用にユニファイドコミュニケーションマネージャを設定するには、次のタスクを実行します。

始める前に

SAML SSO の設定では、ユニファイドコミュニケーションマネージャを設定するのと同時にアイデンティティプロバイダー (IdP) を設定する必要があります。IdP 固有の構成例については、以下を参照してください。

- Active Directory フェデレーション サービス
- Okta
- Open Access Manager
- PingFederate

（注）　上記のリンクは単なる例です。公式なマニュアルについては、IdP のマニュアルを参照してください。

手順

	コマンドまたはアクション	目的
Step 1	Cisco Unified Communications Manager からの UC メタデータのエクスポート（71 ページ）	信頼関係を作成するには、ユニファイドコミュニケーションマネージャと IdP の間でメタデータファイルを交換する必要があります。
Step 2	ID プロバイダ（IdP）での SAML SSO の設定	以下のタスクを実行します。 • 信頼関係の輪を完了するために、ユニファイドコミュニケーションマネージャからエクスポートされた UC メタ

	コマンドまたはアクション	目的
		データファイルをアップロードします。 • IdP での SAML SSO の設定 • IdP メタデータファイルをエクスポートします。このファイルは、ユニファイドコミュニケーションマネージャにインポートされます。
Step 3	Cisco Unified Communications Manager での SAML SSO の有効化	IdP メタデータをインポートし、ユニファイドコミュニケーションマネージャで SAML SSO を有効にします。
Step 4	Cisco Tomcat サービスの再起動 （74 ページ）	SSO の有効化の前後には、SSO が有効になっているすべてのクラスタノードで Cisco tomcat サービスを再起動する必要があります。
Step 5	SAML SSO 設定の検証 （75 ページ）	SAML SSO が正常に設定されていることを確認します。

Cisco Unified Communications Manager からの UC メタデータのエクスポート

サービスプロバイダー (ユニファイドコミュニケーションマネージャ) から UC メタデータファイルをエクスポートするには、次の手順を使用します。信頼関係の輪を構築するために、メタデータファイルが Id プロバイダー (IdP) にインポートされます。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [SAMLシングルサインオン（SAML Single Sign-On）]** を選択します。

Step 2 [SAML シングル サインオン（SAML Single Sign-On）] ウィンドウの [SSO モード（SSO Mode）] フィールドで、以下のいずれかのオプションを選択します。

- [クラスタ全体（Cluster wide）]：クラスタで 1 つの SAML 合意。

  （注） このオプションを選択する場合は、クラスタ内のすべてのノードの tomcat サーバの証明書が同じであることを確認します。これは、マルチサーバ SAN 証明書です。

- **ノードごと**: 各ノードには個別の SAML 契約があります。

Step 3 [**SAML シングルサインオン (SAML Single sign-on**)] ウィンドウで、[**証明書 (Certificate**)] フィールドのオプションのいずれかを選択します。

- **システムで生成された自己署名証明書の使用**
- **tomcat 証明書の使用**

Step 4 [すべてのメタデータのエクスポート（Export All Metadata）] をクリックして、メタデータファイルをエクスポートします。

（注） ステップ3で [**クラスタ全体 (cluster wide**)] オプションを選択すると、クラスタのダウンロード用に1つのメタデータ XML ファイルが表示されます。ただし、[**Per node**] オプションを選択した場合は、クラスタの各ノードに対して1つのメタデータ XML ファイルがダウンロード対象として表示されます。

次のタスク

IdP で次の作業を完了します。

- ユニファイドコミュニケーションマネージャからエクスポートされた UC メタデータファイルをアップロードします。
- IdP での SAML SSO の設定
- IdP メタデータファイルをエクスポートします。このファイルは、信頼関係の輪を完了するために、ユニファイドコミュニケーションマネージャにインポートされます。

Cisco Unified Communications Manager での SAML SSO の有効化

サービスプロバイダー (ユニファイドコミュニケーションマネージャ) で SAML SSO を有効にするには、次の手順を実行します。このプロセスには、IdP メタデータのユニファイドコミュニケーションマネージャサーバへのインポートが含まれます。

重要 シスコでは、SAML SSO を有効または無効にした後に、Cisco tomcat サービスを再起動することを推奨しています。

（注） SAML SSO を有効化または無効化した後は、Cisco CallManager Admin、Unified CM IM and Presence Administration、Cisco CallManager Serviceability、および Unified IM and Presence Serviceability サービスが再起動されます。

始める前に

この手順を完了する前に、次のことを確認してください。

- IdP からエクスポートされたメタデータファイルが必要です。
- エンド ユーザ データが Unified Communications Manager データベースに同期されていることを確認します。
- Unified Communications Manager IM and Presence Cisco Sync Agent サービスが、正常にデータの同期を完了していることを確認します。[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] でこの検査のステータスを確認するには、**[診断（Diagnostics）] > [システム トラブルシュータ（System Troubleshooter）]** を選択します。データ同期が正常に完了した場合は [Sync Agent が関連データ（デバイス、ユーザ、ライセンス情報など）を使用して同期したことを確認する（Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information)）] に [テスト合格（Test Passed）] という結果が表示されます
- Cisco Unified Administration へのアクセスを可能にするために、Standard CCM Super Users グループに少なくとも 1 人の LDAP 同期済みユーザが追加されている。エンド ユーザ データの同期と LDAP 同期済みユーザのグループへの追加の詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「システムの設定」および「エンド ユーザの設定」のセクションを参照してください。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [SAML シングル サインオン（SAML Single Sign-On）]** を選択します。

Step 2 [SAML SSOの有効化（Enable SAML SSO）] をクリックして、[続行（Continue）] をクリックします。

すべてのサーバ接続が再起動されることを伝える警告メッセージが示されます。

Step 3 クラスタ全体の SSO モードを設定している場合は、**[マルチサーバー Tomcat証明書をテストする（Test for Multi server tomcat certificate）]** ボタンをクリックします。それ以外の場合は、このステップを省略できます。

Step 4 [次へ（Next）] をクリックします。

ダイアログボックスが開き、ここで IdP メタデータをインポートできます。IdP とサーバの間の信頼関係を設定するには、IdP から信頼メタデータファイルを取得して、それをすべてのサーバにインポートする必要があります。

Step 5 IdP からエクスポートしたメタデータファイルをインポートします。

a) [参照 **(Browse)**] をクリックして、エクスポートした IdP メタデータファイルを見つけて選択します。
b) [IdP メタデータのインポート（Import IdP Metadata）] をクリックします。
c) [次へ（Next）] をクリックします。
d) **[サーバーメタデータをダウンロードしてIdPにインストール（Download Server Metadata and Install on IdP）]** 画面で **[次へ（Next）]** をクリックします。

（注） [次へ（Next）] ボタンは、IdP メタデータファイルがクラスタ内の 1 つ以上のノードに正常にインポートされた場合にのみ有効になります。

Step 6 接続をテストし、設定を完了します。

a) [エンドユーザの設定（End User Configuration）] ウィンドウで、[権限情報（Permissions Information）] リストボックスから、LDAP で同期され、「標準 CCM スーパーユーザ」としての権限を持つユーザを選択します。

b) [テストを実行（Run Test）] をクリックします。

IdP ログイン ウィンドウが表示されます。

（注） テストが正常に完了するまでは、SAML SSO を有効化できません。

c) 有効なユーザ名とパスワードを入力します。

認証が成功すると、次のメッセージが表示されます。

`SSO テストに成功しました`

このメッセージが表示されたら、ブラウザ ウィンドウを閉じます。

認証に失敗するか、認証に 60 秒以上かかる場合は、「ログインに失敗しました（Login Failed）」というメッセージが IdP ログイン ウィンドウに表示されます。次のメッセージが [SAML シングル サインオン（SAML Single Sign-On）] ウィンドウに表示されます。

`SSO Metadata Test Timed Out`

IdP へのログインを再度試行するには、別のユーザを選択して別のテストを実行します。

d) [完了（Finish）] をクリックして、SAML SSO の設定を完了します。

SAML SSO が有効になり、SAML SSO に参加しているすべての Web アプリケーションが再起動されます。Web アプリケーションが再起動するまでに 1 ～ 2 分かかることがあります。

Cisco Tomcat サービスの再起動

SAML シングルサインオンの有効化または無効化の前後には、シングルサインオンが実行されているすべての Cisco Unified CM クラスタノードと IM and Presence Service クラスタノードで、Cisco Tomcat サービスを再起動します。

手順

Step 1 コマンドライン インターフェイスにログインします。

Step 2 `utils service restart Cisco Tomcat` CLI コマンドを実行します。

Step 3 シングルサインオンが有効化されているすべてのクラスタ ノードで、この手順を繰り返します。

SAML SSO 設定の検証

サービスプロバイダー (ユニファイドコミュニケーションマネージャ) と IdP の両方で SAML SSO を設定した後、ユニファイドコミュニケーションマネージャで次の手順を使用して、設定が機能していることを確認します。

始める前に

次の内容を確認します。

- Unified CM Administration の [SAMLシングルサインオンの設定（SAML Single Sign-On Configuration）] ウィンドウに、**IdP メタデータ信頼**ファイルが正常にインポートされたことが表示されます。
- サービスプロバイダーのメタデータファイルは、IdP にインストールされます。

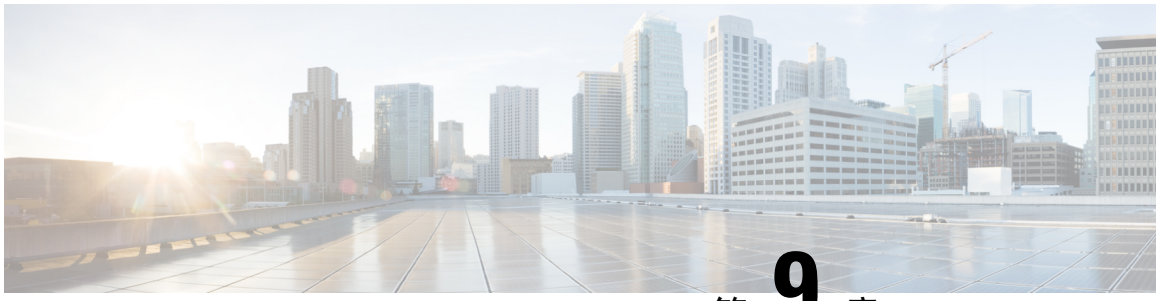
手順

Step 1 Cisco Unified CM Administration のユーザ インターフェイスで、**[システム（System）] > [SAMLシングルサインオン（SAML Single Sign-On）]** を選択して [SAMLシングルサインオンの設定（SAML Single Sign-On Configuration）] ウィンドウを開き、[次へ（Next）] をクリックします。

Step 2 [有効な管理者のユーザ名（Valid Administrator Usernames）] 領域から管理ユーザを選択し、[SSO テストの実行…（Run SSO Test…）] ボタンをクリックします。

（注） テスト用のユーザには管理者権限が必要であり、IdP サーバではユーザとして追加されています。[Valid Administrator Usernames（有効な管理者のユーザ名）] 領域には、テストの実行を指示できるユーザのリストが表示されます。

テストが成功すると、SAML SSO が正常に設定されます。



第 9 章

デバイスプールのコア設定の設定

デバイスプールの概要

デバイスプールは、デバイスのグループに対して一連の共通設定を提供します。デバイスプールは、電話、ゲートウェイ、トランク、CTI ルートポイントなどのデバイスに割り当てることができます。デバイスプールを作成すると、各デバイスを個別に設定する代わりに、各デバイスがデバイスプールの設定を継承するように関連付けることができます。

デバイスプールを使用すると、日時グループ、リージョン、電話用 NTP リファレンスなど、ロケーションに関連した情報を割り当てることによって、デバイスをロケーションに応じて設定できます。デバイスプールは必要なだけ作成できますが、通常はロケーションごとに 1 つです。ただし、デバイスプールを適用することで、職務に応じて設定を適用することもできます（たとえば会社にコールセンターがある場合、コールセンターの電話と事務管理部門の電話を別々のデバイスプールに割り当てることが考えられます）。

このセクションでは、次のように、デバイスプールのコア設定を設定するために必要な手順について説明します。

- Network Time Protocol：電話用 NTP リファレンスを設定して、デバイスプール内の SIP デバイスに NTP サポートを提供します。
- リージョン：特定のリージョンとの間のコールに使用する帯域幅とサポートされる音声コーデックを管理します。
- Cisco Unified Communications Manager グループ：デバイスに対してコール処理の冗長性と分散コール処理を設定します。

ネットワーク タイム プロトコル

NTP を使用すると、ネットワーク デバイスは、そのクロックをネットワーク タイム サーバまたはネットワーク対応のクロックと同期させることができます。NTP は、すべてのネットワークデバイスの時刻を同じにし、監査ログのタイムスタンプがネットワーク時間と一致するようにするために重要です。請求およびコール詳細レコードなどの機能は、ネットワーク上の正確なタイムスタンプに依存します。また、システム管理者は、トラブルシューティングのために監査ログに正確なタイムスタンプを必要とします。これによって、異なるシステムの監査ログを比較し、信頼できるタイムラインと一連のイベントを作成できます。

インストール時に、Unified Communications Manager パブリッシャノード用の NTP サーバをセットアップする必要があります。その後、サーバノードは、リリースサーバノードからそれらの時間を同期させます。

最大 5 個の NTP サーバを割り当てることができます。

電話用 NTP リファレンス

- **SIP 電話**の場合: 電話機の NTP 参照を設定し、デバイスプールを使用してそれらを割り当てる必要があります。これらの参照により、ネットワーク時間を提供できる適切な NTP サーバに SIP 電話が送信されます。プロビジョニングされた電話用 NTP リファレンスから SIP 電話が日時を取得できない場合、電話は Unified Communications Manager に登録したときにこの情報を受信します。
- **SCCP 電話**機の場合: 電話機の場合: 電話機は、sccp 電話機から、sccp 信号によって直接ネットワーク時間を取得できるため、電話機の NTP 参照は必要ありません。

認証済み NTP

ネットワークの NTP の領域についてネットワークセキュリティを強化するために、認証済み NTP を設定できます。認証済み NTP は、Cisco Unified Communications Manager パブリッシャノードで設定します。サブスクライバノードと IM and Presence ノードは、Unified CM パブリッシャノードから時刻を同期します。

次の認証方式のいずれかを選択できます。

- **対称キー**を使用した認証: このオプションを選択すると、ネットワーク内のデバイスは、対称キーを使用して NTP メッセージの暗号化と認証を行います。このオプションは、RedHat などのベンダーで推奨されています。
- **Autokey (PKI ベースのインフラストラクチャ)**を使用した認証: このオプションを選択すると、ネットワーク内のデバイスは、オートキープロトコルを使用して NTP メッセージを暗号化および認証します。この方法は、共通の条件に準拠するために必須です。
- **認証**なし:オートキーメソッドを使用した対称キーまたは認証を使用して認証を設定しない場合、NTP メッセージは認証されません。

リージョンの概要

リージョンは、特定のコールについて帯域幅を制限する可能性がある Unified Communications Manager のマルチサイト導入環境向けに、キャパシティ管理を提供します。たとえば、リージョンを使用して、内部コールには高い帯域幅を維持しながら、WAN リンク経由で送信されるコールの帯域幅を制限することができます。リージョンを使用すると、リージョン内またはリージョン間のコールの最大ビットレートを設定することにより、音声コールとビデオ コールの帯域幅を制限できます。

また、特定のコーデックのみをサポートするアプリケーションを使用している場合、システムはリージョンを使用してオーディオ コーデックの優先順位を設定します。サポートされているオーディオ コーデックの優先順位付きリストを設定し、特定のリージョンとの間のコールに適用することができます。

[リージョンの設定（Region Configuration）] ウィンドウで最大オーディオ ビットレートを設定する場合（または [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウのサービスパラメータを使用して）、この設定はフィルタとして機能します。コールでオーディオ コーデックが選択されると、Unified Communications Manager が、適合するコーデックをコール レッグの両側から選択し、設定された最大オーディオ ビットレートを超えるコーデックを除外して、リストに残ったコーデックの中から優先されるコーデックを選択します。

Unified Communications Manager は、最大 2000 のリージョンをサポートします。

サポートされているオーディオ コーデック

Unified Communications Manager は、ビデオ ストリームの暗号化および次の音声コーデックをサポートしています

オーディオ コーデック	説明
G.711	最も一般的にサポートされているコーデックで、Public Switched Telephone Network（PSTN; 公衆電話交換網）経由で使用されます。
G.722	ビデオ会議でよく使用されるワイドバンド コーデックです。Unified Communications Manager では常に G.711 に優先されます。ただし、G.722 が無効になっている場合を除きます。
G.722.1	24 kb/s および 32 kb/s で動作する、低複雑度のワイドバンド コーデックです。G.722 と同様のオーディオ品質を、半分以下のビット レートで実現します。
G.728	ビデオ エンドポイントがサポートする低ビット レート コーデックです。
G.729	Cisco IP 電話 7900 にサポートされる 8 kb/s 圧縮を使用する低ビットレートコーデックで、通常 WAN リンクでの発信に使用されます。

オーディオ コーデック	説明
GSM	Global System for Mobile Communications（GSM）コーデックです。GSM は Unified Communications Manager で動作するように、GSM ワイヤレス ハンドセットに対して MNET システムを有効にします。
L16	Advanced Audio Coding-Low Delay（AAC-LD）は、優れた品質の音声や音楽を提供する超広帯域オーディオ コーデックです。このコーデックは、低ビット レートの古いコーデックに対してさえ同等あるいはより良い音質を提供します。
AAC-LD（mpeg4-generic）	SIP（Session Initiation Protocol）デバイス、特に Cisco TelePresence Systems でサポートされます。
AAC-LD（MP4A-LATM）	Low-overhead MPEG-4 Audio Transport Multiplex（LATM）は、優れた音質を提供する超広帯域オーディオ コーデックです。Tandberg やいくつかのサードパーティ エンドポイントを含む SIP（Session Initiation Protocol）デバイスでサポートされます。 （注） AAC-LD（mpeg4-generic）や AAC-LD（MPA4-LATM）とは互換性がありません。
Internet Speech Audio Codec（iSAC）	特に低ビット レートと中ビット レートのアプリケーション両方で、低遅延のワイドバンド音質を提供するように設計された適応型広帯域オーディオ コーデックです。
インターネット低ビット レート コーデック（iLBC）	独立してエンコードされた音声フレームが原因の損失性ネットワークにおいて音声品質のグレースフルデグラデーションを可能にしつつ、15.2 kb/s と 13.3 kb/s のビット レートで G.711 から G.729 の間の音声品質を提供します。iLBC は、SIP、SCCP、H323、MGCP デバイスでサポートされています。 （注） H.323 アウトバンド FastStart は、iLBC コーデックをサポートしません。
アダプティブ マルチレート（AMR）	GSM に基づく、2.5G/3G ワイヤレス ネットワークで必須の標準規格コーデックです（WDMA、EDGE、GPRS）。このコーデックは、7.4 kb/s 以上のトール品質音声により、4.75 kb/s から 12.2 kb/s の範囲の可変ビット レートでナローバンド（200 ～ 3400 Hz）信号をエンコードします。AMR は SIP（Session Initiation Protocol）デバイスでのみサポートされます。

オーディオ コーデック	説明
アダプティブ マルチレート ワイドバンド（AMR-WB）	G.722.2 として体系化されており、公式にはワイドバンドとして知られる ITU-T 標準規格音声コーデックは、音声を約 16 kb/s で符号化します。このコーデックは、50 Hz から 7000 Hz の広い音声帯域幅により、優れた音声品質を提供するので、AMR や G.711 などの他のナローバンド音声コーデックに優先されます。AMR-WB は SIP（Session Initiation Protocol）デバイスでのみサポートされます。
Opus	Opus コーデックは、インタラクティブな音声およびオーディオコーデックで、特に Voice over IP、ビデオ会議、ゲーム内チャットやライブ配信される音楽演奏などの多様なインタラクティブ オーディオアプリケーションを処理するために設計されています。 このコーデックは、6 kb/s から 510 kb/s までのナローバンド低ビット レートから超高ビット レートまでをサポートします。 Opus codec のサポートは、すべての SIP デバイスでデフォルトで有効になっています。**Opus Codec Enabled**サービスパラメータを使用して Opus サポートを再構成できます (デフォルト設定は、**すべてのデバイスで有効になっています**)。このパラメータを再設定することで、Opus codec のサポートを無効にしたり、非録音デバイスのみのサポートを有効にしたりできます。 （注） Opusには g.722 コーデックへの依存関係があります。SIP デバイスで Opus を使用するためには、[G.722コーデックのアドバタイズ（Advertise G.722 Codec）] エンタープライズパラメータも [有効（Enabled）] に設定する必要があります。

Cisco Unified CM グループの概要

Unified Communications Manager グループは、デバイスが登録できる最大 3 台の冗長構成のサーバについての、優先順位付きリストです。各グループには、1 個のプライマリ ノードと最大 2 個のバックアップ ノードが含まれます。ノードをリストする順序によって、1 番目のノードがプライマリ ノード、2 番目のノードがバックアップ ノード、3 番目のノードが第 3 ノードとして優先順位が決定されます。[デバイスプールの設定（Device Pool Configuration）] を使用して、Cisco Unified Communictions Manager グループにデバイスを割り当てることができます。

Unified Communications Manager グループは、システムに 2 つの重要な機能を提供します。

- コール処理の冗長性：デバイスが登録するときに、そのデバイスプールに割り当てられているグループ内のプライマリ（1 番目）Unified Communications Manager への接続を試みます。プライマリ Unified Communications Manager が使用可能ではない場合、デバイスは最初のバックアップ ノードに接続しようとし、そのノードが使用可能ではない場合は、第 3 のノードに接続を試みます。各デバイスプールには Unified Communications Manager グループが 1 つ割り当てられます。

- 分散コール処理：複数のデバイスプールと Unified Communications Manager グループを作成することで、デバイスの登録を複数の Unified Communications Manager に均等に分散できます。

ほとんどのシステムでは、より適切な負荷分散と冗長性を実現するために、複数のグループに対して Unified Communications Manager を割り当てます。

コール処理の冗長性

Unified Communications Manager グループは、コール処理の冗長性と回復の機能を提供します。

- フェールオーバー：グループのプライマリ Unified Communications Manager で障害が発生し、そのグループのバックアップ Unified Communications Manager にデバイスが再登録するときに実行されます。
- フォールバック：障害が発生したプライマリ Unified Communications Manager が復旧し、そのグループのデバイスがプライマリ Unified Communications Manager に再登録されるときに実行されます。

通常動作では、グループ内のプライマリ Unified Communications Manager は、電話およびゲートウェイなど、そのグループに関連付けられたすべての登録デバイスのコール処理を制御します。

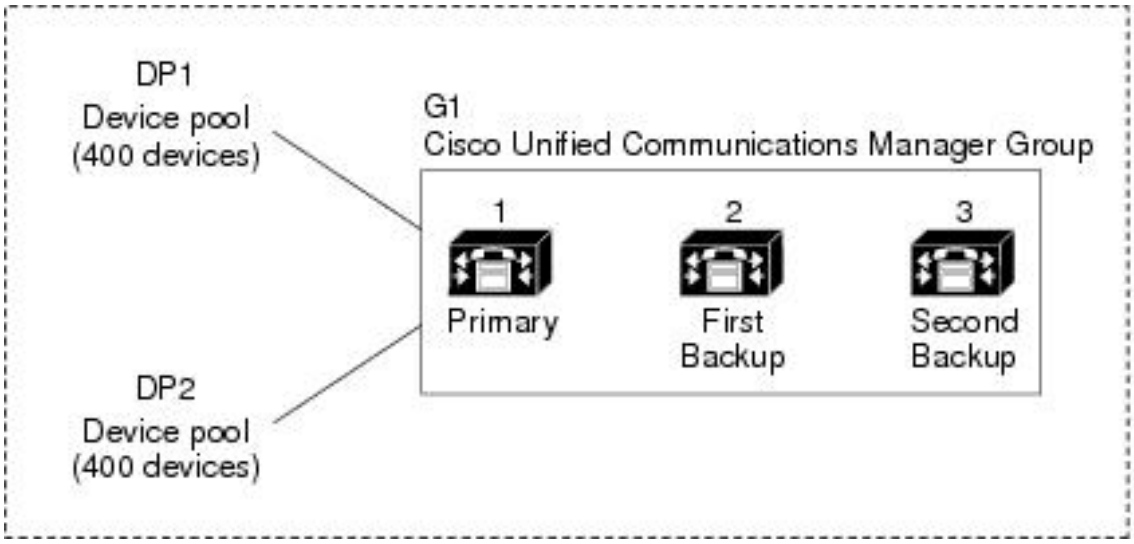
プライマリの Unified Communications Manager で何らかの理由で障害が発生した場合、グループの 1 番目のバックアップ Unified Communications Manager が、プライマリ Unified Communications Manager に登録されたデバイスを制御します。グループに 2 番目のバックアップ Unified Communications Manager を指定する場合、プライマリと 1 番目のバックアップ両方の Unified Communications Manager で障害が発生した場合には、2 番目がデバイスを制御します。

障害が発生したプライマリ Unified Communications Manager の機能が回復すると、グループの制御が戻り、そのグループのデバイスは自動的にプライマリ Unified Communications Manager に再登録されます。

例

たとえば、次の図は、1 つのグループに 3 つの Unified Communications Manager があり、800 台のデバイスを制御しているシンプルなシステムを示しています。

図 *4 : Unified Communications Manager* グループ



この図には、DP1 と DP2 の 2 つのデバイスプールが割り当てられた Unified Communications Manager グループ G1 が示されています。Unified Communications Manager 1 は、グループ G1 のプライマリ Unified Communications Manager として、通常動作時には DP1 と DP2 の 800 台のデバイスをすべて制御します。Unified Communications Manager 1 で障害が発生すると、800 台のデバイスの制御は Unified Communications Manager 2 に移ります。Unified Communications Manager 2 でも障害が発生すると、800 台のデバイスの制御は Unified Communications Manager 3 に移ります。

この構成ではコール処理に冗長性が提供されますが、この例の 3 つの Unified Communications Manager 間では、コール処理の負荷はうまく分散されていません。Unified Communications Manager グループとデバイスプールを使用して、クラスタ内で分散コール処理を提供する方法については、次のトピックを参照してください。

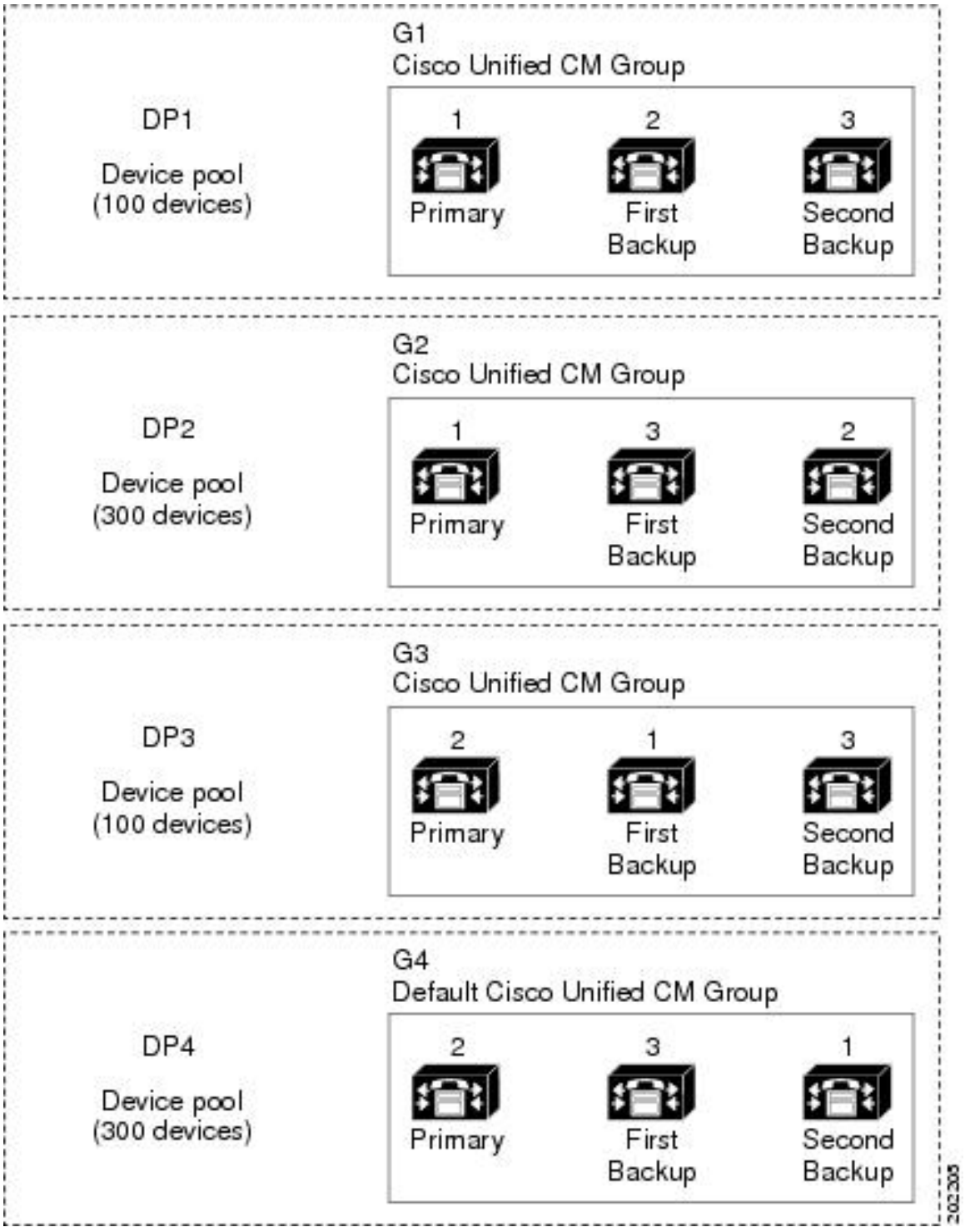
（注） 空の Unified Communications Manager グループは機能しません。

分散コール処理

Unified Communications Manager グループは、コール処理の冗長化と分散型コール処理の両方を実現します。デバイス、デバイスプール、および Unified Communications Manager をどのようにグループに割り当てるかによって、システムの冗長性とロード バランシングのレベルが決まります。

多くの場合、グループ内の 1 つの Unified Communications Manager に障害が起きたら、他の Unified Communications Manager が過負荷にならないようにデバイスを分散する必要があります。次の図は、3 つの Unified Communications Manager と 800 台のデバイスから成るシステムで分散型コール処理と冗長化を実現するために、Unified Communications Manager グループとデバイスプールを設定する方法の一例を示しています。

図 *5:* 分散型コール処理と組み合わせた冗長化



この図は、設定されてデバイスプールに割り当てられた Unified Communications Manager グループを表します。Unified Communications Manager 1 は、G1 と G2 の 2 つのグループでプライマリコン

トローラとして機能します。Unified Communications Manager 1 で障害が発生した場合、デバイスプール DP1 の 100 台のデバイスは Unified Communications Manager 2 に再登録され、DP2 の 300 台のデバイスはUnified Communications Manager 3 に再登録されます。同様に、Unified Communications Manager 2 は、グループ G3 と G4 のプライマリコントローラとして機能します。Unified Communications Manager 2 で障害が発生した場合、DP3 の 100 台のデバイスは Unified Communications Manager 1 に再登録され、DP4 の 300 台のデバイスはUnified Communications Manager 3 に再登録されます。Unified Communications Manager 1 と Unified Communications Manager 2 の両方で障害が発生した場合は、すべてのデバイスが Unified Communications Manager 3 に再登録されます。

デバイスプールの前提条件

デバイスプールは、設定する前に、適切に計画してください。デバイスプールおよび冗長構成の Unified Communications Manager グループを設定する場合は、電話機向けにサーバの冗長性を提供すると同時に、登録を複数のクラスタに均等に分散させることを推奨します。システムについて計画を立てる際に使用できる詳細情報については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html にある『*Cisco Collaboration* システム ソリューション リファレンス ネットワーク デザイン』を参照してください。

Unified Communications Manager に最新のタイム ゾーン情報が含まれるようにするには、Unified Communications Manager のインストール後に、タイム ゾーン情報を更新する Cisco Options Package（COP）ファイルをインストールすることができます。大規模なタイム ゾーン変更イベント後には、最新の COP ファイルを https://software.cisco.com/download/navigator.html でダウンロードできることをお知らせします。

CMLocal の設定をローカルの日付と時刻に変更します。

デバイスプールの追加設定

この章では、Unified Communications Manager グループを使用した、電話用 NTP リファレンス、リージョン、コール処理の冗長性などの主な設定について説明します。ただし、デバイスプール設定を使用して次のオプション機能とコンポーネントをデバイスに適用することもできます。

- メディアリソース：会議ブリッジなどのメディアリソースと、保留音（MOH）を、デバイスプール内のデバイスに割り当てます。詳細については、本ドキュメントの「メディアリソース構成タスクフロー」のセクションを参照してください。
- Survivable Remote Site Telephony（SRST）：導入環境で WAN 接続を使用している場合は、SRST を設定することで、WAN が停止した場合に IP ゲートウェイが限定的なコール サポートを提供できるようになります。詳細については、本ドキュメントの「*Survivable Remote Site Telephony* の設定タスクフロー」のセクションを参照してください。
- コールルーティング情報：クラスタ間でコールをルーティングする方法の詳細については、本ドキュメントの「コールルーティングの設定タスクフロー」のセクションを参照してください。

- デバイス モビリティ：デバイス モビリティ グループを設定することで、デバイスが物理的な場所に基づいて設定を使用できるようになります。詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「デバイス モビリティの設定」の章を参照してください。

デバイスプールのコア設定の設定タスクフロー

デバイスプールをセットアップし、リージョン、電話用 NTP リファレンス、およびそのデバイスプールを使用するデバイスの冗長性などの設定を適用するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
Step 1	Network Time Protocol の設定 （86 ページ）	このタスクフローのタスクを実行して、システムに NTP をセットアップします。電話機の NTP 参照を設定し、デバイスプールに割り当てることができる日付/時刻グループにそれらを適用します。
Step 2	リージョンの関係の設定 （93 ページ）	これらのタスクを実行して、システムのリージョンを設定します。最大で 2,000 のリージョンを作成し、リージョンで提供できる内容に基づいて、カスタマイズしたオーディオ コーデック設定やビット レート制限など、カスタマイズした設定を指定できます。
Step 3	Cisco Unified CM グループの設定 （94 ページ）	コール処理の冗長性と負荷分散のための Unified Communications Manager グループを構成します。
Step 4	デバイスプールの設定 （95 ページ）	システム デバイスのデバイスプールを設定します。設定された他のコア設定をデバイスプールに適用します。これらの設定をこのデバイスプールを使用するデバイスに適用します。

Network Time Protocol の設定

システムの Network Time Protocol（NTP）を設定するには、次のタスクを完了します。電話機の NTP 参照を設定し、これらの参照を日付/時刻グループに適用して、デバイスプールに適用できるようにします。

手順

	コマンドまたはアクション	目的
Step 1	NTP サーバの追加 （87 ページ）	（オプション）NTP サーバを追加する必要がある場合は、この手順を使用します。最大5台のNTPサーバーを追加できます。 （注） システムのインストール時に、Unified Communications Manager を 1 台の NTP サーバにポイントするように要求されました。NTP サーバを追加する場合は、この手順を使用することができます。その他の場合は、このタスクをスキップします。
Step 2	次のいずれかの方法を選択して、NTP メッセージを認証します。 • 対称キー経由での NTP 認証キーの設定 （88 ページ） • オートキー経由での NTP 認証キーの設定 （88 ページ）	（オプション）セキュリティを強化するには、認証済み NTP を設定します。認証を設定するには、対称キーを使用するか、またはキーを使用する必要があります。オートキー メソッドは、共通の条件に準拠するために必要です。
Step 3	電話用 NTP リファレンスの設定 （89 ページ）	SIP 電話では、電話用 NTP リファレンスを設定してから、日時グループとデバイス プールを介してそれらを適用する必要があります。
Step 4	日時グループの追加 （90 ページ）	システムに接続されているさまざまなデバイスのタイム ゾーンを定義し、設定した電話用 NTP リファレンスを適切な日時グループに割り当てます。

（注） `utils ntp*` コマンド セットなど、NTP のトラブルシューティングと設定に使用する CLI コマンドの詳細については、『コマンドライン インターフェイス リファレンス ガイド』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

NTP サーバの追加

NTP サーバを Unified Communications Manager に追加します。

（注） [Cisco Unified OSの管理（Cisco Unified OS Administration）] ウィンドウで **[設定（Settings）] > [NT サーバ（NTP Servers）]** を選択して、[NTP サーバの設定（NTP Server Configuration）] ウィンドウで NTP サーバを追加することもできます。

手順

Step 1 コマンドライン インターフェイスにログインします。

Step 2 パブリッシャノードが NTP サーバに到達できることを確認するには、**utils network ping <ip_address>** を実行します。このとき、ip_address は NTP サーバのアドレスを表します。

Step 3 サーバに到達可能であれば、`utils ntp server add <ip_address>` を実行してサーバを追加します。

Step 4 `utils ntp restart` コマンドを使用して NTP サービスを再起動します。

対称キー経由での NTP 認証キーの設定

対称キーを使用してネットワークで NTP メッセージを認証するには、次の手順を実行します。

（注） SHA1 キーは必ず 1 文字ずつ入力してください。現在、CLI フレームワークは貼り付けられた値を読み取りません。

手順

Step 1 Cisco Unified Communications Manager パブリッシャノードで、コマンドライン インターフェイスにログインします。

Step 2 `utils ntp auth-symmetric key status` コマンドを実行して、現在の NTP 認証設定のステータスを確認します。

Step 3 次のいずれかを実行します。

- 対称キーによる NTP 認証を有効化するには、CLI コマンド `utils ntp auth symmetric-key enable` を実行します。
- 対称キーによる NTP 認証を無効化するには、CLI コマンド `utils ntp auth symmetric-key disable` を実行します。

Step 4 プロンプトに従って、NTP サーバのキー ID と対称キーを入力します。

オートキー経由での NTP 認証キーの設定

PKI ベースの自動キーを使用して NTP 認証を設定する場合は、次の手順を使用します。

（注） 対称キーを使用した NTP 認証が有効になっている場合は、自動キーによる認証を有効にする前に、その設定を無効にする必要があります。対称キーを使用した NTP 認証を無効化するには、「対称キー経由での NTP 認証キーの設定 （88 ページ）」を参照してください。

始める前に

オートキーを介したNTP認証を有効にするには、共通条件モードを有効にする必要があります。コモン クライテリア モードを有効にする方法の詳細については、『*Cisco Unified Communications Manager* セキュリティガイド』の「FIPS セットアップ」の章を参照してください。

手順

Step 1 コマンドライン インターフェイスにログインします。

Step 2 `utils ntp auth auto-key status` コマンドを実行して、現在の NTP 認証設定を確認します。

Step 3 次のいずれかを実行します。

- NTP 認証を有効化するには、CLI コマンド **utils ntp auth auto-key enable** を実行します。
- NTP 認証を無効化するには、CLI コマンド **utils ntp auth auto-key disable** を実行します。

Step 4 NTP 認証を有効または無効にする NTP サーバの番号を入力します。

Step 5 認証を有効にする場合は、IFF クライアントキーを入力します。NTP サーバのクライアントキーを貼り付けます。

電話用 NTP リファレンスの設定

SIP 電話に必須の電話用 NTP リファレンスを設定するには、この手順を使用します。作成した NTP リファレンスは、日時グループを使用してデバイスプールに割り当てることができます。このリファレンスは、ネットワーク時刻を提供できる適切な NTP サーバに SIP 電話をポイントします。SCCP 電話機の場合、この設定は必要ありません。

（注） Unified Communications Manager は、マルチキャスト モードおよびエニーキャスト モードをサポートしていません。これらのモードを選択した場合ではデフォルトのダイレクト ブロードキャスト モードに設定されます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [電話用NTPリファレンス（Phone NTP Reference）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 電話機が使用するアドレス方式に従って、NTP サーバの IPv4 アドレス、または IPv6 アドレスを入力します。

（注） 電話用 NTP リファレンスの保存には、IPv4 アドレスまたは IPv6 アドレスのいずれかの入力が必要です。IPv4 電話と IPv6 電話の両方を展開している場合、NTP サーバに、IPv4 アドレスと IPv6 アドレスの両方を設定します。

Step 4 [説明（Description）] フィールドに、電話用 NTP リファレンスの説明を入力します。

Step 5 [モード（Mode）] ドロップダウンリストで、電話用NTPリファレンスのモードを次のオプションから選択します。

- [ユニキャスト（Unicast）]：このモードを選択すると、電話機は、指定した NTP サーバに NTP クエリ パケットを送信します。
- [ダイレクト ブロードキャスト（Directed Broadcast）]：このデフォルトの NTP モードを選択すると、電話機は任意のNTPサーバの日時情報を利用しますが、リストされているNTPサーバ（1 番目 = プライマリ、2 番目 = セカンダリ）を優先します。

（注） Cisco TelePresence および Cisco Spark デバイス タイプは、ユニキャスト モードのみをサポートします。

Step 6 [保存（Save）] をクリックします。

次のタスク

電話用NTPリファレンスを日時グループに割り当てます。詳細については、「日時グループの追加 （90 ページ）」を参照してください。

日時グループの追加

システムのタイム ゾーンを定義するための日時グループを設定します。設定した電話用 NTP リファレンスを、適切なグループに割り当てます。新しい日時グループをデータベースに追加した後で、そのグループをデバイスプールに割り当てることで、デバイスプール内のすべてのデバイスで日付と時刻の情報を設定することができます。

変更を適用するには、デバイスをリセットする必要があります。

ヒント Cisco IP Phone が世界中に分布している場合は、タイムゾーンごとに日時グループを作成します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]** > **[日時グループ（Date/Time Group）]** の順に選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 このグループに NTP リファレンスを割り当てます。

a) [電話用NTPリファレンスの追加（Add Phone NTP References）] をクリックします。

b) [電話用NTPリファレンスの検索と一覧表示（Find and List Phone NTP References）] ポップアップ ウィンドウで、[検索（Find）] をクリックして、前のタスクで設定した電話用 NTP リファレンスを選択します。

c) [選択項目の追加（Add Selected）] をクリックします。

d) 複数の参照を追加した場合は、上下の矢印を使用して優先順位を変更します。上部にある参照は、優先順位が高くなります。

Step 4 残りのフィールドを**日付と時刻**のセットウィンドウに設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 5 [保存（Save）] をクリックします。

リージョンの設定

デバイスプールのリージョンを設定するには、次のタスクを実行します。リージョン間の関係を設定して、より適切に帯域幅を管理します。リージョンを使用して、特定のタイプのコール（ビデオ コールなど）の最大ビット レートを制御し、特定のオーディオ コーデックに優先順位を設定することができます。

手順

	コマンドまたはアクション	目的
Step 1	音声コーデック設定のカスタマイズ（92 ページ）	（オプション）この手順は、使用しているオーディオコーデックの優先順位をカスタマイズする場合に使用します。このようにして、特定のオーディオコーデックを他のコーデックの先で優先することができます。それ以外の場合は、デフォルトのオーディオコーデックリストのいずれかをデバイスプールに割り当てることができます。
Step 2	リージョンにおけるクラスタ全体のデフォルト値の設定 （92 ページ）	リージョンにおけるクラスタ全体のデフォルト値を設定します。[リージョンの設定（Region Configuration）] で異なる値を設定しない限り、すべてのリージョンでこのデフォルト値が使用されます。
Step 3	リージョンの関係の設定 （93 ページ）	新しいリージョンを設定するか、既存のリージョンの設定を編集します。リージョン間およびリージョン内の両方のコールについて、関係を設定します。

音声コーデック設定のカスタマイズ

オーディオ コーデックの優先順位をカスタマイズするには、この手順を使用します。既存のリストから設定をコピーして新しいオーディオ コーデックの初期設定リストを作成し、新しいリストで優先順位を編集します。

（注） オーディオコーデックの優先順位をカスタマイズする必要がない場合は、このタスクを省略できます。デバイスプールを設定するときに、デフォルトのオーディオ コーデックの初期設定リストのいずれかを割り当てることができます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [リージョン情報（Region Information）] > [オーディオコーデックの初期設定リスト（Audio Codec Preference List）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [オーディオコーデックの初期設定リスト（Audio Codec Preference Lists）] ドロップダウンリストボックスから、既存のオーディオコーデックの初期設定リストのいずれかを選択します。
選択したリストに対して、優先順位付きのオーディオ コーデック リストが表示されます。

Step 4 [コピー（Copy）] をクリックします。コピー元のリストでの優先順位付きリストが、新しく作成したリストに適用されます。

Step 5 新しいオーディオ コーデック リストの [名前（Name）] を編集します。たとえば、`customizedCodecList` のように設定します。

Step 6 [説明（Description）] を編集します。

Step 7 [リスト内のコーデック（Codecs in List）] リストボックスに表示される優先順位内でコーデックを移動させるには、上向き矢印と下向き矢印を使用します。

Step 8 [保存（Save）] をクリックします。

新しいリストをリージョンに適用してから、そのリージョンをデバイスプールに適用する必要があります。デバイスプール内のすべてのデバイスで、このオーディオコーデックの初期設定リストが使用されます。

リージョンにおけるクラスタ全体のデフォルト値の設定

リージョンのデフォルト値を設定するには、次の手順を使用します。これらの設定は、[リージョンの設定（Region Configuration）] ウィンドウ内の個々のリージョンに対してリージョンの関係を設定していない限り、デフォルトですべてのリージョンに対するコールに適用されます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 [サーバ（Server）] ドロップダウンリストから、Unified Communications Manager パブリッシャノードを選択します。

Step 3 [**サービス（Service**）] ドロップダウンリストから、**Cisco CallManager** サービスを選択します。[サービスパラメータ設定（Service Parameter Configuration）] ウィンドウが表示されます。

Step 4 [クラスタ全体のパラメータ（システム-ロケーションとリージョン）（Clusterwide Parameters (System Location and Region)）] で、必要な新しいサービスパラメータ設定を入力します。サービスパラメータの説明については、パラメータ名をクリックしてヘルプの説明を参照してください。

Step 5 [保存（Save）] をクリックします。

リージョンの関係の設定

リージョンを作成し、特定のリージョン間のコールにカスタム設定を割り当てるには、この手順を使用します。優先するオーディオ コーデックおよび最大ビットレートなどの設定を編集できます。たとえば、ネットワークの他の部分よりも帯域幅が小さいリージョンがある場合は、そのリージョンに対するビデオコールのセッション ビットレートの最大値を編集することができます。この値は、そのリージョンで提供可能な値にリセットすることができます。

（注） 拡張性を高めるため、また、システムが使用するリソースを少なくするために、[サービスパラメータの設定（Service Parameters Configuration）] ウィンドウでは、できるだけデフォルト値を使用することを推奨します。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [リージョン情報（Region Information）] > [リージョン（Regions）]** を選択します。

Step 2 次のいずれかを実行します。

- **[検索（Find）]** をクリックします。
- **[新規追加（Add New）]**をクリックして新しいパーティションを作成します。
- リージョンの [名前（Name）] を入力します。たとえば「`NewYork`」と入力します。
- [保存（Save）] をクリックします。

読み取り専用の [リージョンの関係（Region Relationships）] 領域には、選択したリージョンと別のリージョンの間で設定したカスタマイズ済みの設定が表示されます。

Step 3 このリージョンと別のリージョンの間（またはリージョン内コールの場合は同一リージョン）の設定を変更するには、[他のリージョンとの関係を変更（Modify Relationships to other Regions）] 領域の設定を編集します。

a) [リージョン（Region）] 領域で、他方のリージョンを強調表示します（リージョン内コールの場合は、設定中の同じリージョンを強調表示します）。

b) 隣接するフィールドの設定を編集します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

c) [保存（Save）] をクリックします。
新しい設定が、[リージョンの関係（Region Relationships）] 領域にカスタム ルールとして表示されます。

（注） 一方のリージョン内でリージョンの関係を編集すると、その設定が他方のリージョンで自動的に更新されるため、他のリージョンにその設定を複製する必要はありません。たとえば、[リージョンの設定（Region Configuration）] ウィンドウでリージョン1を開き、リージョン2とのカスタム関係を設定するとします。次にリージョン2を開くと、[リージョンの関係（Region Relationships）] 領域にカスタム関係が表示されます。

Cisco Unified CM グループの設定

デバイスプール内のデバイスに対して、コール処理の冗長性、ロードバランシング、およびフェールオーバーを行うための Unified Communications Manager グループを設定するには、この手順を使用します。

ヒント クラスタノード間でデバイス登録が均等に分散される分散コール処理を提供するために、複数のグループとデバイスプールを設定して、各グループのプライマリサーバがそれぞれ異なるようにします。

（注） デフォルトサーバグループは名前から内容がわからず、混乱が起きる可能性があるため、使用しないでください。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [Cisco Unified CMグループ（Cisco Unified CM Group）]** を選択します。

Step 2 [名前（Name）] にグループの名前を入力します。

（注） グループを簡単に区別できるように、名前でノードの順序を識別することを検討してください。たとえば、CUCM_PUB-SUB のような名前にします。

Step 3 この Unified Communications Manager グループを、自動登録を有効化したときのデフォルトの Unified Communications Manager グループにする場合は、[自動登録のCisco Unified Communications Managerグループ（Auto-registration Cisco Unified Communications Manager Group] チェックボックスをオンにします。

Step 4 [使用可能なCisco Unified Communications Manager （Available Cisco Unified Communications Managers）] のリストから、このグループに追加するノードを選択し、下向き矢印をクリックして選択します。グループには最大 3 台のサーバを追加できます。
このグループのサーバは、[選択されたCisco Unified Communications Manager（Selected Cisco Unified Communications Managers）] リスト ボックスに表示されます。リストの 1 番上にあるサーバがプライマリ サーバです。

Step 5 プライマリ サーバおよびバックアップ サーバを変更するには、[選択されたCisco Unified Communications Manager（Selected Cisco Unified Communications Managers）] リスト ボックスの横にある矢印を使用します。

Step 6 [保存（Save）] をクリックします。

デバイスプールの設定

システム デバイスのデバイスプールを設定します。設定された他のコア設定をデバイスプールに適用します。これらの設定をこのデバイスプールを使用するデバイスに適用します。導入のニーズに合わせて、複数のデバイスプールを設定できます。

始める前に

SRST 設定を割り当てる場合は、「Survivable Remote Site Telephony の設定タスクフロー（132 ページ）」を参照してください。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]** > **[デバイスプール（Device Pool）]** を選択します。

Step 2 次のいずれかを実行します。

- [新規追加（Add New）] をクリックして新しいデバイスプールを作成します。
- [検索（Find）] をクリックし、既存のデバイス グループを選択します。

Step 3 [デバイスプール名（Device Pool Name）] フィールドに、デバイスプールの名前を入力します。

Step 4 [Cisco Unified Communications Managerグループ（Cisco Unified Communications Manager Group）] ドロップダウンで、コール処理の冗長性と負荷分散を処理するように設定したグループを選択します。

Step 5 [日時グループ（Date/Time Group）] ドロップダウンリストから、このデバイスプールを使用するデバイスの日付、時刻、および電話用 NTP リファレンスを処理するように設定したグループを選択します。

Step 6 [リージョン（Region）] ドロップダウンリストボックスから、このデバイスプールに適用するリージョンを選択します。

Step 7 [メディアリソースグループリスト（Media Resource Group List）] ドロップダウンリストから、このデバイスプールに適用するメディアリソースが含まれるリストを選択します。

Step 8 このデバイスプールに SRST 設定を適用します。

a) [SRSTリファレンス（SRST Reference）] ドロップダウンリストから、SRST リファレンスを割り当てます。

b) [接続モニタ時間（Connection Monitor Duration）] フィールドに値を割り当てます。この設定では、電話機が SRST から登録解除して Unified Communications Manager に再登録するまでに、Unified Communications Manager との接続をモニタする時間を定義します。

Step 9 [デバイスプールの設定（Device Pool Configuration）] ウィンドウで、残りのフィールドに入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 10 [保存（Save）] をクリックします。

次のタスク

導入要件に応じて、複数のデバイスプールを設定します。

基本的なデバイスプール設定フィールド

表 *5:* 基本的なデバイスプール設定フィールド

フィールド	説明
デバイスプール名（Device Pool Name）	新しいデバイスプールの名前を入力します。名前は最大50文字までで、英数字、ピリオド（.）、ハイフン（-）、アンダースコア（_）、および空白を使用できます。
Cisco Unified CMグループ（Cisco Unified Communications Manager Group）	このデバイスプール内のデバイスに割り当てる Cisco Unified Communications Manager グループを選択します。Cisco Unified Communications Manager グループでは、最大3つの Unified Communications Manager ノードについて優先順位を設定したリストを指定します。リストの最初のノードはそのグループのプライマリ ノードとして動作し、グループの他のメンバーは、冗長性のためのバックアップ ノードとして動作します。
日時グループ（Date/Time Group）	このデバイスプール内のデバイスに割り当てる日時グループを選択します。日時グループは、タイム ゾーンと日時の表示形式を指定します。
リージョン（Region）	このデバイスプール内のデバイスに割り当てるリージョンを選択します。リージョンの設定値は、リージョン内および他のリージョン間でコールに使用できる音声コーデックを指定します。

コール保持

Unified Communications Manager のコール保留機能は、Unified Communications Manager で障害が発生したとき、またはコールをセットアップする Unified Communications Manager とデバイスの間の通信で障害が発生したときに、コールが中断しないようにするものです。

Unified Communications Manager は、幅広い Cisco Unified Communications デバイスに対してコール保存を完全にサポートしています。このサポートには、Cisco Unified IP Phone、Foreign Exchange Office（FXO）（非ループスタート トランク）および Foreign Exchange Station（FXS）インターフェイスをサポートする Media Gateway Control Protocol（MGCP）ゲートウェイが含まれ、会議ブリッジ、MTP、およびトランスコーディング リソース デバイス間のコール保持もある程度含まれます。

高度なサービスパラメータ、[ピアがH.323コールを保持できるようにする（Allow Peer to Preserve H.323 Calls）] を [True] に設定することで、H.323 コール保持を有効にします。

次のデバイスおよびアプリケーションは、コール保持をサポートしています。双方が以下のいずれかのデバイスを介して接続すると、Unified Communications Manager はコール保存を維持します。

- Cisco Unified IP Phone
- SIP トランク
- ソフトウェア会議ブリッジ
- ソフトウェア MTP
- ハードウェア会議ブリッジ（Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module、Cisco Catalyst 4000 Access Gateway Module）
- トランスコーダ（Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module、Cisco Catalyst 4000 Access Gateway Module）
- 非 IOS の MGCP ゲートウェイ（Catalyst 6000 24 Port FXS Analog Interface Module、Cisco DT24+、Cisco DE30+、Cisco VG200）
- Cisco IOS H.323 ゲートウェイ（Cisco 2800 シリーズ、Cisco 3800 シリーズなど）
- Cisco IOS MGCP ゲートウェイ（Cisco VG200、Catalyst 4000 Access Gateway Module、Cisco 2620、Cisco 3620、Cisco 3640、Cisco 3660、Cisco 3810）
- Cisco VG248 Analog Phone Gateway

次のデバイスとアプリケーションでは、コール保存をサポートしていません。

- アナンシエータ
- H.323 エンドポイント（NetMeeting またはサードパーティの H.323 エンドポイントなど）
- CTI アプリケーション
- TAPI アプリケーション

- JTAPI アプリケーション

コール保持のシナリオ

次の表で、さまざまなシナリオでコール保存がどのように処理されるのかを説明します。

表 *6*: コール保持のシナリオ

シナリオ	コール保持の処理
Cisco Unified Communications Managerで障害が発生した場合。	Cisco Unified Communications Manager で障害が発生すると、障害が発生した Unified Communications Manager によってセットアップされたすべてのコールのコール処理機能が失われます。 Cisco Unified Communications Manager は、エンドユーザーがコールを終了するか、メディア接続の解放をデバイスが判別できるまで、影響を受けるアクティブなコールを維持します。ユーザーは、この障害の結果として維持されているコールに対して、コール処理機能を呼び出すことはできません。

シナリオ	コール保持の処理
Cisco Unified Communications Managerとデバイスの間で通信障害が発生した場合。	デバイスとそれを制御する Cisco Unified Communications Manager との間で通信障害が発生すると、デバイスが障害を認識し、アクティブな接続を維持します。Cisco Unified Communications Manager が通信障害を認識し、通信が失われたデバイスでのコールに関連付けられているコール処理エンティティを消去します。 Cisco Unified Communications Manager は、影響を受けるコールに関連付けられている、障害が発生していないデバイスの制御を維持します。Cisco Unified Communications Manager は、エンドユーザーがコールを終了するか、メディア接続の解放をデバイスが判別できるまで、影響を受けるアクティブなコールを維持します。ユーザーは、この障害の結果として維持されているコールに対して、コール処理機能を呼び出すことはできません。 （注） • フェールオーバーが実行された場合、キープアライブタイマー内で Cisco Unified Communications Manager ノードを表示すると、コールが保存モードになっていても、電話機は現在のノードに登録されたままになります。これは、キープアライブ タイマーが有効である場合に発生する可能性があります。 • ピアが SIP トランクであり、IP Phone と SIP トランクの間でコールが確立されるシナリオを考えます。電話機が Cisco Unified Communications Manager との通信を失った場合、トランク側からのメディア変更は、理由ヘッダーに原因値 38（ネットワークエラー）を含む488（受け入れられないメディア）応答になります。
デバイスの故障 （電話機、ゲートウェイ、会議ブリッジ、トランスコーダ、MTP）	デバイスに障害が発生すると、デバイス経由で存在する接続によってストリーミング メディアが停止します。アクティブなCisco Unified Communications Manager は、デバイスの障害を認識し、障害が発生したデバイスでのコールに関連付けられているコール処理エンティティを消去します。 Cisco Unified Communications Manager は、影響を受けるコールに関連付けられている、障害が発生していないデバイスの制御を維持します。問題が発生していないユーザーがコールを終了するか、問題が発生していないデバイスがメディア接続の解放を判別できるまで、Cisco Unified Communications Manager が、問題が発生していないデバイスに関連付けられているアクティブな接続（コール）を維持します。

第 10 章

トランクの設定

SIP トランクの概要

コール制御シグナリング用に SIP を展開する場合、SIP ゲートウェイ、SIP プロキシサーバ、Unified Communications アプリケーション、会議ブリッジ、リモートクラスタ、または Session Management Edition などの外部デバイスに Cisco Unified Communications Manager を接続するための SIP トランクを設定します。

Cisco Unified CM Administration の内部では、[SIP トランクの設定（SIP Trunk Configuration）] ウィンドウに、Cisco Unified Communications Manager が SIP コールの管理に使用する SIP シグナリング設定が含まれています。

1 つの SIP トランクに、IPv4 または IPv6 のアドレッシング、完全修飾ドメイン名、または単一の DNS SRV レコードを使用して、最大 16 個の異なる宛先アドレスを割り当てることができます。

SIP トランクの前提条件

SIP トランクを設定する前に、次の操作を実行してください。

- トランク接続を理解できるようにネットワークトポロジを計画します。
- トランクを接続するデバイスと、それらのデバイスが SIP を実装する方法を理解していることを確認します。
- トランク用に設定されたデバイスプールがあることを確認してください。

- トランクに IPv6 を導入する場合は、クラスタ全体のエンタープライズパラメータを使用して、またはトランクに適用できる共通デバイス設定を使用して、トランクのアドレッシングプリファレンスを設定する必要があります。
- トランクを使用するアプリケーションと SIP 相互運用性の問題がある場合は、デフォルトの SIP 正規化または透明性スクリプトのいずれかを使用する必要がある場合があります。デフォルトのスクリプトのいずれも要件に合わない場合は、独自のスクリプトを作成できます。カスタマイズされた SIP 正規化および透過性スクリプトの作成の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。

SIP トランクの設定タスクフロー

SIP トランクを設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
Step 1	SIP プロファイルの設定 （102 ページ）	SIP トランクに適用する共通の SIP 設定を行います。
Step 2	SIP トランク セキュリティ プロファイルの設定 （103 ページ）	TLS シグナリングまたはダイジェスト認証などのセキュリティ設定を使用して、セキュリティ プロファイルを設定します。
Step 3	SIP トランクの設定 （104 ページ）	SIP トランクをセットアップして、そのトランクに SIP プロファイルとセキュリティ プロファイルを適用します。

SIP プロファイルの設定

共通 SIP 設定を使用して SIP プロファイルを設定するには、この手順を使用します。設定した SIP プロファイルは、このプロファイルを使用する SIP デバイスおよびトランクに割り当てることができます。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[SIPプロファイル（SIP Profile）]** を選択します。

Step 2 次のいずれかの手順を実行します。

- 既存のプロファイルを編集するには、**[検索（Find）]**をクリックし、SIP プロファイルを選択して既存のプロファイルを編集します。
- 新しいプロファイルを作成するには、[新規追加（Add New）] をクリックします。

Step 3 SIP 電話とトランクで IPv4 と IPv6 のスタックをサポートする場合は、[ANATの有効化（Enable ANAT）] チェックボックスをオンにします。

Step 4 SDP の相互運用性を解決するために SDP 透過性プロファイルを割り当てる場合は、[SDP透過性プロファイル（SDP Transparency Profile）] ドロップダウンリストから割り当てます。

Step 5 SIP の相互運用性の問題を解決するために正規化スクリプトまたは透過性スクリプトを割り当てる場合は、[正規化スクリプト（Normalization Script）] ドロップダウンリストからスクリプトを選択します。

Step 6 （任意）Cisco Unified Border Element 全体にコールをルーティングする必要がある場合は、グローバル ダイヤル プラン レプリケーションの導入環境向けに、[ILS学習送信先ルート文字列を送信（Send ILS Learned Destination Route String）] チェックボックスをオンにします。

Step 7 [SIPプロファイルの設定（SIP Profile Configuration）] ウィンドウで、残りのフィールドを入力します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

SIP トランク セキュリティ プロファイルの設定

ダイジェスト認証や TLS シグナリング暗号化などのセキュリティ設定を使用して、SIP トランクのセキュリティ プロファイルを設定します。プロファイルを SIP トランクに割り当てると、トランクはセキュリティプロファイルの設定を取得します。

（注） SIP トランクに SIP トランクのセキュリティ プロファイルを割り当てない場合、Cisco Unified Communications Manager は、デフォルトで非セキュアプロファイルを割り当てます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [セキュリティ（Security）] > [SIP トランクのセキュリティプロファイル（SIP Trunk Security Profile）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 TLS を使用した SIP シグナリング暗号化を有効化するには、次の手順を実行します。

a) [デバイスのセキュリティモード（Device Security Mode）] ドロップダウンリストから、[暗号化（Encrypted）] を選択します。

b) [着信転送タイプ（Incoming Transport Type）] および [発信転送タイプ（Outgoing Transport Type）] のドロップダウンリストから、[TLS] を選択します。

c) デバイスの認証用に、[X.509 のサブジェクト名（X.509 Subject Name）] フィールドに X.509 証明書のサブジェクト名を入力します。

d) [着信ポート（Incoming Port）] フィールドに、TLS リクエストを受信するポートを入力します。TLS のデフォルトは 5061 です。

Step 4 ダイジェスト認証を有効にするには、次の内容を実行します。

a) [ダイジェスト認証を有効化（Enable Digest Authentication）] チェックボックスをオンにします。

b) システムが新しいナンスを生成するまでの時間（秒数）を [ナンス有効時間（Nonce Validity Time）] に入力します。デフォルトは 600（10 分）です。

c) アプリケーションのダイジェスト認証を有効にするには、[アプリケーションレベル認証を有効化（Enable Application Level Authorization）] チェックボックスをオンにします。

Step 5 [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）] ウィンドウで追加フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 6 [保存（Save）] をクリックします。

（注） トランクが設定を使用できるように、[トランクの設定（Trunk Configuration）] ウィンドウで、このプロファイルをトランクに割り当てる必要があります。

SIP トランクの設定

SIP トランクを設定するには、この手順を使用します。1 つの SIP トランクには最大 16 個の宛先アドレスを割り当てることができます。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]>[トランク（Trunk）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [トランクタイプ（Trunk Type）] ドロップダウン リストから [SIPトランク（SIP Trunk）] を選択します。

Step 4 [プロトコルタイプ（Protocol Type）] ドロップダウンリストから、導入環境に適した SIP トランクのタイプを選択し、[次へ（Next）] をクリックします。

- **[なし（None）]（デフォルト）**
- **コール制御検出**
- **[クラスタ間の Extension Mobility（Extension Mobility Cross Cluster）]**
- **[Cisco Intercompany Media Engine]**
- **[IP マルチメディア システム サービス コントロール（IP Multimedia System Service Control）]**

Step 5 （オプション）このトランクに**共通デバイス設定**を適用する場合は、ドロップダウンリストから設定を選択します。

Step 6 暗号化されたメディアをトランクを介して送信する場合は、[SRTPを許可（SRTP Allowed）]チェックボックスをオンにします。

Step 7 すべてのクラスタ ノードに対してトランクを有効化する場合は、[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）] チェックボックスをオンにします。

Step 8 SIP トランクの宛先アドレスを設定します。

a) [宛先アドレス（Destination Address）]テキストボックスに、トランクに接続するサーバまたはエンドポイントの IPv4 アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

b) トランクがデュアル スタック トランクの場合は、[宛先アドレス IPv6（Destination Address IPv6）] テキスト ボックスに、トランクに接続するサーバーまたはエンドポイントの IPv6 アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

c) 宛先が DNS SRV レコードの場合は、[宛先アドレスは SRV（Destination Address is an SRV）] チェック ボックスをオンにします。

d) 接続先を追加するには、**[+]** をクリックします。

Step 9 **[SIP トランク セキュリティプロファイル（SIP Trunk Security Profile）]** ドロップダウンリスト ボックスから、このトランクに SIP トランク セキュリティプロファイルを割り当てます。このオプションを選択しない場合は、非セキュアプロファイルが割り当てられます。

Step 10 [SIPプロファイル（SIP Profile）] ドロップダウンリストから、SIP プロファイルを割り当てます。

Step 11 （任意） この SIP トランクに正規化スクリプトを割り当てる場合は、[正規化スクリプト（Normalization Script）] ドロップダウンリストから、割り当てるスクリプトを選択します。

Step 12 [Trunk Configuration] ウィンドウのその他のフィールドを設定します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 13 [保存（Save）] をクリックします。

SIP トランクの連携動作および制限

特長	説明
同じ宛先に対する複数のセキュアな SIP トランク	リリース 12.5(1) では、Cisco Unified Communications Manager は、同じ宛先 IP アドレスと宛先ポート番号に対する複数のセキュア SIP トランクの設定をサポートします。これには、以下の新しい機能や利点があります。 • 帯域幅の最適化：緊急コール用に帯域幅が制限されないルートを提供します。 • 特定のリージョンまたはコーリングサーチスペースの設定に基づく選択的ルーティング
同じ接続先に対する複数の非セキュアな SIP トランク	異なるリスニングポートを持つ複数の非セキュア SIP トランクが同じ接続先またはポートを指している場合、コール中の INVITE でポートが誤って使用される可能性があります。そのため、通話が中断します。

特長	説明
SIP 180 Ringing を受信すると、Unified Communications Manager は、SIP-UPDATE メッセージを送信します	「UPDATE」値がコールフローでサポートされている場合、SIP トランクは、「183 Session Progress」の後に「180 Ringing」を受信すると、「UPDATE」SIP メッセージを送信します。
BFCP を使用したプレゼンテーション共有	シスコのエンドポイント向けにプレゼンテーション共有を導入する場合は、すべての中継 SIP トランクの SIP プロファイルで **[BFCPを使用したプレゼンテーション共有を許可（Allow Presentation Sharing with BFCP）]** チェックボックスがオンになっていることを確認します。 （注） サードパーティ SIP エンドポイントの場合は、**[電話の設定（Phone Configuration）]** ウィンドウでも同じチェックボックスがオンになっていることを確認してください。
IX チャネル	iX メディア チャネルを導入する場合は、すべての中継 SIP トランクで て使用される SIP プロファイルで [iXアプリケーションメディアを許可（Allow iX Application Media）] チェックボックスがオンになっていることを確認します。 （注） 暗号化された iX チャネルの詳細については、『*Cisco Unified Communications Manager* セキュリティガイド』を参照してください。
90 日間の評価ライセンス	90 日の評価期間を使用して実行している間、セキュア SIP トランクを導入することはできません。セキュア SIP トランクを導入するには、製品登録トークンで [エクスポート管理された機能を許可（Allow export-controlled functionality）] を選択した Smart Software Manager アカウントにシステムを登録してある必要があり ます。

H.323 トランクの概要

（注） リリース 15 以降、H.323 ゲートキーパー制御オプションは Unified Communications Manager で使用できなくなります。したがって、Location Bandwidth Manager（LBM）で SIP トランクを使用することをお勧めします。

H.323 を導入している場合は、H.323 トランクがリモート クラスタと、ゲートウェイなどのその他の H.323 デバイスに接続を提供します。H.323 トランクは、Unified Communications Manager がクラスタ内通信でサポートするオーディオコーデックおよびビデオコーデックのほとんどをサポートします。ただし、広帯域オーディオおよび広帯域ビデオについてはサポートしません。H.323 トランクは、コール制御シグナリング用に H.225 プロトコルを使用し、メディア シグナリング用に H.245 プロトコルを使用します。

Cisco Unified CM Administration で、クラスタ間トランク（ゲートキーパー非制御）トランクタイプとプロトコルオプションを使用して H.323 トランクを設定できます。

非ゲートキーパー H.323 導入環境の場合は、Unified Communications Manager が IP WAN 経由でコールできるように、リモート クラスタ内の各デバイスプールに個別のクラスタ間トランクを設定する必要があります。クラスタ間トランクは、リモートデバイスの IPv4 アドレスまたはホスト名を静的に指定します。

単一のトランクには最大 16 件の宛先アドレスを設定できます。

クラスタ間トランク

2 つのリモート クラスタ間にクラスタ間トランク接続を設定する場合は、一方のトランクが使用する宛先アドレスがリモート クラスタのトランクが使用するコール処理ノードと一致するように、クラスタごとにクラスタ間トランクを設定し、トランク設定を一致させる必要があります。次に例を示します。

- リモート クラスタ トランクが [すべてのアクティブ ノードで実行（Run on all Active Nodes）] を使用する：リモート クラスタ トランクは、コール処理とロード バランシングにすべてのノードを使用します。ローカルクラスタ内から始まるローカルクラスタ間トランクでは、リモート クラスタ内の各サーバの IP アドレスまたはホスト名を追加します。
- リモート クラスタで [すべてのアクティブノードで実行（Run on all Active Nodes）] を使用しない：リモート クラスタ トランクは、コール処理およびロード バランシング用にトランクのデバイスプールに割り当てられた Unified Communications Manager グループのサーバを使用します。ローカルのクラスタ間トランク設定では、リモートクラスタトランクのデバイスプールで使用される Unified Communications Manager グループから各ノードの IP アドレスまたはホスト名を追加する必要があります。

セキュアなトランク

H.323 トランクのセキュアなシグナリングを設定するには、トランクに IPSec を設定する必要があります。詳細については、『*Cisco Unified Communications Manager* セキュリティガイド』を参照してください。メディア暗号化を許可するようにトランクを設定するには、**[トランクの設定（Trunk Configuration）]** ウィンドウで [SRTP を許可する（SRTP allowed）] チェックボックスをオンにします。

H.323 トランクの前提条件

H.323 導入トポロジを計画します。クラスタ間トランクの場合は、対応するリモートクラスタトランクがコール処理とロードバランシングにどのサーバを使用するかを明確化します。リモートクラスタ内のトランクによって使用される各コール処理サーバに接続するように、ローカルクラスタ間トランクを設定する必要があります。

トランクでのロードバランシングのためにトランクデバイスプールに割り当てられた Cisco Unified Communications Manager を使用している場合は、「デバイスプールのコア設定の設定タスクフロー（86 ページ）」セクションの設定を実行します。

H.323 トランクの設定

H.323 を導入したトランクを設定するには、次の手順を使用します。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]>[トランク（Trunk）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [トランクタイプ（Trunk Type）] ドロップダウンリストボックスから、[クラスタ間トランク（ゲートキーパー制御なし）（Inter-Cluster Trunk (Non-Gatekeeper Controlled)）] を選択します。

Step 4 [プロトコル（Protocol）] ドロップダウンリストボックスから、[クラスタ間トランク（Inter-Cluster Trunk）] を選択します。

Step 5 [デバイス名（Device Name）] テキストボックスに、トランクの一意の識別子を入力します。

Step 6 [デバイスプール（Device Pool）] ドロップダウンリスト ボックスから、このトランクに設定したデバイスプールを選択します。

Step 7 このトランクの処理のためにローカルクラスタのすべてのノードを使用するには、[すべてのアクティブな Unified CM ノードで実行する（Run on all Active Unified CM Nodes）] チェックボックスをオンにします。

Step 8 暗号化されたメディアをトランクで許可するには、[SRTPの許可（SRTP Allowed）] チェックボックスをオンにします。

Step 9 H.235 パススルーを設定するには、[H.235パススルーを許可（H.235 Pass Through Allowed）] チェックボックスをオンにします。

Step 10 [リモートのCisco Unified CM情報（Remote Cisco Unified Communications Manager Information）] セクションで、このトランクの接続先のリモートサーバごとに 1 つの IP アドレスまたはホスト名を入力します。

第 11 章

ゲートウェイの設定

ゲートウェイの概要

シスコは広範な音声およびビデオ ゲートウェイを提供しています。ゲートウェイは、Unified Communications ネットワークと外部ネットワークとの通信を可能にするインターフェイスを提供します。従来、ゲートウェイは、PSTN、構内交換機（PBX）、またはアナログ電話や FAX 装置を含むレガシーデバイスなどのレガシー電話インターフェイスに IP ベースの Unified Communications ネットワークを接続するために使用されてきました。最も単純な形では、音声ゲートウェイが IP インターフェイスとレガシー電話インターフェイスを備え、2 つのネットワークが通信できるようにゲートウェイが 2 つのネットワーク間でメッセージを変換します。

ゲートウェイ プロトコル

大半のシスコのゲートウェイには、複数の導入オプションがあり、多数のプロトコルのいずれかを使用して導入できます。導入するゲートウェイに応じて、次の通信プロトコルのいずれかを使用してゲートウェイを設定できます。

- メディア ゲートウェイ コントロール プロトコル（MGCP）
- Skinny Call Control Policy（SCCP）
- Session Initiation Protocol（SIP）
- H.323

インターフェイス カード

外部ネットワークに接続インターフェイスを提供するには、ベンダーインターフェイスカード (VIC) をゲートウェイにインストールする必要があります。ほとんどのゲートウェイには複数の VIC オプションが用意されており、各 VIC ではアナログ接続とデジタル接続に対して、さまざまなポートや接続タイプを提供できます。

ゲートウェイで提供されているプロトコル、カード、および接続については、ゲートウェイのマニュアルを参照してください。

音声ゲートウェイのセットアップ前提条件

ハードウェアのインストール

Cisco Unified Communications Manager にゲートウェイを設定する前に、ゲートウェイ ハードウェアに対して次の作業を行う必要があります。

- ゲートウェイのインストールと設定
- ゲートウェイに任意のベンダー インターフェイス カード（VIC）をインストールします。
- CLI を使用して、ゲートウェイの IOS を設定します。

詳細については、ご使用のゲートウェイに付属しているハードウェアとソフトウェアのマニュアルを参照してください。

（注） 多くのゲートウェイデバイスの場合、デフォルトの Web ページは、そのゲートウェイの IP アドレスを使用して表示できます。ハイパーリンクの URL を http://x.x.x.x/ にします。ここで、x.x.x.x はデバイスのドット形式の IP アドレスです。各ゲートウェイの Web ページには、ゲートウェイのデバイス情報とリアルタイムのステータスが含まれています。

ゲートウェイの導入計画

Cisco Unified Communications Manager にゲートウェイを設定する前に、ゲートウェイに設定する接続のタイプを十分に考慮してください。多くのゲートウェイは、MGCP、SIP、H.323、または SCCP のいずれかをゲートウェイ プロトコルとして使用して設定できます。各導入タイプの接続タイプは、選択するプロトコルおよびゲートウェイにインストールされている VIC によって異なります。次の点を確認してください。

- 使用ゲートウェイでサポートされているゲートウェイ プロトコル。
- ゲートウェイの VIC でサポートされているポート接続のタイプ。
- 設定予定の接続のタイプ。
- アナログ接続の場合、PSTN、レガシー PBX、またはレガシー デバイスに接続しているか。
- デジタルアクセス接続の場合、T1 CAS インターフェイスまたは PRI インターフェイスに接続しているか。
- FXO 接続の場合、着信コールをどのように転送するか。着信コールを IVR や自動応答機能に転送しているか。

ゲートウェイの設定タスクフロー

Unified Communications Manager にネットワークゲートウェイを追加するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
Step 1	導入するプロトコルに応じて、次の手順のいずれかを実行します。 • MGCP ゲートウェイの設定（111 ページ） • SCCP ゲートウェイの設定（120 ページ） • SIP ゲートウェイの設定（124 ページ） • H.323 ゲートウェイの設定（127 ページ）	Unified Communications Manager でゲートウェイを設定します。多くの Cisco ゲートウェイは、ALP および SCCP、SIP、または H のいずれかを使用して展開できます。ゲートウェイプロトコルとして使用できます。ゲートウェイのマニュアルを参照して、お使いのゲートウェイがサポートしているプロトコルと導入に最適なプロトコルを確認してください。
Step 2	ゲートウェイに対するクラスタ全体のコール分類の設定（128 ページ）	（**オプション**）ネットワーク内のゲートウェイポートから着信するすべてのコールを内部 (OnNet) または 外部 (OffNet) に分類するように、クラスタサービスのパラメータを設定します。
Step 3	オフネットゲートウェイ転送のブロック（128 ページ）	（**オプション**）外部（オフネット）ゲートウェイ間のコールを Unified Communications Manager が転送しないようにブロックし、[オフネット間の転送をブロック（Block OffNet to Offnet Transfer）] パラメータを設定します。

MGCP ゲートウェイの設定

MGCP 設定を使用するためにシスコのゲートウェイを設定するには、次のタスクを実行します。

始める前に

MGCP ゲートウェイの Unified CM ポート接続を確認します。Cisco Unified CM Administration で、**[システム（System）]** > **[Cisco Unified CM]** に移動し、サーバを選択して、MGCP リッスンポートと MGP キープアライブ ポートの設定を確認します。ほとんどの場合、デフォルトのポート設定を変更する必要はありません。

手順

	コマンドまたはアクション	目的
Step 1	MGCP（IOS）ゲートウェイの設定 （112 ページ）	Cisco Unified CM Administration にゲートウェイを追加し、ゲートウェイ プロトコルとして[MGCP] を選択します。適切なスロットとベンダーのインターフェイス カード（VIC）でゲートウェイを設定します。
Step 2	ゲートウェイ ポート インターフェイスの設定 （113 ページ）	ゲートウェイにインストールされている VIC に接続するデバイス用のゲートウェイ ポート インターフェイスを設定します。ほとんどの VICs には、複数のポート接続とオプションが含まれているため、いくつかの異なるポートインターフェイスタイプを設定する必要があります。 **ヒント** ポート インターフェイスの設定後に、[関連リンク（Related Links）] ドロップダウンリストから [BGCP設定に戻る（Back to MGCP Configuration）] オプションを選択し、[ゲートウェイの設定（Gateway Configuration）] ウィンドウに戻ります。そのウィンドウで、別のポート インターフェイスを選択して設定できます。
Step 3	MGCP ゲートウェイでのデジタル アクセス T1 ポートの追加 （118 ページ）	**オプション**デジタルアクセス T1 CAS ポート インターフェイスを設定したら、ゲートウェイに T1 CAS ポートを追加します。個別にポートを追加したり、同時にポート範囲を追加したりできます。
Step 4	ゲートウェイのリセット （120 ページ）	設定の変更は、ゲートウェイをリセットした後に反映されます。

MGCP（IOS）ゲートウェイの設定

Unified Communications Manager に MGCP（IOS）ゲートウェイを追加して設定するには、次の手順を実行します。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ゲートウェイ (Gateway)]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [ゲートウェイタイプ（Gateway Type）] ドロップダウンリストからゲートウェイを選択して、[次へ（Next）] をクリックします。

Step 4 [プロトコル（Protocol）] ドロップダウンリストから [MGCP] を選択して、[次へ（Next）] をクリックします。

Step 5 [設定済みのスロット、VIC、およびエンドポイント（Configured Slots、VICs and Endpoints）] 領域で次の手順を実行します。

a) 各 **[モジュール（Module）]** ドロップダウンリストで、ゲートウェイにインストールされているネットワーク インターフェイス モジュール ハードウェアに対応するスロットを選択します。

b) 各 **[サブユニット（Subunit）]** ドロップダウンリストで、ゲートウェイにインストールされている VIC を選択します。

c) [保存（Save）] をクリックします。
[ポート（Port）] アイコンが表示されます。各ポートアイコンは、ゲートウェイで使用可能なポート インターフェイスに対応しています。ポート インターフェイスを設定するには、該当するポートのアイコンをクリックします。

Step 6 [ゲートウェイの設定（Gateway Configuration）] ウィンドウでその他のフィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 7 [保存（Save）] をクリックします。

ゲートウェイ ポート インターフェイスの設定

ゲートウェイにインストールされている VIC に接続するデバイスのポート接続を設定できます。ほとんどの VICs には、複数のポート接続とオプションが含まれているため、いくつかの異なるポートインターフェイスタイプを設定する必要があります。

設定するインターフェイスのタイプに応じて、次のいずれかのタスクを選択します。

- デジタルアクセス優先ポートの設定 （114 ページ）
- MGCP ゲートウェイのデジタルアクセス T1 ポートの設定 （114 ページ）
- FXS ポートの設定 （115 ページ）
- FXO ポートの設定 （116 ページ）
- BRI ポートの設定 （117 ページ）

デジタルアクセス優先ポートの設定

MGCP（IOS）ゲートウェイの PRI ポート インターフェイスを設定します。

始める前に

MGCP（IOS）ゲートウェイの設定 （112 ページ）

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ゲートウェイ（Gateway）]** を選択します。

Step 2 [検索（Find）] をクリックし、PRI ポートを設定するゲートウェイを選択します。

Step 3 [設定済みのスロット、VICおよびエンドポイント（Configured Slots, VICs, and Endpoints）] 領域で、設定する BRI ポートを含むモジュールとサブユニットを見つけ、設定する BRI ポートに対応する [ポート（Port）] アイコンをクリックします。
[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、BRI ポート インターフェイスが表示されます。

Step 4 [デバイスプール（Device Pool）] ドロップダウンリストから、デバイスプールを選択します。

Step 5 [ゲートウェイの設定（Gateway Configuration）] ウィンドウでその他のフィールドを設定します。フィールドの説明については、オンライン ヘルプを参照してください。

Step 6 [保存（Save）] をクリックします。

Step 7 （任意）ゲートウェイ用にさらにポートインターフェイスを設定するには、[関連リンク（Related Links）] ドロップダウンリストから [MGCPの設定に戻る（Back to MGCP Configuration）] を選択し、[移動（Go）] をクリックします。

[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、ゲートウェイで使用可能なポート インターフェイスが表示されます。

ポート インターフェイスの設定が完了したら、「ゲートウェイのリセット （120 ページ）」を参照してください。

MGCP ゲートウェイのデジタルアクセス T1 ポートの設定

MGCP （IOS）ゲートウェイでデジタルアクセス T1 CAS ポートのポート インターフェイスを設定します。

始める前に

MGCP（IOS）ゲートウェイの設定 （112 ページ）

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ゲートウェイ（Gateway）]** を選択します。

Step 2 [検索（Find）] をクリックして、T1 ポートを設定するゲートウェイを選択します。

Step 3 [設定済みのスロット、VICおよびエンドポイント（Configured Slots, VICs and Endpoints）] 領域で、デジタルアクセス T1（T1-CAS）ポートを設定するモジュールとサブユニットを探し、対応する [ポート（Port）] アイコンをクリックします。

Step 4 [デバイスプロトコル（Device Protocol）] ドロップダウンリストから [デジタルアクセスT1（Digital Access T1）] を選択して、[Next（次へ）] をクリックします。

Step 5 適切なゲートウェイ設定を入力します。

フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 6 [保存（Save）] をクリックします。

デジタルアクセス T1 CAS ポート インターフェイスに対するポートの追加の詳細については、「MGCP ゲートウェイでのデジタルアクセス T1 ポートの追加（118 ページ）」を参照してください。

FXS ポートの設定

MGCP ゲートウェイで Foreign Exchange Station（FXS）のポートを設定します。FXS ポートを使用して、単純な旧式の電話サービス（POTS）の従来型の電話や、ファックス装置、スピーカーフォン、従来型のボイスメッセージング システム、自動音声応答（IVR）などの従来型のデバイスに、ゲートウェイを接続することができます。

始める前に

ポートを設定する前に、ゲートウェイを追加する必要があります。

手順

Step 1 Cisco Unified CM Administration で、**[デバイス（Device）] > [ゲートウェイ（Gateway）]** を選択します。

Step 2 [検索（Find）] をクリックして、FXS ポートを設定するゲートウェイを選択します。

Step 3 [設定済みのスロット、VIC、およびエンドポイント（Configured Slots, VICs, and Endpoints）] 領域で、設定するポートに対応する [FXSポート（FXS Port）] アイコンをクリックします。
[ポートの選択（Port Selection）] エリアが表示されます。

Step 4 [ポートタイプ（Port Type）] ドロップダウンリストから、設定する接続タイプを選択します。

- [POTS]：従来の電話機などの POTS デバイスにこのポートを接続する場合は、このオプションを選択します。
- [グラウンドスタート（Ground Start）]：グラウンドスタート シグナリングを使用して、ファックス装置、従来型のボイスメッセージング システム、IVR などの従来型の無人デバイスにこのポートを接続する場合は、このオプションを選択します。
- [ループスタート（Loop Start）]：ループ スタート シグナリングを使用して、ファックス装置、従来型のボイスメッセージング システム、IVR などの従来型の無人デバイスにこのポートを接続する場合は、このオプションを選択します。

Step 5 [次へ（Next）] をクリックします。
[ポートの設定（Port Configuration）] ウィンドウには、デバイス プロトコルとしてアナログ アクセスを使用するポート インターフェイスの設定が表示されます。

Step 6 [デバイスプール（Device Pool）] ドロップダウンリストから、デバイスプールを選択します。

Step 7 [電話の設定（Phone Configuration）] ウィンドウで、残りのフィールドを入力します。

フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

Step 9 （任意） MGCP IOS ゲートウェイでさらにポート インターフェースを設定するには、[関連リンク（Related Links）] ドロップダウンリストから [ゲートウェイに戻る（Back to Gateway）] リンクを選択し、[移動（Go）] をクリックします。

[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、ゲートウェイで使用可能なポートが表示されます。

ポート インターフェイスの設定が完了したら、「ゲートウェイのリセット （120 ページ）」を参照してください。

FXO ポートの設定

MGCP（IOS）ゲートウェイの Foreign Exchange Office (FXO) を設定します。FXO ポートを使用して、ゲートウェイを PSTN またはレガシー PBX に接続できます。

（注） Unified Communications Manager は、すべてのループスタートトランクに確実な接続解除監視がないと見なします。サーバのフェールオーバー中もアクティブなコールを維持できるように、確実な接続解除監視をグラウンド スタートに指定してトランクを設定します。

始める前に

MGCP（IOS）ゲートウェイの設定 （112 ページ）

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ゲートウェイ（Gateway）]** を選択します。

Step 2 **[検索（Find）]** をクリックし、ルート クラス シグナリングを設定するゲートウェイを選択します。

Step 3 [設定済みのスロット、VICおよびエンドポイント（Configured Slots, VICs, and Endpoints）] 領域で、FXO ポート インターフェイスをセットアップする FXO ポートを含む**モジュール**および**サブユニット**を見つけて、設定するポートに対応する [ポート（Port）] アイコンをクリックします。

Step 4 [ポート タイプ（Port Type）] ドロップダウンリストから、[グラウンドスタート（Ground-Start）] または [ループスタート（Loop-Start）] を選択します。

（注） VIC-2 FXO ポートを設定している場合は、サブユニット モジュールの両方のポートに同じポート タイプを選択する必要があります。

Step 5 [デバイスプール（Device Pool）] ドロップダウンリストから、デバイスプールを選択します。

Step 6 [アテンダントDN（Attendant DN）]ボックスに、このポート接続からのすべての着信コールをルーティングする電話番号を入力します。たとえば、1つのアテンダントの場合は、0またはディレクトリ番号が表示されます。

Step 7 [ポートの設定（Port Configuration）] ウィンドウの他のフィールドに入力します。フィールドの説明については、オンライン ヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

Step 9 （任意） MGCP IOS ゲートウェイでさらにポート インターフェースを設定するには、[関連リンク（Related Links）] ドロップダウンリストから [ゲートウェイに戻る（Back to Gateway）] リンクを選択し、[移動（Go）] をクリックします。

[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、ゲートウェイで使用可能なポートが表示されます。

ポート インターフェイスの設定が完了したら、「ゲートウェイのリセット （120 ページ）」を参照してください。

BRI ポートの設定

MGCP（IOS）ゲートウェイの BRI ポート インターフェイスを設定します。

始める前に

MGCP（IOS）ゲートウェイの設定 （112 ページ）

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ゲートウェイ（Gateway）]** を選択します。

Step 2 BRI ポートを設定するゲートウェイを選択するには、[検索（Find）] をクリックします。

Step 3 [設定済みのスロット、VICおよびエンドポイント（Configured Slots, VICs, and Endpoints）] セクションで、BRIポートを使用するサブユニットを探し、設定するポートに対応する [ポート（Port）] アイコンをクリックします。
[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、BRI ポート インターフェイスの情報が表示されます。

Step 4 [デバイスプール（Device Pool）] ドロップダウンリストから、デバイスプールを選択します。

Step 5 適切なゲートウェイおよびポートの設定情報を入力します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 6 [保存（Save）] をクリックします。

Step 7 （任意）ゲートウェイ用にさらにポートインターフェイスを設定するには、[関連リンク（Related Links）] ドロップダウンリストから [MGCPの設定に戻る（Back to MGCP Configuration）] を選択し、[移動（Go）] をクリックします。

[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、MGCP ゲートウェイで使用可能なポート インターフェイスが表示されます。

ポート インターフェイスの設定が完了したら、「ゲートウェイのリセット （120 ページ）」を参照してください。

MGCP ゲートウェイでのデジタル アクセス T1 ポートの追加

MGCP ゲートウェイで、T1 CAS ポートを T1 デジタル アクセス ポート インターフェイスに追加および設定します。最大 24 の T1 CAS ポートを追加および設定できます。ポートを単独に追加したり、一連のポートを追加したり構成したりすることもできます。特定のポート範囲を入力する場合、Unified Communications Manager がそのポート範囲全体に設定を適用します。

始める前に

MGCP ゲートウェイのデジタルアクセス T1 ポートの設定 （114 ページ）

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ゲートウェイ（Gateway）]** を選択します。

Step 2 [検索（Find）] をクリックし、T1 CAS ポート インターフェイスを含むゲートウェイを選択します。

Step 3 [新規ポートの追加（Add a New Port）] をクリックします。

Step 4 [ポートタイプ（Port Type）] ドロップダウンリストボックスから、追加するポートのタイプを選択して、[次へ（Next）] をクリックします。

Step 5 [開始ポート番号（Beginning Port Number）] と [終了ポート番号（Ending Port Number）] フィールドにポート番号を入力し、追加と設定を行うポート範囲を指定します。

たとえば、1 から 10 のポートを、ポート インターフェイスに同時に追加するには、1 と 10 を入力します。

Step 6 [通信の方向（Port Direction）] ドロップダウンリストボックスから、このポートを通過するコールの方向を設定します。

- [双方（Bothways）]：発着信コールの両方を許可する場合、このオプションを選択します。
- [インバウンド（Inbound）]：着信コールのみを許可する場合、このオプションを選択します。
- [アウトバウンド（Outbound）]：アウトバウンド コールのみを許可する場合、このオプションを選択します。

Step 7 EANDM ポートの場合、[発信者の選択（Calling Party Selection）] ドロップダウンリストで、このポートに接続されているデバイスからの発信コールの発信者番号をどのように表示するかを選択します。

- [発信元（Originator）]：発信側デバイスの電話番号を送信します。
- [最初のリダイレクト番号（First Redirect Number）]：リダイレクト側デバイスの電話番号を送信します。
- [最後のリダイレクト番号（Last Redirect Number）]：コールをリダイレクトする最後のデバイスの電話番号を送信します。
- [最初のリダイレクト番号（外線）（First Redirect Number (External)）]：外部電話マスクが適用されている、リダイレクトを行う最初のデバイスの電話番号を送信します。
- [最後のリダイレクト番号（外線）（First Redirect Number (External)）]：外部電話マスクが適用されている、リダイレクトを行う最後のデバイスの電話番号を送信します。

Step 8 [保存（Save）] をクリックします。

Step 9 MGCP ゲートウェイ用に追加のポートを設定するには、[関連リンク（Related Links）] から、[ゲートウェイに戻る（Back to Gateway）] を選択し、[移動（Go）] をクリックします。デジタルアクセス T1 ポート インターフェイスが表示されたら、次のいずれかの手順を実行します。

- このポート インターフェイスに追加のデジタルアクセス T1 CAS ポートを追加するには、この手順のステップ 3（「**新規ポートの追加**」）に戻ります。
- ゲートウェイでさらにポートインターフェイスを設定するには、[関連リンク（Related Links）] から、[MGCPの設定に戻る（Back to MGCP Configuration）] を選択し、[移動（Go）] をクリックします。[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、ゲートウェイのサブユニット モジュールで使用可能なポートが表示されます。
- ポート インターフェイスの設定が完了したら、「ゲートウェイのリセット（120 ページ）」を参照してください。

ゲートウェイのリセット

ほとんどのゲートウェイは、設定の変更が適用されるようにリセットする必要があります。リセットを行う前に、必要なゲートウェイ設定をすべて完了することをお勧めします。

（注） H.323 ゲートウェイをリセットしても、Unified Communications Manager にロードされた設定が再初期化されるだけで、ゲートウェイの物理的な再起動やリセットは行われません。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ゲートウェイ (Gateway)]** を選択します。

Step 2 [検索（Find）] をクリックして、ゲートウェイを選択します。

Step 3 リセットするゲートウェイの横のチェック ボックスをクリックして、[リセット選択済み（Reset Selected）] をクリックします。[デバイス リセット（Device Reset）] ダイアログ ボックスが表示されます。次のいずれか 1 つの処理を実行します。

Step 4 [リセット（Reset）] をクリックします。

MGCP 発信者 ID 制限

着信 SIP リクエストの FROM ヘッダーに特殊文字が含まれている場合、SIP-MGCP/323 コールフローに影響を与え、システムが通話を切断するか、問題を表示します。したがって、リクエストが Unified Communications Manager に到達するネットワークノードを修正します。

次に例を示します。

- 「Per%cent」など、アルファベットに含まれる特殊文字は、表示名に影響します。
- 「0%09%0A%01%05%0A%01%03%0A%01%04」のような多くの特殊文字は、CRCX に問題が発生する可能性があるため、MGCP 側に送信されるリモート名としての通話を切断する場合があります。

SCCP ゲートウェイの設定

SCCP 設定を使用するように Cisco ゲートウェイを設定するには、このタスクを実行します。

手順

	コマンドまたはアクション	目的
Step 1	ゲートウェイプロトコルとしての SCCP の設定 （121 ページ）	ゲートウェイ プロトコルとして SCCP を使用するように、Cisco ゲートウェイを設定します。
Step 2	未設定のアナログ FXS ポートの自動登録の有効化	未設定のアナログ FXS ポートの自動登録を有効にします。
Step 3	アナログ電話の自動登録の有効化 （122 ページ）	指定したポートで自動登録を有効化にして、自動登録 DN のプールから DN を取得します。

ゲートウェイプロトコルとしての SCCP の設定

ゲートウェイ プロトコルとして SCCP を使用するように、Cisco ゲートウェイを設定できます。この導入オプションを使用して、FXS または BRI ポートを使用して、Unified Communications Manager をアナログアクセスデバイスまたは ISDN BRI デバイスに接続できます。SCCP ゲートウェイをデジタルアクセスの T1 トランクまたは E1 トランクに接続することはできません。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ゲートウェイ (Gateway)]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 **[ゲートウェイ タイプ（Gateway Type）]** ドロップダウンリスト ボックスで、[Cisco VG200] を選択し、[次へ（Next）] をクリックします。

Step 4 [プロトコル（Protocol）] ドロップダウンリストから、[SCCP] を選択します。

Step 5 [設定済みのスロット、VICおよびサブユニット（Configured Slots, VICs and Subunits）] セクションで、次の手順を実行します。

a) 個々の [モジュール（Module）] ドロップダウンリストで、ゲートウェイにインストールされているネットワーク インターフェイス モジュールのハードウェアに対応するスロットを選択します。

b) 各 [サブユニット（Subunit）] で、ゲートウェイにインストールされている VIC を選択します。

Step 6 [ゲートウェイの設定（Gateway Configuration）] ウィンドウでその他のフィールドを設定します。

フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 7 [保存（Save）] をクリックします。
[ポート（Port）] アイコンは、サブユニット モジュールの横に表示されます。各ポートのアイコンは、ゲートウェイで設定可能なポートのインターフェイスに対応します。該当するポートのアイコンをクリックして、ポートのアナログ アクセスまたは ISDN BRI 電話を設定できます。

Step 8 更新を完了したときに、ゲートウェイに変更を適用します。

a) [ゲートウェイのリセット（Reset Gateway）]をクリックします。[ゲートウェイの再起動（Restart Gateway）] ポップアップが表示されます。

b) [リセット（Reset）] をクリックします。

アナログ電話の自動登録の有効化

自動登録 Dn のプールから電話番号を取得するために、指定されたポートの自動登録を有効にします。デフォルトでは、ユニファイドコミュニケーションマネージャはアナログ電話の自動登録を許可しません。管理者は、SCCPプロトコルを使用して、対応するゲートウェイを介して、アナログ電話機を自動登録するようにゲートウェイモジュールを設定する必要があります。

（注） サポートされているゲートウェイタイプは、VG310、VG350、VG400、VG450、および ISR4K シリーズです。

始める前に

- 自動登録を有効化して、新しいエンドポイントがネットワークに接続している間にに割り当てられる DN の範囲を指定します。詳細については、「自動登録の有効化（446ページ）」の項を参照してください。
- ゲートウェイで SCCP プロトコルを使用して自動設定を有効にします。詳細については、『SCCP ゲートウェイのための CUCM 自動設定』ガイドを参照してください。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[デバイス（Device）] > [ゲートウェイ（Gateway）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 **[ゲートウェイ タイプ（Gateway Type）]** ドロップダウンリスト ボックスで、[Cisco VG200] を選択し、[次へ（Next）] をクリックします。

Step 4 [プロトコル（Protocol）] ドロップダウンリストから、[SCCP] を選択します。

Step 5 **[ゲートウェイの詳細 (Gateway Details)]** セクションで、次の手順を実行します。

a) テキストボックスに、**MAC アドレス**の最後の 10 桁を入力します。MAC アドレスを入力すると、[説明（Description）] フィールドの値が自動的に入力されます。

（注） ゲートウェイの MAC アドレスは、イーサネット MAC アドレスか、または SCCP ゲートウェイのインターフェイスで割り当てられた仮想 MAC アドレスであり、Unified Communications Manager と通信します。

MAC アドレスを指定すると、各 FXS ポートは、設定された MAC アドレスとそのポート番号からポート名を取得します。対応するアナログ電話機が自動的にこのゲートウェイに登録されます。

たとえば、[スロット0のモジュール（Module in Slot 0）] ドロップダウンリストで [NM-4VWIC-MBRD] が選択され、[サブユニット0（Subunit 0）] ドロップダウンリストで [VIC3-4FXS/DID-SCCP] が選択された場合、4 個の FXS ポートの値はそれぞれ [0/0/0]、[0/0/1]、[0/0/2]、[0/0/3] と表示されます。各ポートをクリックすると、[電話の設定（Phone Configuration）] ウィンドウの [説明（Description）] フィールドに、対応するポート名が表示されます。表示されるポート名は、MAC アドレスとポート値の組み合わせです。

ゲートウェイは、設定に基づいて、仮想 MAC アドレスまたはイーサネット MAC アドレスを使用して、設定に基づいて Unified Communication Manager と通信します。仮想 MAC アドレスは、破損したゲートウェイを交換した場合でも使用できるため、Unified Communication Manager アプリケーションで設定を変更する必要はありません。

b) 必要な **Cisco Unified Communications Manager グループ**をドロップダウンリストから選択して、自動登録を有効化します。

Step 6 [設定済みのスロット、VICおよびエンドポイント（Configured Slots, VICs and Endpoints）] セクションで、次の手順を実行します。

a) 各 [モジュール（Module）] ドロップダウンリストで、ゲートウェイにインストールされているネットワーク インターフェイス モジュール ハードウェアに対応するスロットを選択し、[保存（Save）] をクリックして、それぞれの**サブユニット**を有効化します。

b) 1 つ以上のサブユニットについて、ゲートウェイにインストールされている対応する VIC を選択して、[保存（Save）] をクリックします。

（注） スロットとモジュールは、どのスロットとモジュールに FXS ポートが設定されているかを示します。また、FXS ポートの数も示します。

ポートは自動登録されて自動DNを取得するため、ゲートウェイの設定は、ポートレベルまででではなくサブユニットレベルまでとします。たとえば、FXSに対してサブユニットが選択されている場合、対応する FXS ポートが自動登録 DN プールで使用可能な DN を 1 つ選択して、選択されたポートに DN を割り当てます。

Step 7 **[設定の適用（Apply Config）]** をクリックします。

ゲートウェイは、ポートが電話に接続されているかどうかに関係なく、FXS で設定されたすべてのポートに登録要求を送信します。

未設定のアナログ FXS ポートの自動登録の有効化

未設定のアナログ FXS ポートの自動登録を有効にするには、次の手順を実行します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[システム（System）] > [サービスパラメータ（Service Parameters）]**

Step 2 [サーバ（Server）] ドロップダウンリストから、実行中の目的のサーバを選択します。

Step 3 [サービス（Service）] ドロップダウンリストから、[Cisco Call Manager（アクティブ）（Cisco CallManager(Active)）] を選択します。

Step 4 [クラスタ全体のパラメータ（デバイス-PRIおよびMGCPゲートウェイ）（Clusterwide Parameters (Device-PRI and MGCP Gateway)）] セクションで、[FXSポートの自動登録の有効化（Enable Auto Registration for FXS Ports）] ドロップダウンリストが [はい（True）] に設定されていることを確認します。

（注） 未設定のアナログFXSポートの自動登録を無効にするには、[FXSポートの自動登録の有効化（Enable Auto Registration for FXS Ports）] の値を [いいえ（False）] に設定します。

Step 5 [保存（Save）] をクリックします。

トラブルシューティングのヒント

ポートが登録されていることを確認し、自動DNを取得するには、Unified Communications Managerで次の手順を実行します。

1. SCCP をゲートウェイタイプとして設定します。
2. 自動登録を有効にします。
3. デバイスタイプとしてアナログ電話を選択します。
4. 音声ポートの数に対応できる十分な数の DN がプール内にあることを確認します。

SIP ゲートウェイの設定

次のタスクを実行して、Unified Communication Manager で SIP ゲートウェイを設定します。多くのCiscoゲートウェイとサードパーティゲートウェイは、SIPを使用するように設定することができます。Unified Communication Managerには、SIP ゲートウェイ用のゲートウェイデバイスタイプが含まれていません。

始める前に

ネットワークにゲートウェイハードウェアをインストールし、Unified Communication Manager にゲートウェイを追加する前に、ゲートウェイ上で IOS ソフトウェアを設定する必要があります。

手順

	コマンドまたはアクション	目的
Step 1	SIP プロファイルの設定 （125 ページ）	Sipプロファイルを設定し、sipプロファイルに適用します。トランクはこの設定を使用して SIP ゲートウェイに接続します。
Step 2	SIP トランク セキュリティ プロファイルを構成します。 （126 ページ）	SIP トランクセキュリティプロファイルを設定して、トランクが SIP ゲートウェイに接続するためにこれを使用するようにします。デバイスのセキュリティモード、要約されたアイデンティティの検証、および着信/転送タイプの設定などのセキュリティ設定ができます。
Step 3	SIP ゲートウェイ向け SIP トランクの設定 （126 ページ）	SIP ゲートウェイを指すようにすべての SIP トランクを構成します。SIP トランク セキュリティ プロファイルをトランクに適用します。

SIP プロファイルの設定

SIP ゲートウェイ接続の SIP プロファイルを設定します。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]**>**[デバイスの設定（Device Settings）]**>**[SIPプロファイル（SIP Profile）]** を選択します。

Step 2 次のいずれかの手順を実行します。

- 新しいプロファイルを作成するには、[新規追加（Add New）] をクリックします。
- 既存の SIP プロファイルを選択するには、[検索（Find）] をクリックします。

Step 3 [SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウの各フィールドを設定します。

フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 4 [保存（Save）] をクリックします。

SIP トランク セキュリティ プロファイルを構成します。

SIP ゲートウェイに接続するトランクのセキュリティ設定とともに SIP トランクセキュリティプロファイルを設定します。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [セキュリティ（Security）] > [SIP トランク セキュリティプロファイル（SIP Trunk Security Profile）]** を選択します。

Step 2 次のいずれかの手順を実行します。

a) 既存のプロファイルを選択するには、[検索（Find）] をクリックします。

b) 新しいプロファイルを作成するには、[新規追加（Add New）] をクリックします。

Step 3 [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）] ウィンドウの各フィールドに入力します。

フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 4 [保存（Save）] をクリックします。

SIP ゲートウェイ向け SIP トランクの設定

SIP を使用するシスコまたはサードパーティのゲートウェイに Unified Communications Manager を接続するように、SIP トランクを設定します。この設定では、[**ゲートウェイの設定 (gateway configuration**)] ウィンドウでゲートウェイをデバイスとして入力しないでください。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]>[トランク（Trunk）]** を選択します。

Step 2 [新規追加（Add New）] をクリックして、新しい SIP トランクを設定します。

Step 3 [トランクタイプ（Trunk Type）] ドロップダウンリストから、[SIP トランク（SIP Trunk）] を選択します。

Step 4 [プロトコル（Protocol）] ドロップダウンリストから [なし（None）] を選択します。

Step 5 [SIP 情報（SIP Information）] ペインの [宛先アドレス（Destination Address）] フィールドに、SIP ゲートウェイの IP アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

Step 6 [SIP トランクのセキュリティプロファイル（SIP Trunk Security Profile）] ドロップダウンリストから、このゲートウェイ用に設定した SIP トランクのセキュリティプロファイルを選択します。

Step 7 [SIP プロファイル（SIP Profile）] ドロップダウンリスト ボックスから、このゲートウェイに設定した SIP プロファイルを選択します。

Step 8 [SIP トランク設定（SIP Trunk Configuration）] ウィンドウで各フィールドを設定します。フィールドの説明については、オンライン ヘルプを参照してください。

Step 9 [保存（Save）] をクリックします。

H.323 ゲートウェイの設定

Unified Communications Manager で、非ゲートキーパー H.323 の導入環境に対する H.323 ゲートウェイを設定します。

（注） H.323 ゲートキーパーを導入しない場合は、ゲートキーパー制御の H.225 トランクをセットアップして、H.323 ゲートウェイを追加することもできます。ゲートキーパーの使用率は、近年減少傾向にあるため、このシナリオは本書には記載していません。ゲートキーパーおよび H.225 ゲートキーパー制御のトランクを設定する場合は、『*Cisco Unified Communications Manager* リリース *10.0(1)* アドミニストレーション ガイド』を参照してください。

（注） ゲートウェイを Unified Communications Manager に登録した後に Unified Communications Manager でゲートウェイの登録ステータスが「不明」と表示される場合があります。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ゲートウェイ (Gateway)]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [ゲートウェイタイプ（Gateway Type）] ドロップダウンリストから、[H.323ゲートウェイ（H.323 Gateway）] を選択します。

Step 4 [デバイス名（Device Name）] フィールドに、ゲートウェイの IP アドレスまたはホスト名を入力します。

Step 5 H.235 を使用してセキュア チャネルを設定するには、[H.235 データのパススルー（H.235 Data Passthrough）] チェックボックスをオンにします。

Step 6 [ゲートウェイの設定（Gateway Configuration）] ウィンドウのフィールドを設定します。

フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 7 [保存（Save）] をクリックします。

Step 8 [リセット（Reset）] をクリックしてゲートウェイをリセットし、変更を適用します。

ほとんどのゲートウェイでは、設定の変更を適用するためにリセットする必要があります。リセットを行う前に、必要なゲートウェイ設定をすべて完了することをお勧めします。

ゲートウェイに対するクラスタ全体のコール分類の設定

ネットワーク ゲートウェイの [コールの分類（Call Classification）] を設定します。この設定は、システムがネットワークでゲートウェイが内部（OnNet）、または外部（OffNet）であると見なすかどうかを決定します。

[コールの分類（Call Classification）] フィールドが、個々のゲートウェイ ポート インターフェイスの設定ウィンドウに表示されます。デフォルトでは、各ゲートウェイ ポートインターフェイスはクラスタ全体のサービスパラメータの設定を使用するように設定されています。ただし、ポートでの [コールの分類（Call Clasification）] の設定がクラスタ全体のサービスパラメータとは異なる場合、ポートでの設定がサービスパラメータの設定よりも優先されます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 [サーバ（Server）] ドロップダウン リストから、Cisco CallManager サービスを実行しているサーバを選択します。

Step 3 [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。

Step 4 [クラスタ全体のパラメータ（デバイス - 概要）（Clusterwide Parameters (Device - General)）] で、[コールの分類（Call Classification）] サービスパラメータに次の値のいずれかを設定します。

- [オンネット（OnNet）]：このゲートウェイからのコールが、企業ネットワーク内から発信されているものと分類されます。
- [オフネット（OffNet）]：このゲートウェイからのコールが、企業ネットワーク外から発信されているものと分類されます。

Step 5 [保存（Save）] をクリックします。

オフネットゲートウェイ転送のブロック

外部（オフネット）ゲートウェイ間で転送されるコールをブロックするようにシステムを設定する場合は、この手順を使用します。デフォルトでは、ある外部ゲートウェイから別の外部ゲートウェイへの転送は許可されます。

ゲートウェイが外部（OffNet）であるか内線（OnNet）であるかどうかを判別する設定は、コール分類設定によって決定されます。これは、クラスタ全体のサービスパラメータを使用するか、次のいずれかのポート インターフェイスを設定することで設定します。

- MGCP T1/E1 ポート インターフェイス
- MGCP FXO ポート インターフェイス
- H.323 ゲートウェイ
- SIP トランク

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 [サーバ（Server）] ドロップダウン リストから、Cisco CallManager サービスを実行しているサーバを選択します。

Step 3 [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。

Step 4 [オフネットからオフネットへの転送をブロック（Block OffNet to Offnet Transfer）] サービスパラメータを設定します。

- **True**：2つの外部（オフネット）ゲートウェイ間の転送をキャンセルするには、このオプションを選択します。
- **False**：2 つの外部（オフネット）ゲートウェイ間の転送を許可するには、このオプションを選択します。これがデフォルトのオプションです。

Step 5 [保存（Save）] をクリックします。

（注） ゲートウェイをルートパターンに関連付け、[ルートパターンの設定（Route Pattern Configuration）] ウィンドウで [コールの分類（Call Classification）] を設定することで、ゲートウェイを介してコールをオンネットまたはオフネットに分類することもできます。

第 12 章

SRST の設定

Survivable Remote Site Telephony の概要

Survivable Remote Site Telephony（SRST）は、Unified Communications Manager ノードとのワイド エリア ネットワーク（WAN）接続に依存するサイト用のオプション機能です。SRST リファレンスは、Unified Communications Manager 管理インターフェイスで構成されています。WAN の故障が発生した場合、IP ゲートウェイは、次のようにリモートサイトの IP 電話に限定されたテレフォニーサービスを提供することができます。

- リモート サイトの IP 電話は互いにコールできます。
- PSTN からのコールは IP 電話に到達できます。
- IP 電話からのコールは PSTN を介して外部に到達できます。

リモート サイトの電話が、関連付けられているすべての Unified Communications Manager ノードに接続できない場合、SRST リファレンスの IP ゲートウェイに接続します。IP 電話のステータス行には、IP 電話がバックアップ SRST ゲートウェイにフェールオーバーしたことが示されます。Unified Communications Manager への接続が復元されると、Unified Communications Manager と完全なテレフォニーサービスに再登録された IP 電話が復元されます。

SRST は、PSTN ゲートウェイ アクセスに加えて、SCCP および SIP エンドポイントが混在している可能性があるリモート サイトをサポートします。

接続モニタ間隔

ワイド エリア ネットワーク（WAN）を介して SRST ゲートウェイに接続する IP 電話は、WAN リンクを介した Unified Communications Manager との接続を確立できると直ちに Unified Communications Manager に再接続します。ただし、WAN リンクが不安定な場合、IP 電話は SRST に切り替えたり、Unified Communications Manager に切り替えたりします。このため、電話サービスが一時的に失われます（ダイヤル トーンが聞こえません）。このような再接続の試行は、WAN

リンク フラッピング問題と呼ばれ、IP 電話が Unified Communications Manager に正常に再接続するまで続きます。

Unified Communications Manager と SRST ゲートウェイの間での WAN リンク フラッピングの問題を解決するために、IP 電話が Unified Communications Manager から SRST ゲートウェイを登録解除して再登録するまでに、IP 電話が Unified Communications Manager との接続をモニタする秒数（接続モニタ間隔）を定義することができます。IP 電話は、XML 構成ファイルに指定された接続モニタ間隔の値を受信します。

Survivable Remote Site Telephony の設定タスクフロー

始める前に

ダイヤル プランを検証します。ダイヤル プランに 7 か 8 桁の数字があるとき、場合によりトランスレーションルールを設定する必要があります。トランスレーションルールの詳細については、「変換パターンの設定 （216 ページ）」を参照してください。

手順

	コマンドまたはアクション	目的
Step 1	SRST 参照の設定 （133 ページ）	他のすべての Unified Communications Manager ノードに到達できない場合に、制限付きのコール制御機能を提供するゲートウェイを設定します。
Step 2	デバイスプールへの SRST リファレンスの割り当て （133 ページ）	各デバイスプールに対して、Unified Communications Manager を使用できない場合に、コールの完了を試みる発信側デバイスが検索するゲートウェイを割り当てます。
Step 3	次のいずれかの操作を実行します。 • クラスタの接続モニタ期間の設定 （134 ページ） • デバイスプールの接続モニタ期間の設定 （134 ページ）	**任意：**接続モニタ期間を設定します。クラスタ全体のデフォルト値を適用することも、デバイスプール内のデバイスに設定を適用することもできます。
Step 4	SRST ゲートウェイでの SRST の有効化 （135 ページ）	ゲートウェイで SRST パラメータを設定します。

SRST 参照の設定

SRST リファレンスは、デバイスのその他すべての Cisco Unified Communications Manager ノードが到達不能の場合に、Cisco Unified Communications Manager の一部機能を利用できるゲートウェイで構成されます。

手順

Step 1 Cisco Unified CM Administration にログインし、**[システム（System）]** > **[SRST（SRST）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [SRSTリファレンスの設定（SRST Reference Configuration）] ウィンドウの各フィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 4 [保存（Save）] をクリックします。

デバイスプールへの SRST リファレンスの割り当て

電話機の各デバイスプールに SRST を設定できます。デバイスプールに SRST リファレンスを割り当てると、デバイスプールのすべての電話機が、Cisco Unified Communications Manager のノードに到達できない場合、割り当てた SRST に接続を試みます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]** > **[デバイスプール（Device Pool）]** を選択します。

Step 2 [検索（Find）] をクリックし、リモート IP 電話が登録されているデバイスプールを選択します。

Step 3 [ローミングに合わせて変化する設定（Roaming Sensitive Settings）] エリアの [SRST リファレンス（SRST Reference）] ドロップダウンリストから SRST を選択します。

[SRST リファレンス（SRST Reference）] ドロップダウンリストには次のオプションがあります。

- [無効（Disable）]：電話機は、Cisco Unified Communications Manager のいずれのノードにも到達できない場合、SRST ゲートウェイへの接続を試みません。
- [デフォルト ゲートウェイを使用（Use Default Gateway）]：電話機は、Cisco Unified Communications Manager のいずれのノードにも到達できない場合、IP ゲートウェイを SRST ゲートウェイとして接続を試みます。
- [ユーザ定義（User-Defined）]：電話が任意の Cisco Unified Communications Manager ノードに接続できない場合、SRST ゲートウェイへの接続を試みます。

Step 4 [保存（Save）] をクリックします。

クラスタの接続モニタ期間の設定

この手順は省略可能です。接続モニタ間隔のシステム値（エンタープライズパラメータ）を変更する場合だけ、この手順を完了します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

Step 2 [接続モニタ間隔（Connection Monitor Duration）] フィールドに値を入力します。デフォルト値は 120 秒です。フィールドに入力できる最大秒数は、2592000 秒です。

Step 3 [保存（Save）] をクリックします。

（注） 変更を有効にするにはすべてのサービスを再起動する必要があります。

このエンタープライズパラメータには、接続モニタ期間に対するクラスタのデフォルトを設定します。ただし、それよりも優先される設定がデバイスプールに存在する場合、その設定が、デバイスプールを使用するデバイスのエンタープライズパラメータ設定よりも優先されます。

デバイスプールの接続モニタ期間の設定

この手順は省略可能です。この操作は、次の項目に該当する場合に限り実行します。

- 接続モニタの期間について、クラスタ全体の値を使用しない場合。
- このデバイスプールの接続モニタ期間の値を個別に定義する場合。

ヒント デバイスプールの接続モニタ間隔の値を変更する場合、値は更新されるデバイスプールだけに適用されます。その他すべてのデバイスプールは、各自の [接続モニタ間隔（Connection Monitor Duration）] フィールドの値を使用するか、[接続モニタ間隔（Connection Monitor Duration）] エンタープライズパラメータで設定されたクラスタ全体用の値を使用します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [デバイスプール（Device Pool）]** を選択します。

Step 2 [検索（Find）] をクリックし、リモート IP 電話が登録されているデバイスプールを選択します。

Step 3 [ローミングに合わせて変化する設定（Roaming Sensitive Settings）] エリアで、[接続モニタ間隔（Connection Monitor Duration）] フィールドに値を入力します。フィールドに入力できる最大秒数は、2592000 秒です。

（注） この設定は、エンタープライズパラメータの接続モニタ間隔設定をオーバーライドします。

Step 4 [保存（Save）] をクリックします。

SRST ゲートウェイでの SRST の有効化

始める前に

- デバイスプールへの SRST リファレンスの割り当て （133 ページ）
- （オプション）次のいずれかのタスクを実行します。
  - クラスタの接続モニタ期間の設定 （134 ページ）
  - デバイスプールの接続モニタ期間の設定 （134 ページ）

手順

Step 1 SRST ゲートウェイ（ルータ）にログインします。

Step 2 **Call-manager-fallback** コマンドを入力します。
このコマンドは、ルータの SRST を有効にします。

Step 3 **max-ephones** max-phones コマンドを入力します。ここで、max-phones は、サポート対象の Cisco IP Phone の最大数です。

Step 4 **max-dn** max-directory-numbers コマンドを入力します。ここで、max-directory-numbers は、ルータでサポートできる電話番号（DN）または仮想化音声ポートの最大数です。

Step 5 **ip source-address** ip-address コマンドを入力します。ここで、ip-address は既存のルータ IP アドレスで、通常はルータのイーサネットポートのアドレスの 1 つです。
このコマンドにより、SRSTルータは、指定されたIPアドレスを介してシスコIP電話からメッセージを受信することができます。

SRST の制限

制限事項	説明
SRST リファレンスの削除	デバイスプールまたはその他の項目によって使用されている SRST リファレンスは削除できません。SRST リファレンスを使用しているデバイスプールを特定するには、[SRSTリファレンスの設定（SRST Reference Configuration）] ウィンドウの [依存関係レコード（Dependency Records）] リンクをクリックします。システムで依存関係レコードが有効でない場合、[依存関係レコードサマリー（Dependency Records Summary）] ウィンドウにメッセージが表示されます。使用中の SRST リファレンスを削除しようとすると、Unified Communications Manager にエラー メッセージが表示されます。現在使用中の SRST リファレンスを削除する前に、次のタスクのいずれかまたは両方を実行します。 • 削除する SRST リファレンスを使用しているすべてのデバイスプールに別の SRST リファレンスを割り当てます。 • 削除する SRST リファレンスを使用しているデバイスプールを削除します。 （注） SRST リファレンスを削除するときは、削除する SRST リファレンスが正しいかどうかを慎重に確認してください。削除した SRST リファレンスを元に戻すことはできません。SRST リファレンスを誤って削除した場合は、再作成する必要があります。

第 13 章

メディアリソースの設定

メディアリソースについて

Cisco Unified Communications Manager の機能では、メディアリソースが使用されます。Cisco Unified Communications Manager には次のようなメディアリソースが含まれます。

- アナンシエータ
- 音声自動応答（IVR）
- メディア ターミネーション ポイント（MTP）
- トランスコーダ
- トラステッド リレー ポイント
- 会議ブリッジ
- 保留音または保留中ビデオ

メディアリソースをメディアリソースグループの一覧に割り当て、そのリストをデバイスプールまたは個々のデバイスに割り当てることによって、電話で利用可能にすることができます。個々のデバイスのデフォルト設定では、デバイスが使用しているデバイスプールに割り当てられているメディアリソースを使用します。

（注） 保留音の設定の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。

メディア ターミネーション ポイント

メディア ターミネーション ポイント（MTP）は、2 つの全二重メディアストリームを受信して、それらをまとめてブリッジし、個別に設定と分解を行えるようにするためのエンティティです。Cisco Unified Communications Manager は、MTP をメディアパスに挿入して、次のようなさまざまな状況を解決できます。

- Trusted Relay Point（TRP）として動作する場合
- RTP ストリームに対して IPv4 と IPv6 の変換を提供する場合
- SIP トランク経由で SIP アーリーオファーを配信する場合
- DTMF トランスポートの不一致に対処する場合
- RSVP エージェントとして動作する場合

H.323 コールの MTP

メディア ターミネーション ポイントをH.323 コールのメディア パスに挿入することで、H.323 エンドポイントにコールがルーティングされた場合に通常は利用できない補完的サービス（コール保留、コール転送、通話パーク、会議など）を拡張できます。H.323 補足サービスで MTP が必要となるのは、Empty Capability Set（ECS）または FastStart をサポートしていないエンドポイントのみです。ECS および FastStart をサポートしているすべての Cisco および他のサードパーティ製エンドポイントでは、MTP は必要ありません。

MTP タイプ

Cisco Unified Communications Manager では、次の MTP タイプがサポートされています。

- IOS ゲートウェイのソフトウェア MTP
- IOS ゲートウェイのハードウェア MTP
- Cisco IP Voice Media Streaming サービスが提供するソフトウェア MTP

シスコ メディア ターミネーション ポイント ソフトウェアの MTP タイプでは、ネットワークの速度とネットワーク インターフェイス カード（NIC）に応じて、デフォルトで 48 個のユーザ設定可能な MTP リソースが提供されます。たとえば、100 MB のネットワーク/NIC カードが 48 の MTP リソースをサポートできるのに対して、10 MB の NIC カードは同数のリソースをサポートできません。

10 MB のネットワーク/NIC カードの場合は、約24の MTP リソースを提供できます。ただし、使用可能な MTP リソースの正確な数は、PC 上の他のアプリケーションが消費しているリソース、プロセッサの速度、ネットワーク負荷、その他のさまざまな要因によって異なります。

MTP 登録

MTP デバイスは、プライマリ Cisco Unified Communications Manager が使用可能である場合は常にその Cisco Unified Communications Manager に登録され、サポートしている MTP リソースの数を

Cisco Unified Communications Manager に通知します。同じ Cisco Unified Communications Manager に複数の MTP を登録できます。特定の Unified Communications Manager に複数の MTP が登録されている場合、その Cisco Unified Communications Manager は、MTP ごとのリソース セットを制御します。

たとえば、MTP サーバ 1 が 48 の MTP リソース用に設定され、MTP サーバ 2 は 24 のリソース用に設定されているとします。両方の MTP が同じ Unified Communications Manager を登録する場合、その Unified Communications Manager は両方のリソース セット、つまり、合計 72 の登録済み MTP リソースを保持します。

Unified Communications Manager は、コール エンドポイントで MTP が必要であると判定すると、アクティブ ストリームが最も少ない MTP から MTP リソースを割り当てます。その MTP リソースは、エンドポイントの代わりにコールに挿入されます。MTP リソースの使用は、システムのユーザにも、リソースが代わりに挿入されたエンドポイントにも見えない形で行われます。MTP リソースが必要なときに、そのリソースが使用できない場合、コールは MTP リソースを使用せずに接続されるため、そのコールは補足サービスを利用できないことになります。

SRTP DTMF インターワーキング

重要 このセクションは、リリース 14SU3 以降に適用されます。

現在、Unified CM は、セキュアコールと非セキュアコールの両方で DTMF の不一致に対して MTP を挿入します。ただし、セキュアコールの場合、DTMF の不一致に対して MTP が挿入されますが、MTP は当事者間のメディアを通過するだけです。したがって、DTMF イベントは当事者間で送信されません。Unified CM Release 14SU3 より前のリリースでは、DTMF の不一致に対して MTP が割り当てられている場合、DTMF 変換は非セキュアコールに対してのみ機能していました。

ゲートウェイ IOS バージョン 17.10.1a 以降では、DTMF 変換のゲートウェイ側からのセキュアな MTP がサポートされています。 Unified Communications Manager に登録されているセキュアな IOS ベースの MTP は、SRTP DTMF インターワークをサポートするようになりました。リリース 14SU3 以降のゲートウェイからのこのサポートの追加により、Unified CM は、セキュアなエンドポイント間の DTMF の不一致に対してハードウェア MTP（SRTP DTMF インターワークサポート付き）を呼び出すことができます。

Unified Communications Manager は、SCCP メッセージで SRTP キーを MTP に送信するようになりました。MTP はキーを使用して、インバンド DTMF イベントをアウトオブバンドイベントに復号化し、他のコールレッグに送信します。同様に、アウトオブバンド DTMF イベントの場合、Unified Communications Manager は暗号化されたインバンド DTMF イベントを他のコールレッグに挿入します。

重要な考慮事項

- Unified Communications Manager のリリース 14SU3 以降では、次の Cisco IOS XE 17.10.1a 以降でこの機能がサポートされています。
  - Cisco 4461 サービス統合型ルータ（ISR）

- Cisco Catalyst 8200 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8300 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8000V Edge ソフトウェア

（注） この機能に必要なゲートウェイ設定の詳細については、サポートされている Cisco IOS XE 17.10.1a 以降のプラットフォームのそれぞれの『設定ガイド』を参照してください。

- Unified Communications Manager とゲートウェイ間の正常な TLS 1.2 接続は必須です。TLS 1.2 の設定の詳細については、Cisco Unified Communications Manager セキュリティ ガイドを参照してください。
- この機能は、パススルーモードのハードウェア MTP、つまり、パススルーモードで DTMF-SRTP インターワークをサポートする IOS ゲートウェイを使用して登録された MTP でのみサポートされます。
- この機能は、IPVMS ベースの MTP および H.323 コール フローではサポートされていません。

メディア ターミネーション ポイントの連携動作と制限事項

表 *7:* メディア ターミネーション ポイントの連携動作と制限事項

制限事項	説明
Cisco IP 音声ストリーム アプリケーション	1 台のサーバでアクティブにできる Cisco IP Voice Streaming Application は 1 つに限定されます。追加の MTP リソースを提供するには、ネットワーク上にある他のサーバで Cisco IP Voice Streaming アプリケーションをアクティブにすることができます。 Cisco Unified Communications Manager のパフォーマンスに悪影響を与える可能性があるため、コール処理の負荷が大きい Cisco Unified Communications Manager 上では Cisco IP Voice Streaming Media Application をアクティブにしないようにすることを強くお勧めします。
Cisco Unified Communications Manager への登録	各 MTP が一度に登録できる Cisco Unified Communications Manager は 1 つに限定されます。システム内には、設定内容に応じて、複数の MTP を存在させることができます。各 MTP は、1 つの Cisco Unified Communications Manager に登録できます。

制限事項	説明
フェールオーバーとフォールバック	ここでは、MTP デバイスが登録されている Cisco Unified Communications Manager が到達不能になったときの、MTP デバイスのフェールオーバーとフォールバックの方法について説明します。 • プライマリ Cisco Unified Communications Manager に障害が発生した場合、MTP は、MTP が属するデバイスプールに対して指定された Cisco Unified Communications Manager グループ内で、次に使用可能な Cisco Unified Communications Manager への登録を試みます。 • プライマリ Cisco Unified Communications Manager が障害後に使用可能な状態に戻り、現在まだ使用されていない場合、MTP デバイスはただちにプライマリ Cisco Unified Communications Manager に再登録されます。 • コール保存モードでアクティブだったコールまたは会議は、すべてのパーティが切断されるまで、システムによって保持されます。システムは、補足サービスを使用可能にしません。 • MTP が新しい Cisco Unified Communications Manager への登録を試み、登録確認応答を受信しなかった場合、MTP は次の Cisco Unified Communications Manager に登録されます。 MTP デバイスは、ハード リセットまたはソフト リセット後に登録を解除し、続いて接続を解除します。リセットが完了すると、デバイスは Cisco Unified Communications Manager に再登録されます。

トランスコーダ

トランスコーダは、コーデック変換を実行するデバイスで、あるコーデックからの入力ストリームを、別のコーデックを使用する出力ストリームに変換します。たとえば、トランスコーダは G.711 コーデックのストリームを取り込み、それを G.729 ストリームにリアルタイムで変換できます。通話中にエンドポイントが異なる音声コーデックを使用すると、Cisco Unified Communications Manager が、そのメディアパスでトランスコーダを呼び出します。トランスコーダは、2 つの互換性のないコーデック間でデータストリームを変換して、デバイス間で通信をできるようにします。トランスコーダは、その通話に関係するユーザーやエンドポイントには表示されません。

トランスコーダのリソースは、メディアリソースマネージャー (MRM) によって管理されます。

Opus コーデック トランスコーダのサポート

Important このセクションは、リリース 14SU1 以降に適用されます。

Cisco Unified Communications Manager には、Skinny Client Control Protocol（SCCP）制御の iOS ベースの登録済みメディアリソースが含まれています。これは、メディアネゴシエーションの成功に必要な Opus オーディオコーデックのトランスコーディングをサポートしています。

Cisco エンドポイントのほとんどは、Opus コーデックをサポートしています。Opus コーデックは、低帯域幅環境でG711/G729よりも優れた品質を提供します。Opusコーデックトランスコーダのサポートにより、Unified CM は、Opus コーデックの不一致に対してトランスコーダを呼び出し、Opusコーデック側で低いビットレートを、リモート側で高いビットレートを可能にします。ただし、Opus コーデックでサポートされているトランスコーダの Unified CM への登録が完了している必要があります。

サポートされるバージョン

Opus トランスコーディング 機能は、次の Unified Communications Manager とゲートウェイバージョンで動作します。

- Unified CM バージョン 14 SU1 以降
- ゲートウェイ IOS バージョン IOS XE 17.6.1
- DSP ファームウェアバージョン 58.2.0 以降

構成

1. Opus コーデック トランスコーディングをサポートする Integrated Service Router（ISR）ゲートウェイを使用してトランスコーダを構成します。Opus コーデックをトランスコーダ プロファイルに追加する必要があります。
2. Opus コーデックをサポートするトランスコーダを Cisco Unified Communications Manager DSPFARM プロファイルに登録します。
3. トランスコーダを、トランスコーディングを要求するエンドポイントまたはトランクのメディア リソース グループ リスト（MRGL）に関連付け、両方の発呼側間のリージョン設定を7kbpsに構成します。

Note トランスコーダで構成される MRGL を両方の発呼者のデバイスプールに関連付けると、Unified CM はメディアネゴシエーションのために適切なトランスコーダを呼び出します。詳細については、トランスコーダの設定を参照してください。

MTP 機能を使用したトランスコーダ

コーデック変換に加えて、トランスコーダは、メディアターミネーションポイント (MTP) と同じ機能を提供できます。コーダ機能と MTP 機能が両方とも必要な場合、システムは、両方の機能セットを同時に提供できるため、トランスコーダを割り当てます。MTP 機能のみが必要な場合は、システムはリソースプールからトランスコーダまたは MTP のいずれかを割り当てます。リソースの選択は、メディアリソースグループによって決定されます。

ソフトウェア MTP リソースが必要なときに利用できない場合、コールは、**[Cisco Unified CM Administration]** > **[システム（System）]** > **[サービスパラメータ（Service Parameters）]** > **[サービスパラメータ構成（Service Parameter Configuration）]** ウィンドウの **[信頼されるリレーポイントの割り当てに失敗した場合通話も失敗（Fail Call If Trusted Relay Point Allocation Fails）]** フィー

ルドと **[MTP割り当てに失敗した場合通話も失敗（Fail Call If MTP Allocation Fails）]** フィールドが「False」に設定されている場合、MTP リソースと MTP/TRP サービスを使用せずに接続を試行します。ハードウェア トランスコーダ機能が（あるコーデックを別のコーデックに変換するために）必要であり、トランスコーダが使用できない場合、コールは失敗します。

トランスコーダタイプ

Cisco Unified Communications Manager の管理ページにおけるトランスコーダタイプは次の表のとおりです。

（注） トランスコーダは、G.711 とすべてのコーデック（トランスコーダとして機能している G.711 や MTP/TRP 機能を提供している G.711 を含む）の間のトランスコーディングをサポートします。

表 *8:* トランスコーダタイプ

トランスコーダタイプ	説明
Cisco Media Termination Point Hardware	このタイプは Cisco Catalyst 4000 WS-X4604-GWY および Cisco Catalyst 6000 WS-6608-T1 または WS-6608-E1 をサポートし、次のトランスコーディング セッション数を提供します。 Cisco Catalyst 4000 WS-X4604-GWY の場合 • G.711 へのトランスコーディング：16 の MTP トランスコーディング セッション Cisco Catalyst 6000 WS-6608-T1 または WS-6608-E1 の場合 • G.723 から G.711 へのトランスコーディング/G.729 から G.711 へのトランスコーディング：1 つの物理ポート当たり 24 の MTP トランスコーディング セッション、1 つのモジュール当たり 192 セッション
Cisco IOS Media Termination Point（ハードウェア）	このタイプは Cisco 2600XM、Cisco 2691、Cisco 3725、Cisco 3745、Cisco 3660、Cisco 3640、Cisco 3620、Cisco 2600、および Cisco VG200 ゲートウェイをサポートし、次のトランスコーディング セッション数を提供します。 NM-HDV 単位 • G.711 から G.729-60 へのトランスコーディング • G.711 から GSM FR/GSM EFR へのトランスコーディング：45

トランスコーダタイプ	説明
Cisco IOS Enhanced Media Termination Point（ハードウェア）	**NM-HD 単位** このタイプは Cisco 2600XM、Cisco 2691、Cisco 3660、Cisco 3725、Cisco 3745、および Cisco 3660 アクセス ルータをサポートし、次のトランスコーディング セッション数を提供します。 • G.711 から G.729a/G.729ab/GSMFR へのトランスコーディング：24 • G.711 から G.729/G.729b/GSM EFR へのトランスコーディング：18 **NM-HDV2 単位** このタイプは Cisco 2600XM、Cisco 2691、Cisco 3725、Cisco 3745、および Cisco 3660 アクセス ルータをサポートし、次のトランスコーディング セッション数を提供します。 • G.711 から G.729a/G.729ab/GSMFR へのトランスコーディング：128 • G.711 から G.729/G.729b/GSM EFR へのトランスコーディング：96 **PVDM4** • オンボード PVDM4 モジュール（PVDM4-32、PVDM4-64、PVDM4-128、PVDM4-256） • T1/E1 モジュールの DSP モジュール（PVDM4-32、PVDM4-64、PVDM4-128、PVDM4-256） • DSP NIM（NIM-PVDM4-32、NIM-PVDM4-64、NIM-PVDM4-128、NIM-PVDM4-256） これらのタイプは ISR4K (ISR44xx、ISR43xx)、C83xx、および C82xx プラットフォームをサポートし、次の数のトランスコーディング セッションを提供します。 • G.711 から G.729a/G.729ab/GSMFR へのトランスコーディング：24 • G.711 から G.729/G.729b/GSM EFR へのトランスコーディング：18 • G.711 から G.729a/G.729ab/GSMFR へのトランスコーディング：128 • G.711 から G.729/G.729b/GSM EFR へのトランスコーディング：96 • G.711/G.729/G.729ab/G.729a/G.729b から Opus へのトランスコーディング

トランスコーダタイプ	説明
Cisco Media Termination Point (WS-SVC-CMM)	このタイプは、装着されているドーターカード当たり64のトランスコーディング セッションを提供します。1 枚のドーター カードでは 64 のトランスコーディング セッション、2 枚のドーター カードでは 128 のトランスコーディング セッション、3 枚のドーター カードでは 192 のトランスコーディング セッション、4 枚のドーター カード（最大）では 256 のトランスコーディング セッションを提供します。 このタイプは、次のコーデックの任意の組み合わせの間でトランスコーディングを提供します。 • G.711 a-law および G.711 mu-law • G.729 annex A および annex B • G.723.1 • GSM（FR） • GSM（EFR）

トランスコーダの連携動作と制限事項

トランスコーダの連携動作と制限事項

連携動作または制限事項	説明
トランスコーダの削除	メディアリソースグループに割り当てられているトランスコーダは、削除できません。トランスコーダを使用しているメディアリソースグループを検索するには、**[トランスコーダの設定(Transcoder Configuration)]** ウィンドウの **[関連リンク(Related Links)]** ドロップダウンリストボックスから **[依存関係レコード(Dependency Records)]** を選択し、**[移動(Go)]** をクリックします。[依存関係レコードサマリー(Dependency Records Summary)] ウィンドウに、トランスコーダを使用しているメディアリソースグループに関する情報が表示されます。メディアリソースグループに関するより詳細な情報を見つけるには、メディアリソースグループをクリックして [依存関係レコード詳細(Dependency Records Detail)] ウィンドウを表示します。システムで依存関係レコードが有効でない場合、[依存関係レコードサマリー（Dependency Records Summary）] ウィンドウにメッセージが表示されます。使用中のトランスコーダを削除しようとすると、Cisco Unified Communications Manager からメッセージが表示されます。現在使用されているトランスコーダを削除する前に、割り当てられているメディアリソースグループからトランスコーダを削除する必要があります。

連携動作または制限事項	説明
フェールオーバーとフォールバック	トランスコーダのフェールオーバーとフォールバックは以下のように動作します。 • プライマリ Unified Communications Manager ノードに障害が発生した場合、トランスコーダは、トランスコーダに属するデバイスプールに指定されたUnified Communications Manager Group で利用可能な次のノードで登録を試行します。 • プライマリ Cisco Unified Communications Manager が使用可能な状態に戻ると、そのトランスコーダは、ただちにプライマリ Cisco Unified Communications Manager に登録されます。 • トランスコーダデバイスは、到達不能になった Unified Communications Manager ノードの登録を解除します。トランスコーディングにこのトランスコーディングプロファイルを使用していた通話は保存状態に移行し、トランスコーダは次に使用可能なノードの登録を試行します。ゲートウェイは、RTP/RTCP タイムアウトを使用して、登録済みの Unified Communications Manager にリソースの解放を通知します。 • トランスコーダが新規 Unified Communications Manager ノードの登録を試行したが、登録確認応答を受信しない場合は、トランスコーダはリスト内の次のノードを登録します。 トランスコーダ デバイスは、ハード リセットまたはソフト リセット後に登録を解除し、続いて接続を解除します。リセットが完了すると、デバイスはプライマリ Cisco Unified Communications Manager ノードに再登録されます。

連携動作または制限事項	説明
Opus コーデック トランスコーダのサポート	トランスコーダプロファイルが Unified Communications Manager で登録されている場合、次のシナリオが挙げられます。 • ISR ゲートウェイが Opus トランスコーディングをサポートしていて、Unified CM が Opus トランスコーディングをサポートしていない場合、システムはコーデックの不一致に対してトランスコーダを割り当てます。ただし、必要なパラメータがこれらの SCCP メッセージに存在しないため、ISR ゲートウェイは、OpenReceiveChannel（ORC）および StartMediaTransmission（SMT）SCCP メッセージを拒否します。 • ISR ゲートウェイが Opus トランスコーディングをサポートしておらず、Unified CM が Opus コーデック トランスコーディングをサポートしている場合、Opus のトランスコーダ割り当て要求は失敗します。 • ファイル マルチキャスト トランスポート プロトコル（FMTP）の「sprop-stereo」パラメータ値の 1 つが SDP で 1 に設定されている Opus コーデックをエンドポイントがサポートしている場合、システムは 1 に設定されている「sprop-stereo」の ORC/SMT メッセージを OLC/SMT を拒否するゲートウェイに送信します。これにより、最終的に通話が切断されます。

トラステッドリレーポイントの概要

トラステッドリレーポイント (TRP) は、Cisco Unified Communications Manager がメディアストリームに挿入してコールメディアの制御ポイントとして機能する MTP またはトランスコーダです。TRP は、ストリームに対してさらなる処理を提供し、ストリームが特定のパスに従っていることを確認できます。

コールにトラステッドリレーポイントが必要な場合、Cisco Unified Communications Manager は、TRP 機能で有効になっている MTP またはトランスコーダを割り当てます。

構成

MTP およびトランスコーダ は、**[メディアターミネーションポイントの設定]**または**[トランザクションの設定]** ウィンドウの **[トラステッドリレーポイント]** チェックボックスをオンにすることによって TRP 機能を提供するように設定できます。

個々のコールの TRP 要件を設定するには、次の設定ウィンドウの **[トラステッドリレーポイントを使用する]** フィールドを **[オン]**に設定します。

- 電話の設定（Phone Configuration）
- ゲートウェイの設定（Gateway Configuration）

- ボイスメールポート設定（Voicemail Port Configuration）
- トランクの設定（Trunk Configuration）
- CTI ルートポイントの設定（CTI Route Point Configuration）
- 共通デバイス設定（Common Device Configuration）
- ユニバーサルデバイステンプレートの設定（Universal Device Template Configuration）
- さまざまなメディアリソースの設定（アナンシエータ、IVR、MTP、トランスコーダ、会議ブリッジ、保留音)

トラステッド リレー ポイントの連携動作と制限事項

機能	連携動作と制限事項
Resource Reservation Protocol（RSVP）	コールで RSVP が有効になっている場合、Cisco Unified Communications Manager はまず、TRP のラベルも付いている RSVPAgent を割り当てようとします。それ以外の場合は、別の TRP デバイスが RSVPAgent とエンドポイントの間に挿入されます。
コールのトランスコーダ	トランスコーダがコールに必要であり、それを TRP を必要とするエンドポイントと同じ側に割り当てる必要がある場合、Cisco Unified Communications Manager はまず、TRP のラベルも付いているトランスコーダを割り当てようとします。それ以外の場合は、別の TRP デバイスがトランスコーダとエンドポイントの間に挿入されます。
エンドポイントの MTP 割り当て	エンドポイント向けに、[メディアターミネーションポイントが必須（Media Termination Point Required）] チェックボックスおよび [トラステッドリレーポイントを使用（Use Trusted Relay Point）] チェックボックスをオンにすると、Cisco Unified Communications Manager は、TRP を兼ねる MTP を割り当てます。管理者がそのような MTP または TRP の割り当てに失敗すると、コールの状態が表示されます。
TRP 割り当て	ほとんどの場合、TRP はユーザがコールに応答した後に割り当てられるため、TRP の割り当てに失敗したためにコールが失敗すると、ユーザがコールに応答した後に速いビジートーンが聞こえる可能性があります。（MTP が必要な SIP アウトバウンド レッグ、つまり H.323 アウトバウンド FastStart は例外です）。

機能	連携動作と制限事項
エンドポイントの TRP 挿入	エンドポイントまたはデバイスに関連付けられているデバイスプールのいずれかで、[トラステッドリレーポイントを使用（Use Trusted Relay Point）]チェックボックスをオンにした場合、Cisco Unified Communications Manager はそのエンドポイント向けに TRP を挿入する必要があります。[トラステッドリレーポイントの割り当てに失敗した場合コールを失敗させる（Fail Call If Trusted Relay Point Allocation Fails）] サービスパラメータが、**True** に設定されている場合、Cisco Unified Communications Manager が TRP の割り当てに失敗すると、コールが失敗することがあります。
TRP とリモートユーザー	在宅リモートユーザーからの作業に安全なソリューションを提供するためには、TRP はお勧めしません。Expressway のモバイルおよびリモートアクセスが推奨されるソリューションです。

TRP リソースが不足したときのコール動作

次の項では、十分な MTP リソースが割り当てられていない場合に Cisco Unified Communications Manager がコールを処理する方法の例について説明します。最終的なコール動作は、これらのエンドポイントに MTP および TRP が必要かどうかと、MTP または TRPS の割り当てが失敗したときに自動的にコールを終了するようにシステムが設定されているかどうかによって異なります。

MTP と TRP の両方が必要な場合

次の表に、エンドポイントで[メディアターミネーションポイントが必須（Media Termination Point Required）] と [トラステッドリレーポイントを使用（Use Trusted Relay Point）] の両方のオプションが選択されており、MTP と TRP のリソースが不足した場合に、コールが終了するかどうかを示します。

最終的なコールのステータスは、[トラステッドリレーポイントの割り当てに失敗したらコールを終了（Fail Call If Trusted Relay Point Allocation Fails）] と [MTPの割り当てに失敗したらコールを終了（Fail Call if MTP Allocation Fails）] サービスパラメータが、コールの自動終了に設定されているかどうかによって異なります。

TRP の割り当てに失敗したらコールを終了（Fail Call If TRP Allocation Fails） サービスパラメータ	**MTP の割り当てに失敗したらコールを終了（Fail Call If MTP Allocation Fails） サービスパラメータ**	**Unified CM がコー**
True	True	はい
True	False	はい
False	True	はい（MTP が H 合）。いいえ（ 要な場合）
False	False	×

MTP/TRP リソースが不足した場合のコールの自動終了が有効化されていない場合

次の表に、MTP または TRP のリソースが不足しており、[トラステッドリレーポイントの割り当てに失敗したらコールを終了（Fail Call If Trusted Relay Point Allocation Fails）] と [MTPの割り当てに失敗したらコールを終了（Fail Call If MTP Allocation Fails）] のサービスパラメータが [False] に設定されている場合のコール動作を示します。

MTP が必須 = はい（Yes)	TRP を使用 = はい（Yes）	リソース割り当てのステータス	コールの動作
Y	Y	TRP 割り当て済み	パススルーのサポートが存在しないため、オーディオ コールのみ。
Y	Y または N	MTP のみ	オーディオコールのみ。TRP のサポートは存在しません。
Y	Y または N	割り当てなし	H.323 エンドポイントで [メディアターミネーションポイントが必須(Media Termination Point Required)] チェックボックスがオンになっている場合、補足サービスは無効になります。
N	Y	TRP 割り当て済み	エンドポイントの機能に応じてオーディオまたはビデオ コール、およびコールアドミッション制御（CAC）。補足サービスは引き続き機能します。
N	Y	割り当てなし	オーディオまたはビデオ コール。補足サービスは引き続き機能しますが、TRP のサポートは存在しません。

アナンシエータの概要

アナンシエータは、Cisco Unified Communications Manager で動作し、録音されたメッセージやトーンを Cisco IP Phone およびゲートウェイに送信することが可能な、SCCP ソフトウェアデバイスです。そのノード上で Cisco IP Voice Media Streaming service をオンにすると、アナンシエータがクラスタノード上でアクティブ化されます。MLPP、SIP トランク、IOS ゲートウェイ、ソフトウェア会議ブリッジなどの機能は、定義済みのメッセージを一方向のメディアストリーム経由で電話機またはゲートウェイに送信するように、アナンシエータに依存しています。さらに、

- IPv4 と IPV6 の両方がサポートされています。アナンシエータは、システムのプラットフォームが IPv6 に対して設定されており、IPv6 エンタープライズパラメータが有効化されている場合、自動的にデュアルモードに設定されます。
- SRTP がサポートされています

アナンシエータのスケーラビリティ

デフォルトでは、アナンシエータは48のメディアストリームを同時にサポートしています。追加ノードでアナンシエータをアクティブにするか、[コール数（Call Count）] サービスパラメータを使用してアナンシエータのメディア ストリームのデフォルト数を変更することで、キャパシティを増やすことができます。ただし、当該のノードで **Cisco CallManager** サービスが非アクティブ化されていない限り、ノードでこの値を増やすことは推奨しません。

Cisco CallManager サービスが実行されていない専用のサブスクライバ ノードでアナンシエータを実行する場合、アナンシエータは最大 255 の同時アナウンス ストリームをサポートできます。専用のサブスクライバーノードが 1 万ユーザの OVA バーチャルマシン設定に適合する場合、警報装置は最大 400 の同時アナウンスストリームをサポートできます。

⚠

注意 コール処理の負荷が高い Unified Communications Manager ノードではアナンシエータをアクティブにしないでください。

会議ブリッジを使用したアナンシエータ

このアナンシエータは、次の条件の下で会議ブリッジに使用できます。

- アナンシエータを含むメディアリソース グループ リストが、会議ブリッジが存在するデバイス プールに割り当てられている場合。
- アナンシエータがデフォルトのメディアリソースとして設定されている場合。

メディア リソース グループ リストが会議を制御するデバイスに直接割り当てられている場合は、会議ブリッジでアナンシエータを使用できません。

会議ごとにアナウンスを 1 つだけサポートします。現在のアナウンスの再生中に、システムが別のアナウンスを要求した場合は、新しいアナウンスによって再生中のアナウンスがプリエンプション処理されます。

デフォルトのアナンシエータのアナウンスおよびトーン

Cisco Unified Communications Manager では Cisco IP Media Streaming Application サービスが有効になると、録音されたアナンシエータアナウンスを自動的に提供します。アナウンスまたはトーンは、次の条件で再生されます。

- アナウンス：Cisco Multilevel Precedence and Preemption 用に設定されたデバイス向けに再生されます。
- 割り込み音：参加者がアドホック会議に参加する前に聞こえます。
- リングバックトーン: IOS ゲートウェイを介して PSTN 経由でコールを転送する場合、コールがアクティブになっていてもゲートウェイが音を再生できないため、アナンシエータがトーンを再生します。
- リングバックトーン：H.323 クラスタ間トランクを介してコールを転送するときに、トーンを再生します。

- リングバック トーン：SCCP を実行している電話機から SIP クライアントにコールを転送するとき、トーンを再生します。

デフォルトの事前に録音されたアナンシエータ アナウンスを変更したり、アナウンスを追加したりすることはできません。Cisco Unified Communications Manager ロケールインストーラがインストールされており、Cisco Unified IP Phone またはデバイスプールにロケールが設定されている場合は、アナウンスのローカリゼーションがサポートされます。ロケールインストーラと、ユーザおよび（対応する）ネットワーク ロケール用にインストールするファイルの詳細については、『*Cisco Unified Communications Manager* のインストール』を参照してください。ロケール インストーラをダウンロードするには、www.cisco.com のサポート ページを参照してください。

表 *9*：録音済みのアナンシエータ アナウンス

条件	アナウンス
同等またはそれ以上の優先コールが進行中です。	緊急度の高い電話が使用中のため、電話をおつなぎできません。一度電話をお切りになってから、もう一度おかけ直しください。これは録音メッセージです。
優先順位のアクセス制限が存在します。	緊急度の高い電話が使用中のため、電話をおつなぎできません。一度電話をお切りになってから、もう一度おかけ直しください。これは録音メッセージです。
許可されない優先順位の使用を試みた人物がいます。	ご使用になった優先度は、回線で認証されていません。認証された優先度をお使いになるか、交換手までお問い合わせください。これは録音メッセージです。
コールがビジー状態です。または管理者がコール待機用または優先処理用の電話番号を設定していません。	おかけになった番号は、大変込み合っており、この番号には割り込み機能が備わっておりません。一度電話をお切りになってから、もう一度おかけ直しください。これは録音メッセージです。
システムがコールを確立できません。	おかけになった電話番号では、正しくおつなぎできません。番号を確認してからもう一度おかけ直しいただくか、交換手までお問い合わせください。これは録音メッセージです。
サービスが中断されました。	サービス障害のため、電話をおつなぎできません。緊急の場合は、交換手までお電話ください。これは録音メッセージです。

次の表に、アナンシエータでサポートされるトーンを示します。

表 *10*：トーンの説明

タイプ	説明
話中音	ダイヤルされた番号が使用中の場合は、ビジートーンが聞こえます。
割り込みトーン	参加者がアドホック会議に参加する前に会議割り込みトーンが聞こえます。

タイプ	説明
リングバックトーン	次のシナリオでは、アラートトーンが聞こえます。 • IOS ゲートウェイ経由で PSTN を介してコールを転送する場合。 • H.323 クラスタ間トランクを介してコールを転送する場合。 • SCCP 電話機から SIP クライアントにコールを転送する場合。

自動音声応答の概要

自動音声応答（IVR）装置を使用すれば、Cisco Unified Communications Manager で、事前に録音した機能アナウンス（.wav ファイル）を Cisco Unified IP Phone やゲートウェイなどのデバイスに出力することができます。これらのアナウンスは、開催中の会議のように IVR アナウンスを必要とする機能を使用しているデバイスで再生されます。

ノードを追加すると、IVR 装置が自動的にそのノードに追加されます。IVR 装置は、そのノード上で Cisco IP Voice Media Streaming Application サービスがアクティブになるまで非アクティブのままです。

IVR は、デフォルトで、48 の同時発信者をサポートします。IVR 発信者の数は、Cisco IP Voice Media Streaming Application サービスパラメータを使用して変更できます。ただし、1 つのノードの IVR 発信者数を 48 より多くしないことをお勧めします。IVR 発信者数は、Conference Now に参加する場合に想定される IVR への同時コール数に基づいて設定できます。

注意 コール処理負荷の高い Cisco Unified Communications Manager ノードでは IVR デバイスを有効化しないでください。

デフォルトの IVR アナウンスとトーン

Cisco Unified Communications Manager は、Cisco IP Media Streaming Application サービスが有効化されたときに、一連の事前に録音された自動音声応答（IVR）アナウンスを自動的に提供します。デフォルトの録音済みの IVR アナウンスを置き換えることができます。アナウンスは、次の条件で再生されます。

表 *11* : 録音済みの *IVR* アナウンス

アナウンス	条件
ConferenceNowAccessCodeFailed アナウンス	出席者が誤ったアクセスコードを入力し最大試行回数を超えた場合に再生されます。
ConferenceNowAccessCodeInvalid アナウンス	出席者が誤ったアクセスコードを入力したときに再生されます。

アナウンス	条件
ConferenceNowCFBFailed アナウンス	会議の開始中に会議ブリッジのキャパシティ制限を超える場合に再生されます。
ConferenceNowEnterAccessCode アナウンス	出席者が会議に参加しホストが出席者のアクセスコードを設定するときに再生されます。
ConferenceNowEnterPIN アナウンス	主催者または出席者がミーティングに参加しようとするときに再生されます。
ConferenceNowFailedPIN アナウンス	ホストが、正しい PIN を入力するための最大試行回数を超えた後に再生されます。
ConferenceNowGreeting アナウンス	今すぐ会議用のグリーティングプロンプトを再生します。
ConferenceNowInvalidPIN アナウンス	ホストが間違った PIN を入力したときに再生されます。
ConferenceNowNumberFailed アナウンス	ホストまたは出席者が誤ったアクセスコードを入力し最大試行回数を超えた場合に再生されます。
ConferenceNowNumberInvalid アナウンス	ホストまたは出席者が間違ったミーティング番号を入力したときに再生されます。

自動音声応答制限

機能	制限事項
ロード バランシング	自動音声応答（IVR）は、共通のメディアデバイスドライバを介して Real-Time Protocol（RTP）ストリームを使用します。このデバイスドライバは、保留音（MOH）、ソフトウェア メディア ターミネーション ポイント（MTP）、ソフトウェア会議ブリッジ（CFB）、アナンシエータなど、Cisco IP Voice Media Streaming Application サービスによって提供される他のソフトウェア メディア デバイスによっても使用されます。 通話音量を大きくすると、システムのパフォーマンスに影響します。これは、同じサーバノード上で CallManager サービスがアクティブになっている場合のコール処理にも影響します。
DTMF ディジット	IVR は、帯域外 (OOB) の DTMF ディジットコレクション方式のみをサポートしています。通話デバイスと IVR の間に DTMF 機能の不一致がある場合、MTP が割り当てられます。

機能	制限事項
コーデック	IVR がサポートしているのは、G.711 (つまり、a-law と mu-law)、G.729、ワイド帯域 256 mb のみです。発信側デバイスと IVR の間でコーデックが一致していない場合、トランスコーダが割り当てられます。

アナウンスの概要

Cisco Unified Communications Manager Administration で、メニューパス **[メニューリソース]** > **[アナウンス（Announcements）]** を使用して、アナウンスを設定します。アナウンスには次の 2 つの分類があります。

- [システム アナウンス（System Announcements）]：通常のコール処理で使用されるか、機能アナウンスのサンプルとして提供される、事前定義されたアナウンス。
- [機能アナウンス（Feature Announcements）]：保留音（MOH）、コール キューイングまたは外部コール制御を伴うハントパイロットなどの特定の機能で使用されます。シスコが提供するオーディオ ファイルをアップロードするか、またはカスタムの `.wav` ファイルをアップロードすることで、機能アナウンスをカスタマイズできます。すべてのカスタム アナウンスの `.wav` ファイルを、クラスタ内のすべてのサーバにアップロードします。

（注） トランクまたはゲートウェイ経由で接続している場合は、警告やリオーダー音などのカスタム アナウンスが再生されることがあります。ただし、2 台の IP 電話間、または IP 電話と Jabber クライアントの間のコールでは、カスタム アナウンスは再生されません。

形式

アナウンスに推奨される形式には次の仕様が含まれます。

- 16 ビット PCM wav ファイル
- ステレオまたはモノラル
- 48 kHz、44.1 kHz、32 kHz、16 kHz、8 kHz のサンプル レート

デフォルトのアナウンス

カスタムアナウンス wav ファイルをアップロード、またはシステムアナウンス用にシスコが提供したファイルを変更することは可能です。ただし、アナウンス識別子を変更することはできません。たとえば、発信者が無効な番号をダイヤルすると、システム アナウンス（VCA_00121）が再生されます。これは一般に「空席コールのアナウンス」として知られています。

表 *12 : [*アナウンスの検索と一覧表示*(Find and List Announcements)]* ウィンドウのアナウンス

アナウンス ID	説明
Gone_00126	システム：現在使用されていない
MLPP-BNEA_00123	システム：MLPP ビジーが備わっていない
MLPP-BPA_00122	システム：MLPP 以上の優先レベル
MLPP-ICA_00120	システム：MLPP サービス障害
MLPP-PALA_00119	システム：MLPP 優先順位のアクセス制限
MLPP-UPA_00124	システム： MLPP で許可されていない優先レベル
Mobility_VMA	接続するには 1 を押してください
MonitoringWarning_00055	システム：モニタリングまたは録音中
RecordingWarning_00038	システム：録音中
TemporaryUnavailable_00125	システム：一時的に利用不可
VCA_00121	システム：欠番/無効な番号がダイヤルされた
Wait_In_Queue_Sample	ビルトイン：キューに入った発信者用の定期的なアナウ
Welcome_Greeting_Sample	ビルトイン：発信者へのグリーティング（サンプル）

メディアリソース構成タスクフロー

システムのメディアリソースを設定するには、この手順を実行します。

手順

	コマンドまたはアクション	目的
Step 1	ソフトウェアメディアリソースのアクティブ化 （157 ページ）	IPVMS サービスをオンにすると、サーバ上のソフトウェアメディアリソースがアクティブになります。
Step 2	メディア ターミネーション ポイントの設定 （158 ページ）	システムのメディア ターミネーション ポイント（MTP）を設定します。
Step 3	トランスコーダの設定 （158 ページ）	システムにトランスプログラマリソースを追加します。

	コマンドまたはアクション	目的
Step 4	自動音声応答（IVR）の設定 （159 ページ）	システム IVR のデフォルト設定を行います。
Step 5	アナンシエータの設定 （160 ページ）	アナンシエータのシステム設定を指定します。
Step 6	メディアリソースグループの設定 （160 ページ）	メディアリソースをメディアリソースグループに追加します。リソースのさまざまな組み合わせで複数のグループを設定します。
Step 7	メディア リソース グループ リストの設定 （161 ページ）	エンドポイントまたはエンドポイントのクラスに割り当てることができるメディアリソースグループのリストを作成します。
Step 8	デバイスまたはデバイスプールへのメディアリソースの割り当て （161 ページ）	デバイスまたはデバイスプールにメディアリソースを割り当てることによって、エンドポイントでメディアリソースを使用できるようにします。
Step 9	アナウンスの設定 （162 ページ）	（**オプション**）特定のアナウンスメントの設定を行います。アナウンスメントは、通常の処理、または保留音や IVR などの機能に使用されます。
Step 10	カスタマイズされたアナウンスのアップロード （163 ページ）	（**オプション**）事前に録音したアナウンスをアップロードします。新規または既存のアナウンスメントにファイルを割り当てます。

ソフトウェアメディアリソースのアクティブ化

次のソフトウェア メディア リソースを有効にするには、**Cisco IP Voice Media Streaming** サービスをアクティブ化します。

- アナンシエータ
- 音声自動応答（IVR）
- メディア ターミネーション ポイント（MTP）
- ソフトウェア会議ブリッジ
- 保留音

手順

Step 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスのアクティブ化（Service Activation）]** を選択します。

Step 2 [サーバ（Server）] から、Unified Communications Manager パブリッシャノードを選択します。

Step 3 [Cisco IP Voice Media Streaming Service] をオンにして [保存（Save）] をクリックします。

メディア ターミネーション ポイントの設定

ソフトウェアメディアポイント (MTP) を設定するには、次の手順を実行します。

始める前に

ソフトウェアのメディアターミネーションポイント (MTP) をアクティブ化するには、Cisco IP Voice Media サービスが実行されている必要があります。

必要な MTP リソース数と、これらのリソースの提供に必要な MTP デバイス数を決定します。

手順

Step 1 Cisco Unified CM Administration から、**[メディアリソース（Media Resources）] > [メディアターミネーションポイント（Media Termination Point）]** を選択します。

Step 2 次のいずれかを実行します。

- **[検索（Find）]** をクリックし、既存の MTP を選択します。
- **[新規追加（Add New）]** をクリックし、新規 MTP を作成します。

Step 3 **[メディア ターミネーション ポイント名（Media Termination Point Name）]**を割り当てます。

Step 4 **デバイスプール**を割り当てます。

Step 5 この MTP を**トラステッドリレーポイント (TRP)** として指定する場合は、[トラステッドリレーポイント] チェックボックスをオンにします。

Step 6 [保存（Save）] をクリックします。

トランスコーダの設定

トランスコーダは、あるコーデックからの入力ストリームを、別のコーデックを使用し出力ストリームに変換するデバイスです。

始める前に

IVR がアクティブになるためには、Cisco IP Voice Media Streaming サービスが実行されている必要があります。

必要なトランスコーダ リソースの数とリソースの提供に必要なトランスコーダデバイスの数を決定します。

手順

Step 1 Cisco Unified CM Administration にログインし、**[メディアリソース（Media Resources）] > [トランスコーダ（Transcoder）]**.を選択します。

Step 2 次のいずれかを実行します。

- 既存のトランスコーダを選択するには、[検索（Find）] をクリックします。
- [新規追加（Add New）] をクリックします。

Step 3 [トランスコーダタイプ（Transcoder Type）] を選択します。

Step 4 トランスコーダの [MACアドレス（MAC Address）] を入力します。

Step 5 ドロップダウン メニューから [デバイスプール（Device Pool）] を割り当てます。

Step 6 このトランスコーダをトラステッドリレーポイントとして使用する場合は、[トラステッドリレーポイント（Trusted Relay Point）] チェックボックスをオンにします。

Step 7 [保存（Save）] をクリックします。

自動音声応答（IVR）の設定

IVR の設定項目を指定するには、この手順を使用します。

始める前に

自動音声応答（IVR）がアクティブになるためには、Cisco IP Voice Media Streaming サービスが実行されている必要があります。

手順

Step 1 Cisco Unified CM Administration で、**[メディアリソース（Media Resources）] > [自動音声応答（Interactive Voice Response）]** を選択します。

Step 2 [検索（Find）] をクリックして、IVR を選択します。

Step 3 [名前（Name）] と [説明（Description）] を入力します。

Step 4 IVR コールが信頼できるリレーポイントを使用するようにするには、[**Use Trusted Relay point**] ドロップダウンを**[On]** に設定します。

Step 5 [自動音声応答の設定（Interactive Voice Response Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 6 [保存（Save）] をクリックします。

アナンシエータの設定

アナンシエータのシステム設定を指定します。

始める前に

アナンシエータがアクティブになるためには、Cisco IP Voice Media Streaming サービスが実行されている必要があります。

手順

Step 1 Cisco Unified CM Administration で、**[メディアリソース（Media Resources）] > [アナンシエータ（Annunciator）]** を選択します。

Step 2 [検索（Find）] をクリックして、アナンシエータを選択します。

Step 3 [名前（Name）] と [説明（Description）] を入力します。

Step 4 [デバイスプール（Device Pool）] を選択します。

Step 5 アナンシエータでトラステッド リレー ポイントを使用する場合は、[トラステッドリレーポイントを使用（Use Trusted Relay Point）] ドロップダウンを [オン（On）] に設定します。

Step 6 [保存（Save）] をクリックします。

メディアリソースグループの設定

メディアリソースグループには、エンドポイントまたはエンドポイントのグループに割り当てるメディアリソースの一覧が含まれています。

手順

Step 1 Cisco Unified CM Administration で、**[メディアリソース（Media Resources）] > [メディアリソースグループ（Media Resource Group）]** を選択します。

Step 2 次のいずれかを実行します。

- 既存のメディアリソースグループを選択するには、[検索（Find）] をクリックします。
- 新しいメディアリソースグループを作成するには、[新規追加（Add New）] をクリックします。

Step 3 [メディアリソースグループの設定（Media Resource Group Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 4 グループの [名前（Name）] と [説明（Description）] を入力します。

Step 5 [使用可能なメディアリソース（Available Media Resources）] から、このグループに追加するリソースを選択し、矢印を使用してリソースを [選択されたメディアリソース（Selected Media Resources）] に移動します。

Step 6 （オプション）保留音オーディオにマルチキャストを使用するには、[MOHオーディオにマルチキャストを使用（Use Multi-cast for MOH Audio）] チェックボックスをオンにします。

Step 7 [保存（Save）] をクリックします。

メディア リソース グループ リストの設定

メディアリソースグループの優先順位付けされたリストを作成します。このリストは、個々のデバイスまたはデバイスプールに割り当てることができます。

手順

Step 1 Cisco Unified CM Administration で **[メディアリソース（Media Resources）] > [メディアリソースのグループ リスト（Media Resource Group List）]** を選択します。

Step 2 次のいずれかを実行します。

- 既存のリストを選択するには、[検索（Find）] をクリックします。
- 新しいリストを作成するには、[新規追加（Add New）] をクリックします。

Step 3 メディア リソース グループ リストの [名前（Name）] を入力します。

Step 4 [使用可能なメディアリソースグループ（Available Media Resource Groups）] から、追加するグループを選択し、矢印を使用して [選択されたメディアリソースグループ（Selected Media Resource Groups）] に移動させます。

Step 5 [保存（Save）] をクリックします。

（注） エンドポイントでこれらのメディアリソースを使用するには、デバイスプール、ゲートウェイポート、またはデバイスにリストを割り当てる必要があります。

デバイスまたはデバイスプールへのメディアリソースの割り当て

優先順位付きのメディアリソース グループのリストをデバイスプールまたは個別のデバイスに関連付けることで、エンドポイントにメディアリソースを割り当てます。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。

- デバイスプールにメディアリソースを追加するには、**[システム（System）]** > **[デバイスプール（Device Pools）]** を選択します。
- エンドポイントにメディアリソースを直接追加するには、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

Step 2 [検索（Find）] をクリックして、これらのメディアリソースを割り当てるデバイスプールまたはデバイスを選択します。

Step 3 **[メディアリソースグループリスト（Media Resource Group List）]** ドロップダウンリストから、リストを選択します。

Step 4 [保存（Save）] をクリックします。

Step 5 [選択項目への設定の適用（Apply Config to Selected）] をクリックします。
デバイス名および適切な設定変更を示した [設定の適用（Apply Configuration）] ウィンドウが表示されます。

アナウンスの設定

システムアナウンスまたは機能アナウンスとして使用できるアナウンスを設定することができます。システムアナウンスは、コール処理またはサンプル機能アナウンスを使用するために使用されますが、機能アナウンスは、ハントパイロットのコールキューまたは外部コール制御と関連付けられた特定の機能 (MOH) などに使用されます。

既存のアナウンスを変更したり、Cisco Unified Communications Manager で新しいアナウンスを設定したりすることができます。

手順

Step 1 Cisco Unified CM Administration から、**[メディアリソース（Media Resources）]** > **[アナウンス（Announcement）]** を選択します。

Step 2 次のいずれかを実行します。

- [検索 (Find)] をクリックして、編集する既存のアナウンスを選択します。
- **[新規追加（Add New）]** をクリックして新しいアナウンスを追加します。

Step 3 **[アナウンスの設定]** ウィンドウのフィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 4 [保存（Save）] をクリックします。

カスタマイズされたアナウンスのアップロード

別のアナウンスを使用して、アップロードしたカスタム.wavファイルを伴うデフォルトのアナウンスを変更することができます。音声ソースファイルをインポートすると、Unified Communications Managerがファイルを処理し、保留音(MOH)サーバでの使用に適した形式にファイルを変換します。

（注） アナウンスはロケール（言語）で特定されます。インストールに複数の言語ロケールが使用されている場合、各カスタムアナウンスは各言語で別個の.wavファイルとして録音し、正しいロケール指定でアップロードする必要があります。また、米国英語以外の言語のカスタム アナウンス.wavファイルをアップロードする前に、正しいロケール パッケージを各サーバにインストールする必要もあります。

MoH オーディオ ソースなど、アナウンスに推奨される形式には次の仕様が含まれます。

- 16 ビット PCM .wav ファイル
- ステレオまたはモノラル
- 48 kHz、44.1 kHz、32 kHz、16 kHz、8 kHz のサンプル レート

Unified Communications Manager の [アナウンスの検索と一覧表示（Find and List Announcements）] ウィンドウで、ハイパーリンクが設定されていないアナウンスは更新できません。このウィンドウでハイパーリンクされた下線付きのシスコ提供のアナウンスの場合は、カスタマイズされたアナウンスを追加できます。たとえば、MLPP-ICA_00120 と MonitoringWarning_00055 があります。

手順

Step 1 Cisco Unified CM Administration から、**[メディアリソース（Media Resources）]** > **[アナウンス（Announcement）]** を選択します。

Step 2 [アナウンスの検索と一覧表示（Find and List Announcements）] ウィンドウで、検索条件を入力して、[検索（Find）] をクリックし、結果リストからアナウンスのハイパーリンクをクリックします。

Step 3 [アナウンスの設定（Announcement Configuration）] ウィンドウで、[ファイルのアップロード（Upload File）] をクリックします。

Step 4 [ファイルのアップロード（Upload Files）] ポップアップ ウィンドウから、ロケールを選択し、ファイル名を入力して参照し、.wavファイルを選択して、[ファイルのアップロード（Upload File）] をクリックします。

アップロードプロセスが始まり、処理が完了した後にステータスが更新されます。[閉じる（Close）] を選択して [ファイルのアップロード（Upload File）] ウィンドウを閉じます。

Step 5 （任意）Unified Communications Manager でシスコが提供するアナウンスを再生する代わりに、カスタマイズしたアナウンスを再生する場合は、[アナウンスの設定（Announcements Configuration）]

ウィンドウの [ロケール別のアナウンス（Announcement by Locale）] ペインで [有効（Enable）] チェックボックスをオンにします。

[有効（Enable）] チェックボックスがオフになっている場合、Unified Communications Manager は、シスコが提供するアナウンスを再生します。

Step 6 [保存（Save）] をクリックします。

次のタスク

クラスタ内のサーバ間ではアナウンス ファイルが伝搬されないため、クラスタ内の各ノードにアナウンスをアップロードします。クラスタ内の各サーバで Cisco Unified Communications Manager の管理を参照し、アップロード プロセスを繰り返します。

第 14 章

会議ブリッジの設定

会議ブリッジの概要

Cisco Unified Communications Manager の会議ブリッジは、ソフトウェアまたはハードウェアアプリケーションで、アドホックおよびミートミーの両方式の音声会議を可能にするように設計されています。追加の会議ブリッジ タイプは、ビデオ会議など、その他の会議タイプをサポートします。各会議ブリッジは、複数のマルチパーティ会議を同時にホストできます。ハードウェア会議とソフトウェア会議の両方の会議ブリッジを同時にアクティブにすることができます。ソフトウェアの会議デバイスとハードウェアの会議ブリッジでは、サポートするストリームの数とコーデックのタイプについて違いがあります。新しいサーバを追加すると、システムによってソフトウェア会議ブリッジが自動的に追加されます。

（注） Cisco Unified Communications Managerサーバが作成されると、ソフトウェア会議ブリッジも自動的に作成され、削除できません。Cisco Unified Communications Manager Administration に会議ブリッジソフトウェアを追加することはできません。

会議ブリッジ タイプ

Cisco Unified Communications Manager の管理ページには、次の会議ブリッジタイプが存在します。

表 *13*：会議ブリッジ タイプ

会議ブリッジ タイプ	説明
シスコ会議ブリッジ ハードウェア	このタイプは Cisco Catalyst 4000 および 6000 音声ゲートウェイ モジュールをサポートし、次の会議セッション数をサポートします。 **Cisco Catalyst 6000** • G.711 または G.729a 会議：1 ポート当たりの参加者数 32 人、1 会議当たりの最大参加者数 6 人、1 モジュール当たりの合計参加者数 256 人、参加者数 3 人でのブリッジの数は 10。 • GSM：1 ポート当たりの参加者数 24 人、1 会議当たりの最大参加者数 6 人、1 モジュール当たりの合計参加者数 192 人。 **Cisco Catalyst 4000** G.711 会議のみ：会議参加者数 24 人。各会議の参加者が 6 人の場合、会議の最大数は 4。
シスコ会議ブリッジソフトウェア	ソフトウェア会議デバイスは、デフォルトで G.711 コーデックをサポートします。 このタイプの発信者の最大数は 256 です。256 の設定では、ソフトウェア会議ブリッジがそれぞれ 4 当事者の 64 会議セッションをサポートできます。会議セッションの発信者の最大数は、[最大アドホック会議（Maximum Ad Hoc Conference）] および [最大ミートミー会議ユニキャスト（Maximum MeetMe Conference Unicast）] サービスパラメータによって指定します。 **注意** このタイプの会議ブリッジ（SW 会議ブリッジ）は、実装が簡単です。参加者の数が多い場合は、単純な合計アルゴリズムを使用している当事者を識別できないので、会議の音声品質が低下する可能性があります。
Cisco IOS 会議ブリッジ	• NM-HDV または NM-HDV-FARM ネットワーク モジュールを使用。 • G.711 a/mu-law、G.729、G.729a、G.729b、および G.729ab の参加者が 1 つの会議に参加可能です。 • 最大 6 人の参加者が 1 つの会議コールに参加可能です。 Cisco Unified Communications Manager は、会議リソースをコールに動的に割り当てます。 Cisco IOS Conferencing and Transcoding for Voice Gateway Router の詳細については、この製品に付属の Cisco IOS のドキュメントを参照してください。

会議ブリッジ タイプ	説明
Cisco IOS 拡張ブリッジ	• Cisco 2800 シリーズおよび 3800 シリーズの音声ゲートウェイ ルータ上でオンボードの Cisco Packet Voice/Fax Digital Signal Processor Modules（PVDM2）を使用、あるいはNM-HD ネットワーク モジュールまたは NM-HDV2 ネットワーク モジュールを使用。 • G.711 a-law/mu-law、G.729、G.729a、G.729b、G.729ab、GSM FR、および GSM EFR の参加者が 1 つの会議に参加可能です。 • 最大 8 人の参加者が 1 つのコールに参加可能です。 （注） ISR4000 ルータおよび SM-X-PVDM-3000/ SM-X-PVDM-2000/ SM-X-PVDM-1000/ SM-X-PVDM-500 では、Unified Communications Manager の最大ストリームは 4096 に制限されているため、各会議ブリッジ プロファイルで最大 512 のセッションを登録できます。 Cisco Unified Communications Manager は、会議リソースをコールに動的に割り当てます。 Cisco IOS Enhanced Conferencing and Transcoding for Voice Gateway Router の詳細については、この製品に付属の Cisco IOS のドキュメントを参照してください。 この会議ブリッジタイプでは、ISR 4000 シリーズゲートウェイが展開されている場合に、サポートされている SIP 電話の AES_CM_128_HMAC_SHA1_80 での SRTP メディア暗号化をサポートしています。SCCP 電話とサポートされていない SIP 電話は、AES_CM_128_HMAC_SHA1_32 暗号化にフォールバックします。 （注） ゲートウェイのロードが暗号化をサポートしていることを確認してください。サポートの詳細については、ゲートウェイのドキュメントを参照してください。
シスコ会議ブリッジ（WS-SVC-CMM）	この会議ブリッジ タイプは、Cisco Catalyst 6500 シリーズおよび Cisco 7600 シリーズの Communication Media Module（CMM）をサポートします。 これは、会議ごとに最大 8 人の参加者、ポート アダプタごとに最大 64 の会議をサポートします。この会議ブリッジタイプでは、次のコーデックをサポートしています。この会議ブリッジタイプでは、アドホック会議をサポートしています。 • G.711 a-law/mu-law • G.729 annex A および annex B • G.723.1

会議ブリッジ タイプ	説明
シスコ ビデオ会議ブリッジ（IPVC-35xx）	Cisco Video Conference Bridge は、Cisco IP Video Phone、H.323 エンドポイント、および音声専用の Cisco Unified IP Phone にオーディオおよびビデオによる会議機能を提供します。Cisco Video Conference Bridge はビデオの H.261、H.263、および H.264 コーデックに対応しています。
Cisco IOS Heterogeneous Video Conference Bridge	第 2 世代シスコ サービス統合型ルータ（ISR G2）は、アドホックおよびミートミー ビデオ会議をサポートする IOS ベースの会議ブリッジとして動作できます。ルータを会議ブリッジとして機能させるには、DSP モジュールをルータに取り付ける必要があります。 異種間ビデオ会議では、すべての会議参加者が、使用するビデオ形式属性が異なる電話機を使用して会議ブリッジに接続します。異種間会議では、様々なフォーマットの信号を変換する必要があるため、トランスコーディング機能とトランスサイジング機能が DSP に求められます。 異種間ビデオ会議では、次のどちらかの条件に該当する場合、発信者はオーディオ参加者として会議に接続します。 • DSP リソースが不足している場合。 • ビデオ電話機の機能をサポートするように会議ブリッジが設定されていない。 ISR G2 ルータでのビデオ会議の詳細については、ドキュメント『*Configuring Video Conferences and Video Transcoding*（ビデオ会議とビデオ トランスコーディングの設定）』を参照してください。
Cisco Guaranteed Audio Video Conference Bridge	第 2 世代シスコ サービス統合型ルータ（ISR G2）は、アドホックとミートミーの音声およびビデオ会議をサポートする IOS ベースの会議ブリッジとして動作できます。ルータを会議ブリッジとして機能させるには、DSP モジュールをルータに取り付ける必要があります。 会議のオーディオ部分向けに DSP リソースが留保されますが、ビデオ サービスは保証されません。ビデオ電話の発信者は、会議の開始時に DSP リソースを利用できる場合は、ビデオ サービスを利用できる場合があります。使用可能でない場合、発信側はオーディオ参加者として会議に接続します。 ISR G2 ルータでのビデオ会議の詳細については、ドキュメント『*Configuring Video Conferences and Video Transcoding*（ビデオ会議とビデオ トランスコーディングの設定）』を参照してください。

会議ブリッジ タイプ	説明
Cisco IOS 同種間ビデオ会議ブリッジ（Cisco IOS Homogeneous Video Conference Bridge）	第 2 世代シスコ サービス統合型ルータ（ISR G2）は、アドホックおよびミートミー ビデオ会議をサポートする IOS ベースの会議ブリッジとして動作できます。ルータを会議ブリッジとして機能させるには、DSP モジュールをルータに取り付ける必要があります。 Cisco IOS Homogeneous Video Conference Bridge は、同種間ビデオ会議をサポートする IOS ベースの会議ブリッジ タイプを指定します。同種間ビデオ会議は、すべての参加者が同じビデオ フォーマット属性を使用して接続するビデオ会議です。すべてのビデオ電話機が同一のビデオ形式をサポートし、会議ブリッジは同じデータ ストリーム形式をすべてのビデオ参加者に送信します。 会議ブリッジが電話機のビデオ フォーマットをサポートするように設定されていない場合、その電話機の発信側は、オーディオのみの参加者として会議に接続します。 ISR G2 ルータでのビデオ会議の詳細については、ドキュメント『*Configuring Video Conferences and Video Transcoding*（ビデオ会議とビデオ トランスコーディングの設定）』を参照してください。

会議ブリッジ タイプ	説明
Cisco TelePresence MCU	Cisco TelePresence MCU は、Cisco Unified Communications Manager 用のハードウェア会議ブリッジのセットです。 Cisco TelePresence MCU は、高解像度（HD）のマルチポイント ビデオ会議ブリッジです。毎秒 30 フレームで最大 1080p の性能を持ち、あらゆる会議で十分な連続表示を実現し、フルトランスコーディング機能を備えているため、マルチベンダーの HD エンドポイント環境に最適です。 Cisco TelePresence MCU では、シグナリング コール制御プロトコルとして SIP をサポートしています。詳細に設定でき、システムおよび会議を制御およびモニタする、ビルトイン Web サーバを装備しています。Cisco TelePresence MCU には、HTTP 通信による XML 管理 API が用意されています。 Cisco TelePresence MCU は、アドホックおよびミートミー音声会議とビデオ会議の両方ができます。各会議ブリッジは、複数のマルチパーティ会議を同時にホストできます。 Cisco Unified Communications Manager は、Unified Communications Manager と Cisco TelePresence MCU の間で Binary Floor Control Protocol によるプレゼンテーション共有をサポートします。 Cisco TelePresence MCU は、ポート予約モードで設定する必要があります。詳細については、『*Cisco TelePresence MCU* コンフィギュレーション ガイド』を参照してください。 （注） Cisco TelePresence MCU は、一般的なアウトオブバンド DTMF 方式をサポートしていません。デフォルト設定では、Cisco Unified Communications Manager はメディア ターミネーション ポイント（MTP）を必要としません。ただし、[メディア ターミネーション ポイントが必須(Media Termination Point Required)] チェックボックスがオンになっている場合は、Cisco Unified Communications Manager によって MTP が割り当てられ、SIP トランクは RFC 2833 に従って DTMF をネゴシエートします。

会議ブリッジ タイプ	説明
Cisco TelePresence Conductor	Cisco TelePresence Conductor はインテリジェントな電話会議管理制御を提供します。複数の MCU 間にわたるロードバランシングと複数デバイスの可用性を高めるためのクラスタ化を実現する、スケーラブルなサポート デバイスです。管理者は Cisco TelePresence Conductor を、Cisco Unified Computing System（Cisco UCS）プラットフォームまたはサードパーティ ベースのプラットフォームをサポートするアプライアンス、または、VMware 上の仮想アプライアンスとして実装できます。 Cisco TelePresence Conductor は、新しい会議ごとに最適な Cisco TelePresence リソースを動的に選択します。アドホック、「ミートミー」、およびスケジュールされた音声およびビデオ会議は動的に拡大し、個々の MCU のキャパシティを超えることがあります。最大 3 つの Cisco TelePresence Conductor アプライアンスまたは仮想アプリケーションをクラスタ化して、復元力をさらに高めることができます。1 つの Cisco TelePresence Conductor アプライアンスまたは Cisco TelePresence Conductor クラスタには 30 の MCU または 2400 の MCU ポートがあります。
Cisco Meeting Server	Cisco Meeting Server 会議ブリッジ ソリューションにより、アドホック会議、ミートミー会議、開催中の会議、ランデブー会議が可能になります。会議ブリッジは、施設内での音声、ビデオ、ウェブ会議を実現し、サードパーティのオンプレミスインフラストラクチャと連携します。あらゆる規模の導入に拡張できるほか、必要に応じて徐々に容量を増やすこともでき、組織の現在および将来のニーズに確実に対応することができます。この会議ブリッジは高度な相互運用性を提供します。任意の数の参加者が会議を作成し、参加することができます。 • シスコまたはサードパーティの会議室システムまたはデスクトップ ビデオ システム • Cisco Jabber クライアント • Cisco ミーティング アプリケーション（ネイティブ、または WebRTC 互換ブラウザを使用可能） • Skype for Business Cisco Meeting Server 会議ブリッジを使用するには、Cisco Meeting Server 2.0 以上のリリースが必要です。 Cisco Meeting Server は、シグナリング コール制御プロトコルとして SIP をサポートしています。詳細に設定でき、システムおよび会議を制御およびモニタする、ビルトイン Web サーバを装備しています。Cisco Meeting Server は、HTTP に対する XML 管理 API を提供します。 （注） Cisco Meeting Server は、H.265 ビデオ コーデックと遠端カメラ制御をサポートしていません。

会議ブリッジの設定タスクフロー

手順

	コマンドまたはアクション	目的
Step 1	会議ブリッジの設定 （172 ページ）	アドホック音声会議とミートミー音声会議を可能にするためにハードウェアまたはソフトウェア会議ブリッジを設定します。
Step 2	会議ブリッジのサービスパラメータの設定（172 ページ）	ネットワークに Cisco IOS コンファレンスブリッジと Cisco IOS 拡張会議ブリッジの両方が含まれている場合は、次の手順を実行します。
Step 3	会議ブリッジへの SIP トランク接続の設定（173 ページ）	この手順を実行して、会議ブリッジへの SIP トランク接続を設定する

会議ブリッジの設定

アドホック音声会議とミートミー音声会議を可能にするためにハードウェアまたはソフトウェア会議ブリッジを設定する必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[メディアリソース（Media Resources）] > [会議ブリッジ（Conference Bridge）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [会議ブリッジの設定（Conference Bridge Configuration）] ウィンドウで各フィールドを設定します。フィールドの説明の詳細については、オンライン ヘルプを参照してください。

Step 4 [保存（Save）] をクリックします。

次のタスク

ネットワークに Cisco IOS 会議ブリッジおよび Cisco IOS の拡張会議ブリッジが含まれる場合、「会議ブリッジのサービスパラメータの設定 （172 ページ）」を実行します。

会議ブリッジのサービスパラメータの設定

ネットワークに Cisco IOS コンファレンスブリッジと Cisco IOS 拡張会議ブリッジの両方が含まれている場合は、次の手順を実行します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

Step 3 [クラスタ全体のパラメータ（機能 - 会議）（Clusterwide Parameters (Features - Conference)）] セクションで、次のパラメータを 6 に設定します。

- [アドホック会議の最大参加者数（Maximum Ad Hoc Conference）]
- [ミートミー会議の最大ユニキャスト数（Maximum MeetMe Conference Unicast）]

Step 4 [保存（Save）] をクリックします。

会議ブリッジへの SIP トランク接続の設定

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [トランク（Trunk）]** を選択します。

Step 2 次のいずれかの手順を実行します。

- 新しい SIP トランクを作成するには、[新規追加（Add New）] をクリックします。
- その接続を既存のトランクに追加するには、[検索（Find）] をクリックし、適切なトランクを選択します。

Step 3 [デバイスプロトコル（Device Protocol）] で、[SIP] を選択します。

Step 4 [トランクサービスの種類（Trunk Service Type）] で、[なし（None）] を選択します。

Step 5 [接続先（Destination）] 領域で、会議ブリッジの IP アドレスまたはホスト名を追加して、会議ブリッジのエントリを作成します。新しい回線が必要な場合は、**(+)** をクリックして追加することができます。

Step 6 [正規化スクリプト（Normalization Script）] ドロップダウンリストボックスから、正規化スクリプトを選択します。たとえば、次のスクリプトは必須です。

- **cisco-telepresence-conductor-interop**：このトランクを Cisco TelePresence Conductor に接続している場合は、このスクリプトを選択します。
- **cisco-telepresence-mcu-ts-direct-interop**：このトランクを Cisco TelePresence Conductor MCU に接続している場合は、このスクリプトを選択します。
- **cisco-meeting-server-interop**：このトランクを Cisco Meeting Server に接続している場合は、このスクリプトを選択します。

Step 7 [トランクの設定（Trunk Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

第 15 章

拡張ロケーション コールアドミッション制御の設定

拡張ロケーション コールアドミッション制御の概要

拡張ロケーション コール アドミッション制御（CAC）を使用すると、複雑な WAN トポロジおよびクラスタ間ネットワークで、オーディオ品質とビデオの可用性を調整できます。これには、多層ネットワークとマルチホップ ネットワークが含まれます。

ネットワークトポロジ全体のモデルを作成して、さまざまなロケーション（LAN）と、それらのロケーションを接続する WAN リンクを示すことができます。個々のロケーションと WAN リンクについて、そのリンク経由のすべてのコールで一度に使用可能な合計帯域幅を表す、帯域幅の制限を割り当てます。特定のコールで帯域幅を使用できない場合、コールはビジー信号で拒否されます。これにより、WAN リンクがオーバーサブスクライブ状態になった結果として、音声およびビデオの品質が低下するのを防ぎます。

ロケーション帯域幅マネージャ (LBM) レプリケーショングループのクラスタ間レプリケーション機能を使用すると、クラスタ間ネットワーク全体でロケーション設定を複製できるため、大規模なクラスタ間ネットワークでの管理が容易になります。

拡張ロケーション CAC のコンポーネント

この機能では、次のコンポーネントを使用します。

- ロケーション：ロケーションはLANを表します。これは、エンドポイントを含み、または単にWANネットワークのモデル化に対してリンク間の中継場所として機能します。Cisco Unified Communications Manager では、最大 2,000 のロケーションがサポートされます。
- リンク：2 つのロケーション間の接続です。この機能を設定する場合は、各リンクに帯域幅の割り当てと重みを割り当てます。

- 重み付け：ロケーションの任意のペアの間で有効なパスを形成する、リンクの相対的な優先順位。重みは、2つのロケーション間に複数のパスが存在する場合にのみ使用されます。重みは、有効なパス (最小の重み値を持つパス) を計算するために使用されます。
- 帯域幅割り当て：特定のタイプのトラフィック（オーディオ、デスクトップ ビデオ、イマーシブ ビデオ）に割り当てられた合計帯域幅。帯域幅は、ロケーション内のコールにも割り当てることができます（デフォルト設定は [無制限（Unlimited）]）。
- ロケーション帯域幅マネージャ（LBM）：拡張ロケーションCACを機能させるために、Cisco Unified Serviceability でアクティブ化する必要のある機能サービス。このサービスは、ネットワークモデルを組み立て、送信元と宛先の間のすべてのリンクとロケーションの重みを追加し、最小の累積重みを持つパスを選択することによって、ロケーション間の効果的なパスを計算します。

ロケーションとリージョンの関係

拡張ロケーション コールアドミッション制御のロケーション設定は、リージョンと連動してコールの帯域幅を管理します。

- リージョン設定内の帯域幅割り当てでは、2つの地域間のコールのエンドポイントが使用できる帯域幅の合計量が割り当てられます。
- ロケーション内の帯域幅割り当ては、それらのロケーション間のすべてのコールが使用できる帯域幅の総量を割り当てます。個々のコールの場合、リージョン設定内の帯域幅は、ロケーション設定で使用可能な帯域幅の量から差し引かれます。たとえば、ロケーション設定で、特定のリンク上で 160 kb/s の帯域幅が使用可能であることが指定されている場合、そのリンクは2つの G を同時に 80 kb/s でサポートできます。

（注） 実稼働時間中に Location Bandwidth Manager の帯域幅やリンク構成を変更しないでください。変更すると、サーバの CPU 使用率が不必要に急増する可能性があります。

Cisco Unified Communications Manager は、クラスタごとに最大 2,000 のロケーションと 2,000 のリージョンをサポートします。

クラスタ間 LBM のレプリケーション

ロケーション帯域幅マネージャハブグループのクラスタ間レプリケーション機能を使用すると、より大規模なクラスタ間ネットワーク全体でロケーションとリンクの割り当てを複製できます。LBMをLBMハブのロールに割り当てることで、メッシュされたクラスタ間ネットワーク全体で、ロケーションおよびリンク情報をアクティブに複製できます。LBMハブは、共通の接続を介して互いに探索し、フル メッシュ構造のレプリケーション ネットワークを形成します。スポークのロールが割り当てられた LBM は、そのクラスタの LBM ハブを介してクラスタ間レプリケーションに間接的に参加できます。

クラスタ間トポロジの管理

クラスタ間ネットワークを設定および管理するには、複数の方法があります。次の表に、クラスタ間トポロジを設定および管理するための2つのアプローチを要約します。

設計へのアプローチ	説明
ロケーションおよびリンク管理	クラスタ間ネットワーク全体のすべてのリンクの帯域幅割り当てを設定および管理するには、単一のクラスタを使用します。このアプローチにより、特に多くの共通ロケーションを持つ導入での設定のオーバーヘッドが簡素化されます。クラスタ間の設定方法は次のとおりです。 管理クラスタで、トポロジ全体のすべてのロケーションとリンク (帯域幅の割り当てと重みを含む) を設定します。この情報はクラスタ間ネットワークに複製されます。 トポロジ内の他のクラスタの場合は、次のようになります。 • ローカルクラスタのロケーションのみを設定します。これは、デバイスをロケーションに関連付けるためだけです。 • リンク情報は設定しないでください。 • ローカルクラスタ内のすべての帯域幅割り当てを**無制限**のままにします。管理クラスタがローカルクラスタよりも少ない帯域幅割り当てを複製すると、より制限の厳しい設定が適用されます。
クラスタ間拡張ロケーション CAC	このアプローチでは、次のように設定します。 • 各クラスタ内で、ローカルロケーションとリンク情報を隣接クラスタにのみ設定します。 • Weighth と帯域幅の割り当てを含むリンク情報を隣接クラスタにのみ割り当てます。トポロジの残りの部分は、 • Hub_None の場所は、クラスタごとに名前を変更する必要があります。そうしないと、クラスタ間で共通の場所になります。 • 各クラスタには一意のクラスタ ID が必要です。 （注） これは、すべてのクラスタに consistenly 名前クラスタのレプリケーションにとって重要です。

拡張ロケーション CAC の前提条件

この機能を設定する前に、LAN および WAN ネットワークトポロジを理解していることを確認してください。これは、ロケーションとリンクの帯域幅を割り当てるために必要です。

拡張ロケーション CAC のタスクフロー

ご使用のシステムで拡張ロケーション コールアドミッション制御を設定するには、この手順を実行します。

手順

	コマンドまたはアクション	目的
Step 1	ロケーション帯域幅マネージャのアクティブ化 （178 ページ）	少なくとも 1 つのクラスタ ノードで、シスコロケーション帯域幅マネージャ機能サービスが実行されている必要があります。
Step 2	LBM グループの設定 （179 ページ）	デフォルトでは、Cisco CallManager サービスはローカル LBM サービスと通信します。ただし、LBM グループを使用してこの通信を管理し、冗長性を確保するためにアクティブおよびスタンバイの LBM を提供できます。
Step 3	ロケーションとリンクの設定 （180 ページ）	ネットワークのロケーション（LAN）を作成し、それらのロケーションを接続する WAN リンクに帯域幅を割り当てます。
Step 4	LBM クラスタ間レプリケーション グループの設定 （181 ページ）	設定された CAC 情報を他のクラスタに複製するクラスタ間レプリケーショングループを作成します。
Step 5	SIP クラスタ間トランクの設定 （181 ページ）	ネットワーク内の SIP クラスタ間トランクに**シャドウ**ロケーションを割り当てます。
Step 6	コールアドミッション制御のサービスパラメータの設定 （182 ページ）	（オプション）コールアドミッション制御のサービスパラメータの設定を指定します。ほとんどの展開では、デフォルト設定で十分です。

ロケーション帯域幅マネージャのアクティブ化

拡張ロケーションコールの制御については、クラスタ内の少なくとも1つのノードでCisco Location帯域幅マネージャ機能サービスをアクティブにする必要があります。このサービスはデフォルトでオフになっています。

手順

Step 1 Cisco Unified Serviceability から、**[ツール（Tools）]** > **[サービスのアクティブ化（Service Activation）]** を選択します。

Step 2 [サーバ（Server）] ドロップダウンリストから、サービスを実行するクラスタ ノードを選択して [移動（Go）] をクリックします。

Step 3 [CMサービス（CM Services）] で、[シスコロケーション帯域幅マネージャ（Cisco Location Bandwidth Manager）] サービスをオンにします。

Step 4 [保存（Save）] をクリックします。

Step 5 さらに他のノードでサービスを開始する場合は、このタスクを繰り返します。

（注） シスコでは、Cisco CallManager サービスも実行しているクラスタ内の各サブスクライバノードで、シスコロケーション帯域幅マネージャサービスを実行することを推奨しています。

LBM グループの設定

LBM グループを設定するには、次の手順を使用します。デフォルトでは、Cisco CallManager サービスはローカル LBM サービスと通信します。ただし、LBM グループを使用してこの通信を管理し、冗長性を確保するためにアクティブおよびスタンバイの LBM を提供できます。

（注） Cisco CallManager サービスが LBM を使用する順序は次のとおりです。

- LBM グループの指定
- ローカル LBM (共存)

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]** > **[ロケーション（Locations）]** > **[ロケーション帯域幅マネージャ グループ（Location Bandwidth Manager Group）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 グループに [名前（Name）] を割り当てます。

Step 4 [アクティブメンバー（Active Member）] ドロップダウンから、このグループのアクティブなメンバーを選択します。

Step 5 [**スタンバイメンバー (Standby member)**] ドロップダウンから、アクティブなメンバーが使用できない場合に使用する必要があるスタンバイを選択します。

Step 6 [保存（Save）] をクリックします。

ロケーションとリンクの設定

ネットワーク内にロケーション（LAN）を作成するには、この手順を使用します。これらのロケーション間で WAN リンクを使用するコールに、合計帯域幅と重み付けを割り当てます。フィールドおよびその設定についてのヘルプは、オンライン ヘルプを参照してください。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]** > **[ロケーション情報（Location Info）]** > **[ロケーション（Location）]** を選択します。

Step 2 [新規追加（Add New）] をクリックし、新しいロケーションを作成します。

Step 3 ロケーションに [名前（Name）] を割り当てます。

Step 4 [リンク-このロケーションと隣接ロケーション間の帯域幅（Links - Bandwidth Between This Location and Adjacent Locations）] 領域で、別のロケーションに対する WAN リンクの設定を指定します。

a) [ロケーション（Location）] リスト ボックスから、2 つ目のロケーションを選択します。
b) 有効なパスの形成する際のこのリンクの相対的な優先順位を反映した [重み付け（Weight）] を設定します。
c) オーディオ、ビデオ、イマーシブ ビデオ（TelePresence）の各コールの合計帯域幅を設定します。
d) さらに別のロケーションに対するリンクを設定するには、この手順を繰り返します。

Step 5 （オプション）[ロケーション内-このロケーション内のデバイスの帯域幅（Intra-location - Bandwidth for Devices Within This Location）] 領域を展開し、新しく作成したロケーションのロケーション内コールに対する帯域幅の割り当てを設定します。これらのコールについては、すべてのメディアタイプでデフォルト設定が [無制限（Unlimited）] になっています。

Step 6 [他のロケーションの設定を変更（Modify Settings to Other Locations）] 領域で、他のロケーションに対する RSVP 設定を指定します。

a) [ロケーション（Location）] 列で、他のロケーションを選択します。
b) これらのロケーション間でのコールに関する [RSVP設定（RSVP Setting）] を選択します。
c) さらに他のロケーションとのコールについてRSVP設定を追加するには、これらのサブステップを繰り返します。

Step 7 [保存（Save）] をクリックします。

Step 8 追加のロケーションを作成し、それらの新しいロケーションとの間のリンクを設定するには、この手順を繰り返します。

LBM クラスタ間レプリケーション グループの設定

LBM クラスタ間レプリケーショングループを設定するには、次の手順を使用します。これは、クラスタ間ネットワーク全体に拡張ロケーションアドミッション制御の帯域幅情報を複製するために必要です。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]**>**[ロケーション情報（Location Info）]**>**[ロケーション帯域幅マネージャ（LBM）のクラスタ間レプリケーショングループ（Location Bandwidth Manager (LBM) Intercluster Replication Group）]**を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [名前（Name）] にグループの名前を入力します。

Step 4 [ブートストラップサーバ（Bootstrap Servers）] 領域で、他のハブに接続情報を複製する責任を負う LBM サーバを 1 台以上割り当てます。

Step 5 [ロールの割り当て（Role Assignments）] 領域で、上向き矢印と下向き矢印を使用して、ハブとして機能するローカル LBM サーバと、スポークのままにする LBM サーバを選択します。

Step 6 [保存（Save）] をクリックします。

SIP クラスタ間トランクの設定

拡張位置のコールの呼制御を使用する場合は、クラスタ間ネットワーク内の SIP クラスタ間トランクにシャドウロケーションを割り当てる必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[トランク（Trunks）]** を選択します。

Step 2 [検索（Find）] をクリックして、適切なクラスタ間トランクを選択します。

Step 3 [ロケーション（Location）] ドロップダウンリストから [シャドウ（Shadow）] を選択します。

Step 4 [トランクの設定（Trunk Confiiguration）] ウィンドウで、その他の必要なフィールドを入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 5 [保存（Save）] をクリックします。

Step 6 拡張ロケーション コールアドミッション制御の情報を複製するクラスタ間トランクが他にもあれば、この手順を繰り返します。

コールアドミッション制御のサービスパラメータの設定

拡張ロケーション コールアドミッション制御に関するオプションのサービスパラメータを設定するには、この手順を使用します。

手順

Step 1 Cisco Unified CM Administration から、**[システム(System)]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 [サーバ（Server）] ドロップダウンリストから、クラスタ ノードを選択します。

Step 3 **Cisco CallManager** サービスのサービスパラメータを設定します。

a) **[サービス]** ドロップダウンリストから、**[Cisco CallManager]** を選択します。

b) [クラスタ全体のパラメータ（コールアドミッション制御）（Clusterwide Parameters (Call Admission Control)）] 領域で、任意のサービスパラメータを設定します。パラメータに関するヘルプの説明を参照するには、GUI でパラメータの名前をクリックします。

c) [保存（Save）] をクリックします。

Step 4 **シスコロケーション帯域幅マネージャ**サービスの設定を指定します。

a) [サービス（Service）] ドロップダウンリストから、[シスコロケーション帯域幅マネージャ（Cisco Location Bandwidth Manager）] を選択します。

b) 目的のサービスパラメータを設定します。パラメータに関するヘルプの説明を参照するには、GUI でパラメータの名前をクリックします。

c) [保存（Save）] をクリックします。

拡張ロケーション CAC の連携動作の制限

次の表に、拡張ロケーション コールアドミッション制御の機能の連携動作と制限を示します。

機能	連携動作と制限事項
LBMセキュリティモード	デフォルトでは、LBMセキュリティモードはセキュアではありません。この設定は、[LBMセキュリティモード（LBM Security Mode）] エンタープライズパラメータを使用して再設定できます。このパラメータは、[セキュア（Secure）]、[非セキュア（Insecure）]、または [混合（Mixed）] に設定できます。 [混合（Mixed）] 設定は、すべてのクラスタをセキュアにする間も通信を維持するために一時的に使用し、後で [セキュア（Secure）] に変更することができます。 このパラメータを変更した後は、設定を反映させるために、クラスタ内のすべての Cisco LBM サービス ハブをリセットする必要があります。

機能	連携動作と制限事項
ビデオコールでのオーディオ帯域幅の差し引き	デフォルトでは、ビデオコールのオーディオ部分の帯域幅はビデオプールから差し引かれます。[ビデオコールのオーディオ部分をオーディオプールから差し引く（Deduct Audio Portion from Audio Pool for Video Calls）]サービスパラメータを**True**に設定することで（デフォルト設定は**False**）、ビデオ コールのオーディオ部分をオーディオ プールから差し引くようにシステムを再設定できます。
ビデオ コールの分類	Cisco TelePresence エンドポイントには、設定を変更できないビデオコール分類である**イマーシブ**が用意されています。 その他のエンドポイントには、設定を変更できないビデオコール分類である**デスクトップ**が用意されています。 SIP トランクについては、関連付けられた SIP プロファイルで [ビデオコールのトラフィッククラス（Video Call Traffic Class）] を設定することで、ビデオ分類（デスクトップ、イマーシブ、または混合）を設定できます。
メディアリソース	メディアリソースの帯域幅は、コールの入園制御によって割り当てられません。
ロケーションの有用性	シスコユニファイドサービスインターフェイスには、ロケーショントポロジを管理およびモニタリングするための追加のツールが含まれています。詳細については、『*Cisco Unified Serviceability* アドミニストレーション ガイド』の「ロケーション」のトピックを参照してください。
セッション帯域幅修飾子	[SIP プロファイルの設定 (SIP Profile Configuration)] ウィンドウで、SIP エンドポイントで使用されるセッション帯域幅修飾子を割り当てることができます。
帯域幅の割り当ての競合	共通のリンクまたはロケーションで帯域幅容量または重み付け割り当ての競合が発生した場合は、ローカルクラスタが割り当てられた最小値を使用します。
デバイス サポート	Unified CM と LBM は、IP 電話、ゲートウェイ、H.323 トランク接続先、および SIP トランク接続先を含む、あらゆるタイプのエンドデバイスの帯域幅を管理します。ただし、クラスタ間拡張ロケーション CAC には、システム ロケーションのシャドウに割り当てられた SIP ICT が必要です。他のタイプのデバイスは、一般（固定）ロケーションに割り当てられている場合にのみサポートされます。
ネットワーク障害	ネットワーク障害が発生した場合は、Unified CM が計算した帯域幅予約経路にネットワーク状態が正確に反映されない可能性があります。このシナリオを許可する申し分のない方法はモデル内に存在しません。

機能	連携動作と制限事項
同期に関する問題	システムによって作成されたモデルは常に完全に同期されるわけではありません。保守的な帯域幅割り当てを使用して、この制約に適応できます。
WANを介したクラスタリング	WAN およびローカルフェールオーバーを介したクラスタリングを使用した展開では、クラスタ内 LBM トラフィックはすでに WAN 帯域幅の計算によって計算されています。
フレキシブル DSCP マーキング	追加の QoS の場合、DSCP マーキングを使用して、特定のタイプのコールフローに優先順位付けされたマーキングを他のユーザに割り当てることができます。たとえば、ネットワークが輻輳している場合でも、ビデオメディアがブロックされている場合でも、基本的な通信は音声を介して継続できるように、音声に優先順位を付けることができます。 DSCP マーキングは、次の2つの方法で設定できます。 • サービスパラメータ：[サービスパラメータの設定（Service Parameter Configuration）] ウィンドウの [クラスタ全体のパラメータ（システム-QoS）（Clusterwide Parameters (System - QoS)）] セクションで、クラスタ全体の DSCPのデフォルト値を設定します。 • SIP プロファイル：SIP プロファイルでカスタマイズされた DSCP 設定項目を設定し、それを特定の SIP デバイスのグループに割り当てます。この設定は、クラスタ全体のデフォルトを上書きします。
APIC-EM コントローラ	APIC_EM コントローラを使用して、外部 QoS 管理用の SIP メディアフローを管理できます。詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。

第 16 章

Resource Reservation Protocol（RSVP）の設定

RSVP コールアドミッション制御の概要

Resource Reservation Protocol（RSVP）は、IP ネットワーク内のリソースを予約するための、トランスポート レベルのリソース予約プロトコルです。拡張ロケーション コール アドミッション制御（CAC）の代わりに RSVP を使用できます。RSVP は、特定のセッションにリソースを予約します。セッションとは、特定の宛先アドレス、宛先ポート、およびプロトコル識別子（TCP または UDP）を持つフローです。

RSVP コールアドミッション制御の前提条件

IPv4 アドレッシングを使用する必要があります。RSVP は IPv6 をサポートしていません。

RSVP の設定タスクフロー

手順

	コマンドまたはアクション	目的
Step 1	クラスタ全体のデフォルト RSVP ポリシーの設定 （186 ページ）	クラスタ内の全ノードについて RSVP ポリシーを設定します。
Step 2	ロケーション ペア RSVP ポリシーの設定 （187 ページ）	（オプション）ロケーション ペアにクラスタの他とは別のポリシーを使用する場

	コマンドまたはアクション	目的
		合、特定のロケーション ペアの RSVP ポリシーを設定できます。
Step 3	RSVP の再試行の設定 （188 ページ）	RSVP の再試行の頻度と番号を設定します。
Step 4	コール中の RSVP エラー処理の設定 （189 ページ）	コール中に RSVP が失敗したときにシステムがどのように応答するかを設定します。
Step 5	MLPP から RSVP への優先レベルマッピングの設定 （190 ページ）	（オプション）複数レベルの優先順位およびプリエンプト (MLPP) を使用する場合は、発信者 MLPP 優先レベルを RSVP 優先順位にマップします。
Step 6	RSVP エージェントを構成します。	ゲートウェイ デバイスで次の IOS 手順を実行します。RSVP エージェントの設定方法については、デバイスのドキュメントを参照してください。
Step 7	アプリケーション ID の設定 （191 ページ）	RSVP アプリケーション ID を設定すると、音声およびビデオ トラフィックの両方に ID が追加され、受信した ID をもとに、Cisco RSVP エージェントは、それぞれのトラフィック タイプに帯域幅の制限を設定できます。
Step 8	DSCP マーキングの設定 （192 ページ）	DSCP マーキングを設定して、RSVP の予約が失敗した場合、システムが RSVP エージェントまたはエンドポイント デバイスに指示してメディアの差別化サービス コントロール ポイントのマーキングをベストエフォートに変更できるようにします。そうでないと、EF マークの付いた過度のメディア パケットにより、たとえ予約のあるフローの場合でも Quality of Service （QoS） が劣化する可能性があります。

クラスタ全体のデフォルト RSVP ポリシーの設定

クラスタ内の全ノードについて RSVP ポリシーを設定します。

手順

Step 1 Cisco Unified Communications Manager Administration で、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

Step 2 [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

Step 3 [クラスタ全体のパラメータ（システム-RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで、Default interlocation RSVP Policy サービスパラメータを設定します。

このサービスパラメータを次の値に設定できます。

- [予約なし（No Reservation）]：どの 2 つのロケーション間にも RSVP 予約は作成されません。
- [オプション（ビデオ優先）（Optional (Video Desired)）]：オーディオ ストリームおよびビデオ ストリームの両方の予約を取得できない場合は、ベストエフォートとして、オーディオのみのコールを継続できます。RSVP エージェントはオーディオに関する RSVP 予約を引き続き試み、予約が成功した場合は、Cisco Unified Communication Manager に通知します。
- [必須（Mandatory）]：Cisco Unified Communications Manager は、オーディオ ストリームに対する（コールがビデオ コールの場合はビデオ ストリームに対する）RSVP 予約が成功するまで、終了デバイスを呼び出しません。
- [必須（ビデオ優先）（Mandatory (Video Desired)）]：オーディオ ストリームの予約は成功したが、ビデオ ストリームの予約に失敗する場合は、音声のみでビデオ通話を行うことができます。

次のタスク

次のいずれかのオプションを選択します。

- ロケーション ペアで、残りのクラスタと異なるポリシーを使用する場合は、「ロケーション ペア RSVP ポリシーの設定 （187 ページ）」に進みます。
- クラスタ内の全ノードに同一の RSVP ポリシーを使用している場合は、「RSVP の再試行の設定 （188 ページ）」に進みます。

ロケーション ペア RSVP ポリシーの設定

ロケーションペアにクラスタの他とは別のポリシーを使用する場合、特定のロケーションペアの RSVP ポリシーを設定できます。次の手順を使用するとき、ロケーション ペアに設定する RSVP ポリシーは、クラスタに設定したポリシーをオーバーライドします。

手順

Step 1 Cisco Unified Communications Manager の管理ページで、**[システム(System)]** > **[ロケーション(Location)]** メニュー オプションを選択します。

Step 2 ロケーション ペアの一方のロケーションを検索し、そのロケーションを選択します。

Step 3 選択したロケーションと別のロケーション間の RSVP ポリシーを変更するには、ロケーション ペアのもう一方のロケーションを選択します。

Step 4 [RSVP 設定（RSVP Settings）] ドロップダウンリストで、このロケーション ペアの RSVP ポリシーを選択します。

このフィールドに次の値を設定できます。

- [システム デフォルトを使用（Use System Default）]：ロケーション ペアの RSVP ポリシーが、クラスタ全体の RSVP ポリシーと一致します。
- [予約なし（No Reservation）]：任意の 2 つのロケーション間で RSVP 予約が作られません。
- [音声優先（オプション）（Video Desired (Optional)）]：音声およびビデオ ストリームの予約を取得できない場合、ベストエフォート、音声のみのコールとして処理されます。RSVP エージェントは、音声の RSVP の予約を引き続き試行し、予約が成功すると Cisco Unified Communications Manager に通知します。オーディオ ストリームに対する（コールがビデオ コールの場合はビデオ ストリームに対する）RSVP 予約が成功するまで、終端デバイスを呼び出しません。
- [音声優先（Video Desired）] – オーディオ ストリームの予約は成功したが、ビデオ ストリームの予約が成功しない場合、ビデオ コールは音声のみコールとして処理されます。

次のタスク

RSVP の再試行の設定 （188 ページ）

RSVP の再試行の設定

RSVP の再試行の頻度および回数を設定するには、次の手順を実行します。

始める前に

- クラスタ全体のデフォルト RSVP ポリシーの設定 （186 ページ）
- （オプション） ロケーション ペア RSVP ポリシーの設定 （187 ページ）

手順

Step 1 Cisco Unified Communications Manager Administration で、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

Step 2 [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

Step 3 [クラスタ全体のパラメータClusterwide（System - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで指定されたサービスパラメータを設定します。

これらのサービスパラメータを次の値に設定できます。

- [RSVP 再試行タイマー（RSVP Retry Timer）]：RSVP 再試行タイマーの値を秒単位で指定します。このパラメータを 0 に設定すると、システムで RSVP の再試行が無効になります。
- [必須RSVPミッドコール再試行カウンタ（Mandatory RSVP Midcall Retry Counter）]：RSVP ポリシーが [必須（Mandatory）] に指定され、ミッドコールエラー処理オプションが「次の再試行カウンタを超えるとコールは失敗する（call fails following retry counter exceeds）」に設定されているときに、ミッドコール RSVP 再試行カウンタを指定します。デフォルト値は 1 回です。サービスパラメータを -1 に設定すると、予約が成功するか、コールが切断されるまで、いつまでも再試行が続行されます。

次のタスク

コール中の RSVP エラー処理の設定 （189 ページ）

コール中の RSVP エラー処理の設定

コール中の RSVP エラー処理の設定には、次の手順を使用します。

始める前に

RSVP の再試行の設定 （188 ページ）

手順

Step 1 Cisco Unified Communications Manager Administration で、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

Step 2 [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

Step 3 [クラスタ全体のパラメータ（システム - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで、指定されたサービスパラメータを設定します。

通話中の強制 RSVP エラー処理のオプション サービスパラメータに次の値を設定できます。

- [Call becomes best effort]： コール中に RSVP が失敗した場合、コールはベスト エフォート型のコールになります。再試行を有効にすると、RSVP の再試行が同時に開始されます。
- [Call fails following retry counter exceeded]：Mandatory RSVP Mid-call Retry Counter サービスパラメータに数値「N」を指定し、コール中に RSVP が失敗した場合、RSVP の再試行を N 回実行した後に、コールは失敗します。

次のタスク

ゲートウェイのデバイスに RSVP エージェントを設定します。RSVP エージェントの設定方法については、デバイスのドキュメントを参照してください。ゲートウェイで RSVP エージェントを設定した後は、Cisco Unified Communications Manager Administration に戻り、次のいずれかのオプションを選択します。

- （オプション）ネットワーク内でマルチレベルの優先順位とプリエンプションを使用している場合は、「MLPP から RSVP への優先レベルマッピングの設定 （190 ページ）」に進みます。
- アプリケーション ID の設定 （191 ページ）

MLPP から RSVP への優先レベルマッピングの設定

（オプション）発信者の MLPP 優先順位から RSVP 優先レベルへのマッピングを設定するには、次に示すクラスタ全体（システム - RSVP）のサービスパラメータを使用します。

- MLPP EXECUTIVE OVERRIDE To RSVP Priority Mapping
- MLPP FLASH OVERRIDE To RSVP Priority Mapping
- MLPP FLASH To RSVP Priority Mapping
- MLPP IMMEDIATE To RSVP Priority Mapping
- MLPP PL PRIORITY To RSVP Priority Mapping
- MLPP PL ROUTINE To RSVP Priority Mapping

これらのサービスパラメータを選択し、設定するには、次の手順を実行します。

手順

Step 1 Cisco Unified Communications Manager Administration で、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

Step 2 [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

Step 3 [クラスタ全体のパラメータClusterwide（System - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで指定されたサービスパラメータを設定します。

これらのサービスパラメータは、次のように機能します。

- サービスパラメータ値が高いほど、優先度を上げるという設定に基づいて RSVP 予約を開始するとき、Cisco Unified Communications Manager は発信者の優先度レベルを RSVP 優先度にマップします。
- IOS ルータは RSVP 優先度に基づいてコールをプリエンプション処理します。
- RSVP エージェントは、プリエンプションの理由を含め、RSVP 予約の失敗の理由について Cisco Unified Communications Manager に通知する必要があります。
- Cisco Unified Communication Manager は、既存の MLPP メカニズムを使用して、優先処理の対象となった発信側と着信側に優先処理に関する通知を行います。

次のタスク

ゲートウェイのデバイスに RSVP エージェントを設定します。RSVP エージェントの設定方法については、デバイスのドキュメントを参照してください。ゲートウェイで RSVP のエージェントを設定した後は、Cisco Unified Communications Manager Administration と「アプリケーション ID の設定 （191 ページ）」に戻ります。

アプリケーション ID の設定

RSVP アプリケーション ID を設定すると、音声およびビデオ トラフィックの両方に ID が追加され、受信した ID をもとに、Cisco RSVP エージェントは、それぞれのトラフィック タイプに帯域幅の制限を設定できます。

この手順を開始する前に、ゲートウェイ デバイスで RSVP のエージェントを設定します。RSVP エージェントの設定方法については、デバイスのドキュメントを参照してください。

始める前に

ネットワークに RSVP アプリケーション ID を導入するには、Cisco RSVP Agent ルータで、Cisco IOS Release 12.4(6)T 以降を使用する必要があります。

手順

Step 1 Cisco Unified Communications Manager Administration で、**[システム（System）]**>**[サービスパラメータ（Service Parameters）]** を選択します。

Step 2 [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

Step 3 [クラスタ全体のパラメータ（システム - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで、RSVP Audio Application ID サービスパラメータを設定します。

デフォルトは AudioStream です。

Step 4 [クラスタ全体のパラメータ（システム - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで、RSVP Video Application ID を設定します。

デフォルトは VideoStream です。

次のタスク

DSCP マーキングの設定 （192 ページ）

DSCP マーキングの設定

RSVP 予約が失敗した場合、 は RSVP エージェントまたはエンドポイント（RSVP エージェントの割り当てに失敗した場合）に、メディアの Differentiated Services Control Point（DSCP）マークをベストエフォート型に変更するよう指示します。そうでないと、EF マークの付いた過度のメディアパケットにより、たとえ予約のあるフローの場合でも Quality of Service（QoS）が劣化する可能性があります。

始める前に

アプリケーション ID の設定 （191 ページ）

手順

Step 1 Cisco Unified Communications Manager Administration で、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

Step 2 [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

Step 3 [クラスタ全体のパラメータ（システム - QoS）（Clusterwide Parameters (System - QoS)）] セクションで、**DSCP for Audio Calls When RSVP Fails** のサービスパラメータを設定します。

Step 4 [クラスタ全体のパラメータ（システム - QoS）（Clusterwide Parameters (System - QoS)）] セクションで、**DSCP for Video Calls When RSVP Fails** のサービスパラメータを設定します。

第 17 章

プッシュ通知の設定

プッシュ通知の概要

クラスタでプッシュ通知が有効になっている場合、Unified Communications Manager および IM and Presence Service は、一時停止モード（バックグラウンドモードとも呼ばれます）で動作している Android および iOS 用 Cisco Jabber または Cisco Webex クライアントに音声通話、ビデオ通話、インスタントメッセージの通知をプッシュするために、Google 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ます。プッシュ通知によって、システムは Cisco Jabber または Cisco Webex と永続的な通信を維持できます。プッシュ通知は、エンタープライズネットワーク内から接続する Android および iOS 用 Cisco Jabber および Cisco Webex クライアントと、Expressway のモバイルおよびリモートアクセス機能を通じてオンプレミス展開に登録するクライアントの両方で必要となります。

プッシュ通知の動作

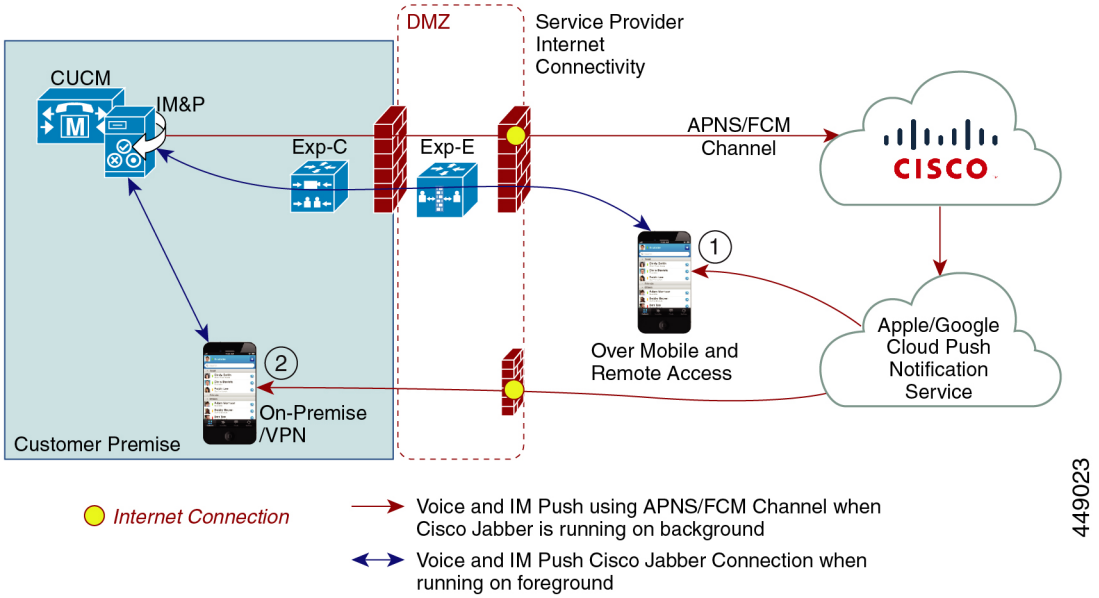
Android および iOS プラットフォームデバイスにインストールされているクライアントは、起動時に Unified Communications Manager、IM and Presence Service、および Google と Apple のクラウドに登録します。モバイルおよびリモートアクセス展開では、クライアントは Expressway 経由でオンプレミスサーバに登録します。Cisco Jabber および Cisco Webex クライアントがフォアグラウンドモードになっている限り、Unified Communications Manager および IM and Presence Service は、コールとインスタントメッセージをクライアントに直接送信することができます。

ただし、Cisco Jabber または Cisco Webex クライアントが（たとえばバッテリ寿命を長持ちさせるために）サスペンドモードに移行すると、標準の通信チャネルは使用不可となり、Unified Communications Manager および IM and Presence Service がクライアントと直接通信することはできなくなります。プッシュ通知は、パートナークラウドを介してクライアントに到達するための別のチャネルを提供します。

（注） 次の条件のいずれかに当てはまる場合、Cisco Jabber と Cisco Webex はサスペンドモードで動作していると見なされます。

- Cisco Jabber または Cisco Webex アプリケーションがオフスクリーン（バックグラウンド）で実行されている。
- Android または iOS デバイスがロックされている。
- Android または iOS デバイスの画面がオフになっている。

図 *6*: プッシュ通知アーキテクチャ



上の図は、Android および iOS 用 Cisco Jabber または Cisco Webex クライアントが、バックグラウンドで動作している場合と停止している場合の動作を示したものです。この図では、(1) クライアントが Expressway 経由でオンプレミスの Cisco Unified Communications Manager および IM and Presence Service 展開に接続するモバイルおよびリモートアクセス展開と、(2) エンタープライズネットワーク内からオンプレミス展開に直接接続する Android および iOS 用 Cisco Jabber または Cisco Webex クライアントを示しています。

（注） iOS13 の Apple クライアントおよびサポートされている Android クライアントでは、音声通話とメッセージは別々のプッシュ通知チャネル（「VoIP」と「Message」）を使用して、バックグラウンドモードで動作しているクライアントに到達します。ただし、全般的なフローはどちらのチャネルでも同じです。iOS 12 では、音声通話とメッセージは同じチャネルを使用して配信されます。

Cisco Jabber および Cisco Webex のプッシュ通知の動作

次の表は、Unified Communications Manager および IM and Presence Service に登録された iOS 用 Cisco Jabber または Cisco Webex クライアントの iOS 12 および iOS 13 での動作を説明したものです。

Cisco Jabber または Cisco Webex クライアントの動作モード	Cisco Jabber が iOS12 デバイスで実行されている場合	Cisco Jabber が iOS13 デバイスまたは Android デバイスで実行されている場合
フォアグラウンドモード	音声/ビデオ通話 Unified Communications Manager は、標準の SIP 通信チャネルを使用して、音声通話とビデオ通話を Cisco Jabber または Cisco Webex クライアントに直接送信します。 通話の場合、Unified Communications Manager はプッシュ通知もフォアグラウンドモードの Cisco Jabber または Cisco Webex クライアントに送信します。ただし、通話の確立には、プッシュ通知チャネルではなく標準の SIP チャネルが使用されます。 メッセージ IM and Presence Service は、標準の SIP 通信チャネルを使用してメッセージをクライアントに直接送信します。メッセージの場合、フォアグラウンドモードのクライアントにプッシュ通知は送信されません。	動作は iOS12 の場合と同じです。

Cisco Jabber または **Cisco Webex** クライアントの動作モード	**Cisco Jabber** が **iOS12** デバイスで実行されている場合	**Cisco Jabber** が **iOS13** デバイスまたは **Android** デバイスで実行されている場合
サスペンドモード（バックグラウンドモード）	ビデオまたはビデオ コール 標準の通信チャネルは使用できません。Unified CM はプッシュ通知チャネルを使用します。 通知を受信すると、Cisco Jabber または Cisco Webex クライアントは自動的にフォアグラウンドモードに戻り、クライアントが呼出音を鳴らします。 メッセージ 標準の通信チャネルは使用できません。IM and Presence サービスは、プッシュ通知チャネルを使用して、次のように IM 通知を送信します。 **1.** IM and Presence サービスは、Cisco Cloud のプッシュ REST サービスに IM 通知を送信します。これにより、通知が Apple クラウドに転送されます。 **2.** Apple クラウドは Cisco Jabber または Cisco Webex クライアントに IM 通知をプッシュし、Cisco Jabber または Cisco Webex クライアントに通知が表示されます。 **3.** ユーザが通知をクリックすると、Cisco Jabber または Cisco Webex クライアントは再びフォアグラウンドに移行します。Cisco Jabber または Cisco Webex クライアントは、IM and Presence Service とのセッションを再開し、インスタントメッセージをダウンロードします。 （注） Cisco Jabber または Cisco Webex クライアントがサスペンドモードの間、ユーザのプレゼンスステータスは「**退席中**（**Away**）」と表示されます。	iOS13 では、コールトラフィックとメッセージトラフィックは別々のプッシュ通知チャネルに分けられます。コールには「VoIP」チャネル、メッセージングには「Message」チャネルが使用されます。 ビデオまたはビデオ コール 標準の通信チャネルは使用できません。Unified CM は「VoIP」プッシュ通知チャネルを使用します。 VoIP 通知を受け取ると、Jabber は発信者 ID を使用して CallKit を起動します。 この動作は、Cisco Jabber または Cisco Webex iOS クライアントに適用されます。 メッセージ 標準の通信チャネルは使用できません。IM and Presence Service は、「Message」プッシュ通知チャネルを使用します。 **1.** IM and Presence サービスは、Cisco Cloud のプッシュ REST サービスに IM 通知を送信します。これにより、通知が Apple クラウドに転送されます。 **2.** Apple クラウドは、Cisco Jabber または Cisco Webex クライアントに IM 通知をプッシュします。 **3.** ユーザが通知をクリックすると、Cisco Jabber または Cisco Webex クライアントはフォアグラウンドモードに移行します。Cisco Jabber または Cisco Webex クライアントは、IM and Presence Service とのセッションを再開し、メッセージをダウンロードします。 （注） Cisco Jabber または Cisco Webex クライアントがサスペンドモードの間、ユーザのプレゼンスは「**退席中**（**Away**）」と表示されます。

プッシュ通知がサポートされるクライアント

クライアント	OS	プラットフォームクラウド	クラウドサービス
iPhone および iPad の Cisco Jabber	iOS	Apple	Appleプッシュ通知サービス（APNS）
Android の Cisco Jabber	Android	Google	Android PNS サービス
iOS での Webex	iOS	Apple	Appleプッシュ通知サービス（APNS）
Android での Webex	Android	Google	Android PNS サービス

プッシュ通知の設定

プッシュ通知の設定および導入の方法の詳細は、『*iPhone* および *iPad* での *Cisco Jabber* のプッシュ通知の導入』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）を参照してください。

第 II 部

ダイヤル プラン

第 18 章

パーティションの設定

パーティションの概要

パーティションは、次のいずれかの論理グループです。

- ルートパターン
- ボイス メールのディレクトリ番号（DN）
- 変換パターン
- 変換パターン
- ユニバーサルリソース識別子（URI）
- ハントパイロット

パーティションによって組織、ロケーション、通話タイプを基にルートプランを論理サブセットに分割することで、コールルーティングが容易になります。

コーリングサーチスペースの概要

呼び出し先の検索スペース (CSS) は、パーティションの優先順位リストです。検索スペースの呼び出しによって、発信者がコールするために使用できるコール通知先が決定されます。コール先は、発信者の呼び出し用検索スペースで利用可能なパーティションに存在する必要があります。また、発信者はその通知先を呼び出すことができません。コール検索スペースは、ディレクトリ番号と、電話やゲートウェイなどのデバイスに割り当てることができます。

発信者の電話機と発信者のディレクトリ番号の両方に、検索スペースが割り当てられている場合、システムはその 2 つを連結して、発信者のための CSS を提供します。

コール権限に従って、パーティションを使用し、検索スペースを呼び出すことによってシステムを編成できます。たとえば、次のようにすることができます。

- 一部の従業員が長距離通話に対応しないように制限する
- ロビー電話から CEO への直接コールの発信者を制限する

サービスクラス

パーティションを使用して、検索スペース (CSS) を呼び出して、サービスのクラスを設定することができます。次の表に、PSTN アクセスを提供するサービスクラスのために作成できる、パーティションの例と、検索スペースの発信スペースを示します。

- 緊急コール
- ローカル コール
- ナショナル コール
- 国際通話

表 *14 :* パーティションとコーリングサーチスペース

コーリングサーチスペース	ルート パーティション 1	ルート パーティション 2	ルート パーティション 3	機能
Base_CSS	Base_PT	—	—	• 緊急 • オンネット
LocalPSTN_CSS	PSTN_Local_PT	—	—	• 緊急 • オンネット • ローカル
NationalPSTN_CSS	PSTN_Local_PT	PSTN_National_PT	—	• 緊急 • オンネット • ローカル • 国内

コーリングサーチスペース	ルート パーティション 1	ルート パーティション 2	ルート パーティション 3	機能
InternationalPSTN_CSS	PSTN_Local_PT	PSTN_National_PT	PSTN_Intl_PT	• 緊急 • オンネット • ローカル • 国内 • 国際

デバイスは、Base_CSS のようなコール対象の検索スペースに自動的に登録されます。これにより、すべてのデバイスでオフネット番号と緊急オンネット番号の両方にダイヤルできるようになります。ローカル 7 桁またはローカル 10 桁、国内、および国際ダイヤリング機能を提供するには、ユーザデバイスプロファイルで残りのコーリングサーチスペースを電話番号に割り当てる必要があります。

パーティションの設定タスクフロー

手順

	コマンドまたはアクション	目的
Step 1	パーティションの設定 （203 ページ）	パーティションを設定して、到達可能性の特徴が類似したシステム リソースの論理グループを作成します。
Step 2	コーリング サーチ スペースの設定 （205 ページ）	コーリングサーチスペースは、コールを完了しようとする発信側デバイスが検索するパーティションを決定します。

パーティションの設定

パーティションを設定して、到達可能性の特徴が類似したシステム リソースの論理グループを作成します。次のいずれに対してもパーティションを作成できます。

- ルートパターン
- ボイス メールのディレクトリ番号（DN）
- 変換パターン
- 変換パターン
- ユニバーサルリソース識別子（URI）

- ハントパイロット

パーティションを作成することで、ルートプランが組織、場所、通話タイプに基づいた論理サブセットに分割されることになり、コールルーティングが容易になります。複数のパーティションを設定できます。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[コールルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [パーティション（Partition）]** を選択します。

Step 2 [新規追加（Add New）] をクリックして新しいパーティションを作成します。

Step 3 [パーティション名、説明（Partition Name, Description）] フィールドに、ルート プランに固有のパーティション名を入力します。

パーティション名には、英数字とスペースの他にハイフン（-）とアンダースコア（_）を使用できます。パーティション名に関するガイドラインについては、オンライン ヘルプを参照してください。

Step 4 パーティション名の後にカンマ（,）を入力し、パーティションの説明を同じ行に入力します。

説明には、任意の言語で最大50文字を使用できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）、角括弧（[]）は使用できません。

説明を入力しなかった場合は、Cisco Unified Communications Manager が、このフィールドに自動的にパーティション名を入力します。

Step 5 複数のパーティションを作成するには、各パーティション エントリごとに 1 行を使います。

Step 6 [スケジュール（Time Schedule）] ドロップダウンリストから、このパーティションに関連付けるスケジュールを選択します。

スケジュールでは、パーティションが着信コールの受信に利用可能となる時間を指定します。[なし（None）] を選択した場合は、パーティションが常にアクティブになります。

Step 7 次のオプション ボタンのいずれかを選択して、[タイム ゾーン（Time Zone）] を設定します。

- [発信側デバイス（Originating Device）]：このオプション ボタンを選択すると、発信側デバイスのタイムゾーンと [スケジュール（Time Schedule）] が比較され、パーティションが着信コールの受信に使用できるかどうかが判断されます。
- [特定のタイム ゾーン（Specific Time Zone）]：このオプション ボタンを選択した後、ドロップダウン リストからタイム ゾーンを選択します。選択されたタイム ゾーンと [スケジュール（Time Schedule）] が比較され、着信コールの受信にパーティションが使用できるかどうかが判断されます。

Step 8 [保存（Save）] をクリックします。

パーティション名のガイドライン

コーリングサーチスペースのパーティションのリストは最大1024文字に制限されています。つまり、CSS 内のパーティションの最大数は、パーティション名の長さによって異なります。次の表を使用して、パーティション名が固定長である場合のコーリングサーチスペースに追加できるパーティションの最大数を決定します。

表 *15*：パーティション名のガイドライン

パーティション名の長さ	パーティションの最大数
2 文字	340
3 文字	256
4 文字	204
5 文字	172
...	...
10 文字	92
15 文字	64

コーリング サーチ スペースの設定

コーリング サーチ スペースは、通常はデバイスに割り当てられるルート パーティションの番号付きリストです。コーリングサーチスペースでは、発信側デバイスが電話を終了しようとする際に検索できるパーティションが決定されます。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[コールルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [コーリングサーチスペース（Calling Search Space）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [名前（Name）] フィールドに、名前を入力します。

各コーリング サーチ スペース名がシステムに固有の名前であることを確認します。この名前には、最長 50 文字の英数字を指定することができ、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて含めることが可能です。

Step 4 [説明（Description）] フィールドに、説明を入力します。

説明には、任意の言語で最大50文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

Step 5 [使用可能なパーティション（Available Partitions）] ドロップダウン リストから、次の手順のいずれかを実施します。

- パーティションが 1 つの場合は、そのパーティションを選択します。
- パーティションが複数ある場合は、Ctrl キーを押した状態で適切なパーティションを選択します。

Step 6 ボックス間にある下矢印を選択し、[選択されたパーティション（Selected Partitions）] フィールドにパーティションを移動させます。

Step 7 （任意）[選択されたパーティション（Selected Partitions）] ボックスの右側にある矢印キーを使用して、選択したパーティションの優先順位を変更します。

Step 8 [保存（Save）] をクリックします。

パーティションの連携動作と制限

表 *16 :* パーティション制限

機能またはアクション	制限事項
パーティションの削除	パーティションを削除する前に、次のいずれかのタスクを完了してください。 • コーリングサーチスペース、デバイス、または削除するパーティションを使用しているその他の項目に異なるパーティションを割り当てる。 • コーリングサーチスペース、デバイス、または削除するパーティションを使用しているその他の項目を削除する。 削除されたパーティションは取得できなくなるため、正しいパーティションを削除していることを慎重に確認してください。誤ってパーティションを削除した場合は、それを再構築する必要があります。
変換パターン	変換パターンにはディジット操作が含まれており、パーティションに割り当てられます。コールが変換パターンと一致する場合、Unified CM が変換を実行し、その変換パターンで指定されるコーリングサーチスペースを使用してコールを再ルーティングします。変換パターンの詳細については、「コールルーティングの設定」の章を参照してください。
時間帯ルーティング	パーティションが着信コールを受け入れ可能なスケジュールを設定します。ルーティングの時間設定の詳細については、「コールルーティングの設定」の章を参照してください。

機能またはアクション	制限事項
論理パーティション設定	**任意**：ゲートウェイおよびトランクアクセスを使用して内部VoIPネットワークを外部ネットワークから分割できます。ほとんどの導入環境では論理パーティションの使用は任意ですが、インドのように、内部ネットワークから外部へのコールをすべてローカルPSTNゲートウェイに接続することが規制により必須となっている国では必須です。論理パーティショニングの設定の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「論理パーティション分割を設定する」のセクションを参照してください。

第 19 章

国内番号計画のインストール

国内番号計画の概要

Unified Communications Manager では、デフォルトで北米電話番号計画（NANP）を提供しています。設定されているダイヤルプラン要件が異なる国の場合は、シスコの国際ダイヤルプランをインストールし、それを使用して、要件特有の一意の番号計画を作成できます。

番号計画には、数字破棄命令（DDI）と、その番号計画に固有のタグが含まれています。これらの項目は、コールルーティングを設定するときに、番号計画に適したルーティングルールを作成するために使用できます。

この章では、国内番号計画をインストールする方法について説明します。国内番号計画の使用の詳細については、『*Unified Communications Manager* ダイヤルプラン導入ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

国内番号計画の前提条件

北米以外の国の国内番号計画をインストールする場合は、現在のリリース用の国際ダイヤルプランが含まれている Cisco Option Package（COP）ファイルをダウンロードします。COP ファイルでは、IDP v.*x* という命名規則が使用されています。このファイルは、シスコの Web サイトから入手できます。

- https://software.cisco.com/download/navigator.html

このファイルを、Unified Communications Manager がアクセスできる外部 FTP サーバまたは SFTP サーバに配置します。

国内番号計画のインストールタスクフロー

手順

	コマンドまたはアクション	目的
Step 1	COP ファイルのインストール （210 ページ）	（**省略可**）北米以外の国における番号計画をインストールするには、現在のリリース用の国際ダイヤルプランを含む Cisco Option Package（COP）ファイルをダウンロードします。
Step 2	国内番号計画のインストール （211 ページ）	クラスタ内のそれぞれの Unified Communications Manager ノードに国内の番号計画をインストールします。北米以外の国の国内番号計画をインストールする場合場合にのみ、次の手順を実行します。
Step 3	CallManager サービスの再起動 （212 ページ）	変更は、サービスを再起動した後に有効になります。

COP ファイルのインストール

国際ダイヤルプランを含む Cisco Option Package（COP）ファイルをインストールするには、次の手順を実行します。

手順

Step 1 Unified Communication Manager のパブリッシャ ノードで、この手順を開始します。Cisco Unified Communications OS の管理で、**[ソフトウェアアップグレード（Software Upgrades）]>[インストール（Install）]** を選択します。
[ソフトウェアのインストール/アップグレード（Software Installation/Upgrade）] ウィンドウが表示されます。

Step 2 [ソース（Source）] フィールドで、[リモート ファイル システム（Remote File System）] を選択します。

Step 3 [ソフトウェアのインストール/アップグレード（Software Installation/Upgrade）] ウィンドウで、フィールドを設定します。フィールドとその設定オプションの詳細については、「関連項目」を参照してください。

Step 4 [次へ（Next）] をクリックします。
ウィンドウが更新され、使用可能なソフトウェアのオプションとアップグレードのリストが表示されます。

Step 5 [オプション/アップグレード（Options/Upgrades）] ドロップダウンリストで、[DP COP] ファイルを選択して、[次へ（Next）] をクリックします。
[インストール ファイル（Installation File）] ウィンドウが開き、FTP サーバからファイルをダウンロードします。ウィンドウにダウンロードの進捗が表示されます。

Step 6 [チェックサム（Checksum）] ウィンドウが表示されたら、そのチェックサムの値をダウンロードしたファイルのチェックサムの値と比較検証します。

Step 7 [次へ（Next）] をクリックして、ソフトウェア アップグレードに進みます。
警告メッセージとして、インストールするために選択した DP COP ファイルが表示されます。

Step 8 [インストール（Install）] をクリックします。
[インストール状況（Install Status）] ウィンドウが表示されます。

Step 9 [完了（Finish）] をクリックします。

Step 10 Unified Communication Manager サブスクライバ ノードで、この手順を繰り返します。クラスタ内の全ノードに COP ファイルをインストールする必要があります。

関連トピック

COP ファイル インストールのフィールド, on page 211

COP ファイル インストールのフィールド

フィールド	説明
ディレクトリ（Directory）	COP ファイルが配置されているディレクトリを入力します。
リモート サーバ（Remote Server）	COP ファイルが配置されているサーバのホスト名または IP アドレスを入力します。
リモート ユーザ（Remote User）	リモート サーバのユーザ名を入力します。
リモート パスワード（Remote Password）	リモート サーバのパスワードを入力します。
転送プロトコル（Transfer Protocol）	リモート サーバと接続する場合に使用するプロトコルを選択します。

国内番号計画のインストール

北米以外の国の国内番号計画をインストールする場合場合にのみ、次の手順を実行します。

クラスタ内のそれぞれの Unified Communications Manager ノードに国内の番号計画をインストールします。Unified Communication Manager publisher ノードから始めます。

手順

Step 1 Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ダイヤルプランインストーラ（Dial Plan Installer）]** を選択します。

Step 2 検索条件を入力して [検索（Find）] をクリックします。

Step 3 インストールするダイヤル プランのバージョンを [利用可能なバージョン（Available Version）] ドロップダウンリストから選択します。

Step 4 [インストール（Install）] をクリックします。
ステータスに、ダイヤル プランがインストールされたことが表示されます。

Step 5 クラスターのサブスクライバ ノードごとにこの手順を繰り返します。

CallManager サービスの再起動

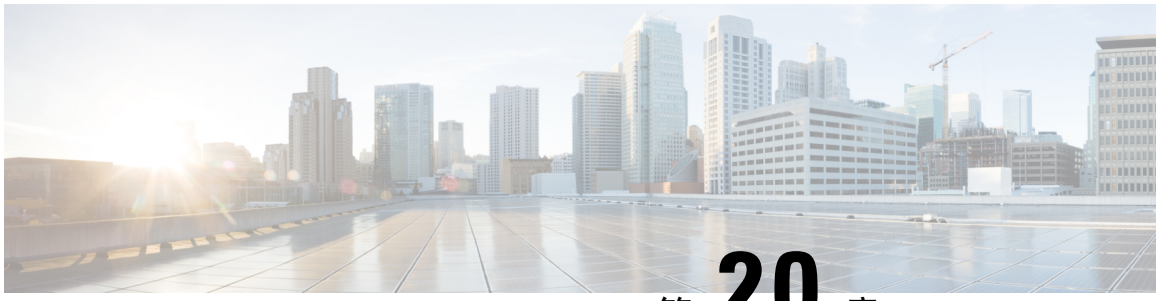
手順

Step 1 Cisco Unified Serviceability インターフェイスで、**[ツール（Tools）] > [コントロールセンター - 機能サービス（Control Center - Feature Services）]** を選択します。

Step 2 [サーバ（Servers）] ドロップダウンリストから、Cisco Unified Communications Manager サーバを選択します。
CM の [サービス（Services）] 領域で、[サービス名（Service Name）] 列に Cisco CallManager が表示されます。

Step 3 Cisco CallManager サービスに対応するラジオ ボタンをクリックします。

Step 4 [再起動（Restart）] をクリックします。
サービスが再起動し、「サービスは正常に再起動しました（Service Successfully Restarted）」というメッセージが表示されます。



第 20 章

コールルーティングの設定

コールルーティングの概要

このシステムでは、クラスタ間でのコールのルーティング方法、およびプライベート ネットワークまたは公衆電話交換網（PSTN）に対する外部コールのルーティング方法を決定するために、ルートプランを使用します。設定したルートプランにより、各通話タイプをルーティングするためにシステムが使用するパスが指定されます。たとえば、オンネットコールにIPネットワークを使用するルートプランや、ローカル PSTN コールと国際コールに別々のキャリアを使用するルートプランを作成できます。

変換パターン

トランスレーションパターンを設定すると、任意のタイプのコールの数字を操作できます。変換パターンは、ルートパターンと同じ一般規則に従い、同じワイルドカードを使用します。ルートパターンと同じように、変換パターンをパーティションに割り当てます。ただし、ダイヤルされた数字が変換パターンと一致する場合、Unified CM は、ゲートウェイなどの外部エンティティにコールをルーティングしません。代わりに、まず変換を実行した後、変換パターン内で設定されたコーリングサーチスペースを使用して、コールを再度ルーティングします。

（注） 選択したパーティション、ルートフィルタ、および番号計画の組み合わせを使用する変換パターンが固有であることを確認してください。それには、ルートパターン/ハントパイロット、変換パターン、電話番号、通話パーク番号、コール ピックアップ番号、またはミートミー番号の設定ウィンドウを確認して、重複するエントリがあることを示すエラーを受け取っていないかどうかを調べます。

変換パターン

変換パターンを使用すると、数字の破棄、プレフィックス番号の追加、発信側変換マスクの追加を行えます。また、システムが電話機または PSTN にコールを送信する前に発信者番号の表示を制御することもできます。

変換パターンを設定し、それらをルートパーティションに関連付けて、そのパーティションを含むコーリングサーチスペースにパターンを割り当てます。[設定 (configuration)] ウィンドウの発呼側変換 CSS または着信側変換 CSS フィールドを使用して、特定のデバイス、デバイスプール、ゲートウェイ、またはトランクのコール設定にパターンを割り当てることができます。

次の変換パターンを設定できます。

- **発信側変換パターン**：発信者番号のグローバル形式を、ゲートウェイまたはトランクなどのルートグループ デバイスに接続されているクラスタ外のネットワークで必要となるローカルの形式に適応させることができます。

  着信側変換パターン：着信番号のグローバル形式を、ルートグループ デバイスに接続されているクラスタ外のネットワークで必要となるローカル形式に適応させることができます。

ルートパターン

このシステムには、次のコンポーネントを使用するルーティングを計画するための 3 階層方式があります。

- **ルートパターン**：システムは、外部向けのダイヤル文字列と合致する設定済みのルートパターンを検索し、それを使用して、ゲートウェイまたはルートリストにコールを転送します。ルートパターンは、ゲートウェイ、トランク、または 1 つ以上のルートグループを含むルートリストに割り当てることができます。
- **ルートリスト**：コールで使用可能なパスの優先順位付きリスト。
- **ルート グループ**：使用可能なパス。ルート グループは、ゲートウェイとトランクにコールを分配します。

追加のコールルーティング

ルートプランには、次のオプションコンポーネントを含めることもできます。

- **ローカルルートグループ**:複数のサイトがある場合は、ローカルルートグループを使用して、ルートパターンの設定ではなく、デバイスプールで指定されたゲートウェイにオフネットコールをルーティングできるようにすることができます。これにより、複数のロケーションに単一のルートパターンセットを使用できます。
- **ルートフィルタ**:ルートフィルタを作成し、ルートパターンまたはハントパイロットに追加して、ユーザによるパターンの使用を制限します。ルートフィルタは必須ですが、ダイヤルプランインストーラファイルを使用していますが、手動のダイヤルプラン設定ではオプションです。手動設定では、パターンが @ ワイルドカードを使用している場合にのみ、ルートフィルタが適用されます。

- **自動代替ルーティング**：帯域幅不足のためシステムがコールをブロックしたときに、PSTNまたは別のネットワークを介してコールを自動的に再ルーティングします。
- **時間指定ルーティング**：特定のパーティションが着信コールを受信できる時間を指定するスケジュールを作成します。

コールルーティングの前提条件

- パーティションの設定タスクフロー（203 ページ）の操作を実行します。
- 次の情報が用意されていることを確認してください。
  - 内部番号（内線）
  - 各ゲートウェイに転送されるコールをリストしているプラン

コールルーティングの計画の詳細については、『シスココラボレーションシステムソリューションリファレンスネットワーク設計』の「コール制御とルーティング」のトピックを参照してください。

コールルーティングの設定タスクフロー

手順

	コマンドまたはアクション	目的
Step 1	変換パターンの設定（216 ページ）	トランスレーションパターンを設定して、特定のパーティション内のコールのディジット変換を完了する方法を指定します。
Step 2	発信側変換パターンの設定（217ページ）	このプロセスを使って呼び出し元の番号を変換します。例えば、PSTNを呼び出したときに、発信者の内線番号をオフィスのマスター番号で置き換える変換モードを設定しても良い。
Step 3	着信側変換パターンの設定（218ページ）	この手順を使用して、着信側の番号を変換します。たとえば、10 桁の発信者の最後の 5 桁のみを保持する変換パターンを設定できます。
Step 4	ローカルルートグループの設定（218ページ）	（**オプション**）ローカルルートグループを使用すると、複数のロケーションに対して単一のルートパターンセットを使用できます。ユニファイド CM は、ルート

	コマンドまたはアクション	目的
		パターンではなく、発信側デバイスの場所に基づいてゲートウェイを割り当てます。
Step 5	ルートグループの設定 （221 ページ）	（**オプション**）ゲートウェイのデバイスの選択順序を設定するようにルート グループを設定します。ルート グループには、1 つ以上のデバイスが含まれています。
Step 6	ルートリストの設定 （221 ページ）	（**オプション**）ルートリストには、1 つ以上のルート グループが含まれています。ルート グループの選択順序を制御するためにルートリストを設定します。
Step 7	ルートフィルタの設定 （222 ページ）	（**オプション**）ルートパターンが許可する特定の数字を制限するためにルーティングのフィルタを使用します。
Step 8	ルートパターンの設定 （226 ページ）	ルーティングモードを設定し、特定の装置に呼を向け、特定のデジタルモードを含むかまたは除外する。
Step 9	クラスタ全体の自動代替ルーティングの有効化 （231 ページ）	（**オプション**）自動代替ルーティング（AAR）を有効化すると、帯域幅不足のためにコールがブロックされたときに、システムは PSTN または別のネットワークを介してコールを再ルーティングします。
Step 10	AAR グループの設定 （231 ページ）	（**オプション**）自動代替ルーティングに適用するディジット変換を使用して、AAR グループを設定します。
Step 11	時間帯ルーティングの設定（232ページ）	（**オプション**）特定のパーティションが着信コールに応答可能な時間を指定するタイムスケジュールを作成します。

変換パターンの設定

ダイヤル文字列がパターンと一致したときに発信番号と着信番号にディジット操作を適用するには、変換パターンを設定します。システムは数字の変換を完了してから、コールを再ルーティングします。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [トランスレーションパターン（Translation Pattern）]** を選択します。

Step 2 次のいずれかのオプションを選択します。

- 新しい変換パターンを追加するには、[新規追加（Add New）] をクリックします。
- 既存の変換パターンを選択するには、[検索（Find）] をクリックします。

Step 3 [トランスレーションパターン（Translation Pattern）] フィールドに、このパターンを使用するダイヤル文字列と照合するパターンを入力します。

Step 4 [パーティション（Partition）] ドロップダウンリストから、このパターンを割り当てるパーティションを選択します。

Step 5 [トランスレーションパターンの設定（Translation Pattern Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 6 [保存（Save）] をクリックします。

発信側変換パターンの設定

このプロセスを使って呼び出し元の番号を変換します。例えば、PSTNを呼び出したときに、発信者の内線番号をオフィスのマスター番号で置き換える変換モードを設定しても良い。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[Call Routing（コールルーティング）] > [変換（Transformation）] > [変換パターン（Transformation Pattern）] > [着信側変換パターン（Calling Party Transformation Pattern）]**。

Step 2 次のいずれかのオプションを選択します。

- 新しい変換後のパターンを追加するには、**[新規追加（Add New）]** をクリックします。
- 既存のパターンを選択するには、[検索（Find）] をクリックします。

Step 3 [**パターン (** pattern)] フィールドで、発信者番号と一致させるパターンを入力します。

（注） **発信コールの場合：**

事前変換発信側番号に基づいて、発信者の変換マスクが選択されます。（IP 電話に割り当てられた内線番号）。

SIP トランクで発信側変換マスクを選択する間に、ルートパターンまたはグループで発信側番号が別の番号に変換された場合、発信側変換マスクの選択には常に事前変換発信側番号が使用されます。

Dialed Number Analyzer（DNA）に従っている限り、変換された番号を使用して発信側変換マスクが選択されます。ただし、これはDNAの動作としては正しくありません。

Step 4 **[関係者の変換パターンの設定]** ウィンドウで、残りのすべてのフィールドに入力します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 5 [保存（Save）] をクリックします。

着信側変換パターンの設定

この手順を使用して、着信側の番号を変換します。着信番号の変換：たとえば、10 桁の番号としてダイヤルされたコールの最後の 5 桁のみを保持する。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [変換（Transformation）] > [変換パターン（Transformation Pattern）] > [着信側変換パターン（Called Party Transformation Pattern）]** を選択します。

Step 2 次のいずれかのオプションを選択します。

- 新しい着信側変換パターンを追加するには、[新規追加（Add New）] をクリックします。
- 既存のパターンを選択するには、[検索（Find）] をクリックします。

Step 3 [パターン（Pattern）] フィールドで、着信番号と一致させるパターンを入力します。

Step 4 **[着信側変換パターンの設定（Called Party Transformation Pattern Configuration）]**ウィンドウで、残りのフィールドに入力します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 5 [保存（Save）] をクリックします。

ローカルルートグループの設定

（省略可）ローカルルートグループを設定して、必要なルートリストの数を減らすことができます。リストのポイントを、PSTNゲートウェイのロケーションに基づいて、システムが発信をルーティングするのに使用する PSTN ゲートウェイにルーティングします。代替として、ゲートウェ

イへのアクセスに使用されるルートパターンから PSTN ゲートウェイのロケーションを分離するためにローカルルートグループを使用できます。この設定により、異なるロケーションにある電話やその他のデバイスが単一セットのルートパターンを使用できますが、Cisco Unified Communications Manager が適切なゲートウェイを選択してコールをルーティングします。

たとえば、ローカルルートグループを使用すると、国のすべての市で別々のダイヤル プランを持つのではなく、国全体で単一のダイヤル プランを持つことができます。このアプローチが有効なのは、一元化されたコール導入のシナリオについてだけです。

手順

	コマンドまたはアクション	目的
Step 1	ローカルルートグループの設定（219ページ）	（**オプション**）システムは、標準ローカルルートグループと呼ばれるデフォルトのローカルルートグループを提供しますが、追加のローカルルートグループを設定できます。追加のローカルルートグループを指定するには、次の手順を使用します。
Step 2	ローカルルートグループとデバイスプールの関連付け （220 ページ）	システムの各デバイスがそのローカルルートグループを知るためにプロビジョニングされることを確認するためには、ローカルルートグループをデバイスプールに関連付けます。
Step 3	ローカルルートグループのルートリストへの追加 （220 ページ）	（**オプション**）ルートリストに追加できるローカルルートグループを設定します。ローカルルートグループを作成すると、システムはデバイスプール レベルのユーザに対して定義されたゲートウェイに発信コールをルーティングします。

ローカルルートグループの設定

（**省略可**）システムは、標準ローカルルートグループと呼ばれるデフォルトのローカルルートグループを提供しますが、追加のローカルルートグループを設定できます。追加のローカルルートグループを指定するには、次の手順を使用します。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートパターン（Route Pattern）]** を選択します。

Step 2 [行の追加（Add Row）] をクリックします。

Step 3 新しいローカルルートグループの名前と説明を入力します。

Step 4 [保存（Save）] をクリックします。

ローカルルートグループとデバイスプールの関連付け

発信側デバイスのデバイスプールの設定に基づいて、ローカルルートグループが既存のルートグループを使用するよう割り当てることができます。この設定により、異なるロケーションにある電話やその他のデバイスが単一セットのルートパターンを使用できますが、Unified Communications Manager が適切なゲートウェイを選択してコールをルーティングします。

システムの各デバイスがそのローカルルートグループを知るためにプロビジョニングされることを確認するためには、ローカルルートグループをデバイスプールに関連付けます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [デバイスプール（Device Pool）]** を選択します。

Step 2 検索条件を入力し、[検索（Find）] をクリックして、結果のリストからデバイスプールを選択します。

Step 3 [ローカルルートグループの設定（Local Route Group Settings）] 領域で、[標準ローカルルートグループ（Standard Local Route Group）] ドロップダウンリストからルートグループを選択します。

Step 4 [保存（Save）] をクリックします。

ローカルルートグループのルートリストへの追加

ルートリストに追加できるローカルルートグループを設定します。ローカルルートグループを作成すると、システムはデバイスプール レベルのユーザに対して定義されたゲートウェイに発信コールをルーティングします。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートリスト（Route List）]** を選択します。

Step 2 次のいずれかのオプションを選択します。

- [新規追加（Add New）] をクリックして、新しいルートリストを追加します。
- 既存のルートリストの設定を変更するには、[検索（Find）] をクリックし、結果のリストからルートリストを選択します。

[ルートリストの設定（Route List Configuration）] ウィンドウが表示されます。

Step 3 ルートリストにローカルルートグループを追加するには、[ルートグループの追加（Add Route Group）] ボタンをクリックします。

Step 4 **[ルートグループ（Route Group）]** ドロップダウンリストから、ルートリストを追加するローカルルートグループを選択します。標準ローカルルートグループの追加、または作成したカスタムローカルルートグループの追加ができます。

Step 5 **[保存（Save）]** をクリックします。

Step 6 **[設定の適用（Apply Config）]** をクリックします。

ルートグループの設定

システムが発信コール用ゲートウェイを選択するときの優先順位を示したルートグループを設定します。グループ内の任意のゲートウェイでコールを発信できるように、同様の特性を持つゲートウェイをグループ化するには、次の手順を使用します。ルートグループを設定したときに指定した順序で、システムは使用するゲートウェイを選択します。

1 つのデバイスを複数のルートグループに割り当てることができます。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）]** > **[ルート/ハント（Route/Hunt）]** > **[ルートグループ（Route Group）]** を選択します。

[ルートグループの設定（Route Group Configuration）] ウィンドウが表示されます。

Step 2 次のいずれかのオプションを選択します。

- 新しいルートグループを追加するには、[新規追加（Add New）] をクリックします。
- 既存のルートグループの設定を変更するには、[検索（Find）] をクリックし、結果のリストからルートグループを選択します。

[ルートグループの設定（Route Group Configuration）] ウィンドウが表示されます。

Step 3 [ルートグループの設定（Route Group Configuration）] ウィンドウで各フィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 4 [保存（Save）] をクリックします。

ルートリストの設定

一連のルートグループを特定し、優先順位を付けるには、ルートリストを設定します。Unified Communications Manager は、ルートリストの順序を使用して、発信コールに使用可能なデバイスを検索します。

ルートリストを設定すると、少なくとも 1 つのルートグループを設定する必要があります。ルートリストに含められるのは、ルートグループとローカルルートグループだけです。

（注） 発信コールがルートリストを介して送信される場合、ルートリストのプロセスは、発信デバイスをロックして、コールが完了する前にアラート メッセージが送信されないようにします。発信デバイスがロックされた後は、ハントリストが着信コールの追跡を停止します。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートリスト（Route List）]** を選択します。

Step 2 次のいずれかのオプションを選択します。

- 新しいルートリストを作成するには、[新規追加（Add New）] をクリックします。
- 既存のルートリストの設定を変更するには、[検索（Find）] をクリックし、結果のリストからルートリストを選択します。

Step 3 [ルートリストの設定（Route List Configuration）] ウィンドウで各フィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 4 ルートグループをルートリストに追加するには、[ルートグループの追加（Add Route Group）] ボタンをクリックします。

Step 5 [ルートグループ（Route Group）] ドロップダウンリストから、ルートリストに追加するルートグループを選択します。

Step 6 **[保存（Save）]** をクリックします。

Step 7 **[設定の適用（Apply Config）]** をクリックします。

ルートフィルタの設定

ルートフィルタは、コールの処理方法を決定するためにダイヤル数字列を使用します。ルートフィルタは、ワイルドカード@を含むルートパターンを設定するときにのみ適用されます。ルートパターンが@ワイルドカードを含む場合、Unified Communications Manager は、この手順で指定する番号計画に従ってコールをルーティングします。

ダイヤルプランインストーラを使用している場合、ルートフィルタは必須です。つまり、ダイヤルプランファイルをインストールして、その番号計画に基づいてルートパターンを設定します。ダイヤル プランを手動で設定する場合は、ルートプランの使用は任意です。

ダイヤル プランを手動で設定すると、@ワイルドカードを含むルートパターンがあるたびにルートフィルタを設定する必要があります。ルートパターンに@ワイルドカードが含まれていると、システムは、ルートフィルタで指定する番号計画に応じて、コールをルーティングします。

（注） コールルーティングを設定するときは、1 つのルートフィルタを多数のルートパターンに割り当てないでください。数百のルートパターンが関連付けられたルートフィルタを編集した場合、システム コアに発生します。これは、ルートフィルタを使用するすべてのルートパターンのコールルーティングの更新に新たなシステム処理が必要になるためです。重複するルートフィルタを作成し、1 つのルートフィルタを 250 を超えるルートパターンに関連付けないようにします。

手順

Step 1 Cisco Unified CM Administration から、[コールルーティング（Call Routing）] > [ルートフィルタ（Route Filter）] を選択します。

Step 2 [番号計画（Numbering Plan）] ドロップダウンリストからダイヤルプランを選択し、[次へ（Next）] をクリックします。

Step 3 [ルートフィルタ名（Route Filter Name）] フィールドに名前を入力します。

各ルートフィルタ名がルートプランに一意であることを確認します。

Step 4 ルートフィルタのタグと演算子を選択し、データを入力して、このルートフィルタ用の句を作成します。

使用可能なルートフィルタのタグの詳細については、「ルートフィルタタグ （224 ページ）」を参照してください。

（注） EXISTS、DOES-NOT-EXIST、NOT-SELECTED の演算子を使用するタグにはルートフィルタのタグ値を入力しないでください。

Step 5 ルートフィルタの演算子を選択し、該当する場合は、このルートフィルタのフレーズを作成するためにデータを入力します。

使用可能なルートフィルタの演算子の詳細については、「ルートフィルタの演算子 （225 ページ）」を参照してください。

Step 6 **[保存（Save）]** をクリックします。

Step 7 **[設定の適用（Apply Config）]** をクリックします。

ルートフィルタの設定項目

ルートフィルタは、特定のルートがローカルのルートデータベースに含めるように考慮されていないプロセスです。ルートパターンが設定されている場合にのみ適用されます。

ルートフィルタの設定に関する情報を次のトピックに示します。

ルートフィルタタグ

タグは、ルートフィルタのコア コンポーネントです。タグでは、ダイヤルされる数字列の一部に名前を適用しています。たとえば、NANP 番号 972-555-1234 は、LOCAL-AREA-CODE (972)、OFFICE-CODE (555)、および SUBSCRIBER (1234) ルートフィルタタグで構成されています。

ルートフィルタタグには、演算子が必要であり、フィルタに掛けるコールを決定するには、その他の値も必要な場合があります。

ルート フィルタ タグ フィールドの値には、ワイルドカード文字 X、*、#、[、]、-、^、および 0 ～ 9 の数字を使用できます。次の表の説明では、表記 [2-9] と XXXX を使用して、実際の数字を表しています。この表記では、[2-9] は、2 ～ 9 の範囲の任意の 1 桁の数字を表し、X は、0 ～ 9 の範囲の任意の 1 桁の数字を表します。したがって、「[2-9]XX の形式の 3 桁のエリア コード」という記述は、実際の数字 200 ～ 999、またはすべてのワイルドカード、または結果としてその範囲のパターンになる実際の数字とワイルドカードの任意の組み合わせを入力できるという意味です。

ルートフィルタタグは、[ルートフィルタの設定(Route Filter Configuration)] ウィンドウの [番号計画(Numbering Plan)] ドロップダウンリスト ボックスで選択する番号計画によって異なります。次の表に、北米計画番号のルートフィルタタグを示します。

表 *17:* ルートフィルタタグ

タグ	説明
AREA-CODE	[2-9]XX の形式のこの 3 桁のエリア コードは、長距離コールのエリア コードを指定します。
国番号	この 1 桁、2 桁、または 3 桁のコードは、国際コールの宛先国を指定します。
END-OF-DIALING	この 1 文字は、ダイヤルされた数字列の末尾を指定します。NANP 内でダイヤルされる国際番号には、# 文字がダイヤル終了信号として使用されます。
INTERNATIONAL-ACCESS	この 2 桁のアクセス コードは、国際ダイヤルを指定します。日本国内で発信するコールは、このコードに 01 を使用します。
INTERNATIONAL-DIRECT-DIAL	この 1 桁のコードは、直接ダイヤルされる国際コールを指定します。日本国内で発信するコールは、このコードに 1 を使用します。
INTERNATIONAL-OPERATOR	この 1 桁のコードは、オペレータ経由の国際コールを指定します。米国内で発信されるコールでは、このコードに 0 を指定します。
LOCAL-AREA-CODE	[2-9]XX の形式のこの 3 桁のローカル エリア コードは、10 桁のローカル コールのローカル エリア コードを指定します。
LOCAL-DIRECT-DIAL	この 1 桁のコードは、直接ダイヤルされるローカル コールを指定します。NANP コールでは、このコードに 1 を使用します。
LOCAL-OPERATOR	この 1 桁のコードは、オペレータ経由のローカル コールを指定します。NANP コールでは、このコードに 0 を使用します。

タグ	説明
LONG-DISTANCE-DIRECT-DIAL	この1桁のコードは、直接ダイヤルされる長距離コールを指定します。NANP コールでは、このコードに 1 を使用します。
LONG-DISTANCE-OPERATOR	この 1 桁または 2 桁のコードは、NANP 内のオペレータ経由の長距離コールを指定します。オペレータ経由のコールでは、このコードに 0 を使用し、オペレータにアクセスするには 00 を使用します。
NATIONAL-NUMBER	このタグは、国際コール用の数字列の中の、各国固有の部分を指定します。
OFFICE-CODE	このタグは、7 桁の電話番号の最初の 3 桁（[2-9]XX の形式）を指定します。
SATELLITE-SERVICE	この 1 桁のコードは、国際コール用の衛星接続にアクセスできるようにします。
SERVICE	この 3 桁のコードは、緊急用の 911、修理サービス用の 611、問い合わせ用の 411 を指定します。
SUBSCRIBER	このタグは、7 桁の電話番号の最後の 4 桁（XXXX の形式）を指定します。
TRANSIT-NETWORK	この 4 桁の値は、長距離通信事業者を識別します。 TRANSIT-NETWORK 値には、先行する 101 通信事業者アクセス コード接頭部を指定しないでください。詳細については、TRANSIT-NETWORK-ESCAPE を参照してください。
TRANSIT-NETWORK-ESCAPE	この 3 桁の値は、長距離通信事業者 ID に先行します。このフィールドの値には 101 が指定されています。TRANSIT-NETWORK-ESCAPE 値に、4 桁の通信事業者識別コードを指定しないでください。詳細については、TRANSIT-NETWORK を参照してください。

ルートフィルタの演算子

ルートフィルタタグの演算子は、そのタグに関連したダイヤル数字列の有無、さらに、場合によってはそのダイヤル数字列の内容に基づいて、コールがフィルタに掛けられるかどうかを決定します。演算子 EXISTS および DOES-NOT-EXIST は、ダイヤル数字列のその部分が存在するかどうかだけをチェックします。演算子 == は、実際にダイヤルされる数字を、指定された値またはパターンと突き合わせます。次の表に、ルートフィルタタグと共に使用できる演算子を示します。

表 *18* : ルートフィルタの演算子

演算子	説明
NOT-SELECTED	このタグに関連したダイヤル数字列に基づいて、コールをフィルタに掛けないことを指定します。 （注） 演算子が関連付けられるタグの有無によって、Cisco Unified Communications Manager がコールをルーティングすることが妨げられることはありません。

演算子	説明
EXISTS	このタグに関連したダイヤル数字列が検出されたときに、コールをフィルタに掛けることを指定します。 （注） Cisco Unified Communications Manager は、タグに関連付けられている任意の数字シーケンスがダイヤル数字列に含まれる場合のみ、コールをルーティングするかブロックします。
DOES-NOT-EXIST	このタグに関連したダイヤル数字列が検出されないときに、コールをフィルタに掛けることを指定します。 （注） Cisco Unified Communications Manager は、タグに関連付けられている任意の数字シーケンスがダイヤル数字列に含まれない場合のみ、コールをルーティングするかブロックします。
==	このタグに関連したダイヤル数字列が、指定された値と一致するときに、コールをフィルタに掛けることを指定します。 （注） Cisco Unified Communications Manager は、タグに関連付けられていて、関連するフィールドで指定された番号範囲内である任意の数字シーケンスがダイヤル数字列に含まれる場合のみ、コールをルーティングするかブロックします。

ルートフィルタの例

例 1：AREA-CODE と演算子 DOES-NOT-EXIST を使用するルートフィルタは、エリア コードを含まないすべてのダイヤル数字列を選択します。

例 2：AREA-CODE、演算子 ==、および項目 515 を使用するルートフィルタは、エリア コード 515 を含むすべてのダイヤル数字列を選択します。

例 3：AREA-CODE、演算子 ==、および項目 5[2-9]X を使用するルートフィルタは、520 ～ 599 の範囲のエリア コードを含むすべてのダイヤル数字列を選択します。

例 4：TRANSIT-NETWORK、演算子 ==、および項目 0288 を使用するルートフィルタは、通信事業者アクセス コード 1010288 を持つすべてのダイヤル数字列を選択します。

ルートパターンの設定

Unified Communication Manager は、ルートパターンを使用して、内部と外部のコールをルーティングまたはブロックします。ゲートウェイ、トランク、1 つ以上のルートグループを含むルートリストにルートパターンを割り当てることができます。

（注） ルートパターンでゲートウェイを直接指定することもできますが、ルートリストおよびルートグループを設定することを推奨します。このアプローチでは、コールルーティングの柔軟性に加え、拡張性を最大限に発揮します。

ルートパターンがゲートウェイまたはトランクに直接割り当てられている場合、そのゲートウェイまたはトランクをルートグループに関連付けることはできません。同様に、すでにルートリストのメンバーであるゲートウェイまたはトランクは、ルートパターンへの関連付けには使用できません。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）]** > **[ルート/ハント（Route/Hunt）]** > **[ルートパターン（Route Pattern）]** を選択します。

Step 2 次のいずれかの操作を行います。

- 新しいルートパターンを作成するには、[新規追加（Add New）] をクリックします。
- 既存のルートパターンを選択するには、[検索（Find）] をクリックします。

[ルートパターンの設定（Route Pattern Configuration）] ウィンドウが表示されます。

Step 3 [ルートパターン（ Route Pattern）] フィールドに、ダイヤル文字列が一致する必要がある番号パターンを入力します。

Step 4 [ゲートウェイ/ルート（Gateway/Route）] ドロップダウンリストから、このルートパターンに一致するコール送信先を選択します。

Step 5 [ルートパターンの設定（Route Pattern Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 6 [保存（Save）] をクリックします。

ルートパターンの設定項目

ルートパターンは、数字列（アドレス）とルートリストへのコールまたはゲートウェイへのコールを指定する関連番号操作セットから構成されます。

設定するルートパターンの種類の例を以下に示します。

- ルート パターンのワイルドカードと特殊文字 （228 ページ）
- ドットの前の数字を削除する例 （230 ページ）
- プレフィックス番号の例 （230 ページ）
- オンネットパターンとオフネットパターンの例 （230 ページ）
- ブロックおよびルートパターンの例 （231 ページ）

ルート パターンのワイルドカードと特殊文字

ルートパターンにワイルドカードおよび特殊文字を使用すると、1 つのルートパターンで、電話番号（アドレス）の範囲に一致させることができます。これらのワイルドカードと特殊文字を使用して、Unified Communications Manager が隣接システムに送信する前に番号を操作できるようにする指示も作成できます。

次の表に、Unified Communications Manager がサポートするワイルドカードと特殊文字を示します。

表 *19*：ワイルドカードおよび特殊文字

文字	説明	例
@	アットマーク（@）ワイルドカードは、国別番号計画のすべての番号に一致します。 各ルート パターンで、@ ワイルドカードは1 文字だけ使用できます。	ルートパターン9.@は、国別番号計画が認識するすべての電話番号をルーティングまたはブロックします。 @ ワイルドカードが含む、国別番号計画の番号のルート パターンの例を次に示します。 • [0] • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	X ワイルドカードは、0 ～ 9 の範囲にある数字の任意の 1 桁に一致します。	ルート パターン 9XXX は、9000 ～ 9999 の範囲のすべての数字をルーティングするか、またはブロックします。
!	感嘆符（!）ワイルドカードは、0 ～ 9 の範囲にある数字の 1 桁以上に一致します。	ルート パターン 91! は、910 ～ 919999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
?	疑問符（?）ワイルドカードは、直前の数字またはワイルドカード値の 0 回以上の繰り返しに一致します。 （注） 疑問符（??）ワイルドカードを使用した場合、2 つ目の疑問符は空の入力には一致しません。ルータパターンの例：*33X?*X?*X?#	ルート パターン 91X? は、91 ～ 919999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。

文字	説明	例
+	プラス記号（+）ワイルドカードは、直前の数字またはワイルドカード値の1回以上の繰り返しに一致します。	ルート パターン 91X+ は、910 ～ 9199999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
[ ]	角カッコ（[]）文字は、値の範囲を囲みます。	ルート パターン 813510[012345] は、8135100 ～ 8135105 の範囲のすべての数字をルーティングするか、またはブロックします。
-	ハイフン（-）文字は、角カッコと一緒に使用して値の範囲を示します。	ルート パターン 813510[0-5] は、8135100 ～ 8135105 の範囲のすべての数字をルーティングするか、またはブロックします。
^	ハット（^）文字は、角カッコと一緒に使用して値の範囲外を示します。この文字は、開始角カッコ（[）の直後に配置してください。 各ルート パターンで、^ 文字は 1 文字だけ使用できます。	ルート パターン 813510[^0-5] は、8135106 ～ 8135109 の範囲のすべての数字をルーティングするか、またはブロックします。
.	デリミタとして使用されるドット（.）文字は、Cisco Unified Communications Manager のアクセス コードをディレクトリ番号から分離します。 この特殊文字を、桁を無視する指定と一緒に使用すると、隣接システムに番号を送信する前に Cisco Unified Communications Manager のアクセス コードを削除できます。 各ルート パターンで、（.）文字は1文字だけ使用できます。	ルートパターン 9.@ は、最初の 9 を、国別番号計画に発信する Cisco Unified Communications Manager アクセス コードとして認識します。
*	アスタリスク（*）文字は、特別な着信番号の追加の桁として利用できます。	ルートパターン *411 を設定して、内部オペレータのディレクトリ案内の利用を可能にします。

文字	説明	例
#	シャープ（#）文字は、一般にダイヤルシーケンスの終了を特定します。 #文字がパターンの最後の文字になるようにします。	ルートパターン901181910555#は、国別番号計画内からダイヤルされる国際番号をルーティングまたはブロックします。末尾の5の後の#文字は、この桁をシーケンスの最後の桁として特定します。
\+	\+のように、バックスラッシュにプラス記号が続くと、国際番号用エスケープ文字+の設定を示します。	\+の使用は、国際番号用エスケープ文字+がワイルドカードではなく、ダイヤル可能な桁であることを意味します。

ドットの前の数字を削除する例

ルートパターンでのドット単位の数字の削除を使用する1つの例は、電話機のユーザが外線に接続するためにアクセスコードをダイヤルする場合です。北米では、通常、ユーザは9をダイヤルして外部回線にアクセスします。次のルートパターンを使用して指定できます。

- ローカルコール：**9.@** または **9.[2-9]XXXXXX**
- 国内コール：**9.1[2-9]XX**
- 国際コール：**9.011!#**

これらのパターンでは、9は外線用のアクセス コードであり、ドット（.）は、どれがネットワーク内の番号でどれが外線番号なのかを示すことによって、ルートパターンの形式指定を可能にする区切り文字です。システムがダイヤルされた番号をPSTNへ送信する場合は、PSTNがコールをルーティングできるように、[番号の削除（Discard Digits）] オプションを使用して、ドットの前の番号をダイヤルされた文字列から取り除くことができます。

プレフィックス番号の例

ルートパターンでプレフィックス番号を使用する例として、サイト間のオンネット ダイヤリングを設定する場合があります。ルートパターンを作成して、組織内のユーザがサイト間でコールする際に8+XXX-XXXX をダイヤルするように設定できます。オフネット コールの場合は、プレフィックス番号（8）を外して、新しいプレフィックス 1<area code> を追加することで、E.164 形式でコールを PSTN にルーティングできます。

オンネットパターンとオフネットパターンの例

[コールの分類（Call Classification）] フィールドを使用して、ルートパターンをオンネットまたはオフネットとして設定できます。コールを組織外に接続中であることをユーザに知らせるために2番目のダイヤルトーンを聞かせる場合は、コールをオフネットに分類できます。たとえば、ユーザが外線にダイヤルする際に9をダイヤルさせるルートパターンを作成し、それをオフネットのパターンとして分類した場合、システムは次のダイヤルトーンを鳴らします。

- 電話機がオフフック状態で、9をダイヤルする前のダイヤルトーン。

- 9をダイヤルした後に、公衆交換電話網（PSTN）番号にコールできる状態であることを示す、2 番目のダイヤルトーン。

このオプションを使用する場合は、必ず、[デバイスのオーバーライドを許可（Allow Device Override）] チェックボックスをオフにしてください。

ブロックおよびルートパターンの例

ブロックパターンとルートパターンを使用すると、ルーティングする必要のない発信コールまたは着信コールを阻止できます。ブロックパターンは、次のような目的に使用します。

- 特定のパターンをブロックする。たとえば、パターン 91900XXXXXXX をブロックすると、ユーザが 900 サービスに対してコールを発信するのを防ぐことができます。
- 特定の市外局番とロケーションに対するコールをブロックすることで、通信料金詐欺を防止する。

クラスタ全体の自動代替ルーティングの有効化

クラスタに対して自動代替ルーティング（AAR）を有効化します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 [サーバ（Server）] ドロップダウンリストでノードを選択します。

Step 3 [サービス（Service）] ドロップダウンリストから、[Cisco Call Manager] を選択します。

Step 4 [クラスタ全体のパラメータ（システム - CCM 自動代替ルーティング）（Clusterwide Parameters (System - CCM Automated Alternate Routing)）] 領域で、[自動代替ルーティングの有効化（Automated Alternate Routing Enable）] パラメータを [True] に設定します。

AAR グループの設定

自動代替ルーティング（AAR）を設定することで、ロケーションの帯域幅不足のためシステムがコールをブロックしたときに、PSTN またはその他のネットワークを通じてコールを自動的に再ルーティングすることができます。AAR を使用すると、発信者は電話を切って着信側をダイヤルし直す必要がなくなります。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [AARグループ（AAR Group）]** を選択します。

Step 2 次のいずれかのオプションを選択します。

- 新しい AAR グループを追加するには、[新規追加（Add New）] をクリックします。
- 既存の AAR グループの設定を変更するには、[検索（Find）] をクリックし、結果のリストから AAR グループを選択します。

[AAR グループの設定（AAR Group Configuration）] ウィンドウが表示されます。

Step 3 [名前（Name）] フィールドに、新しい AAR グループに割り当てる名前を入力します。

この名前には、最長 20 文字の英数字を指定でき、スペース、ピリオド（.）、ハイフン（-）、および下線文字（_）を任意に組み合わせることが可能です。

ウィンドウが更新され、その他のフィールドが表示されます。

Step 4 [AAR グループの設定（AAR Group Configuration）] ウィンドウの各フィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 5 [保存（Save）] をクリックします。

（注） （**オプション**）AAR がハントパイロットと連携できるようにするには、「ハントパイロットの設定タスクフロー （245 ページ）」を参照してください。

時間帯ルーティングの設定

（オプション）着信コールを受信するためにパーティションが利用可能となる時間帯を指定するスケジュールを作成します。

（注） 時間帯ルーティングは、メッセージ待機インジケータ（MWI）の代行に対しては機能しません。

手順

	コマンドまたはアクション	目的
Step 1	時間帯の設定 （233 ページ）	時間帯を定義するには、この手順を使用します。開始時刻および終了時刻を定義し、さらに年次カレンダーで指定日または曜日として繰り返し間隔を指定します。
Step 2	タイムスケジュールの設定（233 ページ）	スケジュールを作成するには、この手順を実行します。上記の手順で設定した時間帯は、このスケジュールの構成要素です。時間帯は、複数のスケジュールに割り当てることができます。

	コマンドまたはアクション	目的
Step 3	パーティションとスケジュールの関連付け（233 ページ）	パーティションとスケジュールを関連付けて、発信側デバイスが特定の時間帯にコールの完了を試みたときに検索する場所を決定します。

時間帯の設定

時間帯を定義するには、この手順を使用します。開始時刻および終了時刻を定義し、さらに年次カレンダーで指定日または曜日として繰り返し間隔を指定します。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [スケジュールの設定（Time Schedule）]** を選択します。

Step 2 [時間帯の設定（Time Period Configuration）] ウィンドウで各フィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 3 [保存（Save）] をクリックします。

タイムスケジュールの設定

スケジュールを作成するには、この手順を実行します。上記の手順で設定した時間帯は、このスケジュールの構成要素です。時間帯は、複数のスケジュールに割り当てることができます。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [スケジュールの設定（Time Schedule）]** を選択します。

Step 2 [スケジュールの設定（Time Schedule）] ウィンドウのフィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 3 [保存（Save）] をクリックします。

パーティションとスケジュールの関連付け

パーティションとスケジュールを関連付けて、発信側デバイスが特定の時間帯にコールの完了を試みたときに検索する場所を決定します。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [パーティション（Partition）]** を選択します。

Step 2 [スケジュール（Time Schedule）] ドロップダウンリストから、このパーティションに関連付けるスケジュールを選択します。
スケジュールでは、パーティションが着信コールの受信に利用可能となる時間を指定します。[なし（None）] を選択した場合は、パーティションが常にアクティブになります。

Step 3 [保存（Save）] をクリックします。

コールルーティングの制限

機能	制限事項
ルートフィルターの関連付け	コールルーティングを設定する場合、単一ルートフィルタを多くのルートパターンに割り当てないようにしてください。数百個のルートパターンが関連付けられているルートフィルタを編集しようとすると、システム コア クラッシュが発生する可能性があります。これは、ルートフィルタを使用するすべてのルートパターンのコールルーティングの更新に新たなシステム処理が必要になるためです。発生しないようにするには、重複するルートフィルタを作成します。
外部コール制御	外部コール制御によって、アジャンクトルートサーバは、Cisco Unified Routing Rules Interface を使用して Unified Communications Manager のコールルーティングを決定できます。外部コール制御を設定すると、Unified Communications Manager が、発信側および着信側の情報が入ったルート要求をアジャンクトルートサーバに発行します。そのサーバは、要求を受信し、適切なビジネスロジックを適用し、コールのルーティング方法と適用すべきその他のコール処理方法をお使いのシステムに指示するルート応答を返します。 詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「外部コール制御」の章を参照してください。

機能	制限事項
コール制御検出	コール制御検出を使用すると、Service Advertisement Framework（SAF）と呼ばれる Cisco IOS サービス ルーティング プロトコルに登録することによって、Unified Communications Manager クラスタがホストする DN 範囲を自動的に交換できます。SAF CCD によって、クラスタは、それぞれにホストされた DN 範囲をネットワークにアドバタイズし、ネットワーク内の他のコールエージェントによって生成されたアドバタイズメントにサブスクライブできます。 SAF CCD を使用することの主な利点は次のとおりです。 • 同じ SAF CCD ネットワークに参加するコールエージェント間でコールルーティング情報を自動的に配布でき、したがって新しいコールエージェントが追加されたり、コールエージェントに新しい DN 範囲が追加されたりした場合に設定作業が徐々に増大することがなくなります。 • 集中型ダイヤル プラン解決コントロール ポイントに依存しなくなります。 • 複数の Unified CM クラスタが組み合わせられた場合を含め、ルーティングが変更された場合に、コールエージェント間のコールルーティング情報が自動的に回復されます。 コール制御検出を設定するには、『*Cisco Unified Communications Manager* 機能設定ガイド』の「コール制御検出の設定」の章を参照してください。
ルートプランレポート	詳細なルートプランは、Cisco Unified CM Administration（[コールルーティング（Call Routing）] > [ルートプランレポート（Route Plan Report）]）の [ルートプランレポート（Route Plan Report）] ウィンドウで表示できます。ルーティング計画の報告により、ルーティング計画の一部または全部のリストを確認し、レポートのモード/ディレクトリ番号、パーティションまたはルーティングの詳細情報列の項目をクリックして、直接に関連する設定ウィンドウに移動します。 さらに、ルートプランレポートを使用してレポートデータを .csv ファイルに保存し、そのファイルを他のアプリケーションにインポートすることもできます。保存される .csv ファイルには、ウェブページより詳細な情報（電話機の電話番号、ルートパターン、パターン使用法、デバイス名、デバイスの説明など）が含まれます。

Dialed Number Analyzer によるトラブルシューティング

Dialed Number Analyzer は、Cisco Unified Communications Manager とともに、機能サービスの 1 つとしてインストールできます。このツールにより、Cisco Unified Communications Manager のダイヤルプラン設定を展開前にテストできます。また、このツールを使用して、展開後のダイヤルプランを分析することもできます。

ダイヤル プランが複雑になり、複数のデバイス、変換パターン、ルートパターン、ルートリスト、ルートグループ、発信側および着信側の変換、およびデバイスレベルの変換が関係すると、ダイヤル プランに誤りが含まれる場合があります。Dialed Number Analyzer を使用してダイヤル プランをテストするには、ダイヤルされた番号を入力に使用します。ダイヤルされた番号が分析され、コールの詳細が表示されます。その結果を使用してダイヤル プランを診断し、問題があれば特定し、ダイヤル プランを調整してから展開できます。

Dialed Number Analyzer のセットアップと使用の方法の詳細については、『*Cisco Unified Communications Manager Dialed Number Analyzer* ガイド』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

回線グループの設定

この章では、回線グループの追加または削除、または回線グループからの電話番号の追加または削除を行う方法について説明します。

詳細については、『*Cisco Unified Communications Manager* システム ガイド』の、ルートプランの理解に関するトピックを参照してください。

回線グループの設定について

Cisco Unified Communications Manager Administration で、**[コールルーティング（Call Routing）]** > **[ルート/ハント（Route/Hunt）]** > **[回線グループ（Line Group）]** メニューパスを使用して回線グループを設定します。

回線グループを使用して、電話番号を選択する順序を指定できます。Cisco Unified Communications Manager は、コール分配アルゴリズムと無応答（RNA）予約のタイムアウト設定に基づいて、回線グループのアイドル状態のまたは対応可能なメンバーにコールを分配します。

（注） 回線グループに属する DN へのコールは、ダイレクト コール ピックアップ機能を使用してピックアップできません。

ヒント メンバー（電話番号）のない空の回線グループを設定することはできますが、Cisco Unified Communications Manager はコールのルーティングに対してこの設定をサポートしません。回線グループにメンバーが含まれていない場合は、コールが空の回線グループにルーティングされたときにハントリストがハンティングを停止します。このような状況を回避するために、回線グループ内に 1 つ以上のメンバーが設定されていることを確認してください。

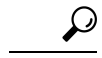
回線グループの設定に関するヒント

回線グループを設定する前に、1 つ以上の電話番号を定義する必要があります。

回線グループを設定または更新したら、その回線グループに対してメンバーを追加または削除することができます。

回線グループの削除

1つ以上のルート/ハントリストが参照している回線グループを削除できます。使用中の回線グループを削除しようとすると、Cisco Unified Communications Manager からエラー メッセージが表示されます。



ヒント 依存関係レコードは回線グループではサポートされていません。ベスト プラクティスとして、回線グループを削除する前に、必ず設定を確認してください。

回線グループの設定項目

フィールド	説明
回線グループ情報	
回線グループ名（Line Group Name）	この回線グループの名前を入力します。この名前には、最長 50 文字の英数字を指定でき、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて使用することが可能です。回線グループ名は、そのルートプランで一意の名前にしてください。 **ワンポイント アドバイス** 回線グループの名前は、簡潔で分かりやすいものにします。通常は、CompanynameLocationGroup の形式を使用すると、十分な詳細さでありながら、回線グループをすばやく簡単に識別できる簡潔さを実現できます。たとえば CiscoDallasAA1 は、ダラスにあるシスコ オフィスの Cisco Access Analog という回線グループを示します。
RNA 復帰タイムアウト（RNA Reversion Timeout）	コールに応答がない場合、かつ、1 つ目のハンド オプションである [次のメンバーを試し、続いてハントリスト内の次のグループを試します（Try next member; then, try next group in Hunt List）] が選択されている場合に、Unified Communications Manager がこの回線グループの次に応答可能なメンバーまたはアイドル状態のメンバー、または次の回線グループにコールを分配するまでの時間を、秒単位で入力します。[RNA 復帰タイムアウト（RNA Reversion Timeout）] は、回線グループ レベルですべてのメンバに適用されます。

フィールド	説明
[分配アルゴリズム（Distribution Algorithm）]	回線グループ レベルで適用する分配アルゴリズムを、ドロップダウン リスト ボックスのオプションから選択します。 • [上から（Top Down）]：この分配アルゴリズムを選択した場合、Unified Communications Manager は、回線グループ内でアイドル状態または応答可能である最初のメンバーから最後のメンバーまで順番にコールを分配します。 • [循環（Circular）]：この配布アルゴリズムを選択すると、Unified Communications Manager は、ルートグループ内でアイドル状態または応答可能である (n+1) 番目のメンバーから順番にコールを配布します。このとき、n 番目のメンバーは、リスト内で次の順番にあたり、アイドル状態であるかビジー状態ではあるものの「停止状態」「」ではないメンバーです。n 番目のメンバーがルートグループ内の最後のメンバーである場合、Unified Communications Manager は、そのルートグループの先頭からコールを配布します。 • [最長アイドル時間（Longest Idle Time）]：この分配アルゴリズムを選択した場合、Unified Communications Managerは、回線グループ内でアイドル状態が最も長いメンバーから最も短いメンバーの順番で、コールを配布します。 • [ブロードキャスト（Broadcast）]：この配布アルゴリズムを選択した場合、Unified Communications Managerは、回線グループ内のアイドル状態または応答可能であるすべてのメンバーに対して同時にコールを配布します。[ブロードキャスト（Broadcast）] 分配アルゴリズムを使用する場合の制約事項については、[選択された DN/ルート パーティション（Selected DN/Route Partition）] フィールドの説明にある「注」を参照してください。 デフォルト値は [最長アイドル時間（Longest Idle Time）] です。
ハント オプション（Hunt Options）	

フィールド	説明
無応答（No Answer）	特定の分配アルゴリズムで、コールが分配された回線グループのメンバーが応答しない場合に Unified Communications Manager が使用するハント オプションを選択します。このオプションはメンバー レベルで適用されます。ドロップダウンリストボックスのオプションから選択します。 • [次のメンバーを試し、続いてハントリスト内の次のグループを試します（Try next member; then, try next group in Hunt List）]：このハント オプションを選択した場合、Unified Communications Manager は、回線グループ内でアイドル状態または応答可能である最初のメンバーから最後のメンバーまで、順番にコールを分配します。分配がうまくいかない場合、Unified Communications Manager は、ハントリスト内の次の回線グループに対して分配を試行します。 • [次のメンバーを試しますが、次のグループに進みません（Try next member, but do not go to next group)]：このハント オプションを選択した場合、Unified Communications Managerは、回線グループ内でアイドル状態または応答可能である最初のメンバーから最後のメンバーまで、順番にコールを割り当てます。現在の回線グループ内で最後のメンバーに到達すると、Unified Communications Manager は試行を中止します。 • [残りのメンバーをスキップし、次のグループに直接進みます（Skip remaining members, and go directly to next group）]：このハント オプションを選択した場合、最初のメンバーの RNA 復帰タイムアウト値が経過したときに、Unified Communications Manager はその回線グループの残りのメンバーをスキップし、Unified Communications Manager はハントリスト内の次の回線グループに直接進みます。 • [追跡を停止します（Stop hunting）]：このハントオプションを選択した場合、Unified Communications Managerは、その回線グループ内の最初のメンバーにコールの分配を試みたがメンバーがコールに応答しなかったとき、ハントを停止します。
無応答時にハントメンバーを自動的にログアウト（Automatically Logout Hunt Member on No Answer）	このチェックボックスをオンにした場合、回線メンバーはハントリストから自動的にログオフします。回線メンバーを再度ログインさせるには、「HLOG」ソフトキーまたは PLK を使用します。

フィールド	説明
ビジー（Busy）	特定の分配アルゴリズムについて、コールが分配された回線グループのメンバーがビジー状態だった場合に Unified Communications Manager が使用するハント オプションを選択します。ドロップダウンリスト ボックスのオプションから選択します。 • [次のメンバーを試し、続いてハントリスト内の次のグループを試します（Try next member; then, try next group in Hunt List）]：このハント オプションを選択した場合、Unified Communications Manager は、回線グループ内でアイドル状態または応答可能である最初のメンバーから最後のメンバーまで、順番にコールを分配します。分配がうまくいかない場合、Unified Communications Manager は、ハントリスト内の次の回線グループに対して分配を試行します。 • [次のメンバーを試しますが、次のグループに進みません（Try next member, but do not go to next group)]：このハント オプションを選択した場合、Unified Communications Managerは、回線グループ内でアイドル状態または応答可能である最初のメンバーから最後のメンバーまで、順番にコールを割り当てます。現在の回線グループ内で最後のメンバーに到達すると、Unified Communications Manager は試行を中止します。 • [残りのメンバーをスキップし、次のグループに直接進みます（Skip remaining members, and go directly to next group）]：このハント オプションを選択した場合、Unified Communications Managerは、ビジー状態のメンバーにあたったときにその回線グループの残りのメンバーをスキップし、Unified Communications Managerはハントリスト内の次の回線グループに直接進みます。 • [追跡を停止します（Stop hunting）]：このハントオプションを選択した場合、Unified Communications Managerは、その回線グループ内でコールの分配を試みた際にビジー状態のメンバーに最初にあたった時点でハントを停止します。

フィールド	説明
使用不可（Not Available）	特定の分配アルゴリズムについて、コールが分配された回線グループのメンバーが使用不可だった場合に Unified Communications Manager が使用するハント オプションを選択します。[使用不可（Not Available）] 状態が発生するのは、該当する DN に関連付けられている電話機がいずれも登録されていない場合です。エクステンションモビリティが使用されていて、DN/ユーザがログインしていない場合にも [使用不可（Not Available）] 状態になります。ドロップダウンリストボックスのオプションから選択します。 • [次のメンバーを試し、続いてハントリスト内の次のグループを試します（Try next member; then, try next group in Hunt List）]：このハント オプションを選択した場合、Unified Communications Manager は、回線グループ内でアイドル状態または応答可能である最初のメンバーから最後のメンバーまで、順番にコールを分配します。分配がうまくいかない場合、Unified Communications Manager は、ハントリスト内の次の回線グループに対して分配を試行します。 • [次のメンバーを試しますが、次のグループに進みません（Try next member, but do not go to next group)]：このハント オプションを選択した場合、Unified Communications Managerは、回線グループ内でアイドル状態または応答可能である最初のメンバーから最後のメンバーまで、順番にコールを割り当てます。現在の回線グループ内で最後のメンバーに到達すると、Unified Communications Manager は試行を中止します。 • [残りのメンバーをスキップし、次のグループに直接進みます（Skip remaining members, and go directly to next group）]：このハント オプションを選択した場合、Unified Communications Managerは、使用不可のメンバーに最初にあたった時点でその回線グループの残りのメンバーをスキップし、Unified Communications Managerはハントリストの次の回線グループに直接進みます。 • [追跡を停止します（Stop hunting）]：このハント オプションを選択した場合、Unified Communications Managerは、その回線グループ内で分配を試みた際に使用不可のメンバーに最初にあたった時点でハントを停止します。
回線グループメンバー情報（Line Group Member Information）	
回線グループに追加するディレクトリ番号の検索（Find Directory Numbers to Add to Line Group）	

フィールド	説明
パーティション（Partition）	ドロップダウンリスト ボックスから、この回線グループのルート パーティションを選択します。デフォルト値は、<なし（None）> です。 [検索（Find）] をクリックすると、[使用可能DN/ルートパーティション（Available DN/Route Partition）] リスト ボックスに、選択したパーティションに属するすべての DN が表示されます。
次を含むディレクトリ番号（Directory Number Contains）	探しているディレクトリ番号に含まれる文字を入力し、[検索（Find）] ボタンをクリックします。入力した文字と一致する電話番号が [使用可能 DN/ルート パーティション（Available DN/Route Partition）] ボックスに表示されます。
使用可能 DN/ルート パーティション（Available DN/Route Partition）	[使用可能DN/ルートパーティション（Available DN/Route Partition）] リストボックスでディレクトリ番号を選択し、[回線グループに追加（Add to Line Group）] をクリックして、[選択されたDN/ルートパーティション（Selected DN/Route Partition）] リスト ボックスに追加します。
現在の回線グループメンバー（Current Line Group Members）	
共有回線 DN を使用したブロードキャストアルゴリズム（Broadcast algorithm with shared line DNs）	ディレクトリ番号の優先度を変更するには、[選択されたDN/ルートパーティション（Selected DN/Route Partition）] リストボックスでディレクトリ番号を選択します。リスト ボックスの右側にある矢印をクリックして、そのディレクトリ番号をリスト内で上下に移動します。 [選択されたDN/ルートパーティション（Selected DN/Route Partition）] リスト ボックスでディレクトリ番号の優先順位を逆にするには、[選択されたDN/ルートパーティションの順番を逆にする（Reverse Order of Selected DNs/Route Partitions）] をクリックします。 （注） DN およびルート パーティションを回線グループに追加する際は、共有回線である DN を、ブロードキャスト分配アルゴリズムを使用する回線グループに入れないでください。ブロードキャスト配信アルゴリズムを使用する回線グループのメンバーになっている DN を共有回線として設定したデバイスでは、Unified Communications Managerは、共有回線であるすべての DN を表示できません。
削除された DN/ルート パーティション（Removed DN/Route Partition）	[選択されたDN/ルートパーティション（Selected DN/Route Partition）] リストボックスでディレクトリ番号を選択し、[削除されたDN/ルートパーティション（Removed DN/Route Partition）] リスト ボックスに追加するには、2 つのリスト ボックスの間にある下向き矢印をクリックします。
ディレクトリ番号	

フィールド	説明
（この回線グループに現在属している DN のリスト）	特定のディレクトリ番号の [ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウに移動するには、このリストでディレクトリ番号をクリックします。 （注） 新しい回線グループを追加しても、回線グループを保存するまでは、このリストに表示されません。

回線グループへのメンバーの追加

新しい回線グループまたは既存の回線グループにメンバーを追加できます。次の手順では、既存の回線グループにメンバーを追加する方法を説明します。

始める前に

この手順を実行する前に、1つ以上の電話番号を定義する必要があります。

手順

Step 1 **[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [回線グループ（Line Group）]** を選択します。

Step 2 メンバーを追加する回線グループを見つけます。

Step 3 電話番号を検索する必要がある場合は、[パーティション (Partition)] ドロップダウンリストボックスからルートパーティションを選択し、[電話番号を含む (Directory Number Contains)] フィールドに検索文字列を入力して、[検索 (Find)] をクリックします。パーティションに属するすべての電話番号を検索するには、[Directory Number Contains] フィールドを空白のままにして [Find] をクリックします。

一致するディレクトリ番号のリストが [使用可能な DN/ルートパーティション (Available DN/Route Partition)] リストボックスに表示されます。

Step 4 [使用可能なDN/ルートパーティション（Available DN/Route Partition）] リスト ボックスで、追加するディレクトリ番号を選択し、[回線グループに追加（Add to Line Group）] をクリックして、そのディレクトリ番号を [選択されたDN/ルートパーティション（Selected DN/Route Partition）] リスト ボックスに移動します。この回線グループに追加するメンバーごとに、この手順を繰り返します。

Step 5 [選択された DN/ルートパーティション (Selected DN/Route Partition)] リストボックスで、この回線グループで新しい電話番号にアクセスする順序を選択します。順序を変更するには、電話番号をクリックし、リストボックスの右側にある上下の矢印を使用して、電話番号の順序を変更します。

Step 6 新しい電話番号を追加し、この回線グループの電話番号の順序を更新するには、[保存 (Save)] をクリックします。

回線グループからのメンバーの削除

新しい回線グループから、または既存の回線グループからメンバーを削除できます。次の手順では、既存の回線グループからの電話番号の削除について説明します。

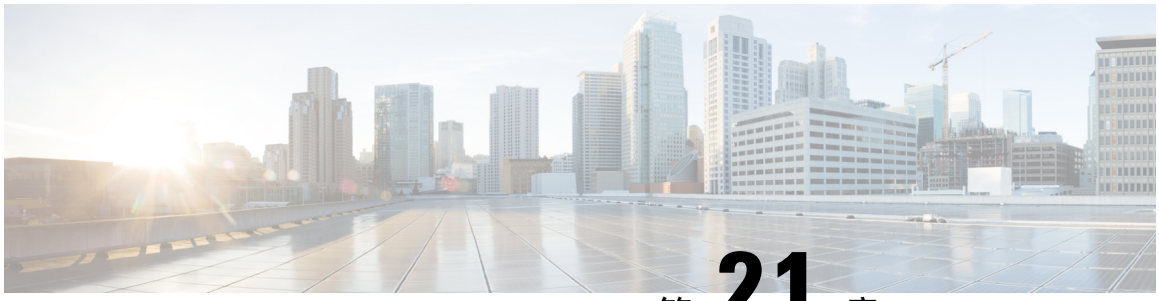
手順

Step 1 **[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [回線グループ（Line Group）]** を選択します。

Step 2 電話番号を削除する回線グループを見つけます。

Step 3 [選択されたDN/ルートパーティション（Selected DN/Route Partition）] リスト ボックスで、削除するディレクトリ番号を選択し、リストボックスの下にある下向き矢印をクリックして、[削除されたDN/ルートパーティション（Removed DN/Route Partition）] リスト ボックスにそのディレクトリ番号を移動します。この回線グループから削除するメンバーごとに、この手順を繰り返します。

Step 4 メンバーを削除するには、[保存 (Save)] をクリックします。



第 21 章

ハントパイロットの設定

ハントパイロットの概要

ハントパイロットは、数値またはパターンと、回線グループ内の電話のグループまたはディレクトリ番号へのコールをルーティングできる関連付けられた一連のディジット操作で構成されています。

ハントパイロットは、着信コールの優先順位を付けられたパス (回線グループ) の優先順位リストを使用して、ハントリストと連携します。ハントパイロットの DN にコールが発信されると、システムは、ハントリストで指定されている最初の回線グループにコールを提供します。最初の回線グループのいずれかの人がコールに応答しない場合、システムは、ハントリストで指定されている次の回線グループにコールを提供します。回線グループは、コールがグループ内の電話に配信される順序を制御します。回線グループは、特定の内線番号（通常は、IP Phone 内線番号またはボイスメール ポート）を指しています。回線グループは、コンピュータ テレフォニー インテグレーション（CTI）ポートと CTI ルートポイントを指すことができないため、ハントパイロットを使用して、Cisco Customer Response Solution（CRS）や IP 自動音声応答（IP IVR）などの CTI アプリケーションによって制御されるエンドポイントにコールを配信することはできません。

ハントパイロットは、回線グループとハントパイロットが異なるパーティションに存在する場合でも、割り当てられた回線グループのいずれかにコールを配信できます。ハントパイロットが分配するコールは、すべてのパーティションおよびコーリングサーチスペース制限を上書きします。

ハントパイロットの設定タスクフロー

システムのハントパイロットを設定するには、次のタスクを完了します。ハントパイロットは、回線グループ内の電話またはディレクトリ番号のグループにコールをルーティングするために使用できます。

手順

	コマンドまたはアクション	目的
Step 1	回線グループの設定 （246 ページ）	回線グループを作成して、複数の電話機が単一のディレクトリ番号 (DN) に送信されたコールに応答できるようにします。
Step 2	ハントリストの設定 （247 ページ）	回線グループの優先順位に従って、ハントリストを設定します。
Step 3	ハントパイロットの設定 （247 ページ）	ハントパイロット番号またはシステムがハントリストへのコールを指示するために使用するパターンを設定します。

回線グループの設定

回線グループを使用すると、1 つのディレクトリ番号に送信されるコールに複数の電話で応答できます。グループ内の電話に着信コールが分配される順序は、分配アルゴリズムが制御します。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [回線グループ（Line Group）]** を選択します。

Step 2 次のいずれかのオプションを選択します。

- 新しい回線グループを作成するには、[新規追加（Add New）] をクリックします。
- 既存の回線グループを選択するには、[検索（Find）] をクリックします。

Step 3 [回線グループ名（Line Group Name）] を入力します。

Step 4 [分配アルゴリズム（Distribution Algorithm）] フィールドで、コールの分配に使用するアルゴリズムのタイプを選択します。

Step 5 回線グループにディレクトリ番号を追加するには、[回線グループに追加する回線グループメンバー（Line Group Members to Add to Line Group）] セクションのフィールドを設定します。

a) 追加するディレクトリ番号が存在する [パーティション（Partition）] を選択します。
b) （オプション）[次を含むディレクトリ番号（Directory Number Contains）] フィールドを入力して、検索にフィルタを適用します。
c) [検索（Find）]をクリックします。指定したパーティションからのディレクトリ番号のリストがボックスに表示されます。
d) [使用可能なDN/ルートパーティション（Available DN/Route Partition）] リスト ボックスで、グループに追加する個別のディレクトリ番号を選択し、[回線グループに追加（Add to Line Group）] をクリックします。

Step 6 [回線グループの設定（Line Group Configuration）] ウィンドウで、残りのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 7 [保存（Save）] をクリックします。

ハントリストの設定

ハントリストは、回線グループの優先順位リストです。ハントリストを介してコールをルーティングする場合、システムは、ハントリストで定義されている順序で回線グループを使用します。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ハントリスト（Hunt List）]** を選択します。

Step 2 次のいずれかのオプションを選択します。

- **[新規追加（Add New）]**をクリックして、新しいルートリストを作成します。
- 既存のリストを選択するには、[検索（Find）] をクリックします。

Step 3 ハントリストの**名前**を入力します。

Step 4 ハントリストを登録する **Cisco Unified Communications Manager グループ**を選択します。

Step 5 [このハントリストを有効にする（Enable this Hunt List）] チェックボックスをオンにすると、[保存（Save）] をクリックしたときに即座にハントリストが有効になります。

Step 6 このハントリストがボイスメール用である場合は、[ボイスメール用（For Voice Mail Usage）] チェックボックスをオンにします。

Step 7 [保存（Save）] をクリックします。

Step 8 ハントリストへの回線グループの追加

a) [回線グループの追加（Add Line Group）] をクリックします。
b) [回線グループ（Line Group）] ドロップダウンリストから、ハントリストに追加する回線グループを選択します。
c) [保存（Save）] をクリックします。
d) さらに回線グループを追加するには、こらの手順を繰り返します。

ハントパイロットの設定

回線グループに対してコールをルーティングするためにシステムが使用するハントパイロット番号またはパターンを設定します。

（注） ハントパイロットで使用できるワイルドカードと特殊文字の詳細については、「ハントパイロットのワイルドカードと特殊文字 （248 ページ）」を参照してください。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ハントパイロット（Hunt Pilot）]** を選択します。

Step 2 次のいずれかのオプションを選択します。

- 新しいハントパイロットを作成するには、[新規追加（Add New）] をクリックします。
- 既存のハントパイロットを選択するには、[検索（Find）] をクリックします。

Step 3 [ハントパイロット（Hunt Pilot）] フィールドに、コールのルーティングに使用する番号またはパターンを入力します。

Step 4 [ハントリスト（Hunt List）] ドロップダウンから、ハントパイロット番号に一致するコールを送信するためのハントリストを選択します。

Step 5 [ハントパイロットの設定（Hunt Pilot Configuration）] ウィンドウで、残りのフィールドに入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 6 コール キューイングを有効化する場合は、[コールをキューイング（Queue Calls）] チェックボックスをオンにし、[キューイング（Queuing）] セクションのフィールドを設定します。

Step 7 発信者、接続先、着信者に適用するディジット 変換パターンを割り当てます。

Step 8 [保存（Save）] をクリックします。

ハントパイロットのワイルドカードと特殊文字

ルートパターンおよびハントパイロットでワイルドカードおよび特殊文字を使用すると、単一ルートパターンまたはハントパイロットをある範囲の番号（アドレス）と一致させることができます。また、これらのワイルドカードおよび特殊文字を使って指示を組み立てると、Cisco Unified Communications Manager が処理した番号を隣接システムに送信できます。

Cisco Unified Communications Manager がサポートするワイルドカードおよび特殊文字を次の表で説明します。

表 *20 :* ワイルドカードおよび特殊文字

文字	説明	例
@	アットマーク（@）ワイルドカードは、国別番号計画のすべての番号に一致します。 各ルート パターンで、@ ワイルドカードは1文字だけ使用できます。	ルート パターン9.@は、国別番号計画が認識するすべての電話番号をルーティングまたはブロックします。 @ワイルドカードが含む、国別番号計画の番号のルート パターンの例を次に示します。 • [0] • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	X ワイルドカードは、0 ～ 9 の範囲にある数字の任意の1桁に一致します。	ルート パターン 9XXX は、9000 ～ 9999 の範囲のすべての数字をルーティングするか、またはブロックします。
!	感嘆符（!）ワイルドカードは、0 ～ 9 の範囲にある数字の 1 桁以上に一致します。	ルート パターン 91! は、910 ～ 9199999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
?	疑問符（?）ワイルドカードは、直前の数字またはワイルドカード値の0回以上の繰り返しに一致します。 （注） 疑問符（??）ワイルドカードを使用した場合、2つ目の疑問符は空の入力には一致しません。ルータパターンの例：*33X?*X?*X?#	ルート パターン 91X? は、91 ～ 9199999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
+	プラス記号（+）ワイルドカードは、直前の数字またはワイルドカード値の1回以上の繰り返しに一致します。	ルート パターン 91X+ は、910 ～ 9199999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。

文字	説明	例
[ ]	角カッコ（[]）文字は、値の範囲を囲みます。	ルート パターン 813510[012345] は、8135100 ～ 8135105 の範囲のすべての数字をルーティングするか、またはブロックします。
-	ハイフン（-）文字は、角カッコと一緒に使用して値の範囲を示します。	ルート パターン 813510[0-5] は、8135100 ～ 8135105 の範囲のすべての数字をルーティングするか、またはブロックします。
^	ハット（^）文字は、角カッコと一緒に使用して値の範囲外を示します。この文字は、開始角カッコ（[）の直後に配置してください。 各ルート パターンで、^ 文字は 1 文字だけ使用できます。	ルート パターン 813510[^0-5] は、8135106 ～ 8135109 の範囲のすべての数字をルーティングするか、またはブロックします。
.	デリミタとして使用されるドット（.）文字は、Cisco Unified Communications Manager のアクセス コードをディレクトリ番号から分離します。 この特殊文字を、桁を無視する指定と一緒に使用すると、隣接システムに番号を送信する前に Cisco Unified Communications Manager のアクセス コードを削除できます。 各ルート パターンで、（.）文字は 1 文字だけ使用できます。	ルートパターン 9.@ は、最初の 9 を、国別番号計画に発信する Cisco Unified Communications Manager アクセス コードとして認識します。
*	アスタリスク（*）文字は、特別な着信番号の追加の桁として利用できます。	ルート パターン *411 を設定して、内部オペレータのディレクトリ案内の利用を可能にします。
#	シャープ（#）文字は、一般にダイヤル シーケンスの終了を特定します。 # 文字がパターンの最後の文字になるようにします。	ルート パターン 901181910555# は、国別番号計画内からダイヤルされる国際番号をルーティングまたはブロックします。末尾の 5 の後の # 文字は、この桁をシーケンスの最後の桁として特定します。

文字	説明	例
\+	\+のように、バックスラッシュにプラス記号が続くと、国際番号用エスケープ文字+の設定を示します。	\+ の使用は、国際番号用エスケープ文字 + がワイルドカードではなく、ダイヤル可能な桁であることを意味します。

ハントパイロットのパフォーマンスと拡張性

次のようなパフォーマンスおよび拡張性の制限が適用されます。

- 単一の Cisco Unified Communications Manager クラスタ は、最大で 15,000 個のハントリスト デバイスをサポートします。
- 単一の Cisco Unified Communications Manager サブスクライバは、ノードごとにコール キューイングが有効にされたハントパイロットを最大で 100 個サポートします。
- ハントリストデバイスは、各ハントリストに 10 台の IP 電話を含む 1500 のハントリスト、各ハントリストに 20 台の IP 電話を含む 750 のハントリストの組み合わせ、または同様の組み合わせにすることができます。

（注） コール カバレッジにブロードキャスト アルゴリズムを使用する場合、ハントリスト デバイスの数は、Busy Hour Call Attempts（BHCA）の数によって制限されます。ブロードキャスト アルゴリズムを使用して、10 台の電話機を含むハントリストまたはハント グループを指すハントパイロットに対して 10 回の BHCA を行うことは、10 回の BHCA を行う 10 台の電話機と同じです。

- コールキューを有効にしたハントパイロットの最大数は、Unified CM サブスクライバノードあたり 100 個です。キューで許可される発信者数が 32 に設定されている場合、ノードあたりのキュースロットの合計数（ノード上のコールキューが有効なすべてのハントパイロットの [キューで許可されている最大発信者数] を合わせた値）は、3200 に制限されます。各ハントパイロットのキューに同時に含められる発信者の最大数は 100 です。つまり、ハントパイロットごとにキューで許可される発信者数は 100 となり、ハントパイロットの最大数は 32 に減少します。すべてのハントリストに含まれるメンバの最大数は、コール キューイングが有効のときには変更されません。
- 設定できる各ハントパイロットのキュー内にある最大待ち時間は、0～3600 秒（デフォルトは 900）です。ハントリストの数が増えると、Unified Communications Manager サービスパラメータで指定するダイヤルプラン初期化タイマーを増やす必要があります。シスコでは、1500 個のハントリストを設定している場合、ダイヤル プラン初期化タイマーを 600 秒に設定することをお勧めします。
- コールキューを使用したブロードキャストアルゴリズムを使用する場合は、1 つの回線グループに対して 35 ディレクトリ番号が含まれないようにすることを推奨します。また、ブロードキャスト回線グループの数は、BHCC によって決まります。Unified CM システム内に複数の

ブロードキャスト回線グループがある場合、回線グループ内のディレクトリ番号の数は、35よりも少なくする必要があります。すべてのブロードキャスト回線グループの最繁時呼数（BHCA）の数が、1 秒あたり 35 コール セットアップを超えないようにします。

ハントパイロットの連携動作と制限

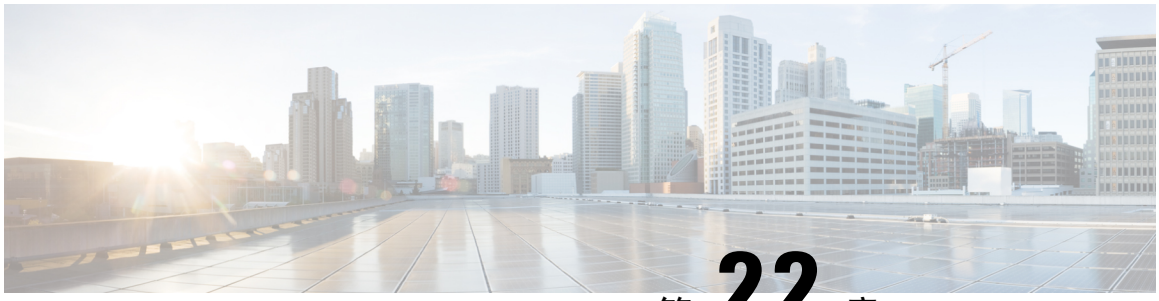
機能	連携動作と制限事項
ハント グループのシングル ナンバー リーチ	ハント グループが設定済みで、ハンド グループが指し示す 1 つ以上の電話番号でシングル ナンバー リーチ（SNR）が有効な場合には、ハント グループのすべてのデバイスがログインしない限り、SNR リモート接続先にコールが転送されません。 ハント グループ内の各デバイスについて、[電話の設定（Phone Configuration）] ウィンドウで [ハント グループにログイン（Logged into Hunt Group）] チェックボックスをオンにする必要があります。
コールキューイング	コールキューイングは、ハントパイロットのサブ機能です。コールキューが有効になっていて、特定のハントパイロットに着信コールの要求がコールを応答するために使用可能なハントメンバーの数を超える場合、システムは、ハントメンバーが応答できるようになるまで着信コールをキューにキューに転送します。待機中に発信者とその音楽を再生するように、保留中のアナウンスと音楽を設定することができます。 追加の設定の詳細については、『Cisco Unified Communications Manager 機能設定ガイド』の「コールキューイングの設定」の章を参照してください。
Unified Mobility	ハントパイロットで Unified Mobility デバイスを設定することはお勧めしません。

分配されないコール

表 *21 :* 循環アルゴリズムでコールが分配されない

制限事項	説明
BOT および TCT デバイスを含む回線グループの循環アルゴリズムで、コールが正しく配布されていません。	ログオフ状態にあるエージェントにコールが到達し、そのコールが **"Huntlogout"** タイプ以外の拒否タイプで拒否された場合。その後、インデックスが 1 つ増加しないため、前のコールに応答したのと同じエージェントにコールが送られます。

制限事項	説明
回線グループの循環アルゴリズムで、コールが正しく分配されません。	循環アルゴリズムでコールを分配している間、1 人のエージェントがビジー状態のとき、コールは次に使用可能なエージェントに到達します（つまり、ビジー状態のエージェントの代わりに次のエージェントがコールに応答します）。 （注） 複数のコールが同時に実行された場合、次に対応可能なエージェントがそのコールに応答します。



第 22 章

クラスタ間ルックアップ サービスの設定

ILS の概要

シスコ クラスタ間検索サービス（ILS）を使用すると、データを共有するリモート Cisco Unified Communications Manager クラスタで構成されるマルチクラスタ ネットワークを簡単に作成できます。

ILS を使用すると、管理者がクラスタ間の接続を手動で設定する必要がなくなります。ハブクラスタで ILS を設定したら、新しいクラスタで ILS を有効にし、新しいクラスタを既存のハブに向けることによって、新しいクラスタに接続できます。ILS はクラスタを自動的に接続し、両方のクラスタがより大規模な ILS ネットワークのトポロジを認識できるようにします。

ILS ネットワークコンポーネント

ILS ネットワークは次のコンポーネントで構成されます。

- **ハブクラスタ**：ハブクラスタは、自動メッシュ機能を使用して ILS ネットワークのバックボーンを形成し、他のハブクラスタとのフルメッシュトポロジを作成します。ハブクラスタは、さまざまな機能のために ILS ネットワーク全体で情報をリレーおよび共有します。
- **スポーク クラスタ**：スポーク クラスタはそれぞれのローカルのハブ クラスタにのみ接続し、他のハブ クラスタやスポーク クラスタに直接接続することはありません。スポーククラスタは、ローカルハブに依存して、ネットワーク全体で情報を共有およびリレーします。
- **グローバルダイヤルプランのインポートされたカタログ**：このオプションのコンポーネントは、グローバル ダイヤル プラン レプリケーションが設定されており、Cisco TelePresence Video Communications Server またはサードパーティのコール制御システムと相互運用している場合に適用されます。他のシステムからエクスポートされた CSV ファイルからディレクトリ URI または +E.164 番号のカタログを手動でインポートすると、ILS ネットワーク内のユーザが別のシステムのユーザにコールできるようになります。

クラスタビュー

ILSのリモートクラスタビュー機能を使用して、ネットワークをマッピングすることができます。各クラスタは、ピア情報ベクターと呼ばれる更新メッセージを交換します。これは、ネットワーク内の各クラスタのステータスをリモート クラスタに通知するものです。更新メッセージには、ネットワーク内の既知のクラスタに関する次の情報が含まれます。

- クラスタ ID
- パブリッシャーのピア Id
- クラスタの説明とバージョン
- ホストの完全修飾ドメイン名（FQDN）を指定します。
- ILS がアクティブ化されているクラスタ ノードの IP アドレスとホスト名

機能サポート

グローバルダイヤルプランレプリケーションやエクステンションモビリティローミングなどの機能は、ILS に依存して、クラスタがダイヤルプラン情報を共有するクラスタ間ネットワークを作成します。これにより、ビデオコール、URI ダイヤリング、およびクラスタ間モビリティを使用してクラスタ間コールネットワークを設定できます。

ILSは、imandプレゼンスの中央クラスタを複数のテレフォニークラスタに接続している場合に、IM and プレゼンスサービスの集中展開によっても使用されます。ILS は、IM and プレゼンス中央クラスタとテレフォニークラスタ間の接続を作成するために使用されます。

ILS ネットワーキング キャパシティ

ILS ネットワークを計画する際に念頭に置くべき推奨キャパシティは以下のとおりです。

- ILS ネットワーキングは最大 10 個のハブ クラスタをサポートしており、ハブあたりのスポーク クラスタ数は 20 個であるため、合計で最大 200 個のクラスタを使用できます。ハブとスポークの組み合わせによるトポロジは、各クラスタ内で多数の TCP 接続が作成されるのを回避するために使用します。
- ハブ クラスタとスポーク クラスタを最大数まで、またはそれを超えて使用すると、パフォーマンスに影響が出る可能性があります。1 つのハブに多数のスポーク クラスタを追加すると余分な接続が作成され、メモリまたは CPU の処理量が増加する可能性があります。1 つのハブクラスタに接続するスポーククラスタは 20 個以下にすることを推奨します。
- ILS ネットワーキングは、追加の CPU 処理をシステムに追加します。CPU 使用率と同期時間は、クラスタ全体で同期されているレコードの数によって異なります。ハブアンドスポークトポロジを計画する場合は、ハブクラスタのCPUが負荷を処理するように設定されていることを確認します。

（注） これらの推奨事項は、システムテストに基づいており、リソース使用率を考慮しています。システムでは、これらの推奨事項を超えないようにすることはできませんが、リソースの過大な負荷にさらされるリスクがあります。最適なパフォーマンスを得るには、上記のキャパシティを推奨します。

ILS の設定タスクフロー

ILS ネットワークを設定するには、次のタスクを実行します。

始める前に

どのクラスタがハブクラスタであり、スポーククラスタになるかを把握できるように、ILS トポロジを計画してください。

手順

	コマンドまたはアクション	目的
Step 1	クラスタ ID の設定 （257 ページ）	ILS ネットワーク内の各クラスタには、一意のクラスタ ID が必要です。
Step 2	ILS の設定 （258 ページ）	ネットワークのさまざまなクラスタで ILS を設定し、アクティブにします。
Step 3	ILS の実行状態の確認 （259 ページ）	ILS ネットワークが実行中であることを確認します。
Step 4	リモート クラスタ ビューの設定（259ページ）	ILS ネットワークのリモート クラスタ ビューを設定します。

クラスタ ID の設定

ILS ネットワーク内の各クラスタには、一意のクラスタ ID が必要です。リモートクラスタがクラスタ ID のデフォルトの**StandAloneCluster**値を保持している場合、ILS は機能しません。

手順

Step 1 パブリッシャノードで Cisco Unified CM Administration にログインします。

Step 2 **[システム（System）]**>**[エンタープライズパラメータ（Enterprise Parameters）]** と選択します。

Step 3 クラスタ**ID**の値を、クラスタを一意に識別する値に設定します。

Step 4 [保存（Save）] をクリックします。

Step 5 各クラスタのパブリッシャノードで、この手順を繰り返します。

ILS の設定

ネットワーク内のクラスタ間検索サービス(ILS)をアクティブ化して設定するには、次の手順を実行します。

（注） 設定する最初のクラスタは、ハブクラスタである必要があります。

手順

Step 1 パブリッシャノードで Cisco Unified CM Administration にログインします。

Step 2 **[拡張機能（Advanced Features）] > [ILS設定（ILS Configuration）]** を選択します。

Step 3 [ロール（Role）] ドロップダウンリストボックスから、設定するクラスタのタイプに応じて、[ハブクラスタ（Hub Cluster）] または [スポーククラスタ（Spoke Cluster）] を選択します。

Step 4 グローバル ダイヤル プラン レプリケーションを有効化する場合は、[リモートクラスタとグローバルダイヤルプランレプリケーションデータを交換（Exchange Global Dial Plan Replication Data with Remote Clusters）] チェックボックスをオンにします。

（注） URI パターン（`user@domain`）をアドバタイズするときは、[SIPプロファイルの設定（SIP Profile Configuration）] ウィンドウで、[ダイヤル文字列の解釈（Dial String Interpretation）] フィールドが [常にすべてのダイヤル文字列をURIアドレスとして処理（Always treat all dial strings as URI addresses）] に設定されていることを確認します。これは、デバイスがディレクトリ番号パターンとしてユーザ セクションの数字のみを使用して URI 学習パターンにダイヤルするのを防ぐことが目的です。その代わりに、ILS を介して、ユーザ セクションのテキスト文字列を使用して URI パターンのみをアドバタイズすることもできます。

Step 5 ネットワーク内のさまざまなクラスタ間で [ILS認証の詳細（ILS Authentication Details）] を設定します。

- TLS 認証の場合は、[TLS証明書の使用（Use TLS Certificates）] チェックボックスをオンにします。このオプションを選択する場合、クラスタ内のノード間で CA 署名付き証明書も交換する必要があります。
- パスワード認証（TLS を使用するかどうかに関係なく）については、[パスワードの使用（Use Password）] チェックボックスをオンにして、パスワードの詳細を入力します。

Step 6 [保存（Save）] をクリックします。

Step 7 [ILSクラスタ登録（ILS Cluster Registration）] ポップアップで、登録の詳細を設定します。

a) [登録サーバ（Registration Server）] テキスト ボックスに、このクラスタに接続するハブ クラスタのパブリッシャノードの IP アドレスまたは FQDN を入力します。これがネットワーク内の最初のハブ クラスタであれば、このフィールドを空白のままにしておくことができます。
b) [このクラスタにあるパブリッシャでクラスタ間検索サービスをアクティブ化（Activate the Intercluster Lookup Service on the publisher in this cluster）] チェックボックスがオンになっていることを確認します。
c) [OK] をクリックします。

Step 8 ILS ネットワークに追加する各クラスタのパブリッシャノードでこの手順を繰り返します。新しいクラスタをハブまたはスポーククラスタとして追加します。

（注） 設定した同期値によっては、クラスタ情報がネットワーク全体に伝播する間に遅延が生じることがあります。

クラスタ間で Transport Layer Security（TLS）認証を使用するには、ILS ネットワークの各クラスタのパブリッシャノード間で、Tomcat 証明書を交換する必要があります。Cisco Unified オペレーティング システムの管理から、証明書の一括管理機能を使用して、以下を行います。

- 証明書を各クラスタのパブリッシャノードから中央の場所にエクスポートします
- エクスポートされた証明書を ILS ネットワークに統合します
- ネットワークの各クラスタのパブリッシャノードに証明書をインポートします

詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の「証明書の管理」の章を参照してください。

ILS の実行状態の確認

ILS ネットワークが実行中であることを確認します。

手順

Step 1 任意のテレフォニー クラスタでパブリッシャノードにログインします。

Step 2 Cisco Unified CM Administration から、**[詳細機能（Advanced Features）] > [ILS設定（ILS Configuration）]** を選択します。

Step 3 [ILSクラスタとグローバルダイヤルプランインポート済みカタログ（ILS Clusters and Global Dial Plan Imported Catalogs）] セクションをオンにします。ILS ネットワーク トポロジが表示されます。

リモート クラスタ ビューの設定

ILS ネットワークのリモートクラスタビューを設定するには、次の手順を実行します。

手順

Step 1 Cisco Unified CM Administration で、**[高度な機能（Advanced Features）]** > **[クラスタビュー（Cluster View）]** を選択します。

Step 2 **[リモートクラスタの検索と一覧表示]** ウィンドウで、以前作成したリモートクラスタを選択します。

Step 3 このウィンドウから、クラスタ間のエクステンション モビリティ、TFTP、RSVP エージェントといったサービスをリモート クラスタ用に設定できます。

Step 4 [保存（Save）] をクリックします。

ILS の連携動作および制限

ILS の連携動作

表 *22 : ILS* の連携動作

機能	連携動作
クラスタの検出	ILS のクラスタ検出を使用すると、管理者がそれらのクラスタ間の接続を手動で設定しなくても Cisco Unified Communications Manager はリモート クラスタの詳細を動的に学習できます。 ILS ネットワークの各クラスタは更新メッセージをやり取りします。これはピア情報ベクターと呼ばれ、ネットワーク内の各クラスタのステータスをリモートクラスタに知らせることを目的としています。更新メッセージには、ネットワーク内の既知のクラスタに関する次の情報が含まれます。 • クラスタ ID • クラスタの説明とバージョン • ホストの完全修飾ドメイン名 • ILS がアクティブ化されているクラスタ ノードの IP アドレスとホスト名 **[詳細機能（Advanced Features）]** > **[クラスタビュー（Cluster View）]** を選択すると、ILS クラスタ検出機能が Cisco Unified CM Administration で表示できるリモート クラスタのリストを自動的に読み込みます。このウィンドウから、リモート クラスタの Extension Mobility Cross Cluster、TFTP、RSVP エージェントなどのサービスを設定できます。 （注） [クラスタビュー（Cluster View）] に表示されるリモート クラスタの完全修飾ドメイン名には、ILS 検出で解決可能な DNS を指定する必要があります。

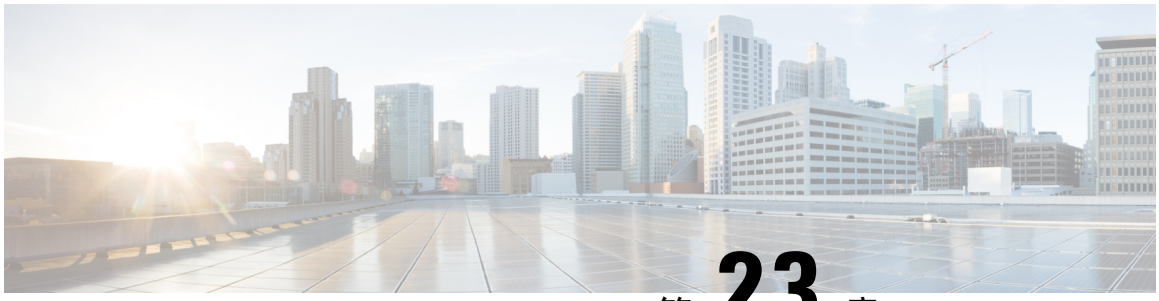
機能	連携動作
グローバル ダイヤル プラン レプリケーション	ILS ネットワークでグローバル ダイヤル プラン レプリケーションが有効な場合、ILS ネットワーク内のリモート クラスタは次のデータを含め、グローバル ダイヤル プラン データを共有します。 • ディレクトリ URI • 代替番号 • 代替番号パターン • ルート文字列 • PSTN フェールオーバー番号
着信コール	ILS ベースのネットワークで、発信者番号に基づいて着信コールをブロックするには、SIP ルートパターンのパーティションを発信者の CSS に含める必要があります。たとえば、コールが SIP トランクから発信される場合、SIP トランク受信 CSS には sip ルートパターンのパーティションが含まれている必要があります。

ILS の制限

表 *23 : ILS* の制限

制限事項	説明
ILS サービス	ILS サービスは、Unified Communications Manager のパブリッシャノードでのみ動作します。
クラスタ	ハブ クラスタは複数のスポークを持つことができますが、スポーク クラスタは 1 つのハブ クラスタしか持つことができません。
ILS ネットワーク	サードパーティ コール制御システムを ILS ネットワークに接続することはできません。
クラスタインポート	サードパーティのカタログは、ハブ クラスタにのみインポートできます。
重複した URI	取得した ILS クラスタに、別のリモートクラスタからの重複した Uri が含まれている場合、その URI にコールが配置されると、その uri が取得されてデータベースに挿入されているクラスタにルーティングされます。
データベースの複製ステータス	グローバルダイヤルプランデータは ILS ネットワーク上で正常に交換されますが、ILS 受信クラスタはデータベースレプリケーションステータスを完了するまで、学習した情報をデータベースに書き込みません。

制限事項	説明
インポート	インポートするサードパーティのディレクトリ URI およびパターンでは、そのCSVファイル形式が、管理ウィンドウのサンプルファイルが示すような正確なシンタックスと一致する必要があります。一致しない場合は、インポートに失敗します。
ILS ハブ	ILS ネットワークに追加のハブクラスタを追加するときは、プライマリ ILS ハブノードで、次の条件が満たされていることを確認します。 • クラスタ ID が ILS クラスタ内のすべてのハブノードで一意である。 • 完全修飾ドメイン名（FQDN）が設定されている。 • UDS および EM サービスが、ILS クラスタのすべてのハブノードで動作している。 • DNS プライマリと逆引きの名前解決が適切に機能している。 • 統合された Tomcat 証明書をすべてのハブノードからインポートする。 条件が満たされない場合は、クラスタの再起動やエラーの修正を行っても、[リモートクラスタの検索と一覧表示（Find and List Remote Clusters）] ウィンドウに「バージョン」情報が表示されません。これを回避するには、ハブクラスタをILSネットワークから削除し、上記の条件を満たした後に、ILSネットワークに再度追加します。



第 23 章

グローバルダイヤルプランレプリケーションの設定

グローバル ダイヤル プラン複製の概要

グローバル ダイヤル プラン レプリケーションを使用すると、URI ダイヤリング、エンタープライズ番号、または E.164 番号のいずれかをダイヤリングに使用するビデオコールによって、クラスタ間 VoIP ネットワークを簡単にセットアップできます。

グローバルダイヤルプランレプリケーションでは、ILS ネットワーク内のリモートクラスタにグローバルダイヤルプランデータ要素を複製することによって、Cisco Intercluster Lookup サービスを活用します。ILS ネットワーク内の各クラスタは、ホームクラスタのルート文字列とともに、他のクラスタのグローバルダイヤルプラン要素を学習します。

ILS 経由のグローバルなアドバタイズ

グローバルダイヤルプランレプリケーションは、次のダイヤルプラン要素を ILS ネットワークにアドバタイズし、リモートクラスタにこのデータを複製します。

- **ディレクトリ URI**：ローカルクラスタで、電子メール形式のディレクトリ URI（alice@cisco.com など）をプロビジョニングします。URI ダイヤリングは、ユーザ中心のコールを発信する方法を提供します。グローバルダイヤルプランレプリケーションでは、ディレクトリ Uri のローカルカタログを ILS ネットワーク内の他のクラスタにアドバタイズして、クラスタ間 URI ダイヤリングを有効にすることができます。
- **エンタープライズおよび E.164 代替番号**: 代替番号は、先頭の番号の指示が付いたマスクを元の電話番号に適用することによって作成される元の内線番号のエイリアスです。代替番号は、ILS ネットワーク内のどこからでもダイヤルできます。代替番号には2つのタイプがあります。ローカルクラスタで代替番号をプロビジョニングし、各番号を ILS ネットワークにアド

バタイズするか、または代替番号の範囲をまとめたアドバタイズされた番号パターンを設定して、ILS ネットワークにパターンをアドバタイズすることができます。

- **アドバタイズされたパターン**：アドバタイズされたパターンは、エンタープライズ代替番号または E.164 代替番号の範囲を要約したものです。リモートクラスタにデータベーススペースを保存するために、個々の代替番号ではなく、ILS ネットワーク全体でパターンを複製できます。アドバタイズされたパターンは、ILS ネットワーク内のリモートクラスタからのみ使用されます。ローカルコールをルーティングするためにこれらのパターンを使用することはできません。

- **PSTN フェールオーバー番号**：このオプションを使用すると、エンタープライズ代替番号または E.164 代替番号を PSTN フェールオーバー番号として割り当てることができます。グローバルダイヤルプラン要素へのコールルーティングが VoIP チャネル経由で失敗した場合、フェールオーバー番号によって代替ルーティング方式が提供されます。リモートクラスタでは、適切なゲートウェイに PSTN フェールオーバーをルーティングするルートパターンを設定する必要があります。

- **ルート文字列**：各クラスタには、グローバル ダイヤル プラン カタログと共に複製されるルート文字列があります。ルート文字列は、ディレクトリ URI または代替番号のホームクラスタを識別します。クラスタ間コールの場合は、ルート文字列をそのホームクラスタにルーティングする各リモートクラスタで SIP ルートパターンを設定する必要があります。

- **学習されたグローバル ダイヤル プラン データ**：複製されたデータが ILS ネットワーク内のすべてのクラスタに到達するように、各クラスタは、ローカルにプロビジョニングされたグローバル ダイヤル プラン データを、他のクラスタから学習したカタログとともに複製します。

- **インポートされたグローバル ダイヤル プラン データ**：Cisco Unified Communications Manager を Cisco TelePresence Video Communications Server またはサードパーティのコール制御システムと相互運用する場合は、相手のシステムからグローバル ダイヤル プラン データを csv ファイルにエクスポートし、その csv ファイルを ILS ネットワーク内のハブ クラスタにインポートします。グローバルダイヤルプランレプリケーションは、インポートしたカタログを ILS ネットワーク内の他のクラスタに複製します。これにより、他のシステムに登録されているディレクトリ Uri と代替番号にコールを発信することができます。

グローバルダイヤルプランマッピングの例

次に、電話内線番号4001にマッピングされるグローバルダイヤルプランデータ要素の例を示します。コールルーティングが正しく設定されていることを前提として、これらの番号のいずれかをダイヤルすると内線番号4001が鳴ります。

- エンタープライズ代替番号：番号マスク 5XXXX が内線 4001 に適用され、エンタープライズ代替番号 54001 が作成されます。

- E.164 代替番号：番号マスク 1972555XXXX が内線 4001 に適用され、+E.164 代替番号 19725554001 が作成されます。

- PSTN フェールオーバー：エンタープライズ代替番号または +E.164 代替番号を PSTN フェールオーバーとして割り当て、適切なゲートウェイにコールをルーティングします。

- アドバタイズされたパターン：パターン 54XXX を使用して、54000 ～ 54999 の範囲のすべてのエンタープライズ代替番号を集約できます。エンタープライズ代替番号と +E.164 代替番号用にパターンを作成できます。
- ディレクトリ URI：alice@cisco.com

（注） ディレクトリ URI は、電話番号またはエンドユーザに割り当てることができます。エンドユーザに関連付けられたディレクトリ URI はユーザのプライマリ内線番号（ディレクトリ番号）にも関連付けられ、プライマリ内線番号が割り当てられている場合はその内線番号を呼び出します。

URI ダイヤル

URI ダイヤリングはグローバル ダイヤル プラン レプリケーションのサブ機能であり、発信者がディレクトリ URI をダイヤル文字列として使用してコールを発信できるようにします。ディレクトリ URI は、電子メールアドレスのように見える英数字の文字列です(たとえば、alice@cisco.com)。

URI は電子メールアドレスに似ていますが、ディレクトリ URI はルーティング可能なエンティティではありません。ローカルコールの場合、ディレクトリ URI が発信者のコーリングサーチスペース内のパーティションにある場合に限り、そのディレクトリ URI に対するコールをルーティングできます。クラスタ間コールの場合、システムはグローバルダイヤルプランレプリケーションで複製されたクラスタルート文字列をプルし、SIP ルートパターンをルート文字列と照合しようとします。

ディレクトリ URI のタイプ

ディレクトリ URI には次の2つのタイプがあり、ディレクトリ URI のプロビジョニング方法によってタイプが決定されます。

- ユーザベースの URI：このディレクトリ URI は、[エンドユーザの設定（End User Configuration）] でユーザに割り当てられます。これらの URI はすべて、ローカルのディレクトリ URI パーティションに自動的に割り当てられます。これは、ローカルにある削除できないパーティションです。ユーザにプライマリ内線番号も設定されている場合、URI はその内線番号のプライマリ URI として [電話番号の設定（Directory Number Configuration）] にも表示されます。
- 回線ベースの URI：[電話番号の設定（Directory Number Configuration）] ウィンドウで、1 つの電話番号に最大 5 個のディレクトリ URI を直接割り当てることができます。これらの URI には、任意のローカルパーティションを割り当てることができます。

Directory URI の形式

ディレクトリ URI は、@記号で区切られたユーザとホストアドレスで構成される英数字の文字列です。

Cisco Unified Communications Manager は次のディレクトリ URI の形式をサポートしています。

- user@domain（例：joe@cisco.com）
- user@ip_address（例：joe@10.10.10.1）

システムはディレクトリ URI のユーザ部分（@ 記号の前の部分）では次の形式をサポートします。

- 使用できる文字は次のとおりです。a ～ z、A ～ Z、0 ～ 9、!、$、%、&、*、_、+、~、-、=、?、、‘、 、、 .、/、(および)。
- ユーザ部分は最大 47 文字までです。
- ディレクトリ URI がデータベースに保存されている場合、Cisco Unified Communications Manager は、次の文字にパーセント エンコーディングを自動的に適用します。

  # % ^ ` { } | \ : ” < > [ ] \ ‘ およびスペース。

（注） デフォルトでは、ディレクトリ URI のユーザ部分で大文字と小文字が区別されます。[URI検索ポリシー（URI Lookup Policy）] エンタープライズパラメータを編集することで、ユーザの部分で大文字と小文字を区別しないように編集できます。

パーセントエンコーディングを適用すると、ディレクトリ URI の桁数が増えます。たとえば、joe smith#@cisco.com（20 文字）をディレクトリ URI として入力した場合、Unified Communications Manager は、joe%20smith%23@cisco.com（24 文字）としてディレクトリ URI をデータベースに保存します。データベースの制限により、[ディレクトリURI（Directory URI）] フィールドの最大長は 254 文字となります。

Cisco Unified Communications Manager は、ディレクトリ URI のホスト部分（@ 記号の後の部分）で次の形式をサポートしています。

- IPv4 アドレスまたは完全修飾ドメイン名をサポートします。
- 使用可能な文字は、英数字、ハイフン（-）、ドット（.）です。
- ホスト部分をハイフン（-）で開始または終了することはできません。
- ホスト部分に、連続した 2 つのドットを含めることはできません。
- ホスト部分の最短の長さは 2 文字です。
- ホスト部分では、大文字と小文字は区別されません。

（注） **Cisco Unified Communications Manager Administration** で、一括管理を使用して、二重引用符とカンマが埋め込まれたディレクトリ URI を含む CSV ファイルをインポートする場合は、ディレクトリ URI 全体を二重引用符（"）で囲む必要があります。

URI への通話転送

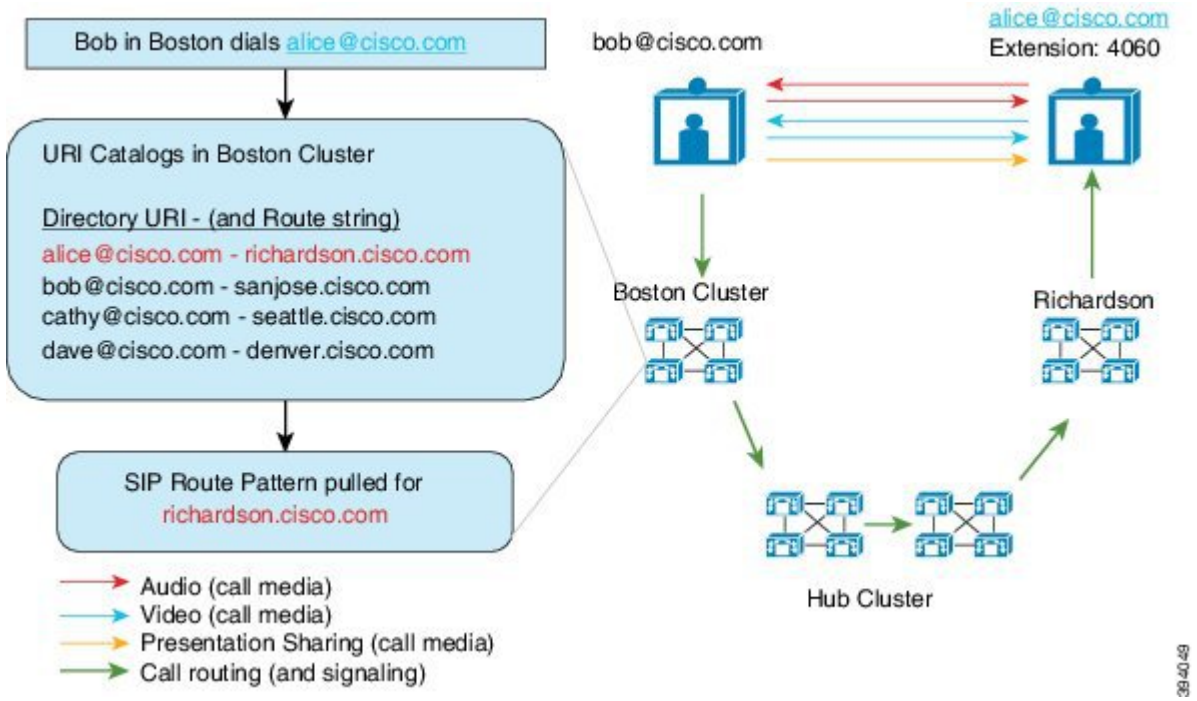
- URI への通話転送は、物理的な電話からはできません。
- URI への通話転送は、その URI がすでに Unified Communications Manager データベースにある場合にのみ、アプリケーションを介して構成できます。URI がデータベースにない場合、アプリケーションは、通話転送を構成しようとしているときに、「通話転送の設定に失敗しました /n 通話転送に失敗しました: 新しい番号」というエラーを出力します。
- 通話転送は、URI がデータベースに存在するかどうかに関係なく、Unified Communications Manager の管理ページで構成できます。
- URI への通話転送は、データベースに存在するかどうかに関係なく、**Cisco Unified Communications Self Care Portal** > **エンドユーザー** ページで構成できます。次の文字を入力する際は、「パーセントエンコーディング」を使用する必要があります。 **# % ^ ` { } | \ : ? < > [ ] \ ‘**。たとえば、**%3A** は、**:** をメンションする際に使用され、**%20** は、スペースをメンションするために使用されます。
- 通話を URI「mobile: 12345@cisco.com」に転送する必要がある場合は、**Cisco Unified Communications Self Care Portal** > **エンドユーザー**ページ の [通話転送（Call-Forward）] セクションで「**mobile%3A%2012345@cisco.com**」を指定する必要があります。

グローバル ダイヤル プラン レプリケーションのコールルーティング

クラスタ内コールの場合、グローバルダイヤルプランデータはパーティションとコーリングサーチスペースを介してルーティングされます。ローカルディレクトリ URI へのコール、エンタープライズ代替番号または e.164 代替番号が機能するには、発信側が使用しているコーリングサーチスペース内のパーティションに URI または番号が存在している必要があります。

クラスタ間コールは、グローバルダイヤルプランレプリケーションがアドバタイズするクラスタルート文字列を使用して、着信側のホームクラスタにコールを送信します。発信者が別のクラスタをホームとするディレクトリ URI または代替番号にコールを発信すると、システムは関連付けられたルート文字列を取得し、そのルート文字列の SIP ルートパターンに一致させ、SIP ルートパターンが指定した宛先にコールを送信します。これを機能させるには、ルート文字列をホームクラスタにルーティングするために、リモートクラスタの SIP ルートパターンを設定する必要があります。

コールルーティングが失敗した場合、システムは関連付けられた PSTN フェールオーバー番号を使用することもできます。ただし、PSTN フェールオーバーコールを適切なゲートウェイに送信できるように、リモートクラスタにルートパターンを設定する必要があります。



グローバル ダイヤル プラン レプリケーションの前提条件

次の作業が必要です。

- シスコ クラスタ間検索サービス（ILS）の設定
- グローバルダイヤルプランの展開方法の計画
  - ユーザのディレクトリ URI をプロビジョニングすることで URI ダイヤリングを展開する場合、グローバル ダイヤル プラン レプリケーションを使用して、ILS ネットワーク全体にディレクトリ URI を複製できます。
  - 代替番号ダイヤリングを展開する場合、エンタープライズ代替番号と E.164 代替番号のどちらを使用し、PSTN フェールオーバーとして使用するのはどちらかを計画します。
  - 代替番号を展開する場合は、番号計画を策定します。大規模なネットワークでは、個々の代替番号ではなく番号パターンを ILS ネットワークにアドバタイズすることで、データベースの領域と帯域幅を節約できます。

グローバル ダイヤル プラン レプリケーションの設定タスクフロー

グローバルダイヤルプランのレプリケーションと URI ダイヤリングを設定するには、次のタスクを実行します。ILS ネットワークの各クラスタでこれらのタスクを実行する必要があります。

手順

	コマンドまたはアクション	目的
Step 1	グローバルダイヤルプラン複製に対する ILS サポートの有効化 （270 ページ）	ローカルクラスタでグローバル ダイヤル プラン レプリケーションのサポートを有効化します。
Step 2	SIP プロファイルの設定 （271 ページ）	グローバルダイヤルプランのレプリケーションと URI ダイヤリングをサポートする SIP 設定を設定します。
Step 3	URI ダイヤリング用の SIP トランクの設定 （271 ページ）	URI ダイヤリングの場合は、システムが連絡先ヘッダーにディレクトリ URI、電話番号、または混合アドレスを挿入するかどうかを設定します。
Step 4	SIP ルートパターンの設定 （272 ページ）	クラスタ間ルーティングの場合は、学習したルート文字列をルーティングする各クラスタの SIP ルートパターンをホームクラスタに設定します。
Step 5	学習したデータに対するデータベース制限の設定 （273 ページ）	ILS がローカルデータベースに書き込むデータ量の上限を設定します。
Step 6	学習番号とパターンのパーティションの設定 （274 ページ）	エンタープライズ代替番号、+E.164 代替番号、および学習された番号パターンのルートパーティションを割り当てます。
Step 7	代替番号のアドバタイズパターンの設定 （275 ページ）	オプション。エンタープライズ代替番号または+E.164 代替番号の範囲を要約する番号パターンをアドバタイズします。
Step 8	学習したパターンのブロック （275 ページ）	オプション。特定の番号または番号パターンへのコールをブロックするパターンを設定します。この設定はローカルに適用され、ILS ネットワークには複製されません。

	コマンドまたはアクション	目的
Step 9	グローバル ダイヤル プランのデータをインポート（278 ページ）	オプション。Cisco TelePresence Video Communications Server またはサードパーティのコール制御システムと相互運用する場合は、そのシステムから ILS ネットワーク内のハブ クラスタに、ディレクトリ URI、+E.164 番号、および PSTN フェールオーバー番号のカタログをインポートします。
Step 10	グローバルダイヤルプランデータのプロビジョニング（276 ページ）	ディレクトリ URI、エンタープライズ代替番号、+E.164 代替番号を電話番号に割り当てます。 （注） 複数のユーザに対しては、LDAP ディレクトリ同期または一括管理を使用して、多数のユーザに対してグローバルダイヤルプランデータを1つの操作で割り当てることができます。このガイドの「ユーザのプロビジョニング」のセクションを参照してください。

グローバル ダイヤル プラン複製に対する ILS サポートの有効化

ローカルクラスタのグローバル ダイヤル プラン レプリケーションの ILS サポートを有効にするには、次の手順に従います。

手順

Step 1 Cisco Unified Communications Manager のパブリッシャノードにログインします。

Step 2 Cisco Unified CM Administration から、**[詳細機能（Advanced Features）] > [ILS 設定（ILS Configuration）]** を選択します。

Step 3 [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）] チェックボックスをオンにします。

Step 4 [アドバタイズルート文字列（Advertised Route String）] テキスト ボックスで、ローカルクラスタのルート文字列を入力します。

Step 5 [保存（Save）] をクリックします。

SIP プロファイルの設定

この手順を使用して、グローバルダイヤルプランレプリケーションと URI ダイヤリングをサポートするようにネットワーク内の SIP プロファイルを編集します。

手順

Step 1 Cisco Unified CM Administration で、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIP プロファイル（SIP Profile）]** を選択します。

Step 2 **[検索（Find）]** をクリックし、既存の SIP プロファイルを選択します。

Step 3 [ダイヤル文字列の解釈（Dial String Interpretation）] ドロップダウンリストから、コールをディレクトリ URI または電話番号としてルーティングするかどうかを決定するためにシステムが使用するポリシーを設定します。

- [常にすべてのダイヤル文字列をURIアドレスとして処理（Always treat all dial strings as URI addresses）]
- [電話番号は0～9、A～D、*、+で構成（これ以外はURIアドレスとして処理）（Phone number consists of characters 0–9, A–D, *, and + (others treated as URI addresses)）]
- [電話番号は0～9、*、+で構成（これ以外はURIアドレスとして処理）（Phone number consists of characters 0-9, *, and + (others treated as URI addresses)）]：これがデフォルトのオプションです。

Step 4 [SIP要求で完全修飾ドメイン名を使用（Use Fully Qualified Domain Name in SIP Requests）] チェックボックスをオンにします。

Step 5 オプション。Cisco Unified Border Element 全体でクラスタ間コールをルーティングできるようにするには、[トランク固有の設定（Trunk-Specific Configuration）] で、[ILS学習接続先ルート文字列を送信（Send ILS Learned Destination Route String）] チェックボックスをオンにします。

Step 6 [保存（Save）] をクリックします。

URI ダイヤリング用の SIP トランクの設定

URI ダイヤルを展開している場合は、ネットワークの SIP トランクの連絡先ヘッダーアドレス指定ポリシーを設定します。このオプションは、Cisco Unified Communications Manager が、ディレクトリ番号、ディレクトリ URI、またはディレクトリ番号とディレクトリ URI の両方を含む混合アドレスを、発信 SIP メッセージの SIP ID ヘッダーに挿入できるかどうかを決定します。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [トランク（Trunk）]** を選択します。

Step 2 [検索（Find）] をクリックして、既存の SIP トランクを選択します。

Step 3 [発信コール（Outbound Calls）] 領域で、[発呼側および接続側情報形式（Calling and Connected Party Info Format）] ドロップダウンリストから、次のいずれかを選択します。

- [接続側にのみDNを配信（Deliver DN only in connected party）]：発信 SIP メッセージで、Unified Communications Manager が SIP コンタクトヘッダー情報に発信者の電話番号を挿入します。これがデフォルトの設定です。
- [接続側にURIのみを配信（使用可能な場合）（Deliver URI only in connected party, if available）]：発信 SIP メッセージで、Unified Communications Manager が SIP コンタクトヘッダーに発信者のディレクトリ URI を挿入します。ディレクトリ URI が利用可能でない場合、Unified Communication Manager は代わりに電話番号を挿入します。
- [接続側にURIおよびDNを配信（使用可能な場合）（Deliver URI and DN in connected party, if available）]：発信 SIP メッセージで、Unified Communications Manager が SIP コンタクトヘッダーに発信者のディレクトリ URI と電話番号を含む混合アドレスを挿入します。Directory URI が利用可能でない場合、Unified Communications Manager は電話番号だけを含めます。

Step 4 [保存（Save）] をクリックします。

SIP ルートパターンの設定

グローバルダイヤルプランレプリケーションと URI ダイヤリングを使用したクラスタ間コールルーティングの場合は、学習したルート文字列をルーティングする SIP ルートパターンをホームクラスタに戻すように設定する必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [SIPルートパターン（SIP Route Pattern）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [**パターン使用率 (Pattern Usage)**] ドロップダウンから、[**ドメインルーティング (Domain Routing)**] を選択します。

Step 4 IPv4 または IPv6 を展開しているかどうかに応じて、[**Ipv4 アドレス (Ipv4 address)**] または [**Ipv6 アドレス (ipv6 address)**] テキストボックスにルート文字列を入力します。

Step 5 [**Sip trunk/Route list**] で、ルート文字列のホームクラスタに戻るルートのネクストホップクラスタにつながる sip トランクまたはルートリストを選択します。

Step 6 [SIPルートパターンの設定（SIP Route Pattern Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 7 [保存（Save）] をクリックします。

Step 8 学習した各ルート文字列の SIP ルートパターンを作成します。

Step 9 ILS ネットワークの各クラスタに対してこれらのタスクを繰り返します。

（注） SIPルートのパターン名にダッシュが含まれている場合は、ダッシュの間に数字がないことを確認する必要があります。ただし、ダッシュが 2 つ以上ある場合は、文字と数字の組み合わせか、文字のみを使用できます。SIP ルートパターンの良い例と悪い例は次のとおりです。

正しいパターン:

- abc-1d-efg.xyz.com
- 123-abc-456.xyz.com

無効なパターン:

- abc-123-def.xyz.com
- 1bc-2-3ef.xyz.com

学習したデータに対するデータベース制限の設定

データベースの制限を設定して、Unified Communications Manager がローカル データベースに書き込むことができる学習オブジェクトの数を決定します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 [サーバ（Server）] ドロップダウンリストから、パラメータを設定するサーバを選択します。

Step 3 [サービス（Service）] ドロップダウンリストから、[シスコ クラスタ間検索サービス（アクティブ）（Cisco Intercluster Lookup Service (Active)）] を選択します。サービスがアクティブと表示されていない場合は、Cisco Unified Serviceability でサービスをアクティベートしたことを確認します。

Step 4 [クラスタ全体のパラメータ（ILS)（Clusterwide Parameters (ILS)）] セクションで、[データベース内の学習オブジェクトの最大数（ILS Max Number of Learned Objects in Database）] サービスパラメータの上限を設定します。

Step 5 [保存（Save）] をクリックします。

（注） このサービスパラメータは、Unified Communications Manager が ILS によって学習するデータに対してデータベースに書き込むことができるエントリの最大数を決定します。このサービスパラメータのデフォルト値は 10 万個で、最大値は 100 万個です。

このサービスパラメータを、データベースに保存されている ILS 学習エントリの現在の数より小さい値に設定した場合、Unified Communications Manager は、ILS 学習オブジェクトをそれ以上データベースに書き込みません。ただし、既存のデータベース エントリはそのままです。

学習番号とパターンのパーティションの設定

パーティションに学習番号と学習パターンを割り当てる必要があります。独自のパーティションを定義することも、事前定義されたデフォルトのパーティションを使用することもできます。Unified Communication Manager は学習代替番号と番号パターンに対して、次の事前定義されたパーティションでインストールされます。

- グローバル学習エンタープライズ番号
- グローバル学習 E.164 番号
- グローバル学習エンタープライズ パターン
- グローバル学習 E.164 パターン

（注） NULL パーティションに学習番号または学習パターンを割り当てることはできません。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [グローバル ダイヤル プラン レプリケーション（Global Dial Plan Replication）] > [学習した番号とパターンのパーティション（Partitions for Learned Numbers and Patterns）]** を選択します。

Step 2 [学習した番号とパターンのパーティション（Partitions for Learned Numbers and Patterns）] ウィンドウのフィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 3 [保存（Save）] をクリックします。

（注） また、パーティションの番号にコールを配置するために、発信者が使用する呼び出し先の検索スペースにもルートパーティションが存在する必要があります。

代替番号のアドバタイズパターンの設定

アドバタイズされたパターンを使用して、エンタープライズの代替番号の範囲またはE.iの代替番号を要約します。このパターンを ILS ネットワークに通知して、クラスタ間でパターンに一致する番号への発信を可能にすることができます。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [グローバル ダイヤル プラン レプリケーション（Global Dial Plan Replication）] > [アドバタイズパターン（Advertised Patterns）]** の順に選択します。

Step 2 [アドバタイズされたパターンの検索と一覧表示（Find and List Advertised Patterns）] ウィンドウで、次のいずれかを実行します。

- 既存のパターンを選択するには、[検索（Find）] をクリックします。
- 新しいパターンを作成するには、[新規追加（Add New）] をクリックします。

Step 3 [パターン（Pattern）] フィールドに、番号パターンを入力します。たとえば、54XXX は、54000 ～ 54999 の範囲の番号を要約しています。

Step 4 [パターンタイプ（Pattern Type）] フィールドで、[エンタープライズ番号パターン（Enterprise Number Pattern）] または「E.164番号パターン（E.164 Number Pattern）] を選択します。

Step 5 ラジオボタンで、PSTN フェールオーバーを適用するかどうかを選択します。

- **[PSTNフェールオーバーを使用しない（Don't use PSTN Failover）]**
- **[パターンをPSTNフェールオーバーとして使用する（Use Pattern as PSTN Failover）]**
- [削除桁数および付加番号をパターンに適用して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）]：このオプションを選択する場合、[PSTNフェールオーバー削除桁数（PSTN Failover Strip Digits）] および [PSTNフェールオーバー付加番号（PSTN Failover Prepend Digits）] フィールドに数字を入力します。

Step 6 [保存（Save）] をクリックします。

学習したパターンのブロック

ローカルクラスタで、特定のエンタープライズ代替番号、+E.164 代替番号、または ILS を通じて学習された番号パターンに対するコールルーティングを防止するブロッキングルールを設定する場合は、このオプションのタスクを実行します。

コールを学習した番号または学習したパターンにルーティングする前に、ILS はローカル ブロッキングルールがダイヤル文字列に一致するかどうかを確認します。ブロッキングルールと一致する場合、Unified Communications Manager はコールをルーティングしません。

手順

Step 1 Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [グローバルダイヤルプランレプリケーション（Global Dial Plan Replication）] > [学習した番号とパターンのブロック（Block Learned Numbers and Patterns）]** を選択します。

Step 2 次のいずれかの操作を実行します。

- 既存のブロッキングルールを選択して編集するには、[検索（Find）] をクリックして、します。
- 新しいルートパターンを作成するには、[新規追加（Add New）] をクリックします。

Step 3 [パターン（Pattern）]フィールドに、ブロックするパターンまたは番号を入力します。たとえば、2065551212 へのコールをブロックするのに、206XXXXXXX というパターンを使用できます。

Step 4 ダイヤル文字列プリフィックスに基づいてコールをブロックする場合は、[プレフィックス（Prefix）] を入力します。

Step 5 コールが特定のクラスタに送信されないようにブロックする場合は、そのクラスタの**[クラスタID（Cluster ID）]**を入力します。

Step 6 [パターンタイプ（Pattern Type）] ドロップダウンリストから、ブロッキングルールを適用する方法を選択します。

- [任意（Any）]：エンタープライズ番号パターンと +E.164 パターンの両方にブロッキングルールを適用する場合は、このオプションを選択します。
- [エンタープライズパターン（Enterprise Pattern）]：エンタープライズ番号パターンにのみブロッキングルールを適用する場合は、このオプションを選択します。
- [+E.164パターン（+E.164 Pattern）]：+E.164 番号パターンにのみブロッキングルールを適用する場合は、このオプションを選択します。

Step 7 [保存（Save）] をクリックします。

グローバルダイヤルプランデータのプロビジョニング

ディレクトリ URI、エンタープライズ代替番号、+E.164 代替番号、および PSTN フェールオーバールールをディレクトリ番号に追加するには、この手順を使用します。

（注） ユーザの数が多い場合は、ユニバーサル回線テンプレートを設定し、LDAP 同期または一括管理などのプロビジョニングツールを使用してそれらを適用することで、多数のユーザのグローバルダイヤル プラン データを 1 回の操作でプロビジョニングできます。このマニュアルの「プロビジョニングユーザ」の項を参照してください。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）]** > **[電話番号（Directory Number）]** の順に選択します。

Step 2 次のいずれかを実行します。

- グローバル ダイヤル プラン データを追加する既存のディレクトリ番号を選択するには、[検索（Find）] をクリックします。
- 新しいディレクトリ番号を作成するには、[新規追加（Add New）] をクリックします。

Step 3 新しい番号を作成する場合は、[電話番号（Directory Number）] を入力し、[保存（Save）] をクリックします。

Step 4 エンタープライズ代替番号を追加するには、[エンタープライズ代替番号の追加（Add an Enterprise Alternate Number）] ボタンをクリックして、次の操作を実行します。

a) [番号マスク（Number Mask）] を入力します。たとえば、4001 の代替番号として「5XXXX」と入力します。結果として生成されたエンタープライズ代替番号（54001）が、[代替番号（Alternate Number）] フィールドに表示されます。
b) ローカルルートパーティションに追加するには、[ローカルルートパーティションに追加（Add to Local Route Partition）] チェックボックスをオンにします。
c) [ルートパーティション（Route Partition）] ドロップダウンから、パーティションを選択します。
d) この代替番号を ILS ネットワークにアドバタイズする場合は、[ILS経由でグローバルにアドバタイズ（Advertise Globally via ILS）] をオンにします。

（注） エンタープライズ代替番号または +E.164 代替番号がパターンの範囲内に収まるように、アドバタイズされたパターンを設定する場合は、代替番号を個別にアドバタイズする必要はありません。

Step 5 +E.164 代替番号を追加するには、[+E.164代替番号の追加（Add an +E.164 Alternate Number）] をクリックして、次の操作を実行します。

a) [番号マスク（Number Mask）] を入力します。たとえば、内線 4001 の代替番号として「1972555XXXX」と入力します。結果として生成された +E.164 代替番号（19725554001）が、[代替番号（Alternate Number）] フィールドに表示されます。
b) ローカルルートパーティションに追加するには、[ローカルルートパーティションに追加（Add to Local Route Partition）] チェックボックスをオンにします。
c) [ルートパーティション（Route Partition）] ドロップダウンから、パーティションを選択します。
d) この代替番号を ILS ネットワークにアドバタイズする場合は、[ILS経由でグローバルにアドバタイズ（Advertise Globally via ILS）] をオンにします。

Step 6 [ディレクトリURI（Directory URIs）] セクションで、この電話番号にディレクトリ URI を追加します。

a) [URI] フィールドに、ディレクトリ URI の詳細情報を入力します。たとえば、alice@cisco.com のように入力します。

b) [パーティション（Partition）] ドロップダウンから、ディレクトリ URI をローカルパーティションに割り当てます。
c) アドバタイズされたカタログにこのディレクトリ URI を含めるには、[ILS経由でグローバルにアドバタイズ（Advertise Globally via ILS）] チェックボックスをオンにします。
d) [行を追加（Add Row）] をクリックし、ディレクトリ URI を追加します。最大 5 個のディレクトリ URI を追加できます。

Step 7 [アドバタイズされたフェールオーバー番号（Advertised Failover Number）] フィールドで、エンタープライズ代替番号または +E.164 代替番号を PSTN フェールオーバーとして選択します。

Step 8 [電話番号の設定（Directory Number Configuration）] ウィンドウの残りのフィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 9 [保存（Save）] をクリックします。

グローバル ダイヤル プランのデータをインポート

Cisco TelePresence Video Communications Server、サードパーティのコール制御システム、または ILS を実行していない別のシステムと相互運用する場合に、この手順を使用します。ディレクトリ URI、+E.164 パターン、および PSTN フェールオーバー ルールのカタログを、他のシステムから ILS ネットワーク内のハブ クラスタにインポートできます。ILS が ILS ネットワーク全体にカタログを複製し、クラスタが他のシステムにコールを発信できるようになります。

始める前に

ダイヤル プラン カタログを他のシステムから CSV ファイルにエクスポートします。

手順

Step 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）] > [グローバル ダイヤル プラン レプリケーション（Global Dial Plan RepIication）] > [グローバル ダイヤル プラン レプリケーション（Imported Global Dial Plan Catalog）]** を選択します。

Step 2 [インポートしたグローバル ダイヤル プラン カタログの検索とリスト（Find and List Imported Global Dial Plan Catalogs）] ウィンドウで、次のいずれかのタスクを実行します。

- 結果のリストから既存のカタログを選択するには、[検索（Find）] をクリックします。
- 新しいカタログを追加するには、[新規追加（Add New）] をクリックします。

Step 3 [インポートしたグローバル ダイヤル プラン カタログ（Imported Global Dial Plan Catalog Settings）] ウィンドウの [名前（Name）] フィールドに、インポートするカタログを識別する一意の名前を入力します。

Step 4 （任意） [説明（Description）] フィールドに、カタログの説明を入力します。

Step 5 [ルート文字列（Route String）] フィールドに、カタログをインポートしているシステムのルート文字列を作成します。

（注） ルート文字列は最大 250 文字長の英数字であり、ドットおよびダッシュを含めることができます。

Step 6 [保存（Save）] をクリックします。

Step 7 Cisco Unified CM Administration から、**[一括管理（Bulk Administration）] > [ファイルのアップロード/ダウンロード（Upload/Download Files）]** を選択します。

- [新規追加（Add New）] をクリックします。
- [参照（Browse）] をクリックして、インポートするカタログの CSV ファイルを選択します。

（注） インポートに使用する CSV ファイルが Cisco Unified Communication Manager と互換性があることを確認します。たとえば、バージョン 9.0(1) へのインポートをサポートする CSV ファイルは、バージョン 10.0(1) とは互換性がありません。

Step 8 [ターゲットを選択（Select the Target）] ドロップダウンリストで、[インポートしたディレクトリ URL とパターン（Imported Directory URIs and Patterns）] を選択します。

Step 9 [トランザクション タイプを選択（Select Transaction Type）] ドロップダウンリストで、[インポートしたディレクトリ URL とパターンを挿入（Insert Imported Directory URIs and Patterns）] を選択します。

Step 10 [保存（Save）] をクリックします。

Step 11 Cisco Unified CM Administration で、**[一括管理（Bulk Administration）] > [ディレクトリ URI とパターン（Directory URIs and Patterns）] > [インポート済みディレクトリ URI およびパターンの挿入（Insert Imported Directory URIs and Patterns）]** の順に選択します。

Step 12 [ファイル名（File Name）] ドロップダウンリストで、インポートするカタログを含む CSV ファイルを選択します。

Step 13 [インポートしたディレクトリ URI カタログ（Imported Directory URI Catalog）] ドロップダウンリストで、[インポートしたグローバル ダイヤル プラン カタログ（Imported Global Dial Plan Catalog）] ウィンドウで名前を付けたカタログを選択します。

Step 14 [ジョブの説明（Description）] テキスト ボックスで、実行するジョブの名前を入力します。

Step 15 次のいずれかの手順を実行します。

- ジョブをただちに実行する場合は、[今すぐ実行（Run Immediately）] オプションを選択し、[送信（Submit）] をクリックします。
- 所定の時刻に実行するようにジョブをスケジュールするには、[後で実行（Run Later）] ラジオ ボタンをオンにして、[送信（Submit）] をクリックします。

（注） [後で実行（Run Later）] オプションを選択した場合は、ジョブの実行時刻をスケジュールするのに、一括管理ジョブ スケジューラーを使用する必要があります。

Cisco Unified Communication Manager は、インポートしたすべての +E.164 パターンを,グローバルな学習された +E.164 パターン パーティションに保存します。

（注） この手順では、すべてのローカル設定されたディレクトリ URI、+E.164 番号パターン、および関連する PSTN フェールオーバー ルールを、他のコール制御システムにインポート可能な CSV ファイル形式でエクスポートする方法について説明します。詳細については、**[一括管理（Bulk Administration）]** > **[ディレクトリURIとパターン（Directory URIs and Patterns）]** > **[ローカルディレクトリURIとパターンのエクスポート（Export Local Directory URIs and Patterns）]** のメニューを参照してください。

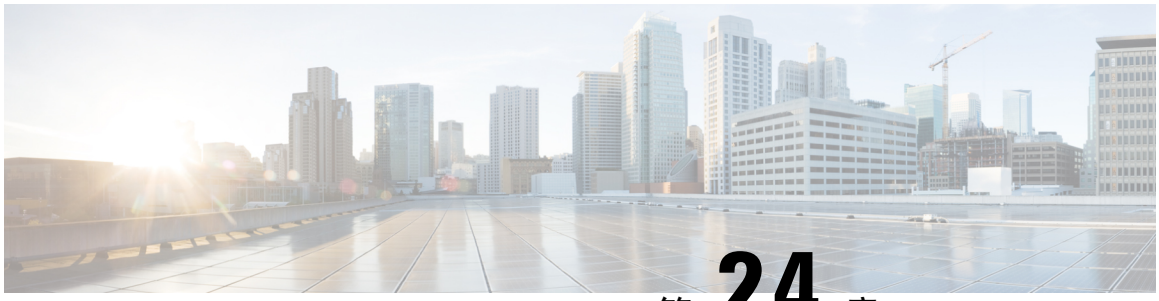
グローバルダイヤルプランレプリケーションの連携動作と制限事項

次の表に、グローバルダイヤルプランレプリケーションと URI ダイヤリングの機能インタラクションの一部を要約します。

機能	連携動作と制限事項
ディレクトリ URI と +E.164 パターンのエクスポート	ローカルクラスタで設定されているすべてのディレクトリ URI と +E.164 番号パターンを csv ファイルにエクスポートして、別のシステムにインポートすることもできます。 **1.** Cisco Unified CM Administration で、**[一括管理（Bulk Adminstration）] > [ディレクトリURIとパターン（Directory URIs and Patterns）] > [ローカルディレクトリURINEとパターンのエクスポート（Export Local Directory URIs and Patterns）]** を選択します。 **2.** 次のラジオボタンのいずれかをクリックして、エクスポートファイルに付加するドメイン名を定義します。 • [組織のトップレベルドメイン（Organizational Top Level Domain）]：[組織のトップレベルドメイン（Organizational Top Level Domain）] エンタープライズパラメータの値をエクスポートファイルのドメイン名に使用する場合は、このラジオボタンをクリックします。 • [ルート文字列ドメイン（Route String Domain）]：[ILSの設定（ILS Configuration）] で設定した [ルート文字列（Route String）] フィールドの値をエクスポート ファイルのドメイン名に使用する場合は、このラジオ ボタンをクリックします。 • [ユーザ定義ドメイン（User Defined Domain）]：エクスポートファイルに付加するカスタマイズされたドメイン名を作成する場合は、このラジオ ボタンをクリックします。このオプションを選択する場合は、[ドメイン名（Domain Name）] テキストボックスにドメイン名を入力します。 **3.** [ローカルディレクトリ URI とパターンのエクスポート（Export Local Directory URIs and Patterns）] ボタンをクリックします。 **4.** CSV ファイルをローカル ドライブに保存します。

機能	連携動作と制限事項
URI ダイヤリングを使用したパーティション化	ディレクトリ URI のパーティション分割は、ディレクトリ URI のプロビジョニング方法によって異なります。 • [エンドユーザの設定（End User Configuration）] でエンドユーザに割り当てたユーザベースのディレクトリ URI の場合、削除できないローカルのディレクトリ URI パーティションが自動的に URI に割り当てられます。別のパーティションを割り当てることはできませんが、[ディレクトリURIエイリアスパーティション（Directory URI Alias Partition）] エンタプライズパラメータを設定することで、管理者が管理するパーティションをローカルディレクトリ URI パーティションのエイリアスとして使用できます。 • [電話番号の設定（Directory Number Configuration）] で URI が電話番号に直接割り当てられている回線ベースのディレクトリ URI の場合、各 URI をローカルのパーティションに個別に割り当てることができます。 LDAP 同期や一括管理などのツールを使用してディレクトリ URI をプロビジョニングする場合は、次のようになります。 • LDAP 同期によってプロビジョニングされるディレクトリ URI はユーザベースであり、[エンドユーザの設定（End User Configuration）] でユーザに割り当てられます。これらの URI は、ローカルのディレクトリ URI パーティションに割り当てられます。ユーザにプライマリ内線番号が設定されている場合、この URI は、[電話番号の設定（Directory Number Configuration）] でもプライマリ URI として表示されます。ただし、割り当てられたパーティションはディレクトリ URI パーティションです。 • 一括管理でプロビジョニングされたディレクトリ URI の場合は、更新の適用方法によって異なります。たとえば、`bat.xlt` スプレッドシートを使用して csv インポート ファイルを作成する場合、スプレッドシートの [ユーザ（Users）] タブまたは [ユーザの更新（Update Users）] タブを使用してディレクトリ URI を追加すると、ユーザはユーザベースの URI になります。ただし、[ファイル形式の作成（Create File Format）] をクリックすると表示される [回線フィールド（Line Fields）] オプションを使用してディレクトリ URI を追加する場合は、その URI を電話番号に割り当て、ローカルパーティションを URI ディレクトリに割り当てることができます。
ディレクトリ URI の大文字と小文字の区別	デフォルトでは、ディレクトリ URI のユーザ部分（@ の前の部分）では、大文字と小文字が区別されます。[URI検索ポリシー（URI Lookup Policy）]エンタープライズパラメータを編集することで、ユーザの部分で大文字と小文字を区別しないように設定できます。

機能	連携動作と制限事項
コーリングサーチスペース	ディレクトリ URI、エンタープライズ代替番号、および +E.164 代替番号がダイアル可能になるためには、発信者のコーリングサーチスペースで使用可能なパーティションにそれらのURIまたは番号が存在する必要があります。
URI ダイヤリングを使用したディジット変換	番号変換を使用していて、クラスタ間URIダイヤリングを展開している場合は、電話機の設定または電話機が使用するデバイスプールに対してディジット変換を適用します。 • 個別の電話に対しては、[リモート番号（Remote Number）]セクションの [発信側変換CSS（Calling Party Transformation CSS）] フィールドで変換を適用します。 • デバイスプールの場合は、[デバイスモビリティ関連情報（Device Mobility Related Information）] の下にある [発信側変換CSS（Calling Party Transformation CSS）] フィールドで変換を適用できます。 （注） ローミング デバイスの場合は、[電話の設定（Phone Configuration）] ウィンドウの [デバイスプールの発信側変換CSSを使用（Use Device Pool Calling Party Transformation CSS）] チェックボックスがオフの場合でも、デバイスプールの設定が電話の設定よりも優先されます。



第 24 章

発信側の正規化

発信側の正規化の概要

発信側の正規化によって電話番号のグローバル化やローカライズが可能になるため、適切な発信番号が電話機に表示されます。発信側の正規化を使用して、一部の電話機のダイヤル機能を強化し、コールが複数の地理的ロケーションにルーティングされる場合の折返し機能を向上させます。この機能は、電話機のコールログディレクトリのディレクトリ番号を変更することなく電話機がコールバックできるよう、グローバル発信者番号をローカライズされた番号にマッピングできます。

発信者番号のグローバル化

Cisco Unified CM Administration で [発信者番号タイプ（Calling Party Number Type）] とプレフィックスを設定することで、着信側の電話に表示する発信者電話番号を、（国際国番号などのプレフィックスを含むグローバル化バージョンに）再フォーマットするように Cisco Unified Communications Manager を設定できます。それによって、世界中のどこからでもその番号をダイヤルできます。

Cisco Unified Communications Manager は、[発信者番号タイプ（Calling Party Number Type）] の値とともにルートパターンや変換パターンなどのさまざまな番号パターンを使用して、電話番号をグローバル化できます。たとえば、Cisco Unified Communications Manager は、サブスクライバ発信者番号タイプのローカライズされたドイツの電話番号 069XXXXXXX を、ドイツの国番号と都市コードを含む +49 40 69XXXXXXX にグローバル化するように設定できます。

複数の地理的場所にルーティングされるコールの場合、各ルーティング パスに適用される異なるトランスレーション設定によって、発信者番号は各コール パスで一意にグローバル化できます。Cisco Unified Communications Manager では、電話でローカライズされた発信者番号を電話画面に表示し、グローバル化された番号を電話の通話履歴ディレクトリに表示するように設定することもできます。電話ユーザがコールを発信する前に、電話の通話履歴ディレクトリのエントリを編

集する必要がないようにするため、グローバル発信者番号をそのローカル バージョンにマッピングします。

発信者番号のローカリゼーション

発信者番号の最終表示用に、発信者番号タイプ（国内、国際、サブスクライバ、不明）ごとに発信側変換パターンを設定し、そのコールの発信者番号タイプに固有のストリップ桁数とプレフィックスの手順を適用できます。これによって、Cisco Unified Communications Manager は、着信側の電話に表示される発信者番号が不要な国コードや国際アクセス コードを含まないローカライズされた番号となるように、発信者番号を再フォーマットできます。

たとえば、PSTN から到着した着信番号が、グローバル化された番号 +49 40 69XXXXXXX で（+49 が国番号、40 が都市コードを表す）、発信者番号タイプがサブスクライバであるとします。Cisco Unified Communications Manager には、国番号、都市コードを取り除き、プレフィックス 0 を追加する手順とともに、発信側の変換パターンを設定できます。手順が適用された後、発信者番号はダイヤルされた電話に 069XXXXXXX として表示されます。

グローバル化された発信者番号のローカライズ バージョンへのマッピング

電話ユーザがコールを発信する前に、電話の通話履歴ディレクトリのエントリを編集する必要がないようにするため、ルートパターンと着信側変換パターンを使用して、グローバル発信者番号をローカライズされたバージョンにマッピングできます。これによって、着信側がコールを返す場合に、Cisco Unified Communications Manager は確実に正しいゲートウェイにコールをルーティングできます。

グローバル発信者番号のマッピングによって、コールバック機能が改善され、着信側は電話の通話履歴ディレクトリ内の電話番号を変更する必要なく、コールバックできます。

発信側の正規化の要件

発信側の正規化を設定する前に、Cisco Unified Serviceability で **Cisco CallManager** サービスをアクティブにする必要があります。詳細については、『*Cisco Unified Serviceability* アドミニストレーション ガイド』を参照してください。

Cisco Unified Communications Manager に発信者番号タイプを判別させるには、想定するコールに一致する [発信者番号タイプ（Calling Party Number Type）] 値を割り当てるパターンを設定します。次の設定ウィンドウで、パターンを作成して適用することができます。

- ルートパターン
- ハントパイロット
- 変換パターン
- 発信番号変換パターン

（注） 発信者による変換は、元の発信者に対してのみ機能します。番号をリダイレクトするために行った変更は、転送ヘッダーに対してのみ適用されます。[SIP トランク] チャプターから設定を確認し、SIP トランク自体に転送ヘッダーを追加します。

発信側の正規化の設定タスクフロー

発信側の正規化のプレフィックスと削除桁数ルールは、Unified Communications Manager でさまざまな場面で適用できます。たとえば、デバイスプール、ルートパターン、変換パターン、ハントパイロット、ゲートウェイ、およびトランクに桁数の変換を適用できます。桁数の変換を適用する方法は、ダイヤル プラン、デバイス、およびトランクの導入方法に応じて変わります。詳細については、ダイヤル プラン、ルートパターン、変換パターン、および変換パターンに関連するトピックを参照してください。

手順

	コマンドまたはアクション	目的
Step 1	Unified Communications Manager に発信者番号タイプを判断させる場合は、予想されるコールと合致する発信者番号タイプを作成して設定する必要があります。次の設定ウィンドウで、パターンを作成して適用することができます。 • ルートパターン • ハントパイロット • 変換パターン • 発信番号変換パターン	
Step 2	発信側番号のグローバル化（288ページ）	PSTN 経由で受信する着信コールの場合は、発信者番号をグローバライズするための設定を構成します。
Step 3	コーリングサーチスペースの設定 （289ページ）	パーティションとコーリングサーチスペースを設定します。
Step 4	発信側変換パターンの作成（289ページ）	発信者番号をグローバル化されたバージョンまたはローカライズされたバージョンに変換し、各パターンをパーティションに割り当てる、通話相手の変換のパターンを作成します。

	コマンドまたはアクション	目的
Step 5	コーリングサーチスペースへの発信側変換パターンの適用 （290 ページ）	デバイスプール、ゲートウェイ、およびトランクのように、着信通話関係者変換CSSをデバイスに適用します。

発信側番号のグローバル化

PSTN経由で到達する着信コールの場合は、発信者番号をグローバル化する設定を行います。発信者番号をグローバル化し、それをデバイスプールまたは個々のデバイスに適用する設定できます。また、クラスタ全体に、発信者番号の正規化設定を適用するサービスパラメータを設定できます。

発信者番号をグローバル化するには、次の手順を実行します。

手順

Step 1 発信者番号の正規化設定を特定のデバイスに適用するには、次の手順を実行します。

a) 設定を適用するデバイスの設定ウィンドウを開きます。たとえば、デバイスプール、ゲートウェイ、電話、トランクです。

b) 設定ウィンドウの [着信コールの発信側の設定（Incoming Calling Party Settings）] セクションで、各発信者番号タイプのプレフィックスおよび削除桁数の指示を適用します。

（注） Cisco Unified Communications Manager には、コール転送、通話パーク、ボイス メッセージング、CDR データなどの補足サービスのような、すべての追加アクションの発信者番号フィールドにプレフィックスが含まれます。

Step 2 サービスパラメータを使用して、クラスタ全体のすべてのデバイスの発信者番号をグローバル化する場合には、次の手順を実行します。

a) Cisco Unified CM Administration から、**[システム（System）] > [サービスパラメータ（Service Parameters）]** の順に選択します。

b) [サーバ（Server）] ドロップダウンリストから、サービスを実行するサーバを選択します。

c) [サービス（Service）] ドロップダウンリストから、[Cisco CallManager] を選択します。

d) [詳細設定（Advanced）] をクリックします。

e) 以下のパラメータの値を設定します。この値は、クラスタ全体から電話、MGCP ゲートウェイ、H.323 ゲートウェイに適用できます。

- [発信者の国内番号プレフィックス（Incoming Calling Party National Number Prefix）]
- [発信者の国際番号プレフィックス（Incoming Calling Party International Number Prefix）]
- [発信者の不明な着信番号プレフィックス（Incoming Calling Party Unknown Number Prefix）]
- [発信者の加入者番号プレフィックス（Incoming Calling Party Subscriber Number Prefix）]

（注） Cisco Unified Communications Manager で、特定の電話のクラスタ全体のサービスパラメータ設定を適用するには、デバイスとデバイスプール レベルの両方で、その電話のプリフィックス設定をデフォルト オプションに設定する必要があります。

コーリングサーチスペースの設定

呼び出し側の正規化機能を処理するためにコーリングサーチスペースを設定する場合は、この手順を使用します。

手順

Step 1 Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [パーティション（Partitions）]** の順に選択します。

Step 2 ネットワークのパーティションを作成します。

Step 3 Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [コーリングサーチスペース（Calling Search Space）]** の順に選択します。

Step 4 発信側変換パターンのコーリングサーチスペースを作成します。

Step 5 コーリングサーチスペースごとに、パーティションをコーリングサーチスペースに割り当てます。

発信側変換パターンの作成

発信側の正規化機能を処理するために発信側変換パターンを設定している場合、次の手順を使用します。

手順

Step 1 Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [変換パターン（Transformation Pattern）] > [発信側変換パターン（Calling Party Transformation Pattern）]** を選択します。

Step 2 変換パターンを作成します。

Step 3 作成する発信側変換パターンそれぞれには、発信側番号を国際対応または国内対応するために、先頭に付加または除外している番号コマンドを割り当てます。

Step 4 それぞれの発信側変換パターンには、コーリングサーチスペースの1つに関連付けられているパーティションを割り当てます。

コーリングサーチスペースへの発信側変換パターンの適用

デバイスプール、ゲートウェイ、トランクなどのデバイスに、着信する発信側変換 CSS を割り当てます。

手順

Step 1 Cisco Unified CM Administration で、発信側変換を適用するデバイスに該当する設定ウィンドウを選択します。

- [ゲートウェイ（Gateways）]
- [トランク（Trunks）]
- [デバイスプール（Device Pools）]

Step 2 発信者番号をローカライズするには、[コーリングサーチスペース（Calling Search Space）] ドロップダウンリスト ボックスで、適用する発信側変換パターンを含む CSS を選択します。

（注） デバイスプールに対して CSS を設定する場合、電話機にもそのデバイスプールを適用する必要があります。

Step 3 発信者番号をグローバル化するには、[着信の発信者番号設定（Incoming Calling Party Settings）] セクションで、適用する発信側変換パターンを含むコーリングサーチスペースを選択します。

発信側の正規化サービスパラメータの例

次のパラメータは、電話機、MGCP ゲートウェイ、または H.323 に対して、クラスタ全体に適用することができます。特定のデバイスでクラスタ全体パラメータを使用するためには、デバイス設定のプレフィックスをデフォルトに設定する必要があります。

- [発信者の国内番号プレフィックス（Incoming Calling Party National Number Prefix）]
- [発信者の国際番号プレフィックス（Incoming Calling Party International Number Prefix）]
- [発信者の不明な着信番号プレフィックス（Incoming Calling Party Unknown Number Prefix）]
- [発信者の加入者番号プレフィックス（Incoming Calling Party Subscriber Number Prefix）]

次の表に、プレフィックスとストリップディジットの設定の例と、これらの値を使用して、発信者番号の表示を変換する方法を示します。サービスパラメータの設定の場合、コロンの後の数字は、呼び出し者番号の先頭から除外する桁数を表し、コロンの後の数字は、発信者番号の先頭に追加されるプレフィックスを表します。

表 *24 :* 発信側の正規化のサービスパラメータ例

元の着信番号	サービスパラメータ値	説明	最終着信番号
04423452345	+:1	最初の桁を削除してから、+ のプレフィックスを追加します	+4423452345
04423452345	:2	先頭 2 桁を取り除きます	423452345
552345	+1:6	先頭 6 桁を取り除き、プレフィックスとして+1 を追加します	+1
552345	+1:8	使用可能な桁数より多くの桁数が取り除かれるため、最終的な番号は空白になります	
552345	123	プレフィックスとして 123 を追加します	123552345
空白	+1:2	発信者番号が空白の場合、プレフィックスは適用されません	空白
0442345	:26	発信者番号の正規化で取り除くことができる桁数は、24 桁のみです	Cisco Unified Communications Manager では、この設定は許可されません

発信側の正規化の連携動作と制限事項

発信側の正規化の連携動作

発信側の正規化機能との連携動作を次の表で説明します。

機能	連携動作
転送コール	転送機能は、発信時の更新と発信者の正規化に依存しており、各コールホップの初期コール設定が行われるため、発信者の正規化がサポートされない場合があります。次に示すのは、発信者の正規化を転送に使用する方法の一例です。 内線番号 12345、電話番号 972 500 2345 の電話機 A が、内線番号 54321、電話番号 972 500 4321 の電話機 B にコールを発信します。電話 B では、発信者番号 12345 が表示されますが、電話 B はそのコールをサンホセゲートウェイを介して電話 C に転送します。最初の転送時には、電話 C は 972 500 4321 の発信者番号が表示されますが、転送が完了した後、電話機 C は電話 A の発信者番号を 12345 として表示します。
コールの転送	転送されたコールは、発信者側番号のグローバル化およびローカル化をサポートします。たとえば、ダラスの PSTN 経由で発信者が電話機 F を使用して電話機 G にコールを発信します。電話機 G では、すべてのコールがサンノゼにある電話機 H に自動転送されます。着信するダラスゲートウェイでは、発信者番号は 555-5555/Subscriber と表示されますが、そのコールはサンノゼのゲートウェイに転送されます。ダラスからの発信コールは 972 555 5555 として表示されます。サンホセゲートウェイでの受信時には、+ 1 がプリフィックスされ、電話 F は +1 972 555 5555 というコール番号を表示します。
コール詳細レコード	発信側の正規化が呼詳細（CDR）と動作する方法の詳細については、『*Cisco Unified Communications Manager Call Detail Records* アドミニストレーション ガイド』を参照してください。
Cisco Unified Communications Manager Assistant	発信側の正規化機能を設定すると、Cisco Unified Communications Manager Assistant により、ローカライズおよびグローバル化されたコールが自動的にサポートされます。Cisco Unified Communications Manager Assistant は、ローカライズされた発信側番号をユーザ インターフェイスに表示できます。また、マネージャに対する着信コールの場合、Cisco Unified Communications Manager Assistant は、フィルタ パターンに一致したときに、ローカライズされた発信側番号とグローバル化された発信側番号を表示できます。Cisco Unified Communications Manager Assistant の設定方法の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）を参照してください。

機能	連携動作
Cisco Unity Connection	Cisco Unity Connection は、国際エスケープ文字（+）をサポートしていません。このため、ボイス メッセージング機能を正常に動作させるには、Cisco Unity Connection へのコールに（+）が含まれていないことを確認する必要があります。 Cisco Unity Connection が予想どおりに動作するようにするには、このアプリケーションをデバイスとして扱い、発信側変換を設定して、このボイスメール アプリケーションに + が送信されないようにする必要があります。Cisco Unity Connection サーバで北米ベースのダイヤル プランを使用している場合は、Cisco Unity Connection で発信側番号を受信する前に、その発信側番号を NANP 形式にローカライズします。Cisco Unified Communications Manager の管理ページにはボイスメール ポート用の発信側変換 オプションがないため、ボイスメール ポートに関連付けられているデバイスプールで発信側番号変換を設定するようにしてください。発信側番号をローカライズするには、ボイスメール アプリケーションが特定の機能（Live Reply など）用の番号に容易にリダイヤルできるよう、アクセスコードにプレフィックスを付加することも検討してください。たとえば、+12225551234 を 912225551234 に変換したり、国際番号 +4423453456 に国際エスケープ コードを含めて 90114423453456 のように変換したりできます。
デバイス モビリティ	ローミング用デバイスプールの発信側変換 CSS は、[電話の設定(Phone Configuration)] ウィンドウで [デバイスプールの発信側変換CSSを使用(Use Device Pool Calling Party Transformation CSS)] チェックボックスがオフの場合でも、同じデバイスモビリティグループ内でローミングする電話機のデバイスレベルの設定をオーバーライドします。 次の例は、発信者側の正規化が、ホームロケーションはダラスだけれども、現在はサンノゼにローミングしている電話のデバイスモビリティと動作するようすを示しています。 電話機がサンノゼでローミングしているときに、ダラスの 972 500 1212 <国内> から PSTN 経由でコールを受けます。サンノゼの着信ゲートウェイでは、発信側番号がグローバル形式の + 1 408 500 1212 に変換されます。現在サンノゼにある電話機では、発信側番号は 1 972 500 1212 として表示されます。 電話機がサンノゼでローミングしているときに、サンノゼの 7 桁のダイヤル エリア内の 500 1212 <加入者> から PSTN 経由でコールを受けます。サンノゼの着信ゲートウェイでは、発信側番号がグローバル形式の + 1 408 500 1212 に変換されます。現在サンノゼにある電話機では、発信側番号は 9 500 1212 として表示されます。

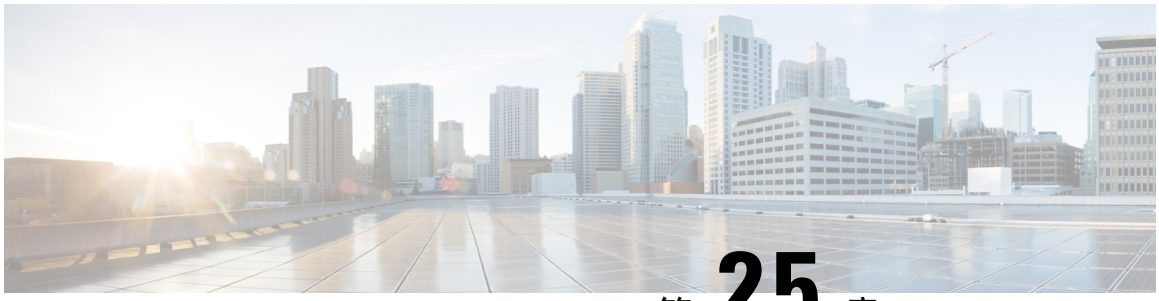
発信側の正規化の制限事項

次の表は、通話相手の正規化機能が、Cisco Unified Communications Manager の特定の機能とシステムコンポーネントを使用している場合の制限を示しています。

表 *25 :* 発信側の正規化の制限事項

機能	制限事項
共有回線	共有回線の場合に表示される発信側番号は、Cisco Unified Communications Manager 内の一連のコール制御イベントによって決まります。ローカライズされた正しくない発信側番号が共有回線で表示されるのを回避するため、特に、共有回線が地理的に異なる場所にまたがる場合は、同じ回線を共有する異なるデバイスに同じ発信側変換 CSS を設定する必要があります。
SIP トランクおよびMGCP ゲートウェイ	SIP トランクおよび MGCP ゲートウェイでは、コールごとに国際エスケープ文字（+）の送信をサポートしています。H.323 ゲートウェイは、+ をサポートしていません。QSIG トランクは、+の送信を試みません。+をサポートするゲートウェイ経由の発信コールの場合、Cisco Unified Communications Manager は、ダイヤルされた数字とともに+をゲートウェイに送信できます。+をサポートしないゲートウェイ経由の発信コールの場合、Cisco Unified Communications Manager がゲートウェイにコール情報を送信すると、国際エスケープ文字 + が除去されます。
SIP	SIP は番号タイプをサポートしないため、SIP トランク経由のコールは、発信側番号の種類が不明（Unknown）である [着信番号（Incoming Number）] 設定のみをサポートします。
QSIG	QSIG設定は、通常、均一のダイヤルプランをサポートします。QSIGを使用している場合、番号とプレフィックスの変換により機能の連携動作に問題が発生することがあります。
発信側変換 CSS	発信側番号をローカライズする場合、デバイスは、番号分析を使用して変換を適用する必要があります。[発信側変換CSS（Calling Party Transformation CSS）] を **[None]** に設定した場合、変換は一致せず、適用されません。ルーティングに使用されない Null 以外のパーティションで、必ず [発信側変換パターン（Calling Party Transformation Pattern）] を設定してください。
T1-CAS および FXO ポート	発信側変換 CSS（Calling Party Transformation CSS）設定は、ゲートウェイ上の T1-CAS と FXO ポートには適用されません。

機能	制限事項
Cisco Unity Connection	Cisco Unity Connection は、国際エスケープ文字（+）をサポートしていません。このため、ボイスメッセージング機能を正常に動作させるには、Cisco Unity Connection へのコールに（+）が含まれていないことを確認する必要があります。 Cisco Unity Connection の詳細については、http://www.cisco.com/c/en/us/products/unified-communications/unity-connection/index.html を参照してください。



第 25 章

ダイヤルルールの設定

ダイヤルルールの概要

Unified CM は、次のタイプのダイヤルルールをサポートしています。

- **アプリケーション ダイヤル ルール**：Cisco Web Dialer や Cisco Unified Communications Manager などのアプリケーション用にダイヤルルールを追加したり優先順位を並べ替えたりするには、管理者がアプリケーション ダイヤルルールを使用します。
- **ディレクトリ検索ダイヤル ルール**：発信者識別番号を変換したり、Cisco Unified Communications Manager Assistant などのアプリケーションでアシスタント コンソールからディレクトリ検索を実行したりするには、管理者がディレクトリ検索ダイヤル ルールを使用します。
- **SIP ダイヤルルール**：システム番号の分析とルーティングを実行するには、管理者が SIP ダイヤルルールを使用します。管理者は SIP ダイヤルルールを設定し、コール処理が実行される前に、その SIP ダイヤルルールを Cisco Unified IP Phone に追加します。

ダイヤルルールの前提条件

- SIP ダイヤルルール設定の場合は、デバイスが SIP を実行している必要があります。
- 管理者は、Cisco IP Phone 7911、7940、7941、7960、7961、7970、および 7971 とともに SIP ダイヤルルールを次のデバイスに関連付けます。

ダイヤルルールの設定タスクフロー

手順

	コマンドまたはアクション	目的
Step 1	アプリケーション ダイヤル ルールの設定（298 ページ）	Cisco Web Dialer、Cisco Unified Communications Manager Assistant などのアプリケーションのダイヤルルールの優先順位を追加し並べ替える、アプリケーション ダイヤル ルールを設定します。
Step 2	ディレクトリ検索ダイヤルルールの設定（299 ページ）	発信者の ID 番号をディレクトリで検索可能な番号に変換するには、ディレクトリ検索ダイヤルルールを設定します。
Step 3	SIP ダイヤルルールの設定 （300 ページ）	SIP を実行している電話のダイヤルプランを設定するには、SIP ダイヤルルールの設定を使用します。
Step 4	ダイヤルルールの優先順位の変更 （303 ページ）	（オプション）複数のダイヤルルールがある場合は、[Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] ウィンドウでダイヤルルールの優先順位を変更します。

アプリケーション ダイヤル ルールの設定

Cisco Unified Communications Manager は、アプリケーション ダイヤル ルールをサポートし、Cisco Web Dialer や Cisco Unified Communications Manager Assistant のようなアプリケーションのダイヤルルールの優先順位の追加と並べ替えができます。アプリケーション ダイヤル ルールを適用すると、ユーザがダイヤルする電話番号に対して数字の追加と削除が自動的に行われます。たとえば、外線発信する場合にはアプリケーションのダイヤルルールにより、7 桁の電話番号の先頭に番号 9 が自動で付加されます。

（注） Cisco Unified Communications Manager は自動的に、CTI リモート デバイスのすべてのリモート接続先番号にアプリケーション ダイヤル ルールを適用します。

新しいアプリケーション ダイヤル ルールを追加する、または既存のアプリケーション ダイヤル ルールを更新するには、次の手順を実行します。

手順

Step 1 Cisco Unified Communications Manager Administrationから、**[コールルーティング（Call Routing）]** > **[ダイヤルルール（Dial Rules）]** > **[アプリケーションダイヤルルール（Application Dial Rules）]** を選択します。

Step 2 [アプリケーション ダイヤル ルールの検索と一覧表示（Find and List Application Dial Rules）] ウィンドウで、次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックします。
- [検索（Find）] をクリックし、既存のアプリケーション ダイヤル ルールを選択します。

Step 3 [アプリケーション ダイヤル ルールの設定（Application Dial Rule Configuration）] ウィンドウのフィールドを設定します。フィールドの説明の詳細については、オンライン ヘルプを参照してください。

Step 4 [保存（Save）] をクリックします。

次のタスク

次の作業を行います。

- ディレクトリ検索ダイヤルルールの設定 （299 ページ）
- SIP ダイヤルルールの設定 （300 ページ）

ディレクトリ検索ダイヤルルールの設定

ディレクトリ検索ダイヤルルールは、発信者の識別情報を、ディレクトリで検索可能な番号に変換します。各ルールでは、先頭の数字および番号の長さに基づいて、変換する数字を指定します。たとえば、10 桁の電話番号から市外局番と 2 桁の局番を自動的に削除するディレクトリ検索ダイヤルルールを作成できます。たとえば、4085551212 は、51212 になります。

新しいディレクトリ検索ダイヤルルールを追加するか、既存のディレクトリ検索ダイヤルルールを更新するには、次の手順を実行します。

手順

Step 1 Cisco Unified Communications Manager Administration から、**[コールルーティング（Call Routing）]** > **[ダイヤルルール（Dial Rules）]** > **[ディレクトリ検索ダイヤルルール（Directory Lookup Dial Rules）]** を選択します。

Step 2 [ディレクトリ検索ダイヤルルールの検索と一覧表示（Directory Lookup Dial Rule Find and List）] ウィンドウで、以下のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックします。
- [検索（Find）] をクリックし、既存のディレクトリ検索ダイヤルルールを選択します。

Step 3 [ディレクトリ検索ダイヤルルール（Directory Lookup Dial Rules）] ウィンドウ内の各フィールドを設定します。フィールドの説明の詳細については、オンライン ヘルプを参照してください。

Step 4 [保存（Save）] をクリックします。

次のタスク

SIP ダイヤルルールの設定 （300 ページ）

SIP ダイヤルルールの設定

SIP ダイヤルルールによって、SIP を実行している Cisco IP 電話のローカル ダイヤル プランが提供されるため、ユーザは、コールが処理される前にキーを押したり、タイマーを待機したりする必要はありません。管理者が SIP ダイヤルルールを設定し、SIP を実行している電話機に適用します。

手順

	コマンドまたはアクション	目的
Step 1	SIP ダイヤルルールの設定 （301 ページ）	SIP ダイヤルルールを設定および更新し、それらを SIP を実行している電話機と関連付けます。
Step 2	SIP ダイヤルルールのリセット （302 ページ）	SIP ダイヤルルールを更新したときに、SIP を実行している電話機をリセットまたは再起動して、電話機を新しい SIP ダイヤルルールで更新する手順は、次のとおりです。
Step 3	SIP ダイヤルルール設定と SIP 電話の同期 （303 ページ）	設定変更された SIP ダイヤルルールと SIP 電話を同期化するには、次の手順を行います。この手順によって、中断を最小限に抑えた方法で未処理の設定が適用されます。（たとえば、影響を受ける SIP 電話の中には、リセットまたは再起動が不要なものがあります）。

関連トピック

パターンの形式, on page 301

パターンの形式

表 *26 : SIP* ダイヤルルールのパターンフォーマット

ダイヤルルールパターン	値
7940_7960_OTHER	• ピリオド（.）は、すべての文字に一致します。 • シャープ記号（#）は、終了キーとして機能します。終了が適用されるのは、マッチングで>#にヒットした後だけです。または、終了キーとしてアスタリスク (*) を使用することもできます。 （注） シャープ記号を [7940_7960_OTHER] で有効にするには、パターン フィールドにシャープ記号を設定する必要があります。 • アスタリスク (*) は 1 つ以上の文字に一致し、ワイルドカード文字として処理されます。* の前にバックスラッシュ（\）エスケープ シーケンスを置いて * というシーケンスにすると、* を通常の文字として処理できます。\ は電話機が自動的に削除するため、発信ダイヤル文字列には現れません。* は、ダイヤル番号として受信された場合、ワイルドカード文字 * とピリオド（.）に一致します。 • カンマ（,）を使用すると、電話機が第 2 発信音を生成します。 7 で始まるすべての 4 桁 DN に一致します。8,..... 8,..... 8 に一致し、第2発信音（デフォルト値）を再生した後、すべての 5 桁 DN に一致します。

SIP ダイヤルルールの設定

SIP を実行している電話機のダイヤルプランを設定します。

手順

Step 1 Cisco Unified Communications Manager Administration から、**[コールルーティング（Call Routing）]** > **[ダイヤルルール（Dial Rules）]** > **[SIPダイヤルルール（SIP Dial Rules）]**.を選択します。

Step 2 [SIPダイヤルルールの検索/一覧表示（Find and List SIP Dial Rules）] ウィンドウで、次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックします。
- [検索（Find）] をクリックし、既存の SIP ダイヤルルールを選択します。

Step 3 [SIP ダイヤルルールの設定（SIP Dial Rule Configuration）] ウィンドウの各フィールドを設定します。フィールドの説明の詳細については、オンライン ヘルプを参照してください。

Step 4 [保存（Save）] をクリックします。

（注） Cisco Unified Communication Manager Administration で SIP ダイヤルルールを追加または更新すると、Cisco TFTP サービスによってすべての電話機構成ファイルが再構築されます。そのため、Cisco TFTP サービスを実行するサーバ上の CPU にスパイクが発生することがあり、これは多くの電話が接続された大規模なシステムでは顕著になります。CPU にスパイクを発生させないためには、SIP ダイヤルルールの追加や更新をメンテナンス時間枠内で行うか、または設定変更を行う前に Cisco Unified Serviceability で Cisco TFTP サービスを一時的に停止するかしてください。Cisco TFTP サービスを停止した場合は、SIP ダイヤルルールを追加または更新した後、必ず Cisco Unified Serviceability でサービスを再開してください。

次のタスク

SIP ダイヤルルールのリセット （302 ページ）

関連トピック

パターンの形式, on page 301

SIP ダイヤルルールのリセット

SIP ダイヤルルールを更新したときに、新しい SIP ダイヤルルールで電話機が更新されるよう、次の手順を実行して SIP を実行している電話機をリセットまたは再起動します。

始める前に

SIP ダイヤルルールの設定 （301 ページ）

手順

Step 1 Cisco Unified Communications Manager Administrationから、**[コールルーティング（Call Routing）]** > **[ダイヤルルール（Dial Rules）]** > **[アプリケーションダイヤルルール（Application Dial Rules）]** を選択します。

Step 2 [SIP ダイヤルルールの検索と一覧表示（Find and List SIP Dial Rules）] ウィンドウで、[検索（Find）] をクリックし、リセットする既存の SIP ダイヤルルールを選択します。

Step 3 [SIP ダイヤルルールの設定（SIP Dial Rule Configuration）] ウィンドウで、[リセット（Reset）] をクリックします。

Step 4 [デバイス リセット（Device Reset）] ダイアログ ボックスで、次のタスクのいずれかを実行します。

- 選択したデバイスをシャット ダウンせずに再起動し、Cisco Unified Communications Manager に登録するには、[再起動（Restart）] をクリックします。

- デバイスをシャット ダウンしてから再起動するには、[リセット（Reset）] をクリックします。
- 操作を実行せずに [デバイス リセット（Device Reset）] ダイアログ ボックスを閉じるには、[閉じる（Close）] をクリックします。

管理者が SIP ダイヤルルールを設定して SIP を実行している電話機に適用すると、データベースから TFTP サーバに通知が送信されます。これによって、SIP を実行している電話機の新しい構成ファイルを作成できます。TFTP サーバは Cisco Unified Communications Manager に新しい構成ファイルについて通知し、更新された構成ファイルが電話機へ送られます。詳細については、SIP を実行する Cisco Unified IP Phone の「**TFTP サーバの設定**」を参照してください。

次のタスク

SIP ダイヤルルール設定と SIP 電話の同期 （303 ページ）

SIP ダイヤルルール設定と SIP 電話の同期

SIP 電話機と設定が変更された SIP ダイヤルルールを同期するには、次の手順を実行します。

始める前に

SIP ダイヤルルールのリセット （302 ページ）

手順

Step 1 Cisco Unified Communications Manager Administration から、**[コールルーティング（Call Routing）]** > **[ダイヤルルール（Dial Rules）]** > **[SIPダイヤルルール（SIP Dial Rules）]**.を選択します。

Step 2 [SIP ダイヤルルールの検索と一覧表示（Find and List SIP Dial Rules）] ウィンドウで、[検索（Find）] をクリックし、適切な SIP 電話機を同期する既存の SIP ダイヤルルールを選択します。

Step 3 追加の設定変更を行い、[SIP ダイヤルルールの設定（SIP Dial Rule Configuration）] で [保存（Save）] をクリックします。

Step 4 [設定の適用（Apply Config）] をクリックします。

Step 5 **[OK]** をクリックします。

ダイヤルルールの優先順位の変更

[ダイヤルルールの設定（Dial Rule Configuration）] ウィンドウでダイヤルルールの優先順位を追加およびソートするには、次の手順を実行します。

手順

Step 1 Cisco Unified Communications Manager の管理から、**[コールルーティング（Call Routing）] > [ダイヤルルール（Dial Rules）]** を選択します。

Step 2 次のいずれかを選択します。

- **[アプリケーション ダイヤル ルール（Application Dial Rules）]**
- **[ディレクトリ検索ダイヤルルール（Directory Lookup Dial Rules）]**
- **[SIP ダイヤルルール（SIP Dial Rules）]**

Step 3 [検索と一覧表示（Find and List）] ウィンドウで、ダイヤルルールを選択し、ダイヤルルールの名前をクリックします。
[ダイヤルルールの設定（Dial Rule Configuration）] ウィンドウが表示されます。

Step 4 上矢印と下矢印を使用して、リスト内でダイヤルルールを上または下に移動します。

Step 5 順序の優先順位付けが完了したら、[保存（Save）] をクリックします。

連携動作と制限事項

SIP ダイヤルルールの連携動作

SIP ダイヤルルールの連携動作

Cisco Unified IP Phone	連携動作
SIP を実行している 7911、7941、7961、7970、7971	これらの電話機は、7940_7960_OTHER ダイヤルルール パターンを使用します。キー プレス マークアップ言語（KPML）では、Cisco Unified Communications Manager に数字を 1 桁ごとに送信できます。SIP ダイヤルルールを使用すると、Cisco Unified Communications Manager に送信する前に、電話で数字のパターンをローカルに収集できます。SIP ダイヤルルールを設定しないと、KPML が使用されます。Cisco Unified Communications Manager のパフォーマンスを向上させるために（処理されるコール数の増加）、シスコは SIP ダイヤルルールを設定することをお勧めします。

Cisco Unified IP Phone	連携動作
SIP を実行している 7940 および 7960	これらの電話機は 7940_7960_OTHER ダイヤルルールパターンを使用し、KPML をサポートしていません。これらの電話機で SIP のダイヤルプランを設定していないと、ユーザは数字が Cisco Unified Communications Manager に送信されて処理される前に、指定された時間だけ待機する必要があります。その結果、実際のコールの処理が遅延します。

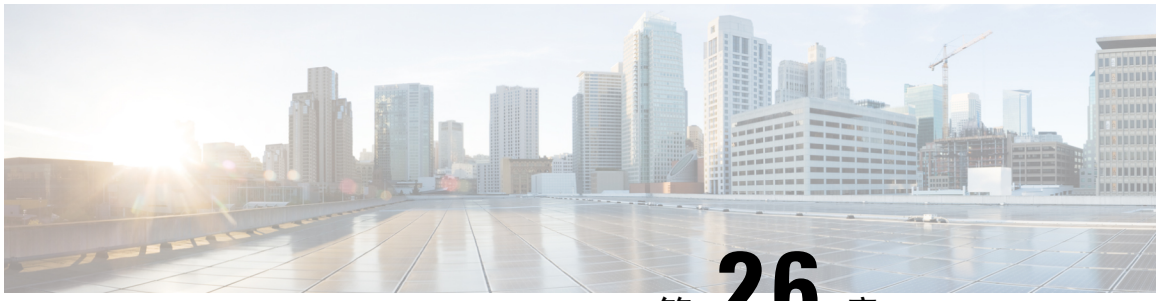
ディレクトリ検索ダイヤルルールの制限

ディレクトリ検索ダイヤルルールの制限

フィールド	制限事項
開始番号（Number Begins With）	このフィールドでは、数字と文字 +、*、# のみを使用できます。長さは 100 文字以内でなければなりません。
桁数（Number of Digits）	このフィールドは数字のみをサポートします。このフィールドの値は、パターン フィールドに指定されているパターンの長さより小さくすることはできません。
削除する合計桁数（Total Digits to be Removed）	このフィールドは数字のみをサポートします。このフィールドの値は、[桁数（Number of Digits）] フィールドの値より大きくすることはできません。
プレフィックス パターン（Prefix with Pattern）	このフィールドでは、数字と文字 +、*、# のみを使用できます。長さは 100 文字以内でなければなりません。 （注） 1 つのダイヤルルールの [削除する合計桁数（Total Digits to be Removed）] フィールドと [プレフィックス パターン（Prefix With Pattern）] フィールドの両方を空白にすることはできません。

第 III 部

アプリケーションの統合



第 26 章

シスコ アプリケーションの統合

Cisco Unity Connection

ボイスメールとメッセージングのシステムを設定する時には、ユーザの追加、機能の有効化、Cisco Unified Communications Manager と Cisco Unity Connection との統合の各オプションに注意します。

Cisco Unity Communications Manager と統合されると、Cisco Unity Connection (ボイスメールおよびメッセージングシステム) は、AXL サービスまたは LDAP 統合を使用して手動で設定するユーザにボイスメッセージ機能を提供します。メールボックスにボイスメッセージを受信すると、ユーザの電話機にメッセージ受信のライトが点灯します。ユーザは内線または外線通話でボイスメッセージ システムにアクセスして、メッセージの取得、聞き取り、返信、転送、および削除ができます。

お客様のシステムは、直接接続されたメッセージシステムとゲートウェイベースのメッセージシステムをサポートしています。直接接続された音声メッセージシステムは、パケットプロトコルを使用してCisco Unified Communications Managerと通信します。ゲートウェイベースのボイスメッセージ システムは、シスコ ゲートウェイに接続するアナログまたはデジタル トランクを使用してCisco Unified Communications Managerに接続します。

Unified Communications Manager と Cisco Unity Connection を統合すると、ユーザに次の機能を設定できます。

- パーソナル グリーティングへの自動転送
- 通話中グリーティングへの自動転送

- 発信者 ID
- 容易なメッセージアクセス（ユーザはIDを入力しなくてもメッセージを取得できます。Cisco Unity Connectionでは、通話発信元の内線番号に基づいてユーザを識別します。パスワードが必要になる場合があります）
- 識別されたユーザのメッセージ（Cisco Unity Connectionでは、転送された内線通話中にメッセージを残したユーザを、通話発信元の内線番号に基づいて自動的に識別します）
- メッセージ待機インジケータ（MWI）
- Cisco Unified Communications Manager と Cisco Unity Connection サーバ間のセキュアな SIP トランクの統合の設定には、Cisco Unified Communications Manager クラスタが混合モードで設定されている必要があります。

Cisco Unified Communications Manager と Cisco Unity Connection は、次のいずれかのインターフェイスを介して連携します。

- SIP トランク：SIP を使用して Cisco Unity Connection と Unified Communications Manager を統合できます。SIPは、従来の統合に含まれている複数のSCCPポートではなく、Unity Connectionサーバにつき1個のトランクを使用します。SIPインテグレーションでは、ボイスメールポートとメッセージ待機インジケータ (MWI) のディレクトリ番号を設定する必要がなくなります。
- SCCPプロトコル：音声メールポートを作成することで、インタフェースを直接接続された音声メッセージシステムとして構成できます。これらは、Unified CommunicationsManagerとCisco Unity Connectionとの間にリンクを確立します。

  ボイスメッセージ システムへの複数の同時コールを処理するには、複数のボイスメールポートを作成し、それらのポートを回線グループに割り当て、その回線グループをルート/ハントリストに割り当てます。

  Cisco Unified Communications Manager は、SCCP メッセージを生成します。 Cisco Unity Connection がそのメッセージを変換します。ボイスメールシステムは、メッセージ待機の on と off の番号をコールしてメッセージ受信兆候 (MWIs) を送信します。

  ボイスメール ポートやCisco Unity SCCPデバイスにセキュリティを設定すると、各デバイスが他のデバイスの証明書を受け付けた後、認証済みのデバイスに対してTLS接続（ハンドシェイク）が開きます。同様に、デバイスに暗号化を設定した場合、システムはデバイス間にSRTP ストリームを送信します。

  デバイスのセキュリティモードが認証または暗号化に設定されている場合、Cisco Unity TSP は、Cisco Unified Communications Manager の TLS ポートを介して Unified Communications Manager に接続します。セキュリティ モードが非セキュアの場合、Cisco Unity TSP は Cisco Unified Communications Manager の SCCP ポートを介して Unified Communications Manager に接続します。

Cisco Unity Connection をシステムに統合する設定の詳細については、『*Cisco Unity Connection* 向け *Cisco Unified Communications Manager SCCP* インテグレーション ガイド』または『*Cisco Unity Connection* 向け *Cisco Unified Communications Manager SIP* トランク インテグレーション ガイド』

（http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html）を参照してください。

PIN同期の有効化

PIN 同期を有効にし、エンドユーザが、エクステンション モビリティ、開催中の会議、モバイル コネクト、および Cisco Unity Connection ボイスメールに同じ PIN を使用してログインできるようにするには、次の手順を実行します。

（注） Cisco Unified Communications Manager パブリッシャ データベース サーバが実行されており、そのデータベースのレプリケーションが完了した場合のみ、Cisco Unity Connection と Cisco Unified Communications Manager 間の PIN の同期に成功します。Cisco Unity Connection で PIN の同期に失敗すると、次のエラーメッセージが表示されます。「CUCMで暗証番号のアップデートに失敗しました。（Failed to update PIN on CUCM.）原因：PIN の取得中にエラーが発生しています。（Reason: Error getting the pin.）」

PIN 同期が有効で、エンドユーザーが PIN を変更した場合は、Cisco Unified Communications Manager で PIN を更新します。この現象は、少なくとも 1 つの構成済みの Unity Connection アプリケーション サーバで、PIN の更新が成功している場合に発生します。

（注） PIN の同期を有効にするには、機能が正常に有効化された後で、管理者がユーザに各自の PIN を変更するよう強制する必要があります。

始める前に

この手順では、すでにアプリケーションサーバが Cisco Unity Connection のセットアップに接続されていることを前提としています。使用していない場合、新しいアプリケーションサーバを追加する方法については、「関連項目」を参照してください。

PIN 同期機能を有効にするには、まず [Cisco Unified OSの管理（Cisco Unified OS Administration）] ページから Cisco Unified Communications Manager tomcat-trust に、有効な証明書をアップロードする必要があります。証明書をアップロードする方法の詳細については、「Cisco Unified Communications Manager アドミニストレーション ガイド」（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）の「セキュリティ証明書の管理」の章を参照してください。

Cisco Unity Connection サーバのユーザ ID は、Cisco Unified Communications Manager のユーザ ID と一致する必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]>[アプリケーションサーバ（Application Servers）]** を選択します。

Step 2 Cisco Unity Connection をセットアップするアプリケーション サーバを選択します。

Step 3 [エンドユーザのPIN同期（Enable End User PIN Synchronization）] チェックボックスをオンにします。

Step 4 [保存（Save）] をクリックします。

関連トピック

アプリケーション サーバの設定

Cisco Expressway

Cisco Unified Communications Manager は Cisco Expressway と統合して、Cisco Unified Communications Mobile & Remote Access を提供します。Cisco Unified Communications の Mobile & Remote Access は Cisco Collaboration Edge アーキテクチャの中核を成します。Cisco Jabber などのエンドポイントが企業ネットワーク外にある場合に、Cisco Unified Communications Manager（Unified CM）への登録、呼制御、プロビジョニング、メッセージング、およびプレゼンスの機能を使用することができるようになります。Expressway は、Unified CM 登録にセキュアなファイアウォール トラバーサルと回線側サポートを提供します。

ソリューション全体で、次の機能が提供されます。

- オフプレミス アクセス：ネットワーク外で、Cisco Jabber および EX/MX/SX シリーズ クライアントに一貫性のあるエクスペリエンスを提供
- セキュリティ：セキュアな企業間（B2B）通信
- クラウドサービス：エンタープライズクラスの柔軟性と拡張性に優れたソリューションにより、Webex の統合とさまざまなサービスプロバイダーに対応
- ゲートウェイおよび相互運用性サービス：メディアおよびシグナリングの正規化、標準以外のエンドポイントのサポート。

導入の詳細については、『*Cisco Expressway* 経由の *Mobile and Remote Access* 導入ガイド』（https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html）を参照してください。

Cisco Emergency Responder

Cisco Emergency Responder（Emergency Responder）は、緊急コールに効率的に応答したり、緊急コールの処理について地方自治体の規定を順守したりできるように、テレフォニー ネットワーク

で緊急コールを管理するのに役立ちます。北米では、これらの地方条例は「Enhanced 911（E911）」と呼ばれています。同様の規定が他の国やロケールに存在します。

緊急コールに関する条例は、国、地域、州、または都市圏の中でも場所によって異なることがあるため、Emergency Responder は、特定のローカル要件に併せて緊急コール設定を指定できる柔軟性を備えています。ただし、条例は場所によって異なり、セキュリティ要件は会社によって異なるため、Emergency Responder を展開する前に、自社のセキュリティ上のニーズと法的なニーズを調査する必要があります。

Cisco Emergency Responder をインストールして Cisco Unified Communications Manager と統合する方法の詳細については、『*Cisco Emergency Responder* アドミニストレーション ガイド』（https://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-maintenance-guides-list.html）を参照してください。

Cisco Unified Communications Manager での機能のサポート

Cisco Unified Communications Manager の次の機能は、Cisco Emergency Responder との統合をサポートしています。Cisco Unified Communications Manager でこれらの機能を設定する方法の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）を参照してください。

- ロケーション認識
- 緊急ハンドラ

Cisco Paging Server

Cisco Unified Communications Manager は、Cisco Paging Server と統合して Cisco IP Phone やさまざまなエンドポイントに基本的なページング サービスを提供するように設定できます。Cisco Paging Server 製品は、InformaCast 仮想アプライアンスを介して提供され、次の導入オプションを提供します。

- 基本的なページング：Cisco IP Phone に対して電話間およびグループでのライブオーディオページングを提供します。システムのすべてのユーザは、基本的なページの確立と受信に参加できます。
- 高度な通知：すべての機能を備えた緊急通知ソリューションを提供します。これにより、テキストと、ライブまたは事前に録音されたオーディオメッセージを使用して、無制限の数の電話機に到達できます。

Cisco Paging Server の詳細およびドキュメントについては、https://www.cisco.com/c/en/us/products/unified-communications/paging-server/index.html を参照してください。

構成

Cisco Unified Communications Manager の基本ページングまたは高度な通知の設定方法の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「ページング」の章を参照してください。

Cisco Unified Contact Center Enterprise

Cisco Unified Contact Center Enterprise（Unified CCE）をシステムで使用して、インテリジェントコールルーティング、ネットワークとデスクトップ間のコンピュータ/テレフォニーインテグレーション（CTI）、およびIPネットワークを介したコンタクトセンターエージェントへのマルチチャネル コンタクト管理を統合します。Unified CCE は、ソフトウェア IP の自動コール配布 (ACD) を Cisco Unified Communications と組み合わせたもので、詳細な分散型の連絡先センターを迅速に導入できます。

Unified CCE をシステムに統合するための設定方法の詳細については、『*Cisco Unified Contact Center Enterprise* 設置およびアップグレードガイド』（http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html）を参照してください。

Cisco Unified Contact Center Express

Cisco Unified Contact Center Express（Unified CCX）は、シングルまたはデュアルサーバの導入において、パッケージ化された大規模なコンタクトセンターの機能をシステムに提供します。Unified CCX は、最大 400 人の同時エージェント、42 人のスーパバイザ、150 のエージェントグループ、および 150 のスキルグループに対応するように拡張できます。また、電子メール、チャット、発信コール、着信コール、ワークフォース最適化、およびレポート機能が含まれています。

Unified CCX は、Unified CCX に代わってすべてのコンタクトセンターのコールを管理する Unified Communications Manager と連携します。コールがヘルプデスクに送信されると、コールシステムは、その番号が Unified CCX アプリケーションサーバを宛先としていることを認識します。この設定では、Unified CCX が着信コールを受信し、ダイヤルした内線番号に基づいて要求を処理します。スクリプトは、番号を収集し、必要に応じて、発信者からの情報を使用して適切なエージェントを選択します。割り当てられたエージェントが利用できない場合、そのコールは適切なキューに入れられ、録音されたメッセージまたは音楽が発信者にストリーミングされます。エージェントが対応可能になるとすぐに、Unified CCX はそのエージェントの電話を鳴らすように Unified Communications Manager に指示します。

エージェントが電話に出ると、関連するコールコンテキストがそのエージェントのデスクトップアプリケーションに提供されます。この手順により、顧客をサポートするための適切な情報がエージェントに表示されます。

Unified CCE をシステムに統合するための設定方法の詳細については、『*Cisco Unified CCX* アドミニストレーション ガイド』（http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-installation-and-configuration-guides-list.html）を参照してください。

高度な QoS APIC-EM コントローラ

APIC EM は、ネットワークトラフィックを集中管理するためのシステムを提供しているため、ネットワークの輻輳がある場合でも、常に通信を維持できるようになっています。Cisco Unified Communications Manager を設定して、APIC-EM コントローラを使用し SIP メディアフローを管理するように設定すると、次のような利点がもたらされます。

- QoS 管理を一元化し、エンドポイントによる DSCP 値の割り当てが不要になります。
- メディアフローごとに異なる QoS 処理を適用できます。たとえば、ネットワーク帯域幅が少ない場合でも、基本的な音声通信が常に維持されるように、オーディオの優先順位を付けることができます。
- SIP プロファイルの外部 QoS 設定では、APIC-EM を使用するようにユーザを設定できます。たとえば、Cisco Jabber ユーザは APIC-EM を使用してメディアフローを管理し、一方で Cisco Unified IP Phone ユーザは Cisco Unified Communications Manager の DSCP 設定を使用できます。

設定の詳細

APIC_EM コントローラと統合するように Cisco Unified Communications Manager を設定する方法など、詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「APIC-EM コントローラによる QoS の設定」の章を参照してください。

Cisco WebDialer サーバの設定

[WebDialersの一覧（List of WebDialers）] サービスパラメータの代わりに Cisco WebDialer アプリケーションサーバを設定して、ユーザが入力できる文字数を制限します。[アプリケーションサーバの設定（Application Server Configuration）] ウィンドウで Cisco WebDialer アプリケーションサーバを追加すると、Cisco WebDialer Web サービスの [サービスパラメータの設定（Service Parameter Configuration）] ウィンドウで、そのサーバが [WebDialersの一覧（List of WebDialers）] フィールドに表示されます。Cisco WebDialer の設定の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）を参照してください。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]>[アプリケーションサーバ（Application Server）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [アプリケーションサーバタイプ（Application Server Type）] ドロップダウンリストから、[Cisco Web Dialer] を選択し、[次へ（Next）] をクリックします。

Step 4 [ホスト名/IPアドレス（Host name/IP Address）] フィールドに、WebDialer サーバのホスト名または IP アドレスを入力します。

Step 5 [リダイレクタノード（Redirector Node）] ドロップダウンリストから、[<なし>（< None >）] または特定の Unified Communications Manager ノードを選択します。

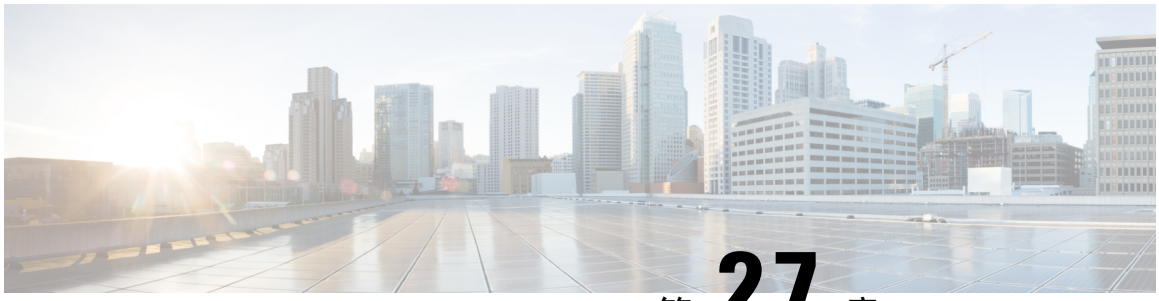
[<なし>（< None >）] の場合は、WebDialer サーバがすべてのノードに適用されることを示します。

Step 6 [保存（Save）] をクリックします。

Step 7 Cisco Unified Serviceability で **[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択します。

Step 8 [Cisco WebDialer Webサービス（Cisco WebDialer Web Service）] ラジオボタンをクリックします。

Step 9 [再起動（Restart）] をクリックします。



第 27 章

CTI アプリケーションの設定

CTI アプリケーションの概要

コンピュータテレフォニーインテグレーション（CTI）を使用して、コンピュータ処理機能を活用しながら、電話コールの発信、受信、および管理を行うことができます。CTI アプリケーションを使用すると、発信者 ID を使用してデータベースから顧客情報を取得したり、対話式音声自動応答 (IVR) で収集した情報を使用して、顧客のコールをその情報とともに、適切なカスタマーサービス担当者にルートすることができます。

コールのメディアをルートポイントで終端するアプリケーションは、コール単位でコールのメディアおよびポートを指定する必要があります。CTI アプリケーションは、静的な IP アドレスまたは動的な IP アドレスとポート番号を使用して、CTI ポートおよび CTI ルートポイントでメディアを終了させることができます。

この章では、Cisco Unified Communications Manager を CTI アプリケーションとともに動作するように設定する方法について説明します。特定のアプリケーションの設定方法については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。

利用可能な Cisco CTI アプリケーションの一部を次に示します。

- Cisco IP Communicator：コンピュータをフル機能の電話機に変えるデスクトップ アプリケーションです。コールトラッキング、デスクトップ コラボレーション、オンライン電話帳からのワンクリックダイヤルなどの機能を利用できます。
- Cisco Unified Communications Manager 自動応答：Unified Communications Manager と連携して、特定の内線電話番号でコールを受信し、発信者が適切な内線番号を選択できるようにします。
- Cisco Web Dialer：Cisco Unified IP Phone ユーザは ウェブ およびデスクトップ アプリケーションからコールを発信できます。
- Cisco Unified Communications Manager Assistant：マネージャとそのアシスタントがより効果的に協力して作業できます。この機能は、コールルーティング サービス、マネージャおよびア

シスタント用の電話機拡張機能、および主にアシスタントが使用するアシスタント コンソール インターフェイスから構成されています。

（注） どの Unified Communications Manager CTI アプリケーションが SIP IP Phone をサポートしているかを確認するには、アプリケーション固有のマニュアルを参照してください。

CTI ルートポイントの概要

CTI ルートポイント仮想デバイスは、アプリケーションによって制御されるリダイレクトのための複数の同時コールを受信できます。ユーザがアプリケーションにアクセスするためにコールできる CTI ルートポイント上で 1 つ以上の回線を設定できます。アプリケーションはルートポイントでコールに応答することができ、コールを CTI ポートまたは IP Phone にリダイレクトすることもできます。CTI アプリケーションがリダイレクト API を使用してコールをリダイレクトすることを要求した場合、Cisco Unified Communications Manager は、リダイレクト先の通話者のために回線/デバイス コーリングサーチスペースの設定を使用します。

CTI ルートポイントでは、次のことができます。

- コールへの応答
- 複数のアクティブなコールの発信および受信
- コールのリダイレクト
- コールの保留
- コールの保留解除
- コールのドロップ

Cisco Unified Communications Manager の CTI 冗長性

クラスタ内の Unified Communications Manager ノードに障害が発生した場合、CTIManager は、影響を受けた CTI ポートおよびルートポイントを別の Unified Communications Manager ノードで開き直すことによって、これらのデバイスを回復します。アプリケーションによって電話デバイスが開かれていた場合、その電話が別の Unified Communications Manager にフェールオーバーしたときに CTIManager がその電話を開き直します。Cisco IP Phone が別の Unified Communications Manager にフェールオーバーしない場合、CTIManagerは、その電話または電話機の回線を開くことができません。CTIManager は、デバイスプールに割り当てられている Unified Communications Manager グループを使用して、アプリケーションによって開かれた CTI デバイスと電話を回復するのにどの Unified Communications Manager を使用するかを決定します。

CTIManager 上の CTI 冗長性

CTIManager に障害が発生した場合、その CTIManager に接続されているアプリケーションは、これらのデバイスを別の CTIManager 上で再度開くことによって、影響を受けたリソースを回復できます。アプリケーションは、そのアプリケーションの設定時にプライマリとバックアップとして定義された CTIManager に基づいて、どの CTIManager を使用するかを決定します（そのアプリケーションによってサポートされている場合）。アプリケーションは、新しい CTIManager に接続すると、以前に開かれたデバイスと回線を再度開くことができます。アプリケーションは、電話が新しい Unified Communications Manager にリホームする前であれば Cisco IP Phone を開き直すことができますが、リホームが完了するまではその電話を制御できません。

（注） プライマリ CTIManager が作動状態に戻っても、アプリケーションはその CTIManager にリホームしません。アプリケーションがプライマリ CTIManager にフォールバックするのは、そのアプリケーションを再起動するか、またはバックアップ CTIManager に障害が発生した場合です。

アプリケーション障害の CTI 冗長性

アプリケーション（TAPI/JTAPI、または CTIManager に直接接続されているアプリケーション）に障害が発生した場合、CTIManager はそのアプリケーションを閉じ、CTI ポートおよびルートポイントでまだ終了していないコールを、設定された Call Forward On Failure（CFOF）番号にリダイレクトします。CTIManager はまた、そのアプリケーションが回復してこれらのデバイスを再登録するまで、これらの CTI ポートおよびルートポイントへの後続のコールを、設定された Call Forward No Answer（CFNA）番号にルーティングします。

CTI アプリケーションの前提条件

CTI アプリケーション用に Cisco Unified Communications Manager を設定する前に、デバイスプールを設定しておく必要があります。

CTI アプリケーションごとに IP Phone を追加して設定します。IP 電話を追加して設定する方法の詳細については、「Cisco Unified IP Phone」を参照してください。

CTI アプリケーションを使用するエンド ユーザとアプリケーションユーザーを設定する

コンピュータ テレフォニー統合（CTI）では、IPv4 アドレスと IPv6 アドレスをサポートできる JTAPI および TAPI インターフェイスを通して IP アドレス情報が提供されます。IPv6 アドレスをサポートする必要がある場合は、アプリケーションが IPv6 をサポートする JTAPI/TAPI クライアントインターフェイスバージョンを使用していることを確認してください。

CTI アプリケーションの設定タスクフロー

CTI アプリケーション用に Cisco Unified Communications Manager を設定するには、次のタスクに従います。

手順

	コマンドまたはアクション	目的
Step 1	CTIManager サービスのアクティブ化（321 ページ）	アクティブになっていない場合、適切なサーバで CTIManager サービスをアクティブにします。
Step 2	CTIManager と Cisco Unified Communications Manager のサービスパラメータの設定（321 ページ）	CTI のスーパープロバイダー機能と連携して使用される、CTIManager のクラスタ全体の拡張サービスパラメータを設定します。
Step 3	CTI ルートポイントを設定するには、次の手順を実行します。 • CTI ルートポイントの設定（322 ページ） • 新しいコール受け付けタイマーの設定（323 ページ） • 同時アクティブ通話の設定（323 ページ） • CTI ルートポイントの同期化（324 ページ）	アプリケーション制御のリダイレクションに複数の同時コールを受信できる 1 つ以上の CTI ルートポイントの仮想デバイスを設定します。
Step 4	CTI デバイスの電話番号の設定（324 ページ）	CTI デバイスの電話番号を設定します。
Step 5	デバイスとグループの関連付け（325 ページ）	アプリケーションユーザーとエンドユーザーがアプリケーションで使用するすべてのデバイスを、適切な Cisco Unified Communications Manager グループに関連付けます（デバイスプール経由）。
Step 6	エンドユーザとアプリケーションユーザの追加（325 ページ）	エンドユーザとアプリケーションユーザを [標準CTIを有効にする（Standard CTI Enabled）] ユーザグループに追加して、Cisco Unified Communications Manager システムに設定されている CTI 制御可能なデバイスを CTI アプリケーションで制御できるようにします。

	コマンドまたはアクション	目的
Step 7	（オプション） アプリケーション障害時の CTI 冗長性の設定 （327 ページ）	CTIManager が、連続する 2 回の間隔内でアプリケーションからメッセージを受信するまで待機する間隔を定義します。

CTIManager サービスのアクティブ化

手順

Step 1 Cisco Unified Serviceability で、**[ツール（Tools）]** > **[サービスのアクティブ化（Service Activation）]** を選択します。

Step 2 [サーバ（Server）] ドロップダウンリストからノードを選択します。

Step 3 [CM サービス（CM Services）] セクションで、[Cisco CTIManager] チェックボックスをオンにします。

Step 4 [保存（Save）] をクリックします。

CTIManager と Cisco Unified Communications Manager のサービスパラメータの設定

CTI のスーパープロバイダー機能と連携して使用される、CTIManager のクラスタ全体の拡張サービスパラメータを設定します。

（注） 設定した限度を超えた場合、CTI がアラームを生成しますが、アプリケーションは追加デバイスの処理を続行します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 [サーバ（Server）] ドロップダウンリストからノードを選択します。

Step 3 [サービス（Service）] ドロップダウンリストから [Cisco CTIManager（アクティブ）（Cisco CTIManager（Active））] を選択します。

Step 4 [サービスパラメータの設定（Service Parameter Configuration）] ウィンドウで、[詳細設定（Advanced）] をクリックします。

Step 5 [プロバイダーあたりの最大デバイス数（Maximum Devices Per Provider）] フィールドに、単一の CTI アプリケーションが開くことのできるデバイスの最大数を入力します。デフォルトは 2000 デバイスです。

Step 6 [ノードあたりの最大デバイス数（Maximum Devices Per Node）] フィールドに、Unified Communications Manager システム内の任意の CTIManager ノード上ですべての CTI アプリケーションが開くことのできるデバイスの最大数を入力します。デフォルトは 800 デバイスです。

Step 7 [保存（Save）] をクリックします。

CTI ルートポイントの設定タスクフロー

手順

	コマンドまたはアクション	目的
Step 1	CTI ルートポイントの設定（322 ページ）	新規の CTI ルートポイントを追加するか、既存のポイントを変更します。
Step 2	新しいコール受け付けタイマーの設定（323 ページ）	コールがルートポイントに到着したとき、アプリケーションが指定時間内に処理（受信、応答、リダイレクト）するように新しいコール受け入れタイマーを設定します。
Step 3	同時アクティブ通話の設定（323 ページ）	ルートポイントの同時アクティブ コール数を設定します。
Step 4	**オプション**：CTI ルートポイントの同期化（324 ページ）	CTI ルートポイントを最新の設定変更と同期すると、割り込みを最小限に抑えながら、適用されていない構成設定を適用できます。（たとえば、影響を受けるデバイスの一部でリセットまたは再起動を行う必要がない場合があります）。

CTI ルートポイントの設定

新規の CTI ルートポイントを追加するか、既存のポイントを変更します。

手順

Step 1 Cisco Unified CM Administration から **[デバイス（Device）] > [CTIルートポイント（CTI Route Point）]** の順にクリックします。

Step 2 次のいずれかの操作を実行します。

- [新規追加（Add New）] をクリックして、新しいゲートウェイを追加します。

- 既存の CTI ルートポイントの設定を変更するには、[検索（Find）] をクリックし、結果のリストから CTI ルートポイントを選択して、検索条件を入力します。

Step 3 [CTI ルートポイントの設定 （CTI Route Point Configuration）] ウィンドウで各フィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 4 [保存（Save）] をクリックします。

新しいコール受け付けタイマーの設定

コールがルートポイントに到着したとき、アプリケーションが指定時間内に処理（受信、応答、リダイレクト）するように新しいコール受け入れタイマーを設定します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 [サーバ（Server）] ドロップダウンリストからノードを選択します。

Step 3 [サービス（Service）] ドロップダウンリストから [Cisco CallManager（アクティブ）（Cisco CallManager (Active)）] を選択します。

Step 4 [CTIの新しいコール受け付けタイマー（CTI New Call Accept Timer）] フィールドで、コールの応答を許可する時間を指定します。デフォルト値は 4 です。

Step 5 [保存（Save）] をクリックします。

同時アクティブ通話の設定

ルートポイントの同時アクティブ コール数を設定します。

（注） TAPI アプリケーションを使用し、Cisco CallManager Telephony Service Provider（TSP）を使用して CTI ポート デバイスを制御することを計画している場合は、CTI ポート デバイスごとに 1 つの回線を設定するだけで済みます。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [電話番号（Directory Number）]** をクリックします。

Step 2 [電話番号の設定（Directory Number Configuration）] ウィンドウで、[新規追加（Add New）] をクリックします。

Step 3 必須フィールドに入力します。

Step 4 [保存（Save）] をクリックします。

CTI ルートポイントの同期化

CTI ルートポイントを最新の設定変更と同期すると、割り込みを最小限に抑えながら、適用されていない構成設定を適用できます。（たとえば、影響を受けるデバイスの一部でリセットまたは再起動を行う必要がない場合があります）。

手順

Step 1 Cisco Unified CM Administration から **[デバイス（Device）] > [CTIルートポイント（CTI Route Point）]** の順にクリックします。

Step 2 [CTIルートポイントの検索と一覧表示（Find and List CTI Route Points）] ウィンドウで、[検索（Find）] をクリックして、CTI ルートポイントの一覧を表示します。

Step 3 同期させるCTIルートポイントの横にあるチェックボックスをオンにします。ウィンドウ内のCTIルートポイントをすべて選択するには、検索結果表示のタイトルバーにあるチェックボックスをオンにします。

Step 4 [選択項目への設定の適用（Apply Config to Selected）] をクリックします。

Step 5 **[OK]** をクリックします。

CTI デバイスの電話番号の設定

CTI デバイスの電話番号を設定します。

手順

Step 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [電話番号（Directory Number）]** の順に選択します。

Step 2 [電話番号の検索/一覧表示（Find and List Directory Numbers）] ウィンドウで、[新規追加（Add New）] をクリックします。

Step 3 [電話番号の設定（Directory Number Configuration）] ウィンドウで、必要なフィールドを入力します。

Step 4 [保存（Save）] をクリックします。

デバイスとグループの関連付け

アプリケーションユーザーとエンドユーザーがアプリケーションで使用するすべてのデバイスを、適切な Cisco Unified Communications Manager グループに関連付けます（デバイスプール経由）。

手順

Step 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）] > [アプリケーションユーザー（Application User）]** をクリックします。

Step 2 [アプリケーションユーザの検索/一覧表示（Find and List Application Users）] ウィンドウで、[新規追加（Add New）] をクリックします。[アプリケーションユーザーの設定（Application User Configuration）] ウィンドウが表示されます。

Step 3 [デバイス情報（Device Information）] ペインで、[使用可能なデバイス（Available Devices）] リストから [制御するデバイス（Controlled Devices）] リストに移動して、デバイスを関連付けます。

Step 4 [保存（Save）] をクリックします。

Step 5 エンドユーザのデバイスを関連付けるには、**[ユーザの管理（User Management）] > [エンドユーザ（End User）]** をクリックします。

Step 6 ステップ 2 ～ 4 を繰り返します。

エンドユーザとアプリケーションユーザの追加

エンドユーザとアプリケーションユーザを [標準CTIを有効にする（Standard CTI Enabled）] ユーザグループに追加して、Cisco Unified Communications Manager システムに設定されている CTI 制御可能なデバイスを CTI アプリケーションで制御できるようにします。

手順

Step 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アクセス制御グループ（Access Control Group）]** をクリックします。

Step 2 [アクセス制御グループの検索と一覧表示（Find and List Access Control Groups）] ウィンドウで、[検索（find）] をクリックして、アクセス制御グループの現在のリストを表示します。

Step 3 [標準 CTI を有効にする（Standard CTI Enabled）] をクリックすると、このグループの [アクセス制御グループの設定（Access Control Group Configuration）] ウィンドウが表示されます。すべての CTI ユーザが [標準 CTI を有効にする（Standard CTI Enabled）] ユーザ グループに含まれることを確認します。使用可能なグループとその機能の完全な一覧については、「アクセス制御グループ設定のオプション」を参照してください。

Step 4 エンド ユーザを追加する場合は、[グループにエンド ユーザを追加（Add End Users to Group）] をクリックします。アプリケーションユーザーを追加する場合は、[アプリケーションユーザーをグループに追加（Add App Users to Group）] をクリックします。

Step 5 [Find（検索）] をクリックして現在のユーザの一覧を表示します。

Step 6 [標準 CTI を有効にする（Standard CTI Enabled）] ユーザ グループに割り当てるユーザのチェックボックスをオンにします。

Step 7 [選択項目の追加（Add Selected）] をクリックします。

アクセス制御グループの設定オプション

（注） CTI アプリケーションは、割り当て先の指定されたユーザグループをサポートしている必要があります。

（注） Standard CTI Allow Control of All Devices ユーザ グループに関連付けられているユーザは、Standard CTI Secure Connection ユーザ グループにも関連付けることをお勧めします。

（注） 適切に機能させるには、次の表に示すすべてのロールの **[制御対象デバイス（Controlled Devices）]** の下に特定のデバイスを追加する必要があります。

フィールド	説明
標準 CTI 通話モニタリング許可（Standard CTI Allow Call Monitoring）	このユーザ グループでは、アプリケーションがコールをモニタできます。
標準 CTI コールパークモニタリング許可（Standard CTI Allow Call Park Monitoring）	このユーザ グループでは、コールがすべての通話パークディレクトリの番号にパーク/パーク解除されるとき、アプリケーションが通知を受信できます。
[標準 CTI 通話録音許可（Standard CTI Allow Call Recording）	このユーザ グループでは、アプリケーションがコールを記録できます。
標準 CTI 発信者番号の変更許可（Standard CTI Allow Calling Number Modification）	このユーザ グループでは、サポートされている CTI アプリケーションの発信側番号をアプリケーションが変更できます。
標準 CTI によるすべてのデバイスの制御（Standard CTI Allow Control of All Devices）	このユーザ グループでは、システムの CTI 制御可能なデバイスをアプリケーションが制御またはモニタできます。
標準 CTI SRTP 重要素材の受信許可（Standard CTI Allow Reception of SRTP Key Material）	このユーザ グループでは、暗号化されたメディアのストリームの復号に必要な情報をアプリケーションが受け取ることができます。通常、このグループは記録およびモニタのために使用されます。

フィールド	説明
標準 CTI 対応（Standard CTI Enabled）	すべての CTI アプリケーションに必要なこのユーザ グループでは、アプリケーションが Cisco Unified Communications Manager に接続し、CTI の機能を利用できます。
標準 CTI セキュア接続（Standard CTI Secure Connection）	このグループに入るためには、アプリケーションが Cisco Unified Communications Manager にセキュア（TLS）な CTI 接続が可能で、Cisco Unified Communications Manager のクラスタのセキュリティが有効になっていることが必要です。

アプリケーション障害時の CTI 冗長性の設定

CTIManager が、連続する 2 回の間隔内でアプリケーションからメッセージを受信するまで待機する間隔を定義します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 [サーバ（Server）] ドロップダウンリストからノードを選択します。

Step 3 [サービス（Service）] ドロップダウンリストから、[Cisco CTI Manager（アクティブ）（Cisco CTIManager (Active)）] を選択します。

Step 4 **[サービスパラメータの設定（Service Parameter Configuration）]** ウィンドウで、**[詳細設定（Advanced）]** をクリックします。

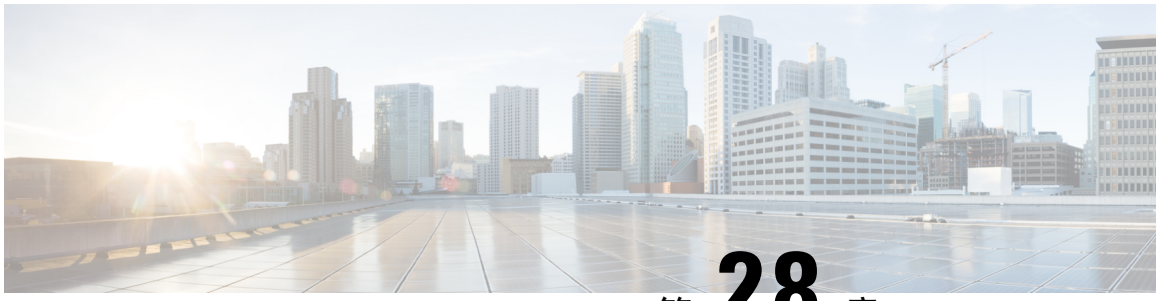
Step 5 **[アプリケーションハートビート最小間隔（Application Heartbeat Minimum Interval）]** フィールドに、最小間隔の時間を入力します。デフォルトは 5 です。

Step 6 **[アプリケーションハートビート最大間隔（Application Heartbeat Maximum Interval）]** フィールドに、最大間隔の時間を入力します。デフォルトは 3600 です。

Step 7 [保存（Save）] をクリックします。

第 IV 部

エンドユーザのプロビジョニング



第 28 章

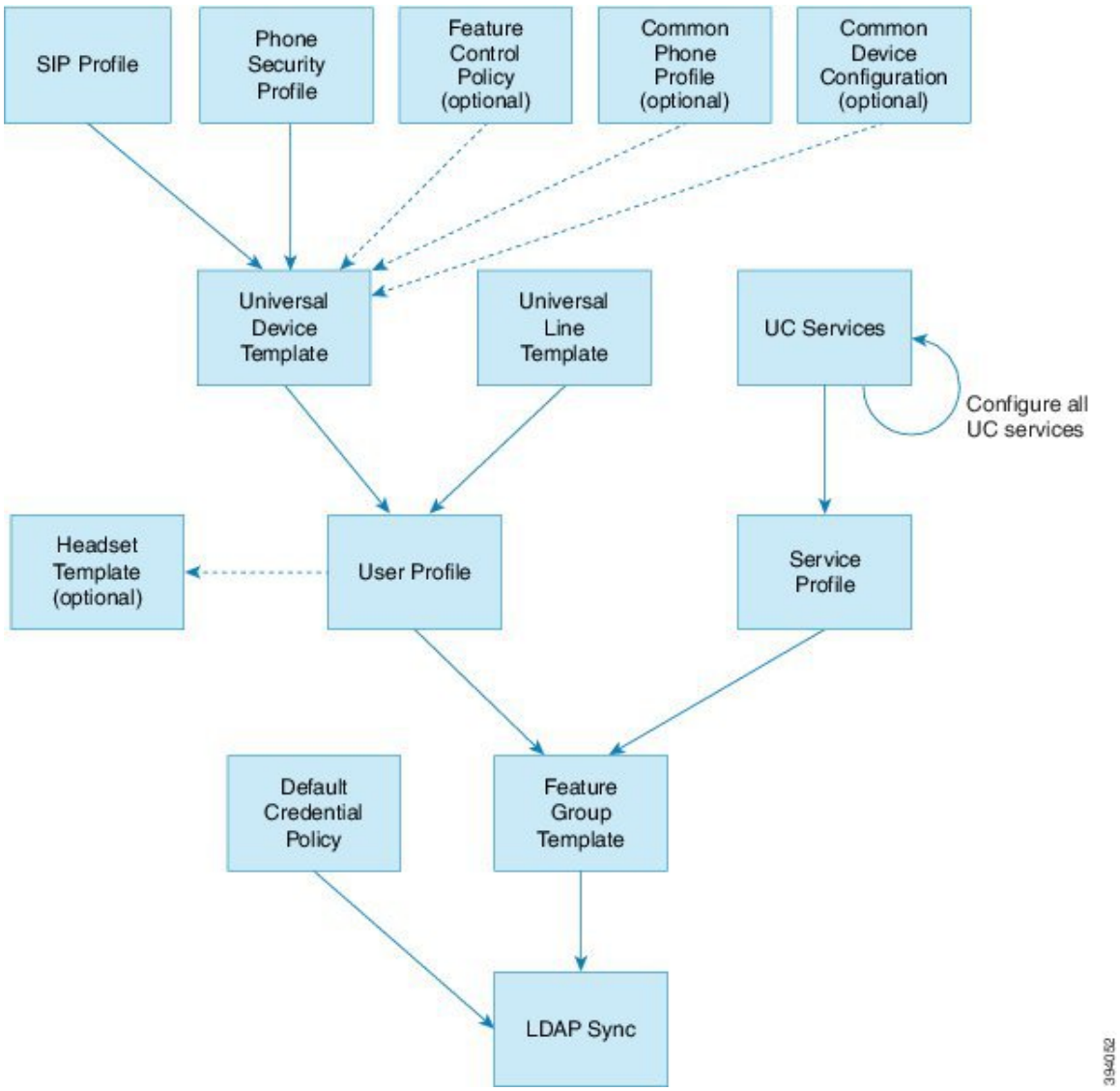
プロビジョニング プロファイルの設定

プロビジョニング プロファイルの概要

ユニファイドコミュニケーションマネージャには、新しいユーザに割り当てることができるプロファイルとテンプレートのセットが含まれています。これらのプロファイルと共通の設定を事前に設定した場合、新しいユーザをプロビジョニングしてデバイスを割り当てると、ユーザとデバイスが適用される設定に基づいて自動的に設定されます。

ユーザをプロビジョニングするときは、必要な設定が含まれているユーザプロファイルとサービスプロファイルにそれらを関連付けます。さらに、ユーザにデバイスを追加すると、そのユーザのユーザプロファイルに関連付けられているユニバーサル回線およびユニバーサルデバイステンプレートを使用して、デバイスと電話番号がすぐに設定されます。

次のプロファイルとテンプレートを使用して、ユーザのニーズに基づいて共通の設定をユーザとエンドポイントに適用できます。



プロビジョニング プロファイルのタスクフロー

プロビジョニングするユーザとデバイスが多数ある場合は、テンプレートを使用してユーザプロファイルとサービスプロファイルを設定し、特定のグループ (カスタマーサポートなど) のユーザに適用する共通の設定を行うことで、設定プロセスを簡素化できます。

ユーザをプロビジョニングするときは、必要な設定が含まれているユーザプロファイルとサービスプロファイルにそれらを関連付けます。さらに、ユーザにデバイスを追加すると、そのユーザのユーザプロファイルに関連付けられているユニバーサル回線およびユニバーサルデバイステンプレートを使用して、デバイスと電話番号がすぐに設定されます。

次のプロファイルとテンプレートを使用して、ユーザのニーズに基づいて共通の設定をユーザとエンドポイントに適用できます。

手順

	コマンドまたはアクション	目的
Step 1	SIP プロファイルの設定 （334 ページ）	展開する SIP エンドポイントに関連付けられる共通の SIP 設定をセットアップします。
Step 2	電話機のセキュリティ プロファイルの設定 （335 ページ）	プロビジョニングされたエンドポイントに割り当てるセキュリティプロファイルを設定します。TLS や TFTP 暗号化などの設定を割り当てます。
Step 3	機能管理ポリシーの作成 （336 ページ）	（**オプション**）このポリシーを使用すると、特定の機能を有効化して、電話機のソフトキーの外観を制御できます。
Step 4	共通の電話プロファイルの作成（337ページ）	（**オプション**）このプロファイルを使用して、TFTPデータと製品固有の設定のデフォルトを、エンドポイントのグループに割り当てることができるプロファイルに割り当てます。
Step 5	共通デバイス設定の構成 （338 ページ）	（**オプション**）エンドポイントにユーザ固有の設定と IPv6 設定を割り当てるには、この設定を使用します。
Step 6	ユニバーサル デバイス テンプレートの設定 （339 ページ）	このテンプレートには、新しくプロビジョニングされた電話機の設定に使用される共通の設定が含まれています。設定したプロファイルをこのテンプレートに割り当てることもできます。
Step 7	ユニバーサル回線テンプレートの設定 （340 ページ）	このテンプレートには、新しくプロビジョニングされた拡張機能を設定するために使用される共通の設定が含まれています。内線用のエンタープライズ番号および E.164 番号を設定することもできます。
Step 8	ユーザプロファイルの設定（340ページ）	デバイステンプレート、回線テンプレート、および新しくプロビジョニングされたユーザの共通設定を使用して、ユーザプロファイルを設定します。
Step 9	ヘッドセットテンプレートの設定 （342 ページ）	（**オプション**）Ciscoヘッドセットを使用して、設定したユーザプロファイルにヘッドセットテンプレートを割り当てる予定の場合。

	コマンドまたはアクション	目的
Step 10	UC サービスの設定 （343 ページ）	IM and Presence Service やディレクトリ サービスなどの UC サービスを設定します。
Step 11	サービス プロファイルの設定 （344 ページ）	プロビジョニングされたユーザに割り当てる UC サービスを含む、サービス プロファイルを作成します。
Step 12	機能グループ テンプレートの設定 （345 ページ）	LDAP 同期の場合、LDAP 同期されたユーザに割り当てることができる機能グループテンプレートにユーザプロファイルとサービスプロファイルを追加します。
Step 13	デフォルトのクレデンシャル ポリシーの設定 （346 ページ）	新しくプロビジョニングされたユーザに割り当てるクレデンシャルポリシーを設定します。

次のタスク

- 新しいユーザをプロビジョニングするための LDAP 同期の設定
- LDAP を展開していない場合は、一括管理を使用してユーザを一括でプロビジョニングできます。

SIP プロファイルの設定

共通 SIP 設定を使用して SIP プロファイルを設定するには、この手順を使用します。設定した SIP プロファイルは、SIP デバイスに割り当てることができます。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）][デバイスの設定（Device Settings）][SIP プロファイル（SIP Profile）]** を選択します。

Step 2 次のいずれかの手順を実行します。

- 既存のプロファイルを編集するには、[検索（Find）] をクリックし、SIP プロファイルを選択します。
- 新しいプロファイルを作成するには、[新規追加（Add New）] をクリックします。

Step 3 プロファイルの **[名前（Name）]** を入力します。

Step 4 URI ダイヤリングを展開する場合は、[ダイヤル文字列の解釈（Dial String Interpretation）] を設定して、コールをディレクトリ URI または電話番号として処理するかどうかをシステムに指示します。

Step 5 [電話で使用されるパラメータ（Parameters Used in Phone）] で DSCP 設定を指定して、このプロファイルを使用するコールのタイプに対する QoS 処理を定義します。

Step 6 （オプション）正規化スクリプトを割り当てる必要がある場合は、[正規化スクリプト（Normalization Script）] ドロップダウンリストからいずれかのデフォルトスクリプトを選択します。

（注） 独自のスクリプトを作成することもできます。詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。

Step 7 このプロファイルで IPv4 と IPv6 の両方のスタックを同時にサポートする場合は、[ANATの有効化（Enable ANAT）] チェックボックスをオンにします。

Step 8 ユーザがプレゼンテーションを共有できるようにするには、[BFCPを使用するプレゼンテーションの共有を許可（Allow Presentation Sharing using BFCP）] チェックボックスをオンにします。

Step 9 [SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウで残りのフィールドを入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 10 [保存（Save）] をクリックします。

電話機のセキュリティ プロファイルの設定

エンドポイントの TLS シグナリング、CAPF、ダイジェスト認証の要件などのセキュリティ機能を有効にする場合は、エンドポイントに適用できる新しいセキュリティプロファイルを設定する必要があります。

（注） デフォルトでは、プロビジョニングされたデバイスに SIP 電話セキュリティプロファイルを適用しない場合、デバイスは非セキュアプロファイルを使用します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [セキュリティ（Security）] > [電話セキュリティプロファイル（Phone Security Profile）]** の順に選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [電話のセキュリティプロファイルのタイプ（Phone Security Profile Type）] ドロップダウンリストから [ユニバーサルデバイステンプレート（Universal Device Template）] を選択し、デバイス テンプレートを使用してプロビジョニングする際に使用できるプロファイルを作成します。

（注） 必要に応じて、特定のデバイスモデルのセキュリティプロファイルを作成することもできます。

Step 4 プロトコルを選択します。

Step 5 [名前（Name）] フィールドにプロファイルの適切な名前を入力します。

Step 6 TLS シグナリングを使用してデバイスに接続する場合は、[デバイスのセキュリティモード（Device Security Mode）] を [認証済み（Authenticated）] または [暗号化（Encrypted）] に設定し、[トランスポートタイプ（Transport Type）] を [TLS] に設定します。

Step 7 （任意）電話でダイジェスト認証を使用する場合は、[OAuth認証の有効化（Enable OAuth Authentication）] チェックボックスをオンにします。

Step 8 （任意）暗号化された TFTP を使用する場合は、[TFTP暗号化設定（TFTP Encrypted Config）] チェックボックスをオンにします。

Step 9 [電話のセキュリティプロファイルの設定（Phone Security Profile Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 10 [保存（Save）] をクリックします。

機能管理ポリシーの作成

機能管理ポリシーを作成するには、次の手順に従います。このポリシーを使用して、特定の機能を有効化または無効化し、電話に表示されるソフトキーの外観を制御します。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[機能管理ポリシー（Feature Control Policy）]** を選択します。

Step 2 次のいずれかの操作を実行します。

- 既存のポリシーの設定を変更するには、検索条件を入力して **[検索（Find）]** をクリックし、結果のリストからポリシーを選択します。
- 新しいポリシーを追加するには、**[新規追加（Add New）]** をクリックします。

[機能管理ポリシーの設定（Feature Control Policy Configuration）] ウィンドウが表示されます。

Step 3 [名前（Name）] フィールドに機能管理ポリシーの名前を入力します。

Step 4 [説明（Description）] フィールドに、この機能管理ポリシーの説明を入力します。

Step 5 [機能管理セクション（Feature Control Section）] でリストされている各機能に対して、システムデフォルトをオーバーライドするか、次の設定を有効/無効にするかを選択します。

- デフォルトで有効な機能の設定を無効にする場合は、[デフォルトをオーバーライド（Override Default）] チェックボックスをオンにして、[設定を有効にする（Enable Setting）] チェックボックスをオフにします。
- デフォルトで無効な機能の設定を有効にする場合は、[デフォルトをオーバーライド（Override Default）] チェックボックスをオンにして、[設定を有効にする（Enable Setting）] チェックボックスをオンにします。

Step 6 [保存（Save）] をクリックします。

共通の電話プロファイルの作成

共通の電話プロファイルは、プロファイルを使用する電話の TFTP データと製品固有の設定のデフォルトを設定するために使用できるオプションのプロファイルです。

手順

Step 1 Cisco Unified CM Administration から、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）] メニューパスを選択して、共通の電話プロファイルを設定します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 プロファイルの **[名前（Name）]** を入力します。

Step 4 プロファイルの [説明（Description）] を入力します。

Step 5 このプロファイルを使用する電話に [機能管理ポリシー（Feature Control Policy） を設定する場合は、ドロップダウンリストからポリシーを選択します。

Step 6 [共通の電話プロファイルの設定（Common Phone Profile Configuration）] ウィンドウで、残りのフィールドを設定します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 7 [製品固有の設定レイアウト（Product-Specific Configuration Layout）] の下にあるフィールドを設定します。フィールドの説明については、[?] をクリックして、フィールド固有のヘルプを参照してください。

Step 8 （オプション）モバイルおよびリモートアクセスの電話機用に Interactive Connectivity Establishment（ICE）を有効にするには、次の手順を実行します。

a) [ICE] ドロップダウンを [有効（Enabled）] に設定します。

b) [デフォルト候補タイプ（Default Candidate Type）] を次のいずれかに設定します。

- [ホスト（Host）]：ホスト デバイスで IP アドレスを選択することで取得される候補。これはデフォルトです。
- [サーバ再帰（Server Reflexive）]：STUN 要求を送信することで取得される IP アドレスとポートの候補。多くの場合、これは NAT のパブリック IP アドレスを表している可能性があります。
- **[中継（Relayed）]**：TURN サーバから取得される IP アドレスとポートの候補。IP アドレスとポートは、メディアが TURN サーバを介して中継されるように、TURN サーバに常駐しています。

c) 残りの ICE フィールドを設定します。

Step 9 [保存（Save）] をクリックします。

共通デバイス設定の構成

共通デバイス設定は、任意指定のユーザ固有の機能属性で構成されます。IPv6 を導入している場合は、この設定を使用して SIP トランクまたは SCCP 電話に IPv6 優先設定を割り当てることができます。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通デバイス設定（Common Device Configuration）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 SIP トランク、SIP 電話または SCCP 電話の場合、[IPアドレッシングモード（IP Addressing Mode）] ドロップダウンリストの値を選択します。

- [IPv4 のみ（IPv4 Only）]—デバイスはメディアやシグナリングに IPv4 アドレスだけを使用します。
- [IPv6 のみ（IPv6 Only）]—デバイスはメディアやシグナリングに IPv6 アドレスだけを使用します。
- [IPv4 および IPv6（IPv4 and IPv6）]—（デフォルト）デバイスはデュアルスタック デバイスで、利用できる IP アドレスのタイプを使用します。両方の IP アドレスのタイプがデバイスに設定されている場合、デバイスのシグナリングには、[シグナリグ用IPアドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）] 設定を使用し、メディア デバイスには、[メディア用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Media）] エンタープライズパラメータの設定を使用します。

Step 4 前のステップで IPv6 を設定した場合は、[シグナリング用のIPアドレッシングモード（IP Addressing Mode for Signaling）] ドロップダウンリストで IP アドレッシング設定を指定します。

- [IPv4（IPv4）]—デュアル スタック デバイスでシグナリングに IPv4 アドレスを優先して使用します。
- [IPv6（IPv6）]—デュアル スタック デバイスでシグナリングに IPv6 アドレスを優先して使用します。
- [システム デフォルトを使用（Use System Default）]—デバイスは、[シグナリグ用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）] エンタープライズパラメータの設定を使用します。

Step 5 [共通デバイス設定（Common Device Configuration）] ウィンドウで、残りのフィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

Step 6 [保存（Save）] をクリックします。

ユニバーサル デバイス テンプレートの設定

ユニバーサルデバイステンプレートを使用すると、新しくプロビジョニングしたデバイスに簡単に設定を適用できます。プロビジョニングされたデバイスは、ユニバーサルデバイステンプレートの設定を使用します。さまざまなユーザグループのニーズを満たすために、異なるデバイステンプレートを設定できます。設定したプロファイルをこのテンプレートに割り当てることもできます。

手順

Step 1 Cisco Unified CM Administration で、**[ユーザの管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサル デバイス テンプレート（Universal Device Template）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 次の必須フィールドに入力します。

a) テンプレートの [デバイスの説明（Device Description）] を入力します。
b) [デバイスプールタイプ（Device Pool Type）] を65Device Pools選択します。
c) [デバイスのセキュリティプロファイル（Device Security Profile）] をドロップダウン リストから選択します。
d) [SIPプロファイル（SIP Profile）] をドロップダウンリストから選択します。
e) [電話ボタンテンプレート（Phone Button Template）] をドロップダウンリストから選択します。

Step 4 [ユニバーサルデバイステンプレートの設定（Universal Device Template Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドの説明については、オンライン ヘルプを参照してください。

Step 5 [電話の設定（Phone Settings）] で、次の任意指定のフィールドを入力します。

a) [共通の電話プロファイル（Common Phone Profile）] を設定した場合は、そのプロファイルを割り当てます。
b) [共通デバイス設定（Common Device Configuration）] を設定した場合は、その設定を割り当てます。
c) [機能管理ポリシー（Feature Control Policy）] を設定した場合は、そのポリシーを割り当てます。

Step 6 [保存（Save）] をクリックします。

ユニバーサル回線テンプレートの設定

ユニバーサル回線テンプレートを使用すると、新しく割り当てられたディレクトリ番号に共通の設定を簡単に適用できます。さまざまなユーザ グループのニーズに合わせて、異なるテンプレートを設定します。

手順

Step 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサル回線テンプレート（Universal Line Template）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [ユニバーサル回線テンプレートの設定（Universal Line Template Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 4 代替番号を使用したグローバル ダイヤル プラン レプリケーションを展開する場合は、[エンタープライズ代替番号（Enterprise Alternate Number）] セクションと [+E.164代替番号（+E.164 Alternate Number）] セクションを展開して、次の手順を実行します。

a) [エンタープライズ代替番号の追加（Add Enterprise Alternate Number）] ボタンまたは [+E.164代替番号の追加（Add +E.164 Alternate Number）] ボタンのいずれか、または両方をクリックします。

b) 代替番号への割り当てに使用する [番号マスク（Number Mask）] を追加します。たとえば、4桁の内線番号では、エンタープライズ番号マスク として 5 XXXX を使用し、+E.164 代替番号マスクとして 1972555XXXX を使用することが考えられます。

c) 代替番号を割り当てるパーティションを割り当てます。

d) ILS を通じてこの番号をアドバタイズする場合は、[ILS経由でグローバルにアドバタイズ（Advertise Globally via ILS）] チェックボックスをオンにします。アドバタイズされたパターンを使用して一定の代替番号の範囲を要約している場合は、個別の代替番号をアドバタイズする必要はありません。

e) [PSTNフェールオーバー（PSTN Failover）] セクションを展開して、通常のコール ルーティングが失敗した場合に使用するPSTNフェールオーバーとして、[エンタープライズ番号（Enterprise Number）] または [+E.164代替番号（+E.164 Alternate Number）] を選択します。

Step 5 [保存（Save）] をクリックします。

ユーザ プロファイルの設定

ユーザ プロファイルを使用して、ユニバーサル回線テンプレートとユニバーサル デバイス テンプレートをユーザに割り当てます。さまざまなユーザ グループ用に複数のユーザプロファイルを

設定します。このサービス プロファイルを使用するユーザに対してセルフプロビジョニングを有効にすることもできます。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザプロファイル（User Profile）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 ユーザ プロファイルの [名前（Name）] および [説明（Description）] を入力します。

Step 4 [ユニバーサルデバイステンプレート（Universal Device Template）] を、ユーザの [デスクフォン（Desk Phones）] 、[モバイルおよびデスクトップデバイス（Mobile and Desktop Devices）] 、および[リモート接続先/デバイスプロファイル（Remote Destination/Device Profiles）]に割り当てます。

Step 5 [ユニバーサル回線テンプレート（Universal Line Template）] をこのユーザ プロファイルのユーザの電話回線に適用するために割り当てます。

Step 6 このユーザ プロファイルのユーザに自分の電話をプロビジョニングするセルフプロビジョニング機能の使用を許可するには、次の手順を実行します

a) [エンドユーザに自分の電話のプロビジョニングを許可（Allow End User to Provision their own phones）] チェックボックスをオンにします。

b) **[エンドユーザーのプロビジョニングする電話数を制限（Limit Provisioning once End User has this many phones）]** フィールドに、ユーザーがプロビジョニングできる電話の最大数を入力します。最大値は 20 です。

c) このプロファイルに関連付けられたユーザーに、別のユーザーがすでに所有しているデバイスを移行または再割り当てする権限があるかどうかを判断するには、**[すでに別のエンドユーザーに割り当てられた電話機のプロビジョニングを許可する（Allow Provisioning of a phone already assigned to a different End User）]** チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

Step 7 このユーザープロファイルに関連付けられた Cisco Jabber ユーザーがモバイルおよびリモートアクセス機能を使用できるようにするには、**[モバイルおよびリモートアクセスの有効化（Enable Mobile and Remote Access）]** チェックボックスをオンにします。

（注）
- デフォルトでは、このチェックボックスはオンです。このチェックボックスをオフにすると、**[クライアントポリシー（Client Policies）]**セクションが無効になり、サービス クライアント ポリシー オプションは、デフォルトで選択されません。
- この設定は、OAuth 更新ログインを使用している Cisco Jabber のユーザにのみ必須です。非 Jabber ユーザは、この設定がなくてもモバイルおよびリモートアクセスを使用できます。モバイルおよびリモートアクセス機能は、Jabber のモバイルおよびリモートアクセスユーザにのみ適用され、他のエンドポイントまたはクライアントには適用されません。

Step 8 このユーザプロファイルにJabberポリシーを割り当てます。**[デスクトップクライアントポリシー（Desktop Client Policy）]**および**[モバイルクライアントポリシー（Jabber Mobile Client Policy）]**のドロップダウンリストから、次のいずれかのオプションを選択します。

- [サービスなし（No Service）]：このポリシーでは、すべての Cisco Jabber サービスへのアクセスが禁止されます。
- [IM & Presence のみ（IM & Presence only）]：このポリシーは、インスタントメッセージとプレゼンス機能だけを有効にします。
- [IM & Presence、音声およびビデオ通話（IM & Presence, Voice and Video calls）]：このポリシーは、オーディオまたはビデオデバイスを所有しているすべてのユーザーに対して、インスタントメッセージング、プレゼンス、ボイスメール、および会議機能を有効にします。これがデフォルトのオプションです。

（注） Jabber デスクトップ クライアントには、Windows ユーザ用 Cisco Jabber と、Mac ユーザ用 Cisco Jabber が含まれています。Jabber モバイル クライアントには、iPad および iPhone ユーザ用 Cisco Jabber と、Android ユーザ用 Cisco Jabber が含まれています。

Step 9 このユーザプロファイルのユーザがCisco Unified Communicationsセルフケアポータルで Extension Mobility または Extension Mobility Cross Cluster の最大ログイン時間を設定できるようにするには、**[エンドユーザに Extension Mobility の最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）]** チェックボックスをオンにします。

（注） デフォルトでは**[エンドユーザに Extension Mobility の最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）]** チェックボックスはオフになっています。

Step 10 [保存（Save）] をクリックします。

ヘッドセットテンプレートの設定

シスコ ヘッドセットに適用できるカスタマイズされた設定でヘッドセットテンプレートを設定するには、次の手順を使用します。カスタマイズしたテンプレートを作成するか、システム定義の標準のデフォルトのヘッドセットテンプレートを使用できます。

（注） 標準のデフォルトのヘッドセット設定テンプレートは、システム定義のテンプレートです。標準のデフォルトのヘッドセットテンプレートに新しいユーザプロファイルを割り当てることはできますが、テンプレートを編集することはできません。デフォルトでは、すべてのユーザプロファイルがこのテンプレートに割り当てられます。このテンプレートからユーザプロファイルの関連付けを解除するには、新しいテンプレートにプロファイルを割り当てる必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ヘッドセット（Headset）] > [ヘッドセットテンプレート（Headset Template）]** を選択します。

Step 2 次のいずれかを実行します。

- 既存のテンプレートを編集するには、テンプレートを選択します。
- 新しいテンプレートを作成するには、既存のテンプレートを選択し、[**コピー(Copy)**] をクリックします。既存の設定が新しいテンプレートに適用されます。

Step 3 テンプレートの [名前（Name）] と [説明（Description）] を追加します。

Step 4 [モデルとファームウェアの設定（Model and Firmware Settings）] で、このテンプレートに適用するカスタマイズされたヘッドセット設定を割り当てます。新しい設定を追加するには、[追加（Add）] ボタンをクリックして設定項目を指定します。

Step 5 上下の矢印を使用して、このテンプレートに割り当てるユーザプロファイルを、[割り当てられているユーザプロファイル（Assigned Users Profiles）] リストボックスに移動します。これらのプロファイルに割り当てられているすべてのユーザは、このヘッドセットテンプレートにも割り当てられます。

Step 6 [保存（Save）] をクリックします。

Step 7 デフォルトのテンプレート設定に戻すには、[デフォルトに設定（Set to Default）] ボタンを使用します。

Step 8 [設定の適用（Apply Config）] をクリックします。

標準のデフォルトヘッドセット構成テンプレートでは、以下に対して [設定の適用（Apply Config）] ボタンが有効になります。

- 割り当てられたユーザプロファイルリストに追加したユーザが所有しているデバイス
- 名前非表示のデバイス

カスタマイズされたヘッドセット構成テンプレートでは、[割り当てられているユーザプロファイル（Assigned User Profiles）] リストに追加されたユーザが所有するデバイスに対してのみ [設定の適用（Apply Config）] ボタンが有効になります。

UC サービスの設定

ユーザが使用する UC サービス接続を設定するには、次の手順を使用します。次の UC サービスの接続を設定できます。

- ボイスメール
- メールストア
- 会議

- ディレクトリ
- IM and Presence Service
- CTI
- ビデオ会議スケジュールポータルの設定
- Jabber クライアント設定（jabber-config.xml）

（注） フィールドは、設定する UC サービスによって異なる場合があります。

手順

Step 1 Cisco Unified CM Administration から、[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [UCサービス（UC Services）] を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [UCサービスタイプ（UC Service Type）] ドロップダウンリストから、設定する UC サービスを選択し、[次へ（Next）] をクリックします。

Step 4 [製品タイプ（Product Type）] を選択します。

Step 5 [名前（Name）] にサービスの名前を入力します。

Step 6 サービスが存在するサーバーの**ホスト名またはIPアドレス**を入力します。

Step 7 [ポート（Port）] および [プロトコル（Protocol）] の情報を入力します。

Step 8 残りのフィールドを設定します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。フィールドオプションは、導入している UC サービスによって異なります。

Step 9 [保存（Save）] をクリックします。

Step 10 必要なすべてのUCサービスをプロビジョニングするまで、この手順を繰り返します。

（注） サービスを複数のサーバに配置する場合は、別のサーバを指す複数の UC サービス接続を設定します。たとえば、IM and Presence Service の集中展開では、複数の IM and Presence UC サービスがそれぞれ異なる IM and Presence ノードを指すように設定することを推奨します。すべてのUC接続を設定した後、それらをサービスプロファイルに追加することができます。

サービス プロファイルの設定

このプロファイルを使用するエンドユーザに割り当てる UC サービスを含む、サービス プロファイルを設定します。

始める前に

サービス プロファイルに追加する前に、Unified Communications（UC）サービスをセットアップする必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [サービスプロファイル（Service Profile）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 選択したサービス プロファイルの設定の [名前（Name）] を入力します。

Step 4 選択したサービス プロファイルの設定の [説明（Description）] を入力します。

Step 5 このプロファイルに含める各 UC サービスに、そのサービス用の [プライマリ（Primary）]、[セカンダリ（Secondary）]、および [ターシャリ（Tertiary）] の接続を割り当てます。

Step 6 [サービスプロファイルの設定（Service Profile Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドの詳細については、オンライン ヘルプを参照してください。

Step 7 [保存（Save）] をクリックします。

機能グループ テンプレートの設定

機能グループ テンプレートは、プロビジョニングされたユーザ用に、電話、回線、および機能をすばやく設定できるようにすることで、システムの展開をサポートします。企業の LDAP ディレクトリからユーザを同期している場合は、ディレクトリからユーザを同期させるユーザ プロファイルおよびサービスプロファイルを使用して機能グループテンプレートを設定します。このテンプレートを使用して、同期されたユーザに対して IM and Presence Service を有効化することもできます。

手順

Step 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [機能グループ テンプレート（Feature Group Template）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 機能グループ テンプレートの [名前（Name）] と [説明（Description）] を入力します。

Step 4 このテンプレートを使用するすべてのユーザのホームクラスタとしてローカルクラスタを使用する場合は、[ホーム クラスタ（Home Cluster）] チェック ボックスをオンにします。

Step 5 このテンプレートを使用するユーザがインスタント メッセージおよびプレゼンス情報を交換できるようにするには、[Unified CM IM and Presenceのユーザを有効化（Enable User for Unified CM IM and Presence）] チェックボックスをオンにします。

Step 6 ドロップダウン リストから、[サービスプロファイル（Services Profile）] および [ユーザプロファイル（User Profile）] を選択します。

Step 7 [機能グループ テンプレートの設定（Feature Group Template Configuration）] ウィンドウの残りのフィールドに入力します。フィールドの説明については、オンライン ヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

次のタスク

機能グループ テンプレートと LDAP ディレクトリ同期を関連付け、テンプレートの設定を同期したエンド ユーザに適用します。

デフォルトのクレデンシャル ポリシーの設定

新しくプロビジョニングされたユーザに適用されるクラスタ全体のデフォルトクレデンシャルポリシーを設定するには、次の手順を使用します。次の各ログイン情報タイプに対して、個別のログイン情報ポリシーを適用できます。

- アプリケーション ユーザ パスワード
- エンド ユーザのパスワード
- エンドユーザ PIN

手順

Step 1 クレデンシャル ポリシーの設定を入力します。

a) Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [クレデンシャルポリシー（Credential Policy）]** を選択します。

b) 次のいずれかを実行します。

- **[検索（Find）]** をクリックし、既存のクレデンシャル ポリシーを選択します。
- [新規追加（Add New）] をクリックして、新しいクレデンシャルポリシーを作成します。

c) ABCD や 123456 のようなハッキングされやすいパスワードをシステムにチェックさせる場合は、[単純すぎるパスワードのチェック（Check for Trivial Passwords）] チェックボックスをオンにします。

d) [クレデンシャル ポリシーの設定（Credential Policy Configuration）] ウィンドウの各フィールドに入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

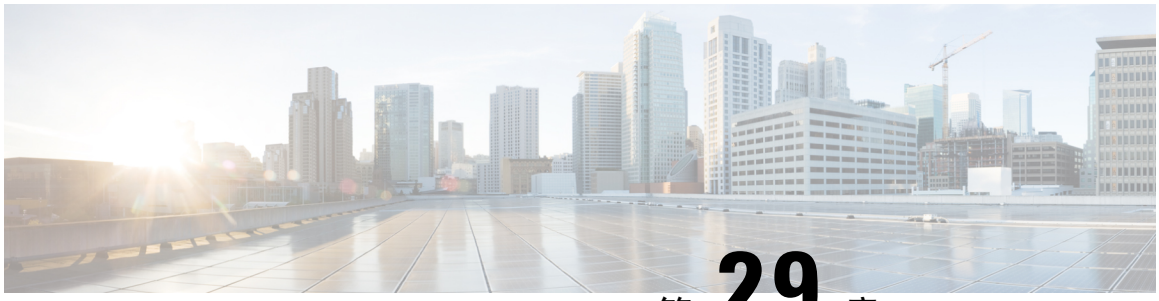
e) [保存（Save）] をクリックします。

f) 他のクレデンシャルタイプのいずれかに対して異なるクレデンシャルポリシーを作成する場合は、これらの手順を繰り返します。

Step 2 クレデンシャルポリシーをクレデンシャルタイプのいずれかに適用します。

a) Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [クレデンシャルポリシーのデフォルト（Credential Policy Default）]** を選択します。
b) クレデンシャルポリシーを適用するクレデンシャルタイプを選択します。
c) **[クレデンシャルポリシー (Credential policy)]** ドロップダウンから、このクレデンシャルタイプに適用するクレデンシャルポリシーを選択します。たとえば、作成したクレデンシャルポリシーを選択することもできます。
d) [クレデンシャルの変更（Change Credential）] フィールドと [クレデンシャルの確認（Confirm Credential）] フィールドの両方にデフォルトのパスワードを入力します。ユーザは次のログイン時にこれらのパスワードを入力する必要があります。
e) [クレデンシャル ポリシーのデフォルトの設定（Credential Policy Default Configuration）] ウィンドウで、残りのフィールドを設定します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。
f) [保存（Save）] をクリックします。
g) 他のクレデンシャルタイプのいずれかにクレデンシャルポリシーを割り当てる場合は、これらの手順を繰り返します。

（注） 個人ユーザに対して、[エンドユーザの設定（End User Configuration）] ウィンドウ、またはそのユーザの [アプリケーションユーザの設定（Application User Configuration）] ウィンドウから、特定のユーザログイン情報にポリシーを割り当てることもできます。ログイン情報タイプ（パスワードまたは PIN）の隣にある [ログイン情報の編集（Edit Credential）] ボタンをクリックして、そのユーザログイン情報に関する [ログイン情報の設定（Credential Configuration）] を開きます。



第 29 章

LDAP 同期の設定

LDAP 同期の概要

Lightweight Directory Access Protocol（LDAP）の同期は、システムのエンドユーザのプロビジョニングと設定を支援します。LDAP の同期中、システムは外部 LDAP ディレクトリから Cisco Unified Communications Manager データベースにユーザのリストと関連するユーザ データをインポートします。インポートしている間に、エンドユーザを設定することもできます。

（注） Unified Communication Manager は、LDAPS（SSL を使用した LDAP）をサポートしますが、StartTLS を使用した LDAP はサポートしていません。LDAP サーバ証明書を Unified Communication Manager に Tomcat-Trust 証明書としてアップロードします。

サポートされている LDAP ディレクトリの詳細については、*Cisco Unified Communications Manager と IM and Presence Service* の互換性マトリクスを参照してください。

LDAP 同期では、以下の機能がアドバタイズされます。

- **エンド ユーザのインポート：** LDAP 同期を使用して、システムの初期設定時にユーザ一覧を会社の LDAP ディレクトリから Unified Communication Manager のデータベースにインポートできます。機能グループテンプレート、ユーザプロファイル、サービスプロファイル、ユニバーサルデバイス、回線テンプレートなどの設定項目が設定されている場合は、設定をユーザに適用することができ、また、同期プロセス中に設定したディレクトリ番号とディレクトリ Uri を割り当てることができます。LDAP同期プロセスは、ユーザーリストとユーザー固有のデータをインポートし、設定した構成テンプレートを適用します。

（注） 初期同期が実行された以降は、LDAP 同期を編集することはできません。

- **スケジュールされた更新**：Unified Communication Manager をスケジュールされた間隔で複数の LDAP ディレクトリと同期するように設定できます。これによって確実にデータベースが定期的に更新され、すべてのユーザ データを最新に保ちます。
- **エンドユーザの認証**：LDAP 同期を使用して、システムが Cisco Unified Communications Manager データベースではなく、LDAP ディレクトリに対してエンドユーザ パスワードを認証するように設定できます。LDAP 認証によって、企業は、すべての企業内アプリケーションに対応する単一のパスワードをエンド ユーザに割り当てることができます。この機能は、PIN またはアプリケーションユーザー パスワードには適用されません。
- **Cisco モバイルおよびリモートアクセス クライアントおよびエンドポイントのディレクトリ サーバユーザ検索**：企業ファイアウォールの外部で操作している場合でも、社内ディレクトリサーバを検索できます。この機能を有効にすると、ユーザデータ サービス（UDS）がプロキシとして機能し、Unified Communication Manager データベースにユーザ検索要求を送信する代わりに、それを社内ディレクトリに送信します。

LDAP 同期の前提条件

前提タスク

LDAP ディレクトリからエンドユーザをインポートする前に、次のタスクを実行します。

- ユーザ アクセスを設定します。ユーザに割り当てるアクセス制御グループを決定します。ほとんどの導入環境では、デフォルトのグループで十分です。ロールとグループをカスタマイズする必要がある場合は、アドミニストレーション ガイドの「ユーザアクセスの管理」の章を参照してください。
- 新しくプロビジョニングされたユーザーにデフォルトで適用されるクレデンシャル ポリシーに、デフォルトのクレデンシャルを設定します。
- LDAP ディレクトリからユーザを同期する場合は、機能グループ テンプレートが設定されていることを確認してください。このテンプレートには、ユーザープロファイル、サービス プロファイル、ユーザの電話と電話の内線に割り当てるユニバーサル回線テンプレートおよびユニバーサル デバイス テンプレートの設定が含まれます。

（注） システムにデータを同期するユーザについては、Active Directory サーバでの電子メール ID フィールドが一意のエントリであるか空白であることを確認してください。

LDAP 同期の設定タスクフロー

外部 LDAP ディレクトリからユーザ リストをプルし、Unified Communication Manager のデータベースにインポートするには、以下のタスクを使用します。

（注） LDAP ディレクトリをすでに一度同期している場合、外部 LDAP ディレクトリから新しい項目を同期することはできますが、Unified Communication Manager 内の新しい設定を LDAP ディレクトリ同期に追加することはできません。この場合は、一括管理ツールを使用して、ユーザの更新やユーザの挿入などのメニューを使用できます。『*Cisco Unified Communications Manager* 一括アドミニストレーション ガイド』を参照してください。

手順

	コマンドまたはアクション	目的
Step 1	Cisco DirSync サービスの有効化 （352 ページ）	Cisco Unified Serviceability にログインし、Cisco DirSync サービスを有効にします。
Step 2	LDAP ディレクトリ同期の有効化 （352 ページ）	Unified Communication Manager の LDAP ディレクトリ同期を有効化します。
Step 3	LDAP フィルタの作成 （353 ページ）	（**オプション**）Unified Communication Manager に社内 LDAP ディレクトリからユーザのサブセットだけを同期するには、LDAP フィルタを作成します。
Step 4	LDAP ディレクトリの同期の設定 （353 ページ）	アクセス制御グループ、機能グループのテンプレートとプライマリ エクステンションのフィールド設定、LDAP サーバのロケーション、同期スケジュール、および割り当てなどの LDAP ディレクトリ同期を設定します。
Step 5	エンタープライズ ディレクトリ ユーザ検索の設定 （356 ページ）	（**オプション**）エンタープライズ ディレクトリ サーバ ユーザを検索するシステムを設定します。システムの電話機とクライアントをデータベースの代わりにエンタープライズディレクトリ サーバに対してユーザの検索を実行するように設定するには、次の手順に従います。
Step 6	LDAP 認証の設定 （357 ページ）	（**オプション**）エンド ユーザのパスワード認証に LDAP ディレクトリを使用するには、LDAP 認証を設定します。
Step 7	LDAP アグリーメント サービスパラメータのカスタマイズ （358 ページ）	（**オプション**）任意指定の [LDAP同期（LDAP Synchronization）] サービスパラメータを設定します。ほとんどの導入の場合、デフォルト値のままで問題ありません。

Cisco DirSync サービスの有効化

Cisco Unified Serviceability で Cisco DirSync サービスをアクティブ化するには、次の手順を実行します。社内の LDAP ディレクトリからエンドユーザの設定を同期するには、このサービスをアクティブ化する必要があります。

手順

Step 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスのアクティブ化（Service Activation）]** を選択します。

Step 2 [サーバ（Server）] ドロップダウンリストからパブリッシャノードを選択します。

Step 3 [**ディレクトリサービス**(Directory Services **)]**の下で、[Cisco DirSync] ラジオボタンをクリックします。

Step 4 [保存（Save）] をクリックします。

LDAP ディレクトリ同期の有効化

エンドユーザの設定を社内 LDAP ディレクトリから同期させるには、以下の手順で Unified Communication Manager を設定します。

（注） LDAP ディレクトリをすでに一度同期している場合、外部 LDAP ディレクトリから新しい項目を同期することはできますが、Unified Communications Manager 内の新しい設定を LDAP ディレクトリ同期に追加することはできません。また、機能グループテンプレートやユーザプロファイルなどの基になる構成アイテムの編集を追加することもできません。すでに 1 回の LDAP 同期を完了しており、別の設定でユーザを追加する場合は、ユーザの更新やユーザの挿入などの一括管理メニューを使用できます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [LDAP] > [LDAPシステム（LDAP System）]** を選択します。

Step 2 Unified Communications Manager で LDAP ディレクトリからユーザをインポートするには、[LDAP サーバからの同期を有効にする（Enable Synchronizing from LDAP Server）] チェックボックスをオンにします。

Step 3 [LDAPサーバタイプ（LDAP Server Type）] ドロップダウンリストから、使用する LDAP ディレクトリサーバの種類を選択します。

Step 4 [ユーザ IDのLDAP属性（LDAP Attribute for User ID）] ドロップダウンリストで、[エンドユーザの設定（End User Configuration）] ウィンドウの [ユーザID（User ID）] フィールドに関して、Unified Communications Manager で同期する社内 LDAP ディレクトリから属性を選択します。

Step 5 [保存（Save）] をクリックします。

LDAP フィルタの作成

LDAP フィルタを作成することで、LDAP 同期を LDAP ディレクトリからのユーザのサブセットのみに制限することができます。LDAP フィルタを LDAP ディレクトリに適用する場合、Unified Communications Manager は、フィルタに一致するユーザのみを LDAP ディレクトリからインポートします。

（注） LDAP フィルタを設定する場合は、RFC4515 に指定されている LDAP 検索フィルタ標準に準拠する必要があります。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [LDAP(LDAP)] > [LDAP フィルタ（LDAP Filter）]** を選択します。

Step 2 [新規追加（Add New）] をクリックして、新しい LDAP フィルタを作成します。

Step 3 [フィルタ名（Filter Name）] テキスト ボックスに、LDAP フィルタの名前を入力します。

Step 4 [フィルタ（Filter）] テキスト ボックスに、フィルタを入力します。フィルタは、UTF-8 で最大 1024 文字まで入力できます。また、丸カッコ（ ()）で囲みます。

Step 5 [保存（Save）] をクリックします。

LDAP ディレクトリの同期の設定

LDAP ディレクトリと同期するように Unified Communications Manager を設定するには、この手順を使用します。LDAP ディレクトリの同期により、エンドユーザのデータを外部の LDAP ディレクトリから Unified Communication Manager データベースにインポートして、エンド ユーザの設定ウィンドウに表示することができます。ユニバーサル回線とデバイステンプレートを使用する機能グループテンプレートがセットアップされている場合は、新しくプロビジョニングされるユーザとその内線番号に自動的に設定を割り当てることができます。

ヒント アクセス制御グループまたは機能グループ テンプレートを割り当てる場合は、LDAP フィルタを使用して、インポートを同じ設定要件のユーザ グループに限定できます。

手順

Step 1 Cisco Unified CM Administration で、**[System（システム）] > [LDAP] > [LDAP Directory（LDAP ディレクトリ)]** を選択します。

Step 2 次のいずれかの手順を実行します。

- [検索（Find）] をクリックし、既存の LDAP ディレクトリを選択します。
- [新規追加（Add New）] をクリックして、新しい LDAP ディレクトリを作成します。

Step 3 [LDAPディレクトリの設定（LDAP Directory Configuration）] ウィンドウで、次のように入力します。

a) [LDAP設定名（LDAP Configuration Name）] フィールドで、LDAP ディレクトリに一意の名前を割り当てます。

b) [LDAP マネージャ識別名（LDAP Manager Distinguished Name）] フィールドに、LDAP ディレクトリ サーバにアクセスできるユーザ ID を入力します。

c) パスワードの詳細を入力し、確認します。

d) [LDAPユーザサーチスペース（LDAP User Search Space）] フィールドに、サーチ スペースの詳細を入力します。

e) [ユーザ同期用のLDAPカスタムフィルタ（LDAP Custom Filter for Users Synchronize）] フィールドで、[ユーザのみ（Users Only）] または [ユーザとグループ（Users and Groups）] を選択します。

f) （オプション）特定のプロファイルに適合するユーザのサブセットのみにインポートを限定する場合は、[グループ用LDAPカスタムフィルタ（LDAP Custom Filter for Groups）] ドロップダウンリストから LDAP フィルタを選択します。

Step 4 [LDAPディレクトリ同期スケジュール（LDAP Directory Synchronization Schedule）] フィールドに、外部 LDAP ディレクトリとデータ同期を行うために Unified Communication Manager が使用するスケジュールを作成します。

Step 5 [同期対象の標準ユーザ フィールド（Standard User Fields To Be Synchronized）] セクションを記入します。各エンドユーザのフィールドで、それぞれ LDAP 属性を選択します。同期プロセスが LDAP 属性の値を Unified Communication Manager のエンドユーザ フィールドに割り当てます。

Step 6 URIダイヤリングを展開する場合は、ユーザのプライマリディレクトリURIアドレスに使用されるLDAP属性が割り当てられていることを確認してください。

Step 7 [同期対象のカスタムユーザフィールド（Custom User Fields To Be Synchronized）] セクションで、必要な LDAP 属性を持つカスタムユーザフィールド名を入力します。

Step 8 インポートしたエンドユーザを、インポートしたすべてのエンドユーザに共通するアクセス制御グループに割り当てるには、次の手順を実行します。

a) [アクセス制御グループに追加（Add to Access Control Group）] をクリックします。

b) ポップアップ ウィンドウで、インポートされたエンド ユーザに割り当てる各アクセス制御グループごとに、対応するチェックボックスをオンにします。

c) [選択項目の追加（Add Selected）] をクリックします。

Step 9 機能グループ テンプレートを割り当てる場合は、[機能グループテンプレート（Feature Group Template）] ドロップダウンリストからテンプレートを選択します。

（注） エンドユーザは、そのユーザが存在しない初回のみ、割り当てられた**機能グループテンプレート**と同期されます。既存の [機能グループ テンプレート（Feature Group Template）] が変更され、関連付けられた LDAP の完全同期が実行される場合、変更点は更新されません。

Step 10 インポートされた電話番号にマスクを適用して、プライマリ内線番号を割り当てるには、次の手順を実行します。

a) [挿入されたユーザの新規回線を作成するために、同期された電話番号にマスクを適用する（Apply mask to synced telephone numbers to create a new line for inserted users）] チェックボックスをオンにします。

b) [マスク（Mask）] を入力します。たとえば、インポートされた電話番号が 8889945 である場合、11XX のマスクによって 1145 のプライマリ内線番号が作成されます。

Step 11 電話番号のプールからプライマリ内線番号を割り当てる場合は、次の手順を実行します。

a) [同期された LDAP 電話番号に基づいて作成されなかった場合、プール リストから新しい回線を割り当て（Assign new line from the pool list if one was not created based on a synced LDAP telephone number）] チェック ボックスをオンにします。

b) [DN プールの開始（DN Pool Start）] テキスト ボックスと [DN プールの終了（DN Pool End）] テキスト ボックスに、プライマリ内線番号を選択する電話番号の範囲を入力します。

Step 12 （オプション）Jabber エンドポイント プロビジョニング セクションで、Jabber デバイスを作成する場合は、以下のドロップダウンから自動プロビジョニングに必要な Jabber デバイスを 1 つ選択します：

- Cisco Dual Mode for Android（BOT）
- Cisco Dual Mode for iPhone（TCT）
- Cisco Jabber for Tablet（TAB）
- Cisco Unified Client Services Framework（CSF）

（注） **[LDAPへのライトバック（Write back to LDAP）]**オプションにより、Unified CM から選択されたプライマリ DN を LDAP サーバーにライトバックすることができます。ライトバック可能な LDAP 属性は、**telephoneNumber**、**ipPhone**、および**mobile**です。

Step 13 [LDAPサーバ情報（LDAP Server Information）] セクションで、LDAP サーバのホスト名または IP アドレスを入力します。

Step 14 TLS を使用して LDAP サーバに対するセキュアな接続を作成する場合は、[TLSを使用（Use TLS）] チェックボックスをオンにします。

（注） Tomcat の再起動後にセキュアポートを介してユーザーを同期しようとすると、ユーザーが同期されないことがあります。ユーザーの同期を正常に行うには、Cisco DirSync サービスを再起動する必要があります。

Step 15 [保存（Save）] をクリックします。

Step 16 LDAP 同期を完了させるには、[完全同期を今すぐ実行（Perform Full Sync Now）] をクリックします。それ以外の場合は、スケジュールされた同期を待つことができます。

（注） LDAP で削除されたユーザは、24 時間後に Unified Communications Manager から自動的に削除されます。また、削除されたユーザが次のいずれかのデバイスのモビリティユーザとして設定されている場合、それらの非アクティブデバイスも自動的に削除されます。

- リモート宛先プロファイル
- リモート接続先プロファイルテンプレート
- モバイルスマートクライアント
- CTI リモート デバイス
- Spark リモートデバイス
- Nokia S60
- Cisco Dual Mode for iPhone
- IMS 統合モバイル（ベーシック）
- キャリア統合モバイル
- Cisco Dual Mode for Android

エンタープライズ ディレクトリ ユーザ検索の設定

データベースではなくエンタープライズディレクトリ サーバに対してユーザ検索を実行するように、システムの電話機とクライアントを設定するには、次の手順を使用します。

始める前に

- LDAP ユーザ検索に選択するプライマリ、セカンダリ、および第 3 サーバが Unified Communication Manager のサブスクライバ ノードに到達可能なネットワークにあることを確認します。
- **[システム（System）] > [LDAP] > [LDAPシステム（LDAP System）]** を選択し、[LDAPシステムの設定（LDAP System Configuration）] ウィンドウの [LDAPサーバタイプ（LDAP Server Type）] ドロップダウンリストから LDAP サーバのタイプを設定します。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [LDAP] > [LDAP 検索（LDAP Search）]** を選択します。

Step 2 エンタープライズLDAPディレクトリ サーバを使用してユーザ検索を実行するには、[エンタープライズ ディレクトリ サーバのユーザ検索を有効にする（Enable user search to Enterprise Directory Server）] チェックボックスをオンにします。

Step 3 [LDAP 検索の設定（LDAP Search Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 4 [保存（Save）] をクリックします。

（注） OpenLDAP サーバでルーム オブジェクトとして表される会議室を検索するには、カスタム フィルタを (| (objectClass=intOrgPerson)(objectClass=rooms)) に設定します。これにより、Cisco Jabber クライアントは部屋に関連付けられた名前およびダイヤル番号で会議室を検索できます。

会議室は、ルーム オブジェクトの OpenLDAP サーバに、**givenName**、**sn**、**mail**、**displayName**、または **telephonenumber** の属性が設定されていると検索可能です。

LDAP 認証の設定

LDAP 認証を有効にして、会社の LDAP ディレクトリに割り当てられているパスワードに対してエンド ユーザのパスワードが認証されるようにするには、この手順を実行します。この設定は、エンド ユーザのパスワードにのみ適用され、エンド ユーザの PIN またはアプリケーション ユーザのパスワードには適用されません。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [LDAP] > [LDAP認証（LDAP Authentication）]** を選択します。

Step 2 [エンドユーザにLDAP認証を使用（Use LDAP Authentication for End Users）] チェックボックスをオンにして、ユーザ認証に LDAP ディレクトリを使用します。

Step 3 [LDAPマネージャ識別名（LDAP Manager Distinguished Name）] フィールドに、LDAP ディレクトリへのアクセス権を持つ LDAP マネージャのユーザ ID を入力します。

Step 4 [パスワードの確認（Confirm Password）] フィールドに、LDAP マネージャのパスワードを入力します。

（注） Unified Communications Manager をリリース 11.5(1)SU2 からリリース 14SU3 以降にアップグレードする場合は、必ず LDAP パスワードを使用してください。

Step 5 [LDAPユーザ検索ベース（LDAP User Search Base）] フィールドに、検索条件を入力します。

Step 6 [LDAPサーバ情報（LDAP Server Information）] セクションで、LDAP サーバのホスト名または IP アドレスを入力します。

Step 7 TLS を使用して LDAP サーバに対するセキュアな接続を作成する場合は、[TLSを使用（Use TLS）] チェックボックスをオンにします。

Step 8 [保存（Save）] をクリックします。

次のタスク

LDAP アグリーメント サービスパラメータのカスタマイズ（358 ページ）

LDAP アグリーメント サービスパラメータのカスタマイズ

LDAP アグリーメントのシステムレベルでの設定をカスタマイズする、任意指定のサービスパラメータを設定するには、この手順を実行します。これらのサービスパラメータを設定しない場合、Unified Communications Manager により、LDAP ディレクトリ統合のデフォルト設定が適用されます。パラメータの説明については、ユーザ インターフェイスでパラメータ名をクリックしてください。

サービスパラメータを使用して次の設定をカスタマイズできます。

- [最大アグリーメント数（Maximum Number of Agreements）]：デフォルト値は 20 です。
- [最大ホスト数（Maximum Number of Hosts）]：デフォルト値は 3 です。
- [ホスト障害時の再試行の遅延（秒）（Retry Delay On Host Failure (secs)）]：ホスト障害のデフォルト値は 5 です。
- [ホストリスト障害時の再試行の遅延（分）（Retry Delay On HotList failure (mins)）]：ホストリスト障害のデフォルト値は 10 です。
- [LDAP接続のタイムアウト（秒）（LDAP Connection Timeouts (secs)）]：デフォルト値は 5 です。
- [遅延同期の開始時間（分）（Delayed Sync Start time (mins)）]：デフォルト値は 5 です。
- [ユーザカスタマーマップの監査時間（User Customer Map Audit Time）]

手順

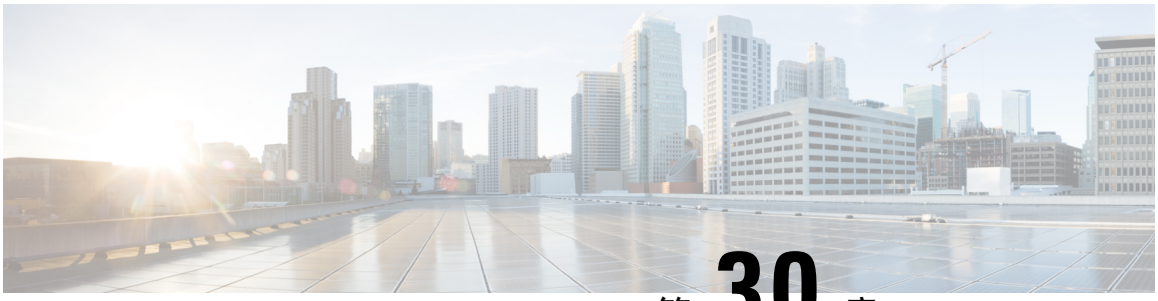
Step 1 Cisco Unified CM Administration から、**[システム（System）] > [サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 [サーバ（Server）] ドロップダウンリスト ボックスからパブリッシャノードを選択します。

Step 3 [サービス（Service）] ドロップダウンリスト ボックスから、[Cisco DirSync] を選択します。

Step 4 Cisco DirSyncサービスパラメータの値を設定します。

Step 5 [保存（Save）] をクリックします。



第 30 章

一括管理ツールを使用したユーザおよびデバイスのプロビジョニング

一括管理ツールの概要

一括管理ツール（BAT）は、Unified Communications Manager データベースに対してバルク トランザクションを実行するのに使用できる Web ベースのアプリケーションです。BAT を使用することで、類似する大量の電話、ユーザ、またはポートを一度に追加、更新、削除できます。

（注） [一括管理（Bulk Administration）] メニューは、Unified Communications Manager サーバの最初のノードでのみ表示されます。

Cisco Unified CM Administration の [一括管理（Bulk Administration）] メニューから送信されたすべてのジョブは、Cisco Bulk Provisioning Service（BPS）によって管理および保守されます。このサービスは、Cisco Unified Serviceability から開始できます。Cisco Bulk Provisioning Service は、Unified Communications Manager の最初のノード上でのみアクティブ化する必要があります。

BAT を使用して、次の操作を実行できます。

- 多数の電話機を一括で追加、更新、または削除する
- 新しい電話のグループを追加する共通の電話属性を定義する
- 新しい BAT 電話テンプレートを作成する
- 新規ユーザのグループを追加し、ユーザを電話機やその他の IP テレフォニーデバイスに関連付ける
- BAT スプレッドシートからユーザ CSV データファイルを作成する

- 電話とユーザをバッチで追加するための CSV データファイルを作成する
- 電話機とユーザのグループを Unified Communications Manager データベースとディレクトリに追加する

一括管理ツールの前提条件

- ユーザプロファイルとサービスプロファイルの設定

一括管理ツールのタスクフロー

手順

	コマンドまたはアクション	目的
Step 1	データベースへの電話機の追加（361 ページ）	BAT を使用して、電話およびその他の IP テレフォニー デバイスを Unified Communications Manager データベースに一括で追加します。
Step 2	新しいBAT電話テンプレートの作成（362 ページ）	新しいBAT電話テンプレートを作成できます。
Step 3	BAT スプレッドシートを使用した電話用CSVデータファイルの作成（367ページ）	BAT で使用するよう設計された .xls 形式のスプレッドシートを使用して、新しい電話またはIPテレフォニーデバイスをシステムに追加できます。
Step 4	テキストエディタを使用したカスタム電話機ファイル形式の作成 （370 ページ）	テキストエディタを使用して、テキストベースのCSVデータファイルのカスタム電話機ファイル形式を作成できます。
Step 5	Unified Communications Manager への電話の挿入 （372 ページ）	電話、Cisco VGC Phone、CTI ポート、または H.323 クライアントを Unified Communications Manager データベースに追加できます。
Step 6	ユーザの追加 （374 ページ）	BAT を使用して、新しいユーザのグループを追加し、ユーザを電話機やその他の IP テレフォニーデバイスに関連付けることができます。

	コマンドまたはアクション	目的
Step 7	BAT スプレッドシートを使用したユーザ用 CSV データファイルの作成（374 ページ）	Unified Communications Manager データベースに新しいユーザを追加するための詳細情報を BAT スプレッドシートに入力し、それを CSV データファイルに変換することができます。
Step 8	Unified Communications Manager データベースへのユーザの挿入 （376 ページ）	CSV データファイルを使用して、ユーザのグループを Unified Communications Manager データベースに追加できます。
Step 9	電話およびユーザ ファイル形式の追加（378 ページ）	テキストベースの CSV データファイルで電話とユーザのファイル形式を追加できます。CSV データファイルを作成した後、ファイル形式をテキストベースの CSV データファイルと関連付ける必要があります。
Step 10	Unified Communications Manager への電話機とユーザの挿入 （379 ページ）	電話とユーザのグループを Unified Communications Manager データベースとディレクトリに追加できます。

データベースへの電話機の追加

BAT を使用して、電話およびその他の IP テレフォニーデバイスを Unified Communications Manager データベースに一括で追加する場合は、個々の電話に複数の回線、サービス、および短縮ダイヤルを追加できます。CTI ポートや H.323 クライアントを追加することもできます。

電話機の CSV データファイルの作成には、2 つのオプションがあります。

- BAT スプレッドシート（BAT.xlt）を使用して、データを CSV 形式にエクスポートする
- テキストエディタを使用して、CSV 形式のテキストファイルを作成する（経験豊富なユーザ向け）

手順

Step 1 **[一括管理（Bulk Administration）] > [電話（Phones）] > [電話テンプレート（Phone Template）]** の順に選択します。

[電話テンプレートの検索/一覧表示（Find and List Phone Templates）] ウィンドウが表示されます。

Step 2 CSV ファイルを作成して、電話テンプレートを挿入します。

次のいずれかの選択肢を実行します。

a) BAT スプレッドシートを使用して CSV データファイルを作成します。
b) 以下のようにテキスト エディタを使用して CSV データファイルを作成します。

1. **[一括管理（Bulk Administration）] > [電話（Phones）] > [電話ファイル形式（Phone File Format）] > [ファイル形式の作成（Create File Format）]** の順に選択します。
2. テキスト エディタを使用して、電話機の CSV データファイルを作成します。このファイルは、使用するファイル形式に従います。
3. **[一括管理（Bulk Administration）] > [電話（Phones）] > [電話ファイル形式（Phone File Format）] > [ファイル形式の追加（Add File Format）]** を選択し、テキストベースのファイル形式を CSV データファイルと関連付けます。

Step 3 **[一括管理（Bulk Administration）] > [電話（Phones）] > [電話の確認（Validate Phones）]** の順に選択します。

Step 4 **[一括管理（Bulk Administration）] > [電話（Phones）] > [電話の挿入（Insert phones）]** を選択して、電話レコードを Unified Communications Manager データベースに挿入します。

新しい BAT 電話テンプレートの作成

新しい BAT 電話テンプレートを作成できます。電話テンプレートを作成したら、回線、サービス、および短縮ダイヤルを追加できます。

手順

Step 1 **[一括管理（Bulk Administration）] > [電話（Phones）] > [電話テンプレート（Phone Template）]** の順に選択します。

Step 2 [新規追加（Add New）] をクリックします。[新しい電話テンプレートの追加（Add a New Phone）] ウィンドウが表示されます。

Step 3 電話タイプ のドロップダウンリストから、テンプレートを作成する電話機モデルを選択します。[次へ（Next）] をクリックします。

Step 4 **デバイスプロトコルの選択**のドロップダウンリストから、デバイスのプロトコルを選択します。[次へ（Next）] をクリックします。

[電話テンプレートの設定（Phone Template Configuration）] ウィンドウが、選択したデバイス タイプのフィールドとデフォルト エントリと共に表示されます。

Step 5 [テンプレート名（Template Name）] フィールドに、テンプレートの名前を入力します。

名前には、最大 50 文字の英数字を使用できます。

Step 6 [デバイス情報（Device Information）] 領域に、このバッチの共通の電話設定を入力します。

一部の電話モデルとデバイス タイプには、一覧に示されている属性がすべて揃っていないものもあります。すべての属性の詳細については、電話機モデルのマニュアルを参照してください。

Step 7 この BAT 電話テンプレートのすべての設定を入力したら、[保存（Save）] をクリックします。

ステータスにトランザクションが完了したことが示されたら、回線の属性を追加できます。

BAT テンプレート内の電話回線の追加または更新

BAT テンプレートに 1 つ以上の回線を追加したり、既存の回線を更新したりできます。BAT テンプレートに使用されるボタン テンプレートによって、追加または更新できる回線の数が決定されます。複数回線を持つプライマリ電話テンプレートを作成することができます。その標準テンプレートを使用して、単一回線の電話機、または標準テンプレート内の回線数を上限とする複数回線の電話機を追加できます。このバッチ内のすべての電話機またはユーザデバイスプロファイルが、選択された設定を使用することになります。

回線テンプレートの値には英数字を使用することが推奨されています。数字のみを指定した場合、実際の電話番号と競合してしまう可能性があります。英数字を使用することにより、コール ピックアップ グループ番号や通話パーク番号などの機能とも競合せずに済みます。

BAT テンプレートに表示される回線の最大数は、BAT 電話テンプレートの作成時に選択したモデルおよびボタン テンプレートに応じて異なります。一部の Cisco Unified IP Phone モデルでは、Cisco Unified IP Phone サービスと短縮ダイヤルもテンプレートに追加できます。

手順

Step 1 回線を追加する電話テンプレートを見つけます。

Step 2 [電話テンプレートの設定（Phone Template Configuration）] ウィンドウで、[関連情報（Associated Information）] 領域にある [回線 [1] - 新規 DN の追加（Line [1] Add a new DN）] をクリックします。

[回線テンプレートの設定（Intercom Template Configuration）] ウィンドウが表示されます。

Step 3 回線の設定に適切な値を入力するか、選択します。

Step 4 [保存（Save）] をクリックします。

Step 5 その他の回線の設定を追加するには、Step 2 （363 ページ） ～Step 4 （363 ページ） を繰り返します。

[回線テンプレートの設定（Line Template Configuration）] ウィンドウの右上隅にある [関連リンク（Related Links）] ドロップダウンリスト ボックスから [検索/一覧表示に戻る（Back to Find/List）] を選択した場合、[回線テンプレートの検索/一覧表示（Find and List Line Template）] ウィンドウが表示されます。

a) 既存の回線テンプレートを検索するには、適切な検索条件を入力し、[検索（Find）]をクリックします。

b) 新しい回線テンプレートを追加するには、[新規追加（Add New）] をクリックします。

BAT テンプレートでの IP サービスの追加または更新

この機能が BAT テンプレートに直接含まれている Cisco Unified IP Phone モデルに、Cisco Unified IP Phone サービスを登録できます。ユーザや電話を IP サービスに一括で登録するには、IP サービスに共通のサービスパラメータが必要で、電話テンプレートを使用して登録する必要があります。固有のサービスパラメータを持つ IP サービスは一括登録できません。固有のパラメータを持つサービスの場合、CSV ファイルを使用します。

手順

Step 1 IP サービスを追加する電話テンプレートを見つけます。

Step 2 [電話テンプレートの設定（Phone Template Configuration）] ウィンドウから、[関連情報（Associated Information）] 領域にある [新規SURLの追加（Add a new SURL）] をクリックします。
ポップアップ ウィンドウが表示されます。このウィンドウで、使用可能な Cisco Unified IP Phone サービスに登録できます。

Step 3 [サービスの選択（Select a Service）] ドロップダウンリスト ボックスで、すべての電話を登録するサービスを選択します。[サービスの説明（Service Description）] ボックスには、選択したサービスの詳細が表示されます。

Step 4 [次へ（Next）] をクリックします。

Step 5 [サービス名（Service Name）] フィールドで、必要に応じてサービスの名前を変更します。

Step 6 選択したサービスを関連付けるか、他のサービスをテンプレートに追加します。

a) これらの電話サービスを電話テンプレートに関連付けるには、[保存（Save）] をクリックします。

b) さらにサービスを追加するには、Step 3 （364 ページ） ～ Step 6 （364 ページ） を繰り返します。

c) すべてのサービスをテンプレートに追加するには、[更新（Update）] をクリックします。

選択したテンプレートに対してサービスの追加または更新を実行した後は、次のステップに進みます。

Step 7 ポップアップ ウィンドウを閉じます。

BAT テンプレート内の短縮ダイヤルの追加または更新

電話ボタン テンプレートに短縮ダイヤル ボタンがある場合、一般の電話用および Cisco VGC 電話用の BAT テンプレートで短縮ダイヤルを追加したり、更新したりできます。BAT テンプレートに使用される電話ボタンテンプレートによって、使用できる短縮ダイヤルボタンの数が決定します。

手順

Step 1 短縮ダイヤルを追加する電話テンプレートを見つけます。

Step 2 [電話テンプレートの設定（Phone Template Configuration）] ウィンドウから、次のいずれかを実行します。

a) [関連情報（Associated Information）] 領域にある [新規 SDの追加（Add a new BLF SD）] をクリックします。

b) ウィンドウの右上隅にある [関連リンク（Related Links）] ドロップダウンリスト ボックスから [短縮ダイヤルの追加/更新（Add/Update Speed Dials）] を選択します。

ポップアップ ウィンドウが表示されます。このウィンドウで、Cisco Unified IP Phone と拡張モジュールの短縮ダイヤルボタンを指定できます。

Step 3 [短縮ダイヤルの設定（Speed Dial Settings）] 領域の [番号（Number）] フィールドに、電話番号（アクセス コードまたは長距離コードを含む）を入力します。

（注） 電話番号を入力する際に、必要に応じて、強制承認コード（FAC）/クライアント識別コード（CMC）を続けて入力することもできます。このフィールドには電話番号、FAC、CMC を連続して、またはカンマ（,）で区切って入力できます。短縮ダイヤルには、コールが接続された後に DTMF ディジットとして送信される PIN、パスワード、またはその他の数字を含めることができます。短縮ダイヤルで接続するときに一時停止を必要とする場合、1 つ以上のカンマ（,）を入力することができます。各カンマは 2 秒間の一時停止を表します。DTMF ディジットは、コールが接続され、カンマの数に対応する適切な一時停止期間が経過した後に送信されます。

Step 4 [ラベル（Label）] フィールドに、短縮ダイヤル番号に対応するラベルを入力します。

Step 5 [短縮ダイヤル設定（Abbreviated Dial Settings）] 領域で、該当する IP フォン モデルの短縮ダイヤルを設定できます。Step 3 （365 ページ） を繰り返します。

Step 6 [保存（Save）] をクリックします。
BAT によってテンプレートに短縮ダイヤルの設定が挿入され、ポップアップ ウィンドウが閉じます。

BAT テンプレート内の話中ランプフィールドの追加または更新

電話ボタン テンプレートに短縮ダイヤル ボタンがある場合、一般の電話用および Cisco VGC 電話用の BAT テンプレートで話中ランプフィールドを追加したり、更新したりできます。BAT テンプレートに使用される電話ボタン テンプレートによって、使用できる BLF SD ボタンの数が決定します。

手順

Step 1 短縮ダイヤルを追加する電話テンプレートを見つけます。

Step 2 [電話テンプレートの設定（Phone Template Configuration）] ウィンドウで、次のいずれかを実行します。

a) [関連情報（Associated Information）] 領域にある [新規BLF SDの追加（Add a new BLF SD）] をクリックします。

b) ウィンドウの右上にある [関連リンク（Related Links）] ドロップダウンリストから、[話中ランプフィールドスピードダイヤルの追加/更新（Add/Update Busy Lamp Field Speed Dials）] を選択します。

ポップアップ ウィンドウが表示されます。このウィンドウで、Cisco Unified IP Phone および拡張モジュールに対して話中ランプフィール スピードダイヤル（BLF SD）ボタンを指定できます。

Step 3 [短縮ダイヤルの設定（Speed Dial Settings）] 領域の [接続先（Destination）] フィールドに、接続先（アクセス コードまたは長距離コードを含む）を入力します。

Step 4 ドロップダウンリストから電話番号を選択します。[検索（Find）] をクリックして、電話番号を検索できます。

Step 5 [ラベル（Label）] フィールドに、BLF SD 番号に対応するラベルを入力します。

Step 6 [保存（Save）] をクリックします。
BAT によってテンプレートに BLF SD の設定が挿入され、ポップアップ ウィンドウが閉じます。

BAT テンプレート内の話中ランプフィール ダイレクト通話パークの追加または更新

電話ボタンテンプレートに短縮ダイヤルボタンが備えられている場合、一般の電話用およびCisco VGC電話用のBATテンプレートで話中ランプフィール（BLF）ダイレクト通話パークを追加したり、更新したりできます。この BAT テンプレートに使用される電話ボタン テンプレートによって、使用できる BLF ダイレクト通話パーク ボタンの数が決定されます。

手順

Step 1 BLF ダイレクト通話パークを追加する電話テンプレートを見つけます。

Step 2 [電話テンプレートの設定（Phone Template Configuration）] ウィンドウで、次のいずれかを実行します。

a) [関連情報（Associated Information）] 領域にある [新規 BLF ダイレクト通話パークの追加（Add a new BLF Directed Call Park）] をクリックします。

b) ウィンドウの右上隅にある [関連リンク（Related Links）] ドロップダウンリストボックスから [BLF ダイレクト通話パークの追加/更新（Add/Update BLF Directed Call Park）] を選択します。

ポップアップ ウィンドウが表示されます。このウィンドウで、Cisco Unified IP Phone および拡張モジュールに対して、BLF ダイレクト通話パーク ボタンを指定できます。

Step 3 [割り当てられていない話中ランプフィールド/ダイレクトコールパークの設定（Unassigned Busy Lamp Field/Directed Call Park Settings）] 領域で、ドロップダウンリストから電話番号を選択します。[検索（Find）] をクリックして、電話番号を検索できます。

Step 4 [ラベル（Label）] フィールドに、BLF ダイレクト通話パーク番号に対応するラベルを入力します。

Step 5 [保存（Save）] をクリックします。
BAT によってテンプレートに BLF ダイレクト通話パークの設定が挿入され、ポップアップ ウィンドウが閉じます。

BAT テンプレート内のインターコムテンプレートの追加または更新

1 つ以上のインターコムテンプレートを BAT テンプレートに追加できます。または既存のインターコムテンプレートを BAT テンプレートで更新できます。BAT テンプレートに使用しているボタン テンプレートによって、追加または更新できる回線数が決定します。複数回線を持つ標準電話テンプレートを作成することができます。その標準テンプレートを使用して、単一回線の電話機、または標準テンプレート内の回線数を上限とする複数回線の電話機を追加できます。このバッチ内のすべての電話機またはユーザデバイスプロファイルは、インターコムテンプレートに選択した設定を使用します。

インターコムテンプレートには英数字を使用することを推奨します。番号を指定すると、実際の電話番号と競合する可能性があるためです。英数字を使用することにより、コール ピックアップ グループ番号や通話パーク番号などの機能とも競合せずに済みます。

BAT テンプレートに表示される回線の最大数は、BAT 電話テンプレートの作成時に選択したモデルおよびボタン テンプレートによって異なります。一部の Cisco Unified IP Phone モデルでは、Cisco Unified IP Phone サービスと短縮ダイヤルもテンプレートに追加できます。

手順

Step 1 インターコムテンプレートを追加する電話テンプレートを見つけます。

Step 2 [電話テンプレートの設定（Phone Template Configuration）] ウィンドウで、[関連情報（Associated Information）] 領域にある [インターコム[1] -新規インターコムの追加（Intercom [1] - Add a new Intercom）] をクリックします。
[インターコムテンプレートの設定（Intercom Template Configuration）] ウィンドウが表示されます。

Step 3 インターコムテンプレートの設定に適切な値を入力するか、選択します。

Step 4 [保存（Save）] をクリックします。
BAT によって、インターコムテンプレートが電話テンプレートの設定に追加されます。

Step 5 その他のインターコムテンプレートの設定を追加するには、Step 2 （367 ページ） ～Step 4 （367 ページ） を繰り返します。

[インターコムテンプレートの設定（Intercom Template Configuration）] ウィンドウの右上隅にある [関連リンク（Related Links）] ドロップダウンリスト ボックスから [検索/一覧表示に戻る（Back to Find/List）] を選択した場合、[インターコム電話番号の検索/一覧表示（Find and List Intercom Directory Number）] ウィンドウが表示されます。

（注） [インターコムテンプレートの設定（Intercom Template Configuration）] ウィンドウの右上隅にある [関連リンク（Related Links）] ドロップダウンリスト ボックスから [検索/一覧表示に戻る（Back to Find/List）] を選択した場合、[インターコム電話番号の検索/一覧表示（Find and List Intercom Directory Number）] ウィンドウが表示されます。

a) 既存のインターコム電話番号を検索するには、[検索（Find）]をクリックし、適切な検索条件を入力します。
b) 新しいインターコム電話番号を追加するには、[インターコム電話番号の検索/一覧表示（Find and List Intercom Directory Number）] ウィンドウで、[新規追加（Add New）] をクリックします。

BAT スプレッドシートを使用した電話用 CSV データファイルの作成

BAT スプレッドシートを使用して、CSV データファイルを作成します。スプレッドシート内でファイル形式を定義できます。そうすると、BAT スプレッドシートは、そのデータファイル形式を使用して CSV データファイルのフィールドを表示します。

（注） いずれかのフィールドにカンマを入力すると、BAT 形式にエクスポートする際に BAT.xlt はそのフィールド エントリを二重引用符で囲みます。

BAT スプレッドシートに空の行を含めると、その空の行がファイルの終わりとして扱われます。空の行より後に入力されたデータは BAT 形式に変換されません。

CTI ポートの追加時に、ダミー MAC アドレス オプションを使用できます。このオプションを使用すると、ダミー MAC アドレスの形式で、各 CTI ポートに一意のデバイス名が指定されます。このデバイス名は、後で Cisco Unified Communications Manager Administration または Unified CM Auto-Register Phone Tool を使用して手動で更新できます。ダミー MAC アドレス オプションは、H.323 クライアント、VGC 電話機、または VGC 仮想電話機に使用しないでください。

ダミーMACアドレス オプションは、自動的に、次の形式でダミーMACアドレスを生成します。

XXXXXXXXXXXX

ここで、X は、任意の 12 文字の 16 進数値（0 ～ 9 と A ~ F）を表します。

注目 BAT スプレッドシートで電話機用に定義する回線や短縮ダイヤルの数は、BAT 電話テンプレートで定義された数を超えないようにしなければなりません。超えてしまうと、CSV データファイルや BAT テンプレートを挿入しようとするときにエラーが発生します。

BAT スプレッドシート内のすべてのフィールドの編集が終了したら、その内容を CSV 形式のデータファイルにエクスポートできます。エクスポートされた CSV 形式のデータファイルには、次のようなデフォルトのファイル名が割り当てられます。

```
<tabname>-<timestamp>.txt
```

ここで、<tabname> は電話機などの作成された入力ファイルのタイプを表し、<timestamp> はファイルが作成された正確な日時を表します。

エクスポートしたファイルをローカル ワークステーションに保存したら、CSV 形式のデータファイルの名前を変更できます。

（注） CSV ファイル名にカンマが含まれていると（例：abcd,e.txt）、Unified Communications Manager サーバにアップロードできません。

手順

Step 1 BAT スプレッドシートを開くには、BAT.xlt ファイルを探してダブルクリックします。

Step 2 スプレッドシートの機能を使用するように求められたら、[マクロを有効にする（Enable Macros）] をクリックします。

Step 3 電話のオプションを表示するには、スプレッドシートの下部にある [電話（Phone）] タブをクリックします。

Step 4 次のいずれかのデバイスタイプを表すラジオボタンを選択します。

選択するデバイスタイプによって、BAT スプレッドシートでのデータの検証基準が決まります。

- 電話機
- CTI ポート（CTI Port）
- H.323 クライアント（H.323 Client）
- VGC フォン（VGC Phones）
- VGC 仮想電話機（VGC Virtual Phones）
- Cisco IP Communicator フォン（Cisco IP Communicator Phone）

スプレッドシートには、選択されたデバイスに対して選択可能なオプションが表示されます。たとえば、電話を選択すると、電話回線や短縮ダイヤルの数に関するフィールドが表示されます。

Step 5 各電話機の BAT スプレッドシートに表示されるデバイスや回線のフィールドを選択します。次の手順を実行します。

a) [ファイル形式の作成（Create File Format）] をクリックします。

b) デバイス フィールドを選択するには、[デバイスフィールド（Device Field）] ボックスでデバイスフィールド名をクリックしてから、矢印をクリックしてそのフィールドを [選択済みのデバイスフィールド（Selected Device Fields）] ボックスに移動します。

CSV データファイルには、[MAC アドレス/デバイス名（MAC Address/Device Name）] と [説明（Description）] が含まれている必要があります。そのため、これらのフィールドは常に選択されたままになります。

ヒント リスト内のアイテムの範囲を選択するには、**Shift** キーを押したままにします。ランダムなフィールド名を選択するには、**Ctrl** キーを押しながらフィールド名をクリックします。

c) [回線フィールド（Line Field）] ボックスで回線フィールド名をクリックしてから、矢印をクリックしてそのフィールドを [選択済みの回線フィールド（Selected Line Fields）] ボックスに移動します。

ヒント [選択済みの回線（Selected Line）] および [デバイス（Device）] ボックス内のアイテムの順序を変更するには、アイテムを選択して、上矢印と下矢印を使用してそのフィールドをリスト内で上下に移動します。

d) 既存の CSV 形式を上書きするかどうかを尋ねるメッセージが表示されます。[作成（Create）] をクリックして、CSV データファイル形式を変更します。

e) [OK] をクリックします。
選択されたフィールドの新しい列が指定された順序で BAT スプレッドシート内に表示されます。

Step 6 右にスクロールして [電話回線数（Number of Phone Lines）] ボックスを見つけ、電話機の回線数を入力します。

（注） BAT テンプレートで設定された回線の数を超えた回線数を入力することはできません。

Step 7 電話機では、[短縮ダイヤルの最大数（Maximum Number of Speed Dials）] ボックスに、短縮ダイヤル ボタンの数を入力する必要があります。

（注） BAT テンプレートで設定された短縮ダイヤルの数を超えた短縮ダイヤル数を入力することはできません。

数値を入力すると、短縮ダイヤル番号ごとの列が表示されます。

Step 8 [BLF 短縮ダイヤルの最大数（Maximum Number of BLF Speed Dials）] ボックスに、話中ランプ フィールド（BLF）短縮ダイヤル ボタンの数を入力します。
数値を入力すると、BLF 短縮ダイヤル番号ごとの列が表示されます。

Step 9 スプレッドシートで、各回線の個々の電話についてデータを入力します。

すべての必須フィールドと関連するオプション フィールドに値を入力します。各列の見出しではフィールドの長さが指定され、また必須であるか、オプションであるかも指定されます。電話フィールドの説明については、オンライン ヘルプを参照してください。

Step 10 各電話の MAC アドレスを入力しなかった場合は、[ダミー MAC アドレスの作成（Create Dummy MAC Address）] チェックボックスをオンにする必要があります。

注目 ダミー MAC アドレス オプションは、H.323 クライアント、VGC 電話機、または VGC 仮想電話機に使用しないでください。

Step 11 BAT Excel スプレッドシートから CSV 形式のデータファイルにデータを移すには、[BAT 形式にエクスポート（Export to BAT Format）] をクリックします。

ヒント エクスポートされた CSV データファイルを読み取る方法については、BAT の [電話の挿入（Insert phones）] ウィンドウにある [サンプルファイルの表示（View Sample File）] へのリンクをクリックします。

ファイルは、デフォルトのファイル名 `<tabname>-<timestamp>.txt` でローカル ワークステーション上の選択したフォルダに保存されます。

テキスト エディタを使用したカスタム電話機ファイル形式の作成

テキストエディタを使用して、テキストベースのCSVデータファイルのカスタム電話機ファイル形式を作成できます。

手順

Step 1 **[一括管理（Bulk Administration）]>[電話（Phones）]>[電話ファイル形式（Phone File Format）]>[ファイル形式の作成（Create File Format）]** の順に選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 **[形式名（Format Name）]** フィールドに、このカスタム形式の名前を入力します。

Step 4 カスタムファイル形式に表示するフィールドを選択します。次の手順を実行します。

a) デバイスフィールドを選択するには、**[デバイスフィールド（Device Field）]** ボックスでデバイスフィールド名をクリックしてから、矢印をクリックしてそのフィールドを**[選択済みのデバイスフィールド（Selected Device Fields）]** ボックスに移動します。

CSV データファイルには、[MAC アドレス/デバイス名（MAC Address/Device Name）] と [説明（Description）] が含まれている必要があります。そのため、これらのフィールドは常に選択されたままになります。

ヒント リスト内のアイテムの範囲を選択するには、**Shift** キーを押したままにします。ランダムなフィールド名を選択するには、**Ctrl** キーを押しながらフィールド名をクリックします。

b) [回線フィールド（Line Field）] ボックスで回線フィールド名をクリックしてから、矢印をクリックしてそのフィールドを [選択済みの回線フィールド（Selected Line Fields）] ボックスに移動します。

c) [インターコム DN フィールド（Intercom DN Field）] ボックスでインターコム DN フィールド名をクリックし、矢印をクリックしてそのフィールドを [選択済みのインターコム DN フィールド順序（Selected Intercom DN Fields Order）] ボックスに移動します。

ヒント [選択済みの回線フィールド（Selected Line Fields）] ボックス、[選択済みのデバイス フィールド（Selected Device Fields）] ボックス、および [選択済みのインターコム DN フィールド順序（Selected Intercom DN Fields Order）] ボックス内のアイテムの順序を変更できます。アイテムを選択して、上矢印と下矢印を使用してそのフィールドをリスト内で上下に移動します。

Step 5 [IP 電話サービスの最大数（IP Phone Services Maximums）] 領域で、以下のフィールドに最大値を入力します。

- 短縮ダイヤルの最大数（Maximum Number of Speed Dials）
- BLF 短縮ダイヤルの最大数（BLF Maximum Number of Speed Dials）
- BLF ダイレクト通話パークの最大数（Maximum Number of BLF Directed Call Parks）
- IP 電話サービスの最大数（Maximum Number of IP Phone Services）
- IP 電話サービスパラメータの最大数（Maximum Number of IP Phone Service Parameters）

Step 6 [保存（Save）] をクリックします。

[電話ファイル形式の検索/一覧表示（Find and List Phone File Formats）] ウィンドウの [ファイル形式名（File Format Names）] リストに、カスタム ファイル形式の名前が表示されます。

Unified Communications Manager への電話の挿入

電話機レコードを Unified Communications Manager データベースに挿入するときは、ターゲット CSV データファイルと、電話機レコードの挿入方法を定義します。既存の電話機レコードを上書きするには、次の操作から任意の組み合わせを選択します。または、アップロード時にレコードを挿入することもできます。

- 新しいスピードダイヤルを追加する前に既存のすべての短縮ダイヤルを削除
- 新しい BLF 短縮ダイヤルを追加する前に既存のすべての BLF 短縮ダイヤルを削除
- 新しい BLF ダイレクトコールパークを追加する前に既存のすべての BLF ダイレクトコールパークを削除
- 新しいサービスを追加する前に既存の登録済みサービスをすべて削除

（注） 電話機レコードは、挿入前に検証する必要があります。

（注） BAT は、次の形式による電話番号 URI フィールドを想定しています。

電話番号 1 での URI 1、電話番号 1 での URI 1 ルート パーティション、電話番号 1 での URI 1 プライマリ。

ダミー MAC アドレス オプションを使用できます。CTI ポートを追加するときにこのオプションを使用すると、ダミー MAC アドレスの形式で、各 CTI ポートに一意のデバイス名が指定されます。このデバイス名は、後で Unified Communications Manager Administration または Unified CM Auto-Register Phone Tool を使用して手動で更新できます。ダミー MAC アドレス オプションは、H.323 クライアント、VGC 電話機、または VGC 仮想電話機に使用しないでください。

ダミーMACアドレスオプションは、自動的に、次の形式でダミーMACアドレスを生成します。

XXXXXXXXXXXX

ここで、X は、任意の 12 文字の 16 進数値（0 ～ 9 と A ~ F）を表します。

始める前に

- 追加するデバイス用に、Unified Communications Manager 一括管理（BAT）の電話テンプレートが必要です。データファイル アップロードのターゲットと方法を選択することができます。電話機レコードは、挿入前に検証する必要があります。
- 電話機または他の IP テレフォニーデバイス固有の詳細情報を含むカンマ区切り値（CSV）形式のデータファイルが必要です。

手順

Step 1 **[一括管理（Bulk Administration）] > [電話（Phones）] > [電話の挿入（Insert Phones）]** の順に選択します。

Step 2 アップロードする電話機レコードのファイル形式タイプを指定します。

a) カスタマイズされたファイル形式を使用する電話機レコードを挿入するには、[電話固有の詳細の挿入（Insert Phones Specific Details）] ラジオ ボタンをクリックして、Step 3 （373 ページ）と Step 5 （373 ページ） に進みます。

b) [すべての詳細（All Details）] オプションを使用して生成したエクスポート済みの電話ファイルから電話レコードを挿入するには、[電話のすべての詳細の挿入（Insert Phones All Details）] ラジオ ボタンをクリックします。

Step 3 [ファイル名（File Name）] ドロップダウンリスト ボックスで、この特定の一括トランザクションのために作成した CSV データファイルを選択します。次に、[カスタムファイルを使用した電話の更新の許可（Allow Update Phone with Custom File）] チェックボックスをオンにして、選択したカスタム ファイルを使用して電話機を更新できるようにします。

Step 4 [既存の設定の上書き（Override the existing configuration）] チェックボックスをオンにすると、既存の電話の設定が、挿入するファイルに含まれている情報で上書きされます。次に、アップロード中に実行するアップロードアクションの横にあるチェックボックスをオンにします。

[既存の設定の上書き（Override the existing configuration）] チェックボックスをオンにした場合は、次のアップロード アクションが選択可能になります。

- 新しい短縮ダイヤルを追加する前に既存のすべての短縮ダイヤルを削除
- 新しい BLF 短縮ダイヤルを追加する前に既存のすべての BLF 短縮ダイヤルを削除
- 新しい BLF ダイレクトコールパークを追加する前に既存のすべての BLF ダイレクトコールパークを削除
- 新しいサービスを追加する前に既存の登録済みサービスをすべて削除

（注） アップロード時に CSV データファイルの既存のレコードにこれらのレコードを追加する場合は、このチェックボックスをオフにします。

Step 5 [固有の詳細（Specific Details）] オプションを選択した場合は、[電話テンプレート名（Phone Template Name）] ドロップダウンリストで、このタイプのバルク トランザクション用に作成した BAT 電話テンプレートを選択します。

注目 CSV データファイルに個別の MAC アドレスを入力しなかった場合は、[ダミー MAC アドレスの作成（Create Dummy MAC Address）] チェックボックスをオンにする必要があります。この情報は後で手動で更新できます。Step 8 （374 ページ） にスキップします。データ入力ファイルで MAC アドレスまたはデバイス名を指定した場合は、このオプションを選択しないでください。

ユーザに割り当てられる電話機の MAC アドレスがわからない場合には、このオプションを選択します。電話機が接続されると、そのデバイス用に MAC アドレスが登録されます。

Step 6 [ジョブ情報（Job Information）] 領域に、ジョブの説明を入力します。

Step 7 挿入方法を選択します。次のいずれかを実行します。

a) すぐに電話機レコードを挿入する場合は、[今すぐ実行（Run Immediately）] をクリックします。

b) 後で電話レコードを挿入する場合は、[後で実行（Run Later）] をクリックします。

Step 8 電話機レコードを挿入するためのジョブを作成するには、[送信（Submit）] をクリックします。

このジョブをスケジュール設定またはアクティブ化するには、[ジョブの設定（Job Configuration）] ウィンドウを使用します。

次のタスク

挿入される電話機が Cisco Unified Mobile Communicator タイプである場合は、挿入ジョブの完了後にデバイスをリセットする必要があります。電話機をリセットするには、**[一括管理（Bulk Administration）] > [電話（Phones）] > [電話のリセット/リスタート（Reset/Restart Phones）]** オプションを使用できます。

ユーザの追加

BAT スプレッドシートを使用して複数の新しいユーザを Unified Communications Manager データベースに一括で追加するには、CSV データファイルを作成する必要があります。Cisco IP SoftPhone のように CTI ポートを必要とするアプリケーションを使用するユーザのために、BAT で CTI ポートを既存のユーザに関連付けることができます。

手順

Step 1 追加する各ユーザに対して個別の値を定義するには、カンマ区切り値（CSV）データファイルを作成します。

Step 2 BAT を使用して、ユーザを Unified Communications Manager データベースに挿入します。

BAT スプレッドシートを使用したユーザ用 CSV データファイルの作成

Unified Communications Manager データベースに新しいユーザを追加するための詳細情報を BAT スプレッドシートに入力し、それを CSV データファイルに変換することができます。

（注） BAT スプレッドシートに空の行を含めると、その空の行がファイルの終わりとして扱われます。空の行より後に入力されたデータは BAT 形式に変換されません。

BAT スプレッドシートでユーザを追加するためのフィールドを編集し終えたら、その内容を CSV 形式のデータファイルにエクスポートできます。エクスポートされた CSV 形式のデータファイルには、次のようなデフォルトのファイル名が割り当てられます。

```
<tabname>-<timestamp>.txt
```

ここで、<tabname> は電話機などの作成された入力ファイルのタイプを表し、<timestamp> はファイルが作成された正確な日時を表します。

エクスポートしたファイルをローカル ワークステーションに保存したら、CSV 形式のデータファイルの名前を変更できます。いずれかのフィールドにカンマを入力すると、BAT 形式にエクスポートする際に BAT.xlt はそのフィールド エントリを二重引用符で囲みます。

（注） CSV ファイル名にカンマが含まれていると（例：abcd,e.txt）、Unified Communications Manager サーバにアップロードできません。

手順

Step 1 BAT スプレッドシートを開くには、BAT.xlt ファイルを探してダブルクリックします。

Step 2 スプレッドシートの機能を使用するように求められたら、[マクロを有効にする（Enable Macros）] をクリックします。

Step 3 ユーザを追加するには、スプレッドシートの下部にある [ユーザ（Users）] タブをクリックします。

Step 4 すべての必須フィールドと関連するオプション フィールドに値を入力します。各列の見出しではフィールドの長さが指定され、また必須であるか、オプションであるかも指定されます。

各行に、オンライン ヘルプ ファイルの説明に従って情報を入力します。

- ユーザが複数のデバイスを使用している場合は、デバイスごとに、デバイス名フィールドに入力する必要があります。
- 新規ユーザに関連付ける追加のデバイス名を入力するには、[制御するデバイスの数（Number of Controlled Devices）] テキスト ボックスに値を入力します。

（注） CTI ポート、ATA ポート、H.323 クライアントを含む、すべてのデバイスをユーザと関連付けることができます。

Step 5 新規ユーザに関連付ける追加のデバイス名を入力するには、[制御するデバイスの数（Number of Controlled Devices）] テキスト ボックスに値を入力します。

Step 6 [BAT 形式にエクスポート（Export to BAT Format）] をクリックして、BAT Excel スプレッドシートから CSV 形式データファイルにデータを転送します。

このファイルは、デフォルトのファイル名（<tabname>-<timestamp>.txt）で、C:\XLSDataFiles に保存されます。または [参照（Browse）] を使用して別の既存フォルダに保存することもできます。

ヒント　エクスポートされた CSV データファイルを読み取る方法については、BAT の [ユーザの挿入（Insert Users）] ウィンドウにある [サンプル ファイルの表示（View Sample File）] へのリンクをクリックします。

次のタスク

CSV データファイルを Unified Communications Manager データベース サーバの最初のノードにアップロードして、BAT がデータファイルにアクセスできるようにする必要があります。

Unified Communications Manager データベースへのユーザの挿入

CSV データファイルを使用して、ユーザのグループを Unified Communications Manager データベースに追加できます。ユーザを挿入する目的で CSV ファイルに入力したフィールド値は、ユーザテンプレートに入力された値よりも優先されます。

注目　クレデンシャル ポリシーで [単純すぎるパスワードの確認（check for trivial password）]「」が有効になっており、しかもユーザ テンプレート内のパスワードがユーザ ID である場合、単純すぎるパスワードに関する基準をユーザ ID が満たしていなければ、BAT を使ったユーザ挿入が失敗することがあります。

管理対象デバイスとしてどのデバイスも選択されないまま、プライマリ エクステンションが設定された状態で、BAT を使用してユーザを挿入できます。それには、BAT を使用してユーザを挿入する前に、Unified Communications Manager で DN を定義しておく必要があります。DN を事前に設定する手順の概要は、次のとおりです。

1. DN ページで、ユーザのプライマリ内線番号に関連付ける DN の範囲を作成します。
2. プライマリ エクステンションが設定された BAT テンプレートを作成します（同じ DN の事前設定）。
3. 次の手順に示すように、BAT を使用してユーザを挿入します。

始める前に

ユーザ名、制御するデバイスの名前、および電話番号が格納されている、UTF-8 符号化形式で保存された CSV データファイルが必要です。次のいずれかの方法を使用して、CSV データファイルを作成できます。

- CSV 形式に変換される BAT スプレッドシート
- ユーザ データのエクスポート ファイルを生成するエクスポート ユーティリティ

（注） エクスポート済み BAT ファイルを使ってユーザを挿入するとき、複数ファイルにエクスポートされたユーザに関して、[ユーザID はすでに存在します（User ID already exists）]「」というエラーが表示されることがあります。たとえば、最初の回線マネージャのリストとユーザのリストの両方に、同じマネージャ ユーザ ID が含まれている場合です。

手順

Step 1 **[一括管理（Bulk Administration）] > [ユーザ（Users）] > [ユーザの挿入（Insert Users）]** の順に選択します。

Step 2 [ファイル名（File Name）] フィールドで、この一括トランザクション用に作成した CSV データファイルを選択します。

Step 3 エクスポート ユーティリティを使って CSV データファイルを作成した場合は、[ユーザのエクスポートで作成されたファイル（File created with Export Users）] チェックボックスをオンにします。

Step 4 [ユーザテンプレート名（User Template Name）] ドロップダウンリストから、この挿入で使用するユーザ テンプレートを選択します。

（注） ユーザープロファイル、制御するデバイスの名前、およびディレクトリ番号が、Unified Communications Manager データベースに存在している必要があります。管理対象デバイス名の全体を入力する必要があります。デバイス名に MAC アドレスしか含まれていない場合は、デバイスが存在しないことを示すエラーが BAT に表示されます。

Step 5 [ジョブ情報（Job Information）] 領域に、ジョブの説明を入力します。

Step 6 挿入方法を選択します。次のいずれかを実行します。

a) ユーザ レコードをすぐに挿入する場合は、[今すぐ実行（Run Immediately）] をクリックします。

b) ユーザ レコードを後で挿入する場合は、[後で実行（Run Later）] をクリックします。

Step 7 ユーザ レコードを挿入するためのジョブを作成するには、[送信（Submit）] をクリックします。

このジョブをスケジュールするか、アクティブ化するには、[一括管理（Bulk Administration）] メイン メニューの [ジョブスケジューラ（Job Scheduler）] オプションを使用します。

BAT スプレッドシートを使用したユーザと電話機の追加

電話機とユーザを一括して追加するための CSV データファイルを作成します。

手順

Step 1 BAT スプレッドシートを開くには、BAT.xlt ファイルを探してダブルクリックします。

BAT.xlt ファイルをダウンロードできます。

Step 2 スプレッドシートの機能を使用するように求められたら、[マクロを有効にする（Enable Macros）] をクリックします。

Step 3 スプレッドシートの下部にある [電話-ユーザ（Phone-Users）] タブをクリックします。

Step 4 BAT スプレッドシートを使用した電話用 CSV データファイルの作成（367 ページ）のステップ 4 から 10 に従います。

電話およびユーザ ファイル形式の追加

テキストベースのCSVデータファイルで電話とユーザのファイル形式を追加できます。CSVデータファイルを作成した後、ファイル形式をテキストベースのCSVデータファイルと関連付ける必要があります。ファイル形式を CSV ファイルと関連付けると、各フィールドの名前は CSV データファイルの最初のレコードとして表示されます。この情報を使用して、正しい順序で各フィールドに値を入力したことを確認できます。

始める前に

更新する各ユーザに対して個別の値を定義するCSVデータファイルを作成する必要があります。

テキストエディタを使用してCSVデータファイルを作成する際に、テキストベースのファイルに値を入力するためのファイル形式を作成します。ファイル形式によって指定した順序でテキストファイルに値を入力します。

手順

Step 1 **[一括管理（Bulk Administration）] > [電話とユーザ（Phones and Users）] > [電話とユーザのファイル形式（Phones & Users File Format）] > [ファイル形式の割り当て（Assign File Format）]** の順に選択します。
[ファイル形式の設定の追加（Add File Format Configuration）] ウィンドウが表示されます。

Step 2 [ファイル名（File Name）] フィールドで、このトランザクション用に作成したテキストベースの CSV ファイルを選択します。

Step 3 [ファイル形式名（Format File Name）] フィールドで、このタイプの一括トランザクション用に作成したファイル形式を選択します。

Step 4 一致するファイル形式をCSVデータファイルと関連付けるジョブを作成するには、[送信（Submit）] をクリックします。

Step 5 このジョブをスケジュールするか、アクティブ化するには、[一括管理（Bulk Administration）] メイン メニューの [ジョブスケジューラ（Job Scheduler）] オプションを使用します。

（注） ファイル形式を追加すると、ユーザ フィールドが自動的に作成されます。

Unified Communications Manager への電話機とユーザの挿入

電話とユーザのグループを Unified Communications Manager データベースとディレクトリに追加できます。

（注） 電話機レコードは、挿入前に検証する必要があります。

ダミー MAC アドレス オプションを使用できます。CTI ポートを追加するときにこのオプションを使用すると、ダミー MAC アドレスの形式で、各 CTI ポートに一意のデバイス名が指定されます。このデバイス名は、後で Unified Communications Manager Administration または Unified CM Auto-Register Phone Tool を使用して手動で更新できます。ダミー MAC アドレス オプションは、H.323 クライアント、VGC 電話機、または VGC 仮想電話機に使用しないでください。

ダミーMACアドレス オプションは、自動的に、次の形式でダミーMACアドレスを生成します。

XXXXXXXXXXXX

ここで、X は、任意の 12 文字の 16 進数値（0 ～ 9 と A ~ F）を表します。

始める前に

1. カンマ区切り値（CSV）データファイルを作成して、挿入する電話とユーザごとに個々の値を定義します。ユーザを伴う電話を追加するために BAT スプレッドシート（BAT.xlt）を使って CSV データファイルを作成することも、ユーザと電話の組み合わせを追加するために CSV 形式のカスタム テキスト ファイルを作成することもできます。
2. ファイル形式を CSV データファイルに関連付けます。
3. 電話機とユーザ レコードを検証します。

手順

Step 1 **[一括管理（Bulk Administration）] > [電話とユーザ（Phones & Users）] > [ユーザ付きの電話の挿入（Insert Phones with Users）]** の順に選択します。

Step 2 [ファイル名（File Name）] フィールドで、この一括トランザクション用に作成した CSV データファイルを選択します。

Step 3 [電話テンプレート名（Phone Template Name）] フィールドで、このトランザクションに使用した BAT 電話機テンプレートを選択します。

注目 CSV データファイルに個別の MAC アドレスを入力しなかった場合は、[ダミー MAC アドレスの作成（Create Dummy MAC Address）] チェックボックスをオンにする必要があります。この情報は後で手動で更新できます。データ入力ファイルで MAC アドレスまたはデバイス名を指定した場合は、このオプションを選択しないでください。

ユーザに割り当てられている電話の MAC アドレスがわからない場合には、このオプションを選択します。電話機が接続されると、そのデバイス用に MAC アドレスが登録されます。

Step 4 [ユーザテンプレート名（User Template Name）] フィールドで、このトランザクションに使用した BAT ユーザ テンプレートを選択します。

Step 5 [ジョブ情報（Job Information）] 領域に、ジョブの説明を入力します。

Step 6 挿入方法を選択します。次のいずれかを実行します。

a) すぐにユーザ付き電話を挿入する場合は、[今すぐ実行（Run Immediately）] をクリックします。

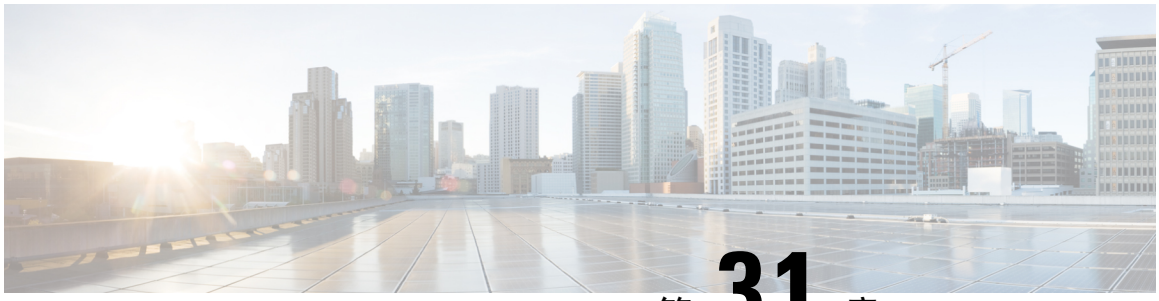
b) 後でユーザ付き電話を挿入する場合は、[後で実行（Run Later）] をクリックします。

Step 7 電話機とユーザのレコードを挿入するためのジョブを作成するには、[送信（Submit）] をクリックします。

このジョブをスケジュールしてアクティブ化するには、[一括管理（Bulk Administration）] メインメニューの [ジョブ スケジューラ（Job Scheduler）] オプションを使用します。

第 V 部

エンドポイントのプロビジョニング



第 31 章

エンドポイントの設定

エンドポイント プロビジョニングのデフォルト値

この項の情報を使用して、エンドポイント デバイスを設定し、エンドポイントにユーザを関連付けます。

ユニファイドコミュニケーションマネージャには、エンドポイントを追加する前にプロビジョニングできるデバイスのデフォルトのセットが含まれています。これらのデバイスのデフォルト設定を事前に設定した場合、新しいユーザをプロビジョニングすると、適用される設定に基づいてデバイスが自動的に設定されます。

次に、エンドポイントプロビジョニングの2つのデフォルト設定を示します。

- デバイスのデフォルト値の設定
- エンタープライズ電話設定の構成

エンドポイントプロビジョニングのデフォルトの前提条件

エンドポイントの登録用に設定されているポートを確認します。Cisco Unified CM Administration から、**[システム（System）] > [Cisco Unified CM]** に移動し、サーバを選択して、構成されているポート設定を確認します。

（注） ほとんどの場合、ポートをデフォルト設定から変更する必要はありません。

エンドポイントプロビジョニングのデフォルトのタスクフロー

システムのデバイスを設定するには、このタスクフローを実行します。

手順

	コマンドまたはアクション	目的
Step 1	デバイスのデフォルト値の設定（385 ページ）	Unified Communications Manager ノードに自動登録するデバイスに適用される、デフォルト設定を変更できます。各タイプのデバイスには、特定のデフォルトのセットが設定されています。
Step 2	デバイスプロファイルの設定（388 ページ）	（**オプション**）ユーザ用の特定のデバイスに関連付けられている一連の属性で構成される、デバイス プロファイルを設定できます。
Step 3	デフォルト デバイス プロファイルの設定（386 ページ）	ユーザ デバイス プロファイルが設定されていない電話機にユーザがログインするたびに電話機が取得する、デフォルトのデバイス プロファイルを設定できます。
Step 4	デフォルトのデバイスプロファイルでのソフトキーテンプレートの設定（386 ページ）	（**オプション**）ソフトキー テンプレートに追加するデフォルトのデバイスプロファイルを追加できます。
Step 5	エンタープライズ電話の設定（389 ページ）	同じクラスタ内のすべての電話に適用されるエンタープライズ電話の基本設定を指定できます。

デバイスのデフォルト値の設定

デバイスのデフォルト設定の更新

デバイスのデフォルト設定を構成するには、次の手順を実行します。この設定では、デフォルトのファームウェアロード、デフォルトのデバイスプール、ソフトキーテンプレート、および登録方法（自動登録またはアクティベーションコード）を割り当てることができます。

始める前に

デバイスのデフォルト設定を更新する前に、システムに適用する次のタスクを実行します。

- TFTP サーバにデバイスの新しいファームウェア ファイルを追加します。
- デバイスのデフォルトを使用して、ディレクトリに存在しないファームウェア ロードを割り当てると、それらのデバイスは割り当てられたファームウェアをロードできません。
- 新しいデバイスプールを設定します。デバイスが電話の場合は、新しい電話テンプレートを設定します。

手順

Step 1 Cisco Unified CM Administration で、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [デバイスのデフォルト（Device Defaults）]** を選択します。

Step 2 [デバイスのデフォルト設定（Device Defaults Configuration）] ウィンドウで、更新するデバイス タイプに適用可能な設定を変更し、[保存（Save）] をクリックします。フィールドの説明については、オンライン ヘルプを参照してください。

- ロード情報（Load Information）
- デバイスプール（Device Pool）
- 電話テンプレート（Phone Template）

Step 3 そのタイプのすべてのデバイスをリセットして、クラスタ内の全ノードにある該当するタイプのすべてのデバイスに新しいデフォルトをロードするには、デバイス名の左側にある [リセット（Reset）] アイコンをクリックします。

すべてのデバイスをリセットしない場合は、ノードに自動登録された新しいデバイスにだけ、更新されたデフォルト値が設定されます。

デフォルト デバイス プロファイルの設定

ユーザがユーザデバイスプロファイルのない電話機にログインした場合、電話機は必ずデフォルトのデバイス プロファイルを使用します。

デフォルトのデバイスプロファイルには、デバイスタイプ（電話機）、ユーザロケール、電話ボタンテンプレート、ソフトキーテンプレート、マルチレベル優先順位およびプリエンプション（MLPP）情報が含まれています。

手順

Step 1 Cisco Unified CM Administration ウィンドウで、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [デフォルトのデバイス プロファイル（Default Device Profile）]** を選択します。

Step 2 [デフォルトのデバイスプロファイルの設定（Default Device Profile Configuration）] ウィンドウで、[デバイスプロファイルタイプ（Device Profile Type）] ドロップダウンリストから、該当する Cisco Unified IP Phone を選択します。

Step 3 [次へ（Next）] をクリックします。

Step 4 [デバイスプロトコル（Device Protocol）] ドロップダウンリストから、適切なプロトコルを選択します。

Step 5 [次へ（Next）] をクリックします。

Step 6 [デフォルトのデバイスプロファイルの設定（Default Device Profile Configuration）] ウィンドウで、フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 7 [保存（Save）] をクリックします。

デフォルトのデバイスプロファイルでのソフトキーテンプレートの設定

Cisco Unified Communications Manager には、コール処理およびアプリケーション用の標準のソフトキー テンプレートが含まれています。カスタム ソフトキー テンプレートを作成するときは、標準テンプレートをコピーして、必要に応じて変更します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [ソフトキーテンプレート（Softkey Template）]** を選択します。

Step 2 新しいソフトキー テンプレートを作成するには、この手順を実行します。それ以外の場合は、次のステップに進みます。

a) [新規追加（Add New）] をクリックします。

b) デフォルトのテンプレートを選択して、[コピー（Copy）] をクリックします。
c) [ソフトキーテンプレート名（Softkey Template Name）] フィールドに、テンプレートの新しい名前を入力します。
d) [保存（Save）] をクリックします。

Step 3 既存のテンプレートにソフトキーを追加するには、次の手順を実行します。

a) [検索（Find）] をクリックして、検索条件を入力します。
b) 必要な既存のテンプレートを選択します。

Step 4 [デフォルト ソフトキー テンプレート（Default Softkey Template）] チェックボックスをオンにし、このソフトキー テンプレートをデフォルトのソフトキー テンプレートとして指定します。

（注） あるソフトキーテンプレートをデフォルトのソフトキーテンプレートとして指定した場合、先にデフォルトの指定を解除してからでないと、そのテンプレートは削除することができません。

Step 5 右上隅にある [関連リンク（Related Links）] ドロップダウン リストから [ソフトキー レイアウトの設定（Configure Softkey Layout）] を選択し、[移動（Go）] をクリックします。

Step 6 [設定するコール状態の選択（Select a Call State to Configure）] ドロップダウン リストから、ソフトキーに表示するコール状態を選択します。

Step 7 [選択されていないソフトキー（Unselected Softkeys）] リストから追加するソフトキーを選択し、右矢印をクリックして [選択されたソフトキー（Selected Softkeys）] リストにそのソフトキーを移動します。新しいソフトキーの位置を変更するには、上矢印と下矢印を使用します。

Step 8 追加のコール状態でのソフトキーを表示するには、前述のステップを繰り返します。

Step 9 [保存（Save）] をクリックします。

Step 10 次のいずれかの操作を実行します。

- すでにデバイスに関連付けられているテンプレートを変更した場合は、[設定の適用（Apply Config）] をクリックしてデバイスを再起動します。
- 新しいソフトキー テンプレートを作成した場合は、そのテンプレートをデバイスに関連付けた後にデバイスを再起動します。詳細については、「共通デバイス設定へのソフトキー テンプレートの追加」と「電話機のセクションとソフトキー テンプレートの関連付け」を参照してください。

次のタスク

次のいずれかの設定ウィンドウにあるソフトキーテンプレートドロップダウンからテンプレートを選択すると、カスタマイズされたソフトキーテンプレートをデバイスに適用できます。

- 電話の設定（Phone Configuration）
- ユニバーサルデバイステンプレート（Universal Device Template）
- BAT テンプレート（BAT Template）
- 共通デバイス設定（Common Device Configuration）

- デバイスプロファイル（Device Profile）
- デフォルトのデバイスプロファイル（Default Device Profile）
- UDP プロファイル（UDP Profile）

デバイスプロファイルの設定

デバイスプロファイルは特定のデバイスに関連付けられた属性のセットで構成されます。Cisco Extension Mobility 機能を使用するために、作成したデバイスプロファイルをエンドユーザに関連付けることができます。

手順

Step 1 Cisco Unified CM Administration ウィンドウで、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [デバイスプロファイル（Devicec Profile）]** を選択します。

Step 2 [デバイスプロファイルの設定（Device Profile Configuration）] ウィンドウで、[デバイスプロファイル タイプ（Device Profile Type）] ドロップダウンリストから、該当する Cisco Unified IP Phone を選択します。

Step 3 [次へ（Next）] をクリックします。

Step 4 [デバイスプロトコル（Device Protocol）] ドロップダウンリストから、適切なプロトコルを選択します。

Step 5 [次へ（Next）] をクリックします。

Step 6 [電話ボタンテンプレート（Phone Button Template）] ドロップダウンリストから、テンプレートを選択します。

Step 7 （オプション）[ソフトキーテンプレート（Softkey Template）] ドロップダウンリストから、ソフトキー テンプレートを選択します。

Step 8 [デバイスプロファイルの設定（Device Profile Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 9 [保存（Save）] をクリックします。

（注） デバイスプロファイルを使用して Cisco Extension Mobility をセットアップする方法の詳細については、『*Cisco Unified Communications Manager* リリース *12.5(1)SU1* 機能設定ガイド』を参照してください。

エンタープライズ電話の設定

エンタープライズ電話設定の構成

ネットワーク内の電話機で使用可能なデフォルトの製品固有の設定フィールドを設定するには、次の手順を使用します。

このウィンドウで設定するパラメータは、各種デバイスの [共通の電話プロファイル（Common Phone Profile）] ウィンドウおよび [電話の設定（Phone Configuration）] ウィンドウにも表示されます。これらの他のウィンドウでも同じパラメータを設定した場合、それらの設定の優先順位は、1）[電話の設定（Phone Configuration）] ウィンドウでの設定、2）[共通の電話プロファイル（Common Phone Profile）] ウィンドウでの設定、3）[エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウでの設定の順になります。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configuration）]** を選択します。

Step 2 [製品固有の設定レイアウト（Product Specific Configuration Layout）] セクションの必須フィールドに入力します。

すべてのエンタープライズ電話パラメータについて説明を表示するには、[エンタープライズ電話パラメータの設定（Enterprise Phone Parameters Configuration）] ウィンドウで [?] ボタンをクリックします。

Step 3 [エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

電話の設定

Unified Communications Manager データベースに電話を手動で追加するには、この手順を実行します。自動登録を使用している場合は、次の手順を実行する必要はありません。自動登録を選択すると、Unified Communications Manager が自動的に電話を追加し、ディレクトリ番号を割り当てます。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [電話（Phone）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [電話タイプ（Phone Type）] ドロップダウンリストから、該当する Cisco IP Phone モデルを選択します。

Step 4 [次へ（Next）] をクリックします。

Step 5 [デバイス プロトコルの選択（Select the device protocol）] ドロップダウンリストから、次のいずれかを選択します。

- **SCCP**
- **SIP**

Step 6 [次へ（Next）] をクリックします。

Step 7 [電話の設定（Phone Configuration）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

（注） セキュリティプロファイルで設定されている CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウに表示される Certificate Authority Proxy Function の設定に関係するものです。製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）に関連する証明書操作の CAPF 設定を設定する必要があります。電話の設定ウィンドウで更新する CAPF 設定がセキュリティプロファイルの CAPF 設定に与える影響の詳細については、『Cisco Unified Communications Manager セキュリティガイド』を参照してください。

Step 8 [保存（Save）] をクリックします。

Step 9 [関連付け（Association）] エリアで、[回線 [1] - 新規 DN を追加（Line [1] - Add a new DN）] をクリックします。

Step 10 [ディレクトリ番号（Directory Number）] フィールドに、電話に関連付ける電話番号を入力します。

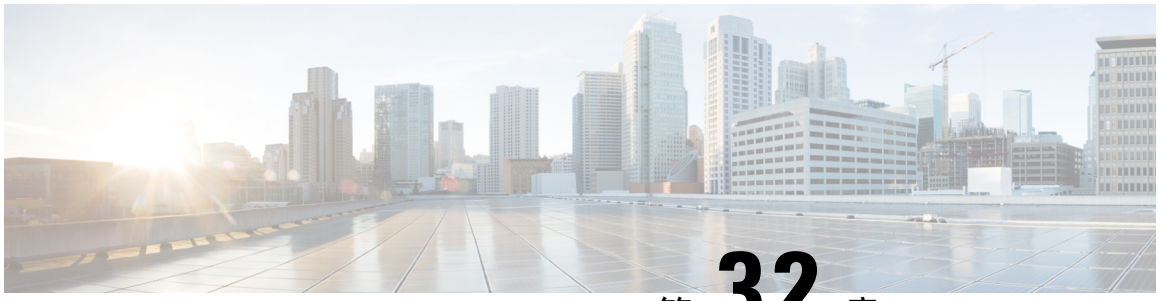
Step 11 [保存（Save）] をクリックします。

セルフケアポータル

セルフケアポータルは、展開プロセスの一部として、新しい電話機のプロビジョニングと設定を行うために使用できます。

- エンドユーザは、ポータルを使用して電話機の機能と設定をカスタマイズできます。
- アクティベーションコードによるデバイスのオンボーディングでは、ポータルを使用して電話機をアクティブ化するオプションがユーザに提供されます。
- ユーザは、ポータルを使用して、自分用のシングルナンバーリーチのリモート接続先をセルフプロビジョニングすることもできます。

ポータルを使用する前に、エンドユーザにアクセス権を設定する必要があります。ポータルのセットアップ方法の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「セルフケアポータル」の章を参照してください。



第 32 章

CAPF の設定

認証局プロキシ機能（CAPF）の概要

Cisco 認証局プロキシ機能（CAPF）は、ローカルで有効な証明書（LSC）を発行し、Cisco エンドポイントを認証する Cisco 専有サービスです。CAPF サービスは、Unified Communications Manager 上で実行され、次のタスクを実行します。

- サポートされる Cisco Unified IP 電話 に対して LSC を発行する。
- 混合モードが有効になっている場合に電話機を認証する。
- 電話機用の既存の LSC をアップグレードする。
- 表示とトラブルシューティングのために電話機証明書を取得する。

CAPF の実行モード

CAPF は、次のモードで動作するように設定することができます。

- Cisco Authority プロキシ機能：Unified Communications Manager の CAPF サービスが、CAPF サービス自体によって署名された LSC を発行します。これがデフォルトのモードです。
- オンライン CA：外部オンライン CA によって電話機用の LSC に署名する場合は、このオプションを使用します。CAPF サービスは自動的に外部 CA に接続します。CSR が送信されると CA が署名し、CA で署名された LSC が自動的に返されます。
- オフライン CA：オフラインの外部 CA によって電話機用の LSC に署名する場合は、このオプションを使用します。このオプションでは、LSC を手動でダウンロードし、CA に提出して、CA で署名された証明書の準備ができたら、それらをアップロードする必要があります。

（注） サードパーティ CA を使用して LSC に署名する必要がある場合、シスコでは、オフライン CA ではなくオンライン CA のオプションを使用することを推奨します。オンライン CA ではプロセスが自動化されるため、はるかに高速で、問題が発生する可能性も低くなります。

CAPF サービス証明書

統合コミュニケーションマネージャがインストールされている場合、CAPF サービスが自動的にインストールされ、CAPF 固有のシステム証明書が生成されます。セキュリティが適用されると、Cisco CTL クライアントは、すべてのクラスタノードに証明書をコピーします。

電話機の証明書タイプ

シスコは次の X.509v3 証明書タイプを電話で使用します。

- ローカルで有効な証明書（LSC）：このタイプの証明書は Cisco Certificate Authority Proxy Function（CAPF）に関連する必要な作業の実行後に、電話にインストールされます。デバイス セキュリティ モードを認証または暗号化に設定した後で、LSC は Unified Communications Manager と電話の間の接続を保護します。

（注） オンライン CA の場合、LSC の有効性は CA に基づいています。また、CA が許可している限り使用できます。

- 製造元でインストールされる証明書（MIC）：Cisco Manufacturing は MIC をサポートされている電話モデルに自動的にインストールします。製造元でインストールされる証明書は LSC インストールの Cisco Certificate Authority Proxy Function（CAPF）を認証します。製造元でインストールされる証明書を上書きしたり、削除することはできません。

（注） 製造元でインストールされる証明書（MIC）を LSC のインストールでのみ使用することが推奨されます。シスコでは Unified Communications Manager との TLS 接続の認証のために LSC をサポートしています。MIC ルート証明書は侵害される可能性があるため、TLS 認証またはその他の目的に MIC を使用するように電話を設定するお客様は、ご自身の責任で行ってください。MIC が侵害された場合シスコはその責任を負いません。

CAPF 経由の LSC 生成

CAPF を設定した後、電話機に設定されている認証文字列を追加します。キーと証明書の交換は、電話機と CAPF の間で行われ、以下が発生します。

- 電話機は、設定された認証方法を使用して CAPF に対して自身を認証します。
- 電話機は公開/秘密キー ペアを生成します。
- 電話機は、署名されたメッセージの中で、公開キーを CAPF に転送します。
- 秘密キーは電話に残り、外部に公開されることはありません。
- 証明書は CAPF によって署名され、署名付きメッセージによって電話に送り返されます。

（注） 電話のユーザが証明書操作の中断や、電話の動作ステータスの確認を実行できることに注意してください。

（注） キーの生成を低い優先順位で設定すると、アクションの発生中に、電話機が機能します。電話機は証明書生成中に機能しますが、TLS トラフィックが追加された場合、電話機でのコールプロセスの中断が最小限に抑えられる可能性があります。たとえば、インストールの最後に証明書がフラッシュに書き込まれると、音声信号が発生することがあります。

CAPF 前提条件

LSC 生成用の認証局のプロキシ機能を設定する前に、次の手順を実行します。

- サードパーティ CA を使用して LSCs に署名したい場合は、CA を外部に設定します。
- 電話機を認証する方法を計画します。
- LSC を生成する前に、次の条件を満たしていることを確認してください。
  - Unified Communications Manager リリース 12.5 以降。
  - 証明書に CAPF を使用するエンドポイント（Cisco IP 電話 および Jabber を含む）。
  - Microsoft Windows Server 2012 および 2016。
  - ドメインネームサービス（DNS）が構成されている。
- これは、リリース 14 SU2 以降に適用されます。

（注） CAPF 証明書には、次のデフォルトの X509 拡張を含める必要があります。

X509v3 基本制約：

CA:TRUE, pathlen:0

X509v3 キーの用途：

デジタル署名、証明書署名

CAPF 証明書にこれらの拡張機能がない場合、TLS 接続が失敗します。

- LSC を生成する前に、CA ルート証明書と HTTPS 証明書をアップロードする必要があります。セキュア SIP 接続では、HTTPS 証明書は CAPF 信頼を通過し、CA ルート証明書は CAPF 信頼と CallManager 信頼を通過します。インターネット インフォメーション サービス（IIS）は、HTTPS 証明書をホストします。CA ルート証明書は、証明書署名要求 (CSR) への署名に使用されます。

  証明書をアップロードする必要がある場合のシナリオを次に示します。

表 *27*：証明書のアップロードシナリオ

シナリオ	結果
CA ルート証明書と HTTPS 証明書が同じ。	CA ルート証明書をアップロードする。
CA ルート証明書と HTTPS 証明書が異なり、HTTPS 証明書は同じ CA ルート証明書によって発行される。	CA ルート証明書をアップロードする。
中間 CA 証明書と HTTPS 証明書が異なり、CA ルート証明書によって発行される。	CA ルート証明書をアップロードする。
CA ルート証明書と HTTPS 証明書が異なり、同じ CA ルート証明書によって発行される。	CA ルート証明書と HTTPS 証明書をアップロードする。

（注） 複数の証明書を同時に生成するとコール処理中断の原因となるため、スケジュールされたメンテナンスの時間帯に CAPF を使用することを強く推奨します。

認証局プロキシ機能の設定タスクフロー

次のタスクを実行して、証明機関プロキシ機能 (CAPF) サービスがエンドポイント用 LSCs を発行するように設定します。

（注） 新しい CAPF 証明書を再生成またはアップロードした後に、CAPF サービスを再起動する必要はありません。

手順

	コマンドまたはアクション	目的
Step 1	サードパーティの認証局のルート証明書のアップロード	LSC にサードパーティの CA 署名を適用する場合は、CA ルート証明書チェーンを CAPF 信頼ストアにアップロードします。その他の場合は、このタスクをスキップします。
Step 2	認証局（CA）ルート証明書のアップロード （396 ページ）	CA ルート証明書を Unified Communications Manager 信頼ストアにアップロードします。
Step 3	オンライン認証局の設定 （397 ページ）	電話機の LSC 証明書を生成するには、次の手順を使用します。
Step 4	オフライン認証局の設定の設定	オフライン CA を使用して電話機 LSC 証明書を生成するには、次の手順を使用します。
Step 5	CAPF サービスのアクティブ化または再起動	CAPF システム設定を構成した後、必須の CAPF サービスをアクティブにします。
Step 6	次のいずれかの手順を使用 して、Unified Communications Manager で CAPF 設定を構成します。 • ユニバーサル デバイス テンプレートでの CAPD 設定の構成（401 ページ） • 一括管理による CAPF 設定の更新（402 ページ） • 電話機の CAPF 設定の構成（403 ページ）	次のオプションのいずれかを使用して、CAPF 設定を電話機の設定に追加します。 • まだ LDAP ディレクトリを同期していない場合、CAPF 設定をユニバーサルデバイステンプレートに追加し、初期 LDAP 同期を使用して設定を適用します。 • 一括管理ツールを使用すると、1 回の操作で多数の電話機に CAPF 設定を適用できます。

	コマンドまたはアクション	目的
		• CAPF 設定を電話機ごとに適用することができます。
Step 7	キープアライブ タイマーの設定（404 ページ）	（オプション）ファイアウォールがタイムアウトしないように、CAPF エンドポイント接続のキープアライブ値を設定します。デフォルト値は 15 分です。

サードパーティの認証局のルート証明書のアップロード

CA ルート証明書を CAPF 信頼ストアと Unified Communications Manager 信頼ストアにアップロードし、外部 CA を使用して LSC 証明書に署名します。

（注） LSC の署名にサードパーティ CA を使用しない場合は、このタスクをスキップします。

手順

Step 1 [Cisco Unified OS Administration] から **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

Step 2 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

Step 3 **[証明書の目的（Certificate Purpose）]** ドロップダウンリストで、**[CAPF 信頼（CAPF-trust）]** を選択します。

Step 4 証明書の説明を [説明（Description）] に入力します。たとえば、**外部 LSC 署名 CA の証明書**のように指定します。

Step 5 [参照（Browse）] をクリックしてファイルに移動してから、[開く（Open）] をクリックします。

Step 6 [アップロード（Upload）] をクリックします。

Step 7 このタスクを繰り返し、[証明書の用途（Certificate Purpose）] を [CallManager 信頼（callmanager-trust）] として証明書をアップロードします。

認証局（CA）ルート証明書のアップロード

（注） 中間またはルート CA 証明書の共通名に「CAPF-」サブストリングが含まれていないことを確認します。「CAPF-」共通名は、CAPF 証明書用に予約されています。

手順

Step 1 Cisco Unified OS の管理から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

Step 2 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

Step 3 **[証明書目的（Certificate Purpose）]** ドロップダウンリストで、**[CallManager 信頼（CallManager-trust）]** を選択します。

Step 4 証明書の説明を [説明（Description）] に入力します。たとえば、**外部 LSC 署名 CA の証明書**のように指定します。

Step 5 [参照（Browse）] をクリックしてファイルに移動してから、[開く（Open）] をクリックします。

Step 6 [アップロード（Upload）] をクリックします。

重要 これは、リリース 14 SU2 以降に適用されます。

（注） ルートまたは中間 CA 証明書には、次のデフォルトの X509 拡張を含める必要があります。

X509v3 基本制約：

CA:TRUE, pathlen:0

X509v3 キーの用途：

デジタル署名、証明書署名

証明書にこれらの拡張機能がない場合、TLS 接続が失敗します。

重要 この注記は、リリース 14 SU3 以降の IPSec 証明書にのみ適用されます。

（注） CA 署名付き IPSec 証明書には、次の拡張子を含めないでください。

X509v3 基本制約：

CA:TRUE

オンライン認証局の設定

オンライン CAPF を使用 して電話機 LSC を生成するには、Unified Communications Manager でこの手順を使用します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 **[サーバ（Server）]** ドロップダウンリストから、[Cisco Certificate Authority Proxy Function（アクティブ）（Cisco Certificate Authority Proxy Function (Active)）] サービスをアクティブにしたノードを選択します。

Step 3 **[サービス（Service）]** ドロップダウンリストで、**[Cisco証明書認証プロキシ機能（アクティブ）（Cisco Certificate Authority Proxy Function (Active)）]** を選択します。サービス名の横に「Active」と表示されることを確認します。

Step 4 [エンドポイントへの証明書発行者（Certificate Issuer to Endpoint）] ドロップダウンリストから、[オンラインCA（Online CA）] を選択します。CA 署名付き証明書の場合、オンライン CA を使用することを推奨します。

Step 5 [証明書の有効期間（日数）（Duration Of Certificate Validity (in Days)）] フィールドに、CAPF が発行した証明書が有効である日数を表す数値を、1 ～ 1825 の間で指定します。

Step 6 [オンラインCAパラメータ（Online CA Parameters）] セクションで、次のパラメータを設定して、オンライン CA セクションへの接続を作成します。

- [オンラインCAホスト名（Online CA Hostname）]：サブジェクト名または共通名（CN）は、HTTPS 証明書の完全修飾ドメイン名（FQDN）と同じである必要があります。

  （注） 設定されたホスト名は、Microsoft CA で実行されているインターネット インフォメーション サービス（IIS）によってホストされる HTTPS 証明書の共通名（CN）と同じです。

- [オンラインCAポート（Online CA Port）]：オンライン CA のポート番号を入力します。たとえば、443 のように指定します。
- [オンラインCAテンプレート（Online CA Template）]：テンプレートの名前を入力します。Microsoft CA がテンプレートを作成します。

  （注） このフィールドは、[オンライン CA タイプ（Online CA Type）] が [Microsoft CA] のときのみ有効です。

- [オンライン CA タイプ（Online CA Type）]：エンドポイント証明書の自動登録には、Microsoft CA または EST でサポートされる CA を選択します。
  - [Microsoft CA]：CA が Microsoft CA である場合、このオプションを使用して、デジタル証明書をデバイスに割り当てます。

    （注） FIPSS 対応モードは、Microsoft CA ではサポートされていません。

  - **重要** リリース 14SU2 以降でサポートされます。

    [EST サポート CA（EST Supported CA）]：CA が自動登録用の組み込み EST サーバーモードをサポートしている場合は、このオプションを使用します。

- [オンラインCAユーザ名（Online CA Username）]：CA サーバのユーザ名を入力します。
- [オンラインCAパスワード（Online CA Password）]：CA サーバのユーザ名のパスワードを入力します。

- [証明書登録プロファイルラベル（Certificate Enrollment Profile Label）]：EST がサポートする CA のデジタル ID を有効な文字で入力します。

  （注） このフィールドは、[オンライン CA タイプ（Online CA Type）] が [EST サポート CA（EST Supported CA）] の場合にのみ有効です。

Step 7 残りの CAPF サービスパラメータを完了します。サービスパラメータのヘルプシステムを表示するには、パラメータ名をクリックします。

Step 8 [保存（Save）] をクリックします。

Step 9 変更内容を有効にするには、**Cisco Certificate Authority Proxy Function** を再起動します。Cisco Certificate Enrollment サービスが自動的に再起動します。

現在のオンライン CA の制限

- CA サーバが英語以外の言語を使用している場合、オンライン CA 機能は動作しません。CA サーバは英語でのみ応答します。
- オンライン CA 機能は、CA での mTLS 認証をサポートしていません。
- LSC 操作にオンライン CA を使用している場合、LSC 証明書に「デジタル署名」と「キー暗号化」のキー使用法が指定されていないと、デバイスのセキュア登録は失敗します。
- LSC 操作にオンライン CA を使用している場合、LSC 証明書に「デジタル署名」と「キー暗号化」が指定されていないと、デバイスのセキュア登録は失敗します。

オフライン認証局の設定の設定

オフライン CA を使用して電話機 LSC 証明書を生成することを決定した場合は、次の高度なプロセスに従うことができます。

（注） オフライン CA オプションを使用すると、オンライン CA よりも時間がかかり、手動による手順が非常に多くなります。証明書の生成および送信プロセス中に問題（たとえば、ネットワークの停止や電話機のリセットなど）が発生した場合は、プロセスを再起動する必要があります。

手順

Step 1 サードパーティ認証局からルート証明書チェーンをダウンロードします。

Step 2 ルート証明書チェーンを Unified Communications Manager 内の必要な信頼（CallManager 信頼 CAPF 信頼）にアップロードします。

Step 3 [エンドポイントへの証明書の発行（Certificate Issue to Endpoint）] サービスパラメータを [オフライン CA（Offline CA）] に設定して、オフライン CA を使用するように Unified Communications Manager を設定します。

Step 4 お使いの電話機の LSC 用に **CSR** を生成します。

Step 5 認証局に**CSR** を送信します。

Step 6 **CSR** から署名付き証明書を取得します。

オフライン CA を使用して電話機 LSC を生成する方法の詳細な例については、「CUCM サードパーティ CA 署名済み LSC の作成およびインポートの設定」を参照してください。

CAPF サービスのアクティブ化または再起動

CAPF システム設定を構成した後、必須の CAPF サービスをアクティブにします。CAPF サービスがすでにアクティブ化されている場合は、再起動します。

手順

Step 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスアクティベーション（Service Activation）]** を選択します。

Step 2 [サーバ（Server）] ドロップダウンリストからパブリッシャノードを選択し、[移動（Go）] をクリックします。

Step 3 [セキュリティサービス（Security Services）] ペインで、適用されるサービスを確認します。

- **Cisco Certificate Enrollment Service**：オンライン CA を使用している場合は、このサービスをオンにし、そうでない場合はオフのままにします。
- **Cisco Certificate Authority Proxy Function**：オフになっている（非アクティブ）場合は、このサービスをオンにします。このサービスがすでにアクティブ化されている場合は、再起動します。

Step 4 設定を編集した場合は、[保存（Save）] をクリックします。

Step 5 **Cisco Certificate Authority Proxy Function** サービスがすでにチェックされている場合は（アクティブ）、再起動します。

a) **[関連リンク（Related Links）]** ドロップダウンリストから **[コントロールセンター - 機能サービス（Control Center - Feature Services）]** を選択し、**[移動（Go）]** をクリックします。

b) [セキュリティ設定（Security Settings）] ペインで、[Cisco Certificate Authority Proxy Function] サービスをオンにして、[再起動（Restart）] をクリックします。

Step 6 次の手順のいずれかを実行して、個々の電話機に対して CAPF 設定を構成します。

a) ユニバーサル デバイス テンプレートでの CAPD 設定の構成 （401 ページ）

b) 一括管理による CAPF 設定の更新 （402 ページ）

c) 電話機の CAPF 設定の構成 （403 ページ）

ユニバーサル デバイス テンプレートでの CAPD 設定の構成

CAPF 設定をユニバーサルデバイステンプレートに設定するには、次の手順を実行します。テンプレートは、機能グループテンプレートの設定を使用して、LDAP ディレクトリ同期に適用することができます。テンプレートの CAPF 設定は、このテンプレートを使用する同期のすべてのデバイスに適用されます。

（注） ユニバーサルデバイステンプレートは、まだ同期されていない LDAP ディレクトリにしか追加することができません。初期 LDAP 同期が発生した場合は、一括管理を使用して電話機を更新します。詳細については、「一括管理による CAPF 設定の更新（402 ページ）」を参照してください。

手順

Step 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサルデバイステンプレート（Universal Device Template）]** を選択します。

Step 2 次のいずれかを実行します。

- [検索（Find）] をクリックして、既存のテンプレートを選択します。
- [新規追加（Add New）] をクリックします。

Step 3 [認証局プロキシ機能（CAPF）の設定（Certificate Authority Proxy Function (CAPF) Settings）] 領域を展開します。

Step 4 [証明書の操作（Certificate Operation）] ドロップダウンリストで、[インストール/アップグレード（Install/Upgrade）] を選択します。

Step 5 [認証モード（Authentication Mode）] ドロップダウンリスト メニューから、デバイスを認証するためのオプションを選択します。

Step 6 認証文字列の使用を選択した場合は、[認証文字列（Authentication String）] テキストボックスに文字列を入力するか、または [文字列を生成（Generate String）] をクリックして、システムによって文字列が生成されるようにします。

（注） この文字列がデバイス上で設定されていない場合、認証は失敗します。

Step 7 残りのフィールドで、キー情報を設定します。フィールドの詳細については、オンラインヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

（注） このテンプレートを使用するデバイスは、この手順で割り当てたのと同じ認証方式で設定されていることを確認してください。それ以外の場合、デバイス認証は失敗します。電話機の認証を設定する方法の詳細については、電話機のマニュアルを参照してください。

Step 9 次の手順に従って、このプロファイルを使用しているデバイスにテンプレートの設定を適用します。

a) ユニバーサル デバイス テンプレートを [機能グループテンプレートの設定（Feature Group Template Configuration）] に追加します。
b) 同期されていない LDAP ディレクトリ設定に機能グループテンプレートを追加します。
c) LDAP 同期を完了します。CAPF 設定は、同期されているすべてのデバイスに適用されます。

機能グループテンプレートと LDAP ディレクトリの設定の詳細については、『Cisco Unified Communications Manager システム設定ガイド』の「エンドユーザの設定」の項を参照してください。

一括管理による CAPF 設定の更新

Bulk Administrationの**電話機の更新**クエリを使用して、1 回の操作で多数の既存の電話機に CAPF 設定と LSC 証明書を設定します。

（注） まだ電話機をプロビジョニングしていない場合は、一括管理の [電話機の挿入（Insert phone）] メニューを使用して、CSV ファイルからの CAPF 設定で新しい電話機をプロビジョニングできます。CSV ファイルから電話機を挿入する方法の詳細については、『Cisco Unified Communications Manager 一括管理ガイド』の「電話機の挿入」セクションを参照してください。

電話機は、この手順で追加する文字列と認証方式と同じ文字列と認証方式で設定されていることを確認します。それ以外の場合、お使いの電話機は CAPF に対して認証しません。電話機で認証を設定する方法の詳細については、電話ドキュメンテーションを参照してください。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[一括管理（Bulk Administration）] > [電話機（Phones）] > [電話機の更新（Update Phones）] > [クエリ（Query）]**

Step 2 フィルタオプションを使用して、更新する電話機に検索を制限し、[検索（Find）] をクリックします。

たとえば、[電話機の検索場所（Find phones where）] ドロップダウンリストを使用して、特定の日付の前に LSC の有効期限が切れる電話機や、特定のデバイスプールにある電話機をすべて選択します。

Step 3 [次へ（Next）] をクリックします。

Step 4 [ログアウト/リセット/リスタート（Logout/Reset/Restart）] セクションで、[設定の適用（Apply Config）] ラジオボタンを選択します。ジョブを実行すると、CAPF アップデートは更新されたすべての電話に適用されます。

Step 5 [認証局プロキシ機能（CAPF）情報（Certification Authority Proxy Function (CAPF) Information）] で、[証明書の操作（Certificate Operation）] チェックボックスをオンにします。

Step 6 [証明書の操作（Certificate Operation）] ドロップダウンリストから、[インストール/アップグレード（Install/Upgrade）] を選択して、新しい LSC 証明書を電話機にインストールします。

Step 7 [認証モード（Authentication Mode）] ドロップダウンリストから、LSC のインストール時に電話機を認証する方法を選択します。

（注） 電話機で同じ認証方式を設定します。

Step 8 [認証モード（Authentication Mode）]として [認証文字列による（By Authentication String）] を選択した場合は、次の手順のいずれかを実行します。

- 各デバイスに対して一意の認証文字列を使用する場合は、[各デバイスに対して一意の認証文字列を生成する（Generate unique authentication string for each device）] をオンにします。
- すべてのデバイスに同じ認証文字列を使用する場合は、[認証文字列（Authentication String）] テキストボックスに文字列を入力するか、[文字列の生成（Generate String）] をクリックします。

Step 9 [電話の更新（Update Phones）] ウィンドウの [認証局プロキシ機能（CAPF）情報（Certification Authority Proxy Function (CAPF) Information）] セクションで、残りのフィールドを入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 10 [ジョブ情報（Job Information）] セクションで、[今すぐ実行（Run Immediately）]を選択します。

（注） スケジュールされた時刻にジョブを実行する場合は、[後で実行（Run Later）] を選択します。ジョブのスケジュール設定の詳細については、『Cisco Unified Communications Manager 一括管理ガイド』の「スケジュールされたジョブの管理」セクションを参照してください。

Step 11 [送信（Submit）] をクリックします。

（注） この手順で [設定の適用（Apply Config）] オプションを選択しなかった場合は、[電話機の設定（Phones Configuration）] ウィンドウですべての更新された電話機に設定を適用します。

電話機の CAPF 設定の構成

個々の電話機の LSC 証明書の CAPF 設定を設定するには、次の手順を実行します。

（注） LDAP 設定を多数の電話機に適用するには、一括管理または CAPF ディレクトリ同期を使用します。

この手順で追加するのと同じ文字列と認証方式で電話機を設定します。それ以外の場合、電話機は CAPF に対してそれ自体を認証しません。電話機で認証を設定する方法の詳細については、電話ドキュメンテーションを参照してください。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[デバイス（Device）] > [電話（Phone）]**

Step 2 既存の電話機を選択するには、[検索（Find）] をクリックします。[電話の設定（Phone Configuration）] ページが表示されます。

Step 3 [認証局プロキシ機能（CAPF）情報（Certification Authority Proxy Function (CAPF) Information）] ペインに移動します。

Step 4 [証明書の操作（Certificate Operation）] ドロップダウンリストから、[インストール/アップグレード（Install/Upgrade）] を選択して、新しい LSC 証明書を電話機にインストールします。

Step 5 [認証モード（Authentication Mode）] ドロップダウンリストから、LSC のインストール時に電話機を認証する方法を選択します。

（注） 電話機は、同じ認証方式を使用するように設定する必要があります。

Step 6 [認証文字列による（By Authentication String）] を選択した場合は、テキスト文字列を入力するか、[文字列の生成（Generate String）] をクリックして文字列を生成します。

Step 7 [電話の設定（Phone Configuration）] ページの [認証局プロキシ機能（CAPF）情報（Certification Authority Proxy Function (CAPF) Information）] ペインで、残りのフィールドに詳細を入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

キープアライブ タイマーの設定

ファイアウォールによって接続がタイムアウトしないように、次の手順を実行して、CAPF-エンドポイント接続のクラスターワイド キープアライブ タイマーを設定します。デフォルト値は 15 分です。各間隔の後、CAPF サービスは電話機にキープアライブ信号を送信して、接続を開いた状態にします。

手順

Step 1 コマンド ライン インターフェイスを使用して、パブリッシャノードにログインします。

Step 2 `utils capt set keep_alive` CLI コマンドを実行します。

Step 3 5 ～ 60（分）の間の数値を入力し、**Enter** キーを押します。

CAPF の管理タスク

CAPF を設定し、LSC 証明書を発行した後、次のタスクを使用して LSC 証明書を継続的に管理します。

証明書ステータスのモニタリング

証明書のステータスを自動的に監視するようにシステムを設定することができます。証明書が期限切れに近づいたときにシステムから電子メールが送信され、期限切れ後に証明書が失効します。

証明書の監視の確認の設定方法の詳細については、「証明書の管理」の章の「証明書の監視と失効のタスクフロー」を参照してください。

古い LSC レポートの実行

次の手順を使用して、古い LSC レポートを Cisco ユニファイドレポートから実行します。古い LSC とは、エンドポイント CSR への応答として生成された証明書ですが、その LSC がインストールされる前にエンドポイントによって新しい CSR が生成されたため、インストールされなかったものです。

（注） パブリッシャーノードで `utils capf stale-lsc list` CLI コマンドを実行して、古い LSC 証明書のリストを取得することもできます。

手順

Step 1 Cisco Unified Reporting から、[システムレポート（System Reports）] を選択します。

Step 2 左側のナビゲーションバーで、[古いLSC（Stale LSCs）] を選択します。

Step 3 [新規レポートの作成（Generate a new Report）] をクリックします。

保留中の CSR リストの表示

保留中の CAPF CSR ファイルのリストを表示するには、この手順を使用します。すべての CSR ファイルはタイムスタンプされます。

手順

Step 1 コマンド ライン インターフェイスを使用して、パブリッシャノードにログインします。

Step 2 `utils core active list` CLI コマンドを実行します。

保留中の CSR ファイルのタイムスタンプリストが表示されます。

古い LSC 証明書の削除

古い LSC 証明書をシステムから削除するには、次の手順を使用します。

手順

Step 1 コマンド ライン インターフェイスを使用して、パブリッシャノードにログインします。

Step 2 `utils capf stale-lsc delete all` CLI コマンドを実行します。
古い LSC 証明書はすべてシステムから削除されます。

CAPF システムの連携動作と制限事項

機能	連携動作
認証文字列	電話の CAPF 認証方式については、アップグレードまたはインストールの後に同じ認証文字列を電話に入力する必要があります。入力されなかった場合、操作が失敗します。[TFTP Encrypted Config] エンタープライズパラメータが有効な状態で認証文字列の入力に失敗した場合、電話の設定は失敗し、該当する認証文字列が電話に入力されるまで回復しません。
クラスタ サーバ クレデンシャル	CAPF が Unified Communications Manager クラスタのすべてのサーバを認証できるよう、クラスタ内のすべてのサーバで管理者のユーザ名とパスワードを同じものにする必要があります。
セキュアな電話機の移行	セキュアな電話が別のクラスタに移動されると、Unified Communications Manager はその電話が送信する LSC 証明書を信頼しなくなります。これは、その LSC 証明書が、CTL ファイル内に証明書が存在しない別の CAPF によって発行されたものであるためです。 セキュアな電話機を登録できるようにするには、既存の CTL ファイルを削除します。その後、[Install/Upgrade] オプションを使用して新しい CAPF を使用して新しい LSC 証明書をインストールし、電話機を新しい CTL ファイルにリセット (または MIC を使用) することができます。電話機を移動する前に既存の LSC を削除するには、[電話の設定 (Phone Configuration)] ウィンドウの [CAPF] セクションの [削除 (Delete)] オプションを使用します。

機能	連携動作
Cisco Unified IP 電話 6900 シリーズ、7900 シリーズ、および 8900 シリーズ、および 9900	将来的な互換性の問題を回避するため、Unified Communications Manager との TLS 接続に LSC を使用するために Cisco Unified IP 電話 6900 シリーズ、7900 シリーズ、8900 シリーズ、9900 シリーズをアップグレードし、MIC ルート証明書を CallManager 信頼ストアから削除することが推奨されます。Cisco Unified Communications Manager との TLS 接続に MIC を使用する一部の電話モデルは登録できない場合があることに注意してください。 管理者は、CallManager 信頼ストアから次の MIC ルート証明書を削除する必要があります。 • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048
停電	以下の情報は、通信障害や電源障害の発生時に適用されます。 • 電話機で証明書のインストールが行われている間に通信障害が発生した場合、電話機は30秒間隔で証明書の取得を3回試行します。これらの値は設定できません。 • 電話機が CAPF とのセッションを試行している間に電源障害が発生した場合、電話機はフラッシュに保存されている認証モードを使用します。つまり、電話機の再起動後に、電話機が TFTP サーバから新しい構成ファイルをロードできない場合です。証明書の操作が完了すると、システムはフラッシュの値をクリアします。
証明書の暗号化	Cisco Unified Communications Manager リリース 11.5(1)SU1 以降、CAPF サービスによって発行されるすべての LSC 証明書は、SHA-256 アルゴリズムで署名されています。したがって、IP 電話 7900/8900/9900 シリーズのモデルは、SHA-256 署名済み LSC 証明書および外部 SHA2 アイデンティティ証明書（Tomcat、CallManager、CAPF、TVS など）をサポートします。署名の検証が必要な、その他の暗号化の操作では、SHA-1 のみがサポートされます。 （注） ソフトウェア メンテナンスが終了またはサポートが終了した電話モデルを使用する場合は、Unified Communications Manager の 11.5(1)SU1 より前のリリースの使用を強くお勧めします。

7942 および 7962 電話機での CAPF の例

ユーザまたは Unified Communications Manager によって電話がリセットされたときの CAPF と Cisco Unified IP 電話 7962 および 7942 とのインタラクションについては、以下の情報を考慮してください。

（注） 以下の例では、電話機に LSC が存在せず、CAPF 認証モードとして [既存の証明書（By Existing Certificate）] が選択されている場合、CAPF 証明書操作が失敗します。

例：非セキュア デバイス セキュリティ モード

この例では、[Device Security Mode] を **[Nonsecure]** に設定し、[CAPF Authentication Mode] を **[By Null String]** または **[By Existing Certificate (Precedence...)]** に設定した後、電話がリセットされます。リセットした電話は直ちにプライマリ Unified Communications Manager に登録され、構成ファイルを受信します。その後、電話機は CAPF とのセッションを自動的に開始して LSC をダウンロードします。電話機が LSC をインストールした後、デバイスセキュリティモードを [認証済み (Authenticated)] または [暗号化 (Encrypted)] に設定します。

例：認証済み/暗号化済みデバイス セキュリティ モード

この例では、**[Device Security Mode]** を **[Authenticated]** または **[Encrypted]** に設定し、[CAPF Authentication Mode] を **[By Null String]** または **[By Existing Certificate (Precedence...)]** に設定した後、電話がリセットされます。CAPF セッションが終了し LSC がインストールされるまで、電話はプライマリ Unified Communications Manager に登録されません。セッションが終了すると、電話機が登録され、すぐに認証モードまたは暗号化モードで実行されます。

この例では、電話が自動的に CAPF サーバに接続されないため、**[By Authentication String]** を設定できません。電話に有効な LSC がない場合、登録は失敗します。

IPv6 アドレッシングとの CAPF のインタラクション

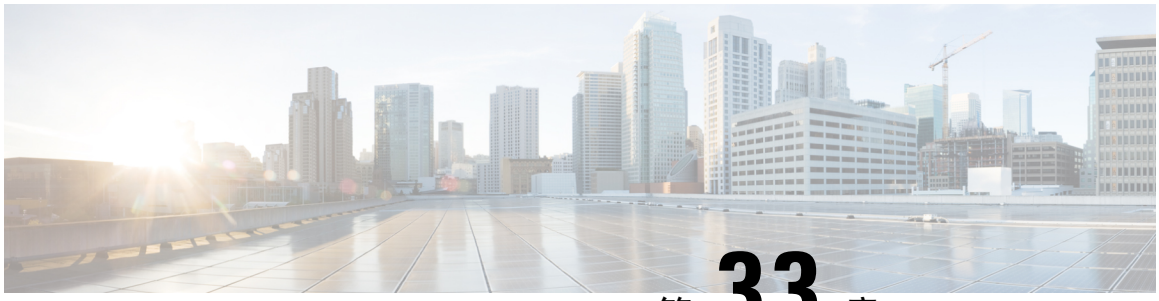
CAPF は、IPv4、IPv6、または両方のタイプのアドレスを使用する電話機に証明書を発行し、アップグレードすることができます。IPv6 アドレスを使用する SCCP を実行する電話の証明書の発行またはアップグレードを実行するには、[Unified Communications Manager Administration] で [Enable IPv6] サービスパラメータを **[True]** に設定する必要があります。

電話機が CAPF に接続して証明書を取得すると、CAPF は [IPv6 を有効にする (Enable IPv6)] エンタープライズパラメータの設定を使用して、電話機に証明書を発行するか、またはアップグレードするかを決定します。エンタープライズパラメータが**False**に設定されている場合、Capf は IPv6 アドレスを使用する電話機からの接続を無視または拒否し、電話機は証明書を受信しません。

次の表では、IPv4、IPv6、または両方のタイプのアドレスを持つ電話機が CAPF に接続する方法について説明します。

表 *28 : IPv6* または *IPv4* 電話機の *CAPF* への接続方法

電話機の IP モード	電話機の IP アドレス	CAPF IP アドレス	電話機から CAPF への接続方法
2 スタック	IPv4 と IPv6 が利用可能	IPv4、IPv6	電話機は、IPv6 アドレスを使用して CAPF に接続します。電話機が IPv6 アドレスを介して接続できない場合は、IPv4 アドレスを使用して接続を試みます。
2 スタック	IPv4	IPv4、IPv6	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv6	IPv4、IPv6	電話機は、IPv6 アドレスを使用して CAPF に接続します。試行に失敗した場合、電話機は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4 と IPv6 が利用可能	IPv6	電話機は、および IPv6 アドレスを使用して CAPF に接続します。
2 スタック	IPv4 と IPv6 が利用可能	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4	IPv6	電話機が CAPF に接続できません。
2 スタック	IPv6	IPv4	電話機が CAPF に接続できません。
2 スタック	IPv6	IPv6	電話機は IPv6 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv4、IPv6	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv6 スタック	IPv6	IPv4、IPv6	電話機は、IPv6 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv6	電話機が CAPF に接続できません。
IPv6 スタック	IPv6	IPv6	電話機は IPv6 アドレスを使用して CAPF に接続します。
IPv6 スタック	IPv6	IPv4	電話機が CAPF に接続できません。



第 33 章

TFTP サーバの設定

プロキシ TFTP 展開の概要

プロキシ簡易ファイル転送プロトコル(TFTP)サーバを使用して、ネットワークのエンドポイントに必要な構成ファイル (ダイヤルプラン、着信音ファイル、デバイス構成ファイルなど) を指定します。展開内の任意のクラスタに TFTP サーバをインストールして、複数クラスタのエンドポイントからの要求を処理することができます。DHCP スコープは、構成ファイルを取得するために使用するプロキシ TFTP サーバの IP アドレスを指定します。

冗長およびピアプロキシ TFTP サーバ

単一クラスタの導入では、クラスタは少なくとも 1 つのプロキシ TFTP サーバを備えている必要があります。冗長性を確保するために、クラスタに別のプロキシ TFTP サーバを追加することができます。2 台目のプロキシ TFTP サーバは、IPv4 のオプション 150 に追加されます。IPv6 の場合、第 2 TFTP サーバを、DHCP スコープの TFTP サーバ アドレスサブオプションタイプ 1 に追加します。

複数のクラスタ展開では、最大 3 台のリモートプロキシ TFTP サーバをプライマリプロキシ TFTP サーバのピアクラスタとして指定できます。これは、複数の DHCP スコープに対して 1 台のプロキシ TFTP サーバだけを設定する場合、または 1 つの DHCP スコープのみを設定する場合に便利です。プライマリプロキシ TFTP サーバは、ネットワーク内のすべての電話機とデバイスに構成ファイルを提供します。

各リモートプロキシTFTPサーバとプライマリプロキシTFTPサーバの間にピア関係を作成する必要があります。

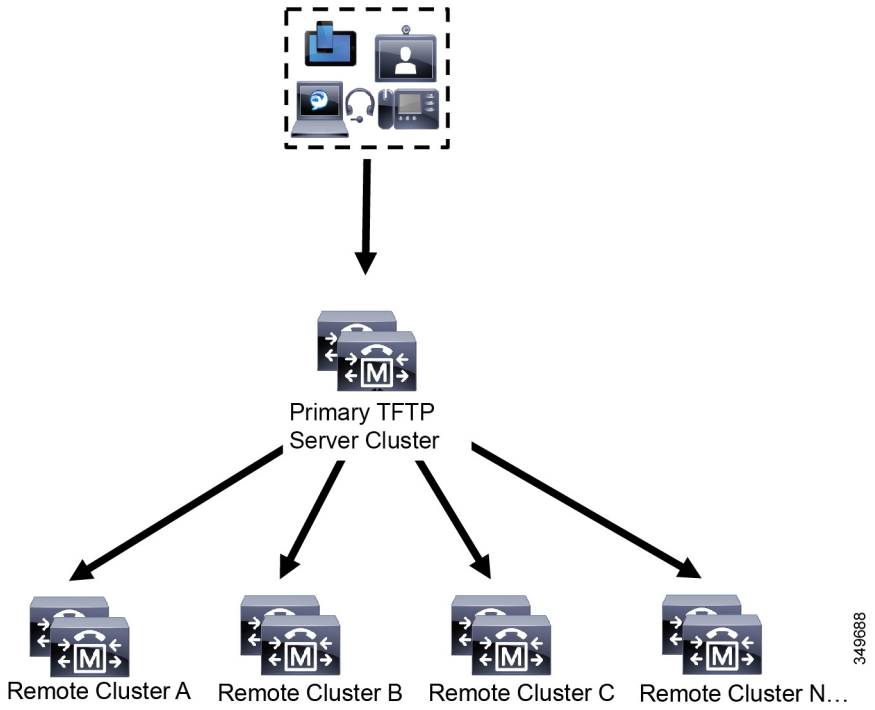
ヒント　ネットワーク内のリモートプロキシ TFTP サーバ間にピア関係を設定する場合は、関係を階層構造にしておきます。ループの発生を回避するために、リモートクラスタ上のピアプロキシ TFTP サーバが相互にポイントしないようにします。たとえば、プライマリノード A にノード B と C のピアリレーションシップがあるとします。ノード B と C の間にピア関係を作成しないでください。作成すると、ループが作成されます。

プロキシ TFTP

マルチクラスタ システムでは、プロキシ TFTP サービスは、1 つのプライマリ TFTP サーバを介して複数のクラスタから TFTP ファイルを提供できます。単一のサブネットまたは VLAN に複数のクラスタからの電話機が含まれている場合や、複数のクラスタが同じ DHCP TFTP オプション（150）を共有している場合、プロキシ TFTP はそれらの状況に対する単一の TFTP 参照として機能できます。

プロキシ TFTP サービスは、図に示すように、単一レベルの階層として機能します。より複雑な複数レベル階層はサポートされません。

図 *7:* プロキシ *TFTP* のシングル レベル階層



上の図では、デバイスのグループが構成ファイルのプライマリ TFTP サーバと通信します。デバイスから TFTP の要求を受信すると、プライマリ TFTP は、構成ファイルだけでなく、リモートクラスタ A、B、C、N (構成されている他のリモートクラスタ) などリモートで構成された他のクラスタについて、それぞれ自身のローカルキャッシュを検索します。

プライマリ TFTP サーバ上では、任意の数のリモートクラスタを設定できます。ただし、各リモートクラスタには最大 3 個の TFTP IP アドレスしか含めることができません。冗長性を確保するための推奨設計は、クラスタごとに 2 台の TFTP サーバを使用することです。したがって、プライマリ TFTP サーバ上のリモートクラスタあたり 2 つの IP アドレスを使用して冗長性を確保できます。

ユースケースとベストプラクティス

プロキシ TFTP の使用方法と実装に関するベストプラクティスとして、次のシナリオを検討してください。

1. クラスタは、他の用途に対応しない専用のプロキシTFTPクラスタとして動作できます。このようなクラスタは他のクラスタと関係を持たず、コールの処理も行いません。このシナリオでは、リモートクラスタ TFTP を手動で定義し、8.0 よりも前にロールバックすることを推奨します。

（注） このシナリオでは自動登録は機能しません。

2. クラスタはリモートクラスタであり、リモートクラスタに対するプロキシTFTPサーバとしても動作します。リモートクラスタは手動で定義されます。自動登録は有効にしないでください。

IPv4 および IPv6 デバイスに対する TFTP サポート

IPv4 の電話機とゲートウェイで DHCP カスタムオプション 150 を使用して、TFTP サーバの IP アドレスを検出することを推奨します。オプション 150 を使用すると、ゲートウェイと電話機は TFTP サーバの IP アドレスを検出します。詳細については、デバイスに同梱されているマニュアルを参照してください。

IPv6 ネットワークでは、Cisco ベンダー固有の DHCPv6 情報を使用して、TFTP サーバ IPv6 アドレスをエンドポイントに渡すことを推奨します。この方法では、TFTP サーバの IP アドレスをオプション値として設定します。

IPv4 を使用するエンドポイントと IPv6 を使用するエンドポイントがある場合は、IPv4 には DHCP カスタム オプション 150 を、IPv6 には Cisco ベンダー固有情報オプションである TFTP サーバアドレスのサブオプションタイプ 1 を使用することをお勧めします。TFTP サーバが IPv4 を使用して要求を処理しているときに、エンドポイントが IPv6 アドレスを取得して要求を TFTP サーバに送信した場合、TFTP サーバは IPv6 スタックで要求を受信していないため、その要求を受信しません。この場合、エンドポイントを Cisco Unified Communications Manager に登録できません。

IPv4 および IPv6 デバイスが TFTP サーバの IP アドレスを検出するために使用できる別の方法があります。たとえば、IPv4 デバイスに DHCP オプション 066 または CiscoCM1 を使用できます。IPv6 デバイスの場合、他の方法として、TFTP サービスのサブオプションタイプ 2 を使用する方法と、エンドポイントで TFTP サーバの IP アドレスを設定する方法があります。これらの代替手

段は推奨されません。代替手段を使用する前に、シスコのサービス プロバイダーに問い合わせてください。

TFTP 展開のエンドポイントおよび構成ファイル

SCCP 電話機、SIP 電話およびゲートウェイは、初期化時に構成ファイルを要求します。デバイス設定を変更すると、更新された構成ファイルがエンドポイントに送信されます。

構成ファイルには、Unified Communications Managerノードの優先順位リスト、これらのノードに接続するために使用される TCP ポート、さらに他の実行可能ファイルが含まれます。一部のエンドポイント用の構成ファイルには、電話機のボタン（メッセージ、ディレクトリ、サービス、および情報）用のロケール情報およびURLが保存されています。ゲートウェイ用の構成ファイルには、デバイスが必要とする設定情報がすべて保存されています。

プロキシ TFTP のセキュリティに関する考慮事項

Cisco プロキシ TFTP サーバは、署名付きの要求と署名されていない要求の両方を処理し、非セキュアモードと混在モードのどちらでも動作します。プロキシ TFTP サーバは、電話機がファイルを要求したときにローカルファイルシステムまたはデータベースを検索し、見つからない場合は要求をリモートクラスタに送信します。電話機がサーバに共通ファイル（`ringlist.xml.sgn` のような名前のファイルやロケールファイルなど）を要求した場合、サーバは、電話機のホームクラスタにあるファイル自体の代わりに、そのファイルのローカルコピーを送信します。

プロキシ TFTP からファイルを受信したとき、このファイルにはプロキシサーバの署名が含まれていて電話機の初期信頼リスト（ITL）と一致しないため、署名の検証に失敗し、ファイルは電話機に拒否されます。この問題を解決するには、電話機のデフォルトのセキュリティ（SBD）を無効にするか、またはプロキシ TFTP の CallManager 証明書を新しい（リモート/ホーム）クラスタの phone-sast-trust にインポートします。その後、電話機から信頼検証サービス（TVS）に接続し、プロキシ TFTP 証明書を信頼できます。展開環境で EMCC が有効になっている場合は、一括証明書交換が必要です。

デフォルトのセキュリティを無効にするには、『Cisco Unified Communications Manager セキュリティ ガイド』の「Cisco Unified IP Phone の ITL ファイルの更新」セクションを参照してください。

混在モードのプロキシ TFTP

混在モードで動作しているリモートクラスタ上の TFTP サーバでは、プライマリプロキシ TFTP サーバ証明書をCisco証明書信頼リスト（CTL）ファイルに追加する必要があります。追加しない場合、セキュリティが有効になっているクラスタに登録されたエンドポイントで必要なファイルをダウンロードできなくなります。これを行うには、証明書の一括インポート/エクスポートの実行後に CTL ファイルを更新します。

詳細については、IP Phoneをクラスタ間で移行して証明書の一括エクスポートを実行するときに、『Cisco Unified Communications Manager セキュリティ ガイド』の「証明書の一括エクスポート」セクションを参照してください。

プロキシ TFTP 環境におけるクラスタ間での電話機の移動

プロキシ TFTP 環境のリモートクラスタ間で電話機を移動する場合は、次の手順を実行します。

1. リモートクラスタ B（移動先クラスタ）に電話機の詳細を追加します。
2. リモートクラスタ A（移動元クラスタ）から電話機を削除します。

（注） プロキシ TFTP の電話機の設定が期限切れになるまでには 30 分かかります。ファイルが見つからないという応答が返されるのを避けるために、プロキシクラスタの TFTP サービスを再起動します。

3. 電話機をリセットして、リモートクラスタ B から構成ファイルをダウンロードし、リモートクラスタ B に登録します。

TFTP サーバの設定タスクフロー

クラスタに対して拡張モビリティクロスクラスタ (EMCC) が設定されている場合は、システムがプロキシ TFTP サーバを動的に設定できます。そうしない場合は、TFTP サーバを設定して、セキュリティモードを手動で設定することができます。

手順

	コマンドまたはアクション	目的
Step 1	次のいずれかの方法を使用して、TFTP サーバをセットアップします。 • TFTP サーバのダイナミック設定（416 ページ） • TFTP サーバの手動設定（417 ページ）	クラスタ間ルックアップサービス (ILS) が設定されている場合は、TFTP サーバを動的に設定することができます。 EMCC が設定されていない場合は、TFTP サーバを手動でセットアップします。クラスタがセキュアであるか、あるいは非セキュアであるかを示す必要があります。クラスタは、デフォルトでは非セキュアとして扱われます。
Step 2	（任意） TFTP サーバの CTL ファイルの更新 （418 ページ）	CTL クライアントプラグインをインストールし、混在モードで動作しているすべてのリモートクラスタ内のすべてのプロキシ TFTP サーバの Cisco Certificate Trust List (CTL) ファイルにプライマリプロキシ TFTP サーバを追加します。
Step 3	（任意） エンドポイント デバイスに対応するドキュメントを参照してください。	プロキシ TFTP 展開にリモートクラスタがある場合は、プロキシ TFTP サーバをすべ

	コマンドまたはアクション	目的
		てのリモートエンドポイントの信頼検証リスト (TVL) に追加する必要があります。
Step 4	（任意）TFTP サーバの非構成ファイルの変更 （419 ページ）	プロキシ TFTP サーバからエンドポイントを要求した非構成ファイルを変更できます。
Step 5	（任意）TFTP サービスの停止と開始（419 ページ）	エンドポイントの変更済みの設定されていないファイルをアップロードした場合は、プロキシ TFTP ノード上で TFTP サービスを停止して再起動します。
Step 6	（任意） DHCP サーバに対応するドキュメントを参照してください。	複数のクラスタに展開する場合は、プライマリプロキシ TFTP サーバの IP アドレスが含まれるように、個々のリモートノードの DHCP スコープを変更します。

TFTP サーバのダイナミック設定

ネットワークに設定されているクラスタルックアップサービス (ILS) を使用している場合は、Cisco proxy TFTP サーバを動的に設定することができます。

始める前に

ネットワークの EMCC を設定します。詳細については、『*Cisco Unified Communications Manager* 機能およびサービス ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

重要 リリース 14SU1 以降は、SIP OAuth が有効になっている場合は、オフクラスタの Tomcat 証明書のルート CA 証明書をプロキシ電話 Edge Trust にコピーする必要があります。

手順

Cisco Unified Communications Manager の管理ページで、**[拡張機能(Advanced Features)]** > **[クラスタビュー(Cluster View)]** > **[今すぐリモートクラスタを更新(Update Remote Cluster Now)]** を選択します。TFTP サーバはクラスタに対して自動的に設定されます。

次のタスク

エンドポイントの信頼検証リスト (TVL) にリモートプロキシ TFTP サーバを追加する必要があります。そうでない場合は、リモートクラスタ上のプロキシ TFTP サーバからの構成ファイルは受け入れられません。詳細については、お使いのエンドポイント デバイスに対応するマニュアルを参照してください。

TFTP サーバの手動設定

EMCC が設定されていない場合にネットワークで TFTP を設定するには、手動の手順を実行する必要があります。

[クラスタ ビュー（Cluster View）] で、プライマリ プロキシ TFTP サーバとその他の TFTP サーバ間のピア関係をセットアップします。最大 3 台のピア TFTP サーバを追加できます。

プロキシ TFTP 導入環境の各リモート TFTP サーバには、プライマリ プロキシ TFTP サーバとのピア関係が含まれる必要があります。ループの作成を回避するため、リモート クラスタのピア TFTP サーバが互いを指し示していないことを確認します。

始める前に

重要 リリース 14SU1 以降は、SIP OAuth が有効になっている場合は、オフクラスタの Tomcat 証明書のルート CA 証明書をプロキシ電話 Edge Trust にコピーする必要があります。

手順

Step 1 リモート クラスタを作成します。次のアクションを実行します。

a) Cisco Unified CM Administration で、**[高度な機能（Advanced Features）] > [クラスタの表示（Cluster View）]** を選択します。

b) [新規追加（Add New）] をクリックします。[リモート クラスタの設定（Remote Cluster Configuration）] ウィンドウが表示されます。

c) TFTP サーバの最大 50 文字のクラスタ ID と完全修飾ドメイン名（FQDN）を入力し、[保存（Save）] をクリックします。

クラスタ ID の有効な値には、英数字、ピリオド（.）、ハイフン（-）が含まれます。FQDN の有効な値には、英数字、ピリオド（.）、ハイフン（-）、アスタリスク（*）、およびスペースが含まれます。

d) （任意）[リモート クラスタ サービスの設定（Remote Cluster Service Configuration）] ウィンドウで、リモート クラスタの最大 128 文字の説明を入力します。

二重引用符（“）、山カッコ（>）、バックスラッシュ（\）、ハイフン（-）、アンパサンド（&）、またはパーセント記号（%）は使用しないでください。

Step 2 リモート クラスタの TFTP を有効にするには、[TFTP] チェック ボックスをオンにします。

Step 3 [TFTP] をクリックします。

Step 4 [リモート クラスタ サービスの手動上書き設定（Remote Cluster Service Manually Override Configuration）] ウィンドウで、[リモート サービス アドレスの手動設定（Manually configure remote service addresses）] を選択します。

Step 5 これらの TFTP サーバとピア関係を作成するには、TFTP サーバの IP アドレスを入力します。

TFTP サーバの IP アドレスは 3 つまで入力できます。

Step 6 （任意）プロキシ TFTP サーバがセキュアなクラスタに展開されている場合は、[クラスタは安全です（Cluster is Secure）] チェック ボックスをオンにします。

Step 7 [保存（Save）] をクリックします。

次のタスク

エンドポイントの Trust Verification List（TVL）に、すべてのリモート TFTP サーバを追加する必要があります。追加しないと、エンドポイントがリモート クラスタにあるプロキシ TFTP サーバからの構成ファイルの受け入れが拒否されます。詳細については、お使いのエンドポイント デバイスに対応するマニュアルを参照してください。

TFTP サーバの CTL ファイルの更新

混在モードの各クラスタで `utils ctl` を実行して、パブリッシャノードから CTL ファイルを更新します。プロキシ TFTP サーバとすべてのクラスタの間に完全なセキュリティネットワークが確立していて、プロキシとリモートクラスタ間で一括インポートおよびエクスポートによる証明書の交換が可能であることを確認します。

CTLClient を使用して、混在モードで動作しているリモートクラスタ内のすべての TFTP サーバの Cisco 証明書信頼リスト（CTL）ファイルに、プライマリ TFTP サーバまたはプライマリ TFTP サーバの IP アドレスを追加する必要があります。これは、セキュリティ対応クラスタ内のエンドポイントが構成ファイルを正常にダウンロードできるようにするために必要です。

セキュリティと Cisco CTL CLI の使用方法の詳細については、『Cisco Unified Communications Manager セキュリティ ガイド』の「Cisco CTL の設定について」セクションを参照してください。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[アプリケーション（Application）] > [プラグイン（Plugins）]**

Step 2 [検索（Find）] をクリックして、インストールできるすべてのプラグインの一覧を表示します。

Step 3 Cisco CTL クライアントの**ダウンロード**リンクをクリックします。
システムは TFTP サーバ上に保管される証明書にデジタル署名をするクライアントをインストールします。

Step 4 TFTP サーバをリブートします。

TFTP サーバの非構成ファイルの変更

ロードファイルや`RingList.xml`など、設定されていないファイルを、プロキシ TFTP サーバからのエンドポイント要求であるように変更できます。この手順を完了したら、変更したファイルをプロキシ TFTP サーバの TFTP ディレクトリにアップロードします。

手順

Step 1 Cisco Unified Communications Operating System Administration で、**[ソフトウェア アップグレード（Software Upgrades）] > [TFTP ファイル管理（TFTP File Management）]** を選択します。
[TFTPファイル管理（TFTP File Management）] ウィンドウが表示されます。

Step 2 [ファイルのアップロード（Upload File）] をクリックします。
[ファイルのアップロード（Upload File）] ポップアップが表示されます。

Step 3 次のいずれかの操作を実行します。

- **[参照]** をクリックして、アップロードするファイルのディレクトリの場所を参照します。
- 更新されたファイルの完全なディレクトリパスを**[ディレクトリ]**フィールドに貼り付けます。

Step 4 [ファイルのアップロード（Upload File）] をクリックするか、[閉じる（Close）] をクリックしてファイルをアップロードせずに終了します。

次のタスク

Cisco Unified Serviceability Administration を使用して、プロキシ TFTP ノード上の Cisco TFTP サービスを停止して再起動します。

TFTP サービスの停止と開始

次の手順に従って、プロキシ TFTP ノード上の TFTP サービスを停止して再開します。

サービスの有効化、無効化、および再起動についての詳細は、『*Cisco Unified Serviceability* アドミニストレーション ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

手順

Step 1 Cisco Unified Serviceability で、**[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。

Step 2 [コントロール センター-機能サービス（Control Center–Feature Services）] ウィンドウで、[サーバ（Server）] ドロップダウンリストからプロキシ TFTP ノードを選択します。

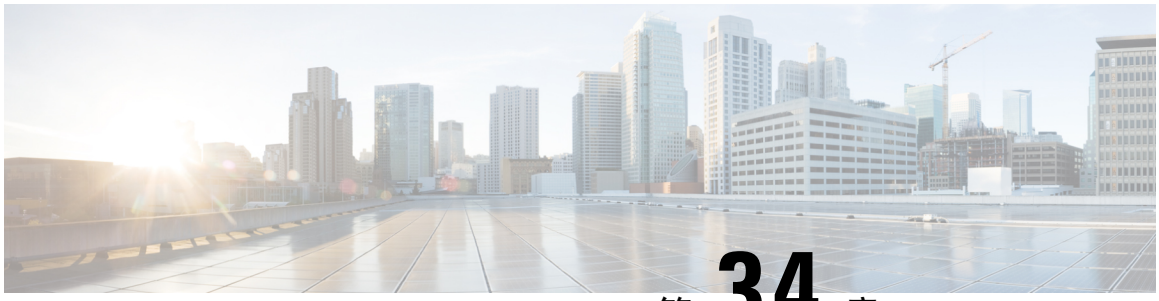
Step 3 [CMサービス（CM Services）] 領域で TFTP サービスを選択し、[停止（Stop）] をクリックします。

ステータスが変化し、更新されたステータスが反映されます。

ヒント サービスの最新のステータスを表示するには、[更新（Refresh）] をクリックします。

Step 4 [CM サービス（CM Services）] 領域で TFTP サービスを選択し、[開始（Start）] をクリックします。

ステータスが変化し、更新されたステータスが反映されます。



第 34 章

アクティベーション コードによるデバイスのオンボーディング

アクティベーション コードの概要

アクティベーションコードにより、新しくプロビジョニングされた電話機が簡単にプロビジョニングされます。アクティベーション コードは、1 回だけ使用できる 16 桁の値であり、電話機を登録する際にユーザが電話機に入力する必要がああります。アクティベーション コードは、電話機のプロビジョニングとオンボーディングを効率化する方法であり、管理者が手動で個々の電話機の MAC アドレスを収集して入力する必要がありません。これは自動登録の代替となるシンプルな方法法であり、この方法で多数の電話機のプロビジョニング、1 台の電話機のプロビジョニング、または既存の電話機の再登録も可能です。

モバイルおよびリモートアクセスに準拠したデバイスを使用して、アクティベーションコードによる登録をモバイルおよびリモートアクセス経由で簡単かつ安全に実行することもできます。

アクティベーションコードデバイスのオンボードは、次のモードで動作します。

- オンプレミス
- モバイル アンド リモート アクセス（MRA）

（注） TFTP プロキシのセットアップは、アクティベーションコードのオンボーディングと MRA を使用したエンドポイントの登録をサポートしていません。

アクティベーション コードには次の利点があります。

- アクティベーション コードを使用したオンボーディングによって、新しくプロビジョニングされた電話機または信頼されていない電話機すべてについて、それぞれの Manufacturing Installed Certificate（MIC）の評価と検証を Unified Communications Manager に実行させることができます。

（注） オンボードアクティビティを実行するには、シスコの製造ルート証明書が CallManager 信頼ストアに存在している必要があります。

- 実際の MAC アドレスを手動で入力する必要はありません。管理者はダミーの MAC アドレスを使用することができ、電話機は登録時に実際の MAC アドレスを使用して設定を自動的に更新します。
- 電話名を BAT から SEP に変換するために、タップなどの IVR を導入する必要はありません。

[アクティベーション可能状態になっている電話機を表示（Show Phone Ready To Activate）] エンタープライズパラメータが True に設定されている場合、電話機のユーザは、セルフケアポータルを使用してアクティベーションコードを取得できます。それ以外の場合は、管理者が電話機のユーザにコードを提供する必要があります。

（注） BAT MAC アドレスを使用してプロビジョニングすると、アクティベーションコードはその電話機モデルに関連付けられます。BAT MAC は、「BAT」で始まるデバイス名への参照であり、その後に、MAC アドレスのように見えるランダムな 12 桁の 16 進数が続きます。空白の MAC アドレスフィールドを使用してデバイス設定ページを保存すると、この形式のランダムな名前が作成されます。電話機をアクティブ化するには、電話機のモデルに一致するアクティベーションコードを入力する必要があります。

セキュリティを強化するために、電話機の実際の MAC アドレスを使用して電話機をプロビジョニングできます。このオプションでは、管理者がプロビジョニング時に個々の電話機の MAC アドレスを収集して入力する必要があるため、設定項目が多くなりますが、ユーザが電話機の実際の MAC アドレスと一致するアクティベーション コードを入力する必要があるため、セキュリティが向上します。

技術的な制限により、アクティベーションコードを介したデバイスのオンボーディングは、プロキシ TFTP 展開ではサポートされていません。

オンプレミス モードでのオンボーディングのプロセス フロー

次に、されている場合に、アクティベーションコードを使用して新しい電話機をオンボードするプロセスフローを示します。

1. 管理者は、ユーザがオンボードのアクティベーションコードを入力するように設定を設定します。
2. 管理者が電話機をプロビジョニングして設定します。BAT MAC アドレスが使用されている場合、管理者は実際の MAC アドレスを入力しません。
3. 電話機は、DHCP opt 150 を介して、または電話機の設定で設定されている代替 TFTP から TFTP の IP アドレスを取得します。電話機は XMLDefault ファイルをダウンロードし、アクティベーションコードが使用中であることを検出します。
4. ユーザが電話機のアクティベーションコードを入力します。
5. 電話機は、アクティベーションコードと製造元でインストールされた証明書を使用して Cisco Unified Communications Manager を認証します。
6. 電話のオンボーディングにアクティベーションコードを使用する場合、電話には TVS サービスが必要です。ITL ファイルは、Unified CM サーバーの TCP ポート 2445 で実行される TVS サービスの証明書を含む TVS 機能を提供します。
7. Cisco Unified Communications Manager は、実際の MAC アドレスを使用してデバイス設定を更新します。TFTP サーバは、電話機のデバイス設定を検知し、電話機を登録できるようにします。デバイス登録は最大で5分間可能であることに注意してください。

（注） オンプレミスでのアクティベーションコードによるオンボーディングのために、デフォルトの通信マネージャグループに追加のサブスクライバを含めておくことをお勧めします。追加のサブスクライバが存在しない場合、デフォルトの通信マネージャグループ内のノードが停止すると、オンボーディングの問題が発生する可能性があります。

モバイルおよびリモートアクセスモードでのオンボーディングプロセス フロー

以下は、モバイルおよびリモートアクセスモードを使用する場合に、アクティベーションコードによる新しい電話機のオンボーディングを実行するプロセスフローを示しています。

1. 管理者は、クラウド/ハイブリッド通信を設定して Cisco Cloud を使用したアクティベーションコードによるオンボーディングを有効化し、モバイルおよびリモートアクセス アクティベーション ドメインを指定します。
2. また、必要に応じて追加のモバイルおよびリモートアクセス サービス ドメインを設定します。

3. 管理者は、MAC アドレス（BAT、AXL、GUI）を指定せずに完全なデバイス設定を作成します。デバイス名は、ランダムな BAT MAC アドレスになります。
4. 管理者が、このデバイスのアクティベーション コードを要求します。デバイスアクティベーションサービスは、クラウドベースのデバイスアクティベーションサービスからコードを要求します。
5. ユーザはセルフケアポータルからコードを取得できます。または、管理者がそのコードをユーザに送信することもできます。
6. ユーザが電話機の電源を投入し、アクティベーションコードを入力します。
7. 電話機が、クラウドから Expressway のロケーションを学習し、モバイルおよびリモートアクセスまたは Cisco Unified Communications Manager に対して認証します。
8. デバイス アクティベーション サービスが、電話機の MAC アドレスでデータベース内のデバイス設定を更新します。

   これで電話機は、TFTP に登録して通常のモバイルおよびリモートアクセスなどの電話機固有の構成ファイルを取得し、Cisco Unified Communications Manager に登録できるようになりました。

（注） 在宅勤務のリモートユーザー向けに安全なソリューションを提供するには、TRP ではなく Expressway の モバイルおよびリモートアクセスが推奨ソリューションです。

アクティベーション コードの前提条件

リリース 12.5(1) では、次の Cisco IP Phone モデルでアクティベーション コードによるオンボーディングがサポートされます。7811、7821、7832、7841、7861、8811、8841、8845、8851、8851NR、8861、8865、および 8865NR。

リリース 12.5 SR3 は、オンプレミスと MRA の両方の Cisco IP Phone モデルでのオンボードをサポートしています。

さらに、リリース 12.5(1)SU1 では、次の Cisco IP 電話モデルがサポートされます。8832 および 8832NR

クラウドのオンボードプロセスでは、次のドメイン名が Cisco Unified Communications Manager によって解決される必要があります。

- fos-a.wbx2.com
- idbroker.webex.com
- push.webexconnect.com
- btpush.webexconnect.com

セルフケアポータル

ユーザにセルフケアポータルを使用して電話をオンボードさせる場合は、ユーザがアクセスできるようにポータルを事前にセットアップする必要があります。詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「セルフケアポータル」の章を参照してください。

オンプレミスモードでのアクティベーションコードを使用したデバイスのオンボーディングのタスクフロー

アクティベーションコードを使用して新しい電話をオンボードするには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
Step 1	デバイス アクティベーショ ンサービスの有効化 （426 ページ）	Cisco Unified Serviceability で**シスコ デバイス アクティベーション サービス**が実行されている必要があります。
Step 2	アクティベーション コードを使用する登録方法の設定 （426 ページ）	[デバイスのデフォルト設定（Device Defaults）] で、サポートされている電話機モデルについて、アクティベーションコードを使用するようにデフォルトの登録方法を設定します。
Step 3	アクティベーション コードを要件とする電話機をプロビジョニングします。プロビジョニングのオプションの例を2つ示します。 • アクティベーション コードを要件とする電話機の追加 （427 ページ） • 一括管理によるアクティベーション コードを使用した電話の追加 （428 ページ）	Cisco Unified Communications Manager には、左側のオプションを含むさまざまなプロビジョニング方法があります。どの方法を選択する場合も、その電話機の [電話の設定（Phone Configuration）] で [オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）] チェックボックスがオンになっていることを確認してください。
Step 4	電話機のアクティブ化 （431 ページ）	アクティベーション コードをユーザに配布します。電話機を使用するためには、ユーザがその電話機にコードを入力する必要があります。

デバイス アクティベーショ ンサービスの有効化

アクティベーション コードを使用するには、Cisco Unified Serviceability で**シスコ デバイス アクティベーション サービス**が実行されている必要があります。サービスが実行されていることを確認するには、この手順を使用します。

手順

Step 1 Cisco Unified Serviceability から、**[ツール（Tools）]>[サービスのアクティブ化（Service Activation）]** を選択します。

Step 2 [サーバ（Server）] ドロップダウンリストから、Unified Communications Manager パブリッシャノードを選択して [移動（Go）] をクリックします。

Step 3 [CMサービス（CM Services）] で、**シスコ デバイス アクティベーション サービス**のステータスが [アクティブ化（Activated）] になっていることを確認します。

Step 4 サービスが実行されていない場合は、隣接するチェックボックスをオンにして、[保存（Save）] をクリックします。

次のタスク

アクティベーション コードを使用する登録方法の設定 （426 ページ）

アクティベーション コードを使用する登録方法の設定

特定のモデルタイプの電話機で Unified Communications Manager への登録にアクティベーション コードを使用するようにシステムのデフォルト値を設定するには、次の手順を使用します。

（注） この手順は、オンプレミスのエンドポイントのオンボーディングにのみ適用されます。[デバイスのデフォルト（Device Defaults）] のオンボーディング方式の設定は、アクティベーションコードを使用したモバイルおよびリモートアクセス エンドポイントのオンボーディングには適用されません。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]>[デバイスの設定（Device Settings）]>[デバイスのデフォルト（Device Defaults）]** を選択します。

Step 2 **[デバイスのデフォルト設定（Device Defaults Configuration）]** ウィンドウの **[デュアルバンク情報（Dual Bank Information）]** セクションで、登録にアクティベーションコードを使用するデバイス タイプを選択し、**[オンプレミスオンボーディング方式（On-Premise Onboarding Method）]** を **[自**

動登録（**Auto Registration**）] から **[アクティベーションコード（Activation Code）]** に変更します。

Step 3 [保存（Save）] をクリックします。

（注） 以前に電話機のタイプに対して自動登録が使用されていた場合にデバイスのデフォルトをアクティベーションコードに設定すると、以降に追加される新しい電話機は、アクティベーションコードによるオンボーディングか、電話機の手動設定（MACアドレスを使用）と登録に従うことになります。

新しい電話機のプロビジョニングの詳細については、「アクティベーション コードを要件とする電話機の追加」および「一括管理によるアクティベーション コードを使用した電話の追加」セクションを参照してください。

アクティベーション コードを要件とする電話機の追加

アクティベーション コードを要件として新しい電話機をプロビジョニングする場合は、この手順を使用します。

始める前に

適用する設定を入力したユニバーサルデバイステンプレートおよびユニバーサル回線テンプレートを設定することで、プロビジョニング プロセスを迅速化できます。

（注） テンプレートを使用しない場合は、新しい電話機を追加して手動で設定するか、またはBATテンプレートを使用して設定を追加することができます。いずれの場合も、[電話機の設定（Phone Configuration）] ウィンドウで [オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）] チェックボックスをオンにする必要があります。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[デバイス（Device）] > [電話（Phone）]**

Step 2 [テンプレートからの新規の追加（Add New From Template）] をクリックして、ユニバーサル回線テンプレートまたはユニバーサル デバイス テンプレートから設定を追加します。

Step 3 [電話のタイプ（Phone Type）] ドロップダウン メニューから、電話機モデルを選択します。

Step 4 [MACアドレス（MAC Address）] フィールドに、MACアドレスを入力します。アクティベーション コードでは、ダミーの MAC アドレスまたは電話機の実際の MAC アドレスを使用できます。

次のシナリオでは、電話機の MAC アドレスを変更できます。

- **BAT{mac}->SEP{mac}**：保存時にプレフィックスを `?BAT?` から `?SEP?` に変更するデバイス名を正確に知っている必要があります。

- **SEP{mac}->BAT{mac}**：プレフィックスを ?SEP? から ?BAT? に変更する MAC アドレスと、プレフィックスが ?BAT? の新しいデバイス名を空白にできます。

アクティベーション コードが有効化されている場合、[MACアドレス（MAC Address）] フィールドは空白のままにすることができます。ダミーの MAC アドレスが自動入力されます。

Step 5 [デバイステンプレート（Device Template）] ドロップダウンリストから、適用する設定が含まれる既存のユニバーサル デバイス テンプレートなどのテンプレートを選択します。

Step 6 [ディレクトリ番号（Directory Number）] フィールドから、既存のディレクトリ番号を選択するか、[新規（New）] をクリックして次の手順を実行します。

a) [新規内線の追加（Add New Extension）] ポップアップで、適用する設定が含まれている新しいディレクトリ番号と回線テンプレートを入力します。

b) [保存（Save）] をクリックして、さらに [閉じる（Close）] をクリックします。
新しい内線番号が [ディレクトリ番号（Directory Number）] フィールドに表示されます。

Step 7 （オプション）[ユーザ（User）] フィールドで、この電話機に適用するユーザ ID を選択します。

Step 8 [追加（Add）] をクリックします。

Step 9 [オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）] チェックボックスをオンにします。モバイルおよびリモートアクセスモードの場合は、[モバイルおよびリモートアクセス経由のアクティベーションコードを許可する（Allow Activation Code via Mobile and Remote Access）] チェックボックスをオンにします。

Step 10 適用するその他の設定を入力します。フィールドおよびその設定についてのヘルプは、オンライン ヘルプを参照してください。

Step 11 [保存（Save）] をクリックし、[OK] をクリックします。
この電話機の設定によって新しいアクティベーション コードが生成されます。コードを表示する場合は、[アクティベーション コードの表示（View Activation Code）] をクリックします。

次のタスク

電話機のアクティブ化（431 ページ）

一括管理によるアクティベーション コードを使用した電話の追加

このオプションのタスクフローには、一括管理ツールの電話の挿入機能を使用して 1 回の操作で多数の電話をプロビジョニングするプロビジョニング例が含まれます。これらの電話では、登録にアクティベーション コードを使用します。

手順

	コマンドまたはアクション	目的
Step 1	BAT プロビジョニングテンプレートの設定（429 ページ）	プロビジョニングされた電話に適用する設定を含むBATテンプレートを設定します。

	コマンドまたはアクション	目的
Step 2	新しい電話機での CSV ファイルの作成（430 ページ）	追加する新しい電話を含む CSV ファイルを作成します。
Step 3	電話の挿入（431 ページ）	一括管理の電話の挿入機能を使用して、新しい電話をデータベースに追加します。

BAT プロビジョニングテンプレートの設定

特定の電話機モデルの新しくプロビジョニングされた電話に対して一括管理から適用できる、共通設定を入力した電話テンプレートを作成するには、この手順を使用します。

始める前に

この手順では、ユーザがすでにシステムに展開されており、ニーズに合ったデバイスプール、SIP プロファイル、および電話セキュリティ プロファイルがすでに設定済みであることを前提としています。

手順

Step 1 Cisco Unified CM Administration から、**[一括管理（Bulk Administration）] > [電話（Phones）] > [電話テンプレート（Phone Template）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [電話のタイプ（Phone Type）] ドロップダウンリストから、テンプレートを作成する電話機モデルを選択します。

Step 4 [テンプレート名（Template Name）] を入力します。

Step 5 [オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）] チェックボックスをオンにします。モバイルおよびリモートアクセスモードの場合は、[モバイルおよびリモートアクセス経由のアクティベーションコードを許可する（Allow Activation Code via Mobile and Remote Access）] チェックボックスをオンにします。

Step 6 次の必須フィールドに値を入力します。

- デバイスプール（Device Pool）
- [電話ボタンテンプレート（Phone Button Template）]
- オーナーのユーザ ID（Owner User ID）
- デバイスのセキュリティプロファイル（Device Security Profile）
- SIP プロファイル（SIP Profile）

Step 7 [電話テンプレートの設定（Phone Template Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

次のタスク

新しい電話機での CSV ファイルの作成 （430 ページ）

新しい電話機での CSV ファイルの作成

新しい電話機で新しい csv ファイルを作成するには、次の手順を使用します。

（注） Csv ファイルは手動で作成することもできます。

手順

Step 1 Cisco Unified CM Administration から、**[一括管理（Bulk Administration）]>[ファイルのアップロード/ダウンロード（Upload/Download Files）]** を選択します。

Step 2 [検索（Find）] をクリックします。

Step 3 **bat.xlt** スプレッドシートを選択してダウンロードします。

Step 4 スプレッドシートを開き、[電話（Phones）] タブに移動します。

Step 5 新しい電話機の詳細をスプレッドシートに追加します。ダミーMACアドレスを使用する場合は、[MACアドレス（MAC Address）] フィールドを空白のままにします。[オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）] チェックボックスをオンにします。モバイルおよびリモートアクセスモードの場合は、[モバイルおよびリモートアクセス経由のアクティベーションコードを許可する（Allow Activation Code via Mobile and Remote Access）] チェックボックスをオンにします。

Step 6 入力が完了したら、[BAT形式にエクスポート（Export to BAT Format）] をクリックします。

Step 7 Cisco Unified CM Administration から、**[一括管理（Bulk Administration）]>[ファイルのアップロード/ダウンロード（Upload/Download Files）]** を選択します。

Step 8 CSV ファイルをアップロードします。

a) [新規追加（Add New）] をクリックします。
b) [**ファイルの選択 (Choose file)**] をクリックして、アップロードする csv ファイルを選択します。
c) ターゲットとして [電話（Phones）] を選択します。
d) [**Insert phone]:** トランザクションタイプに固有の詳細を選択します。
e) [保存（Save）] をクリックします。

次のタスク

電話の挿入 （431 ページ）

電話の挿入

CSV ファイルから新しい電話機を挿入するには、この手順を使用します。

手順

Step 1 **[一括管理（Bulk Administration）] > [電話（Phones）] > [電話の挿入（Insert Phones）]** を選択します。

Step 2 [ファイル名（File Name）] ドロップダウンリストから、CSV ファイルを選択します。

Step 3 [電話テンプレート名（Phone Template Name）] ドロップダウンリストから、作成したプロビジョニング テンプレートを選択します。

Step 4 [ダミーMACアドレスの作成（Create Dummy MAC Address）] チェックボックスをオンにします。

（注） セキュリティを強化するために、この CSV ファイルに実際の MAC アドレスを追加することで、一致する MAC アドレスを持つ電話機でのみアクティベーション コードを使用できるようになります。その場合は、このチェックボックスをオフのままにします。

Step 5 ジョブをすぐに実行するには、[今すぐ実行（Run Immediately）] チェックボックスをオンにします。後で実行することを選択した場合は、一括管理ツールのジョブ スケジューラでジョブのスケジュールを設定する必要があります。

Step 6 [送信（Submit）] をクリックします。

次のタスク

電話機のアクティブ化 （431 ページ）

電話機のアクティブ化

プロビジョニング後に、電話機のユーザにアクティベーションコードを配布して、電話機をアクティブ化できるようにします。アクティベーションコードを収集して配布するには、次の2つのオプションがあります。

- セルフケアポータル: 電話機のユーザは、電話機に適用されるアクティベーションコードを取得するために、セルフケアポータルにログインできます。電話機にコードを手動で入力するか、電話機のビデオカメラを使用して、セルフケアで表示されるバーコードをスキャンすることができます。どちらの方法でも動作します。セルフケアを使用して電話機をアクティブ化するには、Cisco Unified Communications Manager で、[アクティベーション可能状態になっている電話機を表示（Show Phones Ready to Activate）] エンタープライズパラメータを [はい（True）] に設定する必要があります（これがデフォルト設定です）。

（注） セルフケアポータルのユーザアクセスの設定方法に関する追加要件については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「セルフケアポータル」の章を参照してください。

- CSV ファイル: 未処理のユーザとアクティベーションコードのリストを csv ファイルにエクスポートすることもできます。これをユーザに配布できます。手順については、「アクティベーション コードのエクスポート（432 ページ）」を参照してください。

登録プロセス

電話機のユーザは、電話機を使用するために、電話機にアクティベーションコードを入力する必要があります。電話機のユーザが電話機で正しいアクティベーションコードを入力すると、次のことが発生します。

- 電話機は Cisco Unified Communications Manager で認証されます。
- Cisco Unified Communications Manager の電話機の設定は、電話機の実際の MAC アドレスを使用して更新されます。
- 電話機は、TFTP サーバからコンフィギュレーションファイルおよびその他の関連ファイルをダウンロードし、Cisco Unified Communications Manager に登録します。

次の作業

これで、電話機を使用できる状態になりました。

アクティベーション コードのエクスポート

アクティベーション コードとそれに対応する電話機およびユーザと共に CSV ファイルにエクスポートするには、この手順を使用します。このファイルを使用して、アクティベーション コードをユーザに配布できます。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [電話（Phone）]** を選択します。

Step 2 [関連リンク（Related Links）] から [アクティベーションコードのエクスポート（Export Activation Codes）] を選択し、[移動（Go）] をクリックします。

デバイス オンボーディング タスク フロー（モバイルおよびリモートアクセスモード）

モバイルおよびリモートアクセスモードでアクティベーションコードを使用して新しい電話機のオンボーディングを実行するには、次のタスクを実行します。

始める前に

Cisco Unified Serviceability で**シスコ デバイス アクティベーション サービス**が実行されている必要があります（このサービスはデフォルトで実行されます）。サービスが実行されていることを確認するには、「デバイス アクティベーション サービスの有効化（426 ページ）」を参照してください。

手順

	コマンドまたはアクション	目的
Step 1	モバイルおよびリモートアクセスによる Cisco Cloud オンボーディングの有効化（434 ページ）	[クラウドオンボーディング（Cloud Onboarding）] でバウチャーを生成し、アクティベーションコードによるオンボーディングを有効にして、モバイルおよびリモートアクセス アクティベーション ドメインを指定します。
Step 2	モバイルおよびリモートアクセス サービス ドメインの設定（オプション）（434 ページ）	クラウドへのクラスタのオンボーディングを実行して、モバイルおよびリモートアクセスのリモートデバイスを、特定のモバイルおよびリモートアクセス アクティベーション ドメインにオンボーディングできるようにします。
Step 3	カスタム証明書のアップロード (オプション)（435 ページ）	オンプレミスの場合、HTTPのデフォルトは8090、HTTPSのデフォルトは8181です。独自のカスタム証明書を使用する場合は、リモートのモバイルおよびリモートアクセス エンドポイントでクラウドから証明書をダウンロードし、Expressway への接続に使用できるようにします。
Step 4	アクティベーション コードを要件とする電話機をプロビジョニングします。プロビジョニングのオプションのサンプルを2つ示します。	Unified CM database で電話機をプロビジョニングする必要があります。Unified CM では、サンプルとして挙げたオプションを含めて、さまざまなプロビジョニング方法を使用できます。

	コマンドまたはアクション	目的
	• アクティベーション コードを要件とする電話機の追加（427 ページ） • 一括管理によるアクティベーション コードを使用した電話の追加（428 ページ）	
Step 5	電話機のアクティブ化（431 ページ）	アクティベーション コードをユーザに配布します。電話機を使用するためには、ユーザがその電話機にコードを入力する必要があります。

モバイルおよびリモートアクセスによるCisco Cloudオンボーディングの有効化

手順

Step 1 クラウドベースのデバイス アクティベーション サービスに接続するためにクラスタ（CCMActサービス）を認証するには、[バウチャーの生成（Generate Voucher）] ボタンをクリックしてバウチャーを生成します。

Step 2 モバイルおよびリモートアクセスアクティベーションドメインを指定します（これは、モバイルおよびリモートアクセスのサービスドメインリストに自動的にコピーされます）。

Step 3 アクティベーションコードによるオンボーディングを有効にするには、[アクティベーションコードによるオンボーディングを有効化（Enable the Activation Code Onboarding）] チェックボックスと [モバイルおよびリモートアクセスによるオンボーディングを許可（Allow Mobile and Remote Access Onboarding）] チェックボックスをオンにします。自動登録によるオンボーディングをデバイスのデフォルトとして設定した場合、[モバイルおよびリモートアクセスによるオンボーディングを許可（Allow Mobile and Remote Access Onboarding）] チェックボックスは無効化され、自動的にオンになります。この設定は、モバイルおよびリモートアクセスモードの電話機でのみ機能するためです。アクティベーション コードを使用したオンボーディングをデバイスのデフォルトとして設定した場合は、両方のチェックボックスを使用できます。

Step 4 [保存（Save）] をクリックします。

モバイルおよびリモートアクセスサービスドメインの設定（オプション）

電話機のモバイルおよびリモートアクセス サービス ドメインを設定するには、次の手順を実行します。

手順

Step 1 [高度な機能（Advanced Features）]>[モバイルおよびリモートアクセスサービスドメイン（Mobile and Remote Access Service Domain）] を選択して、[モバイルおよびリモートアクセスサービスドメイン（Mobile and Remote Access Service Domain）] ウィンドウにアクセスします。

Step 2 モバイルおよびリモートアクセス サービス ドメイン名を入力します。

Step 3 アクティベーションに使用される Expressway-E の SRV レコードを入力します。

Step 4 選択したドメインの横にある [デフォルト（Default）] チェックボックスをオンにして、デフォルトのモバイルおよびリモートアクセスサービスドメインを選択します。これは、デバイスプールレベルで [< None >] を選択した場合に使用されるドメインです。

Step 5 そのレコードの行にあるリンクを使用して依存関係レコードにアクセスし、依存関係の数も表示します。

カスタム証明書のアップロード(オプション)

カスタム証明書をアップロードするには、次の手順を使用します。

手順

Step 1 証明書をエクスプレス Sway にアップロードします。他の証明書は削除しないでください。

Step 2 **[CUCM OSの管理（CUCM OS Administration）]** > **[証明書の管理（Certificate Management）]** のパスを使用して、新しい証明書を Unified Communications Manager にアップロードします。「電話エッジ信頼」タイプを使用します（Unified Communications Manager は、これらの証明書をクラウドに送信してから、Expressway にアクセスするために電話機に送信します）。

Step 3 必要に応じて、その他の「電話エッジ信頼」タイプの証明書を削除して、カスタム証明書が使用中の証明書だけになるようにします。

アクティベーションコードの追加タスク

次の表に、アクティベーションコードに必要となる追加タスクを示します。

タスク	手順
登録済み電話機のアクティベーションコードの生成	すでに登録されている電話機のアクティベーションコードを生成するには、次のようにします。 **1.** Cisco Unified CM Administration から、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。 **2.** アクティベーション コードを生成する電話機を検索して [電話機の設定（Phone Configuation）] を開きます。 **3.** [オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）] チェックボックスをオンにして、[保存（Save）] をクリックします。
未登録の電話機のアクティベーション コードを生成する	未登録の電話機用に新しいアクティベーション コードを生成するには、次の手順を実行します。これは、新しい電話機のアクティベーションプロセスが失敗した場合などに必要になる可能性があります。 **1.** Cisco Unified CM Administration から、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。 **2.** アクティベーション コードを生成する電話機を検索して [電話機の設定（Phone Configuation）] を開きます。 **3.** [アクティベーションコードの解放（Release Activation Code）] をクリックします。 **4.** [新しいアクティベーションコードの生成（Generate New Activation Code）] をクリックし、[保存（Save）] をクリックします。

タスク	手順
アクティベーション コードのオプション パラメータの設定	アクティベーション コードのオプションのサービスパラメータを設定する場合は、次の手順を実行します。 **1.** Cisco Unified CM Administration から、[システム（System）]>[サービスパラメータ（Service Parameters）] の順に選択します。 **2.** [サーバ（Server）] ドロップダウンリストからパブリッシャノードを選択します。 **3.** [サービス（Service）] ドロップダウンリストから [シスコデバイスアクティベーションサービス（Cisco Device Activation Service）] を選択します。 **4.** 以下に示すオプションのサービスパラメータの値を設定します。設定の詳細については、状況依存ヘルプを参照してください。 • [アクティベーション有効期間（時間）（Activation Time to Live (Hours)）]：アクティベーション コードが有効である時間数。デフォルトは 168 です。 • [モバイルおよびリモートアクセス アクティベーションの有効化（Enable Mobile and Remote Access Activation）]：モバイルおよびリモートアクセス アクティベーションを有効にするには、この値を [はい（True）]（デフォルト設定）にします。 • [モバイルおよびリモートアクセスアクティベーションドメイン（Mobile and Remote Access Activation Domain）]：モバイルおよびリモートアクセスデバイスのアクティベーションが実行されるドメイン。 **5.** [保存（Save）] をクリックします。

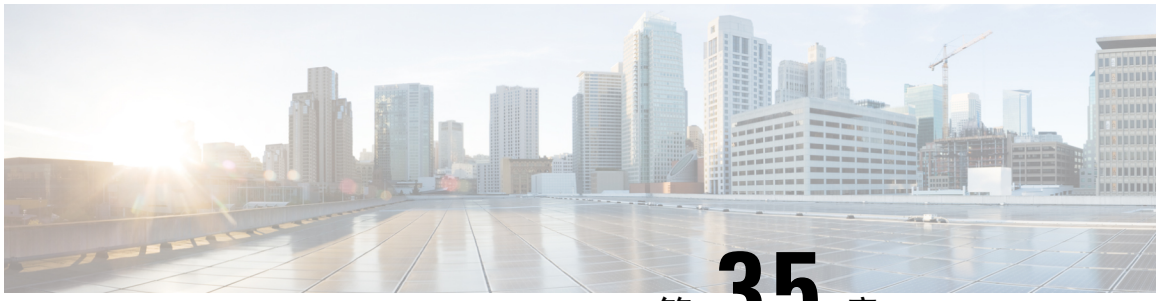
アクティベーション コードの使用例

次の表に、アクティベーションコードによるデバイスのオンボードの使用例を示します。

使用例	説明
既存の電話機の交換	アクティベーションコードを使用すると、既存の電話機を簡単に置き換えることができます。たとえば、リモートワーカーの電話機が破損し、新しい電話機が必要になったとします。 • 管理者が、Unified Communications Manager で破損した電話機の [電話機の設定（Phone Configuration）] を開きます。 • 管理者は、[MAC アドレス（MAC Address）] を空白にし、[オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）] チェックボックスをオンにして、[保存（Save）] をクリックします。 • ユーザが同じモデルの新しい電話機を入手し、その電話機をネットワークに接続します。 • ユーザはセルフケアにログインしてアクティベーションコードを取得し、電話機にコードを入力します。電話機のオンボーディングが正常に終了します。 （注） このシナリオでは、ユーザは、破損した電話機と同じ電話機モデルである限り、新しい電話機をオンボードできます。より安全な環境では、古い電話機を交換するために、管理者が交換用電話機をプロビジョニングする必要がある場合があります (以下を参照)。
アクティベーションコードを使用した新しい電話機の安全な配送	より安全な環境では、次のように、特定のMACアドレスにアクティベーションコードを使用して、電話機の出荷プロセスが安全であることを確認できます。 • 管理者が、Unified Communications Manager で新しい電話機をプロビジョニングします。 • 管理者は、新しい電話機の [電話機の設定（Phone Configuration）] で、電話機の実際のMACアドレスを入力し、[オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）] チェックボックスをオンにします。 • 管理者が、電話機を梱包してユーザに発送します。 • ユーザが新しい電話機をネットワークに接続します。 • ユーザがセルフケアにログインしてアクティベーションコードを取得し、電話機にコードを入力します。電話機のオンボーディングが正常に終了します。 （注） このシナリオでは、ユーザはその特定の電話機のみをオンボードできます。

使用例	説明
新しい電話機の安全な配送（自動登録）	アクティベーション コードの代わりに、自動登録および TAPS を使用して、リモート ワーカーに電話機を安全に配送することもできます。 • 管理者は、[デバイスのデフォルト設定（Device Defaults Configuration）] で、その電話モデルの [オンボーディング方式（Onboarding Method）] を [自動登録（Autoregistration）] に設定します。 • 管理者が、Unified Communications Manager で新しい電話機をプロビジョニングします。管理者は、新しい電話機の [電話機の設定（Phone Configuration）] で、電話機の実際の MAC アドレスを空白にします。 • 管理者が、電話機を梱包してユーザに発送します。 • ユーザが新しい電話機をネットワークに接続し、自動登録を実行させます。 • ユーザは、TAPS を使用して、自動登録されたレコードを古いレコードにマッピングします。 （注） このシナリオでは、自動登録と TAPS の両方を設定する必要があります。
自動登録による電話機の再オンボーディング	[デバイスのデフォルト設定（Device Defaults Configuration）] ウィンドウの **[オンプレミスのオンボーディング方式（On-Premise Onboarding Method）]** フィールドで、特定の電話機モデルのオンボーディング方式を、アクティベーション コードか自動登録に切り替えることができます。 （注） 既存の電話機の再オンボーディングを自動登録によって実行する場合、自動登録を機能させるには、既存のレコードをデータベースから削除する必要があります。

使用例	説明
モバイルおよびリモートアクセスモードで使用するためのオンプレミス電話機のオンボーディング	電話機のオンボーディングをオンプレミスで実行した後、モバイルおよびリモートアクセスモードでもう一度オンボーディングを実行するように電話機を設定すると、Expressway への OAuth 接続と Expressway から Cisco Unified Communications Manager への信頼できる接続で提供されるセキュリティを活用できます。 このシナリオでは、[モバイルおよびリモートアクセス経由のアクティベーションコードを許可する（Allow Activation Code via Mobile and Remote Access）] を有効にしてオンプレミスで電話機のオンボーディングを実行し、受信した OAuth アクセストークンを検証した後、モバイルおよびリモートアクセスモードに切り替えて Expressway との通信を開始します。内部ネットワークでオンプレミスからのライン Sway との通信が許可されていない場合、電話機は登録されませんが、オフプレミスの電源がオンになっているときには、その電話機に接続する準備ができています。 （注） 未登録のオフプレミスの電話機は、ファームウェアのロードを更新できません。このシナリオは、最新のファームウェアをダウンロードし、アクティベーションコード機能を使用するためにオンプレミスにする必要がある、すぐに設定された電話機で役立ちます。 電話機は、[MRA経由のアクティベーションコードを許可する（Allow Activation Code via MRA）] チェックボックスがオンになっていて、MRA サービスドメインと OAuth トークンがある場合に MRA モードに切り替わります。
ゼロタッチオンボーディングによるオンプレミス電話機のオンボーディング	オンプレミスの電話機を登録するとき、セキュリティプロファイルが OAuth に設定されていると、電話機のリセット時または再起動時に暗黙的にアクセストークンが取得されます。



第 35 章

自動登録の設定

自動登録の概要

自動登録では、新しい電話機をネットワークに接続したときに、Unified Communications Manager がそれらの電話機にディレクトリ番号を自動的に割り当てることができます。

現在、自動登録はセキュア モードで有効になっています。この拡張機能によって、新しい電話のプロビジョニング中にクラスタを保護できるため、システムのセキュリティが強化されます。また、新しい電話を登録する際にクラスタ セキュリティを無効にする必要がないため、登録プロセスが簡素化されるメリットもあります。

911（緊急）および 0（オペレータ）コールのみを許可するデバイスプールを作成しておくと、自動登録が有効になっている場合に許可されていないエンドポイントがネットワークに接続するのを防ぐために使用できます。新しいエンドポイントはこのプールに登録できますが、アクセスは制限されます。連続して起動しネットワークへの登録を試みる不正なデバイスによる不正アクセスは阻止されます。電話番号に影響を与えることなく、自動登録された電話を新しい場所に移動し、別のデバイスプールに割り当てることができます。

システムは、自動登録されている新しい電話機が SIP または SCCP を実行しているかどうかを認識していないため、自動登録を有効にするときにこれを指定する必要があります。SIP と SCCP の両方をサポートするデバイス（Cisco IP 電話 7911、7940、7941、7960、7961、7970、および7971 シリーズなど）は、Auto Registration Phone Protocol と呼ばれるエンタープライズパラメータで指定されたプロトコルで自動登録されます。

1 つのプロトコルのみをサポートするデバイスは、そのプロトコルを使用して自動登録されます。自動登録の電話プロトコル設定は無視されます。たとえば、SCCP のみをサポートするすべての Cisco IP 電話は、自動登録電話プロトコルパラメータが [SIP] に設定されていても、SCCP でのみ自動登録します。

ネットワークに追加する電話機が 100 に満たない場合は、自動登録機能を使用することをお勧めします。100 台を超える電話機を追加するには、一括管理ツール（BAT）を使用します。詳細については、『*Cisco Unified Communications Manager* 一括アドミニストレーション ガイド』

（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

自動登録の設定タスクフロー

自動登録を有効にすると、セキュリティ上のリスクが伴います。ネットワークに新しいエンドポイントを追加している間は、短時間の自動登録のみを有効にしてください。

手順

	コマンドまたはアクション	目的
Step 1	自動登録のパーティションの設定 （443 ページ）	自動登録された電話を内部コールのみに制限するために、自動登録専用に使用するルートパーティションを設定します。
Step 2	自動登録用コーリングサーチスペースの設定 （444 ページ）	自動登録電話を内線専用に制限するには、自動登録専用のコーリングサーチスペースを設定します。
Step 3	自動登録用デバイスプールの設定 （445 ページ）	自動登録用に設定されているコーリングサーチスペースを使用するデバイスプールを作成します。
Step 4	自動登録のデバイスプロトコルタイプの設定 （446 ページ）	自動登録する電話機のタイプに一致するように、プロトコルを SCCP または SIP に設定するには、次の手順を使用します。
Step 5	自動登録の有効化 （446 ページ）	自動登録で使用する Cisco Unified Communications Manager グループに対して自動登録を有効にするには、自動登録用ノードで自動登録を有効にして、[自動登録 Cisco Unified Communications Manager グループ（Auto-registration Cisco Unified Communications Manager Group）] パラメータを設定します。
Step 6	自動登録の無効化 （448 ページ）	新しいデバイスの登録が完了したらすぐに、ノードの自動登録を無効にします。
Step 7	自動登録番号の再利用 （449 ページ）	（オプション）無効になっているデバイスの自動登録番号は再利用できます。自動登録ディレクトリ番号の範囲をリセットした場合、開始番号から再度検索するようにシステムに強制します。利用可能なディレクトリ番号は再利用されます。

自動登録のパーティションの設定

自動登録された電話を内部コールのみに制限するために、自動登録専用に使用するルートパーティションを設定します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[コールルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [パーティション（Partition）]** を選択します。

Step 2 [新規追加（Add New）] をクリックして新しいパーティションを作成します。

Step 3 [パーティション名、説明（Partition Name, Description）] フィールドに、ルート プランに固有のパーティション名を入力します。

パーティション名には、英数字とスペースの他にハイフン（-）とアンダースコア（_）を使用できます。パーティション名に関するガイドラインについては、オンライン ヘルプを参照してください。

Step 4 パーティション名の後にカンマ（,）を入力し、パーティションの説明を同じ行に入力します。

説明には、任意の言語で最大50文字を使用できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）、角括弧（[]）は使用できません。

説明を入力しなかった場合は、Cisco Unified Communications Manager が、このフィールドに自動的にパーティション名を入力します。

Step 5 複数のパーティションを作成するには、各パーティション エントリごとに 1 行を使います。

Step 6 [スケジュール（Time Schedule）] ドロップダウンリストから、このパーティションに関連付けるスケジュールを選択します。

スケジュールでは、パーティションが着信コールの受信に利用可能となる時間を指定します。[なし（None）] を選択した場合は、パーティションが常にアクティブになります。

Step 7 次のオプション ボタンのいずれかを選択して、[タイム ゾーン（Time Zone）] を設定します。

- [発信側デバイス（Originating Device）]：このオプション ボタンを選択すると、発信側デバイスのタイムゾーンと [スケジュール（Time Schedule）] が比較され、パーティションが着信コールの受信に使用できるかどうかが判断されます。
- [特定のタイム ゾーン（Specific Time Zone）]：このオプション ボタンを選択した後、ドロップダウン リストからタイム ゾーンを選択します。選択されたタイム ゾーンと [スケジュール（Time Schedule）] が比較され、着信コールの受信にパーティションが使用できるかどうかが判断されます。

Step 8 [保存（Save）] をクリックします。

次のタスク

自動登録用コーリングサーチスペースの設定 （444 ページ）

自動登録用コーリングサーチスペースの設定

自動登録電話を内線専用に制限するには、自動登録専用のコーリングサーチスペースを設定します。

始める前に

自動登録のパーティションの設定 （443 ページ）

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[コールルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [コーリングサーチスペース（Calling Search Space）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [名前（Name）] フィールドに、名前を入力します。

各コーリング サーチ スペース名がシステムに固有の名前であることを確認します。この名前には、最長 50 文字の英数字を指定することができ、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて含めることが可能です。

Step 4 [説明（Description）] フィールドに、説明を入力します。

説明には、任意の言語で最大50文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

Step 5 [使用可能なパーティション（Available Partitions）] ドロップダウン リストから、次の手順のいずれかを実施します。

- パーティションが 1 つの場合は、そのパーティションを選択します。
- パーティションが複数ある場合は、Ctrl キーを押した状態で適切なパーティションを選択します。

Step 6 ボックス間にある下矢印を選択し、[選択されたパーティション（Selected Partitions）] フィールドにパーティションを移動させます。

Step 7 （任意）[選択されたパーティション（Selected Partitions）] ボックスの右側にある矢印キーを使用して、選択したパーティションの優先順位を変更します。

Step 8 [保存（Save）] をクリックします。

次のタスク

自動登録用デバイスプールの設定 （445 ページ）

関連トピック

サービスクラス, on page 202

自動登録用デバイスプールの設定

自動登録にデフォルトのデバイスプールを使用するか、SIP用とSCCPデバイス用に自動登録に使用する個別のデバイスプールを設定することができます。

自動登録用のデフォルトのデバイスプールを設定するには、デフォルトのCisco Unified Communications Managerグループと、自動登録コーリングサーチスペース(CSS)をデフォルトのデバイスプールに割り当てます。SIPデバイスとSCCPデバイス用に個別のデフォルトデバイスプールを設定する場合は、デフォルトのデバイスプール値を使用します。

始める前に

自動登録用コーリングサーチスペースの設定 （444 ページ）

手順

Step 1 Cisco Unified Communications Manager の管理ページで、**[システム(System)]** > **[デバイスプール(Device Pool)]** を選択します。

Step 2 自動登録のデフォルトデバイスプールを変更するには、次の操作を実行します。

a) **[検索（Find）]**をクリックし、デバイスプールのリストから **[デフォルト]** を選択します。

b) [デバイスプールの設定（Device Pool Configuration）] ウィンドウで、[自動登録用コーリングサーチスペース（Calling Search Space for Auto-registration）] フィールドで自動登録に使用する CSS を選択し、[保存（Save）] をクリックします。

Step 3 自動登録用の新しいデバイスプールを作成するには、次の操作を実行します。

a) [新規追加（Add New）] をクリックします。

b) [デバイスプールの設定（Device Pool Configuration）] ウィンドウで、デバイスプールの一意の名前を入力します。

名前は最大 50 文字までで、英数字、ピリオド（.）、ハイフン（-）、アンダースコア（_）、および空白を使用できます。

c) 次のフィールドをデフォルトのデバイスプールと一致するように設定します。フィールドの説明については、オンライン ヘルプを参照してください。

- [Cisco Unified Communications Manager グループ（Cisco Unified Communications Manager Group）] で、[デフォルト（Default）] を選択します。
- [日時グループ（Date/Time Group）] で、[CMLocal] を選択します。
- [リージョン（Region）] で、[デフォルト（Default）] を選択します。

d) [自動登録用コーリングサーチスペース（Calling Search Space for Auto-registration）] フィールドで自動登録に使用する CSS を選択し、[保存（Save）] をクリックします。

次のタスク

自動登録のデバイスプロトコルタイプの設定 （446 ページ）

自動登録のデバイスプロトコルタイプの設定

SIPおよびSCCPデバイスが自動登録されている場合は、まず自動登録の電話プロトコルパラメータを SCCP に設定し、SCCP を実行しているすべてのデバイスをインストールする必要があります。次に、Auto Registration Phone Protocol パラメータを [SIP] に変更し、SIP を実行するすべての電話を自動登録する必要があります。

始める前に

自動登録用デバイスプールの設定 （445 ページ）

手順

Step 1 Cisco Unified Communications Manager の管理で、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** の順に選択します。

Step 2 [エンタープライズパラメータ設定（Enterprise Parameters Configuration）] ウィンドウで、[自動登録電話プロトコル（Auto Registration Phone Protocol）] ドロップダウンリストから [SCCP] または [SIP] を選択し、[保存（Save）] をクリックします。

次のタスク

自動登録の有効化 （446 ページ）

自動登録の有効化

自動登録が有効の場合は、ネットワークに接続する際に新しいエンドポイントに割り当てられる電話番号の範囲を指定する必要があります。新しいエンドポイントが接続される度に、次の使用可能な電話番号が割り当てられます。自動登録に使用できる電話番号がなくなった場合、エンドポイントを自動登録することはできません。

新しいエンドポイントは、[自動登録Cisco Unified CMグループ（Auto-Registration Cisco Unified Communications Manager Group）] 設定が有効になっているグループ内の最初の Unified Communications Manager ノードを使用して、自動登録されます。その後、デバイス タイプに基づき、自動登録された各エンドポイントがデフォルトのデバイスプールに自動で割り当てられます。

始める前に

自動登録のデバイスプロトコルタイプの設定 （446 ページ）

- デバイス プール、コーリング サーチ スペース、および内線発信のみ許可するように自動登録するデバイスのアクセスを制限するルート パーティションを作成します。

- 電話番号が自動登録範囲で利用できることを確認します。
- 新しい電話を登録するために利用できるライセンス ポイントが十分にあることを確認します。
- [デバイスのデフォルト設定（Device Defaults Configuration）] ウィンドウに、SIP および SCCP の電話イメージ名が正しく表示されていることを確認します。共通デバイス設定ファイルのほとんどは TFTP サーバ上で利用できますが、デバイスの設定ファイルが存在することを確認します。
- Cisco TFTP サーバが起動して実行中であること、および TFTP の DHCP オプションで適切なサーバが指定されていることを確認します。

手順

Step 1 Cisco Unified Communications Manager Administration から、**[システム（System）] > [Cisco Unified CM]** を選択し、[Cisco Unified Communications Managerの検索と一覧表示（Find and List Cisco Unified Communications Managers）] ウィンドウの [検索（Find）] をクリックします。

Step 2 自動登録を使用するには、クラスタの [Cisco Unified Communications Manager] を選択します。

が表示されます。

Step 3 [Cisco Unified CM Configuration（Cisco Unified CM Configuration）] ウィンドウで、[自動登録情報（Auto-registration Information）]セクションのノードの自動登録パラメータを設定し、[保存（Save）] をクリックします。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

a) ユニバーサル デバイス テンプレートを選択して、ドロップダウン リストから自動登録を使用します。

自動登録用に作成されているユニバーサルデバイス テンプレートがない場合は、[デフォルトのユニバーサル デバイス テンプレート（Default Universal Device Template）] を選択します。選択したテンプレートで、デバイス プールが指定されていることを確認します。これは、**[ユーザの管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサルデバイステンプレート（Universal Device Template）]** からの自動登録で使用されます。

b) ドロップダウン リストからの自動登録に使用するユニバーサル ライン テンプレートを選択します。

自動登録用に作成されているユニバーサル ライン テンプレートがない場合は、[デフォルトのユニバーサル ライン テンプレート（Default Universal Line Template）] を選択します。選択したテンプレートで、コーリング サーチ スペースおよびルート パーティションが指定されていることを確認します。これは、**[ユーザの管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサル回線テンプレート（Universal Line Template）]** からの自動登録で使用されます。

c) 電話番号の最初と最後を [開始電話番号（Starting Directory Number）] および [終了電話番号（Ending Directory Number）] フィールドに入力します。

電話番号の最初と最後を同じ値に設定すると、自動登録は無効になります。

d) [このCisco Unified CM では自動登録は無効にする（Auto-registration Disabled on this Cisco Unified Communications Manager）] のチェックボックスをオフにして、このノードの自動登録を有効にします。

選択した Unified Communications Manager ノードでのみ自動登録を常に有効化または無効化します。自動登録機能をクラスタ内の別のノードに切り替える場合は、使用する Unified Communications Manager ノード、デフォルトの Unified Communications Manager グループ、およびデフォルトのデバイスプールを設定し直す必要があります。

Step 4 **[システム（System）] > [Cisco Unified CM Group]**を選択し、**[Cisco Unified CMグループの検索と一覧表示（Find and List Cisco Unified Communications Manager Groups）]** ウィンドウの **[検索（Find）]** をクリックします。

Step 5 自動登録を有効化する Unified Communications Manager グループを選択します。

このグループ名は、ほとんどの場合 [デフォルト（Default）] になります。別の Cisco Unified Communications Manager グループを選択することもできます。このグループでは、最低 1 つのノードを選択する必要があります。

Step 6 このグループの [Cisco Unified CMグループの設定（Cisco Unified CM Group Configuration）] ウィンドウで、[自動登録Cisco Unified CMグループ（Auto-registration Cisco Unified Communications Manager Group）] を選択して、グループの自動登録を有効にし、[保存（Save）] をクリックします。

ヒント [選択済みのCisco Unified CM（Selected Cisco Unified Communications Managers）] のリストに、自動登録用に設定したノードが含まれていることを確認します。矢印を使用して、リストに表示するノードを移動します。表示されている順に、Unified Communications Manager ノードが選択されます。変更を [保存（Save）] します。

Step 7 自動登録するデバイスをインストールします。

（注） 自動登録された電話を再設定し、その電話を永続的なデバイス プールに割り当てます。電話のロケーションを変更しても、電話に割り当てられている電話番号は変更されません。

（注） 別の種類の電話を登録するには、デバイスのプロトコル タイプを変更し、そのデバイスを取り付けてから自動登録を無効にします。

自動登録の無効化

新しいデバイスの登録が完了したらすぐに、ノードの自動登録を無効にします。

始める前に

自動登録の有効化 （446 ページ）

手順

Step 1 [Cisco Unified Communications Manager Administration] で、**[システム（System）]** > **[Cisco Unified CM]** を選択し、**[Cisco Unified CM の検索と一覧表示]** ウィンドウの **[検索（Find）]** をクリックします。

Step 2 ノードのリストから **Cisco Unified Communications Manager**を選択します。

Step 3 選択したノードの **[Cisco Unified CM Configuration]** ウィンドウで、 **[この Cisco Unified Communications Manager で自動登録を無効にする]**チェックボックスにチェックし、このノードの自動登録を無効にし、**[保存（Save）]** をクリックします。

ヒント [開始電話番号(Starting Directory Number)] フィールドと [終了電話番号(Ending Directory Number)] フィールドに同じ値を設定した場合も、自動登録が無効になります。

次のタスク

（オプション）自動登録されたデバイスのディレクトリ番号を手動で変更した場合や、そのデバイスをデータベースから削除した場合は、 そのディレクトリ番号を再使用することができます。詳細については、「自動登録番号の再利用 （449 ページ）」を参照してください。

自動登録番号の再利用

新しいデバイスがネットワークに接続されると、 システムは、次に使用可能な（未使用の）自動登録電話番号をそのデバイスに割り当てます。自動登録されたデバイスの電話番号を手動で変更した場合や、そのデバイスをデータベースから削除した場合は、そのデバイスの自動登録されていたディレクトリ番号を再使用することができます。

デバイスが自動登録しようとすると、 システムは管理者が指定した自動登録番号の範囲を検索して次に使用可能な電話番号を検出し、そのデバイスに割り当てます。Cisco Unified Communications Manager は、最後に割り当てられた電話番号の次の番号から順に、検索を開始します。範囲内の最後のディレクトリ番号に達すると、システムは範囲の開始ディレクトリ番号から検索し続けます。

自動登録のディレクトリ番号の範囲をリセットし、システムがその範囲の開始番号から検索するようにすることができます。

手順

Step 1 Cisco Unified Communications Manager Administration で、**[システム（System）]** > **[Cisco Unified Communications Manager]** を選択します。

Step 2 自動登録をリセットするには、[Cisco Unified Communications Manager] を選択します。

Step 3 現在の設定を [開始のディレクトリ番号（Starting Directory Number）] と [最後のディレクトリ番号（Ending Directory Number）] フィールドに書き留めます。

Step 4 [この Cisco Unified Communications Manager で自動登録を無効化（Auto-registration Disabled on this Cisco Unified Communications Manager）] をクリックしてから、[保存（Save）] をクリックします。

自動登録が無効の間、新しい電話は自動登録できません。

Step 5 [開始ディレクトリ番号（Starting Directory Number）] と [最後のディレクトリ番号（Ending Directory Number）] フィールドを以前の値に設定してから、[保存（Save）] をクリックします。

ヒント これらのフィールドを新しい値に設定できます。

第 36 章

セルフプロビジョニングの設定

セルフプロビジョニングの概要

セルフプロビジョニング機能は、管理者に連絡することなく自分の電話をプロビジョニングする機能をエンドユーザに提供することにより、ネットワークの電話機をプロビジョニングするのに役立ちます。システムでセルフプロビジョニングが設定されており、個別のエンドユーザでセルフプロビジョニングが有効化されている場合、そのエンドユーザは電話をネットワークに接続して所定のいくつかのプロンプトに従うことで、新しい電話機をプロビジョニングできます。Cisco Unified Communications Managerは、事前設定されたテンプレートを適用することによって、電話と電話回線を設定します。

セルフプロビジョニングは、管理者がエンドユーザの代わりに電話機をプロビジョニングする際に使用するか、またはエンドユーザがセルフプロビジョニングを使用して自分の電話機をプロビジョニングするために使用することができます。

セルフプロビジョニングは、クラスタのセキュリティ設定が非セキュア モードまたは混在モードであるかどうかにかかわらずサポートされます。

セキュリティモード

次の 2 つのモードのいずれかで、セルフプロビジョニングを設定できます。

- セキュアモード:セキュアモードでは、ルフプロビジョニングにアクセスするためにはユーザまたは管理者がセ認証されている必要があります。エンドユーザは、そのパスワードまたは暗証番号に対して認証を受けることができます。管理者は、事前設定された認証コードを入力できます。
- 非セキュアモード: 非セキュアモードでは、ユーザまたは管理者は、ユーザ ID またはセルフプロビジョニング ID を入力して、電話機をユーザアカウントに関連付けることができます。セキュリティで保護されていないモードは、日々の使用には推奨されていません。

ユニバーサル回線とデバイステンプレートによる設定

セルフプロビジョニングは、エンドユーザに対して、プロビジョニング済みの電話機と電話回線を設定するために、ユニバーサル回線テンプレートとユニバーサルデバイステンプレートの設定を使用します。ユーザが自分の電話機をプロビジョニングすると、システムはそのユーザのユーザプロファイルを参照し、対応するユニバーサルラインテンプレートを、プロビジョニングされた電話回線に、ユニバーサルデバイステンプレートを、プロビジョニングされた電話機に適用します。

プロビジョニングされた電話

この機能を設定したら、次の手順を実行して電話をプロビジョニングできます。

- 電話機をネットワークに接続します。
- セルフプロビジョニング IVR 内線番号をダイヤルします。
- プロンプトに従って、電話機を設定し、電話機をエンドユーザに関連付けます。セルフプロビジョニングの設定方法に応じて、エンドユーザは、ユーザパスワード、PIN、または管理者の認証コードを入力することができます。

ヒント　エンドユーザに代わって多数の電話をプロビジョニングしている場合、セルフプロビジョニング IVR 拡張に転送するユニバーサル デバイス テンプレートに短縮ダイヤルを設定します。

アナログ FXS ポートのセルフプロビジョニング

ユーザがセルフプロビジョニング IVR を呼び出して、関連付けられた DN をそのアナログポートに割り当てることができるように、アナログ FXS ポートでセルフプロビジョニングを有効にすることができます。さらに、プロビジョニングされた電話機では、ユーザはアナログ音声ゲートウェイポートに関連付けられている DN の割り当てを解除し、別のユーザに割り当てることができます。

手順

1. プラグインは、ゲートウェイの FXS 音声ポートのアナログ電話機です。ポートは自動登録または事前設定されている (手動で) ため、電話機は自動登録プールまたは割り当てられた DN から自動的に DN を取得します。
2. 自動登録されたアナログデバイスからのセルフプロビジョニング IVR を呼び出します。
3. セルフサービス ID と PIN を入力します。

（注）　確認時に、アナログデバイスはエンドユーザのプライマリ内線番号を使用してプロビジョニングされます。自動登録 DN がプールに解放されます。

セルフプロビジョニングの前提条件

エンドユーザがセルフプロビジョニングを使用できるようにするには、次の項目を使用してエンドユーザを設定する必要があります。

- エンドユーザには、プライマリ内線番号が必要です。
- エンドユーザは、ユニバーサルラインテンプレートのユニバーサルデバイステンプレートを含む、ユーザプロファイルまたは機能グループテンプレートに関連付けられている必要があります。ユーザープロファイルは、セルフプロビジョニング用に有効にする必要があります。

セルフプロビジョニングの設定タスクフロー

手順

	コマンドまたはアクション	目的
Step 1	セルフプロビジョニングのサービスの有効化 （454 ページ）	Cisco Unified Serviceability で、**セルフプロビジョニング IVR** サービスと **CTI Manager** サービスを有効にします。
Step 2	セルフプロビジョニングの自動登録の有効化 （454 ページ）	セルフプロビジョニング用の自動登録パラメータを有効にします
Step 3	CTI ルートポイントの設定 （455 ページ）	セルフプロビジョニング IVR サービスを処理するように CTI ルートポイントを設定します。
Step 4	CTI ルートポイントへの電話番号の割り当て （455 ページ）	ユーザが自動プロビジョニング IVR にアクセスするためにダイヤルインする内線番号を設定し、その内線番号を CTI ルートポイントに関連付けます。
Step 5	セルフプロビジョニングのアプリケーションユーザーの設定 （456 ページ）	セルフプロビジョニング IVR 向けのアプリケーションユーザの設定CTI ルートポイントをアプリケーションユーザに関連付けます。
Step 6	セルフプロビジョニングのシステムの設定 （457 ページ）	アプリケーションユーザと CTI ルートポイントをセルフプロビジョニングの IVR に関連付けるなど、セルフプロビジョニングのシステムの設定を構成します。

	コマンドまたはアクション	目的
Step 7	ユーザープロファイルでのセルフプロビジョニングの有効化 （458 ページ）	ユーザが割り当てられているユーザプロファイルで電話機をセルフプロビジョニングできるようにします。

セルフプロビジョニングのサービスの有効化

セルフプロビジョニング機能をサポートするサービスをアクティブ化するには、次の手順を使用します。セルフプロビジョニング用 IVR サービスと Cisco CTI Manager サービスの両方が実行されていることを確認します。

手順

Step 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスのアクティブ化（Service Activation）]** を選択します。

Step 2 [サーバ（Server）] ドロップダウンリストからパブリッシャノードを選択し、[移動（Go）] をクリックします。

Step 3 [CMサービス（CM Services）] で、[Cisco CTI Manager] をオンにします。

Step 4 [CTIサービス（CTI Services）] で、[セルフプロビジョニングIVR（Self Provisioning IVR）] をオンにします。

Step 5 [保存（Save）] をクリックします。

セルフプロビジョニングの自動登録の有効化

セルフプロビジョニングにこの手順を使用するためには、パブリッシャで自動登録パラメータを設定する必要があります。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [Cisco Unified CM（Cisco Unified CM）]** を選択します。

Step 2 パブリッシャノードをクリックします。

Step 3 プロビジョニングされた電話機に適用する**ユニバーサルデバイステンプレート**を選択します。

Step 4 プロビジョニングされた電話機の電話回線に適用する**ユニバーサル回線テンプレート**を選択します。

Step 5 [開始電話番号（Starting Directory Number）] および [終了電話番号（Ending Directory Number）] フィールドを使用して、プロビジョニングする電話に適用する電話番号の範囲を入力します。

Step 6 [このCisco Unified CMでは自動登録は無効にする（Auto-registration Disabled on the Cisco Unified Communications Manager）] チェックボックスをオフにします。

Step 7 SIP 登録に使用するポートを確認します。ほとんどの場合、ポートをデフォルト設定から変更する必要はありません。

Step 8 [保存（Save）] をクリックします。

CTI ルート ポイントの設定

セルフプロビジョニング IVR 用の CTI ルートポイントを設定するには、この手順を使用します。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [CTIルートポイント（CTI Route Point）]** を選択します。

Step 2 次のいずれかの手順を実行します。

a) [検索（Find）] をクリックし、既存の CTI ルートポイントを選択します。

b) [新規追加（Add New）] をクリックして、新しい CTI ルートポイントを作成します。

Step 3 [デバイス名（Device Name）] フィールドに、ルートポイントを識別する一意の名前を入力します。

Step 4 [デバイスプール（Device Pool）] ドロップダウンリストで、このデバイスのプロパティを指定するデバイスプールを選択します。

Step 5 [ロケーション（Location）] ドロップダウンリストから、このCTIルートポイントの適切なロケーションを選択します。

Step 6 [トラステッド リレーポイントを使用（Use Trusted Relay Point）] ドロップダウンリストから、Unified Communications Manager がこのメディア エンドポイントを使用してトラステッド リレーポイント（TRP）デバイスを挿入するかどうかを選択します。デフォルト設定では、このデバイスに関連付けられている共通デバイス設定の設定が使用されます。

Step 7 [CTIルートポイントの設定（CTI Route Point Configuration）] ウィンドウで、残りのフィールドに入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

CTI ルートポイントへの電話番号の割り当て

セルフプロビジョニング用の IVR にアクセスするためにユーザがダイヤルする内線番号を設定するには、この手順を使用します。この内線を、セルフプロビジョニングに使用する CTI ルートポイントに関連付ける必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[CTI ルートポイント（CTI Route Point）]** を選択します。

Step 2 [**[検索（Find）]**] をクリックして、セルフプロビジョニング用に設定した CTI ルートポイントを選択します。

Step 3 **[割り当て（Association）]** で、**[回線 [1] - 新しい DN の追加（Line [2] – Add a new DN）]** をクリックします。
[電話番号の設定(Directory Number Configuration)] ウィンドウが表示されます。

Step 4 [電話番号（Directory Number）] フィールドに、セルフプロビジョニング IVR サービスにアクセスするためにダイヤルする内線番号を入力します。

Step 5 [保存（Save）] をクリックします。

Step 6 [電話番号の設定（Directory Number Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 7 [保存（Save）] をクリックします。

セルフプロビジョニングのアプリケーションユーザーの設定

セルフプロビジョニング IVR 用にアプリケーションユーザーを設定し、アプリケーションユーザーに作成した CTI ルーティング ポイントを関連付ける必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[ユーザ（User）]** > **[アプリケーションユーザー（Application User）]** を選択します。

Step 2 次のいずれかの手順を実行します。

a) 既存のアプリケーションユーザーを選択するには、[検索（Find）] をクリックして、アプリケーションユーザーを選択します。

b) 新しいアプリケーションユーザーを作成するには、[新規追加（Add New）] をクリックします。

Step 3 [ユーザ ID（User ID）] テキストボックスに、アプリケーションユーザーの一意の名前を入力します。

Step 4 アプリケーションユーザーの [BLF プレゼンス グループ（BLF Presence Group）] を選択します。

Step 5 アプリケーションユーザーに作成した CTI ルーティング ポイントを関連付けるには、次の手順を実行します。

a) 作成した CTI ルーティング ポイントが、[使用可能なデバイス（Available Devices）] リストボックスに表示されない場合は、[別のルートポイントを検索（Find More Route Points）] をクリックします。
作成した CTI ルーティング ポイントが、使用可能なデバイスとして表示されます。

b) [使用可能なデバイス（Available Devices）] リストで、セルフプロビジョニング用に作成した CTI ルートポイントを選択し、下向き矢印をクリックします。
CTI ルートポイントが [制御するデバイス（Controlled Devices）] リストに表示されます。

Step 6 [アプリケーションユーザーの設定（Application User Configuration）] ウィンドウの他のフィールドを設定します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 7 [保存（Save）] をクリックします。

セルフプロビジョニングのシステムの設定

システムをセルフプロビジョニング用に設定するには、次の手順を使用します。セルフプロビジョニングは、ネットワーク内のユーザが管理者に連絡をとらずに IVR システムを介して自分のデスクフォンを追加できる機能を提供します。

（注） セルフプロビジョニング機能を使用するには、エンドユーザのユーザープロファイルでも該当機能を有効にする必要があります。

手順

Step 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [セルフプロビジョニング（Self-Provisioning）]** を選択します。

Step 2 セルフプロビジョニング IVR でエンドユーザを認証するかどうかを設定するには、次のオプション ボタンのいずれかをクリックします。

- [認証が必要（Require Authentication）]：セルフプロビジョニング IVR を使用するには、エンドユーザが自分のパスワード、PIN、またはシステム認証コードを入力する必要があります。
- [認証は必要なし（No Authentication Required）]：エンド ユーザは認証なしでセルフプロビジョニング IVR にアクセスできます。

Step 3 セルフプロビジョニング IVR で認証を要求するように設定されている場合、次のオプション ボタンのいずれかをクリックして、IVR がエンド ユーザを認証する方法を設定します。

- [エンド ユーザのみを認証（Allow authentication for end users only）]：エンド ユーザは自分のパスワードまたは PIN を入力する必要があります。
- [ユーザ（Password/PIN の入力）および管理者（認証コードの入力）を認証（Allow authentication for users (via Password/PIN) and Administrators (via Authentication Code)）]：エンド ユーザは認証コードを入力する必要があります。このオプションを選択した場合、認証コードとして、0 から 20 桁までの整数を [認証コード（Authentication Code）] テキストボックスに入力します。

Step 4 [IVR 設定（IVR Settings）] のリストボックスから、矢印を使用して IVR プロンプトで使用する言語を選択します。使用可能な言語は、システムにインストールした言語パックによって異なります。追加の言語パックをダウンロードするには、cisco.com のダウンロードセクションを参照してください。

Step 5 [CTIルートポイント（CTI Route Points）] ドロップダウンリストから、セルフプロビジョニング IVR 用に設定した CTI ルートポイントを選択します。

Step 6 [アプリケーションユーザ（Application User）] ドロップダウンリストから、セルフプロビジョニング用に設定したアプリケーションユーザーを選択します。

Step 7 [保存（Save）] をクリックします。

ユーザープロファイルでのセルフプロビジョニングの有効化

ユーザが電話をセルフプロビジョニングできるようにするには、その機能が割り当てられているユーザプロファイルで有効になっている必要があります。

（注） ユーザが使用しているユーザープロファイルがわからない場合は、[エンドユーザの設定（End User Configuration）] ウィンドウでユーザの設定を開き、[ユーザプロファイル（User Profile）] フィールドで正しいプロファイルを確認できます。

手順

Step 1 Cisco Unified CM Administration から、[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザプロファイル（User Profile）] を選択します。

Step 2 [検索 (Find)] をクリックして、ユーザが割り当てられている**ユーザプロファイルを選択**します。

Step 3 そのユーザープロファイルに**ユニバーサル回線テンプレート**と**ユニバーサルデバイステンプレート**を割り当てます。

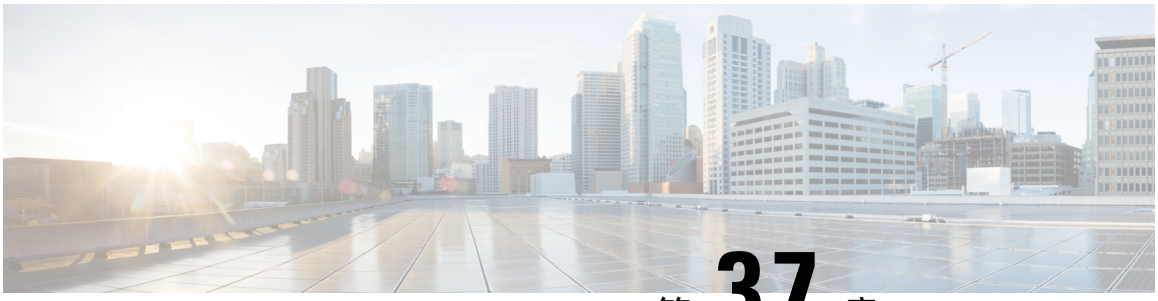
Step 4 セルフプロビジョニング用のユーザの設定

- [エンドユーザに自分の電話のプロビジョニングを許可（Allow End User to Provision their own phones）] チェックボックスをオンにします。
- ユーザがプロビジョニングできる電話機の数の制限を入力します。デフォルトは 10 です。
- ユーザがセルフプロビジョニングを使用して以前に割り当てられた電話機を無効にしたい場合は、古いデバイスのエンドユーザに関連付けられているユーザープロファイルページで、別のエンド ユーザに割り当てられている電話機の **[別のエンドユーザーにすでに割り当てられている電話のプロビジョニングを許可する]** 設定を確認します。以前に割り当てられた電話機をユーザが再割り当てできるのは、古いデバイスに関連付けられているユーザプロファイル内でこのチェックボックスをオンにした場合のみです。

Step 5 [保存（Save）] をクリックします。

第 VI 部

参考情報



第 37 章

Cisco Unified Communications Manager の TCP および UDP ポートの使用

Cisco Unified Communications Manager の TCP と UDP ポートの使用に関する概要

Cisco Unified Communications Manager の TCP および UDP ポートは、次のカテゴリに整理されます。

- Cisco Unified Communications Manager サーバーがクラスタ間で使用するポート
- 共通サービス ポート
- Cisco Unified Communications Manager と LDAP ディレクトリの間のポート
- CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求
- Cisco Unified Communications Manager から電話機への Web 要求
- 電話機と Cisco Unified Communications Manager の間のシグナリング、メディア、およびその他の通信
- ゲートウェイと Cisco Unified Communications Manager の間のシグナリング、メディア、およびその他の通信
- アプリケーションと Cisco Unified Communications Manager の間の通信
- CTL クライアントとファイアウォールの通信
- HP サーバ上の特殊なポート

上記のそれぞれのカテゴリのポートの詳細については、「「ポートの説明」」を参照してください。

（注） シスコでは、これらのポートで想定されるすべての設定シナリオを検証しているわけではありません。この一覧を参考にした結果、設定に問題が発生した場合は、シスコのテクニカルサポートにお問い合わせください。

ポート設定は、特に Cisco Unified Communications Manager に適用されます。リリースによってポートが異なる場合があり、今後のリリースで新しくポートが追加される可能性もあります。このため、インストールされている Cisco Unified Communications Manager のバージョンに一致するバージョンのマニュアルを使用していることを確認してください。

事実上すべてのプロトコルが双方向で行われますが、セッション開始側から見た方向を記載しています。デフォルトのポート番号は、管理者が手動で変更できる場合もありますが、ベスト プラクティスとしてこのような変更は推奨しません。Cisco Unified Communications Manager が内部使用に限って複数のポートを開くことに注意してください。

Cisco Unified Communications Manager ソフトウェアをインストールすると、デフォルトでは有用性のために次のネットワーク サービスが自動的にインストールされてアクティブになります。詳細については、「Cisco Unified Communications Manager サーバの間のクラスタ内ポート」を参照してください。

- Cisco Log Partition Monitoring（共通パーティションを監視および消去します。このサービスは、カスタム共通ポートを使用しません）
- Cisco Trace Collection Service（TCTS ポート使用）
- Cisco RIS Data Collector（RIS サーバ ポート使用）
- Cisco AMC Service（AMC ポート使用）

ファイアウォール、ACL、または QoS の設定は、トポロジ、テレフォニー デバイスおよびテレフォニー サービスの配置とネットワーク セキュリティ デバイスの配置との関係、および使用中のアプリケーションとテレフォニー拡張機能によって異なります。また、デバイスやバージョンによって、ACL のフォーマットが異なることにも注意してください。

（注） Cisco Unified Communications Manager でマルチキャスト保留音（MoH）ポートを設定することもできます。このマニュアルにはマルチキャスト MOH のポート値を記載していません。

（注） システムのエフェメラル ポートの範囲は 32768 ～ 61000 であり、電話を登録したままにするには、これらのポートを開く必要があります。詳細については、「http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html」を参照してください。

（注） ポート 22 への接続が開き、抑えられないように、ファイアウォールを設定します。IM and Presence サブスクライバ ノードのインストール中に、Cisco Unified Communications Manager パブリッシャ ノードに対する複数の接続が短時間に連続して開かれます。これらの接続をスロットリングすると、インストールが失敗する可能性があります。

ポート説明

Cisco Unified Communications Manager サーバーがクラスタ間で使用するポート

表 *29 : Cisco Unified Communications Manager* サーバーがクラスタ間で使用するポート

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
エンドポイント	Unified Communications Manager	514 / UDP	システム ロギン
Unified Communications Manager	Unified Communications Manager	443 / TCP	このポートは、サ バノードでの CO のインストール中 クライバとパブ 通信に使用され
Unified Communications Manager	RTMT	1090、1099 / TCP	RTMT パフォー ター、データ収 グ、およびアラー Cisco AMC サー
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1500、1501 / TCP	データベース接 TCP はセカンダ
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1510 / TCP	CAR IDS DB。C ジンが、クライア 接続要求を監視
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1511 / TCP	CAR IDS DB。ア ド時に、CAR ID タンスをもう 1 つ めに使用される

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1515 / TCP	インストール時のノ のデータベース レプ ション
Cisco Extended Functions（QRT）	Unified Communications Manager（DB）	2552 / TCP	Cisco Unified Commu Managerデータベー 知をサブスクライバ きるようにします。
Unified Communications Manager	Unified Communications Manager	2551 / TCP	アクティブ/バックア 別のための Cisco Ex Services 間のクラス
Unified Communications Manager（RIS）	Unified Communications Manager（RIS）	2555 / TCP	Real-time Information （RIS）データベー バー
Unified Communications Manager（RTMT、AMC、またはSOAP）	Unified Communications Manager（RIS）	2556 / TCP	Cisco RIS 向け Real- Information Services データベース クライ
Unified Communications Manager（DRS）	Unified Communications Manager（DRS）	4040 / TCP	DRS プライマリエー ト
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5001 / TCP	このポートは、SOA ターがリアルタイム ターリング サービス します。
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5002 / TCP	このポートは、SOA ターがパフォーマン ター サービスに使用 す。
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5003 / TCP	このポートは、SOA ターがコントロール ター サービスに使用 す。
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5004 / TCP	このポートは、SOA ターがログ コレクシ サービスに使用しま
標準 CCM 管理者ユーザ / 管理者	Unified Communications Manager	5005 / TCP	このポートは SOAP CDROnDemand2 サ よって使用されます

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5007 / TCP	SOAP モニター
Unified Communications Manager（RTMT）	Unified Communications Manager（TCTS）	エフェメラル / TCP	Cisco Trace Colle Service（TCTS） Trace and Log Cer 向けのバックエ ス
Unified Communications Manager（Tomcat）	Unified Communications Manager（TCTS）	7000、7001、7002 / TCP	このポートは、 Collection Tool S Cisco Trace Colle との通信に使用
Unified Communications Manager（DB）	Unified Communications Manager（CDLM）	8001 / TCP	クライアント デ 変更通知
Unified Communications Manager（SDL）	Unified Communications Manager（SDL）	8002 / TCP	クラスタ間通信
Unified Communications Manager（SDL）	Unified Communications Manager（SDL）	8003 / TCP	クラスタ間通信 （CTI 対象）
Unified Communications Manager	CMI マネージャ	8004 / TCP	Cisco Unified Co Manager と CMI とのクラスタ間
Unified Communications Manager（Tomcat）	Unified Communications Manager（Tomcat）	8005 / TCP	Tomcat シャット リプトで使用さ ニング ポート
Unified Communications Manager（Tomcat）	Unified Communications Manager（Tomcat）	8080 / TCP	診断テストのた 間の通信
ゲートウェイ	Unified Communications Manager	8090	CUCM と GW（ ターフェイス） Recording 機能の に使用する HTT
Unified Communications Manager	ゲートウェイ		
Unified Communications Manager（IPSec）	Unified Communications Manager（IPSec）	8500 / TCP および UDP	IPSec クラスタ よるシステム デ スタ間複製
Unified Communications Manager（RIS）	Unified Communications Manager（RIS）	8888 ～ 8889 / TCP	RIS サービス マ ステータス要求

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Location Bandwidth Manager（LBM）	Location Bandwidth Manager（LBM）	9004 / TCP	LBM 間のクラスタ
Unified Communications Manager パブリッシャ	Unified Communications Manager サブスクライバ	22 / TCP	Cisco SFTP サービス スクライバを新しく トールする場合は、 トを開く必要があり
Unified Communications Manager	Unified Communications Manager	8443 / TCP	ノード間のコントロ ター機能とネットワ ビスへのアクセスを ます。

共通サービス ポート

表 *30 :* 共通サービス ポート

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
エンドポイント	Unified Communications Manager	7	Internet Control Message Protocol（ICMP）。このプロトコル番号がエコー関連のトラフィックを伝送します。列見出しに示すようなポートとなるものではありません。
Unified Communications Manager	エンドポイント		
Unified Communications Manager (DRS、コール詳細レコード)	SFTP サーバー	22 / TCP	SFTP サーバーにバックアップ データを送信します。（DRS ローカル エージェント） コール詳細レコードデータを SFTP サーバーに送信します。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
エンドポイント	Unified Communications Manager（DHCP サーバー）	67 / UDP	DHCPサーバーとして機能する Cisco Unified Communications Manager （注） Cisco Unified Communications Manager 上で DHCP サーバーを実行することは推奨しません。
Unified Communications Manager	DHCP サーバー	68 / UDP	DHCPクライアントとして機能する Cisco Unified Communications Manager （注） Cisco Unified Communications Manager 上で DHCP クライアントを実行することは推奨しません。その代わりに、Cisco Unified Communications Manager には固定 IP アドレスを設定します。
エンドポイントまたはゲートウェイ	Unified Communications Manager	69、6969、次にエフェメラル / UDP	電話、ゲートウェイへの TFTP サービス
エンドポイントまたはゲートウェイ	Unified Communications Manager	6970 / TCP	プライマリサーバーとプロキシサーバー間の TFTP。 電話機とゲートウェイに対する TFTP サーバーの HTTP サービス
Unified Communications Manager	NTP サーバー	123 / UDP	Network Time Protocol（NTP）
SNMP サーバー	Unified Communications Manager	161 / UDP	SNMPサービス応答（管理アプリケーションからの要求）

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
CUCM サーバ SNMP プライマリ エージェント アプリケーション	SNMP トラップの宛先	162 / UDP	SNMP トラップ
SNMP サーバー	Unified Communications Manager	199 / TCP	SMUX サポート用組み込み SNMPエージェントリスニングポート
Unified Communications Manager	DHCP サーバー	546 / UDP	DHCPv6。IPv6 用の DHCP ポート。
Unified Communications Manager Serviceability	Location Bandwidth Manager（LBM）	5546 / TCP	Enhanced Location CAC Serviceability
Unified Communications Manager	Location Bandwidth Manager（LBM）	5547 / TCP	コール アドミッションの要求および帯域幅の縮小
Unified Communications Manager	Unified Communications Manager	6161 / UDP	プライマリエージェントとネイティブエージェント間の通信に使用され、ネイティブエージェントの MIB 要求を処理します。
Unified Communications Manager	Unified Communications Manager	6162 / UDP	プライマリエージェントとネイティブエージェント間の通信に使用され、ネイティブエージェントから生成された通知を転送します。
中央集中型 TFTP	代替 TFTP（Alternate TFTP）	6970 / TCP	中央集中型 TFTP ファイル ロケータ サービス
Unified Communications Manager	Unified Communications Manager	7161 / TCP	SNMPプライマリエージェントとサブエージェント間の通信に使用されます。
SNMP サーバー	Unified Communications Manager	7999 / TCP	Cisco Discovery Protocol（CDP）エージェントが、CDP 実行可能機器と通信します。
エンドポイント	Unified Communications Manager	443、8443/TCP	Cisco ユーザー データ サービス（UDS）の要求に使用されます。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager	Unified Communications Manager	9050 / TCP	Cisco Unified Communications Manager にある TAPS を利用して CRS 要求を処理します。
Unified Communications Manager	Unified Communications Manager	61441 / UDP	Cisco Unified Communications Manager アプリケーションが、UDP でこのポートにアラームを送信します。Cisco Unified Communications Manager MIB エージェントが、Cisco Unified Communications Manager MIB 定義に従って、このポートを監視し、SNMP トラップを生成します。
Unified Communications Manager	Unified Communications Manager	5060、5061 / TCP	トランクベースの SIP サービスを提供します。
Unified Communications Manager	Unified Communications Manager	7501	クラスタ間検索サービス（ILS）の証明書ベースの認証に使用されます。
Unified Communications Manager	Unified Communications Manager	7502	ILS がパスワードベースの認証に使用します。
Unified Communications Manager	Unified Communications Manager	9,966	ファイアウォールが有効になっているときに、クラスタ内のノード間で通信するために Cisco プッシュ通知サービスによって使用されます。
Unified Communications Manager	Unified Communications Manager	9560	ローカルプッシュ通知サービス（LPNS）で使用されます。
--	--	8000-48200	ASR および ISR G3 プラットフォームでは、デフォルトのポート範囲が指定されています。
		16384 ～ 32766	ISR G2 プラットフォームのデフォルトポート範囲。

Cisco Unified Communications Manager と LDAP ディレクトリの間のポート

表 *31 : Cisco Unified Communications Manager* と *LDAP* ディレクトリの間のポート

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager	外部ディレクトリ	389、636、3268、3269/TCP	外部ディレクトリ（Active Directory、Netscape Directory）への Lightweight Directory Access Protocol（LDAP）クエリー
外部ディレクトリ	Unified Communications Manager	エフェメラル	

CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求

表 *32 : CCMAdmin* または *CCMUser* から *Cisco Unified Communications Manager* への *Web* 要求

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
ブラウザ	Unified Communications Manager	80、8080/TCP	ハイパーテキスト転コル（HTTP）
ブラウザ	Unified Communications Manager	443、8443/TCP	Hypertext Transport P over SSL（HTTPS）
ブラウザ	Unified Communications Manager	9463 / TCP	Hypertext Transport P over SSL（HTTPS） TLS1.3 の v6 のみが です。

Cisco Unified Communications Manager から電話機への Web 要求

表 *33 : Cisco Unified Communications Manager* から電話機への *Web* 要求

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager • QRT • RTMT • [電話の検索と一覧表示（Find and List Phones）] ページ • [電話の設定（Phone Configuration）] ページ	電話	80/TCP	ハイパーテキスコル（HTTP）

電話機と Cisco Unified Communications Manager の間のシグナリング、メディア、およびその他の通信

表 *34 :* 電話機と *Cisco Unified Communications Manager* の間のシグナリング、メディア、およびその他の通信

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
電話	DNS サーバー	53 / TCP	Session Initiation Protocol（SIP）電話機が、ドメインネーム システム（DNS）を使用して、完全修飾ドメイン名（FQDN）を解決します。 （注） デフォルトでは、一部のワイヤレス アクセス ポイントは TCP の 53 番ポートをブロックし、FQDN を使用しながら CUCM を設定しているときに、ワイヤレス SIP 電話機が登録されないようにします。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
電話	Unified Communications Manager（TFTP）	69、次にエフェメラル / UDP	ファームウェアおよび設定ファイルのダウンロードに使用される Trivial File Transfer Protocol（TFTP）
電話	Unified Communications Manager	2000 / TCP	Skinny Client Control Protocol（SCCP）
電話	Unified Communications Manager	2443 / TCP	Secure Skinny Client Control Protocol（SCCPS）
電話	Unified Communications Manager	2445 / TCP	エンドポイントに信頼検証サービスを提供します。
電話	Unified Communications Manager（CAPF）	3804 / TCP	ローカルで有効な証明書（LSC）を IP 電話に発行するための認証局プロキシ機能（CAPF）リスニング ポート
電話	Unified Communications Manager	5060 / TCP および UDP	Session Initiation Protocol（SIP）電話機
Unified Communications Manager	電話		
電話	Unified Communications Manager	5061 TCP	Secure Session Initiation Protocol（SIPS）電話機
Unified Communications Manager	電話		
電話	Unified Communications Manager（TFTP）	6970 TCP	ファームウェアおよび設定ファイルの HTTP ベースのダウンロード
電話	Unified Communications Manager（TFTP）	6971、6972 / TCP	TFTP への HTTPS インターフェイス。電話機が、TFTP からセキュアな設定ファイルをダウンロードするためにこのポートを使用します。
電話	Unified Communications Manager	8080 / TCP	XML アプリケーション、認証、ディレクトリ、サービスなどの電話 URL。これらのポートをサービス単位で設定できます。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
電話	Unified Communications Manager	9443 / TCP	電話機が、認証された連絡先検索にこのポートを使用します。
電話	Unified Communications Manager	9444	電話は、このポート番号を使用してヘッドセット管理機能を利用します。
iPhone/iPad（Webex アプリ）	Unified Communications Manager	9560/セキュア WebSocket	Webex アプリは、LPNS 機能にこのポート番号を使用します。
IP VMS	電話	16384 ～ 32767 / UDP	Real-Time Protocol（RTP）、Secure Real-Time Protocol（SRTP） （注） 他のデバイスは全範囲を使用しますが、Cisco Unified Communications Manager は 24576 ～ 32767 だけを使用します。
電話	IP VMS		

ゲートウェイと Cisco Unified Communications Manager の間のシグナリング、メディア、およびその他の通信

表 *35 :* ゲートウェイと *Cisco Unified Communications Manager* の間のシグナリング、メディア、およびその他の通信

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
ゲートウェイ	Unified Communications Manager	47、50、51	Generic Routing E （GRE）、Encap Security Payload 証ヘッダー（AH のプロトコル番号 された IPSec トラ 伝送します。列見 ようなポートとか ありません。
Unified Communications Manager	ゲートウェイ		

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
ゲートウェイ	Unified Communications Manager	500 / UDP	IP Security（IPSec）ル確立のためのイン ト キー エクスチェ （IKE）
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager（TFTP）	69、次にエフェメラル/UDP	トリビアル ファイ ロトコル（TFTP）
Cisco Intercompany Media Engine（CIME）トランクを使用した Unified Communications Manager	CIME ASA	1024 ～ 65535 / TCP	ポート マッピング ス。CIME オフパス ルでのみ使用しま
Gatekeeper	Unified Communications Manager	1719 / UDP	ゲートキーパー（H RAS
ゲートウェイ	Unified Communications Manager	1720 / TCP	H.323 ゲートウェイ ラスタ間トランク けの H.225 シグナリ サービス
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	エフェメラル / TCP	ゲートキーパー制御 上の H.225 シグナリ サービス
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	エフェメラル / TCP	音声、ビデオ、およ を確立するための H ナリング サービス （注） ゲートウ 種類によ なる、リ システム される H ポート。 IOS ゲー イでの H ポート範 11000 ～ です。
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	2000 / TCP	Skinny Client Contro （SCCP）

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
ゲートウェイ	Unified Communications Manager	2001 / TCP	Cisco Unified Co Manager の導入 6608 ゲートウェ グレード ポート
ゲートウェイ	Unified Communications Manager	2002 / TCP	Cisco Unified Co Manager の導入 6624 ゲートウェ グレード ポート
ゲートウェイ	Unified Communications Manager	2427 / UDP	Media Gateway C Protocol（MGCP ウェイ コントロ
ゲートウェイ	Unified Communications Manager	2428 / TCP	Media Gateway C Protocol（MGCP ホール
--	--	4000 ～ 4005 / TCP	Cisco Unified Co Manager に音声、 よび D チャネル ないときには、 トがこのような ファントム Real Transport Protoco ポートおよび Re Transport Control （RTCP）ポート されます。
ゲートウェイ	Unified Communications Manager	5060 / TCP および UDP	Session Initiation （SIP）ゲートウ クラスタ間トラ
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	5061 / TCP	Secure Session In Protocol（SIPS） イおよびクラス （ICT）
Unified Communications Manager	ゲートウェイ		

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
ゲートウェイ	Unified Communications Manager	16384 ～ 32767 / UDP	Real-Time Protocol（ Secure Real-Time Pro （SRTP） （注） 他のデバ 全範囲を ますが、 Unified Commun Manager ～ 32767 使用しま
Unified Communications Manager	ゲートウェイ		

アプリケーションと Cisco Unified Communications Manager の間の通信

表 *36* : アプリケーションと *Cisco Unified Communications Manager* の間の通信

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
CTL クライアント	Unified Communications Manager CTL プロバイダ	2444 / TCP	Cisco Unified Commu Managerの証明書信 （CTL）プロバイダ ング サービス
Cisco Unified Communications アプリケーション	Unified Communications Manager	2748 / TCP	CTI アプリケーショ バー
Cisco Unified Communications アプリケーション	Unified Communications Manager	2749 / TCP	CTI アプリケーショ （JTAPI/TSP）と C Manager 間の TLS 接
Cisco Unified Communications アプリケーション	Unified Communications Manager	2789 / TCP	JTAPIアプリケーシ バー
Unified Communications Manager Assistant Console	Unified Communications Manager	2912 / TCP	Cisco Unified Commu Manager Assistant サ （以前の IPMA）
Unified Communications Manager Attendant Console	Unified Communications Manager	1103 ～ 1129 / TCP	Cisco Unified Commu Manager Attendant C （AC）JAVA RMI レ リ サーバー

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager Attendant Console	Unified Communications Manager	1101 / TCP	RMI サーバーは ルバック メッセ らのポートを使用 アントに送信し
Unified Communications Manager Attendant Console	Unified Communications Manager	1102 / TCP	Attendant Console サーバー バイン RMI サーバーは ポートに RMI メ 送信します。
Unified Communications Manager Attendant Console	Unified Communications Manager	3223 / UDP	Cisco Unified Co Manager Attendan （AC）サーバー ポートは、Atten サーバーから pi 録メッセージを Attendant Consol 回線状態を送信
Unified Communications Manager Attendant Console	Unified Communications Manager	3224 / UDP	Cisco Unified Co Manager Attendan （AC）クライア 線状態情報およ 態情報のために に登録されます
Unified Communications Manager Attendant Console	Unified Communications Manager	4321 / UDP	Cisco Unified Co Manager Attendan （AC）クライア コール制御のた バーに登録され
SAF/CCD を使用する Unified Communications Manager	SAF イメージを実行する IOS ルータ	5050 / TCP	EIGRP/SAF プロ 行するマルチサ ルータ。
Unified Communications Manager	Cisco Intercompany Media Engine（IME）サーバー	5620 / TCP このポートでは、ポート番号 5620 の使用を推奨しますが、CLI コマンドの add ime vapserver または set ime vapserver port を Cisco IME サーバーで実行することにより、値を変更できます。	VAP プロトコル Intercompany Me サーバーとの通信 ます。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Cisco Unified Communications アプリケーション	Unified Communications Manager	8443 / TCP	課金アプリケーショ テレフォニー管理ア ションなどのサード が、Cisco Unified Communications Mar タベースに対してプ で読み書きするため る AXL/SOAP API。

CTL クライアントとファイアウォールの通信

表 *37 : CTL* クライアントとファイアウォールの通信

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
CTL クライアント	TLS プロキシ サーバ	2444 / TCP	ASA ファイアウォ 明書信頼リスト（C バイダー リスニン ス

Cisco Smart Licensing Service と Cisco Smart Software Manager 間の通信

Unified Communications Manager の Cisco Smart Licensing Service は、Call Home を介して Cisco Smart Software Manager との直接通信を設定します。

***Table 38: Cisco Smart Licensing Service* と *Cisco Smart Software Manager* 間の通信**

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager（Cisco Smart Licensing Service）	Cisco Smart Software Manager（CSSM）	443 / HTTPS	Smart Licensing Service はライセンスの使用状況を CSSM に送信して、Unified CM が問題であるかどうかを確認します。

HP サーバ上の特殊なポート

表 *39 : HP* サーバ上の特殊なポート

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
エンドポイント	HP SIM	2301/TCP	HP エージェント ポート
エンドポイント	HP SIM	2381/TCP	HP エージェント ポート
エンドポイント	Compaq 管理エージェント	25375、25376、25393/UDP	COMPAQ 管理エ 拡張（cmaX）
エンドポイント	HP SIM	50000 ～ 50004/TCP	HP SIM への HT

ポート参照

ファイアウォール アプリケーション インスペクション ガイド

ASA シリーズ参考情報

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html

PIX アプリケーション Inspection Configuration Guides

http://www.cisco.com/c/en/us/support/security/pix-firewall-software/products-installation-and-configuration-guides-list.html

『FWSM 3.1 Application Inspection Configuration Guide』

http://www-author.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/inspct_f.html

IETF TCP/UDP ポート割り当てリスト

インターネット割り当て番号局（IANA）IETF 割り当てポート リスト

http://www.iana.org/assignments/port-numbers

IP テレフォニー設定とポート使用に関するガイド

『Cisco CRS 4.0 (IP IVR and IPCC Express) Port Utilization Guide』

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

『Port Utilization Guide for Cisco ICM/IPCC Enterprise and Hosted Editions』

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

Cisco Unified Communications Manager Express Security Guide to Best Practices

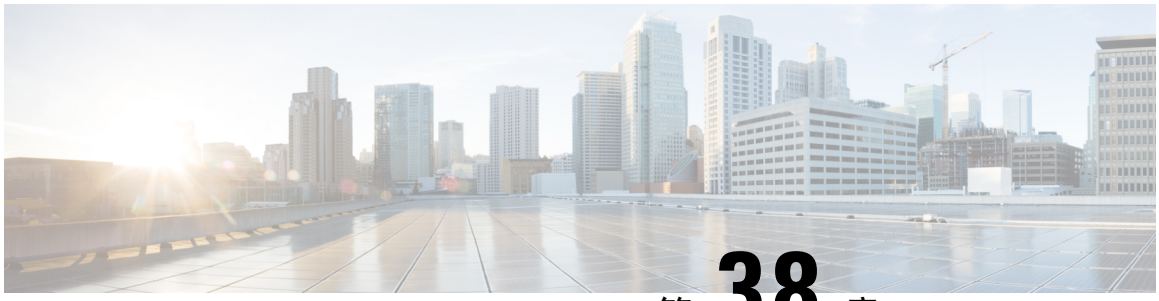
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

Cisco Unity Express Security Guide to Best Practices

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e31.html#wp41149

VMware ポート割り当てリスト

vCenter Server、ESX ホスト、およびその他のネットワーク コンポーネントの管理アクセス用の TCP ポートおよび UDP ポート



第 38 章

IM and Presence Service のポートの使用情報

IM and Presence Service ポート利用の概要

このマニュアルには、 IM and Presence Service が、クラスタ内接続用および、外部アプリケーションまたは外部デバイスとの通信用に使用する TCP および UDP ポートの一覧を示します。これは、IP Communications ソリューションの実装時に、ネットワークにファイアウォール、アクセス制御リスト（ACL）、および Quality of Service（QoS）を設定するうえで重要な情報となります。

（注） シスコでは、これらのポートで想定されるすべての設定シナリオを検証しているわけではありません。この一覧を参考にした結果、設定に問題が発生した場合は、シスコのテクニカルサポートにお問い合わせください。

事実上すべてのプロトコルが双方向で行われますが、このマニュアルではセッション開始側から見た方向を記載しています。デフォルトのポート番号は、管理者が手動で変更できる場合もありますが、ベスト プラクティスとしてこのような変更は推奨しません。IM and Presence Serviceは、内部使用に限定していくつかのポートを開くことに留意してください。

このドキュメントのポートは、IM and Presence サービスに特別に適用されます。リリースによってポートが異なる場合があり、今後のリリースで新しくポートが追加される可能性もあります。このため、参照しているマニュアルのバージョンが、インストールされている IM and Presence Service のバージョンと一致していることを確認してください。

ファイアウォール、ACL、または QoS の設定内容は、トポロジ、ネットワーク セキュリティ デバイスの配置に対するデバイスとサービスの配置、および使用するアプリケーションとテレフォニー拡張機能の種類に応じて異なります。また、デバイスやバージョンによって、ACL のフォーマットが異なることにも注意してください。

表に記載の情報

この表は、このマニュアルの表で確認できる情報を示します。

表 *40 :* 表の内容

表の項目	説明
From	ポートに要求を送信するクライアント
送信先	ポートで要求を受信するクライアント
ロール	クライアントまたはサーバのアプリケーションまたはプロセス
プロトコル	通信の確立と終了に使用されるセッション層プロトコル、またはトランザクションの要求と応答に使用されるアプリケーション層プロトコルのどちらか。
トランスポートプロトコル	コネクション型（TCP）またはコネクションレス型（UDP）のトランスポート層プロトコル
宛先/リスナー	要求の受信に使用されるポート
ソース/送信元	要求の送信に使用されるポート

IM and Presence サービス ポート リスト

次のテーブルは、IM and Presence サービスがクラスタ内とクラスタ間のトラフィックに使用するポートを示します。

表 *41 : IM and Presence* サービス ポート：*SIP* プロキシの要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
SIP ゲートウェイ --- IM and Presence	IM and Presence --- SIP ゲートウェイ	SIP	TCP/UDP	[5060]	エフェメラル	デフォルトの SIP プロキシの UDP および TCP リスナー
SIP ゲートウェイ	IM and Presence	SIP	TLS	5061	エフェメラル	TLS サーバー認証のリスナー ポート

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	IM and Presence	SIP	TLS	5062	エフェメラル	TLS 相互認証のリスナー ポート
IM and Presence	IM and Presence	SIP	UDP/TCP	5049	エフェメラル	内部ポート。ローカルホスト トラフィック専用。
IM and Presence	IM and Presence	HTTP	TCP	8081	エフェメラル	設定の変更を示す設定のエージェントからの HTTP 要求に使用されます。
サードパーティ製クライアント	IM and Presence	HTTP	TCP	8082	エフェメラル	デフォルトの IM and Presence HTTPのリスナー。サードパーティ製クライアントからの接続に使用されます。
サードパーティ製クライアント	IM and Presence	HTTPS	TLS/TCP	8083	エフェメラル	デフォルトの IM and Presence HTTPS リスナー。サードパーティ製クライアントからの接続に使用されます。

表 *42 : IM and Presence* サービス ポート：*Presence* エンジンの要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	IM and Presence（Presence エンジン）	SIP	UDP/TCP	5080	エフェメラル	デフォルトの SIP UDP/TCP リスナー ポート
IM and Presence（Presence エンジン）	IM and Presence（Presence エンジン）	Livebus	UDP	50000	エフェメラル	内部ポート。ローカルホスト トラフィック専用。LiveBus メッセージング ポート。IM and Presence サービスは、クラスタ通信に対してこのポートを使用します。

表 *43 : IM and Presence* サービス ポート：シスコの *Tomcat WebRequests*

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
ブラウザ	IM and Presence	HTTPS	TCP	8080	エフェメラル	ウェブアクセスに使用されます。
ブラウザ	IM and Presence	AXL/HTTPS	TLS/TCP	8443	エフェメラル	SOAP によりデータベースおよびサービスアビリティへのアクセスを提供します。
ブラウザ	IM and Presence	HTTPS	TLS/TCP	8443	エフェメラル	Web 管理へのアクセスを提供します。
ブラウザ	IM and Presence	HTTPS	TLS/TCP	8443	エフェメラル	ユーザー オプション ページへのアクセスを提供します。
ブラウザ	IM and Presence	SOAP	TLS/TCP	8443	エフェメラル	SOAP により Cisco Unified Personal Communicator、Cisco Unified Mobility Advantage、およびサードパーティ製の API クライアントへのアクセスを提供します。
ブラウザ	IM and Presence	HTTPS	TCP	9463	エフェメラル	Hypertext Transport Protocol over SSL（HTTPS）では、TLS1.3 の v6 のみが使用可能です。

表 *44 : IM and Presence* サービス ポート：外部社内ディレクトリ要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence --- 外部企業ディレクトリ	外部企業ディレクトリ --- IM and Presence	LDAP	TCP	389 / 3268	エフェメラル	ディレクトリプロトコルを外部企業ディレクトリと統合できるようにします。この LDAP ポートは、統合される社内ディレクトリによって異なります（デフォルトは 389）。Netscape Directory の場合は、別のポートで LDAP トラフィックを受信するよう設定できます。 認証用に IM&P と LDAP サーバー間の通信を LDAP に許可します。
IM and Presence	外部企業ディレクトリ	LDAPS	TCP	636	エフェメラル	ディレクトリプロトコルを外部企業ディレクトリと統合できるようにします。この LDAP ポートは、統合される社内ディレクトリによって異なります（デフォルトは 636）。

表 *45 : IM and Presence* サービス ポート：リクエストの設定

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（設定エージェント）	IM and Presence（設定エージェント）	TCP	[TCP]	8600	エフェメラル	設定エージェントのハートビート ポート

表 *46 : IM and Presence* サービス ポート：*Certificate Manager* の要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	証明書マネージャ	TCP	[TCP]	7070	エフェメラル	内部ポート。ローカルホストトラフィック専用。

表 *47 : IM and Presence* サービス ポート：*IDS*データベースの要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（データベース）	IM and Presence（データベース）	TCP	[TCP]	1500	エフェメラル	データベースクライアント用の内部 IDS ポート。ローカルホストトラフィック専用。
IM and Presence（データベース）	IM and Presence（データベース）	TCP	[TCP]	1501	エフェメラル	内部ポート：アップグレード中に IDS の 2 次インスタンスを始動するための代替ポートです。ローカルホストトラフィック専用。
IM and Presence（データベース）	IM and Presence（データベース）	XML	TCP	1515	エフェメラル	内部ポート。ローカルホストトラフィック専用。DB レプリケーション ポート。

表 *48 : IM and Presence Service* ポート：*IPSec* マネージャの要求

送信元 送信者	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（IPSec）	IM and Presence（IPSec）	専用	UDP/TCP	8500	8500	内部ポート：ipsec_mgr デーモンがプラットフォーム データ（ホスト）の証明書のクラスタレプリケーションに使用するクラスタ マネージャ ポートです。

表 *49 : IM and Presence* サービス ポート：*DRF*にマスター エージェント サーバー要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（DRF）	IM and Presence（DRF）	TCP	[TCP]	4040	エフェメラル	DRF Master Agent サーバー ポート。Local Agent、GUI、および CLI からの接続を受け入れます。

表 *50 : IM and Presence* サービス ポート：*RISDC* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（RIS）	IM and Presence（RIS）	TCP	[TCP]	2555	エフェメラル	Real-time Information Services（RIS）データベース サーバー。クラスタの 別の RISDC に接続し、クラスタ全体のリアルタイム情報を提供します。
IM and Presence（RTMT/AMC/SOAP）	IM and Presence（RIS）	TCP	[TCP]	2556	エフェメラル	Cisco RIS 向け Real-time Information Services（RIS）データベース クライアント。RIS クライアント接続で、リアルタイム情報を取得できるようにする
IM and Presence（RIS）	IM and Presence（RIS）	TCP	[TCP]	8889	8888	内部ポート。ローカル ホスト トラフィック専用。サービス ステータスの要求および応答用として、RISDC（システム アクセス）が TCP で servM にリンクするために使用します。

表 *51 : IM and Presence* サービス ポート：*SNMP* の要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
SNMP サーバー	IM and Presence	SNMP	UDP	161、8161	エフェメラル	SNMP ベースの管理アプリケーションにサービスを提供
IM and Presence	IM and Presence	SNMP	UDP	6162	エフェメラル	SNMP マスター エージェントから転送される要求を受信するネイティブ SNMP エージェント。
IM and Presence	IM and Presence	SNMP	UDP	6161	エフェメラル	ネイティブ SNMP エージェントからのトラップ情報を受信し、管理アプリケーションに転送する SNMP マスター エージェント。
SNMP サーバー	IM and Presence	TCP	[TCP]	7999	エフェメラル	CDP Agent が CDP バイナリと通信するためにソケットとして使用します。
IM and Presence	IM and Presence	TCP	[TCP]	7161	エフェメラル	SNMP マスターエージェントとサブエージェント間の通信に使用されます。
IM and Presence	SNMP トラップ モニター	SNMP	UDP	162	エフェメラル	SNMP トラップを管理アプリケーションに送信します。
IM and Presence	IM and Presence	SNMP	UDP	設定可能	61441	内部 SNMP トラップ レシーバ

表 *52 : IM and Presence* サービス ポート：*Racoon* サーバー要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
ゲートウェイ ---------- IM and Presence	IM and Presence ---------- ゲートウェイ	Ipsec	UDP	500	エフェメラル	Internet Security Association と KeyManagement Protocol を有効化

表 *53 : IM and Presence* サービス ポート：システム サービス要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（RIS）	IM and Presence（RIS）	XML	TCP	8888 および 8889	エフェメラル	内部ポート。ローカル ホスト トラフィック専用。RIS サービス マネージャ（servM）と通信するクライアントを受信するために使用します。

表 *54 : IM and Presence* サービス ポート：*DNS* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	DNS サーバー	DNS	UDP	53	エフェメラル	DNS サーバーが IM and Presence DNS 照会を受信するポート。 宛先:DNS サーバー|送信元:IM and Presence

表 *55 : IM and Presence* サービス ポート：*SSH/SFTP* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	エンドポイント	SSH/SFTP	TCP	22	エフェメラル	多くのアプリケーションが、サーバーへのコマンドラインアクセスを行うために使用します。ノード間で証明書などのファイル交換（sftp）にも使用されます。

表 *56 : IM and Presence* サービス ポート：*ICMP* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence ---------- Cisco Unified Communications Manager	Cisco Unified Communications Manager ---------- IM and Presence	ICMP	IP	N/A	エフェメラル	インターネット制御メッセージプロトコル（ICMP）。Cisco Unified Communications Manager サーバーとの通信に使用されます。

表 *57 : IM and Presence* サービス ポート：*NTP* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	NTP サーバー	NTP	UDP	123	エフェメラル	Cisco Unified Communications Manager は NTP サーバーとして動作します。サブスクライバノードが、パブリッシャノードと時刻を同期するために使用されます。

表 *58 : IM and Presence* サービス ポート：*Microsoft Exchange* 通知要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
Microsoft Exchange	IM and Presence	HTTP（HTTPu）	) WebDAV：HTTP /UDP/IP 通知 2) EWS - HTIP/TCP/IP SOAP 通知	IM and Presence サーバー ポート（デフォルト 50020）	エフェメラル	Microsoft Exchange は、このポートを使用してカレンダーイベントの特定のサブスクリプション識別子に対する変更を示す通知（NOTIFY メッセージによって示される）を送信します。ネットワーク構成内にある Exchange サーバーと統合する場合に使用されます。どちらのポートも作成されます。送信されるメッセージの種類は、設定するカレンダー プレゼンス バックエンドゲートウェイのタイプによって異なります。

表 *59 : IM and Presence* サービス ポート：*SOAP* サービス リクエスト

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（Tomcat）	IM and Presence（SOAP）	TCP	[TCP]	5007	エフェメラル	SOAP モニター ポート

表 *60 : IM and Presence* サービス ポート：*AMC RMI* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	RTMT	TCP	[TCP]	1090	エフェメラル	AMC RMI オブジェクト ポートRTMT パフォーマンス モニター、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。
IM and Presence	RTMT	TCP	[TCP]	1099	エフェメラル	AMC RMI レジストリ ポートRTMT パフォーマンス モニター、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。

表 *61 : IM and Presence* サービス ポート：*XCP* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
XMPP クライアント	IM and Presence	TCP	[TCP]	5222	エフェメラル	クライアント アクセス ポート
IM and Presence	IM and Presence	TCP	[TCP]	5269	エフェメラル	サーバー間接続（S2S）ポート
サードパーティ製 BOSH クライアント	IM and Presence	TCP	[TCP]	7335	エフェメラル	XCP Web Connection Manager が、BOSH を使用するサードパーティ製 API との接続に使用する HTTP リスニング ポート

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（XCP サービス）	IM and Presence（XCP ルータ	TCP	[TCP]	7400	エフェメラル	XCP ルータ マスター アクセス ポート。オープン ポート設定からルータに接続する XCP サービス（XCP 認証コンポーネント サービスなど）は、通常このポートを使用して接続します。
IM and Presence（XCP ルータ	IM and Presence（XCP ルータ	UDP	UDP	5353	エフェメラル	MDNS ポート。クラスタ内の XCP ルータはこのポートを使用してお互いを検出します。
IM and Presence（XCP ルータ	IM and Presence（XCP ルータ	TCP	[TCP]	7336	HTTPS	MFT ファイル転送（オンプレミスのみ）。

表 *62 : IM and Presence* サービスポート ― 外部データベースリクエスト

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	PostgreSQL データベース	TCP	[TCP]	5432 [1]	エフェメラル	PostgreSQL データベース リスニング ポート
IM and Presence	Oracle データベース	TCP	[TCP]	1521	エフェメラル	Oracle データベース リスニング ポート
IM and Presence	MSSQL データベース	TCP	[TCP]	1433	エフェメラル	MSSQL データベース リスニング ポート

[1] これがデフォルトのポートですが、任意のポートで受信するよう PostgreSQL データベースを設定できます。

表 *63 : IM and Presence* サービス ポート：高可用性の要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（Server Recovery Manager）	IM and Presence（Server Recovery Manager）	TCP	[TCP]	20075	エフェメラル	Cisco Server Recovery Manager が管理 RPC リクエストを行うために使用するポート。
IM and Presence（Server Recovery Manager）	IM and Presence（Server Recovery Manager）	UDP	UDP	21999	エフェメラル	Cisco Server Recovery Manager がピアとの通信に使用するポート。

表 *64 : IM and Presence* サービス ポート：*In Memory* データベース レプリケーションのメッセージ

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	IM and Presence	専用	TCP	6603*	エフェメラル	Cisco Presence Datastore
IM and Presence	IM and Presence	専用	TCP	6604*	エフェメラル	Cisco Login Datastore
IM and Presence	IM and Presence	専用	TCP	6605*	エフェメラル	Cisco SIP Registration Datastore
IM and Presence	IM and Presence	専用	TCP	9003	エフェメラル	Cisco Presence Datastore デュアル ノード プレゼンス冗長グループの複製。
IM and Presence	IM and Presence	専用	TCP	9004	エフェメラル	Cisco Login Datastore デュアル ノード プレゼンス冗長グループの複製。
IM and Presence	IM and Presence	専用	TCP	9005	エフェメラル	Cisco SIP Registration Datastore デュアル ノード プレゼンス冗長グループの複製。

* 管理 CLI 診断ユーティリティを実行するには、`utils imdb_replication status` コマンドを使用します。これらのポートは、クラスタの IM and Presence Service ノード間で設定されているすべてのファイアウォールでオープンである必要があります。このセットアップは、通常の運用では必要ありません。

表 *65 : IM and Presence* サービス ポート：*In Memory* データベース *SQL* メッセージ

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	IM and Presence	専用	TCP	6603	エフェメラル	Cisco Presence Datastore SQL クエリ。
IM and Presence	IM and Presence	専用	TCP	6604	エフェメラル	Cisco Login Datastore SQL クエリ。
IM and Presence	IM and Presence	専用	TCP	6605	エフェメラル	Cisco SIP Registration Datastore SQL クエリ。
IM and Presence	IM and Presence	専用	TCP	6606	エフェメラル	Cisco Route Datastore SQL クエリ。

表 *66 : IM and Presence* サービス ポート：*In Memory* データベースの通知メッセージ

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	IM and Presence	専用	TCP	6607	エフェメラル	Cisco Presence Datastore XML ベースの変更通知。
IM and Presence	IM and Presence	専用	TCP	6608	エフェメラル	Cisco Login Datastore XML ベースの変更通知。
IM and Presence	IM and Presence	専用	TCP	6609	エフェメラル	Cisco SIP Registration Datastore XML ベースの変更通知。
IM and Presence	IM and Presence	専用	TCP	6610	エフェメラル	Cisco Route Datastore XML ベースの変更通知。

表 *67 : IM and Presence Service* ポート *:* 強制手動同期*/X.509* 証明書更新要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（Intercluster Sync Agent）	IM and Presence（Intercluster Sync Agent）	TCP	[TCP]	37239	エフェメラル	Cisco Intercluster Sync Agent サービスは、このポートを使用してコマンドを処理するためのソケット接続を確立します。

表 *68 : IM and Presence* サービス ポート：*ICMP* 要求

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
エンドポイント/IM and Presence	IM and Presence	7	Internet Control Mess Protocol（ICMP）。トコル番号がエコーラフィックを伝送し見出しに示すようなるものではありま
IM and Presence	エンドポイント/IM and Presence		

表 *69 : IM and Presence* に使用するポート *- Cisco Unified CM* 通信および *IM and Presence Publisher - Subscriber* 通信

送信元（送信者）	送信先（リスナー）	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	1500	双方向	データベースクライアント用内部 ID ポート。ローカルホスト トラフィック専用。
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	8443	双方向	Web 管理へのアクセスを提供します。
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	1090	双方向	AMC RMI オブジェクト ポートRTMT パフォーマンス モニター、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。

送信元（送信者）	送信先（リスナー）	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	2555	双方向	双方向 Real-time Information Services（RIS）データベースサーバークラスタの 別の RISDC に接続し、クラスタ全体のリアルタイム情報を提供します。
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	8500	双方向	内部ポート ー プラットフォームデータ（ホスト）証明書のクラスタレプリケーションに対して ipsec_mgr デーモンが使用するクラスタ管理ポート。
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	8600	双方向	設定エージェントのハートビート ポート
Cisco Unified Communications Manager	IM and Presence Publisher	UDP	123	双方向	同期に使用する Network Time Protocol（NTP）。
IM and Presence Publisher	IM and Presence Subscriber	UDP	50000	双方向	内部ポート。ローカルホスト トラフィック専用。LiveBus メッセージング ポート。IM and Presence サービスは、クラスタ通信に対してこのポートを使用します。
IM and Presence Publisher	IM and Presence Subscriber	UDP	21999	双方向	Cisco Server Recovery Managerがピアとの通信に使用するポート。
IM and Presence Publisher	Cisco Unified Communications Manager	[TCP]	4040	双方向	DRF Master Agent サーバー ポート。Local Agent、GUI、および CLI からの接続を受け入れます。
IM and Presence Publisher	Cisco Unified Communications Manager	[TCP]	8001	双方向	常設チャットの構成中に使用されます。

送信元（送信者）	送信先（リスナー）	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence Publisher	Cisco Unified Communications Manager	[TCP]	6379	双方向	マネージド ファイル転送（MFT）の構成中に使用されます。
IM and Presence Publisher	IM and Presence Subscriber	[TCP]	7	双方向	外部データベース（MSSQL）の構成中に使用されます。
IM and Presence Publisher	IM and Presence Subscriber	[TCP]	20075	双方向	Cisco Server Recovery Manager が管理 RPC リクエストを行うために使用するポート。
IM and Presence Publisher	IM and Presence Subscriber	[TCP]	8600	双方向	設定エージェントのハートビート ポート
IM and Presence Subscriber	IM and Presence Publisher	[TCP]	9005	双方向	Cisco SIP Registration Datastore デュアル ノード プレゼンス冗長グループの複製。
IM and Presence Subscriber	IM and Presence Publisher	[TCP]	9003	双方向	Cisco Presence Datastore デュアル ノードプレゼンス冗長グループの複製。
IM and Presence Subscriber	IM and Presence Publisher	[TCP]	20075	双方向	Cisco Server Recovery Manager が管理 RPC リクエストを行うために使用するポート。
IM and Presence Subscriber	IM and Presence Publisher	[TCP]	9004	双方向	Cisco Login Datastoreデュアル ノードプレゼンス冗長グループの複製。
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	5070	双方向	コール構成で使用
IM and Presence Publisher	IM and Presence Subscriber	[TCP]	44000	双方向	コール構成で使用

表 *70 : On-a-call_Presence*

送信元（送信者）	送信先（リスナー）	送信元ポート	宛先ポート	プロトコル	備考
Cisco Unified Communications Manager	IM and Presence Publisher	[37240 – 61000]	5070	TCP	
IM and Presence Publisher	XMPP クライアント（Jabber）	5222	64846	[TCP]	クライアント アクセス ポート
IM and Presence Publisher	XMPP クライアント（Jabber）	5222	56361	[TCP]	クライアント アクセス ポート

表 *71 : MS-SQL DB* 構成

送信元（送信者）	送信先（リスナー）	送信元ポート	宛先ポート	プロトコル
IM and Presence Publisher	データベース	[37240 – 61000]	7	TCP

表 *72 : MS-SQL* 持続チャット構成

送信元（送信者）	送信先（リスナー）	送信元ポート	宛先ポート	プロトコル
IM and Presence Publisher	データベース	37240 – 61000	1433	[TCP]

表 *73 :* マネージド ファイル転送（*MFT*）構成

送信元（送信者）	送信先（リスナー）	送信元ポート	宛先ポート	プロトコル
IM and Presence Publisher	外部ファイルサーバ	37240 – 61000	7	TCP
IM and Presence Publisher	外部ファイルサーバ	37240 – 61000	22	TCP
IM and Presence Publisher	外部ファイルサーバ	37240 – 61000	5432	TCP
IM and Presence Publisher	データベース	54288 - 54292	5432	TCP

SNMP については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

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