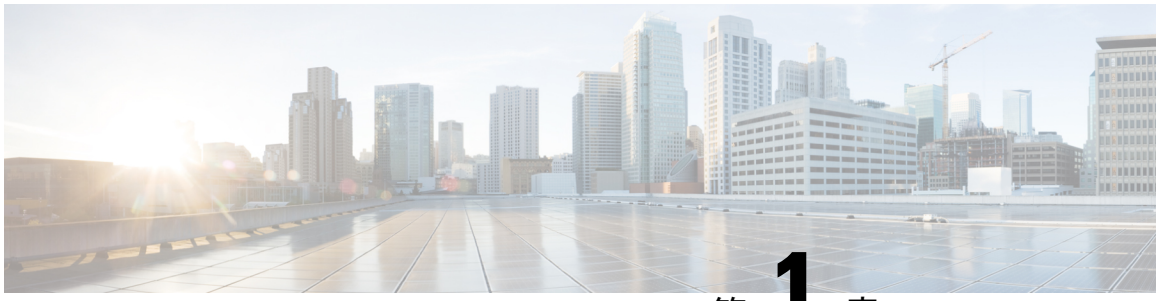
Cisco Unified Communications Manager リリース 12.0(1) システム設定ガイド

初版：2017 年 8 月 17 日

最終更新：2021 年 6 月 23 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。



第 1 章

システム設定の概要

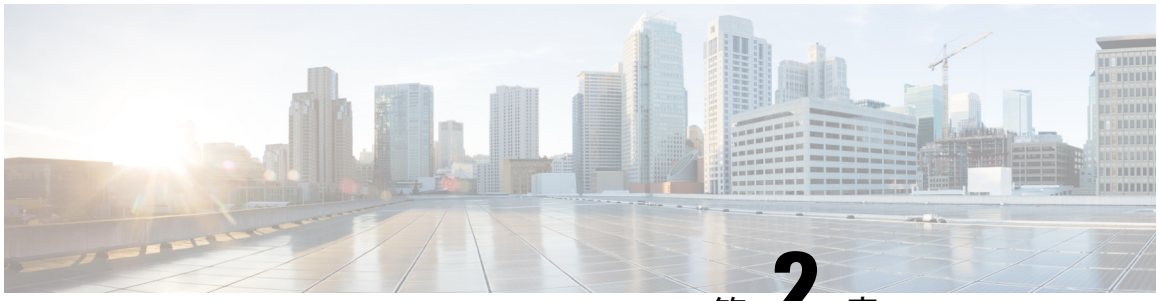
システム設定について

このドキュメントでは、コール制御システムの設定で実行する必要があるタスクに関する情報を提供しています。タスク フロー、手順、前提条件などの情報が含まれています。

システムの計画については、「http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html」を参照してください。

第 部

システムの初期パラメータの設定



第 2 章

初期システムパラメータ

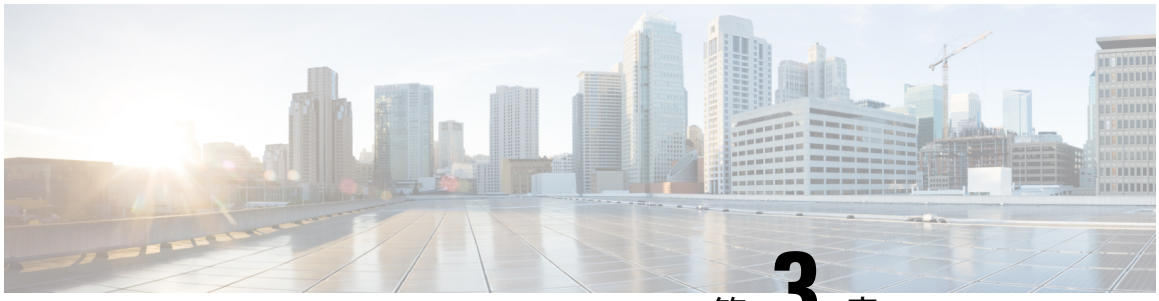
初期設定について

このセクションの各章では、コール制御システムの設定を開始する前に実行する必要がある初期セットアップタスクについて説明しています。

初期設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	スマート ソフトウェア ライセンシングのタスク フロー （11 ページ）	使用するシステムのライセンス要件を管理します。
ステップ 2	サーバの設定タスク フロー （21 ページ）	サーバ名やポートの設定など、サーバの基本的な情報を設定します。
ステップ 3	システムとエンタープライズの初期設定タスク フロー （28 ページ）	初めてノードを設定する際に必要なシステム全体のパラメータを設定します。
ステップ 4	サービス パラメータの設定タスク フロー （40 ページ）	初めてノードを設定する際に必要なサービスパラメータを設定します。
ステップ 5	デバイス プールのコア設定の設定タスク フロー （56 ページ）	サーバ グループ、タイム ゾーン情報、リージョン（コーデックの選択）などのコア システムを設定します。上記は基本設定であり、基本的なデバイスプールの基盤となります。



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。

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。

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。

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 アカウントのセットアップ詳細については、https://software.cisco.com/ を参照してください。

（省略可）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
ステップ 1	製品インスタンスの登録トークンの取得（11 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。
ステップ 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 （12 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。
ステップ 3	Cisco Smart Software Manager への登録（13 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。
  - [IPアドレス/ホスト名（IP Address/Host Name）]
  - [ポート（Port）]：HTTPS の場合、port 443 を使用します。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

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

ステップ 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。

ステップ 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、6 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
ステップ 1	認証を更新 （15 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を手動で更新するにはこの手順を実行 h 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。
ステップ 2	登録の更新 （16 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。

	コマンドまたはアクション	目的
		（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。
ステップ 3	登録解除 （17 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。
ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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、6 時間ごとに自動的に更新されます。フィールドとその設定オプションの詳細については、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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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、6 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 [OK] をクリックします。

ステップ 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、6 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、「Cisco Unified Communications Managerセキュリティ ガイド」（http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-maintenance-guides-list.html）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、「Tokenless CTL との CUCM 混合モード」（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-tech-notes-list.html）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 （11 ページ）。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 5 [OK] をクリックします。

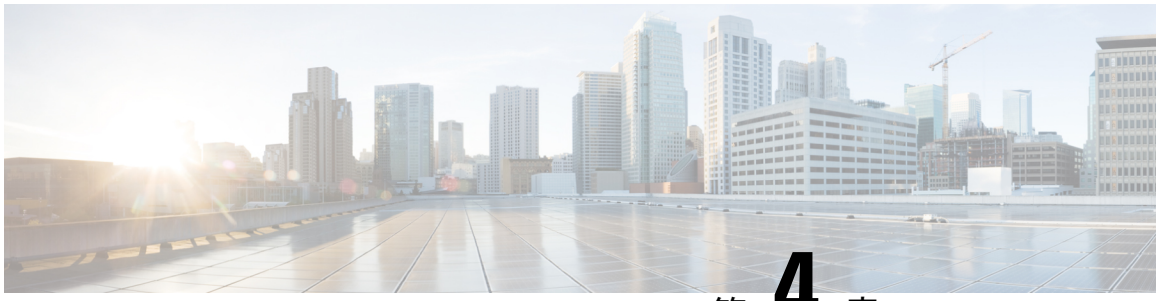
ステップ 6 [製品インスタンス登録トークン（Product Instance Registration Token）] セクションで、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトを使用して生成し、コピーまたは保存した「登録トークン キー」を貼り付けます。

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

ステップ 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。

ステップ 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、6 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。



第 4 章

サーバ情報の設定

システム情報の概要

この章では、Unified Communications Manager ノードのプロパティの設定方法を説明します。

（注） Unified Communications Manager、Cisco Unity Connection、Cisco IM and Presence などのすべての Unified Communications 製品で、インターフェイスは 1 つだけです。したがって、これらの製品ごとにIP アドレスを 1 つづつ割り当てることができます。

サーバの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	サーバ情報の設定 （22 ページ）	Unified Communications Manager ノードの名前を指定し、説明を追加します。
ステップ 2	ポートの設定 （22 ページ）	次のポートを設定します。 • [イーサネット電話ポート（Ethernet Phone Port）] • [MGCPリッスンポート（MGCP Listen Port）]

	コマンドまたはアクション	目的
		• [MGCPキープアライブ ポート（MGCP Keep-alive Port）] • [SIP電話ポート（SIP Phone Port）] • [SIP電話セキュアポート（SIP Phone Secure Port）]

サーバ情報の設定

Unified Communications Manager ノードの名前を指定し、説明を追加します。この手順で、次の読み取り専用情報を表示することもできます。

- コンピュータ テレフォニー インテグレーション ID（CTI ID）。
- Unified Communications Manager がインストールされるサーバです。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[システム（System）] > [Cisco Unified CM]** を選択します。
[Cisco Unified CM の検索と一覧表示（Find and List Cisco Unified CMs）] ウィンドウが表示されます。

ステップ 2 適切な検索条件を入力し、[検索（Find）] をクリックします。
一致するすべての Cisco Unified Communications Manager が表示されます。

ステップ 3 表示する Cisco Unified CM を選択します。
[Cisco Unified CM の設定（Cisco Unified CM Configuration）] ウィンドウが表示されます。

ステップ 4 [名前（Name）] フィールドで、この Cisco Unified Communications Manager に割り当てる名前を入力します。

ステップ 5 [説明（Description）] フィールドに、ノードの説明を入力します。

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。

ステップ 6 [保存（Save）] をクリックします。

ポートの設定

SCCPデバイス登録、SIPデバイス登録、MGCP ゲートウェイ接続などの接続に使用されるポートの設定を変更するには、この手順を使用します。

（注） 通常、デフォルトのポート設定を変更する必要はありません。この手順は、デフォルトを変更する場合にのみ使用します。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[システム（System）] > [Cisco Unified CM]** を選択します。
[Cisco Unified CM の検索と一覧表示（Find and List Cisco Unified CMs）] ウィンドウが表示されます。

ステップ 2 適切な検索条件を入力し、[検索（Find）] をクリックします。
一致するすべての Cisco Unified Communications Manager が表示されます。

ステップ 3 表示する Cisco Unified CM を選択します。
[Cisco Unified CM の設定（Cisco Unified CM Configuration）] ウィンドウが表示されます。

ステップ 4 [このサーバの Cisco Unified Communications Manager TCP ポートの設定（Cisco Unified Communications Manager TCP Port Settings for this Server）]セクションに移動します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [設定の適用（Apply Config）] をクリックします。

ステップ 7 [OK] をクリックします。

ポート設定

フィールド	説明
[イーサネット電話ポート（Ethernet Phone Port）]	システムは、この TCP ポートを使用してネットワークの Cisco Unified IP Phone（SCCP 専用）と通信します。 • このポートがシステムですでに使用中でない限り、デフォルトポートの値 2000 を受け入れます。2000 を選択すると、このポートは非セキュアとして識別されます。 • すべてのポートエントリが一意であることを確認してください。 • 有効なポート番号の範囲は 1024 ～ 49151 です。

フィールド	説明
[MGCPリッスンポート（MGCP Listen Port）]	システムは、TCPポートを使用して、その関連するMGCPゲートウェイからのメッセージを検出する。 • このポートがシステムですでに使用中でない限り、デフォルトポート 2427 を受け入れます。 • すべてのポートエントリが一意であることを確認してください。 • 有効なポート番号の範囲は 1024 ～ 49151 です。
[MGCPキープアライブポート（MGCP Keep-alive Port）]	システムは、このTCPポートを使用して、その関連するMGCPゲートウェイとアクティブメッセージを交換する。 • このポートがシステムですでに使用中でない限り、デフォルトポート 2428 を受け入れます。 • すべてのポートエントリが一意であることを確認してください。 • 有効なポート番号の範囲は 1024 ～ 49151 です。
[SIP電話ポート（SIP Phone Port）]	このフィールドでは、Unified Communications Manager が TCP と UDP を介して SIP 回線登録をリッスンするのに使用するポート番号を指定します。
[SIP電話セキュアポート（SIP Phone Secure Port）]	このフィールドでは、システムが TLS を介して SIP 回線登録をリッスンするのに使用するポート番号を指定します。
SIP 電話 OAuth ポート（SIP Phone OAuth Port）	このフィールドは、Cisco Unified Communications Manager が TLS（Transport Layer Security）を介して、オンプレミスの Jabber デバイスによる SIP 回線への登録をリッスンするために使用するポート番号を指定します。デフォルト値は 5090 です。範囲は 1024 ー 49151 です。
SIPモバイルおよびリモートアクセスOAuthポート	このフィールドでは、Cisco Unified Communications Manager が MTLS（Mutual Transport Layer Security）を介してExpressway 上の Jabber からの SIP 回線登録を受信するために使用するポート番号を指定します。デフォルト値は 5091 です。範囲は 1024 ー 49151 です。

ホスト名の設定

表 5-2 に、Unified Communications Manager サーバーのホスト名を設定できるロケーション、ホスト名に使用できる文字数、ホスト名に推奨される最初の文字と最後の文字を示します。ホスト名が正しく設定されていないと、通信マネージャの一部のコンポーネント（オペレーティングシステム、データベース、インストールなど）が正常に動作しない可能性があります。

注意 表5-2にリストされたロケーションのホスト名またはIPアドレスを変更する前に、「Unified Communications Manager 8.5(1) の IP アドレスおよびホスト名の変更」を参照してください。設定後のホスト名や IP アドレスを正しく更新しないと、Unified Communications Manager に問題が発生することがあります。

表 *1 : Cisco Unified Communications Manager* におけるホスト名の設定

ホスト名の場所	可能な設定	指定できる文字数	推奨されるホスト名の先頭文字	推奨されるホスト名の最終文字
[ホスト名/IP アドレス（Host Name/IP Address）] フィールド Cisco Unified Communications Manager Administration の **[システム（System）]** > **[サーバ（Server）]**	サーバのホスト名を追加または変更できます。	2 ～ 63	英字	英数字
[ホスト名（Hostname）] フィールド Cisco Unified Communications Manager のインストール時	クラスタ内のサーバのホスト名を追加できます。	1 ～ 63	英字	英数字
[ホスト名（Hostname）] フィールド Cisco Unified Communications オペレーティングシステムの **[設定（Settings）]** > **[IP]** > **[イーサネット（Ethernet）]**	サーバーのホスト名ではなく変更できます。	1 ～ 63	英字	英数字

ホスト名の場所	可能な設定	指定できる文字数	推奨されるホスト名の先頭文字	推奨されるホスト名の最終文字
set network hostname ホスト名 コマンドラインインターフェイス	サーバーのホスト名ではなく変更できます。	1 ～ 63	英字	英数字

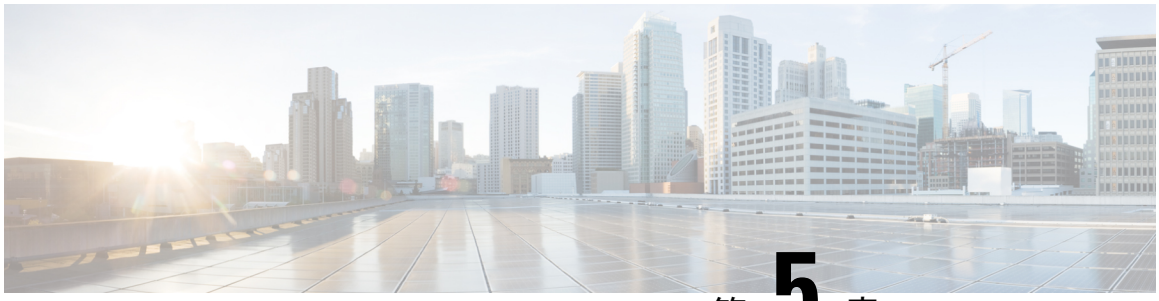
ヒント　このホスト名は、ARPANETホスト名の規則に従う必要があります。ホスト名の先頭文字と最終文字の間には、英数文字とハイフンを入力できます。

表 5-2 のいずれかのロケーションでホスト名を設定する前に、次の情報を確認してください。

- [サーバの設定（Server Configuration）] ウィンドウの [ホスト名/IP アドレス（Host Name/IP Address）] フィールドは、デバイスとサーバ間、アプリケーションとサーバ間、および異なるサーバ間の通信をサポートします。このフィールドには、ドット区切り形式の IPv4 アドレスまたはホスト名を入力できます。

  このフィールドでは、Unified Communications Manager が DNS サーバにアクセスしてホスト名をIPアドレスに解決できる場合は、ホスト名のみを設定します。Unified Communications Manager の名前とアドレス情報は、必ず DNS サーバで設定してください。

ヒント　DNS サーバで Unified Communications Manager 情報を設定するのに加えて、Unified Communications Manager のインストール中に DNS 情報を入力することもできます。



第 5 章

システム パラメータとエンタープライズ パラメータの設定

システムおよびエンタープライズパラメータの初期パラメータの概要

Unified Communications Manager ノードを初めてセットアップする場合は、次のシステム全体のパラメータを検討してください。必要に応じて、導入におけるシステム全体のパラメータを変更できますが、ほとんどの場合、推奨されるデフォルト設定で動作します。

- 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。
- （省略可）クラスタが MLPP を使用している場合は、Multilevel Precedence and Preemption（MLPP）を有効にします。
- （省略可）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。
- （省略可）リモート syslog サーバ名前を入力します。
- （省略可）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。
- （省略可）依存関係レコードを有効にします。

システムとエンタープライズの初期設定タスク フロー

始める前に

Unified Communications Manager のノードとポートの設定を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	システムおよびエンタープライズのパラメータ設定 （28 ページ）	Unified Communications Manager 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。推奨されるシステム設定のリストについては、「よくある企業パラメータ （30 ページ）」を参照してください。
ステップ 2	iOS Cisco Jabber の SSO ログインの動作設定 （36 ページ）	制御されたモバイル デバイス管理（MDM）の環境で IdP による証明書ベースの認証を Cisco Jabber で実行するために必要なエンタープライズ パラメータを設定します。
ステップ 3	RTMT への SSO の設定 （37 ページ）	Real-Time Monitoring Tool（RTMT）用に SAML SSO を有効化するには、Unified Communications Manager を使用してエンタープライズパラメータを設定します。

次のタスク

Unified Communications Manager クラスタで設定されているすべてのデバイスに適用する共通設定の基盤とする、デバイス プールの一部のコア設定を構成します。「デバイス プールのコア設定の設定タスク フロー （56 ページ）」を参照してください。

システムおよびエンタープライズのパラメータ設定

Cisco Unified Communication Manager 管理を使用して、特定の展開のシステムパラメータとエンタープライズパラメータを設定することができます。最初のシステム設定にとって重要なパラメータがリストされていますが、ほとんどの導入では推奨されるデフォルト設定が有効になっています。

コール トレース ログの有効化など、トラブルシューティングに役立つパラメータは、ネットワークのパフォーマンスに影響があるため、問題が解決した後は無効にする必要があります。

ほとんどのパラメータは、変更を有効にするためにすべてのデバイスをリセットする必要があります。すべての設定手順を完了してから、すべてのデバイスをリセットしてください。すべてのデバイスをリセットするのは、稼働率の低い時間帯に実行することを推奨します。

（注） リリース 10.0(1) から、Unified Communications Manager と IM and Presence Service で同じエンタープライズ パラメータが使用されます。IM and Presence Service のエンタープライズ パラメータの値を変更すると、変更された値が Unified Communications Manager に対して自動的に更新されます。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[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。

ステップ 2 クラスタの IP 電話が、TCP 接続が使用可能になったときに、プライマリ ノードに戻るまでの時間を、[エンタープライズ パラメータの設定（Enterprise Parameters Configuration）] セクションの [接続モニター間隔（Connection Monitor Duration）] フィールドに秒数を入力してから、[保存（Save）] をクリックします。デフォルト値は 120 秒です。

ヒント すべてのデバイスをリセットしないで、クラスタ内の影響を受けるデバイスに変更を適用するには、[設定の適用（Apply Config）] をクリックしてからし、[OK（OK）] をクリックします。

ステップ 3 [ユーザー データ サービス パラメータ（User Data Service Parameters）] セクションの [ユーザー検索をすべて有効にする（Enable All User Search）] セクションで、[True（True）] を選択して、姓、名、または電話番号が指定されていないときに、すべてのユーザーを組織内名簿で検索することを許可します。

ステップ 4 [クラスタ全体のドメイン設定（Clusterwide Domain Configuration）] セクションで、クラスタ全体のドメインをセットアップします。

a) [組織の最上位ドメイン（Organization Top Level Domain）] フィールドで組織の最上位ドメインを入力します。最大長は 255 文字です。

b) [クラスタの完全修飾ドメイン名（Cluster Fully Qualified Domain Name）] フィールドに、クラスタの完全修飾ドメイン名（FQDN）を入力します。最大長は 255 文字です。

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。

ステップ 5 Cisco Jabber セクションで、[ビデオ通話を開始しない] フィールドで [False] を選択します。

ステップ 6 （任意）[**Mlpp および機密にアクセスレベルパラメータ** (mlpp)] セクションで、マルチレベルの優先順位と [プリエンプトアクセスレベルパラメータ (mlpp)] を入力し、デバイスが mlpp を使用できるようにします。

a) Mlpp サービスのドメインを**Mlpp ドメイン識別子**フィールドに入力します。このパラメータには 16 進値（0x で始まる値）を指定できます。

b) Mlpp **表示ステータス**フィールドで [mlpp インジケータをオンにする (on)] を選択します。

ステップ 7 （任意） **[Ipv6**] セクションで、[**ipv6 の**有効化 (**Enable ipv6)] フィールドを True に設定します**。

ステップ 8 （任意） [**Cisco syslog Agent**] セクションで、リモート syslog サーバーの名前または IP アドレスを [**リモート syslog サーバー名 1**] フィールドに入力します。サーバー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。

ステップ 9 （任意）[セッション**トレース**用のコールトレースログの設定]セクションで、コールトレースログを設定して、セッショントレースの SIP コール情報を収集できるようにします。

Real-Time Monitoring Tool（RTMT）のセッション トレース機能は、トラブルシューティングに役立つコール フロー図を生成するためにこの情報を使用します。

a) [コール**トレースログの有効化** (Enable **Call Trace Log)] フィールドを [True] に設定します**。

b) [コールトレースログファイルの最大数] フィールドで、Unified Communication Manager が生成できる SIP コールトレースログファイルの最大数を入力します。

デフォルト値は 2000 です。有効範囲は 5 ~ 4000 です。

c) 呼追跡ログフィールドには、SIP呼追跡ログファイルの最大ファイルサイズ**メガバイト**を入力します。

デフォルト値は 2 です。有効な範囲は 1 ～ 10 です。

（注） SIP コール トラフィック量が多い期間は、ある程度のパフォーマンスの低下が生じることがあります。システム パフォーマンスの影響を低減するには、[セッション トレースのコール関連の REFER/NOTIFY/SUBSCRIBE SIP メッセージをログに記録する（Log Call-Related REFER/NOTIFY/SUBSCRIBE SIP Messages for Session Trace）] という Cisco CallManager サービス パラメータを [False] に設定します。これによって、SIP コール トレースから REFER、NOTIFY、および SUBSCRIBE メッセージが除外されます。

ステップ 10 **Ccmadmin**パラメータセクションので、[依存関係**の有効化 (Enable Records**)] フィールドで [True] を選択します。

ステップ 11 [保存（Save）] をクリックします。

ステップ 12 [**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。すべてのデバイスをリセットするのは、稼働率の低い時間帯に実行することを推奨します。

ヒント すべてのデバイスをリセットするには、システム内の全デバイスプールをリセットします。

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場合があります。 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ります。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

パラメータ名	説明
クラスタ全体のドメイン設定	
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。 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。

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。

iOS Cisco Jabber の SSO ログインの動作設定

手順

ステップ 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。

ステップ 2 オプトイン制御を設定するには、[SSOの設定（SSO Configuration）] セクションで、[iOS向けSSOログイン動作（SSO Login Behavior for iOS）] パラメータで、[ネイティブブラウザの使用（Use Native Browser）] オプションを選択します。

（注） [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にすると、Cisco Jabber は SSO の認証に、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。このオプションは、デフォルトで有効です。
- [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にすると、Cisco Jabber は、iOS デバイスで Apple Safari フレームワークを使用し、MDM の導入で、ID プロバイダー（IdP）を利用する証明書ベースの認証を実行します。

  （注） ネイティブブラウザの使用は組み込みブラウザの使用ほど安全ではないため、制御された MDM の導入での利用を除いては、このオプションの設定を推奨しません。

ステップ 3 [保存（Save）] をクリックします。

RTMT への SSO の設定

手順

ステップ 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。

ステップ 2 RTMT に SSO を設定するには、[SSOの設定（SSO Configuration）] セクションで、[RTMTでのSSOの使用（Use SSO for RTMT）] パラメータに **True** を選択します。

（注） [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。

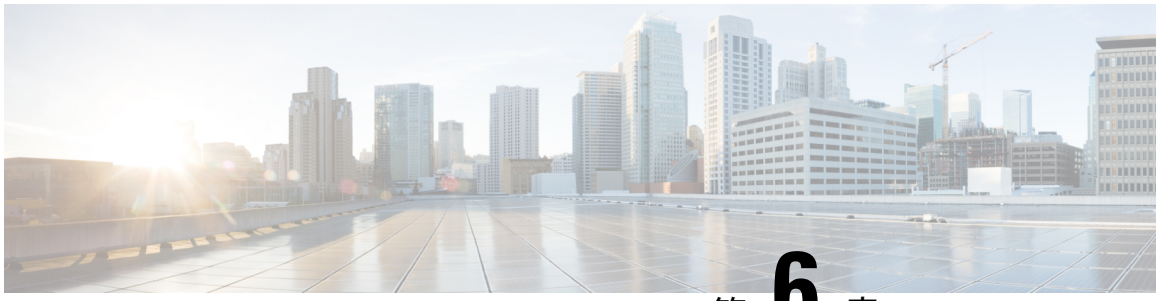
- [True]：このオプションを選択すると、RTMT は、SAML SSO ベースの IdP ログイン ウィンドウを表示します。

  （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。

ステップ 3 [保存（Save）] をクリックします。



第 6 章

サービス パラメータの設定

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。

サービス パラメータの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	基本サービスのアクティブ化 （40 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および非アクティブ化できます。パブリッシャ ノードの推奨サービス リストについては、パブリッシャ ノードに推奨するサービス （41 ページ）を参照してください。サブスクライバ ノードの推奨サービス リストについては、サブスクライバーノード用の推奨サービス （42 ページ）を参照してください。
ステップ 2	サービス パラメータの設定 （43 ページ）	Cisco Unified Communications Manager パブリッシャ ノードとクラスタ内のサブスクライバ ノードのサービス パラメータを設定します。
ステップ 3	クラスタ全体のサービス パラメータ設定の表示 （44 ページ）	Cisco Unified Communications Manager Administration および Cisco Unified Serviceability を使用するノードのサービスを表示できます。サービス パラメータ設定およびパラメータの説明を表示するには、Cisco Unified Communications Manager Administration を使用します。

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 （41 ページ）
- サブスクライバーノード用の推奨サービス （42 ページ）

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

タイプ	サービス名
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
	シスコソープ-顧客ニーズサービス
	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
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 （40 ページ）」を参照してください。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

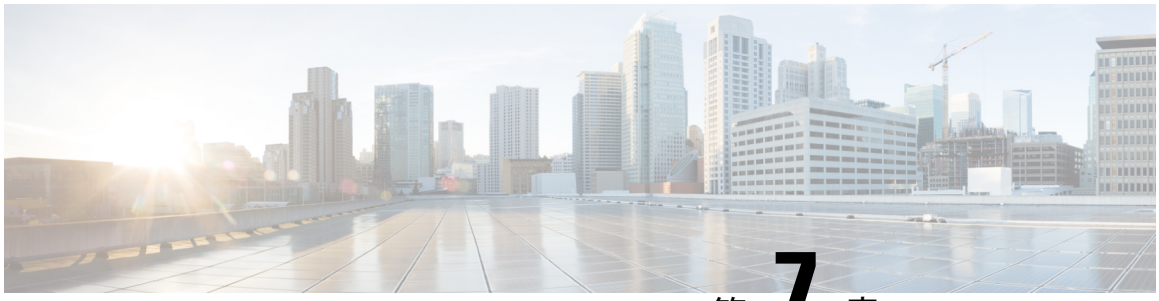
ステップ 2 クラスタ内の全ノードに関する特定のサービスのサービス パラメータを表示するには、[サービス パラメータ設定（Service Parameter Configuration）] ウィンドウの [関連リンク（Related

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。

ステップ 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 7 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。このオプションを選択した場合は、ネットワーク内のデバイスが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。この機能はリリース 11.5(1)SU3 でサポートされています。

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。

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。
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。

オーディオ コーデック	説明
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。
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。

オーディオ コーデック	説明
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。

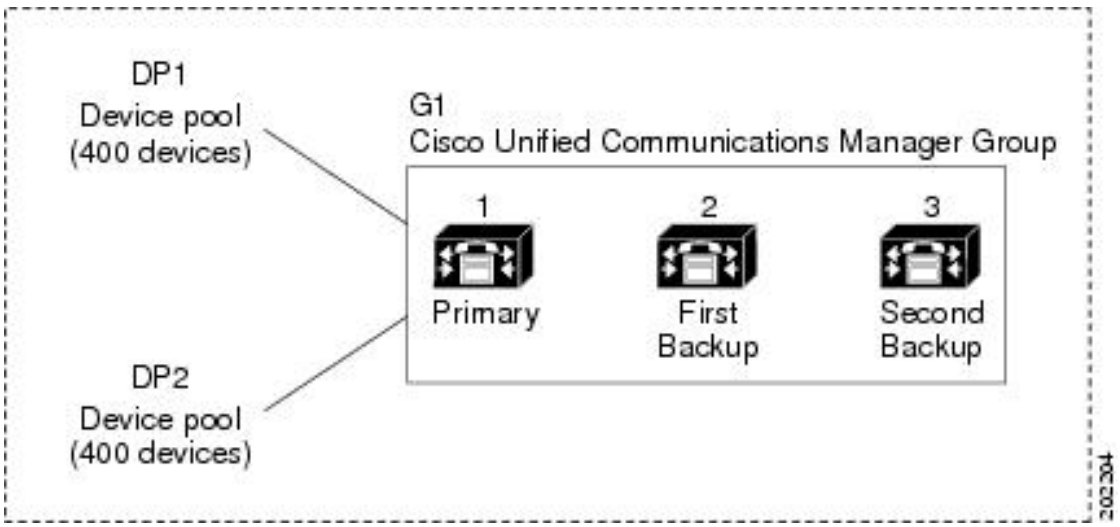
プライマリの Unified Communications Manager で何らかの理由で障害が発生した場合、グループの 1 番目のバックアップ Unified Communications Manager が、プライマリ Unified Communications Manager に登録されたデバイスを制御します。グループに 2 番目のバックアップ Unified Communications Manager を指定する場合、プライマリと 1 番目のバックアップ両方の Unified Communications Manager で障害が発生した場合には、2 番目がデバイスを制御します。

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 *1 : 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。

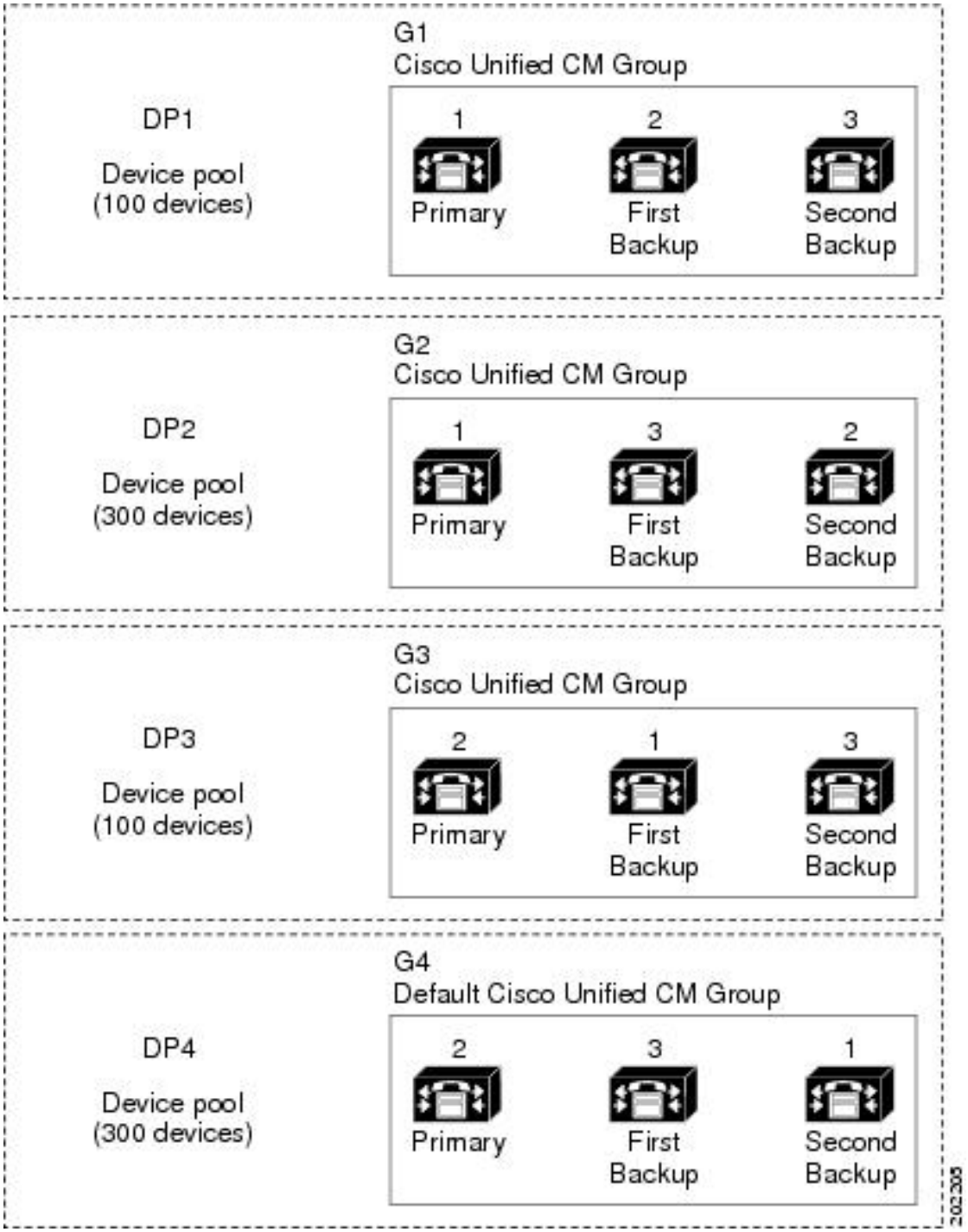
（注） 空の Unified Communications Manager グループは機能しません。

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 *2:* 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、『*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』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html）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。メディアリソースの設定の詳細については、このマニュアルの「メディアリソースの設定"の"」を参照してください。メディアリソース構成タスクフロー （580 ページ）を参照してください。
- Survivable リモートサイトテレフォニー (SRST): 導入環境で WAN 接続を使用している場合は、SRST を設定することによって、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。Survivable Remote Site Telephony の設定タスク フロー （128 ページ）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については、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 （152 ページ）。

- 装置の移動度ー装置の移動度グループを構成し、装置がその物理的位置に応じて設定できるようにする。詳細については、シスコ統一通信マネージャ機能構成ガイドの「装置移動度の設定」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
ステップ 1	Network Time Protocol の設定 （56 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。
ステップ 2	リージョンの関係の設定 （62 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。
ステップ 3	Cisco Unified CM グループの設定 （63 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。
ステップ 4	デバイス プールの設定 （64 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
ステップ 1	NTP サーバの追加 （57 ページ）	（省略可）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。
ステップ 2	対称キー経由での NTP 認証キーの設定（58 ページ）	（省略可）システムのセキュリティをさらに強化するためには、対称キーを使用して認証済み NTP を設定します。
ステップ 3	電話用 NTP リファレンスの設定 （58 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。
ステップ 4	日時グループの追加 （59 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

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 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。

ステップ 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。

ステップ 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。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （59 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

ステップ 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。

ステップ 2　[新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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
ステップ 1	音声コーデック設定のカスタマイズ（61 ページ）	（省略可）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

	コマンドまたはアクション	目的
		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。
ステップ 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 （62 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。
ステップ 3	リージョンの関係の設定 （62 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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [説明（Description）] を編集します。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （128 ページ）」を参照してください。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

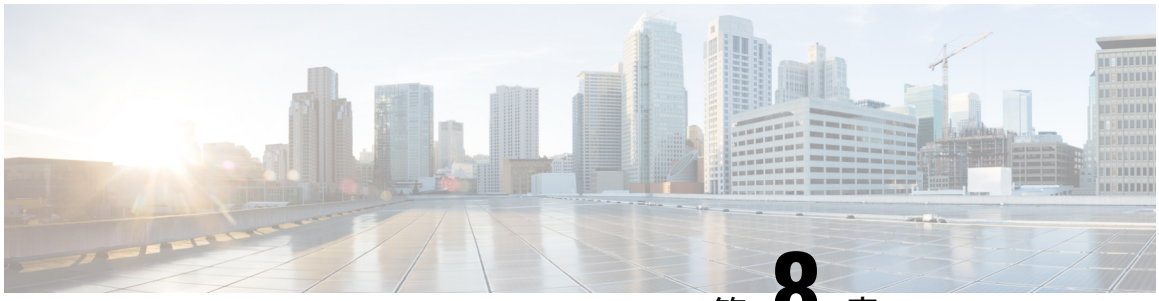
表 *6:* コール保持のシナリオ

シナリオ	コール保持の処理
Unified Communications Manager で障害が発生した場合。	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。 Unified Communications Manager は、エンドユーザ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。
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 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。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。 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。Unified Communications Manager は、エンドユーザ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 Unified CM 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。

シナリオ	コール保持の処理
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 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。 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、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 II 部

発着信コールの有効化



第 8 章

発着信コールの概要

インバウンドおよびアウトバウンドコールの概要

このパートでは、システムの着信コールと発信コールの設定方法について説明します。

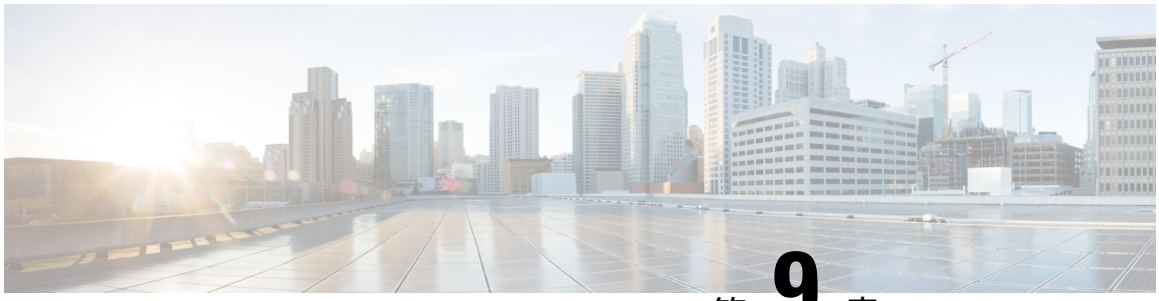
着信コールと発信コールの情報

次のタスク フローを実行すると、システムの応用的なコール処理を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	ゲートウェイの設定タスク フロー （79 ページ）	システムにゲートウェイを追加します。
ステップ 2	SIP の正規化および透過性の設定タスク フロー （97 ページ）	（省略可）Sip トランクまたは SIP デバイスに割り当てて、sip の相互運用性に関する問題を解決するための SIP 正規化および透過スクリプトを設定できます。
ステップ 3	SDP 透過性プロファイルの設定 （102 ページ）	（省略可）SIP 展開で、Unified Communications Manager によってネイティブにサポートされていない SDP 属性のサポートが必要な場合は、サポートされていない属性を含む SDP 透過性プロファイルを設定します。
ステップ 4	SIP プロファイルの概要 （105 ページ）	Sip トランクと SIP デバイス用の SIP プロファイルを設定します。

	コマンドまたはアクション	目的
ステップ 5	IPv6 の設定タスク フロー （108 ページ）	（省略可）SIP 導入で IPv6 デバイスのサポートが必要な場合は、システム内でデュアルスタック IPv6 サポートを設定します。デュアルスタックは、SIP 展開に対してのみ設定できます。
ステップ 6	SIP トランクの設定タスク フロー （117 ページ）	システムの SIP トランクを設定します。
ステップ 7	H.323 トランクの概要 （123 ページ）	システムのトランクを設定します。
ステップ 8	Survivable Remote Site Telephony の設定タスク フロー （128 ページ）	SRST を使用するようにシステムを設定します。



第 9 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。

ポートおよびトランクの接続タイプ

以下は、ゲートウェイ上で設定可能なポート接続の主なタイプです。

- 外部交換 ステーション (FXS): アナログ電話、スピーカーフォン、従来のボイスメールシステムなどのアナログ放送に接続するための FXS ポート。
- 異種交換オフィス (FXO): FXO ポートは、PSTN または従来の PBX へのアナログ接続を提供します。
- T1チャンネルシグナリング (T1/E1 CAS): t1/e1 cas 接続は、中央オフィス、PBX、またはその他のアナログデバイスへのデジタルトランク接続を提供します。
- [プライマリレートインターフェイス (T1/E1 PRI)]: デジタルアクセス PRI の接続は、社内の通信で広く使用されています。T1 PRIは、北米と日本で広く使用されており、1.544 Mb/s の割合で共通のチャネル信号を提供する音声とデータ用に 23 の B チャンネルを提供しています。E 1はヨーロッパで広く使用され、30の音声とデータチャネル、1つの通常のシグナリングチャネルと1つのフレームチャネルを提供します。E1 PRIが使用する速度は2.048 Mb/s です。
- 小規模オフィスと家庭の通信リンクに使用される基本速度インターフェイス（BRI）は、音声とデータ用に 2 つの B チャネルと、シグナリング用に 1 つの D チャネルを提供します。

接続プロトコル

次の接続タイプが用意されています。

- TI/E1 PRI デジタルアクセス
- T1 CAS
- BRI
- FXO
- FXS

SCCP ゲートウェイには、次の接続タイプが用意されています。

- FXS
- BRI

SIP ゲートウェイには、次の接続が用意されています。

- FXS
- FXS-DID

- E&M
- BRI
- BRI QSIG
- T1 CAS
- T1 FGD
- E1 CAS
- T1/E1 PRI
- T1/E1 QSIG
- T 1/E 1 NFAS
- T1/E1 PRI (メガコムISDN)
- Centralized Automatic Message Accounting（CAMA）
- J1

H: 323 ゲートウェイには、次の接続タイプが用意されています。

- FXS
- FXS-DID
- E&M
- BRI
- BRI QSIG
- T1 CAS
- T1 FGD
- E1 CAS
- T1/E1 PRI
- T1/E1 QSIG
- T 1/E 1 NFAS
- T1/E1 PRI (メガコムISDN)
- Centralized Automatic Message Accounting（CAMA）
- J1

音声ゲートウェイのセットアップ要件

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

次のタスクを実行して、ネットワークゲートウェイを Unified Communication Manager に追加します。

始める前に

音声ゲートウェイのセットアップ要件 （78 ページ）を確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Unified Communications Manager でゲートウェイを設定します。次のいずれかの手順を、導入するプロトコルに応じて実行します。 • MGCPゲートウェイの設定 （80 ページ） • SCCP ゲートウェイの設定 （89 ページ） • SIP ゲートウェイの設定 （90 ページ） • H.323 ゲートウェイの設定 （92 ページ）	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。 SCCP ゲートウェイは、アナログアクセスまたは ISDN BRI 接続にのみ接続できます。
ステップ 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 （93 ページ）	（省略可）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。 （注） 個々のゲートウェイポートインターフェイスのポート設定のコール分類設定は、[clusterwide setting] を無効にします。ただし、デフォルトでは、[ゲートウェイポート (clusterwide service)] パラメータの設定を使用して設定されています。
ステップ 3	オフネット ゲートウェイ転送のブロック （94 ページ）	（省略可）1 つの外部 (OffNet) ゲートウェイから別の外部ゲートウェイへのコールを Unified Communication Manager

	コマンドまたはアクション	目的
		が転送できないようにするには、[ブロックオフライン転送 (Block on Net to offnet Transfer service)] パラメータを設定します。デフォルトでは、このサービス パラメータは、外部（OffNet）ゲートウェイから別のゲートウェイへの転送を許可するように設定されています。

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

音声ゲートウェイのセットアップ要件 （78 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	MGCP（IOS）ゲートウェイの設定 （81 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。
ステップ 2	ゲートウェイ ポートのインターフェイスを設定します。設定するインターフェイスのタイプによって、次の任意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 （86 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 （84 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のポート接続を設定します。ほとんどの VIC には複数のポート接続とオプションがあります。したがって、いくつか別のポートのインターフェイス タイプを設定する必要がある場合があります。

	コマンドまたはアクション	目的
	• FXS ポートの設定 （82 ページ） • FXO ポートの設定 （83 ページ） • BRI ポートの設定 （87 ページ）	ヒント ポートのインターフェイスを設定後、[関連リンク（Related Links）] ドロップダウン リスト ボックスで、[ゲートウェイの設定（Gateway Configuration）] ウィンドウに戻るために [MGCP 設定に戻る（Back to MGCP Configuration）] オプションを選択します。ここで、別のポート インターフェイスを選択して設定します。
ステップ 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 （85 ページ）	（省略可）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。
ステップ 4	ゲートウェイのリセット （88 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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 7 [保存（Save）] をクリックします。

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

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 8 [保存（Save）] をクリックします。

ステップ 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 （88 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 （81 ページ）

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 8 [保存（Save）] をクリックします。

ステップ 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 （88 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 （81 ページ）

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （85 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 （84 ページ）

手順

ステップ 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。

ステップ 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。

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 8 [保存（Save）] をクリックします。

ステップ 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（88ページ）」を参照してください。

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（81 ページ）

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 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 （88 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 （81 ページ）

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 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 （88 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

ステップ 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。

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

ステップ 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。

ステップ 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

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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

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
ステップ 1	SIP プロファイルの設定 （90 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。
ステップ 2	SIP トランク セキュリティ プロファイルの設定 （91 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。
ステップ 3	SIP ゲートウェイ向け SIP トランクの設定 （91 ページ）	SIP ゲートウェイを指すようにすべての SIP トランクを設定する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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 [保存（Save）] をクリックします。

SIP トランク セキュリティ プロファイルの設定

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 7 [保存（Save）] をクリックします。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

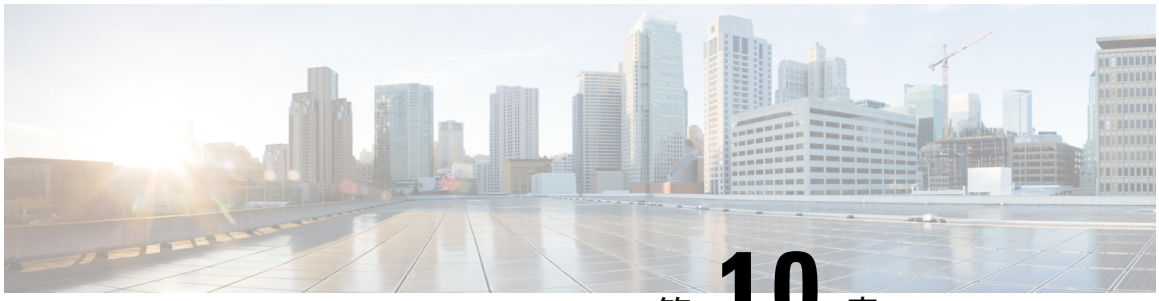
ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。

ステップ 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。

ステップ 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 10 章

SIP の正規化および透過性の設定

SIP の正規化および透過性に関する概要

SIP の正規化と透過性はオプションの機能で、Unified Communications Manager とエンドポイント、サービスプロバイダー、Pbx、または別の SIP を実装するゲートウェイ間の SIP の相互運用性に関する問題を処理します。SIP の正規化と透過性を設定するには、カスタマイズされた LUA スクリプトを SIP トランクまたは SIP 回線に適用します。このスクリプトは、Unified Communications Manager によって、SIP トランクまたは SIP 回線を通過する SIP メッセージに適用されます。

インストール時に、Unified Communications Manager には、システム内の SIP トランクおよび SIP プロファイルに割り当てることができるデフォルトの正規化スクリプトと透過性スクリプトが含まれています。また、独自のカスタマイズされたスクリプトを作成し、インポートできます。

SIP 正規化スクリプト

SIP 正規化スクリプトは、着信と発信の SIP メッセージを変更します。たとえば、Unified Communications Manager を Cisco TelePresence Video Communications Server と相互運用する場合は、その 2 つを接続する SIP トランクに *vcs-interop* スクリプトを適用します。このスクリプトは、2 つの製品が通信できるように SIP メッセージの違いを解決します。

正規化スクリプトは、どの SIP トランク接続にも適用できます。SIP トランクを結合するエンドポイントで使用されているプロトコルには関係ありません。

SIP 透過性

SIP 透過性スクリプトを使用すると、Unified Communications Manager を使用して、固有のヘッダーなどの SIP 情報をコール レッグ間で透過的に渡すことができます。透過性が機能するためには、両方のコール レッグが SIP である必要があります。

SIP 透過性の別の機能として、REFER 透過があります。これを使用すると、Unified Communications Manager は、REFER 要求を処理することなく渡します。REFER 透過性をコール センター環境で使用できます。コール センターでは、中央集中型エージェントがコールに応答すると、その発信者と同じ地理的領域にいるエージェントにコールを転送します。REFER 透過を使用すると、集中型 Unified Communications Manager がコールを切断してコール制御を新しいエージェントに移動することができます。

SIP の正規化および透過性のためのデフォルトスクリプト

インストール時に、Cisco Unified Communications Manager には、SIP の正規化と透過性に対応する次のデフォルト スクリプトが含まれます。これらのスクリプトを SIP トランクまたは SIP プロファイルに適用することはできますが、これらのスクリプトを編集することはできません。これらのスクリプトのいずれも要件を満たしていない場合は、独自のスクリプトを作成できます。

- **HCS-PCV-PAI passthrough**：Cisco HCS プラットフォームとエンタープライズ IMS の統合を提供します。
- **cisco-telepresence-conductor-interop**：TelePresence Conductor に登録されたエンドポイントの相互運用性を提供します。
- **cisco-telepresence-mcu-ts-direct-interop**：Cisco Unified Communications Manager と Cisco TelePresence MCU または Cisco TelePresence Server との間で相互運用性を提供します。
- **cisco-meeting-server-interop**：Cisco Unified Communications Manager と Cisco Meeting Server（CMS）の間で相互運用性を提供します。
- **diversion-counter**：転送カウンタを調整する機能を提供します。
- **refer-passthrough**：SIP トランク間のブラインド転送のために、コールから Cisco Unified Communications Manager を削除します。
- **vcs-interop**：Cisco TelePresence Video Communications サーバに登録されているエンドポイントの相互運用性を提供します。

SIP の正規化および透過性の前提条件

- Cisco Unified Communications Manager には、SIP の正規化と透過性のデフォルトのスクリプトが用意されています。既存のスクリプトとシステム設定を確認して、前提条件を満たしているか確認してください。スクリプトの詳細については、「SIP の正規化および透過性のためのデフォルトスクリプト （96 ページ）」を参照してください。
- サードパーティ製品の SIP 要件に加えて、ご使用の環境の SIP 要件を把握していることを確認してください。Cisco Unified Communications Manager の SIP の実装に関する情報については、『*Cisco Unified Communications Manager SIP* 回線メッセージング ガイド（*Standard Edition*）』（http://www.cisco.com/c/en/us/support/unified-communications/

unified-communications-manager-callmanager/products-programming-reference-guides-list.html）を参照してください。

- カスタマイズされたSIP正規化スクリプトの開発を計画している場合は、『*Developer Guide for SIP Normalization and Transparenc*（*SIP* 正規化および透過性に関する開発者ガイド）』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html）を参照してください。

SIP の正規化および透過性の設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	新しいSIPの正規化および透過性スクリプトの作成 （98 ページ）	（省略可）事前インストール済みスクリプトのいずれもニーズを満たしていない場合は、次の手順を使用して、カスタマイズされたスクリプトを設定します。[SIP 正規化スクリプトの設定（SIP Normalization Script Configuration）] ウィンドウで新しいスクリプトを作成するか、またはカスタマイズされたスクリプトをインポートできます。
ステップ 2	SIP トランクへの正規化スクリプトまたは透過性スクリプトの適用 （99 ページ）	[トランクの設定（Trunk Configuration）] ウィンドウで、SIP トランクにスクリプトを直接適用します。Cisco Unified Communication Manager は、このスクリプトを、トランクを通過するすべての SIP メッセージに適用します。
ステップ 3	SIPデバイスに対する正規化または透過性の適用 （99 ページ）	SIP回線に正規化スクリプトまたは透過性スクリプトを適用する場合は、その SIP 回線に関連付けられている SIP プロファイルにスクリプトを適用します。CiscoUnified Communications Manager は、そのSIPプロファイルを使用するすべてのSIPメッセージにこのスクリプトを適用します。

新しい SIP の正規化および透過性スクリプトの作成

デフォルトの正規化と透過性スクリプトが要望を満たさない場合は、次の手順を使用して新しいLUA スクリプトを作成します。Cisco Unified Communications Manager で新しいスクリプトを作成するか、またはシステムにファイルをインポートすることができます。

ヒント　ユーザが作成するスクリプトがデフォルトのスクリプトに類似していたら、[SIP 正規化スクリプト設定（SIP Normalization Script Configuration）] ウィンドウでデフォルト スクリプトを開き、[コンテンツ（Contents）]テキスト ボックスをコピーします。新しいスクリプトを作成して、その内容を [コンテンツ（Contents）] テキスト ボックスに貼り付けます。これで、新しいスクリプトの内容を編集できます。

（注）　SIP 正規化スクリプトのメモリ使用量は、各スクリプトではなく各トランクに基づきます。

手順

ステップ 1　Cisco Unified CM Administration で、**[デバイス（Device）]**>**[デバイス設定（Device Settings）]**>**[SIP 正規化スクリプト（SIP Normalization Script）]** を選択します。

ステップ 2　[新規追加（Add New）] をクリックします。
[SIP 正規化スクリプト設定（SIP Normalization Script Configuration）] ウィンドウが表示されます。

ステップ 3　スクリプトの [名前（Name）] と [説明（Description）] を入力します。

ステップ 4　新しいスクリプトを作成している場合は、[コンテンツ（Contents）] テキストボックスのスクリプトを編集します。

ステップ 5　（省略可）インポートする外部ファイルがあれば、次の手順を実行します

a) [ファイルのインポート（Import File）] をクリックします。
b) [参照（Browse）] してファイルを見つけ、選択します。
c) [ファイルのインポート（Import File）] をクリックします。
[SIP 正規化スクリプト設定（SIP Normalization Script Configuration）] ウィンドウに、[コンテンツ（Contents）]テキスト ボックスにインポートしたファイルの内容が表示されます。

ステップ 6　[SIP正規化スクリプト設定（SIP Normalization Script Configuration）] ウィンドウのフィールドを完成します。フィールドとその内容については、オンライン ヘルプを参照してください。

ステップ 7　[保存（Save）] をクリックします。

次のタスク

スクリプトを SIP プロファイルまたは SIP トランクに割り当てます。

• SIP デバイスに対する正規化または透過性の適用 （99 ページ）
• SIP トランクへの正規化スクリプトまたは透過性スクリプトの適用 （99 ページ）

SIP トランクへの正規化スクリプトまたは透過性スクリプトの適用

SIP トランクに SIP の正規化または透過性スクリプトを適用するには、次の手順を使用します。Cisco Unified Communications Manager は、トランクを通過する SIP メッセージにスクリプトを適用します。

手順

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

ステップ 2 [検索（Find）] をクリックして、 スクリプトを適用するトランクを選択します。

ステップ 3 [正規化スクリプト（Normalization Script）] ドロップダウン リストで、トランクに適用するスクリプトを選択します。

ステップ 4 （任意） SIP メッセージング内の特定のパラメータを正規化する場合は、次の操作を実行します。

a) 正規化する [パラメータ名（Parameter Name）] と、そのパラメータに適用する値 [パラメータ値（Parameter Value）] を入力します。たとえば、[ロケーション（Location）] パラメータと、値として「North Carolina」を入力します。

b) さらにパラメータを追加するには、**(+)** ボタンをクリックして追加の行を作成します。その行で追加のパラメータと値を入力できます。

ステップ 5 （任意） スクリプトに対して SDI トレースを作成するには、[トレースを有効化（Enable Trace）] チェック ボックスをオンにします。

（注） シスコでは、スクリプトをデバッグするときにトレースを有効にすることをお勧めします。

ステップ 6 [保存（Save）] をクリックします。

SIP デバイスに対する正規化または透過性の適用

デバイスで使用される SIP プロファイルにスクリプトを適用することによって、カスタマイズされた SIP 正規化および透過性スクリプト、またはカスタマイズされた SDP 透過性プロファイルを SIP 電話に適用することができます。

手順

ステップ 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。

ステップ 2 [検索（Find）] をクリックして、スクリプトを適用する SIP プロファイルを選択します。

ステップ 3 [SDP情報（SDP Information）] 領域の [SDP透過性プロファイル（SDP Transparency Profile）] ドロップダウン リストでプロファイルを選択します。

ステップ 4 [正規化スクリプト（Normalization Script）] ドロップダウン リストで、トランクに適用するスクリプトを選択します。

ステップ 5 （任意） SIP メッセージング内の特定のパラメータを正規化する場合は、次の操作を実行します。

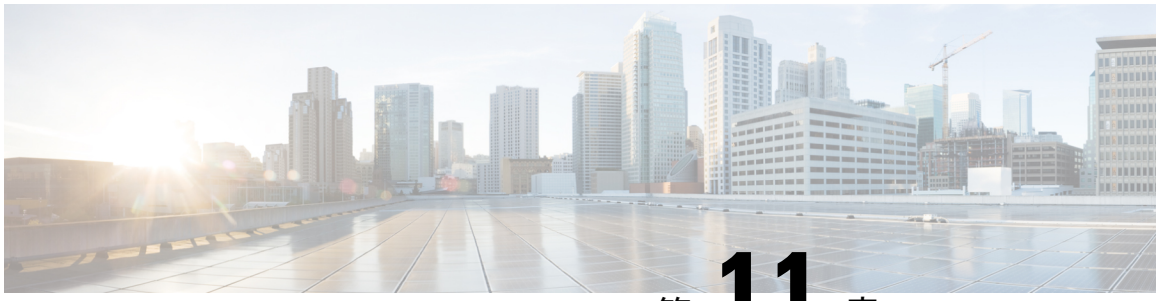
a) 正規化する [パラメータ名（Parameter Name）] と、そのパラメータに適用する値 [パラメータ値（Parameter Value）] を入力します。たとえば、[ロケーション（Location）] パラメータと、値として「North Carolina」を入力します。

b) さらにパラメータを追加するには、**(+)** ボタンをクリックして追加の行を作成します。その行で追加のパラメータと値を入力できます。

ステップ 6 （任意） スクリプトに対して SDI トレースを作成するには、[トレースを有効化（Enable Trace）] チェック ボックスをオンにします。

（注） シスコでは、スクリプトをデバッグするときにトレースを有効にすることをお勧めします。

ステップ 7 [保存（Save）] をクリックします。



第 11 章

SDP 透過性プロファイルの設定

SDP 透過性プロファイルの概要

SDP 透過性プロファイルには、宣言的な SDP 属性のルールのセットが含まれており、これによりシステムは、Unified Communications Manager によってネイティブにサポートされていない宣言属性を、入口から出口コール区間に渡すことができます。SDP透過性プロファイルがないと、Unified Communications Manager は、サポートされていない SDP 属性を削除します。

複数のルールを使用して SDP 透過性プロファイルを設定し、SIP プロファイルを介して SIP デバイスに適用することができます。SDP 透過性プロファイルを適用するには、両方のコールレッグが SIP である必要があります。次のタイプの SDP 属性ルールを設定できます。

- [プロパティ（Property）]：プロパティ属性にルールが設定されている場合、属性に値が設定されていない限り、Unified Communications Manager は SDP 属性をパススルーします。
- 任意の値：ルールが任意の値に対して設定されると、値が 1 つ以上の空白以外の文字で構成されている限り、SDP 属性はパス スルーされます。
- リストからの値：ルールがこのオプションを使用して設定されると、値が指定された値のいずれかに一致する限り、SDP 属性はパス スルーされます。可能な値を 5 個まで設定することができます。

SDP透過性プロファイルの制限

SDP透過性プロファイルには次の制限が適用されます。これらの状況のいずれかが出力コールレッグに発生すると、Cisco Unified Communications Manager は宣言型 SDP 属性を通過させません。

- パススルーをサポートしていない、1つ以上のメディア ターミネーション ポイント（MTPs）またはトラステッド リレー ポイントが割り当てられます
- [メディア ターミネーション ポイントが必要（Media Termination Point Required）] チェックボックスを、SIP トランク用にチェックします
- トランスコーダが使用されます
- RSVP が使用されます
- 入力コール レッグではディレイド オファーが使用されている一方、出力コール レッグではアーリー オファーが使用されている場合。
- メディアの回線は拒否されました（port=0）
- いずれかのコール レッグが、SIP 以外のプロトコルを使用している場合

SDP 透過性プロファイルの前提条件

サードパーティ SIP 製品の導入を計画している場合は、製品がセッション記述プロトコル(SDP)を実装する方法を理解していることを確認してください。

SDP 透過性プロファイルの設定

Cisco Unified Communications Manager がネイティブでサポートしていない宣言型 SDP 属性のルール セットを使用して、カスタマイズされた SDP 透過性プロファイルを設定します。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[デバイス設定（Device Settings）]** > **[SDP透過性プロファイル（SDP Transparency Profile）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] を入力します。

ステップ 4 [属性情報（Attribute Information）] ペインで、パススルーする SDP 属性のルールを作成します。

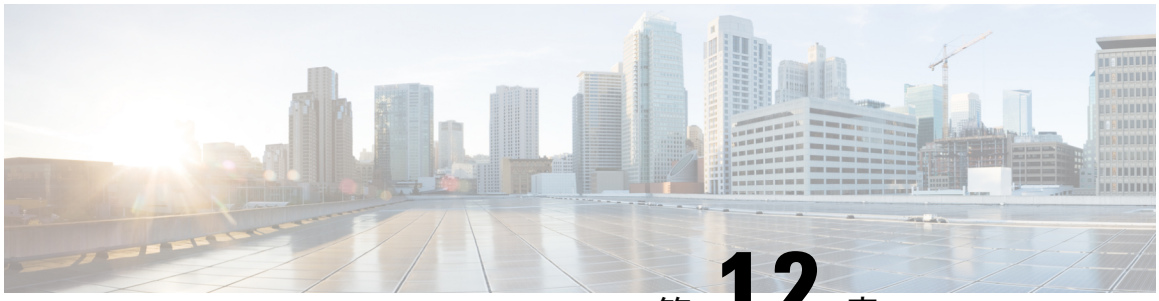
- プロパティの属性をパス スルーするには、[名前（Name）] テキスト ボックスに「a=recvonly」などの属性を入力し、[タイプ（Type）] ドロップダウン リストから [プロパティ（Property）] を選択します。
- 値属性をパススルーするには、[名前（Name）] テキスト ボックスに属性（たとえば a=rtpmap）を入力し、[タイプ（Type）] ドロップダウン リスト ボックスから [値（Any Value）] を選択します。
- 最大 5 個の値のいずれかを指定した値の属性をパス スルーするには、[名前（Name）] フィールドに「a=rtpmap」などの属性を入力し、**[タイプ（Type）]** ドロップダウン リスト

から [任意の値（Any Value）] を選択します。[結果**値 (** value)] テキストボックスに、属性の値を入力します。[+] をクリックして、この属性に最大 5 つの値を追加できます。

ステップ 5 この透過性プロファイル用に追加の SDP 属性を入力できる新しい行を作成するには、**[+]** をクリックします。

ステップ 6 [保存（Save）] をクリックします。

（注） SIP プロファイルを使用するデバイスが SDP 透過性プロファイルを使用するには、このプロファイルを SIP プロファイルに適用する必要があります。



第 12 章

SIP プロファイルの設定

SIP プロファイルの概要

SIP プロファイルは、共通の SIP 設定で構成されるテンプレートです。ネットワーク内に SIP デバイスまたは SIP トランクを導入する場合は、SIP プロファイルを使用して共通の SIP 設定をデバイス グループに適用できます。SIP エンドポイントのグループに対して複数のプロファイルを設定できます。多様なデフォルトの SIP プロファイルから選択するか、または独自の SIP プロファイルを作成することができます。

SIP プロファイルを使用しない場合は、ネットワーク内のすべての SIP トランクと SIP デバイスに対して SIP 設定を個別に設定する必要があります。ただし、SIP プロファイルを使用して、次のようなさまざまな SIP の設定を割り当てることができます。

- MTP テレフォニー ペイロード タイプ
- SIP ヘッダー詳細
- SIP メッセージのタイマーとカウンタ
- SDP の相互運用性のための SDP 透過性プロファイル
- SIP 回線用の SIP 正規化と透過性スクリプト
- SIP 設定
- SIP 早期提供サポート
- コールピックアップ URI

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

ステップ 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。

ステップ 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。

ステップ 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。

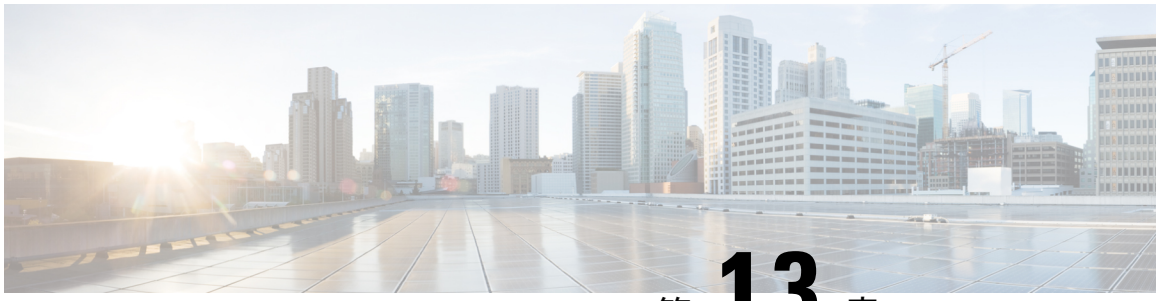
ステップ 4 SDP の相互運用性を解決するために SDP 透過性プロファイルを割り当てる場合は、[SDP透過性プロファイル（SDP Transparency Profile）] ドロップダウン リストから割り当てます。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 8 [保存（Save）] をクリックします。



第 13 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 （853 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
ステップ 1	オペレーティング システムの IPv6 の設定 （109 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。
ステップ 2	IPv6 向けのサーバ設定 （110 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。
ステップ 3	IPv6 の有効化 （110 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。
ステップ 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 （111 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。

	コマンドまたはアクション	目的
	• デバイス用 IP アドレッシング モードの優先順位の設定 （111 ページ）	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。
ステップ 5	サービスの再起動 （113 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

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

ステップ 2 [Enable IPv6] チェックボックスをオンにします。

ステップ 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。

ステップ 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、 **fd62:6:96:21e: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。

ステップ 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。

ステップ 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

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

ステップ 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。

ステップ 3 [保存（Save）] をクリックします。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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 （111 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 （111 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （113 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 （853 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

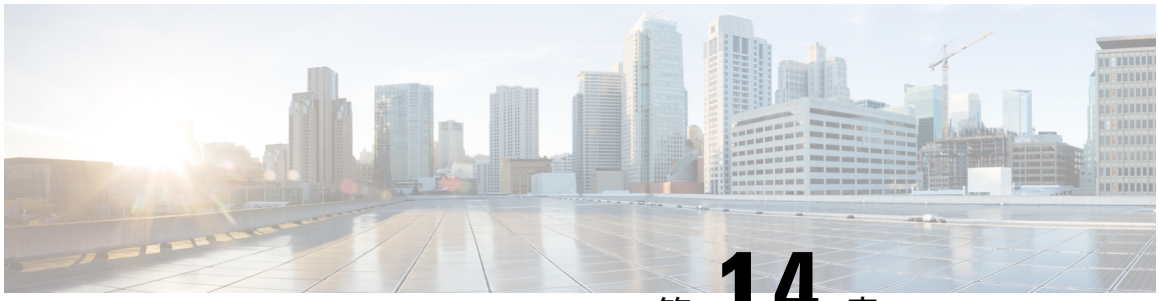
ステップ 1 Cisco Unified Serviceability にログインして、**[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択します。

ステップ 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

ステップ 3 [再起動（Restart）] をクリックします。

ステップ 4 [OK] をクリックします。



第 14 章

SIP 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の SIP を展開している場合、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、リモート クラスタ、またはセッション管理エディションなどの外部デバイスに Cisco Unified Communications Manager を接続する SIP トランクを設定します。

Cisco Unified CM Administration の内部で、[SIP Trunk Configuration] ウィンドウには、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。

SIP トランクに対して最大 16 の異なる宛先アドレスを割り当てることができます。IPv4 または IPv6 のアドレス指定、完全修飾ドメイン名、または 1 つの DNS SRV レコードを使用できます。

SIP トランクでは、次の機能を設定できます。

- 回線と名称識別サービス
- 遅延されたサービス、初期オファー、ベストエフォート
- 信号およびメディア認証と暗号化
- メディア暗号化（SRTP）
- デュアルスタックのサポート
- ビデオ
- BFCP を使用したプレゼンテーションの共有
- 遠端カメラ制御

- DTMF リレー
- 発信側の正規化
- URI ダイヤル
- Q.SIG サポート
- T.38 ファクス サポート
- SIP OPTIONS
- DTMF シグナリングの選択

（注） クラスタ A からクラスタ B で小規模 IP テレフォニー（SIPT）の Q.SIG を有効にした場合、匿名またはテキストで "INVITE" を受領しても、Cisco Unified Communications Manager は "INVITE" を Q.SIG データにエンコードしません。リーフ クラスタで同じようにデコードすると、何も表示されず、空の番号が転送されます。

（注） Q.SIG を有効にすると、URI ダイヤルが予期したとおりに応答しません。Q.SIG を無効にすると、Cisco Call Back が 2 つのクラスタ間で応答しません。

IPv6 デュアル スタックのサポート

共通デバイス設定で IP アドレッシングモードを設定し、その設定を SIP トランクに適用することによって、IPv6 デュアル スタックをサポートする SIP トランクを設定することもできます。

（注） クラスタ全体のサービス パラメータを使用して、クラスタ全体に IPv6 を設定することもできます。ただし、共通デバイス設定の設定値は、クラスタ全体のデフォルト値よりも優先されます。

安全な SIP トランク

SIP トランク セキュリティ プロファイルを設定して、ダイジェスト認証、シグナリングとメディアの暗号化などのセキュリティで自分のトランクを設定することもできます。このプロファイルにはダイジェスト認証やTLS シグナリングが含まれ、そのプロファイルをネットワークの SIP トランクに関連付けます。トランクでコール メディアを暗号化できるようにするには、トランクで SRTP メディアを許可するように設定する必要もあります。

SIP トランク セキュリティ プロファイルの概要

ネットワーク内の各 SIP 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る必要があります。デフォルトでは、Cisco Unified Communications Manager がすべての SIP トランクに、事前に定義された非セキュアな SIP トランク セキュリティ プロファイルを適用します。

SIP トランク セキュリティ プロファイルを使用することにより、ネットワークの SIP トランクの TLS シグナリング暗号化とダイジェスト認証のようなセキュリティを設定できます。SIP トランク セキュリティ プロファイルを設定し、そのプロファイルを SIP トランクに割り当てると、プロファイルのセキュリティの設定がトランクに適用されます。

ネットワークに異なる SIP トランクの設定がある場合に、複数の SIP トランク セキュリティ プロファイルを設定することで、さまざまなセキュリティ要件に対応できます。

（注） ネットワークにセキュリティを設定するには、CTL クライアントをセットアップし、IPSec を設定する必要もあります。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。

SIP トランク設定の前提条件

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。これらのデバイスが SIP を実装している場合は、SIP 正規化スクリプトを適用する必要がある場合があります。
- トランク用の SIP プロファイルを設定します。

さらに、SIP トランクを設定する前に、次の設定を構成します。

- SIP の正規化および透過性の設定タスク フロー （97 ページ）
- SIP プロファイルの設定 （106 ページ）

SIP トランクの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	SIP トランク セキュリティ プロファイルの設定 （118 ページ）	SIP トランクに適用する任意のセキュリティ設定を使用して、SIP トランク セ

	コマンドまたはアクション	目的
		キュリティプロファイルを設定します。たとえば、ダイジェスト認証、デバイスセキュリティ モード、および SIP シグナリングの TLS 暗号化を設定できます。 SIP トランク セキュリティ プロファイルを設定しなければ、デフォルトで、Cisco Unified Communication Manager によって非セキュアの SIP トランク セキュリティ プロファイルが適用されます。
ステップ 2	共通デバイス設定の構成 （119 ページ）	トランクの共通デバイス設定を実行します。デュアルスタック トランクの場合、IP アドレッシングの優先順位を設定します。
ステップ 3	SIP トランクの設定 （120 ページ）	ネットワークの SIP トランクを設定します。[トランクの設定（Trunk Configuration）] ウィンドウで、トランクの SIP 設定を実行します。SIP プロファイル、SIP トランク セキュリティ プロファイル、および共通デバイス設定を SIP トランクに割り当てます。また、トランク接続に必要な SIP の正規化および透過性スクリプトを割り当てます。たとえば、SIP トランクが Cisco TelePresence VCS に接続する場合、*vcs-interop* スクリプトを SIP トランクに割り当てる必要があります。

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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [保存（Save）] をクリックします。

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

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

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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）**
- **[Call Control Discovery（コール制御検出）]**
- **[クラスタ間のエクステンション モビリティ（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）]**

ステップ 5 （任意）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。

ステップ 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。

ステップ 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。

ステップ 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。

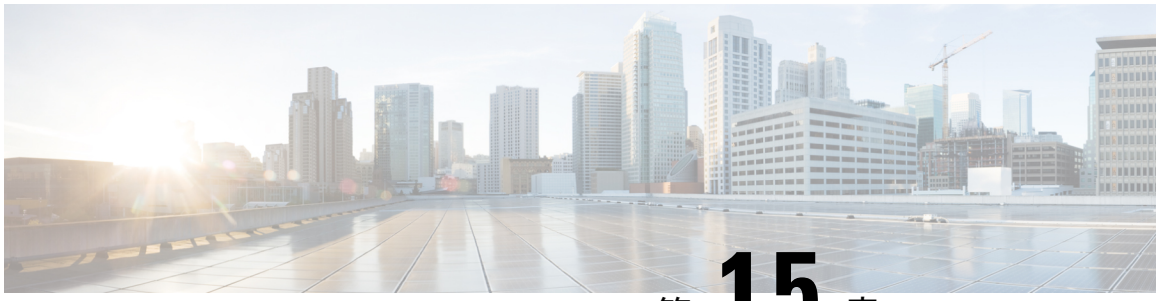
ステップ 9 **[SIP トランク セキュリティプロファイル（SIP Trunk Security Profile）]** ドロップダウン リスト ボックスから、このトランクに SIP トランク セキュリティプロファイルを割り当てます。このオプションを選択しない場合は、非セキュアプロファイルが割り当てられます。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 13 [保存（Save）] をクリックします。



第 15 章

H.323 トランクの設定

H.323 トランクの概要

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。

（注） ゲートキーパーは今では広く使用されていませんが、ゲートキーパー制御のトランクを使用するように H.323 導入を設定することもできます。ゲートキーパー制御のトランクを設定する方法の詳細については、『*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。

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、「トランクの設定」の章の「デバイス プール設定のコア設定のタスクフロー」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

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

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

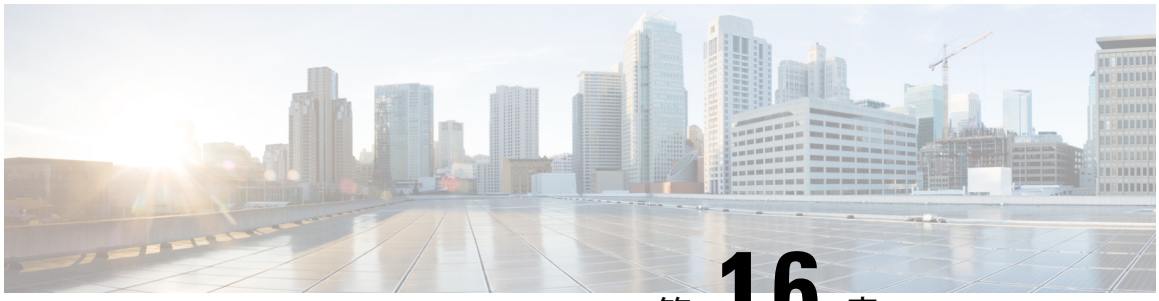
ステップ 6 [デバイスプール（Device Pool）] ドロップダウン リスト ボックスから、このトランクに設定したデバイスプールを選択します。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 16 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 設定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、「トランスレーション パターンの設定 （200 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
ステップ 1	SRST 参照の設定 （129 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。
ステップ 2	デバイス プールへの SRST リファレンスの割り当て （129 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。
ステップ 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 （130 ページ） • デバイス プールの接続モニタ期間の設定 （130 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。
ステップ 4	SRST ゲートウェイでの SRST の有効化 （131 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

ステップ 1 Cisco Unified CM Administration にログインし、**[システム（System）]** > **[SRST（SRST）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （129 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 （130 ページ）
  - デバイス プールの接続モニタ期間の設定 （130 ページ）

手順

ステップ 1 SRST ゲートウェイ（ルータ）にログインします。

ステップ 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。

ステップ 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。

ステップ 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。

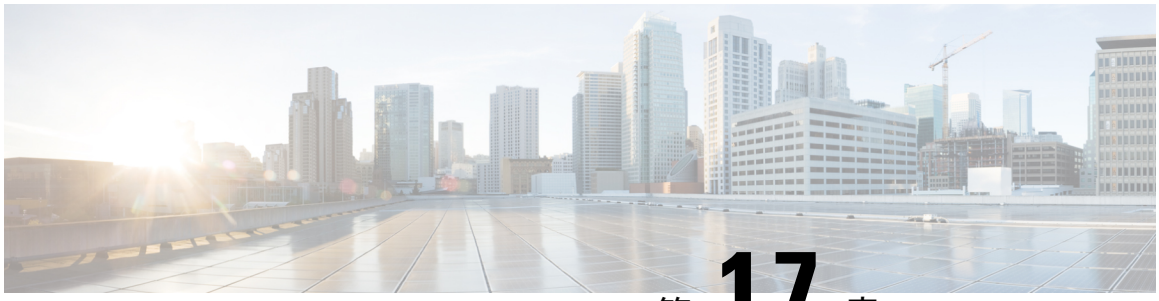
ステップ 5 **ip source-address** ip-address コマンドを入力します。ここで、ip-address は既存のルータ IP アドレスで、通常はルータのイーサネットポートのアドレスの 1 つです。
このコマンドにより、SRSTルータは、指定されたIPアドレスを介してシスコIP電話からメッセージを受信することができます。

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 III 部

ダイヤル プランの設定



第 17 章

ダイヤル プランの概要

ダイヤルプランの概要

ダイヤル プランで、 Cisco Unified Communications Manager システムにコールのルーティングに関する指示を出します。ダイヤルプランを設定する場合は、次のようにルールを定義します。

- 許可されているコールのタイプ
- コールを発信するためにシステムが使用する優先パスと、代替パス
- 内線番号のダイヤル方法
- 電話番号の表示方法

ダイヤル プランの前提条件

ダイヤルプランを設定する前に、次のタスクを実行します。

- 初期設定タスク フロー （5 ページ）
- 着信コールと発信コールの情報 （73 ページ）

ダイヤル プラン設定

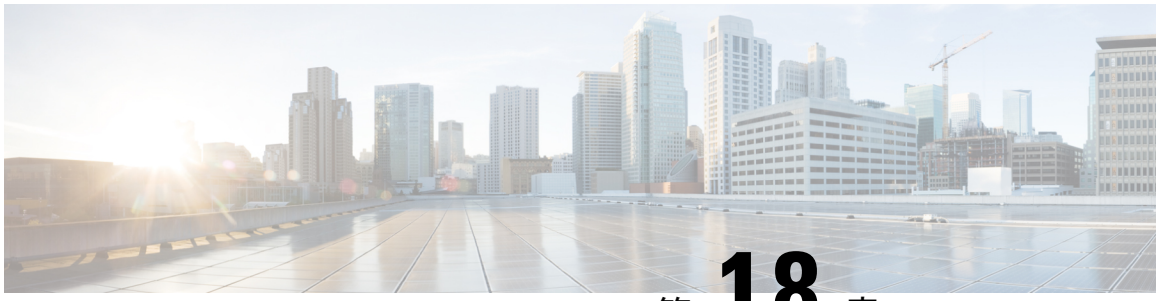
次のタスク フローを実行すると、システムのダイヤル プランを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	パーティションの設定タスクフロー（141 ページ）	パーティションを設定して、ディレクトリ番号（DN）の論理グループと、到達可能性の特徴が類似したルート パターンを作成します。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、コール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。
ステップ 2	国内番号計画のインストールタスクフロー （148 ページ）	（省略可）Cisco Unified CM Administration では、デフォルトで、北米番号計画（NANP）を使用できます。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。国内の番号計画を使用している場合は、@ 記号とルートフィルタを使用するルートパターンを設定して、国内コール、国際コール、長距離コール、緊急コール用にパターンを作成できます。 国内番号のダイヤルプランの使用は任意です。国内の番号契約を使用しない場合は、手動で設定できます。
ステップ 3	コールルーティングの設定タスクフロー （152 ページ）	ルーティング計画を設定して、専用ネットワークまたは公衆交換電話網（PSTN）に内部呼と外部呼をルーティングする。
ステップ 4	ハントパイロットの設定タスクフロー（190 ページ）	番号の 1 つ以上のリストにコールを拡張する場合は、各リストで探している順序を指定する必要がある場合は、ハントパイロットを設定します。これらのリストからコールがハントパーティに転送され、パーティが応答できなかった、または話中であった場合、次のハントパーティでハントが再開されます

	コマンドまたはアクション	目的
ステップ 5	トランスレーション パターンの設定タスク フロー （200 ページ）	ボイスゲートウェイからの着信番号を Cisco Unified Communications Manager に操作する変換パターンを設定します。コールを受信側エンドポイントに転送する前に、変換パターンを使用して、呼び出し番号とコール番号を変更できます。この変換は透過的であり、内線をパブリックからプライベート ネットワークにマップすることができます。
ステップ 6	トランスフォーメーション パターンの設定タスク フロー （201 ページ）	着信コールの通話番号表示を変更する場合は、電話機の変換パターンを設定します。発信コール用に送信される発信コールまたはコール番号表示を変更する場合は、ゲートウェイまたはトランクの変換パターンを設定します。また、変換のパターンを使用して、発信するリダイレクト番号 (SIP デバイスの転送ヘッダーとして知られる) を変更することもできます。
ステップ 7	ダイヤル ルールの設定タスク フロー （206 ページ）	さまざまな種類のダイアルルールを設定できます。アプリケーションダイアル規則、ディレクトリ検索ダイアル規則、およびSIPダイアルルール。 • 異なる種類のダイヤル規則を設定できます。アプリケーションダイヤル規則、ディレクトリ検索ダイヤル規則、SIPダイヤル規則。 • ディレクトリ検索ダイヤル ルールにより、発信者 ID がディレクトリで検索可能な番号に変換されます。 • SIP ダイヤルルールを設定して、SIP を実行している電話機のダイヤルパターンを作成します。これは、レガシーの SIP 電話の一般的な手順です。
ステップ 8	ILS の設定タスクフロー （217 ページ）	リモートの Cisco Unified Communications Manager クラスタのネットワークを作

	コマンドまたはアクション	目的
		成するには、intercluster ルックアップ サービス (ILS) を設定します。ペアのクラスタにメーター着陸システムを配置して、メーター着陸システムネットワークを形成するためにこれらのクラスタを追加することができます。
ステップ 9	グローバル ダイヤル プラン レプリケーションのタスク フロー（232 ページ）	グローバル ダイヤル プラン レプリケーションによって、ディレクトリ URI のクラスタ間ダイヤルと ILS ネットワーク全体にまたがる代替番号を含む、グローバル ダイヤル プランを作成できます。
ステップ 10	URI ダイヤルの設定タスク フロー（245 ページ）	コールアドレスとしてディレクトリ URI を使用してエンドポイントにコールをルーティングする場合は、[URI ダイヤリングを設定する (URI ダイヤリングの設定)。ディレクトリ URIはユーザ名@ホストフォーマットに従い、ホスト部分はIPv 4アドレスまたは完全に定義されたドメイン名である。



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）
- トランスレーション パターン
- トランスフォーメーション 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、コール 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 7: 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
ステップ 1	パーティションの設定 （141 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。
ステップ 2	コーリング サーチ スペースの設定 （143 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）
- トランスレーション パターン
- トランスフォーメーション 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、コール 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 *8*: 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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 *9:* 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。
トランスレーション パターン	トランスレーション 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。コールがトランスレーション パターンと一致する場合、Unified CM が変換を実行し、そのトランスレーション 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。トランスレーション 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 Communication Manager* 機能設定ガイド』の「論理パーティション分割の設定」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
ステップ 1	COP ファイルのインストール（148 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。
ステップ 2	国内番号計画のインストール（149 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。
ステップ 3	CallManager サービスの再起動（150 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 9 [完了（Finish）] をクリックします。

ステップ 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 （149 ページ）

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

ステップ 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。

ステップ 2 検索条件を入力して [検索（Find）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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、各コール 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で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。

システムは、ルート プランに、次のコンポーネントを使用する 3 階層のアプローチを用います。

- 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対応するルート リストを選択します。
- 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。

これらの構成要素に加えて、ルート プランは次のコンポーネントを含みます。

- ローカル ルート グループ：PSTN ゲートウェイのロケーションを、ゲートウェイにアクセスするため使用されるルート パターンから分離します。
- ルート フィルタ：ルート パターンで許可されている特定の番号を制限します。

- 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：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 （141 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設定タスクフロー

手順

	コマンドまたはアクション	目的
ステップ 1	ローカル ルート グループの設定 （153 ページ）	**（省略可）**必要なルート リストの数を減らすには、ローカル ルート グループを設定します。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、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。
ステップ 2	ルート グループの設定 （156 ページ）	**（省略可）**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。

	コマンドまたはアクション	目的
ステップ 3	ルート リストの設定 （157 ページ）	（省略可）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。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。
ステップ 4	ルートフィルタの設定 （157 ページ）	（省略可）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。 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している場合、ルート フィルタはオプションです。 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。
ステップ 5	ルート パターンの設定 （162 ページ）	特定のデバイスにコールを導き、特定の数字パターンを含めるか排除するようにルート パターンを設定します。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。
ステップ 6	時間帯ルーティングの設定 （166 ページ）	（省略可）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。

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
ステップ 1	ローカル ルート グループの設定 （154 ページ）	（**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。
ステップ 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 （155 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。
ステップ 3	ローカル ルート グループのルートリストへの追加 （155 ページ）	（**省略可**）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

ステップ 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。

ステップ 2 [行の追加（Add Row）] をクリックします。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 5 [保存（Save）] をクリックします。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （159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。

ステップ 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 （161 ページ）」を参照してください。

ステップ 6 [保存（Save）] をクリックします。

ステップ 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 （159 ページ）
- ルート フィルタの演算子 （161 ページ）
- ルート フィルタの例 （161 ページ）

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 *10* : 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。
COUNTRY CODE	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。

タグ	説明
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。
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 *11* : 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。
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。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （163 ページ）

• ドットの前の数字を削除する例 （165 ページ）
• プレフィックス番号の例 （166 ページ）
• オンネットパターンとオフネットパターンの例 （166 ページ）
• ブロックおよびルート パターンの例 （166 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 *12*：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 ～ 91999999999999999999999 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
?	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。
+	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 ～ 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。
[ ]	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。

文字	説明	例
.	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。
\+	\+ 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。

時間帯ルーティングの設定

（省略可）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
ステップ 1	時間帯の設定 （167 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。
ステップ 2	タイム スケジュールの設定 （167 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。
ステップ 3	パーティションとスケジュールの関連付け （168 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

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 3 [保存（Save）] をクリックします。

コールルーティングの制限

特長	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。

特長	制限事項
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。
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。

特長	制限事項
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。

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	

フィールド	説明
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）]	

フィールド	説明
	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

フィールド	説明
	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）	

フィールド	説明
	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

フィールド	説明
	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）	

フィールド	説明
	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、

フィールド	説明
	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）	

フィールド	説明
	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

フィールド	説明
	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）	
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）	

フィールド	説明
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（Directory Numbers）	

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

ステップ 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。

ステップ 2 メンバーを追加する回線グループを見つけます。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 2 電話番号を削除する回線グループを見つけます。

ステップ 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。

ステップ 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
ステップ 1	回線グループの設定 （190 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。
ステップ 2	ハント リストの設定 （191 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。
ステップ 3	ハント パイロットの設定 （192 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

ステップ 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。

ステップ 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。

ステップ 3 [回線グループ名（Line Group Name）] を入力します。

ステップ 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。

ステップ 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) （省略可）[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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 3 ハントリストの名前を入力します。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 7 [保存（Save）] をクリックします。

ステップ 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 （192 ページ）」を参照してください。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 7 発信者、接続先、着信者に適用するディジット トランスフォーメーション パターンを割り当てます。

ステップ 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 *13 :* 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 ～ 91999999999999999999 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 ～ 91999999999999999999 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 ～ 91999999999999999999 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 キューイングがイネーブル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

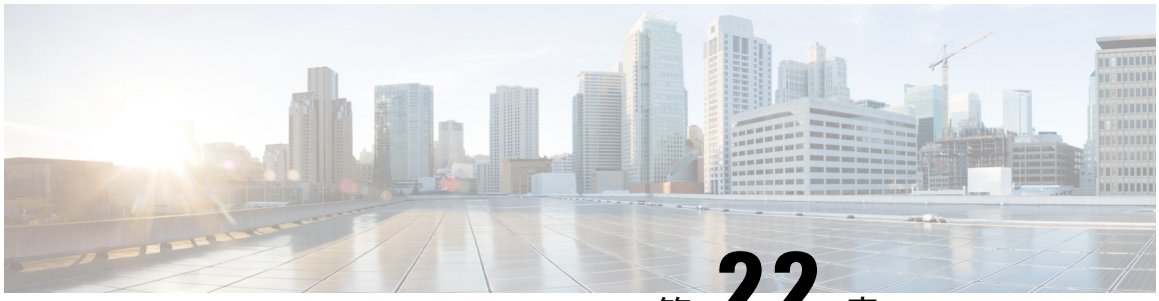
機能	連携動作と制限事項
ハント グループのシングル ナンバー リーチ	ハント グループが設定済みで、ハンド グループが指し示す 1 つ以上の電話番号でシングル ナンバー リーチ（SNR）が有効な場合には、ハント グループのすべてのデバイスがログインしない限り、SNR リモート接続先にコールが転送されません。 ハント グループ内の各デバイスについて、[電話の設定（Phone Configuration）] ウィンドウで [ハント グループにログイン（Logged into Hunt Group）] チェックボックスをオンにする必要があります。
コールキューイング	コールキューイングは、ハントパ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 *14*：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

トランスレーション パターンの設定

トランスレーション パターンの概要

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。トランスレーション パターンは、ルート パターンと同じ一般規則に従い、同じワイルドカードを使用します。ルート パターンと同じように、トランスレーション パターンをパーティションに割り当てます。ただし、ダイヤルされた数字がトランスレーション パターンと一致する場合、Cisco Unified Communications Manager は、ゲートウェイなどの外部エンティティにコールをルーティングしません。代わりに、まず変換を実行した後、トランスレーション パターン内で設定されたコーリング サーチ スペースを使用して、コールを再度ルーティングします。

トランスレーション パターンの要件

変換パターンを設定する前に、次のタスクを実行する必要があります。

- パーティションの設定タスクフロー （141 ページ）
- コールルーティングの設定タスクフロー （152 ページ）

（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トランスレーション 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、トランスレーション パターン、電話番号、コール 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。

トランスレーション パターンの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	トランスレーション パターンの設定（200 ページ）	コールされてからコールをルーティングされる方法を指定するには、トランスレーション パターンを設定します。

トランスレーション 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、トランスレーション 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

ステップ 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。

ステップ 2 次のいずれかのオプションを選択します。

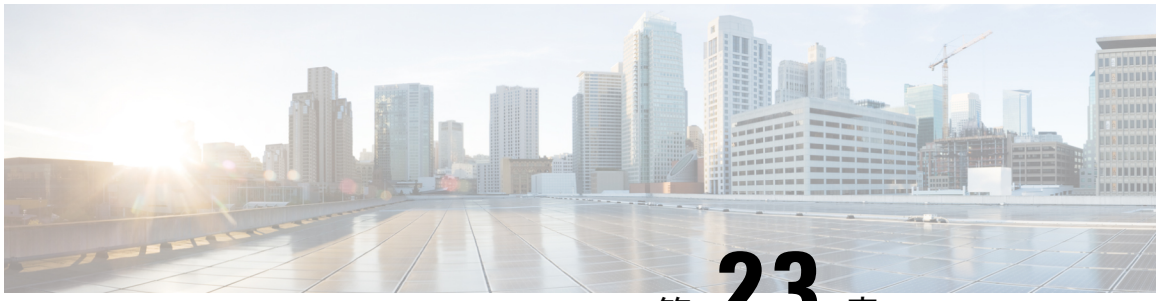
- 新しいトランスレーション パターンを追加するには、[新規追加（Add New）] をクリックします。
- 既存のトランスレーション パターンを選択するには、[検索（Find）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [保存（Save）] をクリックします。



第 23 章

トランスフォーメーション パターンの設定

変換パターンの概要

変換パターンは、着信コールまたは発信コールでダイヤルされた数字をシステムがどのように操作するかを決定します。コールまたは呼び出された番号を、システムが電話機または PSTN に送信する前に変更する必要がある場合は、変換パターンを設定できます。

変換パターンを使用して、数字、プレフィックスの付いた数字の廃棄、発信者のトランスフォームマスクの追加、発信者番号のプレゼンテーションの制御を行うことができます。

次のことが可能です。

- 呼び出された関係者変換 CSS を使用して、通話関係のパターンにヒットします。
- コール関係者変換の CSS を使用して、通話先変換のパターンにヒットします。

トランスフォーメーションパターンの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	発信側トランスフォーメーションパターンの設定 （202 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。

	コマンドまたはアクション	目的
ステップ 2	着信側トランスフォーメーション パターンの設定 （203 ページ）	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。
ステップ 3	変換プロファイルの設定 （203 ページ）	**オプション**: 次の手順は、Cisco の会社間メディアエンジン (cisco IME) を使用している場合にのみ実行してください。ダイヤルされた番号を E.164 形式に変換するには、トランスフォーメーション プロファイルを設定する必要があります。

発信側トランスフォーメーション 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

ステップ 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）] > [トランスフォーメーション（Transformation）] > [トランスフォーメーションパターン（Transformation Pattern）] > [着信側トランスフォーメーション パターン（Calling Party Transformation Pattern）]**。

ステップ 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。

ステップ 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**：

事前トランスフォーメーション発信側番号に基づいて、発信者のトランスフォーメーション 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 トランクで発信側トランスフォーメーション 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、発信側トランスフォーメーションマスクの選択には常に事前トランスフォーメーション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トランスフォーメーション 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。

ステップ 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。

ステップ 5 [保存（Save）] をクリックします。

着信側トランスフォーメーション 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

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [トランスフォーメーション（Transformation）] > [トランスフォーメーションパターン（Transformation Pattern）] > [着信側トランスフォーメーション パターン（Called Party Transformation Pattern）]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しい着信側トランスフォーメーション 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。

ステップ 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。

ステップ 4 **[着信側トランスフォーメーションパターンの設定（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。

ステップ 5 [保存（Save）] をクリックします。

変換プロファイルの設定

Cisco Intercompany Media Engine（Cisco IME）を使用している場合にのみ、次の手順を実行します。ダイヤルされた番号をE.164形式に変換するには、トランスフォーメーションプロファイルを設定する必要があります。E.164形式では、国際対応の「+」が先頭につきます。たとえば、「+14085551212」です。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [トランスフォーメーション（Transformation）] > [トランスフォーメーション プロファイル（Transformation Profile）]** を選択します。

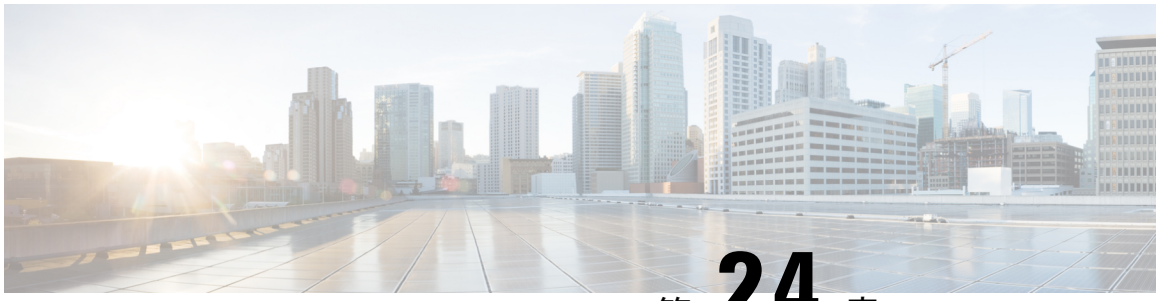
ステップ 2 次のいずれかのオプションを選択します。

- 新しいトランスフォーメーション プロファイルを追加するには、[新規追加（Add New）] をクリックします。
- 既存のトランスフォーメーションプロファイルの設定を変更するには、[検索（Find）] をクリックし、結果のリストからパターンを選択します。

[トランスフォーメーションプロファイルの設定（Transformation Profile Configuration）] ウィンドウが表示されます。

ステップ 3 [トランスフォーメーションプロファイルの設定（Transformation 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。

ステップ 4 [保存（Save）] をクリックします。



第 24 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

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
ステップ 1	アプリケーション ダイヤル ルールの設定 （206 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。
ステップ 2	ディレクトリ検索ダイヤル ルールの設定 （207 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。
ステップ 3	SIP ダイヤル ルールの設定 （208 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。
ステップ 4	ダイヤル ルールの優先順位の変更 （211 ページ）	（省略可）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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （207 ページ）
- SIP ダイヤル ルールの設定 （208 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （208 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
ステップ 1	SIP ダイヤル ルールの設定 （209 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。
ステップ 2	SIP ダイヤル ルールのリセット （210 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。
ステップ 3	SIP ダイヤル ルール設定と SIP 電話の同期 （211 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 （209 ページ）

パターンの形式

表 *15 : 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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設定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 （210 ページ）

関連トピック

パターンの形式 （209 ページ）

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 （209 ページ）

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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設定ファイルを作成できます。TFTP サーバは Cisco Unified Communications Manager に新しい設定ファイルについて通知し、更新された設定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 （211 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 （210 ページ）

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 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

ステップ 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。

ステップ 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）]**

ステップ 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。

ステップ 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。

ステップ 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

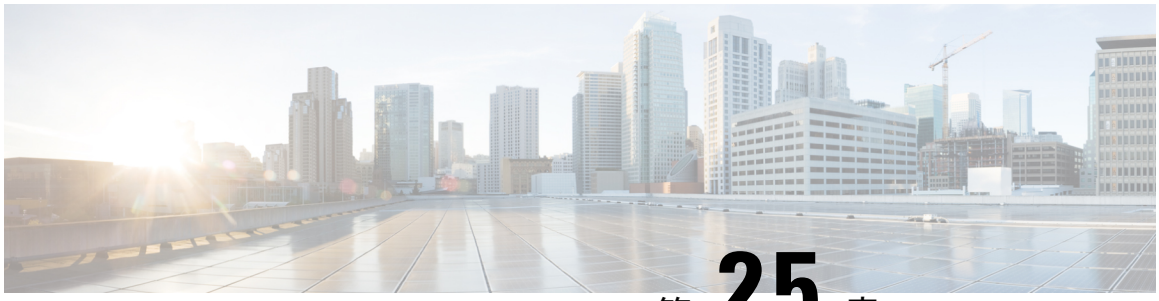
Cisco Unified IP Phone	連携動作
SIP を実行している 7911、7941、7961	これらの電話機は、7940_7960_OTHER ダイヤル ルール パターンを使用します。キープレス マークアップ言語（KPML）では、Cisco Unified Communications Manager に数字を 1 桁ごとに送信できます。 SIP ダイヤル ルールを使用すると、Cisco Unified Communications Managerに送信する前に、電話で数字のパターンをローカルに収集できます。SIP ダイヤル ルールを設定しないと、KPML が使用されます。Cisco 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 25 章

クラスタ間ルックアップ サービスの設定

クラスタ間検索サービスの概要

クラスタ間検索サービス（ILS）を使用すると、リモートの Cisco Unified Communications Manager クラスタのネットワークを作成できます。複数のクラスタで ILS を設定すると、ILS ネットワークにあるリモート クラスタの現在のステータスで Cisco Unified Communications Manager が更新されます。

Cisco Unified CM Administration では、一対のクラスタで ILS を設定し、それらのクラスタを結合して ILS ネットワークを形成できます。ILS を使用すると、各クラスタ間の接続を設定することなく、ネットワークに追加クラスタを参加させることができます。

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
- スポーク クラスタ
- グローバル ダイヤル プラン インポート済みカタログ

ハブ クラスタ

ハブ クラスタは ILS ネットワークのバックボーンを形成します。ハブ クラスタは ILS ネットワーク内の他のハブ クラスタとの間で ILS の更新を交換し、次いでスポーク クラスタとの間でその情報のやり取りを中継します。

新しいハブ クラスタが既存の ILS ネットワーク内の別のハブ クラスタに登録されると、ILS は ILS ネットワーク内のすべての既存のハブ クラスタと新しいハブ クラスタとの間にフル メッシュ接続を自動的に作成します。

スポーク クラスタ

ILS ネットワーク内のスポーク クラスタは ILS 更新を ILS ネットワークの他の部分とやり取りするために、接続されているハブ クラスタに依存して、これを中継してもらいます。スポーク クラスタはローカル ハブ クラスタのみと接続し、他のハブ クラスタまたは他のスポーク クラスタとは直接接続しません。

グローバル ダイヤル プラン インポート済みカタログ

ただし、サードパーティ システムに URI ダイヤリングの互換性を提供するために、ILS ネットワークの任意のハブ クラスタに CSV ファイルからサードパーティ ディレクトリ URI カタログまたは+E.164 番号のカタログを手動でインポートできます。ILS は、インポートされたカタログを保持し、そのカタログをネットワーク内の他のクラスタに複製します。ILS ネットワーク内の任意のサーバから、サードパーティディレクトリ Uri または + E: 164 番号のカタログのいずれかをダイヤルできます。

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 10 個であるため、合計で最大 100 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 10 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 の要件

ネットワークを研究し、ILS トポロジを設計します。

ソリューション リファレンス ネットワーク デザインの詳細については、『*Cisco Unified Communications* ソリューション リファレンス ネットワーク デザイン』ガイド（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html）を参照してください。

ILS 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
ステップ 1	クラスタ間検索サービスの有効化（218 ページ）	クラスタ Id とリモートクラスタを設定するために、Intercluster ルックアップ サービスをアクティブにします。
ステップ 2	クラスタ ID の設定（218 ページ）	ILS ネットワーク内の各クラスタに対して、一意の識別子を指定します。
ステップ 3	リモートクラスタの設定（219 ページ）	ILS ネットワーク内でリモートクラスタを設定します。
ステップ 4	さまざまなクラスタの ILS をアクティブにするには、次のタスクを実行します。 • ハブ クラスタでの ILS のアクティブ化（220 ページ） • スポーククラスタでの ILS の有効化（221 ページ）	ネットワーク内の最初の ILS ハブ クラスターで ILS をアクティブにする （注） ILS ネットワークの各クラスタは、ハブ クラスタまたはスポーク クラスタのいずれかに設定する必要があります。
ステップ 5	(クラスタ間の認証を設定します。デバイスを選択するには、次のいずれかの手順を使用します。 • クラスタ間での TLS 認証の有効化（222 ページ） • クラスタ間でのパスワード認証の有効化（223 ページ） • クラスタ間でパスワード認証付きの TLS を有効にする（223 ページ）	ILS ネットワーク内のクラスタ間で TLS 認証を使用します。 ILS ネットワーク内のリモートクラスタ間でパスワード認証を使用します。 クラスタ間の自己署名証明書を交換せずに、共通の認証局 (CA) の署名付き証明書を使用して ILS ネットワークをセットアップするには、TLS およびパスワード認証を使用します。

	コマンドまたはアクション	目的
ステップ 6	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（234ページ）	(グローバルダイヤルプランのレプリケーションのILSサポートを有効にして、参加しているILS対応クラスタ間でダイヤルプラン情報を共有します。
ステップ 7	ILS ネットワークへのカタログのインポート （225 ページ）	（省略可）サードパーティシステムとのURIダイヤル互換性を提供するために、サードパーティディレクトリURIまたは＋E.1.164番号ディレクトリを手動でcsvファイルからILSネットワーク内の任意のハブクラスタに導入することができます。

クラスタ間検索サービスの有効化

クラスタ Id とリモートクラスタを設定するには、インタークラスタルックアップサービスをアクティブにする必要があります。

手順

ステップ 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。

ステップ 2 **サーバ**のドロップダウンリストから、Ciscoクラスタ間の検索サービスをアクティブにするノードを選択し、**開始**をクリックします。

ステップ 3 **シスコ クラスタ間検索サービス**

ステップ 4 [保存（Save）] をクリックします。

次のタスク

クラスタ ID の設定 （218 ページ）

クラスタ ID の設定

ILS ネットワーク内の各クラスタに対して、一意のクラスタ ID を設定する必要があります。また、固有のピア ID を使用していることも確認する必要があります。クラスタは、ステータスメッセージを交換するときに、この一意のクラスタ ID とピア ID を使用します。

たとえば、4 つの Cisco Unified Communication Manager クラスタがある既存の ILS ネットワークに別のクラスタを追加する場合は、新しいクラスタでILSを設定した後、そのクラスタを既存の ILS ネットワークの任意のハブ クラスタに登録できます。ILS は、既存のネットワークにあるすべてのクラスタについて、新しいクラスタに自動的に通知します。

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
- 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

ネットワーク内のクラスタごとに一意の識別子を設定するには、次の手順を実行します。

始める前に

クラスタ間検索サービスの有効化 （218 ページ）

手順

ステップ 1 Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 Cisco Unified Communication Manager, **システム** > **エンタープライズパラメータ**を選択します。

ステップ 3 **[エンタープライズパラメータ設定 (** Configuration **)]** [設定 (Configuration)] ウィンドウクラスタ ID] フィールドに、ネットワーク内で設定するクラスタの名前を入力します。

最大 50 文字を入力できます。入力できる文字は、英数字、ピリオド（.）、ハイフン（-）です。デフォルトでは、StandAloneCluster に設定されています。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

リモートクラスタの設定 （219 ページ）

リモートクラスタの設定

ILS ネットワーク内のリモートクラスタを設定するには、次の手順を実行します。

始める前に

クラスタ ID の設定 （218 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[詳細機能（Advanced Features）]** > **[クラスタ ビュー（Cluster View）]** を選択します。

ステップ 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。

ステップ 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。

次のタスク

次のいずれかの手順を実行します。

- ハブ クラスタでの ILS のアクティブ化 （220 ページ）
- スポーククラスタでの ILS の有効化 （221 ページ）

ハブ クラスタでの ILS のアクティブ化

ILS ネットワークの各クラスタは、ハブクラスタまたはスポーククラスタのいずれかに設定してください。各 ILS ネットワークには、少なくとも 1 つのハブ クラスタが必要です。他のハブ クラスタにハブ クラスタを接続することも、ネットワークの唯一のハブ クラスタとしてハブ クラスタを設定することもできます。また、複数のスポーク クラスタにハブ クラスタを接続することも、スポーク クラスタを使用することなくハブ クラスタを設定することもできます。

ILS ネットワークのハブ クラスタで ILS をアクティブ化するには、次の手順を実行します。

始める前に

リモートクラスタの設定 （219 ページ）

手順

ステップ 1 Cisco Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 **[高度な機能（Advanced Features）]** > **[ILS の設定（ILS Configuration）]** を選択します。

ステップ 3 **[ILS の設定（ILS Configuration）]** ウィンドウで、**[ロール（Role）]** ドロップダウンリストから **[ハブクラスタ（Hub Cluster）]** を選択し、**[保存（Save）]** をクリックします。

（注） ILS ネットワーク内の特定のクラスタを削除するには、**[ILS の設定（ILS Configuration）]** ウィンドウの **[ロール（Role）]** ドロップダウンリストから **[スタンドアロン（Standalone）]** を選択して **[保存（Save）]** をクリックします。

ステップ 4 **[ILS 設定の登録（ILS Configuration Registration）]** ポップアップウィンドウで、**[登録サーバー（Registration Server）]** テキストボックスを空欄にしたままで **[OK]** をクリックします。

次のタスク

- スポーククラスタでの ILS の有効化 （221 ページ）

スポーククラスタでの ILS の有効化

ILS ネットワーク内のスポーク クラスタは ILS 更新を ILS ネットワークの他の部分とやり取りするために、接続されているハブ クラスタに依存して、これを中継してもらいます。スポーククラスタの ILS をアクティブにするには、次の手順に従います。

始める前に

- クラスタ ID の設定 （218 ページ）
- リモートクラスタの設定 （219 ページ）

手順

ステップ 1 Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 Cisco Unified CM Administration で、**[詳細機能（Advanced Features）]** > **[ILSの設定（ILS Configuration）]** を選択します。

ステップ 3 [ロール（Role）] ドロップダウン リストから、[スポーク クラスタ（Spoke Cluster）] を選択し、[保存（Save）] をクリックします。

ステップ 4 [ILS 設定の登録（ILS Configuration Registration）] ポップアップ ウィンドウで、[登録サーバ（Registration Server）] テキストボックスに表示された ILS ネットワークにある既存ハブ クラスタのパブリッシャノードの IP アドレス、または完全修飾ドメイン名を入力して、[OK] をクリックします。

ステップ 5 [ILS クラスタとグローバル ダイヤル プラン インポート カタログ（ILS Clusters and Global Dial Plan Imported Catalogs）] セクションでネットワークを表示して、ILS ネットワークが設定されていることを確認します。

すべてのネットワークが表示されたら、ILS ネットワークでクラスタ ディスカバリが設定されています。

次のタスク

次のオプションのいずれかの手順を実行します。

- クラスタ間でパスワード認証付きの TLS を有効にする （223 ページ）

クラスタ間での TLS 認証の有効化

(ILS ネットワーク内のリモートクラスタ間の通信を暗号化するには、次の手順を使用します。

始める前に

クラスタ間のトランスポート層セキュリティ（TLS）認証を使用するには、ILSネットワーク内の各クラスタの発行元ノード間でTomcat証明書を交換する必要があります。Cisco Unified Operating System Administration から、証明書の一括管理機能を使用して、以下を行います。

- ネットワーク内の各クラスタで、証明書をパブリッシャ ノードから中央ロケーションにエクスポートする。
- ILS ネットワーク内のすべてのパブリッシャ ノード サーバから、エクスポートされた証明書を統合する。
- ネットワーク内の各クラスタで、そのクラスタのパブリッシャ ノードに証明書をインポートする。

（注） クラスタ間の TLS 認証を有効に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）を参照してください。

手順

ステップ 1 Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 Cisco Unified CM Administration で、**[詳細機能（Advanced Features）] > [ILSの設定（ILS Configuration）]** を選択します。

ステップ 3 [ILS 設定（ILS Configuration）] ウィンドウで、ILS 認証の下の [TLS 認証を使用（Use TLS Certificates）] のチェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

次の任意の手順を実行します。

- クラスタ間でのパスワード認証の有効化 （223 ページ）

- 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 （234 ページ）

クラスタ間でのパスワード認証の有効化

リモートクラスタ間でパスワード認証を使用する場合は、ILSネットワーク内のクラスタ間で行われるすべての通信にパスワードを割り当てます。

手順

ステップ 1 Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 Cisco Unified CM Administration で、**[詳細機能（Advanced Features）] > [ILSの設定（ILS Configuration）]** を選択します。

ステップ 3 [ILSの設定（ILS Configuration）] ウィンドウで、ILS 認証の下の [パスワードを使用（Use Password）] チェックボックスをオンにします。

ステップ 4 [パスワードを使用（Use Password）] テキストボックスにパスワードを入力します。

（注） ネットワーク内のすべてのクラスタを同じパスワードで設定する必要があります。

ステップ 5 [パスワードの確認（Confirm Password）] テキストボックスにパスワードを再入力します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

次の任意の手順を実行します。

- クラスタ間での TLS 認証の有効化 （222 ページ）
- 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 （234 ページ）

クラスタ間でパスワード認証付きの TLS を有効にする

始める前に

クラスタ間で証明書を交換せずにトランスポートレイヤセキュリティ (TLS) とパスワード認証を使用するには、証明機関のルート証明書を Tomcat の信頼にアップロードし、証明書によって署名された Tomcat 証明書を取得する必要があります。認証ルート証明書。次に、証明書が同じクラスタに再度インポートされます。すべてのクラスタに対して同じパスワードを使用して証明書がアップロードされると、クラスタを Intercluster ルックアップサービス (ILS) ネットワークに接続できます。

（注） クラスタ間の TLS 認証を有効に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）を参照してください。

手順

ステップ 1 Cisco Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 Cisco Unified CM Administration で、**[詳細機能（Advanced Features）] > [ILSの設定（ILS Configuration）]** を選択します。

ステップ 3 [ILSの設定（ILS Configuration）] ウィンドウで、[ILS認証（ILS Authentication）] の下にある [TLS証明書を使用（Use TLS Certificates）] チェックボックスをオンにします。

ステップ 4 [ILSの設定（ILS Configuration）] ウィンドウで、ILS 認証の下の [パスワードを使用（Use Password）] チェックボックスをオンにします。

ステップ 5 [パスワードを使用（Use Password）] テキストボックスにパスワードを入力します。

（注） ネットワーク内のすべてのクラスタを同じパスワードで設定する必要があります。

ステップ 6 [パスワードの確認（Confirm Password）] テキストボックスにパスワードを再入力します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

（任意）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 （234 ページ）

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

（任意）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

ステップ 1 Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 Cisco Unified CM Administration で、**[詳細機能（Advanced Features）] > [ILS 設定（ILS Configuration）]** を選択します。

ステップ 3 [ILS 設定（ILS Configuration）] ウィンドウで、[グローバル ダイヤル プラン レプリケーション データとリモート クラスタの交換（Exchange Global Dial Plan Replication Data with Remote Clusters）] のチェックボックスをオンにします。

ステップ 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。

ステップ 5 [保存（Save）] をクリックします。

（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。

次のタスク

ILS ネットワークへのカタログのインポート （225 ページ）

ILS ネットワークへのカタログのインポート

（省略可）サードパーティ システムに URI ダイヤリング互換性を持たせるためには、サードパーティの Directory URI または +E.164 番号カタログを、csv ファイルから ILS ネットワークのハブクラスタに手動でインポートします。ILS ネットワークにカタログをインポートするには、次の手順に従ってください。

手順

ステップ 1 [Cisco Unified CMの管理（Cisco Unified Communications Manager 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複製（Global Dial Plan Replication）] > [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 Catalogs）]** を選択します。

ステップ 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、[新規追加（Add New）] をクリックします。

ステップ 3 カタログの名前、説明、ルート文字列を入力して、[保存（Save）] とクリックします。

ステップ 4 [Cisco Unified CM Administration （Cisco Unified Communications Manager Administration）] で、**[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。

ステップ 5 [選択（Choose）] をクリックし、カタログとしてインポートするCSVファイルを選択します。

ステップ 6 [ターゲットの選択（Select the Target）] ドロップダウン リストから [インポート済みディレクトリURIおよびパターン（Imported Directory URIs and Patterns）] を選択します。

ステップ 7 [トランザクションタイプの選択（Select Transaction Type）] ドロップダウン リストから [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）] を選択します。

ステップ 8 [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 *16 : 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。

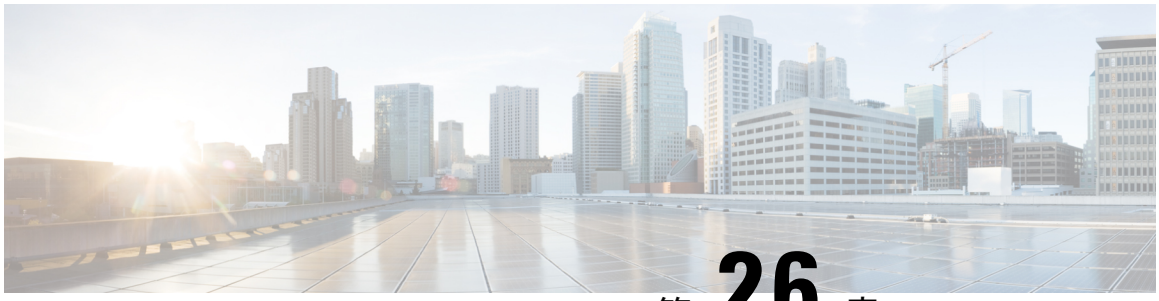
機能	連携動作
グローバル ダイヤル プラン レプリケーション	ILS ネットワークでグローバル ダイヤル プラン レプリケーションが有効な場合、ILS ネットワーク内のリモート クラスタは次のデータを含め、グローバル ダイヤル プラン データを共有します。 • ディレクトリURI • 代替番号 • 代替番号パターン • ルート文字列 • PSTN フェールオーバー番号
着信コール	ILS ベースのネットワークで、発信者番号に基づいて着信コールをブロックするには、SIP ルートパターンのパーティションを発信者の CSS に含める必要があります。たとえば、コールが SIP トランクから発信される場合、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 *17 : 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 26 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のレプリケーションを使用して、複数のクラスタルックアップサービス (ILS) ネットワークにまたがるグローバルダイヤルプランを作成します。ネットワーク全体でグローバル ダイヤル プラン レプリケーションを有効にすると、1 つのクラスタのダイヤル プラン コンポーネントを設定するだけで、ILS によって ILS ネットワーク全体にその情報が複製されます。

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 ネットワーク内の各クラスタが、それぞれのグローバル ダイヤル プランのデータを ILS ネットワークにアドバタイズします。このデータには、ローカルで設定されたグローバル ダイヤル プランのデータや、他のクラスタから学習したデータが含まれます。グローバル ダイヤル プランのデータには、次のようなものがあります。

- ユニバーサル リソース識別子（URI）
- 代替番号
- アドバタイズ パターン
- PSTN フェールオーバー
- ルート文字列
- 学習されたグローバル ダイヤル プラン データ
- インポート済みグローバル ダイヤル プラン データ

[ディレクトリURI（Directory URIs）]

[ILS経由でグローバルにアドバタイズ（Advertise Globally via ILS）]オプションを選択すると、ローカルに設定されたディレクトリURIの完全なカタログがILSによってアドバタイズされます。URIダイヤリングの設定方法の詳細については、「URI ダイヤルの概要 （243 ページ）」を参照してください。

代替番号

代替番号によりグローバルにルーティング可能な番号を設定することができ、ILS ネットワーク内のどこからでもダイヤル可能になります。Cisco Unified Communications Manager では、次の 2 つのタイプの代替番号を作成できます。

- エンタープライズ代替番号
- +E.164 代替番号

アドバタイズ パターン

アドバタイズ パターンを使用すると、代替エンタープライズ番号または +E.164 番号の範囲をまとめたルーティング手順を作成し、そのパターンを ILS ネットワーク全体に複製することで、ILS ネットワーク内のすべてのクラスタがパターンを認識できるようになります。アドバタイズされたパターンを使用すると、代替番号ごとにルーティング情報を設定する必要がなくなります。アドバタイズ パターンが設定されたローカル クラスタでは、アドバタイズ パターンを使用しないでください。アドバタイズパターンは、ILSでパターンを認識するリモートクラスタでのみ使用します。また、ILS によってアドバタイズされたパターンに関する PSTN フェールオーバー情報を設定することもできます。

PSTN フェールオーバー

Unified Communications Manager は、PSTN フェールオーバーを使用して、ILS を通じて学習されたパターン、代替番号、またはディレクトリのURIに対して発信されたコールのみを再ルーティングします。Communications Manager は、ローカルに設定されたパターン、代替番号、およびディレクトリのURIに対して発信されたコールについては、PSTN フェールオーバー番号に再ルーティングしません。

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は、学習ディレクトリ URI、学習番号、学習パターンに関するPSTNフェールオーバー ルールを複製するようにILSを設定できます。発信コールのダイヤル文字列が、学習されたパターン、学習された代替番号、または学習されたディレクトリの URI と一致しており、Unified Communications Manager が SIP 経由でコールをルーティングできない場合、Unified Communications Managerは発信側の自動代替ルーティング（AAR）CSSを使用して、関連付けられているPSTNフェールオーバー番号にコールを再ルーティングします。

ルート文字列

ILSはILSネットワークにローカル ルート文字列をアドバタイズします。グローバル ダイヤル プラン データの各要素は、その要素のホーム クラスタを特定するルート文字列に関連付けられます。リモート クラスタは、ルート文字列と SIP ルート パターンを使用して、ILS ネット

ワーク内のさまざまなクラスタへのルーティングを行います。リモートクラスタのユーザが、ILS を介して学習されたディレクトリ URI または代替番号にダイヤルすると、Unified Communications Manager は、関連付けられたルート文字列と SIP ルート パターンを照合して、SIP ルート パターンで指定されているトランクにコールをルーティングします。

ユーザがクラスタにルート文字列を割り当てると、ILS は、そのルート文字列を同じクラスタ（ローカルに設定されたディレクトリ URI、代替番号、アドバタイズされたパターン、PSTN フェールオーバー情報を含む）に対してローカルである全グローバル ダイヤル プラン データに割り当てます。

（注） SIP ルート パターン名にダッシュが含まれる場合、ダッシュ間に数字が含まれてい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、文字と数字または文字のみの組み合わせを使用できます。

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

学習されたグローバル ダイヤル プラン データ

Unified Communications Manager が ILS 経由で学習したグローバル ダイヤル プラン データはローカル データベースに保存されます。ローカルで設定されたグローバル ダイヤル プランのデータ以外に、ILS は、ローカル クラスタが ILS ネットワーク内の他のクラスタから学習したすべてのグローバル ダイヤル プランのデータをアドバタイズします。これにより、アドバタイズされたすべてのデータが、ILS ネットワーク内の各クラスタに到達します。学習グローバル ダイヤル プランのデータには、学習したディレクトリ URI や学習した代替番号、代替パターン、学習した PSTN フェールオーバー ルール、学習したルート文字列などが含まれます。

Cisco Unified CM Administration で、次のタイプの学習されたグローバル ダイヤル プラン データを表示できます。

- [学習代替番号（Learned Alternate Numbers）]
- [学習エンタープライズ番号と学習 +E.164 パターン（Learned Enterprise and +E.164 Patterns）]
- [学習ディレクトリ URI（Learned Directory URIs）]

インポート済みグローバル ダイヤル プラン データ

Unified Communications Manager を使用すると、グローバルダイヤルプランデータを CSV ファイルから ILS ネットワーク内の任意のハブクラスタにインポートできます。Cisco Unified Communications Manager を使用すれば、グローバル ダイヤル プラン データを CSV ファイルから ILS ネットワーク内の任意のハブ クラスタにインポートできます。ILS では、このインポート済みグローバル ダイヤルプランデータを ILS ネットワーク全体に複製します。これにより、Cisco Unified Communications Manager をシスコテレプレゼンスビデオ通信サーバー 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ことができます。インポートされたグローバル ダイヤル プランのデータには、ディレクトリ URI や +E.164 パターン、シスコテレプレゼンスビデオ通信サーバー またはサードパーティのコール制御システムの CSV ファイルから手動でインポートした PSTN フェールオーバー ルールなどが含まれます。

（注） インポート済みデータに含まれているのは、Cisco Unified Communications Manager に手動でインポートされたグローバル ダイヤル プラン データだけです。インポート済みグローバル ダイヤル プラン データに、ILS を通じて学習されたデータは含まれていません。

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

ILS の設定タスクフロー （217 ページ）の手順に従って、で ILS ネットワークをセットアップします。

グローバル ダイヤル プラン レプリケーションのタスクフロー

手順

	コマンドまたはアクション	目的
ステップ 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 （234 ページ）。	参加している ILS 対応のクラスタ間でダイヤルプラン情報を共有できるように、グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にします。
ステップ 2	代替番号の設定 （234 ページ）。	（省略可）クラスタ間でダイヤル可能な代替番号を設定するには、代替番号のレプリケーションを設定します。

	コマンドまたはアクション	目的
ステップ 3	代替番号のアドバタイズパターンの設定（235 ページ）。	（省略可）パターンを使用して代替番号を集約するには、アドバタイズされたパターンをセットアップして、パターンの PSTN フェールオーバー ルールを指定します。
ステップ 4	PSTN フェールオーバーの設定（236 ページ）。	（省略可）特定のディレクトリ URI または代替番号の PSTN フェールオーバー番号をセットアップするには、特定の電話番号に関連付けられているすべてのディレクトリ URI および代替番号の PSTN フェールオーバー番号として代替番号を指定します。
ステップ 5	学習番号とパターンのパーティションの設定（237 ページ）。	（省略可）ILS を通して、ルート パーティションをローカル クラスタが学習する代替の番号およびパターンに指定します。
ステップ 6	学習したパターンのブロック（238 ページ）。	（省略可）ローカルの Unified Communications Manager クラスタが、学習した代替番号または学習した代替番号パターンにコールをルーティングするのを防ぐために、そのクラスタでローカルのブロッキング ルールを設定できます。
ステップ 7	学習したデータに対するデータベース制限の設定（239 ページ）。	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。
ステップ 8	グローバル ダイヤル プランのデータをインポート（239 ページ）。	（省略可）ILS ネットワークを Cisco TelePresence Video Communication 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、他のシステムの CSV ファイルから ILS ネットワーク内のハブ クラスタにディレクトリ URI のカタログをインポートします。

次のタスク

クラスタ全体でディレクトリのユニバーサル リソース識別（URI）をダイアルするには、ローカル クラスタに URI ダイヤルをセットアップします。詳細については、「URI ダイヤルの概要（243 ページ）」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

ステップ 1 Cisco Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 Cisco Unified CM Administration から、**[詳細機能（Advanced Features）] > [ILS 設定（ILS Configuration）]** を選択します。

ステップ 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。

ステップ 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。

ステップ 5 [保存（Save）] をクリックします。

代替番号の設定

エンタープライズ代替番号または +E.164 代替番号を作成し、電話番号と代替番号を関連付けます。代替番号をダイヤルすると、関連する電話番号に登録されている電話機の呼び出し音が鳴ります。

（注） 設定したそれぞれの代替番号は、単一の電話番号に関連付ける必要があります。ただし、その電話番号はエンタープライズ代替番号と +E.164 代替番号の両方に同時に関連付けることができます。

始める前に

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 （234 ページ）。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [ディレクトリ番号（Directory Number）]** を選択します。

ステップ 2 [ディレクトリ番号の検索と一覧表示（Find and List Directory Numbers）] ウィンドウから、代替番号を関連付ける電話番号を検索して選択します。

ステップ 3 [ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウから、割り当てる代替番号のタイプに応じて次のいずれかのオプションをクリックします。

- [エンタープライズ代替番号の追加（Add Enterprise Alternate Number）]
- [+E.164代替番号の追加（Add +E.164 AlternateNumber）]

ステップ 4 [番号マスク（Number Mask）] フィールドで、電話番号に適用する番号マスクを入力します。

[代替番号（Alternate Number）] フィールドには、Cisco Unified Communications Manager が番号マスクを適用した後にどのように代替番号が表示されるかが示されます。

ステップ 5 （省略可）代替番号のローカル ルーティングを有効にするには、次の手順を実行します。

a) [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。

b) [ルートパーティション（Route Partition）] ドロップダウン リストから、ローカル コーリング サーチ スペースに割り当てられるルート パーティションを選択します。

ステップ 6 （省略可）番号パターンを使用してこの代替番号のクラスタ間ルーティングを設定する場合、[保存（Save）] をクリックします。

ステップ 7 （省略可）この代替番号のクラスタ間ルーティングを設定する場合、代替番号の [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。

ステップ 8 （省略可）この代替番号に PSTN フェールオーバー番号を割り当てる場合、[PSTN のフェールオーバー（PSTN failover）] ドロップダウン リストから、PSTN フェールオーバーとして番号を割り当てます。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

代替番号のアドバタイズパターンの設定 （235 ページ）.

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [保存（Save）] をクリックします。

PSTN フェールオーバーの設定

ディレクトリ URI または代替番号の PSTN フェールオーバー番号を割り当て、PSTN フェールオーバー番号をILSネットワークにアドバタイズするには、次の手順を実行します。リモートクラスタでは、学習ディレクトリ URI または学習代替番号へのコールに PSTN フェールオーバー番号を使用できます。

始める前に

代替番号のアドバタイズパターンの設定 （235 ページ）。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [ディレクトリ番号（Directory Number）]** を選択します。

ステップ 2 [電話番号の検索と一覧表示（Find and List Directory Numbers）] ウィンドウから、PSTN フェールオーバー番号を割り当てるディレクトリ URI または代替番号に関連付けられる電話番号を検索して選択します。
が表示されます。

ステップ 3 (PSTN フェールオーバーとして使用する代替番号が存在しない場合は、[**ディレクトリ番号の設定**] ウィンドウで、割り当てる代替番号のタイプに応じて、次のいずれかのオプションを選択します。

- [エンタープライズ代替番号の追加（Add Enterprise Alternate Number）]
- [+E.164代替番号の追加（Add +E.164 AlternateNumber）]

ステップ 4 [PSTN のフェールオーバー（PSTN Failover）] ドロップダウン リストで、PSTN フェールオーバーとして使用する代替番号を選択します。

ステップ 5 [保存（Save）] をクリックします。

Cisco Unified Communications Manager は、その PSTN フェールオーバー番号を電話番号に関連付けます。グローバル ダイヤル プラン レプリケーションは、電話番号に割り当てられるすべてのディレクトリ URI および代替番号の PSTN フェールオーバー番号として、その番号を ILS ネットワークにアドバタイズします。

次のタスク

学習番号とパターンのパーティションの設定 （237 ページ）.

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

ステップ 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。

ステップ 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。

ステップ 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。

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 7 [保存（Save）] をクリックします。

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 10 [保存（Save）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

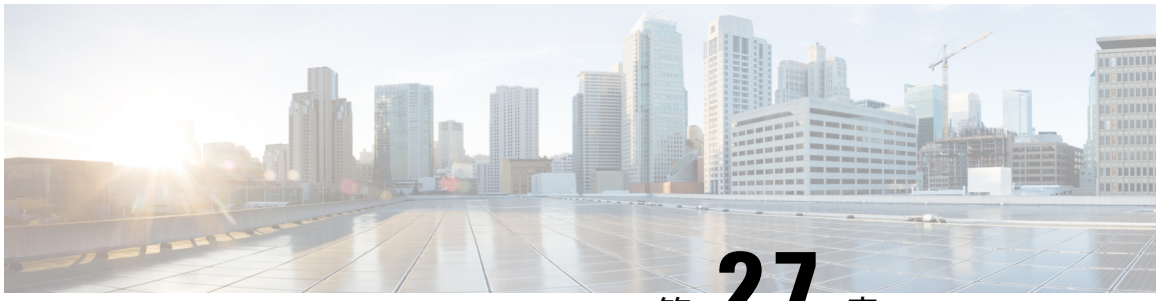
ステップ 15 次のいずれかの手順を実行します。

- 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。



第 27 章

URI ダイヤリングの設定

URI ダイヤルの概要

Unified Communications Manager は、コールアドレッシングにディレクトリ URI を使用するダイヤリングをサポートしています。ディレクトリ URI は、ユニフォーム リソース識別子で、電話番号を識別するために使用できる文字列です。ディレクトリ URI は電子メール アドレスに似ており、username@host という形式になります。ホスト部分は IPv4 アドレスまたは完全修飾ドメイン名です。ディレクトリ番号を電話に割り当てると、Unified Communications Manager は、ディレクトリ URI を使用して、その電話にコールをルーティングできます。URI ダイヤルは、ディレクトリ URI をサポートしている SIP および SCCP エンドポイントで使用できます。

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。

URI ダイヤルの要件

クラスタ間に URI ダイヤルを設定する場合は、ILS ネットワークを設定して ILS ネットワークのグローバル ダイヤル プラン レプリケーションを有効にする必要があります。このタスクを実行するには、次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 レプリケーションのタスク フロー （232 ページ）
- ILS の設定タスクフロー （217 ページ）

URI ダイヤルの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ディレクトリ URI をネットワーク内のローカル クラスタに割り当てます。 • ユーザへのディレクトリ URI の割り当て （246 ページ） • ディレクトリ URI とディレクトリ番号の関連付け （247 ページ）	エンド ユーザをシステムにプロビジョニングし、ディレクトリ URI をそれらのエンドユーザに割り当てます。また、電話番号を設定し、ディレクトリ URI をその電話番号と関連付けます。 （注） エンド ユーザの設定と電話番号の設定の両方で、一括管理を使用して、エンドユーザ、ディレクトリ URI、電話番号および話を Cisco Unified Communications Mana にインポートすることもできます。詳細については、『*Cisco Unified Communicatio Manager* 一括管理ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanag products-maintenance-guides-list.html）を照してください。

	コマンドまたはアクション	目的
ステップ 2	デフォルトディレクトリ URI パーティションの割り当て （248 ページ）	デフォルトのディレクトリ URI パーティションをコーリング サーチ スペースにある既存のパーティションに割り当てます。
ステップ 3	URI ダイヤリング用の SIP プロファイルの設定 （248 ページ）	SIP プロファイルを設定して、ネットワーク内のクラスタ間ダイヤリングを設定します。
ステップ 4	URI ダイヤリング用の SIP トランクの設定 （249 ページ）	Cisco Unified Communications Manager が電話番号、ディレクトリ URI、または電話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 ヘッダーに挿入するかどうかを決定します。
ステップ 5	SIP ルート パターンの設定 （250 ページ）	クラスタ間ディレクトリ URI コールをルーティングするように、SIP ルートパターンを設定します。
ステップ 6	ILS ネットワーク内の全クラスタについて手順 1 ～ 5 を繰り返します。	この手順は、ILS ネットワーク内に複数のクラスタがある場合に実行します。
ステップ 7	ディレクトリ URI カタログのインポート （251 ページ）	ディレクトリ URI から 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にコールする場合は、他のシステムの CSV ファイルから ILS ネットワーク内のいずれかのハブ クラスタにディレクトリ URI カタログをインポートします。

ユーザへのディレクトリ URI の割り当て

次の手順を実行して、ディレクトリ URI をエンドユーザに割り当てます。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザの管理（User Management）]** > **[エンドユーザ（End User）]** を選択します。

ステップ 2 **ユーザの検索/一覧表示（Find and List Users）** ウィンドウで、**検索（Find）** をクリックします。

ステップ 3 リストからユーザを選択します。[エンド ユーザの設定（End User Configuration）] ウィンドウが表示されます。

ステップ 4 この**エンドユーザ**に関連付けるディレクトリ URI を入力します。ディレクトリ URI は電子メールアドレスに似ており、user@host 形式で指定されます。

（注） ディレクトリ URI を入力し、さらに **[プライマリ内線（Primary Extension）]** フィールドに電話番号を入力すると、このディレクトリ URI は自動的に、その電話番号に関連付けられているプライマリ ディレクトリ URI になります。

ステップ 5 [保存（Save）] をクリックします。

ディレクトリ URI とディレクトリ番号の関連付け

ディレクトリ URI をディレクトリ番号に関連付けるには、次の手順を実行します。ディレクトリ番号を電話に割り当てると、Cisco Unified Communications Manager では、ディレクトリ URI を使用してその電話にダイヤルできます。

始める前に

ユーザへのディレクトリ URI の割り当て （246 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。[電話の検索と一覧表示（Find and List Phones）] ウィンドウが表示されます。

ステップ 2 フィルタ条件を指定し、[検索（Find）] をクリックします。

ステップ 3 ディレクトリ番号を関連付けるデバイスをクリックします。[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 [関連付け（Association）] ペインで以下を実行します。

- 既存のディレクトリ番号をクリックします。
- ディレクトリ番号が設定されていない場合、[新しい DN を追加（Add a new DN）] をクリックします。

ステップ 5 [ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウで、[URI] テキストボックスにディレクトリ URI アドレスを入力します。

ステップ 6 [パーティション（Partition）] ドロップダウン リストから、ディレクトリ URI が属するパーティションを選択します。

ユーザが入力するディレクトリ URI は、選択したパーティション内で一意であることを確認します。URI へのアクセスを制限しない場合、パーティションに対して [なし（None）] を選択します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

デフォルトディレクトリ URI パーティションの割り当て （248 ページ）

デフォルトディレクトリ URI パーティションの割り当て

デフォルトのディレクトリ URI パーティションを割り当てるには、次の手順を実行します。

始める前に

ディレクトリ URI とディレクトリ番号の関連付け （247 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[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 パラメータ設定（Enterprise Parameters Configuration）] ウィンドウが表示されます。

ステップ 2 **「最終ユーザパラメータ」**エリアのディレクトリuriの別名**パーティション**については、既存の検索空間にある既存のパーティションを選択してください。

ステップ 3 [保存（Save）] をクリックします。

次のタスク

URI ダイヤリング用の SIP プロファイルの設定 （248 ページ）

URI ダイヤリング用の SIP プロファイルの設定

始める前に

デフォルトディレクトリ URI パーティションの割り当て （248 ページ）

手順

ステップ 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。[SIP プロファイルの検索と一覧表示（Find and List VPN Profile）] ウィンドウが表示されます。

ステップ 2 適切な検索条件を入力し、[検索（Find）] をクリックします。既存の SIP プロファイルのリストが表示されます。

ステップ 3 ネットワークに使用する SIP プロファイルを選択します。[SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウが表示されます。

ステップ 4 **ドロップダウン リスト**から、次のオプションのいずれかを選択します。

- [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）]：URI アドレスを着信コールのアドレスとして処理するには、このオプションを選択します。
- [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））]：SIP ID ヘッダーのユーザ部分のすべての文字がこの範囲に含まれる場合は、このオプションを選択して、着信コールを電話番号として扱います。アドレスのユーザ部分で、この範囲外の文字を使用している場合は、アドレスは URI として扱われます。
- [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））]：SIP ID ヘッダーのユーザ部分のすべての文字がこの範囲に含まれる場合は、このオプションを選択して、着信コールを電話番号として扱います。アドレスのユーザ部分で、この範囲外の文字を使用している場合は、アドレスは URI として扱われます。

ステップ 5 ネットワーク内のすべての SIP プロファイルの [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。

ステップ 6 [設定の適用（Apply Config）] をクリックします。

次のタスク

URI ダイヤリング用の SIP トランクの設定 （249 ページ）

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

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

ステップ 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。

ステップ 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。

ステップ 4 [保存（Save）] をクリックします。

SIP ルート パターンの設定

クラスタ間のディレクトリ URI コールをルーティングするには SIP ルート パターンを設定する必要があります。

SIP ルート パターンを設定するには、次の手順に従います。

始める前に

URI ダイヤリング用の SIP トランクの設定 （249 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[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。

ステップ 2 次のいずれかのオプションを選択します。

- 新しい SIP ルート パターンを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存の SIP ルート パターン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 SIP ルート パターンを選択します。

ステップ 3 [SIP ルート パターンの設定（SIP Route Pattern 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。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

（省略可） ディレクトリ URI カタログのインポート （251 ページ）

ディレクトリ URI カタログのインポート

Cisco Unified Communications Manager により、グローバル ダイヤル プランを CSV ファイルから ILS ネットワークのハブ クラスタにインポートできます。ILS はインポートしたグローバル ダイヤル プランのデータを ILS ネットワーク全体に複製して、Cisco Unified Communications Manager が Cisco TelePresence Video Communications Server や サードパーティ コール制御システムと相互運用できるようにします。

（省略可）ディレクトリ URI カタログをインポートするには、次の手順を実行します。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 10 [保存（Save）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

第 IV 部

コール アドミッション制御の設定

第 28 章

コール アドミッション制御の概要

コール アドミッション制御について

コール アドミッション制御は、WAN リンク上でユーザが期待するレベルの音声品質を維持する場合に使用します。

リンク上に存在するアクティブ コール数が増えすぎて帯域幅の使用量が過剰になると、音声品質が低下し始める場合があります。コールアドミッション制御は、特定のリンク上で同時にアクティブにするコール数を制限することにより、音声品質を調整します。コールアドミッション制御を使用して、リンク上で特定レベルの音質を保証することはできませんが、リンク上のアクティブ コールが消費する帯域幅を調整できます。

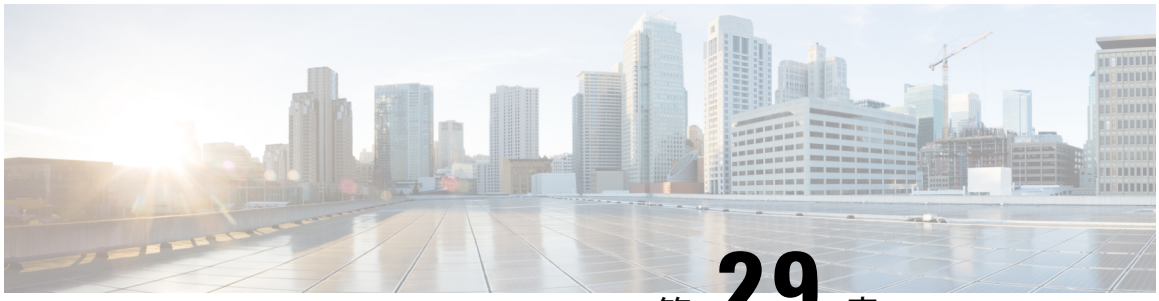
コール アドミッション制御は、帯域幅とポリシーでコールを拒否することによって機能します。コールがコールアドミッション制御によって拒否された場合、着信側の電話機は呼び出し音が鳴らず、発信者にはビジー音が聞こえます。また、発信者には、電話機に「帯域幅不足です」などのメッセージが表示されます。自動代替ルーティング (AAR) を有効にしている場合、コール受付制御は、WAN 帯域を利用できないときに、代替公衆交換電話網 (PSTN) の着信コールを自動的に diverts します。

コール アドミッション制御の設定

コール アドミッション制御（CAC）を実装するには、次のいずれかのタスク フローを選択します。

コール アドミッション制御の設定

タスク フロー	説明
拡張ロケーションコールアドミッション制御のタスク フロー	複数のクラスタが同じ WAN アップリンクを使用して同じ物理サイトのデバイスを管理する、分散導入環境では拡張ロケーション CAC を使用します。拡張ロケーション CAC により、ロケーション間のリンク上のコールに使用可能な帯域幅を制限して、音声品質を調整できます。さらに、TelePresence などのイマーシブ ビデオ コールに対してコール アドミッションを他のビデオ コールとは別に制御できます。
RSVP の設定タスク フロー	RSVP を使用して、IP テレフォニーやビデオ会議アプリケーションを含む複雑な、複数の階層型トポロジにおいてコール アドミッション制御を実装します。RSVP でも帯域幅を動的に変更できます。



第 29 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

拡張場所コール受付制御 (CAC) を使用すると、複雑な WAN トポロジに加え、複数のクラスタが同じアップリンクを使用して同じ物理サイトのデバイスを管理する分散導入の WAN 帯域幅を制御できます。拡張位置の位置CACでは、他のビデオコールとは別のテレプレゼンスなど、イマーシブビデオコールのコールの入園を制御することもできます。

これにより、クラスタが互いに通信し、ロケーションに割り当てられている帯域幅をクラスタ間で予約、解放、および調整でき、クラスタ間のロケーションを「共有」できるようになります。[1]

ネットワーク モデリング

システムでメディアをどのように処理するかを定義するには、場所とリンクの概念を中心としたネットワークモデルを構成します。

場所は、ローカルエリアネットワーク (LAN) を表します。エンドポイントを包含したり、WAN ネットワーク モデリングのリンク間の通過ロケーションとして機能したりできます。

[1] 場所メディア資源オーディオビットレート方針：このパラメータは、トランスコーダなどのメディアリソースがメディア経路に挿入された場合とより複雑なシナリオの場合に、オーディオ専用コールの相手のロケーション内およびロケーション間のオーディオ帯域幅プールから削減するビット レート値を決定します。このサービス パラメータは、いずれかのコールレッグにメディアが存在しない場合、何の影響も及ぼしません。このような場合、場所の帯域幅マネージャーは、その場所の利用可能な帯域幅から送信元の宛先に対して設定されている最大ホップ帯域幅を deducts します。

リンク相互接続位置は、位置間の利用可能な帯域幅を定義するために使用される。リンクはWAN リンクを表します。

重量は、帯域幅経路の測定です。重み付けは「コスト」を「有効経路」に割り当てるためにリンク上で使用されます。重み付けは任意の2ロケーション間の経路が複数存在する場合にのみ適用されます。

システムは、すべての場所からすべての場所に対して最短のパス(コスト)を計算し、有効なパスを作成します。これらは、全体的な重量が最小で、最も効率的な経路です。

システムは、ネットワークモデルが示すリンクの帯域幅を、元の場所から終端位置に追跡します。

ロケーション帯域幅マネージャ

位置帯域幅マネージャー (LBM) サービスは、ソースの場所から移行先の場所への実効パスを計算します。この機能は、Unified Communications Manager のコール制御による帯域幅要求の処理や、クラスタ内およびクラスタ間での帯域幅情報のレプリケートなど、内部の便利な機能を提供します。この機能によって、この機能が保守管理に提供する設定情報およびリアルタイム情報を見つけることができます。

場所メディア資源オーディオビットレート方針：このパラメータは、トランスコーダなどのメディアリソースがメディア経路に挿入された場合とより複雑なシナリオの場合に、オーディオ専用コールの相手のロケーション内およびロケーション間のオーディオ帯域幅プールから削減するビット レート値を決定します。このサービス パラメータは、いずれかのコールレッグにメディアが存在しない場合、何の影響も及ぼしません。このような場合、場所の帯域幅マネージャーは、その場所の利用可能な帯域幅から送信元の通知先に設定されている最大ホップ帯域幅を deducts します。

（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、サーバーの CPU 使用率が不必要に急増する可能性があります。

クラスタ間拡張ロケーションのコール アドミッション コントロール

クラスタによる拡張機能は、拡張された場所の CAC ネットワークモデリングを複数のクラスタにわたって拡張します。各クラスタは、独自のネットワークトポロジを管理します。次に、それらのトポロジをlbmトランクレプリケーションネットワークで設定されている他のクラスタに propogate します。

共有場所は、LBM レプリケーションネットワークに参加しているクラスタに同じ名前で設定されている場所です。

この場所の種類は、次の目的で使用されます。

- クラスタが、設定された各トポロジーを互いに共有できるようにする
- 同じ場所で CAC を実行するには、複数のクラスタを使用します。

拡張ロケーションコールアドミッション制御の前提条件

- 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、クラスタの中で拡張された位置には、CAC では、システムシャドウの場所 (他の場所へのリンクを持たず、帯域の割り当てを行わない) に割り当てられた SIP インタークラスタトランクが必要です。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。
- Unified Communications Manager および LBM は、メディア リソースの帯域幅は管理しません。メディア リソースがコールの帯域幅要件を変更した場合は、カスタマーが最小帯域幅と最大帯域幅のどちらを予約するかを決定するグローバル オプション設定を変更できます。

拡張ロケーション コール アドミッション制御のタスクフロー

手順

	コマンドまたはアクション	目的
ステップ 1	LBM サービスの有効化 （261 ページ）	Cisco Location Bandwidth Manager サービスが有効化されているか確認します。新しいシステムをインストールする場合、任意のノードのサービスを手動で有効にする必要があります。拡張ロケーション CAC が正常に動作するには、このサービスのインスタンスが各クラスタで実行されている必要があります。
ステップ 2	LBM グループの作成 （261 ページ）	LBM が同じノードで実行されていない場合は、LBM グループを設定し、サーバにこの LBM グループを割り当てます。LBM グループでは、ネットワークの遅延およびパフォーマンスを最適化できます。各サーバは、LBM サービスと通信して、各コールで使用可能な帯域幅を特定し、各通話時間の帯域幅を除外します。
ステップ 3	ロケーションとロケーション リンクの設定 （262 ページ）	一元化されたコール処理システムで実装コール アドミッション制御を実装する

	コマンドまたはアクション	目的
		ロケーションを設定します。ロケーションは、ローカル エリア ネットワーク（LAN）を表しており、エンドポイントを含むか、ワイドエリア ネットワーク（WAN）のネットワーク モデリングのリンク間の中継場所として機能します。ロケーションでは、ロケーション内部だけでなく、ロケーションの内外でも帯域幅アカウンティングを使用できます。リンクでは、ロケーションとインターコネクト ロケーション間の帯域幅アカウンティングを使用できます。
ステップ 4	（任意） ロケーション間帯域幅の割り当て （263 ページ）	デフォルトの無制限帯域幅が不要になった場合は、内部ロケーションの帯域幅をロケーションに割り当てます。デフォルトでは、新しいロケーションを作成すると、オーディオ帯域幅が無制限、ビデオ帯域幅が 384 kbps、実体験ビデオ帯域幅は 384 kbps で、新しく追加したロケーションから Hub_None へのリンクも追加されます。この再割り当てを調整して、ネットワーク モデルに一致させることができます。
ステップ 5	外部通信の確立 （263 ページ）	ハブとして機能する LBM サーバで、リモート クラスタの LBM サーバを検索できるように、LBM ハブ グループを設定します。この手順では、このクラスタとの外部通信を確立します。LBM ハブ グループが割り当てられると、LBM サービスはハブとして機能します。LBM ハブ グループが割り当てられている LBM サービスはすべて、同じ、または重複する LBM ハブ グループが割り当てられているその他すべての LBM サーバとの通信を確立します。
ステップ 6	拡張ロケーション コール アドミッション向け SIP クラスタ間トランクの設定 （264 ページ）	SIP クラスタ間トランク（ICT）をシャドウ ロケーションに割り当て、適切なクラスタ間オペレーションを確立します。SIP トランクが、SIP ゲートウェイなどの特定のロケーションのデバイスにリンクされている場合は、通常のロケー

	コマンドまたはアクション	目的
		ションに割り当てることができます。シャドウ ロケーションは、他のロケーションへのリンクを含まず、帯域幅も割り当てられていない特別なロケーションです。
ステップ 7	（任意） ビデオ通話の音声プールからの音声帯域幅の控除 （265 ページ）	オーディオ帯域幅とビデオ帯域幅の除外分をビデオ コール用の別のプールに分割する場合は、次の手順を使用します。デフォルトでは、ビデオ プールの音声ストリームとビデオ ストリームの両方の帯域幅要件が、システムによってビデオ コール用に差し引かれます。

LBM サービスの有効化

Cisco Location Bandwidth Manager サービスが有効化されているか確認します。新しいシステムをインストールする場合、任意のノードのサービスを手動で有効にする必要があります。拡張ロケーション CAC が正常に動作するには、このサービスのインスタンスが各クラスタで実行されている必要があります。

手順

ステップ 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。

ステップ 2 [サーバ（Server）] ドロップダウン リストからサーバを選択し、[移動（Go）] をクリックします。

ステップ 3 必要に応じて、[Cisco Location Bandwidth Manager] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

LBM グループの作成

LBM が同じノードで実行されていない場合は、LBM グループを設定し、サーバにこの LBM グループを割り当てます。LBM グループでは、ネットワークの遅延およびパフォーマンスを最適化できます。各サーバは、LBM サービスと通信して、各コールで使用可能な帯域幅を特定し、各通話時間の帯域幅を除外します。

手順

ステップ 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 グループ（Location Bandwidth Manager Group）]** を選択します。

ステップ 2 次のいずれかの操作を実行します。

- 既存の LBM グループの設定を変更するには、[検索（Find）] をクリックし、結果のリストから既存の LBM グループを選択します。
- 新しい LBM 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。

ステップ 3 [Location Bandwidth Manager グループの設定（Location Bandwidth Manager 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。

ステップ 4 [保存（Save）] をクリックします。

ロケーションとロケーション リンクの設定

一元化されたコール処理システムで実装コールアドミッション制御を実装するロケーションを設定します。ロケーションは、ローカル エリア ネットワーク（LAN）を表しており、エンドポイントを含むか、ワイドエリア ネットワーク（WAN）のネットワーク モデリングのリンク間の中継場所として機能します。ロケーションでは、ロケーション内部だけでなく、ロケーションの内外でも帯域幅アカウンティングを使用できます。リンクでは、ロケーションとインターコネクト ロケーション間の帯域幅アカウンティングを使用できます。

手順

ステップ 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。

ステップ 2 次のいずれかの操作を実行します。

- 既存のロケーションの設定を変更するには、[検索（Find）] をクリックし、結果のリストから既存のロケーションを選択します。
- **[追加（Add）]** をクリックして、カタログに新しい項目を追加します。

ステップ 3 [ロケーションの設定（Location 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。

ステップ 4 [保存（Save）] をクリックします。

ロケーション間帯域幅の割り当て

デフォルトの無制限帯域幅が不要になった場合は、内部ロケーションの帯域幅をロケーションに割り当てます。デフォルトでは、新しいロケーションを作成すると、オーディオ帯域幅が無制限、ビデオ帯域幅が 384 kbps、実体験ビデオ帯域幅は 384 kbps で、新しく追加したロケーションから Hub_None へのリンクも追加されます。この再割り当てを調整して、ネットワークモデルに一致させることができます。

ヒント　音声品質が悪い場合、または途切れる場合は、帯域幅の設定を低くします。たとえば、ISDN の場合は、56 kbps または 64 kbps の倍数を使用します。

手順

ステップ 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。

ステップ 2　検索条件を入力し、[検索（Find）] をクリックして、表示された一覧からユーザを選択します。

ステップ 3　[詳細表示（Show Advanced）] をクリックし、内部ロケーションの帯域幅フィールドを表示します。

ステップ 4　必要に応じて、[オーディオの帯域幅（Audio Bandwidth）] の [kbps] オプション ボタンを選択し、テキスト ボックスに帯域幅の値を入力します。

ステップ 5　必要に応じて、[ビデオの帯域幅（Video Bandwidth）] の [kbps] オプション ボタンを選択し、テキストボックスに帯域幅の値を入力します。

ステップ 6　必要に応じて、[イマーシブビデオの帯域幅（Immersive Video Bandwidth）] の [kbps] オプション ボタンを選択し、テキストボックスに帯域幅の値を入力します。

ステップ 7　[保存（Save）] をクリックします。

外部通信の確立

ハブとして機能する LBM サーバで、リモート クラスタの LBM サーバを検索できるように、LBM ハブ グループを設定します。この手順では、このクラスタとの外部通信を確立します。LBM ハブ グループが割り当てられると、LBM サービスはハブとして機能します。LBM ハブ グループが割り当てられている LBM サービスはすべて、同じ、または重複する LBM ハブ グループが割り当てられているその他すべての LBM サーバとの通信を確立します。

手順

ステップ 1　Cisco Unified CM Administration から、**[システム（System）] > [ロケーション情報（Location Info）] > [Location Bandwidth Manager（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。

ステップ 2 次のいずれかの操作を実行します。

- LBM クラスタ間レプリケーション グループの設定を変更するには、[検索（Find）] をクリックして、結果のリストから既存の LBM クラスタ間レプリケーション グループを選択します。
- 新しい LBM クラスタ間レプリケーション 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。

ステップ 3 [Location Bandwidth Managerのクラスタ間レプリケーショングループの設定（Location Bandwidth Manager Intercluster Replication 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。

ステップ 4 [保存（Save）] をクリックします。

拡張ロケーション コール アドミッション向け SIP クラスタ間トランクの設定

SIP クラスタ間トランク（ICT）をシャドウ ロケーションに割り当て、適切なクラスタ間オペレーションを確立します。SIP トランクが、SIP ゲートウェイなどの特定のロケーションのデバイスにリンクされている場合は、通常のロケーションに割り当てることができます。シャドウ ロケーションは、他のロケーションへのリンクを含まず、帯域幅も割り当てられていない特別なロケーションです。

始める前に

SIP 間クラスタトランクが設定されている必要があります。詳細については、「SIP トランクの設定タスク フロー （117 ページ）」を参照してください。

手順

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

ステップ 2 検索条件を入力し、[検索（Find）] をクリックし、結果リストから既存の SIP クラスタ間トランクを選択します。

ステップ 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。

ステップ 4 [保存（Save）] をクリックします。

ビデオ通話の音声プールからの音声帯域幅の控除

オーディオ帯域幅とビデオ帯域幅の除外分をビデオ コール用の別のプールに分割する場合は、次の手順を使用します。デフォルトでは、ビデオ プールの音声ストリームとビデオ ストリームの両方の帯域幅要件が、システムによってビデオ コール用に差し引かれます。

（注） この機能を有効にすると、CACには、IPまたはUDPネットワークオーバーヘッドに必要な帯域幅が、オーディオ帯域幅控除に含まれます。この音声帯域幅の減少は、オーディオビットレートとIP/UDPネットワークオーバーヘッド帯域幅の要件に相当します。ビデオ帯域幅の控除はビデオのビットレートにすぎません。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 [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、[ビデオ コール用音声プールからオーディオ帯域幅部分を除外する（Deduct Audio Bandwidth Portion from Audio Pool for a Video Call）] サービス パラメータ値を [True] に設定します。

（注） **ビデオコール**サービスパラメータの [オーディオプール (差し引く audio 帯域幅)] パラメータをTrueに設定すると、ビデオおよびイマーシブビデオパラメータは、セッションレベルではなく、メディアレベルと見なされます。したがって、ビデオコールの場合、リージョンとロケーションごとに音声とビデオプールから音声とビデオの帯域場を個別に割り当てることができます。ビデオおよびイマーシブ ビデオの帯域幅制限は、音声とビデオ メディア ストリームの組み合わせではなく、ビデオ メディア ストリームにのみ適用されます。

ステップ 5 [保存（Save）] をクリックします。

拡張ロケーション コール アドミッション コントロールの連携動作および制限

拡張ロケーションのコール アドミッション コントロールの連携動作

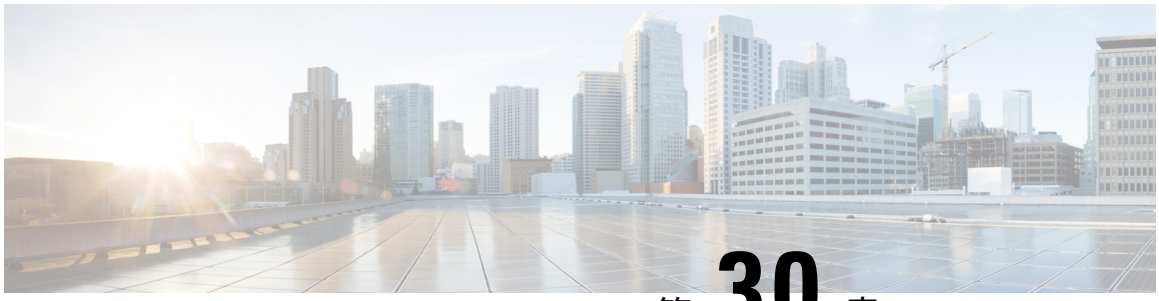
表 *18 :* 拡張ロケーションのコール アドミッション コントロールの連携動作

機能	連携動作
帯域幅	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。

拡張ロケーション コール アドミッション制御の制限

表 *19 :* 拡張ロケーション コール アドミッション コントロールの制限

制限事項	説明
帯域予約	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。
帯域幅とビデオ機能	ビデオ機能が有効になっている場合、音声の帯域幅はビデオから割り当てられます。
同期	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。



第 30 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
ステップ 1	クラスタ全体のデフォルト RSVP ポリシーの設定 （268 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。
ステップ 2	ロケーション ペア RSVP ポリシーの設定 （269 ページ）	（省略可）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。
ステップ 3	RSVP の再試行の設定 （270 ページ）	RSVP の再試行の頻度と番号を設定します。
ステップ 4	コール中の RSVP エラー処理の設定 （271 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。
ステップ 5	MLPP から RSVP への優先レベル マッピングの設定 （272 ページ）	（省略可）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。
ステップ 6	RSVP エージェントの設定	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。
ステップ 7	アプリケーション ID の設定 （273 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。
ステップ 8	DSCP マーキングの設定 （274 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

ステップ 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。

ステップ 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。

ステップ 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 （269 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 （270 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （270 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 （268 ページ）
- （省略可） ロケーション ペア RSVP ポリシーの設定 （269 ページ）

手順

ステップ 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。

ステップ 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。

ステップ 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 （271 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 （270 ページ）

手順

ステップ 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。

ステップ 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。

ステップ 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。

- （省略可）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 （272 ページ）」に進みます。
- アプリケーション ID の設定 （273 ページ）

MLPP から RSVP への優先レベル マッピングの設定

（省略可）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

ステップ 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。

ステップ 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。

ステップ 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 （273 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （274 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 （273 ページ）

手順

ステップ 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。

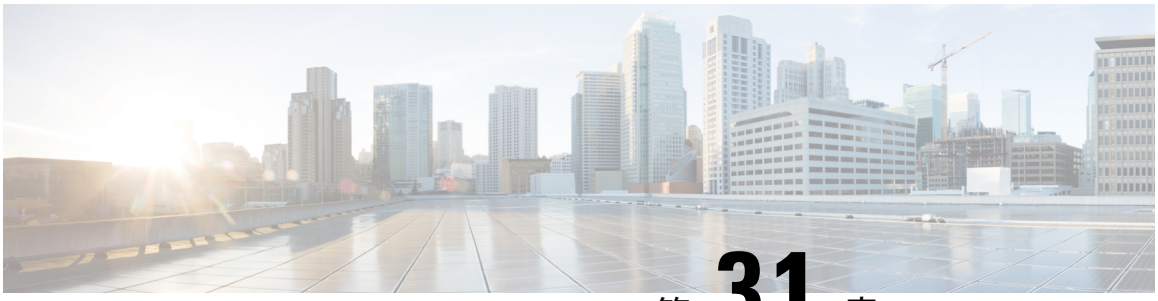
ステップ 2 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 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。

ステップ 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 V 部

エンド ユーザの設定



第 31 章

エンド ユーザの設定の概要

エンドユーザの設定について

このパートの各章では、システムのエンドユーザをプロビジョニングおよび設定する方法について説明しています。

エンドユーザは、Cisco Unified Communications Manager 機能の主な利用者です。エンドユーザは、電話機やディレクトリの番号を使用して割り当てることができるため、エンドユーザはコールを行ったり、システム内の他のユーザとやり取りしたり、PSTN などの外部ネットワークにコールを配置したりすることができます。

一度に多数のエンドユーザをプロビジョニングするために、Cisco Unified Communications Manager には次の機能が用意されています。

- LDAP ディレクトリの統合: Cisco Unified Communications Manager を外部の LDAP ディレクトリと同期して、LDAP ディレクトリからエンドユーザデータをインポートできるようにします。
- 一括管理ツール:一括管理ツールを使用すると、多数のエンドユーザ、関連付けられたユーザデータを 1 回の操作で CSV ファイルからインポートして設定することができます。

エンドユーザがプロビジョニングされた後、電話サービス、クレデンシャルポリシーに加え、ユーザが自身の電話をプロビジョニングできるようにユーザプロファイルなどのユーザ設定を設定できます。

エンド ユーザの設定

次のタスク フローを実行すると、システムのエンド ユーザを設定できます。

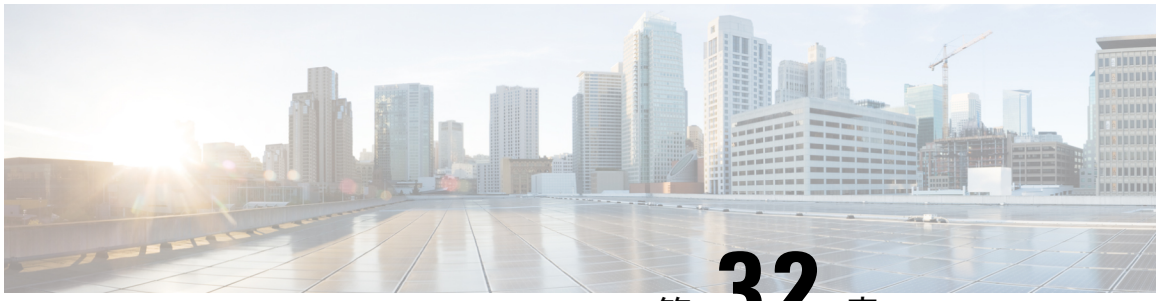
エンド ユーザの設定

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザ アクセスの設定タスク フロー（284 ページ）	エンド ユーザのロールとアクセス制御グループを計画します。システム定義されたロールおよびアクセス制御グループに、導入に必要なアクセス権限を付与するかどうかに加え、新しいロールおよびアクセス制御グループを作成する必要があるかどうかを決定します。
ステップ 2	クレデンシャル ポリシーの設定タスク フロー （307 ページ）	エンド ユーザのクレデンシャル ポリシーを設定します。
ステップ 3	ユーザ プロファイルの設定タスク フロー （312 ページ）	アクセスと機能に関する同じ要件を満たすユーザのグループにユーザ プロファイルを設定します。ユーザ プロファイルは、共通の電話および電話回線設定で構成されており、ユーザ プロファイルを使用するユーザ向けに新しい電話や電話回線をすばやく設定できます。このプロファイルを使用するユーザ向けにセルフプロビジョニングを有効化できます。
ステップ 4	サービス プロファイルの設定タスク フロー （318 ページ）	Unified Communications（UC）サービスの設定で、サービス プロファイルを設定します。このサービス プロファイルは、同じサービス要件が設定されているユーザのグループに適用できます。サービス プロファイルでは、このサービス プロファイルを使用するユーザ向けにプロビジョニングされている新しい電話向けに UC サービスを設定できます。
ステップ 5	機能グループ テンプレートの設定 （328 ページ）	（省略可）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には、一般的な機能の設定と、ユーザプロファイルとサービスプロファイルを割り当てることができます。LDAP 同期ユーザの場合、LDAP 同期中に機能グループ テンプレートを割り当てられるため、ユーザ プロファイル、サービス プロファイル、回線およびサービステンプレート、セルフプロビジョニング機能がユーザに割り当てられます。

	コマンドまたはアクション	目的
ステップ 6	LDAP 同期の設定タスク フロー （334 ページ）	会社用 LDAP ディレクトリを導入する場合は、カンパニー ディレクトリ (LDAP) からエンド ユーザを Cisco Unified Communications Manager データベースに直接インポートできます。
ステップ 7	LDAP 同期の設定タスク フロー （334 ページ）	LDAP ディレクトリからエンド ユーザをインポートしていない場合は、一括管理ツールを使用して、エンド ユーザ リストやエンド ユーザ設定を CSV ファイルで Cisco Unified Communications Manager データベースにインポートできます。 一括管理ガイドを使用して、データベースにバルク トランザクションを実行する方法については、『*Cisco Unified Communications Manager* 一括管理ガイド』（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。
ステップ 8	エンド ユーザの手動設定タスク フロー （346 ページ）	（省略可）データベースに手動で新しいユーザを追加します。

エンド ユーザの設定



第 32 章

ユーザ アクセスの設定

ユーザ アクセスの概要

次の項目を設定して、Cisco Unified Communications Manager に対するユーザ アクセスを管理します。

- [アクセス制御グループ（Access Control Groups）]
- [ロール（Roles）]
- [ユーザ ランク（User Rank）]

ロールの概要

エンドユーザをプロビジョニングする場合、ユーザにどのようなロールを割り当てるか決定する必要があります。ロールはエンドユーザ、アプリケーションユーザ、またはアクセス制御グループに割り当てることができます。単独のユーザに複数のロールを割り当てることができます。

各ロールには、特定のリソースまたはアプリケーションに接続される一連の権限が含まれます。たとえば、標準 CCM エンドユーザのロールは、そのロールが割り当てられているユーザに、Cisco Unified Communications セルフ ケア ポータルへのアクセス権を提供します。また、Cisco Unified Communications Manager の管理、Cisco CDR Analysis and Reporting、Dialed Number Analyzer、CTI インターフェイスなどのリソースへのアクセスを提供するロールを割り当てることもできます。特定の設定ウィンドウのようなグラフィカル ユーザ インターフェイスを使用する大部分のリソースでは、ロールに接続された権限によって、そのウィンドウのデータ、または関連するウィンドウのグループ内のデータを閲覧したり更新できます。

ロールの設定と割り当て

標準ロールをユーザに割り当てるか、またはカスタム ロールを作成するかを決定する必要があります。

- 標準ロール：標準ロールとは、Cisco Unified Communications Manager に最初からインストールされている、デフォルトの事前定義のロールです。ロールの権限を編集または変更することはできません。
- カスタム ロール：カスタム ロールは自分で作成するロールです。ユーザに割り当てる権限を含む標準ロールがないときに、カスタム ロールを作成できます。たとえば、標準ロールを割り当てようとしたが、権限の 1 つを変更したい場合、標準ロールの権限をカスタム ロールにコピーし、そのカスタム ロールで権限を編集できます。

権限のタイプ

各ロールには、特定のリソースに接続される一連の権限が含まれます。リソースに割り当てられる権限には 2 種類あります。

- [読み取り（Read）]：読み取り権限では、ユーザはそのリソースの設定を閲覧できますが、設定を更新することはできません。たとえば、この権限ではユーザが特定の設定ウィンドウの設定を閲覧できますが、そのアプリケーションの設定ウィンドウには更新ボタンやアイコンは表示されません。
- [更新（Update）]：更新権限では、ユーザはそのリソースの設定を変更できます。たとえば、この権限ではユーザが特定の設定ウィンドウで更新を実行できます。

エンドユーザ ロールと管理者ロール

標準 CCM エンドユーザ（Standard CCM End Users）ロールは、Cisco Unified Communications セルフ ケア ポータルへのアクセス権をエンドユーザに提供します。CTI アクセスなどの追加権限については、標準 CTI 対応（Standard CTI Enabled）ロールなどの追加ロールを割り当てる必要があります。

標準 CCM 管理ユーザ（Standard CCM Admin Users）ロールは、すべての処理タスクのベースロールであり、認証ロールとして機能します。このロールは、Cisco Unified Communications Manager Administration のユーザ インターフェイスへの管理者アクセスを提供します。Cisco Unified CM Administration では、このロールを Cisco Unified Communications Manager Administration にログインするために必要なロールとして定義しています。

関連トピック

標準ロールとアクセス制御グループ （290 ページ）

アクセス制御グループの概要

ロールとともにアクセス制御グループを使用して、同様のアクセス要件のユーザ グループにネットワークへのアクセス権限をすばやく指定できます。

アクセス制御グループは、エンドユーザとアプリケーションユーザのリストです。類似したアクセスの必要性を共有するエンド ユーザとアプリケーション ユーザに、必要なロールとアクセス権限を含むアクセス制御グループを指定できます。エンドユーザまたはアプリケーションユーザをアクセス制御グループに割り当てるためには、ユーザがそのアクセス制御グループの最小ランク要件を満たしている必要があります。たとえば、ユーザ ランクが 4 であるユーザは、最小ランク要件が 4 ～ 10 のアクセス制御グループにのみ割り当てることができます。

システムには、一連の事前定義された標準アクセス制御グループが含まれています。それぞれの標準アクセス制御グループには、デフォルトで割り当てられている一連のロールがあります。ユーザをそのアクセス制御グループに割り当てると、それらのロールもそのエンドユーザに割り当てられます。

標準アクセス制御グループに割り当てられたロールは編集できません。ただし、カスタマイズされたアクセス制御グループを作成し、選択したロールをそのカスタマイズされたアクセス制御グループに割り当てることができます。

関連トピック

標準ロールとアクセス制御グループ （290 ページ）

ユーザ ランクの概要

ユーザ ランクのアクセス制御では、管理者がエンド ユーザやアプリケーション ユーザに提供できるアクセス レベルに対する一連の制御を行います。

エンド ユーザやアプリケーション ユーザをプロビジョニングする場合、管理者は各ユーザのユーザ ランクを割り当てる必要があります。管理者は、各アクセス制御グループにもユーザ ランクを割り当てる必要があります。Conttrol グループにアクセスするユーザを追加する場合、管理者は、ユーザのユーザのランク要件がグループのランク要件を満たしているグループにのみユーザを割り当てることができます。たとえば、あるエンド ユーザのユーザ ランクが 3 の場合、3 ～ 10 のユーザ ランクが設定されているアクセス制御グループに割り当てることができます。ただし、管理者は、そのユーザを 1 または 2 のユーザランク要件を持つアクセス制御グループに割り当てることはできません。

管理者は、[ユーザ順位の**設定**] ウィンドウ内に独自のユーザランク階層を作成し、ユーザをプロビジョニングし、アクセス制御グループを使用して、その階層を使用することができます。ユーザランクの階層を設定しない場合や、ユーザをプロビジョニングするとき、または conrol グループにアクセスするときにユーザランクの設定を指定しない場合は、すべてのユーザとアクセス制御グループにはデフォルトのユーザランク 1 (可能な限り高いランク) が割り当てられます。

ユーザ アクセスの前提条件

エンドユーザをプロビジョニングする前に、次のことを実行します。

- 標準ロールとアクセス制御グループ （290 ページ） ：定義済みのロールとアクセス制御グループのリストを確認します。カスタマイズされたロールとグループを設定する必要があるかどうかを判断します。

- ユーザとグループに割り当てるユーザのランクを計画します。

ユーザ アクセスの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザ ランク階層の設定 （285 ページ）	システムのユーザのランク階層を設定します。
ステップ 2	新しいロールを作成する必要がある場合は、次のいずれかの方法を使用します。 • カスタム ロールの作成 （285 ページ） • 既存のロールのコピー （286 ページ）	新しいロールをまったく最初から作成して設定するには、「作成（Create）」手順を実行します。新しいロールが既存のロールと同様の権限を持つ場合は、「コピー（Copy）」手順を実行します。既存のロールから新しいロールに権限をコピーしてから、新しいロールの権限を編集します。
ステップ 3	新しいアクセス制御グループを作成する必要があるときは、次のいずれかの方法を使用します。 • アクセス制御グループの作成 （287 ページ） • アクセス制御グループのコピー （288 ページ）	新しいアクセス制御グループをまったく最初から作成するには、「作成（Create）」手順を実行します。既存のアクセス制御グループに新しいアクセス制御グループと類似の設定があれば、「コピー（Copy）」手順を実行します。既存のアクセス制御グループから新しいグループに設定をコピーしてから編集できます。
ステップ 4	アクセス制御グループへの権限の割り当て （289 ページ）	新しいアクセス制御グループを作成したら、アクセス制御グループにロールを割り当てます。
ステップ 5	重複する権限ポリシーの設定 （290 ページ）	重複するアクセス権限をカバーするには、エンタープライズ ポリシーを設定します。これはエンドユーザやアプリケーションのユーザが複数のアクセス制御グループまたはロールに割り当てられ、それぞれが相反する権限設定になっている場合をカバーしています。

関連トピック

標準ロールとアクセス制御グループ （290 ページ）

ユーザ ランク階層の設定

カスタムのユーザ ランク階層を作成するには、この手順を使用します。

（注） ユーザ ランク階層を設定しない場合は、すべてのユーザおよびアクセス制御グループにデフォルトで 1（最高ランク）が割り当てられます。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザランク（User Rank）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [ユーザランク（User Rank）] ドロップダウン メニューから、1 ～ 10 のランク設定を選択します。最も高いランクは 1 です。

ステップ 4 [ランク名（Rank Name）] と [説明（Description）] を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 ユーザ ランクをさらに追加するには、この手順を繰り返します。
ユーザおよびアクセス制御グループにユーザ ランクを割り当てることで、ユーザをどのグループに割り当てることができるかを制御できます。

カスタム ロールの作成

必要な権限設定を備えたシステム定義のロールがないとき、カスタム ロールを作成します。

ヒント 自分が作成する新しいロールの権限が既存のロールの権限に似ている場合、「既存のロールのコピー（286ページ）」の手順を実行して、編集可能な新しいロールに既存の権限をコピーします。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [権限（Role）]** をクリックします。

ステップ 2 次のいずれかを実行します。

- 新しいロールを作成するには、**[新規追加（Add New）]** をクリックします。このロールを関連付ける [アプリケーション（Application）] を選択し、[次へ (Next)] をクリックします。

- 既存のロールから設定をコピーするには、[検索（Find）] をクリックして、既存のロールを開きます。[コピー（Copy）] をクリックし、新しいロールの名前を入力します。[OK] をクリックします。

ステップ 3 このロールの [名前（Name）] と [説明（Description）] を入力します。

ステップ 4 リソースごとに、該当するチェックボックスをオンにします。

- ユーザがリソースの設定を表示できるようにする場合には、[読み取り（Read）] チェックボックスをオンにします。
- ユーザがリソースの設定を編集できるようにする場合は、[更新（Update）] チェックボックスをオンにします。
- リソースに対するアクセスを提供しない場合は、両方のチェックボックスをオフにします。

ステップ 5 この権限のページに表示されるすべてのリソースに特権を付与する場合は、[すべてにアクセス権を付与（Grant access to all）] ボタンをクリックし、すべてのリソースから特権を削除する場合は、[すべてにアクセスを許可しない（Deny access to all）] をクリックします。

（注） リソースのリストが複数のページにわたって表示される場合、このボタンは、現在のページに表示されるリソースに限り適用されます。他のページのリストにあるリソースのアクセス権を変更するには、それらのページを表示し、表示されたページでこのボタンを使用する必要があります。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

アクセス制御グループの作成 （287 ページ）

既存のロールのコピー

[コピー（Copy）] コマンドを使用すると、既存のロール設定に基づいて、新しいロールを作成できます。Cisco Unified Communication Manager では、標準ロールを編集できません。ただし、[コピー（Copy）] コマンドで標準ロールとリソースと権限が同一の新しいロールを作成できます。そして自分が作成した新しいロールの権限を編集できます。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ロール（Role）]** をクリックします。

ステップ 2 [検索（Find）] をクリックし、コピーするリソースと権限が含まれるロールを選択します。

ステップ 3 [コピー（Copy）] をクリックします。

ステップ 4 新しいロールの名前を入力し、[OK] をクリックします。

[ロールの設定（Role Configuration）] ウィンドウに新しいロールの設定が表示されます。新しいロールの権限は、コピーしたロールの権限と同じです。

ステップ 5 新しいロールのリソースのいずれかで、次のようにして権限を編集します。

- [読み取り（Read）]チェックボックスをオンにして、ユーザにリソースの表示を許可します。
- [更新（Update）] チェックボックスをオンにして、ユーザにリソースの編集を許可します。
- リソースへのアクセスを制限するには、両方のチェックボックスをオフにします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

次のいずれかの方法で新しいアクセス制御グループを作成します。

- アクセス制御グループの作成 （287 ページ）
- アクセス制御グループのコピー （288 ページ）

関連トピック

標準ロールとアクセス制御グループ （290 ページ）

アクセス制御グループの作成

この手順では、新しいアクセス制御グループを作成する必要があります。システム定義アクセス制御グループが導入環境のニーズを満たさない場合、新しいアクセス制御グループを作成する必要があります。

始める前に

新しいロールを作成する必要がある場合は、次のいずれかの手順を実行します。

- カスタム ロールの作成 （285 ページ）
- 既存のロールのコピー （286 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[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）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [名前（Name）] にアクセス制御グループの名前を入力します。

ステップ 4 [ユーザで利用できるユーザランク（Available for Users with User Rank as）] ドロップダウンから、このグループに割り当てる、ユーザの最低ランクを選択します。デフォルトのユーザランクは 1 です。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

アクセス制御グループへの権限の割り当て （289 ページ）

アクセス制御グループのコピー

既存のアクセス制御グループから設定をコピーして、カスタムアクセス制御グループを作成します。既存のアクセス制御グループをコピーすると、システムにより、新しいアクセス制御グループにすべての設定（割り当てた権限やユーザを含む）がコピーされます。ただし、デフォルトのアクセス制御グループとは異なり、カスタムアクセス制御グループに割り当てられた権限は編集できます。

始める前に

新しい権限を作成する必要がある場合、次のステップのいずれかを実行します。

- カスタム ロールの作成 （285 ページ）
- 既存のロールのコピー （286 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[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）]** を選択します。

ステップ 2 [検索（Find）] をクリックして、設定をコピーする対象のアクセス制御グループを選択します。

ステップ 3 [コピー（Copy）] をクリックします。

ステップ 4 新しいアクセス制御グループの名前を入力し、[OK] をクリックします。

ステップ 5 [ユーザで利用できるユーザランク（Available for Users with User Rank as）] ドロップダウンから、このグループに割り当てる、ユーザの最低ランクを選択します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

アクセス制御グループへの権限の割り当て （289 ページ）

関連トピック

標準ロールとアクセス制御グループ （290 ページ）

アクセス制御グループへの LDAP 同期ユーザの割り当て （343 ページ）
アクセス制御グループへのエンド ユーザの割り当て （347 ページ）

アクセス制御グループへの権限の割り当て

作成したすべての新しいアクセス制御グループに権限を割り当てます。既存のグループからアクセス制御グループをコピーした場合、権限の削除が必要になることもあります。

（注） デフォルトで設定されている標準アクセス制御グループの権限の割り当てはいずれも編集できません。

始める前に

新しいアクセス制御グループを作成するには、次のタスクのいずれかを実行します。

- アクセス制御グループの作成 （287 ページ）
- アクセス制御グループのコピー （288 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[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）]** を選択します。

ステップ 2 [検索（Find）] をクリックし、アクセス制御グループを選択します。

ステップ 3 [関連リンク（Related Links）] ドロップダウン リスト ボックスで、[アクセス制御グループへの権限の割り当て（Assign Role to Access Control Group）] を選択し、[移動（Go）] をクリックします。

ステップ 4 権限を割り当てる必要がある場合は、以下の手順に従います。

a) [グループにロールを割り当て（Assign Role to Group）] をクリックします。
b) [権限の検索と一覧表示（Find and List Roles）] ウィンドウで、グループに割り当てる権限の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。

ステップ 5 権限を削除する必要がある場合は、以下の手順に従います。

a) [ロール（Role）] リスト ボックスで、削除する権限を強調表示します。
b) [割り当てたロールの削除（Delete Role Assignment）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

重複する権限ポリシーの設定 （290 ページ）

重複する権限ポリシーの設定

アクセス制御グループの割り当てで重複するユーザ権限を Cisco Unified Communication Manager がどのように処理するのかを設定します。これにより、エンドユーザが複数のアクセス制御グループに割り当てられ、それぞれのロールとアクセス権限が相反する状況に対応できます。

始める前に

アクセス制御グループへの権限の割り当て （289 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[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。

ステップ 2 [ユーザ管理パラメータ（User Management Parameters）] で、[重複したユーザ グループとロールの実質的なアクセス権（Effective Access Privileges For Overlapping User Groups and Roles）] に次のいずれかの値を設定します。

- [最大（Maximum）]—実質的な権限は、重複したすべてのアクセス制御グループの最大限の権限になります。これがデフォルトのオプションです。
- [最小（Minimum）]—実質的な権限は、重複したすべてのアクセス制御グループの最小限の権限になります。

ステップ 3 [保存（Save）] をクリックします。

標準ロールとアクセス制御グループ

次の表は、Cisco Unified Communications Manager にあらかじめ設定されている標準権限およびアクセス制御グループの概要です。標準権限が持つ特権はデフォルトで設定されています。また、標準権限に関連付けられたアクセス制御グループも、デフォルトで設定されています。

標準権限、および標準権限に関連付けられたアクセス制御グループの両方で、特権または権限の割り当てを編集できません。

表 *20 :* 標準権限、特権 およびアクセス制御グループ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 AXL API アクセス	AXL データベース API へのアクセスを許可します。	[標準CCMスーパーユーザー（Standard CCM Super Users）]
標準AXL APIユーザー	AXL API を実行するログイン権限を付与します。	

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 AXL 読み取り専用 API アクセス	AXL 読み取り専用 API（API の一覧表示、API の取得、SQL Query API の実行）の実行をデフォルトで許可します。	
標準管理 Rep Tool 管理	Cisco Unified Communications Manager CDR Analysis and Reporting（CAR）の表示および設定が可能になります。	標準 CAR 管理ユーザー、標準 CCM スーパー ユーザー
標準監査ログ管理	監査ロギング機能の次のタスクを実行できます。 • Cisco Unified Serviceability の [監査ログ設定（Audit Log Configuration）] ウィンドウでの、監査ロギングの表示および設定 • Cisco Unified Serviceability でのトレースの表示と設定、および Real-Time Monitoring Tool の監査ログ機能向けトレースの収集 • Cisco Unified Serviceability での Cisco Audit Event Service の表示、開始、停止 • RTMT での、関連付けられたアラートの表示および更新	標準監査ユーザー
標準 CCM 管理ユーザー	Cisco Unified Communications Manager Administration へのログイン権限を付与します。	標準 CCM 管理ユーザー、標準 CCM ゲートウェイ管理、標準 CCM 電話管理、標準 CCM 読み取り専用、標準 CCM サーバー モニタリング、標準 CCM スーパー ユーザー、標準 CCM サーバー メンテナンス、標準 パケット スニファ ユーザー
[標準CCMエンドユーザー（Standard CCM End Users）]	Cisco Unified Communications セルフケアポータルにログインする権限をエンド ユーザーに付与します。	[標準CCMエンドユーザー（Standard CCM End Users）]

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ

標準 CCM 機能管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。
	• 一括管理ツールによる次の項目の表示、削除、挿入：
	  • クライアント関連のコードと強制承認コード
	  • コール ピックアップ グループ
	• Cisco Unified Communications Manager Administration で、の次の項目を表示、設定できます。
	  • クライアント関連のコードと強制承認コード
	  • コール パーク
	  • コール ピックアップ
	  • ミートミーの番号またはパターン
	  • メッセージ受信
	  • Cisco Unified IP Phone サービス
	  • ボイスメール パイロット、ボイスメール ポート ウィザード、ボイスメール ポート、ボイスメール プロファイル
		[標準CCMサーバーメンテナンス（Standard CCM Server Maintenance）]

標準 CCM ゲートウェイ管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。 • 一括管理ツールによるゲートウェイ テンプレートの表示および設定 • ゲートキーパー、ゲートウェイ、およびトランクの表示および設定	標準 CCM ゲートウェイ管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ

標準 CCM 電話管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。
	• 一括管理ツールによる電話の表示とエクスポート
	• 一括管理ツールによるユーザーデバイスプロファイルの表示と挿入
	• Cisco Unified Communications Manager Administration で、次の項目を表示および設定できます。
	  • BLF 短縮ダイヤル
	  • CTI ルート ポイント
	  • デフォルトデバイスプロファイルまたはデフォルト プロファイル
	  • 電話番号、および回線の状態
	  • ファームウェア ロード情報
	  • 電話ボタンテンプレートまたはソフトキー テンプレート
	  • 電話機
	  • [電話の設定（Phone Configuration）] ウィンドウの [ボタン項目を変更（Modify Button Items）] をクリックすることによる、特定の電話に対する電話ボタンの情報の並べ替え
		標準 CCM 電話管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM ルート プラン計画管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。 • アプリケーション ダイヤル ルールの表示および設定 • コーリング サーチ スペースおよびパーティションの表示および設定 • ダイヤル ルール パターンを含むダイヤル ルールの表示および設定 • ハント リスト、ハント パイロット、回線グループの表示および設定 • ルート フィルタ、ルート グループ、ルート ハント リスト、ルートリスト、ルートパターン、ルート プラン レポートの表示および設定 • 時間帯およびスケジュールの表示および設定 • トランスレーション パターンの表示および設定	

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ

標準 CCM サービス管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。
	• 次の項目を表示および設定できます。
	  • アナンシエータ、会議ブリッジ、トランスコーダ
	  • オーディオ ソースおよび MOH サーバー
	  • メディア リソース グループおよびメディア リソース グループ リスト
	  • Media Termination Point; メディア ターミネーション ポイント
	  • Cisco Unified Communications Manager Assistant ウィザード
	• 一括管理ツールの [マネージャの削除（Delete Managers）]、[マネージャ/アシスタントの削除（Delete Managers/Assistants）] および [マネージャ/アシスタントの挿入（Insert Managers/Assistants）] ウィンドウでの表示および設定ができます。
		[標準CCMサーバーメンテナンス（Standard CCM Server Maintenance）]

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ

標準 CCM システム管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。
	• 次の項目を表示および設定できます。
	  • 代替ルーティング（AAR）グループの自動化
	  • Cisco Unified Communications Manager（Cisco Unified CM）および Cisco Unified Communications Manager グループ
	  • 日時グループ
	  • デバイス デフォルト
	  • デバイス プール
	  • エンタープライズパラメータ
	  • エンタープライズ電話の設定
	  • ロケーション
	  • Network Time Protocol（NTP）サーバー
	  • プラグイン
	  • Skinny Call Control Protocol（SCCP）または Session Initiation Protocol（SIP）を実行する電話用のセキュリティプロファイル、SIP トランク用のセキュリティプロファイル
	  • Survivable Remote Site Telephony（SRST）の参照
	  • サーバー
	• 一括管理ツールの、[ジョブ スケジューラ（Job Scheduler）] ウィンドウでの表示と設定
		標準CCMサーバメンテナンス（Standard CCM Server Maintenance）

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM ユーザー権限管理	Cisco Unified Communications Manager Administration で、アプリケーションユーザの表示および設定を実行できます。	
標準CCMADMIN管理（Standard CCMADMIN Administration）	CCMAdmin システムのすべての面を利用できます。	
標準CCMADMIN管理（Standard CCMADMIN Administration）	Cisco Unified Communications Manager Administration および一括管理ツールのすべての項目を表示および設定できます。	[標準CCMスーパーユーザー（Standard CCM Super Users）]
標準CCMADMIN管理（Standard CCMADMIN Administration）	Dialed Number Analyzer の情報を表示および設定できます。	
標準CCMADMIN読み取り専用（Standard CCMADMIN Read Only）	すべての CCMAdmin リソースの読み取りを許可します。	
標準CCMADMIN読み取り専用（Standard CCMADMIN Read Only）	Cisco Unified Communications Manager Administration および一括管理ツールの項目を表示できます。	標準 CCM ゲートウェイ管理、標準 CCM 電話管理、標準 CCM 読み取り専用、標準 CCM サーバー メンテナンス、標準 CCM サーバー モニタリング
標準CCMADMIN読み取り専用（Standard CCMADMIN Read Only）	Dialed Number Analyzer で、ルーティング設定の分析ができます。	
標準 CCMUSER 管理	Cisco Unified Communications セルフケアポータルへのアクセスを許可します。	標準CCMエンドユーザ（Standard CCM End Users）
標準 CTI 通話モニタリング許可	CTI アプリケーションまたはデバイスでコールをモニターできます。	標準 CTI 通話モニタリング許可

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CTI コール パーク モニタリング許可	CTI アプリケーションまたはデバイスでコールパークを使用できます。 **重要** 開通している回線およびパーク回線の最大数は 65,000 を超えてはなりません。 合計が 65,000 を超える場合は、アプリケーションユーザから Standard CTI Allow Call Park Monitoring ロールを削除するか、設定されているパーク回線の数を減らします。	標準 CTI コール パーク モニタリング許可
標準 CTI 通話録音許可	CTIアプリケーション/デバイスで通話を録音できます。	標準 CTI 通話録音許可
標準 CTI 発信者番号の変更許可	CTI アプリケーションが発信者番号を通話中に変更できます。	標準 CTI 発信者番号の変更許可
標準CTIによるすべてのデバイスの制御	CTI で制御可能なすべてのデバイスを制御できます。	標準CTIによるすべてのデバイスの制御
標準 CTI 接続された転送と会議をサポートする電話の制御許可	接続された転送および会議をサポートするすべてのCTIデバイスを制御できます。	標準 CTI 接続された転送と会議をサポートする電話の制御許可
標準 CTI ロールオーバー モードをサポートする電話の制御許可	ロールオーバーモードをサポートするすべての CTI デバイスを制御できます。	標準 CTI ロールオーバー モードをサポートする電話の制御許可
標準 CTI SRTP 重要素材の受信許可	CTI アプリケーションが、SRTP を使用する重要な素材にアクセスしたり、その素材を配信したりできるようにします。	標準 CTI SRTP 重要素材の受信許可
標準 CTI 対応	CTI アプリケーションの制御を可能にします。	標準 CTI 対応
標準 CTI セキュア接続	Cisco Unified Communications Manager へのセキュアなCTI接続が可能になります。	標準 CTI セキュア接続
標準CUReporting（Standard CUReporting）	アプリケーションユーザーが、さまざまなソースからレポートを作成できます。	

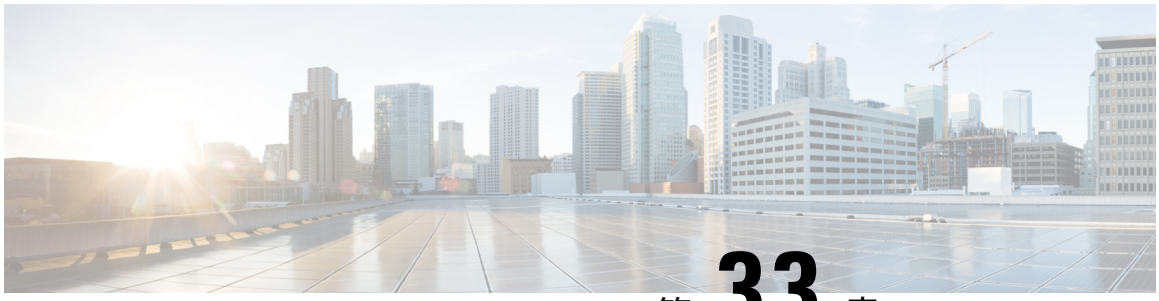
標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準CUReporting（Standard CUReporting）	Cisco Unified Reporting での、レポートの表示、ダウンロード、作成、およびアップロードができます。	標準 CCM 管理ユーザー、標準 CCM スーパー ユーザー
標準 EM 認証プロキシ権限	アプリケーションで使用する Cisco Extension Mobility（EM）の認証権限を管理します。この権限は、（Cisco Unified Communications Manager Assistant や Cisco Web Dialer などの）Cisco Extension Mobility と対話するすべてのアプリケーションユーザに必要です。	標準 CCM スーパー ユーザー、標準 EM 認証プロキシ権限
標準パケット スニッフィング	Cisco Unified Communications Manager の管理にアクセスし、パケットスニッフィング（キャプチャ）ができます。	標準パケット スニファ ユーザー
標準RealtimeAndTraceCollection（Standard RealtimeAndTraceCollection）	Cisco Unified Serviceability および Real-Time Monitoring Tool にアクセスし、次の項目を表示および使用できます。 • Simple Object Access Protocol（SOAP）Serviceability AXL API • SOAP コール レコード API • SOAP 診断ポータル（Analysis Manager）データベース サービス • 監査ログ機能のトレースの設定 • トレース収集などの、Real-Time Monitoring Tool の設定	標準RealtimeAndTraceCollection（Standard RealtimeAndTraceCollection）

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 SERVICEABILITY		標準 CCM サーバー モニタリング、標準 CCM スーパー ユーザー

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
	Cisco Unified Serviceability または Real-Time Monitoring Tool で、次のウィンドウを表示および設定できます。 • [アラーム設定およびアラーム定義（Alarm Configuration and Alarm Definitions）]（Cisco Unified Serviceability） • [監査トレース（Audit Trace）]（読み取りおよび表示のみ可能なマークが付けられています） • SNMP 関連のウィンドウ（Cisco Unified Serviceability） • [トレースの設定（Trace Configuration）] および [トレース設定のトラブルシューティング（Troubleshooting of Trace Configuration）]（Cisco Unified Serviceability） ） • ログパーティションのモニタリング • [アラートの設定（Alert Configuration）]（RTMT）、[プロファイルの設定（Profile Configuration）]（RTMT）、および [トレース収集（Trace Collection）]（RTMT） SOAP Serviceability AXL API、SOAP Call Record API、および SOAP 診断ポータル（Analysis Manager）データベースサービスを表示および使用できます。 SOAP コールレコード API については、RTMT Analysis Manager Call Record の権限が、このリソースを介して制御されます。 SOAP 診断ポータルデータベースサービスについては、RTMT Analysis	

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
	Manager Hosting Database アクセスが、このリソースを介して制御されます。	
標準 SERVICEABILITY 管理	有用性の管理者は、Cisco Unified Communications Manager の管理に表示されるプラグイン ウィンドウにアクセスでき、このウィンドウからプラグインをダウンロードできます。	
標準SERVICEABILITY管理（Standard SERVICEABILITY Administration）	Dialed Number Analyzer の有用性をすべての面で管理できます。	
標準SERVICEABILITY管理（Standard SERVICEABILITY Administration）	Cisco Unified Serviceability および Real-Time Monitoring Tool のすべてのウィンドウを表示および設定できます（[監査トレース（Audit Trace）] では表示のみ可能です）。 すべての SOAP Serviceability AXL API を表示および使用できます。	
標準SERVICEABILITY読み取り専用（Standard SERVICEABILITY Read Only）	Dialed Number Analyzer のコンポーネントで使用する有用性に関するすべてのデータを表示できます。	標準 CCM 読み取り専用
標準SERVICEABILITY読み取り専用（Standard SERVICEABILITY Read Only）	Cisco Unified Serviceability および Real-Time Monitoring Tool で、設定を表示できます。（標準監査ログ管理の権限により表示される監査設定ウィンドウは除きます） SOAP Serviceability AXL API、SOAP Call Record API、および SOAP 診断ポータル（Analysis Manager）データベース サービスをすべて表示できます。	
標準システム サービス管理	Cisco Unified Serviceability で、サービスを表示、アクティベート、開始、および停止できます。	
標準 SSO 設定管理	SAML SSO の設定をすべての面で管理できます。	
標準機密アクセス レベル ユーザー	すべての機密アクセス レベル ページにアクセスできます。	標準 Cisco Call Manager 管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCMADMIN 管理	CCMAdmin システムをすべての面で管理できます。	標準 Cisco Unified CM IM およびプレゼンスの管理
標準CCMADMIN読み取り専用（Standard CCMADMIN Read Only）	すべての CCMAdmin リソースの読み取りを許可します。	標準 Cisco Unified CM IM およびプレゼンスの管理
標準CUReporting（Standard CUReporting）	アプリケーションユーザーが、さまざまなソースからレポートを作成できます。	標準 Cisco Unified CM IM & Presenceのレポーティング



第 33 章

クレデンシャル ポリシーの設定

クレデンシャル ポリシーの概要

クレデンシャル ポリシーは、Cisco Unified Communications Manager 内のリソースの認証プロセスを制御します。クレデンシャルポリシーは、失敗したログイン試行、エンドユーザ パスワードの有効期限とロックアウト期間、エンドユーザ PIN、アプリケーション ユーザ パスワードなどのパスワード要件とアカウント ロックアウトの詳細を定義します。クレデンシャル ポリシーは、すべてのエンド ユーザ PIN などの特定のクレデンシャル タイプのすべてのアカウントに広く割り当てることも、特定のアプリケーション ユーザやエンド ユーザ用にカスタマイズすることもできます。

クレデンシャル タイプ

[クレデンシャル ポリシー設定（Credential Policy Configuration）] で、新しいクレデンシャル ポリシーを設定し、次の 3 つのクレデンシャル タイプのそれぞれのデフォルト クレデンシャル ポリシーとして新しいポリシーを適用できます。

- エンド ユーザ PIN
- エンド ユーザ パスワード
- アプリケーション ユーザ パスワード

また、特定のエンド ユーザ PIN、エンド ユーザ パスワード、またはアプリケーション ユーザ パスワードにクレデンシャル ポリシーを適用することもできます。

LDAP 認証が有効になっている場合のログイン情報ポリシー

社内ディレクトリで LDAP 認証用にシステムが設定されている場合は、次の条件を実行します。

- LDAP 認証が有効になっている場合、ログイン情報ポリシーはエンドユーザパスワードに適用されません。

- ログイン情報ポリシーは、LDAP 認証が有効になっているかどうかに関係なく、エンド ユーザの PIN とアプリケーション ユーザ パスワードに適用されます。これらのパスワードタイプは、ローカル認証を使用します。

（注） クレデンシャル ポリシーは、オペレーティング システムのユーザまたは CLI のユーザには適用されません。オペレーティング システムの管理者は、オペレーティング システムでサポートされている標準のパスワード検証手順を使用します。

単純なパスワード

単純なパスワードと PIN を確認するようにシステムを設定できます。単純なパスワードとは、ABCD や 123456 といった容易に推測できるパスワードなどで、これらは簡単にハッキングできるクレデンシャルです。

単純でないパスワードは、次の要件を満たしています。

- 大文字、小文字、数字、記号の 4 種類の文字のうち 3 種類を含んでいる。
- 3 回以上連続して同じ文字や数字を使用していない。
- 繰り返しや、エイリアス、ユーザ名、内線番号を含んでいない。
- 連続する文字または数字で構成されていない。たとえば、654321 または ABCDEFG などのパスワードは許容されません。

PIN には、数字（0 ～ 9）のみを使用できます。単純でない PIN は、次の条件を満たすものとします。

- 3 回以上連続して同じ数字を使用していない。
- 繰り返しや、ユーザの内線番号、メールボックス、またはユーザの反転させた内線番号やメールボックスを含んでいない。
- 3 つの異なる数字を含んでいる。たとえば、121212 などの PIN は単純です。
- ユーザの姓または名の数字表現（たとえば、名前によるダイヤル）が使用されていない。
- たとえば、408408 などの複数の数字の繰り返しや、2580、159、753 などのキーパッド上で直線上にあるダイヤルのパターンを含んでいない。

クレデンシャル ポリシーの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	クレデンシャル ポリシーの設定 （307 ページ）	エンド ユーザとアプリケーション ユーザにクレデンシャル ポリシーを設定します。
ステップ 2	クレデンシャル ポリシーのデフォルト クレデンシャルの設定 （308 ページ）	3 つのクレデンシャル タイプのいずれか（エンド ユーザ パスワードとアプリケーション ユーザ）にデフォルトのクレデンシャル ポリシーとして設定されているクレデンシャル ポリシーを適用します。デフォルトのクレデンシャル ポリシーは、新規にプロビジョニングされたユーザのクレデンシャル タイプにデフォルトで適用されます。

関連トピック

エンド ユーザへのクレデンシャル ポリシーの適用 （348 ページ）

クレデンシャル ポリシーの設定

エンド ユーザの PIN またはパスワードなどの特定のクレデンシャル タイプに一致するすべてのクレデンシャルのデフォルトのクレデンシャル ポリシーとして適用可能なクレデンシャル ポリシーを設定します。

（注） CTI アプリケーションユーザーに対して、クレデンシャル ポリシー設定の下の **[許可される非アクティブ日数]** パラメータが 0 に設定されていることを確認します。そうしないと、アプリケーションユーザーが予期せず非アクティブになり、再起動後に CTI アプリケーションが Unified CM に接続できないことがあります。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（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。

ステップ 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。

ステップ 3 [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。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

クレデンシャル ポリシーのデフォルト クレデンシャルの設定 （308 ページ）

クレデンシャル ポリシーのデフォルト クレデンシャルの設定

クレデンシャル ポリシーのデフォルト クレデンシャルを設定するには、次の手順を実行します。ユーザが次のログインで変更する必要がある一時的なパスワードを割り当てるために、デフォルト クレデンシャルを割り当てることができます。

始める前に

クレデンシャル ポリシーの設定 （307 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザの管理（User Management）] > [ユーザ設定（User Settings）] > [クレデンシャルポリシーデフォルト（Credential Policy Default）]** を選択します。

ステップ 2 [クレデンシャル ポリシー（Credential Policy）] ドロップダウン リスト ボックスから、このグループのクレデンシャル ポリシーを選択します。

ステップ 3 [クレデンシャルの変更（Change Credential）] と [クレデンシャルの確認（Confirm Credential）] の両方にパスワードを入力します。

ステップ 4 このクレデンシャルをユーザに変更させない場合は、[ユーザは変更不可（User Cannot Change）] チェックボックスをオンにします。

ステップ 5 ユーザが次のログイン時に変更する必要がある、一時的なクレデンシャルを設定する場合は、[次回ログイン時に変更必要（User Must Change at Next Login）] チェックボックスをオンにします。

（注） このボックスをオンにすると、ユーザはパーソナル ディレクトリ サービスを使用して PIN を変更できなくなることに注意してください。

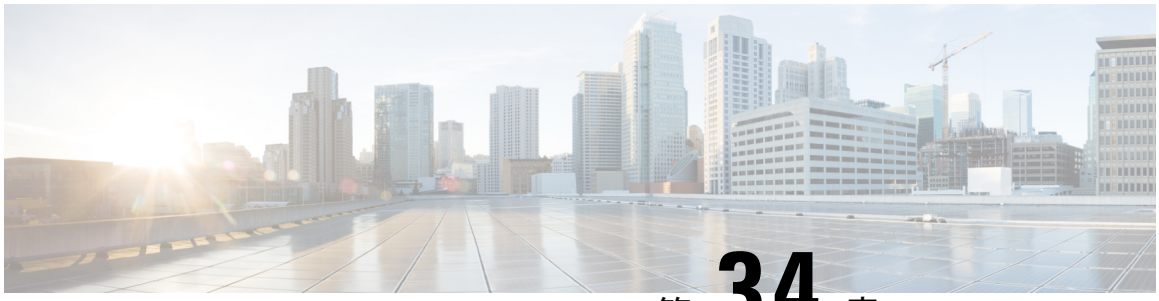
ステップ 6 クレデンシャルの期限を設定しない場合は、[有効期限なし（Does Not Expire）] チェックボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

特定のエンドユーザまたは PIN にクレデンシャル ポリシーを適用する場合：

- エンド ユーザへのクレデンシャル ポリシーの適用 （348 ページ）



第 34 章

ユーザ プロファイルの設定

ユーザプロファイルの概要

ユーザプロファイルには、一般的なディレクトリ番号とデバイスの設定が含まれています。最も一般的なディレクトリ番号の設定と、ユーザが必要とするデバイスの設定を含むさまざまなユーザプロファイルを設定し、各ユーザプロファイルを設定する必要があるユーザに割り当てることができます。各ユーザの電話回線と電話の設定要件に応じて、社内のユーザグループごとに異なるユーザプロファイルを設定できます。

セルフプロビジョニングが有効になっているエンドユーザに対して、ユーザプロファイルからの電話機と電話回線の設定は、ユーザがプロビジョニングするすべての新しい電話機に適用されます。ユーザがセルフプロビジョニングに対応していない場合、ユーザプロファイルの設定は、エンドユーザの代わりに管理者がプロビジョニングした任意の新しい電話機に適用できます。

ユーザプロファイルは、次の電話機と電話回線テンプレートの設定を使用してエンドユーザのプロファイルを作成します。

- ユニバーサル回線テンプレート: 通常、ディレクトリ番号に割り当てられる、一般的な電話回線の設定の集合。ユニバーサル回線テンプレートを使用すると、エンドユーザに割り当てられた新しいディレクトリ番号の電話回線をすばやく設定できます。
- ユニバーサルデバイステンプレート: 電話機またはその他のデバイスに通常割り当てられる、一般的なデバイス設定の集合。ユニバーサルデバイステンプレートを使用すると、エンドユーザに割り当てられた新しい電話機をすばやく設定することができます。

ユーザ プロファイルの前提条件

ユーザプロファイルを設定する前に、導入時にどのように電話をプロビジョニングするかの計画を立てることを確認します。セルフプロビジョニングを使用して、エンドユーザが自分の電話をプロビジョンできるようにするかどうかを決定します。

ユーザ プロファイルの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ユニバーサル回線テンプレートの設定（312 ページ）	電話番号に一般的に適用される共通設定を使用して、ユニバーサル回線テンプレートを設定します。
ステップ 2	ユニバーサル デバイス テンプレートの設定 （313 ページ）	電話に一般的に適用される共通設定を使用して、ユニバーサル デバイス テンプレートを設定します。
ステップ 3	ユーザ プロファイルの設定 （314 ページ）	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 プロファイルに割り当てます。

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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 5 [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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 7 このユーザプロファイルに関連付けられた Cisco Jabber ユーザ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。

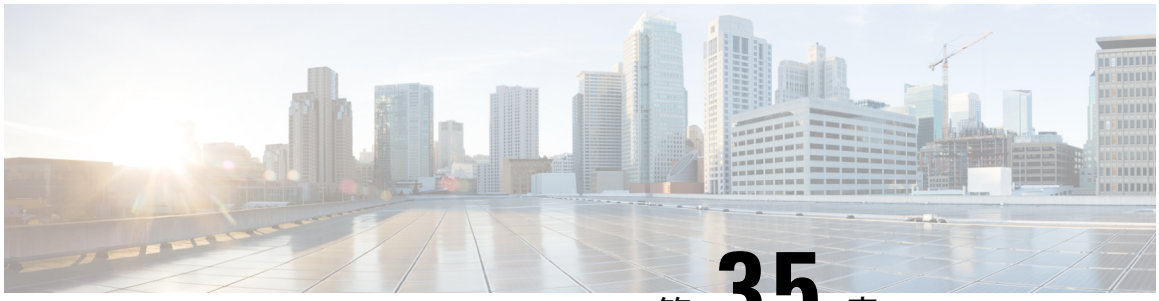
（注）
- デフォルトでは、このチェックボックスはオンです。このチェックボックスをオフにすると、[Jabber ポリシー（Jabber Policies）] セクションが無効になり、サービス クライアント ポリシー オプションは、デフォルトで選択されません。
- この設定は、OAuth 更新ログインを使用している Cisco Jabber のユーザにのみ必須です。非 Jabber ユーザは、この設定がなくてもモバイルおよびリモートアクセスを使用できます。モバイルおよびリモートアクセス機能は、Jabber のモバイルおよびリモートアクセスユーザにのみ適用され、他のエンドポイントまたはクライアントには適用されません。

ステップ 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。[Jabberデスクトップクライアントポリシー（Jabber Desktop Client Policy）] および [Jabber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。

ステップ 9 [保存（Save）] をクリックします。



第 35 章

サービス プロファイルの設定

サービスプロファイルの概要

サービス プロファイルにより、Unified Communications（UC）サービスの共通設定で構成されるプロファイルを作成できます。サービス プロファイルをエンド ユーザに適用し、サービス プロファイルにあるUCサービスの構成時の設定をそのエンドユーザに割り当てることができます。企業内の異なるユーザ グループごとに異なるサービスを設定でき、その結果、各グループのユーザが、仕事に合わせて設定された適切なサービスを利用できます。

サービス プロファイルは、次の UC サービスの構成時の設定で構成されます。

- ボイスメール
- メールストア
- 会議
- ディレクトリ
- IM and Presence
- CTI
- ビデオ会議サービス

エンド ユーザへのサービス プロファイルの適用

エンド ユーザにサービス プロファイルを適用するには、次の方法を使用します。

- LDAP 同期されたユーザ向け：LDAP ディレクトリからエンド ユーザをインポートした場合、サービス プロファイルを機能グループ テンプレートに割り当てることができ、その機能グループ テンプレートをエンド ユーザに適用できます。
- アクティブ ローカル ユーザ（非 LDAP ユーザなど）向け：エンド ユーザの設定で、サービス プロファイルを個別のエンド ユーザに割り当てることができます。また、サービス

プロファイルを多くのエンドユーザに一度に割り当てるには、一括管理ツールを利用できます。詳細については、『*Cisco Unified Communications Manager* 一括管理ガイド』を参照してください。

サービス プロファイルの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	このサービス プロファイルに割り当てる次の Unified Communications（UC）サービスを設定します。 • ボイスメール サービスの追加（318 ページ） • メールストア サービスの追加（319 ページ） • 会議サービスの追加（320 ページ） • ディレクトリ サービスの追加（321 ページ） • IM and Presence サービスの追加（322 ページ） • CTI サービスの追加（323 ページ） • ビデオ会議スケジュールサービスの追加（324 ページ）	サービス プロファイル用に設定する UC サービス設定を実行します。
ステップ 2	サービス プロファイルの設定（326 ページ）	このサービス プロファイルに適用する UC サービスを示すように、ユーザのサービス プロファイルを設定します。

ボイスメール サービスの追加

システムにボイスメール サービスを追加します。複数のボイスメールサービスを追加して、サービスプロファイルに追加するサービスを選択することができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [UC サービス タイプ（UC Service Type）] ドロップダウン リスト ボックスから [ボイスメール（Voicemail）] を選択します。

ステップ 4 [製品タイプ（Product Type）] ドロップダウン リスト ボックスから、[Unity] または [Unity Connection] を選択します。

ステップ 5 [名前（Name）] にボイスメール サービスの名前を入力します。

ステップ 6 サービスを区別しやすくするための [説明（Description）] を入力します。

ステップ 7 [ホスト名/IP アドレス（Hostname/IP Address）] フィールドに、ボイスメール サービスをホストするサーバのホスト名、IP アドレス、または完全修飾ドメイン名を入力します。

ステップ 8 [ポート（Port）] フィールドに、ボイスメール サービスに接続するポートを入力します。デフォルトのポートは 443 です。

ステップ 9 [プロトコル（Protocol）] フィールドに、ボイス メッセージをルーティングするために使用するプロトコルを入力します。使用可能なオプションは、[HTTP] と [HTTPS] のみです。

（注） Cisco Unity サーバおよび Cisco Unity Connection サーバのボイスメール転送プロトコルには、[HTTPS] を使用することを推奨します。ネットワーク設定で [HTTPS] がサポートされない場合に限り [HTTP] に変更してください。

ステップ 10 [保存（Save）] をクリックします。

次のタスク

メールストア サービスの追加 （319 ページ）

メールストア サービスの追加

システムにボイスメールサービスを追加します。Cisco Jabber クライアントでは、ビジュアル ボイスメール機能にメールストア サービスを利用します。

（注） Cisco Unity では、Microsoft Exchange サーバでのメッセージ保存用にサブスクライバ メールボックスが作成されます。

Cisco Unity Connection は通常、メールストア サービスを提供し、同じサーバ上でメールストア サービスをホストします。

始める前に

ボイスメール サービスの追加 （318 ページ）

手順

ステップ 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 Service）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **UCサービスタイプ**のドロップダウンリストボックスから**ボイスメール**を選択します。

ステップ 4 ボイスメールサービスに**名前**を入力します。

ステップ 5 Mailstore **サービス**の説明を入力します。

ステップ 6 **ホスト名/ipアドレス**フィールドに、ボイスメールサービスをホストするサーバのホスト名、ipアドレス、または完全修飾ドメイン名を入力します。

ステップ 7 [**ポート (** Port)] フィールドで、mailstore サービスの利用可能なポートと一致する 1 ~ 65535 のポートを指定します。~ 1-65535 の間の数字。デフォルトのmailstore ポートは、143です。

（注） Cisco Unity Connectionを使用したセキュア ボイスメッセージングの場合は、7993を使用してください。

ステップ 8 [**プロトコル (** protocol)] フィールドで、ボイスメールメッセージのルーティングに使用するプロトコルを入力します。TCP (デフォルト)、TLS、UDP、または SSL のいずれかになります。

（注） Cisco Unity Connection を使用したセキュア メッセージングの場合は、TLS を使用してください。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

会議サービスの追加 （320 ページ）

会議サービスの追加

システムに会議サービスを追加します。

始める前に

メールストア サービスの追加 （319 ページ）

手順

ステップ 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 Service）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **UCサービスタイプ**のドロップダウンリストボックスから**カンファレンス**を選択します。

ステップ 4 [**製品タイプ**] ドロップダウンリストボックスから、会議で使用する製品を選択します。

- MeetingPlace Classic
- ミーティングプレイスエクスプレス
- Webex

ステップ 5 カンファレンスサービスに**名前** を入力します。

ステップ 6 カンファレンスサービスの**説明** を入力します。

ステップ 7 **ホスト名/ipアドレス** フィールドに、会議サービスをホストするサーバのホスト名、ip アドレス、または完全修飾ドメイン名を入力します。

ステップ 8 **ポート**フィールドに、会議サービスの利用可能なポートと一致するポート値を入力します。推奨値は次のとおりです：

- 80 (デフォルト設定): HTTP にこのポートを使用します。
- 443: HTTPSにこのポートを使用します。

ステップ 9 **プロトコル**ドロップダウンリストボックスから、エンドポイントがサービスにアクセスするために使用するプロトコルを選択します。

- TCP（デフォルト設定）
- UDP
- [SSL]
- [TLS]

（注） Cisco Unity Connection を使用したセキュア メッセージングの場合は、TLS を使用してください。

ステップ 10 [保存（Save）] をクリックします。

次のタスク

ディレクトリ サービスの追加 （321 ページ）

ディレクトリ サービスの追加

ディレクトリ検索で、Cisco Unified Communications Manager に外部の LDAP ディレクトリを参照させる場合は、ディレクトリ サービスをシステムに追加します。

始める前に

会議サービスの追加 （320 ページ）

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[UC サービス（UC Service）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [UC サービスの種類（UC Service Type）] ドロップダウン リスト ボックスから、[ディレクトリ（Directory）] を選択します。

ステップ 4 [製品のタイプ（Product Type）] フィールドから、次のいずれかを選択します。

- [ディレクトリ（Directory）]：クライアントがUDSを使用してCisco Unified Communications Managerデータベースに接続して、ディレクトリ検索をする場合は、このオプションを選択します。
- [拡張ディレクトリ（Enhanced Directory）]：クライアントが外部のLDAPディレクトリに接続して、ディレクトリ検索をする場合は、このオプションを選択します。

ステップ5 ディレクトリ サービスの名前を [名前（Name）] に入力します。

ステップ6 ディレクトリ サービスの説明を [説明（Description）] に入力します。

ステップ7 [ホスト名/IPアドレス（Hostname/IP Address）]フィールドに、クライアントがディレクトリ検索に利用するディレクトリ サービスをホストするサーバの、ホスト名、IP アドレス、または完全修飾ドメイン名を入力します。

（注） 外部のLDAPディレクトリをディレクトリ検索に使用している場合は、そのLDAPディレクトリのホスト名、IP アドレス、または完全修飾ドメイン名を入力します。

ステップ8 [ポート（Port）] フィールドに、ディレクトリ サービスで使用可能なポート番号と一致するポート番号を入力します。デフォルトのポート値は389です。また、ポート636、3628、3629は、外部のLDAPディレクトリに接続できます。

ステップ9 [プロトコル（Protocol）] フィールドに、ディレクトリ サービスとエンドポイント間の通信のルーティングに使用するプロトコルを入力します。次のオプションを使用できます。

- TCP（デフォルト設定）
- UDP
- TLS

ステップ10 [保存（Save）] をクリックします。

次のタスク

IM and Presence サービスの追加 （322 ページ）

IM and Presence サービスの追加

システムに IM and Presence サービスを追加します。

始める前に

ディレクトリ サービスの追加 （321 ページ）

手順

ステップ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 Service）]** を選択します。

ステップ2 [新規追加（Add New）] をクリックします。

ステップ 3 [UC サービス タイプ（UC Service Type）] ドロップダウンリスト ボックスから、IM and Presence を選択します。

ステップ 4 [製品タイプ（Product Type）] ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。

- Unified CM（IM and Presence）
- Webex（IM and Presence）

ステップ 5 [名前（Name）] に IM and Presence サービスの名前を入力します。

ステップ 6 [説明（Description）] に IM and Presence サービスの説明を入力します。

ステップ 7 [ホスト名/IP アドレス（Hostname/IP Address）] フィールドに、IM and Presence サービスをホストするサーバのホスト名、IP アドレス、または DNS SRV を入力します。

ヒント ユーザに適した IM and Presence サービスをクライアントが見つけやすい DNS SRV を推奨します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

CTI サービスの追加 （323 ページ）

CTI サービスの追加

システムに CTI サービスを追加します。

始める前に

IM and Presence サービスの追加 （322 ページ）

手順

ステップ 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 Service）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **UCサービスタイプ**のドロップダウンリストボックスから**CTI**を選択します。

ステップ 4 CTIサービスの**名前**を入力します。

ステップ 5 CTIサービスの**説明**を入力します。

ステップ 6 **ホスト名/ipアドレス**フィールドに、CTIサービスをホストするサーバのホスト名、ipアドレス、または完全修飾ドメイン名を入力します。

ステップ 7 **ポートフィールド**にCTIサービスのポート番号を入力します。デフォルトのポートは2748です

ステップ 8 [保存（Save）] をクリックします。

次のタスク

ビデオ会議スケジュールサービスの追加 （324 ページ）

ビデオ会議スケジュールサービスの追加

ビデオ会議のスケジュールサービスを追加します。このサービスは、ビデオ会議のスケジュールを設定するためのポータルをテレプレゼンス管理システムに提供します。

始める前に

CTI サービスの追加 （323 ページ）

手順

ステップ 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 Service）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [名前（Name）] にサービスの名前を入力します。

ステップ 4 サービスの**説明**を入力します。

ステップ 5 **IPアドレス/ホスト**フィールドに、ビデオ会議のスケジュールサービスをホストするサーバのホスト名、ip アドレス、または完全修飾ドメイン名を入力します。

ステップ 6 **ポート**フィールドに、ビデオ会議のスケジュールサービスで使用可能なポートに一致するポート番号を入力します。利用可能なポートは次のとおりです。

- 80(デフォルト)または8080:HTTPに対して次のポートを使用します。
- 443または8443:HTTPSに対して次のポートを使用します。

ステップ 7 **プロトコル**ドロップダウンリストボックスで、次のプロトコルのいずれかを選択して、ビデオ会議のスケジュールサービスと通信します。

- HTTP
- HTTPS

ステップ 8 **ポータルURL**フィールドに、テレプレゼンス管理システムへのURLを入力します。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

サービス プロファイルの設定 （326 ページ）

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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 4 [製品タイプ（Product Type）] を選択します。

ステップ 5 [名前（Name）] にサービスの名前を入力します。

ステップ 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。

ステップ 7 [ポート（Port）] および [プロトコル（Protocol）] の情報を入力します。

ステップ 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。

ステップ 9 [保存（Save）] をクリックします。

ステップ 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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

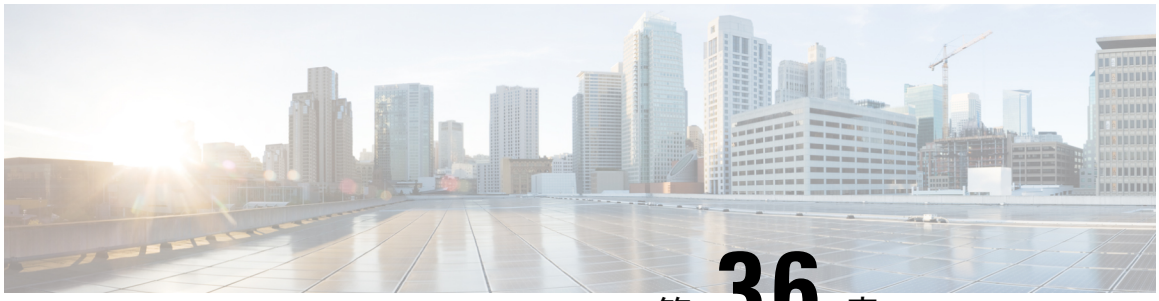
ステップ 3 選択したサービス プロファイルの設定の [名前（Name）] を入力します。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 7 [保存（Save）] をクリックします。



第 36 章

機能グループ テンプレートの設定

機能グループ テンプレートの概要

機能グループテンプレートは、設定された電話機および電話回線を使用してエンドユーザを展開するのに役立ちます。機能グループテンプレートを使用すると、その機能グループテンプレートが割り当てられているすべてのユーザーに公衆電話、電話回線、サービス設定を割り当てることができます。エンドユーザのセルフプロビジョニングも有効にしている場合、機能グループテンプレートを使用すると、ユーザは、目的の電話、電話回線、サービスの設定を使用して、簡単にプロビジョニングと電話機の設定を行うことができます。

機能グループテンプレートの設定には、機能グループテンプレートに割り当てることができる次のプロファイルが含まれています。

- ユーザプロファイル: 一般的な電話機と電話回線の設定のセットが含まれています。共通の電話回線の設定を割り当てるユニバーサル回線テンプレートと、共通の電話回線の設定を割り当てるユニバーサルデバイステンプレートを使用して、ユーザプロファイルを設定する必要があります。これらのテンプレートは、セルフプロビジョニングを設定しているユーザが自分の電話機を設定するのをサポートします。
- サービス プロファイル：会議やディレクトリ サービスなどの Unified Communications サービスにおける共通の設定グループが含まれます。

ユーザ プロファイルとサービス プロファイルを含むように機能グループ テンプレートを設定し、その後、その機能グループ テンプレートをユーザに割り当てると、エンド ユーザがプロビジョニングする新しい電話にユーザ プロファイルとサービス プロファイルが伝搬されます。

IM and Presence サービスを展開する場合は、機能グループ テンプレートを使用して、インスタント メッセージおよびプレゼンス機能で LDAP 同期ユーザを有効にできます。

機能グループテンプレートの要件

機能グループテンプレートを設定する前に、エンドユーザ用のユーザプロファイルとサービスプロファイルを設定します。

- ユーザ プロファイルの設定タスク フロー （312 ページ）
- サービス プロファイルの設定タスク フロー （318 ページ）

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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

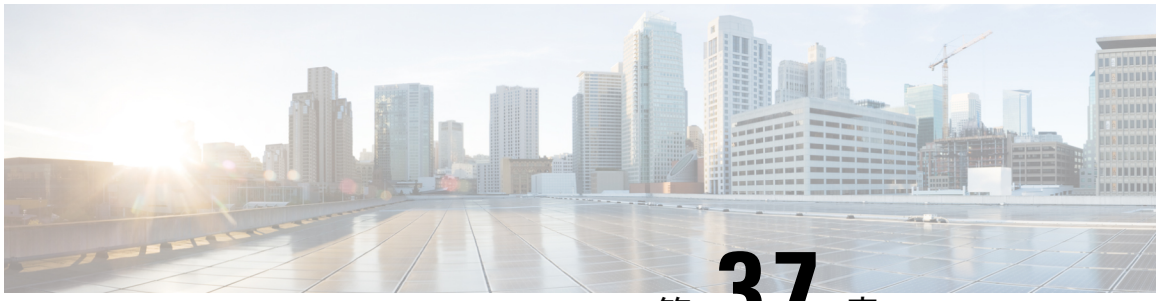
ステップ 6 ドロップダウン リストから、[サービスプロファイル（Services Profile）] および [ユーザプロファイル（User Profile）] を選択します。

ステップ 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。

ステップ 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。



第 37 章

LDAPディレクトリからのユーザのインポート

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 Communication 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 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。

エンド ユーザ用 LDAP 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 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向けディレクトリ サーバ ユーザ検索

以前のリリースでは、Ciscoモバイルおよびリモートアクセス クライアント（たとえば、Cisco Jabber）またはエンドポイント（たとえば、Cisco DX 80 電話）を使用しているユーザが企業ファイアウォールの外部でユーザ検索を実行した場合、結果は Cisco Unified Communications Managerに保存されたユーザアカウントに基づいていました。データベースには、ローカルで設定されたか、または社内ディレクトリから同期されたユーザアカウントも含まれています。

このリリースでは、Cisco モバイルおよびリモート アクセス クライアントとエンドポイントは、企業ファイアウォールの外部で動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、Cisco Unified Communications 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。

この機能を使用して、次の結果を実現できます。

- 地理的な場所にかかわらず同じユーザ検索結果を配信: 企業ファイアウォール外に接続されている場合でも、モバイルおよびリモートアクセスクライアントとエンドポイントは、社内ディレクトリを使用してユーザ検索を実行できます。
- Cisco Unified Communications Manager データベースに設定されているユーザアカウントの数を減らす: モバイルクライアントが社内ディレクトリ内のユーザを検索できるようになりました。以前のリリースでは、ユーザの検索結果はデータベースに設定されているユーザに基づいています。ユーザの検索に使用するデータベースに対しては、管理者がユーザアカウントを設定または同期する必要がなくなりました。管理者は、クラスタによって提供されているユーザアカウントのみを設定する必要があります。データベース内のユーザアカウントの総数を減らすと、ソフトウェアアップグレードの時間枠が短縮され、データベースの全体的なパフォーマンスが向上します。

この機能を構成するには、**LDAP検索構成ウィンドウ**で**エンタープライズディレクトリサーバー**のユーザー検索を有効にし、LDAPディレクトリサーバーの詳細を構成する必要があります。詳細については、「エンタープライズディレクトリ ユーザ検索の設定（339ページ）」の手順を参照してください。

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* 一括管理ガイド』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
ステップ 1	Cisco DirSync サービスの有効化 （335 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。
ステップ 2	LDAP ディレクトリ同期の有効化 （335 ページ）	Unified Communication Manager の LDAP ディレクトリ同期を有効化します。
ステップ 3	LDAP フィルタの作成 （336 ページ）	（省略可）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。
ステップ 4	LDAP ディレクトリの同期の設定 （337 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。
ステップ 5	エンタープライズ ディレクトリ ユーザ検索の設定 （339 ページ）	（省略可）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。

	コマンドまたはアクション	目的
ステップ 6	LDAP 認証の設定 （341 ページ）	（省略可）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。
ステップ 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 （342 ページ）	（省略可）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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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) （省略可）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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 12 [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。

ステップ 13 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。

ステップ 14 [保存（Save）] をクリックします。

ステップ 15 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

ステップ 1 Cisco Unified CM Administration で、**[システム（System）] > [LDAP] > [LDAP 検索（LDAP Search）]** を選択します。

ステップ 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。

ステップ 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。

ステップ 4 [保存（Save）] をクリックします。

ディレクトリサーバの UDS 検索のための LDAP 属性

次の表に、**ユーザ検索をエンタープライズディレクトリサーバ**に入力可能にするオプションが有効になっているときに、UDSユーザ検索リクエストが使用するLDAP属性を示します。これらのタイプのディレクトリ要求に対しては、UDSはプロキシとして機能し、企業ディレクトリサーバに検索要求をリレーします。

（注） UDS ユーザの応答タグは、いずれかの LDAP 属性にマップできます。属性のマッピングは、**LDAPサーバタイプ**ドロップダウンリストから選択したオプションによって決定されます。**システム** > **LDAP** > **LDAPシステム設定**ウィンドウからこのドロップダウンリストにアクセスします。

UDS ユーザの応答タグ	LDAP 属性
userName	• samAccountName • uid
firstName	givenName
lastName	sn
middleName	• initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	• telephonenumber • ipPhone
homeNumber	homephone
mobileNumber	mobile
email	mail
directoryUri	• msRTCSIP-primaryuseraddress • mail

UDS ユーザの応答タグ	LDAP 属性
department	• department • 部署番号
manager	manager
title	title
pager	pager

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

ステップ 1 Cisco Unified CM Administration で、**[システム（System）] > [LDAP] > [LDAP認証（LDAP Authentication）]** を選択します。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （342 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 Cisco DirSyncサービスパラメータの値を設定します。

ステップ 5 [保存（Save）] をクリックします。

LDAP ディレクトリ サービス パラメータ

サービス パラメータ	説明
最大アグリーメント数	設定可能なLDAPディレクトリの最大数。デフォルトの設定値は20です。
最大ホスト数	フェールオーバー用として設定できるLDAPホスト名の最大数を指定します。デフォルト値は 3 です。

サービス パラメータ	説明
ホスト障害再試行の遅延(secs)	ホストで障害が発生した後、Cisco Unified Communications Manager が最初の LDAP サーバ（ホスト名）への接続を再試行する前の遅延秒数です。デフォルト値は 5 です。
ホストリストの失敗再試行の遅延(mins)	ホストリストで障害が発生した後、Cisco Unified Communications Manager が設定された各 LDAP サーバ（ホスト名）への接続を再試行する前の遅延分数です。デフォルトは 10 です。
LDAP Connection Timeout (secs)	Cisco Unified Communications Manager が LDAP 接続を確立できる秒数です。指定した時間内に接続を確立できない場合、LDAP サービス プロバイダーは接続試行を中止します。デフォルトは 5 です。
遅延同期の開始間隔(mins)	Cisco DirSync サービスの起動後に、Cisco Unified Communications Manager がディレクトリ同期プロセスを開始するまでの遅延分数です。デフォルトは 5 です。

LDAP 同期済みユーザをローカル ユーザに変換する

LDAP ディレクトリと Cisco Unified Communications Manager を同期すると、LDAP に同期されたエンドユーザについては、ローカルユーザに変換しないかぎり、[エンドユーザの設定（End User Configuration）] ウィンドウ内のフィールドは編集できません。

[エンド ユーザの設定（End User Configuration）] ウィンドウで LDAP 同期ユーザのフィールドを編集するには、そのユーザをローカル ユーザに変換します。ただし、この変換を行うと、Cisco Unified Communications Manager を LDAP ディレクトリと同期したときにエンド ユーザが更新されなくなります。

手順

ステップ 1 Cisco Unified CM Administration で、**[エンド ユーザ（End Users）] > [エンド ユーザ管理（End User Management）]** を選択します。

ステップ 2 [検索（Find）] をクリックして、エンド ユーザを選択します。

ステップ 3 [ローカル ユーザへの変換（Convert to Local User）] ボタンをクリックします。

ステップ 4 [エンド ユーザ設定（End User Configuration）] ウィンドウでフィールドを更新します。

ステップ 5 [保存（Save）] をクリックします。

アクセス制御グループへの LDAP 同期ユーザの割り当て

LDAP と同期するユーザを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。

始める前に

エンド ユーザと外部 LDAP ディレクトリが同期されるように Cisco Unified Communication Manager を設定する必要があります。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム（System）] > [LDAP] > [LDAPディレクトリ（LDAP Directory）]** を選択します。

ステップ 2 [検索（Find）] をクリックし、設定した LDAP ディレクトリを選択します。

ステップ 3 [アクセス制御グループに追加（Add to Access Control Group）] ボタンをクリックします。

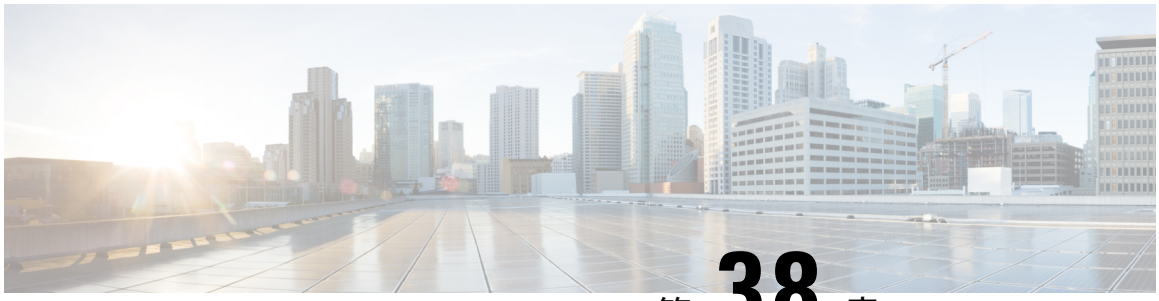
ステップ 4 この LDAP ディレクトリのエンド ユーザに適用するアクセス制御グループを選択します。

ステップ 5 [選択項目の追加（Add Selected）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [完全同期を実施（Perform Full Sync）] をクリックします。
Cisco Unified Communication Manager が外部 LDAP ディレクトリと同期し、同期したユーザが正しいアクセス制御グループに挿入されます。

（注） 同期したユーザは、アクセス制御グループを初めて追加した時にのみ、選択したアクセス グループに挿入されます。完全同期の実行後に LDAP に追加するグループは、同期したユーザに適用されません。



第 38 章

エンドユーザの手動設定

エンド ユーザの手動プロビジョニングの概要

LDAPディレクトリからエンドユーザをインポートしていない場合は、次のいずれかの方法を使用して、Unified Communications Manager データベースにエンド ユーザを追加することができます。

- 一括管理ツールを使用し、インポートをする
- 手動で新しいユーザを追加する

エンドユーザプロビジョニングの手動での前提条件

エンドユーザをインポートする前に、エンドユーザのロール、アクセス制御グループ、クレデンシャル ポリシーを計画して設定します。

- ユーザ アクセスの設定タスク フロー （284 ページ）
- クレデンシャル ポリシーの設定タスク フロー （307 ページ）

バルク管理を使用してエンドユーザをインポートする

一括管理ツールを使用して、多数のエンドユーザ、電話、およびポートのインポートや更新を含め、Cisco Unified Communications Manager データベースに対する、大量のトランザクションを単一のプロセスで実行できます。バルク管理ツールを使用すると、エンドユーザのリストとエンドユーザの設定をCSVファイルからデータベースにインポートできます。

一括管理ツールを使用してエンド ユーザをインポートする方法の詳細については、『*Cisco Unified Communications Manager* 一括管理ガイド』を参照してください。

エンド ユーザの手動設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	新規エンドユーザの追加 （346ページ）	データベースに新しいエンド ユーザを手動で追加します。
ステップ 2	アクセス制御グループへのエンド ユーザの割り当て （347 ページ）	必要な権限を備えたアクセス制御グループをプロビジョニングするローカル エンド ユーザを割り当てます。ローカル ユーザには、手動でプロビジョニングするエンド ユーザと、一括管理ツールを使用してインポートするエンド ユーザが含まれます。ローカル ユーザには、エンドユーザ設定で「アクティブ ローカル ユーザ」のユーザ ステータスがあります。
ステップ 3	エンド ユーザへのクレデンシャル ポリシーの適用 （348 ページ）	（省略可）デフォルトのクレデンシャル ポリシーが、このエンドユーザに適用できるかどうかを確認します。適用できなければ、エンドユーザ PIN またはパスワードにクレデンシャル ポリシーを適用します。
ステップ 4	ローカル エンドユーザへの機能グループ テンプレートの割り当て （348 ページ）	エンドユーザに機能グループテンプレートを割り当てます。機能グループ テンプレートを割り当てると、システムはエンドユーザにその機能グループ テンプレートに関連付けられているユーザ プロファイル、サービス プロファイル、ユニバーサル回線とデバイステンプレート、セルフプロビジョニング設定を割り当てます。

新規エンド ユーザの追加

Cisco Unified Communications Manager のデータベースに新しいエンドユーザを手動で追加するには、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザの管理（User Management）] > [エンドユーザ（End User）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 ユーザの**ユーザID**と**苗字**を入力します。

ステップ 4 ドロップダウンリストで**ユーザ名**を選択します。

ステップ 5 [エンド ユーザ設定（End User Configuration）] ウィンドウのフィールドを設定します。フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

アクセス制御グループへのエンド ユーザの割り当て （347 ページ）

アクセス制御グループへのエンド ユーザの割り当て

プロビジョニングされたユーザーをアクセス制御グループに割り当てるには、この手順を使用します。LDAP 同期中にアクセス制御グループに割り当てた LDAP 同期ユーザに、次の手順を使用して追加のアクセス制御グループを割り当てることができます。この手順は、LDAP 同期設定に共通のアクセス制御グループがあっても、一部のユーザに権限に応じた追加のアクセス制御グループを割り当てる必要がある場合に便利です。

手順

ステップ 1 Cisco Unified CM Administration で、**[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）]** を選択します。

ステップ 2 [検索（Find）] をクリックし、アクセス制御グループを選択します。

ステップ 3 [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。

ステップ 4 [ユーザの検索と一覧表示（Find and List Users）] ウィンドウで、グループに追加するエンド ユーザを選択します。

ステップ 5 [選択項目の追加（Add Selected）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

エンド ユーザへのクレデンシャル ポリシーの適用

設定されたクレデンシャル ポリシーを特定のエンドユーザ パスワードまたはエンドユーザの暗証番号に適用します。デフォルトのクレデンシャルポリシーから更新を行う必要がある場合に、この操作が必要になることがあります。

（注） また、アプリケーション ユーザ パスワードにクレデンシャル ポリシーを適用することもできます。詳細については、『*Cisco Unified Communication Manager* 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

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）] > [エンドユーザ（End User）]** を選択します。

ステップ 2 [検索（Find）] をクリックして、エンド ユーザを選択します。

ステップ 3 クレデンシャル ポリシーを適用するクレデンシャルに応じて、パスワードまたは暗証番号に対応する [クレデンシャルの編集（Edit Credential）] ボタンをクリックします。

ステップ 4 **認証ルール**ドロップダウンリストから、適用するクレデンシャルポリシーを選択します。

ステップ 5 [クレデンシャルの設定（Credential Configuration）] ウィンドウのその他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。

ステップ 6 [保存（Save）] をクリックします。

ローカル エンドユーザへの機能グループ テンプレートの割り当て

ローカル エンドユーザに機能グループ テンプレートを割り当てます。ローカル エンドユーザとは、データベースに手動で追加された、または一括管理ツールを使用してインポートされたエンドユーザです。ローカル エンドユーザは外部 LDAP ディレクトリと同期されません。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユーザ/電話のクイック追加（Quick User/Phone Add）]** を選択します。

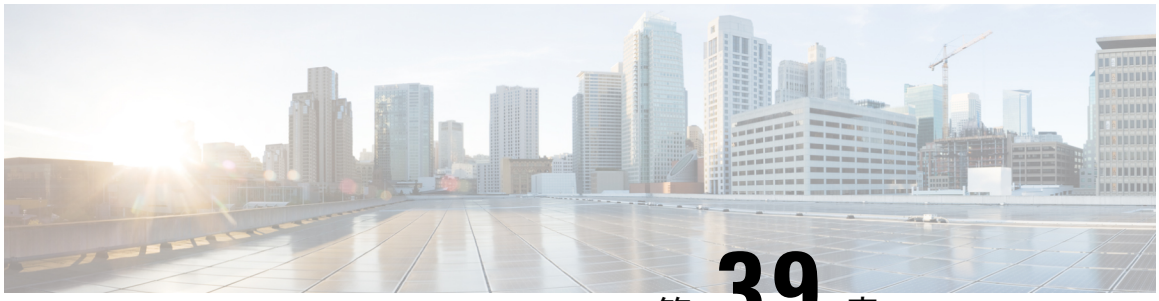
ステップ 2 [検索（Find）] をクリックしてエンド ユーザを選択します。

ステップ 3 [機能グループテンプレート（Feature Group Template）] ドロップダウン リストで、このエンドユーザー用に設定した機能グループ テンプレートを選択します。

ステップ 4 [保存（Save）] をクリックします。

第 VI 部

エンドポイント デバイスの設定



第 39 章

エンドポイント デバイスの概要

エンドポイント デバイス設定について

このパートの各章には、エンドポイントデバイスの構成方法、およびエンドポイントにユーザを関連付ける方法に関する情報が記載されています。

エンドポイント デバイス設定

次のタスク フローを実行すると、システムのエンド ユーザを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	アナログ電話アダプタの設定 （366 ページ）	アナログ電話機と IP ベースのテレフォニーネットワーク間のインターフェイスとして動作するアナログ電話アダプタを設定します。
ステップ 2	ソフトウェアベースのエンドポイントの設定 （419 ページ）	CTIポート、H、323 クライアント、Cisco IP Communicatorなど、ソフトウェアベースのエンドポイントを設定します。
ステップ 3	Cisco IP 電話の設定タスク フロー （433 ページ）	ネットワーク上で機能するようにCisco IP電話を設定します。
ステップ 4	Diagnostics and Reporting の設定タスク フロー （463 ページ）	Cisco IP電話のコール品質を保証するには、コール診断と品質報告ツール(QRT)を使用します。

	コマンドまたはアクション	目的
ステップ 5	サードパーティ SIP エンドポイントの設定タスク フロー （478 ページ）	サードパーティのSIPエンドポイントを構成します。
ステップ 6	デバイス プロファイルとテンプレートの設定タスク フロー （486 ページ）	特定のデバイスに関連付けられたサービス、機能、およびディレクトリ番号を定義するプロファイルとテンプレートを設定します。
ステップ 7	ユーザおよびデバイスの設定タスク フロー （499 ページ）	デバイスをエンドユーザーとアプリケーションユーザーに関連付けます。

第 40 章

モバイルおよびリモートアクセスの設定

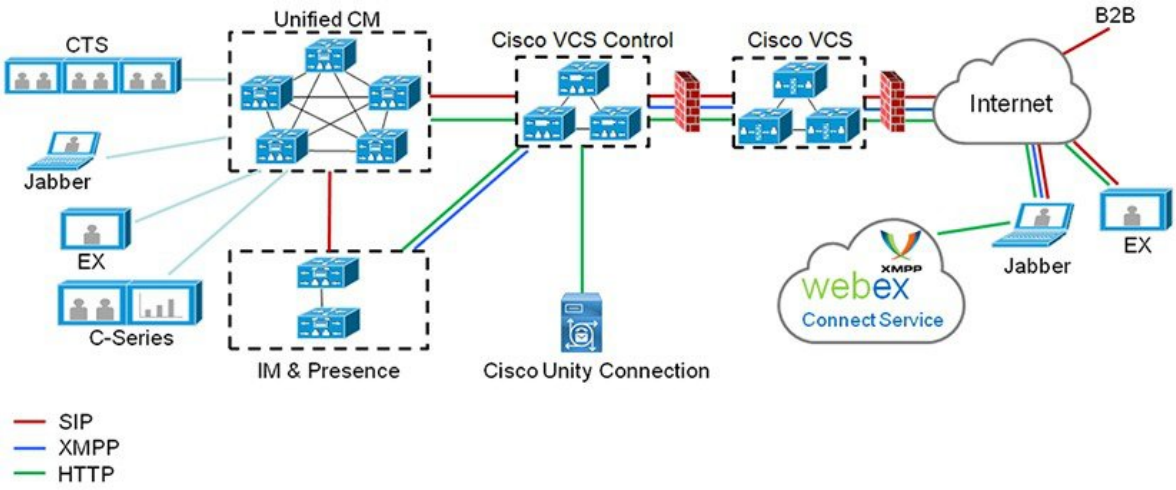
モバイルおよびリモート アクセスの概要

Unified Communications Managerモバイルおよびリモート アクセスは、Cisco Collaboration Edge アーキテクチャの中核的なコンポーネントです。これを使用することで、Cisco Jabber などのエンドポイントで、エンドポイントがエンタープライズ ネットワーク内にない場合でも、Unified Communications Manager が提供する登録、コール制御、プロビジョニング、メッセージング、およびプレゼンス サービスを使用できます。Cisco Expressway は、モバイル エンドポイントをオンプレミス ネットワークに接続し、Unified CM の登録に対してセキュアなファイアウォール トラバースと回線側のサポートを提供します。

ソリューション全体で提供されるものは以下の通りです。

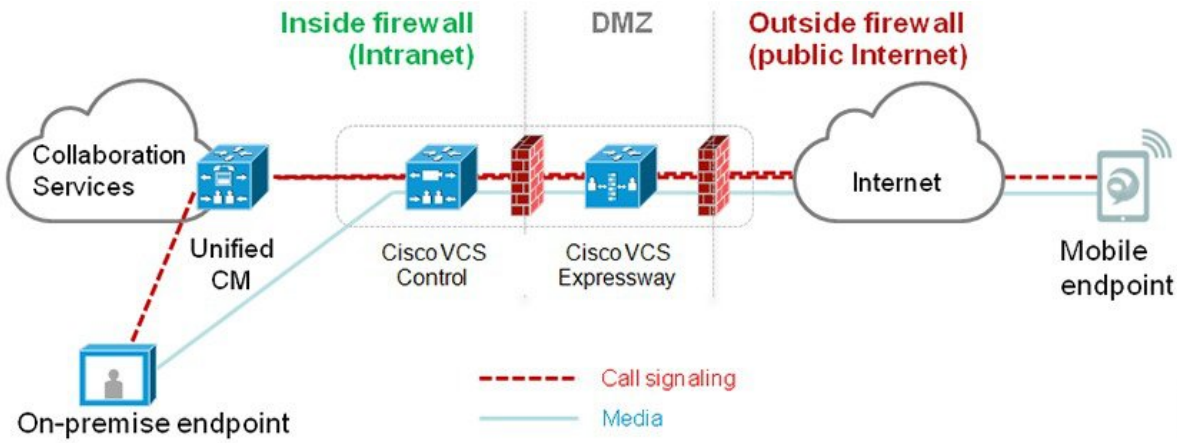
- オフプレミスアクセス：企業ネットワーク外においても、JabberおよびEX/MX/SXシリーズ クライアントで一貫したエクスペリエンスを提供
- セキュリティ：セキュアな Business-to-Business（B2B）コミュニケーション
- クラウド サービス：豊富な Webex 統合とサービス プロバイダ製品を提供する、柔軟で拡張性に優れたエンタープライズ クラスのソリューション
- ゲートウェイと相互運用性サービス:：メディアおよびシグナリングの正規化、非標準エンドポイントのサポート

図 *3 : Unified Communications* : モバイルおよびリモート アクセス



サードパーティのSIPまたはH.323デバイスはExpressway-Cに登録でき、必要に応じてSIPトランクを介して統合されたCM登録デバイスと相互運用することもできます。

図 *4 :* 一般的なコール フロー : シグナリングとメディア パス



- Unified CM は、モバイルとオンプレミスの両方のエンドポイントにコール制御を提供します。
- シグナリングは、モバイル エンドポイントと Unified CM の間で Expressway ソリューションを横断します。
- メディアは Expressway ソリューションを横断し、エンドポイント間で直接リレーされます。すべてのメディアが Expressway-C とモバイル エンドポイント間で暗号化されます。

モバイルおよびリモートアクセスの設定

Cisco Jabber を使用してモバイルおよびリモートアクセス機能を有効にするには、Unified Communications Manager の [ユーザプロファイルの設定（User Profile Configuration）] ウィンド

ウでモバイルおよびリモートアクセスのユーザポリシーをセットアップします。非 Jabber のエンドポイントには、モバイルおよびリモートアクセスのアクセスユーザポリシーは不要です。

また、モバイルおよびリモート アクセスで Cisco Expressway を設定する必要もあります。詳細については、『Cisco Expressway を介したモバイルおよびリモートアクセスの導入ガイド』を参照してください。

モバイルおよびリモートアクセスの前提条件

Cisco Unified Communications Managerの要求

以下の要件が適用されます。

- 複数の Unified Communications Manager クラスタを導入する場合は、ILS ネットワークをセットアップします。
- モバイルおよびリモートアクセスでは、展開用の NTP サーバを設定する必要があります。ネットワーク用の NTP サーバが導入されていて、SIPエンドポイントの電話機 NTP リファレンスであることを確認してください。

DNS 要件

Cisco Expressway との内部接続には、次の Unified Communications Manager をポイントする、ローカルで解決可能な DNS SRV を設定します。

```
_cisco-uds._tcp&lt;domain&gt;
```

モバイルおよびリモート アクセスで使用するすべての Unified Communications ノードに対して、正引きと逆引きの両方のルックアップ用に内部 DNS レコードを作成する必要があります。これにより、IPアドレスまたはホスト名が FQDNの代わりに使用されている場合に、のノードを検索することができます。SRVレコードは、ローカルネットワークの外部で解決できないことを確認します。

Cisco Expressway の要件

この機能を使用するには、Unified Communications Manager と Cisco Expressway を統合する必要があります。モバイルおよびリモート アクセス用の Cisco Expressway 設定の詳細については、『Cisco Expressway 導入ガイド』の「モバイルおよびリモート アクセス」を参照してください。

Cisco Jabber を使用したモバイルおよびリモートアクセスのアクセスポリシーをサポートする Expressway の最小リリースは X8.10 です。

証明書の前提条件

Unified Communications Manager、IM and Presence Service、および Cisco Expressway-C の間で証明書を交換する必要があります。シスコでは、各システムで同じ CA による CA 署名付き証明書を使用することを推奨します。その場合、次のようになります。

- 各システムに CA ルート証明書チェーンをインストールします（Unified Communications Manager および IM and Presence Service サービスの場合は tomcat 信頼ストアに証明書チェーンをインストールします）。
- Unified Communications Manager の場合は、CA 署名付き tomcat（AXL および UDS トラフィック用）証明書と Cisco CallManager （SIP 用）証明書を要求するための CSR を発行します。
- IM and Presence Service の場合は、CA 署名付き tomcat 証明書を要求するための CSR を発行します。

（注） 別の CA を使用する場合は、各 CA のルート証明書チェーンを Unified Communications Manager、IM and Presence Service サービス、および Expressway-C にインストールする必要があります。

（注） また、 Unified Communications ManagerIM and Presence Serviceとサービスの両方に自己署名証明書を使用することもできます。この場合は、Unified Communications Manager 用の tomcat 証明書と Cisco CallManager 証明書、IM and Presence Service サービス用の tomcat 証明書を Expressway-C にアップロードする必要があります。

モバイルおよびリモート アクセスの設定タスク フロー

モバイルおよびリモートアクセスのエンドポイントを展開する場合、次の手順を Cisco Unified Communications Manager で実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco AXL Web Service の有効化 （357 ページ）	パブリッシャ ノードで Cisco AXL Web サービスが有効になっていることを確認します。
ステップ 2	ビデオの最大セッションビットレートの設定 （358 ページ）	（省略可）MRA エンドポイントのリージョン固有の設定を指定します。例えば、MRA エンドポイントでビデオを使用する予定がある場合は、[ビデオコールの最大セッションビットレート（Maximum Session Bit Rate for Video Calls）]設定を増やすのが望ましい場合があります。これは、ビデオ エンドポ

	コマンドまたはアクション	目的
		イントによっては、デフォルト設定の384 kbps では低すぎる場合があるためです。
ステップ 3	モバイルおよびリモートアクセス用にデバイスプールの設定 （358 ページ）	このMRAエンドポイントが使用するデバイス プールに [日時グループ（Date/Time Group）] と [リージョンの設定（Region configuration）] を割り当てます。
ステップ 4	モバイルおよびリモートアクセス用の電話セキュリティプロファイルの設定（360 ページ）	MRA エンドポイントで使用する電話セキュリティ プロファイルを設定するには、この手順を使用します。
ステップ 5	Cisco Jabber ユーザの MRA アクセス ポリシーの設定 （361 ページ）	Cisco Jabber のみ。Cisco Jabberのユーザに MRAアクセスポリシーをセットアップします。MRA 機能を使用するには、Cisco Jabberユーザーのユーザー プロファイルで MRA アクセスを有効にする必要があります。
ステップ 6	MRA ユーザの設定 （363 ページ）	Cisco Jabber のユーザに対しては、セットアップするユーザポリシーをエンドユーザの設定に適用する必要があります。
ステップ 7	MRA のエンドポイントの設定 （363 ページ）	MRA 機能を使用するエンドポイントを設定およびプロビジョニングします。

Cisco AXL Web Service の有効化

パブリッシャ ノードでCisco AXL Web サービスがアクティブ化されていることを確認します。

手順

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

ステップ 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。

ステップ 3 **データベースと管理サービス**の下で、**Cisco AXL Web Service** が**有効になっていること**を確認します。

ステップ 4 サービスがアクティブ化されていない場合は、対応する**チェック**ボックスをオンにし、[保存(Save)] をクリックしてサービスをアクティブにします。

ビデオの最大セッションビットレートの設定

モバイルおよびリモートアクセスエンドポイントのリージョンの設定を指定します。多くの場合はデフォルト設定で十分と思われますが、モバイルおよびリモートアクセスのエンドポイントでビデオを使用する予定がある場合は、[リージョンの設定（Region Configuration）] で**[ビデオコールの最大セッションビットレート（Maximum Session Bit Rate for Video Calls）]** を上げる必要があります。DX シリーズなどの一部のビデオエンドポイントでは、デフォルト設定の 384 kbps では低すぎる場合があります。

手順

ステップ 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）] > [リージョン情報（Region Information）] > [リージョン（Region）]** を選択します。

ステップ 2 次のいずれかの操作を行います。

- 既存のリージョン内のビットレートを編集するには、[検索（Find）] をクリックしてリージョンを選択します。
- **[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。

ステップ 3 [他のリージョンとの関係を変更（Modify Relationship to other Region] 領域で、[ビデオコールの最大セッションビットレート（Maximum Session Bit Rate for Video Calls）] の新しい設定値を入力します。たとえば、6000 kbps のようになります。

ステップ 4 [リージョンの設定（Region 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。。

ステップ 5 [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用にデバイスプールの設定

新しいリージョンを作成した場合は、モバイルおよびリモートアクセスのエンドポイントが使用するデバイスプールにリージョンを割り当てます。

手順

ステップ 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）] > [デバイス プール（Device Pool）]**。

ステップ 2 次のいずれかを実行します。

- **[検索（Find）]**をクリックし、既存のデバイスグループを選択します。
- [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。

ステップ 3 **デバイスプール名**を入力します。

ステップ 4 冗長**Cisco Unified Communications Managerグループ**を選択します。

ステップ 5 設定した**日付と時刻**グループを割り当てます。このグループには、モバイルおよびリモートアクセスのエンドポイント用に設定した電話用NTP参照が含まれています。

ステップ 6 **[リージョン（Region）]** ドロップダウンリストから、モバイルおよびリモートアクセス用に設定したリージョンを選択します。

ステップ 7 [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。

ステップ 8 [保存（Save）] をクリックします。

ICE の設定

モバイルおよびリモートアクセスのコールの設定を処理するためにICEを導入する場合は、この手順を使用します。ICEはオプションの導入であり、モバイルおよびリモートアクセスおよびTURNサービスを使用して、MRAコールの利用可能なメディアパスを分析し、最適なパスを選択します。ICE を使用すると、コールセットアップ時間が増える可能性がありますが、モバイルおよびリモートアクセスのコールの信頼性は向上します。

始める前に

ICE を導入する方法を決定します。電話グループに対する ICEは、[共通の電話プロファイルの設定（Common Phone Profile Configuration）] で個別の Cisco Jabber デスクトップ デバイスに対して設定するか、すべての電話に適用するシステム全体のデフォルト設定を使用して設定します。

フォールバックメカニズムとして、ICE は、TURNサーバを使用してメディアをリレーできます。TURNサーバが導入されていることを確認してください。

手順

ステップ 1 Cisco Unified CMの管理：

- システム**の** > **デフォルトを** ICE に設定するには、[システム (Enterprise Phone)] を選択します。
- **デバイス** > **デバイスの設定** > **共通電話プロファイル**を選択して、端末グループにICEを設定し、編集するプロファイルを選択します。
- 個別の Cisco Jabber デスクトップ エンドポイント用の ICE を設定し、編集するエンドポイントを選択するには、**[デバイス（Device）]** > **[電話機（Phone）]** を選択します。

ステップ 2 下方向にスクロールして、[対話型接続の確立（ICE）（Interactive Connectivity Establishment (ICE)）] セクションに移動します。

ステップ 3 [ICE] ドロップダウン リストを [有効（Enabled）] に設定します。

ステップ 4 **デフォルトの候補タイプ**を設定する：

- [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アドレスを表す場合があります。
- **[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。

ステップ 5 [サーバの再帰アドレス（Server Reflexive Address）] ドロップダウン リストから、このフィールドを [有効（Enabled）] または [無効（Disabled）] に設定することで、STUN と同様のサービスを有効化するかかどうかを選択します。デフォルトの候補としてサーバRelexiveを設定した場合は、このフィールドを有効に設定する必要があります。

ステップ 6 プライマリサーバーとセカンダリサーバーのipアドレスまたはホスト名を入力します。

ステップ 7 TURN Server **のトランスポート**タイプを [**自動 (default)](defaultsetting)**、UDP 、TCP、または TLS に設定します。

ステップ 8 ターンサーバーに**ユーザ名**と**パスワード**を入力します。

ステップ 9 [保存（Save）] をクリックします。

（注） 共通の電話プロファイル用に ICE を設定した場合は、電話機を使用して、そのプロファイルを使用できるようにする共通の電話プロファイルに電話機を関連付ける必要があります。[電話の設定（Phone Configuration）] ウィンドウから、プロファイルを電話に適用できます。

モバイルおよびリモートアクセス用の電話セキュリティプロファイルの設定

モバイルおよびリモートアクセスのエンドポイントで使用する電話セキュリティプロファイルを設定するには、この手順を使用します。

手順

ステップ 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）]**>**[セキュリティ（Security）]**>**[電話セキュリティ プロファイル（Phone Security Profile）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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、デバイス タイプを選択します。たとえば、Jabber アプリケーションであれば **Cisco Unified Client Service Framework** を選択できます。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 プロファイルの [名前（Name）] を入力します。モバイルおよびリモートアクセスの場合、名前は FQDN 形式である必要があり、エンタープライズドメインを含める必要があります。

ステップ 6 [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。

（注） このフィールドは、[暗号化（Encrypted）] に設定する必要があります。そうでない場合、Expressway が通信を拒否します。

ステップ 7 [トランスポートタイプ（Transport Type）] を [TLS] に設定します。

ステップ 8 このオプションを有効化した電話機ではモバイルおよびリモートアクセスが機能しないため、次の電話機では [**TFTP暗号化設定（TFTP Encrypted Config**）] チェックボックスをオフのままにします。DX シリーズ、IP Phone 7800、または IP Phone 8811、8841、8845、8861、および 8865

ステップ 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。

ステップ 10 [保存（Save）] をクリックします。

（注） 各モバイルおよびリモートアクセスのエンドポイントの電話機の設定にこのプロファイルを適用する必要があります。

Cisco Jabber ユーザの MRA アクセス ポリシーの設定

Cisco Jabber のユーザに MRA アクセスポリシーを設定するには、次の手順を使用します。MRA 機能を使用するには、Cisco Jabberユーザーのユーザー プロファイルで MRA アクセスを有効にする必要があります。Cisco Jabber を使用した MRA アクセス ポリシーをサポートする Expressway の最小リリースは X8.10 です。

（注） 非 Jabber のユーザには、MRA アクセスポリシーは不要です。

（注） ユーザプロファイルの詳細については、「ユーザプロファイルの概要（311 ページ）」を参照してください。

手順

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 7 このユーザプロファイルに関連付けられた Cisco Jabber ユーザ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、[Jabber ポリシー（Jabber 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。

ステップ 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。[Jabberデスクトップクライアントポリシー（Jabber Desktop Client Policy）] および [Jabber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。

ステップ 9 [保存（Save）] をクリックします。

MRA ユーザの設定

Cisco Jabber のユーザの場合、設定した MRA アクセスポリシーは、LDAP 同期中に Cisco Jabber ユーザに関連付ける必要があります。エンドユーザをプロビジョニングする方法については、「エンド ユーザの設定 （277 ページ）」を参照してください。

MRA のエンドポイントの設定

モバイルおよびリモートアクセス用のエンドポイントをプロビジョニングし、設定します。

- Cisco Jabber クライアントについては、次の手順を参照してください。 Cisco Jabber の設定タスク フロー （569 ページ）
- その他のエンドポイントについては、次の手順を参照してください。 エンドポイント デバイス設定 （351 ページ）

Cisco Expresswayのモバイルおよびリモートアクセスの設定

モバイルおよびリモートアクセス用の Cisco Expressway の設定方法に関しては、『Cisco Expressway 導入ガイド』の「モバイルおよびリモートアクセス」を参照してください。

第 41 章

アナログ電話アダプタの設定

アナログ電話アダプタの概要

Cisco アナログ電話アダプタ（ATA）は、通常のアナログ電話と IP ベースのテレフォニー ネットワークとのインターフェイスとなるアナログ電話アダプタとして機能します。Cisco ATA は通常のアナログ電話をインターネット電話に変換します。各アダプタは 2 個の音声ポートをサポートし、それぞれに固有の電話番号を割り当てることができます。

他の IP デバイスと同様に、Cisco ATA は TFTP サーバからプロファイルと Unified Communications Manager のリストを受信します。TFTP サーバに設定ファイルが存在しない場合、Cisco ATA は、TFTP サーバの名前または IP アドレスとポート番号を、プライマリ Unified Communications Manager の名前または IP アドレスとポート番号として使用します。

Cisco ATA：

- 1 つの 10 BaseT RJ-45 ポート、および 2 つの RJ-11 FXS 標準アナログ電話ポート
- G.711 alaw、G.711 mulaw、G.723とG.729a音声コーデックなど、さまざまなコーデックに対応しています
- 音声を IP データパケットに変換します。
- リダイヤル、スピードダイヤル、自動転送、コール待機、コール保留、転送、会議、ボイスメッセージング、メッセージ受信インジケータ、オフフック呼び出し音、発信者 ID、被発信者 ID、およびコール待機の発信者 ID をサポート

ATA 180 シリーズは SCCP を使用しますが、ATA 190 シリーズは SIP を使用します。詳細については、ATAのドキュメントを参照してください。

- ATA 180シリーズ： https://www.cisco.com/c/en/us/support/unified-communications/ata-180-series-analog-telephone-adaptors/tsd-products-support-series-home.html
- ATA 190シリーズ： https://www.cisco.com/c/en/us/support/unified-communications/ata-190-series-analog-telephone-adapters/tsd-products-support-series-home.html

アナログ電話アダプタの設定

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。**[電話の検索と一覧表示（Find and List Phones）]** ウィンドウが表示されます。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウン リストから、使用しているアナログ電話アダプタ モデルを選択して、[次へ（Next）] をクリックします。
[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 [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、「関連項目」の項を参照してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [設定の適用（Apply Config）] をクリックして、電話に変更を適用し、同期します。

アナログ電話アダプタ 186 設定フィールド

表 *21* : アナログ電話アダプタ *186* 設定フィールド

フィールド	説明
MAC アドレス（MAC Address）	ATA 186 を特定する Media Access Control（MAC）アドレスを入力します。値が 12 桁の 16 進文字列で構成されていることを確認します。 次のいずれかの方法で、ATA 186 の MAC アドレスを判別できます。 • ATA 186 の背面にある MAC ラベルを確認します。 • ATA 186 の ウェブ ページを表示し、[デバイス情報（Device Information）] ハイパーリンクをクリックします。
[説明（Description）]	ATA 186 の説明テキストを入力します。 このフィールドには、128 文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。

フィールド	説明
[デバイスプール（Device Pool）]	ATA 186 を割り当てるデバイス プールを選択します。デバイス プールでは、複数のデバイスに共通の特性（リージョン、日時グループ、ソフトキー テンプレートなど）のセットを定義します。 デバイス プール構成の設定を確認するには、[詳細の表示（View Details）] リンクをクリックします。
[共通デバイス設定（Common Device Configuration）]	ATA 186 を割り当てる共通デバイス設定を選択します。 [共通デバイス設定（Common Device Configuration）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[電話ボタンテンプレート（Phone Button Template）]	適切な電話ボタン テンプレートを選択します。電話ボタン テンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能（回線、スピード ダイヤルなど）を使用するかを特定します。
[共通の電話プロファイル（Common Phone Profile）]	ドロップダウン リストで、使用可能な共通の電話プロファイルのリストから共通の電話プロファイルを選択します。 [共通の電話プロファイル（Common Phone Profile）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[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を使用から、コーリングサーチスペースを選択するか、コーリングサーチスペースをデフォルトの [なし（None）] のままにします。
[AARコーリングサーチスペース（AAR Calling Search Space）]	ドロップダウン リストから、自動代替ルーティング（AAR）を実行したときに使用するデバイスの適切なコーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[メディアリソースグループリスト（Media Resource Group List）]	適切なメディア リソース グループ リストを選択します。メディア リソース グループ リストは、優先順位順に並べられたメディア リソース グループから構成されます。 [<なし>（<None>）] を選択すると、Cisco Unified CM はデバイス プールで定義されたメディア リソース グループ リストを使用します。
[ロケーション（Location）]	ドロップダウン リストから、デバイス プール内の電話およびゲートウェイと関連付けられている場所を選択します。
[AARグループ（AAR Group）]	このデバイスの自動代替ルーティング（AAR）グループを選択します。AAR グループはプレフィックス番号を設定します。この番号は、帯域幅不足のためにブロックされるコールをルーティングする際に使用されます。Cisco Unified CM は、デバイス プールまたは回線と関連付けられている AAR グループを使用します。

フィールド	説明
[ユーザーロケール（User Locale）]	ドロップダウン リストから、ATA 186 と関連付けられているユーザー ロケールを選択します。そのユーザー ロケールは、言語とフォントを含んだ、ユーザーをサポートする一連の詳細情報を識別します。 ユーザー ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたユーザー ロケールを使用します。
[ネットワークロケール（Network Locale）]	ドロップダウン リストから、ATA 186 と関連付けられているネットワーク ロケールを選択します。ネットワーク ロケールには、特定の地理的領域の電話が使用するトーンとパターンの定義が含まれています。 ネットワーク ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたネットワーク ロケールを使用します。
[デバイスモビリティモード（Device Mobility Mode）]	ドロップダウン リストから、このデバイスのデバイス モビリティ機能をオンまたはオフにします。デフォルトのデバイス モビリティ モードを使用する場合は、[デフォルト（Default）] を選択します。デフォルト設定では、デバイス移行モードのサービスパラメータの値が使用されます。
[オーナー（Owner）]	オーナータイプには、[ユーザー（User）]または[匿名（Anonymous）]（パブリック/共有スペース）を選択します。
[オーナーのユーザーID（Owner User ID）]	ドロップダウン リストから、割り当てられた電話ユーザーのユーザー ID を選択します。ユーザー ID は、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。ユーザー ID をデバイスに割り当てると、そのデバイスが [ライセンスの使用状況レポート（License Usage Report）] で 「」[未割り当てのデバイス（Unassigned Devices）] から 「」[ユーザー（Users）] に移動することにもなります。 （注） エクステンションモビリティを使用する場合は、このフィールドを設定しないでください。エクステンション モビリティでは、デバイスのオーナーはサポートされていません。
[電話ロード名（Phone Load Name）]	ATA 186のカスタムソフトウェアを入力します。

フィールド	説明
[トラステッドリレーポイントを使用（Use Trusted Relay Point）]	次の値のいずれかを選択します。 • [オフ（Off）]：このデバイスで、トラステッドリレー ポイント（TRP）の使用を無効にするには、この値を選択します。この設定は、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[トラステッドリレーポイントを使用（Use Trusted Relay Point）]設定よりも優先されます。 • [オン（On）]：このデバイスでTRPの使用を有効にする場合は、この値を選択します。この設定は、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[トラステッドリレーポイントを使用（Use Trusted Relay Point）]設定よりも優先されます。 • [デフォルト（Default）]：この値を選択した場合、このデバイスが関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用（Use Trusted Relay Point）]設定を使用します。
常にプライム回線を使用する（Always Use Prime Line）	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。 • [オン（On）]：電話機がアイドル状態（オフ フック）になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールは鳴り続け、電話機ユーザはそれらの他の回線を選択して、これらのコールに応答する必要があります。 • デフォルト：Unified Communications Managerは、[常にプライム回線を使用する（Always Use Prime Line）]サービス パラメータの設定を使用します。これにより、Cisco CallManagerサービスがサポートされます。

フィールド	説明
ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態の場合、電話のメッセージ ボタンを押すと、ボイス メッセージが設定されている回線からボイスメッセージシステムに自動的にダイヤルされます。Unified Communications Manager は、常に音声メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザーが [メッセージ（Messages）] ボタンを押すと、プライマリ回線が使用されます。 • [オン（On）]：電話がアイドル状態の場合に電話のメッセージ ボタンを押すと、電話のプライマリ回線がボイス メッセージを受信するアクティブな回線になります。 • [デフォルト（Default）]：Unified Communications Manager は、[ボイスメッセージに常にプライム回線を使用する（Always Use Prime Line for Voice Message）] サービス パラメータの設定を使用します。これにより、Cisco CallManager サービスがサポートされます。
[地理位置情報（GeoLocation）]	ドロップダウン リストから地理位置情報を選択します。 [未指定の地理位置情報（Unspecified geolocation）] を選択すると、このデバイスを地理位置情報に関連付けないように指定できます。 さらに、**[システム（System）] > [地理位置情報の設定（Geolocation Configuration）]** メニュー オプションで設定した地理位置情報も選択できます。
[プレゼンテーションインジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）]	コール単位でコール表示制限を設定する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、Unified Communications Manager は内線コールについて受信するすべての表示制限を無視します。 この設定と、トランスレーション パターン レベルでの発信者回線 ID の表示および接続回線 ID の表示の設定を組み合わせて使用します。これらの設定を組み合わせて使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。

フィールド	説明
[CTIからのデバイスの制御を許可（Allow Control of Device from CTI）]	CTI に対してこのデバイスの制御と監視を許可する場合は、このチェックボックスをオンにします。 関連付けられている電話番号が共有回線を指定している場合、少なくとも 1 つの関連付けられているデバイスで、CTI がサポートするデバイス タイプとプロトコルの組み合わせが指定されていれば、チェックボックスを有効にする必要があります。
[ハントグループにログイン（Logged into Hunt Group）]	CTIポートをハントリストに追加したら、管理者はこのチェックボックスをオン（またはオフ）にすることによって、ユーザーをログインまたはログアウトさせることができます。 ユーザーは電話のソフトキーを使用して、電話をハント リストにログインまたはログアウトします。
[リモートデバイス（Remote Device）]	このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。 **ヒント** この機能はリソースを消費するため、シグナリングの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。
[ホットラインデバイス（Hot Line Device）]	このデバイスをホットラインデバイスにするには、このチェックボックスをオンにします。ホットライン デバイスは他のホットライン デバイスにのみ接続できます。これは PLAR の拡張機能です。PLAR では、電話がオフフックになった場合に自動的に 1 つの電話番号にダイヤルするよう電話を設定します。ホットラインによって、PLAR を使用するデバイスに追加の制限を適用できます。 ホットラインを実装するには、補足サービス ソフトキーを含まないソフトキー テンプレートを作成し、それをホットライン デバイスに適用する必要があります。

[番号表示トランスフォーメーション（Number Presentation Transformation）]

表 *22 : [*この電話からのコールの発信者*ID*（*Caller ID For Calls From This Phone*）*]*

フィールド	説明
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーション CSS に、このデバイスに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。

フィールド	説明
[デバイスプールの発信側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイス プールに設定されている発信側トランスフォーメーションCSSを使用する場合は、このボックスをオンにします。このチェックボックスを選択しない場合、デバイスは [トランク設定（Trunk Configuration）] ウィンドウで設定した発信側変換 CSS を使用します。

表 *23* : [リモート番号（*Remote Number*）]

フィールド	説明
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	ドロップダウン リストから、このデバイスに受信したコールのリモート発信者番号に適用する、発信側トランスフォーメーション パターンを含むコーリング サーチ スペース（CSS）を選択します。
[デバイスプールの発信側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	リモート通話とリモート接続番号の変換に、このデバイスが属するデバイス プールで設定されている発信側トランスフォーメーション CSS を適用するには、このチェックボックスをオンにします。

表 *24* : [プロトコル固有情報（*Protocol Specific Information*）]

フィールド	説明
[BLFプレゼンスグループ（BLF Presence Group）]	ドロップダウン リストから、エンドユーザーの話中ランプ フィールド（BLF）プレゼンス グループを選択します。選択したグループは、エンド ユーザーがモニター可能な接続先を指定します。 BLF プレゼンス グループのデフォルト値は [標準のプレゼンスグループ（Standard Presence group）] であり、インストール時に設定されます。Cisco Unified CM Administration で設定されている BLF プレゼンス グループは、ドロップダウン リストにも表示されます。
[デバイスのセキュリティプロファイル（Device Security Profile）]	デバイスに適用するセキュリティ プロファイルを選択します。 Unified Communications Manager Administration で設定するすべてのデバイスに、セキュリティ プロファイルを適用する必要があります。

フィールド	説明
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされるSUBSCRIBEコーリングサーチスペースは、エンドユーザから受け取ったプレゼンス要求をUnified Communications Managerがルーティングする方法を決定します。この設定では、エンドユーザーのプレゼンス（SUBSCRIBE）要求のコール処理サーチスペースと別にコーリングサーチスペースを適用できます。 ドロップダウンリストから、エンドユーザーのプレゼンス要求に使用するSUBSCRIBEコーリングサーチスペースを選択します。Cisco Unified Communications Manager Administrationで設定するすべてのコーリングサーチスペースが、[SUBSCRIBEコーリングサーチスペース（SUBSCRIBE Calling Search Space）]ドロップダウンリストに表示されます。 ドロップダウンリストから、エンドユーザーに別のコーリングサーチスペースを選択しない場合、SUBSCRIBEコーリングサーチスペースのデフォルトは[なし（None）]に設定されます。 この目的専用のSUBSCRIBEコーリングサーチスペースを設定するには、他のコーリングサーチスペースと同様に新しいコーリングサーチスペースを設定します。
[不在ポート（Unattended Port）]	このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。
[RFCC 2833 Disabled（RFCC 2833の無効化）]	SCCPを実行しているデバイスの場合は、このチェックボックスをオンにしてRFC2833のサポートを無効にします。

表 *25 :* 製品固有の設定

フィールド	説明
デバイス製造元が定義するモデル固有の設定フィールド	製品固有の設定項目のフィールドの説明とヘルプを表示するには、[製品固有の設定（Product Specific Configuration）]エリアで[?]「」情報アイコンをクリックし、ポップアップダイアログボックスでヘルプを表示します。 詳細については、ATA 186のマニュアルを参照してください。

アナログ電話アダプタ 187 設定フィールド

表 *26 :* アナログ電話アダプタ *187* 設定フィールド

フィールド	説明
MACアドレス（MAC Address）	ATA 187 を識別する Media Access Control（MAC）アドレスを入力します。値が 12 桁の 16 進文字列で構成されていることを確認します。 次のいずれかの方法で、ATA 187 の MAC アドレスを判別できます。 • ATA 187 の背面にある MAC ラベルを確認する。 • ATA 187 の ウェブ ページを表示し、[デバイス情報（Device Information）] ハイパーリンクをクリックする。
[説明（Description）]	ATA 187 のテキストの説明を入力します。 このフィールドには、128 文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。
[デバイスプール（Device Pool）]	ATA 187 を割り当てるデバイス プールを選択します。デバイス プールでは、複数のデバイスに共通の特性（リージョン、日時グループ、ソフトキー テンプレートなど）のセットを定義します。 デバイス プール構成の設定を確認するには、[詳細の表示（View Details）] リンクをクリックします。
[共通デバイス設定（Common Device Configuration）]	ATA 187 を割り当てる共通デバイス設定を選択します。 [共通デバイス設定（Common Device Configuration）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[電話ボタンテンプレート（Phone Button Template）]	適切な電話ボタンテンプレートを選択します。電話ボタンテンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能（回線、スピード ダイヤルなど）を使用するかを特定します。
[共通の電話プロファイル（Common Phone Profile）]	ドロップダウン リストで、使用可能な共通の電話プロファイルのリストから共通の電話プロファイルを選択します。 [共通の電話プロファイル（Common Phone Profile）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストを使用から、コーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。

フィールド	説明
[AARコーリングサーチスペース（AAR Calling Search Space）]	ドロップダウン リストから、自動代替ルーティング（AAR）を実行したときに使用するデバイスの適切なコーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[メディアリソースグループリスト（Media Resource Group List）]	適切なメディア リソース グループ リストを選択します。メディア リソース グループ リストは、優先順位順に並べられたメディア リソース グループから構成されます。 [<なし>（<None>）] を選択すると、Cisco Unified CM はデバイス プールで定義されたメディア リソース グループ リストを使用します。
[ユーザー保留 MOH 音源（User Hold MOH Audio Source）]	ドロップダウン リストから、ユーザーが保留操作を開始する場合に保留音（MOH）として使用するオーディオ ソースを選択します。
[ロケーション（Location）]	ドロップダウン リストから、デバイス プール内の電話およびゲートウェイと関連付けられている場所を選択します。
[AARグループ（AAR Group）]	このデバイスの自動代替ルーティング（AAR）グループを選択します。AAR グループはプレフィックス番号を設定します。この番号は、帯域幅不足のためにブロックされるコールをルーティングする際に使用されます。AAR グループが指定されていない場合、Cisco Unified CM はデバイス プールまたは回線に関連付けられている AAA グループを使用します。
[ユーザーロケール（User Locale）]	ドロップダウン リストから、CTI ポートに関連付けられたユーザー ロケールを選択します。そのユーザー ロケールは、言語とフォントを含んだ、ユーザーをサポートする一連の詳細情報を識別します。 ユーザー ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたユーザー ロケールを使用します。
[ネットワークロケール（Network Locale）]	ドロップダウン リストから、CTI ポートに関連付けられたネットワーク ロケールを選択します。ネットワーク ロケールには、特定の地理的領域の電話が使用するトーンとパターンの定義が含まれています。 ネットワーク ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたネットワーク ロケールを使用します。

フィールド	説明
[ビルトインブリッジ（Built In Bridge）]	[ビルトインブリッジ（Built In Bridge）] ドロップダウン リストを使用して割り込み機能用の組み込み型会議ブリッジを有効または無効にします。次のいずれかを実行します。 • オン • オフ • デフォルト
[プライバシー（Privacy）]	プライバシーについて、[プライバシー（Privacy）] ドロップダウン リストから [オン（On）] を選択します。
[デバイスモビリティモード（Device Mobility Mode）]	ドロップダウン リストから、このデバイスのデバイス モビリティ機能をオンまたはオフにします。デフォルトのデバイス モビリティ モードを使用する場合は、[デフォルト（Default）] を選択します。デフォルトの設定では、デバイスの [デバイス モビリティ モード（Device Mobility Mode）] サービス パラメータの値が使用されます。
[オーナー（Owner）]	オーナーのタイプとして、[ユーザー（User）] または [名前非表示（パブリック/共有スペース）（Anonymous (Public/Shared Space)）] を選択します。
[オーナーのユーザー ID（Owner User ID）]	ドロップダウン リストから、割り当てられた電話ユーザーのユーザー ID を選択します。ユーザー ID は、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。デバイスにユーザー ID を割り当てると、[ライセンスの使用状況レポート（License Usage Report）] でデバイスが [未割り当てデバイス（Unassigned Devices）] から [ユーザー（Users）] に移動します。 （注） エクステンション モビリティを使用する場合は、このフィールドを設定しないでください。エクステンション モビリティでは、デバイスのオーナーはサポートされていません。
[電話ロード名（Phone Load Name）]	ATA 187 のカスタム ソフトウェアを入力します。

フィールド	説明
[トラステッドリレーポイントを使用（Use Trusted Relay Point）]	次の値のいずれかを選択します。 • [オフ（Off）]：このデバイスで、トラステッド リレー ポイント（TRP）の使用を無効にするには、この値を選択します。この設定は、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[トラステッドリレーポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • [オン（On）]：このデバイスでの TRP の使用を有効にする場合は、この値を選択します。この設定は、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[トラステッドリレーポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • [デフォルト（Default）]：この値を選択した場合、デバイスはこのデバイスが関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用（Use Trusted Relay Point）] 設定を使用します。
常にプライム回線を使用する（Always Use Prime Line）	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。 • [オン（On）]：電話機がアイドル状態（オフ フック）になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールは鳴り続け、電話機ユーザはそれらの他の回線を選択して、これらのコールに応答する必要があります。 • デフォルト：Unified Communications Manager は、[常にプライム回線を使用する（Always Use Prime Line）] サービス パラメータの設定を使用します。これにより、Cisco CallManager サービスがサポートされます。

フィールド	説明
ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態の場合、電話のメッセージ ボタンを押すと、ボイス メッセージが設定されている回線からボイス メッセージ システムに自動的にダイヤルされます。Unified Communications Manager は、常に音声メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザーが [メッセージ（Messages）] ボタンを押すと、プライマリ回線が使用されます。 • [オン（On）]：電話がアイドル状態の場合に電話のメッセージ ボタンを押すと、電話のプライマリ回線がボイス メッセージを受信するアクティブな回線になります。 • [デフォルト（Default）]：Unified Communications Manager は、[ボイスメッセージに常にプライム回線を使用する（Always Use Prime Line for Voice Message）] サービス パラメータの設定を使用します。これにより、Cisco CallManager サービスがサポートされます。
[地理位置情報（GeoLocation）]	ドロップダウン リストから地理位置情報を選択します。 [未指定の地理位置情報（Unspecified geolocation）] を選択すると、このデバイスを地理位置情報に関連付けないように指定できます。 さらに、**[システム（System）] > [地理位置情報の設定（Geolocation Configuration）]** メニュー オプションで設定した地理位置情報も選択できます。
[プレゼンテーション インジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）]	コール単位でコール表示制限を設定する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、Unified Communications Manager は内線コールについて受信するすべての表示制限を無視します。 この設定と、トランスレーション パターン レベルでの発信者回線 ID の表示および接続回線 ID の表示の設定を組み合わせて使用します。これらの設定を組み合わせて使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。
[ハントグループにログイン（Logged into Hunt Group）]	ATA 187 をハント リストに追加したら、管理者はこのチェックボックスをオン（またはオフ）にすることによって、ユーザーをログインまたはログアウトさせることができます。 ユーザーは電話のソフトキーを使用して、電話をハント リストにログインまたはログアウトします。

フィールド	説明
[リモートデバイス（Remote Device）]	このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。 **ヒント** この機能はリソースを消費するため、シグナリングの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。
[保護されたデバイス（Protected Device）]	電話機を保護されたデバイスとして指定するには、このチェックボックスをオンにします。この場合、電話機が2秒間トーンを再生してユーザーにコールが暗号化されていることを通知できます。また、発信側と着信側の両方の電話機が保護されたデバイスとして設定できます。このトーンは、コールが応答されたとき、発信側と着信側の両者に対して再生されます。このトーンは、発信側と着信側の両方の電話機が保護されていて、なおかつ暗号化メディア上でコールが行われたときでなければ再生されません。 このチェックボックスをオンにすると、再生するセキュア通知トーンの複数の設定要件のうち 1 つのみが表示されます。セキュア通知トーン機能と設定要件の詳細については、『*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。 このチェックボックスがオンで、システムがコールは暗号化されていないと判断すると、電話は非セキュア通知トーンを再生して、コールが保護されていないことをユーザーに通知します。

[番号表示トランスフォーメーション（Number Presentation Transformation）]

表 *27 : [*この電話からのコールの発信者*ID*（*Caller ID For Calls From This Phone*）*]*

フィールド	説明
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーション CSS に、このデバイスに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。
[デバイスプールの発信側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイス プールに設定されている発信側トランスフォーメーション CSS を使用する場合は、このボックスをオンにします。このチェックボックスを選択しない場合、デバイスは [トランク設定（Trunk Configuration）] ウィンドウで設定した発信側変換 CSS を使用します。

表 *28 : [*リモート番号（***Remote Number***）*]*

フィールド	説明
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	ドロップダウン リストから、このデバイスに受信したコールのリモート発信者番号に適用する、発信側トランスフォーメーション パターンを含むコーリング サーチ スペース（CSS）を選択します。
[デバイスプールの発信側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	リモート通話とリモート接続番号の変換に、このデバイスが属するデバイス プールで設定されている発信側トランスフォーメーション CSS を適用するには、このチェックボックスをオンにします。

表 *29 : [*プロトコル固有情報（***Protocol Specific Information***）*]*

フィールド	説明
[パケットキャプチャモード（Packet Capture Mode）]	この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。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。 • [なし（None）]：このオプションは、パケット キャプチャが発生しないことを示します（デフォルト設定）。この設定は、パケット キャプチャの完了後に行います。 • [バッチ処理モード（Batch Processing Mode）]：Cisco Unified CM が、復号されたメッセージや暗号化されていないメッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムでは、毎日新しいファイルが新しい暗号キーを使用して作成されます。Cisco Unified CM はファイルを 7 日間保存し、さらにファイルを暗号化するキーを安全な場所に保存します。Cisco Unified CM は、PktCap 仮想ディレクトリにファイルを保存します。1 つのファイルの中に、タイムスタンプ、送信元 IP アドレス、送信元 IP ポート、宛先 IP アドレス、パケットのプロトコル、メッセージの長さ、およびメッセージが保持されます。TAC のデバッグ ツールでは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを保持している暗号化済みファイルを 1 つだけ要求します。同様にこのツールでは、暗号化ファイルを復号化するためのキー情報を要求します。

フィールド	説明
[パケットキャプチャ時間（Packet Capture Duration）]	この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。 このフィールドには、1 つのパケット キャプチャ セッションに割り当てる時間の上限（分単位）を指定します。デフォルト設定は 0 で、範囲は 0 ～ 300 分です。 パケット キャプチャを開始するには、フィールドに 0 以外の値を入力します。パケット キャプチャが完了すると、値 0 が表示されます。
[BLFプレゼンスグループ（BLF Presence Group）]	ドロップダウン リストから、エンドユーザーの話中ランプ フィールド（BLF）プレゼンス グループを選択します。選択したグループは、エンド ユーザーがモニター可能な接続先を指定します。 BLF プレゼンス グループのデフォルト値は [標準のプレゼンスグループ（Standard Presence group）] であり、インストール時に設定されます。Cisco Unified CM Administration で設定されている BLF プレゼンス グループは、ドロップダウン リストにも表示されます。
[SIPダイヤルルール（SIP Dial Rules）]	必要に応じて、適切な SIP ダイヤル ルールを選択します。SIP ダイヤル ルールは、Cisco Unified IP Phone 7940 および 7960 のローカル ダイヤル プランを提供するため、ユーザーは、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。 SIP を実行している IP 電話にダイヤル ルールを適用しない場合は、[SIP ダイヤルルール（SIP Dial Rules）] フィールドを [<なし>（<None>）] に設定したままにします。これは、コールが処理される前に、ユーザーがダイヤル ソフトキーを使用するか、タイマーが切れるまで待つ必要があることを示します。
[MTP優先発信コーデック（MTP Preferred Originating Codec）]	メディア ターミネーション ポイントが SIP のコールに必要な場合は、ドロップダウン リストから使用するコーデックを選択します。
[デバイスのセキュリティプロファイル（Device Security Profile）]	デバイスに適用するセキュリティ プロファイルを選択します。 Unified Communications Manager Administration で設定するすべてのデバイスに、セキュリティ プロファイルを適用する必要があります。

フィールド	説明
[再ルーティング用コーリングサーチスペース（Rerouting Calling Search Space）]	ドロップダウン リストから、再ルーティングに使用するコーリング サーチ スペースを選択します。 リファラーの再ルーティング コーリング サーチ スペースを使用して、参照先へのルートが検索されます。再ルーティング コーリング サーチ スペースが原因で参照が失敗すると、Refer Primitive は 「405 Method Not Allowed」 メッセージによって要求を拒否します。 リダイレクト（3xx）プリミティブおよび転送機能も再ルーティング コーリング サーチ スペースを使用して、リダイレクト先または転送先を検索します。
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされる SUBSCRIBE コーリング サーチ スペースは、エンドユーザから受け取ったプレゼンス要求を Unified Communications Manager がルーティングする方法を決定します。この設定では、エンド ユーザーのプレゼンス（SUBSCRIBE）要求のコール処理サーチ スペースと別にコーリング サーチ スペースを適用できます。 ドロップダウン リストから、エンドユーザーのプレゼンス要求に使用する SUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified Communications Manager Administration で設定するすべてのコーリング サーチ スペースが、[SUBSCRIBE コーリングサーチスペース（SUBSCRIBE Calling Search Space）] ドロップダウン リストに表示されます。 ドロップダウン リストから、エンド ユーザーに別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは [なし（None）] に設定されます。 この目的専用の SUBSCRIBE コーリング サーチ スペースを設定するには、他のコーリング サーチ スペースと同様に新しいコーリング サーチ スペースを設定します。
[SIPプロファイル（SIP Profile）]	デフォルトの SIP プロファイルまたは作成済みの特定のプロファイルを選択します。SIP プロファイルでは、登録タイマーおよびキープアライブ タイマー、メディア ポート、Do Not Disturb（サイレント）制御など、電話機の特定の SIP 情報を提供します。
[ダイジェストユーザー（Digest User）]	ダイジェスト認証（SIP セキュリティ）で使用するこの設定の電話機に関連付けるエンド ユーザーを選択します。 選択するユーザーのダイジェスト クレデンシャルが [エンドユーザーの設定（End User Configuration）] ウィンドウで設定されていることを確認してください。 電話設定を保存し、設定の更新内容を電話に適用すると、ユーザーのダイジェスト クレデンシャルが電話の設定ファイルに追加されます。

フィールド	説明
[メディアターミネーションポイントが必須（Media Termination Point Required）]	このフィールドを使用して、ATA 187 がサポートしない機能（保留や転送など）を実装するために、メディア ターミネーションポイントを使用するかどうかを指示します。 MTP を使用して機能を実装する場合は、[メディアターミネーションポイントが必須（Media Termination Point Required）] チェックボックスをオンにします。MTP を使用して機能を実装しない場合は、[メディアターミネーションポイントが必須（Media Termination Point Required）] チェックボックスをオフにします。 このチェックボックスは、ATA 187 クライアントおよび H.245 Empty Capabilities セットをサポートしない ATA 187 デバイスの場合、または単一のソースを介してメディア ストリーミングを終了させる場合にのみ使用します。 このチェックボックスをオンにして、MTP を必須とし、このデバイスをビデオ コールのエンドポイントにすると、コールはオーディオのみになります。
[不在ポート（Unattended Port）]	このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。
[DTMF受信が必要（Require DTMF Reception）]	SIP と SCCP を実行しているデバイスの場合に、この電話の DTMF 受信を必須にするには、このチェックボックスをオンにします。 （注） Cisco Unified Mobility 機能の設定で、SIP トランク（クラスタ間トランク（ICT）またはゲートウェイ）経由で IP 電話のリモート接続先としてクラスタ間 DN を使用する場合、エンタープライズ機能アクセス ミッドコール機能に不可欠な DTMF 番号をアウト オブ バンドで受信できるように、このチェックボックスをオンにします。

表 *30 : [*認証局プロキシ機能（*CAPF*）情報（*Certification Authority Proxy Function (CAPF) Information*）*]*

フィールド	説明
[証明書の操作（Certificate Operation）]	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [保留中の操作なし（No Pending Operation）]：証明書の操作が行われない場合に表示されます（デフォルトの設定）。 • [インストール/更新（Install/Upgrade）]：電話機に新しい証明書をインストールするか、既存のローカルで有効な証明書をアップグレードします。 • [削除（Delete）]：電話機に存在するローカルで有効な証明書を削除します。 • [トラブルシューティング（Troubleshoot）]：ローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）を取得し、CAPF トレース ファイルで証明書クレデンシャルを表示できます。電話機に両方の証明書タイプが存在する場合、Cisco Unified CM は、証明書のタイプごとに 1 つずつ、2 つのトレース ファイルを作成します。 [トラブルシューティング（Troubleshooting）] オプションを選択して、電話に LSC または MIC が存在することを確認できます。

フィールド	説明
[認証モード（Authentication Mode）]	

フィールド	説明
	このフィールドでは、電話機が CAPF 証明書の操作時に使用する認証方法を選択できます。 ドロップダウン リストから、次のオプションのいずれかを選択します。 • [認証文字列（By Authentication String）]：ユーザーが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 • [Null ストリング（By Null String）]：ユーザーの介入なしで、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 このオプションではセキュリティが確保されません。したがって、セキュアな閉じた環境の場合にだけこのオプションを選択することを強く推奨します。 • [既存の証明書（LSCを優先）（By Existing Certificate (Precedence to LSC)）]：電話機に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）が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に MIC と LSC が存在する場合、LSC によって認証が行われます。電話機に LSC が存在しないが、MIC が存在する場合、MIC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • [既存の証明書（MICを優先）（By Existing Certificate (Precedence to MIC)）]：電話機に LSC または MIC が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に MIC が存在する場合、電話機に LSC が存在するかどうかに関係なく、MIC によって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在すること

フィールド	説明
	を確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 （注） [電話セキュリティプロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
[認証文字列（Authentication String）]	[認証モード（Authentication Mode）] ドロップダウン リストの [認証文字列（By Authentication String）] オプションを選択した場合、このフィールドが適用されます。手動で文字列を入力するか、[文字列の生成（Generate String）] ボタンをクリックして、文字列を生成します。4 桁から 10 桁の文字列になるようにしてください。 ローカルで有効な証明書をインストール、アップグレード、削除、トラブルシューティングするには、電話機ユーザーまたは管理者が電話機に認証文字列を入力する必要があります。
[キー サイズ（ビット）（Key Size (Bits)）]	CAPF で使用されるこの設定では、ドロップダウン リストから証明書のキー サイズを選択します。デフォルト設定は 1024 です。その他のオプションには 512 と 2048 があります。 デフォルトの設定より大きいキー サイズを選択すると、電話機でキーの生成に必要なエントロピーを生成するのに時間がかかります。キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。 （注） [電話セキュリティプロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
[操作の完了期限（Operation Completes by）]	このフィールドは、[インストール/アップグレード（Install/Upgrade）]、[削除（Delete）]、[トラブルシューティング（Troubleshoot）] の証明書の操作オプションをサポートし、操作の完了期限を指定します。 表示される値は、パブリッシャ データベース サーバーに適用されます。
[証明書の操作ステータス（Certificate Operation Status）]	このフィールドには、証明書の操作の進捗状況が表示されます。たとえば、<操作タイプ>保留中、失敗、成功などです。ここで、操作タイプは [インストール/アップグレード（Install/Upgrade）]、[削除（Delete）]、[トラブルシューティング（Troubleshoot）] 証明書の操作オプションのいずれかになります。このフィールドに表示される情報は変更できません。

表 *31* : *[セキュアシェルユーザー（Secure Shell User）]*

フィールド	説明
[セキュアシェルユーザー（Secure Shell User）]	セキュア シェル ユーザーのユーザー ID を入力します。最大 50 文字の英数字または特殊文字を入力できます。無効な文字は、"、%、&、<、>、\ です。このフィールドは、設定している電話デバイスが SSH アクセスをサポートしている場合に表示されます。 Cisco Technical Assistance Center（TAC）では、トラブルシューティングやデバッグを行うときにセキュア シェルを使用します。TAC にお問い合わせください。 Cisco Unified CM が SSH クレデンシャルを平文で電話機に送信しないようにするために、暗号化された電話の設定ファイルを設定する方法については、このリリースの『*Cisco Unified Communications Manager* セキュリティ 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。
[セキュアシェルパスワード（Secure Shell Password）]	セキュア シェル ユーザーのパスワードを入力します。最大 200 文字の英数字または特殊文字を入力できます。無効な文字は、"、%、&、<、>、\ です。TAC にお問い合わせください。 『*Cisco Unified Communications Manager* セキュリティ 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。

表 *32* : 製品固有の設定

フィールド	説明
デバイス製造元が定義するモデル固有の設定フィールド	製品固有の設定項目のフィールドの説明とヘルプを表示するには、[製品固有の設定（Product Specific Configuration）] エリアで [?]「」情報アイコンをクリックし、ポップアップ ダイアログボックスでヘルプを表示します。 詳細については、ATA 187 のドキュメントを参照してください。

アナログ電話アダプタ 190 設定フィールド

表 *33 :* アナログ電話アダプタ *190* 設定フィールド

フィールド	説明
MACアドレス（MAC Address）	ATA 190 を特定する Media Access Control（MAC）アドレスを入力します。値が 12 桁の 16 進文字列で構成されていることを確認します。 次のいずれかの方法で、ATA 190 の MAC アドレスを判別できます。 • ATA 190 の背面にある MAC ラベルを確認します。 • ATA 190 の ウェブ ページを表示し、[デバイス情報（Device Information）] ハイパーリンクをクリックします。
[説明（Description）]	ATA 190 の説明テキストを入力します。 このフィールドには、128 文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。
[デバイスプール（Device Pool）]	ATA 190 を割り当てるデバイス プールを選択します。デバイス プールでは、複数のデバイスに共通の特性（リージョン、日時グループ、ソフトキー テンプレートなど）のセットを定義します。 デバイス プール構成の設定を確認するには、[詳細の表示（View Details）] リンクをクリックします。
[共通デバイス設定（Common Device Configuration）]	ATA 190 を割り当てる共通デバイス設定を選択します。 [共通デバイス設定（Common Device Configuration）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[電話ボタンテンプレート（Phone Button Template）]	適切な電話ボタンテンプレートを選択します。電話ボタンテンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能（回線、スピード ダイヤルなど）を使用するかを特定します。
[共通の電話プロファイル（Common Phone Profile）]	ドロップダウン リストで、使用可能な共通の電話プロファイルのリストから共通の電話プロファイルを選択します。 [共通の電話プロファイル（Common Phone Profile）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストを使用から、コーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。

フィールド	説明
[AARコーリングサーチスペース（AAR Calling Search Space）]	ドロップダウン リストから、自動代替ルーティング（AAR）を実行したときに使用するデバイスの適切なコーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[メディアリソースグループリスト（Media Resource Group List）]	適切なメディア リソース グループ リストを選択します。メディア リソース グループ リストは、優先順位順に並べられたメディア リソース グループから構成されます。 [<なし>（<None>）] を選択すると、Cisco Unified CM はデバイス プールで定義されたメディア リソース グループ リストを使用します。
[ユーザー保留 MOH 音源（User Hold MOH Audio Source）]	ドロップダウン リストから、ユーザーが保留操作を開始する場合に保留音（MOH）として使用するオーディオ ソースを選択します。
[ロケーション（Location）]	ドロップダウン リストから、デバイス プール内の電話およびゲートウェイと関連付けられている場所を選択します。
[AARグループ（AAR Group）]	このデバイスの自動代替ルーティング（AAR）グループを選択します。AAR グループはプレフィックス番号を設定します。この番号は、帯域幅不足のためにブロックされるコールをルーティングする際に使用されます。AAR グループが指定されていない場合、Cisco Unified CM はデバイス プールまたは回線に関連付けられている AAA グループを使用します。
[ユーザーロケール（User Locale）]	ドロップダウン リストから、CTI ポートに関連付けられたユーザー ロケールを選択します。そのユーザー ロケールは、言語とフォントを含んだ、ユーザーをサポートする一連の詳細情報を識別します。 ユーザー ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたユーザー ロケールを使用します。
[ネットワークロケール（Network Locale）]	ドロップダウン リストから、CTI ポートに関連付けられたネットワーク ロケールを選択します。ネットワーク ロケールには、特定の地理的領域の電話が使用するトーンとパターンの定義が含まれています。 ネットワーク ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたネットワーク ロケールを使用します。

フィールド	説明
[ビルトインブリッジ（Built In Bridge）]	[ビルトインブリッジ（Built In Bridge）] ドロップダウン リストを使用して割り込み機能用の組み込み型会議ブリッジを有効または無効にします。次のいずれかを実行します。 • オン • オフ • デフォルト
[プライバシー（Privacy）]	プライバシーについて、[プライバシー（Privacy）] ドロップダウン リストから [オン（On）] を選択します。
[デバイスモビリティモード（Device Mobility Mode）]	ドロップダウン リストから、このデバイスのデバイス モビリティ機能をオンまたはオフにします。デフォルトのデバイス モビリティ モードを使用する場合は、[デフォルト（Default）] を選択します。デフォルトの設定では、デバイスの [デバイス モビリティ モード（Device Mobility Mode）] サービス パラメータの値が使用されます。
[オーナー（Owner）]	オーナーのタイプとして、[ユーザー（User）] または [名前非表示（パブリック/共有スペース）（Anonymous (Public/Shared Space)）] を選択します。
[オーナーのユーザー ID（Owner User ID）]	ドロップダウン リストから、割り当てられた電話ユーザーのユーザー ID を選択します。ユーザー ID は、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。デバイスにユーザー ID を割り当てると、[ライセンスの使用状況レポート（License Usage Report）] でデバイスが [未割り当てデバイス（Unassigned Devices）] から [ユーザー（Users）] に移動します。 （注） エクステンション モビリティを使用する場合は、このフィールドを設定しないでください。エクステンション モビリティでは、デバイスのオーナーはサポートされていません。
[電話ロード名（Phone Load Name）]	ATA 190 のカスタム ソフトウェアを入力します。

フィールド	説明
[トラステッドリレーポイントを使用（Use Trusted Relay Point）]	次の値のいずれかを選択します。 • [オフ（Off）]：このデバイスで、トラステッド リレー ポイント（TRP）の使用を無効にするには、この値を選択します。この設定は、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[トラステッドリレーポイントを使用（Use Trusted Relay Point）]設定よりも優先されます。 • [オン（On）]：このデバイスでの TRP の使用を有効にする場合は、この値を選択します。この設定は、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[トラステッドリレーポイントを使用（Use Trusted Relay Point）]設定よりも優先されます。 • [デフォルト（Default）]：この値を選択した場合、デバイスはこのデバイスが関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用（Use Trusted Relay Point）]設定を使用します。
常にプライム回線を使用する（Always Use Prime Line）	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。 • [オン（On）]：電話機がアイドル状態（オフ フック）になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールは鳴り続け、電話機ユーザはそれらの他の回線を選択して、これらのコールに応答する必要があります。 • デフォルト：Unified Communications Manager は、[常にプライム回線を使用する（Always Use Prime Line）]サービス パラメータの設定を使用します。これにより、Cisco CallManager サービスがサポートされます。

フィールド	説明
ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態の場合、電話のメッセージ ボタンを押すと、ボイス メッセージが設定されている回線からボイス メッセージ システムに自動的にダイヤルされます。Unified Communications Manager は、常に音声メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザーが [メッセージ（Messages）] ボタンを押すと、プライマリ回線が使用されます。 • [オン（On）]：電話がアイドル状態の場合に電話のメッセージ ボタンを押すと、電話のプライマリ回線がボイス メッセージを受信するアクティブな回線になります。 • デフォルト：Unified Communications Manager は、[ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）] サービス パラメータの設定を使用します。これにより、Cisco CallManager サービスがサポートされます。
[地理位置情報（GeoLocation）]	ドロップダウン リストから地理位置情報を選択します。 [未指定の地理位置情報（Unspecified geolocation）] を選択すると、このデバイスを地理位置情報に関連付けないように指定できます。 さらに、**[システム（System）] > [地理位置情報の設定（Geolocation Configuration）]** メニュー オプションで設定した地理位置情報も選択できます。
[プレゼンテーション インジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）]	コール単位でコール表示制限を設定する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、Unified Communications Manager は内線コールについて受信するすべての表示制限を無視します。 この設定と、トランスレーション パターン レベルでの発信者回線 ID の表示および接続回線 ID の表示の設定を組み合わせて使用します。これらの設定を組み合わせて使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。
[ハントグループにログイン（Logged into Hunt Group）]	ATA 190 をハント リストに追加すると、管理者はこのチェックボックスをオン（またはオフ）にして、ユーザーをログインまたはログアウトさせることができます。 ユーザーは電話のソフトキーを使用して、電話をハント リストにログインまたはログアウトします。

フィールド	説明
[リモートデバイス（Remote Device）]	このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。 ヒント　この機能はリソースを消費するため、シグナリングの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。
[保護されたデバイス（Protected Device）]	電話機を保護されたデバイスとして指定するには、このチェックボックスをオンにします。この場合、電話機が2秒間トーンを再生してユーザーにコールが暗号化されていることを通知できます。また、発信側と着信側の両方の電話機が保護されたデバイスとして設定できます。このトーンは、コールが応答されたとき、発信側と着信側の両者に対して再生されます。このトーンは、発信側と着信側の両方の電話機が保護されていて、なおかつ暗号化メディア上でコールが行われたときでなければ再生されません。 このチェックボックスをオンにすると、再生するセキュア通知トーンの複数の設定要件のうち 1 つのみが表示されます。セキュア通知トーン機能および設定要件の詳細については、『*Cisco Unified Communications Manager* セキュリティ 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。 このチェックボックスがオンで、システムがコールは暗号化されていないと判断すると、電話は非セキュア通知トーンを再生して、コールが保護されていないことをユーザーに通知します。

[番号表示トランスフォーメーション（Number Presentation Transformation）]

表 *34 : [*この電話からのコールの発信者*ID*（*Caller ID For Calls From This Phone*）*]*

フィールド	説明
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーション CSS に、このデバイスに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。
[デバイスプールの発信側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイス プールに設定されている発信側トランスフォーメーション CSS を使用する場合は、このボックスをオンにします。このチェックボックスを選択しない場合、デバイスは [トランク設定（Trunk Configuration）] ウィンドウで設定した発信側変換 CSS を使用します。

表 35 : [リモート番号（Remote Number）]

フィールド	説明
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	ドロップダウン リストから、このデバイスに受信したコールのリモート発信者番号に適用する、発信側トランスフォーメーション パターンを含むコーリング サーチ スペース（CSS）を選択します。
[デバイスプールの発信側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	リモート通話とリモート接続番号の変換に、このデバイスが属するデバイス プールで設定されている発信側トランスフォーメーション CSS を適用するには、このチェックボックスをオンにします。

表 36 : [プロトコル固有情報（Protocol Specific Information）]

フィールド	説明
[パケットキャプチャモード（Packet Capture Mode）]	この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケット キャプチャを実行すると、CPU の使用率が上昇して、コール処理が妨げられる可能性があります。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。 • [なし（None）]：このオプションは、パケット キャプチャが発生しないことを示します（デフォルト設定）。この設定は、パケット キャプチャの完了後に行います。 • [バッチ処理モード（Batch Processing Mode）]：Cisco Unified CM が、復号されたメッセージや暗号化されていないメッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムでは、毎日新しいファイルが新しい暗号キーを使用して作成されます。Cisco Unified CM はファイルを 7 日間保存し、さらにファイルを暗号化するキーを安全な場所に保存します。Cisco Unified CM は、PktCap 仮想ディレクトリにファイルを保存します。1 つのファイルの中に、タイムスタンプ、送信元 IP アドレス、送信元 IP ポート、宛先 IP アドレス、パケットのプロトコル、メッセージの長さ、およびメッセージが保持されます。TAC のデバッグ ツールでは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを保持している暗号化済みファイルを 1 つだけ要求します。同様にこのツールでは、暗号化ファイルを復号化するためのキー情報を要求します。

フィールド	説明
[パケットキャプチャ時間（Packet Capture Duration）]	この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。 このフィールドには、1 つのパケット キャプチャ セッションに割り当てる時間の上限（分単位）を指定します。デフォルト設定は 0 で、範囲は 0 ～ 300 分です。 パケット キャプチャを開始するには、フィールドに 0 以外の値を入力します。パケット キャプチャが完了すると、値 0 が表示されます。
[BLFプレゼンスグループ（BLF Presence Group）]	ドロップダウン リストから、エンドユーザーの話中ランプ フィールド（BLF）プレゼンス グループを選択します。選択したグループは、エンド ユーザーがモニター可能な接続先を指定します。 BLF プレゼンス グループのデフォルト値は [標準のプレゼンスグループ（Standard Presence group）] であり、インストール時に設定されます。Cisco Unified CM Administration で設定されている BLF プレゼンス グループは、ドロップダウン リストにも表示されます。
[SIPダイヤルルール（SIP Dial Rules）]	必要に応じて、適切な SIP ダイヤル ルールを選択します。SIP ダイヤル ルールは、Cisco Unified IP Phone 7940 および 7960 のローカル ダイヤル プランを提供するため、ユーザーは、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。 SIP を実行している IP 電話にダイヤル ルールを適用しない場合は、[SIP ダイヤルルール（SIP Dial Rules）] フィールドを [<なし>（<None>）] に設定したままにします。これは、コールが処理される前に、ユーザーがダイヤル ソフトキーを使用するか、タイマーが切れるまで待つ必要があることを示します。
[MTP優先発信コーデック（MTP Preferred Originating Codec）]	メディア ターミネーション ポイントが SIP のコールに必要な場合は、ドロップダウン リストから使用するコーデックを選択します。
[デバイスのセキュリティプロファイル（Device Security Profile）]	デバイスに適用するセキュリティ プロファイルを選択します。 Unified Communications Manager Administration で設定するすべてのデバイスに、セキュリティ プロファイルを適用する必要があります。

フィールド	説明
[再ルーティング用コーリングサーチスペース（Rerouting Calling Search Space）]	ドロップダウン リストから、再ルーティングに使用するコーリング サーチ スペースを選択します。 リファラーの再ルーティング コーリング サーチ スペースを使用して、参照先へのルートが検索されます。再ルーティング コーリング サーチ スペースが原因で参照が失敗すると、Refer Primitive は 「405 Method Not Allowed」 メッセージによって要求を拒否します。 リダイレクト（3xx）プリミティブおよび転送機能も再ルーティング コーリング サーチ スペースを使用して、リダイレクト先または転送先を検索します。
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされる SUBSCRIBE コーリング サーチ スペースは、エンドユーザから受け取ったプレゼンス要求を Unified Communications Manager がルーティングする方法を決定します。この設定では、エンド ユーザーのプレゼンス（SUBSCRIBE）要求のコール処理サーチ スペースと別にコーリング サーチ スペースを適用できます。 ドロップダウン リストから、エンドユーザーのプレゼンス要求に使用する SUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified Communications Manager Administration で設定するすべてのコーリング サーチ スペースが、[SUBSCRIBE コーリングサーチスペース（SUBSCRIBE Calling Search Space）] ドロップダウン リストに表示されます。 ドロップダウン リストから、エンド ユーザーに別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは [なし（None）] に設定されます。 この目的専用の SUBSCRIBE コーリング サーチ スペースを設定するには、他のコーリング サーチ スペースと同様に新しいコーリング サーチ スペースを設定します。
[SIPプロファイル（SIP Profile）]	デフォルトの SIP プロファイルまたは作成済みの特定のプロファイルを選択します。SIP プロファイルでは、登録タイマーおよびキープアライブ タイマー、メディア ポート、Do Not Disturb（サイレント）制御など、電話機の特定の SIP 情報を提供します。

フィールド	説明
[ダイジェストユーザー（Digest User）]	ダイジェスト認証（SIP セキュリティ）で使用するこの設定の電話機に関連付けるエンド ユーザーを選択します。 選択するユーザーのダイジェスト クレデンシャルが [エンドユーザーの設定（End User Configuration）] ウィンドウで設定されていることを確認してください。 電話設定を保存し、設定の更新内容を電話に適用すると、ユーザーのダイジェスト クレデンシャルが電話の設定ファイルに追加されます。 ダイジェスト認証の詳細については、『*Cisco Unified Communications Manager* セキュリティ 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。
[メディアターミネーションポイントが必須（Media Termination Point Required）]	このフィールドを使用して、ATA 190 でサポートされていない機能（保留や転送など）を実装するために、メディア ターミネーション ポイントを使用するかどうかを指示します。 MTP を使用して機能を実装する場合は、[メディアターミネーションポイントが必須（Media Termination Point Required）] チェックボックスをオンにします。MTP を使用して機能を実装しない場合は、[メディアターミネーションポイントが必須（Media Termination Point Required）] チェックボックスをオフにします。 このチェックボックスは、ATA 190 クライアントおよび H.245 Empty Capabilities Set をサポートしていない ATA 190 デバイスの場合、または単一ソースを通してメディア ストリーミングを終了させる場合にのみ使用します。 このチェックボックスをオンにして、MTP を必須とし、このデバイスをビデオ コールのエンドポイントにすると、コールはオーディオのみになります。
[不在ポート（Unattended Port）]	このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。
[DTMF受信が必要（Require DTMF Reception）]	SIP と SCCP を実行しているデバイスの場合に、この電話の DTMF 受信を必須にするには、このチェックボックスをオンにします。 （注） Cisco Unified Mobility 機能の設定で、SIP トランク（クラスタ間トランク（ICT）またはゲートウェイ）経由で IP 電話のリモート接続先としてクラスタ間 DN を使用する場合、エンタープライズ機能アクセス ミッドコール機能に不可欠な DTMF 番号をアウト オブ バンドで受信できるように、このチェックボックスをオンにします。

表 37 : [認証局プロキシ機能（CAPF）情報（Certification Authority Proxy Function (CAPF) Information）]

フィールド	説明
[証明書の操作（Certificate Operation）]	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [保留中の操作なし（No Pending Operation）]：証明書の操作が行われない場合に表示されます（デフォルトの設定）。 • [インストール/更新（Install/Upgrade）]：電話機に新しい証明書をインストールするか、既存のローカルで有効な証明書をアップグレードします。 • [削除（Delete）]：電話機に存在するローカルで有効な証明書を削除します。 • [トラブルシューティング（Troubleshoot）]：ローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）を取得し、CAPF トレース ファイルで証明書クレデンシャルを表示できます。電話機に両方の証明書タイプが存在する場合、Cisco Unified CM は、証明書のタイプごとに 1 つずつ、2 つのトレース ファイルを作成します。 [トラブルシューティング（Troubleshooting）] オプションを選択して、電話に LSC または MIC が存在することを確認できます。 CAPF 操作の詳細については、『*Cisco Unified Communications Manager* セキュリティ 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。

フィールド	説明
[認証モード（Authentication Mode）]	

フィールド	説明
	このフィールドでは、電話機が CAPF 証明書の操作時に使用する認証方法を選択できます。 ドロップダウン リストから、次のオプションのいずれかを選択します。 • [認証文字列（By Authentication String）]：ユーザーが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 • [Null ストリング（By Null String）]：ユーザーの介入なしで、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 このオプションではセキュリティが確保されません。したがって、セキュアな閉じた環境の場合にだけこのオプションを選択することを強く推奨します。 • [既存の証明書（LSCを優先）（By Existing Certificate (Precedence to LSC)）]：電話機に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）が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に MIC と LSC が存在する場合、LSC によって認証が行われます。電話機に LSC が存在しないが、MIC が存在する場合、MIC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • [既存の証明書（MICを優先）（By Existing Certificate (Precedence to MIC)）]：電話機に LSC または MIC が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に MIC が存在する場合、電話機に LSC が存在するかどうかに関係なく、MIC によって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在すること

フィールド	説明
	を確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 （注） [電話セキュリティプロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
[認証文字列（Authentication String）]	[認証モード（Authentication Mode）] ドロップダウン リストの [認証文字列（By Authentication String）] オプションを選択した場合、このフィールドが適用されます。手動で文字列を入力するか、[文字列の生成（Generate String）] ボタンをクリックして、文字列を生成します。4 桁から 10 桁の文字列になるようにしてください。 ローカルで有効な証明書をインストール、アップグレード、削除、トラブルシューティングするには、電話機ユーザーまたは管理者が電話機に認証文字列を入力する必要があります。
[キー サイズ（ビット）（Key Size (Bits)）]	CAPF で使用されるこの設定では、ドロップダウン リストから証明書のキー サイズを選択します。デフォルト設定は 1024 です。その他のオプションには 512 と 2048 があります。 デフォルトの設定より大きいキー サイズを選択すると、電話機でキーの生成に必要なエントロピーを生成するのに時間がかかります。キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。 （注） [電話セキュリティプロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
[操作の完了期限（Operation Completes by）]	このフィールドは、[インストール/アップグレード（Install/Upgrade）]、[削除（Delete）]、[トラブルシューティング（Troubleshoot）] の証明書の操作オプションをサポートし、操作の完了期限を指定します。 表示される値は、パブリッシャ データベース サーバーに適用されます。
[証明書の操作ステータス（Certificate Operation Status）]	このフィールドには、証明書の操作の進捗状況が表示されます。たとえば、<操作タイプ>保留中、失敗、成功などです。ここで、操作タイプは [インストール/アップグレード（Install/Upgrade）]、[削除（Delete）]、[トラブルシューティング（Troubleshoot）] 証明書の操作オプションのいずれかになります。このフィールドに表示される情報は変更できません。

表 *38* : *[セキュアシェルユーザー（Secure Shell User）]*

フィールド	説明
[セキュアシェルユーザー（Secure Shell User）]	セキュア シェル ユーザーのユーザー ID を入力します。最大 50 文字の英数字または特殊文字を入力できます。無効な文字は、"、%、&、<、>、\ です。このフィールドは、設定している電話デバイスが SSH アクセスをサポートしている場合に表示されます。 Cisco Technical Assistance Center（TAC）では、トラブルシューティングやデバッグを行うときにセキュア シェルを使用します。TAC にお問い合わせください。 Cisco Unified CM が SSH クレデンシャルを平文で電話機に送信しないようにするために、暗号化された電話の設定ファイルを設定する方法については、このリリースの『*Cisco Unified Communications Manager* セキュリティ 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。
[セキュアシェルパスワード（Secure Shell Password）]	セキュア シェル ユーザーのパスワードを入力します。最大 127 文字の英数字や特殊文字を入力できます。無効な文字は、"、%、&、<、>、\ です。TAC にお問い合わせください。 Cisco Unified CM が SSH クレデンシャルを平文で電話機に送信しないようにするために、暗号化された電話の設定ファイルを設定する方法については、このリリースの『*Cisco Unified Communications Manager* セキュリティ 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。

表 *39* : 製品固有の設定

フィールド	説明
デバイス製造元が定義するモデル固有の設定フィールド	製品固有の設定項目のフィールドの説明とヘルプを表示するには、[製品固有の設定（Product Specific Configuration）] エリアで [?]「」情報アイコンをクリックし、ポップアップ ダイアログボックスでヘルプを表示します。 詳細については、ATA 190 のドキュメントを参照してください。

アナログ電話アダプタ 191 設定フィールド

表 *40 :* アナログ電話アダプタ *191* 設定フィールド

フィールド	説明
MACアドレス（MAC Address）	ATA 191 を識別する Media Access Control（MAC）アドレスを入力します。値が 12 桁の 16 進文字列で構成されていることを確認します。 次のいずれかの方法で、ATA 191 の MAC アドレスを判別できます。 • ATA 191 の背面にある MAC ラベルを確認する。 • ATA 191 の ウェブ ページを表示し、[デバイス情報（Device Information）] ハイパーリンクをクリックする。
[説明（Description）]	ATA 191 のテキストの説明を入力します。 このフィールドには、128 文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。
[デバイスプール（Device Pool）]	ATA 191 を割り当てるデバイス プールを選択します。デバイス プールでは、複数のデバイスに共通の特性（リージョン、日時グループ、ソフトキー テンプレートなど）のセットを定義します。 デバイス プール構成の設定を確認するには、[詳細の表示（View Details）] リンクをクリックします。
[共通デバイス設定（Common Device Configuration）]	ATA 191 を割り当てる共通デバイス設定を選択します。 [共通デバイス設定（Common Device Configuration）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[電話ボタンテンプレート（Phone Button Template）]	適切な電話ボタンテンプレートを選択します。電話ボタンテンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能（回線、スピード ダイヤルなど）を使用するかを特定します。
[共通の電話プロファイル（Common Phone Profile）]	ドロップダウン リストで、使用可能な共通の電話プロファイルのリストから共通の電話プロファイルを選択します。 [共通の電話プロファイル（Common Phone Profile）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストを使用から、コーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。

フィールド	説明
[AARコーリングサーチスペース（AAR Calling Search Space）]	ドロップダウン リストから、自動代替ルーティング（AAR）を実行したときに使用するデバイスの適切なコーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[メディアリソースグループリスト（Media Resource Group List）]	適切なメディア リソース グループ リストを選択します。メディア リソース グループ リストは、優先順位順に並べられたメディア リソース グループから構成されます。 [<なし>（<None>）] を選択すると、Cisco Unified CM はデバイス プールで定義されたメディア リソース グループ リストを使用します。
[ユーザー保留 MOH 音源（User Hold MOH Audio Source）]	ドロップダウン リストから、ユーザーが保留操作を開始する場合に保留音（MOH）として使用するオーディオ ソースを選択します。
[ロケーション（Location）]	ドロップダウン リストから、デバイス プール内の電話およびゲートウェイと関連付けられている場所を選択します。
[AARグループ（AAR Group）]	このデバイスの自動代替ルーティング（AAR）グループを選択します。AAR グループはプレフィックス番号を設定します。この番号は、帯域幅不足のためにブロックされるコールをルーティングする際に使用されます。AAR グループが指定されていない場合、Cisco Unified CM はデバイス プールまたは回線に関連付けられている AAA グループを使用します。
[ユーザーロケール（User Locale）]	ドロップダウン リストから、CTI ポートに関連付けられたユーザー ロケールを選択します。そのユーザー ロケールは、言語とフォントを含んだ、ユーザーをサポートする一連の詳細情報を識別します。 ユーザー ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたユーザー ロケールを使用します。
[ネットワークロケール（Network Locale）]	ドロップダウン リストから、CTI ポートに関連付けられたネットワーク ロケールを選択します。ネットワーク ロケールには、特定の地理的領域の電話が使用するトーンとパターンの定義が含まれています。 ネットワーク ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたネットワーク ロケールを使用します。

フィールド	説明
[ビルトインブリッジ（Built In Bridge）]	[ビルトインブリッジ（Built In Bridge）] ドロップダウン リストを使用して割り込み機能用の組み込み型会議ブリッジを有効または無効にします。次のいずれかを実行します。 • オン • オフ • デフォルト
[プライバシー（Privacy）]	プライバシーについて、[プライバシー（Privacy）] ドロップダウン リストから [オン（On）] を選択します。
[デバイスモビリティモード（Device Mobility Mode）]	ドロップダウン リストから、このデバイスのデバイス モビリティ機能をオンまたはオフにします。デフォルトのデバイス モビリティ モードを使用する場合は、[デフォルト（Default）] を選択します。デフォルトの設定では、デバイスの [デバイス モビリティ モード（Device Mobility Mode）] サービス パラメータの値が使用されます。
[オーナー（Owner）]	オーナーのタイプとして、[ユーザー（User）] または [名前非表示（パブリック/共有スペース）（Anonymous (Public/Shared Space)）] を選択します。
[オーナーのユーザー ID（Owner User ID）]	ドロップダウン リストから、割り当てられた電話ユーザーのユーザー ID を選択します。ユーザー ID は、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。デバイスにユーザー ID を割り当てると、[ライセンスの使用状況レポート（License Usage Report）] でデバイスが [未割り当てデバイス（Unassigned Devices）] から [ユーザー（Users）] に移動します。 （注） エクステンション モビリティを使用する場合は、このフィールドを設定しないでください。エクステンション モビリティでは、デバイスのオーナーはサポートされていません。
[電話ロード名（Phone Load Name）]	ATA 191 のカスタム ソフトウェアを入力します。

フィールド	説明
[トラステッドリレーポイントを使用（Use Trusted Relay Point）]	次の値のいずれかを選択します。 • [オフ（Off）]：このデバイスで、トラステッド リレー ポイント（TRP）の使用を無効にするには、この値を選択します。この設定は、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[トラステッドリレーポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • [オン（On）]：このデバイスでの TRP の使用を有効にする場合は、この値を選択します。この設定は、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[トラステッドリレーポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • [デフォルト（Default）]：この値を選択した場合、デバイスはこのデバイスが関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用（Use Trusted Relay Point）] 設定を使用します。
常にプライム回線を使用する（Always Use Prime Line）	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。 • [オン（On）]：電話機がアイドル状態（オフ フック）になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールは鳴り続け、電話機ユーザはそれらの他の回線を選択して、これらのコールに応答する必要があります。 • [デフォルト（Default）]：Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [常にプライム回線を使用する（Always Use Prime Line）] サービス パラメータの設定を使用します。

フィールド	説明
ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態の場合、電話のメッセージ ボタンを押すと、ボイス メッセージが設定されている回線からボイス メッセージ システムに自動的にダイヤルされます。Cisco Unified Communications Manager は常にボイス メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザーが [メッセージ（Messages）] ボタンを押すと、プライマリ回線が使用されます。 • [オン（On）]：電話がアイドル状態の場合に電話のメッセージ ボタンを押すと、電話のプライマリ回線がボイス メッセージを受信するアクティブな回線になります。 • [デフォルト（Default）]：Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）] サービス パラメータの設定を使用します。
[地理位置情報（GeoLocation）]	ドロップダウン リストから地理位置情報を選択します。 [未指定の地理位置情報（Unspecified geolocation）] を選択すると、このデバイスを地理位置情報に関連付けないように指定できます。 さらに、**[システム（System）] > [地理位置情報の設定（Geolocation Configuration）]** メニュー オプションで設定した地理位置情報も選択できます。
[プレゼンテーション インジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）]	コール単位でコール表示制限を設定する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、Cisco Unified Communications Manager は内線コールに対して受信したすべての表示制限を無視します。 この設定と、トランスレーション パターン レベルでの発信者回線 ID の表示および接続回線 ID の表示の設定を組み合わせて使用します。これらの設定を組み合わせて使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。
[ハントグループにログイン（Logged into Hunt Group）]	ATA 191 をハント リストに追加したら、管理者はこのチェックボックスをオン（またはオフ）にすることによって、ユーザをログインまたはログアウトさせることができます。 ユーザーは電話のソフトキーを使用して、電話をハント リストにログインまたはログアウトします。

フィールド	説明
[リモートデバイス（Remote Device）]	このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。 **ヒント** この機能はリソースを消費するため、シグナリングの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。
[保護されたデバイス（Protected Device）]	電話機を保護されたデバイスとして指定するには、このチェックボックスをオンにします。この場合、電話機が2秒間トーンを再生してユーザーにコールが暗号化されていることを通知できます。また、発信側と着信側の両方の電話機が保護されたデバイスとして設定できます。このトーンは、コールが応答されたとき、発信側と着信側の両者に対して再生されます。このトーンは、発信側と着信側の両方の電話機が保護されていて、なおかつ暗号化メディア上でコールが行われたときでなければ再生されません。 このチェックボックスをオンにすると、再生するセキュア通知トーンの複数の設定要件のうち 1 つのみが表示されます。セキュア通知トーン機能および設定要件の詳細については、『*Cisco Unified Communications Manager* セキュリティ 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。 このチェックボックスがオンで、システムがコールは暗号化されていないと判断すると、電話は非セキュア通知トーンを再生して、コールが保護されていないことをユーザーに通知します。

[番号表示トランスフォーメーション（Number Presentation Transformation）]

表 *41 : [*この電話からのコールの発信者*ID*（*Caller ID For Calls From This Phone*）*]*

フィールド	説明
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーション CSS に、このデバイスに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。
[デバイスプールの発信側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイス プールに設定されている発信側トランスフォーメーション CSS を使用する場合は、このボックスをオンにします。このチェックボックスを選択しない場合、デバイスは [トランク設定（Trunk Configuration）] ウィンドウで設定した発信側変換 CSS を使用します。

表 *42 : [*リモート番号（***Remote Number***）*]*

フィールド	説明
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	ドロップダウン リストから、このデバイスに受信したコールのリモート発信者番号に適用する、発信側トランスフォーメーション パターンを含むコーリング サーチ スペース（CSS）を選択します。
[デバイスプールの発信側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	リモート通話とリモート接続番号の変換に、このデバイスが属するデバイス プールで設定されている発信側トランスフォーメーション CSS を適用するには、このチェックボックスをオンにします。

表 *43 : [*プロトコル固有情報（***Protocol Specific Information***）*]*

フィールド	説明
[パケットキャプチャモード（Packet Capture Mode）]	この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。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。 • [なし（None）]：このオプションは、パケット キャプチャが発生しないことを示します（デフォルト設定）。この設定は、パケット キャプチャの完了後に行います。 • [バッチ処理モード（Batch Processing Mode）]：Cisco Unified CM が、復号されたメッセージや暗号化されていないメッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムでは、毎日新しいファイルが新しい暗号キーを使用して作成されます。Cisco Unified CM はファイルを 7 日間保存し、さらにファイルを暗号化するキーを安全な場所に保存します。Cisco Unified CM は、PktCap 仮想ディレクトリにファイルを保存します。1 つのファイルの中に、タイムスタンプ、送信元 IP アドレス、送信元 IP ポート、宛先 IP アドレス、パケットのプロトコル、メッセージの長さ、およびメッセージが保持されます。TAC のデバッグ ツールでは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを保持している暗号化済みファイルを 1 つだけ要求します。同様にこのツールでは、暗号化ファイルを復号化するためのキー情報を要求します。

フィールド	説明
[パケットキャプチャ時間（Packet Capture Duration）]	この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。 このフィールドには、1 つのパケット キャプチャ セッションに割り当てる時間の上限（分単位）を指定します。デフォルト設定は 0 で、範囲は 0 ～ 300 分です。 パケット キャプチャを開始するには、フィールドに 0 以外の値を入力します。パケット キャプチャが完了すると、値 0 が表示されます。
[BLFプレゼンスグループ（BLF Presence Group）]	ドロップダウン リストから、エンドユーザーの話中ランプ フィールド（BLF）プレゼンス グループを選択します。選択したグループは、エンド ユーザーがモニター可能な接続先を指定します。 BLF プレゼンス グループのデフォルト値は [標準のプレゼンスグループ（Standard Presence group）] であり、インストール時に設定されます。Cisco Unified CM Administration で設定されている BLF プレゼンス グループは、ドロップダウン リストにも表示されます。
[SIPダイヤルルール（SIP Dial Rules）]	必要に応じて、適切な SIP ダイヤル ルールを選択します。SIP ダイヤル ルールは、Cisco Unified IP Phone 7940 および 7960 のローカル ダイヤル プランを提供するため、ユーザーは、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。 SIP を実行している IP 電話にダイヤル ルールを適用しない場合は、[SIP ダイヤルルール（SIP Dial Rules）] フィールドを [<なし>（<None>）] に設定したままにします。これは、コールが処理される前に、ユーザーがダイヤル ソフトキーを使用するか、タイマーが切れるまで待つ必要があることを示します。
[MTP優先発信コーデック（MTP Preferred Originating Codec）]	メディア ターミネーション ポイントが SIP のコールに必要な場合は、ドロップダウン リストから使用するコーデックを選択します。
[デバイスのセキュリティプロファイル（Device Security Profile）]	デバイスに適用するセキュリティ プロファイルを選択します。 Unified Communications Manager Administration で設定するすべてのデバイスに、セキュリティ プロファイルを適用する必要があります。

フィールド	説明
[再ルーティング用コーリングサーチスペース（Rerouting Calling Search Space）]	ドロップダウン リストから、再ルーティングに使用するコーリング サーチ スペースを選択します。 リファラーの再ルーティング コーリング サーチ スペースを使用して、参照先へのルートが検索されます。再ルーティング コーリング サーチ スペースが原因で参照が失敗すると、Refer Primitive は 「405 Method Not Allowed」 メッセージによって要求を拒否します。 リダイレクト（3xx）プリミティブおよび転送機能も再ルーティング コーリング サーチ スペースを使用して、リダイレクト先または転送先を検索します。
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされる SUBSCRIBE コーリング サーチ スペースは、エンドユーザから受け取ったプレゼンス要求を Unified Communications Manager がルーティングする方法を決定します。この設定では、エンド ユーザーのプレゼンス（SUBSCRIBE）要求のコール処理サーチ スペースと別にコーリング サーチ スペースを適用できます。 ドロップダウン リストから、エンドユーザーのプレゼンス要求に使用する SUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified Communications Manager Administration で設定するすべてのコーリング サーチ スペースが、[SUBSCRIBE コーリングサーチスペース（SUBSCRIBE Calling Search Space）] ドロップダウン リストに表示されます。 ドロップダウン リストから、エンド ユーザーに別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは [なし（None）] に設定されます。 この目的専用の SUBSCRIBE コーリング サーチ スペースを設定するには、他のコーリング サーチ スペースと同様に新しいコーリング サーチ スペースを設定します。
[SIPプロファイル（SIP Profile）]	デフォルトの SIP プロファイルまたは作成済みの特定のプロファイルを選択します。SIP プロファイルでは、登録タイマーおよびキープアライブ タイマー、メディア ポート、Do Not Disturb（サイレント）制御など、電話機の特定の SIP 情報を提供します。

フィールド	説明
[ダイジェストユーザー（Digest User）]	ダイジェスト認証（SIP セキュリティ）で使用するこの設定の電話機に関連付けるエンド ユーザーを選択します。 選択するユーザーのダイジェスト クレデンシャルが [エンドユーザーの設定（End User Configuration）] ウィンドウで設定されていることを確認してください。 電話設定を保存し、設定の更新内容を電話に適用すると、ユーザーのダイジェスト クレデンシャルが電話の設定ファイルに追加されます。 ダイジェスト認証の詳細については、『*Cisco Unified Communications Manager* セキュリティ 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。
[メディアターミネーションポイントが必須（Media Termination Point Required）]	このフィールドを使用して、ATA 191 がサポートしない機能（保留や転送など）を実装するために、メディア ターミネーション ポイントを使用するかどうかを指示します。 MTP を使用して機能を実装する場合は、[メディアターミネーションポイントが必須（Media Termination Point Required）] チェックボックスをオンにします。MTP を使用して機能を実装しない場合は、[メディアターミネーションポイントが必須（Media Termination Point Required）] チェックボックスをオフにします。 このチェックボックスは、H.245機能セットをサポートしていないATA191クライアントとATA191デバイスに対してのみ使用するか、単一のソースからメディアフローを終了する場合に使用します。 このチェックボックスをオンにして、MTP を必須とし、このデバイスをビデオ コールのエンドポイントにすると、コールはオーディオのみになります。
[不在ポート（Unattended Port）]	このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。
[DTMF受信が必要（Require DTMF Reception）]	SIP と SCCP を実行しているデバイスの場合に、この電話の DTMF 受信を必須にするには、このチェックボックスをオンにします。 （注） Cisco Unified Mobility 機能の設定で、SIP トランク（クラスタ間トランク（ICT）またはゲートウェイ）経由で IP 電話のリモート接続先としてクラスタ間 DN を使用する場合、エンタープライズ機能アクセス ミッドコール機能に不可欠な DTMF 番号をアウト オブ バンドで受信できるように、このチェックボックスをオンにします。

表 *44 : [*認証局プロキシ機能（*CAPF*）情報（*Certification Authority Proxy Function (CAPF) Information*）*]*

フィールド	説明
[証明書の操作（Certificate Operation）]	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [保留中の操作なし（No Pending Operation）]：証明書の操作が行われない場合に表示されます（デフォルトの設定）。 • [インストール/更新（Install/Upgrade）]：電話機に新しい証明書をインストールするか、既存のローカルで有効な証明書をアップグレードします。 • [削除（Delete）]：電話機に存在するローカルで有効な証明書を削除します。 • [トラブルシューティング（Troubleshoot）]：ローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）を取得し、CAPF トレース ファイルで証明書クレデンシャルを表示できます。電話機に両方の証明書タイプが存在する場合、Cisco Unified CM は、証明書のタイプごとに 1 つずつ、2 つのトレース ファイルを作成します。 [トラブルシューティング（Troubleshooting）]オプションを選択して、電話に LSC または MIC が存在することを確認できます。 CAPF 操作の詳細については、『*Cisco Unified Communications Manager* セキュリティ 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。

フィールド	説明
[認証モード（Authentication Mode）]	

フィールド	説明
	このフィールドでは、電話機が CAPF 証明書の操作時に使用する認証方法を選択できます。 ドロップダウン リストから、次のオプションのいずれかを選択します。 • [認証文字列（By Authentication String）]：ユーザーが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 • [Null ストリング（By Null String）]：ユーザーの介入なしで、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 このオプションではセキュリティが確保されません。したがって、セキュアな閉じた環境の場合にだけこのオプションを選択することを強く推奨します。 • [既存の証明書（LSCを優先）（By Existing Certificate (Precedence to LSC)）]：電話機に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）が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に MIC と LSC が存在する場合、LSC によって認証が行われます。電話機に LSC が存在しないが、MIC が存在する場合、MIC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • [既存の証明書（MICを優先）（By Existing Certificate (Precedence to MIC)）]：電話機に LSC または MIC が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に MIC が存在する場合、電話機に LSC が存在するかどうかに関係なく、MIC によって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在すること

フィールド	説明
	を確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 （注） [電話セキュリティプロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
[認証文字列（Authentication String）]	[認証モード（Authentication Mode）] ドロップダウン リストの [認証文字列（By Authentication String）] オプションを選択した場合、このフィールドが適用されます。手動で文字列を入力するか、[文字列の生成（Generate String）] ボタンをクリックして、文字列を生成します。4 桁から 10 桁の文字列になるようにしてください。 ローカルで有効な証明書をインストール、アップグレード、削除、トラブルシューティングするには、電話機ユーザーまたは管理者が電話機に認証文字列を入力する必要があります。
[キー サイズ（ビット）（Key Size (Bits)）]	CAPF で使用されるこの設定では、ドロップダウン リストから証明書のキー サイズを選択します。デフォルト設定は 1024 です。その他のオプションには 512 と 2048 があります。 デフォルトの設定より大きいキー サイズを選択すると、電話機でキーの生成に必要なエントロピーを生成するのに時間がかかります。キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。 （注） [電話セキュリティプロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
[操作の完了期限（Operation Completes by）]	このフィールドは、[インストール/アップグレード（Install/Upgrade）]、[削除（Delete）]、[トラブルシューティング（Troubleshoot）] の証明書の操作オプションをサポートし、操作の完了期限を指定します。 表示される値は、パブリッシャ データベース サーバーに適用されます。
[証明書の操作ステータス（Certificate Operation Status）]	このフィールドには、証明書の操作の進捗状況が表示されます。たとえば、<操作タイプ>保留中、失敗、成功などです。ここで、操作タイプは [インストール/アップグレード（Install/Upgrade）]、[削除（Delete）]、[トラブルシューティング（Troubleshoot）] 証明書の操作オプションのいずれかになります。このフィールドに表示される情報は変更できません。

表 *45 : [*セキュアシェルユーザー（*Secure Shell User*）*]*

フィールド	説明
[セキュアシェルユーザー（Secure Shell User）]	セキュア シェル ユーザーのユーザー ID を入力します。最大 50 文字の英数字または特殊文字を入力できます。無効な文字は、"、%、&、<、>、\ です。このフィールドは、設定している電話デバイスが SSH アクセスをサポートしている場合に表示されます。 Cisco Technical Assistance Center（TAC）では、トラブルシューティングやデバッグを行うときにセキュア シェルを使用します。TAC にお問い合わせください。 Cisco Unified CM が SSH クレデンシャルを平文で電話機に送信しないようにするために、暗号化された電話の設定ファイルを設定する方法については、このリリースの『*Cisco Unified Communications Manager* セキュリティ 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。
[セキュアシェルパスワード（Secure Shell Password）]	セキュア シェル ユーザーのパスワードを入力します。最大 127 文字の英数字や特殊文字を入力できます。無効な文字は、"、%、&、<、>、\ です。TAC にお問い合わせください。 Cisco Unified CM が SSH クレデンシャルを平文で電話機に送信しないようにするために、暗号化された電話の設定ファイルを設定する方法については、このリリースの『*Cisco Unified Communications Manager* セキュリティ 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。

表 *46 :* 製品固有の設定

フィールド	説明
デバイス製造元が定義するモデル固有の設定フィールド	製品固有の設定項目のフィールドの説明とヘルプを表示するには、[製品固有の設定（Product Specific Configuration）] エリアで [?]「」情報アイコンをクリックし、ポップアップ ダイアログボックスでヘルプを表示します。 詳細については、ATA 191 のドキュメントを参照してください。

第 42 章

ソフトウェアベースのエンドポイントの設定

ソフトウェアベースのエンドポイントの設定

この章のタスクを完了すると、CTI ポート、H、323 クライアント、Cisco IP Communicator などのソフトウェアベースのエンドポイントを設定することができます。

CTI ポートの設定

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。**[電話の検索と一覧表示（Find and List Phones）]** ウィンドウが表示されます。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウン リストから [CTI ポート（CTI Port）] を選択して、[次へ（Next）] をクリックします。
[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 [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、「関連項目」の項を参照してください。

ステップ 5 [保存（Save）] をクリックします。

CTI ポート設定

表 *47 : CTI* ポート設定

フィールド	説明
[デバイス名（Device Name）]	所有者ユーザーIDに基づいて自動的に入力される CTI ポートの名前を指定します。 デバイス名の形式は、デフォルトで *CTIRD<OwnerUserID>* です。 このフィールドは編集できます。デバイス名には最大15文字を含めることができます。使用できる文字は、英字、数字、ダッシュ（-）、ピリオド、スペース、およびアンダースコアです。
[説明（Description）]	CTI ポートの説明文を入力します。 このフィールドには、128文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。
[デバイスプール（Device Pool）]	CTI ポートを割り当てるデバイス プールを選択します。デバイス プールでは、複数のデバイスに共通の特性（リージョン、日時グループ、ソフトキー テンプレートなど）のセットを定義します。 デバイス プール構成の設定を確認するには、[詳細の表示（View Details）] リンクをクリックします。
[共通デバイス設定（Common Device Configuration）]	CTI ポートを割り当てる共通デバイス設定を選択します。 [共通デバイス設定（Common Device Configuration）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。

フィールド	説明
[共通の電話プロファイル（Common Phone Profile）]	ドロップダウン リスト ボックスで、使用可能な共通の電話プロファイルのリストから共通の電話プロファイルを選択します。 [共通の電話プロファイル（Common Phone Profile）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストを使用から、コーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[AARコーリングサーチスペース（AAR Calling Search Space）]	ドロップダウンリストから、自動代替ルーティング（AAR）を実行したときに使用するデバイスの適切なコーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[メディアリソースグループリスト（Media Resource Group List）]	適切なメディア リソース グループ リストを選択します。メディア リソース グループ リストは、優先順位順に並べられたメディア リソース グループから構成されます。 [<なし>（<None>）] を選択すると、Cisco Unified CM はデバイス プールで定義されたメディア リソース グループ リストを使用します。
[ユーザー保留 MOH 音源（User Hold MOH Audio Source）]	ドロップダウン リストから、ユーザーが保留操作を開始する場合に保留音（MOH）として使用するオーディオ ソースを選択します。
[ネットワーク保留MOH音源（Network Hold MOH Audio Source）]	ドロップダウン リストから、ネットワークが保留操作を開始したときの MOH に使用するオーディオ ソースを選択します。
[ロケーション（Location）]	ドロップダウン リストから、デバイス プール内の電話およびゲートウェイと関連付けられている場所を選択します。

フィールド	説明
[AARグループ（AAR Group）]	このデバイスの自動代替ルーティング（AAR）グループを選択します。AAR グループはプレフィックス番号を設定します。この番号は、帯域幅不足のためにブロックされるコールをルーティングする際に使用されます。AAR グループが指定されていない場合、Cisco Unified CM はデバイス プールまたは回線に関連付けられている AAA グループを使用します。
[ユーザーロケール（User Locale）]	ドロップダウン リスト ボックスから、CTI ポートに関連付けるユーザー ロケールを選択します。そのユーザーロケールは、言語とフォントを含んだ、ユーザーをサポートする一連の詳細情報を識別します。 ユーザー ロケールが指定されなかった場合、Cisco Unified CM はデバイス プールに関連付けられたユーザー ロケールを使用します。
[ネットワークロケール（Network Locale）]	ドロップダウン リスト ボックスから、CTI ポートに関連付けるネットワーク ロケールを選択します。ネットワーク ロケールには、特定の地理的領域の電話が使用するトーンと音の周期の定義が含まれます。 ネットワーク ロケールが指定されなかった場合、Cisco Unified CM はデバイス プールに関連付けられたユーザーロケールを使用します。
[プライバシー（Privacy）]	プライバシーについては、[プライバシー（Privacy）] ドロップダウン リスト ボックスで [オン（On）] を選択します。
[オーナー（Owner）]	オーナー タイプには、[ユーザー（User）] または [匿名（Anonymous）]（パブリック/共有スペース）を選択します。
[オーナーのユーザーID（Owner User ID）]	ドロップダウン リストから、割り当てられた CTI ポート ユーザーのユーザー ID を選択します。ユーザー ID は、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。デバイスにユーザー ID を割り当てると、[ライセンスの使用状況レポート（License Usage Report）] でデバイスが [未割り当てデバイス（Unassigned Devices）] から [ユーザー（Users）] に移動します。

フィールド	説明
[複数ライン同時通話（Join Across Lines）]	ドロップダウン リスト ボックスから、このデバイスの [回線をまたいで参加（Join Across Lines）] 機能を有効または無効にするか、あるいは[デフォルト（Default）] を選択してサービス パラメータ設定を使用します。
[トラステッドリレーポイントを使用（Use Trusted Relay Point）]	次の値のいずれかを選択します。 • [オフ（Off）]：このデバイスで、トラステッド リレー ポイント（TRP）の使用を無効にするには、この値を選択します。この設定は、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[トラステッドリレーポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • [オン（On）]：このデバイスで TRP の使用を有効にする場合は、この値を選択します。この設定は、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[トラステッドリレーポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • [デフォルト（Default）]：この値を選択した場合、このデバイスが関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用（Use Trusted Relay Point）] 設定を使用します。

フィールド	説明
常にプライム回線を使用する（Always Use Prime Line）	ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。 • [オフ（Off）]：電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。 • [オン（On）]：電話機がアイドル状態（オフ フック）になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールは鳴り続け、電話機ユーザはそれらの他の回線を選択して、これらのコールに応答する必要があります。 • [デフォルト（Default）]：Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [常にプライム回線を使用する（Always Use Prime Line）] サービス パラメータの設定を使用します。

フィールド	説明
ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）	ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。 • [オフ（Off）]：電話がアイドル状態の場合、電話のメッセージ ボタンを押すと、ボイス メッセージが設定されている回線からボイス メッセージ システムに自動的にダイヤルされます。Cisco Unified Communications Manager は常にボイス メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザーが [メッセージ（Messages）] ボタンを押すと、プライマリ回線が使用されます。 • [オン（On）]：電話がアイドル状態の場合に電話のメッセージ ボタンを押すと、電話のプライマリ回線がボイス メッセージを受信するアクティブな回線になります。 • [デフォルト（Default）]：Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）] サービス パラメータの設定を使用します。
[地理位置情報（GeoLocation）]	ドロップダウン リスト ボックスから、地理位置情報を選択します。 [未指定の地理位置情報（Unspecified geolocation）] を選択すると、このデバイスを地理位置情報に関連付けないように指定できます。 さらに、**[システム（System）] > [地理位置情報の設定（Geolocation Configuration）]** メニュー オプションで設定した地理位置情報も選択できます。

フィールド	説明
[プレゼンテーションインジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）]	コール単位でコール表示制限を設定する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、Cisco Unified Communications Manager は内線コールに対して受信したすべての表示制限を無視します。 この設定と、トランスレーション パターン レベルでの発信者回線 ID の表示および接続回線 ID の表示の設定を組み合わせて使用します。これらの設定を組み合わせて使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。
[ハントグループにログイン（Logged into Hunt Group）]	CTI ポートをハント リストに追加したら、管理者はこのチェックボックスをオン（またはオフ）にすることによって、ユーザーをログインまたはログアウトさせることができます。 ユーザーは電話のソフトキーを使用して、電話をハント リストにログインまたはログアウトします。
[リモートデバイス（Remote Device）]	このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。 **ヒント** この機能はリソースを消費するため、シグナリングの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。

[番号表示トランスフォーメーション（Number Presentation Transformation）]

表 48 : [この電話からのコールの発信者ID（Caller ID For Calls From This Phone）]

フィールド	説明
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーション CSS に、このデバイスに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。

フィールド	説明
[デバイスプールの発信側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイスプールに設定されている発信側トランスフォーメーション CSS を使用する場合は、このボックスをオンにします。このチェックボックスを選択しない場合、デバイスは[トランク設定（Trunk Configuration）] ウィンドウで設定した発信側変換 CSS を使用します。

表 *49 : [リモート番号（Remote Number）]*

フィールド	説明
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	ドロップダウン リスト ボックスから、このデバイスで受信したコールのリモート着信者番号に適用する、発信側変換パターンを含むコーリング サーチ スペース（CSS）を選択します。
[デバイスプールの発信側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	リモート通話とリモート接続番号の変換に、このデバイスが属するデバイス プールで設定されている発信側トランスフォーメーション CSS を適用するには、このチェックボックスをオンにします。

表 *50 : [プロトコル固有情報（Protocol Specific Information）]*

フィールド	説明
[BLFプレゼンスグループ（BLF Presence Group）]	ドロップダウン リスト ボックスから、エンドユーザーのビジー ランプ フィールド（BLF）プレゼンス グループを選択します。選択したグループは、エンド ユーザーがモニター可能な接続先を指定します。 BLF プレゼンス グループのデフォルト値は [標準のプレゼンスグループ（Standard Presence group）] であり、インストール時に設定されます。Cisco Unified 管理ページで設定される BLF プレゼンス グループは、ドロップダウン リスト ボックスにも表示されます。

フィールド	説明
[デバイスのセキュリティプロファイル（Device Security Profile）]	デバイスに適用するセキュリティ プロファイルを選択します。 Cisco Unified Communications Manager の管理ページで設定されるすべてのデバイスにセキュリティ プロファイルを適用する必要があります。
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされる SUBSCRIBE コーリング サーチ スペースは、Cisco Unified Communications Manager がエンドユーザーから発信されたプレゼンス要求をルーティングする方法を決定します。この設定では、エンド ユーザーのプレゼンス（SUBSCRIBE）要求のコール処理サーチ スペースと別にコーリング サーチ スペースを適用できます。 ドロップダウン リストから、エンドユーザーのプレゼンス要求に使用する SUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified Communications Manager Administration で設定するすべてのコーリング サーチ スペースが、[SUBSCRIBE コーリングサーチスペース（SUBSCRIBE Calling Search Space）] ドロップダウン リストに表示されます。 ドロップダウン リストから、エンドユーザーに別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは [なし（None）] に設定されます。 この目的専用の SUBSCRIBE コーリング サーチ スペースを設定するには、他のコーリング サーチ スペースと同様に新しいコーリング サーチ スペースを設定します。
[不在ポート（Unattended Port）]	このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。

表 *51 : [MLPP* および機密アクセス レベル情報（*MLPP and Confidential Access Level Information*）*]*

フィールド	説明
[MLPPドメイン（MLPP Domain）]	ドロップダウン リストから、このデバイスに関連付ける Multilevel Precedence and Preemption（MLPP）ドメインを選択します。このフィールドが空欄にすると、デバイスの MLPP ドメインはデバイス プールに対して設定された値から継承されます。デバイス プールに [MLPP ドメイン（MLPP Domain）] の設定がない場合、このデバイスの MLPP ドメインは [MLPP ドメイン ID（MLPP Domain Identifier）] エンタープライズ パラメータの設定値から継承されます。 MLPP ドメインのデフォルト値では [なし（None）] が指定されています。
[機密アクセス モード（Confidential Access Mode）]	ドロップダウン リスト ボックスから、機密アクセス レベル モードとして次のいずれかのオプションを選択します。 • [固定（Fixed）] : 機密アクセス レベル値はコールの完了よりも優先されます。 • [可変（Variable）] : コールの完了に CAL のレベルより高い優先順位が設定されます。
[機密アクセスレベル（Confidential Access Level）]	ドロップダウン リスト ボックスから、適切な [機密アクセス レベル（Confidential Access Level）] 値を選択します。

表 *52 :* サイレント情報

フィールド	説明
[サイレント（Do Not Disturb）]	リモート デバイスのサイレント機能を有効にするには、このチェックボックスをオンにします。

フィールド	説明
[DNDオプション（DND Option）]	DND を有効にした場合、[コール拒否（Call Reject）]オプションは、着信コール情報をユーザーに提示しないように指定します。[DND着信コール警告（DND Incoming Call Alert）] パラメータの設定に応じて、デバイスはビープを再生するか、コールの点滅通知を表示します。
[DND着信コール警告（DND Incoming Call Alert）]	DND の [呼出音オフ（Ringer Off）] オプションまたは [コール拒否（Call Reject）] オプションを有効にした場合、このパラメータはデバイスでコールを表示する方法を指定します。 ドロップダウン リストから、次のオプションのいずれかを選択します。 • [なし（None）]：このオプションは、[共通の電話プロファイル（Common Phone Profile）] ウィンドウの [DND 着信コール警告（DND Incoming Call Alert）] 設定をこのデバイスで使用するように指定します。 • [無効（Disable）]：このオプションは、コールを通知するビープ音とフラッシュの両方を無効にしますが、DND の [呼出音オフ（Ringer Off）] オプションの場合、着信コール情報が表示されます。[DND コール拒否（DND Call Reject）] オプションの場合、コール アラートが表示されず、デバイスに情報が送信されません。 • [ビープ音のみ（Beep Only）]：着信コールの場合、このオプションによって、デバイスでビープ音のみが再生されます。 • [フラッシュのみ（Flash Only）]：このオプションを選択した場合、着信コールがあると、デバイスのフラッシュ アラートだけが表示されます。

H.323 クライアントの設定

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [電話（Phone）]** を選択します。**[電話の検索と一覧表示（Find and List Phones）]** ウィンドウが表示されます。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウンリストから [H.323 Client] を選択して、[次へ（Next）] をクリックします。
[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 [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、「関連項目」の項を参照してください。

ステップ 5 [保存（Save）] をクリックします。

H.323 クライアントの設定

Cisco IP Communicator の設定

Cisco IP Communicator は、ソフトウェア ベースのアプリケーションです。ユーザがパーソナル コンピュータを電話機として使用し、電話のコールが受信できるようにします。フル装備の Cisco Unified IP Phone と同じ機能を利用できます。Cisco IP Communicator は、Cisco Unified Communication Manager のコール処理システムを利用して、テレフォニー機能と Voice-over-IP 機能を提供します。Cisco Unified CM Administration の [電話の設定（Phone Configuration）] ウィンドウで、電話デバイスとして Cisco IP Communicator を設定します。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [電話（Phone）]** を選択します。**[電話の検索と一覧表示（Find and List Phones）]** ウィンドウが表示されます。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウン リストから、[Cisco IP Communicator] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [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、[SCCP] または [SIP] を選択して、[次へ（Next）] をクリックします。
[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 5 [電話の設定（Phone Configuration）] ウィンドウで次の必須フィールドを設定します。

- [デバイス名（Device Name）]：Cisco IP Communicator のデバイスを識別する名前を入力します。
- [デバイス プール（Device Pool）]：この電話機を割り当てるデバイス プールを選択します。デバイス プールでは、複数のデバイスに共通の特性（リージョン、日時グループ、ソフトキー テンプレートなど）のセットを定義します。
- [電話ボタン テンプレート（Phone Button Template）]：該当する電話ボタン テンプレートを選択します。電話ボタンテンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能（回線、短縮ダイヤルなど）を使用するかを特定します。
- [オーナーのユーザ ID（Owner User ID）]：ドロップダウン リストボックスから、割り当てられた電話ユーザのユーザ ID を選択します。
- [デバイスのセキュリティ プロファイル（Device Security Profile）]：デバイスに適用するセキュリティ プロファイルを選択します。

残りのフィールドにデフォルト設定を使用できます。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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [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。

ステップ 8 [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。

ステップ 9 [保存（Save）] をクリックします。

第 43 章

Cisco IP Phone の設定

Cisco IP 電話の概要

Cisco IP 電話は機能が充実した電話機であり、IP ネットワークを介して音声通信を提供します。この機能を提供するために、IP 電話は、Unified Communications Manager、DNS と DHCP サーバ、TFTP サーバ、メディア リソース、Cisco Power over Ethernet（PoE）など、他の重要な Cisco Unified IP テレフォニーおよびネットワーク コンポーネントとやり取りします。これらの IP 電話は、デジタル ビジネス電話と同様に機能し、コールの発信や着信のほか、ミュート、保留、転送、短縮ダイヤル、コール転送などの機能も利用できます。また、Cisco IP 電話はデータ ネットワークに接続されているため、ネットワーク情報やサービスへのアクセス、カスタマイズ可能な機能やサービスなど、IP 電話機能が強化されています。ファイル認証、デバイス認証、シグナリングの暗号化、メディアの暗号化などのセキュリティ機能もサポートします。

この章では、電話機を設定してシステムで使用できるようにする方法について説明します。コール パーク、コール転送、話中ランプ フィールド（BLF）、コール ピックアップ、短縮ダイヤルなどの機能を設定するには、『*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。

Cisco IP 電話の設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	電話機の設定 （435 ページ）	SIP または SCCP の電話機を設定するには、このタスクを実行します。

	コマンドまたはアクション	目的
ステップ 2	EnergyWise の設定 （441 ページ）	電力消費量を減らすには、電話機を電源切断 (スリープ) および電源投入 (スリープ解除) 用に自動的に設定します。
ステップ 3	クライアント サービス フレームワーク デバイスの設定 （443 ページ）	次の手順を実行して、クライアントサービスフレームワークデバイスを設定します。Cisco Unified Client Services Framework デバイスは、次のいずれかになります。 • Cisco Unified Communications Integration for Microsoft Office Communicator • Cisco Unified Communications Integration for Webex Connect • Cisco Unified Personal Communicator （Release 8.0 以降）
ステップ 4	CTI リモート デバイスの設定 （446 ページ）	次の手順を実行して、CTI リモートデバイスを設定します。CTI リモート デバイスは、ユーザが Cisco UC アプリケーションと一緒に使用できるオフクラスタ電話を代表するデバイス タイプです。デバイス タイプには、1 つ以上の回線 （ディレクトリ番号） と 1 つ以上のリモート接続先が設定されます。
ステップ 5	Cisco Spark リモート デバイスの設定 （453 ページ）	次の手順を実行して、Cisco Webex リモートデバイスを設定します。Cisco Webex リモートデバイスは、ユーザーが Cisco UC アプリケーションで使用できる Cisco Webex クライアントを表します。このデバイス タイプでは、設定されたリモート接続先に対して、複数のアクティブ コールを行うことができます。 Cisco Spark リモートデバイスには、次の場合を除き、強化されたライセンスが必要です。 • Cisco Spark リモート デバイスのオーナーのユーザ ID に IP 電話 または Jabber クライアントを割り当てる際、1 つの Enhanced ライセン

	コマンドまたはアクション	目的
		スが両方のデバイスで使用されている。 • Cisco Spark リモート デバイスのオーナーのユーザ ID に、TelePresence デバイスも割り当てる際、1 つの TelePresence ライセンスが両方のデバイスで使用されている。 **注意** Cisco Spark リモート デバイスは、シスコのクラウド サービスにオンプレミス環境を接続する場合にのみ使用できます。その他の目的で、このリモート デバイスを使用することはできません。
ステップ 6	電話データの移行 （459 ページ）	別の電話に移行し、古い電話を使用する必要がなくなった場合は、次の手順を実行します。

電話機の設定

手順

	コマンドまたはアクション	目的
ステップ 1	SIP 電話を設定するには、次の手順を実行します。 • SIP 電話のセキュア ポートの設定 （436 ページ） • サービスの再起動 （437 ページ） • SIP プロファイルの設定 （437 ページ） • 電話機のセキュリティ プロファイルの設定 （480 ページ） • 電話の設定 （439 ページ） • Cisco IP 電話サービスの設置 （440 ページ） • VPNクライアントの設定。	Session Initiation Protocol（SIP）を使用する電話機がある場合、この手順を実行します。SIPは、電話と他のネットワークコンポーネント間の主要なインタフェースを提供します。SIPに加えて、IPアドレスの割り当てに使用するDHCP、ドメイン名の解決に使用するDNS、イメージと構成データをダウンロードするTFTPなど、さまざまな機能に使用されています。 VPN クライアントの設定に関する詳細な手順については、『*Cisco Unified Communications Manager* 機能設定ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/

	コマンドまたはアクション	目的
		unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）を参照してください。
ステップ 2	SCCP電話を設置するには、次の手順に従います。 • 電話機のセキュリティ プロファイルの設定 （480 ページ） • 電話の設定 （439 ページ） • Cisco IP 電話サービスの設置 （440 ページ） • VPNクライアントの設定。	Skinny Client 制御プロトコル (SCCP) を使用している Cisco IP Phone を設定する場合は、次の手順を実行します。SCCP は、IP デバイスと Cisco Unified Communication Manager 間で、シスコ独自のメッセージを使用して通信します。複数プロトコル環境でも SCCP は簡単に共存できます。登録時、Cisco Unified IP Phone は Cisco Unified Communication Manager から回線などの設定すべてを受信します。 VPN クライアントの設定に関する詳細な手順については、『*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。

次のタスク

電源の供給、ネットワーク接続の検証、Cisco Unified IP Phone のネットワーク設定を実行します。ネットワーク設定の詳細は、ご使用の Cisco Unified IP Phone のモデルの『*Cisco Unified IP Phone* アドミニストレーション ガイド』を参照してください。

SIP 電話のセキュア ポートの設定

ポートを設定するには、次の手順に従います。Cisco Unified Communications Manager はこのポートを使用して SIP 回線の登録用の SIP 電話を TLS を介してリッスンします。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [Cisco Unified CM（Cisco Unified CM）]** を選択します。

ステップ 2 [このサーバのCisco Unified Communications Manager TCPポート設定（Cisco Unified Communications Manager TCP Port Settings for this Server）] で、[SIP電話セキュアポート（SIP Phone Secure Port）] フィールドにポート番号を指定するか、またはデフォルト値をそのまま使用します。デフォルト値は5061です。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 [OK] をクリックします。

サービスの再起動

Cisco CallManager サービスと Cisco CTL Provider サービスを再起動するには、次の手順を実行します。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 5 手順 3 と手順 4 を繰り返して、Cisco CTL Provider サービスを再起動します。

SIP プロファイルの設定

AS-SIP エンドポイント と SIP トランクの SIP プロファイルを、SIP 設定を使用して設定するには、次の手順を使用します。

始める前に

- SIP 電話のセキュア ポートの設定 （436 ページ）
- サービスの再起動 （437 ページ）

手順

ステップ 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。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 プロファイルをコピーする場合は、[コピー（Copy）] 列のファイル アイコンをクリックします。

ステップ 4 新しいプロファイルの名前と説明を入力します。

ステップ 5 IPv6 スタックが構成されていて、2 つのスタックを展開する場合は、[ANATを有効化（Enable ANAT）] チェックボックスをオンにします。

（注） この設定は、Unity Connection を展開しているかどうかに適用されます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

電話機のセキュリティ プロファイルの設定 （480 ページ）

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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 4 プロトコルを選択します。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 10 [保存（Save）] をクリックします。

電話の設定

Cisco Unified Communications Manager データベースに電話を手動で追加するには、次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、Cisco Unified Communications Manager が自動的に電話を追加し、電話番号を割り当てます。自動登録の有効化の詳細については、「自動登録の設定タスク フロー （680 ページ）」を参照してください。

始める前に

- 電話用 NTP リファレンスの設定 （58 ページ）
- 電話機のセキュリティ プロファイルの設定 （480 ページ）
- 日時グループの追加 （59 ページ）
- SIP ダイヤル ルールの設定 （209 ページ） （SIP 電話を設定する場合）

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 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**

ステップ 6 [次へ（Next）] をクリックします。

ステップ 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。

ステップ 8 [保存（Save）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

SIP または SCCP 電話の場合：

Cisco IP 電話サービスの設置 （440 ページ）

Cisco IP 電話サービスの設置

企業のディレクトリ、ビジュアルボイスメール、天気予報などの電話サービスを Cisco IP Phone に提供する場合は、Cisco IP Phone 用のサービスを設定します。Cisco Unified Communications Manager とともに自動でインストールされるデフォルトの IP 電話サービスを利用できます。サイト用にカスタムの Cisco IP 電話サービスを作成することもできます。Unified Communications Manager でカスタマイズされたサービスを設定するには、次の手順を実行します。

始める前に

電話の設定 （439 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[デバイス（Device）]**>**[デバイスの設定（Device Settings）]**>**[電話サービス（Phone Services）]** を選択します。

ステップ 2 **[新規追加]** をクリックします。

ステップ 3 [IP 電話サービスの設定（IP Phone Services 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。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- エンタープライズサブスクリプションとしてサービスが分類されていない場合は、データベースで電話にサービスを追加します。Bulk Administrative Tool（BAT）またはCisco Unified Communications セルフ ケア ポータルを使用して電話にサービスを追加できます。詳細については、『*Cisco Unified Communications Manager* 一括管理ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）および『*Cisco Unified Communications* セルフ ケア ポータル ユーザ ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-user-guide-list.html）を参照してください。
- 電話ボタンにサービスを割り当てることができます（電話モデルがこれらのボタンをサポートする場合）。サービスの割り当ての詳細については、ご使用の電話モデルの『Cisco IP 電話ユーザ ガイド』を参照してください。
- VPN クライアントを設定します（任意）。

EnergyWise の設定

始める前に

- システムに EnergyWise コントローラが含まれることを確認します。たとえば、Cisco 製スイッチは有効な EnergyWise 機能を備えています。
- 使用している電話機モデルが EnergyWise 機能をサポートするかどうかを確認するには、電話機モデルのユーザ マニュアルを参照してください。

手順

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

ステップ 2 検索条件を指定して、[検索（Find）] をクリックします。
Cisco Unified Communications Manager で設定されている電話機の一覧が表示されます。

ステップ 3 EnergyWise 機能を設定する電話を選択します。

ステップ 4 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションの EnergyWise 関連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」の項を参照してください。

ステップ 5 [保存（Save）] をクリックします。

EnergyWise の設定フィールド

表 *53 : EnergyWise* の設定フィールド

フィールド	説明
[Power Save Plus の有効化（Enable Power Save Plus）]	電話機の電源を自動的にオフにする曜日を選択します。Ctrlキーを押しながら複数の日数を選択し、スケジュールされた日数をクリックすることができます。 デフォルトでは、どの日も選択されていません。
[電話機をオンにする時刻（Phone On Time）]	このフィールドには、時刻を24時間形式で入力します（00:00は午前0時）。**Power Save Plusの有効化**フィールドで選択した日について、電話機の電源を自動的にオンにする時刻を決定します。 （注） 電話機を**ウェイク時間**の前に復帰させるには、電話機の電源をスイッチからオンにする必要があります。詳細については、スイッチのマニュアルを参照してください。
[電話機をオフにする時刻（Phone Off Time）]	このフィールドには、時刻を24時間形式で入力します（00:00は午前0時）。**Power Save Plusの有効化**フィールドで選択した日について、電話機の電源を自動的にオンにする時刻を決定します。**電話機をオンにする時刻**フィールドと**電話機をオフにする時刻**フィールドに同じ値が含まれている場合、電話機はオフになりません。
[電話機をオフにするアイドル タイムアウト（Phone Off Idle Timeout）]	電話機の電源を切るまでの、アイドル状態である必要のある期間を指定します。20分から1440分の任意の値を指定できます。デフォルト値は60分です。
[音声アラートを有効にする（Enable Audio Alert）]	このチェックボックスをオンにして、電話が**電話を切る時間**フィールドで指定した時間より10分前、7分前、4分後、30秒前に音声アラームを再生するように指示します。このチェックボックスは、**Power Save Plus の有効化**リストボックスが1日以上選択されている場合にのみ使用できます。

フィールド	説明
[EnergyWise ドメイン（EnergyWise Domain）]	電話機がある EnergyWise ドメインを指定します。許容される最大長は 127 文字です。
[EnergyWise シークレット（EnergyWise secret）]	EnergyWiseドメイン内のエンドポイントとの通信に使用するセキュリティ秘密パスワードを指定します。許容最大長は 127 文字です。
[EnergyWise オーバーライドを許可（Allow EnergyWise Overrides）]	Power Save Plus を無効にするには、このチェックボックスをオンにします。このチェックボックスをオンにすると、EnergyWise ドメイン コントローラ ポリシーによって、[電源をオンにする時刻（Power On Time）] および [電源をオフにする時刻（Power Off Time）] の値がオーバーライドされます。 （注） [Power Save Plusの有効化（Enable Power Save Plus）] フィールドで、日数を選択しないまま [EnergyWiseオーバーライドを許可（Allow EnergyWise Overrides）] チェックボックスをオンのままにしておくと、Power Save Plus は無効になりません。

クライアント サービス フレームワーク デバイスの設定

次の手順を実行して、クライアントサービスフレームワークデバイスを設定します。Cisco Unified Client Services Framework デバイスは、次のいずれかになります。

- Cisco Unified Communications Integration for Microsoft Office Communicator
- Cisco Unified Communications Integration for Webex Connect
- Cisco Unified Personal Communicator（Release 8.0 以降）

手順

	コマンドまたはアクション	目的
ステップ 1	クライアント サービス フレームワーク デバイスの追加 （444 ページ）	クライアントサービスフレームワークを使用するデバイスを追加します。
ステップ 2	エンド ユーザとデバイスの関連付け（445 ページ）	エンドユーザーアカウントをクライアントサービスフレームワークに関連付けます。

クライアント サービス フレームワーク デバイスの追加

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウン リストから、[Cisco Unified Client Services Framework] を選択します。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [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、「関連項目」の項を参照してください。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [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。

ステップ 8 [ディレクトリ番号（Directory Number）] フィールドに、クライアント サービス フレームワーク デバイスに関連付ける電話番号を入力します。

ステップ 9 [保存（Save）] をクリックします。

クライアント サービス フレームワーク デバイスの設定フィールド

表 *54 :* クライアント サービス フレームワーク デバイスの設定フィールド

フィールド	説明
[デバイス名（Device Name）]	クライアント サービス フレームワーク デバイスを識別する名前を入力します。この名前には、最長 15 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。 （注） Cisco Unified Personal Communicator のデバイス名を設定する場合は、名前が UPC で始まっていることを確認します。
[説明（Description）]	デバイスの簡単な説明を入力します。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。

フィールド	説明
[デバイスプール（Device Pool）]	このデバイスを割り当てるデバイスプールを選択します。
[電話ボタンテンプレート（Phone Button Template）]	[標準クライアントサービスフレームワーク（Standard Client Services Framework）] を選択します。
[オーナーのユーザID（Owner User ID）]	割り当てられたクライアント サービス フレームワーク デバイスのユーザのユーザ ID を選択します。ユーザ ID は、呼詳細レコード（CDR）で、このデバイスから発信されるすべてのコールに対して記録されます。
[デバイスのセキュリティプロファイル（Device Security Profile）]	[Cisco Unified Client Services Framework：標準非セキュアプロファイル（Cisco Unified Client Services Framework - Standard SIP Non-secure Profile）] を選択します。
[SIPプロファイル（SIP Profile）]	[標準SIPプロファイル（Standard SIP Profile）] を選択します。

エンド ユーザとデバイスの関連付け

クライアント サービス フレームワーク デバイスにエンド ユーザを関連付けるには、この手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）]** > **[エンドユーザ（End User）]** を選択します。

ステップ 2 [検索（Find）] をクリックして、デバイスに関連付けるユーザを選択します。

ステップ 3 [デバイス情報（Device Information）] セクションで、[デバイスの関連付け（Device Association）] を選択します。
[ユーザデバイス割り当て（User Device Association）] ウィンドウが表示されます。

ステップ 4 [検索（Find）] をクリックすると、使用可能なデバイスのリストが表示されます。

ステップ 5 関連付けるデバイスを選択して、[選択/変更の保存（Save Selected/Changes）] をクリックします。

ステップ 6 [関連リンク（Related Links）] から、[ユーザの設定に戻る（Back to User）] を選択し、[移動（Go）] をクリックします。
[エンドユーザの設定（End User Configuration）] ウィンドウが表示され、選択し、割り当てたデバイスが、[制御するデバイス（Controlled Devices）] ペインに表示されます。

CTI リモート デバイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	CTI リモート デバイスの設定 （446 ページ）	CTIリモートデバイスを作成します。
ステップ 2	デバイスへのディレクトリ番号の追加 （450 ページ）	CTIリモートデバイスを登録するには、そのデバイスに電話番号を追加する必要があります。
ステップ 3	リモート接続先の設定 （451 ページ）	最大4つの一意のリモート接続先を設定して、CTIリモートデバイスに関連付けることができます。

CTI リモート デバイスの設定

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウン リストから [CTI リモート デバイス（CTI Remote Device）] を選択して、[次へ（Next）] をクリックします。

ステップ 4 [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、「関連項目」の項を参照してください。

ステップ 5 [保存（Save）] をクリックします。

CTI リモート デバイス設定フィールド

CTI リモート デバイス情報

表 55 : [デバイス情報（Device Information）]

フィールド	説明
[登録（Registration）]	CTI リモート デバイスの登録ステータスを指定します。
[デバイスの状態（Device Status）]	デバイスがアクティブか非アクティブかを指定します。
[デバイスの信頼性（Device Trust）]	デバイスが信頼できるかどうかを指定します。

フィールド	説明
[アクティブなリモート接続先（Active Remote Destination）]	アクティブなリモート接続先かどうかを指定します。CTI クライアントは、任意の 1 つの時点で1つのリモート接続先を指定できます。着信コールと Dial via Office（DVO）コールは、アクティブなリモート接続先に転送されます。
[オーナーのユーザーID（Owner User ID）]	ドロップダウン リストから、割り当てられた電話ユーザーのユーザー ID を選択します。ユーザーIDは、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。
[デバイス名（Device Name）]	所有者のユーザーIDに基づいて自動的に入力される CTI のリモート デバイスの名前を指定します。 デバイス名の形式は、デフォルトで *CTIRD<OwnerUserID>* です。 このフィールドは編集できます。デバイス名には最大15文字を含めることができます。使用できる文字は、英字、数字、ダッシュ（-）、ピリオド、スペース、およびアンダースコアです。
[説明（Description）]	CTI リモート デバイスの説明テキストを入力します。 このフィールドには、128文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。
[デバイスプール（Device Pool）]	CTI のリモート デバイスの一般的な特性を定義するデバイス プールを選択します。 デバイスプールの設定方法の詳細については、「デバイス プールの構成時の設定」を参照してください。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストを使用から、コーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。

フィールド	説明
[ユーザー保留 MOH 音源（User Hold MOH Audio Source）]	ドロップダウン リストから、ユーザーが保留操作を開始する場合に保留音（MOH）として使用するオーディオ ソースを選択します。
[ネットワーク保留MOH音源（Network Hold MOH Audio Source）]	ドロップダウン リストから、ネットワークが保留操作を開始したときの MOH に使用するオーディオ ソースを選択します。
[ロケーション（Location）]	ドロップダウンリストから、デバイス プール内の電話およびゲートウェイと関連付けられている場所を選択します。
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーション CSS に、このデバイス プールに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。
[プレゼンテーションインジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）]	コール単位でコール表示制限を設定する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、Cisco Unified CM は内線コールに対して受信したすべての表示制限を無視します。

[コールルーティング情報（Call Routing Information）]

表 *56* : 着信/発信コール情報

フィールド	説明
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーション CSS に、このデバイスに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。
[デバイスプールの発信側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイス プールに設定されている発信側トランスフォーメーション CSS を使用する場合は、このボックスをオンにします。このチェックボックスを選択しない場合、デバイスは[トランク設定（Trunk Configuration）] ウィンドウで設定した発信側変換 CSS を使用します。

表 *57 : [*プロトコル固有情報（***Protocol Specific Information***）*]*

フィールド	説明
[プレゼンスグループ（Presence Group）]	このフィールドは、プレゼンス機能に対して設定します。 このアプリケーション ユーザーをプレゼンス機能とともに使用していない場合は、プレゼンス グループの設定をデフォルトの [なし（None）] のままにします。 ドロップダウン リストから、アプリケーション ユーザーのプレゼンス グループを選択します。選択したグループは、IPMASysUser などのアプリケーション ユーザーがモニターする宛先を指定します。
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされる SUBSCRIBE コーリング サーチ スペースは、Cisco Unified Communications Manager がエンド ユーザーから発信されたプレゼンス要求をルーティングする方法を決定します。この設定では、エンド ユーザーのプレゼンス（SUBSCRIBE）要求のコール処理サーチ スペースと別にコーリング サーチ スペースを適用できます。 ドロップダウン リストから、エンドユーザーのプレゼンス要求に使用する SUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified Communications Manager Administration で設定するすべてのコーリング サーチ スペースが、[SUBSCRIBE コーリングサーチスペース（SUBSCRIBE Calling Search Space）] ドロップダウン リストに表示されます。 ドロップダウン リストから、エンドユーザーに別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは [なし（None）] に設定されます。 この目的専用の SUBSCRIBE コーリング サーチ スペースを設定するには、他のコーリング サーチ スペースと同様に新しいコーリング サーチ スペースを設定します。

フィールド	説明
[再ルーティング用コーリングサーチスペース（Rerouting Calling Search Space）]	ドロップダウン リストから、再ルーティングに使用するコーリング サーチ スペースを選択します。 リファラーの再ルーティング コーリング サーチ スペースを使用して、参照先へのルートが検索されます。再ルーティング コーリング サーチ スペースが原因で参照メッセージが失敗すると、Refer Primitive は「405 Method Not Allowed」メッセージを表示して要求を拒否します。 リダイレクト（3xx）プリミティブおよび転送機能も再ルーティング コーリング サーチ スペースを使用して、リダイレクト先または転送先を検索します。

表 *58 :* サイレント情報

フィールド	説明
[サイレント（Do Not Disturb）]	リモート デバイスのサイレント機能を有効にするには、このチェックボックスをオンにします。
[DNDオプション（DND Option）]	電話機で DND を有効にすると、[着信拒否（Call Reject）] オプションの指定により、着信コール情報がユーザーに表示されなくなります。[DND着信コール警告（DND Incoming Call Alert）] パラメータの設定に応じて、電話はビープを再生するか、コールの点滅通知を表示します。

デバイスへのディレクトリ番号の追加

CTI リモート デバイスを登録するには、そのデバイスにディレクトリ番号を追加する必要があります。ディレクトリ番号のない CTI リモート デバイスを登録することはできません。CTI リモート デバイスには最大 5 つのディレクトリ番号を追加できます。

手順

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

ステップ 2 フィルタ条件を指定して、ディレクトリ番号を関連付ける CTI リモート デバイスをクリックします。

ステップ 3 [関連付け（Association）] ペインで、[新規DNを追加（Add a new DN）] リンクをクリックします。

ステップ 4 [ディレクトリ番号の設定（Directory Number 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。

ステップ 5 [保存（Save）] をクリックします。

リモート接続先の設定

CTIリモートデバイスには、1つ以上のリモート送信先を設定できます。リモート接続先とは、リモート接続先ピックアップ（ユーザのデスクの電話機から転送を受け入れる）を実行し、Cisco Unified Mobility の着信コールを受け入れるように、設定できるモバイルなどの電話機です。CTI のリモート デバイスに関連付けられているリモート接続先では、リモート デバイスに到達するための電話番号を指定します。CTIのリモートデバイスに設定可能なリモート接続先の最大数は、オーナーのユーザ ID に設定されたリモート接続先の制限値で決まります。

リモート接続先には、次のいずれかのデバイスを含めることができます。

- シングルモード携帯（セルラー）電話
- スマートフォン
- デュアルモード電話
- デスクの電話機と同じクラスタにない社内の IP 電話
- PSTN 内の自宅の電話番号

手順

ステップ 1 Cisco Unified CMの管理から、**デバイス** > **電話** > **CTIリモートデバイス** > **関連付けられたリモート接続先**を選択します。

ステップ 2 フィルタ条件を指定し、リモート通知先を設定するCTI リモートデバイスをクリックします。

ステップ 3 **関連付けられたリモート接続先**区画で**新規リモート接続先の追加**を選択します。

別の方法として、**デバイス** > **電話** > **機 [**新しいメニューの追加 (Add New)] を使用してリモート通知先を設定することもできます。

ステップ 4 **リモート接続先の設定**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」の項を参照してください。

ステップ 5 [保存（Save）] をクリックします。

リモート接続先の設定フィールド

表 *59 :* リモート接続先の設定フィールド

フィールド	説明
名前	リモート宛先の名前を入力します。
[宛先番号（Destination Number）]	企業内でダイヤルする番号を入力します。市外局番、および外線の取得に必要な追加番号を含めてください。フィールドの最大長は24文字です。値には、0～9の数字、*、#、および+を入力できます。リモート接続先の発信者 ID を設定することを推奨します。
[オーナーのユーザID（Owner User ID）]	ドロップダウンリストから、リモート通知先の所有者を選択します。
[Unified Mobility 機能を有効にする（Enable Unified Mobility features）]	Unified Mobility機能を有効にするチェックボックスをオンにします。
[リモート接続先プロファイル（Remote Destination Profile）]	[設定 (From)] ドロップダウンリストで、設定したプロファイルを選択します。
[シングル ナンバー リーチを有効にする（Enable Single Number Reach）]	チェックボックスをオンにして、リモートの通知先に対して単一の Number_Reach を有効にします。
[携帯電話への移動を有効にする（Enable Move to Mobile）]	これはオプションのフィールドです。この電話が携帯電話の場合は、このチェックボックスをオンにします。

Cisco Spark リモート デバイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Spark リモート デバイスの設定（453 ページ）	Cisco Spark リモート デバイスを作成します。
ステップ 2	Cisco Spark デバイスへのディレクトリ番号の追加 （459 ページ）	Cisco Spark リモート デバイスを登録するには、そのデバイスに電話番号を追加する必要があります。

Cisco Spark リモート デバイスの設定

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウン リストから、[Cisco Spark リモート デバイス（Cisco Spark Remote Device）] を選択して、[次へ（Next）] をクリックします。

ステップ 4 [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、「関連項目」の項を参照してください。

ステップ 5 [保存（Save）] をクリックします。

Cisco Spark リモート デバイス設定フィールド

表 *60 : Webex* リモート デバイス設定フィールド

フィールド	説明
[デバイス情報（Device Information）]	
[登録（Registration）]	Webex リモート デバイスの登録ステータスを指定します。
[デバイスの状態（Device Status）]	デバイスがアクティブか非アクティブかを指定します。
[デバイスの信頼性（Device Trust）]	デバイスを信頼できるか信頼できないかを指定します。
[アクティブなリモート接続先（Active Remote Destination）]	リモート接続先がアクティブであるかどうかを指定します。デフォルトでは、Webex クライアントのアクティブなリモート接続先は 1 つだけです。着信コールはすべてアクティブなリモート接続先にルーティングされます。このフィールドは、アクティブなリモート接続先に関連付けられている場合でも [なし（None）] に設定されます。
[オーナーのユーザーID（Owner User ID）]	ドロップダウン リストから、割り当てられた電話ユーザーのユーザー ID を選択します。ユーザーIDは、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。

フィールド	説明
[デバイス名（Device Name）]	[オーナーのユーザー ID（Owner User ID）] に基づいて自動的に入力される Webex リモート デバイスの名前を使用します。 デフォルトでは、デバイス名の形式は *SparkRD*<オーナーユーザー*ID*> です。デフォルトのデバイス名 *SparkRD* は変更できません。 このフィールドは編集できます。デバイス名には最大 15 文字を含めることができます。使用できる文字は、英字、数字、ダッシュ（-）、ピリオド、スペース、およびアンダースコアです。
[説明（Description）]	Webex リモート デバイスの説明テキストを入力します。 このフィールドには、128 文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。
[デバイスプール（Device Pool）]	Webex リモート デバイスの共通の特性を定義するデバイス プールを選択します。 デバイスプールの設定方法の詳細については、「デバイス プールの構成時の設定」を参照してください。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストを使用から、コーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[ユーザー保留 MOH 音源（User Hold MOH Audio Source）]	ドロップダウン リストから、ユーザーが保留操作を開始したときの保留音（MOH）に使用するオーディオ ソースを選択します。 **注意** 現在、Cisco Spark リモート デバイスには保留/復帰機能が実装されていないため、MOH はサポートされていません。

フィールド	説明
[ネットワーク保留MOH音源（Network Hold MOH Audio Source）]	ドロップダウン リストから、ネットワークが保留操作を開始したときの MOH に使用するオーディオ ソースを選択します。 **注意** 現在、Cisco Spark リモート デバイスには保留/復帰機能が実装されていないため、MOH はサポートされていません。
[ロケーション（Location）]	ドロップダウン リストから、デバイス プール内の電話およびゲートウェイと関連付けられている場所を選択します。
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーション CSS に、このデバイス プールに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。
[プレゼンテーションインジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）]	コール単位でコール表示制限を設定する場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、Cisco Unified CM は内線コールに対して受信したすべての表示制限を無視します。
[コールルーティング情報（Call Routing Information）]	
[着信コールと発信コールの情報（Inbound and Outbound Calls Information）]	
[発信側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発信側トランスフォーメーション CSS に、このデバイスに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。
[デバイスプールの発信側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイス プールに設定されている発信側トランスフォーメーション CSS を使用する場合は、このボックスをオンにします。このチェックボックスをオンにしない場合、デバイスは[トランクの設定（Trunk Configuration）] ウィンドウで設定した発信側トランスフォーメーション CSS を使用します。

フィールド	説明
[プロトコル固有情報（Protocol Specific Information）]	
[プレゼンスグループ（Presence Group）]	このフィールドは、プレゼンス機能に対して設定します。 このアプリケーション ユーザーをプレゼンス機能とともに使用していない場合は、プレゼンス グループの設定をデフォルトの [なし（None）] のままにします。 ドロップダウン リストから、アプリケーション ユーザーのプレゼンス グループを選択します。選択したグループは、IPMASysUser などのアプリケーション ユーザーがモニターする宛先を指定します。 **注意** 現在、プレゼンス グループは Cisco Spark リモート デバイスではサポートされていません。

フィールド	説明
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされるSUBSCRIBE コーリング サーチ スペースによって、 Cisco Unified Communications Manager がエンド ユーザーから発信されるプレゼンス要求をルーティングする方法が決まります。この設定では、エンド ユーザーのプレゼンス（SUBSCRIBE）要求のコール処理サーチ スペースと別にコーリング サーチ スペースを適用できます。 ドロップダウン リストから、エンドユーザーのプレゼンス要求に使用するSUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified Communications Manager Administration で設定するすべてのコーリング サーチ スペースが、[SUBSCRIBE コーリングサーチスペース（SUBSCRIBE Calling Search Space）] ドロップダウン リストに表示されます。 ドロップダウン リストから、エンドユーザーに別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは [なし（None）] に設定されます。 この目的専用の SUBSCRIBE コーリング サーチ スペースを設定するには、他のコーリング サーチ スペースと同様に新しいコーリング サーチ スペースを設定します。 **注意** 現在、SUBSCRIBE コーリングサーチスペースはCisco Spark リモートデバイスではサポートされていません。

フィールド	説明
[再ルーティング用コーリングサーチスペース（Rerouting Calling Search Space）]	ドロップダウン リストから、再ルーティングに使用するコーリング サーチ スペースを選択します。 リファラーの再ルーティング コーリング サーチ スペースを使用して、参照先へのルートが検索されます。再ルーティング コーリング サーチ スペースが原因で参照メッセージが失敗すると、Refer Primitive は「405 Method Not Allowed」メッセージを表示して要求を拒否します。 リダイレクト（3xx）プリミティブおよび転送機能も再ルーティング コーリング サーチ スペースを使用して、リダイレクト先または転送先を検索します。
[サイレントの情報（Do Not Disturb Information）]	
[サイレント（Do Not Disturb）]	リモート デバイスのサイレント機能を有効にするには、このチェックボックスをオンにします。 **注意** DND オプションが有効になっている場合、コールは Cisco Spark クライアントにはルーティングされません。 **注意** 現在、サイレント機能は Cisco Spark リモート デバイスではサポートされていません。
[DNDオプション（DND Option）]	電話機で DND を有効にすると、[着信拒否（Call Reject）] オプションの指定により、着信コール情報がユーザーに表示されなくなります。[DND着信コール警告（DND Incoming Call Alert）] パラメータの設定に応じて、電話はビープを再生するか、コールの点滅通知を表示します。 **注意** 現在、サイレント機能は Cisco Spark リモート デバイスではサポートされていません。

Cisco Spark デバイスへのディレクトリ番号の追加

Webex リモート デバイスを登録するには、そのデバイスにディレクトリ番号を追加します。ディレクトリ番号のないWebexリモートデバイスを登録することはできません。Webexリモート デバイスには最大 5 つのディレクトリ番号を追加できます。

手順

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

ステップ 2 フィルタの条件を指定して、ディレクトリ番号を関連付ける Cisco Spark のリモート デバイスをクリックします。

ステップ 3 [関連付け（Association）] ペインで、[新規DNを追加（Add a new DN）] リンクをクリックします。

ステップ 4 [ディレクトリ番号の設定（Directory Number 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。

ステップ 5 [保存（Save）] をクリックします。

電話データの移行

手順

	コマンドまたはアクション	目的
ステップ 1	電話テンプレートの作成 （459 ページ）	一括管理ツール(BAT)で、データを移行する電話番号とプロトコルの電話テンプレートを作成します。
ステップ 2	電話データの移行 （460 ページ）	電話機のデータを別の電話に移行します。

電話テンプレートの作成

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 5 **電話の設定**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。

ステップ 6 [保存（Save）] をクリックします。

電話データの移行

始める前に

- 電話機をネットワークから切り離します。
- 新しい電話について、十分なデバイス ライセンス ユニットがあることを確認します。
- 電話機モデルが電話移行をサポートしていることを確認します。

手順

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

ステップ 2 検索条件を指定して、[検索（Find）] をクリックします。

ステップ 3 移行する電話機の設定を選択してクリックします。

ステップ 4 **関連リンク** ドロップダウンリストから**電話の移行**を選択します。
[電話の移行設定（Phone Migration Configuration）] ウィンドウが表示されます。

ステップ 5 ドロップダウン リストから、電話設定を移行する電話モデルの電話テンプレートを選択します。

ステップ 6 設定の移行先とする新規 **Cisco Unified IP Phone** のメディア アクセス コントロール（MAC）アドレスを入力します。MACアドレスには、12桁の16進数文字を使用する必要があります。

ステップ 7 (オプション)新しい電話の説明を入力します。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。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 新しい電話機は機能が失われる可能性があるという警告が表示されたら、[OK] をクリックします。

次のタスク

新しい電話機をネットワークに接続し、デバイスを登録します。

第 44 章

Cisco IP Phone電話の通話診断と品質レポートを設置する

診断およびレポートの概要

Cisco Unified Communications Manager には、Cisco IP Phone の通話品質を保証するためのオプションが 2 つあります。

- コール診断: コールの診断には、コール管理レコード (CMR) と音声品質メトリックの生成が含まれています。
- 品質報告ツールQRT-QRTはCisco Unified IP電話の音声品質と一般的な問題報告ツールです。このツールを使用すると、ユーザはIP電話に音声やその他の一般的な問題を簡単に、かつ正確にレポートできます。

コール診断の概要

コール診断を収集するために、SCCP と SIP を実行している Cisco IP Phone を設定することができます。通話診断には、診断記録とも呼ばれる通話管理記録(CMR)と音声品質指標が含まれる。

音声品質メトリックは、デフォルトで有効になっており、ほとんどの Cisco IP Phone でサポートされています。Cisco IP Phone は、MOS (平均意見四つ角) 値に基づいて音声品質メトリックを計算します。音声品質メトリックでは、ノイズや歪みは考慮されません。フレーム損失だけが考慮されます。

CMR レコードには、コールの音声ストリームの品質に関する情報が格納されます。CMR を生成するように Unified Communications Manager を設定できます。この情報は、請求レコードの生成やネットワーク分析などの後処理活動に使用できます。

品質レポートツールの概要

品質レポート ツール（QRT）は、Cisco IP 電話の音声品質と一般的な問題をレポートするツールです。このツールを使用すると、ユーザはIP電話に音声やその他の一般的な問題を簡単に、かつ正確にレポートできます。

システム管理者は、ユーザの IP 電話に QRT ソフトキーを表示するソフトキー テンプレートを設定して割り当てることで、QRT 機能を有効化できます。QRT を使用して行うユーザ インタラクションのレベルに応じて、2 つの異なるユーザ モードを選択できます。次に、システムにおける機能の動作を定義するため、システム パラメータを設定し、Cisco Unified Serviceability ツールを設定します。QRT Viewer アプリケーションを使用して、電話の問題レポートを作成、カスタマイズ、および表示できます。

ユーザーの IP 電話で問題が発生した場合、ユーザーは、コールの状態がオンフックまたは接続済みのときに Cisco IP 電話の QRT ソフトキーを押すことで、問題のタイプとその他の関連統計をレポートできます。ユーザは IP 電話で報告されている問題を最もよく表している理由コードを選択できます。カスタマイズされた電話の問題レポートには、具体的な情報が表示されます。

ユーザが QRT ソフトキーを押して問題の種類を選択すると、QRT はストリーミングの統計情報を収集しようとします。ストリーミングの統計情報を収集するには、QRT でコールを 5 秒以上アクティブにする必要があります。

前提条件

コール診断の要件

Cisco Unified IP Phone がコール診断をサポートしているかどうかを確認します。

次の表を使用して、電話機がコール診断をサポートしているかどうかを確認します。コール診断の凡例は、次のようにサポートされています。

- X：SCCP と SIP の両方を実行している電話機によるサポート
- S：SCCP 機能のみ

表 *61 :* コール診断のデバイスサポート

デバイス	コール診断のサポート
Cisco Unified IP Phone 7906	X
Cisco Unified IP Phone 7911	X
Cisco Unified IP Phone 7931	X
Cisco Unified IP Phone 7940	S

デバイス	コール診断のサポート
Cisco Unified IP Phone 7941	X
Cisco Unified IP Phone 7942-G	X
Cisco Unified IP Phone 7942-G/GE	X
Cisco Unified IP Phone 7945	X
Cisco Unified IP Phone 7960	S
Cisco Unified IP Phone 7961	X
Cisco Unified IP Phone 7962-G	X
Cisco Unified IP Phone 7962-G/GE	X
Cisco Unified IP Phone 7965	X
Cisco Unified IP Phone 7972-G/GE	X
Cisco Unified IP Phone 7975	X

品質レポートツールの要件

Cisco IP電話の機能：

- ソフトキー テンプレートのサポート
- IP Phone サービスのサポート
- CTI による制御が可能
- 内部 HTTP サーバを含む

詳細については、お使いの電話モデルのガイドを参照してください。

Diagnostics and Reporting 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
ステップ 1	コール診断の設定 （464 ページ）	このタスクを実行すると、CMR を生成するように Cisco Unified Communication Manager を設定できます。CMR レコードには、コールの音声ストリームの品質に関する情報が格納されます。CDRへのアクセスの詳細については、『*Cisco*

	コマンドまたはアクション	目的
		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。 音声品質メトリックは、Cisco IP Phone で自動的に有効になります。音声品質メトリックへのアクセス方法の詳細については、ご使用の電話機モデルの『Cisco Unified IP Phone アドミニストレーション ガイド』を参照してください。
ステップ 2	品質レポート ツールの設定 （465 ページ）を行うには、次のサブタスクを実行します。 • QRT ソフトキーを含むソフトキー テンプレートの設定 （466 ページ） • 共通デバイス設定と QRT ソフトキーテンプレートの関連付け （467 ページ） • 電話機への QRT ソフトキー テンプレートの追加 （469 ページ） • Cisco Unified Serviceability での QRT の設定 （470 ページ） • 品質レポートツールのサービスパラメータの設定 （473 ページ）	品質レポートツール(QRT)を設定して、IP phone で問題が発生したユーザが、QRT ソフトキーを押すことによって、問題のタイプやその他の関連統計情報をレポートできるようにします。

コール診断の設定

手順

ステップ 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。

ステップ 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。

ステップ 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。
[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。

ステップ 4 [クラスタ全体のパラメータ（デバイス - 全般）（Clusterwide Parameters (Device - General)）] エリアで、[コール診断有効（Call Diagnostics Enabled）] サービス パラメータを設定します。次のオプションを使用できます。

• [無効（Disabled）]：CMR は生成されません。

- [CDR有効フラグが True の場合のみ有効化（Enabled Only When CDR Enabled Flag is True）]：[呼詳細レコード（CDR）有効化フラグ（Call Detail Records (CDR) Enabled Flag ）] サービス パラメータが True に設定されている場合のみ、CMR が生成されます。
- [CDR 有効化フラグに関係なく有効化（Enabled Regardless of CDR Enabled Flag）]：[CDR 有効化フラグ（CDR Enabled Flag）] サービス パラメータの値に関係なく、CMR が生成されます。

（注） [CDR有効化フラグ（CDR Enabled Flag）] サービス パラメータを有効にせずに CMR を生成すると、制御されずにディスク容量が消費される場合があります。CMR を有効にする場合は、CDR を有効にすることをお勧めします。

ステップ 5 [保存（Save）] をクリックします。

品質レポート ツールの設定

品質レポートツール (QRT) を設定して、IP phone で問題が発生したユーザが、QRT ソフトキーを押すことによって、問題のタイプやその他の関連統計情報をレポート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
ステップ 1	QRT ソフトキーを含むソフトキー テンプレートの設定 （466 ページ）	QRTソフトキーのオンフック状態と接続済みコール状態を設定する必要があります。次のコール状態も利用できます。 • 接続された会議 • 接続転送
ステップ 2	（任意） 共通デバイス設定と QRT ソフトキー テンプレートの関連付け （467 ページ） を行うには、次のサブタスクを実行します。 • 共通デバイス設定への QRT ソフトキー テンプレートの追加 （468 ページ） • 電話機と共通デバイス設定の関連付け （469 ページ）	ソフトキー テンプレートを電話で使用できるようにするには、この手順か次の手順のいずれかを実行する必要があります。システムが [共通デバイス設定（Common Device Configuration）] を使用して設定オプションを電話機に適用する場合は、この手順に従います。これは、電話機でソフトキー テンプレートを使用できるようにする際に、最も一般的に使用されている方法です。
ステップ 3	（任意） 電話機への QRT ソフトキー テンプレートの追加 （469 ページ）	次の手順は、ソフトキー テンプレートと共通デバイス設定を関連付けるための代替手段として、または共通デバイス設定と共に使用します。ソフトキー テン

	コマンドまたはアクション	目的
		プレートを適用して、共通デバイス設定での割り当てや、他のデフォルトのソフトキーの割り当てを上書きする必要がある場合は、次の手順を共通デバイス設定と共に使用します。
ステップ 4	Cisco Unified Serviceability での QRT の設定 （470ページ）を行うには、次のサブタスクを実行します。 • Cisco Extended Functions サービスの有効化 （470 ページ） • アラームの設定 （471 ページ） • トレースの設定 （472 ページ）	
ステップ 5	（任意） 品質レポートツールのサービスパラメータの設定 （473 ページ）	

QRT ソフトキーを含むソフトキー テンプレートの設定

QRTソフトキーのオンフック状態と接続済みコール状態を設定する必要があります。次のコール状態も利用できます。

- 接続された会議
- 接続転送

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 9 [保存（Save）] をクリックします。

ステップ 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

次のいずれかの手順を実行します。

- 共通デバイス設定への QRT ソフトキー テンプレートの追加 （468 ページ）
- 電話機への QRT ソフトキー テンプレートの追加 （469 ページ）

共通デバイス設定と QRT ソフトキー テンプレートの関連付け

（省略可）ソフトキー テンプレートを電話機に関連付ける方法は 2 つあります。

- ソフトキー テンプレートを電話機設定に追加する。
- ソフトキー テンプレートを共通デバイス設定に追加する。

ここに示す手順では、ソフトキーテンプレートを共通デバイス設定に関連付ける方法について説明します。システムが共通デバイス設定を使用して設定オプションを電話機に適用する場合は、この手順に従ってください。これは、電話機でソフトキーテンプレートを使用できるようにする際に、最も一般的に使用されている方法です。

別の方法を使用するには、「電話機への QRT ソフトキーテンプレートの追加 （469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
ステップ 1	共通デバイス設定への QRT ソフトキーテンプレートの追加 （468 ページ）	
ステップ 2	電話機と共通デバイス設定の関連付け（469 ページ）	

共通デバイス設定への QRT ソフトキー テンプレートの追加

始める前に

QRT ソフトキーを含むソフトキー テンプレートの設定 （466 ページ）

手順

ステップ 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）] > [共通デバイス設定（Common Device Configuration）]** を選択します。

ステップ 2 新しい共通デバイス設定を作成し、それにソフトキーテンプレートを関連付けるには、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) [名前（Name）] フィールドに、共通デバイス設定の名前を入力します。
c) [保存（Save）] をクリックします。

ステップ 3 既存の共通デバイス設定にソフトキーテンプレートを追加するには、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) 既存の共通デバイス設定をクリックします。

ステップ 4 [ソフトキー テンプレート（Softkey Template）] ドロップダウン リストで、使用可能にするソフトキーが含まれているソフトキー テンプレートを選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 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共通デバイス設定を変更した場合は、[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。
- 新しい共通デバイス設定を作成してその設定をデバイスに関連付けた後に、デバイスを再起動します。

次のタスク

電話機と共通デバイス設定の関連付け （469 ページ）

電話機と共通デバイス設定の関連付け

始める前に

共通デバイス設定への QRT ソフトキー テンプレートの追加 （468 ページ）

手順

ステップ 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）]**。

ステップ 2 **[検索 (Find)]** をクリックし、ソフトキーテンプレートを追加する電話デバイスを選択します。

ステップ 3 [共通デバイス設定（Common Device Configuration）] ドロップダウン リストから、新しいソフトキー テンプレートが含まれている共通デバイス設定を選択します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [リセット（Reset）] をクリックして、電話機の設定を更新します。

電話機への QRT ソフトキー テンプレートの追加

始める前に

QRT ソフトキーを含むソフトキー テンプレートの設定 （466 ページ）

手順

ステップ 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）]**。

ステップ 2 [検索（Find）] をクリックして、設定済みの電話のリストを表示します。

ステップ 3 電話ボタン テンプレートを追加する電話を選択します。

ステップ 4 [電話ボタン テンプレート（Phone Button Template）] ドロップダウン リストで、新しい機能ボタンが含まれる電話ボタン テンプレートを選択します。

ステップ 5 [保存（Save）] をクリックします。
電話の設定を更新するには[リセット（Reset）]を押すというメッセージ付きのダイアログ ボックスが表示されます。

Cisco Unified Serviceability での QRT の設定

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Extended Functions サービスの有効化 （470 ページ）	Cisco 拡張ファンクションサービスをアクティブにすると、品質レポートツールなどの音声品質機能がサポートされます。
ステップ 2	アラームの設定 （471 ページ）	QRT のアラームを設定して、SysLog ビュアー内のアプリケーションログのエラーをログに記録します。この機能は、アラームをログに記録し、アラームの説明と推奨される操作を提供します。Syslog ビューアにはCisco Unified Real-Time Monitoring Toolからアクセスできます。
ステップ 3	トレースの設定 （472 ページ）	音声アプリケーションのトレース情報をログに記録するように、QRT のトレースを設定します。QRTのトレースファイルに含める情報を構成したら、Cisco Unifie Rreal-Time監視ツールのトレースとログセンターオプションを使用して、トレースファイルを収集して表示できます。

Cisco Extended Functions サービスの有効化

Cisco 拡張ファンクションサービスをアクティブにすると、品質レポートツールなどの音声品質機能がサポートされます。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）]** > **[サービスの有効化（Service Activation）]** を選択します。

ステップ 2 **サーバ**ドロップダウンリストから、Cisco Extended Functionsサービスを有効にするノードを選択します。

ステップ 3 **Cisco Extended Functions**チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

アラームの設定 （471 ページ）

アラームの設定

QRT のアラームを設定して、SysLog ビュアー内のアプリケーションログのエラーをログに記録します。この機能は、アラームをログに記録し、アラームの説明と推奨される操作を提供します。Syslog ビューアにはCisco Unified Real-Time Monitoring Toolからアクセスできます。

始める前に

Cisco Extended Functions サービスの有効化 （470 ページ）

手順

ステップ 1 Cisco Unified Serviceability で、**アラーム** > **設定** を選択します。

ステップ 2 **サーバ**ドロップダウンリストから、ノードを設定する サーバを選択します。

ステップ 3 **サービスグループ**ドロップダウンリストから、**CMサービス**を選択します。

ステップ 4 [サービス（Service）] ドロップダウン リストから、[Cisco Extended Functions] を選択します。

ステップ 5 ローカルSyslogsとSDIトレースの両方について**アラームの有効化**チェックボックスをオンにします。

ステップ 6 こ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、ローカルSyslogsとSDIトレースの両方に アラームイベントレベルを設定します。

- **緊急**：このレベルは、システムが使用不可であることを示します。
- **アラート**：このレベルは、ただちに処置が必要であることを示します。
- **重要**：システムが重要な状態を検出したことを示します。
- **エラー**: エラー条件が検出されたことを示します。
- **警告**：このレベルは、警告状態が検出されたことを示します。
- **注意**: 通常の重要な条件が検出されていることを示します。
- **情報**：情報メッセージのみを示す。
- **デバッグ**：Cisco技術サポートセンター(TAC)エンジニアにデバッグ用の詳細なイベント情報を指示します。

デフォルト値は **Error** です。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

トレースの設定 （472 ページ）

トレースの設定

音声アプリケーションのトレース情報をログに記録するように、QRT のトレースを設定します。QRTのトレースファイルに含める情報を構成したら、Cisco Unifie Rreal-Time監視ツールのトレースとログセンターオプションを使用して、トレースファイルを収集して表示できます。

始める前に

アラームの設定 （471 ページ）

手順

ステップ 1 Cisco Unified Serviceability から **トレース** > **設定**を選択します。

ステップ 2 **サーバ**ドロップダウンリストから、トレースを構成するノードを選択します。

ステップ 3 **サービスグループ**ドロップダウンリストから、**CMサービス**を選択します。

ステップ 4 [サービス（Service）] ドロップダウン リストから、[Cisco Extended Functions] を選択します。

ステップ 5 **トレースオン**チェックボックスをオンにします。

ステップ 6 こ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、**デバッグトレースレベル**を設定します。

- **エラー**：すべてのエラー状態、およびプロセスとデバイス初期化メッセージを追跡します。
- **特殊**：通常運転中に発生したすべての特殊な条件とサブシステムの状態遷移を追跡します。コール処理イベントをトレースします。
- **状態遷移**通常の操作中に発生したすべての状態遷移条件とメディア層イベントを追跡します。
- **重要**：すべての重要条件とルーチンの入り口と出口を追跡します。すべてのサービスがこの追跡レベルを使用するわけではありません。
- **Entry_exit**：すべての入力条件と終了条件、および基礎となるデバッグ情報を追跡します。
- **任意**：すべての条件と詳細なデバッグ情報を追跡します。
- **詳細**：アラート状態とイベントを追跡します。異常なパスで生成されたすべてのトレースに使用します。最小の CPU サイクル数を使用します。

デフォルト値は **Error** です。

ヒント トラブルシューティングのためには、このセクションにあるすべてのチェックボックスをオンにするようにしてください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

（省略可） 品質レポートツールのサービスパラメータの設定 （473 ページ）

品質レポートツールのサービスパラメータの設定

注意 Cisco Technical Assistance Center（TAC）の指示があった場合を除き、デフォルトのサービスパラメータ設定の使用をお勧めします。

手順

ステップ 1 Cisco Unified Communications Managerの管理ページで、**システム** > **サービスパラメータ**を選択します。

ステップ 2 QRT アプリケーションが存在するサーバを選択します。

ステップ 3 **Cisco Extended Functions**サービスを選択します。

ステップ 4 サービスパラメータを設定します。サービスパラメータとその設定オプションの詳細については、「関連項目」セクションを参照してください。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

品質レポート ツールのサービス パラメータ （473 ページ）

品質レポート ツールのサービス パラメータ

表 *62 :* 品質レポート ツールのサービス パラメータ

パラメータ	説明
拡張 QRT メニューの選択肢を表示する（Display Extended QRT Menu Choices）	拡張メニュー選択項目をユーザに表示するかどうかを決定します。次のいずれかの設定オプションを選択できます。 • このフィールドを [True] に設定すると、拡張メニュー選択項目が表示されます（対話モード）。 • このフィールドを [False] に設定すると、拡張メニュー選択項目が表示されません（サイレント モード）。 • 推奨するデフォルト値としてFalse（サイレント モード）が設定されています。

パラメータ	説明
ストリーミング統計のポーリング期間（Streaming Statistics Polling Duration）	ストリーミング統計情報のポーリングに使用する間隔を決定します。次のいずれかの設定オプションを選択できます。 • このフィールドを[-1]に設定すると、コールが終了するまでポーリングが行われます。 • このフィールドを[0]に設定すると、ポーリングはまったく行われません。 • このフィールドを任意の正の値に設定すると、その秒数の間、ポーリングが行われます。コールが終了すると、ポーリングは停止します。 • 推奨するデフォルトの値として、-1（コールが終了するまでポーリングを行う）が設定されています。
ストリーミング統計のポーリング頻度（秒）（Streaming Statistics Polling Frequency (seconds)）	ポーリング間に待機する秒数を入力します。 値の範囲は、30～3600です。推奨するデフォルトの値として30が設定されています。
最大ファイル数（Maximum No. of Files）	ファイルカウントを再起動し、古いファイルを上書きする前に、最大ファイル数を入力します。 有効な値は1~1万です。推奨するデフォルトの値は250です。
1ファイルあたりの最大回線数（Maximum No. of Lines per File）	各ファイルでの行の最大数を入力します。この数を超えると、次のファイルが始まります。 • 値の範囲は、100～2000です。 • 推奨するデフォルトの値として2000が設定されています。

パラメータ	説明
CTI Managerに安全に接続するためのCAPFプロファイルインスタンスID（CAPF Profile Instance Id for Secure Connection to CTI Manager）	CTI マネージャへのセキュアな接続を開くために Cisco Extended Function サービスが使用する、アプリケーションユーザ CCMQRTSysUser の CAPF アプリケーション プロファイルのインスタンス ID を入力します。CTI Manager Connection Security Flag パラメータが有効な場合、このパラメータを設定する必要があります。 （注） CTI Manager Connection Security Flag サービスパラメータを有効にすることで、セキュリティをオンにします。変更を有効にするためには、Cisco Extended Functions サービスを再起動する必要があります。
CTI Manager接続セキュリティフラグ（CTI Manager Connection Security Flag）	Cisco Extended Functions サービスの CTI Manager接続のセキュリティを有効にするか、または無効にするかを選択します。有効にすると、Cisco Extended Functions はアプリケーション ユーザ CCMQRTSysUser のインスタンス ID に設定された CAPF アプリケーション プロファイルを使用して、CTI マネージャへのセキュアな接続を開きます。 値は True または False を選択します。CTI へのセキュアな接続を有効にするには、True を選択する必要があります。

第 45 章

サードパーティ製 SIP 電話の設定

サードパーティ SIP エンドポイントの概要

Unified Communications Manager では、SIP を実行する Cisco IP Phone に加えて、さまざまなサードパーティ SIP エンドポイントをサポートしています。Cisco Unified Communications Manager の管理ページで、次のサードパーティ製 SIP エンドポイントを設定できます。

- サードパーティのSIP デバイス（アドバンスト）：この8回線の SIPデバイスは、RFC3261 に準拠し、SIPを実行しているサードパーティ製の電話機です。
- サードパーティのSIP デバイス（ベーシック）：この1回線の SIP デバイスは、RFC3261 に準拠し、SIP を実行しているサードパーティ製の電話機です。このデバイスには3つのデバイス ライセンス ユニット（DLU）が必要です。
- Assured Services SIP（AS-SIP）エンドポイントは、MLPP、DSCP、TLS/SRTP、および IPv6 の要件に準拠したSIPエンドポイントです。AS-SIP は、Unified Communications Manager上で複数のエンドポイントインターフェイスを実現します。
- Generic Desktop Video Endpoint：このSIPデバイスは、ビデオ、セキュリティ、設定可能な信頼、およびシスコの拡張機能をサポートします。このデバイスは8回線をサポートします。コールとビジー トリガーの最大数はそれぞれ 4 と 2 です。
- Generic Single Screen Room System：このSIP デバイスは、単一画面のテレプレゼンス（ルーム システム）、ビデオ、セキュリティ、設定可能な信頼、およびシスコの拡張機能をサポートします。このデバイスは8回線をサポートします。コールとビジートリガーの最大数はそれぞれ 4 と 2 です。
- Generic Single Screen Room System：このSIPデバイスは、複数画面のテレプレゼンス（ルームシステム）、ビデオ、セキュリティ、設定可能な信頼、およびシスコの拡張機能をサポートします。このデバイスは8回線をサポートします。コールとビジートリガーの最大数はそれぞれ 4 と 2 です。

サードパーティ SIP エンド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
ステップ 1	ダイジェストユーザの設定 （479 ページ）	ダイジェスト認証を有効にするには、ダイジェストユーザであるエンドユーザを設定します。SIP トランクにチャレンジを開始すると、Cisco Unified Communications Manager は、**エンドユーザー構成**ウィンドウで指定した要約証明書を使用して SIP ユーザーエージェントの応答を検証します。 サードパーティの sip 電話がサマリー・ユーザーをサポートしていない場合は、ユーザー ID がサードパーティの SIP 電話のディレクトリ番号と一致するユーザーを作成します。たとえば、1000 という名前のエンド ユーザを作成し、電話機に 1000 というカタログ番号を作成します。このユーザを電話機に割り当てます。
ステップ 2	SIP プロファイルの設定 （437 ページ）	SIP トランクに関連付けられている SIP 属性のセットを提供します。
ステップ 3	電話機のセキュリティ プロファイルの設定 （480 ページ）	ダイジェスト認証を使用するには、新しい電話セキュリティ プロファイルを設定する必要があります。自動登録用に提供されている標準の非セキュア SIP プロファイルの 1 つを使用する場合は、ダイジェスト認証を使用可能にできません。
ステップ 4	サードパーティ SIP エンドポイントの追加 （481 ページ）	サードパーティエンドポイントを設定します。
ステップ 5	エンドユーザへのデバイスの関連付け （482 ページ）	サードパーティのエンドポイントをエンドユーザーに関連付けます。

次のタスク

電源を供給し、ネットワーク接続を検証し、サードパーティの SIP エンドポイントのネットワーク設定を構成します。ネットワーク設定の設定の詳細については、サードパーティ SIP エンドポイントのユーザガイドを参照してください。

ダイジェストユーザの設定

ダイジェストユーザとして、エンドユーザを設定するには、次の手順を実行します。ダイジェスト認証によって、Cisco Unified Communications Manager は接続してくるデバイスが正当なものかどうかを確認できます。確認するとき、デバイスはユーザ名とパスワードに類似したダイジェスト クレデンシャルを検証用に Cisco Unified Communications Manager に送ります。送られたクレデンシャルがデータベース内に設定されたそのデバイスに対するクレデンシャルと一致した場合、ダイジェスト認証は成功となり、Cisco Unified Communications Manager によって SIP リクエストが処理されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）] > [エンドユーザ（End User）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [ユーザ ID（User ID）] を入力します。

ステップ 4 [姓（Last Name）] に入力します。

ステップ 5 [ダイジェスト クレデンシャル（Digest Credentials）] を入力します。ダイジェスト クレデンシャルは英数文字列です。

ステップ 6 [エンドユーザの設定（End User Configuration）] ウィンドウでその他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。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

SIP 電話のセキュア ポートの設定 （436 ページ）

SIP プロファイルの設定

AS-SIP エンドポイント と SIP トランクの SIP プロファイルを、SIP 設定を使用して設定するには、次の手順を使用します。

始める前に

- SIP 電話のセキュア ポートの設定 （436 ページ）
- サービスの再起動 （437 ページ）

手順

ステップ 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。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 プロファイルをコピーする場合は、[コピー（Copy）] 列のファイル アイコンをクリックします。

ステップ 4 新しいプロファイルの名前と説明を入力します。

ステップ 5 IPv6 スタックが構成されていて、2 つのスタックを展開する場合は、[ANATを有効化（Enable ANAT）] チェックボックスをオンにします。

（注） この設定は、Unity Connection を展開しているかどうかに適用されます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

電話機のセキュリティ プロファイルの設定 （480 ページ）

電話機のセキュリティ プロファイルの設定

Cisco Unified Communications Manager は、自動登録用の事前に定義された非セキュアなセキュリティプロファイル一式を提供します。電話のセキュリティ機能を有効にするには、新しいセキュリティプロファイルを設定し、それを電話に適用する必要があります。次の手順を実行して、新しいセキュリティプロファイルを設定します。

始める前に

SIP 電話を設定する場合は、次の手順を完了します。

- SIP 電話のセキュア ポートの設定 （436 ページ）
- サービスの再起動 （437 ページ）
- SIP プロファイルの設定 （437 ページ）

手順

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 4 プロトコルを選択します。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 10 [保存（Save）] をクリックします。

サードパーティ SIP エンドポイントの追加

始める前に

ダイジェストユーザの設定 （479 ページ）

手順

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

ステップ 2 次のいずれかの手順を実行します。

- 新しいサードパーティ エンドポイントを作成するには、[新規追加（Add New）] をクリックします。
- 既存のサードパーティ エンドポイントを選択するには、[検索（Find）] をクリックして検索します。

ステップ 3 [電話タイプ（Phone Type）] ドロップダウン リストから、次のいずれかを選択します。

- [サードパーティ SIP デバイス（基本）（Third-party SIP Device (Basic)）]
- [サードパーティ SIP デバイス（拡張）（Third-party SIP Device (Advanced)）]
- [サードパーティ AS-SIP デバイス（Third-Party AS-SIP Device）]

- [サードパーティ AS-SIP エンドポイント（Third-party AS-SIP Endpoint）]
- [汎用デスクトップ ビデオ エンドポイント（Generic Desktop Video Endpoint）]
- [汎用 1 画面ルーム システム（Generic Single Screen Room System）]
- [汎用複数画面ルーム システム（Generic Multiple Screen Room System）]

ステップ 4 [ダイジェストユーザ（Digest User）] ドロップダウン リストから、作成したユーザを選択します。

ステップ 5 [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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 サードパーティのエンドポイントの電話番号を設定するには、ウィンドウの左側にある [関連付け情報（Association Information）] エリアに表示される、[新しい DN を追加（Add a New DN）] リンクをクリックします。
[電話番号の設定（Directory Number Configuration）] ウィンドウが表示されます。

ステップ 8 [ディレクトリ番号の設定（Directory Number 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。

次のタスク

エンドユーザへのデバイスの関連付け （482 ページ）

エンドユーザへのデバイスの関連付け

サードパーティのエンドポイントにエンドユーザを関連付けるには、この手順を実行します。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）] > [エンドユーザ（End User）]** を選択します。

ステップ 2 [検索（Find）] をクリックして、デバイスに関連付けるユーザを選択します。

ステップ 3 [デバイス情報（Device Information）] セクションで、[デバイスの関連付け（Device Association）] を選択します。
[ユーザデバイス割り当て（User Device Association）] ウィンドウが表示されます。

ステップ 4 [検索（Find）] をクリックすると、使用可能なデバイスのリストが表示されます。

ステップ 5 関連付けるデバイスを選択して、[選択/変更の保存（Save Selected/Changes）] をクリックします。

ステップ 6 [関連リンク（Related Links）] から、[ユーザの設定に戻る（Back to User）] を選択し、[移動（Go）] をクリックします。
[エンドユーザの設定（End User Configuration）] ウィンドウが表示され、選択し、割り当てたデバイスが、[制御するデバイス（Controlled Devices）] ペインに表示されます。

サードパーティ製品の連携動作と制限事項

サードパーティ製品の制限

表 *63* : サードパーティ *SIP* エンドポイントの制限

制限事項	説明
サードパーティ SIP エンドポイントに登録されている Cisco Video Communications Server (VCS) の Ringback トーン制限	Cisco Unified Communications Manager に登録された VCS エンドポイント上で発生する転送を要求するためのブラインド転送やスイッチには、リングバック トーンはありません。コール転送を行う場合は、[保留 (MOH)] で音楽を割り当てますが、ringback 音は割り当てません。

第 46 章

デバイス プロファイルとテンプレート

デバイスプロファイルおよびテンプレートの概要

この章では、デバイスプロファイルとテンプレートを構成する方法について説明します。特定の機能の設定については、『*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-maintenance-guides-list.html）を参照してください。

デバイス プロファイル

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サービス、機能、ディレクトリ番号を定義します。デバイスプロファイルを設定すると、ユーザデバイスプロファイルをユーザに割り当てることができるため、ユーザがデバイスにログインすると、その機能とサービスがデバイスで使用できるようになります。

エンドポイントの SIP プロファイル

SIP プロファイルは、SIP エンドポイントに関連付けられている一連の SIP 属性で構成されています。SIP プロファイルには、名前、説明、タイミング、再試行、コール ピックアップ URI などが含まれます。プロファイルに含まれる一部の標準エントリは、削除または変更ができません。

デバイス プロファイルとテンプレート

Cisco Unified Communications Manager は、デバイス プロファイルのデフォルトもサポートします。ユーザーがユーザーデバイスプロファイルが存在しない電話番号にログインするたびに、Cisco Unified Communications Managerはデフォルトデバイスプロファイルを使用します。

ピアツーピアのイメージ配信

ピアファームウェア共有機能は、高速なキャンパス LAN を設定する場合に次の利点をもたらします。

- 中央集中型 TFTP サーバへの TFTP 転送で、輻輳が抑制されます。
- ファームウェアのアップグレードを手動で制御する必要がありません。
- アップグレード中に多数のデバイスを同時にリセットするとき、電話機のダウンタイムが削減されます。

ピアファームウェア共有機能は、帯域幅の限られた WAN リンク経由で事業所が配置されているシナリオにおいて、ほとんどの状況でファームウェアのアップグレードを最適化します。

この機能を有効になっている場合、電話でサブネット上の類似した電話を検出できるようになります。これらの電話はファームウェアイメージを構成するファイルを要求しており、ファイルごとに階層を自動的に結合することができます。ファームウェアイメージを構成する個々のファイルを TFTP サーバから取得できるのは、階層内のルート電話機だけです。ファイルは、TCP 接続を使用して転送階層の下方向にすぐに転送され、サブネット上の他の電話機に到達します。

デバイス プロファイルとテンプレートの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	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 （488 ページ）	デフォルト デバイス プロファイルをソフトキー テンプレートに追加します。
ステップ 2	共通デバイス設定とソフトキー テンプレートの関連付け （489 ページ）	（省略可）電話機でソフトキーテンプレートを使用できるようにするには、テンプレートを共通デバイス設定に関連付けるか、電話機に直接関連付ける必要があります。システムが共通のデバイス構成を使用して電話に設定オプションを適用する場合は、この手順を実行します (これは、電話でソフトキーテンプレートを使用できる最も一般的な方法です)。

	コマンドまたはアクション	目的
		（注） 一括管理ツールを使用して複数の電話て通デバイス構成を関連付ける方法の詳細ついては、『*Cisco Unified Communicatio Manager*一括管理ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanag products-maintenance-guides-list.html）を照してください。.
ステップ 3	電話機とソフトキー テンプレートの関連付け （491 ページ）	（省略可）次の手順は、ソフトキー テンプレートと共通デバイス設定を関連付けるための代替手段として、または共通デバイス設定と共に使用します。ソフトキーテンプレートを適用して、共通デバイス設定での割り当てや、他のデフォルトのソフトキーの割り当てを上書きする必要がある場合は、次の手順を共通デバイス設定と共に使用します。
ステップ 4	機能管理ポリシーの設定タスク フロー（491 ページ）	（省略可）この手順は、ソフトキーテンプレートを設定する代わりに使用します。特定の機能を有効または無効にする機能制御ポリシーを設定して、電話機に表示されるソフトキーの表示を制御できます。共通の機能セットを使用させるユーザ グループの機能制御ポリシーを作成できます。たとえば、コール パーク機能とコール ピックアップ機能は一般に営業グループの従業員に使われますが、社内の従業員すべてには使われません。これら2つの機能のみ有効にする機能制御ポリシーを作成し、営業グループにそのポリシーを指定します。機能制御ポリシーを作成したら、そのポリシーを各電話機、電話機のグループ、またはシステム内のすべての電話機に関連付けます。
ステップ 5	電話ボタン テンプレートの設定 （495 ページ） • 電話機とボタン テンプレートの関連付け （496 ページ）	次の手順を使用して、各 Cisco IP Phone モデルのデフォルトテンプレートを含めることができます。電話を追加する場合は、電話ボタン テンプレートの 1 つを

	コマンドまたはアクション	目的
		電話に割り当てるか、独自のテンプレートを作成します。
ステップ 6	デバイスプロファイルの設定（496 ページ）	SIP または SCCP をサポートしている任意の電話機モデル用のデバイスプロファイルを設定します。
ステップ 7	エンドポイントの SIP プロファイルの設定（497 ページ）	電話機の新しい SIP プロファイルを設定します。
ステップ 8	デフォルト デバイス プロファイルの設定（497 ページ）	SIP または SCCP をサポートしている任意の電話機モデル用のデフォルトのデバイスプロファイルを設定します。

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 9 [保存（Save）] をクリックします。

ステップ 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）

共通デバイス設定とソフトキー テンプレートの関連付け

（省略可） ソフトキー テンプレートを電話機に関連付ける方法は 2 つあります。

- ソフトキー テンプレートを [電話の設定（Phone Configuration）] に追加する。

- ソフトキー テンプレートを**共通デバイス設定**に追加する。

ここに示す手順では、ソフトキーテンプレートを**共通デバイス設定**に関連付ける方法について説明します。システムが**共通デバイス設定**を使用して設定オプションを電話機に適用する場合は、この手順に従ってください。これは、電話機でソフトキーテンプレートを使用できるようにする際に、最も一般的に使用されている方法です。

別の方法を使用するには、「電話機とソフトキーテンプレートの関連付け」のセクションを参照してください。

手順

ステップ 1 共通デバイス設定へのソフトキー テンプレートの追加 （490 ページ）
ステップ 2 電話機と共通デバイス設定の関連付け （491 ページ）

共通デバイス設定へのソフトキー テンプレートの追加

手順

ステップ 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）] > [共通デバイス設定（Common Device Configuration）]** を選択します。

ステップ 2 新しい共通デバイス設定を作成し、それにソフトキーテンプレートを関連付けるには、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) [名前（Name）] フィールドに、共通デバイス設定の名前を入力します。
c) [保存（Save）] をクリックします。

ステップ 3 既存の共通デバイス設定にソフトキーテンプレートを追加するには、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) 既存の共通デバイス設定をクリックします。

ステップ 4 [ソフトキー テンプレート（Softkey Template）] ドロップダウン リストで、使用可能にするソフトキーが含まれているソフトキー テンプレートを選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 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共通デバイス設定を変更した場合は、[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。
- 新しい共通デバイス設定を作成してその設定をデバイスに関連付けた後に、デバイスを再起動します。

電話機と共通デバイス設定の関連付け

手順

ステップ 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）]**。

ステップ 2 [**検索 (Find**)] をクリックし、ソフトキーテンプレートを追加する電話デバイスを選択します。

ステップ 3 [共通デバイス設定（Common Device Configuration）] ドロップダウン リストから、新しいソフトキー テンプレートが含まれている共通デバイス設定を選択します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [リセット（Reset）] をクリックして、電話機の設定を更新します。

電話機とソフトキー テンプレートの関連付け

（省略可）ソフトキーテンプレートを共有デバイス設定に関連付ける代わりに、この手順を使用します。この手順は、共通デバイス設定とともにも機能します。共有デバイス設定での割り当て、またはその他のデフォルトのソフトキー割り当てをオーバーライドするソフトキーテンプレートを割り当てる場合に、この手順を使用できます。

手順

ステップ 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）]**。

ステップ 2 [検索（Find）] をクリックして、ソフトキー テンプレートを追加する電話を選択します。

ステップ 3 [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、新しいソフトキーが含まれているテンプレートを選択します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [リセット（Reset）] を押して、電話機の設定を更新します。

機能管理ポリシーの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	電話機能一覧の生成 （492 ページ）	Cisco Unified Reporting にログインし、電話機能リスト レポートを実行して、

	コマンドまたはアクション	目的
		機能管理ポリシーをサポートする電話を決定します。
ステップ 2	機能管理ポリシーの作成 （493 ページ）	Cisco IP 電話の機能管理ポリシーを作成します。
ステップ 3	次のいずれかの操作を実行します。 • 電話への機能管理ポリシーの適用 （493 ページ） • 共通の電話プロファイルへの機能管理ポリシーの適用 （494 ページ） • すべての電話への機能管理ポリシーの適用 （494 ページ）	機能管理ポリシーを設定したら、そのポリシーを各電話機、電話機のグループ、またはシステム内のすべての電話機に関連付ける必要があります。各電話の機能管理ポリシーは、クラスタ全体の機能管理ポリシーより優先されます。 （注） 一括管理ツールを使用して複数の電話に機能管理ポリシーを適用する方法については、『*Cisco Unified Communications Manager* 一括管理ガイド』を参照してください。

電話機能一覧の生成

電話機能一覧のレポートを生成し、設定したい機能をどのデバイスがサポートしているのか判別します。

手順

ステップ 1 Cisco Unified Reporting から **[System Reports]** をクリックします。

ステップ 2 レポートのリストから、[Unified CM 電話機能一覧（Unified CM Phone Feature List）] をクリックします。

ステップ 3 次のいずれかの手順を実行します。

- [レポートの新規生成（Generate New Report）] （棒グラフのアイコン）を選択し、新しいレポートを生成します。
- レポートが存在する場合は、**Unified CM電話機能一覧**を選択します。

ステップ 4 [製品（Product）] ドロップダウン リストから、[All] を選択します。

ステップ 5 設定の対象となる機能の名前をクリックします。

ステップ 6 レポートを生成するには、[送信（Submit）] 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [保存（Save）] をクリックします。

電話への機能管理ポリシーの適用

始める前に

- 電話モデルが機能管理ポリシーをサポートしていることを確認します。詳細については、「電話機能一覧の生成 （492 ページ）」を参照してください。
- 機能管理ポリシーの作成 （493 ページ）

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [電話（Phone）]** を選択します。
ステップ 2 検索条件を入力し、[検索（Find）] をクリックします。
Cisco Unified Communications Manager で設定されている電話機の一覧が表示されます。
ステップ 3 機能管理ポリシーを適用する電話を選択します。
ステップ 4 [機能管理ポリシー（Feature Control Policy）] ドロップダウン リストから、必要な機能管理ポリシーを選択します。
ステップ 5 [保存（Save）] をクリックします。
ステップ 6 [設定の適用（Apply Config）] をクリックします。
ステップ 7 [OK] をクリックします。

共通の電話プロファイルへの機能管理ポリシーの適用

共通の電話プロファイルを使用すると、機能管理ポリシーを設定し、そのプロファイルを使用するネットワーク内のすべての電話にこれらの設定を適用できます。

始める前に

機能管理ポリシーの作成 （493 ページ）

手順

ステップ 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）]** を選択します。
ステップ 2 検索条件を入力し、[検索（Find）] をクリックします。
ステップ 3 機能管理ポリシーを適用する共通の電話プロファイルを選択します。
ステップ 4 [機能管理ポリシー（Feature Control Policy）] ドロップダウン リストから、必要な機能管理ポリシーを選択します。
ステップ 5 [保存（Save）] をクリックします。
ステップ 6 [設定の適用（Apply Config）] をクリックします。
ステップ 7 [OK] をクリックします。

すべての電話への機能管理ポリシーの適用

始める前に

機能管理ポリシーの作成 （493 ページ）

手順

ステップ 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。

ステップ 2 [機能管理ポリシー（Feature Control Policy）] ドロップダウン リストから、必要な機能管理ポリシーを選択します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 [OK] をクリックします。

電話ボタン テンプレートの設定

手順

ステップ 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）]** > **[電話ボタンテンプレート（Phone Button Template）]**。

ステップ 2 [**検索 (Find)**] をクリックして、サポートされる電話テンプレートのリストを表示します。

ステップ 3 新しい電話ボタン テンプレートを作成する場合は、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) 電話機モデルのデフォルトのテンプレートを選択し、[コピー（Copy）] をクリックします。

b) [電話ボタン テンプレート情報（Phone Button Templates Information）] フィールドに、テンプレートの新しい名前を入力します。

c) [保存（Save）] をクリックします。

ステップ 4 既存のテンプレートに電話ボタンを追加するには、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) 既存のテンプレートを選択します。

ステップ 5 [回線（Line）] ドロップダウン リストから、テンプレートに追加する機能を選択します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 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。

電話機とボタン テンプレートの関連付け

始める前に

電話ボタン テンプレートの設定 （495 ページ）

手順

ステップ 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）]**。

ステップ 2 [検索（Find）] をクリックして、設定済みの電話のリストを表示します。

ステップ 3 電話ボタン テンプレートを追加する電話を選択します。

ステップ 4 [電話ボタン テンプレート（Phone Button Template）] ドロップダウン リストで、新しい機能ボタンが含まれる電話ボタン テンプレートを選択します。

ステップ 5 [保存（Save）] をクリックします。
電話の設定を更新するには[リセット（Reset）]を押すというメッセージ付きのダイアログ ボックスが表示されます。

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

ステップ 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。

ステップ 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。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 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。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 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。

ステップ 7 （省略可）[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。

ステップ 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。

ステップ 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。

エンドポイントの SIP プロファイルの設定

Cisco Unified Communications ManagerはSIPプロファイルを使用して、SIPトランクとCisco Unified IP電話に関連するSIPプロパティを定義します。

手順

ステップ 1 **Cisco Unified CMの管理**ウィンドウで、**デバイス** > **デバイスの設定** > **SIPプロファイル**を選択します。

ステップ 2 新しいsipプロファイルを追加するには、「新規を追加」ボタンをクリックします。**[新規追加(Add New)]** ボタンをクリックします。

ステップ 3 **SIPプロファイルの設定**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。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

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

ステップ 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。

ステップ 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。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 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。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 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。

ステップ 7 [保存（Save）] をクリックします。

電話のピアツーピア イメージの配信機能の設定

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、**[デバイス（Device）] > [電話（Phone）]** を選択します。

ステップ 2 [電話機の検索とリスト] ウィンドウで電話を選択するには、[電話機の検索 (where)] フィールドで適切なフィルターを指定し、[検索 (find)] をクリックして電話機のリストを取得してから、リストから電話機を選択します。

ステップ 3 [電話の設定 (Phone Configuration)] ウィンドウで、[プロダクト固有の設定] レイアウトペインの [ピアファームウェア共有 (ピア)] 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。

- **有効**(デフォルト)：電話でピアイメージ配信(PPID)がサポートされていることを示します。
- **無効**：電話がピアイメージ配信(PPID)をサポートしていないことを示します。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

第 47 章

ユーザとエンドポイントの関連付け

エンドポイントの関連付けの概要

この章では、デバイスをエンドユーザーとアプリケーションユーザーに関連付ける方法について説明します。エンドユーザは、関連付けられているデバイスを制御できます。ユーザーとして認識されるアプリケーションは、電話とコンピュータ電話の統合(CTI)ポートなどのデバイスを制御できます。

ユーザとエンドポイントの関連付け

エンドユーザとアプリケーションユーザをエンドユーザとユーザに設定してから、エンドユーザとエンドユーザをエンドユーザに関連付けます。「エンドユーザとデバイスの関連付け （500 ページ）」および「アプリケーション ユーザとデバイスの関連付け （503 ページ）」を参照してください。

ユーザおよびデバイスの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	エンド ユーザとデバイスの関連付け （500 ページ）。	エンドユーザをデバイスに関連付けます。
ステップ 2	アプリケーション ユーザとデバイスの関連付け （503 ページ）。	デバイスへのアプリケーション ユーザの関連付け

エンド ユーザとデバイスの関連付け

Cisco Unified Communications Manager では、エンド ユーザ ID の重複は許可されていません。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）] > [エンドユーザ（End User）]** を選択します。

ステップ 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、[検索（Find）] をクリックします。

ステップ 3 エンド ユーザのリストを表示するウィンドウで、該当するエンド ユーザのリンクをクリックします。

ステップ 4 [エンド ユーザの設定（End User Configuration）] ウィンドウで、[デバイス情報（Device Information）] 領域までスクロール ダウンし、エンド ユーザに関連付けるデバイスを選択します。[使用可能なデバイス（Available Devices）] ボックスで、アプリケーション ユーザに関連付けるデバイスを選択し、ボックスの下にある下矢印をクリックします。

（注） [デバイス情報（Device Information）] 領域にデバイスがない場合は、[デバイスの割り当て（Device Associations）] ボタンをクリックして、[ユーザとデバイスの関連付け（User Device Association）] ウィンドウを開きます。1 つまたは複数のデバイスを選択し、[選択/変更を保存（Save Selected/Changes）] ボタンをクリックします。選択したデバイスは、[デバイス情報（Device Information）] 領域の [制御されたデバイス（Controlled Devices）] リスト ボックスに表示されます。次に、ステップ 1 ～ 4 に従ってデバイスを関連付けます。

ステップ 5 （任意）ライン アピアランスをプレゼンスのエンド ユーザに関連付けるには、またこのライン アピアランスがオフフックの場合に、IM and Presence のクライアントに対して通話中のステータス情報を有効にするには、[ライン アピアランスのプレゼンスからの関連付け（Line Appearance Association from Presence）] ボタンをクリックします。[ライン アピアランスのプレゼンスとの関連付け（Line Appearance Association for Presence）] ウィンドウが表示され、ここで製品タイプ、デバイス名、ディレクトリ、パーティション、または説明を選択できます。このウィンドウで利用できる選択肢は、制御されたデバイスと関連付けられた回線によって異なります。[保存（Save）] をクリックします。

ステップ 6 [エンド ユーザの設定（End User Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。

ステップ 7 [保存（Save）] をクリックします。

エンドユーザとデバイスの設定値

表 *64 :* ユーザ情報

フィールド	説明
[ユーザID（User ID）]	エンド ユーザの識別名を入力します。Cisco Unified Communications Manager では、ユーザ ID の作成後の変更はできません。使用できる特殊文字は、=、+、<、>、#、;、\、,、“”、および空白です。
[パスワード（Password）]	エンド ユーザのパスワードとなる 5 文字以上の英数字または特殊文字を入力します。使用できる特殊文字は、=、+、<、>、#、;、\、,、“”および空白です。
[PIN]	個人識別番号（PIN）となる 5 文字以上の英数字を入力します。
[姓（Last Name）]	エンド ユーザの姓を入力します。使用できる特殊文字は、=、+、<、>、#、;、\、,、および空白です。
[ミドルネーム（Middle Name）]	エンドユーザのミドル ネームを入力します。使用できる特殊文字は、=、+、<、>、 #、;、\、,、“”および空白です。
[名（First Name）]	エンド ユーザの名を入力します。使用できる特殊文字は、=、+、<、>、#、;、\、,、および空白です。

表 *65 : [*デバイスの割り当て（*Device Associations***）*]***

フィールド	説明
製品タイプ（Product Type）	ドロップダウンリストから、このエンドユーザに関連付けるデバイスのタイプを選択します。
[MAC アドレス（MAC Address）]	新しいユーザに関連付ける新しいデバイスの固有の MAC アドレスを入力します。MAC アドレスは、12 桁の 16 進数（0 ～ 9、A ～ F）から構成されます。
[DNのコーリングサーチスペース(Calling Search Space DN)]	ドロップダウンリストボックスから、このユーザとデバイスに関連付ける電話番号用のコーリング サーチ スペースを選択します。

フィールド	説明
[電話機のコーリングサーチスペース(Calling Search Space Phone)]	ドロップダウンリストから、このユーザとデバイスに関連付ける電話機用のコーリングサーチ スペースを選択します。
[外部電話番号マスク（External Phone Number Mask）]	関連付けられたデバイスから発信される外部（発信）コールに対して、発信者 ID 情報をフォーマットするのに使用するマスクを指定します。 • このマスクには、最長 24 文字までを指定できます。有効な文字は 0 ～ 9、*、#、および X です。 • 発信者ID情報に表示する数字列を入力します。関連付けられたデバイスの電話番号を表すには、X を使用します。 • 外線コールを発信するために使用されるルート パターンで [外線電話番号マスクを使用（Use External Phone Number Mask）] オプションがオンになっている場合に、マスク 972813XXXX を指定すると、内線 1234 からの外部コールには、発信者 ID の番号として 9728131234 が表示されます。代表番号を表すために 9728135000 などのすべてのリテラル文字のマスクを指定すると、そのリテラル番号（9728135000）は自動登録された関連のデバイスからの外線コールの発信者 ID として表示されます。
[内線(Extension)]	新しいユーザと電話機の内線番号を入力します。使用できる文字は次のとおりです。0 ～ 9、?、[、]、+、-、*、^、#、! です。 このフィールドは、エンド ユーザのプライマリ電話番号を表します。エンド ユーザは、電話機に複数の回線を接続できます。
[ルートパーティション（Route Partition）]	ドロップダウンリストから、内線フィールドで指定した電話番号のパーティションを選択します。

フィールド	説明
[ボイスメールプロファイル（Voice Mail Profile）]	ドロップダウンリストから、電話番号のボイスメールプロファイルを選択します。 システム デフォルトを使用する場合は、なしを選択します。
[エクステンションモビリティの有効化（Enable Extension Mobility）]	エクステンション モビリティを有効にする場合は、このチェックボックスをオンにします。 新しいユーザを追加した後は、**[ユーザ管理（User Management）] > [エンドユーザ（End User）]** メニュー オプションを使用して、エクステンション モビリティ プロファイルを選択できます。

アプリケーション ユーザとデバイスの関連付け

アプリケーションユーザにデバイスを関連付け、アプリケーションユーザがそのデバイスのコントロール権を持つようにすることができます。電話機などのデバイスは、アプリケーションユーザが制御できます。ユーザとして識別されるアプリケーションは、CTI ポートなどその他のデバイスを制御できます。アプリケーションユーザが電話機のコントロール権を持つ場合、その電話機の特定の設定値（たとえば、スピード ダイヤルや自動転送）を制御できます。

始める前に

エンド ユーザとデバイスの関連付け （500 ページ）。

手順

ステップ 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（Application User）]** を選択します。
が表示されます。

ステップ 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、[検索（Find）] をクリックします。

ステップ 3 アプリケーションのユーザのリストから、該当するアプリケーションのユーザのリンクをクリックします。

ステップ 4 **アプリケーションユーザー構成**ウィンドウで、**デバイス情報**セクションまでスクロールします。[使用可能なデバイス（Available Devices）] ボックスで、アプリケーション ユーザに関連付けするデバイスを選択し、ボックスの下にある下向き矢印をクリックします。
選択したデバイスが**制御対象のデバイス**ボックスに移動します。

ステップ 5 利用可能なデバイスのリストに追加するには、次のいずれかのボタンをクリックします。

- **さらに電話を検索**：このアプリケーションユーザーに関連付ける電話番号を検索します。

- **別のルートポイントを検索**：このアプリケーションユーザーに関連付けるCTIルーティングポイントを検索します。
- **別のパイロットポイントを検索**：このアプリケーションユーザに関連付ける別のパイロットポイントを検索するには、このボタンをクリックします。

ステップ 6 アプリケーション ユーザに割り当てるデバイスごとに、上記ステップ 5 を繰り返します。

ステップ 7 [保存（Save）] をクリックします。

エンドポイントとユーザを関連付ける際の相互作用と制限

ユーザーとエンドポイントを関連付ける相互作用

表 *66 :* エンドポイントの相互作用を持つユーザー

機能	連携動作
非 CTI の制御可能なデバイス	H.323 デバイスのような CTI を制御できないデバイスの場合、使用可能なデバイスのリストのデバイス アイコンの横にアスタリスク（*）が表示されます。
Cisco Extension Mobility	Cisco Extension Mobility機能を使用して、Cisco IP電話を一時的にエンドユーザーの電話として表示するように設定します。エンドユーザが電話機にサインインすると、そのエンドユーザのエクステンションモビリティプロファイル（回線とスピードダイヤル番号を含む）が、その電話機上に置かれます。この機能は、エンドユーザに電話機が恒常的に割り当てられていない環境で主に使用されます。
IM and Presence Service	エンド ユーザがIM and Presence サービスのアベイラビリティを受信し、インスタントメッセージ（IM）サービスを受けられるようにするには、Cisco Unified Communications Managerを使用して、エンド ユーザをIM and Presence サービスサーバ ノードおよびクラスタに割り当てます。

エンドポイントとのユーザの関連付けに関する制限事項

表 *67 :* エンドポイント関連の制約があるユーザー

制限事項	説明
エンドユーザ情報の変更	LDAP サーバとの同期が使用可能でない場合に限り、エンド ユーザ情報を変更できます。LDAP サーバとの同期が使用可能であるかどうかを調べるには、**システム** > **LDAP** > **LDAP システム** を選択します。

第 VII 部

アプリケーションの統合

第 48 章

アプリケーションの統合の概要

アプリケーション統合の概要

このパートの各章では、アプリケーションを統合することによってシステムの機能を拡張する方法について説明します。ボイスメール、連絡先センターの機能、リッチ会議、または機能などのさまざまな機能を追加して、システムの状態を監視することができます。Cisco Unified Real-Time Monitoring Tool など、一部のアプリケーションはシステムに組み込まれ管理インターフェイスからダウンロードできます。Cisco Jabber や Cisco Unified Contact Center Express などの他のアプリケーションは、外部システムであり、Unified Communications Manager と相互運用するように設定できます。

アプリケーションの統合

次のタスク フローを実行すると、システムの統合アプリケーションを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	アプリケーション サーバのタスク フロー （513 ページ）	アプリケーション サーバを設定して他の製品サーバをクラスタに追加し、その間のセキュアな動作を確立します。
ステップ 2	プラグインのインストールのタスク フロー （518 ページ）	システムの機能を拡張するには、アプリケーション プラグインを使用します。
ステップ 3	プレゼンス冗長グループのタスク フロー （522 ページ）	同じクラスタからの 2 つの IM and Presence Service ノードで設定されているプレゼンス冗長グループを設定します。このグループは、IM and Presence Service

アプリケーションの統合

	コマンドまたはアクション	目的
		クライアントとアプリケーションの冗長性とリカバリの両方を提供します。
ステップ 4	Cisco Unity Connection （545 ページ）	ユーザにボイスメールとメッセージング機能を提供できるように、システムに Cisco Unity Connection を統合します。
ステップ 5	Cisco Unified Contact Center Enterprise （549 ページ）	高度な分散コンタクト センターを導入するように Cisco Unified Contact Center Enterprise（Unified CCE）を設定します。Unified CCE は、インテリジェント コール ルーティング、ネットワーク対デスクトップのコンピュータ テレフォニー インテグレーション（CTI）、マルチチャネル コンタクト管理を、IP ネットワークを介してコンタクト センターのエージェントに提供します。
ステップ 6	Cisco Unified Contact Center Express （551 ページ）	Cisco Unified Contact Center Express（Unified CCX）を設定して、単一またはデュアル サーバ導入にパッケージされた大規模なコンタクト センターの機能を提供します。
ステップ 7	CTI アプリケーションの設定タスクフロー （556 ページ）	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、電話の発信、受信、管理をすると同時に、コンピュータ処理機能を活用します。CTI アプリケーションを使用すると、発信者 ID に基づいてデータベースから顧客情報を取得したり、顧客の発信を適切なカスタマー サービス担当者に顧客情報と併せて渡すために自動音声応答（IVR）システムによって収集された情報を操作したりといったタスクを実行できます。
ステップ 8	Cisco TelePresence （565 ページ）	システムに TelePresence 機能を統合します。Unified Communications Manager が主なコール処理エージェントである場合は、Cisco Video Communications Server（VCS）を追加すると、H.323 のエンドポイントとのフル機能の相互運用性、サードパーティ製ビデオ エンドポイントとの SIP 統合インターワーキング、会議の代替ソリューションを提供できま

	コマンドまたはアクション	目的
		す。使用しているシステムまたは Cisco VCS と関連して動作する Cisco TelePresence Conductor を追加して、会議とマルチポイント デバイスを簡素化することもできます。TelePresence Conductor は、アドホック、ランデブー、スケジュールの複数の会議ブリッジ（Cisco MCU および TelePresence サーバ）を管理できます。
ステップ 9	Cisco Jabber の設定 （567 ページ）	Unified Communications アプリケーション スイートの 1 つである Cisco Jabber を設定すると、ユーザは、どこからでも担当者とシームレスに対話できます。このスイートは、さまざまなプラットフォームで IM、応答可能性、オーディオとビデオ発信、ボイスメールと会議を行えるようにします。

アプリケーションの統合

第 49 章

アプリケーション サーバの設定

アプリケーション サーバの概要

アプリケーションサーバ機能を使用して、Cisco Unified Communications Manager と、cisco Unity Connection、Cisco 緊急応答などの外部アプリケーション間の関連付けを維持します。アプリケーションサーバは、Cisco Unified Communications Manager と Cisco WebDialer などのアプリケーションの間でも情報を同期します。

アプリケーション サーバの要件

Cisco UnityとCisco Unity Connection の場合、AXL Web Service が Cisco UnityとCisco Unity Connection サーバと通信するように構成されている Cisco Unified Communications Manager ノードで実行されていることを確認してください。

アプリケーション サーバのタスク フロー

設定するアプリケーションサーバのタイプに応じて、次のいずれか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
ステップ 1	アプリケーション サーバの設定 （514 ページ）	クラスタ内で安全に参加し、相互運用し、その情報を共有するアプリケーションサーバを設定します。

	コマンドまたはアクション	目的
ステップ 2	Cisco WebDialer サーバの設定 （515 ページ）	[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。

アプリケーション サーバの設定

クラスタ内で安全に参加し、相互運用し、その情報を共有するアプリケーションサーバを設定します。

手順

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [**アプリケーションサーバタイプ** (Application Server)] ドロップダウンリストで、次のいずれかのサーバオプションを選択します。

- **Cisco Unityボイスメール4.x以上**
- **Cisco Unity Connection**
- **CUMA構成サーバ**
- **CERロケーション管理**
- **リモート システム ログ サーバ**

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [アプリケーション サーバの設定（Application Server 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。

ステップ 6 [保存（Save）] をクリックします。

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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

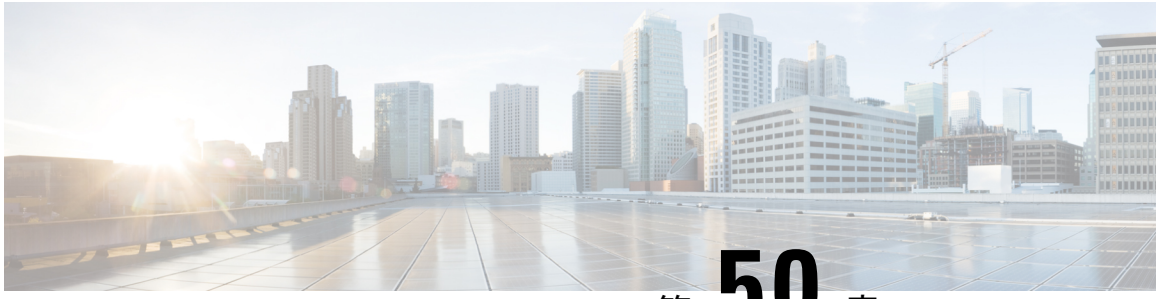
[<なし>（< None >）] の場合は、WebDialer サーバがすべてのノードに適用されることを示します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 9 [再起動（Restart）] をクリックします。



第 50 章

プラグインのインストール

プラグインの概要

アプリケーション プラグインにより、お使いのシステムの機能を拡張できます。

[アプリケーション（Application）] > **[プラグイン（Plugins）]** メニューから、次のプラグインを使用できます。

- Cisco AXL Toolkit：このプラグインにより、開発者はパブリッシャ ノード上のプロビジョニング オブジェクトを作成、読み取り、更新、削除するアプリケーションを作成できます。zip ファイルには、SOAP を使用して HTTP/HTTPS で AXL 要求および応答を送受信する Java ベースのライブラリが含まれています。
- Cisco JTAPI クライアント：Java プログラミング言語で作成された通信対応アプリケーションの標準プログラミング インターフェイスを提供します。
- Cisco TAPI クライアント：Microsoft Windows で実行される通信対応アプリケーションの標準プログラミング インターフェイスを提供します。
- Cisco Tool for Auto-Registered Phone Support（TAPS）：ユーザがリモートで事前設定済みの電話設定を電話機にダウンロードし、デバイスをプロビジョニングできるようにします。
- Cisco Unified CM Assistant Console：アシスタントがマネージャのコールをより効率的に処理できるようにします。Assistant Console は、Cisco Unified Communications Manager IP Manager Assistant（IPMA）に接続してログインおよびディレクトリ サービスに対応します。
- Cisco Unified Real-Time Monitoring Tool：デバイスのステータス、システム パフォーマンス、デバイス検出、およびクラスタで実行中の CTI アプリケーションをリアルタイムでモニタします。また、RTMT はデバイスに直接接続してトラブルシューティングを支援します。

プラグインのインストールのタスク フロー

必要に応じて、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
ステップ 1	プラグインのダウンロード （518 ページ）	プラグインをダウンロードしてから、実行可能ファイルまたはZIP ファイルからインストール手順を実行します。システムをアップグレードした後は、すべてのプラグインを再インストールする必要があります。
ステップ 2	（任意） プラグイン URL の更新 （519 ページ）	ドメインネームサーバ (DNS) が変更された場合は、プラグインUrlを更新します。システムのインストール時に、DNSによってプラグイン URL の基礎が提供されます。DNSが変更された場合、URLは自動的に更新されません。

プラグインのダウンロード

プラグインをダウンロードしてから、実行可能ファイルまたはZIP ファイルからインストール手順を実行します。システムをアップグレードした後は、すべてのプラグインを再インストールする必要があります。

始める前に

プラグインがインストールされているサーバで実行するすべての侵入検知サービスまたはウイルス対策サービスを一時的に無効にします。

手順

ステップ 1 Cisco Unified CM Administration から、**[アプリケーション（Application）] > [プラグイン（Plugins）]** を選択します。

ステップ 2 検索条件を入力するか、またはダイアログボックスを空白**のままにして [検索 (Find)] をクリックします**。

表示されるウィンドウには、アプリケーションプラグインに関する詳細情報が含まれています。

ステップ 3 **ダウンロード**をクリックして、ダウンロードとインストールするプラグインを取得します。

[**ダウンロード (Download)**] を右**クリックし**、[名前を付けて保存 (Save As)] をクリックして、検索しやすいフォルダーを選択することもできます。

ステップ 4 （任意） プラグインが ZIP ファイルの場合は、組み込みまたはサードパーティの zip プログラムを使用してこのファイルを解凍します。

ステップ 5 実行可能ファイルを実行するか、必要に応じて、ZIP ファイルに含まれている readme ファイルを参照します。

次のタスク

実行可能ファイルの指示に従ってプラグインをインストールします。

プラグイン URL の更新

ドメインネームサーバ (DNS) が変更された場合は、プラグイン Url を更新します。システムのインストール時に、DNS によってプラグイン URL の基礎が提供されます。DNSが変更された場合、URLは自動的に更新されません。

手順

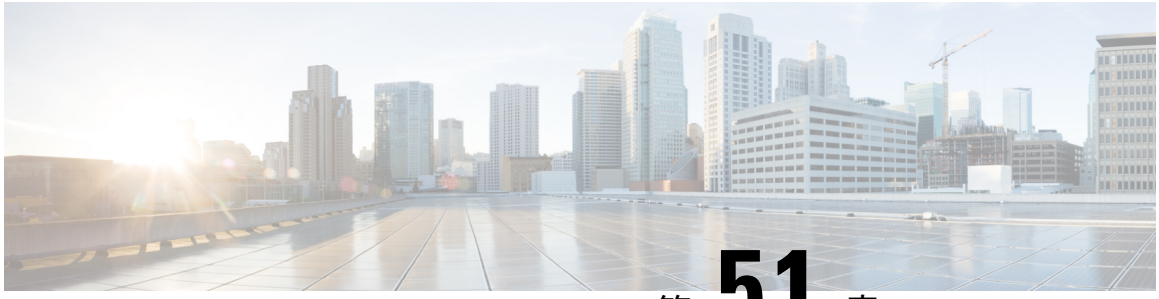
ステップ 1 Cisco Unified CM Administration から、**[アプリケーション（Application）]** > **[プラグイン（Plugins）]** を選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 更新するプラグイン名をクリックします。

ステップ 4 [**カスタム url (** Custom url)] フィールドに、プラグイン用に更新された url を入力します。

ステップ 5 [保存（Save）] をクリックします。



第 51 章

プレゼンス冗長グループの設定

プレゼンス冗長グループの概要

プレゼンス冗長グループは、同じクラスタからの 2 つの IM and Presence Service ノードで設定されています。プレゼンス冗長グループ内の各ノードは、ピア ノードのステータスまたはハートビートをモニタします。プレゼンス冗長グループを設定して、IM ane Presence サービスのクライアントとアプリケーションの両方の冗長性と回復を提供することができます。

- フェールオーバー：プレゼンス冗長グループ内の IM and Presence サービス ノード上で 1 つ以上の重要なサービスが失敗した場合、またはグループ内のノードが失敗した場合、プレゼンス冗長グループ内で行われます。クライアントは、そのグループ内のもう 1 つの IM and Presence サービス ノードに自動的に接続します。
- フォールバック：以下のいずれかの状況で、フォールバック コマンドが CLI またはCisco Unified Communications Manager から発行されると行われます。
  - 失敗した IM and Presence サービス ノードがサービスを再開し、すべての重要なサービスが動作している場合。サービスが再開されると、グループ内のフェールオーバーしていたクライアントは回復したノードに再接続されます。
  - 重要なサービスの不具合のために、アクティブ化されていたバックアップ IM and Presence サービス ノードが失敗し、ピア ノードがフェールオーバー状態であり、自動回復フォールバックをサポートしている場合。

たとえば、ローカルの IMとプレゼンスサービスノードのサービスまたはハードウェアで障害が発生した場合、Cisco Jabber クライアントは、プレゼンス冗長グループを使用してバックアッ

プ用 IMとプレゼンスサービス ノードにフェールオーバーします。障害が発生したノードが再びオンラインになると、自動フォールバックを構成すると、クライアントは自動的にローカルのIMとプレゼンスサービスノードに再接続されます。自動フォールバックを設定していない場合は、失敗したノードがオンラインになったときに、手動でフォールバックを開始できます。

プレゼンス冗長性グループでは、冗長性と回復だけでなく、クラスタの高可用性を設定することもできます。

高可用性

IMとプレセンスサービスは、マルチノード導入の高可用性をサポートしています。

プレゼンス冗長グループを設定した後は、そのグループの高可用性を有効にすることができます。高可用性を実現するには、ペアのノードが必要です。各ノードには、独立型のデータベースと一連のユーザが存在し、これらは、共通のユーザをサポートできる共有アベイラビリティデータベースとともに運用されます。

すべてのIMとプレゼンスサービスノードが、プレゼンス冗長グループに属している必要があります。このグループは、単一の IMとプレゼンスサービスノード、またはペアのIMとプレゼンスサービスノードで構成されている場合があります。

高可用性を設定するには、次の 2 つの異なるモードを使用します。

- バランスモード: このモードでは、自動ユーザロードバランシング機能と、コンポーネントの障害や停電が原因で障害が発生した場合のユーザフェイルオーバー機能を備えた、冗長高可用性を提供します。
- プライマリスペアモード:プライマリノードに障害が発生した場合、スタンバイノードは自動的にプライマリノードを引き継ぎます。自動ロードバランシング機能は提供しません。

IMとプレゼンスサービの導入を高可用性の導入として設定することをお勧めします。シングル導入で高可用性と非高可用性状態の冗長グループを同時に構成することは可能ですが、この構成は推奨されません。

プレゼンス冗長グループの要件

WANを使用した配置の場合、各IMとプレゼンスサービス クラスタに対して最低 10 メガビット/秒の専用帯域幅と、80ミリ秒以下のラウンドトリップ遅延が必要です。この推奨帯域幅よりも小さい帯域幅では、パフォーマンスに悪い影響を及ぼす可能性があります。

プレゼンス冗長グループのタスク フロー

1 つの IM and Presence Service ノードは、1 つのプレゼンス冗長グループのみに割り当てることができます。高可用性を実現するには、同じクラスタから 2 つのノードをプレゼンス冗長グループに割り当て、グループの高可用性を確保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
ステップ 1	データベースのレプリケーションの確認（523 ページ）	データベース レプリケーションが IM and Presence サービス クラスタで設定されていることを確認します。
ステップ 2	サービスの確認 （524 ページ）	重要なサービスがプレゼンス冗長グループに追加予定のノード上で実行されていることを確認します。
ステップ 3	プレゼンス冗長グループの設定 （525 ページ）	IM and Presence Service クライアントとアプリケーションの冗長性とリカバリを提供します。
ステップ 4	フェール オーバーのハートビート間隔の設定 （526 ページ）	（省略可）プレゼンス冗長グループ内の各ノードは、ピア ノードのステータスまたはハートビートをモニタします。各ノードがピアをモニタする間隔を設定できます。
ステップ 5	高可用性の有効化 （527 ページ）	（省略可）プレゼンス冗長グループを設定したときに高可用性を有効にしなかった場合は、この手順を実行します。
ステップ 6	ユーザ割り当てモードの設定 （528 ページ）	Sync Agent が IM and Presence サービス クラスタのさまざまなノード全体にユーザを分散する方法を設定します。この設定は、システムがフェールオーバーと負荷分散を処理する方法に影響します。

データベースのレプリケーションの確認

状態冗長グループの高可用性を有効にする前に、IMとプレゼンスサービスクラスタでデータベースレプリケーションが設定されていることを確認してください。

手順

ステップ 1 次のいずれかの方法を使用して CLI セッションを開始します。

- リモート システムの場合は、SSH を使用して Cisco Unified オペレーティング システムにセキュアに接続します。SSH クライアントで、**ssh *adminname* @ *hostname***を入力してパスワードを入力します。
- シリアル ポートへの直接接続を介して、自動的に表示されるプロンプトでクレデンシャルを入力します。

ステップ 2 **utils dbreplication status** コマンドを実行して、データベース テーブルのエラーまたは不一致を確認します。

ステップ 3 **utils dbreplication runtimestate** コマンドを実行して、ノードでデータベース レプリケーションがアクティブであることを確認します。

出力にはすべてのノードが一覧表示されます。データベース レプリケーションがセットアップされて正常であれば、各ノードの **replication setup** の値は **2** になります。

2 以外の値が返された場合は、続行する前にエラーを解決する必要があります。

次のタスク

サービスの確認 （524 ページ）

サービスの確認

重要なサービスがプレゼンス冗長グループに追加予定のノード上で実行されていることを確認します。高可用性を有効にする前に、重要なサービスを実行する必要があります。重要なサービスがいずれのノードでも動作していない場合、障害状態に高可用性をオンにするとプレゼンス冗長グループは Failed 状態になります。重要なサービスが 1 つのノードで実行されていない場合、高可用性をオンにすると、そのノードが他のノードにフェールオーバーします。

始める前に

データベースのレプリケーションの確認 （523 ページ）

手順

ステップ 1 [Cisco Unified IM and Presenceのサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、**[ツール（Tools）] > [コントロールセンター-ネットワークサービス（Control Center - Network Services）]** を選択します。

ステップ 2 [サーバ（Server）] リストから、適切なノードを選択し、[移動（Go）] をクリックします。

ステップ 3 [IM and Presence サービス（IM and Presence Services）] で、次のサービスが開始されていることを確認します。

- **Cisco Client Profile Agent**
- **Cisco Sync Agent**
- **Cisco XCP Router**

ステップ 4 [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-ネットワークサービス（Control Center - Network Services）] を選択し、[移動（Go）] をクリックします。

ステップ 5 [IM and Presence サービス（IM and Presence Services）] で、次のサービスが開始されていることを確認します。

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

次のタスク

プレゼンス冗長グループの設定 （525 ページ）

プレゼンス冗長グループの設定

Cisco Unified Communications Managerを使用して、IMとプレゼンスサービスノードのの冗長性を構成します。

各状態冗長グループには、2つのIMとプレゼンスサービスノードを含めることができます。各ノードは、1つのプレゼンス冗長グループにのみ割り当て可能です。プレゼンス冗長グループの両方のノードが同一クラスタ上にあり、同じ IM and Presence サービス データベース パブリッシャ ノードを持つ必要があります。

始める前に

- サービスの確認 （524 ページ）
- 状態冗長グループに追加するIMとプレゼンスサービスノードが同じソフトウェアバージョンを実行していることを確認します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]**>**[プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

ステップ 2 **[新規追加]** をクリックします。

ステップ 3 ステータスが冗長なグループの一意の名前を入力します。

アンダースコア（_）とダッシュ（-）を含む最大 128 字の英数字を入力できます。

ステップ 4 グループの説明を入力します。

記号を含む最大128字の英数字を入力できますが、、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、スラッシュ（\）、山カッコ（<>）は使用できません。

ステップ 5 IM and Presence Serviceの 2 つの異なるノードを [プレゼンス サーバ（Presence Server）] フィールドで選択し、グループに割り当てます。

ステップ 6 （任意）[高可用性を有効にする（Enable High Availability）] チェックボックスをオンにして、プレゼンス冗長グループの高可用性を有効にします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

フェール オーバーのハートビート間隔の設定 （526 ページ）

フェール オーバーのハートビート間隔の設定

プレゼンス冗長グループ内の各ピアが、ピアがアクティブであることを確認するためには、ピア ノードのハートビート（ステータス）をモニタするキープ アライブ設定を決定する任意指定のサービス パラメータを設定します。フェールオーバーは、設定したタイマーの有効期限が切れた後にピア ノードが応答しなくなった場合に開始されます。

（注） シスコでは、このパラメータのデフォルト値を使用することを推奨しています。ただし、必要に応じて値を設定し直すことも可能です。

手順

ステップ 1 Cisco Unified CM IM and Presence Administration で、**システム** > **サービス パラメータ**を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストから、IM and Presence ノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウンから、**Cisco Server Recovery Manager**（**アクティブ**）を選択します。

ステップ 4 [一般的なServer Recovery Managerパラメータ（クラスタ全体）（General Server Recovery Manager Parameters (Clusterwide)）] で、プレゼンス冗長グループ内の各ノードがピア ノードのハートビートのモニタに使用する、クラスタ全体のキープアライブ設定を指定します。フェールオーバーは、ピア ノードが応答しない場合に開始することができます。

- **[サービスポート（Service Port）]**：このパラメータでは、Cisco Server Recovery Manager がピアとの通信に使用するポートを指定します。デフォルトは 22001 です。
- **[管理RPCポート（Admin RPC Port）]**：このパラメータでは、Cisco Server Recovery Manager が管理 RPC 要求を提供するために使用するポートを指定します。デフォルトは 20075 です。
- **[重要なサービス遅延（Critical Service Delay）]**：このパラメータでは、フェールオーバーが開始されるまでに重要なサービスを停止しても無視される期間を、秒単位で指定します。デフォルトは 90 です。
- **[自動フォールバックの有効化（Enable Automatic Fallback）]**：このパラメータでは、自動フォールバックを実行するかどうかを指定します。フェールオーバーが発生した場合、プライマリ ノードが正常な状態に戻った 30 分後に、IM and Presence Service がユーザをバックアップ ノードからプライマリ ノードに自動的に移動します。デフォルト値は [False] です。

- **[初期化キープアライブ（ハートビート）タイムアウト（Initialization Keep Alive (Heartbeat) Timeout）]**：このパラメータでは、フェールオーバーが開始されるまでに、初期化中にピアとの間でハートビートが喪失しても無視される期間を、秒単位で指定します。デフォルトは 120 です。
- **[キープアライブ（ハートビート）タイムアウト（Keep Alive (Heartbeat) Timeout）]**：このパラメータでは、フェールオーバーが開始されるまでに、ピアとの間でハートビートが喪失しても無視される期間を、秒単位で指定します。デフォルトは 60 です。
- **[キープアライブ（ハートビート）間隔（Keep Alive (HeartBeat) Interval）]**：このパラメータでは、ピア ノードに送信されるキープ アライブ（ハートビート）メッセージの間隔を指定します。デフォルトは 15 です。

ステップ 5 次の追加パラメータを設定して、CUPC 8.5 以降のクライアントに、再ログインを試行するまでの待機時間を指定します。前述のパラメータとは異なり、これらのパラメータは、クラスタノード毎に個別に設定する必要があります。

- **[クライアントの再ログインの下限（Client Re-Login Lower Limit）]**：このパラメータでは、CUPC 8.5 以降がこのサーバに再ログインするまでの待機時間の加減を秒単位で指定します。デフォルトは 120 です。
- **[クライアントの再ログインの上限（Client Re-Login Upper Limit）]**：このパラメータでは、CUPC 8.5 以降がこのサーバに再ログインするまでの待機時間の上限を秒単位で指定します。デフォルトは 537 です。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

プレゼンス冗長グループを設定したときに高可用性の有効化（527 ページ）を実行しなかった場合は、ここで実行します。

高可用性の有効化

注意 IM and Presence Service クラスタのレプリケーションのセットアップに失敗したが、すべての重要なサービスが実行されている場合、現在の冗長グループで有効な場合は、すぐにフェール オーバーする場合があります。

始める前に

- プレゼンス冗長グループの設定 （525 ページ）
- IM and Presence Service クラスタでレプリケーションがセットアップされていることを確認します。
- すべての重要なサービスが動作していることを確認します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]**>**[プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

ステップ 2 検索情報を指定し、[検索（Find）] をクリックします。

ステップ 3 設定したプレゼンス冗長グループを選択します。

ステップ 4 高可用性を有効にするには、[高可用性を有効にする（Enable High Availability）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

ユーザ割り当てモードの設定

この手順を使用して、同期エージェントがクラスタ内のノードにユーザーを割り当てる方法を構成します。この設定は、フェールオーバーと負荷分散を管理するのに役立ちます。

手順

ステップ 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。

ステップ 2 [ユーザ管理パラメータ（User Management Parameters）] 領域で、[プレゼンスサーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] パラメータに次のいずれかのオプションを選択します。

- [バランス（Balanced）]：このモード（デフォルト）では、ユーザを各サブクラスタのそれぞれのノードに均等に割り当て、各ノードにユーザの合計数が均等に分散するようにします。 これがデフォルトのオプションです。
- [アクティブスタンバイ（Active-Standby）]：このモードでは、サブクラスタの最初のノードにすべてのユーザを割り当て、セカンダリ サーバをバックアップのままにします。
- **[なし（None）]**：このモードでは、Sync Agent でクラスタのノードにユーザが割り当てられません。

ステップ 3 [保存（Save）] をクリックします。

冗長連携動作および制限事項

機能	連携動作
ユーザの追加	いずれかのクラスタ ノードがフェールオーバー状態である間は、IM and Presence Service クラスタに新規ユーザを追加できません。
Multiple Device Messaging	フェールオーバーが発生した場合、Multiple Device Messaging 機能により、IM and Presence サービスでサーバ回復に遅延が発生します。Multiple Device Messaging が設定されているシステムでサーバのフェールオーバーが発生すると、通常、[Cisco Server Recovery Manager] サービス パラメータで指定された時間の 2 倍かかります。

機能	連携動作
プッシュ通知の高可用性	11.5(1)SU3 では、プッシュ通知の展開で高可用性がサポートされます。プッシュ通知が有効化されており、ノードがフェールオーバーした場合、iPhone および iPad 版 Cisco Jabber クライアントで次の処理が行われます。 • フォアグラウンド モードの Cisco Jabber クライアントの場合、Jabber クライアントは、メイン ノードが回復するまでの間、自動的にバックアップ ノードにログインします。バックアップ ノードが引き継いだとき、またはメイン ノードが回復したときのいずれも、サービスは中断しません。 • バックグラウンド モードの Cisco Jabber クライアントの場合、バックアップ ノードが引き継ぎますが、プッシュ通知が送信されるまでに遅延が生じます。Jabber クライアントがバックグラウンド モードで動作しているためにアクティブなネットワーク接続がない場合、バックアップ ノードへのログインは自動的には行われません。バックアップ ノードがプッシュ通知を送信できるようになるには、バックグラウンド モードになっていたすべてのフェールオーバー ユーザ向けに JSM セッションを再作成する必要があります。 遅延の長さは、システムの負荷によって異なります。テストでは、ユーザが HA ペアに均等に分散されている 15,000 ユーザ OVA の場合、フェールオーバー後のプッシュ通知の送信までに 10 ～ 20 分かかることが明らかになっています。この遅延は、バックアップ ノードが引き継いだとき、およびメイン ノードが回復した後に、確認することができます。 （注） ノード障害または予期しない Cisco XCP Router のクラッシュの場合、IM 履歴を含むユーザの IM セッションは、ユーザ アクションを必要とすることなく維持されます。ただし、Cisco Jabber on iPhone または iPad のクライアントが保留モードであった場合、サーバのクラッシュ時にサーバ上にキューされていた未開封メッセージを取得することはできません。

機能	連携動作
ユーザの一時的なプレゼンス ステータス	ユーザの一時的なプレゼンス ステータスで、フェールオーバー、フォールバック、およびユーザの移動の後に、古いプレゼンス ステータスが表示されます。これは、一時的なプレゼンスに対するサブスクリプションが削除されたためであり、ユーザの有効な一時的プレゼンス ステータスを表示するためには、ユーザが一時的なプレゼンスに登録し直す必要があります。 たとえば、ユーザ A がユーザ B の一時的なプレゼンスに登録されており、ユーザ B が割り当てられている IM and Presence ノードでフェールオーバーが発生した場合、ユーザ B がバックアップ ノードに再ログインした後でも、ユーザ B はユーザ A に対してオフラインと表示されます。これは、ユーザ B の一時的なプレゼンスに対するサブスクリプションが削除され、ユーザ A が削除を認識していないためです。ユーザ A は、ユーザ B の一時的な存在を再度サブスクライブする必要があります。 ユーザ A が Jabber クライアントから User B の検索を削除すると、ユーザ B の一時的なプレゼンスの検索を試みるまでに、ユーザ A は少なくとも 30 秒待つ必要があります。一致しない場合、ユーザ A にはユーザ B の古いプレゼンスが表示されします。Jabber クライアントは、有効な一時プレゼンス ステータスを取得するために、同じユーザに対する 2 回の検索の間で少なくとも 30 秒待つ必要があります。

手動によるフェールオーバー、フォールバック、リカバリ

Cisco Unified Communications Manager Administrationを使用して、プレゼンス冗長グループの IM and Presence Service ノードの手動フェールオーバー、手動フォールバック、手動リカバリを開始します。CLI を使用して Cisco Unified Communications Manager または IM and Presence Service からこれらのアクションを開始することもできます。詳細については、『*Cisco Unified Communications* ソリューション コマンドライン インターフェイス ガイド』を参照してください。

- 手動フェールオーバー：手動フェールオーバーを開始すると、Cisco Server Recovery Manager は失敗したノードの重要なサービスを停止します。失敗したノードのすべてのユーザが切断されるので、バックアップ ノードに再ログインする必要があります。

（注） 手動フェイルオーバーの後、手動ロールバックを呼び出すまで、重要なサービスは再起動されません。

- 手動フォールバック：手動フォールバックを開始すると、Cisco Server Recovery Manager はプライマリ ノード上の重要なサービスを再起動し、フェールオーバーされていたすべてのユーザを切断します。切断されたユーザは、割り当てられたノードに再ログインする必要があります。
- 手動リカバリ：プレゼンス冗長グループの両方のノードが失敗状態になって手動リカバリを起動すると、IM and Presence サービス がプレゼンス冗長グループの両方のノードの Cisco Server Recovery Manager サービスを再起動します。

手動フェールオーバーの開始

Cisco Unified Communications Manager Administration を使用して、プレゼンス冗長グループ内の IM and Presence Service ノードのフェールオーバーを手動で開始できます。

手順

ステップ 1 **[システム（System）]** > **[プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

[プレゼンス冗長グループの検索と一覧表示（Find and List Presence Redundancy Groups）] ウィンドウが表示されます。

ステップ 2 プレゼンス冗長グループの検索パラメータを選択して、[検索（Find）] をクリックします。

一致するレコードが表示されます。

ステップ 3 [プレゼンス冗長グループの検索と一覧表示（Find and List Presence Redundancy Groups）] ウィンドウにリストされたプレゼンス冗長グループを選択します。

[Presence Redundancy Group Configuration（プレゼンス冗長グループの設定）] ウィンドウが表示されます。

ステップ 4 [サーバアクション（ServerAction）] フィールドで、[フェールオーバー（Failover）] をクリックします。

（注） このボタンは、サーバとプレゼンス冗長グループが正常な状態である場合にのみ表示されます。

手動フォールバックの開始

Cisco Unified Communications Manager 管理 を使用して、フェールオーバーしたプレゼンス冗長グループの IM and Presence サービス ノードのフォールバックを手動で実行します。プレゼンス冗長グループ ノードのステータスの詳細については、ノードの状態、状態変更の原因、推奨処置に関するトピックを参照してください。

手順

ステップ 1 **[システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

[プレゼンス冗長グループの検索と一覧表示（Find and List Presence Redundancy Groups）] ウィンドウが表示されます。

ステップ 2 プレゼンス冗長グループの検索パラメータを選択して、[検索（Find）] をクリックします。

一致するレコードが表示されます。

ステップ 3 [プレゼンス冗長グループの検索と一覧表示（Find and List Presence Redundancy Groups）] ウィンドウにリストされたプレゼンス冗長グループを選択します。

[Presence Redundancy Group Configuration（プレゼンス冗長グループの設定）] ウィンドウが表示されます。

ステップ 4 [サーバアクション（ServerAction）] フィールドで、[フォールバック（Fallback）] をクリックします。

（注） このボタンは、サーバとプレゼンス冗長グループが正常な状態である場合にのみ表示されます。

手動リカバリの開始

手動リカバリは、プレゼンス冗長グループ内の両方のノードで障害が発生した状態の場合に必要となります。障害が発生した状態にあるプレゼンス冗長グループ内の IM and Presence Service ノードのリカバリを手動で開始するには、Cisco Unified Communications Manager Administration を使用します。

プレゼンス冗長グループ ノードのステータスの詳細については、ノードの状態、状態変更の原因、推奨処置に関するトピックを参照してください。

始める前に

手動リカバリは、プレゼンス冗長グループ内の両方のノードで障害が発生した状態の場合に必要となります。障害が発生した状態にあるプレゼンス冗長グループ内の IM and Presence Service

ノードのリカバリを手動で開始するには、Cisco Unified Communications Manager Administration を使用します。

手順

ステップ 1 **[システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

[プレゼンス冗長グループの検索と一覧表示（Find and List Presence Redundancy Groups）] ウィンドウが表示されます。

ステップ 2 プレゼンス冗長グループの検索パラメータを選択して、[検索（Find）] をクリックします。

一致するレコードが表示されます。

ステップ 3 [プレゼンス冗長グループの検索と一覧表示（Find and List Presence Redundancy Groups）] ウィンドウにリストされたプレゼンス冗長グループを選択します。

[Presence Redundancy Group Configuration（プレゼンス冗長グループの設定）] ウィンドウが表示されます。

ステップ 4 **[回復(Recover)]** をクリックします。

（注） このボタンは、サーバとプレゼンス冗長グループが正常な状態である場合にのみ表示されます。

ノード状態の定義

表 *68 :* プレゼンス冗長グループのノード状態の定義

状態	説明
初期化中（Initializing）	Cisco Server Recovery Manager サービスが開始した際の一時的な初期（遷移）状態です。
アイドル（Idle）	フェールオーバーが発生してサービスが停止すると、IM and Presence サービスはアイドル状態になります。アイドル状態では、IM and Presence Service ノードは可用性サービスやインスタント メッセージ サービスを提供しません。[Cisco Unified CMの管理（Cisco Unified CM Administration）]ユーザインターフェイスを使用して、このノードへのフォールバックを手動で開始できます。

状態	説明
正常（Normal）	安定した状態です。IM and Presence Service が正常に稼働しています。この状態では、[Cisco Unified CMの管理（Cisco Unified CM Administration）] ユーザ インターフェイスを使用して、このノードへのフェールオーバーを手動で開始できます。
バックアップモードで実行中（Running in Backup Mode）	安定した状態です。IM and Presence サービス ノードは、ピア ノードのバックアップとして機能中です。ユーザはこの（バックアップ）ノードに移動されました。
テイク オーバー中（Taking Over）	遷移状態です。IM and Presence サービス ノードは、ピア ノードのテイクオーバー中です。
フェールオーバー中（Failing Over）	遷移状態です。IM and Presence サービス ノードは、ピア ノードによってテイクオーバーされています。
フェールオーバー済み（Failed Over）	安定した状態です。IM and Presence Service ノードがフェールオーバーしましたが、重要なサービスはダウンしていません。この状態では、[Cisco Unified CMの管理（Cisco Unified CM Administration）] ユーザ インターフェイスを使用して、このノードへのフォールバックを手動で開始できます。
フェールオーバー済み（重要なサービスは非実行）（Failed Over with Critical Services Not Running）	安定した状態です。IM and Presence Service ノード上の一部の重要なサービスが停止または失敗しました。
フォールバック中（Falling Back）	遷移状態です。システムは、バックアップ モードで実行中のノードから、この IM and Presence サービス ノードにフォールバック中です。
テイク バック中（Taking Back）	遷移状態です。障害が発生した IM and Presence Service ノードが、ピアから引き継ぎ直します。
障害モードで実行中（Running in Failed Mode）	遷移状態または [バックアップモードで実行中（Running in Backup Mode）] 状態のときにエラーが発生しました。
不明（Unknown）	ノード状態は不明です。 考えられる原因は、IM and Presence Service ノードで高可用性が適切に有効化されていないことです。プレゼンス冗長グループの両方のノードで、Server Recovery Manager サービスを再起動します。

ノードの状態、原因、および推奨するアクション

[Cisco Unified CMの管理(Cisco Unified CM Administration)] ユーザ インターフェイスを使用してグループを選択する場合、[プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウのプレゼンス冗長グループでノードのステータスを表示できます。

表 *69 :* プレゼンス冗長グループ ノードの高可用性状態、原因、および推奨されるアクション

ノード 1		ノード 2		
状態	理由	状態	理由	原因/推奨するアクション
正常（Normal）	正常（Normal）	正常（Normal）	正常（Normal）	正常（Normal）
フェールオーバー中（Failing Over）	管理者の要求による	テイクオーバー中（Taking Over）	管理者の要求による	管理者がノード1からノード2への手動フェールオーバーを開始しました。手動フェールオーバーの処理中です。
アイドル（Idle）	管理者の要求による	バックアップモードで実行中（Running in Backup Mode）	管理者の要求による	管理者が開始したノード 1 からノード 2 への手動フェールオーバーが完了しました。
テイクバック中（Taking Back）	管理者の要求による	フォールバック中（Falling Back）	管理者の要求による	管理者がノード2からノード1への手動フォールバックを開始しました。手動フォールバックの処理中です。
アイドル（Idle）	初期化	バックアップモードで実行中（Running in Backup Mode）	管理者の要求による	ノード1が「アイドル」状態のとき、管理者がノード1上でSRMサービスを再起動しました。

ノード1		ノード2		
状態	理由	状態	理由	原因/推奨するアクション
アイドル（Idle）	初期化	バックアップモードで実行中（Running in Backup Mode）	初期化	プレゼンス冗長グループの手動フェールオーバー モードのとき、管理者がプレゼンス冗長グループの両方のノードを再起動したか、両方のノードの SRM サービスを再起動しました。
アイドル（Idle）	管理者の要求による	バックアップモードで実行中（Running in Backup Mode）	初期化	ノード 2 がバックアップ モードで実行しているとき、ノード 1 のハートビートのタイムアウト前に、管理者がノード 2 の SRM サービスを再起動しました。
フェールオーバー中（Failing Over）	管理者の要求による	テイクオーバー中（Taking Over）	初期化	ノード 2 のテイクオーバー中、ノード 1 のハートビートのタイムアウト前に、管理者がノード 2 の SRM サービスを再起動しました。
テイクバック中（Taking Back）	初期化	フォールバック中（Falling Back）	管理者の要求による	ノード 1 のテイクバック中、ノード 2 のハートビートのタイムアウト前に、管理者がノード 1 の SRM サービスを再起動しました。テイクバック プロセスの完了後、両方のノードは「通常」状態になります。
テイクバック中（Taking Back）	自動フォールバック	フォールバック中（Falling Back）	自動フォールバック	ノード 2 からノード 1 への自動フォールバックが開始され、現在処理中です。

ノード1		ノード2		
状態	理由	状態	理由	原因/推奨するアクション
フェールオーバー済み（Failed Over）	初期化または重要なサービスのダウン	バックアップモードで実行中（Running in Backup Mode）	重要なサービスのダウン	次のいずれかの条件が発生すると、ノード1は「フェールオーバー完了」状態に遷移します。 • ノード1のリブートにより、重要なサービスの状態が元に戻る。 • ノード1が「重要サービスを実行せずにフェールオーバー完了」状態のとき、管理者がノード1で重要なサービスを開始する。 ノード1が「フェールオーバー完了」状態に遷移する際、プレゼンス冗長グループのノードを「通常」状態へ復元するために、管理者がノード1を手動フォールバックできる状態にある。
重要サービスを実行せずにフェールオーバー完了	重要なサービスのダウン	バックアップモードで実行中（Running in Backup Mode）	重要なサービスのダウン	ノード1で重要なサービスがダウンしました。IM and Presence サービスが、ノード2への自動フェールオーバーを実行します。 **推奨するアクション**： **1.** ノード1でダウンしている重要なサービスを確認し、手動でそのサービスの開始を試みます。 **2.** ノード1の重要なサービスが開始しない場合は、ノード1をリブートします。 **3.** リブート後にすべての重要なサービスが稼働中である場合、手動でフォールバックを実行して、プレゼンス冗長グループのノードを [Normal（正常）] 状態に復元します。

ノード1		ノード2		
状態	理由	状態	理由	原因/推奨するアクション
重要サービスを実行せずにフェールオーバー完了	データベース障害	バックアップモードで実行中（Running in Backup Mode）	データベース障害	ノード 1 のデータベース サービスがダウンしました。IM and Presence サービスが、ノード 2 への自動フェールオーバーを実行します。 **推奨するアクション**： **1.** ノード 1 をリブートします。 **2.** リブート後にすべての重要なサービスが稼働中である場合、手動でフォールバックを実行して、プレゼンス冗長グループのノードを [Normal（正常）] 状態に復元します。
障害モードで実行中（Running in Failed Mode）	重要なサービスの開始に失敗	障害モードで実行中（Running in Failed Mode）	重要なサービスの開始に失敗	他のノードからプレゼンス冗長グループのノードへのテイクバック中は、重要なサービスを開始できません。 **推奨処置。**テイクバック中のノードで、次の操作を実行します。 **1.** ノードにダウンしている重要なサービスがないかどうかを確認します。これらのサービスを手動で開始するには、[プレゼンス冗長グループの設定）Presence Redundancy Group Configuration）] ウィンドウの [回復（Recovery）] をクリックします。 **2.** 重要なサービスが開始されない場合は、ノードをリブートします。 **3.** リブート後にすべての重要なサービスが稼働中である場合、手動でフォールバックを実行して、プレゼンス冗長グループのノードを [Normal（正常）] 状態に復元します。

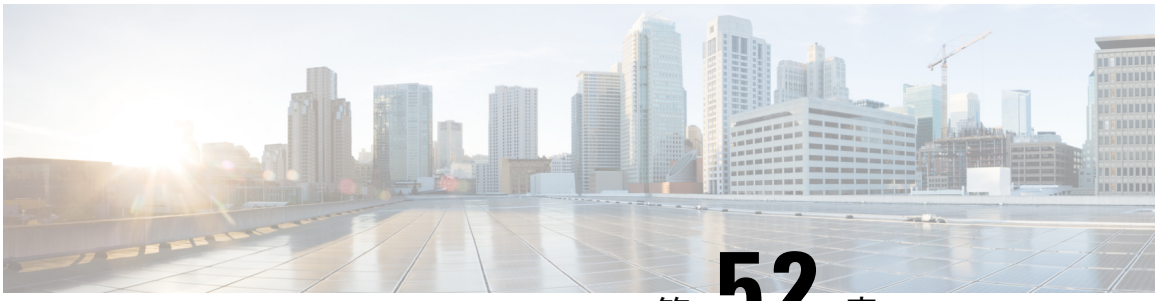
ノード 1		ノード 2		
状態	理由	状態	理由	原因/推奨するアクション
障害モードで実行中（Running in Failed Mode）	重要なサービスのダウン	障害モードで実行中（Running in Failed Mode）	重要なサービスのダウン	バックアップ ノードで重要なサービスがダウンしました。両方のノードが障害状態になります。 **推奨するアクション**： **1.** バックアップ ノードにダウンしている重要なサービスがないかどうかを確認します。これらのサービスを手動で開始するには、[プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウで [回復（Recovery）] をクリックします。 **2.** 重要なサービスが開始されない場合は、ノードをリブートします。

ノード1		ノード2		
状態	理由	状態	理由	原因/推奨するアクション
ネットワーク接続が喪失しているか、SRM サービスが実行されていないために、ノード 1 がダウンしました。		バックアップ モードで実行中（Running in Backup Mode）	ピア ダウン	ノード 2 がノード 1 からのハードビートを失いました。IM and Presence サービスが、ノード2への自動フェールオーバーを実行します。 **推奨するアクション**：ノード1が起動したら、次の操作を実行します。 **1.** プレゼンス冗長グループのノード間のネットワーク接続を確認して修復します。ノード間のネットワーク接続を再確立すると、ノードが失敗状態になる場合があります。正常の状態にノードを復元するには、[プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウの [回復（Recovery）] をクリックします。 **2.** 正常（Normal）状態にプレゼンス冗長グループのノードをリストアするために、SRMサービスを開始し、手動フォールバックを実行します。 **3.** （ノードがダウンしている場合）ノード 1 を修復して電源を入れます。 **4.** ノードが起動中で、すべての重要なサービスが稼働中である場合、手動でフォールバックを実行してプレゼンス冗長グループのノードを [正常（Normal）] 状態に復元します。

ノード1		ノード2		
状態	理由	状態	理由	原因/推奨するアクション
（電源切断、ハードウェア障害、シャットダウン、リブートなどにより）ノード1がダウンしました。		バックアップモードで実行中（Running in Backup Mode）	ピア リブート	ノード1で次のような条件が発生したため、IM and Presence サービスがノード2への自動フェールオーバーを実行しました。 • ハードウェア障害 • 電源切断 • 再起動 • シャットダウン **推奨するアクション**： **1.** ノード1を修復して電源を入れます。 **2.** ノードが起動中で、すべての重要なサービスが稼働中である場合、手動でフォールバックを実行してプレゼンス冗長グループのノードを [正常（Normal）] 状態に復元します。
重要サービスを実行せずにフェールオーバー完了、またはフェールオーバー完了	初期化	バックアップモード	初期化中のピア ダウン	起動中、ノード2はノード1を参照しません。 **推奨するアクション**： ノード1が起動してすべての重要なサービスが実行されたら、手動フォールバックを実行してプレゼンス冗長グループのノードを「通常」状態に復元します。
障害モードで実行中（Running in Failed Mode）	Cisco Server Recovery Manager がユーザのテイクオーバーに失敗	障害モードで実行中（Running in Failed Mode）	Cisco Server Recovery Manager がユーザのテイクオーバーに失敗	テイクオーバー プロセス中にユーザを移動することはできません。 **推奨するアクション**： データベースエラーの可能性があります。[プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウの [回復（Recovery）] をクリックします。問題が解決しない場合は、ノードをリブートします。

ノード1		ノード2		
状態	理由	状態	理由	原因/推奨するアクション
障害モードで実行中（Running in Failed Mode）	Cisco Server Recovery Manager がユーザのテイクバックに失敗	障害モードで実行中（Running in Failed Mode）	Cisco Server Recovery Manager がユーザのテイクバックに失敗	フォールバック プロセス中にユーザを移動することはできません。 **推奨するアクション**： データベース エラーの可能性があります。[プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウの [回復（Recovery）] をクリックします。問題が解決しない場合は、ノードをリブートします。
障害モードで実行中（Running in Failed Mode）	不明（Unknown）	障害モードで実行中（Running in Failed Mode）	不明（Unknown）	他のノードが失敗状態であるか、内部システム エラーの発生中に、ノードの SRM が再起動しました。 **推奨するアクション**： [プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウの [回復（Recovery）] をクリックします。問題が解決しない場合は、ノードをリブートします。
バックアップのアクティブ化	データベースの自動リカバリに失敗	フェールオーバーがサービスに影響	データベースの自動リカバリに失敗	バックアップ ノードでデータベースがダウンしました。ピア ノードはフェールオーバー モードであり、プレゼンス冗長グループのすべてのユーザをテイクオーバーできます。自動リカバリ操作が自動的に開始され、すべてのユーザはプライマリ ノードに移動します。
バックアップのアクティブ化	データベースの自動リカバリに失敗	フェールオーバーがサービスに影響	重要サービスのダウンの自動リカバリ	バックアップ ノードで重要なサービスがダウンしました。ピア ノードはフェールオーバー モードであり、プレゼンス冗長グループのすべてのユーザをテイクオーバーできます。自動リカバリ操作が自動的に開始され、すべてのユーザはピア ノードに移動します。

ノード 1		ノード 2		
状態	理由	状態	理由	原因/推奨するアクション
不明（Unknown）		不明（Unknown）		ノード状態は不明です。 考えられる原因は、IM and Presence Service ノードで高可用性が適切に有効化されていないことです。 **推奨するアクション**： プレゼンス冗長グループの両方のノードで、Server Recovery Manager サービスを再起動します。



第 52 章

ボイスメールとメッセージング用の Cisco Unity Connection の設定

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。

ボイスメールおよびメッセージング用の Cisco Unity Connection 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
ステップ 1	Cisco Unity Connection で、ボイスメールとメッセージングを設定します。	Cisco Unity Connection の設定については、次の場所にある『*Cisco Unified Communications Manager SCCP* インテグレーション ガイド for Cisco Unity Connection』または『*Cisco Unified Communications Manager SIP* トランク インテグレーション ガイド *for Cisco Unity Connection*』を参照してください。 http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html
ステップ 2	PIN同期の有効化 （547 ページ）	（省略可）共通の PIN 同期を有効にするには、次の手順を使用します。

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

ステップ 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。

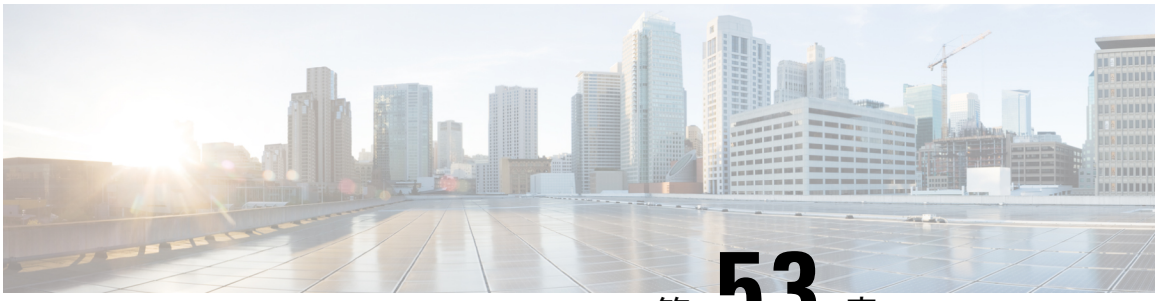
ステップ 2 Cisco Unity Connectionをセットアップするアプリケーション サーバを選択します。

ステップ 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。

ステップ 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 （514 ページ）



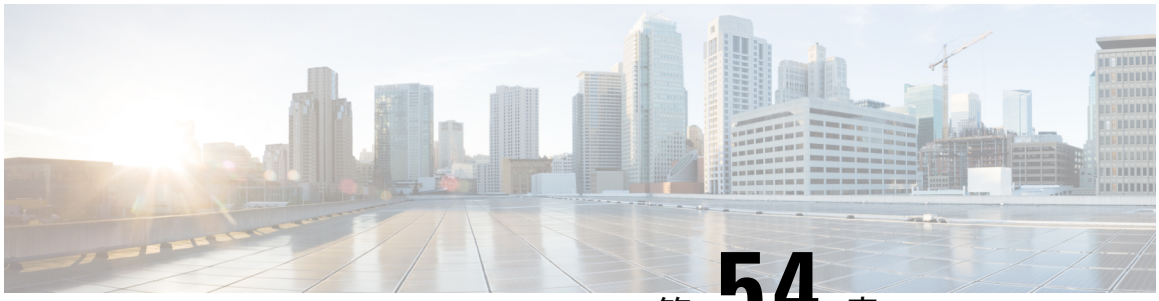
第 53 章

Cisco Unified Contact Center Enterprise の設定

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* インストレーション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。



第 54 章

Cisco Unified Contact Center Express の設定

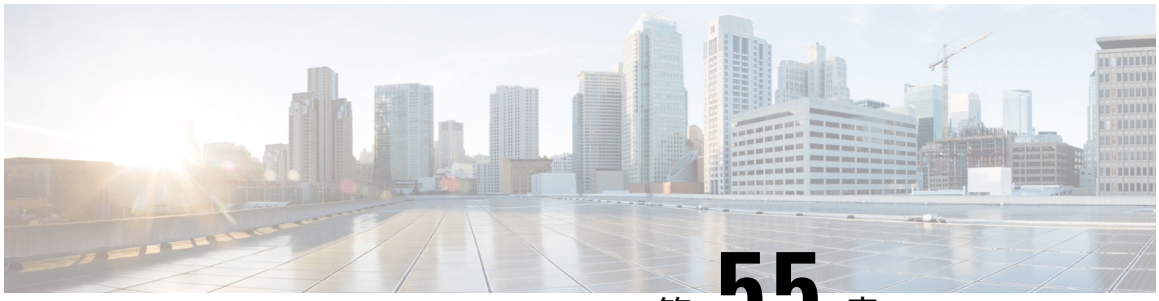
Cisco Unified Contact Center Express

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。



第 55 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
ステップ 1	CTIManager サービスのアクティブ化（557 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。
ステップ 2	CTIManager と Cisco Unified Communications Manager のサービスパラメータの設定 （557 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。
ステップ 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 （558 ページ） • 新しいコール受け付けタイマーの設定 （559 ページ） • 同時アクティブ通話の設定 （559 ページ） • CTI ルート ポイントの同期化 （560 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。
ステップ 4	CTI デバイスの電話番号の設定 （560 ページ）	CTI デバイスの電話番号を設定します。
ステップ 5	デバイスとグループの関連付け （561 ページ）	アプリケーション ユーザとエンド ユーザ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）。
ステップ 6	エンドユーザとアプリケーションユーザの追加 （561 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
ステップ 7	（省略可） アプリケーション障害時の CTI 冗長性の設定 （563 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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
ステップ 1	CTI ルート ポイントの設定 （558 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。
ステップ 2	新しいコール受け付けタイマーの設定 （559 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。
ステップ 3	同時アクティブ通話の設定 （559 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。
ステップ 4	**任意指定**：CTI ルート ポイントの同期化 （560 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 3 必須フィールドに入力します。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 [選択項目への設定の適用（Apply Config to Selected）] をクリックします。

ステップ 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

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [電話番号（Directory Number）]** を選択します。

ステップ 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。

ステップ 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。

ステップ 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とエンドユーザ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

ステップ 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（Application User）]** をクリックします。

ステップ 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 ユーザの設定（Application User Configuration）] ウィンドウが表示されます。

ステップ 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。

ステップ 4 [保存（Save）] をクリックします。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 ユーザを追加する場合は、[アプリケーション ユーザをグループに追加（Add App Users to Group）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

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、コールがすべてのコール 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

ステップ 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。

ステップ 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。

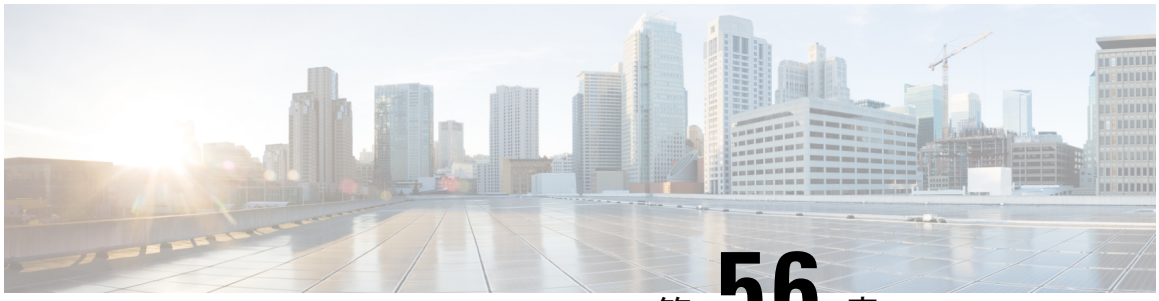
ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco CTI Manager（アクティブ）（Cisco CTIManager (Active)）] を選択します。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 7 [保存（Save）] をクリックします。



第 56 章

Cisco TelePresence の設定

Cisco TelePresence

Cisco TelePresence Conductor

Cisco TelePresence Conductor によって、マルチパーティのビデオ通信が容易になります。Cisco TelePresence Conductor は、ビデオ通信ネットワーク内に配置され、1 つ以上の会議ブリッジと 1 つ以上のコール制御デバイス（Cisco TelePresence Video Communication Server（Cisco VCS）または Unified Communications Manager）と連動して機能します。自発的な会議やランデブー会議を簡単にプロビジョニング、開始、アクセス、および管理できるようにビデオ ネットワークを設定できます。

アドホック会議の場合、Unified Communications Manager と TelePresence Conductor 間で SIP トランクが使用されます。Unified Communications Manager の SIP トランクの宛先として、関連する TelePresence Conductor のロケーションのアドホック IP アドレスを設定します。このロケーションのアドホック コールは、その SIP トランクにルーティングできます。

ランデブー会議の場合、Unified Communications Manager と TelePresence Conductor 間で別の SIP トランクが使用されます。Unified Communications Manager の SIP トランクの宛先として、関連する TelePresence Conductor のロケーションのランデブー IP アドレスを設定します。このロケーションのランデブー コールは、その SIP トランクにルーティングできます。

Cisco TelePresence Conductor を使用してシステムを設定する方法の詳細については、導入ガイド（http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html）を参照してください。

Cisco TelePresence 会議ブリッジ

Cisco TelePresence Server は、Cisco Unified Communications Manager と連携してユニファイド コミュニケーションの導入環境にマルチパーティ ビデオ機能を提供するスケーラブルなビデオ会議ブリッジです。マルチパーティ ビデオ会議向けに柔軟なビデオ機能、音声機能、コンテンツ共有機能を備えています。標準ベースのビデオエンドポイント、モバイルデバイス、Cisco

Webex クライアント、およびサードパーティ ビデオエンドポイントを使用して、会議の作成、開始、および参加を容易に行うことができます。

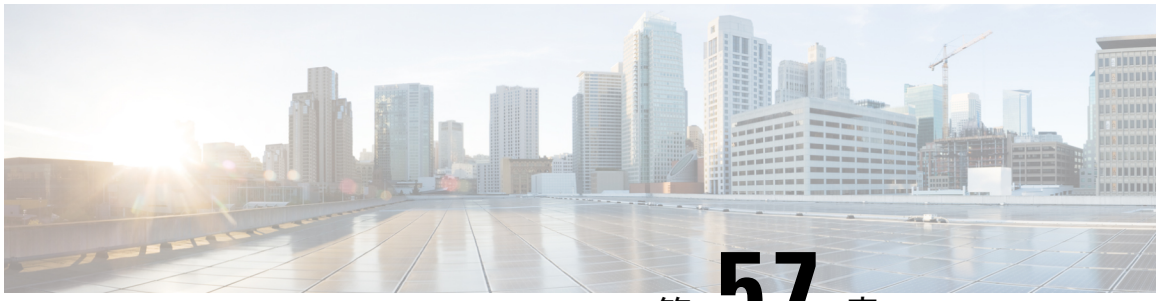
Cisco TelePresence MCU は、高解像度（HD）マルチポイントビデオ会議ブリッジです。毎秒 30 フレームで最大 1080p の性能を提供し、あらゆる会議で十分な連続表示、フルトランスコーディング機能を提供するため、混合した高解像度のエンドポイント環境を設定する場合は最適です。Cisco TelePresence MCU では、シグナリング コール制御プロトコルとして SIP をサポートしています。詳細に設定でき、システムおよび会議を制御およびモニタする、ビルトイン Web サーバを装備しています。

Cisco TelePresence サーバは主に Cisco TelePresence Conductor により制御されています。システム内でのこれらの会議ブリッジを設定する方法の詳細については、導入ガイド（http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html）を参照してください。

Cisco TelePresence Video Communication Server

Cisco TelePresence Video Communication Server（VCS）は、テレプレゼンス会議のセッション管理と制御を簡素化します。VCS は、セキュア通信、シンプルな大規模プロビジョニング、およびネットワーク管理を Cisco TelePresence Management Suite (Cisco TMS) と連携して提供します。VCS は Cisco Unified Communications Manager（Unified Communications Manager）と相互に作用して、システムに多彩なテレプレゼンス サービスを提供します。

Cisco TelePresence VCS をシステムと統合するための設定方法の詳細については、導入ガイド（http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html）を参照してください。



第 57 章

Cisco Jabber の設定

Cisco Jabber の設定

Cisco Jabberは、あらゆる場所から連絡先とのシームレスな対話を実現するUnified Communicationsアプリケーションスイートです。Cisco Jabber は、IM、プレゼンス、音声およびビデオ通話、ボイスメール、および会議を提供します。

Cisco Jabber 製品ファミリには、次のようなアプリケーションが含まれています。

- Cisco Jabber for Windows
- Cisco Jabber for Mac
- Cisco Jabber for iPhone and iPad
- Android 版 Cisco Jabber
- Cisco Jabber Softphone for VDI

Cisco Jabber 製品スイートの詳細については、https://www.cisco.com/go/jabber または https://www.cisco.com/c/en/us/products/unified-communications/jabber-softphone-for-vdi/index.html を参照してください。

Cisco Jabber を使用して動作するようにシステムを設定する方法の詳細については、『http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html』の『*Cisco Jabber* 導入ガイド』および『インストールガイド』を参照してください。

Cisco Jabber の OAuth 更新ログイン

Jabber リリース 11.9 時点の Cisco Jabber クライアントは、OAuth 更新ログインを使用して Cisco Unified Communications Manager と IM ane Presence サービスとの認証を行うことができます。この機能は、次の利点を提供することによって、Cisco Jabber のユーザエクスペリエンスを向上します。

- 最初のログイン後は、更新トークンの有効期間にわたってリソースへのシームレスなアクセスを提供します。
- Cisco Jabber クライアントが頻繁に再認証されないようにする必要がありません。
- SSO 環境と非 SSO 環境で、一貫したログイン動作を提供します。

OAuth 更新ログインを使用すると、Cisco Unified Communications Manager は OAuth 規格を使用して、クラスタ全体アクセストークンを発行し、トークンを更新します。Cisco Unified Communications Manager と IM ane Presence サービスは、短時間アクセストークンを使用して Jabber を認証します (アクセストークンのデフォルト寿命は 60 分です)。期間の長い更新トークンは、古いアクセストークンが期限切れになったときに、Jabber に新しいアクセストークンを提供します。更新トークンが有効である限り、Jabber クライアントは新しいアクセストークンを動的に取得できます (デフォルトの更新トークン寿命は 60 日です)。

すべてのアクセストークンは、JWT 形式 (RFC7519) を使用して暗号化され、署名され、自己完結型になっています。更新トークンは署名されていますが、暗号化されていません。

（注） また、OAuth 認証は、Cisco Expressway と Cisco Unified Connection でもサポートされています。互換性のあるバージョンについては、それらの製品で確認してください。互換性のないバージョンを実行している場合の Jabber の動作の詳細については、Cisco Jabber のドキュメントを参照してください。

認証プロセス

Cisco Jabber クライアントが認証する場合、または更新トークンが送信される場合、Cisco Unified Communications Manager が次の条件をチェックします。認証の各条件が満たされる必要があります。

- 署名を確認します。
- トークンを復号化して検証します。
- アクティブなユーザであることを確認します。たとえば、外部 LDAP ディレクトリから削除された LDAP 同期ユーザはデータベース内に残りますが、エンド ユーザ設定のユーザ ステータスには無効なユーザとして表示されます。
- 自分のロール、アクセス制御グループ およびユーザ ランク設定で指定されたとおりに、ユーザがリソースにアクセスできることを確認します。

（注） 後方互換性については、古い Jabber クライアントおよび Cisco Unified Real-Time Monitoring Tool などのサポート アプリケーションは、デフォルトで有効に設定されている暗黙の許可フロー モデルを使用して認証できます。

Cisco Jabber 前提条件

Cisco Jabber 統合には、次の前提条件があります。

- OAuth 更新ログインを使用する場合は、すべての UC システムでこの機能を有効にする必要があります。Cisco Jabber、Cisco Unity Connection および Cisco Expressway 展開が OAuth 更新ログインをサポートしていることを確認してください。
- iPhone および iPad 版 Cisco Jabber に対するプッシュ通知を導入している場合は、*iPhone* および *iPad* 版 *Cisco Jabber* と *Cisco Unified Communications Manager* のプッシュ通知で、プッシュ通知の前提条件および設定の完全なリストを参照します。

Cisco Jabber の設定タスク フロー

Cisco Jabber クライアントを使用するようにシステムを設定するには、Cisco Unified Communications Manager でこれらのタスクを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Jabber の更新ログインの設定 （571 ページ）	Cisco Unified Communications Manager と IM & Presence サービスを有効にして、Cisco Jabber 認証に OAuth 更新ログインを使用できるようにします。

	コマンドまたはアクション	目的
		（注） OAuth 更新ログインは、Cisco Unified Communications Manager ではデフォルトで無効になっていますが、Cisco Expressway ではデフォルトで無効になっています。Cisco Unified Communications Manager でこの機能を有効にしない場合は、Cisco Expressway でこの機能を無効にする必要があります。そうでないと、設定の不一致が発生する可能性があります。
ステップ 2	プッシュ通知の設定 （773 ページ）	iPhone および iPad 版 Cisco Jabber を展開している場合、システムのプッシュ通知を有効にします。 （注） iPhone および iPad 版 Cisco Jabber のプッシュ通知は必須設定です。Android、Mac、または Windows ユーザにこの機能は必要ありません。
ステップ 3	追加の Cisco Jabber 設定を構成します。	ご使用のプラットフォームの『*Cisco Jabber* オンプレミス展開ガイド』を参照してください。 • Android—http://www.cisco.com/c/en/us/support/unified-communications/jabber-android/products-installation-guides-list.html • iPhone または iPad—http://www.cisco.com/c/en/us/support/customer-collaboration/jabber-iphone-ipad/products-installation-guides-list.html • Mac—http://www.cisco.com/c/en/us/support/unified-communications/jabber-mac/products-installation-guides-list.html • Windows—http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

Cisco Jabber の更新ログインの設定

次の手順を使用して、OAuth アクセストークンによる更新ログインを有効にし、Cisco Unified Communications Manager でトークンを更新します。OAuth 更新ログインは、ネットワークの変更後にユーザを再ログインする必要がない効率的なログインフローを提供します。

（注） 互換性を実現するために、Cisco Jabber、Cisco Expressway、Cisco Unity Connection などの展開で Unified Communications のさまざまなコンポーネントが更新ログインをサポートしていることを確認してください。OAuth 更新ログインを有効にした後、この機能を無効にするには、すべての Cisco Jabber クライアントをリセットする必要があります。

始める前に

Cisco Jabber 11.9 の最低限のリリースを実行している必要があります。旧バージョンの Jabber では、以前のリリースの暗黙的な許可フロー認証モデルが使用されます。

手順

ステップ 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）] > [エンタープライズパラメータ（Enterprise Parameters）]**。

ステップ 2 **[SSO 設定]** で、次のいずれかの操作を実行します。

- OAuth 更新ログインを有効にするには、[更新ログインフローを使用したOAuth（OAuth with Refresh Login Flow）] エンタープライズパラメータを [有効（Enabled）] に設定します。
- OAuth 更新ログインを無効にするには、[更新ログインフローを使用したOAuth（OAuth with Refresh Login Flow）] エンタープライズパラメータを [無効（Disabled）] に設定します。これがデフォルトの設定です。

ステップ 3 OAuth 更新ログインが有効な場合は、次のエンタープライズ パラメータを設定してアクセストークンおよび更新トークンの有効期限を指定します。

- [OAuthアクセストークン失効タイマー（分）（OAuth Access Token Expiry Timer (minutes)）]：このパラメータは、各 OAuth アクセス トークンの失効タイマーを分単位で指定します。OAuthアクセストークンは、タイマーの期限が切れた後は無効ですが、Jabberクライアントは、更新トークンが有効である限り、ユーザが再認証する必要なく、新しいアクセストークンを要求して取得できます。デフォルト値は 60 分です。有効な範囲は 1 ～ 1440 分です。
- [OAuth更新トークン有効期限タイマー（日）（OAuth Refresh Token Expiry Timer (days)）]：このパラメータは、OAuth 更新トークンの有効期限タイマーを日単位で指定します。タイマーの期限が切れた後、更新トークンは無効になり、Jabber クライアントは新しい更新トークンを取得するために再認証する必要があります。有効範囲は 1 ～ 365 日、デフォルトは 60 日です。

ステップ 4 [保存（Save）] をクリックします。

（注） 設定を保存したら、すべての Cisco Jabber クライアントと Webex クライアントをリセットします。

OAuth 更新ログイン用のキーの再生成

コマンドラインインターフェイスを使用して暗号キーと署名キーの両方を再生成するには、この手順を使用します。Cisco Jabber が Unified Communications Manager との OAuth 認証に使用する暗号キーまたは署名キーが侵害された場合にのみ、この作業を実行します。署名キーは非対称で RSA ベースであるのに対し、暗号キーは対称キーです。

このタスクを完了すると、これらのキーを使用する現在のアクセストークンと更新トークンは無効になります。

エンドユーザへの影響を最小限に抑えるために、このタスクは営業時間外に完了することを推奨します。

暗号キーは、以下の CLI を使用してのみ再生成できますが、パブリッシャノードの Cisco Unified OS の管理 GUI を使用して署名キーを再生成することもできます。**[セキュリティ（Security）]**> **[証明書の管理（Certificate Management）]** を選択し、**AUTHZ** 証明書を選択して、**[再作成（Regenerate）]** をクリックします。

手順

ステップ 1 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。

ステップ 2 暗号キーを再生成するには、次の手順を実行します。

a) `set key regen authz encryption` コマンドを実行します。

b) 「`yes`」と入力します。

ステップ 3 署名キーを再生成するには、次の手順を実行します。

a) `set key regen authz signing` コマンドを実行します。

b) 「`yes`」と入力します。
Unified Communications Manager パブリッシャ ノードがキーを再生成し、IM and Presence サービスのローカル ノードを含めたすべての Unified Communications Manager クラスタ ノードに新しいキーを複製します。

すべての UC クラスタで新しいキーを再生成して同期する必要があります。

- IM and Presence 中央クラスタ：IM and Presence 集中型展開の場合、IM and Presence ノードはテレフォニーとは別のクラスタ上で実行されています。この場合、IM and Presence Service の中央クラスタの Unified Communications Manager パブリッシャ ノードで、この手順を繰り返します。

- Cisco Expressway または Cisco Unity Connection：これらのクラスタ上でもキーを再生成します。詳細については、Cisco Expressway および Cisco Unity Connection のマニュアルを参照してください。

（注） キーを再割り当てした後、クラスタ内のすべてのノードで Cisco CallManager サービスを再起動します。

既存の OAuth 更新トークンの取り消し

既存の OAuth 更新トークンを取り消すには、AXL API を使用します。たとえば、ある従業員が退社した場合、この API を使用してその従業員の現在の更新トークンを取り消し、その従業員が新しいアクセストークンを取得したり、企業アカウントへログインできないようにすることができます。API は、AXL クレデンシャルで保護されている REST ベースの API です。任意のコマンドライン ツールを使用して API を呼び出すことができます。次のコマンドは、更新トークンを取り消すために使用できる cURL コマンドの例を示しています。

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

引数の説明

- `admin:password` は、Cisco Unified Communications Manager の管理者アカウントのログイン ID とパスワードです。
- `UCMaddress` は、Cisco Unified Communications Manger のパブリッシャ ノードの FQDN または IP アドレスです。
- `end_user` は、更新トークンを取り消すユーザのユーザ ID です。

Cisco Jabber の連携動作と制限事項

特長	連携動作
正常登録	正常登録では、2 つの Cisco Jabber クライアントから同じデバイス名を使用して(たとえば、オフィスのラップトップおよびホームオフィスのラップトップ上で動作する Jabber)、デュアル登録が行われます。この機能によって、最初の登録が自動的に解除され、2 番目の登録を続行することができるようになります。登録解除済み Jabber クライアントは再登録されません。 Cisco Jabber の正常登録は、Jabber がモバイルおよびリモートアクセス (MRA) 展開に展開されている場合を除き、自動的にサポートされます。MRA の展開では、登録解除された Jabber クライアントが登録を再登録しようとします。 MRA 導入では、同じデバイス名を持つ 2 台のデバイスで Cisco Jabber を実行している場合、他のデバイスを使用する前に必ず Jabber をログに記録するようにしてください。

OAuth SSO 設定のトラブルシューティング

次の表に、OAuth SSO 設定のトラブルシューティングに役立つログを示します。これらのログに対してトレースを設定する必要はありません。

（注） SAML SSO ログを詳細レベルに設定するには、`set samltrace level debug` CLI コマンドを実行します。

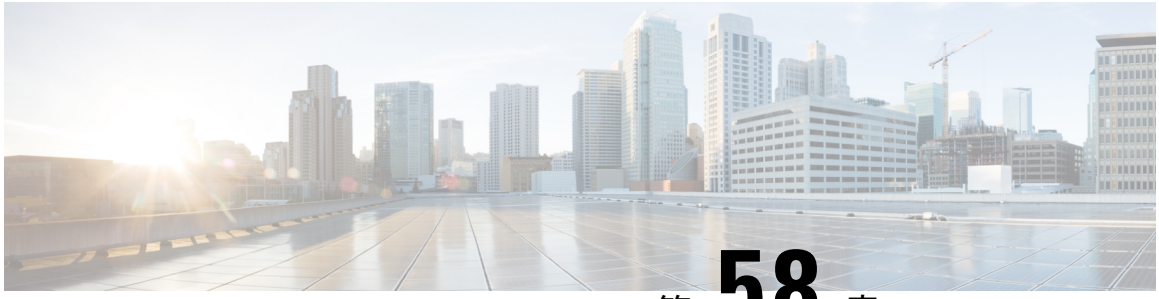
表 *70 : OAuth* 更新ログインのトラブルシューティングのログ

ログ	ログの詳細
SSO ログ	新しい SSO アプリ操作が完了するたびに、次の新しいログエントリが生成されます。 `/var/log/active/platform/log/ssoApp.log`
Ssosp ログ	SSO 操作と OAuth 操作は、ssosp ログに記録されます。SSO が有効化されるたびに、新しいログファイルが次のように作成されます。 `/usr/local/thirdparty/Jakarta-tomcat/logs/ssosp/log4j/`

ログ	ログの詳細
SSO および OAuth の設定	証明書ログは、次の場所にあります。Authz 証明書が再生成されるたびに、新しいログファイルが生成されます。 `/var/log/active/platform/log/certMgmt * .log`

第 VIII 部

メディア リソースの設定



第 58 章

メディア リソースの概要

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。

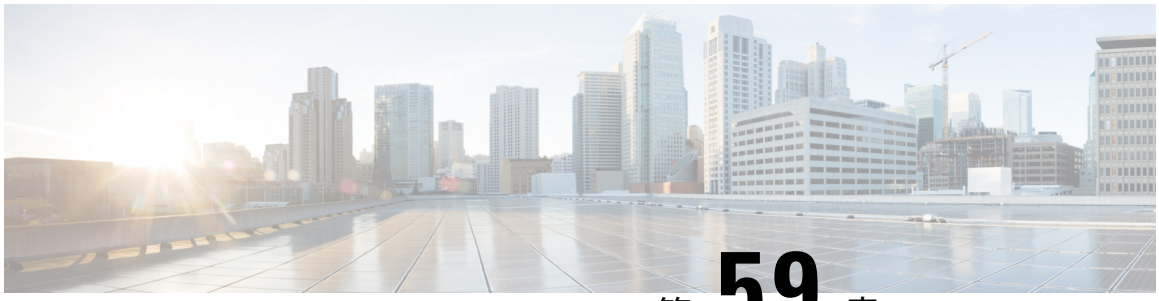
メディアリソース構成タスクフロー

次のタスク フローを実行すると、システムのメディア リソースを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	メディア リソース グループのタスク フロー （584 ページ）	この章の手順を使用して、メディアサーバの論理グループを定義します。
ステップ 2	トラステッド リレー ポイントのタスク フロー （592 ページ）	トラステッド リレー ポイントをメディア ストリームに挿入し、そのストリームのコントロール ポイントとして機能させます。TRP を使用すると、そのストリームにさらに処理を加えることができます。また、ストリームが特定のパスを通るようにする手段として TRP を使用することも可能です。
ステップ 3	アナンシエータの設定タスク フロー （604 ページ）	アナンシエータを設定することで、Unified Communications Manager は、録音済みのアナウンス（.wav ファイル）を再生したり、Cisco Multilevel Precedence and Preemption 用に設定された Cisco IP Phone やゲートウェイなどのデバイスにトーンを送信したりできます。
ステップ 4	自動音声応答の設定タスク フロー （611 ページ）	自動音声応答（IVR）装置を使用して、録音済みの機能アナウンス（.wav ファイル）を Cisco IP Phone やゲートウェイなどのデバイスで再生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。
ステップ 5	保留中ビデオ設定のタスク フロー （618 ページ）	ビデオ コンタクト センターにコールを発信する顧客が、コンタクト センターでのエージェントとの最初のコンサルティングの後に、特定のビデオを視聴できるように、ビデオ コンタクト センターに Video On Hold を設定します。

	コマンドまたはアクション	目的
ステップ 6	アナウンスの設定タスク フロー （623 ページ）	この章の手順を使用して、事前定義済みのアナウンスを使用するか、またはカスタム アナウンスをアップロードできます。
ステップ 7	会議ブリッジの設定タスクフロー （632 ページ）	アドホック/ミートミー ビデオ会議およびビデオ会議を可能にするソフトウェアとハードウェアのアプリケーションを設定します。
ステップ 8	DSCP 設定の設定タスク フロー （637 ページ）	フレキシブル DSCP マーキングおよびビデオ プロモーションを使用して、コールアドミッション制御（CAC）と Quality of Service（QoS）の処理でどのアプリケーションを最も優先するかを指定するポリシーを設定できます。
ステップ 9	トランスコーダと MTP の設定タスク フロー （652 ページ）	1 つの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するために、トランスコーダを設定します。



第 59 章

メディア リソースの定義

メディア リソース グループの概要

メディア リソース グループでは、メディア サーバの論理的なグループ化が定義されます。必要に応じて、メディア リソース グループを地理上の場所またはサイトと関連付けることができます。さらに、サーバの使用または目的のサービスのタイプ（ユニキャストまたはマルチキャスト）を制御するメディア リソース グループを形成することもできます。

システムにはメディア リソースを管理する 2 層構造のアプローチがあります。

- メディア リソース グループ：メディア サーバの論理グループ。
- メディア リソース グループ リスト：優先順位付けされたメディア リソース グループの一覧。アプリケーションは、[メディア リソース グループリスト（Media Resource Group List）] で定義された優先順位に従って、使用可能なメディア リソースから必要なメディア リソース（保留音サーバなど）を選択します。メディア リソース グループ リストは、デバイスに関連付けられていて、メディア リソース グループの冗長化を実現しています。

次のタイプのデバイスを、1 つのメディア リソース グループにグループ化することができます。

- 会議ブリッジ（CFB）
- メディア ターミネーション ポイント（MTP）
- 保留音サーバ（MOH）
- トランスコーダ（XCODE）
- アナンシエータ（Annunciator）（ANN）

（注） メディア リソースが設定された後にメディア リソース グループをまだ定義していない場合は、すべてのメディア リソースがデフォルト グループに属するため、特定のクラスタ内のすべての Cisco Unified Communications Manager ですべてのメディア リソースを使用できます。

[メディアリソースグループリスト（Media Resource Group List）]

メディアリソースグループリストは、優先順位を付けてメディア リソースグループをグループ化します。アプリケーションは、[メディアリソースグループリスト（Media Resource Group List）] で定義された優先順位に従って、使用可能なメディアリソースから必要なメディアリソース（保留音サーバなど）を選択します。メディア リソース グループ リストは、デバイスまたはデバイス プールに関連付けられていて、メディア リソース グループの冗長化を実現しています。

メディアリソースグループの前提条件

Cisco Unified Communications Manager にはメディア リソースがあり、アナンシエータ、トランスコーディング、会議、保留音、メディア ターミネーションなどのサービスを提供することを確認します。

メディア リソース グループのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	メディア リソース グループの設定 （585 ページ）。	メディアリソースグループが、メディア サーバの論理的なグループ化を定義するように設定します。
ステップ 2	メディア リソース グループへのデバイスの割り当て （586 ページ）。	メディア リソース グループにデバイスを割り当てます。 （注） デバイスを割り当てる順序は重要ではありません。
ステップ 3	メディア リソース グループ リストの設定 （586 ページ）。	メディアリソースグループリストを作成して、メディアリソースグループを優先

	コマンドまたはアクション	目的
		順に並べたリストを指定します。メディア リソース グループ リストは、デバイスまたはデバイス プールに関連付けられていて、メディア リソース グループの冗長化を実現しています。 （注） デバイスを割り当てる順序は重要です。
ステップ 4	メディア リソース グループ リストへのメディア リソース グループの割り当て（587 ページ）。	新規に作成されたメディアリソースグループをメディアリソースグループリストに割り当てます。
ステップ 5	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 （588 ページ）。	既存または新規作成メディアリソースグループリストをデバイスまたはデバイスプールに割り当てます。
ステップ 6	（任意）メディア リソース冗長性の設定 （588 ページ）。	メディアリソースに障害が発生したときは、メディアリソースの冗長性を確認します。

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 グループの [名前（Name）] と [説明（Description）] を入力します。

ステップ 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。

ステップ 6 （省略可）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。

ステップ 7 [保存（Save）] をクリックします。

メディア リソース グループへのデバイスの割り当て

アナンシエータ(ANN)、自動音声応答 (IVR)、会議ブリッジ (CFB)、メディアターミネーションポイント (MTP)、保留音 (MOH)サーバおよびトランスコーダなどのデバイスを、メディアリソースグループに割り当てることができます。デバイスを割り当てる順序は重要ではありません。

始める前に

メディア リソース グループの設定 （585 ページ）。

手順

ステップ 1 Cisco Unified CM Administration から、**[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。

ステップ 2 既存のメディアリソースグループを設定するには、**[メディアリソースグループの検索と一覧表示]** ウィンドウで、適切なフィルタを指定し、**[検索（Find）]** をクリックします。

ステップ 3 新しいメディア リソース グループ リストを設定するには、**[新規追加（Add New）]** をクリックします。

ステップ 4 **[Available Media Resources]** フィールドで、1 つまたは複数のデバイスを選択し、下矢印キーをクリックします。
選択したデバイスが **[選択したメディアリソース (selected Media Resources)]** フィールドに表示されます。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

メディア リソース グループ リストの設定 （586 ページ）.

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の作成このリストは、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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

メディア リソース グループ リストへのメディア リソース グループの割り当て

始める前に

メディア リソース グループ リストの設定 （586 ページ）。

手順

ステップ 1 Cisco Unified CM Administration から、**[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。

ステップ 2 既存のメディアリソースグループを設定するには、**[メディアリソースグループの検索と一覧表示]** ウィンドウから、適切なフィルタを指定し、**[検索（Find）]** をクリックします。

ステップ 3 **[利用可能なメディアリソース]** フィールドで、1 つまたは複数のメディアリソースを選択し、下矢印キーをクリックします。
選択したメディアリソースが、**[選択したメディアリソース]** リストに表示されます。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

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 （588 ページ）.

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 [保存（Save）] をクリックします。

ステップ 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。

メディア リソース冗長性の設定

メディア リソース グループ リストでは、メディア リソース グループの優先リストを指定して、メディア リソースの冗長性を確保します。アプリケーションは、メディア リソース リストで定義されている優先順位に従って、使用できる対象から必要なメディア リソースを選択できます。

メディア リソース グループおよびメディア リソース リストに冗長性を設定するには、「メディア リソース グループの設定（585 ページ）」と「[メディアリソースグループリスト（Media Resource Group List）]（584 ページ）」の手順を実行します。

メディアリソースグループの連携動作と制限事項

メディア リソース グループの連携動作

表 *71 :* メディア リソース グループの連携動作

機能	連携動作
コール処理	コール処理は、メディアリソースグループリストが選択されている場合に、メディアリソースグループリストをデバイスレベルで使用します。リソースが見つからない場合、コール処理はデフォルトの割り当てからリソースを取得できます。 メディアリソースグループリストがデバイスレベルで選択されていない場合だけ、コール処理はデバイスプール内のメディア リソースグループリストを使用します。リソースが見つからない場合、コール処理はデフォルトの割り当てからリソースを取得できます。
アナンシエータリソースサポート	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、会議ブリッジのあるデバイスプールに割り当てられている場合、Cisco Unified Communications Manager は会議ブリッジにアナンシエータリソースのサポートを提供します。 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、Cisco Unified Communications Manager は会議ブリッジにアナンシエータ リソースのサポートを提供しません。
テレビ会議	ビデオ会議を保留にするときにビデオ会議ブリッジだけが使用されるようにするには、そのビデオ会議ブリッジをメディア リソース グループに追加します。メディア リソース グループをメディア リソース グループ リストに追加し、ビデオ会議ブリッジを使用するデバイスまたはデバイス プールにそのメディア リソース グループ リストを割り当てます。

メディア リソース グループの制限事項

表 *72:* メディア リソース グループの制限事項

制限事項	説明
メディアリソースグループの定義	メディア リソース グループ リストに割り当てられているメディア リソース グループは、削除できません。
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。
メディアリソースの削除	メディアリソースグループに含まれるメディアリソース（会議ブリッジなど）を削除するには、その前に、そのリソースをメディアリソースグループから削除するか、そのメディアリソースを含むメディアリソースグループを削除する必要があることに注意してください。

第 60 章

トラステッドリレーポイント（TRP）の設定

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 ポイントのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	デバイスのトラステッド リレー ポイントの設定 （593 ページ）。	メディアが終了し、TRP をCisco Unified Communications Managerに挿入する 1 つまたは複数のデバイス向けの、トラステッドリレーポイント(TRP) を設定します。
ステップ 2	メディア ターミネーション ポイントのトラステッド リレー ポイントの設定（593 ページ）。	デバイスをトラステッドリレーポイントとして使用できるように、メディア終端ポイント (MTP) を設定します。 （注） Cisco Unified Communications Manager で TRP として設定されたデバイスについて、その TRP とコールに関連したすべてのエンドポイントの間に適切なネットワーク接続および設定が存在することを確認する必要があります。
ステップ 3	トランスコーダに対するトラステッド リレー ポイントの設定（594ページ）。	デバイスをトラステッドリレーポイントとして使用できるように、トランスコーダを設定します。 （注） Cisco Unified Communications Manager で TRP として設定されたデバイスについて、その TRP とコールに関連したすべてのエンドポイントの間に適切なネットワーク接続および設定が存在することを確認する必要があります。
ステップ 4	トラステッド リレー ポイントのサービス パラメータの有効化（595ページ）。	TRPサービスパラメータを有効にして、どのTRPリソースも利用できない場合、

	コマンドまたはアクション	目的
		TRP を必要とするコールを続行できるかどうかを判断します。

デバイスのトラステッド リレー ポイントの設定

メディアの終端である 1 つまたは複数のデバイスのトラステッド リレー ポイント（TRP）を設定したり、Cisco Unified Communications Manager に TRP を挿入できます。デバイスの TRP を設定することによって、デバイスは、そのストリームでさらに処理を実行したり、ストリームが特定のパスをたどっていることを確認できます。

手順

ステップ 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）]** の順に選択します。

ステップ 2 既存デバイスのトラステッド リレー ポイントを設定するには、[共通デバイス設定の検索と一覧表示（Find and List Common Device Configurations）] ウィンドウから、適切なフィルタを指定して [検索（Find）] をクリックします。

ステップ 3 新規デバイスのトラステッド リレー ポイントを設定するには、[共通デバイス設定（Common Device Configuration）] ウィンドウから、[新規追加（Add New）] をクリックします。

ステップ 4 [共通デバイス設定（Common Device 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。

ステップ 5 [共通デバイス設定情報（Common Device Configuration Information）] セクションで、[トラステッド リレー ポイントを使用（Use Trusted Relay Point）] チェック ボックスをクリックします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

メディア ターミネーション ポイントのトラステッド リレー ポイントの設定 （593 ページ）.

メディア ターミネーション ポイントのトラステッド リレー ポイントの設定

デバイスをトラステッドリレーポイント（TRP）として利用できるようにメディア ターミネーション ポイント（MTP）を設定できます。

始める前に

デバイスのトラステッド リレー ポイントの設定 （593 ページ）。

手順

ステップ 1 Cisco Unified CM Administration で、**[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。

ステップ 2 既存のメディア ターミネーション ポイントに TRP を設定するには、[メディアターミネーションポイントの検索と一覧表示（Find and List Media Termination Points）] ウィンドウから、該当するフィルタを指定し、[検索（Find）] をクリックします。

ステップ 3 新しいメディア ターミネーション ポイントに TRP を設定するには、[新規追加（Add New）] をクリックします。

ステップ 4 [メディア ターミネーション ポイントの設定（Media Termination 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。

ステップ 5 [メディア ターミネーション ポイント情報（Media Termination Point Information）] セクションで、[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ます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

トランスコーダに対するトラステッド リレー ポイントの設定 （594 ページ）.

トランスコーダに対するトラステッド リレー ポイントの設定

トラステッド リレー ポイント（TRP）としてデバイスを使用できるようにトランスコーダを設定できます。

始める前に

メディア ターミネーション ポイントのトラステッド リレー ポイントの設定 （593 ページ）。

手順

ステップ 1 Cisco Unified CM Administration で、**[メディア リソース（Media Resources）] > [トランスコーダ（Transcoder）]** の順に選択します。

ステップ 2 既存のトランスコーダに対する TRP を設定するには、[トランスコーダの検索と一覧表示（Find and List Trancoder）] ウィンドウから、該当するフィルタを指定し、[検索（Find）] をクリックします。

ステップ 3 新しいトランスコーダに対して TRP を設定するには、[新規追加（Add New）] をクリックします。

ステップ 4 [トランスコーダの設定（Transcoder 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。

ステップ 5 [メディア サーバ トランスコーダ情報（Media Server Transcoder Info）] セクションで、[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ます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

トラステッド リレー ポイントのサービス パラメータの有効化 （595 ページ）.

トラステッド リレー ポイントのサービス パラメータの有効化

TRP サービス パラメータを有効にすると、TRP リソースが使用できない場合に、TRP を必要とするコールの続行を許可するかどうかを決定できます。

始める前に

トランスコーダに対するトラステッド リレー ポイントの設定 （594 ページ）。

手順

ステップ 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。

[サーバ（Server）] ドロップダウン リストのみが表示されます。

ステップ 2 [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 リストからサーバを選択します。
[サービス（Service）] ドロップダウン リストが表示されます。

ステップ 3 [サーバ（Server）] 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。
選択されたサーバおよびサービスに基づいて、サービス パラメータが表示されます。

ステップ 4 [クラスタ全体のパラメータ（デバイス - 全般）（Clusterwide Parameters (Device - General)）] セクションから、[トラステッドリレーポイントの割り当てが失敗するとコールは失敗する（Fail Call If Trusted Relay Point Allocation Fails）] ドロップダウン リストの [True] を選択します。フィールドとその設定オプションについては、「関連項目」のセクションを参照してください。

ステップ 5 [クラスタ全体のパラメータ（デバイス - H323）（Clusterwide Parameters (Device - H323)）] セクションから、[MTP の割り当てが失敗するとコールは失敗する（Fail Call If MTP Allocation Fails）] ドロップダウン リストの [True] を選択します。フィールドとその設定オプションについては、「関連項目」のセクションを参照してください。

ステップ 6 [保存（Save）] をクリックします。

MTP と TRP サービスパラメータが選択されている場合のコールステータス

エンドポイントの**[メディアターミネーションポイントが必須(Media Termination Point Required)]** チェックボックスと **[トラステッドリレーポイントを使用(Use Trusted Relay Point)]** チェックボックスの両方がオンになっている場合、Cisco Unified Communications Manager は、信頼されたリレーポイント（TRP）でもあるメディアターミネーションポイント（MTP）を割り当てます。管理者がこのようなMTP またはTRP の割り当てに失敗すると、コール ステータスが表示されます。

次の表に、コールが失敗した場合の**Fail Call If Trusted Relay Point Allocation Fails**サービスパラメータおよび**Fail Call if MTP Allocation Fails**サービスパラメータの値を備えたコールステータスを表示します。

Fail Call If TRP Allocation Fails	Fail Call If MTP Allocation Fails	コールが失敗するか
True	True	はい
True	False	はい
False	True	はい（MTP が H.323 エンドポイントに必要な場合）。いいえ（MTP が SIP エンドポイントに必要な場合）
False	False	×

MTP と TRP サービスパラメータが選択されていない場合のコールステータス

Fail Call If Trusted Relay Point Allocation Fails サービス パラメータおよび **Fail Call If MTP Allocation Fails** サービスパラメータがいずれも **`False`** に設定されている場合、以下の表には、必要なMTP に関連するコールの動作を示します。動作に関係するのは、**[信頼されたリレーポイントを使用(Use Trusted Relay Point)]** の設定、およびリソース割り当てのステータスです。

[メディアターミネーションポイントが必須(Media Termination Point Required)]	[信頼されたリレーポイントを使用(Use Trusted Relay Point)]	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。

[メディアターミネーションポイントが必須(Media Termination Point Required)]	[信頼されたリレーポイントを使用(Use Trusted Relay Point)]	リソース割り当てのステータス	コールの動作
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。

トラステッド リレー ポイントの連携動作と制限事項

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。

機能	連携動作と制限事項
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）。
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。

トラステッド リレー ポイントの制限事項

表 *73:* トラステッド リレー ポイントの制限事項

制限事項	説明
エンドポイント向けトラステッドリレーポイントの挿入	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。
エンドポイント向けメディア ターミネーション ポイントの割り当て	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。
トラステッド リレー ポイントの割り当て	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）。

第 61 章

アナンシエータの設定

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 74 : 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 75 : 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。
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。

会議ブリッジでのアナンシエータの使用

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。

アナンシエータの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	アナンシエータの有効化 （605 ページ）	ノードで Cisco IP Voice Media Streaming Application サービスをアクティブにして、そのノードのアナンシエータをアクティブにします。クラスタ内で有効にする Cisco IP Voice Media Streaming Application サービスは 1 つだけに限定します。
ステップ 2	必須: メディア リソース グループのタスク フロー （584 ページ）	メディアリソースグループとリストにアナンシエータを追加して、Cisco Unified Communications Manager 管理を使用してメディアリソースを管理します。**[依存関係レコード要約(Dependency Records Summary)]** ウィンドウに、アナンシエータを使用するメディアリソースグループが表示されます。
ステップ 3	デバイス プールの設定 （64 ページ）	Cisco Unified Communications Manager 管理を使用して、デバイスプールにアナンシエータを含むメディアリソースグループを追加します。各アナンシエータに対してこの手順を繰り返します。各アナンシエータはデバイス プールに所属する必要があります。

	コマンドまたはアクション	目的
ステップ 4	（任意） メディアストリームのデフォルト数を変更する （606 ページ）	アナンシエータ用のデフォルトのメディアストリーム数を変更できます。
ステップ 5	（任意） アナンシエータのセキュリティモードの上書き （606 ページ）	Cisco Unified Communications Manager がセキュアに展開されている場合、アナンシエータとセキュリティが有効なデバイスとの間のメディア ストリーミングは Secure Real-Time Protocol（SRTP）で自動的に暗号化されます。アナンシエータのセキュリティ設定を上書きし、セキュアなアナンシエータから配信されたストリーム メディアが暗号化されないようにすることができます。
ステップ 6	（任意） アナンシエータがあるメディア リソース グループ リストを表示（607 ページ）	どのメディア リソース グループがアナンシエータ デバイスを使用するかを確認できます。
ステップ 7	（任意） 会議ブリッジに対するアナンシエータの設定 （608 ページ）	アナンシエータと会議ブリッジが同じデバイス プールに属している時は、会議ブリッジでアナンシエータを使用できます。

アナンシエータの有効化

クラスタ内で有効にする Cisco IP Voice Media Streaming Application サービスは 1 つだけに限定します。

注意 コール処理負荷が高い Cisco Unified Communications Manage ノードでは、アナンシエータをアクティブにしないことをお勧めします。

手順

ステップ 1 Serviceability GUI から、**[ツール（Tools）]**>**[アクティブ化（Activation）]** を選択します。[サービスアクティベーション（Service Activation）] ウィンドウが表示されます。

ステップ 2 [サーバ（Server）] フィールドのノードを選択し、[移動（Go）] をクリックします。

ステップ 3 **Cisco IP Voice Media Streaming Application**にチェックを入れ、**[保存(Save)]**をクリックします。

次のタスク

メディアリソースグループを設定していない場合は、それをデバイスプールに割り当てますメディアリソース構成タスクフロー （580 ページ）。

それ以外の場合は、メディアストリームのデフォルト数を変更する （606 ページ）.

メディアストリームのデフォルト数を変更する

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。アナンシエータのサービスパラメータを使用して、デフォルトのメディアストリームの数を変更できます。ただし、1 つのノードでは、48 の警報ストリームを超えることは推奨されていません。

始める前に

アナンシエータの有効化 （605 ページ）

手順

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

ステップ 2 **[サービスパラメータの設定]** ウィンドウで、サーバを選択してから、Cisco IP Voice Media Streaming App と呼ばれるサービスを選択します。

ステップ 3 **[サービスパラメータの設定]** ウィンドウで、**[アナンシエータパラメータ]** セクションの **[コールカウント (Call Count)]** フィールドに同時メディアストリームの数を入力し、**[保存 (Save)]** をクリックします。

アナンシエータを更新するときに、アクティブアナウンスが再生されていなければ、アナンシエータがアイドル状態になったときに自動的に変更されます。

次のタスク

アナンシエータのセキュリティモードの上書き （606 ページ）

アナンシエータのセキュリティモードの上書き

[クラスタ セキュリティ モード（Cluster Security Mode）] と呼ばれるエンタープライズパラメータが 1（混合モード）に設定されると、アナになります。アナンシエータは、Secure Real-Time Protocol （SRTP）を有効にした Cisco Unified Communications Manager で、セキュアな SRTP デバイスとして登録されます。ロックされたアイコンは、SRTP 対応デバイスに表示されます。セキュアなアナンシエータからのアナウンスは、受信側デバイスも SRTP 対応であれば暗号化されます。SRTP 対応ではない場合は、保護されていないアナウンスとトーンが送信されます。

[Make Annunciator Non-secure when Cluster Security is Mixed（クラスタのセキュリティが混在している場合はアナンシエータを非セキュアに設定）] というサービス パラメータを使用して、アナンシエータのセキュリティ モードをオーバーライドできます。アナンシエータのセキュリティ モードが上書きされると、受信側デバイスで SRTP が有効でも暗号化されていないアナウンスが再生されます。

始める前に

メディアストリームのデフォルト数を変更する （606 ページ）

手順

ステップ 1 必須: Cisco Unified CM Administration で、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

ステップ 2 [サーバ（Server）] フィールドでノードを選択します。

ステップ 3 [サービス（Service）] フィールドで [Cisco Unified IP ボイス メディア ストリーミング アプリケーション（Cisco Unified IP Voice Media Streaming Application）] を選択します。

ステップ 4 [クラスタのセキュリティが混在している場合はアナンシエータを非セキュアに設定（Make Annunciator Non-secure when Cluster Security is Mixed）] を **True** に設定して、[保存（Save）] をクリックします。

ヒント [クラスタのセキュリティが混在している場合はアナンシエータを非セキュアに設定（Make Annunciator Non-secure when Cluster Security is Mixed）] パラメータが表示されていないときは、[詳細機能（Advanced）] をクリックします。

次のタスク

アナンシエータがあるメディア リソース グループ リストを表示 （607 ページ）

アナンシエータがあるメディア リソース グループ リストを表示

どのメディア リソース グループがアナンシエータ デバイスを使用するかを確認するには、[依存レコード サマリー（Dependency Records Summary）] ウィンドウを表示します。

始める前に

アナンシエータのセキュリティモードの上書き （606 ページ）

手順

ステップ 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。

ステップ 2 システム用に設定されているアナンシエータを選択します。

ステップ 3 [関連リンク（Related Links）] ドロップダウン リスト ボックスで、[依存レコード（Dependency Records）] を選択し、[移動（Go）] をクリックします。
[依存レコード サマリー（Dependency Records Summary）] ウィンドウは、アナンシエータ デバイスを使用するメディア リソース グループを表示します。

次のタスク

会議ブリッジに対するアナンシエータの設定 （608 ページ）

会議ブリッジに対するアナンシエータの設定

このアナンシエータを会議ブリッジに使用することができます。

始める前に

アナンシエータがあるメディア リソース グループ リストを表示 （607 ページ）

手順

ステップ 1 メディアリソースグループのリストにアナンシエータを追加します。

ステップ 2 その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を会議ブリッジのデバイスプールに割り当てて、そのアナンシエータをクラスタ内のすべてのデバイスで利用可能にします。

第 62 章

自動音声応答の設定

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 *76 :* 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。
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

特長	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。
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。

自動音声応答の設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	音声自動応答のアクティブ化（612 ページ）	ノードで Cisco IP Voice Media Streaming Application サービスをアクティブにして、そのノードの IVR をアクティブにします。クラスタ内の各 IVR デバイスで有効にする Cisco IP Voice Media Streaming Application サービスは 1 つだけに限定します。
ステップ 2	必須: IVR を保持するメディア リソース グループのリストの表示（612 ページ）	メディアリソースグループとリストに IVR を追加して、Cisco Unified Communications Manager 管理を使用してメディアリソースを管理します。

	コマンドまたはアクション	目的
ステップ 3	（任意） メディアストリームのデフォルト数を変更する （606 ページ）	IVR用のデフォルトのメディアストリーム数を変更できます。

音声自動応答のアクティブ化

クラスタに登録された自動音声応答 (IVR) デバイスを使用するには、各ノードに対して 1 つ以上の Cisco IP Voice Media ストリーミングアプリケーションサービスをアクティブ化します。

⚠

注意 コール処理負荷が高い Cisco Unified Communications Manage ノードでは、IVR をアクティブにしないでください。

手順

ステップ 1 Cisco Unified 有用性 GUI から、**ツール** > **アクティベーション**を選択します。[サービスアクティベーション（Service Activation）] ウィンドウが表示されます。

ステップ 2 [サーバ（Server）] フィールドのノードを選択し、[移動（Go）] をクリックします。

ステップ 3 **Cisco IP Voice Media Streaming Application**チェックボックスにチェックを入れ、**[保存(Save)]** をクリックします。

IVR を保持するメディア リソース グループのリストの表示

手順

ステップ 1 Cisco Unified CM Administration から、**[メディア リソース（Media Resources）]** > **[自動音声応答（IVR）（Interactive Voice Response (IVR)）]** を選択します。
[自動音声応答（IVR）の検索と一覧表示（Find and List Interactive Voice Response (IVR)）] ウィンドウが表示されます。

ステップ 2 [自動音声応答（IVR）の検索と一覧表示（Find and List Interactive Voice Response (IVR)] ウィンドウから、[検索（Find）] をクリックします。
Cisco Unified Communications Manager で使用可能な IVR のリストが表示されます。

ステップ 3 メディア リソース グループの関連付けリストを表示する IVR を選択します。

ステップ 4 [関連リンク（Related Links）] ドロップダウン リストから [依存関係レコード（Dependency Records）] ノードを選択し、[移動（Go）] 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、[依存関係レコード要約（Dependency Records Summary）] ウィンドウにメッセージが表示されます。

IVR の設定

フィールド	説明
[サーバ（Server）]	デフォルトでは、事前設定済みサーバ（サーバはインストール中に追加されます）を表示します。
[名前（Name）]	デバイスが Cisco Unified Communications Manager に登録するときに使用する名前を指定します。英数字で最大 15 文字の名前を入力します（ピリオド、ダッシュ、およびアンダースコアを使用できます）。
説明	英数字で最大128文字の説明を入力します（ピリオド、ダッシュ、およびアンダースコアを使用できます）。デフォルトでは、プレフィクス IVR_ を含むサーバ名が使用されます。
[デバイスプール（Device Pool）]	[デフォルト（Default）] を選択するか、設定済みのデバイス プールのドロップダウン リストからデバイス プールを選択します。
[ロケーション（Location）]	一元化されたコール処理システムでコール アドミッション制御（CAC）を実装するには、ロケーションを使用します。CAC を使用すれば、ロケーション間のリンク経由で音声通話とビデオ通話に使用可能な帯域幅を制限することによって、音声の品質とビデオの可用性を調整することができます。ロケーションは、このロケーションとの間で送受信されるコールで使用可能な帯域幅の合計を指定します。 ドロップダウン リストから、この IVR に適切なロケーションを選択します。 Hub_None のロケーション設定は、ロケーション機能がこの IVR によって消費される帯域幅を追跡しないことを意味します。ロケーションを [ファントム（Phantom）] に設定すると、H.323 プロトコルまたは SIP を使用するクラスタ間トランクの間で正常に CAC を有効にしているロケーションが指定されます。 新しいロケーションを設定するには、**[システム（System）]**>**[ロケーション（Location）]** メニュー オプションを使用します。 クラスタ間トランク経由のロケーション ベースの CAC のセットアップ方法については、『*Cisco Unified Communications Manager* システム設定ガイド』を参照してください。

フィールド	説明
[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 リストで、Unified Communications Manager による、このメディア エンドポイントを使用するトラステッド リレー ポイント（TRP）デバイスの挿入を有効化するか無効化するかを選択します。次の値のいずれかを選択します。 • [オフ（Off）]：当該デバイスでの TRP の使用を無効にする場合は、この値を選択します。 • オン（On）：このデバイスで TRP の使用を有効にするには、この値を選択します。 トラステッドリレーポイント（TRP）デバイスはトラステッドリレーポイントとしてラベル付けされている MTP またはトランスコーダ デバイスを指定します。 エンドポイントに複数のリソース（トランスコーダや RSVPAgent など）が必要な場合、Unified Communications Manager は、関連付けられたエンドポイント デバイスに最も近い TRP を配置します。 TRP と MTP の両方がエンドポイントに必要な場合は、TRP が必須の MTP として使用されます。 エンドポイントに TRP と RSVPAgent の両方が必要な場合、Unified Communications Manager は、TRP としても使用可能な RSVPAgent を検索します。 TRP とトランスコーダの両方がエンドポイントに必要な場合は、Cisco Unified Communications Manager が、TRP としても指定されているトランスコーダを検索します。

IVR パラメータの変更

手順

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。[サービスパラメータ設定（Service Parameter Configuration）] ウィンドウが表示されます。

ステップ 2 サーバを選択し、[Cisco IP Voice Media Streaming App] と呼ばれる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。

ステップ 3 **[自動音声応答 (IVR)]** パラメータセクションの **[コールカウント (Call Count)]** フィールドで、同時メディアストリームの数を入力し、**[保存 (Save)]** をクリックします。

IVR を更新するときに、アクティブアナウンスが再生されていなければ、IVR がアイドル状態になったときに自動的に変更されます。

第 63 章

保留中ビデオサーバの設定

保留中ビデオの概要

保留中ビデオは、ビデオコンタクトセンターに発信する顧客が、コンタクトセンターでエージェントと最初の受け答えを終えた後に、特定のビデオを視聴できるビデオコンタクトセンター向けの機能です。この場合、エージェントが、保留中に顧客に対して再生するビデオストリームを選択します。

保留中ビデオサーバは、Cisco Unified Communications Manager から指示が出されると、オーディオとメディアをストリーミングできるメディア コンテンツ サーバです。メディア コンテンツ サーバは、SIP をシグナリング プロトコルとして使用して、Unified Communications Manager の制御下でオーディオおよびビデオ コンテンツを格納およびストリーミングできる外部デバイスです。メディア コンテンツ サーバでは、1080p や 720p といった高解像度ビデオ コンテンツ、または 360p などの低解像度ビデオ コンテンツを提供できます。Cisco MediaSense は、メディア コンテンツ サーバとして使用されます。

導入に汎用保留中ビデオ機能が必要になる場合、ビデオコンタクトセンターに加え、企業内のどこでも保留中ビデオを導入できます。保留中ビデオサーバの**デフォルトビデオコンテンツ ID**を設定して、保留中のユーザに再生するビデオストリームを識別することができます。

（注） Customer Voice Portal（CVP）による発信者情報の転送を導入するユニファイド コンタクト センターで、保留中ビデオの機能を利用するには、Unified Communications Manager と CVP 間の SIP トランクに保留中ビデオのリソースを割り当てる必要があります。

保留中ビデオ設定のタスク フロー

始める前に

手順

	コマンドまたはアクション	目的
ステップ 1	SIP トランクを MediaSense サーバに作成する （618 ページ）	Cisco MediaSense クラスタに SIP トランクを設定します。
ステップ 2	保留中ビデオサーバの設定 （619 ページ）	MediaSense サーバに保存されているビデオコンテンツを識別する、Cisco Unified Communications Manager にある保留中ビデオサーバを設定します。

SIP トランクを MediaSense サーバに作成する

Unified Communications Manager には、Cisco MediaSense クラスタへの SIP トランクを設定する必要があります。Cisco MediaSense サーバへの SIP トランクには、Cisco MediaSense ノードの IP アドレスが含まれています。Unified Communications Manager SIP トランクは、最大 16 の宛先 IP アドレスをサポートします。

（注） Cisco MediaSense クラスタには、冗長性と拡張性のために 2 個以上のノードが必要です。

SIP トランクにデフォルト設定を設定します。SIP トランク上では、Video on Hold 機能に対応したその他の設定はサポートされていません。

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 4 [デバイスプロトコル（Device Protocol）] ドロップダウン リストから、プロトコルとして [SIP] が入力されていることを確認し、[次へ（Next）] をクリックします。

ステップ 5 [デバイス情報（Device Information）] エリアで、次のフィールドに入力します。

- [デバイス名（Device Name）]：トランクの名前を入力します。
- [説明（Description）]：トランクの説明を入力します。

- デバイス プール（Device Pool）：SIP トランクの適切なデバイス プールを選択します。
- ロケーション（Location）：このトランクの適切なロケーションを選択します。

ステップ 6 [SIP 情報（SIP Information）] エリアで、次のフィールドに入力します。

- 宛先アドレス（Destination Address）：Cisco MediaSense サーバの IP アドレスを入力します。複数の IP アドレスを指定できます。
- 宛先ポート（Destination Port）：ポート番号を入力します。デフォルトのポート番号 5060 を受け入れることを推奨します。複数のポートを指定できます。
- 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 リストから SIP トランク セキュリティ プロファイルを選択します。
- SIPプロファイル（SIP Profile）：ドロップダウン リストから SIP プロファイルを選択します。オプションの ping が設定された SIP プロファイルを選択します。存在しない場合は、作成します。これは必須ではありませんが、ユーザ エクスペリエンスが向上します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

保留中ビデオサーバの設定 （619 ページ）

保留中ビデオサーバの設定

保留中ビデオ サーバの SIP トランクは Cisco MediaSense サーバを指し、デフォルトコンテンツ ID は MediaSense サーバ上に存在するストリーム ID を指します。コンテンツ ID には任意の英数字文字列を指定できます。

始める前に

SIP トランクを MediaSense サーバに作成する （618 ページ）

手順

ステップ 1 **Cisco Unified Communications Manager の管理**ページで、**[メディアリソース(Media Resources)]** > **[保留ビデオサーバ(Video on Hold Server)]** を選択します。

ステップ 2 **[新規追加(Add New)]** をクリックして、新規の保留中ビデオサーバを設定します。

ステップ 3 保留中ビデオサーバの名前を入力します。

ステップ 4 サーバの説明を入力します。

ステップ 5 **デフォルトのビデオコンテンツ ID**の英数字文字列を入力します。

ステップ 6 ドロップダウンリストから、使用する SIP トランクを選択します。SIP トランクを新しく作成する必要がある場合には、**[SIP トランクの作成(Create SIP Trunk)]** ボタンをクリックします。

ステップ 7 [保存（Save）] をクリックします。

保留中ビデオの連携動作

Enhanced Location コールアドミッションコントロール機能では、Cisco MediaSense サーバを Unified Communications Manager クラスタに配置できます（Cisco MediaSense クラスタは、保留側が登録されるクラスタに直接接続されます）。その場合、Unified Communications Manager クラスタが、保留側の場所と Cisco MediaSense の場所の間の帯域幅を差し引く役目を果たします。保留中ビデオの連携動作は 720p または 1080p のビデオ ストリームを利用するので、既存のセッションのビデオ品質を維持するために、新しいセッションを許可する前に帯域幅の使用を考慮に入れることは重要です。

第 64 章

アナウンスの設定

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 *77 : [*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ンス（サンプル）
Welcome_Greeting_Sample	ビルトイン：発信者へのグリーティング（サンプル）

アナウンスの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	アナウンスの設定 （623 ページ）。	保留音（MOH）、発信キューイングまたは外部コール制御などの機能とともに使用できるアナウンスを設定します。
ステップ 2	カスタマイズされたアナウンスのアップロード （624 ページ）。	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します。ただし、アナウンス識別子を変更することはできません。カスタマイズされたアナウンスは、ハイパーリンクに下線が付いており、Cisco Unified Communications Manager の **[アナウンスの検索と一覧表示]** ウィンドウに表示されます。

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 65 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 *78 :* 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 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。

会議ブリッジ タイプ	説明
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
ステップ 1	会議ブリッジの設定 （633 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。
ステップ 2	会議ブリッジのサービスパラメータの設定 （633 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

	コマンドまたはアクション	目的
		ジの両方が含まれている場合は、次の手順を実行します。
ステップ 3	会議ブリッジへの SIP トランク接続の設定 （634 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

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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 （633 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

ステップ 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。

ステップ 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。

ステップ 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）]

ステップ 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

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

ステップ 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。

ステップ 3 [デバイスプロトコル（Device Protocol）] で、[SIP] を選択します。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 8 [保存（Save）] をクリックします。

第 66 章

フレキシブル DSCP マーキングおよびビデオ プロモーションの設定

フレキシブル DSCP マーキングとビデオプロモーションの概要

デバイスおよびアプリケーションは、DiffServ コードポイント（DSCP）マーキングを使用し、IP 通信の Quality of Service（QoS）処理を示します。たとえば、デスクトップ ビデオ エンドポイントはビデオ メディア ストリームにマルチメディア会議 AF41 マーキングを使用し、その一方、高解像度のビデオ ルーム システムはリアルタイム インタラクティブ CS4 マーキングを使用することがあります。アプリケーションが同じタイプのアプリケーションとの間で IP 通信を送受信するとき、DSCP マーキングは対称であり、それぞれのアプリケーションが送受信する IP 通信の QoS 処理は同じです。ただし、アプリケーションが異なるタイプのアプリケーションとの間でメディアを送受信する場合には、DSCP マーキングは非対称であり、それぞれのアプリケーションが送受信する IP 通信の QoS 処理は一貫しません。たとえば、ビデオ ルーム システムがデスクトップ ビデオ エンドポイントから受信する QoS 処理は、ビデオ ルーム システムで必要とされる品質をサポートするには不十分であることがあります。

デバイスやアプリケーションは、確立されたセッション中に十分な帯域幅を確保するため、コール アドミッション制御（CAC）に従います。確立されたセッションによって利用される帯域幅は、セッションの開始時と終了時に更新されます。新しいセッションを確立しようとする際、そのセッションによって利用可能な帯域幅を超える場合には、そのセッションがブロックされます。利用可能な帯域幅は、デバイスや異なるタイプのアプリケーションごとに個別に追跡できます。たとえば、ビデオ メディア ストリームを送受信するデスクトップ ビデオ エン

ドポイントと高解像度ビデオ ルーム システムについて、帯域幅を個別に追跡することができます。

同じタイプのデバイスやアプリケーションが通信を送受信すると、各方向で同じタイプの帯域幅削減が行われます。ただし、異なるタイプのデバイスやアプリケーションが通信を送受信する場合には、各方向で異なるタイプの帯域幅削減を行う必要があります。また帯域幅削減の量は、IP ネットワークの通常の動作を反映し、通常、計画的に対称となります。その結果、異なるタイプのデバイスやアプリケーションが通信を送受信すると、帯域幅削減の合計が、実際に利用されているネットワーク量の最大2倍にまで達することがあります。帯域幅におけるこの計算の不一致により、新しいセッションを確立しようとしても、不必要にブロックされてしまうことがあります。

フレキシブル DSCP マーキングとビデオプロモーション機能を使用すると、ビデオプロモーションポリシーを設定して、帯域幅アカウンティングの不整合を調整し、より好ましい CAC および QoS の取り扱いを受信するアプリケーションが優先されます。たとえば、デスクトップ ビデオ エンドポイントと高解像度ビデオ ルーム システムの間のセッションがビデオ ルーム システムを優先して調整される場合、その調整はデスクトップ ビデオ エンドポイントのプロモーションと見なされます。

異なるタイプのデバイスとアプリケーションの間で調整が行われている場合、調整で優先されているアプリケーションのタイプについてのみ帯域幅が削減されます。このタイプの承認対象のセッションに対して充分な帯域幅がある場合には、調整で優先されていないタイプのデバイスまたはアプリケーションは、使用する DSCP マーキングを、調整で優先されるタイプのアプリケーションで使用されるマーキングに変更するように指示を受けます。たとえば、デスクトップ ビデオ エンドポイントが、高解像度ビデオ ルーム システムとのセッションでプロモートされると、そのデスクトップ ビデオ エンドポイントがビデオ ルーム システムと同じタイプのアプリケーションであるものとして帯域幅計算が行われます。デスクトップ ビデオ エンドポイントは、その DSCP マーキングを、ビデオ ルーム システムで使用されるものに変更するように指示を受けます。QoS 処理は両方向において一致します。帯域幅は、ビデオ ルーム システムと同じタイプのデバイスやアプリケーションの間のセッションに対して削減され、デスクトップ ビデオ エンドポイントと同じタイプのデバイスやアプリケーションの間のセッションに対しては削減されません。

フレキシブル DSCP マーキングとビデオプロモーション機能がアクティブになっていると、Unified Communications Manager は、ネゴシエートされた各メディアストリームを示すトラフィッククラスラベルをデスクトップビデオデバイスに動的に伝達します。

ユーザに対するカスタム QoS の設定

SIP プロファイル内の [サービス品質（QoS）（Quality of Service (QoS)）] 設定をカスタマイズして、それらの設定をユーザに適用することができます。[SIP プロファイル設定（SIP Profile Configuration）] ウィンドウは、次の QoS 設定で拡張されています。

- オーディオとビデオ ストリームのカスタム DSCP 値
- オーディオとビデオ ストリームのカスタム UDP ポート範囲

オーディオとビデオのカスタム DSCP 値

SIP プロファイル内のオーディオとビデオ コール用 DSCP 値を設定し、そのプロファイルを使用する SIP 電話に適用できます。[SIP プロファイル設定（SIP Profile Configuration）] ウィンドウには、次のタイプのコール用にカスタム DSCP の設定が含まれています。

- 音声通話
- ビデオ コール
- ビデオ コールの音声部分
- TelePresence コール
- TelePresence コールの音声部分

営業チームや CEO など、大半の従業員よりも QoS の優先順位の高い設定を必要とする一団が社内にいる場合、SIP プロファイル設定を使用して、これらのユーザのカスタム DSCP 値を設定できます。SIP プロファイル内の設定は、対応するクラス全体のサービス パラメータ設定を上書きします。

オーディオとビデオのカスタム UDP ポート範囲

SIP コールのオーディオ ストリームとビデオ ストリームに対して、個々に UDP ポート範囲を設定できます。通常、ビデオにはオーディオよりもかなり多くの帯域幅が必要であるため、メディアのタイプごとに専用のポート範囲を使用することで、ネットワーク帯域幅の管理を簡素化できます。また、オーディオ ストリームが広帯域幅のビデオ ストリームから分離された専用チャネルを持つことを保証することにより、オーディオストリームの劣化を防ぐことができます。

SIP ファイルの [メディア ポート範囲（Media Port Ranges）] フィールドを設定すれば、この設定を [オーディオとビデオに個別のポート範囲（Separate Port Ranges for Audio and Video）] に適用できます。SIP プロファイルを電話に関連付けて、設定を電話に適用できます。

トラフィック クラス ラベル

フレキシブル DSCP とビデオ プロモーション機能は、ビデオ プロモーション ポリシーに基づき、トラフィック クラス ラベル（TCL）を使用して動的に SIP エンドポイントを指示し、その DSCP をコールごとにマークします。TCL はメディア回線ごとに定義された SIP Session Description Protocol（SDP）属性のため、TCL とその関連 DSCP マーキングは、ビデオ コールのオーディオ メディア回線とビデオ メディア回線で異なることがあります。ビデオコールのオーディオ ストリームとビデオ ストリームに異なる DSCP マーキングを選択できます。

DSCP 設定の設定タスク フロー

次のタスクを実行して、ネットワークの DSCP 値とビデオプロモーションポリシーを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	フレキシブル DSCP マーキングおよびビデオ プロモーション ポリシーの設定（638 ページ）	さまざまなタイプのビデオを処理するビデオプロモーションポリシーを設定します。
ステップ 2	ユーザのカスタム QoS ポリシーの設定（640 ページ）	御社に社内の他のユーザよりも高い優先順位を必要とするユーザが存在する場合は、オーディオストリームとビデオストリームのカスタム DSCP 値を含む SIP プロファイルを設定します。たとえば、社内に高い優先順位を必要とする電話営業部隊または CEO がいる場合は、それらのユーザの電話機にカスタマイズされた SIP プロファイルを適用できます。

フレキシブル DSCP マーキングおよびビデオ プロモーション ポリシーの設定

以下の手順に従いさまざまなタイプのビデオを処理するビデオプロモーションポリシーを設定します。

手順

ステップ 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。

ステップ 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。

ステップ 3 [サービス（Service）] ドロップダウン リストで、[Cisco CallManager（アクティブ）（Cisco CallManager (Active)）] サービスを選択します。

サービスが「Active」と表示されていない場合は、そのサービスを Cisco Unified Serviceability でアクティブにします。

ステップ 4 デスクトップビデオエンドポイントをイマーシブビデオエンドポイントにプロモートするビデオ プロモーションポリシーを設定するには、**Use Video BandwidthPool for Immersive Video Calls** パラメータを **[False]** に設定し、**Video Call QoS Marking Policy** パラメータを **[Promote to Immersive]** に設定します。

ステップ 5 パラメータを設定するには、**[サービスパラメータ設定(Service Parameter Configuration)]** ウィンドウで該当の領域にスクロールし、パラメータ値を更新します。サービスパラメータとその設定オプションの詳細については、「フレキシブル DSCP マーキングおよびビデオ プロモーション サービス パラメータ （639 ページ）」を参照してください。

ステップ 6 [保存（Save）] をクリックします。

フレキシブル DSCP マーキングおよびビデオ プロモーション サービス パラメータ

（注） サービス パラメータについては、パラメータ名をクリックするか、**[サービスパラメータ設定(Service Parameter Configuration)]** ウィンドウに表示される疑問符（?）アイコンをクリックしてください。

表 *79 :* フレキシブル *DSCP* マーキングおよびビデオ プロモーション サービス パラメータ

パラメータ	説明
クラスタ全体のパラメータ（システム - QoS）	サービスパラメータのこのセクションには、さまざまなオーディオおよびビデオコールタイプのクラスタ全体の DSCP 値が含まれています。これには、音声通話の DSCP、ビデオコールのオーディオ部分、TelePresence コール、TelePresence コールのオーディオ部分などさまざまなオーディオとビデオコールが含まれています。 別途、シスコのサポートエンジニアからの指示がない限り、これらのパラメータをデフォルトのままにしておくことを強く推奨します。
クラスタ全体のパラメータ (コールアドミッションコントロール)	
Video Call QoS Marking Policy	このパラメータを使用すると、デスクトップ ビデオ エンドポイントと Cisco TelePresence イマーシブ ビデオ エンドポイントの間の帯域幅割り当ての不一致をイマーシブ エンドポイントを優先して調整するように、Promote to Immersive ポリシーを設定できます。プロモーションが実行されると、オーディオおよびビデオ帯域幅はイマーシブ帯域幅プール割り当てから予約されます。Promote to Immersive ポリシーは、フレキシブル DSCP マーキングをサポートするイマーシブ ビデオ デバイスとデスクトップ ビデオ デバイスの間のコールでのみ適用されます。
[Clusterwide Parameters (System - Location and Region)]	
Default Intraregion Max Immersive Video Call Bit Rate（Includes Audio）	このパラメータは、リージョンとそれ自体の関係の **[リージョンの設定(Region Configuration)]** ウィンドウで、**最大イマーシブビデオコールビットレート**として **[システムデフォルトの使用(Use System Default)]** オプションが選択された場合に、特定のリージョン内の各イマーシブビデオコールのデフォルトの最大合計ビットレートを指定します。

パラメータ	説明
Default Interregion Max Immersive Video Call Bit Rate（Includes Audio）	このパラメータは、そのリージョンと別のリージョンの関係の **[リージョンの設定(Region Configuration)]** ウィンドウで、**最大イマーシブビデオコールビットレート**として **[システムデフォルトの使用(Use System Default)]** オプションが選択された場合に、特定のリージョンと別のリージョンの間の各イマーシブビデオ コールのデフォルトの最大合計ビット レートを指定します。
Use Video BandwidthPool for Immersive Video Calls	このパラメータは、Unified Communications Manager がイマーシブ ビデオ コールのデスクトップ ビデオ帯域幅プールから帯域幅を予約するかどうかを指定します。

ユーザのカスタム QoS ポリシーの設定

次のタスクを実行して、ユーザのカスタムサービス品質 (QoS) ポリシーを設定します。電話のセールスや CEO など、社内のそれ以外の人々と異なる QoS 要件を持つユーザがいる場合は、カスタムポリシーを適用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
ステップ 1	カスタム QoS 設定を SIP プロファイルで設定する （640 ページ）	オーディオおよびビデオストリームのカスタマイズされた DSCP 値と UDP ポート範囲を使用して、SIP プロファイルを設定します。
ステップ 2	電話機へのカスタム QoS ポリシーの適用 （641 ページ）	電話機に SIP プロファイルを適用します。SIP プロファイルの DSCP 設定は、DSCP クラスタ全体のサービスパラメータ設定を上書きします。

カスタム QoS 設定を SIP プロファイルで設定する

この SIP プロファイルを使用する電話機に対して、カスタム DSCP 値と UDP ポート範囲を設定します。これらの設定を使用して、ネットワーク内の特定の電話機とユーザに適用できる QoS ポリシーをカスタマイズできます。営業または CEO など、社内の特定のユーザに特定の QoS 設定を適用する場合は、この方法を使用することができます。

手順

ステップ 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。

ステップ 2 次のいずれかの手順を実行します。

- 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。
- 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。

ステップ 3 [メディア ポートの範囲（Media Port Ranges）] フィールドで、オーディオ メディアおよびビデオ メディアの両方に対応する単一の UDP ポート範囲、またはオーディオ ストリームおよびビデオ ストリームそれぞれに対応するポート範囲のどちらを割り当てるかを選択します。

- オーディオ メディアおよびビデオ メディアに 1 つのポート範囲を設定するには、[開始メディア ポート（Start Media Port）] および [終了メディアポート（Stop Media Port）] フィールドにポート範囲を入力します。有効なポートは 2048 ～ 65535 です。
- オーディオストリームおよびビデオストリームにそれぞれポート範囲を設定する場合は、[開始メディア ポート（Start Media Port）] および [終了メディアポート（Stop Media Port）] フィールドを使用して、オーディオ ポートの範囲を入力します。[開始メディア ポート（Start Media Port）] および [終了メディアポート（Stop Media Port）] フィールドを使用して、ビデオ ポートの範囲を入力します。各ポートの有効な値は、 2048 ～ 65535 です。2 つのポート範囲を重複させることはできません。

ステップ 4 次のフィールドで、オーディオ ストリームおよびビデオ ストリーム用にカスタマイズされた DSCP 値を設定します。

- [オーディオ コールの DSCP（DSCP for Audio Calls）]
- [ビデオ コールの DSCP（DSCP for Audio Calls）]
- [ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）]
- [TelePresence コールの DSCP（DSCP for TelePresence Calls）]
- [TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）]

（注） デフォルトでは、上記の各フィールドは、対応するサービスパラメータの値を使用するように設定されています。新しい値を割り当てると、サービスパラメータ設定は新しい値に上書きされます。

ステップ 5 [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。

ステップ 6 [保存（Save）] をクリックします。

電話機へのカスタム QoS ポリシーの適用

DSCP 値や、音声およびビデオ メディアの UDP ポート範囲などのカスタマイズされた QoS 設定を含む SIP プロファイルを適用するには、次の手順を使用します。この SIP プロファイルを電話機に適用すると、電話機は SIP プロファイルのカスタム設定を使用します。

手順

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

ステップ 2 次のいずれかの手順を実行します。

- 既存の電話機を選択するには、[検索（Find）] をクリックします。
- 新しい電話機を作成するには、[新規追加（Add New）] をクリックします。

ステップ 3 **[SIP プロファイル（SIP Profile）]** ドロップダウン リストから、カスタム DSCP 値と UDP ポート範囲の値を設定する SIP プロファイルを選択します。

ステップ 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。

ステップ 5 [保存（Save）] をクリックします。

フレキシブル DSCP マーキングとビデオプロモーションの連携動作と制限事項

次の操作を実行できます。

- フレキシブル DSCP マーキングとビデオ プロモーションの連携動作 （642 ページ）
- フレキシブル DSCP マーキングおよびビデオ プロモーションの制約事項 （643 ページ）

フレキシブル DSCP マーキングとビデオ プロモーションの連携動作

表 *80 :* フレキシブル *DSCP* マーキングとビデオ プロモーションの連携動作

デバイス	データのやり取り
SIP クラスタ間トランク	フレキシブル DSCP マーキングとビデオ プロモーション機能は、SIP クラスタ間経由でサポートされます。
Skinny Client Control Protocol （SCCP） デバイス	フレキシブル DSCP マーキングとビデオプロモーション機能は、SCCP デバイスでサポートされています。
パススルー MTP	パススルー MTP がコールに挿入されると、Unified Communications Manager は、ビデオ ストリームのパケットを最初に発したエンドポイント デバイスから求められる DSCP マーキングで、パケットをマークするように MTP に信号を送ります。1 つのコール内の 2 つのエンドポイントで異なる DSCP マーキングが使用されている場合（たとえば、Cisco TelePresence イマーシブ ビデオ エンドポイントとビデオ プロモーションなしのデスクトップ ビデオエンドポイントなど）には、MTP は各ストリーム方向で DSCP マーキングを保持します。

フレキシブル DSCP マーキングおよびビデオ プロモーションの制約事項

表 *81* : フレキシブル *DSCP* マーキングおよびビデオ プロモーションの制約事項

制限事項	説明
トランクおよびゲートウェイ	フレキシブルDSCPマーキングとビデオプロモーション機能は、H.323トランクやMedia Gateway Control Protocol（MGCP）ゲートウェイ経由ではサポートされません。
Multilevel Precedence and Preemption	シスコでは、フレキシブル DSCP マーキングとビデオ プロモーション機能を Multilevel Precedence and Preemption（MLPP）サービス コールで使用しないようにお勧めしています。MLPPサービス機能が必要な場合には、シスコでは、Video Call QoS Marking Policy および Use Video BandwidthPool for Immersive Video Calls サービス パラメータをそれぞれのデフォルト値に設定することを推奨しています。Video Call QoS Marking Policy および Use Video BandwidthPool for Immersive Video Calls サービス パラメータのデフォルト値を使用すると、Unified Communications Managerとエンドポイントはメディア パケットにMLPP DSCP マーキングを使用します。
SIP ビデオ エンドポイント	フレキシブルDSCPマーキングおよびビデオプロモーション機能は、デスクトップSIPビデオエンドポイントのサポートによって異なります。現在、Cisco DX650 シリーズの SIP 電話のみが、必要なエンドポイントのサポートを提供しています。

第 67 章

トランスコーダとメディアターミネーション ポイントの設定

トランスコーダとメディアターミネーションポイントの概要

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。

（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。

トランスコーダおよびメディアリソースマネージャ

Cisco Unified Communications Manager ノードはすべて、メディア リソース マネージャ（MRM）を使用してトランスコーダにアクセスできます。MRM は、トランスコーダへのアクセスを管理します。

MRM は、Cisco Unified Communications Manager のメディア リソース グループとメディア リソース グループ リストを使用します。メディア リソース グループ リストによって、トランスコーダは、割り当てられたメディア リソース グループ内の他のデバイスと通信できるようになります。さらにこれにより、クラスタ内のリソースの管理が可能になります。

トランスコーダ制御プロセスは、データベースで定義されている各トランスコーダ デバイスに対して作成されます。MRM はトランスコーダ リソースを追跡し、クラスタ全体にその可用性をアドバタイズします。

メディアターミネーションポイントとしてのトランスコーダ

ハードウェアベースのトランスコーダリソースは、メディアターミネーションポイント（MTP）および/またはトラストリレーポイント (TRP) 機能にも対応しています。この機能では、コール内の 1 つのエンドポイントが MTP または TRP を要求していることを Cisco Unified Communications Manager が判別すると、Cisco Unified Communications Manager はトランスコーダ リソースを割り当て、コールに挿入することができます。このトランスコーダは、MTP トランスコーダのように動作します。

Cisco Unified Communications Manager は、MTP および TRP とトランスコーディング機能を同時にサポートします。たとえば、コールが（G723 リージョンに存在する）Cisco Unified IP Phone から（G711 リージョンに存在する）NetMeeting に発信された場合、1 つのトランスコーダ リソースが MTP とトランスコーディング機能を同時にサポートします。

ソフトウェア MTP リソースが必要なときに使用できない場合、コールは MTP リソースおよび MTP/TRP サービスを使用せずに接続しようとします。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。

（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。

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 *82*：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）	

トランスコーダタイプ	説明
	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

トランスコーダ タイプ	説明
	ディング
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）

トランスコーダのフェールオーバーとフォールバック

次に、トランスコーダが登録されている Cisco Unified Communications Manager ノードが非アクティブになったときの、トランスコーダ デバイスの回復方法について説明します。

- プライマリ Cisco Unified Communications Manager ノードに障害が発生した場合、トランスコーダは、トランスコーダの属するデバイス プールに対して指定された Cisco Unified Communications Manager グループ内で、次に使用可能なノードへの登録を試みます。
- 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 Cisco Unified Communications Manager ノードから登録解除されます。そのノード上のコールが、リスト内の次の Cisco Unified Communications Managerノードに登録されます。
- トランスコーダが新しい Cisco Unified Communications Manager ノードへの登録を試み、登録確認応答を受信しなかった場合、トランスコーダはリストにある次のノードに登録されます。

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。

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）により、Cisco Unified Communications Manager は SIP や H.323 エンドポイントまたはゲートウェイ経由でルーティングされるコールを中継できます。メディア ターミネーション ポイントは、コール保留、コール転送、コール パーク、会議などの補足サービスを拡張します。これらのサービス通常は、コールが H.323 エンドポイントにルーティングされる場合は、MTP がないと使用できません。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 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。

MTP フェールオーバーおよびフォールバック

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。

ソフトウェアメディアターミネーションポイントタイプ

Cisco Unified Communications Manager の管理におけるソフトウェアメディアターミネーションポイントのタイプは次の表のとおりです。

ソフトウェア MTP タイプ	[説明（Description）]
Cisco Media Termination Point Software	1 つの MTP は、デフォルトで 48（ユーザ設定可能）の MTP リソースを提供します。この数は、ネットワークとネットワーク インターフェイス カード（NIC）の速度に応じて変わります。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、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、その 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、ネットワークの負荷、その他のさまざまな要因によって決まります。

トランスコーダと MTP 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
ステップ 1	トランスコーダの設定 （653 ページ）には、以下のサブタスクを実行します： • トランスコーダの設定 （653 ページ） • メディア リソース グループへのトランスコーダの追加 （654 ページ）	トランスコーダを設定する必要がある場合は、この手順を実行します。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する出力ストリームに変換します。

	コマンドまたはアクション	目的
ステップ 2	ソフトウェア MTP の設定 （655 ページ）には、以下のサブタスクを実行します： • メディア ターミネーション ポイントの設定 （656 ページ） • ソフトウェア MTP をメディア リソース グループに追加する （657 ページ）	ソフトウェアの MTP を設定する必要がある場合は、この手順を実行します。ソフトウェア MTP を使用すれば、Cisco Unified Communications Manager は、SIP または H.323 エンドポイントまたはゲートウェイ経由でルーティングされた発信を中継することができます。

トランスコーダの設定

手順

	コマンドまたはアクション	目的
ステップ 1	必要なトランスコーダ リソースの数と、これらのリソースの提供に必要なトランスコーダ デバイスの数を判別します。	マルチサイト配置の場合は、トランスコーダを必要な各サイトにローカルに配置することを推奨します。複数のコーデックが必要な場合は、すべてのコーデックをサポートしないエンドポイントの数、これらのエンドポイントを配置する場所、これらのリソースにアクセスする他のグループ、これらのデバイスがサポートする同時コールの最大数、およびネットワーク上でこれらのリソースを配置する場所を検討する必要があります。
ステップ 2	トランスコーダの設定 （653 ページ）	1 つの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するために、トランスコーダを設定します。
ステップ 3	メディア リソース グループへのトランスコーダの追加 （654 ページ）	新しいトランスコーダを適切なメディア リソース グループに追加します。
ステップ 4	トランスコーダ デバイスを再起動します。	詳細については、トランスコーダのドキュメンテーションを参照してください。

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

ステップ 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。

ステップ 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。

ステップ 3 [トランスコーダタイプ（Transcoder Type）] を選択します。

ステップ 4 トランスコーダの [MACアドレス（MAC Address）] を入力します。

ステップ 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。

ステップ 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。

ステップ 7 [保存（Save）] をクリックします。

メディア リソース グループへのトランスコーダの追加

始める前に

トランスコーダの設定 （653 ページ）

手順

ステップ 1 **[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。

ステップ 2 [検索（Find）] をクリックして、設定されたメディア リソース グループのリストを表示します。

ステップ 3 必要なメディア リソース グループをクリックします。
[メディアリソースグループの設定（Media Resource Group Configuration）] ウィンドウが表示されます。

ステップ 4 トランスコーダを [使用可能なメディア リソース（Available Media Resources）] のリストから選択し、[選択されたメディア リソース（Selected Media Resources）] のリストに追加します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **[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）]** に移動します。

ステップ 7 [トランスコーダの検索と一覧表示（Find and List Transcoders）] ウィンドウで、同期させるトランスコーダの隣にあるチェックボックスをオンにします。ウィンドウ内のトランスコーダ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。

ステップ 8 [選択項目への設定の適用（Apply Config to Selected）] をクリックします。
[設定情報の適用（Apply Configuration Information）] ダイアログ ボックスが表示されます。

ステップ 9 [OK] をクリックします。

次のタスク

トランスコーダ デバイスを再起動します。

トランスコーダの同期化

トランスコーダを最新の設定変更と同期させる手順は、次のとおりです。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、影響を受けるデバイスの一部は、リセットまたはリスタートが不要な場合があります）。

手順

ステップ 1 **[メディアリソース(Media Resources)] > [トランスコーダ(Transcoder)]** を選択します。
[トランスコーダの検索と一覧表示(Find and List Transcoders)] ウィンドウが表示されます。

ステップ 2 使用する検索条件を選択します。

ステップ 3 [検索（Find）] をクリックします。

検索条件に一致するトランスコーダがウィンドウに表示されます。

ステップ 4 同期させるトランスコーダの横にあるチェックボックスをオンにします。ウィンドウ内のトランスコーダ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。

ステップ 5 [選択項目への設定の適用（Apply Config to Selected）] をクリックします。
[設定情報の適用（Apply Configuration Information）] ダイアログ ボックスが表示されます。

ステップ 6 [OK] をクリックします。

ソフトウェア MTP の設定

この手順はソフトウェアを設定する手順について説明しています。ハードウェア MTP の設定については、「トランスコーダの設定 （653 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
ステップ 1	メディア ターミネーション ポイントの設定 （656 ページ）	SIP エンドポイントまたはゲートウェイ経由でルーティングされたコールをリレーするには、メディア ターミネーション ポイントを設定します。
ステップ 2	ソフトウェア MTP をメディア リソース グループに追加する （657 ページ）	適切なメディア リソース グループに新しいメディア ターミネーション ポイントを追加します。
ステップ 3	メディア ターミネーション ポイントのデバイスを再起動します。	

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 **デバイスプール**を割り当てます。

ステップ 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。

ステップ 6 [保存（Save）] をクリックします。

ソフトウェア MTP をメディアリソースグループに追加する

始める前に

メディア ターミネーション ポイントの設定 （656 ページ）

手順

ステップ 1 **[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。

ステップ 2 [検索（Find）] をクリックして、設定されたメディア リソース グループのリストを表示します。

ステップ 3 必要なメディア リソース グループをクリックします。
[メディアリソースグループの設定（Media Resource Group Configuration）] ウィンドウが表示されます。

ステップ 4 **利用可能なメディアリソース**のリストからトランスコーダを選択し、**[選択されたメディアリソース]** リストに追加します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

メディアターミネーションポイントデバイスを再起動します。

トランスコーダおよび MTP 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

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。

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 *83 :* 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。
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。

第 IX 部

デバイスの登録

第 68 章

デバイスの登録の概要

デバイスの登録について

このセクションの各章では、新規エンドポイントデバイスの登録と、エンドポイントとゲートウェイデバイス用のプロキシ TFTP サーバの設定を行うために実行するタスクについて説明します。

新しい電話機を手動で登録するか、または自動登録を使用するかを選択できます。100 台を超える電話機を登録するには、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 Bulk Administration* 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。

（注） BAT を使用して新しい設定を作成することはできませんが、BAT を使用して電話機を登録する場合は、電話のパラメータを設定できます。デバイス プール、場所、コーリング サーチスペース、ボタンテンプレート、ソフトキーテンプレートなどの電話設定が Cisco Unified Communications Manager Administration を使用してすでに設定済みであることを確認します。

デバイスの登録

次のタスク フローを実行すると、システムのデバイスを登録できます。

手順

	コマンドまたはアクション	目的
ステップ 1	TFTP サーバの設定タスク フロー （669 ページ）	ネットワークのエンドポイントの設定ファイルを提供するプロキシ Trivial File Transfer Protocol（TFTP）サーバを設定します。
ステップ 2	（任意） デバイスのデフォルトの更新タスク フロー （675 ページ）	デバイスのロード、デバイスプール、および電話ボタンのテンプレート値を、登録時にエンドポイントに適用される値に変更します。
ステップ 3	自動登録の設定タスク フロー （680 ページ）	ネットワークの自動登録を有効にします。デバイスをネットワーク上で自動的に登録できるという本質的なセキュリティリスクがあるため、新しいエンドポイントを登録したらすぐに自動登録を無効にすることを推奨します。
ステップ 4	手動によるデバイス登録タスク フロー （689 ページ）	手動で IP 電話を登録し、新しいディレクトリ番号を割り当てます。
ステップ 5	セルフプロビジョニングの設定タスク フロー （695 ページ）	（省略可）エンドユーザが、管理者を使用せずに自身の電話機をプロビジョニングできるようにするには、セルフプロビジョニングを設定します。

第 69 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設定ファイル(ダイヤルプラン、着信音ファイル、デバイス設定ファイルなど)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、設定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設定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。

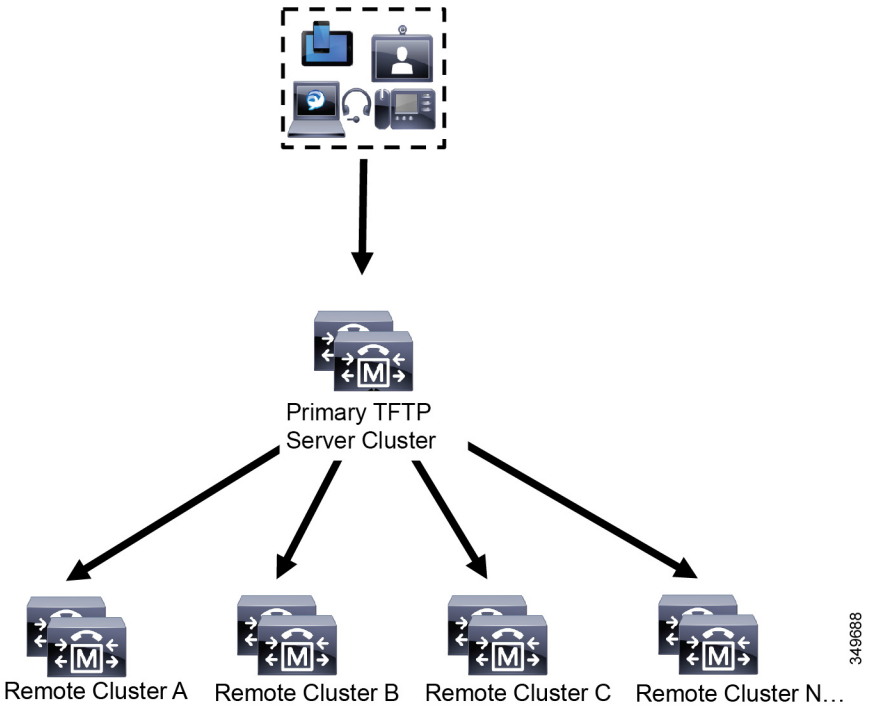
ヒント　ネットワーク内のリモートプロキシTFTPサーバ間にピア関係を設定する場合は、関係を階層構造にしておきます。ループの発生を回避するために、リモートクラスタ上のピアプロキシTFTPサーバが相互にポイントしないようにします。たとえば、プライマリノードAにノードBとCのピアリレーションシップがあるとします。ノードBとCの間にピア関係を作成しないでください。作成すると、ループが作成されます。

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 *5:* 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、設定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設定ファイル

SCCP 電話機、SIP 電話およびゲートウェイは、初期化時に設定ファイルを要求します。デバイス設定を変更すると、更新された設定ファイルがエンドポイントに送信されます。

設定ファイルには、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設定ファイルには、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。ゲートウェイ用の設定ファイルには、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
ステップ 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（670 ページ） • TFTP サーバの手動設定 （671 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。
ステップ 2	（任意） TFTP サーバの CTL ファイルの更新 （672 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。

	コマンドまたはアクション	目的
ステップ 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。
ステップ 4	（任意） TFTP サーバの非設定ファイルの変更 （672 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設定ファイルを変更できます。
ステップ 5	（任意） TFTP サービスの停止と開始（673 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。
ステップ 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。

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 サーバからの設定ファイル

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。

手順

ステップ 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。

ステップ 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。

ステップ 3 [TFTP] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 サーバからの設定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設定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

ステップ 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）]**

ステップ 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。

ステップ 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。

ステップ 4 TFTP サーバをリブートします。

TFTP サーバの非設定ファイルの変更

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

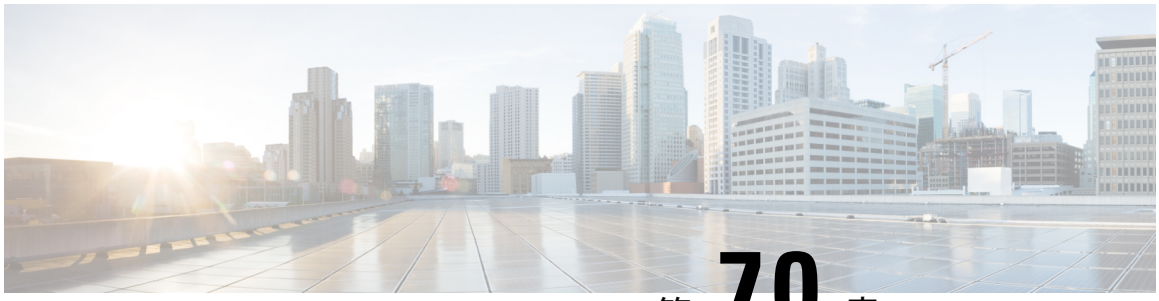
ステップ 3 [CMサービス（CM Services）] 領域で TFTP サービスを選択し、[停止（Stop）] をクリックします。

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。

ステップ 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 70 章

デバイスのデフォルトの更新

デバイスのデフォルトの概要

Cisco Unified Communications Managerノードに登録されている各デバイスは、その種類のデバイスのデフォルトで設定されています。デバイスのデフォルトは、クラスタ内のすべての自動登録デバイスに適用されます。登録後に、デバイスの設定を変更することができます。

新しいデバイスのデフォルトを作成したり既存のものを削除したりすることはできませんが、自動登録されるデバイスに適用されるデフォルトの設定を変更することはできます。

これらは、変更可能なデバイスのデフォルト設定です。

- デバイス ロード
- デバイス プール
- 電話ボタン テンプレート

Cisco Unified Communications Manager をインストールすると、デバイスのデフォルトが自動的に設定されます。

デバイスのデフォルトの更新タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	デバイスのデフォルト設定の更新 （676 ページ）	Cisco Unified Communications Manager ノードに自動登録され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。

	コマンドまたはアクション	目的
		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。

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）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

ステップ 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。

ステップ 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）

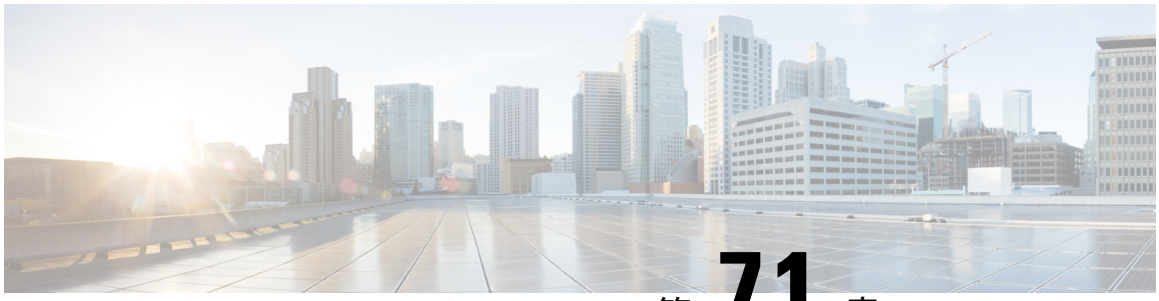
ステップ 3 そのタイプのすべてのデバイスをリセットして、クラスタ内の全ノードにある該当するタイプのすべてのデバイスに新しいデフォルトをロードするには、デバイス名の左側にある [リセット（Reset）] アイコンをクリックします。

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。

デバイスのデフォルトの設定項目

表 *84 :* デバイスのデフォルトの設定項目

フィールド名	説明
デバイスタイプ（Device Type）	このフィールドには、デフォルトが適用されるデバイスのタイプが表示されます。
[プロトコル（Protocol）]	このフィールドには、このタイプのデバイスに使用されるプロトコルが表示されます。
[ロード情報（Load Information）]	ハードウェアデバイスの特定のタイプに使用されるファームウェア ロードの ID 番号を入力します。アップグレード ロードかパッチ ロードをインストールする場合は、新しいロードを使用する各タイプのデバイスのロード情報を更新する必要があります。
[デバイスプール（Device Pool）]	各タイプのデバイスに関連付けられているデバイスプールを選択します。デバイス プールは、そのプールに含まれるすべてのデバイスに共通の特性を定義します。
[電話テンプレート（Phone Template）]	各タイプの Cisco IP Phone が使用する電話ボタンテンプレートを選択します。このテンプレートは、電話機のキーの機能を定義します。



第 71 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 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* 一括管理ガイド』（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
ステップ 1	自動登録のパーティションの設定 （681 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。
ステップ 2	自動登録用コーリングサーチスペースの設定 （682 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。
ステップ 3	自動登録用デバイスプールの設定 （683 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。
ステップ 4	自動登録のデバイスプロトコルタイプの設定 （684 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。
ステップ 5	自動登録の有効化 （684 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。
ステップ 6	自動登録の無効化 （687 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。
ステップ 7	自動登録番号の再利用 （687 ページ）	（省略可）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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （682 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 （681 ページ）

手順

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （683 ページ）

関連トピック

サービスクラス （140 ページ）

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 （682 ページ）

手順

ステップ 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。

ステップ 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。

ステップ 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 （684 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 （683 ページ）

手順

ステップ 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。

ステップ 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 （684 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 （684 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （684 ページ）

手順

ステップ 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。

ステップ 2 ノードのリストから **Cisco Unified Communications Manager**を選択します。

ステップ 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

（省略可）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 （687 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

ステップ 1 Cisco Unified Communications Manager Administration で、**[システム（System）]** > **[Cisco Unified Communications Manager]** を選択します。

ステップ 2 自動登録をリセットするには、[Cisco Unified Communications Manager] を選択します。

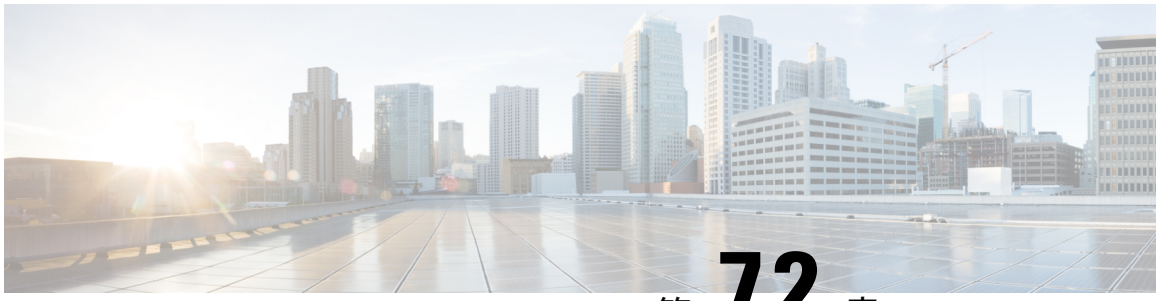
ステップ 3 現在の設定を [開始のディレクトリ番号（Starting Directory Number）] と [最後のディレクトリ番号（Ending Directory Number）] フィールドに書き留めます。

ステップ 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。

ステップ 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 72 章

電話機の手動登録

電話機の手動登録の概要

新しい Cisco IP Phone を手動で登録するには、Unified Communications Manager を使用して、その電話機を Unified Communications Manager ノードに追加してから、電話機のディレクトリ番号を設定する必要があります。

新しい電話機が Unified Communications Manager ノードの場所を確認できるように、プロキシ TFTP サーバーの IP アドレスを使用して新しい電話機を設定しておく必要があります。ご使用の電話機シリーズの『*Cisco IP Phone* アドミニストレーション ガイド』を参照してください。

手動によるデバイス登録タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ご使用の電話機シリーズの『*Cisco IP* 電話アドミニストレーション ガイド』を参照してください。	新しい電話が Unified Communications Manager ノードの検出方法を理解できるように、プロキシ TFTP サーバの IP アドレスを使用して新しい電話機を設定します。
ステップ 2	システムへの電話機の手動での追加 （690 ページ）	電話機をUnified Communications Manager ノードに追加します。
ステップ 3	電話機のディレクトリ番号の手動設定 （690 ページ）	電話機の電話番号を追加し、電話番号のある基本設定を行います。

システムへの電話機の手動での追加

Cisco Unified Communications Managerノードに新しい電話機を手動で追加します。

手順

ステップ 1 [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] で、**[デバイス（Device）]** > **[電話（Phone）]** を選択し、**[新規追加（Add New）]**をクリックします。

ステップ 2 **[新しい電話を追加]**ウィンドウで、**電話機のタイプ**フィールドから電話機の機種を選択してから、**[次へ (Next)]** をクリックします。

ステップ 3 **[電話の設定** (Phone Configuration)] ウィンドウで、**[デバイスプロトコルの選択]** フィールドでデバイスのプロトコルタイプを選択し、**[次へ (Next)]** をクリックします。

ステップ 4 **[デバイス情報]** 領域で、次の操作を実行します。

a) **[デバイス名（Device Name）]** フィールドに名前を入力します。

ここに入力する名前は、電話機で設定されているデバイス名と一致している必要があります。詳細については、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。

b) デバイスプールのリストから、電話機のデバイスプールを選択します。

c) [電話ボタン テンプレート（Phone Button Template）] のリストから使用する電話ボタン テンプレートを選択します。

ステップ 5 [**プロトコル固有の情報**] 領域で、[**デバイスのセキュリティプロファイル (Device Security profile**)] フィールドに、使用している電話機のセキュリティで保護されていないプロファイルを選択します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

電話機のディレクトリ番号の手動設定 （690 ページ）

電話機のディレクトリ番号の手動設定

Cisco Unified Communications Manager Administration を使用してディレクトリ番号（DN）を手動で追加し、設定するには、複数の方法があります。

- **[コールルーティング（Call Routing）]** > **[ディレクトリ番号（Directory Number）]** を使用して、**[ディレクトリ番号の設定（Directory Number Configuration）]** ウィンドウから。
- **[デバイス（Device）]** > **[電話（Phone）]** を使用して、**[電話の設定（Phone Configuration）]** ウィンドウから、**[割り当て情報（Association Information）]** 領域で、**[回線 [1] - 新規 DN を追加（Line [1] - Add a new DN）]** または **[回線 [2] - 新規 DN を追加（Line [2] - Add a new DN）]** リンクを選択して。

- 電話機をコールルーティングに追加した後で、**[コールルーティング（Call Routing）]** > **[電話（Phone）]** を使用して、**[電話の設定（Phone Configuration）]** ウィンドウから。
- **[デバイス（Device）]** > **[CTI ルートポイント（CTI Route Point）]** を使用して、**[CTI ルートポイントの設定（CTI Route Point Configuration）]** ウィンドウから。

この手順では、**[電話の設定（Phone Configuration）]** ウィンドウを使用して新しい電話の DN を設定することを前提としています。このウィンドウは、Unified Communications Manager ノードに新しい電話を追加した後に表示されます。

この方法を使用して表示されるのは、電話機モデルに適用される設定のみです。

ヒント　電話機の新しいDNを追加すると同時に、電話機の機能を設定することができます。使用可能なすべての DN の設定を表示するには、ユーザ インターフェイスのコール ルーティングから [ディレクトリ番号の設定（Directory Number Configuration）]ウィンドウにアクセスする必要があります。

始める前に

電話機がノードに追加されます。登録している新しい電話機に対する [電話の設定（Phone Configuration）] ウィンドウを表示したままにします。

システムでパーティションを使用する場合、ルートパーティションとコーリングサーチスペースを特定し、新しい電話に対して使用します。

手順

ステップ 1　[電話の設定（Phone Configuration）] ウィンドウの [関連付け（Association）]領域で [回線 [1] - 新規 DN を追加（Line [1] - Add a new DN）] をクリックします。

ヒント　[電話の設定（Phone Configuration）] ウィンドウが表示されていない場合は、**[デバイス（Device）]** > **[電話（Phone）]** を選択し、[検索（Find）] をクリックしてから、電話機のリストから電話を選択します。

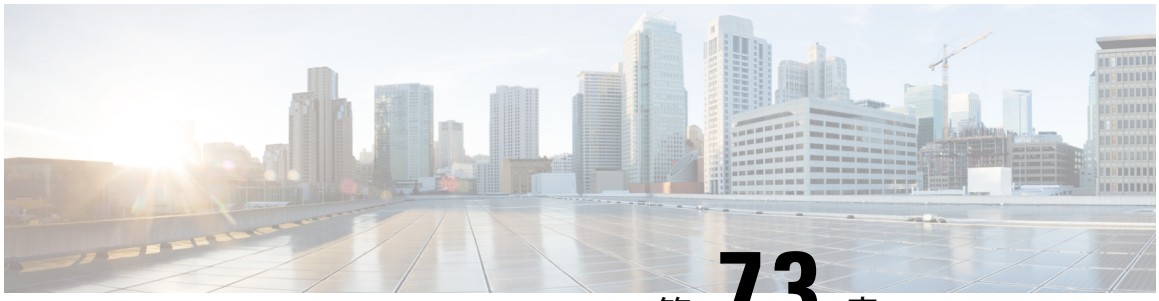
ステップ 2　[ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウで、[ディレクトリ番号（Directory Number）] フィールドにダイヤル可能な電話番号を入力します。

ステップ 3　（任意） [ルート パーティション（Route Partition）] フィールドでパーティションを選択します。

ステップ 4　（任意） [ディレクトリ番号の設定（Directory Number Settings）]エリアの [コーリング サーチ スペース（Calling Search Space）] フィールドでコーリング サーチ スペースを選択します。

ステップ 5　（任意） 新しい電話機に適用できる他のディレクトリ番号機能を設定し、[保存（Save）]をクリックします。

たとえば、すでに新しい電話のユーザ名を知っている場合は、[表示（発信者 ID）（Display (Caller ID)）] フィールドにその名前を入力できます。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。



第 73 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。

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
ステップ 1	セルフプロビジョニングのサービスの有効化 （695 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。
ステップ 2	セルフプロビジョニングの自動登録の有効化 （696 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
ステップ 3	CTI ルート ポイントの設定 （696 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。
ステップ 4	CTI ルートポイントへの電話番号の割り当て （697 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。
ステップ 5	セルフプロビジョニングのアプリケーション ユーザの設定 （698 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。
ステップ 6	セルフプロビジョニングのシステムの設定 （698 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。

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

ステップ 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。

ステップ 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。

ステップ 3 [CMサービス（CM Services）] で、[Cisco CTI Manager] をオンにします。

ステップ 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。

ステップ 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

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]** > **[Cisco Unified CM（Cisco Unified CM）]** を選択します。

ステップ 2 パブリッシャノードをクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 5 [保存（Save）] をクリックします。

ステップ 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。

ステップ 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 ユーザを設定し、アプリケーション ユーザに作成した 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

ステップ 1 Cisco Unified CM Administration から、**[ユーザ（User）] > [アプリケーション ユーザ（Application User）]** を選択します。

ステップ 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 ユーザを選択します。

b) 新しいアプリケーション ユーザを作成するには、[新規追加（Add New）] をクリックします。

ステップ 3 [ユーザ ID（User ID）] テキスト ボックスに、アプリケーション ユーザの一意の名前を入力します。

ステップ 4 アプリケーション ユーザの [BLF プレゼンス グループ（BLF Presence Group）] を選択します。

ステップ 5 アプリケーション ユーザに作成した 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。

ステップ 6 [アプリケーション ユーザの設定（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。

ステップ 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 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 ユーザを選択します。

ステップ 7 [保存（Save）] をクリックします。

ユーザ 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 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

ステップ 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。

ステップ 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。

ステップ 3 そのユーザプロファイルに**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。

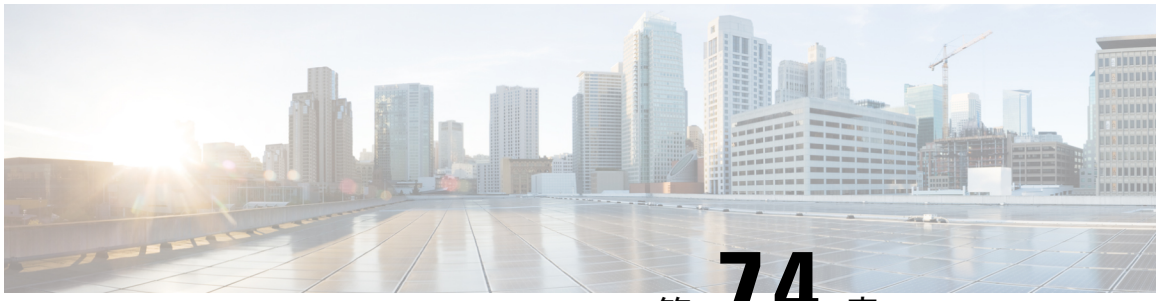
ステップ 4 セルフプロビジョニング用のユーザの設定

- [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。

ステップ 5 [保存（Save）] をクリックします。

第 X 部

応用的なコール処理の設定



第 74 章

応用的なコール処理の概要

応用的なコール処理の概要

このパートの各章では、システムの拡張コール処理を設定するためのさまざまな方法について説明します。このパートで説明した機能を使用して、不在転送のような基本的なコール処理機能よりもより精密なレベルで、コールフロー内の任意の時点でのコールの処理方法を設定できます。このパートのタスク フローでは、各コール処理機能を一覧して、その設定目的を説明し、さらに詳細に説明している適切な章へのリンクを示します。

応用的なコール処理の設定

次のタスク フローを実行すると、システムの応用的なコール処理を設定できます。

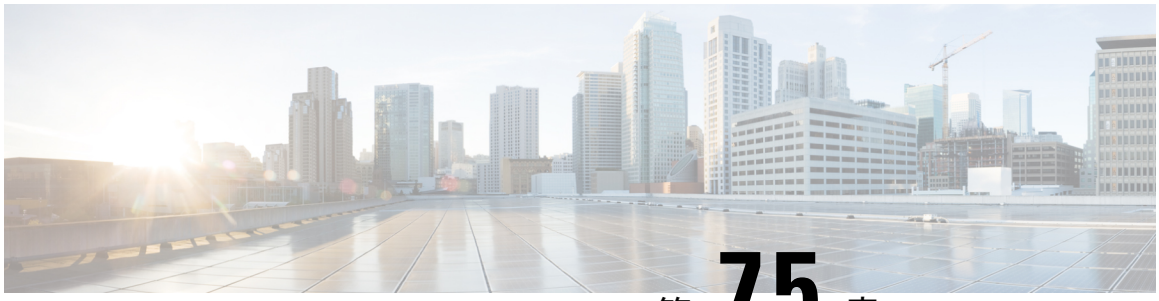
手順

	コマンドまたはアクション	目的
ステップ 1	APIC-EM コントローラの設定タスク フロー （708 ページ）	SIP コールのネットワークサービス品質（QoS）を管理するには、Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（APIC-EM）を導入します。APIC-EM は、Cisco Unified Communications Manager で管理された SIP エンドポイントおよびトランク間の通信セッションで作成されたメディア フローに DSCP マーキングを適用します。DSCP マーキングをメディア フローに適用すると、音声およびビデオ メディアが、

	コマンドまたはアクション	目的
		電子メール、印刷ジョブ、ソフトウェアのダウンロードなどの優先順位の低い他のネットワーク トラフィックによってブロックされなくなります。
ステップ 2	コール制御検出の設定タスク フロー（716 ページ）	Service Advertisement Framework（SAF）ネットワークを使用する他のコール制御エンティティに Cisco Unified Communications Manager をアドバタイズするには、コール制御検出を設定します。これらのコール制御エンティティは、アドバタイズされた情報を使用して、コールのルーティング操作を動的に設定できます。
ステップ 3	外部コール制御の設定タスク フロー（728 ページ）	付加ルート サーバーでシステムのコールルーティングを決定できるようにするには、外部コール制御を設定します。Unified Communications Manager は、付加ルート サーバーにルート要求を発行し、コールのルーティング方法と、適用する追加のコール処理について指示します。
ステップ 4	コール キューイング タスク フロー（743 ページ）	ハント メンバーが応答可能になるまで発信者をキューに入れておくには、コール キューイングを設定します。
ステップ 5	コール スロットリングの設定 （758 ページ）	システムの状態により、オフフックになってからダイヤル トーンを受信するまでの間隔に遅延が生じる可能性があるとき、新しいコール試行を自動的に制限または拒否するには、コール スロットリングを設定します。コール スロットリングのパラメータは、シスコ カスタマーサポートに指示された場合を除き、変更しないことを推奨します。
ステップ 6	発信側の正規化の設定タスク フロー（763 ページ）	着信電話番号のフォーマットを変更して、グローバル化またはローカライズされた電話番号として受信者の電話機に表示するには、発信側の正規化を設定します。この機能を使用すれば、コールが複数の場所にルーティングさ

	コマンドまたはアクション	目的
		れる際のコールバック機能を改善できます。また、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。
ステップ 7	論理パーティションの設定タスク フロー （779 ページ）	トールバイパスが禁止されている市場で規制要件を満たすには、論理パーティショニングを設定します。たとえば、会議の参加やリダイレクトなどの通話中機能を使用して、ユーザーが制限されたコールを開始できないようにするポリシーを設定できます。
ステップ 8	地理位置情報とロケーションの伝達タスク フロー （793 ページ）	すべてのデバイスの地理位置を特定し、クラスタ全体に地理位置情報を伝達します。地理位置情報がデバイスに民間アドレスを割り当てることで、特定の国の法的要件に基づいてデバイス間の通信を制御できます。
ステップ 9	ロケーション認識の設定タスク フロー （804 ページ）	ロケーション認識によって、管理者は企業ネットワークに接続している電話の接続元となる物理的な場所を決定できます。
ステップ 10	AAR の設定タスク フロー （809 ページ）	場所の帯域幅不足のためシステムがコールをブロックする場合、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ようシステムを設定します。自動代替ルーティングにより、発信者が通話を終了して着信側にリダイヤルする必要はなくなります。
ステップ 11	Multilevel Precedence and Preemption Precendence のタスク フロー （828 ページ）	検証済みのユーザーにプライオリティコールの発信を許可するには、Multilevel Precedence and Preemption （MLPP）を設定します。これらのユーザーは、必要に応じて優先順位の低いコールをプリエンプション処理できます。

	コマンドまたはアクション	目的
ステップ 12	2 つのスタック（IPv4 と IPv6）の設定タスク フロー （854 ページ）	エンドポイントで IPv4 と IPv6 の両方のアドレス指定をサポートできるようにするには、このタスクを実行してエンドポイントで 2 つのスタックのサポートを設定します。



第 75 章

APIC-EM コントローラによる QoS の設定

APIC-EM コントローラの概要

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。

SIP メディアフロー管理

APIC-EM を使用した SIP コールの場合、Cisco Unified Communications Manager は、設定されているメディアフローの APIC-EM に通知するコールの初期段階で、ポリシー要求を APIC-EM コントローラに送信します。ポリシー要求には、発信元および宛先のデバイスの IP アドレスやポート、フローのメディアタイプ、およびプロトコルを含む、コールに関する情報が含まれています。

APIC-EM は、関連付けられているメディアフローの DSCP 値のコールフローの先頭にスイッチを通知します。スイッチは、これらの DSCP 値を個々のメディアパケットに挿入し、エンドポイントが挿入する値を上書きします。コールフロー内のゲートウェイに輻輳が発生すると、ゲートウェイは、最初により高い DSCP 値を持つパケットを送信します。これにより、優先順

位の高いオーディオおよびビデオストリームが、電子メール、印刷ジョブ、ソフトウェアダウンロードなどの優先順位の低いネットワークトラフィックによってブロックされることがなくなります。通話が終了すると、Cisco Unified Communications Manager が APIC-EM に通知し、APIC-EM は、そのフローを削除するようスイッチに通知します。

外部 QoS サポート

Cisco Unified Communicatins Manager が APIC-EM を使用してメディアフローを管理するには、外部 QoS パラメータを両方のシステムレベルでは、クラスタ全体のサービスパラメータを介して、さらにデバイスレベルでは、SIP プロファイルを介して有効にする必要があります。

APIC-EM コントローラ前提条件

APIC-EM を使用する前に、次の手順を実行する必要があります。

- Cisco Unified Communications Manager で、さまざまな SIP メディアフローの DSCP 優先順位を設定します。詳細については、「DSCP 設定の設定タスク フロー （637 ページ）」を参照してください。
- ネットワーク内で APIC EM コントローラハードウェアを設定します。詳細については、APIC-EM コントローラ付属のハードウェア ドキュメンテーションを参照してください。

APIC-EM コントローラの設定タスク フロー

これらのタスクを Cisco Unified Communications Manager で完了すると、APIC EM コントローラが SIP メディアフローを管理できるようになります。

始める前に

- APIC-EM コントローラ前提条件 （708 ページ）を確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	APIC-EM コントローラ証明書のアップロード （710 ページ）	APIC EM 証明書を Cisco Unified OS 管理者にアップロードします。
ステップ 2	APIC-EM コントローラへの HTTPS 接続の設定 （710 ページ）	APIC-EM サービスをポイントする HTTP プロファイルを設定します。
ステップ 3	システムの外部 QoS サービスを有効にする （711 ページ）	**外部 QoS Enable** サービスパラメータを有効にすると、APIC を使用してメディアフローを管理するようにシステムが設定されます。SIP メディアフロー管理の

	コマンドまたはアクション	目的
		APIC-EM を使用するには、デバイスのサービスパラメータを有効にする必要があります。 （注） SIP メディアフロー管理の APIC EM を使用するデバイスに対しては、SIPプロファイル内の外部 QoS も有効にする必要があります。
ステップ 4	SIPプロファイル レベルの外部 QoS サービスの設定 （712 ページ）	SIP プロファイル内の外部 QoS を有効にします。この SIP プロファイルを使用するすべてのデバイスは、APIC-EM を使用して SIP メディアフローを管理することができます [SIP プロファイル] の設定を使用して、APIC-EM でメディアフローを管理するデバイスとデバイスタイプを設定することができます。
ステップ 5	電話機への SIP プロファイルの割り当て （713 ページ）	外部の QoS 対応 SIP プロファイルを電話機に関連付けます。

APIC-EM コントローラの設定

ユーザとして Cisco Unified Communications Manager を追加するには、APIC-EM コントローラで次の手順を使用します。APIC-EMのロールベースアクセスコントロール機能により、Cisco Unified Communications Manager で APIC-EM リソースの利用が可能になります。

手順

ステップ 1 APIC-EM コントローラで、**[設定（Settings）]**>**[内部ユーザ（Internal Users）]** を選択します。

ステップ 2 **ROLE_POLICY_ADMIN** ロールを指定して新しいユーザを作成します。Cisco Unified Communications Manager の [HTTPプロファイル（HTTP Profile）] ウィンドウで同一のクレデンシャルを入力する必要があるため、入力するユーザ名とパスワードを記録しておきます。

ステップ 3 [ディスカバリ（Discovery）] タブに移動し、CDP による検出、または使用可能なデバイスの IP アドレスの範囲を追加します。

ステップ 4 [デバイスインベントリ（Device Inventory）] タブを選択し、到達可能なデバイスを選択します。

ステップ 5 [ポリシータグの設定（Set Policy Tag）] をクリックします。

ステップ 6 ポリシー タグを作成し、そのタグをデバイスに設定します。

ステップ 7 [EasyQoS] タブで、作成したポリシーを選択し、[DynamicQoS] を有効にします。

次のタスク

APIC-EM コントローラ証明書のアップロード （710 ページ）

APIC-EM コントローラ証明書のアップロード

この手順を使用して、APIC-EM コントローラ証明書を Cisco Unified Communications Manager にアップロードします。

手順

ステップ 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。

ステップ 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。
[証明書/証明書チェーンのアップロード] ポップアップウィンドウが表示されます。

ステップ 3 **[証明書目的（Certificate Purpose）]** ドロップダウンリストで、**[CallManager-trust]** を選択します。

ステップ 4 証明書の説明を [説明（Description）] に入力します。

ステップ 5 **[参照（Browse）]** をクリックして、該当する証明書を選択します。

ステップ 6 [アップロード（Upload）] をクリックします。

次のタスク

APIC-EM コントローラへの HTTPS 接続の設定 （710 ページ）

APIC-EM コントローラへの HTTPS 接続の設定

Cisco Unified Communications Manager を APIC-EM コントローラに接続するように HTTP プロファイルを設定するには、次の手順を使用します。この接続では、Cisco Unified Communications Manager は HTTP ユーザとして機能し、APIC-EM は HTTP サーバとして機能します。

始める前に

APIC-EM コントローラ証明書のアップロード （710 ページ）

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）] > [HTTP プロファイル（HTTP Profile）]** を選択します。

ステップ 2 [名前（Name）] にサービスの名前を入力します。

ステップ 3 この HTTP 接続の [ユーザ名（User Name）] と [パスワード（Password）] を入力します。ユーザ名を Cisco Unified Communications Manager で設定済みのエンドユーザとする必要はありませんが、ユーザ名とパスワードは、APIC-EM コントローラに設定された値に一致する必要があります。

ステップ 4 [Web サービスのルート URI（Web Service Root URI）] テキスト ボックスで、APIC-EM サービスの IP アドレスまたは完全修飾ドメイン名を入力します。

ステップ 5 [HTTP プロファイル（HTTP Profile）] ウィンドウで、残りのフィールドを設定します。フィールドとそのオプションに関するヘルプは、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

システムの外部 QoS サービスを有効にする （711 ページ）

システムの外部 QoS サービスを有効にする

QoS の管理に外部サービスを使用するように Cisco Unified Communications Manager を設定するには、次の手順を使用します。QoS に APIC-EM コントローラを使用するには、このサービス パラメータを有効にする必要があります。

始める前に

APIC-EM コントローラへの HTTPS 接続の設定 （710 ページ）

手順

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

ステップ 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。

ステップ 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。

ステップ 4 [外部 QoS 機能を有効にする（External QoS Enabled）] サービス パラメータの値を [True] に設定します。

ステップ 5 [保存（Save）] をクリックします。

（注） APIC-EM を使用してデバイスのコール フローを管理するには、デバイスの SIP プロファイル内の外部 QoS を有効にする必要があります。

次のタスク

SIP プロファイル レベルの外部 QoS サービスの設定 （712 ページ）

SIP プロファイル レベルの外部 QoS サービスの設定

クラスタ全体のサービス パラメータである [外部QoS有効（External QoS Enabled）] を有効にした場合、次の手順を使用して、この SIP プロファイルを使用する SIP デバイスの外部 QoS を有効にします。

（注） 外部 QoS は、APIC-EM を使用して QoS を管理するためにシステム レベルと SIP プロファイルの両方で有効にする必要があります。

始める前に

システムの外部 QoS サービスを有効にする （711 ページ）

手順

ステップ 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。

ステップ 2 次のいずれかを実行します。

- 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。
- 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。

ステップ 3 [外部QoSの有効化（Enable External QoS）] チェックボックスをオンにします。この SIP プロファイルを使用して APIC-EM コントローラで QoS を管理する電話の場合、このチェックボックスをオンにする必要があります。

ステップ 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。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

電話機への SIP プロファイルの割り当て （713 ページ）

電話機への SIP プロファイルの割り当て

作成した外部 QoS 対応 SIP プロファイルを電話機に割り当てるには、次の手順を使用します。

ヒント　多数の電話機を選択した SIP プロファイルの更新を一度の操作で行うには、一括管理ツールを使用します。詳細については、『*Cisco Unified Communications Manager* 一括管理ガイド』を参照してください。

始める前に

電話機への SIP プロファイルの割り当て （713 ページ）

手順

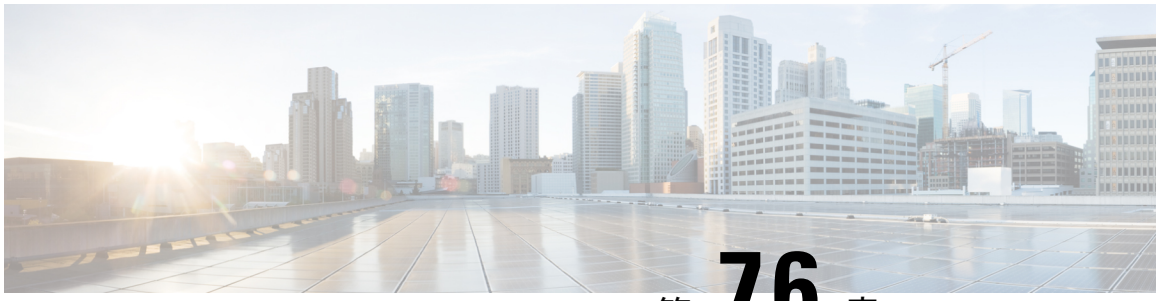
ステップ 1　Cisco Unified CM Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2　[検索（Find）] をクリックし、既存の電話機を選択します。

ステップ 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、トラフィック管理に APIC-EM コントローラを使用する電話機向けに更新した SIP プロファイルを選択します。

ステップ 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。

ステップ 5　[保存（Save）] をクリックします。



第 76 章

コール制御検出の設定

コール制御検出の概要

コール制御発見 (CCD) を使用しUnified Communications Managerて、ディレクトリ番号のパターンなどの他の重要な属性と共に情報を提供します。Service Advertisement Framework (SAF) ネットワークを使用するその他のコール制御エンティティは、アドバタイズされた情報を使用して、それらのルーティング操作を動的に設定し、調整することができます。SAF を使用するすべてのエンティティは、他の重要な情報とともにディレクトリ番号パターンを通知します。他のリモートコール制御エンティティは、このブロードキャストから情報を取得し、コールのルーティング操作を調整できます。

コール制御検出の前提条件

- SAF 対応の SIP または H.323 クラスタ間（非ゲートキーパー制御）トランク
- SAF ネットワークをサポートして使用するリモートコール制御エンティティ。たとえば、他の Unified Communications Manager、または Cisco Unified Communications Manager Express サーバ
- SAF フォワーダとして設定されている Cisco IOS ルータ

コール制御検出の設定タスク フロー

始める前に

- コール制御検出の前提条件 （715 ページ）を確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco IOS ルータをサポートするドキュメントを参照してください。Cisco Feature Navigator（http://www.cisco.com/go/cfn）を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。	Cisco IOS ルータを SAF フォワーダとして設定します。
ステップ 2	SAF セキュリティ プロファイルの設定 （718 ページ）	SAF フォワーダと Unified Communications Manager の間にセキュアな接続を確立するために、SAF フォワーダ向けに SAF セキュリティ プロファイルを設定します。
ステップ 3	SAF フォワーダの設定 （719 ページ）	SAF フォワーダを設定します。これは、SAF 向けに設定された Cisco IOS ルータです。SAF フォワーダは、リモート呼制御エンティティがホスト DN パターンをアドバタイズすると、ローカル クラスタに通知します。さらに、それぞれ設定されているローカル クラスタからのパブリッシング要求や、設定されている登録トランクが SAF フォワーダに送信されます。パブリッシング要求には、Cisco Unified Communications Manager の DN パターン、PSTN フェールオーバー設定、トランク、SIP トランクのリスニング ポートに加え、トランクの URI を含む SIP ルート ヘッダー フィールドが含まれます。
ステップ 4	クラスタ間 SIP または H.323 トランクの設定 （719 ページ）	SAF をサポートするには、SIP または H.323 クラスタ間（ゲートキーパー非

	コマンドまたはアクション	目的
		制御）トランクを設定します。ローカルクラスタは、CCD要求サービスに割り当てられているSAF対応のトランクを使用して、SAFネットワークを使用するリモートの呼制御に発信コールをルーティングします。
ステップ5	ホストDNグループの設定（720ページ）	ホストDNグループを設定します。これは、ホストDNパターンのコレクションです。ホストDNグループをCCDアドバタイジングサービスに割り当てると、CCDアドバタイジングサービスは、ホストDNグループに含まれているすべてのホストDNパターンをアドバタイズします。1つのCCDアドバタイジングサービスに割り当てられるホストDNグループは1つのみです。
ステップ6	ホストDNパターンの設定（721ページ）	ホストDNパターンを設定します。これは、Unified Communications Managerに属する電話番号パターンです。CCDアドバタイジングサービスは、SAFネットワークを使用する他のリモート呼制御エンティティにこのパターンをアドバタイズします。このパターンをホストDNグループに関連付けます。関連付けることで、複数のパターンをかんたんにCCDアドバタイジングサービスに関連付けることができます。
ステップ7	アドバタイジングサービスの設定（721ページ）	コール制御検出アドバタイジングサービスを設定します。これにより、Unified Communications Managerで、クラスタのホストDNとPSTNフェイルオーバー設定を、SAFネットワークを使用するリモートコール制御エンティティにアドバタイズします。
ステップ8	コール制御検出のパーティション設定（721ページ）	コール制御検出パーティションを確認して、学習パターンがこのパーティションの番号分析に挿入されていることを確認します。
ステップ9	要求側サービスの設定（722ページ）	ローカルクラスタから、SAFネットワークのアドバタイズメントを検出で

	コマンドまたはアクション	目的
		きるようにするには、コール制御検出の要求サービスのいずれかを設定して、SAF ネットワークを使用するリモート コール制御のアドバタイズメントをリッスンします。また、CCD 要求サービスは、学習パターンが番号分析に挿入されていることを確認します。
ステップ 10	学習パターンのブロック （723 ページ）	リモート コール制御エンティティからローカル Unified Communications Manager に送信される学習パターンをブロックします。今後使用しない学習パターンについては、次の手順を実行します。

SAF セキュリティ プロファイルの設定

SAF フォワーダと Unified Communications Manager の間にセキュアな接続を確立するために、SAF フォワーダ向けに SAF セキュリティ プロファイルを設定します。

ヒント ルータ（SAF フォワーダ）で入力したものと同じユーザ名とパスワードを使用します。

始める前に

Cisco IOS ルータを SAF フォワーダとして設定します。（http://www.cisco.com/go/cfn にある Cisco Feature Navigator を参照してください）

手順

ステップ 1 Cisco Unified CM Administration から、**[詳細機能（Advanced Features）] > [SAF] > [SAF セキュリティ プロファイル（SAF Security Profile）]** を選択します。

ステップ 2 [SAF セキュリティ プロファイルの設定（SAF Security 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。

ステップ 3 [保存（Save）] をクリックします。

SAF フォワーダの設定

SAF フォワーダを設定します。これは、SAF 向けに設定された Cisco IOS ルータです。SAF フォワーダは、リモート呼制御エンティティがホスト DN パターンをアドバタイズすると、ローカル クラスタに通知します。さらに、それぞれ設定されているローカル クラスタからのパブリッシング要求や、設定されている登録トランクが SAF フォワーダに送信されます。パブリッシング要求には、Cisco Unified Communications Manager の DN パターン、PSTN フェールオーバー設定、トランク、SIP トランクのリスニング ポートに加え、トランクの URI を含む SIP ルート ヘッダー フィールドが含まれます。

ヒント [選択された Cisco Unified Communications Manager（Selected Cisco Unified Communications Managers）] ペインに複数のノードが表示される場合、「@」がクライアント ラベル値に付加されます。各ノードが SAF フォワーダの登録に同じクライアント ラベルを使用した場合にエラーが発生することがあるからです。

手順

ステップ 1 Cisco Unified CM Administration から、**[詳細機能（Advanced Features）] > [SAF（SAF）] > [SAF フォワーダ（SAF Forwarder）]** を選択します。

ステップ 2 [SAF フォワーダの設定（SAF Forwarder 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。

ステップ 3 [保存（Save）] をクリックします。

クラスタ間 SIP または H.323 トランクの設定

SAF をサポートするには、SIP または H.323 クラスタ間（ゲートキーパー非制御）トランクを設定します。ローカル クラスタは、CCD 要求サービスに割り当てられている SAF 対応のトランクを使用して、SAF ネットワークを使用するリモートの呼制御に発信コールをルーティングします。

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 次のいずれかの操作を実行します。

- SIP トランク：

1. **[トランクサービスタイプ(Trunk Service Type)]** タイプドロップダウン リストから、**[コール制御検出]**を選択します。ドロップダウンリストから選択した後でトランクサービスタイプを変更することはできません。
2. [次へ（Next）] をクリックします。
3. [トランクの設定（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。

- クラスタ間トランク（非ゲートキーパー制御）：

1. [次へ（Next）] をクリックします。
2. **[SAF 有効化]** チェックボックスをオンにします。
3. **[トランクの設定（Trunk 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。

ステップ 4 [保存（Save）] をクリックします。

ホスト DN グループの設定

ホスト DN グループを設定します。これは、ホスト DN パターンのコレクションです。ホスト DN グループを CCD アドバタイジング サービスに割り当てると、CCD アドバタイジング サービスは、ホスト DN グループに含まれているすべてのホスト DN パターンをアドバタイズします。1 つの CCD アドバタイジング サービスに割り当てられるホスト DN グループは 1 つのみです。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）]** > **[コール制御検出（Call Control Discovery）]** > **[ホストDNグループ（Hosted DN Group）]** を選択します。

ステップ 2 [ホスト DN グループの設定（Hosted DN Groups 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。

ステップ 3 [保存（Save）] をクリックします。

ホスト DN パターンの設定

ホスト DN パターンを設定します。これは、Unified Communications Manager に属する電話番号パターンです。CCD アドバタイジング サービスは、SAF ネットワークを使用する他のリモート呼制御エンティティにこのパターンをアドバタイズします。このパターンをホスト DN グループに関連付けます。関連付けることで、複数のパターンを かんたんに CCD アドバタイジング サービスに関連付けることができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）] > [コール制御検出（Call Control Discovery）] > [ホスト DN パターン（Hosted DN Patterns）]** を選択します。

ステップ 2 [ホスト DN パターンの設定（Hosted DN Patterns 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。

ステップ 3 [保存（Save）] をクリックします。

アドバタイジング サービスの設定

コール制御検出アドバタイジング サービスを設定します。これにより、Unified Communications Manager で、クラスタのホスト DN と PSTN フェイルオーバー設定を、SAF ネットワークを使用するリモート コール制御エンティティにアドバタイズします。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [コール制御ディスカバリ（Call Control Discovery）] > [アドバタイジングサービス（Advertising Service）]** を選択します。

ステップ 2 [アドバタイジング サービスの設定（Advertising Service 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。

ステップ 3 [保存（Save）] をクリックします。

コール制御検出のパーティション設定

コール制御検出パーティションを確認して、学習パターンがこのパーティションの番号分析に挿入されていることを確認します。

（注） CCD パーティションは、Cisco Unified Communications Manager Administration の **[コールルーティング（Call Routing）] > [制御のクラス（Class of Control）] > [パーティション（Partition）]** には表示されないことに注意してください。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [コール制御検出（Call Control Discovery）] > [アドバタイジングサービス（Advertising Service）]** を選択します。

ステップ 2 [コール制御検出パーティションの設定（Call Control Discovery Partition 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。

ステップ 3 [保存（Save）] をクリックします。

要求側サービスの設定

注意 [学習されたパターンのプレフィックス（Learned Pattern Prefix）] フィールドまたは [ルート パーティション（Route Partition）] フィールドの更新は、システム パフォーマンスに影響を与える可能性があります。システム パフォーマンスの問題を回避するため、これらのフィールドはオフピークの時間帯に更新することを推奨します。

ローカル クラスタから、SAF ネットワークのアドバタイズメントを検出できるようにするには、コール制御検出の要求サービスのいずれかを設定して、SAF ネットワークを使用するリモート コール制御のアドバタイズメントをリッスンします。また、CCD 要求サービスは、学習パターンが番号分析に挿入されていることを確認します。

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）] > [コール制御検出（Call Control Discovery）] > [要求サービス（Requesting Service）]** を選択します。

ステップ 2 [要求サービスの設定（Requesting Service 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。

ステップ 3 [保存（Save）] をクリックします。

SAF ネットワークを使用するには、リモート コール制御エンティティを設定します。（リモート コール制御エンティティのマニュアルを参照してください）。

学習パターンのブロック

リモート コール制御エンティティからローカル Unified Communications Manager に送信される学習パターンをブロックします。今後使用しない学習パターンについては、次の手順を実行します。

始める前に

SAF ネットワークを使用するには、リモート コール制御エンティティを設定します。お使いのリモート コール制御デバイスに対応するマニュアルを参照してください。

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）]** > **[コール制御ディスカバリ（Call Control Discovery）]** > **[学習パターンのブロック（Block Learned Patterns）]** を選択してください。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 次のいずれかのフィールドを設定します。

- [学習パターン（Learned Pattern）] フィールドで、ブロックする学習パターンを正確に入力します。Cisco Unified Communications Manager にブロックさせるパターンを正確に入力する必要があります。
- [学習パターンのプレフィックス（Learned Pattern Prefix）] フィールドに、パターンの先頭に付加されているプレフィックスに基づいて学習パターンをブロックするプレフィックスを入力します。

例：

[学習パターン（Learned Pattern）] では、235XX パターンをブロックするには 235XX を入力します。

例：

[学習パターン プレフィックス（Learned Pattern Prefix）] では、+1 を使用するパターンをブロックするには +1 を入力します。

ステップ 4 [リモート コール制御デバイス（Remote Call Control Entity）] フィールドに、ブロックするパターンをアドバタイズするリモート コール制御デバイスの名前を入力します。

ステップ 5 [リモート IP（Remote IP）] フィールドに、学習パターンをブロックするリモート コール制御デバイスの IP アドレスを入力します。

ステップ 6 [保存（Save）] をクリックします。

コール制御検出の連携動作と制限事項

コール制御検出の連携動作

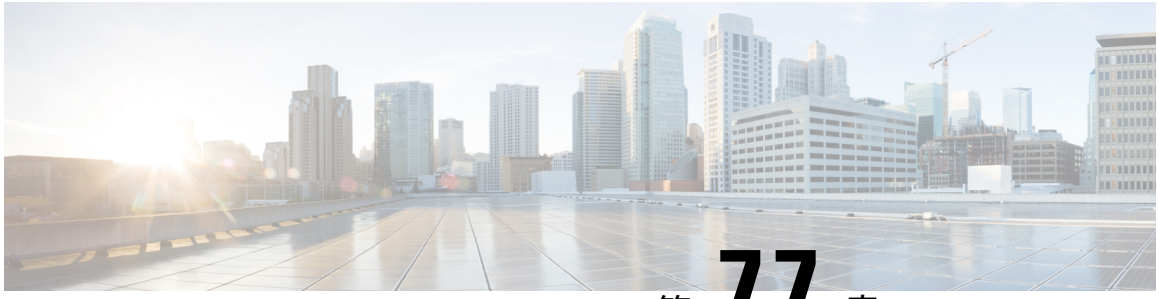
表 *85 :* コール制御検出の連携動作

機能	連携動作
アラーム	Cisco Unified サービスアビリティは、コール制御検出機能をサポートするためアラームを提供します。アラームの設定方法の詳細については、『*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。
BLF 登録	ユーザが SAF 学習パターンの BLF ステータスを登録する場合、Unified Communications Manager は SIP 登録メッセージを SIP トランク経由でリモート クラスタに送信します。 この機能は SAF 対応 SIP トランクだけでサポートされます。
一括管理ツール	一括管理ツールでは、SAF セキュリティ プロファイル、SAF フォワーダ、CCD アドバタイジングサービス、CCD 要求サービス、ホステッド DN グループ、ホステッド DN パターンなどの設定をインポートおよびエクスポートできます。
コール詳細レコード	Unified Communications Manager は、リダイレクション理由を SS_RFR_SAF_CCD_PSTNFAILOVER とした、onBehalfOf の SAFCCDRequestingService としてのリダイレクトをサポートしています。これは、コールが PSTN フェールオーバー番号にリダイレクトされることを示しています。

機能	連携動作
着信コールの着信側の設定（Incoming Called Party Settings）	H.323 プロトコルでは、国際エスケープ文字（+）はサポートされていません。H.323 ゲートウェイまたはトランク経由の着信コールについて SAF/コール制御検出で正しい DN パターンが使用されるようにするには、サービスパラメータ、デバイスプール、H.323 ゲートウェイ、またはH.323 トランクのウィンドウで着信側設定項目を設定する必要があります。つまり、着信の着信側設定項目を設定することで、着信コールがH.323 ゲートウェイまたはトランクからである場合に、Unified Communications Manager は着信側番号を、トランクまたはゲートウェイ経由で送信された元の値に戻します。 たとえば、発信者が Unified Communications Manager A に対して +19721230000 に発信します。 Unified Communications Manager A は +19721230000 を受信し、コールを H.323 トランクに送信する前に番号を 55519721230000 に変換します。この場合、設定は国際タイプのコールについて、国際エスケープ文字 + を除去して 555 を前に付加することを指定しています。 トランクからのこの着信コールの場合、Unified Communications Manager B は 55519721230000 を受信し、発信者が送信した値を番号分析で使用できるように、番号を +19721230000 に戻します。この場合、着信コールの着信側設定項目の設定は、国際タイプの着信側番号に対して、555 を除去して +1 を前に付加することを指定しています。
ダイジェスト認証	Unified Communications Manager は、ダイジェスト認証（TLS なし）を使用して、SAF フォワーダを認証します。Unified Communications Manager がメッセージを SAF フォワーダに送信すると、Unified Communications Manager は SHA1 チェックサムを計算してメッセージの MESSAGE-INTEGRITY フィールドに含めます。
QSIG	[H.323の設定（H.323 Configuration）] ウィンドウの [QSIGバリエーション（QSIG Variant）] および [ASN.1 ROSE OIDエンコーディング（ASN.1 ROSE OID Encoding）] 設定は、CCD アドバタイジング サービスによってアドバタイズされます。これらの設定は、着信トンネル化コールの QSIG メッセージのデコードに影響します。コール制御検出では、発信コールには影響しません。 リモート コール制御エンティティが、H.323 トランク経由の発信コールにQSIG トンネリングが必要かどうかを判別します。リモート コール制御エンティティによってQSIG トンネリングが必要であるとアドバタイズされると、Cisco Unified CM Administration の [H.323の設定（H.323 Configuration）] ウィンドウで QSIG サポートが必要ないことが示されている場合でも、発信コールのメッセージ内に QSIG メッセージがトンネル化されます。

コール制御検出の制限

すべての クラスタは、同じ Autonomous System（AS; 自律システム）内のアドバタイズまたは学習されたルートに制限されます。



第 77 章

外部コール制御の設定

外線コール制御の概要

Unified Communications Manager では、外部コール制御により、付加ルートサーバが、Cisco Unified Routing Rules Interface を使用してコールルーティングを決定できます。外部コール制御の設定に際して、Unified Communications Manager は、発信側および着信側の情報が入ったルート要求を別建てルーティング 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。

付加ルータは、コールの許可/転送/拒否、発信側および着信側の情報の変更、発信者への音声案内、付加ボイスメールサーバと IVR サーバが発信側/着信側の情報を適切に解釈できるようにするためのコール履歴のリセット、コールが転送または拒否された理由を示す理由コードの記録をお使いのシステムに指示します。

外部コール制御は、次の機能を提供します。

- 最高品質のボイス ルーティング：付加ルート サーバは、音声ゲートウェイ経由でコール参加者全員に高音質のコールが送信されるように、ネットワーク リンクの可用性、帯域幅使用、遅延、ジッタ、および MOS スコアを監視します。
- 最小コストルーティング：コールがコスト効率の最も高いリンクを経由してルーティングされるように、付加ルートサーバはローカルアクセスおよびトランスポートエリア（LATA）およびLATA 間の料金プラン、トランキングコスト、バースト使用コストなどのキャリアとの契約情報を使用して設定されます。
- 倫理的境界：付加ルート サーバには、通信の可否を決定する企業ポリシー（ユーザ 1 がユーザ 2 にコールを発信できるかなど）が構成されています。

外部コール制御の要件

この機能を使用するには、Cisco Unified ルーティングルールの XML インターフェイスが必要です。これは、システムにコールの処理方法を指示します。

詳細については、『*Cisco Unified Routing Rules Interface Developers Guide*』（CURRI のドキュメント）（https://developer.cisco.com）を参照してください。

外部コール制御の設定タスク フロー

始める前に

- 外部コール制御の要件 （728 ページ）を確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	外部コール制御用コーリング サーチ スペースの設定 （730 ページ）	ルートサーバが Divert オブリゲーションを送信したときに使用されるコーリングサーチスペースを設定しますコーリングサーチスペースは、デバイスに割り当てたルートパーティションの番号付きリストで構成されます。コーリングサーチスペースは、コールを完了しようと試み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。
ステップ 2	外部コール制御プロファイルの設定 （731 ページ）	外部コール制御プロファイルに、付加ルートサーバの URI、コールの即時転送に使用されるコーリングサーチスペース、お使いのシステムが付加ルートサーバからの応答を待機する時間を示すタイマーを設定します。
ステップ 3	トランスレーション パターンへのプロファイルの割り当て （731 ページ）	外部コール制御で使用するトランスレーションパターンに、外部コール制御プロファイルを割り当てますトランスレーションパターンに一致するコールが発生すると、システムはすぐにコールルーティングクエリーを付加ルートサーバに送信し、付加ルートサーバはシステムにコールの処理方法を指示します。

	コマンドまたはアクション	目的
ステップ 4	（任意） 信頼されたストアへのルートサーバ証明書のインポート （732 ページ）	ルートサーバで HTTPS が使用されている場合は、ルートサーバの証明書をシステムノードにある信頼ストアにインポートします。ルート サーバにルーティング クエリーを送信する可能性のあるクラスタ内のノードごとに、この作業を実行する必要があります。外部コール制御プロファイルのプライマリ ウェブ サービス URI またはセカンダリ ウェブ サービス URI に HTTPS を指定した場合、証明書を使用して設定済の付加ルートサーバへの TLS 接続を介する相互認証を行います。
ステップ 5	（任意） ルートサーバへの自己署名証明書のエクスポート （733 ページ）	ルートサーバで HTTPS が使用されている場合は、Cisco Unified Communications Manager 自己署名証明書をルートサーバにエクスポートします。ルート サーバにルーティング クエリーを送信する可能性のあるクラスタ内のノードごとに、この作業を実行する必要があります。プライマリルートサーバと冗長ルートサーバが常に https を介して Cisco Unified Communications Manager に対して認証されるように、システムにディレクティブを送信する各付加ルートサーバにインポートできる自己署名証明書を生成する必要があります。 プライマリ付加ルートサーバおよび冗長付加ルートサーバに接続できるクラスタ内のノードごとに、この手順を実行します。
ステップ 6	（任意） シャペロン機能の設定 （734 ページ）	ルートサーバのルーティングルールで、監察者によるコールの監視や録音が必要であることが指定されている場合は、監察者機能を設定します。監察者とは、コールに対する企業ポリシーの通知、コールの監視、およびコールの録音をて実行できる、指定された電話機ユーザです。
ステップ 7	（任意） カスタム アナウンスの設定 （735 ページ）	ルーティングルールで、アナウンスが一部のコールに対して再生され、Cisco 提

	コマンドまたはアクション	目的
		供のアナウンスを使用しないようにする必要がある場合は、次の手順に従ってください。

外部コール制御用コーリング サーチ スペースの設定

ルートサーバがDivertオブリゲーションを送信したときに使用されるコーリングサーチスペースを設定しますコーリングサーチスペースは、デバイスに割り当てたルートパーティションの番号付きリストで構成されます。コーリングサーチスペースは、コールを完了しようと試み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。

手順

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

外部コール制御プロファイルの設定 （731 ページ）

外部コール制御プロファイルの設定

外部コール制御プロファイルに、付加ルートサーバの URI、コールの即時転送に使用されるコーリングサーチスペース、お使いのシステムが付加ルートサーバからの応答を待機する時間を示すタイマーを設定します。

始める前に

外部コール制御用コーリング サーチ スペースの設定 （730 ページ）

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [外部コール制御プロファイル（External Call Control Profile）]** を選択します。

ステップ 2 次のいずれかの操作を行います。

- 既存の外部コール制御プロファイルの設定を変更するには、検索条件を入力し、[検索（Find）] をクリックし、結果リストから既存の外部コール制御プロファイルを選択します。
- 新しい外部コール制御プロファイルを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [外部コール制御プロファイルの設定（External Call Control 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。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

トランスレーション パターンへのプロファイルの割り当て （731 ページ）

トランスレーション パターンへのプロファイルの割り当て

外部コール制御プロファイルに、付加ルートサーバの URI、コールの即時転送に使用されるコーリングサーチスペース、お使いのシステムが付加ルートサーバからの応答を待機する時間を示すタイマーを設定します。

始める前に

外部コール制御プロファイルの設定 （731 ページ）

手順

ステップ 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。

ステップ 2 次のいずれかの操作を行います。

- 既存のトランスレーションパターン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、結果のリストから既存のトランスレーションパターンを選択します。
- 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。

ステップ 3 **[外部コール制御プロファイル(External Call Control Profile)]** ドロップダウンリストから、パターンに割り当てる外部コール制御プロファイルを選択します。

ステップ 4 **[トランスレーション パターンの設定]** ウィンドウ内の各フィールドを必要に応じて設定します。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。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

（省略可） 信頼されたストアへのルートサーバ証明書のインポート （732 ページ）

信頼されたストアへのルートサーバ証明書のインポート

ルートサーバで HTTPS が使用されている場合は、ルートサーバの証明書をシステムノードにある信頼ストアにインポートします。ルート サーバにルーティング クエリーを送信する可能性のあるクラスタ内のノードごとに、この作業を実行する必要があります。外部コール制御プロファイルのプライマリ ウェブ サービス URI またはセカンダリ ウェブ サービス URI に HTTPS を指定した場合、証明書を使用して設定済の付加ルートサーバへの TLS 接続を介する相互認証を行います。

始める前に

トランスレーション パターンへのプロファイルの割り当て （731 ページ）

手順

ステップ 1 [Cisco Unifiedオペレーティングシステムの管理(Cisco Unified Operating System Administration)] で、**[セキュリティ(Security)] > [証明書の管理]** の順に選択します。

ステップ 2 **[証明書のアップロード]** をクリックします。

ステップ 3 **[証明書のアップロード(Upload Certificate)]** ポップアップ ウィンドウで、**[証明書の名前(Certificate Name)]** ドロップダウンリストから **[CallManagerの信頼性(CallManager-trust)]** を選択し、付加ルートサーバの証明書を参照します。

ステップ 4 [ファイルのアップロード（Upload File）] フィールドに証明書が表示されたら、[アップロード（Upload）] をクリックします。

ステップ 5 （任意） システムが冗長付加ルートサーバに接続できる場合は、この手順を再度実行します。

次のタスク

ルートサーバへの自己署名証明書のエクスポート （733 ページ）

ルートサーバへの自己署名証明書のエクスポート

ルートサーバで HTTPS が使用されている場合は、Cisco Unified Communications Manager 自己署名証明書をルートサーバにエクスポートします。ルート サーバにルーティング クエリーを送信する可能性のあるクラスタ内のノードごとに、この作業を実行する必要があります。プライマリルートサーバと冗長ルートサーバが常に https を介して Cisco Unified Communications Manager に対して認証されるように、システムにディレクティブを送信する各付加ルートサーバにインポートできる自己署名証明書を生成する必要があります。

プライマリ付加ルートサーバおよび冗長付加ルートサーバに接続できるクラスタ内のノードごとに、この手順を実行します。

始める前に

信頼されたストアへのルートサーバ証明書のインポート （732 ページ）

手順

ステップ 1 [Cisco Unified Operating Administration] で、 **[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

ステップ 2 [証明書リスト（Certificate List）] ウィンドウで、[新規作成（Generate New）] をクリックします。

ステップ 3 [証明書の名前（Certificate Name）] ドロップダウン リストで、[CallManager] を選択します。

ステップ 4 [新規作成（Generate New）] をクリックします。

ステップ 5 [証明書の検索と一覧表示（Find and List Certificates）] ウィンドウで、作成した [CallManager.pem] の証明書を選択します。

ステップ 6 証明書のファイル データが表示されたら、[ダウンロード（Download）] をクリックして、アジャンクト ルート サーバへ証明書をエクスポートするために使用するロケーションに証明書をダウンロードします。

ステップ 7 命令を送信する各付加ルート サーバに証明書をエクスポートします。

次のタスク

（省略可） シャペロン機能の設定 （734 ページ）

シャペロン機能の設定

ルートサーバのルーティングルールで、監察者によるコールの監視や録音が必要であることが指定されている場合は、監察者機能を設定します。監察者とは、コールに対する企業ポリシーの通知、コールの監視、およびコールの録音をて実行できる、指定された電話機ユーザです。

Cisco Unified Communications Manager は、アジャンクト ルート サーバの指示に従ってな監察機能をサポートする、次の機能を提供します。

- 監察者、ハント グループ、監察者リストに着信コールをリダイレクトします。
- 監察者はコールを記録できます。

監察者が発信者に接続するか、または監察対象の会議が確立されると、コールの録音を開始できるように、[録音（Record）] ソフトキーまたはプログラム可能なライン キー（PLK）（電話モデル固有）が電話機でアクティブになります。コールの録音は現在のコールに対してのみ実行され、現在のコールが終了すると、録音が停止します。監察者が録音ソフトキーまたはPLKを押すと、録音ステータスを示すメッセージが電話機に表示されることがあります。

始める前に

（省略可） ルートサーバへの自己署名証明書のエクスポート （733 ページ）

手順

ステップ 1 電話で録音を有効にするには、[電話の設定（Phone Configuration）] ウィンドウで [ビルトインブリッジ（Built-in Bridge）] を [オン（On）] に設定します。

ステップ 2 次のとおり録音プロファイルを作成します。

a) **[デバイス（Device）]>[デバイスの設定（Device Settings）]>[録音プロファイル（Recording Profile）]** の順に選択します。

b) 監察対象の会議を録音できる電話機に対してコール録音プロファイルを作成します。

ステップ 3 ライン アピアランスに録音プロファイルを適用します。

ステップ 4 レコーダーのポイントに SIP トランクを追加します。

ステップ 5 SIP トランクを指すルート パターンを作成します。

ステップ 6 次のサービス パラメータを設定します。

a) [監察ターゲットで録音通知トーンを再生する（Play Recording Notification Tone to Observed Target）]

b) [接続済み監察ターゲットで録音通知トーンを再生する（Play Recording Notification Tone to Observed Connected Target）]

ステップ 7 監察者が使用している電話機で標準監察用電話ソフトキー テンプレートを割り当てます。

ステップ 8 新しい電話機に対しては、**[コール ルーティング（Call Routing）] > [電話番号（Directory Number）]** を、または電話機がすでに設定されている場合は、**[デバイス（Device）] > [電話（Phone）]** から次の手順を実行します。

a) 監察者の電話機で電話番号（DN）を 1 つだけ設定します。
b) 監察者の電話機の DN に、[録音オプション（Recording Options）] ドロップダウン リストから [コールの録音をデバイスが開始する（Device Invoked Call Recording Enabled）] を選択します。
c) 監察者の電話機の DN に、[コールの最大数（Maximum Number of Calls）] 設定に **2** を入力し、[ビジー トリガー（Busy Trigger）] 設定に **1** を入力します。

ステップ 9 [録音（Record）] ソフトキーをサポートする Cisco Unified IP Phone の場合、標準監察用電話ソフトキーテンプレートを設定して、[会議（Conference）]、[録音（Record）]、[コール終了（End Call）] ソフトキーだけが接続状態の電話機に表示されるようにします。

ステップ 10 録音用プログラム可能なライン キー（PLK）をサポートする Cisco Unified IP Phone の場合、[電話ボタン テンプレートの設定（Phone Button Template Configuration）] ウィンドウで PLK を設定します。

ステップ 11 （任意） クラスタに複数の監察者がいる場合、監察ハント リストに割り当てる予定である監察者回線グループに監察者の DN を追加します。

この手順により、利用可能な監察者が必ず通話をモニタできます。

次のタスク

（省略可） カスタム アナウンスの設定 （735 ページ）

カスタム アナウンスの設定

ルーティングルールで、アナウンスが一部のコールに対して再生され、Cisco 提供のアナウンスを使用しないようにする必要がある場合は、次の手順に従ってください。

ヒント アナウンス ID には埋め込みスペースを使用しないでください。

他の言語ロケールがインストールされている場合は、このアナウンスに必要な他の .wav ファイルをアップロードして、これらのロケールで使用することができます。

手順

ステップ 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。

ステップ 2 次のいずれかの操作を実行します。

- 新規のお知らせを追加するには：

a) [新規追加（Add New）] をクリックします。
b) **[アナウンス ID]** フィールドに、アナウンス ID を入力します。
c) **[説明]** に、アナウンスの説明を入力します。
d) 必要に応じて、**[デフォルトアナウンスメント]** ドロップダウンリストから、Cisco 提供のデフォルトアナウンスを選択します。
e) [保存（Save）] をクリックします。

- お知らせ用のカスタム .wav ファイルをアップロードするには、次のようにします。

a) [ファイルのアップロード] をクリックします。
b) ロケールを変更するには、**[ロケール]** ドロップダウンリストから、アナウンス用の言語を選択します。
c) **[ファイルの選択]** をクリックして、アップロードする .wav ファイルを選択します。
d) [ファイルのアップロード] をクリックします。
e) アップロードが完了したら、**[閉じる]** をクリックしてウィンドウを更新し、アップロードされたアナウンスを表示します。

外部コール制御の連携動作と制限事項

外部コール制御の連携動作

表 *86 :* 外部コール制御の連携動作

機能	連携動作
コールの高音質ルーティング	コールに使用するゲートウェイを決定するルーティングルールを、付加ルートサーバ上に設定して、音声の品質を考慮に入れることができます。たとえば、ゲートウェイ A は最高の音声品質を提供するので、そのコールに使用されます。付加ルート サーバは、音声ゲートウェイ経由でコール参加者全員に高音質のコールが送信されるように、ネットワーク リンクの可用性、帯域幅使用、遅延、ジッタ、および平均オピニオン評点（MOS）を監視します。
コール詳細レコード	外部コール制御機能が呼詳細レコードに表示されることがあります。たとえば、付加ルートサーバがコールを許可したか、それとも拒否したかが呼詳細レコードに示されることがあります。さらに、Cisco Unified Communications Manager が付加ルートサーバからの決定を受信していない場合に、Cisco Unified Communications Manager がコールをブロックしたか許可したかが呼詳細レコードに示されることもあります。

機能	連携動作
コール転送	外部コール制御はトランスレーション パターン レベルでコールを代行受信しますが、コール転送は電話番号レベルでコールを代行受信します。外部コール制御はコール転送に優先されます。コール転送が起動されるコールの場合、トランスレーションパターンが外部コール制御プロファイルに割り当てられていると、Cisco Unified Communications Manager は付加ルートサーバにルーティングクエリを送信します。コール転送がトリガーされるのは、付加ルートサーバが Cisco Unified Communications Manager に Continue オブリゲーションと許可決定を送信する場合だけです。 （注） 外部コール制御に対応した **[コール転送ホップカウント（Call Diversion Hop Count）]** サービスパラメータと、コール転送に対応した **[コール転送コールホップカウント（Call Forward Call Hop Count）]** サービスパラメータは相互に独立しており、個別に機能します。
コール ピックアップ（Call Pickup）	電話機ユーザがコールピックアップ機能を使用してコールを受信しようとすると、外部コール制御が起動します。つまり、 Cisco Unified Communications Manager は、そのコール部分に対してはルーティングクエリを付加ルートサーバに送信しません。
監察者	監察者とは、コールに対する企業ポリシーの通知、コールの監視、およびコールの録音を必要に応じて実行できる、指定された電話機ユーザです。コールに参加するユーザが監察者の不在時に会話できないという、監察者の制限があります。
Cisco Unified Mobility	次の Cisco Unified Mobility 機能に対しては、Cisco Unified Communications Manager は付加ルートサーバからのルート決定を優先します。 • モバイル ボイス アクセス • エンタープライズ機能アクセス • Dial-via-Office リバース コールバック Cisco Unified Communications Manager は、次の Cisco Unified Mobility 機能に対してルーティング クエリを送信しません。 • 携帯電話ピックアップ • デスク ピックアップ • セッション ハンドオフ
会議	電話機ユーザが会議を作成すると、プライマリコールと打診コールに対して外部コール制御が呼び出されることがあります。

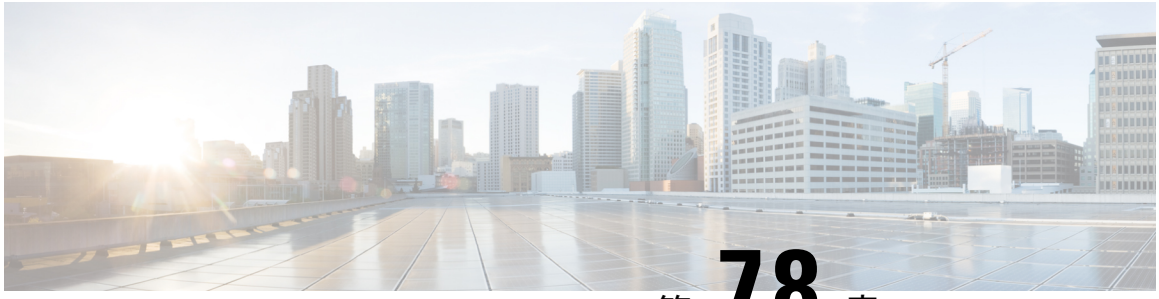
機能	連携動作
ディレクトリ番号（Directory Numbers）	ネット上ダイヤリングで 4 桁または 5 桁がサポートされている場合、電話番号を 4 桁または 5 桁の内線（エンタープライズ拡張）として設定する際に、2つのトランスレーションパターンを設定する必要があります。1つ目のトランスレーションパターンは発信側番号と着信側番号のグローバル化をサポートし、2つ目のトランスレーションパターンは発信側番号と着信側番号のローカライズをサポートします。
サイレント（Do Not Disturb）	デフォルトでは、ユーザの DND 設定は、付加ルートサーバのユーザルールで、付加ルートサーバが継続オブリゲーションを送信することが指定されている場合に有効になります。たとえば、付加ルート サーバが Continue オブリゲーションを送信した場合、ユーザの DND-R が有効になっていると、Cisco Unified Communications Manager はコールを拒否します。
緊急コールの処理	**注意** 緊急コール（911 や 9.11 など）に対しては、ルート サーバに接続してコール処理方法の指示を受けなくてもコールが適切な接続先（Cisco Emergency Responder やゲートウェイなど）にルーティングされるように、明示的な緊急コールのパターン セットを設定しておくことを強く推奨します。
転送	電話機ユーザがコールを転送すると、プライマリコールと打診コールの両方に対して外部コール制御が呼び出されることがあります。ただし、Cisco Unified Communications Manager は、転送側と転送先との間に付加ルート サーバからのルーティング ルールを実施できません。

外部コール制御の制限事項

表 *87 :* 外線コール制御の制限事項

制限事項	説明
通話者の追加	監察者は、会議の開始後に電話機を使用して会議にユーザを追加できません。これは、監察者がユーザを追加するには、コールを保留にする必要があるためです。 会議の他のユーザは会議にユーザを追加できる可能性があります。他のユーザが会議に参加者を追加できるかどうかは、Cisco CallManager サービスがサポートされている **Advanced Ad Hoc Conference Enabled** サービスパラメータの設定によって決まります。このサービス パラメータが **True** に設定されている場合は、他のユーザが会議に参加者を追加できます。
コールの転送	監察者は、電話機を使用して会議コールを別のユーザに転送できません。

制限事項	説明
会議ログアウト	監察者が会議から退出すると、会議全体が終了します。
会議のソフトキー	監察者が会議を作成した後で、その **[会議]** ソフトキーは電話で無効になります。
保留	監察者は、電話機を使用して会議コールを保留にすることができません。
録音（Recording）	監察者が、会議への参加が必要なユーザに打診コールを行う前に録音を開始した場合、監察者が打診コールを行う間、Cisco Unified Communications Managerでは録音が中断されます。会議が確立されると、録音が再開されます。



第 78 章

コール キューイングの設定

コール キューイングの概要

Cisco Unified Communications Manager は、コールキューイングを提供し、発信者をハントメンバーが応答可能になるまでキュー内にとどめておくことができます。管理者は、通話がエージェントに転送される前に、発信者が初期グリーティングアナウンスを受け取るようにデフォルトを設定できます。またはこのデフォルトを変更して、初期アナウンスを、発信者がキューに入れられて保留音または保留トーンが流されてから再生することもできます。発信者がキューに入れられたまま指定時間が経過すると、通話に応答できるようになるまで、または最大待機タイマーが満了するまで、セカンダリ アナウンスが設定された間隔で再生されます。

着信コールがハントパイロットに到達すると、次の機能が提供されます。

- 発信者は、次に進む前に最初のカスタマイズ可能なグリーティングアナウンスに接続されます。
- 1 人以上の回線メンバがハントパイロットにログインしており、アイドル状態であったときで、かつ、キューに入っているコールがない場合は、そのコールは最も長い時間アイドル状態であった回線メンバに送達されます。
- 回線メンバーが通話に応答しない場合、その発信者はキューに入れられません。[応答中、ログイン中、または登録済みのハントメンバが存在しない場合(When no hunt members answer, are logged in, or registered)] の設定に応じて、コールは新しい接続先にルーティングされるか、切断されます。
- 回線メンバがキュー有効コールに応答しないと、回線グループ 設定ウィンドウで **[無応答時にハントメンバを自動的にログアウト(Automatically Logout Hunt Member on No Answer)]** がオンの場合に限り、その回線メンバはハントグループからログオフされます。
- 通話はすべてのメンバーが話し中である場合にのみキューに入れられます。
- キューで待機している発信者は、保留音と反復される（カスタマイズ可能な）定期的なアナウンスが聞こえます。

- ある回線メンバがアイドル状態になると、複数のハントグループ間で最も待機時間の長い発信者が、そのアイドル状態の回線メンバに送達されます。アイドル状態の回線メンバがそのコールに応答しない場合、発信者はキューの以前の場所に戻されます。
- キュー内のコールが最大待機時間を超える場合、またはキューに許可されている発信者の最大数を超える場合、コールは代替番号にルーティングするか、またはハントパイロットの設定に応じて切断することができます。代替番号は次のいずれかにすることができます。
  - キューイングが有効または無効のいずれかに設定されたハント パイロット DN
  - ボイスメール DN
  - 回線 DN
  - 共有 DN
- 回線メンバーは、キュー対応ハント パイロットのキュー ステータスを表示できます。キュー ステータスには次のタイプの情報が表示されます。
  - ハント パイロットのパターン
  - 各ハント パイロットのキューに入っている発信者数
  - 最大待機時間

通話のキューイングは既存のハントパイロットとともに機能しますが、キューイングまたは非キューイングのどちらのハント パイロットのハンティング操作もその動作に変更はありません。通話のキューイングが有効になっているハント パイロットは、次の機能を提供します。

- 回線メンバーが受けることができるキューイング対応ハントパイロットでの通話は、一度に 1 つのみです。2 つのキューイング対応ハント パイロットでの通話を、1 人の回線メンバーに提供することはできません。回線メンバが自分の DN に直接かかってきたコールまたはキューイングしていないハントパイロットからのコールのみを受信できます。
- 回線メンバーがハントパイロットによりルーティングされる通話に応答しない場合、ハント パイロットは自動的にログアウトします。回線メンバは、キューを有効にしたハントパイロットのコールを受信せず、タイムアウトが発生するまでそのコールに応答しなかった場合、そのデバイスを自動的にログアウトします。共有回線配置の場合、同じ共有回線で設定されたすべてのデバイスがログアウトします。この挙動は[Line Group] 設定ウィンドウで [Automatically Logout Hunt Member on No Answer] を選択して設定できます。回線メンバーは、このチェックボックスがオンの場合にのみログアウトします。

コールキュー監視またはアナウンス監視の詳細については、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

キューイングが有効なハントパイロットの中で、コールがハントメンバーに拡張されているときに、着信コールを接続コールの状態に変更するように設定することができます。

コールキューの前提条件

- Cisco IP Voice Media Streaming（IPVMS）アプリケーション。クラスタ内の少なくとも 1 ノード上でアクティブ化されている必要があります

- クラスタ内の少なくとも 1 台のサーバ上で稼動している Cisco CallManager サービス
- Cisco CallManager サービスと同じサーバ上で稼動している Cisco RIS Data Collector サービス
- Cisco Unified Communications Manager ロケール インストーラ（英語以外の電話ロケールまたは国独自のトーンを使用する場合）。

コール キューイング タスク フロー

始める前に

アナウンスの設定

Cisco Unified Communications Manager では以下が可能です：

- Cisco 提供の既存のアナウンスを使用する
- アナウンスが再生するメッセージまたはトーンを変更するには、
- カスタムアナウンスメントの .wav ファイルを挿入
- アナウンスメント用のロケールを割り当て、
- アナウンスの説明の変更、
- アナウンスが再生するメッセージまたはトーンを変更します。

機能アナウンスは、ハントパイロット発信キューイングまたは外部コール制御と関連する保留音（MOH）などの特定の機能に使用されるアナウンスです。

最大 50 個の機能アナウンスが利用可能です。これらのアナウンスは、Cisco が適用する音声ファイルか、アップロードされたカスタム wav ファイルです。

カスタムアナウンスの wav ファイルはすべて、クラスタの全サーバにアップロードされる必要があります。

手順

ステップ 1 Cisco Unified Communications Manager で、**[メディアリソース(Media Resources)]** > **[アナウンス(Announcements)]** を選択します。

[アナウンスの検索と一覧表示] ウィンドウが表示されます。

ステップ 2 使用するアナウンスへのハイパーリンクを選択します。

例：

ハイパーリンク: Wait_In_Queue_Sample

アナウンスの説明を編集したり、アップロードする場合は、カスタマイズされたアナウンスを選択することができます。

ステップ 3 カスタムアナウンスとして使用する .wav ファイルをアップロードするには、**[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]ウィンドウが開きます。

ステップ 4 **[ファイルのアップロード(Upload File)]** ポップアップ ウィンドウでロケールを選択し、ファイル名を入力するか、または参照して .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。

アップロード処理が開始されます。ファイルによっては数分かかることがあります。処理が完了するとステータスが更新されます。

ステップ 5 **[閉じる]** をクリックして、ウィンドウを閉じます。
[アナウンス設定(Announcement Configuration)] ウィンドウがリフレッシュされ、アップロードしたファイルのステータスが更新されます。

ステップ 6 カスタム アナウンスを再生する場合は、**[アナウンス設定(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てください。

ステップ 7 **[アナウンス設定(Announcements Configuration)]** ウィンドウで変更を加えたら、**[保存(Save)]** をクリックします。

次のタスク

アナウンス ファイルはクラスタ内のサーバ間では伝搬されないため、クラスタ内の各ノードにアナウンスをアップロードする必要があります。クラスタ内の各サーバで Cisco Unified Communications Manager の管理ページを参照し、アップロードプロセスを繰り返します。

保留音の設定

発信者が最初に保留中になったときにオプションのイニシャル通知を再生し、定期的にアナウンスを定期的に再生するように、[保留音 (MoH)] に設定することができます。これらのアナウンスには、シスコが提供するオーディオファイルのいずれか、または、システムにアップロードされたファイルを使用できます。

保留音オーディオ ソースの追加変更、既存のオーディオソースをオーディオストリーム番号へ関連付け、またはカスタムオーディオソースのアップロードをするには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified Communication Manager] で、**[メディア リソース（Media Resources）]** > **[保留音オーディオソース（Music On Hold Audio Source）]** を選択します。

[保留音オーディオ ソースの検索と一覧表示（Find and List Music On Hold Audio Sources）] ウィンドウが表示されます。

ステップ 2 新しい保留音オーディオ ソースを追加するには、**[新規追加(Add New)]** をクリックします。保留音オーディオソースを更新するには、対象となる保留音オーディオソースを検索します。指定した検索条件に基づいて、すべての条件に一致するレコードの検索結果がシステムに表示されます。

ステップ 3 保留音のオーディオ ソース フィールド （745 ページ） に示すように、適切な設定を入力します。

ステップ 4 [保存（Save）] をクリックします。
ウィンドウ下部のリストボックスに新しい保留音のオーディオ ソースが表示されます。[MOH オーディオ ソース ファイル ステータス（MOH Audio Source File Status）] ペインに、追加されたソースに対する MOH オーディオ トランスレーション ステータスが表示されます。

保留音のオーディオ ソース フィールド

表 *88* : 保留音のオーディオ ソース情報

フィールド	説明
[MOH オーディオストリーム番号（MOH Audio Stream Number）]	この MOH オーディオ ソースのストリーム番号を選択するには、このフィールドを使用します。ドロップダウン矢印をクリックし、リストから値を選択します。既存の MOH オーディオ ソースの場合、値は MOH オーディオ ソースのタイトルで表示されます。
MOH オーディオ ソース ファイル（MOH Audio Source File）	この MOH オーディオ ソースのファイルを選択するには、このフィールドを使用します。ドロップダウン矢印をクリックし、リストから値を選択します。
[MOH オーディオ ソース名（MOH Audio Source Name）]	MOH オーディオ ソースの一意の名前を、このフィールドに入力します。この名前には、文字、数字、スペース、ダッシュ、ドット（ピリオド）およびアンダースコアを含み、最大で 50 の有効な文字を使用できます。
マルチキャストを許可（Allow Multicasting）	選択した MOH オーディオ ソースのマルチキャストを許可するには、このチェックボックスをオンにします。

フィールド	説明
MOH オーディオ ソース ファイル ステータス（MOH Audio Source File Status）	このペインには、選択したMOHオーディオ ソースのファイルに関する次の情報が表示されます。 • [InputFileName] • ErrorCode • ErrorText • DurationSeconds • DiskSpaceKB • LowDateTime • HighDateTime • [OutputFileList] • [MOH オーディオ変換の完了日（MOH Audio Translation completion date）] （注） [OutputFileList] にはULAW、ALAW、G.729およびワイドバンドWAV ファイルと、ステータス オプションについての情報が含まれます。

表 *89* : アナウンスの設定

フィールド	説明
最初のアナウンス（Initial Announcement）	ドロップダウン リストから最初のアナウンスを選択します。 （注） 最初のアナウンスなしで MoH を選択するには、[オフ（Not Selected）] オプションを選択します。 [詳細の表示（View Details）]リンクをクリックすると、[最初のアナウンス（Initial Announcement）] に関する次の情報が表示されます。 • アナウンス ID • 説明 • [デフォルトのアナウンス（Default Announcement）] （注） • オーディオ ソースの [マルチキャストを許可（Allow Multi-casting）]「」がオフで、[再生される最初のアナウンス（Initial Announcement Played）]「」が [キューされたコールのみ（Only for queued calls）] に設定されている場合にのみ、MOH サーバーによって再生されます。 • [マルチキャストを許可（Allow Multi-casting）]「」のチェックがオンか、[再生される最初のアナウンス（Initial Announcement Played）]「」が [常時（Always）] に設定されている場合、ANN によって再生されます。

フィールド	説明
再生される最初のアナウンス（Initial Announcement Played）	次のうち 1 つを選択して、最初のアナウンスを再生するタイミングを決定します。 • ハント メンバーへのルーティング前にアナウンスを再生（Play announcement before routing to Hunt Member） • コールがキューに入る場合アナウンスを再生（Play announcement if call is queued）
定期アナウンス（Periodic Announcement）	定期アナウンスをドロップダウン リストから選択します。 （注） 定期アナウンスを持たない MOH を選択するには、[選択なし（Not Selected）] オプションを選択します。 [詳細表示（View Details）] リンクをクリックすると、次のような定期アナウンスの情報を参照できます。 • アナウンス ID • 説明 • [デフォルトのアナウンス（Default Announcement）] （注） MOH サーバは、他の設定に関係なく常に定期アナウンスを再生します。
定期アナウンスの間隔（Periodic Announcement Interval）	定期アナウンスの間隔を指定する値（秒単位）を入力します。有効な値は 10 ～ 300 です。デフォルト値は 30 です。

フィールド	説明
[アナウンスのロケール（Locale Announcement）]	[アナウンスのロケール（Locale Announcement）]は、インストールされているロケールインストールパッケージに応じて異なります。 （注） • MOH によって再生される音声ガイダンスでは、[アナウンスのロケール（Locale Announcement）] の設定が使用されます。 • ANNが再生する音声ガイダンスは、発信者のユーザー ロケールを使用します。

表 *90 :* 保留音のオーディオ ソース

フィールド	説明
（MOH オーディオ ソースのリスト）	このリストボックスには、追加するMOHオーディオソースが表示されます。MOHオーディオソースを設定するには、そのMOHオーディオソースのオーディオストリーム番号を選択します。 オーディオ ソース ID は、保留音サーバー内のオーディオ ソースを示すIDです。このオーディオソースには、ディスク上のファイルか、ソース ストリーム保留音サーバーがストリーミング データを取得する固定デバイスのどちらかを含めることができます。MOHサーバーは、最大で 51 のオーディオ ソース ID をサポートします。オーディオ ソース ID が示す各オーディオソースは、必要に応じてユニキャストおよびマルチキャスト モードでストリームできます。 （注） [<なし>（<None>）]を選択すると、MOH オーディオ ソースにはシステムのデフォルトである MOH オーディオ ソース サービス パラメータ（[デフォルトのネットワーク保留MoHオーディオソースID（Default Network Hold MoH Audio Source ID）]）が使用されます。

フィールド	説明
ファイルのアップロード（Upload File）	ドロップダウン リストに表示されていない MOH オーディオ ソース ファイルをアップロードするには、[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）] ウィンドウで、音源ファイルのパスを入力するか、[参照（Browse）] をクリックしてファイルまで移動します。オーディオ ソース ファイルを指定した後、[ファイルのアップロード（Upload File）] をクリックしてアップロードを完了します。オーディオ ファイルをアップロードしたら、[アップロード結果（Upload Result）] ウィンドウにアップロードの結果が表示されます。[閉じる（Close）] をクリックしてウィンドウを閉じます。 （注） ファイルをアップロードすると、そのファイルは Cisco Unified Communications Manager サーバにアップロードされ、オーディオ変換が実行されて、MOH 用にコーデック特有のオーディオ ファイルが作成されます。元ファイルのサイズによっては、処理が完了するまでに数分を要することがあります。 （注） 音源ファイルを MOH サーバにアップロードすると、そのファイルは 1 つの MOH サーバにしかアップロードされません。クラスタ内の各 MOH サーバに音源ファイルをアップロードするためには、各サーバで Cisco Unified Communications Manager Administration を使用する必要があります。MOH 音源ファイルは、クラスタ内の他の MOH サーバに自動的には伝達されません。

ハントパイロットキューの設定

ハント メンバーが一定時間で処理できるより多くのコールが、ハント パイロットに、コール分配機能を介して届いた場合、応答可能になるまで、キュー内のコールは、コール キューイングにより保留されます。

キューイングを有効にすると、[無応答時ハント転送（Forward Hunt No Answer）] と [話中ハント転送（Forward Hunt Busy）] の両方が自動的に無効になります。逆に、[無応答時ハント転送（Forward Hunt No Answer）] または [話中ハント転送（Forward Hunt Busy）] を有効にすると、キューイングが自動的に無効になります。

手順

ステップ 1 Cisco Unified CM Administration で、**[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、ハント パイロットを設定します。

ステップ 2 キューイングに設定する必要があるハント パイロットを選択します。

ステップ 3 [ハント パイロットの設定（Hunt Pilot Configuration）] ウィンドウの [キューイング（Queuing）] セクションに移動します。

ステップ 4 キューイングを有効にするには、[コールのキューイング（Queue Calls）] チェックボックスをオンにします。

ステップ 5 アナウンスの再生とキューの保留処理のために使用されるドロップダウン リスト ボックスから保留音（MoH）ソースを選択します。

MOH ソースはユニキャストまたはマルチキャストとして設定できます。発信者側のメディア リソース グループ リスト（MRGL）では、マルチキャスト、ユニキャストに優先順位を設定します。

ソースを選択しない場合、デフォルトのネットワークによる保留 MoH/MoH ソースとアナウンスが使用されます。

MoH ソース アナウンス ロケールはアナウンスに使用する言語を判別するために使用されます。1 つのハント パイロットで再生できるのは、1 つの言語アナウンス タイプだけです。

ステップ 6 [キューに入れられる発信者の最大数（Maximum Number of Callers Allowed in Queue）] フィールドに、このハント パイロットでキューに入れられる発信者の最大数を整数で入力します。

デフォルト値は 32 です。値の範囲は 1 ～ 100 です。

ステップ 7 キューの発信者が最大数に達したとき、次のいずれかのオプションを選択します。

- 後に続くコールを切断する場合は、[コールを切断（Disconnect the call）] を選択します。
- 後に続くコールを 2 番目の接続先にルーティングする場合は、[コールをこの接続先にルーティングする（Route the call to this destination）] を選択します。特定のデバイス DN、共有回線 DN、または別のハント パイロット DN を指定します。
- （省略可）ドロップダウン リストから、[コーリング サーチ スペースの完全キュー（Full Queue Calling Search Space）] を選択できます。コールを完了するように試みるとき、検索するパーティションを判別するために使用されます。

ステップ 8 [キューの最大待機時間（Maximum Wait Time in Queue）] フィールドで、キューの最大待機時間を秒単位の整数値を入力します。

デフォルト値は 900 秒です。有効な範囲は 10 ～ 3600 秒です。

ステップ 9 最大待機時間に達したとき、次のいずれかのオプションを選択します。

- コールを切断する場合は、[コールを切断（Disconnect the call）] を選択します。
- コールを 2 番目の接続先にルーティングする場合は、[コールをこの接続先にルーティングする（Route the call to this destination）] を選択します。特定のデバイス DN、共有回線 DN、または別のハント パイロット DN を入力します。
- （任意）ドロップダウン リストから、[最大待機時間コーリング サーチ スペース（Maximum Wait Time Calling Search Space）] を選択することもできます。コールを完了するように試みるとき、検索するパーティションを判別するために使用されます。

ステップ 10 回線メンバーがログインしていない、または着信コール時に登録されていないとき、次のオプションのいずれかを選択します。

- コールを切断する必要がある場合は、[コールを切断（Disconnect the call）] を選択します。
- コールを 2 番目の接続先にルーティングする必要がある場合は、[コールをこの接続先にルーティングする（Route the call to this destination）]を選択します。特定のデバイス DN、共有回線 DN、または別のハント パイロット DN を入力します。
- （省略可）ドロップダウン リストから [ハント メンバーがコーリング サーチ スペースに登録またはログ インしていない（No hunt members logged in or registered Calling Search Space）] を選択することもできます。コールを完了するように試みるとき、検索するパーティションを判別するために使用されます。

ステップ 11 [保存（Save）] をクリックします。

[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）]

手順

ステップ 1 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）**]を選択して回線グループを設定します。

ステップ 2 設定する必要がある回線グループを [回線グループの検索と一覧表示（Find and List Line Group）] ウィンドウから選択します。

ステップ 3 [回線グループの設定（Line Group Configuration）] ウィンドウの [ハント オプション（Hunt Options）] セクションに移動します。

ステップ 4 [無応答時にハント メンバー自動的にログアウトする（Automatically Logout Hunt Member on No Answer）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

コール キューイングの連携動作と制限事項

コール キューイングの連携動作

機能	連携動作
SIP Rel1XXオプション（SIP Rel1XX Options）	コールが SIP ICT を通じてキューイング対応ハントパイロットにルーティングされる場合、SIP ICT は、SIP Rel1XX オプションが [1XXにSDPが含まれる場合PRACKを送信（Send PRACK if 1XX contains SDP）] に設定されているSIPプロファイルを使用します。その結果、コールが回線メンバに接続される前に、コールごとに最初の通知が再生されます。 Cisco Unified CM 管理の**デバイスデバイスの設定SIP プロファイル** > **トランク固有の設定**の下で、**[キューアナウンスの再生前に着信コールを接続]** チェックボックスをオンにした場合、SIP ICT の蒸気の既存の連携動作は適用されません。 **[キューアナウンスの再生前に着信コールを接続]** チェックボックスがオフになっている場合、SIP ICT の連携動作は変わりません。ただし、最初のアナウンスが PSTN 側の発信者によって常に聞こえることを保証するものではありません。コールで Connect メッセージを受信するまで PSTN プロバイダーがボイスパスを開かない場合、PSTN 側からの発信者には初期アナウンスが表示されません。

機能	連携動作
ハント パイロットとハント グループ	• ハントグループのログオフ通知機能は、コールキューイングがハントパイロットで有効になると変更されます。コールキューイングがハントパイロットで有効である場合、ユーザがハントグループからログアウトしているとき、またはキュー内で自分の順番を逃したためにログオフされた場合には、ハントグループのログオフ通知は再生されません。 • ハントリストに複数の回線グループが含まれている場合、これらの回線グループでは、**[無応答時にハントメンバを自動的にログアウト(Automatically Logout Hunt Member on No Answer)]** の設定を同じにする必要があります。 • ハントパイロットは、すべてのハントメンバーがログアウトしていてもコールをキューしています。回線グループメンバーは 1 つ以上の回線グループに追加するべきではありません。2番目の回線グループに追加されていても、2番目の回線グループは同じハントリストに含まれないようにする必要があります。 • すべてのハントオプションを[次のメンバへ、その後ハントリスト内の次のグループへ(Try next member; then, try next group in Hunt List)] に設定する必要があります。

コールキューイングの制限事項

次の一般的な制限がコールキューイングに適用されます。

- H323 Fast Start はコールキューイングに対応していません。
- キューステータス PLK がサポートされるのは、SCCP と SIP: 6921、6941、6945、6961、7911G、79 31G、7945G 42G、7965G、7962G、、75G、8961、8945、8941、9951、9971、7800、および 8800 シリーズの両方で次の LCD ディスプレイ電話機のみです。
- ハントグループからのログアウト (HLog) は Cisco Extension Mobility クロスクラスタ (EMCC) と互換性がありません。コールキューイングを EMCC で展開することはできません。
- Cisco Unified Communications Manager は、コールキューイングのある Unified Mobility に対応していません。

- H323 から SIP への対話のシナリオでは、ユーザが初期のアナウンス、MoH、定期的なアナウンスを聞いていないことがあります。また、その他の動作遅延が原因で、ネイティブのコールキューイングフローが失敗しています。このようなシナリオでは、SIP プロトコルのみを使用することを推奨します。

コールキューイングを使用するハントパイロットのパフォーマンスとスケーラビリティ

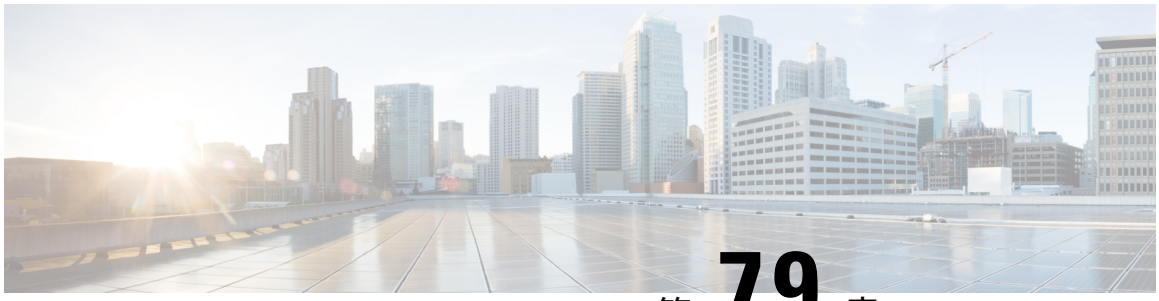
次のようなパフォーマンスおよび拡張性の制限が適用されます。

- 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 キューイングがイネーブル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。



第 79 章

コール スロットリングの設定

コールスロットリングの概要

コールスロットルを使用すると、システムは自動的に新しいコールを調整または拒否することができます。この操作は、条件によって、ユーザが電源オフフックの間に遅延を発生させ、ダイヤルトーンを受信する場合に発生します。

この遅延によって発生する可能性のある要因は次のとおりです。

- 重いコールアクティビティ
- CPU 使用率が低い
- ルーティングループ
- ディスク I/O の制限
- ディスクフラグメンテーション

システムは、コールスロットリングパラメータで指定されている値を使用して、ダイヤルトーンの遅延の可能性を評価し、コールスロットリングが必要でなくなった状態を判断します。

ダイヤルトーンの過剰な遅延を回避するためにスロットリングが必要になったときに、システムは Code Yellow 状態に入り、新しいコールの試行がスロットル（拒否）されます。

ダイヤル トーンの遅延が、コール スロットリング関連のサービスパラメータで設定されているしきい値を超えるとシステムにより計算された場合、Unified Communications Manager は新しいコールを拒否します。コールスロットリングが有効であるとき、新しいコールを試行するユーザはリオーダー音を受信します。電話機モデルによっては、電話機のディスプレイにプロンプトが表示される場合もあります。

コールスロットルを使用すると、ユーザがシステム管理者または電話機が故障しているかどうかについて不満を示す非常に長い遅延が回避されます。システムはそのような遅延が発生するタイミングを予測するため、複雑なアルゴリズムを使用して常時システムを監視します。

ダイヤルトーンへの遅延がコールスロットリングサービスパラメータのガイドラインの範囲内である場合は、Unified Communications Manager は Code Yellow 状態を終了してスロットリングを中止し、新しいコールは再び許可されるようになります。

コール スロットリングの設定

⚠

注意 コール スロットリング パラメータは、カスタマー サポートに指示された場合を除き、変更しないことを推奨します。

コール スロットリングは、システムが過負荷なコール アクティビティ、低い CPU の可用性、ディスク フラグメンテーションなどの状況を検出すると自動的に発生します。これらの状況が修正されると、システムはスロットリングを自動的に終了します。

コール スロットリングの設定

コール スロットリングは、システムが過負荷なコール アクティビティ、低い CPU の可用性、ディスク フラグメンテーションなどの状況を検出すると自動的に発生します。これらの状況が修正されると、システムはスロットリングを自動的に終了します。コール スロットリングは、拡張サービスパラメータを使用して設定します。ほとんどの導入環境では、デフォルト設定で十分です。

⚠

注意 コール スロットリング パラメータは、カスタマー サポートに指示された場合を除き、変更しないことを推奨します。

手順

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

ステップ 2 [サーバ（Server）] ドロップダウン リストからサーバを選択します。

ステップ 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。

ステップ 4 [詳細設定（Advanced）] をクリックします。

ステップ 5 [コールスロットリング（Call Throttling）] で、コール スロットリングのサービス パラメータの値を設定します。パラメータに関するヘルプの説明を参照するには、GUI でパラメータ名をクリックします。

- [コードイエローエントリ遅延（Code Yellow Entry Latency）]
- [コードイエロー終了遅延カレンダー（Code Yellow Exit Latency Calendar）]
- [コードイエロー継続時間（Code Yellow Duration）]
- [最大許容イベント数（Max Events Allowed）]

- [システムスロットルのサンプルサイズ（System Throttle Sample Size）]

ステップ 6 [保存（Save）] をクリックします。

メモリ スロットリングの設定

システムのメモリ スロットリングを設定するには、このの手順を使用します。

手順

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

ステップ 2 [サーバ（Server）] ドロップダウン リストから、Unified Communications Manager サーバを選択します。

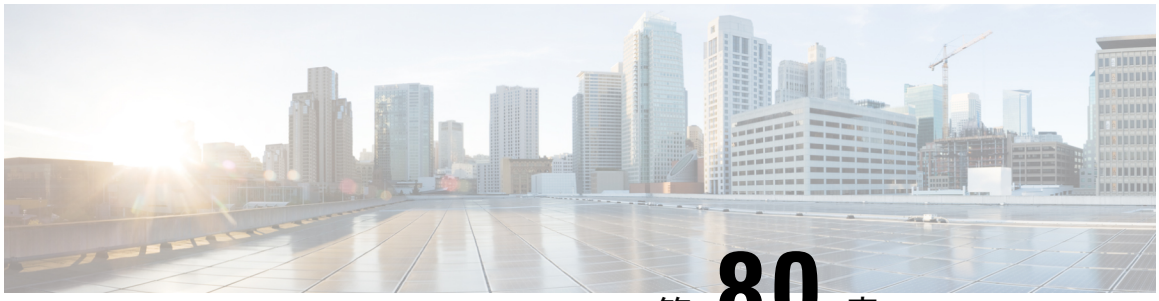
ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。

ステップ 4 [詳細設定（Advanced）] をクリックします。

ステップ 5 [メモリ スロットリングの有効化（Enable Memory Throttling）] パラメータを True に設定します。

ステップ 6 [メモリ スロットル（Memory Throttling）] 領域で、追加のサービス パラメータの値を設定します。パラメータのヘルプを参照するには、GUI でパラメータ名をクリックします。

ステップ 7 [保存（Save）] をクリックします。



第 80 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 パターンやトランスレーション 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）ごとに発信側トランスフォーメーションパターンを設定し、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、発信側のトランスフォーメーション 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 パターンと着信側トランスフォーメーション 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
- トランスレーション パターン
- 発信番号トランスフォーメーション 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、トランスレーション 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、トランスレーション パターン、およびトランスフォーメーション 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
ステップ 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 • トランスレーション パターン • 発信番号トランスフォーメーション パターン	
ステップ 2	発信側番号のグローバル化 （764 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。
ステップ 3	コーリング サーチ スペースの設定 （765 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する
ステップ 4	発信側トランスフォーメーション パターンの作成 （765 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
ステップ 5	コーリング サーチ スペースへの発信側トランスフォーメーション パターンの適用 （766 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

ステップ 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、コール 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。

ステップ 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

ステップ 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。

ステップ 2 ネットワークのパーティションを作成します。

ステップ 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。

ステップ 4 発信側トランスフォーメーション パターンのコーリング サーチ スペースを作成します。

ステップ 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。

発信側トランスフォーメーション 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トランスフォーメーション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

ステップ 1 Cisco Unified CM Administration で、**[コール ルーティング（Call Routing）] > [トランスフォーメーション パターン（Transformation Pattern）] > [発信側トランスフォーメーション パターン（Calling Party Transformation Pattern）]** を選択します。

ステップ 2 トランスフォーメーション パターンを作成します。

ステップ 3 作成する発信側トランスフォーメーション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。

ステップ 4 それぞれの発信側トランスフォーメーション 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トランスフォーメーション 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、着信する発信側トランスフォーメーション CSS を割り当てます。

手順

ステップ 1 Cisco Unified CM Administration で、発信側トランスフォーメーション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）]

ステップ 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、適用する発信側トランスレーション 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。

ステップ 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、適用する発信側トランスレーション 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 *91* : 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、発信側トランスフォーメーションを設定して、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 ポート用の発信側トランスフォーメーション 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トランスフォーメーション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 プールの発信側トランスフォーメーション CSS は、[電話の設定(Phone Configuration)] ウィンドウで [デバイス プールの発信側トランスフォーメーション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。

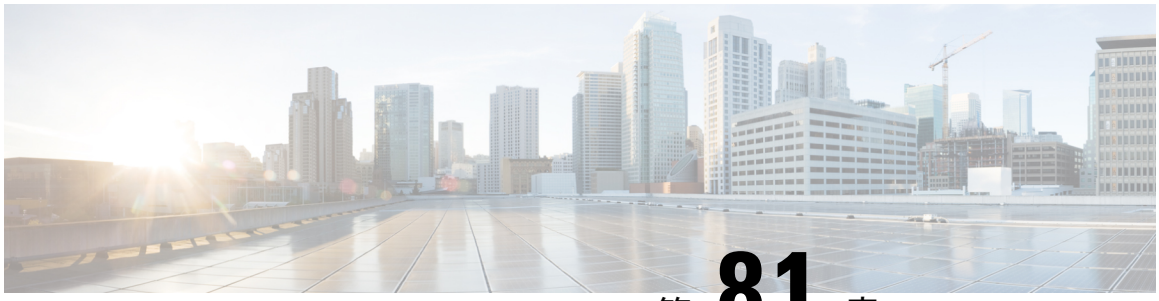
発信側の正規化の制限事項

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 *92 :* 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トランスフォーメーション 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。
発信側トランスフォーメーション 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トランスフォーメーションを適用する必要があります。[発信側トランスフォーメーション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 [発信側トランスフォーメーションパターン（Calling Party Transformation Pattern）] を設定してください。

機能	制限事項
T1-CAS および FXO ポート	発信側トランスフォーメーション 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。
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 81 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

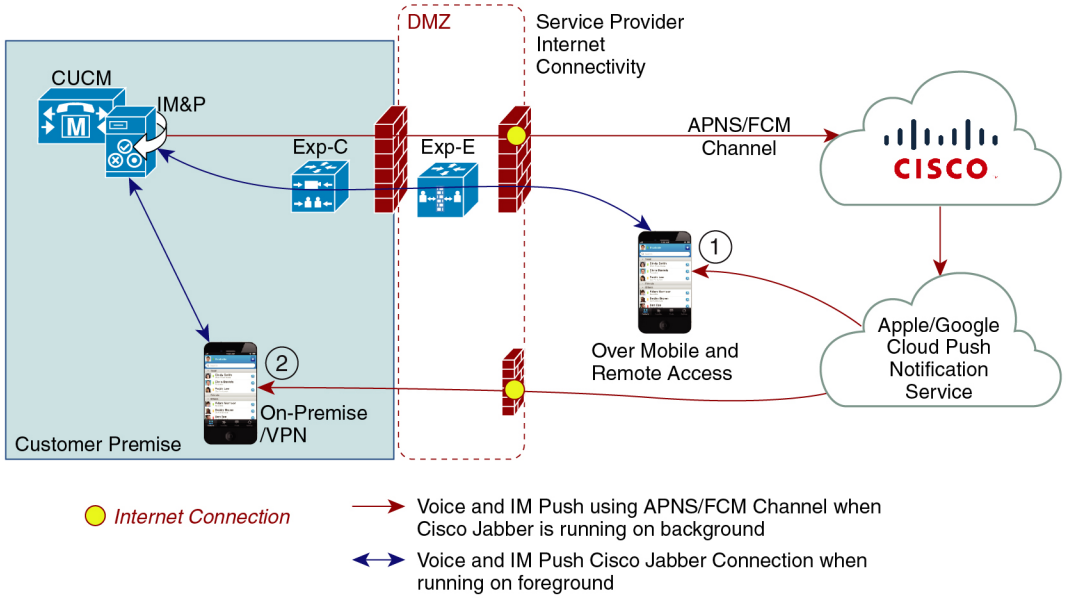
Android および iOS プラットフォームデバイスにインストールされているクライアントは、起動時に Unified Communications Manager、IM and Presence Service、および Google と Apple のクラウドに登録します。モバイルおよびリモートアクセス展開では、クライアントは Expressway 経由でオンプレミスサーバに登録します。Cisco Jabber および Cisco Webex クライアントがフォアグラウンドモードになっている限り、Unified Communications Manager および IM and Presence 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。

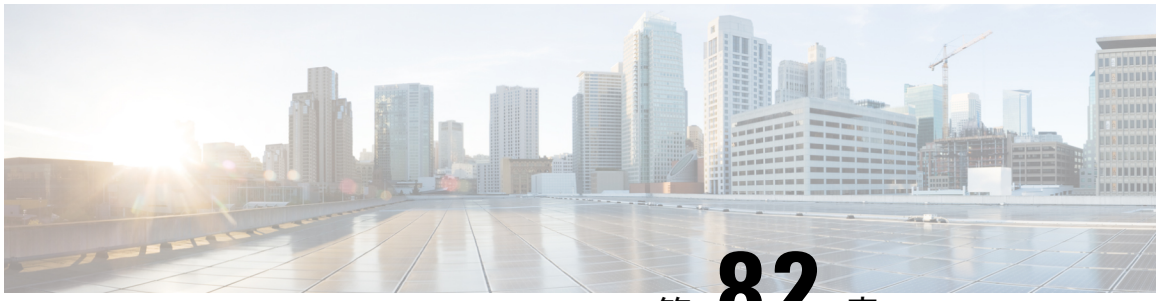
Cisco Jabber または Cisco Webex クライアントの動作モード	Cisco Jabber が iOS12 デバイスで実行されている場合	Cisco Jabber が iOS13 デバイスまたは Android デバイスで実行されている場合
サスペンドモード（バックグラウンドモード）	ビデオまたはビデオ コール 標準の通信チャネルは使用できません。Unified CM はプッシュ通知チャネルを使用します。 通知を受信すると、Cisco Jabber または Cisco Webex クライアントは自動的にフォアグラウンドモードに戻り、クライアントが呼出音を鳴らします。 メッセージ 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 82 章

論理パーティション分割の設定

論理パーティションの概要

論理パーティショニングを使用すると、コールの分離に関する規制要件を満たす一方で、単一のシステム上で PSTN と VoIP のコールをサポートできます。たとえば、インドの規制の制約の下では、外部電話機で送受信されたすべてのコールは、接続の完全な長さに応じたローカルまたは長距離のサービスプロバイダーによって送受信される必要があります。発信者の所在地と電話番号に従って PSTN または VoIP ネットワークに適切にコールをルーティングする単一の Unified Communications Manager クラスタを作成することができます。

論理パーティション設定では、どの VoIP デバイスが相互に通信できるかを定義します。ユーザは、1 本の PSTN と 1 回線を使用して VoIP を使用していることを覚えておく必要はありません。オフネットコールを行う電話機は、PSTN ゲートウェイとのみ通信することができます。VoIP および PSTN コールを個別に処理するために 2 つのネットワークを用意するのと似ていますが、デュアルインフラストラクチャの費用はかかりません。

論理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
ステップ 1	論理パーティションの有効化 （780 ページ）	論理パーティションの有効化
ステップ 2	地理位置情報の設定 （781 ページ） を行うには、次のサブタスクを実行します。 • 地理位置情報の作成 （781 ページ）	地理位置情報を設定するのは、ロケーションの定義とそのデバイスへの割り当ての 2 段階のプロセスです。また、クラ

	コマンドまたはアクション	目的
	• 地理位置情報の割り当て （782 ページ） • デフォルトの地理位置情報の設定 （782 ページ）	スタ内の全デバイスが使用するデフォルトのロケーションを設定できます。
ステップ 3	論理パーティション分割のデフォルトポリシーの設定 （783 ページ）	位置情報または位置情報フィルタに関連付けられていないデバイスのデフォルトポリシーを設定します。このポリシーでは、これらのデバイス間の PSTN コールを許可または拒否します。
ステップ 4	論理パーティションのチェックを回避するためのデバイスの設定 （783 ページ）	デバイスとデバイスプールをパーティショニング チェックから特に除外できます。
ステップ 5	地理位置情報フィルタの設定 （784 ページ）を行うには、次のサブタスクを実行します。 • 地理位置情報フィルタ ルールの作成 （785 ページ） • 地理位置情報フィルタの割り当て （785 ページ） • デフォルトの地理位置情報フィルタの設定 （786 ページ）	論理パーティショニングでは、ロケーションに基づいて、各デバイスに一意の ID を割り当てます。1 つのデバイスが別のデバイスをコールすると、コールを許可するかどうかと、ルートが適切であるかを判別するために、これらの ID を使用します。この識別子の作成に使用するフィールドを選択できます。たとえば、ビルディング内の部屋またはフロアに応じて異なるポリシーを適用できます。
ステップ 6	論理パーティション ポリシー レコードの定義 （786 ページ）	地理位置情報中のコールを許可または拒否するための論理的なパーティショニング ポリシーのセットを定義します。地理位置情報間のコールの続行が許可される前に、システムはこれらのポリシーに基づいて指定された地理位置情報間でコールが許可されていることを確認します。
ステップ 7	（任意） ロケーション伝達の有効化 （787 ページ）	デバイスに関する位置情報をクラスタ間で伝達する必要がある場合は、ロケーション伝達を設定します。

論理パーティションの有効化

論理パーティション分割機能を有効化するには、この手順を使用します。

手順

ステップ 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。

ステップ 2 [論理パーティションを有効にする（Enable Logical Parititioning）] エンタープライズ パラメータのドロップダウン リストから [True] を選択します。

ステップ 3 [保存（Save）] をクリックします。

地理位置情報の設定

地理位置情報を設定するのは、ロケーションの定義とそのデバイスへの割り当ての2段階のプロセスです。また、クラスタ内の全デバイスが使用するデフォルトのロケーションを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	地理位置情報の作成 （781 ページ）	地理位置情報を指定するには、地理的な場所を設定します。この情報は、デバイスを論理パーティション分割などの規制機能と関連付けるために使用されます。地理位置情報は、国内の規制など、ポリシーの判断で使用されます。
ステップ 2	地理位置情報の割り当て （782 ページ）	デバイスまたはデバイス プールに地理位置情報を割り当てます。
ステップ 3	デフォルトの地理位置情報の設定 （782 ページ）	このクラスタ内のすべてのデバイスとデバイスプールのデフォルトの地理位置情報を指定します。

地理位置情報の作成

システムのデバイスに割り当てる地理位置情報を作成するには、次の手順を使用します。論理パーティションには地理位置情報を使用できます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [地理位置情報の設定（Geolocation Configuration）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 地理位置情報の [名前（Name）] を入力します。

ステップ 4 [地理位置情報の設定（Geolocation 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。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 さらに地理位置情報を作成するには、この手順を繰り返します。

地理位置情報の割り当て

デバイスまたはデバイス プールに地理位置情報を割り当てます。

手順

ステップ 1 Cisco Unified CM Administration から、次のいずれかのメニュー項目を選択します。

- **[デバイス（Device）] > [電話（Phone）]**
- **[デバイス（Device）] > [トランク（Trunk）]**
- **[デバイス（Device）] > [ゲートウェイ（Gateway）]**
- **[システム（System）] > [デバイスプール（Device Pool）]**

ステップ 2 次のいずれかの操作を実行します。

- 既存のデバイスまたはデバイスプールの設定を変更するには、[検索（Find）]をクリックします。検索条件を入力し、結果のリストから既存のデバイスまたはデバイスプールを選択します。
- 新しいデバイスまたはデバイス プールを追加するには、[新規追加（Add New）] をクリックします。デバイスについては、必要に応じてデバイスのタイプとプロトコルを選択し、[次へ（Next）] をクリックします。

ステップ 3 地理位置情報ドロップダウンリストから、設定した地理位置情報を選択します。

ステップ 4 [保存（Save）] をクリックします。

デフォルトの地理位置情報の設定

このクラスタ内のすべてのデバイスとデバイスプールのデフォルトの地理位置情報を指定します。

手順

ステップ 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。

ステップ 2 [デフォルトの地理位置情報（Default Geolocation）] ドロップダウン リストから、設定した地理位置情報を選択します。デフォルト値は、[未指定（Unspecified）] です。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 （任意） 特定のデバイスまたはデバイス プールでこのデフォルトをオーバーライドする必要がある場合は、[デバイス設定（Device Configuration）] または [デバイス プール設定（Device Pool Configuration）] ウィンドウのいずれかに値を入力し、[保存（Save）] をクリックします。

論理パーティション分割のデフォルト ポリシーの設定

位置情報または位置情報フィルタに関連付けられていないデバイスのデフォルトポリシーを設定します。このポリシーでは、これらのデバイス間の PSTN コールを許可または拒否します。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [論理パーティション分割ポリシーの設定（Logical Partitioning Policy Configuration）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [論理パーティション分割ポリシーの設定（Logical Partitioning Policy 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。

ステップ 4 [保存（Save）] をクリックします。

（注） 値の [許可（Allow）] が含まれていたポリシーの値が、後で [拒否（Deny）] に変更された場合、そのポリシーは [拒否（Deny）] のままになります。逆も同様です。前に [拒否（Deny）] に設定されていて、後で [許可（Allow）] に変更されたポリシーは、[許可（Allow）] になります。**[Cisco Unified Reporting] > [地理位置情報ポリシー レポート（Geolocation Policy Report）]** を使用して、重複するポリシーを特定できます。

論理パーティションのチェックを回避するためのデバイスの設定

デバイスとデバイスプールをパーティショニング チェックから特に除外できます。

手順

ステップ 1 Cisco Unified CM Administration から、次のいずれかのメニュー項目を選択します。

- **[デバイス（Device）] > [電話（Phone）]**

- **[デバイス（Device）] > [トランク（Trunk）]**
- **[デバイス（Device）] > [ゲートウェイ（Gateway）]**
- **[システム（System）] > [デバイスプール（Device Pool）]**

ステップ 2 次のいずれかの操作を実行します。

- 既存のデバイスまたはデバイス プールの設定を変更するには、[検索（Find）] をクリックします。検索条件を入力し、結果のリストから既存のデバイスまたはデバイス プールを選択します。
- 新しいデバイスまたはデバイス プールを追加するには、[新規追加（Add New）] をクリックします。デバイスについては、必要に応じてデバイスのタイプとプロトコルを選択し、[次へ（Next）] をクリックします。

ステップ 3 **地理位置情報**ドロップダウンリストから、**未指定**を選択します。

ステップ 4 [保存（Save）] をクリックします。

地理位置情報フィルタの設定

論理パーティショニングでは、ロケーションに基づいて、各デバイスに一意の ID を割り当てます。1 つのデバイスが別のデバイスをコールすると、コールを許可するかどうかと、ルートが適切であるかを判別するために、これらの ID を使用します。この識別子の作成に使用するフィールドを選択できます。たとえば、ビルディング内の部屋またはフロアに応じて異なるポリシーを適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	地理位置情報フィルタ ルールの作成（785 ページ）	地理位置情報識別子を作成するために使用するフィールドを指定するために、地理位置情報フィルタを設定します。この機能は、地理位置情報オブジェクトのサブセットで、ポリシー決定を行うために使用されます。
ステップ 2	地理位置情報フィルタの割り当て （785 ページ）	
ステップ 3	デフォルトの地理位置情報フィルタの設定 （786 ページ）	デフォルトの地理位置情報フィルタエンタープライズパラメータを設定して、クラスタのデフォルトの地理位置情報フィルタを指定します。このパラメータは、地理位置情報が関連付けられていないすべてのデバイスおよびデバイスプールのデフォルトの地理位置情報フィルタ設定を決定します。

地理位置情報フィルタ ルールの作成

論理パーティション分割の決定に使用できる地理位置情報フィルタを作成するには、この手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [地理位置情報フィルタ（Geolocation Filter）]** の順に選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 フィルタの [名前（Name）] と [説明（Description）] を入力します。

ステップ 4 論理パーティション分割の決定に使用する項目に対応するチェックボックスをオンにします。

ステップ 5 [地理位置情報フィルタの設定（Geolocation Filter 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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 これらの手順を繰り返して、追加の地理位置情報フィルタを作成します。

地理位置情報フィルタの割り当て

手順

ステップ 1 Cisco Unified CM Administration から、次のいずれかのメニュー項目を選択します。

- **[デバイス（Device）] > [電話（Phone）]**
- **[デバイス（Device）] > [トランク（Trunk）]**
- **[デバイス（Device）] > [ゲートウェイ（Gateway）]**
- **[システム（System）] > [デバイスプール（Device Pool）]**

ステップ 2 次のいずれかの操作を実行します。

- 既存のデバイスまたはデバイス プールの設定を変更するには、[検索（Find）] をクリックします。検索条件を入力し、結果のリストから既存のデバイスまたはデバイスプールを選択します。
- 新しいデバイスまたはデバイス プールを追加するには、[新規追加（Add New）] をクリックします。デバイスについては、必要に応じてデバイスのタイプとプロトコルを選択し、[次へ（Next）] をクリックします。

ステップ 3 **地理位置情報フィルタ** ドロップダウンリストから、設定した地理位置情報を選択します。

ステップ 4 [保存（Save）] をクリックします。

デフォルトの地理位置情報フィルタの設定

手順

ステップ 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。

ステップ 2 [デフォルトの地理位置情報（Default Geolocation）] ドロップダウン リストから、設定した地理位置情報を選択します。デフォルト値は、[未指定（Unspecified）] です。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 （任意） 特定のデバイスまたはデバイス プールでこのデフォルトをオーバーライドする必要がある場合は、[デバイス設定（Device Configuration）] または [デバイス プール設定（Device Pool Configuration）] ウィンドウのいずれかに地理位置情報フィルタのデフォルト値を入力し、[保存（Save）] をクリックします。

論理パーティション ポリシー レコードの定義

地理位置情報中のコールを許可または拒否するための論理的なパーティショニング ポリシーのセットを定義します。地理位置情報間のコールの続行が許可される前に、システムはこれらのポリシーに基づいて指定された地理位置情報間でコールが許可されていることを確認します。

手順

ステップ 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）] > [論理パーティションポリシーの設定（Logical Partitioning Policy Configuration）]** を選択します。

ステップ 2 次のいずれかの操作を実行します。

- 既存の論理パーティション ポリシーの設定を変更するには、[検索（Find）] をクリックします。検索条件を入力し、結果のリストから既存の論理パーティション ポリシーを選択します。
- 新しい論理パーティション 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。

ステップ 3 [論理パーティション ポリシーの設定（Logical Partitioning Policy 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。

（注） ポリシーに設定値を指定せずに空欄のままにした場合、ブランクの地理位置情報ポリシーになります。論理パーティション分割が空欄になっている特定のデバイスタイプに対して論理ポリシーを設定すると、Unified Communications Managerによって、設定されたデバイス タイプにポリシーの値（[許可（Allow）] または [拒否（Deny）]）が追加されます。

ステップ 4 [保存（Save）] をクリックします。

ロケーション伝達の有効化

ロケーション伝達は、クラスタ間で地理位置情報を共有できるようにするためのオプションの設定です。

手順

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

ステップ 2 次のいずれかを実行します。

- 既存のトランクを選択するには、[検索（Find）] をクリックします。
- **[新規追加（Add New）]** をクリックして、新しいトランクを設定します。

ステップ 3 **[トランクの設定]** 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。

ステップ 4 **[位置情報]** 領域で、**地理位置情報**と**地理位置情報フィルター**を選択します。

ステップ 5 場所の伝達を有効にするには、**[地理位置情報を送信する]** チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

論理的パーティションの連携動作と制限事項

論理パーティション分割の連携動作

表 *93 :* 論理パーティション分割の連携動作

機能	連携動作
アドホック会議、参加、複数ライン同時通話機能、不在転送、コール転送	論理パーティション分割は、次の状況では行われません。 • すべての参加者が VoIP 電話機である場合。 • 位置情報と位置情報フィルタがどのデバイスにも関連付けられていない場合。
割り込み、C 割り込み、およびリモート再開	論理パーティション分割は、次の状況では行われません。 • 発信側と着信側の両方のデバイスが VoIP 電話機であるときに、論理パーティション ポリシー チェックが無視される場合。 • C 割り込み/割り込みの参加者の場合、論理パーティション ポリシー チェックが存在せず、論理パーティション拒否シナリオを防止できません。
Cisco Unified Mobility	論理パーティション分割は、次の状況では行われません。 • 位置情報または位置情報フィルタが、参加するデバイスに関連付けられていない場合。 • デュアル モードの電話機を使用するとき、論理パーティション分割サポートはありません。
CTI 処理	論理パーティション分割は、次の状況では行われません。 • 位置情報または位置情報フィルタがデバイスに関連付けられていないときに、処理が発生しない場合。 • 参加しているすべてのデバイスが VoIP 電話機であるときに、処理が発生しない場合。

機能	連携動作
エクステンションモビリティ	論理パーティション分割は、次の状況では行われません。 • 地理位置情報または地理位置情報フィルタが、Cisco Extension Mobility にログインする VoIP 電話機にも、発信側と着信側のデバイスにも関連付けられない場合。 • Cisco Extension Mobility にログインする VoIP 電話機がコールするか、または VoIP 電話機からのコールを取得する場合。
Meet-Me 会議	論理パーティション分割は、次の状況では行われません。 • すべての参加者が VoIP 電話機であるときに、処理が発生しない場合。 • 位置情報または位置情報フィルタがデバイスに関連付けられていないと、そのデバイスに対してポリシー チェックが実行されない場合。
ルートリストおよびハント パイロット	論理パーティション分割は、次の状況では行われません。 • 発信側と着信側の両方のデバイスが VoIP 電話機であるときに、処理が発生しない場合。 • すべてのデバイスに位置情報と位置情報フィルタの両方を関連付ける必要がある場合。デバイスに位置情報も位置情報フィルタも関連付けられていない場合、処理は発生しません。
共有回線	論理パーティション分割は、次の状況では行われません。 • 発信側と着信側の両方のデバイスが VoIP 電話機であるときに、処理が発生しない場合。 • 位置情報または位置情報フィルタがデバイスに関連付けられていないときに、処理が発生しない場合。

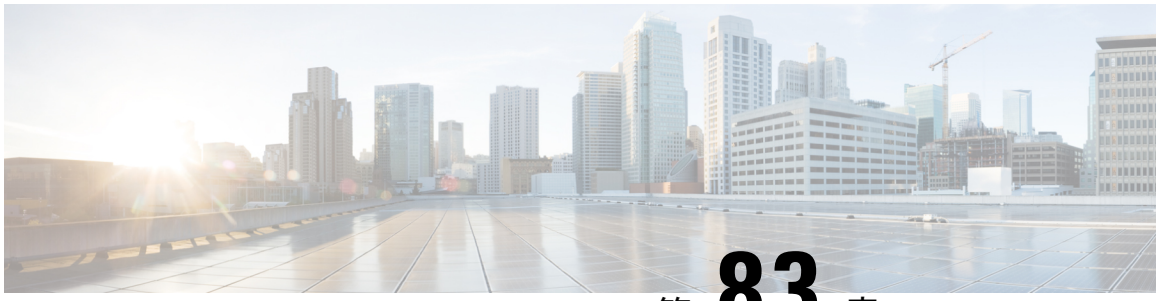
論理パーティション分割の制限事項

表 *94* : 論理パーティション分割の制限事項

制限事項	説明
割り込み/C 割り込み	Barge/cBarge は発生しません。コールインスタンスが削除されます。 C 割り込み/割り込みの参加者の場合、論理パーティション ポリシー チェックが存在せず、論理パーティション拒否シナリオを防止できません。

制限事項	説明
BLF プレゼンス	論理パーティション ポリシーでは、BLF プレゼンス通知はチェックされません。
Cisco Extension Mobility	Cisco Extension Mobilityが別の位置情報の電話機にログインする場合、ローカルルートグループが設定されているときに、発信 PSTN コールが発生する可能性があります。着信 PSTN コールは電話機に対して発信されませんが、リオーダー音を受信します。
Cisco Unified MeetingPlace	システムは、Cisco Unified MeetingPlace または Cisco Unified MeetingPlace Express に関連するコールの論理パーティション機能をサポートしていません。
会議	会議チェーンで会議をまたぐ参加者に対して論理パーティション チェックがサポートされない。 たとえば、ミートミーおよびアドホックの会議チェーンには、論理パーティション拒否の参加者が参加できます。
H.225 ゲートキーパー制御トランク	Cisco Unified Communications Manager は、H.225 ゲートキーパー制御のトランク経由で位置情報を通知しない。
323 および MGCP ゲートウェイ	Cisco Unified Communications Manager は、塵位置情報を H.323 または MGCP ゲートウェイに通知しない。 SIP トランクのチェックボックスに基づいて、SIP ゲートウェイへの通信を無効にすることができます。
モビリティ携帯電話ピックアップ	携帯電話でコールに応答すると、論理パーティション拒否処理が実行されます。 コールが携帯電話に発信される前に、論理パーティションポリシーチェックは発生しません（基本 SNR コールの場合には発生します）。システムは、携帯電話がコールに応答した後、論理パーティション分割ポリシーを確認します。
QSIG クラスタ間トランク	Q.SIG プロトコルを使用したクラスタ間トランク (ICT) は、発信者または受信側デバイスの地理位置情報を通信することを許可されていません。Q.SIG トンネル化プロトコルが選択されたときには、「[地理位置情報の送信]」 の ICT 設定が無効になります。
リオーダー音	IOS H.323 ゲートウェイおよび SIP ゲートウェイでは、コールの接続がリリースされても、論理パーティション ポリシーにより、リオーダー音が発生しません。
共有回線アクティブコール	論理パーティションが制限されるシナリオでは、ある機能によって共有回線コールが許可カテゴリに移動される場合でも、共有回線はコール期間中にアクティブ コール情報をドロップします。

制限事項	説明
User Agent Server; ユーザ エージェント サーバ	この位置情報を受信する論理パーティション対応クラスタで実行される論理パーティションポリシーチェックでは、ポリシーが拒否されると、コールがキャンセルされることがあります。



第 83 章

地理位置情報とロケーション伝達の設定

地理位置情報およびロケーション伝達の概要

地理位置情報を使用して、ポリシーの決定で使用するデバイスの地理的な場所 (または都市の住所) を定義します。たとえば、ある電話から別の電話へのコールが許可されているかどうかなどです。位置情報は、Request for Comments（RFC）4119 標準に基づいています。

コールが確立され、コール中に、塵位置情報の伝達を使用して、あるクラスタから別のクラスタに、地理位置情報の通信を許可します。

地理位置情報とロケーションの伝達タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	地理位置情報の設定 （794 ページ）を行うには、次のサブタスクを実行します。 • 位置情報の設定 （794 ページ） • 地理位置情報の割り当て （795 ページ） • デフォルトの地理位置情報の設定 （795 ページ） • ロケーション配信の設定 （796 ページ）	地理位置情報を指定するには、地理的な場所を設定します。この情報は、デバイスを論理パーティション分割などの規制機能と関連付けるために使用されます。地理位置情報は、国内の規制など、ポリシーの判断で使用されます。
ステップ 2	地理位置情報フィルタの設定 （797 ページ）を行うには、次のサブタスクを実行します。	地理位置情報フィルタを設定して、地理位置情報の識別子を作成するために使用するフィールドを選択します。この機能

	コマンドまたはアクション	目的
	• 地理位置情報フィルタの設定 （797 ページ） • 地理位置情報フィルタの割り当て （798 ページ） • デフォルトの地理位置情報フィルタの設定 （798 ページ）	は、地理位置情報オブジェクトのサブセットで、ポリシー決定を行うために使用されます。地理位置情報フィルタでは、異なるデバイスの地理位置情報を比較するときに使用する地理位置情報のオブジェクトを定義します。たとえば、電話機のグループには、それらの電話機が置かれている部屋やフロアを除いて、同じジオロケーションが割り当てられる可能性があります。各電話の実際のジオロケーションは異なりますが、フィルタ処理されたジオロケーションは同じになります。

地理位置情報の設定

手順

	コマンドまたはアクション	目的
ステップ 1	位置情報の設定 （794 ページ）	地理位置情報を指定するには、地理的な場所を設定します。この情報は、デバイスを論理パーティション分割などの規制機能と関連付けるために使用されます。地理位置情報は、国内の規制など、ポリシーの判断で使用されます。
ステップ 2	地理位置情報の割り当て （795 ページ）	デバイスまたはデバイス プールに地理位置情報を割り当てます。
ステップ 3	デフォルトの地理位置情報の設定 （795 ページ）	このクラスタ内のすべてのデバイスとデバイスプールのデフォルトの地理位置情報を指定します。
ステップ 4	（任意） ロケーション配信の設定 （796 ページ）	デバイスに関する位置情報をクラスタ間で伝達する必要がある場合は、ロケーション伝達を設定します。

位置情報の設定

地理位置情報を指定するには、地理的な場所を設定します。この情報は、デバイスを論理パーティション分割などの規制機能と関連付けるために使用されます。地理位置情報は、国内の規制など、ポリシーの判断で使用されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [地理位置情報の設定（Geolocation Configuration）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 地理位置情報の [名前（Name）] を入力します。

ステップ 4 [地理位置情報の設定（Geolocation 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。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 さらに地理位置情報を作成するには、この手順を繰り返します。

地理位置情報の割り当て

デバイスまたはデバイス プールに地理位置情報を割り当てます。

手順

ステップ 1 Cisco Unified CM Administration から、次のいずれかのメニュー項目を選択します。

- **[デバイス（Device）] > [電話（Phone）]**
- **[デバイス（Device）] > [トランク（Trunk）]**
- **[デバイス（Device）] > [ゲートウェイ（Gateway）]**
- **[システム（System）] > [デバイスプール（Device Pool）]**

ステップ 2 次のいずれかの操作を実行します。

- 既存のデバイスまたはデバイス プールの設定を変更するには、[検索（Find）] をクリックします。検索条件を入力し、結果のリストから既存のデバイスまたはデバイスプールを選択します。
- 新しいデバイスまたはデバイス プールを追加するには、[新規追加（Add New）] をクリックします。デバイスについては、必要に応じてデバイスのタイプとプロトコルを選択し、[次へ（Next）] をクリックします。

ステップ 3 地理位置情報ドロップダウンリストから、設定した地理位置情報を選択します。

ステップ 4 [保存（Save）] をクリックします。

デフォルトの地理位置情報の設定

このクラスタ内のすべてのデバイスとデバイスプールのデフォルトの地理位置情報を指定します。

始める前に

地理位置情報の割り当て （795 ページ）

手順

ステップ 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。

ステップ 2 [デフォルトの地理位置情報（Default Geolocation）] ドロップダウン リストから、設定した地理位置情報を選択します。デフォルト値は、[未指定（Unspecified）] です。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 （任意） 特定のデバイスまたはデバイス プールでこのデフォルトをオーバーライドする必要がある場合は、[デバイス設定（Device Configuration）] または [デバイス プール設定（Device Pool Configuration）] ウィンドウのいずれかに値を入力し、[保存（Save）] をクリックします。

次のタスク

- （省略可） ロケーション配信の設定 （796 ページ）
- 地理位置情報フィルタの設定 （797 ページ）

ロケーション配信の設定

デバイスに関する位置情報をクラスタ間で伝達する必要がある場合は、ロケーション伝達を設定します。

始める前に

- 位置情報の設定 （794 ページ）
- 地理位置情報の割り当て （795 ページ）
- デフォルトの地理位置情報の設定 （795 ページ）

手順

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

ステップ 2 次のいずれかを実行します。

- 既存のトランクを選択するには、[検索（Find）] をクリックします。
- **[新規追加（Add New）]** をクリックして、新しいトランクを設定します。

ステップ 3 **[トランクの設定]**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。

ステップ 4 **[位置情報]**領域で、**地理位置情報**と**地理位置情報フィルター**を選択します。

ステップ 5 場所の伝達を有効にするには、**[地理位置情報を送信する]**チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

地理位置情報フィルタの設定

地理位置情報フィルタを設定して、地理位置情報の識別子を作成するために使用するフィールドを選択します。この機能は、地理位置情報オブジェクトのサブセットで、ポリシー決定を行うために使用されます。地理位置情報フィルタでは、異なるデバイスの地理位置情報を比較するときに使用する地理位置情報のオブジェクトを定義します。たとえば、電話機のグループには、それらの電話機が置かれている部屋やフロアを除いて、同じジオロケーションが割り当てられる可能性があります。各電話の実際のジオロケーションは異なりますが、フィルタ処理されたジオロケーションは同じになります。

手順

	コマンドまたはアクション	目的
ステップ 1	地理位置情報フィルタの設定 （797 ページ）	地理位置情報識別子を作成するために使用するフィールドを指定するために、地理位置情報フィルタを設定します。この機能は、地理位置情報オブジェクトのサブセットで、ポリシー決定を行うために使用されます。
ステップ 2	地理位置情報フィルタの割り当て （798 ページ）	
ステップ 3	デフォルトの地理位置情報フィルタの設定 （798 ページ）	デフォルトの地理位置情報フィルタエンタープライズパラメータを設定して、クラスタのデフォルトの地理位置情報フィルタを指定します。このパラメータは、地理位置情報が関連付けられていないすべてのデバイスおよびデバイスプールのデフォルトの地理位置情報フィルタ設定を決定します。

地理位置情報フィルタの設定

地理位置情報識別子を作成するために使用するフィールドを指定するために、地理位置情報フィルタを設定します。この機能は、地理位置情報オブジェクトのサブセットで、ポリシー決定を行うために使用されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [地理位置情報フィルタ（Geolocation Filter）]** の順に選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 フィルタの [名前（Name）] と [説明（Description）] を入力します。

ステップ 4 論理パーティション分割の決定に使用する項目に対応するチェックボックスをオンにします。

ステップ 5 [地理位置情報フィルタの設定（Geolocation Filter 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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 これらの手順を繰り返して、追加の地理位置情報フィルタを作成します。

地理位置情報フィルタの割り当て

手順

ステップ 1 Cisco Unified CM Administration から、次のいずれかのメニュー項目を選択します。

- **[デバイス（Device）] > [電話（Phone）]**
- **[デバイス（Device）] > [トランク（Trunk）]**
- **[デバイス（Device）] > [ゲートウェイ（Gateway）]**
- **[システム（System）] > [デバイスプール（Device Pool）]**

ステップ 2 次のいずれかの操作を実行します。

- 既存のデバイスまたはデバイスプールの設定を変更するには、[検索（Find）] をクリックします。検索条件を入力し、結果のリストから既存のデバイスまたはデバイスプールを選択します。
- 新しいデバイスまたはデバイスプールを追加するには、[新規追加（Add New）] をクリックします。デバイスについては、必要に応じてデバイスのタイプとプロトコルを選択し、[次へ（Next）] をクリックします。

ステップ 3 **地理位置情報フィルタ** ドロップダウンリストから、設定した地理位置情報を選択します。

ステップ 4 [保存（Save）] をクリックします。

デフォルトの地理位置情報フィルタの設定

デフォルトの地理位置情報フィルタエンタープライズパラメータを設定して、クラスタのデフォルトの地理位置情報フィルタを指定します。このパラメータは、地理位置情報が関連付け

られていないすべてのデバイスおよびデバイスプールのデフォルトの地理位置情報フィルタ設定を決定します。

始める前に

地理位置情報フィルタの割り当て （798 ページ）

手順

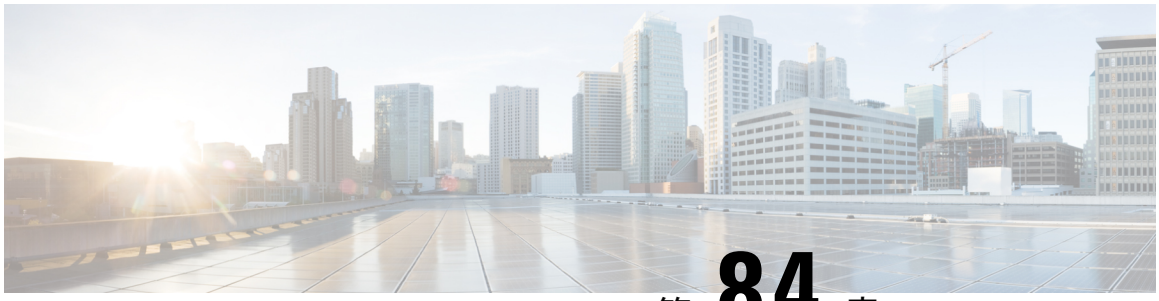
ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

ステップ 2 [デフォルトの地理位置情報（Default Geolocation）] ドロップダウン リストから、設定した地理位置情報を選択します。デフォルト値は、[未指定（Unspecified）] です。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 （任意） 特定のデバイスまたはデバイス プールでこのデフォルトをオーバーライドする必要がある場合は、[デバイス設定（Device Configuration）] または [デバイス プール設定（Device Pool Configuration）] ウィンドウのいずれかに地理位置情報フィルタのデフォルト値を入力し、[保存（Save）] をクリックします。



第 84 章

ロケーション認識の設定

場所の認識の概要

ロケーション認識によって、管理者は企業ネットワークに接続している電話の接続元となる物理的な場所を決定できます。ワイヤレスネットワークの場合は、ワイヤレスアクセスポイントインフラストラクチャと、それらのアクセスポイントに現在関連付けられているモバイルデバイスを表示できます。有線ネットワークの場合は、イーサネットスイッチインフラストラクチャを表示して、どのデバイスが現在それらのスイッチに接続しているか確認できます。これにより、コールが配置された建物、階、およびキューブを特定できます。

ネットワーク インフラストラクチャは、**Cisco Unified CM Administration** > **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points** > **Find and List Switches and Access Points** ウィンドウから表示できます。

この機能は、Unified Communications Manager データベースを次の情報を使用して動的に更新します。

- 各インフラストラクチャデバイスの、IP アドレス、BSSID 情報 (該当する場合)を含むスイッチや、ワイヤレスアクセスポイントなどのネットワークインフラストラクチャデバイス
- 各インフラストラクチャデバイスに関連付けられているエンドポイント (以下を含む)
  - ワイヤレスネットワークの場合は、ワイヤレスアクセスポイントに現在関連付けられているデバイスのリスト。
  - 有線ネットワークの場合は、イーサネットスイッチに現在接続されているデバイスとデバイスタイプのリストが表示されます。

Cisco Emergency Responder 統合

場所の認識により、Cisco Emergency Responder などの統合アプリケーションが、緊急コールを発信したユーザの物理的な場所を特定するのに役立ちます。位置認識が有効になっている場合、Cisco Emergency Responder は、新しいワイヤレスアクセスポイントに関連付けられたモバイルデバイス、または新しいイーサネットスイッチに接続されているデスク電話機との間のインフラストラクチャの関連付けに新しいデバイスを学習します。

Cisco Emergency Responder を初めて起動すると、現在のデバイスの Unified Communications Manager データベースとネットワーク インフラストラクチャの関連付けが照会されます。2 分おきに、Cisco Emergency Responder は、既存の関連付けが更新されていないかどうかを確認します。そのため、モバイルの発信者が移動中に緊急コールを受信した場合でも、Cisco Emergency Responder は、発信者の物理的な場所を迅速に判断し、適切な建物、階、またはキューブに緊急サービスを送信できます。

ワイヤレスネットワークの更新

ワイヤレスインフラストラクチャのロケーション認識を有効にするには、Unified Communications Manager で、Cisco Wireless LAN コントローラと同期するように設定します。Unified Communications Manager と最大 50 台のコントローラを同期できます。同期プロセス中に、Unified Communications Manager は、そのコントローラが管理しているアクセス ポイント インフラストラクチャでデータベースを更新します。Cisco Unified CM 管理者は、各アクセスポイントに関連付けられているモバイルクライアントのリストを含む、ワイヤレスアクセスポイントのステータスを表示できます。

モバイル クライアントがアクセス ポイント間を移動すると、エンドポイントからの SIP および SCCP シグナリングが、新しいデバイスとアクセスポイントの関連付けを Unified Communications Manager に伝達し、Unified Communications Manager がデータベースを更新します。また、Cisco Emergency Responder は、新しいエンドポイントが関連付けを変更したときに数分ごとに Unified Communications Manager データベースに照会することによって、新しい関連付けについて学習します。そのため、モバイルクライアントが緊急コールを発信すると、Cisco Emergency Responder は、そのコールを配置したユーザの物理的な場所に関する正確な情報を保持します。

ワイヤレス アクセス ポイント コントローラの定期的な同期スケジュールがある場合、Unified Communications Manager は、各同期の後にデータベースからのアクセス ポイントを動的に追加または更新します。

バルク管理を使用してアクセスポイントを挿入する

サードパーティ製のワイヤレス アクセス ポイント コントローラを使用している場合、またはシスコの主要インフラストラクチャからアクセスポイントをエクスポートする場合は、一括管理ツールを使用して、CSV ファイルからのワイヤレス アクセス ポイント インフラストラクチャを Unified Communications Manager データベースに一括挿入することができます。一括挿入後、モバイルデバイスから次の場所を更新すると、現在のアクセスポイントの関連付けによってデータベースが更新されます。

ただし、一括管理では、新しいアクセスポイントがワイヤレスネットワークに追加されたときにアクセスポイントインフラストラクチャを動的に更新することはできません。モバイルコールが、一括挿入後に追加されたアクセス ポイントを使用して配置された場合、そのアクセスポイントはデータベース内のレコードを持たないため、Unified Communications Manager は新しいアクセス ポイントの BSSID と一致しなくても、インフラストラクチャをマークすることになります。ワイヤレス デバイスの場合は、未識別 AP として使用されます。

一括管理ツールの詳細については、『*Cisco Unified Communications Manager* 一括管理ガイド』の「インフラストラクチャ デバイスの管理」の章を参照してください。

有線ネットワークの更新

有線インフラストラクチャについてロケーション認識を有効にするために何も設定する必要はありません。機能は自動的に有効になります。

有線電話を登録する際、電話機と Cisco Unified Communications Manager の間のシグナリングによって、スイッチ インフラストラクチャでデータベースが動的に更新されます。Cisco Unified CM Administration での会社のスイッチ インフラストラクチャに関する詳細を、特定のスイッチに接続されている電話機のリストも含め表示できます。

モバイルデバイスと異なり、有線デバイスは、通常、1 つのスイッチから別のスイッチにローミングしません。会社内で従業員が席を替わったときなどに起こり得る、電話機が移動しない場合は、電話機が新しいロケーションから再登録されると、新しいスイッチ情報でデータベースが更新されます。Cisco Unified Communications Manager で、新しいスイッチは移動された電話を接続されたエンドポイントとして表示されます。

スイッチが廃止され、ネットワーク インフラストラクチャから削除される場合、そのスイッチは、Cisco Unified Communications Manager 内で見えたままです。インフラストラクチャのビューから古いスイッチを削除するには、[アクセスポイントとスイッチの設定（Access Point and Switch Configuration）] ウィンドウで非アクティブ化する必要があります。

ロケーション認識をサポートするエンドポイント

次のエンドポイントは、位置認識によるトラッキングをサポートしています。

- Cisco Uniifed Wireless IP Phone 7925G
- Cisco Unified Wireless IP Phone 7921G-EX
- Cisco Unified Wireless IP Phone 7926G
- Cisco Jabber クライアント: 12.5 (1) SU1 でサポートされています。
- Cisco Wireless IP Phone 8821：12.5(1)SU1 でサポート
- Webex アプリ：12.5(1)SU1 でサポート

これらのエンドポイントは、BSSID などの上流のインフラストラクチャ情報を、Cisco Unified Communications Manager に提供します。Cisco Emergency Responder は、AXL の変更通知を介して、関連付けられたアクセスポイントを使用してデバイスを追跡できます。

デバイスのトラッキングを動作させるには、ワイヤレスアクセスポイントを Cisco Unified Communications Manager で定義する必要があります。これを行うには、ワイヤレスアクセスポイントコントローラを同期するか、または一括管理を使用してワイヤレスアクセスポイントインフラストラクチャをインポートします。

場所の認識の前提条件

この機能を使用すると、複数の Cisco Wireless LAN コントローラを使用して、Cisco Unified Communications Manager データベースを同期することができます。また、Cisco Wireless LAN Controller ハードウェア、およびアクセスポイントのインフラストラクチャもセットアップする必要があります。詳細については、コントローラのドキュメンテーションを参照してください。

ロケーション認識の設定タスク フロー

Cisco Unified Communications Manager でロケーション認識をセットアップするには、次のタスクを実行します。

始める前に

手順

	コマンドまたはアクション	目的
ステップ 1	ワイヤレスインフラストラクチャの同期のためのサービスの開始（805 ページ）	Cisco Unified Serviceability で、ロケーション認識機能をサポートするサービスを開始します。
ステップ 2	ワイヤレス アクセス ポイント コントローラの設定 （805 ページ）	データベースとワイヤレス アクセス ポイント コントローラを同期します。同期すると、無線インフラストラクチャがデータベースにインポートされます。 **ヒント** 自動更新の同期スケジュールをセットアップします。
ステップ 3	インフラストラクチャ デバイスの挿入（806 ページ）	（省略可）Cisco Prime Infrastructure の無線インフラストラクチャを追加するか、またはサードパーティのワイヤレス LAN コントローラを使用している場合は、一括管理を使用して、CSV ファイルでデータベースを更新します。

	コマンドまたはアクション	目的
		（注） このメソッドを使用して、自動更新をセットアップすることはできません。
ステップ 4	インフラストラクチャ デバイス トラッキングの非アクティブ化（808 ページ）	（省略可）同期内容に追跡を望まないアクセスポイントが含まれている場合（たとえば同期することでラボのアクセスポイントが制御される場合）は、アクセス ポイントを非アクティブにできるため、Cisco Unified Communications Manager がアクセス ポイントの更新を追跡することはありません。

ワイヤレスインフラストラクチャの同期のためのサービスの開始

場所認識機能をサポートするために、Cisco Wireless LAN コントローラとの同期をサポートするサービスを開始するには、次の手順を使用します。

手順

ステップ 1 Cisco Unified Serviceability にログインして、**[ツール（Tools）] > [サービスの開始（Service Activation）]** を選択します。

ステップ 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。

ステップ 3 次のサービスがオンになっていることを確認します。

- **Cisco CallManager**
- **Cisco AXL Web Service**
- **Cisco Wireless Controller Synchronization サービス**

ステップ 4 （省略可）一括管理を使用して CSV ファイルからネットワーク インフラストラクチャをインポートする場合、[一括プロビジョニング サービス（Bulk Provisioning Service）] がオンになっていることを確認します。

ステップ 5 [保存（Save）] をクリックします。

ワイヤレス アクセス ポイント コントローラの設定

次の手順を使用して、データベースを Cisco ワイヤレスアクセスポイントコントローラと同期します。同期プロセス中に、Unified Communications Manager は、そのコントローラが管理しているアクセスポイント インフラストラクチャでデータベースを更新します。最大で 50 のワイヤレスアクセスポイントコントローラを追加できます。

手順

ステップ 1 Cisco Unified CM Administration で、**[詳細機能（Advanced Features）] > [デバイスの位置のトラッキング サービス（Device Location Tracking Services）] > [ワイヤレス アクセスポイント]** を選択します。

ステップ 2 設定するコントローラを選択します。

- **[検索（Find）]**をクリックして、既存のコントローラを編集するコントローラを選択します。
- 新しいコントローラを設定するには、**[新規追加（Add New）]** をクリックします。

ステップ 3 **名前** フィールドに、コントローラの IP アドレスまたはホスト名を入力します。

ステップ 4 コントローラの**説明**を入力します。

ステップ 5 次の手順を実行して、コントローラーへの SNMP メッセージに使用される SNMP 設定を行います。

a) [SNMPバージョン（SNMP Version）] ドロップダウン リストから、コントローラで使用する SNMP バージョン プロトコルを選択します。
b) 残りのSNMP認証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。
c) [SNMP設定のテスト（Test SNMP Settings）] をクリックし、入力した SNMP 設定が有効であることを確認します。

ステップ 6 スケジュールされた同期を設定して、データベースを定期的に更新する場合は、次のようにします。

a) **[スケジュール同期を有効にしてインフラストラクチャ デバイスを検出する（Enable scheduled synchronization to discover Infrastructure Devices）]**をチェックします。
b) **[すべての再同期を実行してください]** フィールドで、同期スケジュールを作成します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 （任意） データベースをすぐに更新するには、**[同期 (Synchronize)]** をクリックします。

（**省略可**）同期によって、管理する必要のないアクセスポイント (たとえば、使用中でないラボ機器やアクセスポイント) がプルされた場合、そのアクセスポイントをトラッキングから削除できます。

インフラストラクチャ デバイスの挿入

次の手順を使用して、CSV ファイルから Unified Communications Manager データベースにワイヤレス アクセス ポイント インフラストラクチャを一括インポートします。この手順を使用して、Cisco Prime Infrastructure からエクスポートされた CSV ファイルをインポートしたり、またはサードパーティ ワイヤレス アクセス ポイント コントローラからアクセスポイントをインポートしたりできます。

始める前に

次に列挙する列を含む、カンマ区切り値（CSV）形式のデータ ファイルが必要です。

- アクセス ポイントまたはスイッチ名
- IPv4 アドレス
- IPv6 アドレス
- BSSID：ワイヤレス アクセス プロトコル（WAP）インフラストラクチャ デバイスの場合に必要
- 説明：場所識別子、スイッチ タイプと場所の組み合わせ、または他の意味のある識別子

（注） IPv4 アドレスと IPv6 アドレスの両方を定義することも、どちらか一方だけを定義することもできます。

（注） BSSID 値に関しては、アクセス ポイントを一意に識別する、0 で終わる BSSID マスクを入力します（アクセス ポイント上の個々のチャネルの BSSID とは異なります）。

手順

ステップ 1 **[一括管理（Bulk Administration）]**>**[インフラストラクチャ デバイス（Infrastructure Device）]**>**[インフラストラクチャ デバイスの挿入（Insert Infrastructure Device）]** の順に選択します。
[インフラストラクチャデバイス設定の挿入（Insert Infrastructure Device Configuration）] ウィンドウが表示されます。

ステップ 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 CSV データ ファイルを選択します。

ステップ 3 [ジョブ情報（Job Information）] 領域に、ジョブの説明を入力します。

デフォルトの説明は、[インフラストラクチャデバイスの挿入（Insert Infrastructure Device）] です。

ステップ 4 ジョブを実行するタイミングを次のように選択します。

- すぐにジョブを実行する場合は、**[今すぐ実行（Run Immediately）]** ラジオ ボタンを選択します。
- 後でジョブを実行する場合は、**[後で実行（Run Later）]** ラジオ ボタンを選択します。

ステップ 5 [送信（Submit）] をクリックします。
すぐにジョブを実行するように選択した場合は、ジョブが実行されます。

ステップ 6 後でジョブを実行するように選択した場合は、ジョブを実行するタイミングをスケジュールします。

a) **[一括管理（Bulk Administration）] > [ジョブスケジューラ（Job Scheduler）]** を選択します。
b) [検索（Find）] をクリックして、さきほど作成したジョブを選択します。
c) [ジョブスケジューラ（Job Scheduler）] ウィンドウで、ジョブを実行するタイミングをスケジュールします。
d) [保存（Save）] をクリックします。
スケジュールされた時刻に、ジョブが実行されます。

インフラストラクチャ デバイス トラッキングの非アクティブ化

同期に、トラッキングする必要のないアクセスポイントまたはスイッチが含まれている場合(たとえば、使用されていないラボ機器またはアクセスポイントで同期をプルする場合)は、アクセスポイントを非アクティブ化したり、追跡から切り替えたりすることができます。このアクセスポイントまたはスイッチのステータスは、Unified Communications Manager によって更新されません。

手順

ステップ 1 Cisco Unified CM Administration で、**[詳細機能（Advanced Features）] > [デバイスの位置のトラッキングサービス（Device Location Tracking Services）] > [スイッチとアクセスポイント（Switches and Access Points）]** を選択します。
ステップ 2 [検索（Find）] をクリックして、追跡を停止するスイッチまたはアクセス ポイントを選択します。
ステップ 3 [選択項目の非アクティブ化（Deactivate Selected）] をクリックします。

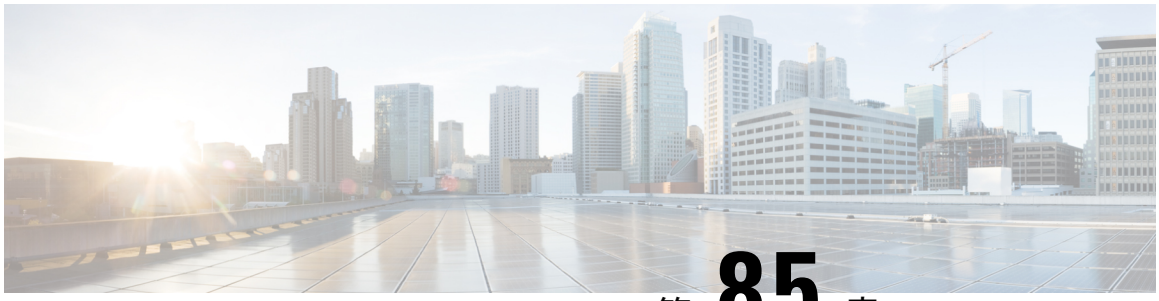
関連資料

システムの設定が完了し、システムが稼動している場合は、次の章のタスクを使用して、インフラストラクチャを継続的に管理することができます。

詳細については、『Administration Guide for Cisco Unified Communications Manager and IM and Presence Service』の「インフラストラクチャの管理」を参照してください。

場所の認識制限

機能	連携動作と制限事項
Meraki アクセスポイント	ロケーション認識機能は、Meraki アクセスポイントをサポートしていません。



第 85 章

自動代替ルーティングの設定

自動代替ルーティングの概要

場所の帯域幅不足のためシステムがコールをブロックする場合、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ように自動代替ルーティング(AAR)を設定します。自動代替ルーティングにより、発信者が電話を切ってから着信側をリダイヤルする必要がなくなります。

AAR 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
ステップ 1	クラスタ全体の自動代替ルーティングの有効化 （809 ページ）	クラスタの自動代替ルーティングを有効にします。
ステップ 2	AAR グループの設定 （810 ページ）	自動代替ルーティング（AAR）は、その場所の帯域幅が不十分であることが原因で Cisco Unified Communications Manager がコールをブロックした場合、代替番号を使用して PSTN またはその他のネットワークを通じてコールを再ルーティングするメカニズムを提供します。

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

ステップ 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。

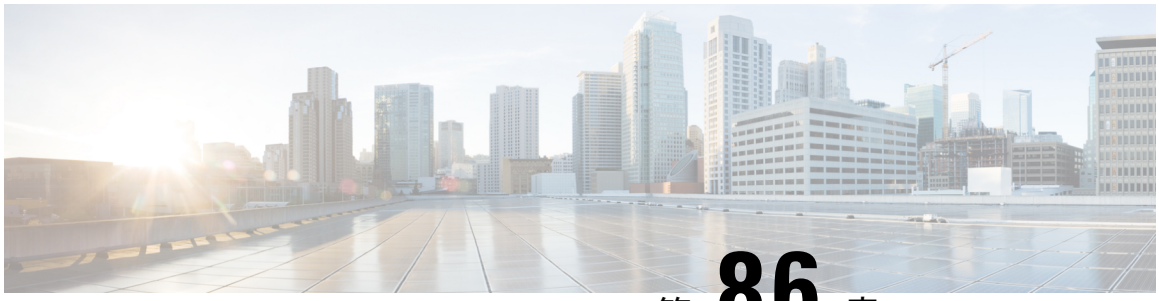
この名前には、最長 20 文字の英数字を指定でき、スペース、ピリオド（.）、ハイフン（-）、および下線文字（_）を任意に組み合わせることが可能です。

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。

ステップ 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。

ステップ 5 [保存（Save）] をクリックします。

（注） **（省略可）** 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 （190 ページ）」を参照してください。



第 86 章

AS-SIP エンドポイントの設定

AS-SIP の概要

Assured Services SIP（AS-SIP）エンドポイントは、MLPP、DSCP、TLS/SRTP、および IPv6 に準拠しています。AS-SIP は、Unified Communications Manager 上で複数のエンドポイント インターフェイスを実現します。

多くの Cisco IP 電話は、AS-SIP をサポートしています。加えて、サードパーティ製 AS-SIP エンドポイントデバイスタイプを使用すれば、サードパーティ製 AS-SIP 準拠のエンドポイントを設定して Cisco Unified Communications Manager で使用できるようになります。加えて、サードパーティ製 AS-SIP エンドポイントデバイスタイプを使用すれば、サードパーティ製 AS-SIP 準拠の汎用エンドポイントを設定して Cisco Unified Communications Manager で使用できるようになります。

AS-SIP の機能

AS SIP エンドポイントに対しては、次の機能が実装されているか使用可能になっています。

- MLPP
- TLS
- SRTP
- 優先レベルの DSCP
- エラー応答
- V.150.1 MER
- 会議ファクトリ フローのサポート
- AS-SIP 回線早期オファー

サードパーティ AS-SIP 電話

サードパーティの電話機は、サードパーティー製 AS-SIP エンドポイントデバイスタイプを使用して、Cisoc Unified Communications Manager でプロビジョニングすることができます。

AS-SIP を実行しているサードパーティ製電話機は、Cisco Unified Communications Manager TFTP サーバを使用して設定されません。お客様が、ネイティブ電話機設定メカニズム（通常は、ウェブ ページまたは tftp ファイル）を使用して、電話機を設定する必要があります。お客様は、Cisco Unified Communications Manager データベース内のデバイスおよび回線の設定と、ネイティブ電話機設定の同期を保つ必要があります（たとえば、電話機の内線番号 1002 と Cisco Unified Communications Manager の 1002）。また、回線のディレクトリ番号が変更された場合、Unified CM Administration とネイティブの電話機設定メカニズムの両方で、そのディレクトリ番号が変更されていることを確認する必要があります。

サードパーティの電話機の識別

SIP を実行しているサードパーティ製の電話機は MAC アドレスを送信しないため、ユーザ名を使用して自分自身の身元を証明する必要があります。REGISTER メッセージには次のヘッダーが含まれています。

```
Authorization: Digest
username="swhite",realm="ccmsipline",nonce="GBauADss2qoWr6k9y3hGGVDAqnLfoLk5",uri
="sip:172.18.197.224",
algorithm=MD5,response="126c0643a4923359ab59d4f53494552e"
```

ユーザ名 **swhite** は、Cisco Unified Communications Manager の **[エンドユーザの設定(End User Configuration)]** ウィンドウで設定されたユーザと一致する必要があります。管理者は、**[電話の設定(Phone Configuration)]** ウィンドウの **[ダイジェストユーザ(Digest User)]** フィールド内のユーザ（**swhite など**）を使用してサードパーティ製 SIP 電話機を設定します。

（注） 各ユーザ ID は、1 つのサードパーティの電話機にのみ割り当てることができます。同じユーザ ID がダイジェスト ユーザとして複数の電話機に割り当てられている場合、そのエンドユーザ ID が割り当てられているサードパーティ製電話機は正しく登録されません。

サードパーティ AS-SIP 電話および Cisco IP 電話の設定

下の表は、Cisco Unified IP Phone と AS-SIP を実行しているサードパーティ製電話機の設定上の違いを比較したものです。

表 *95 : Cisco IP* 電話とサードパーティ製電話機の設定の違いの比較

AS-SIP を実行している電話機	中央集中型 TFTP との統合	MAC アドレスの送信	ソフトキー ファイルのダウンロード	ダイヤル プラン ファイルのダウンロード	Unified Communications Manager のフェールオーバーとフォールバックのサポート	リセットと再起動のサポート
Cisco IP Phone	はい	はい	はい	はい	はい	はい
サードパーティ製 AS-SIP デバイス	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

（注） すべての Cisco IP 電話が AS-SIP をサポートしているわけではありません。サポート情報については、ご使用の電話機モデルの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 を使用して、SIP を実行するサードパーティの電話機を設定します（「SIP プロファイルの設定 （437 ページ）」を参照してください）。管理者は、SIP を実行するサードパーティの電話機で設定手順を実行する必要があります。次の例を参照してください。

- 電話機のプロキシ アドレスが、Cisco Unified Communications Manager の IP または完全修飾ドメイン名（FQDN）であることを確認します。
- 電話機のディレクトリ番号が、Cisco Unified CM Administration でデバイスに対して設定したディレクトリ番号と一致していることを確認します。
- 電話機のダイジェスト ユーザ ID（承認 ID とも言います）が、Cisco Unified CM Administration で設定したダイジェスト ユーザ ID と一致していることを確認します。

詳細については、サードパーティの電話機に付属するドキュメントを参照してください。

AS-SIP 会議

機能の呼び出し元（保留元、転送元、または会議開催者）でシスコ独自の機能シグナリングがサポートされている場合は、MOH がそのターゲット（保留先、転送直前の転送先、または参加直前の会議出席者）に適用されます。機能の呼び出し元でシスコ独自の機能シグナリングがサポートされていない場合は、MOH がそのターゲットに適用されません。また、エンドポイントが会議ミキサーであることを明示的に伝達する場合は、MOH がそのターゲットで再生されません。AS-SIP 会議には次の 2 つの形態があります。

- ローカル混合
- 会議ファクトリ

ローカル混合

Unified CM からは、会議開催者が他の会議参加者のそれぞれに対してアクティブ コールを同時に確立したようにしか見えません。会議はイニシエータによってホストされ、そこで音声が混合されます。会議開催者からのコールには MOH ソースへの接続を拒否する特殊なシグナリングが含まれています。

会議ファクトリ

会議イニシエータは SIP トランクの外側に設置された会議ファクトリサーバを呼び出します。そして、IVR シグナリングを通して、会議ブリッジを予約するように会議ファクトリに指示します。会議ファクトリから会議イニシエータに数値アドレス（ルーティング可能な DN）が返され、会議開催者はブリッジとの登録を確立して、参加者を追跡するための会議リスト情報を受け取ります。会議ファクトリにより、MOH ソースへの接続を拒否する特殊なシグナリングが送信されます。

AS-SIP の要件

十分なデバイス ライセンス ユニットが使用可能かどうかを調べます。詳細は、スマート ソフトウェア ライセンシング （7 ページ） をご覧ください。

AS-SIP エンドポイントの設定タスク フロー

次のタスクを完了して、AS-SIP エンドポイントを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	ダイジェストユーザの設定 （815 ページ）	SIP リクエストにダイジェスト認証を使用するようにエンドユーザを設定します。
ステップ 2	SIP 電話のセキュア ポートの設定 （436 ページ）	Cisco Unified Communications Manager はこのポートを使用して SIP 回線の登録用の SIP 電話を TLS を介してリッスンします。
ステップ 3	サービスの再起動 （437 ページ）	セキュアポートを設定した後、Cisco CallManager サービスと Cisco CTL Provider サービスを再起動します。

	コマンドまたはアクション	目的
ステップ 4	AS-SIP 用 SIP プロファイルの設定 （817 ページ）	AS-SIP エンドポイントと SIP トランクの SIP 設定を SIP プロファイルで設定します。 （注） 電話機固有のパラメータはサードパーティ製 AS-SIP 電話機にダウンロードされません。Cisco Unified Communications Manager でのみ使用されます。サードパーティ製電話機では同じ設定値をローカルに設定する必要があります。
ステップ 5	AS-SIP 用電話セキュリティプロファイルの設定 （818 ページ）	電話セキュリティプロファイルを使用して、TLS、SRTP、ダイジェスト認証などのセキュリティ設定を割り当てることができます。
ステップ 6	AS-SIP エンドポイントの設定 （819 ページ）	Cisco IP 電話またはサードパーティエンドポイントを AS-SIP サポートとともに設定します。
ステップ 7	エンド ユーザとデバイスの関連付け （820 ページ）	エンドポイントをユーザに関連付けます。
ステップ 8	AS-SIP 用 SIP トランク セキュリティ プロファイルの設定 （821 ページ）	トランクセキュリティプロファイルを使用して、TLS 認証やダイジェスト認証などのセキュリティ機能を SIP トランクに割り当てることができます。
ステップ 9	AS-SIP 用 SIP トランクの設定 （821 ページ）	SIP トランクを AS-SIP サポートで設定します。
ステップ 10	AS-SIP 機能の設定 （822 ページ）	MLPP、TLS、V.150、IPv6 などの追加の SIP 機能を設定します。

ダイジェストユーザの設定

ダイジェスト認証を使用するダイジェスト ユーザとしてエンド ユーザを設定するには、この手順を使用します。ユーザに関連付けられているデバイスは、ユーザのダイジェスト クレデンシャルを使用して認証されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）] > [エンドユーザ（End User）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいユーザを作成するには、[新規追加（Add New）] をクリックします。
- 既存のユーザを選択するには、[検索（Find）] をクリックします。

ステップ 3 次の必須フィールドが入力されていることを確認してください。

- [ユーザID（User ID）]
- [姓（Last Name）]

ステップ 4 [ダイジェスト認証（Digest Credentials）] フィールドにパスワードを入力します。エンド ユーザは、エンドポイントを使用する際に、このパスワードを使用して認証する必要があります。

ステップ 5 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。

ステップ 6 [保存（Save）] をクリックします。

SIP 電話のセキュア ポートの設定

ポートを設定するには、次の手順に従います。Cisco Unified Communications Manager はこのポートを使用して SIP 回線の登録用の SIP 電話を TLS を介してリッスンします。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [Cisco Unified CM（Cisco Unified CM）]** を選択します。

ステップ 2 [このサーバのCisco Unified Communications Manager TCPポート設定（Cisco Unified Communications Manager TCP Port Settings for this Server）] で、[SIP電話セキュアポート（SIP Phone Secure Port）] フィールドにポート番号を指定するか、またはデフォルト値をそのまま使用します。デフォルト値は5061です。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 [OK] をクリックします。

サービスの再起動

Cisco CallManager サービスと Cisco CTL Provider サービスを再起動するには、次の手順を実行します。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 5 手順 3 と手順 4 を繰り返して、Cisco CTL Provider サービスを再起動します。

AS-SIP 用 SIP プロファイルの設定

AS-SIP エンドポイントと SIP トランクの SIP プロファイルを、SIP 設定を使用して設定するには、次の手順を使用します。

手順

ステップ 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。

ステップ 2 次のいずれかを実行します。

- 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。
- **[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。

ステップ 3 SIP プロファイルの [名前（Name）] と [説明（Description）] を入力します。

ステップ 4 [Assured Services SIPとの適合（Assured Services SIP conformance）] チェックボックスをオンにします。

（注） このチェックボックスは、SIP トランクおよびサードパーティ AS-SIP 電話に対してオンにする必要があります。これは、AS-SIP をサポートしている Cisco IP 電話では必須ではありません。

ステップ 5 [電話で使用されるパラメータ（Parameters used in Phone）] セクションで、作成する予定のコール タイプ向けに DSCP 優先度の値を設定します。

（注） クラスタ全体のサービスパラメータを使用して DSCP 値を設定することもできます。ただし、SIP プロファイルで設定した DSCP 値は、その SIP プロファイルを使用するすべてのデバイスで、クラスタ全体の設定よりも優先されます。

ステップ 6 [音声コールおよびビデオコールのアーリー オファー サポート（Early Offer support for voice and video calls）] ドロップダウン リストで、次のいずれかのオプションを選択し、このプロファイルを使用する SIP トランク向けのアーリー オファー サポートを設定します。

- [無効（Disabled）]
- [ベストエフォート（MTP挿入なし）（Best Effort (no MTP inserted)）]
- [必須（必要に応じてMTPを挿入）（Mandatory (insert MTP if needed)）]

ステップ 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。

ステップ 8 [保存（Save）] をクリックします。

AS-SIP 用電話セキュリティプロファイルの設定

AS-SIP エンドポイント用の電話セキュリティプロファイルを設定するには、次の手順を使用します。このセキュリティプロファイルを使用して、TLS や SRTP などのセキュリティ設定を割り当てることができます。

手順

ステップ 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。

ステップ 2 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして、新しい電話セキュリティ プロファイルを作成します。
- **[検索（Find）]** をクリックし、既存のプロファイルを編集します。

ステップ 3 新しいプロファイルの場合、**[電話機のセキュリティプロファイル]** ドロップダウンからオプションを選択し、**[サードパーティー製 AS-SIP エンドポイント]** を選択して、**[次へ]** をクリックします。

- Cisco IP 電話の場合は、電話機のモデルを選択して、**[次へ (Next)]** をクリックします。
- サードパーティ製 AS-SIP エンドポイント の場合は、**[サードパーティ製 AS-SIP エンドポイント]** を選択し、**[次へ (Next)]** をクリックします。

ステップ 4 プロトコルには、**[SIP]**を選択し、**[次へ (Next)]** をクリックします。

ステップ 5 プロトコルの **[名前（Name）]** と **[説明（Description）]** を入力します。

ステップ 6 次のいずれかの設定に**デバイスセキュリティモード**を割り当てます。

- **[認証（Authenticated）]**：Cisco Unified Communications Manager は TLS シグナリングを使用して、電話機に整合性および認証を提供します。
- **[暗号化]**：Cisco Unified Communications Manager は TLS シグナリングを使用して、電話機に整合性および認証を提供します。また、SRTP はメディア ストリームも暗号化します。

ステップ 7 [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。

ステップ 8 **[電話のセキュリティプロファイルの設定]** 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。

ステップ 9 [保存（Save）] をクリックします。

AS-SIP エンドポイントの設定

次の手順を使用して、AS-SIP エンドポイントを設定します。多くの Cisco IP 電話は、AS-SIP をサポートしています。さらに、サードパーティエンドポイントの AS-SIP を設定することもできます。

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウン リストから、AS-SIP をサポートする Cisco IP Phone を選択します。それ以外の場合は、[サードパーティ AS-SIP エンドポイント（Third-Party AS-SIP Endpoint）] を選択します。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 次の必須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。

- [デバイス信頼モード（Device Trust Mode）]：サードパーティ AS-SIP エンドポイントでのみ使用します。[信頼済み（Trusted）] または [信頼されていない（Not Trusted）] を選択します。
- [MAC アドレス（MAC Address）]
- 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）]：AS-SIP 用にセットアップした電話のセキュリティ プロファイルを選択します。

- [SIPプロファイル（SIP Profile）]：設定した AS-SIP 対応の SIP プロファイルを選択します。
- [ダイジェストユーザ（Digest User）]：ダイジェストユーザとして設定するユーザ ID を選択します。このユーザはダイジェスト認証が有効化されている必要があります。
- [DTMF受信が必要（Require DTMF Reception）]：エンドポイントで DTMF 番号を受け付けられるようにするには、このチェックボックスをオンにします。
- [音声コールとビデオコールに対するアーリーオファーサポート（Early Offer support for voice and video calls）]：このチェックボックスをオンにすると、アーリー オファー サービス サポートが有効になります。このフィールドは、サードパーティの電話機でのみ表示されます。

ステップ 6 [MLPPおよび機密アクセスレベル情報（MLPP and Confidential Access Level Information）] セクションのフィールドを設定します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 ディレクトリ番号を追加します。

a) 左のナビゲーション バーで、[新規DNを追加（Add a New DN）] をクリックします。[ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウが開きます。
b) **ディレクトリ番号**を追加します。
c) [ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウで、残りのフィールドを入力します。
d) [保存（Save）] をクリックします。

ステップ 9 [関連リンク（Related Links）] から、[デバイスの設定（Configure Device）] を選択し、[移動（Go）] をクリックします。

ステップ 10 **[設定の適用（Apply Config）]** をクリックします。

エンド ユーザとデバイスの関連付け

エンドユーザを AS-SIP エンドポイントに関連付けるには、次の手順を使用します。

手順

ステップ 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）]** > **[エンドユーザ（End User）]**。

ステップ 2 [検索（Find）] をクリックして、デバイスに関連付けるユーザを選択します。

ステップ 3 **[デバイス情報（Device Information）]** セクションで、**[デバイスの関連付け（Device Association）]** を選択します。
[ユーザデバイス割り当て（User Device Association）] ウィンドウが表示されます。

ステップ 4 [検索（Find）] をクリックすると、使用可能なデバイスのリストが表示されます。

ステップ 5 関連付けるデバイスを選択して、[選択/変更の保存（Save Selected/Changes）] をクリックします。

ステップ 6 [関連リンク（Related Links）] から、[ユーザの設定に戻る（Back to User）] を選択し、[移動（Go）] をクリックします。
[エンドユーザの設定（End User Configuration）] ウィンドウが表示され、選択し、割り当てたデバイスが、[制御するデバイス（Controlled Devices）] ペインに表示されます。

AS-SIP 用 SIP トランク セキュリティ プロファイルの設定

AS-SIP をサポートする SIP トランク用のセキュリティ プロファイルを設定するには、この手順を使用します。

手順

ステップ 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。
ステップ 2 [新規追加（Add New）] をクリックします。
ステップ 3 セキュリティ プロファイルの [名前（Name）] を入力します。
ステップ 4 [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）] または [認証済み（Authenticated）] を選択します。
ステップ 5 [着信転送タイプ（Incoming Transport Type）] フィールドと [発信転送タイプ（Outgoing Transport Type）] フィールドが、自動的に [TLS] に変更されます。
ステップ 6 [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。
ステップ 7 V.150 を導入する場合は、[SIP V.150アウトバウンドSDPオファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）] ドロップダウン リストの値を設定します。
ステップ 8 [SIP トランクのセキュリティプロファイルの設定] 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。
ステップ 9 [保存（Save）] をクリックします。

AS-SIP 用 SIP トランクの設定

AS-SIP をサポートする SIP トランクを設定するには、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [トランク（Trunk）]** を選択します。
ステップ 2 次のいずれかを実行します。

- 既存のトランクを選択するには、[検索（Find）] をクリックします。

- **[新規追加（Add New）]** をクリックし、新規トランクを作成します。

ステップ 3 新しいトランクについては、[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。

ステップ 4 [トランクサービスタイプ（Trunk Service Type）] ドロップダウン リストで、[なし（None）]（デフォルト）を選択し、[次へ（Next）] をクリックします。

ステップ 5 トランクの**デバイス名**を入力します。

ステップ 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。

ステップ 7 **[宛先アドレス]** フィールドに、トランクを接続するサーバのアドレスを入力します。

ステップ 8 [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、AS-SIP 用に作成したプロファイルを選択します。

ステップ 9 **[SIP プロファイル（SIP Profile）]** ドロップダウン リストから、AS-SIP 用に設定した SIP プロファイルを選択します。

ステップ 10 **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。

ステップ 11 [保存（Save）] をクリックします。

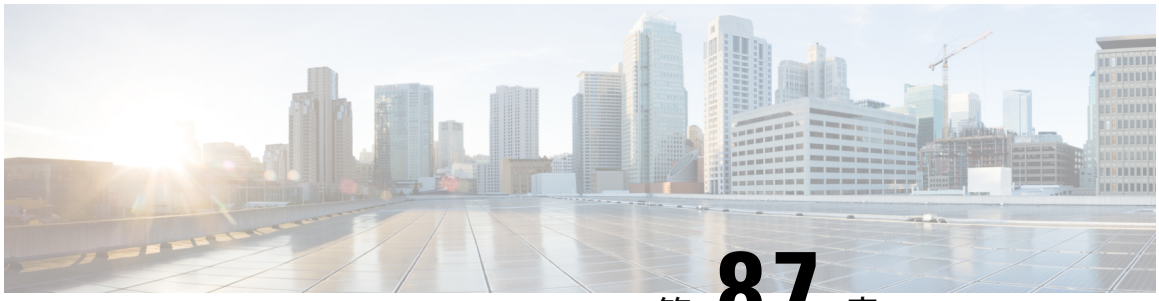
AS-SIP 機能の設定

前述のタスク フローの手順では、エンドポイントとトランクの AS-SIP サポートを設定する方法について説明しています。次の表に、導入可能な AS-SIP の各機能の概要と、それぞれの構成参照を示します。

AS-SIP 機能	[設定の説明（Configuration Description）]
早期オファー	SIP 早期提供では、エンドポイントが INVITE 要求および 200OK 応答の間にメディアをネゴシエートできます。早期提供には次の 2 つのモードがあります。 • ベストエフォート早期提供（MTP 挿入なし） • 必須早期提供 (必要に応じて MTP を挿入) 次の設定ウィンドウのフィールドを使用して、早期サービスサポートを設定します。詳細な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。 **SIP プロファイル設定** ウィンドウ • 音声とビデオコールの早期提供サポート: SIP トランクでの早期提供サポートを有効にするため、このフィールドを設定します。 • アーリーオファーおよび再招待の SDP セッション レベル帯域幅修飾子 • [通話中 INVITE での送受信 SDP の送信（Send send-receive SDP in mid-call INVITE）] **[電話の設定]** ウィンドウ (サードパーティ製 AS-SIP エンドポイントデバイスタイプが使用されている場合のみ) • 音声とビデオ通話の早期提供サポート: このチェックボックスをオンにすると、早期サービスサポートが有効になります。

AS-SIP 機能	[設定の説明（Configuration Description）]
会議ファクトリ	IMS クライアントが会議を設定するために使用する URI を指定します。 1. Cisco Unified CM Administration から、**[システム（System）]>[サービスパラメータ（Service Parameters）]** を選択します。 2. [サーバ（Server）] ドロップダウン リストから、ご使用の Cisco Unified Communications Manager サーバを選択します。 3. [サービス（Service）] から、**Cisco CallManager** を選択します。 4. [クラスタ全体のパラメータ（機能 - 会議）（Clusterwide Paramters (Feature - Conference)）] で、**IMS 会議ファクトリ URI** を割り当てます。 5. [保存（Save）] をクリックします。
DSCP マーキング	DSCP 設定を使用すると、ネットワーク内の QoS と帯域幅を管理できます。DSCP 設定を使用して、優先順位付けされたトラフィッククラスラベルをコールごとのコールに割り当てます。 サービス パラメータを使用して、クラスタ全体の DSCP 設定を指定できます。また、SIP プロファイルを使用して、そのプロファイルを使用するユーザに対してカスタマイズされた QoS ポリシーを割り当てることができます。たとえば、エグゼクティブ（CEO など）や営業チームのコールに高い優先順位を割り当て、ネットワーク帯域幅の問題が発生した場合にそれらのコールが切断されないようにすることができます。 DSCP の設定については、「DSCP 設定の設定タスク フロー（637 ページ）」を参照してください。
IPv6	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することで、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することができます。 IPv6 の設定については、次の項目を参照してください。 IPv6 の設定タスク フロー （108 ページ）

AS-SIP 機能	[設定の説明（Configuration Description）]
Multilevel Precedence and Preemption（MLPP）	Multilevel Precedence and Preemption（MLPP）サービスを使用すると、優先コールをかけることができます。この機能により、国家の非常事態やネットワークの機能低下など、ネットワークに負荷がかかっている場合に、優先順位の高いユーザが重要な組織や担当者への通信を確実に行うことができます。 MLPP の設定については、「Multilevel Precedence and Preemption Precendence のタスク フロー（828 ページ）」を参照してください。
Secure Real-Time Transport Protocol（SRTP）	Secure Real-time Transport Protocol (SRTP) を使用すると、コール内のメディアストリームに暗号化と認証を提供できます。 SRTP は、電話機が使用する**電話機のセキュリティプロファイル設定**内の電話機用に設定できます。**[デバイスセキュリティモード(Device Security Mode)]**フィールドを **[暗号化済]** に設定する必要があります。
トランスポート層のシグナリング (TLS)	Transport Layer Security（TLS）はセキュアポートと証明書交換を使用して、2 つのシステム間またはデバイス間でセキュアで信頼できるシグナリングやデータ転送を実現します。 TLS を設定するには、『*Cisco Unified Communications Manager* セキュリティ ガイド』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）の「TLS の設定」の章を参照してください。
V.150	「V. 150 最低必須要件」機能を使用すると、IP ネットワーク経由のモデムで安全なコールを行うことができます。この機能では、ダイヤルアップモデムを使用して、従来の公衆交換電話網 (PSTN) 上で動作するモデムとテレフォニーデバイスを大規模に設置します。 V.150 を設定するには、『*Cisco Unified Communications Manager* セキュリティ ガイド』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）の「Cisco V.150 Minimum Essential Requirements（MER）」の章を参照してください。



第 87 章

Multilevel Precedence and Preemption の設定

マルチレベルの優先およびプリエンプションの概要

Multilevel Precedence and Preemption（MLPP）サービスを使用すると、優先コールをかけることができます。適切に検証されたユーザは、優先順位の低いコールよりも優先順位の高いコールを優先させることができます。認証されたユーザは、宛先ステーションへ、または完全にサブスクライブされた TDM トランクを介して、コールをプリエンプション処理することができます。この機能により、国家の非常事態やネットワークの機能低下など、ネットワークに負荷がかかっている場合に、優先順位の高いユーザが重要な組織や担当者への通信を確実に行うことができます。

Multilevel Precedence and Preemption の前提条件

サポートされる SCCP 電話または SIP 電話。機能サポートと詳細情報については、ご使用の電話機の『*Cisco IP Phone* アドミニストレーション ガイド』および『*Cisco IP Phone* ユーザ ガイド』を参照してください。

Multilevel Precedence and Preemption Precedence のタスク フロー

始める前に

手順

	コマンドまたはアクション	目的
ステップ 1	ドメインおよびドメインリストの設定（830ページ）を行うには、次のサブタスクを実行します。 • Multilevel Precedence and Preemption ドメインの設定 （831 ページ） • リソース プライオリティ ネームスペース ネットワーク ドメインの設定 （832 ページ） • リソース プライオリティ ネームスペース ネットワーク ドメイン リストの設定 （832 ページ）	MLPP サブスクライバに関連付けられるリソースのデバイスを指定するには、MLPP ドメインを設定します。
ステップ 2	共通デバイス設定での Multilevel Precedence and Preemption 設定 （833 ページ）	一般的なデバイス設定には、複数のユーザとそのデバイスに適用できる MLPP 関連の情報が含まれています。各デバイスは一般的なデバイス設定に関連付けられていることを確認します。これらの設定は、エンタープライズパラメータの設定を上書きします。
ステップ 3	Multilevel Precedence and Preemption のエンタープライズ パラメータの設定（833 ページ）	MLPP の通知とプリエンプションを有効にするには、エンタープライズパラメータを設定します。個々のデバイスや一般的なデバイス設定のデバイスがデフォルトの MLPP 設定になっていると、MLLP 関連のエンタープライズ パラメータは、これらのデバイス、および一般的なデバイス設定に適用されます。
ステップ 4	Multilevel Precedence and Preemption のパーティションの設定 （835 ページ）	パーティションを設定して、電話番号（DN）の論理グループと、到達可能性の特徴が類似したルート パターンを作成します。パーティションに通常、配

	コマンドまたはアクション	目的
		置されるデバイスは、DNs とルート パターンを含みます。これらのエンティティは、ユーザがダイヤルする DNs に関連付けられます。わかりやすくするために、パーティション名は通常、その特性を反映しています。
ステップ 5	Multilevel Precedence and Preemption のコーリング サーチ スペースの設定（837 ページ）	コーリング サーチ スペースは、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 スペースは、IP 電話、ソフトフォン、ゲートウェイなどのコーリングデバイスがコールを完了しようとしたときに検索できるパーティションを決めます。
ステップ 6	Multilevel Precedence and Preemption（MLPP）のルート パターンの設定（837 ページ）	内部および外部コールの両方をルーティングまたはブロックするためにルート パターンを設定します。
ステップ 7	Multilevel Precedence and Preemption のトランスレーション パターンの設定（839 ページ）	コールされてからコールをルーティングされる方法を指定するには、トランスレーションパターンを設定します。トランスレーションパターンを設定すると、システムで必要に応じて発信と発信された数字を処理できます。パターン一致が発生していることを確認すると、システムは後続の一致を実行するためにトランスレーションパターン用に設定されたコーリングサーチスペースを使用します。
ステップ 8	ゲートウェイの Multilevel Precedence and Preemption の設定 （840 ページ）	非 IP 通信デバイスと通信するように Cisco Unified Communications Manager を設定します。
ステップ 9	電話機の Multilevel Precedence and Preemption の設定 （841 ページ）	
ステップ 10	Multilevel Precedence and Preemption コールの電話番号の設定 （844 ページ）	デバイスを設定した後、更新された [デバイス設定（Device Configuration）] ウィンドウから回線（ディレクトリ番号）を追加できます。
ステップ 11	Multilevel Precedence and Preemption のユーザ デバイス プロファイルの設定（844 ページ）	ユーザ プロファイルが電話機に割り当てられると、その電話は、ユーザに関連付けられている CSS を含む割り当て

	コマンドまたはアクション	目的
		られたユーザの設定を継承します。しかし、電話のCSSは、ユーザプロファイルを上書きします。パターン一致が発生すると、Cisco Unified Communications Managerは、そのコールへのダイヤルパターンに関連付けられる優先度レベルを割り当てます。システムは、割り当てられた優先度レベルで優先度の高いコールとしてコール要求を設定します。
ステップ 12	Multilevel Precedence and Preemption のデフォルトのデバイスプロファイルの設定 （846 ページ）	ユーザがユーザデバイスプロファイルがない電話機モデルにログインするたびに、デフォルト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は、特定のデバイスに関連付けられている機能とサービスで構成されています。

ドメインおよびドメインリストの設定

MLPP サブスクライバに関連付けられるリソースのデバイスを指定するには、MLPP ドメインを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Multilevel Precedence and Preemption ドメインの設定 （831 ページ）	デバイスとリソースを MLPP サブスクライバーに関連付けます。特定のドメインに属している MLPP サブスクライバが、同じドメインに属している別の MLPP サブスクライバに優先度の高いコールを発信する場合、MLPPサービスでは、着信側 MLPP サブスクライバが対応中の既存のコールを優先度の高いコールにプリエンプション処理できます。MLPPサービスの可用性は、単一のドメインに制限されます。 発信ユーザによる MLPP ドメインへの加入によって、コールのドメインとその接続が決まります。あるドメイン内の優先レベルの高いコールだけが、同じドメ

	コマンドまたはアクション	目的
		イン内のコールが使用している接続を差し替えることができます。
ステップ 2	リソース プライオリティ ネームスペース ネットワーク ドメインの設定 （832 ページ）	SIP トランクを使用する Voice over Secured IP（VoSIP）ネットワーク向けの名前空間ドメインを設定します。お使いのシステムが SIP シグナル化されたリソースに優先順位を付けることによって、電話回線、IP 帯域幅、およびゲートウェイに緊急事態や輻輳が発生した場合にこれらのリソースが最も効率的に利用されます。エンドポイントは、優先順位およびプリエンプション情報を受信します。
ステップ 3	リソース プライオリティ ネームスペース ネットワーク ドメイン リストの設定（832 ページ）	許容可能なネットワークドメインの一覧を設定します。許容可能なネットワークドメインがこのリストに含まれている場合、着信コールはこのリストと比較された上で処理されます。

Multilevel Precedence and Preemption ドメインの設定

デバイスとリソースを MLPP サブスクライバーに関連付けます。特定のドメインに属している MLPP サブスクライバが、同じドメインに属している別の MLPP サブスクライバに優先度の高いコールを発信する場合、MLPP サービスでは、着信側 MLPP サブスクライバが対応中の既存のコールを優先度の高いコールにプリエンプション処理できます。MLPP サービスの可用性は、単一のドメインに制限されます。

発信ユーザによる MLPP ドメインへの加入によって、コールのドメインとその接続が決まります。あるドメイン内の優先レベルの高いコールだけが、同じドメイン内のコールが使用している接続を差し替えることができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [MLPP] > [ドメイン（Domain）] > [MLPP ドメイン（MLPP Domain）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [ドメイン名（Domain Name）] フィールドに、新しい MLPP ドメインに割り当てる名前を入力します。

最長 50 文字の英数字を入力でき、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。

ステップ 4 [ドメイン ID（Domain ID）] フィールドに、MLPP ドメイン ID として一意の 6 文字の 16 進数を入力します。

ドメイン ID は 000001 と FFFFFF の範囲で指定する必要があります。（000000 は、デフォルトの MLPP ドメイン ID に予約されています）

ステップ 5 [保存（Save）] をクリックします。

リソース プライオリティ ネームスペース ネットワーク ドメインの設定

SIP トランクを使用する Voice over Secured IP（VoSIP）ネットワーク向けの名前空間ドメインを設定します。お使いのシステムが SIP シグナル化されたリソースに優先順位を付けることによって、電話回線、IP 帯域幅、およびゲートウェイに緊急事態や輻輳が発生した場合にこれらのリソースが最も効率的に利用されます。エンドポイントは、優先順位およびプリエンプション情報を受信します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [MLPP（MLPP）] > [ネームスペース（Namespace）] > [リソースプライオリティネームスペースネットワークドメイン（Resource Priority Namespace Network Domain）]** を選択します。

ステップ 2 [情報（Information）] セクションで [リソース プライオリティ ネームスペース ネットワーク ドメイン（Resource Priority Namespace Network Domain）] の名前を入力します。ドメイン名の最大文字数は 100 です。

ステップ 3 ドメイン名の説明を入力します。

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（&）、山カッコ（<>）は使用できません。

ステップ 4 ドメイン名をデフォルトにする場合は、[このリソース プライオリティ ネームスペース ネットワーク ドメインをデフォルトにする（Make this the Default Resource Priority Namespace Network Domain）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

リソース プライオリティ ネームスペース ネットワーク ドメイン リストの設定

許容可能なネットワークドメインの一覧を設定します。許容可能なネットワーク ドメインがこのリストに含まれている場合、着信コールはこのリストと比較された上で処理されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[MLPP]** > **[ネームスペース（Namespace）]** > **[リソースプライオリティネームスペースリスト（Resource Priority Namespace List）]** を選択します。

ステップ 2 リソース優先度名前空間リストの名前を入力します。最大文字数は 50 です。

ステップ 3 リストの説明を入力します。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。

ステップ 4 上矢印および下矢印を使用して、リソース優先順位のネットワークドメインを **[選択したリソースの優先名前空間]** フィールドに移動します。

ステップ 5 [保存（Save）] をクリックします。

共通デバイス設定での Multilevel Precedence and Preemption 設定

一般的なデバイス設定には、複数のユーザとそのデバイスに適用できる MLPP 関連の情報が含まれています。各デバイスは一般的なデバイス設定に関連付けられていることを確認します。これらの設定は、エンタープライズ パラメータの設定を上書きします。

手順

ステップ 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）]** > **[共通デバイス設定（Common Device Configuration）]** を選択します。

ステップ 2 次のいずれかの操作を実行します。

- 既存の共通デバイス設定を変更するには、[検索（Find）] をクリックし、検索結果のリストから共通デバイス設定を選択します。
- 新しい共通デバイス設定を追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [共通デバイス設定（Common Device 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。

ステップ 4 [保存（Save）] をクリックします。

Multilevel Precedence and Preemption のエンタープライズ パラメータの設定

MLPP の通知とプリエンプションを有効にするには、エンタープライズ パラメータを設定します。個々のデバイスや一般的なデバイス設定のデバイスがデフォルトの MLPP 設定になってい

ると、MLLP 関連のエンタープライズパラメータは、これらのデバイス、および一般的なデバイス設定に適用されます。

手順

ステップ 1 **[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。

ステップ 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 MLPP エンタープライズパラメータを設定します。パラメータとその設定オプションの詳細については、「関連項目」セクションを参照してください。

ステップ 3 [保存（Save）] をクリックします。

Multilevel Precedence and Preemption のエンタープライズ パラメータ

表 96 : Multilevel Precedence and Preemption のエンタープライズ パラメータ

パラメータ	説明
MLPP Domain Identifier	このパラメータは、ドメインを定義するために設定します。MLPP サービスはドメインに適用されるため、Cisco Unified Communications Manager は、指定されたドメイン内の MLPP ユーザからのコールに属す接続とリソースだけに優先レベルのマークを付けます。Cisco Unified Communications Manager は、同じドメイン内の MLPP ユーザからの優先順位の低いコールだけを差し替えることができます。 デフォルトは **000000** です。
MLPP 表示ステータス（MLPP Indication Status）	このパラメータは、デバイスが MLPP 優先コールを示すために MLPP トーンと特別な表示を使用するかどうかを指定します。エンタープライズで MLPP 通知を有効にするには、このパラメータを [MLPP Indication turned on] に設定します。 デフォルトは **メール通知サーバオフ**。
MLPP Preemption Setting	このパラメータは、優先度の高いコールに対応するため、デバイスが（プリエンプショントーンなどの）プリエンプションやプリエンプション シグナリングを適用する必要があるかどうかを決定します。企業全体で MLPP プリエンプションを有効にするには、このパラメータを [強制プリエンプション（Forceful Preemption）] に設定します。 デフォルトは **No preemption allowed**です。

パラメータ	説明
Precedence Alternate Party Timeout	優先コールでは、着信側が別の相手への転送を登録している場合、このタイマーは、着信側がプリエンプションを承認しないまたは優先コールに応答しなかった場合に、Cisco Unified Communications Manager がコールを別の相手に転送するまでの秒数を示します。 デフォルトは **30** 秒です。
Standard VM Handling For Precedence コールの使用	このパラメータは、優先コールがボイスメール システムに自動転送されるかどうかを指定します。 このパラメータが False に設定される場合は、優先順位が高いコールがボイスメッセージング システムに転送されません。このパラメータが [True] に設定されている場合、優先コールはボイスメール システムに転送されます。 MLPP では、ボイスメールシステムではなくユーザが常に優先コールに応答する必要があるので、このパラメータを [False] に設定することをお勧めします。 デフォルトは **[False]** です。

Multilevel Precedence and Preemption のパーティションの設定

パーティションを設定して、電話番号（DN）の論理グループと、到達可能性の特徴が類似したルート パターンを作成します。パーティションに通常、配置されるデバイスは、DNs とルート パターンを含みます。これらのエンティティは、ユーザがダイヤルする DNs に関連付けられます。わかりやすくするために、パーティション名は通常、その特性を反映しています。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 8 [保存（Save）] をクリックします。

パーティション命名のガイドライン

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 *97*：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

Multilevel Precedence and Preemption のコーリング サーチ スペースの設定

コーリング サーチ スペースは、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 スペースは、IP 電話、ソフトフォン、ゲートウェイなどのコーリング デバイスがコールを完了しようとしたときに検索できるパーティションを決めます。

手順

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 8 [保存（Save）] をクリックします。

Multilevel Precedence and Preemption（MLPP）のルート パターンの設定

内部および外部コールの両方をルーティングまたはブロックするためにルートパターンを設定します。

手順

ステップ 1 Cisco Unified CM の管理から、**[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。

ステップ 2 次のいずれかの作業を実行します。

- 既存のルーティングパターン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、結果のリストから既存のルーティングパターンを選択します。
- 新規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。**

ステップ 3 **[ルートパターンの設定（Route Pattern Configuration）]** ウィンドウ内の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、「関連項目」の項を参照してください。

ステップ 4 [保存（Save）] をクリックします。

Multilevel Precedence and Preemption のルート パターン設定フィールド

表 *98 : Multilevel Precedence and Preemption* のルート パターン設定フィールド

フィールド	説明
ルート パターン（Route Pattern）	番号やワイルドカードなどを含む、ルートパターンを入力します。たとえば、NANP の場合には、標準的なローカル アクセス用に「9.@」と入力したり、標準的なプライベート ネットワーク番号計画用に「8XXX」と入力したりします。有効な文字には大文字 A、B、C、D、および国際エスケープ文字（+）を表す \+ が含まれます。
MLPP優先度（MLPP Precedence）	ドロップダウン リストから、このルート パターンの MLPP 通知設定を選択します。 • [エグゼクティブオーバーライド（Executive Override）]：MLPP コールで最も高い優先度設定です。 • [フラッシュ オーバーライド（Flash Override）]：MLPP コールで 2 番目に高い優先度設定。 • [フラッシュ（Flash）]：MLPP コールで 3 番目に高い優先度設定。 • [即時（Immediate）]：MLPP コールで 4 番目に高い優先度設定。 • [優先度（Priority）]：MLPP コールで 5 番目に優先される設定です。 • [標準（Routine）]：MLPP コールで最も低い優先度設定。 • [デフォルト（Default）]：着信の優先レベルはオーバーライドされず、元のままになります。

フィールド	説明
ブロックコール率の適用（Apply Call Blocking Percentage）	宛先コード制御（DCC）機能を有効にするには、このチェックボックスをオンにします。DCC を有効にすると、優先度がフラッシュ以上に設定されているコールを除き、接続先に発信されたすべてのコールがフィルタ処理され、その接続先に設定されているブロック コール率の割り当てに基づいてコールが許可またはブロックされます。優先度がフラッシュ以上に設定されているコールは、常に許可されます。DCC はデフォルトで無効になっています。 [コールブロック率の適用（Apply Call Blocking Percentage）] フィールドが有効にされるのは、MLPP レベルが即時、優先度、標準、またはデフォルトの場合のみです。
コールブロック率（%）（Call Blocking Percentage (%)）	この接続先に対してコールをブロックするパーセンテージを数値で入力します。この値は、ルート パターンによってブロックされる、この接続先に対して発信された優先度の低いコールのパーセンテージを指定します。このパーセンテージで制限されるのは、優先度の低いコールのみです。この接続先に対して行われる、優先度がフラッシュ以上のコールは、常に許可されます。 [コールブロック率（%）（Call Blocking Percentage (%)）] フィールドが有効にされるのは、[コールブロック率の適用（Apply Call Blocking Percentage）] チェックボックスがオンにされている場合のみです。
リソースプライオリティ名前空間ネットワークドメイン（Resource Priority Namespace Network Domain）	ドロップダウン リストから [リソース プライオリティ名前空間ネットワーク ドメイン（Resource Priority Namespace Network Domain）] を選択します。リソース優先度名前空間ネットワーク ドメインを設定するには、[システム（System）][MLPP][名前空間][リソース優先度名前空間ネットワークドメイン（Resource Priority Namespace Network Domain）] の順に選択します。

Multilevel Precedence and Preemption のトランスレーション パターンの設定

コールされてからコールをルーティングされる方法を指定するには、トランスレーション パターンを設定します。トランスレーションパターンを設定すると、システムで必要に応じて発信と発信された数字を処理できます。パターン一致が発生していることを確認すると、システムは後続の一致を実行するためにトランスレーションパターン用に設定されたコーリングサーチスペースを使用します。

手順

ステップ 1 Cisco Unified CM Administration で、**[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。

ステップ 2 次のいずれかの操作を実行します。

- 既存のトランスレーション パターンの設定を変更するには、検索条件を入力し、[検索（Find）] をクリックし、結果リストから既存のトランスレーション パターンを選択します。
- 新しいトランスレーション 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。

ステップ 3 [MLPP 優先設定（MLPP Precedence）] ドロップダウン リストから、トランスレーション パターンに次のいずれかの設定を選択します。

- [エグゼクティブ オーバーライド（Executive Override）]：MLPP コールに関する最高優先設定。
- [フラッシュ オーバーライド（Flash Override）]：MLPP コールに関する 2 番目に高い優先設定。
- [フラッシュ（Flash）]：MLPP コールに関する 3 番目に高い優先設定。
- [イミディエート（Immediate）]：MLPP コールに関する 4 番目に高い優先設定。
- [プライオリティ（Priority）]：MLPP コールに関する 5 番目に高い優先設定。
- [ルーチン（Routine）]：MLPP コールに関する最低優先設定。
- [デフォルト（Default）]：入力優先レベルをオーバーライドせずに、そのまま通過させます。

ステップ 4 [リソース プライオリティ ネームスペース ネットワーク ドメイン（Resource Priority Namespace Network Domain）] ドロップダウン リストから、設定したリソース プライオリティ ネームスペース ネットワーク ドメインを選択します。

ステップ 5 [コーリング サーチ スペース（Calling Search Space）] ドロップダウン リストから、設定したコーリング サーチ スペースを選択します。

ステップ 6 [保存（Save）] をクリックします。

ゲートウェイの Multilevel Precedence and Preemption の設定

非 IP 通信デバイスと通信するように Cisco Unified Communications Manager を設定します。

始める前に

- 次のいずれかのゲートウェイを設定します。
  - Cisco Catalyst 6000 24 ポート FXS ゲートウェイ
  - Cisco Catalyst 6000 E1 VoIP Gateway
  - Cisco Catalyst 6000 T1 VoIP Gateway
  - Cisco DE-30+ ゲートウェイ
  - Cisco DT-24+ ゲートウェイ

• H.323 ゲートウェイ

手順

ステップ 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。

ステップ 2 次のいずれかの操作を実行します。

- 既存のゲートウェイ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、結果のリストからゲートウェイを選択します。
- 新しいゲートウェイを追加するには：
  1. [新規追加（Add New）] をクリックします。
  2. [ゲートウェイ タイプ（Gateway Type）] ドロップダウン リストから、サポート ゲートウェイ モデルのいずれかを選択します。
  3. [次へ（Next）] をクリックします。

ステップ 3 [ゲートウェイの設定（Gateway Configuration）] ウィンドウで MLPP 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、「関連項目」の項を参照してください。

ステップ 4 [保存（Save）] をクリックします。

電話機の Multilevel Precedence and Preemption の設定

⚠

注意 デバイスに対して、[MLPP通知（MLPP Indication）] を [オフ（Off）] または [デフォルト（Default）]（デフォルトがオフの場合）に設定したとき、[MLPPプリエンプション（MLPP Preemption）] を [強制（Forceful）] に設定しないでください。

手順

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

ステップ 2 検索条件を入力します。

ステップ 3 [検索（Find）] をクリックして、結果リストから電話を選択します。

ステップ 4 [電話の設定（Phone Configuration）] ウィンドウで MLPP 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、「関連項目」の項を参照してください。

電話の Multilevel Precedence and Preemption 設定

表 *99* : 電話の *Multilevel Precedence and Preemption* 設定

電話機の MLPP 設定 フィールド	説明
共通デバイス設定（Common Device Configuration）	設定した共通デバイス構成を選択します。共通デバイス設定には、特定のユーザに関連付けられている属性（サービスまたは機能）が含まれています。
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から、設定したコーリングサーチスペース(CSS)を選択します。コーリングサーチスペースは、検索対象のパーティションのコレクションで構成され、ダイヤル番号のルーティング方法を決めるために使用されます。デバイス用のコーリングサーチスペースと電話番号用のコーリングサーチスペースは併用することができます。電話番号の CSS は、デバイスの CSS に優先します。
MLPPドメイン（MLPP Domain）	MLPP ドメインのドロップダウンリストから、このデバイスに関連付ける MLPP ドメインを選択します。値を **[なし（None）]** のままにすると、このデバイスは共通デバイス設定に設定されている MLPP ドメインを継承します。共通デバイス設定に MLPP ドメインが設定されていない場合、このデバイスは、[MLPP ドメイン ID（MLPP Domain Identifier）] エンタープライズパラメータに設定されている MLPP ドメインを継承します。

電話機の MLPP 設定 フィールド	説明
MLPP通知（MLPP Indication）	利用可能な場合、この設定は、優先トーンを再生できるデバイスで、MLPP 優先コールを発信するときにその機能を使用するかどうかを指定します。 ドロップダウン リストから、このデバイスに割り当てる設定として次のオプションのいずれかを選択します。 • **[デフォルト（Default）]**：このデバイスは共通デバイス設定から MLPP 通知設定を継承します。 • [オフ（Off）]：MLPP 優先コールの通知を処理しません。 • **[オン（On）]**：MLPP 優先コールの通知を処理します。 （注） デバイスに対して、[MLPP通知（MLPP Indication）] を [オフ（Off）] または [デフォルト（Default）]（デフォルトがオフの場合）に設定したとき、[MLPPプリエンプション（MLPP Preemption）] を [強制（Forceful）] に設定しないでください。 MLPP 通知をオンにすると（エンタープライズ パラメータまたはデバイス レベルで）、MLPP 通知がデバイスでオフになっている（オーバーライドされている）場合を除き、デバイスの回線の通常の呼び出し音設定の動作が無効になります。
MLPP プリエンプション（MLPP Preemption）	この設定は、一部のデバイスでは利用できません。使用できる場合、この設定は、進行中のコールをプリエンプション処理可能なデバイスが MLPP 優先コールを発信するときにこの機能を使用するかどうかを指定します。 ドロップダウン リストから、このデバイスに割り当てる設定として次のオプションのいずれかを選択します。 • **Default** ：このデバイスは、共通デバイス設定から MLPP 優先コール設定を継承します。 • [無効（Disabled）]：このデバイスは、高優先コールの実行が必要なときに、低優先コールのプリエンプションの実行を許可しません。 • [強制（Forceful）]：このデバイスは、高優先コールの実行が必要なときに、低優先コールのプリエンプションの実行を許可します。

Multilevel Precedence and Preemption コールの電話番号の設定

デバイスを設定した後、更新された [デバイス設定（Device Configuration）] ウィンドウから回線（ディレクトリ番号）を追加できます。

手順

ステップ 1 Cisco Unified CM Administration の [デバイスの設定（Device Configuration）] ウィンドウで、該当する行の **[新規 DN を追加（Add a new DN）]** をクリックします。

ステップ 2 [ターゲット（接続先）（Target (Destination)）] フィールドに、この電話番号が優先コールを受信し、この番号とそのコール転送先の両方が優先コールに応答しない場合に、MLPP 優先コールを転送する番号を入力します。

値には、数字、シャープ（#）およびアスタリスク（*）を使用できます。

ステップ 3 [MLPP コーリング サーチ スペース（MLPP Calling Search Space）] ドロップダウン リストから、MLPP 代替パーティのターゲット（接続先）番号に関連付けるコーリング サーチ スペースを選択します。

ステップ 4 [MLPP 無応答時の着信転送までの時間（秒）（MLPP No Answer Ring Duration (seconds)）] で、この電話番号とそのコール転送先が優先コールに応答しない場合に、MLPP 優先コールをこの電話番号の代替パーティに転送するまでに待機する秒数（4 ～ 60）を入力します。

[優先代替パーティ タイムアウト（Precedence Alternate Party Timeout）] エンタープライズ パラメータで設定した値を使用するには、この設定を空白のままにします。

ステップ 5 [保存（Save）] をクリックします。

Multilevel Precedence and Preemption のユーザ デバイス プロファイルの設定

ユーザ プロファイルが電話機に割り当てられると、その電話は、ユーザに関連付けられている CSS を含む割り当てられたユーザの設定を継承します。しかし、電話の CSS は、ユーザ プロファイルを上書きします。パターン一致が発生すると、Cisco Unified Communications Manager は、そのコールへのダイヤル パターンに関連付けられる優先度レベルを割り当てます。システムは、割り当てられた優先度レベルで優先度の高いコールとしてコール要求を設定します。

手順

ステップ 1 Cisco Unified CM Administration 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（Device Profile）]** を選択します。

ステップ 2 次のいずれかの操作を実行します。

- 既存のデバイス プロファイルを変更するには、検索条件を入力して **[検索（Find）]** をクリックし、結果のリストから既存のデバイス プロファイルを選択します。
- 新しいデバイスプロファイルを追加するには、次のようにします。
  - [新規追加（Add New）] をクリックします。
  - **[デバイスプロファイルタイプ]** ドロップダウンリストから、プロファイルタイプを選択します。
  - [次へ（Next）] をクリックします。
  - **[デバイスプロトコル]** ドロップダウンリストから **[SIP]** または **SCCP** を選択します。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 **[MLPP ドメイン]** ドロップダウンリストから、設定した MLLP ドメインを選択します。

ステップ 5 [MLPP 通知（MLPP Indication）] ドロップダウン リストから、以下のいずれかの設定を選択して、MLPP 優先コールがあったときに優先トーンを再生できるデバイスで機能を使用するかどうかを指定します。

- [デフォルト（Default）] : MLPP 表示設定をデバイス プールから継承します。
- [オフ（Off）] ：このデバイスは、MLPP 優先コールの通知を処理しません。
- [オン（On）] : MLPP 優先コールの通知を処理します。

ステップ 6 [MLPPプリエンプション（MLPP Preemption）] リストから、以下のいずれかの設定を選択して、MLPP 優先コールがあったときに進行中のコールをプリエンプション可能かどうかを指定します。

- [デフォルト（Default）] ：このデバイスは、デバイス プールから MLPP プリエンプションを継承します。
- [無効（Disabled）] : このデバイスは、高優先コールの実行が必要なときに、低優先コールのプリエンプションの実行を許可しません。
- [強制（Forceful）] ：このデバイスは、高優先コールの実行が必要なときに、低優先コールのプリエンプションの実行を許可します。

ステップ 7 [保存（Save）] をクリックします。

Multilevel Precedence and Preemption のデフォルトのデバイス プロファイルの設定

ユーザがユーザ デバイス プロファイルがない電話機モデルにログインするたびに、デフォルト 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 プロファイルは、特定のデバイスに関連付けられている機能とサービスで構成されています。

⚠

注意 次の設定の組み合わせを使って、デフォルトのデバイス プロファイルを設定しないでください。[MLPP 通知（MLPP Indication）] を [オフ（Off）] または [デフォルト（Default）]（デフォルトがオフの場合）に設定し、[MLPP プリエンプション（MLPP Preemption）] を [強制（Forceful）] に設定。

手順

ステップ 1 Cisco Unified CM Administration で、**[デバイス（Device）]** > **[デバイス設定（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。

ステップ 2 次のいずれかの操作を実行します。

- 既存のデフォルトのデバイス プロファイルの設定を変更するには、[デバイス プロファイルのデフォルト（Device Profile Defaults）] セクションから既存のデフォルトのデバイス プロファイルを選択します。
- 新しいデフォルトのデバイス プロファイルを追加するには、ドロップダウン リストからデバイス プロファイルの種類を選択後、[次へ（Next）] をクリックしてデバイス プロトコルを選択し、[次へ（Next）] をクリックします。

ステップ 3 [MLPP Domain（MLPP ドメイン）] ドロップダウン リストから、デバイスに関連付けるために設定した MLPP ドメインを選択します。

ステップ 4 [MLPP 通知（MLPP Indication）] ドロップダウン リストから、以下のいずれかの設定を選択して、MLPP 優先コールがあったときに優先トーンを再生できるデバイスで機能を使用するかどうかを指定します。

- [デフォルト（Default）]：MLPP 表示設定をデバイス プールから継承します。
- [オフ（Off）]：このデバイスは、MLPP 優先コールの通知を処理しません。
- [オン（On）]：MLPP 優先コールの通知を処理します。

ステップ 5 [MLPPプリエンプション（MLPP Preemption）] リストから、以下のいずれかの設定を選択して、MLPP 優先コールがあったときに進行中のコールをプリエンプション可能かどうかを指定します。

- [デフォルト（Default）]：このデバイスは、デバイス プールから MLPP プリエンプションを継承します。
- [無効（Disabled）]：このデバイスは、高優先コールの実行が必要なときに、低優先コールのプリエンプションの実行を許可しません。

- [強制（Forceful）]：このデバイスは、高優先コールの実行が必要なときに、低優先コールのプリエンプションの実行を許可します。

ステップ 6 [保存（Save）] をクリックします。

マルチレベルの優先順位および優先権の連携動作と制限事項

Multilevel Precedence and Preemption の連携動作

表 *100 : Multilevel Precedence and Preemption* の連携動作

機能	連携動作
729 Annex A	729 Annex A をサポートしています。
Cisco Extension Mobility	ユーザが Extension Mobility を使用してデバイスにログインしている場合、MLPP サービス ドメインはユーザ デバイス プロファイルに関連付けられたままになります。MLPP の表示とプリエンプションの設定も、Extension Mobility によって伝搬されます。デバイスまたはデバイス プロファイルのいずれかが MLPP をサポートしていない場合、これらの設定は伝搬されません。
Cisco Unified Communications Manager Assistant	MLPP は、Cisco Unified Communications Manager と次のように相互作用します。 • Cisco Unified Communications Manager Assistant で MLPP 優先コールが処理される場合、Cisco Unified Communications Manager Assistant によりコール優先順位が保持されます。 • Cisco Unified Communications Manager Assistant は、他のすべてのコールと同じように MLPP 優先コールをフィルタリングします。コールの優先順位は、コールがフィルタリングされるかどうかには影響を与えません。 • Cisco Unified Communications Manager Assistant はコールの優先順位を登録しないので、Assistant Console でコールの優先順位について追加のインジケータを送信することはありません。

機能	連携動作
即時転送	即時転送は、コールのタイプ（たとえば、優先コールなど）に関係なく、コールをボイスメッセージングメールボックスに転送します。Alternate Party Diversion（コールの優先順位）がアクティブになっている場合は、無応答時転送（CFNA）も非アクティブになります。
Resource Reservation Protocol（RSVP）	RSVP は MLPP の本質的機能をサポートしています。RSVP がアクティブな場合の MLPP の動作については、『Cisco Unified Communications Manager システム ガイド』に説明があります。
補足サービス	MLPP は、複数ラインアピアランス、コール転送、不在転送、三者通話、コールピックアップ、およびハントパイロットと通信します。各サービスとのインタラクションについて説明している後続の項を参照してください。

Multilevel Precedence and Preemption の制限事項

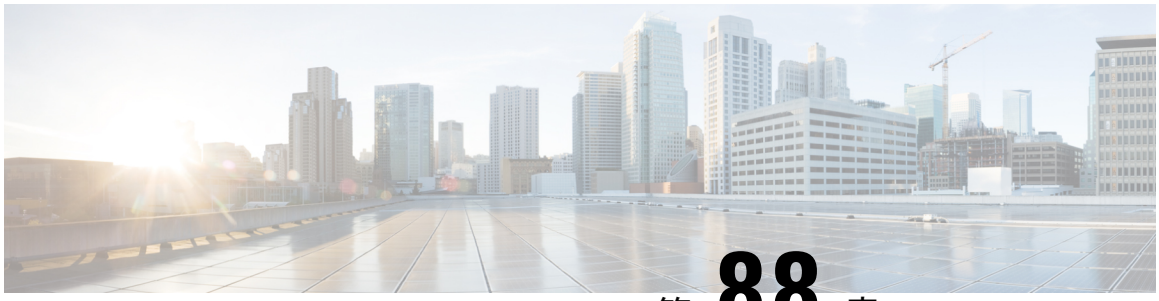
表 *101 : Multilevel Precedence and Preemption* の制限事項

制限事項	説明
帯域幅	Cisco Unified Communications Manager は、優先度の高いコール用にビデオ帯域幅を調整するときに、低優先コールをプリエンプション処理します。帯域幅がプリエンプション処理十分でない場合、Cisco Unified Communications Manager は、以前に予約した低ビデオ帯域幅を使用するようにエンドポイントに指示します。Cisco Unified Communications Manager がビデオ コールをプリエンプション処理するとき、プリエンプション処理される相手はプリエンプション トーンを受信し、コールがクリアされます。
コール詳細レコード	DRSN の場合、CDR は値 0、1、2、3、および 4 の優先レベルを表しており、DSN で使用されているように 0 はエクゼクティブ オーバーライドを示し、4 は標準を示します。このように CDR は DRSN フォーマットを使用していません。
一般的なネットワーク機能のプリエンプション	一般的なネットワーク機能のプリエンプション サポートは、Cisco Unified Communications Manager が MGCP プロトコルを使用して制御し、MLPP プリエンプションを有効に設定された、標的型の Voice over IP ゲートウェイの T1-CAS および T1-PRI（北米）インターフェイスでのみ存在します。

制限事項	説明
クラスタ間トランク	クラスタ間トランクMLPPは、ダイヤルされた数値によって優先順位情報を送達します。ドメイン情報は保存されないため、着信コールのトランクごとに設定する必要があります。
回線グループ（Line Groups）	MLPP 対応デバイスは回線グループではサポートされません。次のガイドラインを推奨します。 • 回線グループ内ではMLPP対応デバイスを設定しないでください。ただし、ルートグループはサポートしています。トランク選択とハンティングの両方の方法がサポートされています。 • MLPP対応デバイスが回線グループまたはルートグループで設定されると、プリエンプション処理が行われたときに、ルートリストがデバイスをロックしない場合、プリエンプション処理されたコールは、ルート/ハントリスト内の他のデバイスに再ルーティングされ、コールを受け取ることができるデバイスがなくなった後でのみ、プリエンプションの通知を返すことができます。 • ルートリストは、トランク選択および優先コールのハンティングのいずれかのアルゴリズムをサポートするように設定できます。方法 1 では、Preemptive 検索を直接実行します。方法2では、最初に一般的な検索を実行します。この検索がうまく行かない場合は、Preemptive 検索を実行します。方法2では、ルートリストのデバイス全体に2回繰り返す必要があります。方法2にルートリストが設定されている場合、回線グループを含む特定のシナリオでは、ルートリストはデバイス全体を2度繰り返して優先コールを検索することになります。
Look Ahead For Busy	Cisco Unified Communications Manager は Look Ahead for Busy（LFB）オプションをサポートしていません。
MLPP 通知	トーンや呼び出し音など、MLPP 関連の通知を生成するのは MLPP 通知対応のデバイスだけです。MLPP 通知対応ではないデバイスで優先コールが終了した場合、優先順位呼び出し音は再生されません。MLPP 通知対応ではないデバイスから優先コールが発信された場合、優先順位呼び戻し音は再生されません。MLPP 通知対応でないデバイスがプリエンプト処理されたコール（つまり、コールが開始したプリエンプションの相手側）に関与する場合、プリエンプショントーンはデバイスに適用されません。

制限事項	説明
電話機およびトランク	電話では、MLPP 通知が無効化された（つまり、MLPP 通知がオフに設定されている）デバイスではプリエンプション処理ができません。トランクでは、MLPP 通知とプリエンプションは個別に機能します。
リング設定動作	[MLPP通知(MLPP Indication)] を（エンタープライズ パラメータ、共通デバイス設定、またはデバイス レベルで）オンにすると、デバイスの [MLPP通知(MLPP Indication)] がオフ（無効）になっていない限り、デバイス上の回線では通常の呼び出し音設定の動作が無効になります。
SCCP	IOS ゲートウェイは、Cisco Unified Communications Manager への SCCP インターフェイスをサポートします。Cisco Unified Communications Manager でサポート対象の電話機モデルとして表示される BRI とアナログ電話機をサポートします。SCCP 電話機は、MLPP 機能をサポートしており、特定の SIP ロードを備えた電話機もサポートしています。Cisco IP 電話のサポート情報については、関連する電話機の管理とユーザガイドを参照してください。

制限事項	説明
補足サービス	補足サービスに対するMLPPサポートでは、次の制限事項が指定されます。 • MLPPは、他グループ ピックアップではなく、基本のコール ピックアップ機能およびグループ コール ピックアップ機能だけに対応しています。 • 着信 MLPP コールの不在転送（CFA）サポートにより、MLPP代替パーティ（MAP）ターゲットが設定されている場合には、着信側の MAP ターゲットにコールが常に転送されます。設定が誤っている場合（MAP ターゲットが指定されていない場合）、コールは拒否され、発信側にリオーダー音が聞こえます。 • 着信 MLPP コールの無応答時転送（CFNA）サポートにより、コールはCFNA ターゲットに1回転送されます。MAP ターゲットが設定されている場合、最初のホップの後にコールに対する応答がないと、コールは元の着信側のMAP ターゲットに転送されます。設定が誤っている場合（MAP ターゲットが指定されていない場合）、コールは拒否され、発信側にリオーダー音が聞こえます。 • 着信 MLPP コールに対する話中転送（CFB）サポートでは、転送ホップに設定されている最大数までコールを自動転送します。最大ホップ数に達した場合、MAP ターゲットが設定されていれば、コールは元の着信側の MAP ターゲットに送信されます。設定が正しくない場合（つまり、MAP ターゲットが指定されていない場合）、コールは拒否され、発信側ではリオーダー音が聞こえます。 • ハント パイロットのサポートでは、ハント グループ アルゴリズムが最長アイドル時間、優先度順、またはラウンドロビンを指定している必要があります。ビジー処理、応答なし処理、および未登録処理のハント グループ オプションが [次のメンバへ、ただし次のグループにはハントしない(Try next member, but do not go to next group)] に設定されていることを確認します。プリエンプションは単独のハント グループでのみ行われます。
ユーザアクセスチャネル	ユーザ アクセス チャネルは、MLPP プリエンプションが有効として設定されている必要がある、次の Cisco Unified IP Phone モデルでのみサポートされます。 • Cisco Unified IP Phone 7960、7962、7965 • Cisco Unified IP Phone 7940、7942、7945



第 88 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 （108 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
ステップ 1	SIP プロファイル用 ANAT の設定 （854 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。
ステップ 2	SIP 電話への ANAT の適用 （855 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。
ステップ 3	SIP トランクへの ANAT の適用 （855 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。
ステップ 4	サービスの再起動 （856 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

ステップ 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。

ステップ 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。

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

ステップ 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。

ステップ 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

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （120 ページ）を参照してください。

手順

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 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。

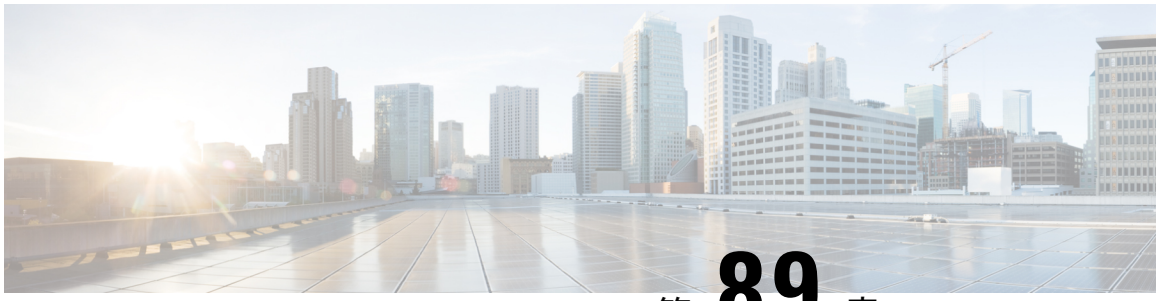
- Cisco CallManager
- Cisco CTIManager
- Cisco Certificate Authority Proxy Function
- Cisco IP Voice Media Streaming App

ステップ 3 [再起動（Restart）] をクリックします。

ステップ 4 [OK] をクリックします。

第 XI 部

参考情報



第 89 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 *102 : 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 ロギング サービス
Unified Communications Manager	Unified Communications Manager	443 / TCP	このポートは、サブスクライバノードでの COP ファイルのインストール中に、サブスクライバとパブリッシャ間の通信に使用されます。
Unified Communications Manager	RTMT	1090、1099 / TCP	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
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1500、1501 / TCP	データベース接続（1501 / TCP はセカンダリ接続）

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）	1510 / TCP	CAR IDS DB。CAR IDS エンジンが、クライアントからの接続要求を監視します。
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1511 / TCP	CAR IDS DB。アップグレード時に、CAR IDS のインスタンスをもう 1 つ開始するために使用される代替ポート。
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1515 / TCP	インストール時のノード間でのデータベース レプリケーション
Cisco Extended Functions（QRT）	Unified Communications Manager（DB）	2552 / TCP	Cisco Unified Communications Manager データベース変更通知をサブスクライバが受信できるようにします。
Unified Communications Manager	Unified Communications Manager	2551 / TCP	アクティブ/バックアップ判別のための Cisco Extended Services 間のクラスタ間通信
Unified Communications Manager（RIS）	Unified Communications Manager（RIS）	2555 / TCP	Real-time Information Services（RIS）データベース サーバー
Unified Communications Manager（RTMT、AMC、またはSOAP）	Unified Communications Manager（RIS）	2556 / TCP	Cisco RIS 向け Real-time Information Services（RIS）データベース クライアント
Unified Communications Manager（DRS）	Unified Communications Manager（DRS）	4040 / TCP	DRS プライマリエージェント
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5001 / TCP	このポートは、SOAP モニターがリアルタイム モニターリング サービスに使用します。

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）	5002 / TCP	このポートは、SOAP モニターがパフォーマンス モニター サービスに使用します。
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5003 / TCP	このポートは、SOAP モニターがコントロール センター サービスに使用します。
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5004 / TCP	このポートは、SOAP モニターがログ コレクション サービスに使用します。
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 サービスによって使用されます
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 Collection Tool Service（TCTS）：RTMT Trace and Log Central（TLC）向けのバックエンド サービス
Unified Communications Manager（Tomcat）	Unified Communications Manager（TCTS）	7000、7001、7002 / TCP	このポートは、Cisco Trace Collection Tool Service と Cisco Trace Collection Servlet との通信に使用されます。
Unified Communications Manager（DB）	Unified Communications Manager（CDLM）	8001 / TCP	クライアント データベース変更通知
Unified Communications Manager（SDL）	Unified Communications Manager（SDL）	8002 / TCP	クラスタ間通信サービス
Unified Communications Manager（SDL）	Unified Communications Manager（SDL）	8003 / TCP	クラスタ間通信サービス（CTI 対象）

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager	CMI マネージャ	8004 / TCP	Cisco Unified Communications Manager と CMI マネージャとのクラスタ間通信
Unified Communications Manager（Tomcat）	Unified Communications Manager（Tomcat）	8005 / TCP	Tomcat シャットダウンスクリプトで使用される内部リスニングポート
Unified Communications Manager（Tomcat）	Unified Communications Manager（Tomcat）	8080 / TCP	診断テストのためのサーバー間の通信
ゲートウェイ	Unified Communications Manager	8090	CUCM と GW（Cayuga インターフェイス）が Gateway Recording 機能のための通信に使用する HTTP ポート
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 マネージャによるシステムデータのクラスタ間複製
Unified Communications Manager（RIS）	Unified Communications Manager（RIS）	8888 ～ 8889 / TCP	RIS サービス マネージャのステータス要求と応答
Location Bandwidth Manager（LBM）	Location Bandwidth Manager（LBM）	9004 / TCP	LBM 間のクラスタ間通信
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。サブスクライバを新しくインストールする場合は、このポートを開く必要があります。
Unified Communications Manager	Unified Communications Manager	8443 / TCP	ノード間のコントロールセンター機能とネットワークサービスへのアクセスを可能にします。

共通サービス ポート

表 *103 :* 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、CDR）	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） SFTP サーバーに CDR データを送信します。
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。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
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	電話機およびゲートウェイに対する Trivial File Transfer Protocol（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	プライマリサーバとプロキシサーバ間のトリビアルファイル転送プロトコル（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）
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

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
SNMP サーバー	Unified Communications Manager	199 / TCP	SMUX サポートのためのネイティブ 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。

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	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。
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 のパスワード ベース認証に使用されます。
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。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
--	--	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 *104 : 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 *105 : 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送プロトコル（HTTP）
ブラウザ	Unified Communications Manager	443、8443/TCP	Hypertext Transport Protocol over SSL（HTTPS）

Cisco Unified Communications Manager から電話機への Web 要求

表 *106 : 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	ハイパーテキスト転送プロトコル（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 *107 :* 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	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。
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）

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	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、サービスなどで電話機が使用する URL。サービスごとにこれらのポートを設定できます。
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。

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	9444	
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 *108 :* 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 Encapsulation（GRE）、Encapsulating Security Payload（ESP）、認証ヘッダー（AH）。これらのプロトコル番号は、暗号化された IPSec 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	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	500 / UDP	IP Security（IPSec）プロトコル確立のためのインターネット キー エクスチェンジ（IKE）
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（TFTP）	69、次にエフェメラル / UDP	トリビアルファイル転送プロトコル（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 サービス。CIME オフパス導入モデルでのみ使用します。
Gatekeeper	Unified Communications Manager	1719 / UDP	ゲートキーパー（H.225）RAS
ゲートウェイ	Unified Communications Manager	1720 / TCP	H.323 ゲートウェイおよびクラスタ間トランク（ICT）向けの H.225 シグナリング 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トランク上の H.225 シグナリング 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、およびデータを確立するための H.245 シグナリング サービス （注） ゲートウェイの種類によって異なる、リモート システムで使用される H.245 ポート。 IOS ゲートウェイでの H.245 ポート範囲は、11000 ～ 65535 です。
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	2000 / TCP	Skinny Client Control Protocol（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 Communications Manager の導入で使用する 6608 ゲートウェイ用アップグレードポート
ゲートウェイ	Unified Communications Manager	2002 / TCP	Cisco Unified Communications Manager の導入で使用する 6624 ゲートウェイ用アップグレードポート
ゲートウェイ	Unified Communications Manager	2427 / UDP	Media Gateway Control Protocol（MGCP）ゲートウェイ コントロール
ゲートウェイ	Unified Communications Manager	2428 / TCP	Media Gateway Control Protocol（MGCP）バックホール
--	--	4000 ～ 4005 / TCP	Cisco Unified Communications Manager に音声、ビデオ、およびDチャネルのポートがないときには、これらのポートがこのようなメディアのファントム Real-Time Transport Protocol（RTP）ポートおよび Real-Time Transport Control Protocol（RTCP）ポートとして使用されます。
ゲートウェイ	Unified Communications Manager	5060 / TCP および UDP	Session Initiation Protocol（SIP）ゲートウェイおよびクラスタ間トランク（ICT）
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	5061 / TCP	Secure Session Initiation Protocol（SIPS）ゲートウェイおよびクラスタ間トランク（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（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。
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 *109 :* 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 Communications Manager の証明書信頼リスト（CTL）プロバイダ リスニング サービス
Cisco Unified Communications アプリケーション	Unified Communications Manager	2748 / TCP	CTI アプリケーション サーバー
Cisco Unified Communications アプリケーション	Unified Communications Manager	2749 / TCP	CTI アプリケーション（JTAPI/TSP）と CTI Manager 間の TLS 接続
Cisco Unified Communications アプリケーション	Unified Communications Manager	2789 / TCP	JTAPI アプリケーション サーバー
Unified Communications Manager Assistant Console	Unified Communications Manager	2912 / TCP	Cisco Unified Communications Manager Assistant サーバー（以前の IPMA）

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	1103 ～ 1129 / TCP	Cisco Unified Communications Manager Attendant Console（AC）JAVA RMI レジストリ サーバー
Unified Communications Manager Attendant Console	Unified Communications Manager	1101 / TCP	RMI サーバーは、RMI コールバック メッセージをこれらのポートを使用するクライアントに送信します。
Unified Communications Manager Attendant Console	Unified Communications Manager	1102 / TCP	Attendant Console（AC）RMI サーバー バインドポート：RMI サーバーは、これらのポートに RMI メッセージを送信します。
Unified Communications Manager Attendant Console	Unified Communications Manager	3223 / UDP	Cisco Unified Communications Manager Attendant Console（AC）サーバー回線状態ポートは、Attendant Console サーバーから ping および登録メッセージを受信し、Attendant Console サーバーに回線状態を送信します。
Unified Communications Manager Attendant Console	Unified Communications Manager	3224 / UDP	Cisco Unified Communications Manager Attendant Console（AC）クライアントは、回線状態情報およびデバイス状態情報のために AC サーバーに登録されます。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager Attendant Console	Unified Communications Manager	4321 / UDP	Cisco Unified Communications Manager Attendant Console（AC）クライアントは、コール制御のために AC サーバーに登録されます。
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 プロトコルを実行するマルチサービス IOS 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 プロトコルは、Cisco Intercompany Media Engine サーバーとの通信に使用されます。
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ンまたはテレフォニー管理アプリケーションなどのサードパーティが、Cisco Unified Communications Manager データベースに対してプログラムで読み書きするために使用する AXL/SOAP API。

CTL クライアントとファイアウォールの通信

表 *110 : 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 ファイアウォールの証明書信頼リスト（CTL）プロバイダー リスニング サービス

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 111: 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 *112 : 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 エージェントへの HTTP ポート
エンドポイント	HP SIM	2381/TCP	HP エージェントへの HTTPS ポート
エンドポイント	Compaq 管理エージェント	25375、25376、25393/UDP	COMPAQ 管理エージェント拡張（cmaX）
エンドポイント	HP SIM	50000 ～ 50004/TCP	HP SIM への HTTPS ポート

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 90 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 *113* : 表の内容

表の項目	説明
送信元	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 *114* : *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

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	SIP	TLS	5061	エフェメラル	TLSサーバー認証のリスナー ポート
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 *115 : 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

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（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 *116 : 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。

表 *117 : 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 *118 : 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 *119 : 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 *120 : 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 *121 : 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 *122 : 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 *123 : 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 *124 : 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 *125 : 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 *126 : 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 *127 : 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 *128 : 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 *129 : 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 *130 : 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 *131 : 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 - HTTP/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 *132 : 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 *133 : 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 *134 : 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 *135 : 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 [2]	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

[2] 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 *136 : 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 *137 : 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 *138 : 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 *139 : 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 *140 : 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 *141 : 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 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。
IM and Presence	エンドポイント/IM and Presence		

表 *142 : 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 *143 : 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 *144 : 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 *145 : 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 *146 :* 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。