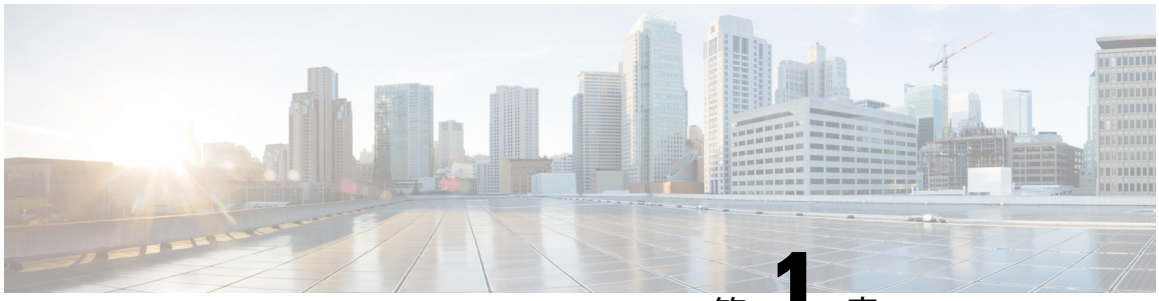
Cisco Unified Communications Manager 機能設定ガイド, リリース 15 および SUs

最終更新：2024 年 10 月 28 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。

目 次



第 1 章

新規および変更情報

新規および変更情報

次の表は、この最新リリースに関するこのガイドでの機能に対する大幅な変更の概要を示したものです。ただし、このリリースに関するガイドの変更点や新機能のなかには、この表に記載されていないものもあります。

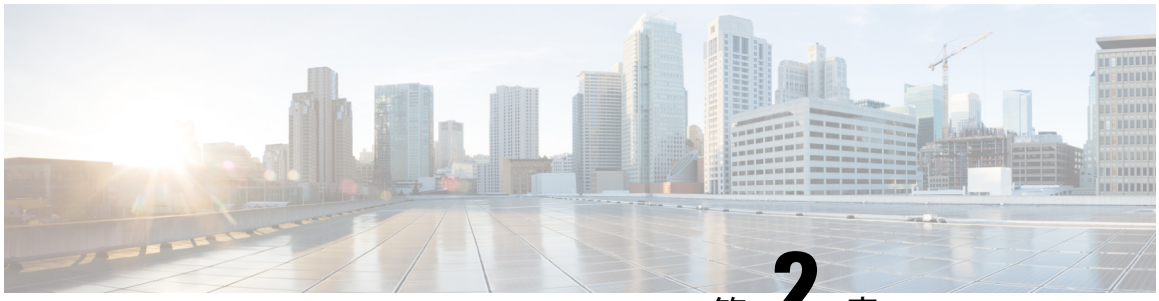
表 *1 : Unified Communications Manager* と *IM* およびプレゼンスサービスでの新機能と変更された動作

日付（Date）	説明	参照先
2024 年 10 月 01 日	TLS 1.3 のサポート	• リダイレクタ Servlet の設定 （347 ページ） • InformaCast への接続の設定 （380 ページ） • Extension Mobility Cross Cluster の概要 （521 ページ）
2024 年 10 月 01 日	Windows 11 サポートの前提条件を追加しました	Manager Assistant の前提条件 （199 ページ）
2023 年 12 月 18 日	Unified Communications Manager Assistant Administration および Assistant Console に対する Windows 11 のサポート。	Manager Assistant の前提条件 （199 ページ）

新規および変更情報

第 I 部

はじめに



第 2 章

機能設定の概要

この機能設定ガイドについて

このガイドでは、Unified Communications Manager システムで機能を設定するために実行する必要があるタスクについて説明します。 このガイドは、「初日」の設定（着信コールおよび発信コール、ダイヤル プラン、ネットワーク リソースなど）をはじめとするコール制御システムの設定後に利用します。 コール制御システムの設定の詳細については、Cisco Unified Communications Manager システム設定ガイド を参照してください。

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。

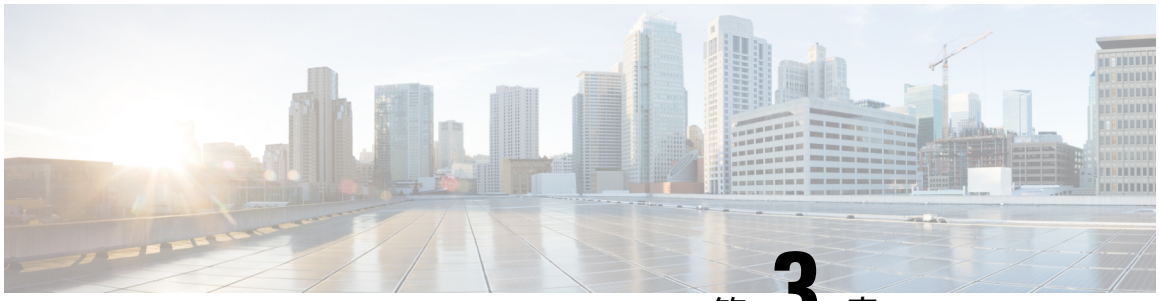
ステップ 3 次のいずれかの手順を実行します。

- [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。



第 3 章

構成ツール

この機能設定ガイドについて

このガイドでは、Unified Communications Manager システムで機能を設定するために実行する必要があるタスクについて説明します。 このガイドは、「初日」の設定（着信コールおよび発信コール、ダイヤル プラン、ネットワーク リソースなど）をはじめとするコール制御システムの設定後に利用します。 コール制御システムの設定の詳細については、Cisco Unified Communications Manager システム設定ガイド を参照してください。

構成ツールの概要

このガイドの手順では、次の 2 つの構成ツールを使用する必要があります。

- Cisco Unified Communications Manager Administration
- Cisco Unified Serviceability

この章では、ツールとそれらにアクセスする方法について簡単に説明します。

Cisco Unified Communications Manager Administration

Cisco Unified Communications Manager Administration 管理は、Unified Communications Manager ノードに対する個々の設定変更を手動で行うための Web ベースのアプリケーションです。 このガイドの手順では、このアプリケーションを使用して機能を設定する方法について説明します。

一括設定タスクを実行する必要があり、設定プロセスを自動化する場合は、Unified Communications Manager 一括管理ツール（BAT）を使用して同時に多数の変更を設定に加える

ことができます。 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。

Cisco Unified CM の管理へのログイン

次の手順を使用して、Cisco Unified Communications Manager Administration にログインします。[Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] にログインした後、メイン ウィンドウに、Unified Communications Manager のライセンスの現在の状態を示すメッセージが表示されることがあります。 たとえば、Unified Communications Manager で次の状況が確認されることがあります。

- Unified Communications Manager は現在、スターター（デモ）ライセンスで動作しているので、適切なライセンス ファイルをアップロードしてください。
- Unified Communications Manager は現在、ライセンス数が不足している状態のため、追加のライセンス ファイルをアップロードしてください。
- Unified Communications Manager は現在、適切なソフトウェア機能のライセンスを使用していません。 この状況では、Cisco CallManager サービスは停止し、適切なソフトウェア バージョンのライセンスをアップロードして Cisco CallManager サービスを再起動するまで開始しません。

次の手順でサーバを参照して、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] にログインします。

手順

ステップ 1 優先オペレーティング システムのブラウザを開始します。

ステップ 2 Web ブラウザのアドレス バーに、大文字と小文字を区別して次の URL を入力します。

`https://<Unified CM-server-name>:{8443}/ccmadmin/showHome.do`

ここで:`<Unified CM-server-name>` はサーバの名前または IP アドレスと同じ

（注） オプションで、ポート番号を指定できます。

ステップ 3 [セキュリティの警告（Security Alert）] ダイアログボックスが表示されます。 適切なボタンをクリックします。

ステップ 4 [Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] ウィンドウで、Unified Communications Manager のインストール時に指定したユーザ名とパスワードを入力し、**[ログイン（Login）]** をクリックします （両方のフィールドの内容をクリアする場合は、**[リセット（Reset）]** をクリックします。）

（注） セキュリティ目的で、Cisco Unified Communications Manager Administration は30分間無活動状態が続くとユーザをログアウトするため、ログインし直す必要があります。

Cisco Unified Communications Manager Serviceability

このガイドの一部の手順では、Cisco Unified Serviceability アプリケーションを使用して、Unified Communications Manager ノードでサービスを起動または再起動する必要があります。

Cisco Unified Serviceability は 用の Web ベースのトラブルシューティング ツールであり、次の機能を備えています。

- トラブルシューティング用にアラームとイベントを保存し、アラーム メッセージの定義を提供します。
- トレース情報を、トラブルシューティング用にログ ファイル保存します。
- Cisco Unified Real-Time Monitoring Tool（Unified RTMT）を使用して、コンポーネントの動作をリアルタイムで監視します。
- ユーザーによる、またはユーザー処理の結果としてのシステムの設定変更を記録することによって、監査機能を提供します。 この機能は、Unified Communications Manager および Cisco Unity Connection の情報保証機能をサポートします。
- [サービスの開始（Service Activation）]ウィンドウによりアクティブ化、非アクティブ化、および表示を行うことができる機能サービスを提供します。
- 日次レポート（警告サマリーやサーバ統計レポートなど）の生成とアーカイブ。
- Unified Communications Manager、IM and Presence Service および Cisco Unity Connectionが、Simple Network Management Protocol (SNMP) リモート管理およびトラブルシューティングの管理対象デバイスとして動作できるようにする。
- 1 つのノード（またはクラスタ内の全ノード）のログ パーティションのディスク使用を監視します。
- システム内のスレッドとプロセスの数をモニタする。キャッシュを使用してパフォーマンスを向上させます。
- **Unified Communications Manager** のみ：Cisco Unified Communications Manager CDR Analysis and Reporting. を使用して、サービス品質、トラフィック、請求情報の Unified Communications Manager レポートを生成します。

Cisco Unified Communications Manager Serviceability にログイン

Cisco Unified Serviceability にログインするには、次の手順を使用します。

手順

ステップ 1 優先オペレーティング システムのブラウザを開始します。

ステップ 2 Web ブラウザのアドレス バーに、大文字と小文字を区別して次の URL を入力します。

`https://<Unified CM-server-name>:{8443}/ccmadmin/showHome.do`

ここで:`<Unified CM-server-name>` はサーバの名前または IP アドレスと同じ

ステップ 3 [セキュリティの警告（Security Alert）] ダイアログボックスが表示されます。 適切なボタンをクリックします。

ステップ 4 [ナビゲーション（Navigation）] メニューのドロップダウン リストから[Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[Cisco Unified Serviceability]** を選択し、**[移動（Go）]** をクリックします。

ステップ 5 Unified Communications Manager のインストール時に指定したユーザ名とパスワードを入力して、**[ログイン（Login）]** をクリックします。

（注） セキュリティ目的で、30 分間無活動状態が続くとログアウトされ、ログインし直す必要があります。

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。

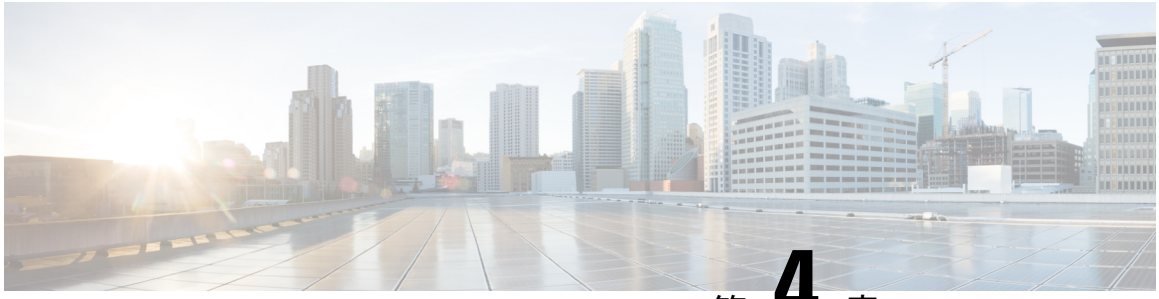
ステップ 4 [製品（Product）]ドロップダウン リストから、[All]を選択します。

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。

第 II 部

リモート ワーカー機能



第 4 章

Cisco Unified Mobility

Cisco Unified Mobility の概要

Cisco Unified Mobility 一連のモビリティ関連機能を提供し、これらを使用すると、ユーザはどこからでも、どのデバイスを使用していても、Unified Communications アプリケーションを操作できます。 ホームオフィスの電話機、Wi-Fi 接続のデュアルモード Cisco Jabber クライアント (iPhone または Android)、別の移動体通信事業者の携帯電話のいずれでも、Unified Communications の機能にアクセスし、社内でコールをアンカーできます。

たとえば、設定済みの電話機からエンタープライズ番号に転送されたコールに応答し、さらにそのコールを携帯電話に転送できます。これにより、オフィスから移動する際にも進行中の会話を継続できます。

Cisco Unified Mobility のメリット

ほとんどのモビリティ機能には社内のコール アンカリングが備わっています。モバイル デバイスでコールが発信/着信する場合でも、そのコールはエンタープライズ ゲートウェイ経由でルーティングされます。

これには次の利点があります。

- 使用しているデバイスや、オフィス内またはオフィス外のどこにいるかに関係なく、1 つのエンタープライズ電話番号とボイスメールですべてのビジネスコールに対応します。

- ビジネスコールをモバイルデバイスに転送し、オフィスの電話を使っているかのようにそのコールを続けることができます。
- モバイルデバイスから発信されたコールはエンタープライズにアンカーされ、エンタープライズ ゲートウェイ経由でルーティングされます。 これにより UC の通話中機能、集中型請求方式、コール詳細レコードを利用できるため、高価な携帯電話ネットワークを回避することでコストを削減できる可能性があります。
- ネットワーク間でローミングでき、コールはドロップされません。

Wi-Fi から LTE へのコールハンドオフ

重要 このセクションは、リリース 14SU1 以降に適用されます。

この機能により、ソフトクライアントエンドユーザーは、ネットワークの切り替え中にアクティブコールを切断することなく、Wi-Fi ネットワークと LTE ネットワーク間またはその逆を切り替えられる柔軟性が得られます。 Wi-Fi から LTE へのコールハンドオフ機能は自動的に有効になりますが、Unified Communications Manager リリース 14SU1 以降が必要です。

通話中に、ソフトクライアントがネットワークの変更を検出し、登録を切り替え、切り替えに関するエンドユーザーへの音声による表示によってアクティブコールを再接続します。 ただし、ユーザーはコールで引き続きシームレスな音声とビデオのエクスペリエンスを利用できます。

（注） この機能は、アクティブコールのハンドオーバーのみをサポートします。 コール録音がアクティブな場合、録音は停止され、ハンドオーバー後に継続されません。 また、ネットワークハンドオーバーでは、通話中機能（保留や転送など）、画面共有、会議通話、コールセンター機能がサポートされていません。 詳細については、Webex（Unified CM）での通話のための導入ガイドの「*Webex*（*Unified CM*）での通話のための環境の準備（*Prepare Your Environment for Calling in Webex (Unified CM)*）」の章を参照してください。

Cisco デスクトップと最新の Webex Mobile（WebexApp 41.8）バージョンは、この機能をサポートしています。 詳細については、Webex（Unified CM）での通話のための導入ガイドの「*Webex*（*Unified CM*）での通話に関する既知の問題と制限（*Known Issues and Limitations with Calling in Webex (Unified CM)*）」のセクションを参照してください。

モビリティ機能

Cisco Unified Mobility Cisco Unified Mobility には次のモビリティ関連機能があります。

モビリティ機能	説明
シングル ナンバー リーチ	この機能では1つの企業電話番号とボイスメールがユーザに付与されます。これにより、発信者がオフィスやゴルフコースなど、どこにいてもユーザに到達できます。 ユーザの企業電話番号がダイヤルされると、デスクフォンまたは設定されているリモート接続先（ホームオフィスの電話機、デュアルモードの Cisco Jabber クライアント（iPhone または Android）、別の移動体通信事業者の携帯電話など）で応答できます。
携帯電話に移動	継続中のコールを、デスクフォンからリモート接続先として設定済みのモバイル デバイスに転送できます。そうするには Cisco IP 電話の [**モビリティ（Mobility**）] ソフトキーを押します。 この機能は、リモート接続先の設定でシングル ナンバー リーチと密接に関連しています。 [**モバイルへ移動**] オプションに似ているオプションとして [**デスクピックアップ**] があります。これは、たとえばモバイル コールで通話中にオフィスに到着したという状況に適しています。 モバイル デバイスで通話を切断した後、[**デスクピックアップの最大待機時間（Maximum Wait Time for Desk Pickup**）] タイマーが期限切れになる前に（デフォルトは 10 秒）デスクフォンをピックアップすると、通話を速やかに再開できます。 このオプションは、シングル ナンバー リーチ設定の一部として有効にされています。 • **[保留中のコールにプライバシー設定を強制適用する（Enforce Privacy Setting on Held Calls）]** サービス パラメータを [False] に設定したことを確認します。 • また、リモート接続先とデスクフォンの間でコールを転送するには、エンタープライズ機能アクセス コードとセッション ハンドオフ コードも使用できます。
モバイル ボイス アクセス	この機能により、リモートの電話機からコールを発信し、コールを企業内にアンカーして、着信側に対してはオフィスの電話から通話しているかのように示されます。 この機能を使用する場合は、モバイル デバイスからシステム音声自動応答にダイヤル インする必要があります。 システムで発信者の認証が完了し、プロンプトに応じてコール先を入力した後は、エンタープライズ電話から発信しているかのようにコールが発信されます。 また、**モバイル音声アクセス** プロンプトを使用して、リモート接続先の**シングル ナンバー リーチ**を有効または無効にできます。

モビリティ機能	説明
エンタープライズ機能アクセス .	設定されたリモート宛先から 2 段階ダイヤリングを実行します。 また、発信元に提示されたコールが、デスク フォンから発信されたコールと同じ方法で着信側に表示されます。 **モバイル音声アクセス**とは異なり、**エンタープライズ機能アクセス**を使用するには、設定されているリモート接続先からダイヤルする必要があります。 また**エンタープライズ機能アクセス**では、リモート接続先からのコールで通話中に通話中機能を利用できます。 通話中機能にアクセスするには、各種機能（保留、独占保留、転送など）のコードを表すDTMF保留中、排他的保留、転送などのさまざまな機能のコードを表すDTMFディジットを送信します。
インテリジェントセッション制御	この機能では、企業からリモート接続先の番号に直接発信されたコール（たとえば、リモート接続先として設定されている携帯電話へ企業から発信されたコールなど）の自動コール アンカリングが有効になります。 サービス パラメータを設定することで、このようなコールを関連付けられているエンタープライズ番号に自動的にリダイレクトできます。これによりコストが削減され、UC 機能が追加されます。
デュアルモード電話	iPhone および Android の Cisco Jabber クライアントは、デュアルモード デバイスとしてプロビジョニングできます。 **デュアル モード電話**には、Wi-Fi または携帯電話ネットワーク経由で接続する機能があります。 クライアントがエンタープライズ ネットワーク内にある場合、Cisco Jabber は Wi-Fi 経由で Unified Communications Manager に登録でき、UC のコール機能とインスタント メッセージ機能を利用できます。 モバイル デバイスの電話番号を使用してモバイル ID を設定すると、エンタープライズ ネットワークを離れるときに Jabber から携帯電話にコールを転送できます。 （注） Cisco Jabber モバイル クライアントで使用できる別の機能は、モバイルおよびリモートアクセスです。この機能により、Cisco Jabber クライアントがエンタープライズ ネットワーク外部にある場合にデータ ネットワークに接続できます。 詳細については、の『Feature Configuration Guide for Cisco Unified Communications Manager』「*Mobile & Remote Access* の設定」の項を参照してください。

Cisco Unified Mobility の前提条件

次の前提条件を参照してください。

- モビリティ機能を有効にするには、ダイヤル プランとコール ルーティングの設定によって展開ニーズを満たせるように、適切な計画を策定する必要があります。 詳細について

は、『*Cisco Collaboration System Solution Reference Network Designs*』の「*Mobile Collaboration*」セクションを参照してください。

- モビリティ機能をサポートしている Cisco IP 電話の詳細については、電話機能一覧の生成（5 ページ） を参照してください。
  - モビリティ ソフトキーをサポートしている Cisco IP 電話 をリストするには、**モビリティ**機能のレポートを実行します。
  - サポートされているデュアル モード電話をリストするには、**デュアル モード**機能のレポートを実行します。
- モバイル音声アクセスを展開して、追加のロケールをシステムで使用可能にする場合（英語以外の電話ロケールまたは国特有のトーンを使用する場合）には、ロケールインストーラを cisco.com からダウンロードし、[Cisco Unified OS の管理（Cisco Unified OS Administration）] インターフェイスでインストールします。 ロケールをインストールする方法の詳細については、Cisco Unified Communications Manager および IM and Presence Service のインストールガイド を参照してください。
- セルフプロビジョニングを設定します。これにより電話ユーザは各自の Cisco Jabber クライアントとリモート接続先をプロビジョニングできます。 詳細については、Cisco Unified Communications Manager システム設定ガイド の「セルフ プロビジョニングの設定」および「エンド ユーザのプロビジョニング」のセクションを参照してください。

注意 シスコ モビリティ ソリューションは、シスコ機器でのみ検証されています。 このソリューションは他のサードパーティ製 PSTN ゲートウェイとセッション ボーダー コントローラ（SBC）でも機能しますが、各機能はここで説明するように機能しない可能性があります。 サードパーティ製 PSTN ゲートウェイまたは SBC でこのソリューションを使用している場合、シスコ テクニカル サポートが発生した問題を解決できない可能性があります。

Cisco Unified Mobility の設定タスク フロー

展開環境向けにモビリティ機能を設定するには、次のタスクをすべて行います。

手順

	コマンドまたはアクション	目的
ステップ 1	次のいずれかを実行します。 • モビリティ ユーザの設定 （21 ページ） • 一括管理を使用したモビリティ ユーザの設定 （22 ページ）	個々のエンド ユーザにモビリティ機能を追加します。 多数の既存のエンド ユーザに対してモビリティ機能を設定するには、一括管理ツールを使用します。

	コマンドまたはアクション	目的
	• LDAP を使用したモビリティ ユーザのプロビジョニング （23 ページ）	モビリティ機能で新しいユーザをプロビジョニングするには、機能グループ テンプレートと LDAP 同期を使用できます。
ステップ 2	IP フォンのモビリティの設定 （24 ページ）	Cisco IP 電話をモビリティ機能に対応して設定します（シングル ナンバー リーチ（SNR）機能と携帯電話に移動機能の設定など）。 これにより、エンタープライズ電話を使用するユーザは、エンタープライズ コールをさまざまなモバイル デバイス（ホームオフィスの電話や携帯電話など）へ転送できます。
ステップ 3	モバイル音声アクセスの設定 （31 ページ）	（オプション） モバイル音声アクセスにはシステム IVR が備わっています。これにより、モバイル ユーザはモバイル デバイスからコールを発信し、着信側に対しては、発信側が会社のデスクフォンからダイヤルしているかのように示されます。
ステップ 4	エンタープライズ機能アクセスの設定 （39 ページ）	（オプション） この機能では、設定済みのリモート接続先から 2 段階ダイヤリングを実行でき、着信側に対してはデスクフォンからコールが発信されたかのように示されます。 また、この機能ではリモート接続先からのコールで通話しているときに通話中機能を利用できます。
ステップ 5	インテリジェント セッション コントロールの設定 （40 ページ）	関連付けられているエンタープライズ番号が使用可能な場合に、リモート接続先への着信コールがその番号に再ルーティングされるように、システムを設定します。 これにより、社内でモビリティ コールのための自動コール アンカリングが実現し、その結果コストを削減し、Unified Communications 機能がさらに追加されます。
ステップ 6	モビリティ サービス パラメータの設定 （41 ページ）	（オプション）Cisco Unified Mobility の動作を変更するには、オプションのモビリティ関連サービス パラメータを設定します。

	コマンドまたはアクション	目的
ステップ 7	Cisco Jabber デュアルモードの設定 （41 ページ）	Cisco Jabber でモビリティを設定することで、ユーザは自分のスマートフォンの Jabber クライアントでエンタープライズ通信機能にアクセスできます。
ステップ 8	その他のデュアルモード デバイスの設定 （42 ページ）	その他のデュアルモードデバイス（WiFi 経由で接続できる FMC または IMS クライアントなど）を展開する場合には、このタスク フローに従います。

モビリティ ユーザの設定

モビリティ機能を使用してエンド ユーザを設定するには、この手順を実行します。

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 **[ユーザの検索と一覧表示（Find and List Users）]** ウィンドウで、次のタスクのいずれかを実行します。

- **[検索 （Find ）]** をクリックし、既存のユーザを選択して設定を変更します。
- 新しいユーザを設定するには、[新規追加] をクリックします。

ステップ 3 以下のフィールドに値を設定します。

- **ユーザー ID**
- **Last Name**

ステップ 4 **[モビリティ情報（Mobility Information）]** 領域で、次のフィールドに入力します。

a) **[モビリティの有効化（Enable Mobility）]** チェックボックスをオンにします。

b) **（オプション）** このユーザがモバイル音声アクセスを使用できるようにするには、**[モバイル音声アクセスの有効化（Enable Mobile Voice Access）]** チェックボックスをオンにします。

c) **[デスクピックアップの最大待機時間（Maximum Wait Time for Desk Pickup）]** フィールドにミリ秒単位の値を入力します。このタイマーは、リモート接続先から通話を切った後にユーザがデスクフォンからコールを再開できる期間を表します。

d) [リモート接続先制限（Remote Destination Limit）]フィールドには、各ユーザがシングル ナンバー リーチ（SNR）の対象にできるリモート接続先の数を入力します。

ステップ 5 [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。

一括管理を使用したモビリティ ユーザの設定

[一括管理（Bulk Administration）] の [**ユーザの更新（Update Users**）] メニューを使用して、モビリティ機能を既存のエンドユーザに一括追加するには、次の手順に従います。

（注） [一括管理（Bulk Administration）] には、既存のユーザを一括で更新するためのその他の機能があります。たとえば、エクスポート機能とインポート機能を使用して、新しいモビリティ設定でCSV ファイルをインポートできます。 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。

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。**[一括管理（Bulk Administration）] > [ユーザ（Users）] > [ユーザの更新（Update Users）] > [クエリー（Query）]**。

ステップ 2 フィルタを適用し、**[検索（Find）]** をクリックして、モビリティユーザとして割り当てるユーザを選択します。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 **[モビリティ情報（Mobility Information）]** エリアで、次の 4 つのフィールドを編集します。最初に左端にあるチェックボックスをオンにして、このフィールドを更新することを示し、次に右側で次のように設定を行います。

- **[モビリティの有効化（Enable Mobility）]**：このテンプレートでプロビジョニングしたユーザに対しモビリティ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。
- [モバイル音声アクセスの有効化（Enable Mobile Voice Access）]：プロビジョニング済みのユーザがモバイル音声アクセスを使用できるようにするには、このチェックボックスをオンにします。
- **[デスクピックアップの最大待機時間（Maximum Wait Time for Desk Pickup）]**：このフィールドは、携帯電話でコールを中断した時点からデスクフォンでコールを再開するまでの許容時間を表します。
- **[リモート接続先の制限（Remote Destination Limit）]**：このフィールドは、このテンプレートを使用してプロビジョニングされたユーザに対して割り当てることができるリモート接続先またはモバイル ID の数を表します。

ステップ 5 **[ジョブ情報（Job Information）]** の下の **[今すぐ実行（Run Immediately）]** をオンにします。

ステップ 6 [送信（Submit）]をクリックします。

LDAP を使用したモビリティ ユーザのプロビジョニング

LDAPディレクトリをまだ同期していない場合は、この手順に従い、機能グループテンプレート設定を使って同期済みエンド ユーザにモビリティ機能を設定できます。 新たに同期されたユーザは、テンプレートからモビリティ設定を継承します。

（注） この手法は、LDAPディレクトリをまだ同期していない場合にのみ有効です。 初回同期の実行後には、新しい機能グループ テンプレート設定を LDAP ディレクトリ同期に割り当てることはできません。

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）]** > **[ユーザ電話/追加（User Phone/Add）]** > **[機能グループテンプレート（Feature Group Template）]**。

ステップ 2 **[機能グループ テンプレートの検索と一覧表示（Find And List Feature Group Templates）]** ウィンドウで、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テンプレートを設定します。
- **[検索（Find）]** をクリックして、設定する既存のテンプレートを選択します。

ステップ 3 テンプレートに**名前**を割り当てます。

ステップ 4 次のモビリティ フィールドを設定します。

- **[モビリティの有効化（Enable Mobility）]**：このテンプレートでプロビジョニングしたユーザに対しモビリティ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。
- [モバイル音声アクセスの有効化（Enable Mobile Voice Access）]：プロビジョニング済みのユーザがモバイル音声アクセスを使用できるようにするには、このチェックボックスをオンにします。
- **[デスク ピックアップの最大待機時間（Maximum Wait Time for Desk Pickup）]**：このフィールドは、携帯電話でコールを中断した時点からデスクフォンでコールを再開するまでの許容時間（ミリ秒単位）を表します。
- **[リモート接続先の制限（Remote Destination Limit）]**：このフィールドは、このテンプレートを使用してプロビジョニングされたユーザに対して割り当てることができるリモート接続先またはモバイル ID の数を表します。

ステップ 5 **[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、オンラインヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

（注） 設定した機能グループ テンプレートを、まだ同期されていない LDAP ディレクトリに割り当てます。 新たに同期したユーザは、モビリティが有効になっています。 LDAP を使用したユーザのプロビジョニングの詳細については、Cisco Unified Communications Manager システム設定ガイドの「プロビジョニング エンドユーザ」の章を参照してください。

IP フォンのモビリティの設定

Cisco IP 電話 でモビリティ機能を設定するには、次のタスクをすべて行います。 これには、シングル ナンバー リーチ（SNR） および携帯電話に移動機能の設定が含まれます。 これにより、ユーザのすべてのデバイスを呼び出す 1 つのエンタープライズ番号が割り当てられます。 また、どのデバイスが着信してもアクセスできるエンタープライズ レベルのボイスメールも割り当てられます。 また、ユーザはアクティブなコールをデスクフォンとモバイル デバイスの間で転送することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	モビリティ用のソフトキー テンプレートの設定 （25 ページ）	モビリティ ソフトキーを含む Cisco IP 電話 のモビリティ ソフトキー テンプレートを設定します。 ユーザはソフトキーを押すだけでデスクフォンから携帯電話にコールを転送できます。
ステップ 2	IP フォンのモビリティの設定 （27 ページ）	IP Phone でモビリティを設定して、エンタープライズ番号への着信コールをユーザのリモート接続先に転送できるようにします。
ステップ 3	リモート接続先プロファイルの設定 （27 ページ）	ユーザのすべてのリモート接続先番号に適用する共通設定を設定します。
ステップ 4	リモート接続先の設定 （28 ページ）	リモート接続先とは、ユーザに到達できるモバイル デバイスを表します（ホーム オフィスの電話機や携帯電話ネットワークの携帯電話など）。 リモート接続先の多くの設定は、ユーザのデスクフォンと同じです。
ステップ 5	アクセス リストの設定 （29 ページ）	（オプション） どのコールがリモート接続先を呼び出すか、およびその時間帯を制御します。 アクセス リストによって発信者 ID に基づいて発信者をフィル

	コマンドまたはアクション	目的
		タリングでき、さらにリモート接続先の呼び出しスケジュール中にその発信者からのコールを許可またはブロックできます。

モビリティ用のソフトキー テンプレートの設定

モビリティ ソフトキーを含むソフトキーテンプレートを設定するには、次の手順に従います。このテンプレートを使用しているすべての電話機でソフトキーが有効になります。

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。**[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）]**。

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、次の手順に従います。 それ以外の場合は、次のステップに進みます。

a) [新規追加] 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]** をクリックします。

ステップ 3 既存のテンプレートにモビリティ ソフトキーを追加するには、次の手順に従います。

a) 検索条件を入力して **[検索（Find）]** をクリックします。
b) 既存のテンプレートを選択します。

ステップ 4 （任意） 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するには、[**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 **[保存]** をクリックします。

ステップ 6 [**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 7 [**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、ソフトキーを追加するコール状態を選択します。 通常、コール状態 [**オンフック（OnHook**）] と [**接続中（Connected**）] の両方にソフトキーを追加します。

ステップ 8 [**選択されていないソフトキー（Unselected Softkeys**）] リストから**モビリティ** ソフトキーを選択し、右矢印を使用して [**選択されたソフトキー（Selected Softkeys**）] リストに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 9 追加のコール状態のソフトキーを表示するには、上記のステップを繰り返します。

ステップ 10 **[保存]** をクリックします。

（注） 新しいソフトキー テンプレートを作成した場合は、[**電話の設定（Phone Configuration**）] ウィンドウでテンプレートを 1 台の電話に割り当てるか、[一括管理（Bulk Administration）] の [**電話の更新（Update Phones**）] でテンプレートを電話機グループに割り当てることができます。

プロビジョニング中にソフトキーテンプレートを電話機に割り当てるには、いくつかの方法があります。 たとえば、**ユニバーサル デバイス テンプレート**の設定を使用する方法や、特定モデルのデフォルト デバイス プロファイルとして割り当てる方法などあります。

機能管理ポリシーでのモビリティの有効化

機能管理ポリシーでCisco IP 電話 の機能を有効または無効にするように設定済みの場合は、それに加えて、Cisco IP 電話 が使用するポリシーでモビリティを有効にする必要もあります。 電話が使用する機能管理ポリシー設定でこの機能を無効にすると、そのポリシーを使用するすべての Cisco IP 電話 でモビリティ ソフトキーが無効になります。

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。**[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）]**。

ステップ 2 [**検索（Find**）]をクリックし、該当するポリシーを選択します。

（注） 他の関連機能とともにモビリティを有効にするために電話機に割り当てる新しい機能管理ポリシーを作成する必要がある場合は、[**新規追加（Add New**）] を選択できます。 **[電話の設定（Phone Configuration）]** ウィンドウで電話機にポリシーを割り当てるか、または **[共通の電話プロファイルの設定（Common Phone Profile Configuration）]** で一連の電話にポリシーを割り当てることができます。 また、ユニバーサル デバイス テンプレートにポリシーを割り当てて、電話機のプロビジョニング時に電話機にそのポリシーを割り当てることもできます。

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。 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。 各機能管理ポリシー名がシステムに固有の名前であることを確認します。

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。 この説明には、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含めることが可能です。

ステップ 5 [**機能管理（Feature Control**）] エリアで、モビリティ ソフトキーに対応する [**デフォルトの上書き（Override Default**）] と [**設定の有効化（Enable Setting**）] の両方の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。

IP フォンのモビリティの設定

シングル ナンバー リーチまたは携帯電話への移動を設定済みの場合は、次の手順に従ってデスクフォンでモビリティ機能を設定すると、エンタープライズ コールをリモート接続先にリダイレクトできるようになります。

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。**[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 次のいずれかの作業を実行します。

- **[検索 （Find ）]** をクリックし、既存の電話を選択して、設定を変更します。
- 新しい電話を追加するには、**[新規追加（Add New）]** をクリックして、**[電話のタイプ（Phone Type）]** ドロップダウン リストから電話を選択します。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 [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、設定したモビリティ ソフトキー テンプレートを選択します。

ステップ 5 [所有者のユーザ ID（Owner User ID）]ドロップダウン リストから、モビリティを有効にしたユーザ アカウントを選択します。

（注） **[所有者のユーザ ID]** または **[モビリティ ユーザ ID]** フィールド のいずれかを設定できます。モビリティ ユーザはモビリティ対応デバイス用に設定され、所有者ユーザは非モビリティ デバイス用に設定されます。 両方のユーザを同じデバイスに対してする設定は推奨されません。

ステップ 6 （任意） **[機能管理ポリシー（Feature Control Policy）]** を使用して機能を有効にする場合は、ドロップダウンリストからポリシーを選択します。

ステップ 7 **[保存（Save）]** をクリックします。

リモート接続先プロファイルの設定

ユーザのすべてのリモート接続先番号に適用する共通設定を設定します。

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。**[デバイス（Device）] > [デバイス プロファイル（Device Profile）] > [リモート接続先プロファイル（Remote Destination Profile）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 プロファイル名を入力します。

ステップ 4 **[ユーザ ID（User ID）]** ドロップダウン リストから、このプロファイルを適用するエンド ユーザを選択します。

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、このプロファイルを含めるデバイス プールを選択します。

ステップ 6 [リモート接続先プロファイルの設定（Remote Destination Profile 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、オンライン ヘルプを参照してください。

ステップ 7 **[保存]** をクリックします。

ステップ 8 [**関連付け情報（Association Information**）] の下にある、[**新規 DN を追加（Add a New DN**）] をクリックします。

ステップ 9 [**電話番号（Directory Number**）] フィールドに、ユーザのデスクの電話の電話番号を追加します。

リモート接続先の設定

リモート接続先とは、ユーザに到達できるモバイル デバイスを表します（ホーム オフィスの電話、携帯電話ネットワークの携帯電話、PSTN 電話など）。 リモート接続先の多くの設定は、ユーザのデスク フォンと同じです。

（注）

- 企業のユーザがリモート接続先から Cisco Jabber へのコールを開始すると、Unified Communications Manager は、Cisco TelePresence Video Communication Server（VCS）に INVITE メッセージを送信することによって、Cisco Jabber とのデータ コールの確立を試みます。 コールは VCS から応答を受信するかどうかに関係なく確立されます。
- セルフプロビジョニングが有効になっている場合は、エンド ユーザがセルフ ケア ポータルで各自の電話をプロビジョニングできます。システムでのセルフプロビジョニングの設定については、Cisco Unified Communications Manager システム設定ガイド と「セルフプロビジョニングの設定」の章を参照してください。ユーザ プロファイルの一部としてユーザのセルフプロビジョニングを有効にするには、「エンドユーザのプロビジョニング」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。**[デバイス（Device）] > [リモート接続先（Remote Destination）]** 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 [着信先（Destination）] フィールドにリモート接続先の番号を入力します。 たとえば、携帯電話番号または PSTN 番号を入力できます。

ステップ 4 [**モビリティ ユーザ ID（Mobility User ID）**] フィールドから、このリモート接続先を使用するモビリティ対応エンド ユーザを選択します。

ステップ 5 [**Unified Mobility 機能を有効にする（Enable Unified Mobility features）**] チェックボックスをオンにします。

ステップ 6 [**リモート接続先プロファイル（Remote Destination Profile）**] ドロップダウン リストから、このリモート接続先を所有するユーザに対して設定するプロファイルを選択します。

ステップ 7 [**シングル ナンバー リーチ ボイスメール ポリシー（Single Number Reach Voicemail Policy）**] ドロップダウン リストを使用してボイスメール ポリシーを設定します。

a) [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ます。

b) **[携帯電話への移動を有効化（Enable Move to Mobile）]** チェックボックスをオンにして、ユーザがデスクフォンで**モビリティ** ソフトキーを押したときに表示される選択可能な接続先の一覧に、このリモート接続先を追加します。

ステップ 8 （任意） このリモート接続先へのエンタープライズ コールを特定の期間（営業日など）に限定するには、[**呼び出しスケジュール（Ring Schedule）**] を設定します。

ステップ 9 [**上記の呼び出しスケジュール中に着信があったとき（When receiving a call during the above ring schedule）**] エリアで、このリモート接続先に対して設定されたリストを適用します。

ステップ 10 [リモート接続先の設定（Remote Destination 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、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。

アクセス リストの設定

アクセス リストはオプションのリモート接続先設定であり、どのコールがどのリモート接続先をどの時間に呼び出すことができるかを制御したい場合に利用できます。 アクセス リストでは発信者 ID に基づいて発信者をフィルタリングでき、さらにリモート接続先の呼び出しスケジュール中にコールを許可またはブロックできます。

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）]**>**[管理のクラス（Class of Control）]**>**[アクセス リスト（Access List）]**。

ステップ 2 [**新規追加（Add New**）]をクリックして、新しいアクセス リストを作成します。

ステップ 3 新しいアクセス リストを指定するには、名前と説明を入力します。

ステップ 4 [オーナー（Owner）] ドロップダウン リストから ID を選択し、ユーザにアクセス リストを関連付けます。

ステップ 5 次のいずれかのオプションを選択します。

- [許可（Allowed）]：アクセス リストのすべての番号が許可されます。
- [ブロック済み（Blocked）]：アクセス リストのすべての番号がブロックされます。

ステップ 6 **[保存]** をクリックします。

ステップ 7 [フィルタ マスク（Filter Mask）] ドロップダウン リストから、アクセス リストに適用するフィルタを選択します。

- [使用不可（Not Available）]：使用不可のステータスをアドバタイズするすべての発信者がアクセス リストに追加されます。
- [非公開（Private）]：非公開のステータスをアドバタイズするすべての発信者がアクセス リストに追加されます。
- [**電話番号（Directory Number**）]：指定したすべての電話番号またはディレクトリ文字列がアクセス リストに追加されます。 このオプションを選択すると、[DN マスク（DN Mask）] フィールドのすべての番号または番号文字列が追加されます。

ステップ 8 [**保存（Save**）] を選択します。

ステップ 9 リモート接続先にアクセス リストを適用します。

a) [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[デバイス（Device）]**>**[リモート接続先（Remote Destination）]** を選択して、作成したリモート接続先を再び開きます。

b) このアクセス リストの**呼び出しスケジュール**を設定し、次のいずれかを実行します。

- 許可アクセス リストを作成したら、発信者が [発信者が次のアクセスリストに登録されている場合のみ、この接続先を呼び出す（Ring this destination only if caller is in）] ラジオ ボタンをクリックして、ドロップダウン リストから作成したアクセス リストを選択します。
- 拒否アクセス リストを作成したら、発信者が [発信者が次のアクセスリストに登録されている場合は、この接続先を呼び出さない（Do not ring this destination if caller is in）] ラジオ ボタンをクリックして、ドロップダウン リストから作成したアクセス リストを選択します。

c) **[保存（Save）]** をクリックします。

モバイル音声アクセスの設定

システムでモバイル音声アクセスを設定するには、次のタスクをすべて行います。モバイル音声アクセスにより、ユーザはどのデバイスからでもエンタープライズ アンカー コールを発信できます。 ユーザがシステム IVR にダイヤルして認証された後、コールがエンタープライズ コールとして発信され、エンドユーザに対してはこのコールがオフィスの電話から発信されたかのように表示されます。

始める前に

モバイル音声アクセスを使用するには：

- [エンドユーザの設定（Configuration）] で [モバイル ボイス アクセスの有効化（Enable Mobile Voice Access）] をオンにして、ユーザをモビリティ ユーザとして有効にしておく必要があります。詳細については、モビリティ ユーザの設定 （21 ページ）を参照してください。
- 音声自動応答サービスがアクティブであること、およびトランクで使用されるメディア リソース グループ リストにそれが含まれていることが必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified Mobile Voice Access Service の有効化 （32 ページ）	Cisco Unified Serviceability で、Cisco Unified Mobile Voice Access 機能サービスがアクティブになっていることを確認します。
ステップ 2	モバイル音声アクセスの有効化 （33 ページ）	モバイル音声アクセス（MVA）を有効にし、ユーザが会社にアクセスするためにダイヤルする電話番号を指定します。
ステップ 3	モバイル音声アクセスの電話番号の設定 （33 ページ）	社外からダイヤル インするユーザに対して限られたプロンプトを指定するには、モバイル ボイス アクセス（MVA）を設定します。
ステップ 4	Cisco CallManager サービスの再起動 （34 ページ）	モバイル音声アクセス機能をアクティブにした後は、Cisco CallManager 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 5	次のいずれかのタスクを実行して、ゲートウェイにレガシー MVA またはエンタープライズ機能アクセス（EFA）を設定します。 • 既存の H.323 または SIP ゲートウェイの System Remote Access の設定（35 ページ） • 新規 H.323 ゲートウェイの Remote Access 用設定 （37 ページ）	（注） モバイル音声アクセスではゲートウェイの設定が必須ではなくなりました。 これは、ISR G2 ルータ経由でのレガシー モバイル音声アクセスを設定する場合だけのオプション設定です。 システム要件に基づいて、MVA または EFA を経由して社外からのコールを処理できるように新しいゲートウェイを追加または既存ゲートウェイを設定できます。 システムの既存の H.323 または SIP PSTN ゲートウェイがあれば、MVA をこれに設定できます。 この機能には、H.323 または SIP VoiceXML（VXML）ゲートウェイで応答および処理されるシステム設定の DID 番号を呼び出すことによってアクセスします。 ゲートウェイを設定すると、MVA ユーザに再生される自動音声応答（IVR）のプロンプトをプルするためにパブリッシャ ノードの vxml スクリプトが使用されます。 これらのプロンプトは、ユーザ認証とユーザが自分の電話のキーパッドでダイヤルする必要がある番号の入力を要求します。 既存の H.323 または SIP PSTN ゲートウェイがなく、モバイル音声アクセスを設定する場合は、新しい H.323 ゲートウェイを追加し、ヘアピニング メソッドを使用した MVA 機能を設定する必要があります。 技術的な視点では、このメソッドは着信コールを受信する 2 番目のゲートウェイを使用して MVA サービスを適用し、システムが MVA サービスを適用したあとに着信コール レッグが PSTN ゲートウェイ（元の送信元）に返します。

Cisco Unified Mobile Voice Access Service の有効化

パブリッシャ ノードでこの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。

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[ツール（Tools）] > [サービス アクティベーション（Service Activation）]** を選択します。

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 [移動（Go）]をクリックします。

ステップ 4 [**CM サービス（CM Services**）] で、[**Cisco Unified Mobile Voice Access Service**] 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。

モバイル音声アクセスの有効化

モバイル音声アクセス（MVA）を有効にし、ユーザが IVR にアクセスするためにダイヤルする電話番号または PSTN DID 番号を指定します。

始める前に

モバイル音声アクセスが機能するためには、Cisco Unified Mobile Voice Access 機能サービスがアクティブになっている必要があります。

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）] > [サービス パラメータ（Service Parameters）]**。

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 次のサービス パラメータを設定します。

- [**モバイル音声アクセスの有効化（Enable Mobile Voice Access**）] サービス パラメータを [**はい（True**）] に設定します。
- [モバイル音声アクセス番号（Mobile Voice Access Number）] : エンタープライズにアクセスするときにユーザがダイヤルするアクセス番号を入力します。

ステップ 5 **[保存（Save）]** をクリックします。

モバイル音声アクセスの電話番号の設定

社外からダイヤル インするユーザに対して限られたプロンプトを指定するには、モバイル ボイス アクセス（MVA）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。**[メディア リソース（Media Resources）]** > **[モバイル音声アクセス（Mobile Voice Access）]**。

ステップ 2 [モバイル音声アクセスの電話番号（Mobile Voice Access Directory Number）]に、ゲートウェイからのモバイル音声アクセス コールを受信する内部電話番号（DN）を入力します。

長さ 1 ～ 24 桁の値を入力します。 有効な値は0-9 です。

ステップ 3 [ローカリゼーション（Localization）]ペインで矢印を使用して、選択するロケールをこのペインとの間で移動します。

（注） モバイル音声アクセスでは、[モバイル音声アクセス（Mobile Voice Access）]ウィンドウの [選択済みのロケール（Selected Locales）] ペインに表示されている最初のロケールが使用されます。 たとえば、[選択済みのロケール（Selected Locales）] ペインに [英語（米国）（English United States）] が最初に表示されている場合、コール中に IVR を使用すると、Cisco Unified Mobility ユーザには英語が聞こえます。

ステップ 4 **[保存（Save）]** をクリックします。

Cisco CallManager サービスの再起動

モバイル音声アクセス機能を有効にした後は、Cisco CallManager サービスを再起動します。

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[ツール]** > **[コントロールセンター][機能サービス]**

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

ステップ 3 [**CM サービス（CM Services）**] で、**Cisco CallManager** サービスに対応するラジオボタンを選択します。

ステップ 4 **再起動（Restart）**をクリックします。

次のタスク

Unified Communications Manager でモバイル音声アクセスのネイティブ サポートを設定するために必要なタスクがすべて完了しました。 ただし、ISR G2 ルータによって IVR プロンプトと音声プロンプトが提供されるレガシー モバイル音声アクセスを設定するには、以下の 2 つのオプションのタスクを実行できます。

既存の H.323 または SIP ゲートウェイの System Remote Access の設定

システムの既存の H.323 または SIP PSTN ゲートウェイがあれば、MVA をこれに設定できます。 この機能には、H.323 または SIP VoiceXML（VXML）ゲートウェイで応答および処理されるシステム設定の DID 番号を呼び出すことによってアクセスします。 ゲートウェイを設定すると、MVA ユーザに再生される自動音声応答（IVR）のプロンプトをプルするためにパブリッシャ ノードの vxml スクリプトが使用されます。 これらのプロンプトは、ユーザ認証とユーザが自分の電話のキーパッドでダイヤルする必要がある番号の入力を要求します。

始める前に

モバイル音声アクセスの電話番号の設定 （33 ページ）

手順

ステップ 1 PSTN から PRI の T1/E1 コントローラを設定します。

例：

```
controller T1 1/0
framing esf
linecode b8zs
pri-group timeslots 1-24
```

ステップ 2 PRI （T1/E1）のシリアル インターフェイスを設定します。

例：

```
interface Serial 1/0:23
ip address none
logging event link-status none
isdn switch-type primary 4ess
isdn incoming-voicevoice
isdn bchan-number-order ascending
no cdp enable
```

ステップ 3 パブリッシャ ノードから VXML アプリケーションをロードします。

例：

IOS バージョン 12.3(13) 以降の設定例

```
application service CCM
http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
```

例：

IOS バージョン 12.3 (12) 以前の設定例：

```
call application voice Unified CCM
http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
```

注意 バージョン 12.2(11) で VXML が追加されましたが、12.3(8)、12.3(9)、12.3(14)T1、および 12.2(15) などのその他のバージョンでは VXML の問題があります。

ステップ 4 ダイヤル ピアを設定して、Cisco Unified Mobility アプリケーションをシステム リモート アクセスに関連付けます。

例：

IOS 12.3 (13) およびそれ以降の設定例：

```
dial-peer voice 58888 pots
service CCM (Cisco Unified Mobility VXML application)
incoming called-number 58888
```

例：

IOS 12.3 (12) およびそれ以前の設定例：

```
dial-peer voice 100 pots
application CCM (Cisco Unified Mobility VXML application)
incoming called-number 58888
```

（58888 は、モバイル音声アクセス（MVA）の番号を示しています）

ステップ 5 MVA DN にコールを転送するためにダイヤル ピアを追加します。

例：

プライマリ Unified Communications Manager の設定例：

```
dial-peer voice 101 voip
preference 1
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.3
codec g711ulaw
dtmf-relay h245-alphanumeric
no vad
```

例：

Sample configuration for secondary Unified Communications Manager（if needed）:

```
dial-peer voice 102 voip
preference 2
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.4
codec g711ulaw
dtmf-relay h245-alphanumeric
no vad
```

（注） コールを終了するための汎用ダイヤル ピアがすでに設定されており、MVA DN と一致している場合は、この手順を実行する必要はありません。

例：

SIP ゲートウェイ VoIP ダイヤル ピアの設定例：

```
dial-peer voice 80 voip
destination-pattern <Mobile Voice Access DN>
rtp payload-type nse 99
session protocol sipv2
session target ipv4:10.194.107.80
incoming called-number .T
```

```
dtmf-relay rtp-nte
codec g711ulaw
```

新規 H.323 ゲートウェイの Remote Access 用設定

既存の H.323 または SIP PSTN ゲートウェイがなく、モバイル音声アクセスを設定する場合は、新しい H.323 ゲートウェイを追加し、ヘアピニング メソッドを使用した MVA 機能を設定する必要があります。 技術的な視点では、このメソッドは着信コールを受信する 2 番目のゲートウェイを使用して MVA サービスを適用し、システムが MVA サービスを適用したあとに着信コール レッグが PSTN ゲートウェイ（元の送信元）に返します。

（注） ヘアピニングを使用したモバイル ボイス アクセスの場合、システムを呼び出しているユーザは発信者 ID によって自動的に特定されません。 代わりに、ユーザは PIN を入力する前にリモート接続先番号を手動で入力する必要があります。 その理由は、PSTN ゲートウェイは、ヘアピニングされたモバイル ボイス アクセス ゲートウェイに到達するために、まず、コールを Unified Communications Manager にルーティングする必要があるためです。 このルート パスのため、携帯電話の番号からエンタープライズディレクトリ番号への発信者番号の変換は、モバイル ボイス アクセス ゲートウェイが通話を処理する前に行われます。 その結果、このゲートウェイでは、発信者番号と設定されているリモート接続先の照合を行うことができず、そのためユーザはリモート接続先番号の入力を求められます。

始める前に

モバイル音声アクセスの電話番号の設定 （33 ページ）

手順

ステップ 1 パブリッシャ ノードから VXML アプリケーションをロードします。

例：

IOS バージョン 12.3(13) 以降の設定例

```
application service CCM
http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
```

例：

IOS バージョン 12.3 (12) 以前の設定例：

```
call application voice CCM
http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
```

注意 バージョン 12.2(11) で VXML が追加されましたが、12.3(8)、12.3(9)、12.3(14)T1、および 12.2(15) などのその他のバージョンでは VXML の問題があります。

ステップ 2 ダイヤル ピアを設定して、Cisco Unified Mobility アプリケーションをシステム リモート アクセスに関連付けます。

例：

IOS 12.3 (13) およびそれ以降の設定例：

```
dial-peer voice 1234567 voip
service CCM
incoming called-number 1234567
codec g711u
session target ipv4:<ip_address of call manager>
```

例：

IOS 12.3 (12) およびそれ以前の設定例：

```
dial-peer voice 1234567 voip
application CCM
incoming called-number 1234567
codec g711u
session target ipv4:<ip_address of call manager>
```

ステップ 3 通話を モバイル ボイス アクセス（MVA）DN に転送するため、ダイヤルピアを追加します。

例：

プライマリ Unified Communications Manager の設定例：

```
dial-peer voice 101 voip
preference 1
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.3
voice-class h323 1
codec g711ulaw
dtmf-relay h245-alphanumeric
novad
```

例：

Sample configuration for secondary Unified Communications Manager（if needed）:

```
dial-peer voice 102 voip
preference 2
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.4
voice-class h323 1
codec g711ulaw
dtmf-relay h245-alphanumeric
novad
```

（注） コールを終了するための汎用ダイヤル ピアがすでに設定されており、MVA DN と一致している場合は、この手順を実行する必要はありません。

ステップ 4 ヘアピンを設定します。

```
voice service voip
allow-connections h323 to h323
```

ステップ 5 Unified Communications Manager で、vxml スクリプトがロード済みである H.323 ゲートウェイに着信 MVA 番号をリダイレクトするための新しいルート パターンを作成します。 新しいルー

トパターンを作成したパーティションにゲートウェイの着信 CSS がアクセスできることを確認してください。

エンタープライズ機能アクセスの設定

次の手順を使用して、リモートの通知先からのエンタープライズ機能アクセスを設定します。

- 設定されているリモート接続先からエンタープライズ コールを発信する 2 段階ダイヤリング。着信側に対しては、関連付けられているデスクフォンからコールが発信されたかのように示されます。
- リモート接続先は通話中機能にアクセスするときに EFA コードを使用します。このコードは、リモート接続先から DTMF ディジットを使用して送信されます。

（注） モバイル音声アクセスとは異なり、エンタープライズ機能アクセスでは、設定済みのリモート接続先からダイヤルする必要があります。

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。**[コールルーティング（Call Routing）] > [モビリティ（Mobility）] > [エンタープライズ機能アクセス番号設定（Enterprise Feature Access Number Configuration）]** の順に選択します。

ステップ 2 **[番号（Number）]** フィールドに、モバイル ユーザがエンタープライズ機能アクセス機能を使用するためにリモート接続先からダイヤルする一意の DID 番号を入力します。

ステップ 3 **[ルート パーティション（Route Partition）]** ドロップダウン リストから、DID が含まれているパーティションを選択します。

ステップ 4 （任意） この EFA 番号を、このシステムのデフォルトにする場合は、**[デフォルトのエンタープライズ機能アクセス番号（Default Enterprise Feature Access Number）]** チェックボックスをオンにします。

ステップ 5 **[保存]** をクリックします。

ステップ 6 エンタープライズ機能アクセスのサービス パラメータを設定します。

a) [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）]**。

b) [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。

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) **[エンタープライズ機能アクセスの有効化（Enable Enterprise Feature Access）]** サービス パラメータを **[はい（True）]** に設定します。

e) （任意） In the **Clusterwide Parameters （System - Mobility）** area, edit the DTMF digits that you must enter to access midcall features through Enterprise Feature Access. たとえば、**[エンター**

プライズ機能アクセス コード（**Enterprise Feature Access Code for Hold**）] サービス パラメータ（デフォルト値：***81**）を編集できます。 デフォルト値は次のとおりです。

- 保留：*81
- 特別な保留：*82
- 再開：*83
- 転送：*84
- 会議：*85
- セッション ハンドオフ：*74
- 選択的な録音の開始：*86
- 選択的な録音の停止：*87
- [ハント グループ ログイン（Hunt group login）]：新しいコードを入力します。
- [ハント グループ ログアウト（Hunt group logout）]：新しいコードを入力します。

f) **[保存（Save）]** をクリックします。

インテリジェント セッション コントロールの設定

関連付けられているエンタープライズ番号が使用可能な場合に、リモート接続先への着信コールがその番号に再ルーティングされるように、システムを設定します。 これにより、社内でモビリティ コールのための自動コールアンカリングが実現し、その結果コストを削減し、Unified Communications 機能がさらに追加されます。

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）]** > **[サービス パラメータ（Service Parameters）]**。

ステップ 2 **[サーバ（Server）]** ドロップダウン リストから、Cisco Unified Communications Manager 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（機能 - エンタープライズ番号へのリモート接続先コールの再ルーティング）（Clusterwide Parameters （Feature - Reroute Remote Desination Calls to Enterprise Number））]** で次のサービス パラメータを設定します。

- **[エンタープライズ番号へのリモート接続先コールの再ルーティング（Reroute Remote Desination Calls to Enterprise Number）]**：インテリジェント セッション コントロールを有効にするには、このパラメータを **[はい（True）]** に設定します。

- **[すべての共有回線を呼び出す]**—パラメータの値を **True** に設定します。 インテリジェント セッション コントロールが有効で、しかもこのパラメータが有効な場合、コールは社内のリモート接続先にアンカーされ、ユーザのすべての共有電話が呼び出されます。
- **[企業 DN でのすべてのコール転送を無視する]**—このパラメータは、Intelligent Session Control が有効になっている場合、リモート接続先への発信コールにのみ適用されます。デフォルトでは、このパラメータは **[はい（True）]** に設定されています。

ステップ 5 **[保存（Save）]** をクリックします。

モビリティ サービス パラメータの設定

オプションのモビリティ関連サービス パラメータを設定するには、次の手順を使用します。

手順

ステップ 1 [Cisco Unified CM 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）]**。

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 編集するサービス パラメータを設定します。 モビリティ関連パラメータは次の見出しの下にリストされています。 ヘルプを参照するには、パラメータ名をクリックします。

- **クラスタ全体のパラメータ（システム - モビリティ）（Clusterwide Parameters (System - Mobility)）**
- **クラスタ全体のパラメータ（システム - モビリティ シングル ナンバー リーチ ボイスメール）（Clusterwide Parameters (System - Mobility Single Number Reach Voicemail)）**
- **クラスタ全体のサービス パラメータ （機能 - リモート接続先へのコールのエンタープライズ番号への再ルーティング）（Clusterwide Parameters (Feature - Reroute Remote Destination Calls to Enterprise Number)）**

ステップ 5 **[保存（Save）]** をクリックします。

Cisco Jabber デュアルモードの設定

iPhone または Android の Cisco Jabber を Wifi 経由で接続可能なデュアルモード モバイル デバイスとして設定するには、以下の作業を行います。 Cisco Jabber は WiFi 経由で Unified Communications Manager に登録され、ユーザのモバイル ID でシングル ナンバー リーチが有効になっている場合はエンタープライズ番号経由で Cisco Jabber にアクセスできます。

手順

	コマンドまたはアクション	目的
ステップ 1	モビリティ プロファイルの設定 （43 ページ）	Dial through Office コールを発信する Jabber モバイル クライアントに対して一貫した発信者 ID が送信されるように、モビリティ プロファイルを設定します。
ステップ 2	Cisco Jabber のデュアルモード デバイスの追加 （44 ページ）	Cisco Jabber for iPhone または Android クライアントにデュアル モード デバイス タイプを設定します。
ステップ 3	モビリティ アイデンティティの設定 （47 ページ）	デバイスの電話番号（iPhone の電話番号など）をポイントするモビリティ ID を Jabber モバイル クライアントに追加することで、Jabber が WiFi のカバー範囲から離れても通話できるようになります。 モバイル IDで シングル ナンバー リーチの接続先を有効にします。
ステップ 4	必須: ハンドオフ番号の設定 （48 ページ）	社外に移動するデュアルモード デバイスのハンドオフ番号を設定します。 デバイスがエンタープライズ WiFi ネットワークから切断されても、リモート モバイル ネットワークや携帯電話ネットワークに再接続し、進行中のコールを中断せずに維持できます。

その他のデュアルモード デバイスの設定

携帯電話ネットワーク経由でコールを発信でき、WiFi 経由でも接続できるその他のデュアルモードモバイルデバイスを設定するには、次のタスクをすべて行います。 次に例を示します。

- Fixed Mobile Convergence（FMC）ネットワーク経由で接続するキャリア統合モバイル デバイス。
- IP マルチメディア ネットワーク経由で接続する IMS 統合モバイル デバイス

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Jabber のデュアルモード デバイスの追加 （44 ページ）	IMS または FMC デュアルモード デバイスを設定します。

	コマンドまたはアクション	目的
ステップ 2	モビリティ アイデンティティの設定（47 ページ）	実際のデバイスの電話番号を指すモビリティ ID を追加します。
ステップ 3	必須: ハンドオフ番号の設定 （48 ページ）	社外に移動するデュアルモード デバイスのハンドオフ番号を設定します。 デバイスがエンタープライズ WiFi ネットワークから切断されても、リモート モバイル ネットワークや携帯電話ネットワークに再接続し、進行中のコールを中断せずに維持できます。

モビリティ プロファイルの設定

iPhone または Android のデュアルモード Cisco Jabber クライアントのモビリティ プロファイルを設定します。 このプロファイルでは、Dial via Office コールのために一貫性のある発信者 ID を使用してクライアントが設定されます。

（注） 技術的な見地から見ると、この発信者 ID は、モビリティ アイデンティティまたは別のコールバック番号へのコールの Dial via Office Reverse（DVO-R）コールバック ポーションの間に送信されます。 DVO-R コール機能は、en bloc ダイヤルを使用します。 モビリティ ID にモビリティ プロファイルが割り当てられていない場合、または [コールバック発信者 ID（Callback Caller ID）] フィールドが空白のままである場合、システムは、デフォルトのエンタープライズ機能アクセス番号を送信します。

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）]>[モビリティ（Mobility）]>[モビリティ プロファイル（Mobility Profile）]** 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 プロファイル名を入力します。

ステップ 4 **[モバイル クライアントのコール オプション（Mobile Client Calling Option）]** ドロップダウン リストから、[Dial via Office リバース（Dial via Office Reverse）] を選択します。

（注） フィールドのオプションに関係なく、[Dial-via-Office 転送（Dial via Office Forward））] は使用できません。

ステップ 5 [Dial via Office リバース（Dial via Office Reverse）] の [コールバック発信者 ID（Callback Caller ID）] を設定します。

ステップ 6 [モビリティ プロファイルの設定（Mobility 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、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。

Cisco Jabber のデュアルモード デバイスの追加

Cisco Jabber on iPhone または Android クライアント用のデュアルモード デバイス タイプを設定するには、次の手順を使用します。

始める前に

エンドユーザがモビリティ対応であることを確認します。 また、Jabber クライアントにリモート接続先を追加する必要がある場合は、モビリティ ソフトキーを含むソフトキー テンプレートが存在す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。**[デバイス（Device）]** > **[電話（Phone）]**。

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、既存のデバイスを編集します。
- **[新規追加（Add New）]** をクリックし、電話機モデルとして **[Cisco Dual Mode for Android]** または **[Cisco Dual Mode for iPhone]** のいずれかを選択して、新しいデバイスを追加します。 [次へ（Next）]をクリックします。

ステップ 3 [電話の設定（Phone Configuration）]ウィンドウのフィールドを設定します。

製品固有の設定レイアウト フィールドの詳細については、http://www.cisco.com/go/jabber の Jabber クライアント マニュアルを参照してください。

ステップ 4 次の必須フィールドを設定します。

- デバイス名
- [デバイス プール（Device Pool）]
- ソフトキー テンプレート（Softkey Template）
- オーナーのユーザ ID（Owner User ID）：ユーザがモビリティに対応している必要があります。
- モビリティ ユーザ ID（Mobility User ID）：ユーザがモビリティに対応している必要があります。
- デバイス セキュリティ プロファイル（Device Security Profile）
- [SIPプロファイル（SIP Profile）]

ステップ 5 **[保存]** をクリックします。

ステップ 6 ディレクトリ番号を追加します。

a) 左の [関連付け（Association）] エリアで、[新規 DN を追加（Add a New DN）]をクリックします。

b) [ディレクトリ番号（Directory Number）]に新しい番号を入力し、[保存（Save）]をクリックします。

c) [ディレクトリ番号の設定（Directory Number Configuration）]ウィンドウで、設定したいフィールドに入力し、[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、オンライン ヘルプを参照してください。

d) **[エンド ユーザの関連付け]** をクリックします。

e) [検索（Find）]をクリックし、この DN を所有するモビリティ対応エンド ユーザを選択します。

f) **[選択項目の追加(Add Selected)]** をクリックします。

g) **[保存]** をクリックします。

次のタスク

iPhone または Android の電話番号を指すモビリティ ID を追加します。 これにより、Wi-Fi の範囲外へ移動した場合にコールを電話機に転送できます。 また、シングル ナンバー リーチの接続先としてこのデバイスを追加することもできます。詳細は、モビリティ アイデンティティの設定 （47 ページ）を参照してください。

必要に応じて、Cisco Jabber クライアントにリモート接続先とシングル ナンバー リーチを追加します。 Jabber クライアントを呼び出すと、リモート接続先も呼び出されます。 リモート接続先の設定 （28 ページ）.

デュアルモード デバイス設定フィールド

表 *2:* デュアルモード デバイス設定フィールド

フィールド	説明
ソフトキーテンプレート（Softkey Template）	モビリティ ソフトキー テンプレートを選択します。
[オーナーのユーザ ID(Owner User ID)]	割り当てられた電話機ユーザのユーザ 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。
モビリティ ユーザ ID（Mobility User ID）	このデュアルモード フォンを割り当てるユーザのユーザ ID を選択します。

フィールド	説明
デバイスセキュリティ 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 Administration で設定されているすべての電話にセキュリティ プロファイルを適用する必要があります。 電話機のセキュリティ機能を有効にするには、デバイス タイプとプロトコルに応じた新しいセキュリティ プロファイルを設定してから、電話機に適用する必要があります。
再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）	設定されたリモート接続先にコールをルーティングするためのコーリング サーチ スペースと、このデバイスに対して設定されたモビリティ アイデンティティを選択します。
[SIPプロファイル（SIP Profile）]	[モバイル デバイスの標準 SIP プロファイル（Standard SIP Profile for Mobile Device）]を選択します。

その他のデュアルモード デバイスの追加

別のデュアル モード デバイス（ネットワークベースの FMC 用**キャリア統合モバイル デバイス**や**IMS 統合モバイル デバイス**など）を追加するには、この手順を使用します。

始める前に

エンド ユーザがモビリティ対応であることを確認します。 ユーザのモビリティを有効にする方法の詳細については、この章の以前のトピック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。**[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 **[電話機モデル（Phone Model）]** ドロップダウン リストから **[キャリア統合モバイル デバイス（Carrier-integrated Mobile Device）]** または **[IMS 統合モバイル デバイス（IMS-integrated Mobile Device）]** を選択します。

ステップ 4 次の必須フィールドを設定します。

- デバイス名
- [デバイス プール（Device Pool）]
- オーナーのユーザ ID（Owner User ID）：ユーザがモビリティに対応している必要があります。
- モビリティ ユーザ ID（Mobility User ID）：ユーザがモビリティに対応している必要があります。

ステップ 5 [電話の設定（Phone Configuration）]ウィンドウの残りのフィールドを設定します。 フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

ステップ 7 ディレクトリ番号を追加します。

a) 左の [関連付け（Association）] エリアで、[新規 DN を追加（Add a New DN）]をクリックします。

b) [ディレクトリ番号（Directory Number）]に新しい番号を入力し、[保存（Save）]をクリックします。

c) [ディレクトリ番号の設定（Directory Number Configuration）]ウィンドウで、設定したいフィールドに入力し、[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、オンライン ヘルプを参照してください。

d) **[エンド ユーザの関連付け]** をクリックします。

e) [検索（Find）]をクリックし、この DN を所有するモビリティ対応エンド ユーザを選択します。

f) **[選択項目の追加(Add Selected)]** をクリックします。

g) **[保存（Save）]** をクリックします。

モビリティ アイデンティティの設定

エンタープライズ番号で呼び出すことができるシングル ナンバー リーチとしてデバイスを有効にするには、デバイスの電話番号を指すモビリティ ID を追加します。

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）]** > **[電話（Phone）]**。

ステップ 2 必要に応じて検索条件を入力し、**[検索（Find）]** をクリックして、作成したデュアルモードデバイスを選択します。

ステップ 3 **[新規モビリティ アイデンティティの追加（Add New Mobility Identity）]** をクリックします。

ステップ 4 [着信先（Destination）] フィールドにモバイル デバイスの電話番号を入力します。 たとえば iPhone の Cisco Jabber クライアントの場合、これは iPhone の電話番号です。

ステップ 5 Cisco Jabber のみ。 設定した**モビリティ プロファイル**を選択します。

ステップ 6 このモバイル ID をエンタープライズ電話番号から使用できるようにするには、次の手順に従います。

a) [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ます。

b) [シングル ナンバー リーチ ボイスメール（Single Number Reach Voicemail）]ポリシーを設定します。

ステップ 7 [Dial-via-Office リバース ボイス メール（Dial-via-Office Reverse Voicemail）]ポリシーを設定します。

ステップ 8 [モビリティ アイデンティティの設定（Mobility Identity 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、オンライン ヘルプを参照してください。

ステップ 9 **[保存]** をクリックします。

（注） 呼び出しスケジュールとアクセス リストを適用してこのモバイル ID へのコールを特定の時間とユーザに制限するには、アクセス リストの設定 （29 ページ）を参照してください。

ハンドオフ番号の設定

ユーザが社内から外に出る間もコールを維持するには、デュアルモード電話のハンドオフモビリティを設定します。 ユーザのデバイスがエンタープライズ Wi-Fi ネットワークから切断され、モバイル音声や携帯電話ネットワークに再接続しても、進行中のコールは中断せず保持されます。

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）] > [モビリティ（Mobility）] > [ハンドオフ設定（Handoff Configuration）]** を選択します。

ステップ 2 [**ハンドオフ番号（Handoff Number）**] フィールドに、Wi-Fi とモバイル音声または携帯電話ネットワーク間のハンドオフ用のダイヤルイン方式（DID）番号を入力します。

国際エスケープ文字（+）から始まる番号の場合は、（+）の前にバックスラッシュ（\）を付ける必要があります。 例：\+15551234

ステップ 3 [**ルート パーティション（Route Partition）**] ドロップダウン リストから、ハンドオフ DID 番号が属するパーティションを選択します。

ステップ 4 **[保存（Save）]** をクリックします。

Cisco Unified Mobility コール フロー

このセクションでは、Cisco Unified Mobility一般的にシングル ナンバー リーチ （snr） として知られている着信および発信コールフローについて説明します。Unified Communications Manager デスクフォンがモバイル デバイスにコールを転送できるようにするために snr が設定されている場合、個別の発呼側番号と請求番号機能をサポートします。

たとえば、ユーザ A が PSTN ネットワークから、電話番号が SNR に設定されているユーザ B に対してコールするとします。 SIP プロファイルで [**外部プレゼンテーション名と番号の有効化（Enable External Presentation Name and Number**）] チェックボックスがオンになっており、[**外部プレゼンテーション名と番号の表示（Display External Presentation Name and Number**）] の値が [はい（*True*）]に設定されている場合、Unified Communications Manager は、ユーザ B のデスク フォンと設定済みのリモート接続先デバイスの両方に FROM ヘッダーの情報を表示します。 同様に、1 つのオプションが無効の場合、Unified Communications Manager は着信側デバイスに P-Asserted-Identity（PAID）ヘッダー情報を表示します。

同様に、発信コールのシナリオでは、電話番号設定ページで外部プレゼンテーション情報を使用して設定されているユーザ B（SNRD 回線）が SIP トランク経由で PSTN ネットワークへのコールを開始します。 SIP プロファイルで [**外部プレゼンテーション名と番号（External Presentation Name and Number**）] が設定されている場合、Unified Communications Manager は、外部プレゼンテーション情報を発信 SIP メッセージの FROM ヘッダーで送信し、着信側デバイスに表示されます。

[**外部プレゼンテーション名と番号の有効化（Enable External Presentation Name and Number**）] チェックボックスが無効になっている場合、Unified Communications Manager は、電話番号情報を FROM および PAID で送信し、着信側デバイスと、X-Cisco-Presentation ヘッダーの設定済み外部プレゼンテーション情報に表示されます。

[**匿名の外部プレゼンテーション（Anonymous External Presentation**）] チェックボックスをオンにすると、設定済みの**外部プレゼンテーション名**と**外部プレゼンテーション番号**が、着信側デバイスで匿名として表示される各フィールドおよび外部プレゼンテーションから削除されます。

外部プレゼンテーション情報の設定の詳細については、Cisco Unified Communications Manager システム設定ガイド の「電話番号の設定」の章を参照してください。

スマート クライアントを使用しない SIP トランク経由の FMC

Unified Communications Manager サービス プロバイダーは、モバイル上のスマート クライアントを使用しないトランク経由のエンタープライズダイヤリング、SNR、シングル VM、コール移動、通話中などの基本 PBX 内線機能を提供できます。 SNR、デスク電話ピックアップ、携帯電話へのコールの送信、モバイル ボイス アクセス、通話中 DTMF などの基本的なモバイル機能がサポートされています。 内線ダイヤリングは、ネットワーク上に実装され、そのネットワークが Unified Communications Manager と統合されている場合にサポートされます。 これらの機能は任意のタイプのトランクで提供できます。

Unified Communications Manager 携帯 DN がダイヤルされたときに共有回線が鳴動するように Ring All Shared Lines サービス パラメータで設定できます。

（注） Ring All Shared Lines を実行するには、Reroute Remote Destination Calls to Enterprise Number 機能を有効にする必要があります。 Reroute Remote Destination Calls to Enterprise Number はデフォルトで無効になっています。

IMS 共有回線は Ring All Shared Lines パラメータの値にのみ基づいて鳴動します。

以前のバージョンで使用していたリモート接続先機能をこの新しいデバイス タイプに移行することもできます。

通信事業者統合モバイル デバイスのハント グループ ログインとログアウト

デバイス タイプのキャリア統合モバイルを設定する場合は、[オーナーのユーザID(Owner User ID)] 値をモバイル ユーザ ID に設定します。 モバイル ユーザ ID は設定に表示されません。 モビリティが有効になっているエンド ユーザだけが、エンド ユーザ ページの **[オーナーのユーザ]** ドロップダウンに表示され、1つの回線 (DN) を FMC デバイスに関連付けることができます。 ユーザはモバイル ID を FMC に関連付ける必要があります。 これは、デバイスの追加後に FMC デバイスの設定ページで実行できます。 モバイル ID の数までコールを送達するためには、ユーザが **[モバイル ID]** ウィンドウで Cisco Unified Mobility を有効にする必要があります。

キャリア統合モバイル デバイスは、企業の機能アクセス コードを使用してハント グループのログインとログアウトをサポートするように設定できます。 次のことが設定されるか確認します。

- 企業の機能アクセス番号は、**[コール ルーティング]** > **[モビリティ]** > **[企業の機能アクセス設定]** に設定されている必要があります。
- サービス パラメータの **[ハント グループ ログイン]** フィールドと **[ハント グループ ログアウト用の企業機能アクセス番号]** フィールドで、企業機能アクセス番号の値を割り当てる必要があります。

これらを設定した後、設定された企業機能アクセス番号をダイヤルして、キャリア統合モバイル デバイスからハント グループにログインまたはログアウトできます。 ユーザが特定のハント ログイン アクセス コード番号をダイヤルした場合、キャリア統合モバイル デバイスは、ユーザがハント グループのリストに参加できるようにします。 ハント ログアウト アクセス コードがダイヤルされた場合、ユーザはハント グループのリストから外れ、コールが到達しません。

（注） キャリア統合モバイルデバイスのユーザは、企業の機能アクセス コードを使用してミッドコール機能を呼び出しできます。 企業の機能アクセスを設定して使用する方法の詳細については、エンタープライズ機能アクセスの設定セクションを参照してください。

Cisco Unified Mobility の連携動作

表 *3 : Cisco Unified Mobility* の連携動作

機能	データのやり取り
自動コール ピックアップ	Cisco Unified Mobility サービス パラメータの設定内容に応じて、自動コール ピックアップと連動します。[自動コール ピックアップが有効（Auto Call Pickup Enabled）] サービス パラメータが [True] に設定されている場合は、[ピックアップ（PickUp）] ソフトキーを押すだけで、コールをピックアップできます。 このサービス パラメータが [False] に設定されている場合は、[ピックアップ（PickUp）]、[G ピック（GPickUp）]、または [他グループ（OPickUp）] ソフトキーを押してから、[応答（Answer）] ソフトキーを押す必要があります。
自動代替ルーティング	Cisco Unified Mobility 次のように自動代替ルーティング（AAR）をサポートします。 • ロケーション ベースのサービス用の帯域幅が不足して拒否が発生した場合は、拒否によって AAR がトリガーされ、コールが PSTN 経由で再ルーティングされるため、発信者は電話を切ってリダイヤルする必要がありません。 • Resource Reservation Protocol（RSVP）が原因で拒否が発生した場合は、AAR がリモート接続先へのコールに対してトリガーされず、コールが中断されます。
拡張と接続	Cisco Unified Mobility と 拡張と接続 の両方の機能が必要なユーザは、リモート デバイス プロファイルと CTI リモート デバイスの両方のタイプのオーナー ID が同じ場合に、それらに同じリモート接続先を設定できます。 この設定では、Cisco Unified Mobility 機能と 拡張と接続 を同時に使用できます。 詳細については、「拡張と接続」 の章を参照してください。

機能	データのやり取り
外部コール制御	外部コール制御が設定されている場合、Unified Communications Manager は次の Cisco Unified Mobility 機能用の付加ルート サーバのルート決定に従います。 • Cisco Unified Mobility • 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 Unified Communications Manager は、次の Cisco Unified Mobility の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
インテリジェントセッション制御とセッション ハンドオフ	エンタープライズ番号に固定されたリモート接続先へのダイレクト コールの場合は、モバイル ユーザがセッション ハンドオフ機能を使用してデスクフォンへコールをハンドオフできます。 インテリジェント セッション制御を実装する前に、Cisco Unified Mobility を有効にする必要があります。
ライセンス	Cisco Unified Mobility ベーシックからプロフェッショナルまでのすべてのユーザ ベースのライセンスに含まれています。
ローカルルートグループ（Local Route Groups）	リモート接続先に対するシングル ナンバー リーチ コールの場合は、発信側のデバイス プールによって標準のローカル ルート グループの選択が決定されます。 （注） BiB（ビルトインブリッジ）との AgentGreeting が呼び出される場合は、ローカル ルート グループはサポートされません。

機能	データのやり取り
サポートされるコールの数	リモート接続先ごとに最大 6 つのアクティブ コールがサポートされます。ただし、サポートされるコールの数は、Unified Communications Manager の設定によって異なります。 たとえば、Cisco Unified Mobility ユーザがリモート接続先向けの 6 つのコールをすでに持っているとき、または、ユーザが DTMF を使用してリモート接続先からのコールを転送中または会議中に、コールを受信した場合です。 受信したコールは、次の場合に企業のボイスメールに送信されます。 • ユーザが使用中のコール数がビジー トリガー設定を超えています • CFB が設定されている • すべての共有電話がビジー状態です （注） 企業のボイスメールに送信されるコールは、サポートされる最大コール数に基づいていません。
Cisco Unified Border Element を使用した SIP トランク	Cisco Unified Mobility は、Cisco Unified Border Element（CUBE）を使用した SIP トランク経由の通話中機能を使用しない Cisco Unified Mobility 機能をサポートします。

Cisco Unified Mobility の制限

表 *4 : Cisco Unified Mobility* の連携動作

制約事項	説明
自動応答	自動応答が有効になっているとリモート接続先のコールは機能しません。 （注） 自動応答は、デュアルモード電話機ではサポートされていません。

制約事項	説明
未登録時コール転送	iPhone および Android の Cisco Jabber では未登録時コール転送（CFUR）は次のようにサポートされます。 • iPhone および Android の Cisco Jabber でモバイル ID とリモート接続先のどちらも設定されていない場合は、CFUR がサポートされます。 • リモート接続先が設定されている場合は CFUR がサポートされず、機能しません。 • 携帯電話番号を使ってモバイル ID が設定されており、シングル ナンバー リーチが有効な場合、CFUR はサポートされず、機能しません。 モバイル ID またはリモート接続先が設定されている場合は、代わりに話中転送または応答時転送を使用してください。
コールキューイング	Unified Communications Manager は、Cisco Unified Mobility でのコールキューイングをサポートしていません。
会議	ユーザはモバイル音声アクセスを使用し、会議コントローラとしてミートミー会議を開始できませんが、ミートミー会議に参加することはできます。 既存の会議コールが共有回線の IP フォンやデュアルモード電話、またはリモート接続先であるスマートフォンから開始された場合、コールが携帯電話に送信された後またはデュアルモードのハンドオフの操作が発生した後は、新規で会議の参加者を追加することはできません。 新規の会議参加者の追加を許可するには、[高度なアドホック会議有効化（Advanced Ad Hoc Conference Enabled）]サービス パラメータを使用します。
携帯電話からの + 文字のダイヤル	ユーザは携帯電話のデュアルトーン多重周波数（DTMF）を使用して + 記号をダイヤルし、国際番号用エスケープ文字を指定できます。 Cisco Unified Mobility 電話番号に + 文字を含むエンタープライズ IP フォンに携帯電話から発信するための、IVR の DTMF を使用した + のダイヤリングをサポートしません。 Cisco Unified Mobility 電話番号に + 文字を含むエンタープライズ IP フォンに携帯電話から発信するための、2 段階ダイヤリングの DTMF を使用した + のダイヤリングをサポートしません。

制約事項	説明
デスク フォンでのサイレントとリモート接続先へのダイレクトコール	デスク フォンでサイレント（DND）を有効にすると、デスク フォンをリモートで使用中の状態にすることはできず、次のシナリオではコールはアンカーされません。 • コールの拒否オプションでサイレントが有効になっている。 • デスク フォンの [サイレント（DND）] ソフトキーを押してサイレントが有効化されている。 ただし、呼出音オフのオプション付きで DND が有効になっている場合、コールはアンカーされます。
デュアルモード電話	**デュアルモード ハンドオフと発信者 ID** デュアルモード ハンドオフのハンドオフ DN 方法では、携帯電話ネットワークで発信者 ID が必要です。 モビリティ ソフトキーの方法では、発信者 ID は必要ありません。 **デュアルモード電話と CTI アプリケーション** デュアルモード電話が Wi-Fi エンタープライズ モードのときは、どの CTI アプリケーションもコントロールやモニタリングを行いません。 デュアルモード電話が WLAN の範囲外になると、WLAN の共有回線コールでのデュアルモード電話の [リモートで使用中（In Use Remote）]インジケータが消えます。 **デュアルモード電話と SIP 登録期間** デュアルモード電話では、Unified Communications Manager は、**[SIP ステーション キープアライブ間隔（SIP Station KeepAlive Interval）]** サービス パラメータが指定する値ではなく、電話機に関連付けられている SIP プロファイルの **[レジスタのタイムアウト値（秒）（Timer Register Expires (seconds)）]** フィールドの値を使用して、登録期間を決定します。 モバイル デバイスの標準 SIP プロファイルは、そのプロファイルの [レジスタのタイムアウト値（Time Register Expires）]フィールドで定義されているように登録期間を決定します。
携帯電話ネットワークからのエンタープライズ機能	携帯電話ネットワークからのエンタープライズ機能にはアウトオブバンド DTMF が必要です。 クラスタ間 DN を SIP トランク（クラスタ間トランクまたはゲートウェイのいずれか）を介した IP フォンのリモート接続先として使用する場合、IP フォンの設定の際に [DTMF 受信が必要（Require DTMF Reception）]チェックボックスをオンにします。 これにより、エンタープライズ機能アクセス通話中機能に不可欠な DTMF 番号がアウト オブ バンドで受信できます。

制約事項	説明
ゲートウェイとポート	モバイル音声アクセスではH.323 ゲートウェイと SIP VoIP ゲートウェイの両方がサポートされています。 T1 CAS、FXO、FXS、BRI では、Cisco Unified Mobility 機能はサポートされていません。 SNR（シングルナンバー リーチ）は、MGCP（Media Gateway Controlled Protocol）ではサポートされません。
Jabber デバイス	初期設定すると、Jabberデバイスは登録済みデバイスとしてカウントされます。 これらのデバイスは、[登録済みデバイスの最大数（Maximum Number of Registered Devices）] サービス パラメータで設定される、ノード内の登録済みデバイスの数を増やします。
ロケール	Cisco Unified Mobility 最大 9 つのロケールをサポートしています。 10 個以上のロケールがインストールされている場合、[使用可能なロケール（Available Locales）] ペインに表示されますが、[選択済みのロケール（Selected Locales）] のペインには 9 つまでしか保存できません。 Cisco Unified Mobility で 10 個以上のロケールの設定を試みた場合、次のメッセージが表示されます：「更新に失敗しました。（Update failed.） Check constraint (informix.cc_ivruserlocale_orderindex) failed.」というメッセージが表示されます。」
デスクトップのコール ピックアップの最大待機時間	ユーザがリモート接続先（スマートフォンまたは任意の他の電話のいずれか）から *81 DTMF コードを押してコールを保留にした場合、ユーザのデスク フォンには [復帰（Resume）] ソフトキーが表示されます。 ただし、デスク フォンではデスクトップのコール ピックアップ用のタイマーは適用されません。 エンド ユーザがコールに応答するまでの時間として設定したタイムアウトが過ぎ、コールがドロップされない場合でも **[復帰（Resume）]** キーは表示され続けます。 代わりに、ユーザはリモート電話でコールを切断する必要があります。これにより、デスク フォンはデスクトップ コール ピックアップのタイマーを適用し始めます （この設定を変更するには、**[エンド ユーザの設定]** ウィンドウの **[デスク ピックアップの最大待機時間]** フィールドを使用します）。
複数レベルの優先順位とプリエンプション	Cisco Unified Mobility マルチレベル優先順位およびプリエンプション（MLPP）とは連携しません。 コールが MLPP によってプリエンプション処理された場合は、そのコールに対する Cisco Unified Mobility 機能が無効になります。
オーバーラップ送信	オーバーラップ送信パターンはインテリジェント セッション制御機能ではサポートされません。
Q シグナリング	モビリティではQシグナリング（QSIG）はサポートされていません。

制約事項	説明
QSIG パス置換	QSIG パス置換はサポートされていません。
サービス パラメータ	エンタープライズ機能アクセス サービス パラメータは標準の電話とスマートフォンに適用されます。ただし、一般にスマートフォンはワンタッチ キーを使用して適切なコードを送信します。 Cisco Unified Mobility と共に使用するすべてのスマートフォンを、エンタープライズ機能アクセス用のデフォルトのコードまたはスマートフォンのドキュメンテーションで指定されているコードのいずれかを使用するように設定する必要があります。
セッション ハンドオフ	セッション ハンドオフ機能には次の制限が適用されます。 • セッション ハンドオフは携帯電話からデスク フォンに対してのみ行えます。 デスク フォンから携帯電話へのセッション ハンドオフの場合、現在のリモート接続先のピックアップ方法の規定により、携帯電話へのコールの送信を使用する必要があります。 • 音声通話のセッション ハンドオフのみサポートされています。
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。
SIP トランク	Cisco Unified Mobility 機能がサポートされるのは、一次群速度インターフェイス（PRI）公衆電話交換網（PSTN）接続のみです。 SIP トランクの場合、Cisco Unified Mobility は IOS ゲートウェイまたはクラスタ間トランクを介してサポートされます。
SIP URI とリモート接続先への直接コール	インテリジェント セッション制御機能は直接の URI ダイヤリングをサポートしていません。 したがって、SIP URI への発信はエンタープライズ番号にアンカーすることはできません。
Unified Communications Manager のパブリッシャ依存機能	クラスタ環境では、シングル ナンバー リーチを有効化または無効化するには、パブリッシャが到達可能である必要があります。 パブリッシャがアクティブに実行されていない場合、一部の機能が動作しない可能性があります。 パブリッシャノードが到達可能でない場合、モバイル音声アクセスは利用できません。モバイル音声アクセス用の IVR のプロンプトはパブリッシャでのみ保存されています。

制約事項	説明
ビデオ通話	Cisco Unified Mobility サービスはビデオ通話には拡張されません。 デスク フォンで受信したビデオ通話を携帯電話で取ることはできません。
モバイル ボイス アクセス（MVA）	Cisco 4000 シリーズ サービス統合型ルータは、音声 XML（VXML）をサポートしていません。そのため、これらのルータが Cisco Unified Communications Manager を備えたユニファイド コミュニケーション ゲートウェイとして機能するときには、モバイル音声アクセス（MVA）アプリケーションをサポートしません。

関連トピック

アドホック会議のサービス パラメータ （281 ページ）

Cisco Unified Mobility のトラブルシューティング

デスク フォンでコールを再開できない

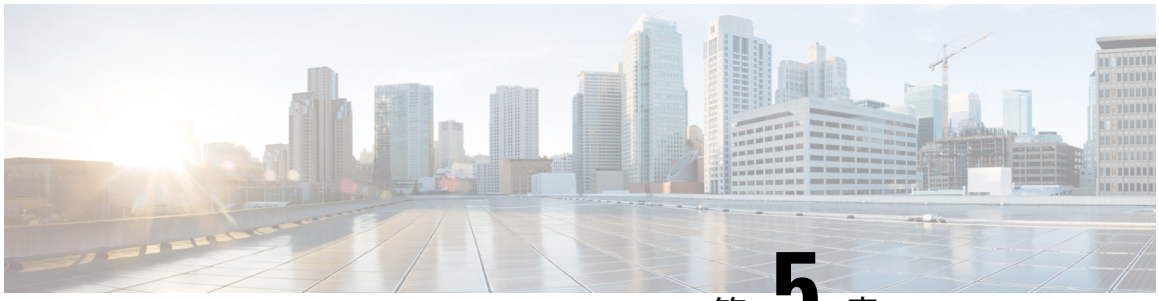
問題 リモート接続先（携帯電話）がスマートフォンではなく、この携帯電話へのコールが Cisco Unified Communications Manager を使用して固定されている場合、ユーザは、携帯電話を切り、デスク フォンに [**復帰（Resume）**] ソフトキーが表示されてコールを再開できることを期待します。 ユーザは、デスクトップ電話機でこのコールを再開できません。

考えられる原因 携帯電話が切れたときに、発呼側がビジー音、リオーダー音、または切断音を受信する場合、携帯電話のプロバイダーによってメディアが切断されなかった可能性があります。 プロバイダーから切断信号が送信されません。 この可能性を確認するため、発信側が 45 秒間待機するようにします。 この待機時間の経過後に、サービス プロバイダーはタイムアウトになり切断信号を送信します。この時点で、Cisco Unified Communications Manager はコールを再開するための [**復帰（Resume）**] ソフトキーを提供できます。

- 次のコマンドをゲートウェイに追加します。

```
voice call disc-pi-off
```

- Cisco CallManager サービスの場合は、[**アクティブ コールで PI との切断時にメディアを維持する（Retain Media on Disconnect with PI for Active Call）**] サービス パラメータを [**いいえ（False）**] に設定します。



第 5 章

デバイス モビリティ

デバイス モビリティの概要

デバイス モビリティにより、モバイル ユーザはサイト間をローミングし、ローカル サイトのサイト固有の設定を受け入れることができます。 この機能が設定されている場合、Cisco Unified Communications Manager はローミング デバイスの IP アドレスとデバイス モビリティ設定の IP サブネットを照合し、デバイスの物理的な位置を判別します。これにより、適切なデバイス プールを割り当てることができます。 この動的に割り当てられたデバイス プールからの設定によって、そのデバイスの [電話の設定（Phone Configuration）] の設定がオーバーライドされ、新しい電話のロケーションに対して音声品質とリソースの割り当てが適切なものになります。

ローミング モバイル デバイスの場合、この機能によりネットワーク リソースの使用効率が向上します。

- モバイル ユーザが別の場所に移動する際には、コール アドミッション制御（CAC）により、移動先のロケーションにとって適切な帯域幅割り当てでビデオ品質と音声品質を確保できます。
- モバイル ユーザが PSTN コールを発信すると、電話はローカル ゲートウェイにルーティングされます。 それ以外の場合、PSTN コールは最初に IP WAN 接続経由でホーム サイトにルーティングされ、その後ホーム サイトの PSTN ゲートウェイにルーティングされます。
- モバイル ユーザがホーム ロケーションにコールする場合、Cisco Unified Communications Manager は、リージョンに適切なコーデックを割り当てることができます。

サイト固有の設定

ローミング デバイスの場合、Cisco Unified Communications Manager は、動的に割り当てられたデバイス プールからの値で、デバイス設定の次のデバイス プール パラメータをオーバーライドします。

- 日時グループ
- リージョン
- ロケーション。
- ネットワークロケール
- SRST リファレンス
- 接続モニタ間隔
- 物理的な場所
- デバイスモビリティ グループ
- メディアリソースグループリスト

ネットワークが米国外のロケーションにまたがる場合、デバイス モビリティ グループを設定すると、電話ユーザのローミング先に関係なく、設定済みのダイヤルプランをユーザが使用できるようになります。 デバイスが移動中であっても、同じデバイス モビリティ グループに保持されている場合は、Cisco Unified Communications Manager は次のデバイス プール パラメータも上書きします。

- [AARグループ(AAR Group)]
- [AARコーリングサーチスペース(AAR Calling Search Space)]
- [デバイスコーリングサーチスペース(Device Calling Search Space)]

電話機がホーム ロケーションに戻ると、ローミング デバイス プールの関連付けが解除され、ホーム ロケーションから設定がダウンロードされ、デバイスがリセットされます。 デバイスはホーム ロケーションの設定を使用して登録されます。

（注） Cisco Unified Communications Manager は、必ず、電話レコード内の Communications Manager Group 設定を使用します。 デバイスは、ローミング中でも、必ず、そのホーム ロケーションの Cisco Unified Communications Manager サーバに登録されます。 電話のローミング中には、帯域幅割り当て、メディア リソース割り当て、地域の設定、AAR グループなどのネットワーク ロケーション設定だけが変更されます。

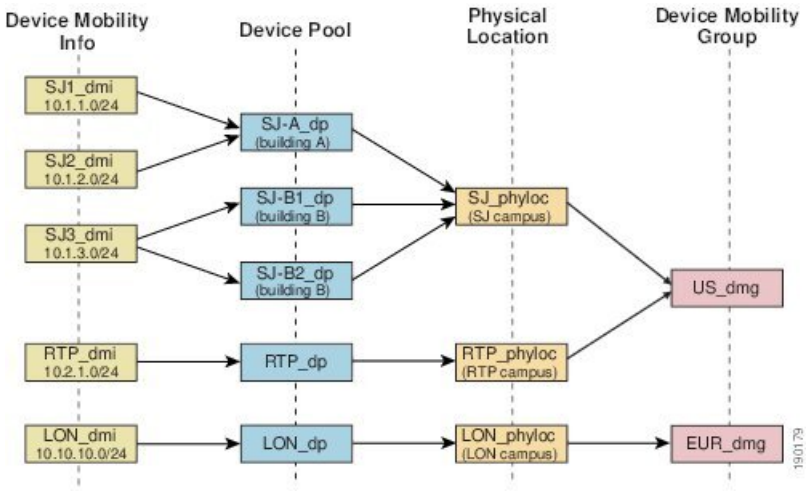
設定

この機能は、システム レベルとデバイス レベルの両方で有効にする必要があります。 システム レベルでは、この機能は次のコンポーネントを使用します。

- 物理ロケーション：デバイス プールの物理ロケーション。 適切なデバイス プールを割り当てる目的で、登録中にデバイス登録ロケーションが [デバイスモビリティ情報（Device Mobility Info）] のサブネットと照合されます。
- デバイス プール：メディア リソース、地域、および SRST 参照などのロケーション固有のデバイス設定。 ローミング デバイスの場合、デバイスの物理ロケーションに一致するデバイス プールが割り当てられます。
- デバイスモビリティ グループ：ダイヤリング パターンが類似しているサイトの論理グループ。 たとえば、世界規模のネットワークを所有する企業は、個々の国を表すグループを設定できます。 デバイス モビリティ グループ設定は、デバイスが同じ地理的エンティティ内を移動するかどうかを決定します。その主な目的は、ユーザが自分のダイヤルプランを維持できるようにすることです。
- デバイス モビリティ情報：この情報には、システムで提供されるローミング デバイスのサブネットと、このいずれかのサブネットに登録されるローミング デバイスに割り当て可能なデバイス プールが含まれます。

デバイスでこの機能を使用できるようにするには、デバイス レベルでこの機能をオンにする必要があります。

図 *1:* デバイス モビリティ関連の設定



デバイス プールの割り当て

この項では、デバイス モビリティが有効な際に、Unified Communications Manager がどうデバイス プールを割り当てるかについて説明します。 デバイスがローミングするかどうかに応じて、デバイスにはローカル サイトのデバイス プールが割り当てられるか、またはホーム サイトのデバイス プールが使用されます。

初期化の後に、デバイス モビリティ機能は次のプロセスに従って動作します。

1. モバイルとしてプロビジョニングされている IP フォンの電話デバイス レコードが作成され、電話がデバイス プールに割り当てられます。 電話機が Unified Communications Manager に登録され、登録プロセスの一環として IP アドレスが割り当てられます。
2. Unified Communications Manager は、デバイスの IP アドレスを、[デバイスモビリティ情報の設定（Device Mobility Info Configuration）] ウィンドウでデバイス モビリティ用に設定されたサブネットと比較します。 最適な組み合わせでは、IP サブネット マスクでの最大ビット数を使用します（最長一致ルール）。 たとえば、IP アドレス 9.9.8.2 は、サブネット 9.9.0.0/16 ではなくサブネット 9.9.8.0/24 と一致します。
3. 電話機レコードのデバイス プールが、一致するサブネットのデバイス プールと一致する場合、電話はホーム ロケーション内にあると見なされ、ホーム デバイス プールのパラメータを保持します。
4. 電話機レコードのデバイス プールが、一致するサブネットのデバイス プールと一致しない場合、電話はローミングであると見なされます。 次の表に、デバイス モビリティとシステム応答の考えられるシナリオについて説明します。

表 *5:* デバイス モビリティのシナリオ

シナリオ	システム応答
電話デバイス プールの物理ロケーション設定が、対応するサブネットに関連付けられているデバイス プールの物理ロケーション設定と一致する。 （注） 電話がサブネット間を移動した可能性がありますが、物理ロケーションと関連サービスは変更されていません。	システムは電話がローミング中であると見なさず、ホーム ロケーション デバイス プールの設定を使用します。
対応するサブネットに 1 つのデバイス プールが割り当てられており、サブネット デバイス プールがホーム ロケーション デバイス プールと異なり、物理ロケーションが異なる。	システムは電話がローミング中であると見なします。 一致するサブネットのデバイス プールのパラメータを使用して登録されます。
物理ロケーションが異なり、一致するサブネットに複数のデバイス プールが割り当てられている。	システムは電話がローミング中であると見なします。 新しいデバイス プールがラウンド ロビン ルールに従って割り当てられます。 ローミング デバイスがサブネットに登録されるたびに、使用可能なデバイス プールのセットの次のデバイス プールが割り当てられます。

シナリオ	システム応答
ホーム デバイス プールに対して物理ロケーションが定義されているが、対応するサブネットに関連付けられているデバイス プールには物理ロケーションが定義されていない。	物理ロケーションは変更されず、電話はホーム デバイス プールに登録されたままになります。
ホーム デバイス プールに対して定義されていない物理ロケーションが、一致するサブネットに関連付けられているデバイス プールに対して定義されている。	システムは、定義されている物理ロケーションに電話がローミング中であると見なし、一致するサブネットのデバイス プールのパラメータを使用して電話が登録されます。
サブネットが更新または削除される。	残りのサブネットを使用して、ローミングとデバイス プールの割り当てに関するルールが適用されます。

（注） デバイスの IP アドレスと一致するデバイス モビリティ情報エントリがない場合、デバイスはホーム ロケーションのデバイス プール設定を使用します。

デバイス モビリティ グループの動作の概要

デバイス モビリティ グループを使用して、デバイスが地理的実体内の別のロケーションに移動する時点を把握できます。これにより、ユーザは各自のダイヤル プランを使用できます。たとえば、米国と英国にそれぞれ個別のデバイス モビリティ グループを設定できます。 電話機が異なるモビリティ グループに移動した場合（たとえば、米国から英国へ）、Unified Communications Managerは、ローミング ロケーションではなく電話レコードにあるコーリング サーチ スペース、AAR グループ、および AAR CSS を使用します。

デバイスが同じモビリティ グループ内の別のロケーションに移動する場合（米国内のRichardsonから米国内のBoulderへ移動する場合など）、CSS情報はローミング デバイス プール設定から取得されます。 この方法では、ユーザが PSTN 接続先をダイヤルすると、ユーザはローカル ゲートウェイにアクセスすることになります。

次の表は、さまざまなシナリオでシステムにより使用されるデバイス プール パラメータについて説明します。

表 *6:* デバイス モビリティ グループのシナリオ

シナリオ	使用するパラメータ
ローミングデバイスが同一デバイス モビリティ グループ内の別のロケーションに移動する。	[ローミング用デバイスプール（Roaming Device Pool）]：[はい（yes）] [ロケーション（Location）]：ローミング用デバイス プールの設定 [地域（Region）]：ローミング用デバイス プールの設定 [メディア リソース グループリ スト（Media Resource Group List）]：ローミング用デバイス プールの設定 [デバイス CSS（Device CSS)]：ローミング用デバイス プールの設定（[デバイスモビリティ CSS（Device Mobility CSS）]） [AAR グループ（AAR Group）]：ローミング用デバイス プールの設定 [AAR CSS]：ローミング用デバイス プールの設定
ローミングデバイスが異なるデバイスモビリティ グループ内の別のロケーションに移動する。	[ローミング用デバイスプール（Roaming Device Pool）]：[はい（yes）] [ロケーション（Location）]：ローミング用デバイス プールの設定 [地域（Region）]：ローミング用デバイス プールの設定 [メディア リソース グループリ スト（Media Resource Group List）]：ローミング用デバイス プールの設定 [デバイス CSS（Device CSS）]：ホーム ロケーションの設定 [AARグループ（AAR Group）]：ホーム ロケーションの設定 [AAR CSS]：ホーム ロケーションの設定
デバイスが移動したが、デバイス モビリティ グループは、ホーム デバイス プールにも、ローミング用デバイスプールにも定義されていない。	デバイスは移動中のため、ローミング用デバイス プールの設定（[デバイス モビリティ コーリング サーチ スペース（Device Mobility Calling Search Space）]、[AAR コーリング サーチ スペース（AAR Calling Search Space）]、および [AAR グループ（AAR Group）] など）を取得します。

デバイス モビリティの前提条件

- デバイス モビリティを使用するために、電話機にはダイナミック IP アドレスが必要です。スタティック IP アドレスが設定されている電話がローミングする場合、Unified Communications Manager はそのホーム ロケーションの設定を使用します。
- デバイス モビリティ機能を使用するには、サイト固有の設定を使用してデバイス プールを設定する必要があります。 この章では、デバイス モビリティに関連するデバイス プール設定のみを説明します。 デバイス プールの設定の詳細については、Cisco Unified

Communications Manager システム設定ガイド の「デバイス プールの設定」の章を参照してください。

- Cisco Database Layer Monitor サービスを、Cisco CallManager サービスと同じノードで実行しておく必要があります
- Cisco TFTP サービスを、クラスタの少なくとも 1 つのノードで実行しておく必要があります
- 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）。
- SCCP または SIP のいずれかを実行している電話。

デバイス モビリティの設定タスク フロー

デバイス モビリティを設定するには、次のタスクをすべて行います。

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 レベルでデバイス モビリティを有効にするには、次のいずれかのタスクを実行します。 • クラスタ全体でのデバイス モビリティの有効化 （66 ページ） • 個々のデバイスのデバイス モビリティの有効化 （66 ページ）	clusterwide サービス テンプレートまたは、**[電話の設定（Phone Configuration）]** ウィンドウの個別のデバイスでデバイス サポートを有効にします。
ステップ 2	物理的な場所の設定 （67 ページ）	デバイス プールに割り当てる物理ロケーションを設定します。
ステップ 3	デバイス モビリティ グループの設定 （67 ページ）	デバイス モビリティ グループは、ダイヤリング パターンが類似しているサイトの論理グループです。
ステップ 4	デバイス モビリティのデバイス プールの設定 （68 ページ）	物理ロケーション、デバイスモビリティ グループ、およびその他のデバイス モビリティ関連情報を、デバイス モビリティのために使用されるデバイス プールに割り当てます。
ステップ 5	デバイス モビリティ情報の設定 （69 ページ）	ローミング デバイスの登録場所として可能な IP サブネットと、これらのローミング デバイスに割り当てることができるデバイス プールを割り当てます。

クラスタ全体でのデバイス モビリティの有効化

次の手順を使用して、電話機の**[電話機の設定（Phone Configuration）]**で設定が上書きされている場合を除き、クラスタ全体のすべての電話でデフォルトのデバイスモビリティ設定を**オン**に設定するサービス パラメータを設定します。

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）]**。

ステップ 2 [サーバ（Server）]ドロップダウン リストで、Cisco CallManager サービスを実行している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（Cisco CallManager Service）]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 - 電話機）（Clusterwide Parameters (Device - Phone)）]で[デバイスモビリティモード（Device Mobility Mode）]サービスパラメータを[オン（On）]に設定します。

ステップ 5 **[保存]** をクリックします。

すでに登録済みのデバイスの場合、この新しい設定を有効にするには **Cisco CallManager** サービスを再起動する必要があります。

次のタスク

個々のデバイスのデバイスモビリティ設定を行うには、個々のデバイスのデバイスモビリティの有効化 （66 ページ）を参照してください。

それ以外の場合は、デバイス モビリティに対応するシステムの設定を開始できます。 物理的な場所の設定 （67 ページ） に進みます。

個々のデバイスのデバイス モビリティの有効化

個々のデバイスのデバイス モビリティを有効にするには、次の手順を使用します。 この設定は、クラスタ全体のサービスパラメータ [デバイスモビリティ モード（Device Mobility Mode）] をオーバーライドします。

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）] > [電話（Phone）]**。

ステップ 2 [検索（Find）] をクリックして、設定するデバイスを選択します。

ステップ 3 **[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、次のいずれかを選択します。

- [オン（On）]：このデバイスでデバイス モビリティが有効になります。
- [オフ（Off）]：このデバイスでデバイス モビリティが無効になります。
- [デフォルト（Default）]：デバイスは、クラスタ全体のサービス パラメータ [デバイス モビリティ モード（Device Mobility Mode）] の設定を使用します。 これがデフォルト設定です。

ステップ 4 **[保存（Save）]** をクリックします。

物理的な場所の設定

デバイス プールに割り当てる物理ロケーションを設定するには、次の手順を使用します。 デバイス モビリティでは、デバイス登録のロケーションを使用して適切なデバイス プールを割り当てます。

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）]** > **[物理ロケーション（Physical Location）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 ロケーションの名前を入力します。

ステップ 4 ロケーションの説明を入力します。

ステップ 5 **[保存（Save）]** をクリックします。

デバイス モビリティ グループの設定

次の手順を使用して、デバイス モビリティ グループを設定します。これは、同様のダイヤル パターンを使用したサイトの論理的なグルーピングです。 たとえば、世界規模のネットワークを所有する企業は、個々の国を表すデバイス モビリティ グループを設定できます。

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。**[システム（System）]** > **[デバイス モビリティ（Device Mobility）]** > **[デバイス モビリティ グループ（Device Mobility Group）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 デバイス モビリティ グループの**名前**を入力します。

ステップ 4 デバイス モビリティ グループの**説明**を入力します。

ステップ 5 **[保存（Save）]** をクリックします。

デバイス モビリティのデバイス プールの設定

デバイス モビリティ用に設定したパラメータを使用してデバイス プールを設定するには、次の手順を使用します。

手順

ステップ 1 [Cisco Unified CM 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 [ローミングに合わせて変化する設定（Roaming Sensitive Settings）] で、以前のデバイス モビリティ タスクで設定したパラメータを割り当てます。

- **[物理ロケーション（Physical Location）]**：ドロップダウン リストから、このデバイス プールに設定する物理ロケーションを選択します。 デバイス モビリティは、ローミング デバイスにデバイス プールを割り当てるときにこのロケーションを使用します。
- **[デバイス モビリティ グループ（Device Mobility Group）]**：ドロップダウン リストから、このデバイス プールに設定するデバイス モビリティ グループを選択します。

ステップ 4 [デバイス モビリティ関連情報（Device Mobility Related Information）] で次のデバイス モビリティ関連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、オンライン ヘルプを参照してください。

- [デバイス モビリティ コーリング サーチ スペース（Device Mobility Calling Search Space）]：このデバイス プールを使用するローミング デバイスが使用する CSS を選択します。
- [AAR コーリング サーチ スペース（AAR Calling Search Space）]：自動代替ルーティング（AAR）の実行時にデバイスが使用するコーリング サーチ スペースを選択します。
- [AARグループ（AAR Group）]：AAR が設定されている場合に、このデバイスの AAR グループを選択します。
- **[発呼側トランスフォーメーション CSS（Calling Party Transformation CSS）]**：このデバイス プールを使用するローミング デバイスの発信側トランスフォーメーション CSS を選択します。

（注）
- **[発呼側トランスフォーメーション CSS（Calling Party Transformation CSS）]** は、**[電話の設定（Phone Configuration）]** ウィンドウの **[デバイス プールの発呼側トランスフォーメーション CSS を使用（Use Device Pool Calling Party Transformation CSS）]** チェックボックスがオフの場合でも、ローミング デバイスのデバイス レベルの設定をオーバーライドします。
- [着信側トランスフォーメーション CSS（Called Party Transformation CSS）] 設定は、ローミング デバイスではなくゲートウェイに適用されます。

ステップ 5 [デバイス プールの設定（Device Pool 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。

デバイス モビリティ情報の設定

デバイスモビリティ情報を設定するには、次の手順に従います。この情報は、ローミングデバイスの登録先として可能な IP サブネットと、ローミング デバイスに割り当てることができる対応するデバイス プールを表します。

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）]**>**[デバイス モビリティ（Device Mobility）]**>**[デバイス モビリティ情報（Device Mobility Info）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 デバイス モビリティ情報の**名前**を入力します。

ステップ 4 ローミング デバイス登録の IP サブネットの詳細を入力します。
- モバイル デバイスに IPv4 アドレスを使用している場合は、IPv4 サブネットの詳細を入力します。
- モバイル デバイスに IPv6 アドレスを使用している場合は、IPv6 サブネットの詳細を入力します。

ステップ 5 いずれかのサブネットに登録するローミング デバイスに割り当てるデバイス プールを選択します。 矢印を使用して、適切なデバイス プールを [選択されたデバイス プール（Selected Device Pools）] リスト ボックスから [使用可能なデバイス プール（Available Device Pools）] リスト ボックスに移動します。

ステップ 6 **[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、オンライン ヘルプを参照してください。

ローミング デバイス プールのパラメータの表示

次の手順を使用して、デバイスの現在のデバイス モビリティ設定を表示および確認します。

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。**[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 検索条件を入力して[検索（Search）]をクリックし、デバイス モビリティ モードが有効なデバイスを見つけます。

ステップ 3 [デバイス モビリティ モード（Device Mobility Mode）]の横の [現在のデバイス モビリティの設定を表示する（View Current Device Mobility Settings）]をクリックします。

ローミング デバイス プールの設定が表示されます。 デバイスがローミングしない場合には、ホームの場所の設定が表示されます。

デバイス モビリティの連携動作

表 *7*: デバイス モビリティの連携動作

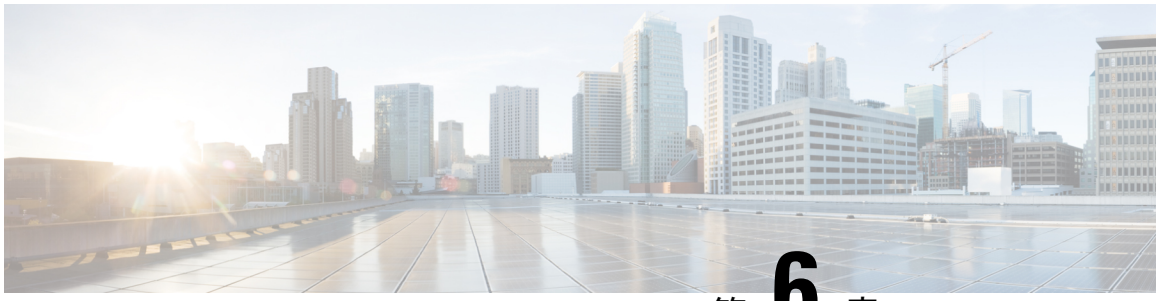
機能	データのやり取り
発信側の正規化	発信側の正規化は、一部の電話機のダイヤリング機能を強化し、コールが複数の地理的場所にルーティングされる場合のコールバック機能を改善します。つまり、この機能を使用すれば、着信側が電話機の通話履歴ディレクトリ内の電話番号を変更しなくてもコールバックできます。 加えて、発信側の正規化を使用すれば、電話番号のグローバル化とローカル化が可能になるため、正しい発信者番号が電話機に表示されます。

機能	データのやり取り
ローミング	デバイスが同一のデバイス モビリティ グループ内をローミングしているとき、Unified Communications Manager はローカル ゲートウェイへの到達にデバイス モビリティ CSS を使用します。 ユーザが電話で不在転送（CFA）を設定し、CFA CSS が [なし（None）] に設定され、CFA CSS アクティベーション ポリシーが [デバイス/回線 CSS のアクティブ化を使用（With Activating Device/Line CSS）] に設定されている場合は、デバイスの場所に応じて、次のように動作が異なります。 • デバイスがホームの場所に設置されている場合は、デバイス CSS と回線 CSS が CFA CSS として使用されます。 • デバイスが同じデバイス モビリティ グループ内をローミングしている場合は、ローミング デバイス プールからのデバイス モビリティ CSS と回線 CSS が CFA CSS として使用されます。 • デバイスが別のデバイス モビリティ グループ内をローミングしている場合は、デバイス CSS と回線 CSS が CFA CSS として使用されます。

デバイス モビリティの制約事項

表 *8:* デバイス モビリティの制約事項

制約事項	説明
IP アドレス（IP Address）	デバイス モビリティ機能は、Unified Communications Manager に登録されているデバイスの IPv4 アドレスまたは IPv6 アドレスによって異なります。 • デバイス モビリティを使用するために、電話にはダイナミック IPv4 アドレスまたは IPv6 アドレスが必要です。 • ネットワーク アドレス変換（NAT）またはポート アドレス変換（PAT）を使用してデバイスに IP アドレスが割り当てられている場合、登録時に提供する IP アドレスは、デバイスの実際の IP アドレスに一致しない可能性があります。 • Cisco IP 電話が IPv4 のみのスタックまたは IPv6 のみのスタックをサポートする場合、定義された IP アドレッシング モードの設定に基づいて、電話は IPv4 または IPv6 デバイス モビリティ情報のいずれかと再度関連付けられます。 たとえば、電話が IPv6 設定を使用して定義されているが一致するデバイス モビリティ情報（IPv6 サブネットおよびマスク サイズ）がない場合、IPv4 と関連付けられます。 一致する IPv6 デバイス モビリティ情報を追加すると、電話は IPv6 デバイス モビリティ情報と再度関連付けられます。



第 6 章

拡張と接続

????? の概要

拡張と接続 機能により、管理者は、あらゆるエンドポイントと相互作用するUnified Communications Manager（UC）コンピュータテレフォニーインテグレーション（CTI）アプリケーションを導入できます。 拡張と接続 により、ユーザは、位置を問わず、どのデバイスからでも UC アプリケーションにアクセスできます。

Unified Communications Manager の 拡張と接続 機能には、次の UC 機能が含まれています。

- 着信エンタープライズ コールの受信
- 発信
- 切断
- 保留と復帰
- リダイレクトと転送
- すべてのコールの転送
- 話中転送
- 無応答時転送
- 取り込み中
- デュアルトーン多重周波数（DTMF）の再生（アウトオブバンドおよびインバンド）
- 打診転送、会議

- リモート接続先の追加、編集、および削除
- リモート接続先の「アクティブ」または「非アクティブ」の設定
- 永続的接続（Persistent Connection）
- ウィスパー アナウンスメントの再生

????? の前提条件

- Cisco Jabber リリース 9.1(1) 以降
- Cisco Unified Workspace License（CUWL）Standard、CUWL Professional、または Cisco User Connect License（UCL）- Enhanced

拡張と接続 の設定タスク フロー

この項では、Unified Communications Manager ユーザに 拡張と接続 機能をプロビジョニングするために必要な手順について説明します。 Windows 版 Cisco Jabber ユーザの 拡張と接続 のプロビジョニングについては、の『Windows 版 Cisco Jabber インストールおよび設定ガイド』を参照してください。

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	ユーザ アカウントの設定 （75 ページ）	ユーザのモビリティを有効にして、CTI リモート デバイスを使用できるようにします。 CTI デバイスは、Cisco UC アプリケーションと連動するオフクラスタ電話です。
ステップ 2	ユーザ権限の追加 （75 ページ）	アクセス制御グループのアクセス許可を追加します。
ステップ 3	CTI リモート デバイスの作成 （76 ページ）	ユーザが Cisco UC アプリケーションで使用できるオフクラスタ電話を設定します。
ステップ 4	デバイスへの電話番号の追加 （77 ページ）	CTI リモート デバイスに電話番号を関連付けます。

	コマンドまたはアクション	目的
ステップ 5	リモート接続先の追加 （78 ページ）	ユーザが所有する他の電話を表す数値アドレスまたはディレクトリ URI を追加します。
ステップ 6	リモート接続先の確認 （79 ページ）	リモート接続先が正常にユーザに追加されたかどうかを確認します。
ステップ 7	ユーザとデバイスの関連付け （80 ページ）	CTI リモート デバイスにエンド ユーザ アカウントを関連付けます。

ユーザ アカウントの設定

次の手順を使用して Unified Communications Manager に新規または既存のユーザを設定し、ユーザ モビリティを有効にして CTI リモート デバイスを使用できるようにする必要があります。ユーザのモビリティが有効でない場合、そのユーザを CTI リモート デバイスの所有者として割り当てることはできません。

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 次のいずれかを実行します。

- 新しいユーザを設定するには、**[新規追加（Add New）]** をクリックします。
- **[ユーザを次の条件で検索（Find Users Where）]** フィールドを使用してフィルタを適用し、**[検索（Find）]** をクリックしてユーザのリストを取得します。

（注） LDAP 統合またはローカル設定から、新しいユーザ アカウントを追加できます。

ステップ 3 **[モビリティ情報（Mobility Information）]** セクションを探します。

ステップ 4 **[モビリティの有効化（Enable Mobility）]** 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。

ユーザ権限の追加

エンド ユーザを Unified Communications Manager でアクティブにしてから、アクセス制御グループ権限を追加します。

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 [**ユーザを次の条件で検索（Find User where**）] フィールドで適切なフィルタを指定した後、[**検索（Find**）] を選択してユーザのリストを取得します。

ステップ 3 ユーザを一覧から選択します。

ステップ 4 [**権限情報（Permissions Information**）] セクションを探します。

ステップ 5 [アクセス コントロール グループに追加（Add to Access Control Group）]をクリックします。

[アクセス コントロール グループの検索と一覧表示（Find and List Access Control Groups）] ウィンドウが表示されます。

ステップ 6 **[検索(Find)]** をクリックします。

標準ユーザのアクセス コントロール グループのリストが表示されます。

ステップ 7 次の権限の隣にあるチェックボックスをオンにします。

- [標準 CCM エンド ユーザ（Standard CCM End-Users）]
- [標準CTIを有効にする（Standard CTI Enabled）]

ステップ 8 **[選択項目の追加(Add Selected)]** をクリックします。

ステップ 9 **[保存（Save）]** をクリックします。

CTI リモート デバイスの作成

CTI リモートデバイスを作成するには、次の手順を使用します。ユーザが Cisco UC アプリケーションで使用できるオフクラスタ電話を表すデバイス タイプです。 デバイス タイプには、1 つ以上の回線（電話番号）と 1 つ以上のリモート接続先が設定されます。

Unified Communications Manager 公衆電話交換網（PSTN）の電話や構内交換機（PBX）などのデバイスへのコールを制御するための 拡張と接続 機能を提供します。

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）] > [電話（Phone）]**。

ステップ 2 [新規追加] 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）]** を選択します。続いて **[次へ（Next）]** をクリックします。

ステップ 4 [オーナーのユーザ ID（Owner User ID）]ドロップダウン リストから対象のユーザ ID を選択します。

（注） [オーナーのユーザ ID（Owner User ID）]ドロップダウン リストには、モビリティの有効化が利用可能なユーザのみが表示されます。

Unified Communications Manager は、**[デバイス名（Device Name）]** フィールドにユーザ ID と CTIRD 接頭辞（*CTRIDusername* など）を入力します。

ステップ 5 必要に応じて、[デバイス名（Device Name）]フィールドのデフォルト値を編集します。

ステップ 6 [説明（Description）]フィールドに分かりやすい説明を入力します。

（注） Cisco Jabber によって、デバイスの説明がユーザに表示されます。 Cisco Jabber ユーザが同一モデルのデバイスを複数持っている場合、Unified Communications Manager の説明によってそれらを区別できます。

ステップ 7 **[プロトコル固有情報（Protocol Specific Information）]** セクションの **[再ルーティング 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、適切なオプションを選択してください。

[再ルーティング コーリング サーチ スペース（Rerouting Calling Search Space）]ドロップダウン リストは、再ルーティング用のコーリング サーチ スペースを定義します。これにより、ユーザは CTI リモート デバイスからコールを発信および受信できるようになります。

ステップ 8 [電話の設定（Phone Configuration）]ウィンドウの残りのフィールドを設定します。 フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 9 **[保存]** をクリックします。

電話番号を関連付け、リモート接続先を追加するためのフィールドが、[電話の設定（Phone Configuration）]ウィンドウに表示されます。

デバイスへの電話番号の追加

電話番号（DN）は、CTI リモート デバイスで回線として設定される数値アドレスです。 通常、DN はユーザのプライマリ電話番号を表します（2000 または + 1 408 200 2000 など）。

（注）
- コーリング サーチ スペース（CSS）と DN のパーティションは、デバイスで必須です。
- CTI リモート デバイスは、自身の DN をブロックしてはいけません。 CSS は、CTIRD デバイスが自身の DN に到達するために重要です。

CTI リモート デバイスに電話番号を追加するには、次の手順に従います。

手順

ステップ 1 **[電話の設定（Phone Configuration）]** ウィンドウで、**[割り当て情報（Association Information）]** セクションに移動します。

ステップ 2 [新規DNを追加（Add a new DN）]をクリックします。

ステップ 3 **[電話番号（Directory Number）]** フィールドで、電話番号を指定します。

ステップ 4 その他の必須フィールドすべてを設定します。 フィールドと設定オプションの詳細については、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。

リモート接続先の追加

リモート通知先を追加するには、次の手順を使用します。ユーザが所有する他の電話機（自宅のオフィス回線やその他の PBX 電話など）を表す数値アドレスまたはディレクトリ URI。 リモート接続先が、オフクラスタ デバイスである可能性があります。 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。 デフォルトで、デバイスあたり 4 つのリモート接続先がサポートされます。 **[エンド ユーザ設定（End User Configuration）]** ウィンドウで、デバイスあたり最大数 10 個のリモート接続先に設定できます。

（注） どのリモート接続先で Jabber クライアントが有効に設定されているかは、Cisco Unified Communications Manager Administration インターフェイスの **[電話機の設定（Phone Configuration）]** ウィンドウで確認できます。

（注） Unified Communications Manager のユーザは、Cisco Jabber インターフェイスを使用してリモート接続先を追加できます。 詳細については、『Windows 版 Cisco Jabber インストールおよび設定ガイド』を参照してください。

- Unified Communications Manager は、Cisco Jabber ユーザがクライアント インターフェイスで追加したリモート接続先にコールをルートできるかどうかを自動的に確認します。
- Unified Communications Manager は、Cisco Unified Communications Manager の管理インターフェイスを介して追加されたリモート接続先にコールをルーティングできるかどうかは確認しません。

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 [電話を次の条件で検索（Find Phone where）]フィールドで適切なフィルタを指定した後、[検索（Find）]をクリックして電話のリストを取得します。

ステップ 3 一覧から CTI リモート デバイスを選択します。

ステップ 4 [**関連付けられたリモート接続先（Associated Remote Destinations**）] セクションを探します。

ステップ 5 [**新規リモート接続先の追加（Add a New Remote Destination**）] を選択します。

ステップ 6 [**接続先番号（Destination Number**）] フィールドに接続先番号を入力します。

Cisco Jabber クライアントでリモート接続先を使用するには、接続先名を *JabberRD* として設定する必要があります。

ステップ 7 [**リモート接続先情報（Remote Destination Information**）] ウィンドウの残りのフィールドを設定します。 フィールドと設定オプションの詳細については、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。

リモート接続先の確認

リモート接続先がユーザに正常に追加されたかどうかを確認するには、次の手順を実行します。

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）] > [電話（Phone）]**。

ステップ 2 [電話を次の条件で検索（Find Phone where）]フィールドで適切なフィルタを指定した後、[検索（Find）]をクリックして電話のリストを取得します。

ステップ 3 一覧から CTI リモート デバイスを選択します。

ステップ 4 [関連付けられたリモート接続先（Associated Remote Destinations）] セクションを見つけ、リモート接続先が使用可能であることを確認します。

ステップ 5 **[設定の適用（Apply Config）]** をクリックします。

（注） [**電話の設定（Phone Configuration**）] ウィンドウの [デバイス情報（Device Information）] セクションに、リモート接続先が Cisco Jabber でアクティブになっているか、または制御されているかが表示されます。

ユーザとデバイスの関連付け

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。**[ユーザ管理（User Management）] > [エンド ユーザ（End User）]**。

ステップ 2 [ユーザを次の条件で検索（Find Users Where）]フィールドで適切なフィルタを指定した後、[検索（Find）]をクリックしてユーザのリストを取得します。

ステップ 3 ユーザを一覧から選択します。

ステップ 4 [デバイス情報（Device Information）]セクションを探します。

ステップ 5 [デバイスの割り当て（Device Association）]をクリックします。

ステップ 6 適切な CTI リモート デバイスを探して選択します。

ステップ 7 関連付けを完了するには、[選択/変更の保存（Save Selected/Changes）]をクリックします。

ステップ 8 **[関連リンク（Related Links）]** ドロップダウン リストから **[ユーザの設定に戻る（Back to User）]** を選択し、**[検索（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（CTIRD）のコール フロー

Unified Communications Manager ユーザが CTI リモート デバイスとして追加されると、発信側番号と請求先番号の分離機能がサポートされます。 各 CTI リモート デバイスは、ユーザの電話番号（DN）（2000 など）と、オフクラスタ デバイス（番号が +1 408 111 1111 の PBX 電話など）を表すリモート接続先を使用して設定されます。

PSTN ネットワークから CTIRD 回線へのコールが開始されると、Unified Communications Manager は FROM ヘッダーと PAID ヘッダーの情報を検索します。 FROM ヘッダーには外部プレゼンテーションの名前と番号が含まれ、PAID にはユーザの ID（ユーザの DN または DDI）が含まれています。

FROM ヘッダーと PAID ヘッダーに異なる番号が指定され、SIP プロファイルで **[外部プレゼンテーション名と番号の有効化（Enable External Presentation Name and Number）]** チェックボックスがオンであり、**[外部プレゼンテーション名と番号の表示（Display External Presentation Name and Number）]** の値が [はい（*True*）] に設定されている場合、Unified Communications Manager は、着信側デバイスに FROM ヘッダーの情報を表示します。 同様に、1 つのオプションが無効の場合、Unified Communications Manager は着信側デバイスに PAID ヘッダー情報を表示します。

同様に発信コールのシナリオでは、ユーザは、電話番号設定ページで外部プレゼンテーションの名前と番号を使用して設定されているリモート接続先（CTIRD 回線）から、SIP プロファイルで [外部プレゼンテーションの名前と番号を有効化（Enable External Presentation Name and

Number）] が設定されている SIP トランク経由で PSTN にコールします。 次に、Unified Communications Manager は [電話番号の設定（Directory Number Configuration）] ページで設定された外部プレゼンテーション情報を、発信 SIP メッセージの FROM ヘッダーで送信し、この情報が着信側デバイスに表示されます。

[**外部プレゼンテーション名と番号の有効化（Enable External Presentation Name and Number**）] チェックボックスがオフになっている場合、Unified Communications Manager は、電話番号情報を FROM および PAID で送信し、着信側デバイスと、X-Cisco-Presentation ヘッダーの設定済み外部プレゼンテーション情報に表示されます。

[**匿名の外部プレゼンテーション（Anonymous External Presentation**）] チェックボックスをオンにすると、設定済みの外部プレゼンテーション名と番号が、着信側デバイスで各フィールドおよび匿名として表示されている外部プレゼンテーションから削除されます。

外部プレゼンテーション情報の設定の詳細については、Cisco Unified Communications Manager システム設定ガイド の「電話番号の設定」の章を参照してください。

????? 連携動作

表 *9*：拡張と接続 連携動作

機能	データのやり取り
Directory URI ダイヤリング	Directory URI を CTI リモート デバイスの DN、リモート接続先、またはその両方として設定します。
Unified Mobility	Extend and Support は、Cisco Unified IP 電話 とリモート接続先の間のアクティブ コールの移動をサポートしません。 Unified Mobility と 拡張と接続 の両方の機能が必要な場合は、リモート デバイス プロファイルと CTI リモート デバイスに同じリモート接続先を設定できますが、それは両方のタイプのオーナー ID が同じ場合です。 この設定では、Cisco Mobility 機能と 拡張と接続 を同時に使用できます。 両方のデバイス タイプで同じリモート接続先を設定する機能は、Cisco Unified Communications Manager リリース 10.0(1) 以降を使用してサポートされます。 Cisco Dual-mode for iPhone、Cisco Dual-mode for Android、Carrier-integrated Mobile のデバイス タイプでは、Cisco 拡張と接続 機能で使用するりモード接続先を設定しないでください。 同じリモート接続先アドレスを区別するためにプレフィックスを使用しないでください。 たとえば、91-4085555555 と +1-4085555555 は同じ番号として処理します。

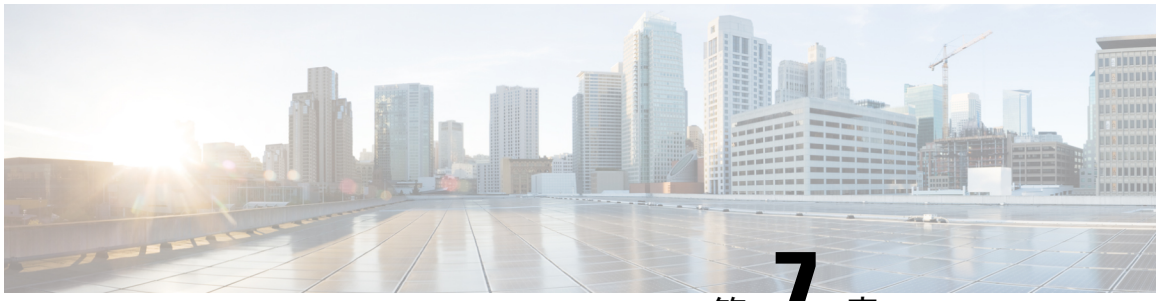
機能	データのやり取り
ハント リスト	拡張と接続 機能を使用すれば、以下の条件下で、リモート接続先の電話機でハント コールを受信できます。 • ユーザが Cisco Unified IP Phone を所有している。 • Cisco Unified IP Phone を使用してハント コールに応答できる（ログイン/HLog）。 • Cisco Jabber が 拡張と接続 モードで実行している。
発信者 ID 情報	• 発信者 ID 情報（名前と電話番号）は、Jabber クライアントに表示されます。 • 使用しているキャリアとトランクの設定によっては、この情報がデバイスに表示されることもあります。 • リモート接続先への発信 Dial via Office コールには、名前として *Voice Connect* が、番号としてトランク DID が表示されます。 • トランク DID は、Unified CM のトランク パターン、ルート パターン、またはCisco ゲートウェイで設定します。 この設定は、キャリアによって割り当てられることもあります。 トランク DID が設定されていない場合は、番号フィールドが空白として表示されます。 • 必要な通話相手への発信コールでは、Unified Communications Manager で設定されている CTI リモートデバイスの表示名と電話番号（DN）が表示されます。 • 着信側にリモート接続先番号が表示されることはありません。

????? の制約事項

表 *10* : 拡張と接続 の制約事項

制約事項	説明
リモート接続先の最大数	CTI リモート デバイスあたり 10 個までリモート接続先を設定できます。 （注） デフォルトで、デバイスあたり 4 つのリモート接続先がサポートされます。 デバイスごとにリモート接続先の最大数を 10 個まで設定できます。

制約事項	説明
オフクラスタデバイス	• リモート接続先番号は、オフクラスタ デバイスを表している必要があります。 • リモート接続先は、オフクラスタ URI にすることができます。
ディレクトリ番号	ディレクトリ番号をリモート接続先番号として設定することはできません。
Cisco Jabber	Cisco Jabber を使用して設定されたリモート接続先を保存する前に、設定されたダイヤル プランによってリモート接続先にルーティング可能かどうかを確認します。
アプリケーション ダイヤル ルール	アプリケーション ダイヤル ルールは、Cisco Unified Communications Manager Administration インターフェイスと Cisco Jabber を通じて CTI リモート デバイスに設定された、すべてのリモート接続先に適用されます。 （注） アプリケーション ダイヤル ルールでサポートするように設定された番号形式（nn-nnn-nnnn、E.164、その両方など）をエンド ユーザに通知します。
リモート接続先番号	リモート接続先番号は、クラスタ内で一意にする必要があります。 （注） 複数のユーザーが同じリモート接続先番号を使用することはできません。
リモート接続先検証	• リモート接続先番号は、CTI リモート デバイスの再ルーティング コーリング サーチ スペースを使用して検証されます。 • Cisco Unified Communications Manager Administration インターフェイスと AXL インターフェイスを使用して設定されたリモート接続先は検証されません。
転送制限を問い合わせる	CTI リモートデバイスから内部 IP 電話機または別の拡張接続対応デバイスへのコンサルト転送が開始されると、転送を開始した CTI リモートデバイスに関連付けられたリモート接続先でリングバックは聞こえません。
未登録時の不在転送	拡張と接続 は、未登録内線の不在転送または未登録外線の不在転送をサポートしていません。
発呼側番号によるネクストホップのルート	[発信側番号によるルート ネクスト ホップ] オプションが有効になっている場合、拡張および接続では変換パターンがサポートされません。



第 7 章

リモート ワーカー緊急コール

リモート ワーカー緊急コールの概要

リモート ワーカー緊急コール機能により、顧客はリモート バーチャル プライベート ネットワーク（VPN）接続を使用した信頼性の高い緊急コール サポートをリモート ワーカーに提供できます。 オフプレミス ユーザからの緊急コールは公安応答局（PSAP）にルーティングされ、各コールではユーザが提供するロケーション情報が配信されます。

この機能を使用するには、デバイス登録が中断されるたびにリモート ワーカーがロケーションを確認または更新する必要があります。 最初に、オフプレミス向けデバイス（顧客のネットワークにリモート接続するデバイス）にカスタマイズ可能な免責事項通知が表示されます。この通知は、正しいロケーション情報を提供するようユーザに指示します。 ロケーション情報が提供されると、指定したデバイスに現在関連付けられているオフプレミス ロケーションが表示されます。 ユーザは現在のロケーションを確認するか、または保存されている別のロケーションをデバイスのディスプレイで選択します。新規ロケーションの場合、ユーザに対し、新規ロケーションを作成するための Cisco Emergency Responder Off-Premises User Web ページが表示されます。

管理者はこのプロセスを完了する前に、デバイスがコールできる接続先を、設定されている 1 つの接続先だけに制限できます。 この操作により、デバイスのユーザは免責事項に同意し、現在のロケーション情報を提供した後で、デバイスを通常どおり使用できるようになります。

リモート ワーカー緊急コールの前提条件

リモート ワーカー緊急コール機能を設定する前に、Cisco Emergency Responder で Intrado（サードパーティ製アプリケーション）を設定する必要があります。 Cisco Emergency Responder での Intrado の設定の詳細については、Cisco Emergency Responder Administration Guide を参照してください。

リモート ワーカー緊急コールの設定タスク 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	リモート ワーカーとしてのユーザの設定 （86 ページ）	構外デバイスをデバイスの所有者と関連付けます。
ステップ 2	緊急コールの代替ルーティングの指定（87 ページ）	これらのパラメータは、コーリング サーチ スペースと接続先番号を指定します。これらは、ユーザがロケーションを設定しないことを選択した、登録済みの構外デバイスから発信されたコールのルーティングを制限するために使用されます。 これらのパラメータが設定されていない場合、コールは通常どおりルーティングされます。
ステップ 3	アプリケーション サーバの設定 （87 ページ）	エンドユーザを、デバイスのロケーションを入力したアプリケーション サーバに直接接続します。
ステップ 4	E911 メッセージの設定 （88 ページ）	構外のエンドユーザの電話機に表示される E911 メッセージを設定します。

リモート ワーカーとしてのユーザの設定

始める前に

Cisco Emergency Responder に Intrado が設定されていることを確認します。 Cisco Emergency Responder での Intrado の設定の詳細については、Cisco Emergency Responder Administration Guide 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。**[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 電話機を検索するのに適切な検索条件を入力して、[検索（Find）]をクリックします。
検索基準に一致する電話機のリストが表示されます。

ステップ 3 リモート ワーカー緊急コールを設定する電話機を選択します。
[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 **[デバイス情報（Device Information）]** セクションで、**[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適切なユーザー ID を選択して、**[オフプレミスの場所が必要（Require off-premise location）]** 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。

緊急コールの代替ルーティングの指定

コーリング サーチ スペースと接続先番号を設定するには、次の手順を実行します。 これらのパラメータは、ユーザがロケーションを設定していない構外に登録してあるデバイスからのコールのルーティングを制限するために使用されます。 これらのパラメータを設定しない場合、コールは通常どおりにルーティングされます。

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）]** > **[サービス パラメータ（Service Parameters）]**。

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。
[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 ワイド パラメータ（構外のロケーションへの緊急コール）（Clusterwide Parameters（Emergency Calling for Required Off-premise Location））]セクションで[緊急コールの接続先の指定（Alternate Destination for Emergency Call）]を指定します。

ステップ 5 [緊急コール用コーリング サーチ スペースの指定（Alternate Calling Search Space for Emergency Call）]を指定します。

ステップ 6 **[保存（Save）]** をクリックします。

アプリケーション サーバの設定

E911 プロキシが Cisco Emergency Responder と通信できるようにするには、アプリケーション サーバを設定する必要があります。 E911 プロキシは、ユーザがデバイスの場所を入力するアプリケーション サーバにユーザを転送するために使用されます。

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）] > [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] をクリックします。
[**アプリケーション サーバ（Application Server**）] ウィンドウが表示されます。

ステップ 3 [**アプリケーション サーバのタイプ（Application Server Type**）] ドロップダウン リストで [**CER のロケーション管理（CER Location Management**）] 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 **[名前（Name**）] フィールドで、設定するアプリケーション サーバを特定する名前を指定します。

ステップ 6 [**IP アドレス（IP Address**）] フィールドに、設定するサーバの IP アドレスを入力します。

ステップ 7 [使用可能なアプリケーション ユーザ（Available Application Users）]のリストから、アプリケーション ユーザを選択し、下向きの矢印をクリックします。

ステップ 8 [**エンド ユーザの URL（End User URL**）] フィールドに、このアプリケーション サーバに関連付けられるエンド ユーザの URL を入力します。

ステップ 9 **[保存]** をクリックします。

E911 メッセージの設定

次の手順を使用して、構外デバイスの E911 メッセージを選択して編集します。

手順

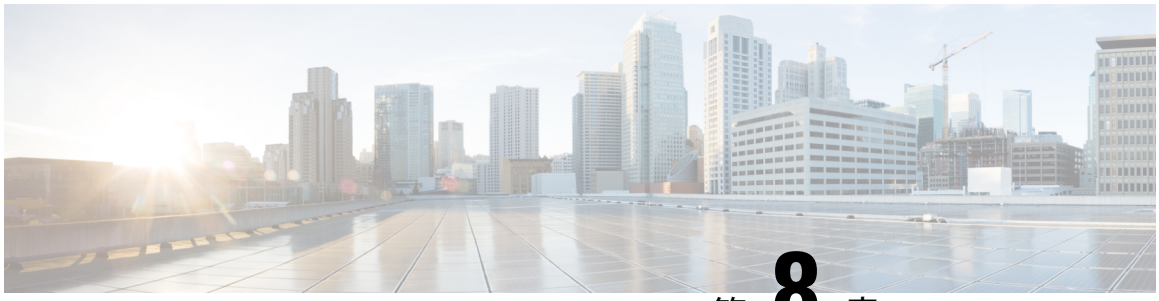
ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[システム（System）] > [E911 メッセージ（E911 Messages）]**。

ステップ 2 E911 メッセージの必要な言語リンクを選択します。

[E911 メッセージの設定（E911 Messages Configuration）] ページには、利用規約、免責事項、およびエラー メッセージが表示されます。

ステップ 3 （任意） 構外デバイスに表示される E911 メッセージを編集します。

ステップ 4 **[保存]** をクリックします。



第 8 章

モバイルおよびリモートアクセスの設定

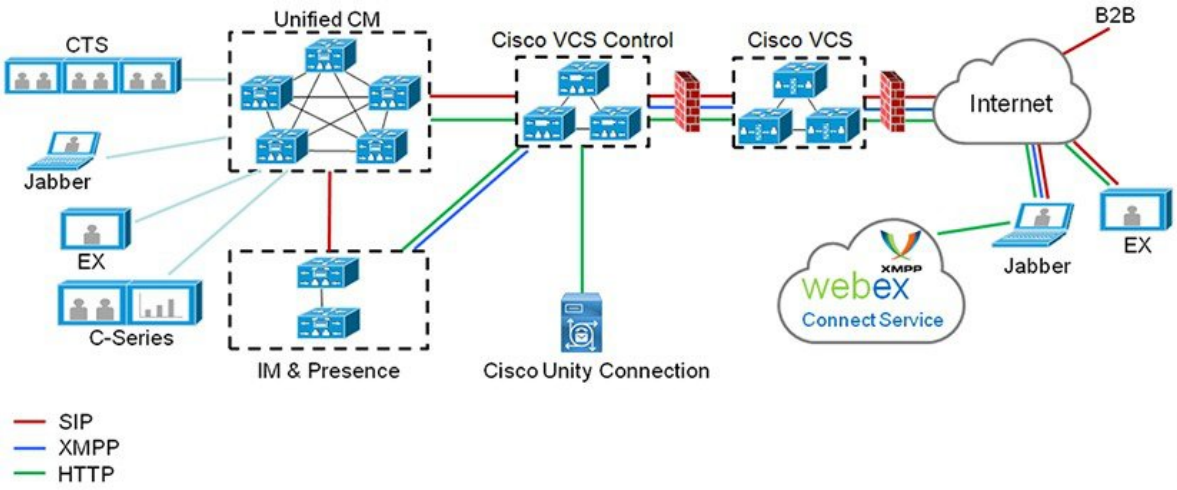
モバイルおよびリモートアクセスの概要

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。

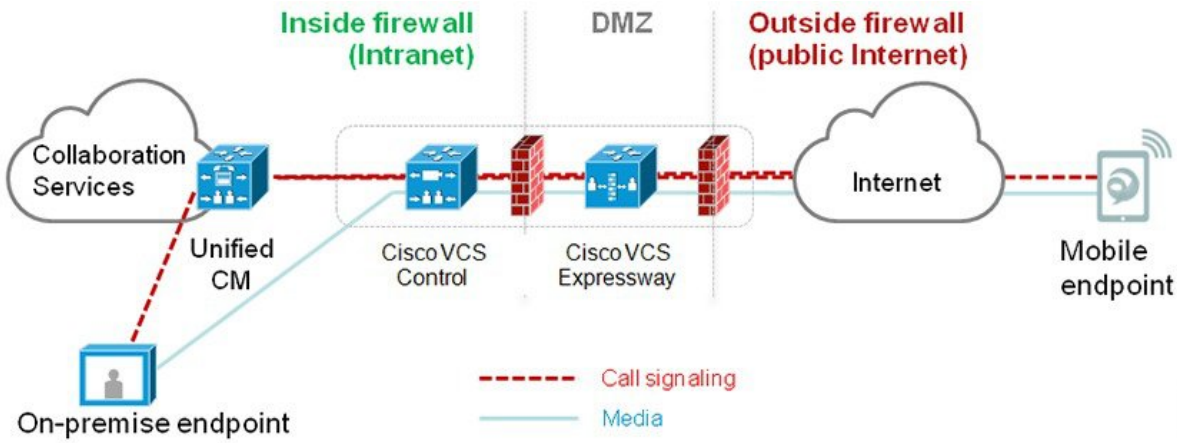
- オフプレミスアクセス：企業ネットワーク外においても、Jabber および EX/MX/SX シリーズ クライアントで一貫したエクスペリエンスを提供
- セキュリティ：セキュアな Business-to-Business（B2B）コミュニケーション
- クラウド サービス：豊富な Webex 統合とサービス プロバイダ製品を提供する、柔軟で拡張性に優れたエンタープライズ クラスのソリューション
- ゲートウェイと相互運用性サービス: メディアおよびシグナリングの正規化、非標準エンドポイントのサポート

図 *2 : 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 *3 :* 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] 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。モバイルおよびリモートアクセスのユーザ ポリシーは、Jabber 以外のエンドポイントでは必要ありません。

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。
- メディアパスを最適化するためにICE を導入する場合は、TURN およびSTUN サービスを提供できるサーバを導入する必要があります。

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<domain>
```

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

証明書は、Unified Communications ManagerIM and Presence サービスと Cisco Expressway-C の間で交換する必要があります。 Cisxo では、各システムに対して同じ CA を持つ CA 署名付き証明書を使用することを推奨しています。 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 エンドポイントを展開するには、これらのタスクを 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 （94 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 （94 ページ）	（オプション） モバイルおよびリモートアクセスの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、モバイルおよびリモートアクセスのエン

	コマンドまたはアクション	目的
		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]** 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のデバイス プール設定 （95 ページ）	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[日時グループ]と[リージョンの設定]を割り当てます。
ステップ 4	ICE の設定 （95 ページ）	**（オプション）** 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 コールの信頼性は向上します。
ステップ 5	モバイルおよびリモートアクセス用の電話機セキュリティ プロファイルの設定 （97 ページ）	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。
ステップ 6	Cisco Jabber ユーザのモバイルおよびリモートアクセスのアクセス ポリシーの設定 （98 ページ）	Cisco Jabber のみ。 Cisco Jabber のユーザに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セットアップします。Cisco Jabber ユーザは、モバイルおよびリモートアクセスの機能を使用するために、ユーザ プロファイル内でモバイルおよびリモートアクセスのアクセスを使用して有効にする必要があります。
ステップ 7	モバイルおよびリモートアクセスのユーザ設定 （100 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 8	モバイルおよびリモートアクセス用のエンドポイントの設定 （100 ページ）	モバイルおよびリモートアクセス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。

	コマンドまたはアクション	目的
ステップ 9	Cisco Expresswayのモバイルおよびリモートアクセスの設定 （100 ページ）	モバイルおよびリモート アクセスに対して Cisco Expressway を設定します。

Cisco AXL Web Service の有効化

パブリッシャ ノードで Cisco AXL Web サービスが有効になっていることを確認します。

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[ツール（Tools）]** > **[サービス アクティベーション（Service Activation）]** を選択します。

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の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] で **[ビデオコールの最大セッションビットレート]** 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実行します。

- 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のデバイス プール設定

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]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 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 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)]: ホストデバイスの IP アドレスを選択することによって得られる候補。 これはデフォルトです。
- **サーバ再帰**: STUN要求の送信によって取得される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**: TURNサーバから取得したIPアドレスとポートの候補。 IPアドレスとポートは、TURNサーバによってメディアが中継されるように、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（Auto）（デフォルト設定）]**、**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]** 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機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] 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 プロファイル名を入力します。 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]** 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]** 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 ユーザのモバイルおよびリモートアクセスのアクセス ポリシーの設定

Cisco Jabber のユーザに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設定するには、次の手順を使用します。 Cisco Jabber ユーザは、モバイルおよびリモートアクセスの機能を使用するために、ユーザプロファイル内でモバイルおよびリモートアクセスのアクセスを使用して有効にする必要があります。 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。

（注） モバイルおよびリモートアクセスのポリシーは、Jabber 以外のユーザには必要ありません。

ユーザ プロファイルの詳細については、『Cisco Unified Communications Manager システム設定ガイド』の「ユーザ プロファイルの概要」章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）]**。

ステップ 2 [新規追加] 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、**[ユニバーサルデバイステンプレート（Universal Device Template）]** を割り当てます。

ステップ 5 [ユニバーサル回線テンプレート（Universal Line Template）]を割り当て、このユーザプロファイルのユーザの電話回線に適用します。

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機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) [エンドユーザがプロビジョニングする電話機数を制限（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。

c) このプロファイルに関連付けられたエンドユーザーに、別のユーザーがすでに所有しているデバイスを移行または再割り当てする権限があるかどうかを判断するには、**[すでに別のエンドユーザーに割り当てられた電話機のプロビジョニングを許可する（Allow Provisioning of a phone already assigned to a different End User）]** チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

ステップ 7 このユーザープロファイルに関連付けられた Cisco Jabber ユーザーがモバイルおよびリモートアクセス機能を使用できるようにするには、**[モバイルおよびリモートアクセスの有効化（Enable Mobile and Remote Access）]** チェックボックスをオンにします。

（注）
- デフォルトでは、このチェックボックスはオンになっています。 このチェックボックスをオフにすると、**[クライアントポリシー（Client Policies）]** セクションが無効になり、サービス クライアント ポリシー オプションは、デフォルトで選択されません。
- この設定は、OAuth 更新ログインを使用している Cisco Jabber のユーザにのみ必須です。 Jabber ユーザではない場合、この設定を行わずともモバイルおよびリモートアクセス機能を使用できます。 モバイルおよびリモートアクセス機能は、Jabber モバイルおよびリモートアクセスのユーザにのみ適用され、他のエンドポイントや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。**[デスクトップ クライアント ポリシー（Desktop Client Policy）]** と **[モバイル クライアント ポリシー（Mobile Client Policy）]** のドロップダウンメニューから、次のオプションのいずれかを選択します。

- サービスなし：このポリシーは、すべての Cisco Jabber サービスへのアクセスを禁止します。
- IMとプレゼンスのみ：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のみを有効にします。
- IM とプレゼンス、音声とビデオ通話：このポリシーは音声やビデオ デバイスを使うすべてのユーザに対して、インスタントメッセージ、プレゼンス、ボイスメールと会議機能を有効化します。 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 版 Cisco Jabber および Mac 版 Cisco Jabber が含まれています。 Jabber モバイルクライアントには、iPad/iPhone ユーザ用 Cisco Jabber および Android 版 Cisco Jabber が含まれています。

ステップ 9 このユーザ プロファイルのユーザが Cisco Unified Communications セルフケア ポータルで Extension Mobility または Extension Mobility Cross Cluster の最大ログイン時間を設定できるようにするには、[エンドユーザにエクステンションモビリティの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）]チェックボックスをオンにします。

（注） デフォルトでは [エンドユーザにエクステンションモビリティの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）]チェックボックスはオフになっています。

ステップ 10　**[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のユーザ設定

Cisco Jabber のユーザの場合、設定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の詳細については、Cisco Unified Communications Manager システム設定ガイド の「エンド ユーザの設定」項を参照してください。

モバイルおよびリモートアクセス用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、Cisco Unified Communications Manager システム設定ガイド の「*Cisco Jabber* 構成タスク フロー」項を参照してください。
- その他のエンドポイントについては、Cisco Unified Communications Manager システム設定ガイド の「エンドポイント デバイスの設定」項を参照してください。

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。

軽量キープアライブを使用した MRA フェールオーバー

重要　このセクションは、リリース 14 以降に適用されます。

エンドポイント登録の場合、高い可用性を備えた Cisco Webex と Cisco Jabber は、Cisco Expressway-E、Cisco Expressway-C、および登録パス内のCisco Unified Communications Manager Administrationといったようなネットワーク要素の障害を検出し、次に利用可能なパスを経由して Unified CM に再登録するために修正措置を取る事が可能になります。

エンドポイントは軽量の STUN キープアティブ メッセージを送信し、登録パスでの接続性を確認します。 Unified Communications Managerが軽量 STUN キープアティブ メッセージを受信すると、Cisco Expressway-C IP を検証してメッセージに応答します。 Unified CM は、他の IP アドレスから受信された場合、STUN キープアティブ メッセージを破棄します。

登録パス内のノードが失敗した場合、エンドポイントは受信した軽量の STUN キープアティブ応答によって失敗を学習し、今後のメッセージ用に別のルート パスを選択します。 このサー

ビスは、ユーザが機能停止や他のメンテナンス モードに関係なく、スムーズで継続的な着信通話および発信通話を実行するのに役立ちます。

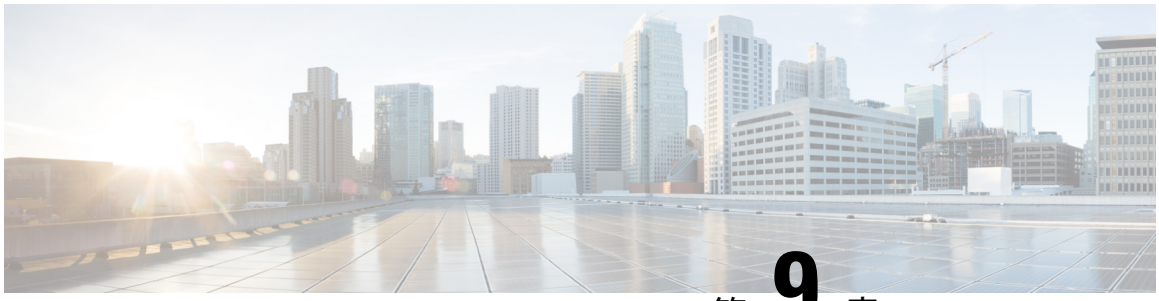
Cisco Webex またはCisco Jabber が MRA デバイスとして Unified Communications Manager に登録されると、Unified CMのExpressway-C の IP が表示されます（[**Device** > **Phone** > **IPv4 Address**] 列）。

（注） Cisco IP 電話は、登録フェールオーバーをサポートしていません。

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。

第 III 部

リモート ネットワーク アクセス



第 9 章

ワイヤレス LAN

ワイヤレス LAN の概要

この機能は、電話機で WiFi パラメータを設定するユーザの手間を省きます。 ユーザに代わって WiFi プロファイルを設定できます。 デバイスは、自動的に、システムから WiFi 設定をダウンロードして適用できます。 VPN 接続と HTTP プロキシの設定に関連した新しいセキュリティ層を含む、ネットワーク アクセス プロファイルを設定できます。

ワイヤレス LAN 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 （5 ページ）	ワイヤレス LAN プロファイルのデバイスを特定するためにレポートを生成します。
ステップ 2	ネットワーク アクセス プロファイルの設定 （106 ページ）	**オプション**：ワイヤレス LAN プロファイルにリンクできるように VPN および HTTP プロキシを設定する場合は、ネットワーク アクセス プロファイルを設定します。
ステップ 3	無線LANプロファイルの設定 （106ページ）	企業のデバイスまたはデバイス プールに適用する共通の WiFi 設定を使用してワイヤレス LAN 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 4	ワイヤレス LAN プロファイル グループの設定 （107 ページ）	ワイヤレス LAN プロファイルをまとめてグループ化します。
ステップ 5	デバイスまたはデバイス プールへの無線 LAN プロファイル グループのリンク（107 ページ）を行うには、次のサブタスクのいずれかを実行します。 • デバイスへのワイヤレス LAN プロファイル グループのリンク （108 ページ） • デバイス プールへのワイヤレス LAN プロファイル グループのリンク （108 ページ）	デバイス リンクが完了すると、TFTP は既存のデバイス コンフィギュレーション ファイルにワイヤレス LAN プロファイル グループを追加し、デバイス（またはデバイス プールに結び付けられたデバイス）がダウンロードします。

ネットワーク アクセス プロファイルの設定

ワイヤレス LAN プロファイルにリンクできるように VPN および HTTP プロキシを設定する場合は、ネットワーク アクセス プロファイルを設定します。

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。**[デバイス（Device）] > [デバイス設定（Device Settings）] > [ネットワーク アクセス プロファイル（Network Access Profile）]**

ステップ 2 [新規追加] をクリックします。

ステップ 3 [ネットワーク アクセス プロファイルの設定（Network Access Profile 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、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。

無線 LAN プロファイルの設定

企業のデバイスまたはデバイス プールに適用する共通の WiFi 設定を使用してワイヤレス LAN プロファイルを設定します。

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。[**Device** > **device SETTINGS]** > **[Wireless LAN Profile]**

ステップ 2 [新規追加] をクリックします。

ステップ 3 [無線 LAN プロファイルの設定（Wireless LAN 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、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。

ワイヤレス LAN プロファイル グループの設定

ワイヤレス LAN プロファイルをグループ化します。

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）]** > **[デバイス設定（device SETTINGS）]** > **[ワイヤレス LAN プロファイル（Wireless LAN Profile）]**

ステップ 2 [新規追加] をクリックします。

ステップ 3 [ワイヤレス LAN プロファイル グループ設定（Wireless LAN Profile 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、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。

デバイスまたはデバイス プールへの無線 LAN プロファイル グループのリンク

デバイス リンクが完了すると、TFTP によって、既存のデバイス コンフィギュレーション ファイルにワイヤレス LAN プロファイル グループが追加されます。続いて、これらは、デバイスや、デバイス プールに関連するデバイスによってダウンロードされます。

手順

	コマンドまたはアクション	目的
ステップ 1	デバイスへのワイヤレス LAN プロファイル グループのリンク （108 ページ）	
ステップ 2	デバイス プールへのワイヤレス LAN プロファイル グループのリンク （108 ページ）	

デバイスへのワイヤレス LAN プロファイル グループのリンク

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 次のいずれかの作業を実行します。

- 検索条件を入力し、[検索（Find）]をクリックして、結果一覧から既存デバイスを選択します。
- **[新規追加（Add New）]** をクリックして、**[電話のタイプ（Phone 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。

ステップ 3 [ワイヤレス LAN プロファイル グループ（Wireless LAN Profile Group）]ドロップダウン リストから、作成したワイヤレス LAN プロファイル 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。

デバイス プールへのワイヤレス LAN プロファイル グループのリンク

デバイス レベルおよびデバイス プール レベルでワイヤレス LAN プロファイル グループをリンクする場合、システムはデバイス プール設定を使用します。

手順

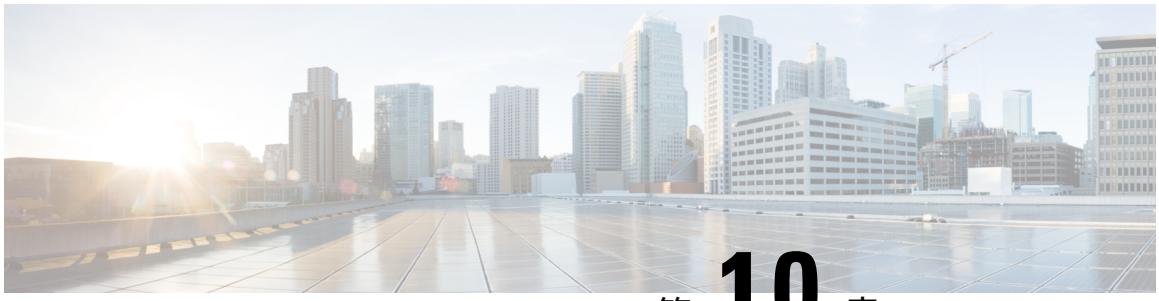
ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[システム（System）] > [デバイス プール（Device Pool）]**。

ステップ 2 次のいずれかの作業を実行します。

- 検索条件を入力し、[検索（Find）]をクリックして、結果一覧から既存デバイス プールを選択します。
- [新規追加] をクリックします。

ステップ 3 [ワイヤレス LAN プロファイル グループ（Wireless LAN Profile Group）]ドロップダウン リストから、作成したワイヤレス LAN プロファイル 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。



第 10 章

VPN クライアント

VPN クライアントの概要

Cisco Unified IP 電話 向け Cisco VPN Client により、在宅勤務の従業員のためのセキュアな VPN 接続が実現します。 Cisco VPN Client の設定はすべて Cisco Unified Communications Manager Administration で設定します。 社内で電話を設定したら、ユーザはその電話をブロードバンド ルータにつなぐだけで瞬時に組織のネットワークに接続できます。

（注） VPN メニューとそのオプションは、米国無制限輸出対象バージョンの Unified Communications Manager では利用できません。

VPN クライアントの前提条件

電話を事前にプロビジョニングし、社内ネットワーク内で初期接続を確立し、電話の設定を取得します。 設定はすでに電話に取り込まれているため、これ以降は VPN を使用して接続を確立できます。

VPN クライアント設定のタスク フロー

電話を事前にプロビジョニングし、社内ネットワーク内で初期接続を確立し、電話の設定を取得します。 設定はすでに電話に取り込まれているため、これ以降は VPN を使用して接続を確立できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco IOS の前提条件の完了 （113 ページ）	Cisco IOS の前提条件を満たします。 Cisco IOS VPN を設定するには、このアクションを実行します。
ステップ 2	IP Phone をサポートするための Cisco IOS SSL VPN の設定 （113 ページ）	IP Phone で VPN クライアントの Cisco IOS を設定します。 Cisco IOS VPN を設定するには、このアクションを実行します。
ステップ 3	AnyConnect 用の ASA 前提条件への対応 （115 ページ）	AnyConnect 用の ASA 前提条件を満たします。 ASA VPN を設定するには、このアクションを実行します。
ステップ 4	IP Phone での VPN クライアント用の ASA の設定 （116 ページ）	IP Phone で VPN クライアントの ASA を設定します。 ASA VPN を設定するには、このアクションを実行します。
ステップ 5	VPN ゲートウェイごとに VPN コンセントレータを設定します。	ユーザがリモート電話のファームウェアや設定情報をアップグレードするときに遅延が長くなるのを回避するため、VPN コンセントレータはネットワーク内の TFTP サーバまたは Unified Communications Manager サーバの近くにセットアップします。 これがネットワーク内で不可能な場合、代替 TFTP サーバまたはロード サーバを VPN コンセントレータの横にセットアップすることもできます。
ステップ 6	VPN コンセントレータの証明書のアップロード （118 ページ）	VPN コンセントレータの証明書をアップロードします。
ステップ 7	VPN ゲートウェイの設定 （119 ページ）	VPN ゲートウェイを設定します。
ステップ 8	VPN グループの設定 （120 ページ）	VPN グループを作成した後、設定した VPN ゲートウェイのいずれかをそのグループに追加できます。
ステップ 9	次のいずれかを実行します。 • VPN プロファイルの設定 （122 ページ） • VPN機能のパラメータの設定 （123 ページ）	VPN プロファイルを設定する必要があるのは、複数の VPN グループを使用している場合だけです。 [VPN Profle] フィールドは、[VPN Feature Configuration] フィールドよりも優先されます。

	コマンドまたはアクション	目的
ステップ 10	共通の電話プロファイルへの VPN の詳細の追加 （125 ページ）	共通の電話プロファイルに VPN グループおよび VPN プロファイルを追加します。
ステップ 11	Cisco Unified IP 電話 のファームウェアを、VPN をサポートしているバージョンにアップグレードします。	To run the Cisco VPN client, a supported Cisco Unified IP 電話 must be running firmware release 9.0（2） or higher. ファームウェアのアップグレードの詳細については、ご使用の Cisco Unified IP 電話 モデルの Unified Communications Manager に関する『*Cisco Unified IP Phone Administration Guide*』を参照してください。
ステップ 12	サポートされている Cisco Unified IP 電話 を使用して、VPN 接続を確立します。	Cisco Unified IP 電話 を VPN に接続します。

Cisco IOS の前提条件の完了

次の手順を使用して、Cisco IOS の前提条件を完了します。

手順

ステップ 1 Cisco IOS ソフトウェアバージョン 15.1(2)T 以降をインストールします。

機能セット/ライセンス：Universal（Data & Security & UC）for IOS ISR-G2 および ISR-G3

機能セット/ライセンス：Advanced Security for IOS ISR

ステップ 2 SSL VPN ライセンスをアクティベートします。

IP Phone をサポートするための Cisco IOS SSL VPN の設定

IP 電話をサポートするための Cisco IOS SSL VPN を実行するには、次の手順を使用します。

手順

ステップ 1 Cisco IOS をローカルで設定します。

a) ネットワーク インターフェイスを設定します。

例：

```
router(config)# interface GigabitEthernet0/0
router(config-if)# description "outside interface"
router(config-if)# ip address 10.1.1.1 255.255.255.0
router(config-if)# duplex auto
router(config-if)# speed auto
router(config-if)# no shutdown
router#show ip interface brief (shows interfaces summary)
```

b) 次のコマンドを使用してスタティック ルートとデフォルト ルートを設定します。

router(config)# **ip route** <*dest_ip*> < *mask*> < *gateway_ip*>

例：

```
router(config)# ip route 10.10.10.0 255.255.255.0 192.168.1.1
```

ステップ 2 CAPF 証明書を生成および登録して LSC の入った IP Phone を認証します。

ステップ 3 Unified Communications Manager から CAPF 証明書をインポートします。

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

（注） この場所は Unified Communications Manager のバージョンに基づきます。

b) Cisco_Manufacturing_CA および CAPF 証明書を見つけます。 .pem ファイルをダウンロードし、.txt ファイルとして保存します。

c) Cisco IOS ソフトウェアでトラストポイントを作成します。

```
hostname(config)# crypto pki trustpoint trustpoint_name
hostname(config-ca-trustpoint)# enrollment terminal
hostname(config)# crypto pki authenticate trustpoint
```

Base 64 で暗号化された CA 証明書を求められた場合は、ダウンロードした .pem ファイルのテキストを BEGIN 行および END 行とともにコピーし、貼り付けます。 この手順を他の証明書にも繰り返します。

d) 次の Cisco IOS 自己署名証明書を生成して Unified Communications Manager に登録するか、または CA からインポートした証明書で置き換えます。

- 自己署名証明書を生成します。

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 2048 2048
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Unified Communications Manager の VPN プロファイルでホスト ID チェックを有効にして、自己署名証明書を生成します。

例：

```
Router> enable
Router# configure terminal
```

```
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# fqdn <full domain
name>Router(config-ca-trustpoint)# subject-name CN=<full domain
name>, CN=<IP>Router(ca-trustpoint)#authorization username
subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- 生成された証明書を Unified Communications Manager に登録します。

  例：

  ```
  Router(config)# crypto pki export <name> pem terminal
  ```

  端末からテキストをコピーして、.pem ファイルとして保存し、これを Cisco Unified OS の管理を使用して、Unified Communications Manager にアップロードします。

ステップ 4 AnyConnect を Cisco IOS にインストールします。

AnyConnect パッケージを cisco.com からダウンロードし、フラッシュにインストールします。

例：

```
router(config)#webvpn install svc
flash:/webvpn/anyconnect-win-2.3.2016-k9.pkg
```

ステップ 5 VPN 機能を設定します。

（注） 電話で証明書とパスワード認証の両方を使用する場合は、電話の MAC アドレスを使用してユーザを作成します。 ユーザ名の照合では、大文字と小文字が区別されます。 次に例を示します。

username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted

AnyConnect 用の ASA 前提条件への対応

AnyConnect の前提条件を完了するには、次の手順を使用します。

手順

ステップ 1 ASA ソフトウェア（バージョン 8.0.4 以降）および互換性のある ASDM をインストールします。

ステップ 2 互換性のある AnyConnect パッケージをインストールします。

ステップ 3 ライセンスをアクティベートします。

a) 次のコマンドを実行して、現在のライセンスの機能を確認してください。

show activation-key detail

b) 必要な場合は、追加の SSL VPN セッションで新しいライセンスを取得し、Linksys 電話を有効にします。

ステップ 4 デフォルト以外の URL を持つトンネル グループが設定されていることを確認します。

```
tunnel-group phonevpn type remote-access
tunnel-group phonevpn general-attribute
  address-pool vpnpool
tunnel-group phonevpn webvpn-attributes
  group-url https://172.18.254.172/phonevpn enable
```

デフォルト以外の URL を設定するときは、次のことを考慮してください。

- ASA の IP アドレスにパブリック DNS エントリが含まれている場合、これを完全修飾ドメイン名（FQDN）に置き換えることができます。
- Unified Communications Manager では、VPN ゲートウェイに対して単一 URL（FQDN または IP アドレス）のみを使用できます。
- 証明書 CN またはサブジェクト代行名が必要な場合は、グループ URL の FQDN または IP アドレスを一致させます。
- ASA 証明書の CN や SAN が FQDN や IP アドレスと一致しない場合は、Unified Communications Manager のホスト ID チェックボックスをオフにします。

IP Phone での VPN クライアント用の ASA の設定

VPN クライアント用の ASA を IP 電話で設定するには、次の手順を使用します。

（注） ASA 証明書を置き換えると、Unified Communications Manager は使用できなくなります。

手順

ステップ 1 ローカル設定

a) ネットワーク インターフェイスを設定します。

例：

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto
ciscoasa(config-if)# speed auto
ciscoasa(config-if)# no shutdown
ciscoasa#show interface ip brief (shows interfaces summary)
```

b) スタティック ルートとデフォルト ルートを設定します。

ciscoasa(config)# **ルート** <interface_name> <ip_address> <netmask> <gateway_ip>

例：

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.89.79.129
```

c) DNS を設定します。

例：

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

ステップ 2 Unified Communications Manager と ASA に必要な証明書を生成して登録します。

Unified Communications Manager から次の証明書をインポートします。

- CallManager：TLS ハンドシェイク時の Cisco UCM の認証（混合モードのクラスタでのみ必要）。
- Cisco_Manufacturing_CA：製造元でインストールされる証明書（MIC）を使用した IP Phone の認証。
- CAPF：LSC を使用した IP Phone の認証。

これら Unified Communications Manager 証明書をインストールするには、次の手順を実行します。

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

b) 証明書 Cisco_Manufacturing_CA と CAPF を見つけます。 `.pem` ファイルをダウンロードし、`.txt` ファイルとして保存します。

c) ASA でトラストポイントを作成します。

例：

```
ciscoasa(config)# crypto ca trustpoint trustpoint_name
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

Base 64 でエンコードされた CA 証明書を求められた場合は、ダウンロードした `.pem` ファイル内のテキストを BEGIN 行および END 行とともにコピーして、貼り付けます。 この手順を他の証明書にも繰り返します。

d) 次の ASA 自己署名証明書を生成して Unified Communications Manager に登録するか、または CA からインポートした証明書で置き換えます。

- 自己署名証明書を生成します。

例：

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# keypair <name>
```

```
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Unified Communications Manager の VPN プロファイルでホスト ID チェックを有効にして、自己署名証明書を生成します。

  例：

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# fqdn <full domain name>
ciscoasa(config-ca-trustpoint)# subject-name CN=<full domain name>,CN=<IP>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- 生成された証明書を Unified Communications Manager に登録します。

  例：

```
ciscoasa(config)# crypto ca export <name> identity-certificate
```

  端末からテキストをコピーして、.pem ファイルとして保存し、Unified Communications Manager にアップロードします。

ステップ 3 VPN 機能を設定します。 以下に示すサンプル ASA 設定の概要を、設定のガイドとして利用できます。

（注） 電話で証明書とパスワード認証の両方を使用する場合は、電話の MAC アドレスを使用してユーザを作成します。 ユーザ名の照合では、大文字と小文字が区別されます。 次に例を示します。

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9
encrypted
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB attributes
ciscoasa(config-username)# vpn-group-policy GroupPhoneWebvpn
ciscoasa(config-username)#service-type remote-access
```

ASA 証明書の設定

ASA 証明書の設定に関する詳細は、「ASA 上の証明書認証を使用した AnyConnect VPN 電話の設定」を参照してください。

VPN コンセントレータの証明書のアップロード

VPN 機能をサポートするようにセットアップする際に、ASA で証明書を生成します。 生成された証明書を PC またはワークステーションにダウンロードしてから、この項で説明されている手順に従って、Unified Communications Manager にアップロードします。Unified Communications Manager は証明書を Phone-VPN-trust リストに保存します。

ASA は SSL ハンドシェイク時にこの証明書を送信し、Cisco Unified IP 電話 は、この証明書を電話と VPN 間の信頼リストに格納されている値と比較します。

ローカルで重要な証明書 (LSC) が Cisco Unified IP 電話 にインストールされている場合、デフォルトではその LSC が送信されます。

デバイス レベルの証明書認証を使用するには、ASA にルート MIC または CAPF 証明書をインストールして、Cisco Unified IP 電話 が信頼されるようにします。

Unified Communications Manager に証明書をアップロードするには、Cisco Unified OS Administration を使用します。

手順

ステップ 1 [Cisco Unified OS 管理（Cisco Unified OS Administration）] から、以下を選択します。**[セキュリティ] > [証明書の管理]**

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

ステップ 4 [ブラウズ（Browse）] をクリックして、アップロードするファイルを選択します。

ステップ 5 [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 6 アップロードする別のファイルを選択するか、[閉じる（Close）] をクリックします。

詳細については、「証明書の管理」の 章を参照 してください。

VPN ゲートウェイの設定

VPN ゲートウェイごとに VPN コンセントレータが設定されていることを確認します。 VPN コンセントレータの設定後、VPN コンセントレータの証明書をアップロードします。 詳細については、VPN コンセントレータの証明書のアップロード（118 ページ） を参照してください。

VPN ゲートウェイを設定するには、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。**[拡張機能（Advanced Features）] > [VPN] > [VPN ゲートウェイ（VPN Gateway）]** 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。

a) **[新規追加（Add New）]** をクリックして、新しいプロファイルを設定します。

b) コピーする VPN ゲートウェイの横にある **[コピー（Copy）]**をクリックします。

c) 適切な VPN ゲートウェイを見つけて、設定を変更し、既存のプロファイルを更新します。

ステップ 3 [VPN Gateway Configuration] ウィンドウでフィールドを設定します。 詳細については、VPN クライアントの VPN ゲートウェイ フィールド （120 ページ） 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。

VPN クライアントの VPN ゲートウェイ フィールド

VPN クライアントの VPN ゲートウェイフィールドについての説明をします。

表 *11 : VPN* クライアントの *VPN* ゲートウェイ フィールド

フィールド	説明
[VPNゲートウェイ名(VPN Gateway Name)]	VPN ゲートウェイの名前を入力します。
[VPNゲートウェイの説明(VPN Gateway Description)]	VPN ゲートウェイの説明を入力します。
[VPNゲートウェイのURL(VPN Gateway URL)]	ゲートウェイ内の主要な VPN コンセントレータの URL を入力します。 （注） VPN コンセントレータに 1 つのグループ URL を設定し、この URL をゲートウェイ URL として使用する必要があります。 設定情報については、次のような VPN コンセントレータのマニュアルを参照してください。 • 『*SSL VPN Client (SVC) on ASA with ASDM Configuration Example*』
[この場所のVPN証明書(VPN Certificates in this Location)]	上矢印キーおよび下矢印キーを使用して、証明書をゲートウェイに割り当てます。 ゲートウェイに証明書を割り当てないと、VPN クライアントはこのコンセントレータへの接続に失敗します。 （注） 最大 10 の証明書を 1 つの VPN ゲートウェイに割り当てることができます。また、各ゲートウェイに少なくとも 1 つの証明書を割り当てる必要があります。 電話と VPN 間の信頼性権限に関係付けられた証明書だけが、使用可能な VPN 証明書のリストに表示されます。

VPN グループの設定

VPN グループを設定するには、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。**[拡張機能（Advanced Features）]** > **[VPN]** > **[VPN グループ（VPN Group）]** 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。

a) **[新規追加（Add New）]** をクリックして、新しいプロファイルを設定します。

b) 既存の VPN グループをコピーする VPN グループの横にある **[コピー（copy）]** をクリックします。

c) 適切な VPN ゲートウェイを見つけて、設定を変更し、既存のプロファイルを更新します。

ステップ 3 [VPN Group Configuration] ウィンドウ内の各フィールドを設定します。詳細については、フィールド説明の詳細について、VPN クライアントの VPN ゲートウェイ フィールド（120 ページ）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。

VPN クライアントの VPN グループ フィールド

この表では、VPN クライアントの VPN グループフィールドについて説明しています。

表 *12 : VPN* クライアントの *VPN* グループ フィールド

フィールド	定義
[VPNグループ名(VPN Group Name)]	VPN グループの名前を入力します。
[VPNグループの説明(VPN Group Description)]	VPN グループの説明を入力します。
[使用可能なすべてのVPNゲートウェイ(All Available VPN Gateways)]	スクロールして、使用可能なすべての VPN ゲートウェイを表示します。
[このVPNグループ内で選択されたゲートウェイ(Selected VPN Gateways in this VPN Group)]	上矢印ボタンと下矢印ボタンを使用して、使用可能な VPN ゲートウェイをこの VPN グループに入れたりグループから外したりします。 VPN クライアントで重要なエラーが発生し、特定の VPN ゲートウェイに接続できない場合は、リストの次の VPN ゲートウェイへの移動を試みます。 （注） 1 つの VPN グループに最大 3 つの VPN ゲートウェイを追加できます。また、VPN グループ内の証明書数は、合計で 10 までです。

VPN プロファイルの設定

VPN 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。**[拡張機能（Advanced Features）] > [VPN] > [VPN プロファイル（VPN Profile）]** 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。

a) **[新規追加（Add New）]** をクリックして、新しいプロファイルを設定します。

b) 既存のプロファイルをコピーする VPN プロファイルの横にある **[コピー （copy ）]** をクリックします。

c) 既存のプロファイルを更新するには、該当するフィルタを [Find VPN Profile Where] で指定し、[検索（Find）] をクリックして設定を変更します。

ステップ 3 [VPN Profile Configuration] ウィンドウで各フィールドを設定します。 詳細については、フィールド説明の詳細について、VPN クライアントの VPN プロファイル フィールド （122 ページ）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。

VPN クライアントの VPN プロファイル フィールド

この表では、VPN プロファイルフィールドの詳細について説明します。

表 *13 : VPN* プロファイル フィールドの詳細

フィールド	定義
名前	VPN プロファイルの名前を入力します。
説明	VPN プロファイルの説明を入力します。
[自動ネットワーク検出を有効化(Enable Auto Network Detect)]	このチェックボックスをオンにすると、VPN クライアントは、社内ネットワーク外にあることが検出された場合に限り実行できます。 デフォルト：[無効(Disabled)]
MTU	最大伝送ユニット（MTU）のサイズをバイト数で入力します。 デフォルト：1290 バイト
[接続の失敗(Fail to Connect)]	VPN トンネルの作成中に、ログインまたは接続操作が完了するまで待機する時間を指定します。 デフォルト：30 秒

フィールド	定義
[ホストIDチェックを有効化(Enable Host ID Check)]	このチェックボックスがオンの場合、ゲートウェイ証明書の subjectAltName または CN が、VPN クライアントの接続先の URL と一致している必要があります。 デフォルト：[有効(Enabled)]
[クライアント認証方式(Client Authentication Method)]	ドロップダウン リストから、クライアント認証方式を選択します。 • [ユーザおよびパスワード(User and password)] • [パスワードのみ(Password only)] • [証明書(Certificate)]（LSC または MIC）
[永続的パスワードを有効化(Enable Password Persistence)]	このチェックボックスをオンにすると、ログインの失敗、ユーザによる手動のパスワードのクリア、電話のリセット、または電源が切れるまで、ユーザのパスワードは電話に保存されます。

VPN 機能のパラメータの設定

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。**[拡張機能（Advanced Features）] > [VPN] > [VPN 機能設定（VPN Feature Configuration）]**。

ステップ 2 [VPN Feature Configuration] ウィンドウのフィールドを設定します。 詳細については、VPN 機能のパラメータ （123 ページ） を参照してください。

ステップ 3 **[保存]** をクリックします。

次の作業を行います。

- Cisco Unified IP Phone のファームウェアを、VPN をサポートしているバージョンにアップグレードします。 ファームウェアのアップグレード方法の詳細については、ご使用の Cisco Unified IP 電話 モデルの『*Cisco Unified IP Phone Administration Guide*』を参照してください。
- サポートされている Cisco Unified IP 電話 を使用して、VPN 接続を確立します。

VPN 機能のパラメータ

VPN 機能パラメータの説明を表に示します。

表 *14 : VPN* 機能のパラメータ

フィールド	デフォルト
[自動ネットワーク検出を有効化(Enable Auto Network Detect)]	[True] の場合、VPN クライアントは、社内ネットワーク外にあることが検出された場合に限り実行できます。 デフォルト：False
MTU	最大伝送単位を指定します。 デフォルト：1290 バイト 最小値：256 バイト 最大値：1406 バイト
[キープ アライブ（Keep Alive）]	キープ アライブ メッセージを送信する間隔を指定します。 （注） この値がゼロ以外であり、かつ Unified Communications Manager で指定された値よりも小さい場合、VPN コンセントレータのキープアライブ設定によってこの設定が上書きされます。 デフォルト：60 秒 最小値：0 秒 最大値：120 秒
[接続の失敗(Fail to Connect)]	VPN トンネルの作成中に、ログインまたは接続操作が完了するまで待機する時間を指定します。 デフォルト：30 秒 最小値：0 秒 最大値：600 秒
[クライアント認証方式(Client Authentication Method)]	ドロップダウン リストから、クライアント認証方式を選択します。 • [ユーザおよびパスワード(User and password)] • [パスワードのみ(Password only)] • [証明書(Certificate)]（LSC または MIC） デフォルト：[ユーザおよびパスワード(User and password)]

フィールド	デフォルト
[永続的パスワードを有効化(Enable Password Persistence)]	Trueの場合、リセットにResetボタンまたは「**#**」が使用されていると、ユーザーのパスワードが電話機に保存されます。 電話機の電源が切れた場合、または工場出荷時の設定にリセットされた場合、パスワードは保存されず、電話機は認証情報の入力を求めるプロンプトを表示します。 デフォルト：False
[ホストIDチェックを有効化(Enable Host ID Check)]	[True] の場合、ゲートウェイ証明書の subjectAltName または CN が、VPN クライアントの接続先の URL と一致している必要があります。 デフォルト：[True]

共通の電話プロファイルへの VPN の詳細の追加

一般的な電話プロファイルに VPN の詳細を追加するには、次の手順を使用します。

手順

ステップ 1 [Cisco Unified CM 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）] > [共通の電話プロファイル（Common Phone Profile）]**。

ステップ 2 [**検索（Find**）] をクリックして、VPN の詳細を追加する共通電話プロファイルを選択します。

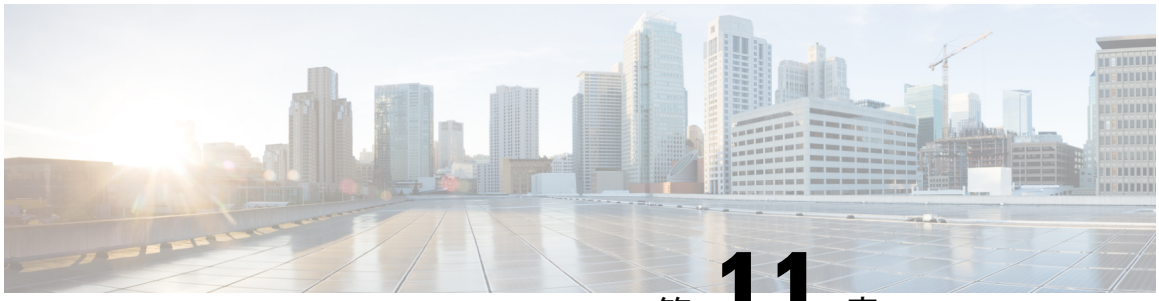
ステップ 3 [VPN情報（VPN Information）] セクションで、適切な [VPNグループ（VPN Group）] および [VPNプロファイル（VPN Profile）] を選択します。

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

ステップ 5 設定の適用ウィンドウで [**OK**] をクリックします。

第 IV 部

ライセンス



第 11 章

ライセンス

ライセンス

Cisco Unified Communications Manager のライセンスは、Cisco Unified Communications Licensing の全体的な商用オファーの一部です。

		User Connect Licensing (Essential)	User Connect Licensing (Basic)	User Connect Licensing (Enhanced/ Enhanced Plus）	Unified Workspace Licensing
Cisco Unified CM の機能	**モバイル コネクト（SNR）**	なし	○	○	○

		User Connect Licensing (Essential)	User Connect Licensing (Basic)	User Connect Licensing (Enhanced/ Enhanced Plus）	Unified Workspace Licensing
デバイスのサポート	デバイス数	1	1	1/2	10
	デバイス タイプのサポート	アナログ/音声 (詳細については、ユーザとデバイスの表を参照)	音声 (詳細については、ユーザとデバイスの表を参照)	音声 (詳細については、ユーザとデバイスの表を参照)	音声 (詳細については、ユーザとデバイスの表を参照)
	ユーザ プロファイル数	1	1	1	1
[Clients]	Jabber Mobile	なし	なし	○	○
	Jabber Desktop	なし	なし	○	○
	Jabber IM/Presence	○	○	○	○
Application	Webex Meetings	アドオン	アドオン	アドオン	○
	Webex Social	アドオン	アドオン	アドオン	○
	Unity Connection	アドオン	アドオン	アドオン	○
	Cisco Unified CM	○	○	○	○

Cisco Unified Communications Manager のライセンスは、ユーザとユーザの機能、設定されたデバイスの統計によって決定されます。 Cisco Unified Communications Manager が、（ユーザの機能と関連デバイスを持つ）ユーザと、システムで設定されたデバイスの合計数に基づいて、ライセンスの使用率を算出します。 Cisco Unified Communications Manager は、すべてのライセンスの使用量を Cisco Smart Software Manager へレポートし、ライセンスの準拠または非準拠ステータスを取得します。

Unified Communications Manager のライセンス

Cisco Unified Workspace Licensing (UWL)、略称 CUWL は、コスト効果の高いシンプルなパッケージで広範なシスコ コラボレーション アプリケーションおよびサービスにアクセスできるライセンスです。 これには、ソフトウェア クライアント、アプリケーション サーバ、ユーザごとのライセンスが含まれています。

Cisco User Connect Licensing (UCL) は各 Cisco Unified Communications 製品のユーザベース ライセンスです。 ソフトウェア クライアント、アプリケーション サーバ ソフトウェア ライセンス、基本的な Unified Communications アプリケーションが含まれています。 必要性と選択するデバイスに応じて、UCL の Essential、Basic、Enhanced、Enhanced Plus のいずれかを使用できます。

Unified Communications Manager ライセンスのタイプは、次のとおりです。

UC Manager Essential	Essential User Connect ライセンス：基本ボイスを提供するデバイスまたはアナログ デバイス（電話機またはファクス）1 台をサポート（例：アナログ電話機、ATA 186、ATA 187、Cisco 3905、Cisco 6901）。
UC Manager Basic	Basic User Connect ライセンス：すべての Essential デバイスを含む 1 台のデバイスと、基本的な（ボイスおよびビデオ）コール制御機能をサポート （例：Cisco 6911、Cisco 6921）。
UC Manager Enhanced	Enhanced User Connect ライセンス：すべての Basic デバイスを含む 1 台のデバイスと、デスクトップおよび携帯クライアントを含む拡張（ボイスおよびビデオ）コール制御機能をサポート （例：Cisco 3911、Cisco 3951、Cisco 6941、Cisco 6945、Cisco 6961、Cisco 79xx、Cisco 89xx、Cisco 99xx、Cisco E20、Cisco TelePresence EX60、Cisco TelePresence EX90、サード パーティ SIP）。
UC Manager Enhanced Plus	Enhanced Plus User Connect ライセンス：すべての Enhanced デバイスを含む最大 2 台デバイスをサポート。
UC Manager CUWL	デスクトップやモバイル、プロのコラボレーション 作業スペース アプリケーション機能を含む高度な (音声およびビデオ) コール制御機能をサポートし、ユーザ 1 人あたり最大で 10 台のデバイスをサポートします。

UC Manager TelePresence Room	TelePresence Room ライセンス：イマーシブおよびマルチパーパスの Cisco TelePresence System エンドポイントおよび Spark Room に基づくルームをサポート （例：Cisco TelePresence System シリーズ 3200、3000、1300、Cisco TelePresence MX シリーズ、Cisco TelePresence TX シリーズ、Cisco TelePresence System Profile シリーズ）。

ライセンス コンプライアンス

Unified Communications Manager を初めてインストールすると、Cisco Smart Software Manager または Cisco Smart Software Manager に正常に登録されるまで、90 日間の評価のデモンストレーション モードで完全に動作します。 登録後、Unified Communications Manager は定期的に Cisco Smart Software Manager と通信します。 Unified Communications Manager は、すべてのライセンス要件をタイプ別に Cisco Smart Software Manager へレポートし、ライセンスのステータスを取得します。

Unified Communications Manamer で非コンプライアンスの状態のライセンスは、90 日間のライセンス超過期間の後に適用されます。 猶予期間を過ぎると Unified Communications Manager は非コンプライアンスに設定され、次のようなサービスの低下が発生します。

デバイスとユーザのプロビジョニングはできません。ライセンスに影響するユーザの設定（たとえば、[IM and Presenceの有効化/無効化] や [モビリティの有効化/無効化] のチェックボックスの変更）はできません。

スマート ライセンス操作の詳細については、次を参照してください。 Cisco Unified Communications Manager システム設定ガイド

「ユーザのみ」ライセンス

システムで設定されているユーザがデバイスに関連付けられていない場合、そのユーザはデバイスを所有せず「ユーザのみ」となります。 デバイスの [OwnerUserID] フィールドにそのユーザのユーザ ID が入力されると、ユーザはデバイスに関連付けられ、そのデバイスを「所有」したことになります。デバイスに関連付けられていないユーザ向けの「ユーザのみ」ライセンスについては、「ユーザとデバイスのサポート」の表に示されています。

ユーザがデバイスを所有していない場合、またはライセンスが必要なユーザ機能を使用していない場合は、システムにユーザを追加してもライセンスが消費されることはありません。ただし、ライセンスが必要なユーザ機能がユーザに設定されている場合や、ユーザがデバイスを所有している場合は、ライセンスが消費されます。現在ライセンスされている機能は、モバイルコネクト (モビリティまたはシングルナンバーリーチまたは SNR とも呼ばれる) のみです。

ユーザのモバイルコネクト(またはモビリティまたはシングルナンバーリーチ)は、エンドユーザをデバイスの所有者 (ユーザ ID フィールド) に設定したリモート接続先プロファイル (RDP) が作成されている場合に設定されます。

デバイスのみ

デバイスが Cisco Unified Communications Manager に追加され、デバイス設定ウィンドウに [OwnerUserID] フィールドのエントリがない場合、そのデバイスはユーザに割り当てられていない、または関連付けられていないとみなされ、「デバイスのみ」と分類されます。「デバイスのみ」のデバイスのライセンスは、「Cisco Unified Communications Manager Licensing – ユーザおよびデバイスのサポート」の表に一覧で記載されています。 デバイスが Cisco Unified Communications Manager に追加され、[OwnerUserID] フィールドのエントリがない場合、そのデバイスには、デバイスのタイプごとに決められた最低限のライセンスタイプが必要となります。必要なライセンスは、「Licensing – ユーザおよびデバイスのサポート」の表に示されています。

ユーザとデバイス

デバイスの [OwnerUserID] フィールドにユーザ ID を入力し、デバイスをユーザに割り当てると、またはデバイスをユーザに関連付けると、そのユーザとデバイスのライセンス要件は、デバイスのタイプおよびそのユーザに割り当てられているデバイス数によって決定されます。 1 つのデバイスを所有するユーザの場合、ユーザのユーザ ID が 1 つの Essential デバイス（3905、6901、アナログ デバイスなど）に OwnerUserID として追加されると、ユーザとデバイスに必要な最小ライセンスは 1 つの Essential ライセンスになります。 つまり、1 つの Essential ライセンスによって、ユーザとデバイスの両方がサポートされます。 その一方で、ユーザのユーザ ID が 1 つの Basic デバイス（6911、6921 など）に OwnerUserID として追加された場合、ユーザとデバイスに必要な最小ライセンスは 1 つの Basic ライセンスになります。 ユーザのユーザ ID が 1 つの Enhanced デバイスに OwnerUserID として追加された場合、ユーザとデバイスに必要な最小ライセンスは 1 つの Enhanced ライセンスになります。

複数のデバイスを所有するユーザの場合、最小ライセンスはそのユーザが所有するデバイスの数によって決定されます。 「Cisco Unified Communications Manager ライセンス」の表に、1 つのユーザライセンスでサポートされるデバイスの最大数を示します。 2 つのデバイスを所有するユーザには、少なくとも 1 つの Enhanced Plus ライセンスが必要です。 3 つ以上のデバイスを所有するユーザは、少なくとも CUWL ライセンスが必要です。

「Cisco Unified Communications Manager ライセンス - ユーザとデバイスのサポート」の表に、ユーザのみ、デバイスのみ、およびユーザとデバイス向けの Cisco Unified Communications Manager ライセンスについて示します。

表 *15 : Cisco Unified Communications Manager* ライセンス - ユーザとデバイスのサポート

ライセンス タイプ	デバイスのみ	ユーザとデバイス	ユーザのみ
UC Manager Essential	• Cisco Unified SIP 電話 3905 • Cisco Unified IP 電話 6901 • アナログ デバイス	1 つの Essential デバイスを所有する 1 人のユーザ。	該当なし
UC Manager Basic	Cisco Unified IP Phone 6911 および 6921 モデル または **UC Manager Essential** ライセンスタイプのデバイス	1 つの Basic デバイスを所有する 1 人のユーザ。 または **UC Manager Essential** ライセンスタイプのユーザおよび関連デバイス。	シングル ナンバー リーチが有効な 1 人のユーザ（モバイル コネクト）。 または **UC Manager Essential** の必須ライセンスタイプを持つユーザ。

ライセンス タイプ	デバイスのみ	ユーザとデバイス	ユーザのみ
UC Manager Enhanced		1 台の拡張デバイスを持つユーザ。 または **UC Manager Essential** または **UC Manager Basic** ライセンスタイプのユーザおよび関連デバイス。	該当なし

ライセンス タイプ	デバイスのみ	ユーザとデバイス	ユーザのみ
	• Cisco Unified IP 電話 3911、3941、3951 • Cisco Unified IP Phone 6941、6945、および 6961 モデル • Cisco Unified IP Phone 7900 シリーズ（7900G、7911G、7912G、7931G、794xG、796xG、および 7975G モデル） • Cisco Unified IP Phone 8900 シリーズ（8941、8945、および 8961 モデル） • Cisco Unified IP Phone 9900 シリーズ（9951 および 9971 モデル）（カメラ付き/カメラなし） • Cisco Unified ワイヤレス IP 電話 シリーズ（792xG および 7925G-EX モデル） • Cisco Unified IP Conference Station（7936G および 7937G Station） • Cisco Unified Softphone（Cisco Unified Personal Communicator、Cisco UC Integration for Lync、Cisco UC		

ライセンス タイプ	デバイスのみ	ユーザとデバイス	ユーザのみ
	Integration for Connect、および Cisco IP Communicator） • Jabber クライアント（Jabber for Mac、Jabber for Windows、Jabber for iPhone、Jabber for Android、Jabber for iPad、および Jabber SDK） • ボイスおよびビデオ ファームウェアを含む Cisco Virtual Experience Client（VXC） • Cisco IP Video Phone E20 • Cisco TelePresence System EX シリーズ（EX60 および EX90） • サードパーティの SIP デバイス • Cisco Desktop Collaboration Experience DX600 シリーズ • Transnova S3 • Cisco Spark Webex Room Device • IMS または UC Manager Essential または UC Manager Basic ライセンスタイプのデバイス。		

ライセンス タイプ	デバイスのみ	ユーザとデバイス	ユーザのみ
UC Manager Enhanced Plus	該当なし	2 つのデバイスを所有する 1 人のユーザ。 または **UC Manager Essential**、**UC Manager Basic**、**UC Manager Enhanced**、または **UC Manager Enhanced Plus** ライセンスタイプを含むユーザおよび関連デバイス。	該当なし

ライセンス タイプ	デバイスのみ	ユーザとデバイス	ユーザのみ
UC Manager TelePresence Room ライセンス		1 UC Manager TelePresence Room デバイスが関連付けられているユーザ。	該当なし

ライセンス タイプ	デバイスのみ	ユーザとデバイス	ユーザのみ
	• Cisco TelePresence System 500 シリーズ • Cisco TelePresence System 1100 • Cisco TelePresence System 1300 シリーズ • Cisco TelePresence System 3000 シリーズ • Cisco TelePresence System 3200 シリーズ • Cisco TelePresence TX9000 シリーズ（TX9000、TX9200） • Cisco TelePresence TX1300 シリーズ • Cisco TelePresence System Profile シリーズ（42 インチ 6000 MXP、52 インチ MXP、52 インチ Dual MXP、65 インチ、および 65 インチ デュアル） • Cisco TelePresence System Codec C90/C60/C40 • Cisco TelePresence System Quick Set C20 • Cisco TelePresence MX シリーズ（MX300 および MX200）		

ライセンス タイプ	デバイスのみ	ユーザとデバイス	ユーザのみ
	• Cisco TelePresence 1000 • Cisco TelePresence SX シリーズ • Cisco Webex Devices • Generic Desktop Video Endpoint • Generic Multiple Screen Room System • Generic Single Screen Room System		

「**デバイスのみ**」とは、Cisco Unified Communications Manager で設定された、ユーザによる関連付けがない（[OwnerUserID] フィールドが空白である）デバイスを意味します。

「**ユーザとデバイス**」とは、Cisco Unified Communications Manager で設定された、ユーザによる関連付けがある（[OwnerUserID] フィールドにユーザ ID が登録されている）デバイスを意味します。

「**ユーザのみ**」とは、Cisco Unified Communications Manager で設定された、デバイスが関連付けられていない（Cisco Unified Communications Manager デバイスで OwnerUserID としてのユーザ ID が見つからない）ユーザを意味します。

前述の表の**ボールドで示されているテキスト**は、ライセンスの置換によってデバイスがサポートされることを示しています。この場合は、リストされているライセンスタイプの使用可能なライセンスを使用して、低いレベルのライセンス要件を満たすことができます。 Cisco Smart Software Manager で完了しています。

（注） MGCP FXS ポートはアナログ電話と見なされないため、これらのポートにはライセンスは必要ありません。

ユーザごとの最大デバイス数

Essential ライセンス、基本ライセンス、および Enhanced ライセンスは、関連デバイスを 1 つ所有するユーザをサポートします。ユーザ ID は 1 つのデバイスの [オーナーのユーザID] フィールドに入力されます。 Enhanced Plus ライセンスは、関連付けられた 2 デバイスを使用するユー

ザをサポートします。 UWL は、関連デバイスを 3 つ以上（最大 10 個）所有するユーザをサポートします。

TelePresence Room ライセンス

多目的 TelePresence デバイスとイマーシブ テレプレゼンス デバイスは、個別のデバイス ライセンス タイプの TelePresence Room ライセンスに基づいてライセンス付与されます。 TelePresence デバイスおよび電話機の [OwnerUserID] フィールドに電話機と同じユーザ ID が入力されている場合に限り、TelePresence デバイスと Cisco Unified Communications Manager に登録されている電話機が TelePresence Room ライセンスの対象になります。 TelePresense デバイスと電話機の両方の [OwnerUserID] に同じユーザ ID が入力されていない場合、デバイスは関連付けられず、2 つのライセンスが必要になります。つまり、デバイス用の TelePresence Room ライセンスと電話機用の Enhanced が必要になります。 TelePresence タッチ デバイスは Cisco Unified Communications Manager に登録されません。このため、別のライセンスまたは OwnerUserID の関連付けは必要ありません。

ライセンスの代替

Cisco Smart Software Manager (CSSM) は、コンプライアンスを有効にするために、使用可能なライセンスの階層ライセンス代替を許可します。 ライセンス代替を管理し、使用可能な上位レベルのライセンスは下位レベルのライセンス要件に合うように代用または貸し出されます。 たとえば、お客様が 100 件の UC Manager CUWL ライセンスを所持しているにもかかわらず、Cisco Unified Communications Manager が 10 件の CUWL ライセンスおよび 50 件の UC Manager Enhanced Plus ライセンス要件をレポートで返す場合、CSSM は 100-10、つまり 90 件の UC Manager CUWL ライセンスが下位の階層への貸し出しに使用できると計算します。 90 件の使用可能な UC Manager CUWL ライセンスのうち、50 件の CUWL ライセンスが 50 件の Enhanced Plus ライセンス要件に合わせて使用されます。 CSSM には、使用可能な 40 件の UC Manager CUWL ライセンスが表示されます。

（注） シスコ スマート ソフトウェア マネージャ オンプレミス（Cisco SSM On-Prem）または Smart Software Manager サテライトが Unified Communications Manager でライセンス付与に使用されている場合、Cisco SSM On-Prem と比較すると、CSSM でのライセンス階層置換の内訳の表示方法に違いがあります。 Unified CM のライセンス認証ステータスがコンプライアンス違反である場合の不十分なライセンス情報の詳細については、Cisco SSM On-Prem ユーザーインターフェイスを参照してください。 詳細については、CSCwf47221 を参照してください。

（注） 仮想アカウントが直接通信を使用して製品インスタンスによってすでに使用されており、ライセンスが特定のライセンスの予約用に予約されている場合、利用可能なライセンス数量は正しく表示されません。 詳細については、CSCwf47223 を参照してください。

ライセンス処理のシナリオ

次のライセンス処理のシナリオでは、ライセンス要件となる Cisco Unified Communications Manager の管理の設定変更を段階的に説明します。

ユーザの追加

[エンドユーザの設定] または一括管理ツールによって、新規ユーザ（ユーザ A）が Cisco Unified Communications Manager の管理 に最初に追加される際に、そのユーザが [モビリティの有効化] でリモート デバイス プロファイルを所有していないため、その新規ユーザにライセンスは必要ありません。

新規ユーザ（ユーザ B）が最初に Cisco Unified Communications Manager に追加され、そのユーザに [モビリティの有効化] でリモート接続先プロファイルが設定されている場合、その新規ユーザ（ユーザ B）には基本ライセンスが必要です。

ユーザー ID	ライセンスを持つユーザの機能	必要なライセンス	（注）
ユーザ A	None	None	割り当てデバイスなし
ユーザ B	モビリティ	基本	割り当てデバイスなし

未割り当てデバイスの追加

今度は新規のデバイスを Cisco Unified Communications Manager に登録して、そのデバイスの [オーナーのユーザ ID] フィールドにユーザ ID が入力されていない場合、そのデバイスはユーザに未割り当てで、『Cisco Unified Communications Manager Licensing』の「User and Device Support」の表に表示されているように、未割り当てデバイスのデバイス タイプごとにライセンスが必要となります。 たとえば、Device6901 が追加されると Essential ライセンスが必要となります。 Device6921 が追加されると Basic ライセンスが必要となります。 DeviceEX60 が追加されると Enhanced ライセンスが必要になります。

Enhanced Plus、CUWL Standard、または CUWL Professional ライセンスを必要とするデバイスは現在ありません。 そのため Enhanced Plus など前述のライセンスを必要とする未割り当てデバイスに関する Cisco Unified Communications Manager の要件は表示されていません。

表 *16* : ライセンス要件があるデバイスの例

Device	必要なライセンス	（注）
Device6901	UC Manager Essential	オーナーのユーザ ID なし
Device6921	UC Manager Basic	オーナーのユーザ ID なし

Device	必要なライセンス	（注）
DeviceEX60	UC Manager Enhanced	オーナーのユーザ ID なし

関連デバイスへのユーザの追加

デバイスを追加してそのデバイスがユーザに関連付けられている場合は、ユーザとデバイスはライセンスを共有します。 1 ユーザにつき 1 デバイスのため、必要なライセンスは、必要なユーザ ライセンスまたはデバイス ライセンスのうち、数が大きな方になります。 次のシナリオでは、1 ユーザにつき 1 デバイスの場合の、デバイスとユーザ関連の各種組み合わせを検討します。

ユーザに関連付けられた必須デバイス

OwnerUserID = UserA と入力することによって Device6901（Essential デバイス）が User A に割り当てられた場合、デバイスとユーザの両方が 1 つの Essential ライセンスでサポートされます。

しかし、 OwnerUserID = UserC（または UserD）と入力することで Device6901（Essential デバイス）が UserB（Basic ユーザ）に割り当てられると、デバイスとユーザの両方が 1 つの Basic ライセンスでサポートされます。

ユーザに関連付けられた Basic デバイス

OwnerUserID = UserA と入力することによって Device6921（Basic デバイス）が User A に割り当てられた場合、デバイスとユーザの両方が 1 つの Basic ライセンスでサポートされます。 同様に、User B と入力することによってDevice6921（Basic デバイス）が User B（Basic ユーザ）に割り当てられた場合、デバイスとユーザの両方が 1 つの Basic ライセンスでサポートされます。

ユーザに関連付けられた拡張デバイス

ほとんどの物理的な電話やソフト クライアント、また EX60 や EX90 などのデスクトップ ビデオ デバイスは、Enhanced デバイス レベルに付属しています。 OwnerUserID = User A と入力することによってDevice EX60（Enhanced デバイス）が User A に割り当てられた場合、デバイスとユーザの両方が 1 つの Enhanced ライセンスでサポートされます。 同様に、User B と入力することによって DeviceEX60（Enhanced デバイス）が User B（Basic ユーザ）に割り当てられた場合、デバイスとユーザの両方が 1 つの Enhanced ライセンスでサポートされます。

表 *17*：ユーザとデバイスのライセンス要件の例

Device	OwnerUserID	ライセンスを持つユーザの機能	必要なライセンス
Device6901	ユーザ A	None	UC Manager Essential
	ユーザ B	モビリティ	UC Manager Basic

Device	OwnerUserID	ライセンスを持つユーザの機能	必要なライセンス
Device6921	ユーザ A	None	UC Manager Basic
	ユーザ B	モビリティ	UC Manager Basic
DeviceEX60	ユーザ A	None	UC Manager Enhanced
	ユーザ B	モビリティ	UC Manager Enhanced

ユーザごとのデバイス数

上記のユーザとデバイスの例は、ユーザが1つのデバイスに関連付けられている場合にのみ適用されます。この場合、ユーザ ID は 1 つのデバイス構成の [オーナーのユーザ ID] フィールドにのみ表示されます。 ユーザが複数のデバイスに関連付けられている場合は、デバイス タイプにかかわらず、上位レベルのライセンスが必要となります。

ユーザ A が 1 つのデバイスの [オーナーのユーザ ID] に割り当てられている場合、上記のシナリオが当てはまります。 ただし、ユーザ A が 2 つのデバイスの [オーナーのユーザ ID] に割り当てられている場合、Enhanced Plus ライセンス 1 件がユーザおよび 2 つの関連デバイスの両方に必要となります。 ユーザ A が 2 つよりも多いデバイスの [オーナーのユーザ ID] に割り当てられている場合は、UWL Standard ライセンス 1 件が必要となります。 ユーザ A は、UWL Standard ライセンス 1 件につき最大 10 個のデバイスに割り当てることができます。 ユーザ 1 人に対して 10 個より多いデバイスが割り当てられる場合は、ユーザは UWL Standard ライセンス 1 件に加えて、追加のデバイスに対して追加のライセンスが必要となります。

ライセンスの使用状況レポート

使用状況の詳細には、ライセンスのタイプ、ユーザ、および未割り当てのデバイスが含まれます。 使用情報は6時間に1回更新されますが、[使用状況の詳細の更新(Update Usage Details)] をクリックして手動で更新することができます。 [使用状況の詳細の更新(Update Usage Details)] をクリックするとリソースが集中的に使用されるため、システムのサイズによっては処理が完了するまでに数分かかることがあります。 Unified Communications のライセンス情報を確認するリンクは、**[すべてのライセンスタイプの説明とデバイスの分類の表示]** にあります。

アラームまたはライセンス アラート（ライセンスの非コンプライアンス状態）が発生すると、**ステータス** メッセージが表示されます。 ステータス メッセージの詳細については、「アラーム、アラート、およびライセンス ステータス通知」を参照してください。 ライセンスのコンプライアンスおよび非コンプライアンスの詳細については、「ライセンス コンプライアンス」を参照してください。

[ライセンス要件(タイプ別)(icense Requirements by Type)]テーブルには、現在のシステム ライセンス要件が表示されます。 これには、現在のライセンスの使用状況（必要なライセンス数）がライセンスのタイプ別に示され、ライセンスが必要なユーザ数および未割り当てのデバイス数

がライセンスのタイプ別にまとめられます。 ライセンス タイプ別レポートのリンクは、ユーザ（数）または未割り当てのデバイス（数）ごとに表示され、ドリルダウン リンクが含まれています。 ユーザ レポートでは、ユーザ ID リンクによって、ユーザ ID ごとのユーザ設定の詳細が表示されます。 ビューの詳細リンクは、ユーザ ID ごとにライセンス要件を提供します。 割り当てられていないデバイス レポートでは、割り当てられていないデバイスごとに必要なデバイス タイプとライセンス タイプが表示されます。

ユーザおよび未割り当てのデバイス別にまとめられたライセンスの使用状況レポートも使用できます。 [ユーザ(Users)] 行には、システムに設定されたユーザの合計数が表示され、 ユーザの [使用状況レポートの表示(View Usage Report)] では、システムに設定されたすべてのユーザと対応する各ライセンス要件のレポートが表示されます。 また、未割り当てのデバイスの [使用状況レポートの表示(View Usage Report)] では、未割り当てのデバイス（ユーザに関連付けられていないデバイス）の合計数が表示されます。

（注） Cisco Unified Communications の管理ページでユーザ ID をデバイスに割り当てると、そのデバイスはライセンスの使用状況レポートの [未割り当てのデバイス] から ユーザに移動します。 ただし、エンドユーザの制御するデバイスのリストにデバイスを追加しても、そのデバイスに関する「ライセンスの使用状況レポート」の出力結果は変わりません。

Cisco Unified のレポート

次のレポートは、Cisco Unified Communicationsソリューションの Cisco Unified Reporting コンソールで見ることができます。

1. Cisco Unified Communications Manager の管理のログイン ページのナビゲーション バーで、[Cisco Unified Reporting] をクリックします。
2. [システムレポート] を選択します。
3. [Unified CMデバイス数の集計] を選択します。

生成されたレポートでは、各モデルのデバイス数をクラスタごとに集計します。

1. Cisco Unified Communications Manager の管理のログイン ページのナビゲーション バーで、[Cisco Unified Reporting] をクリックします。
2. [システムレポート] を選択します。
3. [Unified CMユーザ デバイス数] を選択します。

生成されたレポートは、電話機とユーザの関係を、ユーザのいない電話機の数、1 台電話機を持っているユーザの数、2 台以上電話機を持っているユーザの数で、クラスタごとにまとめます。

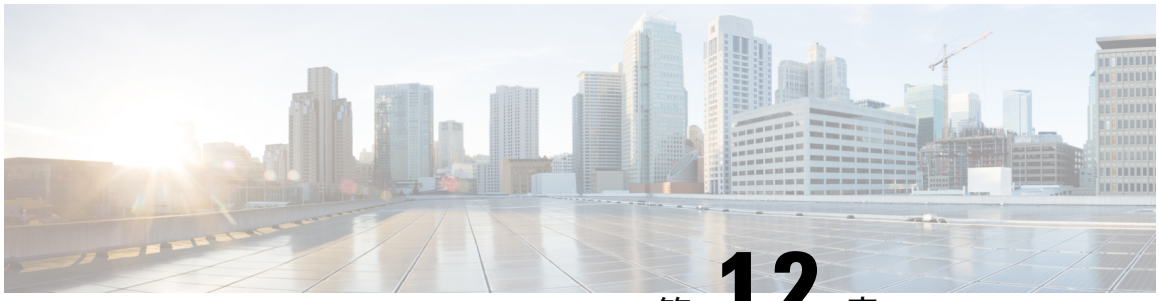
1. Cisco Unified Communications Manager の管理のログイン ページのナビゲーション バーで、[Cisco Unified Reporting] をクリックします。

2. [システムレポート] を選択します。
3. [Unified CMユーザ デバイス数] を選択します。

生成されたレポートは、電話機とユーザの関係を、ユーザのいない電話機の数、1 台電話機を持っているユーザの数、2 台以上電話機を持っているユーザの数で、クラスタごとにまとめます。

第 V 部

モニタリングおよび録音



第 12 章

サイレント モニタリング

サイレント モニタリングの概要

サイレント コール モニタリングを使用すると、スーパーバイザが電話での会話を傍受できます。 これが最も一般的に使用されるのは、コール エージェントが顧客と会話するコール センターです。 コール センターでは、コール センターのエージェントが提供するカスタマー サービスの品質を保証できるようにする必要があります。 サイレント モニタリングにより、スーパーバイザは、両方の通話者の声を聞くことができますが、どちらの通話者にもスーパーバイザの声は聞こえません。

サイレント モニタリングを呼び出すことができるのは、JTAPI または TAPI インターフェイスを介した CTI アプリケーションのみです。 Cisco Unified Contact Center Enterprise や Cisco Unified Contact Center Express などのシスコの多数のアプリケーションには、サイレント モニタリングの機能があります。 コールをモニタする CTI アプリケーションには、application-user または end-user アカウントについて有効な対応するモニタリング権限が必要です。

サイレント モニタリングはコール ベースです。 スーパーバイザがサイレント モニタリング セッションを呼び出すと、以下が発生します。

- スーパーバイザは、モニタする特定のコールを選択します。
- アプリケーションからの開始モニタリング要求により、スーパーバイザの電話はオフフックとなり、エージェントに対するモニタリング コールが自動的にトリガーされます。
- エージェントの電話はモニタリング コールに自動で応答します。 モニタリング コールは、エージェントに表示されません。

セキュア サイレント モニタリング

セキュア サイレント モニタリングを設定することもできます。 セキュア サイレント モニタリングにより、暗号化されたメディア（sRTP）コールのモニタリングが可能です。 コールのモニタリングは、監視対象のコールのセキュリティ ステータスに関係なく、エージェントの電話の機能により決定される最高レベルのセキュリティを使用して常に確立されます。 セキュリティの最高レベルは顧客、エージェント、およびスーパーバイザ間のいずれかのコールでのセキュア メディア キーの交換により維持されます。 保護されたメディアを使用したコールのモニタリングにより、約4000 bpsのさらなる帯域幅のオーバーヘッドが伝送されますが、これは標準的なセキュア メディア（sRTP）コールと同様です。

エージェントの電話で暗号化が有効になっている場合、セキュア サイレント モニタリングを可能にするにはスーパーバイザの電話でも暗号化が有効になっている必要があります。 エージェントの電話で暗号化が有効になっているが、スーパーバイザの電話では有効になっていない場合、モニタリング要求は失敗します。

ウィスパー コーチング

Unified Communications Manager 顧客が聞いていなくてもモニタリング セッションが実行されている一方で、スーパーバイザはエージェントと会話できるサイレント モニタリングでのCTI強化であるウィスパー コーチングもサポートしています。 ウィスパー コーチングはCTI アプリケーションでのみ開始できます。 サイレント モニタリングが既に設定されている場合、ウィスパー コーチングにはUnified Communications Manager の追加設定は必要ありません。

サイレント モニタリングの前提条件

サイレント モニタリングを呼び出すことができるのは、外部CTIアプリケーションのみです。Cisco Unified Contact Center Enterprise や Cisco Unified Contact Center Express などのシスコ アプリケーションは、サイレント モニタリング セッションを開始できます。 詳細については、次を参照してください。

- Cisco Unified Contact Center Enterprise：Cisco Unified Contact Center Enterprise でサイレント モニタリングをセットアップする方法の詳細については、『Cisco Remote Silent Monitoring Installation and Administration Guide』を参照してください。
- Cisco Unified Contact Center Express—この章には、Cisco Finesse を介した Unified Contact Center Express のサイレント モニタリングを設定するためのサンプル設定が含まれています。 Cisco Unified Contact Center Express に関連するその他のマニュアルは、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series-home.html を参照してください。

サイレント モニタリングの設定タスク フロー

このタスク フローでは、CTI アプリケーションでのモニタリング機能の使用を許可するために、Unified Communications Manager 内で実行する必要があるタスクについて説明します。

始める前に

- 電話機能リストのレポートを実行して、どの電話機でサイレントモニタリングがサポートされているかを判別します。 詳細については、電話機能一覧の生成 （5 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	次のいずれかの手順を実行します。 • クラスタ全体の電話での組み込みブリッジの有効化 （153 ページ） • 電話での組み込みブリッジの有効化 （154 ページ）	エージェントの電話機で組み込みのブリッジをオンにします。 サービス パラメータを使用してクラスタ全体のデフォルトを設定するか、または個々の電話機で組み込みのブリッジを有効化できます。 （注） 個々の電話機のブリッジ設定は、クラスタ全体のデフォルト設定を上書きします。
ステップ 2	スーパーバイザのモニタリング権限の有効化 （155 ページ）	サイレント モニタリングを許可するグループにスーパーバイザを追加します。
ステップ 3	モニタリング コーリング サーチ スペースの割り当て （155 ページ）	スーパーバイザの電話機でモニタリング コーリング サーチ スペースを設定します。
ステップ 4	サイレント モニタリングの通知トーンの設定 （156 ページ）	コールの参加者に通知トーンを再生するかどうかを設定します。
ステップ 5	セキュア サイレント モニタリングの設定 （156 ページ）	**（オプション）** コールを暗号化する場合、セキュア サイレント モニタリングを設定します。
ステップ 6	Unified Contact Center Express のサイレント モニタリングの設定 （158 ページ）	Unified Contact Center Express 導入では、Cisco Finesse を使用してサイレント モニタリングを設定します。

クラスタ全体の電話での組み込みブリッジの有効化

組み込みブリッジのクラスタ全体のサービス パラメータを有効に設定すると、クラスタ内のすべての電話で組み込みブリッジのデフォルト設定が有効に変わります。 ただし、[電話の設定（Phone Configuration）] ウィンドウの組み込みブリッジ設定は、クラスタ全体のサービス パラメータを上書きします。

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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

ステップ 2 [サーバ（Server）] ドロップダウン リストから、CallManager サービスが実行され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 [有効な組み込みブリッジ（Builtin Bridge Enable）] サービス パラメータを [オン（On）] に設定します。

ステップ 5 **[保存（Save）]** をクリックします。

電話での組み込みブリッジの有効化

個々の電話で組み込みブリッジを有効にするには、次の手順を使用します。 個々の電話の組み込みブリッジ設定は、クラスタ全体のサービス パラメータを上書きします。

始める前に

クラスタ内のすべての電話で組み込みブリッジをデフォルトに設定するには、サービス パラメータを使用します。 詳細については、クラスタ全体の電話での組み込みブリッジの有効化（153 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。**[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 **[検索 （Find ）]** をクリックして、エージェントの電話を選択します。

ステップ 3 [組み込みブリッジ（Built in Bridge）] 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。

- [オン（On）]：組み込みブリッジが有効になります。
- [オフ（Off）]：組み込みブリッジが無効になります。
- [デフォルト（Default）]：[組み込みブリッジの有効化（Builtin Bridge Enable）] クラスタ全体サービス パラメータの設定が使用されます。

ステップ 4 **[保存（Save）]** をクリックします。

スーパーバイザのモニタリング権限の有効化

スーパーバイザがエージェントのカンバセーションをモニタできるようにするには、スーパーバイザはモニタリングが許可されるグループの一部である必要があります。

始める前に

次のいずれかの手順を実行して、エージェントの電話でビルトインブリッジを有効にします。

- クラスタ全体の電話での組み込みブリッジの有効化 （153 ページ）
- 電話での組み込みブリッジの有効化 （154 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。**[ユーザ管理（User Management）] > [エンド ユーザ（End User）]**。

ステップ 2 スーパーバイザをユーザの一覧から選択します。

ステップ 3 [**権限情報（Permissions Information**）] セクションで、[**アクセスコントロールグループに追加（Add to Access Control Group**）] をクリックします。

ステップ 4 [標準 CTI 許可コール モニタリング（Standard CTI Allow Call Monitoring）] および [標準 CTI を有効にする（Standard CTI Enabled）] ユーザ グループを追加します。

ステップ 5 **[保存（Save）]** をクリックします。

モニタリング コーリング サーチ スペースの割り当て

モニタリングを機能させるには、モニタリング コーリング サーチ スペースをスーパーバイザの電話回線に割り当てる必要があります。 モニタリング コーリング サーチ スペースには、スーパーバイザの電話回線およびエージェントの電話回線の両方を含める必要があります。

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。**[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 [**検索（Find**）] をクリックしてスーパーバイザの電話機を選択します。
左側のナビゲーション ウィンドウに、スーパーバイザの電話機で利用可能な電話回線が表示されます。

ステップ 3 モニタリングに使用されるスーパーバイザの電話回線ごとに、次の手順を実行します。

a) 電話回線をクリックします。[**電話番号の設定（Directory Number Configuration**）] ウィンドウに、電話回線の設定情報が表示されます。

b) [**モニタリング コーリング サーチ スペース（Monitoring Calling Search Space**）] ドロップダウン リストから、スーパーバイザの電話回線およびエージェントの電話回線の両方を含むコーリング サーチ スペースを選択します。
c) **[保存（Save）]** をクリックします。

サイレント モニタリングの通知トーンの設定

特定の管轄区域では、コールがモニタされていることを示す通知トーンを、エージェント、顧客、あるいはその両方向けに再生する必要があります。デフォルトでは、Unified Communications Manager は、通知音を鳴らしません。 通知トーンを有効にするには、サービス 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 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）]**。
ステップ 2 [**サーバ（Server**）] ドロップダウン リストから、CallManager サービスが実行され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 次のサービス パラメータの値を設定します。

- エージェントに対して通知トーンを再生するには、[**観察対象のターゲットにモニタリング通知トーンを再生（Play Monitoring Notification Tone To Observed Target**）] サービス パラメータの値を [**はい（True**）] に変更します。
- 顧客に対して通知トーンを再生するには、[**観察対象の接続先にモニタリング通知トーンを再生（Play Monitoring Notification Tone To Observed Connected Parties**）] サービス パラメータの値を [**True]** に変更します。

ステップ 5 **[保存]** をクリックします。
ステップ 6 サービス パラメータの設定を変更した場合は、エージェント電話をリセットします。

セキュア サイレント モニタリングの設定

sRTP を使用したセキュア サイレント モニタリングを設定するには、暗号化を含む電話機のセキュリティ プロファイルを設定し、それをスーパーバイザの電話機と、モニタ対象のすべてのエージェントの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	暗号化電話セキュリティ プロファイルの設定 （157 ページ）	エージェントの電話機とスーパーバイザの電話機に暗号化を含む電話セキュリティ プロファイルを設定します。
ステップ 2	電話へのセキュリティ プロファイルの割り当て （158 ページ）	エージェントの電話機とスーパーバイザの電話機に暗号化された電話セキュリティ プロファイルを適用します。

暗号化電話セキュリティ プロファイルの設定

セキュア サイレント モニタリングを設定するには、スーパーバイザの電話機とエージェントの電話機の電話セキュリティ プロファイルで、[デバイス セキュリティ モード（Device Security Mode）] に [暗号化済（Encrypted）] を指定するよう設定する必要があります。

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）]**>**[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 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、既存の電話セキュリティ プロファイルを選択します。

ステップ 3 新しい電話セキュリティ プロファイルを作成した場合は、**[電話セキュリティ プロファイル タイプ（Phone Security Profile Type）]** ドロップダウン リストから、お使いの電話モデルを選択します。

ステップ 4 電話セキュリティ プロファイルの [名前（Name）] を入力します。

ステップ 5 **[デバイス セキュリティ モード（Device Security Mode）]** ドロップダウン リストから、**[暗号化済（Encrypted）]** を選択します。

ステップ 6 **[保存]** をクリックします。

ステップ 7 スーパーバイザの電話機とエージェントの電話機の電話セキュリティ プロファイルを設定するまで、上記の手順を繰り返します。

電話へのセキュリティ プロファイルの割り当て

次の手順を実行して、電話に電話セキュリティ プロファイルを割り当てます。 セキュア サイレント モニタリングを機能させるには、電話セキュリティ プロファイルをエージェントの電話とスーパーバイザの電話の両方に割り当てる必要があります。

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。I **[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 [検索（Find）] をクリックして、電話セキュリティ プロファイルを設定するエージェント電話を選択します。

ステップ 3 [**デバイス セキュリティ プロファイル（Device Security Profile**）] ドロップダウン リストから、設定した電話セキュリティ プロファイルを選択します。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 スーパーバイザの電話に対しても、前述の手順を繰り返します。

Unified Contact Center Express のサイレント モニタリングの設定

次の手順には、Cisco Finesse を介した Cisco Unified Contact Center Express 設定のサイレント モニタリングの例が含まれています。

始める前に

エージェントとスーパーバイザーの両方の電話機が Cisco Finesse に対応していることを確認してください。 https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html の『*Unified CCX* ソフトウェア互換性マトリクス』を参照してください。

手順

ステップ 1 テスト エージェントとスーパーバイザーを、Unified Contact Center Express 上に設定します。

（注） エージェントとスーパーバイザーの IP 連絡先センター（IPCC）の内線番号は、一意である必要があります。 これは、**[コール ルーティング（Call Routing）] > [ルート プラン レポート（Route Plan Report）]**の下にある Cisco Unified Communications Manager から確認でき ます。

ステップ 2 エージェントの電話に組み込み型の Bridge（BIB）があることを確認します。 これは、電話またはクラスタ レベルで行うことができます（デフォルトの [サービス（Service）] パラメータをオンに設定）。

ステップ 3 エージェントとして Finesse にログインします。

ステップ 4 Finesse にスーパーバイザーとしてログインし、スーパーバイザーが [NOT READY] になっていることを確認します。

ステップ 5 Resource Manager Contact Manager（RMCM）ユーザには、コール モニタリングとコール録音の必須のロールがあることを確認します。標準のコンピュータ テレフォニー インテグレーション（CTI）はコール モニタリングと録音を許可します。

（注） これは、RMCM ユーザの最初のセットアップ時に、Unified Contact Center Expres によって自動的に実行されます。 Cisco Unified Communications Managerの [**アプリケーション ユーザ（Application User**）] ウィンドウでロールが存在することを確認します。

ステップ 6 エージェントの回線のパーティションを含めるために、モニタリング用CSS（コーリング サーチ スペース）をスーパーバイザーの電話機に割り当てます。

ステップ 7 コールをエージェント ログインにルーティングするには、Unified Contact Center Express に電話をかけます。エージェントが TALKING 状態になったら、スーパーバイザーから、サイレント モニタリングを開始します。その後、スーパーバイザーは、エージェントと発信者の間の会話を聞くことができるようになります

サイレント モニタリングの連携動作

機能	データのやり取り
通話保持	モニタ対象のエージェント コールが通話保護モードになると、Unified Communications Manager はモニタリング コールも通話保持モードにします。
セキュア モニタリング コールの転送	Unified Communications Manager 接続先のスーパーバイザ デバイスが、モニタされているエージェントのセキュリティ機能を超えている限り、セキュア モニタリング セッションの転送をサポートします。
録音トーン	録音およびモニタリングされるコールに関しては、録音トーンがモニタリング トーンよりも優先されます。 コールの録音およびモニタが行われると、録音トーンだけ再生されます。

機能	データのやり取り
セキュア トーン	セキュア トーンが設定されていてコールがセキュアな場合、モニタリング トーンが設定されているかどうかに関係なく、コールの開始時にコール参加者にセキュア トーンが再生されます。 セキュア トーンとモニタリング トーンの両方が設定されていると、セキュア トーンが一度再生され、続いてモニタリング トーンが再生されます。 セキュア トーン、モニタリング トーン、および録音トーンすべてが設定されていて、コールが録音およびモニタされている場合、セキュア トーンが一度再生され、続いて録音トーンが再生されます。 モニタリング トーンは再生されません。

サイレント モニタリングの制約事項

機能	制約事項
割込み	Unified Communications Manager サイレント モニタリングを使用した割り込みはサポートされません。 エージェント コールがモニタされている場合、共有回線からの割り込みコールが失敗します。 エージェント コールへの割り込みがすでに行われている場合、モニタリング コールが失敗します。
クラスタ間トランク経由でのセキュアなサイレント モニタリングの転送	Unified Communications Manager クラスタ間トランク経由でのセキュアなサイレント モニタリングの転送をサポートしません。
サイレントモニタリングの制限事項	スーパーバイザが非セキュアモードでログインし、エージェントが MRA モードにログインすると、モニタリングは失敗します。 詳細については、「セキュアサイレントモニタリング」の項を参照してください。

第 13 章

録音

録音の概要

コール録音はUnified Communications Managerの機能の1つであり、これを利用すると録音サーバでエージェントの会話を記録できます。 コール録音は、コール センターや金融機関などの企業には不可欠な機能の 1 つです。 コール録音機能は、エージェントとエンドユーザ メディア ストリームのコピーを SIP トランク経由で録音サーバに送信します。 幅広い音声分析アプリケーションに適切に対応できるように、各メディア ストリームは個別に送信されます。

Unified Communications Manager IP フォンベースまたはネットワークベースの録音機能を提供します。

- IP フォン ベースの録音では、録音メディアのソースは電話機です。 電話機は、2 つのメディア ストリームをレコーディング サーバに分岐させます。
- ネットワーク ベースの録音では、録音メディアのソースは電話機またはゲートウェイです。 ネットワーク ベースの録音を実装する場合、ネットワーク内のゲートウェイは、SIP トランクを介して Unified Communications Manager に接続する必要があります。

Unified Communications Manager 単一クラスタと複数クラスタの両方の環境でコール録音をサポートしており、以下の 3 つの異なる録音モードを提供します。

- **自動サイレント録音**：自動サイレント録音では、回線アピアランスのすべてのコールが自動的に記録されます。Unified Communications Managerは、アクティブな録音セッションが確立されている電話で、視覚的な通知なしで、録音セッションを自動的に起動します。
- **選択的サイレント録音**：スーパーバイザはCTI対応デスクトップを介して録音セッションを開始または停止できます。 また、レコーディング サーバは、事前に定義済みのビジネ

ス ルールとイベントに基づいてセッションを起動できます。 アクティブな録音セッションが確立されたことを示す視覚的な表示は電話機上に出ません。

- **選択的ユーザ コールの録音**：エージェントがどのコールを録音するかを選択できます。エージェントは CTI 対応デスクトップ経由か、ソフトキーまたはプログラム可能な回線キーを使用して録音セッションを起動します。 選択的ユーザ録音を使用すると、Cisco IP 電話上に録音セッションのステータス メッセージが表示されます。

Unified Communications Manager 1 つの録音サーバへの録音をサポートし、メディア プロキシとして CUBE を使ってこれを展開することで、複数の録音サーバに録音できます。

- マルチフォーク録音では、Unified Communications Manager は SIP トランク経由で CUBE メディア プロキシに接続します。 CUBE Media Proxy サーバは電話とゲートウェイから 2 つのメディア ストリームを受け取り、これらのメディア ストリームを 1 つ以上の録音サーバに同時に分岐します。
- 1 つの録音サーバへの録音の場合、Unified Communications Manager は SIP トランク経由で録音サーバに直接接続します。 電話機またはゲートウェイは、2 つのメディア ストリームを録音サーバに分岐させます。

マルチフォーク録音

Unified Communications Manager メディア プロキシとして Cisco Unified Border Element（CUBE）を通じて同時マルチストリーム録音をサポートします。 マルチフォーク録音では、録音ストリームが CUBE Media Proxy サーバに送信され、このプロキシ サーバがメディア ストリームを最大 5 つの録音サーバに同時にリレーします。 これは、電話ベースの録音とネットワークベースの録音、さらに自動録音と選択録音の両方でサポートされています。

マルチ フォーク機能には、次の利点があります。

- 録音展開環境に冗長性とフェールオーバー機能を追加します。
- 音声の分析とモニタリングのための追加メディア ストリームを提供します。
- 金融業界などの組織は、冗長性のために顧客からのコールを複数サーバに録音するよう義務付けている MiFID 要件に準拠できます。

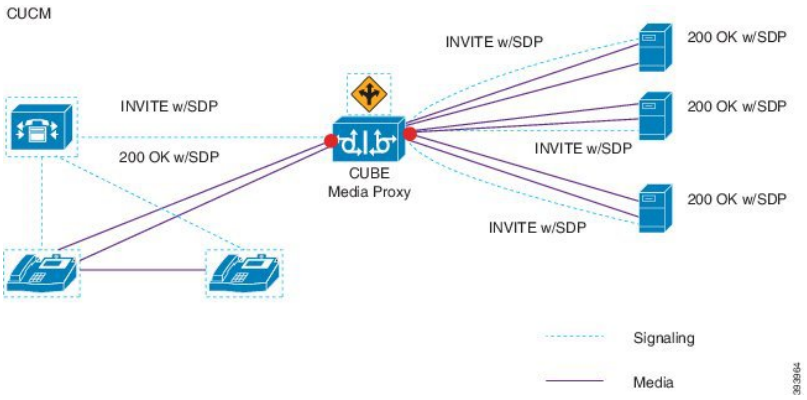
マルチフォーク録音を実装する場合、ネットワークで SIP トランク経由で Unified Communications Manager に接続する CUBE Media Proxy サーバを設定する必要があります。

詳細については、『Cisco Unified Border Element Configuration Guide』の「*CUBE Media Proxy*」のセクションを参照してください。

（注） SIP トランク経由で Unified Communications Manager から CUBE Media Proxy サーバに接続するには、Early Offer を使用して設定する必要があります。

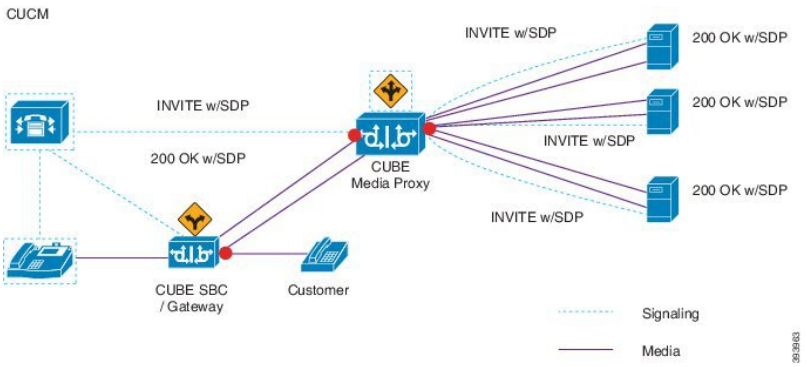
次の例は、CUBE Media Proxy を使用したマルチフォーク録音の電話ベースの録音を示しています。

図 *4*：電話ベースの録音



次の例は、CUBE Media Proxy を使用したマルチフォーク録音のネットワークベースの録音を示しています。

図 *5*：ネットワーク ベースの録音



この方法の概要については、『Cisco Unified JTAPI Developers Guide for Cisco Unified Communications ManagerRelease 12.5(1)』の「*Cisco Device-Specific Extensions*」セクションを参照してください。

サポートされるプラットフォーム

CUBE Media Proxy サーバ経由でのマルチフォーク録音は、Cisco IOS XE Gibraltar Release 16.10.1 が実行されている次の Cisco Router プラットフォームでサポートされます。

- Cisco 4000 シリーズ サービス統合型ルータ（ISRR G3 - ISR4331、ISR4351、ISR4431、ISR4451）。
- Cisco アグリゲーション サービス ルータ（ASR - ASR1001-X、ASR1002-X、ASR1004 with RP2、ASR1006 with RP2）。
- Cisco Cloud Services Router（CSR 1000V シリーズ）。

CUBE Media Proxy を使用したマルチフォーク録音の制約事項

CUBE Media Proxy サーバ経由でのマルチフォーク録音では、次の機能はサポートされません。

- ビデオ録画。
- 非セキュア コールのセキュア メディア（SRTP）分岐
- SRTP フォールバック。
- 通話中のブロック。

録音メディア ソースの選択

ネットワークベースの録音を設定すると、エージェントの電話回線の録音メディアの優先ソースとして電話またはゲートウェイを設定する必要があります。 ただし、展開方法によっては、Unified Communications Manager は録音メディア ソースとして望ましい選択肢を選択しない可能性があります。 次の表に、Unified Communications Manager が録音メディア ソースを選択する際のロジックを示します。

表 *18 :* 録音メディア ソースの選択

優先メディア ソース	メディア タイプ	コール パスのゲートウェイか?	選択された優先メディア ソース
ゲートウェイ（Gateway）	非セキュア（RTP）	可	ゲートウェイ（Gateway）
		不可	電話（Phone）
	セキュア（sRTP）	可	電話（Phone）
		不可	電話（Phone）
電話（Phone）	非セキュア（RTP）	可	電話（Phone）
		不可	電話（Phone）
	セキュア（sRTP）	可	電話（Phone）
		不可	電話（Phone）

最初の選択が利用できない場合の代替録音メディア ソース

Unified Communications Manager が選択する録音メディア ソースが使用不可の場合、Unified Communications Manager は代替ソースの利用を試みます。 次の表に、Unified Communications Manager が録音メディアの代替ソースを選択するために使用するロジックを示します。

表 *19* : 最初の選択が利用できない場合の代替録音メディア ソース

選択された優先メディア ソース	ゲートウェイを優先	電話を優先
最初の試行	コール パスの最初のゲートウェイ	電話（Phone）
2 番目の試行	コール パスの最後のゲートウェイ	コール パスの最初のゲートウェイ
3 番目の試行	電話（Phone）	コール パスの最後のゲートウェイ

録音の前提条件

- Cisco Unified IP 電話 サポート：録音をサポートしている Cisco Unified IP 電話 のリストを表示するには、Cisco Unified Reporting にログインして、[Unified CM Phone 機能一覧（Unified CM Phone Feature List）] レポートを実行し、機能として **[録音（Record）]** を選択します。詳細な手順については、電話機能一覧の生成 （5 ページ）を参照してください。
- ゲートウェイの対応機種：録音に対応しているゲートウェイの詳細については、https://developer.cisco.com/web/sip/wiki/-/wiki/Main/Unified+CM+Recording+Gateway+Requirementsを参照してください。
- マルチ ストリーム録音を設定する場合は、CUBE Media Proxy を展開して設定します。 詳細については、『Cisco Unified Border Element Configuration Guide』の「*CUBE Media Proxy*」のセクションを参照してください。

録音の設定タスク 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	録音プロファイルの作成 （166 ページ）	録音プロファイルを作成します。
ステップ 2	録音に使用する SIP プロファイルの設定（167 ページ）	**（オプション）** レコーダーに会議ブリッジ ID を提供する場合は、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 3	録音に使用する SIP トランクの設定 （168 ページ）	レコーダー サーバまたは CUBE Media Proxy を SIP トランク デバイスとして設定します。
ステップ 4	録音のルート パターンの設定 （169 ページ）	レコーダー サーバまたは CUBE Media Proxy にルーティングするルート パターンを作成します。
ステップ 5	録音のためのエージェント プロファイル回線の設定 （169 ページ）	録音用のエージェント電話回線を設定します。
ステップ 6	エージェントの電話のビルトインブリッジを有効にします。 次のいずれかのタスクを実行して、録音用のビルトインブリッジを有効にします。 • クラスタでの組み込みブリッジの有効化 （170 ページ） • 電話での組み込みブリッジの有効化 （170 ページ）	エージェントの電話を録音メディアのソースとして使用するには、電話のビルトイン ブリッジを録音用に有効にする必要があります。 サービス パラメータを使用して、ビルトイン ブリッジのデフォルトをクラスタ全体に設定したり、個々の電話のビルトイン ブリッジを有効にしたりできます。 （注） 個々の電話のビルトインブリッジの設定により、クラスタ全体のデフォルトがオーバーライドされます。
ステップ 7	録音向けのゲートウェイの有効化 （171 ページ）	ゲートウェイにユニファイド コミュニケーションのサービスを設定します。
ステップ 8	録音通知トーンの設定 （172 ページ）	通話の録音時に、通知音を再生するかどうかを設定します。
ステップ 9	電話で機能ボタンを使用するか、ソフトキーを使用するかに応じて、次のいずれかの手順を実行します。 • 録音機能ボタンの設定 （172 ページ） • [録音 （Record）] ソフトキーの設定 （174 ページ）	電話の [録音 （Record）] 機能ボタンまたはソフトキーを設定します。

録音プロファイルの作成

この手順を使用して、録音プロファイルを作成します。

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）] > [録音プロファイル（Recording Profile）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [名前（Name）]フィールドに、録音プロファイルの名前を入力します。

ステップ 4 [録音コーリング サーチ スペース（Recording Calling Search Space）]フィールドで、レコーディング サーバ用に設定されたルート パターンを持つパーティションを含むコーリング サーチ スペースを選択します。

ステップ 5 **[録音接続先アドレス（Recording Destination Address）]** フィールドに、録音サーバの電話番号または URL、または CUBE Media Proxy サーバの URL を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

録音に使用する SIP プロファイルの設定

この手順を使用して、会議ブリッジ ID をレコーダーに配信し、SIP プロファイルを設定します。

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。**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIP プロファイル（SIP Profile）]** の順に選択します。

ステップ 2 ネットワークに使用する SIP プロファイルを選択します。

ステップ 3 **[音声コールとビデオコールに対する早期オファーサポート（Early Offer Support for Voice and Video calls）]** フィールドの値を設定します。 Early Offer サポートのために、Unified Communications Manager から CUBE Media Proxy サーバへの SIP トランクを有効にする必要があります。設定オプションは、**[Best Effort（MTP の挿入なし）（Best Effort (no MTP inserted)）]** と **[Mandatory（必要に応じてMTPを挿入）（Mandatory (insert MTP if needed)）]** です。

（注） SIP トランクで [必須（必要に応じてMTPを挿入）（Mandatory (insert MTP if needed)）] を有効にすることをお勧めします。

ステップ 4 [会議ブリッジ ID を配信する（Deliver Conference Bridge Identifier）]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。

録音に使用する SIP トランクの設定

[**SIP トランクの設定 （SIP Trunk Configuration** ）] ウィンドウで録音サーバの情報を割り当てるには、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。**[デバイス(Device)]** > **[トランク(Trunk)]**。

ステップ 2 [新規追加] 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。

[**デバイス プロトコル（Device Protocol**）] が **SIP** に自動的に取り込まれます。これが使用可能な唯一のオプションです。

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から、ネットワークで使用するサービス タイプを選択します。 デフォルト値は [なし（None）] です。

ステップ 5 [次へ（Next）]をクリックします。

ステップ 6 **[SIP 情報（SIP Information）]** ペインの **[接続先アドレス（Destination Address）]** フィールドに、録音サーバまたは CUBE Media Proxy の IP アドレス、完全修飾ドメイン名、または DNS SRV を入力します。

ステップ 7 **[SIP 情報（SIP Information）]** ペインの **[SIP プロファイル（SIP Profile）]** ドロップダウン リストから、ネットワークで使用する SIP プロファイルを選択します。

ステップ 8 [**録画情報（Recording Information**）] ペインから、次のいずれかのオプションを選択します。

- なし—トランクは録音には使用されません。
- このトランクは録音対応ゲートウェイに接続します。
- このトランクは録音対応ゲートウェイのある他のクラスタに接続します。

ステップ 9 **[保存]** をクリックします。

（注） Unified Communications Manager から Media Proxy への SIP トランクに使用される SIP プロファイルで、このトランクが早期オファーサポートのために有効になっている必要があります。 設定オプションは [必須（必要に応じてMTPを挿入）（Mandatory (insert MTP if needed)）] と [ベストエフォート（MTPの挿入なし）（Best Effort (no MTP inserted)）] です。

録音のルート パターンの設定

この手順を使用して、レコーダーに固有のルート パターンの設定を説明します。 録音サーバまたは CUBE Media Proxy サーバにルーティングするルート パターンを設定する必要があります。

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）] > [ルート/ハント（Route/Hunt）] > [ルート パターン（Route Pattern）]**。

ステップ 2 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 **[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 通話録音するには、次のフィールドに値を入力します。

- [パターン（Pattern）]—録音プロファイルから録画宛先アドレスに一致するパターンを入力します。
- [ゲートウェイ/ルート リスト（Gateway/Route List）]—レコーディング サーバまでを示した SIP トランクまたはルート リストを選択します。

ステップ 5 **[保存（Save）]** をクリックします。

録音のためのエージェント プロファイル回線の設定

この手順を使用して、録音用のエージェント電話回線を設定します。

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。**[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 **[検索(Find)]** をクリックします。

ステップ 3 エージェントの電話を選択します。

ステップ 4 左側の [関連付け（Association）] ペインで、エージェントの電話回線をクリックして、設定を表示します。

ステップ 5 **[録音オプション（Recording Option）]** 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。

- [通話録音の無効化（Call Recording Disabled）]：この電話回線の通話は録音されません。

- [通話録音の自動有効化（Automatic Call Recording Enabled）]：この電話回線の通話はすべて録音されます。
- [通話録音の選択的有効化（Selective Call Recording Enabled）]：この電話回線の選択された通話のみ録音されます。

ステップ 6 [**録音プロファイル（Recording Profile**）] ドロップダウン リストから、エージェントに対して設定されている録音プロファイルを選択します。

ステップ 7 [**録音メディア ソース（Recording Media Source**）] ドロップダウン リストから、録音メディアの優先ソースとしてゲートウェイまたは電話を使用するかどうかを選択します。

ステップ 8 マルチレベル優先順位およびプリエンプション（MLPP）も設定している場合は、[**話中トリガー（Busy Trigger**）] フィールドを最小値の **3** に設定します。

ステップ 9 **[保存（Save）]** をクリックします。

クラスタでの組み込みブリッジの有効化

エージェントの電話を録音メディア ソースとして使用するには、この手順を使用して、電話のビルトイン ブリッジを有効にします。

組み込みブリッジのクラスタ全体のサービスパラメータを有効に設定すると、クラスタ内のすべての電話で組み込みブリッジのデフォルト設定が有効に変わります。ただし、個々の電話の [電話の設定（Phone Configuration）]ウィンドウでの [組み込み型ブリッジ（Built-in-Bridge）] の設定は、該当する電話でデフォルト オプションが選択されていない場合、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。

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）]**。

ステップ 2 [サーバ（Server）]ドロップダウン リストから、CallManager サービスが実行され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 [有効な組み込みブリッジ（Builtin Bridge Enable）]サービス パラメータを [オン（On）]に設定します。

ステップ 5 **[保存（Save）]** をクリックします。

電話での組み込みブリッジの有効化

個々の電話機で組み込みブリッジを有効にするには、次の手順を使用します。デフォルトのオプションが選択されていない場合、[電話機の設定（Phone Configuration）] ウィンドウの [組み

込みブリッジ設定（Built in Bridge setting）] がクラスタ全体のサービス パラメータを上書きします。

必要に応じて、サービスパラメータを使用して、クラスタ全体での組み込みブリッジのデフォルトを設定します。詳細については、クラスタでの組み込みブリッジの有効化 （170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。**[デバイス] > [電話]**

ステップ 2 **[検索 （Find ）]** をクリックして、エージェントの電話を選択します。

ステップ 3 [組み込みブリッジ（Built in Bridge）]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。

- [オン（On）] : 組み込みブリッジが有効になります。
- [オフ（Off）] : 組み込みブリッジが無効になります。
- [デフォルト（Default）] : [組み込みブリッジの有効化（Builtin Bridge Enable）]クラスタ全体サービス パラメータの設定が使用されます。

（注） レコーディングは、**Built-in-Bridge** がオンで、**[メディアターミネーション ポイントが必要]** チェックボックスをオンにすると失敗する可能性があります。

ステップ 4 **[保存（Save）]** をクリックします。

録音向けのゲートウェイの有効化

この手順を使用して、録音のためのゲートウェイを設定します。 ユニファイド コミュニケーション ゲートウェイ サービスを有効にする必要があります。 次のタスク フローには、ユニファイド コミュニケーション ゲートウェイ サービスを有効にするためのプロセスの概要が含まれています。

手順

ステップ 1 デバイスで Unified Communications Manager IOS サービスを設定します。

ステップ 2 XMF プロバイダーを設定します。

ステップ 3 ユニファイド コミュニケーション ゲートウェイ サービスを確認します。

例を含む詳細な設定手順については、次のいずれかのドキュメントの「Cisco Unified Communications ゲートウェイ サービス」の章を参照してください。

- ASR ルータの詳細については、『Cisco Unified Border Element （Enterprise） Protocol-Independent Features and Setup Configuration Guide』を参照してください。 Cisco IOS XE リリース 35。
- ISR ルータの詳細については、『Cisco Unified Border Element Protocol-Independent Features and Setup Configuration Guide, Cisco IOS Release 15M&T』を参照してください。

録音通知トーンの設定

この手順を使用して、通話の録音時に、通知音を再生するかどうかを設定します。 法的なコンプライアンスのため、周期的なトーンの形で明確な通知をエージェント、発信者、またはその両方に聴覚的に伝達し、録音セッションが進行中であることを示すことができます。 このトーンを無効にすることもできます。

（注） 録音トーンとモニタリング トーンの両方の設定が同じコールに対して有効になっている場合、録音トーンの設定は、モニタリング トーン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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

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 通知トーンをエージェントに対して再生するには、**[録音通知トーンを監視対象のターゲット（エージェント）に対して再生する（Play Recording Notification Tone to Observed Target (agent)）]** サービス パラメータを **[True]** に設定します。

ステップ 5 通知トーンを顧客に対して再生するには、**[録音通知トーンを監視対象の接続済み参加者（顧客）に対して再生する（Play Recording Notification Tone To Observed Connected Parties (customer)）]** サービス パラメータを **[True]** に設定します。

ステップ 6 **[保存（Save）]** をクリックします。

録音機能ボタンの設定

電話が機能ボタンを使用する場合は、この手順を使用して、録音機能ボタンを電話に割り当てます。

手順

	コマンドまたはアクション	目的
ステップ 1	録音の電話ボタン テンプレートの設定（173 ページ）	[録音（Record）] ボタンを含む電話ボタン テンプレートを設定します。
ステップ 2	電話と電話ボタン テンプレートの関連付け （174 ページ）	録音用に作成した電話ボタンテンプレートを電話に関連付けます。

録音の電話ボタン テンプレートの設定

この手順を使用して、録音機能ボタンを含む電話ボタン テンプレートを作成します。

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）]** > **[電話ボタンテンプレート（Phone button template）]** の順に選択します。

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]** 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]** をクリックします。

ステップ 7 次のいずれかの作業を実行します。

- 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。

電話と電話ボタン テンプレートの関連付け

この手順を使用して、電話の [録音（Record）] ボタン用に作成した電話ボタン テンプレートを関連付けます。

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、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]** 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。

[録音（Record）] ソフトキーの設定

電話機がソフトキーを使用している場合は、次の手順を使用して電話機に [録音 （Record）] ソフトキーを追加します。 [録音（Record）] ソフトキーは機能ハードキー テンプレートを備えた Cisco Chaperone Phone に接続されたコールの状態にのみ使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	録音のソフトキー テンプレートの設定（175 ページ）	[録音（Record）] ソフトキーが含まれたソフトキーテンプレートを設定します。
ステップ 2	次のいずれかの手順を実行します。 • 電話機とソフトキー テンプレートの関連付け （176 ページ） • 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 （176 ページ）	ソフトキーテンプレートを電話に直接、または共通デバイス設定に関連付けます。 そのあとに、共通デバイス設定を電話機のグループに関連付けることができます。

録音のソフトキー 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）] > [ソフトキー テンプレート（Softkey Template）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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。

電話機とソフトキー テンプレートの関連付け

この手順を使用して、[録音（Record）] ソフトキーが含まれているソフトキーテンプレートを電話機に直接関連付けることによって、電話機に [録音（Record）] ソフトキーを割り当てることができます。

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。

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

この手順を使用して、共通デバイス設定にソフトキーテンプレートを関連付けることにより、電話に [録音（Record）] ソフトキーを追加します。

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ソフトキー テンプレートの追加 （177 ページ）	
ステップ 2	電話への共通デバイス設定の追加 （177 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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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。

電話への共通デバイス設定の追加

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）] > [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。

録音コール フローの例

ネットワークベースのコール録音と IP フォンベースのコール録音の両方のコール フローの例については、次の URL にある「*Call Recording Examples for Network-Based and Phone-Based Recording*」を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/configExamples/cucm_b_recording-use-cases.html

録音の連携動作と制約事項

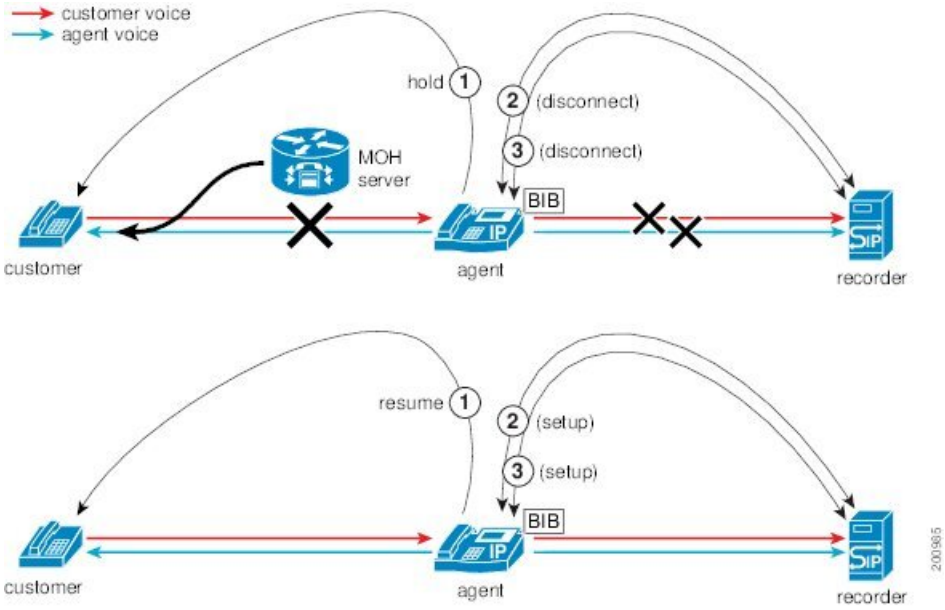
機能	連携動作と制限事項
モニタリング トーン（Monitoring Tones）	録音およびモニタリングされるコールに関しては、録音トーンがモニタリング トーンよりも優先されます。 両方が設定されていて、コールの録音およびモニタリングの両方が行われる場合、録音トーンが再生されます。
複数レベルの優先順位とプリエンプション	また、マルチレベルの優先およびプリエンプションも設定している場合、録音を行うエージェント電話回線の [ビジー トリガー（Busy Trigger）]の設定は少なくとも 3 に設定する必要があります。
セキュア トーン	セキュア トーンが設定されている場合、録音トーンが設定されているかどうかに関わらず、通話の両側でセキュア コールの最初にセキュア トーンが再生されます。 セキュア トーンと録音トーンの両方が設定されていてコールがセキュアである場合、コールの最初にセキュア トーンが 1 回再生され、続いて録音トーンが再生されます。 セキュア トーン、録音トーン、モリタリング トーンのすべてが設定されており、コールがセキュアで録音とモニタリングが行われる場合、セキュア トーンが 1 回再生され、続いて録音トーンが再生されます。 モニタリング トーンは再生されません。
Customer Voice Portal	エージェント：Customer Voice Portal を経由してルーティングされる顧客のコールは、エージェントの電話機を録音ソースとして使用して録音できます。
SIP プロキシ サーバ	ゲートウェイを録音ソースとして使用している場合、Unified Communications Manager とゲートウェイの間に SIP プロキシ サーバを配置することはできません。

機能	連携動作と制限事項
Busy Hour Call Completion レート（Busy Hour Call Completion Rate）	録音のセッションはそれぞれ Busy Hour Call Completion（BHCC）のレートに 2 コールを追加し、CTI リソースへの影響を最小限に抑えます。
Media Sense を使用した選択的な録音	選択的な録音が設定されている場合、Media Sense サーバでは転送中のコンサルト コールは録音されません。 たとえば、エージェントと顧客間のコールが録音中であり、エージェントが次のエージェントにコールの転送を開始した場合、コールが転送される前にこの 2 つのエージェント間で発生するコンサルト コールは録音されません。 コンサルト コールが必ず録音されるようにするには、エージェントはコンサルト コールの開始時に [録音（Record）] ソフトキーを押す必要があります。
認証された電話での録音	認証された電話の通話を録音するには、Cisco Unified CM Service の [パラメータ（Parameter）] ページで、[認証済み電話の録音（Authenticated Phone Recording）]フィールドを [録音の許可（Allow Recording）]に設定します。 デフォルト値は **[録音を許可しない（Do Not Allow）]** です。Unified Communications Manager は、非セキュア レコーダーを使用しているときに、認証された電話機のコール録音を許可します。 安全なレコーダーの場合、レコーダーが Secure Real-Time Transport protocol（SRTP）フォールバックをサポートしている場合にのみ、録音できます。
会議の選択と参加でのコールの自動録音のためのコーデック ロック	Skinny Client Control Protocol（SCCP）電話は、録音が有効であり、Unified Communications Manager で会議の選択と参加が実行されると、1 つのコーデックをアドバタイズします。

エージェントがコールを保留にすると録音コールは存続しない

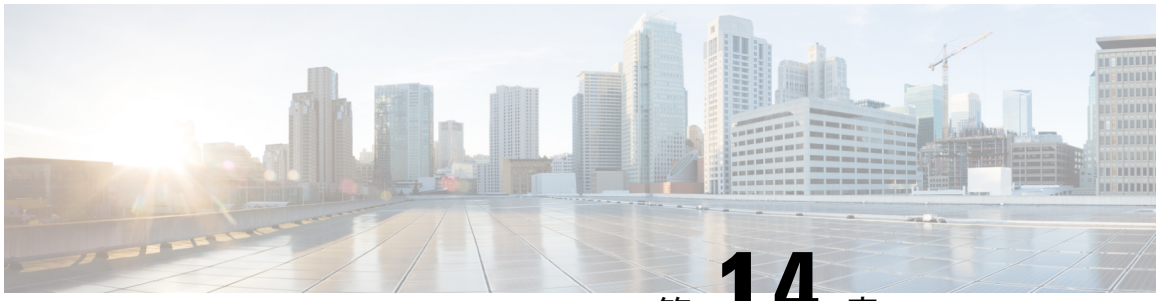
エージェントがコールを保留にすると録音コールは中断され、エージェントがコールを再開すると録音コールが再開されます。

図 *6:* エージェントがコールを保留にすると録音コールは存続しない



第 VI 部

コール センター機能



第 14 章

エージェントのグリーティング

エージェント グリーティングの概要

エージェント グリーティングにより、Unified Communications Manager は、エージェント デバイスへのメディア接続が成功した後で、録音済みのアナウンスを自動的に再生できます。エージェント グリーティングは、エージェント側にもカスタマー側にも聞こえます。

グリーティングの録音プロセスは、ボイスメールのメッセージの録音に似ています。コンタクトセンターのセットアップ方法に応じて、発信者のタイプごとに再生される異なるグリーティングを録音できます（たとえば、英語を話す人には英語のグリーティング、イタリア語を話す人にはイタリア語のグリーティングなど）。

デフォルトでは、エージェント デスクトップにログインするときにエージェント グリーティングが有効になりますが、必要に応じてオフまたはオンにできます。

エージェント グリーティングの前提条件

- Cisco Unified Contact Center Enterprise のインストール。『Cisco Unified Contact Center Enterprise Installation and Upgrade Guide』を参照してください。
- Cisco Unified Customer Voice Portal のインストール。『Installation and Upgrade Guide for Cisco Unified Customer Voice Portal』を参照してください。
- ビルトインブリッジを有効にしてください。詳細を表示するには、ビルトインブリッジの設定 （185 ページ）を参照してください。

エージェントのグリーティング設定のタスク フロー

エージェントのグリーティング設定タスクは、Cisco Unified Contact Center Enterprise（Unified CCE）および Cisco Unified Customer Voice Portal（Unified CVP）で完了します。 次のタスクの詳細な手順を表示するには、『Cisco Unified Contact Center Enterprise Features Guide』の「Agent Greeting」セクションを参照してください。

始める前に

- エージェント グリーティングの前提条件 （183 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	エージェントのグリーティングのメディア サーバを設定します。 • メディア サーバとして機能するサーバを設定します。 • Unified CVP でメディア サーバを追加します。 • ファイルを記述するメディア サーバを設定します。	エージェントのグリーティングは Unified CVP メディア サーバを使用して、プロンプトおよびグリーティング ファイルを格納して提供します。
ステップ 2	Voice Extensible Markup Language（VXML）ゲートウェイに .tcl スクリプトを再パブリッシュします。	Unified CVP Release 9.0(1) と共に出荷される .tcl スクリプト ファイルには、エージェントのグリーティングをサポートするための更新が含まれています。 これらの更新されたファイルを VXML ゲートウェイに再パブリッシュする必要があります。 VXML ゲートウェイへのスクリプトの再パブリッシュは Unified CVP アップグレードでの標準作業です。 Unified CVP のアップグレードとスクリプトの再パブリッシュを行わなかった場合、エージェントのグリーティングを使用する前にスクリプトを再パブリッシュする必要があります。
ステップ 3	VXML ゲートウェイのキャッシュ サイズを設定します。	十分なパフォーマンスを保証するには、VXML ゲートウェイで最大に許容されるキャッシュのサイズを設定しま

	コマンドまたはアクション	目的
		す。 最大サイズは 100 メガバイトです。デフォルトは15キロバイトです。VXML ゲートウェイで最大に許容されるキャッシュのサイズの設定に失敗すると、メディア サーバへのトラフィックの増加に対するパフォーマンスが遅くなる可能性があります。
ステップ 4	グリーティングを録音するためのボイス プロンプトを作成します。	エージェントがグリーティングの録音時に聞く各ボイス プロンプトのオーディオ ファイルを作成します。
ステップ 5	コール タイプを設定します。	エージェントのグリーティングの録音および再生を完了します。
ステップ 6	着信番号を設定します。	エージェントのグリーティングの録音および再生を完了します。
ステップ 7	スクリプトをスケジュールします。	
ステップ 8	ネットワーク VRU スクリプトを定義します。	Unified CVP と対話するためのエージェントのグリーティング レコードとプレイ スクリプトの場合、ネットワーク VRU スクリプトが必要です。
ステップ 9	（オプション）サンプルのエージェント グリーティングのスクリプトをインポートします。	
ステップ 10	Unified CCE コール ルーティング スクリプトを変更します。	エージェント グリーティングの再生スクリプトを使用するために Unified CCE コール ルーティング スクリプトを変更します。

ビルト イン ブリッジの設定

個々の電話の **[電話の設定（Phone Configuration）]** ウィンドウの **[組み込みブリッジ（Built in Bridge）]** フィールドの設定は、**[組み込みブリッジの有効化（Builtin Bridge Enable）]** クラスタ全体サービス 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）]** > **[電話（Phone）]**。

ステップ 2 **[検索 （Find ）]** をクリックして、エージェントの電話を選択します。

ステップ 3 [組み込みブリッジ（Built in Bridge）]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。

- [オン（On）]：組み込みブリッジが有効になります。
- [オフ（Off）]：組み込みブリッジが無効になります。
- [デフォルト（Default）]：[組み込みブリッジの有効化（Builtin Bridge Enable）]クラスタ全体サービス パラメータの設定が使用されます。

ステップ 4 **[保存（Save）]** をクリックします。

エージェントグリーティングのトラブルシューティング

エージェント グリーティングの問題をトラブルシューティングする方法については、『Agent Greeting and Whisper Announcement Feature Guide for Cisco Unified Contact Center Enterprise Guide』の「「Troubleshooting Agent Greeting」」の章を参照してください。

第 15 章

自動応答

自動応答の概要

自動応答により、発信者は受付と対話せずに組織内のユーザを見つけることができます。 発信者に対して再生される音声ガイダンスをカスタマイズできます。

自動応答は Unified Communications Manager と連携して、特定の内線番号へのコールを受信します。 このソフトウェアは、発信者と対話し、連絡しようとしている組織内の通話相手の内線番号を発信者が検索して選択できるようにします。

自動応答には次の機能があります。

- 通話に応答します。
- ユーザが設定可能なウェルカム音声ガイダンスを再生します。
- 発信者に次の 3 つのアクションの 1 つを実行するように求めるメイン メニューの音声ガイダンスを再生します。
  - オペレータにつなぐ場合は「0」を押します。
  - 内線番号を入力する場合は「1」を押します。
  - 名前をスペルで入力する場合は「2」を押します。

    発信者が名前をスペルで入力することを選択した場合（2 を押した場合）、システムは入力された文字を、使用可能な内線番号に設定されている名前と比較します。 結果は次のいずれかになります。
    - 一致する名前が存在する場合、システムは一致したユーザへの転送をアナウンスし、発信者がデュアルトーン多重周波数（DTMF）キーを押して転送を停止できるよう 2 秒間待機します。 発信者が転送を停止しない場合は、明示的な確認を行

います（名前を確認する音声ガイダンスを再生し、そのユーザのプライマリ エクステンションにコールを転送します）。

- 複数のユーザに一致した場合、システムは正しい内線番号を選択するよう発信者に求めます。
- 非常に多くのユーザが一致する場合、システムはさらに文字を入力するよう発信者に求めます。
- 一致する名前が存在しない場合、つまりユーザが誤ったオプションを押した場合には、システムは音声ガイダンスでユーザが誤ったオプションを押したことを通知し、ユーザに対し正しいオプションを押すように指示します。

- 発信者が接続先を指定した場合、システムはコールを転送します。
- 回線が通話中であるか、現在使用されていない場合、システムは発信者に通知し、メインメニューの音声ガイダンスを再生します。

自動応答ソリューションは、次のように、自動音声応答機能を備えたさまざまなシスコ製品を使用して 3 通りの方法で導入できます。

- Cisco Unity Connection（CUC）を使用した自動応答：顧客に最も広く利用されている自動応答ソリューション構成です。
- Cisco Unified Contact Center Express（Unified CCX）を使用した自動応答
- Cisco Unity Express（CUE）を使用した自動応答

Cisco Unity Connection の設定

Cisco Unity Connection サーバは、外部発信者と内部発信者の両方に自動応答機能を提供します。 自動応答機能では、オペレータや受付が介入することなく、発信者が内線番号に自動で転送されます。

自動応答機能にはメニューシステムがあります。また、発信者が特定の番号（通常は「「0」」）をダイヤルして実際のオペレータに接続することもできます。 個々のサイト ロケーションをサポートするために、複数の自動応答機能を実装できます。 Cisco Unity Connection では、自動応答はカスタム アプリケーション ツリー構造になっています。この構造は、複数のコール ハンドラを作成してリンクすることで作成されます。 自動応答は、入力点と出口点、および発信者が選択する DTMF 入力に基づく中間ルーティング決定によって定義されます。

自動応答のデフォルトの動作と例の詳細については、『System Administration Guide for Cisco Unity Connection』を参照してください。

Cisco Unity Connection の設定タスク フロー

このタスク フローを使用して、Cisco Unity Connection を使用する自動応答を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	CTI ルート ポイントの設定 （190 ページ）	[Cisco Unified CM の管理（Cisco Unified CM Administration）] で、このタスクを実行します。 企業のダイヤルイン（DID）番号（ボード番号）にマッピングする CTI ルート ポイントを作成します。
ステップ 2	自動応答システム コール ハンドラの設定 （191 ページ）	コール ハンドラは、コールへの応答、録音済みプロンプトによる発信者へのグリーティング、発信者への情報およびオプションの提供、コールのルーティング、およびメッセージの取得を行います。 （注） **[編集（Edit）]>[グリーティング（Greetings）]** の順に選択することによって、自動応答コール ハンドラのグリーティングをカスタマイズできます。 グリーティングのカスタマイズの詳細については、『System Administration Guide for Cisco Unity Connection』 を参照してください。
ステップ 3	発信者入力オプションの設定 （191 ページ）	発信者入力オプションを使用すると、ユーザの内線番号、緊急連絡先番号、コール ハンドラ、インタビュー ハンドラ、またはディレクトリ ハンドラを表す単一の数字を指定できます。 発信者が完全な内線番号を入力する代わりに、コール ハンドラ グリーティングの途中で単一のキーを押すと、それに応じて Cisco Unity Connection が応答します。 さまざまな異なるキーを発信者入力オプションとして設定することで、コール ハンドラ グリーティングで発信者に選択メニューが提供されます。
ステップ 4	オペレータ コール ハンドラの内線番号の設定 （192 ページ）	コール ハンドラ グリーティング中に発信者がオペレータと会話できるようにするには、オペレータの内線番号を設定します。

	コマンドまたはアクション	目的
ステップ 5	オペレータの標準コール転送ルールの変更 （192 ページ）	発信者がオペレータと会話するために 0 を押したときにコールがオペレータに転送されるようにするには、標準コール転送ルールを変更します。
ステップ 6	デフォルトのシステム転送規制テーブルの更新 （193 ページ）	デフォルトのシステム転送規制テーブルを更新します。 デフォルトのシステム転送規制テーブルでは、識別できない発信者を指定した番号に転送するための発信者システム転送に使用できる番号を制限します。

CTI ルート ポイントの設定

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）] > [CTI ルート ポイント（CTI Route Point）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [デバイス名（Device Name）]フィールドに、ルート ポイントのデバイス名を入力します

ステップ 4 [デバイス プール（Device Pool）]ドロップダウン リストから、[デフォルト（Default）]を選択します。

ステップ 5 **[保存]** をクリックします。
「Add successful」というメッセージが表示されます。

ステップ 6 **[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。
[ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウが表示されます。

ステップ 7 [ディレクトリ番号（Directory Number）]フィールドに、会社の DND と一致する電話番号を入力します。

ステップ 8 [ルート パーティション（Route Partition）]ドロップダウン リストから、必要なルート パーティションを選択します。

ステップ 9 [コール転送とコール ピックアップの設定（Call Forward and Call Pickup Settings）]エリアで、[すべて転送（Forward All）]に関して、適切なコーリング サーチ スペースを選択し、[ボイスメール（Voice Mail）]チェックボックスをオンにします。

ステップ 10 **[保存（Save）]** をクリックします。

自動応答システム コール ハンドラの設定

手順

ステップ 1 Cisco Unity Connection の管理で、左側の [Cisco Unity Connection] ツリーから、[コール管理（Call Management）] に移動し、[システム コール ハンドラ（System Call Handlers）] を選択します。

ステップ 2 [新規追加] をクリックします。
[**新しいコールハンドラ（New Call Handler**）] ウィンドウが表示されます。

ステップ 3 [**表示名（Display Name**）] フィールドに「**AutoAttendant**」と入力します。

ステップ 4 [**拡張（Extension**）] フィールドに、CTI ルート ポイントに関して指定したものと同じ内線番号を入力します。

ステップ 5 **[保存]** をクリックします。
[コール ハンドラの基本設定の編集（自動アテンダント）（Edit Call Handler Basics (AutoAttendant)）] ウィンドウが表示されます。

ステップ 6 必須フィールドを編集して [**保存（Save**）] をクリックします。

発信者入力オプションの設定

手順

ステップ 1 Cisco Unity Connection の管理で、左側の [Cisco Unity Connection] ツリーから、[コール管理（Call Management）] に移動し、[システム コール ハンドラ（System Call Handlers）] を選択します。

ステップ 2 [AutoAttendant]をクリックします。
[コール ハンドラの基本設定の編集（自動アテンダント）（Edit Call Handler Basics (AutoAttendant)）] ウィンドウが表示されます。

ステップ 3 **[編集（Edit）]** > **[発信者入力（Caller Inputs）]** を選択します。
[発信者入力（Caller Input）]ウィンドウが表示されます。

ステップ 4 **[キー（Key）]** 列で **[0]** をクリックします。
[発信者入力の編集（0）（Edit Caller Input (0)）]ウィンドウが表示されます。

ステップ 5 [コール ハンドラ（Call Handler）]オプション ボタンをクリックし、ドロップダウン リストから [オペレータ（Operator）]を選択して、[転送試行（Attempt Transfer）]オプション ボタンをクリックします。

ステップ 6 **[保存]** をクリックします。
「更新された発信者入力（`Updated Caller Input`）」ステータス メッセージが表示されます。

ステップ 7 **[編集（Edit）]** > **[発信者入力（Caller Inputs）]** を選択します。
[発信者入力（Caller Input）]ウィンドウが表示されます。

ステップ 8 **[キー（Key）]** 列で **[1]** をクリックします。

[発信者入力の編集（0）（Edit Caller Input (0)）]ウィンドウが表示されます。

ステップ 9 [メッセージ交換（Conversation）]オプション ボタンで、ドロップダウン リストから [発信者のシステム転送（Caller System Transfer）]を選択します。

ステップ 10 **[保存（Save）]** をクリックします。
「更新された発信者入力（Updated Caller Input）」ステータス メッセージが表示されます。

オペレータ コール ハンドラの内線番号の設定

手順

ステップ 1 Cisco Unity Connection の管理で、左側の [Cisco Unity Connection] ツリーから、[コール管理（Call Management）] に移動し、[システム コール ハンドラ（System Call Handlers）] を選択します。

ステップ 2 [オペレータ（Operator）] をクリックします。
[コール ハンドラの基本設定の編集（Edit Call Handler Basics）]（オペレータ）ウィンドウが表示されます。

ステップ 3 オペレータの内線番号を [内線番号（Extension）]フィールドに入力し、[保存（Save）]をクリックします。
「更新された発信者入力（Updated Caller Input）」ステータス メッセージが表示されます。

オペレータの標準コール転送ルールの変更

手順

ステップ 1 Cisco Unity Connection の管理で、左側の [Cisco Unity Connection] ツリーから、[コール管理（Call Management）] に移動し、[システム コール ハンドラ（System Call Handlers）] を選択します。

ステップ 2 [オペレータ（Operator）] をクリックします。
[コール ハンドラの基本設定の編集（Edit Call Handler Basics）]（オペレータ）ウィンドウが表示されます。

ステップ 3 [編集（Edit）]メニューで、[転送ルール（Transfer Rules）]を選択します。
[転送ルール（Transfer Rules）]ウィンドウが表示されます。

ステップ 4 [標準（Standard）]をクリックします。
[転送ルールの編集（標準）（Edit Transfer Rule (Standard)）]ウィンドウが表示されます。

ステップ 5 [コールの転送先（Transfer Calls to）]オプションで、[内線（Extension）]オプション ボタンをクリックしてから、設定したオペレータ内線番号を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

デフォルトのシステム転送規制テーブルの更新

手順

ステップ 1 Cisco Unity Connection Administration の左側にある Cisco Unity Connection ツリーで、[システム設定（System Settings）]に移動し、[規制テーブル（Restriction Tables）]を選択します。

ステップ 2 [デフォルトのシステム転送（Default System Transfer）]をクリックします。
[規制テーブルの基本の編集（デフォルトのシステム転送）（Edit Restriction Table Basics (Default System Transfer)）]ウィンドウが表示されます。

ステップ 3 **[順番（Order）]** 列の 6 に関して **[ブロック（Blocked）]** 列のチェック 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。

Cisco Unity Connection 自動応答のトラブルシューティング

Cisco Unity Connection を使用した自動応答のトラブルシューティングの詳細については、次の参照先を参照してください。

- http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/107517-calltrf.html
- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/troubleshooting/guide/8xcuctsgx/8xcuctsg110.html
- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/troubleshooting/guide/8xcuctsgx/8xcuctsg040.html
- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/troubleshooting/guide/8xcuctsgx/8xcuctsg180.html

Cisco Unified CCX の設定

自動応答は、Cisco Unified Contact Center Express（統合 CCX）の 5 シート バンドルに標準として組み込まれています。

（注） Unified Communications Manager でサポートされている Cisco Unified CCX のバージョンについては、『Cisco コラボレーション システム リリース サマリー マトリックス』を参照してください。

スクリプトの概要については、『Cisco Unified Contact Center Express Getting Started with Scripts』を参照してください。

Cisco Unified CCX の前提条件

- 自動応答を使用する前に、Cisco Unified CCX をインストールして設定する必要があります。 Cisco Unified CCX は、ソフトウェアと、このソフトウェアからテレフォニー システムへの接続を制御します。
- Unified Communications Manager でユーザを設定します。

Cisco Unified CCX 自動応答タスク フロー

自動応答の設定タスクは Cisco Unified Contact Center Express（Unified CCX）で完了します。 次のタスクの詳細な手順を表示するには、『Cisco Unified CCX Administration Guide』および『Cisco Unified Contact Center Express Getting Started with Scripts』をそれぞれ参照してください。

始める前に

- 自動応答機能については、自動応答の概要 （187 ページ）を確認してください。
- 自動応答機能を備える Cisco UCCX の詳細については、以下を確認してください。Cisco Unified CCX の設定 （193 ページ）
- Cisco Unified CCX の前提条件 （194 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 CM Telephony のコール コントロール グループを設定します。	Unified CCX システムは Unified CM Telephony コール制御グループを使用して、Unified CCX サーバが発着信するコールの対応に使用する一連の CTI ポートをまとめてプールします。
ステップ 2	Cisco Media Termination（CMT）ダイアログ コントロール グループを追加します。	Cisco Media サブシステムは、Unified CCX Engine のサブシステムです。 Cisco Media サブシステムは、CMT メディア リソースを管理します。 CMT チャネルは、Unified CCX がメディアを再生または録音するのに必要です。 Cisco Media サブシステムは、ダイアログ グループを使用してアプリケーション間のリソースを整理して共有します。

	コマンドまたはアクション	目的
		ダイアログ グループはダイアログ チャネルのプールです。そのプールでは、各チャネルが発信者とのダイアログ対話を実行するために使用されます。その間に、発信者はタッチトーン電話のボタンを押すことで自動プロンプトに応答します。 **注意** すべてのメディア ターミネーション文字列は 「auto」 で始まり、コール制御グループと同じ ID が含まれます（CMT ダイアログ グループではなく）。 デフォルトのメディア ターミネーションが設定され、ID が異なる場合、次の手順を実行します。
ステップ 3	Cisco スクリプト アプリケーションを設定します。	Unified CCX スクリプト アプリケーションは、Unified CCX Editor で作成したスクリプトに基づくアプリケーションです。 これらのアプリケーションは、すべての Unified CCX システムに付属しており、Unified CCX Editor で作成したスクリプトを実行します。
ステップ 4	Unified CM Telephony トリガーをプロビジョニングします。	Unified CM Telephony トリガーは、コールに対応するテレフォニーおよびメディア リソースを選択してコールを処理するアプリケーション スクリプトを起動することで、特定のルート ポイントに着信したコールに応答します。
ステップ 5	自動応答をカスタマイズします。 • 既存の自動応答インスタンスを変更します。 • 自動応答プロンプトを設定します。	[Cisco Unified CCX Administration] ページを使用すると、既存の自動応答インスタンスを必要に応じて変更できます。 Cisco Unified CCX により、Cisco Unified CCX Administration の [メディアの設定（Media Configuration）] ウィンドウの自動応答プロンプトをカスタマイズできます。 ここでは、ウェルカム音声ガイダンスの録音、ウェルカム プロンプトの設定、音声名のアップロードが可能です。

Cisco Unity Express の設定

Cisco Unity Express を使用した自動応答設定については、『Cisco Unity Express VoiceMail and Auto Attendant CLI Administrator Guide for 3.0 and Later Versions』の「「Configuring Auto Attendants」」の章を参照してください。

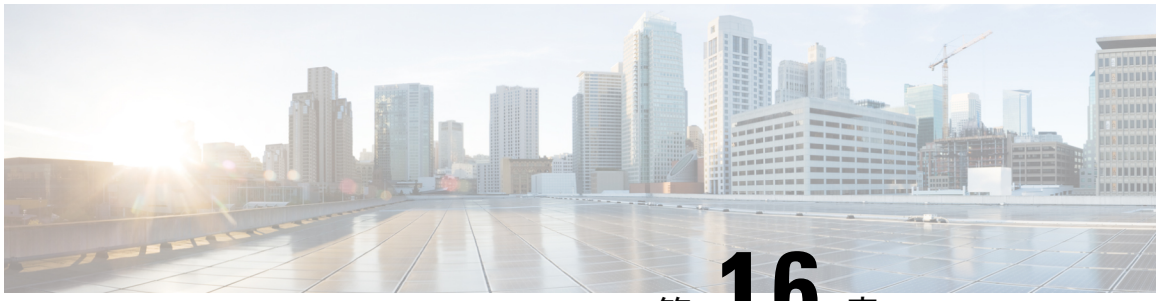
サンプル自動応答スクリプトの導入については、『Getting Started with Cisco Unified IP IVR』の「「Deployment of sample script aa.aef」」の章を参照してください。

自動応答の例については、『Cisco Unity Express Guide to Writing and Editing Scripts for 7.0 and Later Versions』の「「Auto Attendant Script Example」」の章を参照してください。

自動応答の設計に関する考慮事項については、『Cisco Unity Express Design Guide』の「「Auto Attendant Design Considerations」」の章を参照してください。

Cisco Unity Express 自動応答のトラブルシューティング

Cisco Unity Connection を使用した自動応答のトラブルシューティングについては、『Excerpts from Cisco IP Communications Express: CallManager Express with Cisco Unity Express』の「「Troubleshooting Cisco Unity Express Automated Attendant」」を参照してください。



第 16 章

Manager Assistant

Cisco Unified Communications Manager Assistant の概要

Unified Communications Manager Assistant 機能は、アシスタントがマネージャの代理でコールを処理し、マネージャ コールを代行受信して適切にルーティングするために使用できるプラグインです。

Manager Assistant では最大 3500 人のマネージャと 3500 人のアシスタントがサポートされています。 このユーザ数に対応するため、1 つの Unified Communications Manager クラスタで最大 3 つの Manager Assistant アプリケーションを設定し、マネージャとアシスタントを各アプリケーション インスタンスに割り当てることができます。

Manager Assistant では、共有回線とプロキシ回線がサポートされています。

Manager Assistant のアーキテクチャ

Manager Assistant のアーキテクチャは次の項目で構成されています。

- **Cisco IP Manager Assistant サービス**：Unified Communications Manager のインストール後に、Cisco Unified Serviceability インターフェイスからこのサービスをアクティブにします。
- **Assistant Console インターフェイス**：アシスタントが各自のコンピュータから Manager Assistant の機能にアクセスして、マネージャのコールを処理できます。 Manager Assistant は、アシスタント宛のコールと最大 33 人のマネージャ宛のコールを処理します。
- **Cisco Unified IP 電話インターフェイス**：マネージャとアシスタントはソフトキーと [Cisco Unified IP 電話Services] ボタンを使用して、Manager Assistant の機能にアクセスできます。

詳細については、『Feature Configuration Guide for Cisco Unified Communications Manager』の「Manager Assistant」の章を参照してください。

Manager Assistant データベース アクセス アーキテクチャ

データベースには、Manager Assistant 設定情報がすべて保管されています。マネージャまたはアシスタントがログインすると、Cisco IP Manager Assistant サービスはそのマネージャとアシスタントに関連するすべてのデータをデータベースから取得し、メモリに格納します。このデータベースには 2 種類のインターフェイスがあります。

- **マネージャ インターフェイス**：マネージャの電話で、[マネージャの設定（Manager Configuration）] 以外のマネージャ機能を使用できます。Cisco IP Manager Assistant サービスの開始時に、Manager Assistant によりマネージャは Cisco IP Manager Assistant サービスに自動でログインします。

（注） マネージャは、サイレントや即時転送などの Unified Communications Manager 機能にもアクセスできます。

- **アシスタント インターフェイス**：アシスタントは、アシスタント コンソール アプリケーションと Cisco Unified IP 電話 を使用して Manager Assistant 機能にアクセスします。Assistant Console アプリケーションは、応答、転送、保留などのコール制御機能を提供します。アシスタントは Assistant Console を使用して、ログインとログアウト、アシスタント設定、および[マネージャの設定（Manager Configuration）]ウィンドウ（マネージャ設定に使用）の表示を行います。

詳細については、『Feature Configuration Guide for Cisco Unified Communications Manager』の「Manager Assistant」の章を参照してください。

ソフトキー

Manager Assistant では次のソフトキーがサポートされています。

- リダイレクト
- ボイスメールへの転送
- 取り込み中

Manager Assistant では次のソフトキー テンプレートがサポートされています。

- [標準マネージャ（Standard Manager）]：プロキシモードのマネージャをサポートします。
- [標準共有モード マネージャ（Standard Shared Mode Manager）]：共有モードのマネージャをサポートします。
- [標準アシスタント（Standard Assistant）]：プロキシ モードまたは共有モードのアシスタントをサポートします。

- [標準ユーザ（Standard User）]：[標準ユーザ（Standard User）] テンプレートでは、コール処理（[保留（Hold）] や [ダイヤル（Dial）] など）ソフトキーが使用可能です。

Manager Assistant の共有回線の概要

Manager Assistant を共有回線モードに設定すると、マネージャとアシスタントが電話番号（8001 など）を共有できるため、アシスタントは共有する電話番号でマネージャのコールを処理することができます。 マネージャが 8001 でコールを受信した場合、マネージャの電話機およびアシスタントの電話機の両方が鳴ります。

共有回線モードに適用されない Manager Assistant の機能には、[デフォルト アシスタント選択（Default Assistant Selection）]、[アシスタント ウォッチ（Assistant Watch）]、[コール フィルタリング（Call Filtering）]、[すべてのコールの転送（Divert All Calls）] などがあります。 アシスタントは、アシスタント コンソール アプリケーションでこれらの機能を確認したり、アクセスしたりできません。

Manager Assistant プロキシ回線の概要

プロキシ回線モードで Manager Assistant を設定すると、アシスタントはプロキシ番号を使用してマネージャのコールを処理します。 プロキシ番号は、マネージャの電話番号ではありませんが、システムによって選択された代替番号であり、アシスタントがマネージャのコールを処理するために使用します。 プロキシ回線モードでは、マネージャとアシスタントには Manager Assistant で使用できるすべての機能へのアクセスが与えられます。これには、デフォルトでのアシスタント選択、アシスタント モニタ、コール フィルタリング、すべての通話の転送が含まれます。

Manager Assistant の前提条件

- ユーザーは、Manager Assistant Client をリリース 11.5(1)SU9、12.0(1)SU4、および 14 以降の新しいバージョンにアップグレードする前に、32 または 64 ビットの Windows プラットフォームに対して、JRE をインストールする必要があります。

重要 アップグレードを実行する前に、現在マシンにインストールされている Cisco Unified Communications Manager Assistant クライアントをアンインストールしてください。 これは、リリース 12.0(1)SU4 および 14 以降から適用されます。

- Windows 11 プラットフォームでは、ユーザーは Manager Assistant クライアントをリリース 15SU2 以降の新しいバージョンにアップグレードする前に、64 ビット Windows プラットフォームに JRE 1.8 をインストールする必要があります。
- Manager Assistant は、次のブラウザとプラットフォームをサポートします。

- Unified Communications Manager Assistant Administration および Assistant Console は Windows 10 および 11（64 ビット）を搭載した Internet Explorer 11、Windows 10 および 11（64 ビット）以降を搭載した Firefox、および MacOS（10.x）以降を搭載した Safari でサポートされています。

（注） Unified Communications Manager リリース 15SU1 以前のバージョンの Windows 11 で IPMA プラグインを実行するには、サポートされている OS プラットフォーム（Windows 10、Windows 2019、および Windows 2022）のいずれかに IPMA リリース 15 バージョンのプラグインをインストールする必要があります。その後、インストールされているバージョンの IPMA プラグインを Windows 11 にコピーし、IMPA を起動します。

- Windows 10 および 11 または Apple Mac OS X を実行しているコンピュータでは、上で指定したブラウザのいずれかを開くことができます。

- 他言語の Manager Assistant 機能を表示するには、Manager Assistant を設定する前にロケールのインストーラをインストールします。
- Assistant Console アプリケーションは、Windows 10 および 11、Windows 2019 および Windows 2022 を実行するコンピュータでサポートされます。
- 電話とユーザ、およびユーザに関連付けられているデバイスを設定する必要があります。また、マネージャとアシスタントとの間の共有ライン アピアランスについては、マネージャのプライマリ回線とアシスタントのセカンダリ回線で同じ電話番号を設定する必要があります。
- マネージャとアシスタントを一括で追加するには Cisco Unified Communications Manager 一括管理ツールをインストールします。 詳細については、『*Bulk Administration Guide*』を参照してください。

Manager Assistant のプロキシ回線のタスク フロー

始める前に

- Manager Assistant の前提条件 （199 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 Unified CM Assistant 設定ウィザードの実行 （201 ページ）	

	コマンドまたはアクション	目的
ステップ 2	プロキシ回線のマネージャの設定とアシスタントの割り当て （208 ページ）	
ステップ 3	プロキシ回線のアシスタント ライン アピアランスの設定 （210 ページ）	
ステップ 4	Assistant Console プラグインのインストール （234 ページ）	アシスタントは、アシスタント コンソール アプリケーションと Cisco Unified IP Phone を使用して Unified Communications Manager Assistant 機能にアクセスします。 Assistant Console には、応答、転送、保留などの呼制御機能が備えられています。
ステップ 5	マネージャ アプリケーションとアシスタント コンソール アプリケーションを設定します。	『Cisco Unified Communications Manager Assistant User Guide for Cisco Unified Communications Manager』を参照してください。

Cisco Unified CM Assistant 設定ウィザードの実行

Cisco Unified CM Assistant 設定ウィザードを実行すると、パーティション、コーリング サーチ スペース、およびルート ポイントを自動的に作成できます。 また、ウィザードによって、マネージャの電話機、アシスタントの電話機、およびその他すべてのユーザの電話機の一括管理ツール（BAT）テンプレートも作成されます。 BAT テンプレートを使用して、マネージャ、アシスタント、およびその他すべてのユーザを設定できます。 BAT 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。

始める前に

設定ウィザードが一括管理ツールと同じサーバ（Unified Communications Manager サーバ）で実行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。**[アプリケーション（Application）] > [Cisco Unified CM Assistant 設定ウィザード（Cisco Unified CM Assistant Configuration Wizard）]**。

ステップ 2 [次へ（Next）]をクリックして、Cisco Unified CM Assistant 設定ウィザードのプロセスを開始します。

ステップ 3 [マネージャ用のパーティション（Partition for Managers）]ウィンドウで、名前と説明を入力して[次へ（Next）]をクリックします。 また、デフォルトのパーティション名および説明を使用することもできます。

ステップ 4 [CTI ルート ポイント用のパーティション（Partition for CTI Route Point）]ウィンドウで、名前と説明を入力して [次へ（Next）]をクリックします。 また、デフォルトの CTI ルート ポイント名を使用することもできます。

ステップ 5 [すべてのユーザ用のパーティション（Partition for All Users）]ウィンドウで、名前と説明を入力して [次へ（Next）]をクリックします。また、すべてのユーザのデフォルトのパーティション名および説明を使用することもできます。

ステップ 6 [インターコム パーティション（Intercom Partition）]ウィンドウで、名前と説明を入力して [次へ（Next）]をクリックします。 また、デフォルトのインターコム パーティション名を使用することもできます。

ステップ 7 [アシスタント コーリング サーチ スペース（Assistant Calling Search Space）]ウィンドウで、名前と説明を入力します。 また、デフォルトのコーリング サーチ スペース名および説明を使用することもできます。
このコーリング サーチ スペースの [ルート パーティション（Route Partitions）] の下にある [使用可能なパーティション（Available Partitions）] と [選択されたパーティション（Selected Partition）] ボックスに、アシスタント コーリング サーチ スペースのパーティションが自動的にリストされます。 デフォルト値を使用するか、[使用可能なパーティション（Available Partitions）]ボックスから適切なパーティションを選択できます。 1 つのボックスから他のボックスにパーティションを移動するには、上矢印および下矢印を使用します。

ステップ 8 [次へ（Next）]をクリックします。

ステップ 9 [全員のコーリング サーチ スペース（Everyone Calling Search Space）]ウィンドウで、名前と説明を入力します。 また、全員のコーリング サーチ スペースのデフォルトの名前および説明を使用することもできます。
このコーリング サーチ スペースの [ルート パーティション（Route Partitions）] の下にある [使用可能なパーティション（Available Partitions）] と [選択されたパーティション（Selected Partition）] ボックスに、アシスタント コーリング サーチ スペースのパーティションが自動的にリストされます。 デフォルト値を使用するか、[使用可能なパーティション（Available Partitions）]ボックスから適切なパーティションを選択できます。 1 つのボックスから他のボックスにパーティションを移動するには、上矢印および下矢印を使用します。

ステップ 10 [次へ（Next）]をクリックします。
システムで設定されている既存のコーリング サーチ スペースがある場合、[既存のコーリング サーチ スペース（Existing Calling Search Spaces）]ウィンドウが表示されます。表示されない場合は、次の手順に進みます。

Manager Assistant では、既存のコーリング サーチ スペースに対して **Generated_Route Point** および **Generated_Everyone** というプレフィックスを持つパーティションを追加する必要があります。 [使用可能なコーリング サーチ スペース（Available Calling Search Spaces）] および [選択されたコーリング サーチ スペース（Selected Calling Search Spaces）] ボックスに、これらのパーティションが自動的にリストされます。 1 つのボックスから他のボックスにパーティションを移動するには、上矢印および下矢印を使用します。

（注） 管理者がパーティション名を変更した場合、既存のコーリング サーチ スペースに追加されたプレフィックスも変更されることがあります。

ステップ 11 [次へ（Next）]をクリックします。

ステップ 12 [CTI ルート ポイント（CTI Route Point）]ウィンドウで、[CTI ルート ポイント名（CTI route point name）] フィールドに名前を入力します。または、デフォルトの CTI ルート ポイント名を使用します。

ステップ 13 ドロップダウン リストから、適切なデバイス プールを選択します。

ステップ 14 ルート ポイント電話番号を入力します。または、デフォルトのルート ポイント電話番号を使用します。

ステップ 15 ドロップダウン リストから、適切な番号計画を選択して、[次へ（Next）]をクリックします。

ステップ 16 [電話サービス（Phone Services）]ウィンドウで、プライマリ電話サービス名を入力します。または、デフォルトの電話サービス名を使用します。

ステップ 17 ドロップダウン リストから、プライマリ Cisco Unified Communications Manager Assistant サーバを選択するか、サーバ名または IP アドレスを入力します。

ステップ 18 セカンダリ電話サービス名を入力します。または、デフォルトの電話サービス名を使用します。

ステップ 19 ドロップダウン リストから、セカンダリ Cisco Unified Communications Manager Assistant サーバを選択するか、サーバ名または IP アドレスを入力して、[次へ（Next）]をクリックします。[確認（Confirmation）]ウィンドウが表示されます。 ここには、選択したすべての情報が表示されます。 情報が正しくなければ、設定プロセスをキャンセルするか、前の設定ウィンドウに戻ることができます。

ステップ 20 [終了（Finish）]をクリックします。
完了すると、最終的なステータスを示すウィンドウが表示されます。

設定ウィザードで生成されたエラーは、トレース ファイルに送信されます。 次の CLI コマンドを使用して、このファイルにアクセスします。**file get activelog tomcat/logs/ccmadmin/log4j**

次のタスク

Cisco Unified CM Assistant 設定ウィザードで作成されるのは、Cisco IP Manager Assistant サービス パラメータのみです。 残りのサービス パラメータは、手動で入力する必要があります。サービス パラメータの詳細については、プロキシ回線の Manager Assistant サービス パラメータ （203 ページ） を参照してください。

プロキシ回線の Manager Assistant サービス パラメータ

[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）]**。 Cisco IP Manager Assistant サービスがアクティブであるサーバを選択してから、[?]をクリックして詳細な説明を表示します。

設定	説明
Cisco IP Manager Assistant（アクティブ）パラメータ	

設定	説明
CTIManager（プライマリ）IP アドレス	このパラメータは、この Cisco IPMA サーバがコールの処理に使用するプライの IP アドレスを指定します。 デフォルト値はありません。
CTIManager（バックアップ）IP アドレス	このパラメータは、プライマリ CTIManager がダウンしている場合に、この がコールの処理に使用するバックアップ CTIManager の IP アドレスを指定し デフォルト値はありません。
プロキシ モードのルート ポイント デバイス名	このパラメータは、インテリジェント コール ルーティングのためにマネージ線へのすべてのコールを代行受信するために、この Cisco IPMA サーバが使用ポイントのデバイス名を指定します。 シスコは、IPMA サービスを実行しているすべてのサーバで同じ CTI ルート を使用することをお勧めします。 マネージャまたはアシスタントがプロキシように設定されると、CTI ルート ポイント デバイス名を設定する必要があり
CAPF Profile Instance ID for Secure Connection to CTIManager	このサービス パラメータは、この Manager Assistant が CTIManager へのセキ ために使用するアプリケーション ユーザ **IPMASecureSysUser** の Application C スタンス ID を指定します。 [CTIManager Connection Security Flag] が有効になっている場合、このパラメー
クラスタ全体のパラメータ（すべてのサーバに適用するパラメータ） **重要** [（Advanced）] をクリックして非表示のパラメータを表示します。	
Cisco IPMA サーバ（プライマリ）IP アドレス	このパラメータは、プライマリ Cisco IPMA サーバの IP アドレスを指定しま デフォルト値はありません。
Cisco IPMA サーバ（バックアップ）IP アドレス	このパラメータは、バックアップ Cisco IPMA サーバの IP アドレスを指定し プ サーバは、プライマリ IPMA サーバが失敗すると IPMA サービスを提供し デフォルト値はありません。
Cisco IPMA サーバ ポート	このパラメータは、IPMA Assistant Console ソケットが接続を開く際に接続す バで TCP/IP ポートを指定します。 ポートの競合が存在する場合、パラメータ デフォルト値：2912
Cisco IPMA Assistant Console ハートビート間隔	このパラメータは、Cisco IPMA サーバが IPMA Assistant Console にキープア （通常はハートビートと呼ばれる）を送信する間隔を秒単位で指定します。 Console は、このパラメータに指定されている時間が過ぎた後で、サーバから 受信に失敗するとフェールオーバーを開始します。 デフォルト値：30 秒

設定	説明
Cisco IPMA Assistant Console 要求のタイムアウト	このパラメータは、Cisco IPMA サーバからの応答を受信するまで IPMA A する時間を秒単位で指定します。 デフォルト値：30 秒
Cisco IPMA RNA 転送コール	このパラメータは、Cisco IPMA 無応答（RNA）転送が有効かどうかを指定 [True（True）]（Cisco IPMA は無応答のコールを次に利用可能なアシスタン たは [False（False）]（Cisco IPMA はコールを転送しません）です。 このパラメータは、[Cisco IPMA RNA タイムアウト（Cisco IPMA RNA Tim 連動します。つまり、コールは [Cisco IPMA RNA タイムアウト（Cisco IP パラメータで指定された時間が過ぎると転送されます。 ボイスメールプロ 定すると、アシスタントに転送できない無応答コールが、このタイマーが イスメールに送信されます。 デフォルト値：False
英数字のユーザ ID	このパラメータは、Cisco IPMA Assistant の電話で英数字のユーザ ID また 使用するかどうかを指定します。 デフォルト値：True
Cisco IPMA RNA のタイムアウト	このパラメータは、Cisco IPMA サーバが、応答のないコールを次の応答可 転送するまで待機する時間を秒単位で指定します。 このパラメータは、[コール（Cisco IPMA RNA Forward Calls）] パラメータと連動します。つま のは [Cisco IPMA RNA 転送コール（Cisco IPMA RNA Forward Calls）] パラメ に設定される場合のみです。 デフォルト値：10 秒
CTIManager Connection Security Flag	このパラメータは、Cisco IP Manager Assistant サービスの CTIManager 接続 定します。 これを有効にすると、Cisco IPMA は、アプリケーション ユーザ のインスタンス ID（**[CTIManager へのセキュアな接続の CAPF プロファ（CAPF Profile Instance ID for Secure Connection to CTIManager）]** サービ される）に設定される CAPF プロファイルを使用して CTIManager へのセキ す。 デフォルト値：[非セキュア（Non Secure）] セキュリティを有効にするには、[CTIManager へのセキュアな接続の CAP スタンス ID（CAPF Profile Instance ID for Secure Connection to CTIManager） タでインスタンス ID を選択する必要があります。
アシスタントに到達できない場合のマネージャへのコールのリダイレクト	このパラメータは、コールが選択されたプロキシ アシスタントに到達でき るマネージャに戻すために、Cisco Unified IP Manager Assistant アプリケーシ イレクトするかどうかを指定します。 デフォルト値：False

設定	説明
クラスタ全体の詳細パラメータ	
重要	同じ Cisco IPMA サーバの IP アドレスが複数のプールに表示されないように、各プール レスを設定します。
Enable Multiple Active Mode	このパラメータは、Cisco IP Manager Assistant サービスの複数のインスタンス 実現する必要があるかどうかを指定します。 これを有効にすると、Cisco IPM びプール 3 で設定されたその他のノードで実行できます。 複数のアクティブ モードを有効にするには、Cisco IPMA インスタンスをさら の IP アドレスを入力する必要があります。 これらのノードで Cisco IP Manag ス パラメータを設定します。 デフォルト値：False
プール 2：Cisco IPMA サーバ（プライマリ）IP アドレス	複数のアクティブ モードを有効にすると、このパラメータは、Cisco IPMA の ンスのプライマリ Cisco IPMA サーバの IP アドレスを指定します。 このノードで Cisco IP Manager Assistant サービス パラメータを設定します。
プール 2：Cisco IPMA サーバ（バックアップ）IP アドレス	複数のアクティブ モードを有効にすると、このパラメータは、Cisco IPMA の ンスのバックアップ Cisco IPMA サーバの IP アドレスを指定します。 バック プライマリ IPMA サーバが失敗すると IPMA サービスを提供します。 このノードで Cisco IP Manager Assistant サービス パラメータを設定します。
プール3：Cisco IPMA サーバ（プライマリ）IP アドレス	複数のアクティブ モードを有効にすると、このパラメータは、Cisco IPMA の ンスのプライマリ Cisco IPMA サーバの IP アドレスを指定します。 このノードで Cisco IP Manager Assistant サービス パラメータを設定します。
プール3：Cisco IPMA サーバ（バックアップ）IP アドレス	複数のアクティブ モードを有効にすると、このパラメータは、Cisco IPMA の ンスのプライマリ Cisco IPMA サーバの IP アドレスを指定します。 バックア ライマリ IPMA サーバが失敗すると IPMA サービスを提供します。 このノードで Cisco IP Manager Assistant サービス パラメータを設定します。
クラスタ全体のパラメータ（ソフトキー テンプレート）	
重要	マネージャおよびアシスタントに Manager Assistant 自動設定を使用するには、次のパ ます。
アシスタント ソフトキー テンプレート	このパラメータは、自動設定時にアシスタントデバイスに割り当てられるア キー テンプレートを指定します。 このパラメータで指定した値は、**[Cisco IP** **（Cisco IPMA Assistant Configuration）]** ページで **[自動設定（Automatic Confi** クボックスがオンのときに使用されます。
プロキシ モードのマネージャ ソフトキー テンプレートの管理	このパラメータは、自動設定時にマネージャ デバイスに割り当てられるマネ テンプレートを指定します。 このパラメータは、プロキシモードを使用する 適用されます。

設定	説明
クラスタ全体のパラメータ（プロキシ モードの IPMA のデバイス設定のデフォルト）	
マネージャ パーティション	このパラメータは、IPMA が自動設定時にマネージャのデバイスで処理す に割り当てられるパーティションを定義します。 使用するパーティショ の管理（Cisco Unified CM Administration）] にすでに追加されていることを IPMA 設定ウィザード（Cisco IPMA Configuration Wizard）] が実行されてい 力されます。 このパラメータは、プロキシモードを使用するマネージャに
すべてのユーザ パーティション	このパラメータは、自動設定時にすべてのプロキシ回線とアシスタント コム回線、およびマネージャ デバイス上のインターコム回線で設定され 定します。 使用するパーティションが [Cisco Unified CM の管理（Cisco U Administration）] にすでに追加されていることを確認します。 [Cisco IPMA 設 IPMA Configuration Wizard）] が実行されている場合、この値が入力されま は、プロキシ モードを使用するマネージャまたはアシスタントにのみ適用
IPMA コーリング サーチ スペース	このパラメータは、自動設定時に IPMA が処理するマネージャ デバイス_ インターコム回線、およびアシスタントデバイス上のアシスタントイン れるコーリング サーチ スペースを指定します。 使用するコーリング サー Unified CM の管理（Cisco Unified CM Administration）] にすでに追加され す。 [Cisco IPMA 設定ウィザード（Cisco IPMA Configuration Wizard）] が実 この値が入力されます。 このパラメータは、プロキシモードを使用する スタントにのみ適用されます。
マネージャのコーリング サーチ スペース	このパラメータは、自動設定時にアシスタント デバイス上のプロキシ回線 ジャ コーリング サーチ スペースを定義します。 このコーリング サーチ ス にすでに存在するコーリング サーチ スペースである必要があります。 [C ザード（Cisco IPMA Configuration Wizard）] が実行されている場合、この このパラメータは、プロキシ モードを使用するアシスタントにのみ適用さ
Cisco IPMA のプライマリ電話サービス	このパラメータは、自動設定時にマネージャまたはアシスタントデバイス サービスを定義します。 [Cisco IPMA 設定ウィザード（Cisco IPMA Config 行されている場合、この値が入力されます。 このパラメータは、プロキシ ネージャまたはアシスタントにのみ適用されます。
Cisco IPMA のセカンダリ電話サービス	このパラメータは、自動設定時にマネージャまたはアシスタント デバイス ダリ IP Phone サービスを定義します。 [Cisco IPMA 設定ウィザード（Cisc Wizard）] が実行されている場合、この値が入力されます。 このパラメー ドを使用するマネージャまたはアシスタントにのみ適用されます。
クラスタ全体のパラメータ（プロキシ モードでのプロキシ電話番号の範囲）	
開始電話番号（Starting Directory Number）	このパラメータは、IPMA のアシスタント設定時にプロキシ電話番号の自 して使用される開始電話番号を指定します。 自動生成されたプロキシ回線 に使用されると、次のアシスタント用に次の数が生成されるという具合に メータは、プロキシ モードを使用するアシスタントにのみ適用されます。

設定	説明
終了電話番号（Ending Directory Number）	このパラメータは、IPMA のアシスタント設定時のプロキシ電話番号の自動生号を指定します。 設定はこの番号で停止します。 このパラメータは、プロキするアシスタントにのみ適用されます。
クラスタ全体のパラメータ（プロキシ モードでのプロキシ電話番号の範囲）	
[マネージャ DN から削除される文字数（Number of Characters to be Stripped from Manager DN）]	このパラメータは、プロキシ DN の生成プロセスにおいて、マネージャの電削除される文字数を指定します。 プロキシ DN を生成すると、一部の桁の削スの追加が行われる場合があります。 桁の削除は左側から行われます。 このロキシ モードを使用するアシスタントにのみ適用されます。
マネージャ DN のプレフィックス	このパラメータは、プロキシ DN の生成プロセスにおいて、マネージャの DNレフィックスを指定します。 プロキシ DN を生成すると、桁の一部削除とプ加が行われる場合があります。 このパラメータは、プロキシモードを使用すのみ適用されます。

プロキシ回線のマネージャの設定とアシスタントの割り当て

新しいユーザの設定とデバイスのユーザへの関連付けについては、『Administration Guide for Cisco Unified Communications Manager』を参照してください。

（注） アシスタントのアシスタント情報を設定する前に、マネージャ情報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 [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)]** をクリックします。
検索結果には、Unified Communications Manager で設定されているすべてのエンド ユーザが表示されます。

ステップ 3 [関連リンク（Related Links）]ドロップダウン リストから [マネージャの設定（Manager Configuration）]を選択し、[移動（Go）]をクリックします。

ヒント　既存のアシスタント設定情報を表示するには、[関連付けられているアシスタント（Associated Assistants）] リストのアシスタント名をクリックし、[詳細の表示（View Details）]をクリックします。 [Cisco Unified CM アシスタント - アシスタントの設定（Cisco Unified CM Assistant - Assistant Configuration）]ウィンドウが表示されます。 マネージャ設定情報に戻るには、[関連付けられているマネージャ（Associated Managers）] リストのマネージャ名をクリックし、[詳細の表示（View Details）]をクリックします。

[Cisco Unified CM アシスタント - マネージャの設定（Cisco Unified CM Assistant - Manager Configuration）]ウィンドウが表示されます。

ステップ 4　マネージャとデバイス名またはデバイス プロファイルを関連付けるには、**[デバイス名/プロファイル（Device Name/Profile）]** ドロップダウン リストから、デバイス名またはデバイス プロファイルを選択します。 Manager Assistant によるエクステンションモビリティの詳細については、Manager Assistant の連携動作 （236 ページ） を参照してください。

（注）　マネージャが在宅勤務する場合は、[モバイル マネージャ（Mobile Manager）]チェック ボックスをクリックし、必要に応じて、[デバイス名/プロファイル（Device Name/Profile）] ドロップダウンリストからデバイス プロファイルを選択します。 デバイス プロファイルを選択した後は、マネージャは、Manager Assistant にアクセスする前にエクステンションモビリティを使用して電話にログインする必要があります。

ステップ 5　[インターコム回線（Intercom Line）] ドロップダウン リストから、マネージャのインターコム回線アピアランスを選択します（該当する場合）。

（注）　選択したインターコム回線は、Manager Assistant と Unified Communications Manager のインターコム機能に適用されます。

ステップ 6　[アシスタント プール（Assistant Pool）] ドロップダウン リストから、適切なプール番号（1 ～ 3）を選択します。

ステップ 7　[使用可能な回線（Available Lines）]選択ボックスから、Manager Assistant で制御する回線を選択し、下矢印をクリックしてその回線を [選択済みの回線（Selected Lines）] 選択ボックスに表示させます。 Manager Assistant で制御する回線を最大 5 つ設定します。

ヒント　[選択済みの回線（Selected Lines）] 選択ボックスから回線を削除して Manager Assistant による制御を解除するには、上矢印をクリックします。

ステップ 8　ソフトキーテンプレートを自動設定し、Manager Assistant で制御される選択された回線およびインターコム回線の Manager Assistant 電話サービス、コーリング サーチ スペース、およびパーティションと、Cisco IP Manager Assistant サービス パラメータに基づくマネージャ電話機のインターコム回線用のスピーカフォンによる自動応答を登録するには、[自動設定（Automatic Configuration）]チェック ボックスをオンにします。

（注）　インターコムの自動設定は、Cisco Unified IP Phone 7940 および 7960 用の Manager Assistant インターコム機能を使用する場合にのみ適用されます。

ステップ 9　**[保存]** をクリックします。
[自動設定（Automatic Configuration）]チェック ボックスをオンにしている場合、サービス パラメータが無効なときは、メッセージが表示されます。 サービス パラメータが有効であること

を確認してください。 自動設定が正常に完了すると、マネージャ デバイスがリセットされます。 デバイス プロファイルを設定する場合は、設定を有効にするためにマネージャがデバイスからログアウトして、ログインする必要があります。

プロキシ回線のアシスタント ライン アピアランスの設定

プロキシ回線は、アシスタント Cisco Unified IP 電話 に表示される電話回線を指定します。 Manager Assistant は、プロキシ回線を使用してマネージャへのコールを管理します。 管理者は、アシスタントの電話の回線をプロキシ回線として動作するように手動で設定できます。または、[自動設定（Automatic Configuration）]チェック ボックスを有効にして DN を作成し、アシスタントの電話に回線を追加することもできます。

（注）
1. いずれかのアシスタントのアシスタント情報を設定する前に、マネージャ情報を設定し、マネージャにアシスタントを割り当てる必要があります。
2. アシスタントの電話にプロキシ回線を自動で設定するには、**[プロキシ電話番号の範囲（Proxy Directory Number Range）]** セクションと **[プロキシ電話番号のプレフィックス（Proxy Directory Number Prefix）]** セクションでサービス パラメータを設定します。

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。**[ユーザ管理（User Management）]** > **[エンド ユーザ（End User）]**。

ステップ 2 **[検索(Find)]** をクリックします。

ステップ 3 選択したアシスタントのユーザ情報を表示するには、ユーザ名をクリックします。
[エンド ユーザ設定（End User Configuration）] ウィンドウが表示されます。

ステップ 4 **[関連リンク（Related Links）]** ドロップダウン リストから **[アシスタントの設定（Assistant Configuration）]** を選択し、**[移動（Go）]** をクリックします。

（注） **[自動設定（Automatic Configuration）]** チェック ボックスをオンにすると、システムは、Cisco IP Manager Assistant サービス パラメータの設定に基づいて、ソフトキー テンプレートとインターコム回線を自動的に設定します。 さらに、システムは、インターコム回線のスピーカーフォンで自動応答を設定します。

[アシスタントの設定（Assistant Configuration）] ウィンドウが表示されます。

ステップ 5 **[デバイス名（Device Name）]** ドロップダウン リストから、アシスタントに関連付けるデバイス名を選択します。

ステップ 6 **[インターコム回線（Intercom Line）]** ドロップダウン リストから、アシスタントのインターコム ライン アピアランスを選択します。

ステップ 7 [プライマリ ライン（**Primary Line**）] ドロップダウン リストから、アシスタントのプライマリ ラインを選択します。

ステップ 8 マネージャ回線をアシスタント回線に関連付けるには、[アシスタント回線へのマネージャの関連付け（Manager Association to Assistant Line）] 選択ボックスで、次の手順を実行します。

a) [**使用可能な回線（Available Lines**）] ドロップダウン リストから、マネージャ回線に関連付けるアシスタント回線を選択します。

b) [**マネージャ名（Manager Names**）] ドロップダウン リストから、このプロキシ回線を適用する事前設定されたマネージャ名を選択します。

c) [**マネージャ回線（Manager Lines**）] ドロップダウン リストから、このプロキシ回線を適用するマネージャ回線を選択します。

ステップ 9 **[保存]** をクリックします。
更新はすぐに有効になります。[**自動設定（Automatic Configuration**）] を選択すると、アシスタント デバイスが自動的にリセットされます。

Manager Assistant の共有回線のタスク フロー

始める前に

- Manager Assistant の前提条件 （199 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	Manager Assistant 共有回線サポートのパーティションの設定 （213 ページ）	Manager Assistant によって使用される回線のパーティションを設定します。
ステップ 2	Manager Assistant の共有回線サポートのコーリング サーチ スペースの設定 （214 ページ）	マネージャおよびアシスタントの回線のコーリング サーチ スペースを設定します。
ステップ 3	Cisco IP Manager Assistant サービス パラメータの設定 （215 ページ）	マネージャおよびアシスタントに対して自動設定を使用するには、次のパラメータを設定します。
ステップ 4	インターコムの設定 • インターコム パーティションの設定 （216 ページ） • インターコム コーリング サーチ スペースの設定 （392 ページ） • インターコム電話番号の設定 （393 ページ）	

	コマンドまたはアクション	目的
	• インターコム トランスレーション パターンの設定 （392 ページ）	
ステップ 5	複数の Manager Assistant プールの設定（219 ページ）	多数のマネージャおよびアシスタントをサポートする必要がある場合には、複数のプールを設定します。 マネージャとアシスタントを最大2500ペアとして管理するアクティブな Cisco IP Manager Assistant サーバを最大で 3 台設定できます。
ステップ 6	Manager Assistant の CTI へのセキュアな TLS 接続の設定 • IPMASecureSysUser アプリケーション ユーザの設定 （221 ページ） • CAPF プロファイルの設定 （221 ページ） • Cisco Webダイヤラー Web サービスの設定 （224 ページ）	システムが混合モードで稼動している場合、次の手順に従います。
ステップ 7	CTI ルート ポイントの設定 （225 ページ）	Cisco Unified Communications Manager Assistant マネージャからのコールをインターセプトし、ルーティングするには、CTI ルート ポイントの作成が必要です。
ステップ 8	マネージャおよびアシスタントの IP Phone サービスの設定 （225 ページ）	
ステップ 9	マネージャ、アシスタント、および全ユーザの電話ボタン テンプレートの設定 （230 ページ）	
ステップ 10	共有回線モードのマネージャの設定とアシスタントの割り当て （232ページ）	
ステップ 11	共有回線のアシスタント ラインアピアランスの設定 （233 ページ）	
ステップ 12	Assistant Console プラグインのインストール （234 ページ）	アシスタントは、Assistant Cisco Unified Communications Manager Assistant Consoleアプリケーションとを使用して機能にCisco Unified IP 電話アクセスします。 Assistant Console には、応答、転送、保留などの呼制御機能が備えられています。

	コマンドまたはアクション	目的
ステップ 13	マネージャ アプリケーションとアシスタント コンソール アプリケーションを設定します。	『Cisco Unified Communications Manager Assistant User Guide for Cisco Unified Communications Manager』を参照してください。

Manager Assistant 共有回線サポートのパーティションの設定

Generated_Everyone、Generated_Managers、および Generated_Route_Point の 3 つのパーティションを作成する必要があります。

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。**コール ルーティング** > **コントロールのクラス** > **パーティション**。

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。

説明にはどの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサイド（&）、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。

Manager Assistant 共有回線サポートの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 *20* : 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

Manager Assistant の共有回線サポートのコーリング サーチ スペースの設定

コーリング サーチ スペースは、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。

2 つのコール コーリング サーチ スペース（Generated_CSS_I_E および Generated_CSS_M_E）を作成する必要があります。

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。**コール ルーティング** > **コントロールのクラス** > **コーリングサーチスペース**。

ステップ 2 [新規追加] 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、どの言語でも最大 50 文字まで指定できますが、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、**コントロール（Ctrl）**キーを押したまま、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。

Cisco IP Manager Assistant サービス パラメータの設定

マネージャおよびアシスタントに Manager Assistant 自動設定を使用するには、Cisco IP Manager Assistant サービス パラメータを設定します。 インストールされている各 Cisco IP Manager Assistant サービスのすべての Cisco IP Manager Assistant サービス パラメータと汎用パラメータに対して、クラスタ全体のパラメータを指定する必要があります。

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）] > [サービス パラメータ（Service Parameters）]**。

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、Cisco IP Manager Assistant サービスがアクティブになっ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 IP Manager Assistant（Cisco IP Manager Assistant）]** サービスを選択します。
パラメータを一覧表示する [サービス パラメータ設定（Service Parameter Configuration）]ウィンドウが開きます。

ステップ 4 **[Cisco IP Manager Assistant パラメータ（Cisco IP Manager Assistant Parameters）]**、**[クラスタ全体のパラメータ（すべてのサーバに適用されるパラメータ）（Clusterwide Parameters**

(Parameters that apply to all servers)）]、および [**クラスタ全体のパラメータ（ソフトキー テンプレート）（Clusterwide Parameters (Softkey Templates)**）] を設定します。

詳細については、[?] をクリックしてください。

ステップ 5 **[保存（Save）]** をクリックします。

インターコムの設定

手順

	コマンドまたはアクション	目的
ステップ 1	インターコム パーティションの設定（216 ページ）	
ステップ 2	インターコム コーリング サーチ スペースの設定 （217 ページ）	
ステップ 3	インターコム電話番号の設定（218 ページ）	
ステップ 4	インターコム トランスレーション パターンの設定 （218 ページ）	

インターコム パーティションの設定

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。**コール ルーティング** > **インターコム** > **インターコムルートパーティション**。

インターコム パーティションの検索と一覧表示（Find and List Intercom Partitions）] ウィンドウが表示されます。

ステップ 2 [新規追加] をクリックします。

[新規インターコム パーティションの追加（Add New Intercom Partition）] ウィンドウが表示されます。

ステップ 3 [**インターコム パーティション情報（Intercom Partition Information**）] セクションの [**名前（Name**）] ボックスに、追加するインターコム パーティションの名前と説明を入力します。

（注） 複数のパーティションを入力するには、各パーティション エントリごとに 1 行を使います。 最大 75 のパーティションを入力できます。名前と説明には合計 1475 文字を使用できます。 パーティション名は、50 文字以内です。 各行のパーティション名と説明を区別するには、カンマ（,）を使用します。 説明が入力されなかった場合、Unified Communications Manager はパーティション名を説明として使用します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 設定するパーティションを探します。
[インターコムパーティションの設定（Intercom Partition Configuration）] ウィンドウが表示されます。

ステップ 6 [インターコム パーティションの設定（Intercom Partition Configuration）] フィールド エリア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]** をクリックします。

[インターコム パーティションの設定（Intercom Partition Configuration）] ウィンドウが表示されます。

ステップ 8 適切な設定値を入力します。 [インターコム パーティションの設定（Intercom Partition Configuration）] パラメータの詳細については、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。

ステップ 10 **[設定の適用（Apply Config）]** をクリックします。

インターコム コーリング サーチ スペースの設定

手順

ステップ 1 メニュー バーで、**[コール ルーティング（Call Routing）] > [インターコム（Intercom）] > [インターコム コーリング サーチ スペース（Intercom Calling Search Space）]** 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 [インターコム コーリング サーチ スペース（Intercom Calling Search Space）] フィールド領域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、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。

インターコム電話番号の設定

手順

ステップ 1 **[コール ルーティング（Call Routing）] > [インターコム（Intercom）] > [インターコム電話番号（Intercom Directory Number）]** を選択します。

[インターコム電話番号の検索と一覧表示（Find and List Intercom Directory Numbers）]ウィンドウが表示されます。

ステップ 2 特定のインターコム電話番号を検索するには、検索条件を入力して [検索（Find）]をクリックします。
検索基準に一致するインターコム電話番号の一覧が表示されます。

ステップ 3 次のいずれかのタスクを実行します。

a) インターコム 電話番号を追加するには、**[新規追加]** をクリックします。

b) インターコム電話番号を更新するには、更新するインターコム電話番号をクリックします。

[インターコム電話番号の設定（Intercom Directory Number Configuration）]ウィンドウが表示されます。

ステップ 4 [インターコム電話番号の設定（Intercom Directory Number Configuration）] フィールド領域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、オンライン ヘルプを参照してください。

ステップ 5 **[保存]** 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 **[電話のリセット（Reset Phone）]** をクリックします。

ステップ 8 デバイスを再起動します。

再起動中に、ゲートウェイのコールがドロップされることがあります。

インターコム トランスレーション パターンの設定

手順

ステップ 1 **[コール ルーティング（Call Routing）] > [インターコム（Intercom）] > [インターコム トランスレーション パターン（Intercom Translation Pattern）]** を選択します。

[インターコム トランスレーション パターンの検索/一覧表示（Find and List Intercom Translation Patterns）] ウィンドウが表示されます。

ステップ 2 次のいずれかのタスクを実行します。

a) 既存のインターコム トランスレーション パターンをコピーするには、設定するパーティションを探し、コピーするインターコム トランスレーション パターンの横にある [**コピー（Copy）**] ボタンをクリックします。
b) 新しいインターコム 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）]** ボタンをクリックします。

ステップ 3 [インターコム トランスレーション パターンの設定（Intercom Translation Pattern Configuration）] フィールド領域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、オンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

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インターコム トランスレーション パターンが一意であることを確認します。重複入力を示すエラーを受け取ったら、ルート パターンまたはハント 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ます。

[インターコム トランスレーション パターンの設定（Intercom Translation Pattern Configuration）] ウィンドウに、新しく設定したインターコム トランスレーション パターンが表示されます。

次のタスク

Manager Assistant の共有回線のタスク フロー （211 ページ）を参照して、次のタスクを決定、完了します。

複数の Manager Assistant プールの設定

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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

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、Cisco IP Manager Assistant サービスがアクティブになっ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 IP Manager Assistant]サービスを選択します。
パラメータを一覧表示する [サービス パラメータ設定（Service Parameter Configuration）]ウィンドウが開きます。

ステップ 4 [詳細設定（Advanced）]をクリックします。
[クラスタ全体のパラメータ（すべてのサーバに適用されるパラメータ）（Clusterwide Parameters（Parameters that apply to all servers））]の高度なパラメータが表示されます。

ステップ 5 [クラスタ全体のパラメータ（すべてのサーバに適用されるパラメータ）（Clusterwide Parameters（Parameters that apply to all servers））]で、複数のマネージャ アシスタント プールを追加する次のパラメータを設定します。

a) [複数のアクティブ モードの有効化（Enable Multiple Active Mode）]：デフォルト値は [False] です。 このパラメータを [True] に設定すると、管理者は、複数のプールを使用して最大 7000 名のマネージャおよびアシスタントを設定できます。

b) プール 2：Cisco IPMA サーバ（プライマリ）IP アドレス：デフォルトではありません。 管理者は、この IP アドレスを手動で入力する必要があります。 管理者は、このアドレスに最大 2500 名のマネージャおよびアシスタントを割り当てることができます。

c) プール 2：Cisco IPMA サーバ（バックアップ）IP アドレス：デフォルトではありません。管理者は、この IP アドレスを手動で入力する必要があります。

d) プール 3：Cisco IPMA サーバ（プライマリ）IP アドレス：デフォルトではありません。 管理者は、この IP アドレスを手動で入力する必要があります。このアドレスに最大 2500 名のマネージャおよびアシスタントを割り当てることができます。

e) プール 3：Cisco IPMA サーバ（バックアップ）IP アドレス：デフォルトではありません。管理者は、この IP アドレスを手動で入力する必要があります。

詳細については、[?] をクリックしてください。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

Manager Assistant の共有回線のタスク フロー （211 ページ）を参照して、次のタスクを決定、完了します。

Manager Assistant の CTI へのセキュアな TLS 接続の設定

Manager Assistant は、WDSecureSysUser アプリケーション ユーザ クレデンシャルを使用して CTI へのセキュアな TLS 接続を確立し、コールを発信します。

セキュアな TLS 接続を確立するように WDSecureSysUser アプリケーション ユーザを設定するには、次の作業を実行します。

始める前に

- Cisco CTL Client をインストールし、設定します。

  CTL クライアントの詳細については、Cisco Unified Communications Manager セキュリティ ガイドを参照してください。

- [エンタープライズパラメータ設定（Enterprise Parameters Configuration）]ウィンドウの [クラスタ セキュリティ モード（Cluster Security Mode）] を **1** に設定します（混合モード）。システムを混合モードで操作することは、システムの他のセキュリティ機能に影響を及ぼします。 システムが現在混合モードで動作していない場合、これらの相互作用を理解していないときは、混合モードに切り替えないでください。 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。

- **[エンタープライズパラメータ設定（Enterprise Parameters Configuration）]** ウィンドウの **[クラスタ SIPOAuth モード（Cluster SIPOAuth Mode）]** フィールドが **[有効（Enabled）]** に設定されていることを確認します。
- 最初のノードでのみCisco認証局プロキシ機能（CAPF）サービスをアクティブにします。

手順

	コマンドまたはアクション	目的
ステップ 1	IPMASecureSysUser アプリケーション ユーザの設定 （221 ページ）	IPMASecureSysUser アプリケーション ユーザを設定します。
ステップ 2	CAPF プロファイルの設定 （221 ページ）	IPMASecureSysUser アプリケーション ユーザの認証局プロキシ機能（CAPF）プロファイルを設定します。
ステップ 3	Cisco Webダイヤラー Web サービスの設定 （224 ページ）	Cisco IP Manager Assistant サービスのサービス パラメータを設定します。

IPMASecureSysUser アプリケーション ユーザの設定

IPMASecureSysUser アプリケーション ユーザを設定するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[ユーザ管理（User Management）]** > **[アプリケーション ユーザ（Application User）]** 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 [**アプリケーション ユーザの検索と一覧表示のアプリケーション（Find and List Application Users Application）**] ウィンドウから、[**WDSecureSysUser**] を選択します。

ステップ 4 [**アプリケーション ユーザの設定（Application User Configuration）**] ウィンドウの各フィールドを設定し、[**保存（Save）**] をクリックします。

CAPF プロファイルの設定

認証局プロキシ機能（CAPF）は、セキュリティ証明書を発行して、認証するタスクを実行するコンポーネントです。 アプリケーション ユーザの CAPF プロファイルを作成すると、プロファイルは設定の詳細を使用してアプリケーションの安全な接続を開きます。

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。**[User Management]** > **[Application User CAPF Profile]**。

ステップ 2 次のいずれかの作業を実行します。

- 新しい CAPF プロファイルを追加するには、**[検索（Find）]** ウィンドウで **[新規追加]** をクリックします。
- **[コピー（Copy）]** 列にあるそのレコードの **[コピー（Copy）]** をクリックして、既存のプロファイルをコピーし、適切なプロファイルを見つけます。

既存のエントリを更新するには、適切なプロファイルを見つけて表示します。

ステップ 3 関連する CAPF プロファイル フィールドを設定または更新します。 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]** をクリックします。

ステップ 5 セキュリティを使用するアプリケーション ユーザおよびエンド ユーザごとに、この手順を繰り返します。

CAPF プロファイルの設定

設定	説明
[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、CAPF 操作のアプリケーション ユーザを選択します。この設定には、設定されているアプリケーションユーザが表示されます。 この設定は、[**エンド ユーザ CAPF プロファイル（End User CAPF Profile**）] ウィンドウには表示されません。
[エンドユーザID(End User ID)]	ドロップダウン リストから、CAPF 操作のエンド ユーザを選択します。 この設定には、設定済みのエンド ユーザが表示されます。 この設定は、[**アプリケーション ユーザ CAPF プロファイル（Application User CAPF Profile**）] ウィンドウには表示されません。

設定	説明
インスタンス ID（Instance ID）	1 ～ 128 文字の英数字（a ～ z、A ～ Z、0 ～ 9）を入力します。 インスタンス ID は、認証操作のユーザを指定します。 1 つのアプリケーションに複数の接続（インスタンス）を設定できます。 アプリケーションと CTIManager との接続を保護するため、アプリケーション PC（エンド ユーザの場合）またはサーバ（アプリケーション ユーザの場合）で実行されるそれぞれのインスタンスに固有の証明書があることを確認します。 このフィールドは、Web サービスおよびアプリケーションをサポートする CAPF Profile Instance ID for Secure Connection to CTIManager サービス パラメータに関連しています。
[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。 （デフォルト設定） • [インストール/アップグレード（Install/Upgrade）]：このオプションを選択すると、アプリケーションに新しい証明書がインストールされるか、既存のローカルで有効な証明書がアップグレードされます。
認証モード（Authentication Mode）	証明書の操作が [インストール/アップグレード（Install/Upgrade）] の場合、認証モードとして [認証ストリング（By Authentication String）] が指定されます。つまり、ユーザ/管理者によって [**JTAPI/TSP 設定（JTAPI/TSP Preferences**）] ウィンドウに CAPF 認証文字列が入力された場合にのみ、ローカルで有効な証明書のインストール/アップグレードまたはトラブルシューティングが CAPF によって実行されます。
認証文字列（Authentication String）	独自の認証文字列を作成するには、一意の文字列を入力します。 各文字列は 4 ～ 10 桁である必要があります。 ローカルで有効な証明書のインストールまたはアップグレードを実行する場合、アプリケーション PC の JTAPI/TSP 設定 GUI に管理者が認証文字列を入力することが必要です。 この文字列は、1 回だけ使用できます。あるインスタンスに文字列を使用した場合、その文字列をもう一度使用することはできません。
[文字列を生成(Generate String)]	認証文字列を自動的に生成するには、このボタンをクリックします。 4 ～ 10 桁の認証文字列が [**認証文字列（Authentication String**）] フィールドに表示されます。

設定	説明
キー サイズ（ビット数）（Key Size (bits)）	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。キーサイズに512を選ぶこともできます。 キー生成を低いプライオリティで設定すると、アクションの実行中もアプリケーションの機能を利用できます。 キーの生成には最大 30 分かかります。
[操作の完了期限(Operation Completes By)]	このフィールドは、すべての証明書操作をサポートし、操作を完了する必要がある期限の日付と時刻を指定します。 表示される値は、最初のノードに適用されます。 この設定は、証明書の操作を完了する必要がある期間のデフォルトの日数を指定する [**CAPF 操作有効期間（日数）（CAPF Operation Expires in (days)**）] エンタープライズ パラメータと併用します。 このパラメータはいつでも更新できます。
[証明書の操作ステータス(Certificate Operation Status)]	このフィールドは、pending、failed、successful など、証明書操作の進行状況を表示します。 このフィールドに表示される情報は変更できません。

Cisco Webダイヤラー Web サービスの設定

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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

ステップ 2 [サーバ（Server）]ドロップダウン リストから、Cisco Webダイヤラー Web サービスがアクティブになっ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 IP Manager Assistant][Cisco Webダイヤラー Web]サービスを選択します。
パラメータのリストが表示されます。

ステップ 4 [CTIManager Connection Security Flag] パラメータおよび [CAPF Profile Instance ID for Secure Connection to CTIManager] パラメータを選択して更新します。

パラメータの説明を表示するには、パラメータ名のリンクをクリックします。

（注） CTIManager は IPv4 および IPv6 のアドレスをサポートします。

ステップ 5 **[保存]** をクリックします。

ステップ 6 サービスがアクティブになっているサーバごとに、この手順を繰り返します。

次のタスク

Manager Assistant の共有回線のタスク フロー （211 ページ）を参照して、次のタスクを決定、完了します。

CTI ルート ポイントの設定

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）] > [CTI ルート ポイント（CTI Route Point）]**。

ステップ 2 [新規追加] をクリックします。
[CTI ルート ポイントの設定（CTI Route Point Configuration）] ウィンドウが表示されます。

ステップ 3 [デバイス名（Device Name）]フィールドに、デバイス名を入力します。

ステップ 4 [デバイス プール（Device Pool）]ドロップダウン リストから、[デフォルト（Default）]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 [Generated_CSS_M_E]を選択します。

ステップ 6 [デバイス プールの発呼側トランスフォーメーション CSS を使用（Use Device Pool Calling Party Transformation CSS）]チェックボックスをオンにします。

ステップ 7 **[保存]** をクリックします。
[追加に成功しました（Add successful）] ステータス メッセージが表示されます。

ステップ 8 [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。
[ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウが表示されます。

ステップ 9 [電話番号（Directory Number）]フィールドに電話番号を入力します。

ステップ 10 [ルート パーティション（Route Partition）]ドロップダウン リストから [Generated_Route_Point] を選択します。

ステップ 11 **[保存（Save）]** をクリックします。

マネージャおよびアシスタントの IP Phone サービスの設定

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）] > [電話サービス（Phone Services）]**。

ステップ 2 [新規追加] をクリックします。
[IP Phone サービスの設定（IP Phone Services Configuration）]ウィンドウが表示されます。

ステップ 3 マネージャおよびアシスタントのサポートされている電話ごとに、必須フィールドに値を入力し、[保存（Save）]をクリックします。 フィールドとその設定オプションの詳細については、Cisco IP 電話 サービス設定フィールド （226 ページ）を参照してください。
「更新に成功しました（Update successful）」というメッセージが表示されます。

Cisco IP 電話 サービス設定フィールド

フィールド	説明
サービス情報（Service Information）	
サービス名（Service Name）	サービスの名前を入力します。 サービスがエンタープライズ サブスクリプションとしてマークされていない場合、サービスに登録できる領域（Cisco Unified Communications セルフ ケア ポータルなど）にそのサービス名が表示されます。 サービス名として入力できる文字数は最大で 128 文字です。 Java MIDlet サービスの場合、サービス名は、Java Application Descriptor（JAD）ファイルで定義されている名前と正確に一致している必要があります。 （注） Unified Communications Manager 2 つ以上の IP フォン サービスを同じ名前で作成できます。 ほとんどまたはすべての電話機ユーザが上級者であるか、管理者が常に IP Phone サービスを設定する場合以外は、同じ名前を付けないことを推奨します。 AXL やサードパーティ ツールが設定のために IP Phone サービスのリストにアクセスする場合は、IP Phone サービスに対して固有の名前を使用する必要があります。 （注） サービス URL がカスタマイズされた外部 URL をポイントしている場合、電話のデバイス ロケールに基づいてサービス名をローカライズすることはできません。 サービス名は、英語のアルファベットでのみ表示されます。
[ASCIIサービス名(ASCII Service Name)]	電話機が Unicode を表示できない場合に表示するサービス名を入力します。
[サービスの説明(Service Description)]	サービスが提供するコンテンツ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（"）と一重引用符（'）は使用できません。

フィールド	説明
サービス URL（Service URL）	IP Phone サービスのアプリケーションが置かれているサーバの URL を入力します。 このサーバは、Unified Communications Manager クラスタに含まれるサーバから独立している必要があります。 Unified Communications Manager サーバまたは Unified Communications Manager に関連付けられているサーバ（TFTP サーバ、ディレクトリ データベース パブリッシャ サーバなど）は指定しないでください。 サービスを使用するには、Unified Communications Manager クラスタの電話機がサーバとネットワーク接続されている必要があります。 シスコの署名付き Java MIDlet の場合は、JAD ファイルをダウンロード可能な場所を入力します。たとえば、Java MIDlet の通信先である Web サーバやバックエンド アプリケーション サーバです。 シスコ提供のデフォルトサービスの場合は、サービス URL はデフォルトでは「`Application:Cisco/<name of service>`」と表示されます。たとえば、`Application:Cisco/CorporateDirectory` です。 シスコが提供するデフォルト サービスのサービス URL を変更する場合は、[サービス プロビジョニング（Service Provisioning）]に [両方（Both）] を設定していることを確認してください。この設定は、[電話（Phone）]、[エンタープライズ パラメータ（Enterprise Parameter）]、および [共通の電話プロファイルの設定（Common Phone Profile Configuration）]ウィンドウに表示されます。 たとえば、カスタムの社内ディレクトリを使用する場合は `Application:Cisco/CorporateDirectory` をカスタム ディレクトリの外部サービス URL に変更するので、[サービスのプロビジョニング（Services Provisioning）]の値は [両方（Both）]に設定します。

フィールド	説明
[セキュアサービス URL(Secure-Service URL)]	Cisco Unified IP 電話 サービス アプリケーションが保存されているサーバのセキュア URL を入力します。 このサーバは、Unified Communications Manager クラスタに含まれるサーバから独立している必要があります。 Unified Communications Manager サーバ、または Unified Communications Manager に関連付けられているサーバ（TFTP サーバやパブリッシャ データベース サーバなど）を指定しないでください。 サービスを使用するには、Unified Communications Manager クラスタの電話機がサーバとネットワーク接続されている必要があります。 （注） [セキュアサービスURL(Secure-Service URL)] を指定しないと、デバイスでは非セキュア URL が使用されます。 セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。
[サービスカテゴリ (Service Category)]	サービス アプリケーションのタイプ（XML または Java MIDlet）を選択します。 Java MIDlet を選択した場合、電話機は最新の設定ファイルを受信すると、指定のサービス URL からシスコの署名入りの MIDlet アプリケーション（JAD および JAR）を取得してインストールします。
[サービスタイプ(Service Type)]	サービスが電話の [サービス（Services）]、[ディレクトリ（Directories）]、または [メッセージ（Messages）] ボタンまたはオプションのいずれにプロビジョニングされるか（電話にこれらのボタンまたはオプションがある場合）を選択します。 ご使用の電話でこれらのボタンまたはオプションがサポートされているかどうかを判断するには、ご使用の電話のモデルに対応する『*Cisco Unified IP Phone Administration Guide*』を参照してください。
サービス ベンダー（Service Vendor）	サービスのベンダーまたは製造元を指定できます。 このフィールドは、XML アプリケーションの場合はオプションですが、シスコの署名入りの Java MIDlet の場合は必須です。 シスコの署名入りの Java MIDlet の場合、このフィールドに入力する値は MIDlet JAD ファイルに定義されているベンダーと一致する必要があります。 このフィールドは、シスコが提供するデフォルト サービスの場合はブランクとなります。 入力できるのは最大 64 文字です。

フィールド	説明
[サービスバージョン (Service Version)]	アプリケーションのバージョン番号を入力します。 XML アプリケーションの場合、このフィールドはオプションであり、情報提供だけを目的としています。 シスコの署名入りの Java MIDlet の場合は、次の点を考慮してください。 • バージョンを入力する場合、その値は JAD ファイルに定義されているバージョンと一致する必要があります。 入力したバージョンが電話機にインストールされているものと異なる場合、電話機は MIDlet をアップグレードまたはダウングレードしようとします。 • このフィールドがブランクの場合は、バージョンは [サービス URL（Service URL）]から取得されます。 このフィールドをブランクのままにしておくと、電話は Unified Communications Manager に再登録するたびに、また、シスコの署名付き Java MIDlet が起動するたびに、JAD ファイルのダウンロードを試みます。したがって、管理者が**[サービス バージョン（Service Version）]** フィールドを手動で更新しなくても、電話は常に最新バージョンのシスコ署名付き Java MIDlet を実行します。 このフィールドは、シスコが提供するデフォルト サービスの場合はブランクとなります。 このフィールドには、（最大 16 ASCII 文字の）数字およびピリオドを入力できます。
有効（Enable）	このチェックボックスにより、[Cisco Unified CM の管理（Cisco Unified CM Administration）]Cisco Unified Communications Manager Administration から設定を削除せずに（およびデータベースからサービスを削除せずに）、サービスを有効化または無効化できます。 このチェックボックスをオフにすると、サービスは電話機設定ファイルおよび電話機から削除されます。
サービス パラメータ情報	

フィールド	説明
パラメータ	この IP Phone サービスに適用されるサービス パラメータがリストされます。 このペインでは、次のボタンを使用してサービス パラメータを設定します。 • [新規パラメータ（New Parameter）]：このボタンをクリックすると、[Cisco Unified IP Phone サービス パラメータの設定（Configure Cisco Unified IP Phone Service Parameter）]ウィンドウが表示されます。このウィンドウでは、IP Phone サービスの新規サービス パラメータを設定します。 • [パラメータの編集（Edit Parameter）]：[パラメータ（Parameters）]ペインに表示されるサービス パラメータを強調表示してこのボタンをクリックすると、[Cisco Unified IP Phone サービス パラメータの設定（Configure Cisco Unified IP Phone Service Parameter）]ウィンドウが表示されます。このウィンドウでは、この IP Phone サービスの選択されたサービス パラメータを編集できます。 • [パラメータの削除（Delete Parameter）]：[パラメータ（Parameters）]ペインに表示されるサービス パラメータを強調表示してこのボタンをクリックすると、この IP Phone サービスからサービス パラメータが削除されます。 削除の確認を求めるポップアップ ウィンドウが表示されます。

マネージャ、アシスタント、および全ユーザの電話ボタンテンプレートの設定

この項の手順は、マネージャとアシスタント向けに電話機のボタンを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	Manager Assistant の電話ボタン テンプレートの設定 （231 ページ）	この手順を実施することで、マネージャとアシスタント ボタン機能を回線または短縮ダイヤル キーに割り当てることができます。
ステップ 2	電話機と Manager Assistant ボタン テンプレートの関連付け （231 ページ）	電話機でマネージャおよびアシスタント ボタンを設定するには、次の手順を実行します。

Manager Assistant の電話ボタン テンプレートの設定

Manager Assistant 機能の電話ボタン テンプレートを設定するには、この手順を実行します。

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）]** > **[電話ボタンテンプレート（Phone button template）]** の順に選択します。

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]** 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]** をクリックします。

ステップ 7 次のいずれかの作業を実行します。

- 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 Manager Assistant ボタン テンプレートの関連付け

始める前に

Manager Assistant の電話ボタン テンプレートの設定 （231 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]** 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。

共有回線モードのマネージャの設定とアシスタントの割り当て

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)]** をクリックします。
検索結果には、Unified Communications Manager で設定されているすべてのエンド ユーザが表示されます。

ステップ 3 [関連リンク（Related Links）]ドロップダウン リストから [マネージャの設定（Manager Configuration）]を選択し、[移動（Go）]をクリックします。

ステップ 4 Cisco IP Manager Assistant サービス パラメータに基づいて、マネージャの電話のインターコム回線のスピーカーフォンでソフトキー テンプレートと [自動応答（Auto Answer）] を自動設定するには、[**自動設定（Automatic Configuration**）] チェックボックスをオンにします。

（注） インターコムの [**自動設定（Automatic Configuration**）] は、Unified Communications Manager Assistant インターコム機能が Cisco Unified IP Phone 7940 および 7960 で使用されるときにのみ適用されます。

ステップ 5 [**共有回線を使用（Uses Shared Lines**）] チェックボックスをオンにします。

ステップ 6 マネージャとデバイス名またはデバイス プロファイルを関連付けるには、**[デバイス名/プロファイル（Device Name/Profile）]** ドロップダウン リストから、デバイス名またはデバイス プロファイルを選択します。

（注） マネージャが在宅勤務の場合は、[**エクステンションモビリティを使用（Mobile Manager**）] チェックボックスをオンにし、必要に応じて [**デバイス名/プロファイル（Device Name/Profile**）] ドロップダウン リストからデバイス プロファイルを選択します。 デバイス プロファイルを選択した場合、マネージャは、Manager Assistant にアクセスする前に Cisco Extension Mobility を使用して電話にログインする必要があります。

エクステンションモビリティおよびManager Assistant 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 7 [インターコム回線（Intercom Line）]ドロップダウン リストから、マネージャのインターコム回線アピアランスを選択します（該当する場合）。

選択したインターコム回線は、Manager Assistant と Unified Communications Manager のインターコム機能に適用されます。

ステップ 8 [アシスタント プール（Assistant Pool）]ドロップダウン リストから、適切なプール番号（1 ～ 3）を選択します。

ステップ 9 アシスタントをマネージャに割り当てるには、[利用可能なアシスタント（Available Assistants）] 選択ボックスからアシスタントの名前を選択し、下向き矢印をクリックして [関連付けられたアシスタント（Associated Assistants）] 選択ボックスに移動させます。

アシスタント名を強調表示してから、**[詳細情報の表示（View Details）]** リンクをクリックすることにより、**[アシスタントの設定（Assistant Configuration）]** ウィンドウに移動できます。

ステップ 10 Manager Assistant によって制御される回線を設定するには、[使用可能な回線（Available Lines）] リストボックスから該当する回線を選択し、下向き矢印をクリックして [選択した回線（Selected Lines）] リスト ボックスに移動させます。
制御される回線が、常に共有回線 DN であることを確認します。

ステップ 11 **[保存]** をクリックします。
[**自動設定（Automatic Configuration**）] チェックボックスをオンにした場合、サービス パラメータが無効になると、メッセージが表示されます。 サービス パラメータが有効であることを確認してください。 自動設定が正常に完了すると、マネージャ デバイスがリセットされます。 デバイス プロファイルを設定した場合、マネージャは、ログアウトしてからデバイスにログインして、変更を有効にする必要があります。

共有回線のアシスタント ライン アピアランスの設定

管理者は、共有ラインアピアランスを使用して1つまたは複数の回線を設定できます。 Unified Communications Manager システムでは、電話番号が同じパーティション内の複数のデバイスに表示される場合、その電話番号は共有電話とみなされます。

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。**[ユーザ管理（User Management）]** > **[エンド ユーザ（End User）]**。

ステップ 2 **[検索(Find)]** をクリックします。
検索結果には、Unified Communications Manager で設定されているすべてのエンド ユーザが表示されます。

ステップ 3 選択したアシスタントのユーザ情報を表示するには、ユーザ名をクリックします。
[エンド ユーザ設定（End User Configuration）] ウィンドウが表示されます。

ステップ 4 [**関連リンク（Related Links**）] ドロップダウン リストから [**アシスタントの設定（Assistant Configuration**）] を選択し、[**移動（Go**）] をクリックします。
[**アシスタントの設定（Assistant Configuration**）] ウィンドウが表示されます。 [**自動設定（Automatic Configuration**）] チェックボックスをオンにすると、システムは、Cisco IP Manager Assistant サービス パラメータの設定に基づいて、ソフトキー テンプレートとインターコム回

線を自動的に設定します。さらに、システムは、インターコム回線のスピーカーフォンで自動応答を設定します。

ステップ 5 [**デバイス名（Device Name**）] ドロップダウン リストから、アシスタントに関連付けるデバイス名を選択します。

ステップ 6 [**インターコム回線（Intercom Line**）] ドロップダウン リストから、アシスタントのインターコム ライン アピアランスを選択します。

ステップ 7 [**プライマリ ライン（Primary Line**）] ドロップダウン リストから、アシスタントのプライマリ ラインを選択します。

a) 既存のマネージャの設定情報を表示するには、[**関連付けられたマネージャ（Associated Managers**）] リストでマネージャ名を強調表示してから、[**詳細情報の表示（View Details**）] をクリックします。
[**マネージャの設定（Manager Configuration**）] ウィンドウが表示されます。

b) [**アシスタントの設定（Assistant Configuration**）] ウィンドウに戻るには、アシスタント名を強調表示してから、**[マネージャの設定（Manager Configuration**）] ウィンドウで [**詳細情報の表示（View Details**）] リンクをクリックします。

[**関連付けられたマネージャ（Associated Manager**）] 選択リスト ボックスに、以前に設定されたマネージャの名前が表示されます。

ステップ 8 マネージャ回線をアシスタント回線に関連付けるには、[アシスタント回線へのマネージャの関連付け（Manager Association to Assistant Line）] 選択ボックスで、次の手順を実行します。

a) [**使用可能な回線（Available Lines**）] ドロップダウン リストから、マネージャ回線に関連付けるアシスタント回線を選択します。

b) [**マネージャ名（Manager Names**）] ドロップダウン リストから、このプロキシ回線を適用する事前設定されたマネージャ名を選択します。

c) [**マネージャ回線（Manager Lines**）] ドロップダウン リストから、このプロキシ回線を適用するマネージャ回線を選択します。

ステップ 9 **[保存]** をクリックします。
更新はすぐに有効になります。[**自動設定（Automatic Configuration**）] を選択すると、アシスタント デバイスが自動的にリセットされます。

Assistant Console プラグインのインストール

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）]**。
[プラグインの検索と一覧表示（Find and List Plugins）]ウィンドウが表示されます。

ステップ 2 **[検索(Find)]** をクリックします。
インストール可能なアプリケーション プラグインの一覧が表示されます。

ステップ 3 Cisco Unified CM Assistant Console の [ダウンロード（Download）]リンクをクリックして、実行可能ファイルを特定の場所に保存します。

ステップ 4 実行可能ファイルを実行します。

（注） Windows Vista PC にアプリケーションをインストールすると、セキュリティ ウィンドウが表示されることがあります。インストールの続行を許可します。

[Cisco Unified CallManager Assistant Console]インストール ウィザードが表示されます。

ステップ 5 [概要（Introduction）]ウィンドウで、[次へ（Next）]をクリックします。

ステップ 6 [ライセンス契約書（License Agreement）]ウィンドウで、[次へ（Next）]をクリックします。

ステップ 7 アプリケーションをインストールする場所を選択し、[次へ（Next）]をクリックします。

（注） デフォルトでは、`C:\Program Files\Cisco\ Unified CallManager Assistant Console` にアプリケーションがインストールされます。

ステップ 8 [インストール前の概要（Pre-installation Summary）]ウィンドウで概要を確認し、[インストール（Install）]をクリックします。
インストールが開始されます。

ステップ 9 インストールが完了したら、[終了（Finish）]をクリックします。

ステップ 10 コンソールにログインするために必要なユーザ名とパスワードをアシスタントに提供します。

ステップ 11 Assistant Console を起動するには、デスクトップのアイコンをクリックするか、**[プログラム開始（Start...Programs）]** メニューから **[Cisco Unified Communications Manager Assistant]** > **Assistant Console**を選択します。

ステップ 12 **[Cisco Unified Communications Manager Assistant の設定（Cisco Unified Communications Manager Assistant Settings）]** ウィンドウの **[詳細（Advanced）]** タブで、Assistant Console のトレースを有効化できます。

ステップ 13 Cisco IP Manager Assistant サービスがアクティブになっている Unified Communications Manager サーバのポート番号と IP アドレスまたはホスト名をアシスタントに提供します。 アシスタントが初めてコンソールにログインしたときには、アシスタントは、[Cisco Unified Communications Manager Assistant Server のポート（Cisco Unified Communications Manager Assistant Server Port）] と [Cisco Unified Communications Manager Assistant Server のホスト名または IP アドレス（Cisco Unified Communications Manager Assistant Server Hostname or IP Address）] の各フィールドに情報を入力する必要があります。

Manager Assistant の連携動作

機能	データのやり取り
一括管理ツール	一括管理ツールを使用して、ユーザを個々に追加するのではなく多数のユーザ（マネージャおよびアシスタント）を一度に追加できます。 一括管理ツールのテンプレートは、Cisco Unified IP 電話向けに [Cisco Unified CM Assistant 設定ウィザード（Cisco Unified CM Assistant Configuration Wizard）] で作成され、Unified Communications Manager インターコム回線のみをサポートします。 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。
発信側の正規化	発信側の正規化機能を設定している場合、Manager Assistant はローカライズおよびグローバル化されたコールを自動的にサポートします。 Manager Assistant はローカライズされた発信者番号をユーザインターフェイスに表示できます。 また、マネージャ宛の着信通話の場合、フィルタ パターンの一致が発生すると、Manager Assistant はローカライズおよびグローバル化された発信者番号を表示できます。
エクステンションモビリティ	Manager Assistant と Cisco エクステンションモビリティ機能を同時に使用できます。 エクステンションモビリティを使用して Cisco Unified IP 電話 にログインすると、その電話の Cisco IP Manager Assistant サービスは自動的に有効になります。 その後、Manager Assistant 機能にアクセスできます。 Cisco エクステンションモビリティの詳細については、エクステンションモビリティの概要 （501 ページ）を参照してください。
Internet Protocol Version 6（IPv6）	Manager Assistant は IPv6 をサポートしないため、Manager Assistant では電話の [IP アドレッシング モード（IP Addressing Mode）] が [IPv6 のみ（IPv6 Only）] の電話を使用することはできません。 電話で Manager Assistant を使用するには、電話で [IP アドレッシング モード（IP Addressing Mode）] を [IPv4 のみ（IPv4 Only）] または [IPv4 と IPv6（IPv4 and IPv6）] に設定していることを確認してください。

機能	データのやり取り
レポート ツール	Manager Assistant によって CDR Analysis and Reporting（CAR）ツールに統計情報が提供され、変更ログに設定の変更の概要が示されます。 管理者は、Unified CM の AssistantChangeLog*.txt でマネージャまたはアシスタント設定に行った変更の概要を表示できます。マネージャは、URL からマネージャの設定へアクセスすることで、デフォルトを変更できます。 アシスタントは、Assistant Console からマネージャのデフォルトを変更できます。 URL および マネージャの設定の詳細については、『*Cisco Unified Communications Manager Assistant User Guide*』を参照してください。 マネージャまたはアシスタントが変更を加えると、その変更は **ipma_changeLogxxx.log** と呼ばれるログ ファイルに送信されます。 ログ ファイルは、Cisco IP Manager Assistant サービスを実行するサーバに存在します。次のコマンドを使用してログファイルを取得します。 **file get activelog tomcat/logs/ipma/log4j/** ログファイルのダウンロードの詳細については、『*Cisco Unified Real -Time Monitoring Tool Administration Guide*』を参照してください。
CDR Analysis and Reporting	Manager Assistant は、マネージャとアシスタントの通話終了の統計とインベントリ レポートをサポートします。 CAR ツールは通話終了の統計をサポートします。Cisco Unified Serviceability はインベントリ レポートをサポートします。 詳細については、次のガイドを参照してください。 • 『*Cisco Unified Serviceability Administration Guide*』 • Call Reporting and Billing Administration Guide for Cisco Unified Communications Manager

機能	データのやり取り
マルチレベルの優先およびプリエンプション	次の点において、共有回線サポートを持つ Manager Assistant および MLPP の間の連携動作について説明します。 • システムは、Manager Assistant によるコールの処理においてコールの優先順位を保持します。 たとえば、アシスタントがコールを転送すると、システムはコールの優先順位を保持します。 • 優先順位の高いコールのフィルタリングは、他のすべてのコールと同様に発生します。 コールの優先順位は、コールがフィルタ処理されるかどうかには影響しません。 • Manager Assistant にはコールの優先順位に関する情報がないため、Assistant Console でコールの優先順位が改めて示されることはありません。
インターコム	Manager Assistant は、次の 2 つのタイプのインターコムをサポートします。 • Manager Assistant インターコム（Cisco Unified IP 電話 7940 および 7960 で使用）。 DN 設定およびエンド ユーザ（マネージャとアシスタント）の設定ウィンドウを使用して、このインターコム機能を設定できます。 • Unified Communications Manager インターコム（Cisco Unified IP 電話 7940 および 7960 で使用）。 インターコム パーティション、インターコム コーリング サーチ スペース、インターコム電話番号、インターコム トランスレーション パターン、DN、およびエンド ユーザ（マネージャとアシスタント）の設定ウィンドウを使用して、このインターコム機能を設定できます。
メッセージ受信インジケータ	メッセージ受信インジケータ機能は、プロキシ回線サポートのみと連携して動作します。 メッセージ受信インジケータ（MWI）のオンまたはオフ番号には、コーリング サーチ スペースのマネージャ回線のパーティションが必要です。 パーティションは、それぞれのコーリング サーチ スペース内で任意の優先順位に設定できます。

機能	データのやり取り
Time-of-Day ルーティング	Time-of-Day 機能は、プロキシ回線サポートのみと連携して動作します。 Time-of-Day ルーティングは、コールが作成された時間に応じて、コールをそれぞれの場所にルーティングします。たとえば、営業時間中は、コールはマネージャのオフィスにルーティングされ、それ以降の時間は、コールはボイスメール サービスに直接送信されます。 時間帯ルーティングの詳細については、Cisco Unified Communications Manager システム設定ガイドを参照してください。

Manager Assistant の制約事項

機能	制約事項
アシスタント コンソール アプリケーション	Microsoft Internet Explorer 7（以降）を持つコンピュータにアシスタント コンソール アプリケーションをインストールするには、Assistant Console をインストールする前に、Microsoft Java 仮想マシン（JVM）をインストールします。
コール管理機能	Assistant Console では、ハント グループまたはキュー、録音とモニタリング、ワンタッチ コール ピックアップ、およびオンフック転送（転送を完了するために [転送（Transfer）] ソフトキーを押してオンフックにすることでコールを転送する機能）はサポートされません。

機能	制約事項
Cisco IP 電話	Manager Assistant は Cisco Unified IP 電話 7940 と 7960 を除く Cisco Unified IP 電話 7900 シリーズの SIP をサポートします。 Manager Assistant は、複数の Cisco IP Manager Assistant サーバ（プール）を設定して、最大 3500 名のマネージャと 3500 名のアシスタントをサポートします。複数のプールを有効にする場合、マネージャおよびそのマネージャに設定されたアシスタントが同じプールに属している必要があります。 Cisco Unified IP 電話 7960 と 7940 は Unified Communications Manager Assistant インターコム回線機能のみをサポートします。Cisco Unified IP 電話 7900（7940 と 7960 を除く）は Unified Communications Manager インターコム機能のみをサポートします。 1 名のマネージャには最大 10 名のアシスタントを指定でき、1 名のアシスタントは最大 33 名のマネージャをサポートできます（各マネージャに 1 つの Unified Communications Manager 制御回線がある場合）。 1 名のマネージャを一度に支援できるのは 1 名のアシスタントのみです。 Manager Assistant は、Unified Communications Manager クラスタあたり最大 3500 人のマネージャと 3500 人のアシスタントをサポートします。
インターコム	アップグレード後に、着信インターコム回線を使用する Manager Assistant ユーザは、Unified Communications Manager インターコム機能に自動的にアップグレードされません。 システムは Unified Communications Manager インターコム機能と通常回線の間のコールをサポートしていません（Manager Assistant インターコム回線として設定される可能性があります）。
シングル サインオン	Manager Assistant は、シングル サインオン環境ではサポートされません。
スピード ダイヤル	Cisco Unified IP 電話 7940、7942、および 7945 は、2 つの回線または短縮ダイヤル ボタンのみサポートします。

Cisco Unified Communications Manager Assistant のトラブルシューティング

ここでは、Manager Assistant とクライアントデスクトップのトラブルシューティング ツール、および Manager Assistant のトラブルシューティングについて説明します。

ツールの説明	Location
Cisco Unified CM Assistant サーバのトレース ファイル	トレース ファイルは、Cisco IP Manager Assistant サービスを実行するサーバに存在します。 これらのファイルは次のいずれかの方法でサーバからダウンロードできます。 • CLI コマンド **file get activelog tomcat/logs/ipma/log4j** を使用する。 • Cisco Unified Real-Time Monitoring Tool（RTMT）のトレース収集機能を使用する。 詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。 デバッグ トレースをイネーブルにするには、**[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] > [トレース（Trace）] > [設定（Configuration）]** を選択します。
Cisco IPMA クライアントのトレース ファイル	クライアントのデスクトップ上にある **$INSTALL_DIR\logs\ACLog*.txt**（Unified CM Assistant の Assistant Console と同じ場所）。 デバッグ トレースを有効にするには、Assistant Console の **[設定（Settings）]** ダイアログボックスに移動します。 **[詳細設定（Advanced）]** パネルで、**[トレースを有効にする（Enable Trace）]** チェックボックスをオンにします。 （注） このチェックボックスをオンにすると、デバッグ トレースだけが有効になります。 エラー トレースは常にオンになっています。
Cisco IPMA クライアントのインストール トレース ファイル	クライアントのデスクトップ上にある **$INSTALL_DIR\InstallLog.txt**（Assistant Console と同じ場所）。
Cisco IPMA クライアントの AutoUpdater トレース ファイル	クライアントのデスクトップ上にある **$INSTALL_DIR\UpdatedLog.txt**（Unified CM Assistant Console と同じ場所）。

ツールの説明	Location
インストール ディレクトリ	デフォルトでは、C:\Program Files\Cisco\Unified Communications Manager Assistant Console\

発信側にリオーダー音が聞こえる

問題

発信側に次のリオーダー音またはメッセージが聞こえます。

「ダイヤルしたコールを完了できません。（This call cannot be completed as dialed.）」

考えられる原因

発信側回線のコーリング サーチ スペースが適切に設定されていません。

ソリューション

回線のコーリング サーチ スペースを確認します。 設定の詳細については、Cisco Unified Communications Manager システム設定ガイド を参照してください。

また、Cisco Dialed Number Analyzer サービスを使用して、コーリング サーチ スペース内の不備を確認することもできます。 詳細については、『*Cisco Unified Communications Manager Dialed Number Analyzer Guide*』を参照してください。

フィルタリングをオン/オフにするとコールがルーティングされない

問題

コールが適切にルーティングされません。

考えられる原因 1

Cisco CTI Manager サービスが停止している可能性があります。

ソリューション 1

[Cisco Unified Serviceability] > **[ツール（Tools）]** > **[コントロール センターの機能サービス（Control Center - Feature Services）]** から、Cisco CTI Manager および Cisco IP Manager Assistant サービスを再起動します。

考えられる原因 2

Unified Communications Manager Assistant ルート ポイントが適切に設定されていません。

ソリューション 2

Unified Communications Manager Assistant CTI ルート ポイントの電話番号と、Unified Communications Manager に設定されているすべてのマネージャのプライマリ 電話番号に一致するようにワイルド カードを使用します。

考えられる原因 3

マネージャの電話機のステータス ウィンドウに「フィルタ使用不可（Filtering Down）」というメッセージが表示されます。 このメッセージは、Unified Communications Manager Assistant CTI ルート ポイントが削除されているか、稼働していない可能性があることを示します。

ソリューション 3

次の手順を実行して、CTI ルート ポイントを設定し、Cisco IP Manager Assistant サービスを再起動します。

1. Cisco Unified CM 管理（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。
2. 該当するルート ポイントを見つけるか、または新しいルート ポイントを追加します。 設定の詳細については、Cisco Unified Communications Manager システム設定ガイド を参照してください。
3. **[Cisco Unified Serviceability] > [ツール（Tools）] > [コントロール センターの機能サービス（Control Center - Feature Services）]** から、Cisco CTI Manager および Cisco IP Manager Assistant サービスを再起動します。

Cisco IP Manager Assistant Service に到達できない

問題

Assistant Console を開くと、次のメッセージが表示されます。

`Cisco IPMA サービスに到達できません（Cisco IPMA Service Unreachable）`

考えられる原因 1

Cisco IP Manager Assistant サービスが停止している可能性があります。

ソリューション 1

[Cisco Unified Serviceability] > [ツール（Tools）] > [コントロール センターの機能サービス（Control Center—Feature Services）] から Unified Communications Manager Assistant を再起動します。

考えられる原因 2

プライマリおよびセカンダリ Unified Communications Manager Assistant サーバのサーバ アドレスが DNS 名として設定されていますが、それらの DNS 名が DNS サーバで設定されていません。

ソリューション 2

次の手順を実行して DNS 名を置き換えます。

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）] > [サーバ（Server）]**。
2. サーバの DNS 名を対応する IP アドレスに置き換えます。
3. **[Cisco Unified Serviceability] > [ツール（Tools）] > [コントロール センターの機能サービス（Control Center—Feature Services）]** から Unified Communications ManagerAssistant を再起動します。

考えられる原因 3

Cisco CTI Manager サービスが停止している可能性があります。

ソリューション 3

[Cisco Unified Serviceability] > [ツール（Tools）] > [コントロール センターの機能サービス（Control Center—Feature Services）] から Unified Communications Manager Assistant を再起動します。

考えられる原因 4

Unified Communications Manager Assistant サービスは CTI 接続をセキュア モードで開くように設定されているかもしれませんが、セキュリティ設定が完了していない可能性があります。

この状況が発生した場合は、アラーム ビューアまたは Unified Communications Manager Assistant サービス ログに次のメッセージが表示されます。

`IPMA サービスが初期化できません。プロバイダーを取得できませんでした（IPMA Service cannot initialize - Could not get Provider）`

ソリューション #4

Cisco IP Manager Assistant サービスのサービス パラメータで、セキュリティ設定を確認します。

[Cisco Unified Serviceability] > [ツール（Tools）] > [コントロール センターの機能サービス（Control Center—Feature Services）] から Unified Communications Manager Assistant を再起動します。

Cisco IP Manager Assistant Service を初期化できない

問題

Cisco IP Manager Assistant サービスで CTI Manager への接続をオープンできず、次のメッセージが表示されます。

`IPMA サービスが初期化できません。プロバイダーを取得できませんでした（IPMA Service cannot initialize - Could not get Provider）`

考えられる原因

Cisco IP Manager Assistant サービスで CTIManager への接続をオープンできません。 アラームビューアまたは Unified CM Assistant サービス ログでメッセージを確認できます。

ソリューション

[Cisco Unified Serviceability] > **[ツール（Tools）]** > **[コントロール センターの機能サービス（Control Center - Feature Services）]** から、Cisco CTI Manager および Cisco IP Manager Assistant サービスを再起動します。

Web からの Assistant Console のインストールが失敗する

問題

Web からの Assistant Console のインストールが失敗します。 次のメッセージが表示されます。

例外：`java.lang.ClassNotFoundException: InstallerApplet.class（Exception: java.lang.ClassNotFoundException: InstallerApplet.class）`

考えられる原因

Unified Communications Manager Assistant Console の標準インストールで Microsoft JVM の代わりに Sun Java プラグイン仮想マシンを使用するとエラーの原因となります。

ソリューション

管理者は、Sun Java プラグインをサポートしている JSP ページである次の URL にユーザを誘導してください。

`https://<servername>:8443/ma/Install/IPMAConsoleInstallJar.jsp`

HTTP ステータス 503：アプリケーションは現在使用できません

問題

http://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp で次のエラー メッセージが表示されます。

HTTP ステータス 503：アプリケーションは現在使用できません

考えられる原因

Cisco IP Manager Assistant サービスがアクティブになっていないか、または実行されていません。

ソリューション

Cisco IP Manager Assistant サービスがアクティブになっていることを確認します。確認するには、**[Cisco Unified Serviceability]** > **[ツール（Tools）]** > **[サービスの開始（Service Activation）]** で、サービスのアクティベーション ステータスをチェックします。

Cisco IP Manager Assistant サービスがすでにアクティブになっている場合は、**[Cisco Unified Serviceability]** > **[ツール（Tools）]** > **[コントロール センターの機能サービス（Control Center—Feature Services）]** から Unified Communications Manager を再起動します。

マネージャがログアウトしてもサービスが動作している

問題

マネージャが Unified Communications Manager Assistant からログアウトしても、サービスは継続して実行されます。 マネージャの IP Phone のディスプレイの表示が消えます。 フィルタリングがオンになっていますがコールはルーティングされません。マネージャがログアウトしたことを確認するには、Cisco Unified Real-Time Monitoring Tool を使用してアプリケーション ログを表示します。 Cisco IP Manager Assistant サービスがログアウトされたことを示す、Cisco Java アプリケーションからの警告がないかどうかを調べます。

考えられる原因

マネージャがソフトキーを 1 秒間に 5 回以上押しました（最大許容回数は 4 回）。

ソリューション

Unified Communications Manager の管理者は、マネージャの設定を更新する必要があります。次の手順を実行して問題を修正します。

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）]**。

   [ユーザの検索と一覧表示（Find and List Users）] ウィンドウが表示されます。

2. [検索（Search）] フィールドにマネージャ名を入力し、[検索（Find）]をクリックします。
3. 検索結果リストから、更新するマネージャを選択します。

   [エンド ユーザ設定（End User Configuration）] ウィンドウが表示されます。

4. **[関連リンク（Related Links）]** ドロップダウン リストから **[Cisco IPMA マネージャ（Cisco IPMA Manager）]** を選択し、**[移動（Go）]** をクリックします。

5. マネージャの設定に必要な変更を行い、[更新（Update）]をクリックします。

マネージャがアシスタントプロキシ回線で鳴っているコールを代行受信できない

問題

マネージャがアシスタント プロキシ回線で呼び出しているコールを代行受信できません。

考えられる原因

プロキシ回線のコーリング サーチ スペースが適切に設定されていません。

ソリューション

アシスタント電話機のプロキシ回線のコーリング サーチ スペースを確認します。 次の手順を実行して問題を修正します。

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）]**。

   [電話の検索と一覧表示（Find and List Phones）] 検索ウィンドウが表示されます。

2. アシスタント電話機をクリックします。

   [電話の設定（Phone Configuration）] ウィンドウが表示されます。

3. 電話機と電話番号（回線）のコーリング サーチ スペース設定を確認し、必要に応じて更新します。

「ページが見つかりません（No Page Found）」エラー

問題

`http://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp` で次のエラーメッセージが表示されます。

「ページが見つかりません（No Page Found）」エラー

考えられる原因 1

ネットワークに問題があります。

ソリューション 1

クライアントがサーバに接続していることを確認します。 URL で指定されているサーバ名に対して ping を実行し、到達可能であることを確認します。

考えられる原因 2

URL のつづりが間違っています。

ソリューション 2

URL では大文字と小文字が区別されるため、URL が指示にある URL と正確に一致していることを確認します。

システムエラーが発生しました。システム管理者にお問い合わせください。（System Error - Contact System Administrator）

問題

Assistant Console を開くと、次のメッセージが表示されます。

システム エラーが発生しました。システム管理者にお問い合わせください。（System Error - Contact System Administrator）

考えられる原因 1

Unified Communications Manager をアップグレードした可能性があります。 Unified Communications Manager をアップグレードするときに、システムは Assistant Console を自動的にアップグレードしません。

ソリューション 1

[スタート（Start）] > [プログラム（Programs）] > [Cisco Unified Communications Manager Assistant] > [Assistant Console のアンインストール（Uninstall Assistant Console）] を選択してコンソールをアンインストールし、URL **https://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp** からコンソールを再インストールします。

考えられる原因 2

ユーザがデータベースに正しく設定されていません。

ソリューション 2

[Cisco Unified CM の管理（Cisco Unified CM Administration）] を使用してユーザ ID とパスワードが Unified Communications Manager のユーザとして実行されていることを確認します。

考えられる原因 3

アシスタントからマネージャを削除したときに、[Cisco Unified CM の管理（Cisco Unified CM Administration）] でアシスタントに空白行が残されました。

ソリューション 3

[アシスタントの設定（Assistant Configuration）] ウィンドウでプロキシ行を再割り当てします。

Cisco IP Manager Assistant サービスがダウンしているときにマネージャにコールできない（Unable to Call Manager When Cisco IP Manager Assistant Service is Down）

問題

Cisco IP Manager Assistant サービスがダウンしているときに、コールがマネージャに適切にルーティングされません。

考えられる原因

Unified Communications Manager Assistant CTI ルート ポイントで [無応答時転送（Call Forward No Answer）] が有効になっていません。

ソリューション

次の手順を実行して、Unified Communications Manager Assistant ルート ポイントを適切に設定します。

1. Cisco Unified CM 管理（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。

   [CTI ルートポイントの検索と一覧表示（Find and List CTI Route Points）] 検索ウィンドウが表示されます。

2. **[検索(Find)]** をクリックします。

   設定済み CTI ルート ポイントのリストが表示されます。

3. 更新する Unified Communications Manager Assistant CTI ルート ポイントを選択します。

4. [CTI ルートポイントの設定（CTI Route Point Configuration）] ウィンドウの [関連付け（Association）] 領域で、更新する回線をクリックします。

5. [コール転送とコール ピックアップの設定（Call Forward and Call Pickup Settings）] セクションで、[無応答時転送（Forward No Answer Internal、内部）] チェックボックスおよび [無応答時転送（Forward No Answer External、外部）] チェックボックスをオンにし、[カバレッジ/接続先（Coverage/Destination）] フィールドに CTI ルート ポイントの DN を入力します（たとえば、ルート ポイント DN 1xxx の場合、CFNA に 1xxx を入力します）。

6. [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 [CSS-M-E]（または、該当するコーリング サーチ スペース）を選択します。

7. **[更新(Update)]** をクリックします。

ユーザ認証に失敗する

問題

Assistant Console からログイン ウィンドウを使用してサイン インするときにユーザ認証に失敗します。

考えられる原因

次の原因が考えられます。

- データベースでユーザが正しく管理されていない。
- アシスタントまたはマネージャとしてユーザが正しく管理されていない。

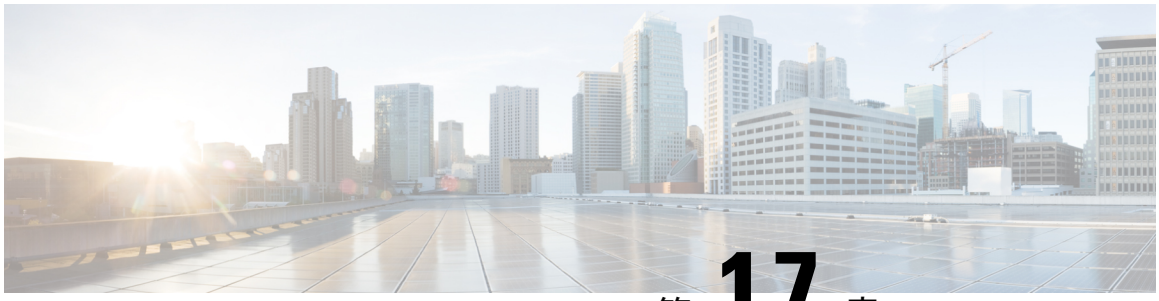
ソリューション

[Cisco Unified CM の管理（Cisco Unified CM Administration）] を使用してユーザ ID とパスワードが Unified Communications Manager のユーザとして実行されていることを確認します。

Unified Communications Manager Assistant ユーザ情報を関連付けることによって、ユーザをアシスタントまたはマネージャとして実行する必要があります。ユーザ情報には、[Cisco Unified CM Administration] で **[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** を選択してアクセスします。

第 VII 部

ボイス メッセージング機能



第 17 章

オーディオ メッセージ受信インジケータ

オーディオ メッセージ受信インジケータの概要

ユーザに新しいボイス メッセージを通知するために、Cisco Unified IP 電話 で断続ダイヤル トーンを再生するようにオーディオ メッセージ受信インジケータ（AMWI）を設定できます。 ボイス メッセージが残されている回線で電話がオフフックになるたびに、断続ダイヤル トーンが鳴ります。

クラスタ内のすべての電話機または特定の電話番号で AMWI を設定できます。 電話番号レベルの設定は、クラスタ全体の設定よりも優先されます。

オーディオ メッセージ受信インジケータの前提条件

AMWI は、電話ファームウェア リリース 8.3(1) 以降が動作している Cisco Unified IP 電話でのみ設定できます。

オーディオ メッセージ受信インジケータ設定のタスク フロー

始める前に

- オーディオ メッセージ受信インジケータの前提条件 （253 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	電話機能一覧の生成 （5 ページ）	オーディオ メッセージ受信インジケータ機能をサポートするデバイスを特定するためにレポートを生成します。
ステップ 2	オーディオ メッセージ受信インジケータのサービス パラメータの設定 （254 ページ）	クラスタ内のすべての電話で AMWI のデフォルト設定を行います。
ステップ 3	電話番号のオーディオ メッセージ受信インジケータの設定 （255 ページ）	デバイスに関連付けられている電話番号の AMWI を設定します。
ステップ 4	SIP プロファイルでのオーディオ メッセージ受信インジケータの設定 （255 ページ）	SIP プロファイルの AMWI を設定します。 SIP 電話の AMWI を設定するには、次の手順を実行します。

オーディオ メッセージ受信インジケータのサービス パラメータの設定

この手順では、クラスタ内のすべての電話機に AMWI デフォルト設定を実行する方法について説明します。

始める前に

電話機能一覧の生成 （5 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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

ステップ 2 [サーバ（Server）] ドロップダウン リストで、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（機能 - 全般）（Clusterwide Parameters (Feature - General)**）] セクションで、[**オーディオ メッセージ受信インジケータのポリシー（Audible Message Waiting Indication Policy**）] サービス パラメータを選択します。 このパラメータによって、クラスタ内の全デバイスでオーディオ メッセージ受信インジケータをオンにするかオフにするか決定します。

ステップ 5 **[保存（Save）]** をクリックします。

電話番号のオーディオ メッセージ受信インジケータの設定

デバイスに関連付けられている電話番号用に AMWI を設定するには、次の手順に従ってください。

（注） 個々の電話番号での AMWI 設定は、クラスタ全体の設定より優先されます。

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。**[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 [関連付け（Association）]セクションで、[新規 DN を追加（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 3 [オーディオ メッセージ受信インジケータのポリシー（Audible Message Waiting Indicator Policy）] を選択します。 次のいずれかのオプションを選択します。

- **[オフ（Off）]**
- **[オン（On）]**：このオプションを選択すると、ハンドセットを取り上げたときにユーザは断続ダイヤル トーンを受信します。

  .
- **[デフォルト(Default)]**：このオプションを選択すると、電話機は、システム レベルで設定されたデフォルトを使用します。

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 5 **[保存（Save）]** をクリックします。

SIP プロファイルでのオーディオ メッセージ受信インジケータの設定

SIP プロファイルのオーディオ メッセージ受信インジケータ（AMWI）を設定するには、次の手順に従います。

（注） 個々の SIP プロファイルの AMWI 設定は、クラスタ全体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）] > [SIP プロファイル（SIP Profile）]** の順に選択します。
[**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 使用する検索条件を入力し、[**検索（Find**）] をクリックします。
ウィンドウに検索条件と一致する SIP プロファイルのリストが表示されます。

ステップ 3 更新する SIP プロファイルをクリックします。
[**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 電話がオフフックで、メッセージを受信している場合の断続ダイヤル トーンを有効にするには、[**メッセージがある場合は断続音（Stutter Message Waiting**）] 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。

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

オーディオメッセージ受信インジケータのトラブルシューティング

電話でオーディオ メッセージ受信インジケータが再生されない

問題 新着ボイス メッセージをユーザに通知する断続ダイヤル トーンが電話で再生されません。

ユーザが SCCP 電話を使用している場合には、次の点を確認してください。

- 電話ファームウェアのリリースが 8.3(1) 以降であることを確認します。
- ユーザがオフフックになった回線と電話の AMWI 設定を確認します。
- Cisco CallManager サービスがサーバ上で実行されていることを確認します。
- 電話機と Unified Communications Manager の間のスニファ トレースをキャプチャします。トーン タイプが 42 の StartTone メッセージが電話で受信されることを確認します。

ユーザが SIP 電話を使用している場合には、次の点を確認してください。

- 電話ファームウェアのリリースが 8.3(1) 以降であることを確認します。

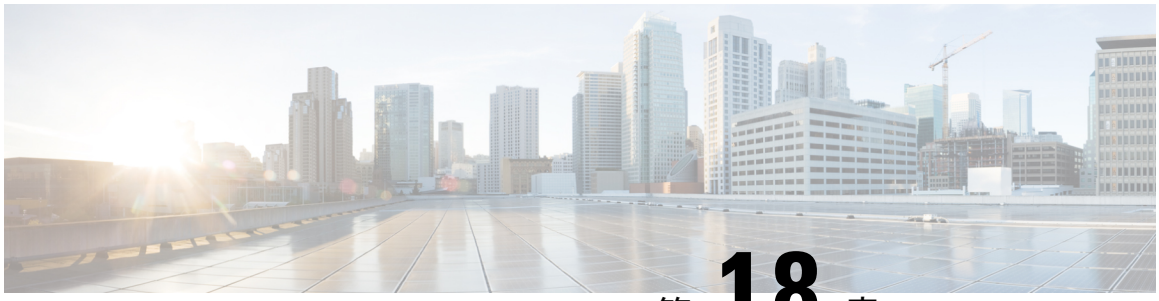
- 回線（電話番号）の設定を確認します。 電話には、line1_msgWaitingAMWI : 1、line2_msgWaitingAMWI : 0 などの設定が表示される必要があります。
- [Cisco Unified CM の管理（Cisco Unified CM Administration）] の **[SIP プロファイルの設定（SIP Profile Configuration）]** ウィンドウで **[メッセージがある場合は断続音（Stutter Message Waiting）]** チェック ボックスがオンになっていることを確認します。

ローカライズされた AMWI トーンが特定のロケールで再生されない

問題 英語以外のロケールに設定されている電話機で、ローカライズされたトーンが再生されません。

解決法 次の点をチェックします。

- Cisco Unified CM の管理から、[デバイス プロファイルの設定（Device Profile Configuration）] ウィンドウ（**[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）]**）の [ユーザ ロケール（User Locale）] を確認します。
- ロケールの変更後、ユーザは電話機をリセットする必要があります。
- `user/local/cm/tftp /<locale name>` ディレクトリを確認し、AMWI トーンがローカライズされた g3-tones.xml ファイルで定義されていることを確認します。



第 18 章

即時転送

即時転送の概要

即時転送機能とは、コールをボイスメール システムに即時に転送できるようにする Unified Communications Manager の補足サービスです。 即時転送機能によりコールが転送されると、回線が新しいコールの発信または着信に使用できるようになります。 即時転送機能にアクセスするには、IP フォンで [即転送（iDivert）] または [転送（Divert）] ソフトキーを使用します。

即時転送には次の機能があります。

- コールを次の方法でボイスメール システムに転送します。
  - 従来の即転送では、即転送機能を起動したユーザのボイス メールボックスにコールが転送されます。
  - 拡張即転送では、即転送機能を起動したユーザのボイス メールボックスまたは元の着信側のボイス メールボックスのいずれかに、コールが転送されます。
- [コール オファリング（Call Offering）]、[コール保留中（Call on Hold）]、または [コール アクティブ（Call Active）] 状態にある着信コールを転送します。
- [コール アクティブ（Call Active）] および [コール保留中（Call on Hold）] 状態の発信コールを転送します。

（注） CTI アプリケーションでは即時転送機能を使用できませんが、即時転送と同じ機能を実行する CTI リダイレクト操作があります。アプリケーション開発者は、即時転送に CTI リダイレクト操作を使用できます。

即時転送の前提条件

- ボイスメール プロファイルとハント パイロットを設定する必要があります。

  ボイスメール プロファイルとハント パイロットの設定方法については、下記を参照してください。Cisco Unified Communications Manager システム設定ガイド

- 以下のデバイスが即時転送をサポートします。
  - Skinny Client Control Protocol（SCCP）を使用する Cisco Unity Connection などのボイス メッセージング システム。
  - [クラスタ全体で従来の即転送を使用する（Use Legacy Immediate Divert）] とクラスタ全体で [即転送中の QSIG を許可する（Allow QSIG During iDivert）] サービス パラメータの設定による QSIG デバイス（QSIG 対応 H.323 デバイス、MGCP PRI QSIG T1 ゲートウェイ、および MGCP PRI QSIG E1 ゲートウェイ）。
  - 次の表に、[転送（Divert）] ソフトキーまたは [即転送（iDivert）] ソフトキーを使用する電話を示します。

表 *21 :* 即転送ソフトキーを使用する *Cisco Unified IP* 電話

Cisco Unified IP 電話モデル	**[転送（Divert）] ソフトキー**	**[即転送（iDivert）] ソフトキー**	**ソフトキー テンプレートで設定するもの**
Cisco Unified IP Phone 6900 シリーズ（6901 と 6911 を除く）	X		iDivert
Cisco Unified IP Phone 7900 シリーズ		X	iDivert
Cisco Unified IP Phone 8900 シリーズ	X		デフォルトで設定される
Cisco Unified IP Phone 9900 シリーズ	X		デフォルトで設定される

（注） Cisco Unified IP 電話 8900 および 9900 シリーズには、デフォルトで、[転送（Divert）] ソフトキーが割り当てられます。

即時転送の設定タスク フロー

始める前に

- 即時転送の前提条件 （260 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	即時転送のサービス パラメータの設定（262 ページ）	即時転送をさまざまなデバイスやアプリケーションにわたって有効にするには、サービス パラメータを設定します。
ステップ 2	即時転送のソフトキー テンプレートの設定 （263 ページ）	ソフトキー テンプレートを作成および設定し、そのテンプレートに [即転送（iDivert）] ソフトキーを追加します。
ステップ 3	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 （264ページ）を行うには、次のサブタスクを完了します。 • 共通デバイス設定へのソフトキー テンプレートの追加 （265ページ） • 電話機と共通デバイス設定の関連付け （266 ページ）	**（オプション）** 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 4	電話機とソフトキー テンプレートの関連付け （266 ページ）	**（オプション）** 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。

即時転送のサービス パラメータの設定

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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

ステップ 2 [サーバ（Server）] ドロップダウン リストで、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 該当するサービス パラメータを設定し、[保存（Save）] をクリックします。

表 *22*：即時転送のサービス パラメータ フィールド

フィールド	説明
[コール パークの表示タイマー（Call Park Display Timer）]	IP Phone の即転送のテキスト表示のためのタイマーを制御するために、0 ～ 100（1 と 100 を含む）の数値を入力します。 このサーバまたは Cisco CallManager サービスと即転送が設定されているクラスタ内の各サーバに対してこのタイマーを設定します。 このサービス パラメータのデフォルト値は 10 秒です。
[レガシーの即転送の使用（Use Legacy Immediate Divert）]	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。 • [はい（True）]：即転送機能を呼び出すユーザは、着信コールを自分独自のボイス メールボックスのみに転送できます。 これがデフォルト設定です。 • [いいえ（FALSE）]：即転送により、元の着信側のボイス メールボックスまたは即転送機能を呼び出すユーザのボイス メールボックスのいずれかへの着信コールの転送が可能です。
[即転送中の QSIG の許可（Allow QSIG During iDivert）]	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。 • [はい（True）]：即転送は、コールを QSIG、SIP、および QSIG 対応 H.323 デバイスに到達できるボイスメール システムに転送します。 • [いいえ（FALSE）]：即転送は、QSIG または SIP トランクを介したボイスメール システムへのアクセスをサポートしていません。 これがデフォルト設定です。

フィールド	説明
[即転送ユーザ応答タイマー（Immediate Divert User Response Timer）]	コールの転送先を選択するために即転送ソフトキー ユーザに与えられる時間を指定するために 5 ～ 30（5 と 30 を含む）の数字を入力します。 ユーザが転送先を選択しない場合、コールは接続されたままになります。 このサービス パラメータのデフォルト値は 5 秒です。

即時転送のソフトキー テンプレートの設定

着信コールまたは発信コールを転送するには、ソフトキーテンプレートを設定し、そのテンプレートに [即時転送（iDivert）] ソフトキーを割り当てます。 [即時転送（iDivert）] ソフトキーは、次のコール状態で設定できます。

- 接続されている状態
- 保留中
- 呼び出し

即時転送は、次のコール状態をサポートします。

- 着信：
  - コールのオファー（ソフトキー テンプレートでは呼び出しとして示される）。
  - 保留されているコール
  - 通話中のコール
- 発信：
  - 保留されているコール
  - 通話中のコール

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）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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。

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

これはオプションです。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）]** に追加します。
- ソフトキー テンプレートを**共通デバイス設定**に追加します。

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、次を参照してください。電話機とソフトキーテンプレートの関連付け （266 ページ）

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ソフトキー テンプレートの追加 （265 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 （266 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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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

（オプション） 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。

始める前に

即時転送のソフトキー テンプレートの設定 （263 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、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。

即時転送の連携動作

機能	データのやり取り
マルチレベルの優先およびプリエンプション	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。 代替パーティ転送（コールの優先順位）がアクティブ化されると、無応答時転送（CFNA）は非アクティブ化されます。
通話転送	[電話番号の設定（Directory Number Configuration）] ウィンドウで [無応答時転送（Forward No Answer）] が設定されていない場合、コール転送はクラスタ全体の CFNA タイマー サービス パラメータ [無応答時転送タイマー（Forward No Answer Timer）] を使用します。 コールが転送されるのと同時にユーザが [即転送（iDivert）] ソフトキーを押すと、コールはボイス メッセージ メールボックスではなく、割り当てられたコール転送電話番号に転送されます（これはタイマーが短すぎたためです）。 この状況を解決するには、CFNA タイマー サービス パラメータに十分な時間（例：60 秒）を設定します。
呼詳細レコード（CDR）	即時転送は CDR のフィールド（たとえば、joinOnbehalfOf および lastRedirectRediectOnBehalfOf など）の [代表（Onbehalf）] の即時転送コード番号を使用します。
コールパークとダイレクト コール パーク	ユーザ A がユーザ B に発信し、ユーザ B がコールをパークすると、ユーザ B はコールを取得し、[即転送（iDivert）] または [転送（Divert）] ソフトキーを押すことで、コールをボイス メッセージング メールボックスに送信することを決定します。 ユーザ A はユーザ B のボイス メッセージ メールボックスのグリーティングを取得します。
会議	会議参加者が [即転送（iDivert）] ソフトキーを押すと、残りの会議参加者は即時転送イニシエータのボイス メッセージング メールボックスのグリーティングを受信します。 会議タイプには、アドホック、ミートミー、割り込み、C 割り込み、および参加があります。

機能	データのやり取り
ハント リスト	ハント リスト パイロットを通じて（ハンティング アルゴリズムの一部として）電話に直接届くコールの場合、[レガシー即転送の使用（Use Legacy Immediate Divert）] クラスタ全体サービス パラメータが True に設定されていれば、[即転送（iDivert）] ソフトキーはグレー表示になります。それ以外の場合、グレー表示にはなりません。 ハント リスト パイロットを通じて（ハンティング アルゴリズムの一部として）電話に直接届かないコールの場合、[レガシー即転送の使用（Use Legacy Immediate Divert）] クラスタ全体サービス パラメータが True または False に設定されていれば、[即転送（iDivert）] ソフトキーはグレー表示にはなりません。 （注） デスク フォン モードの Jabber では、iDivert 機能の VM へのリダイレクションは CTI アプリケーションで行われます。この場合、[レガシー即時転送を使用する]パラメータは有効ではなく、HP 番号が音声メール サーバに転送情報として送信されます。
自動コール ピックアップ	[レガシー即転送の使用（Use Legacy Immediate Divert）] クラスタ全体サービス パラメータが False に設定され、[自動コール ピックアップ有効化（Auto Call Pickup Enabled）] クラスタ全体サービス パラメータが True に設定され、コール ピックアップ グループのユーザがコール ピックアップを使用してコールに応答する場合、[即転送（iDivert）] ソフトキーが押されると、IP フォンのディスプレイにユーザの選択肢は何も表示されません。

即時転送の制約事項

制約事項	説明
ボイス メール プロファイル（Voice Mail Profile）	ボイスメール システムとの QSIG 統合を使用している場合は、ボイス メール パイロットとボイスメール マスクのどちらかまたはその両方を含むボイスメール プロファイルで、[これをシステムのデフォルト ボイス メール プロファイルにする（Make this the default Voice Mail Profile for the System）]チェックボックスをオフのままにする必要があります。 デフォルトの [ボイス メール プロファイル（Voice Mail Profile）] 設定が、常に [ボイス メールなし（No Voice Mail）] に設定されていることを確認します。
不在転送（CFA）と話中転送（CFB）	不在転送（CFA）と話中転送（CFB）がアクティブになっている場合、システムは即時転送をサポートしません（CFA と CFB が即時転送より優先されます）。

制約事項	説明
ビジー ボイスメール システム	即転送は、ローカルまたはSCCP接続経由でボイスメール システムに到達したときに、ボイスメール ポートのビジー状態を検出します。 (注) 即時転送は、ビジー ボイスメール ポートにコールを転送できません。ボイスメール ポートは、ルートまたはハント リストのメンバーとして存在できます。 コールはビジー ボイスメール システムに転送できませんが、元のコールは維持されます。 即転送を呼び出した電話機に、コールが転送されなかったことを示す「ビジー（Busy）」メッセージが表示されます。 ボイスメール システムにQSIGまたはSIPトランク経由で到達した場合は、即転送を検出できますが、コールは維持されません。[クラスタ全体で即転送中のQSIGを許可する（Allow QSIG During iDivert clusterwide）]サービス パラメータが[True]に設定されている場合、または[クラスタ全体で従来の即転送を使用する（Use Legacy Immediate Divert clusterwide）]サービス パラメータが[False]に設定されている場合、即時転送はQSIGまたはSIPトランク経由で到達可能なボイスメール システムへのアクセスをサポートします。 [クラスタ全体で即転送中のQSIGを許可する（Allow QSIG During iDivert clusterwide）]サービス パラメータが[False]に設定されており、[クラスタ全体で従来の即転送を使用する（Use Legacy Immediate Divert clusterwide）]サービス パラメータが[True]に設定されている場合、即時転送はQSIGまたはSIPトランク経由のボイスメール システムへのアクセスをサポートしません。
迷惑呼の発信者 ID	システムは、悪意のある発信者 IDと即時転送機能の併用をサポートしません。
無応答時転送タイムアウト	[即転送（iDivert）] ソフトキーを押すと、無応答時転送タイムアウトに関連した競合状態が発生します。 たとえば、無応答時転送タイムアウト直後にマネージャが[即転送（iDivert）] ソフトキーを押すと、コール転送によりコールが事前に設定されている電話番号に転送されます。 しかし、マネージャが無応答時転送タイムアウトの前に[即転送（iDivert）] ソフトキーを押した場合は、即時転送によってコールがマネージャのボイスメッセージング メールボックスに転送されます。
発信元と着信側	発信側と着信側は、両方が同時に[即転送（iDivert）] ソフトキーを押した場合に、コールをボイス メールボックスに転送できます。

制約事項	説明
会議タイプ	会議の参加者の 1 人が [即転送（iDivert）] ソフトキーを押すと、残りのすべての参加者が [即転送（iDivert）] を押した参加者の発信グリーティングを受信します。 会議タイプには、ミートミー、アドホック、C 割り込み、参加が含まれます。
離脱または参加操作	コールに対する最後のアクションが自動ピックアップ、コール転送、コール パーク、コール パーク復帰、電話会議、ミートミー会議、あるいは離脱または参加操作を実行するアプリケーションだった場合、拡張即転送はボイス メールボックスを選択する画面を着信側に提示しません。 代わりに、拡張即転送は、着信側に関連付けられたボイス メールボックスにコールを即時転送します。

即時転送のトラブルシューティング

キーがアクティブでない

ユーザが [即転送（iDivert）] を押すと、電話に次のメッセージが表示されます。

キーがアクティブでない

[即転送（iDivert）] を押したユーザの音声メッセージング プロファイルに音声メッセージング パイロットがありません。

ユーザの音声メッセージング プロファイルに音声メッセージング パイロットを設定します。

一時エラー発生

ユーザが [即転送（iDivert）] を押すと、電話に次のメッセージが表示されます。

一時エラー発生

音声メッセージング システムが機能していないか、またはネットワークに問題があります。

音声メッセージング システムのトラブルシューティングを行います。 トラブルシューティングか、音声メッセージングのドキュメンテーションを参照してください。

ビジー

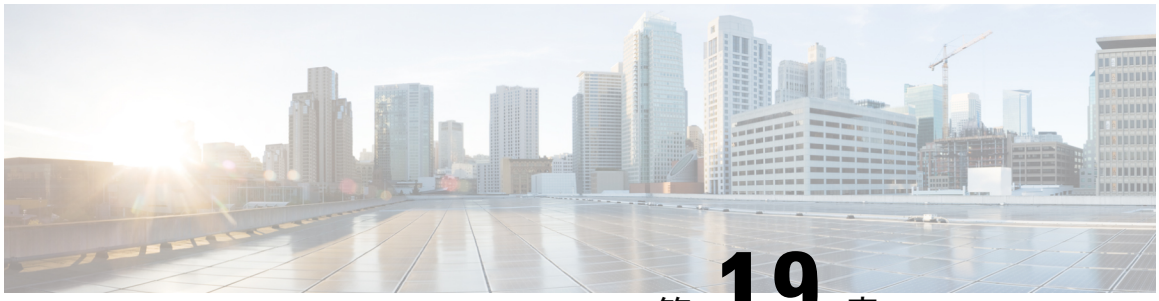
ユーザが [即転送（iDivert）] を押すと、電話に次のメッセージが表示されます。

ビジー

このメッセージは音声メッセージング システムが取り込み中であることを示しています。音声メッセージング ポートを追加設定するか、再実行してください。

第 VIII 部

会議機能



第 19 章

アドホック会議

アドホック会議の概要

アドホック会議では、会議の開催者（場合によっては別の参加者）が会議に参加者を追加できます。

アドホック会議には基本の会議と高度な会議の 2 種類があります。 基本のアドホック会議では、会議の開始者が会議の開催者の役割を果たし、他の参加者を追加または削除できる唯一の参加者となります。 高度なアドホック会議では、全参加者が他の参加者を追加または削除できます。 高度なアドホック会議では、複数のアドホック会議をリンクすることもできます。

高度なアドホック会議では、個人の参加者と同様にアドホック会議を他のアドホック会議に追加して、複数のアドホック会議をリンクできます。 [高度なアドホック会議を有効にする（Advanced Ad Hoc Conference Enabled）] サービス パラメータが [いいえ（False）] に設定されている場合に複数の会議をリンクしようとすると、IP 電話にメッセージが表示されます。 個人の参加者をアドホック会議に追加する場合に使用できる方法で、アドホック会議を他のアドホック会議に追加することもできます。

アドホック会議のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	会議用のソフトキー テンプレートの設定 （276 ページ）	ソフトキー テンプレートに、[会議リスト（Conference List）]、[参加（Join）]、および [会議の最後のパーティの削除

	コマンドまたはアクション	目的
		（Remove Last Conference Party）] の各ソフトキーを追加します。
ステップ 2	ソフトキー テンプレートと共通デバイスの関連付け （278 ページ）を行うには、次のサブタスクを完了します。 • 共通デバイス設定へのソフトキー テンプレートの追加 （279 ページ） • 電話機と共通デバイス設定の関連付け （280 ページ）	（オプション） 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	電話機とソフトキー テンプレートの関連付け （280 ページ）	（オプション）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	アドホック会議の設定 （280 ページ）	高度な会議を有効にし、参加者の最大数を指定して、会議の接続を切断する時期を指定します。
ステップ 5	複数ライン同時通話機能の設定 （284 ページ）	複数ライン同時通話機能を有効にして電話会議を作成します。

会議用のソフトキー テンプレートの設定

次の手順を使用して、以下の会議用ソフトキーを使用できるようにします。

ソフトキー	説明	コール状態
会議リスト（**ConfList**）	アドホック会議内にある参加者のディレクトリ番号のリストを表示します。 [Cisco Unified CM Administration （Cisco Unified Communications Manager Administration）]で設定されている場合は、参加者の名前が表示されます。	オンフック（On Hook） 接続されている状態
参加（Join）	最大 15 の確立されたコール（合計で 16）を参加させて会議を作成します。	保留（On Hold）
会議の最後の参加者の削除（**Remove**）	会議コントローラは、会議リストを呼び出し、[削除（Remove）]ソフトキーを使用して会議の参加者を削除することができます。	オンフック（On Hook） 接続されている状態

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）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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。

- ソフトキー テンプレートと共通デバイスの関連付け （278 ページ）
- 電話機とソフトキー テンプレートの関連付け （280 ページ）

ソフトキー テンプレートと共通デバイスの関連付け

（オプション） 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）]** に追加します。
- ソフトキー テンプレートを**共通デバイス設定**に追加します。

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、以下を行います。電話機とソフトキーテンプレートの関連付け （280 ページ）

始める前に

会議用のソフトキー テンプレートの設定 （276 ページ）

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ソフトキー テンプレートの追加 （279 ページ）	共通デバイス設定に会議のソフトキー テンプレートを追加するには、次の手順を実行します。
ステップ 2	電話機と共通デバイス設定の関連付け （280 ページ）	会議のソフトキーの共通デバイス設定を電話にリンクするには、次の手順を実行します。

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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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

（**オプション**） 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。

アドホック会議の設定

高度なアドホック会議の設定により、開催者以外の参加者が他の参加者を追加および削除したり、全参加者がアドホック会議をリンクしたりできます。

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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

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 [（クラスタ全体のパラメータ（機能 - 電話会議）（Clusterwide Parameters (Features - Conference)）] エリアの各フィールドを設定します。パラメータの説明については、アドホック会議のサービス パラメータ （281 ページ）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

複数ライン同時通話機能の設定 （284 ページ）

アドホック会議のサービス パラメータ

アドホック会議の主要なサービス パラメータを次の表に示します。 その他の会議サービス パラメータについては、[**サービスパラメータ設定（Service Parameter Configuration**）] ウィンドウの [**詳細設定（Advanced**）] オプションを参照してください。 会議サービス パラメータは [**クラスタ全体のパラメータ（機能 - 会議）（Clusterwide Parameters (Feature - Conference)**）] の下に表示されます。

表 *23:* アドホック会議のサービス パラメータ

サービス パラメータ	説明
[アドホック会議の削除（Drop Ad Hoc Conference）]	[アドホック会議の削除（Drop Ad Hoc Conference）] は、電話料金の詐欺行為を防止します。このような詐欺行為では、内部の会議開催者は会議から切断されますが、外部発信者は接続されたままになります。このサービス パラメータの設定値は、アドホック会議が削除される条件を指定します。 • [なし（Never）]：会議が削除されることはありません （意図しない会議の終了を防ぐため、デフォルト オプションを使用することが推奨されます）。 • [**会議にオンネット参加者がいなくなった時点（When No OnNet Parties Remain in the Conference**）]：アクティブな会議の最後のオンネット参加者がコールを切断するかまたは会議から退席すると、その会議が削除されます。Unified Communications Manager は、会議に割り当てられているすべてのリソースを解放します。 （注） 学習したルート パターンがオンネットに分類されるため、ILS 導入でのアドホック会議のドロップ機能が **[会議に OnNet パーティが誰も残っていないとき]** に設定した場合、関係者はドロップされません。 • [**会議の開催者が退席した時点（When Conference Controller Leaves**）]：主要開催者（会議作成者）がコールを切断すると、アクティブな会議が終了します。Unified Communications Manager は、会議に割り当てられているすべてのリソースを解放します。 （注） このサービス パラメータを [**なし（Never**）] に設定することが推奨されます。 その他の設定では、意図しない会議の終了が発生する可能性があります。 [アドホック会議の削除（Drop Ad Hoc Conference）] サービス パラメータの効果は、SIP を実行している Cisco Unified IP 電話7940 または 7960 から開始された会議コールと、SIP を実行しているサードパーティの電話から開始された会議コールでは異なります .
[アドホック会議の最大参加者数（Maximum Ad Hoc Conference）]	このパラメータは、1 つのアドホック会議に参加可能な最大参加者数を指定します。 デフォルト値：4

サービス パラメータ	説明
[高度なアドホック会議の有効化（Advanced Ad Hoc Conference Enabled）]	このパラメータは、高度なアドホック会議機能が有効であるかどうかを指定します。 これには、開催者以外の参加者が他の参加者を追加および削除できる機能や、全参加者がアドホック会議をリンクできる機能などが含まれます。
[非線形アドホック会議リンクの有効化（Non-linear Ad Hoc Conference Linking Enabled）]	このパラメータは、3 つ以上のアドホック会議を 1 つのアドホック会議に非線形で直接リンクできるかどうか（3 つ以上の会議を 1 つの会議にリンクできるかどうか）を決定します。
[ビデオ会議の代わりに暗号化音声会議を選択する（Choose Encrypted Audio Conference Instead Of Video Conference）]	このパラメータは、会議の開催者の [デバイス セキュリティ モード（Device Security Mode）] が [認証（Authenticated）] または [暗号化（Encrypted）] のいずれかに設定されており、2 人以上の会議参加者がビデオに対応している場合に、Unified Communications Manager が、アドホック会議コールに暗号化オーディオ会議ブリッジまたは非暗号化ビデオ会議ブリッジのいずれを選択するかを決定します。 このリリースでは暗号化ビデオ会議ブリッジがサポートされていないため、Unified Communications Manager は暗号化オーディオ会議ブリッジと非暗号化ビデオ会議ブリッジのいずれかを選択する必要があります。 デフォルト値は [**はい（True**）] です。
[ビデオ会議割り当てのための最小ビデオ対応参加者数（Minimum Video Capable Participants To Allocate Video Conference）]	このパラメータは、ビデオ会議ブリッジを割り当てるためにアドホック会議に存在している必要があるビデオ対応会議参加者の数を指定します。 ビデオ対応参加者の数がこのパラメータで指定されている数よりも少ない場合、Unified Communications Manager はオーディオ会議ブリッジを割り当てます。 ビデオ対応参加者の数がこのパラメータに指定されている数以上の場合、Unified Communications Manager は、ビデオ会議ブリッジが使用可能であれば、設定されているメディア リソース グループ リスト（MRGL）からビデオ会議ブリッジを割り当てます。 値 0 を指定すると、会議にビデオ対応参加者がいない場合を含め、常にビデオ会議ブリッジが割り当てられます。 オーディオ ブリッジを使用して確立された会議に追加のビデオ対応参加者が参加すると、この会議はオーディオ ブリッジのままで、ビデオに変換されることはありません。 デフォルト値は **2** です。

サービス パラメータ	説明
[ビデオ会議ブリッジの優先度が高い場合に音声のみの会議にビデオ会議ブリッジを割り当てる（Allocate Video Conference Bridge For Audio Only Conferences When The Video Conference Bridge Has Higher Priority）]	このパラメータは、メディア リソース グループ リスト（MRGL）でビデオ会議ブリッジの優先度がオーディオ会議ブリッジよりも高い場合に、Unified Communications Manager が音声のみのアドホック会議コールに対し、ビデオ会議ブリッジが使用可能であればビデオ会議ブリッジを選択するかどうかを指定します。 MRGL でオーディオ会議ブリッジの優先度がすべてのビデオ会議ブリッジよりも高い場合、Unified Communications Manager はこのパラメータを無視します。 このパラメータは、ローカル会議ブリッジがビデオブリッジであり（かつ MRGL で高い優先度が設定されており）、オーディオ会議ブリッジがリモート ロケーションでのみ使用可能な場合に便利です。このような状況でこのパラメータを有効にすると、Unified Communications Managerは音声のみの会議コールに対しても最初にローカル ビデオ会議ブリッジの使用を試行します。 デフォルト値は [**False**] です。
[サードパーティ アプリケーションでクリックツー会議機能を有効にする（Enable Click-to-Conference for Third-Party Applications）]	このパラメータは、SIP トランクでのクリックツー会議機能を Unified Communications Manager で有効にするかどうかを指定します。 クリックツー会議機能により、サードパーティのアプリケーションが SIP アウトオブダイアログ REFER メソッドを使用して会議をセットアップし、SIP SUBSCRIBE/NOTIFY により会議イベント パッケージのために SIP トランクに登録できるようになります。 **警告** このパラメータを有効にすると、この機能をサポートするようにコーディングされている CTI アプリケーションに悪影響を及ぼす可能性があります。 デフォルト値：False
[クラスタ会議プレフィックス ID（Cluster Conferencing Prefix Identifier）]	このパラメータは、SIP 会議ブリッジ（Cisco TelePresence MCU や Cisco TelePresence Conductor など）でホストされるアドホック会議とミートミー会議に対して生成される会議 ID にプレフィックスとして追加される最大 8 桁の番号（例：0001）を定義します。 このフィールドには、Unified Communications Manager が管理する SIP 会議ブリッジが、ネットワーク内の複数クラスタによって共有される場合に、管理者が値を指定する必要があります。 アドホック会議とミートミー会議の会議 ID が一意であるようにするため、すべてのクラスタに固有のプレフィックスを設定する必要があります。 会議リソースがクラスタ間で共有されない場合、このフィールドに値を指定されないことがあります。

複数ライン同時通話機能の設定

複数ライン同時通話機能では、ユーザが（異なる電話番号、または同じ電話番号で異なるパーティションの）複数の電話回線のコールに参加して会議を作成できます。

始める前に

- 電話機が複数ライン同時通話機能をサポートするモデルかどうかを確認します。電話機能一覧の生成 （5 ページ）
- アドホック会議の設定 （280 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）]** > **[デバイス設定（Device Settings）]** > **[デバイス プロファイル（Device Profile）]**。[デフォルト デバイス プロファイルの設定（Default Device Profile Configuration）]ウィンドウが表示されます。

ステップ 2 [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、電話機のモデルを選択します。

ステップ 3 [デバイス プロトコル（Device Protocol）] ドロップダウン リストから、関連する SCCP または SIP プロトコルを選択します。

ステップ 4 [複数ライン同時通話機能（Join Across Lines）]を [オン（On）]に設定します。

ステップ 5 **[保存（Save）]** をクリックします。

会議の連携動作

機能	データのやり取り
[C 割込（cBarge）] を使用した会議	会議を開始するには、**[C 割込（cBarge）]** ソフトキーを押すか、またはシングル ボタン C 割り込み機能が有効な場合にはアクティブ コールの共有回線ボタンを押します。C割り込みが開始されると、共有会議ブリッジが使用可能な場合には、このブリッジを使用して割り込みコールが設定されます。 元のコールが分割され、会議ブリッジに参加します。 参加者全員の通話情報が [会議（Conference）] に変わります。 割り込み先コールが会議コールになり、割り込み対象デバイスが会議の開催者になります。 会議の開催者は、会議にさらに参加者を追加するか、または参加者を削除できます。 いずれかの参加者がコールを解放すると、会議には2人の参加者が残されます。この残り2名の参加者に対し短い中断が発生し、これらの参加者はポイントツーポイント コールとして再接続されます。これにより、共有会議リソースが解放されます。

機能	データのやり取り
コールパーク、コール転送、およびリダイレクトの連携動作	会議の開催者が会議の転送、パーク、または他の参加者へのリダイレクトを行うと、コールを取得する参加者が、会議の実質的な開催者となります。 実質的な開催者は、会議への参加者の追加や、会議に追加されている参加者の削除はできませんが、会議の転送、パーク、または他の参加者へのリダイレクトを行うことができます。会議が他の参加者にリダイレクトされると、そのリダイレクト先の参加者が、会議の実質的な開催者となります。 この実質的な開催者がコールを終了すると、会議が終了します。
SIP 電話のソフトキー表示	[参加者（ConfList）] および [削除（Remove）] ソフトキー機能は、SCCP 電話でのみ使用できます。 SIP 電話では [詳細を表示（Show Details）] ボタンに類似の機能が設定されています。

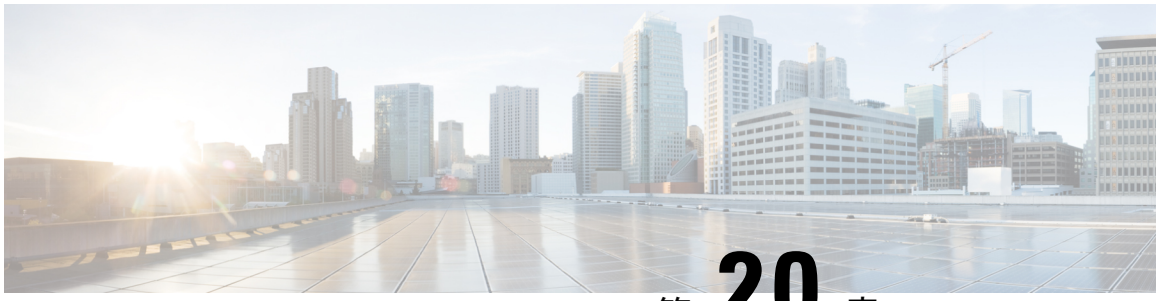
会議の制約事項

アドホック会議には次の制約事項が適用されます。

機能	制約事項
アドホック会議	Unified Communications Manager各 Unified Communications Manager サーバに対して最大 100 の同時 Ad Hoc 会議がサポートされています。 Cisco Unified Communications Manager では、アドホック会議あたり最大 64 人の参加者がサポートされています（十分な会議リソースが使用可能である場合）。 リンクされたアドホック会議の場合、システムでは各会議が 1 人の参加者として扱われます。
SIP 電話でのアドホック会議： • Cisco Unified IP 電話 7911 • Cisco Unified IP 電話 7941 • Cisco Unified IP 電話 7961	Unified Communications Manager は、新しい参加者が追加されると「「ビープ」」音を鳴らし、新しい参加者がアドホック会議から退席すると「「ビープ ビープ」」音を鳴らします。 参加者がアドホック会議に追加されるときに、SIP を実行している電話のユーザにはビープ音が聞こえないことがあります。参加者がアドホック会議から退席するときに、SIP を実行している電話のユーザには「「ビープ ビープ」」音が聞こえないことがあります。 ユーザにビープ音が聞こえない原因は、Unified Communications Manager が会議プロセス中に接続のセットアップと切断にかかる時間にあります。 SIP を実行する電話のアドホック会議リンクを起動するには、会議機能と転送機能を使用する必要があります。 直接転送と参加はサポートされていません。 SIP を実行するサポートされる電話は、Cisco Unified IP 電話 7911、7941、7961 です。

機能	制約事項
SIP 電話でのアドホック会議： • Cisco Unified IP 電話 7940 • Cisco Unified IP 電話 7960 • サードパーティの電話	• 電話には、個々のコールが会議コールとして表示されます。Cisco Unified IP Phones 7940 と 7960 では、ローカル会議コールを作成できますが、アドホック会議コールは作成できません。 • 会議リスト（ConfList）は使用できません。 • 会議への最後の参加者の削除（RmLstC）機能は使用できません。 • アドホック会議の削除機能はサポートされていません。 • SIP プロファイルの [会議参加が有効（Conference Join Enabled）] パラメータは、会議開催者がローカルでホストされている会議を退席するときの、SIP を実行する電話の動作を制御します。 [会議参加が有効（Conference Join Enabled）] チェックボックスがオフの場合、会議開催者がアドホック会議コールを終了すると、すべてのレッグが切断されます。[会議参加が有効（Conference Join Enabled）] チェックボックスがオンの場合、残り 2 人の参加者が接続されたままの状態になります。 • [アドホック会議の削除（Drop Ad Hoc Conference）] パラメータの設定によって、SCCP を実行する電話から開始される会議コールに対して適用されるのと同じ制御レベルを実現するため、管理者は、SIP を実行する電話（Cisco Unified IP 電話 7940 または 60）から開始される会議に対し、[会議参加が有効（Conference Join Enabled）] SIP プロファイル パラメータと [オフネット間転送のブロック（Block OffNet to OffNet Transfer）] サービス パラメータを組み合わせて使用できます（SIP を実行する電話は、会議コールからドロップアウトすると転送を実行するため、[オフネット間転送のブロック（Block OffNet to OffNet Transfer）] を使用して 2 つのオフネット電話がコールに残ることができないようにすることで、電話料金の詐欺行為を防止できます）。 • Unified Communications Manager は、新しい参加者が追加されると「「ビープ」」音を鳴らし、新しい参加者がアドホック会議から退席すると「「ビープ ビープ」」音を鳴らします。 参加者がアドホック会議に追加されるときに、SIP を実行している電話のユーザにはビープ音が聞こえないことがあります。参加者がアドホック会議から退席するときに、SIP を実行している電話のユーザには「「ビープ ビープ」」音が聞こえないことがあります。 ユーザにビープ音が聞こえない原因は、Unified Communications Manager が会議プロセス中に接続のセットアップと切断にかかる時間にあります。

機能	制約事項
2 人の参加者が接続している場合でも電話に [会議（To Conference）] が表示される	パブリッシャ（CmA11）とサブスクライバ（CmA2）を使用して Call Manager クラスタを設定します。 電話 A、B、C は CmA1 に登録されています。 電話 D は CmA2 に登録されています。 • A（1000）、B（4000）、C（5000）、D（6000）間で、A を開催者として、コンサルタティブまたはブラインド アドホック会議を設定します。 • Cma2 をシャットダウンします。 • 電話 D は通話保護モードになります。[終了（End Call）] ソフトキーを押します。 • 電話 A、B、C が会議に参加しています。 • 電話 A、B、C が会議に参加しています。 • 電話 A を切断します。これで電話 B と C がダイレクト コールになります。 問題：電話 B と C はまだ会議に参加しています。 • 電話 A を切断します。これで電話 B と C がダイレクト コールになります。 問題：電話 B と C はまだ会議に参加しています。 • 電話 B を切断します。電話 C にはコールはありません。電話 B と C はまだ会議に参加しています。 問題：電話 C はまだ会議に参加しています。



第 20 章

ミートミー会議

ミートミー会議の概要

ユーザはミートミー会議を使用して、電話会議を設定するか、電話会議に参加できます。 電話会議を設定するユーザは、会議コントローラと呼ばれます。 電話会議に参加するユーザは、参加者と呼ばれます。

ミートミー会議のタスク フロー

始める前に

- ルータに付属されていた構成ドキュメンテーションを参照し、ミートミー会議のタスク フローに進む前に、必要な設定を確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	ミートミー会議のソフトキーテンプレートの設定 （290 ページ）	ソフトキーテンプレートに[ミートミー（Meet-Me）]ソフトキーを追加します。
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 （291 ページ）を行うには、次のサブタスクを完了します。 • 共通デバイス設定へのソフトキー テンプレートの追加 （292 ページ）	（オプション） 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。

	コマンドまたはアクション	目的
	• 電話機と共通デバイス設定の関連付け （292 ページ）	
ステップ 3	共通デバイス設定電話機とソフトキーテンプレートの関連付け （293 ページ）	（**オプション**）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	ミートミー会議番号の設定 （293 ページ）	高度な会議を有効にし、参加者の最大数を指定して、会議の接続を切断する時期を指定します。

ミートミー会議のソフトキー テンプレートの設定

オフフック発信状態でミートミー ソフトキーを使用可能にするには、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。**[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）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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。

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

（オプション） 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）]** に追加します。
- ソフトキー テンプレートを**共通デバイス設定**に追加します。

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 （293 ページ）」を参照してください。

始める前に

ミートミー会議のソフトキー テンプレートの設定 （290 ページ）

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ソフトキー テンプレートの追加 （292 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（292 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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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

始める前に

共通デバイス設定へのソフトキー テンプレートの追加 （292 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。

電話機とソフトキー テンプレートの関連付け

（オプション） 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。

始める前に

ミートミー会議のソフトキー テンプレートの設定 （290 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、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。

ミートミー会議番号の設定

Cisco Unified Communications Manager の管理者は、ミートミー会議の電話番号の範囲をユーザに提供します。これにより、ユーザがその機能にアクセスできるようになります。 ユーザは、ミートミー番号またはパターンに指定された範囲から電話番号を選択して、ミートミー会議を確立し、会議コントローラになります。

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。**[コールルーティング（Call Routing）]** > **[ミートミー番号/パターン（Meet-Me Number/Pattern）]** を選択します。
[ミートミー番号の検索/一覧表示（Find and List Meet-Me Numbers）] 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。
一致するすべてのレコードが表示されます。

ステップ 3 レコードのリストで、表示するレコードへのリンクをクリックします。

ステップ 4 次のいずれかのタスクを実行します。

- ミートミー番号またはパターンをコピーするには、コピーするミートミー番号またはパターンをクリックします。 **[ミートミー番号/パターンの設定（Meet-Me Number/Pattern Configuration）]** ウィンドウが表示されます。 [Copy]をクリックします。
- ミートミー番号/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。
- 既存のミートミー番号/パターンを更新するには、更新するミートミー番号またはパターンをクリックします。

ステップ 5 適切な設定値を入力します。

フィールドとその設定オプションの詳細については、「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。

ミートミー番号とパターンの設定値

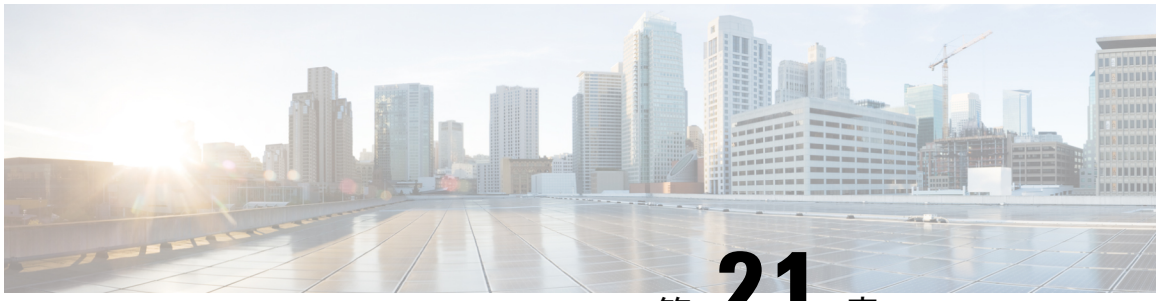
フィールド	説明
[電話番号またはパターン(Directory Number or Pattern)]	ミートミー番号または番号の範囲を入力します。 範囲を設定するには、角カッコ内にダッシュとそれに続く数値を入力する必要があります。たとえば、範囲 1000 ～ 1050 を設定するには、10[0-5]0 と入力します。
説明	説明には、任意の言語で 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、山カッコ（<>）は使用できません。

フィールド	説明
パーティション	パーティションを使用してミートミー番号またはパターンへのアクセスを制限する場合は、ドロップダウン リスト ボックスから適切なパーティションを選択します。 ミートミー番号またはパターンへのアクセスを制限しない場合は、パーティションに [<None>] を選択します。 Max List Box Items エンタープライズ パラメータを使用すると、このドロップダウン リスト ボックスに表示されるパーティションの数を設定できます。 Max List Box Items エンタープライズ パラメータの指定よりも多くのパーティションが存在する場合は、このドロップダウン リスト ボックスの横に **[検索(Find)]** ボタンが表示されます。 **[検索(Find)]** ボタンをクリックすると、[パーティションの検索/一覧表示(Find and List Partitions)]ウィンドウが表示されます。 （注） リスト ボックス項目の最大数を設定するには、**[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、[CCMAdmin Parameters] の下の [Max List Box Items] フィールドを更新します。 （注） ミートミー番号またはパターンとパーティションの組み合わせが、Unified Communications Manager クラスタ内で一意であることを確認します。
[最小セキュリティレベル(Minimum Security Level)]	このミートミー会議番号またはパターンの最小ミートミー会議セキュリティ レベルを、ドロップダウン リスト ボックスから選択します。 • **[認証のみ(Authenticated)]**：非セキュアな電話機を使用した参加者が会議に参加することをブロックします。 • **[暗号化(Encrypted)]**：認証済みまたは非セキュアな電話機を使用した参加者が会議に参加することをブロックします。 • **[非セキュア(Non Secure)]**：すべての参加者が会議に参加できます。 （注） この機能を使用するには、セキュアな会議ブリッジが設定済みで使用可能になっている必要があります。

ミートミー会議の制限

Unified Communications Manager は、Unified Communications Manager サーバごとに最大 100 の同時ミートミー会議をサポートします。

その電話会議に指定された参加者の最大数を超過すると、他の発信者は電話会議に参加できません。



第 21 章

開催中の会議

[今すぐ会議(Conference Now)]の概要

「開催中の会議」機能は小規模企業のお客様向けの基本的な音声会議ソリューションであり、内部と外部の発信者が集中型 IVR 経由で会議に参加できます。

会議を主催するには、設定済みのユーザが、会議の開始時に入力する必要のある会議PINと会議番号を設定する必要があります。 主催者は他の会議参加者に対し、関連する会議情報（時間枠、会議番号（通常はホストの内線番号）、セキュアな会議のためのオプションのアクセスコードなど）を通知します。 指定された時間になると、他の参加者は IVR にダイヤルし、プロンプトに会議情報を入力することで、コールに参加できます。

管理者は、[開催中の会議」機能で会議を主催できるようエンドユーザを設定する必要があります。 この機能を設定した後は、会議主催者がセルフケア ポータルで会議アクセス コードを編集できます。

（注） 「開催中の会議」には IPVMS ソフトウェアベースの会議ブリッジを使用することをお勧めします。 他の会議ブリッジを使用する場合、会議の参加/退出トーンが参加者に再生されないことがあります。

開催中の会議の前提条件

「開催中の会議」を使用するには、以下のメディア リソースが設定されていること、会議を開始するデバイスからそれらを使用できることを確認する必要があります。

- [会議ブリッジ（Conference Bridge）]：ユーザ エクスペリエンスを快適にするため、ソフトウェアベースの Cisco IPVMS 会議 ブリッジを使用することを推奨します。 他の会議ブリッジを使用すると、会議参加者の参加退出トーンが再生されない可能性があります。
- 音声自動応答（IVR）（Interactive Voice Response (IVR)）

リソースを設定した後、これらのリソースをデバイスで使用可能にすることができます。そうするには、これらのリソースを含むメディア リソース グループ リストを設定し、そのメディア リソース グループ リストを、デバイスが使用するデバイス プールまたは個々のデバイスに関連付けます。 Conference Bridges、Interactive Voice Response および Media Resource Groups の設定に関する詳細は、『Cisco Unified Communications Manager システム設定ガイド』の「メディア リソースの設定」項を参照してください。

Cisco IP Voice Media Streaming のアクティブ化

IVR サービスと開催中の会議を使用するには、Cisco IP Voice Media Streaming サービスが実行されている必要があります。

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[ツール（Tools）]** > **[サービス アクティベーション（Service Activation）]** を選択します。

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

ステップ 3 [Cisco IP Voice Media Streaming Application]が無効になっている場合は、対応するチェックボックスをオンにして、[保存（Save）]をクリックします。

開催中の会議の設定の構成

Unified Communications Manager で Conference Now システムを設定するには、次の手順を使用します。

手順

ステップ 1 [Cisco Unified CM 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）]** > **[会議中（Conference Now）]**。

ステップ 2 外部の発信者がアクセスできるように、**[開催中の会議の IVR ディレクトリ番号（Conference Now IVR Directory Number）]** フィールドで、Unified Communications Manager クラスタの [DID（ダイヤルイン方式）（DID (Direct Inward Dial)）] 番号を入力します。

ステップ 3 [ルート パーティション（Route Partition）] ドロップダウン リストからパーティションを選択します。

（注） 番号とパーティションの組み合わせは、クラスタ内で一意である必要があります。

ステップ 4 [開催中の会議の設定（Conference NowConfiguration）]ウィンドウのその他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、オンライン ヘルプを参照してください。

ステップ 5 **[保存]** をクリックします。

次のタスク

エンド ユーザに対してこの機能を次のように有効にします。

- LDAP ディレクトリをまだ同期していない場合は、LDAP 同期に「開催中の会議」を追加してください。これにより、新たに同期されたユーザは「開催中の会議」を主催できます。 LDAP 経由での開催中の会議の有効化 （300 ページ）を参照してください。
- 既存のエンドユーザに対してこの機能を有効にするには、ユーザに対する開催中の会議の有効化 （299 ページ）を参照してください。

ユーザに対する開催中の会議の有効化

既存のエンドユーザが「開催中の会議」を主催できるように設定するには、次の手順に従います。

（注） [一括管理（Bulk Administration）] の [ユーザの更新（Update Users）] を使用すると、多数のユーザに対して CSV ファイルを使用して開催中の会議を有効にできます。 次のタスクに示されているのと同じ内容を確実に設定する必要があります。 Update Users の使用方法に関しては、『Cisco Unified Communications Manager 一括管理ガイド』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）]** > **[エンド ユーザ（End User）]**。

ステップ 2 [検索（Find）] をクリックして、開催中の会議を追加するユーザを選択します。

ステップ 3 [開催中の会議（Conference Now）] の [エンドユーザによる会議のホストを有効化（Enable End User to Host Conference Now）] チェックボックスをオンにします。

ステップ 4 （任意） セキュア会議の場合は、**参加者アクセス コード**を入力します。 エンドユーザはセルフケア ポータルで各自のアクセス コード設定を変更できることに注意してください。

（注） ユーザに**セルフサービス ユーザ ID** が割り当てられている場合は、開催中の会議の**会議番号**に**セルフ サービス ユーザ ID** の値が事前に取り込まれます。デフォルトではこの値はユーザのプライマリ内線です。

ステップ 5 [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。

LDAP 経由での開催中の会議の有効化

LDAPディレクトリをまだ同期していない場合は、同期対象ユーザで「開催中の会議」を有効にすることができます。有効にするには、機能グループテンプレートにオプションを追加し、その機能グループテンプレートを初回LDAP同期に追加します。LDAP同期によりプロビジョニングされる新しいユーザの場合は、開催中の会議が有効になります。

（注） 初回同期がすでに発生した場合、LDAPディレクトリ同期に機能グループテンプレートの編集内容を適用することはできません。 編集内容を LDAP 同期に適用するには、初回同期がまだ発生していない必要があります。

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。**[ユーザ管理（User Management）]** > **[ユーザ電話/追加（User Phone/Add）]** > **[機能グループテンプレート（Feature Group Template）]**。

ステップ 2 次のいずれかを実行します。

- [検索（Find）] を選択し、既存のテンプレートを選択します。
- [新規追加（Add New）] をクリックして新しいテンプレートを作成します。

ステップ 3 ドロップダウン リストから **[サービス プロファイル（Service Profile）]** を選択します。

ステップ 4 ドロップダウン リストから **[ユーザ プロファイル（User Profile）]** を選択します。

ステップ 5 [エンド ユーザによる会議のホストを有効化（Enable End User to Host Conference Now）]チェックボックスをオンにします。

ステップ 6 **[保存]** をクリックします。

次のタスク

LDAP ディレクトリ同期にテンプレートを割り当てます。これにより、同期ユーザで「開催中の会議」を設定できます。 LDAP 同期の設定に関しては、『Cisco Unified Communications Manager システム設定ガイド』の「エンド ユーザ設定」項を参照してください。

あるいは、[ユーザ/電話のクイック追加（Quick User/Phone Add）] メニューを使用して新しいユーザを「開催中の会議」機能に追加することもできます。プライマリ内線番号の割り当てに加えて、この機能グループテンプレートを使用する新しいユーザを追加する必要があります。

開催中の会議の連携動作

機能	連携動作
モビリティ EFA（エンタープライズ機能アクセス）	モビリティ ユーザが、リモート接続先からエンタープライズ機能アクセス DID 番号にダイヤルします。 コールが接続されると、リモート接続先の電話を使用して DTMF 番号が PSTN ゲートウェイ経由で Unified Communications Manager に送信されます。 Unified Communications Manager では最初に、# キーの前に入力されるユーザ PIN が認証されます。 ユーザ PIN の認証が正常に完了したら、1 と # キーを押して 2 段階ダイヤル コールであることを示し、その後電話番号を入力します。 ダイヤルした電話番号が開催中の会議の IVR 電話番号であり、ユーザが会議ホストである場合、ユーザは PIN をもう一度入力する必要があります。

機能	連携動作
モビリティ MVA（モバイル音声アクセス）	コールはエンタープライズ PSTN H.323 または SIP ゲートウェイ経由で Unified Communications Manager に転送されます。 IVR がユーザに対し、ユーザ ID、# キー、PIN、# キー、番号 1（モバイル音声アクセス コールにするため）、該当する電話番号をこの順序で入力するよう指示します。電話番号が開催中の会議の IVR 電話番号であり、ユーザが会議ホストである場合、ユーザは PIN をもう一度入力する必要があります。 （注） ユーザがリモート接続先から直接ダイヤルする場合、ユーザに対して PIN の入力は指示されません。ただし、ユーザが異なる電話からモバイル音声アクセス電話番号にダイヤルすると、コール発信前に PIN を入力するよう指示されます。ユーザが開催中の会議の IVR 電話番号をコールすると、PIN をもう一度入力するよう指示されます。

開催中の会議の制約事項

「開催中の会議」機能には次の制約事項があります。

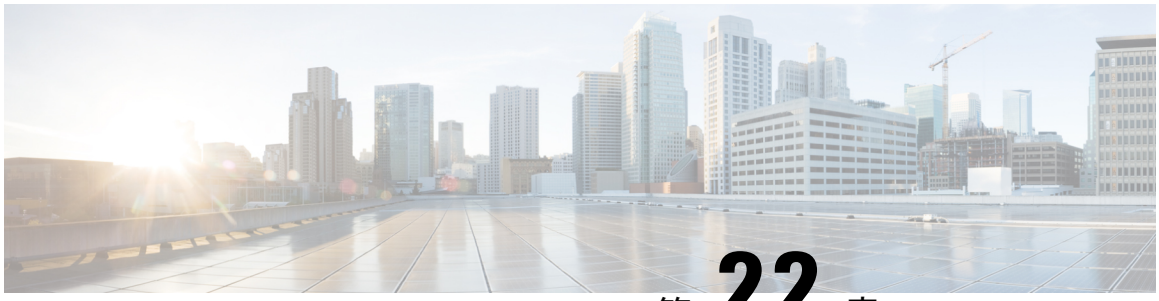
- ホストは参加者をミュートできません。
- 参加者は DTMF 番号を入力して音声をミュートにすることはできません。
- 開催中の会議の参加者のリストはサポートされていません。
- 1 つの会議の最大参加者数は、既存の CallManager サービス パラメータ [最大ミートミー会議ユニキャスト（Maximum MeetMe Conference Unicast）] により制御されます。 これは内部と外部の両方の発信者に適用されます。
- 同時に実行できる開催中の会議とミートミー会議インスタンスの合計最大数は、Unified Communications Manager CallManager ノードあたり 100 です。
- 保留ビデオはサポートされません。
- IPVMS ソフトウェア会議ブリッジでは、コーデック G.711（ALaw および ULaw）とワイドバンド 256k だけがサポートされています。 発信側デバイスとソフトウェア会議ブリッジ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。
- 会議参加者の参加音と退出音を再生するには、次のうち 1 つ以上の条件を満たしている必要があります。
  - 少なくとも 1 人の会議参加者が Cisco IP 電話 を使用している。
  - 割り当てられているソフトウェア会議ブリッジが IPVMS である。

- 会議ブリッジが設定されている場合、ホストが在席しているかどうかに関係なく、残りの参加者で会議が続行されます。 ホストが参加者アクセス コードを設定している場合、ホストが会議に再度参加しようとすると、参加者アクセス コードの入力を求めるアナウンスが再生されます。 ホストは参加者のスケジュールを設定することや、参加者をミュートにすることはできません。したがってホスト ステータスは無効になります。
- ホストが会議に参加する最初のユーザである場合は、音声アナウンスは再生されません。ただし、ホストが内部の IP フォンから開催中の会議にダイヤルすると、IP フォンに「会議（To Conference）」を示すビジュアルが表示されます。

（注） ホストが外部の電話から開催中の会議に参加する場合、電話にはビジュアルは表示されません。

第 IX 部

発信



第 22 章

コールバック

コールバックの概要

コールバック機能により、話中の内線番号がコールを受信できるようになった時点で通知を受信できます。

電話と同じ Unified Communications Manager クラスタ内にある接続先の電話、または QSIG トランクまたは QSIG 対応クラスタ間トランクを介したリモート Private Integrated Network Exchange（PINX）にある接続先の電話のコールバックをアクティブにできます。

コールバック通知を受信するには、話中音またはリングバック トーンが再生されている間に [コールバック（CallBak）] ソフトキーまたは機能ボタンを押します。 リオーダー音の再生中にコールバックをアクティブにできます。リオーダー音は、「応答なし」タイマーが期限切れになると再生されます。

一時停止/再開

コールバック機能により、コールバックを発信したユーザが話中の場合にコール完了サービスを一時停止できます。 発信元ユーザが利用可能になると、そのユーザに対してコール完了サービスが再開されます。

（注） コールバックでは、クラスタ間トランクと、クラスタ間 QSIG トランクまたは QSIG 対応クラスタ間トランクの両方で、コールバック一時停止/コールバック再開の通知がサポートされています。

コールバックの前提条件

コールバック機能を使用するには、接続先の電話が次のいずれかの場所に配置されている必要があります。

- ユーザの電話機と同じ Unified Communications Manager クラスタ内
- リモート PINX over QSIG トランク上
- リモート PINX over QSIG 対応クラスタ間トランク上

英語以外の電話ロケールまたは国別のトーンを使用する場合は、ロケールをインストールする必要があります。

- コールバック機能をサポートするデバイスは次のとおりです。
  - Cisco Unified IP Phone 6900、7900、8900、および 9900 シリーズ（6901 と 6911 を除く）
  - Cisco IP 電話 7800 および 8800 シリーズ
  - Cisco VGC Phone（Cisco VG248 ゲートウェイを使用）
  - Cisco アナログ電話アダプタ（ATA）186 および 188
  - Cisco VG224 エンドポイントの Busy Subscriber
  - Cisco VG224 エンドポイントの No Answer
- サポートされている電話にコールを転送する CTI ルート ポイント

コールバックの設定タスク フロー

電話でソフトキーとボタンのどちらがサポートされているかに応じて、いずれかのタスク フローを完了します。

次の表を使用して、コールバック対応 IP フォンで [コールバック（CallBack）] ソフトキーまたはボタンのどちらを設定するかを判別します。

表 *24 :* コールバック ソフトキーとボタンを使用する *Cisco IP* 電話

Cisco 電話モデル	コールバック ソフトキー	コールバック ボタン
Cisco Unified IP Phone 6900 シリーズ（6901 と 6911 を除く）	X	X
Cisco Unified IP Phone 7900 シリーズ	X	

Cisco 電話モデル	コールバック ソフトキー	コールバック ボタン
Cisco IP 電話 7800 および 8800 シリーズ	X	X
Cisco Unified IP Phone 8900 シリーズ	X	X
Cisco Unified IP Phone 9900 シリーズ	X	X
Cisco IP Communicator	X	

始める前に

- コールバックの前提条件 （308 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	コールバック用のソフトキーテンプレートの設定 （309 ページ）	[コールバック （CallBack）] ソフトキーをテンプレートに追加し、共通デバイス設定または電話機を使用してソフトキーを設定するには、この手順を実行します。
ステップ 2	[コールバック （CallBack）] ボタンの設定 （313 ページ）	電話機に [コールバック （CallBack）] ボタンを追加して設定するには、この手順を実行します。

コールバック用のソフトキー テンプレートの設定

CallBack ソフトキーには次のコール状態があります。

- オンフック （On Hook）
- 発信 （Ring Out）
- 接続転送 （Connected Transfer）

以下の手順を使用して、CallBack ソフトキーを使用できるようにします。

始める前に

電話機がコールバック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 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）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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。

- 共通デバイス設定とコールバック ソフトキー テンプレートの関連付け （311 ページ）
- 電話機とコールバック ソフトキー テンプレートの関連付け （312 ページ）

共通デバイス設定とコールバック ソフトキー テンプレートの関連付け

（**オプション**） 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）]** に追加します。
- ソフトキー テンプレートを**共通デバイス設定**に追加します。

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、「電話機とコールバック ソフトキーテンプレートの関連付け （312 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コールバック ソフトキーテンプレートの追加 （311 ページ）	共通デバイス設定にコールバック 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。
ステップ 2	電話機と共通デバイス設定の関連付け （312 ページ）	コールバック ソフトキーの共通デバイス設定を電話にリンクするには、次の手順を実行します。

共通デバイス設定へのコールバック 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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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。

電話機とコールバック ソフトキー テンプレートの関連付け

オプション：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、つまり共通デバイス設定との連携のために、次の手順を使用します。 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。

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。

[コールバック（CallBack）] ボタンの設定

この項の手順では、[コールバック（CallBack）] ボタンを設定する方法を説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	コールバックの電話ボタン テンプレートの設定 （313 ページ）	[コールバック（CallBack）] ボタン機能を回線または短縮ダイヤル キーに割り当てるには、次の手順を実行します。
ステップ 2	電話機とボタン テンプレートの関連付け （314 ページ）	電話の [コールバック（CallBack）] ボタンを設定するには、次の手順を実行します。

コールバックの電話ボタン テンプレートの設定

回線または短縮ダイヤル キーに機能を割り当てるには、次の手順に従います。

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。**[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）]** の順に選択します。

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]** 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]** をクリックします。

ステップ 7 次のいずれかの作業を実行します。

- 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

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]** 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。

コールバックの連携動作

機能	データのやり取り
通話転送	コールバック通知画面から発信したコールは、着信側 DN で設定されている通話転送の設定値をすべて上書きします。 コールバック リコール タイマーが期限切れになる前にコールを発信する必要があります。このようにしないと、コールは通話転送の設定値を上書きしません。

機能	データのやり取り
SIP を実行する電話でのコールバック通知	CallBack 通知は、7960 と 7940 の Cisco Unified IP Phones でのみ動作します。他のすべての SIP フォンとすべての SCCP 電話機は、オンフックおよびオフフック通知をサポートします。 Unified Communications Manager が、SIP 7960 または 7940 電話で回線が使用可能になったことを認識する唯一の方法は、Unified Communications Manager が電話から受信する SIP INVITE メッセージをモニタすることです。 電話から Unified Communications Manager に SIP INVITE が送信され、電話がオンフックになると、Unified Communications Manager は音声およびコールバック通知画面を Cisco Unified IP Phone 7960 および 7940（SIP）ユーザに送信します。
サイレント（DND）	コールバックは、発信側または着信側で [**DND 拒否（DND-Reject）**] が [**オフ（Off）**] に設定されている場合は通常どおりに機能します。 [**DND 拒否（DND-Reject）**] が [**オン（On）**] に設定されている場合にのみ、動作が異なります。 • **発信側で [DND 拒否（DND-Reject）] がオンである**：ユーザ A がユーザ B に対してコールを発信し、コールバックを起動します。 ユーザ A は DND-R に進みます。 ユーザ B が利用可能になった後でも、ユーザ A のコールバック通知が引き続き表示されます。つまり DND ステータスに関係なく、他の参加者が利用可能であるかどうかがユーザに通知されます。 • **着信側で [DND 拒否（DND-Reject）] がオンである**：ユーザ A がユーザ B にコールを発信し、ユーザ B は [**DND 拒否（DND-Reject）**] を [**オン（On）**] に設定しています。 ユーザ A にはファスト ビジー音が聞こえます。 ユーザ A はビジーエンドポイントでコールバックを開始できます。 ユーザ B が [DND 拒否（DND-Reject）] であり、オフフックになってからオンフックになると、ユーザ A は「ユーザ B と通話できますがユーザ B は DND-R です（User B is available now but on DND-R）」という通知を受け取ります。 ユーザ A がキャンセルしない場合、ユーザ B が [**DND 拒否（DND-Reject）**] を [**オフ（Off）**] に設定するまで、コールバックにより引き続きユーザ B がモニタされます。

機能	データのやり取り
Cisco Extension Mobility	Cisco エクステンションモビリティ ユーザがログインまたはログアウトすると、コールバックに関連付けられているアクティブ コールの完了はすべて自動的にキャンセルされます。 コールバックが着信側の電話からアクティブにされた後で、システムからこの着信側の電話が削除される場合、発信者が [ダイヤル（Dial）] ソフトキーを押すと、リオーダー音が聞こえます。ユーザはコールバックをキャンセルまたは再度アクティブにできます。

コールバックの制約事項

機能	制約事項
CUBE 間のビデオを使用したコールバック	Qsig 対応 SIP トランクを使用して CUBE 経由で接続されている2つのユニファイド CM クラスタ間でコールが発信されると、コールバック機能はビデオコールに対して機能しません。 詳細については、CSCun46243 を参照してください。
SIP トランク	コールバックは SIP トランクではサポートされていませんが、QSIG 対応 SIP トランクではサポートされています。
発信側または着信側の名前と番号でサポートされている文字	コールバックでは、発信側と着信側の名前と番号に、スペースと 0 から 9 までの数字がサポートされています。 コールバックを使用する場合、発信側と着信側の名前と番号にはシャープ記号（#）やアスタリスク（*）は使用できません。
ボイスメール	すべてのコールをボイス メッセージング システムに転送する場合、コールバックをアクティブにすることはできません。

コールバックのトラブルシューティング

このセクションでは、さまざまなシナリオでの問題、考えられる原因、および解決策と、コールバックについて IP Phone に表示されるエラー メッセージについて説明します。

[コールバック（CallBack）] ソフトキーを押してからコールバックが発生するまでの間の電話のプラグの取り外し/リセット

問題

[コールバック（CallBack）] ソフトキーを押してから、コールバックがアクティブになる前に電話のプラグを抜くかリセットしました。

考えられる原因

Unified Communications Manager コールバック アクティベーションをキャンセルします。

ソリューション

発信者の電話を登録すると、リセット後、発信者の電話には[コールバックのアクティベーション（Call Back activation）] ウィンドウは表示されません。 アクティブなコールバック サービスを表示するには、[コールバック（CallBack）] ソフトキーを押す必要があります。 電話にコールバック通知が発生します。

発信者が対応可能通知に気付かずに電話機をリセットする

問題

クラスタ内コールバックまたはクラスタ間コールバックのシナリオで、発信者が対応不可のユーザ（ユーザ B とする）に対してコールバックを開始しました。 ユーザ B が対応可能になると、発信側の電話機に対応可能通知画面が表示されます。 発信者が何らかの理由で対応可能通知に気付かず、電話機がリセットされました。

たとえば、発信者が別のユーザ（ユーザ C とする）に連絡し、ユーザ C が通話中だったため [コールバック（CallBack）] ソフトキーを押します。 発信側の電話機に置換/保持画面が表示されますが、ユーザ B の対応可能通知がすでに発生したことが画面に示されません。

考えられる原因

ユーザが電話機をリセットしました。

ソリューション

電話機のリセット後、アクティブなコール中でないときに電話機のコールバック通知を確認します。 [折返し（Callback）] ソフトキーを押します。

コールバックのエラー メッセージ

ここでは、IP フォンの画面に表示されるエラー メッセージについて説明します。

コールバックがアクティブでない

問題

次のエラー メッセージが表示されます。

```
CallBack is not active. Press Exit to quit this screen.
```

考えられる原因

ユーザがアイドル状態で [コールバック（Callback）] ソフトキーを押しました。

ソリューション

エラー メッセージで指定された推奨アクションを実行してください。

コールバックがすでにアクティブになっている

問題

次のエラー メッセージが表示されます。

```
CallBack is already active on xxxx. Press OK to activate on yyyy. Press Exit to quit
this screen.
```

考えられる原因

ユーザがコールバックをアクティブにしようとしましたが、すでにアクティブになっています。

問題

エラー メッセージで指定された推奨アクションを実行してください。

コールバックをアクティブにできない

問題

次のエラー メッセージが表示されます。

```
CallBack cannot be activated for xxxx.
```

考えられる原因

ユーザがコールバックをアクティブにしようとしたときに、Unified Communications Manager データベースで内線番号が使用できないか、接続先への QSIG ルートが存在せず（つまり、内線番号が非QSIG トランク経由で接続されたリモートプロキシに属している）、データベース内で内線番号が見つかりません。

ソリューション

ユーザが再試行する必要があります。または、管理者が Cisco Unified CM Administration に電話番号を追加する必要があります。

キーがアクティブではありません

問題

コール中に、[コールバック（CallBack）] ソフトキーが電話に表示され、ユーザは電話が鳴る前に [コールバック（CallBack）] ソフトキーを押します。 ですが、電話に以下のエラー メッセージが表示されます。

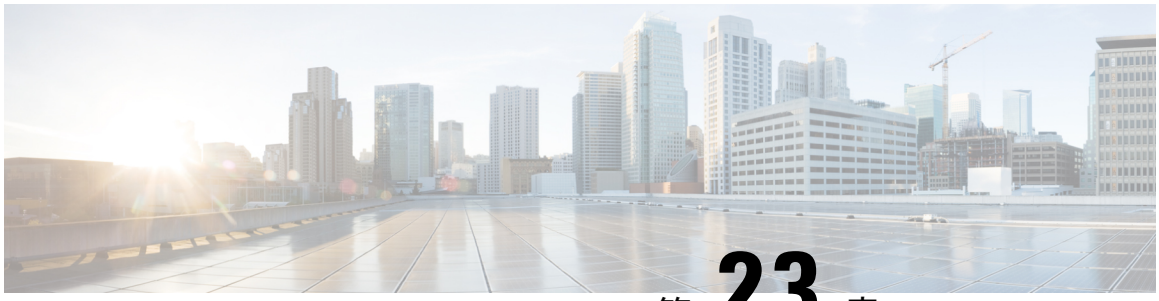
```
Key Not Active
```

考えられる原因

ユーザが [折返し（Callback）] ソフトキーを押すタイミングが適切でない可能性があります。

ソリューション

ユーザは呼び出し音またはビジー信号を聞いたあとで [折返し（Callback）] ソフトキーを押す必要があります。 間違ったタイミングでソフトキーを押すと、電話機にエラー メッセージが表示されることがあります。



第 23 章

ホットライン

ホットラインの概要

ホットライン機能はプライベート回線自動リングダウン（PLAR）機能を拡張し、ユーザーがオフフックしたとき（またはNewCallソフトキーや回線キーが押されたとき）に、すぐに所定の番号をダイヤルするよう電話機を設定できるようにします。 この機能は、緊急または「ホットライン」の番号の発信用に指定されている電話機に便利です。

管理者は、最大 15 秒の遅延を設定できます。 これにより、電話機がデフォルトでホットライン番号に設定される前にコールを発信する時間がユーザーに与えられます。 このタイマーは、パラメータ **[オフフックから最初の数字タイマー（Off Hook To First Digit Timer）]**（**[デバイス（Device）]** > **[デバイス設定（Device Settings）]** > **[SIP プロファイル（SIP Profile）]** で設定可能です。

ホットラインは、PLAR を使用する電話機に対して、次の新たな制限と管理者コントロールを追加します。

- コールを受信するホットラインデバイス（ホットラインを使用するように設定されたデバイス）は、他のホットラインデバイスからしかコールを受信せず、ホットライン以外の発信者を拒否します。
- ホットライン電話機は、コールのみ、受信のみ、またはコールと受信の両方に設定できます。
- ソフトキーテンプレートを電話機に適用することにより、ホットライン電話機上で使用可能な機能を制限できます。
- アナログ ホットライン電話機は、着信フックフラッシュ信号を無視します。

ルート クラス シグナリング

ホットラインは、ルート クラス シグナリングを使用して、ホットライン電話機が他のホットライン電話機からのコールしか受信できないようにします。 ルート クラスは、コールのトラフィックのクラスを識別する DSN コードです。 ルート クラスを通して、ルーティングや終端に関する特殊な要件が下流のデバイスに通知されます。 ホットライン電話機は、同じルート クラスを持つホットライン電話機からのコールしか受信できません。

通話の発信者名確認

ホットラインは、発信者 ID に基づく、設定可能な通話の発信者名確認も提供します。 設定可能な通話の発信者名確認を使用すれば、受信側のホットライン電話機は、発信者 ID 情報に基づいてコールを検査し、スクリーニング リストにある発信者にのみ接続を許可できます。

ホットラインのシステム要件

Unified Communications Manager には、次のホットライン システム要件があります。

- Unified Communications Manager クラスタ内の各サーバで 8.0（1）以降
- MGCP ゲートウェイ POTS 電話（FXS）
- SCCP ゲートウェイ POTS 電話（FXS）

ヒント Cisco Feature Navigator 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 Feature Navigator にアクセスするには、http://cfn.cloudapps.cisco.com/ITDIT/CFN/に進みます。

Cisco Feature Navigator にアクセスするには Cisco.com アカウントは必要ありません。

ホットラインの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	電話機能一覧の生成 （5 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、ホットラインをサポートする電話を決定します。
ステップ 2	カスタム ソフトキー テンプレートの作成 （323 ページ）	これはオプションです。 ホットライン電話の機能を制限する場合は、必要な機

	コマンドまたはアクション	目的
		能だけを許可するソフトキーテンプレートを作成します。
ステップ 3	電話でのホットラインの設定 （324 ページ）	電話をホットライン デバイスとして有効にします。
ステップ 4	ルート クラス シグナリングの設定タスク フロー （325 ページ）	ホットライン機能をサポートするルート クラス シグナリングを設定します。
ステップ 5	発信専用または受信専用のホットラインの設定タスク フロー （330 ページ）	**（オプション）** ホットライン電話の機能をコールの発信またはコールの受信のみに制限する場合は、発信と受信の設定を行います。
ステップ 6	コーリング サーチ スペースでのコール スクリーニングの設定 （333 ページ）	**（オプション）** コーリング サーチ スペースとパーティションを使用して、ホットライン電話のコール スクリーニング リストを設定します。

カスタム ソフトキー テンプレートの作成

ホットラインを設定すると、ホットライン電話で使用可能にする機能だけを表示するソフトキー テンプレートをカスタマイズできます。

Unified Communications Manager コール処理とアプリケーション用の標準ソフトキーテンプレートが含まれます。 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。

始める前に

電話機能一覧の生成 （5 ページ）

手順

ステップ 1 **[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 [新規追加] をクリックします。

ステップ 3 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、[コピー（Copy）]をクリックして新しいテンプレートを作成します。

ステップ 4 [ソフトキー テンプレート名（Softkey Template Name）]フィールドに、ソフトキー テンプレートを特定する一意の名前を入力します。

ステップ 5 テンプレートの使用方法を表す説明を入力します。 説明には、どの言語でも最大 50 文字まで指定できますが、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 このソフトキー テンプレートを標準のソフトキー テンプレートとして指定するには、[デフォルトのソフトキー テンプレート（Default Softkey Template）]チェックボックスをオンにします。

（注） デフォルト ソフトキー テンプレートとしてソフトキー テンプレートを指定した場合は、デフォルトの指定を削除しない限り、このソフトキー テンプレートを削除できません。

ステップ 7 **[保存]** をクリックします。

ソフトキー テンプレートがコピーされると、**[ソフトキー テンプレートの設定（Softkey Template Configuration）]** ウィンドウが再表示されます。

ステップ 8 （任意） [アプリケーションの追加（Add Application）]ボタンをクリックします。

ステップ 9 Cisco Unified IP 電話 LCD 画面上のソフトキーの位置を設定します。

ステップ 10 設定を保存するには、[保存（Save）]をクリックします。

電話でのホットラインの設定

電話をホットライン デバイスとして有効にするには、次の手順を使用します。

始める前に

これはオプションです。ホットライン電話に対して使用可能にする機能のみを表示するカスタム ソフトキー テンプレートを作成する場合は、カスタム ソフトキー テンプレートの作成（323 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。**[デバイス（Device）]** > **[電話（Phone）]**。

ステップ 2 [検索（Find）]をクリックして、ホットライン デバイスとして有効にする電話を選択します。

ステップ 3 [ホットライン デバイス（Hotline Device）]チェックボックスをオンにします。

ステップ 4 ホットライン電話専用のカスタム ソフトキー テンプレートを作成したら、[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 5 **[保存]** をクリックします。

（注） デバイス プールにソフトキーテンプレートを割り当てて、そのデバイス プールを電話に割り当てることもできます。

ルート クラス シグナリングの設定タスク フロー

ホットライン コールのルート クラス シグナリングを設定するには、このタスク フローを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	クラスタでのルート クラス シグナリングの有効化 （326 ページ）	トランクとゲートウェイのルート クラス シグナリングのクラスタ全体のデフォルトを有効に設定します。 （注） 個々のゲートウェイおよびトランクの設定は、クラスタ全体のデフォルト設定を上書きします。このサービス パラメータを使用してクラスタ全体でルート クラス シグナリングを有効にすると、ルート クラス シグナリングは、個々のトランクまたはゲートウェイで無効化できます。
ステップ 2	トランクでのルート クラス シグナリングの有効化 （326 ページ）	個々のトランクのルート クラス シグナリングを有効にします。
ステップ 3	ゲートウェイでのルート クラス シグナリングの有効化 （327 ページ）	MGCP T1/CAS または MGCP PRI ゲートウェイのルート クラス シグナリングを有効にします。
ステップ 4	ホットライン ルート クラスのシグナリング ラベルの設定 （328 ページ）	ホットライン ルート クラスの SIP シグナリング ラベルを設定します。
ステップ 5	ホットライン ルート パターンでのルート クラスの設定 （328 ページ）	ホットライン コールをルーティングするルート パターンのルート クラスを設定します。
ステップ 6	ホットライン トランスレーション パターンでのルート クラスの設定 （329 ページ）	（**オプション**） ホットライン コールでトランスレーション パターンを使用する場合は、トランスレーション パターンのルート クラスを設定します。

クラスタでのルート クラス シグナリングの有効化

[有効なルート クラス トランク シグナリング（Route Class Trunk Signaling Enabled）]サービス パラメータを [True]に設定すると、ルート クラス シグナリングをサポートするクラスタ内の全トランクまたはゲートウェイのデフォルトのルート クラス シグナリングが有効に設定されます。

（注） 個々のゲートウェイおよびトランクの設定は、クラスタ全体のデフォルト設定を上書きします。このサービス パラメータを使用してクラスタ全体でルート クラス シグナリングを有効にすると、ルート クラス シグナリングは、個々のトランクまたはゲートウェイで無効化できます。

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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

ステップ 2 [有効なルート クラス トランク シグナリング（Route Class Trunk Signaling Enabled）]サービス パラメータを [True]に設定します。

ステップ 3 **[保存]** をクリックします。

次のタスク

個々のトランクまたはゲートウェイでルート クラス シグナリングを設定するには、次の手順を使用します。

トランクでのルート クラス シグナリングの有効化 （326 ページ）

ゲートウェイでのルート クラス シグナリングの有効化 （327 ページ）

トランクでのルート クラス シグナリングの有効化

個々のトランクのルート クラス シグナリングを有効にするには、次の手順を使用します。個々のトランクの設定は、クラスタワイド サービス パラメータ設定を上書きします。

始める前に

クラスタでのルート クラス シグナリングの有効化（326ページ）の手順に従って、クラスタワイド サービス パラメータを使用し、クラスタ内の全トランクにデフォルトのルート クラス シグナリング設定を設定します。

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。**[デバイス(Device)]** > **[トランク(Trunk)]**。

ステップ 2 [検索（Search）]をクリックして、ルート クラス シグナリングを有効にする SIP トランクを選択します。

ステップ 3 [ルート クラス シグナリングの有効化（Route Class Signaling Enabled）]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。

- [デフォルト（Default）]—このトランクは [ルート クラス シグナリングの有効化（Route Class Signaling Enabled）]サービス パラメータの設定を使用します。
- [オフ（Off）]—このトランクに対して、ルート クラス シグナリングが無効です。
- [オン（ON）]—このトランクに対して、ルート クラス シグナリングが有効です。

ステップ 4 **[保存（Save）]** をクリックします。

ゲートウェイでのルート クラス シグナリングの有効化

この手順を使用して、個々の MGCP PRI または MGCP T1/CAS ゲートウェイでルート クラス シグナリングを有効にします。 個々のゲートウェイの設定は、クラスタ全体のサービス パラメータの設定よりも優先されます。

始める前に

クラスタでのルート クラス シグナリングの有効化（326ページ）の手順に従い、クラスタ全体のサービス パラメータを使用して、クラスタ内のゲートウェイのデフォルト ルート クラス シグナリング設定を指定します。

トランクでのルート クラス シグナリングの有効化（326ページ）の手順を実行して、個々のトランクのルート クラス シグナリングを設定します。

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。**[デバイス（Device）]** > **[ゲートウェイ（Gateway）]**。

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 [ルート クラス シグナリングの有効化（Route Class Signaling Enabled）]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。

- デフォルト（Default）：このゲートウェイは、クラスタ全体のサービスパラメータの [ルート クラス シグナリングの有効化（Route Class Signaling Enabled）] を使用します。

- オフ（Off）：このゲートウェイでルートクラス シグナリングが無効になります。
- オン（On）：このゲートウェイでルートクラス シグナリングが有効になります。

ステップ 4 音声コールの音声ルート クラスをエンコードする場合は、[音声ルート クラスのエンコード（Encode Voice Route Class）]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。

ホットライン ルート クラスのシグナリング ラベルの設定

使用するホットライン ルート クラスの SIP シグナリング ラベル値を設定する必要があります。

始める前に

トランクとゲートウェイのルート クラス シグナリングを有効にします。 詳細については、クラスタでのルート クラス シグナリングの有効化 （326 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）]**。

ステップ 2 [サーバ（Server）]ドロップダウン リストから、CallManager サービスが実行され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 [詳細設定（Advanced）]をクリックします。

ステップ 5 **[SIP ルート クラス命名機関（SIP Route Class Naming Authority）]** サービス パラメータ フィールドに、命名機関を表す値と、SIP シグナリングでルート クラスを表すために使用されるラベルのコンテキストを入力します。 デフォルト値は **[cisco.com]** です。

ステップ 6 **[SIP ホットライン ボイス ルート クラス ラベル（SIP Hotline Voice Route Class Label）]** サービス パラメータ フィールドに、ホットライン ボイス ルート クラスを表すラベルを入力します。 デフォルト値は [hotline]です。

ステップ 7 **[SIP ホットライン データ ルート クラス ラベル（SIP Hotline Data Route Class Label）]** サービス パラメータ フィールドに、ホットライン データ ルート クラスを表すラベルを入力します。 デフォルト値は **[ccdata]** です。

ステップ 8 **[保存（Save）]** をクリックします。

ホットライン ルート パターンでのルート クラスの設定

この手順では、ホットラインデバイスに特有のコール ルーティング手順について説明します。 ネットワークでルートパターンおよびトランスレーションパターンを設定する方法の詳細については、Cisco Unified Communications Manager システム設定ガイドを参照してください。

ホットライン コールをルーティングする予定のルート パターンごとに、そのルート パターンのルート クラスを[**ホットライン ボイス（Hotline Voice**）] または[**ホットライン データ（Hotline Data**）] に設定する必要があります。

始める前に

ホットライン ルート クラスのシグナリング ラベルの設定 （328 ページ）

この手順を実行する前に、ルート パターンを使用してネットワーク コール ルーティングを設定してください。

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。**[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）]** の順に選択します。

ステップ 2 **[検索（Find）]** をクリックして、ネットワークのルート パターンのリストを表示します。

ステップ 3 ホットライン コールのルーティングに使用される各 T1/CAS ルート パターンについて、次のように設定します。

a) **[ルート パターンの検索と一覧表示（Find and List Route Patterns）]** ウィンドウから、ルート パターンを選択します。

b) **[ルート クラス（Route Class）]** ドロップダウン リスト ボックスから、**[ホットライン ボイス（Hotline Voice）]** または **[ホットライン データ（Hotline Data）]** のいずれかをこのルート パターンのルート クラスとして選択します。

c) **[保存（Save）]** をクリックします。

ホットライン トランスレーション パターンでのルート クラスの設定

始める前に

この手順を実行する前に、ルート パターンとトランスレーション パターンを指定してネットワーク コール ルーティングを設定しておく必要があります。

ホットライン ルート パターンでのルート クラスの設定 （328 ページ）の手順を実行します。

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）] > [トランスレーション パターン（Translation Pattern）]**。

ステップ 2 クラスタのトランスレーション パターンを表示するには、[検索（Find）]をクリックします。

ステップ 3 ホットライン番号で使用するトランスレーション パターンごとに、次の手順を実行します。

a) [ルート クラス（Route Class）]ドロップダウン リスト ボックスから、[ホットライン ボイス（Hotline Voice）]または [ホットライン データ（Hotline Data）]を選択します。
b) **[保存（Save）]** をクリックします。

発信専用または受信専用のホットラインの設定タスク フロー

このタスク フローの設定例では、ホットラインの電話を発信専用、または受信専用のどちらかに設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	発信専用/受信専用のホットラインのパーティションの設定 （330 ページ）	2 つのパーティションを作成します。1 つは空で、もう 1 つは新しい CSS に割り当てます。
ステップ 2	発信専用/受信専用のホットラインのコーリング サーチ スペースの設定 （331 ページ）	新しいコーリング サーチ スペースを作成し、新しい CSS の 1 つをこの CSS に割り当てます。 この CSS には他のパーティションは含まれません。
ステップ 3	次のいずれかの手順を実行します。 • 発信専用ホットライン電話の設定（332 ページ） • 受信専用ホットライン電話の設定（332 ページ）	発信専用に設定する場合、空のパーティションを電話回線に割り当てます。 受信専用に設定するには、その電話に新しい CSS を割り当てます。

発信専用/受信専用のホットラインのパーティションの設定

ホットライン電話を発信専用または受信専用に設定する場合、2 つのパーティションを作成する必要があります。

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。**[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）]**。
ステップ 2 [新規追加] をクリックします。
ステップ 3 新しいパーティションを作成します。

ステップ 4 パーティションの一意の名前と説明を入力します。 たとえば、IsolatedPartitionのように入力します。

（注） このパーティションを CSS に割り当てることはできません。

ステップ 5 [保存]をクリックします。

ステップ 6 手順2から5までを繰り返し、2番目のパーティションを作成します。 たとえば、EmptyPartitionのように入力します。

（注） このパーティションは、電話回線に割り当てられず、NoRouteCSS に割り当てられます。

発信専用/受信専用のホットラインのコーリング サーチ スペースの設定

コーリング サーチを作成し、作成した 2 つのパーティションのいずれかをコーリング サーチ スペースに割り当てる必要があります。

始める前に

発信専用/受信専用のホットラインのパーティションの設定 （330 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** > **コントロールのクラス** > **コーリングサーチスペース**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 コーリング サーチ スペースの**名前**と**説明**を入力します。

ステップ 4 [**使用可能なパーティション（Available Partitions）**] リスト ボックスから、矢印を使用して [**EmptyPartition**] パーティションを選択します。

（注） パーティションがこのコーリング サーチ スペースのみに割り当てられ、電話回線に割り当てられていないことを確認します。

ステップ 5 [保存]をクリックします。

次のタスク

次のいずれかの手順を実行します。

- 発信専用ホットライン電話の設定 （332 ページ）
- 受信専用ホットライン電話の設定 （332 ページ）

発信専用ホットライン電話の設定

パーティションとコーリング サーチ スペースを設定した後、ホットライン電話を発信専用に設定するには、次の手順を実行します。

始める前に

発信専用/受信専用のホットラインのコーリング サーチ スペースの設定 （331 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）] > [電話（Phone）]**。

ステップ 2 [検索（Find）]をクリックして、ホットライン電話機を選択します。

ステップ 3 左側のナビゲーション ウィンドウで、電話回線をクリックします。
[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 [**ルート パーティション（Route Partition**）] ドロップダウン リストから、作成した空のパーティションを選択します。

ステップ 5 **[保存（Save）]** をクリックします。

受信専用ホットライン電話の設定

コーリング サーチ スペースとパーティションをすでに作成している場合、次の手順を実行して、ホットライン電話機をコールの受信専用に設定します。

始める前に

発信専用/受信専用のホットラインのコーリング サーチ スペースの設定 （331 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、ホットライン電話機を選択します。

ステップ 3 [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、前の手順で作成した新しい CSS を選択します。

ステップ 4 **[保存（Save）]** をクリックします。

コーリング サーチ スペースでのコール スクリーニングの設定

パーティション内にあるホットライン電話だけが互いにコールできるようにする固有の CSS を割り当てて、（回線間で）イントラスイッチされたホットライン コールのコール スクリーニングを設定します。

（注） それぞれのパターンが許可またはスクリーニングする各番号パターンと一致するトランスレーション パターンを作成して、コール スクリーニングを設定することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	ホットライン コール発信者名確認のためのパーティションの設定 （333 ページ）	ホットライン電話回線用の新しいパーティションを作成します。
ステップ 2	ホットライン コール発信者名確認のためのコーリング サーチ スペースの作成 （334 ページ）	スクリーニング リストの新しい CSS を作成します。 CSS には、許可するホットライン番号だけを含むパーティションを含める必要があります。
ステップ 3	ホットライン電話でのコール発信者名確認の設定 （335 ページ）	新しい CSS とパーティションをホットライン電話に割り当てます。

ホットライン コール発信者名確認のためのパーティションの設定

コーリング サーチ スペースを使用したホットライン電話機のコール発信者名確認を設定するには、発信者名の確認を許可するホットライン番号のみを対象としたパーティションをセットアップする必要があります。

ホットライン コールの発信者確認リストのために新しいパーティションを作成する必要がある場合、次の手順を実行します。

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** > **コントロールのクラス** > **パーティション**。

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。

説明にはどの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサイド（&）、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。

ホットライン コール発信者名確認のためのコーリング サーチ スペースの作成

次の手順を実行して、通話の発信者名確認リストでホットライン電話用の新しいコーリング サーチ スペースを作成します。 この CSS 用に選択したパーティション内のホットライン番号のみが、通話の発信者名確認リストで許可するホットライン番号であることを確認します。スクリーニングで除外するホットライン番号がこの CSS のパーティションに含まれないようにします。

始める前に

ホットライン コール発信者名確認のためのパーティションの設定 （333 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** > **コントロールのクラス** > **コーリングサーチスペース**。

ステップ 2 [新規追加] 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、どの言語でも最大50文字まで指定できますが、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、**コントロール（Ctrl）**キーを押したまま、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。

ホットライン電話でのコール発信者名確認の設定

ホットライン コール スクリーニング用にコーリング サーチ スペースおよびパーティションをすでに設定している場合は、この手順を実行してホットライン電話機にコーリング サーチ スペースおよびパーティションを割り当てます。

始める前に

ホットライン コール発信者名確認のためのコーリング サーチ スペースの作成 （334 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、ホットライン電話機を選択します。

ステップ 3 **[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、ホットライン コール スクリーニング リスト用に作成した新しいコーリング サーチ スペースを選択します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 左側のナビゲーション ウィンドウから、ホットライン コールに使用する電話回線をクリックします。
[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 6 [**ルート パーティション（Route Partition**）] ドロップダウン リストから、設定するコーリング サーチ スペースに含まれるパーティ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。

ホットラインのトラブルシューティング

次の表に、ホットライン コールが正しくダイヤルされない場合のトラブルシューティング情報を示します。

表 *25：*ホットライン コールが正しくダイヤルされない場合のトラブルシューティング

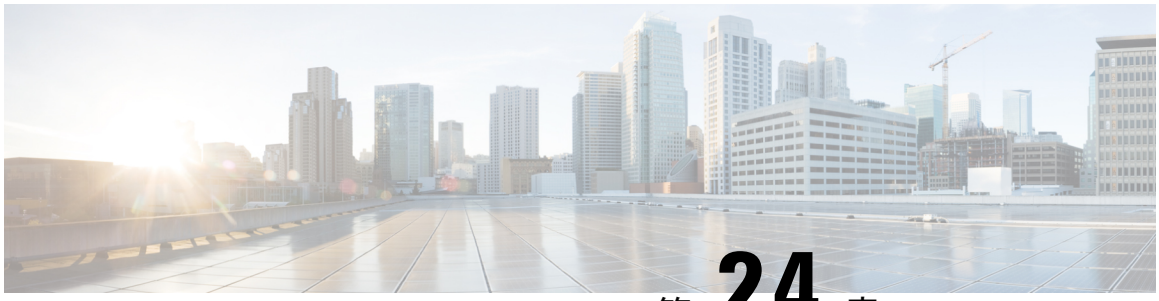
問題	ソリューション
ダイヤル トーン	PLAR 設定を確認します。
リオーダー トーンまたはVCA（クラスタ内コール）	• PLAR 設定を確認します。 • 両端の電話機がホットライン電話機として設定されていることを確認します。
リオーダー トーンまたは VCA（クラスタ内または TDM コール）	• PLAR 設定を確認します。 • 両端の電話機がホットライン電話機として設定されていることを確認します。 • トランクでルート クラス シグナリングがイネーブルになっていることを確認します。 • CAS ゲートウェイのルート クラス トランスレーションの設定を確認します。

次の表に、発信者 ID に基づくコール スクリーニングが機能しない場合のトラブルシューティング情報を示します。

表 *26：*発信者 *ID* に基づくコール スクリーニングの問題のトラブルシューティング

問題	ソリューション
コールが許可されない	• 発信者 ID を確認します。 • パターンをスクリーンCSS に追加します。

問題	ソリューション
コールが許可される	パターンをスクリーン CSS から削除します。



第 24 章

スピード ダイヤルと短縮ダイヤル

スピード ダイヤルと短縮ダイヤルの概要

管理者は、ユーザに対して短縮ダイヤル ボタンを表示する場合、または特定のユーザが割り当てられていない電話を設定する場合に、電話の短縮ダイヤル番号を設定できます。 ユーザは Cisco Unified Communications セルフ ケア ポータルで各自の電話の短縮ダイヤル ボタンを変更できます。 短縮ダイヤル エントリを設定すると、一部の短縮ダイヤル エントリが IP フォンの短縮ダイヤル ボタンに割り当てられ、その他の短縮ダイヤル エントリが固定短縮ダイヤルに使用されます。 ユーザが番号のダイヤルを開始すると、[短縮（AbbrDial）] ソフトキーが表示されます。ユーザは、固定短縮ダイヤルの適切なインデックス（コード）を入力することで、任意の短縮ダイヤル エントリにアクセスできます。

電話の短縮ダイヤル設定は電話の物理ボタンに関連付けられていますが、固定短縮ダイヤル設定は電話のボタンには関連付けられていません。

一時停止による短縮ダイヤルのプログラミング

短縮ダイヤルでコンマをプログラムすると、強制承認コード（FAC）、クライアント識別コード（CMC）、ダイヤル中のポーズ、または付加的なディジット（ユーザ内線、会議のアクセス コード、ボイスメールのパスワードなど）を必要とする接続先にダイヤルできます。 短縮ダイヤル内では、各コンマ（,）は次のいずれかを表します。

- 宛先コールアドレスと FAC または CMC コードを区切る区切り文字
- 接続後の DTMF ディジットを送信する 2 秒前

たとえば、FAC コードと CMC コードを含み、その後に IVR プロンプトが続く短縮ダイヤルが必要だとします。

- 着信番号は 91886543 です。
- FAC コードは 8787 です。

- CMC コードは 5656 です。
- IVR 応答は 987989＃です。これは、通話が接続されてから 4 秒後に入力する必要があります。

この場合、短縮ダイヤルとして **91886543,8787,5656,,987989＃** をプログラムします。

スピード ダイヤルと短縮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	電話機能一覧の生成 （5 ページ）	スピード ダイヤル機能と短縮ダイヤル機能をサポートするデバイスを特定するためのレポートを作成します。
ステップ 2	スピード ダイヤルと短縮ダイヤルの設定 （340 ページ）	スピード ダイヤル番号と短縮ダイヤル番号を設定します。

スピード ダイヤルと短縮ダイヤルの設定

全部で 199 のスピード ダイヤルおよび短縮ダイヤルを設定できます。 電話機の物理的なボタンにスピード ダイヤルを設定します。 短縮ダイヤルでアクセスするスピード ダイヤル番号の短縮ダイヤルを設定します。 同じウィンドウでスピード ダイヤル エントリと短縮ダイヤル インデックスを設定できます。

FAC や CMC と同様に、ポスト接続 DTMF のディジットをスピード ダイヤルに含めて設定できます。

スピード ダイヤルと短縮ダイヤルを設定するには、次の手順を実行します。

（注） すべての Cisco IP 電話 で短縮ダイヤルをサポートしているわけではありません。 該当の電話機のユーザ ガイドを参照してください。

始める前に

電話機能一覧の生成 （5 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）]**。 検索条件を入力し、[**検索（Find**）] をクリックします。 スピード ダイヤル ボタンを設定する電話を選択します。

ステップ 2 [**電話の設定（Phone Configuration**）] ウィンドウで、ウィンドウ上部の関連リンクのドロップダウン リストから [**スピード ダイヤルの追加/更新（Add/Update Speed Dials**）] を選択し、[**移動（Go**）] をクリックします。
[**スピード ダイヤルと短縮ダイヤルの設定（Speed Dial and Abbreviated Dial Configuration**）] ウィンドウが電話機に表示されます。

ステップ 3 [**番号（Number**）] フィールドに、ユーザがスピード ダイヤル ボタンまたは短縮ダイヤルの短縮ダイヤル インデックスを押すときにダイヤルされる番号を入力します。 0 ～ 9 の数字、*、#、および + （国際エスケープ文字）を入力できます。 スピード ダイヤルにポーズを含めるには、DTMF のディジットを送信する前にデリミタとしてカンマ（,）を入力できます。 文字列に含める各カンマは、追加の 2 秒間のポーズを表します。 たとえば、2 個のカンマ（,,）は、4 秒間のポーズを表します。 このポーズは、スピード ダイヤル文字列の中の他の数字と、FAC および CMC を区別するためにも使用できます。

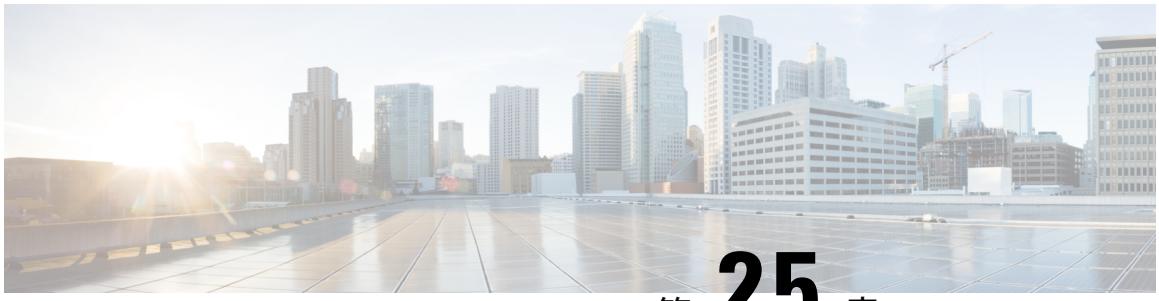
（注） スピード ダイヤル文字列に FAC および CMC を含めるとき、次の要件が満たされていることを確認してください。

- スピード ダイヤル文字列では、FAC が常に CMC よりも前に来る必要があります。
- FAC および DTMF のディジットを含むスピード ダイヤルには、スピード ダイヤル ラベルが必要です。
- 文字列内の FAC および CMC のディジット間に入力できるカンマは 1 つだけです。

ステップ 4 [**ラベル（Label**）] フィールドで、スピード ダイヤル ボタンまたは短縮ダイヤル番号に対して表示するテキストを入力します。

（注） このフィールドは、どの電話でも使用できるわけではありません。 このフィールドが Cisco Unified IP Phone で使用可能かどうかを判断するには、使用している電話機モデルのユーザ マニュアルを参照してください。

ステップ 5 （任意） スピード ダイヤルにポーズを設定する場合、FAC、CMC、および DTMF のディジットが電話画面に表示されないようにラベルを追加する必要があります。



第 25 章

Webダイヤラー

Webダイヤラー の概要

Cisco Webダイヤラー は Unified Communications Managerノードにインストールされ、Unified Communications Manager とともに使用されます。 これにより、Cisco Unified IP 電話 ユーザは Web 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することができます。

Cisco Webダイヤラー は社員名簿にあるハイパーリンクされた電話番号を使用します。そのため、相手の電話番号を Web ページでクリックすればコールを発信できます。 Cisco Webダイヤラー は、IPv4 と IPv6 アドレスの両方をサポートします。

Cisco Unified Communications セルフケア ポータルの [ディレクトリ（Directory）] ウィンドウで、以下のような URL を使用して Cisco Webダイヤラー を起動します。

```
https://<IP address of Cisco Unified Communications Manager server>:8443/webdialer/
Webdialer
```

Cisco Webダイヤラー 画面で、**[ログイン（Login）]** をクリックして WebdDialer システムにアクセスします。 新しいポップアップウィンドウで、Unified Communications Manager の **[ユーザー ID（User ID）]** と **[パスワード（Password）]** を入力して、必要なコールの実行に必要なアクティビティを実行できます。

Webダイヤラー の前提条件

Cisco Webダイヤラー では、次のソフトウェア コンポーネントが必要です。

- CTI 対応の Cisco Unified IP 電話

Webダイヤラー の設定タスク フロー

始める前に

- Webダイヤラー の前提条件 （343 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	Webダイヤラーの有効化 （345ページ）	Webダイヤラー サービスをアクティベートします。
ステップ 2	（任意） Webダイヤラー トレースの有効化 （346 ページ）	Webダイヤラー トレースを表示するには、トレースを有効にします。
ステップ 3	（任意） Webダイヤラー Servlet の設定 （347 ページ）	Webダイヤラー servlet を設定します。
ステップ 4	（任意） リダイレクタ Servlet の設定 （347 ページ）	HTTPS over HTTP インターフェイスを使用して開発するマルチクラスタ アプリケーションを使用する場合、リダイレクタ servlet を設定します。
ステップ 5	（任意） Webダイヤラー アプリケーション サーバの設定 （348 ページ）	Cisco Webダイヤラー のリダイレクタを設定します。
ステップ 6	（任意） CTI へのセキュア TLS 接続の設定 （348 ページ） を行うには、次のサブ タスクを完了します。 • WDSecureSysUser アプリケーション ユーザの設定 （349 ページ） • CAPF プロファイルの設定 （221 ページ） • Cisco Webダイヤラー Web サービスの設定 （224 ページ）	Webダイヤラー では、発信するときに、WDSecureSysUser アプリケーションのユーザ クレデンシャルを使用して CTI へのセキュアな TLS 接続を確立します。システムが混合モードで稼動している場合、次の手順に従います。
ステップ 7	Webダイヤラー の言語ロケールの設定 （352 ページ）	Cisco Unified Communications のセルフケア ポータル メニューのロケール フィールドを設定し、Webダイヤラーの表示言語を定義します。
ステップ 8	WebDialer アラームの設定 （353 ページ）	Web Dialer 機能に問題がある場合、管理者に警告します。

	コマンドまたはアクション	目的
ステップ 9	（任意） アプリケーション ダイヤル ルールの設定 （354 ページ）	アプリケーションに複数のクラスタが必要な場合、アプリケーションのダイヤル ルールを設定します。
ステップ 10	標準 CCM エンド ユーザ グループへのユーザの追加 （354 ページ）	各 Webダイヤラー ユーザを Cisco Unified Communications Manager の標準エンドユーザ グループに追加します。
ステップ 11	（任意） プロキシ ユーザの設定 （355 ページ） を行うには、次のサブ タスクを完了します。 • Webダイヤラー エンドユーザの追加 （356 ページ） • 認証プロキシ権限の割り当て （356 ページ）	makeCallProxy HTML over HTTP インターフェイスを使用して、Cisco Webダイヤラーを使用するためのアプリケーションを開発している場合、プロキシ ユーザを作成します。

Webダイヤラー の有効化

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[ツール（Tools）] > [サービス アクティベーション（Service Activation）]** を選択します。

ステップ 2 **[サーバ（Server）]** ドロップダウン リストから、リストされている Unified Communications Manager サーバを選択します。

ステップ 3 [CTI サービス（CTI Services）]から、[Cisco Webダイヤラー Web サービス（Cisco Webダイヤラー Web Service）]チェック ボックスをオンにします。

ステップ 4 **[保存]** をクリックします。

ステップ 5 [Cisco Unified Serviceability] から、以下を選択します。**[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択して、CTI Manager サービスがアクティブでスタート モードになっていることを確認します。

Webダイヤラー を正しく機能させるには、CTI Manager サービスをアクティブにして、スタート モードにする必要があります。

次のタスク

Webダイヤラー の言語ロケールの設定 （352 ページ） または、次のオプション タスクの一部または全部を実行します。

- Webダイヤラー トレースの有効化 （346 ページ）

- Webダイヤラー Servlet の設定 （347 ページ）
- リダイレクタ Servlet の設定 （347 ページ）
- Webダイヤラー アプリケーション サーバの設定 （348 ページ）
- CTI へのセキュア TLS 接続の設定 （348 ページ）

Webダイヤラー トレースの有効化

Cisco Webダイヤラー のトレースを有効にするには、Cisco Unified Serviceability 管理アプリケーションを使用します。 トレースの設定は、Webダイヤラー Servlet と Redirector Servlet の両方に適用されます。 トレースを収集するには、Real-Time Monitoring Tool（RTMT）を使用します。

Webダイヤラー トレース ファイルにアクセスするには、次の CLI コマンドを使用します。

- **file get activelog tomcat/logs/Webダイヤラー/log4j**
- **file get activelog tomcat/logs/redirector/log4j**

トレースの詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

始める前に

Webダイヤラー の有効化 （345 ページ）

手順

ステップ 1 Cisco Unified Communications Manager アプリケーションのナビゲーション ドロップダウン リストから、**[Cisco Unified Serviceability]** を選択し、**[移動（Go）]** をクリックします。

ステップ 2 **[トレース（Trace）]** > **[設定（Configuration）]** を選択します。

ステップ 3 [サーバ（Server）]ドロップダウン リストから、トレースを有効にするサーバを選択します。

ステップ 4 [サービス グループ（Service Group）]ドロップダウン リストから、[CTI サービス（CTI Services）]を選択します。

ステップ 5 **[サービス（Service）]** ドロップダウン リストから、**Cisco Webダイヤラー Web サービス**を選択します。

ステップ 6 [トレースの設定（Trace Configuration）]ウィンドウで、トラブルシューティングの要件に応じてトレースの設定を変更します。

（注） Webダイヤラー トレースの構成時の設定の詳細については、『*Cisco Unified Serviceability Administration Guide*』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。

Webダイヤラー Servlet の設定

Webダイヤラー Servlet は、特定のクラスタ内の Cisco Unified Communications Manager のユーザがコールを発信および完了できるようにする Java Servlet です。

始める前に

Webダイヤラー の有効化 （345 ページ）

手順

ステップ 1 **[System（システム）]** > **[Service Parameters（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、Cisco Webダイヤラー Web サービス パラメータを設定する Cisco Unified Communications Manager サーバを選択します。

ステップ 3 **[サービス（Service）]** ドロップダウンメニューから、**[Cisco Webダイヤラー Web Service]** を選択します。

ステップ 4 関連する Webダイヤラー Web サービスのパラメータを設定します。 パラメータの詳細については、オンライン ヘルプを参照してください。

ステップ 5 新しいパラメータ値を有効にするには、Cisco Webダイヤラー Web サービスを再起動します。

リダイレクタ Servlet の設定

リダイレクタ Servlet は Java ベース Tomcat Servlet です。 Cisco Webダイヤラー ユーザが要求を行うと、リダイレクタ Servlet が Cisco Unified Communications Manager のクラスタでその要求を検索し、Cisco Unified Communications Manager のクラスタ内にある特定の Cisco Webダイヤラー サーバにその要求をリダイレクトします。 リダイレクタ Servlet は、HTML over HTTPS インターフェイスを使用して開発されたマルチクラスタ アプリケーションでのみ使用できます。

（注） Unified Communications Manager のクラスタ間 HTTPS 通信用にセットアップされたすべてのノードが、設定されている最小の TLS バージョンをサポートしていることを確認します。

始める前に

Webダイヤラー の有効化 （345 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。**[システム（System）]** > **[サービス パラメータ（Service Parameters）]**。

ステップ 2 [サーバ（**Server**）] ドロップダウン リストから、リダイレクタ サーブレットを設定する Cisco 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 Webダイヤラー Web サービスを選択します。

ステップ 4 関連する Webダイヤラー Web サービスのパラメータを設定します。 パラメータの詳細については、オンライン ヘルプを参照してください。

ステップ 5 新しいパラメータ値を有効にするには、Cisco Webダイヤラー Web サービスを再起動します。

Webダイヤラー Web サービスの詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

Webダイヤラー アプリケーション サーバの設定

アプリケーション サーバは Redirector Servlet を設定するために必要です。 リダイレクタは、1 つのクラスタに複数の Unified Communications Manager サーバを設定している場合にのみ必要です。

始める前に

Webダイヤラー の有効化 （345 ページ）

手順

ステップ 1 [Cisco Unified CM の管理アプリケーション サーバ（Cisco Unified Communications Manager Administration Application server）] ウィンドウから、**[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 [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ダイヤラー アプリケーション サーバ（Cisco Webダイヤラー application server**）] を選択します。
選択したサーバは、Cisco Webダイヤラー Web サービスの [**サービスパラメータの設定（Service Parameter Configuration**）] ウィンドウの [**Webダイヤラー の一覧（List of Webダイヤラーs**）] フィールドに表示されます。

CTI へのセキュア TLS 接続の設定

Webダイヤラー では、発信するときに、WDSecureSysUser アプリケーションのユーザ クレデンシャルを使用して CTI へのセキュアな TLS 接続を確立します。 セキュアな TLS 接続を確立するように WDSecureSysUser アプリケーション ユーザを設定するには、次の作業を実行します。

始める前に

- Cisco CTL Client をインストールし、設定します。 CTL クライアントの詳細については、Cisco Unified Communications Manager セキュリティガイドを参照してください。
- [エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウの [クラスタ セキュリティ モード（Cluster Security Mode）] を 1 に設定します（混合モード）。 システムを混合モードで操作することは、システムの他のセキュリティ機能に影響を及ぼします。 システムが現在混合モードで動作していない場合、これらの相互作用を理解していないときは、混合モードに切り替えないでください。 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。
- [クラスタ SIPOAuth モード（Cluster SIPOAuth Mode）] フィールドが [有効（Enabled）] に設定されていることを確認します。
- 最初のノードで Cisco 認証局プロキシ機能 サービスをアクティブにします。
- Webダイヤラー の有効化 （345 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	WDSecureSysUser アプリケーション ユーザの設定 （349 ページ）	WDSecureSysUser アプリケーション ユーザを設定します。
ステップ 2	CAPF プロファイルの設定 （221 ページ）	WDSecureSysUser アプリケーション ユーザの CAPF プロファイルを設定します。
ステップ 3	Cisco Webダイヤラー Web サービスの設定 （224 ページ）	Cisco Webダイヤラー Web サービスのサービス パラメータを設定します。

WDSecureSysUser アプリケーション ユーザの設定

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。**[ユーザ管理（User Management）]** > **[アプリケーション ユーザ（Application User）]** 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 [**アプリケーション ユーザの検索と一覧表示のアプリケーション（Find and List Application Users Application）**] ウィンドウから、[**WDSecureSysUser**] を選択します。

ステップ 4 [**アプリケーション ユーザの設定（Application User Configuration）**] ウィンドウの各フィールドを設定し、[**保存（Save）**] をクリックします。

次のタスク

CAPF プロファイルの設定 （221 ページ）

CAPF プロファイルの設定

認証局プロキシ機能（CAPF）は、セキュリティ証明書を発行して、認証するタスクを実行するコンポーネントです。 アプリケーション ユーザの CAPF プロファイルを作成すると、プロファイルは設定の詳細を使用してアプリケーションの安全な接続を開きます。

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。**[User Management]** > **[Application User CAPF Profile]**。

ステップ 2 次のいずれかの作業を実行します。

- 新しい CAPF プロファイルを追加するには、**[検索対象（Find）]** ウィンドウで **[新規追加]** をクリックします。
- 既存のプロファイルをコピーするには、適切なプロファイルを見つけ、**[コピー（Copy）]** 列内にあるそのレコード用の **[コピー（Copy）]** アイコンをクリックします

既存のエントリを更新するには、適切なプロファイルを見つけて表示します。

ステップ 3 関連する CAPF プロファイル フィールドを設定または更新します。 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]** をクリックします。

ステップ 5 セキュリティを使用するアプリケーション ユーザおよびエンド ユーザごとに、この手順を繰り返します。

CAPF プロファイルの設定

設定	説明
[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、CAPF 操作のアプリケーション ユーザを選択し が表示されます。 この設定は、[**エンド ユーザ CAPF プロファイル（End User CAPF Profile）**]
[エンドユーザID(End User ID)]	ドロップダウン リストから、CAPF 操作のエンド ユーザを選択します。 この この設定は、[**アプリケーション ユーザ CAPF プロファイル（Application Use**

設定	説明
インスタンス ID（Instance ID）	1 ～ 128 文字の英数字（a ～ z、A ～ Z、0 ～ 9）を入力します。 インスタ 1 つのアプリケーションに複数の接続（インスタンス）を設定できます。 ケーション PC（エンドユーザの場合）またはサーバ（アプリケーション 書があることを確認します。 このフィールドは、Web サービスおよびアプリケーションをサポートする ス パラメータに関連しています。
[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 • [インストール/アップグレード（Install/Upgrade）]：このオプションを るか、既存のローカルで有効な証明書がアップグレードされます。
認証モード（Authentication Mode）	証明書の操作が [インストール/アップグレード（Install/Upgrade）] の場合、 指定されます。つまり、ユーザ/管理者によって [**JTAPI/TSP 設定（JTAPI** 合にのみ、ローカルで有効な証明書のインストール/アップグレードまたは
認証文字列（Authentication String）	独自の認証文字列を作成するには、一意の文字列を入力します。 各文字列は 4 ～ 10 桁である必要があります。 ローカルで有効な証明書のインストールまたはアップグレードを実行する 文字列を入力することが必要です。 この文字列は、1 回だけ使用できます 度使用することはできません。
[文字列を生成(Generate String)]	認証文字列を自動的に生成するには、このボタンをクリックします。 4 ～ ルドに表示されます。
キー サイズ（ビット数）（Key Size (bits)）	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 キー生成を低いプライオリティで設定すると、アクションの実行中もアプ かります。
[操作の完了期限(Operation Completes By)]	このフィールドは、すべての証明書操作をサポートし、操作を完了する必 表示される値は、最初のノードに適用されます。 この設定は、証明書の操作を完了する必要がある期間のデフォルトの日数 **in (days)**）] エンタープライズ パラメータと併用します。 このパラメータ
[証明書の操作ステータス(Certificate Operation Status)]	このフィールドは、pending、failed、successful など、証明書操作の進行状 このフィールドに表示される情報は変更できません。

Cisco IP Manager Assistant 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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

ステップ 2 [サーバ（Server）] ドロップダウン リストから、Cisco Webダイヤラー Web サービスがアクティブになっ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 IP Manager Assistant][Cisco Webダイヤラー Web]サービスを選択します。
パラメータのリストが表示されます。

ステップ 4 [CTIManager Connection Security Flag] パラメータおよび [CAPF Profile Instance ID for Secure Connection to CTIManager] パラメータを選択して更新します。

パラメータの説明を表示するには、パラメータ名のリンクをクリックします。

（注） CTIManager は IPv4 および IPv6 のアドレスをサポートします。

ステップ 5 **[保存]** をクリックします。

ステップ 6 サービスがアクティブになっているサーバごとに、この手順を繰り返します。

次のタスク

Manager Assistant の共有回線のタスク フロー （211 ページ）を参照して、次のタスクを決定、完了します。

Webダイヤラー の言語ロケールの設定

Cisco Webダイヤラー の言語ロケールを設定するには、Cisco Unified Communications セルフ ケア ポータルを使用します。 デフォルトの言語は英語です。

始める前に

Webダイヤラー の有効化 （345 ページ）

手順

ステップ 1 Cisco Unified Communications セルフ ケア ポータルから、[**全般設定（General Settings）**] タブをクリックします。

ステップ 2 [**言語（Language）**] をクリックします。

ステップ 3 [表示言語（**Display Language**）] ドロップダウン リストから、言語ロケールを選択して、[保存（**Save**）] をクリックします。

WebDialer アラームの設定

Cisco Webダイヤラー サービスは、Cisco Tomcat を使用してアラームを生成します。

始める前に

Webダイヤラー の言語ロケールの設定 （352 ページ）

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[アラーム（Alarm）] > [設定（Configuration）]**。

ステップ 2 [サーバ（Server）] ドロップダウン リストから、アラームを設定するサーバを選択し、[移動（Go）] をクリックします。

ステップ 3 [サービス グループ（Services Group）] ドロップダウン リストから、[プラットフォーム サービス（Platform Services）] を選択し、[移動（Go）] をクリックします。

ステップ 4 [サービス（Services）] ドロップダウン リストから、[Cisco Tomcat（Cisco Tomcat）] を選択し、[移動（Go）] をクリックします。

ステップ 5 設定でクラスタがサポートされる場合は、[すべてのノードに適用（Apply to All Nodes）] チェック ボックスをオンにして、クラスタ内の全ノードにアラーム設定を適用します。

ステップ 6 「アラーム設定」の説明に従って設定を行います。この項ではモニタおよびイベント レベルについても説明されています。

（注） アラーム設定の詳細については、『*Cisco Unified Serviceability Guide*』を参照してください。

ステップ 7 **[保存]** をクリックします。

次のタスク

標準 CCM エンド ユーザ グループへのユーザの追加 （354 ページ）。または（任意で）アプリケーションに複数のクラスタが必要な場合は、アプリケーション ダイヤル ルールの設定 （354 ページ）を参照してください。

アプリケーション ダイヤル ルールの設定

始める前に

WebDialer アラームの設定 （353 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）] > [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）]**。

ステップ 2 [名前（Name）]フィールドに、ダイヤル ルールの名前を入力します。

ステップ 3 [説明（Description）]フィールドに、ダイヤル ルールの説明を入力します。

ステップ 4 [開始番号（Number Begins With）]フィールドに、このアプリケーション ダイヤル ルールを適用する電話番号の先頭部分の数字を入力します。

ステップ 5 [桁数（Number of Digits）]フィールドに、このアプリケーション ダイヤル ルールを適用するダイヤル番号の長さを入力します。

ステップ 6 **[削除する合計桁数（Total Digits to be Removed）]** フィールドに、このダイヤル ルールに適用されるダイヤル番号の開始部分から Unified Communications Manager が削除する桁数を入力します。

ステップ 7 [プレフィックス パターン（Prefix With Pattern）]に、アプリケーション ダイヤル ルールに適用する、ダイヤル番号に付加するパターンを入力します。

ステップ 8 [アプリケーション ダイヤル ルールの優先順位（Application Dial Rule Priority）]で、ダイヤル ルールの優先順位を上位、下位、中位から選択します。

ステップ 9 **[保存（Save）]** をクリックします。

標準 CCM エンド ユーザ グループへのユーザの追加

Unified Communications Manager の [ユーザ ディレクトリ（User Directory windows）] ウィンドウの Cisco Webダイヤラー リンクを使用するには、各ユーザを標準の Unified Communications Manager エンド ユーザ グループに追加する必要があります。

手順

ステップ 1 **[ユーザ管理（User Management）] > [ユーザグループ（User Group）]** の順に選択します。

ステップ 2 [ユーザグループの検索/一覧表示（Find and List User Group）] ウィンドウで、[検索（Find）] をクリックします。

ステップ 3 [**Standard CCM End Users**] をクリックします。

ステップ 4 [ユーザグループの設定（User Group Configuration）] ウィンドウで [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 5 [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。 特定のユーザの条件を入力できます。

ステップ 6 ユーザ グループに 1 人以上のユーザを追加するには、次のいずれかの手順を実行します。

- 1 人以上のユーザを追加するには、各ユーザの横にあるチェックボックスをオンにしてから [選択項目の追加（Add Selected）] をクリックします。
- すべてのユーザを追加するには、[すべて選択（Select All）] をクリックして [選択項目の追加（Add Selected）] をクリックします。

ユーザは、[**ユーザグループの設定（User Group Configuration**）] ウィンドウの [グループ（Group）] テーブルの [ユーザ（Users）] に表示されます。

プロキシ ユーザの設定

makeCallProxy HTML over HTTP インターフェイスを使用して、Cisco Webダイヤラー を使用するためのアプリケーションを開発している場合、プロキシユーザを作成します。 makeCallProxy インターフェイスについては、『*Cisco Web*ダイヤラー *API Reference Guide*』の「makeCallProxy」の項を参照してください。

（注） [MakeCallProxy HTTP メソッド（MakeCallProxy HTTP Methods）] は、Webダイヤラー サービスのサービス パラメータです。 このパラメータは、MakeCallProxy API が受け入れる HTTP メソッドを制御します。 HTTP GET は安全でないと見なされます。これは、API に必要なクレデンシャルが HTTP GET 要求にパラメータとして含まれるためです。 これらの HTTP GET パラメータがアプリケーション ログや Web ブラウザの履歴から判明する可能性があります。

サービス パラメータ [MakeCallProxy HTTP メソッド（MakeCallProxy HTTP Methods）] が [セキュア（Secure）] に設定されている場合、HTTP GET による要求は拒否されます。 デフォルトでは [MakeCallProxy HTTP メソッド（MakeCallProxy HTTP Methods）] パラメータは [非セキュア（Insecure）] に設定されており、API は GET メソッドと POST メソッドの両方を受け入れ、後方互換性が維持されます。

始める前に

標準 CCM エンド ユーザ グループへのユーザの追加 （354 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	（任意） Webダイヤラー エンド ユーザの追加 （356 ページ）	新規のユーザの追加。 ユーザが存在する場合は、次のタスクに進むことができます。
ステップ 2	認証プロキシ権限の割り当て （356 ページ）	エンド ユーザに認証プロキシ権限を割り当てます。

Webダイヤラー エンド ユーザの追加

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。**[ユーザ管理（User Management）] > [エンド ユーザ（End User）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [姓（Last Name）] に入力します。

ステップ 4 [パスワード（Password）] に入力し、確認します。

ステップ 5 [暗証番号（PIN）] に入力し、確認します。

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、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。

認証プロキシ権限の割り当て

次の手順を実行して、既存のユーザの認証プロキシ権限を有効にします。

手順

ステップ 1 **[ユーザ管理（User Management）] > [ユーザグループ（User Group）]** の順に選択します。[ユーザグループの検索/一覧表示（Find and List User Group）] ウィンドウが表示されます。

ステップ 2 **[検索(Find)]** をクリックします。

ステップ 3 [標準 EM 認証プロキシ権限（Standard EM Authentication Proxy Rights）] リンクをクリックします。
[ユーザ グループの設定（User Group Configuration）] ウィンドウが表示されます。

ステップ 4 **[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。
[ユーザの検索と一覧表示（Find and List Users）]ウィンドウが表示されます。

ステップ 5 **[検索(Find)]** をクリックします。 特定のユーザの条件を追加することもできます。

ステップ 6 1 人以上のユーザにプロキシ権限を割り当てるには、次のいずれかの手順を実行します。

ステップ 7 単一ユーザを追加するには、ユーザを選択し、[選択項目の追加（Add Selected）] を選択します。

ステップ 8 リストに表示されるすべてのユーザを追加するには、[すべて選択（Select All）] をクリックして [選択項目の追加（Add Selected）] をクリックします。
ユーザは、[ユーザ グループの設定（User Group Configuration）] ウィンドウの [グループ（Group）] テーブルの [ユーザ（Users）] に表示されます。

Webダイヤラー の連携動作

機能	データのやり取り
クライアント識別コード（CMC）	CMC の使用時には、トーンが再生されたら適切なコードを入力する必要があります。入力しないと、IP フォンが切断され、ユーザに対してリオーダー音が再生されます。
強制承認コード（FAC）	FAC の使用時には、トーンが再生されたら適切なコードを入力する必要があります。入力しないと、IP フォンが切断され、ユーザに対してリオーダー音が再生されます。
ApplicationDialRule テーブル	Cisco Webダイヤラー は、最新のダイヤル ルールを追跡および使用するために、ApplicationDialRule データベース テーブルの変更通知を使用します。

機能	データのやり取り
クライアント識別コードと強制承認コード	Web Dialer は、次の方法で CMC と FAC をサポートします。 • ユーザは、WD HTML ページまたは SOAP 要求のダイヤル テキスト ボックスに接続先番号を入力してから、電話機に手動で CMC または FAC を入力できます。 • ユーザは、WD HTML ページまたは SOAP 要求のダイヤル テキスト ボックスに、接続先番号に続けて、FAC または CMC を入力できます。 たとえば、接続先番号が 5555、FAC が 111、CMC が 222 の場合は、5555111#（FAC）、5555222#（CMC）、または 5555111222#（CMC と FAC）をダイヤルすることにより、コールを発信できます。 （注） • Webダイヤラー は、接続先番号の検証を行いません。 電話機が必要な検証を処理します。 • ユーザがコードを入力しない場合、または誤ったコードを入力した場合、コールは失敗します。 • ユーザが特殊文字を含む DN を使って WebApp からコールを発信した場合は、特殊文字を削除するとコールが正常に動作します。 SOAP UI にはこのルールは該当しません。

Webダイヤラー の制約事項

機能	制約事項
電話機	Cisco Webダイヤラー では、Cisco Computer Telephony Integration（CTI）でサポートされる Skinny Client Control Protocol（SCCP）および Session Initiation Protocol（SIP）を実行する電話がサポートされています。 （注） いくつかの古い電話モデルでは、SIP を実行する Cisco Web Dialer がサポートされていません。

Webダイヤラー のトラブルシューティング

認証エラー

問題

Cisco Webダイヤラー には次のメッセージが表示されます。

認証に失敗しました。もう一度入力してください（Authentication failed, please try again）

考えられる原因

ユーザが入力したユーザ ID またはパスワードが正しくありません。

ソリューション

ログイン時に各自の Unified Communications ManagerCisco Unified Communications Manager ユーザ ID とパスワードを使用していることを確認してください。

サービスが一時的に使用できない

問題

Cisco Webダイヤラー には次のメッセージが表示されます。

サービスは一時的に使用できない状態です。あとでもう一度実行してください（Service temporarily unavailable, please try again later）

考えられる原因

同時 CTI セッションの制御制限 3 に達したため、Cisco CallManager サービスが過負荷になりました。

ソリューション

しばらくしてから接続を再試行します。

ディレクトリ サービスがダウンしている

問題

Cisco Webダイヤラー には次のメッセージが表示されます。

サービスは一時的に使用できない状態です。あとでもう一度実行してください: ディレクトリ サービスがダウンしています（Service temporarily unavailable, please try again later: Directory service down）

考えられる原因

Cisco Communications Manager のディレクトリ サービスがダウンしている可能性があります。

ソリューション

しばらくしてから接続を再試行します。

Cisco CTIManager がダウンしている

問題

Cisco Webダイヤラー には次のメッセージが表示されます。

サービスは一時的に使用できない状態です。あとでもう一度実行してください：Cisco CTIManager がダウンしています（Service temporarily unavailable, please try again later: Cisco CTIManager down）

考えられる原因

Cisco Web Dialer に設定されている Cisco CTIManager サービスがダウンしました。

ソリューション

しばらくしてから接続を再試行します。

セッションの期限切れ、再ログイン

問題

Cisco Webダイヤラー には次のメッセージが表示されます。

セッションの期限が切れました。もう一度ログインしてください。

考えられる原因

次のいずれかの場合に、Cisco Web Dialer セッションの期限が切れます。

- Webダイヤラー servlet の設定後
- Cisco Tomcat サービスの再起動時

ソリューション

Unified Communications Manager のユーザ ID とパスワードを使用してログインします。

ユーザがログインしているデバイスがない

問題

Cisco Web Dialer には次のメッセージが表示されます。

ユーザがログインしているデバイスがありません（User Not Logged in on Any Device）

考えられる原因

ユーザが Cisco Webダイヤラー の初期設定ウィンドウで Cisco Extension Mobility の使用を選択していますが、いずれの IP Phone にもログインしていません。

ソリューション

- 電話にログインしてから Cisco Webダイヤラー を使用します。
- [Extension Mobility を使用する（Use Extension Mobility）] オプションを選択する代わりに、ダイアログボックスの Cisco Webダイヤラー 初期設定リストからデバイスを選択します。

デバイス/回線を開くことができない

問題

ユーザがコールを発信しようとすると、Cisco Webダイヤラー には次のメッセージが表示されます。

ユーザがログインしているデバイスがありません（User Not Logged in on Any Device）

考えられる原因

- ユーザが、Unified Communications Manager に登録されていない Cisco Unified IP 電話 を選択しました。 たとえば、アプリケーションを起動する前に、Cisco IP SoftPhone を優先デバイスとして選択しています。
- 新しい電話機があるユーザが、すでに稼働していない古い電話機を選択しています。

ソリューション

Unified Communications Manager に登録され、稼働している電話機を選択します。

転送先に到達できない

問題

Cisco Webダイヤラー の [通話終了（End Call）] ウィンドウに次のメッセージが表示されます。

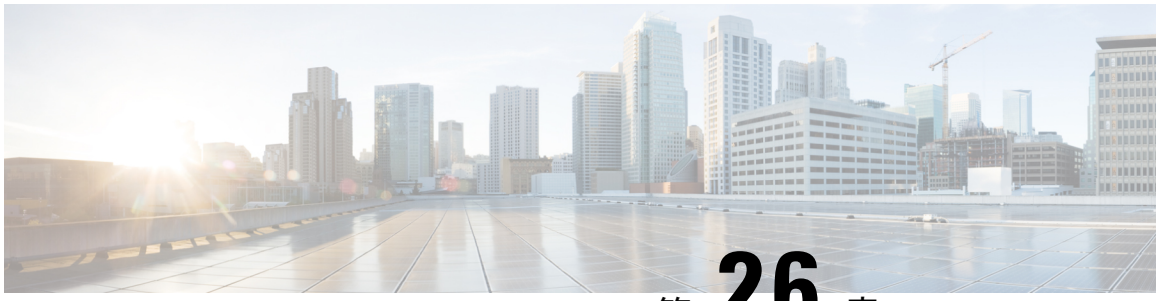
転送先に到達できません。

考えられる原因

- ユーザが間違った番号をダイヤルしました。
- 適切なダイヤル ルールが適用されていません。 たとえば、ユーザが 95550100 ではなく 5550100 をダイヤルしました。

ソリューション

ダイヤル ルールを確認します。



第 26 章

ページング

ページングの概要

Unified Communications Manager は、Cisco Paging Server と連携して、Cisco Unified IP 電話 やさまざまなエンドポイントに Basic Paging サービスを提供するように設定できます。 Cisco Paging Server 製品は、InformaCast 仮想アプライアンスを介して提供され、次の導入オプションを提供します。

InformaCast Basic Paging

InformaCast Basic Paging は、電話機間のライブ オーディオ ポケットベルを個々の Cisco IP 電話または最大 50 台の電話グループに同時に提供します。 InformaCast Basic Paging は、すべての Unified Communications Manager ユーザとすべての Cisco Business Edition 6000 および Cisco Business Edition 7000 ユーザに無料で提供されます。

InformaCast Advanced Notification

InformaCast Advanced Notification は、フル装備の緊急通知と、無制限の Cisco IP 電話 とテキストおよびオーディオ メッセージを使用するさまざまなデバイスやシステムにリーチできるページング ソリューションです。

設定プロセスを合理化するため、Unified Communications Manager には、高度な通知サービスを迅速に設定できるプロビジョニング ウィザードが付属しています。

次のような機能があります。

- Cisco IP 電話 およびその他のエンドポイントへのテキストおよび音声（ライブまたは事前録音）

- アナログおよび IP オーバーヘッド ページング システムの統合
- 911 または緊急通報のモニタリング、アラートまたは録音
- Cisco Jabber の統合
- Cisco Spark の統合
- 自動気象通知
- 動的にトリガーされた緊急電話会議
- 事前に録画またはスケジューリングされたブロードキャスト（始業ベルまたはシフト変更）
- メッセージの確認およびレポートによるイベントのアカウンタビリティ
- コンピュータ デスクトップへの通知（Windows および Mac OS）
- 設備の統合（照明の制御、ドアのロック）
- セキュリティの統合（パニック ボタンまたは脅迫状態ボタン、モーション ディテクタ、火事）

InformaCast Advanced Notification 機能にアクセスするためのライセンス キーを購入します。

InformaCast Mobile

InformaCast Mobile は、iOS または Android で動作するモバイル デバイスにユーザが画像、テキスト、および事前に録音された音声を送信することを可能にするクラウドベース サービスです。 また、このサービスは、InformaCast Advanced Notification と双方向で統合されます。

次のような機能があります。

- iOS または Android で動作するモバイル デバイスを介して InformaCast メッセージを送受信する機能
- InformaCast Advanced Notification との双方向の統合
- メッセージの確認と開封確認
- 無料の通話または SMS メッセージング

InformaCast Mobile は Singlewire Software から直接購入する必要があります。 詳細およびダウンロードについては、Singlewire の Web サイトを参照してください。

すでに InformaCast Advanced Notification と連携するように Unified Communications Manager を設定してある場合は、Unified Communications Manager の追加の設定は不要です。

ページングの前提条件

Cisco Paging Server はマルチキャスト環境で動作するように設計されています。 マルチキャスト用にネットワークを設定する必要があります。

ページングをサポートする Cisco Unified IP 電話 の一覧については、以下のリンクにある Singlewire の『Compatibility Matrix』の「**Cisco Unified IP 電話**」のセクションを参照してください。

http://www.singlewire.com/compatibility-matrix.html.

Basic Paging の Cisco Unified Communications Manager 設定のタスク フロー

次のタスクを実行して、Unified Communications Manager を InformaCast Basic Paging 展開用に Cisco Paging Server と統合するように設定します。

始める前に

- この機能については、以下を参照してください。
  - ページングの概要 （363 ページ）
  - InformaCast Basic Paging （363 ページ）
- ページングの前提条件 （365 ページ）を確認してください。
- このセクションの設定は、Advanced Notification ページングの設定タスク フロー ウィザードを使用する場合に自動化されます。

手順

	コマンドまたはアクション	目的
ステップ 1	SNMP サービスの有効化 （367 ページ）	Unified Communications Manager で SNMP を設定します。
ステップ 2	デフォルト コーデック G.711 の設定 （368 ページ）	デフォルト コーデックを G.711 に設定します。
ステップ 3	ページング用デバイス プールの設定 （369 ページ）	デバイス プールを設定します。
ステップ 4	InformaCast ページングのルート パーティションの設定 （370 ページ）	Basic Paging のルート パーティ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 5	InformaCast ページングのコーリング サーチ スペースの設定 （370 ページ）	Basic Paging のコーリング サーチ スペースを設定します。
ステップ 6	ページングに対応した CTI ポートの設定 （371 ページ）	CTI ポートを設定します。
ステップ 7	AXL アクセスを使うアクセス コントロール グループの設定 （372 ページ）	AXL アクセス コントロール グループを設定します。
ステップ 8	ページングに対応したアプリケーション ユーザの設定 （373 ページ）	アプリケーション ユーザを設定します。
ステップ 9	次のいずれかの手順で、電話機の Web アクセスを有効にします。 • 電話機での Web アクセス有効化 （374 ページ） • 共通の電話プロファイルでの Web アクセスの有効化 （374 ページ） • エンタープライズ電話の Web アクセス有効化設定 （375 ページ）	Web アクセスは、エンタープライズ電話の設定を使用してすべての電話機でグローバルに、または共通の電話プロファイルを使用して電話機のグループに、あるいは個々の電話機で有効にできます。
ステップ 10	認証 URL の設定 （375 ページ）	Unified Communications Manager の認証 URL が InformaCast を指すように設定して、InformaCast が Cisco Unified IP 電話にブロードキャストをプッシュしたときに、その電話が InformaCast で認証されるようにします。

Cisco Unified Communications Manager および Cisco Paging Server の設定手順の詳細については、*InformaCast Virtual Appliance Basic Paging* のインストール/ユーザ ガイドを参照してください。

ページングに対応した SNMP の設定

Basic Paging または Advanced Notification の導入のため、クラスタ。

手順

	コマンドまたはアクション	目的
ステップ 1	SNMP サービスの有効化 （367 ページ）	クラスタで SNMP その他のサービスを有効にします。
ステップ 2	InformaCast SNMP コミュニティ文字列の作成 （367 ページ）	SNMP コミュニティ文字列を設定します。

SNMP サービスの有効化

ページングを設定するには、クラスタの各ノードで SNMP を有効にする必要があります。 さらに、次のサービスを有効にする必要があります。

- Cisco CallManager SNMP サービス：クラスタ内の全ノードで有効にします。
- Cisco CallManager：少なくとも 1 つのノードで有効にします。
- Cisco AXL Web サービス：少なくとも 1 つのノードで有効にします。
- Cisco CTIManager：少なくとも 1 つのノードで有効にします。

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[ツール（Tools）] > [サービス アクティベーション（Service Activation）]** を選択します。

ステップ 2 **[サーバ（Serve）]** ドロップダウン リストから、SNMP を設定するサーバを選択します。

ステップ 3 **[Cisco CallManager SNMPサービス（Cisco CallManager SNMP Service）]**に対応するチェックボックスをオンにします。

ステップ 4 クラスタ内の少なくとも 1 つのサーバで、**[Cisco CallManager]** サービス、**[Cisco CTIManager]** サービス、および **[Cisco AXL Web Service]** サービス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 **[保存]** をクリックします。

ステップ 6 **OK**をクリックします。

ステップ 7 クラスタ内の全ノードに対して、これまでの手順を繰り返します。

InformaCast SNMP コミュニティ文字列の作成

SNMP コミュニティ文字列を設定するため、Basic Paging するには、次の手順を実行します。

始める前に

SNMP サービスの有効化 （367 ページ）

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[SNMP] > [V1/V2c] > [コミュニティ文字列（Community String）]**。

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

ステップ 3 [新規追加] をクリックします。

ステップ 4 [コミュニティ文字列名（Community String Name）]フィールドに、**ICVA** と入力します。

ステップ 5 **[アクセス権限（Access Privileges）]** ドロップダウン リストから、**[読み取り専用（ReadOnly）]** を選択します。

ステップ 6 [すべてのノードに適用（Apply to All Nodes）]チェック ボックスがアクティブな場合、オンにします。

ステップ 7 **[保存]** をクリックします。

ステップ 8 **OK**をクリックします。

次のタスク

デフォルト コーデック G.711 の設定 （368 ページ）

ページングの地域の設定

Basic Paging の場合、ページングの導入には地域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	デフォルト コーデック G.711 の設定 （368 ページ）	その他の地域へのコール用に G.711 コーデックを使用する地域を作成します。
ステップ 2	ページング用デバイス プールの設定 （369 ページ）	ページングのデバイス プールを設定し、そのデバイス プールに対して作成した地域を割り当てます。

デフォルト コーデック G.711 の設定

他の地域へのコールのデフォルト コーデックとして G.711 を使用する InformaCast 地域を作成する必要があります。

始める前に

ページングに対応した SNMP の設定 （366 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。**[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 [新規追加] をクリックします。

ステップ 3 [名前（Name）]フィールドに、**ICVA** と入力します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 [地域（Regions）]テキスト ボックスで、[Ctrl]キーを押しながら選択した地域をすべてクリックすることで、すべての地域を選択します。

ステップ 6 **[最大オーディオ ビットレート（Maximum Audio Bit Rate）]** ドロップダウンリストから、**[64 kbps (G.722, G.711)]** を選択します。

ステップ 7 [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）]列で、[なし（None）]オプション ボタンをクリックします。

ステップ 8 **[保存（Save）]** をクリックします。

ページング用デバイス プールの設定

ページング導入用のデバイス プールを設定するには、この手順を実行します。

始める前に

デフォルト コーデック G.711 の設定 （368 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。**[システム（System）]** > **[デバイス プール（Device Pool）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [**デバイス プール名（Device Pool Name）**] フィールドに、**ICVA** と入力します。

ステップ 4 **[Cisco Unified Communications Manager グループ]** ドロップダウン リストから、InformaCast 仮想アプライアンスが通信する Cisco Unified Communications Manager クラスタを含む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、日/時グループを選択します。 時刻によるダイヤル制限を実行していない限りは、**[CMLocal]** を選択します。

ステップ 6 **[地域（Region）]** ドロップダウン リストから、**[ICVA]** を選択します。

ステップ 7 [**SRST リファレンス（SRST Reference）**] ドロップダウン リストから、[**無効（Disable）**] を選択します。

ステップ 8 **[保存（Save）]** をクリックします。

ページングのパーティションとコーリング サーチ スペースの設定

ページングのパーティションとコーリング サーチ スペース（CSS）を次のように設定するには、次の作業を実行します。

- 基本的なページングの導入では、InformaCast ページング用に単一パーティションと CSS を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	InformaCast ページングのルート パーティションの設定 （370 ページ）	InformaCast ページングのルート パーティションを設定します。
ステップ 2	InformaCast ページングのコーリング サーチ スペースの設定 （370 ページ）	InformaCast ページングのコーリング サーチ スペースを設定します。

InformaCast ページングのルート パーティションの設定

InformaCast ページングのルート パーティションを作成します。

始める前に

ページング用デバイス プールの設定 （369 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）] > [ルート パーティション（Route Partitions）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [名前（Name）] フィールドで、パーティション次の名前と説明を入力します。
`ICVA-CTIOutbound,ICVA-Do not add to any phone CSS`

ステップ 4 **[保存（Save）]** をクリックします。

InformaCast ページングのコーリング サーチ スペースの設定

InformaCastページングのコーリング サーチ スペースを設定するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified CM 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 > コントロールのクラス > コーリングサーチスペース**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [名前（Name）]フィールドに、**`ICVA`** と入力します。

ステップ 4 [利用可能なパーティション（Available Partitions）]リスト ボックスから [選択されたパーティション（Selected Partitions）]リスト ボックスへ、矢印を使用して次のパーティションを移動させます。

- InformaCast ページングに作成したパーティション
- ユーザの内線番号とアナログ ページングの内線番号を含むパーティション

ステップ 5 **[保存（Save）]** をクリックします。

ページングに対応した CTI ポートの設定

ページング導入のためのCTIポートを設定するには、次の手順を実行します。 必要なCTIポートの番号は、導入のタイプとアプリケーションの使用方法によって異なります。

- Basic Paging を導入するには、InformaCast ページング用に少なくとも 2 つの CTI ポートを作成する必要があります。

始める前に

InformaCast ページングのコーリング サーチ スペースの設定 （370 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 [新規追加] 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）]** を選択します。

ステップ 4 [デバイス名（Device Name）]フィールドに、CTI ポートの名前を入力します たとえば、InformaCast ポートの場合には **`ICVA-IC-001`** と入力します。

ステップ 5 [説明（Description）]フィールドに、ポートの説明を入力します。 たとえば、**`InformaCast Recording Port`**for Call Monitoring のように入力します。

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、**[ICVA]** を選択します。

ステップ 7 **[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 **[ICVA]** を選択します。

ステップ 8 **[デバイスのセキュリティ プロファイル（Device Security Profile）]** ドロップダウン リストから、**[Cisco CTI ポート：標準 SCCP 非セキュア プロファイル（Cisco CTI Port - Standard SCCP Non-Secure Profile）]** を選択します。

ステップ 9 **[保存]** をクリックします。

ステップ 10 **OK**をクリックします。

ステップ 11 左の関連付け領域で、[回線 [1] - 新規 DN を追加（Line [1] - Add a new DN）]をクリックします。

ステップ 12 [電話番号（Directory Number）]フィールドに電話番号を入力します。 この電話番号は、ページング コールの作成以外の目的には使用できません。 電話に割り当てるべきではなく、ダイヤルインの範囲内に含めるべきでもありません。

ステップ 13 **[ルートパーティション（Route Partition）]** ドロップダウン リストから、次ののポートを選択します。

- InformaCast には、[ICVA-CTIOutbound]を選択します。

ステップ 14 [**表示（内部発信者ID）（Display（Internal Caller ID）**）]テキスト ボックスに、設定するポートのタイプに応じて **`InformaCast`**と入力します。

ステップ 15 [ASCII表示（内部発信者ID）（ASCII Display（Internal Caller ID）]テキスト ボックスに、設定するポートのタイプに応じて **`InformaCast`**と入力します。

ステップ 16 **[保存]** をクリックします。

ステップ 17 必要な CTI ポートごとに、この手順を繰り返します。

次のタスク

AXL アクセスを使うアクセス コントロール グループの設定

AXL アクセスを含むアクセス コントロール グループを作成するのに 次の手順を実行します。

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）]** > **[ユーザ設定（User Settings）]** > **[アクセス コントロール グループ（Access Control Group）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [名前（Name）]テキスト ボックスに **`ICVA ユーザ グループ`**を入力します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 **[関連リンク（Related Links）]** ドロップダウン リストから、**[検索/一覧表示に戻る（Back to Find/List）]** を選択し、**[移動（Go）]** をクリックします。

ステップ 6 [権限（Roles）]欄で、新しいアクセス コントロール グループに対応する [i]アイコンをクリックします。

ステップ 7 [グループに権限を割り当て（Assign Role to Group）]をクリックします。

ステップ 8 **[検索(Find)]** をクリックします。

ステップ 9 [標準 AXL API アクセス（Standard AXL API Access）]チェックボックスを選択し、[選択したものを追加（Add Selected）]をクリックします。

ステップ 10 **[保存（Save）]** をクリックします。

ページングに対応したアプリケーション ユーザの設定

に対応したアプリケーション ユーザを設定するには、次の手順を実行します。

- Basic Paging の場合は、InformaCast アプリケーション ユーザを設定します。

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。**[ユーザ管理（User Management）]** > **[アプリケーション ユーザ（Application User）]** 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 [**ユーザ ID**（**User ID**）] テキスト ボックスに、アプリケーション ユーザのユーザ ID を入力します。 例：**`ICVA InformaCast`**。

ステップ 4 [Password] および [Confirm Password] フィールドにパスワードを入力します。

ステップ 5 [**使用可能デバイス**（**Available Devices**）] リスト ボックスで、導入のために作成した CTI ポートをクリックし、矢印を使用してデバイスを [**制御デバイス**（**Controlled Devices**）] リスト ボックスに移動します。 たとえば、InformaCast の場合は [ICVA-IC-001]、CallAware の場合は [ICVA-CA-001]を選択します。

ステップ 6 [**アクセス コントロール グループに追加**（**Add to Access Control Group**）] をクリックします。

ステップ 7 **[検索(Find)]** をクリックします。

ステップ 8 以下のチェックボックスをオンにします（他に指示がない限り、すべてのアプリケーション ユーザに対してこれらのアクセス許可を選択します）。

- [ICVA ユーザ グループ（ICVA User Group）]
- [標準 CTI によるすべてのデバイスの制御（Standard CTI Allow Control of All Devices）]
- [標準 CTI による接続時の転送および会議をサポートする電話の制御（Standard CTI Allow Control of Phones supporting Connected Xfer and conf）]
- [標準 CTI によるロールオーバー モードをサポートする電話の制御の許可（Standard CTI Allow Control of Phones supporting Rollover Mode）]
- [標準CTIを有効にする（Standard CTI Enabled）]

ステップ 9 **[選択項目の追加(Add Selected)]** をクリックします。

ステップ 10 **[保存]** をクリックします。

電話機での Web アクセス有効化

Cisco Unified IP 電話 の Web アクセスを有効にするには、Basic Pagingで次の手順を実行します。 また、プロファイルを使用した電話のグループの Web アクセスを有効にするには、共通の電話プロファイルを使用することもできます。 詳細については、共通の電話プロファイルでの Web アクセスの有効化 （374 ページ）を参照してください。

始める前に

ページングに対応したアプリケーション ユーザの設定 （373 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、Web アクセスを有効にする電話を選択します。

ステップ 3 **[製品固有の設定レイアウト（Product Specific Configuration Layout）]** エリアで、**[Web アクセス（Web Access）]** ドロップダウン リストから **[有効化（Enable）]** を選択します。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

認証 URL の設定 （375 ページ）

共通の電話プロファイルでの Web アクセスの有効化

共通の電話プロファイルを使用する Cisco Unified IP Phone のグループに Web アクセスを許可するには、Basic Paging または ので、この手順を実行します。 また、個々の電話機の Web アクセスを有効にすることもできます。 詳細については、電話機での Webアクセス有効化 （374 ページ）を参照してください。

始める前に

ページングに対応したアプリケーション ユーザの設定 （373 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。I **[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）]**。

ステップ 2 [検索（Find）]をクリックして、Web アクセスを有効にする電話機のグループに適用するプロファイルを選択します。

ステップ 3 [製品固有の設定レイアウト（Product Specific Configuration Layout）]エリアで、[Web アクセス（Web Access）]ドロップダウン リストから [有効化（Enable）]を選択します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 [設定を適用（Apply Config）]をクリックして、共通の電話プロファイルを使用する電話機をリセットします。

ステップ 6 **OK**をクリックします。

次のタスク

認証 URL の設定 （375 ページ）

エンタープライズ電話の Web アクセス有効化設定

Unified Communications Manager で次の手順を実行して、共通の電話プロファイルを使用する Cisco Unified IP 電話 のグループについて Web アクセスを有効にします。 また、個々の電話機の Web アクセスを有効にすることもできます。 詳細については、電話機での Web アクセス有効化 （374 ページ）を参照してください。

始める前に

ページングに対応したアプリケーション ユーザの設定 （373 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。**[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configuration）]**。

ステップ 2 **[Webアクセス（Web Access）]** ドロップダウン リストから、**[有効（Enable）]** を選択します。

ステップ 3 **[保存]** をクリックします。

ステップ 4 [設定を適用（Apply Config）]をクリックして、共通の電話プロファイルを使用する電話機をリセットします。

ステップ 5 **OK**をクリックします。

認証 URL の設定

次のタスクを実行して、InformaCast を指す認証 URL を設定して、InformaCast がブロードキャストを Cisco Unified IP Phones にプッシュしたとき、電話が Unified Communications Manager ではなく InformaCast を認証するようにします。

手順

	コマンドまたはアクション	目的
ステップ 1	認証 URL の設定 （376 ページ）	InformaCast を指すように、Unified Communications Manager の認証 URL を設定します。
ステップ 2	電話のリセット （376 ページ）	電話機が新しい設定を使用するように導入中の電話機をリセットします。
ステップ 3	電話のテスト （377 ページ）	導入中の電話機が新しい認証 URL の設定を使用することを確認します。

認証 URL の設定

次の手順を実行して、Unified Communications Manager の認証 URL が InformaCast 仮想アプライアンスを指すように設定します。

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）] > [エンタープライズ パラメータ（Enterprise parameters）]**。

ステップ 2 **[電話 URL パラメータ（Phone URL Parameters）]** エリアにスクロールし、**[URL 認証（URL Authentication）]** フィールドに **`http://<IP Address>:8081/InformaCast/phone/auth`** と入力します。ここで <IP Address> は InformaCast 仮想アプライアンスの IP アドレスです。

（注） [URL 認証（URL Authentication）]フィールドの既存の URL をメモします。InformaCast の設定時に必要になる場合があります。 詳細については InformaCast のマニュアルを参照してください。

ステップ 3 **[保護電話 URL パラメータ（Secured Phone URL Parameters）]** エリアにスクロールし、**[保護認証 URL（Secured Authentication URL）]** フィールドに **`http://<IP Address>:8081/InformaCast/phone/auth`** と入力します。ここで <IP Address> は InformaCast 仮想アプライアンスの IP アドレスです。

ステップ 4 **[保存（Save）]** をクリックします。

電話のリセット

InformaCast 仮想アプライアンスをポイントするように認証 URL を設定した後、電話をリセットする必要があります。 この手順では、デバイス プールの電話を手動でリセットする方法について説明します。 電話をリセットする多くの方法があります。 たとえば、一括管理ツールを使用して、業務時間外にリセットを実施するようスケジュール設定できます。 一括管理ツー

ルの詳細については、『*Cisco Unified Communications Manager Bulk Administration Guide*』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。**[デバイス] > [電話]**

ステップ 2 [電話の場所（From Phone Where）]ボックスで、[デバイス プール（Device Pool）]を選択します。

ステップ 3 他のドロップダウン メニューとフィールド項目を、使用中の電話を含むデバイス プールを立ち上げる設定にします。

ステップ 4 **[検索(Find)]** をクリックします。

ステップ 5 リセットするデバイス プールを選択します。

ステップ 6 [選択したアイテムのリセット（Reset Selected）] をクリックします。

ステップ 7 [**リセット（Reset**）] をクリックします。

電話のテスト

電話機が InformaCast 仮想アプライアンスで認証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。**[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 [電話の検索と一覧表示（Find and List Phones）] ウィンドウのドロップダウン メニューとフィールドを使用して、新しい認証 URL を使用する必要のある電話機の検索をフィルタリングし、**[検索（Find）]** をクリックします。

ステップ 3 新しい設定を使用する必要がある電話機に関して、[IPv4 アドレス（IPv4 Address）]列の [IP アドレス（IP Address）] リンクをクリックします。

ステップ 4 [ネットワーク構成（Network Configuration）] をクリックします。
[ネットワーク構成（Network Configuration）] ページが表示されます。

ステップ 5 [認証 URL（Authentication URL）]フィールドに、[URL 認証（URL Authentication）]エンタープライズ パラメータに関して入力した InformaCast 仮想アプライアンスの IP アドレスが表示されていることを確認します。 正しい URL が表示されない場合は、認証 URL を設定する必要があります。

Advanced Notification ページングの設定タスク フロー

次のタスクを実行して、InformaCast Paging Server を Unified Communications Manager と統合し、IP ページングおよび緊急コール アラートを行います。 このツールには次の機能があります。

- InformaCast Advanced Notification
- パニックボタンの設定
- ユーザが緊急サービス番号をダイヤルしたときのIP Phoneへのテキストおよび音声通知（CallAware）

手順

	コマンドまたはアクション	目的
ステップ 1	InformaCast 仮想アプライアンスのインストール （378 ページ）.	Singlewire Web サイトから InformaCast OVA ファイルをダウンロードし、vSphere にアップロードします。
ステップ 2	InformaCast への接続の設定 （380 ページ）.	Unified Communications Manager と InformaCast を設定します。
ステップ 3	パニック ボタンの設定 （382 ページ）.	パニック ボタンを設定して、IP 電話にテキストおよび音声通知を送信します。
ステップ 4	CallAware 緊急通報アラートの設定 （384 ページ）.	緊急通報のテキストと音声の通知を設定します。

InformaCast 仮想アプライアンスのインストール

Singlewire は、VMware ESXi プラットフォーム上の InformaCast Virtual Appliance をサポートします。このプラットフォームは、vSphere クライアントを介して管理されます。

（注） Singlewireでサポートされている VMware ESXiのバージョンのリストを表示するには、次のURLにアクセスしてください。https://www.singlewire.com/compatibility-matrix[InformaCastプラットフォーム]セクションの[サーバプラットフォーム]リンクをクリックしてください。

（注） ライセンスを購入した場合は、https://www.singlewire.com/icva-kb-activateを参照してください。ライセンスを有効にします。 これにより、90 日間のトライアル後に緊急通知が有効になるようになります。

（注） InformaCast の画面キャプチャを含むインストールの詳細については、次の URL を参照してください：https://www.singlewire.com/icva-kb-install。

始める前に

vSphere Client を使用して InformaCast Virtual Appliance をインポートします。 これは、VMware サーバからダウンロードできます。

手順

ステップ 1 シングルワイヤー Webサイトから**OVA**ファイルをダウンロードしてから、vSphereクライアントにログインします。

（注） Communications Manager Business Edition 6000 で InformaCast を使用している場合は、OVA を含むパッケージ（物理メディア）で DVD が提供されます。

[vSphere Client]ウィンドウが表示されます。

ステップ 2 **[vSphere クライアント（vSphere Client）]**ウィンドウから、**[ファイル（File）]** > **[OVF テンプレートの展開（Deploy OVF Template）]**を選択します。
[OVF テンプレートの展開（Deploy OVF Template）] ダイアログボックスが表示されます。

ステップ 3 **[ファイルから展開]**ラジオボタンをクリックし、**[参照]**をクリックして、保存したOVAファイル（または付属のDVDのOVAファイル）を選択します。 OVA ファイルを選択したら、**開く**をクリックします。
ソースの場所は**[OVF テンプレートの展開（Deploy OVF Template）]**ダイアログボックスで選択されています。

ステップ 4 [次へ(Next)]をクリックして続行します。
[OVF テンプレートの展開（Deploy OVF Template）]ダイアログボックスが更新され、**[OVFテンプレートの詳細（OVF Template Details）]**が表示されます。

ステップ 5 **[次へ]**をクリックして**名前と場所**を確認し、**[次へ]**をクリックして新しい仮想マシンファイルを保存するネットワークを選択します。

ヒント 仮想アプライアンスを Cisco Unified Communications Managerと同じVLANに配置することをお勧めします。

ステップ 6 **[次へ]**をクリックして続行し、**[完了]**をクリックします。
InformaCast バーチャルアプライアンスがインポートを開始します。

ステップ 7 **[vSphere クライアント（vSphere Client）]**ウィンドウで、**[ホストとクラスタ（Hosts and Clusters）]**アイコンをクリックしてからホストサーバーを選択します。
[vSphere クライアント（vSphere Client）] ウィンドウが更新されます。

ステップ 8 **[構成]** タブをクリックして、**[ソフトウェア]** セクションの **[仮想マシンの起動/シャットダウン]** リンクを選択します。

ステップ 9 **[プロパティ]**リンクをクリックします。
仮想マシンの起動とシャットダウンダイアログボックスが表示されます。

ステップ 10 **[システム設定]** の下にある [システム] チェックボックスで、**[仮想マシンの起動と停止を自動的に許可する]** をオンにします。

ステップ 11 **[スタートアップ注文（Startup Order）]**の下で、**[手動スタートアップ（Manual Startup）]** セクションまでスクロールして仮想マシン（デフォルトではSinglewire InformaCast VM）を選択し、**[上に移動（Move Up）]** ボタンを使用して **[手動スタートアップ（Manual Startup）]** セクションから **[自動スタートアップ（Automatic Startup）]** セクションに移動します。 移動後、**OK**をクリックします。
InformaCast 仮想アプライアンスは、ホストされているサーバで自動的に起動および停止します。 これで、InformaCast の仮想マシンをオンにし、ネットワーク構成を設定できます。

ステップ 12 **インベントリ** > **VMsとテンプレート** > **表示**を選択してから、仮想マシンを選択します。

ステップ 13 **イベントリ** > **仮想マシン** > **オープンコンソール**を選択してください
Singlewire InformaCast VM コンソールウィンドウが表示されます。

ステップ 14 InformaCast の設定がはじめて開始されます。 この設定中、InformaCast バーチャルアプライアンスで次のタスクを実行します。

a) シスコのエンドユーザ使用許諾契約書（EULA）に同意する
b) シングルワイヤEULAに同意する
c) ホスト名の設定
d) IPアドレス、サブネットマスク、デフォルトゲートウェイを設定する
e) DNS サーバの IP アドレスとドメイン名を設定する
f) NTP サーバ（IP アドレスまたはホスト名）を設定する
g) タイム ゾーンを設定する
h) SSL（Secure Socket Layer）証明書のパラメータを設定する
i) SSL サブジェクトの代替名を設定する（オプション）
j) OS 管理者パスワードを設定する
k) InformaCast と PTT（PushToTalk）管理者パスワードを設定します。 このパスワードは、Cisco Unified CMの管理の**高度な機能** > **緊急通知ページング**でCisco Unified Communications ManagerとInformaCastを接続するために必要です。
l) バックアップと通信のセキュリティパスフレーズを設定する

設定が成功すると、「Singlewire InformaCast へようこそ」メッセージが表示されます。

ステップ 15 **続ける**をクリックして、Singlewire InformaCast と連携する。

InformaCast への接続の設定

この手順を使用して、Unified Communications Manager Tomcat 信頼ストアに InformaCast 証明書をロードします。

（注） InformaCast サーバーが、Unified CM で設定された最小 TLS バージョンをサポートしていることを確認してください。

始める前に

InformaCast 仮想アプライアンスのインストール （378 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。**[高度な機能（Advanced Features）]** > **[緊急通知ページング（Emergency Notifications Paging）]**。

ステップ 2 [InformaCast緊急通知の入門（Introduction to InformaCast Emergency Notifications）]ページで、[次へ（Next）]をクリックして続行します。
[InformaCast仮想アプライアンスのインストール（Installing the InformaCast Virtual Appliance）] ページが表示されます。

ステップ 3 [InformaCast仮想アプライアンスのインストール（Installing the InformaCast Virtual Appliance）] ページで、[次へ（Next）]をクリックして続行します。

（注） Unified Communications Manager を使用して設定するには、InformaCast 仮想アプライアンスを正常にインストールしておく必要があります。

[Cisco Unified Communications Manager と InformaCastの接続（Connecting Cisco Unified Cummunications Manager and InformaCast）] ページが表示されます。

ステップ 4 [InformaCast VMのIPアドレス（IP address of InformaCast VM）]フィールドに、IP アドレスまたはホスト名を入力します。

（注） デフォルトでは、ユーザ名は **[InformaCastで使用するユーザ名（Username to use in InformaCast）]** に `admin` として記載されており、編集することはできません。

ステップ 5 [管理アプリケーションユーザのパスワード（Password for admin app user）]フィールドに、InformaCast アプリケーションの管理者パスワードを入力します。
InformaCast 証明書のサムプリントを表示したダイアログボックスが表示されます。

ステップ 6 **[OK]** をクリックして、Unified Communications Manager Tomcat 信頼ストアに InformaCast 証明書をロードします。
設定プロセスが開始します。

（注） 設定が成功すると、[ステータス（Status）]フィールドに完了ステータスが表示されます。

ステップ 7 [次へ（Next）]をクリックします。
ウィザードは次のタスクを実行します。

- SNMP サービスのアクティブ化
- ローカルで生成されたランダム クレデンシャルを使用した SNMP サービスの設定
- CTI マネージャ サービスのアクティブ化
- InformaCast のための Unified Communications Manager の設定
  - 新しい領域の作成（1 クラスタあたり 1 つ）
  - 新しいデバイス プールの作成（1 クラスタあたり 1 つ）
  - SIP トランクの作成（1 クラスタあたり 1 つ）
  - ルート グループの作成（1 クラスタあたり 1 つ）
  - ルート リストの作成
  - ロールの作成
  - アプリケーション ユーザの作成
- InformaCast の設定 Unified Communications Manager
  - クラスタの作成
  - 受信者グループの更新
  - SIP アクセスを拒否に設定
  - SIP アクセスの作成

パニック ボタンの設定

この手順を使用してパニック ボタンを設定し、IP 電話にテキストおよび音声通知を送信します。 これにより、緊急時にワンクリック アラームを開始することができます。

始める前に

InformaCast への接続の設定 （380 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。**[高度な機能（Advanced Features）] > [緊急通知ページング（Emergency Notifications Paging）]**。

ステップ 2 [InformaCast緊急通知の入門（Introduction to InformaCast Emergency Notifications）]ページで、[次へ（Next）]をクリックして続行します。

ステップ 3 [InformaCast仮想アプライアンスのインストール（Installing the InformaCast Virtual Appliance）]ページで、[次へ（Next）]をクリックして続行します。

ステップ 4 **[Cisco Unified Communications ManagerとInformaCast の接続（Connecting Cisco Unified Communications Manager and InformaCast）]** ページで、**[次へ（Next）]** をクリックして続行します。
[パニックボタンの設定（Configuring a Panic Button）]ページが表示されます。

ステップ 5 [名前で事前録音されたメッセージを選択（Choose pre-recorded message by name）]ドロップダウンリストから、緊急時に Cisco Unified IP 電話 およびさまざまなデバイスとシステムに表示される事前録音済みメッセージを選択します。

（注） InformaCast の管理で、必要に応じて事前に録音されたメッセージを変更できます。

ステップ 6 [パニックボタンをトリガーするDNの入力（Enter DN to trigger the panic button）]フィールドに、0 ～ 9 の数字、アスタリスク（*） およびシャープ記号（#）を含む電話番号（DN）を入力します。 デフォルト値は ***5 です。

ステップ 7 **[ルート パーティション（Route Partition）]** ドロップダウン リストから、ルート パターンへのアクセスを制限するパーティションを選択します。

（注） ルートパターン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 8 [通知を送信する電話機を選択（Choose Phones to Send Notification）]ボタンをクリックします。
[通知を送信する電話機（Phones to Send Notification）]ダイアログボックスが表示されます。

ステップ 9 [通知を送信する電話機（Phones to Send Notification）]ダイアログボックスで、事前に録音されたメッセージを送信する Cisco Unified IP 電話 を選択します。 ユーザが入力したダイヤル パターン（たとえば、***5）は、選択した電話に短縮ダイヤルとして設定されます。
選択した Cisco Unified IP 電話 は、**[通知の送信に選択された電話機（Selected Phones to Send Notification）]** リスト ボックスに表示されます。

ステップ 10 **[ルールの追加（Add Rules）]** をクリックして、選択した Cisco Unified IP 電話 が通知を受信するための新しいルールを作成します。

a) ドロップダウン リストから、いずれかのパラメータを選択します。 使用可能なオプションは、[デバイスプール（Device Pool）]、[説明（Description）]および[電話番号（Directory Number）] です。
b) 2 番目のドロップダウン リストで、次のオプションの中から条件を選択します。
   - 次をする（Does）
   - 次をしない（Does not）
c) 3 番目のドロップダウン リストで、次のオプションの中から条件を選択します。
   - 次で始まる
   - 次で終わる
   - 含む

d) テキスト ボックスに、検索条件を入力します。

（注） 少なくとも 1 つの新しいルール、最大で 5 つの新しいルールを作成できます。 5 つのルールが作成されると、[ルールの追加（Add Rules）]ボタンが無効になります。

（注） ルールを削除するには、**[ルールの削除（Delete Rules）]** をクリックします。

e) 作成したルールを検証するには、[ルールのテスト（Test Rules）]をクリックします。 テストルールが複数の電話機で完了すると、**[次へ（Next）]**ボタンが有効になります。

（注） このルールに一致し、Cisco Unified Communications Manager に後で追加された電話機は、このグループへの通知の受信者として含まれます。

ステップ 11 [次へ（Next）]をクリックします。

ウィザードは次のタスクを実行します。

- 選択された電話機に、入力された DN の短縮ダイヤルを追加します。 選択された電話機に既存の電話ボタンテンプレートに割り当てられている未使用の短縮ダイヤルがある場合、この短縮ダイヤルは選択された電話機に直接表示されます。 選択された電話機に未使用の短縮ダイヤル ボタンがない場合は、パニック ボタン短縮ダイヤルが作成されますが、電話機には表示されません。
- 作成されたルート リストを使用して、選択されたパーティションに入力された DN のルート パターンを追加します。
- 選択されたルールに一致する電話機に選択されたメッセージを送信するために、入力された DN の InformaCast DialCast エントリを作成します。

CallAware 緊急通報アラートの設定

この手順を使用して、CallAware 緊急通報アラートの詳細を設定します。 これにより、緊急電話番号がダイヤルされたときに、テキストと音声の通知が IP フォンに送信されます。 また、911 以外の番号へのコールを検出することもできます。

始める前に

パニック ボタンの設定 （382 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。**[高度な機能（Advanced Features）]** > **[緊急通知ページング（Emergency Notifications Paging）]**。

ステップ 2 [InformaCast緊急通知の入門（Introduction to InformaCast Emergency Notifications）]ページで、[次へ（Next）]をクリックして続行します。

ステップ 3 [InformaCast仮想アプライアンスのインストール（Installing the InformaCast Virtual Appliance）]ページで、[次へ（Next）]をクリックして続行します。

ステップ 4 **[Cisco Unified Communications ManagerとInformaCast の接続（Connecting Cisco Unified Communications Manager and InformaCast）]** ページで、**[次へ（Next）]** をクリックして続行します。

ステップ 5 [パニックボタンの設定（Configuring a Panic Button）]ページで、[次へ（Next）]をクリックして続行します。
[CallAware緊急通報アラートの設定（Configuring CallAware Emergency Call Alerting）]ページが表示されます。

ステップ 6 [名前で事前録音されたメッセージを選択（Choose pre-recorded message by name）]ドロップダウンリストから、緊急時に Cisco Unified IP 電話 およびさまざまなデバイスとシステムに表示される事前録音済みメッセージを選択します。

（注） InformaCast の管理で、必要に応じて事前に録音されたメッセージを変更できます。

ステップ 7 [緊急ルートパターンの選択（Choose Emergency Route Patterns）]ボタンをクリックします。
[ルートパターン（Route Patterns）]ダイアログボックスが表示されます。

ステップ 8 [ルートパターン（Route Patterns）]ダイアログボックスで、目的のパターンの横にあるボックスをオンにすることによってルート パターンを選択します。

a) [選択/変更の保存（Save Selected/Changes）]ボタンをクリックします。

選択したルート パターンが [選択されたルートパターン（Selected Route Patterns）]リスト ボックスに表示されます。

ステップ 9 **[ルールの追加（Add Rules）]** をクリックして、選択した Cisco Unified IP 電話 が通知を受信するための新しいルールを作成します。

a) ドロップダウン リストから、いずれかのパラメータを選択します。 使用可能なオプションは、[デバイスプール（Device Pool）]、[説明（Description）] および [電話番号（Directory Number）] です。

b) 2 番目のドロップダウン リストで、次のオプションの中から条件を選択します。

- 次をする（Does）
- 次をしない（Does not）

c) 3 番目のドロップダウン リストで、次のオプションの中から条件を選択します。

- 次で始まる
- 次で終わる
- 含む

d) テキスト ボックスに、検索条件を入力します。

（注） 少なくとも 1 つの新しいルール、最大で 5 つの新しいルールを作成できます。 5 つのルールが作成されると、[ルールの追加（Add Rules）]ボタンが無効になります。

（注） ルールを削除するには、**[ルールの削除（Delete Rules）]** をクリックします。

e) 作成したルールを検証するには、[ルールのテスト（Test Rules）]をクリックします。 1 つ以上の電話でルールの検証が完了すると、[完了（Finish）]ボタンが有効になります。

（注） このルールに一致し、Unified Communications Manager に後で追加された電話機は、このグループへの通知の受信者に含まれます。

ステップ 10 [終了（Finish）]をクリックします。

ウィザードは次のタスクを実行します。

- InformaCast 用の外部コール制御プロファイルを追加します
- 選択されたルート パターンごとに、外部コール制御プロファイルを参照するようにそのルート パターンを変更します
- 通知を受信する電話機と一致するルールを持つ受信者グループを作成します
- 選択されたメッセージと受信者グループを含む InformaCast ルーティング要求を作成します

[概要（Summary）] ページが表示されるので、InformaCast が Unified Communications Manager を使用して正しく設定されていることを確認します。 詳細は、次を参照してください。 https://www.singlewire.com

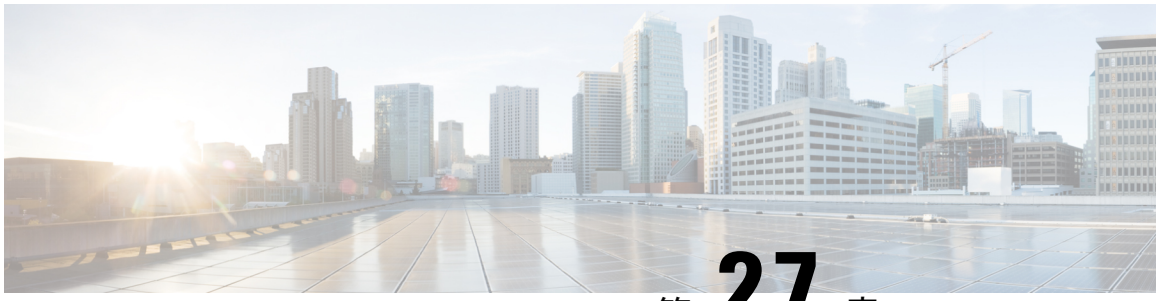
ページングの連携動作

- Advanced Notification ページングの連携動作 （387 ページ）

Advanced Notification ページングの連携動作

表 *27 : Advanced Notification* ページングの連携動作

機能	データのやり取り
緊急通知ページング	緊急通知ページング ウィザードは、InformaCast リリース 11.5(1)SU3 以降のバージョンを使用して基本ページング モードでのみ設定できます。 緊急通知ページング ウィザードでのみ数字を含むパターンをルーティングするようにコール モニタリングを設定できます。 ワイルドカード文字を含むルート パターンの場合は、InformaCast で設定します。



第 27 章

インターコム

インターコムの概要

インターコムは、従来の回線と短縮ダイヤルの機能を組み合わせた電話回線タイプです。インターコム回線を使用すると、ユーザは別のユーザのインターコム回線にコールできます。この別のユーザは、片通話ウィスパーに自動で応答します。 受信者は、ウィスパー コールを認識し、双方向インターコムコールを開始します。

インターコム回線を使用して、インターコム パーティション内の任意のインターコム回線をダイヤルできます。あるいはインターコム パーティション外部のインターコム回線をターゲットとするように回線を事前設定できます。

インターコムにより、ユーザは事前に定義したターゲットへコールを発信できます。 着信側は、ミュートがオンになっているスピーカーフォン モードで自動的にこのコールに応答します。 これにより、開始者と宛先の間に一方向音声パスがセットアップされます。したがって着信側がビジーまたはアイドルであるかに関係なく、開始者が短いメッセージを送信できます。

インターコム コールに対して自動応答する場合、着信側の音声が発信者に戻されないようにするため、Unified Communications Manager にはウィスパー インターコムが実装されています。ウィスパー インターコムにより、発信側から着信側への片通話だけが行われます。 着信側から発信者へ通話するには、着信側が手動でキーを押す必要があります。

自動応答トーンは、送信側と受信側の両方でウィスパーインターコム状態が開始することを通知します。

インターコムとデフォルト デバイス

インターコム回線ごとにデフォルト デバイスが必要です。 インターコム回線は、指定されたデフォルト デバイスにしか表示されません。

管理者がインターコム回線をデバイスに割り当てると、まだ設定されていなければ、システムがそのデバイスをインターコム回線用のデフォルト デバイスとして設定します。 管理者は、インターコム回線用のデフォルト デバイスを変更できます。 管理者がデフォルト デバイスを別のデバイスに変更すると、インターコム回線が元のデバイスに割り当てられていても、そのデバイスから削除されます。

インターコム回線は、デバイス プロファイルに割り当てることができます。 ユーザがデバイス プロファイルを使用してインターコム回線のデフォルト デバイスと一致するデフォルト デバイスにログインしている場合にだけ、インターコム回線が使用可能になります。 そうでない場合は、ユーザのログイン時にインターコム回線が表示されません。

インターコムの前提条件

インターコム機能には次のシステム要件があります。

- Cisco Unified IP 電話ファームウェア リリース 8.3（1）以降

インターコムの設定タスク フロー

始める前に

- インターコムの前提条件 （390 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	インターコム パーティションの設定 （391 ページ）	新しいインターコムのパーティションを追加するか、既存のパーティションを設定します。
ステップ 2	インターコム コーリング サーチ スペースの設定 （392 ページ）	新しいインターコムのコーリング サーチ スペースを追加します。
ステップ 3	インターコム トランスレーション パターンの設定 （392 ページ）	新しいインターコムのトランスレーション パターンを追加するか、既存のインターコムのトランスレーション パターンを設定します。

	コマンドまたはアクション	目的
ステップ 4	インターコム電話番号の設定（393 ページ）	インターコムの電話番号を追加または更新します。
ステップ 5	インターコム回線と短縮ダイヤルの設定（394 ページ）	インターコム回線と短縮ダイヤルを設定します。

インターコム パーティションの設定

始める前に

電話モデルが特定のリリースおよびデバイス パックのインターコム機能をサポートすることを確認します。電話機能一覧の生成 （5 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** > **インターコム** > **インターコムルートパーティション**。

インターコム パーティションの検索と一覧表示（Find and List Intercom Partitions）] ウィンドウが表示されます。

ステップ 2 [新規追加] をクリックします。

[**新規インターコム パーティションの追加（Add New Intercom Partition**）] ウィンドウが表示されます。

ステップ 3 [**インターコム パーティション情報（Intercom Partition Information**）] セクションの [**名前（Name**）] ボックスに、追加するインターコム パーティションの名前と説明を入力します。

（注） 複数のパーティションを入力するには、各パーティション エントリごとに 1 行を使います。 最大 75 のパーティションを入力できます。名前と説明には合計 1475 文字を使用できます。 パーティション名は、50 文字以内です。 各行のパーティション名と説明を区別するには、カンマ（,）を使用します。 説明が入力されなかった場合、Unified Communications Manager はパーティション名を説明として使用します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 設定するパーティションを探します。
[インターコムパーティションの設定（Intercom Partition Configuration）] ウィンドウが表示されます。

ステップ 6 [インターコム パーティションの設定（Intercom Partition Configuration）] フィールド エリア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]** をクリックします。

[インターコム パーティションの設定（Intercom Partition Configuration）] ウィンドウが表示されます。

ステップ 8 適切な設定値を入力します。 [インターコム パーティションの設定（Intercom Partition Configuration）] パラメータの詳細については、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。

ステップ 10 **[設定の適用（Apply Config）]** をクリックします。

インターコム コーリング サーチ スペースの設定

始める前に

インターコム パーティションの設定 （391 ページ）

手順

ステップ 1 メニュー バーで、**[コール ルーティング（Call Routing）]** > **[インターコム（Intercom）]** > **[インターコム コーリング サーチ スペース（Intercom Calling Search Space）]** 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 [インターコム コーリング サーチ スペース（Intercom Calling Search Space）] フィールド領域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、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。

インターコム トランスレーション パターンの設定

始める前に

インターコム コーリング サーチ スペースの設定 （392 ページ）

手順

ステップ 1 **[コール ルーティング（Call Routing）]** > **[インターコム（Intercom）]** > **[インターコム トランスレーション パターン（Intercom Translation Pattern）]** を選択します。

[インターコム トランスレーション パターンの検索/一覧表示（Find and List Intercom Translation Patterns）] ウィンドウが表示されます。

ステップ 2 次のいずれかのタスクを実行します。

a) 既存のインターコム トランスレーション パターンをコピーするには、設定するパーティションを探し、コピーするインターコム トランスレーション パターンの横にある [**コピー（Copy**）] ボタンをクリックします。
b) 新しいインターコム 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**）] ボタンをクリックします。

ステップ 3 [インターコム トランスレーション パターンの設定（Intercom Translation Pattern Configuration）] フィールド領域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、オンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

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インターコム トランスレーション パターンが一意であることを確認します。重複入力を示すエラーを受け取ったら、ルート パターンまたはハント 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ます。

[**インターコム トランスレーション パターンの設定（Intercom Translation Pattern Configuration**）] ウィンドウに、新しく設定したインターコム トランスレーション パターンが表示されます。

インターコム電話番号の設定

インターコム電話番号には、パターン（352XX など）を割り当てることができます。インターコム電話番号にパターンを割り当てる場合は、ユーザの混乱を避けるために、インターコム DN の設定フィールド（[回線テキスト ラベル（Line Text Label）]、[ディスプレイ（内部発信者 ID）（Display (Internal Caller ID)）]、[外部電話番号マスク（External Phone Number Mask）]）にテキストまたは数字を追加します。 これらのフィールドは、インターコム電話番号を追加し、そのインターコム電話番号と電話を関連付けた場合にのみ、そのインターコム電話番号に対して表示されます。

たとえば、ユーザ名を回線テキスト ラベルおよび内部発信者 ID に追加し、外部回線番号を外線番号マスクに追加した場合、コール情報の表示時には、352XX ではなく、John Chan と表示されます。

手順

ステップ 1 **[コール ルーティング（Call Routing**）] > **[インターコム（Intercom**）] > **[インターコム電話番号（Intercom Directory Number**）]** を選択します。

[インターコム電話番号の検索と一覧表示（Find and List Intercom Directory Numbers）]ウィンドウが表示されます。

ステップ 2 特定のインターコム電話番号を検索するには、検索条件を入力して [検索（Find）]をクリックします。
検索基準に一致するインターコム電話番号の一覧が表示されます。

ステップ 3 次のいずれかのタスクを実行します。

a) インターコム 電話番号を追加するには、**[新規追加]** をクリックします。

b) インターコム電話番号を更新するには、更新するインターコム電話番号をクリックします。

[インターコム電話番号の設定（Intercom Directory Number Configuration）]ウィンドウが表示されます。

ステップ 4 [インターコム電話番号の設定（Intercom Directory Number Configuration）] フィールド領域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、オンライン ヘルプを参照してください。

ステップ 5 **[保存]** 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 **[電話のリセット（Reset Phone）]** をクリックします。

ステップ 8 デバイスを再起動します。

再起動中に、ゲートウェイのコールがドロップされることがあります。

インターコム回線と短縮ダイヤルの設定

始める前に

インターコム電話番号の設定 （393 ページ）

手順

ステップ 1 **[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）]** を選択し、インターコム回線を既存の電話ボタン テンプレートに追加するか、または新しいテンプレートを作成します。

（注） インターコム回線はプライマリ回線としては設定できません。

ステップ 2 [ボタン情報（Button Information）]エリアの [機能（Feature）]ドロップダウン リストから [インターコム（Intercom）]を選択します。

ステップ 3 [ボタン情報（Button Information）]エリアの [機能（Feature）]ドロップダウン リストから [短縮ダイヤル（Speed Dial）]を選択します。

（注） 定義済みの接続先（短縮ダイヤル）を指定してインターコム回線を設定して、高速アクセスを許可できます。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 **[設定の適用（Apply Config）]** をクリックします。

インターコムの連携動作

機能	データのやり取り
一括管理ツール	Unified Communications Manager 管理者は一括管理ツールを使用して、多数のインターコム ユーザを個別に追加する代わりに一度に追加できます。 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。
割込み	インターコム接続先が割り込み対象の場合でも、Cisco Unified IP 電話はウィスパー インターコムをサポートできます。 接続先発信者がインターコム ボタンを押してインターコム発信者との通話を選択すると、元のコールは保留状態になり、割り込み発信側が解放されます。
サイレント（DND）	インターコム コールは接続先の電話機でサイレントよりも優先されます。
通話保持	通話が保持されると、エンドユーザが通話を切断してからでないと、Unified Communications Manager に電話機を再登録できません。 インターコム コールがウィスパー モードの場合、一方向のメディアを表し、終端側にはユーザがまったくいない可能性があります。したがって、応答モードのインターコム コールのみが保持されます（ウィスパー インターコムは保持されません）。
Cisco Unified Survivable Remote Site Telephony（SRST）	Cisco Unified IP 電話 が SRST で登録される場合、電話機はインターコム回線を登録しません。したがって、電話機が SRST で登録されてもこの機能は使用できません。
Cisco Unified Communications Manager Assistant	Cisco Unified Communications Manager Assistant 構成ウィザードを使用すると、**Cisco Unified Communications Manager Assistant** の設定にかかる時間を短縮し、エラーを除去できます。 管理者が構成ウィザードを正常に実行して完了すると、パーティション、コーリング サーチ スペース、ルート ポイント、およびトランスレーション パターンが自動的に作成されます。

機能	データのやり取り
[CTI]	CTI/JTAPI/TSP を使用して、インターコム回線向けに事前設定されたターゲットの電話番号を設定または変更できます。 ターゲットの電話番号が Cisco Unified Communications Manager Administration を通じて更新または再設定された場合、通知を受信します。 インターコム回線がアプリケーションによって制御されるように設定しない場合、CTI/JTAPI/TSP は後方互換であることに注意してください。 インターコム回線がアプリケーション ユーザ リスト内で設定されている場合、変更を行い、互換性をテストする必要がある場合があります。
Cisco Extension Mobility	インターコム機能は Cisco Extension Mobility と連携します。 ユーザがログインに使用するデバイス プロファイルにプロビジョニングされたインターコム回線が含まれる場合、Cisco Extension Mobility を使用して機能をサポートする電話機にログインするユーザに対して、システムはインターコム回線を提供します。 電話機はそのインターコム回線のデフォルトのデバイスである必要があります。
Internet Protocol Version 6（IPv6）	インターコムは、IP アドレッシング モードが IPv4 のみまたは IPv4 および IPv6 の電話機をサポートします。 インターコム コールの際、応答モードは、発信者がインターコム コールを開始するときに使用されるメディア ストリームと同じ IP バージョンでメディア ストリームを確立します。
インターコム電話番号（回線）	インターコム電話番号（回線）は、インターコム回線ごとに1つのデバイスに制限されます。 Cisco Extension Mobility は広く使用されています。モバイル ユーザにはインターコム機能が必要ですが、単一のデバイスでのみそれを使用可能にする必要があります。 インターコム回線を通常のデバイスまたは Extension Mobility プロファイルのどちらかに割り当てることができますが、システムはインターコム回線が通常のデバイスまたは Extension Mobility プロファイルのどちらかに関連付けられることを強制する必要があります。
Extension Mobility プロファイル	1 つの Extension Mobility プロファイルを複数の電話機で同時に使用できます。どのデバイスがこのインターコム回線を表示できるかを指定するには、[**インターコム電話番号の設定（Intercom Directory Number Configuration**）] ウィンドウの [**デフォルトのアクティブ デバイス（Default Activated Device**）] フィールドを使用します（**[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [コール ルーティング（Call Routing）] > [インターコム（Intercom）] > [インターコム電話番号の設定（Intercom Directory Number Configuration）]**）。 Extension Mobility に使用されないインターコム回線についても [デフォルトのアクティブ デバイス（Default Activated Device）] フィールドの設定が必要です。

インターコムの制約事項

インターコム機能には、次のような制約事項が適用されます。

機能	制約事項
保留 (Hold)	インターコム コールを保留にすることは許可されません。
通話転送	インターコム コールを転送することはできません。
転送	インターコム コールを転送することは許可されません。
iDivert	インターコム コールを即時転送することは許可されません。
コール ピックアップ/ダイレクト コール ピックアップ	コール ピックアップ グループにインターコム コールは含まれません。
DND	インターコムはサイレント（DND）よりも優先します。
帯域幅	十分な帯域幅がない場合、インターコム コールは失敗します。
コール ターゲット	2つのインターコム コールがターゲットに振り向けられた場合、最初のコールは接続され、2 番目のコールは失敗して話中音が出力されます。
割り込みとC割り込み	インターコムでは割り込みと C 割り込みは機能しません。
会議	インターコム コールを電話会議に含めることは許可されません。
モニタリングおよび録音	アクティブなコールがモニタまたは記録されているときに、ユーザはインターコム コールを受信も発信もできません。
ビデオ	ビデオはインターコムではサポートされません。
インターコム パーティション	コーリング サーチ スペースなどの項目またはルート パターンに割り当てられたインターコム パーティションは削除できません。
インターコム コーリング サーチ スペース	デバイス、回線（DN）、トランスレーション パターン、またはその他の項目が使用しているインターコム コーリング サーチ スペースは削除できません。

インターコムのトラブルシューティング

インターコム回線のダイヤル アウト時の話中音

問題

ユーザがインターコム回線でダイヤル アウトするときに、電話機でビジー トーンが再生されます。

考えられる原因

DN が発信者番号と同じインターコム パーティション内にありません。

ソリューション

- DN が発信番号と同じインターコム パーティションにあることを確認します。
- I

  同じインターコム パーティションにある場合は、ダイヤル アウトした DN が別の電話機に設定されており、その電話機が同じ Unified Communications Manager クラスタに登録されていることを確認します。

インターコム コールが、スピーカー、ハンドセット、またはヘッドセットでの応答機能を使用できない

問題

ヘッドセット、ハンドセット、またはスピーカーを使用時に、インターコム コールを応答モードにすることができません。

考えられる原因

これは仕様上の問題です。 インターコム コールを接続状態にするには、対応する回線ボタンを押す方法しかありません。

ソリューション

スピーカー、ハンドセット、またはヘッドセットを使用してコールを終了できます。

SCCP のトラブルシューティング

インターコム回線が電話に表示されない

問題

インターコム回線が電話機に表示されません。

考えられる原因

電話機のバージョンが 8.3(1) よりも前か、ボタンテンプレートが電話機に割り当てられていない可能性があります。

ソリューション

- 電話機のバージョンを調べ、 8.3(1) 以降であることを確認します。
- ボタン テンプレートが電話機に割り当てられているかどうかを確認します。
- Cisco Unified Communications Manager と電話機間のスニファ トレースをキャプチャします。 ボタン テンプレートの応答時に、インターコム回線が電話機に送信されるかどうかを確認します（ボタン定義 = Ox17）。

電話機が SRST にフォールバックしてもインターコム回線が表示されない

問題

Unified Communications Manager リリース 6.0(x) 以降で設定された電話機に 2 つのインターコム回線があります。Unified Communications Manager は停止し、SRST に戻ります。 しかし、インターコム回線が表示されません。

考えられる原因

SRST の SCCP バージョンで SCCP バージョン 12 がサポートされていません。

ソリューション

- SRST の SCCP バージョンを確認します。 SRST で SCCP バージョン 12 がサポートされている場合は、インターコム回線がサポートされます。
- SRST で SCCP バージョン 12 がサポートされている場合は、スニファ トレースをキャプチャし、電話から送信されたボタンテンプレートにインターコム回線が含まれていることを確認します。

SIP のトラブルシューティング

SIP を実行している電話のデバッグ

デバッグ コマンド **Debug sip-messages sip-task gsmfsmIsm sip-adapter** を使用します。

SIP を実行している電話機の設定

show config：電話機に対してこのコマンドを実行すると、インターコム回線が標準回線（featureid-->23）として設定されているかどうかが表示されます。

Cisco Extension Mobility ユーザがログインしてもインターコム回線が表示されない

問題

Cisco Extension Mobility ユーザが電話機にログインしてもユーザのインターコム回線が表示されません。

考えられる原因

[デフォルトのアクティブ デバイス（Default Activated Device）] が正しく設定されていません。

ソリューション

- [デフォルトのアクティブ デバイス（Default Activated Device）] がインターコムの電話番号に対して設定されていることを確認します。
- [デフォルトのアクティブ デバイス（Default Activated Device）] が、ログインしたデバイスと一致することを確認します。

インターコム回線が電話に表示されない

問題

インターコム回線が設定され電話に割り当てられていますが、電話に表示されません。

考えられる原因

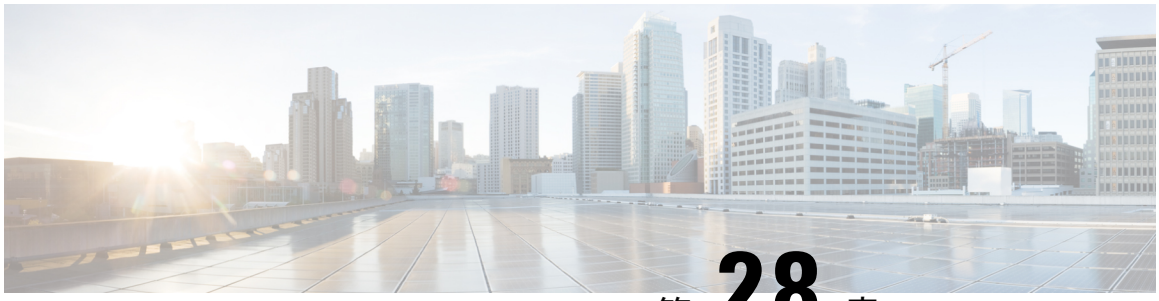
[デフォルトのアクティブ デバイス（Default Activated Device）] の値がこのデバイスのインターコム回線に設定されています。

ソリューション

設定が完了している場合は、電話をリセットしてください。

第 X 部

コールの受信



第 28 章

プライム回線サポート

プライム回線サポートの概要

[Cisco Unified CM の管理（Cisco Unified CM Administration）] でプライム回線サポートを設定できます。設定後、電話がオフフックのときに、いずれかの回線でコールを受信すると、システムは常にコールのプライマリ回線を選択します。

プライム回線サポートの前提条件

プライム回線サポート機能と互換性のあるデバイスを次に示します。

Cisco Unified IP Phone 7900 シリーズ、8900 シリーズ、および 9900 シリーズ

サポートされているデバイスの詳細については、最新バージョンの『*Cisco Unified IP Phone Guide*』および『*Cisco Unified IP Phone Administration Guide*』を参照してください。

プライム回線サポートの設定タスク フロー

Cisco CallManager サービス、またはデバイスとデバイスプロファイルに、プライム回線サポート機能を設定するには、次のいずれかの手順を実行します。

始める前に

- プライム回線サポートの前提条件 （403 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	クラスタ全体のプライム回線サポートの設定 （404 ページ）	（オプション）。 Cisco CallManager サービスにプライム回線サポートを設定します。その場合、この機能はクラスタ全体に適用されます。
ステップ 2	デバイスのプライム回線サポートの設定（405 ページ）	（オプション）。 クラスタ全体でプライム回線サポート機能を有効にする必要がない場合には、クラスタ内の特定のデバイスにこの機能を設定します。 （注） このパラメータを設定すると、オフフックになった場合、同じ電話の別の回線でコールの呼出音が鳴ったとしても、第一の回線のみがアクティブになります。 そのため、他の回線でのコールへの応答は行われません。

クラスタ全体のプライム回線サポートの設定

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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

ステップ 2 [サーバ（Server）] ドロップダウン リストで、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 [常にプライム回線を使用（Always Use Prime Line）]クラスタ全体サービス パラメータから、次のいずれかのオプションをドロップダウン リストから選択します。

- [はい（True）]：電話機がオフフックになると、プライマリ回線が選択され、アクティブ回線になります。
- [いいえ（False）]：電話機がオフフックになると、IP Phone がアクティブ回線として使用可能な回線を自動的に選択します。

このサービス パラメータのデフォルト値は [いいえ（False）]です。

ステップ 5 SIP 電話でこの変更を有効化するには、[Cisco Unified CM の管理（Cisco Unified CM Administration）] で [設定の適用（ApplyConfig）]ボタンをクリックします（たとえば、[デバイス設定（Device Configuration）]ウィンドウや [デバイス プールの設定（Device Pool Configuration）]ウィンドウのほか、[設定の適用（ApplyConfig）] がオプションになっているウィンドウにあります）。

（注） 新しい設定が SIP 電話に適用されない場合、SIP プライム回線サポートの機能変更は、Cisco CallManager サービスの次のリセットまたは影響を受ける各デバイスがリセットされるまで実装されません。

デバイスのプライム回線サポートの設定

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）] > [共通の電話プロファイル（Common Phone Profile）]**。

ステップ 2 [検索と一覧表示（Find and List）]ウィンドウで、[常にプライム回線を使用する（Always Use Prime Line）] の設定を変更する電話を選択します。
[電話の設定（Phone Configuration）]ウィンドウが表示されます。

ステップ 3 [常にプライム回線を使用する（Always Use Prime Line）] ドロップダウン リストで、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、このコールにプライマリ回線が選択されます。他の回線のコールの呼び出し音は鳴り続けます。電話のユーザは、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）]**：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 パラメータから、Cisco CallManager サービスをサポートしている設定を使用します。

ステップ 4 **[保存（Save）]** をクリックします。

プライム回線サポートの連携動作

機能	データのやり取り
[常にプライム回線を使用する(Always Use Prime Line)]	**[デバイス プロファイル（Device Profile）]** または **[デフォルトのデバイス プロファイル設定（Default Device Profile Configuration）]** ウィンドウの **[常にプライム回線を使用する（Always Use Prime Line）]** パラメータで **[オン（On）]** を選択した場合、Cisco Extension Mobility ユーザは、Cisco Extension Mobility をサポートするデバイスにログイン後にこの機能を使用できます。
[コール最大数（Maximum Number of Calls）] と [ビジー トリガー（Busy Trigger）] の設定	電話機の回線にすでにコールがあるとき、Unified Communications Manager は [最大コール数（Maximum Number of Calls）] と [ビジー トリガー（Busy Trigger）] の設定を使用して、コールのルーティング方法を決定します。
自動応答	Cisco Unified CM Administration の [自動応答（Auto Answer）]ドロップダウンリストから [ヘッドセットで自動応答（Auto Answer with Headset）] または [スピーカフォンで自動応答（Auto Answer with Speakerphone）] オプションを選択した場合、[自動応答（Auto Answer）] の設定が [常にプライム回線を使用する（Always Use Prime Line）]パラメータより優先されます。

プライム回線サポートのトラブルシューティング

プライム回線サポートを True に設定すると機能しない

問題　クラスタ全体のサービス パラメータ **[常にプライム回線を使用する（Always use Prime Line）]** が **[はい（True）]** に設定されており、IP フォンがオフフックになると、プライマリ回線がアクティブ回線になります。セカンダリ回線で電話の呼び出し音が鳴っている場合でも、ユーザがオフフックになると、最初の回線だけがアクティブになります。電話はセカンダリ回線の着信コールには応答しません。 ただし、複数のライン アピアランスを備えた IP フォンを 7.1.2 電話ロードで使用すると、セカンダリ回線で呼び出し音が鳴る場合、電話はプライマリ回線を使用しません。ユーザがハンドセットを取ると、電話はセカンダリ回線のコールに応答します。

解決法　プライマリ回線の回線ボタンを押します。これにより、コール開始時にセカンダリ回線が話中になりません。

着信コールに応答できない

問題　IP Phone がオフフックになると、ユーザは着信コールに自動で応答することはできず、コールに応答するために [応答（Answer）] ソフトキーを押す必要があります。

解決法　問題を解決するには、次の手順を実行します。

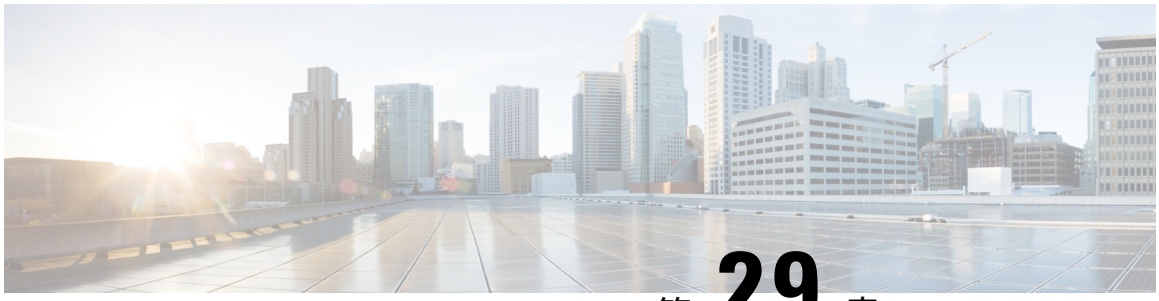
1. [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。
2. [サーバ（Server）] ドロップダウン リストで、Cisco CallManager サービスを実行しているサーバを選択します。
3. [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。
4. クラスタ全体のパラメータ（デバイス - 電話）で、[常にプライム回線を使用する（Always Use Prime Line）] を [いいえ（False）] に設定します。

着信コールに自動で応答する

問題　着信コールを IP Phone の共有回線で受信すると、ハンドセットを上げるとコールの応答が即時に行われ、コールに応答するか、発信コールを行うかを選択できない。 この動作は [自動回線選択（Auto Line Select）] を無効に設定しても変わりません。

解決法　問題を解決するには、次の手順を実行します。

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）]**。
2. [サーバ（Server）] ドロップダウン リストで、Cisco CallManager サービスを実行しているサーバを選択します。
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。
4. クラスタ全体のパラメータ（デバイス - 電話）で、[常にプライム回線を使用する（Always Use Prime Line）] を [いいえ（False）] に設定します。



第 29 章

通話転送

コール転送の概要

ユーザは Cisco Unified IP Phone がコールを別の電話に転送するように設定できます。 次のコール転送タイプがサポートされています。

- [帯域幅不足時転送（Call Forward No Bandwidth）]：帯域幅不足が原因で電話番号へのコールが失敗すると、コールが転送されます。また、公衆電話交換網（PSTN）をボイスメール システムへの代替ルートとして使用する自動代替ルーティング（AAR）接続先への転送機能が提供されます。
- [代替宛先への転送（Call Forward with Alternate Destination）]：電話番号と転送先へのコールに応答がない場合にコールが転送されます。 最終的な手段としてコールは代替接続先に転送されます。 このコール転送タイプは「MLPP 代替パーティ接続先」とも呼ばれます。
- **不在転送（CFA）**：すべてのコールが 1 つの電話番号に転送されます。
- **話中転送（CFB）**：回線が使用中であり、設定されている話中転送（CFB）トリガー値に到達した場合にのみコールが転送されます。
- **無応答時転送（CFNA）**：設定されている [無応答時の呼び出し時間（No Answer Ring Duration）] タイマーが期限切れになるか、接続先の登録が解除された後で、電話が応答しない場合にコールが転送されます。
- **カバレッジなし時転送（CFNC）**：ハントリストの電話番号をすべて使用したか、またはタイムアウトになった場合にコールが転送されます。カバレッジの関連ハントパイロットにより、最終転送に「個人の初期設定を使用（Use Personal Preferences）」が指定されます。
- [未登録不在転送（CFU）（Call Forward Unregistered (CFU)）]：リモート WAN リンクの障害が原因で電話が未登録の場合にコールが転送されます。また、公衆電話交換網（PSTN）

経由での自動再ルーティング機能が提供されます。 発信者のタイプ（内部または外部）に基づいてコールを転送することもできます。

- **CFA 接続先オーバーライド**：コールの転送先ユーザ（ターゲット）が、コールが転送されるユーザ（開始ユーザ）にコールを発信するときに、コールが転送されます。 ターゲットにコールが転送される代わりに、イニシエータの電話で呼出音が鳴ります。

不在転送（CFA ループ防止と CFA ループ ブレークアウトを含む）

不在転送（CFA）では、電話ユーザが 1 つの電話番号にすべてのコールを転送できます。

CFA は内線コールと外線コールに設定できます。また、コーリング サーチ スペース（CSS）を設定することによって、ボイスメール システムまたはダイヤルした接続先番号にコールを転送できます。Unified Communications Manager には、CFA 用の 2 番目のコーリング スペース設定フィールドが含まれます。 CFA のセカンダリ CSS と、CFA の既存の CSS との組み合わせにより、代替 CSS システム設定がサポートされます。 CFA をアクティブにすると、CFA 接続先の検証および CFA 接続先へのコールのリダイレクトには、CFA のプライマリ CSS とセカンダリ CSS だけが使用されます。 これらのフィールドが空白の場合、ヌル CSS が使用されます。 CFA のプライマリ CSS で設定されている CSS フィールドと、CFA のセカンダリ CSS のフィールドだけが使用されます。 電話から CFA をアクティブにすると、CFA の CSS と CFA のセカンダリ CSS を使用して CFA 接続先が検証され、この CFA 接続先がデータベースに書き込まれます。 CFA がアクティブな場合、CFA 接続先は常に、CFA の CSS および CFA のセカンダリ CSS に対して検証されます。

Unified Communications Manager CFA ループが識別されると、電話での CFA のアクティブ化を防止します。 たとえば、ユーザが電話番号 1000 を持つ電話機で C FwdALL ソフトキーを押し、CFA の宛先として 1001 を入力した場合、Unified Communications Manager はコール転送ループを識別し、1001 は、すべてのコールをディレクトリ番号 1002 に転送し、すべてのコールをディレクトリ番号 1003 に転送します。この場合、ループが発生し、ディレクトリ番号 1000 の電話機での CFA アクティベーションが防止されることを Unified Communications Manager が識別します。

ヒント 同一電話番号が異なるパーティションに存在している場合、たとえばパーティション 1 と 2 に電話番号 1000 が存在している場合、Unified Communications Manager はその電話での CFA のアクティブ化を許します。

CFA ループは呼処理には影響しません。これは、Unified Communications Manager は CFA ループ ブレークアウトをサポートしており、これにより CFA ループが特定されると、転送チェーンの電話番号の 1 つで CFNA、CFB などの転送オプションが CFA とともに設定されている場合でも、コールが転送チェーン全体を通過し、不在転送ループを抜けて、ループが予期されているとおりに完了することが保証されるためです。

たとえば、電話番号 1000 の電話のユーザがすべてのコールを電話番号 1001 に転送し、1001 がすべてのコールを電話番号 1002 に転送し、1002 がすべてのコールを電話番号 1000 に転送すると、CFA ループが発生します。 また、電話番号 1002 は、ディレクトリ番号 1004 に CFNA を

設定しています。電話番号 1003 を持つ電話機のユーザは電話番号 1000 を呼び出し、1001 に転送し、1002 に転送します。Unified Communications Manager は CFA ループを識別し、ループから抜けるコールは、電話番号 1002 への接続を試行します。電話番号 1002 のユーザがコールに応答する前に、[応答なし呼び出し時間（No Answer Ring Duration）] タイマーが切れた場合、Unified Communications Manager はコールを電話番号 1004 に転送します。

1 つのコールについて Unified Communications Manager が複数の CFA ループを識別することがあります。この場合、各ループが識別されるたびに、コールの接続が試みられます。

コール転送の設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	コール転送のパーティションの設定（412 ページ）	管理者は、設計基準と要件に基づいて、特定の番号へのコール転送を制限するようにパーティションを設定できます。
ステップ 2	コール転送のコーリング サーチ スペースの設定 （413 ページ）	管理者は、設計基準と要件に基づいて、特定の番号へのコール転送を制限するようにコーリング サーチ スペースを設定できます。
ステップ 3	ハント リストが使用できない場合またはハント タイマーが期限切れになった場合のコール転送の設定（414 ページ）	ハントが失敗したときにコールを転送できます（つまり、ハント パーティが応答せずにハントが終了した場合。これは、リストのハント番号の電話が取られなかった、またはハント タイマーがタイムアウトしたことが原因です）。
ステップ 4	帯域幅不足時転送の設定 （417 ページ）	帯域幅が不十分であるために発信された電話番号へのコールが失敗した場合、代替ルートとして公衆電話交換網（PSTN）を使用して自動代替ルーティング（AAR）の接続先に、またはボイスメール システムに、コールを転送できます。
ステップ 5	代替宛先への転送の設定 （418 ページ）	応答されなかったコールは、電話番号と転送された接続先に転送できます。 最終的な手段としてコールは代替接続先に転送されます。
ステップ 6	その他のコール転送タイプの設定 （420 ページ）	CFA、CFB、CFNA、CFNC、CFU などの追加の転送タイプを設定できます。

	コマンドまたはアクション	目的
		これらすべての転送タイプは、[電話番号の設定（Directory Number Configuration）]ウィンドウから設定できます。
ステップ 7	コール転送の転送先オーバーライドの有効化 （430 ページ）	管理者は、CFA の接続先が CFA の転送元に発信したときに CFA をオーバーライドできます。 これにより、CFA の接続先は、重要なコールがある場合に転送元に到達できるようになります。

コール転送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。

設計基準と要件に基づいて特定の番号へのコール転送を制限するために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** > **コントロールのクラス** > **パーティション**。

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。

説明にはどの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサイド（&）、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。

コール転送の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 *28*：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

コール転送のコーリング サーチ スペースの設定

コーリング サーチ スペースは、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。

特定の番号へのコール転送を設計基準と要件に基づいて制限するには、コーリング サーチ スペースを設定します。

始める前に

コール転送のパーティションの設定 （412 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** > **コントロールのクラス** > **コーリングサーチスペース**。

ステップ 2 [新規追加] 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、どの言語でも最大 50 文字まで指定できますが、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、**コントロール（Ctrl）**キーを押したまま、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。

ハント リストが使用できない場合またはハント タイマーが期限切れになった場合のコール転送の設定

ハントの概念はコール転送とは異なります。 ハントを使用すると、Unified Communications Manager は 1 つ以上の番号リストにコールを転送でき、各リストは一定のアルゴリズムのセットから選択されるハント順序を指定します。 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 （次のハント パーティは現在のハント アルゴリズムによって異なります。） このときハントでは、試行するパーティに対して無応答時転送（CFNA）、話中転送（CFB）、または不在転送（CFA）の設定値が無視されます。

コール転送では、着信側が応答できない、または通話中で、ハントが行われない場合に、コールを転送する方法（転送またはリダイレクト）について詳細に制御することができます。たとえば、回線の CFNA 値がハント パイロット番号に設定されている場合、その回線へのコールに応答がないと、コールはハント パイロット番号に転送され、ハントが開始されます。

始める前に

コール転送のコーリング サーチ スペースの設定 （413 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）] > [ルート/ハント（Route/Hunt）] > [ハント パイロット（Hunt Pilot）]** の順に選択します。
[ハント パイロットの検索と一覧表示（Find and List Hunt Pilots）] ウィンドウが表示されます。

ステップ 2 **[検索(Find)]** をクリックします。
設定済みのハント パイロットのリストが表示されます。

ステップ 3 ハントが失敗した場合にコール処理を設定するパターンを選択します。
[ハント パイロットの設定（Hunt Pilot Configuration）] ウィンドウが表示されます。

ステップ 4 **[ハント コール処理設定（Hunt Call Treatment Settings）]** エリアで **[ハント パイロットの設定（Hunt Pilot Configuration）]** 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、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。

コール転送に関するハント コール処理フィールド

フィールド	説明
ハント コール処理の設定（Hunt Call Treatment Settings）	
（注）	[無応答時ハント転送（Forward Hunt No Answer）]フィールドまたは [話中ハント転送（Forward Hunt Busy）]フィールドは、ルート リスト経由でコールを移動するために設計されたものです。 キューイングはルート リスト内で発信者を保持するために使用されます。 そのため、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。

フィールド	説明

[無応答時ハント転送(Forward Hunt No Answer)]	ハント リストを介して分配されるコールに対して一定の時間応答がない場合、このフィールドでコールの転送先を指定します。 次のいずれかのオプションを選択します。
	• **無応答コールを転送しない（Do Not Forward Unanswered Calls）**
	• [回線グループ メンバーの転送設定を使用（Use Forward Settings of Line Group Member）]（[個人の初期設定を使用（Use Personal Preferences）]チェックボックスの代わり）
	• **無応答コールを転送する（Forward Unanswered Calls to）**
	  • [宛先（Destination）]—コールを転送する必要がある電話番号を入力します。
	  • [コーリング サーチ スペース（Calling Search Space）]—この電話番号を使用するすべてのデバイスに適用されるコーリング サーチ スペースをドロップダウン リストから選択します。
	• [最大ハント タイマー（Maximum Hunt Timer）]—キューイングを使用しないハンティングの最大時間を指定する値（秒単位）を入力します。
	有効な値は 1~3600 です。デフォルト値は 1800 秒（30 分）です。
	注意 関連付けられた回線グループの [最大ハントタイマー(Maximum Hunt Timer)] と [RNA復帰タイムアウト(RNA Reversion Timeout)] には同じ値を指定しないでください。
	無応答転送タイマーは、回線グループの RNA タイマーよりも大きくする必要があります。
	無応答転送タイマーは、回線グループの RNA タイマーの倍数にしてはいけません。
	このタイマーは、期限が切れる前に、ハント メンバーがコールに応答するか、ハント リストが使い果たされた場合に、キャンセルされます。 このタイマーの値を指定しなかった場合は、ハント メンバーが応答するか、ハント リストが使い果たされるまで、ハンティングが継続されます。 どちらのイベントも発生しなかった場合は、最終処理用のコールが受信されてから 30 分間ハンティングが継続されます。
	（注） ハンティングが [転送最大ホップ数（Forward Maximum Hop Count）]サービス パラメータで指定されたホップ数を超えた場合は、ハンティングが 30 分の最大ハント タイマー値の前に期限切れになり、発信者にリオーダー音が流されます。

フィールド	説明

話中ハント転送（Forward Hunt Busy）	ハント リストを介して分配されるコールに対して一定の時間応答がない場合、このフィールドでコールの転送先を指定します。 次のいずれかのオプションを選択します。
	• **無応答コールを転送しない（Do Not Forward Unanswered Calls）**
	• **回線グループ メンバーの転送設定を使用（Use Forward Settings of Line Group Member）**
	• **無応答コールを転送する（Forward Unanswered Calls to）**
	  • [宛先（Destination）]—コールを転送する必要がある電話番号を入力します。
	  • [コーリング サーチ スペース（Calling Search Space）]—この電話番号を使用するすべてのデバイスに適用されるコーリング サーチ スペースをドロップダウン リストから選択します。

帯域幅不足時転送の設定

始める前に

ハント リストが使用できない場合またはハント タイマーが期限切れになった場合のコール転送の設定 （414 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）] > [電話番号の設定（Directory Number Configuration）]**。
[電話番号の検索/一覧表示（Find and List Directory Numbers）] ウィンドウが表示されます。

ステップ 2 **[検索(Find)]** をクリックします。
設定済みの電話番号のリストが表示されます。

ステップ 3 帯域幅が不足しているときのコール転送を設定する電話番号を選択します。
[ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウが表示されます。

ステップ 4 [AAR 設定（AAR Settings）] 領域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、コール転送に関する電話番号設定フィールド （418 ページ）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。

コール転送に関する電話番号設定フィールド

フィールド	説明
[ボイスメール（Voice Mail）]	コールをボイスメールに転送する場合にこの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をオンにすると、Unified Communications Manager は **[接続先（Destination）]** および **[コーリング サーチ スペース（Calling Search Space）]** フィールドの値を無視します。
[AAR接続先マスク（AAR Destination Mask）]	外部電話番号マスクを使用する代わりに、ダイヤルする AAR 接続先を決定するための接続先マスクを入力します。
[AARグループ（AAR Group）]	ドロップダウン リストから AAR グループを選択します。 これは、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ために使用するプレフィックス番号を提供します。[なし（None）] を選択した場合、サーバはブロックされたコールを再ルーティングしようとしません。 この値は、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** から、**[優先代替パーティ タイムアウト（Precedence Alternate Party Timeout）]** サービス パラメータを設定することもできます。
この接続先を不在転送履歴に保持する（Retain this destination in the call forwarding history）	デフォルトで、電話番号設定によってコールの AAR レッグがコール履歴に保持されます。これにより、ボイスメール システムへの AAR 転送でユーザがボイス メッセージを残すよう確実に促されます。 このチェックボックスをオンにすると、コールの AAR レッグがコール転送履歴に残されます。

代替宛先への転送の設定

始める前に

帯域幅不足時転送の設定 （417 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）] > [電話番号の設定（Directory Number Configuration）]**。
[電話番号の検索/一覧表示（Find and List Directory Numbers）] ウィンドウが表示されます。

ステップ 2 **[検索(Find)]** をクリックします。
設定済みの電話番号のリストが表示されます。

ステップ 3 代替宛先を設定する電話番号を選択します。
[ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウが表示されます。

ステップ 4 [MLPP 代替パーティと機密アクセス レベルの設定（MLPP Alternate Party And Confidential Access Level Settings）] 領域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、コール転送のための MLPP 代替パーティおよび社外秘アクセス レベル設定フィールド （419 ページ）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。

コール転送のための MLPP 代替パーティおよび社外秘アクセス レベル設定フィールド

フィールド	説明
転送先（Target、接続先）	ディレクトリ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。
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。
[MLPP 無応答時の呼び出し時間（秒）（MLPP No Answer Ring Duration (seconds)）]	このディレクトリ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 優先コールをこのディレクトリ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。 この値は、Cisco Unified CM の管理の **[システム（System）]>[サービス パラメータ（Service Parameters）]** から、**[優先代替パーティ タイムアウト（Precedence Alternate Party Timeout）]** で設定できます。

その他のコール転送タイプの設定

[電話番号の設定（Directory Number Configuration）] ウィンドウから、不在転送（CFA）、話中転送（CFB）、無応答時転送（CFNA）、カバレッジなし時転送（CFNC）、および未登録の不在転送（CFU）を設定できます。

始める前に

- コール転送機能が意図したとおりに動作するように、さまざまなパーティションの設定済みの電話と電話番号に対して、コール転送のコーリング サーチ スペースも設定することをお勧めします。そうしないと、転送が失敗する可能性があります。コール転送の接続先にコールが転送またはリダイレクトされると、設定されているコール転送のコーリング サーチ スペースがコール転送に使用されます。
- 代替宛先への転送の設定 （418 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）] > [電話番号の設定（Directory Number Configuration）]**。

[電話番号の検索/一覧表示（Find and List Directory Numbers）] ウィンドウが表示されます。

ステップ 2 [電話番号の設定（Directory Number Configuration）] ウィンドウの [コール転送とコール ピックアップの設定（Call Forwarding and Call Pickup Settings）] フィールドで、CFA、CFB、CFNA、CFNC、および CFU を設定します。 フィールドとその設定オプションについては、コール転送のフィールド （420 ページ）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。

コール転送のフィールド

フィールド	説明
[コール転送とコールピックアップの設定（Call Forward and Call Pickup Settings）]	

フィールド	説明
[コーリングサーチスペースのアクティベーションポリシー (Calling Search Space Activation Policy)]	このオプションには、3 つの値があります。 • [システム デフォルトを使用（Use System Default）]：コール転送に使用される不在転送コーリング サーチ スペースを決定する [CFA CSS アクティベーション ポリシー（CFA CSS Activation Policy）] サービス パラメータ。**[CFA CSS アクティベーション ポリシー（CFA CSS Activation Policy）]**サービス パラメータを **[設定済み CSS を使用（With Configured CSS）]** に設定した場合、不在転送コーリング サーチ スペースと不在転送セカンダリ コーリング サーチ スペースがコール転送に使用されます。 これがデフォルト設定です。 • [設定済み CSS を使用（With Configured CSS）]：[電話番号の設定（Directory Number Configuration）] ウィンドウで明示的に設定された不在転送コーリング サーチ スペースにより、不在転送のアクティブ化とコール転送が制御されます。 不在転送コーリング サーチ スペースが [なし（None）]に設定されている場合、CSS は不在転送のために設定されません。パーティションが設定された任意の電話番号への不在転送をアクティブにすることはできません。 不在転送のアクティブ化中に、不在転送コーリング サーチ スペースおよび不在転送セカンダリ コーリング サーチ スペースの変更は発生しません。 • [アクティブなデバイス/回線 CSS を使用（With Activating Device/Line CSS）]：電話番号コーリング サーチ スペースとデバイス コーリング サーチ スペースの組み合わせにより、不在転送のアクティブ化とコール転送が制御されます。その際、不在転送コーリング サーチ スペースの明示的な設定は不要です。 電話から不在転送をアクティブにした場合、デバイスをアクティブにするため、不在転送コーリング サーチ スペースと不在転送セカンダリ コーリング サーチ スペースに、電話番号コーリング サーチ スペースとデバイス デバイス コーリング サーチ スペースが自動的に入力されます。 不在転送コーリング サーチ スペースに [なし（None）]が設定されている場合、不在転送が電話からアクティブにされると、電話番号コーリング サーチ スペースとアクティブにするデバイスのコーリング サーチ スペースの組み合わせにより、不在転送の試行が制御されます。 [CFA CSS アクティベーション ポリシー（CFA CSS Activation Policy）]：転送が想定どおりに動作するために、[サービス パラメータ設定（Service Parameter Configuration）]ウィンドウでこのサービス パラメータを必ず正しく設定してください。 このサービス パラメータの 2 つの有効値を次に示します。 • [設定済み CSS を使用（With Configured CSS）]：プライマリおよびセカンダリ CFA コーリング サーチ スペースによりコール転送の試行が制御されます。 • [アクティブなデバイス/回線 CSS を使用（With Activating Device/Line CSS）]：プライマリおよびセカンダリ CFA コーリング サーチ スペースが、プライマリ回線のコーリング サーチ スペースとアクティブにするデバイスのコーリング サーチ スペースによって更新されます。 [ローミング（Roaming）]：デバイスが同一のデバイス モビリティ グループ内をローミングしているとき、Cisco Unified Communications Manager はデバイス モビリティ CSS を使用してローカル ゲートウェイに到達します。ユーザが電話で不在転送を設定している場合、CFA CSS が **[なし（None）]** に設定されていて、[CFA CSS アクティベーション ポリシー（CFA CSS Activation Policy）] が **[アクティブなデバイス/回線 CSS を使用（With Activating Device/Line CSS）]** に設定されていると、次のようになります。 • デバイスがホーム ロケーションにあるときに CFA CSS としてデバイス CSS と回線 CSS が使用されます。 • デバイスが同一のデバイス モビリティ グループ内をローミングしているとき、CFA CSS としてローミング デバイス プールからのデバイス モビリティ CSS と回線 CSS が使用されます。 • デバイスが別のデバイス モビリティ グループ内をローミングしているとき、CFA CSS としてデバイス CSS と回線 CSS が使用されます。

フィールド	説明
[不在転送（Forward All）]	この行のフィールドは、不在転送先として設定されている電話番号へのコール転送処理を指定します。[コーリングサーチスペース（Calling Search Space）]フィールドの値は、ユーザが電話から不在転送をアクティブにするときに入力した不在転送先を検証するときに使用されます。 またこのフィールドは、不在転送先にコールをリダイレクトするときにも使用されます。 次の値を設定します。 • [ボイスメール（VoiceMail）]：[ボイスメールプロファイルの設定（Voice Mail Profile Configuration）]ウィンドウで設定されている値を使用する場合は、この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がオンのときには、Unified Communications Manager は **[接続先（Destination）]** および **[コーリング サーチ スペース（Calling Search Space）]** フィールドの値を無視します。 • [接続先（Destination）]：このフィールドは、すべてのコールの転送先電話番号を示します。 外部の電話番号を含め、ダイヤル可能な任意の電話番号を使用します。 • [コーリングサーチスペース（CallingSearch Space）]：この値は、この電話番号を使用するすべてのデバイスに適用されます。 • [転送の最大ホップ数（Forward Maximum Hop Count）]：[Cisco Unified CM の管理（Cisco Unified CM Administration）] からこのパラメータを設定する場合は、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** を選択します。 このサービス パラメータは、1 つのコールの最大転送回数を指定します。QSIG コールについては特殊な考慮事項があります。 着信 QSIG コールの場合、最大値は（ISO 仕様に基づき）15 です。これよりも大きい値をこのフィールドに指定すると、指定された値は非 QSIG コールに適用され、着信 QSIG コールの最大転送回数は 15 回になります。 QSIG トランクが設定されている場合、このパラメータを 15 に設定することが推奨されます。 たとえば、このパラメータの値が 7 であり、（7 つのホップからなる）不在転送チェーンが電話番号 1000 から 007 で連続して発生する場合、Cisco Unified Communications Manager では、電話番号 2000 の電話ユーザが電話番号 1000 への CFA をアクティブにすることを防止します。これは、1 回のコールでは 7 つを超える転送ホップがサポートされていないためです。
[不在転送のセカンダリコーリングサーチスペース（Secondary Calling Search Space for Forward All）]	コール転送は回線ベースの機能であるため、デバイス コーリング サーチ スペースが不明な場合は、コールの転送に回線コーリング サーチ スペースだけが使用されます。回線コーリング サーチ スペースは限定的でありルーティングできないため、転送は失敗します。 不在転送のセカンダリ コーリング サーチ スペースを追加すると、転送を有効化できます。 不在転送のプライマリ コーリング サーチ スペースとセカンダリ コーリング サーチ スペースが連結されます（プライマリ CFA CSS + セカンダリ CFA CSS）。Unified Communications Manager は、この組み合わせを使用して、CFA 接続先を検証し、コールを転送します。

フィールド	説明
話中転送（Forward Busy Internal、内部）	この行のフィールドは、電話番号が通話中の場合のこの電話番号への内線コールの転送処理を指定します。[接続先（Destination）]フィールドと [コーリングサーチスペース（Calling Search Space）]フィールドの値を使用して、コールが転送先にリダイレクトされます。 次の値を設定します。 • [ボイスメール（VoiceMail）]：内線コールに [ボイスメールプロファイルの設定（Voice Mail Profile Configuration）]ウィンドウで設定されている値を使用する場合は、この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がオンのときには、ボイスメール パイロットのコーリング サーチ スペースが使用されます。Unified Communications Manager は、**[接続先（Destination）]** および **[コーリング サーチ スペース（Calling Search Space）]** フィールドの値を無視します。 （注） 内線コールでこのチェックボックスをオンにすると、外線コールの **[ボイスメール(Voice Mail)]** チェックボックスが自動的にオンになります。外線コールをボイスメールシステムに転送しない場合は、外線コールの [ボイス メール（Voice Mail）]チェックボックスをオフにする必要があります。 • [接続先（Destination）]：このフィールドは、内線コールの話中転送の接続先を示します。 外部の電話番号を含め、ダイヤル可能な任意の電話番号を使用します。 （注） 内線コールの宛先の値を入力すると、外線コールの **[接続先(Destination)]** フィールドにこの値が自動的にコピーされます。 外線コールを別の接続先に転送する場合は、外線コールの [接続先（Destination）]フィールドに別の値を入力する必要があります。 • [コーリング サーチ スペース（Calling Search Space）]：話中転送（内部）の接続先にコールを転送するため、話中転送（内部）のコーリング サーチ スペースが使用されます。 これは、この電話番号を使用するすべてのデバイスに適用されます。 （注） システムでパーティションとコーリング サーチ スペースが使用される場合には、コール転送のコーリング サーチ スペースを設定することが推奨されます。 コール転送の接続先にコールが転送またはリダイレクトされると、設定されているコール転送のコーリング サーチ スペースがコール転送に使用されます。 [コーリング サーチ スペース（Calling Search Space）]フィールドに [なし（None）]が設定されている場合、システムでパーティションとコーリング サーチ スペースが使用されていると転送操作が失敗します。 たとえば話中転送の接続先を設定する場合、話中転送のコーリング サーチ スペースも設定する必要があります。 パーティションで話中転送のコーリング サーチ スペースと話中転送接続先を設定していない場合、転送操作が失敗します。 （注） 内線コールのコーリング サーチ スペースを選択すると、外線コールのコーリング サーチ スペース設定に、この値が自動的にコピーされます。 外線コールを別のコーリング サーチ スペースに転送する場合は、外線コールの [コーリング サーチ スペース（Calling Search Space）] フィールドで別の値を選択する必要があります。 ライン アピアランスごとに [話中転送（Call Forward Busy）] トリガーが設定されます。このトリガーは、ライン アピアランスで設定されている最大コール数よりも大きくすることはできません。[話中転送（Call Forward Busy）] トリガーにより、[話中転送（Call Forward Busy）] 設定がアクティブになるまでのアクティブ コールの数（例：10 コール）が決定されます。 **ヒント** ユーザがコールを発信して転送を実行できるようにするため、話中転送トリガーは、コール最大数よりやや少ない値にしてください。 **ヒント** コールの転送先電話番号が通話中の場合、そのコールは完了しません。

フィールド	説明
話中転送（Forward Busy External、外部）	この行のフィールドは、電話番号が通話中の場合のこの電話番号への外線コールの転送処理を指定します。[接続先（Destination）]フィールドと [コーリングサーチスペース（Calling Search Space）]フィールドを使用して、コールが転送接続先にリダイレクトされます。 次の値を設定します。 • [ボイスメール（VoiceMail）]：外線コールに [ボイスメールプロファイルの設定（Voice Mail Profile Configuration）]ウィンドウで設定されている値を使用する場合は、この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がオンのときには、ボイスメール パイロットのコーリング サーチ スペースが使用されます。Unified Communications Manager は、**[接続先（Destination）]** および **[コーリング サーチ スペース（Calling Search Space）]** フィールドの値を無視します。 （注） 内線コールでこのチェックボックスをオンにすると、外線コールの **[ボイスメール(Voice Mail)]** チェックボックスが自動的にオンになります。外線コールをボイスメールシステムに転送しない場合は、外線コールの [ボイス メール（Voice Mail）]チェックボックスをオフにする必要があります。 • [接続先（Destination）]：このフィールドは、外線コールの話中転送の接続先を示します。 外部の電話番号を含め、ダイヤル可能な任意の電話番号を使用します。 （注） 内線コールの宛先の値を入力すると、外線コールの **[接続先(Destination)]** フィールドにこの値が自動的にコピーされます。 外線コールを別の接続先に転送する場合は、外線コールの [接続先（Destination）]フィールドに別の値を入力する必要があります。 • [コーリング サーチ スペース（Calling Search Space）]：話中転送（外部）のコーリング サーチ スペースにより、話中転送（外部）の接続先にコールが転送されます。 これは、この電話番号を使用するすべてのデバイスに適用されます。 （注） システムでパーティションとコーリング サーチ スペースが使用される場合には、コール転送のコーリング サーチ スペースを設定することが推奨されます。 コール転送の接続先にコールが転送またはリダイレクトされると、設定されているコール転送のコーリング サーチ スペースがコール転送に使用されます。 [コーリング サーチ スペース（Calling Search Space）]フィールドに [なし（None）]が設定されている場合、システムでパーティションとコーリング サーチ スペースが使用されていると転送操作が失敗します。 たとえば話中転送の接続先を設定する場合、話中転送のコーリング サーチ スペースも設定する必要があります。パーティションで話中転送のコーリング サーチ スペースと話中転送接続先を設定していない場合、転送操作が失敗します。 （注） 内線コールのコーリング サーチ スペースを選択すると、外線コールのコーリング サーチ スペース設定に、この値が自動的にコピーされます。 外線コールを別のコーリング サーチ スペースに転送する場合は、外線コールの [コーリング サーチ スペース（Calling Search Space）] フィールドで別の値を選択する必要があります。

フィールド	説明
無応答時転送（Forward No Answer Internal、内部）	この行のフィールドは、電話番号が応答しない場合のこの電話番号への内線コールの転送処理を指定します。[接続先（Destination）]フィールドと [コーリング サーチ スペース（Calling Search Space）]フィールドを使用して、コールが転送接続先にリダイレクトされます。 次の値を設定します。 • [ボイスメール（VoiceMail）]：[ボイスメールプロファイルの設定（Voice Mail Profile Configuration）]ウィンドウで設定されている値を使用する場合は、この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がオンのときには、ボイスメール パイロットのコーリング サーチ スペースが使用されます。Unified Communications Manager は、**[接続先（Destination）]** および **[コーリング サーチ スペース（Calling Search Space）]** フィールドの値を無視します。 （注） 内線コールでこのチェックボックスをオンにすると、外線コールの**[ボイスメール(Voice Mail)]** チェックボックスが自動的にオンになります。外線コールをボイスメールシステムに転送しない場合は、外線コールの [ボイス メール（Voice Mail）]チェックボックスをオフにする必要があります。 • [接続先（Destination）]：このフィールドは、内線コールに応答がない場合にこのコールが転送される電話番号を示します。 外部の電話番号を含め、ダイヤル可能な任意の電話番号を使用します。 （注） 内線コールの宛先の値を入力すると、外線コールの **[接続先(Destination)]** フィールドにこの値が自動的にコピーされます。 外線コールを別の接続先に転送する場合は、外線コールの [接続先（Destination）]フィールドに別の値を入力する必要があります。 • [コーリング サーチ スペース（Calling Search Space）]：無応答時転送（内部）接続先にコールを転送するため、無応答時転送（内部）のコーリング サーチ スペースが使用されます。 これは、この電話番号を使用するすべてのデバイスに適用されます。 （注） システムでパーティションとコーリング サーチ スペースが使用される場合には、コール転送のコーリング サーチ スペースを設定することが推奨されます。 コール転送の接続先にコールが転送またはリダイレクトされると、設定されているコール転送のコーリング サーチ スペースがコール転送に使用されます。 [コーリング サーチ スペース（Calling Search Space）]フィールドに [なし（None）]が設定されている場合、システムでパーティションとコーリング サーチ スペースが使用されていると転送操作が失敗します。 たとえば無応答時転送の接続先を設定する場合、無応答時転送のコーリング サーチ スペースも設定する必要があります。パーティションで無応答時転送のコーリング サーチ スペースと無応答時転送の接続先を設定していない場合、転送操作が失敗します。 （注） 内線コールのコーリング サーチ スペースを選択すると、外線コールのコーリング サーチ スペース設定に、この値が自動的にコピーされます。 外線コールを別のコーリング サーチ スペースに転送する場合は、外線コールの [コーリング サーチ スペース（Calling Search Space）]フィールドで別の値を選択する必要があります。

フィールド	説明
無応答時転送（Forward No Answer External、外部）	この行のフィールドは、電話番号が応答しない場合のこの電話番号への外線コールの転送処理を指定します。[接続先（Destination）]フィールドと [コーリング サーチ スペース（Calling Search Space）]フィールドを使用して、コールが転送接続先にリダイレクトされます。 次の値を設定します。 • [ボイスメール（VoiceMail）]：[ボイスメールプロファイルの設定（Voice Mail Profile Configuration）]ウィンドウで設定されている値を使用する場合は、この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がオンのときには、ボイスメール パイロットのコーリング サーチ スペースが使用されます。Unified Communications Manager は、**[接続先（Destination）]** および **[コーリング サーチ スペース（Calling Search Space）]** フィールドの値を無視します。 （注） 内線コールでこのチェックボックスをオンにすると、外線コールの **[ボイスメール(Voice Mail)]** チェックボックスが自動的にオンになります。外線コールをボイスメールシステムに転送しない場合は、外線コールの [ボイス メール（Voice Mail）]チェックボックスをオフにする必要があります。 • [接続先（Destination）]：このフィールドは、外線コールに応答がない場合にこのコールが転送される電話番号を示します。 外部の電話番号を含め、ダイヤル可能な任意の電話番号を使用します。 （注） 内線コールの宛先の値を入力すると、外線コールの **[接続先(Destination)]** フィールドにこの値が自動的にコピーされます。 外線コールを別の接続先に転送する場合は、外線コールの [接続先（Destination）]フィールドに別の値を入力する必要があります。 • [コーリング サーチ スペース（Calling Search Space）]：無応答時転送（外部）の接続先にコールを転送するため、無応答時転送（外部）のコーリング サーチ スペースが使用されます。 これは、この電話番号を使用するすべてのデバイスに適用されます。 （注） システムでパーティションとコーリング サーチ スペースが使用される場合には、コール転送のコーリング サーチ スペースを設定することが推奨されます。 コール転送の接続先にコールが転送またはリダイレクトされると、設定されているコール転送のコーリング サーチ スペースがコール転送に使用されます。 [コーリング サーチ スペース（Calling Search Space）]フィールドに [なし（None）]が設定されている場合、システムでパーティションとコーリング サーチ スペースが使用されていると転送操作が失敗します。 たとえば話中転送の接続先を設定する場合、無応答時転送のコーリング サーチ スペースも設定する必要があります。 パーティションで無応答時転送のコーリング サーチ スペースと無応答時転送の接続先を設定していない場合、転送操作が失敗します。 （注） 内線コールのコーリング サーチ スペースを選択すると、外線コールのコーリング サーチ スペース設定に、この値が自動的にコピーされます。 外線コールを別のコーリング サーチ スペースに転送する場合は、外線コールの [コーリング サーチ スペース（Calling Search Space）] フィールドで別の値を選択する必要があります。

フィールド	説明
カバレッジなし時転送（Forward No Coverage Internal、内部）	[接続先（Destination）]フィールドと [コーリング サーチ スペース（Calling Search Space）]フィールドを使用して、コールが転送接続先にリダイレクトされます。 次の値を設定します。 • [ボイスメール（VoiceMail）] : [ボイスメールプロファイルの設定（Voice Mail Profile Configuration）]ウィンドウで設定されている値を使用する場合は、この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がオンのときには、Unified Communications Manager は **[接続先（Destination）]** および **[コーリング サーチ スペース（Calling Search Space）]** フィールドの値を無視します。内線コールでこのチェックボックスをオンにすると、外線コールの **[ボイスメール(Voice Mail)]** チェックボックスが自動的にオンになります。 外線コールをボイスメール システムに転送しない場合は、外線コールの [ボイス メール（Voice Mail）]チェックボックスをオフにします。 • [接続先（Destination）] : このフィールドは、電話番号を制御するアプリケーションが失敗した場合に、接続されなかった内線コールが転送される電話番号を指定します。外部の電話番号を含め、ダイヤル可能な任意の電話番号を使用します。 （注） 内線コールの宛先の値を入力すると、外線コールの **[接続先(Destination)]** フィールドにこの値が自動的にコピーされます。 外線コールを別の接続先に転送する場合は、外線コールの [接続先（Destination）]フィールドに別の値を入力する必要があります。 • [コーリング サーチ スペース（Calling Search Space）] : カバレッジなし時転送（内部）の接続先にコールを転送するため、カバレッジなし時転送（内部）のコーリング サーチ スペースが使用されます。 この値は、この電話番号を使用するすべてのデバイスに適用されます。 （注） システムでパーティションとコーリング サーチ スペースが使用される場合には、コール転送のコーリング サーチ スペースを設定することが推奨されます。 コール転送の接続先にコールが転送またはリダイレクトされると、設定されているコール転送のコーリング サーチ スペースがコール転送に使用されます。 [コーリング サーチ スペース（Calling Search Space）]フィールドに [なし（None）] が設定されている場合、システムでパーティションとコーリング サーチ スペースが使用されていると転送操作が失敗します。 たとえば話中転送の接続先を設定する場合、カバレッジなし時転送のコーリング サーチ スペースも設定する必要があります。 パーティションでカバレッジなし時転送のコーリング サーチ スペースと話中転送接続先を設定していない場合、転送操作が失敗します。 （注） 内線コールのコーリング サーチ スペースを選択すると、外線コールのコーリング サーチ スペース設定に、この値が自動的にコピーされます。 外線コールを別のコーリング サーチ スペースに転送する場合は、外線コールの [コーリング サーチ スペース（Calling Search Space）] フィールドで別の値を選択する必要があります。

フィールド	説明
カバレッジなし時転送（Forward No Coverage External、外部）	[接続先（Destination）]フィールドと [コーリング サーチ スペース（Calling Search Space）]フィールドを使用して、コールが転送接続先にリダイレクトされます。 次の値を指定します。 • [ボイスメール（VoiceMail）] : [ボイスメールプロファイルの設定（Voice Mail Profile Configuration）]ウィンドウで設定されている値を使用する場合は、この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がオンのときには、Unified Communications Manager は **[接続先（Destination）]** および **[コーリング サーチ スペース（Calling Search Space）]** フィールドの値を無視します。内線コールでこのチェックボックスをオンにすると、外線コールの **[ボイスメール(Voice Mail)]** チェックボックスが自動的にオンになります。 外線コールをボイスメール システムに転送しない場合は、外線コールの [ボイス メール（Voice Mail）]チェックボックスをオフにします。 • [接続先（Destination）] : このフィールドは、電話番号を制御するアプリケーションが失敗した場合に、接続されなかった内線コールが転送される電話番号を指定します。外部の電話番号を含め、ダイヤル可能な任意の電話番号を使用します。 （注） 内線コールの宛先の値を入力すると、外線コールの **[接続先(Destination)]** フィールドにこの値が自動的にコピーされます。 外線コールを別の接続先に転送する場合は、外線コールの [接続先（Destination）]フィールドに別の値を入力する必要があります。 • [コーリング サーチ スペース（Calling Search Space）] : カバレッジなし時転送（外部）接続先にコールを転送するため、カバレッジなし時転送（外部）のコーリング サーチ スペースが使用されます。 この値は、この電話番号を使用するすべてのデバイスに適用されます。 （注） システムでパーティションとコーリングサーチスペースが使用される場合には、コール転送のコーリング サーチ スペースを設定することが推奨されます。 コール転送の接続先にコールが転送またはリダイレクトされると、設定されているコール転送のコーリング サーチ スペースがコール転送に使用されます。 [コーリング サーチ スペース（Calling Search Space）]に [なし（None）]が設定されている場合、システムでパーティションとコーリング サーチ スペースが使用されていると転送操作が失敗することがあります。 たとえば、カバレッジなし時転送の転送先を設定した場合は、カバレッジなし時転送のコーリング サーチ スペースも設定する必要があります。 カバレッジなし時転送のコーリング サーチ スペースが設定されていない場合、カバレッジなし時転送の転送先がパーティション内にあると、自動転送動作が失敗することがあります。 （注） 内線コールのコーリング サーチ スペースを選択すると、外線コールのコーリング サーチ スペース設定に、この値が自動的にコピーされます。 外線コールを別のコーリング サーチ スペースに転送する場合は、外線コールの [コーリングサーチスペース（Calling Search Space）] フィールドで別の値を選択します。

フィールド	説明
[CTI障害時転送(Forward on CTI Failure)]	このフィールドは、CTIルートポイントおよびCTIポートだけに適用されます。 この行のフィールドは、CTIルートポイントまたはCTIポートで障害が発生した場合に、このCTIルートポイントまたはCTIポートへの外線コールの自動転送をどのように扱うのかを指定します。 次の値を設定します。 • [ボイスメール（VoiceMail）]：[ボイスメールプロファイルの設定（Voice Mail Profile Configuration）]ウィンドウで設定されている値を使用する場合は、この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がオンのときには、Unified Communications Manager は **[接続先（Destination）]** および **[コーリング サーチ スペース（Calling Search Space）]** フィールドの値を無視します。 • [接続先（Destination）]：このフィールドは、電話番号を制御するアプリケーションが失敗した場合に、接続されなかった内線コールが転送される電話番号を指定します。 外部の電話番号を含め、ダイヤル可能な任意の電話番号を使用します。 • [コーリングサーチスペース（CallingSearch Space）]：この値は、この電話番号を使用するすべてのデバイスに適用されます。
[未登録内線の不在転送(Forward Unregistered Internal)]	このフィールドは未登録の内部 DN コールに適用されます。 コールは指定された接続先またはボイスメールに再ルーティングされます。 （注） [サービス パラメータ設定（Service Parameters Configuration）]ウィンドウで、[DN への最大転送未登録ホップ数（Max Forward UnRegistered Hops to DN）]サービス パラメータに電話番号の最大転送回数を指定する必要もあります。 このパラメータは、電話番号に対して同時に許可される最大未登録ホップ数を指定します。 このパラメータは、転送ループが発生した場合に、未登録DNが原因でコールを転送できる回数を制限します。このカウントを使用して、未登録のコール転送の外部コールの転送ループを停止します。Unified Communications Manager は、このサービス パラメータで指定された値を超えたときに、コールを終了します。
[未登録外線の不在転送(Forward Unregistered External)]	このフィールドは未登録の外部 DN コールに適用されます。 コールは指定された接続先またはボイスメールに再ルーティングされます。 （注） [サービス パラメータ設定（Service Parameters Configuration）]ウィンドウで、[DN への最大転送未登録ホップ数（Max Forward UnRegistered Hops to DN）]サービス パラメータに電話番号の最大転送回数を指定する必要もあります。 このパラメータは、電話番号に対して同時に許可される最大未登録ホップ数を指定します。 このパラメータは、転送ループが発生した場合に、未登録DNが原因でコールを転送できる回数を制限します。このカウントを使用して、未登録のコール転送の外部コールの転送ループを停止します。Unified Communications Manager は、このサービス パラメータで指定された値を超えたときに、コールを終了します。
[無応答時の呼び出し時間（秒）（No Answer Ring Duration (seconds)）]	このフィールドは、無応答時転送の接続先が指定されている場合に、無応答コールをこの接続先に転送するまでに待機する時間を秒単位で指定します。 このパラメータに指定する値が、[T301 タイマー（T301 Timer）]サービス パラメータに指定されている値よりも少ないことを確認してください。 [無応答時転送タイマー（Forward No Answer Timer）]サービス パラメータの値が [T301 タイマー（T301 Timer）]サービスパラメータに指定されている値よりも大きい場合は、コールは転送されず、発信者はビジー信号を受信します。 Cisco Unified Communications Manager の [無応答時転送タイマー（Forward No Answer Timer）]サービス パラメータに値を設定する場合は、このフィールドには何も指定しないでください。

コール転送の転送先オーバーライドの有効化

コール転送の転送先オーバーライドを有効にすると、Unified Communications Manager は CFA の宛先が発信者番号と一致したときにCFAの宛先を無視します。 オーバーライドは、内部コールと外部コールの両方に適用されます。

発信者番号が変換されている場合、発信者番号は CFA の宛先と一致せず、オーバーライドは発生しません。

始める前に

その他のコール転送タイプの設定 （420 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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。
[サービス パラメータの設定（Service Parameter Configuration）]ウィンドウが表示されます。

ステップ 2 [クラスタ全体のパラメータ（機能 - 保留復帰（Clusterwide Parameters (Feature - Hold Reversion)）] 領域で、[CFA の宛先オーバーライド（CFA Destination Override）]サービス パラメータ値を [はい（True）]に設定します。

コール転送の連携動作

機能	データのやり取り
コールバック	コールバック通知画面から発信したコールは、着信側DNで設定されているすべてのコール転送設定値をオーバーライドします。コールバック リコール タイマーが期限切れになる前にコールを発信する必要があります。このようにしないと、コールはコール転送設定値をオーバーライドしません。
コール表示の制限	接続番号表示制限は、このシステムから発信されるすべてのコールに適用されます。 この値を [**はい（True）**] に設定すると、このフィールドは既存の Unified Communications Manager アプリケーション、機能、および呼処理と透過的に連携して動作します。この値は、システムの内部または外部で終了するすべてのコールに適用されます。 接続番号表示が更新され、不在転送または話中転送の転送先にコールがルーティングされるか、コール転送または CTI アプリケーションでリダイレクトされる場合、変更された番号またはリダイレクトされた番号が表示されるようになりました。

機能	データのやり取り
取り込み中	Cisco Unified IP 電話 では、サイレント（DND）機能がアクティブであることを示すメッセージがユーザに新しいボイス メッセージが届いていることを示すメッセージよりも優先されます。 ただし、不在転送機能がアクティブであることを通知するメッセージが DND よりも優先されます。
外部コール制御	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。 外部コール制御が優先されます。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 パターンに外部コール制御プロファイルが割り当てられていると、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 Unified Communications Manager に Continue 義務付きの Permit 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。
クラスタ間のエクステンション モビリティ	Cisco Extension Mobility Cross Cluster はコール転送をサポートしています。
拡張と接続	拡張と接続 は不在転送をサポートしています。
即時転送	[**電話番号の設定（Directory Number Configuration**）] ウィンドウの [無応答時転送（Forward No Answer）] フィールドが設定されていない場合、コール転送はクラスタ全体の CFNA タイマー サービス パラメータ [**無応答時転送タイマー（Forward No Answer Timer**）] を使用します。 コール転送と同時にユーザが [即転送（iDivert）] ソフトキーを押すと、コールはボイスメールではなく、割り当てられているコール転送電話番号に転送されます。これは、タイマーで設定されている時間が短すぎるためです。 この状況を解決するには、CFNA タイマー サービス パラメータに十分な時間（例：60 秒）を設定します。
論理パーティション設定	Unified Communications Manager 着信および転送デバイスに関連付けられている地理位置 ID 情報を使用して、論理パーティション ポリシー チェックを実行します。 この処理はすべてのコール転送に適用されます。

機能	データのやり取り
マルチレベルの優先およびプリエンプション	

機能	データのやり取り
	話中転送 • 必要に応じて、MLPP対応ステーションに事前設定の優先代替パーティ ターゲットを設定できます。 • Cisco Unified Communications Managerは、優先コールに優先代替パーティ転送手順を適用する前に、通常の方法で優先コールを転送するため話中転送機能を適用します。 • 複数の転送コール間ではコールの優先度が維持されます。 • 着信優先コールの優先度が既存のコールの優先度より高い場合は、プリエンプションが実行されます。 優先コールの転送先ステーションがコールを切断するまで、アクティブコールのプリエンション側に対し、連続的なプリエンプショントーンが再生され続けます。 コール切断後は、優先コールの転送先ステーションに対し、優先呼び出し音が再生されます。 転送先ステーションは、オフフックになるとプリエンプション コールに接続します。 **無応答時転送** • 優先レベルが [プライオリティ（Priority）] 以上のコールの場合、呼処理により、転送プロセスでコールの優先レベルが維持され、転送先ユーザがプリエンプション処理されることがあります。 • 優先コールの転送先として代替パーティが設定されている場合、優先コール代替パーティタイムアウトが期限切れになった後で、呼処理により優先コールは代替パーティに転送されます。 優先コールの転送先で [代替パーティ（Alternate Party）] 値が設定されていない場合、呼処理により優先コールが [無応答時転送（Call Forward No Answer）] 値に転送されます。 • 通常、優先コールはボイスメール システムではなくユーザにルーティングされます。 管理者は、優先コールがボイスメール システムにルーティングされることを防ぐため、**[優先コールに標準 VM 処理を使用する（Use Standard VM Handling For Precedence Calls）]** エンタープライズ パラメータを設定します。 着信優先コールの優先度が既存のコールの優先度以下の場合、呼処理では通常のコール転送が実行されます。 優先コールの転送先ステーションがプリエンプティブ処理可能ではない場合（MLPPが設定されていない場合）、呼処理ではコール転送が実行されます。

機能	データのやり取り
	代替パーティ転送（APD）は、特殊なコール転送で構成されます。 ユーザが APD に対して設定されていて、優先コールの転送先電話番号（DN）が通話中か、応答しない場合、APDが実行されます。 MLPP APD は、優先コールだけに適用されます。 MLPP APD コールにより、優先コールの [DN無応答時転送（DN Call Forward No Answer）] 値は無効になります。
通信履歴の元の着信側名	着信側デバイスの SIP プロファイルでのみプライバシーが設定されており、不在転送（CFA）、話中転送（CFB）、または未登録不在転送（CFUR）が有効である場合、設定されている呼び出し表示が「「private」」の代わりに表示されます。 コール転送で「「private」」が表示されるようにするには、SIP プロファイルではなくトランスレーション パターンまたはルート パターンで名前表示制限を設定することが推奨されます。
ロールオーバー回線	コール転送設定を使用して、共有回線のロールオーバー回線を作成できます。 コールセンターの状況によっては、これが役立つことがあります。 ロールオーバー回線を使用すると、番号（1-800-HOTLINE など）がダイヤルされたとき、常に特定の電話回線にコールがルーティングされます。 複数の電話で共有される共有回線をこれに設定することができます。 回線 1 が通話中の場合にはコールは回線 2 にロールオーバーされ、回線 2 が通話中の場合にはコールは回線 3 にロールオーバーされます。 回線 2 または 3 は、回線 1 が通話中の場合にのみ使用可能です。 次のように話中転送の設定とビジー トリガーを使用すると、このタイプのコール機能が可能になります。 • 回線 1 で [ビジー トリガー（Busy Trigger）] を 1 に設定し、[話中転送（Call Forward Busy）] をチェーンの 2 番目の回線に設定します。 • 回線 2 で [ビジー トリガー（Busy Trigger）] を 1 に設定し、[話中転送（Call Forward Busy）] をチェーンの 3 番目の回線に設定します。 • 必要に応じて任意の数の回線でこの設定を行います。
セキュア トーン	保護されている電話では不在転送がサポートされています。
セッション ハンドオフ	ユーザがコールを切り替えると、新しいコールがデスク フォンに表示されます。 デスク フォンが点滅している場合、デスク フォンでは切り替えたコールに対する不在転送がトリガーされません。

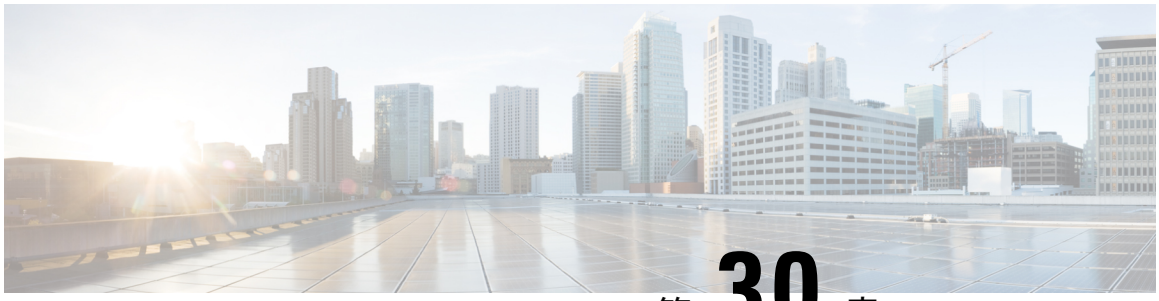
機能	データのやり取り
共有電話	不在転送（CFA）設定で共有回線を使用し、発信トランクの [リダイレクトされたパーティの外部電話番号（Redirected Party's External Phone Number)] プレゼンテーションとして [電話番号（Calling Number）] を選択した場合、共有回線で設定されている E164 の番号が異なっている場合に、表示されるリダイレクトされた番号が一致しない可能性があります。 そのため、共有回線全体で同じ E164 番号を使用することをお勧めします。

コール転送の制約事項

機能	制約事項
通話転送	• Unified Communications Manager または Cisco Unified Communications セルフ ケア ポータルで不在転送がアクティブになった場合、Unified Communications Manager は CFA ループを防止しません。 • Unified Communications Manager 不在転送ループを防止するのは、CFA が電話からアクティブにされている場合、不在転送コールのホップ数が、[転送の最大ホップ数（Forward Maximum Hop Count）] サービス パラメータに指定されている値を超えている場合、および転送チェーン内のすべての電話で（CFB、CFNA、およびその他のコール転送オプションではなく）CFA がアクティブになっている場合です。 たとえば、電話番号 1000 のユーザが電話番号 1001 に不在転送し、電話番号 1001 では CFB と CFNA が電話番号 1002 に設定されており、電話番号 1002 では CFA が電話番号 1000 に設定されている場合、Unified Communications Manager ではコールが発信されます。これは、電話番号 1002 が、電話番号 1001 の（CFA ではなく）CFB および CFNA 接続先として動作するためです。 • ボイスメール システムに不在転送する場合は、コールバックをアクティブにできません。 • [即転送（iDivert）] ソフトキーを押すと、[不在転送タイムアウト（Forward No Answer Timeout）] に関連する一般的ではない状態が発生します。 たとえば、無応答時転送タイムアウト直後にマネージャが [即転送（iDivert）] ソフトキーを押すと、コール転送によりコールが事前に設定されている電話番号に転送されます。 ただし、無応答時転送タイムアウト前にマネージャが [即転送（iDivert）] ソフトキーを押すと、即時転送によりコールがマネージャのボイスメールに転送されます。
即時転送	不在転送（CFA）と話中転送（CFB）がアクティブになっている場合、システムは即時転送をサポートしません（CFA と CFB が即時転送より優先されます）。
インターコム	インターコム コールを転送することはできません。

機能	制約事項
ハント グループからのログアウト	SIP を実行している電話（7906、7911、7941、7961）がハント グループにログインしていて [不在転送（Call Forward All）] がアクティブになっている場合、コールは SIP を実行している電話に表示されます。 SIP を実行する 7940 および 7960 IP フォンがハント グループにログインし、不在転送がアクティブな場合、この電話はスキップされ、回線グループの次の電話が呼び出されます。
論理パーティション設定	論理パーティション分割は、次の状況では行われません。 • 発信者と転送されたデバイスの両方が Voice over IP（VoIP）電話の場合。 • 地理位置情報または地理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。
マルチレベルの優先およびプリエンプション	マルチレベルの優先およびプリエンプションによる補足サービスのサポートにより、コール転送に関する次の制約事項が指定されます。 • 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 コールの話中転送（CFB）サポートにより、設定されている転送ホップの最大数までコールが転送されます。 MAP ターゲットが設定されている場合、最大ホップ数に達すると、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。

機能	制約事項
コール転送を使用したコール転送の分類	コールが転送されると、コールの分類では、元のレッグではなく、転送されたレッグの分類が行われます。 次に例を示します。 • PSTN からの着信コールは、受付によって受信されます。これは外部コールです。 • 電話を内線 3100 に転送します。転送されたコールが内部コールになります。 • 内線3100のユーザは話中ですが、外部コールを受付に送信するように外部転送が設定されています。 ただし、コールは 2 番目のレッグ（内部）の分類によって行われるため、コールはボイスメールに転送されます。



第 30 章

コール ピックアップ

コール ピックアップの概要

コール ピックアップ機能により、ユーザは自分以外の電話番号に着信したコールに応答できます。

グループ コール ピックアップの概要

グループ コール ピックアップ機能を使用すると、ユーザは別のグループ内の着信コールをピックアップできます。 Cisco Unified IP Phone からこの機能をアクティブにした場合は、ユーザが適切なコール ピックアップ グループ番号をダイヤルする必要があります。 このタイプのコール ピックアップには [G ピック（GPickUp）] ソフトキーを使用します。 ピックアップ グループに複数のコールが着信しているときに電話のグループ コール ピックアップ機能をユーザが起動すると、最も長く鳴っていた着信コールに接続されます。 電話のモデルに応じて、プログラム可能な機能ボタン [グループ ピックアップ（Group Pickup）] または [グループ ピックアップ（Group Pickup）] ソフトキーのいずれかを使用して、着信コールをピックアップします。 自動グループ コール ピックアップが有効ではない場合、ユーザは [G ピックアップ（GPickUp）] ソフトキーを押し、別のピックアップ グループのグループ番号をダイヤルし、コールに応答して接続する必要があります。

他のグループ ピックアップの概要

他のグループ ピックアップ機能により、自身のグループに関連付けられているグループ内の着信コールをピックアップできます。 Unified Communications Manager は、ユーザが Cisco Unified IP Phone からこの機能をアクティブにすると、関連グループ内で着信コールが自動的に検索して、このコールを接続します。 ユーザはこのタイプのコール ピックアップに [他 Grp（OPickUp）] ソフトキーを使用します。 自動他グループ ピックアップが有効な場合、コール

を接続するには [他 Grp（OPickUp）] および [応答（Answer）] ソフトキーを押す必要があります。 電話のモデルに応じて、プログラム可能な機能ボタン [コール ピックアップ（Call Pickup）] または [コール ピックアップ（Call Pickup）] ソフトキーのいずれかを使用して、着信コールをピックアップします。

複数の関連グループが存在する場合、1 番目の関連グループが、コール応答の優先順位が最も高いグループになります。 たとえば、グループ A、B、および C がグループ X に関連付けられている場合、コール応答の優先度はグループ A が最も高く、グループ C が最も低くなります。 グループ X はグループ A の着信コールをピックアップしますが、グループ C で、グループ A での着信コールよりも前に着信したコールがある可能性があります。

（注） 複数の着信コールが当該グループ内で発生する場合に最初にピックアップされるコールは、最も長くアラート状態になっているコール（呼び出し時間が最も長いコール）です。 他のグループ コール ピックアップ機能では、複数の関連ピックアップ グループが設定されている場合には呼び出し時間よりも優先度が優先されます。

ダイレクト コール ピックアップの概要

ダイレクト コール ピックアップ機能では、ユーザが [G ピック（GPickUp）] または [グループ ピックアップ（Group Pickup）] ソフトキーを押し、呼び出し音が鳴っているデバイスの電話番号を入力することで、その DN で呼び出し中のコールに直接応答できます。 自動ダイレクト コール ピックアップ機能が有効になっていない場合、ユーザは [G ピック（GPickUp）] ソフトキーを押し、呼び出し音が鳴っている電話の DN をダイヤルし、コールに応答する必要があります。これによりユーザの電話で呼び出し音が鳴り、接続が確立されます。Unified Communications Manager は、関連するグループ メカニズムを使用して、ダイレクト コール ピックアップを使用して着信コールに応答するユーザの権限を制御します。ユーザの関連グループによって、そのユーザが属するピックアップ グループに関連する 1 つ以上のコール ピックアップ グループが指定されます。

DN からの呼び出しコールをユーザが直接ピックアップするには、ユーザの関連グループに、その DN が属するピックアップ グループが含まれている必要があります。 2 人のユーザがそれぞれ異なる 2 つのコール ピックアップ グループに属しており、一方のユーザの関連グループにもう一方のユーザのコール ピックアップ グループが含まれていない場合、そのユーザは、もう一方のユーザからのコールをピックアップするためにダイレクト コール ピックアップを起動できません。

ユーザがダイレクト コール ピックアップ機能を起動し、DN を入力して着信コールをピックアップすると、そのユーザは指定した電話に着信するコールに接続されます。そのコールが、DN が属するコール ピックアップ グループ内で最も長く鳴っているコールかどうかは問われません。 特定の DN で複数のコールが呼び出し音を鳴らし、ユーザがダイレクト コール ピックアップを起動して DN からのコールをピックアップすると、ユーザは指定された DN で最も長く鳴っていた着信コールに接続されます。

BLF コール ピックアップの概要

BLF コール ピックアップ機能によって、Unified Communications Manager は、コールが BLF DN からの応答を待っているとき、電話をユーザに通知できます。 BLF コール ピックアップ イニシエータ（コールに応答する電話）は、次に利用可能な回線または指定された回線として選択されます。 指定された回線を使用するには、BLF SD ボタンが押されるまで、回線をオフフックのままにする必要があります。 ハント リスト メンバー DN を BLF DN として設定し、ハント リスト メンバーへの着信コールに BLF コール ピックアップ イニシエータが応答するように設定できます。 ハント リスト メンバーへの着信コールは、ハント リストからの着信の場合と、ダイレクト コールの場合があります。 それぞれのケースの動作は、ハント リスト メンバー DN、BLF DN、ハント パイロット番号に対してコール ピックアップを設定する方法によって異なります。 [有効な自動コール ピックアップ（Auto Call Pickup Enabled）] サービス パラメータが無効に設定されているときにコール ピックアップが発生した場合、電話をオフフックのままにするか、ユーザが応答キーを押してコールに応答する必要があります。

電話の BLF SD ボタンは、次のいずれかの状態になっています。

- アイドル：BLF DN へのコールがないことを示します。
- 話中：BLF DN への少なくとも 1 つのアクティブなコールがありますが、アラートは存在しないことを示します。
- アラート：BLF DN への少なくとも 1 つの着信コールがあることを点滅によって示します。

BLF DN への着信コールがある場合、BLF コール ピックアップ イニシエータである電話の BLF SD ボタンが点滅して、BLF DN への着信コールがあることを示します。 [自動コール ピックアップ（Auto Call Pickup）] が設定されている場合、ユーザがコール ピックアップ イニシエータである電話の BLF SD ボタンを押して着信コールに応答します。 自動コール ピックアップが設定されていない場合、電話をオフフックのままにするか、ユーザが応答キーを押してコールに応答する必要があります。

コール ピックアップの設定タスク 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 ピックアップ グループの設定（445 ページ）	使用するコール ピックアップ機能それぞれに、コール ピックアップ グループを設定します。 • コール ピックアップ • グループ コール ピックアップ • 他のコール ピックアップ

	コマンドまたはアクション	目的
		• ダイレクト コール ピックアップ • BLF コール ピックアップ 一意の名前と電話番号を持つグループを定義する必要があります。
ステップ 2	電話番号へのコール ピックアップ グループの割り当て （445 ページ）	コール ピックアップを有効にする電話に関連付けられた電話番号に、作成した各コール ピックアップ グループを割り当てます。 この機能を使用するには、電話番号をコール ピックアップ グループに割り当てる必要があります。 作成したコール ピックアップ グループごとにこの手順を繰り返します。
ステップ 3	別のコール ピックアップ グループを作成し、ステップ 1 （441 ページ） で作成した BLF コール ピックアップ グループに関連付けます。 1 つのコール ピックアップ グループを複数の BLF DN コール ピックアップ グループに関連付けることができます。	BLF コール ピック アップを設定している場合、この手順を実行します。 （注） 別のコール ピックアップ グループを必ず作成する必要があるわけではありません。 たとえば、イニシエータ DN と接続先 DN の両方が含まれる単独のコール ピックアップ グループを設定できます。 このような場合、BLF コール ピックアップ グループにそれ自体を関連付けます。
ステップ 4	コール ピックアップのパーティションの設定 （446 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電話番号（DN）の論理グループを作成します。 コール ピックアップ グループへのアクセスを制限するためにパーティションを使用できます。 コール ピックアップ グループ番号をパーティションに割り当てると、そのパーティションに含まれる番号にダイヤルできる電話機だけがコール ピックアップ グループを使用できます。 ダイレクト コール ピックアップでは、この手順を実行する必要があります。 他の種類のコール ピックアップではオプション。

	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 スペースの設定（447 ページ）	パーティションを設定する場合、コーリングサーチスペースも設定する必要があります。コーリングサーチスペースを設定し、発信側デバイスがコールを終了しようとする際に検索できるパーティションを指定します。 ダイレクト コール ピックアップでは、この手順を実行する必要があります。他の種類のコール ピックアップではオプション。
ステップ 6	ハント パイロットへのコール ピックアップ グループの割り当て（448 ページ）	（オプション）。回線グループ メンバーにアラートを発信するコールを取ることができるように、ハント パイロット DN にコール ピックアップ グループを割り当てます。コール ピックアップ グループに割り当てられたハント リストは、コール ピックアップ、グループ コール ピックアップ、BLF コール ピックアップ、他のグループ ピックアップ、ダイレクト コール ピックアップを使用できます。
ステップ 7	通知の設定： • コール ピックアップ通知の設定（449 ページ） • 電話番号のコール ピックアップ通知の設定（451 ページ） • BLF コール ピックアップ通知の設定（452 ページ）	（オプション）。ピックアップ グループ内の他のメンバーがコールを受信したときに通知を設定します。音声やビジュアル通知、あるいはその両方を設定できます。
ステップ 8	ダイレクト コール ピックアップの設定： • 時間帯の設定（453 ページ） • スケジュールの設定（454ページ） • パーティションとスケジュールの関連付け（454 ページ）	ダイレクト コール ピックアップを設定する前に、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必要があります。ダイレクト コール ピックアップでは、ダイレクト コール ピックアップ機能を要求したユーザのコーリング サーチ スペースに、ユーザがコールをピックアップする DN のパーティションを含める必要があります。 期間およびタイム スケジュールは、関連付けられたグループ内のメンバーが

	コマンドまたはアクション	目的
		コールに応答可能な時刻を指定します。
ステップ 9	自動コール応答の設定： • 自動コール ピックアップの設定（455 ページ） • BLF 自動ピックアップの設定（456 ページ）	（**オプション**）。自動コール応答を有効にして、自動コール応答のタイマーを設定します。
ステップ 10	電話ボタン テンプレートの設定： • コール ピックアップの電話ボタン テンプレートの設定（457ページ） • 電話機とコール ピックアップ ボタン テンプレートの関連付け（458 ページ） • BLF コール ピックアップ イニシエータの BLF 短縮ダイヤル番号の設定（458 ページ）	使用するコール ピックアップ機能向けに電話ボタンテンプレートを設定します。 • 短縮ダイヤル BLF • コール ピックアップ • グループ コール ピックアップ • 他のグループのピックアップ ダイレクト コール ピックアップでは、グループ コール ピックアップ ボタンを使用します。
ステップ 11	コール ピックアップのソフトキーの設定（459 ページ） • コール ピックアップのソフトキー テンプレートの設定（460ページ） • 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（461 ページ） • 電話機とソフトキーテンプレートの関連付け（463 ページ）	使用するコール ピックアップ機能向けにソフトキーを設定します。 • コール ピックアップ（Pickup） • グループ コール ピックアップ（GPickup） • 他のグループ ピックアップ（OPickup） ダイレクト コール ピックアップでは、グループ コール ピックアップ ソフトキーを使用します。

コール ピックアップ グループの設定

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。**[コール ルーティング（Call Routing）] > [コール ピックアップ グループ（Call Pickup Group）]** の順に選択します。
[コール ピックアップ グループの検索と一覧表示（Find and List Call Pickup Groups）] ウィンドウが表示されます。

ステップ 2 [新規追加] をクリックします。
[コール ピックアップ グループの設定（Call Pickup Group Configuration）] ウィンドウが表示されます。

ステップ 3 [コール ピックアップ グループの設定（Call Pickup Group 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。

電話番号へのコール ピックアップ グループの割り当て

ここでは、電話番号にコール ピックアップ グループを割り当てる方法について説明します。コール ピックアップ グループに割り当てられた電話番号だけが、コール ピックアップ、グループ コール ピックアップ、BLF コール ピックアップ、他のグループ ピックアップ、ダイレクト コール ピックアップを使用できます。 パーティションがコール ピックアップ番号と一緒に使用される場合、コール ピックアップ グループに割り当てられた電話番号に、適切なパーティションを含むコーリング サーチ スペースがあることを確認します。

始める前に

コール ピックアップ グループの設定 （445 ページ）

手順

ステップ 1 **[デバイス（Device）] > [電話またはコール ルーティング（Phone or Call Routing）] > [電話番号（Directory Number）]** を選択します。

ステップ 2 コール ピックアップ グループに割り当てる電話機または電話番号の検索に適した検索条件を入力し、**[検索（Find）]** をクリックします。

検索基準に一致する電話機または電話番号のリストが表示されます。

ステップ 3 コール ピックアップ グループを割り当てる電話機または電話番号を選択します。

ステップ 4 **[電話の設定（Phone Configuration）]** ウィンドウの **[関連付け情報（Association Information）]** リストから、コール ピックアップ グループを割り当てる電話番号を選択します。

ステップ 5 [コール転送およびコール ピックアップ設定（Call Forward and Call Pickup Settings）] エリアに表示される [**コール ピックアップ グループ**（**Call Pickup Group**）] ドロップダウン リストから、目的のコール ピックアップ グループを選択します。

ステップ 6 データベースに変更を保存するには、[**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。

- コール ピックアップのパーティションの設定 （446 ページ）
- コーリング サーチ スペースの設定 （447 ページ）

コール ピックアップのパーティションの設定

パーティションをコール ピックアップ グループ番号に割り当てることにより、コール ピックアップ グループへのアクセスを制限できます。 この設定を使用する場合は、コール ピックアップ グループ番号が割り当てられたパーティションを含むコーリング サーチ スペースを持つ電話機だけが、そのコール ピックアップ グループに参加できます。 パーティションとグループ番号の組み合わせがシステム全体で一意であることを確認してください。 複数のパーティションを作成できます。

コール ピックアップ グループ番号をパーティションに割り当てると、そのパーティションに含まれる番号にダイヤルできる電話機だけがコール ピックアップ グループを使用できます。 パーティションがマルチテナント構成内のテナントを表す場合は、必ず、テナントごとにピックアップ グループを適切なパーティションに割り当ててください。

始める前に

電話番号へのコール ピックアップ グループの割り当て （445 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** > **コントロールのクラス** > **パーティション**。

ステップ 2 [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 3 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。

説明にはどの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサイド（&）、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 4 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 5 [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 6 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 7 **[保存（Save）]** をクリックします。

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。

始める前に

コール ピックアップのパーティションの設定 （446 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** > **コントロールのクラス** > **コーリングサーチスペース**。

ステップ 2 [新規追加] 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、どの言語でも最大 50 文字まで指定できますが、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、**コントロール（Ctrl）**キーを押したまま、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。

ハント パイロットへのコール ピックアップ グループの割り当て

コール ピックアップ グループに割り当てられたハント リストだけが、コール ピックアップ、グループ コール ピックアップ、BLF コール ピックアップ、他のグループ ピックアップ、ダイレクト コール ピックアップを使用できます。ハント パイロットにコール ピックアップ グループを割り当てるには、次の手順を実行します。

始める前に

コーリング サーチ スペースの設定 （447 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）]** > **[ルート/ハント（Route/Hunt）]** > **[ハント パイロット（Hunt Pilot）]** の順に選択します。

ステップ 2 コール ピックアップ グループに割り当てるハント パイロットの検索に適した検索条件を入力し、**[検索（Find）]** をクリックします。 検索条件に一致するハント パイロットのリストが表示されます。

ステップ 3 コール ピックアップ グループを割り当てるハント パイロットを選択します。

ステップ 4 **[ハント転送設定（Hunt Forward Settings）]** エリアに表示される **[コール ピックアップ グループ（Call Pickup Group）]** ドロップダウン リストから、目的のコール ピックアップ グループを選択します。

ステップ 5 **[保存（Save）]** をクリックします。

コール ピックアップ通知の設定

コール ピックアップ通知は、システム レベル、コール ピックアップ グループ レベル、個々の電話レベルで設定できます。

始める前に

ハント パイロットへのコール ピックアップ グループの割り当て （448 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	コール ピックアップ グループのコール ピックアップ通知の設定 （449 ページ）	音声やビジュアルのアラートがピックアップ グループに送信される前に、元の着信側がコールをピックアップできるようにします。
ステップ 2	電話番号のコール ピックアップ通知の設定 （451 ページ）	電話がアイドルであるか、またはアクティブ コールがあるときに提供される音声アラートのタイプを設定します。
ステップ 3	BLF コール ピックアップ通知の設定 （452 ページ）	

コール ピックアップ グループのコール ピックアップ通知の設定

始める前に

ハント パイロットへのコール ピックアップ グループの割り当て （448 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）] > [コール ピックアップ グループ（Call Pickup Group）]** の順に選択します。
[**コール ピックアップ グループ（Call Pickup Group**）] ウィンドウが表示されます。

ステップ 2 [コール ピックアップ グループの設定（Call Pickup Group Configuration）] ウィンドウで、[コールピックアップグループの通知設定（Call Pickup Group Notification Settings）] セクション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、コール ピックアップのコール ピックアップ通知のフィールド （450 ページ）を参照してください。

（注） コール ピックアップの設定に影響を及ぼす機能の連携動作と制限については、**コール ピックアップの連携と制限**を参照してください。

コール ピックアップのコール ピックアップ通知のフィールド

フィールド	説明
コール ピックアップ グループ通知ポリシー（Call Pickup Group Notification Policy）	ドロップダウン リストから通知ポリシーを選択します。 選択可能なオプションは、[アラートなし（No Alert）]、[オーディオ アラート（Audio Alert）]、[ビジュアル アラート（Visual Alert）]、および [オーディオおよびビジュアルアラート（Audio and Visual Alert）] です。
コール ピックアップ グループ通知タイマー（Call Pickup Group Notification Timer）	コールが最初に元の着信側に着信したときから、コール ピックアップ グループの残りの番号に通知が送信されるまでの時間差の秒数（1 ～ 300 の範囲の整数）を入力します。
[発呼側情報(Calling Party Information)]	コール ピックアップ グループへのビジュアル通知メッセージに発呼側の ID を加えるには、このチェックボックスをオンにします。[コールピックアップグループ通知ポリシー(Call Pickup Group Notification Policy)] が [ビジュアルアラート(Visual Alert)] または [オーディオおよびビジュアルアラート(Audio and Visual Alert)] に設定されている場合にだけ、この設定を使用できます。 （注） 通知はデバイスのプライマリ回線だけに送信されます。
[着信側情報（Called Party Information）]	コール ピックアップ グループへのビジュアル通知メッセージに元の着信側の ID を加えるには、このチェックボックスをオンにします。[コールピックアップグループ通知ポリシー(Call Pickup Group Notification Policy)] が [ビジュアルアラート(Visual Alert)] または [オーディオおよびビジュアルアラート(Audio and Visual Alert)] に設定されている場合に、この設定を使用できます。

電話番号のコール ピックアップ通知の設定

電話機がアイドル状態または使用中に提供される音声通知の種類を設定するには、次の手順を実行します。

始める前に

コール ピックアップ グループのコール ピックアップ通知の設定 （449 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）]** > **[電話番号（Directory Number）]** を選択します。
[電話番号の検索/一覧表示（Find and List Directory Numbers）]ウィンドウが表示されます。

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 コール ピックアップ通知を設定する電話番号をクリックします。
[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 [関連付けられたデバイス（Associated Devices）]ペインでデバイス名を選択し、[ライン アピアランスの編集（Edit Line Appearance）]ボタンをクリックします。
[電話番号の設定（Directory Number Configuration）]ウィンドウが更新され、選択したデバイスの DN に対するライン アピアランスが表示されます。

ステップ 5 [コール ピックアップ グループのオーディオ アラート設定（電話アイドル）（Call Pickup Group Audio Alert Setting(Phone Idle)）]ドロップダウン リストで、次のいずれかを選択してください。

- [システムデフォルトの使用（Use System Default）]
- [無効（Disable）]
- [一度鳴らす（Ring Once）]

ステップ 6 [コール ピックアップ グループのオーディオ アラート設定（電話アクティブ）（Call Pickup Group Audio Alert Setting(Phone Active)）]ドロップダウン リストで、次のいずれかを選択してください。

- [システムデフォルトの使用（Use System Default）]
- [無効（Disable）]
- [ビープ音のみ（Beep Only）]

ステップ 7 **[保存（Save）]** をクリックします。

BLF コール ピックアップ通知の設定

始める前に

電話番号のコール ピックアップ通知の設定 （451 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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

ステップ 2 [サーバ（Server）] ドロップダウン リストで、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 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、クラスタ全体に対するパラメータ（[デバイス（Device）] - [電話（Phone）]）セクション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、BLF コール ピックアップ通知のサービス パラメータ フィールド （452 ページ）を参照してください。

BLF コール ピックアップ通知のサービス パラメータ フィールド

フィールド	説明
[アイドル ステーションのコール ピックアップ グループ オーディオ アラートの設定（Call Pickup Group Audio Alert Setting of Idle Station）]	このパラメータは、電話がアイドル状態（使用されていない状態）であり、そのコール ピックアップ グループでの着信コールについてアラートが必要な場合に提供されるオーディオ通知の種類を決定します。 有効な値は、次のとおりです。 • [無効（Disable）] • [一度鳴らす（Ring Once）]
[ビジー ステーションのコール ピックアップ グループ オーディオ アラートの設定（Call Pickup Group Audio Alert Setting of Busy Station）]	このパラメータは、電話がビジー状態（使用されている状態）であり、そのコール ピックアップ グループでの着信コールについてアラートが必要な場合に提供されるオーディオ通知の種類を決定します。 有効な値は、次のとおりです。 • [無効（Disable）] • [ビープ音のみ（Beep Only）]

フィールド	説明
[アイドル ステーションの BLF ピックアップ グループ オーディオ アラートの設定（BLF Pickup Group Audio Alert Setting of Idle Station）]	このパラメータは、電話がアイドル状態であり、BLF ピックアップ ボタンでの着信コールについてアラートが必要な場合に提供されるオーディオ通知の種類を決定します。 有効な値は、次のとおりです。 • [呼出音なし（No Ring）] • [一度鳴らす（Ring Once）]
[ビジー ステーションの BLF ピックアップ グループ オーディオ アラートの設定（BLF Pickup Group Audio Alert Setting of Busy Station）]	このパラメータは、電話がビジー状態であり、BLF ピックアップ ボタンでの着信コールについてアラートが必要な場合に提供されるオーディオ通知の種類を決定します。有効な値は、次のとおりです。 • [呼出音なし（No Ring）] • [ビープ音のみ（Beep Only）]

ダイレクト コール ピックアップの設定

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 （453 ページ）	自分のグループに関連付けられたグループのメンバーの時間帯を設定します。
ステップ 2	スケジュールの設定 （454 ページ）	自分のグループに関連付けられたグループのメンバーのスケジュールを設定します。
ステップ 3	パーティションとスケジュールの関連付け （454 ページ）	特定の時間内にコールを完了しようとする場合、パーティションとスケジュールを関連付けてコーリング デバイスの検索が行われ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。

スケジュールの設定

始める前に

時間帯の設定 （453 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）] > [タイムスケジュール（Time Schedule）]**。

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、オンライン ヘルプを参照してください。

パーティションとスケジュールの関連付け

特定の時間中にコールを完了しようとする場合、パーティションとスケジュールを関連付けてコーリング デバイスの検索が行われる場所を決定します。

始める前に

スケジュールの設定 （454 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）] > [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。

自動コール応答の設定

手順

	コマンドまたはアクション	目的
ステップ 1	自動コール ピックアップの設定 （455 ページ）	コール ピックアップ、グループ ピックアップ、その他のグループ ピックアップ、ダイレクト コール ピックアップ、および BLF コール ピックアップを自動化できます。 自動コール応答が有効になっていない場合は、追加のソフトキーまたはダイヤル グループ番号を押して接続を完了する必要があります。
ステップ 2	BLF 自動ピックアップの設定 （456 ページ）	

自動コール ピックアップの設定

自動コール ピックアップは、ユーザを着信コールに接続します。ユーザが電話機でソフトキーを押すと、Unified Communications Manager はグループ内の着信コールを検索し、コール接続を実行します。 コール ピックアップ、グループ ピックアップ、その他のグループ ピックアップ、ダイレクト コール ピックアップ、および BLF コール ピックアップを自動化できます。自動コール応答が有効になっていない場合は、追加のソフトキーまたはダイヤル グループ番号を押して接続を完了する必要があります。

始める前に

パーティションとスケジュールの関連付け （454 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。**[システム（System）]** > **[サービス パラメータ（Service Parameters）]**。

ステップ 2 [サーバ（Server）] ドロップダウン リストで、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（機能 - コール ピックアップ）（Clusterwide Parameters (Feature – Call Pickup)）]セクションで、[自動コール ピックアップ有効化（Auto Call Pickup Enabled）]ドロップダウン リストから [はい（True）]または [いいえ（False）]を選択して、コール ピックアップ グループの自動コール応答を有効または無効にします。

ステップ 5 [自動コール コールピックアップ有効化（Auto Call Pickup Enabled）]サービス パラメータが [いいえ（False）] の場合は、[コール ピックアップ無応答タイマー（Call Pickup No Answer Timer）] フィールドに 12 ー 300 の値を入力します。 このパラメータによって、コール ピックアップ、グループ コール ピックアップ、またはその他のグループ コール ピックアップを使用してコールがピックアップされたものの応答されなかった場合に、コールが復元されるまでの時間が制御されます。

ステップ 6 [**ピックアップの場所タイマー（Pickup Locating Timer**）] フィールドに 1~5 の値を入力します。このサービス パラメータは、クラスタ内のすべてのノードからのすべてのアラート コールを Cisco Unified Communications Manager コールを識別するための最大時間（秒）を指定します。その後、この情報は、キュー内で最も長く待機していたコールを、PickUp、GPickUp、または OPickUp ソフトキーを押した次のユーザに確実にまわすために使用されます。

ステップ 7 **[保存（Save）]** をクリックします。

BLF 自動ピックアップの設定

始める前に

自動コール ピックアップの設定 （455 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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

ステップ 2 [サーバ（Server）] ドロップダウン リストで、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 次のクラスタ全体のサービス パラメータの値を設定します。

- アイドル状態のステーションの BLF ピックアップ オーディオ アラート設定：コール ピックアップ グループの自動コール応答を有効または無効にするには、ドロップダウン リストから [True]または [False]を選択します。 このサービス パラメータのデフォルト値は [いいえ（FALSE）] です。
- 使用中のステーションの BLF ピックアップ オーディオ アラートの設定：自動コール ピックアップ有効化サービス パラメータを [False] にする場合、12 ～ 300 の値を入力します（包括的）。 このパラメータによって、コール ピックアップ、グループ コール ピックアッ

プ、またはその他のグループ コール ピックアップを使用してコールがピックアップされたものの応答されなかった場合に、コールが復元されるまでの時間が制御されます。

コール ピックアップの電話ボタンの設定

手順

	コマンドまたはアクション	目的
ステップ 1	コール ピックアップの電話ボタン テンプレートの設定 （457 ページ）	電話ボタン テンプレートにコール ピックアップ機能を追加します。
ステップ 2	電話機とコール ピックアップ ボタン テンプレートの関連付け （458 ページ）	
ステップ 3	BLF コール ピックアップ イニシエータの BLF 短縮ダイヤル番号の設定 （458 ページ）	

コール ピックアップの電話ボタン テンプレートの設定

電話ボタン テンプレートにコール ピックアップ機能を追加するには、次の手順に従います。

始める前に

自動コール応答の設定 （455 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）]** > **[電話ボタンテンプレート（Phone button template）]** の順に選択します。

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]** 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]** をクリックします。

ステップ 7 次のいずれかの作業を実行します。

- 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。

電話機とコール ピックアップ ボタン テンプレートの関連付け

始める前に

コール ピックアップの電話ボタン テンプレートの設定 （457 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]** 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。

BLF コール ピックアップ イニシエータの BLF 短縮ダイヤル番号の設定

始める前に

電話機とコール ピックアップ ボタン テンプレートの関連付け （458 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 BLF コール ピックアップ イニシエータとして使用したい電話を選択します。

ステップ 3 [**関連付け（Association）**] ペインで、[**BLF SD 新規追加（Add a new BLF SD）**] リンクを選択します。
[**話中ランプ フィールド短縮ダイヤル設定（Busy Lamp Field Speed Dial Configuration**）] ウィンドウが表示されます。

ステップ 4 BLF DN ボタンでモニタする [**電話番号（Directory Number**）]（BLF DN）を選択します。

ステップ 5 BLF コール ピックアップと BLF 短縮ダイヤルに BLF SD ボタンを使用する場合は、[**コール ピックアップ（Call Pickup**）] 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フにすると、BLF SD ボタンは、BLF 短縮ダイヤルにのみ使用されます。

ステップ 6 **[保存（Save）]** をクリックします。

コール ピックアップのソフトキーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	コール ピックアップのソフトキー テンプレートの設定 （460 ページ）	ソフトキー テンプレートに、Pickup、GPickup、および OPickup ソフトキーを追加します。
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 （461 ページ）を行うには、次のサブタスクを完了します。 • 共通デバイス設定へのソフトキー テンプレートの追加 （462 ページ） • 電話機と共通デバイス設定の関連付け （462 ページ）	（**オプション**） 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	電話機とソフトキー テンプレートの関連付け （463 ページ）	（**オプション**）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。

コール ピックアップのソフトキー テンプレートの設定

次の手順を使用して、以下のコール ピックアップ ソフトキーを使用できるようにします。

ソフトキー	説明	コール状態
コール ピックアップ（[Pickup]）	グループ内の別の内線へのコールに応答できます。	オンフック（On Hook） オフフック（Off Hook）
グループ コール ピックアップ（[GPickup]）	グループ外の内線へのコールに応答できます。	オンフック（On Hook） オフフック（Off Hook）
他のグループ ピックアップ（[OPickup]）	グループに関連付けられている他のグループで呼び出し中のコールに応答できます。	オンフック（On Hook） オフフック（Off Hook）

始める前に

コール ピックアップの電話ボタンの設定 （457 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）] > [ソフトキー テンプレート（Softkey Template）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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

次のいずれかの作業を実行します。

- 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 （461 ページ）
- 電話機とソフトキー テンプレートの関連付け （463 ページ）

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

（オプション） 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）]** に追加します。
- ソフトキー テンプレートを**共通デバイス設定**に追加します。

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 （463ページ）」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 （462 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 （462 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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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

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。

コール ピックアップの連携動作

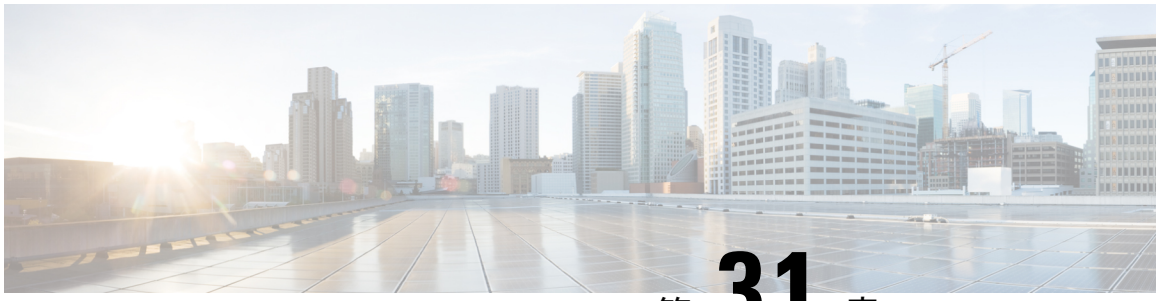
機能	データのやり取り
ルート プラン レポート	ルート プラン レポートには、Unified Communications Manager で設定されているパターンと DN が表示されます。 DN をコール ピックアップ グループに割り当てる前に、ルート プラン レポートを使用して、重複しているパターンと DN を探します。
コーリング サーチ スペースとパーティション	パーティションをコール ピックアップ グループ番号に割り当てると、デバイス コーリング サーチ スペースに基づいて、ユーザへのコール ピックアップ アクセスが制限されます。
時刻（TOD）	関連付けられたグループのメンバーの [時刻（Time of Day）]（TOD）パラメータにより、メンバーは自分のグループと同じ時間帯にコールを受け付けることができます。 TOD はタイムスタンプをコーリング サーチ スペースとパーティションに関連付けます。

機能	データのやり取り
コールアカウンティング	コール ピックアップが自動コール ピックアップを通じて発生すると、システムにより 2 つのコール詳細レコード（CDR）が生成されます。CDR の 1 つはクリアされる元のコールに適用され、もう 1 つの CDR は接続される要求コールに適用されます。 コール ピックアップが非自動コール ピックアップで発生すると、システムにより 1 つのコール詳細レコードが生成され、接続される要求コールに適用されます。 CDR 検索は、特定の時間範囲とその他の検索条件に一致するすべての CDR を返します。 特定の CDR に関連付けられるタイプのコールを検索することもできます。検索結果にはコールがピックアップ コールかどうかを示すコール タイプ フィールドが表示されます。
通話転送	サービス パラメータ [自動コール ピックアップ有効化（Auto Call Pickup Enabled）] が false に設定された状態でコール ピックアップが発生した場合、いずれかのピックアップ ソフトキーが押されると、電話機に設定されたコール転送は無視されます。 コール ピックアップ依頼者がコールに応答しない場合、ピックアップ無応答タイマーが切れた後、元のコールが復元されます。

コール ピックアップの制限

制約事項	説明
異なるコール ピックアップ グループへの別個の電話回線	異なるコール ピックアップ グループに電話の別個の回線を割り当てることもできますが、ユーザには複雑であるため、シスコはこの設定をお勧めしません。
コール ピックアップ グループ番号	• コール ピックアップ グループ番号は、回線または DN に割り当てられると削除できません。 どの行がどのコール ピックアップ グループ番号を使用しているかを決定するには、[コール ピックアップ構成（Call Pickup Configuration）]ウィンドウの [依存関係レコード（Dependency Records）] を使用します。 コール ピックアップ グループ番号を削除するには、各回線または DN に新しいコール ピックアップ グループ番号を再割り当てします。 • コール ピックアップ グループ番号を更新すると、Cisco Unified Communications Manager はそのコール ピックアップ グループに割り当てられているすべての電話番号を自動的に更新します。

制約事項	説明
SIP 電話機	• SIP を実行するいくつかの Cisco Unified IP 電話 では、コール ピックアップの通知をサポートしていません。 • コール ピックアップの通知がサポートされるのは、SIP を実行するライセンスが付与された、サード パーティの電話のみです。
ダイレクト コール ピックアップ	• ハント パイロット番号の呼び出しにより行われたコールによりハント リストに属するデバイスが鳴っている場合、ユーザはダイレクト コール ピックアップ機能を使用してそのようなコールに応答することはできません。 • 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。
BLF ピックアップ	SIP を実行するいくつかの Cisco Unified IP 電話 では、コール ピックアップの通知をサポートしていません。
着信発呼者の国際番号プレフィックス - 電話	プレフィックスを 「[着信発呼者の国際番号プレフィックス-電話（Incoming Calling Party International Number Prefix - Phone）]」サービス パラメータに設定していて、国際コールがコール ピックアップ グループ内のあるメンバーに発信される場合に、コール ピックアップ グループ内の別のメンバーがそのコールに応答すると、プレフィックスは発信側のフィールドに呼び出されません。



第 31 章

コール パークとダイレクト コール

コール パークの概要

コールパーク機能を使用すると、コールを保留にして、Unified Communications Manager システム内の別の電話機（たとえば、別のオフィスの電話機や、会議室の電話機）から取得できます。 アクティブ コールに対応している場合は、[パーク（Park）] ソフトキーを押すと、そのコールをコール パーク内線番号にパークできます。 システム内の別の電話からコール パーク内線番号にダイヤルして、その通話を受けることができます。

コール パーク内線番号として使用するために、単一のディレクトリ番号を定義することも、ディレクトリ番号の範囲を定義することもできます。 各コール パーク内線番号にパークできるコールは 1 つだけです。

コール パーク機能は Unified Communications Manager クラスタ内で機能します。クラスタ内の各 Unified Communications Manager ノードにはコール パーク内線番号が定義されている必要があります。 コール パーク内線番号として使用するために、単一のディレクトリ番号を定義することも、ディレクトリ番号の範囲を定義することもできます。 電話番号または番号範囲が一意であることを確認します。 異なるパーティションで同じパーク範囲を使用する場合、ユーザーの CSS に、コールのパークと取得ができるパーティションが 1 つだけであることを確認

します。 複数のパーティションがある場合、誤ったパーティションが選択される可能性があります。

ユーザは、割り当てられているルート パターン（例：クラスタ間トランクのルート パターンは80XX）とコール パーク番号（例：8022）にダイヤルし、別のUnified Communications Managerクラスタからパークされているコールを取得できます。 コーリング サーチ スペースとパーティションが正しく設定されていることを確認する必要があります。 コール パークはクラスタ間で機能します。

有効なコール パーク内線番号は、整数とワイルドカード文字 X からなります。コール パーク内線番号には最大でXXを設定できます（例：80XX）。これにより、最大100件のコール パーク内線番号を提供できます。 コールがパーク中になると、Unified Communications Manager は次に使用可能なコールパーク内線番号を選択し、電話にその番号を表示します。

パーク モニタリング

パーク モニタリングは、タイマーが期限切れになるまで Cisco Unified Communications Manager がパークされたコールのステータスをモニタする、オプションのコール パーク機能です。 タイマーが期限切れになると、コールは事前に設定されている番号に転送されるか、ボイスメールに送信されるか、またはコールのパーク元に戻ります。 パーク モニタリングは電話回線とハント パイロットに適用できます。

コール パークの前提条件

クラスタ間でコール パークを使用する場合は、パーティションとコーリング サーチ スペースを設定しておく必要があります。

表 *29 :* パーク ソフトキー テンプレートとコール パーク ボタン テンプレートをサポートしている *Cisco Unified IP Phone*

電話機のモデル	ソフトキー テンプレートでのサポート	電話ボタン テンプレートでのサポート
Cisco Unified IP 電話s 6900 シリーズ（6901 および 6911 を除く）	X	X
Cisco IP 電話 7800 シリーズ	X	X
Cisco Unified IP 電話s 7900 シリーズ（7921、7925、7936、7937 を除く）	X	
Cisco IP 電話 8800 シリーズ	X	X
Cisco Unified IP 電話s 8900 シリーズ	X	X

電話機のモデル	ソフトキー テンプレートでのサポート	電話ボタン テンプレートでのサポート
Cisco Unified IP 電話s 9900 シリーズ	X	X
Cisco Unified IP 電話s 7900 シリーズ（7906、7911、7921、7925、7936、7937 を除く）		X

（注） プログラム可能な回線キー機能を使用して、回線 1 以外のすべての回線またはボタンでコールパークを設定できます。

コール パークの設定タスク フロー

始める前に

- コール パークの前提条件 （468 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	クラスタ全体のコール パークの設定（470 ページ）	**（オプション）。** クラスタ全体のコール パークを設定するか、ステップ 3 の手順を使用してクラスタ内のサーバにコール パークを設定します。
ステップ 2	コール パークのパーティションの設定（471 ページ）	コールパーク番号を追加するためのパーティションを作成します。
ステップ 3	コール パーク番号の設定 （472 ページ）	クラスタ内のサーバでコール パークを使用するためのコール パーク番号を設定します。
ステップ 4	コール パークのソフトキー テンプレートの設定 （475 ページ）	ソフトキー テンプレートに [パーク（Park）] ソフトキーを追加します。
ステップ 5	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 （476 ページ）を行うには、次のサブタスクを完了します。 • 共通デバイス設定へのソフトキー テンプレートの追加 （477 ページ）	**オプション。** 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

	コマンドまたはアクション	目的
	• 電話機と共通デバイス設定の関連付け （478 ページ）	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 6	電話機とソフトキーの関連付け （478 ページ）	**オプション。** 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 7	コール パーク ボタンの設定 （479 ページ）を行うには、次のサブタスクを完了します。 • コール パークの電話ボタン テンプレートの設定 （479 ページ） • 電話機とボタン テンプレートの関連付け （479 ページ）	
ステップ 8	パーク モニタリングの設定 （480 ページ）	次のオプションのタスク フローを実行して、コール パークの設定にパーク モニタリングを追加します。

クラスタ全体のコール パークの設定

手順

ステップ 1 **[System（システム）]** > **[Service Parameters（サービス パラメータ）]** を選択します。

ステップ 2 目的のノードを [サーバ（Server）]、サービスを [Cisco CallManager]（アクティブ）として選択します。

ステップ 3 **詳細設定**をクリックします。

詳細サービスパラメータがウィンドウに表示されます。

ステップ 4 クラスタ全体のパラメータ（機能 - 全般) セクションで、**クラスタ全体のコールパーク番号/範囲の有効化**を**True**に設定します。

デフォルト値は [False] です。 このパラメータは、コール パーク機能をクラスタ全体に適用するか、または特定の Unified CM ノードに制限するかを決定します。

ステップ 5 Cisco CallManager サービスとコールパークが設定されているクラスタ内の各サーバに対して、**コール パーク表示タイマー**を設定します。

デフォルトは 10 秒です。 このパラメータでは、コールをパークした電話機でコールパーク番号を表示する時間を決定します。

ステップ 6 Unified Communications Managerサービスとコールパークが設定されているクラスタ内の各サーバに対して、**コールパーク復帰タイマー**を設定します。

デフォルトは 60 秒です。 このパラメータでは、コールをパーク状態に維持する時間を決定します。 このタイマーの期限が切れると、パークされたコールは、コールをパークしたデバイスに返されます。 ハント グループ メンバーがハント パイロットを通じて着信したコールをパークした場合、そのコールはコール パーク復帰タイマーの期限が切れた時点でハント パイロットに返されます。

（注） コール パーク表示タイマーよりも小さな値をコール パーク復帰タイマーに入力した場合は、コール パーク番号が電話機に表示されないことがあります。

ステップ 7 **[保存（Save）]** をクリックします。

ステップ 8 すべての Unified Communications Manager と CTI Manager サービスを再起動します。

コール パーク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。

始める前に

（オプション） クラスタ全体のコール パークの設定 （470 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 > コントロールのクラス > パーティション**。

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。

説明にはどの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサイド（&）、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。

コール パーク番号の設定

クラスタ内の複数のサーバにわたってコール パークを使用する場合は、各サーバにコール パーク内線番号を設定する必要があります。

各コールパーク電話番号、パーティション、および範囲が Unified Communications Manager 内で固有であることを確認してください。 登録Unified Communications Managerされているデバイスごとに、固有のコールパークディレクトリの番号と範囲が必要です。Cisco Unified Communications Manager Administrationコールパークの設定に使用するコールパークの番号または範囲を検証しません。 無効な番号や範囲、また重複の可能性がある範囲を特定するには、Unified Communications Manager着信番号アナライザツールを使用します。

始める前に

コール パークのパーティションの設定 （471 ページ）

手順

ステップ 1 **[コール ルーティング（Call Routing）]** > **[コール パーク（Call Park）]** 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。

- 新しいコール パーク番号を追加するには、[新規追加] をクリックします。
- コール パーク番号をコピーするには、コール パーク番号または番号の範囲を検索して、[コピー（Copy）]アイコンをクリックします。
- コール パーク番号を更新するには、コール パーク番号または番号の範囲を検索します。

[コール パーク番号の設定（Call Park number configuration）] ウィンドウが表示されます。

ステップ 3 [コール パークの設定（Call Park configuration）] フィールド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、コール パーク設定フィールド（474 ページ）を参照してください。

ステップ 4 新しいコール パーク番号や変更したコール パーク番号を保存するには、[保存（Save）]をクリックします。

コール パーク設定フィールド

フィールド	説明
[コールパーク番号/範囲(Call Park Number/Range)]	コール パーク内線番号を入力します。 数字またはワイルドカード文字 X を入力することもできます（1 つまたは 2 つの X を使用できます）。 たとえば、5555 と入力して 5555 という 1 つのコールパーク内線番号を定義するか、または 55XX と入力して 5500 ～ 5599 のコール パーク内線番号の範囲を定義します。 （注） 1 つのコール パーク範囲の定義で、最大 100 のコール パーク番号を作成できます。 コール パーク番号が一意になっていることを確認します。 （注） Unified Communications Manager サーバ間でコール パーク番号が重複することがないようにしてください。 各 Unified Communications Manager サーバの番号範囲は固有である必要があります。 （注） コール パーク範囲は、コールの発信元のサーバのリストから選択されます。 たとえば、電話機 A （ノード A に登録）が電話機 B （ノード B に登録）にコールし、電話機 B のユーザが [パーク(Park)] を押した場合、電話機 B ではノード A に存在する CSS のコール パーク範囲が必要になります。 マルチノード環境では、電話およびゲートウェイがさまざまなノードと通信し、発信元のサーバを問わずコールのパークが必要になる場合があるため、電話機にはすべてのサーバからのコール パーク範囲が含まれている CSS が必要です。
説明	このコール パーク番号に簡単な説明を付けます。 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。

フィールド	説明
パーティション	パーティションを使用してコール パーク番号へのアクセスを制限する場合は、ドロップダウン リストから必要なパーティションを選択します。 コール パーク番号へのアクセスを制限しない場合は、パーティションに対して [<None>] を選択します。 （注） コールパーク内線番号とパーティションの組み合わせが、Unified Communications Manager内で固有であることを確認してください。
Unified Communications Manager	ドロップダウン リストを使用して、これらのコール パーク番号を適用する Cisco Unified Communications Manager を選択します。

コール パークのソフトキー テンプレートの設定

以下の手順を使用して、**パーク** ソフトキーを使用できるようにします。

パーク ソフトキーには次のコール状態があります。

- オンフック（On Hook）
- 発信（Ring Out）
- 接続転送（Connected Transfer）

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）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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。

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

（オプション） 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）]** に追加します。
- ソフトキー テンプレートを**共通デバイス設定**に追加します。

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 （477 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 （478 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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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の関連付け

（オプション） 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。

コール パーク ボタンの設定

コール パークの電話ボタン 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）]** の順に選択します。

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]** 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]** をクリックします。

ステップ 7 次のいずれかの作業を実行します。

- 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

コール パークの電話ボタン テンプレートの設定 （479 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]** 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。

パーク モニタリングの設定

次のオプション タスクを実行して、コール パーク設定にパーク モニタリングを追加します。

始める前に

パーク モニタリングは、コール パークをサポートする電話のサブセットでのみサポートされます。 次の Cisco Unified IP Phone は、パーク モニタリングをサポートしています。

- Cisco IP 電話 8811
- Cisco IP 電話 8841
- Cisco IP 電話 8845
- Cisco IP 電話 8851
- Cisco IP 電話 8851NR
- Cisco IP 電話 8861
- Cisco IP 電話 8865
- Cisco IP 電話 8865NR
- Cisco Unified IP 電話 8961
- Cisco Unified IP 電話 9951
- Cisco Unified IP 電話 9971

手順

	コマンドまたはアクション	目的
ステップ 1	パーク モニタリング システム タイマーの設定 （481 ページ）	パーク モニタリング機能のシステム レベルのタイマーを設定します。
ステップ 2	ハント パイロットのパーク モニタリングの設定 （482 ページ）	**オプション。** ハント パイロットを展開している場合は、ハント パイロットに

	コマンドまたはアクション	目的
		パーク モニタリングの接続先を割り当てます。
ステップ 3	電話番号のパーク モニタリングの設定（483 ページ）	個々の電話回線のパーク モニタリングの接続先を割り当てます。
ステップ 4	ユニバーサル回線テンプレートを使用したパーク モニタリングの設定（484 ページ）	LDAP ディレクトリ同期を設定していると、パーク モニタリングが設定されている複数のユーザの電話番号設定のプロビジョニングにユニバーサル回線のテンプレートを使用できます。

パーク モニタリング システム タイマーの設定

パーク モニタリング機能のシステム レベルのタイマーを設定するには、次の手順を使用します。

手順

ステップ 1 [Cisco Unified CM 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）]**。

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 次のサービス パラメータの値を設定します。

- [パーク モニタリング復帰タイマー（Park Monitoring Reversion Timer）]：パークしたコールを取得するようにユーザに求めるまで、Cisco Unified Communications Manager が待機する秒数。 個々の電話回線では、この設定は、**[電話番号の設定]** ウィンドウの同じ設定によりオーバーライドされます。 コール パーク復帰タイマーの期限が切れると、コールはハントパイロットに転送されます。
- [パーク モニタリング定期復帰タイマー（Park Monitoring Periodic Reversion Timer）]：コールがパークしたときに復帰を試行する秒数。 Cisco Unified Communications Manager は、パークしたユーザの電話を鳴らしたり、ビープ音を再生したり、点滅させたりすることでユーザにパークしたコールについて求めます。 パークモニタリング復帰タイマーの期限が切れると、コールはハントパイロットではなく、パークされた相手側に転送されます。
- **[パーク モニタリング転送非取得時のタイマー（Park Monitoring Forward No Retrieve Timer）]**：パーク アラーム通知が発生するまでの秒数。その後、パークされたコールは、コールをパークしたユーザが [電話番号の設定（Directory Number Configuration）] で指定した**未取得時のパーク モニタリング転送**の接続先に転送されます。 パークモニタリング転送復帰タイマーが期限切れになると、コールはハントパイロットに転送されます。

（注） これらのフィールドの詳細については、サービス パラメータのオンライン ヘルプを参照してください。

ステップ 5 **[保存]** をクリックします。

次のタスク

これらのオプションのいずれかのタスクを使用して、個々の電話回線およびハントパイロットでの期限切れのタイマーの処理方法を指定します。

- ハント パイロットのパーク モニタリングの設定 （482 ページ）
- 電話番号のパーク モニタリングの設定 （483 ページ）
- ユニバーサル回線テンプレートを使用したパーク モニタリングの設定 （484 ページ）

ハント パイロットのパーク モニタリングの設定

展開でハント パイロットを使用している場合は、このオプションの手順を使用して、ハント パイロットにパーク モニタリングの接続先を割り当てます。

（注） ハント パイロットの設定の概要については、Cisco Unified Communications Manager システム設定ガイド の「ハント パイロットの設定」の章を参照してください。

始める前に

パーク モニタリング システム タイマーの設定 （481 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）]** > **[ルート/ハント（Route/Hunt）]** > **[ハント パイロット（Hunt Pilot）]** の順に選択します。

ステップ 2 [検索（Find）] をクリックして、パーク モニタリングの接続先を設定するハント パイロットを選択します。

ステップ 3 [パーク モニタリング非取得時の接続先（Park Monitoring No Retrieve Destination）] フィールドで、[接続先（Destination）] の電話番号と [コーリング サーチ スペース（Calling Search Space）] を割り当てます。

ステップ 4 [ハント パイロットの設定（Hunt Pilot Configuration）] ウィンドウの残りのフィールドに入力します。フィールドと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。

電話番号のパーク モニタリングの設定

個々の電話回線でパーク モニタリングの接続先を割り当てるには、次の手順を使用します。コールを別の番号に転送したり、ボイスメールに送信したり、コールのパーク元に戻したりすることができます。

（注） 次のツールは、複数の電話回線の設定をプロビジョニングすることができます。

- ユニバーサル回線のテンプレートを使用して、LDAP ディレクトリの同期によって、複数の電話回線のパーク モニタリング設定をプロビジョニングします。 詳細については、ユニバーサル回線テンプレートを使用したパーク モニタリングの設定（484 ページ）を参照してください。
- 一括管理ツールを使用して、多数の電話回線の設定を含む CSV ファイルをインポートします。 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

パーク モニタリング システム タイマーの設定 （481 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）] > [電話番号（Directory Number）]** を選択します。

ステップ 2 [検索（Find）] をクリックして、設定する電話番号を選択します。

ステップ 3 次の [パーク モニタリング（Park Monitoring）] フィールドに値を入力します。

- [パーク モニタリング転送非取得時の接続先（外部）（Park Monitoring Forward No Retrieve Destination External）]：パーク モニタリング転送非取得時のタイマー期限が切れ、パーク先が外部パーティの場合、コールはボイスメールまたは指定した電話番号に転送されます。 このフィールドが空の場合、コールはコールをパークした人の回線に転送されます。
- [パーク モニタリング転送非取得時の接続先（外部）（Park Monitoring Forward No Retrieve Destination External）]：パーク モニタリング転送非取得時のタイマー期限が切れ、パーク先が内部パーティの場合、コールはボイスメールまたは指定した電話番号に転送されます。 このフィールドが空の場合、コールはコールをパークした人の回線に転送されます。
- [パーク モニタリング復帰タイマー（Park Monitor Reversion Timer）]：この電話回線でパークしたコールを取得するようにユーザに求めるまで、Cisco Unified Communications Manager が待機する秒数。 値が 0 または空の場合、Cisco Unified Communications Manager は [パー

ク モニタリング復帰タイマー（Park Monitor Reversion Timer）] サービス パラメータの値を使用します。

ステップ 4 **[ディレクトリ番号の設定（Directory Number Configuration）]** ウィンドウフィールドと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。で、残りのフィールドを入力します。

ステップ 5 **[保存（Save）]** をクリックします。

ユニバーサル回線テンプレートを使用したパーク モニタリングの設定

ユニバーサル回線テンプレートにパーク モニタリングの設定を割り当てるには、次の手順を使用します。 LDAP ディレクトリ同期を設定していると、複数のユーザに設定されたパーク モニタリングの電話番号の設定のプロビジョニングにユニバーサル回線のテンプレート設定を使用できます。

始める前に

パーク モニタリング システム タイマーの設定 （481 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。**[ユーザ管理（User Management）]** > **[ユーザ電話/追加（User/Phone Add）]** > **[ユニバーサル回線テンプレート（Universal Line Template）]**。

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、既存のテンプレートを選択します。
- [新規追加（Add New）] をクリックして新しいテンプレートを作成します。

ステップ 3 セクションを展開し、フィールドに入力します。フィールドの説明については、ユニバーサル回線テンプレートのパーク モニタリング設定 （485 ページ）を参照してください。

ステップ 4 **[保存]** をクリックします。

次のタスク

個々の電話番号にユニバーサル回線テンプレートを適用するには、ユーザ プロファイル、機能グループ テンプレート、および LDAP ディレクトリ同期にテンプレートを割り当てる必要があります。 同期が発生すると、テンプレートの設定は同期の一部である電話回線に適用されます。 LDAP の設定については、Cisco Unified Communications Manager システム設定ガイドの「エンド ユーザの設定」の章を参照してください。

ユニバーサル回線テンプレートのパーク モニタリング設定

次の表に、Cisco Unified Communications Manager の [ユニバーサル回線テンプレートの設定（Universal Line Template Configuration）]ウィンドウの [パーク モニタリング（Park Monitoring）] フィールドを示します。

表 *30*：ユニバーサル回線テンプレートのパーク モニタリング設定

フィールド	説明
[未取得時の外線コールの転送先（Forward Destination for External Calls When Not Retrieved）]	コールがパーク保留されている人物が外部の人であり、[パーク モニタリング未取得時転送タイマー（Park Monitoring Forward No Retrieve Timer）]が時間切れになると、システムは以下の接続先の 1 つにコールを送信します。 • [ボイスメール（Voicemail）]：ボイスメール プロファイルの設定を使用してコールの送信先を決定します。 • **[発信元に戻す（Revert to Originator）]**：コールをパークしている人にコールを戻します。 • コールを別の番号に転送するには、テキストボックスに他の番号を入力します。 どのオプションも選択されていない場合、コールはコールをパークしている人に戻されます。
[未取得時の外線コール転送のコーリング サーチ スペース（Calling Search Space for Forwarding External Calls When Not Retrieved）]	パーク保留中のコールを設定済みの番号にリダイレクトされるように設定した場合、転送先のコーリング サーチ スペースを選択します。
[未取得時の内線コールの転送先（Forward Destination for Internal Calls When Not Retrieved）]	コールがパーク保留されている人物が内部の人であり、[パーク モニタリング未取得時転送タイマー（Park Monitoring Forward No Retrieve Timer）]が時間切れになると、システムは以下の接続先の 1 つにコールを送信します。 • [ボイスメール（Voicemail）]：ボイスメール プロファイルの設定を使用してコールの送信先を決定します。 • **[発信元に戻す（Revert to Originator）]**：コールをパークしている人にコールを戻します。 • コールを別の番号に転送するには、テキストボックスに他の番号を入力します。 どのオプションも選択されていない場合、コールはコールをパークしている人に戻されます。

フィールド	説明
[未取得時の内線コール転送のコーリング サーチ スペース（Calling Search Space for Forwarding Internal Calls When Not Retrieved）]	パーク保留中のコールを設定済みの番号にリダイレクトされるように設定した場合、転送先のコーリング サーチ スペースを選択します。
[パークモニタリング復帰タイマー（秒）（Park Monitor Reversion Timer (seconds)）]	このタイマーは、ユーザがパークしたコールを取得するようにユーザに求めるまで、Unified Communications Manager が待機する秒数を決定します。 このタイマーが開始するのは、ユーザが電話機の [パーク（Park）] ソフトキーを押したときです。タイマーが時間切れになるとアラームが鳴ります。 デフォルト値は 60 秒です。 （注） タイマーの値に0を選択した場合は、このテンプレートを使用する電話回線は [パーク モニタリング復帰タイマー（Park Monitor Reversion Timer）]のクラスタ全体のサービス パラメータの値を使用します。

コール パークの連携動作

機能	データのやり取り
CTI アプリケーション	CTI アプリケーションはコール パーク機能（コール パーク DN でのアクティビティのモニタなど）にアクセスします。 コール パーク DN をモニタするには、CTIアプリケーションに関連付けられているエンド ユーザまたはアプリケーションを、Standard CTI Allow Call Park Monitoring ユーザ グループに追加します。
保留音	保留音を使用すると、ユーザはコールを保留にして、ストリーミング ソースから提供される音楽を再生できます。 コールパークの保留音オーディオ ソースは、**[電話の設定（Phone Configuration）]** ウィンドウの **[ネットワーク保留音オーディオ ソース（Network Hold MOH audio source）]** 設定を設定することによって選択されます。 オーディオ ソースが選択されていない場合、Cisco Unified CM はデバイス プールで定義されているオーディオ ソースを使用します。デバイス プールでオーディオ ソース ID が指定されていない場合はシステム デフォルトが使用されます。
ルート プラン レポート	ルート プラン レポートには、Unified Communications Manager で設定されているパターンと電話番号が表示されます。 コール パークに電話番号を割り当てる前に、ルート プラン レポートで重複するパターンと電話番号を確認します。

機能	データのやり取り
コーリング サーチ スペースとパーティション	デバイスのコーリング サーチ スペースに基づいて、コール パーク アクセスをユーザに限定するため、コール パーク電話番号または範囲をパーティションに割り当てます。
即時転送	コール パークでは、即時転送（[即転送（iDivert）] または [即転送（Divert）] ソフトキー）がサポートされています。 たとえば、ユーザ A がユーザ B にコールし、ユーザ B がこのコールをパークするとします。 ユーザ B はコールを取得してから、[即転送（iDivert）] または [即転送（Divert）] ソフトキーを押してコールをボイスメッセージング メールボックスに送信することを決定します。 ユーザ A はユーザ B のボイスメール グリーティングを受信します。
割込み	• コール パークによる割り込み：相手側の電話（割り込み先の電話）がコールを制御します。割り込み元は、相手側の電話に「ピギーバッグ」します。 相手側の電話には、割り込み先であっても、一般的な機能のほとんどが含まれています。したがって、割り込み元は機能にアクセスできません。 相手側がコールをパークすると、割り込み元はそのコール（割り込み）を解放する必要があります。 • コール パークによる C 割り込み：相手側と割り込み元がピアとして動作します。 C 割り込み機能は会議ブリッジを使用するため、ミートミー会議のように機能します。 相手側と割り込み元の両方の電話は、各自の機能に完全にアクセスできます。
ダイレクト コール パーク	コール パークの [パーク（Park）] ソフトキーとダイレクト コール パークの両方を設定しないことが推奨されますが、この両方が設定される可能性があります。 この両方を設定する場合は、コール パーク番号とダイレクト コール パーク番号が重複していないことを確認してください。
QSIG クラスタ間トランク	ユーザが QSIG クラスタ間トランクまたは QSIG ゲートウェイ トランクでコールをパークすると、パークされた発信者（パーク対象）に対し、[パーク番号（To parked number）] メッセージは表示されません。電話には引き続き、元の接続番号が表示されます。 コールがパークされた場合、コールをパークしたユーザがそのコールを取得できます。 コールがパーク状態から取得されると、コールは続行されますが、パークされた発信者に対して新しい接続番号は表示されません。

コール パークの制約事項

機能	制約事項
コール パーク	Unified Communications Manager 各コール パーク内線番号にパークできるコールは 1 つだけです。
共有回線	ノード間での共有回線デバイスの場合、デバイスが最初に登録したノードにその回線が登録されます。 たとえば、subscriber2 のデバイスが最初に登録され、subscriber2 とパブリッシャ ノードで回線が作成されると、その回線は subscriber2 に属します。 各ノードでコール パーク番号を設定する必要があります。
バックアップ	フェールオーバーまたはフォールバックを実現するには、パブリッシャ ノードとサブスクライバ ノードでコール パーク番号を設定します。 この設定により、プライマリ ノードがダウンすると、回線デバイス関連付けがセカンダリ ノードに変更され、このセカンダリ ノードのコール パーク番号が使用されます。
ダイレクト コール パーク	ダイレクト コール パーク（またはコール パーク）が共有回線から開始され、コールがどのデバイスからも取得されない場合、パークされたコールは常に共有回線の受信者（パークしたユーザ）に戻されます。
会議	共有回線とパーク復帰の発信者の間で会議コールが設定されている場合、またはパーク復帰が失敗した場合、（別の共有回線と発信者の間の）2 者コールが発生します。 これは、パーク復帰では Unified Communications Manager により、回線を共有する両方のデバイスにコールが拡大され、両方の参加者（会議にすでに参加している参加者やパーク保留状態の参加者）を会議に追加しようとするためです。 参加者が、会議にすでに参加している参加者を最初に追加しようとすると、パーク復帰が失敗します。 パーク復帰が失敗しても、共有回線は通常どおりコールに割り込むことができます。
サーバの削除	[**サーバの設定（Server Configuration）**] ウィンドウ（**[システム（System）] > [サーバ（Server）]**）で、削除されるノードに Unified Communications Manager のコール パーク番号が設定されていた場合、ノードの削除は失敗します。 ノードを削除するには、Cisco Unified Communications Manager Administration でコール パーク番号を削除する必要があります。

コール パークのトラブルシューティング

コールをパークできない

問題

コールをパークできない。[パーク（Park）] ソフトキーまたは機能ボタンを押してもコールがパークされません。

ソリューション

クラスタ内の各 Unified Communications Manager に固有のコール パーク番号が割り当てられていることを確認します。

コール パーク番号に割り当てられているパーティションと電話機の電話番号に割り当てられているパーティションが一致しません。 パーティションの詳細については、Cisco Unified Communications Manager システム設定ガイド を参照してください。

コール パーク番号の表示時間が短すぎる

問題

コール パーク番号の表示時間が短すぎる。

ソリューション

コール パーク表示タイマーに、より長い時間を設定します。 タイマーの詳細については、クラスタ全体のコール パークの設定 （470 ページ） を参照してください。

ダイレクト コール パークの概要

ダイレクト コール パークは、ユーザが選択し、待機状態になっているダイレクト コール パーク番号に対して、ユーザがコールを転送できる機能です。 設定されたダイレクト コール パーク番号は、クラスタ全体に存在します。 ダイレクト コール パークのビジー ランプ フィールド（BLF）をサポートする電話機を設定すると、特定のダイレクト コール パーク番号のビジー ステータスおよびアイドル ステータスをモニタできます。 また、BLF はダイレクト コール パーク番号の短縮ダイヤルとしても使用できます。

Unified Communications Manager が、各ダイレクト コール パーク番号でパークできるコールは 1 つだけです。 パークされたコールを取得するには、設定された取得プレフィックスに続けて、コールがパークされたダイレクト コール パーク番号をダイヤルする必要があります。

ダイレクト コール パークの前提条件

導入環境内の電話でダイレクト コール パークがサポートされていることを確認してください。サポートされている電話のリストを確認するには、Cisco Unified Reporting から [**電話機能リスト（Phone Feature List）**] レポートを実行し、機能として [**処理されたダイレクトコールパーク（Assisted Directed Call Park）**] を選択します。 詳細については、電話機能一覧の生成 （5 ページ）を参照してください。

ダイレクト コール パークの設定タスク フロー

始める前に

- ダイレクト コール パークの前提条件 （490 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	クラスタ全体のダイレクト コール パークの設定 （490 ページ）	ダイレクト コール パークのクラスタ全体のパラメータを設定します。
ステップ 2	ダイレクト コール パーク番号の設定 （491 ページ）	1 つのダイレクト コール パーク内線番号または内線番号の範囲を追加、コピー、更新します。
ステップ 3	BLF/ダイレクト コール パーク ボタンの設定 （493 ページ）	BLF/ダイレクト コール パークの電話ボタン テンプレートを設定します。
ステップ 4	影響を受けるデバイスとダイレクト コール パークの同期 （494 ページ）	影響を受けるデバイスとダイレクト コール パークの同期

クラスタ全体のダイレクト コール パークの設定

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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

ステップ 2 タイマーを設定するには、クラスタ全体のパラメータ（一般機能）セクションの [コール パーク復帰タイマー（Call Park Reversion Timer）]フィールドを更新します。

デフォルトは 60 秒です。 このパラメータでは、コールをパーク状態に維持する時間を決定します。 このタイマーが期限切れになると、[ダイレクト コール パークの設定（Directed Call Park Configuration）]ウィンドウで設定した内容に応じて、パークされたコールが元のデバイスに戻るか、指定された別の番号に転送されます。

ダイレクト コール パーク番号の設定

始める前に

ダイレクト コール パーク 電話番号、パーティション、および範囲のそれぞれが Unified Communications Manager 内で一意であることを確認します。 開始する前に、ルートプランレポートを生成します。 また、パーク ソフトキーが有効になっている場合は（非推奨）、コール パーク番号とダイレクト コール パーク番号の間に重複がないことを確認します。 復帰番号が設定されていない場合には、コールパークの復帰タイマーが時間切れになったあと、コールがパーカー（パーキング パーティ）に戻されます。

クラスタ全体のダイレクト コール パークの設定 （490 ページ）

手順

ステップ 1 **[コール ルーティング（Call Routing）] > [ダイレクト コール パーク（Directed Call Park）]** 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。

- 新しいダイレクト コール パーク番号を追加するには、[新規追加] をクリックします。
- ダイレクト コール パーク番号をコピーするには、ダイレクト コール パーク番号または番号の範囲を検索して、**[コピー（Copy）]** アイコンをクリックします。
- ダイレクト コール パーク番号を更新するには、ダイレクト コール パーク番号または番号の範囲を検索します。

[ダイレクト コール パーク番号設定（directed call park number configuration）] ウィンドウが表示されます。

ステップ 3 [ダイレクト コール パークの設定（Directed Call Park settings）] 領域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、ダイレクト コール パークの構成時の設定 （492 ページ）を参照してください。

ステップ 4 新しいコール パーク番号や変更したコール パーク番号をデータベースに保存するには、**[保存（Save）]** をクリックします。

ダイレクト コール パーク番号を更新した場合、Unified Communications Manager は、コール パーク復帰タイマーが期限切れになった後のみ、この番号にパークされたコールを戻します。

ステップ 5 **[設定の適用（Apply Config）]** をクリックします。

[設定の適用情報（Apply Configuration Information）] ダイアログが表示されます。

ステップ 6 [OK]をクリックします。

ステップ 7 BLF を使用してダイレクト コール パーク番号をモニタする場合は、**[ダイレクト コール パーク番号設定（directed call park number configuration）]** ウィンドウの **[デバイスの再起動（Restart Devices）]** をクリックします。 変更通知を使用している場合、この手順はオプションです。

ダイレクト コール パークの構成時の設定

フィールド	説明
番号（Number）	ダイレクトコールパーク番号を入力します。 数字（0～9）またはワイルドカード文字（[]、-、*、^、#）とX（1つまたは2つ）を入力できます。 たとえば、5555を入力して1つのコールパーク番号5555を定義するか、55XXを入力して5500~5599のダイレクトコールパーク内線番号の範囲を定義します。ダイレクト コール パーク番号が固有の番号であり、コール パーク番号と重複しないことを確認します。
説明	このダイレクトコールパーク番号または範囲に簡単な説明を付けます。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（<>）、およびタブは使用できません。
パーティション	パーティションを使用してダイレクト コール パーク番号へのアクセスを制限する場合は、ドロップダウンリストから必要なパーティションを選択します。 ダイレクト コール パーク番号へのアクセスを制限しない場合は、パーティションをデフォルトの [<None>] のままにします。 （注） ダイレクトコールパーク番号とパーティションの組み合わせがUnified Communications Manager内で一意であることを確認します。
[復帰番号(Reversion Number)]	パークされているコールが取得されない場合にそのコールを戻す番号を入力するか、このフィールドを空白にしておきます。 （注） 復帰番号は、数字だけで構成されます。ワイルドカードは使用できません。
[復帰コーリングサーチスペース(Reversion Calling Search Space)]	ドロップダウン リストを使用して、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 [<None>] のままにします。

フィールド	説明
[取得用プレフィックス(Retrieval Prefix)]	この必須フィールドにはパークされたコールを取得するためのプレフィックスを入力します。 パークされたコールを取得する試行とダイレクト パークを開始する試行を区別するための取得用プレフィックスが必要です。

BLF/ダイレクト コール パーク ボタンの設定

始める前に

クラスタ全体のダイレクト コール パークの設定 （490 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）]** > **[電話ボタンテンプレート（Phone button template）]** の順に選択します。

ステップ 2 設定ウィンドウが表示されたら、[関連情報（Association Information）] ペインの [新規 BLF/ダイレクト コール パークの追加（Add new BLF Directed Call Park）] リンクをクリックします。

（注） その電話機に適用された電話ボタンテンプレート、またはデバイス プロファイルが BLF/ダイレクト コール パーク をサポートしていない場合、リンクは [関連情報（Association Information）] ペインに表示されません。

ステップ 3 [BLF]/[ダイレクト コール パーク（Directed Call Park）] フィールド領域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、BLF/ダイレクト コール パークの設定フィールド （494 ページ）を参照してください。

ステップ 4 設定が完了したら、[保存（Save）] をクリックしてウィンドウを閉じます。

電話番号は、[電話機の設定（Phone Configuration）] ウィンドウの [関連情報（Association Information）] ペインに表示されます。

BLF/ダイレクト コール パークの設定フィールド

表 *31 : BLF/*ダイレクト コール パーク ボタンの設定フィールド

フィールド	説明
[電話番号（Directory Number）]	[電話番号（Directory Number）] ドロップダウン リストに、Unified Communications Manager データベースにあるダイレクト コール パーク番号が表示されます。 SIP を実行している SCCP または電話機を実行している電話機の場合は、ユーザが短縮ダイヤル ボタンを押した時にシステムにダイヤルする番号(および表示されている場合は対応するパーティション) を選択します(3 の場合は 6002 など)。特定のパーティションなしで表示される電話番号は、デフォルトのパーティションに属します。
[ラベル（Label）]	BLF/ダイレクト コール パーク ボタンに表示するテキストを入力します。 このフィールドは国際化をサポートしています。 電話機が国際化をサポートしていない場合、システムは [ラベルASCII(Label ASCII)] フィールドに表示されるテキストを使用します。
[ラベルASCII(Label ASCII)]	BLF/ダイレクト コール パーク ボタンに表示するテキストを入力します。 ASCII ラベルは、[ラベル(Label)] フィールドに入力したテキストの非国際化バージョンを表します。 電話機が国際化をサポートしていない場合、システムはこのフィールドに表示されるテキストを使用します。 （注） [ラベル ASCII（Label ASCII）] フィールドに、[ラベル（Label）] フィールドのテキストとは異なるテキストを入力すると、Cisco Unified Communications Manager Administration は、テキストが異なっていても両方のフィールドの設定を受け入れます。

影響を受けるデバイスとダイレクト コール パークの同期

手順

ステップ 1 **[コール ルーティング（Call Routing）]** > **[ダイレクト コール パーク（Directed Call Park）]** を選択します。

[ダイレクト コール パークの検索と一覧表示（Directed Call Parks）] 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ダイレクト コール パークの一覧がウィンドウに表示されます。

ステップ 4 該当する複数の電話機を同期させるダイレクトコールパークをクリックします。**[ダイレクト コール パーク設定（Directed Call Park Configuration）]** ウィンドウが表示されます。

ステップ 5 追加の設定変更を加えます。

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。

[設定の適用情報（Apply Configuration Information）] ダイアログが表示されます。

ステップ 8 [OK]をクリックします。

ダイレクト コール パークの連携動作

ダイレクト コール パーク機能との連携動作を次の表で説明します。

機能	データのやり取り
保留音	ダイレクトコールパークの保留音音源は、**[デフォルトのネットワーク保留 MOH オーディオ ソース（Default Network Hold MOH Audio Source）]** サービスパラメータによって割り当てられます。 パラメータを割り当てるには、次のようにします。 **1.** Cisco Unified CM の管理から、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** の順に選択します。 **2.** **[サーバ（Server）]** ドロップダウンから、Unified Communications Manager クラスタ ノードを選択します。 **3.** [サービス（Service）]ドロップダウン リストから、[Cisco CallManager]を選択します。 **4.** **[クラスタ全体のパラメータ（サービス）（Clusterwide Paramters (Service)）]** で、MOH オーディオ ソースを **[デフォルトのネットワーク保留 MOH 音源 ID（Default Network Hold MOH Audio Source ID）]** パラメータに割り当てます。 デフォルトは **1** です。 **5.** **[保存]** をクリックします。 （注） システムへの MOH オーディオソースの追加の詳細については、このガイドの「保留音の設定」の項を参照してください。

機能	データのやり取り
コーリング サーチ スペースとパーティション	デバイスのコーリング サーチ スペースに基づいて、ダイレクト コール パーク アクセスをユーザに限定するため、ダイレクト コール パーク電話番号または範囲をパーティションに割り当てます。
即時転送	ダイレクト コール パークでは、即時転送（[即転送（iDivert）] または [即転送（Divert）] ソフトキー）がサポートされています。 たとえば、ユーザ A がユーザ B にコールし、ユーザ B がこのコールをパークするとします。 ユーザ B はコールを取得してから、[即転送（iDivert）] または [即転送（Divert）] ソフトキーを押してコールをボイスメッセージング メールボックスに送信することを決定します。 ユーザ A はユーザ B のボイスメール グリーティングを受信します。
割込み	• ダイレクト コール パークによる割り込み：相手側の電話（割り込み対象の電話）がコールを制御します。 割り込み元は、相手側の電話に「ピギーバッグ」します。 相手側の電話には、割り込み先であっても、一般的な機能のほとんどが含まれています。 したがって、割り込み元は機能にアクセスできません。 相手側がダイレクト コール パークを使用してコールをパークすると、割り込み元はそのコール（割り込み）を解放する必要があります。 • ダイレクト コール パークによる C 割り込み：相手側と割り込み元がピアとして動作します。C割り込み機能は会議ブリッジを使用します。これによりミートミー会議と同様に機能します。 相手側と割り込み元の両方の電話は、各自の機能への完全なアクセスを維持します。
コール パーク	コール パークの [パーク（Park）] ソフトキーとダイレクト コール パークの両方を設定しないことが推奨されますが、この両方が設定される可能性があります。 この両方を設定する場合は、コール パーク番号とダイレクト コール パーク番号が重複していないことを確認してください。 ダイレクト コール パーク機能を使用してパークされた発信者（パーク対象）は、パーク中は標準コール パーク機能を使用できません。

ダイレクト コール パークの制約事項

機能	制約事項
ダイレクト コール パーク番号	Unified Communications Manager 1つのパーティが、各ダイレクト コール パーク番号でパークできるコールは 1 つだけです。 デバイスが（[BLF] ボタンを使用して）モニタするように設定されているダイレクト コール パーク番号は削除できません。 ダイレクト コール パーク番号または範囲が使用中であるため削除できないことを通知するメッセージが表示されます。 どのデバイスが番号を使用しているかを特定するには、[ダイレクト コール パークの設定（Directed Call Park 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。
標準コール パーク機能	ダイレクト コール パーク機能を使用してパークされた発信者（パーク対象）は、パーク中は標準コール パーク機能を使用できません。
ダイレクト コール パーク機能	転送とダイレクト コール パークの両方のボタンを同時に押さないことを推奨します。この結果、DPark と転送の両方が失敗する可能性があります。
ダイレクト コール パーク BLF	ダイレクト コール パーク BLF は、ダイレクト コール パーク番号範囲をモニタできません。 ユーザはダイレクト コール パーク BLF を使用して個々のダイレクト コール パーク番号だけをモニタできます。 たとえば、ダイレクト コール パーク番号範囲 8X を設定している場合、ダイレクト コール パーク BLF を使用してその範囲全体（80 ～ 89）をモニタすることはできません。
SIP を実行している電話のダイレクト コール パーク	次の制約事項は、SIP を実行している電話のダイレクト コール パークに適用されます。 • ダイレクト コール パークは、SIP を実行している Cisco Unified IP Phone 7940 と 7960 の [転送（Transfer）] ソフトキーを使用して起動されます。 • SIP を実行している Cisco Unified IP Phone 7940 と 7960 の [ブラインド転送（Blind Transfer）] ソフトキーが使用される場合、システムではダイレクト コール パークがサポートされません。 • SIP を実行する Cisco Unified IP Phone 7940 と 7960、および SIP を実行するサードパーティの電話では、システムでダイレクト コール パーク BLF がサポートされません。

ダイレクト コール パークのトラブルシューティング

パークされたコールを取得できない

パークされたコールを取得できません。パークされたコールを取得するためにダイレクト コール パーク番号をダイヤルしたあと、ユーザにビジー トーンが聞こえ、IP Phone に「パーク スロットが利用できません（Park Slot Unavailable）」というメッセージが表示されます。

ユーザが取得用プレフィックスに続けてダイレクト コール パーク番号をダイヤルしているかどうかを確認します。

コールをパークできない

コールをパークできない。[転送（Transfer）] ソフトキー（使用可能な場合は [転送（Transfer）] ボタン）を押し、ダイレクト コール パークをダイヤルしてもコールがパークされません。

コール パーク番号に割り当てられているパーティションと電話機の電話番号に割り当てられているパーティションが一致していることを確認します。デバイスにパーティションとコーリング サーチ スペースが正しく設定されていることを確認します。 パーティションの詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

復帰タイマーが時間切れになった後でユーザに対してリオーダー音が再生される

コールをパークできない。 復帰タイマーが時間切れになったあと、ユーザにリオーダー トーンが聞こえる。

ユーザが、[転送（Transfer）] ソフトキー（使用可能な場合は [転送（Transfer）] ボタン）を押してからダイレクト コール パーク番号をダイヤルし、ダイレクト コール パーク番号をダイヤルしたあとにもう一度 [転送（Transfer）] ソフトキー（使用可能な場合は [転送（Transfer）] ボタン）を押すか、またはオンフックにしていることを確認します。 ダイレクト コール パークは転送機能であるため、ダイレクト コール パーク番号を単独でダイヤルできません。

（注） Transfer On-hook Enabled サービス パラメータを True に設定している場合は、[転送（Transfer）] ソフトキー（使用可能な場合は [転送（Transfer）] ボタン）を 2 回押す代わりに、オンフックにするだけで転送が完了します。

ユーザに対してリオーダー音またはアナウンスが再生される

コールをパークできない。[転送（Transfer）]ソフトキー（使用可能な場合は[転送（Transfer）]ボタン）を押し、ダイレクトコールパーク番号をダイヤルしたあと、ユーザにリオーダートーンまたはアナウンスが聞こえます。

ダイヤルした番号がダイレクト コール パーク番号として設定されていることを確認します。

ユーザは範囲内の番号にコールをパークできない

ダイレクト コール パーク番号の範囲を設定したあと、範囲内の番号にコールをパークできない。

ダイレクト コール パーク番号の範囲を入力する構文を確認します。 構文に誤りがあると、実際には範囲を設定していない場合でも、範囲を設定するように見えることがあります。

パークされたコールの復帰が早すぎる

パークされたコールの復帰が早すぎます。

コール パーク復帰タイマーの設定時間を長くしてください。

パーク スロットが使用できない

コールをパークできない。[転送（Transfer）]ソフトキー（使用可能な場合は[転送（Transfer）]ボタン）を押し、ダイレクト コール パーク番号をダイヤルした後、ユーザにビジー トーンが聞こえ、IP Phone に「パーク スロットが利用できません（Park Slot Unavailable）」というメッセージが表示されます。

ダイヤルしたダイレクト コール パーク番号が、パークされたコールでまだ使用されていないことを確認するか、または別のダイレクト コール パーク番号にコールをパークします。

パークされたコールが、コールをパークした番号に復帰しない

パークされたコールが、コールをパークした番号に復帰しない。

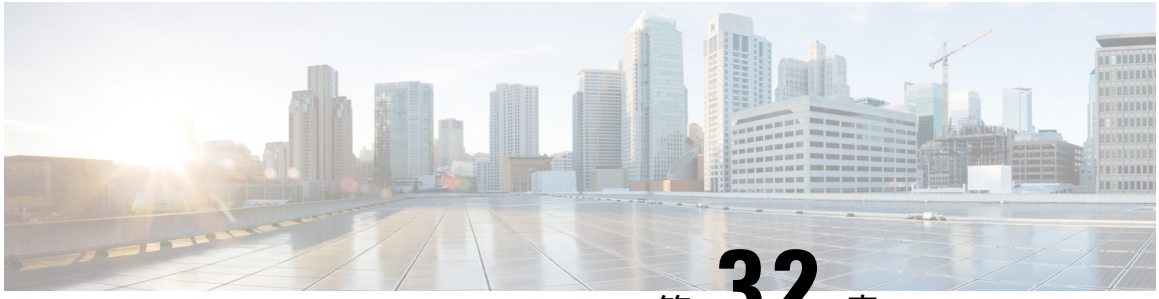
ダイレクト コール パーク番号の設定を調べ、別の電話番号ではなく、コールをパークした番号に復帰するように設定されていることを確認します。

番号または範囲が使用中であるため削除できない

ダイレクト コール パーク番号または範囲を削除しようとすると、番号または範囲が使用中であるため削除できないというメッセージが表示される。

デバイスが監視するように設定されている（[BLF]ボタンを使用）ダイレクトコールパーク番号は削除できません。 どのデバイスが番号を使用しているかを特定するには、[ダイレクトコー

ルパークの設定（Directed Call Park 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。



第 32 章

エクステンションモビリティ

エクステンションモビリティの概要

Cisco Extension Mobility により、ユーザは、お持ちのシステムのその他の電話機から一時的にラインアピアランス、サービス、スピードダイヤルなどの電話機の設定にアクセスできるようになります。 例えば、複数の従業員で単一の電話を使用しているような場合、個々のユーザが電話機にログインし、他のユーザアカウントの設定に影響を及ぼさずに自分の設定にアクセスできるよう、エクステンションモビリティを設定できます。

ユーザがエクステンションモビリティを使用してログインした際に、エクステンションモビリティプロファイルがすでにアプリケーションユーザに関連付けられている場合は、CTI アプリケーションによってデバイス関連情報が送信されます。

CTI アプリケーションはユーザがログインしたデバイスを、デバイスの直接制御が不能な場合でも（エクステンション モビリティ プロファイルを使用して）制御できるため、アプリケーションユーザに関連付けられたデバイスプロファイルを使用することで、デバイスに直接関連付けられていない場合でも録音を行うことができます。

エクステンション モビリティの前提条件

- 到達可能な TFTP サーバ。
- Extension Mobility 機能がほとんどの Cisco Unified IP Phone に拡張されている。 電話のマニュアルを参照して、Cisco Extension Mobility がサポートされていることを確認する。

エクステンションモビリティの設定タスク 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	電話機能一覧の生成 （5 ページ）	Extension Mobility 機能をサポートするデバイスを特定するためのレポートを生成します。
ステップ 2	エクステンションモビリティ サービスの有効化 （503 ページ）	
ステップ 3	Cisco Extension Mobility 電話サービスの設定 （503 ページ）	ユーザが後でExtension Mobilityにアクセスするために登録できる、Extension Mobility IP 電話サービスを設定します。
ステップ 4	ユーザのエクステンションモビリティ デバイスプロファイルの作成 （505 ページ）	Extension Mobility デバイス プロファイルを設定します。 このプロファイルは、ユーザがExtension Mobilityにログインするときに物理デバイスにマッピングするバーチャルデバイスとして機能します。この物理デバイスは、このプロファイルの特性を引き継ぎます。
ステップ 5	ユーザへのデバイス プロファイルの関連付け （505 ページ）	ユーザが別の電話機から設定にアクセスできるように、デバイス プロファイルをユーザに関連付けます。 物理デバイスを関連付けるのと同じ方法で、ユーザにユーザ デバイス プロファイルを関連付けます。
ステップ 6	エクステンションモビリティへの登録 （506 ページ）	Extension Mobility サービスに IP 電話とデバイスプロファイルを登録して、ユーザがExtension Mobilityにログインし、使用し、ログアウトできるようにします。
ステップ 7	クレデンシャル変更 IP 電話サービスの設定 （507 ページ）	ユーザが自身の電話機で PIN を変更できるようにするには、変更クレデンシャル Cisco Unified IP Phone サービスを設定し、ユーザ、デバイス プロファイル、または IP 電話を、変更クレデンシャル

	コマンドまたはアクション	目的
		電話サービスに関連付ける必要があります。
ステップ 8	（任意） Extension Mobility（EM; エクステンションモビリティ）のサービス パラメータの設定 （507 ページ）	Extension Mobilityの動作を変更するには、サービスパラメータを設定します。

エクステンションモビリティ サービスの有効化

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[ツール（Tools）] > [サービス アクティベーション（Service Activation）]** を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストから、必須のノードを選択します。

ステップ 3 、次のサービスを有効化します。

a) Cisco CallManager
b) Cisco Tftp
c) Cisco Extension Mobility
d) ILS サービス

（注） ILS サービスをアクティブ化するには、パブリッシャ ノードを選択する必要があります。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 **OK**をクリックします。

Cisco Extension Mobility 電話サービスの設定

ユーザが後でExtension Mobilityにアクセスするために登録できる、Extension Mobility IP 電話サービスを設定します。

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。**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [電話サービス（Phone Services）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [サービス名（Service Name）] フィールドに、サービスの名前を入力します。

ステップ 4 [**サービス URL**（**Service URL**）] フィールドにサービス URL を入力します。

形式は `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#` です。 `IP` アドレス は、Cisco Extension Mobility が有効化され、実行している Unified Communications Manager の IP アドレスです。

IPv4 アドレスである必要があります。

例：

`http://123.45.67.89:8080/emapp/EMAppServlet?device=#DEVICENAME#`

例：

`http://[2001:0001:0001:0067:0000:0000:0000:0134]:8080/emapp/EMAppServlet?device=#DEVICENAME#`

この形式により、ユーザはユーザ ID と PIN を使用してログインすることができます。 Extension Mobility サービスに登録した IP Phone ユーザのサインイン オプションをさらに多く設定できます。 さらに多くのサインイン オプションを設定するには、`loginType` パラメータを以下の形式でサービス URL に追加します。

- `loginType=DN` により、ユーザはプライマリ内線番号と PIN を使用してログインできます。

  サービス URL の形式は、`http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=DN` です。

- `loginType=SP` により、ユーザはセルフ サービス ユーザ ID と PIN を使用してログインできます。

  サービス URL の形式は、`http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=SP` です。

- `loginType=UID` により、ユーザはユーザ ID と PIN を使用してログインできます。

  サービス URL の形式は、`http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=UID` です。

URL の最後に `loginType` を付加しなかった場合は、デフォルトのサインイン オプションとして [ユーザ ID（User ID）] と [PIN] が表示されます。

ステップ 5 [サービス タイプ（Service Type）] フィールドで、サービスが [サービス（Services）]、[ディレクトリ（Directories）]、または [メッセージ（Messages）] ボタンにプロビジョニングされるかどうかを選択します。

ステップ 6 **[保存（Save）]** をクリックします。

ユーザのエクステンションモビリティ デバイス プロファイルの作成

Extension Mobilityデバイスプロファイルを設定します。 このプロファイルは、ユーザがExtension Mobilityにログインするときに物理デバイスにマッピングするバーチャル デバイスとして機能します。 この物理デバイスは、このプロファイルの特性を引き継ぎます。

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）]>[デバイス設定（Device Settings）]>[デバイス プロファイル（Device Profile）]**。

ステップ 2 次のいずれかの作業を実行します。

- [検索（Find）]をクリックして設定を変更し、結果一覧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、[新規追加（Add New）]をクリックして、[デバイス プロファイルのタイプ（Device Profile Type）] からオプションを選択します。[次へ（Next）]をクリックします。
- [デバイス プロトコル（Device Protocol）]ドロップダウン リストからデバイス 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 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、オンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

ステップ 5 [割り当て情報（Association Information）]領域で、[新規 DN を追加（Add a New DN）]をクリックします。

ステップ 6 [電話番号（Directory Number）]フィールドに電話番号を入力して、[保存（Save）]をクリックします。

ステップ 7 [リセット（Reset）]をクリックし、プロンプトに従います。

ユーザへのデバイス プロファイルの関連付け

ユーザが別の電話機から設定にアクセスできるように、デバイスプロファイルをユーザに関連付けます。 物理デバイスを関連付けるのと同じ方法で、ユーザにユーザ デバイス プロファイルを関連付けます。

ヒント 一括管理ツール（BAT）を使用して、Cisco Extension Mobility の複数のユーザ デバイス プロファイルを一度に追加および削除できます。 Cisco Unified Communications Manager 一括管理ガイドを参照してください。

手順

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 次のいずれかの作業を実行します。

- 既存のユーザ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ユーザを選択します。
- **[新規追加（Add New）]** をクリックして、新しいユーザを追加します。

ステップ 3 **[Extension Mobility]** で、作成したデバイス プロファイルを探して、それを **[使用可能なプロファイル（Available Profiles）]** から **[制御するプロファイル（Controlled Profiles）]** に移動します。

ステップ 4 **[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 **[保存（Save）]** をクリックします。

エクステンションモビリティへの登録

Extension Mobility サービスに IP 電話とデバイス プロファイルを登録して、ユーザがExtension Mobilityにログインし、使用し、ログアウトできるようにします。

手順

ステップ 1 Cisco Unified CM Administration で次のいずれかのタスクを実行します。

- **[デバイス（Device）]>[電話（Phone）]** を選択し、検索条件を指定してから [検索（Find）] をクリックし、Extension Mobilityに使用する電話機を選択します。
- **[デバイス（Device）]>[デバイス設定（Device Settings）]>[デバイス プロファイル（Device Profile）]** を選択し、検索条件を指定してから [検索（Find）]をクリックし、作成したデバイス プロファイルを選択します。

ステップ 2 [関連リンク（Related Links）]ドロップダウン リストから、[サービスの登録/登録解除（Subscribe/Unsubscribe Services）]を選択し、[移動（Go）]をクリックします。

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

ステップ 4 [次へ（Next）]をクリックします。

ステップ 5 [登録（Subscribe）]をクリックします。

ステップ 6 [保存（Save）]をクリックし、ポップアップ ウィンドウを閉じます。

クレデンシャル変更 IP 電話サービスの設定

ユーザが自身の電話機で PIN を変更できるようにするには、変更クレデンシャル Cisco Unified IP Phone サービスを設定し、ユーザ、デバイス プロファイル、または IP 電話を、変更クレデンシャル電話サービスに関連付ける必要があります。

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。**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [電話サービス（Phone Services）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [サービス名（Service Name）]フィールドに、**`Change Credential`** と入力します。

ステップ 4 [サービス URL（Service URL）]フィールドに、次の値を入力すると、サーバがクレデンシャル変更 IP 電話サービスが稼働するサーバとなります。

```
http://server:8080/changecredential/ChangeCredentialServlet?device=#DEVICENAME#
```

ステップ 5 （任意）[セキュア サービス URL（Secure-Service URL）]フィールドに、次の値を入力すると、サーバがクレデンシャル変更 IP 電話サービスが稼働するサーバとなります。

```
https://server:8443/changecredential/ChangeCredentialServlet?device=#DEVICENAME#
```

ステップ 6 **[IP 電話サービス設定（IP Phone Services Configuration）]** の残りのフィールドを設定し、**[保存（Save）]** を選択します。

ステップ 7 Cisco Unified IP 電話 をクレデンシャル変更 IP 電話サービスに登録するには、**[デバイス（Device）] > [電話（Phone）]** を選択します。

ステップ 8 **[電話機の設定（Phone Configuration）]** ウィンドウで、[関連リンク（Related Links）]ドロップダウン リストから、[サービスの登録 / 登録解除（Subscribe/Unsubscribe Services）]を選択します。

ステップ 9 [移動（Go）]をクリックします。

ステップ 10 [サービスの選択（Select a Service）]ドロップダウン リストから[クレデンシャル変更 IP 電話サービス（Change Credential IP phone service）]を選択します。

ステップ 11 [次へ（Next）]をクリックします。

ステップ 12 [登録（Subscribe）]をクリックします。

ステップ 13 **[保存（Save）]** をクリックします。

Extension Mobility（EM; エクステンションモビリティ）のサービス パラメータの設定

（省略可能）

Extension Mobilityの動作を変更するには、サービス パラメータを設定します。

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）]**。

ステップ 2 [サーバ（Server）]フィールドで、Cisco Extension Mobility サービスを実行している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 Extension Mobility]を選択します。

ステップ 4 すべてのサービス パラメータを表示するには、[詳細設定（Advanced）]をクリックします。

これらのサービス パラメータとその設定オプションの詳細については、Extension Mobility サービス パラメータ （508 ページ）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。

Extension Mobility サービス パラメータ

表 *32 : Extension Mobility* サービス パラメータ

サービス パラメータ	説明
クラスタ内最大ログイン時間の強制（Enforce Intra-cluster Maximum Login Time）	ローカル ログインの最大時間を指定するには、[True] を選択します。この時間の経過後に、システムは自動的にデバイスをログアウトさせます。 デフォルト設定の [False] は、ログインの最大時間が存在しないことを意味します。 自動ログアウトを設定するには、このサービス パラメータに [True] を選択し、[クラスタ内最大ログイン時間（Intra-cluster Maximum Login Time）] サービス パラメータにシステムの最大ログイン時間を指定する必要もあります。 その後、Cisco Unified Communications Manager は、すべてのログインに対して自動ログアウト サービスを使用します。 [クラスタ間最大ログイン時間を実施（Enforce Intra-cluster Maximum Login Time）] の値が [False] に設定されており、[クラスタ間最大ログイン時間（Intra-cluster Maximum Login Time）] サービス パラメータに有効な最大ログイン時間を指定すると、[クラスタ間最大ログイン時間を実施（Enforce Intra-cluster Maximum Login Time）] は自動的に [True] に変更されます。

サービス パラメータ	説明
クラスタ内最大ログイン時間（Intra-cluster Maximum Login Time）	このパラメータは、ユーザがローカルにデバイスにログイン可能な最大時間（8:00（8 時間）や :30（30 分）など）を設定します。 [クラスタ内最大ログイン時間の強制（Enforce Intra-cluster Maximum Login Time）] パラメータが [False] に設定されている場合、システムはこのパラメータを無視し、最大ログイン時刻を 0:00 に設定します。 有効な値は HHH:MM の形式で 0:00 ～ 168:00 です。ここで、HHH は時間数を、MM は分数を表します。 （注） 内線モビリティを設定するためにユーザアクセスを許可する場合は、**[ユーザ プロファイル設定（User Profile Configuration）]** の **[エンド ユーザが内線モビリティの最大ログイン時間を設定できるようにする（Allow End User to set their Extension Mobility maximum login time）]** チェックボックスを使用して設定します。ユーザのセルフケア ポータル内の設定は、**[クラスタ内の最大ログイン時間（Intra-cluster Maximum Login Time）]**サービスパラメータの値をオーバーライドします。
同時要求の最大数（Maximum Concurrent Requests）	同時に実行可能なログイン操作またはログアウト操作の最大数を指定します。 この数値により、Cisco Extension Mobility サービスがシステム リソースを過剰に消費するのを防止します。 デフォルト値の 5 は、ほとんどのケースで適切な値です。

サービス パラメータ	説明
複数ログイン動作（Multiple Login Behavior）	ユーザが1つの電話機にログインし、その後同じクラスタまたは別のクラスタにある 2 台目の電話機にログインすると、ユーザは、**[サービスパラメータ設定(Service Parameter Configuration)]** ページで定義されている **[複数ログイン動作（Multiple Login Behavior）]** 設定に基づいて、2 台目の電話機でログイン動作を表示できます。 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。 • [複数のログインを許可する（Multiple Logins Allowed）]：同時に複数のデバイスにログインできます。 • [複数のログインを許可しない（Multiple Logins Not Allowed）]：1 つのデバイスにしかログインできません。 2 台目のデバイスへのログインに失敗すると、電話にはエラー コード「25」（[複数のログインを許可しない（Multiple Logins Not Allowed）]）が表示されます。 最初のデバイスからログアウトした場合にのみ、正常にログインできます。 これがデフォルト値です。 • [自動ログアウト（Auto Logout）]：ユーザが 2 台目のデバイス（Extension Mobility または Extension Mobility Cross Cluster のいずれか）へのログインを試行すると、Cisco Unified Communications Manager が自動的に 1 台目のデバイスからユーザをログアウトさせます。 これは必須フィールドです。 （注） 複数ログイン動作は、2 つの Extension Mobility Cross Cluster ログイン間でも適用されます。
英数字のユーザ ID	ユーザ ID に英数字を含めることを許可するには、[True] を選択します。 [False] を選択すると、ユーザ ID には数字しか含めることができなくなります。 （注） [英数字ユーザ ID（Alphanumeric User ID）] パラメータは、システム全体に適用されます。 英数字ユーザ ID と数字ユーザ ID を混在させることができます。 システムは、英数字キーパッドを使用して入力可能なユーザ ID しかサポートしません。 大文字と小文字が区別されるユーザ ID フィールドでは、小文字を使用する必要があります。

サービス パラメータ	説明
ログインした最後のユーザを記憶する（Remember the Last User Logged In）	**[いいえ（False）]** を選択した場合、システムは電話機にログインした最後のユーザを記憶しません。 ユーザが一時的にしか電話機にアクセスしない場合に、このオプションを使用します。 電話機にログインした最後のユーザを記憶するには、[はい（True）] を選択します。 電話機に1人のユーザしかアクセスしない場合に、このオプションを使用します。 たとえば、Cisco Extension Mobility を使用して、電話機から許可されたコールのタイプを有効化します。 ログインしていない、オフィス電話を使用しているユーザは、内線または緊急コールしか発信できません。 ただし、Cisco Extension Mobility を使用してログインすると、市内、長距離、および国際コールを発信できます。 このシナリオでは、電話機に定期的にログインするのはこのユーザだけです。 この場合は、ログインした最後のユーザ ID を記憶するように Cisco Extension Mobility を設定することには意味があります。
クラスタ内 EM 上の通話履歴の消去（Clear Call Logs on Intra-cluster EM）	Cisco Extension Mobility の手動ログインまたは手動ログアウト中に通話履歴を消去するように指定するには、**[True]** を選択します。 ユーザが IP フォンで Cisco Extension Mobility サービスを利用している間は、すべてのコール（発信、着信、不在）が通話履歴に記録され、IP フォンのディスプレイに表示して確認できます。 プライバシーを保護するには、[通話履歴を全件消去（Clear Call Log）] サービス パラメータを [True] に設定します。 これにより、あるユーザがログアウトして、別のユーザがログインしたときに通話履歴が消去されることが保証されます。 Extension Mobility Cross Cluster（EMCC）では、ユーザが電話機にログインまたは電話機からログアウトするたびに通話履歴が消去されます。 （注） 通話履歴は、手動ログイン/ログアウト時にのみ消去されます。 Cisco Extension Mobility のログアウトが自動的にまたは手動ログアウト以外の方法で発生した場合、通話履歴は消去されません。

サービス パラメータ	説明
IP アドレスの検証（Validate IP Address）	このパラメータは、ログインまたはログアウトを要求している送信元の IP アドレスを検証するかどうかを設定します。 このパラメータが [はい（True）] に設定された場合は、Cisco Extension Mobility のログイン要求またはログアウト要求が発生した IP アドレスが検証され、信頼できるかどうかが確認されます。 検証は、最初に、ログインまたはログアウトするデバイスのキャッシュに対して実行されます。 IP アドレスがキャッシュ内または信頼された IP アドレスのリスト内で見つかった場合や IP アドレスが登録済みデバイスの場合、デバイスはログインまたはログアウトできます。 IP アドレスが見つからなかった場合は、ログインまたはログアウトの試みがブロックされます。 このパラメータが [False] に設定されている場合は、Cisco Extension Mobility のログイン要求またはログアウト要求が検証されません。 IP アドレスの検証は、デバイスへのログインまたはデバイスからのログアウトに必要な時間に影響する可能性がありますが、無許可のログインまたはログアウトの試みを阻止してセキュリティを強化できます。 この機能は、特に、リモート デバイスの別の信頼されたプロキシ サーバからのログインとともに使用することをお勧めします。
信頼された IP のリスト（Trusted List of IPs）	このパラメータは、テキスト ボックスとして表示されます（最大長は 1024 文字です）。 テキスト ボックスには、信頼された IP アドレスまたはホスト名の文字列をセミコロンで区切って入力できます。 IP アドレス範囲と正規表現はサポートされません。
プロキシを許可する（Allow Proxy）	このパラメータが [True] の場合は、ウェブプロキシを使用する Cisco Extension Mobility のログイン操作とログアウト操作が許可されます。 このパラメータが [False] の場合は、プロキシ経由で受信された Cisco Extension Mobility のログイン要求とログアウト要求が拒否されます。 選択した設定は、[IP アドレスの検証（Validate IP Address）] パラメータが [はい（True）] に指定されている場合にのみ適用されます。
Extension Mobility のキャッシュ サイズ（Extension Mobility Cache Size）	このフィールドには、Cisco Extension Mobility によって維持されるデバイス キャッシュのサイズを入力します。 このフィールドの最小値は 1000、最大値は 20000、デフォルト値は 10000 です。 入力した値は、[IP アドレスの検証（Validate IP Address）] パラメータが [はい（True）] に指定されている場合にのみ適用されます。

Cisco Extension Mobility の連携動作

表 *33 : Cisco Extension Mobility* の連携動作

機能	データのやり取り
アシスタント	Cisco Extension Mobility を使用するマネージャは同時に Cisco Unified Communications Manager Assistant を使用できます。 マネージャは Cisco Extension Mobility を使用して Cisco Unified IP 電話 にログインし、次に Cisco IP Manager Assistant サービスを選択します。 Cisco IP Manager Assistant サービスが開始すると、マネージャはアシスタントと Cisco Unified Communications Manager Assistant のすべての機能（コール フィルタリングやサイレントなど）にアクセスできます。
BLF プレゼンス	ユーザ デバイス プロファイルで BLF/スピード ダイヤル ボタンを設定すると、デバイスにログイン後、Cisco Extension Mobility をサポートする電話は、BLF/スピード ダイヤル ボタンに BLF プレゼンス ステータスを表示します。 Extension Mobility ユーザがログアウトすると、Cisco Extension Mobility をサポートする電話は、設定されているログアウト プロファイルの BLF/スピード ダイヤル ボタンに BLF プレゼンス ステータスを表示します。
コール表示の制限	コール表示の制限を有効にした場合、Cisco Extension Mobility は通常どおり機能します。ユーザがデバイスにログインするときの通話情報の表示または制限はそのユーザが関連付けられているデバイス プロファイルにより異なります。 ユーザがログアウトするときの通話情報の表示または制限は、[電話の設定（Phone Configuration）] ウィンドウでその電話に対して定義される設定により異なります。 Cisco Extension Mobility でコール表示の制限を使用するには、**[デバイス プロファイルの設定（Device Profile Configuration）]** ウィンドウと **[電話の設定（Phone Configuration）]** ウィンドウの両方で、**[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)）]** チェックボックスをオンにします。

機能	データのやり取り
不在転送コーリング サーチ スペース	不在転送コーリング サーチ スペース（CSS）の機能強化により、機能性を失わずに Cisco Unified Communications Manager の新しいリリースにアップグレードできます。 [CFA CSS アクティベーション ポリシー（CFA CSS Activation Policy）] サービス パラメータがこの機能強化をサポートします。 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、このパラメータは次の 2 つのオプションとともに [クラスタ全体パラメータ（機能 - 転送）（Clusterwide Parameters (Feature - Forward)）] セクションに表示されます。 • [設定済みCSSを使用(With Configured CSS)]（デフォルト） • [アクティブなデバイス/回線CSSを使用(With Activating Device/Line CSS)]
取り込み中	Extension Mobility の場合、デバイス プロファイル設定にサイレント（DND）着信コール アラートとサイレント ステータスが含まれます。ユーザがログインしてサイレントを有効にすると、DND 着信コール アラートとサイレント ステータスの設定が保存され、ユーザが再度ログインするとこれらの設定が使用されます。 （注） Extension Mobility にログインしているユーザが DND 着信コール アラートまたはサイレント ステータスの設定を変更しても、このアクションは実際のデバイス設定に影響しません。
インターコム	Cisco Extension Mobility はインターコム機能をサポートします。 インターコムをサポートするために、Cisco Extension Mobility はインターコム回線用に設定されるデフォルトのデバイスを使用します。 インターコム回線はデフォルトのデバイスでのみ表示されます。 インターコム回線は、デバイス プロファイルに割り当てることができます。 ユーザがデフォルトのデバイス以外のデバイスにログインしたときは、インターコム回線は表示されません。 Cisco Extension Mobility のインターコムには次の追加の考慮事項が適用されます。 • Unified Communications Manager がインターコム回線をデバイスに割り当て、デフォルトのデバイス値が空の場合、現在のデバイスがデフォルトのデバイスとして選択されます。 • AXL がプログラムでインターコム DN を割り当てる場合、Cisco Unified Communications Manager の管理を使用してデフォルトのデバイスを設定することにより、インターコム DN を個別に更新する必要があります。 • インターコム回線のインターコム デフォルト デバイスとして設定されているデバイスを削除すると、インターコム デフォルト デバイスは削除されたデバイスに設定されなくなります。

機能	データのやり取り
Internet Protocol Version 6（IPv6）	Cisco Extension Mobility は IPv6 をサポートします。 IP アドレッシング モードが IPv6 またはデュアルスタック（IPv4 および IPv6）の電話を使用できます。
プライム回線	**[デバイス プロファイル（Device Profile）]** または **[デフォルトのデバイス プロファイル設定（Default Device Profile Configuration）]** ウィンドウの **[常にプライム回線を使用する（Always Use Prime Line）]** パラメータで **[オン（On）]** を選択した場合、Cisco Extension Mobility ユーザは、Cisco Extension Mobility をサポートするデバイスにログイン後にこの機能を使用できます。

Cisco Extension Mobility の制限

表 *34 : Cisco Extension Mobility* の制限

機能	制約事項
キャッシュ	Cisco Extension Mobility はすべてのログイン中のユーザ情報のキャッシュを 2 分間保持します。 キャッシュに存在するユーザに関する要求が Extension Mobility に届いた場合、ユーザはキャッシュからの情報で認証されます。 たとえば、ユーザがパスワードを変更してログアウトし、2 分以内に再度ログインした場合、古いパスワードと新しいパスワードの両方が認識されます。
コールバック	Cisco Extension Mobility のユーザがデバイスからログアウトすると、その Cisco Extension Mobility ユーザ用に有効になっているすべてのコールバック サービスは自動的にキャンセルされます。
文字表示	ユーザがログインするときに表示される文字は、現在の電話機のロケールによって異なります。 たとえば、電話機が現在英語のロケール（電話機のログアウト プロファイルに基づく）の場合、[ユーザ ID（UserID）] には英語の文字しか入力できません。
保留復帰	Cisco Extension Mobility は保留復帰機能をサポートしていません。
IP フォン	Cisco Extension Mobility には、ログインに物理 Cisco Unified IP 電話 が必要です。 Cisco Extension Mobility で設定されているオフィス電話のユーザは電話機にリモート ログインすることはできません。
ロケール（Locale）	ユーザまたはプロファイルに関連付けられているユーザ ロケールがロケールまたはデバイスと異なる場合、ログインが正常に完了すると、電話機は再起動してからリセットします。 この動作は、電話機設定ファイルが再作成されるために発生します。 プロファイルとデバイス間のアドオン モジュールの不一致でも同じ動作が発生します。

機能	制約事項
ログアウト	Cisco Extension Mobility が停止または再起動した場合、システムはログイン間隔の時間が経過したすでにログイン中のユーザを自動的にログアウトしません。つまりユーザの自動ログアウトは1日1回のみ行われます。電話機または Cisco Unified CM の管理から手動でこのようなユーザをログアウトさせることができます。
セキュア トーン	Cisco Extension Mobility および複数ライン同時通話機能サービスは、保護対象の電話では無効です。
ユーザ グループ	標準EM認証プロキシ権限のユーザ グループにユーザを追加できますが、追加されたユーザはプロキシによって認証する権限を持っていません。
ログインした最後のユーザを記憶する（Remember the Last User Logged In）	[ログインした最後のユーザを記憶する（Remember the Last User Logged In）] サービス パラメータが適用されるのは、デフォルトの Extension Mobility サービス URL、または `loginType` が `UID` に設定されている Extension Mobility サービス URL のみです。

エクステンションモビリティのトラブルシューティング

エクステンションモビリティのトラブルシューティング

手順

- Cisco Extension Mobility トレース ディレクトリを設定し、次の手順を実行してデバッグ トレースを有効にします。
  a) [Cisco Unified Serviceability] から、以下を選択します。**[トレース（Trace）] > [トレース構成（Trace Configuration）]**。
  b) [Server（サーバ）]ドロップダウン リストからサーバを選択します。
  c) [設定されたサービス（Configured Services）]ドロップダウン リストから、[Cisco Extension Mobility]を選択します。
- Cisco Extension Mobility サービスの URL を正しく入力したことを確認します。 URL では、小文字と大文字が区別されます。
- 設定手順をすべて適切に実行したことを確認します。
- Cisco Extension Mobility ユーザの認証で問題が発生する場合は、ユーザ ページに移動して PIN を確認します。

認証エラー

問題 「エラー 201 認証エラー（Error 201 Authentication Error）」が電話機に表示されます。

解決法 正しいユーザ ID と PIN が入力されていることを確認する必要があります。また、ユーザ ID と PIN が正しいことをシステム管理者と一緒に確認する必要があります。

ユーザ ID または PIN が空です

問題 「エラー 202 ユーザ ID または PIN が空です（Error 202 Blank User ID or PIN）」が電話機に表示されます。

解決法 有効なユーザ ID と PIN を入力してください。

ビジー。再実行してください

問題 「エラー 26 ビジー。再実行してください（Error 26 Busy Please Try Again）」が電話機に表示されます。

解決法 同時ログイン/ログアウト要求の数が [同時要求の最大数（Maximum Concurrent requests）] サービス パラメータより多いかどうかを確認します。 大きい場合は同時要求の数を小さくします。

（注） 同時ログイン/ログアウト要求の数を確認するには、Cisco Unified Real-Time Monitoring Tool を使用して Extension Mobility オブジェクト内の Requests In Progress カウンタを表示します。 詳細については、以下で『Cisco Unified Real-Time Monitoring Tool Administration Guide』を参照してください。http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

データベース エラー

問題 「エラー 6 データベース エラー」が電話機に表示されます。

解決法 大量の要求が存在するどうかを確認してください。 大量の要求が存在する場合は、Extension Mobility オブジェクト カウンタの Requests In Progress カウンタに高い値が表示されます。 大量の同時要求が原因で要求が拒否された場合は、Requests Throttled カウンタにも高い値が表示されます。 詳細なデータベース ログを収集します。

デバイスのログオンが無効

問題 「エラー 22 デバイスのログオンが無効（Error 22 Dev Logon Disabled）」が電話機に表示されます。

解決法 **[電話の設定（Phone Configuration）]** ウィンドウ（**[デバイス（Device）]** > **[電話機（Phone）]**）で、**[エクステンションモビリティの有効化（Enable Extension Mobility）]** チェックボックスがオンになっていることを確認してください。

デバイス名が空白です

問題 「エラー 207 デバイス名が空白です（Error 207 Device Name Empty）」が電話に表示されます。

解決法 Cisco Extension Mobility に設定されている URL が正しいことを確認してください。 詳細については、「関連項目」を参照してください。

関連トピック

Cisco Extension Mobility 電話サービスの設定 （503 ページ）

EM サービス接続エラー

問題 「エラー 207 EM サービス接続エラー（Error 207 EM Service Connection Error）」が電話機に表示されます。

解決法 Cisco Unified Serviceability で、**[ツール（Tools）]**>**[コントロール センター - 機能（Control Center—Feature）]** を選択することにより、Cisco Extension Mobility サービスが実行されていることを確認してください。

アップグレード時のエクステンションモビリティパフォーマンス

問題 アップグレード後のパブリッシャのバージョン切り替え時のエクステンションモビリティ（EM）ログインパフォーマンス。

解決法 エクステンションモビリティ（EM）のユーザーが Unified Communications Manager パブリッシャのバージョン切り替えアップグレード時にログインし、パブリッシャが非アクティブである場合、EM ログインデータはバージョン切り替え時に失われ、EM プロファイルはログアウトされます。

（注） バージョンの切り替え後にUnified Communications Managerがアクティブである場合のみ、EM ログインプロファイルはログアウトされ、ユーザーは再度ログインできます。

ホストを検出できません

問題 「ホストを検出できません（Host Not Found）」というエラー メッセージが電話機に表示されます。

解決法 Cisco Unified Serviceability で、**[ツール（Tools）]**>**[コントロール センターのネットワーク サービス（Control Center—Network Services）]** を選択することにより、Cisco Tomcat サービスが実行していることを確認してください。

HTTP エラー

問題 HTTP エラー（503）が電話機に表示されます。

解決法

- **[サービス（Services）]**ボタンを押したときにこのエラーが表示された場合は、Cisco Unified Serviceability で、**[ツール（Tools）] > [コントロール センターのネットワーク サービス（Control Center—Network Services）]** を選択することにより、Cisco IP 電話サービスが実行していることを確認してください。
- Extension Mobility サービスを選択したときにこのエラーが表示された場合は、Cisco Unified Serviceability で、**[ツール（Tools）] > [コントロール センターのネットワーク サービス（Control Center—Network Services）]** を選択することにより、Cisco Extension Mobility Application サービスが実行していることを確認してください。

電話機のリセット

問題 ユーザのログインまたはログアウト後、再起動する代わりに電話機がリセットされます。

考えられる原因 このリセットは、ロケールの変更が原因だと考えられます。

解決法 特に対処の必要はありません。 ログインするユーザまたはプロファイルに関連付けられているユーザ ロケールがロケールまたはデバイスと異なる場合、ログインが正常に完了すると、電話機は再起動し、次にリセットします。 このパターンは、電話機設定ファイルが再作成されるために発生します。

ログイン後に電話サービスが使用できない

問題 ログイン後、電話サービスが使用できません。

考えられる原因 この問題は、電話機にユーザ プロファイルがロードされたときに、ユーザ プロファイルに関連付けられたサービスがないために発生します。

解決法

- ユーザ プロファイルに Cisco Extension Mobility サービスが含まれていることを確認します。
- Cisco Extension Mobility が含まれるように、ユーザがログインする電話機の設定を変更します。 電話機が更新されたあと、ユーザは電話サービスにアクセスできるようになります。

ログアウト後に電話サービスが使用できない

問題 ユーザがログアウトし、電話機がデフォルト デバイス プロファイルに戻った後、電話サービスが使用できなくなります。

解決法

- **[自動デバイス プロファイルと電話の設定間の同期（Synchronization Between Auto Device Profile and Phone Configuration）]** エンタープライズ パラメータが **[はい（True）]** に設定されていることを確認します。
- 電話機を Cisco Extension Mobility サービスに登録します。

ユーザは既にログイン済み

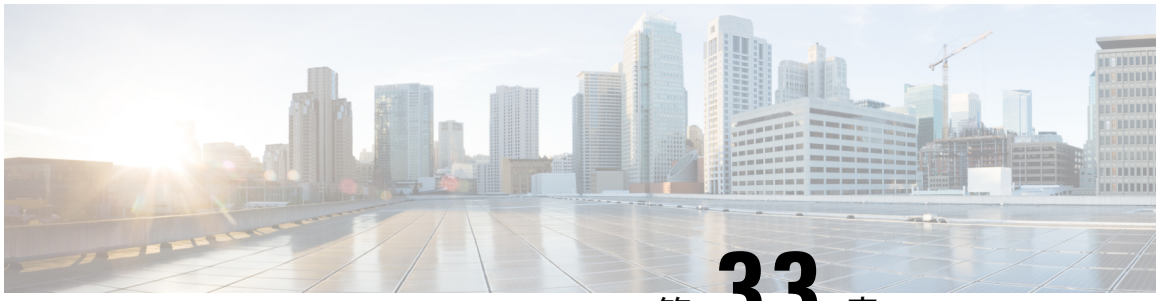
問題 「エラー 25 ユーザは既にログイン済み（Error 25 User Logged in Elsewhere）」が電話機に表示されます。

解決法 ユーザが別の電話機にログインしているかどうかを確認します。 複数のログインを許可する必要がある場合は、[複数のログイン動作（Multiple Login Behavior）] サービス パラメータが [複数のログインを許可（Multiple Logins Allowed）] に設定されていることを確認します。

ユーザ プロファイルなし

問題 「エラー 205 ユーザ プロファイルなし（Error 205 User Profile Absent）」が電話機に表示されます。

解決法 デバイス プロファイルをユーザに関連付けます。



第 33 章

クラスタ間のエクステンションモビリティ

Extension Mobility Cross Cluster の概要

Extension Mobility Cross Cluster（EMCC）機能は、Extension Mobilityと同じ機能をユーザに提供しますが、あるクラスタ（ホーム クラスタ）から移動して、別のリモート クラスタ（訪問先クラスタ）上の一時的な電話機にログインできるようにもします。そこから、ホームオフィスでIP電話を使用している場合のように、任意の場所から自分の電話設定にアクセスできます。

（注） リモートのEMCCクラスターが、ホームクラスタで構成された最小のTLSバージョンをサポートしていることを確認してください。

Extension Mobility Cross Cluster の前提条件

- Extension Mobility Cross Cluster（EMCC）の設定をサポートし、使用しているその他のコール制御エンティティ（その他の Cisco Unified Communications Manager クラスタ、EMCC クラスタ間サービス プロファイル、EMCC リモート クラスタ サービスなど）
- 非セキュアまたは混合モードに設定されたクラスタ。 詳細については、Extension Mobility Cross Cluster とさまざまなクラスタ バージョンのセキュリティ モード （555 ページ）を参照してください。
- セキュア モードまたは非セキュア モードでサポートされる電話機

Extension Mobility Cross Cluster の設定タスク フロー

始める前に

- Extension Mobility Cross Cluster の前提条件 （521 ページ）を確認してください。
- **Extension Mobility Cross Cluster の連携動作と制約事項**のレビュー

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 （5 ページ）	Extension Mobility Cross Cluster 機能をサポートするデバイスを特定するために、レポートを生成します。
ステップ 2	エクステンションモビリティの設定 （524 ページ）を行うには、次のサブタスクを実行します。 • Extension Mobility Cross Cluster のサービスの有効化 （524 ページ） • Extension Mobility 電話サービスの設定 （525 ページ） • Extension Mobility Cross Cluster のデバイス プロファイルの設定 （526 ページ） • ユーザに対する Extension Mobility Cross Cluster の有効化 （535 ページ） • エクステンションモビリティへのデバイスの登録 （536 ページ）	ユーザがクラスタ内の他の電話機から自分の電話機の設定（ライン アピアランス、サービス、短縮ダイヤルなど）に一時的にアクセスできるように Extension Mobility を設定します。 ユーザがホーム クラスタと訪問先クラスタのどちらからでも設定にアクセスできるように、ホーム クラスタとリモート クラスタの両方でこのタスク フローを実行します。
ステップ 3	Extension Mobility Cross Cluster の証明書の有効化 （537 ページ）を行うには、次のサブタスクを実行します。 • 一括プロビジョニング サービスの有効化 （537 ページ） • 一括証明書管理の設定および証明書のエクスポート （538 ページ） • 証明書の統合 （539 ページ） • クラスタへの証明書のインポート （540 ページ）	ホーム クラスタおよびリモート クラスタを適切に設定するには、各クラスタの証明書を同じ SFTP サーバと SFTP ディレクトリにエクスポートし、参加クラスタのいずれか1つでそれらを統合する必要があります。 この手順により、2つのクラスタ間で信頼が確立されていることを確認できます。

	コマンドまたはアクション	目的
ステップ 4	Extension Mobility Cross Cluster のデバイスおよびテンプレートの設定（541 ページ）を行うには、次のサブタスクを実行します。 • 共通デバイス設定の作成（542 ページ） • Extension Mobility Cross Cluster テンプレートの設定（542 ページ） • デフォルト テンプレートの設定（543 ページ） • Extension Mobility Cross Cluster デバイスの追加（543 ページ）	
ステップ 5	Extension Mobility Cross Cluster の位置情報フィルタの設定（544 ページ）	国、州、市の値などのデバイス ロケーションに合った基準を指定する地理位置情報フィルタを設定します。 地理位置情報はデバイスの場所を特定するために使用され、フィルタは地理位置情報のどの部分が重要であるかを示します。
ステップ 6	Extension Mobility Cross Cluster の機能パラメータの設定（544 ページ）	地理位置情報フィルタなどの設定した機能パラメータの値を選択します。
ステップ 7	Extension Mobility Cross Cluster のクラスタ間 SIP トランクの設定（549 ページ）	クラスタ間 PSTN アクセスおよび RSVP エージェント サービスの着信/発信トラフィックを処理するトランクを設定します。 1 つのトランクで PSTN アクセスと RSVP エージェント サービスの両方を処理するよう設定できます。または、サービスごとに 1 つずつトランクを設定することもできます。 Extension Mobility Cross Cluster に必要な SIP トランクは最大 2 つです。
ステップ 8	Extension Mobility Cross Cluster のクラスタ間サービス プロファイルの設定（550 ページ）	クラスタ間サービス プロファイルを設定して、Extension Mobility Cross Cluster を有効化します。 このプロファイルは、結果レポートより上位の設定および結果レポートを提供するすべての設定を収集します。
ステップ 9	リモート クラスタ サービスの設定（550 ページ）	Extension Mobility Cross Cluster のリモート クラスタを設定します。 この手順により、ホーム クラスタとリモート（訪

	コマンドまたはアクション	目的
		問先）クラスタを接続するリンクが確立します。

エクステンションモビリティの設定

ユーザがクラスタ内の他の電話機から自分の電話機の設定（ラインアピアランス、サービス、短縮ダイヤルなど）に一時的にアクセスできるように Extension Mobility を設定します。 ユーザがホーム クラスタと訪問先クラスタのどちらからでも設定にアクセスできるように、ホーム クラスタとリモート クラスタの両方でこのタスク フローを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	Extension Mobility Cross Cluster のサービスの有効化 （524 ページ）	
ステップ 2	Extension Mobility 電話サービスの設定 （525 ページ）	ユーザを登録できるExtension Mobilityの電話サービスを作成します。
ステップ 3	Extension Mobility Cross Cluster のデバイス プロファイルの設定 （526 ページ）	デバイスプロファイルを作成して、ユーザが Extension Mobility Cross Cluster にログインする際に実際のデバイスに設定をマッピングします。
ステップ 4	ユーザに対する Extension Mobility Cross Cluster の有効化 （535 ページ）	
ステップ 5	エクステンションモビリティへのデバイスの登録 （536 ページ）	すべてのデバイスに対してエンタープライズ サブスクリプションを設定していない場合には、エクステンションモビリティをデバイスで有効にし、サービスに登録します。

Extension Mobility Cross Cluster のサービスの有効化

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[ツール（Tools）] > [サービス アクティベーション（Service Activation）]** を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストから、必須のノードを選択します。

ステップ 3 、次のサービスを有効化します。

a) Cisco CallManager
b) Cisco Tftp
c) Cisco Extension Mobility
d) ILS サービス

（注） ILS サービスをアクティブ化するには、パブリッシャ ノードを選択する必要があります。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 **OK**をクリックします。

Extension Mobility 電話サービスの設定

ユーザを登録できるExtension Mobilityの電話サービスを作成します。

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）]** > **[電話サービス（Phone Services）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [サービス名（Service Name）] フィールドに、サービスの名前を入力します。

たとえば、Extension Mobility または EM などの名前を入力します。 Java MIDlet サービスの場合、サービス名は、Java Application Descriptor（JAD）ファイルで定義されている名前と正確に一致している必要があります。

ステップ 4 [サービス URL（Service URL）]フィールドに、次の形式でサービス URL を入力します。

```
http://<IP
Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#.
```

ステップ 5 （任意） HTTPS を使用して安全な URL を作成するには、次の形式でセキュアなサービス URL を入力します。

```
https://<IP
Address>:8443/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#
```

ステップ 6 （任意） さらに多くのサインイン オプションを設定するには、`loginType` パラメータを以下の形式で [サービス URL（Service URL）] に追加します。

- `loginType=DN` は、ユーザが主要内線番号と PIN を使用してサインインできるようにします。サービス URL の形式は、`http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#&loginType=DN` です。
- `loginType=SP` により、ユーザはセルフ サービス ユーザ ID と PIN を使用してログインできます。

サービス URL の形式は、 `http: //<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#&loginType=SP` です。

- `loginType=UID` により、ユーザはユーザ ID と PIN を使用してログインできます。

  サービス URL の形式は、`http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#&loginType=UID` です。

`loginType` パラメータは、セキュアな URL に付加することもできます。URL の最後に `loginType` を付加しなかった場合は、デフォルトのサインイン オプションとして [ユーザ ID（User ID）] と [PIN] が表示されます。

ステップ 7 [サービス カテゴリ（Service Category）]フィールドと [サービスの種類（Service Type）]フィールドのデフォルト値を使用します。

ステップ 8 **[有効（Enable）]** チェックボックスをオンにします。

ステップ 9 （任意） [エンタープライズ登録（Enterprise Subscription）] チェックボックスをオンにして、すべての電話およびデバイス プロファイルをこの電話サービスに登録します。

（注） サービスを初めて設定する際にこのチェックボックスをオンにすると、この IP フォンのサービスをエンタープライズ サブスクリプション サービスとして設定することになります。 社内のすべての電話およびデバイス プロファイルは、この IP Phone サービスに自動的に登録されるため、個別に登録する必要はありません。

ステップ 10 **[保存（Save）]** をクリックします。

Extension Mobility Cross Cluster のデバイス プロファイルの設定

デバイス プロファイルを作成して、ユーザが Extension Mobility Cross Cluster にログインする際に実際のデバイスに設定をマッピングします。

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）]** > **[デバイス設定（Device Settings）]** > **[デバイス プロファイル（Device Profile）]**。

ステップ 2 次のいずれかの作業を実行します。

- 既存のデバイス プロファイルを変更するには、**[検索（Find）]** をクリックして、検索条件を入力します。 結果のリストでデバイス プロファイル名をクリックします。
- 新しいデバイス プロファイルを追加するには、**[新規追加（Add New）]** をクリックして、**[次へ（Next）]** をクリックし、デバイス プロファイルのタイプを選択します。 **[次へ（Next）]** をクリックして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 [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、Extension Mobility Cross Cluster のデバイス プロファイル フィールド （527 ページ）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。

ステップ 5 新しいデバイス プロファイルに電話番号（DN）を追加します。

Extension Mobility Cross Cluster のデバイス プロファイル フィールド

表 *35 :* デバイス プロファイルの設定値

フィールド	説明
[製品のタイプ(Product Type)]	このデバイス プロファイルが適用される製品タイプを表示します。
デバイス プロトコル（Device Protocol）	このデバイス プロファイルが適用されるデバイス プロトコルを表示します。
[デバイスプロファイル名(Device Profile Name)]	一意の名前を入力します。この名前は 50 文字以内で作成してください。
説明	デバイス プロファイルの説明を入力します。 この特定のユーザ デバイス プロファイルを説明する内容を入力してください。
[ユーザ保留MOH音源(User Hold MOH Audio Source)]	ユーザが保留操作を開始したときに再生する音源を指定するには、[ユーザ保留 MOH 音源（User Hold MOH Audio Source）] ドロップダウン リストから音源を選択します。 音源を選択しなかった場合、Unified Communications Manager はデバイス プールで定義されている音源を使用します。または、デバイス プールで音源 ID が指定されていない場合は、システム デフォルトが使用されます。 （注） オーディオ ソースの定義は、[保留音オーディオソースの設定(Music On Hold Audio Source Configuration)] ウィンドウで行います。 このウィンドウにアクセスするには、**[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)]** の順に選択してください。

フィールド	説明
[ユーザロケール(User Locale)]	ドロップダウン リストから、電話機ユーザ インターフェイスに関連付けるロケールを選択します。 ユーザ ロケールは、言語やフォントなど、ユーザをサポートする一連の詳細情報を示します。 Unified Communications Manager ローカリゼーションをサポートする電話機モデルについてのみ、このフィールドを有効にします。 （注） ユーザ ロケールが指定されなかった場合、Unified Communications Manager はデバイス プールに関連付けられているユーザ ロケールを使用します。 情報を英語以外の言語で（電話機上に）表示する必要がある場合は、ユーザ ロケールを設定する前にロケール インストーラがインストールされていることを確認します。 Unified Communications Manager ロケール インストーラのドキュメントを参照してください。
[電話ボタンテンプレート(Phone Button Template)]	[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、電話ボタン テンプレートを選択します。 ヒント プレゼンス モニタリングのためにプロファイルに BLF/スピードダイヤルを設定する場合は、BLF/スピードダイヤル用に設定した電話ボタン テンプレートを選択します。 設定の保存後、[割り当て情報(Association Info)] ペインに [新規BLF SDを追加(Add a New BLF SD)] リンクが表示されます。 BLF/スピードダイヤルの詳細については、『Feature Configuration Guide for Cisco Unified Communications Manager』を参照してください。
ソフトキーテンプレート（Softkey Template）	[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。
[プライバシー（Privacy）]	[プライバシー（Privacy）] ドロップダウン リストから、プライバシーが必要な電話機ごとに [オン（On）] を選択します。 詳細については、『Feature Configuration Guide for Cisco Unified Communications Manager』を参照してください。

フィールド	説明
ワンボタン割り込み（Single Button Barge）	ドロップダウン リストから、次のオプションを選択します。 • [オフ(Off)]：このデバイスで、ユーザはワンボタン割り込み/C 割り込み機能を使用できなくなります。 • [割込み(Barge)]：このオプションを選択すると、ユーザは電話機のワンボタン割り込み共有回線ボタンを押し、割り込みを使用してコールに割り込むことができます。 • [デフォルト(Default)]：このデバイスは、サービス パラメータおよびデバイス プールの設定からワンボタン割り込み/C 割り込みの設定を取得します。 （注） サービス パラメータとデバイス プールの設定が異なる場合、デバイスはサービス パラメータの設定から取得します。 詳細については、『Feature Configuration Guide for Cisco Unified Communications Manager』を参照してください。
[回線をまたいで参加(Join Across Lines)]	ドロップダウン リストから、次のオプションを選択します。 • [オフ(Off)]：このデバイスで、回線をまたいで参加の機能を使用できなくなります。 • [オン(On)]：このデバイスで、複数の回線をまたいでコールに参加できるようになります。 • [デフォルト(Default)]：このデバイスは、サービス パラメータおよびデバイス プールの設定から、回線をまたいで参加の設定を取得します。 （注） サービス パラメータとデバイス プールの設定が異なる場合、デバイスはサービス パラメータの設定から取得します。 詳細については、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
[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。 他の回線のコールの呼び出し音は鳴り続けます。電話のユーザは、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）]：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 パラメータから、Cisco CallManager サービスをサポートしている設定を使用します。
[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。 • [オフ（Off）]：電話がアイドル状態の場合、電話の [メッセージ（Messages）] ボタンを押すと、電話は、ボイス メッセージがある回線のボイス メッセージ システムに自動的にダイヤルします。 Unified Communications Manager は、ボイス メッセージがある最初の回線を常に選択します。 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。 • デフォルト：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 for Voice Message）] サービス パラメータから、Cisco CallManager サービスをサポートする設定を使用します。

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))]	通話表示制限を設定し、内線通話に対して受信した表示制限を無視するには、「[表示インジケータを無視（内線通話のみ）]」チェックボックスをオンにします。 **ヒント** この設定は、トランスレーション パターン レベルで発呼者回線 ID の表示と接続側回線 ID の表示の設定を組み合わせて使用してください。 また、これらの設定値では、コール表示制限を設定して、各コールに対して発呼者の回線または接続側の回線の表示情報を選択的に表示またはブロックできます。コール表示制限の詳細については、『Feature Configuration Guide for Cisco Unified Communications Manager』を参照してください。
取り込み中	サイレント（DND）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を有効にした場合、このパラメータでは、DND機能が着信コールをどのように処理するかを指定します。 • [コール拒否（Call Reject）]：このオプションは、着信通話情報をユーザに表示しないようにします。 [DND着信呼警告（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。 • [呼出音オフ（Ringer Off）]：このオプションは、呼出音をオフにしますが、ユーザがコールを受け付けられるように、着信通話情報をデバイスに表示します。 • [共通の電話プロファイル設定を使用(Use Common Phone Profile Setting)]：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オプション(DND Option)] の設定値をデバイスに使用するように指定します。 （注） SCCP を実行している 7940/7960 電話の場合、選択できるのは [呼出音オフ（Ringer Off）] オプションだけです。 携帯デバイスとデュアルモード電話の場合、[コール拒否（Call Reject）] オプションのみを選択できます。 携帯デバイスまたはデュアルモード電話で [DNDコール拒否（DND Call Reject）] をアクティブにすると、デバイスに通話情報が表示されません。

フィールド	説明
[DND着信呼警告（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、このパラメータは電話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)]：このオプションを指定すると、[共通の電話プロファイル(Common Phone Profile)] ウィンドウの [DND着信呼警告(DND Incoming Call Alert)] 設定がこのデバイスで使用されるようになります。 • [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、着信通話情報が表示されます。 DND のオプションが [コール拒否(Call Reject)] の場合、警告は何も表示されず、デバイスには何の情報も送られません。 • [ビープ音のみ(Beep Only)]：このオプションを選択した場合、着信コールがあると、電話機のビープ音だけが再生されます。 • [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、電話機のフラッシュ アラートだけが表示されます。
[クラスタ間エクステンションモビリティのCSS(Extension Mobility Cross Cluster CSS)]	ドロップダウン リストから、Extension Mobility Cross Cluster機能について、このデバイス プロファイルに使用する既存のコーリング サーチ スペース（CSS）を選択します。 （新しい CSS を設定するか、既存の CSS を変更するには、Unified Communications Manager 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）]** を選択します）。 デフォルト値は、[なし(None)] です。 組織内管理者がこの CSS を指定します。ユーザがこのリモート電話機にログインすると、指定された CSS がデバイス CSS として電話機に割り当てられます。 詳細については、『Feature Configuration Guide for Cisco Unified Communications Manager』を参照してください。

フィールド	説明
[モジュール1（Module 1）]	拡張モジュール フィールド内の拡張モジュール ドロップダウン リストから電話テンプレートを選択することにより、1 つか 2 つの拡張モジュールをこのデバイス プロファイル用に設定できます。 （注） 電話ボタン テンプレート フィールドの隣にある [ボタン リストの表示(View button list)] リンクを選択すると、いつでも電話ボタン リストを表示できます。 新しいダイアログボックスが開き、その特定の拡張モジュール用の電話ボタンが表示されます。 適切な拡張モジュールを選択するか、または [なし(None)] を選択します。
[モジュール2(Module 2)]	適切な拡張モジュールを選択するか、または [なし(None)] を選択します。
[MLPP ドメイン(MLPP Domain)]	このユーザ デバイス プロファイルが MLPP 優先コールに使用される場合は、ドロップダウン リストから [MLPP ドメイン（MLPP Domain）] を選択します。 （注） MLPP ドメインは、[MLPP ドメインの設定(MLPP Domain Configuration)] ウィンドウで定義します。 このウィンドウにアクセスするには、**[システム(System)]** > **[MLPP ドメイン(MLPP Domain)]** を選択します。

フィールド	説明
[MLPP通知(MLPP Indication)]	このユーザ デバイス プロファイルを MLPP 優先コールに使用する場合、[MLPP通知(MLPP Indication)] の設定値をデバイス プロファイルに割り当てます。優先トーンを再生できるデバイスがMLPP優先コールの発信時にその再生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を次のオプションから選択します。 **1.** [デフォルト(Default)]：このデバイス プロファイルは、関連するデバイスのデバイス プールから [MLPP通知(MLPP Indication)] の設定値を引き継ぎます。 **2.** [オフ(Off)]：このデバイスは、MLPP 優先コールの通知の制御も処理もしません。 **3.** [オン(On)]：このデバイス プロファイルは、MLPP 優先コールの通知を制御し処理します。 （注） [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(Off)] の場合）に設定し、かつ [MLPPプリエンプション(MLPP Preemption)] を [強制(Forceful)] に設定するという組み合わせで、デバイス プロファイルを設定することはできません。

フィールド	説明
[MLPPプリエンプション(MLPP Preemption)]	このユーザ デバイス プロファイルを MLPP 優先コールに使用する場合、[MLPPプリエンプション(MLPP Preemption)] 設定をデバイス プロファイルに割り当てます。 進行中のコールを優先できるデバイスが MLPP 優先コールの発信時にその優先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を次のオプションから選択します。 **1.** [デフォルト(Default)]：このデバイス プロファイルは、関連するデバイスのデバイス プールから [MLPPプリエンプション(MLPP Preemption)] の設定値を引き継ぎます。 **2.** [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。 **3.** [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。 （注） [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(Off)] の場合）に設定し、かつ [MLPPプリエンプション(MLPP Preemption)] を [強制(Forceful)] に設定するという組み合わせで、デバイス プロファイルを設定することはできません。
[ログインユーザ ID(Login User Id)]	[ログイン ユーザ ID（Login User ID）] ドロップダウン リストから、有効なログイン ユーザ ID を選択します。 （注） ログアウト プロファイルとしてデバイス プロファイルが使用される場合、その電話機に関連付けられるログイン ユーザ ID を指定します。 ユーザがこのユーザ デバイス プロファイルからログアウトすると、電話機は自動的にこのログイン ユーザ ID にログインします。

ユーザに対する Extension Mobility Cross Cluster の有効化

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 次のいずれかの作業を実行します。

- 既存のユーザ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ユーザを選択します。
- **[新規追加（Add New）]** をクリックして、新しいユーザを追加します。

ステップ 3 [Extension Mobility] ペインで、[クラスタ間のエクステンションモビリティの有効化（Enable Extension Mobility Cross Cluster）] チェックボックスをオンにします。

ステップ 4 [Extension Mobility] ペインの [使用可能なプロファイル（Available Profiles）] リスト ペインからデバイス プロファイルを選択します。

ステップ 5 デバイス プロファイルを [制御するプロファイル（Controlled Profiles）] リスト ペインに移動します。

ステップ 6 **[保存（Save）]** をクリックします。

エクステンションモビリティへのデバイスの登録

すべてのデバイスに対してエンタープライズサブスクリプションを設定していない場合には、エクステンションモビリティをデバイスで有効にし、サービスに登録します。

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）]** > **[電話（Phone）]** から。

ステップ 2 ユーザが Extension Mobility Cross Cluster を使用できる電話を検索します。

ステップ 3 このデバイスでは、**[内線番号情報（Extension Information）]** ペインの **[Extension Mobility の有効化（Enable Extension Mobility）]** チェックボックスをオンにします。

ステップ 4 [電話の設定（Phone Configuration）]ウィンドウで、[関連事項（Related Links）]ドロップダウン リストの [サービスの登録/登録解除（Subscribe/Unsubscribe Services）]を選択します。

ステップ 5 [移動（Go）]をクリックします。

ステップ 6 ポップアップ ウィンドウが開いたら、[サービスの選択（Select a Service）]ドロップダウン リストの [Extension Mobility]サービスを選択します。

ステップ 7 [次へ（Next）]をクリックします。

ステップ 8 [登録（Subscribe）]をクリックします。

ステップ 9 ポップアップ ウィンドウで [保存（Save）]をクリックしてから、ウィンドウを閉じます。

ステップ 10 [電話の設定（Phone Configuration）]ウィンドウで [保存（Save）]をクリックします。

ステップ 11 表示された場合は、[OK]をクリックします。

Extension Mobility Cross Cluster の証明書の有効化

ホーム クラスタおよびリモート クラスタを適切に設定するには、各クラスタの証明書を同じ SFTP サーバと SFTP ディレクトリにエクスポートし、参加クラスタのいずれか 1 つでそれらを統合する必要があります。 この手順により、2 つのクラスタ間で信頼が確立されていることを確認できます。

始める前に

エクステンションモビリティの設定 （524 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	一括プロビジョニング サービスの有効化 （537 ページ）	
ステップ 2	一括証明書管理の設定および証明書のエクスポート （538 ページ）	ホーム クラスタおよびリモート クラスタの両方から証明書をエクスポートするには、[Cisco Unified CM の管理（Cisco Unified CM Administration）] で証明書の一括管理を設定します。
ステップ 3	証明書の統合 （539 ページ）	すべての参加クラスタが証明書をエクスポートしている場合には、証明書を統合します。 このオプションは、複数のクラスタが証明書を SFTP サーバにエクスポートする場合にのみ使用できます。
ステップ 4	クラスタへの証明書のインポート （540 ページ）	ホーム クラスタとリモート（訪問先）クラスタに証明書をインポートします。

一括プロビジョニング サービスの有効化

始める前に

エクステンションモビリティの設定 （524 ページ）

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[ツール（Tools）] > [サービス アクティベーション（Service Activation）]** を選択します。

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 [Cisco Bulk Provisioning Service] 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。

ステップ 5 **OK**をクリックします。

一括証明書管理の設定および証明書のエクスポート

ホーム クラスタおよびリモート クラスタの両方から証明書をエクスポートするには、[Cisco Unified CM の管理（Cisco Unified CM Administration）] で証明書の一括管理を設定します。

この手順では、クラスタ内の全ノードの証明書を含む PKCS12 ファイルを作成します。

（注）
- すべての参加クラスタは、同じ SFTP サーバと SFTP ディレクトリに証明書をエクスポートする必要があります。
- Tomcat、Tomcat-ECDSA、TFTP、CAPF の各証明書がいずれかのクラスタ ノードで再生成されるたびに、クラスタで証明書をエクスポートする必要があります。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から、**[セキュリティ（Security）]** > **[証明書の一括管理（Bulk Certificate Management）]** を選択します。

ステップ 2 ホーム クラスタとリモート クラスタの両方で到達可能な TFTP サーバを設定します。 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]** をクリックします。

ステップ 4 [エクスポート（Export）]をクリックします。

ステップ 5 [証明書の一括エクスポート（Bulk Certificate Export）]ウィンドウの [証明書のタイプ（Certificate Type）]フィールドで、[すべて（All）]を選択します。

ステップ 6 [エクスポート（Export）]をクリックします。

ステップ 7 **[閉じる（Close）]** をクリックします。

（注） 一括証明書エクスポートを実行すると、証明書は次のようにリモート クラスタにアップロードされます。

- CAPF 証明書は Callmanager-trust としてアップロードされます
- Tomcat 証明書は Tomcat-trust としてアップロードされます
- CallManager 証明書は Callmanager-trust としてアップロードされます
- CallManager 証明書は Phone-SAST-trust としてアップロードされます
- ITLRecovery 証明書は、PhoneSast-trust および CallManager-trust としてアップロードされます。

上記の手順は、証明書が自己署名証明書であり、別のクラスタに共通の信頼がない場合に実行されます。 共通の信頼関係または同じ署名者がいる場合は、すべての証明書のエクスポートは必要ありません。

証明書の統合

すべての参加クラスタが証明書をエクスポートしている場合には、証明書を統合します。 このオプションは、複数のクラスタが証明書を SFTP サーバにエクスポートする場合にのみ使用できます。

単一ファイルにするには、この手順で、SFTP サーバのすべての PKCS12 ファイルを統合します。

（注） 統合後に新しい証明書をエクスポートする場合には、新たにエクスポートされた証明書を含めるため、この手順を再度実行する必要があります。

手順

ステップ 1 [Cisco Unified OS 管理（Cisco Unified OS Administration）] から、以下を選択します。**[セキュリティ（Security）] > [証明書の一括管理（Bulk Certificate Management）] > [統合（Consolidate）] > [証明書の一括統合（Bulk Certificate Consolidate）]** を選択します。

ステップ 2 [証明書タイプ（Certificate Type）]フィールドで、[すべて（All）]を選択します。

ステップ 3 [統合（Consolidate）]をクリックします。

（注） 一括証明書統合を実行すると、証明書は次のようにリモート クラスタにアップロードされます。

- CAPF 証明書は Callmanager-trust としてアップロードされます
- Tomcat 証明書は Tomcat-trust としてアップロードされます
- CallManager 証明書は Callmanager-trust としてアップロードされます
- CallManager 証明書は Phone-SAST-trust としてアップロードされます
- ITLRecovery 証明書は、PhoneSast-trust および CallManager-trust としてアップロードされます。

クラスタへの証明書のインポート

ホーム クラスタとリモート（訪問先）クラスタに証明書をインポートします。

（注） アップグレード後、これらの証明書が維持されます。 証明書の再インポートや再統合をする必要はありません。

注意 証明書をインポートした後、クラスタの電話は自動的に再起動します。

手順

ステップ 1 [Cisco Unified OS 管理（Cisco Unified OS Administration）] から、以下を選択します。**[セキュリティ（Security）] > [証明書の一括管理（Bulk Certificate Management）] > [インポート（Import）] > [証明書の一括インポート（Bulk Certificate Import）]** を選択します。

ステップ 2 [証明書タイプ（Certificate Type）] ドロップダウン リストから、[すべて（All）]を選択します。

ステップ 3 [Import] を選択します。

（注） 一括証明書インポートを実行すると、証明書は次のようにリモート クラスタにアップロードされます。

- CAPF 証明書は Callmanager-trust としてアップロードされます
- Tomcat 証明書は Tomcat-trust としてアップロードされます
- CallManager 証明書は Callmanager-trust としてアップロードされます
- CallManager 証明書は Phone-SAST-trust としてアップロードされます
- ITLRecovery 証明書は、PhoneSast-trust および CallManager-trust としてアップロードされます。

（注） 次のタイプの証明書により、再起動する電話が決定されます。

- Callmanager：TFTP サービスが、証明書が属するノード上でアクティブになっている場合にのみ、すべての電話。
- TV：Callmanager グループ メンバーシップに基づいて、一部の電話。
- CAPF：CAPF がアクティブになっている場合にのみ、すべての電話。

Extension Mobility Cross Cluster のデバイスおよびテンプレートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	共通デバイス設定の作成 （542 ページ）	共通デバイス設定を行い、特定のユーザと関連付けられるサービスまたは機能を指定します。
ステップ 2	Extension Mobility Cross Cluster テンプレートの設定 （542 ページ）	Extension Mobility Cross Cluster テンプレートを作成して、共通デバイス設定をこの機能と関連付けます。
ステップ 3	デフォルト テンプレートの設定 （543 ページ）	デフォルト テンプレートとして作成した Extension Mobility Cross Cluster テンプレートを設定します。
ステップ 4	Extension Mobility Cross Cluster デバイスの追加 （543 ページ）	Extension Mobility Cross Cluster デバイスのエントリをシステム データベースに挿入します。 各デバイスは、EMCC1、EMCC2 のような形式の一意の名前で識別されます。 一括管理ツールは、最後

	コマンドまたはアクション	目的
		に使用した番号を取得してデバイス番号を割り当てます。

共通デバイス設定の作成

共通デバイス設定を行い、特定のユーザと関連付けられるサービスまたは機能を指定します。

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。**[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 次のいずれかの作業を実行します。

- 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] 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。

Extension Mobility Cross Cluster テンプレートの設定

Extension Mobility Cross Cluster テンプレートを作成して、共通デバイス設定をこの機能と関連付けます。

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。**[一括管理（Bulk Administration）] > [EMCC] > [EMCCテンプレート（EMCC Template）]** 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 [EMCC テンプレートの設定（EMCC 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。

デフォルト テンプレートの設定

デフォルト テンプレートとして作成した Extension Mobility Cross Cluster テンプレートを設定します。

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。**[一括管理（Bulk Administration）]** > **[EMCC]** > **[EMCCの挿入/更新（Insert/Update EMCC）]** を選択します。

ステップ 2 [EMCC デバイスの更新（Update EMCC Devices）]をクリックします。

ステップ 3 [デフォルト EMCC テンプレート（Default EMCC Template）]ドロップダウン リストから、設定した Extension Mobility Cross Cluster デバイス テンプレートを選択します。

ステップ 4 [今すぐ実行（Run Immediately）]をクリックします。

ステップ 5 [送信（Submit）]をクリックします。

ステップ 6 ジョブの成功を確認します。

a) **[一括管理(Bulk Administration)]** > **[ジョブスケジューラ(Job Scheduler)]** の順に選択します。

b) ジョブのジョブ ID を検索します。

Extension Mobility Cross Cluster デバイスの追加

Extension Mobility Cross Cluster デバイスのエントリをシステム データベースに挿入します。 各デバイスは、EMCC1、EMCC2 のような形式の一意の名前で識別されます。 一括管理ツールは、最後に使用した番号を取得してデバイス番号を割り当てます。

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。 から、**[一括管理（Bulk Administration）]** > **[EMCC]** > **[EMCCの挿入/更新（Insert/Update EMCC）]** を選択します。

ステップ 2 [挿入/更新 EMCC（Insert/Update EMCC）] をクリックします。

ステップ 3 [追加する EMCC デバイスの数（Number of EMCC Devices to be added）] フィールドに、追加するデバイスの数を入力します。

ステップ 4 [今すぐ実行（Run Immediately）] をクリックして、[送信（Submit）] をクリックします。

ステップ 5 ウィンドウを更新し、データベースの [すでにデータベースにある EMCC デバイスの数（Number of EMCC Devices already in database）] の値が追加したデバイスの数を示していることを確認します。

Extension Mobility Cross Cluster の位置情報フィルタの設定

国、州、市の値などのデバイス ロケーションに合った基準を指定する地理位置情報フィルタを設定します。地理位置情報はデバイスの場所を特定するために使用され、フィルタは地理位置情報のどの部分が重要であるかを示します。

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）] > [位置情報フィルタ（Geolocation Filter）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [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、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。

Extension Mobility Cross Cluster の機能パラメータの設定

地理位置情報フィルタなどの設定した機能パラメータの値を選択します。

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。**[拡張機能（Advanced Features）] > [EMCC] > [EMCC 機能設定（VPN Feature Configuration）]**。

ステップ 2 [EMCC機能の設定（EMCC Feature 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、Extension Mobility Cross Cluster の機能パラメータ フィールド （544 ページ）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。

Extension Mobility Cross Cluster の機能パラメータ フィールド

表 *36 : Extension Mobility Cross Cluster* の機能パラメータ フィールド

EMCC パラメータ	説明
[Default TFTP Server for EMCC Login Device]	リモート クラスタから Extension Mobility Cross Cluster（EMCC）にログインしているデバイスが使用する必要のあるデフォルト TFTP サーバのコンピュータ名または IP アドレスを選択します。

EMCC パラメータ	説明
[Backup TFTP Server for EMCC Login Device]	リモート クラスタから EMCC にログインするデバイスが使用するバックアップ TFTP サーバのコンピュータ名または IP アドレスを選択します。
[Default Interval for Expired EMCC Device Maintenance]	期限切れの EMCC デバイスのシステム チェックを行う間隔を分数で指定します。 期限切れの EMCC デバイスは、リモート クラスタから EMCC にログインしていたものの、WAN 障害や接続の問題が原因で、電話機が訪問先クラスタからログアウトしたデバイスです。 接続が復旧すると、デバイスは、訪問先クラスタにログインし直しました。 このメンテナンス ジョブ中に、Cisco Extension Mobility サービスは Unified Communications Manager データベースに期限切れの EMCC デバイスがないかチェックし、それらを自動的にログアウトさせます。 デフォルト値は 1440 分です。 有効な値の範囲は 10 ～ 1440 分です。
[Enable All Remote Cluster Services When Adding A New Remote Cluster]	新しいリモート クラスタを追加したときに、そのクラスタ上のすべてのサービスを自動的に有効にするかどうかを選択します。 有効な値は、[はい（True）]（リモート クラスタ上のすべてのサービスが自動的に有効）または [いいえ（False）]（Unified Communications Manager の [リモート クラスタの設定（Remote Cluster Configuration）] ウィンドウを介して、リモート クラスタ上のサービスを手動で有効）です。 リモート サービスを有効にする前に EMCC 機能のすべてを設定する時間が取れるように、サービスを手動で有効化できます。 デフォルト値は [False] です。

EMCC パラメータ	説明
[CSS for PSTN Access SIP Trunk]	EMCC コールを処理する PSTN アクセス SIP トランクが使用するコーリング サーチ スペース（CSS）を選択します。 PSTN アクセス SIP トランクは、[クラスタ間サービス プロファイル（Intercluster Service Profile）] ウィンドウで、PSTN アクセスに対して設定された SIP トランクです。 このトランク経由のコールは、コールを開始した EMCC ログイン電話機と同じ場所に設置されたローカル PSTN 向けで、それにのみルーティングされます。 有効な値は次のとおりです。 • [トランク CSS を使用する（Use Trunk CSS）]（PSTN コールは、緊急サービス通報を正しくルーティングするのに有用であることがわかっているローカル ルート グループを使用します） • [電話機の元のデバイスの CSS を使用する（Use phone's original device CSS）]（PSTN コールは、リモート電話機で設定されたコール コーリング サーチ スペース、つまり、電話機が EMCC にログインしていないときに使用される CSS を使用してルーティングされます）。 デフォルト値は [トランク CSS を使用する（Use Trunk CSS）] です。
EMCC 地理位置情報フィルタ（EMCC Geolocation Filter）	EMCC を使用するために設定した地理位置情報フィルタを選択します。 別のクラスタから Extension Mobility 経由でログインした電話機に関連付けられた地理位置情報内の情報と、選択された EMCC 地理位置情報フィルタに基づいて、Cisco Unified Communications Manager が電話機をローミング デバイス プールに配置します。 Cisco Unified Communications Manager は、EMCC 地理位置情報フィルタの適用後に電話機の地理位置情報と最も一致するデバイス プールを特定することにより、使用するローミング デバイス プールを決定します。
[EMCC Region Max Audio Bit Rate]	このパラメータは、相手側に関連付けられたリージョンとは無関係に、すべての EMCC コールの最大オーディオ ビット レートを指定します。 デフォルト値は 8 kbps（G.729）です。 （注） すべての参加 EMCC クラスタが EMCC リージョンの最大オーディオ ビット レートに対して同じ値を指定する必要があります。

EMCC パラメータ	説明
[EMCC Region Max Video Call Bit Rate (Includes Audio)]	このパラメータは、相手側に関連付けられたリージョンのビデオ コールの最大ビットレートとは無関係に、すべての EMCC ビデオ コールの最大ビット レートを指定します。 デフォルト値は 384 です。有効値の範囲は 0 ～ 8128 です。 （注） すべての参加 EMCC クラスタが EMCC リージョンの最大ビデオ ビット レートに対して同じ値を指定する必要があります。

EMCC パラメータ	説明
[EMCC Region Link Loss Type]	このパラメータは、任意のリモート クラスタの任意の EMCC 電話機とデバイス間のリンク損失タイプを指定します。 （注） EMCC コールでの双方向オーディオを許可するには、すべての参加 EMCC クラスタが同じ EMCC リージョン リンク損失タイプを使用する必要があります。 選択されたオプションに基づいて、Cisco Unified Communications Manager は、設定された EMCC リージョン最大オーディオ ビット レートを順守しながら、EMCC コールに最適な音声コーデックを使用しようとします。 有効な値は次のとおりです。 • [高損失（Lossy）] : DSL などの何らかのパケット損失が発生する可能性があるリンク。 • [低損失（Low Loss）] : T1 などの低パケット損失が発生するリンク。 このパラメータを [高損失（Lossy）] に設定した場合は、Cisco Unified Communications Manager は音声品質に基づいて、[EMCC リージョン最大オーディオ ビット レート（EMCC Region Max Audio Bit Rate）] で設定された制限内で最適なコーデックを選択します。 何らかのパケット損失が発生します。 このパラメータを [低損失（Low Loss）] に設定した場合は、Cisco Unified Communications Manager は音声品質に基づいて、[EMCC リージョン最大オーディオ ビット レート（EMCC Region Max Audio Bit Rate）] で設定された制限内で最適なコーデックを選択します。 パケット損失は、ほとんど発生しません。 [低損失（Low Loss）] オプションと [高損失（Lossy）] オプション間の音声コーデック優先順位の違いは、リンク損失タイプが [低損失（Low Loss）] に設定された場合は G.722 が Internet Speech Audio Codec（iSAC）より優先され、リンク損失タイプが [高損失（Lossy）] に設定された場合は iSAC が G.722 より優先される点だけです。 デフォルト値は [低損失（Low Loss）] です。

EMCC パラメータ	説明
[RSVP SIP Trunk KeepAlive Timer]	Unified Communications Manager が EMCC RSVP SIP トランク経由の 2 つのクラスタ間のキープアライブ メッセージまたは確認応答の送受信間で待機する秒数を指定します。 EMCC RSVP SIP トランクは、Cisco Extension Mobility Cross Clusterで [トランク サービス タイプ（Trunk Service Type）] として設定され、[クラスタ間サービス プロファイル（Intercluster Service Profile）] ウィンドウで RSVP エージェント用の SIP トランクとして選択された SIP トランクです。 これらのインターバルの 2 つがキープアライブ メッセージまたは確認応答を受信せずに経過した場合、Unified Communications Manager はリモート クラスタを含む RSVP リソースを解放します。 デフォルト値は 15 秒です。 有効な値の範囲は 1 ～ 600 秒です。
[Default Server for Remote Cluster Update]	Cisco Extension Mobility サービスがアクティブになっているこのローカル クラスタ内のプライマリ ノードのデフォルト サーバ名または IP アドレスを選択します。 リモート クラスタはこのノードにアクセスして、このローカル クラスタの情報を取得します。
[Backup Server for Remote Cluster Update]	Cisco Extension Mobility サービスがアクティブになっているこのローカル クラスタ内のセカンダリ ノードのデフォルト サーバ名または IP アドレスを選択します。 リモート クラスタは、プライマリ ノードがダウンしたときに、このノードにアクセスして、このローカル クラスタに関する情報を入手します。
[Remote Cluster Update Interval]	ローカル ノード上の Cisco Extension Mobility サービスがリモート EMCC クラスタに関する情報を収集する間隔を分単位で指定します。 収集される情報には、リモート クラスタ Unified Communications Manager のバージョンとサービス情報などの詳細が含まれます。 デフォルト値は 30 です。有効値の範囲は 15 ～ 10,080 分です。

Extension Mobility Cross Cluster のクラスタ間 SIP トランクの設定

クラスタ間 PSTN アクセスおよび RSVP エージェント サービスの着信/発信トラフィックを処理するトランクを設定します。 1 つのトランクで PSTN アクセスと RSVP エージェント サービスの両方を処理するよう設定できます。または、サービスごとに 1 つずつトランクを設定することもできます。 Extension Mobility Cross Cluster に必要な SIP トランクは最大 2 つです。

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)]** > **[トランク(Trunk)]**。

ステップ 2 [新規追加] 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 [**トランクのサービスの種類（Trunk Service Type**）] ドロップダウン リストから、[**Extension Mobility Cross Clusters**] 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 [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。

Extension Mobility Cross Cluster のクラスタ間サービス プロファイルの設定

クラスタ間サービス プロファイルを設定して、Extension Mobility Cross Cluster を有効化します。このプロファイルは、結果レポートより上位の設定および結果レポートを提供するすべての設定を収集します。

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。**[高度機能（Advance Features）] > [EMCC] > [EMCC クラスタ間サービス プロファイル（EMCC Intercluster Service Profile）]**。

ステップ 2 [EMCC クラスタ間サービス プロファイルの設定（EMCC Intercluster Service 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、オンライン ヘルプを参照してください。

ステップ 3 ポップアップ ウィンドウに失敗のメッセージが表示されていない場合は、[保存（Save）] をクリックします。

リモート クラスタ サービスの設定

Extension Mobility Cross Cluster のリモート クラスタを設定します。この手順により、ホーム クラスタとリモート（訪問先）クラスタを接続するリンクが確立します。

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。から **[高度な機能（Advanced Features）] > [クラスタ ビュー（Cluster View）]**。

ステップ 2 [検索（**Find**）] をクリックして、既存のリモート クラスタの一覧を表示します。

ステップ 3 次のいずれかの手順を実行します。

- リモートクラスタ名をクリックして、設定するリモートクラスタが表示されたら、フィールドを確認します。
- 設定するリモートクラスタが表示されない場合は、**[新規追加（Add New）]** をクリックして、次のフィールドを設定します。

1. [クラスタ ID（Cluster Id）]フィールドで、IDが他のクラスタのクラスタ IDのエンタープライズ パラメータ値と一致することを確認します。
2. **[完全修飾名（Fully Qualified Name）]** フィールドに、リモート クラスタの IP アドレスまたはリモート クラスタ上のノードに解決できるドメイン名を入力します。
3. **[保存]** をクリックします。

（注） Extension Mobility Cross Cluster では、[TFTP]チェックボックスが常に無効である必要があります。

Extension Mobility Cross Cluster の連携動作

表 *37 : Extension Mobility Cross Cluster* の連携動作

機能	データのやり取り
音声	EMCC ログインデバイスのデフォルトのオーディオ ビットレートは最大 8 kbps に設定されます（G.729）。
コール アドミッション制御（CAC）	• ホーム クラスタは、訪問先クラスタの場所と領域を認識しません。 • システムは、クラスタの境界を越えて Cisco Unified Communications Manager の場所とリージョンを適用できません。 • RSVP エージェント ベースの CAC は、訪問先クラスタで RSVP のエージェントを使用します。
通話転送	EMCC はコール転送をサポートしています。
Cisco Extension Mobility のログインおよびログアウト	ユーザ認証は、クラスタ間で行われます。

機能	データのやり取り
訪問先電話機でのメディア リソース	例としては、RSVP エージェント、TRP、保留音（MoH）、MTP、トランスコーダと会議ブリッジがあります。 メディア リソースは、訪問先電話に対してローカルです（RSVP エージェント以外）。
訪問先電話機に対する PSTN アクセス	• E911 コールは PSTN のローカル ゲートウェイにルーティングされます。 • 市内コールは PSTN のローカル ゲートウェイにルーティングされます。 • ローカル ルート グループへのコール切断は、訪問先クラスタのローカル ゲートウェイにルーティングされます。
その他のコール機能とサービス	制約事項の例：インターコム設定が静的デバイスに対する構成を指定するため、EMCC はインターコム機能をサポートしません。
セキュリティ	• Cross-cluster セキュリティはデフォルトで提供されています。 • セキュアな Cisco Unified IP Phones と非セキュアな電話セキュリティ プロファイルがサポートされています。

Extension Mobility Cross Cluster の制約事項

表 *38 : Extension Mobility Cross Cluster* の制約事項

制約事項	説明
サポートされない機能	• インターコムの設定にはスタティック デバイスが必要になるため、EMCC はインターコム機能をサポートしていません。 • EMCC はロケーション CAC をサポートしませんが、RSVP ベースの CAC をサポートします。 • IPv6 専用アドレス モードの電話は EMCC をサポートしません。 IPv4 またはデュアル スタック アドレス モードのいずれかを使用する電話を使用できます。
EMCC デバイスは複数のクラスタでプロビジョニングできません	EMCC を正しく機能させる場合、2 つのクラスタに同じ電話（デバイス名）は設定できません。 そうしないと、重複デバイス エラー (37) によりログインに失敗します。 したがって、EMCC で展開されるクラスタでは、すべての Unified Communication Manager ノードで自動登録を無効にして、EMCC ログアウト後にホーム クラスタに新しいデバイスが作成されるのを防ぐ必要があります。

制約事項	説明
EMCC デバイスの数	Cisco Unified Communications Manager では、電話機の最大数の値として 60,000 をサポートすることができます。 次の計算式を使用して、クラスタでサポートされるデバイスの合計数に EMCC を含めます。 電話 +（2 X EMCC デバイス）= MaxPhones （注） EMCC ログインはホーム クラスタで使用されるライセンスの数に影響を及ぼしません。
訪問先デバイスからのログアウトの制限	• ユーザが EMCC を使用してログインしている間に、ホーム クラスタの管理者がそのユーザの EMCC を無効にした場合、そのユーザは自動的にはログアウトされませんが、そのユーザによるその後の EMCC の使用の試みは許可されません。 現在の EMCC セッションはユーザがログアウトするまで続行されます。 • 訪問先クラスタの [電話の設定（Phone Configuration）]ウィンドウには、Extension Mobilityの [ログアウト（Log Out）] ボタンがあります。このボタンは、訪問先クラスタの管理者が EMCC 電話からログアウトするためにも使用されます。 現時点では、EMCC 電話は訪問先の Cisco Unified Communications Manager には登録されていないため、この操作は訪問先クラスタでのデータベース クリーンアップに似ています。 EMCC 電話は、ホーム クラスタのリセットやホーム クラスタからのログアウトによりその電話が訪問先クラスタに戻るまで、ホームの Cisco Unified Communications Manager に登録されたままになります。

制約事項	説明
訪問先デバイスのログインの制限	参加クラスタのExtension Mobility サービスでは、リモート クラスタの定期的な更新が行われます。 [リモート クラスタ更新間隔（Remote Cluster Update Interval）]機能パラメータで更新間隔を制御します。 デフォルトの間隔は 30 分です。 クラスタ A のエクステンションモビリティ サービスが、この更新に関するリモート クラスタ（クラスタ B など）からの応答を受信しない場合、クラスタ A の [リモート クラスタ] ウィンドウに「クラスタ B のリモート起動サービスが [False] に設定されている」ことが表示されます。 この場合、訪問先クラスタはホーム クラスタから応答を受信しないため、ホーム クラスタのリモート起動サービスの値が [False] に設定されます。 この間、訪問先電話は EMCC を使用してログインできない場合があります。 訪問先電話に「ログイン不可（Login is unavailable）」エラー メッセージが表示されます。 この時点で、訪問先電話から EMCC へのログインの試みは失敗する可能性があり、「ログイン不可（Login is unavailable）」エラー メッセージが電話に表示されます。 このエラーは、ホーム クラスタがアウトオブサービスからインサービスに変わったことを、訪問先クラスタが検出できなかったために発生します。 リモート クラスタのステータスの変更は、EMCC の [リモート クラスタ更新間隔（Remote Cluster Update Interval）] 機能パラメータの値に基づいており、訪問先のExtension Mobility サービスで最後のクエリや更新が実行されると行われます。 **[リモート クラスタ サービスの設定（Remote Cluster Service Configuration）]** ウィンドウ（**[詳細機能（Advanced Features）]** > **[EMCC]** > **[EMCC リモート クラスタ（EMCC Remote Cluster）]**）の **[リモート クラスタを今すぐ更新（Update Remote Cluster Now）]**を選択すると、リモート起動サービスの値を [True] に変更でき、EMCC ログインが可能になります。 それ以外の場合、次の定期的な更新サイクルの後、訪問先電話による EMCC ログインは正常に戻ります。

loginType を使用した異なるクラスタ バージョンの EMCC ログイン結果

次の表に、`loginType` パラメータをサービス URL で使用する場合の各クラスタ バージョンの Extension Mobility Cross Cluster 機能のログイン結果を示します。

表 *39 : loginType* を使用した異なるクラスタ バージョンの *EMCC* ログイン結果

訪問先クラスタのバージョン	ホームクラスタのバージョン	訪問先クラスタ EM URL の `loginType`	EMCC ログイン結果
12.0	12.0	指定なし（デフォルト URL）	成功（Success）
12.0	12.0	UID、SP、または DN	成功（Success）
12.0	11.5 以下	指定なし（デフォルト URL）	成功（Success）
12.0	11.5 以下	UID、SP、または DN	失敗（Fail） 失敗、エラーコード -1 **
11.5 以下	12.0	指定なし（デフォルト URL）	成功（Success）
11.5 以下	12.0	UID、SP、または DN ***	成功（Success）

（注）
- * `loginType` パラメータ オプションは次のとおりです。
  - UID：ユーザ ID および PIN を使用したユーザ ログイン
  - SP - ユーザはセルフサービス ユーザ ID および PIN を使用してログインします
  - DN：プライマリ エクステンションおよび PIN を使用したユーザ ログイン
- ** 失敗、エラーコード - 1：（EMAervice が EMApp または EMService からの XML 要求を解析できなかった場合）
- *** `loginType` は無視され、ユーザ ID または PIN のログイン プロンプトが電話機に読み込まれます

Extension Mobility Cross Cluster とさまざまなクラスタ バージョンのセキュリティ モード

（注） 電話コンフィギュレーション ファイルは、ホーム クラスタと訪問先クラスタの両方のバージョンが 9.x 以降で、TFTP 暗号化設定フラグが有効になっている場合にのみ、暗号化できます。

EMCC のログイン中は、訪問先クラスタとホーム クラスタの両方のバージョンが 9.x 以降の場合に、電話機が次の表に示すさまざまなモードで動作します。

表 *40 :* 訪問先クラスタとホーム クラスタの両方が *9.x* 以降のバージョンの場合にサポートされるセキュリティ モード

ホーム クラスタのバージョン	ホームクラスタのモード	訪問先クラスタのバージョン	訪問先クラスタのモード	訪問先電話機のモード	EMCC のステータス
9.x 以降	混合	9.x 以降	混合	セキュア	セキュア EMCC
9.x 以降	混合	9.x 以降	混合	非セキュア	非セキュア EMCC
9.x 以降	混合	9.x 以降	非セキュア	非セキュア	非セキュア EMCC
9.x 以降	非セキュア	9.x 以降	混合	セキュア	ログインに失敗する
9.x 以降	非セキュア	9.x 以降	非セキュア	非セキュア	非セキュア EMCC

EMCC のログイン中は、訪問先クラスタのバージョンが 8.x でホーム クラスタのバージョンが 9.x 以降の場合に、電話機が次の表に示すさまざまなモードで動作します。

表 *41 :* 訪問先クラスタが *8.x* でホーム クラスタが *9.x* 以降のバージョンの場合にサポートされるセキュリティ モード

ホーム クラスタのバージョン	ホームクラスタのモード	訪問先クラスタのバージョン	訪問先クラスタのモード	訪問先電話機のモード	EMCC のステータス
9.x 以降	混合	8.x	混合	セキュア	サポート対象外
9.x 以降	混合	8.x	混合	非セキュア	非セキュア EMCC
9.x 以降	混合	8.x	非セキュア	非セキュア	非セキュア EMCC
9.x 以降	非セキュア	8.x	混合	セキュア	サポート対象外

ホーム クラスタのバージョン	ホーム クラスタのモード	訪問先クラスタのバージョン	訪問先クラスタのモード	訪問先電話機のモード	EMCC のステータス
9.x 以降	非セキュア	8.x	非セキュア	非セキュア	非セキュア EMCC

EMCC のログイン中は、訪問先クラスタのバージョンが 9.x 以降でホーム クラスタのバージョンが 8.x の場合に、電話機が次の表に示すさまざまなモードで動作します。

表 *42 :* 訪問先クラスタが *9.x* 以降でホーム クラスタが *8.x* のバージョンの場合にサポートされるセキュリティ モード

ホーム クラスタのバージョン	ホーム クラスタのモード	訪問先クラスタのバージョン	訪問先クラスタのモード	訪問先電話機のモード	EMCC のステータス
8.x	混合	9.x 以降	混合	セキュア	ログインに失敗する
8.x	混合	9.x 以降	混合	非セキュア	非セキュア EMCC
8.x	混合	9.x 以降	非セキュア	非セキュア	非セキュア EMCC
8.x	非セキュア	9.x 以降	混合	セキュア	ログインに失敗する
8.x	非セキュア	9.x 以降	非セキュア	セキュア	非セキュア EMCC

Extension Mobility Cross Clusterのトラブルシューティング

エクステンションモビリティ アプリケーションのエラー コード

表 *43 :* エクステンションモビリティ アプリケーションのエラー コード

エラーコード（**Error Code**）	電話機のディスプレイ	短い説明	理由（**Reason**）
201	再度ログインしてください（201）（Please try to login again （201））	認証エラー	EMCCユーザの場合は、**[クラ** **ビスプロファイル（Intercluste** **Profile）]** ウィンドウで 「EMC クティブになっていないときに ラーが発生する可能性があり
202	再度ログインしてください（202）（Please try to login again （202））	ユーザ ID または PIN が空です	ユーザが空白のユーザ ID また 入力しました。
204	ログインできません（204）（Login is unavailable （204））	ディレクトリ サーバ エラー	EMAppは、IMSで指定された ユーザを認証できなかったとき エラーを電話機に送信します。
205	ログインできません（205）（Login is unavailable （204）） ログアウトできません（205）（Logout is unavailable （205））	ユーザ プロファイルなし	キャッシュまたはデータベース ザプロファイル情報を受信でき に発生します。
207	ログインできません（207）（Login is unavailable （207）） ログアウトできません（207）（Logout is unavailable （207））	デバイス名が空白です	デバイス タグまたは名前タグが 内に存在しない場合に発生しま は、実際のデバイスでは発生せ がサードパーティ アプリケーシ 送信された場合にのみ発生する あります。

エラーコード（Error Code）	電話機のディスプレイ	短い説明	理由（Reason）
208	ログインできません（208）（Login is unavailable（208）） ログアウトできません（208）（Logout is unavailable（208））	EM サービス接続エラー	訪問先 EMApp が訪問先 EM 続できません。（サービス いるか、アクティブになって 訪問先 EMService がホーム 接続できません（WAN が るか、証明書が信頼されて
210	ログインできません（210）（Login is unavailable（210）） ログアウトできません（210）（Logout is unavailable（210））	初期化失敗-管理者に確認	EMAppの初期化中にエラー ス接続障害など）が発生し ラーは、起動時にデータベ きなかったことで発生する ます。
211	ログインできません（211）（Login is unavailable（211）） ログアウトできません（211）（Logout is unavailable（211））	EMCCがアクティブになっていない	訪問先クラスタの [クラス プロファイル（Intercluster S Profile）] ウィンドウで、PS ブになっていない場合に発
212	ログインできません（212）（Login is unavailable（212））	クラスタ ID が無効	不正なクラスタ ID をリモー に送信することにより、リ タの更新に失敗した場合に
213	ログインできません（213）（Login is unavailable（213）） ログアウトできません（213）（Logout is unavailable（213））	デバイスは EMCC をサポートしていません	デバイスが EMCC をサポー 場合に発生します。

エラーコード（Error Code）	電話機のディスプレイ	短い説明	理由（Reason）
215	loginType が無効です（215）（loginType invalid (215)）	無効なログイン タイプです。	loginType が無効な場合に発生 使用できる値は次のとおりです • SP（セルフサービス ユー 合） • DN（プライマリ エクステン 場合） • UID（ユーザ ID の場合）
216	DN に複数のユーザが存在します（216）（DN has multiple users（216））	DN に複数のユーザが存在します（DN has multiple users）	EM ログインに使用される内線 数のユーザがプライマリとして られている場合に発生します。

Extension Mobility サービスのエラー コード

表 *44 : Extension Mobility* サービスのエラー コード

エラーコード（Error Code）	電話機のディスプレイ	短い説明	理由（Reason）
0	ログインできません（0）（Login is unavailable（0）） ログアウトできません（0）（Logout is unavailable（0））	未知のエラー（Unknown Error）	理由は不明ですが EMService が失 た。
1	ログインできません（1）（Login is unavailable（1）） ログアウトできません（1）（Logout is unavailable（1））	解析エラー	EMService が EMApp または EMS の XML 要求を解析できない場合。 ラーは、サードパーティ アプリケ がログイン XML（EM API）に間違 リを送信した場合に発生します。 ム クラスタと訪問先クラスタでバ が一致しない場合にも発生する可能 ます。

エラーコード（**Error Code**）	電話機のディスプレイ	短い説明	理由（**Reason**）
2	ログインできません（2）（Login is unavailable（2））	EMCC 認証エラー	ユーザが間違った PIN を入力 EMCC ユーザ ログイン情報を ん。
3	ログインできません（3）（Login is unavailable（3）） ログアウトできません（3）（Logout is unavailable（3））	無効なアプリケーションユーザ（Invalid App User）	無効なアプリケーションユーザ は、主に、EM API が原因で発
4	ログインできません（4）（Login is unavailable（4）） ログアウトできません（4）（Logout is unavailable（4））	ポリシー検証エラー（Policy Validation error）	EM サービスは、不明な理由、 照会中のエラー、キャッシュが 中のエラーにより、ログイン要 アウト要求を検証できなかった エラーを送信します。
5	ログインできません（5）（Login is unavailable（5）） ログアウトできません（5）（Logout is unavailable（5））	デバイスのログオンが無効	ユーザが、**[電話機の設定（Ph Configuration）]** ウィンドウで **Mobility の有効化（Enable Ex Mobility）]** がオフになってい ログインしています。
6	ログインできません（6）（Login is unavailable（6）） ログアウトできません（6）（Logout is unavailable（6））	データベース エラー	EM サービスが要求したクエリ ドプロシージャ（ログイン/ロ はデバイス/ユーザ クエリ）を タベースが例外を返すたびに、 がこのエラー コードを EMApp す。
8	ログインできません（8）（Login is unavailable（8）） ログアウトできません（8）（Logout is unavailable（8））	クエリ タイプ不定（Query type undetermined）	有効なクエリが EMService に送 でした（DeviceUserQuery と Us が有効なクエリです）。この API または間違った XML 入力 します。

エラーコード（Error Code）	電話機のディスプレイ	短い説明	理由（Reason）
9	ログインできません（9）（Login is unavailable（9）） ログアウトできません（9）（Logout is unavailable（9））	Dir. ユーザ情報エラー（User Info Error）	このエラーは、次の2つのケースで す。 1. IMS がユーザを認証しようと 返しました。 2. ユーザに関する情報がキャッ データベースからも取得でき
10	ログインできません（10）（Login is unavailable（10）） ログアウトできません（10）（Logout is unavailable （10））	ユーザにアプリケーション代理権がありません（User lacks app proxy rights）	ユーザが別のユーザの代わりにロ うとしています。 デフォルトでは CCMSysUser は管理権限を持って
11	ログインできません（11）（Login is unavailable（11）） ログアウトできません（11）（Logout is unavailable （11））	デバイスがありません	電話機レコードのエントリがデバ ブルに含まれていません。
12	電話機レコードのエントリがデバイス テーブルに含まれていません。	Dev. プロファイルが見つかりません（Profile not found）	デバイス プロファイルがリモート 関連付けられていません。
18	ログインできません（18）（Login is unavailable（18））	別のユーザがログインしています（Another user logged in）	別のユーザがすでに電話機にログ ます。
19	ログアウトできません（19）（Logout is unavailable （19））	ユーザはログインしていません（No user logged in）	システムが、ログインしていない グアウトしようとしました。この サードパーティ アプリケーション アウト要求を送信中に発生します API）。

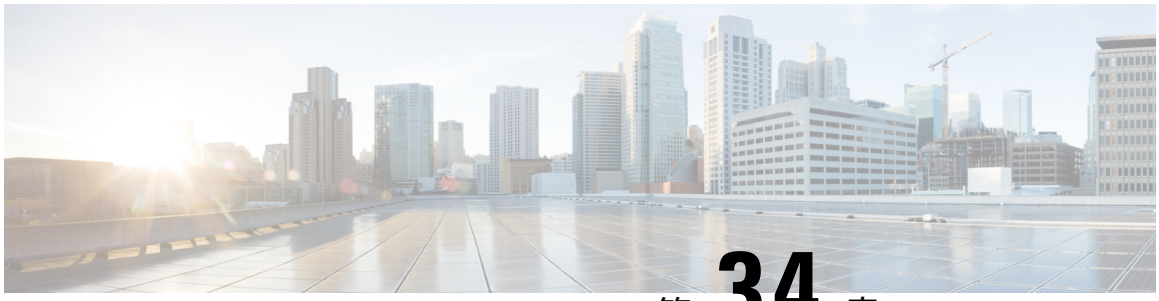
エラーコード（**Error Code**）	電話機のディスプレイ	短い説明	理由（**Reason**）
20	ログインできません（20）（Login is unavailable（20）） ログアウトできません（20）（Logout is unavailable （20））	ホテリング フラグ エラー（Hoteling flag error）	**[電話機の設定（Phone Configu** ンドウで、**[Extension Mobility** **（Enable Extension Mobility）]** ています。
21	ログインできません（21）（Login is unavailable（21）） ログアウトできません（21）（Logout is unavailable（21））	ホテリング ステータス エラー（Hoteling Status error）	現在のユーザ ステータスがロ シュまたはデータベースから取 でした。
22	ログインできません（22）（Login is unavailable（22））	デバイスのログオンが無効	デバイスでEMが有効になって 求がEM API経由で送信された 機で [サービス（Services）] ボ た場合に発生します。
23	ログインできません（23）（Login is unavailable（23）） ログアウトできません（23）（Logout is unavailable （23））	ユーザが存在しません	特定のユーザ ID が見つからな モート クラスタのいずれかで します。
25	マルチログインは許可されていません（25）（Multi-Login Not Allowed（25））	ユーザは既にログイン済み（User logged in elsewhere）	ユーザは現在、ローカル クラ モート クラスタのいずれかの ログインしています。
26	ログインできません（26）（Login is unavailable（26）） ログアウトできません（26）（Logout is unavailable （26））	ビジー。再実行してください（Busy, please try again）	EMService が [同時要求の最大 Concurrent Requests）] サービス のしきい値レベルに到達してい します。

エラーコード（**Error Code**）	電話機のディスプレイ	短い説明	理由（**Reason**）
28	ログインできません（28）（Login is unavailable（28）） ログアウトできません（28）（Logout is unavailable （28））	信頼されない IP エラー（Untrusted IP Error）	[IP アドレスの検証（Validate IP A サービス パラメータが [True] に設 おり、ユーザが、IP アドレスが信 いないマシンでログインまたはロ ようとしたときに発生します。 た サードパーティ アプリケーション からの EM API は、[信頼された Ip （Trusted List of Ips）] サービス パ にリストされません。
29	ログインできません（29）（Login is unavailable（29）） ログアウトできません（29）（Logout is unavailable （29））	RIS がダウンしています。管理者に連絡してください（ris down-contact admin）	Real-Time Information Server Data C （RISDC）キャッシュが作成または れておらず、EMService が RISDC きません。
30	ログインできません（30）（Login is unavailable（30）） ログアウトできません（30）（Logout is unavailable （30））	プロキシは許可されません（Proxy not allowed）	ログインとログアウトがプロキシ経 し（「Via」 が HTTP ヘッダーで記 おり）、[プロキシを許可する（A Proxy）] サービス パラメータが [定されている場合。
31	ログインできません（31）（Login is unavailable（31）） ログアウトできません（31）（Logout is unavailable （31））	ユーザに対して EMCC がアクティブになっていない	ホームクラスタの**[エンドユーザの User Configuration）]** ウィンドウ **タ間の Extension Mobility の有効化 Extension Mobility Cross Cluster**） ボックスがオンになっていない場合 ます。
32	ログインできません（32）（Login is unavailable（32）） ログアウトできません（32）（Logout is unavailable （32））	デバイスは EMCC をサポートしていません	デバイス モデルが EMCC 機能を使 い場合に発生します。

エラーコード（Error Code）	電話機のディスプレイ	短い説明	理由（Reason）
33	ログインできません（33）（Login is unavailable（33）） ログアウトできません（33）（Logout is unavailable （33））	空き EMCC ダミー デバイスなし	すべての EMCC ダミー デバイ EMCC ログインに使用されてい 生します。
35	ログインできません（35）（Login is unavailable（35）） ログアウトできません（35）（Logout is unavailable （35））	訪問先クラスタ情報がホーム クラスタ内に存在しない	ホーム クラスタにこの訪問先 ントリが存在しない場合に発生
36	ログインできません（36）（Login is unavailable（36）） ログアウトできません（36）（Logout is unavailable （36））	リモート クラスタなし	管理者がリモート クラスタを た場合に発生します。
37	ログインできません（37）（Login is unavailable（37）） ログアウトできません（37）（Logout is unavailable （37））	重複するデバイス名	ホーム クラスタと訪問先クラ 同じデバイス名が存在する場合 す。
38	ログインできません（38）（Login is unavailable（38）） ログアウトできません（38）（Logout is unavailable （38））	EMCC が許可されていない	ホーム クラスタで EMCC ログ れていない場合に発生します スタで [クラスタ間の Extension 効化（Enable Extension Mobility Cluster）] チェックボックスが いません）。

エラーコード（**Error Code**）	電話機のディスプレイ	短い説明	理由（**Reason**）
39	再度ログインしてください（201）（Please try to login again （201））	設定の問題	[EMCC 機能設定（EMCC Feature Configuration）] ページで EMCC ロバイスの [デフォルト TFTP サーバ TFTP Server）] および [バックアッサーバ（Backup TFTP Server）] が定されていない場合に発生します （注） これは内部エラーコー
40	再度ログインしてください（23）（Please try to login again （202））	リモートホストからの応答がありません	リモート ホストからの応答がない生します。 （注） これは内部エラーコー
41	PIN 変更が必要です（PIN change is required）	PIN 変更が必要です（PIN change is required）	管理者が PIN に対して [次回ログ更必要（User Must Change at Next L有効にした場合に発生します。 こユーザは [ログイン情報の変更（C credentials）] ページにリダイレクす。 （注） これは内部エラーコー
42	ログインできません（42）（Login is unavailable （42）） ログアウトできません（42）（Logout is unavailable （42））	無効なクラスタ ID	リモート クラスタ ID が有効でない生します。 このエラーは、リモータの更新中に発生する可能性があ
43	ログインできません（43）（Login is unavailable （43））	デバイス セキュリティ モード エラー	EMCCデバイスに関連付けるデバリティプロファイルは、そのデバリティ モードを非セキュアに設定があります。
44	再度ログインしてください（201）（Please try to login again （201））	設定の問題	クラスタ ID が有効でない場合に発す。 （注） これは内部エラーコー
45	ログインに失敗しました（45）（Login is unsuccessful （45））	リモート クラスタ バージョンがサポートされていない	訪問先クラスタのバージョンが 9.モードになっており、電話機がセドで、ホーム クラスタのバージョ場合の EMCC ログイン中に発生し

エラーコード（**Error Code**）	電話機のディスプレイ	短い説明	理由（**Reason**）
46	ログインに失敗しました（46）（Login is unsuccessful （46））	リモート クラスタ セキュリティ モードがサポートされていない	訪問先クラスタのセキュリテ 合モードになっており、電話機 モードで、ホーム クラスタが非 ドになっている場合の EMCC 発生します。
47	DN に複数のユーザが存在します（47）（DN has multiple users（47））	DN に複数のユーザが存在します（DN has multiple users）	ログインに使用される内線番号 ザがプライマリとして関連付け と、EMCC へのログイン時に 発生します。



第 34 章

クラスタ間のエクステンションモビリティローミング

（注） クラスタ間のエクステンションモビリティ ローミングを展開するには、Cisco Unified Communications Manager リリース 12.0(1)SU1 以上を実行している必要があります。

クラスタ間のエクステンションモビリティ ローミングの概要

クラスタ間のエクステンションモビリティ ローミングでは、ユーザが複数のクラスタ間をローミングし、ユーザのホーム クラスタがダウンしている場合でもコールを発信または受信できます。 この機能は、クラスタ間検索サービス（ILS）を使用してすべてのクラスタで Extension Mobility ユーザの電話番号を複製します。

ユーザがローミング クラスタにログインすると、電話番号を使用して電話機がローミング クラスタに登録されます。 訪問先クラスタからホーム クラスタに電話機が登録されるクラスタ間のエクステンションモビリティ（EMCC）とは異なり、このローミング機能の場合、ユーザは訪問先クラスタに関係なく自分の登録を維持できます。

構成の概要

この機能を展開するには、次の操作を行う必要があります。

- ILS ネットワークのセットアップ：ILS は、クラスタ間での電話番号の同期に使用されます。

  ILS の設定の詳細については、Cisco Unified Communications Manager システム設定ガイドの「クラスタ間検索サービスの設定」の章を参照してください。

- 均一のダイヤルプランのセットアップ：ILS ネットワーク上で均一のダイヤルプランが必要です。

  ダイヤルプランをセットアップするには、Cisco Unified Communications Manager システム設定ガイド の「ダイヤルプランの設定」の章を参照してください。

- デバイス プロファイルとユーザ情報は、すべてのクラスタで同期する必要があります。
- エクステンション モビリティを設定します。
- エクステンション モビリティ ユーザのローミング アクセスを設定します。

クラスタ間のエクステンションモビリティ ローミング用のシステム要件

Cisco Unified Communications Manager のシステム要件は次のとおりです。

- Cisco Unified Communications Manager リリース 12.0(1)SU1 以上
- Cisco Extension Mobility サービスが実行されている必要があります。
- クラスタ間検索サービスが実行されている必要があります。

クラスタ間のエクステンションモビリティ ローミングのログイン

ログインに関する用語

次の図は、クラスタ間のエクステンション モビリティ ローミングでのホームクラスタとローミングクラスタを示しています。

図 7: ホーム クラスタとローミング クラスタ

Home Cluster

ホーム クラスタとは、ユーザ デバイス プロファイル、ダイヤル プランなどのユーザ設定が保管されているクラスタです。

ローミング クラスタ

ローミング クラスタとは、ユーザ自身のホーム クラスタの場合と同様に、Extension Mobility に対応する電話機へのエクステンションモビリティ ログインを実行できるクラスタです。

スーパーユーザ

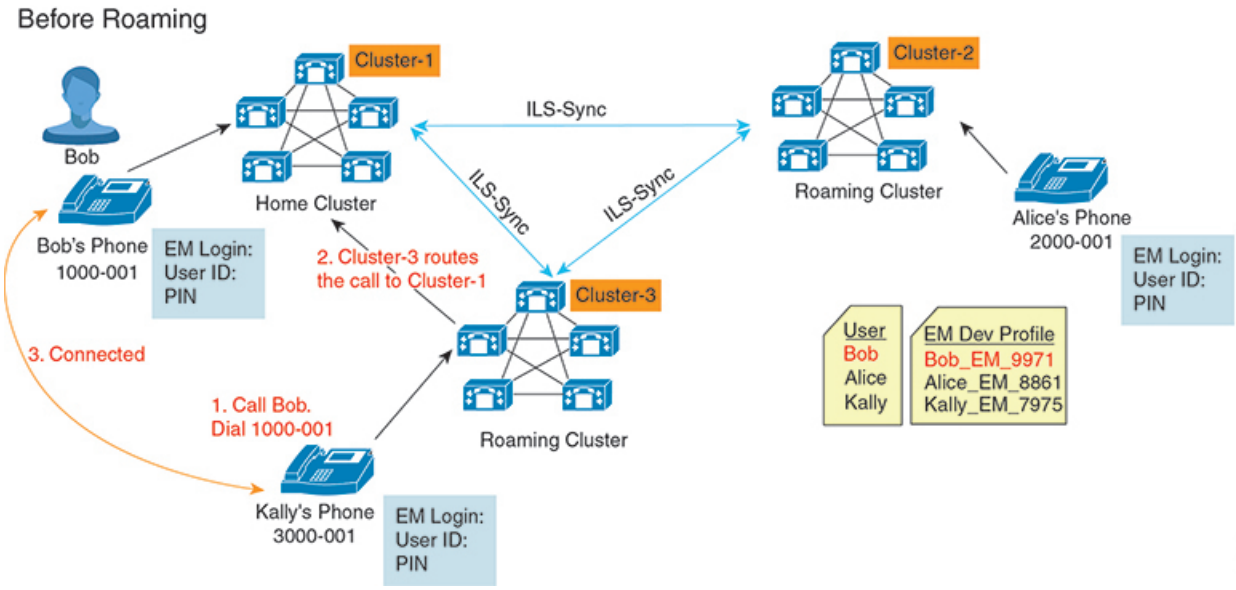
スーパーユーザとは、[クラスタ間標準 EM ローミング スーパーユーザ（Standard EM Roaming Across Clusters Super Users）] アクセス コントロール グループに関連付けられているユーザです。 このユーザには、ローミング クラスタから Extension Mobility ログインを実行する権限があり、コールを発信/受信できます。

（注） スーパーユーザー情報は、ユーザーがログインしているクラスタに関係なく、すべてのクラスタで共有される必要があります。

ログイン プロセス

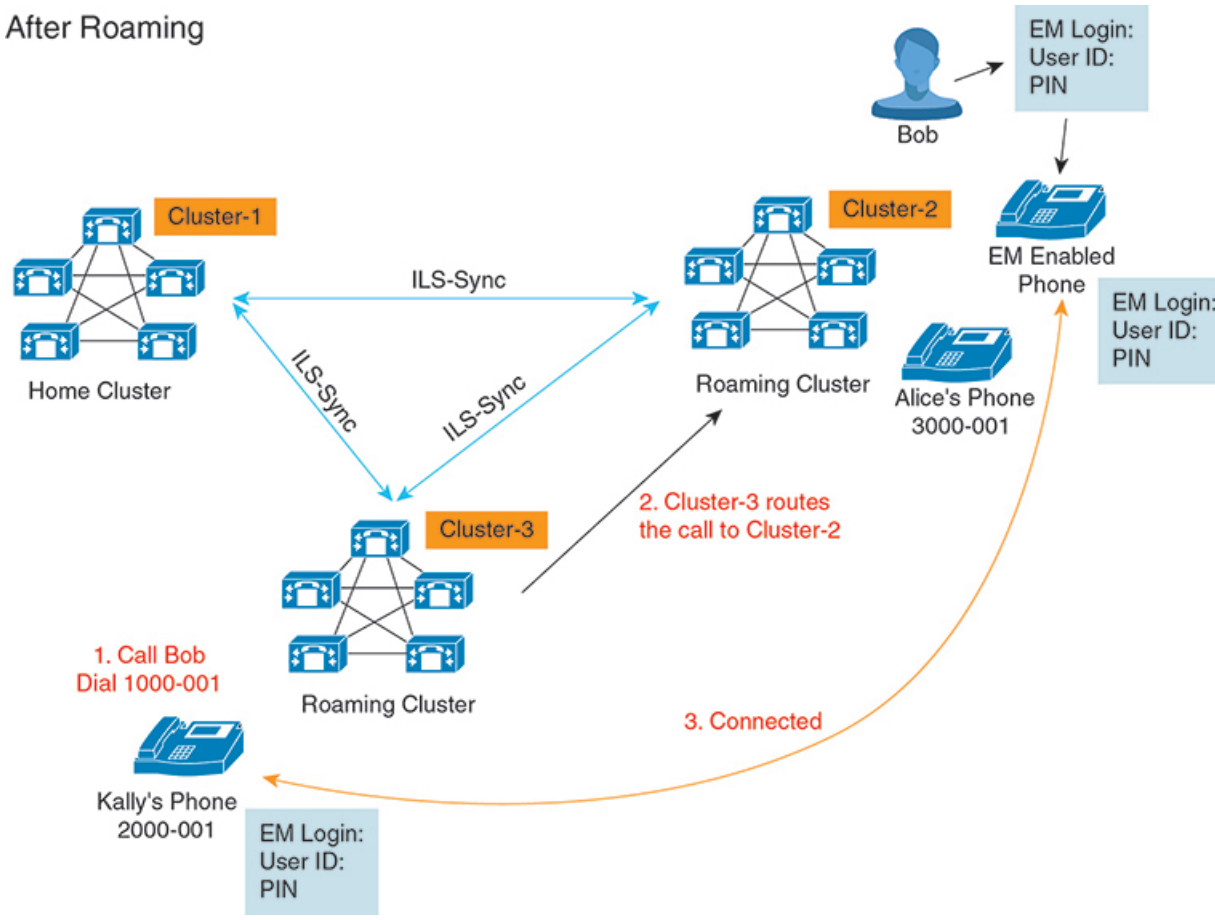
Cisco Unified Communications Manager では、複数クラスタ間で作成されたスーパーユーザの Extension Mobility ログインがサポートされています。 Extension Mobility ログインにより、スーパーユーザはローミング クラスタで各自の電話機設定（ライン アピアランス、サービス、ダイヤル プランなど）にアクセスできます。 スーパーユーザは、ホームクラスタの場合と同様にローミング クラスタからコールを発信または受信できます。

図 *8*: ユーザがホーム クラスタにいる場合のコール フロー



上記の図では、Bob の DN が1000-001 でクラスタ 1 に登録されており、Alice の DN が 2000-001 でクラスタ 2 に登録されており、Kally の DN が 3000-001 でクラスタ 3 に登録されているものとします。 Kally が Bob の DN 1000-001 をダイヤルすると、クラスタ 3 からクラスタ 1 にコールがルーティングされ、Bob と Kally が接続されます。

図 *9*: ユーザがローミング クラスタにいる場合のコール フロー



Bob のホーム クラスタがダウンし、Bob はクラスタ間をローミングできるスーパーユーザとして設定されているとします。 Bob がクラスタ 2 に移動して Extension Mobility ログインを実行すると、ホストの電話機が Bob の設定を使用して再登録されます。 ログインが成功すると、その他のすべてのクラスタが更新され、Bob の新しいロケーションが反映されます。 これで、Kally が Bob の DN 1000-01 をダイヤルすると、クラスタ 3 からクラスタ 2 にコールがルーティングされ、Bob と Kally が接続されます。 同様に、Bob が Kally を呼び出すには DN 3000-001 をダイヤルします。

（注）

- スーパーユーザは、別のクラスタへの Extension Mobility ログインを実行すると、ホーム クラスタから自動的にログアウトします。 クラスタがダウンしている場合、そのクラスタが稼働するまで待って、ユーザの以前のログインからログアウトします。
- クラスタ間のエクステンションモビリティ ローミングではマルチログイン動作がサポートされています。 したがって、スーパーユーザは同じクラスタ内の複数デバイスからログインできますが、クラスタをまたぐことはできません。

ILS の連携動作

Cisco Unified CM の管理では、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 ネットワークが確立したら、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。

Extension Mobility のログインまたはログアウトが行われるたびに、ILS 同期により、使用可能な情報が他のクラスタで更新され始めます。

（注） ユーザをスーパーユーザとして設定すると、ILS の電話番号の設定に関係なく、ILS 同期が自動的に開始されます。

詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）の「Configure Intercluster Lookup Service」の章を参照してください。

クラスタ間のエクステンションモビリティ ローミングのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	電話機能一覧の生成 （5 ページ）	Extension Mobility 機能をサポートするデバイスを特定するためのレポートを生成します。
ステップ 2	Extension Mobility を設定するには、次のサブタスクを示されている順に実行します。 • エクステンションモビリティ サービスの有効化 （503 ページ） • Cisco Extension Mobility 電話サービスの設定 （503 ページ） • ユーザのエクステンションモビリティ デバイス プロファイルの作成 （505 ページ） • ユーザへのデバイス プロファイルの関連付け （505 ページ）	ユーザがリモート クラスタからログインするときに他の電話機から自分の電話機の設定（ライン アピアランス、サービス、短縮ダイヤルなど）に一時的にアクセスできるように、Extension Mobility を設定します。 ユーザがホーム クラスタとリモート クラスタのどちらからでも設定にアクセスできるように、ホーム クラスタとリモート クラスタの両方でこのタスク フローを実行します。

	コマンドまたはアクション	目的
	• エクステンションモビリティへの登録 （506 ページ）	
ステップ 3	Extension Mobility ユーザのローミングの設定 （579 ページ）	Extension Mobility ユーザが、同一ログイン クレデンシャルを使用して ILS ネットワーク内の異なるクラスタ間をローミングするには、次の手順を使用します。

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。

エクステンションモビリティ サービスの有効化

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[ツール（Tools）] > [サービス アクティベーション（Service Activation）]** を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストから、必須のノードを選択します。

ステップ 3 、次のサービスを有効化します。

a) Cisco CallManager
b) Cisco Tftp

c) Cisco Extension Mobility
d) ILS サービス

（注） ILS サービスをアクティブ化するには、パブリッシャ ノードを選択する必要があります。

ステップ 4 **[保存（Save）]** をクリックします。
ステップ 5 **OK**をクリックします。

Cisco Extension Mobility 電話サービスの設定

ユーザが後でExtension Mobilityにアクセスするために登録できる、Extension Mobility IP 電話サービスを設定します。

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。**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[電話サービス（Phone Services）]**。
ステップ 2 [新規追加] をクリックします。
ステップ 3 [サービス名（Service Name）] フィールドに、サービスの名前を入力します。
ステップ 4 [**サービス URL（Service URL）**] フィールドにサービス URL を入力します。

形式は `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#` です。 `IP アドレス` は、Cisco Extension Mobility が有効化され、実行している Unified Communications Manager の IP アドレスです。

IPv4 アドレスである必要があります。

例：

`http://123.45.67.89:8080/emapp/EMAppServlet?device=#DEVICENAME#`

例：

`http://[2001:0001:0001:0067:0000:0000:0000:0134]:8080/emapp/EMAppServlet?device=#DEVICENAME#`

この形式により、ユーザはユーザ ID と PIN を使用してログインすることができます。 Extension Mobility サービスに登録した IP Phone ユーザのサインイン オプションをさらに多く設定できます。 さらに多くのサインイン オプションを設定するには、`loginType` パラメータを以下の形式でサービス URL に追加します。

- `loginType=DN` により、ユーザはプライマリ内線番号と PIN を使用してログインできます。

  サービス URL の形式は、`http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=DN` です。

- `loginType=SP` により、ユーザはセルフ サービス ユーザ ID と PIN を使用してログインできます。

  サービス URL の形式は、`http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=SP` です。

- `loginType=UID` により、ユーザはユーザ ID と PIN を使用してログインできます。

  サービス URL の形式は、`http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=UID` です。

URL の最後に `loginType` を付加しなかった場合は、デフォルトのサインイン オプションとして [ユーザ ID（User ID）] と [PIN] が表示されます。

ステップ 5 [サービス タイプ（Service Type）] フィールドで、サービスが [サービス（Services）]、[ディレクトリ（Directories）]、または [メッセージ（Messages）] ボタンにプロビジョニングされるかどうかを選択します。

ステップ 6 **[保存（Save）]** をクリックします。

ユーザのエクステンションモビリティ デバイス プロファイルの作成

Extension Mobility デバイス プロファイルを設定します。このプロファイルは、ユーザが Extension Mobility にログインするときに物理デバイスにマッピングするバーチャル デバイスとして機能します。 この物理デバイスは、このプロファイルの特性を引き継ぎます。

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）]** > **[デバイス設定（Device Settings）]** > **[デバイス プロファイル（Device Profile）]**。

ステップ 2 次のいずれかの作業を実行します。

- [検索（Find）]をクリックして設定を変更し、結果一覧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、[新規追加（Add New）]をクリックして、[デバイス プロファイルのタイプ（Device Profile Type）] からオプションを選択します。[次へ（Next）]をクリックします。
- [デバイス プロトコル（Device Protocol）]ドロップダウン リストからデバイス 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 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、オンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

ステップ 5 [割り当て情報（Association Information）]領域で、[新規 DN を追加（Add a New DN）]をクリックします。

ステップ 6 [電話番号（Directory Number）]フィールドに電話番号を入力して、[保存（Save）]をクリックします。

ステップ 7 [リセット（Reset）]をクリックし、プロンプトに従います。

ユーザへのデバイス プロファイルの関連付け

ユーザが別の電話機から設定にアクセスできるように、デバイスプロファイルをユーザに関連付けます。 物理デバイスを関連付けるのと同じ方法で、ユーザにユーザ デバイス プロファイルを関連付けます。

ヒント 一括管理ツール（BAT）を使用して、Cisco Extension Mobility の複数のユーザ デバイス プロファイルを一度に追加および削除できます。 Cisco Unified Communications Manager 一括管理ガイドを参照してください。

手順

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 次のいずれかの作業を実行します。

- 既存のユーザ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ユーザを選択します。
- **[新規追加（Add New）]** をクリックして、新しいユーザを追加します。

ステップ 3 **[Extension Mobility]** で、作成したデバイス プロファイルを探して、それを **[使用可能なプロファイル（Available Profiles）]** から **[制御するプロファイル（Controlled Profiles）]** に移動します。

ステップ 4 **[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 **[保存（Save）]** をクリックします。

エクステンションモビリティへの登録

Extension Mobility サービスに IP 電話とデバイス プロファイルを登録して、ユーザがExtension Mobilityにログインし、使用し、ログアウトできるようにします。

手順

ステップ 1 Cisco Unified CM Administration で次のいずれかのタスクを実行します。

- **[デバイス（Device）]>[電話（Phone）]** を選択し、検索条件を指定してから [検索（Find）] をクリックし、Extension Mobilityに使用する電話機を選択します。
- **[デバイス（Device）]>[デバイス設定（Device Settings）]>[デバイス プロファイル（Device Profile）]** を選択し、検索条件を指定してから [検索（Find）]をクリックし、作成したデバイス プロファイルを選択します。

ステップ 2 [関連リンク（Related Links）] ドロップダウン リストから、[サービスの登録/登録解除（Subscribe/Unsubscribe Services）]を選択し、[移動（Go）]をクリックします。

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

ステップ 4 [次へ（Next）]をクリックします。

ステップ 5 [登録（Subscribe）]をクリックします。

ステップ 6 [保存（Save）]をクリックし、ポップアップ ウィンドウを閉じます。

Extension Mobility ユーザのローミングの設定

Extension Mobility ユーザが、同一ログイン クレデンシャルを使用して ILS ネットワーク内の異なるクラスタ間をローミングするには、次の手順を使用します。 これを行うには、選択したユーザを [クラスタ間標準 EM ローミング スーパーユーザ（Standard EM Roaming Across Clusters Super Users）] アクセス コントロール グループに割り当てる必要があります。

始める前に

ILS を使用してクラスタ間でユーザとログインの情報が複製されるので、ILS ネットワークが設定済みである必要があります。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アクセス コントロールグループ（Access Control Group）]** を選択します。

ステップ 2 [検索（Find）] をクリックし、[クラスタ間標準 EM ローミング スーパーユーザ（Standard EM Roaming Across Clusters Super Users）] 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）]** ボタンをクリックします。 [ユーザの検索と一覧表示（Find and List Users）]ポップアップ ウィンドウが表示されます。

ステップ 4 [検索（Find）] をクリックし、ローミング機能を提供するすべての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。

クラスタ間のエクステンションモビリティ ローミングの連携動作と制約事項

クラスタ間のエクステンションモビリティ ローミングの連携動作

ここでは、クラスタ間のエクステンションモビリティ ローミングとその他の Cisco Unified Communications Manager 管理コンポーネントの連携動作について説明します。

- エクステンションモビリティ
- クラスタ間検索サービス（ILS）

クラスタ間のエクステンションモビリティ ローミングの制約事項

ここでは、クラスタ間のエクステンションモビリティ ローミングとその他の Cisco Unified Communications Manager 管理コンポーネントの制約事項について説明します。

- ハブ ILS がダウンしている場合、このハブ ILS に接続しているスポークは、ハブが復旧するまで同期されません。

さまざまなタイプの Extension Mobility

次の表に、Cisco Unified Communications Manager で使用可能な各種 Extension Mobility 機能と、それぞれの機能の違いを説明します。

表 *45 : EM*、*EMCC*、およびクラスタ間のエクステンションモビリティ ローミングの相違点

	エクステンションモビリティ（EM）	クラスタ間のエクステンションモビリティ（EMCC）	クラスタ間のエクステンションモビリティ ローミング
説明	ユーザが同じクラスタ内の他の電話機から各自の電話設定に一時的にアクセスできるようにします。	ユーザが別のクラスタ内の電話機から各自の電話設定にアクセスできるようにします。	ユーザが各自のログイン クレデンシャルを使用してクラスタ間でローミングできるようにします。

	エクステンションモビリティ（EM）	クラスタ間のエクステンションモビリティ（EMCC）	クラスタ間のエクステンションモビリティ ローミング
ユーザが別のクラスタで電話機にログインする場合	該当なし	リモートクラスタの電話機はユーザのホームクラスタに登録され、ホームクラスタの設定にアクセスします。	ローミングクラスタの電話機は、ローミングクラスタだけに登録されます。
クラスタ間	単一クラスタのみ	マルチクラスタ	マルチクラスタ
設定	単一クラスタのみ	ホーム クラスタと、ユーザが訪問する各クラスタで EMCC が設定される必要があります。	すべてのクラスタでエクス テンション モビリティ ローミングが設定される必要があります。
ユーザ情報	単一クラスタのみ	すべてのクラスタで保持する必要があります。	すべてのクラスタで保持されるスーパーユーザ情報。

クラスタ間のエクステンションモビリティ ローミングのトラブルシューティング

ここでは、EMApp と EMService のエラー コードについて説明します。

認証エラー

問題 「エラー 201 認証エラー（Error 201 Authentication Error）」が電話機に表示されます。

解決法 正しいユーザ ID と PIN が入力されていることを確認する必要があります。また、ユーザ ID と PIN が正しいことをシステム管理者と一緒に確認する必要があります。

ユーザ ID または PIN が空です

問題 「エラー 202 ユーザ ID または PIN が空です（Error 202 Blank User ID or PIN）」が電話機に表示されます。

解決法 有効なユーザ ID と PIN を入力してください。

ビジー。再実行してください

問題 「エラー 26 ビジー。再実行してください（Error 26 Busy Please Try Again）」が電話機に表示されます。

解決法 同時ログイン/ログアウト要求の数が [同時要求の最大数（Maximum Concurrent requests）] サービス パラメータより多いかどうかを確認します。 大きい場合は同時要求の数を小さくします。

（注） 同時ログイン/ログアウト要求の数を確認するには、Cisco Unified Real-Time Monitoring Tool を使用して Extension Mobility オブジェクト内の Requests In Progress カウンタを表示します。 詳細については、以下で『Cisco Unified Real-Time Monitoring Tool Administration Guide』を参照してください。http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

データベース エラー

問題 「エラー 6 データベース エラー」が電話機に表示されます。

解決法 大量の要求が存在するどうかを確認してください。 大量の要求が存在する場合は、Extension Mobility オブジェクト カウンタの Requests In Progress カウンタに高い値が表示されます。 大量の同時要求が原因で要求が拒否された場合は、Requests Throttled カウンタにも高い値が表示されます。 詳細なデータベース ログを収集します。

デバイスのログオンが無効

問題 「エラー 22 デバイスのログオンが無効（Error 22 Dev Logon Disabled）」が電話機に表示されます。

解決法 **[電話の設定（Phone Configuration）]** ウィンドウ（**[デバイス（Device）]** > **[電話機（Phone）]**）で、**[エクステンションモビリティの有効化（Enable Extension Mobility）]** チェックボックスがオンになっていることを確認してください。

デバイス名が空白です

問題 「エラー 207 デバイス名が空白です（Error 207 Device Name Empty）」が電話に表示されます。

解決法 Cisco Extension Mobility に設定されている URL が正しいことを確認してください。 詳細については、「関連項目」を参照してください。

関連トピック

Cisco Extension Mobility 電話サービスの設定 （503 ページ）

EM サービス接続エラー

問題 「エラー 207 EM サービス接続エラー（Error 207 EM Service Connection Error）」が電話機に表示されます。

解決法 Cisco Unified Serviceability で、**[ツール（Tools）]** > **[コントロール センター - 機能（Control Center—Feature）]** を選択することにより、Cisco Extension Mobility サービスが実行されていることを確認してください。

ホストを検出できません

問題 「ホストを検出できません（Host Not Found）」というエラー メッセージが電話機に表示されます。

解決法 Cisco Unified Serviceability で、**[ツール（Tools）]** > **[コントロール センターのネットワーク サービス（Control Center—Network Services）]** を選択することにより、Cisco Tomcat サービスが実行していることを確認してください。

HTTP エラー

問題 HTTP エラー（503）が電話機に表示されます。

解決法

- **[サービス（Services）]** ボタンを押したときにこのエラーが表示された場合は、Cisco Unified Serviceability で、**[ツール（Tools）]** > **[コントロール センターのネットワーク サービス（Control Center—Network Services）]** を選択することにより、Cisco IP 電話サービスが実行していることを確認してください。
- Extension Mobility サービスを選択したときにこのエラーが表示された場合は、Cisco Unified Serviceability で、**[ツール（Tools）]** > **[コントロール センターのネットワーク サービス（Control Center—Network Services）]** を選択することにより、Cisco Extension Mobility Application サービスが実行していることを確認してください。

電話機のリセット

問題 ユーザのログインまたはログアウト後、再起動する代わりに電話機がリセットされます。

考えられる原因 このリセットは、ロケールの変更が原因だと考えられます。

解決法 特に対処の必要はありません。 ログインするユーザまたはプロファイルに関連付けられているユーザ ロケールがロケールまたはデバイスと異なる場合、ログインが正常に完了すると、電話機は再起動し、次にリセットします。 このパターンは、電話機設定ファイルが再作成されるために発生します。

ログイン後に電話サービスが使用できない

問題 ログイン後、電話サービスが使用できません。

考えられる原因 この問題は、電話機にユーザ プロファイルがロードされたときに、ユーザ プロファイルに関連付けられたサービスがないために発生します。

解決法

- ユーザ プロファイルに Cisco Extension Mobility サービスが含まれていることを確認します。
- Cisco Extension Mobility が含まれるように、ユーザがログインする電話機の設定を変更します。 電話機が更新されたあと、ユーザは電話サービスにアクセスできるようになります。

ログアウト後に電話サービスが使用できない

問題 ユーザがログアウトし、電話機がデフォルト デバイス プロファイルに戻った後、電話サービスが使用できなくなります。

解決法

- **[自動デバイス プロファイルと電話の設定間の同期（Synchronization Between Auto Device Profile and Phone Configuration）]** エンタープライズ パラメータが **[はい（True）]** に設定されていることを確認します。
- 電話機を Cisco Extension Mobility サービスに登録します。

ユーザは既にログイン済み

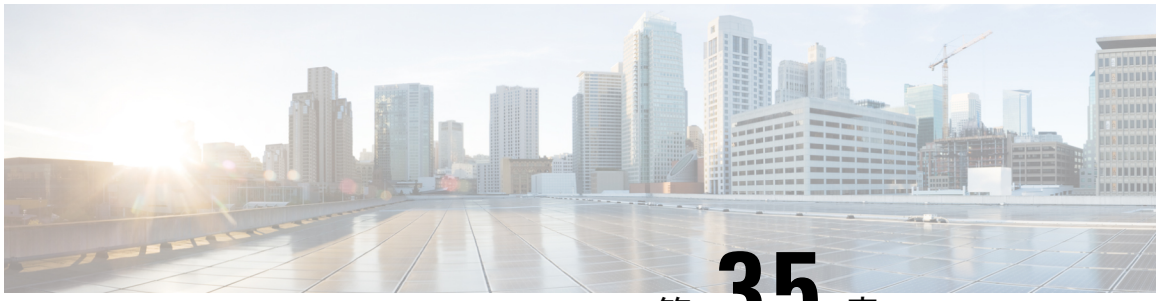
問題 「エラー 25 ユーザは既にログイン済み（Error 25 User Logged in Elsewhere）」が電話機に表示されます。

解決法 ユーザが別の電話機にログインしているかどうかを確認します。 複数のログインを許可する必要がある場合は、[複数のログイン動作（Multiple Login Behavior）] サービス パラメータが [複数のログインを許可（Multiple Logins Allowed）] に設定されていることを確認します。

ユーザ プロファイルなし

問題 「エラー 205 ユーザ プロファイルなし（Error 205 User Profile Absent）」が電話機に表示されます。

解決法 デバイス プロファイルをユーザに関連付けます。



第 35 章

保留復帰

保留復帰の概要

コールを保留にすると、保留されたコールが設定された時間制限を超えたときに、保留復帰機能がアラートを発行します。設定された時間制限が期限切れになると、電話機でアラートが生成され、コールを処理するように通知されます。

以下のアラートを使用できます。

- 一度だけ電話機の呼出音が鳴る、または、ビープ音が鳴る
- ステータス行に「保留復帰（Hold Reversion）」と表示される
- 回線ボタンの横にある LED が連続的に点滅する
- 振動するハンドセット アイコンが表示される

（注） 受信されるアラートのタイプは、電話機の機能によって異なります。

復帰されたコールを取得するには、次の操作を実行できます。

- ハンドセットを取り上げる
- 電話機のスピーカー ボタンを押す
- ヘッドセット ボタンを押す
- 復帰されたコールに関連付けられた回線を選択する
- [復帰（Resume）] ソフトキーを押す

詳細については、特定の電話機モデルのユーザ ガイドを参照してください。

保留復帰の前提条件

- Cisco CallManager サービスを、クラスタの少なくとも 1 つのノードで実行しておく必要があります
- Cisco CTIManager サービスを、クラスタの少なくとも 1 つのノードで実行しておく必要があります
- Cisco Database Layer Monitor サービスを、Cisco CallManager サービスと同じノードで実行しておく必要があります
- Cisco RIS Data Collector サービスを、Cisco CallManager サービスと同じノードで実行しておく必要があります
- Cisco Tftp サービスを、クラスタの少なくとも 1 つのノードで実行しておく必要があります
- 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、Cisco Unified Communications Manager のロケール インストーラをインストールしておく必要があります

保留復帰の設定タスク フロー

電話機の保留復帰を設定するには、次の手順を実行します。 この手順は、電話機に電話番号を設定していること、または自動登録を使用していることを前提としています。

始める前に

- 電話機ユーザに英語以外の言語で保留復帰メッセージを表示する場合、または国に固有のトーンがユーザに聞こえるようにする場合は、ロケールインストーラがインストールされていることを確認します。
- 保留復帰の前提条件 （586 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	電話機能一覧の生成 （5 ページ）	保留復帰機能をサポートする電話機を特定するには、電話機能リスト レポートを実行します。
ステップ 2	保留復帰時のコール フォーカス優先度の設定 （587 ページ）	電話機のデバイスプールに対して、コールのフォーカス優先順位を設定します。
ステップ 3	次のいずれかの手順を実行します。 • クラスタの保留復帰タイマーのデフォルトの設定 （588 ページ）	保留復帰タイマーを設定します。 クラスタ全体のサービス パラメータを使用してタイマを設定するか、個々の電話回線で設定できます。

	コマンドまたはアクション	目的
	• 電話の保留復帰タイマーの設定（588 ページ）	（注） 個々の電話回線での設定は、クラスタ全体のサービスパラメータの設定より優先されます。

保留復帰時のコール フォーカス優先度の設定

管理者は、着信コールと復帰コールに優先度順位をつけることができます。デフォルトでは、すべての着信コールが復帰コールより優先的に取り扱われるようになっていますが、コールフォーカス優先度を設定すると復帰コールの優先度を上げられます。

始める前に

電話機能一覧の生成 （5 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、**[システム（System）]** > **[デバイス プール（Device Pool）]** を選択し、電話に適用するデバイス プールを開きます。

ステップ 2 [復帰コール フォーカス優先度（Reverted Call Focus Priority）]フィールドで、次のいずれかのオプションを選択し、[保存（Save）]をクリックします。

- デフォルト—着信コールの方が復帰コールよりも優先度が高い
- 最高—復帰コールの方が釈伸コールよりも優先度が高い

ステップ 3 **[保存]** をクリックします。

ステップ 4 デバイス プールのデバイスをリセットするには、次の手順を実行します。

a) **[リセット（Reset）]** をクリックします。 **[デバイス リセット（Device Reset）]** ウィンドウが表示されます。

b) **[デバイス リセット（Device Reset）]** ウィンドウで **[リセット（Reset）]** をクリックします。

次のタスク

保留復帰タイマー設定を設定するには、次の手順のいずれかを実行します。

- クラスタの保留復帰タイマーのデフォルトの設定 （588 ページ）
- 電話の保留復帰タイマーの設定 （588 ページ）

クラスタの保留復帰タイマーのデフォルトの設定

クラスタ内のすべての電話機に、保留復帰タイマーのデフォルト設定を適用するクラスタ全体のサービス パラメータを設定するには、次の手順を実行します。

（注） クラスタ全体のサービスパラメータを設定すると、その設定はクラスタ内のすべての電話機の保留復帰タイマーのデフォルト設定として適用されます。 ただし、個々の電話回線の設定は、クラスタ全体のデフォルトをオーバーライドできます。

始める前に

保留復帰時のコール フォーカス優先度の設定 （587 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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

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 次のクラスタ全体のサービス パラメータの値を設定します。

- [保留復帰時間（Hold Reversion Duration）]：Cisco Unified Communications Manager が保留中の電話機に保留復帰アラートを送信するまでの待機時間を 0 ～ 1200 秒（これを含む）で指定します。 0 を入力すると、Cisco Unified Communications Manager は、電話回線で設定されていない限り、保留復帰アラートを送信しません。
- [保留復帰通知間隔（Hold Reversion Interval Notification）]：Cisco Unified Communications Manager が保留中の電話機に保留復帰アラートのリマインダを定期的に送信するまでの待機時間を 0 ～ 1200 秒（これを含む）で指定します。 0 を入力すると、Cisco Unified Communications Manager は、タイマーが電話回線で設定されていない限り、保留復帰アラートのリマインダを定期的に送信しません。

ステップ 5 **[保存（Save）]** をクリックします。

電話の保留復帰タイマーの設定

電話および電話回線の保留復帰タイマーを設定するには、次の手順を実行します。

（注） クラスタ全体のサービスパラメータを使用しても保留復帰タイマーを設定できます。ただし、個々の電話回線の設定は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。

始める前に

保留復帰のクラスタ全体のデフォルトを設定するには、クラスタの保留復帰タイマーのデフォルトの設定 （588 ページ）を実行します。

手順

ステップ 1 Cisco Unified CM の管理で、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 **[検索（Find）]** をクリックして、保留復帰を設定する電話を選択します。

ステップ 3 左側の **[関連付け（Association）]** ペインで、保留復帰を設定する電話回線をクリックします。

ステップ 4 以下のフィールドに値を設定します。

- [保留復帰の呼び出しの時間（Hold Reversion Ring Duration）]：Cisco Unified Communications Manager が復帰コールのアラートを通知するまでの待機時間を秒単位で指定するには、0 ～ 1200 の数値（包括的）を入力します。 0 を入力すると、Cisco Unified Communications Manager はこの DN に復帰コールのアラートを通知しません。 フィールドを空（デフォルト設定）にすると、Cisco Unified Communications Manager が保留復帰時間のサービス パラメータの設定を適用します。
- [保留復帰の呼び出し間隔通知（Hold Reversion Ring Interval Notification）]：Cisco Unified Communications Manager が定期的リマインダのアラートを送信するまでの待機時間を秒単位で指定するには、0 ～ 1200 の数値（包括的）を入力します。 0 を入力すると、Cisco Unified Communications Manager はこの DN に定期的リマインダのアラートを送信しません。 フィールドを空（デフォルト設定）にすると、Cisco Unified Communications Manager が保留復帰間隔通知のサービス パラメータの設定を適用します。

ステップ 5 **[保存]** をクリックします。

ステップ 6 次の手順を実行して電話をリセットします。

a) **[リセット（Reset）]** をクリックします。 **[リセット デバイス（Reset Device）]** ウィンドウが表示されます。

b) **[リセット（Reset）]** をクリックします。

保留復帰の連携動作

表 *46 :* 保留復帰機能の連携動作

機能	連携動作
保留音	MOH が通常の保留コール用に設定されている場合は、復帰したコールに対して MOH がサポートされます。
コール パーク	保留復帰が呼び出され保留された通話相手が [パーク（Park）] ソフトキーを押した場合、保留した側は依然として保留復帰アラートを受信しコールを取得できます。 保留した側がコールを取得すると、設定されていれば、MOH が流れます。 保留された通話相手が、設定された時間制限を保留期間が超える前にパークした場合、コールがピックアップまたはリダイレクトされるまでシステムはすべての保留復帰アラートを抑制します。
MLPP	マルチレベルの優先およびプリエンプションコールが保留されてから復帰した場合、MLPP コールはそのプリエンプション ステータスを失い、復帰したコールはルーチン コールとして処理されます。 コールが復帰した後、システムはプリエンプション呼出音を再生しません。 高優先コールが復帰対象コールになった場合、システムは優先トーンを再生しません。
CTI アプリケーション	CTI アプリケーションは、保留復帰機能が回線またはシステムに対して有効になっている場合に、保留復帰機能にアクセスできます。 Cisco Unified Communications Manager Assistant やアテンダント コンソールなどの Cisco 提供のアプリケーションは、CTI インターフェイスを使用した保留復帰機能を備えています。 保留復帰が呼び出されると、CTI ポートは、Cisco Unified IP 電話 で再生される可聴音ではなく、イベント通知を受信します。 CTI ポートとルート ポイントはイベント通知を一度しか受信しませんが、Cisco Unified IP 電話 は一定の間隔でアラートを受信します。 保留復帰に伴う CTI 要件と連携動作に関する情報については、以下の API ドキュメントを参照してください。 • 『*Cisco Unified Communications JTAPI Developer Guide*』 • 『*Cisco Unified Communications TAPI Developer Guide*』
SIP 電話と通話している SCCP 電話の保留復帰間隔	SCCP 電話機は、最小値として 5 秒の保留復帰の通知間隔（HRNI）をサポートしますが、SIP 電話機は、最小値として 10 秒をサポートします。 HRNI が最小値の 5 秒に設定された SCCP 電話機では、保留復帰の通知で、SIP 電話機を含むコールを処理するときに、10 秒の呼び出しの遅延が発生する可能性があります。

機能	連携動作
共有電話	保留復帰をサポートしている Cisco Unified IP 電話 が保留復帰をサポートしていない電話デバイスと回線を共有している場合は、サポートしているデバイス上の回線に対してのみ保留復帰設定が表示されます。 共有回線デバイスがこの機能を無効にすると、その回線を共有している他のすべてのデバイスで保留復帰が無効になります。
呼出音設定	電話機に対して指定された呼出音設定が無効になっている場合、その電話機では保留復帰機能に対して呼出音が鳴ったり、点滅したり、ビープ音が鳴ったりしません。

保留復帰の制約事項

機能	制約事項
Cisco Extension Mobility と Cisco Web Dialer	Cisco Extension Mobility 機能と Cisco Web Dialer 機能は、保留復帰機能をサポートしていません。
SCCP 電話機	この機能は、ATA 186、DPA-7610、DPA-7630 などの SCCP アナログ電話タイプをサポートしていません。 ノード上で SCCP を実行している特定のオンネット電話デバイスのみが保留復帰機能を呼び出すことができます。
ディレクトリ番号	電話番号が保留復帰をサポートしていない電話機に関連付けられている場合は、**[電話番号の設定（Directory Number Configuration）]** ウィンドウにその電話番号に関する機能設定が表示されません。
共有回線	保留復帰をサポートしている Cisco Unified IP 電話 が保留復帰をサポートしていない電話デバイスと回線を共有している場合は、サポートしているデバイス上の回線に対してのみ保留復帰設定が表示されます。 共有回線デバイスがこの機能を無効にすると、その回線を共有している他のすべてのデバイスで保留復帰が無効になります。
呼出音設定	保留復帰呼出音では、Cisco Unified Communications Manager Administration でそのユーザに対して定義された呼出音設定（無効、点滅のみ、一度鳴らす、鳴らす、ビープ音のみ）が使用されますが、点滅は一回点滅に変換され、「鳴らす」 が「一度鳴らす」に変換されます。 （注） IP Phone コールが通常の保留中の場合、Call Manager からの呼出音設定（電話機のアイドル）が適用されます。

機能	制約事項
復帰するコールの最大数	回線上で復帰するコールの最大数は、システム上のコールの最大数と同じです。
CTI アプリケーション	CTI アプリケーションを使用してこの機能を有効にするには、CTI アプリケーションがこの機能とこのリリースでの操作が認められていることを確認します。 認められていない場合は、保留復帰機能が既存の CTI アプリケーションに影響するため、CTI アプリケーションが失敗します。 この機能は、デフォルトで無効になっています。 CTI 要件に関する情報については、以下の API ドキュメントを参照してください。 • 『*Cisco Unified TAPI Developers Guide for Cisco Unified Communications Manager*』 • 『*Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager*』
Cisco Unified IP 電話	この機能をサポートしていない電話機に関連付けられた DN の保留復帰設定を構成することはできません。 保留復帰機能をサポートしている Cisco Unified IP 電話 の [電話番号の設定（Directory Number Configuration）] ウィンドウにだけ、保留復帰タイマー設定が表示されます。 保留復帰がシステムに対して設定されていても、電話機がその機能をサポートしていなければ機能はアクティブになりません。 保留復帰をサポートしている Cisco Unified IP 電話 モデルについては Cisco Unified IP 電話 のアドミニストレーション ガイドを、保留復帰に伴う電話機の制約事項についてはこのバージョンの Unified Communications Manager を参照してください。

第 36 章

ハント グループのアクセス

ハント グループの概要

ハント グループは階層的に編成された回線のグループで、ハント グループ リストの最初の番号が話中の場合は 2 番目の番号にダイヤルされます。 2 番目の番号が話中の場合は次の番号がダイヤルされるという具合に続きます。

電話ユーザは、ハント グループへのログインまたはハント グループからのログアウトに IP フォンの [ハント（Hlog）] ソフトキーまたは [ハント グループ（Hunt Group）] 回線ボタンを使用します。 電話にはログイン状態が視覚的に表示されるので、ユーザは各自が 1 つ以上の回線グループにログインしているかどうかを確認できます。

ハント グループ機能には次の機能があります。

- ユーザは IP フォンの [ハント（Hlog）] ソフトキーを使用して電話へのログインと電話からのログアウトを切り替えます。
- ハント グループにより、発信者が内線番号グループから使用可能な回線を自動的に検出できます。
- ハント グループ ログオフ機能により、電話ユーザは、電話番号にルーティングされた着信コールを電話機で受信しないように設定できます。 電話に関連付けられている 1 つ以上の回線グループへのコール以外の着信コールの場合、電話のステータスに関係なく電話の呼び出し音が鳴ります。

（注） 電話番号（DN）は、電話に関連付けられている回線グループに属します。

- システム管理者は、ハント グループに自動でログインした電話へのユーザのログインまたはログアウトを実行できます。
- 電話ユーザは[ハント（Hlog）]ソフトキーを使用して、電話の電話番号が属するすべての回線グループから、その電話をログアウトできます。
- Cisco Unified Communications Manager リリース 9.0 以降では、ハント グループ ログオフ機能により、モバイル デバイスをデスク フォンとして使用できるようになりました。 モバイル クライアントから [ハント（Hlog）] ソフトキーを使用する場合、ハント パイロットに対して発信されたコールを受信しません。

ハント グループの前提条件

- 電話機は Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）を実行中である必要があります。
- 電話機の呼出音ファイルは TFTP ディレクトリ（/usr/local/cm/tftp）に存在する必要があります。

ハント グループの設定タスク フロー

始める前に

- ハント グループの前提条件 （594 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	ハント グループのソフトキー テンプレートの設定 （595 ページ）	[ハント（HLog）] ソフトキーのソフトキー テンプレートを設定します。
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 （596ページ）を行うには、次のサブタスクを完了します。 • 共通デバイス設定へのソフトキー テンプレートの追加 （597ページ） • 電話機と共通デバイス設定の関連付け （598 ページ）	これはオプションです。 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。

	コマンドまたはアクション	目的
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 （598 ページ）	これはオプションです。 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	電話でのハント グループ対応設定 （599 ページ）	ハント グループおよびハント リストのログインおよびログアウトが自動的に行われるように電話を設定します。

ハント グループのソフトキー テンプレートの設定

[HLog] ソフトキーは電話が次のコール状態のときに電話に表示されます。

- 接続されている状態
- オンフック （On Hook）
- オフフック （Off Hook）

（注） [HLog] ソフトキーを設定するには新しいソフトキーテンプレートを作成する必要があります。標準ソフトキー テンプレートに [HLog] ソフトキーを設定することはできません。

以下の手順を使用して、[HLog] ソフトキーを使用できるようにします。

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）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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ソフトキー テンプレートの追加 （597 ページ）
- 電話機とソフトキー テンプレートの関連付け （598 ページ）

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

これはオプションです。 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）]** に追加します。
- ソフトキー テンプレートを**共通デバイス設定**に追加します。

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 （598 ページ）」を参照してください。

始める前に

ハント グループのソフトキー テンプレートの設定 （595 ページ）

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ソフトキー テンプレートの追加 （597 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 （598 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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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

始める前に

共通デバイス設定へのソフトキー テンプレートの追加 （597 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。

電話機とソフトキー テンプレートの関連付け

この手順は省略可能です。 この手順を代わりに使用して、ソフトキー テンプレートを共通デバイス設定と関連付けることができます。 また、この手順は共通デバイス設定とも連動しています。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に使用します。

始める前に

ハント グループのソフトキー テンプレートの設定 （595 ページ）

手順

ステップ 1 Cisco Unified CM 管理から、**[デバイス] > [電話機]** 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 ソフトキー テンプレートを追加する電話機を選択します。

[電話の設定（Phone Configuration）]ウィンドウが表示されます。

ステップ 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]** をクリックします。
電話の設定を更新するには [（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。

電話でのハント グループ対応設定

ハント グループとハント リストに自動でログインまたはログアウトするよう電話を設定するには、この手順を使用します。

始める前に

電話の電話番号が 1 つ以上のハント グループに属することを確認します。

ハント グループおよびハント リストに関しては、『Administration Guide for Cisco Unified Communications Manager』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。**[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 次のいずれかの作業を実行します。

a) 既存の電話機についてのフィールドを変更するには、検索条件を入力し、検索結果の一覧から電話機を選択します。 [電話の設定（Phone Configuration）]ウィンドウが表示されます。

b) 新しい電話機を追加するには、[新規追加] をクリックします。

[新規電話を追加（Add a New Phone）]ウィンドウが表示されます。

ステップ 3 [**電話の設定（Phone Configuration**）] ウィンドウで、次のタスクのいずれかを実行します。

a) ハントグループから電話をログアウトさせるには、[ハントグループにログインする（Logged Into Hunt Group）]チェック ボックスをオフにします。

b) ハント グループに電話をログインさせるには、[ハント グループにログインする（Logged Into Hunt Group）]チェック ボックスをオンにします。

（注） すべての電話ではデフォルトで [ハント グループにログイン（Logged Into Hunt Group）] チェックボックスがオンになっています。

ステップ 4 **[保存（Save）]** をクリックします。

ハント グループのサービス パラメータの設定

[**ハント グループ ログオフ通知（Hunt Group Logoff Notification**）] サービス パラメータは、回線グループへの着信コールが電話に到達したものの、その電話がログアウトしている場合に、着信音をオンまたはオフにするオプションを提供します。 この着信音は、ログアウト中のユーザに、自分の回線がメンバーになっているハントリストに着信コールがあることを知らせますが、回線グループのメンバーの電話は、ログアウトしているため、呼出音が鳴りません。

[**ハント グループ ログオフ通知（Hunt Group Logoff Notification**）] サービス パラメータを設定するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified CM の管理から、**[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 リストで、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（Clusterwide Parameters）]（[デバイス - 電話（Device - Phone）]）セクションで、次の [ハント グループ ログオフ通知（Hunt Group Logoff Notification）] サービス パラメータの値を設定します。

回線グループ（ハント グループ）のメンバーがログアウト中の場合に、Cisco IP 電話 が再生する着信音ファイルの名前を入力します。 このサービス パラメータのデフォルト値は [なし（None）] で、これは着信音がないことを意味します。 255 文字まで入力できます。

ステップ 5 **[保存]** をクリックします。
ウィンドウが更新され、Cisco Unified Communications Manager は、変更内容でサービス パラメータを更新します。

ハント グループの連携動作

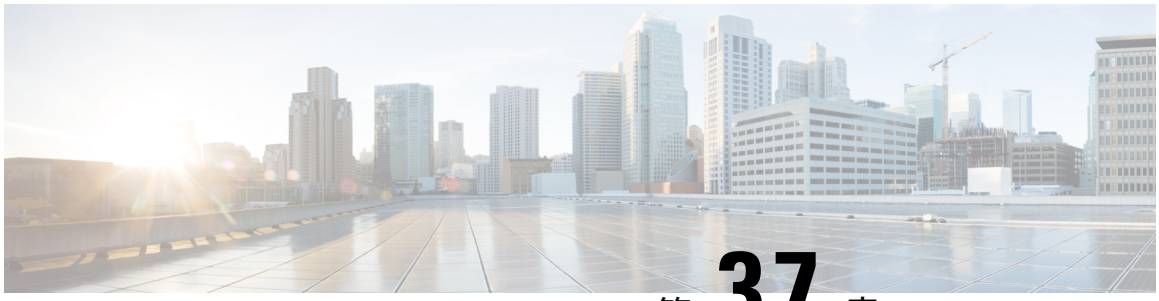
機能	データのやり取り
非共有回線電話番号	電話機が回線グループからログアウトして、その電話機の内線番号が共有されていない場合は、その回線グループ内のその電話番号（DN）で呼出音が鳴りません。 主に回線グループが DN へのコールを提供している場合は、コール処理でその DN がスキップされ、その DN が回線グループに属していないかのように処理されます。

機能	データのやり取り
共有回線電話番号	ハント グループからのログアウト機能はデバイス ベースであるため、ユーザが電話機からログアウトすると、その機能はログアウトされた電話機にのみ影響を与えます。 共有回線電話番号を含む回線グループへのコールは次のように動作します。 • DN を共有しているすべての電話機がログアウトされた場合は、その DN で呼出音が鳴りません。 • DN を共有している 1 つ以上の電話機がログアウトされた場合は、その DN で呼出音が鳴ります。 • ログアウトされた電話機の可聴呼出音は、デフォルトでオフになっています。 Cisco Unified Communications Manager は、コールがログアウトしたハント グループ メンバーに到達したときに別の呼出音が鳴るように設定可能なシステム パラメータを提供しています。

ハント グループの制限

制約事項	説明
複数の回線グループ	ユーザが [ハント（HLog）] ソフトキーを押してハント グループのログオフ機能を有効にすると、電話は関連付けられたすべての回線グループからログアウトします。 これはハント グループのログオフがデバイス ベースの機能であるためです。 電話に複数のグループに属する DN がある場合に [ハント（HLog）] ソフトキーを押すと、電話は関連付けられたすべての回線グループからログアウトします。

制約事項	説明
7940、7960、およびサードパーティ SIP 電話機	• SIP を実行している電話（7906、7911、7941、7961、）がハント グループにログインしていて [不在転送（Call Forward All）] がアクティブになっている場合、コールは SIP を実行している電話に表示されます。 • SIP を実行している 7940 と 7960 電話がハント グループにログインしていて [不在転送（Call Forward All）] がアクティブになっている場合、その電話はスキップされて回線グループの次の電話が鳴ります。 • SIP を実行している 7940 と 7960 電話および SIP を実行しているサードパーティの電話は、[電話の設定（Phone Configuration）] ウィンドウを使用してハント グループにログインまたはログアウトできますが、ソフトキーのサポートはありません。 • SIP を実行している 7940 と 7960 電話および SIP を実行しているサードパーティの電話のステータス行に 「[ハント グループのログアウト（Logged out of hunt groups）]」は表示されません。 • SIP を実行している 7940 と 7960 電話および SIP を実行しているサードパーティの電話は、電話でトーンが設定されているかどうかに関係なく [ハント グループのログオフの通知（Hunt Group Logoff Notification）] トーンは再生されません。



第 37 章

迷惑呼 ID

迷惑呼 ID の概要

迷惑なコールや危険なコールをトラックするために、迷惑呼 ID（MCID）機能を設定できます。 ユーザは、Cisco Unified Communications Manager がネットワーク上の着信コールの発信元を特定して登録するようにリクエストすることで、このようなコールをレポートできます。

MCID 機能を設定すると、次のアクションが実行されます。

1. ユーザが危険なコールを受信し、[迷惑コール（Malicious call）]を押します（または、SCCP ゲートウェイに接続されている POTS 電話機を使用している場合は機能コード *39 を入力します）。
2. Cisco Unified Communications Manager はユーザに確認トーンとテキスト メッセージを送信し（電話機にディスプレイがある場合）、MCID 通知の受信を確認します。
3. Cisco Unified Communications Manager は、迷惑コールとして登録されていることが示されているコールに対して、呼詳細レコード（CDR）を更新します。
4. Cisco Unified Communications Manager は、イベント情報を含むアラームおよびローカルの syslog エントリを生成します。
5. Cisco Unified Communications Manager は、MCID 呼び出しを、ファシリティ メッセージを介して接続されたネットワークに送信します。 ファシリティ情報要素（IE）は、MCID 呼び出しを暗号化します。
6. この通知を受信すると、PSTN または他の接続されたネットワークは、法的機関に通話情報を提供するなどのアクションを実行します。

迷惑呼 ID の前提条件

- MCID をサポートするゲートウェイおよび接続：
  - T1（NI2）と E1（ETSI）接続に MGCP PRI バックホール インターフェイスを使用する PRI ゲートウェイ
  - H.323 トランクおよびゲートウェイ
- MCID をサポートする IP フォン

迷惑呼 ID の設定タスク フロー

始める前に

- 迷惑呼 ID の前提条件 （604 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	電話機能一覧の生成 （5 ページ）	MCID機能をサポートするデバイスを特定するためのレポートを生成します。
ステップ 2	迷惑呼 ID サービス パラメータの設定 （605 ページ）	Cisco Unified Communications Manager が MCID インジケータで呼詳細レコード（CDR）にフラグを設定できるようにします。
ステップ 3	迷惑呼IDアラームの設定 （606ページ）	システム ログにアラーム情報が表示されるようにアラームを設定します。
ステップ 4	迷惑呼IDのソフトキー テンプレートの設定 （607 ページ）	MCID でソフトキー テンプレートを設定します。 （注） Cisco Unified IP Phones 8900 および 9900 シリーズは、機能ボタンを使用する MCID のみをサポートします。
ステップ 5	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 （608ページ）を行うには、次のサブタスクを完了します。 • 共通デバイス設定へのソフトキー テンプレートの追加 （608ページ）	これはオプションです。 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

	コマンドまたはアクション	目的
	• 電話機と共通デバイス設定の関連付け （609 ページ）	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 6	電話機とソフトキー テンプレートの関連付け （610 ページ）	これはオプションです。 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 7	[迷惑呼 ID（Malicious Call Identification）] ボタンの設定 （610 ページ）を行うには、次のサブタスクを完了します。 • 迷惑呼 ID 電話ボタン テンプレートの設定 （611 ページ） • 電話機とボタン テンプレートの関連付け （611 ページ）	MCID ボタンを電話機に追加および設定するには、この手順を実行します。

迷惑呼 ID サービス パラメータの設定

Unified Communications Manager が CDR に MCID インジケータのフラグを付けられるようにするには、CDR フラグを有効にする必要があります。

始める前に

迷惑呼 ID アラームの設定 （606 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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

ステップ 2 **[サーバ（Server）]** ドロップダウン リストから Unified Communications Manager サーバ名を選択します。

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 [システム（System）]エリアで、[CDR 対応フラグ（CDR Enabled Flag）]フィールドを [True]に設定します。

ステップ 5 **[保存（Save）]** をクリックします。

迷惑呼 ID アラームの設定

[ローカル Syslog（Local Syslogs）] で、アラーム イベント レベルを設定し、MCID のアラームをアクティブにする必要があります。

Cisco Business Edition 5000 システムの 1 つのノードのみをサポートします。

始める前に

迷惑呼 ID サービス パラメータの設定 （605 ページ）

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[アラーム（Alarm）]** > **[設定（Configuration）]**。
[アラーム設定（Alarm Configuration）] ウィンドウが表示されます。

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、**[移動（Go）]** をクリックします。

ステップ 3 [サービス グループ（Service Group）]ドロップダウン リストから、[CM サービス（CM Services）]を選択します。 [アラーム設定（Alarm Configuration）]ウィンドウが設定フィールドによって更新されます。

ステップ 4 [サービス（Service）]ドロップダウン リストから、[Cisco CallManager]を選択します。

ステップ 5 [ローカル Syslog（Local Syslogs）] で、[アラーム イベント レベル（Alarm Event Level）]ドロップダウン リストから [情報（Informational）]を選択します。
[アラーム設定（Alarm Configuration）]ウィンドウが設定フィールドによって更新されます。

ステップ 6 [ローカル Syslog（Local Syslogs）] で、[アラームを有効にする（Enable Alarm）] チェックボックスをオンにします。

ステップ 7 すべてのノードについてアラームを有効にする場合は、[すべてのノードに適用（Apply to All Nodes）]チェック ボックスをオンにします。

ステップ 8 情報アラームをオンにするには、[更新（Update）]をクリックします。

迷惑呼 ID のソフトキー テンプレートの設定

（注） Skinny Client Control Protocol（SCCP）IP Phone は MCID 機能を呼び出すためにソフトキーを使用します。

始める前に

迷惑呼 ID アラームの設定 （606 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）] > [ソフトキー テンプレート（Softkey Template）]**。

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] 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]** 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 **[コールステートの選択（Select a call state to configure）]** フィールドで、**[接続済み（Connected）]** を選択します。
[選択されていないソフトキー（Unselected Softkeys）] のリストによって、このコール ステートで利用可能なソフトキーの表示が変わります。

ステップ 7 **[選択されていないソフトキー（Unselected Softkeys）]** ドロップダウン リストで、**[悪意のあるコールのトレース（MCID）の切り替え]** を選択します。

ステップ 8 [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 9 [保存（Save）]をクリックします。

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

これはオプションです。 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）]** に追加します。
- ソフトキー テンプレートを**共通デバイス設定**に追加します。

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 （610ページ）」を参照してください。

始める前に

迷惑呼 ID のソフトキー テンプレートの設定 （607 ページ）

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ソフトキー テンプレートの追加 （608 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 （609 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

始める前に

迷惑呼 ID のソフトキー テンプレートの設定 （607 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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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

始める前に

共通デバイス設定へのソフトキー テンプレートの追加 （608 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。

電話機とソフトキー テンプレートの関連付け

（オプション） 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。

[迷惑呼 ID（Malicious Call Identification）] ボタンの設定

このセクションの手順では、迷惑呼 ID ボタンを設定する方法を説明します。

始める前に

迷惑呼 ID アラームの設定 （606 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	迷惑呼 ID 電話ボタン テンプレートの設定 （611 ページ）.	迷惑呼 ID ボタン機能を回線または短縮ダイヤルキーに割り当てるには、この手順を実行します。
ステップ 2	電話機とボタン テンプレートの関連付け （611 ページ）	電話機の迷惑呼 ID ボタンを設定するには、この手順を実行します。

迷惑呼 ID 電話ボタン テンプレートの設定

始める前に

迷惑呼 ID アラームの設定 （606 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）]** > **[電話ボタンテンプレート（Phone button template）]** の順に選択します。

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]** 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]** をクリックします。

ステップ 7 次のいずれかの作業を実行します。

- 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

迷惑呼 ID 電話ボタン テンプレートの設定 （611 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]** 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。

迷惑呼 ID の連携動作

表 *47 :* 迷惑呼 *ID* の連携動作

機能	データのやり取り
会議コール	ユーザが電話会議に接続されている場合、ユーザはMCID機能を使用してコールに迷惑コールとしてフラグを付けることができます。Cisco Unified Communications Manager は、MCID 通知をユーザに送信したり、アラームを生成したり、CDR を更新したりできます。 ただし、Cisco Unified Communications Manager は、電話会議に関連している可能性のある接続されたネットワークには、MCID呼び出しメッセージを送信しません。
エクステンションモビリティ	エクステンションモビリティのユーザは、[迷惑コール（MCID）] ソフトキーをユーザ デバイス プロファイルの一部として持つことができ、電話機にログインする際にこの機能を使用できます。
コール詳細レコード	CDR を使用して迷惑コールをトラックするには、Cisco CallManager サービス パラメータで、[CDR 有効フラグ（CDR Enabled Flag）]を[はい（True）]に設定する必要があります。 コール中に MCID 機能が使用されると、コールの CDR の [コメント（Comment）] フィールドに **[CallFlag=MALICIOUS]** が書き込まれます。

機能	データのやり取り
アラーム	[ローカル Syslog（Local Syslogs）] 内の MCID 機能のアラームを記録するには、Cisco Unified Serviceability でアラームを設定する必要があります。[ローカル Syslog（Local Syslogs）]で、[情報（Informational）] アラーム イベント レベルのアラームを有効にします。 コール中に MCID 機能が使用されると、システムはアラーム内の SDL トレースと Cisco Unified Communications Manager トレースのログを取ります。 Cisco Unified Serviceability を使用して、[アラーム イベント ログ（Alarm Event Log）]を参照できます。 トレースには、次の情報が含まれます。 • 日付と時刻 • イベントのタイプ：情報 • 情報:迷惑呼 ID 機能は、Cisco Unified Communications Manager で呼び出されます。 • 着信側番号 • 着信側デバイス名 • 着信側の表示名 • 発信側番号 • 発信側デバイス名 • 発信側の表示名 • アプリケーション ID • [クラスタ ID(Cluster ID)] • ノード ID アラームとトレースの詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Cisco Unified Serviceability Administration Guide*』を参照してください。
Cisco ATA 186 アナログ電話ポート	Cisco ATA 186 アナログ電話ポートは、機能コード（*39）を使用して MCID をサポートします。

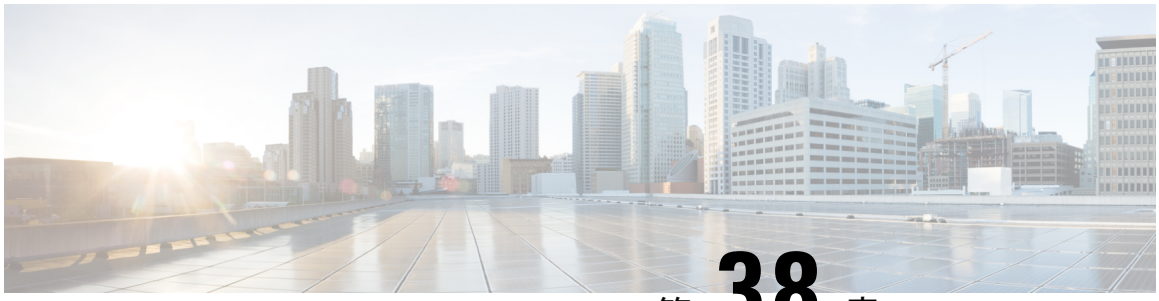
迷惑呼 ID の制約事項

表 *48 :* 迷惑呼 *ID* の制約事項

機能	制約事項
迷惑呼 ID の着信（MCID-T）機能	Cisco Unified Communications Manager は、迷惑呼 ID の発信機能（MCID-O）のみをサポートします。 Cisco Unified Communications Manager は、迷惑呼 ID の着信機能（MCID-T）はサポートしません。 Cisco Unified Communications Manager が迷惑呼 ID のネットワークから通知を受信しても、Cisco Unified Communications Manager は通知を無視します。
クラスタ間トランク	Cisco Unified Communications Manager は MCID-T 機能をサポートしないので、MCID はクラスタ間トランクでは機能しません。
Cisco MGCP FXS ゲートウェイ	Cisco MGCP FXS ゲートウェイは MCID をサポートしません。 フックフラッシュを受け入れて MGCP で機能コードを収集するメカニズムはありません。
QSIG トランク	MCID は QSIG 標準規格ではないため、QSIG トランクでは機能しません。
Cisco VG248 Analog Phone Gateway	Cisco VG248 Analog Phone Gateway は MCID をサポートしません。
SIP トランク	MCID は SIP トランクをサポートしません。
即時転送	システムは MCID と即時転送機能の同時使用をサポートしません。

迷惑呼 ID トラブルシューティング

迷惑呼 ID をトラックし、トラブルシュートするために、Cisco Unified Communications Manager SDL トレースとアラームを使用できます。 MCID のトラップ設定とトレースについては、『*Cisco Unified Serviceability Administration Guide*』を参照してください。 MCID のレポートを作成する方法については、『*Cisco Unified CDR Analysis and Reporting* アドミニストレーションガイド』を参照してください。



第 38 章

コール転送

コール転送の概要

転送機能を使用すると、接続されているコールを自分の電話機から別の番号へリダイレクトできます。 コール転送後にコールは切断され、転送されたコールが新しいコール接続として確立されます。

次に各種コール転送について説明します。

- **打診転送とブラインド転送**：打診転送では、コールに応答した転送先電話のユーザに打診した後で、転送元電話のユーザが発信者を転送先アドレスにリダイレクトできます。 つまり、転送元電話のユーザは、転送先電話のユーザがコールに応答するまで、そのコールに接続した状態になります。 ブラインド転送では、転送元電話のユーザが発信者を接続先回線に接続してから、転送先がコールに応答します。

  ほとんどの電話機では、転送にハードキーまたはソフトキーを使用します。 打診転送とブラインド転送のいずれでも、個別の設定は不要です。 この 2 種類の転送の違いは、転送元のユーザが**[転送（Transfer）]** ボタンを 2 回目に押す時点です。 打診転送では、転送先が応答した後で転送元のユーザが **[転送（Transfer）]** ボタンを押しますが、ブラインド転送では、転送先が応答する前に転送元のユーザが **[転送（Transfer）]** ボタンを押します。

  SCCP が開始したブラインド転送の場合、Cisco Unified Communications Manager では、転送されたユーザに対する呼出音の形でコールの進行状況が示されます。

- **オンフック転送**：このタイプのコール転送では、ユーザが **[転送（Trnsfer）]** ソフトキーを押し、コール転送先の番号をダイヤルし、**[転送（Trnsfer）]** ソフトキーを再度押すか、またはオンフック状態にすると、転送操作が完了します。 **[オンフック転送（Transfer On-Hook）]**サービス パラメータを **[はい（True）]** に設定する必要があります。 このサービス パラメータは、ユーザが転送操作の開始後にオンフックにした場合にコール転送が完了するかどうかを決定します。

オンフック転送オプションは打診転送とブラインド転送の両方で使用されます。

- **直接転送**：このタイプの転送では、ユーザが確立されている2つのコール（保留中のコールまたは接続状態のコール）を結合して1つのコールにし、開始者を転送から削除できます。直接転送では、打診コールが開始されたり、アクティブなコールが保留になったりすることはありません。ユーザは、確立されている2つのコールを結合して開始者を削除するときには **DirTrfr** ソフトキーを使用します。

コール転送の設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	打診転送およびブラインド転送の設定（616 ページ）	転送を使用すると、転送受信者に打診しているかどうかにかかわらず1つのコールを新しい番号にリダイレクトできます。 転送をソフトキーまたはボタンとして設定するには、この手順を実行します。
ステップ 2	オンフック転送の設定 （622 ページ）	（オプション）オンフック転送は、コール転送を完了するためのオプションです。 [転送（Trnsfer）] を押して、コールを転送する番号をダイヤルし、オンフックにして転送を完了します。 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。
ステップ 3	直接転送の設定 （623 ページ）	（オプション）直接転送を使用すると、2つのコールを相互に転送できます（通信は継続されません）。 DirTrfr をソフトキーまたはボタンとして設定するには、この手順を実行します。

打診転送およびブラインド転送の設定

電話でソフトキーとボタンのどちらがサポートされているかに応じて、いずれかのタスク フローを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	転送用のソフトキー テンプレートの設定 （617 ページ）	
ステップ 2	[転送（Transfer）] ボタンの設定 （621 ページ）	

転送用のソフトキー テンプレートの設定

[転送（Trnsfer）] ソフトキーは、コールの打診転送およびブラインド転送に使用します。 [転送（Trnsfer）] ソフトキーには次のコール状態があります。

- 接続されている状態
- 保留中

[転送（Trnsfer）] ソフトキーを使用可能にするには、以下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。**[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）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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。

- 共通デバイス設定と転送ソフトキー テンプレートの関連付け （618 ページ）
- 電話と転送ソフトキー テンプレートの関連付け （620 ページ）

共通デバイス設定と転送ソフトキー テンプレートの関連付け

（オプション） 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）]** に追加します。
- ソフトキー テンプレートを**共通デバイス設定**に追加します。

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、「電話と転送ソフトキーテンプレートの関連付け （620ページ）」を参照してください。

始める前に

転送用のソフトキー テンプレートの設定 （617 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	転送共通デバイス設定へのソフトキー テンプレートの追加 （619 ページ）	共通デバイス設定に転送ソフトキー テンプレートを追加するには、次の手順を実行します。
ステップ 2	電話機と共通デバイス設定の関連付け （620 ページ）	転送ソフトキーの共通デバイス設定を電話にリンクするには、次の手順を実行します。

次のタスク

[転送（Transfer）] ボタンの設定 （621 ページ）

転送共通デバイス設定へのソフトキー テンプレートの追加

始める前に

転送用のソフトキー テンプレートの設定 （617 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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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

始める前に

転送共通デバイス設定へのソフトキー テンプレートの追加 （619 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。

電話と転送ソフトキー テンプレートの関連付け

（オプション） 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。

始める前に

転送用のソフトキー テンプレートの設定 （617 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、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。

[転送（Transfer）] ボタンの設定

この項の手順では、[転送（Transfer）] ボタンの設定方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	転送用の電話ボタン テンプレートの設定 （621 ページ）	[転送（Transfer）] ボタン機能を回線キーまたは短縮ダイヤル キーに割り当てるには、次の手順を実行します。
ステップ 2	電話と転送ボタン テンプレートの関連付け （622 ページ）	電話の [転送（Transfer）] ボタンを設定するには、次の手順を実行します。

転送用の電話ボタン テンプレートの設定

（オプション） 回線または短縮ダイヤル キーに機能を割り当てるには、次の手順に従います。

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。**[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）]** の順に選択します。

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]** 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]** をクリックします。

ステップ 7 次のいずれかの作業を実行します。

- 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。

電話と転送ボタン テンプレートの関連付け

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]** 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。

オンフック転送の設定

始める前に

打診転送およびブラインド転送の設定 （616 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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。
[サービス パラメータの設定（Service Parameter Configuration）]ウィンドウが表示されます。

ステップ 2 **[サーバ（Server）]** ドロップダウン リストで、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。

ステップ 4 **[クラスタ全体パラメータ（デバイス：電話）（Clusterwide Parameters (Device - Phone)）]** の、**[オンフック転送有効化（Transfer On-Hook Enabled）]** サービス パラメータで [True]を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

直接転送の設定

電話でソフトキーとボタンのどちらがサポートされているかに応じて、いずれかのタスク フローを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	直接転送のソフトキー テンプレートの設定 （623 ページ）	[直接転送（Direct Transfer）] ソフトキーをテンプレートに追加し、共通デバイス設定または電話を使用してソフトキーを設定するには、次の手順を実行します。
ステップ 2	[直接転送（Direct Transfer）] ボタンの設定 （627 ページ）	電話機に [直接転送（Direct Transfer）] ボタンを追加して設定するには、この手順を実行します。

直接転送のソフトキー テンプレートの設定

直接転送ソフトキーには次のコール状態があります。

- 接続されている状態
- 保留中

次の手順を使用して、直接転送ソフトキーを使用できるようにします。

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）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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。

- 共通デバイス設定と直接転送ソフトキー テンプレートの関連付け （624 ページ）
- 電話と直接転送ソフトキー テンプレートの関連付け （626 ページ）

共通デバイス設定と直接転送ソフトキー テンプレートの関連付け

（オプション） 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）]** に追加します。
- ソフトキー テンプレートを**共通デバイス設定**に追加します。

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、次を参照してください。電話と直接転送ソフトキーテンプレートの関連付け （626 ページ）

始める前に

直接転送のソフトキー テンプレートの設定 （623 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	直接転送共通デバイス設定へのソフトキーテンプレートの追加 （625 ページ）	共通デバイス設定に直接転送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。
ステップ 2	電話機と共通デバイス設定の関連付け （626 ページ）	共通デバイス設定に直接転送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。

直接転送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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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

始める前に

直接転送共通デバイス設定へのソフトキー テンプレートの追加 （625 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。

電話と直接転送ソフトキー テンプレートの関連付け

（オプション） 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。

始める前に

直接転送のソフトキー テンプレートの設定 （623 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、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。

[直接転送（Direct Transfer）] ボタンの設定

このセクションの手順では、[直接転送（Direct Transfer）] ボタンの設定方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	直接転送の電話ボタン テンプレートの設定 （627 ページ）	[直接転送（Direct Transfer）] ボタン機能を回線または短縮ダイヤル キーに割り当てるには、次の手順を実行します。
ステップ 2	電話と直接転送ボタン テンプレートの関連付け （628 ページ）	電話で [直接転送（Direct Transfer）] ボタンを設定するには、次の手順を実行します。

直接転送の電話ボタン テンプレートの設定

（オプション） 回線または短縮ダイヤルキーに機能を割り当てるには、次の手順に従います。

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。**[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）]** の順に選択します。

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]** 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]** をクリックします。

ステップ 7 次のいずれかの作業を実行します。

- 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。

電話と直接転送ボタン テンプレートの関連付け

始める前に

直接転送の電話ボタン テンプレートの設定 （627 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]** 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。

コール転送の連携動作

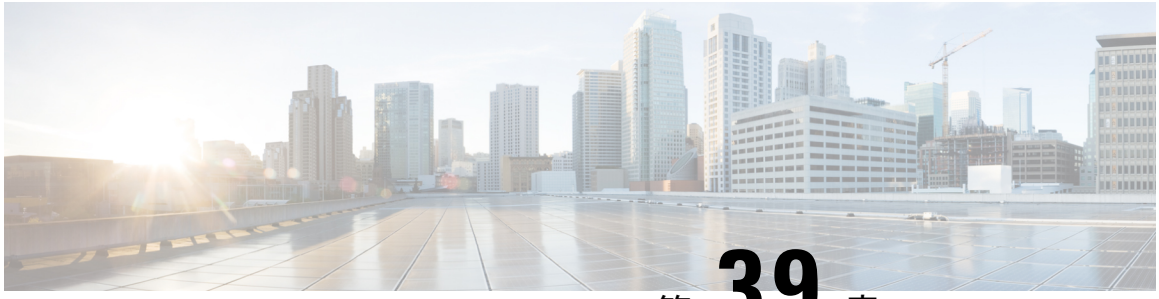
機能	データのやり取り
論理パーティション設定	

機能	データのやり取り
	転送元となるデバイスの地理位置 ID と、転送宛先となるデバイスの地理位置 ID の間で、論理パーティション ポリシー チェックが実行されます。 論理パーティション処理は、次の状況で実行されます。 • 電話ユーザが [転送（Transfer）] ソフトキーを使用してコールを転送する際に、このソフトキーを 2 回押してコール転送機能を起動し、処理する場合。 • 他の転送メカニズム（直接転送、オンフック転送、フックフラッシュ転送、および CTI アプリケーション開始転送など）により、コール転送機能が呼び出される場合。 • 転送元および転送宛先が PSTN 参加者を指定している場合。 • Cisco Unified Communications Manager が、転送元および転送宛先デバイスに関連付けられている地理位置 ID 情報を使用して、論理パーティション ポリシー チェックを実行する場合。 • プライマリ コールとセカンダリ コールの分割前および結合前。 論理パーティション設定では拒否コールが次のように処理されます。 • 「外線転送を制限中（External Transfer Restricted）」メッセージが VoIP フォンに送信されます。 • 通常の転送：SCCP を実行する電話の場合、プライマリ コールは保留中のまま、打診コールはアクティブのままになります。 SIP を実行する電話の場合、プライマリ コールと打診コールの両方が保留中のままになるため、障害発生後にこれらのコールを手動で再開する必要があります。 • オンフック、フックフラッシュ、およびアナログ電話開始転送：原因コード 63（「サービスまたはオプションが使用できません（Service or option not available）」）と Cisco Unified Communications Manager からのリオーダー音を使用して、プライマリ コールとセカンダリ コールの両方がクリアされます。 • [転送失敗回数（Number of Transfer Failures）] perfmon カウンタが増加します。

機能	データのやり取り
マルチレベルの優先およびプリエンプション	優先レベルが同一の 2 つのセグメント間でのコール転送をスイッチが開始すると、これらのセグメントでは、転送時に優先レベルが維持されます。 優先レベルが異なるコール セグメント間でコール転送が実行されると、転送を開始したスイッチは、優先レベルが高いセグメントで接続をマークします。 Cisco Unified Communications Manager では、この要件に対応するため、コール転送操作に使用されるコール レッグの優先レベルをアップグレードします。 たとえば、[プライオリティ（Priority）] 優先レベルが設定されている参加者 B に参加者 A がコールするとします。 参加者 B がその後参加者 C への転送を開始し、ダイヤル時に [フラッシュ（Flash）] 優先番号をダイヤルします。 転送が完了すると、参加者 A の優先レベルが [プライオリティ（Priority）] から [フラッシュ（Flash）] にアップグレードされます。 MLPP が有効になるとコール転送機能が自動的に有効になります。電話では [転送（Transfer）] ソフトキーがサポートされます。 （注） クラスタ間トランク（ICT）や PRI トランクなどのトランクデバイスでは、優先レベルのアップグレードは機能しません。

コール転送の制約事項

機能	制約事項
論理パーティション設定	転送元デバイスと転送宛先デバイスの両方が VoIP 電話の場合、論理パーティション設定処理は行われません。 地理位置情報または地理位置情報フィルタがどのデバイスにも関連付けられていない場合、論理パーティション設定処理は行われません。
外線コール転送の制限	外線コールの転送を制限するには、「外線コール転送の制限」の章を参照してください。
ハント パイロット	アナウンス中にハント パイロットへのコール転送が開始された場合、コールはアナウンスが完了するまでリダイレクトされません。



第 39 章

外線コール転送の制限

外線コール転送の制限の概要

外線コール転送の制限は、ゲートウェイ、トランク、およびルート パターンを、システム レベルでオンネット（内部）デバイスまたはオフネット（外部）デバイスとして設定するために使用できる機能です。デバイスをオフネットとして設定すると、外部デバイスへの外線コールの転送を制限できるため、電話料金の詐欺行為の防止に役立ちます。

[オフネット間転送のブロック（Block OffNet to OffNet Transfer）] サービス パラメータが [はい（True）] に設定されている場合に、オフネット ゲートウェイまたはトランクでコールを転送しようとすると、コールを転送できないことを通知するメッセージがユーザの電話に表示されます。

この章では、次の用語を使用します。

用語	説明
オンネット デバイス	オンネットとして設定されており、ネットワーク内部にあるものと見なされるデバイス。
オフネット デバイス	オフネットであると見なされ、ルーティング時にネットワーク外部にあるものと見なされるデバイス。
ネットワークの場所	ネットワークを基準にしたデバイスの場所（オンネットまたはオフネット）。
発信側	転送されるデバイス。 システムはこのデバイスをオンネットまたはオフネットと見なします。

用語	説明
着信側	転送されたコールを受信するデバイス。 システムはこのデバイスをオンネットまたはオフネットと見なします。
DN への着信コール	オンネットまたはオフネットとして分類するために、ゲートウェイまたはトランク コール分類設定だけが使用されるコール。 ルート パターン コール分類設定は適用されません。
発信コール	トランク、ゲートウェイ、およびルートパターンのコール分類設定が考慮されるコール。 ルート パターンの [デバイスの上書きを許可（Allow Device Override）] 設定により、ルート パターン コール分類設定の代わりに、トランクまたはゲートウェイ コール分類設定が使用されるかどうかが決まります。

外部コール転送の制約事項の設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	コール転送制限のサービス パラメータの設定 （634 ページ）	外部コールが別の外部デバイスや番号に転送されるのをブロックします。
ステップ 2	着信コールを設定するには、次の手順を実行します。 • クラスタ全体のサービス パラメータの設定 （636 ページ） • ゲートウェイでのコール転送制限の設定 （637 ページ） • トランクでのコール転送制限の設定 （637 ページ）	ゲートウェイ設定またはトランク設定を使用するか、クラスタ全体のサービス パラメータを設定して、オンネット（内部）またはオフネット（外部）としてゲートウェイとトランクを設定します。
ステップ 3	発信コールの設定 （638 ページ）	ルート パターンの設定を指定して、転送機能を設定します。

コール転送制限のサービス パラメータの設定

別の外部デバイスまたは番号への外部コールの転送をブロックするには、以下の手順を実行します。

手順

ステップ 1 Cisco Unified CM の管理のユーザ インターフェイスから、**[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、設定する Cisco Unified CM 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（アクティブ）（Cisco CallManager (Active)）]を選択します。

ステップ 4 [オフネット間の転送をブロックする（Block OffNet to OffNet Transfer）] ドロップダウン リストから **[はい（True）]** を選択します。 デフォルト値は False です。

ステップ 5 **[保存（Save）]** をクリックします。

着信コールの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	（任意） クラスタ全体のサービス パラメータの設定 （636 ページ）	Cisco Unified Communications Manager クラスタですべてのゲートウェイまたはトランクを [オフネット（OffNet）]（外部）または [オンネット（OnNet）]（内部）として設定します。
ステップ 2	ゲートウェイでのコール転送制限の設定（637 ページ）	[ゲートウェイの設定（Gateway Configuration）] を使用して、ゲートウェイを [オンネット（OnNet）]（内部）または [オフネット（OffNet）]（外部）として設定します。 この機能を、クラスタ全体のサービス パラメータ [オフネット間転送のブロック（Block OffNet to OffNet Transfer）] と共に使用する場合、設定によってコールをゲートウェイ経由で転送できるかどうかが決まります。 次のデバイスを内部デバイスおよび外部デバイスとして Cisco Unified Communications Manager に設定できます。 • H.323 ゲートウェイ

	コマンドまたはアクション	目的
		• MGCP FXO トランク • MGCP T1/E1 トランク
ステップ 3	トランクでのコール転送制限の設定（637 ページ）	[トランクの設定（Trunk Configuration）] を使用して、トランクを [オンネット（OnNet）]（内部）または [オフネット（OffNet）]（外部）として設定します。この機能を、クラスタ全体のサービス パラメータ [オフネット間転送のブロック（Block OffNet to OffNet Transfer）] と共に使用する場合、設定によってコールをトランク経由で転送できるかどうかが決まります。 次のデバイスを内部デバイスおよび外部デバイスとして Cisco Unified Communications Manager に設定できます。 • InterCluster Trunk; クラスタ間トランク • SIP トランク

クラスタ全体のサービス パラメータの設定

Cisco Unified Communications Manager クラスタで、すべてのゲートウェイまたはトランクを [オフネット（OffNet）]（外部）または [オンネット（OnNet）]（内部）と設定するには、次の手順を実行します。

始める前に

コール転送制限のサービス パラメータの設定 （634 ページ）

手順

ステップ 1 Cisco Unified CM の管理のユーザ インターフェイスから、**[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、設定する Cisco Unified CM 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（アクティブ）（Cisco CallManager (Active)）] を選択します。

ステップ 4 [通話の分類（Call Classification）] ドロップダウン リストから、[オフネット（OffNet）] または [オンネット（OnNet）] を選択します（デフォルトでは [オフネット（OffNet）] が指定されています）。

ゲートウェイでのコール転送制限の設定

オフネット、オンネットまたはシステム デフォルトの使用としてゲートウェイを設定するには、次の手順を実行します。 システムはそれぞれオフネットまたはオンネットとしてのゲートウェイを通ってネットワークに到達するコールと見なします。

始める前に

クラスタ全体のサービス パラメータの設定 （636 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)]** > **[ゲートウェイ(Gateway)]**。

[ゲートウェイの検索と一覧表示（Find and List Gateways）] ウィンドウが表示されます。

ステップ 2 設定されているゲートウェイを一覧表示するには、[検索（Find）]をクリックします。

Unified Communications Manager で設定されたゲートウェイが表示されます。

ステップ 3 オフネットまたはオンネットとして設定するゲートウェイを選択します。

ステップ 4 [コールの分類（Call Classification）] フィールドでオフネットまたはオンネットを選択します。クラスタ全体の制限をすべてのゲートウェイで有効にしている場合、各ゲートウェイを [システム デフォルトの使用（Use System Default）] に設定します（つまり、コールの分類サービス パラメータをゲートウェイの設定として使用します）。

ステップ 5 **[保存（Save）]** をクリックします。

トランクでのコール転送制限の設定

トランクを [オフネット（OffNet）]、[オンネット（OnNet）]、または [システムのデフォルトを使用（Use System Default）] として設定するには、次の手順を実行します。 [オフネット（OffNet）] または [オンネット（OnNet）] として設定されているトランクを通じてネットワークに届くコールは個々に考慮されます。

始める前に

ゲートウェイでのコール転送制限の設定 （637 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)]** > **[トランク(Trunk)]**。

[トランクの検索と一覧表示（Find and List Trunk）] ウィンドウが表示されます。

ステップ 2 設定済みのトランクを一覧表示するには、[**検索（Find**）] をクリックします。

Unified Communications Manager で設定されたトランクが表示されます。

ステップ 3 [オフネット（OffNet）] または [オンネット（OnNet）] として設定するトランクを選択します。

ステップ 4 [コール分類（Call Classification）] ドロップダウン リストから、次のいずれかのフィールドを選択します。

- [オフネット（OffNet）]：このフィールドを選択すると、ゲートウェイは外部ゲートウェイとして識別されます。[オフネット（OffNet）] として設定されているゲートウェイからコールが届くと、接続先デバイスに外部リングが送信されます。
- [オンネット（OnNet）]：このフィールドを選択すると、ゲートウェイは内部ゲートウェイとして識別されます。[オンネット（OnNet）] として設定されているゲートウェイからコールが届くと、接続先デバイスに内部リングが送信されます。
- [**システムデフォルトの使用（Use System Default**）]：このフィールドを選択すると、Unified Communications Manager のクラスタ全体に対するサービス パラメータである [コールの分類（Call Classification）] が使用されます。

（注） すべてのトランクでクラスタ全体の制限を有効にした場合は、各トランクを [システムのデフォルトを使用（Use System Default）] に設定します（つまり、[コール分類（Call Classification）] サービス パラメータの設定が読み込まれ、その設定がトランクに使用されます）。

ステップ 5 [保存（Save）] をクリックします。

発信コールの設定

コールをオンネットまたはオフネットとして分類するには、[**ルート パターン設定（Route Pattern Configuration**）] ウィンドウの [**コール分類（Call Classification**）] フィールドをそれぞれオンネットまたはオフネットに管理者が設定します。 管理者がルート パターン設定の上書きとトランクまたはゲートウェイ設定を使用ができるようにするには、[**ルート パターン設定（Route Pattern Configuration**）] ウィンドウの [**デバイス上書き許可（Allow Device Override**）] チェックボックスをオンにします。

始める前に

トランクでのコール転送制限の設定 （637 ページ）

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、**[検索（Find）]** をクリックしてすべてのルート パターンを一覧にします。

ステップ 2 設定したいルート パターンを選択するか、[新規追加] をクリックします。

ステップ 3 **[ルート パターン設定（Route Pattern Configuration）]** ウィンドウで、ルート パターンの設定と転送機能を設定するには、次のフィールドを使用します。

a) **[コール分類（Call Classification）]** —オフネットまたはオンネットのルート パターンを使用してコールを分類するためにこのドロップダウン リストを使用します。

b) **[外部のダイヤル トーン入力（Provide Outside Dial Tone）]** —コールの分類がオフネットに設定されると、このチェックボックスがチェックされます。

c) **[デバイス上書き許可（Allow Device Override）]**—このチェックボックスをオンにすると、システムは、[ルート パターン設定（Route Pattern Configuration）] ウィンドウの [コール分類（Call Classification）] ではなく、ルート パターンに関連付けられたトランクまたはゲートウェイのコール分類を使用します。

ステップ 4 **[保存（Save）]** をクリックします。

外線コール転送の制限の連携動作

機能	データのやり取り
会議の破棄	会議の破棄機能は、会議の参加者がオフネットとオンネットのどちらに設定されているかをチェックすることにより、既存のアドホック会議を破棄する必要があるかどうかを決定します。 この機能を設定するには、サービスパラメータの [アドホック会議の破棄（Drop Ad Hoc Conference）] を使用して、オプションの [オンネット参加者が会議に残っていない場合（When No OnNet Parties Remain in the Conference）] を選択します。 参加者が使用しているデバイスまたはルートパターンをチェックすることにより、各参加者のオンネット ステータスを判断します。詳細については、「アドホック会議」の章からリンクしているアドホック会議に関するトピックを参照してください。
一括管理	一括管理は、ゲートウェイテンプレートにゲートウェイ設定（オフネットまたはオンネット）を挿入します。 詳細については、『*Cisco Unified Communications Manager Bulk Administration* ガイド』を参照してください。
Dialed Number Analyzer（DNA）	ゲートウェイの番号分析に使用されている場合は、DNA にゲートウェイとルートパターン用に設定されたコール分類が表示されます。詳細については、『*Cisco Unified Communications Manager Dialed Number Analyzer Guide*』を参照してください。

外線コール転送の制限

制約事項	説明
FXS ゲートウェイ	Cisco Catalyst 6000 24 ポートのような FXS ゲートウェイには [ゲートウェイの設定（Gateway Configuration）] ウィンドウの [コールの分類（Call Classification）] フィールドはありません。したがって、システムは常にそれらをオンネットと見なします。
Cisco VG248 ゲートウェイ	システムは [コールの分類（Call Classification）] フィールドがない Cisco VG248 ゲートウェイをサポートしていません。
FXS ポート	Cisco Unified Communications Manager はすべての Cisco Unified IP 電話 と FXS ポートをオフネット（外部）として設定できないオンネット（内部）と見なします。

第 XI 部

プレゼンスおよびプライバシー機能

第 40 章

割込み

割り込みの概要

割り込みを使用すると、共有回線上のリモートでアクティブなコールにユーザを追加できます。 回線のリモートでアクティブなコールとは、その回線で電話番号を共有する別のデバイスとの間のアクティブな（接続された）コールのことです。

パーティ参加トーンを設定すると、基本コールが割り込みコールまたはC割り込みコールに変更されたときに電話機でトーンが再生されます。 また、参加者がマルチパーティ コールから退出したときも別のトーンが再生されます。

電話機は、次の会議モードで割り込みをサポートします。

- 割り込まれる電話機でのビルトイン会議ブリッジ：このモードでは、[割り込み（Barge）] ソフトキーを使用します。 ほとんどの Cisco Unified IP Phone に、ビルトイン会議ブリッジ機能があります。
- 共有会議ブリッジ：このモードでは、[C 割り込み（cBarge）] ソフトキーを使用します。

リモートで使用中のコール状態で [割り込み（Barge）] ソフトキーまたは [C割り込み（cBarge）] ソフトキーを押すと、ユーザがすべての参加者とのコールに追加され、参加者全員が割り込みビープ音を受信します（設定されている場合）。 割り込みに障害が発生した場合、元のコールはアクティブなままとなります。 使用可能な会議ブリッジ（ビルトインまたは共有）がない場合、割り込み要求は拒否され、割り込み発信側のデバイスにメッセージが表示されます。 ネットワークまたは Unified Communications Manager で障害が発生した場合、割り込みコールは保持されます。

（注） Barge と cBarge 両方のソフトキー オプションを表示するには、Unified Communications Manager のユーザ インターフェイスで、回線が共有されているデバイスの **[プライバシー]** オプションを無効にします。

割り込みをサポートする Cisco Unified IP Phone のリストについては、Cisco Unified Reporting にログインして、[Unified CM Phone 機能リスト（Unified CM Phone Feature List）] レポートを実行します。 必ず、機能として [ビルトイン ブリッジ（Built In Bridge）] 選択してください。 詳細については、電話機能一覧の生成 （5 ページ）を参照してください。

ワンボタン割り込みおよびワンボタン C 割り込み

ワンボタン割り込み機能およびワンボタンC割り込み機能を使用すると、ユーザはリモートでアクティブなコールの共有回線ボタンを押してコールに参加できます。参加者全員が、割り込みビープ音を受信します（設定されている場合）。割り込みに障害が発生した場合、元のコールはアクティブなままとなります。

電話機は、次の2つの会議モードでワンボタン割り込みとワンボタンC割り込みをサポートします。

- 割り込まれる電話機でのビルトイン会議ブリッジ：このモードでは、ワンボタン割り込み機能を使用します。
- 共有会議ブリッジ：このモードでは、ワンボタン C 割り込み機能を使用します。

リモートで使用中のコールで共有回線ボタンを押すと、ユーザがすべての参加者とのコールに追加され、参加者全員が割り込みビープ音を受信します（設定されている場合）。割り込みに障害が発生した場合、元のコールはアクティブなままとなります。 使用可能な会議ブリッジ（ビルトインまたは共有）がない場合、割り込み要求は拒否され、割り込み発信側のデバイスにメッセージが表示されます。

組み込み会議

ユーザが [割り込み（Barge）] ソフトキーまたは共有回線ボタンを押すと、組み込み会議ブリッジが使用可能な場合にこのブリッジを使用して割り込みコールが設定されます。 組み込み会議ブリッジは、割り込みが設定されていると元のコールへのメディアの中断および表示変更が行われないため、便利です。

共有会議

ユーザが [C 割り込み（cBarge）] ソフトキーまたは共有回線ボタンを押すと、共有会議ブリッジが使用可能な場合にこのブリッジを使用して割り込みコールが設定されます。 元のコールが分割され、会議ブリッジに参加します。これにより、短いメディア割り込みが発生します。参加者全員の通話情報が 「[割り込み（Barge）]」 に変わります。 割り込み先コールが会議コールになり、割り込み対象デバイスが会議の開催者になります。 会議の開催者は、会議にさらに参加者を追加するか、または参加者を削除できます。 いずれかの参加者がコールを解放する

と、残り 2 人の参加者に対し短い中断が発生し、これらの参加者はポイントツーポイントコールとして再接続されます。これにより、共有会議リソースが解放されます。

組み込み会議と共有会議の相違点

組み込み会議ブリッジと共有会議での割り込みの相違点を次の表に示します。

機能	組み込み会議への割り込み	共有会議への割り込み
標準ソフトキー テンプレートに [割り込み（Barge）]/[C 割り込み（cBarge）] ソフトキーが含まれている。 （注） ワンボタン割り込み/C 割り込み機能が有効な場合、このソフトキーは使用されません。	可	不可
割り込みのセットアップ中にメディアの切断が発生する。	不可	可
設定されている場合、ユーザが割り込み設定トーンを受信する。	可	可
割り込み元の電話にテキストを表示する。	[割り込み XXX（To barge XXX）]	[会議（To Conference）]
相手側の電話にテキストを表示する。	他の参加者へ/他の参加者から	[会議（To Conference）]
その他の電話にテキストが表示される。	着信側へ/着信側から	[会議（To Conference）]
ブリッジで、すでに割り込まれたコールへの 2 回目の割り込みの設定がサポートされている。	不可	可
割り込み元がコールを解放する。	元の 2 人の参加者で、メディアの中断は発生しません。	2 人の参加者のみが残っており、残りの参加者をポイントツーポイントのコールとして再接続するときに、共有会議ブリッジ解放のためメディアの中断が発生します。

機能	組み込み会議への割り込み	共有会議への割り込み
相手側がコールを解放する。	発信側を他の参加者とポイントツーポイント コールとして接続するために、メディアの中断が発生します。	2 人の参加者のみが残っており、残りの参加者をポイントツーポイントのコールとして再接続するときに、共有会議ブリッジ解放のためメディアの中断が発生します。
他の参加者がコールを解放する。	3 人の参加者すべてが解放されます。	2 人の参加者のみが残っており、残りの参加者をポイントツーポイントのコールとして再接続するときに、共有会議ブリッジ解放のためメディアの中断が発生します。
相手側はコールを保留にして、直接転送、参加、またはコール パークを実行する。	割り込み元が解放されます。	発信側および他の参加者は接続されたままになります。

割り込みの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	組み込み会議用のソフトキーテンプレートの設定 （649 ページ）	ソフトキー テンプレートに [割り込み（Barge）] ソフトキーを追加します。組み込みの会議ブリッジの割り込みを設定するには、次の手順に従います。
ステップ 2	共有会議用ソフトキー テンプレートの設定 （650 ページ）	ソフトキーテンプレートに[会議ブリッジの割り込み（cBarge）] ソフトキーを追加します。 共有会議ブリッジの割り込みを設定するには、次の手順に従います。
ステップ 3	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 （652 ページ）を行うには、次のサブタスクを完了します。 • 共通デバイス設定へのソフトキー テンプレートの追加 （653 ページ） • 電話機と共通デバイス設定の関連付け （653 ページ）	これはオプションです。 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

	コマンドまたはアクション	目的
		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 4	電話機とソフトキー テンプレートの関連付け （652 ページ）	これはオプションです。 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 5	組み込み会議の割り込みの設定 （654 ページ）	組み込みの会議ブリッジの割り込みを設定します。
ステップ 6	共有会議の割り込みの設定 （655 ページ）	共有会議ブリッジの割り込みを設定します。
ステップ 7	ユーザとデバイスの関連付け （80 ページ）	ユーザとデバイスを関連付けます。

組み込み会議用のソフトキー テンプレートの設定

割り込みのためのソフトキーテンプレートを設定し、そのテンプレートに[割り込み（Barge）]ソフトキーを割り当てます。 [割り込み（Barge）] ソフトキーは [リモートで使用中（Remote In Use）]のコールの状態で設定できます。

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。**[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）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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ソフトキー テンプレートの追加 （653 ページ）
- 電話機と共通デバイス設定の関連付け （653 ページ）

共有会議用ソフトキー テンプレートの設定

共有会議用ソフトキーテンプレートを設定し、C割り込みソフトキーをそのテンプレートに割り当てます。 [リモート使用中（Remote In Use）] 発信状態で C 割り込みソフトキーを設定できます。

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。**[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）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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。

電話機とソフトキー テンプレートの関連付け

手順

ステップ 1 Cisco Unified CM 管理から、**[デバイス]** > **[電話機]** を選択します。
[**電話の検索/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 ソフトキー テンプレートを追加する電話機を検索します。

ステップ 3 次のいずれかの作業を実行します。

- [**共通デバイス設定（Common Device Configuration**）] ドロップダウン リストから、必要なソフトキー 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。
- [**ソフトキー テンプレート（Softkey Template**）] ドロップダウン リストで、[割り込み（Barge）] または [C 割り込み（cBarge）] 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]** 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。

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

（**オプション**） 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**）] に追加します。
- ソフトキー テンプレートを**共通デバイス設定**に追加します。

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 （652ページ）」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 （462 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 （462 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

始める前に

必要に応じて、次のいずれかまたは両方を実行します。

- 組み込み会議用のソフトキー テンプレートの設定 （649 ページ）
- 共有会議用ソフトキー テンプレートの設定 （650 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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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

始める前に

必要に応じて、次のいずれかまたは両方を実行します。

- 組み込み会議用のソフトキー テンプレートの設定 （649 ページ）
- 共有会議用ソフトキー テンプレートの設定 （650 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。

次のタスク

次のいずれかまたは両方を実行します。

- 組み込み会議の割り込みの設定 （654 ページ）
- 共有会議の割り込みの設定 （655 ページ）

組み込み会議の割り込みの設定

ほとんどの Cisco Unified IP Phone には会議ブリッジ機能が組み込まれています。つまり、これらの Cisco IP 電話 には、割り込み機能をサポートするための小型の会議ブリッジとして動作する内部 DSP が搭載されています。 サポートされる通話者は、電話機自体を含め 3 つまでです。ファームウェアバージョン 11.x 以降、Cisco IP 電話 8800 シリーズには ビルトイン ブリッジ（BIB）機能をデイジーチェーン接続する機能があります。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）]**>**[サービス パラメータ（Service Parameters）]** の順に選択し、[**組み込みブリッジの有効化（Built In Bridge Enable**）] クラスタ全体サービス パラメータを [**オン（On**）] に設定します。

（注） このパラメータが **[オフ（Off）]** に設定されている場合は、**[電話の設定（Phone Configuration）]** ウィンドウの **[組み込みブリッジ（Built in Bridge）]** フィールドを設定することにより、各電話機の割り込みを設定してください。

ステップ 2 **[パーティ参加トーン（Party Entrance Tone）]** クラスタ全体サービス パラメータを **[True]**（トーンに対する要件）に設定するか、**[電話番号の設定（Directory Number Configuration）]** ウィンドウの **[パーティ参加トーン（Party Entrance Tone）]** フィールドを設定します。

ステップ 3 [**ワンボタン割り込み/C 割り込みポリシー（Single Button Barge/CBarge Policy**）] を [**割り込み（Barge**）] に設定します。

（注） このパラメータが **[オフ（Off）]** に設定されている場合は、**[電話の設定（Phone Configuration）]** ウィンドウの **[ワンボタン割り込み（Single Button Barge）]** フィールドを設定することにより、各電話機のワンボタン割り込み機能を設定してください。

ステップ 4 [**呼び出し時の割り込みを許可（Allow Barge When Ringing**）] サービス パラメータを **[はい（True**）] に設定します。

ステップ 5 **[保存（Save）]** をクリックします。

共有会議の割り込みの設定

シスコは割り込みを設定しているユーザに対して共有会議の割り込み（C割り込み）を設定しないことをお勧めします。 各ユーザに対して 1 つの割り込みメソッドを選択します。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）]**>**[サービス パラメータ（Service Parameters）]** の順に選択し、[**組み込みブリッジの有効化（Built In Bridge Enable**）] クラスタ全体サービス パラメータを [**オン（On**）] に設定します。

（注） このパラメータが **[オフ（Off）]** に設定されている場合は、**[電話の設定（Phone Configuration）]** ウィンドウの **[組み込みブリッジ（Built in Bridge）]** フィールドを設定することにより、各電話機の C 割り込みを設定してください。

ステップ 2 **[パーティ参加トーン（Party Entrance Tone）]** クラスタ全体サービス パラメータを **[True]**（トーンに対する要件）に設定するか、**[電話番号の設定（Directory Number Configuration）]** ウィンドウの **[パーティ参加トーン（Party Entrance Tone）]** フィールドを設定します。

ステップ 3 [ワンボタン割り込み機能/C 割り込みポリシー（Single Button Barge/CBarge Policy）]に [C 割り込み（cBarge）]を設定します。

（注） このパラメータを **[Off]** に設定する場合、**[電話の設定（Phone Configuration）]** ウィンドウの **[ワンボタン C 割り込み（Single Button cBarge）]** フィールドを設定することで、電話ごとのワンボタン C 割り込みを設定します。

ステップ 4 [呼び出し時の割り込みを許可（Allow Barge When Ringing）]サービス パラメータを [はい（True）] に設定します。

ステップ 5 **[保存（Save）]** をクリックします。

ユーザとデバイスの関連付け

始める前に

次のいずれかまたは両方を実行します。

- 組み込み会議の割り込みの設定 （654 ページ）
- 共有会議の割り込みの設定 （655 ページ）

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 [ユーザを次の条件で検索（Find Users Where）]フィールドで適切なフィルタを指定した後、[検索（Find）]をクリックしてユーザのリストを取得します。

ステップ 3 ユーザを一覧から選択します。
[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 [デバイス情報（Device Information）]セクションを探します。

ステップ 5 [デバイスの割り当て（Device Association）]をクリックします。
[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 6 適切な CTI リモート デバイスを探して選択します。

ステップ 7 関連付けを完了するには、[選択/変更の保存（Save Selected/Changes）]をクリックします。

ステップ 8 **[関連リンク（Related Links）]** ドロップダウン リストから **[ユーザの設定に戻る（Back to User）]** を選択し、**[検索（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。

割り込みの連携動作

機能	データのやり取り
C 割り込み	[割り込み（Barge）] ソフトキーと [C 割り込み（cBarge）] ソフトキーのどちらかをソフトキー テンプレートに割り当てることをお勧めします。 各デバイスにこれらのソフトキーのどちらかだけを設定することにより、ユーザの混乱を防ぎ、潜在的なパフォーマンスの問題を避けることができます。 （注） デバイスに対してワンボタン割り込み機能またはワンボタン C 割り込み機能を有効にすることはできますが、両方を有効にすることはできません。

機能	データのやり取り
コール パーク	着信側がコールをパークすると、割り込み発信者が解放される（組み込みブリッジを使用している場合）か、割り込み発信者と他の通話相手が接続されたままになります（共有会議を使用している場合）。
参加（Join）	着信側が別のコールを使用してコールに参加すると、割り込み発信者が解放される（組み込みブリッジを使用している場合）か、割り込み発信者と他の通話相手が接続されたままになります（共有会議を使用している場合）。
PLAR（プライベート回線自動リングダウン）	割り込み、C割り込み、ワンボタン割り込み機能の発信者は、割り込みとプライベート回線自動リングダウン（PLAR）用に設定された共有回線経由でコールに割り込むことができます。 割り込み着信側がコール中にPLAR回線に関連付けられた事前に設定された番号を使用している場合は、発信者がそのコールに割り込むことができます。 Cisco Unified Communications Manager は、割り込みコールを接続する前に PLAR 回線に割り込み呼び出しを送信しないため、PLAR 接続先の状態に関係なく割り込みが発生します。 割り込み、C割り込み、ワンボタン割り込み機能をPLARと一緒に使用するには、割り込み、C割り込み、ワンボタン割り込み機能を設定する必要があります。 加えて、PLAR 接続先、つまり、PLAR 専用に使用される電話番号を設定する必要があります。

割り込みの制限

制約事項	説明
追加の発信者	割り込み発信側が別の通話相手を会議に参加させることはできません。
コンピュータテレフォニーインテグレーション（CTI）	CTI は TAPI と JTAPI アプリケーションが起動する API によって割り込みをサポートしていません。 CTI は [割り込み（Barge）] または [C割り込み（cBarge）] ソフトキーを使用して IP Phone から手動で呼び出される割り込みのイベントを生成します。
G.711 コーデック	元のコールにはG.711 コーデックが必要です。 G.711 を使用できない場合、代わりにC 割り込みを使用します。
Cisco Unified IP 電話	[割り込み（Barge）] ソフトキーを含むソフトキー テンプレートをソフトキーを使用するすべてのIP Phoneに割り当てることができます。ただし、一部のIP Phoneでは割り込み機能をサポートしていません。

制約事項	説明
暗号化（Encryption）	Cisco Unified IP 電話 7960 および 7940 に暗号化を設定する場合、暗号化されたコールに参加している間、それらの暗号化されたデバイスは割り込みリクエストを受け付けることができません。 コールが暗号化されていると、割り込みの試行は失敗します。 電話機では、割り込みが失敗したことを示すトーンが再生されます。
コールの最大数	会議の共有回線のユーザ数が割り込みを試行しているデバイスの[コール最大数（Maximum Number of Calls）] 設定と同じか大きい場合、電話機にメッセージ [エラー：過去の制限（Error: Past Limit）] が表示されます。

割り込みのトラブルシューティング

使用可能な会議ブリッジがない

[割り込み（Barge）] ソフトキーを押すと、IP Phone に「使用可能な会議ブリッジがありません（No Conference Bridge Available）」というメッセージが表示されます。

[電話の設定（Phone Configuration）] ウィンドウの **[ビルトイン ブリッジ（Built In Bridge）]** フィールドで対象の電話機が正しく設定されていません。

問題を解決するには、次の手順を実行します。

1. Cisco Unified CM の管理から、**[デバイス（Device）]** > **[電話（Phone）]** を選択して [電話の検索（Find the phone）]をクリックし、問題がある電話機の電話機設定を見つけます。
2. [ビルトイン ブリッジ（Built In Bridge）]フィールドを [オン（On）]に設定します。
3. **[更新(Update)]** をクリックします。
4. 電話機をリセットします。

[エラー：過去の制限（Error: Past Limit）]

電話に、メッセージ [エラー：過去の制限（Error: Past Limit）] が表示されます。

会議の共有回線のユーザ数が割り込みを試行しているデバイスの [コール最大数（Maximum Number of Calls）] フィールドと同じか大きい。

- [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウに移動して、[クラスタ全体のパラメータ（機能 - 会議）（Clusterwide Parameters (Feature - Conference)）] を探します。 必要に応じて、[最大アドホック会議（Maximum Ad Hoc Conference）] パラメータの値を増加させます。
- 割り込みを試行しているデバイスの共有回線の [コール最大数（Maximum Number of Calls）] の値を確認して、必要に応じて値を増加させます。

第 41 章

BLF プレゼンス

BLF プレゼンスの概要

他のユーザの電話番号上でのリアルアイム ステータスまたはUniform Resource Identifier（URI）の Session Initiation Protocol（SIP） を、ウォッチャであるユーザがウォッチャのデバイスからモニタするには、話中ランプ フィールド（BLF）機能を使用します。

ユーザのステータスまたはBLFプレゼンスエンティティ（プレゼンティティとも呼ばれます）をウォッチャがモニタできるようにするには、次のオプションを使用します。

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

既存エントリの BLF ステータスがコール リストとディレクトリに表示されます。 BLF と短縮ダイヤル ボタンを設定すると、BLF プレゼンス エンティティがウォッチャのデバイス上に短縮ダイヤルとして表示されます。

ウォッチャが Cisco Unified Communications Manager に BLF プレゼンス リクエストを送信すると、BLF プレゼンス エンティティのステータスを表示できます。 管理者が BLF プレゼンス機能を設定すると、ウォッチャのデバイスにリアルタイム ステータス アイコンが現れ、BLF プレゼンスエンティティが電話上にあるか、電話上にないか、ステータス不明か、などが表示されます。

エクステンションモビリティ ユーザは、エクステンションモビリティ サポートを使用すると電話の BLF プレゼンス機能を利用できます。

BLF プレゼンス グループの認証により、認証されたウォッチャのみが接続先の BLF プレゼンスステータスにアクセスできるようになります。 BLF または短縮ダイヤルの設定がある場合

にウォッチャが接続先をモニタできるように管理者が認証するため、BLF プレゼンス グループの認証は BLF または短縮ダイヤルには適用されません。

BLF プレゼンスの前提条件

- BLF プレゼンス機能で使用する電話を設定します。
- BLF プレゼンス機能で使用する SIP トランクを設定します。

BLF プレゼンスの設定タスク フロー

始める前に

- BLF プレゼンスの前提条件 （660 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	話中ランプ フィールド（BLF）のクラスタ全体のエンタープライズ パラメータを設定し、同期します。 BLF のクラスタ全体のエンタープライズ パラメータの設定および同期 （662 ページ）を参照してください。	同一クラスタに存在するすべてのデバイスとサービスに適用される BLF オプションを設定します。 エンタープライズ パラメータの設定変更は、最も干渉の少ない方法で、設定されたデバイスと同期できます。 たとえば、影響を受けるデバイスでのリセットや再起動が不要です。
ステップ 2	BLF のクラスタ全体のサービス パラメータを設定します。 BLF のクラスタ全体のサービス パラメータの設定 （663 ページ）を参照してください。	Cisco Unified Communications Manager の管理で選択されたサーバ上でさまざまなサービスを設定するためにプレゼンス サービス パラメータを設定します。
ステップ 3	BLF プレゼンス グループを設定します。 BLF プレゼンス グループの設定 （663 ページ）を参照してください。	BLF プレゼンス グループを、監視者がモニタする接続先を制御できるように設定します。
ステップ 4	BLF プレゼンス グループをデバイスおよびユーザと関連付けるには、次のサブタスクを実行します。 • BLF プレゼンス グループと電話を関連付けます。 BLF プレゼンス グループと電話の関連付け （666 ページ）を参照してください。	電話番号、SIP トランク、SIP を実行する電話、SCCP を実行する電話、アプリケーション ユーザ（プレゼンス要求を SIP トランク経由で送信するアプリケーション ユーザの場合）、またはエンド ユーザに BLF プレゼンス グループを適用します。

	コマンドまたはアクション	目的
	• SIP トランクと BLF プレゼンス グループを関連付けます。 SIP トランクと BLF プレゼンス グループの関連付け（667ページ）を参照してください。 • BLF プレゼンス グループとエンドユーザを関連付けます。 BLF プレゼンス グループとエンド ユーザの関連付け（668ページ）を参照してください。 • BLF プレゼンス グループとアプリケーションユーザを関連付けます。 BLF プレゼンス グループとアプリケーションユーザの関連付け（669ページ）を参照してください。	
ステップ 5	外部トランクとアプリケーションからの BLF プレゼンス要求を承認します。 外部トランクとアプリケーションからの BLF プレゼンス要求の承認（670 ページ）を参照してください。	トランク レベルの認証に加えて、SIP トランクのアプリケーションにアプリケーション レベルの認証を有効にします。
ステップ 6	コーリング サーチ スペースを設定します。 プレゼンス要求のコーリング サーチ スペースの設定（671ページ）を参照してください。	SUBSCRIBE コーリング サーチ スペースを SIP トランク、電話、またはエンドユーザに適用します。 SUBSCRIBE コーリング サーチ スペースは、Cisco Unified Communications Manager がトランクまたは電話から来るプレゼンス要求をどのようにルーティングするかを決定します。 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するパーティションが決定されます。 プレゼンス要求に異なるコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースは、デフォルト オプションである [**なし（None）**] を選択します。
ステップ 7	BLF/短縮ダイヤル ボタンの電話ボタン テンプレートを設定します。 BLF/短縮	電話機またはユーザ デバイス プロファイル向けに BLF と短縮ダイヤル ボタンの電話ボタン テンプレートを設定します。

	コマンドまたはアクション	目的
	ダイヤル ボタンの電話ボタン テンプレートの設定（672 ページ）を参照してください。	（注） テンプレートが BLF と短縮ダイヤルをサポートしない場合、[未指定の関連付けられた項目（Unassigned Associated Items）] ペインに [**BLF SD の新規追加（Add a new BLF SD）**] リンクが表示されます。
ステップ 8	ボタン テンプレートをデバイスに関連付けます。 ボタン テンプレートとデバイスの関連付け（673 ページ）を参照してください。	BLF プレゼンス向けに設定したデバイスと一緒にボタン テンプレートを使用します。
ステップ 9	ユーザ デバイス プロファイルを設定します。 ユーザ デバイス プロファイルの設定（674 ページ）を参照してください。	BLF プレゼンス向けにユーザ デバイス プロファイルを設定します。

BLF のクラスタ全体のエンタープライズ パラメータの設定および同期

エンタープライズパラメータは、同一クラスタに存在するすべてのデバイスやサービスに適用されるデフォルトを設定するために使用します。クラスタは、同じデータベースを共有する一連の Cisco Unified Communications Manager で構成されています。 Cisco Unified Communications Managerの新規インストール時には、エンタープライズパラメータを使用して、デバイスのデフォルトの初期値が設定されます。

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 [エンタープライズパラメータ設定（Enterprise Parameters 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、オンライン ヘルプを参照してください。

ヒント エンタープライズ パラメータについての詳細は、パラメータ名または [エンタープライズ パラメータの設定（Enterprise Parameters Configuration）]ウィンドウに表示される疑問符をクリックします。

ステップ 3 **[保存]** をクリックします。

ステップ 4 （任意） **[設定の適用（Apply Config）]** をクリックして、クラスタ全体のパラメータを同期します。

[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 5 **OK**をクリックします。

BLF のクラスタ全体のサービス パラメータの設定

BLF に関して [**サービス パラメータ設定（Service Parameter Configuration**）] ウィンドウで使用可能な 1 つまたは複数のサービスを設定できます。

始める前に

BLF のクラスタ全体のエンタープライズ パラメータの設定および同期 （662 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。**[システム（System）] > [サービス パラメータ（Service Parameters）]**。

ステップ 2 [**サーバ（Serve**）] 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 [**サービスパラメータ設定（Service Parameter 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、オンライン ヘルプを参照してください。

ヒント サービス パラメータの詳細については、[**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パラメータ名または疑問符をクリックしてください。

ステップ 4 **[保存]** をクリックします。

（注） [デフォルトのプレゼンス間グループ登録（Default Inter-Presence Group Subscription）] パラメータは BLF およびスピード ダイヤルには適用されません。

BLF プレゼンス グループの設定

BLF プレゼンス グループを使用して、モニタできる接続先を制御できます。 BLF プレゼンス グループを設定するには、Cisco Unified Communications Manager Administration にグループを作成し、1 つ以上の接続先と監視者を割り当てます。

新しい BLF プレゼンス グループを追加すると、Unified Communications Manager は初期権限フィールドとしてデフォルト クラスタ フィールドに新しいグループのすべてのグループ関係を定義します。別々のアクセス許可を適用するには、変更する各権限を持つ新しいグループと既存のグループに新しい権限を設定します。

（注） システムは同じ BLF プレゼンス グループ内で BLF プレゼンス要求を常に許可にします。

プレゼンス エンティティのステータスを表示するには、監視者はプレゼンス要求を Unified Communications Manager に送信します。 システムでは、監視者は、プレゼンス エンティティのステータス要求を開始するために、次の要件で承認されている必要があります。

- 監視者の BLF プレゼンス グループは、クラスタの内部または外部に関わらず、プレゼンス エンティティ プレゼンス グループのステータスを得るために承認されている必要があります。
- Unified CM は、外部プレゼンス サーバやアプリケーションからの BLF プレゼンス要求を受信するために承認されている必要があります。

始める前に

BLF のクラスタ全体のサービス パラメータの設定 （663 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。**[システム（System）] > [BLF プレゼンス グループ（BLF Presence Group）]**。

ステップ 2 [BLFプレゼンスグループの設定（BLF Presence Group Configuration）]ウィンドウの各フィールドを設定します。 フィールドとその設定オプションの詳細については、BLF の BLF プレゼンス グループ フィールド （665 ページ）を参照してください。

（注） Cisco CallManager サービスの [デフォルトのプレゼンス グループ間サブスクリプション（Default Inter-Presence Group Subscription）] サービス パラメータを使用します。 サブスクリプションの許可または拒否をする BLF プレゼンス グループのクラスタ全体のアクセス許可パラメータを設定します。 このフィールドは、システム デフォルトの設定、およびクラスタにデフォルト フィールドを使用して、BLF プレゼンス グループ関係を設定できます。

ステップ 3 **[保存]** をクリックします。

（注） BLFプレゼンス グループに設定する権限は、[BLFプレゼンス グループ関係（BLF Presence Group Relationship）]ペインに表示されます。 グループツーグループ関係のシステムデフォルト権限フィールドを使用するアクセス許可は表示されません。

次のタスク

次のサブタスクを実行して、BLF プレゼンス グループをデバイスおよびユーザと関連付けます。

• BLF プレゼンス グループと電話の関連付け （666 ページ）
• SIP トランクと BLF プレゼンス グループの関連付け （667 ページ）
• BLF プレゼンス グループとエンド ユーザの関連付け （668 ページ）
• BLF プレゼンス グループとアプリケーション ユーザの関連付け （669 ページ）

BLF の BLF プレゼンス グループ フィールド

プレゼンス認証は、BLF プレゼンス グループと連携して動作します。 BLF プレゼンス グループ設定フィールドを次の表に示します。

フィールド	説明
名前	設定する BLF プレゼンス グループの名前を入力します。 たとえば Executive_Group などです。
説明	設定する BLF プレゼンス グループの説明を入力します。
[他のプレゼンスグループへの関係を変更(Modify Relationship to Other Presence Groups)]	1 つ以上の BLF プレゼンス グループを選択し、指定したグループの許可フィールドを選択したグループに設定します。
[登録許可(Subscription Permission)]	選択されている BLF プレゼンス グループに対し、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。 • [システムデフォルトの使用（Use System Default）]：許可フィールドに、クラスタ全体のサービス パラメータ フィールド [デフォルトのプレゼンス間グループ登録（Default Inter-Presence Group Subscription）]（[登録の許可（Allow Subscription）] または [登録の拒否（ Disallow Subscription）]）を設定します。 • [登録の許可（Allow Subscription）]：指定されたグループのメンバーが、選択されているグループのメンバーのリアルタイム ステータスを確認できるようにします。 • [登録の拒否（Disallow Subscription）]：指定されたグループのメンバーが、選択されているグループのメンバーのリアルタイム ステータスを確認できないようにします。 [**保存（Save）**] をクリックすると、設定する許可が [BLF プレゼンス グループ（BLF Presence Group）] 関係ペインに表示されます。 システムのデフォルト許可フィールドを使用するグループはすべて表示されません。

デバイスとユーザとの BLF プレゼンス グループの関連付け

次の手順を実行して、電話、SIP トランク、SIP を実行する電話、SCCP を実行する電話、電話番号、アプリケーション ユーザ（プレゼンス要求を SIP トランク経由で送信するアプリケーション ユーザの場合）、およびエンド ユーザに BLF プレゼンス グループを適用します。

（注） 同じ BLF プレゼンス グループ内のメンバー間のプレゼンス要求はシステムで許可されます。

BLF プレゼンス グループと電話の関連付け

電話とトランクにプレゼンス要求を送受信する権限がある場合、電話とトランクの BLF プレゼンスを使用できます。

Cisco Unified Communications Manager はクラスタの内部または外部の Cisco Unified Communications Manager ユーザの BLF プレゼンス要求を処理します。 BLF プレゼンス要求を電話を介して送信する Cisco Unified Communications Manager ウォッチャについては、電話と BLF プレゼンス エンティティがコロケーションを行う場合、Cisco Unified Communications Manager は BLF プレゼンス ステータスで応答します。

始める前に

BLF プレゼンス グループの設定 （663 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[デバイス（Device）] > [電話（Phone）]** を選択して **[新規追加（Add New）]** を選択します。
[新規電話を追加（Add a New Phone）]ウィンドウが表示されます。

ステップ 2 [電話のタイプ（Phone Type）] ドロップダウン リストから、BLF プレゼンス グループを関連付ける電話のタイプを選択します。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 [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） [**SUBSCRIBE コーリング サーチ スペース（SUBSCRIBE Calling Search Space**）] ドロップダウン リストから、電話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 で設定された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 ボックスに表示されます。 ドロップダウン リストから、エンド ユーザに別のコーリング サーチ スペースを選択しない場合、このフィールドの値によってデフォルト値が [None] に設定されます。この目的で明示的に SUBSCRIBE コーリング サーチ スペースを設定するには、すべてのコーリング サーチ スペースを設定する場合と同じようにコーリング サーチ スペースを設定します。

ステップ 5 **[保存]** をクリックします。

次のタスク

次のサブタスクを実行して、BLF プレゼンス グループをデバイスおよびユーザと関連付けます。

- SIP トランクと BLF プレゼンス グループの関連付け （667 ページ）
- BLF プレゼンス グループとエンド ユーザの関連付け （668 ページ）
- BLF プレゼンス グループとアプリケーション ユーザの関連付け （669 ページ）

SIP トランクと BLF プレゼンス グループの関連付け

ダイジェスト認証が SIP トランクで設定されていない場合、トランクが着信サブスクリプションを受け入れるようにトランクを設定できますが、アプリケーション レベルの認証は開始できません。また、Unified CM はグループ認証を実行する前に、すべての着信要求を受け入れます。 ダイジェスト認証をアプリケーション レベルの認証と共に使用すると、Unified CM は BLF プレゼンス要求を送信しているアプリケーションのクレデンシャルの認証も行います。

クラスタの外部にあるデバイスに対する BLF プレゼンス要求が存在する場合、Unified Communications Manager は SIP トランクを介して外部デバイスに照会します。 ウォッチャに外部デバイスをモニタする権限がある場合、SIP トランクは外部デバイスに BLF プレゼンス要求を送信し、BLF プレゼンス ステータスをウォッチャに返します。

ヒント SIP トランクで BLF プレゼンス グループ認証を着信プレゼンス要求と共に使用するには、トランクのプレゼンス グループ（たとえば、External_Presence_Serv_Group1）を設定して、適切な権限をクラスタ内部のその他のグループに設定します。

SIP トランクのプレゼンス要求の両方のレベルの認証を設定する場合、SIP トランクの BLF プレゼンス グループが使用されるのは、BLF プレゼンス グループがアプリケーションの着信要求で特定されない場合のみです。

始める前に

BLF プレゼンス グループの設定 （663 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）] > [トランク（Trunk）]** を選択し、**[新規追加（Add New）]**をクリックします。

ステップ 2 [トランク タイプ（Trunk Type）] ドロップダウン リストから、BLF プレゼンス グループを関連付ける電話のタイプを選択します。
[デバイス プロトコル（Device Protocol）] ドロップダウン リストの値が自動的に入力されます。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 [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。

（注） Unified CM システムによる SIP トランクからの着信 BLF プレゼンス要求の受け入れを承認するには、[SIP トランク セキュリティ プロファイルの設定（SIP Trunk Security Profile Configuration）] ウィンドウの **[プレゼンスのサブスクリプションの許可（Accept Presence Subscription）]** チェックボックスをオンにします。 SIP トランクで着信プレゼンス要求をブロックするには、このチェックボックスをオフにします。 SIP トランクの BLF プレゼンス要求を許可すると、Unified CM はトランクに接続する SIP ユーザ エージェント（SIP プロキシ サーバまたは外部 BLF プレゼンス サーバ）からの要求を承認します。 Unified CM が SIP トランクからの BLF プレゼンス要求を承認するように設定する場合、ダイジェスト認証をオプションと見なします。

ステップ 5 **[保存]** をクリックします。

次のタスク

次のサブタスクを実行して、BLF プレゼンス グループをデバイスおよびユーザと関連付けます。

- BLF プレゼンス グループと電話の関連付け （666 ページ）
- BLF プレゼンス グループとエンド ユーザの関連付け （668 ページ）
- BLF プレゼンス グループとアプリケーション ユーザの関連付け （669 ページ）

BLF プレゼンス グループとエンド ユーザの関連付け

管理者は、エクステンションモビリティを設定するために BLF プレゼンス グループとユーザ ディレクトリおよびコール リストのエンド ユーザを関連付けます。

始める前に

BLF プレゼンス グループの設定 （663 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[ユーザ管理（User Management）]** > **[エンド ユーザ（End User）]** を選択して [新規追加（Add New）] 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 2 [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]** をクリックします。

次のタスク

次のサブタスクを実行して、BLF プレゼンス グループをデバイスおよびユーザと関連付けます。

- BLF プレゼンス グループと電話の関連付け （666 ページ）
- SIP トランクと BLF プレゼンス グループの関連付け （667 ページ）
- BLF プレゼンス グループとアプリケーション ユーザの関連付け （669 ページ）

BLF プレゼンス グループとアプリケーション ユーザの関連付け

管理者は BLF プレゼンス グループと外部アプリケーションのアプリケーション ユーザを関連付けます。 これらの外部アプリケーションは、SIP トランクまたは SIP トランク上で接続されているプロキシ サーバ上のホームである BLF プレゼンス要求を送信します。 たとえば、Web ダイヤル、Meeting Place、会議サーバ、およびプレゼンス サーバです。

始める前に

BLF プレゼンス グループの設定 （663 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[ユーザ管理（User Management）]** > **[アプリケーション ユーザ（Application User）]** を選択して [新規追加] 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 2 [アプリケーション ユーザの設定（Application User 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 3 **[保存]** をクリックします。

次のタスク

次のサブタスクを実行して、BLF プレゼンス グループをデバイスおよびユーザと関連付けます。

- BLF プレゼンス グループと電話の関連付け （666 ページ）
- SIP トランクと BLF プレゼンス グループの関連付け （667 ページ）
- BLF プレゼンス グループとエンド ユーザの関連付け （668 ページ）

外部トランクとアプリケーションからの BLF プレゼンス要求の承認

クラスタ外部からのBLFプレゼンス要求を承認するには、外部トランクまたはアプリケーションの BLF プレゼンス要求を承認するようにシステムを設定します。 クラスタ外部のトランクおよびアプリケーションに BLF プレゼンス グループを割り当てて、BLF プレゼンス グループ認証を呼び出すことができます。

始める前に

次のサブタスクを実行して、BLF プレゼンス グループをデバイスおよびユーザと関連付けます。

- BLF プレゼンス グループと電話の関連付け （666 ページ）
- SIP トランクと BLF プレゼンス グループの関連付け （667 ページ）
- BLF プレゼンス グループとエンド ユーザの関連付け （668 ページ）
- BLF プレゼンス グループとアプリケーション ユーザの関連付け （669 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）]** > **[トランク（Trunk）]** を選択し、**[新規追加（Add New）]**をクリックします。 **[トランクの設定（Trunk Configuration）]** ウィンドウが表示されます。

ステップ 2 SIP トランクから BLF プレゼンス要求を可能にするには、[SIP トランクセキュリティプロファイルの設定（SIP Trunk Security Profile Configuration）] ウィンドウの [プレゼンスの SUBSCRIBE の許可（Accept Presence Subscription）] チェックボックスをオンにします。

ステップ 3 トランク レベルの認証に加えて SIP トランク アプリケーションのアプリケーション レベルの認証を有効にするには、[SIP トランク セキュリティ プロファイルの設定（SIP Trunk Security Profile Configuration）] ウィンドウで次のチェックボックスをオンにします。

- **[ダイジェスト認証を有効化（Enable Digest Authentication）]**
- **[アプリケーションレベル認証を有効化（Enable Application Level Authorization）]**

（注） **[ダイジェスト認証を有効化（Enable Digest Authentication）]** をオンにしないと、**[アプリケーションレベル認証を有効化（Enable Application Level Authorization）]** をオンにすることはできません。

ステップ 4 トランクにプロファイルを適用します。 トランクへの変更が有効になるように、[リセット（Reset）] をクリックします。

（注） **[アプリケーションレベル認証を有効化（Enable Application Level Authorization）]** をオンにする場合、アプリケーションの**[アプリケーションユーザの設定（Application User Configuration）]** ウィンドウの **[プレゼンスの SUBSCRIBE の許可（Accept Presence Subscription）]** チェックボックスをオンにします。

プレゼンス要求のコーリング サーチ スペースの設定

[SUBSCRIBE コーリング サーチ スペース（SUBSCRIBE Calling Search space）] オプションを使用すると、BLF プレゼンス要求のコール処理コーリング サーチ スペースとは別にコーリング サーチ スペースを適用できます。 プレゼンス要求用に別のコーリング サーチ スペースを選択します。選択しない場合は、SUBSCRIBE コーリング サーチ スペースによってデフォルト オプションの[なし（None）]が選択されます。 エンドユーザに関連付けられている SUBSCRIBE コーリング サーチ スペースがエクステンションモビリティ コールに使用されます。

SUBSCRIBE コーリング サーチ スペースは SIP トランク、電話機、またはエンドユーザに適用してください。 エンドユーザに関連付けられている SUBSCRIBE コーリング サーチ スペースがエクステンションモビリティ コールに使用されます。

始める前に

外部トランクとアプリケーションからの BLF プレゼンス要求の承認 （670 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 > コントロールのクラス > コーリングサーチスペース**。

ステップ 2 [コーリングサーチスペースの設定（Calling Search Space configuration）]ウィンドウで、[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からコーリング サーチ スペースを選択します。

ステップ 3 [新規追加] をクリックします。

ステップ 4 [名前（Name）]フィールドに、名前を入力します。

ステップ 5 （任意）[説明（Description）]フィールドに、コーリング サーチ スペースを識別するための説明を入力します。

ステップ 6 [使用可能なパーティション（Available Partitions）]リストから、1 つまたは複数のパーティションを選択し、矢印キーをクリックします。
選択したパーティションは [選択済みのパーティション（Selected Partitions）]リストに表示されます。

ステップ 7 （任意）**[選択済みのパーティション（Selected Partitions）]** リストにパーティションを追加または削除するには、リストボックスの横にある矢印キーをクリックします。

ステップ 8 **[保存]** をクリックします。

Cisco Unified Communications Manager Administration で設定したすべてのコーリング サーチ スペースは、**[トランクの設定（Trunk Configuration）]** ウィンドウまたは **[電話機の設定（Phone Configuration）]** ウィンドウの **[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。

BLF/短縮ダイヤル ボタンの電話ボタン テンプレートの設定

電話機またはユーザのデバイス プロファイルの BLF と短縮ダイヤル ボタンを設定できます。電話機またはデバイス プロファイルにテンプレートを適用（電話機またはデバイス プロファイルの設定を保存）すると、Cisco Unified Communications の [関連情報（Association Information）] ペインに BLF SD の新規追加へのリンクが表示されます。

（注） テンプレートが BLF と短縮ダイヤルをサポートしない場合、**[未指定の関連付けられた項目（Unassigned Associated Items）]** ペインに [BLF SD の新規追加（Add a new BLF SD）] リンクが表示されます。

管理者が SIP URI の BLF と短縮ダイヤル ボタンを追加または変更する際には、ウォッチャが接続先のモニタに許可されていることを確認してください。システムが SIP トランクを使用して SIP URI BLF のターゲットに到達するようにするには、BLF プレゼンス グループが SIP トランクの適用と関連付けられている必要があります。

（注） BLF と短縮ダイヤルの BLF プレゼンス グループまたはデフォルト内部 プレゼンス グループ サブスクリプションのパラメータを設定する必要はありません。

始める前に

プレゼンス要求のコーリング サーチ スペースの設定 （671 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）]** > **[電話ボタンテンプレート（Phone button template）]** の順に選択します。

ステップ 2 [新規追加（Add New）]ボタンをクリックします。
[電話ボタン テンプレートの設定（Phone Button Template Configuration）] ウィンドウが表示されます。

ステップ 3 [ボタン テンプレート名（Button Template Name）]フィールドに、テンプレートの名前を入力します。

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から、電話ボタンのテンプレートを選択します。

ステップ 5 選択されたボタンテンプレートのレイアウトから新しいボタンテンプレートを作成するには、**[コピー（Copy）]** をクリックします。

ステップ 6 **[保存（Save）]** をクリックします。

ボタン テンプレートとデバイスの関連付け

電話機またはユーザ デバイス プロファイルに対して BLF および短縮ダイヤル ボタンを設定します。 BLF 値は、クラスタ上にある必要はありません。 電話機に表示される話中ランプ フィールド（BLF）ステータス アイコンについては、ご使用の電話機をサポートする Cisco Unified IP 電話 のドキュメンテーションを参照してください。 電話で BLF プレゼンスがサポートされているかどうかを確認するには、ご使用の電話とこのバージョンの Unified Communications Manager に対応する Cisco Unified IP 電話 のマニュアルを参照してください。

始める前に

BLF/短縮ダイヤル ボタンの電話ボタン テンプレートの設定 （672 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）]** > **[デバイス設定（Device Settings）]** > **[デバイス プロファイル（Device Profile）]**。

ステップ 2 設定済みの電話ボタンテンプレートを検索するには、検索パラメータを入力し、**[検索（Find）]** をクリックします。
すべての検索条件に一致するレコードが表示されます。

ステップ 3 レコードのいずれかをクリックします。
[デバイス プロファイルの設定（Device Profile Configuration）] ウィンドウが表示されます。

ステップ 4 [電話ボタン テンプレート（**Phone Button Template**）] で、設定済み電話ボタン テンプレートを選択します。

ステップ 5 （任意） 設定されたデバイスの値を変更します。

ステップ 6 **[保存（Save）]** をクリックします。

ユーザ デバイス プロファイルの設定

詳細については、BLF プレゼンスの連携動作 （675 ページ）の「「BLF Presence with Extension Mobility（エクステンションモビリティによる BLF プレゼンス）」」の項を参照してください。

始める前に

ボタン テンプレートとデバイスの関連付け （673 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[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 [新規追加] をクリックします。
[**デバイス プロファイルの設定（Device Profile Configuration**）] ウィンドウが表示されます。

ステップ 3 [デバイス プロファイルの設定（Device Profile 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） 電話機またはデバイス プロファイルに適用した電話ボタン テンプレートが BLF およびスピードダイヤルをサポートしていない場合、このリンクは [割り当て情報（Association Information）]ペインに表示されず、[割り当てられていない関連項目（Unassigned Associated Items）]ペインに表示されます。

ステップ 4 **[保存（Save）]** をクリックします。

BLF プレゼンスの連携動作

機能	データのやり取り
H.323 電話デバイスがプレゼンス エンティティとして動作する場合の H.323 電話の DN のプレゼンス BLF	H.323 電話の状態が [RING IN] の場合、BLF ステータスは [ビジー（Busy）] として報告されます。 SCCP または SIP のいずれかを実行しており、状態が [RING IN] の電話のプレゼンス エンティティの場合、BLF ステータスは [アイドル（Idle）] として報告されます。
H.323 電話デバイスがプレゼンス エンティティとして動作する場合の H.323 電話の DN のプレゼンス BLF	イーサネット ケーブルが電話から抜かれているなどの何らかの理由で H.323 電話が Cisco Unified Communications Manager に接続されていない場合、BLF ステータスは常に [アイドル（Idle）] として報告されます。 SCCP または SIP のいずれかを実行しており、Cisco Unified Communications Manager に接続していない電話のプレゼンス エンティティの場合、BLF ステータスが [不明（Unknown）] として報告されます。
エクステンション モビリティでの BLF プレゼンス	[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] でユーザ デバイス プロファイルの [BLF] ボタンと [短縮ダイヤル（SpeedDial）] ボタンを設定している場合、Cisco Extension Mobility をサポートしている電話にログインすると、この電話の [BLF] ボタンと [短縮ダイヤル（SpeedDial）] ボタンに BLF プレゼンス ステータスが表示されます。 エクステンション モビリティ ユーザがログアウトすると、Cisco Extension Mobility をサポートしている電話に、設定したログアウト プロファイルの [BLF] ボタンと [短縮ダイヤル（SpeedDial）] ボタンに BLF プレゼンス ステータスが表示されます。

BLF プレゼンスの制約事項

制約事項	説明
SIP プレゼンス	Cisco Unified Communications Manager Assistant SIP プレゼンスをサポートしていません。
BLF プレゼンス要求	Cisco Unified Communications Manager Administration ハント パイロットに関連付けられている電話番号への BLF プレゼンス要求を拒否します。
コールのリスト機能の BLF	Cisco Unified IP Phone 7940 と Cisco Unified IP Phone 7960 では、コール リスト BLF 機能はサポートされていません。

制約事項	説明
BLF と短縮ダイヤル	BLF と短縮ダイヤルの設定時、管理者はウォッチャに接続先のモニタが許可されていることを確認します。 BLF プレゼンス グループの認証は BLF および短縮ダイヤルには適用されません。 （注） SIP を実行している電話では、BLF プレゼンス グループの認証は、コール リストに表示される短縮ダイヤルおよび BLF として設定されている SIP URI または電話番号にも適用されません。 異なるパーティションに同じ内線番号がある、重複する DN がある場合は、デバイスに割り当てられている SUBSCRIBE CSS 内で設定されたパーティションの順序に基づいてプレゼンス通知が選択されます。 たとえば、2つの BLF 短縮ダイヤルが電話機に設定されているとします。 • 「内部」パーティションの拡張 1234 • 「外部」パーティションの拡張 1234 SUBSCRIBE CSS 内で最初にリストされているパーティションは、登録されたデバイスに BLF プレゼンスを提供するものです。
BLF プレゼンス承認	複数回線に接続している Cisco Unified IP 電話 は、不在履歴と発信履歴の回線電話番号に関連付けられているキャッシュされた情報を使用して、BLF プレゼンス承認を判別します。 この通話情報がない場合、電話はプライマリ回線を BLF プレゼンス承認のサブスクライバとして使用します。 複数回線が接続する Cisco Unified IP 電話 の [BLF] ボタンと [短縮ダイヤル（SpeedDial）] ボタンの場合、使用可能な最初の回線がサブスクライバとして使用されます。
Cisco Unified IP 電話	SIP を実行している Cisco Unified IP 電話 7960 および 7940 に設定されている電話番号をユーザがモニタするときには、プレゼンス エンティティがオフフックである（ただしコール接続状態ではない）場合、ウォッチャ デバイスに「not on the phone」のステータス アイコンが表示されます。 これらの電話はオフフック ステータスを検出しません。その他のすべての電話タイプでは、プレゼンス エンティティでオフフック状態の場合、ウォッチャ デバイスに「on the phone」ステータス アイコンが表示されます。
SIP トランク	BLF プレゼンス要求と応答は、SIP トランク、または SIP トランクに関連付けられているルートにルーティングされる必要があります。 MGCP および H323 トランク デバイスにルーティングされる BLF プレゼンス要求は拒否されます。

制約事項	説明
SIP を実行している BLF プレゼンス対応電話	SIP を実行している BLF プレゼンス対応電話では、電話番号または SIP URI を [BLF] ボタンまたは [短縮ダイヤル（SpeedDial）] ボタンに設定できます。 SCCP を実行している BLF プレゼンス対応電話では、電話番号だけを [BLF] ボタンおよび [短縮ダイヤル（SpeedDial）] ボタンに設定できます。
SIP を実行している電話	SIP を実行している電話では、BLF プレゼンス グループの認証は、コール リストに表示される短縮ダイヤルおよび BLF として設定されている SIP URI または電話番号にも適用されません。

第 42 章

コール表示の制限

コール表示制限の概要

Cisco Unified Communications Manager には、発信側ユーザと接続側ユーザの両方の番号と名前の情報の表示を許可または制限する柔軟な設定オプションがあります。 接続側の番号と名前は、それぞれ個別に制限できます。

接続側の番号と名前の制限は、SIP トランク レベルまたはコール単位で設定できます。 SIP トランク レベルでの設定は、コール単位の設定をオーバーライドします。

たとえばホテル環境では、客室とフロントデスクの間で行われたコールの情報を表示する必要がある場合があります。 一方、客室間のコールについては、いずれの電話に表示される通話情報も制限できます。

コール表示制限の設定タスク フロー

始める前に

- コール表示制限の連携動作 （691 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	電話機能一覧の生成 （5 ページ）	コール表示制限機能をサポートするエンドポイントを特定するためにレポートを生成します。

	コマンドまたはアクション	目的
ステップ 2	コール表示制限のパーティションの設定（680 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。 たとえば、ホテル環境では、ルーム同士でダイヤルするためのパーティションや、公衆電話交換網（PSTN）にダイヤルするためのパーティションを設定できます。
ステップ 3	コール表示制限のコーリング サーチ スペースの設定 （682 ページ）.	コーリング サーチ スペースを設定し、発信側デバイスがコールを終了しようとする際に検索できるパーティションを指定します。 ルームやフロントデスク、ホテルのその他の内線番号、PSTN、およびルームのパーク範囲（コール パークの場合）に対してコーリング サーチ スペースを作成します。
ステップ 4	接続先番号表示制限のサービス パラメータの設定 （683 ページ）.	接続側の回線 ID をダイヤル番号としてのみ表示するサービス パラメータを設定します。
ステップ 5	トランスレーション パターンの設定（684 ページ）.	異なるレベルの表示制限のトランスレーション パターンを設定します。
ステップ 6	電話機のコール表示制限の設定 （686 ページ）	エンドポイントと、コール表示制限に使用するパーティションおよびコーリング サーチ スペースを関連付けます。
ステップ 7	コール表示制限の PSTN ゲートウェイの設定 （688 ページ）	PSTN ゲートウェイと、コール表示制限に使用するパーティションおよびコーリング サーチ スペースを関連付けます。
ステップ 8	これはオプションです。 SIP トランクでのコール表示制限の設定 （688 ページ）	この手順を使用して、SIP トランク レベルで接続側の番号と名前の制限を設定できます。 SIP トランク レベルの設定は、コール単位の設定を上書きします。

コール表示制限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** > **コントロールのクラス** > **パーティション**。

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。

説明にはどの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサイド（&）、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 *49 :* 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

コール表示制限のコーリング サーチ スペースの設定

コーリング サーチ スペースを設定し、発信側デバイスがコールを終了しようとする際に検索できるパーティションを指定します。ルームやフロントデスク、ホテルのその他の内線番号、PSTN、およびルームのパーク範囲（コールパークの場合）に対してコーリング サーチ スペースを作成します。

始める前に

コール表示制限のパーティションの設定 （680 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** > **コントロールのクラス** > **コーリングサーチスペース**。

ステップ 2 [新規追加] 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、どの言語でも最大 50 文字まで指定できますが、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、**コントロール（Ctrl）**キーを押したまま、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。

接続先番号表示制限のサービス パラメータの設定

接続先番号表示制限は、接続先の回線 ID の表示をダイヤルした番号のみに制限します。 このオプションにより、顧客のプライバシーに関する問題と、電話機のユーザに不要な接続先番号が表示されるという問題が解消されます。

始める前に

コール表示制限のコーリング サーチ スペースの設定 （682 ページ）

手順

ステップ 1 [Cisco Unified 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）]**。

ステップ 2 Cisco CallManager サービスが実行されているサーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [元の着信番号を常に表示（Always Display Original Dialed Number）]サービスのパラメータを[True]に設定してこの機能を有効にします。

デフォルト値は **[False]** です。

ステップ 4 （任意）[トランスレーション時の元の着信番号の名前の表示（Name Display for Original Dialed Number When Translated）]サービスのパラメータを設定します。

デフォルトのフィールドには、トランスレーション前の元の着信番号の呼び出し表示が示されています。 このパラメータを変更して、トランスレーション後の着信番号の呼び出し表示を示すことができます。 このパラメータは、[元の番号を常に表示（Always Display Original Number）]サービスのパラメータが [False]に設定されている場合は、適用されません。

ステップ 5 **[保存（Save）]** をクリックします。

トランスレーション パターンの設定

Unified Communications Manager トランスレーション パターンを使用して、発信をルーティングする前に着信番号を操作します。場合によってシステムは、ダイヤルされた番号を使用しないことがあります。 また、公衆電話交換網（PSTN）が、ダイヤルされた番号を認識できない場合もあります。 コール表示制限機能では、さまざまなトランスレーション パターンを通じてコールがルーティングされた後に、コールが実際のデバイスに接続されます。

始める前に

接続先番号表示制限のサービス パラメータの設定 （683 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）] > [トランスレーション パターン（Translation Pattern）]**。

ステップ 2 [トランスレーション パターンの設定（Translation 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、コール表示制限のトランスレーション パターンのフィールド （684 ページ）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。

コール表示制限のトランスレーション パターンのフィールド

フィールド	説明
[トランスレーションパターン（Translation Pattern）]	数字とワイルドカードを含む、トランスレーション パターンを入力します。 スペースは使用しないでください。 たとえば、NANP では、通常のローカル アクセスの場合は 9.@ を、通常のプライベート ネットワーク番号計画の場合は 8XXX を入力します。 大文字の A、B、C、D、および \+ を指定できます。\+ は、国際的なエスケープ文字 + を表します。
説明	トランスレーション パターン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。

フィールド	説明
[パーティション（Partition）]	ドロップダウン リストから、このトランスレーションパターンに関連付けるパーティションを選択します。
[コーリングサーチスペース(Calling Search Space)]	ドロップダウン リストから、このトランスレーション パターンに関連付けるコーリング サーチスペースを選択します。
[発信側回線 ID の表示（Calling Line ID Presentation）]	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。 • **[デフォルト（Default）]**：発信側回線 ID の表現を変更しない場合は、このオプションを選択します。 • [許可（Allowed）]：発信側電話番号を表示する場合は、このオプションを選択します。 • **[制限あり（Restricted）]**：Cisco Unified Communications Manager で発信側電話番号の表示をブロックする場合は、このオプションを選択します。
発信者名の表示（Calling Name Presentation）	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。 • [デフォルト（Default）]：発信者名の表現を変更しない場合は、このオプションを選択します。 • [許可（Allowed）]：発信側の名前を表示する場合は、このオプションを選択します。 • **[制限あり（Restricted）]**：Cisco Unified Communications Manager で発信者名の表示をブロックする場合は、このオプションを選択します。
接続側回線 ID の表示（Connected Line ID Presentation）	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。 • [デフォルト（Default）]：接続側回線 ID の表現を変更しない場合は、このオプションを選択します。 • [許可（Allowed）]：接続側電話番号を表示する場合は、このオプションを選択します。 • **[制限あり（Restricted）]**：Cisco Unified Communications Manager で接続側電話番号の表示をブロックする場合は、このオプションを選択します。

フィールド	説明
接続先名の表示（Connected Name Presentation）	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。 • [デフォルト（Default）]：接続先名の表現を変更しない場合は、このオプションを選択します。 • [許可（Allowed）]：接続側の名前を表示する場合は、このオプションを選択します。 • [制限あり（Restricted）]：CiscoUnified Communications Manager で接続側名の表示をブロックする場合は、このオプションを選択します。

電話機のコール表示制限の設定

この手順を使用して、コール表示制限に使用するコーリング サーチ スペースやパーティションを電話機に関連付けます。

始める前に

トランスレーション パターンの設定 （684 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 次のいずれかの作業を実行します。

a) 既存の電話機についてのフィールドを変更するには、検索条件を入力し、検索結果の一覧から電話機を選択します。 [電話の設定（Phone Configuration）]ウィンドウが表示されます。

b) 新しい電話機を追加するには、[新規追加] をクリックします。

[新規電話を追加（Add a New Phone）]ウィンドウが表示されます。

ステップ 3 [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、着信番号のルーティング方法を決定する際に、システムが使用するコーリング サーチ スペースを選択します。

ステップ 4 [表示インジケータを無視（内線コールのみ）（Ignore presentation indicators （internal calls only））]チェック ボックスをオンにして、内線コールの表示制限を無視します。

ステップ 5 **[保存]** をクリックします。
電話機がデータベースに追加されます。

ステップ 6 追加した電話機を電話番号に関連付けるには、**[デバイス（Device）]**>**[電話（Phone）]** を選択し、追加した電話機を検索するための検索パラメータを入力します。

ステップ 7 [電話の検索と一覧表示（Find and List Phones）]ウィンドウで、電話機の名前をクリックします。
[電話の設定（Phone Configuration）]ウィンドウが表示されます。

ステップ 8 [関連付け（Association）]ペインから、電話機の名前をクリックして電話番号を追加または変更します。
[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 9 [電話番号の設定（Directory Number Configuration）]ウィンドウの[電話番号（Directory Number）]テキスト ボックスで、電話番号の値を追加または変更し、[ルート パーティション（Route Partition）]ドロップダウン リストの値を選択します。

ステップ 10 **[保存]** をクリックします。

電話設定の例

電話機 A（Room-1）をパーティション P_Room とデバイス/回線コーリング サーチ スペース CSS_FromRoom で設定

{ P_Phones, CSS_FromRoom} : 221/Room-1

電話機 B（Room-2）をパーティション P_Room とデバイス/回線コーリング サーチ スペース CSS_FromRoom で設定

{ P_Phones, CSS_FromRoom} : 222/Room-2

電話機 C（Front Desk-1）をパーティション P_FrontDesk とデバイス/回線コーリング サーチ スペース

CSS_FromFrontDesk を使用し、[表示インジケータを無視（Ignore Presentation Indicators）]チェックボックスをオンにして設定

{ P_FrontDesk, CSS_FromFrontDesk, IgnorePresentationIndicators set} : 100/Reception

電話機 D（Front Desk-2）をパーティション P_FrontDesk とデバイス/回線コーリング サーチ スペース

CSS_FromFrontDesk を使用し、[表示インジケータを無視（Ignore Presentation Indicators）]チェックボックスをオンにして設定

{ P_FrontDesk, CSS_FromFrontDesk, IgnorePresentationIndicators set} : 200/Reception

電話機 E（Club）をパーティション P_Club とデバイス/回線コーリング サーチ スペース CSS_FromClub で設定

{ P_Club, CSS_FromClub) : 300/Club

コール表示制限の PSTN ゲートウェイの設定

PSTNゲートウェイと、コール表示制限に使用するパーティションおよびコーリングサーチスペースを関連付けます。

始める前に

電話機のコール表示制限の設定 （686 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（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 検索条件を入力し、結果のリストから PSTN ゲートウェイを選択します。
[**ゲートウェイの設定（Gateway Configuration**）] ウィンドウが表示されます。

ステップ 3 [**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、PSTN からの着信コールのルーティング方法を決定する際に、システムが使用するコーリング サーチ スペースを選択します。

ステップ 4 [**保存（Save**）] と [**リセット（Reset**）] をクリックして設定の変更を適用します。

ステップ 5 （オプション）使用可能なトランクまたはゲートウェイを関連づけるには、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[**SIP ルート パターン（SIP Route Pattern**）] を選択し、[**SIP トランク/ルートリスト（SIP Trunk/Route List**）] ドロップダウン リストから SIP トランクまたはルートを選択します。

ゲートウェイ設定の例

ルート パターン P_PSTN とコーリング サーチ スペース CSS_FromPSTN を使用して PSTN ゲートウェイ E を設定します。

{CSS_FromPSTN}, RoutePattern {P_PSTN}

SIP トランクでのコール表示制限の設定

SIP トランク レベルで接続側の番号と名前の制限を設定できます。 SIP トランク レベルの設定は、コール単位の設定を上書きします。

始める前に

（**オプション**） コール表示制限の PSTN ゲートウェイの設定 （688 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)] > [トランク(Trunk)]**
[トランクの検索と一覧表示（Find and List Trunks）]ウィンドウが表示されます。

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 更新するトランクの名前を選択します。

ステップ 4 [SIP トランク設定（SIP Trunk 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、コール表示制限の SIP トランクのフィールド（689 ページ）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。

コール表示制限の SIP トランクのフィールド

表 *50* : 着信コール

フィールド	説明
[発信側回線 ID の表示（Calling Line ID Presentation）]	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。 • **[デフォルト（Default）]**：発信側回線 ID の表現を変更しない場合は、このオプションを選択します。 • [許可（Allowed）]：発信側電話番号を表示する場合は、このオプションを選択します。 • **[制限あり（Restricted）]**：Cisco Unified Communications Manager で発信側電話番号の表示をブロックする場合は、このオプションを選択します。

フィールド	説明
発信者名の表示（Calling Name Presentation）	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。 • [デフォルト（Default）]：発信者名の表現を変更しない場合は、このオプションを選択します。 • [許可（Allowed）]：発信側の名前を表示する場合は、このオプションを選択します。 • **[制限あり（Restricted）]**：Cisco Unified Communications Manager で発信者名の表示をブロックする場合は、このオプションを選択します。
[コーリングサーチスペース(Calling Search Space)]	ドロップダウン リストから、このトランスレーション パターンに関連付けるコーリング サーチスペースを選択します。

表 *51 :* 発信コール

フィールド	説明
接続側回線 ID の表示（Connected Line ID Presentation）	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。 • [デフォルト（Default）]：接続側回線 ID の表現を変更しない場合は、このオプションを選択します。 • [許可（Allowed）]：接続側電話番号を表示する場合は、このオプションを選択します。 • **[制限あり（Restricted）]**：Cisco Unified Communications Manager で接続側電話番号の表示をブロックする場合は、このオプションを選択します。

フィールド	説明
接続先名の表示（Connected Name Presentation）	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。 • [デフォルト（Default）]：接続先名の表現を変更しない場合は、このオプションを選択します。 • [許可（Allowed）]：接続側の名前を表示する場合は、このオプションを選択します。 • [制限あり（Restricted）]：CiscoUnified Communications Manager で接続側名の表示をブロックする場合は、このオプションを選択します。

コール表示制限の連携動作

ここでは、コール表示制限機能と Cisco Unified Communications Manager アプリケーションおよびコール処理機能との連携動作について説明します。

機能	データのやり取り
コール パーク	コール パークとコール表示制限機能を使用する場合には、コール表示制限機能を保持するため、個々のコール パーク番号に対して関連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 つのトランスレーション パターンでコール パーク番号の範囲をカバーするように設定することはできません。 次のようなシナリオを例として考えます。 **1.** システム管理者は、77x のコール パーク範囲を作成し、P_ParkRange という名前のパーティションに配置します。（P_ParkRange パーティションを客室の電話のコーリング サーチスペース [CSS_FromRoom] に含めることで、P_ParkRange パーティションが客室の電話に認識されます）。 **2.** 管理者はコール パーク電話番号ごとに個別のトランスレーション パターンを設定し、表示フィールドを [制限あり（Restricted）] に設定します。（このシナリオでは、管理者は 770、771、772...779 のトランスレーション パターンを作成します）。 （注） コール表示制限機能が正しく機能するためには、管理者が番号範囲（77x または 77[0-9] など）に対して 1 つのトランスレーション パターンを設定するのではなく、番号ごとに個別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。 **3.** Room-1 が Room-2 にコールを発信します。 **4.** Room-2 がコールに応答すると、Room-1 がコールをパークします。 **5.** Room-1 がコールを取得すると、Room-2 には Room-1 の通話情報は表示されません。 「コール パークの概要」を参照してください。
会議リスト	コール表示制限を使用すると、会議参加者のリストの表示情報が制限されます。 「アドホック会議の概要」を参照してください。
会議とボイスメール	コール表示制限機能を、会議やボイス メールなどの機能と共に使用すると、電話の通話情報表示にそのステータスが反映されます。 たとえば、会議機能が呼び出されると、通話情報表示に [**会議（To Conference）**] が表示されます。 [メッセージ（Messages）] ボタンを選択してボイス メールにアクセスすると、通話情報表示に [**ボイス メール（To Voicemail）**] が表示されます。

機能	データのやり取り
エクステンションモビリティ	コール表示制限機能をエクステンションモビリティと共に使用するには、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] の [電話の設定（Phone Configuration）] ウィンドウと、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] の [デバイス プロファイルの設定（Device Profile Configuration）] ウィンドウで、**[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)）]** パラメータを有効にします。 Extension Mobilityでコール表示制限機能を有効にする場合、通話情報の表示または制限は、デバイスにログインしているユーザに関連付けられている回線プロファイルに応じて異なります。（ユーザに関連付けられている）ユーザデバイスプロファイルに入力された設定は、（エクステンションモビリティが有効な電話の）電話設定に入力された設定を上書きします。
通話転送	接続番号表示制限は、このシステムから発信されるすべてのコールに適用されます。 この値を [**はい（True**）] に設定すると、このフィールドは既存の Cisco Unified Communications Manager のアプリケーション、機能、およびコール処理と連携します。 この値は、システムの内部または外部で終了するすべてのコールに適用されます。 接続番号表示が更新され、不在転送または話中転送の転送先にコールがルーティングされるか、コール転送またはCTIアプリケーションでリダイレクトされる場合、変更された番号またはリダイレクトされた番号が表示されるようになりました。

コール表示制限機能の制約事項

トランスレーション パターン：トランスレーション パターンではエントリの重複は許可されていません。

第 43 章

取り込み中

サイレントの概要

サイレント（DND）は、次のオプションを提供します。

- [コール拒否（Call Reject）]：このオプションは、着信コールが拒否されるように指定します。 [DND 着信呼警告（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。
- [呼出音オフ（Ringer Off）]：このオプションは、呼出音をオフにしますが、ユーザがコールを受け付けられるように、着信通話情報をデバイスに表示します。

DND を有効にすると、通常の優先順位の新しい着信コールすべては、デバイスの DND 設定を受け入れます。 Cisco Emergency Responder（CER）のコールや、マルチレベルの優先およびプリエンプションのコールなど、優先順位の高いコールの場合、デバイスの呼出音が鳴ります。さらに、DND を有効にすると、自動応答機能は無効になります。

ユーザは、次の方法により電話でサイレントを有効化できます。

- ソフトキー
- 機能ボタン
- Cisco Unified Communications セルフケア ポータル

（注） Cisco Unified Communications Manager から電話ごとに、この機能を有効または無効にすることもできます。

電話機の動作

サイレントを有効にすると、Cisco Unified IP Phone に「サイレントが有効になっています（Do Not Disturb is active）」というメッセージが表示されます。 一部の Cisco Unified IP Phone には、DND ステータス アイコンが表示されます。 個々の電話モデルがサイレントを使用する方法の詳細については、特定の電話モデルに関するユーザ ガイドを参照してください。

DND を有効にすると、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] の [着信呼警告（Incoming Call Alert）] で指定されているとおりに、電話への着信コール通知をユーザは受信しますが、優先順位の高いコール（Cisco Emergency Responder のコールや MLPP のコールなど）の場合を除いて電話が鳴ることはありません。 また、電話が鳴っているときに DND を有効にすると、電話は呼出音を停止します。

ステータス通知

サイレントは、SIP デバイスと Cisco Skinny Call Control Protocol（SCCP）デバイスの両方でサポートされています。

SIP 電話は、SIP PUBLISH メソッドを使用して、DND ステータスの変更を Cisco Unified Communications Manager に通知します。 Cisco Unified Communications Manager は、Remote-cc REFER 要求を使用して、DND ステータスの変更を SIP 電話に通知します。

SCCP 電話は、SCCP メッセージングを使用して、DND ステータスの変更を Cisco Unified Communications Manager に通知します。

サイレントの設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	電話機能一覧の生成 （5 ページ）	どの電話がサイレント設定をサポートしているかを確認するには、[Cisco Unified Reporting] から電話機能レポート一覧を実行します。 （注） SIP を実行する Cisco Unified IP Phone 7940 および 7960 は、サイレント機能の下位互換性を実装しており、SIP プロファイルで設定できます。
ステップ 2	話中ランプ フィールド ステータスの設定 （697 ページ）	話中ランプ フィールド のステータスのサービス パラメータを設定します。
ステップ 3	共通の電話プロファイルでのサイレントの設定 （698 ページ）	これはオプションです。 共通の電話プロファイルに対するサイレント設定ネッ

	コマンドまたはアクション	目的
		トワーク内にある電話機のグループに対してサイレント設定を適用するには、プロファイルで設定します。
ステップ 4	電話へのサイレント設定の適用 （699 ページ） .	電話にサイレント設定を適用します。
ステップ 5	ソフトキーまたは機能ボタンのどちらを使用しているかによって、次のタスクのいずれかを実行します。 • サイレント機能ボタンの設定 （700 ページ） • [サイレント] ソフトキーの設定 （702 ページ）	電話機にサイレント機能ボタンまたはソフトキーを追加します。

話中ランプ フィールド ステータスの設定

[**BLF ステータスが DND を示す（BLF Status Depects DND）**] サービス パラメータを設定することにより、BLF ステータスで着信拒否を示す方法を設定できます。 BLF ステータスを設定するには、次の手順を実行します。

始める前に

（注）
- DND のビジー ランプ フィールド(BLF)プレゼンス ステータスは、共有回線 DN に登録済みのすべてのデバイスが DND に設定されている場合にのみ機能します。
- Jabber for iOS または Jabber for Android を同じ DN 上で使用している場合、Jabber for iOS または Jabber for Android が登録されていないが設定済みである場合でも、登録と見なされます。

電話機能一覧の生成 （5 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[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 設定するサーバの [**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 - プレゼンス）（Clusterwide Parameters （System - Presence））] ペインで、[**BLF ステータスが DND を示す（BLF Status Depects DND）**] サービス パラメータに次のいずれかの値を指定します。

- **はい（True）**：デバイスでサイレントが有効になっている場合、そのデバイスまたはライン アピアランスの BLF ステータス インジケータにサイレント状態が反映されます。
- **いいえ（False）**：デバイスでサイレントが有効になっている場合、そのデバイスまたはライン アピアランスの BLF ステータス インジケータに実際のデバイス状態が反映されます。

次のタスク

次のいずれかの手順を実行します。

共通の電話プロファイルでのサイレントの設定 （698 ページ）

電話へのサイレント設定の適用 （699 ページ）

共通の電話プロファイルでのサイレントの設定

共通の電話プロファイルを使用すると、サイレントを設定し、そのプロファイルを使用するネットワーク内の電話のグループにこれらの設定を適用できます。

始める前に

話中ランプ フィールド ステータスの設定 （697 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、**[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 [**DND オプション（DND Option）**] ドロップダウン リストから、サイレント機能による着信コールの処理方法を選択します。

- **[コール拒否（Call Reject）]**：着信通話情報がユーザに表示されません。[DND着信呼警告（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。
- **[呼出音オフ（Ringer Off）]**：このオプションは、呼出音をオフにしますが、着信通話情報がデバイスに表示されるため、ユーザはコールを受け付けることができます。

（注） 携帯電話とデュアルモード電話の場合、[コール拒否（Call Reject）] オプションのみを選択できます。

ステップ 3 **[着信コール アラート（Incoming Call Alert）]** ドロップダウン リストから、サイレントがオンになっている場合に電話ユーザに着信コールを警告する方法を選択します。

- [無効（Disable）]：コールのビープ通知とフラッシュ通知は障がい者向けです。[DND 呼出音オフ（DND Ringer Off）] オプションを設定すると、着信通話情報は引き続き表示さ

れます。ただし、[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。
- [フラッシュのみ（Flash Only）]：電話は着信コールをフラッシュします。
- [ビープ音のみ（Beep Only）]：電話に着信コールのフラッシュ アラートが表示されます。

ステップ 4 **[保存（Save）]** をクリックします。

電話へのサイレント設定の適用

この手順は、Cisco Unified IP Phone でサイレント設定を適用する方法について説明します。[Cisco Unified CM の管理（Cisco Unified CM Administration）] で [電話機の設定（Phone Configuration）]ウィンドウから、DND 設定を適用できます。または、共通の電話プロファイルに DND 設定を適用して、そのプロファイルを電話機に適用できます。

始める前に

共通の電話プロファイルを使用している場合、共通の電話プロファイルでのサイレントの設定（698 ページ）を実行してください。

それ以外の場合は、話中ランプ フィールド ステータスの設定（697 ページ）を実行してください。

手順

ステップ 1 Cisco Unified CM 管理から、**[デバイス]** > **[電話機]** を選択します。

ステップ 2 [検索（Find）]をクリックして、サイレント設定を適用する電話機を選択します。

ステップ 3 共通の電話プロファイルからサイレント設定を適用するには、**[共通の電話プロファイル（Common Phone Profile）]** ドロップダウン リストから、サイレント設定を適用したプロファイルを選択します。

ステップ 4 電話機でサイレント設定を有効にする場合は、[サイレント]チェックボックスをオンにします。

ステップ 5 **[DND オプション（DND Option）]** ドロップダウン リストで、DND 機能を使用した着信コールの処理方法を次のオプションから選択します。

- **[コール拒否（Call Reject）]**：着信通話情報がユーザに表示されません。 設定に応じて、電話機からビープ音が鳴るか、フラッシュ通知が表示されます。
- **[呼出音オフ（Ringer Off）]**：ユーザがコールに応答できるよう着信通話情報がデバイスに表示されますが、呼出音は鳴りません。
- [共通プロファイル設定を使用（Use Common Profile Setting）]：このデバイスに指定された共通の電話プロファイルのサイレント設定が使用されます。

（注） SCCP を実行している 7940/7960 電話の場合、選択できるのは [呼出音オフ（Ringer Off）] オプションだけです。 携帯デバイスとデュアルモード電話の場合、[コール拒否（Call Reject）] オプションのみを選択できます。 携帯デバイスまたはデュアルモード電話で [DNDコール拒否（DND Call Reject）] をアクティブにすると、デバイスに通話情報が表示されません。

ステップ 6 **[DND 着信コール アラート（DND Incoming Call Alert）]** ドロップダウン リストで、DND がオンの場合に電話機で着信コールを表示する方法を次のオプションから選択します。

- [なし（None）]：共通の電話プロファイルの DND 着信コール アラートの設定がこのデバイスで使用されます。
- **[無効（Disable）]**：DND 呼出音オフ オプションでは、ビープ音およびフラッシュ通知の両方が無効ですが、着信通話情報は表示されます。 コール拒否オプションでは、ビープ音およびフラッシュ通知が無効になり、着信通話情報はデバイスに送られません。
- [ビープ音のみ（Beep only）]：着信コールの際、ビープ音のみ再生されます。
- [フラッシュのみ（Flash only）]：着信コールの際、フラッシュ アラートが表示されます。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

次のいずれかの手順を実行します。

サイレント機能ボタンの設定 （700 ページ）

[サイレント] ソフトキーの設定 （702 ページ）

サイレント機能ボタンの設定

Cisco Unified IP Phone にサイレント機能ボタンを追加するには、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	サイレントの電話ボタン テンプレートの設定 （700 ページ）	サイレント ボタンを含む電話ボタン テンプレートを作成します。
ステップ 2	電話機とボタン テンプレートの関連付け （314 ページ）	サイレント ボタン テンプレートを電話に関連付けます。

サイレントの電話ボタン テンプレートの設定

[サイレント] ボタンが含まれている電話ボタンテンプレートを設定するには、次の手順に従います。

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。**[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）]** の順に選択します。

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]** 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]** をクリックします。

ステップ 7 次のいずれかの作業を実行します。

- 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

サイレントの電話ボタン テンプレートの設定 （700 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]** 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。

[サイレント] ソフトキーの設定

これはオプションです。電話機でソフトキーを使用する場合、次のタスクを実行して、電話にサイレント ソフトキーを追加します。

手順

	コマンドまたはアクション	目的
ステップ 1	サイレントのソフトキー テンプレートの設定 （702 ページ）	[サイレント] ソフトキーを含むソフトキー テンプレートを作成します。
ステップ 2	次のいずれかの手順を実行します。 • 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 （703 ページ） • 電話とソフトキー テンプレートの関連付け （705 ページ）	[共通デバイス設定（Common Device Configuration）] にソフトキーを関連付けて、電話グループにその設定を関連付けるか、電話機にソフトキーテンプレートを直接関連付けることができます。

サイレントのソフトキー テンプレートの設定

[サイレント] ソフトキーを含むソフトキーテンプレートを設定するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified CM 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）]**。

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] 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]** 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]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- 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て、ソフトキー テンプレートを電話に追加します。

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 （703 ページ）

電話とソフトキー テンプレートの関連付け （705 ページ）

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

[サイレント]（DND）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ときに、DND ソフトキーを共通デバイス設定にて使用する Cisco Unified IP Phone のグループに追加できます。

始める前に

サイレントのソフトキー テンプレートの設定 （702 ページ）

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ソフトキー テンプレートの追加 （704 ページ）	共通デバイス設定に DND ソフトキーテンプレートを関連付けます。
ステップ 2	電話機と共通デバイス設定の関連付け（704 ページ）	電話に共通デバイス設定を関連付けることで、電話に DND ソフトキーを追加します。

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] 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]** 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]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 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

始める前に

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 （703 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。

電話とソフトキー テンプレートの関連付け

[サイレント] ソフトキーを含むソフトキー テンプレートを設定していて、そのソフトキー テンプレートを電話に関連付けるには、次の手順を実行します。

始める前に

サイレントのソフトキー テンプレートの設定 （702 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、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。

応答不可の連携動作と制約事項

このセクションは、サイレントの連携動作と制約事項に関する情報を提供します。

連携動作

次の表に、サイレント（DND）機能の連携動作を示します。 特に指定されていない限り、連係動作はサイレント呼び出し音オフおよびサイレントコール拒否オプションの両方に適用されます。

機能	サイレントとの連携動作
すべてのコールの転送	Cisco Unified IP 電話 では、サイレント（DND）機能がアクティブであることを示すメッセージがユーザに新しいボイス メッセージが届いていることを示すメッセージよりも優先されます。 ただし、不在転送機能がアクティブであることを通知するメッセージがDNDよりも優先されます。
パークの復帰	ローカルにパークされたコールでは、パークの復帰がサイレントよりも優先されます。 電話Aのサイレントがオンでコールがパークされた場合、電話Aへのパークの復帰が発生し、電話Aの呼び出し音が鳴ります。 リモートにパークされたコールでは、サイレントがパークの復帰よりも優先されます。 • 電話Aがサイレント着信音オフを有効化し、電話A-primeと回線を共有する場合、電話A-primeがコールをパークすると、電話Aのパークの復帰はサイレント設定に従い、呼び出し音は鳴りません。 • 電話Aがサイレントコール拒否を有効化した場合、パークの復帰は電話Aに表示されません。
ピック	ローカルで発行されたピックアップ要求の場合、ピックアップがサイレントよりも優先されます。 電話Aのサイレントがオンで、任意のタイプのピックアップを開始した場合、ピックアップ コールは通常どおり表示され、電話Aの呼び出し音が鳴ります。 リモートで発行されたピックアップ要求の場合、サイレントが次のようにピックアップよりも優先されます。 • 電話Aがサイレント着信音オフ モードで電話A-primeと回線を共有する場合、電話A-primeがピックアップを開始すると、電話Aへのピックアップ コールはサイレント設定に従い、電話Aの呼び出し音は鳴りません。 • 電話Aがサイレントコール拒否モードの場合、ピックアップ コールは電話Aに表示されません。
保留復帰とインターコム	保留復帰とインターコムはサイレントよりも優先され、コールは通常どおり表示されます。

機能	サイレントとの連携動作
MLPP と CER	マルチレベルの優先およびプリエンプション（SCCP を実行している電話）および Cisco Emergency Responder コールはサイレントよりも優先されます。 マルチレベルの優先およびプリエンプション および Cisco Emergency Responder コールは通常どおり表示され、SCCP および SIP の両方で電話呼出音がサポートされています。
コールバック	発信側ではコールバックがサイレントよりも優先されます。 有効化デバイスがサイレント モードの場合、コールバック通知（音声と表示の両方）は引き続きユーザに表示されます。 着信側では、次のようにサイレントがコールバックよりも優先されます。 • 着信側がサイレント着信音オフの場合、着信側がオフフックおよびオンフックになった後で、[コールバック使用可能（Callback Available）] 画面が送信されます。 • 着信側がサイレントコール拒否で使用可能な場合、有効化デバイスが同じクラスタ内にあれば、新しい画面が有効化デバイスに送信され、「<DirectoryNumber> は応答可能になりましたが、サイレントコール拒否状態です」と表示されます。 コールバック使用可能通知は着信側がサイレント コール拒否を無効化した後にのみ送信されます。
ピックアップ通知	サイレント着信音オフ オプションの場合、デバイスに視覚的な通知のみが表示されます。 サイレント コール拒否オプションの場合、デバイスに通知は表示されません。
ハント リスト	ハント リスト内のデバイスでサイレント着信音オフが有効化されている場合でも、コールは引き続きユーザに表示されます。 ただし、DND 着信呼警告の設定は引き続き適用される場合があります。 ハント リスト内のデバイスでサイレント コール拒否が有効化されている場合、そのハント リストへの任意のコールは次のメンバーへ移り、このデバイスには送信されません。

機能	サイレントとの連携動作
エクステンションモビリティ	エクステンションモビリティの場合、デバイス プロファイル設定に DND 着信呼警告とサイレント ステータスが含まれます。 ユーザがログインしてサイレントを有効にすると、DND着信呼警告とサイレントステータスの設定が保存され、ユーザが再度ログインするとこれらの設定が使用されます。 （注） Extension Mobility にログインしているユーザが DND 着信コール アラートまたはサイレント ステータスの設定を変更しても、このアクションは実際のデバイス設定に影響しません。

制約事項

使用中の電話機やデバイスの種類によっては、DND の使用にいくつかの制約事項が適用されます。

- SCCP を実行している次の電話機のモデルやデバイスは、DND の [呼出音オフ（Ringer Off）] オプションのみサポートしています。
  - Cisco Unified IP 電話 7940
  - Cisco Unified IP 電話 7960
  - Cisco IP Communicator

（注） SIP を実行する Cisco Unified IP 電話 7940 および 7960 は、独自のサイレント機能を実装して使用しており、これには後方互換性があります。

- 次の電話機のモデルやデバイスは、DND の [コール拒否（Call Reject）] オプションのみサポートしています。
  - モバイル デバイス（デュアル モード）
  - リモート宛先プロファイル
  - Cisco Unified Mobile Communicator

応答不可のトラブルシューティング

ここでは、Cisco Unified IP 電話（SCCP および SIP）向けのトラブルシューティング情報を提供します。

SIP 電話の場合、次の情報を使用してトラブルシューティングを行います。

- デバッグ：sip-dnd、sip-messages、dnd-settings
- 表示：config、dnd-settings
- スニファ トレース

SCCP 電話の場合、次の情報を使用してトラブルシューティングを行います。

- デバッグ：jvm all info
- スニファ トレース

トラブルシューティングのエラー

次の表に、サイレントのエラーをトラブルシューティングする方法について説明します。

症状	アクション
DND ソフトキーが表示されません。 または DND 機能ボタンが表示されません。	• この電話のソフトキーまたはボタン テンプレートが DND に含まれていることを確認します。 • スニファ トレースをキャプチャし、電話に正しいソフトキーまたはボタン テンプレートが設定されていることを確認します。 • 電話ファームウェアのバージョンが 8.3(1) 以降であることを確認します。
BLF 短縮ダイヤルには DND ステータスは表示されません。	• BLF DND がエンタープライズ パラメータで有効に設定されていることを確認します。 • スニファ トレースをキャプチャし、電話に正しい通知メッセージが設定されていることを確認します。 • 電話ファームウェアのバージョンが 8.3(1) 以降であることを確認します。
DND の変更はモニタ デバイスには反映されません。	• BOT/TCT デバイスが、DND の状態が **[オフ（OFF）]** に設定された、共有回線デバイスであるかを確認します。 ステータスが **ON** に設定されている 場合、他の共有回線の DND ステータスへの変更は反映されません。 • 監視対象の回線の DND ステータスの変更を反映するために、BOT/TCT デバイスの DND ステータスが [**オフ（OFF**）] に設定されていることを確認します。

第 44 章

[プライバシー（Privacy）]

プライバシーの概要

プライバシー機能により、1 つの回線（DN）を共有する電話のユーザがコール ステータスを確認し、コールに割り込むことができるかどうかを決定できます。プライバシー機能は、電話別またはすべての電話に対して有効化または無効化できます。デフォルトでは、クラスタ内のすべての電話でプライバシーが有効になります。

プライバシーが設定されたデバイスが Cisco Unified Communications Manager に登録されると、プライバシーが設定されている電話の機能ボタンにラベルが表示され、アイコンによってステータスが表示されます。 ボタンにランプがついている場合、ランプが点灯します。

電話が着信コールを受信すると、ユーザは[プライバシー（Privacy）]機能ボタンを押してそのコールをプライベートにします。これにより、通話情報が共有電話に表示されなくなります。[プライバシー（Privacy）] 機能ボタンにより [オン（On）] と [オフ（Off）] が切り替わります。

ご使用の Cisco Unified IP Phone でプライバシー機能がサポートされているかどうかを確認するには、ご使用の電話モデルのユーザ マニュアルを参照してください。

プライバシー保留中

プライバシー保留中 機能により、同じ回線（DN）を共有する電話を使用するユーザの、コール ステータスの確認および保留中のコールの取得機能を有効化または無効化できます。

プライバシー保留中機能は、特定の電話またはすべての電話に対して有効化または無効化できます。 プライバシー保留中 機能が有効な場合、すべてのプライベート コールでこの機能が自動的にアクティブになります。 デフォルトでは、クラスタ内のすべての電話で プライバシー保留中 機能が無効になります。

プライバシー保留中機能をアクティブにするには、プライベート コールの間に[**保留（Hold）**]ソフトキーまたは[**保留（Hold）**]ボタンを押します。 コールに戻るには、[**復帰（Resume）**]ソフトキーを押します。 コールを保留にしている電話には保留中のコールのステータス インジケータが表示され、共有回線には保留中のプライベート コールのステータス インジケータが表示されます。

プライバシーの設定タスク 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 （5 ページ）	プライバシー機能をサポートするデバイスを特定するためにレポートを生成します。
ステップ 2	クラスタ全体のプライバシーの有効化（712 ページ）	クラスタ内のすべての電話のプライバシーをデフォルトで有効にします。
ステップ 3	デバイスのプライバシーの有効化 （713 ページ）	特定のデバイスのプライバシーを有効にします。
ステップ 4	プライバシー電話ボタン テンプレートの設定 （713 ページ）	デバイスのプライバシー電話ボタン テンプレートを設定します。
ステップ 5	電話とプライバシー電話ボタン テンプレートの関連付け （714 ページ）	ユーザに電話ボタン テンプレートを関連付けます。
ステップ 6	共有ライン アピアランスの設定 （715 ページ）	共有ラインアピアランスを設定します。
ステップ 7	（任意） プライバシー保留中 の設定（715 ページ）	プライバシー保留中 を設定します。

クラスタ全体のプライバシーの有効化

クラスタ全体のプライバシーをデフォルトで有効にするには、次の手順を実行します。

手順

ステップ 1 Cisco Unified CM の管理から、**[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（Server）]ドロップダウン リストで、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 [プライバシー設定（Privacy Setting）]ドロップダウン リストから [はい（True）]を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

デバイスのプライバシーの有効化

始める前に

電話機のモデルがプライバシーをサポートす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 （5 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。**[デバイス（Device）]** > **[電話（Phone）]**。

ステップ 2 検索情報を指定し、[検索（Find）] をクリックします。
電話機の検索結果が表示されます。

ステップ 3 電話機を選択します。

ステップ 4 [プライバシー（Privacy）]ドロップダウン リストから [デフォルト（Default）]を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

プライバシー電話ボタン テンプレートの設定

始める前に

デバイスのプライバシーの有効化 （713 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）]** > **[電話ボタンテンプレート（Phone button template）]** の順に選択します。

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]** 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]** をクリックします。

ステップ 7 次のいずれかの作業を実行します。

- 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。

電話とプライバシー電話ボタン テンプレートの関連付け

始める前に

プライバシー電話ボタン テンプレートの設定 （713 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]** 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。

共有ライン アピアランスの設定

始める前に

電話とプライバシー電話ボタン テンプレートの関連付け （714 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）]**。
[**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 特定の電話機を検索するには、検索条件を入力して [**検索（Find**）] をクリックします。
検索基準に一致する電話機のリストが表示されます。

ステップ 3 共有ライン アピアランスを設定する電話機を選択します。
[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）]** ウィンドウの左側の [割り当て情報（Association Information）] 領域で、**[新規 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 5 [**電話番号（Directory Number**）] を入力して、電話番号が属する [**ルート パーティション（Route Partition**）] を選択します。

ステップ 6 [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、オンラインヘルプを参照してください。

ステップ 7 共有ライン アピアランスを作成するすべての電話機でステップ 3 （715 ページ） からステップ 6 （715 ページ） を繰り返します。

（注） 共有ラインアピアランスの一部であるすべての電話機に、同じ電話番号およびルート パーティションが割り当てられていることを確認します。

プライバシー保留中 の設定

手順

ステップ 1 Cisco Unified CM の管理から、**[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（Server）] ドロップダウン リストで、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 [保留中のコールにプライバシー設定を強制適用する（Enforce Privacy Setting on Held Calls）] サービス パラメータを [True]に設定します。

ステップ 5 **[保存（Save）]** をクリックします。

プライバシーの制限

制約事項	説明
[CTI]	• CTI は TAPI や JTAPI アプリケーションが起動する API を介したプライバシーはサポートしていません。 [プライバシー（Privacy）] 機能ボタンを使用して IP フォンでプライバシーが有効または無効になったときに、CTIはイベントを生成します。 • CTI は TAPI や JTAPI アプリケーションが起動する API を介した保留中のプライバシーはサポートしていません。 プライバシーが有効になっているコールが保留中になり、IP フォンで [プライバシー（Privacy）] 機能ボタンを使用して保留中のコールのプライバシーが有効または無効になったときに、CTI はイベントを生成します。

第 45 章

プライベート回線自動リングダウン

プライベート回線自動リングダウン の概要

プライベート回線自動リングダウン（PLAR）機能は、ユーザがオフフック状態（または[新規コール（NewCall）]ソフトキーまたは回線キーが押された場合）になると、すぐに電話機が事前に設定された番号にダイヤルするように電話機を設定します。 ユーザは PLAR を設定された電話回線で他の番号をダイヤルすることはできません。

PLARは、割り込み、C割り込み、ワンボタン割り込み機能のような機能にも対応しています。PLAR とそのような機能を使用する場合、機能のドキュメンテーションで説明されているように機能を設定し、PLAR の接続先を設定する必要があります。これは、PLAR 専用で使用される電話番号です。

SCCP 電話での プライベート回線自動リングダウン の設定タスク フロー

SCCP 電話で プライベート回線自動リングダウン（PLAR）を設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	パーティションの作成 （718 ページ）	PLAR の接続先のパーティションを作成します。 このパーティションに割り当

	コマンドまたはアクション	目的
		てられる唯一の電話番号は、PLAR の接続先です。
ステップ 2	コーリング サーチ スペースへのパーティションの割り当て （718 ページ）	このパーティションを一意の CSS、および PLAR の接続先デバイスを含む CSS に割り当てます。
ステップ 3	プライベート回線自動リングダウン 接続先へのパーティションの割り当て （719 ページ）	PLAR の接続先電話番号に NULL パーティションと CSS を割り当てます。
ステップ 4	電話機での プライベート回線自動リングダウン のトランスレーション パターンの設定 （720 ページ）	NULL のトランスレーション パターンを作成し、それを PLAR の接続先電話番号に割り当てます。

パーティションの作成

プライベート回線自動リングダウン（PLAR）の接続先の新しいパーティションを作成します。この機能を有効にするため、PLAR に設定し、このパーティションに割り当てられるのは、ヌルのトランスレーション パターンのみです。

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** > **コントロールのクラス** > **パーティション**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [名前（Name）]フィールドに、パーティション名と説明をカンマで区切って入力します。

ステップ 4 **[保存（Save）]** をクリックします。

コーリング サーチ スペースへのパーティションの割り当て

SCCP 電話の プライベート回線自動リングダウン（PLAR）については、次の 2 つのコーリング サーチ スペース（CSS）を設定する必要があります。

- 最初の CSS には、ヌルのトランスレーション パターンの新しいパーティションと接続先の電話にルーティングするパーティションを含める必要があります。
- 2 番目の CSS には、ヌルのトランスレーション パターンの新しいパーティションのみ含める必要があります。

始める前に

パーティションの作成 （718 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）]** > **[コールサーチスペース（Calling Search Space）]**）。

ステップ 2 **[検索（Find）]** をクリックして、PLAR 接続先デバイスのコーリング サーチ スペースを選択します。

ステップ 3 矢印を使用して、ヌルのトランスレーション パターン向けに作成された新しいパーティションと接続先デバイスにルーティングするパーティションの両方を **[選択されたパーティション（Selected Partitions）]** リスト ボックスに移動します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 [新規追加] をクリックします。

ステップ 6 コーリング サーチ スペースの名前と説明を入力します。

ステップ 7 矢印を使用して、新しいパーティションを **[選択されたパーティション（Selected Partitions）]** リスト ボックスに移動します。

ステップ 8 **[保存（Save）]** をクリックします。

プライベート回線自動リングダウン接続先へのパーティションの割り当て

SCCP 電話機でプライベート回線自動リングダウン（PLAR）を設定するには、ヌルのパーティションを PLAR 接続先として使用する電話番号に割り当てます。

（注） PLAR 接続先の電話番号にはそれぞれ一意のパーティションが必要です。ヌルのパーティションには PLAR 接続先として作成した電話番号以外の電話番号を追加しないでください。

始める前に

コーリング サーチ スペースへのパーティションの割り当て （718 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[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 [検索（**Find**）] をクリックして、PLAR 接続先として使用する電話番号を選択します。

ステップ 3 [ルート パーティション（**Route Partition**）] フィールドで、PLAR 接続先用に作成したパーティションを選択します。

ステップ 4 [コーリング サーチ スペース（**Calling Search Space**）] ドロップダウン リストで、ヌルのパーティションおよび宛先デバイスの両方を含む CSS を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

電話機での プライベート回線自動リングダウン のトランスレーション パターンの設定

電話機で プライベート回線自動リングダウン（PLAR）を設定するには、ヌルのトランスレーション パターンを設定し、そのトランスレーション パターンに PLAR 接続先番号を割り当てます。

始める前に

プライベート回線自動リングダウン 接続先へのパーティションの割り当て （719 ページ）

手順

ステップ 1 Cisco Unified CM 管理で、**[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 [新規追加（Add New）] をクリックして、新しいトランスレーション パターンを作成します。

ステップ 3 **[トランスレーション パターン（Translation Pattern）]** フィールドを空にしておきます。

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、ヌルのトランスレーション パターン用に作成した新しいパーティションを選択します。

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、新しいパーティションと PLAR 接続先デバイスのパーティションの両方を含むコーリング サーチ スペースを選択します。

ステップ 6 [着信側トランスフォーメーション マスク（**Called Party Transformation Mask**）] フィールドで、PLAR 接続先電話番号を入力します。

ステップ 7 **[保存（Save）]** をクリックします。

SIP 電話での プライベート回線自動リングダウン の設定タスク フロー

SIP 電話の プライベート回線自動リングダウン（PLAR）を設定するには、これら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	プライベート回線自動リングダウン の SIP ダイヤル ルールの作成 （721 ページ）	PLAR 向けの SIP ダイヤル ルールを作成します。
ステップ 2	SIP 電話への プライベート回線自動リングダウン ダイヤル ルールの割り当て （722 ページ）	電話機に PLAR のダイヤル ルールを割り当てます。

プライベート回線自動リングダウン の SIP ダイヤル ルールの作成

SIP 電話の プライベート回線自動リングダウン（PLAR）を設定するには、PLAR の接続先番号の SIP ダイヤル ルールを設定する必要があります。

始める前に

パーティションの作成 （718 ページ）

コーリング サーチ スペースへのパーティションの割り当て （718 ページ）

プライベート回線自動リングダウン 接続先へのパーティションの割り当て （719 ページ）

電話機での プライベート回線自動リングダウン のトランスレーション パターンの設定 （720 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（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）] > [SIP ダイヤル ルール（SIP Dial Rules）]** 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 **[ダイヤル パターン（Dial Pattern）]** ドロップダウン リストから、**[7940_7960_その他（7940_7960_OTHER）]** 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 ダイヤル ルールの名前と説明を入力します。

ステップ 6 [次へ（Next）]をクリックします。

ステップ 7 [**パターン（Pattern）**] フィールドに、PLAR の接続先番号に一致するパターンを入力して、[**PLAR を追加（Add PLAR）**] をクリックします。

ステップ 8 **[保存（Save）]** をクリックします。

SIP 電話への プライベート回線自動リングダウン ダイヤル ルールの割り当て

PLAR 対応 SIP ダイヤルルールを電話機に割り当てることにより、SIP 電話機で プライベート回線自動リングダウン（PLAR）を設定できます。

始める前に

プライベート回線自動リングダウン の SIP ダイヤル ルールの作成 （721 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[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、PLAR を設定する電話機を選択します。

ステップ 3 **[SIP ダイヤル ルール（SIP Dial Rules）]** ドロップダウン リストから、PLAR 用に作成したダイヤル ルールを選択します。

ステップ 4 **[保存（Save）]** をクリックします。

プライベート回線自動リングダウン のトラブルシューティング

SCCP 電話での プライベート回線自動リングダウン トラブルシューティング

症状	ソリューション
電話がオフフックになり、ユーザにはファスト ビジー（リオーダー）音が聞こえる。	PLAR のトランスレーション パターンに割り当てられている CSS に PLAR 接続先のパーティションが含まれていることを確認します。

症状	ソリューション
電話がオフフックになり、ダイヤル トーンが聞こえる。	電話に割り当てられた CSS にヌルの PLAR トランスレーション パターンのパーティションが含まれていることを確認します。

SIP 電話での プライベート回線自動リングダウン トラブルシューティング

症状	ソリューション
電話がオフフックになり、ユーザにはファスト ビジー（リオーダー）音が聞こえる。	SIP 電話の CSS が PLAR 接続先に到達できることを確認します。
電話がオフフックになり、ダイヤル トーンが聞こえる。	SIP ダイヤル ルールが電話で作成され、その電話に割り当てられていることを確認します。

第 46 章

セキュア トーン

セキュア トーンの概要

セキュア トーン機能では、暗号化されているコールの場合にセキュア通知トーンを再生するように電話を設定できます。 このトーンは、コールが保護されており、機密情報が交換可能であることを示します。 2 秒間のトーンでは、長いビープ音が 3 回鳴ります。 コールが保護されている場合、着信側が応答するとすぐに保護対象の電話でトーンの再生が始まります。

コールが保護されていない場合、システムは、保護対象の電話で非セキュア通知トーンを再生します。非セキュア通知トーンでは、短いビープ音が 6 回鳴ります。

（注） 保護対象の電話機の発信者にのみ、セキュア通知トーンと非セキュア通知トーンが聞こえます。 保護されていない電話機の発信者には、これらのトーンは聞こえません。

セキュア通知トーンと非セキュア通知トーンに対応しているコールのタイプを次に示します。

- クラスタ間の IP-to-IP コール
- クラスタ間の保護されたコール
- 保護された MGCP E1 PRI ゲートウェイ経由の IP と時分割多重化（TDM）コール

ビデオ コールの場合、システムにより保護対象デバイスでセキュア通知トーンと非セキュア通知トーンが再生されます。

（注） ビデオ コールの場合、ユーザには、最初にコールの音声部分に対するセキュア通知トーンが聞こえ、次に非セキュア メディア全体に対する非セキュア通知トーンが聞こえます。

Cisco Unified IP Phone に表示されるロック アイコンは、メディアが暗号化されていることを示しますが、その電話が保護対象デバイスとして設定されていることを意味するわけではありません。 ただし、保護された発信にはロック アイコンが表示されている必要があります。

保護対象デバイスのゲートウェイ

Cisco Unified Communications Manager では、サポートされている Cisco Unified IP 電話 と MGCP E1 PRI ゲートウェイだけを保護対象デバイスとして設定できます。

Cisco Unified Communications Manager は、システムがコールの保護ステータスを判別すると、セキュア通知トーンと非セキュア通知トーンを再生するように MGCP Cisco IOS ゲートウェイに指示することもできます。

保護対象デバイスでは次の機能が提供されます。

- SCCP または SIP を実行する電話機を保護対象デバイスとして設定できます。
- 保護対象デバイスは接続先が暗号化されていてもいなくても、保護されていないデバイスに発信できます。 このような場合、コールは保護されていないものとして指定され、システムはコールに関係している電話機で非セキュア通知トーンを再生します。
- 保護されている電話機が保護されている他の電話機に発信し、メディアが暗号化されていない場合、システムはコールに関係している電話機で非セキュア通知トーンを再生します。

セキュア トーンの前提条件

- SRTP 暗号化の MGCP ゲートウェイを設定する必要があります。 以下のコマンドでゲートウェイを設定します。**mgcp package-capability srtp-package**。
- MGCP ゲートウェイでは、[高度な IP サービス（Advanced IP Services）] または [高度な企業サービス（Advanced Enterprise Services）] イメージ（たとえば c3745-adventerprisek9-mz.124-6.T.bin）を指定する必要があります。

セキュア トーン設定のタスク フロー

始める前に

- セキュア トーンの前提条件 （726 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	電話機能一覧の生成 （5 ページ）	セキュア トーン機能をサポートするデバイスを特定するためにレポートを生成します。
ステップ 2	電話機の保護デバイスとしての設定 （727 ページ）	電話機を保護デバイスとして設定します。
ステップ 3	セキュア トーンの電話番号の設定 （728 ページ）	保護されたデバイスの複数のコールとコール ウェイティングを設定します。
ステップ 4	セキュア トーン サービス パラメータの設定 （729 ページ）	サービス パラメータを設定します。
ステップ 5	（任意） MGCP E1 PRI ゲートウェイの設定 （729 ページ）	この設定により、Cisco Unified IP Phone エンドポイントと、MGCP ゲートウェイに接続している保護対象 PBX 電話機との間でコールの保護ステータスを渡すことができます。

電話機の保護デバイスとしての設定

始める前に

電話機能一覧の生成 （5 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 セキュア トーン パラメータを設定する電話をクリックします。
[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 3 ウィンドウの [デバイス情報（Device Information）] 部分の [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、[標準保護電話（Standard Protected Phone）] を選択します。

（注） 保護された電話機用の補足サービス ソフトキーのないソフトキーテンプレートを使用する必要があります。

ステップ 4 [複数ライン同時通話機能（Join Across Lines）] オプションをオフに設定します。

ステップ 5 [保護デバイス（Protected Device）] チェック ボックスをオンにします。

ステップ 6 [**デバイスのセキュリティプロファイル（Device Security Profile**）] ドロップダウンリスト（ウィンドウの [プロトコル指定情報（Protocol Specific Information）] 部分内）から、[**電話セキュリティ プロファイル設定（Phone Security Profile Configuration**）] ウィンドウで設定済みのセキュア電話プロファイルを選択します（**[システム（System）] > [セキュリティ プロファイル（Security Profile）] > [電話セキュリティ プロファイル（Phone Security Profile）]**）。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

次のいずれかの手順を実行します。

- セキュア トーンの電話番号の設定 （728 ページ）
- MGCP E1 PRI ゲートウェイの設定 （729 ページ）

セキュア トーンの電話番号の設定

始める前に

電話機の保護デバイスとしての設定 （727 ページ）

手順

ステップ 1 **[電話の設定（Phone Configuration）]** ウィンドウで、**[関連付け（Association）]** セクションに移動します。

ステップ 2 [新規 DN を追加（Add a new DN）]を選択します。
[ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウが表示されます。

ステップ 3 [**電話番号（Directory Number**）] フィールドで、電話番号を指定します。

ステップ 4 **[電話番号の設定（Directory Number Configuration**）] ウィンドウの **[Multiple Call/Call Waiting Settings on Device [device name]（デバイス [デバイス名] での複数コール/コール待機設定）]** 領域で、**[コールの最大数（Maximum Number of Calls）]** オプションと **[話中トリガー（Busy Trigger）]** オプションを 1 に設定します。

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、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、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。

セキュア トーン サービス パラメータの設定

手順

ステップ 1 [Cisco Unified CM の管理（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 [**クラスタ全体のパラメータ（機能 - セキュア トーン）（Clusterwide Parameters（Feature - Secure Tone）**）] エリアで、[**セキュア/非セキュア コールのステータスを示すトーンの再生（Play Tone to Indicate Secure/Non-Secure Call Status**）] を [True] に設定します。

ステップ 5 **[保存（Save）]** をクリックします。

MGCP E1 PRI ゲートウェイの設定

Cisco Unified IP Phone エンドポイントと、MGCP ゲートウェイに接続している保護対象 PBX 電話機との間でコールの保護ステータスを渡す場合は、次の手順を実行します。

始める前に

電話機の保護デバイスとしての設定 （727 ページ）

手順

ステップ 1 [Cisco Unified Communications Manager の管理（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 適切な検索条件を指定し、[**検索（Find**）] をクリックします。

ステップ 3 MGCP ゲートウェイを選択します。
[**ゲートウェイの設定（Gateway Configuration**）] ウィンドウが表示されます。

ステップ 4 [**グローバル ISDN スイッチ タイプ（Global ISDN Switch Type**）] を [ユーロ（Euro）] に設定します。

ステップ 5 [**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]** をクリックします。

ステップ 7 ウィンドウのサブユニット 0 の右側に表示されている [エンドポイント（Endpoint）]アイコンをクリックします。 [**保護されたファシリティ IE の有効化（Enable Protected Facility IE**）] チェックボックスが表示されます。 このチェックボックスをオンにします。

セキュア トーンの連携動作

機能	データのやり取り
コール転送、電話会議、およびコール ウェイティング	ユーザが保護されている電話でこれらの機能を呼び出すと、コールの最新のステータスを示すためにセキュア通知トーンまたは非セキュア通知トーンが再生されます。
保留と再開および不在転送	これらの機能は、保護されているコールでサポートされています。

セキュア トーンの制約事項

制約事項	説明
Cisco Extension Mobility および複数ライン同時通話機能（Join Across Lines）サービス	Cisco Extension Mobility および複数ライン同時通話機能サービスは、保護対象の電話では無効です。
共有回線の設定	共有回線の設定は、保護対象の電話機では使用できません。
非暗号化メディア	Cisco Unified IP 電話 と MGCP E1 PRI ゲートウェイの間のメディアが暗号化されていないと、コールはドロップされます。

第 XII 部

カスタム機能

第 47 章

ブランディングのカスタマイズ

ブランディングの概要

ブランディング機能では、Cisco Unified Communications Manager のカスタマイズされたブランディングをアップロードできます。 ブランディングは、Cisco Unified CM の管理のログイン ウィンドウと設定ウィンドウに適用されます。 変更できる項目には次のものがあります。

- 企業ロゴ
- 背景色
- 枠線色
- フォントの色

セルフケア ポータルでのロゴの追加

ブランディング機能では、企業ロゴを Unified Communications セルフ ケア ポータルのログイン ページとユーザ インターフェイスのヘッダーに追加できます。 `branding_logo.png` ファイルを `branding.zip` ファイルに含め、zip ファイルを Cisco Unified Communications Manager にアップロードする必要があります。 Cisco Unified Communications Manager でブランディングを有効にすると、ロゴがセルフ ケア ポータルに表示されます。

セルフケア ポータルの背景色やフォントをカスタマイズするオプションはありません。

ブランディングの前提条件

指定したフォルダ構造とファイルを含む`branding.zip`ファイルを作成する必要があります。詳細については、ブランディング ファイルの要件 （737 ページ）を参照してください。

ブランディングのタスク フロー

次のタスクを実行して、Cisco Unified Communications Manager および Unified Communications のセルフケア ポータルでブランディングを適用します。

始める前に

- ブランディングの前提条件 （733 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	次のいずれかの手順を使用してブランディング設定を構成します。 • ブランディングの有効化 （734 ページ） • ブランディングの無効化 （735 ページ）	Cisco Unified Communications Manager クラスタ全体でブランディングを適用します。
ステップ 2	Tomcat サービスの再起動 （736 ページ）	Unified Communications のセルフケア ポータルで新しいブランディング設定を取得するには、Cisco Tomcat サービスを再起動する必要があります。

ブランディングの有効化

この手順を使用して、Unified Communications Manager のブランディングのカスタマイズを有効にします。 システムで SAML シングル サインオンが有効になっている場合でも、ブランディング アップデートが表示されます。

（注） ブランディングを有効にするには、特権レベル 4 のアクセス権を持つプライマリ管理者アカウントを使用する必要があります。 これは、インストール時に作成されるメインの管理者アカウントです。

（注） GUI と CLI の中で 1 つのみを使用して、セキュリティ設定を有効および無効にしてください。たとえば、GUI インターフェイスを使用してロゴの作成を有効にする場合は、GUI インターフェイスそのものを使用して、ブランディングを無効にする必要があります。 そうしないと、正常に機能しません。

始める前に

`branding.zip` ファイルを準備し、Unified Communications Manager がアクセスできる場所に保存します。

手順

ステップ 1 Cisco Unified OS の管理にログインします。

ステップ 2 **[ソフトウェアアップグレード（Software Upgrades）] > [ブランディング（Branding）]** を選択します。

ステップ 3 リモート サーバを**参照**し、`branding.zip` ファイルを選択します。

ステップ 4 [ファイルのアップロード（Upload File）]をクリックします。

ステップ 5 [ブランディングの有効化（Enable Branding）]をクリックします。

（注） **utils Branding enable** CLI コマンドを実行して、ブランディングを有効にすることもできます。

ステップ 6 ブラウザを更新します。

ステップ 7 すべての Cisco Unified Communications Manager クラスタ ノードに対してこの手順を繰り返します。

セルフケア ポータルのユーザ インターフェイスに企業ロゴを追加する場合は、Tomcat サービスの再起動 （736 ページ） 次の手順を参照します。

ブランディングの無効化

この手順を使用して、Cisco Unified Communications Manager クラスタでブランディングを無効にします。 セルフケア ポータルから企業ロゴを削除する場合は、ブランディングを無効にする必要もあります。

（注） ブランディングを無効にするには、特権レベル4のアクセス権を持つプライマリ管理者アカウントを使用する必要があります。 これは、インストール時に作成されるメインの管理者アカウントです。

（注） GUI と CLI の中で 1 つのみを使用して、セキュリティ設定を有効および無効にしてください。たとえば、GUI インターフェイスを使用してロゴの作成を有効にする場合は、GUI インターフェイスそのものを使用して、ブランディングを無効にする必要があります。そうしないと、正常に機能しません。

手順

ステップ 1 Cisco Unified OS の管理にログインします。

ステップ 2 **[ソフトウェアアップグレード（Software Upgrades）]** > **[ブランディング（Branding）]** を選択します。

ステップ 3 [ブランディングの無効化（Disable Branding）]をクリックします。

（注） **utils Branding disable** CLI コマンドを実行して、ブランディングを無効にすることもできます。

ステップ 4 ブラウザを更新します。

ステップ 5 すべての Cisco Unified Communications Manager クラスタ ノードに対してこの手順を繰り返します。

セルフケア ポータルのユーザ インターフェイスから企業ロゴを削除する場合は、次の手順を実行します。Tomcat サービスの再起動 （736 ページ）

Tomcat サービスの再起動

セルフケア ポータルに反映させるには、Cisco Tomcat サービスを再起動してブランディング アップデートを行う必要があります。

始める前に

以下を完了していることを確認します。

- セルフケア ポータルにロゴを追加するには、まず Cisco Unified Communications Manager でブランディングを有効にする必要があります。`branding.zip` アップロード ファイルには、企業ロゴが入った 44x25 ピクセルの `branding_logo.png` ファイルが含まれている必要があります。 詳細は、ブランディングの有効化（734 ページ）を参照してください。
- セルフケア ポータルからロゴを削除するには、Cisco Unified Communications Manager でブランディングを無効にする必要があります。 詳細は、ブランディングの無効化 （735 ページ）を参照してください。

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

ステップ 3 すべての Cisco Unified Communications Manager クラスタ ノードに対してこの手順を繰り返します。

次のタスク

サービスが再起動したら、ブラウザを更新してセルフケア ポータルの変更を確認します。

ブランディング ファイルの要件

カスタマイズしたブランディングをシステムに適用する前に、所定の仕様に従って Branding.zip ファイルを作成します。 リモート サーバ上で、ブランディング フォルダを作成し、指定されたコンテンツをフォルダに入れます。 すべてのイメージ ファイルとサブフォルダを追加したら、フォルダ全体を圧縮し、ファイルを branding.zip として保存します。

ヘッダーに単一のイメージを使用するか、またはヘッダー用のグレーディング効果を得るために 6 つのイメージの組み合わせを使用するかに応じて、フォルダー構造には 2 つのオプションがあります。

表 *52* : フォルダ構造オプション

ブランディング オプション	フォルダ構造
単一ヘッダー オプション	ヘッダーの背景（吹き出し項目 3）に 1 つのイメージが必要な場合は、ブランディング フォルダに次のサブフォルダとイメージ ファイルが含まれている必要があります。 Branding (folder) ccmadmin (folder) BrandingProperties.properties (properties file) brandingHeader.gif (2048*1 pixel image) ciscoLogo12pxMargin.gif (44*44 pixel image) branding_logo.png (44*25 pixel image)

ブランディング オプション	フォルダ構造
勾配ヘッダー オプション	ヘッダーの背景用にグレーディング イメージを作成する場合は、グレーディング効果を得るために6つの個別のイメージファイルが必要です。 ブランディング フォルダには、これらのサブフォルダとファイルが含まれている必要があります。 Branding(folder) ccmadmin (folder) BrandingProperties.properties (file) brandingHeaderBegLTR.gif (652*1 pixel image) brandingHeaderBegRTR.gif (652*1 pixel image) brandingHeaderEndLTR.gif (652*1 pixel image) brandingHeaderEndRTR.gif (652*1 pixel image) brandingHeaderMidLTR.gif (652*1 pixel image) brandingHeaderMidRTR.gif (652*1 pixel image) ciscoLogo12pxMargin.gif (44*44 pixel image) branding_logo.png (44*25 pixel image)

ユーザ インターフェイスのブランディング オプション

次の画像に、Cisco Unified CM の管理ユーザ インターフェイスのカスタマイズ オプションを示します。

図 *10 : Unified CM* 管理ログイン画面のブランディング オプション

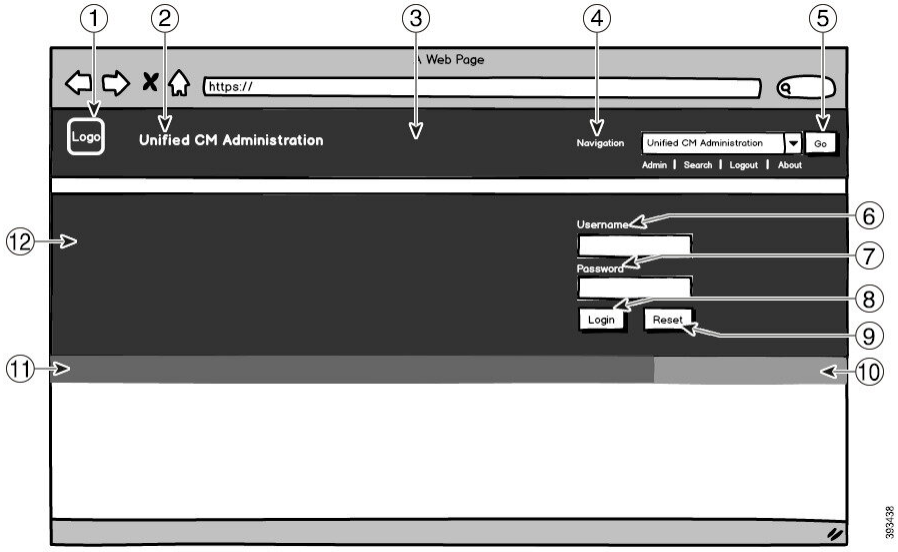
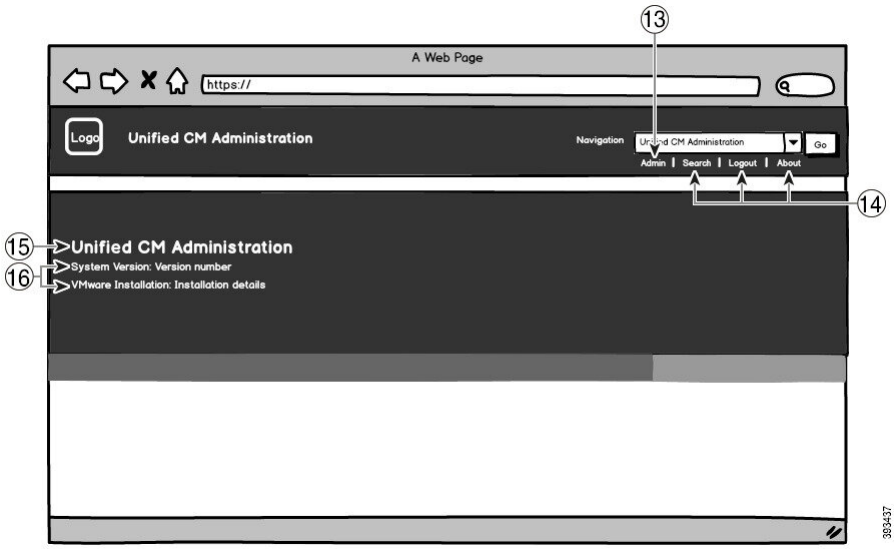


図 *11 : Unified CM* 管理ログイン中画面のブランディング オプション



次の表で、コールアウト オプションについて説明します。

表 *53 :* ユーザ インターフェイスのブランディング オプション：ログイン画面

項目	説明	ブランディングの編集
1	企業ロゴ	Cisco Unified Communications Manager にロゴを追加するには、会社のロゴを次のファイル名で44x44 ピクセルイメージとして保存します。 `ciscoLogo12pxMargin.gif`（44*44 ピクセル） （注） セルフケア ポータルのヘッダーとログイン画面にロゴを追加する場合も、ロゴを 44x25 ピクセルの `branding_logo.png` ファイルとして保存する必要があります。
2	Unified CM 管理ヘッダーのフォントの色	heading.heading.color

項目	説明	ブランディングの編集
3	ヘッダーの背景	1つの画像を使用するか、または6つの画像の組み合わせを使用してグレーディング効果を作成できます。 **シングル イメージ オプション**：単一のイメージとして、ヘッダー背景を保存します。 • brandingHeader.gif（2048*1 ピクセル） **グレーディング バックグラウンド オプション**：グレーディング効果を得るために 6 つのイメージとしてヘッダー背景を保存します。 • brandingHeaderBegLTR.gif（652*1 ピクセル） • brandingHeaderBegRTR.gif（652*1 ピクセル） • brandingHeaderEndLTR.gif（652*1 ピクセル） • brandingHeaderEndRTR.gif（652*1 ピクセル） • brandingHeaderMidLTR.gif（652*1 ピクセル） • brandingHeaderMidRTR.gif（652*1 ピクセル）
4	ナビゲーション テキスト	header.navigation.color
5	[移動（Go）] ボタン	header.go.font.color header.go.background.color header.go.border.color
6	ユーザ名テキスト	splash.username.color
7	パスワードのテキスト	splash.password.color
8	[ログイン（Login）] ボタン	splash.login.text.color splash.login.back.ground.color
9	[リセット（Reset）] ボタン	splash.reset.text.color splash.reset.back.ground.color
10	背景下の色：右側	splash.hex.code.3

項目	説明	ブランディングの編集
11	背景下の色：左側	splash.hex.code.2
12	バナー	splash.hex.code.1

表 *54* : ユーザ インターフェイスのブランディング オプション：ログイン中画面

項目	説明	ブランディングの編集
13	ユーザ テキスト（たとえば、「admin」）	header.admin.color
14	検索、バージョン情報、およびログイン テキスト	header.hover.link.color
15	Unified CM 管理のテキスト見出し	splash.header.color
16	システムのバージョン、VMware のインストール テキスト	splash.reset.text.color splash.version.color

ブランディング プロパティの編集例

ブランディング プロパティは、プロパティ ファイル（`BrandingProperties.properties`）に 16 進コードを追加することで編集できます。 プロパティ ファイルは HTML ベースの 16 進コードを使用します。 たとえば、ナビゲーション テキスト項目（吹き出し項目 #4）の色を赤に変更する場合は、プロパティ ファイルに次のコードを追加します。

```
header.navigation.color="#FF0000"
```

このコードで、`header.navigation.color` は編集するブランディング プロパティで、`"#FF0000"` は新しい設定（赤）です。

第 48 章

クライアント識別コードと強制承認コード

クライアント識別コードと強制承認コードの概要

クライアント識別コード（CMC）と強制承認コード（FAC）により、コール アクセスとアカウンティングを効果的に管理できます。 CMC はクライアントのコール アカウンティングおよび請求を支援し、FAC は特定のユーザが発信できるコールのタイプを規定します。

CMC を使用する場合、ユーザはコードを入力する必要があります。この操作により、コールが特定のクライアント識別に関連していることが指定されます。 コール アカウンティングおよび請求を目的として、クライアント識別コードを顧客、学生、またはその他のグループに割り当てることができます。 FAC を使用する場合、コールが確立する前に、特定のアクセス レベルで割り当てられた有効な認証コードをユーザが入力する必要があります。

クライアント識別コードと強制承認コードの前提条件

- SCCP と SIP を実行する Cisco Unified IP Phone は、CMC と FAC をサポートしています。
- CMC と FAC のトーンは、SCCP または SIP を実行している Cisco Unified IP Phone、TAPI/JTAPI ポート、および MGCP FXS ポートでのみ再生されます。

クライアント識別コードと強制承認コードの設定タスク フロー

CMC と FAC は、別々または一緒に実装できます。 たとえば、特定のクラスのコール（市外通話など）の発信をユーザに許可するとともに、特定のクライアントにコールのクラスを割り当てるとします。 CMC トーンと FAC トーンは、ユーザには同じ音に聞こえます。そのため、両方のコードを設定する場合、この機能では、最初のトーンの後で FAC を入力し、2 番目のトーンの後で CMC を入力するようユーザに指示します。

始める前に

- クライアント識別コードと強制承認コードの前提条件 （743 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	クライアント識別コードの設定 （744 ページ）を行うには、次のサブタスクを完了します。 • クライアント識別コードの追加 （745 ページ） • クライアント識別コードの有効化 （745 ページ）	使用する予定の CMC リストが完成したら、そのコードをデータベースに追加して、ルート パターンで CMC 機能を有効にします。
ステップ 2	強制承認コードの設定 （746 ページ）を行うには、次のサブタスクを完了します。 • 強制承認コードの追加 （746 ページ） • 強制承認コードの有効化 （747 ページ）	使用する予定の FAC リストと認可レベルが決定したら、そのコードをデータベースに追加して、ルート パターンで FAC 機能を有効にします。

クライアント識別コードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	クライアント識別コードの追加 （745 ページ）	使用する一意のクライアント識別コードを決定し、システムに追加します。

	コマンドまたはアクション	目的
		CMC の数は、システムの起動に要する時間の長さに直接影響するので、CMC の数を 60,000 までに制限してください。この最大数を超える CMC を設定する場合は、遅延が非常に大きくなることに注意してください。
ステップ 2	クライアント識別コードの有効化 （745 ページ）	ルート パターンを介してクライアント識別コードを有効にします。

クライアント識別コードの追加

使用する一意のクライアント識別コードを決定し、システムに追加します。 CMC の数は、システムの起動に要する時間の長さに直接影響するので、CMC の数を 60,000 までに制限してください。 この最大数を超える CMC を設定する場合は、遅延が非常に大きくなることに注意してください。

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。**コール ルーティング** > **クライアントの区別コード**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [クライアント識別コード（Client Matter Code）] フィールドで、通話の発信時にユーザが入力する一意のコードを 16 桁以内で入力します。

ステップ 4 [説明（Description）] フィールドに、クライアント識別コードを特定する場合のクライアント名を入力します。

ステップ 5 **[保存（Save）]** をクリックします。

クライアント識別コードの有効化

ルート パターンを介してクライアント識別コードを有効にします。

始める前に

クライアント識別コードの追加 （745 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）]** > **[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。

- 既存のルート パターンを更新するには、検索条件を入力し、[検索（Find）]をクリックして、結果リストからルート 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] 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）]ウィンドウで、[クライアント識別コードの要求（Require Client Matter Code）]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。

強制承認コードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	強制承認コードの追加 （746 ページ）	使用する一意の強制承認コードを定義し、システムに追加します。
ステップ 2	強制承認コードの有効化 （747 ページ）	ルート パターンを介して強制承認コードを有効にします。

強制承認コードの追加

この手順を使用して、使用する一意の強制承認コードを定義し、システムに追加します。 通話を正常にルーティングするためには、ユーザ認可レベルが通話のルート パターンに指定されている認可レベル以上である必要があります。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、**[コール ルーティング（Call Routing）]** > **[強制承認コード（Forced Authorization Codes）]** を選択します。

ステップ 2 [承認コード名（Authorization Code Name）] フィールドに、一意の名前を 50 文字以内で入力します。

この名前は、認証コードを特定のユーザまたはユーザ グループに結び付けます。

ステップ 3 [承認コード（Authorization Code）] フィールドに、一意の承認コードを 16 桁以内で入力します。

ユーザは、FAC 有効ルート パターンを介してコールを発信するときに、このコードを入力します。

ステップ 4 [承認レベル（Authorization Level）] フィールドに、3 桁の承認レベルを 0 ～ 255 の範囲で入力します。

ステップ 5 **[保存（Save）]** をクリックします。

強制承認コードの有効化

この手順を使用して、ルート パターンを介して強制承認コードを有効にします。

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/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。

- **[検索（Find）]** をクリックし、結果のリストからルート パターンを選択して、既存のルート パターンを更新します。
- 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 [ルート パターンの設定（Route Pattern Configuration）]ウィンドウで、[強制承認コードが必要（Require Forced Authorization Code）]チェック ボックスをオンにします。

ステップ 4 [認可レベル（Authorization Level）]フィールドに、0 ～ 255 の間で認可レベルの値を入力します。

ルーティングを成功させるには、ユーザの FAC レベルをコールの設定レベルと等しいか、またはそれよりも大きくする必要があります。

ステップ 5 **[保存（Save）]** をクリックします。

クライアント識別コードと強制承認コードの連携動作

表 *55*：クライアント識別コードと強制承認コードの連携動作

機能	データのやり取り
CDR 分析とレポート（CAR）	CDR Analysis and Reporting（CAR）を使用すれば、クライアント識別コード（CMC）、強制承認コード（FAC）、承認レベルに関するコール詳細を提示するレポートを実行できます。

機能	データのやり取り
CTI、JTAPI、および TAPI アプリケーション	ほとんどの場合、システムは、ユーザがコール中にコードを入力する必要がある CTI、JTAPI、TAPI アプリケーションに警告できます。 ユーザがコールを発信したり、アドホック会議を作成したり、CMC 対応または FAC 対応ルート パターン経由で打診転送を実行したりする場合は、トーンの受信後にコードを入力する必要があります。 ユーザが CMC 対応または FAC 対応ルート パターン経由でコールをリダイレクトまたはブラインド転送した場合は、トーンが流れないため、アプリケーションでコードを Cisco Unified Communications Manager に送信する必要があります。 システムが適切なコードを受信すると、コールが意図した通話相手に接続されます。 システムが適切なコードを受信しなかった場合、Cisco Unified Communications Manager は、コードが見つからないことを示すエラーをアプリケーションに送信します。
Cisco Web Dialer	Web Dialer は、次の方法で CMC と FAC をサポートします。 • ユーザは、WD HTML ページまたは SOAP 要求のダイヤル テキスト ボックスに接続先番号を入力してから、電話機に手動で CMC または FAC を入力できます。 • ユーザは、WD HTML ページまたは SOAP 要求のダイヤル テキスト ボックスに、接続先番号に続けて、FAC または CMC を入力できます。 たとえば、接続先番号が 5555、FAC が 111、CMC が 222 の場合は、5555111#（FAC）、5555222#（CMC）、または 5555111222#（CMC と FAC）をダイヤルすることにより、コールを発信できます。 （注） • Webダイヤラー は、接続先番号の検証を行いません。 電話機が必要な検証を処理します。 • ユーザがコードを入力しない場合、または誤ったコードを入力した場合、コールは失敗します。 • ユーザが特殊文字を含む DN を使って WebApp からコールを発信した場合は、特殊文字を削除するとコールが正常に動作します。 SOAP UI にはこのルールは該当しません。
スピードダイヤルと短縮スピードダイヤル	スピード ダイヤルを使用して、FAC、CMC、ダイヤル中のポーズ、追加の桁（ユーザの内線番号、会議へのアクセス コード、ボイスメールのパスワードなど）が必要な接続先に到達できます。 ユーザが設定されたスピード ダイヤルを押すと、電話機が接続先番号へのコールを確立して、指定された FAC、CMC、ダイヤル中のポーズが挿入された追加の桁を送信します。

クライアント識別コードと強制承認コードの制約事項

表 *56 :* クライアント識別コードと強制承認コードの制約事項

制約事項	説明
アナログ ゲートウェイ	H.323 アナログ ゲートウェイではトーンを再生できないため、この種類のゲートウェイでは CMC や FAC はサポートされていません。
通話転送	コードを入力するユーザがいないため、CMC や FAC が有効になっているルート パターンに転送されるコールは失敗します。 ユーザが [不在（CFwdALL）] ソフトキーを押して CMC や FAC がルート パターン上で有効になっている番号を入力すると、コール転送は失敗します。 呼処理の中断を最小限に抑えるには、コール転送を設定する前に番号をテストします。 これを行うには、転送したい番号をダイヤルしてみます。コードの入力を求められたら、その番号ではコール転送は設定できません。 転送されたコールが意図した接続先に届かないことから生じる苦情の数を削減するために、ユーザにこの方法を勧めてください。
Cisco Unified Mobility	SIP トランク、H.323 ゲートウェイ、MGCP ゲートウェイから発信されているコールが、CMC または FAC が必須のルート パターンに遭遇し、発信者に Cisco Unified Mobility が設定されていない場合、コールは失敗します。
Dial via Office コールバック番号	Cisco Mobility の CMC および FAC 機能では、Dial via Office（DVO）コールバック番号としての代替番号はサポートされていません。 DVO コールバック番号は、[モビリティID（Mobility Identity）]ウィンドウで登録されている番号である必要があります。
フェールオーバー コール	CMC および FAC は、フェールオーバー コールとは連動しません。
聴覚障がいのあるユーザ	電話番号をダイヤル後、聴覚障がいのあるユーザが認証コードやクライアント識別コードを入力するまでに 1 ～ 2 秒間待機する必要があります。
ローカリゼーション	シスコでは、CMC や FAC をローカライズしていません。 CMC および FAC 機能は、Cisco Unified Communications Manager でサポートされているすべてのロケールで同じデフォルトのトーンを使用します。 （注） Cisco Mobility では、CMC と FAC はローカライズされています。

制約事項	説明
オーバーラップ送信	Cisco Unified Communications Manager ではユーザにいつコードの入力を求めればよいかを判断できないため、CMC および FAC 機能はオーバーラップ送信をサポートしません。 **[ルート パターン設定（Route Pattern Configuration）]** ウィンドウで **[強制承認コードが必須（Require Forced Authorization Code）]** や **[クライアント識別コードが必須（Require Client Matter Code）]** のチェックボックスをオンにすると、自動的に **[オーバーラップ送信を許可（Allow Overlap Sending）]** のチェックボックスはオフになり、逆もまた同様です。
スピードダイヤル ボタン	CMC や FAC で短縮ダイヤル ボタンの設定をすることはできません。 システムに入力を求められた場合、コードを入力する必要があります。

第 49 章

カスタム電話呼出音とバックグラウンド

カスタム電話呼出音の概要

カスタム電話呼出音機能では、カスタム電話呼出音を作成し、カスタマイズしたファイルを Cisco Unified Communications Manager TFTP サーバにアップロードできます。このサーバでは、Cisco Unified IP Phone がこれらのファイルにアクセスできます。

Cisco Unified IP Phone には、Chirp1 と Chirp2 というデフォルト呼び出し音タイプが付属しており、これらはハードウェアに内蔵されています。 また、Cisco Unified Communications Manager では次のファイルを電話にアップロードできます。

PCM ファイル

Cisco Unified Communications Manager には、一連の追加の電話呼び出し音がデフォルトで付属しており、これらはパルス符号変調（PCM）オーディオ ファイルとしてソフトウェアに実装されています。 各 PCM ファイルでは 1 つの呼び出し音タイプが指定されます。

Ringlist.xml ファイル

Ringlist.xml ファイルには、電話で使用可能な呼び出し音オプションのリストが記述されています。

カスタム着信音やコールバック トーンなどのカスタマイズした PCM オーディオ ファイルと、変更した Ringlist.xml ファイルを Cisco Unified Communications Manager の TFTP ディレクトリにアップロードできます。

カスタム電話呼出音の前提条件

カスタム電話呼出音には次の前提条件が適用されます。

- カスタム電話呼出音をアップロードするには、Cisco TFTP サービスを実行しておく必要があります。
- Cisco Unified IP 電話 との互換性を保つには、アップロードする PCM ファイルが一連のファイル要件を満たす必要があります。 詳細については、トピックPCM ファイル形式の要件 （754 ページ）を参照してください。
- Ringlist.xml ファイルは、一連の書式ガイドラインを満たす必要があります。 詳細については、トピックRinglist.xml ファイル形式の要件 （754 ページ）を参照してください。

カスタム電話呼出音の設定タスク フロー

始める前に

- カスタム電話呼出音の前提条件 （752 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	カスタム電話呼出音のアップロードの準備 （752 ページ）	カスタマイズされた PCM および Ringlist.xml ファイルを作成します。
ステップ 2	TFTP サーバへのカスタム電話呼出音のアップロード （753 ページ）	カスタマイズされたファイルを Cisco Unified Communications Manager TFTP サーバにアップロードします。
ステップ 3	TFTP サービスの再起動 （753 ページ）	アップロードが完了したら、Cisco TFTP サービスを再起動します。

カスタム電話呼出音のアップロードの準備

手順

ステップ 1 変更する PCM ファイルに加えて、既存の Ringlist.xml ファイルをダウンロードするには、`file get tftp <tftp path>` CLI コマンドを使用します。

ステップ 2 アップロードする各呼出音タイプの PCM ファイルを作成します。 PCM ファイルの Cisco Unified Communications Manager との互換性に関するガイドラインについては、PCM ファイル形式の要件 （754 ページ） を参照してください。

ステップ 3 新しい電話の呼出音で Ringlist.xml ファイルを更新するには、ASCII エディタを使用します。 Ringlist.xml ファイルの形式要件の詳細については、Ringlist.xml ファイル形式の要件 （754 ページ） を参照してください。

TFTP サーバへのカスタム電話呼出音のアップロード

始める前に

カスタム電話呼出音のアップロードの準備 （752 ページ）

手順

ステップ 1 Cisco Unified OS の管理で、**[ソフトウェア アップグレード（Software Upgrades）] > [TFTP] > [ファイル管理（File Management）]** を選択します。

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。

ステップ 3 [検索（Browse）] をクリックして、Ringlist.xml ファイルと、アップロードする PCM ファイルを選択します。

ステップ 4 [ファイルのアップロード（Upload File）]をクリックします。

TFTP サービスの再起動

始める前に

TFTP サーバへのカスタム電話呼出音のアップロード （753 ページ）

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 - 機能サービス（Control Center - Feature Services）]**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、Cisco TFTP サービスが実行されているサーバを選択します。

ステップ 3 **Cisco TFTP** 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。

PCM ファイル形式の要件

電話の呼出音の PCM ファイルは、Cisco Unified IP 電話 で正常に再生するには一連の要件を満たしている必要があります。 PCM ファイルを作成または変更する際は、次のファイル形式要件をサポートしている任意の標準音声編集パッケージをご利用ください。

- Raw PCM
- サンプリング回数：8,000 回/秒。
- 1 サンプルあたり 8 ビット。
- μ-law 圧縮
- 呼出音の最大サイズ：16080 サンプル
- 呼び出し音のサンプル数が 240 で割り切れること
- 呼出音がゼロ交差で開始および終了すること

Ringlist.xml ファイル形式の要件

Ringlist.xml ファイルは、電話呼出音タイプのリストを保持した XML オブジェクトを定義しています。 呼出音タイプごとに、呼出音タイプに使用される PCM ファイルへのポインタ、および Cisco Unified IP 電話 の [呼出音タイプ（Ring Type）] メニューに表示されるテキストを記述します。

CiscoIPPhoneRinglist XML オブジェクトは、次の簡単なタグ セットを使用して情報を記述します。

```
<CiscoIPPhoneRinglist>   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRinglist>
```

定義名については、次の規則があります。

- DisplayName には、関連付けられた PCM ファイルのカスタム呼出音の名前を定義します。この名前は、Cisco Unified IP 電話 の [呼出音タイプ（Ring Type）] メニューに表示されます。
- FileName には、DisplayName に関連付けるカスタム呼出音の PCM ファイルの名前を指定します。

ヒント　DisplayName フィールドと FileName フィールドは、25 文字以下にする必要があります。

次に、2 つの電話呼出音タイプを定義した Ringlist.xml ファイルの例を示します。

```
<CiscoIPPhoneRinglist>   <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.raw</FileName>
   </Ring>
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.raw</FileName>
```

```
   </Ring>
</CiscoIPPhoneRinglist>
```

ヒント　それぞれの電話呼出音タイプについて、必須の DisplayName と FileName を記述する必要があります。 Ringlist.xml ファイルには、呼出音タイプを 50 個まで記述できます。

カスタム バックグラウンド

また、TFTP サーバを使用して、ネットワーク内の電話機に新しいカスタム背景イメージをアップロードすることもできます。 電話機のユーザは、アップロードした画像を電話機の背景として選択できます。 電話ユーザがさまざまな画像から選択できるように、またはすべての電話機に特定の背景イメージを割り当てることができるようにシステムを設定できます。

電話機のユーザが電話機の背景をカスタマイズできるようにするには、新しい画像をアップロードするたびに TFTP サーバに次のファイルを準備してアップロードする必要があります。

- フルサイズの背景イメージ：ご使用の電話機モデルの画像サイズ（ピクセル単位）やカラータイプなど、画像の仕様については、お使いの電話機のマニュアルを参照してください。
- サムネイル画像：これは、電話機のユーザが独自の背景イメージを選択できるようにする場合にのみ必要です。 サムネイル画像の仕様については、お使いの電話機のマニュアルを参照してください
- 編集済みの `List.xml` ファイル：このファイルには、背景イメージのリストが含まれており、電話機のユーザはこのリストから選択できます。 このファイルに新しい画像を追加する必要があります。

すべての電話機に特定の画像を割り当てる場合は、メインの背景イメージのみをアップロードする必要があります。 また、共通の電話プロファイルを更新して、割り当てた画像を使用するように電話機に指示する必要があります。

カスタム バックグラウンドの設定タスク フロー

これらのタスクを実行して、展開内の電話機のカスタマイズされた背景イメージを設定およびアップロードします。 電話機のユーザがさまざまな画像から選択できるように、またはすべての電話機に表示される特定の背景イメージを割り当てることができるようにシステムを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	電話機の背景イメージの作成 （757 ページ）	フルサイズの背景イメージと対応するサムネイル画像を作成します（必要な場合）。 ファイルの種類、イメージのサイズ（ピクセル単位）、色の種類など、イメージの仕様については、ご使用の電話機のマニュアルを参照してください。 （注） 特定の背景イメージを割り当てる場合、サムネイルは必要ありません。
ステップ 2	List.xml ファイルの編集 （757 ページ）	List.xml ファイルを適切な TFTP ディレクトリから新しいイメージで更新します。 これは、電話機のユーザが電話機のバックグラウンド オプションのリストに新しい画像を表示するために必要です。 （注） この手順は、ユーザに自分の背景を選択するオプションを与えている場合にのみ必要です。 特定の背景イメージを割り当てる場合は、このファイルを編集する必要はありません。
ステップ 3	TFTP サーバへのバックグラウンドのアップロード （758 ページ）	ファイルを TFTP サーバにアップロードします。
ステップ 4	TFTP サーバの再起動 （759 ページ）	Cisco TFTP サービスを再起動して、イメージを電話機にプッシュします。
ステップ 5	電話機ユーザの電話機バックグランドの割り当て （759 ページ）	これはオプションです。 デフォルトでは、Cisco Unified Communications Manager は電話機のユーザに自分の電話機の背景イメージを選択するオプションを提供します。 ただし、共通の電話プロファイルを使用して、この共通の電話プロファイルを使用するすべての電話機に特定の背景イメージを割り当てることができます。

電話機の背景イメージの作成

背景イメージの仕様およびサムネイル画像の仕様については、お使いの電話機のマニュアルを参照してください。 これには、イメージ サイズ（ピクセル単位）、ファイルのタイプ、およびその電話機モデルの適切な宛先 TFTP ディレクトリが含まれます（TFTP ディレクトリはイメージ仕様に基づいています）。

- 電話機のユーザがアップロードされた画像を使用するか使用しないかを選択するようにするには、その特定の電話機モデルの仕様に従ってフルサイズの画像とサムネイル画像の両方を準備する必要があります。
- 画像を特定の電話機に割り当てる場合は、フルサイズの画像のみが必要です。

次のタスク

電話機のユーザが自分の背景イメージを選択できるようにする場合は、List.xml ファイルの編集 （757 ページ）。

特定の背景イメージを割り当てる場合は、`List.xml` ファイルを更新する必要はありません。TFTP サーバへのバックグラウンドのアップロード （758 ページ）に進みます。

List.xml ファイルの編集

電話ユーザが背景イメージを選択できるようにするには、この手順を使用して、既存の `List.xml` ファイルにアップロードする新しい背景イメージを追加します。 各 TFTP イメージ ディレクトリには、その TFTP ディレクトリを使用する電話機で使用される `List.xml` ファイルが含まれています。 このファイルは、各背景オプションの特定の背景イメージとサムネイル画像を指し、最大 50 の背景イメージを含むことができます。 画像は、電話機に表示される順序でリストされます。 各イメージについて、ファイルには次の 2 つの属性を含む `<ImageItem>` 要素が含まれています。

- Image：電話機の [背景イメージ（Background Images）] メニューに表示されるサムネール画像の取得先を示す Uniform Resource Identifier（URI）。
- URL：フルサイズ画像の取得先を指定する URI。

例：

次の例（Cisco Unified IP Phone 7971G-GE および 7970G）に、2 つのイメージを定義する `List.xml` ファイルを示します。 それぞれの画像について、必須の Image および URL 属性を記述する必要があります。 この例で表示される TFTP URI は、HTTP URL サポートが提供されていないため、フルサイズ画像およびサムネイル画像にリンクするための唯一のサポートされている方法です。

```
<CiscoIPPhoneImageList>
   <ImageItem Image="TFTP:Desktops/320x212x12/TN-Fountain.png"
URL="TFTP:Desktops/320x212x12/Fountain.png"/>
   <ImageItem Image="TFTP:Desktops/320x212x12/TN-FullMoon.png"
```

```
URL="TFTP:Desktops/320x212x12/FullMoon.png"/>
</CiscoIPPhoneImageList
```

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 `file get tftp <filename>` CLI コマンドを実行します。ここで、<filename> は、適切な TFTP ディレクトリに対する `List.xml` ファイルのファイルとファイルパスを表します。

（注） それぞれのイメージ ディレクトリに独自のファイルがあるので、必ず適切な TFTP ディレクトリから `List.xml` ファイルをダウンロードしてください。 ディレクトリはイメージの仕様に基づいているため、その電話機モデルの適切な TFTP ディレクトリについて、ご使用の電話機のマニュアルを参照してください。

ステップ 3 追加する新しい各背景オプションに対し、新しい `<ImageItem>` 要素で xml ファイルを編集します。

TFTP サーバへのバックグラウンドのアップロード

この手順を使用して、新しい電話機のバックグラウンドファイルを TFTP サーバにアップロードします。

- 電話機のユーザが自分の背景イメージを選択できるようにするには、フルサイズの背景イメージ、サムネイル画像、および更新された `List.xml` ファイルをアップロードする必要があります。
- 特定の背景イメージを割り当てる場合は、フルサイズの背景イメージのみをアップロードする必要があります。

手順

ステップ 1 Cisco Unified OS の管理で、**[ソフトウェア アップグレード（Software Upgrades）]** > **[TFTP][ファイル管理（File Management）]** を選択します。

ステップ 2 [**ファイルのアップロード（Upload File**）] をクリックして、次の手順を実行します。

a) [**ファイルの選択（Choose File**）] をクリックして、アップロードするバックグラウンドファイルを選択します。

b) [**ディレクトリ（Directory**）] フィールドに、その電話機モデルの適切な TFTP ディレクトリを入力します。 TFTP ディレクトリは、画像のサイズと色のタイプに対応しています。画像の仕様については、お使いの電話機のマニュアルを参照してください。

c) [**ファイルのアップロード（Upload File**）] をクリックします。

d) これらの手順を繰り返して、サムネイル画像と `list.xml` ファイルの両方をアップロードします。 これらのファイルは、メインの背景イメージと同じ TFTP ディレクトリにロードする必要があります。

ステップ 3 **[閉じる（Close）]** をクリックします。

TFTP サーバの再起動

カスタム ファイルを TFTP ディレクトリにアップロードしたら、Cisco TFTP サーバを再起動してファイルを電話機にプッシュします。

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 - 機能サービス（Control Center - Feature Services）]**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、Cisco TFTP サービスが実行されているサーバを選択します。

ステップ 3 **Cisco TFTP** 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。

電話機ユーザの電話機バックグランドの割り当て

デフォルトでは、Cisco Unified Communications Manager を使用すると、電話機のユーザは自分の電話機の背景イメージをカスタマイズできます。 ただし、共通の電話プロファイル設定を使用して、この共通の電話プロファイルを使用するすべての電話機に特定の背景イメージを割り当てることができます。

手順

ステップ 1 Cisco Unified CM の管理から、**[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 次のいずれかを実行します。

- **[検索（Find）]** をクリックし、電話機が使用する共通の電話機プロファイルを選択します。
- **[新規追加（Add New）]** をクリックして、新しい共通の電話プロファイルを作成します。

ステップ 3 ユーザが自分の背景イメージを選択できるようにするには、[**背景イメージ設定へのアクセスの有効化（Enable End User Access to Phone Background Image Setting**）] チェックボックスがオンになっていることを確認します（これはデフォルト設定です）。

ステップ 4 このプロファイルを使用する電話機に特定の背景イメージを割り当てる場合は、次の手順を実行します。

- [**背景イメージ設定へのアクセスの有効化（Enable End User Access to Phone Background Image Setting**）] チェックボックスをオフにします。
- [**背景イメージ（Background Image**）] テキストボックスに、割り当てるイメージ ファイルのファイル名を入力します。 また、このテキスト ボックスに対応する [**エンタープライズ設定の上書き（Override Enterprise Settings**）] チェックボックスをオンにします。

ステップ 5 [**共通の電話プロファイル（Common Phone Profile**）] 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のヘルプについては、オンラインヘルプを参照してください。

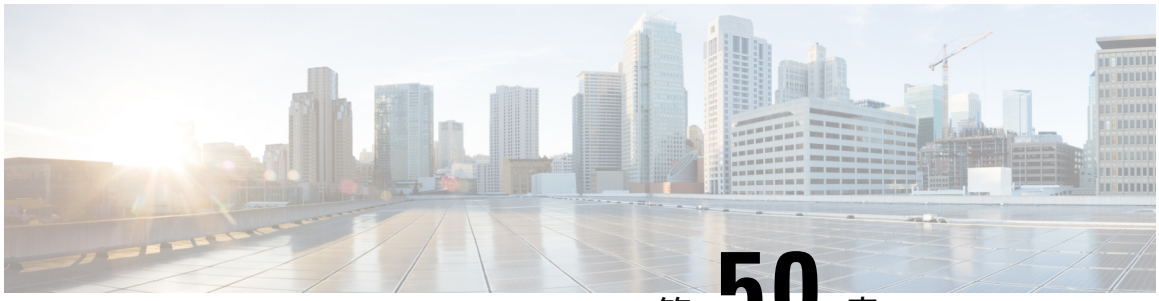
ステップ 6 **[保存]** をクリックします。
特定の背景イメージを割り当てた場合、この共通の電話プロファイルを使用するすべての電話機が、指定されたイメージを使用します。

次のタスク

新しい共通の電話プロファイルを作成した場合は、このプロファイルを使用するように電話機を再設定します。 Cisco Unified Communications Manager で電話機を設定する方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure Endpoint Devices」の項を参照してください。

ヒント 割り当てる電話機が多数ある場合は、一括管理ツールを使用して、1 回の操作で多数の電話機に共通の電話プロファイルを割り当てます。 詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

（注） 設定が完了したら、電話機をリセットします。



第 50 章

保留音

保留音の概要

オンネットとオフネットのユーザを保留にするときに、ストリーミング ソースから音楽を流すには、統合されている保留音（MoH）機能を使用します。 このソースは、保留にしたオンネットまたはオフネット デバイスに音楽を流します。 オンネット デバイスには、自動音声応答（IVR）または着呼分配機能により保留、打診転送保留、パーク転送保留にされるステーション デバイスおよびアプリケーションが含まれます。 オフネット ユーザには、Media Gateway Control Protocol（MGCP）ゲートウェイまたは Skinny Call Control Protocol（SCCP）ゲートウェイ、Cisco IOS H.323 ゲートウェイ、および Cisco IOS Media Gateway Control Protocol ゲートウェイ経由で接続するユーザが含まれます。 Cisco IOS H.323 または MGCP ゲートウェイの Foreign Exchange Station（FXS）ポート経由で Cisco IP ネットワークに接続している Cisco IP POTS フォンに対して、および Cisco MGCP または SCCP ゲートウェイに対しても、保留音機能が使用可能になります。

Cisco Unified Communications Manager を起動し、メディア リソース マネージャを作成します。保留音サーバが、その保留音リソースでメディア リソース マネージャに登録します。 保留音サーバは、保留音オーディオ ソースを提供し、複数のストリームに保留音オーディオ ソースを接続するソフトウェア アプリケーションです。

エンド デバイスまたは機能がコールを保留にすると、Cisco Unified Communications Manager は、その保留にされたデバイスを保留音リソースに接続します。 保留にされたデバイスが復帰すると、そのデバイスは保留音リソースから切り離され、通常のアクティビティを再開します。

発信者固有の保留音

SIP トランク経由で電話に着信する SIP コールの場合、Cisco Unified Communications Manager はさまざまな MOH オーディオ ソースを使用できます。

外部アプリケーション（Cisco Unified Customer Voice Portal（CVP）コンタクト センター ソリューションなど）は、発信者 ID、着信番号、または公衆電話交換網（PSTN）からコールが着信する場合は IVR 連携動作に基づいて、最も適切な MOH オーディオ ソースを判別します。

詳細については、Cisco Unified Customer Voice Portal のドキュメント（http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html）を参照してください。

IP Voice Media Streaming Application のキャパシティの増加と MOH オーディオ ソースの拡張

Cisco IP Voice Media Streaming Application は Cisco Unified Communications Manager のインストール時に自動でインストールされます。 このアプリケーションをアクティブ化して、保留音（MoH）機能を有効にします。

このリリースでは、一意の同時 MOH オーディオ ソースをサポートする Cisco Unified Communications Manager が、保留音サービスが MOH サーバ上で実行されている間、51 から 501 に増加しました。MOH オーディオ ソースには 1~501 の番号が付き、固定 MOH オーディオ ソースは番号 51 のままです。

Cisco Unified Communications Manager は VMware 上での実行時に USB をサポートしないため、固定 MoH デバイスは USB MoH デバイス経由で接続するオーディオ ソースを使用できません。VMware では固定 MoH USB デバイスの使用はサポートされません。 一方、Cisco Unified Survivable Remote Site Telephony（SRST）マルチキャスト MoH を利用する導入向けには、外部のサウンド デバイスをプロビジョニングします。

初期グリーティングとしてのカスタム アナウンス、または音楽を聞く発信者に対して定期的に再生されるアナウンスのいずれかまたは両方を使用するために、各 MOH オーディオ ソースを設定できます。 Cisco Unified Communications Manager には 1 つまたは複数の MOH オーディオ ソースで使用可能なカスタム アナウンスが 500 個用意されています。 これらのアナウンスはクラスタ内の Cisco Unified Communications Manager サーバ間での配信はされません。 これらのカスタム アナウンス ファイルは MoH およびアナウンス サービスを提供する各サーバにアップロードする必要があります。 また、MOH オーディオ ソースの各カスタム音楽ファイルも各サーバにアップロードする必要があります。

サービス付きメディア デバイスのパフォーマンスへの影響

Cisco IP Voice Media Streaming Application は、アナンシエータ（ANN）、ソフトウェア会議ブリッジ、保留音（MOH）、ソフトウェア メディア ターミネーション ポイントの 4 つのメディア デバイス向けのサービスとして実行します。 Cisco Unified Communications Manager のサーバ上で呼処理と共存するようにこのサービスを有効にします。 このサービスを有効にする際、呼処理への影響を避けるために必ず限定的な容量でこれらのメディア デバイスを設定します。

メディア デバイスのデフォルト設定はこの共存操作に基づいて定義されます。 1 つ以上のメディアデバイスの使用を減らし、その他の設定を増加させることでこれらの設定を調整できます。

たとえば、ソフトウェアのメディア ターミネーション ポイント デバイスを使用していない場合、SW MTP 用の [実行フラグ（Run Flag）]設定を [False]にし、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** > **[Cisco IP Voice Media Streaming App サービス（Cisco IP Voice Media Streaming App service）]** > **[MTP パラメータ（MTP Parameters）]** の順に選択します。そして、[MTP コール カウント（MTP Call Count）]設定を**[メディア リソース（Media Resource）]** > **[MOH サーバ（MOH Server）]** > **[最大半二重ストリーム（Maximum Half Duplex Streams）]** 設定に追加します。 コールのトラフィックによって、デフォルト設定を変更できます。 ただし、サーバ パフォーマンスのアクティビティで CPU、メモリ、I/O 待機をモニタします。 ユーザ数 7500 人の OVA 設定を使用しているような、容量の大きなクラスタでは、コール カウントのデフォルトのメディア デバイス設定を 25 %増やすことができます。

保留音のようにメディアデバイスの使用率が高くなることが予期される場合や、コールの数が多くてより多くのメディア接続数が必要とされる場合のインストールでは、呼処理が有効になっていない 1 つ以上の Cisco Unified Communications Manager サーバで Cisco IP Voice Media Streaming Application サービスを有効にします。 このサービスを有効にすると、メディア デバイスの使用によって呼処理などのその他のサービスが受ける影響が限定的なものになります。次に、メディア デバイスのコールの最大数の構成時の設定を増加させることができます。

Cisco Unified Communications Manager サービスと共存するように Cisco IP Voice Media Streaming Application を有効にした場合、呼処理のパフォーマンスに影響を与える可能性があります。 保留音やアナンシエータの容量設定をデフォルトの設定から増やす場合は、Cisco Unified Communications Manager を有効にせずにサーバで Cisco IP Voice Media Streaming Application を有効化することが推奨されています。

アクティブな発信者が保留中になっているときやマルチキャスト MOH のオーディオ ストリームが設定されているときは、CPU のパフォーマンスは MOH に影響されます。

表 *57*：一般的なパフォーマンス結果

設定に関する注意事項	CPU パフォーマンス
専用の MOH サーバ、保留中のコール 1000、グリーティングと定期アナウンスの MOH 音源 500。	25 ～ 45%（7500 ユーザの OVA 設定）
専用 MOH サーバとアナンシエータ サーバでのネイティブのコール キューイング、キューに入ったコール 1000、グリーティングと定期アナウンスの MOH 音源 500。 アナンシエータでは、最大 300 のグリーティング アナウンスを同時に再生できます。	25 ～ 45%（7500 ユーザの OVA 設定）
専用の MOH サーバ、保留中のコール 500、グリーティングと定期アナウンスの MOH 音源 500。	15 ～ 35%（7500 ユーザの OVA 設定）

表 *58 :* 推奨される推定の上限数

設定	推奨される上限数
Cisco IP Voice Media Streaming Application が 2500 OVA 上で Cisco Unified Communications Manager と共存する場合（中程度の呼処理）。	MOH：保留中の発信者 500、MOH 音源 100、アナンシエータの発信者 48 ～ 64。
Cisco IP Voice Media Streaming Application が 2500 OVA 上の専用サーバである場合。	MOH：保留中の発信者 750、MOH 音源 250、アナンシエータの発信者 250。
Cisco IP Voice Media Streaming Application が 7500/10K OVA 上で Cisco Unified Communications Manager と共存する場合（中程度の呼処理）。	MOH：保留中の発信者 500、MOH 音源 250、アナンシエータの発信者 128。
Cisco IP Voice Media Streaming Application が 7500/10K OVA 上の専用サーバである場合。	MOH：保留中の発信者 1000、MOH 音源 500、アナンシエータの発信者 300 ～ 700（MOH のコーデックは 1 つ）。 （注） MOH コーデックが 2 つの場合、アナンシエータの発信者を 300 に減らします。

（注） この推奨の上限数は MOH や ANN デバイス固有のものです。 これらのデバイスをソフトウェアのメディア ターミネーション ポイント（MTP）や話中転送（CFB）デバイスと組み合わせる場合、ストリームを提供するためには上限を減らします。

キャパシティ プランニングに関する設定の制約事項

Cisco IP Voice Media Streaming Application とセルフ プロビジョニング IVR サービスは、メディア カーネル ドライバを使用して Real-Time Transfer Protocol（RTP）ストリームを作成および制御します。 このメディア カーネル ドライバのキャパシティは 6000 ストリームです。 これらのストリームにより、メディア デバイスと IVR はリソースを予約できます。

この予約は、次のキャパシティ計算に基づきます。

メディア デバイス	容量
アナンシエータ	（[コール カウント（Call Count）] サービス パラメータ）* 3 3 はエンドポイントの受信（RX）コールと送信（TX）コール、および 1（.wav ファイル）の合計を示します。
ソフトウェア会議ブリッジ	（[コール カウント（Call Count）] サービス パラメータ）* 2 2 は RX および TX エンドポイントの合計ストリーム数を示します。

メディア デバイス	容量
ソフトウェア メディア ターミネーション ポイント	（[コール カウント（Call Count）] サービス パラメータ）* 2 2はRXおよびTXエンドポイントの合計ストリーム数を示します。
保留音	（（最大半二重ストリーム数）* 3）+（501 * 2 * [有効な MOH コーデックの数]） ここで、 • （最大半二重ストリーム数）は、MOH デバイス設定管理 Web ページの設定値です。 • 3 は、RX、TX、およびグリーティング アナウンスの .wav ファイルの合計ストリーム数を示します。 • 501 は、保留音（MOH）ソースの最大数を示します。 • 2 は、ミュージック .wav ストリームと発生する可能性のあるマルチキャスト TX ストリームを示します。 • [有効な MOH コーデックの数] は、Cisco IP Voice Media Streaming Application のサービス パラメータで有効な MOH コーデックの数に基づいています。
セルフ プロビジョニング IVR サービス	(500 * 2) 500 は発信者、2 は RX および TX ストリームからの合計ストリーム数を示します。

したがって、MOH が最大 1000 人の発信者をサポートできるようにする場合の式は、`1000 * 3 + 501 * 2 * 1 = 4002` ドライバ ストリーム（有効なコーデックの数は 1）、および `1000 * 3 +501 * 2 * 2 = 5004`（有効なコーデックの数は 2）となります。 残りのデバイスの数を減らし、セルフ プロビジョニング IVR サービスを無効にして、合計予約数を 6000 に制限します。これにより、MOHデバイスが予約を実行できるようになります。 また、Cisco IP Voice Media Streaming Application と同じサーバでセルフ プロビジョニング IVR サービスをアクティブにできない場合があります。

メディア デバイスの設定がメディア デバイス ドライバのキャパシティを超える場合、デバイス ドライバに登録されているメディア デバイスが、必要なストリーム リソースを最初に予約できるようになります。 後で登録されるメディア デバイスに対しては、必要なストリーム リソースよりも少ない数に制限されます。 メディアデバイスを後から登録すると、一部のアラーム メッセージがログに記録され、制限されるメディア デバイスのコール数が自動的に削減されます。

（注） キャパシティが 6000 ストリームのメディア カーネル ドライバでは、複数の同時メディア デバイス接続がサポートされていない可能性があります。

外部マルチキャスト MOH からユニキャスト MOH へのインターワーキング

このリリースでは、Cisco Unified Survivable Remote Site Telephony（SRST）ルータをオーディオ ソースとして設定できます。 このルータは、マルチキャスト受信が可能なデバイスに対してマルチキャスト MOH オーディオを提供します。 この方法では、Cisco Unified Communications Manager がマルチキャスト MOH オーディオを送信している場合と同様にデバイスが機能します。 ただし、ユニキャスト受信だけが可能なデバイスでは、外部 MOH ソース（Cisco Unified SRST ルータなど）から送信される MOH オーディオは聞こえません。 ユニキャスト受信のみが可能なデバイスの例としては、公衆電話交換網（PSTN）電話機、セッション ボーダー コントローラ（SBC）の接続先 および Session Initiation Protocol（SIP）トランクなどがあります。

Cisco Unified Communications Manager のこのリリースでは、この機能が拡張され、外部オーディオ ソースからのマルチキャスト MOH オーディオを受信し、ユニキャスト MOH オーディオとして送信できるようになりました。 Cisco Unified Communications Manager はこの機能を使用して、ユニキャスト MOH の受信のみが可能なデバイスに対し、マルチキャスト MOH オーディオをユニキャスト MOH として再生します。 外部 MOH オーディオ ソースの例としては、Cisco Unified SRST ルータや、マルチキャスト MOH オーディオを送信できるソフトウェアなどがあります。

管理者は [Cisco Unified CM の管理（Cisco Unified CM Administration）] の [**保留音オーディオ ソースの設定（Music On Hold Audio Source Configuration**）] ウィンドウでこの機能に関するフィールドを設定できます。

（注）
- この機能は、マルチキャスト受信可能なデバイスに対して外部オーディオ ソースを使用してマルチキャスト MOH オーディオを再生できる既存の機能には影響しません。
- ユニキャスト メディア接続の場合、外部マルチキャスト ソースを使用した MOH オーディオ ソースを設定していても、Cisco Unified Communications Manager MOH サーバは初回アナウンスと定期的なアナウンスを再生します。

コーデック固有の着信オーディオ ストリームに関する設定のヒント

必要なオーディオ フィードをストリーミングするため、MOH サーバに対し、外部マルチキャスト オーディオ ソース（Cisco Unified SRST ルータなど）を設定します。

Cisco Unified SRST ルータなどの外部マルチキャスト オーディオ ソースを設定するには、**[MOH オーディオ ソースの設定（MOH Audio Source Configuration）]** ウィンドウで **[ソースの IPv4 マルチキャスト アドレス（Source IPv4 Multicast Address）]** フィールドと **[ソースのポート番号（Source Port Number）]** フィールドを設定します。

- Cisco Unified Communications Manager は、[**MOH オーディオ ソースの設定（MOH Audio Source Configuration**）] ウィンドウで設定した外部マルチキャスト IP アドレスとポート

で、マルチキャストG.711 μ-lawストリームをリッスンします。 MOHサーバはG.711 μ-lawまたはA-law、あるいはL16 256Kワイドバンド MOH コーデック間の変換を実行できます。 外部マルチキャスト RTP ストリームは、G.711 μ-law または A-law、あるいは L16 256K ワイドバンド MOH コーデックのソースとして、MOH に G.711 μ-law コーデックを使用します。 G.711 A-lawおよびワイドバンドコールの場合、Cisco Unified Communications Manager MOH サーバは、着信 G.711 μ-law ストリームを発信 G.711 A-law またはワイドバンド ストリームに変換してから、デバイスに送信します。

- Cisco Unified Communications Manager は、**[MOH オーディオ ソースの設定（MOH Audio Source Configuration）]** ウィンドウで設定した外部マルチキャストIPアドレスおよびポートの値に 4 を加算したアドレスで、マルチキャスト G.729 μ-law ストリームをリッスンします。 たとえば、239.1.1.1:16384 を使用して MOH オーディオ ソースを設定した場合、Cisco Unified Communications Manager は 239.1.1.1:16384 で G.711 μ-law ストリームをリッスンし、239.1.1.1:16388（ポート値に 4 を加算した値）で G.729 をリッスンします。 MOH サーバは、G.729 コーデックの変換は実行できません。 MOH G.729 コーデックを使用する発信者には、G.729 または G.729a コーデックを使用する外部マルチキャスト RTP ストリームが必要です。

保留音の前提条件

- マルチキャストを設定する前に、MOHサーバと音声送信元を設定することを確認します。固定の音声送信元を使用する場合、マルチキャストを設定する前に設定します。
- ユニキャストまたはマルチキャスト保留音を実行するかどうかを必ず決定してください。
- 導入および設定されるハードウェアのキャパシティを計画し、予想されるネットワークの通話量を確実にサポートできるようにすることが非常に重要です。 MOH リソースのハードウェア キャパシティを知り、このキャパシティに対してマルチキャストMOHおよびユニキャストMOHの実装を考慮する必要があります。 ネットワークの通話量がこの制限を超えないようにします。 MOH セッションがこの制限に達すると、負荷が増加して MOH 品質が低下し、MOH の動作が不規則になり、MOH 機能が失われる可能性があります。
- マルチキャスト MOH を使用し、マルチキャスト MOH ストリームをリッスンするデバイスが同じ IP ネットワーク内にない場合、IP ネットワークでマルチキャスト ルーティングを有効にする必要があります。 マルチキャストルーティングを有効にする場合は、間違って送信されたマルチキャスト パケット（特にWANリンク経由で）によってネットワークの一部でフラッディングが発生する問題を回避するために注意が必要です。 マルチキャストMOHパケットが不要なインターフェイスではマルチキャストを無効にし、[最大ホップ数（Max Hops）] パラメータを使用してください。
- サーバキャパシティを含む保留音の展開の計画の詳細については、『シスココラボレーションシステムソリューションリファレンスネットワーク設計』の「保留音容量」のトピックを参照してください。

保留音設定のタスク フロー

システムの保留音 （MOH） 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	Cisco IP Voice Media Streaming のアクティブ化 （769 ページ）	保留音を有効にするには、**CISCO IP Voice Media Streaming Service アプリケーション**サービスをアクティブにします。
ステップ 2	保留音サーバの設定 （769 ページ）	MOH サーバの基本的なサーバ設定を設定します。
ステップ 3	保留音オーディオファイルのアップロード （770 ページ）	これはオプションです。独自のオーディオファイルをアップロードして、MOH オーディオストリームとして使用できるようにします。
ステップ 4	保留音オーディオ ソースの設定 （771 ページ）	保留音オーディオ ストリームを設定します。 また、アップロードされたオーディオファイルをMOHオーディオストリームに関連付けることもできます。
ステップ 5	固定保留音オーディオ ソースの設定 （772 ページ）	固定保留音オーディオ ソースを設定します。 システムは、1つの固定 MOH オーディオソース （ストリーム 51） をサポートしています。
ステップ 6	メディア リソース グループへの MOH の追加 （773 ページ）	保留音サービスをメディアリソースグループに割り当てます。 このグループは、コールのエンドポイントで使用可能なメディアリソースをコンパイルします。
ステップ 7	メディア リソース グループ リストの設定 （773 ページ）	メディア リソース グループを、優先されるメディア リソース グループ リストに割り当てます。
ステップ 8	デバイス プールへのメディア リソースの追加 （774 ページ）	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ることによって、エンドポイントで保留音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
ステップ 9	MOH サービスパラメータの設定 （775 ページ）	これはオプションです。 保留中のコールのデフォルトのコーデックやデフォルトのオーディオストリームなどのオプションの保留音パラメータを設定します。

Cisco IP Voice Media Streaming のアクティブ化

保留音を有効にするには、[シスコ IP ボイス メディア ストリーミング アプリケーション（Cisco IP Voice Media Streaming Application）]サービスを **有効化**する必要があります。

（注） インストール時に、Unified Communications Manager は保留音のデフォルトのオーディオ ソースをインストールし、設定します。 保留音機能はデフォルトのオーディオ ソースを使用して続行できます。

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。**[ツール（Tools）] > [サービス アクティベーション（Service Activation）]** を選択します。

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 [CM サービス（CM Services）]で、[シスコ IP ボイス メディア ストリーミング アプリケーション（Cisco IP Voice Media Streaming App）] サービスが**有効化**されていることを確認してください。 サービスが非アクティブになっている場合は、サービスを確認し、**[保存 （Save）]** をクリックします。

保留音サーバの設定

始める前に

1 つまたは複数の保留音（MOH）サーバが使用可能であることを確認します。

（注） Cisco Unified Communications Manager MOH サーバは、**Cisco IP Voice Media Streaming Application** サービスを有効にすると自動的に追加されます。

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。**[メディア リソース（Media Resources）] > [保留音サーバ（Music On Hold Server）]**。

ステップ 2 [**検索（Find**）] をクリックして、更新する保留音サーバを選択します。

ステップ 3 [**ホスト サーバ（Host Server**）] を選択します。

ステップ 4 **説明**とともに、記述された**保留音サーバの名前**を入力します。

ステップ 5 そのサーバに使用する [**デバイス プール（Device Pool**）] を選択します。

ステップ 6 次のフィールドを設定して、サーバ キャパシティを設定します。

- [**最大半二重ストリーム（Maximum Half Duplex Stream**）]：任意の時点で、この保留音サーバからストリーミングされるユニキャスト保留音の対象となるデバイスの最大数に設定します。 次の式を使用して、最大値を計算できます。

  （注） （Server and deployment capacity） -（[Number of multicast MOH sources] * [Number of enabled MOH codecs]）

- [**最大マルチキャスト接続数（Maximum Multi-cast Connections**）]：任意の時点でマルチキャスト MOH に配置される可能性のあるデバイス数以上の値に設定します。

ステップ 7 （任意） マルチキャストを有効にするには、[**Enable multi Cast Audio Sources on this MOH Server**] チェックボックスをオンにして、マルチキャスト IP アドレスの範囲を設定します。

ステップ 8 [**保留音サーバの設定（Music On Hold Server Configuration**）] ウィンドウの追加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。

保留音オーディオ ファイルのアップロード

保留音のオーディオ ストリームに使用したいカスタム オーディオ ファイルをアップロードする場合は、この手順を使用します。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[メディア リソース（Media Resources）] > [MOH オーディオ ファイル管理（MOH Audio File Management）]**。

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。

ステップ 3 **[ファイルの選択（Choose File）]** をクリックして、アップロードするファイルを選択します。ファイルを選択したら、[**開く （Open**）] をクリックします。

ステップ 4 [アップロード（Upload）]をクリックします。

[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。 アップロード手順によって、ファイルがアップロードされ、オーディオ変換が実行されて、MoH のためのコーデック固有のオーディオ ファイルが作成されます。 元のファイル サイズによっては、処理が完了するまで数分かかることがあります。

ステップ 5 **[閉じる（Close）]** をクリックして、**[アップロード結果（Upload Result）]** ウィンドウを閉じます。

ステップ 6 追加のオーディオ ファイルをアップロードする場合は、この手順を繰り返します。

（注） 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。 次にオーディオ ソース ファイル有効な入力形式の例を挙げます。

- 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、または 8 kHz のサンプル レート

（注） MOH オーディオ ソース ファイルは、クラスタ内の他の MOH サーバには自動で反映されません。 オーディオ ソース ファイルを各 MOH サーバまたはクラスタの各サーバに個別にアップロードする必要があります。

保留音オーディオ ソースの設定

保留中のオーディオ ソースを設定するには、次の手順を実行します。 オーディオ ストリームを設定し、アップロードされたファイルにオーディオ ストリームを関連付けることができます。 最大 500 のオーディオ ストリームを設定できます。

（注） オーディオ ソース ファイルの新しいバージョンを使用可能にするには、新しいバージョンを使用できるように更新手順を実行します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] 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。

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、既存のオーディオ ストリームを選択します。
- 新しいストリームを設定するには、**[新規追加] をクリックします。**

ステップ 3 **Moh オーディオストリーム番号**から、オーディオストリームを選択します。

ステップ 4 **[MOH オーディオ ソース名（MOH Audio Source Name）]** フィールドに、一意の名前を入力します。

ステップ 5 これはオプションです。 [マルチキャストを許可する（Allow Multi-casting）]チェックボックスをオンにして、このファイルに対してマルチキャストを許可します。

ステップ 6 オーディオ ソースの設定：

- [**MOH WAV ファイル**ソースの使用] オプションボタンをオンにし、**Moh オーディオソースファイル**から、割り当てるファイルを選択します。
- [リブロードキャスト外部マルチキャスト ソース（Rebroadcast External Multicast Source）] ラジオ ボタンをオンにして、マルチキャスト ソース IP アドレスの詳細を入力します。

ステップ 7 [パイロット コールを保留またはハントするアナウンスメント設定（Announcement Settings for Held and Hunt Pilot Calls）]セクションで、そのオーディオ ソースに使用したいアナウンスメントを割り当てます。

ステップ 8 **[保留音オーディオ ソースの設定（Music On Hold Audio Source Configuration）]** ウィンドウの残りのフィールドを設定します。 フィールドと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。

固定保留音オーディオ ソースの設定

For each cluster, you may define one fixed audio source （Source 51）. 各 MOH サーバのクラスタごとに設定される固定オーディオ ソースを設定する必要があります。 この固定オーディオ ソースは、ローカル コンピュータのオーディオ ドライバを使用する固定デバイスから送信されます。

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。**[メディア リソース（Media Resources）]** > **[固定 MOH オーディオ ソース（Fixed MOH Audio Source）]**。

ステップ 2 これはオプションです。 この音源のマルチキャストを許可する場合は、**[マルチキャストを許可する （allow multi鋳造）]** チェックボックスをオンにします。

ステップ 3 固定オーディオソースを有効にするには、**[有効 （enable ）]** 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際は、**名前**が必要です。

ステップ 4 [パイロット コールを保留またはハントするアナウンスメント設定（Announcement Settings for Held and Hunt Pilot Calls）]エリアで、このオーディオ ソースに対するアナウンスメントを設定します。

ステップ 5 **[固定 MOH オーディオ ソースの設定（Fixed MOH Audio Source 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。

メディア リソース グループへの MOH の追加

メディア リソース グループは、メディア リソースの論理グループです。 必要に応じて、メディア リソース グループを地理的な場所またはサイトに関連付けることができます。 またメディア リソース グループを作成して、サーバの使用状況、またはユニキャストやマルチキャストのサービス タイプを制御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。**[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）]**。

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、新しいグループを作成します。

ステップ 3 [Name]と [Description]を入力します。

ステップ 4 **[使用可能なメディアリソース （Available Media resources ）]** リストで、保留音リソースを選択し、下矢印を使用して、**選択したメディアリソース**にリソースを追加します。 このグループに割り当てる他のメディア リソースに対して、この手順を繰り返します。

ステップ 5 （任意） 保留音のマルチキャストを許可する場合は、**[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 6 **[保存（Save）]** をクリックします。

メディア リソース グループ リストの設定

メディア リソース グループ リストは、優先されるメディア リソース グループの一覧を表示します。 アプリケーションは、メディア リソース グループ リストに定義されている優先順位に従って、使用可能なメディア リソースの中から、必要なメディア リソースを選択できます。

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。**[メディア リソース（Media Resources）]** > **[メディア リソース グループ リスト（Media Resource Group List）]**。

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、既存のメディア リソース グループ リストを選択します。

- [新規追加（**Add New**）] をクリックして、新しいメディア リソース グループ リストを作成します。

ステップ 3 リストの名前を **[Name（名前）]** に入力します。

ステップ 4 **[使用可能効なメディア リソース グループ（Available Media Resource Groups）]** リストから、このリストに追加するグループを選択し、下矢印を使用して、**[選択したメディア リソース グループ（Selected Media Resource Groups）]**に移動します。

ステップ 5 [**Selected Media Resource groups**] リストで、リストの右側にある上下の矢印を使用して、グループの優先順位を編集します。

ステップ 6 **[保存（Save）]** をクリックします。

デバイス プールへのメディア リソースの追加

MOH リソースを含む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ることによって、デバイスが MOH を使用できるようにすることができます。

（注） コール中のデバイスは、**[電話の設定 （Phone Configuration ）]** ウィンドウでデバイスに割り当てられているメディア リソース グループ リストを使用します。 何も割り当てられていない場合は、コールに使用されるデバイス プールのメディア リソース グループ リストが使用されます。

手順

ステップ 1 Cisco Unified CM の管理から、次のいずれかを実行します。

- **[システム（System）]** > **[デバイス プール（Device Pool）]** を選択します。
- **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。

ステップ 2 **[検索（Find）]** をクリックして、既存の電話または既存のデバイス プールを選択します。

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、保留音リソースが含まれているメディア リソース グループ リストを選択します。

ステップ 4 設定ウィンドウの残りのフィールドに入力します。フィールドと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。

MOH サービスパラメータの設定

保留音 （MOH） のオプションサービスパラメータを設定するには、次の手順を使用します。ほとんどの導入の場合、デフォルト設定で十分です。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[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 IP Voice Media Streaming**] を選択します。

ステップ 4 クラスタ**全体のパラメータ （[すべてのサーバに適用するパラメータ （parameters of all servers）]**）] エリアで、オプションの moh サービスパラメータを設定します。

ステップ 5 **[保存]** をクリックします。

ステップ 6 [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 7 オプションの MOH パラメータを設定します。 たとえば、クラスタ**全体のパラメータ （サービス**）では、保留のデフォルトのオーディオソースを割り当てることができます。

ステップ 8 **[保存]** をクリックします。

（注） クラスタ全体のグループに含まれるパラメータを除き、すべてのパラメータは現在のサーバにのみ適用されます。

保留音オーディオ ファイルの表示

システムに保存されている既存の保留音のオーディオ ファイルを表示します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）]で、**[メディア リソース（Media Resources）]** > **[MOH オーディオ ファイルの管理（MOH Audio File Management）]** を選択します。
[保留音オーディオ ファイルの管理（Music On Hold Audio File Management）]ウィンドウが表示されます。

ステップ 2 各レコードの次の情報を確認します。

- チェックボックス：オーディオファイルを削除できる場合は、[ファイル名（File Name）] 列の前にチェック ボックスが表示されます。
- [ファイル名（File Name）]：この列には、オーディオファイル名が表示されます。

- [長さ（Length）]：この列には、オーディオファイルの長さが分と秒の単位で表示されます。
- [ファイル ステータス（File Status）]：この列には、オーディオファイルの次のいずれかのステータスが表示されます。
  - [変換完了（Translation Complete）]：このステータスは、ファイルが正常にアップロードされ、保留音オーディオソースのオーディオファイルとして使用可能になると表示されます。
  - [使用中（In Use）]：このステータスは、このオーディオファイルをMOHオーディオソースファイルとして使用する保留音オーディオソースを追加すると表示されます。

（注） ステータスが [使用中（In Use）]のファイルは削除できません。

ユニキャストおよびマルチキャスト オーディオ ソース

ユニキャスト保留音が、システムのデフォルト オプションです。 ただし、必要に応じてマルチキャストを設定する必要があります。 マルチキャストとユニキャストの両方の設定において、保留された通話相手に対するオーディオソースの動作は同じです。 各オーディオ ソースは一度使用され、ストリームは内部で分割されて保留された通話相手に送信されます。 この状況でのマルチキャストとユニキャストの唯一の違いは、データがネットワーク上でどのように送信されるかだけです。

表 *59*：ユニキャストおよびマルチキャスト オーディオ ソースの違い

ユニキャスト オーディオ ソース	マルチキャスト オーディオ ソース
MOH サーバから MoH オーディオ ストリームを要求するエンドポイントに直接送信されるストリームで構成されます。	MOH サーバからマルチキャスト グループの IP アドレスに送信されるストリームで構成されます。 MoH オーディオ ストリームを要求するエンドポイントは、必要に応じてマルチキャスト MoH に参加できます。
ユニキャストMoHストリームは、サーバとエンドポイント デバイス間のポイントツーポイント片通話 RTP ストリームです。	マルチキャストMoHストリームは、MOHサーバとマルチキャスト グループ IP アドレス間の、ポイントツーマルチポイント片通話 RTP ストリームです。

ユニキャスト オーディオ ソース	マルチキャスト オーディオ ソース
ユニキャストMoHは、ユーザまたは接続ごとに別々のソース ストリームを使用します。ユーザまたはネットワーク イベントを介して保留になるエンドポイント デバイスが増えるにつれて、MoHストリームの本数も増加します。	複数のユーザに対して、MoHを提供するために同じオーディオ ソース ストリームを使用できます。
MOH オーディオ ソースには、最初のアナウンス（グリーティング）で設定でき、ユニキャストの保留された通話相手に対して送信されます。 ユニキャスト MoH ユーザの場合、このアナウンスは最初から流されます。	マルチキャスト ユーザの場合、このアナウンスは流されません。
追加のMoHストリームが生成されると、ネットワークのスループットと帯域幅に対してマイナスの影響を与える可能性があります。	マルチキャスト MoH では、システム リソースと帯域幅を節約できます。
マルチキャストが有効ではないか、デバイスがマルチキャストに対応していないネットワークでは非常に有用です。	ネットワークがマルチキャスト対応になっていない状況や、エンドポイント デバイスがマルチキャストを処理できない状況では、問題が生じる可能性があります。
管理デバイスのみを含みます。	管理デバイス、IP アドレスおよびポートを含みます。
保留音サーバを定義するための要件はありません。	マルチキャストを許可するには、管理者は少なくとも 1 つのオーディオ ソースを定義する必要があります。マルチキャストの保留音サーバを定義するには、まずマルチキャストを許可するようにサーバを定義します。
機能するために、MOH オーディオ ソース、MOH サーバまたはメディア リソース グループ リストを設定する必要はありません。	機能するためには、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 リストの両方が、マルチキャスト保留音サーバを含むように定義されている必要があります。 メディア リソース グループには、マルチキャスト用に設定された保留音サーバを含める必要があります。 これらのサーバは、（MOH）[multicast] とラベル付けされます。 また、マルチキャストのメディア リソース グループを定義する場合は、[MoHオーディオにマルチキャストを使用する（Use Multicast for MOH Audio）] チェックボックスをオンにします。

（注） SIP サービス パラメータのマルチキャスト MoH 方向属性により、Cisco Unified Communications Manager がマルチキャスト保留音（MoH）INVITE メッセージ中の Session Description Protocol（SDP）の方向属性を、[sendOnly] に設定するか [recvOnly] に設定するかが決まります。

導入において、Cisco Unified IP 電話 7940 と 7960 に対して SIP 電話機がリリース 8.4 以前を使用するか、Cisco Unified IP 電話7906、7911、7941、および 7961 に対して SIP 電話機がリリース 8.1(x) 以前を使用する場合、このパラメータを [sendOnly]に設定します。 それ以外の場合は、このパラメータをデフォルト値 [recvOnly] のままにします。

保留音の連携動作

機能	データのやり取り
H.323 クラスタ間トランク上のマルチキャスト保留音	H.323 クラスタ間トランク上のマルチキャスト MOH 機能を使用することで、MOH を H.323 クラスタ間トランク（ICT）上でマルチキャストできます。 コールがクラスタ間トランク上で接続され、片方が [保留（Hold）] キーを押すと、MOH がクラスタ間トランク上でストリームされます。 マルチキャスト MOH をオンにし、保留する側とトランクがマルチキャスト MOH サーバを使用するように設定してある場合、MOH はマルチキャストでストリームされます。 このトランク上で保留中のコールの数に関わりなく、1 つのマルチキャスト MOH ストリームのみがトランク上でストリームされます。 この機能に関する追加ポイント： • この機能は、Terminal Capability Set（TCS）および OLC メッセージの新規フィールドが Cisco Unified Communications Manager 間にあるいずれかのミドルボックスを通過しない場合、機能しません。 • この機能を使用する場合、マルチキャスト MOH のフィールドを追加設定する必要はなく、シングルトランスミッタ マルチキャストをサポートする Cisco Unified Communications Manager 間にのみ適用されます。 • 機能はデフォルトでオンですが、**[H.245 OLC メッセージでマルチキャスト MOH を送信（Send Multicast MOH in H.245 OLC Message）]** サービス パラメータを **[いいえ（False）]** に設定することによってオフにできます。 この値を設定することで、この機能によって生じる可能性がある相互運用性の問題を解決できます。

機能	データのやり取り
保留音のフェールオーバーとフォールバック	MOH サーバは、ソフトウェア会議ブリッジとメディア ターミネーション ポイントにより実装されている Cisco Unified Communications Manager のリストとフェールオーバーをサポートします。 フェールオーバーの際、システムは可能な場合、Cisco Unified Communications Manager をバックアップするために接続を維持します。 保留音セッションがアクティブな間に保留音サーバに障害が発生すると、保留された側にはこの時点から音楽が聞こえなくなります。 ただし、この状況は通常のコール機能には影響しません。
コールパークとダイレクト コール パーク	保留音を使用すると、ユーザはコールを保留にして、ストリーミング ソースから提供される音楽を再生できます。 保留音を使用すると、次の 2 種類の保留が可能です。 • ユーザ保留：ユーザが保留ボタンまたは [保留（Hold）] ソフトキーを押した場合、この種類の保留が起動されます。 • ネットワーク保留：ユーザが転送、電話会議、またはコールパーク機能を有効化した場合、この種類の保留が自動的に起動されます。 ダイレクト コール パークは転送機能のため、ダイレクト コール パークにはこの種類の保留が適用されます。 ただし、ダイレクト コール パークは、オーディオ ソースとして、Cisco Call Managerサービス パラメータである、デフォルトのネットワーク保留 MOH オーディオ ソースを使用します。
Extension Mobility Cross Cluster：訪問先電話のメディア リソース	例としては、RSVP エージェント、TRP、保留音（MOH）、MTP、トランスコーダ、および会議ブリッジがあります。 メディア リソースは、訪問先電話に対してローカルです（RSVP エージェント以外）。
保留復帰	MOH が通常の保留コールに設定されている場合、Cisco Unified Communications Manager は復帰したコール上での MOH をサポートします。
メディア リソースの選択	保留中のパーティは、Cisco Unified Communications Manager が保留音のリソースを割り当てるために使用するメディア リソース グループ リストを定義します。

機能	データのやり取り
SRTP を使用したセキュアな保留音	Cisco Unified Communications Manager では、Cisco IP Voice Media Streaming Application サービスが拡張され、Secure Real-Time Protocol（SRTP）をサポートするようになりました。 そのため、Cisco Unified Communications Manager クラスタまたはセキュリティ システムが有効な場合、MOH サーバは、SRTP 対応デバイスとして Cisco Unified Communications Manager に登録されます。 また、受信デバイスも SRTP に対応している場合、音楽メディアは受信デバイスにストリーミングされる前に暗号化されます。 次の点を確認してください。 • クラスタセキュリティは混合モードである必要があります。`utils ctl set-cluster mixed-mode` CLI コマンドを実行します。 • パス内の SIP トランクが SRTP をサポートする：SRTP がトランク上で動作するようにするには、**[トランクの設定（Trunk Configuration）]** ウィンドウで **[SRTP 許可（SRTP Allowed）]** チェックボックスをオンにする必要があります。 • デバイスが SRTP をサポートする：エンドポイントによって使用される電話セキュリティ プロファイルで、**[デバイス セキュリティ モード（Device Security Mode）]** が **[暗号化（Encrypted）]** に設定されている必要があります。

保留音の制約事項

制約事項	説明
マルチキャスト保留音のサポート	コンピュータテレフォニーインテグレーション（CTI）とメディア ターミネーション ポイント（MTP）デバイスは、マルチキャスト保留音機能をサポートしません。 CTI または MTP デバイスを、CTI デバイスのメディア リソース グループ リスト内のマルチキャスト MoH デバイスで設定する場合、コール制御の問題が起こることがあります。 CTI と MTP のデバイスは、ストリーミング メディアのマルチキャストをサポートしません。
インターネットプロトコルのサポート	マルチキャスト保留音は、IPv4 のみをサポートします。 保留音のコンポーネントである Cisco IP Voice Media Streaming Application は、ユニキャスト保留音の IPv4 および IPv6 のオーディオ メディア接続をサポートします。 マルチキャスト保留音は、IPv4 のみをサポートします。 IPv6 の IP アドレッシング モードのみを持つデバイスは、マルチキャストをサポートできません。

制約事項	説明
固定デバイスのオーディオ ソースの配信	Cisco Unified Communications Manager は、メディア リソース グループ内の保留音サーバに対する固定デバイス（ハードウェア）オーディオ ソースの配信をサポートしません。
G.729a コーデックの不適格音質	G.729a コーデックは人の声を対象としているため、音楽の保留音に使用すると適切な音質が得られないことがあります。
Cisco Unified Communications Manager システムのサポート	Cisco Unified Communications Manager クラスタまたはシステムは、Cisco Unified Computing System（UCS）サーバまたはその他のシスコ認定サードパーティ サーバの構成上での仮想展開のみをサポートします。 MoH を外部ソースから提供するノードの場合、保留音機能を外部ソース（USB オーディオ ドングル）と共に使用することはできません。
マルチキャスト サポート	管理者は、マルチキャストをサポートするリソースがある場合は、保留音サーバをユニキャストまたはマルチキャストとして指定できます。
発信者に固有の MoH のサポート	コールが QSIG のトンネル有効 SIP トランクで受信されるか転送される場合、発信者に固有の MoH はサポートされません。
MP3 形式のサポート	保留音機能は MP3 形式をサポートしません。
H.323 と SIP プロトコルとの相互運用性	マルチキャスト MoH は H.323 と SIP プロトコルとの相互運用性をサポートしません。
SRTP のサポート	マルチキャスト MoH オーディオ ストリームは暗号化されておらず、SRTP をサポートしません。
マルチキャスト ストリーム	MTP はマルチキャスト ストリームをサポートしません。
マルチキャスト保留音 RTP ストリームの暗号化	Cisco Unified Communications Manager は、マルチキャスト保留音 RTP ストリームの暗号化をサポートしません。 MOH オーディオの安全性を高めたい場合、マルチキャスト オーディオ ソースを設定するべきではありません。
保留音の固定デバイス	VMware 上で起動している場合、Cisco Unified Communications Manager は USB をサポートしないため、USB 経由で接続される保留音の固定デバイスはオーディオ ソースとして指定できません。 ただし、VMware は内部保留音をサポートします。
MOH サーバの障害	保留音セッションがアクティブな間は、保留音サーバに障害が生じても Cisco Unified Communications Manager は何のアクションも取りません。

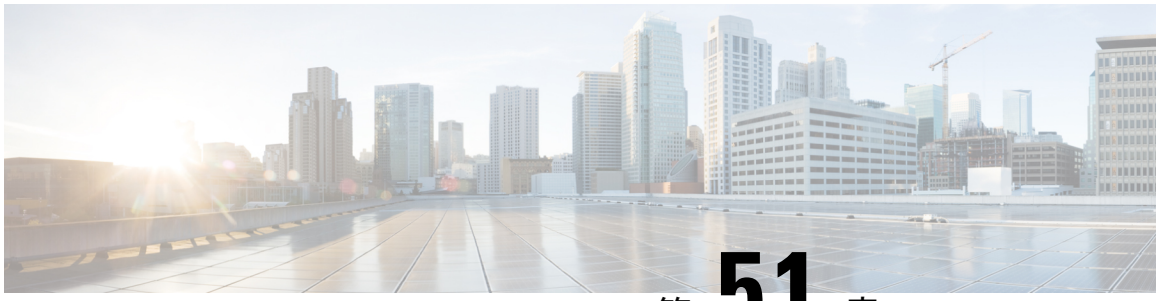
制約事項	説明
マルチキャスト MOH	マルチキャストMoHを使用しているサイトでコール レッグ中にMTP リソースが呼び出されると、Cisco Unified Communications Manager はマルチキャスト MoH の代わりにユニキャスト MoH にフォール バックされます。
プロビジョニング	ユーザ識別子とネットワーク MOH オーディオ ソース識別子をプロビジョニングしない場合や、1つまたは両方の値が無効である場合、SIP ヘッダー内の発信者に固有の MoH 情報は無視されます。 コールは保留トーンに復帰し、無効な MOH オーディオ ソースのアラームが発生します。
ヘッダーの値	• ユーザとネットワーク MOH オーディオ ソース識別子の両方がヘッダーに存在する場合、無効な値はすべてデフォルト値（0）に置換されます。 • 両方の値がゼロであるか、唯一の値がゼロの場合、着信 INVITE 内のヘッダーは無視されます。
MOH オーディオ ソース名	• SIP ヘッダーでMOH オーディオ ソース識別子を 1 つだけ指定する場合（MOH オーディオ ソース識別子の値の前か後にカンマがある場合も含む）、ユーザおよびネットワークMoHの両方に対して同じMoH IDが使用されます。 SIP トランクは、SIP ヘッダーにユーザおよびネットワーク MOH オーディオ ソース識別子の両方を入力し、コール制御が両方の値を必ず受信するようにします。 • ヘッダー内で 3 つ以上の MOH オーディオ ソース識別子の値がカンマで区切られている場合、最初の 2 つの値が使用されます。 後続の値は無視されます。
発信者に固有の MoH 設定の一貫性に関する管理者	複数の Cisco Unified Communications Manager が関連する場合、管理者は発信者に固有のMoH設定の一貫性を維持する責任を負います。
元のコール発信者	コール センターへの元のコール発信者は、コール全体を通じて変更できません。
MoH 情報	保留音情報は、SIP トランク間でのみ共有されます。

保留音のトラブルシューティング

保留音が電話機で再生されない

電話機のユーザに保留音が聞こえません。

- 音楽にはMoHと共にG.729aコーデックが使用されますが、十分な音声品質が提供されないことがあります。
- MTPリソースは、マルチキャストMoHを使用するサイトでのコール レッグで呼び出されます。
- MTPリソースがマルチキャストMoHを使用するサイトでのコール レッグで呼び出される場合、発信者には保留音は聞こえません。 このような状況を避けるため、マルチキャストMoHではなくユニキャストのMoHまたは保留トーンを設定します。



第 51 章

セルフケア ポータル

セルフケアポータルの概要

Cisco Unified Communications セルフ ケア ポータルから、電話の機能や設定をカスタマイズできます。 管理者は、ポータルへのアクセスを制御します。 エンドユーザがポータルにアクセスできるようにするには、その前に、ユーザをデフォルトの**標準 Ccm エンドユーザ**アクセスコントロールグループに追加するか、または**標準 ccm エンドユーザ** ロールが割り当てられたアクセスコントロールグループに追加する必要があります。 さらに、ユーザには、ポータルにアクセスするためのユーザ ID、パスワード、および URL が必要です。 ユーザは、次の URL 経由でポータルにアクセスできます。

http(s)://<server_name>:<port_number>/ucmuser/

引数の説明

- **<server_name>** は、Unified Communications Manager の IP アドレス、ホスト名、または完全修飾ドメイン名を表します
- **<port_number>** は、接続するポートを表します。 ポートはオプションですが、ファイアウォールの場合に便利です。
- **ucmuser** は、セルフケアをポイントする必須サブパスです

オプションで、エンドユーザが設定できる電話設定を割り当てるために、Cisco Unified Communications Manager 内でエンタープライズパラメータを設定することもできます。 たとえば、**Show Call フォワーディング**エンタープライズパラメータは、ユーザがポータル経由でコール転送を設定できるかどうかを決定します。

セルフ ケア ポータルのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザに対するセルフケア ポータルへのアクセス権の付与 （786 ページ）	ポータルにアクセスするには、エンドユーザが**標準 CCM エンド ユーザ** アクセス コントロール グループまたは**標準 CCM エンド ユーザ** ロール割り当てを持つグループに割り当てられている必要があります。
ステップ 2	セルフケア ポータル オプションの設定（787 ページ）	ポータルにアクセスするユーザが使用できる設定オプションを制御するためには、エンタープライズ パラメータを設定します。

ユーザに対するセルフケア ポータルへのアクセス権の付与

ポータルにアクセスするには、エンドユーザが**標準 CCM エンド ユーザ** アクセス コントロール グループまたは**標準 CCM エンド ユーザ** ロール割り当てを持つグループに割り当てられている必要があります。

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。**[ユーザ管理（User Management）] > [エンド ユーザ（End User）]**。

ステップ 2 セルフケアへのアクセスを提供する対象となるユーザを検索します。

ステップ 3 [エンドユーザ（End User）] セクションで、ユーザにパスワードと PIN が設定されていることを確認します。

通常、これらのクレデンシャルは、新しいユーザが追加されるときに入力されます。

ステップ 4 [権限情報（Permission Information）]セクションで[アクセスコントロールグループに追加（Add to Access Control Group）]をクリックします。

ステップ 5 [検索（Find）] をクリックして、[標準 CCM エンドユーザ（Standard CCM End Users）] グループまたは [標準 CCM エンドユーザ（Standard CCM End Users）] ロールが含まれているカスタム グループを選択します。

（注） アクセス制御グループの編集方法、およびアクセス制御グループのロールの割り当ての詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の「ユーザ アクセスの管理」の章を参照してください。

ステップ 6 **保存**を選択します。

セルフケア ポータル オプションの設定

ポータルにアクセスするユーザが使用できる設定オプションを制御するためにセルフケア ポータル エンタープライズ パラメータを設定するには、次の手順に従います。

始める前に

ユーザに対するセルフケア ポータルへのアクセス権の付与 （786 ページ）

手順

ステップ 1 [Cisco Unified Communications Manager の管理（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 [セルフケアポータル パラメータ（Self Care Portal Parameters）] で、ドロップダウンリストから使用可能なサーバのいずれかを選択して、[セルフケアポータル デフォルトサーバ（Self Care Portal Default Server）] を設定します。

このパラメータは、組み込みのセルフケアのオプション ページを表示するのに使用する Cisco Unified CM サーバの Jabber を決定します。 [なし（None）]を選択すると、Jabber はパブリッシャをデフォルトとします。

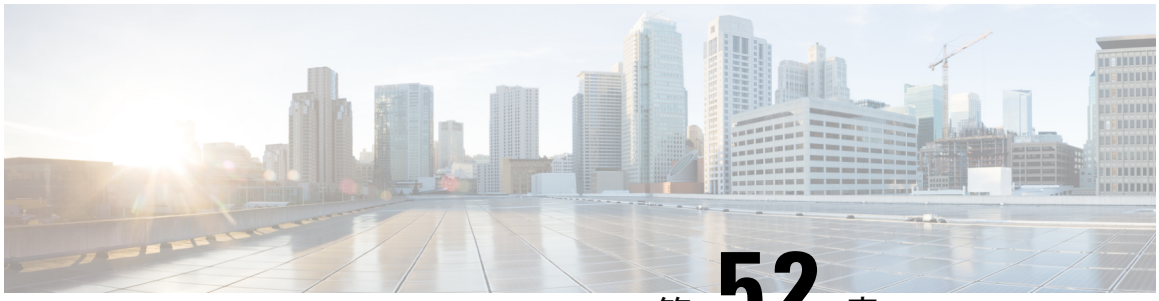
ステップ 3 [セルフケアポータル パラメータ（Self Care Portal Parameters）] のその他のフィールドを設定して、ポータルの機能を有効または無効にします。 フィールドの詳細については、エンタープライズ パラメータのヘルプを参照してください。

ステップ 4 **保存**を選択します。

セルフ ケア ポータルの連携動作と制約事項

次の表に、セルフケア ポータルの機能の連携動作と制約事項を示します。

機能	連携動作または制限事項
アクティベーション コードによるデバイスのオンボーディング	ユーザがセルフケアポータルを使用して電話機をアクティブにできるようにする場合は、**[アクティベーション可能状態になっている電話機を表示]** のエンタープライズ パラメータを **True** に設定する必要があります (これはデフォルトの設定です)。 この機能を使用すると、ユーザはセルフケアポータルにログインしてアクティベーション コードを取得できます。 電話機のビデオカメラを使用してバーコードをスキャンすることもできますし、電話機をアクティブにして登録するために手動で電話機にコードを入力することもできます。 アクティベーション コードの詳細については、『*Cisco Unified Communications Manager* のシステム設定ガイド』の「アクティベーション コード経由でのデバイスオンボード」の章を参照してください。
認証されたユーザの https 要求	認証されたユーザが `https://{CUCM_address}/ucmuser/hostAlive/{host}` に要求すると、次のようになります。 • 要求が `http:{host}/` を取得するのに成功した場合、または要求が `{host}` を ping できる場合、Cisco Unified Communications Manager は文字列「`true`」を返します。 • 要求が失敗した場合、Cisco Unified Communications Manager は文字列「`false`」を返します。
Extension Mobilityの最大ログイン数	エンドユーザがセルフケア ポータル内でこの設定を行うことができるようにするには、管理者は、Cisco Unified CM Administration の関連ユーザ プロファイルで **[エンド ユーザによるExtension Mobilityの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）]** オプションの設定をオンにする必要があります。 このオプションがユーザ プロファイル内で選択されている場合、プロファイルを使用するすべてのユーザについて、セルフケア ポータル設定は、Cisco Unified Communications Manager の [**クラスタ間最大ログイン時間（Intra-cluster Maximum Login Time**）] および [**クラスタ間および最大ログイン時間（Inter-cluster and Maximum Login Time**）] サービス パラメータの管理者設定値をオーバーライドします。



第 52 章

緊急コール ハンドラ

緊急コールハンドラの概要

緊急コール ハンドラにより、当該地域の条例および規制に準拠してテレフォニー ネットワークで緊急コールを管理できます。

緊急電話をかけるときは、次のことが必要です：

- 緊急電話は、発信者の位置に基づいて、地域の公安応答窓口（PSAP）にルーティングする必要があります。
- 発信者の位置情報は緊急オペレータ端末に表示されなければならない。 位置情報は自動位置情報（ALI）データベースから取得できます。

発信者の位置は、緊急ロケーション識別番号（ELIN）によって決まります。 ELIN は、緊急コールが切断された場合や、PSAP が発信者と再度通話する必要がある場合に、緊急コール発信者に再接続するために使用できるダイヤルイン（DID）番号です。 緊急コールは、この番号に関連付けられている位置情報に基づいて PSAP にルーティングされます。

オフィス システムなどのマルチラインの電話システムの場合、電話機を ELIN グループに分類することで、複数の電話機を ELIN と関連付けることができます。 緊急コールハンドラの ELIN グループは、位置を識別します。 この ELIN グループの ELIN は、ALI データベースの場所にマップする必要があります。

各位置には、同時緊急コールに対応するために必要な数の ELIN が作成されている必要があります。 たとえば、5 つの同時コールをサポートするには、ELIN グループ内に 5 つの ELIN が必要です。

（注） 緊急コール ハンドラでは、クラスタあたり最大 100 個の ELIN グループがサポートされています。

ELIN が同じロケーションからの次の緊急コールに使用されるまで、ELIN の元の着信側へのマッピングがアクティブであることを確認します。 ELIN マッピングを使用しない場合、DN は最大 3 時間だけアクティブになります。

ELIN グループを使用するには、次のタイプの電話機が対応しています。

- SIP および SCCP IP Phone
- CTI ポート
- MGCP および SCCP アナログ電話機
- H.323 電話機

緊急コール ハンドラの前提条件

例

緊急コール ハンドラをネットワークに導入する前に、ALI 送信プロセスをテストすることを推奨します。 サービス プロバイダーと協力して、PSAP で ALI データを使用してご使用のネットワークに正常にコールバックできることをテストします。

ローカル PSAP からの ELIN 番号を予約します。 法令や規則は場所や企業によって異なるため、この機能を導入する前に、セキュリティに関するニーズと法的なニーズを調査します。

緊急コール ハンドラのタスク フロー

始める前に

- 緊急コール ハンドラの前提条件 （790 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	緊急コール ハンドラの有効化 （792 ページ）	Cisco Unified Communications Manager の緊急コール ハンドラ機能を有効にします。 緊急コール ハンドラは、基本的な

	コマンドまたはアクション	目的
		緊急コール機能を提供し、スタティック設定による電話場所割り当てを使用して、限られた場所をサポートします。指定場所の数を増やしたり、ダイナミックに場所割り当てをしたりといった高度な緊急コール機能が必要な場合は、Cisco Emergency Responder をご検討ください。
ステップ 2	緊急ロケーション グループの設定 （793 ページ）	特定のサイトまたは場所に対し、緊急場所（ELIN）グループを設定します。
ステップ 3	緊急ロケーション グループへのデバイス プールの追加 （793 ページ）	緊急ロケーション（ELIN）グループを使用するようにデバイス プールを設定します。
ステップ 4	（任意） 緊急ロケーション グループへのデバイスの追加 （794 ページ）	特定の緊急ロケーション（ELIN）グループを使用するように、特定のデバイスを設定します。 このデバイスに関連付けられたデバイス プール（ELIN）グループを使用する場合には、このセクションを無視できます。 （注） デバイス レベルで作成された設定は、デバイス プール レベルで作成されたいかなる設定も上書きします。
ステップ 5	ルート パターンとトランスレーション パターンの有効化 （795 ページ）	ルートパターンまたはトランスレーション パターンの緊急ロケーション（ELIN） サービスを有効にします。 **注意** 緊急コール ハンドラの設定により ELIN を変換する可能性があるため、発信元変換マスクはゲートウェイまたはトランクに設定されません。 （注） ルートパターンまたはトランスレーションパターンいずれかの有効化が必須ですが、両方の有効化も可能です。
ステップ 6	（オプション） ELIN グループの情報と電話の一括管理タスクを実行するには、次の手順を使用します。	このセクションでは、ELIN グループの情報を更新し、新しい ELIN グループに電話を追加する際に使用できる一括管理

	コマンドまたはアクション	目的
	• 緊急ロケーション グループ情報のインポート （796 ページ） • 緊急ロケーション グループ情報のエクスポート （797 ページ） • 新しい緊急ロケーション グループによる電話の更新 （798 ページ）	タスクについて説明します。 詳細については、『*Cisco Unified Communications Manager Administration Guide, Release 11.0(1)*』を参照してください。

緊急コール ハンドラの有効化

Cisco Unified Communications Manager の緊急コール ハンドラ機能を有効にします。 緊急コールハンドラは、基本的な緊急コール機能を提供し、スタティック設定による電話場所割り当てを使用して、限られた場所をサポートします。 指定場所の数を増やしたり、ダイナミックに場所割り当てをしたりといった高度な緊急コール機能が必要な場合は、Cisco Emergency Responder をご検討ください。

（注） Cisco Emergency Responder などの外部緊急コールソリューションをすでに使用している場合は、この機能を有効にしないでください。

この機能を有効にする場合は、外部機能を無効にしてください。

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。**[コールルーティング（Call Routing）] > [緊急コール ハンドラ（Emergency Call Handler）] > [緊急ロケーション（ELIN）グループ（Emergency Location （ELIN） Group）]**。

ステップ 2 [緊急ロケーション設定（Emergency Location Configuration）] ウィンドウから、以下のことを行います。

- 緊急コール ハンドラ機能を有効にするには、**[緊急ロケーション（ELIN）サポートの有効化（Enable Emergency Location (ELIN) Support）]** チェックボックスをオンにします。 デフォルト設定は「無効」です。 これを有効にすると、この機能に関連する設定が [関連設定（Related Settings）] ペインに表示されます。 この機能を動作させるには、これらの設定を行う必要があります。 これらの関連設定を行う方法の詳細については、次のタスクを参照してください。
- 緊急コール ハンドラ機能を無効にするには、**[緊急ロケーション（ELIN）サポートの有効化（Enable Emergency Location (ELIN) Support）]** チェックボックスをオフにします。

  （注） この機能を無効にすると、設定されているすべての関連する設定が削除されます。 設定されているすべての設定については、[関連設定（Related Settings）] ペインを参照してください。

（注） この機能を無効にすることを希望し、ELIN グループに関連付けられているデバイスが 500 を超える場合、機能を無効にする前に、関連付けを 500 未満になるまで手動で削除する必要があります。

ステップ 3 **[保存（Save）]** をクリックします。

緊急ロケーション グループの設定

特定のサイトまたは場所に対し、緊急場所（ELIN）グループを設定します。

始める前に

緊急コール ハンドラの有効化 （792 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）]** > **[緊急コール ハンドラ（Emergency Call Handler）]** > **[緊急ロケーション（ELIN）グループ（Emergency Location (ELIN) Group）]**。

ステップ 2 [緊急ロケーション（ELIN）グループの設定（Emergency Location (ELIN) Group Configuration）] ウィンドウで、[名前（Name）]フィールドにグループの名前を入力します。

ステップ 3 [番号（Number）]フィールドに、公安応答局（PSAP）に登録された DID 番号のプールを入力します。

ステップ 4 **[保存（Save）]** をクリックします。

緊急ロケーション グループへのデバイス プールの追加

緊急ロケーション（ELIN）グループを使用するようにデバイス プールを設定します。

始める前に

緊急ロケーション グループの設定 （793 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。**[システム（System）]** > **[デバイス プール（Device Pool）]**。

ステップ 2 [デバイス プールの検索と表示（Find and List Device Pools）] ウィンドウで、既存のデバイス プールを追加する場合、[検索（Find）] をクリックし、リストからデバイス プールを選択します。 新しいデバイス プールを追加するには、[新規追加] をクリックします。

ステップ 3 [デバイス プールの設定（Device Pool Configuration）] ウィンドウで、[緊急ロケーション（ELIN）グループ（Emergency Location (ELIN) Group）] ドロップダウン リストから、デバイス プールを追加する ELIN グループを選択します。 新しいデバイス プールを追加する場合、そのほかの必須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。

緊急ロケーション グループへのデバイスの追加

特定の緊急ロケーション（ELIN）グループを使用するように、特定のデバイスを設定します。このデバイスに関連付けられたデバイス プール（ELIN）グループを使用する場合には、このセクションを無視できます。

（注） デバイス レベルで作成された設定は、デバイス プール レベルで作成されたいかなる設定も上書きします。

（注） ELIN グループに追加するデバイスは、そのデバイスが配置されている特定の場所を表す ELIN グループに追加する必要があります。

始める前に

緊急ロケーション グループへのデバイス プールの追加 （793 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）]**。

（注） IP フォン以外のタイプの電話機を使用している場合は、そのタイプの電話機の関連設定ページに移動します。

ステップ 2 [電話の検索と一覧表示（Find and List Phones）]ウィンドウで、既存のデバイスを追加する場合は、[検索（Find）]をクリックし、設定するデバイスをリストから選択します。 新しいデバイスを追加する場合は、[新規追加] をクリックします。

ステップ 3 新しい電話機を追加する場合は、[電話機のタイプ（Phone Type）]ドロップダウン リストから追加する電話機のタイプを選択し、[次へ（Next）]をクリックします。

ステップ 4 [電話機の設定（Phone Configuration）]ウィンドウで、デバイスを追加する ELIN グループを [緊急ロケーション（ELIN）グループ（Emergency Location (ELIN) Group）] ドロップダウン リストから選択します。 新しいデバイスを追加する場合は、その他の必要なフィールドにも入力します。

ステップ 5 **[保存（Save）]** をクリックします。

ルート パターンとトランスレーション パターンの有効化

ルート パターンまたはトランスレーション パターンの緊急ロケーション（ELIN） サービスを有効にします。

（注） ルート パターンまたはトランスレーション パターンいずれかの有効化が必須ですが、両方の有効化も可能です。

始める前に

緊急ロケーション グループへのデバイスの追加 （794 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、次のいずれかのウィンドウを選択してください。

- ルート パターンを有効にするには、**[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。
- トランスレーションパターンを有効にするには、**[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 **[ルート パターンの検索と一覧（Find and List Route Patterns）]** または **[トランスレーション パターンの検索と一覧（Find and List Translation Patterns）]** のウィンドウで、[検索（Find）] をクリックし、リストからルートパターンまたはトランスレーションパターンを選択します。

ステップ 3 **[ルート パターン設定（Route Pattern Configuration）]** または **[トランスレーション パターン設定（Translation Pattern）]** ウィンドウで、**[緊急サービス番号（Is an Emergency Services Number）]** のチェックボックスをオンにします。

（注） 緊急コール ハンドラを使用し、Cisco Emergency Responder などその他外部の緊急コールのソリューションを使用しない場合のみ、このチェックボックスをチェックします。

ステップ 4 **[保存（Save）]** をクリックします。

緊急ロケーション グループと電話の一括管理

- 緊急ロケーション グループと電話の一括管理のタスク フロー （796 ページ）

緊急ロケーション グループと電話の一括管理のタスク フロー

このセクションでは、ELIN グループの情報を更新し、新しい ELIN グループに電話を追加する際に使用できる一括管理タスクについて説明します。 一括管理の詳細については、『*Cisco Unified Communications Manager Bulk Administration Guide, Release 11.0(1)*』を参照してください。

（注） 次の手順を実行する前に、緊急コール ハンドラ機能が有効であることを確認します。緊急コール ハンドラの有効化 （792 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	緊急ロケーション グループ情報のインポート （796 ページ）	一括管理ツールを使用して緊急ロケーション（ELIN）グループ情報をインポートします。
ステップ 2	緊急ロケーション グループ情報のエクスポート （797 ページ）	一括管理ツールを使用して緊急ロケーション（ELIN）グループ情報をエクスポートします。
ステップ 3	新しい緊急ロケーション グループによる電話の更新 （798 ページ）	複数の電話を検索して、一覧表示し、新しい緊急ロケーション（ELIN）グループを設定します。

緊急ロケーション グループ情報のインポート

一括管理ツールを使用して緊急ロケーション（ELIN）グループ情報をインポートします。

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。**[一括管理（Bulk Administration）] > [インポート/エクスポート（Import/Export）] > [インポート（Import）]**。

ステップ 2 [ファイル名（File Name）]ドロップダウン リストから、インポートする .tar ファイルの名前を選択して、[次へ（Next）]をクリックします。

ステップ 3 [インポートの設定（Import Configuration）]セクションに、.tar ファイルのすべてのコンポーネントが一覧表示されます。 ユーザがインポートするオプションの ELIN グループ関連のチェック ボックスをオンにします。

ステップ 4 ジョブをすぐに実行するか、後で実行するかを、対応するラジオボタンをクリックして選択します。

ステップ 5 選択したデータをインポートするためのジョブを作成するには、[送信（Submit）]をクリックします。 [ステータス（Status）] セクションのメッセージは、ジョブが正常に送信されたことを通知します。

ステップ 6 このジョブをスケジュール設定したり、アクティブにしたりするには、[一括管理（Bulk Administration）] メイン メニューの [ジョブ スケジューラ（Job Scheduler）] オプションを使用します。

緊急ロケーション グループ情報のエクスポート

一括管理ツールを使用して緊急ロケーション（ELIN）グループ情報をエクスポートします。

始める前に

緊急ロケーション グループ情報のインポート （796 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。**[一括管理（Bulk Administration）] > [インポート/エクスポート（Import/Export）] > [エクスポート（Export）]**。

ステップ 2 [データのエクスポート（Export Data）]ウィンドウの [ジョブ情報（Job Information）]ペインで、[Tar ファイル名（Tar File Name）]フィールドに拡張子を除いた .tar ファイル名を 入力します。 BPS は、このファイル名を使用して設定の詳細をエクスポートします。

（注） 一度にエクスポートされたすべてのファイルは、1 つ（.tar）にまとめられ、サーバからダウンロードできます。

ステップ 3 ELIN グループ情報をエクスポートするには、**[エクスポートするアイテムの選択（Select Items to Export）]** ペインで **[ELIN グループ（Elin Group）]** チェック ボックスをオンにします。

ステップ 4 （任意） 以下の手順を実行します。

- ELIN グループが設定されたデバイス プールをエクスポートするには、[デバイス プール（Device Pools）]チェックボックスをオンにします。
- ELIN グループが設定された電話機をエクスポートするには、[電話機（Phone）]チェックボックスをオンにします。

ステップ 5 [ジョブの説明（Job Descripton）]フィールドに、そのジョブに関して優先する説明を入力します。 「Export Configuration」 がデフォルトの説明です。

ステップ 6 対応するラジオボタンをクリックすることにより、ジョブを今すぐ実行するか後で実行するかを選択できます。

ステップ 7 選択したデータをエクスポートするジョブを作成するには、[送信（Submit）]をクリックします。 [ステータス（Status）]ペインのメッセージにより、ジョブが正常に送信されたことが通知されます。

ステップ 8 このジョブをスケジュール設定したり、アクティブにしたりするには、[一括管理（Bulk Administration）] メイン メニューの [ジョブ スケジューラ（Job Scheduler）] オプションを使用します。

新しい緊急ロケーション グループによる電話の更新

複数の電話を検索して、一覧表示し、新しい緊急ロケーション（ELIN）グループを設定します。

始める前に

緊急ロケーション グループ情報のエクスポート （797 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[一括管理（Bulk Administration）] > [電話（Phones）] > [電話の更新（Update Phone）] > [クエリ（Query）]** の順に選択します。

ステップ 2 [更新する電話の検索および一覧表示（Find and List Phones To Update）]ウィンドウで、検索のパラメータを設定し、[検索（Find）]をクリックします。

（注） すべての電話を更新するには、クエリを指定せずに、[検索（Find）]をクリックします。

ステップ 3 [更新する電話の検索および一覧表示（Find and List Phones To Update）]ウィンドウに選択した電話の詳細が表示されます。 [次へ（Next）]をクリックします。

ステップ 4 [電話の更新（Update Phones）]ウィンドウで、[緊急ロケーション（ELIN）グループ（Emergency Location (ELIN) Group）]のチェックボックスをオンにして、ドロップダウン リストから新規 ELIN グループを選択します。

ステップ 5 [送信（Submit）]をクリックします。

連携動作

機能	データのやり取り
サイレントコール拒否（Do Not Disturb Call Reject）	PSAP コールバックからのコールにより、接続先デバイスのサイレント（DND）設定が上書きされます。 DND 通話拒否が有効になっている場合、トランスレーション パターンを使用して緊急番号がダイヤルされると、ELIN がそのアウトバウンド緊急コールに関連付けられます。 コールが切断され、ELIN が PSAP コールバックを使用して呼び出された場合は、その電話機の DND 設定に関係なく、コールが電話機にルーティングされます。
すべてのコールの転送	PSAP コールバックからのコールにより、接続先デバイスの不在転送（CFA）設定が上書きされます。 電話機でCFAが有効になっており、トランスフォーメーションパターンを使用して緊急番号がダイヤルされると、ELIN がそのアウトバウンド緊急コールに関連付けられます。 コールが切断され、ELIN が PSAP コールバックを使用して呼び出された場合は、その電話機の CFA 設定に関係なく、コールが電話機にルーティングされます。
シングル ナンバー リーチ	PSAP コールバックは、シングル ナンバー リーチ（SNR）設定を無視します。 電話機で SNR が有効になっており、リモート接続先が携帯電話の番号を指している場合。 トランスレーション パターンを使用して緊急番号がダイヤルされると、ELIN がそのアウトバウンド緊急コールに関連付けられます。 コールが切断され、ELIN 番号が PSAP コールバックを使用して呼び出されると、コールはリモート接続先ではなく電話機にルーティングされます。

機能	データのやり取り
エクステンションモビリティ	PSAP コールバック コールでエクステンションモビリティ（EM）ステータスが考慮されます。 EM プロファイル クレデンシャルを使用してログインし、トランスフォーメーション パターンを使用して緊急番号をダイヤルすると、ELIN がそのアウトバウンド緊急コールに関連付けられます。 コールが切断され、ユーザがログインしている ELIN が PSAP コールバックを使用して呼び出されると、コールはコールを開始したデバイスにルーティングされます。 （注） これは、ユーザがまだログインしているデバイスです。
	PSAP コールバックの実行前にユーザが EM からログアウトすると、PSAP コールバックが失敗します。 EM プロファイル クレデンシャルを使用してログインし、トランスフォーメーション パターンを使用して緊急番号をダイヤルすると、ELIN がそのアウトバウンド緊急コールに関連付けられます。 コールが切断されPSAP コールバックを使用して呼び出された場合、ユーザがそれ以降にログアウトしていると、コールは開始されたデバイスにルーティングされず失敗します。
	ユーザが別のデバイスでログインした PSAP コールバック。 ユーザが電話機 A で EM プロファイル クレデンシャルを使用してログインし、トランスフォーメーション パターンを使用して緊急番号をダイヤルすると、ELIN がそのアウトバウンド緊急コールに関連付けられます。 コールが切断された場合は、ユーザが電話機 A からログアウトする必要があります。その後で、ユーザが同じプロファイルを使用して別の電話機（電話機 B）にログインし、ELIN が PSAP コールバックを使用して呼び出されると、コールは通常の優先順位の電話機 B にルーティングされます。これは、CFA 設定が無視され、DND 設定が無視されないことを意味します。
	複数のログインを使用した PSAP コールバック コール。 ユーザが電話機 A で EM プロファイル クレデンシャルを使用してログインし、トランスフォーメーション パターンを使用して緊急番号をダイヤルすると、ELIN 番号がそのアウトバウンド緊急コールに関連付けられます。 コールが切断され、ユーザが電話機 A にログインしたまま同じプロファイルを使用して別の電話機（電話機 B）にログインし、ELIN が PSAP コールバックを使用して呼び出されると、コールはコールを開始したデバイスである電話機 A にのみルーティングされます。

機能	データのやり取り
デバイス モビリティ	ローミング デバイスは、アウトバウンド緊急コールにローミング デバイス プールの ELIN グループを使用します。 デバイス モビリティが有効になっているデバイスをそのホームの場所からローミングの場所に移動し、ローミング デバイス プールに関連付けられるように IP サブネットを変更します。 トランスレーション パターンを使用して緊急番号がダイヤルされると、ELIN がそのアウトバウンド緊急コールに関連付けられます。 ELIN は、ローミング デバイス プールに関連付けられた ELIN グループに属しています。
共有電話	PSAP コールバックは、回線が複数のデバイスで共有されている場合でも、緊急コールを発信したデバイスでのみ鳴動します。 電話機 A と電話機 B が電話番号（DN）を共有します。 トランスレーション パターンを使用して緊急番号がダイヤルされると、ELIN がそのアウトバウンド緊急コールに関連付けられます。 コールが切断され、ELIN が PSAP コールバックを使用して呼び出されると、コールはコールを開始したデバイスである電話機 A にのみルーティングされます。

緊急コール ハンドラのトラブルシューティング

緊急コール ハンドラのトラブルシューティング シナリオ

このセクションでは、次の分野にある緊急コール ハンドラのトラブルシューティング シナリオについて説明します。

- 設定シナリオ
- 発信コールのシナリオ
- 着信コールのシナリオ

Configuration Scenarios

緊急コールがビジー信号を受信し、ルーティングされない

問題：

緊急コールがビジー信号を受信し、ルーティングされません。

ソリューション:

緊急コールをダイヤルしているユーザにリオーダー音が流れている場合は、以下のチェックを実行してください。

- 緊急コールのトランスレーションまたはルート パターンが使用されているかどうかを確認します。 これには、CSS 上のデバイスまたは電話のチェックが必要な場合があります。
- 緊急コールのトランスレーションまたはルート パターンの [緊急サービス番号です（Is an Emergency Services Number）]チェック ボックスがオンになっており、それがゲートウェイに正しくルーティングされていることを確認します。

緊急コールをダイヤルしているユーザが正しいゲートウェイまたは Public Service Answering Point（PSAP）に到達していない場合は、電話またはデバイスの設定またはデバイス プール設定が正しい Emergency Location（ELIN）グループを使用して設定されていることを確認します。

リオーダー音が流れている最中に緊急場所の番号が外部からダイヤルされる

問題：

リオーダー音が流れている最中に緊急場所（ELIN）の番号が外部からダイヤルされます。

原因:

このケースでは、ELIN が発信者の場所を特定するために使用される DID として設定されています。 これは、どの電話機でも、他のどの目的にも使用すべきではありません。

ソリューション：

ELIN の設定情報を確認し、DID として設定されている ELIN を設定解除してください。

Outgoing Calls Scenarios

発信緊急コールに発信者番号が緊急ロケーション番号として含まれていない

問題：

発信緊急コールに、発信者番号が緊急ロケーション（ELIN）番号として含まれていません。

原因:

この ELIN のトランスレーション パターンまたはルート パターンが正しく設定されていませんでした。

ソリューション:

この ELIN のトランスレーション パターンまたはルート パターンが正しく設定されているかどうかを確認し、該当するトランスレーション パターンまたはルート パターンの設定ページで、[緊急サービス番号である（Is an Emergency Services number）]チェック ボックスがオンになっていることを確認します。

発信緊急コールに変更された緊急場所の番号が含まれる

問題：

発信緊急コールに変更された緊急場所の番号（ELIN）が含まれています。

原因:

発信トランクまたはルート リストに ELIN では必要のない余分な変換が含まれています。

ソリューション:

コールに適用された変換を確認し、発信トランクまたはルートリストにELINに必要な変換のみが存在していることを確認します。

Incoming Calls Scenarios

着信 PSAP コールバック コールが失敗する

問題：

着信 PSAP コールバック コールが失敗します。

原因:

元の緊急コールを発信したデバイスが正しく登録されていません。

ソリューション:

元の緊急コールを発信したデバイスがまだ登録されているかどうか、すべてのエクステンションモビリティが機能しているかどうかを確認してください。

着信 PSAP コールバックコールが予測どおりにルーティングされない

問題：

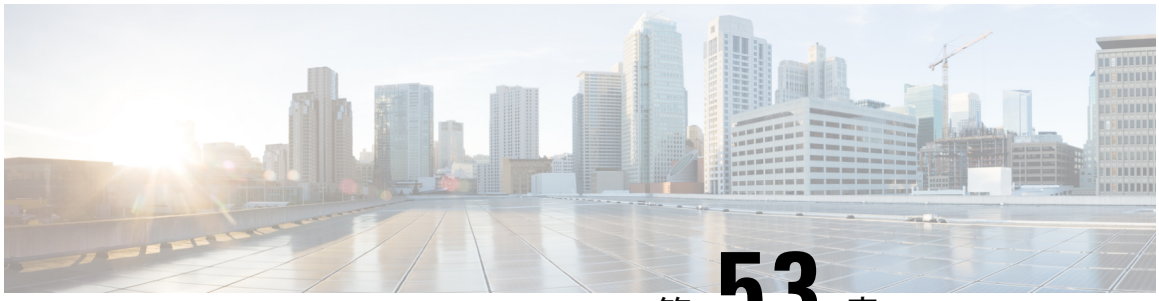
着信 PSAP コールバックコールが予測どおりにルーティングされません。

原因:

緊急ロケーション（ELIN）番号が元の発信者番号と一致しません。

ソリューション:

ELIN に対応する元の発信者を正常に逆マッピングするには、これら 2 つの番号が一致する必要があります。すでに着信ゲートウェイまたはトランクで変換があり、有意な数字が設定されている場合、最終的に変換された着信側が ELIN 番号に一致することを確認します。



第 53 章

RedSky を使用した緊急コールの処理

RedSky を使用した緊急コールの処理の概要

重要 この機能は、リリース 12.5(1) SU7 および 14 SU3 以降に適用されます。

Unified Communications Manager に統合された RedSky ソリューションにより、クライアントは、キャンパス内やリモート環境に関係なくすべての従業員に対して、9-1-1 緊急コールカバレッジのアクティブな場所を設定し、緊急応答者にコールを送信できます。

エンドポイントには、RedSky サーバーから受信したロケーション URI が、HTTP 対応ロケーション配信（HELD）リクエストへの応答として保存されます。 緊急番号 9-1-1 が Webex からダイヤルされると、Unified Communications Manager は、INVITE メッセージ内で以前に保存されているロケーション URI を地理位置情報ヘッダーとして取得し、着信側デバイスの場所に対応する地理位置情報ヘッダーとしてロケーション URI を含む発信 INVITE を使用して RedSky サーバーにコールをルーティングします。 RedSky サーバーは、適切な ELIN で置き換え、緊急送信用の公安応答局（PSAP）にコールを送信します。 E911 Anywhere は、SMS テキスト、メール、およびセキュリティデスク画面アラートを含むコール通知を同時に送信します。

Cisco Emergency Responder は、デバイスが企業全体を通じて移動する際に、すべてのデバイスのディスパッチ可能な場所を自動的に検出して追跡し、E911 規制に準拠できるようにします。 Emergency Responder は、スイッチポートまたはアクセスポイントまたは IP サブネットまたは手動設定によって Cisco IP 電話を追跡します。 Emergency Responder では電話機のステータス（構内、構外、位置未確認）を保持し、ALI（自動ロケーション情報）または ELIN 情報を RedSky に渡します。 電話機のユーザーは Unified CM を使用して、緊急コールを RedSky および指定した緊急プロバイダーにルートします。

構外の電話機の場合、ユーザーの電話機の現在の場所が以前に定義されていない場合、ユーザーは Emergency Responder の構外ユーザーの Web ページに移動して新しい場所を作成しま

す。新しい場所が定義され、アドレスが確認された後、構外の電話機から発信した緊急コールは RedSky を介して完了します。

（注） 従業員が組織サイトの構内で作業している場合は、そのユーザーの場所を発信元システム管理者によって定義することをお勧めします。

緊急コールの処理の設定タスクフロー

管理者は、次のタスクを使用して、9-1-1 緊急コールの動的な位置を設定し、緊急応答者にコールを転送できます。

手順

	コマンドまたはアクション	目的
ステップ 1	RedSky サーバーの設定	RedSky サーバーにコールをルーティングする SIP トランクを作成します。
ステップ 2	サービス プロファイルの設定	緊急コールのエンドユーザーのサービスプロファイルの詳細を追加します。
ステップ 3	サービス プロファイルを割り当てる	作成したサービスプロファイルを Webex クライアントエンドユーザーに割り当てます。
ステップ 4	コールのルーティングのための SIP ルートパターンの設定	ドメイン名を使用して SIP ルートパターンを作成し、前に作成した SIP トランクと同じルートを関連付けます。

RedSky サーバーの設定

RedSky サーバーにコールをルーティングする SIP トランクを作成するには、次の手順を使用します。

（注） ステップ 7、8、および 9 は、オンプレミスの統合でのみ必要です。

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 [新規追加] 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。

ステップ 5 **[SIP 情報（SIP Information）]** 領域で、**[宛先アドレス（Destination Address）]** テキストボックスに、SIP トランクに接続するサーバーまたはエンドポイントの RedSky サーバーの 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。

ステップ 6 **[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、SIP トランクセキュアプロファイルの非セキュアプロファイルが割り当てられます。

ステップ 7 （任意） **[SIP プロファイル（SIP Profile）]** ドロップダウンリストから、Ping オプションを有効にした RedSky SIP プロファイルを割り当てます。

ステップ 8 （任意） **[スクリプトの正規化（Normalization Script）]** 領域の **[スクリプトの正規化（Normalization Script）]** ドロップダウンから、**redsky-alternate-id-interop** を選択します。

ステップ 9 （任意） **[パラメータ名（Parameter Name）]** と **[パラメータ 値（Parameter Value）]** には、それぞれの情報を入力します。

パラメータ名では、次の入力がサポートされています。

- **RedSky-CustomerID**: これは必須フィールドです。 これは RedSky の管理ページの HELD ID です。 これは、発信元の顧客アカウントを識別するために使用されます。
- **Alternate-Callback-Number**: これはオプションのフィールドです。 このフィールドには、緊急コールのオプションのコールバック番号が挿入されます。 これは、コールバックにダイレクト インワード ダイヤル（DID）番号が割り当てされていない発信者に使用する必要があります。
- **Ext-Length**: これはオプションのフィールドです。 このパラメータは、E.164 以外の番号付け規則を使用している顧客に使用されます。 このパラメータは、RedSky E911-User-ID ヘッダーに非 E.164 を入力します。
- **Agent-Ext**：これはオプションのフィールドです。 このパラメータは、一致桁数に基づいてエージェントの内線番号を識別します。 このパラメータを入力すると、エージェントの通話相手が RedSky E911-User-ID ヘッダーに挿入されます。

  このスクリプトは、参照する内線番号の先頭の数字だけを参照するわけではありません。たとえば、Agent-Ext が「5」に設定されている場合、12345678 は一致しますが、12345678 は先頭の数字として 5 がありません。

Agent-Ext が 100200 に設定されている場合、100200 が先頭の数字ではなくても、123410020088 が一致します。

Agent-Ext が 12 に設定されている場合、12 が含まれていないため、446658787 は一致しません。

ステップ 10 **[保存（Save）]** をクリックします。

サービス プロファイルの設定

緊急コール用にエンドユーザーのサービスプロファイルの詳細を追加するには、次の手順を使用します。

始める前に

- 宛先を RedSky サーバーとして使用して SIP トランクを作成し、Ping オプションを有効にした SIP プロファイルを作成する必要があります。 SIP ルートパターンは、必要なドメイン名（RedSky）を使用して作成する必要があります。また、以前に作成したトランクに関連付けられている必要があります。
- サービスプロファイルは、所有者のユーザ ID が指定されている場合にのみ、特定のデバイスに適用されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザー管理（User Management）]** > **[ユーザー設定（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] 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）]** と **[説明（Description）]** を入力します。

（注） 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。 **[サービスプロファイルの設定（Service Profile Configuration）]** ウィンドウのフィールドは、設定する UC サービスによって異なります。

ステップ 4 **[緊急コールプロファイル（Emergency Calling Profile）]** セクションで、次の手順を実行します。

a) [緊急コールの有効化（Enable Emergency Calling）] をオンにして、エンドポイントとソフトクライアントの設定パラメータを有効にして場所を更新し、緊急コールを緊急コールサービスプロバイダに送信します。

b) アカウントが作成され、**[組織 ID（Organization ID）]** および **[秘密（Secret）]** フィールドでサービスが有効になっている場合は、緊急コールサービスプロバイダから提供された企

業 ID とパスフレーズを入力します。 たとえば、RedSky によって提供される 32 文字の英数字文字列です。

c) 緊急コールサービスプロバイダ認証サービスで必要なパスフレーズを **[秘密（Secret）]** フィールドに入力しますたとえば、RedSky によって提供される 16 文字の英数字文字列です。

d) デバイスがリクエストに使用する URL を入力し、**[場所の URL（Location URL）]** フィールドに場所を設定します。

e) **[緊急サービス番号（Emergency Service Numbers)]** を入力します。 デフォルトでは、911、933 が各番号をコンマで区切って入力されます。

（注） Webex クライアントが、緊急番号で設定された緊急パターンをダイヤルすると、地理位置情報ヘッダーとともに SIP トランクに設定されている RedSky サーバーにルーティングされます。

ステップ 5 [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 6 **[保存（Save）]** をクリックします。

サービス プロファイルを割り当てる

作成したサービスプロファイルを Webex クライアントのエンドユーザーに割り当てるには、次の手順を使用します。 Webex が Unified CM に登録されていない場合、エンドユーザーはアクティブにならず、緊急コールを RedSky にルーティングしません。

サービスプロファイルをエンドユーザーに適用し、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。 組織内の異なるユーザーグループごとに異なるサービスプロファイルを設定でき、その結果、各グループのユーザーが、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。

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 **[ユーザーの検索と一覧表示（Find and List Users）]** ウィンドウで、次のタスクのいずれかを実行します。

a) 新しいユーザを設定するには、**[新規追加（Add New）]** をクリックします。

b) **[ユーザーを次の条件で検索（Find Users Where）]** フィールドでフィルタを指定した後、**[検索（Find）]**をクリックしてユーザーのリストを取得します。

（注） デバイスとユーザーの関連付けの詳細については、Cisco Emergency Responder Administration Guideの「デバイスをエンドユーザーに関連付ける」のセクションを参照してください。

ステップ 3 **[サービス設定（Service Settings）]** セクションで、**[UC サービスプロファイル（UC Service Profile）]** ドロップダウンリストから、RedSky サービスプロファイルを選択します。

ステップ 4 [エンドユーザの設定（End User Configuration）]ウィンドウでその他のフィールドに入力します。 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 5 **[保存（Save）]** をクリックします。

コールのルーティングのための SIP ルートパターンの設定

ドメイン名を使用して SIP ルートパターンを作成し、前に作成した SIP トランクと同じルートパターンを関連付ける場合は、次の手順を実行します。

緊急プロバイダーにルーティングされる緊急コールはすべて、ルートパターンと一致する必要があります。ルートパターンによって、コールが RedSky サーバに到達するルートグループ、ルートリスト、SIP トランクまたは PRI ゲートウェイに送信されます。

PRI: RedSky は、顧客にアカウント固有のアクセス番号を提供します。 この場合、番号は顧客 ID、発呼側はユーザリファレンスです。 これは、従来の RP/RG/RL/GW の冗長性に従います。 発呼側の番号は RedSky ユーザの ID と一致する必要があります。

RedSky サーバーに接続するには、SIP トランクを使用することをお勧めします。 専用インスタンスでは、これはデフォルトの方法です。 Unified Communications Manager オンプレミスをオンプレミスで導入している顧客には、RedSky サーバーに到達するために使用するルートパターンを作成する前に、SIP トランク、ルートグループ、およびルートリストを設定する必要があります。

SIP トランクを使用する場合、管理者は事前に定義された LUA スクリプトを使用して、顧客の識別を適切に行う必要があります。 Unified CM 展開の場合、スクリプトをアップロードして SIP トランクに適用する必要があります。 LUA スクリプトでは、RedskyOrgID である 1 つのパラメータのみを使用できます。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）]** > **[SIP ルートパターン（SIP Route Pattern）]** を選択します。

ステップ 2 RedSky ルート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 **[パターンの使用法（Pattern Usage）]** ドロップダウンから **[ドメインルーティング（Domain Routing）]** を選択します。

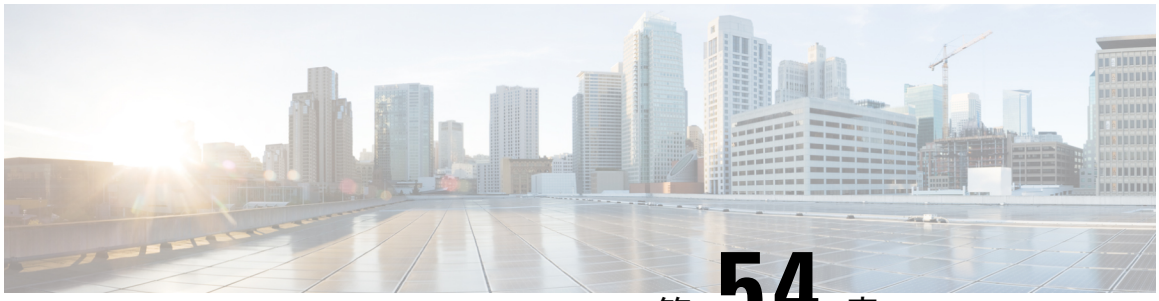
ステップ 4 IPv4 と IPv6 アドレスのどちらを展開するかに応じて、**IPv4 パターン**と **IPv6 パターン** フィールドにルート文字列を入力します。

ステップ 5 **[SIP Trunk/Route List*（SIP トランク/ルートリスト*）]** ドロップダウンリストで RedSky SIP トランクを選択します。

ステップ 6 （任意）**[編集（Edit）]** リンクをクリックして、[トランクの設定（Trunk Configuration）]の詳細を表示または変更します。

ステップ 7 [SIPルートパターンの設定（SIP Route Pattern Configuration）] ウィンドウで、残りのフィールドを入力します。 フィールドの詳細については、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 54 章

エンタープライズ グループ

エンタープライズグループの概要

エンタープライズ グループを設定すると、Cisco Unified Communications Manager は、データベースを外部 LDAP ディレクトリと同期するときにユーザ グループを含めます。 Cisco Unified CM の管理では、[ユーザグループ（User Groups）] ウィンドウで同期されたグループを表示できます。

この機能は、管理者が以下を行う場合にも役立ちます。

- 機能のコメント セット（たとえば、セールス チームやアカウンティング チーム）と同様の特性を持つユーザのプロビジョニング。
- 特定のグループのすべてのユーザを対象にしたメッセージの送信。
- 特定のグループのすべてのメンバーへの統一されたアクセスの設定

この機能は、Cisco Jabber ユーザが共通特性を共有するユーザの連絡先リストをすばやく作成するのにも役立ちます。 Cisco Jabber ユーザは、外部 LDAP ディレクトリでユーザ グループを検索し、それらを連絡先リストに追加できます。 たとえば、Jabber ユーザは外部 LDAP ディレクトリを検索してセールス グループを連絡先リストに追加することで、すべてのセールス チーム メンバーを連絡先リストに追加することができます。 グループが外部ディレクトリで更新されると、ユーザの連絡先リストは自動的に更新されます。

エンタープライズ グループは、Windows 上の Microsoft Active Directory で外部 LDAP ディレクトリとしてサポートされています。

（注） エンタープライズ グループ機能を無効にすると、Cisco Jabber ユーザは、エンタープライズ グループを検索したり、自分の連絡先リストに追加済みのグループを表示したりできません。ユーザがログイン中にその機能を無効にすると、そのユーザがログアウトするまでグループは表示されます。 ユーザが再度ログインすると、グループは表示されません。

セキュリティ グループ

セキュリティ グループは、エンタープライズ グループのサブ機能です。 Cisco Jabber ユーザは、セキュリティ グループを検索して、自分の連絡先リストに追加できます。 この機能を設定するには、管理者がカスタマイズしたLDAPフィルタを設定し、設定されたLDAPディレクトリの同期に適用する必要があります。 セキュリティ グループは、Microsoft Active Directory でのみサポートされています。

許可されるエントリの最大数

エンタープライズグループを設定するときは、グループを処理する連絡先リストの最大値を設定してください。

- 連絡先リストで許可されるエントリの最大数は、連絡先リスト内のエントリ数と、すでに連絡先リストに追加されているグループ内のエントリ数の合計です。
- 連絡先リストの最大エントリ数=（連絡先リストのエントリ数）+（グループのエントリ数）
- エンタープライズグループ機能が有効になっている場合、連絡先リストのエントリ数が許可されている最大エントリ数より少ない場合、Cisco Jabber ユーザはグループをコンタクトリストに追加できます。機能が無効になっているときに許容される最大エントリ数を超えると、その機能が有効になるまでユーザは制限されません。 機能が有効になってからユーザが引き続きログインすると、エラーメッセージは表示されません。ユーザがログアウトして再度ログインすると、余分な項目をクリアするように求めるエラーメッセージが表示されます。

エンタープライズ グループの前提条件

この機能は、以下の条件でLDAPディレクトリの同期スケジュールを設定していることを前提としています。 LDAP ディレクトリ同期を設定方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Import Users from LDAP Directory」の章を参照してください。

- Cisco DirSync サービスが有効になっている必要があります。
- LDAPディレクトリ同期には、ユーザとグループの両方が含まれている必要があります。

- 通常のLDAPディレクトリ同期は、[LDAPディレクトリ同期スケジュール(LDAP Directory Synchronization Schedule)]で設定されているとおりにスケジュールされている必要があります。

サポートされる LDAP ディレクトリ

エンタープライズ グループでは、Microsoft Active Directory のみがサポートされています。

エンタープライズ グループの設定タスク フロー

エンタープライズグループ機能を設定するためにこれらのタスクを完了して下さい。

手順

	コマンドまたはアクション	目的
ステップ 1	LDAPディレクトリからのグループ同期の確認 （815 ページ）	LDAPディレクトリの同期にユーザとグループの両方が含まれていることを確認します。
ステップ 2	エンタープライズ グループの有効化（816 ページ）	Cisco Jabber ユーザが Microsoft Active Directory のエンタープライズ グループを検索して自分の連絡先リストに追加できるようにするには、次のタスクを実行します。
ステップ 3	セキュリティグループを有効にする（817 ページ）	（任意）Cisco Jabber ユーザがセキュリティ グループを検索して自分の連絡先リストに追加できるようにするには、次のタスク フローを完了します。
ステップ 4	ユーザ グループの表示 （819 ページ）	（オプション）Cisco Unified Communications Manager データベースと同期する エンタープライズ グループおよびセキュリティ グループを表示します。

LDAP ディレクトリからのグループ同期の確認

この手順を使用して、LDAPディレクトリの同期にユーザとグループの両方が含ま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。**サーバ** > **LDAP** > **LDAPディレクトリ**

ステップ 2 [検索（Find）]をクリックし、エンタープライズ グループを同期する LDAP ディレクトリを選択します。

ステップ 3 [同期（Synchronize）]フィールドで [ユーザとグループ（Users and Groups）]が選択されていることを確認します。

ステップ 4 [LDAPディレクトリの設定（LDAP Directory configuration）] ウィンドウの残りのフィールドに入力します。フィールドとその設定のヘルプについては、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。

エンタープライズ グループの有効化

LDAP ディレクトリ同期にエンタープライズグループを含めるようにシステムを設定します。

手順

ステップ 1 Cisco Unified CM の管理から、**[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）]で、[Cisco IM and Presenceでのディレクトリグループの操作（Directory Group Operations on Cisco IM and Presence）]パラメータを [有効（Enabled）]に設定します。

ステップ 3 [プレゼンス情報を許可するためにサイズ設定された最大エンタープライズグループ（Maximum Enterprise Group Sized to allow Presence Information）]パラメータの値を入力します。 許可される範囲は 1 ～ 200 ユーザで、デフォルト値は 100 ユーザです。

ステップ 4 **[エンタープライズグループの同期モード（Syncing Mode for Enterprise Groups）]** ドロップダウン リストから、定期的に実行する LDAP 同期を **[なし（None）]**、**[差分同期（Differential Sync）]**、**[完全同期（Full Sync）]** から選択して設定します。

（注） これらのフィールドの構成の詳細については、エンタープライズパラメータの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。

セキュリティグループを有効にする

Cisco Jabber ユーザがセキュリティ グループを自分の連絡先リストに追加できるようにする場合は、以下のオプションのタスクを実行して、セキュリティ グループを LDAP ディレクトリ同期に追加します。

（注） セキュリティ グループの同期は、Microsoft Active Directory からのみ実行できます。

（注） 最初の同期がすでに発生した Cisco Unified Communications Manager では、LDAP ディレクトリの既存の構成に新しい設定を追加できません。

手順

	コマンドまたはアクション	目的
ステップ 1	セキュリティ グループ フィルタの作成（817 ページ）	ディレクトリ グループとセキュリティ グループの両方をフィルタ処理する LDAP フィルタを作成します。
ステップ 2	LDAPディレクトリからセキュリティグループを同期する （818 ページ）	新しい LDAP フィルタを LDAP ディレクトリ同期に追加します。
ステップ 3	セキュリティグループのための Cisco Jabber の設定 （819 ページ）	既存のサービス プロファイルを更新して、そのサービス プロファイルに関連付けられた Cisco Jabber ユーザに、セキュリティ グループを検索および追加するためのアクセス権が付与されるようにします。

セキュリティ グループ フィルタの作成

セキュリティ グループをフィルタリングする LDAP フィルタを作成します。

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** > **LDAP** > **ldap フィルタ**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [フィルタ名]ボックスに一意の名前を入力します。 例えば、`syncSecurityGroups`。

ステップ 4 **[フィルタ（Filter）]** ボックスに `(&(objectClass=group)(CN=*))` と入力します。

ステップ 5 **[保存（Save）]** をクリックします。

LDAP ディレクトリからセキュリティグループを同期する

LDAP ディレクトリ同期にセキュリティ グループ フィルタを追加し、同期を完了します。

（注） 最初の LDAP 同期がすでに発生している場合、Cisco Unified Communications Manager では、LDAP ディレクトリの既存の構成に新しい設定を追加できません。

（注） LDAP ディレクトリ同期を新しく設定する方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure End Users」の項目を参照してください。

始める前に

セキュリティ グループ フィルタの作成 （817 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）]** > **[LDAP（LADP）]** > **[LDAP ディレクトリ（LDAP Directory）]** 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 LDAP ディレクトリを作成します。
- **[検索（Find）]** をクリックして、同期されるセキュリティ グループから LDAP ディレクトリを選択します。

ステップ 3 [**グループの 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、作成したセキュリティ グループ フィルタを選択します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 **[LDAP ディレクトリの構成（LDAP Directory Configuration）]** ウィンドウの残りのフィールドを設定します。 フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 6 **[完全同期を今すぐ実施（Perform Full Sync Now）]** をクリックして、すぐに同期します。 これを行わない場合には、セキュリティ グループはスケジュールされた LDAP 同期が次に発生した際に同期されます。

セキュリティグループのための Cisco Jabber の設定

既存のサービスプロファイルを更新して、そのサービスプロファイルに関連付けられている Cisco Jabberユーザが LDAPディレクトリから自分の連絡先リストにセキュリティグループを追加できるようにします。

（注） 新しいサービス プロファイルを設定し、Cisco Jabber ユーザに割り当てる方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の章「Configure Service Profiles」を参照してください。

始める前に

LDAP ディレクトリからセキュリティグループを同期する （818 ページ）

手順

ステップ 1 **[サービス プロファイルの設定（Service Profile Configuration）]** ウィンドウの残りのフィールドに入力します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ 2 **[検索（Find）]** をクリックし、Jabber ユーザが使用するサービス プロファイルを選択します。

ステップ 3 **[ディレクトリ プロファイル（Directory Profile）]** で、**[Jabber にセキュリティ グループの検索と追加を許可（Allow Jabber to Search and Add Security Groups）]** チェックボックスをオンにします。

ステップ 4 **[保存]** をクリックします。
このサービスプロファイルに関連付けられた Cisco Jabber ユーザは、セキュリティグループを検索して追加できるようになります。

ステップ 5 Cisco Jabber ユーザが使用するすべてのサービスプロファイルに対して、この手順を繰り返します。

ユーザ グループの表示

次の手順を使用して、Cisco Unified Communications Manager データベースと同期されている エンタープライズグループおよびセキュリティグループを表示できます。

手順

ステップ 1 Cisco Unified CM Administration で、次のいずれかを選択します。**ユーザ管理** > **ユーザ設定** > **ユーザ・グループ**。
[ユーザ グループの検索/一覧表示（Find and List User Group）] ウィンドウが表示されます。

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。
検索条件に一致するユーザ グループのリストが表示されます。

ステップ 3 ユーザグループに属するユーザの一覧を表示するには、必要なユーザグループをクリックします。
[ユーザ グループの設定（User Group Configuration）] ウィンドウが表示されます。

ステップ 4 検索条件を入力して **[検索（Find）]** をクリックします。
検索条件に一致するユーザのリストが表示されます。

リスト内のユーザをクリックすると、**[エンド ユーザの設定（End User Configuration）]** ウィンドウが表示されます。

エンタープライス グループの導入モデル（Active Directory）

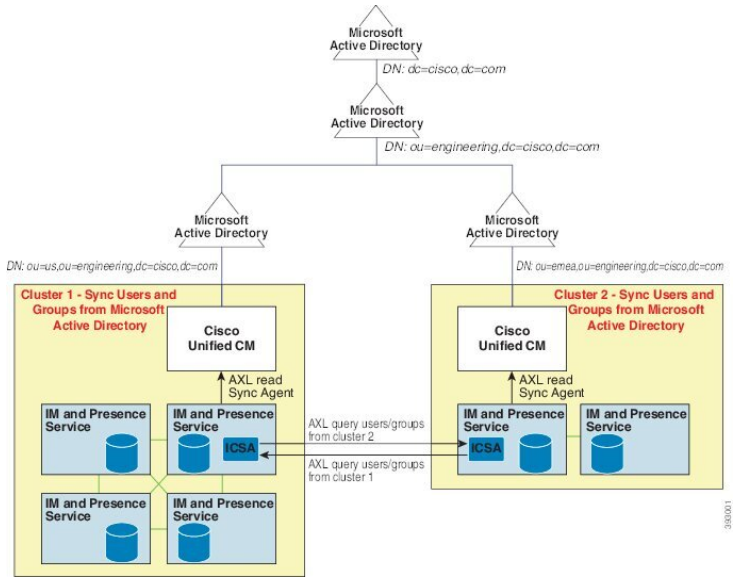
エンタープライズ グループ機能は、Active Directory 用に次の 2 つの導入オプションを提供します。

重要 Cisco Intercluster Sync Agent サービス経由でデータを同期する前に、クラスタ 1 とクラスタ 2 に、UserGroup レコード、UserGroupMember レコード、UserGroupWatcherList レコードの一意のセットが含まれていることを確認します。 両方のクラスタにレコードの一意のセットが含まれている場合、同期後には両方のクラスタにすべてのレコードのスーパーセットが含められています。

エンタープライズ グループ導入モデル 1

この導入モデルでは、クラスタ 1 とクラスタ 2 が Microsoft Active Directory からの異なるユーザとグループのサブセットを同期します。 Cisco Intercluster Sync Agent サービスは、データをクラスタ 2 からクラスタ 1 に複製して、ユーザとグループの完全なデータベースを作成します。

図 *12* : エンタープライズ グループ導入モデル *1*



エンタープライズ グループ導入モデル 2

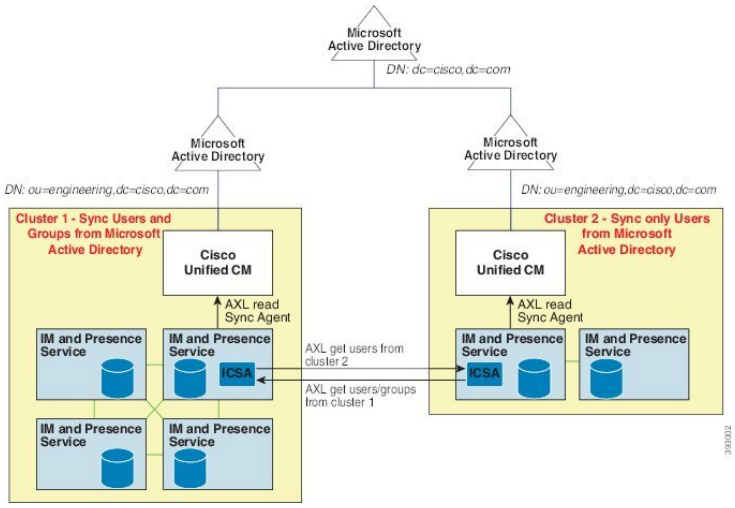
この導入モデルでは、クラスタ 1 が Microsoft Active Directory からのすべてのユーザとグループを同期します。 クラスタ 2 は、Microsoft Active Directory からのユーザのみを同期します。 Cisco Intercluster Sync Agent サービスは、グループ情報をクラスタ 1 からクラスタ 2 に複製します。

注意 この導入モデルを使用する場合は、1 つのクラスタ内のグループ データだけが同期されていることを確認します。 そうでない場合は、エンタープライズ グループ機能が想定どおりに機能しません。

[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > **[プレゼンス（Presence）]** > **[クラスタ間設定（Inter-Clustering）]** ウィンドウで設定を確認できます。

クラスタ間ピアテーブルで **[エンタープライズグループLDAP設定（Enterprise Groups LDAP Configuration）]** パラメータのステータスを確認します。 [矛盾は見つかりませんでした（No conflict found）]は、ピア間に設定ミスがないことを意味します。 矛盾が見つかった場合は、[エンタープライズ グループの矛盾（Enterprise GroupConflicts）] リンクをクリックして、表示された [詳細（details）]ボタンをクリックします。 これにより、レポート ウィンドウが開いて、詳細なレポートが表示されます。

図 *13 :* エンタープライズ グループ導入モデル *2*



エンタープライズ グループの制限事項

表 *60 :* エンタープライズ グループの制限事項

制限事項	説明
全員をブロック（Block everyone）	Cisco Jabber ユーザが [全員をブロック] を有効にした場合このブロックは、Cisco Jabber ポリシー設定内の機能であるため、ブロックしているユーザの連絡先リストに連絡先としてリストされていない限り、他の Jabber ユーザがブロックしているユーザとの IM and Presence の表示または交換を禁止します。 たとえば、Cisco Jabber ユーザ（Andy）は、自分の個人的な Jabber 設定内の[全員をブロック]を有効にしています。 次のリストは、Andy の個人用連絡先リストに含まれているかどうかにかかわらず、Andy のブロックが他の Jabber ユーザにどのように影響するかを示しています。ブロックに加えて、Andy には以下のような個人用連絡先リストがあります。 • Bob を含む - Bob は Andy の個人用連絡先リストに登録されているため、ブロックしていても IM を送信したり、Andy のプレゼンスを表示したりできます。 • キャロルを省略 - ブロックされているので、キャロルはアンディのプレゼンスを表示したり、IM を送信したりできません。 • 個人的な連絡先として Deborah を省略します。 ただし、Deborah は、Andy が連絡先としてリストしている企業グループのメンバーです - Deborah は、Andy のプレゼンスを表示したり、Andy に IM を送信したりすることはできません。 Andy の連絡先リストの企業グループのメンバーであるにもかかわらず、Deborah は Andy のプレゼンスを閲覧したり、IM を Andy に送信したりすることはできないことに留意してください。 エンタープライズグループ連絡先の動作の詳細については、CSCvg48001 を参照してください。

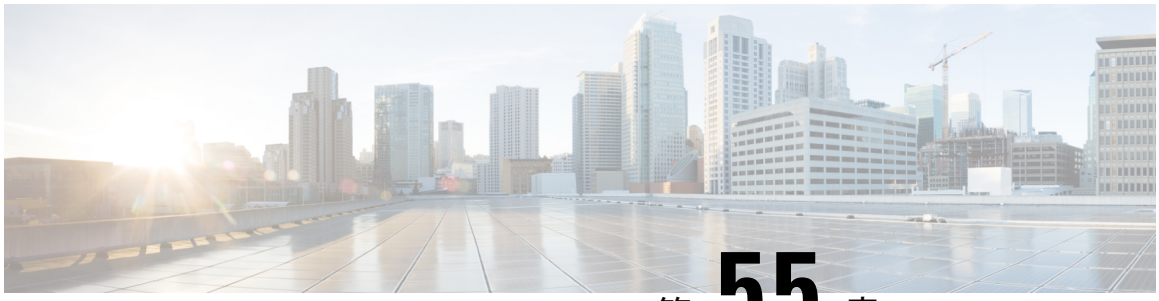
制限事項	説明
10.x クラスタとのクラスタ間ピアリング	エンタープライズ グループは、リリース 11.0(1) 以降でサポートされます。 同期されたグループに 10.x クラスタ間ピアからのグループ メンバーが含まれている場合、より高いクラスタ上のユーザは 10.x クラスタからの同期されたメンバーのプレゼンスを確認できません。 これは、エンタープライズ グループの同期用に 11.0(1) で導入されたデータベース更新が原因です。 この更新は 10.x リリースの一部ではありません。 より高いクラスタをホームにしているユーザが 10.x クラスタをホームにしているグループ メンバーのプレゼンスを確認できることを保証するには、より高いクラスタ上のユーザが自分の連絡先リストに 10.x ユーザを手動で追加する必要があります。 手動で追加されたユーザに関するプレゼンスの問題は存在しません。
複数レベルのグループ分け	複数レベルのグループ分けは、グループ同期に対して許可されません。
グループ専用同期	ユーザ グループとユーザが同じ検索ベース内に存在する場合、グループ専用同期は許容されません。 代わりに、ユーザグループとユーザが同期されます。
ユーザ グループの最大数	Microsoft Active Directory サーバから Unified Communications Manager データベースに最大 15000 のユーザ グループを同期できます。 各ユーザグループには 1 ～ 200 人のユーザを含めることができます。**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]** > **[システム（System）]** > **[サービスパラメータ（Service Parameters）]** ウィンドウで、正確な数量を設定できます。 データベース内のユーザ アカウントの最大数は 160,000 を超えることはできません。
ユーザ グループの移行	ユーザ グループを組織単位間で移動する場合は、元の単位に対して完全同期を実行してから、新しい単位に対して完全同期を実行する必要があります。
ローカル グループ	ローカル グループはサポートされません。 Microsoft Active Directory から同期されたグループのみがサポートされます。
IM and Presence Service ノードに割り当てられていないグループ メンバー	IM and Presence Service ノードに割り当てられていないグループ メンバーは、プレゼンス バブルが灰色表示されて連絡先リストに表示されます。 ただし、これらのメンバーは、連絡先リストで許可されるユーザの最大数を計算する際に考慮されます。

制限事項	説明
Microsoft Office Communications Server からの移行	Microsoft Office Communications Server からの移行中は、ユーザが IM and Presence Service ノードに完全に移行されるまで、グループ エンタープライズ機能がサポートされません。
LDAP 同期	同期の進行中に、[LDAPディレクトリの設定（LDAP Directory Configuration）]ウィンドウで同期オプションを変更しても、既存の同期は影響を受けません。 たとえば、同期の進行中に同期オプションを [ユーザとグループ（Users and Groups）] から [ユーザのみ（Users Only）] に変更しても、ユーザとグループの同期はそのまま継続されます。
エッジ経由のグループ検索機能	エッジ経由のグループ検索機能は、このリリースで提供されますが、完全にテストされているわけではありません。 そのため、エッジ経由のグループ検索のフル サポートは保証できません。 フル サポートは今後のリリースで提供される予定です。
Cisco Intercluster Sync Agent サービスの定期同期	外部 LDAP ディレクトリでグループ名またはグループ メンバー名を更新すると、定期 Cisco Intercluster Sync Agent サービス同期の後でしか Cisco Jabber 連絡先リストが更新されません。 通常、Cisco Intercluster Sync Agent サービスの同期は 30 分ごとに実行されます。
LDAP 設定内の別々の同期アグリーメント経由のユーザとユーザ グループの同期	ユーザとユーザ グループが同じ同期アグリーメントの一部として Cisco Unified Communications Manager データベースに同期されている場合は、同期後に、Cisco Unified Communications Manager データベースで、想定されているようにユーザとグループの関連付けが更新されます。 ただし、ユーザとユーザ グループが別々の同期アグリーメントの一部として同期されている場合は、最初の同期後、ユーザとグループはデータベースで関連付けされないことがあります。 データベース内のユーザとグループの関連付けは、同期アグリーメントが処理される順序によって異なります。 ユーザがグループより前に同期された場合は、データベース内でグループを関連付けに使用できない可能性があります。 その場合は、グループとの同期アグリーメントがユーザとの同期アグリーメントより前にスケジュールされるようにします。 そうでない場合は、グループをデータベースに同期した後、ユーザは次の手動同期または定期的に同期タイプを設定してユーザとグループとして同期した後にグループに関連付けられます。 契約の同期タイプがユーザとグループとして設定されている場合にのみ、ユーザおよび対応するグループ情報がマップされます。 .

制限事項	説明
エンタープライズ グループの検証済 OVA 情報	**検証 シナリオ** 2 つのクラスタを持つクラスタ間の導入では、クラスタ A とクラスタ B が使用されています。 クラスタ A は、Active Directory から同期される 160 k ユーザの IM and Presence Service で 15K OVA および 15K ユーザが有効になっています。 15K OVA クラスタでは、ユーザあたりのエンタープライズグループの検証され、サポートされる平均数は 13 のエンタープライズ グループです。 クラスタ B では、Active Directory から同期される 160 k ユーザの IM and Presence Service で 25K OVA および 25K ユーザが有効になっています。 25K OVA クラスタでは、ユーザあたりのエンタープライズグループの検証され、サポートされる平均数は 8 のエンタープライズ グループです。 名簿に記載されているユーザの個人連絡先と、ユーザの名簿に含まれるエンタープライズグループからの連絡先の、検証済およびサポートされる合計は、200 以下です。 （注） 2つ以上のクラスタがある環境では、これらの数量はサポートされていません。
連絡先リストのエクスポート	**[一括管理（Bulk Administration）] > [連絡先リスト（Contact List）] > [連絡先リストのエクスポート（Export Contact List）]** を使用してユーザの連絡先リストをエクスポートする場合、連絡先リスト CSV ファイルには Jabber クライアントに含まれるエンタープライズグループの詳細は含まれません。

第 XIII 部

デバイス管理



第 55 章

ヘッドセットとアクセサリの管理

ヘッドセットとアクセサリの管理の概要

ヘッドセットとアクセサリの管理によってシスコ ヘッドセットの展開が強化され、管理者は、Cisco Unified Communications Manager からヘッドセットの保守を管理できるようになります。Cisco Unified CM Administration から管理者は以下を行うことができます。

- ワイヤレス電源範囲、オーディオ帯域幅、および Bluetooth のオン/オフをリモートで構成します。
- ヘッドセットまたはアクセサリのファームウェアを定義および制御します。
- 導入環境内のすべてのヘッドセットおよびアクセサリの詳細なインベントリを取得します。
- リモート PRT、コール管理レコード (CMR) のヘッドセットメトリック、およびアラームを使用して、ヘッドセットの診断とトラブルシューティングを行います。

ヘッドセットとアクセサリ管理の機能の互換性

シスコ ヘッドセットとアクセサリ管理は、次のリリースから Unified Communications Manager でサポートされています。

- 12.x リリース用 リリース 12.5 (1) SU4

Unified Communications Manager のバージョンと共に、機能サポートは シスコ ヘッドセットとアクセサリ、Cisco IP 電話、および Cisco Jabber のファームウェアバージョンに依存しています。次の表は、ヘッドセットまたはアクセサリ、電話機、およびUified Communications Managerの使用バージョンに対応した、利用可能なヘッドセットとアクセサリ管理機能を示しています。

（注） シスコ ヘッドセットとアクセサリの管理機能は、12.0 (x) または 12.5 (1) ではサポートされていません。 旧バージョンでは、IP 電話用のヘッドセットとアクセサリの設定テンプレートを `defaultheadsetconfig. json` 設定ファイルと TFTP を使用して手動で送信できるように制限されている場合があります。詳細については、「ヘッドセットのアドミニストレーションガイド」を参照してください。

表 *61 : Cisco IP* 電話のヘッドセット保守性機能

保守性機能	**Unified CM 12.5 (1) 以前 + 電話機ファームウェア 12.1 (1)以前**	**Unified CM 12.5 (1)SU1 以降** ** **+ 電話機ファームウェア 12.1 (1) 以前**	**Unified CM 12.5 (1) 以前 + 電話機ファームウェア 12.5 (1)**	**Unified CM 12.5 (1)SU1 以降** ** **+ 電話機ファームウェア 12.5 (1)**	**Unified CM 12.5 (1) 以前 + 電話機ファームウェア 12.5 (1) SR3**	**Unified CM 12.5 (1)SU1 以降** ** **+ 電話機ファームウェア 12.5 (1)SR3**
手動リモート構成	—	—	X	該当なし	X	—
Unified CM のヘッドセットファームウェア アップグレード	—	—	—	—	—	X
Unified CM を介したリモートヘッドセットとアクセサリの構成	—	—	—	—	—	X
Unified CM のヘッドセットとアクセサリのインベントリ	—	—	—	—	—	X*
電話機 UI での構成リセット	—	—	—	—	X	X
ヘッドセットコール管理レコード（CMR）	—	—	—	—	—	X*

- * この機能は、ヘッドセットファームウェア 1.5 以降を搭載したヘッドセットでのみ使用できます。
- **この機能は、12.0. x および 12.5 (1) リリースではサポートされていません。

- 以前のバージョンから Unified CM 12.5 (1) にアップグレードすると、ほとんどの Cisco IP 電話は自動的に Phone ファームウェア 12.5(1)SR3 以降にアップグレードされます。

表 *62 : Cisco Jabber* のヘッドセット保守性機能

保守性機能	**Unified CM 12.5 (1) 以前 + Jabber バージョン 12.5 (1) 以前**	**Unified CM 12.5 (1)SU1 + Jabber バージョン 12.5 (1) 以前**	**Unified CM 12.5 (1) 以前 + Jabber バージョン 12.6 (1)**	**Unified CM 12.5 (1) 以降 + Jabber バージョン 12.6 (1)**	**Unified CM 12.5 (1) 以前 + Jabber バージョン 12.6 (1) MR**	**Unified CM 12.5 (1) 以降 + Jabber バージョン 12.6 (1)MR**
Unified CM を介したのヘッドセットファームウェア アップグレード	—	—	—	—	—	X
Unified CM を介したリモートヘッドセットとアクセサリの構成	—	—	—	X	—	X
Unified CM のヘッドセットとアクセサリのインベントリ	—	—	—	X*	—	X*
ローカル構成リセット	—	—	—	—	X	X
ローカル UI 構成	—	—	X	X	X	X
ローカルヘッドセットとアクセサリのバージョン表示	—	—	—	—	X	X

- * この機能では、ヘッドセットファームウェア 1.5 以降を搭載したヘッドセットのみを検出できます。
- **この機能は、12.0. x および 12.5 (1) リリースではサポートされていません。

サードパーティのヘッドセットとアクセサリのサポート

サードパーティヘッドセットまたはアクセサリを導入している場合、Unified Communications Manager は、Cisco Unified CM の管理インターフェイスから、サードパーティヘッドセットとアクセサリに関する制限付きの情報によって、ヘッドセットまたはアクセサリのインベントリ管理をサポートします。 Unified Communications Manager は、サードパーティヘッドセット用のヘッドセットまたはアクセサリの設定テンプレート、ファームウェア、診断、およびヘッドセット CMR をサポートしていません。

ワークフロー: ヘッドセット保守の構成

次のワークフローを使用して、シスコ ヘッドセット Serviceability 機能の設定をガイドします。

このワークフローを完了すると、ヘッドセットまたはアクセサ設定の構成、ヘッドセット最新ファームウェアロードの保持、ユーザへのヘッドセットまたはアクセサリの関連付け、ヘッドセットベースのExtension Mobilityの有効化、およびインベントリの保守を行うことができます。

手順

	コマンドまたはアクション	目的
ステップ 1	シスコ ヘッドセット サービスを有効化する （833 ページ）	Cisco Unified Serviceabilityで、シスコヘッドセットサービスをオンにします。
ステップ 2	ヘッドセット COP ファイルを準備する （833 ページ）	COP ファイルを使用して、最新のヘッドセットまたはアクセサリ ファームウェアのインストールとアップグレードを行ってください。
ステップ 3	ヘッドセットユーザ用のユーザプロファイルの設定 （835 ページ）	ユーザのユーザプロファイルがまだ設定されていない場合は、次の手順を使用してプロファイルを設定します。 ユーザプロファイルがすべて設定されている場合は、このタスクをスキップできます。
ステップ 4	エンドユーザにユーザプロファイルを適用する （836 ページ）	ユーザプロファイルをエンドユーザに割り当てます。 すでにユーザプロファイルが割り当てされている場合は、このタスクをスキップできます。
ステップ 5	ヘッドセットとアクセサリのテンプレートの設定 （842 ページ）	シスコ ヘッドセットとアクセサリのテンプレートのデフォルト設定とファームウェアを設定します。 そのユーザプロファイルを使用しているユーザがこのヘッドセットとアクセサリのテンプレートに割り当てられるように、ユーザプロファイルをテンプレートに関連付けます。
ステップ 6	ヘッドセットとアクセサリのインベントリの表示 （846 ページ）	Cisco Unified CM インターフェイスを使用して、導入したヘッドセットとアクセサリのインベントリが表示されることを確認します。

シスコ ヘッドセット サービスを有効化する

Cisco Unified CM の管理インターフェイスを使用してシスコ ヘッドセットとアクセサリを管理する前に、Cisco Unified Communications Manager Serviceabilityで **シスコ ヘッドセットサービス** をオンにする必要があります。

（注） Cisco CallManager サービスが既に実行されている場合は、すべてのユニファイド コミュニケーション マネージャ ノードでシスコ ヘッドセット サービスをアクティブにする必要があります。 Cisco Unified CM の管理インターフェイスを使用してヘッドセットまたはアクセサリを管理するには、ユニファイド コミュニケーション マネージャ ノード上でシスコ ヘッドセット サービスをアクティブにしてください。 Cisco CallManager サービスは、シスコ ヘッドセット サービスを有効にすると自動的にアクティブになります。 必要でない場合は、Cisco CallManager サービスを非アクティブにします。

手順

ステップ 1 Cisco Unified CM 管理から**Cisco Unified Serviceability**へ移動して **[移動（Go）]** をクリックします。

ステップ 2 **[ツール（Tools）]** > **[サービスのアクティベーション（Service Activation）]** を選択します。

ステップ 3 CM Services **セクションの [**シスコ ヘッドセットサービス] チェックボックスをオンにして、**[保存（Save）]** を選択します。

次のタスク

ヘッドセット COP ファイルを準備します。

ヘッドセット COP ファイルを準備する

COP ファイルを使用して、最新のヘッドセットファームウェアをインストールし、アップグレードすることができます。 ヘッドセット COP ファイルには、様々なヘッドセットまたはアクセサリモデルのファームウェアバージョンと構成データがすべて含まれています。

（注） COP ファイルをインストールする前に、シスコ ヘッドセットサービスが起動され、実行されていることを確認してください。

ヘッドセット COP ファイルが、Unified Communications Manager のすべてのノードにインストールされていることを確認します。

1. シスコ ヘッドセットまたはアクセサリを使用を開始する前に、COP ファイルを Unified Communications Manager システムにインストールまたはアップグレードします。

ヘッドセットまたはアクセサリをエンドポイントに接続すると、ヘッドセットまたはアクセサリテンプレートの構成の変更が適用されます。 Unified Communications Manager のヘッドセットまたはアクセサリテンプレート構成にアップデートを行った場合、エンドポイントは、接続されたヘッドセットまたはアクセサリにこれらの構成の更新内容を適用します。

すべての構成の更新は、COP ファイルのヘッドセットとアクセサリテンプレートのバージョンによって異なります。 ヘッドセットとアクセサリテンプレートバージョンが最新の COP ファイルの上位にある場合、Unified Communications Manager の構成ファイルが更新されます。 COP ファイルの構成ファイルがアップグレードされると、Unified Communications Manager のヘッドセットとアクセサリテンプレートバージョンはテンプレートのバージョンに関係なく更新され、その逆も同様です。 次の一覧は、COP ファイルのアップグレード後の様々なテンプレート バージョンの更新シナリオを示しています。

- Unified Communications Manager が、ヘッドセットとアクセサリ テンプレート バージョン 1-10 でインストールされている場合は、ヘッドセットとアクセサリ テンプレート バージョン 1-12 の Unified Communications Manager サーバをアップグレードすると、選択したヘッドセットとアクセサリテンプレート バージョンが 1-12 になります。 Unified Communications Manager は、より高いヘッドセットとアクセサリ テンプレート バージョンを選択します。
- Unified Communications Manager が、ヘッドセットとアクセサリ テンプレート バージョン 1-10 でインストールされている場合は、ヘッドセットとアクセサリ テンプレート バージョン 1-9 の Unified Communications Manager サーバをアップグレードすると、選択したヘッドセットとアクセサリテンプレート バージョンが 1-10 になります。 Unified Communications Manager は、より高いヘッドセットとアクセサリ テンプレート バージョンを選択します。
- Unified Communications Manager が、ヘッドセットとアクセサリ テンプレート バージョン 1-10 でインストールされている場合は、ヘッドセットとアクセサリ テンプレート バージョン 1-12 の Unified Communications Manager サーバをアップグレードすると、選択したヘッドセットとアクセサリテンプレート バージョンが 1-12 になります。 COP ファイルと一緒にインストールされるヘッドセットとアクセサリ テンプレート が推奨オプションです。
- Unified Communications Manager が、ヘッドセットとアクセサリ テンプレート バージョン 1-10 でインストールされている場合は、ヘッドセットとアクセサリ テンプレート バージョン 1-9 の Unified Communications Manager サーバをアップグレードすると、選択したヘッドセットとアクセサリテンプレート バージョンが 1-9 になります。 COP ファイルと一緒にインストールされるヘッドセットとアクセサリ テンプレート が推奨オプションです。
- ヘッドセットとアクセサリ テンプレート バージョンが 1-12 の COP ファイルをインストールし、ヘッドセットとアクセサリ テンプレート バージョン 1-10 の Unified Communications Manager サーバを更新すると、選択したヘッドセットとアクセサリ テンプレート バージョンは 1-12 になります。 Unified Communications Manager は、より高いヘッドセットとアクセサリ テンプレート バージョンを選択します。

ヘッドセットユーザ用のユーザプロファイルの設定

ユーザのユーザプロファイルがまだ設定されていない場合は、次の手順を使用してプロファイルを設定します。ヘッドセットとアクセサリのテンプレートは、ユーザプロファイルを使用してユーザに割り当てられます。すでにユーザプロファイルが設定されている場合は、このタスクをスキップできます。

（注） 導入要件に応じて異なるユーザのグループに複数のユーザプロファイルを構成します。デフォルトでは、すべてのユーザプロファイルがシステムのデフォルトヘッドセットテンプレートに割り当てられます。ヘッドセットとアクセサリのテンプレートを設定する場合は、カスタマイズされたテンプレートに割り当てることができます。

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]** > **[ユーザ設定]** > **[ユーザ プロファイル]**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 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、**[ユニバーサルデバイステンプレート（Universal Device Template）]** を割り当てます。

ステップ 5 [ユニバーサル回線テンプレート（Universal Line Template）]を割り当て、このユーザプロファイルのユーザの電話回線に適用します。

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機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) [エンドユーザがプロビジョニングする電話機数を制限（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]** 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になっています。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。

（注） この設定は、Cisco Jabber ユーザの場合にのみ必須です。 Jabber ユーザではない場合、この設定を行わずともモバイルおよびリモートアクセス機能を使用できます。モバイルおよびリモートアクセス機能は、Jabber モバイルおよびリモートアクセスのユーザにのみ適用され、他のエンドポイントや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)]**と**[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、次のオプションのいずれかを選択します。

- サービスなし：このポリシーは、すべての Cisco Jabber サービスへのアクセスを禁止します。
- IMとプレゼンスのみ：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のみを有効にします。
- IM とプレゼンス、音声とビデオ通話：このポリシーは音声やビデオ デバイスを使うすべてのユーザに対して、インスタントメッセージ、プレゼンス、ボイスメールと会議機能を有効化します。 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 版 Cisco Jabber および Mac 版 Cisco Jabber が含まれています。 Jabber モバイルクライアントには、iPad/iPhone ユーザ用 Cisco Jabber および Android 版 Cisco Jabber が含まれています。

ステップ 9 このユーザプロファイルのユーザが Cisco Unified Communications セルフケア ポータルで Extension Mobility または Extension Mobility Cross Cluster の最大ログイン時間を設定するには、[エンドユーザにエクステンションモビリティの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）]チェックボックスをオンにします。

（注） デフォルトでは [エンドユーザにエクステンションモビリティの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）]チェックボックスはオフになっています。

ステップ 10 **[保存（Save）]** をクリックします。

エンドユーザにユーザプロファイルを適用する

作成したユーザプロファイルにユーザを関連付ける。 このユーザプロファイルはエンドユーザに関連付けられている必要があり、ヘッドセットとアクセサリのテンプレート構成の変更を適用するには、デバイスの MAC を制御されたデバイスの下に追加する必要があります。

（注） すべてのユーザがすでにユーザプロファイルに割り当てられている場合は、このタスクをスキップできます。

手順

ステップ 1 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。

a) **Cisco Unified CM 管理** で、[ユーザの管理（User Management）][エンドユーザ（End User）] を選択します。
b) [新規追加] をクリックします。
c) ユーザの**ユーザID**と**姓**を入力します。
d) ドロップダウンリストから**[ユーザランク（User Rank）]**を選択します。
e) [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。
f) **[保存]** をクリックします。

ステップ 2 デバイスにエンドユーザを関連付けるには、次の手順を実行します。

a) Cisco Unified CM 管理で、**[デバイス（Device）][電話（Phone）]** を選択します。
b) Cisco IP 電話 またはデバイスを選択します。
c) [デバイス情報 (Device Information)] で、**[ユーザ（User）]** を選択し、**[所有者ユーザ ID（Owner User ID）]** を選択します。
d) 構成**の**変更**を有効**にするには、[保存して構成を適用 (Save and Apply Config)] をクリックします。

ヘッドセットとアクセサリ テンプレートの管理

ユーザに対してデフォルトのヘッドセットとアクセサリの設定を構成するには、Cisco Unified Communications Manager で、ヘッドセット テンプレートをユーザ プロファイルに割り当てます。 ヘッドセットとアクセサリのテンプレートでは、ユーザプロファイルを関連付けるオプションが提供されています。 Unified Communications Manager は、次のヘッドセットとアクセサリのテンプレートをサポートしています。

標準デフォルトヘッドセット構成テンプレート

これは、すべてのヘッドセットとアクセサリ モデルシリーズの工場出荷時デフォルト設定が含まれるシステムデフォルトテンプレートです。 このテンプレートには、すべてのヘッドセットまたはアクセサリのモデルシリーズについて、システムにインストール済みの最新ヘッドセッドまたはアクセサリのファームウェアでサポートされるヘッドセットまたはアクセサリの設定が含まれます。 デフォルトの設定は編集できませんが、プロファイル構成の設定を変更することはできます。

（注） 標準デフォルトヘッドセット設定テンプレートが作成されるのは、**シスコ**ヘッドセットサービスが Cisco Unified Serviceability ユーザインターフェイスでアクティブになっている場合のみです。

デフォルトでは、管理者がカスタム定義のヘッドセットテンプレートのいずれかにユーザプロファイルを関連付ける場合を除き、すべてのユーザプロファイルは標準ヘッドセットテンプレートに関連付けられます。 標準のデフォルトヘッドセットテンプレートのコピーを作成して、ヘッドセットまてゃアクセサリのファームウェアバージョンを含むパラメータのカスタマイズ値を用いたカスタムテンプレートを作成することができます。

システム生成のカスタムヘッドセットテンプレート

完全なシスコヘッドセットサービスアビリティ機能をサポートしていない一部の以前のリリースでは、管理者が `defaultheadsetconfig.json` 設定ファイルと TFTP を使用してヘッドセットとアクセサリのテンプレートを手動で設定および導入することができます。 以前のリリースでこの方法を使用した後でこのリリースにアップグレードした場合、設定ファイルは**システムによって生成されたカスタム ヘッドセット テンプレート**に変換され、**[ヘッドセットとアクセサリのテンプレート設定]** ウィンドウに表示されます。 このカスタムテンプレートには、設定ファイルを使用したユーザとデバイスが、アップグレードの後に関連付けられます。

カスタムヘッドセット構成テンプレート

Cisco Unified CM Administration から、**デバイス** > **ヘッドセットとアクセサリ** > **ヘッドセットとアクセサリ テンプレート** ウィンドウを使用して、展開のニーズに応じてヘッドセットとアクセサリのテンプレートをカスタマイズします。同じテンプレートの別のモデルに異なるヘッドセットパラメータを割り当てることができます。 複数のファームウェアロードを別のヘッドセットまたはアクセサリ モデルに割り当てることもできます。 カスタムヘッドセットまたはアクセサリの設定は、ユーザプロファイルをカスタムヘッドセットテンプレートに関連付けることによって、特定のユーザの集合に割り当てることができます。

表 *63 :* ヘッドセットとアクセサリの構成テンプレートの設定

フィールド	説明
ヘッドセットとアクセサリのテンプレートの設定	
名前	ヘッドセットとアクセサリのテンプレートを識別する一意の名前を入力してください。
説明	テンプレートの使用を識別する説明を入力します。
モデルとファームウェアの設定	
モデルシリーズの選択	デバイスに信頼性の高い、高品質のサウンドを提供するサポートされているヘッドセットまたはアクセサリのモデルを選択します。

フィールド	説明
追加	標準テンプレートの場合は、デフォルトの事前定義済みファームウェアバージョンと、ヘッドセットまたはアクセサリのモデルの設定を表示することができます。 デフォルトの値は編集できません。 カスタマイズされたテンプレートの場合は、**[追加]** をクリックして新しいヘッドセットまたはアクセサリ モデルと対応する設定を追加します。 同じテンプレートに、別の既存のヘッドセットまたはアクセサリのモデルを追加することはできません。 カスタマイズされたテンプレートには、さまざまなヘッドセットまたはアクセサリのモデルを追加できます。ただし、ヘッドセットとアクセサリのモデルごとに使用できるファームウェアは 1 つだけです。 headset パラメータの詳細については、次の「Headset Configuration パラメータ」の表を参照してください。 標準デフォルトヘッドセットテンプレート設定では、ヘッドセット COP ファイルをインストールすると設定を編集できます。
ファームウェア	必要なファームウェアバージョンの選択 • 現在のバージョンに残す— ヘッドセットまたはアクセサリを既存のファームウェアバージョンに残す場合 (ヘッドセットまたはアクセサリのファームウェアバージョンが最新のシステムファームウェアバージョンにアップグレードされない場合)、このオプションを選択します。 • 最新 - ヘッドセットまたはアクセサリのファームウェアのバージョンをシステムの最新ファームウェアバージョンと一致させるようアップグレードするには、このオプションを選択します。
[Delete]	カスタマイズされたテンプレートの場合、**[削除]** をクリックしてヘッドセットとアクセサリのテンプレートからヘッドセットまたはアクセサリのモデルを削除します。
プロファイルの設定	
利用可能なユーザプロファイル	このヘッドセットとアクセサリのテンプレートで使用可能な設定済みのユーザプロファイルを一覧表示します。 このテンプレートにユーザプロファイルを関連付けるには、プロファイルを選択し、下矢印をクリックして、割り当てられているユーザプロファイルにテンプレートを移動します。 （注） デフォルトでは、すべてのユーザプロファイルが標準のデフォルトヘッドセット設定テンプレートに割り当てられます。 ユーザプロファイルを別のテンプレートに関連付けるには、新しいテンプレートを作成して、ユーザプロファイルを新しいテンプレートに割り当てます。

フィールド	説明
割り当てられているユーザプロファイル	このヘッドセットとアクセサリの設定テンプレートを使用するユーザプロファイルを一覧表示します。 このプロファイルに割り当てられているユーザの場合、このヘッドセットとアクセサリの設定テンプレート内の設定は、登録中にシスコ ヘッドセットおよびアクセサリに適用されます。 矢印をクリックして、利用可能なユーザプロファイルリストから新しいユーザプロファイルを追加します。

次の表で、各ヘッドセットおよびアクセサリのテンプレートのパラメータについて説明します。

（注） オンプレミスおよびマルチプラットフォームヘッドセットのサービスアビリティ機能は、RJ-9接続では利用できません。

表 *64 :* シスコ ヘッドセット *500* シリーズ

パラメータ	範囲	デフォルト	注記
スピーカーの音量	0 – 15	7	ヘッドセットのサウンドレベルを制御します。 0は低音量、15が最大音量です。 オフィス環境でのノイズに基づいて、この設定を構成します。
マイクロフォンゲイン	ソフト - ラウド	デフォルト	ゲインは、通話中にユーザが相手にどの程度の音量で声を届けるかを制御します。 **ソフト**にすると音声は小さくなり、**ラウド**にするとユーザの音声が大きくなることを意味します。 オフィス環境でのノイズに基づいて、この設定を構成します。
側音	オフ–高	低	ヘッドセットから聞こえるユーザ自身の音量を制御します。**[オフ（Off）]**は側音を無効にし、**[高（High）]**はヘッドセットマイクからより多くのフィードバックを受け取ります。

パラメータ	範囲	デフォルト	注記
イコライザ	ワーム–ブライト	デフォルト	イコライザーの設定を制御します。 ワームに設定すると、ヘッドセットの低音が聞こえやすくなります。ブライト設定にすると、ユーザが高音が聞こえやすくなります。
オーディオ帯域幅	広帯域、狭帯域	広帯域	シスコ ヘッドセット 560シリーズの Digital Enhanced cordless Telecommunications (DECT) コーデックを制御します。 高密度 DECT 環境では、このフィールドを**狭帯域**に設定して、シスコ ヘッドセット 560を 727 コーデックに制限します。
Bluetooth	オン、オフ	オン	シスコ ヘッドセット 560 シリーズ (マルチベース)でBluetooth の使用を制御します。 このパラメータがオフ に設定されている場合、ベースはペアリング済みのデバイスすべてを削除します。
会議	オン、オフ	オン	シスコ ヘッドセット 560シリーズでの会議機能の使用を制御します。 会議機能では、最大 3 台のゲスト用ヘッドセットを同一ベースに一度にペアリングできます。 会議機能の詳細については、シスコヘッドセット 500 シリーズユーザガイドを参照してください。
ファームウェアソース	UCM または Cisco Cloud から許可する (ファームウェアはアップグレードのみ)、UCM のみに制限する (ファームウェアはアップグレードまたはダウングレード可能)	UCM または Cisco Cloud から許可する	ヘッドセットのファームウェアアップグレードソースを制御します。 デフォルトでは、ユーザーは、Unified CM に接続されているデバイスおよびソフトウェアを介して、またはクラウドに接続されているデバイスまたはソフトウェアを介してヘッドセットをアップグレードできます。 ヘッドセットは、Unified CM のソースを使用して、ファームウェアの変更のみを受け入れるように制限できます。

パラメータ	範囲	デフォルト	注記
DECT ラジオレンジ	オートレンジ、中距離、短距離	範囲 (中)	シスコ ヘッドセット 560シリーズとそのベースの最大距離を制御します。 デフォルトでは、理想的な条件が揃えばベースは 330 フィート (100 m) 以上の DECT 範囲になります。 DECT ラジオレンジを中距離または短距離に構成すると、ヘッドセットベースの消費電力は少なくなりますが、ユーザは通話中、ベースから遠くへ離れることはできません。DECT ラジオレンジを高密度**ヘッドセット**導入向けに、短距離に構成してください。 DECT 導入の詳細については、シスコ ヘッドセットの導入に関するホワイトペーパー、シスコ ヘッドセット 560 シリーズの職場での DECTの導入方法を参照してください。
ヘッドセットのドックの動作	オン、オフ	オン	着信通話があるときにヘッドセットをベースから外した場合の シスコ ヘッドセット 560シリーズ の動作を制御します。

ヘッドセットとアクセサリのテンプレートの設定

シスコヘッドセットとアクセサリに適用できるカスタマイズされた設定でヘッドセットとアクセサリテンプレートを設定するには、次の手順を使用します。 カスタマイズしたテンプレートを作成するか、またはシステム定義の標準デフォルトヘッドセットテンプレートを使用することができます。

（注） 標準デフォルトヘッドセット構成テンプレートは、システム定義のテンプレートです。 標準デフォルトヘッドセットテンプレートに新しいユーザプロファイルを割り当てることはできますが、テンプレートを編集することはできません。 デフォルトでは、すべてのユーザプロファイルがこのテンプレートに割り当てられています。 このテンプレートからユーザプロファイルの関連付けを外すには、プロファイルを新しいテンプレートに割り当てる必要があります。

手順

ステップ 1 [Cisco Unified CM 管理] から、**[デバイス] > [ヘッドセットとアクセサリ] > [電話機]** を選択します。

ステップ 2 次のいずれかを実行します。

- 既存のテンプレートを編集するには、そのテンプレートを選択します。
- 新しいテンプレートを作成するには、既存のテンプレートを選択し、**[コピー (Copy)]** をクリックします。 既存の設定が新しいテンプレートに適用されます。

ステップ 3 テンプレートの**[名前（Name）]**と**[説明（Description）]**を追加します。

ステップ 4 **[モデルとファームウェアの設定（Model and Firmware Settings）]** で、カスタマイズしたヘッドセットまたはアクセサリの設定をこのテンプレートに適用するように割り当てます。 新しい設定を追加するには、**[**追加 (add)] ボタンをクリックして設定を構成します。

ステップ 5 上下矢印を使用して、このテンプレートに割り当てるユーザプロファイルを**割当済みユーザプロファイル**リストに移動します。 これらのプロファイルに割り当てられているすべてのユーザは、このヘッドセットとアクセサリのテンプレートにも割り当てられます。

ステップ 6 **[保存]** をクリックします。

ステップ 7 デフォルトの**テンプレート設定**に戻るには、[デフォルトに設定 (Set to Default)] ボタンを使用します。

ステップ 8 **[設定の適用（Apply Config）]** をクリックします。

標準デフォルトヘッドセット構成テンプレートの場合、**[**構成を適用 (Apply Configuration)] ボタンは次の場合有効になります。

- 割当済みユーザプロファイルリストに追加したユーザが所有するデバイス
- 匿名デバイス

カスタマイズされたヘッドセット構成テンプレートでは、**構成を適用**ボタンは、**割当済みユーザプロファイル**リストに追加したユーザが所有するデバイスでのみ有効になります。

ファームウェア管理

Unified Communications Manager に接続されているほとんどの電話機およびデバイスは、シスコヘッドセット 500 シリーズとシスコヘッドセット 700 シリーズをサポートします。 ヘッドセットまたはアクセサリを電話機に接続する前に、最新の電話機のファームウェアリリースおよびデバイスパッケージをインストールしてください。 ヘッドセットまたはアクセサリが最初に接続されると、必要なファームウェアがダウンロードされ、アップグレードプロセスが開始されます。

特定のヘッドセットまたはアクセサリモデルでは、次の2つのファームウェアオプションがサポートされます。

- **現在のバージョンに残す**： ヘッドセットまたはアクセサリを既存のファームウェアバージョンに残す場合 (ヘッドセットまたはアクセサリのファームウェアバージョンが最新のシステムファームウェアバージョンにアップグレードされない場合)、このオプションを選択します。
- **最新**：ヘッドセットまたはアクセサリをアップグレードまたはダウングレードするには、このオプションを選択します。 選択したソフトウェアが、ヘッドセットまたはアクセサリの現在のファームウェアより古いリリースであっても、システムによってインストールおよび実行されます。

  たとえば、最新版として **1-5-1-10** を選択すると、現在ヘッドセットまたはアクセサリに **1-5-1-9** または **1-5-1-11** があるかどうかに関係なく、そのファームウェアがヘッドセットまたはアクセサリにインストールされます。

ファームウェアに関する検討事項

- 標準ヘッドセットテンプレートに割り当てられたユーザは、常に最新のヘッドセットまたはアクセサリファームウェアと設定を受信します。
- ヘッドセットテンプレート構成 (標準とカスタムの両方) に表示される設定は、常にすべてのヘッドセットとアクセサリ モデルシリーズの**最新ファームウェア**に設定されます。

ヘッドセットとアクセサリ インベントリの管理

Cisco IP 電話 は、ヘッドセットとアクセサリが接続済みまたは切断状態になったときに、ヘッドセットとアクセサリのインベントリデータを Unified Communications Manager に送信します。このサーバに導入されているすべてのヘッドセットとアクセサリのインベントリ要約レポートまたはカスタムインベントリレポートを生成できるよう、Unified Communications Managerにはこのインベントリデータが保存されます。

レポート情報には、ヘッドセットまたはアクセサリのシリアル番号とモデル番号、ドッキングステーションの詳細情報、ファームウェア、使用している構成テンプレート、ベンダーの詳細情報、デバイスとのヘッドセットまたはアクセサリ接続ステータスが含まれます。

ヘッドセットとアクセサリのインベントリ

Cisco Unified CM Administration は、 **デバイス** > **ヘッドセットおよびアクセサリ** > **ヘッドセットおよびアクセサリ インベントリ**ウィンドウを使用して、サーバ上に展開されているすべてのヘッドセットおよびアクセサリの一覧を表示します。 この情報を使用して、導入済みのすべてのヘッドセットおよびアクセサリのレポートを生成できます。 デバイスのシリアル番号をクリックすると、個々のヘッドセットおよびアクセサリの詳細がポップアップウィンドウに表示されます。

表 *65 :* ヘッドセットとアクセサリのインベントリの設定

フィールド	説明
シリアル番号（Serial Number）	ヘッドセットまたはアクセサリのシリアル番号。 この番号は、個々のヘッドセットまたはアクセサリごとに固有です。 （注） シスコ以外のヘッドセットまたはアクセサリの場合、デバイス名がシリアル番号として使用されます。 複数の電話機で同じシスコ以外のヘッドセットを使用すると、ヘッドセットレコードの複製が作成されます。 （注） 特定のヘッドセットまたはアクセサリのシリアル番号の位置については、そのヘッドセットまたはアクセサリのモデルのヘッドセットのアドミニストレーションガイドを参照してください。
モデル（Model）	ヘッドセットまたはアクセサリのモデル番号です。
ベンダー	ベンダーの詳細を表示します。
タイプ（Type）	ヘッドセット接続の種類（有線、DECT ワイアレス、または不明）を示します。
ファームウェア	ヘッドセットまたはアクセサリの最新ファームウェアロードを表示します。
ユーザー	電話機またはデバイスを使用してエンドユーザの情報を表示します。
接続された電話所有者のユーザー ID	電話機またはデバイスを使用してエンドユーザの情報を表示します。 ヘッドセットまたはアクセサリが関連付けられている場合、このフィールドは空白です。
ヘッドセット/アクセサリの所有者	ヘッドセットまたはアクセサリのシリアル番号に関連付けられているエンドユーザの情報を表示します。
テンプレート	ヘッドセットまたはアクセサリの構成テンプレートの名前を表示します。
ステータス (以降)	ヘッドセットまたはアクセサリのアクティベーションステータスが表示されます。 接続されているか、または切断されているかを示します。
ドックモデル	ドッキングモデルステーションのタイプを表示します。
デバイス名	ヘッドセットまたはアクセサリが接続されているデバイスの名前。
デバイスモデル	Cisco IP 電話 または Cisco Jabber モデル番号が表示されます。 たとえば、CP-8865 は Cisco IP 電話 モデルです。 CSF は、Mac 版 Cisco Jabber または Windows 版 Cisco Jabber のデバイスタイプのいずれかです。

フィールド	説明
ソフトウェアバージョン	使用しているソフトウェアの最新バージョンが表示されます。 電話機ファームウェアまたはJabberソフトウェアバージョンである場合があります。
ヘッドセット/アクセサリの新しさ (日数)	ヘッドセットの使用日数を表示します。 レコードが削除された場合は、ヘッドセットまたはアクセサリの使用日数がリセットされます。

ヘッドセットとアクセサリのインベントリのダウンロード

重要 このセクションは、リリース 12.5(1)SU4 およびリリース 14 以降に適用されます。

Cisco Unified Communications Manager の管理ページで、**[ヘッドセットとアクセサリ] > [ヘッドセットとアクセサリのインベントリ]** メニュー パスで、関連リンクのドロップダウンリストから**[ヘッドセットとアクセサリのインベントリのダウンロード]**を選択し、ヘッドセットとアクセサリの詳細な情報を CSV ファイル形式でダウンロードします。

この情報を使用して、ヘッドセットやアクセサリの使用状況のトラッキング、展開環境内のサードパーティ製ヘッドセット、ヘッドセットの更新などのユースケースのためにデータを分析できます。

ヘッドセットとアクセサリ インベントリの管理タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ヘッドセットとアクセサリのインベントリの表示 （846 ページ）	サーバ上に展開されているヘッドセットとアクセサリを一覧表示します。
ステップ 2	電話の所有者をヘッドセットまたはアクセサリの所有者として関連付け （847 ページ）	ヘッドセットまたはアクセサリをユーザに関連付けます。

ヘッドセットとアクセサリのインベントリの表示

サーバに導入済みのヘッドセットとアクセサリのすべての一覧を表示できます。 この情報を使用して、導入済みのすべてのヘッドセットおよびアクセサリのレポートを生成できます。

手順

ステップ 1 Cisco Unified CM 管理で **[デバイス]** > **[ヘッドセットとアクセサリ]** > **[ヘッドセットとアクセサリのインベントリ]** 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)]** を選択すると、サーバに導入済みのヘッドセットの完全リストが表示されます。
- 検索ボックスに 1 つまたは複数の検索条件を入力し、**[検索 (Find)]** を選択します。

電話の所有者をヘッドセットまたはアクセサリの所有者として関連付け

ユーザに一括ヘッドセットを関連付けるには、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。**デバイス** > **ヘッドセットおよびアクセサリの** > **ヘッドセットとアクセサリのインベントリ**

ステップ 2 サーバに導入されているヘッドセットとアクセサリの完全なリストを表示するには、**[検索]** をクリックします。

ステップ 3 **[すべて選択]** をクリックするか、必要なシリアル番号を選択し、**[ヘッドセットまたはアクセサリの所有者として電話機の所有者を関連付ける]** をクリックしてヘッドセットまたはアクセサリをユーザーに関連付けます。

（注） すでに関連付けられているか、または電話の所有者が関連付けられていない場合、ヘッドセットまたはアクセサリを関連付けることはできません。 ヘッドセットまたはアクセサリの関連付けは、ページが再ロードされた後、[ヘッドセットまたはアクセサリの所有者] 列で表示されます。

特定のユーザに最大 15 個のヘッドセットまたはアクセサリを関連付けることができます。 特定のユーザの最大制限に達すると、残りのヘッドセットまたはアクセサリは割り当てられず、エラーが表示されます。

ステップ 4 （任意） 必要なシリアル番号を選択し、**[ヘッドセットまたはアクセサリ所有者の割り当て解除]** をクリックして、選択したユーザからヘッドセットまたはアクセサリのシリアル番号を切り離します。

（注） ヘッドセットまたはアクセサリの所有者に関連付けられていないヘッドセットまたはアクセサリの関連付けを解除することはできません。

ステップ 5 （任意） エンド ユーザの設定とヘッドセットまたはアクセサリの関連付けの詳細を表示するには、**[接続された電話機の所有者ユーザ ID]** または**[ヘッドセットまたはアクセサリの所有者]** 列の [ユーザ名] リンクをクリックします。

（注） **[エンドユーザ設定]** ウィンドウに、ヘッドセットまたはアクセサリの関連付けと解除の詳細が表示されます。

ヘッドセットとアクセサリのインベントリの概要

Cisco Unified CM Administration から、**デバイス** > **ヘッドセットとアクセサリ** > **ヘッドセットとアクセサリのインベントリの概要**ウィンドウを使用して、**ヘッドセットとアクセサリのインベントリの概要**ウィンドウで導入されたヘッドセットとアクセサリのの要約を表示することができます。

モデル別のヘッドセットとアクセサリのインベントリ

フィールド	説明
ヘッドセット/アクセサリ モデル	ヘッドセットまたはアクセサリのモデル番号。
数量	導入環境内のモデルタイプごとのヘッドセットまたはアクセサリの数を示します。 （注） **数量**列にあるリンクをクリックして、モデルタイプ別にフィルタを適用した詳細なヘッドセットとアクセサリのインベントリページに移動します。

ステータス別のヘッドセットとアクセサリのインベントリ

ヘッドセット/アクセサリ モデル、**アクティブ**、**非アクティブ**、または**未割り当て**列にあるハイパーリンクをクリックすると、各ステータスの詳細なヘッドセットとアクセサリのインベントリページに移動します。

フィールド	説明
ヘッドセット/アクセサリ モデル	ヘッドセットまたはアクセサリのモデル番号。
アクティブ	ヘッドセットまたはアクセサリが過去 30 日間に接続されたことを示します。
非アクティブ	ヘッドセットまたはアクセサリは過去 30 日間、接続されていないことを示します。

フィールド	説明
未割り当て	ユーザ ID がシステムに存在しないか、またはインベントリレコードにユーザ ID マッピングがありません。

導入済みヘッドセットとアクセサリの集約概要を入手する

ヘッドセットとアクセサリのインベントリの概要ウィンドウに、導入済みのヘッドセットとアクセサリのの集約概要を表示できます。

手順

Cisco Unified CM 管理で **[デバイス]** > **[ヘッドセットとアクセサリ]** > **[ヘッドセットインベントリの概要]** を選択します。

ヘッドセットとアクセサリのインベントリの詳細をモデル別またはヘッドセットとアクセサリのステータス別に表示できます。

ヘッドセットとアクセサリのトラブルシューティングと診断

Unified Communications Manager または Cisco Unified Real-Time Monitoring Tool（RTMT）を設定すると、Cisco IP 電話に接続されているヘッドセットまたはアクセサリの問題レポート ツール（PRT）ログを収集できます。 PRTには、通話品質、使用するコーデック、音声設定、ワイヤレス設定、およびアラートログに関するデータが含まれています。

Unified Communications Managerには、ヘッドセットとアクセサリの通話診断の詳細が保存されています。 Cisco IP 電話は、BYE メッセージまたは BYE メッセージへの 200 OK 応答のいずれかでヘッドセット統計ヘッダのヘッドセットまたはアクセサリの診断データを送信して、Unified Communications Manager の CMR を更新します。

Cisco IP 電話は、ヘッドセットとアクセサリの診断データをユニファイドコミュニケーションマネージャと共有します。この情報は、CMR レコードの以下のフィールドに保存されます。

- SN—ヘッドセットまたはアクセサリのシリアル番号。
- メトリックス—RSSI フレームエラー、接続ドロップの理由、ビーコンの移動、オーディオ設定、および DECT 帯域幅などのヘッドセットとアクセサリのメトリック。

CMR レコードのエクスポートおよび表示方法の詳細については、*Cisco Unified Communications Manager* のコール レポートおよび請求管理ガイドを参照してください 。

（注） ヘッドセット CMR レコードは、シスコ ヘッドセット 500 シリーズに適用されますが、700 シリーズには適用されません。

Unified CM でのエンドポイントの PRT を生成する

この手順を使用して、エンドポイントの問題レポートツール (PRT) をトリガーします。

手順

ステップ 1 Cisco Unified CM 管理から、**[デバイス] > [電話機]** を選択します。

ステップ 2 [**検索** (Find)] をクリックして、ヘッドセットを接続する 1 つまたは複数の電話機を選択します。

ステップ 3 選択した電話機で使用するヘッドセットの PRT ログを収集するには、**[選択対象のPRTを生成する (Generate PRT for Selected)]**をクリックします。

ステップ 4 **[保存]** をクリックします。

Cisco Unified Communications Managerは、SIP Notify メッセージを送信して、電話機のログ収集をリモートでトリガーし、「カスタマーサポートアップロードURL」パラメータで構成されているログサーバにアップロードします。

RTMT でエンドポイントの PRT を生成する

デバイスまたはエンドポイントは、診断およびトラブルシューティング用の重大なイベントごとにアラームを生成します。 これらのアラームは、Cisco Unified Real-Time Monitoring Tool (RTMT)の[トレースコレクション（Trace Collection）]メニュー、または [デバイスモニタリング (Device Monitoring)] メニューで利用可能な問題レポートツール (PRT) を使用して生成されます。

手順

ステップ 1 [Trace & Log Central]オプションを開きます。

ステップ 2 Trace & Log Central ツリー階層で、**Generate PRT** を選択します。
[PRT の生成ウィザード] が表示されます。

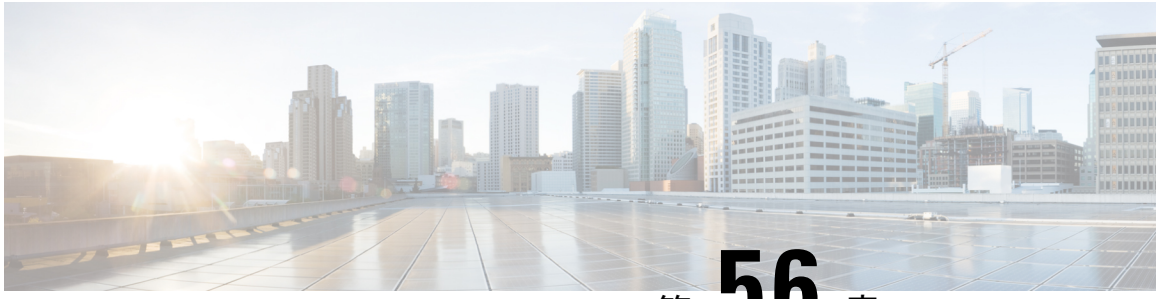
ステップ 3 Cisco Unified CM 管理ユーザインターフェイスの [電話の検索と電話一覧] ページで設定したデバイス名を入力します。

ステップ 4 **PRT の生成** をクリックします。

生成されたレポートは、**Customer support upload URL** にアップロードされます。 ダウンロードオプションは、**カスタマーサポートのアップロード URL**パラメータが、Cisco Unified CM 管

理のユーザインターフェイスで、エンタープライズ、プロファイル、またはデバイスレベルで構成されている場合にのみ利用できます。

（注） [エンタープライズ(Enterprise)]、[プロファイル(Profile)]、または[デバイス（Device)]レベル構成ページの設定で、**カスタマーサポートアップロード URL** パラメータを確認します。 それ以外の場合、PRT は生成できません。



第 56 章

ヘッドセット サービス

ヘッドセット サービスの概要

ヘッドセット サービスを使用すると、サポートされているデバイスにシスコ ヘッドセットを接続して、ヘッドセットベースのエクステンションモビリティなどの、シンプルで統合されたユーザ エクスペリエンスを提供できます。

ヘッドセット ベースのエクステンションモビリティは、ヘッドセット サービスの下で導入された最初の機能です。 シスコ ヘッドセットをエクステンションモビリティ対応デバイスに接続すると、エクステンションモビリティのログインとログアウトにシームレスなログインエクスペリエンスが提供されます。

ヘッドセット サービスを使用すると、管理者とエンド ユーザが、自所有のデバイス、共有スペース、共有エリア デバイスなど、任意のデバイスのヘッドセットを関連付けられます。 この関連付けは、認証を行い、ユーザに合わせてカスタマイズされたエクスペリエンスを作成するのに役立ちます。 この機能は、有線およびワイヤレスの両方のヘッドセットをサポートします。

ヘッドセットの関連付けによって、ユーザの ID がヘッドセットに割り当てされます。 ユーザ ID が必要なサービスにログインできます。

この Unified Communications Managerインターフェイスにより、管理者は次のアクセスを実行できます。

- ヘッドセットとエンドユーザの関連付けおよび関連付け解除、シリアル番号の解除をします。
- ヘッドセットベースのエクステンション モビリティを有効化します。
- バルク ユーザをヘッドセットの関連付けにインポートおよびエクスポートします。

（注） ヘッドセット ベースのエクステンションモビリティ のログインは、拡張機能ではサポートされていません。

ヘッドセットベースのエクステンションモビリティのログインは、モバイルおよびリモートアクセス（MRA）をサポートするデバイスで機能します。 互換性のある電話機のファームウェアバージョンは 14.1(1) です。

ヘッドセット ベースのエクステンションモビリティのログインは、同じユーザー ID がヘッドセットと電話機の両方を制御している場合は機能しません。

ヘッドセット サービスの前提

- エンドユーザがすでに Unified Communications Manager に作成されています。
- ヘッドセットを使用してエクステンションモビリティにログインする場合は、エクステンションモビリティがユーザのデバイスで有効になっている必要があります。 また、**[エクステンションモビリティのサインインおよびサインアウトオプションにヘッドセットを許可する（Allow headset for Extension Mobility sign in and sign out）]** オプションが有効になっているため、ユーザはシスコヘッドセットを使用してエクステンションモビリティのログインまたはログアウトを実行できます。

（注） ヘッドセットベースのエクステンションモビリティ機能は、88XX および 78XX シリーズの Cisco IP 電話の最新ファームウェアのみをサポートしています。

ヘッドセットサービスの管理者設定タスクフロー

管理者は次のタスクを使用して、ヘッドセットをユーザに関連付け、ヘッドセットベースのエクステンションモビリティを有効にできます。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザーへのヘッドセットの関連付け（855 ページ）	シリアル番号をユーザに関連付ける方法および関連付け解除する方法を指定します。
ステップ 2	エンド ユーザ ヘッドセットの関連付けの管理 （856 ページ）	**オプション**: エンドユーザがデバイスのヘッドセットの関連付けを作成できます。

	コマンドまたはアクション	目的
ステップ 3	ヘッドセットベースのエクステンションモビリティの有効化 （856 ページ）	Unified Communications Managerからヘッドセットのエクステンションモビリティを有効にします。
ステップ 4	ピンレス エクステンションモビリティの有効化 （857 ページ）	ピンレスエクステンションモビリティを有効にします。
ステップ 5	エクステンションモビリティヘッドセットのログアウト タイマーの設定 （858 ページ）	ヘッドセットの自動ログアウトのタイムアウト設定を構成します。

ユーザーへのヘッドセットの関連付け

ユーザにヘッドセットを関連付けるには、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]** をクリックし、ヘッドセットを関連付ける既存のユーザを選択します。

ステップ 3 **[関連付けられたヘッドセット]**セクションに、割り当てるヘッドセットのシリアル番号を入力します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 選択したユーザに他のヘッドセットを関連付けるには **[(+)]** をクリックします。

（注） 特定のユーザに最大 15 個のヘッドセットを関連付けることができます。 ヘッドセットのシリアル番号は、個々のヘッドセットごとに固有です。 同じヘッドセットを2人のユーザに関連付けることはできません。 ヘッドセットの関連付けを別のユーザに移動するには、最初のユーザからヘッドセットの関連付けを解除する必要があります。

特定のヘッドセットのシリアル番号の位置については、そのヘッドセットモデルのヘッドセットの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 6 （任意）**[(-)]**をクリックすると、選択したユーザのヘッドセットシリアル番号の関連付けが解除されます。

ステップ 7 **[詳細の表示 (details)]** リンクをクリックすると、ヘッドセットのインベントリの詳細が表示されます。 詳細については、「ヘッドセットとアクセサリの管理」の「ヘッドセット インベントリ設定」セクションを参照して、ヘッドセットの詳細を確認します。

エンド ユーザ ヘッドセットの関連付けの管理

オプション: デバイス画面の [ヘッドセットの関連付け] メニュー オプションを使用してエンド ユーザがヘッドセットを関連付け可能にするには、**Unified Communication Manager** の設定を構成するには、この手順 を使用します。

手順

ステップ 1 [Cisco Unified CM 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 **[エンタープライズ パラメータの設定]** セクションで、エンド ユーザ のヘッドセットをデバイスに関連付ける場合は、次のいずれかを選択します。

- **[すべてのデバイスからヘッドセットの関連付けを開始する場合はユーザをプロンプトする]**を選択し、ヘッドセットが初めてデバイスに接続された場合、**[ヘッドセットの関連付け]** 画面が表示されます。 デフォルトでは、このパラメータ値が選択されています。
- **[ヘッドセットの関連付け]** 画面に**[エクステンションモビリティ対応デバイスからのみヘッドセットの関連付けを開始する場合はユーザをプロンプトする]**を選択し、エクステンションモビリティ対応デバイスにのみ表示します。
- すべてのデバイスで **[ヘッドセットの関連付け]** 画面を無効にするには、**[すべてのデバイスからヘッドセットの関連付けを開始するようにユーザをプロンプトしない]** を選択します。 この設定では、ユーザがデバイス メニューから手動でヘッドセットの関連付けを開始することはできません。

（注） 設定の変更は、エンド ユーザに関連付けられているヘッドセットには適用できません。

ステップ 3 構成の変更を有効にするには、[保存して構成を適用 (Save and Apply Config)] をクリックします。

ヒント 詳細については、**[企業パラメータの設定]** ウィンドウで、パラメータ名または疑問符 **(?)**アイコンをクリックします。

ヘッドセットベースのエクステンション モビリティの有効化

ユーザが関連付けられたヘッドセットからエクステンションモビリティにログインするには、この手順を使用します。

始める前に

ヘッドセットユーザがヘッドセットを使用してエクステンションモビリティにログイン、使用、およびログアウトできるエクステンションモビリティサービスに Cisco IP 電話とデバイス

プロファイルを設定していることを確認してください。詳細については、エクステンションモビリティへの登録 （506 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）]**。

ステップ 2 **[サーバ]** フィールドで、Cisco Extension Mobility サービスを実行している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 Extension Mobility]を選択します。

ステップ 4 **ヘッドセット ベースのエクステンションモビリティ**フィールドで、関連付けられたヘッドセットをエクステンションモビリティのログインに使用するには、次のいずれかを選択します。

- **[エクステンションモビリティのヘッドセットのサインインとサインアウトを許可する]** を選択して、ヘッドセットユーザがエクステンションモビリティでサインインとサインアウトできるようにします。 デフォルトでは、このパラメータ値が選択されています。
- **[エクステンションモビリティ のサインインにヘッドセットを許可しない]**を選択して、ヘッドセットユーザのエクステンションモビリティでのサインインとサインアウトを制限します。 このオプションを選択すると、ヘッドセットの接続時にエンド ユーザにエクステンションモビリティのログインまたはログアウト画面が表示されます。

ステップ 5 **[保存（Save）]** をクリックします。

ピンレス エクステンションモビリティの有効化

ユーザに関連付けられたヘッドセットを使用して、ピンレスでエクステンションモビリティにログインするには、次の手順を実行します。

（注） この機能は、リリース 12.5(1)SU3 以降でサポートされています。

始める前に

[サービスパラメータ設定] > [ヘッドセット接続後の自動ログインタイマー（秒）] フィールドで、システムがユーザー入力を待機してから拡張モビリティプロファイルに自動的にサインインするまでの最大時間を指定します。

（注） 指定した最大継続時間が有効になるのは、**ヘッドセット ベースのログイン フィールドの PIN の入力**が **[必須ではない]** に設定されている場合のみです 。

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）]**。

ステップ 2 **[サーバ]** フィールドで、Cisco Extension Mobility サービスを実行している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 Extension Mobility]を選択します。

ステップ 4 **ヘッドセット ベースのログイン フィールドの PIN エントリ**で、次のいずれかを選択して、ピンレス エクステンションモビリティのログインを有効または無効にします。

- エクステンションモビリティ ログイン用の PIN を入力するようユーザにプロンプトする場合は、**[必須]** を選択します。デフォルトでは、このパラメータ値が選択されています。
- エクステンションモビリティに 1 分以内に自動的にログインする場合は、**[不要]** を選択します。 ユーザは、電話機の UI で PIN の詳細を入力するようプロンプトされません。

重要 ユーザが設定された時間内に自動的にサインアウトしたり、有線またはワイヤレス ヘッドセットを使用して手動でログアウトした場合は、**[キャンセル]** をクリックして、指定された時間内の自動サインインを避け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。

エクステンションモビリティ ヘッドセットのログアウト タイマーの設定

自動ログアウトのタイムアウト設定を構成するには、次の手順を使用します。

（注） **[サービス パラメータ設定]** ウィンドウのヘッドセット ベースのエクステンションモビリティ サービス パラメータのパラメータが **[エクステンションモビリティのサインインとサインアウトをヘッドセットに許可しない]** に設定されている場合、自動ログアウト タイマー値を設定しても効果はありません。

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。**サービス > サービスパラメータ**.

ステップ 2 **[サーバ]** フィールドで、Cisco Extension Mobility サービスを実行している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 Extension Mobility]を選択します。

ステップ 4 **[ヘッドセット切断後の自動ログアウト タイマー]** フィールドに、ヘッドセットがデバイスから切断された場合にシステムがユーザの入力を待ち続け、自動的にユーザがログアウトするまでの最大継続時間値を入力します。

（注） デフォルトでは、5 分で設定されています。 最大値を 15 分に設定できます。

ステップ 5 **[保存（Save）]** をクリックします。

ヘッドセット サービスのエンド ユーザ関連付けタスク フロー

エンド ユーザは次のタスクを使用してヘッドセットを関連付け、関連付けられた ID を使用してエクステンションモビリティを使用してログインできます。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザ ヘッドセットの関連付け （859 ページ）	エンド ユーザへのヘッドセットの関連付けを作成します。
ステップ 2	ヘッドセットの関連付けをスキップする （860 ページ）	特定のエンド ユーザのヘッドセット関連付けをスキップできます。
ステップ 3	ヘッドセットを使用したエクステンションモビリティのログイン （860 ページ）	エクステンションモビリティのログインに関連付けられたヘッドセットを使用することで、カスタマイズしたエクスペリエンスを実現します。
ステップ 4	ヘッドセットを使用したエクステンションモビリティからユーザーをログアウトする （861 ページ）	エクステンションモビリティからヘッドセットをデフォルトの設定時間内にログアウトするのに役立ちます。

ユーザ ヘッドセットの関連付け

ユーザにヘッドセットを関連付けるには、次の手順を使用します。

手順

ステップ 1 ヘッドセットを Cisco IP 電話に接続します。

*[*ヘッドセットをユーザに関連付ける*]* ポップアップ画面が IP Phone の画面に表示されます。

ユーザ名は、デバイスが共有スペースまたは共有エリアにあるか、ユーザがデバイスに関連付けられている場合に自動的に入力されます。 デバイスが匿名の場合、**[ユーザ ID]** フィールドは空白で、エンド ユーザはユーザの資格情報を提供するヘッドセットを関連付けます。

ステップ 2 **ユーザ ID** および **PIN** を入力または変更します。 ログイン情報が分からない場合は、管理者に問い合わせてください。

ステップ 3 [送信（Submit）]をクリックします。

ヘッドセット メッセージの調整が成功すると、ユーザ名が表示されます。

無効なクレデンシャル (**ユーザ ID** または **PIN**)を 3 回以上入力すると 、Cisco IP 電話にエラーメッセージが表示されます。

ヘッドセットの関連付けに失敗した場合は、ヘッドセットの接続を切断接続して、有効なログイン情報を提供するか、管理者に問い合わせてください。

ステップ 4 （任意） Cisco IP 電話を介して手動でヘッドセットを関連付ける場合は、**[設定]** > **[アクセサリ]** > **[シスコ ヘッドセットのセットアップ]** > **[ユーザの関連付け]** を選択します 。

（注） ヘッドセットが接続されていない場合、**[ユーザの関連付け]**オプションはグレー表示になります。 有効にするには、ヘッドセットをデバイスに接続します。

ヘッドセットの関連付けをスキップする

ユーザへのヘッドセットの関連付けをスキップするには、次の手順を使用します。

手順

ステップ 1 ヘッドセットを Cisco IP 電話に接続します。

ステップ 2 ヘッドセットをユーザに関連付ける前に **[終了]** をクリックします。

ステップ 3 ヘッドセットを関連付けない場合は、**[はい]** をクリックします。
ヘッドセットの関連付け画面は、デバイスへの接続時にプロンプトされません。 同じヘッドセットが別のデバイスに接続されている場合、**[ヘッドセットをユーザに関連付ける]** ポップアップ画面が Cisco IP 電話の画面に表示され、関連付けプロセスをユーザに移動します。

ヘッドセットを使用したエクステンションモビリティのログイン

ユーザが関連付けられているヘッドセットを使用してエクステンションモビリティにログインするには、この手順を使用します。

手順

ステップ 1 ヘッドセットを Cisco IP 電話に接続します。

ステップ 2 ヘッドセットが関連付けられている場合は、次の手順を実行します。

a) ヘッドセットをユーザに関連付ける場合は、**ユーザ ID** と **PIN** を入力します。

b) [送信（Submit）]をクリックします。

ログイン画面に、関連付けられたユーザ ID の成功メッセージが表示され、ユーザはエクステンションモビリティでログインできます。

c) **[サインイン]** を クリックしてエクステンションモビリティのログインを完了します。

ステップ 3 ヘッドセットがすでにユーザに関連付けられている場合は、次の手順を実行します。

a) エクステンションモビリティでログインの **PIN** を入力します。

b) 必要なユーザ プロファイルを選択します。

c) [送信（Submit）]をクリックします。

ステップ 4 ユーザがすでにデバイスのエクステンションモビリティにログインしている場合に、以前に関連付けられているヘッドセットを別のユーザが接続すると、ログアウト画面が表示され、ユーザは以前にログインしているユーザからサインアウトできます。

ステップ 5 以前のプロファイルからログアウトするには **[はい]** をクリックします。

ステップ 6 エクステンションモビリティでログインの **PIN** を入力します。

ステップ 7 [送信（Submit）]をクリックします。

（注） 電話機はデバイス プロファイルが変更されるごとにリセットされ、ユーザ プロファイルが元のプロファイルに変更されます。

ヘッドセットを使用したエクステンションモビリティからユーザーをログアウトする

エクステンションモビリティ対応デバイスからヘッドセットをサインアウトするには、次の手順を使用します。

手順

ステップ 1 Cisco IP 電話からヘッドセットを取り外します。

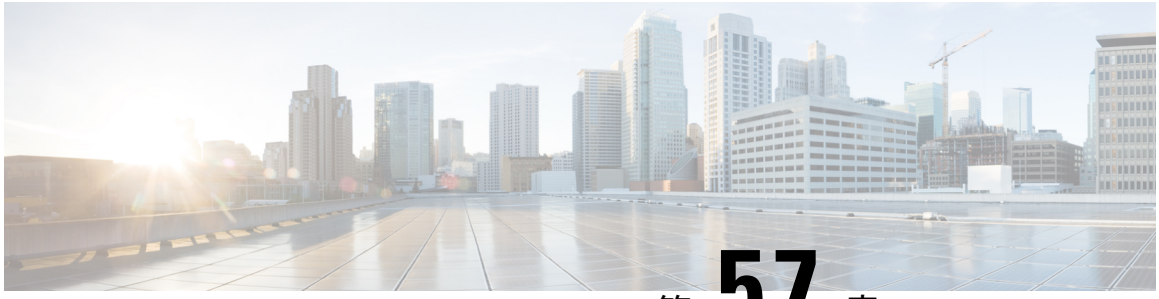
ステップ 2 **[サインアウト（Sign out）]** をクリックします。

（注） 電話機がリセットされ、デバイスプロファイルが元のデバイスプロファイルに変更されます。

対応中のコール (1 対 1 のコールまたは会議コール) 中にヘッドセットを取り外した場合、そのコールは終了しません。エクステンションモビリティのサインアウトは、コールが終了した場合にのみ発生します。

ワイヤレス ヘッドセットから手動でログアウトしたり、範囲を外したりしていない場合は、設定された時間内に自動的にサインアウトされます。 デフォルトでは、設定時間は 5 分です。 詳細については、エクステンションモビリティ ヘッドセットのログアウト タイマーの設定 （858 ページ）を参照してください。

ステップ 3 現在のエクステンションモビリティ セッションを保持する場合は、**[キャンセル]**をクリックします。 デフォルトの設定時間内に再接続すると、ユーザ プロファイルが保持され、リセットが回避されます。



第 57 章

IVR および電話サービスを使用したネイティブ電話機の移行

IVR および電話サービスを使用したネイティブ電話機の移行の概要

電話機の移行機能は、Unified Communications Manager 特有の、簡単でわかりやすい Cisco IP 電話移行ソリューションです。廃止または故障した電話機への置き換えコストと複雑さを最小限に抑えるために使用されます。 このソリューションを使用すると、エンドユーザまたは管理者が、簡単なユーザインターフェイスですべての設定を古い電話機から新しい電話機に簡単に移行できます。 ソリューションは、電話機を移行する次の方法をサポートしています。

- **セルフプロビジョニング IVR サービスの使用**
- **電話移行サービスの使用**
- **Cisco Unified CM の管理インターフェイスの使用**

次の表では、さまざまな電話機移行オプションを簡単に比較しています。

表 *66 :* 異なる電話機の移行オプションと検討事項

	セルフプロビジョニング IVR サービスの使用	電話移行サービスの使用	Unified CM の管理インターフェイスの使用
エンドユーザまたは管理者が駆動する電話機の移行	エンドユーザ (セルフサービス)	エンドユーザ (セルフサービス)	管理者
要自動登録	可	不可	不可
移行手順	• 新しい電話機の自動登録 • セルフプロビジョニング IVR 番号のダイヤル • 音声プロンプトに従う	• 新しい電話機をネットワークに差し込む • プライマリ内線および PIN のキー入力 (オプション)	• Cisco Unified CM の管理インターフェイスへのサインイン • 古い電話機の [電話設定] ページの、[電話機を移行する] オプション • 新しい電話機のタイプ (モデル&プロトコル)と MAC アドレスを入力
管理者の関与	中	低	高

（注） セルフプロビジョニング IVR サービスと電話機移行サービスを使用した電話機の移行では、セルフサービスとしてのエンドユーザによる電話機の移行が容易です。管理者は、これらの方法を使用して、エンド ユーザまたは一般電話機 (ロビー電話機など) に代わって電話機を移行できます。

（注） 電話の移行中に、エンド ユーザが暗証番号を覚えていない場合は、管理者がエンド ユーザに対して、必要に応じてセルフ ケア ポータルにログインして暗証番号を変更してください。

電話機移行用の企業パラメータ

移行は、[エンタープライズ パラメータの設定] ページで次の 2 つのパラメータによって異なります。

- **エンド ユーザに代替電話機をプロビジョニングする場合**: **既存の電話機の保持** (デフォルト オプション) の選択、または**そのエンド ユーザの既存の電話機の削除**を選択できます。 **[既存の電話機を保持]**オプションを選択した場合、移行中に古い電話機が移行済みとしてマークされ、[電話機の検索とリスト]ページでフィルタリングして移行レポートを生成できます。

（注） 管理者が電話移行用に **[既存の電話機を保持]** オプションを選択すると、合計 2 つのライセンスが使われます。つまり、既存の電話機に対してそれぞれ 1 つのライセンスを、移行用にピックアップした新しい電話機です。

（注） 電話機の移行中に、管理者が電話機を移行するために **[既存の電話機を保持]** オプションを選択する場合、インターコム DN は新しいデバイスに 移行されません。 **[そのエンドユーザに対して既存の電話機を削除]** オプションを選択すると、インターコム DN 情報も移行されます。

- **移行された電話機のセキュリティ プロファイル**: このオプションは、電話機の移行中に、移行済み電話機に適用されるセキュリティ プロファイルのタイプ (古い電話機はセキュア モード) を決定します。 **非セキュア** プロファイルを選択すると、デバイスは非セキュア モードになります。

- **電話機の移行ユーザ ID プロンプト**: このパラメータは、ユーザがセルフサービス ユーザ ID を使用して電話機の移行を続行できるかどうか、またはプライマリ内線番号を使用できるかどうかを決定します。 **[エンドユーザセルフサービスユーザ ID を使用]** オプションを選択した場合、エンド ユーザは、電話の移行を実行する前に、固有のセルフサービス ユーザ ID を入力するようプロンプトされます。 **[エンドユーザプライマリ内線番号を使用]**オプションを選択した場合は、プライマリ内線番号の入力後に電話機を移行できます。このモードでは、異なるルート パーティションに同じ DN が存在する場合、IVR または電話機移行サービスを使用した電話機の移行はできません。

  デフォルト値は、**[エンドユーザ プライマリ内線を使用]** です。

安全な電話移行を容易にするために、次の Standard Universal Phone セキュリティ プロファイル テンプレートが追加されています。 古い電話機のセキュリティ プロファイルに基づいて、新しい電話機は次の新しいプロファイルのいずれかを選択します。

- Universal Device Template - セキュリティ プロファイル - 非セキュア
- Universal Device Template - セキュリティ プロファイル – 認証済み
- Universal Device Template - セキュリティ プロファイル – 暗号化済み
- Universal Device Template - セキュリティ プロファイル - 暗号化済み - Device_TFTP

• Universal Device Template - セキュリティ プロファイル - 暗号化済み EC 優先

次の表は、電話機の移行後に新しいデバイスのセキュリティ プロファイルのマッピングを示します。

表 *67*: 電話機のセキュリティ プロファイルの移行データ

古いセキュリティ プロファイル設定				新しいマップされたプロファイル名
[デバイスセキュリティモード (Device Security Mode)]	**TFTP 暗号化設定**	**Transport Type**	**キー順序**	
非セキュア	不可	[TCP]	RSA	Universal Device Template - セキュリティ プロファイル - 非セキュア
認証済み	不可	TLS	RSA	Universal Device Template - セキュリティ プロファイル – 認証済み
暗号化済み	不可	TLS	RSA	Universal Device Template - セキュリティ プロファイル–暗号化済み
暗号化済み	可	TLS	RSA	Universal Device Template - セキュリティ プロファイル - 暗号化済み - Device_TFTP
暗号化済み	可	TLS	EC 優先、RSA バックアップ	Universal Device Template - セキュリティ プロファイル - 暗号化済み - Device_TFTP
暗号化済み	不可	TLS	EC 優先、RSA バックアップ	Universal Device Template - セキュリティ プロファイル - 暗号化済み EC 優先

電話機移行の前提条件

セルフプロビジョニング IVR の使用

エンドユーザが移行でセルフプロビジョニングを使用できるようにする前に、次の設定を構成する必要があります。

- 自動登録の有効化
- エンドユーザには、プライマリ内線番号が必要です。プライマリ DN が電話機またはデバイス上で常に回線 1 であることを確認します。
- エンドユーザは、ユニバーサル回線テンプレート、ユニバーサルデバイステンプレート、および自己プロビジョニングが有効になっている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る必要があります。
- 適切な「CTI ルートポイント」と「アプリケーションユーザ」の設定が選択されていることを確認します。
- セルフプロビジョニングの IVR サービスを有効にします。

電話移行サービスの使用

エンドユーザが移行で電話移行サービスを使用できるようにする前に、次の設定を構成する必要があります。

- 自動登録の無効化
- エンドユーザには、プライマリ内線番号が必要です。プライマリ DN が電話機またはデバイス上で常に回線 1 であることを確認します。
- サポートされる電話機モデル: 88XX、78XX、8832、および 7832。
- サポートされている電話機のバージョンは、リリース 12.8.1 以上です。

セルフプロビジョニング IVR を使用した電話機の移行タスクフロー

次のタスク フローを使用して、電話機の移行手順を説明します。

このワークフローを完了すると、セルフプロビジョニングの IVR サービスを設定したり、古いまたは異常な Cisco IP 電話を移行したり、移行された電話リストを追跡したり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	セルフプロビジョニングのサービスの有効化 （869 ページ）	Cisco Unified Serviceability で、**[セルフプロビジョニング IVR（Self-Provisioning IVR）]** サービスと **[CTI Manager（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 （869 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 （870 ページ）	セルフプロビジョニングの IVR サービスを処理するために、CTI ルートポイントを設定します。
ステップ 4	CTI ルートポイントのディレクトリ番号を追加する （870 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 （871 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 （872 ページ）	自己プロビジョニングシステムの設定を構成します。
ステップ 7	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 （873 ページ）	ユーザが割り当てられているユーザプロファイルで電話機をセルフプロビジョニングできるようにします。
ステップ 8	次のいずれかの手順を使用して電話機を移行します。 • セルフプロビジョニング IVR を使用した電話機の移行 (管理者) （874 ページ） • セルフプロビジョニング IVR を使用した電話機の移行 (電話機ユーザ) （874 ページ）	自分に適用される移行手順を選択します。 セルフプロビジョニングの IVR は、管理者または電話機のいずれかのユーザが電話機を移行する際に使用できます。
ステップ 9	電話機移行レポートの表示 （880 ページ）	移行の後、移行された Cisco IP 電話を示すレポートを表示します。

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にするには、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）] > [サービスの有効化（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]** で、**Cisco CTI Manager** を確認します。

ステップ 4 **CTI サービス**で、**セルフプロビジョニングの IVR** を確認します。

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 **開始ディレクトリ番号**と**終了ディレクトリ番号**フィールドを使用して、プロビジョニングされた電話機に適用する一連のディレクトリ番号を入力します。

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 this 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 ルートポイントのディレクトリ番号を追加する

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 管理（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 **[ディレクトリ番号]**フィールドで、セルフプロビジョニングの IVR サービスにアクセスするためにユーザにダイヤルする内線番号を入力します。

ステップ 5 **[保存]** をクリックします。

ステップ 6 **[ディレクトリ番号設定（Directory Number 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] 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。
- ユーザがセルフプロビジョニングを使用して以前に割り当てられた電話機を無効にしたい場合は、古いデバイスのエンド ユーザに関連付けられているユーザ プロファイル ページで、別のエンド ユーザに割り当てられている電話機の **[別のエンドユーザーにすでに割り当てられている電話のプロビジョニングを許可する]** 設定を確認します。 以前に割り当てられた電話機をユーザが再割り当てできるのは、古いデバイスに関連付けられているユーザプロファイル内でこのチェックボックスをオンにした場合のみです。

ステップ 5 **[保存（Save）]** をクリックします。

電話機移行タスク

セルフプロビジョニング認証をセットアップした後、次の手順を実行して電話機を移行します。

セルフプロビジョニング IVR を使用した電話機の移行 (管理者)

管理者はこの手順を使用して、エンドユーザの代わりに Cisco IP 電話を移行したり、一般的な電話機 (ロビーフォンなど) を移行したりできます。

始める前に

移行を進める前に、古い電話機が「未登録」状態になっていることを確認します。 新しい電話機をネットワークに接続して、電話機が登録されてから移行タスクを実行することができます。 移行が正常に完了すると、デバイスはユーザの電話設定データに再登録されます。

手順

ステップ 1 セルフプロビジョニングの IVR に割り当てられている内線番号を新しい電話機からダイヤルします。

ステップ 2 **2** を 押すと、既存の電話機が置き換え可能です。

ステップ 3 エンドユーザの電話機または共通の電話のプライマリ内線番号の後にポンド キー (#) を入力します。

ステップ 4 **認証コード**の後にポンド キー (#) を入力 します 。

移行は、認証が正常に行われた後に開始されます。 移行の後、電話機は、エンドユーザの古い電話から移行された設定で再起動します。

セルフプロビジョニング IVR を使用した電話機の移行 (電話機ユーザ)

電話機のユーザはこの手順を使用して、新しい Cisco IP 電話に移行できます。

始める前に

移行を進める前に、古い電話機が「未登録」状態になっていることを確認します。 新しい電話機をネットワークに接続して、電話機が登録されてから移行タスクを実行することができます。 移行が正常に完了すると、デバイスはユーザの電話設定データに再登録されます。

手順

ステップ 1 セルフプロビジョニングの IVR に割り当てられている内線番号を新しいCisco IP 電話からダイヤルします。

ステップ 2 2 を 押すと、既存の電話機が置き換え可能です。

ステップ 3 電話機のプライマリ内線番号の後にポンド キー(#)を入力します。

ステップ 4 ポンド キー (#) の後に PIN を入力します。

移行は、認証が正常に行われた後に開始されます。 移行が正常に実行された後、電話機は古い電話から移行された設定で再実行されます。

（注） 電話機を別のユーザに割り当てる場合、管理者がユーザの **[ユーザ プロファイル ウィンドウで別のエンドユーザに割り当てられている電話機のプロビジョニングを許可]** オプションが有効になっている場合、電話機のユーザは電話機を再プロビジョニングできます。 このオプションについて管理者に問い合わせてください。

電話機移行サービスを使用した電話機移行タスクフロー

次のタスク フローを使用して、電話機移行サービスを使用した電話機の移行手順を説明します。

このワークフローを完了すると、古いまたは異常な Cisco IP 電話を移行したり、移行された電話リストを追跡したり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	自動登録の無効化 （876 ページ）	電話機の移行前に、自動登録パラメータを無効にします。
ステップ 2	デフォルト電話機の負荷のセットアップ （876 ページ）	電話機の移行サービスの前に、デフォルトの電話機の負荷を設定します。
ステップ 3	セルフプロビジョニング認証の設定 （876 ページ）	必要なセルフプロビジョニング認証を設定します。
ステップ 4	次のいずれかの手順を使用して電話機を移行します。 • 電話機移行サービスを使用した電話機の移行 (管理者) （877 ページ） • 電話機移行サービス (電話機ユーザー) を使用して電話機を移行する （878 ページ）	自分に適用される移行手順を選択します。 電話機の移行サービスは、管理者または電話機のいずれかのユーザが電話機を移行する際に使用できます。
ステップ 5	電話機移行レポートの表示 （880 ページ）	移行の後、移行された Cisco IP 電話を示すレポートを表示します。

自動登録の無効化

電話機移行サービスを使用するには、自動登録を無効に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] > [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 **[このCisco Unified Communications Manager では自動登録は無効にする]** チェックボックスをオンにします。

ステップ 4 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 5 **[保存（Save）]** をクリックします。

デフォルト電話機の負荷のセットアップ

電話機の移行サービスの前にデフォルトの電話機の負荷を設定するには、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] > [デバイスの設定] > [デバイスのデフォルト]** を選択します。

ステップ 2 移行に必要な電話機モデルを選択します。

ステップ 3 電話機の負荷を入力し、電話機の負荷の**[負荷の入れ替え]**ボタンをクリックしてデフォルトの電話機の負荷になるようにします。

ステップ 4 **[保存（Save）]** をクリックします。

セルフプロビジョニング認証の設定

電話機移行サービスは、セルフ プロビジョニング システム設定を使用して、電話機を移行する前にユーザを認証します。

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**：セルフ プロビジョニングを使用するには、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**：エンド ユーザは認証なしでセルフ プロビジョニング オプションにアクセスできます。

ステップ 3 セルフ プロビジョニング機能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、セルフ プロビジョニング オプションがエンド 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 **[保存（Save）]** をクリックします。

電話機移行タスク

セルフプロビジョニング認証をセットアップした後、次の手順を実行して電話機を移行します。

電話機移行サービスを使用した電話機の移行 (管理者)

管理者はこの手順を使用して、エンドユーザの代わりに Cisco IP 電話を移行したり、一般的な電話機 (ロビーフォンなど) を移行したりできます。

始める前に

移行を進める前に、古い電話機が「未登録」状態になっていることを確認します。 新しい電話機をネットワークに接続し、電話機の移行またはプロビジョニングのプロンプトが表示されるまで待機して、移行プロセスを開始できます。 移行が正常に完了すると、デバイスはユーザの電話設定データに再登録されます。

手順

ステップ 1 新しい Cisco IP 電話をネットワークに接続します。

ステップ 2 オプション **2** を選択します。

（注） 管理者がアクティベーションコードベースのデバイスの導入準備または電話機の移行を設定していない場合、Unified Communications Manager の 11.5(1)SU8 バージョンでアクティベーションコードをサポートしていない場合、電話機にはプライマリ内線番号を入力する画面が表示されます。

ステップ 3 お使いの電話機のプライマリ内線番号を入力します。

ステップ 4 **認証コード**を入力します。

移行は、認証が正常に行われた後に開始されます。 移行が正常に実行された後、電話機は古い電話から移行された設定で再実行されます。

（注） [デバイスのデフォルト設定] ページの **[自動登録]** として **[オンプレミスの導入準備方式]** オプションが選択されているシナリオを検討してください。 電話機の移行の実行中に、エラーメッセージが表示されたときに **[EXIT]** ボタンまたは **[BACK]** ボタンのいずれかを押すと、予想される遅延の後、最初の電話機移行画面に直接移動します。この遅延は、電話機が Unified CM に再登録しようとして、Unified Communications Manager サーバで自動登録が無効になっている場合に発生します。

（注） 同じプライマリ内線を持つユーザ用のデバイスが複数ある場合、ユーザは、移行するデバイスを選択するように求めます。 詳細については、電話機の移行サービス: 複数のデバイスを割り当てられたユーザー （882 ページ） を参照してください。

電話機移行サービス (電話機ユーザー) を使用して電話機を移行する

電話機のユーザはこの手順で、非 IVR 方式を使用して新しい Cisco IP 電話に移行できます。電話機をネットワークに接続すると、電話機は起動して設定を試行します。 デフォルトの電話機負荷から、ユーザは [新しい電話機のプロビジョニング] または [既存の電話機の置き換え] のいずれかを選択するオプションを選択できます。

（注） エンド ユーザは、古いデバイスの所有者である場合にのみ移行を実行する必要があります。

（注） **エンドユーザーに代替電話機をプロビジョニングする場合（When Provisioning a Replacement Phone for an End User）**エンタープライズパラメータから **[既存の電話機を保持（Retain Existing Phone(s)）]** オプションを選択した場合で、かつ電話テンプレートを使用して電話を移行する場合、移行された古い電話設定の詳細は [リストの検索（Find List）] ページに一覧表示されません。 成功した新しい電話移行の詳細のみが一覧表示されます。 これは、**[既存の電話機を保持（Retain Existing Phone(s)）]** オプションは、電話テンプレートではなく、電話タイプに基づく電話の移行にのみ適用できるためです。

始める前に

移行を進める前に、古い電話機が「未登録」状態になっていることを確認します。新しい電話機をネットワークに接続し、電話機の移行またはプロビジョニングのプロンプトが表示されるまで待機して、移行プロセスを開始できます。 移行が正常に完了すると、デバイスはユーザの電話設定データに再登録されます。

手順

ステップ 1 新しい Cisco IP 電話をネットワークに接続します。

ステップ 2 オプション **2** を選択して、既存の電話機と置き換えます。

（注） 管理者がアクティベーション コード ベースのデバイス オンボーディングを構成していない場合、または、アクティベーション コードをサポートしていない 11.5(1)SU8 バージョンの Unified Communications Manager で電話の移行が行われた場合、電話はプライマリ内線番号を入力する画面を表示します。

ステップ 3 お使いの電話機のプライマリ内線番号を入力します。

ステップ 4 **PIN** を入力します。

移行は、認証が正常に行われた後に開始されます。 移行が正常に実行された後、電話機は古い電話から移行された設定で再実行されます。

（注） [デバイスのデフォルト設定] ページの **[自動登録]** として **[オンプレミスの導入準備方式]** オプションが選択されているシナリオを検討してください。 電話機の移行の実行中に、エラーメッセージが表示されたときに **[EXIT]** ボタンまたは **[BACK]** ボタンのいずれかを押すと、予想される遅延の後、最初の電話機移行画面に直接移動します。この遅延は、電話機が Unified CM に再登録しようとして、Unified Communications Manager サーバで自動登録が無効になっている場合に発生します。

（注） 同じプライマリ内線を持つユーザに複数のデバイスがある場合、ユーザは移行するデバイスを選択するようにプロンプトが表示されます。 詳細については、電話機の移行サービス: 複数のデバイスを割り当てられたユーザー （882 ページ） を参照してください。

電話機移行サービス COP ファイル

11.5 (1) から 11.5(1)SU7 まで Unified Communications Manager の任意のバージョンを実行している場合は、電話機移行サービス COP ファイル（ciscocm-migration-service-11-5-1.zip）をインストールして、ネイティブ電話移行機能のサポートを受け取ります。

COP ファイルのインストールの一部として、Unified Communications Manager で「Tftp restart」サービスが自動的に実行されます。

（注） Phone Migration Service COP ファイルのインストール後に Unified CM をアップグレードする場合は、必ず、Unified CM サーバをネイティブ フォン移行機能をネイティブ サポートしているリリース バージョンにアップグレードしてください。

電話機移行レポートの表示

移行されたすべての Cisco IP 電話のリストを表示するには、この手順を使用します。

手順

ステップ 1 [Cisco Unified CM Administration] で、**[デバイス（Device）] > [電話（Phone）]** の順に選択します。

ステップ 2 [電話機の検索とリスト] ページで、**[電話機検索]** ドロップダウン リストから **[移行(古い電話機)]** を選択します。

ステップ 3 **[検索(Find)]** をクリックします。

移行したすべての古いデバイスのリストを表示できます。 このリストが入力されるのは、[エンタープライズ パラメータ] ページで **[既存の電話機を保持する]** オプションが設定されている場合のみです。

Cisco Unified CM の管理インターフェイスを使用して電話機を移行

Cisco Unified CM の管理インターフェイスの **[電話テンプレート(Phone Template)]** または **[電話タイプ(およびプロトコル)]** オプションのいずれかを使用して電話機を移行するには、この手順を使用します。

手順

ステップ 1 [電話の検索と一覧表示(Find and List Phones)] ウィンドウ（**[デバイス > 電話]** で、移行する Cisco IP 電話の設定を検索します。

ステップ 2 移行する Cisco IP 電話の [電話の設定(Phone Configuration)] ウィンドウで、**[関連リンク(Related Links)]** ドロップダウン リストから **[電話機の移行 (Migrate Phone)]** を選択します。

ステップ 3 次のオプションを使用して、電話機を移行できます。

a) **[電話 テンプレート(Phone Template)]**: 電話機の設定を移行する電話機モデルの電話機テンプレートを選択します。

b) **[電話機のタイプ(およびプロトコル)]**: 電話機の設定を移行する Cisco IP 電話モデルを選択します。

ステップ 4 設定を移行する新しい Cisco Unified IP 電話の **MAC アドレス**を入力します。

ステップ 5 **(オプション)** 新しい電話の説明を入力します。 移行の検討事項と設定の詳細については、*Cisco Unified CM* の管理のオンラインヘルプ ページ を参照してください。

ステップ 6 **[保存]** をクリックします。

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メッセージが表示されたら、**[OK]** をクリックします。 移行後、新しいデバイスは古い電話機の設定を継承します。

移行シナリオ

共有電話を使用している電話機

旧バージョンの電話機にプライマリ DN と複数のデバイスが共有されている場合を考えてみましょう。 これらのデバイスは、同じユーザまたは複数のユーザによって所有されている可能性があります。 共有回線を使用してセルフプロビジョニング IVR または電話機移行サービスの方法で古い電話機を新しい Cisco IP Phone で移行しようとするときに、DN を回線 1 として持つデバイスを所有しているユーザにのみ移行を実行できます。ここで、共有回線の機能設定は、電話機の移行後に引き継がされます。

古い電話機が共有回線機能をサポートしていない場合、古い電話機の移行後に古い電話機の回線が削除されます。 新しい電話機は、電話機を移行した後も古い電話機の回線を保持します。

プロキシ TFTP 上で実行されている電話機の移行サービス

電話機移行サービスを使用したネイティブの電話機の移行は、シスコ プロキシ TFTP サーバの導入モデルをサポートします。

プロキシTFTP上で実行されている電話機移行サービスは、すべてのリモートクラスタ上のプライマリ内線番号を検索し、電話機の移行を完了するために、その電話機を自宅またはローカルの電話機移行サービスにリダイレクトします。

プロキシ セットアップ環境では、Unified Communications Manager サーバは、リモート クラスタ内で同じ DN を持つデバイスを検索します。 オフ クラスタの 1 つにも同じ DN を持つ登録済みまたは未登録の状態のデバイスが複数存在する場合、その特定のオフ クラスタからのデバイスは、電話機の移行とは見なされません。 これは、リリース 11.5(1)SU8 では既知の制限です。

（注） プロキシ TFTP で移行が正常に実行された後、電話機は古い電話から移行された設定で再実行されます。 移行が成功した後、電話機を再起動するには2回のリセットサイクルが必要であることに注意してください。

電話機の移行サービス: 複数のデバイスを割り当てられたユーザー

移行用のプライマリ内線が同じユーザ用のデバイスが複数ある場合は、移行するデバイスを選択するように求めるプロンプトが表示されます。

次の表に、考えられるさまざまな移行シナリオを示します。

表 *68 :* デバイスの一覧と移行のシナリオ

	電話機の移行前のデバイスステータス	移行中の電話機の表示
シナリオ 1	デバイス 1: 登録済み デバイス 2: 未登録	デバイス 2 の電話機の設定が移行されます。
シナリオ 2	デバイス 1: 登録済み デバイス 2: 登録済み デバイス 3: 未登録	デバイス 3 の電話機の設定が移行されます。
シナリオ 3	デバイス 1: 登録済み デバイス 2: 未登録 デバイス 3: 未登録	説明、電話機モデル、およびMACアドレスを含むデバイスリストを表示します。 ユーザは、電話機の移行に必要なリストからデバイスを選択する必要があります。

	電話機の移行前のデバイスステータス	移行中の電話機の表示
シナリオ 4	デバイス 1: 未登録 デバイス 2: 未登録 デバイス 3: 未登録	説明、電話機モデル、およびMACアドレスを含むデバイスリストを表示します。 ユーザは、電話機の移行に必要なリストからデバイスを選択する必要があります。
シナリオ 5	デバイス 1: 登録済み デバイス 2: 登録済み デバイス 3: 登録済み	説明、電話機モデル、およびMACアドレスを含むデバイスリストを表示します。 ユーザは、電話機の移行に必要なリストからデバイスを選択する必要があります。
シナリオ 6	登録済みまたは未登録の状態のデバイスが 3 つ以上	説明、電話機モデル、およびMACアドレスを含むデバイスリストを表示します。 ユーザは、電話機の移行に必要なリストからデバイスを選択する必要があります。

Unified CM パラメータ設定に基づくデバイスの表示

次の表は、Cisco Unified Communications Manager のリリース バージョンと関連する設定に基づく新しい電話機の移行画面の動作を示します。

表 *69* : さまざまな *Unified CM* パラメータ設定に基づくデバイスの表示

管理者による事前設定済みの電話機またはデバイス	企業レベルで自動登録を有効にする	デバイスデフォルト レベルでの導入準備方式	電話機移行サービスのない動作	電話機移行サービスでの動作
不可	可	—	デバイスがネットワークに自動登録されます。	デバイスがネットワークに自動登録されます。
不可	不可	—	デバイスはネットワークへの登録を再試行し、設定されたバックオフタイマーに基づいて再試行を続けます。	電話の代替画面で、プライマリ内線番号とPINの入力がプロンプトされます。

管理者による事前設定済みの電話機またはデバイス	企業レベルで自動登録を有効にする	デバイスデフォルト レベルでの導入準備方式	電話機移行サービスのない動作	電話機移行サービスでの動作
可	該当なし	—	デバイスが事前設定で登録されます。	デバイスが事前設定で登録されます。
不可	可	デバイスの種類をアクティベーション コードに設定	電話の「ようこそ」画面で、「アクティベーションコードを入力してください」というメッセージが表示されます。	電話の代替画面で、「新しい電話機のプロビジョニング」または「既存の電話機の置き換え」のいずれかを選択するプロンプトが表示されます。
不可	不可	[デバイスの種類] を [自動登録] に設定	デバイスはネットワークへの登録を再試行し、断念します。	電話機の代替画面には、「既存の電話機を置き換える」というメッセージが表示されます。
不可	不可	デバイスの種類をアクティベーション コードに設定	電話の「ようこそ」画面で、「アクティベーションコードを入力してください」というメッセージが表示されます。	電話の代替画面で、「新しい電話機のプロビジョニング」または「既存の電話機の置き換え」のいずれかを選択するプロンプトが表示されます。
可	該当なし	該当なし	デバイスはネットワークへの登録を再試行し、設定されたバックオフタイマーに基づいて再試行を続けます。	デバイスが事前設定で登録されます。

エクステンションモビリティを使用する電話機

古い電話機がエクステンションモビリティログインをサポートするシナリオでは、移行後に新しいデバイスがエクステンションモビリティ機能をサポートします。 古い電話機が移行前にログインしている場合、ログインしているエクステンションモビリティのユーザは、電話機の移行中に自動的にログアウトします。 ユーザは、新しい電話機で新しいエクステンションモビリティのログインを実行する必要があります。

（注） ネイティブ電話の移行では、エンドユーザのエクステンションモビリティデバイスのプロファイル移行はサポートされていません。

CTI で制御するデバイス

古いデバイスが電話機の移行前にCTI制御されている場合は、新しいデバイスもCTI制御されます。 これは、デバイスの設定が電話機の移行後に引き継がれるためです。

キー拡張モジュール付き電話機

古い電話機に接続されたキー拡張モジュール (KEM) が新しい電話機モデルと互換性がない場合、電話機の移行後、新しい電話機の KEM の「拡張モジュール情報」設定が失われる可能性があります。

次の表に、さまざまなシナリオを示します。

表 *70 : KEM* 移行シナリオ

シナリオ	古い電話機 (モデル 79xx)	新しい電話機 (モデル 88xx)	移行後の予期される動作
• 古い電話機に接続された KEM 1 は、新しい電話機と互換性があります。 • ユーザは KEM 1 を古い電話機から取り外し、新しい電話機で接続します。	KEM 1	KEM 1	KEM 1 の設定は引き継がれます。

シナリオ	古い電話機 (モデル 79xx)	新しい電話機 (モデル 88xx)	移行後の予期される動作
• 古い電話機に接続された KEM 1 は、新しい電話機と互換性がありません。 • ユーザは、対応する KEM 2 (新しいまたは使用された)を新しい電話機に取り付けます。	KEM 1	KEM 2	KEM 1 の設定は KEM 2 に引き継がれます。
• 古い電話機に接続された KEM 1 は廃止されました。 • ユーザは新しい KEM 3 を新しい電話機に接続します。	KEM 1	KEM 3	KEM 1 の設定は KEM 3 に引き継がれます。

プロダクト固有の設定パラメータ

電話機の移行中は、古い電話機の製品固有のパラメータも移行されます。 新しい電話機では、電話機で理解されているパラメータだけが考慮されます。 残りのパラメータはデフォルト値に設定されます。

電話機の移行中に [回線モード] パラメータがすでに設定されている場合は、[回線モード] 設定が引き継がされます。 それ以外の場合、このパラメータはデフォルトで [セッション回線モード] に設定されます。

また、電話機の移行中に古い電話機で「すべてのコールをプライマリ回線に表示」パラメータが古い電話機で設定されている場合、新しい電話機は、電話機の移行後、「プライマリ回線上のすべてのコールを表示」パラメータを保持します。 このパラメータを電話機の移行前に設定していない場合、電話機の移行後はデフォルトで有効になります。

電話ボタン テンプレート

SCCP 電話モデルを SIP Phone モデルに移行する場合、SIP Phone は理解しているパラメータのみを考慮します。 それ以外の場合は、SIP Phone モデルからデフォルトの設定値をとります(たとえば、標準 SIP プロファイル)。

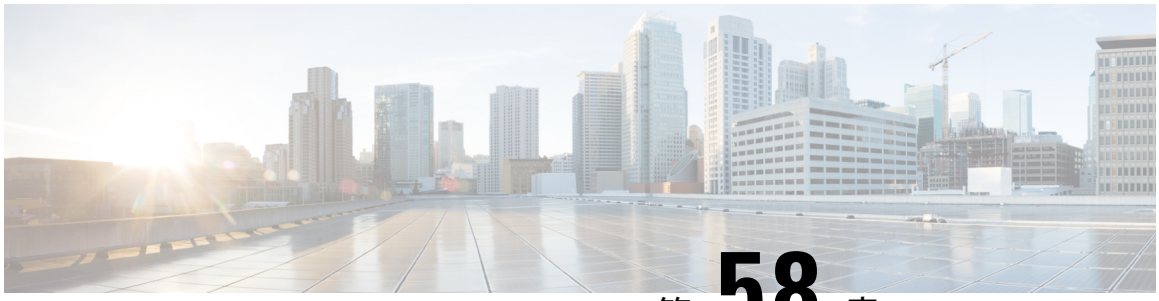
古い電話機に固有のカスタム電話ボタン テンプレートが作成されている場合、新しい電話機は、電話機の移行後、カスタム電話ボタン テンプレートを保持します。 標準の電話ボタン テンプレートの場合、新しいデバイスは電話機モデル固有の標準電話ボタンテンプレートを使用します。

表 *71 :* 電話ボタン テンプレート*:* 移行シナリオ

古いデバイス	古いデバイスの電話ボタン テンプレート	電話機の移行用に選択された新しいデバイス	電話機移行後の新しいデバイスの電話ボタン テンプレート
Cisco Unified IP 電話 7965 SCCP	標準 7965 SCCP	Cisco IP 電話 8861	標準 8861 SIP
Cisco Unified IP 電話 7965 SCCP	ユニバーサルデバイス テンプレートのボタン レイアウト	Cisco IP 電話 8861	ユニバーサルデバイス テンプレートのボタン レイアウト
Cisco Unified IP 電話 7965 SCCP	カスタム 7965 SCCP	Cisco IP 電話 8861	カスタム 7965 SCCP
Cisco Unified IP 電話 8851 SIP	標準 8851 SIP	Cisco IP 電話 8861	標準 8861 SIP

コラボレーション デバイス: ルーム システム、デスク、および IP 電話

- ビデオ エンドポイント デバイスのみ、別のビデオ エンドポイント デバイスに移行できます。
- Unified Communications Manager では、CF (Jabber for Desktop)、TCT (Jabber for iPhone)、TAB (Jabber for iPad)、または MANAGER (Jabber for Android) デバイスへの電話機の移行はサポートされていません。
- 電話機移行サービスを使用してビデオ エンドポイントを移行することはできません。
- 古いビデオ エンドポイント デバイスがロックされた状態の場合、新しいビデオ エンドポイント デバイスは、電話の移行後もロックされた状態は保持されません。



第 58 章

ビデオ エンドポイント管理

ビデオエンドポイント管理の概要

この機能により、管理者が Cisco TelePresence ビデオ エンドポイントをプロビジョニングおよび管理する作業が簡単になります。 管理者は、ユニファイドコミュニケーションマネージャーの Cisco TelePresence エンドポイントの設定をプロビジョニングし、それらの製品固有の設定をエンドポイントにプッシュできます。

12.5 (1) SU1 より前のリリースでは、製品固有の設定の一部だけがユニファイド コミュニケーションマネージャからエンドポイントにプッシュされ、その結果エンドポイントの部分的な設定になりました。 管理者は、すべての設定を構成するために、Cisco TelePresence Management Suite またはテレ プレゼンス エンドポイントの ウェブ インターフェイスに依存する必要がありました。 ユニファイド コミュニケーション マネージャの [電話の設定 (Phone Configuration)] ウィンドウには、エンドポイントでのユーザの表示内容と一致する Cisco TelePresence エンドポイントの完全な製品固有の設定レイアウトが含まれています。 この更新により、管理者はユーザの代わりに設定を適用し、それらの設定をユーザにプッシュすることができます。

（注） 一括管理ツール(BAT)**電話テンプレートの設定**ページには、エンドポイントパラメータの完全なリストをサポートする、新しいモデル固有の設定がタブレイアウトで表示されます。 パラメータのセット全体をインポートしたり、エンドポイントの特定のパラメータを一括して変更したりできます。

ビデオ エンドポイント管理機能には、次の利点があります。

- テレプレゼンス エンドポイントは、ユニファイド コミュニケーション マネージャから完全にプロビジョニングできます。ユニファイド コミュニケーション マネージャーのユー

ザインターフェイスにリストされているエンドポイントパラメータは、Cisco TelePresence モデルの**詳細**設定に記載されている順序と同じ順序になっています。 さまざまな詳細パラメータの詳細については、コラボレーションエンドポイントの管理者ガイドのそれぞれのモデルを参照してください。

- 新しい**製品固有の設定**レイアウト: 新しいレイアウトでは、タブレイアウトのモデル固有の設定が詳細に表示されます。 これは、限られたパラメータセットのみにアクセスを提供した以前の flat 形式からのアップグレードです。 新しいレイアウトにより、Cisco ユニファイド CM の管理インターフェイスで Cisco TelePresence 設定の完全なリストが確保されます。
- ビデオ エンドポイントからの設定データの自動移行: これにより、エンドポイントからユニファイド コミュニケーション マネージャ、またはその逆のデータを自動的に同期することによって、エンドポイントの導入が簡素化されます。 エンドポイントの設定は、工場出荷時の設定にリセットした場合、または製品が & 交換 (RMA) を交換する場合に完全に復元できます。

（注） コラボレーション エンドポイント (CE) ソフトウェア9.8 以降をサポートするエンドポイントは、[電話の設定 (Phone Configuration)] ページの製品固有の設定フィールドにこの新しいプロビジョニングレイアウトを使用できます。 9.8 よりも前の CE ソフトウェア バージョンを使用している場合は、新しい詳細パラメータのセットをすべて表示できます。ただし、新しいパラメータのセットは、CE ソフトウェア バージョンを 9.8 以降にアップグレードした場合にのみ機能します。 サポートされているパラメータのサブセットには、ユーザ インターフェイスの各パラメータ値の右側に「#」が付けられています。デバイスタイプが新しいプロビジョニング フレームワークをサポートできる場合は、デバイスパックをユニファイドコミュニケーション マネージャにロードする必要がありますが、その他のパラメータは表示されません。

ビデオ エンドポイント管理機能の互換性

次の表は、Unified Communications Manager および Collaboration Endpoint（CE）バージョンと互換性のあるビデオ エンドポイント管理機能の詳細を示しています。

Unified Communications Manager のバージョン	CE エンドポイント バージョン	予想される動作
12.5 (1) SU1	9.8 以上	12.5(1) SU1 以前に追加されたデバイス： • 正常にバックアップされたデバイスの高度な構成 UI（タブ付きレイアウト） • まだバックアップされていないデバイスの制限された設定UI（フラット レイアウト） UI/BAT/AXL を介して追加された新しいデバイス： • 高度な構成 UI （注） CE 9.8 以降を実行することを強く推奨します。
12.5 (1) SU1	9.7 以下	12.5(1) SU1 以前に追加されたデバイス： • 制限された構成 UI UI/BAT/AXL を介して追加された新しいデバイス： • 効果を発揮しているパラメータの制限された一式のみを含む高度な設定 UI （注） CE 9.7 またはそれ以前のバージョンの移行では、移行中に既存のエンドポイント構成を維持することはできません。 移行されたデバイスを登録すると、Unified CM は、既存構成をデフォルト設定で上書きします。
12.5(1) 以下	9.8 以上	制限された構成 UI

ビデオ エンドポイントのプロビジョニングと移行の懸念事項

Unified Communications Manager アップグレード後のバックアップ

Unified Communications Manager 12.5(1)SU1 をアップグレードする際、サポートされているエンドポイント タイプの既存の設定が、自動でエンドポイントから Unified Communications Manager に移行されます。

1. Unified Communications Manager を、バージョン 12.5(1)SU1 以降にアップグレードします。
2. エンドポイントが Unified Communications Manager に登録されます。
3. 次に、Unified Communications Manager が、製品固有のパラメータの一連の設定を要求するエンドポイントに SIP Notify メッセージを送信します。
4. CE 9.8 またはそれ以降にアップグレードされたエンドポイントは、SIP REFER メッセージを使用して、設定データ一式を（xConfiguration 形式で）Unified Communications Manager に送信します。
5. Unified Communications Manager は、この設定データを処理し、[Cisco Unified CM Administration] インターフェイスで、Cisco TelePresence 設定（高度な構成 UI）の完全なリストを作成します。

（注） Unified Communications Manager は、Unified CM がエンドポイントから正常にデータをバックアップできた場合にのみ、新しいレイアウトに完全なエンドポイント構成設定を表示します。

構成制御モード

導入のニーズに基づいて、管理者は、[Cisco Unified CM Administration] インターフェイスでさまざまな構成制御モードを設定できます。 構成設定をエンドポイントまたは Unified Communications Manager から集中的に制御するか、または両方を同時に制御するかを決定できます。

[電話機構成（Phone Configuration）] ページの製品固有構成レイアウト セクションにアクセスして、[その他（Miscellaneous）] タブの 「[一般設定（General Settings）]」 にある **[構成制御モード（Configuration Control Mode）]** を選択します。 次のように、さまざまな構成制御モードがあります。

- **Unified CM and Endpoint（デフォルト）**：Unified Communications Manager とエンドポイントをプロビジョニング エンドポイント データに対してマルチプライム ソースとして操作する場合はこのモードを選択します。 Unified CM およびエンドポイントが、構成モードの吐合は、エンドポイントを介したローカルの更新は、Unified CM サーバに同期されます。

- **[Unified CM]**：Unified Communications Manager をプロビジョニング エンドポイント データの中央化プライマリ ソースとして操作し、ローカルのエンドポイントでの設定を許可しない場合は、このモードを使用します。
- **[エンドポイント（Endpoint）]**：エンドポイントを設定データの中央化プライマリ ソースとして操作する場合は、このモードを使用します。 このモードでは、エンドポイントは Unified Communications Manager からの構成データをすべて無視し、ローカルで行った変更を同期しません。 通常、このモードは、Audiovisual（AV）インテグレーターがエンドポイントをインストールしていて、エンドポイントから設定を制御する必要がある場合に使用されます。

（注） **エンドポイント**モードでは、CE デバイスは、リリース 12.5(1)SU1 の前にサポートされていた制限付きパラメータを引き続き許可します。 Unified Communications Manager は、これらパラメータを「#」記号で示します。 CE デバイスは、12.5(1)SU1 リリース以降からサポートされている拡張パラメータの一式を無視します。

オンデマンドの設定プル機能

管理者は、**[電話機から構成を取得（Get Config from Phone）]** オプションを使用して、指定した時点で CE 9.8 エンドポイント デバイスからの構成変更をプルします。

[電話機構成（Phone Configuration）] ページの [製品固有構成レイアウト（Product-Specific Configuration Layout）] セクションにアクセスし、ページの上端にある **[電話機から構成を取得（Get Config from Phone）]** ボタンをクリックし、オンデマンドの CE 9.8 エンドポイントからデータ構成をプルします。 このオプションは、エンドポイントが登録されている場合にのみ有効になります。

ビデオ エンドポイント移行レポート

拡張設定バックアップのビデオエンド ポイントは、12.5(1)SU1 のリリースで [電話機の検索と一覧（Find and List Phones）] ウィンドウに導入された新しいフィルタです。 管理者は、自動的に移行された CE エンドポイント数と、実行できなかった CE エンドポイントの数に関する詳細を検索できます。 この情報に基づいて、修正措置を講じることができます。

（注） [電話機の検索と一覧（Find and List Phones）] では、Collaboration Endpoint（CE）ソフトウェア 9.8 またはそれ以上が実行しているビデオ エンドポイントのみで、**拡張設定バックアップのビデオエンド ポイント** フィルタを適用することができます。

プロビジョニングと移行のシナリオ

次の表では、さまざまなプロビジョニングと移行のシナリオについて説明します。これらのシナリオのすべては、TelePresence ビデオ エンドポイントが、Unified CM からプロビジョニングされた製品固有の設定をサポートする CE リリースにアップグレードされていることを前提としています。Unified CM では、これらの設定は **[製品固有設定（Product-Specific Configuration）]** セクションに表示されますが、エンドポイントでは **[詳細設定（Advanced Configuration）]** に表示されます。

表 *72*: ビデオ エンドポイントのプロビジョニングと移行のシナリオ

タスク	既存の設定の概要	対処方法
ビデオエンドポイントのプロビジョニング	• 新しいデバイスのブランド • デバイスがユニファイド CM でプロビジョニングされていません • デバイスまたはユニファイド CM の既存の設定がありません	最小リリース 12.5 (1) SU1 および CE エンドポイント (9.8) でユニファイド CM を使用すると、新しいエンドポイントをプロビジョニングし、統合 CM から製品固有の設定を管理できます。

タスク	既存の設定の概要	対処方法
VCSからの既存のビデオエンドポイントの移行	• 既存デバイス • デバイスがユニファイドCMでプロビジョニングされていません • デバイスは設定されていますが、ユニファイドCMには設定がありません	既存のビデオ エンドポイントを Cisco TelePresence ビデオ通信サーバから Cisco Unified Communications Manager に移行する場合は、次のようにします。 **ユニファイド CM の [電話の設定 (Phone Configuration)] ウィンドウを使用した電話機の追加:** • 電話機をユニファイド CM に追加しますが、[**保存 (Save)**] をクリックしないでください。 • 電話の登録 登録後、電話機からの既存の **[高度な構成（Advanced Configuration）]** 設定は、ユニファイド CM にアップロードされ、**[電話の設定 (Phone Configuration)]** ウィンドウで **[製品固有の設定（Product-Specific Configurations）]**に表示されます。 • **[電話の設定（Phone Configuration）]** ウィンドウで **[保存（Save）]** をクリックして新しい設定をします。 プロビジョニングされた設定が電話機にダウンロードされます。 詳細な手順の参照先：移行ビデオ エンドポイントを Unified CM に追加する （896 ページ） **一括管理による電話機の追加** プロビジョニングに使用する csv ファイルまたは BAT テンプレートに、製品固有の設定フィールドが含まれていないことを確認してください。 **AXL を介した電話機の追加** AXL 要求に、製品固有の設定フィールドが含まれていないことを確認してください。
登録済みビデオエンドポイントを使用した、以前のリリースのユニファイド CM からのアップグレード	• 既存デバイス • デバイスは、12.5 より前のリリースのユニファイドCMでプロビジョニングされます。 • ユニファイドCMには、デバイスの製品固有の構成時の設定が限定されています。	CE エンドポイントがサポートされているバージョンである限り、ユニファイド CM をアップグレードすると、エンドポイントからの **[高度な構成（Advanced Configuration）]** 設定は、デバイスの登録後に自動的にユニファイド cm に取り込まれ、[**電話の設定 (Phone Configuration)**] ウィンドウの **[製品固有の設定（Product-Specific Configurations）]** セクションに表示されます。 登録後に、必要なすべての設定に加えて、**設定制御モード**を設定できます。

移行ビデオ エンドポイントを Unified CM に追加する

Cisco TelePresence ビデオ通信サーバから既存の Cisco TelePresence ビデオ エンドポイントを Unified Communications Manager に移行する際は、**[電話設定（Phone Configuration）]** ウィンドウで、CE エンドポイントを Unified CM に追加する手順を使用します。これにより、エンドポイントの既存 **Advanced Configurations** をUnified CM の **[電話設定（Phone Configuration）]** から管理することができます。

（注） この手順を厳密に実行してください。デバイスを登録しても、エンドポイントからの設定は、Unified CM に自動的にアップロードされません。

（注） この手順では、Unified CM **[電話設定（Phone Configuration）]** ウィンドウの **[テンプレートの新規追加（Add New from Template）]** 設定を使用します。 また、Bulk Administration や AXL などのツールを使用してもエンドポイントを追加できます。

始める前に

移行する前に、ファームウェアを CE 9.8 以降にアップグレードすることを強く推奨します。CE 9.7 またはそれ以前のバージョンでは、デフォルト設定による登録中に Unified CM は、既存のエンドポイント設定を上書きします。

手順

ステップ 1 Cisco Unified CM 管理から、**[デバイス]** > **[電話機]** を選択します。

ステップ 2 **[テンプレートの新規追加（Add New from Template）]** をクリックし、次の電話の詳細を入力します。

- **[電話の種類（Phone Type）]** ドロップダウン リストから、[モデル（Model）] を選択します。
- エンドポイントの **MAC アドレス** を入力します。
- **[デバイス テンプレート（Device Template）]** ドロップダウン リストで、[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。
- 電話機に追加する**ディレクトリ番号**を選択します。存在しない場合は、**[新規作成（New）]** をクリックして、ディレクトリ番号を設定します。
- **[ユーザ（User）]** ドロップダウン リストから、デバイスを所有するユーザを選択します。

ステップ 3 **[Add（追加）]** をクリックします。 **[電話の設定（Phone Configuration）]** には、電話の設定を記入するためのユニバーサルデバイステンプレートの設定が表示されます。**[製品固有の設定（Product-Specific Configurations）]** セクションも表示されますが、電話機からの既存の設定ではなく、デフォルト設定が使用されます。

（注） **[電話の設定（Phone Configuration）]** ウィンドウの **[新規追加（Add New）]** でもデバイスを追加できますが、この方法は、設定を手動で入力する必要があります。

ステップ 4 **[保存（Save）]** はクリックしないでください。 設定を保存した場合、Unified CM は、電話から既存の設定をロードしなくなります。誤って保存した場合は、この手順の下部に記載されている復旧手順であるトラブルシューティングの注意を参照してください。

ステップ 5 電話の登録
登録中は、電話の既存の **[高度な構成（Advanced Configuration）]** 設定が、Unified CM にプルされ、**[電話の設定（Phone Configuration）]** ウィンドウの **[製品固有の設定（Product-Specific Configuration）]** セクションに表示されます。

ステップ 6 **[電話の設定（Phone configuration）]** ウィンドウで、**[設定制御モード（Configuration Control Mode）]** フィールドを設定してエンドポイント設定をどのように管理するかを設定します。

- **Unified CM and Endpoint（デフォルト）**：Unified Communications Manager とエンドポイントをプロビジョニング エンドポイント データに対してマルチプライム ソースとして操作する場合はこのモードを選択します。 Unified CM とエンドポイントが、設定モードの場合、エンドポイントを介してローカルで実行された更新は、Unified CM と同期され、Unified CM で行った変更は、エンドポイントと同期されます。
- **[Unified CM]**：Unified Communications Manager をプロビジョニング エンドポイント データの中央化プライマリ ソースとして操作し、ローカルのエンドポイントでの設定を許可しない場合は、このモードを使用します。
- **[エンドポイント（Endpoint）]**：エンドポイントを設定データの中央化プライマリ ソースとして操作する場合は、このモードを使用します。 このモードでは、エンドポイントは既存の設定を維持し、Unified Communications Manager からの構成データをすべて無視し、ローカルで行った変更を同期しません。 通常、このモードは、Audiovisual（AV）インテグレーターがエンドポイントをインストールしていて、エンドポイントから設定を制御する必要がある場合に使用されます。

（注） エンドポイントの既存の設定を維持する必要がある場合は、少なくともエンドポイントが登録プロセスを完了するまで、**[エンドポイント（Endpoint）]** モードを選択することを推奨します。 この手順を完了した後に、設定を他のモードのいずれかに切り替えることができます。

ステップ 7 必要な電話機の設定を行います。 フィールドと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。

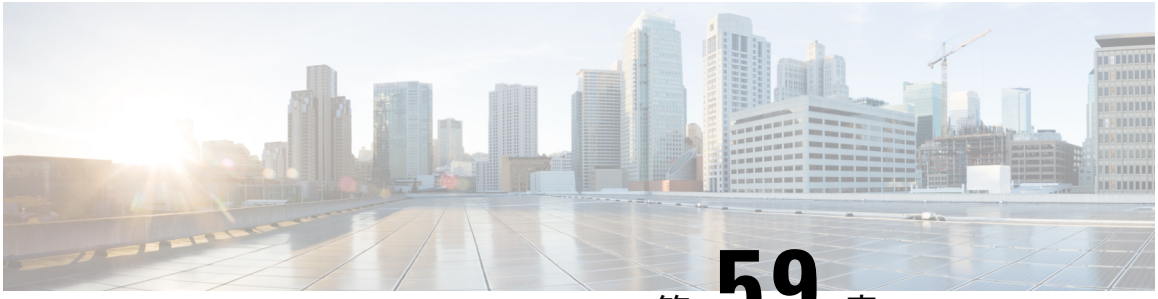
ステップ 8 **[保存]** をクリックします。
Unified Communications Manager 内でプロビジョニングされた設定がエンドポイントにダウンロードされます。

（注） デバイスの登録前に、**[電話の設定（Phone Configuration）]** ウィンドウで誤って **[保存（Save）]** をクリックしてしまった場合、デバイスが登録されても、エンドポイントの既存 **Advanced Configuration** 設定は、Unified CM にロードされません。 リカバリするには、デバイスを登録する前に、次の手順を実行します。

- Unified CM で、**[設定制御モード（Configuration Control Mode）]** を **[エンドポイント（Endpoint）]** に設定し、**[保存（Save）]** をクリックします。
- 電話機が Unified CM に登録されるようにします。
- 登録後に、**[電話の設定（Phone Configuration）]** ウィンドウでデバイスの設定に戻り、**[デバイスからの設定の取得（Get Config from Device）]** ボタンをクリックします。 電話機の既存の**詳細設定**の設定の結果が Unified CM に引き継がれます。このボタンは、デバイスを登録するまで表示されません。
- 設定を完了するために、この手順のステップ 6 に戻ります。

第 XIV 部

高度なコール処理



第 59 章

コール制御検出の設定

コール制御検出の概要

コール制御検出（CCD）を使用して、電話番号のパターンなどの主要の属性とともに Unified Communications Manager 情報をアドバタイズできます。 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

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（904 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 転送の設定 （904 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 （905 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

	コマンドまたはアクション	目的
		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 （906 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 （907 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	広告サービスの設定 （907 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の設定 （907 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	リクエスト サービスの設定 （908 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

	コマンドまたはアクション	目的
		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 （909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 フォワーダの SAF セキュリティ プロファイルを設定して、SAF フォワーダと Unified Communications Manager 間に安全な接続を確立します。

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/%20go/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 転送の設定

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。

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] をクリックします。

ステップ 3 次のいずれかの作業を実行します。

- 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。

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。

広告サービスの設定

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の設定

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。

リクエスト 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]** 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] 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

表 *73 :* コール制御検出の連携動作

機能	データのやり取り
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	データのやり取り
[着信の着呼側設定(Incoming Called Party Settings)]	H.323 プロトコルは、国際的なエスケープ文字 + をサポートしていません。 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 60 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。

外部コール制御の前提条件

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

手順

	コマンドまたはアクション	目的
ステップ 1	外部コール制御のコーリング サーチ スペースの設定 （916 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 （916 ページ）	外部のコール制御プロファイルで、付加ルート サーバの URI、電話の転送に使用するコーリング サーチ スペース、付加ルート サーバからのシステムの応答待機時間を示すタイマーなどを設定します。
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 （917 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。
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 （918 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

	コマンドまたはアクション	目的
		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 （918 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） 監察機能の設定 （919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 （920 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。

外部コール制御のコーリング 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 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）]** > **[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] 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、どの言語でも最大50文字まで指定できますが、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、**コントロール（Ctrl）**キーを押したまま、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 （オプション）**[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。

外部コール制御プロファイルの設定

外部のコール制御プロファイルで、付加ルートサーバのURI、電話の転送に使用するコーリング サーチ スペース、付加ルート サーバからのシステムの応答待機時間を示すタイマーなどを設定します。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [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 次のいずれかの作業を実行します。

- 既存の外部コール制御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）]** ボタンをクリックします。

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。

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

外部のコール制御プロファイルで、付加ルート サーバのURI、電話の転送に使用するコーリング サーチ スペース、付加ルート サーバからのシステムの応答待機時間を示すタイマーなどを設定します。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [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 次のいずれかの作業を実行します。

- **[検索（Find）]** をクリックして、結果の一覧から既存のトランスレーション パターンを選択し、検索条件を入力して既存のトランスレーション パターンの設定を修正します。
- 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]** 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。

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。

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。

ルートサーバへの自己署名証明書のエクスポート

ルーティング サーバで HTTPS が使用されている場合は、Unified Communications Manager の自己署名証明書をルーティング 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 サーバおよび冗長ルート サーバが、Unified Communications Manager を使用して HTTPS 経由で認証できることを確認するには、システムに命令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。

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。

監察機能の設定

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 では次の機能により、付加ルート サーバの指示に従い、監察機能をサポートします。

- 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。

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。

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 次のいずれかの作業を実行します。

• 新規のお知らせを追加するには：

a) [新規追加] 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]** 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（Upload File）]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（Upload File）]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

表 *74*：外部コール制御の連携動作

機能	データのやり取り
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。 また、コール詳細レコードは、Unified Communications Manager が付加ルート サーバからの決定を受信しなかった期間にコールをブロックするか、または許可するかを示すこともできます。

機能	データのやり取り
通話転送	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より高い優先順位を保持しています。外部コール制御プロファイルにトランスレーション パターンが割り当てられている場合、コール転送を呼び出すコールに関して、Unified Communications Manager は、ルーティング クエリを付加ルート サーバに送信します。 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	電話ユーザがコール ピックアップ機能を使用してコールのピックアップを試みた場合、外部コール制御は呼び出されません。Unified Communications Manager は、コールのその部分に関するルーティング 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	Unified Communications Manager によって、次の Cisco Unified Mobility 機能に関する付加ルート サーバからのルート決定が許可されます。 • 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 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	データのやり取り
ディレクトリ番号	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。
取り込み中	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続行義務を送信せず、ユーザがDND-Rを有効にした場合、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、Unified Communications Managerは、転送元と転送先の間に、付加ルート サーバからのルーティング ルールを適用できません。

外線コール制御の制限

表 *75 :* 外線コール制御の制限

制約事項	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。

制約事項	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 (Hold)	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	この機能が会議に参加する通話者に相談コールを行う前に監察者が録音を開始した場合、Unified Communications Manager は監察者が相談コールを行う間録音を一時停止し、会議の確立後に録音を再開します。

第 61 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

Unified Communications Manager は、ハント メンバーが発信者に応答可能になるまで、発信者をキューに入れるための Call Queuing を備えています。 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。

セキュア コールのキューイング

重要 このセクションは、リリース 14SU2 以降に適用されます。

ハント パイロットにセキュアなコールが発信され、すべての回線グループがビジー状態の場合、キューで待機している発信者には、ライブ エージェントがコールに応答するまで、保留音と繰り返しの（カスタマイズ可能な）定期的なアナウンスが流れます。 このプロセスの間、コールは一時的に保留になります。 エンドポイントが SRTP フォールバックをサポートしていない場合、パーキング ロット（非セキュア デバイス）に対するコールは、暗号の不一致によってドロップオフします。

Unified Communications Manager は、ネイティブ コール キューリングに対するセキュアなコール サポートを強化し、一時的な保留コールの暗号機能を利用してコールのドロップオフを回避しました。 Unified CM セキュア リアルタイム トランスポート プロトコル（SRTP）は、代替フォールバック オプションのステータスに関係なく、セキュア コール全体としてコール SRTP 処理します。

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	アナウンスの設定 （928 ページ）	.wav ファイルをアップロードしてアナウンスを設定します。
ステップ 2	保留音の設定 （929 ページ）	保留音（MOH）オーディオ ソースを設定します。
ステップ 3	ハントパイロットキューの設定 （935 ページ）	応答されるまで、キュー内のコールのコールキュー保留オプションを有効にします。
ステップ 4	無応答時のハント メンバーの自動ログアウト （936 ページ）	回線メンバーは、ハント リストから自動的にログオフすることができます。

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
- カスタムアナウンスメントの .wav ファイルを挿入する
- アナウンスメント用のロケールを割り当てる
- アナウンスの説明を変更する
- 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

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 Communications Manager で、**[メディア リソース（Media Resources）] > [保留音のオーディオ 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 （930 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 *76*：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 ソースに対する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 リストをクリックして、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 ソースに対する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 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)]	このフィールドにはMOHオーディオ ソースの一意の名前を入力します。 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。

フィールド	説明
[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。
[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 77: アナウンスの設定値

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、次のような最初のアナウンス情報を参照できます： • [アナウンスID(Announcement Identifier)] • 説明 • [デフォルトのアナウンス(Default Announcement)] （注） • MOHサーバによって再生されるのは、**Multi-casting** が確認されていない状態です、**キュー有効のハントパイロットコール**の最初の**アナウンス通話がキューに入れられる場合**のアナウンスの再生に設定される場合のみです。 • **Multi-casting を許可する**チェックボックスがオンの場合、または**キュー有効ハントパイロット コール**の最初の**アナウンスがハントメンバーにルーティングする前に**アナウンスを再生するに設定されている場合はANNが再生します。
キュー有効ハントパイロットコールの最初のアナウンス	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）]

フィールド	説明
[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(Announcement Identifier)] • 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示す値（秒）を指定します。 有効値は 10～300 です。デフォルト値は 30 です。
[アナウンスのロケール(Locale Announcement)]	アナウンスのロケールは、インストールされているロケール インストールのパッケージによって異なります。 （注） • MOH によって再生されたプロンプトは、[アナウンスのロケール(Locale Announcement)] の設定を使用します。 • ANNによって再生されたプロンプトは、発呼側の[ユーザロケール(User Locale)] を使用します。

表 *78 :* 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、追加した MOH オーディオ ソースが表示されます。 保留音オーディオ ソースのオーディオ ストリーム番号を選択し、その MOH オーディオ ソースを設定します。 オーディオ ソース ID は、保留音サーバ内のオーディオ 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） [**<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。
ファイルのアップロード	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、オーディオ ソース 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を指定します。 音源ファイルを見つけたら、**[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がアップロードされた後、[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、このウィンドウを閉じます。 （注） ファイルをアップロードする際、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向けのコーデック指定のオーディオ ファイルが作成されます。 元のファイル サイズによっては、処理が完了するまで数分かかることがあります。 （注） オーディオ ソース ファイルの MOH サーバへのアップロードでは、ファイルは 1 つの MOH サーバだけにアップロードされます。 したがって、各サーバ上の Cisco Unified Communications Manager の管理ページを使用して、クラスタ内の MOH サーバごとにオーディオ ソース ファイルをアップロードする必要があります。 MOH オーディオ ソース ファイルは、クラスタ内の他の MOH サーバには自動で反映されません。

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 Communications Manager 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 音源のアナウンスメント ロケールは、アナウンスメントに使用する言語を決定するために使用します。 ハントパイロットごとに、1 種類の言語のアナウンスメントのみを再生できます。

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。フィールド範囲は 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 を入力します。

- （オプション）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。 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。
- （オプション）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。
- （オプション）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。

無応答時のハント メンバーの自動ログアウト

回線メンバーは、ハント リストから自動的にログオフすることができます。エージェントが、キュー対応のハントパイロットコールに応答しない場合は、そのエージェントはハントグループからログオフされます。この場合、電話機の [HLOG] ソフトキーを押してハントパイロットにログインしない限り、そのエージェントは、ハント パイロットコールを受信しません。

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。

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

機能	データのやり取り
[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	データのやり取り
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約事項

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。

- ハントパイロットの最大数は、キューで許可されている 32 の発信者で設定されている場合、コールキューが有効になっている Unified CM サブスクライバノードごとに 100 です。ノードごとのキュースロットの総数（ノード上のすべてのコールキュー対応ハントパイロットの「キューで許可される発信者の最大数」の値）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 100 人の発信者がキューに入ることができ、ハントパイロットの最大数は 32 に減らされます。ただしコールキューが有効になっている場合は、すべてのハントリストのメンバーの最大数は変更されません。
- 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、回線グループ内の電話番号の最大数は 35 未満に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頻時発呼数（BHCA）が 1 秒あたり 35 コール設定を超えないようにします。

第 62 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 スロットリングの設定 （942 ページ）	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有効になります。
ステップ 2	メモリ スロットリングの設定 （943 ページ）	システムのメモリス ロットリングを設定します。

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 の管理から、**[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、こののの手順を使用します。

手順

ステップ 1 Cisco Unified CM の管理から、**[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 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 63 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 （946 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 （947 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

	コマンドまたはアクション	目的
	• 地理位置情報の作成 （947ページ） • 地理位置情報の割り当て （948ページ） • デフォルトの地理位置情報の設定 （948 ページ）	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。
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 （949 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 （949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 （950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 （951 ページ） • 地理位置情報フィルタの割り当て （951 ページ） • デフォルトの地理位置情報フィルタの設定 （952 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	一連の論理パーティション分割ポリシーレコードの定義 （952 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 （953 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]** > **[企業パラメータ]** 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 （947 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 （948 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 （948 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] 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]** 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 次のいずれかの作業を実行します。

- 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] 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]** > **[企業パラメータ]** 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]** 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] 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]** 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 次のいずれかの作業を実行します。

- 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] 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（951 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 （951 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 （952 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

	コマンドまたはアクション	目的
		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] 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]** 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 次のいずれかの作業を実行します。

- 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] 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]** > **[企業パラメータ]** 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]** 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。

一連の論理パーティション分割ポリシー 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 次のいずれかの作業を実行します。

- 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] 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]** 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。

論理パーティション分割の連携動作

表 *79 :* 論理パーティション分割の連携動作

機能	データのやり取り
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。

機能	データのやり取り
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。
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。

機能	データのやり取り
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約事項

表 *80* : 論理パーティション分割の制約事項

制約事項	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。
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。

制約事項	説明
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通話情報をドロップします。
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 64 章

ロケーション認識の設定

ロケーション認識の概要

重要　ロケーション認識に対する Meraki アクセスポイントのサポートは、リリース 12.5(1)SU6 および 14SU1 以降にのみ適用されます。

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。

（注）　現在、有線電話はロケーション認識をサポートしていません。

[Cisco Unified CM Administration] > [詳細機能（Advanced Features）] > [デバイス位置追跡サービス（Device Location Tracking Services）] > [スイッチおよびアクセスポイント（Switches and Access Points）] > [スイッチおよびアクセスポイントの検索と表示（Find and List Switches and Access Points）] ウィンドウからネットワーク インフラストラクチャを表示できます。

この機能では、次の情報を使用してUnified Communications Managerデータベースを動的に更新します。

- 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

ロケーション認識により、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。 ロケーション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 が起動すると、まず、現在のデバイスに対するUnified Communications Managerデータベースに対して、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。

ロケーション認識でサポートされるエンドポイント

次のエンドポイントは、ロケーション認識によるトラッキングをサポートしています。

- Cisco Uniifed ワイヤレス IP Phone 7925G
- Cisco Unified ワイヤレス IP 電話 7925G-EX
- Cisco Unified ワイヤレス IP 電話 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。

ロケーション認識の前提条件

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（961 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 （961 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（962 ページ）	これはオプションです。 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。 （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（964 ページ）	これはオプションです。 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

	コマンドまたはアクション	目的
		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

ロケーション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 これはオプションです。 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]** 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]** 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。

（**オプション**） 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

この手順を使用して、ワイヤレスアクセスポイントインフラストラクチャをCSVファイルからUnified Communications Managerデータベースに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、サードパーティの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することができます。

始める前に

データファイルは、カンマ区切り値（CSV）形式で、次のように区切られた列で作成する必要があります：

- 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に必須
- 説明 - ロケーションID、スイッチタイプとロケーションの組み合わせ、またはその他の意味のあるID

（注） IPv4アドレスとIPv6アドレスの両方を定義することも、IPv4アドレスまたはIPv6アドレスを定義することもできます。

差し込みアクセスポイントの場合は、ベースのBSSIDに正規化した後、Unified Communications Managerはデータベースの Basic Service Set 識別子（BSSID）を更新します。 電子アクセスポイントの BSSID マスク計算の詳細については、「Cisco Meraki BSSID MAC アドレスの計算」を参照してください。

非 Meraki CM アクセスポイントでは、Unified CMは、最後のバイトを0でマスクすることにより、データベースの BSSID を更新します。

このマスクロジックは、Unified CM チャネルの BSSID ではなく、アクセスポイントを一意に識別するのに役立ちます。

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）]**.を選択します。**[インフラストラクチャ デバイスの挿入の設定（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。
ジョブをただちにに実行することを選択した場合、ジョブは実行されます。

ステップ 6 ジョブを後で実行するように選択した場合は、ジョブの実行スケジュールを設定します。

a) **[一括管理(Bulk Administration)]**>**[ジョブスケジューラ(Job Scheduler)]** の順に選択します。
b) **[検索（Find）]** をクリックし、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、いつジョブを実行するか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間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。

第 65 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 マーキングおよびビデオ 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
- ビデオ通話
- ビデオ通話の音声部分
- 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（968 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（970 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）]**。

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 （969 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 *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 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）（Clusterwide Parameters (System - 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 アドミッション制御）（Clusterwide Parameters (Call Admission Control)）	
ビデオ コール QoS マーキング ポリシー（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。
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)）	

パラメータ	説明
リージョン内のデフォルトの最大イマーシブビデオ コール ビットレート（オーディオ含む）（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。
リージョン間のデフォルトの最大イマーシブビデオ コール ビットレート（オーディオ含む）（Default Interregion Max 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。
イマーシブ ビデオ コールにビデオ帯域幅プールを使用する（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	SIP プロファイルのカスタム QoS 設定の構成 （971 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 （972 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、

	コマンドまたはアクション	目的
		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。

SIP プロファイルのカスタム QoS 設定の構成

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。

- **[検索（Find）]** をクリックして、既存の SIP プロファイルを選択します。
- 新しい SIP プロファイルを作成するには、[新規追加] 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ヘルプについては、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 管理から、**[デバイス]** > **[電話機]** 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] 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

表 *82:* 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

Device	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。

Device	データのやり取り
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 *83 :* 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

制約事項	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。
マルチレベルの優先およびプリエンプション	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マルチレベルの優先およびプリエンプション（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 66 章

SIP での発信側番号と請求先番号の分離

外部プレゼンテーションの名前と番号の概要

個別の発信者とプレゼンテーション番号を含めるよう Cisco Unified Communications Manager の管理を設定できます。

以前のリリースでは、FROM ヘッダーと PAID ヘッダーで異なる番号を PSTN に送信するために回線単位で Cisco Unified Communications Manager を設定することはできませんでした。 PSTN ユーザに対して同じ発信回線 ID 番号（非地理的 E.164 番号で、課金に使用できない番号）を提示するようユーザ グループが設定されている場合。 したがって、ユーザの実際の DDI を、プレゼンテーション番号とは異なるフィールドに入れて送信しなければなりません。 このリリースの Cisco Unified Communications Manager では、既存の ID 番号や名前とは異なる外部プレゼンテーション名と番号がサポートされています。 設定されるプレゼンテーション名と番号は、次のデバイスで表示されます。

- SIP
- SCCP
- シングル ナンバー リーチの接続先（SNRD）
- CTIRD
- SparkRD

構成の概要

次のページでは、外部プレゼンテーション名と番号の機能を設定できます。

- 電話番号の設定（Directory Number Configuration）
- SIPプロファイルの設定（SIP Profile Configuration）
- トランクの設定（Trunk Configuration）

（注）
- [SIPプロファイルの設定（SIP Profile Configuration）] ページで外部プレゼンテーション情報を設定すると、[SIPプロファイルの設定（SIP Profile Configuration）] ページ上の [外部プレゼンテーション番号（External Presentation Number）] と [外部プレゼンテーション名（External Presentation Name）] の値が使用され、[電話番号（Directory Number）] ページの設定値がオーバーライドされます。
- [トランクの設定（Trunk Configuration）] ページでプレゼンテーション情報を設定すると、[トランクの設定（Trunk Configuration）] ページ上の [プレゼンテーション番号（Presentation Number）] と [プレゼンテーション名（Presentation Name）] の値が使用され、[SIPプロファイルの設定（SIP Profile Configuration）] ページおよび [電話番号の設定（Directory Number Configuration）] ページの指定値がオーバーライドされます。

呼処理

このセクションでは、外部プレゼンテーション名と外部プレゼンテーション番号の機能を設定した場合の着信コールと発信コールの動作について説明します。

着信コール プロセス

PSTN ネットワークからコールが開始されると、Cisco Unified Communications Manager は FROM ヘッダーと PAID ヘッダーの情報を検索します。 FROM ヘッダーには外部プレゼンテーション名と番号が含まれています（設定されている場合）。 ただしこれはユーザの実際の ID ではなく、表示目的でのみ使用されます。 PAID ヘッダーにはユーザの ID（元の DN または DDI）が含まれています。

FROM ヘッダーと PAID ヘッダーに異なる番号が指定され、[SIP プロファイルの設定（SIP Profile Configuration）] ページで [外部プレゼンテーション名と番号の有効化（Enable External Presentation Name and Number）]オプションが有効であり、[外部プレゼンテーション名と番号の表示（Display External Presentation Name and Number）]サービス パラメータの値が [はい（True）]に設定されている場合は、Cisco Unified Communications Manager により着信側デバイスに FROM ヘッダーの情報（設定されている外部プレゼンテーション名と番号）が表示されます。 同様に、1 つのオプションが無効の場合、Cisco Unified Communications Manager により PAID ヘッダーの情報（ユーザの元の DN または DDI）が着信側デバイスに表示されます。

（注）
- デフォルトでは、[外部プレゼンテーション名と番号の有効化（Enable External Presentation Name and Number）]フィールドが選択されています。
- [外部プレゼンテーション名と番号の表示（Display External Presentation Name and Number）] サービス パラメータのデフォルト値は [いいえ（False）] です。

PSTN ネットワークから受信した招待

```
From: "Customer Care" <sip:1800000@example.com>;
To: <sip:someone@example.com>
P-Asserted-Identity: "Your personal adviser <sip:user1@example.com>
Remote-Party-ID: "Your personal adviser <sip:user1@example.com>
```

上記の例では、FROM ヘッダーに PAID ヘッダーとは異なる番号が含まれています。[外部プレゼンテーション名と番号の有効化（Enable External Presentation Name and Number）]チェックボックスをオンにして、[外部プレゼンテーション名と番号の表示（Display External Presentation Name and Number）]の値を [はい（True）]を設定すると、Cisco Unified Communications Manager により **Customer Care / 1800000** が着信側デバイスに表示されます。

[外部プレゼンテーション名と番号の有効化（Enable External Presentation Name and Number）]チェックボックスをオフにするか、または [外部プレゼンテーション名と番号の表示（Display External Presentation Name and Number）]の値を [いいえ（False）]に設定すると、Cisco Unified Communications Manager により着信側デバイスに **Your personal adviser / user1@example.com** が表示されます。

発信コール プロセス

たとえば、外部プレゼンテーション名と番号が設定されたユーザから、**外部プレゼンテーション名と番号**が設定された SIP プロファイルを持つ SIP トランクを介して、PSTN ネットワークに向けてコールが開始されたとします。 次に Cisco Unified Communications Manager は、設定された外部プレゼンテーション情報を発信側 SIP メッセージの FROM ヘッダーで送信し、着信側デバイスに表示します。

[外部プレゼンテーション名と番号の有効化（Enable External Presentation Name and Number）] オプションが無効の場合、または [外部プレゼンテーション番号（External Presentation Number）] と [外部プレゼンテーション名（External Presentation Name）] フィールドが設定されていない場合、Cisco Unified Communications Manager は電話番号情報を FROM ヘッダーと PAID ヘッダーで送信し、着信側デバイスに表示します。

外部プレゼンテーションの番号マスク操作

Cisco Unified Communications Manager では、着信側デバイスに表示する外部プレゼンテーション番号をマスクできます。[電話番号の設定（Directory Number Configuration）]、[SIP プロファイルの設定（SIP Profile Configuration）]、および [トランクの設定（Trunk Configuration）] の各ページでプレゼンテーション番号をマスクできます。

[外部プレゼンテーション番号（External Presentation Number）]フィールドに番号を入力して末尾に X を付けると、値 X は右から左の順番で電話番号情報に置き換えられます。

[電話番号の設定（Directory Number Configuration）] でのマスク操作

[電話番号の設定（Directory Number Configuration）] ページで、電話番号 5551234 の**外部プレゼンテーション番号**を 180011XXXX としてマスクすると、Cisco Unified Communications Manager は着信側デバイスにプレゼンテーション番号を `1800111234` として表示します。

[SIP プロファイルの設定（SIP Profile Configuration）] でのマスクの操作

[電話番号（Directory Number）] ページの **外部プレゼンテーション番号**が 180011XXXX であると仮定します。電話番号が 5551234 の場合、[SIPプロファイルの設定（SIP Profile Configuration）] ページで**外部プレゼンテーション番号**を `180022XXXX` としてマスクすると、Cisco Unified Communications Manager は着信側デバイスにプレゼンテーション番号を 1800221234 として表示します。

[トランクの設定（Trunk Configuration）] でのマスクの操作

[電話番号（Directory Number）] ページと [SIP プロファイル設定（SIP Profile Configuration）] ページの**外部プレゼンテーション番号**がそれぞれ 180011XXXX と 180022XXXX であると仮定します。 [トランク設定（Trunk Configuration）] ページで、電話番号 5551234 の**プレゼンテーション番号**を 180033XXXX としてマスクすると、Cisco Unified Communications Manager は着信側デバイスにプレゼンテーション番号を `1800331234` として表示します。

ディレクトリ番号の概要

電話番号（DN）を設定するには、[Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] で、**[コール ルーティング（Call Routing）] > [電話番号（Directory Number）]** メニューパスを使用します。 [Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] を使用して、特定の電話機に割り当てられている DN を設定および変更できます。

[電話番号の設定（Directory Number Configuration）] ページに [外部プレゼンテーション情報（External Presentation Information）] という新しいセクションが追加されました。 管理者は、選択した任意のプレゼンテーション名とプレゼンテーション番号を、外線コール用のサポート対象デバイスに表示するよう設定できるようになりました。 ユーザの ID を表示させたくない場合、管理者は、着信側デバイスで設定されている**外部プレゼンテーション番号**と**外部プレゼンテーション名**を匿名として表示できる権限があります。

ディレクトリ番号の設定タスク

手順

	コマンドまたはアクション	目的
ステップ 1	次の方法のいずれかを使用して新しいエンド ユーザを追加します。 • LDAP からのエンド ユーザのインポート （979 ページ） • エンドユーザの手動追加 （980 ページ）	システムが会社の LDAP ディレクトリと同期している場合は、新しいエンド ユーザを LDAP から直接インポートできます。 あるいは、エンド ユーザを手動で追加して設定できます。
ステップ 2	次のいずれかのタスクを実行して、新規または既存のエンド ユーザに電話機を割り当てます。 • エンド ユーザ用の新しい電話機の追加 （981 ページ） • エンド ユーザへの既存の電話機の移動 （982 ページ）	「新しい電話機の追加」手順に従い、ユニバーサル デバイス テンプレートの設定を使用して、エンド ユーザの新しい電話機を設定できます。 また、「移動」の手順に従って、以前に設定済みまたは事前設定済みの既存の電話機を割り当てることもできます。
ステップ 3	DN の外部プレゼンテーション情報の設定 （983 ページ）	特定の電話機に割り当てられている DN の外部プレゼンテーション番号と外部プレゼンテーション名を設定するには、次の手順に従います。

LDAP からのエンド ユーザのインポート

社内 LDAP ディレクトリから新しいエンド ユーザを手動でインポートするには、次の手順に従います。 LDAP 同期設定に、機能グループ テンプレートとユーザ プロファイル（ユニバーサル回線テンプレート、ユニバーサル デバイス テンプレートを含む）、および DN プールが含まれている場合、インポート プロセスによりエンド ユーザとプライマリ エクステンションが自動的に設定されます。

（注） 初回同期の実行後には、新しい設定（たとえば、機能グループ テンプレートの追加）を LDAP ディレクトリ同期に追加することはできません。 既存の LDAP 同期を編集する場合は、一括管理を使用するか、または新しい LDAP 同期を設定する必要があります。

始める前に

この手順を開始する前に、Cisco Unified Communications Manager が社内の LDAP ディレクトリとすでに同期していることを確認します。 LDAP 同期には、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 テンプレートと機能グループ テンプレートが含まれている必要があります。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）] > [LDAP（LADP）] > [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、ユーザの追加先 LDAP ディレクトリを選択します。

ステップ 3 [完全同期を実施（Perform Full Sync）]をクリックします。
Cisco Unified Communications Manager が、外部の LDAP ディレクトリと同期します。 LDAP ディレクトリ内の新しいエンドユーザが Cisco Unified Communications Manager データベースにインポートされます。

次のタスク

セルフプロビジョニングが有効になっている場合、エンドユーザがセルフプロビジョニング自動音声応答（IVR）を使用して新しい電話機をプロビジョニングできます。 有効になっていない場合は、次のタスクのいずれかを実行して、電話機をエンド ユーザに割り当てます。

- エンド ユーザ用の新しい電話機の追加 （981 ページ）
- エンド ユーザへの既存の電話機の移動 （982 ページ）

エンド ユーザの手動追加

次の手順を実行して、新しいエンドユーザを追加し、そのエンドユーザをアクセス コントロール グループとプライマリ回線内線番号を指定して設定します。

（注） ユーザを割り当てる役割の権限を持つアクセス制御グループがすでに設定されていることを確認してください。 詳細については、「ユーザーアクセスの管理」の章を参照してください。

始める前に

ユニバーサル回線テンプレートを含むユーザ プロファイルが設定されていることを確認します。 新しい内線番号を設定する必要がある場合は、Cisco Unified Communications Manager でユニバーサル回線テンプレートの設定を使用してプライマリ内線番号を設定します。

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 ユーザの**ユーザID**と**姓**を入力します。

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、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]** をクリックします。

ステップ 5 [ユーザ プロファイル（User Profile）]ドロップダウン リストで、選択したユーザ プロファイルにユニバーサル回線テンプレートが含まれていることを確認します。

ステップ 6 [アクセス コントロール グループ メンバーシップ（Access Control Group Membership）]セクションで、[+]アイコンをクリックします。

ステップ 7 [ユーザの所属グループ（User is a member of）]ドロップダウン リストで、アクセス コントロール グループを選択します。

ステップ 8 [プライマリ内線番号（Primary Extension）]の下で、[+]アイコンをクリックします。

ステップ 9 [内線番号（Extension）]ドロップダウン リストで、[（使用可能）（available）]として表示されている DN を選択します。

ステップ 10 すべての回線内線番号が [（使用済み）（used）]と表示されている場合は、次の手順を実行します。

a) [新規...（New...）]ボタンをクリックします。
[新規内線の追加（Add New Extension）]ポップアップが表示されます。

b) [電話番号（Directory Number）]フィールドに、新しい回線内線番号を入力します。

c) **[回線テンプレート（Line Template）]** ドロップダウン リストから、ユニバーサル回線テンプレートを選択します。

d) **OK**をクリックします。
Cisco Unified Communications Manager が、ユニバーサル回線テンプレートの設定を使用して電話番号を設定します。

ステップ 11 （任意）[ユーザ/電話のクイック追加設定（Quick User/Phone Add Configuration）]ウィンドウで、追加のフィールドに値を入力します。

ステップ 12 **[保存]** をクリックします。

次のタスク

次の手順のいずれかを実行して、このエンド ユーザに電話機を割り当てます。

- エンド ユーザ用の新しい電話機の追加 （981 ページ）
- エンド ユーザへの既存の電話機の移動 （982 ページ）

エンド ユーザ用の新しい電話機の追加

次の手順を実行して、新しいエンド ユーザまたは既存のエンド ユーザ用の新しい電話機を追加します。 エンドユーザのユーザ プロファイルにユニバーサル デバイス テンプレートが含まれていることを確認します。 Cisco Unified Communications Manager が、ユニバーサル デバイス テンプレートの設定を使用して電話機を設定します。

始める前に

次の手順のいずれかを実行して、エンド ユーザを追加します。

- エンド ユーザの手動追加 （980 ページ）
- LDAP からのエンド ユーザのインポート （979 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/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、新しい電話機を追加するユーザを選択します。

ステップ 3 **[デバイスの管理（Manage Devices）]** ボタンをクリックします。
[デバイスの管理（Manage Devices）] ウィンドウが表示されます。

ステップ 4 [電話の新規追加（Add New Phone）] をクリックします。
[ユーザに電話を追加（Add Phone to User）] ポップアップが表示されます。

ステップ 5 [製品タイプ（Product Type）]ドロップダウン リストで、電話機モデルを選択します。

ステップ 6 **[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] または [SCCP] を選択します。

ステップ 7 [デバイス名（Device Name）]テキスト ボックスに、デバイスの MAC アドレスを入力します。

ステップ 8 [ユニバーサル デバイス テンプレート（Universal Device Template）]ドロップダウン リストで、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 9 電話機が拡張モジュールをサポートしている場合は、展開する拡張モジュールの数を入力します。

ステップ 10 エクステンションモビリティを使用して電話機にアクセスするには、[エクステンションモビリティ内（In Extension Mobility）]チェック ボックスをオンにします。

ステップ 11 [電話の追加（Add Phone）]をクリックします。
[電話の新規追加（Add New Phone）] ポップアップが閉じます。 Cisco Unified Communications Manager が、電話機をユーザに追加し、ユニバーサル デバイス テンプレートを使用してその電話機を設定します。

ステップ 12 電話機の設定に追加の編集を加えるには、対応する鉛筆アイコンをクリックして、**[電話の設定（Phone Configuration）]** ウィンドウで電話機を開きます。

エンド ユーザへの既存の電話機の移動

次の手順を実行して、既存の電話機を新しいまたは既存のエンド ユーザに移動します。

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、既存の電話機を移動するユーザを選択します。

ステップ 3 [デバイスの管理（Manage Devices）]ボタンをクリックします。

ステップ 4 [このユーザに移動する電話の検索（Find a Phone to Move To This User）]ボタンをクリックします。

ステップ 5 このユーザに移動する電話機を選択します。

ステップ 6 [選択項目の移動（Move Selected）]をクリックします。

DN の外部プレゼンテーション情報の設定

特定の電話機に割り当てられる DN の外部プレゼンテーション情報を設定するには、次の手順を行います。

始める前に

- [SIP プロファイルの設定（SIP Profile Configuration）] ページの [外部プレゼンテーションの名前と番号を有効化（Enable External Presentation Name and Number）] チェックボックスをオンにします。
- 次の手順のいずれかを実行して、エンド ユーザを追加します。
  - エンド ユーザの手動追加 （980 ページ）
  - LDAP からのエンド ユーザのインポート （979 ページ）
- 次のいずれかのタスクを実行して、新規または既存のエンドユーザに電話機を割り当てます。
  - エンド ユーザ用の新しい電話機の追加 （981 ページ）
  - エンド ユーザへの既存の電話機の移動 （982 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）]** の順に選択します。

ステップ 2 [電話番号の検索/一覧表示（Find and List Directory Numbers）] ページから次のいずれかのステップを実行します。

- DN を更新するには、[検索（Find）] をクリックし、一意の ID を表示する電話番号を選択します。
- 新しい電話番号を作成するには、[新規追加] をクリックします。

ステップ 3 [外部プレゼンテーション情報（External Presentation Information）]ペインで、着信側デバイスに表示する名前および番号を入力します。

（注）
- [外部プレゼンテーション番号（External Presentation Number）]フィールドには最大 32 桁の文字（[0-9、X、*、#、\、+]）を含めることができます。
- [外部プレゼンテーション名（External Presentation Name）]フィールドには最大 50 文字を入力できます。

ステップ 4 （オプション）設定した [外部プレゼンテーション番号（External Presentation Number）]と [外部プレゼンテーション名（External Presentation Name）]を匿名として表示する場合、[名前非表示の外部プレゼンテーション（Anonymous External Presentation）]チェックボックスをオンにします。

（注）
- デフォルトでは、[名前非表示の外部プレゼンテーション（Anonymous External Presentation）]フィールドはオフになっています。
- [名前非表示の外部プレゼンテーション（Anonymous External Presentation）]フィールドをオンにすると、次のようになります。

  [外部プレゼンテーション番号（External Presentation Number）]フィールドと [外部プレゼンテーション名（External Presentation Name）]フィールドは編集できません。 また、これらのフィールドのエントリは表示されなくなります。

ステップ 5 [電話番号の設定（Directory Number Configuration）]ページのその他のフィールドを入力します。 フィールドとその設定のヘルプについては、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 プロファイルの概要

SIP プロファイルは、共通の SIP 設定で成り立つテンプレートです。 ネットワーク内のすべての SIP トランクと SIP デバイスに SIP プロファイルを割り当てる必要があります。 SIP プロファイルを設定し、SIP トランクまたは SIP デバイスにそのプロファイルを割り当てるとき、SIP の設定がそのトランクまたはデバイスに適用されます。

SIP プロファイル設定タスク

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 （985 ページ）	SIP 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 2	SIP プロファイルの外部プレゼンテーション情報の設定 （986 ページ）	SIP プロファイルの外部プレゼンテーション番号と外部プレゼンテーション名を設定するには、次の手順に従います。

SIP プロファイルの設定

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

手順

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 の**統合された境界要素**を越えて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のレプリケーション展開について、[ILS で学習した場合の通知先ルート文字列の送信] 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。

SIP プロファイルの外部プレゼンテーション情報の設定

[SIPプロファイルの設定（SIP Profile Configuration）] ページで、外部プレゼンテーション名と番号を個別に設定するには、この手順を使用します。

始める前に

- [SIPプロファイルの設定（SIP Profile Configuration）]ページの [外部プレゼンテーションの名前と番号を有効化（Enable External Presentation Name and Number）]チェックボックスをオンにします。
- **[サービスパラメータの設定（Service Parameter Configuration）]** ページの [クラスタ全体のパラメータ（デバイス-電話）（Clusterwide Parameters (Device - Phone)）] セクションで、**[外部プレゼンテーション名と番号の表示（Display External Presentation Name and Number）]** パラメータの値を **`True`** に設定します。

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。

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

ステップ 3 [外部プレゼンテーション情報（External Presentation Information）]ペインで、着信側デバイスに表示する名前および番号を入力します。

（注）
- [外部プレゼンテーション番号（External Presentation Number）]フィールドには最大 32 桁の文字（[0-9、X、*、#、\、+]）を含めることができます。
- [外部プレゼンテーション名（External Presentation Name）]フィールドには最大 50 文字を含めることができます。

ステップ 4 （オプション）設定した [外部プレゼンテーション番号（External Presentation Number）]と [外部プレゼンテーション名（External Presentation Name）]を匿名として表示する場合、[名前非表示の外部プレゼンテーション（Anonymous External Presentation）]チェックボックスをオンにします。

（注）
- デフォルトでは、[名前非表示の外部プレゼンテーション（Anonymous External Presentation）]フィールドはオフになっています。
- [名前非表示の外部プレゼンテーション（Anonymous External Presentation）]フィールドをオンにすると、次のようになります。

  [外部プレゼンテーション番号（External Presentation Number）]フィールドと [外部プレゼンテーション名（External Presentation Name）]フィールドは編集できません。 また、これらのフィールドのエントリは表示されなくなります。

ステップ 5 [SIPプロファイルの設定（SIP Profile Configuration）]ページで、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。

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 の管理（Cisco Unified CM Administration）] の [SIP トランクの設定（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 トランクは、既存の発信者 ID DN および発信者名とは異なる個別のプレゼンテーション名と番号をサポートしています。呼び出し中のデバイスで、設定されているプレゼンテーション名と番号が、匿名として表示される新しいチェックボックス **[匿名プレゼンテーション (Anonymous Presentation)]** が提供されます。

トランクの設定タスク

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 （988 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。

	コマンドまたはアクション	目的
		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 Communications 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 （989 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 （990 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。
ステップ 4	SIP トランクのプレゼンテーション情報の設定 （992 ページ）	[SIP トランク （SIP Trunk）] ページでプレゼンテーション名とプレゼンテーション番号を設定するには、次のようにします。

SIP トランク セキュリティ プロファイルの設定

セキュリティ設定を使用してSIP中継セキュリティプロファイルを構成し、要約アイデンティティ認証やトップドメイン名システムシグナリング暗号化などを行う。 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は、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] 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) デバイスの認証で、[X.509 のサブジェクト名（X.509 Subject Name）]フィールドで、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]** をクリックします。

（注） トランクが設定を使用するためには、**そのプロファイル**をトランク設定ウィンドウで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

一般的なデバイス構成は、オプションのユーザ固有特徴属性のセットを含む。 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] 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 を設定する場合は、[シグナリング (シグナリング)] ドロップダウンリストの ip アドレス指定モードの ip アドレス設定を次のように設定します。

- [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 **[共通デバイス構成（Common Device Configuration）]** 画面で、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] 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 （オプション）このトランクに**共通デバイス設定**を適用する場合は、ドロップダウン リストから設定を選択します。

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。

SIP トランクのプレゼンテーション情報の設定

[SIP トランク（SIP Trunk）] ページでプレゼンテーション名とプレゼンテーション番号を設定するには、次の手順に従います。

始める前に

- [SIP プロファイルの設定（SIP Profile Configuration）] ページの [外部プレゼンテーションの名前と番号を有効化（Enable External Presentation Name and Number）] チェックボックスをオンにします。
- SIP トランクの設定 （990 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 [新規追加] 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 **[トランク サービス タイプ（Trunk Service Type）]** ドロップダウン リストから、設定する SIP トランクのタイプを選択します。

- [なし（デフォルト）（None (Default)）]：トランクは、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、Intercompany Media Engine、または IP Multimedia System サービス コントロールには使用されません。
- [コール制御検出（Call Control Discovery）]：トランクはコール制御検出機能をサポートします。
- [クラスタ間のエクステンションモビリティ（Extension Mobility Cross Cluster）]：トランクはクラスタ間のエクステンションモビリティをサポートします。
- [Cisco Intercompany Media Engine]：トランクは Intercompany Media Engine（IME）をサポートします。 トランク タイプを設定する前に、IME サーバがインストールされていることを確認してください。
- [IP Multimedia System サービス コントロール（IP Multimedia System Service Control）]：トランクの IP Multimedia System サービス コントロールのサポートを有効にするには、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。

ステップ 6 [プレゼンテーション情報（Presentation Information）] セクションで、着信側デバイスに表示する名前および番号を入力します。

（注）
- [プレゼンテーション番号（Presentation Number）]フィールドには最大 32 桁の文字（[0-9、X、*、#、\、+]）を入力できます。
- [プレゼンテーション名（Presentation Name）] フィールドには最大 50 文字を入力できます。

ステップ 7 （任意） プレゼンテーション名および番号を匿名で表示する場合、**[匿名のプレゼンテーション（Anonymous Presentation）]** チェックボックスを選択します。

（注）
- デフォルトでは、[匿名のプレゼンテーション（Anonymous Presentation）]フィールドはオフになっています。
- [名前非表示の外部プレゼンテーション（Anonymous External Presentation）] フィールドをオンにすると、次のようになります。

  [プレゼンテーション番号（Presentation Number）] と [プレゼンテーション名（Presentation Name）] のフィールドは編集できません。 また、これらのフィールドのエントリは表示されなくなります。

ステップ 8 （任意） SIP トランクで構成されるプレゼンテーション情報を FROM ヘッダーのみで送信する場合は、**[プレゼンテーション名と番号は FROM ヘッダーでのみ送信し、他のアイデンティティ ヘッダーでは送信しない（Send Presentation Name and Number only in the FROM header and not in the other identity headers）]** チェックボックスをオンにします。

ステップ 9 **[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。

クラスタ間 SME コール フロー

Cisco Unified Communications Manager Session Management Edition ソフトウェアは、クラスタ間またはさまざまなデバイス間のコール ルーティングで主に使用される Cisco Unified Communications Manager と同じです。 このリリースでは、Cisco Unified Communications Manager はクラスタ間 SME コールをサポートします。

着信コール数（Incoming Calls）

PSTN ネットワークのユーザが、自身の SIP プロファイルの [外部プレゼンテーション名と番号の有効化（Enable External Presentation Name and Number）]を有効にして、コールを開始するとします。 [外部プレゼンテーション名と番号の表示（Display External Presentation Name and Number）]サービス パラメータを [はい（True）]に設定すると、Cisco Unified Communications Manager はプレゼンテーション番号情報を X-Cisco-Presentation ヘッダーに

送信し、着信側デバイスに表示します。 FROM ヘッダーと PAID ヘッダーにはユーザの ID （ユーザの DN または DDI）が含まれます。

[外部プレゼンテーション名と番号の表示（Display External Presentation Name and Number）] サービス パラメータを [いいえ（False）]に設定すると、Cisco Unified Communications Manager はプレゼンテーション番号情報を X-Cisco-Presentation ヘッダーに送信します。 FROM ヘッダーと PAID ヘッダーにはユーザの DN または DDI が含まれ、着信側デバイスに表示されます。

発信コール数（Outgoing Calls）

[外部プレゼンテーション名（External Presentation Name）] と [外部プレゼンテーション番号（External Presentation Number）] が設定されたユーザが、クラスタ間 SIP トランクを介して PSTN ネットワークへのコールを開始します。 自身の SIP プロファイルで [外部プレゼンテーション名と番号の有効化（Enable External Presentation Name and Number）]チェックボックスが無効な場合、Cisco Unified Communications Manager は FROM ヘッダーと PAID ヘッダーで元の電話番号情報を送信し、着信側デバイスおよび X-Cisco-Presentation ヘッダーで設定した外部プレゼンテーション情報に表示します。 同様に、自身の SIP プロファイルで [外部プレゼンテーションの名前と番号を有効化（Enable External Presentation Name and Number）]チェックボックスが有効な場合、Cisco Unified Communications Manager は設定した外部プレゼンテーション情報を FROM ヘッダーで送信し、着信側デバイスおよび PAID ヘッダーの元の電話番号に表示します。

第 67 章

SIP OAuth モード

SIP OAuth モードの概要

Unified Communications Managerへのセキュア登録では、CTL ファイルの更新、共通証明書信頼ストアの設定などが行われます。 デバイスが、オンプレミスとオフプレミス間で切り替わる場合、セキュア登録が完了する際は毎回、LSC と 認証局プロキシ機能 登録の更新処理が複雑になります。

SIP OAuth モードでは、セキュアな環境でのすべてのデバイスの認証に OAuth 更新トークンを使用できます。 この機能により、Unified Communications Managerのセキュリティが強化されます。

Unified Communications Managerは、エンドポイントによって提示されたトークンを検証し、許可されたものにのみ構成ファイルを提供します。 Unified Communications Managerクラスタおよびその他のシスコのデバイスで OAuth ベースの認証を有効にすると、SIP 登録中の OAuth トークン検証が完了します。

以下で、SIP 登録の OAuth サポートが拡張されました

- CiscoUnified Communications Manager12.5リリース以降の Cisco Jabber デバイス
- CiscoUnified Communications Managerリリース 14 以降の SIP 電話

（注） デフォルトでは、SIP OAuth が有効になっている場合、TFTP は SIP 電話に対して安全です。 TFTP ファイルのダウンロードは、認証された電話に対してのみ、セキュリティで保護されたチャネルを介して行われます。 SIP OAuth は、オンプレミスおよび MRA を介して CAPF を使用せずに、エンドツーエンドの安全なシグナリングとメディア暗号化を提供します。

次に、OAuth 用に設定できる電話セキュリティプロファイルのタイプを示します。

- Cisco Dual Mode for iPhone（TCT デバイス）
- Cisco Dual Mode For Android（BOT デバイス）
- Cisco Unified Client Services Framework（CSF デバイス）
- Cisco Jabber for Tablet（TAB デバイス）
- ユニバーサル デバイス テンプレート（Universal Device Template）
- Cisco 8811
- Cisco 8841
- Cisco 8851
- Cisco 8851NR
- Cisco 8861
- Cisco 7811
- Cisco 7821
- Cisco 7841
- Cisco 7861
- Cisco 8845
- Cisco 8865
- Cisco 8865NR
- Cisco 7832
- Cisco 8832
- Cisco 8832NR

SIP OAuth モードの前提条件

この機能は、次の作業が完了していることを前提としています。

- モバイルおよびリモートアクセスが設定され、Unified Communication Manager および Expressway 間で接続が確立されていることを確認します。 このルールは、オンプレミス SIP OAuth 導入には適用されません。
- **[エクスポート制御機能を許可する（allow export-controlled）]** 機能を使用して Unified Communications Manager が Smart または Virtual アカウントに登録されていることを確認します。
- クライアントファームウェアが SIPOAuth をサポートしていることを確認します。
- Tomcat および Tomcat-EC 証明書はどちらも同じ CA によって署名された CA によって署名されている必要があります。これは、単一の Phone-Edge-trust 証明書しかアップロードで

きず、Tomcat署名証明書のルート証明書である必要があるためです。 SIP OAuth が機能するには、電話が Tomcat と Tomcat-EC の両方の証明書を信頼する必要があります。

SIP OAuth モードの設定タスク フロー

システムの SIP OAuth 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	Phone Edge TrustへのCA証明書のアップロード	トークンを取得するには、CA 証明書を電話エッジトラストにアップロードします。 この手順は、Cisco Jabber デバイスには適用されません。
ステップ 2	デバイスの OAuth アクセス トークンの有効化	重要　このステップは、リリース 14 以降に適用されます。 Cisco IP 電話 7800 および 8800 企業シリーズでの SIP 登録の OAuth を有効にします。 この手順は、Cisco Jabber デバイスには適用されません。
ステップ 3	更新ログインの設定 （999 ページ）	SIP OAuth を介してデバイスを登録するために、Unified Communications Manager で 更新ログイン フローを使用した OAuth を有効化する。
ステップ 4	OAuth ポートの設定 （1000 ページ）	OAuthが登録されているノードごとに、OAuth 用のポートを割り当てます。
ステップ 5	OAuth Connection を Expressway-C に設定 （1001 ページ）	手動認証された TLS 接続を Expressway-C に設定します。
ステップ 6	SIP OAuthモードの有効化 （1001 ページ）	パブリッシャ ノードで CLI コマンドを使用して OAuth サービスを有効にします。
ステップ 7	Cisco CallManager サービスの再起動 （1002 ページ）	OAuthが登録されているすべてのノードで、このサービスを再起動します。
ステップ 8	電話セキュリティプロファイルでデバイスセキュリティモードを設定する	エンドポイントに対して暗号化を展開する場合、電話セキュリティ プロファイルで、OAuth サポートを設定します。

	コマンドまたはアクション	目的
ステップ 9	（任意）SIPOAuth 登録済み電話を MRA モード用に構成する	重要　このステップは、リリース 14 以降に適用されます。 SIP OAuth 登録済みの電話を MRA モードで構成します。 この手順は、Cisco Jabber デバイスには適用されません。

Phone Edge TrustへのCA証明書のアップロード

この手順を使用して、Tomcat署名付き証明書のルート証明書をパブリッシャノードからPhone EdgeTrust にアップロードします。 証明書はパブリッシャノードでのみ表示されます。

（注）　この手順は Cisco Phone に対してのみ実行され、Cisco Jabber には適用されません。

手順

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

ステップ 2　**[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3　**[証明書/証明書チェーンのアップロード]** ウィンドウで、**[証明書の目的]** ドロップダウンリストから **[電話-エッジ-信頼]** を選択します。

ステップ 4　**[ファイルのアップロード]** フィールドで、**[参照]** をクリックして証明書をアップロードします。

ステップ 5　[アップロード（Upload）]をクリックします。

デバイスの OAuth アクセス トークンの有効化

重要　このセクションは、リリース 14 以降に適用されます。

電話機の OAuth アクセス トークンを有効にするには、次の手順を使用します。

（注） 電話機の SIP 登録に対する OAuth サポートにのみ、このエンタープライズ パラメータを設定します。

SIP OAuth が機能するには、電話証明書（MIC または LSC）が有効である必要があります。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 **[SSO および OAuth の設定]** セクションで、**[デバイスの OAuth アクセス トークン]** ドロップダウン リストの値が **Implicit:Already に登録済みのデバイスに設定されます**。

（注） **デバイスの OAuth アクセストークン**の値を **Explicit:Activation Code** に設定します。デバイスのオンボーディングは、SIP OAuth 登録のトークンの暗黙的な受信を無効にし、アクティベーションコードを介したトークンの受信のみをサポートするために必要です。 セキュリティプロファイルに示されている場合、トークンは SIPOAuth 登録に使用できます。

リリース 14 以降、デバイスのエンタープライズパラメータ **OAuth アクセストークン** のデフォルト値は **Implicit**：**Alreadyregistereddevices** です。

ステップ 3 **[保存（Save）]** をクリックします。

更新ログインの設定

OAuth アクセス トークンを使用して更新ログインを設定し、Cisco Jabber クライアントのトークンを更新するには、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 **[SSO および OAuth 構成（SSO and OAuth Configuration）]** で、**OAuth with Refresh Login Flow** のパラメータを **[有効（Enabled）]** にします。

ステップ 3 （任意） **[SSO および OAuth 構成（SSO and OAuth Configuration）]** セクションで、各パラメータを設定します。 パラメータの説明を確認するには、パラメータ名をクリックします。

ステップ 4 **[保存（Save）]** をクリックします。

OAuth ポートの設定

SIP OAuth に使用するポートを割り当てるには、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。 から、以下を選択します。**[システム（System）]** > **[Cisco Unified CM]**。

ステップ 2 SIP OAuth を使用するサーバごとに次の操作を行います。

ステップ 3 サーバを選択します。

ステップ 4 [Cisco Unified Communications Manager（Cisco Unified Communications Manager）] の **[TCP ポートの設定（TCP Port Settings）]** で、次のフィールドに対してポート値を設定します。

- SIP 電話 OAuth ポート（SIP Phone OAuth Port）

  デフォルト値は 5090 です。設定可能な範囲は 1024 ~ 49151 です。

- SIP モバイルおよびリモートアクセス ポート（SIP Mobile and Remote Access Port）

  デフォルト値は 5091 です。設定可能な範囲は 1024 ~ 49151 です。

（注） Cisco Unified Communications Manager は、SIP Phone OAuth Port (5090) を使用して、TLS 経由の Jabber オンプレミス デバイスから SIP 回線登録をリッスンします。 ただし、ユニファイド CM は、SIP モバイルリモートアクセスポート (デフォルトは 5091) を使用して、 mTLS を介して Jabber からの SIP 回線登録をリッスンします。

両方のポートは、受信 TLS/mTLS 接続に対して Cisco tomcat 証明書と tomcat 信頼を使用します。 Tomcat 信頼ストアが、モバイルおよびリモートアクセスが正常に機能するように、SIP OAuth モードの Expressway-C 証明書を検証できることを確認します。

次の場合は、Expressway-C 証明書を Cisco Unified Communications Manager の tomcat 信頼証明書ストアにアップロードするための追加の手順を実行する必要があります。

- Expressway-C 証明書と Cisco tomcat 証明書は、同じ CA 証明書では署名されません。
- Unified CM Cisco tomcat は、CA 署名はありません。

ステップ 5 **[保存]** をクリックします。

ステップ 6 SIP OAuth を使用する各サーバに対して、この手順を繰り返します。

OAuth Connection を Expressway-C に設定

Cisco Unified Communications Manager Administration に Expressway-C 接続を追加するには、次の手順を使用します。 SIP OAuth を使するモバイルおよびリモートアクセス モードのデバイスには、この構成が必要です。

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** > **Expressway-C**

ステップ 2 （任意）**[Expressway-C の検索 とリスト]** ウィンドウで、**[検索]** をクリックして 、Expressway-C から Unified Communications Manager にプッシュされた X.509 サブジェクト名/サブジェクト代替名を確認します。

（注） 必要に応じて値を変更できます。 また、エントリが存在しない場合は、Expressway-C 情報を追加します。

ユニファイド コミュニケーション マネージャとは別のドメインを持っている場合 、管理者はCisco Unified CM の管理ユーザインターフェイスにアクセスして、Unified CM の設定でドメインを Expressway-C に追加する必要があります。

ステップ 3 [新規追加] をクリックします。

ステップ 4 Expressway-C に対して、IP アドレス、ホスト名または、完全修飾ドメイン名を入力します。

ステップ 5 説明を入力します。

ステップ 6 X.509 のサブジェクト名/Expressway-C のサブジェクトの別名を、Expressway-C 証明書から入力します。

ステップ 7 **[保存（Save）]** をクリックします。

SIP OAuth モードの有効化

SIP OAut モードを有効にするには、コマンドライン インターフェイスを使用します。 パブリッシャ ノードでこの機能を有効にすると、すべてのクラスタ ノードでこの機能が有効になります。

始める前に

リリース 14SU1 以降では、プロキシ TFTP が有効な場合は、オフクラスタの Tomcat 証明書のルート CA 証明書をプロキシ電話機のエッジ信頼にコピーする必要があります。

手順

ステップ 1 Unified Communications Manager のパブリッシャ 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 sipOAuth-mode enable` の CLI コマンドを実行します。
リリース 14 以降では、システムは、読み取り専用の**クラスタ SIPOAuth Mode** 企業パラメータを **[有効]** に更新します。

Cisco CallManager サービスの再起動

CLI で SIP OAuth を有効にした後に、SIP OAuth を介してエンドポイントが登録されるすべてのノードで Cisco CallManager サービスを再起動します。

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[ツール]** > **[コントロールセンター]** > **[機能サービス]**

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 **Cisco CallManager** サービスを確認し、[再起動（Restart）] をクリックします。

電話セキュリティプロファイルでデバイスセキュリティモードを設定する

この手順を使用して、電話機のセキュリティプロファイルで**デバイスセキュリティモード（Device Security Mode）**を設定します。これは、その電話機の**[電話機のセキュリティプロファイル（Phone Security Profile）]**内でデバイスセキュリティモードを**[暗号化（Encrypted）]**に設定している場合にのみ必要です。

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 次のいずれかを実行します。

- 既存の電話セキュリティプロファイルを検索する
- **[新規追加]** をクリックします。

ステップ 3 [電話セキュリティプロファイル情報（Phone Security Profile Information）] セクションの **[デバイス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。

ステップ 4 **[転送タイプ（Transport type）]** ドロップダウンリストで、**[TLS]** を選択します。

ステップ 5 [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 6 **[保存]** をクリックします。

ステップ 7 電話セキュリティプロファイルを電話に関連付けます。 電話セキュリティ電話を適用する方法の詳細については、Cisco Unified Communications Manager セキュリティガイドの「セキュリティプロファイルを電話に適用する」セクションを参照してください。

（注） 変更を有効にするには、スマートフォンをリセットしてください。

（注） [SIP OAuth モード（SIP OAuth Mode）] が有効な場合、**[ダイジェスト認証を有効化（Enable Digest Authentication）]** および **[TFTP 暗号化設定（TFTP Encrypted Config）]** オプションはサポートされません。 電話機は、**https(6971)**を介して TFTP 設定ファイルを安全にダウンロードし、認証にトークンを使用します。

SIPOAuth 登録済み電話を MRA モード用に構成する

この手順を使用して、SIPOAuth 登録済み電話を MRA モードに構成します。

始める前に

重要 このセクションは、リリース 14 以降に適用されます。

電話機がアクティベーションコードを使用するように設定されていることを確認してください。 詳細については、Cisco Unified Communications Manager システム設定ガイドの「アクティベーションコードを使用するための登録方法の設定」セクションを参照してください。

（注） SIP OAuth over MRA を使用する場合、ユーザーはログインにユーザー名/パスワードを使用できませんが、オンボーディングに基づくアクティベーションコードを使用する必要があります

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。**デバイス > 電話**.

ステップ 2 **[検索]** をクリックして、オフプレミスモード用に構成するデバイスを選択します。

ステップ 3 **[デバイス情報]** セクションで、次の手順を実行します。

- **[MRA経由でアクティベーションコードを許可する（Allow Activation Code via MRA）]** チェックボックスをオンにします。
- **[アクティベーションコードMRAサービスドメイン]** ドロップダウンリストから、必要な MRA サービスドメインを選択します。 MRA サービスドメインを設定する方法の詳細については、Cisco Unified Communications Manager システム設定ガイドの「*MRA* サービスドメインの設定」セクションを参照してください。

（注） SIP OAuth over MRA モードの場合、アクティベーションコードのみを使用し、ユーザー名/パスワードベースのログインは使用しないでください。

ステップ 4 **[プロトコル固有の情報]** セクションで、**[デバイスセキュリティプロファイル]** ドロップダウンリストから OAuth 対応の SIP プロファイルを選択します。 電話機が OAuth ファームウェアをサポートしていることを確認してください。セキュリティプロファイルの作成方法の詳細については、Cisco Unified Communications Manager システム設定ガイドの「電話セキュリティプロファイルの設定」セクションを参照してください。

ステップ 5 **[保存（Save）]** と **[構成の適用（Apply Configuration）]** をクリックします。

（注） 電話機は MRA モードに切り替わり、Expressway との通信を開始します。 内部ネットワークでオンプレミスからのライン Sway との通信が許可されていない場合、電話機は登録されませんが、オフプレミスの電源がオンになっているときには、その電話機に接続する準備ができています。

第 XV 部

QoS 管理

第 68 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 の設定を使用できます。

SIP メディア フローの管理

APIC-EM を使用する SIP コールの場合、Cisco Unified Communications Manager はコールの始めに APIC-EM コントローラにポリシー要求を送信して、メディア フローの APIC-EM がセットアップ中であることを通知します。 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 Communications 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 （967 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 コントローラ設定のタスクフロー

APIC-EM コントローラが SIP メディア フローを制御できるようにするには、Cisco Unified Communications Manager で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	APIC-EM コントローラの設定 （1009 ページ）	APIC-EM コントローラに Unified CM を設定します。
ステップ 2	APIC-EM コントローラ証明書のアップロード （1010 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 3	APIC-EM コントローラへの HTTPS 接続の設定 （1010 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 4	システムの外部 QoS サービスを有効にする （1011 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 APIC-EM を使用するには、デバイスの

	コマンドまたはアクション	目的
		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 5	SIP プロファイル レベルの外部 QoS サービスの設定 （1011 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 6	電話への SIP プロファイルの割り当て （1012 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。

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]** 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。

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。

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ですが、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。

システムの外部 QoS サービスを有効にする

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。

手順

ステップ 1 Cisco Unified CM の管理から、**[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 [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]** 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。

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。

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。

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

電話への 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。

手順

ステップ 1 Cisco Unified CM の管理で、**[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 リストから、トラフィックを管理する APIC-EM コントローラを使用する電話にアップロードした [SIP プロファイル（SIP Profile）] 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、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 69 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 フォン

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 *84 : 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 電話	可	可	可	可	可	可
サードパーティ製 AS-SIP デバイス	不可	不可	不可	不可	不可	不可

（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 CM Administration] を使用して、SIP が実行されているサードパーティ製の電話機を設定します（詳細は、『*Cisco Unified Communications Manager* のシステム構成ガイド』の「SIP プロファイルの設定」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 の前提条件

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。 詳細については、『*Cisco Unified Communications Manager* のシステム構成』の「スマート ソフトウェア ライセンシング」の章を参照してください。

AS-SIP エンドポイント設定タスク 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 （1017 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 （1018 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。

	コマンドまたはアクション	目的
ステップ 3	サービスの再起動 （1019 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。
ステップ 4	AS-SIP 用 SIP プロファイルの設定 （1019 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 （1020 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 （1021 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	デバイスとエンド ユーザの関連付け （1022 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 （1023 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 （1023 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 （1024 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] 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。

- ユーザー 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] をクリックします。
- **[検索（Find）]** をクリックして、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
- [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 管理から、**[デバイス]** > **[電話機]** 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 [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 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。 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]** 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]** 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。

デバイスとエンド ユーザの関連付け

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] 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。

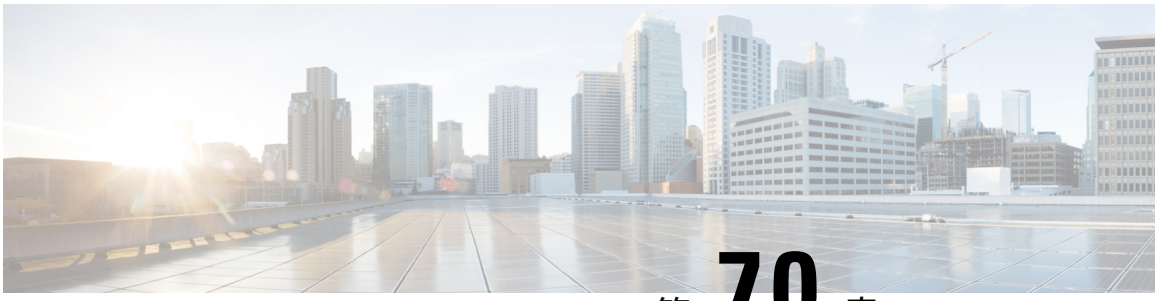
AS-SIP 機能の設定

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
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。
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 の管理から、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。 2. **[サーバ（Server）]** ドロップダウン リストから、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]** をクリックします。

AS-SIP 機能	設定の説明
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 （967 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 の設定の詳細については、『*Cisco Unified Communications Manager* システム構成ガイド』の「デュアル スタック Ipv6 構成タスク フロー」の章を参照してください。
マルチレベルの優先およびプリエンプション	マルチレベルの優先およびプリエンプション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、「マルチレベルの優先およびプリエンプション のタスク フロー （1030 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 の設定に関する詳細は、『*Cisco Unified Communications Manager* のセキュリティ ガイド』の「TLS 設定」の章を参照してください。

AS-SIP 機能	設定の説明
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* のセキュリティ ガイド』の「Cisco V.150 最低要件（MER）」の章を参照してください。



第 70 章

マルチレベルの優先およびプリエンプション 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

マルチレベルの優先およびプリエンプション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。

マルチレベルの優先およびプリエンプションの前提条件

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* 電話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。

マルチレベルの優先およびプリエンプションのタスク 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（1032ページ）を行うには、次のサブタスクを実行します。 • マルチレベルの優先およびプリエンプション ドメインの設定（1033 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（1034 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 ドメイン一覧の設定（1034 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マルチレベルの優先およびプリエンプション設定（1035 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	マルチレベルの優先およびプリエンプション のエンタープライズパラメータの設定（1036 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。

	コマンドまたはアクション	目的
ステップ 4	マルチレベルの優先およびプリエンプション のパーティションの設定 （1037 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	マルチレベルの優先およびプリエンプション のコーリング サーチ スペースの設定 （1039 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	マルチレベルの優先およびプリエンプション のルート パターンの設定 （1040 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	マルチレベルの優先およびプリエンプション のトランスレーション パターンの設定 （1042 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 マルチレベルの優先およびプリエンプション の設定 （1043 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	電話機のマルチレベルの優先およびプリエンプション の構成 （1044 ページ）	
ステップ 10	マルチレベルの優先およびプリエンプション コールの電話番号の設定 （1046 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）]

	コマンドまたはアクション	目的
		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	マルチレベルの優先およびプリエンプション のユーザ デバイス プロファイルの設定 （1047 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	マルチレベルの優先およびプリエンプション のデフォルトのデバイス プロファイルの設定 （1048 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	マルチレベルの優先およびプリエンプション ドメインの設定 （1033 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

	コマンドまたはアクション	目的
		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。
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 （1034 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 ドメイン一覧の設定 （1034 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。

マルチレベルの優先およびプリエンプション 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] 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 ～ FFFFFF である必要があります （000000 は、デフォルトの MLPP ドメイン ID 用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 情報セクションにリソース プライオリティ ネームスペース ネットワーク ドメインの名前を入力します。 ドメイン名の最大数は 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 ドメイン一覧の設定

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 リソースプライオリティ ネームスペース 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、どの言語でも最大 50 文字まで指定できますが、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 マルチレベルの優先およびプリエンプション 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 次のいずれかの作業を実行します。

- 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] 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。

マルチレベルの優先およびプリエンプション 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。

マルチレベルの優先およびプリエンプション のエンタープライズ パラメータ

表 *85 :* マルチレベルの優先およびプリエンプション 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 **MLPP Indication turned off** です。

パラメータ	説明
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。
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。

マルチレベルの優先およびプリエンプション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** > **コントロールのクラス** > **パーティション**。

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。

説明にはどの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサイド（&）、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 *86 :* 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

パーティション名の長さ	パーティションの最大数
...	...
10 文字	92
15 文字	64

マルチレベルの優先およびプリエンプション 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** > **コントロールのクラス** > **コーリングサーチスペース**。

ステップ 2 [新規追加] 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、どの言語でも最大 50 文字まで指定できますが、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、**コントロール（Ctrl）**キーを押したまま、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。

マルチレベルの優先およびプリエンプション 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 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] 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。

マルチレベルの優先およびプリエンプション のルート パターン設定フィールド

表 *87 :* マルチレベルの優先およびプリエンプション 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。 大文字の A、B、C、D、および \+ を指定できます。\+ は、国際的なエスケープ文字 + を表します。

フィールド	説明
[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。 • [エクゼクティブオーバーライド(Executive Override)]：MLPP コールに、一番高い優先度を設定します。 • [フラッシュ オーバーライド（Flash Override）]：MLPP コールに関する 2 番目に高い優先度を設定します。 • [フラッシュ(Flash)]：MLPP コールに、3 番目に高い優先度を設定します。 • [即時(Immediate)]：MLPP コールに、4 番目に高い優先度を設定します。 • [プライオリティ(Priority)]：MLPP コールに、5 番目に高い優先度を設定します。 • [ルーチン（Routine）]：MLPP コールに関する最低優先度を設定します。 • [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。
[ブロックコール率の適用(Apply Call Blocking Percentage)]	Destination Code Control（DCC）機能を使用可能にする場合に、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、この接続先に対するフラッシュ以上の優先レベルのコール以外のすべてのコールがフィルタリングされ、接続先に設定されているブロック コール率のクォータに基づいて許可または拒否されます。 フラッシュ以上の優先レベルのコールは常に許可されます。 DCC は、デフォルトでは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。
[ブロックコール率(%)(Call Blocking Percentage (%))]	この宛先でブロックするコールの割合を数値で入力します。 この値は、この宛先に対する優先順位の低いコールについて、ルート パターンによってブロックされるコールの割合を指定します。 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。

フィールド	説明
[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。

マルチレベルの優先およびプリエンプション 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 管理で、**[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 次のいずれかの作業を実行します。

- 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] 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。

- **[エクゼクティブオーバーライド(Executive Override)]**：MLPP コールに、一番高い優先度を設定します。
- [フラッシュ オーバーライド（Flash Override）]：MLPP コールに関する 2 番目に高い優先度を設定します。
- **[フラッシュ(Flash)]**：MLPP コールに、3 番目に高い優先度を設定します。
- **[即時(Immediate)]**：MLPP コールに、4 番目に高い優先度を設定します。
- **[プライオリティ(Priority)]**：MLPP コールに、5 番目に高い優先度を設定します。
- [ルーチン（Routine）]：MLPP コールに関する最低優先度を設定します。
- [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 マルチレベルの優先およびプリエンプション 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 次のいずれかの作業を実行します。

- 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] 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 マルチレベルの優先およびプリエンプション の構成

⚠

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 管理から、**[デバイス]** > **[電話機]** 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。

電話機への マルチレベルの優先およびプリエンプション の設定

表 *88 :* 電話機への マルチレベルの優先およびプリエンプション の設定

電話機の **MLPP** 設定 フィールド	説明
共通デバイス設定	設定した共通デバイス設定を選択します。 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。

電話機の **MLPP** 設定 フィールド	説明
[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られる 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。 共通のデバイス設定に MLPP ドメイン設定がない場合、このデバイスは、MLPP Domain Identifier エンタープライズ パラメータに設定された値からその MLPP ドメインを継承します。
[MLPP通知(MLPP Indication)]	使用可能な場合、この設定は、優先トーンを再生できるデバイスが MLPP 優先コールの発信時にその再生機能を使用するかどうかを指定します。 ドロップダウン リストにある次のオプションの中から、デバイスに割り当てる設定を選択します。 • **[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)]**：このデバイスは、MLPP 優先コールの通知の制御も処理もしません。 • **[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。 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(MLPP Indication)] をオンにすると、[MLPP通知(MLPP Indication)] をデバイスに対してオフ（上書き）にしない限り、デバイスで回線に対する通常の呼び出し音設定が動作しません。

電話機の MLPP 設定 フィールド	説明
[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使用できないことに注意してください。 使用可能な場合、この設定は、進行中のコールを優先できるデバイスが MLPP 優先コールの発信時にその優先機能を使用するかどうかを指定します。 ドロップダウン リストにある次のオプションの中から、デバイスに割り当てる設定を選択します。 • **デフォルト** ：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。

マルチレベルの優先およびプリエンプション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。

マルチレベルの優先およびプリエンプション 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 次のいずれかの作業を実行します。

- 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] 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)]**：このデバイスは、デバイス プールから [MLPP通知(MLPP Indication)] の設定値を引き継ぎます。
- **[オフ(Off)]**：このデバイスは、MLPP 優先コールの通知の制御も処理もしません。

- **[オン(On)]**：このデバイスは、MLPP 優先コールの通知を制御し処理します。

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(MLPP Preemption)] の設定値を引き継ぎます。
- [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。

マルチレベルの優先およびプリエンプション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 次のいずれかの作業を実行します。

- 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)]**：このデバイスは、デバイス プールから [MLPP通知(MLPP Indication)] の設定値を引き継ぎます。
- **[オフ(Off)]**：このデバイスは、MLPP 優先コールの通知の制御も処理もしません。
- **[オン(On)]**：このデバイスは、MLPP 優先コールの通知を制御し処理します。

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 (MLPP Preemption)] の設定値を引き継ぎます。
- [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およびプリエンプションの連携動作

表 *89 :* マルチレベルの優先およびプリエンプション の連携動作

機能	データのやり取り
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。

機能	データのやり取り
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。
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。

マルチレベルの優先およびプリエンプションの制約事項

表 *90* : マルチレベルの優先およびプリエンプション の制約事項

制約事項	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。
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。

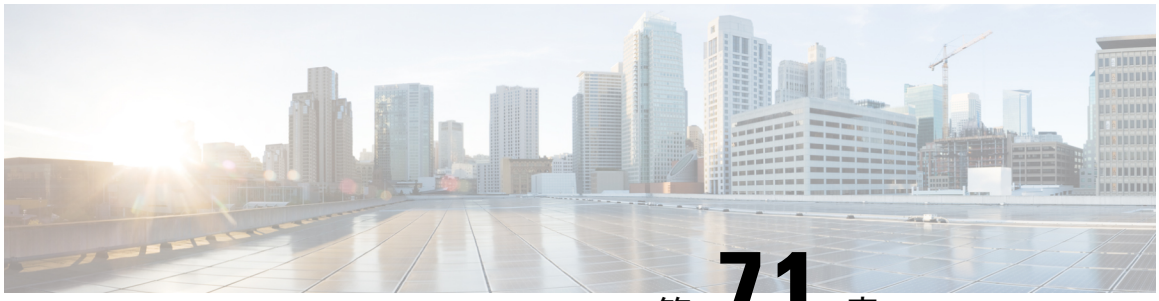
制約事項	説明
回線グループ	MLPP 対応デバイスは回線グループではサポートされません。次のガイドラインを推奨します。 • 回線グループ内ではMLPP対応デバイスを設定しないでください。ただし、ルートグループはサポートしています。トランク選択とハンティングの両方の方法がサポートされています。 • MLPP対応デバイスが回線グループまたはルートグループで設定されると、プリエンプション処理が行われたときに、ルートリストがデバイスをロックしない場合、プリエンプション処理されたコールは、ルート/ハント リスト内の他のデバイスに再ルーティングされ、コールを受け取ることができるデバイスがなくなった後でのみ、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。
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。

制約事項	説明
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。

制約事項	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、次の制約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 電話 7960、7962、7965 • Cisco Unified IP 電話 7940、7942、7945

第 XVI 部

SIP の相互運用性



第 71 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の概要

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。

- **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。
- **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。
- **diversion-counter**：転送カウンタを調整する機能を提供します。
- **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。
- **redsky-alternate-id-interop**: 発信招待に Redsky ヘッダーを追加します。
- **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 （1058 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 （1060 ページ）	これはオプションです。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 （1061 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 Communications 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 （1061 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。 Cisco Unified Communications Manager は、そのSIPプロファイルを使用するすべてのSIPメッセージングに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] 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　これはオプションです。 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 （1061 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 （1061 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。

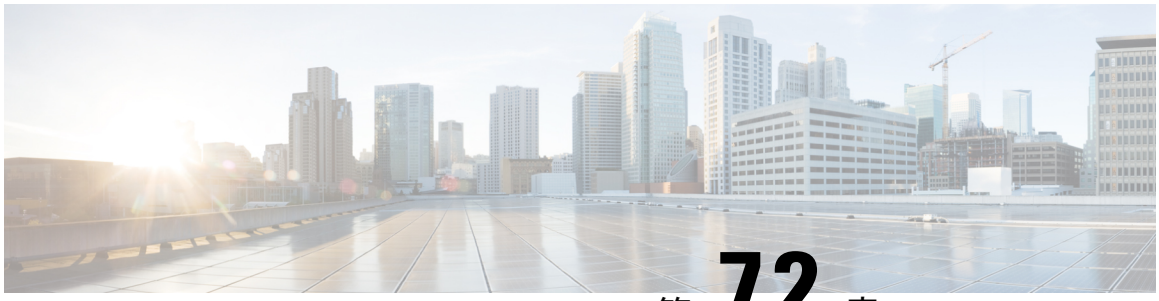
a) 正規化する [パラメータ名（Parameter Name）]と、そのパラメータに適用する値 [パラメータ値（Parameter Value）]を入力します。 たとえば、[ロケーション（Location）]パラメータと、値として「North Carolina」を入力します。

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 72 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 透明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] をクリックします。

ステップ 3 [Name]と [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。

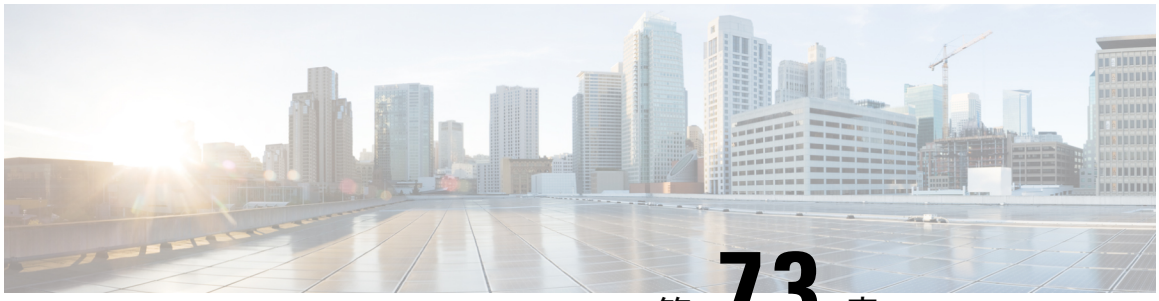
- プロパティの属性をパス スルーするには、[名前（Name）]テキスト ボックスに「a=recvonly」などの属性を入力し、[タイプ（Type）]ドロップダウン リストから [プロパティ（Property）]を選択します。
- 値属性をパススルーするには、[名前（Name）]テキスト ボックスに属性（たとえば a=rtpmap）を入力し、[タイプ（Type）]ドロップダウン リスト ボックスから [値（Any Value）]を選択します。
- 最大 5 個の値のいずれかを指定した値の属性をパス スルーするには、**[名前（Name）]** フィールドに「a=rtpmap」などの属性を入力し、**[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]** 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 73 章

BFCP を使用したプレゼンテーションの共有設定

バイナリフロア制御プロトコルの概要

Unified Communications Manager は、サポートされている Cisco エンドポイントおよびサードパーティのビデオエンドポイントに対して、Binary Floor Control Protocol (BFCP) を使用したプレゼンテーションの共有をサポートします。 この機能を使用すると、ユーザは進行中の音声またはビデオによる会話内でプレゼンテーションを共有できます。

次の例は、BFCP を使用してプレゼンテーションの共有がどのように動作するかを示しています。

- 2 つのテレビ電話間で通話中のビデオによる会話が行われています。 ユーザ A は、会話中にユーザ B とコンテンツを共有することを決定します。 ユーザ A は、画面全体を共有するか、または特定のアプリケーションを共有するかを選択できます。
- BFCP ストリームは、ユーザ B がユーザ A の共有コンテンツを表示できるようにします。

コンテンツ共有を使用した音声ビデオ コールでは、少なくとも 4 つのチャネル (音声、メインビデオ、2 番目のビデオ、BFCP 制御チャネル) が必要です。2 つ目のビデオチャネルでビデオ会議を実行し、プレゼンテーションを共有できます。 コールパーティが、末端のカメラ制御 (FECC) をサポートしている場合は、5 番目のチャネルを確立する必要があります。

BFCP を使用したプレゼンテーションの共有

リリース 12.5(1)SU3 以降から、Unified Communications Manager登録された SIP エンドポイントでは 、BFCP は以下の場合に機能します。

- 音声対応モードで会話を開始するための2つのビデオ対応エンドポイントは、BFCPサポートを使用してコール中にコンテンツを共有します。

• TRP は、コール中に割り当てられます。

BFCP のアーキテクチャ

BFCP を使用したプレゼンテーションの共有は、BFCP が有効な SIP ネットワーク上でのみサポートされています。 エンドポイントデバイスおよびトランクを含むネットワーク全体が SIP である必要があります。

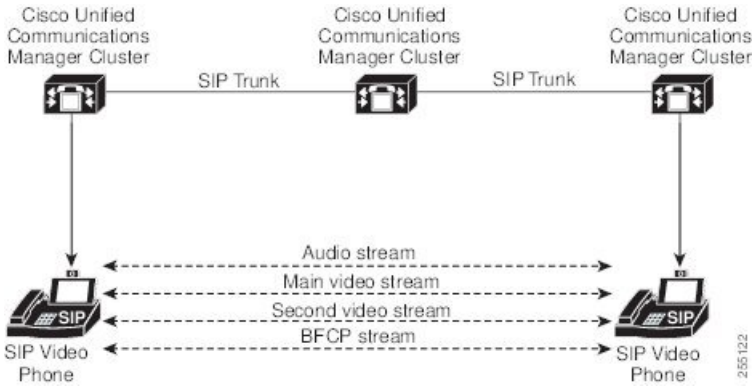
Unified Communications Manager は、2 つのエンドポイント間で SIP メッセージを中継することによって、BFCP ストリームのネゴシエーションを支援します。

このネゴシエーションには、共有リソースへのアクセスの一時的な権限である、フロアの確立を伴います。

BFCP ストリームは、エンドポイント間のポイントツーポイント ストリームです。 Unified Communications Manager は BFCP ストリームのターゲットではありません。

次の図に、複数の Unified Communications Manager クラスタを使用する複雑なビデオ ネットワークの例を示します。 BFCP は、デバイスに接続されているすべてのトランクおよび回線で有効になっている必要があります。 このネットワークの場合、BFCP は、エンドポイントに接続する 4 つの SIP トランクと 2 つの SIP 回線で有効になっている必要があります。

図 *14 : 複数の Cisco Unified Communications Manager* クラスタを使用するビデオ ネットワーク



BFCP に関する制約事項

次のシナリオにおいて、Unified Communications Manager は BFCP ストリー ムを拒否します。

- ネットワーク内の SIP 回線または SIP トランクのうちいずれかの [SIPプロファイル(SIP Profile)] ページの **[BFCPを使用するプレゼンテーション共有を許可(Allow Presentation Sharing using BFCP)]** チェックボックスがオフにされている。
- 一方のエンドポイントが BFCP をオファーするが、相手側のエンドポイントはオファーしない。
- SIP 回線または SIP トランクが MTP (非パススルーモード) またはトランスコーダーを使用している場合。

（注） BFCP 制御チャネルは常に暗号化されています。 ただし、両方の電話機が暗号化されている場合は、プレゼンテーションチャネルが暗号化されます。

BFCP 前提条件を使用したプレゼンテーションの共有

- コールフロー内のすべてのエンドポイントとトランクが SIP プロファイルを実行していることを確認します。
- 電話機サポート手順を確認し、機能 **BFCP サポート**のレポートを生成して、BFCP を使用したプレゼンテーション共有をサポートするシスコ エンドポイントの リストを取得します。 これらのエンドポイントは、BFCP サポートがデフォルトでは有効になっています。 BFCP をサポートするために、追加の設定を行う必要はありません。 詳細については、電話機能一覧の生成 （5 ページ） を参照してください。

BFCP構成タスクフローを使用したプレゼンテーションの共有

バイナリのフロア制御プロトコル (BFCP) を使用したプレゼンテーションの共有を有効にするには、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 トランクの BFCP サポートを有効化 （1069 ページ）	コールフロー内のすべての SIP トランクで BFCP サポートを有効にします。
ステップ 2	サードパーティ製の電話機で BFCP を使用してプレゼンテーションの共有を有効化 （1070 ページ）	サードパーティの SIP エンドポイントを使用している場合は、サードパーティの電話機の設定で BFCP サポートを有効にします。

SIP トランクの BFCP サポートを有効化

プレゼンテーション共有を BFCP と共に使用している場合、この機能は、メッセージングまたはコールフローのすべてのトランクで使用される SIP プロファイルで有効にする必要があります。 BFCP ストリームは、プレゼンテーションの共有をサポートしていないトランクによって拒否されます。

手順

ステップ 1 SIP トランクで使用される SIP プロファイル内で BFCP サポートを有効にします。

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

b) 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] をクリックします。**

c) **[SDP 情報]** セクションで、Unified Communications Manager の BFCP を有効にするには、**[BFCP を使用してプレゼンテーションの共有を許可する]** 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は、デフォルトでオフになっています。プレゼンテーション共有では、Unified CM クラスタ間のすべての SIP トランクに対して BFCP を有効にする必要があります。

d) **[SIP プロファイルの設定（SIP Profile 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。

e) **[保存]** をクリックします。

ステップ 2 BFCP 有効 SIP プロファイルを SIP トランクに関連付けるには、次のようにします。

a) Cisco Unified CM Administration から、**[デバイス]** > **[トランク]** を選択します。

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

c) **[SIP 情報]** セクションで、**SIP プロファイル** ドロップダウン リストから、インタークルースター コール内でプレゼンテーションを共有するために BFCP を有効にした SIP プロファイル を選択します。

d) **[保存]** をクリックします。

e) BFCP セッションのコールフローに含まれるすべての SIP トランクに対してこの手順を繰り返します。

サードパーティ製の電話機で BFCP を使用してプレゼンテーションの共有を有効化

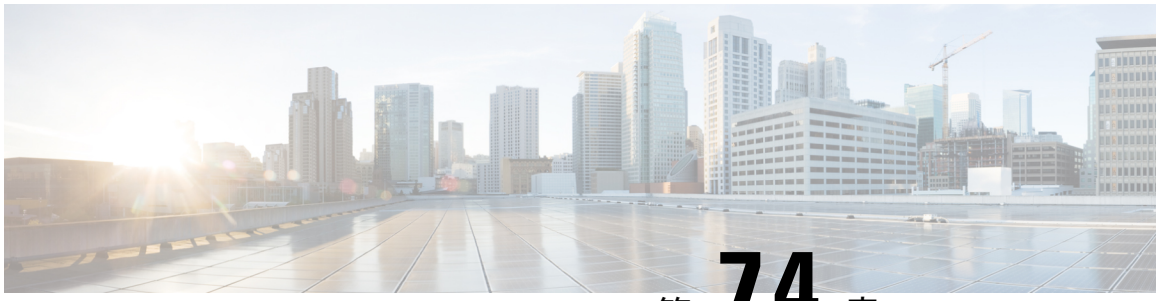
サードパーティ SIP 電話で BFCP を使用してプレゼンテーションの共有を使用する場合は、そのエンドポイントでこの機能が有効になっていることを確認する必要があります。 この機能は、次のサードパーティ製電話タイプでサポートされています。

- [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 エンドポイント（Third-party AS-SIP Endpoint）]

手順

ステップ 1 Cisco Unified CM 管理から、**[デバイス]** > **[電話機]** を選択します。
ステップ 2 **[検索]** をクリックして、既存のサードパーティ SIP 電話を選択します。
ステップ 3 **[BFCP を使用したプレゼンテーション共有を許可する]** 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。



第 74 章

ビデオ テレフォニー

ビデオ テレフォニー の概要

Unified Communications Manager は、音声コールとビデオ コールの領域を一体化するビデオ テレフォニーのサポートを提供します。 ビデオ エンドポイントは、Unified CM のコール処理機能を使用し、音声およびビデオによる統合ソリューションにアクセスすることで、ビデオ コールのダイヤリングおよび接続を行います。

Unified Communications Manager のビデオ テレフォニー ソリューションは、次の機能を提供します。

- 遠端カメラ制御（FECC）などのビデオおよびビデオ関連機能のサポート
- ビデオ ストリームの伝送を許可するために必要な複数の論理チャネルのサポート
- ビデオに必要なメディア関連メッセージのコール中の転送（ビデオ コールに必要なコマンドまたは指示を転送します）
- H.323、Skinny Client Control Protocol（SCCP）、および Session Initiation Protocol（SIP）のサポート
- リージョンとロケーションの拡張による帯域幅の管理
- ビデオ コールに関するコール詳細レコード（CDR）などのサービスアビリティ情報の提供

ビデオ テレフォニーのサポート

次のセクションでは、Cisco Unified Communications Manager 環境におけるビデオ テレフォニーの詳細を説明します。

ビデオ通話

一般的なビデオ コールには、上下用の 2 つまたは 3 つの Real-Time Protocol（RTP）のストリーム（つまり、4 または 6 ストリーム）があります。 コールには、次のタイプのストリームを含めることができます。

- ビデオ（H.261、H.263、H.263+、H.264-SVC、X-H.264UC、H.264-AVC、H.265、AV1、VT Camera wideband video コーデック）
- 遠端カメラ制御（FECC）（オプション）
- Binary Floor Control Protocol（BFCP）

（注） ビデオ コールのコール制御は、他のすべてのコールを管理するコール制御と同じように動作します。 詳細については、『VLAN Configuration Guide』の「メディアリソースの設定」の章を参照してください。 また、Unified Communications Manager がビデオ会議ブリッジを自動的に配分する方法の詳細については、「システム設定ガイド」の「Conference Bridge の設定」の章を参照してください。

MTP トポロジ内の Real-Time Transport Control Protocol のパススルー

15.2（2）T 以前の IOS メディア ターミネーション ポイント（MTP）では、Real-Time Transport Control Protocol（RTCP）パケットをパススルーできないため、Real-Time Protocol（RTP）のフィードバック データを交換して RTP 送信を拡張することはできません。 RTCP の主な機能は、ストリーミング マルチメディア セッションの参加者に統計情報を定期的に送信することにより、メディア配信のフィードバックを提供することです。 RTCP は、メディア接続に関する情報、および送信されたオクテット数とパケット数、失われたパケット数、ジッタ、ラウンドトリップ遅延時間などの情報を収集します。 アプリケーションは、この情報を使用して、フローを制限するか別のコーデックを使用することにより、サービスパラメータの品質を管理できます。

IOS MTP バージョン 15.2（2）T 以降では、MTP が含まれたコールのエンドポイントが RTP 送信で引き続きフィードバックとステータスを送信できるように、RTCP パススルー機能をサポートしています。 RTCP パススルー機能は、メディア チャネルに適用されます。

RTCP パススルー機能は、特定のコール シグナリング プロトコルに限定されません。 たとえば、SIP 間、SIP と非 SIP 間、または非 SIP 間でも構いません。

Unified CM で RTCP パススルー対応 MTP を具体的に割り当てるには、コールが次の条件を満たしている必要があります。

- MTP をメディア パススルー モードにすることが必要な機能で、MTP が必要。 たとえば、TRP、DTMF 変換、IP アドレス V4/V6 変換などです。 RTCP パススルーは、メディアが通過モードの場合にのみ適用されます。
- RTCP パススルーの MTP を、MTP のスポンサーとなるエンドポイントのメディア リソース グループ リスト（MRGL）に含める必要がある。 MTP は、RSVP、TRP、DTMF 不一致の理由により挿入できます。
- コールがビデオ チャネルを確立できる場合、Unified CM が RTCP パススルー対応 MTP の検索を試みる。 たとえば、Unified CM は、MRGL 内の他の RTCP パススルー非対応の MTP の中から RTCP パススルー対応 MTP を選択します。 RTCP パススルー対応 MTP が利用できない場合でも、Unified CM がコールに MTP を割り当てます。
- コールがオーディオ チャネルのみ確立できる場合、Unified CM が、ビデオ コール以外のコールに対して意図的には RTCP パススルー対応 MTP を要求しない。 ただし、MRGL に RTCP パススルー対応 MTP のみ含まれている場合、Unified CM はそれらの MTP のいずれかをオーディオ コールに挿入します。
- RTCP パススルー対応 MTP を割り当てるためには、コールがビデオ コールの現在の CAC 帯域幅も満たしている必要がある。

（注） コールが最初にコール内の RTCP パススルー非対応の MTP（バージョン 15.2（2）T 以前）を使用して確立されており、コールがビデオ対応のコールにエスカレートされる場合、Unified CM は RTCP パススルー対応 MTP に再割り当てしません。 この場合、コールがビデオ コールにエスカレートされても、既存の MTP では RTCP パケットをパススルーできません。

ビデオ コーデック

通常のビデオ コーデックには、古いビデオ コーデックの H.261、インターネット プロトコル（IP）ビデオの提供時に使用される新しいコーデックの H.263、および高品質コーデックの H.264 があります。 システムでは、H.264 は、発信および終端エンドポイントで Skinny Client Control Protocol（SCCP）、H.323、および SIP を使用するコール専用にサポートされています。また、リージョンとロケーションもサポートされています。

Unified Communications Manager は、応答時に可能であれば、オファー側のビデオ コーデックの優先順位を維持します。エンドポイントで利用できる場合、H.265 が優先ビデオ コーデックで、それ以外の場合は、Unified Communications Manager は次のコーデックの設定順に従います。

(設定順)	コーデック	説明
1	H.265 (HEVC)	低い帯域幅を使用して高品質のビデオを提供します。

(設定順)	コーデック	説明
2	H.264 (SVC)	受信したパケットのサブセットを無視して、同じメディア ストリームから品質が可変なビデオをレンダリングできます。 （注） H. 264 SVC は H.264-AVC ビデオ圧縮標準に新しく追加されました。つまり、H.264-AVC をさらに機能強化したものです。 1 つのコンテナにさまざまなフレームレートと解像度で複数のビデオストリームをカプセル化する機能を備えています。
3	X-H.264UC(Lync)	Microsoft が独占所有権を持つバリアント
4	H.264 (AVC)	Advanced Video Coding
5	H.263	H.263 および H.261 コーデックのパラメータおよび標準値は、次のとおりです。 • ビット レートの範囲は、64 kb/s ～数 mb/s です。これらのビット レートは、100 b/s の任意の倍数にすることができます。 H.261 および H.263 はビットレートが 64 kb/s 未満でも機能しますが、このような低ビット レートの場合はビデオ品質が低下します。 • One-quarter Common Interchange Format（QCIF）（解像度は、176x144） • Common Interchange Format（CIF）（解像度は、352x288） • 4CIF（解像度は、704x576） • Sub QCIF（SQCIF）（解像度は、128x96） • 16CIF（解像度は、1408x1152） • Custom Picture Format • Resolution: • フレーム レート：15 fps、30 fps • 付録: F、D、I、J、K、L、P、T、N
6	H.261	

ビデオ コールの帯域幅は、オーディオとビデオの帯域幅の合計に一致します。 合計帯域幅には、オーバーヘッドは含まれません。

384 kb/s のビデオ コールを、64 kb/s（オーディオ）による G.711 と 320 kb/s（ビデオ）で構成することができます。 この合計には、オーバーヘッドは含まれません。 ビデオ コールのオーディオ コーデックが 24 kb/s による G.729 である場合、ビデオ レートは、合計帯域幅 384 kb/s を維持するために増加します。 コールが H.323 エンドポイントを使用する場合、H.323 エンドポイントは、利用可能な合計ビデオ帯域幅より少ない帯域幅を使用することができます。 プロトコルに関係なく、エンドポイントは常にコールの最大ビット レート未満で送信することを選択できます。

AV1 コーデックのサポート

AV1 は、オープン メディアのための同盟によって開発された次世代のビデオコーデックです。AV1 の利点は次のとおりです。

- 他のビデオ エンコーディングと比較して圧縮率が向上し、帯域幅の消費が削減され、ビジュアル品質が向上します。
- 非常に低い帯域幅のネットワーク上でユーザのビデオを有効にする
- 他のコーデックに対すする画面共有効率が大幅な向上

Unified Communication Manager は、エンドポイントが AV1 コーデックをサポートしている場合、メディアを確立するために AV1 コーデックのネゴシエーションをサポートします。

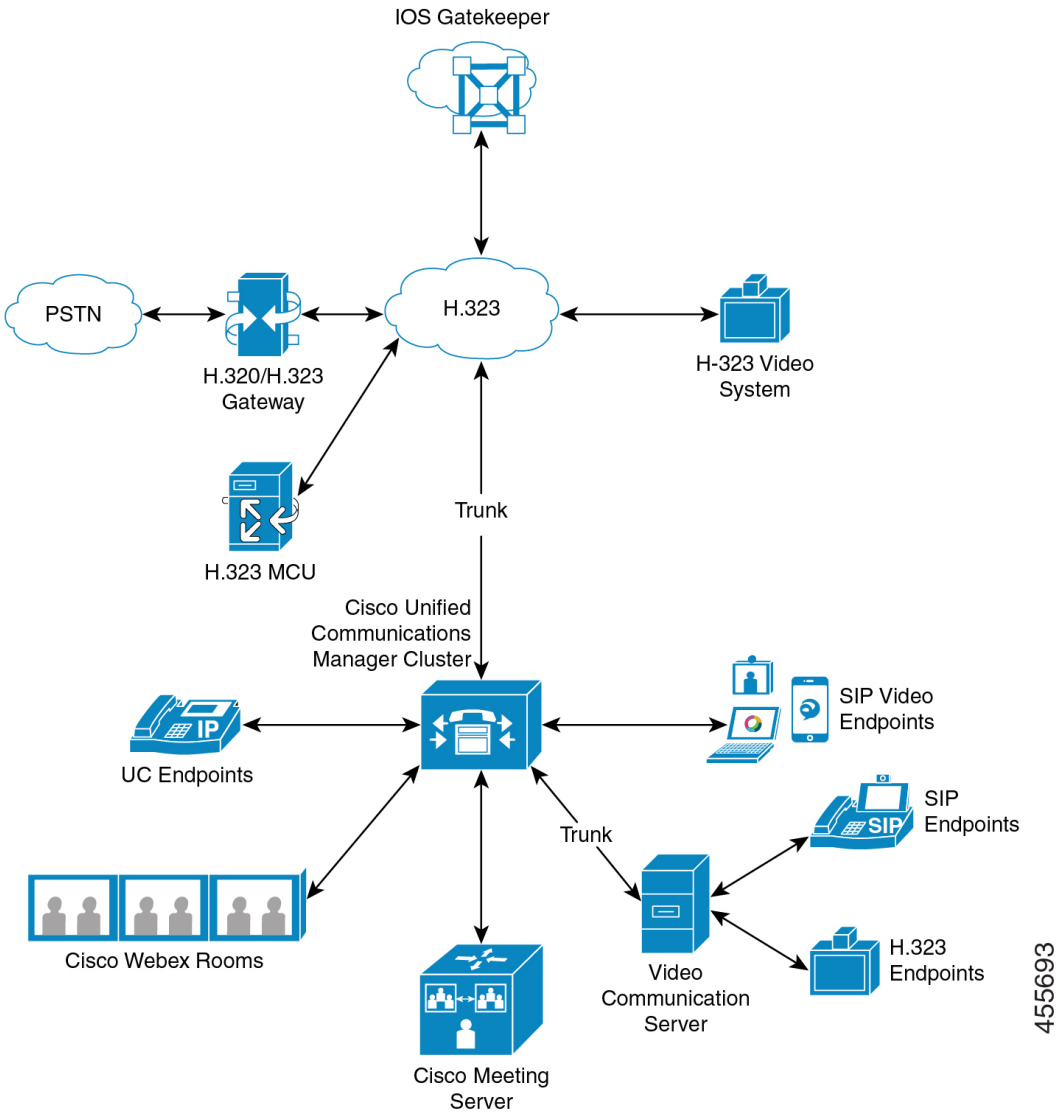
両方のエンドポイントが応答中の複数のコーデックをサポートしている場合、Unified CM は、受信した設定順序に基づいて AV1 を含むすべての一致するコーデックをネゴシエートします。エンドポイントは、ネゴシエートされたコーデック リストのコーデックのいずれかをメディア ストリーミングに使用します。 低帯域幅環境では、AV1 コーデックがネゴシエートされたリストの他のコーデックよりエンドポイントによって優先されます。

コールに関連する両方のエンドポイントが応答中の複数のコーデックをサポートしていない場合で、AV1 が他のコーデックより優先されるコーデックである場合、Unified CM はネゴシエートされたコーデックとして AV1 を選択します。

（注） AV1 コーデックは、テレプレゼンス エンドポイントではまだサポートされていません。

ビデオ ネットワーク

以下の図に、単一の Unified Communications Manager クラスタを使用するビデオ ネットワークの例を示します。 正常なビデオ ネットワークでは、任意のエンドポイントが、他のすべてのエンドポイントにコールできます。 両方のエンドポイントでビデオが有効である場合だけ、ビデオを利用できます。 ビデオ機能は、トランク全体に拡張できます。



シスコのビデオ会議のポートフォリオは、次のビデオ ブリッジで構成されます。

- Cisco TelePresence MCU シリーズ
- Windows インストーラー

Cisco UC エンドポイント ポートフォリオは、ビデオをサポートする次のエンドポイントで構成されます。

ビデオをサポートする Cisco UC エンドポイント ポートフォリオの詳細については、「互換性の合図」を参照してください。

（注） サードパーティの SIP ビデオエンドポイントは、回線側デバイスまたはトランク側デバイスとして Cisco Unified Communications Manager に接続できます。 詳細については、「サードパーティ SIP エンドポイント」を参照してください。

ビデオ テレフォニーの設定タスクフロー

Cisco Unified Communications Manager の管理ページでビデオ テレフォニーを設定するには、次の手順を実行します。

手順

ステップ 1 コール アドミッション制御でリージョンを使用する場合は、ビデオ通話帯域幅に対してリージョンを設定します。

（注） すべてのデバイスには、デフォルト リージョンが設定されています。ビデオのデフォルト値は、384 kb/s です。 リージョン設定で、目的の解像度に十分な高さの帯域幅を設定できます（たとえば、高画質のビデオ コールの場合は 2 Mb/s に増やします）。

ステップ 2 コール アドミッション制御でロケーションを使用する場合は、ビデオ コール帯域幅に対してロケーションを設定します。

ステップ 3 （任意） RSVP を SIP ビデオ コールの帯域幅の管理に使用している場合は、RSVP サービス パラメータを設定するか、[ロケーションの設定] ウィンドウで RSVP ポリシーを設定します。

ステップ 4 Cisco Video Conference Bridge を使用する場合は、ネットワークに対して適切な会議ブリッジを設定します。

ステップ 5 ユーザが他の会議ブリッジではなく、ビデオ会議ブリッジを使用するように設定するには、それに応じてユーザのメディア リソース グループおよびメディア リソース グループ リストを設定します。

ステップ 6 システムに H.323 ゲートウェイを設定して、オーディオ コールとしてビデオ コールを再試行（デフォルト動作）するか、AAR グループおよびルート/ハント リストを設定して、接続できないビデオ コールに対する代替ルーティングを使用します。

ステップ 7 システムに H.323 電話機を設定して、オーディオ コールとしてビデオ コールを再試行（デフォルト動作）するか、AAR グループおよびルート/ハント リストを設定して、接続できないビデオ コールに対する代替ルーティングを使用します。**[ビデオ機能を有効にする]** を選択します。

ステップ 8 システムに H.323 トランクを設定して、オーディオ コールとしてビデオ コールを再試行（デフォルト動作）するか、AAR グループおよびルート/ハント リストを設定して、接続できないビデオ コールに対する代替ルーティングを使用します。

ステップ 9 ビデオをサポートする Cisco Unified IP Phone を設定します。

ステップ 10 ビデオをサポートするサードパーティの SIP エンドポイントを設定します。

ステップ 11 システムにSIPトランクを設定して、オーディオ コールとしてビデオ コールを再試行（デフォルト動作）します。

H.323 ビデオ

H.323 ビデオの特性は、次のとおりです。

- H.323 エンドポイントを H.323 電話機、H.323 ゲートウェイ、または H.323 トランクとして設定可能です。
- 自動転送、ダイヤルプラン、他のコール ルーティング関連機能が、H.323 エンドポイントで機能します。
- H.323 ビデオ エンドポイントは、保留、再開、転送、パーク、およびその他の類似機能を開始することはできません。
- H.323 エンドポイントが Empty Capability Set（ECS）をサポートする場合は、エンドポイントの保留、パークなどが可能です。
- 一部のベンダーでは、コールが転送またはリダイレクトされる際に、コールの帯域幅を増やすことができないようにコール設定を実装しています。 このようなケースでは、最初のコールがオーディオであると、ビデオ エンドポイントに転送された場合に、ユーザはビデオを受信できません。
- 現在、ビデオのメディア ターミネーション ポイント（MTP）またはビデオ トランスコーダは存在しません。 オーディオ トランスコーダまたはMTPがコールに挿入されている場合、そのコールはオーディオだけになります。 これに該当するのは、IPVC オーディオ変換機能を使用していない場合です。 IPVC トランスコーダを使用する場合は、オーディオを変換して、ビデオを送信/受信することができます。
- H.323 ビデオ コールでは、ユーザがビデオ コールの帯域幅を指定する必要があります。

H.323 コールの H.239 拡張ビデオ チャネル

拡張ビデオ チャネル機能は、H.239 プロトコルを介して機能し、複数のビデオ チャネルのサポートを実現します。 Cisco Unified Communications Manager は、ダイレクト ポイントツーポイント H.323 コールで H.239 プロトコルを使用して拡張ビデオ チャネルをネゴシエートする処理をサポートしています。 これには、H.323 クラスタ間トランク上のコールも含まれます。

Cisco Unified Communications Manager は、H.239 の勧告で指定されている H.239 サポート関連の信号とコマンドをすべてサポートしています。

拡張ビデオ チャネル機能の特徴を次の項で説明します。

サードパーティの H.323 デバイスのサポート

拡張ビデオ チャネル機能は、サードパーティのビデオ エンドポイント間での H.239 の相互運用性と、Cisco Unified Voice Conferencing をサポートしています。 Cisco Unified Communications Managerでは、プレゼンテーションや、会議のライブ転送に拡張ビデオチャネルを使用できます。 この機能は、H.245 シグナリングによるマルチ ビデオ チャネルのサポートに重点を置いています。 このマルチチャネルのサポートの基盤となるのが次のプレゼンテーション アプリケーションです。

- Natural Presenter Package（サードパーティ ベンダーのビデオ エンドポイント）
- People+Content（サードパーティ ベンダーの Polycom 製）

Natural Presenter Package と People+Content のいずれも、H.239 プロトコルを使用して機能のネゴシエートを実行し、追加ビデオ チャネルのロールを定義します。

（注） ビデオ エンドポイント による Natural Presenter Package と Polycom 製の People+Content のみがプレゼンテーション モード用に H.239 をサポートしています。

ビデオ エンドポイントと Polycom から提供されているプレゼンテーション アプリケーションはオプションの機能です。 追加ビデオチャネルのネゴシエートを実行するには、このオプション機能のいずれかが使用可能になっている必要がある他、発信者と被発信者の両方のエンドポイントでH.239が有効になっている必要があります。そうでない場合、コールのビデオチャネルが 1 つに制限されます。

H.323 デバイスによるプレゼンテーション機能の起動

シスコとPolycomのビデオエンドポイントを使用すると、さまざまなコンポーネント（VCR、プロジェクタ、PC など）のプレゼンテーション資料を共有できます。 このコンポーネントをエンドポイントに物理的に接続できます。また、ベンダーから提供されるプレゼンテーション アプリケーションを PC で実行して、プレゼンテーション イメージを転送することも可能です。 プレゼンテーション ソースと、ビデオ エンドポイントへのコンポーネントの接続は、H.239 を使用してビデオ チャネルを確立するメカニズムとは無関係です。

（注） プレゼンテーション ソースの設定方法の詳細については、ビデオ エンドポイントのユーザ ガイドを参照してください。

H.239 対応の 2 台のエンドポイントがビデオ コールを確立するとき、これらの端末は、会議の参加者用のメイン ビデオチャネルと、追加ビデオチャネル用の拡張ビデオ機能（H.239機能）を確保するために、自身のビデオ機能を宣言します。 H.239機能の信号は次のように構成されます。

1. H.239 をサポートしていることを示す信号をエンドポイントが送信します。 また、これらの端末は、関連コマンドや追加ビデオ チャネルを管理する指示信号も送信します。 これ

により、両方のエンドポイントがコールで複数のビデオチャネルを開くことができると認識できます。

2. エンドポイントは、1 つまたは複数の拡張ビデオ コーデックの機能を送信して、追加チャネルのビデオ コーデックの機能を提示します。 このエンドポイントでは、追加ビデオチャネルのロールを指定する必要があります。 定義されるロールのラベルを次に示します。
   - ライブ ビデオ：このチャネルは標準的に処理されます。ユーザのライブ ビデオに適しています。
   - プレゼンテーション：このチャネルは、デバイスに配信されるトークン管理のプレゼンテーションを中継します。

機能に関するやり取りが行われた直後、従来のビデオ コールと同じように、両方のエンドポイントは双方向のオーディオ チャネルとメイン ビデオ チャネルを開きます。

追加ビデオ チャネルのオープン

実装されているサードパーティ製のエンドポイントに応じて、ベンダー間で追加ビデオチャネルの処理は異なります。

Natural Presenter Package（Tandberg）

ビデオ エンドポイントの場合、要求に応じて追加ビデオ チャネルが開始されます。 ビデオ エンドポイントのデバイスは、メイン ビデオ チャネルが確立されても、追加ビデオ チャネルをすぐに開きません。 追加チャネルが開かれるのは、発信者のいずれか（プレゼンター）がプレゼンテーションのソースを指定し、プレゼンテーションを開始するコマンドを実行したときです。

ビデオエンドポイントのユーザがプレゼンテーションの共有を開始することを決定すると、ビデオ エンドポイントは、プレゼンテーションのイメージを受信するための拡張ビデオ チャネルを開くことをコール相手に要求します。このため、ビデオエンドポイントのユーザ間のコールでは、一方向のみの追加ビデオ チャネルが使用されます。

People+Content（Polycom）

ビデオ エンドポイントとは異なり、Polycom のビデオ エンドポイントは、そのメカニズムのデフォルトの動作として、両方のビデオ エンドポイントが追加ビデオ チャネルをサポートしていることを確認した後、すぐに追加ビデオ エンドポイントを開きます。

（注） 両方の端末がH.239をサポートし、拡張ビデオチャネル機能が有効になっている場合、チャネルは自動的に確立されますが、どちらかの端末がプレゼンテーションの共有を開始するまで、追加チャネルからは何も表示されません。

Polycomは、追加ビデオチャネルを使用するかどうかに関係なく、追加ビデオチャネルをコール相手に要求します。このため、Polycom ユーザ間のコールでは、1 つのデバイスのみがプレゼンテーションのイメージやビデオを送信する場合でも、双方向のビデオチャネルがデバイス間で開かれます。

このような実装により、何かを提示するトークンを取得することを決定したときには、コールの両端で追加ビデオ チャネルでの転送準備ができていることになります。 2 つのビデオ チャネルのどちらかはアイドル（何も送信しない）状態ですが、Polycomデバイスは帯域幅を制御して負荷を効率化します。

この 2 番目のビデオ チャネルの処理の違いは、H.239 の実装には影響しません。Unified Communications ManagerH.323-H.323 コールでは受信チャネル 要求が開始されません。Unified CommunicationsManager単に、すべてのチャネル要求をある端末から別の端末にリレーします。

Unified Communications Manager は、追加のビデオ チャネルのセットに対して双方向の転送を強制しません。これは、H.239 プロトコルの要件ではないためです。

追加ビデオ チャネルでのコール アドミッション制御（CAC）

Cisco Unified Communications Manager の次のコール アドミッション制御ポリシーが追加ビデオチャネルに適用されます。

Cisco Unified Communications Manager は、ロケーション設定に基づいて、追加ビデオ チャネルによる帯域幅の使用を制限します。 追加ビデオチャネルが確立されているとき、Cisco Unified CommunicationsManagerはロケーションプールで充分なビデオ帯域幅が使用できる状態が維持されることを確認し、適切な帯域幅を予約します。 必要な帯域幅が使用できない場合、Cisco Unified Communications Manager は使用可能な帯域幅をゼロにするようにチャネルに指示します。

リージョンの設定やポリシーが、追加ビデオチャネルをサポートするために変更されることはありません。

従来の Cisco Unified Communications Manager のリージョン ポリシーは、ビデオ チャネルが 1 つのコールのみをサポートしており、このコールの帯域幅の合計使用量がリージョンの設定で指定されている値を超えることはありません。

管理者がH.239コールを対象としてリージョンのビデオ帯域幅に一定の制限を設定した場合、そのリージョンの値が、ビデオチャネルごとに独立して要求される帯域幅に対して使用されるため、Cisco Unified Communications Manager でリージョン ポリシーの違反が発生します。

例

地域のビデオ帯域幅が 384 Kbps に設定され、オーディオチャネルが 64 Kb/s を使用する場合は、次の値を使用します。各ビデオチャネルの最大許容帯域幅は (384 Kb/s - 64 Kb/s)= 320 Kb/s、つまり、H.239 コールで使用される最大帯域幅は audio bw + 2*(384 - audio bw))=704 Kb/s (地域が指定した 384 Kb/s の帯域幅を超える)になります。

（注） H.239 コールのリージョンとロケーションの両方の帯域幅制限を緩和して、Cisco Unified Communications Manager が関与しなくても H.239 デバイスが両方のビデオ チャネルの負荷を再調整およびバランシングできるようにすることを検討する必要があります。

許容ビデオ チャネル数

Unified Communications Manager 次の理由により、最大で 2 つのビデオ チャネルだけをサポートしています。

- シスコと Polycom のいずれも、サポートするビデオチャネルは2つだけです。このうち、1 つはメイン ビデオ用で、もう 1 つはプレゼンテーション用です。
- H.239 では、プレゼンテーションのために H.320 ベースのシステムが従来の H.320 ビデオ チャネルを分割できるようにする Additional Media Channel（AMC）のみが定義されています。

H.239 Command and Indication（C&I）メッセージ

Command and Indication（C&I）メッセージは、H.239 がプレゼンテーション ロールや Live ロールのトークンを管理したり、ビデオ フロー制御の解放要求をデバイスに許可して、追加のメディア チャネルを操作できるようにしたりするために使用されます。 Cisco Unified Communications Manager はすべての C&I メッセージをサポートしています。 Cisco Unified Communications Manager は、C&I メッセージを受け取ると、コール相手に適切に中継します。

フロー制御解放の要求メッセージと応答メッセージは、相手側のフロー制御解放の要求に使用できるため、エンドポイントは指定されたチャネルを指定されたビット レートで送信できます。

（注） コール相手は、フロー制御解放の応答に示されているとおりに要求を受け付けることもあれば、受け付けないこともあります。

プレゼンテーション ロールのトークンのメッセージにより、H.239 デバイスはプレゼンテーションのトークンを取得できます。 コール相手は、要求を受諾または拒否できます。 プレゼンターのデバイスは、不要になった時点で、トークンの解放メッセージを送信します。

トポロジとプロトコルの相互運用性の制限

Cisco Unified Communications Manager は、H.323 対 H.323 のコールで H.239 だけをサポートしています。 Cisco Unified Communications Manager により、H.239 コールを H.323 クラスタ間トランクまたは複数のノード経由で確立できます。 H.239 対応のデバイスが、非 H.323 デバイスにコールを実行した場合、H.239 の機能は無視され、コールは Cisco Unified Communications Manager でサポートされる従来のビデオ コールと同じように実行されます。

メディア ターミネーション ポイントまたはトランスコーダがコールに挿入されていると、追加ビデオ チャネルは Cisco Unified Communications Manager でサポートされません。 この場合、コールは通常のビデオ コールにフォールバックされます。

コール中の機能の制限

Cisco Unified Communications Manager では、H.323 対 H.323 のダイレクト コールでのみ、追加ビデオ チャネルを開くことができます。

⚠

注意 コール転送や保留/再開操作など、コール中の機能を実行しないでください。 実行すると、問題が発生し、追加ビデオ チャネルが切断されることがあります。

ビデオ サポート

Unified Communications Manager は、H.323、SCCP、SIP プロトコルを使用したビデオをサポートします。

Skinny Client Control Protocol ビデオ

Skinny Client Control Protocol ビデオの特性は、次のとおりです。

- Skinny Client Control Protocol 電話機がビデオ機能を通知すると、相手方がビデオをサポートする場合は、Cisco Unified Communications Manager が自動的にビデオ チャネルを開きます。
- Skinny Client Control Protocol ビデオ コールでは、システム管理者がリージョンを使用してビデオ コール帯域幅を決定します。 システムは、ユーザに対してビット レートを問い合わせません。

SIP ビデオ

SIP ビデオは、SIP シグナリング インターフェイス（SSI）を使用して、次のビデオ コールをサポートします。

- SIP から SIP

- SIP から H.323
- SIP から SCCP
- SIP クラスタ間トランク
- H.323 トランク
- SIP および H.323 トランクの組み合わせ

SIP ビデオ コールには、ビデオ会議のメディア制御機能もあります。

Unified Communications Manager ビデオは、SIP をサポートし、SIP のトランクと回線はどちらもビデオ シグナリングをサポートします。 SIP は、H.261、H.263、H.263+、H.264（AVC）、H.264（SVC）、X-H.264UC（Lync）、、AV1 の各ビデオ コーデックをサポートします（VTA で使用される wideband video コーデックはサポートしません）。

（注） AV1 コーデックをサポートするエンドポイントは一部のみです。 詳細については、『Compatibility Matrix』を参照してください。

ビデオ コール用の SIP デバイスの設定

SIP デバイス上でビデオ コールを有効にするには、次の手順を実行します。

SIP トランク

- コールでビデオ接続を使用できないときにオーディオを使用する場合は、Unified Communications Managerページの [トランクの設定] ウィンドウで [**ビデオコール**を**音声**として再試行] チェックボックスをオンにします。
- トランクをリセットします。

サードパーティの SIP エンドポイント

- コールでビデオ接続を使用できないときにオーディオを使用する場合は、Cisco Unified Communications Manager Administrationページの [電話の設定] ウィンドウで [**ビデオコール**を**音声**として再試行] チェックボックスをオンにします。
- エンドポイントをリセットします。

シスコのビデオ会議ブリッジ

Unified Communications Manager ビデオ会議用のさまざまなソリューションをサポートしています。 次のビデオ会議ブリッジは、アドホック ビデオ会議とミートミー ビデオ会議をサポートしています。

- Cisco TelePresence MCU

- Cisco TelePresence Conductor
- Cisco Meeting Server

Cisco TelePresence MCU ビデオ会議ブリッジ

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 を使用すると、アドホックとミートミーの両方の音声会議とビデオ会議を実現できます。 どの方式の会議ブリッジも、複数の参加者による複数の会議を同時にサポートしています。 Cisco TelePresence MCU は、ポート予約モードで設定する必要があります。

Cisco TelePresence Conductor ビデオ会議ブリッジ

Cisco TelePresence Conductor を使用すると、会議の管理をインテリジェントに制御できます。 Cisco TelePresence Conductor は、クラスタ化をサポートする、拡張性の高いデバイスで、MCU 間のロード バランシングを行い、複数のデバイスを利用可能にします。 管理者は、アプライアンスまたは VMware 上の仮想アプリケーションとして Cisco TelePresence Conductor を導入して、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ことができます。 動的な 2 方向または 3 方向会議が可能な多方向会議もサポートしています。

Cisco TelePresence Conductor を使用すると、アドホックとミートミーの両方の音声会議とビデオ会議を実現できます。 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済みの音声会議とビデオ会議では、MCU 単体のキャパシティを超えて動的に規模を拡張できます。 Cisco TelePresence Conductor アプライアンスまたは Cisco TelePresence Conductor クラスタ 1 つで、30 MCU または 2400 MCU ポートをサポートします。 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。

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、AV1コーデックをサポートするように拡張されており、H.265ビデオコーデックと遠端カメラ制御（FECC）をサポートしていません。

ビデオの暗号化

Unified Communications Manager は、通信にかかわる個々のエンドポイントでも暗号化がサポートされている場合、オーディオ、ビデオなどのメディア ストリームの暗号化をサポートします。 Unified CM は、Secure Real-Time Transport Protocol（SRTP）を使用して、メディア ストリームを暗号化します。 次のような機能があります。

- SIP および H.323 のエンドポイントのサポート
- メディア ターミネーション ポイント（MTP）passthru モードで動作時のメインのオーディオおよびビデオ回線の暗号化のサポート
- 複数の暗号化方式のサポート
- RFC 4568 に従った Session Description Protocol（SDP）crypto-suite セッション パラメータのサポート

暗号化された通信を提供するには、SIP コール設定時にエンドポイントと Unified Communications Manager の間で暗号キーが交換されます。 このような理由から、SIP シグナリングは TLS を使用して暗号化する必要があります。 初期コール設定時に、ビデオ エンドポイントは、サポートする暗号化方式のリストを交換し、両方のエンドポイントでサポートされる暗号スイートを選択して、暗号キーを交換します。 エンドポイント間で共通の暗号スイートが得られない場合、メディア ストリームは暗号化されず、Real-Time Transport Protocol（RTP）を使用して転送されます。

（注） 個々のエンドポイントが暗号化をサポートしていない場合、RTP を使用して通信が行われます。

VCS を使用した相互運用の設定

Unified Communications Manager を Cisco VCS に接続する SIP トランクで次の手順を実行して、Unified CM が Cisco VCS と相互運用できるようにします。

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）] > [トランク（Trunk）]**。

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]** 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]** ウィンドウで、Unified Communications Managerを Cisco VCS に接続する**トランク タイプ**、**デバイス プロトコル**、**トランク サービス タイプ**の選択をして、**[次へ]** をクリックします。

ステップ 4 **[SIP プロファイル]** ドロップダウン リストで、**[VCSの標準SIPプロファイル]** を選択します。

ステップ 5 **[正規化スクリプト]** ドロップダウン リストで、**[vcs-interop]** を選択します。

ステップ 6 **[正規化スクリプト]** 領域で、**[パラメータ名]** フィールドと **[パラメータ値]** フィールドを空白のままにします。 これらのフィールドに値が設定されている場合は、フィールドの内容を削除します。

ステップ 7 **[保存（Save）]** をクリックします。

ビデオ機能

SIP ビデオ ネットワークでは、次のビデオ関連機能がサポートされています。

- Binary Floor Control Protocol（BFCP）
- 暗号化された iX チャネル
- 遠端カメラ制御（FECC）

エンドポイントでの Binary Floor Control Protocol のサポート

Unified Communications Manager 特定のシスコのビデオ エンドポイントとサードパーティのビデオ エンドポイントで Binary Floor Control Protocol（BFCP）をサポートします。 BFCP を使用すると、ユーザは通話中のビデオによる会話内でプレゼンテーションを共有できます。

詳細については、『Feature Configuration Guide for Cisco Unified Communications Manager』の章「BFCP を使用したプレゼンテーション共有の設定」の章を参照してください。

暗号化された iX チャネル

Unified Communications Manager 暗号化された iX チャネルをサポートします。 IX チャネルは、ビデオ会議での SIP フォン間でアプリケーションメディアを多重化するための信頼性の高いチャネルを提供します。 暗号化された iX チャネルは、DTLS を使用して導入にセキュリティを追加し、アプリケーションメディアが iX チャネルを介して送信されるようにし、メディアを傍受しようとする中級者が見ることができないようにします。

[パススルーモード] の IOS MTP および RSVP エージェントは、暗号化された iX チャネルもサポートしています。

設定

Unified Communications Managerの暗号化された iX チャネルを有効にするには、次のことを実行する必要があります。

- 任意の中間 SIP トランクによって使用される [SIP プロファイル設定（SIP Profile Configuration）] の [**iX アプリケーション メディアを許可**（**Allow iX Application Media**）] チェックボックスをオンにします。 この設定では、iX チャネルのネゴシエーションがオンになります。
- セキュア着信**アイコン表示ポリシー**サービスパラメータを設定して、セキュアロックアイコンを有効にします。 デフォルトでは、[**BFCP および iX トランスポート以外の全メディアを暗号化すべき**（**All media except BFCP and iX transports must be encrypted**）] に設定されています。

暗号化モード

暗号化された電話機の場合、2 種類のセッション記述プロトコル (SDP) を使用して、Unified Communications Managerがサポートしている暗号化チャネルの暗号化をサポートしています。この暗号化タイプは、エンドポイントがサポートするものであり、Unified Communications Managerの設定可能な項目ではありません。

- **ベストエフォート方式**の暗号化: SDP オファーは暗号化された ix チャネルを目的としていますが、SIP ピアがサポートしていない場合は、暗号化されていない ix チャネルにフォールバックします。 このアプローチは、ソリューションで暗号化が必須ではない場合に使用することができます。

  たとえば、暗号化はクラウドで必須であり、単一の企業ではありません。

ベストエフォート iX 暗号化

M = アプリケーション 12345 **UDP/UDT/IX ***

A = セットアップ: actpass

a=フィンガープリント: SHA-1 <key>

- **強制暗号化**: SDP オファーは、暗号化された iX チャネルに対してのみ使用できます。 このオファーは、SIP ピアが iX チャネルの暗号化をサポートしていない場合には拒否されます。 このアプローチは、エンドポイント間で暗号化が必須になっている展開で使用できます。

  たとえば、2 つの SIP デバイス間の暗号化は必須です。

  強制 iX 暗号化

  m = アプリケーション 12345 **UDP/DTLS/UDT/IX ***

  A = セットアップ: actpass

  a=フィンガープリント: SHA-1 <key>

デフォルトでは、すべての Cisco IP Phone はベストエフォート iX 暗号化を提供するように設定されています。 ただし、Cisco テレプレゼンスエンドポイントの製品固有の設定内で **[暗号化モード（Encryption Mode）]** を**オン**に設定するか、または cisco Meeting Server の設定を再設定することによって、これを強制的に暗号化にすることができます。

非暗号化メディア

Unified Communications Managerエンドポイントが完全なセキュア モードで導入されていない可能性がある場合は、ミーティングのエンドポイントからのメディア パスでセキュア アクティブコントロール メッセージをネゴシエートできます。 たとえば、エンドポイントがオフネットで、モバイルおよびリモートアクセス モードの Unified CM で登録されている場合などです。

前提条件

この機能の使用を開始する前に、次のことを確認してください。

- システムが輸出規制要件を満たしている
- 会議ブリッジへの SIP トランクがセキュアである

Unified CM は、セキュアでないエンドポイントまたはソフトフォンに対してセキュア アクティブ コントロール メッセージの DTLS 情報をネゴシエートし、次の方法でメッセージを受信できます。

- オンプレミスの登録済みエンドポイントまたはソフトフォンに対しては**ベストエフォート方式の暗号化 iX**
- オフプレミスの登録済みエンドポイントまたはソフトフォンに対しては**強制 iX 暗号化**

遠端カメラ制御プロトコルのサポート

遠端カメラ制御（FECC）プロトコルを使用すると、リモートのカメラを制御できます。 ビデオコールでは、FECCにより、コールの一方の側で遠端のカメラを制御することができます。これには、カメラのパンニング、チルト、ズームインとズームアウトが含まれます。 複数のカメラを使用するビデオ会議では、FECC を使用して別のカメラに切り替えることができます。

Unified Communications Manager FECC 対応のビデオエンドポイントで FECC プロトコルをサポートしています。 Cisco Unified Communications Manager は、SIP から SIP へのコールまたは H.323 から H.323 へのコールで FECC をサポートしていますが、SIP から H.323 へのコールではFECC をサポートしていません。 FECC をサポートするため、Unified Communications Manager は SIP または H.323 シグナリングを介したアプリケーションメディアチャネルを設定します。メディア チャネルが確立されると、個々のエンドポイントでFECC シグナリングを伝達できるようになります。

ビデオ ネットワークの QoS

Cisco Unified Communications Manager には、ビデオネットワーク用の Quality of Service (QoS) を管理するための管理ツールが多数含まれています。

- 帯域幅の管理: 特定の地域と場所の帯域幅を調整します。
- 拡張ロケーションのコールアドミッション制御
- セッション レベルの帯域幅修飾子
- フレキシブル DSCP マーキング
- 代替ルーティング

帯域幅管理

オーディオおよびビデオ コールの帯域幅の割り当ては、Cisco Unified Communications Manager Administration で設定するリージョンおよびロケーションによって管理されます。

特定のコールに使用可能な帯域幅の量は、音声、ビデオ、シグナリング、およびBFCPプレゼンテーションなどのその他のメディアを含め、セッションに関連付けられたすべてのメディアストリームの組み合わせを管理できる必要があります。 Cisco Unified Communications Manager は、帯域幅を管理できる機能を備えています。

拡張ロケーションのコールアドミッション制御

拡張ロケーションコールアドミッションコントロール (CAC) では、広域（IP WAN）リンク上で同時に許可されるコール数を制限することにより、このリンクを経由するコールの音質およびビデオ品質を制御できます。 たとえば、メイン キャンパスとリモート サイトを接続する 56 kb/s フレーム リレー回線の音声品質は、コール アドミッション制御で調整できます。

CACは、コールを確立するために使用できる十分な帯域幅があるかどうかを確認します。 CACは、帯域幅が十分でないことを理由に、コールを拒否できます。

Unified Communications Manager では、ロケーションに基づいたコール アドミッション制御をリージョンと併用して、ネットワーク リンクの特性を定義します。 リージョンとロケーションは次のように機能します。

- リージョンにより、ビデオ コールの帯域幅を設定できます。 リージョンでのオーディオ制限によって、ビット レートの高いコーデックが除外されることがあります。 ただしビデオ コールでは、ビデオの制限により、ビデオの品質（解像度と転送速度）が抑制されます。
- ロケーションは、対象のリンクのすべてのコールで利用可能な総帯域幅の容量を定義します。 リンク上にコールが確立すると、そのコールのリージョンの値は、そのリンクに使用できる合計帯域幅から差し引く必要があります。

コールアドミッションコントロールの詳細については、次の「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設定」の章を参照してください。 Cisco Unified Communications Manager システム設定ガイド

.

セッション レベルの帯域幅修飾子

Unified Communications Manager では、セッション レベルの帯域幅修飾子を処理するためのロケーションのコール アドミッション制御のサポートを提供します。 セッション レベルの帯域幅修飾子は、初期 SIP シグナリングの SDP 部分のパラメータの一部として伝達されます。 これらのパラメータは、各エンドポイントがコールのそのタイプに対してサポートする帯域幅の最大量を示します。 これらのパラメータを、リージョンおよびロケーションの設定とともに使用して、各コールの帯域幅を設定します。

通話の初期設定中に、両方の当事者が通話のUnified Communications Manager最大許容帯域幅に通信します。Unified Communications Managerは、この伝達内容を相手側のエンドポイントに渡しますが、エンドポイントで指定されている帯域幅がリージョンの設定よりも大きい場合、Unified Communications Managerはこの値をリージョンの帯域幅の値に置き換えます。

Unified Communications Managerは、次のルールを使用して、特定のコールに割り当てる帯域幅の量を決定します。

- Unified Communications Managerは、エンドポイントからオファーまたはアンサーを受信した場合、SDP にセッション レベルの帯域幅修飾子があるかどうかをチェックします。
  - セッション レベルの帯域幅修飾子がある場合、Unified Communications Manager は、修飾子から帯域幅の値を取得します。 修飾子のタイプが2つ以上ある場合は、Transport Independent Application Specific（TIAS）、Application Specific（AS）、Conference Total（CT）の優先順位で修飾子を取得します。
  - セッション レベルの帯域幅修飾子がない場合、Unified Communications Manager は、メディア レベルの帯域幅修飾子の合計から帯域幅の値を取得します。

- 割り当てる帯域幅は、リージョン設定の最大値を上限として、2 つのエンドポイントがサポートするタイプの最大値です。 割り当てる帯域幅は、リージョン設定を超えることはできません。

Unified Communications Manager は、エンドポイントとの通信時に次のロジックを使用します。

- 2 つ以上のセッション レベルの帯域幅修飾子タイプ（TIAS、AS、CT）を含むエンドポイントへのアンサー、早期オファー、または Re-Invite オファーを生成する場合、Unified Communications Manager は、それぞれに同じ帯域幅の値を使用します。
- アンサーを生成する場合、Unified Communications Manager は初期オファーで受信したものと同じセッション レベルの帯域幅修飾子タイプ（TIAS、CT、AS）を使用します。
- 旧Unified Communications Manager は、ビデオ コールが保留され Music On Hold（MOH; 保留音）が挿入されたときに、セッション レベルの帯域幅修飾子を抑制します。

SIP 電話機のビデオ解像度のサポート

Cisco Unified Communications Manager は、高解像度ビデオ コールの SIP ヘッダーの SDP 部分にある imageattr 行をサポートします。 9951、9971、および 8961 などの w360p（640 x 360）をサポートする Cisco SIP 電話は、次の条件に応じて自動的に最適な解像度をビデオ コールに選択します。

- セッション レベル帯域幅が 800Kb/s より大きく、SDP に imageattr[640 x 480] 行が存在する場合は、VGA が使用されます。
- セッション レベル帯域幅が 800Kb/s より大きく、SDP に imageattr[640 x 480] 行が存在しない場合は、w360p が使用されます。
- セッション レベル帯域幅が 800Kb/s より小さく 480 bps より大きくて、imageattr[640 x 480] 行が存在する場合は、VGA 15 フレーム/秒が使用されます。

（注） 現在、w360p（640 x 360）ビデオ解像度をサポートする Cisco IP 電話モデル 9951、9971、または 8961 があり、Cisco Unified Communications Manager リリース 8.5(1) 以降にアップグレードしている場合は、ビデオ コールの解像度の変更に気付かない可能性があります。 w360p 解像度は、電話機ロード 9.2(1) で導入されました。

次のビデオ コール フローは、imageattr 行をサポートしない 2 台の 9951 電話機（電話機 A と電話機 B）間のフローです（例：Cisco Unified Communications Manager リリース 8.0(1) 以前を使用）。

1. 電話機 A は、SDP に imageattr 行がある SIP メッセージを送信します。
2. Cisco Unified Communications Manager は、SDP の imageattr 行を削除し、変更された SIP メッセージを電話機 B に送信します。

3. SIP ヘッダーの SDP 部分に imageattr 行がないため、電話機 B は、w360p 解像度のビデオを送信しようとします。

次のビデオ コール フローは、imageattr 行をサポートする 2 台の 9951 電話機（電話機 A と電話機 B）間のフローです（例：Cisco Unified Communications Manager リリース 8.5(1) 以降を使用）。

1. 電話機 A は、SDP に imageattr 行がある SIP メッセージを送信します。
2. Cisco Unified Communications Manager は、imageattr 行を削除および変更することなく、SIP メッセージを電話機 B に送信します。
3. 電話機 B は、VGA 解像度のビデオを送信しようとします。

代替ルーティング

エンドポイントが、ビデオ コールに必要な帯域幅を取得できない場合、デフォルトの動作でビデオ コールはオーディオ コールとして再試行します。 このようなビデオ コールでルート/ハント リストまたは自動代替ルーティング（AAR）グループを使用して別のルートを試行するには、該当するゲートウェイ、トランクおよび電話機の [ビデオコールをオーディオとして再試行(Retry Video Call as Audio)] 設定をオフにします。

詳細については、Cisco Unified Communications Manager システム設定ガイドの「コール ルーティングの設定」の章にある「AAR グループの設定」セクションを参照してください。

フレキシブル DSCP マーキング

DiffServ コード ポイント（DSCP）パケット マーキングは、各パケットのサービス クラスを指定するために使用されます。 DSCP マーキングを使用すると、特定のタイプのコールやメディアを他のタイプよりも優先することができます。 たとえば、音声をビデオよりも優先して、ネットワーク帯域幅の問題が起こっても、音声通話に帯域幅の問題は発生しません。

DSCP マーキングは、次のいずれかの方法でカスタマイズできます。

- クラスタ全体のサービス パラメータを設定し、クラスタのデフォルトの DSCP 設定を設定します。
- (オプション) DSCP カテゴリのサブセットについては、SIP プロファイルを介してカスタマイズした DSCP 設定をデバイスに割り当てる必要があります。 プロファイルを使用するデバイスでは、カスタマイズされた設定がサービス パラメータのデフォルトより優先されます。

DSCP マーキングを設定する方法の詳細については、『Feature Configuration Guide for Cisco Unified Communications Manager』の「柔軟な DSCP マーキングとビデオ 送信の設定」の章を参照してください。

ビデオ コール用の電話機の設定

ビデオ対応デバイスの次の設定は、ビデオ コールに影響を与えます。

- [ビデオコールをオーディオとして再試行(Retry Video Call as Audio)]：デフォルトでは、このチェックボックスはオンになっています。 したがって、エンドポイント（電話機、ゲートウェイ、トランク）が、ビデオコールに必要な帯域幅を取得できない場合は、コール制御によってオーディオ コールとしてコールが再試行されます。 この設定は、ビデオ コールの宛先デバイスに適用されます。
- [ビデオ機能の有効/無効(Video Capabilities Enabled/disabled)]：このドロップダウン リスト ボックスは、ビデオ機能のオン/オフを切り替えます。

ビデオ会議に対する会議制御

Unified Communications Manager は、次の会議制御機能をサポートしています。

- Roster/Attendee List
- Drop Participant
- Terminate Conference
- Show Conference Chairperson/Controller
- Continuous Presence

Unified Communications Manager また、Skinny Client Control Protocol 電話機に対する次のビデオ会議機能をサポートしています。

- ビデオ会議の制御を表示します。 SCCP 電話機では、continuous presence モードまたは voice-activated モードを使用すると、ビデオ会議を表示できます。 モードを選択すると、ビデオ チャネルで使用するモードを示すメッセージがブリッジに送信されます。 モードを切り替えても、メディアの再ネゴシエーションは必要ありません。
- ユーザ名などの参加者情報をビデオ ストリームに表示します。 システムでは、参加者情報を、roster などの会議機能に使用することができます。

詳細については、Cisco Unified Communications Manager セキュリティガイドの「暗号化された iX チャネル」の章を参照してください。

ビデオ テレフォニーおよび Cisco Unified Serviceability

Cisco Unified Serviceability は、パフォーマンス モニタリング カウンタ、ビデオ ブリッジ カウンタ、およびコール詳細レコード（CDR）を更新することによって、ビデオ コールおよび会議をトラッキングします。

パフォーマンス カウンタ

ビデオ テレフォニー イベントによって、次の Cisco Unified Serviceability のパフォーマンス モニタリング カウンタが更新されます。

Cisco CallManager

- VCBConferenceActive
- VCBConferenceCompleted
- VCBConferenceTotal
- VCBOutOfConferences
- VCBOutOfResources
- VCBResourceActive
- VCBResourceAvailable
- VideoCallsActive
- VideoCallsCompleted
- VideoOutOfResources

Gatekeeper

- VideoOutOfResources

CiscoH.323

- VideoCallsActive
- VideoCallsCompleted

Cisco Locations

- RSVP VideoCallsFailed
- RSVP VideoReservationErrorCounts
- VideoBandwidthAvailable
- VideoBandwidthMaximum
- VideoOutOfResources

Cisco SIP

- VideoCallsActive
- VideoCallsCompleted

Cisco Video Conference Bridge

- ConferencesActive
- ConferencesAvailable
- ConferencesCompleted
- ConferencesTotal
- OutOfConferences
- OutOfResources
- ResourceActive
- ResourceAvailable
- ResourceTotal

ビデオ ブリッジ カウンタ

ビデオ会議イベントによって、次の Cisco Video Conference Bridge のパフォーマンス モニタリング カウンタが更新されます。

- ConferencesActive
- ConferencesAvailable
- ConferencesCompleted
- ConferencesTotal
- OutOfConferences
- OutOfResources
- ResourceActive
- ResourceAvailable
- ResourceTotal

これらのカウンタは、Cisco Unified Communications Manager オブジェクト内に VCB プレフィックスとともに表示されます。

コール詳細レコード（CDR）

ビデオ テレフォニー イベントによって、Cisco Unified Serviceability 内のコール詳細レコード（CDR）が更新されます。 これらの CDR には、次の情報が含まれます。

- origVideoCap_Codec
- origVideoCap_Bandwidth
- origVideoCap_Resolution
- origVideoTransportAddress_IP

- origVideoTransportAddress_Port
- destVideoCap_Codec
- destVideoCap_Bandwidth
- destVideoCap_Resolution
- destVideoTransportAddress_IP
- destVideoTransportAddress_Port
- origRSVPStat
- destRSVPVideoStat
- origVideoCap_Codec_Channel2
- origVideoCap_Bandwidth_Channel2
- origVideoCap_Resolution_Channel2
- origVideoTransportAddress_IP_Channel2
- origVideoTransportAddress_Port_Channel2
- origVideoChannel_Role_Channel2
- destVideoCap_Codec_Channel2
- destVideoCap_Bandwidth_Channel2
- destVideoCap_Resolution_Channel2
- destVideoTransportAddress_IP_Channel2
- destVideoTransportAddress_Port_Channel2
- destVideoChannel_Role_Channel2

コール管理レコード（CMR）

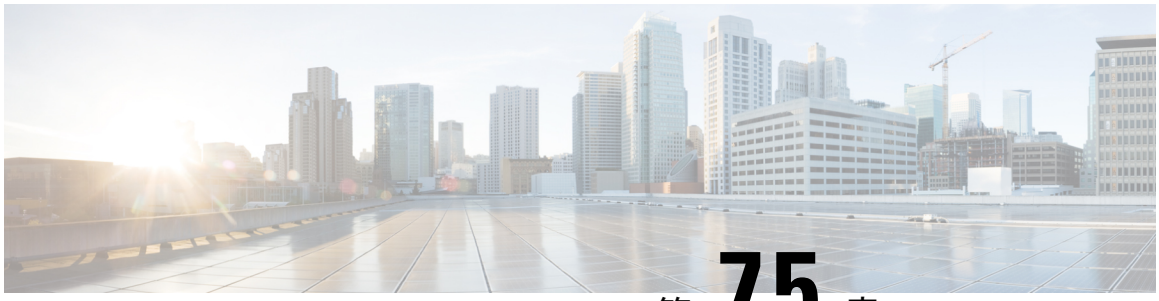
ビデオ テレフォニー イベントによって、Cisco Unified Serviceability 内のコール管理レコード（CMRs）が更新されます。 これらの CMRs には、次の情報が含まれます。

- videoContentType テキスト文字列
- videoDuration 整数
- numberVideoPacketsSent 整数
- numberVideoOctetsSent 整数
- numberVideoPacketsReceived 整数
- numberVideoOctetsReceived 整数
- numberVideoPacketsLost 整数
- videoAverageJitter 整数

- videoRoundTripTime
- videoOneWayDelay
- videoTransmissionMetrics

第 XVII 部

緊急コール ルーティング規制



第 75 章

米国連邦通信委員会 (FCC) 緊急コールルーティング規制

緊急コール ルーティング規制の概要

緊急コール ルーティング 規制は、緊急コール (911) が米国と米国以外のタイム ゾーンでどのように設定され、ルーティングされるのかについて、米国 FCC の法律に準拠した情報を提供します。

米国 FCC は、公安を促し、緊急サービスに対する国全体のシームレスな通信インフラストラクチャの迅速な導入を可能にすることで、公安を容易にするための次の法律に署名しました。

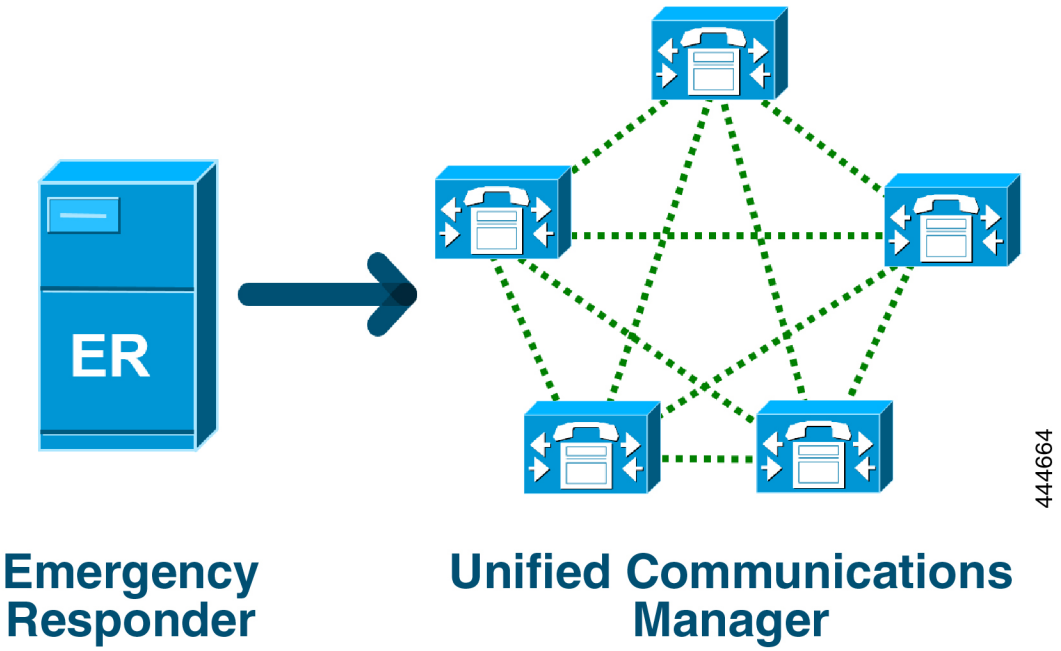
米国 FCC は、緊急通報 (911) ルーティングに関する以下の法律に署名しました。

- カリ法: この法律は、オフィスの建物、キャンパス、ホテルなどの設定でユーザにサービスを提供するマルチライン電話システム (MLTS) に適用されます。 FCC では、プレフィックスをダイヤルせずに 911 を直接ダイヤルし、緊急コールが発信された場合にフロントまたはセキュリティ オフィスに通知する必要があります。
- レイバウム法第506条に基づき、使用されている技術プラットフォームに関係なく、緊急電話で場所の詳細（住所、建物番号、階数、部屋番号）を発信し、911 コールセンターが発信者の場所を自動的に受信して応答者をより迅速にディスパッチできるようにします。

FCC 関連の法律の詳細については、次を参照してください。 https://www.fcc.gov/mlts-911-requirements

緊急応答者は、テレフォニー ネットワーク内のコールを効果的に管理して、すべての緊急コールに対応し、地域の法律に従って処理します。また、場所の詳細もディスパッチされ、通知は Unified Communications Manager にディスパッチされます。

次の図は、緊急応答者と Unified Communications Manager の間の接続を示しています。

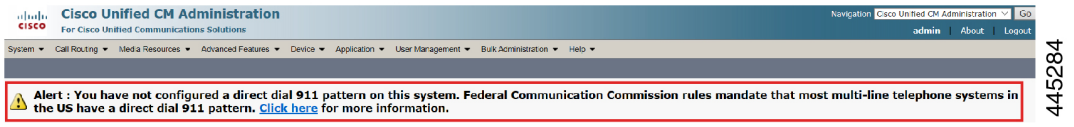


Cisco Emergency Responder の詳細については、Cisco Emergency Responder Administration Guide を参照してください。

MLTS としての Unified Communications Manager

Cisco Unified Communications Manager の管理ページは、米国のタイム ゾーンにインストールされているシステムに対するダイレクト 911 ダイヤル パターンの欠如を検出するインビルド ソフトウェアを備えた MLTS です。

911 ルート パターンが有効になっていない場合、Cisco Unified CM Administration のホーム ページにアラート メッセージが表示されます (**このシステムでは直通 ダイヤル 911 パターンは設定されていません)。 連邦通信委員会のルールでは、米国のほとんどのマルチライン電話システムには、直通ダイヤル 911 パターンが適用されます。**



FCC の法律が適用されない米国以外のタイム ゾーンにシステムがインストールされている場合は、Unified Communications Manager の [緊急コール ルーティング規制] 設定ページが無効になります)。

（注） FCC の法律の適用性について、法律顧問に相談してシステムで承認する必要があります。

緊急コール ルーティング規制の設定

法規制に準拠して直通ダイヤル 911 ルート パターンを確認および設定するように、Unified Communications Manager で緊急コール ルーティング規制が設定されています。

始める前に

FCC 法律を受け入れて設定した後、今後のために必ずバックアップを実行してください。

手順

ステップ 1 **[緊急コール ルーティング規制]** ウィンドウにアクセスするには、次のいずれかを実行します。

- [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**詳細機能** > **緊急コール ルーティング規制**
- アラート通知で利用可能なリンクをクリックして、ホームページの 911 ルート パターンを設定します。

ステップ 2 **[上記の通知を読み、特定の義務を決定するために弁護士に相談しました]** チェックボックスをオンにして通知を確認します。

ステップ 3 **[911 の設定ページに接続する]** チェックボックスをオンにして **[送信]** をクリックして、FCC の法律が適用される場合、直接 911 通知を設定します。 **[ルート パターンの設定]** ウィンドウに移動します。デフォルトでは、**[パターン定義]** セクションで 911 パターンが設定されます。

ステップ 4 設定したパターンに応じて、**[ゲートウェイ/ルート リスト]** ドロップダウン リストから、適切なゲートウェイ、ルート 、またはトランクを選択します。 その他フィールドと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]** をクリックします。

（注） システムが米国のタイムゾーンに設置されていて、FCC 法律が適切でない場合は、**[緊急コール ルーティング規制]** ウィンドウの **[911 の義務に関するその他の通知を無効にする]** のチェックボックスをオンにして、**[送信]** をクリックして 911 通知を無効にします。

法律が適用されない場合、管理者は、今後のアップグレードと 911 ルート パターンの新しいインストールについての通知を免除します。

設定が今後のアップグレードで維持されます。アラート通知はホームページから消え、**[緊急コール ルーティング規制]** ウィンドウは無効になります。

システムがアップグレード中にすでに 911 ルート パターンを作成している場合、またはタイムゾーンが米国以外のタイムゾーンから米国のタイムゾーンに変更された場合、確認ページはグレー表示されます。

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。