Cisco Unified Communications Manager リリース 12.5(1) 管理ガイド

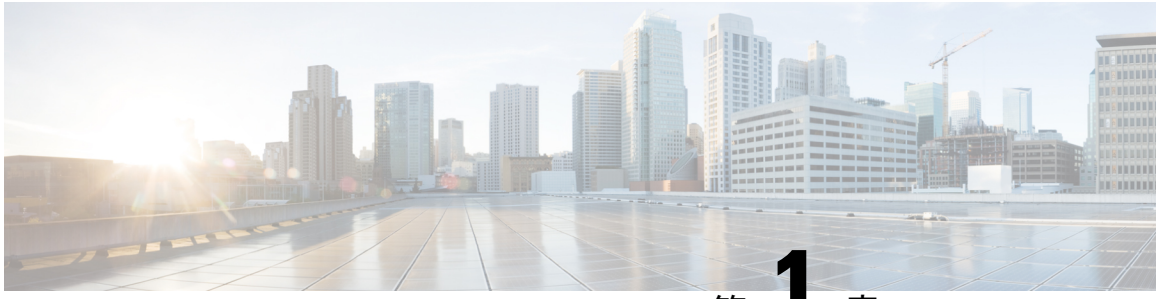
初版：2019 年 1 月 22 日

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/

目 次

第 I 部

管理の概要



第 1 章

管理の概要

Cisco Unified CM の管理の概要

Cisco Unified CM の管理は、Cisco Unified Communications Manager の主要な管理および設定インターフェイスとなる、Web ベースのアプリケーションです。Cisco Unified CM の管理を使用して、一般的なシステム コンポーネント、機能、サーバ設定、コール ルーティング ルール、電話機、エンド ユーザ、メディア リソースなど、システムの幅広い項目を設定できます。

設定メニュー

Cisco Unified CM の管理の設定ウィンドウは、以下のメニューで編成されています。

- [システム（System）]：このメニューに分類されている設定ウィンドウを使用して、一般的なシステム設定（サーバ情報、NTP 設定、日時グループ、リージョン、DHCP、LDAP 統合、エンタープライズ パラメータなど）を構成します。
- [コール ルーティング（Call Routing）]：このタブに分類されている設定ウィンドウを使用して、Cisco Unified Communications Manager によるコールのルーティング方法に関連する項目（ルート パターン、ルート グループ、ハント パイロット、ダイヤル ルール、パーティション、コール サーチ スペース、電話番号、変換パターンなど）を設定します。
- [メディア リソース（Media Resources）]：このタブに分類されている設定ウィンドウを使用して、メディア リソース グループ、会議ブリッジ、アナンシエータ、トランスコーダなどの項目を設定します。
- [拡張機能（Advanced Features）]：このタブに分類されている設定ウィンドウを使用して、ボイスメール パイロット、メッセージ受信、コール制御エージェント プロファイルなどの機能を設定します。

- [デバイス（Device）]：このタブに分類されている設定ウィンドウを使用して、電話機などのデバイス、IP Phone サービス、トランク、ゲートウェイ、ソフトキーテンプレート、SIP プロファイルを設定します。
- [アプリケーション（Application）]：このタブに分類されている設定ウィンドウを使用して、Cisco Unified JTAPI、Cisco Unified TAPI、Cisco Unified Real-Time Monitoring Tool などのプラグインをダウンロードおよびインストールします。
- [ユーザ管理（User Management）]：[ユーザ管理（User Management）] タブに分類されている設定ウィンドウを使用して、システムのエンド ユーザおよびアプリケーション ユーザを設定します。
- [一括管理（Bulk Administration）]：一括管理ツールを使用して、多数のエンドユーザやデバイスを同時にインポートおよび設定します。
- [ヘルプ（Help）]：このメニューをクリックすることで、オンライン ヘルプ システムにアクセスできます。オンライン ヘルプ システムには、システム上の各種設定ウィンドウの設定を構成する際に役立つドキュメントが含まれています。

オペレーティング システムの管理の概要

[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] を使用して、オペレーティング システムの設定と管理、および以下の管理タスクを実行します。

- ソフトウェアとハードウェアのステータスを確認する
- IP アドレスを確認および更新する
- 他のネットワーク デバイスに ping を送信する
- NTP サーバを管理する
- システム ソフトウェアおよびオプションをアップグレードする
- ノードのセキュリティを管理する（IPSec や証明書を含む）
- リモート サポート アカウントを管理する
- システムを再起動する

オペレーティング システムのステータス

以下のものを含め、各種のオペレーティング システム コンポーネントのステータスを確認できます。

- クラスタおよびノード
- ハードウェア
- ネットワーク
- システム
- インストールされているソフトウェアとオプション

オペレーティング システムの設定

オペレーティング システムの次の設定を表示し、更新できます。

- [IP]：アプリケーションのインストール時に入力した IP アドレスおよび DHCP クライアントの設定を更新します。
- [NTP サーバの設定（NTP Server Settings）]：外部 NTP サーバの IP アドレスの設定、および NTP サーバの追加を行います。
- [SMTP 設定（SMTP settings）]：オペレーティング システムが E メール通知の送信に使用する Simple Mail Transfer Protocol（SMTP）ホストを設定します。

オペレーティング システムのセキュリティ設定

セキュリティ証明書および IPsec の設定を管理できます。[セキュリティ（Security）] メニューでは、次のセキュリティ オプションを選択できます。

- [証明書の管理（Certificate Management）]：証明書および証明書署名要求（CSR）を管理します。証明書の表示、アップロード、ダウンロード、削除、および再作成を行うことができます。[証明書の管理（Certificate Management）] を使用して、ノード上の証明書の有効期限をモニタすることもできます。
- [IPsec の管理（IPsec Management）]：既存の IPsec ポリシーの表示や更新、新規の IPsec ポリシーとアソシエーション設定を行います。

ソフトウェアのアップグレード

オペレーティング システムで実行中のソフトウェア バージョンをアップグレードしたり、特定のソフトウェア オプション（Cisco Unified Communications オペレーティング システム ロケール インストーラ、ダイヤル プラン、TFTP サーバ ファイルなど）をインストールできます。

[インストール/アップグレード（Install/Upgrade）] メニュー オプションで、ローカル ディスクまたはリモート サーバからシステム ソフトウェアをアップグレードできます。アップグレードしたソフトウェアは非アクティブなパーティションにインストールされ、その後でシステムの再起動とパーティションの切り替えができます。これにより、システムで新しいソフトウェア バージョンが実行されます。詳細については、『*Upgrade Guide for the Cisco Unified Communications Manager*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html）を参照してください。

（注） Cisco Unified Communications オペレーティング システムのインターフェイスと CLI に含まれるソフトウェア アップグレード機能を使用して、すべてのソフトウェアのインストールとアップグレードを実行する必要があります。このシステムでアップロードおよび処理できるソフトウェアは、シスコによって承認されたものだけです。サードパーティー製または Windows ベースのソフトウェア アプリケーションはインストールまたは使用できません。

サービス

このアプリケーションでは、次のオペレーティング システムユーティリティを使用できます。

- ping：他のネットワーク デバイスとの接続を確認します。
- リモート サポート：シスコのサポート担当者がシステムへのアクセスに使用できるアカウントを設定します。このアカウントは、指定した日数が経過すると自動的に失効します。

CLI

CLI には、オペレーティング システムからアクセスすることも、サーバへのセキュア シェル接続を使用してアクセスすることもできます。詳細については、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』（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。

認証済み Network Time Protocol のサポート

Cisco Unified Communications Manager リリース 12.0(1) では、Unified Communications Manager の認証済み Network Time Protocol（NTP）機能がサポートされています。このサポートは、Unified Communications Manager へのセキュアな NTP サーバ接続を確立するために追加されています。以前のリリースでは、NTP サーバに対する Unified Communications Manager の接続はセキュアではありませんでした。

この機能は、対称キーベースの認証に基づいており、NTPv3 および NTPv4 サーバによってサポートされています。Unified Communications Manager は、SHA1 ベースの暗号化のみをサポートしています。SHA1 ベースの対称キーのサポートは、NTP バージョン 4.2.6 以降で利用できます。

- 対称キー
- 認証なし

NTP サーバの認証ステータスは、**Cisco Unified OS の管理**アプリケーションの管理 CLI または [NTPサーバの一覧（NTP Server List）] ページで確認できます。

自動キー認証済み Network Time Protocol のサポート

Cisco Unified Communications Manager は、自動キー機能（公開キー インフラストラクチャベースの認証）による Network Time Protocol（NTP）認証もサポートしています。この機能は、パブリッシャ ノードでのみ適用できます。

RedHat は自動キーよりも対称キー認証を推奨しています。詳細については、https://access.redhat.com/support/cases/#/case/01871532を参照してください。

この機能は、コモン クライテリア認定のために PKI ベースの認証が必須であるため追加されました。

Cisco Unified Communication Manager でコモン クライテリア モードを有効にしている場合にのみ、NTP サーバで IFF ID スキームによる PKI ベースの認証を設定できます。

Cisco Unified Communications Manager で、対称キーまたは PKI ベースの NTP 認証を有効にできます。

PKI 対応サーバで対称キーを有効にしようとすると、次の警告メッセージが表示されます。

警告 Autokeyを使用したNTP認証が現在有効になっており、対称キーを有効にする前に無効にする必要があります。（NTP authentication using Autokey is currently enabled and must be disabled before the symmetric key is enabled.）コマンド「utils ntp auth auto-key disable」を使用してNTP認証を無効にしてから、このコマンドを再試行してください。（Use the command 'utils ntp auth auto-key disable' to disable NTP authentication, then retry this command.）

対称キー対応サーバで Autokey を有効にしようとすると、次の警告メッセージが表示されます。

警告 対称キーを使用するNTP認証が現在有効になっており、Autokeyを有効にする前に無効にする必要があります。（NTP authentication using symmetric key is currently enabled and must be disabled before Autokey is enabled.）コマンド「utils ntp auth symmetric-key disable」を使用してNTP認証を無効にしてから、このコマンドを再試行してください。（Use the command 'utils ntp auth symmetric-key disable' to disable NTP authentication, then retry this command.）

（注） NTP サーバには ntp バージョン 4 と rpm バージョン ntp-4.2.6p5-1.el6.x86_64.rpm 以上が必要です。

NTP サーバの認証ステータスは、Cisco Unified OS の管理アプリケーションの管理 CLI または [NTPサーバの一覧(NTP Server List)] ページで確認できます。

Cisco Unified Serviceability の概要

Cisco Unified Serviceability は、管理者がシステムを管理する際の、サービス、アラーム、支援ツールのホストを提供する、Web ベースのトラブルシューティング ツールです。Cisco Unified Serviceability が提供する機能を利用して、管理者は以下の作業を行うことができます。

- サービスの開始と停止：管理者はシステムを管理する上で役立つさまざまなサービスを設定できます。たとえば、Cisco CallManager Serviceability RTMT サービスを開始することにより、管理者は Real-Time Monitoring Tool を使ってシステムの正常性をモニタできます。
- SNMP：アプリケーション層プロトコルである SNMP を使用すると、ノードやルータなどのネットワーク デバイス間の管理情報を簡単に交換できます。TCP/IP プロトコル スイートの一部である SNMP を使用すると、管理者はリモートでネットワークのパフォーマンス

を管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。

- アラーム：アラームは、システムの実行時のステータスと状態に関する情報を提供するため、システムに関する問題をトラブルシューティングできます。
- トレース：トレース ツールは、音声アプリケーションの問題をトラブルシューティングするのに役立ちます。
- Cisco Serviceability Reporter：Cisco Serviceability Reporter は、Cisco Unified Serviceability 内で日次レポートを生成します。
- SNMP：アプリケーション層プロトコルである SNMP を使用すると、ノードやルータなどのネットワーク デバイス間の管理情報を簡単に交換できます。TCP/IP プロトコル スイートの一部である SNMP を使用すると、管理者はリモートでネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。
- CallHome：Cisco Unified Communications Manager の Call Home 機能を設定し、Cisco Unified Communications Manager が通信し、診断アラート、インベントリおよびその他のメッセージを Smart Call Home バックエンド サーバに送信できるようにします。

その他の管理インターフェイス

Cisco Unified Serviceability を使用して、サービスを開始し以下の他の管理インターフェイスを使用できます。

- Real-Time Monitoring Tool：Real-Time Monitoring Tool は、システムの正常性をモニタするために利用できる Web ベースのインターフェイスです。RTMT を使用して、アラームやカウンタを確認したり、システムの正常性に関する詳細情報が記載されたレポートを表示したりできます。
- Dialed Number Analyzer：Dialed Number Analyzer は、管理者がダイヤル プランの問題をトラブルシューティングする際に役立つ、Web ベースのインターフェイスです。
- Cisco Unified CDR Analysis and Reporting：CDR Analysis and Reporting は、システムで行われたコールの詳細を記録したレコードを収集します。

Cisco Unified Serviceability の使用方法の詳細については、『*Cisco Unified Serviceability Administration Guide*』（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。

Cisco Unified Reporting の概要

Cisco Unified Reporting Web アプリケーションは、クラスタ データをトラブルシューティングまたは検査するための統合レポートを生成します。このアプリケーションには、Unified

Communications Manager および Unified Communications Manager IM and Presence Service のコンソールでアクセスできます。

このツールは、クラスタデータのスナップショットを簡単に作成する方法を提供します。このツールは、既存のソースからのデータの収集、データの比較、および異常の報告を行います。Cisco Unified Reporting で生成されるレポートは、1 台以上のサーバの 1 つ以上のソースからのデータを 1 つの出力ビューに統合します。システムを管理する際には、たとえば以下のレポートを表示して利用できます。

- [Unified CM クラスタ概要（Unified CM Cluster Overview）]：Cisco Unified Communications Manager and IM and Presence Service のバージョン、サーバのホスト名、ハードウェアの詳細といったクラスタのスナップショットを取得するときに、このレポートを参照します。
- [電話機機能リスト（Phone Feature List）]：機能を設定する際は、このレポートを表示します。このレポートは、どの電話機がどの Unified Communications Manager 機能をサポートしているかを一覧します。
- [回線未使用の Unified CM 電話（Unified CM Phones Without Lines）]：電話回線を使用していない、クラスタ内の電話機を確認するには、このレポートを表示します。

Cisco Unified Reporting が提供するレポートをすべて網羅したリスト、およびこのアプリケーションの使用方法については、『*Cisco Unified Reporting Administration Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

ディザスタ リカバリ システムの概要

ディザスタ リカバリ システム（DRS）は、[Cisco Unified Communications Manager 管理（Cisco Unified Communications Manager Administration）] から呼び出すことができるシステムで、完全なデータ バックアップおよび復元の機能を提供します。ディザスタ リカバリ システムでは、定期的にスケジュールされた自動データ バックアップまたはユーザ起動のデータ バックアップを実行できます。

DRS は、プラットフォームのバックアップ/復元の一環として、独自の設定（バックアップ デバイス設定およびスケジュール設定）を復元します。DRS は `drfDevice.xml` ファイルと `drfSchedule.xml` ファイルをバックアップおよび復元します。これらのファイルとともにサーバを復元するときは、DRS バックアップ デバイスおよびスケジュールを再設定する必要がありません。

ディザスタ リカバリ システムには、次の機能があります。

- バックアップおよび復元タスクを実行するためのユーザ インターフェイス。
- バックアップおよび復元機能を実行するための分散システム アーキテクチャ。
- バックアップのスケジューリング。
- 物理的なテープ ドライブまたはリモート SFTP サーバへのバックアップのアーカイブ。

一括管理ツールの概要

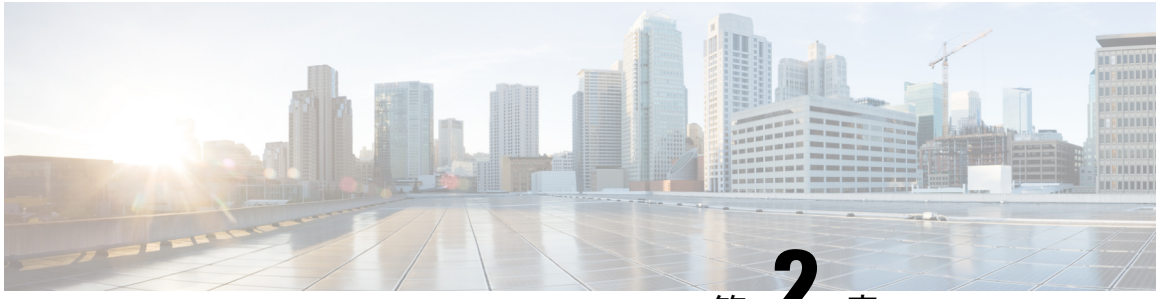
Cisco Unified Communications Manager 内にエンティティを設定するには、Unified CM の管理の [一括管理（Bulk Administration）] メニューおよびサブメニュー オプションで一括管理ツールを使用します。

Unified Communications Manager の一括管理ツール（BAT）は Web ベースのアプリケーションであり、管理者が Unified Communications Manager データベースに対する一括トランザクションを行うために使用できます。BAT では、多数の同じような電話、ユーザ、またはポートを同時に追加、更新、削除できます。Cisco Unified CM の管理を使用する場合、データベース トランザクションごとに個々の手動操作が必要になりますが、BAT はこのプロセスを自動化し、追加、更新、削除の操作を短時間で実行できるようにします。

以下のタイプのデバイスとレコードを処理する場合は BAT を使用できます。

- Cisco IP Phone、ゲートウェイ、電話機、Computer Telephony Interface（CTI）ポート、H.323 クライアントの追加、更新、削除
- ユーザ、ユーザ デバイス プロファイル、Cisco Unified Communications Manager Assistant マネージャおよびアシスタントの追加、更新、削除
- 強制承認コードとクライアント マター コードの追加、削除
- コール ピックアップ グループの追加、削除
- リージョン マトリクスの実装、実装解除
- アクセス リストの挿入、削除、エクスポート
- リモート宛先およびリモート宛先プロファイルの挿入、削除、エクスポート
- インフラストラクチャ デバイスの追加

一括管理ツールの使用方法の詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。



第 2 章

使用する前に

管理インターフェイスへのログイン

システム内の管理インターフェイスのいずれかにサインインする場合に、次の手順を使用します。

手順

ステップ 1 ご使用の Web ブラウザで、Unified Communications Manager インターフェイスを開きます。

ステップ 2 [ナビゲーション（Navigation）] ドロップダウン リストから管理インターフェイスを選択します。

ステップ 3 [移動（Go）] をクリックします。

ステップ 4 ユーザ名とパスワードを入力します。

ステップ 5 [ログイン（Login）] をクリックします。

管理者またはセキュリティ パスワードのリセット

管理者パスワードを消失し、システムにアクセスできない場合は、次の手順を使用してパスワードをリセットします。

始める前に

- この手順を実行するノードに物理的にアクセスできる必要があります。

- どの時点でも、CD または DVD メディアを挿入するように求められたら、VMWare サーバ用の vSphere クライアントを用いて ISO ファイルをマウントする必要があります。指示については、「『Adding DVD or CD Drives to a Virtual Machine』」 https://www.vmware.com/support/ws5/doc/ws_disk_add_cd_dvd.htmlを参照してください。
- セキュリティ パスワードは、クラスタ内のすべてのノードで一致している必要があります。セキュリティパスワードは、すべてのマシン上で変更してください。変更していない場合、クラスタ ノードが通信不能になります。

手順

ステップ 1 次のユーザ名とパスワードを使用して、パブリッシャ ノードで CLI にサインインします。

a) ユーザ名：**`pwrecovery`**

b) パスワード：**`pwreset`**

ステップ 2 何かキーを押して続行します。

ステップ 3 ディスク ドライブに有効な CD または DVD が入っている場合、または ISO ファイルをマウントしてある場合は、VMWare クライアントから取り出します。

ステップ 4 何かキーを押して続行します。

ステップ 5 有効な CD または DVD をドライブに挿入するか、ISO ファイルをマウントします。

（注） このテストでは、データ専用のディスクまたはISOファイルを使用する必要があります。

ステップ 6 最後のステップが確認されると、次のいずれかのオプションを入力して続行するように指示されます。

- **a** を入力して、管理者パスワードをリセットする。
- セキュリティ パスワードをリセットする場合は、**s** を入力します。

（注） セキュリティパスワードを変更したら、クラスタ内の各ノードをリセットする必要があります。ノードをリブートしない場合、システム サービスで問題が発生するほか、サブスクライバ サーバ上の管理ウィンドウで問題が発生します。

ステップ 7 新しいパスワードを入力し、確認のためにもう一度入力します。

管理者のクレデンシャルは、先頭がアルファベットで 6 文字以上必要です。英数字、ハイフン、およびアンダースコアを使用できます。

ステップ 8 新しいパスワードの強度が検証された後、パスワードがリセットされ、任意のキーを押してパスワード リセット ユーティリティを終了するように指示されます。

異なる管理者パスワードを設定する場合は、CLI コマンド **set password** を使用します。詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』（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。

システムのシャットダウンまたは再起動

設定を変更した後などにシステムをシャットダウンまたは再起動する必要がある場合、次の手順を使用します。

始める前に

仮想マシンからサーバのシャットダウンおよび再起動が強制されると、ファイルシステムが破損する可能性があります。強制シャットダウンを回避します。代わりに、この手順の実行後または CLI からの **utils system shutdown** の実行後に、サーバが適切にシャットダウンするまで待ちます。

手順

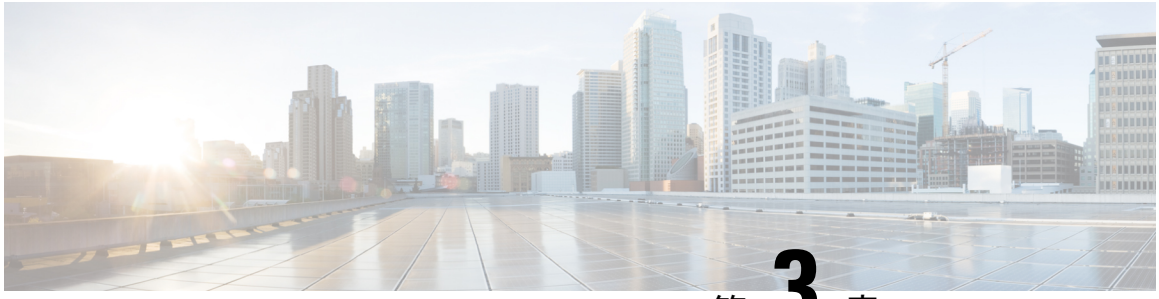
ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から、**[設定（Settings）]** > **[バージョン（Version）]** を選択します。

ステップ 2 次のいずれかの操作を実行します。

- すべてのプロセスを停止し、システムをシャットダウンするには、[シャットダウン（Shutdown）] をクリックします。
- すべてのプロセスを停止し、システムを再起動するには、[再起動（Restart）] をクリックします。

第 II 部

ユーザの管理



第 3 章

ユーザ アクセスの管理

ユーザ アクセスの概要

Cisco Unified Communications Manager に対するユーザ アクセスは、次の項目をエンド ユーザに割り当てることで管理できます。

- ロール
- アクセスコントロールグループ
- ユーザ ランク

ロール、アクセス コントロール グループ、ユーザ ランク コントロールでは、Cisco Unified Communications Manager に対する複数レベルのセキュリティを提供します。各ロールでは、Cisco Unified Communications Manager 内の特定のリソースに対する一連の権限を定義します。アクセス コントロール グループにロールを割り当て、そのアクセス コントロール グループにエンド ユーザを割り当てると、それらのエンド ユーザにそのロールで定義されているすべてのアクセス権限を付与することになります。

ユーザ ランク フレームワークはロールとアクセス コントロール グループ フレームワークをオーバーレイして、エンドユーザが使用可能なグループを決定します。エンドユーザとアプリケーション ユーザは、それぞれのユーザ ランクで許可されるアクセス コントロール グループにのみ割り当てることができます。

ロールの概要

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

各ロールには、特定のリソースまたはアプリケーションに接続される一連の権限が含まれます。たとえば、標準 CCM エンドユーザのロールは、そのロールが割り当てられているユーザに、Cisco Unified Communications セルフ ケア ポータルへのアクセス権を提供します。

また、Cisco Unified Communications Manager の管理、Cisco CDR Analysis and Reporting、Dialed Number Analyzer、CTI インターフェイスなどのリソースへのアクセスを提供するロールを割り当てることもできます。

特定の設定ウィンドウのようなグラフィカル ユーザ インターフェイスを使用する大部分のリソースでは、ロールに接続された権限によって、そのウィンドウのデータ、または関連するウィンドウのグループ内のデータを閲覧したり更新できます。

ロールの設定と割り当て

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

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

権限のタイプ

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

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

エンドユーザ ロールと管理者ロール

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

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

高度なロール設定

カスタマイズされたロールを作成する際に、[アプリケーションユーザ（Application User）] と [エンドユーザ（End User）] 設定ウィンドウで選択されたフィールドに、詳細レベルの制御を追加できます。

[高度なロール設定（Advanced Role Configuration）] ページでは、システムへのアクセスを許可する際に、以下に示すようなタスクへのアクセスを制限できます。

- ユーザの追加
- パスワードの編集
- ユーザ ランクの編集
- アクセス コントロール グループの編集

次の表では、この設定で適用できる制御について詳しく説明します。

表 *1*: 高度なリソース アクセス情報

高度なリソース	アクセス制御
権限情報	アクセス制御グループを追加または編集する機能を次のように制御します。 • [ビュー（View）] : ユーザは、アクセス制御グループを表示することはできますが、追加、編集、または削除することはできません。 • [更新（Update）] : ユーザは、アクセス制御グループを追加、編集、または削除できます。 （注） 両方の値が選択されていないと、[権限情報（Permission Information）] セクションは使用できません。

高度なリソース	アクセス制御
ユーザ ランク	ユーザ ランクを変更する機能を制御します。 • [ビュー（View）] : ユーザは、ユーザ ランクを表示できますが、変更することはできません。 • [更新（Update）] : ユーザはユーザ ランクを変更できます。 （注） 両方の値が選択されていないと、[ユーザ ランク（User Rank）] セクションは使用できません。
新しいユーザの追加	新しいユーザを追加する機能を次のように制御します。 • [はい（Yes）] : ユーザは、新しいユーザを追加できます。 • [いいえ（No）] : [新規追加（Add New）] ボタンは使用できません。
パスワード	パスワードを変更する機能を制御します。 • [はい（Yes）] : ユーザは [アプリケーション ユーザ情報（Application User Information）] セクションでユーザのパスワードを変更できます。 • [いいえ（No）] : [アプリケーションユーザ情報（Application User Information）] セクションで、[パスワード（Password）] と [パスワードの確認（Confirm Password）] は使用できません。

関連トピック

標準権限とアクセス コントロール グループ （34 ページ）

アクセス コントロール グループの概要

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

アクセス コントロール グループは、エンドユーザとアプリケーション ユーザのリストです。類似したアクセスの必要性を共有するエンド ユーザとアプリケーション ユーザに、必要な権限と役割を含むアクセス コントロール グループを指定できます。アクセス コントロール グループに割り当てられるエンドユーザやアプリケーションのユーザは、そのアクセス コントロール グループの最小ランク要件を満たす必要があります。たとえば、4 のユーザ ランクを持つユーザは、最小ランク要件が 4 ～ 10 のアクセス コントロール グループにしか割り当てることができません。

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

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

関連トピック

標準権限とアクセス コントロール グループ （34 ページ）

ユーザ ランクの概要

ユーザ ランクのアクセス コントロールでは、管理者がエンド ユーザやアプリケーション ユーザに提供できるアクセス レベルに対する一連の制御を行います。[ユーザ ランク（User Rank）] パラメータは 1 ～ 10 の整数で指定し、一番高いランクは 1 です。ユーザ ランクはユーザとアクセス コントロール グループの両方に割り当てられるため、特定のアクセス コントロール グループに割り当て可能なユーザを決定するランク階層が作成されます。

エンド ユーザやアプリケーション ユーザをプロビジョニングする場合、管理者は各ユーザのユーザ ランクを割り当てる必要があります。管理者は、各アクセス コントロール グループにもユーザ ランクを割り当てる必要があります。管理者は、同じランクや下のランクのアクセス コントロール グループにのみユーザを割り当てることができます。たとえば、あるエンドユーザのユーザ ランクが 3 の場合、3 ～ 10 のユーザ ランクが設定されているアクセス コントロール グループに割り当てることができます。そのユーザを、ユーザ ランクが 1 である必要があるアクセス コントロール グループに割り当てることはできません。

管理者は、[ユーザ ランクの設定（User Rank Configuration）] ウィンドウ内でユーザ ランクの階層をカスタマイズして、それらのランクをエンド ユーザ、アプリケーション ユーザ、アクセス コントロール グループに割り当てることができます。

ユーザ アクセスの前提条件

新しい役割またはアクセス コントロール グループを作成する前に、システムにあらかじめインストールされている標準権限およびアクセス コントロール グループを確認して、既存のアクセス コントロール グループにユーザに必要な権限とアクセス許可が含まれているかどうかを確認します。

詳細については、標準権限とアクセス コントロール グループ （34 ページ）を参照してください。

ユーザ アクセス設定のタスク フロー

次のタスクを実行して、ユーザ アクセスを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	カスタムユーザ ランクの作成 （21 ページ）	カスタム ユーザ ランクを作成して、ユーザ ランク階層を設定します。
ステップ 2	次のいずれかの方法で新しいロールを作成します。 • カスタム ロールの作成 （22 ページ） • 権限のコピー （23 ページ）	新しいロールを最初から作成して設定するには、[作成（Create）] 手順を使用します。 新しいロールが標準ロールと同様の設定を持つ場合は、[コピー（Copy）] コマンドを使用します。既存の標準ロールから新しいロールに権限設定をコピーできます。続けて、新しいロールの設定を編集できます。
ステップ 3	次のいずれかの方法でアクセス コントロール グループを作成します。 • アクセス コントロール グループの作成 （24 ページ） • アクセス コントロール グループのコピー （24 ページ）	新しいアクセス コントロール グループを作成して設定するには、[作成（Create）] 手順を使用します。 新しいアクセス コントロール グループがデフォルト グループのいずれかとよく似ている場合は、[コピー（Copy）] コマンドを使用できます。既存のグループから新しいグループにロールの割り当てをコピーして、編集できます。
ステップ 4	アクセス コントロール グループへの権限の割り当て （25 ページ）	ロールを追加または削除して、アクセス コントロール グループに割り当てられたロールを更新します。
ステップ 5	アクセス コントロール グループへのユーザの割り当て （26 ページ）	ユーザを追加したり削除して、アクセス コントロール グループのユーザ リストを更新します。グループに割り当てられているすべてのユーザは、グループに割り当てられているロールに設定されている権限を継承します。
ステップ 6	ユーザ権限レポートの表示 （27 ページ）	これはオプションです。ユーザに割り当てられているアクセス権限を確認する必要がある場合は、そのユーザの権限レポートを表示します。
ステップ 7	アクセス コントロール グループの重複する特権ポリシーの設定 （28 ページ）	これはオプションです。Cisco Unified Communications Manager がアクセス コントロール グループの割り当てにより発生する可能性がある、ユーザ権限の重

	コマンドまたはアクション	目的
		複を処理する方法を設定します。これにより、エンド ユーザが複数のアクセス コントロール グループに割り当てられ、ロールや権限の設定に不整合が生まれる状況に対処できます。
ステップ 8	カスタム ヘルプ デスク ロールの作成タスク フロー （28 ページ）	これはオプションです。企業によっては、ヘルプ デスク担当者に特定の管理タスクを実行できる権限を与える必要があると考えている場合があります。電話機の追加やエンド ユーザの追加などのタスクをヘルプ デスク チームのメンバーが実行できるようにする、ヘルプ デスク チームのメンバー用のロールとアクセス コントロール グループを設定します。
ステップ 9	アクセス コントロール グループの削除（31 ページ）	これはオプションです。システムからアクセス コントロール グループを削除する必要がある場合に、この手順を使用します。

カスタム ユーザ ランクの作成

ランク階層を目的として、カスタム ユーザ ランクを作成するには、次の手順を使用します。

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

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

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

ステップ 5 **[保存（Save）]** をクリックします。

カスタム ロールの作成

カスタム権限を作成し、その権限の特権を設定するには、次の手順を実行します。システムで定義された標準権限に、ユーザに割り当てようとする特権と一致する権限がない場合、カスタム権限を作成できます。

手順

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

ステップ 2 [アプリケーション（Application）] ドロップダウンリストボックスから、この権限を関連付けるアプリケーションを選択します。
[権限の設定（Role Configuration）] ウィンドウが表示されます。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 [名前（Name）] テキストボックスに、権限の名前を入力します。

名前は、128 文字まで入力できます。使用できる文字は、英字、数字、ダッシュ（-）、ピリオド、スペース、およびアンダースコアです。

ステップ 5 [説明（Description）] テキストボックスに、権限の説明を入力します。

説明は 128 文字以内にする必要があります。

ステップ 6 新しい権限が各リソースに対して持つ特権を次のように編集します。

- 権限がそのリソースを表示できるようにするには、[読み取り（Read）]チェックボックスをクリックします。
- 権限がそのリソースを編集できるようにするには、[更新（Update）] チェックボックスをクリックします。
- 権限がそのリソースを表示および編集できるようにするには、[読み取り（Read）] と [更新（Update）] の両方のチェックボックスをオンにします。
- 権限に、リソースへのどのようなアクセスも許可しない場合は、両方のチェックボックスをオフのままにします。

ステップ 7 この権限のページに表示されるすべてのリソースに特権を付与する場合は、[すべてにアクセス権を付与（Grant access to all）] ボタンをクリックし、すべてのリソースから特権を削除する場合は、[すべてにアクセスを許可しない（Deny access to all）] をクリックします。

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

ステップ 8 [保存（Save）] をクリックします。

次のタスク

新しいアクセス コントロール グループを設定するには、次のいずれかの手順を実行します。

- アクセス コントロール グループの作成 （24 ページ）
- アクセス コントロール グループのコピー （24 ページ）

権限のコピー

新しい権限に標準権限の設定をコピーして、新しい権限を作成するには、次の手順を実行します。Cisco Unified Communications Manager では、標準権限の特権を編集できませんが、自分が作成した権限の特権は編集できます。

手順

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

ステップ 2 [検索（Find）] をクリックし、コピーするリソースと特権がある権限を選択します。

ステップ 3 [コピー（Copy）] をクリックします。

ステップ 4 新しい権限の名前を入力し、[OK] をクリックします。
[権限の設定（Role Configuration）] ウィンドウに新しい権限の設定が表示されます。新しい権限の特権は、コピーした権限の特権と同じです。

ステップ 5 新しい権限のリソースのいずれかで、次のように特権を編集します。

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

ステップ 6 [保存（Save）] をクリックします。

次のタスク

ユーザに権限を割り当てるには、新しいアクセスコントロールグループを作成し、そのグループに権限を割り当てる必要があります。新しいアクセス コントロール グループを作成するには、次の手順のいずれかを実行します。

- アクセス コントロール グループの作成 （24 ページ）
- アクセス コントロール グループのコピー （24 ページ）

アクセス コントロール グループの作成

新しいアクセス コントロール グループを作成するには、この手順を実行します。

始める前に

アクセス コントロール グループを既存のグループと同様の設定にする場合は、Copy コマンドを使用して、既存のグループの設定を作成した新しいグループにコピーできます。

アクセス コントロール グループのコピー （24 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）] > [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 [新規追加（Add New）] をクリックします。

ステップ 3 [名前（Name）] にアクセス コントロール グループの名前を入力します。

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

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

アクセス コントロール グループへの権限の割り当て （25 ページ）

アクセス コントロール グループのコピー

既存のアクセス コントロール グループから、編集できる新しいグループにロールの設定をコピーして、新しいアクセス コントロール グループを作成するには、次のタスクを実行します。

手順

ステップ 1 Cisco Unified CM の管理で、**[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）] をクリックして、設定をコピーする対象のアクセス コントロール グループを選択します。

ステップ 3 [コピー（Copy）] をクリックします。

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

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

ステップ 6 [保存（Save）] をクリックします。

次のタスク

アクセスコントロールグループに割り当てられたロールを確認し、編集する必要がある場合：

アクセス コントロール グループへの権限の割り当て （25 ページ）

アクセス コントロール グループへの権限の割り当て

アクセス コントロール グループに権限を割り当てるには、次の手順を使用します。既存のグループからアクセス コントロール グループの設定をコピーした場合、権限の削除が必要になることもあります。

管理者などのフル アクセスできるユーザは、アクセス コントロール グループへの権限の割り当てまたは削除ができます。権限を割り当てられたアクセス コントロール グループは、その権限に含まれるすべてのリソースにアクセスできます。

（注） アクセス コントロール グループに権限を割り当てるときには、そのアクセス コントロール グループに Standard Unified CM Admin Users 権限を割り当てる必要があります。この権限により、ユーザは Cisco Unified CM の管理にログインできます。

始める前に

新しいアクセスコントロールグループを作成するには、次のタスクのいずれかを実行します。

- アクセス コントロール グループのコピー （24 ページ）
- アクセス コントロール グループの作成 （24 ページ）

手順

ステップ 1 **[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）]** の順に選択します。

[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 2 [検索（Find）] をクリックし、権限を割り当てるアクセス コントロール グループを選択します。
[アクセス コントロール グループの設定（Access Control Group Configuration）] ウィンドウが開きます。

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

[権限の割り当て（Role Assignment）] ペインが表示されます。

ステップ 4 アクセス コントロール グループに新しい権限を追加するには、次の手順を実行します。

a) [グループに権限を割り当て（Assign Role to Group）] をクリックします。
b) [検索（Find）] をクリックし、権限の一覧を検索します。
c) アクセス コントロール グループに追加する権限を選択します。
d) [選択項目の追加（Add Selected）] をクリックします。
新しい権限が、[権限（Role）] リスト ボックスに表示されます。

ステップ 5 割り当てた権限を、アクセス コントロール グループから削除するには、次の手順を実行します。

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

ステップ 6 [保存（Save）] をクリックします。

権限の割り当ては、データベースのアクセス コントロール グループに追加されます。

次のタスク

アクセス コントロール グループへのユーザの割り当て （26 ページ）

アクセス コントロール グループへのユーザの割り当て

新規ユーザを割り当てるか既存ユーザを削除することによってアクセス コントロール グループのエンド ユーザまたはアプリケーション ユーザのリストを更新するには、このタスクを実行します。

（注） ユーザのランクがアクセス コントロール グループの最低ユーザ ランクと同じかそれより上のユーザのみを追加できます。

始める前に

アクセス コントロール グループへの権限の割り当て （25 ページ）

手順

ステップ 1 **[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）]** の順に選択します。

[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 2 [検索（Find）] をクリックして、ユーザ リストを更新するアクセス コントロール グループを選択します。

ステップ 3 [検索（Find）] をクリックして、ユーザ リストを表示します。

ステップ 4 エンド ユーザまたはアプリケーション ユーザをアクセス コントロール グループに追加するには、次の手順を実行します。

a) [エンド ユーザをアクセス コントロール グループに追加（Add End Users to Access Control Group）] または [アプリケーション ユーザをアクセス コントロール グループに追加（Add App Users to Access Control Group）] をクリックします。

b) 追加するユーザを選択します。

c) [選択項目の追加（Add Selected）] をクリックします。

ステップ 5 アクセス コントロール グループからユーザを削除するには、次の手順を実行します。

a) 削除するユーザを選択します。

b) [選択項目の削除（Delete Selected] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

これはオプションです。特定のエンド ユーザまたはアプリケーション ユーザのユーザ特権レポートを表示する必要がある場合は、次を参照してください。

- ユーザ権限レポートの表示 （27 ページ）

ユーザ権限レポートの表示

既存のエンドユーザや既存のアプリケーションユーザのユーザ権限レポートを表示するには、次の手順を実行します。ユーザ権限レポートは、エンド ユーザまたはアプリケーション ユーザに割り当てられたアクセス制御グループ、ロール、およびアクセス権限が表示されます。

手順

ステップ 1 Cisco Unified CM の管理で、次の手順のいずれかを実行します。

- エンド ユーザの場合は、**[ユーザの管理（User Management）]** > **[エンド ユーザ（End User）]**を選択します。
- アプリケーション ユーザの場合は、**[ユーザの管理（User Management）]** > **[アプリケーション ユーザ（Application User）]**を選択します。

ステップ 2 [検索（Find）] をクリックして、アクセス権限を表示するユーザを選択します。

ステップ 3 [関連リンク（Related Links）] ドロップダウン リストから [ユーザ権限レポート（User Privilege Report ）] を選択し、[移動（Go）] をクリックします。
[ユーザ権限（User Privilege）] ウィンドウが表示されます。

アクセス コントロール グループの重複する特権ポリシーの設定

Cisco Unified Communications Manager がアクセス コントロール グループの割り当てにより発生する可能性がある、ユーザ権限の重複を処理する方法を設定します。これにより、エンドユーザが複数のアクセス コントロール グループに割り当てられ、ロールや権限の設定に不整合が生まれる状況に対処できます。

手順

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

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

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

ステップ 3 **[保存（Save）]** をクリックします。

カスタム ヘルプ デスク ロールの作成タスク フロー

企業によっては、ヘルプデスク担当者に特定の管理タスクを実行できる権限を与える必要があると考えている場合があります。このタスク フロー内の手順に従って、電話機の追加やエンドユーザの追加などのタスクをヘルプ デスク チームのメンバーが実行できるようにする、ヘルプ デスク チームのメンバー用のロールとアクセス コントロール グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	カスタム ヘルプ デスク権限の作成 （29 ページ）	ヘルプ デスク チームのメンバーのカスタム ロールを作成し、新しい電話機の追加や新しいユーザの追加などの項目のロール権限を割り当てます。

	コマンドまたはアクション	目的
ステップ 2	カスタム ヘルプ デスク アクセス コントロール グループの作成 （30 ページ）	ヘルプ デスク ロール用の新しいアクセス コントロール グループを作成します。
ステップ 3	アクセス コントロール グループへのヘルプ デスク ロールの割り当て （30 ページ）	ヘルプ デスク アクセス コントロール グループにヘルプ デスク ロールを割り当てます。このアクセス コントロール グループに割り当てられたユーザには、ヘルプ デスク ロールの権限が割り当てられます。
ステップ 4	アクセス コントロール グループへのヘルプ デスク メンバーの割り当て （31 ページ）	カスタム ヘルプ デスク ロールの権限をヘルプ デスク チームのメンバーに割り当てます。

カスタム ヘルプ デスク権限の作成

この手順を実行して、組織内のヘルプ デスク メンバーに割り当てることができるカスタム ヘルプ デスク権限を作成します。

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [アプリケーション（Application）] ドロップダウン リストから、この権限に割り当てるアプリケーションを選択します。たとえば、[Cisco CallManager Administration] 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 新しい権限の [名前（Name）] を入力します。たとえば、**`Help Desk`** です。

ステップ 6 [読み込みおよび更新権限（Read and Update Privileges）] の下で、ヘルプ デスク ユーザに割り当てる権限を選択します。たとえば、ヘルプ デスク メンバーがユーザおよび電話を追加できるようにする場合は、[ユーザ（User）] Web ページと [電話（Phone）] Web ページの [読み込み（Read）] および [更新（Update）] チェック ボックスをオンにします。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

カスタム ヘルプ デスク アクセス コントロール グループの作成 （30 ページ）

カスタム ヘルプ デスク アクセス コントロール グループの作成

始める前に

カスタム ヘルプ デスク権限の作成 （29 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[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）]** の順に選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 アクセス コントロール グループの名前を入力します。たとえば、「**`Help_Desk`**」と入力します。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

アクセス コントロール グループへのヘルプ デスク ロールの割り当て （30 ページ）

アクセス コントロール グループへのヘルプ デスク ロールの割り当て

次の手順を実行して、ヘルプ デスク ロールからの権限を持つヘルプ デスク アクセス コントロール グループを設定します。

始める前に

カスタム ヘルプ デスク アクセス コントロール グループの作成 （30 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[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、ヘルプ デスク用に作成したアクセス コントロール グループを選択します。
[アクセス コントロール グループの設定（Access Control Group Configuration）] ウィンドウが開きます。

ステップ 3 [関連リンク（Related Links）] ドロップダウン リスト ボックスで、[アクセス コントロール グループに権限を割り当て（Assign Role to Access Control Group）] オプションを選択し、[移動（Go）] をクリックします。
[権限の検索/一覧表示（Find and List Roles）] ポップアップが表示されます。

ステップ 4 [グループに権限を割り当て（Assign Role to Group）] ボタンをクリックします。

ステップ 5 [検索（Find）] をクリックし、ヘルプ デスク ロールを選択します。

ステップ 6 [選択項目の追加（Add Selected）] をクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

アクセス コントロール グループへのヘルプ デスク メンバーの割り当て （31 ページ）

アクセス コントロール グループへのヘルプ デスク メンバーの割り当て

始める前に

アクセス コントロール グループへのヘルプ デスク ロールの割り当て （30 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[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、作成したカスタム ヘルプ デスク アクセス コントロール グループを選択します。

ステップ 3 次のいずれかの手順を実行します。

- ヘルプ デスク チームのメンバーがエンドユーザとして設定されている場合は、[グループにエンド ユーザを追加（Add End Users to Group）] をクリックします。
- ヘルプ デスク チームのメンバーがアプリケーションユーザとして設定されている場合は、[グループにアプリケーション ユーザを追加（Add App Users to Group）] をクリックします。

ステップ 4 [検索（Find）] をクリックし、ヘルプ デスク ユーザを選択します。

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

ステップ 6 [保存（Save）] をクリックします。
Cisco Unified Communications Manager が、作成したカスタム ヘルプ デスク ロールの権限をヘルプ デスク チームのメンバーに割り当てます。

アクセス コントロール グループの削除

アクセス コントロール グループ全体を削除するには、次の手順を使用します。

始める前に

アクセス コントロール グループを削除すると、Cisco Unified Communications Manager がデータベースからすべてのアクセス コントロール グループ データを削除します。アクセス コントロール グループを使用しているロールが判明していることを確認します。

手順

ステップ 1 **[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）]** の順に選択します。

[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 2 削除するアクセス コントロール グループを検索します。

ステップ 3 削除するアクセス ポイント グループの名前をクリックします。

選択したアクセス コントロール グループが表示されます。このアクセス コントロール グループ内のユーザがアルファベット順に一覧表示されます。

ステップ 4 アクセス コントロール グループ全体を削除するには、[削除（Delete）] をクリックします。

アクセス コントロール グループを削除すると元に戻せないことを警告するダイアログボックスが表示されます。

ステップ 5 アクセス コントロール グループを削除するには、[OK] をクリックします。アクションをキャンセルするには、[キャンセル（Cancel）] をクリックします。[OK] をクリックすると、Cisco Unified Communications Manager がデータベースからアクセス コントロール グループを削除します。

既存の OAuth 更新トークンの取り消し

既存の OAuth 更新トークンを取り消すには、AXL API を使用します。たとえば、ある従業員が退社した場合、この API を使用してその従業員の現在の更新トークンを取り消し、その従業員が新しいアクセス トークンを取得したり、企業アカウントへログインできないようにすることができます。API は、AXL クレデンシャルで保護されている REST ベースの API です。任意のコマンドライン ツールを使用して API を呼び出すことができます。次のコマンドは、更新トークンを取り消すために使用できる cURL コマンドの例を示しています。

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

引数の説明

- `admin:password` は、Cisco Unified Communications Manager の管理者アカウントのログイン ID とパスワードです。
- `UCMaddress` は、Cisco Unified Communications Manger のパブリッシャ ノードの FQDN または IP アドレスです。
- `end_user` は、更新トークンを取り消すユーザのユーザ ID です。

非アクティブなユーザ アカウントの無効化

Cisco Database Layer Monitor サービスを使用して非アクティブなユーザ アカウントを無効にするには、次の手順を実行します。

Cisco Database Layer Monitor は、指定日数内に Cisco Unified Communications Manager にログインしていない場合、スケジュールされたメンテナンス タスク時にユーザ アカウント ステータスを非アクティブに変更します。無効にされたユーザは、その後の監査ログで自動的に監査対象になります。

始める前に

Cisco Database Layer Monitor サービスで選択したサーバの [メンテナンス時間（Maintenance Time）]を入力します（**[システム]** > **[サービス パラメータ]**）。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[システム]** > **[サービス パラメータ]** の順に選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リスト ボックスから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 ボックスから [Cisco Database Layer Monitor] パラメータを選択します。

ステップ 4 [Advanced] をクリックします。

ステップ 5 [この期間未使用のユーザ アカウントを無効化する（Disable User Accounts unused for（days））] フィールドに、日数を入力します。たとえば、90 とします。システムはこの入力された値を、非アクティブとしてアカウントの状態を宣言するためのしきい値として使用します。自動無効化をオフにするには、値を 0 と入力します。

（注） これは必須フィールドです。デフォルトおよび最小値は 0 で、単位は日数です。

ステップ 6 **[保存（Save）]** をクリックします。
非アクティブなまま設定された日数（たとえば 90 日間）が経過すると、ユーザは無効になります。監査ログにエントリが作成され、次のメッセージが表示されます。「`<userID>`ユーザは非アクティブとマークされています（<userID> user is marked inactive）」。

リモート アカウントの設定

シスコ サポートがトラブルシューティングのためにご使用のシステムに一時的にアクセスできるよう、Unified Communications Manager でリモート アカウントを設定します。

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、**[サービス（Services）]** > **[リモート サポート（Remote Support）]** を選択します。

ステップ 2 [アカウント名（Account Name）] フィールドに、リモート アカウントの名前を入力します。

ステップ 3 [アカウントの有効期限（Account Duration）] フィールドに、アカウントの有効期限を日数で入力します。

ステップ 4 **[保存（Save）]** をクリックします。
システムは、暗号化パス フレーズを生成します。

ステップ 5 シスコのサポート担当者に連絡して、リモート サポート アカウント名とパス フレーズを提供します。

標準権限とアクセス コントロール グループ

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

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

表 *2:* 標準権限、特権、およびアクセス コントロール グループ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス コントロール グループ
標準 AXL API アクセス	AXL データベース API へのアクセスを許可します。	標準 CCM スーパー ユーザ
標準 AXL API ユーザ	AXL API を実行するログイン権限を付与します。	
標準 AXL 読み取り専用 API アクセス	AXL 読み取り専用 API（API の一覧表示、API の取得、SQL Query API の実行）の実行をデフォルトで許可します。	
標準管理 Rep Tool 管理	Cisco Unified Communications Manager CDR Analysis and Reporting（CAR）の表示および設定が可能になります。	標準 CAR 管理ユーザ、標準 CCM スーパー ユーザ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス コントロール グループ
標準監査ログ管理	監査ロギング機能の次のタスクを実行できます。 • Cisco Unified Serviceability の [監査ログ設定（Audit Log Configuration）] ウィンドウでの、監査ロギングの表示および設定 • Cisco Unified Serviceability でのトレースの表示と設定、および Real-Time Monitoring Tool の監査ログ機能向けトレースの収集 • Cisco Unified Serviceability の Cisco Audit Event Service の表示、開始、停止 • RTMT での、関連付けられたアラートの表示および更新	標準監査ユーザ
標準 CCM 管理ユーザ	Cisco Unified Communications Manager の管理へのログイン権限を付与します。	標準 CCM 管理ユーザ、標準 CCM ゲートウェイ管理、標準 CCM 電話管理、標準 CCM 読み取り専用、標準 CCM サーバ モニタリング、標準 CCM スーパー ユーザ、標準 CCM サーバ メンテナンス、標準 パケット スニファ ユーザ
標準 CCM エンドユーザ	Cisco Unified Communications セルフケアポータルにログインする権限をエンド ユーザに付与します。	標準 CCM エンドユーザ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス コントロール グループ

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

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

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス コントロール グループ

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

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

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス コントロール グループ

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

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス コントロール グループ

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

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス コントロール グループ
標準 CCM ユーザ権限管理	Cisco Unified Communications Manager の管理で、アプリケーションユーザの表示および設定ができます。	
標準 CCMADMIN 管理	CCMAdmin システムのすべての面を利用できます。	
標準 CCMADMIN 管理	Cisco Unified Communications Manager の管理および一括管理ツールのすべての項目を表示および設定できます。	標準 CCM スーパー ユーザ
標準 CCMADMIN 管理	Dialed Number Analyzer の情報を表示および設定できます。	
標準 CCMADMIN 読み取り専用	すべての CCMAdmin リソースの読み取りを許可します。	
標準 CCMADMIN 読み取り専用	Cisco Unified Communications Manager の管理および一括管理ツールの項目を表示できます。	標準 CCM ゲートウェイ管理、標準 CCM 電話管理、標準 CCM 読み取り専用、標準 CCM サーバ メンテナンス、標準 CCM サーバ モニタリング
標準 CCMADMIN 読み取り専用	Dialed Number Analyzer で、ルーティング設定の分析ができます。	
標準 CCMUSER 管理	Cisco Unified Communications セルフケアポータルへのアクセスを許可します。	標準 CCM エンド ユーザ
標準 CTI 通話モニタリング許可	CTI アプリケーションまたはデバイスでコールをモニタできます。	標準 CTI 通話モニタリング許可
標準 CTI コール パーク モニタリング許可	CTI アプリケーションまたはデバイスでコールパークをモニタできます。	標準 CTI コール パーク モニタリング許可
標準 CTI 通話録音許可	CTI アプリケーション/デバイスで通話を録音できます。	標準 CTI 通話録音許可
標準 CTI 発信者番号の変更許可	CTI アプリケーションが発信者番号を通話中に変更できます。	標準 CTI 発信者番号の変更許可
標準 CTI によるすべてのデバイスの制御	CTI で制御可能なすべてのデバイスを制御できます。	標準 CTI によるすべてのデバイスの制御

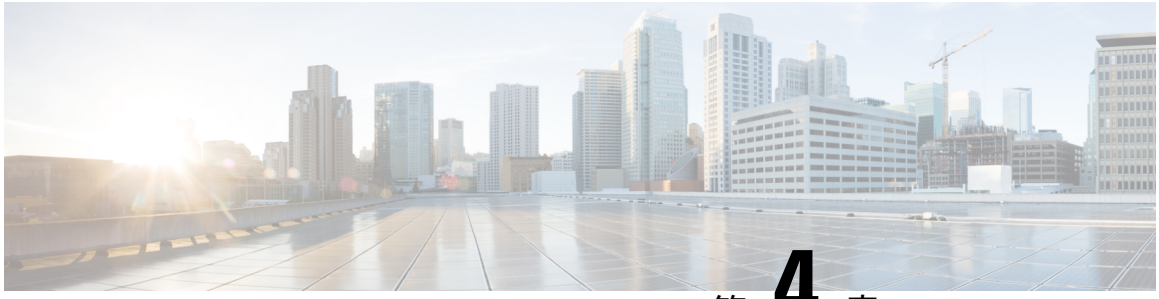
標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス コントロール グループ
標準 CTI 接続された転送と会議をサポートする電話の制御許可	接続された転送および会議をサポートするすべての CTI デバイスを制御できます。	標準 CTI 接続された転送と会議をサポートする電話の制御許可
標準 CTI ロールオーバー モードをサポートする電話の制御許可	ロールオーバーモードをサポートするすべての CTI デバイスを制御できます。	標準 CTI ロールオーバー モードをサポートする電話の制御許可
標準 CTI SRTP 重要素材の受信許可	CTI アプリケーションが、SRTP を使う重要な素材にアクセスしたり、その素材を配信したりできるようにします。	標準 CTI SRTP 重要素材の受信許可
標準 CTI 対応	CTI アプリケーションの制御を可能にします。	標準 CTI 対応
標準 CTI セキュア接続	Cisco Unified Communications Manager へのセキュアな CTI 接続が可能になります。	標準 CTI セキュア接続
標準CUReporting	アプリケーションユーザが、さまざまなソースからレポートを作成できます。	
標準CUReporting	Cisco Unified Reporting での、レポートの表示、ダウンロード、作成、およびアップロードができます。	標準 CCM 管理ユーザ、標準 CCM スーパー ユーザ
標準 EM 認証プロキシ権限	アプリケーションで使用する Cisco Extension Mobility（EM）の認証権限を管理します。この権限は、（Cisco Unified Communications Manager Assistant や Cisco Web Dialer などの）Cisco Extension Mobility と対話するすべてのアプリケーションユーザに必要です。	標準 CCM スーパー ユーザ、標準 EM 認証プロキシ権限
標準パケット スニッフィング	Cisco Unified Communications Manager の管理にアクセスし、パケット スニッフィング（キャプチャ）ができます。	標準パケット スニファ ユーザ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス コントロール グループ
標準 RealtimeAndTraceCollection	Cisco Unified Serviceability および Real-Time Monitoring Tool にアクセスし、次の項目を表示および使用できます。 • Simple Object Access Protocol（SOAP）Serviceability AXL API • SOAP コール レコード API • SOAP 診断ポータル（Analysis Manager）データベース サービス • 監査ログ機能のトレースの設定 • トレース収集などの、Real-Time Monitoring Tool の設定	標準 RealtimeAndTraceCollection

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

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

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス コントロール グループ
標準 CCMADMIN 読み取り専用	すべての CCMAdmin リソースの読み取りを許可します。	標準 Cisco Unified CM IM およびプレゼンスの管理
標準 CUReporting	アプリケーションユーザが、さまざまなソースからレポートを作成できます。	標準 Cisco Unified CM IM およびプレゼンスのレポーティング



第 4 章

エンド ユーザの管理

エンド ユーザの概要

稼働中のシステムを管理する際に、システム内に設定済みのエンドユーザのリストを更新しなければならない場合があります。次の作業が含まれます。

- 新しいユーザの設定
- 新しいエンド ユーザの電話機の設定
- エンド ユーザのパスワードまたは PIN の変更
- IM and Presence Service に対するエンド ユーザの有効化

Cisco Unified CM の管理の [エンド ユーザの設定（End User Configuration）] ウィンドウで、Unified CM エンド ユーザに関する情報を追加、検索、表示、保守できます。また、[ユーザ/電話のクイック追加（Quick User/Phone Add）] ウィンドウを使用して、新規エンドユーザとそのエンド ユーザの新規電話を迅速に設定することもできます。

エンド ユーザ管理タスク

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザ テンプレートの設定 （48 ページ）	ユニバーサル回線テンプレートとデバイス テンプレートを含むユーザ プロファイルまたは機能グループ テンプレートを使用してシステムを設定していない場合は、次のタスクを実行してセットアップします。

	コマンドまたはアクション	目的
		これらのテンプレートを新しいエンドユーザに適用することにより、新しいユーザと電話機を簡単に設定できます。
ステップ 2	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 （53 ページ） • エンド ユーザの手動追加 （54 ページ）	システムが設定済みであり会社の 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。 まだ設定していない場合は、エンドユーザを手動で追加して設定できます。
ステップ 3	次のタスクのどちらかを実行することにより、新しい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 （55 ページ） • エンド ユーザへの既存の電話機の移動 （56 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」手順に従って、すでに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 4	エンド ユーザ PIN の変更 （57 ページ）	（オプション）Cisco Unified Communications Manager Administration でエンド ユーザの PIN を変更する。
ステップ 5	エンド ユーザ パスワードの変更 （57 ページ）	（オプション）Cisco Unified Communications Manager Administration でエンド ユーザのパスワードを変更する。
ステップ 6	Cisco Unity Connection ボイス メールボックスの作成 （58 ページ）	（オプション）Cisco Unified Communications Manager Administration で個別の Cisco Unity Connection ボイス メールボックスを作成する。

ユーザ テンプレートの設定

次のタスクを実行して、ユーザプロファイルおよび機能グループテンプレートを設定します。新しいエンド ユーザを追加したら、回線およびデバイス設定を使用してすばやくエンド ユーザを設定し、エンド ユーザの電話を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	ユニバーサル回線テンプレートの設定（49 ページ）	電話番号に一般的に適用される共通設定を使用して、ユニバーサル回線テンプレートを設定します。
ステップ 2	ユニバーサル デバイス テンプレートの設定 （50 ページ）	電話に一般的に適用される共通設定を使用して、ユニバーサル デバイス テンプレートを設定します。
ステップ 3	ユーザ プロファイルの設定 （50 ページ）	ユニバーサル回線テンプレートとユニバーサル デバイス テンプレートをユーザ プロファイルに割り当てます。セルフプロビジョニング機能を設定している場合は、このプロファイルを使用するユーザに対してセルフプロビジョニングを有効化できます。
ステップ 4	機能グループ テンプレートの設定 （52 ページ）	機能グループ テンプレートにユーザ プロファイルを割り当てます。LDAP 同期ユーザの場合は、機能グループ テンプレートによってユーザ プロファイル設定がエンドユーザに関連付けられます。

ユニバーサル回線テンプレートの設定

電話番号に通常適用される共通設定をユニバーサル回線テンプレートに設定します。1 つまたは複数のユニバーサル回線テンプレートを作成して、自分の組織で最も一般的な電話番号設定を反映した設定セットを作成できます。さらに、ユーザ プロファイルによって、ユーザにプロビジョニングする新しい電話番号にこれらの設定を適用できます。

ユニバーサル回線テンプレートはコピー機能をサポートしています。既存のテンプレートをコピーして新しいテンプレートを作成し、いくつかのマイナーなサイト固有の変更を加えて保存できます。

手順

ステップ 1 Cisco Unified CM の管理で、**[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサル回線テンプレート（Universal Line Template）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [ユニバーサル回線テンプレートの設定（Universal Line Template Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

ユニバーサル デバイス テンプレートの設定 （50 ページ）

ユニバーサル デバイス テンプレートの設定

ユニバーサル デバイス テンプレートを設定します。ユニバーサル デバイス テンプレートには、通常、電話、リモート接続先プロファイル、またはエクステンションモビリティプロファイルに適用される、一連の共通設定が含まれます。組織内で最も共通するデバイス設定を反映した 1 つまたは複数のユニバーサル デバイス テンプレートを作成できます。また、ユーザ プロファイルを通じて、エンドユーザ用にプロビジョニングを行う新しいデバイスのすべてにこれらの設定を適用できます。

ユニバーサル デバイス テンプレートはコピー機能をサポートしています。既存のテンプレートをコピーして新しいテンプレートを作成し、いくつかのマイナーなサイト固有の変更を加えて保存できます。

始める前に

ユニバーサル回線テンプレートの設定 （49 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[ユーザの管理（User Management）]** > **[ユーザ/電話の追加（User/Phone Add）]** > **[ユニバーサル デバイス テンプレート（Universal Device Template）]** を選択します。

ステップ 2 **[新規追加（Add New）]** をクリックします。

ステップ 3 [ユニバーサル デバイス テンプレートの設定（Universal Device Template Configuration）] ウィンドウの各フィールドに入力します。フィールドの説明については、オンラインヘルプを参照してください。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

ユーザ プロファイルの設定 （50 ページ）

ユーザ プロファイルの設定

プロファイルを使用するユーザに割り当てる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 テンプレートを含むユーザ プロファイルを設定します。このサービス プロファイルを使用するユーザに対してセルフ プロビジョニングを有効にすることもできます。

始める前に

ユニバーサル デバイス テンプレートの設定 （50 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザ プロファイル（User Profile）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 ユーザ プロファイルの [名前（Name）] および [説明（Description）] を入力します。

ステップ 4 [ユニバーサル デバイス テンプレート（Universal Device Template）] を、ユーザの [デスク フォン（Desk Phones）] 、[モバイルおよびデスクトップ デバイス（Mobile and Desktop Devices）] 、および [リモート接続先/デバイス プロファイル（Remote Destination/Device Profiles）] に割り当てます。

ステップ 5 [ユニバーサル回線テンプレート（Universal Line Template）] をこのユーザ プロファイルのユーザの電話回線に適用するために割り当てます。

ステップ 6 このユーザプロファイルのユーザに自分の電話をプロビジョニングするセルフプロビジョニング機能の使用を許可するには、次の手順を実行します

a) [自分の電話のプロビジョニングをエンドユーザに許可（Allow end user to provision their own phones）]チェックボックスをオンにします。

b) [エンド ユーザのプロビジョニングする電話数を制限（Limit Provisioning once End User has this many phones）] フィールドに、ユーザがプロビジョニングできる電話の最大数を入力します。最大値は 20 です。

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

（注） デフォルトでは、このチェックボックスはオンです。このチェックボックスをオフにすると、[Jabber ポリシー（Jabber Policies）] セクションが無効になり、サービス クライアント ポリシー オプションは、デフォルトで選択されません。

（注） この設定は、Cisco Jabber ユーザの場合にのみ必須です。非 Jabber ユーザは、この設定がなくても MRA を使用できます。MRA 機能は、Jabber MRA ユーザにのみ適用され、他のエンドポイントまたはクライアントには適用されません。

ステップ 8 このユーザ プロファイルに Jabber ポリシーを割り当てます。[Jabber デスクトップ クライアント ポリシー（Jabber Desktop Client Policy）] および [Jabber モバイル クライアント ポリシー（Jabber Mobile Client Policy）] 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。

- [サービスなし（No Service）] : このポリシーはすべての Jabber サービスへのアクセスを無効にします。
- [IM & Presence のみ（IM & Presence only）] : このポリシーは、インスタント メッセージとプレゼンス機能だけを有効にします。

- [IM とプレゼンス、音声とビデオ コール（IM & Presence, Voice and Video calls）]：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 ユーザ用 Cisco Jabber および Mac ユーザ用 Cisco Jabber が含まれています。Jabber モバイル クライアントには、iPad および iPhone ユーザ用 Cisco Jabber および Android ユーザ用 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。

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。

次のタスク

機能グループ テンプレートの設定 （52 ページ）

機能グループ テンプレートの設定

機能グループテンプレートには、共通の回線、デバイス、および機能設定のセットが含まれています。新しいユーザに機能グループテンプレートを適用すると、その回線、デバイス、および機能設定が、ユーザの電話および電話回線に適用されます。機能グループテンプレートは、プロビジョニングされたユーザの電話、回線、および機能を非常に迅速に設定できるようにすることで、システムの導入をサポートします。

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/電話の追加（User/Phone Add）] > [機能グループ テンプレート（Feature Group Template）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 このテンプレートを使用するすべてのユーザのホーム クラスタとしてローカル クラスタを使用する場合は、[ホーム クラスタ（Home Cluster）] チェック ボックスをオンにします。

ステップ 4 このテンプレートを使用するユーザがインスタントメッセージおよびプレゼンス情報を交換できるようにするには、[Unified CM IM and Presenceのユーザを有効化（Enable Users for Unified CM IM and Presence）] チェックボックスをオンにします。

ステップ 5 ドロップダウン メニューから、[サービス プロファイル（Service Profile）] および [ユーザ プロファイル（User Profile）] を選択します。

ステップ 6 [機能グループ テンプレートの設定（Feature Group Template Configuration）] ウィンドウの残りのフィールドに入力します。フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

新規エンド ユーザを追加します。システムが会社の LDAP ディレクトリと統合されている場合は、LDAP ディレクトリから直接ユーザをインポートできます。そうでない場合は、手動でエンド ユーザを作成します。

- LDAP からのエンド ユーザのインポート （53 ページ）
- エンド ユーザの手動追加 （54 ページ）

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 （55 ページ）
- エンド ユーザへの既存の電話機の移動 （56 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。

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 の管理で、**[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（User ID）] と [姓（Last Name）] 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（Save）]** 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 ボックスで、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 （オプション）[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（Save）]** 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 （55 ページ）
- エンド ユーザへの既存の電話機の移動 （56 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 （54 ページ）
- LDAP からのエンド ユーザのインポート （53 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[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）] ドロップダウンで、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。

次のタスク

すでに設定済みの既存の電話機を割り当てるには、以下の手順を実行します。

エンド ユーザへの既存の電話機の移動 （56 ページ）

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。

始める前に

エンド ユーザ用の新しい電話機の追加 （55 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[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。

エンド ユーザ PIN の変更

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** を選択します。
[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 2 既存のユーザを選択するには、[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、[検索（Find）] をクリックしてユーザのリストを取得した後、リストからユーザを選択します。
[エンド ユーザ設定（End User Configuration）] ウィンドウが表示されます。

ステップ 3 [PIN] フィールドで、暗号化された既存の PIN をダブルクリックして、新しい PIN を入力します。割り当てられている資格情報ポリシーに指定されている文字数以上（1 ～ 127 文字）を入力する必要があります。

ステップ 4 [PIN の確認（Confirm PIN）] フィールドで、既存の暗号化された PIN をダブルクリックし、もう一度、新しい PIN を入力します。

ステップ 5 [保存（Save）] をクリックします。

（注） Cisco Unity Connection の [アプリケーション サーバの設定（Application Server Configuration）] ウィンドウで [エンド ユーザ PIN の同期（End User Pin synchronization）] チェック ボックスが有効になっている場合は、エクステンション モビリティ、開催中の会議、モバイル コネクト、および Cisco Unity Connection ボイスメールに同じエンド ユーザ PIN を使用してログインできます。エンド ユーザは、同じ PIN を使用して、エクステンションモビリティにログインし、自分のボイスメールにアクセスできます。

エンド ユーザ パスワードの変更

LDAP 認証が有効になっている場合は、エンド ユーザ パスワードを変更できません。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** を選択します。
[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 2 既存のユーザを選択するには、[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、[検索（Find）] をクリックしてユーザのリストを取得した後、リストからユーザを選択します。
[エンド ユーザ設定（End User Configuration）] ウィンドウが表示されます。

ステップ 3 [パスワード（Password）] フィールドで、暗号化された既存のパスワードをダブルクリックして、新しいパスワードを入力します。割り当てられている資格情報ポリシーに指定されている文字数以上（1 ～ 127 文字）を入力する必要があります。

ステップ 4 [パスワードの確認（Confirm Password）] フィールドで、既存の暗号化されたパスワードをダブルクリックし、もう一度、新しいパスワードを入力します。

ステップ 5 **[保存（Save）]** をクリックします。

Cisco Unity Connection ボイス メールボックスの作成

始める前に

- Cisco Unified Communications Manager をボイス メッセージング用に設定する必要があります。Cisco Unity Connection を使用するように Cisco Unified Communications Manager を設定する方法については、次で『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

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

- デバイスとプライマリ内線番号をエンド ユーザに関連付ける必要があります。

- このセクションで説明する手順を実行する代わりに、Cisco Unity Connection で使用可能なインポート機能を使用できます。インポート機能の使用方法については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』を参照してください

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** を選択します。
[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 2 既存のユーザを選択するには、[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、[検索（Find）] をクリックしてユーザのリストを取得した後、リストからユーザを選択します。

[エンド ユーザ設定（End User Configuration）] ウィンドウが表示されます。

ステップ 3 プライマリ内線番号がこのユーザに関連付けられていることを確認します。

（注） プライマリ内線番号を定義する必要があります。そうしなかった場合は、[関連リンク（Related Links）] ドロップダウン リストに Cisco Unity ユーザ リンクが表示されません。

ステップ 4 [関連リンク（Related Links）] ドロップダウン リストで、[Cisco Unity ユーザの作成（Create Cisco Unity User）] リンクを選択してから、[移動（Go）] をクリックします。

[Cisco Unity ユーザの追加（Add Cisco Unity User）] ダイアログボックスが表示されます。

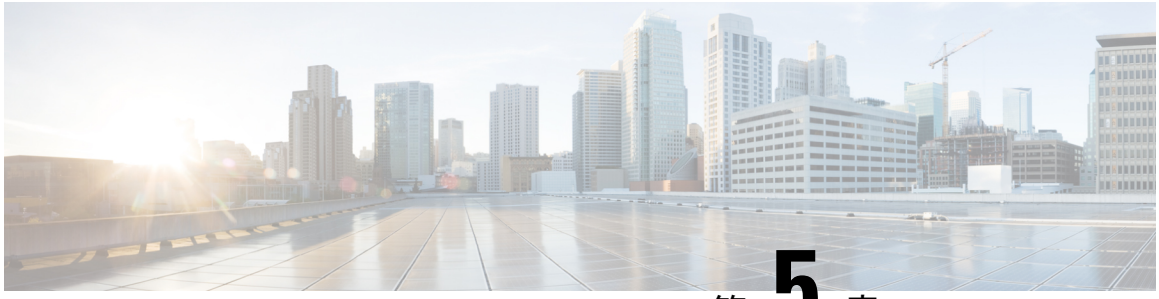
ステップ 5 [アプリケーション サーバ（Application Server）] ドロップダウン リストで、Cisco Unity Connection ユーザを作成する Cisco Unity Connection サーバを選択してから、[次へ（Next）] をクリックします。

ステップ 6 [サブスクライバ テンプレート（Subscriber Template）] ドロップダウン リストで、使用するサブスクライバ テンプレートを選択します。

ステップ 7 **[保存（Save）]** をクリックします。

メールボックスが作成されます。[エンド ユーザの設定（End User Configuration）] ウィンドウの [関連リンク（Related Links）] ドロップダウンリスト内のリンクが [Cisco Unity ユーザの編集（Edit Cisco Unity User）] に変化します。これで、Cisco Unity Connection Administration で、作成したユーザを確認できます。

（注） Cisco Unity Connection ユーザと Cisco Unified Communications Manager エンド ユーザを統合した後は、[エイリアス（Alias）]（Cisco Unified CM の管理内のユーザ ID）、[名（First Name）]、[姓（Last Name）]、[内線番号（Extension）]（Cisco Unified CM の管理内のプライマリ内線番号）などの Cisco Unified CM の管理内のフィールドを編集できなくなります。これらのフィールドは、Cisco Unified CM の管理でしか更新できません。



第 5 章

アプリケーション ユーザの管理

アプリケーション ユーザの概要

Cisco Unified CM の管理の [アプリケーションユーザの設定（Application User Configuration）] ウィンドウで管理者は、Unified Communications Manager アプリケーション ユーザに関する情報を追加、検索、表示、および保守することができます。

Cisco Unified CM の管理には、デフォルトで以下のアプリケーション ユーザが設定されています。

- CCMAdministrator
- CCMSysUser
- CCMQRTSecureSysUser
- CCMQRTSysUser
- IPMASecureSysUser
- IPMASysUser
- WDSecureSysUser
- WDSysUser
- TabSyncSysUser
- CUCService

（注） Standard CCM Super Users グループの管理者ユーザは、Cisco Unified Communications Manager Administration、Cisco Unified Serviceability、および Cisco Unified Reporting のいずれかにシングル サインオンすることによって、このすべてのアプリケーションにアクセスできます。

アプリケーション ユーザのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	新規アプリケーション ユーザの追加 （62 ページ）	新しいアプリケーション ユーザを追加します。
ステップ 2	デバイスとアプリケーション ユーザの関連付け （63 ページ）	アプリケーション ユーザに関連付けるデバイスを割り当てます。
ステップ 3	Cisco Unity または Cisco Unity Connection への管理者ユーザの追加 （63 ページ）	Cisco Unity または Cisco Unity Connection に管理者ユーザとしてユーザを追加します。Cisco Unified CM の管理でアプリケーション ユーザを設定します。その後で、Cisco Unity または Cisco Unity Connection で、そのユーザの追加の設定を構成します。
ステップ 4	アプリケーション ユーザ パスワードの変更 （65 ページ）	アプリケーション ユーザ パスワードを変更します。
ステップ 5	アプリケーション ユーザ パスワード クレデンシャル情報の管理 （65 ページ）	関連する認証ルール、関連するクレデンシャル ポリシー、アプリケーション ユーザの直前のパスワード変更の時刻などのクレデンシャル情報を変更または表示します。

新規アプリケーション ユーザの追加

手順

ステップ 1 Cisco Unified CM の管理で、**[ユーザの管理（User Management）] > [アプリケーション ユーザ（Application User）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [アプリケーション 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 4 **[保存（Save）]** をクリックします。

次のタスク

デバイスとアプリケーション ユーザの関連付け （63 ページ）

デバイスとアプリケーション ユーザの関連付け

手順

ステップ 1 Cisco Unified CM の管理から、**[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。
[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 2 既存のユーザを選択するには、[次の条件でユーザを検索（Find User Where）] フィールドに適切なフィルタを指定し、[検索（Find）] を選択してユーザのリストを取得し、リストからユーザを選択します。

ステップ 3 [使用可能なデバイス（Available Devices）] リストで、アプリケーション ユーザに関連付けするデバイスを選択し、リストの下にある**下向き矢印**をクリックします。選択したデバイスが [制御対象のデバイス（Controlled Devices）] リストに移動します。

（注） 使用可能なデバイスのリストを制限するには、[別の電話を検索（Find more Phones）] ボタンまたは [別のルート ポイントを検索（Find more Route Points）] ボタンをクリックします。

ステップ 4 [別の電話を検索（Find more Phones）] ボタンをクリックすると、[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。検索を実行して、このアプリケーション ユーザに関連付ける電話機を検索します。

アプリケーション ユーザに割り当てるデバイスごとに、上記ステップを繰り返します。

ステップ 5 [別のルート ポイントを検索（Find more Route Points）] ボタンをクリックすると、[CTI ルート ポイントの検索/一覧表示（Find and List CTI Route Points）] ウィンドウが表示されます。検索を実行して、このアプリケーション ユーザに関連付ける CTI ルート ポイントを検索します。

アプリケーション ユーザに割り当てるデバイスごとに、上記ステップを繰り返します。

ステップ 6 **[保存（Save）]** をクリックします。

Cisco Unity または Cisco Unity Connection への管理者ユーザの追加

Cisco Unified Communications Manager と Cisco Unity Connection 7.x 以降を統合する場合は、このセクションで説明する手順を実行する代わりに、Cisco Unity Connection 7.x 以降で使用可能なインポート機能を使用できます。インポート機能の使用方法については、次で Cisco Unity Connection 7.x 以降の『*User Moves, Adds, and Changes* Guide』を参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html。

Cisco Unity または Cisco Unity Connection ユーザが Cisco Unified CM アプリケーション ユーザと統合されている場合は、フィールドを編集できません。これらのフィールドは、Cisco Unified Communications Manager Administration でしか更新できません。

Cisco Unity と Cisco Unity Connection は、Cisco Unified Communications Manager からのデータの同期をモニタします。ツール メニューの [Cisco Unity Administration] または [Cisco Unity Connection Administration] で同期時刻を設定できます。

始める前に

Cisco Unity または Cisco Unity Connection にプッシュする予定のユーザに適切なテンプレートが定義されていることを確認します

[Cisco Unity ユーザの作成（Create Cisco Unity User）] リンクは、適切な Cisco Unity または Cisco Unity Connection ソフトウェアがインストールされ、設定されている場合にのみ表示されます。Cisco Unity に関する『*Cisco Unified Communications Manager Integration Guide*』または Cisco Unity Connection に関する『*Cisco Unified Communications Manager SCCP Integration Guide*』を次で参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html。

手順

ステップ 1 Cisco Unified CM の管理から、**[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 既存のユーザを選択するには、[次の条件でユーザを検索（Find User Where）] フィールドに適切なフィルタを指定し、[検索（Find）] を選択してユーザのリストを取得し、リストからユーザを選択します。

ステップ 3 [関連リンク（Related Links）] ドロップダウン リストで、[Cisco Unity アプリケーション ユーザの作成（Create Cisco Unity Application User）] リンクを選択し、[移動（Go）] をクリックします。
[Cisco Unity ユーザの追加（Add Cisco Unity User）] ダイアログが表示されます。

ステップ 4 [アプリケーション サーバ（Application Server）] ドロップダウン リストで、Cisco Unity または Cisco Unity Connection ユーザを作成する Cisco Unity または Cisco Unity Connection サーバを選択し、[次へ（Next）] をクリックします。

ステップ 5 [アプリケーション ユーザ テンプレート（Application User Template）] ドロップダウン リストで、使用するテンプレートを選択します。

ステップ 6 **[保存（Save）]** をクリックします。
Cisco Unity または Cisco Unity Connection で管理者アカウントが作成されます。[アプリケーション ユーザの設定（Application User Configuration）] ウィンドウの [関連リンク（Related Links）] 内のリンクが [Cisco Unity ユーザの編集（Edit Cisco Unity User）] に変化します。これで、Cisco Unity Administration または Cisco Unity Connection Administration で作成したユーザを表示できるようになります。

アプリケーション ユーザ パスワードの変更

手順

ステップ 1 Cisco Unified CM の管理から、**[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。
[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 2 既存のユーザを選択するには、[次の条件でユーザを検索（Find User Where）] フィールドに適切なフィルタを指定し、[検索（Find）] を選択してユーザのリストを取得し、リストからユーザを選択します。
[アプリケーション ユーザの設定（Application User Configuration）] ウィンドウに、選択されたアプリケーション ユーザに関する情報が表示されます。

ステップ 3 [パスワード（Password）]フィールドで、既存の暗号化されたパスワードをダブルクリックし、新しいパスワードを入力します。

ステップ 4 [パスワードの確認（Confirm Password）] フィールドで、既存の暗号化されたパスワードをダブルクリックし、もう一度、新しいパスワードを入力します。

ステップ 5 **[保存（Save）]** をクリックします。

アプリケーション ユーザ パスワード クレデンシャル情報の管理

次の手順を実行して、アプリケーション ユーザ パスワードに関するクレデンシャル情報を管理します。これにより、パスワードのロック、パスワードへのクレデンシャル ポリシーの適用、最後に失敗したログイン試行時などの情報の表示などの管理業務を実行できます。

手順

ステップ 1 Cisco Unified CM の管理から、**[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。
[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 2 既存のユーザを選択するには、[次の条件でユーザを検索（Find User Where）] フィールドに適切なフィルタを指定し、[検索（Find）] を選択してユーザのリストを取得し、リストからユーザを選択します。
[アプリケーション ユーザの設定（Application User Configuration）] ウィンドウに、選択されたアプリケーション ユーザに関する情報が表示されます。

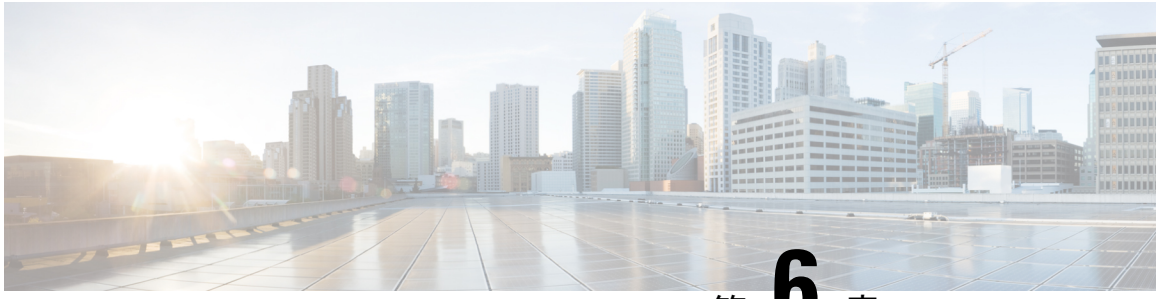
ステップ 3 パスワード情報を変更または表示するには、[パスワード（Password）] フィールドの横にある [クレデンシャルの編集（Edit Credential）] ボタンをクリックします。
ユーザの [クレデンシャル設定（Credential Configuration）] が表示されます。

ステップ 4 [クレデンシャル設定（Credential Configuration）] ウィンドウで、各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 いずれかの設定を変更した場合は、[保存（Save）] をクリックします。

第 III 部

デバイスの管理



第 6 章

電話の管理

電話管理の概要

この章では、ネットワーク内の電話を管理する方法について説明します。このトピックでは、新しい電話の追加、既存の電話の別のユーザへの移動、電話のロック、電話のリセットなどのタスクについて説明します。

ご使用の電話機モデルの『Cisco IP Phone Administration Guide』には、該当する電話機モデルに固有の設定情報が記載されています。

電話ボタン テンプレート

電話ボタン テンプレートは、電話機モデルに基づいて作成されます。一部の電話機モデルでは、特定の電話ボタンテンプレートを使用しませんが、一部電話機モデルには、個々のテンプレートまたはデバイスのデフォルトテンプレートのいずれかの特定されたテンプレートが必要です。

[エンタープライズ パラメータの設定（Enterprise Parameters Configuration）] ページの [非サイズ セーフ電話機の電話テンプレートの選択（Phone Template Selection for Non-Size Safe Phone）] と[自動登録レガシー モード（Auto Registration Legacy Mode）] エンタープライズ パラメータは、使用される電話ボタン テンプレートのタイプを指定します。フィールドの詳細については、オンライン ヘルプを参照してください。

表 *3:* さまざまなシナリオにおける電話ボタン テンプレート

非サイズ セーフ電話機の電話テンプレートの選択	自動登録レガシー モード	電話
個々のテンプレートの作成	False	ユニバーサルデバイス テンプレートからの電話を追加するときに、個々の電話ボタン テンプレートが作成されます。
デバイスのデフォルトからのテンプレートの使用	False	個々の電話ボタン テンプレートは作成されず、デバイスのデフォルトからの電話ボタン テンプレートを取得します。
デバイスのデフォルトからのテンプレートの使用	True	デバイス プール、電話テンプレート、コーリング サーチ スペース、電話ボタン テンプレートの値は、デバイスのデフォルトから取得されます。
個々のテンプレートの作成	True	デバイス プール、電話テンプレート、コーリング サーチ スペース、電話ボタン テンプレートの値は、デバイスのデフォルトから取得されます。 個々のテンプレートは作成されません。 自動登録レガシー モードには、優先度があります。

電話機管理タスク

手順

	コマンドまたはアクション	目的
ステップ 1	エンドユーザの有無にかかわらないテンプレートからの新しい電話機の追加 （72 ページ）	エンドユーザの有無にかかわらないユニバーサルデバイステンプレートからの新しい電話機の追加
ステップ 2	電話機の手動での追加 （71 ページ）	デバイステンプレートなしでのエンドユーザの新しい電話機の追加

	コマンドまたはアクション	目的
ステップ 3	エンドユーザがあるテンプレートからの新しい電話機の追加 （74 ページ）	エンドユーザ用の新しい電話機を追加して、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	既存の電話機の移動 （82 ページ）	設定された電話機を別のエンドユーザに移動します。
ステップ 5	現在ログイン中のデバイスの検索 （82 ページ）	特定のデバイスを検索するか、ユーザが現在ログインしているすべてのデバイスを列挙します。
ステップ 6	リモートでログイン中のデバイスの検索 （83 ページ）	特定のデバイスを検索するか、ユーザがリモートでログインしているすべてのデバイスを列挙します。
ステップ 7	電話機のリモート ロック （84 ページ）	一部の電話機は、リモートでロックすることができます。電話機をリモートでロックすると、ロックを解除するまで使用できなくなります。
ステップ 8	工場出荷時の初期状態への電話機のリセット （85 ページ）	電話機を工場出荷時の設定にリセットします。
ステップ 9	ロックされたデバイスまたはリセットされたデバイスの検索 （85 ページ）	リモートでロックされたデバイスまたはリモートでファクトリーデフォルト設定にリセットされたデバイスを検索します。
ステップ 10	電話の LSC ステータスの表示および CAPF レポートの生成 （86 ページ）	電話機で LSC 失効ステータスを検索し、CAPF レポートも生成します。

電話機の手動での追加

次の手順を実行して、ユーザ用の新しい電話機を手動で追加します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、**[デバイス（Device）] > [電話（Phone）] > [電話の検索とリスト（Find and List Phones）]** の順に選択します。

ステップ 2 [電話の検索とリスト（Find and List Phones）] ページから [新規追加（Add New）] をクリックして電話機を手動で追加します。

[新しい電話の追加（Add a New Phone）] ページが表示されます。

[新しい電話の追加（Add a New Phone）] ページから、[「ここをクリックしてユニバーサル デバイス テンプレートを追加（click here to add a new phone using a Universal Device Template）」] ハイパーリンクをクリックすると、ページは [新しい電話の追加（Add a New Phone）] ページにリダイレクトされ、ユーザの追加の有無にかかわらずテンプレートから電話を追加します。詳細については、エンドユーザの有無にかかわらないテンプレートからの新しい電話機の追加（72 ページ）を参照してください。

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、電話機モデルを選択します。

ステップ 4 [次へ（Next）] をクリックします。
[電話機の設定（Phone Configuration）] ページが表示されます。

ステップ 5 [電話機の設定（Phone Configuration）] ページで、必須フィールドに値を入力します。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。

[製品固有の設定（Product Specific Configuration）] 領域のフィールドの詳細については、ご使用の電話機モデルの『*Cisco IP Phone Administration Guide*』を参照してください。

ステップ 6 電話の設定を保存する場合は、[保存（Save）] をクリックします。

次のタスク

エンド ユーザへの既存の電話機の移動 （56 ページ）

エンドユーザの有無にかかわらないテンプレートからの新しい電話機の追加

次の手順を実行して、ユーザを追加するかどうかにかかわらず、テンプレートから新しい電話機を追加します。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

Cisco Unified Communications Manager でユニバーサル デバイス テンプレートが設定済みであることを確認します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、**[デバイス（Device）] > [電話（Phone）] > [電話の検索とリスト（Find and List Phones）]** の順に選択します。

ステップ 2 [電話の検索とリスト（Find and List Phones）] ページから、[テンプレートからの新規の追加（Add New From Template）] をクリックして、エンド ユーザの追加にかかわりなくデバイス テンプレートからの電話を追加します。

[新しい電話の追加（Add a New Phone）] ページが表示されます。

[新しい電話の追加（Add a New Phone）] ページから、[「ここをクリックしてすべての電話設定を手動で入力する（click here to enter all phone settings manually）」] ハイパーリンクをクリックすると、ページは電話を手動で追加できる既存の [新しい電話の追加（Add a New Phone）] ページにリダイレクトされます。詳細については、電話機の手動での追加 （71 ページ）を参照してください。

ステップ 3 [製品タイプ（およびプロトコル）（Phone Type (and Protocol)）] ドロップダウン リストで、電話機モデルを選択します。

プロトコルのドロップダウンリストは、電話が複数のプロトコルをサポートしている場合にのみ表示されます。

ステップ 4 [名前または MAC アドレス（Name or MAC Address）] テキスト ボックスに、名前または MAC アドレスを入力します。

ステップ 5 [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 テンプレートを選択します。

ステップ 6 [電話番号（回線1）（Directory Number (Line 1)）] ドロップダウンリストで、電話番号を選択します。

ドロップダウンリストのディレクトリ番号がドロップダウンリストの上限を越えている場合、[検索（Find）] タブが表示されます。[検索（Find）] をクリックすると、ディレクトリ番号の検索条件を示すポップアップ ダイアログボックスが開きます。

ステップ 7 （オプション）新しいディレクトリ番号を作成してデバイスに割り当てる場合には、[新規（New）] をクリックしてディレクトリ番号を入力し、ユニバーサル回線テンプレートを選択します。

[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）] に移動して、ユーザに関連付けられたディレクトリ番号を使用して電話を作成することもできます。

ステップ 8 （オプション）[ユーザ（User）] ドロップダウンリストから、新しい電話機を追加するエンドユーザを選択します。

（注） Cisco デュアル モード（モバイル）デバイスのユーザを選択する場合には必須です。

ドロップダウンリストのエンドユーザの数がドロップダウンリストの上限を越えている場合、[検索（Find）] タブが表示されます。[検索（Find）] をクリックすると、エンド ユーザ検索条件を示すポップアップ ダイアログボックスが開きます。

ステップ 9 [Add] をクリックします。

（注） 非サイズセーフ電話機の場合、電話テンプレートは [エンタープライズ パラメータの設定（Enterprise Parameters Configuration）] ページの [非サイズ セーフ電話機の電話テンプレートの選択（Phone Template Selection for Non-Size Safe Phone）] と [自動登録レガシー モード（Auto Registration Legacy Mode）] パラメータの選択に基づいて作成されます。

追加が成功したとのメッセージが表示されます。Cisco Unified Communications Manager で電話機が追加され、[電話の設定（Phone Configuration）] ページが表示されます。[電話の設定（Phone

Configuration）] ページの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。

次のタスク

エンド ユーザへの既存の電話機の移動 （56 ページ）

エンド ユーザがあるテンプレートからの新しい電話機の追加

次の手順を実行して、エンド ユーザ用の新しい電話機を追加します。

始める前に

電話機追加対象のエンド ユーザは、ユニバーサル デバイス テンプレートを含むユーザ プロファイルがセットアップされています。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。

- エンド ユーザ管理タスク （47 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[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）] ドロップダウンで、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。

コラボレーション モバイル コンバージェンス仮想デバイスの概要

CMC デバイスは、それに関連付けられたリモート接続先を表す仮想デバイスです。エンタープライズ電話で CMC デバイスにコールすると、コールはリモート接続先にリダイレクトされます。この機能は、デバイス タイプ [Collaboration モバイル コンバージェンス（Collaboration Mobile Convergence）] を作成することを目的としています。このデバイス タイプはいくつかのカスタマイズがされた Spark リモート デバイスと同じであり、以下の利点を提供します。

- Spark リモート デバイスと同様の機能を持つネイティブ モバイル デバイスを Cisco Unified Communications Manager 上でサポートします。
- 将来の開発機能パリティを含む機能を持つ Spark-RD として利用します。
- モバイルからデスクフォン、デスクフォンからモバイルへコールの移動などの、モバイル固有のユース ケースのカスタマイズができます。（ID ページで deskpickup タイマーを追加し、製品サポート機能の設定で有効にします）。
- CMC デバイスは、ハント グループに含めることができます。
- Spark リモート デバイスで共有回線に対応できます。
- ライセンス：ライセンス使用パースペクティブに応じて個別のデバイスとしてカウントします。複数デバイス ライセンス バンドルはいずれも、CMC RD をサポートする必要があります。

CMC RD デバイス ライセンスの調整

新しいCMCデバイスは、追加されると、ユーザに関連付けられているデバイスの数/タイプに基づいてライセンスを使用します。CMCデバイスによって使用されるライセンスのタイプは、それに関連付けられているエンド ユーザが所有するデバイスの数によって異なります。

- CMC デバイスのみを導入する場合は、拡張ライセンスを使用します。
- CMC デバイスと Spark RD を導入する場合は、拡張ライセンスを使用します。
- CMC と物理デバイス：拡張 Plus ライセンス
- CMC、Spark RD、および物理デバイスの場合：拡張 Plus ライセンス

Collaboration モバイル コンバージェンスの仮想デバイスを追加します。

エンド ユーザ用に Cisco Collaboration モバイル コンバージェンス（CMC）リモート デバイスを追加する次の手順を実行します。

始める前に

電話機追加対象のエンド ユーザは、ユニバーサル デバイス テンプレートを含むユーザ プロファイルがセットアップされている必要があります。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。

手順

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

ステップ 2 [新規追加（Add New）] ボタンをクリックします。

ステップ 3 [ここをクリックしてすべての電話設定を手動で入力する（Click here to enter all phone settings manually）] リンクをクリックします。
[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 4 [電話のタイプ（Phone Type）] ドロップダウン リストから、[Cisco Collaboration モバイル コンバージェンス（Cisco Collaboration Mobile Convergence）] を選択し、[次へ（Next）] をクリックします。
[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 5 [オーナーのユーザ ID（Owner User ID）] ドロップダウンから、デバイスを所有するエンドユーザを選択します。

ステップ 6 [デバイス プール（Device Pool）] ドロップダウンから、デバイス プールを選択します。

ステップ 7 [保存（Save）] をクリックします。
[設定の適用（Apply Config）] ボタンをクリックして変更を有効にすることを求める警告メッセージがポップアップします。[OK] をクリックします。デバイスは正常に追加されました。

ステップ 8 [電話番号（Directory Number）] を設定するには、追加された CMC デバイスをクリックし、[電話番号（Directory Number）] を入力して、[保存（Save）] をクリックします。

ステップ 9 追加された CMC デバイスの新しい [リモート接続先（Remote Destination）] を追加するには、アイデンティティ ボックス内のリンクをクリックします。

ステップ 10 [リモート接続先の設定（Remote Destination Configuration）] ウィンドウで、[名前（Name）]、[接続先の番号（Destination number）] をクリックして、[保存（Save）] をクリックします。

（注） 追加された 1 つの CMC デバイスに対して、1 つだけのリモート接続先を追加できます。

ステップ 11 既存のリモート接続先を更新するには、[新しい名前（New Name）] をクリックして、[保存（Save）] をクリックします。

ステップ 12 既存のリモート接続先を削除するには、メニューで [削除（Delete）] ボタンをクリックします。

永続的な削除を確認する Web ページからのメッセージが表示されます。[OK] をクリックします。

ステップ 13 [デバイス（Device）]ページからCMCデバイスを削除するには、[デバイス（Device）]チェック ボックスを選択し、メニューから [選択の削除（Delete Selected）] をクリックします。

CMC RD 機能の相互作用

表 *4 : CMC RD* 機能の相互作用

機能	データのやり取り
共有回線の処理	• CMC RD および Spark RD と関連付けられている共有デスク フォンがあるセットアップで、ユーザがエンタープライズ電話から CMC デバイス DN にコールすると、CMC RD、Spark RD、および共有デスク フォンの 3 つすべてが鳴ります。 • リモート接続先のいずれかから応答すると、共有デスク フォンに「リモートで使用中（Remote in Use）」メッセージが表示されます。 • 共有デスク フォンのいずれかから応答すると、両方のリモート接続先電話（CMC RD と Spark RD 電話）が切断されます。
Call Manager グループ（CMG）セットアップで動作する CMC デバイス	• CMC デバイスが Call Manager グループに関連付けられている場合は、必ずプライマリ サーバで実行され、プライマリ サーバがダウンした場合にのみ、Call Manager グループの次のアクティブなセカンダリ サーバで実行されます。 • プライマリ サーバがコール中にダウンした場合、進行中のコールは引き続き維持され、コールが終了した後にCMCデバイスがセカンダリ サーバに登録されます。 （注） コールが保持モードの場合、電話間のメディアは引き続きアクティブですが、コールの切断を除く他の操作は実行できません。 • 最初にプライマリ サーバがダウンし、CMCデバイスがセカンダリ サーバに登録されているときにコールが開始され、プライマリ サーバが進行中のコール中に起動した場合、コールは保持モードになり、コールの終了後にCMCデバイスがプライマリ サーバに登録されます。

機能	データのやり取り
コール アンカリング	CMCデバイスからのすべての基本着信コールおよび番号からリモート接続先へのコールは、エンタープライズ ネットワークでは固定されています。 CMCのリモートデバイスが設定されている場合、エンタープライズに固定されているすべてのコールにより、ユーザはモバイル デバイスからコールを発信および受信できます。 • ユーザは、エンタープライズ番号からCMCリモート宛先に直接ダイヤルすることができます。コールはエンタープライズ ネットワークでは固定されています。このシナリオでは、デスク フォン（CMCデバイスの共有回線）は鳴りませんが、[リモートで使用中（Remote in Use）] の状態のままになります。 • ユーザは、CMCリモート接続先から任意のエンタープライズ番号にダイヤルできます。コールは固定されています。このシナリオでは、デスク フォン（CMCデバイスの共有回線）は鳴りませんが、[リモートで使用中（Remote in Use）] の状態のままになります。
シングル ナンバー リーチ	• [リモート接続先の設定（Remote Destination configuration）] ページで、[シングル ナンバー リーチを有効にする（Enable Single Number Reach）] チェックボックスがオフになっている場合、コールは CMC RD まで拡張されず、拒否されます。 • リモート接続先からの着信コールと、[番号からリモート接続先へ（Number to Remote Destination）] の発信コールは、[シングル ナンバー リーチを有効にする（Enable Single Number Reach）] チェックボックスの選択に関係なく、影響を受けません。 • CMC デバイスがある共有デスク フォンがあり、[シングル ナンバー リーチを有効にする（Enable Single Number Reach）] チェックボックスがオフになっている場合、コールはCMC RD ではなく共有デスク フォンに拡張されます。

機能	データのやり取り
時刻（ToD）に基づくコール ルーティング	• リング スケジュールを設定するために、リモート接続先の [時刻（Time of Day）] 設定を使用できます（たとえば、月曜日から金曜日の 9 am ～ 5 pm などといった特定の時間を設定できます）。コールは、これらの時間にのみリモート接続先にリダイレクトされます。 エンタープライズ電話からCMC番号へのコールは、[リモート接続先の設定（Remote Destination configuration）] ページで修正されたリング スケジュールに基づいてルーティングされます。リング スケジュールは次のように指定できます。 • [すべての時間（All the Time）]：コールは常時ルーティングされます。制限はありません。 • [曜日（Day(s) of the week）]: 選択した特定の曜日にのみコールはルーティングされます。 • [特定の時間（Specific time）]：コールは選択した就業時間内にのみルーティングされます。必ずタイム ゾーンを選択します。 • リング スケジュール中にコールを受信する場合、エンタープライズ電話から CMC 番号へのコールは、[リモート接続先の設定（Remote Destination configuration）] ページでアクセス許可リストまたはアクセスブロッキング リストに追加されたコール番号またはパターンに基づいてルーティングされます。 • [アクセス許可リスト（Allowed access list）]：発信者番号またはパターンがアクセス許可リスト内にある場合にのみ接続先が鳴ります。 • [アクセス ブロッキング リスト（Blocked access list）]：発信者番号またはパターンがアクセス ブロッキング リスト内にある場合には接続先は鳴りません。 （注） 任意の時点で、アクセス許可リストまたはアクセス ブロッキング リストのみを使用できます。

機能	データのやり取り
ユーザ ロケールの設定	CMC 仮想デバイスでは、[電話の設定（Phone Configuration）] ウィンドウで設定されているロケール設定を使用して、電話のディスプレイと電話アナウンスのロケールを判断します。このポリシーは、通常のコールと Conference Now 番号に適用されます。 アナウンスの部分は、[ユーザ ロケール（User Locale）] の設定で同じ言語が選択された発信側（任意のエンタープライズ電話）および着信側（CMC デバイス）電話では、発信側とリモート接続先の両方のアナウンスは、[電話の設定（Phone Configuration）] ページで選択された [ユーザ ロケール（User Locale）] 設定に基づくものになります。 （注） たとえば、CMC デバイスに関連付けられている [リモート接続先（Remote Destination）] から [Conference Now 番号（Conference Now 番号）]に発信するときに、アナウンスは CMC デバイスの [電話の設定（Phone configuration）] ページで選択されている [ユーザ ロケール（User Locale）] の設定に基づくものになります。
HLogin および HLogout の新しいアクセス コード	この機能は、管理者が追加のサービス パラメータを使用して、CMC デバイスのハント グループのログインおよびログアウト数を設定するために役立ちます。 • ハント グループ ログインのためのエンタープライズ機能アクセス番号。 • ハント グループ ログアウトのためのエンタープライズ機能アクセス番号。 ユーザが CMC デバイスに関連付けられている RD から Hlogin 番号を入力すると、そのときに限りコールは CMC デバイスに関連付けられているハント パイロット番号のダイヤル時に RD にリダイレクトされます。 ユーザが CMC デバイスに関連付けられている RD から Hlogout 番号を入力すると、コールは CMC デバイスに関連付けられているハント パイロット番号のダイヤル時に RD にリダイレクトされません。 デフォルトでは、CMC デバイスは Hloggedin です。いずれの場合でも、CMC デバイスへの直接コールには影響はありません。

機能	データのやり取り
データベースに設定された [呼び出し前の遅延タイマー（Delay Before Ringing Timer）] に基づく CMC リモート接続先コール エクステンション	**DB の [呼び出し前の遅延タイマー（Delay Before Ringing Timer）] が 5000 に設定されている場合** • エンタープライズ電話から CMC 番号に発信する場合、共有回線が鳴り、コールは5秒後にリモート接続先に到達します。 • エンタープライズ電話から CMC 番号に発信する場合、共有回線が 5 秒前にコールに応答すると、コールはリモート接続先に拡張されません。 • エンタープライズ電話から CMC 番号に発信する場合、共有回線が鳴り、発信側が 5 秒前にコールを切断すると、コールはリモート接続先に拡張されません。 **DB の [呼び出し前の遅延タイマー（Delay Before Ringing Timer）] が 0 に設定されている場合** エンタープライズ電話から CMC 番号へのすべてのコールは、リモート接続先と共有回線に同時にアラートを出します。
一括管理ツール（BAT）サポート	BAT サポートは CMC デバイス向けに提供されています

CMC RD 機能の制約事項

表 *5 : CMC RD* 機能の制約事項

機能	制約事項
CMC リモート接続先の関連付け	次の制約事項が適用されます。 • CMC デバイスには、1 つのリモート接続先のみを関連付けることができます。 。 • エンド ユーザが削除されると、その関連付けられている CMC デバイスおよび RD（リモート接続先）も削除されます。 （注） [モビリティの有効化（Enable Mobility）] チェック ボックスがオンまたはオフになっていても、CMC および RD は影響を受けません。CMC デバイスは削除されません。

既存の電話機の移動

次の手順を実行して、設定された電話機をエンド ユーザに移動します。

手順

ステップ 1 Cisco Unified CM の管理で、**[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。

現在ログイン中のデバイスの検索

Cisco Extension Mobility 機能と Cisco Extension Mobility Cross Cluster 機能により、ユーザが現在ログインしているデバイスの記録が維持されます。Cisco Extension Mobility 機能では、現在ログイン中のデバイスのレポートでローカルユーザが現在ログインしているローカル電話が追跡され、Cisco Extension Mobility Cross Cluster 機能では、現在ログイン中のデバイスのレポートでリモート ユーザが現在ログインしているローカル電話が追跡されます。

Unified Communications Manager には、ユーザがログインしているデバイスを検索するための特定の検索ウィンドウがあります。特定のデバイスを検索する場合、またはユーザが現在ログインしているすべてのデバイスを一覧表示する場合は、次の手順に従います。

手順

ステップ 1 **[デバイス（Device）] > [電話（Phone）]** の順に選択します。

ステップ 2 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 [現在ログイン中のデバイスのレポート（Actively Logged In Device Report）] を選択し、[移動（Go）] をクリックします。

ステップ 3 データベース内で現在ログイン中のデバイスのレコードをすべて検索するには、ダイアログ ボックスが空であることを確認して、ステップ 4 に進みます。

レコードをフィルタリングまたは検索するには、

a) 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
b) 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
c) 必要に応じて、適切な検索テキストを指定します。

（注） 検索条件をさらに追加するには、[+] ボタンをクリックします。条件を追加すると、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-] ボタンをクリックします。追加した検索条件をすべて削除するには、[フィルタのクリア（Clear Filter）] ボタンをクリックします。

ステップ 4 [検索（Find）] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[Rows per Page] ドロップダウン リスト ボックスで別の値を選択します。

ステップ 5 表示されるレコードのリストから、表示するレコードへのリンクをクリックします。

（注） ソート順を逆にするには、リストのヘッダーにある上向き矢印または下向き矢印をクリックします。

ウィンドウに選択した項目が表示されます。

リモートでログイン中のデバイスの検索

Cisco Extension Mobility Cross Cluster 機能は、ユーザがリモートでログインしているデバイスのレコードを保持します。リモートでログイン中のデバイス レポートは、他のクラスタが所有していて、EMCC 機能を使用しているローカル ユーザが現在ログインしている電話機を追跡します。

Cisco Unified Communications Manager は、ユーザがリモートでログインしているデバイスを検索するための特定の検索ウィンドウを提供します。次の手順に従って、特定のデバイスを検索したり、ユーザがリモートでログインしているすべてのデバイスを列挙したりします。

手順

ステップ 1 **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。

ステップ 2 右上にある [関連リンク（Related Links）] ドロップダウン リストで [リモート ログイン デバイス（Remotely Logged In Device）] を選択し、[移動（Go）] をクリックします。

ステップ 3 データベース内のリモートでログイン中のすべてのデバイスのレコードを検索するには、ダイアログボックスが空であることを確認して、ステップ 4 に進みます。

レコードをフィルタリングまたは検索するには、

a) 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
b) 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
c) 必要に応じて、適切な検索テキストを指定します。

（注） 検索条件をさらに追加するには、[+] ボタンをクリックします。条件を追加すると、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-]ボタンをクリックします。追加した検索条件をすべて削除するには、[フィルタのクリア（Clear Filter）] ボタンをクリックします。

ステップ 4 [検索（Find）] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[Rows per Page] ドロップダウン リスト ボックスで別の値を選択します。

ステップ 5 表示されるレコードのリストから、表示するレコードへのリンクをクリックします。

（注） ソート順を逆にするには、リストのヘッダーにある上向き矢印または下向き矢印をクリックします。

ウィンドウに選択した項目が表示されます。

電話機のリモート ロック

一部の電話機は、リモートでロックすることができます。電話機をリモートでロックすると、ロックを解除するまで使用できなくなります。

電話機でリモート ロック機能がサポートされている場合は、右上の隅に [ロック（Lock）] ボタンが表示されます。

手順

ステップ 1 **[デバイス（Device）] > [電話（Phone）]** の順に選択します。

ステップ 2 [電話の検索/一覧表示（Find and List Phones）] ウィンドウから、検索条件を入力し、[検索（Find）] をクリックして特定の電話機を見つけます。

検索条件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 ロックを実行する電話機を選択します。

ステップ 4 [電話の設定（Phone Configuration）] ウィンドウで [ロック（Lock）] をクリックします。

電話機が登録されていない場合は、電話機が次回登録されたときにロックされることを伝えるポップアップ ウィンドウが表示されます。[ロック（Lock）] をクリックします。

[デバイスのロック/ワイプのステータス（Device Lock/Wipe Status）] セクションが表示され、最新の要求、保留中かどうか、および最新の確認応答に関する情報が示されます。

工場出荷時の初期状態への電話機のリセット

一部の電話機では、リモートワイプ機能がサポートされます。リモートで電話機をワイプすると、電話機が工場出荷時の設定にリセットされます。電話機に以前に保存されたすべてのデータが消去されます。

電話機でリモート ワイプ機能がサポートされている場合は、右上の隅に [ワイプ（Wipe）] ボタンが表示されます。

注意 この操作は取り消すことができません。この操作は、確実に電話機を工場出荷時の設定にリセットする必要がある場合にのみ、実行してください。

手順

ステップ 1 **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。

ステップ 2 [電話の検索/一覧表示（Find and List Phones）] ウィンドウで、検索条件を入力し、[検索（Find）] をクリックして特定の電話機を見つけます。

検索条件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 ワイプを実行する電話機を選択します。

ステップ 4 [電話の設定（Phone Configuration）] ウィンドウで [ワイプ（Wipe）] をクリックします。

電話機が登録されていない場合は、電話機が次回登録されたときにワイプされることを伝えるポップアップ ウィンドウが表示されます。[ワイプ（Wipe）] をクリックします。

[デバイスのロック/ワイプのステータス（Device Lock/Wipe Status）] セクションが表示され、最新の要求、保留中かどうか、および最新の確認応答に関する情報が示されます。

ロックされたデバイスまたはリセットされたデバイスの検索

リモートでロックされたデバイスまたはリモートでファクトリーデフォルト設定にリセットされたデバイスを検索できます。次の手順に従って、特定のデバイスを検索したり、リモートでロックされたまたはリモートでワイプされたすべてのデバイスを列挙したりします。

手順

ステップ 1 **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。

[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。このウィンドウには、アクティブな（以前の）クエリーのレコードも表示されることがあります。

ステップ 2 ウィンドウの右上にある [関連リンク（Related Links）] ドロップダウン リストで [電話のロック/ワイプ レポート（Phone Lock/Wipe Report）] を選択し、[移動（Go）] をクリックします。

ステップ 3 データベース内のリモートでロックされたデバイスまたはリモートでワイプされたデバイスのすべてのレコードを検索するには、テキスト ボックスが空であることを確認して、ステップ 4 に進みます。

特定のデバイスのレコードを絞り込むまたは検索するには：

a) 1 つ目のドロップダウン リスト ボックスで、検索するデバイス稼働タイプを選択します。
b) 2 番目のドロップダウン リスト ボックスで、検索パラメータを選択します。
c) 3 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
d) 必要に応じて、適切な検索テキストを指定します。

（注） 検索条件をさらに追加するには、[+] ボタンをクリックします。条件を追加すると、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-] ボタンをクリックします。追加した検索条件をすべて削除するには、[フィルタのクリア（Clear Filter）] ボタンをクリックします。

ステップ 4 [検索（Find）] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[Rows per Page] ドロップダウン リスト ボックスで別の値を選択します。

ステップ 5 表示されるレコードのリストから、表示するレコードへのリンクをクリックします。

（注） ソート順を逆にするには、リストのヘッダーにある上向き矢印または下向き矢印をクリックします。

ウィンドウに選択した項目が表示されます。

電話の LSC ステータスの表示および CAPF レポートの生成

この手順を使用して、Cisco Unified Communications Manager インタフェース内からローカルで有効な証明書（LSC）の有効期限情報を監視します。次の検索フィルタは、LSC情報を表示します。

- [LSC 有効期日（LSC Expires）]：電話の LSC 有効期日を表示します。
- [LSC 発行元（LSC Issued By）]：発行元の名前を表示します。これは、CAPF またはサードパーティのいずれかです。
- [LSC 発行元の有効期日（LSC Issuer Expires By）]：発行元の有効期日を表示します。

（注） 新しいデバイスに LSC が発行されていない場合、[LSC 有効期日（LSC Expires）] および [LSC 発行元の有効期日（LSC Issuer Expires by）] フィールドのステータスは [該当なし（NA）] に設定されます。

Cisco Unified Communications Manager 11.5(1) へのアップグレード前に LSC がデバイスに発行された場合は、[LSC 有効期日（LSC Expires）] および [LSC 発行元の有効期日（LSC Issuer Expires by）] フィールドのステータスは [不明（Unknown）] に設定されます。

手順

ステップ 1 **[デバイス（Device）] > [電話（Phone）]** の順に選択します。

ステップ 2 [電話の検索条件（Find Phone where）] の最初のドロップダウン リストから、次の基準の 1 つを選択します。

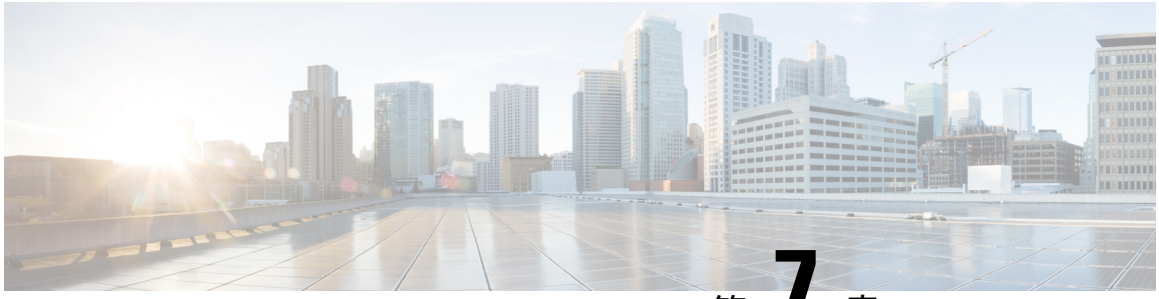
- LSC 有効期日（LSC Expires）
- LSC 発行元（LSC Issued By）
- LSC 発行元の有効期日（LSC Issuer Expires by）

[電話の検索条件（Find Phone where）] の 2 番目のドロップダウン リストから、次の基準の 1 つを選択します。

- が次の日付より前（is before）
- が次の文字列と等しい（is exactly）
- が次の日付より後（is after）
- が次の文字列で始まる（begins with）
- が次の文字列を含む（contains）
- が次の文字列で終わる（ends with）
- が次の文字列と等しい（is exactly）
- が空である（is empty）
- が空ではない（is not empty）

ステップ 3 [検索（Find）] をクリックします。
検出された電話の一覧が表示されます。

ステップ 4 [関連リンク（Related Links）] ドロップダウン リストから [ファイルでの CAPF レポート（CAPF Report in File）] を選択し、[移動（Go）] をクリックします。
レポートがダウンロードされます。



第 7 章

デバイス ファームウェアの管理

デバイス ファームウェアのアップデートの概要

デバイス ロードとは、IP Phone、Telepresence Systems、および Cisco Unified Communications Manager でプロビジョニングおよび登録されているその他のデバイスを対象としたソフトウェアおよびファームウェアのことです。Cisco Unified Communications Manager はインストールまたはアップグレード時に、Cisco Unified Communications Manager の該当するバージョンがリリースされた時期に基づいて、利用可能な最新のロードをインクルードします。シスコでは、新しい機能やソフトウェア フィックスを導入するために更新されたファームウェアを定期的にリリースしています。したがって、新しいロードをインクルードした Cisco Unified Communications Manager アップグレードを待たずに、電話機を新しいロードに更新することができます。

エンドポイントをソフトウェアの新しいバージョンにアップグレードするには、エンドポイントがアクセス可能な場所に新しいロードに必要なファイルがダウンロード可能になっていなければなりません。最も一般的な場所は、Cisco TFTP サービスがアクティブにされている、「TFTP サーバ」と呼ばれる Cisco UCM ノードです。一部の電話機は、「ロード サーバ」と呼ばれる別のダウンロード場所もサポートしています。

任意のサーバ上の tftp ディレクトリ内にあるファイルのリストを取得したり、それらのファイルを表示またはダウンロードしたりするには、CLI コマンドの file list tftp（tftp ディレクトリ内のファイルを一覧表示する場合）、file view tftp（ファイルを表示する場合）、file get tftp（tftp ディレクトリ内のファイルのコピーを取得する場合）を使用します。詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。また、Web ブラウザで URL 「http://<tftp_server>:6970/<filename>」 にアクセスして、任意の TFTP ファイルをダウンロードすることもできます。

ヒント　新しいロードをシステム全体のデフォルトとして設定する前に、単一のデバイスに新規ロードを適用することもできます。この手法は、テスト目的で役立ちます。ただし、該当するタイプのその他すべてのデバイスは、新しいロードでシステム全体のデフォルトを更新するまでは、古いロードを使用することに注意してください。

デバイス パックまたは個々のファームウェアのインストール

デバイス パッケージをインストールして、新しい電話タイプを導入し、複数の電話モデルのファームウェアをアップグレードします。

- 既存のデバイスの個々のファームウェアは次のオプションでインストールまたはアップグレードできます。Cisco Options Package（COP）ファイル：COP ファイルには、ファームウェア ファイルとデータベース アップデートが含まれています。このためパブリッシャにインストールすると、ファームウェア ファイルがインストールされ、さらにデフォルトのファームウェアが更新されます。
- ファームウェア ファイルのみ：zip ファイルで提供されます。zip ファイルに含まれている個々のデバイス ファームウェア ファイルは手動で解凍し、TFTP サーバの適切なディレクトリにおよびアップロードする必要があります。

（注）　COP またはファームウェア ファイル パッケージに固有のインストール手順については、README ファイルを参照してください。

手順

ステップ 1　Cisco Unified OS の管理から、**[ソフトウェア アップグレード（Software Upgrades）] > [インストール/アップグレード（Install/Upgrade）]** の順に選択します。

ステップ 2　ソフトウェアの場所セクションに適切な値を入力し、[次へ（Next）] をクリックします。

ステップ 3　[使用可能なソフトウェア（Available Software）] ドロップダウン リストで、デバイス パッケージ ファイルを選択して、[次へ（Next）] をクリックします。

ステップ 4　MD5 の値が正しいことを確認し、[次へ（Next）] をクリックします。

ステップ 5　警告ボックスで、正しいファームウェアを選択したことを確認し、[インストール（Install）] をクリックします。

ステップ 6　成功メッセージを受信したことを確認します。

（注）　クラスタを再起動している場合は、ステップ 8 に進みます。

ステップ 7 サービスを実行しているすべてのノードで [Cisco TFTP] サービスを再起動します。

ステップ 8 新しいロードにデバイスをアップグレードするには、影響を受けたデバイスをリセットします。

ステップ 9 Cisco Unified CM の管理から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[デバイスのデフォルト（Device Defaults）]** の順に選択し、新しいロードに（特定のデバイスに対して）ロード ファイルの名前を手動で変更します。

ステップ 10 [保存（Save）] をクリックし、デバイスをリセットします。

ステップ 11 すべてのクラスタ ノードで **Cisco Tomcat** サービスを再起動します。

ステップ 12 次のいずれかを実行します。

- 11.5(1)SU4 以下、12.0(1)、または 12.0(1)SU1 を実行している場合は、クラスタを再起動します。
- 11.5(1)SU5 以上での11.5(x) リリース、12.0(1)SU2 以上での任意のリリースを実行している場合は、パブリッシャ ノード上で **Cisco CallManager** サービスを再起動します。ただし、サブスクライバ ノードでのみ **Cisco CallManager** サービスを実行している場合は、このタスクをスキップできます。

ファームウェアのインストールの潜在的な問題

デバイスパックのインストール後に発生する可能性があるいくつかの潜在的な問題を次に示します。

問題	原因/解決
新しいデバイスが登録されません	これはデバイス タイプの不一致により発生する可能性があります。次の原因が考えられます。 • デバイスが [電話の設定（Phone Configuration）] ウィンドウで、不適切なデバイス タイプを使用して追加されました。たとえば、Cisco DX80 が Cisco TelePresence DX80 ではなく電話タイプとして選択されました。適切なデバイス タイプを使用して、デバイスを再設定します。 • **Cisco CallManager** サービスが新しいデバイス タイプを認識しません。この場合、パブリッシャ ノード上で **Cisco CallManager** サービスを再起動します。

問題	原因/解決
エンドポイントが新しいファームウェアにアップグレードしません	Possible reasons: • デバイス パックが TFTP サーバにインストールされていません。その結果、ファームウェアは電話機でダウンロードできません。 • **Cisco TFTP** サービスは、インストール後に再起動されなかったので、新しいファイルについて認識しません。必ず TFTP サーバにデバイス パックをインストールします
Cisco Unified CM Administration の [電話の設定（Phone Configuration）] ウィンドウで、新しいデバイス タイプのアイコン イメージがあるはずの場所に、破損したリンクが表示されます。	CLI からすべてのノードで **Cisco Tomcat** サービスを再起動します。

システムからの未使用のファームウェアの削除

[デバイス ロード管理（Device Load Management）] ウィンドウでは、システムから未使用のファームウェア（デバイスロード）および関連するファイルを削除して、ディスク容量を増やすことができます。たとえば、アップグレード前に未使用のロードを削除して、ディスク容量の不足が原因でアップグレードが失敗しないようにすることができます。ファームウェア ファイルの中には、[デバイス ロード管理（Device Load Management）] ウィンドウにリストされない依存ファイルを持っているものがあります。ファームウェアを削除すると、依存ファイルも削除されます。ただし、その依存ファイルが他のファームウェアに関連付けられている場合は削除されません。

（注） クラスタ内の各サーバで、個別に未使用のファームウェアを削除する必要があります。

始める前に

注意 未使用のファームウェアを削除する前に、適切なロードを削除していることを確認します。削除されたロードは、クラスタ全体の DRS 復元を実行しないと復元できません。ファームウェアを削除する前にバックアップすることを推奨します。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から、**[ソフトウェア アップグレード（Software Upgrades）] > [デバイス ロード管理（Device Load Management）]** の順に選択します。

ステップ 2 検索条件を指定して、[検索（Find）] をクリックします。

ステップ 3 削除するデバイス ロードを選択します。必要な場合は、複数のロードを選択できます。

ステップ 4 [選択されたロードの削除（Delete Selected Loads）] をクリックします。

ステップ 5 [OK] をクリックします。

電話モデルのデフォルト ファームウェアの設定

この手順を使用して、特定の電話モデルにデフォルトのファームウェア ロードを設定します。新しい電話が登録されると、Cisco Unified Communications Manager は、[電話の設定（Phone Configuration）] ウィンドウでデフォルトを上書きするファームウェア ロードが指定されていないかぎり、デフォルトのファームウェアを電話に送信しようとします。

（注） 個々の電話については、[電話の設定（Phone Configuration）] ウィンドウの [電話ロード名（Phone Load Name）] フィールドの設定により、その特定の電話のデフォルト ファームウェア ロードが上書きされます。

始める前に

ファームウェアが TFTP サーバにロードされていることを確認します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [デバイスのデフォルト（Device Defaults）]** を選択します。[デバイスのデフォルト設定（Device Defaults Configuration）] ウィンドウが表示され、Cisco Unified Communications Manager がサポートする様々な電話モデルのデフォルト ファームウェア ロードが示されます。ファームウェアは [ロード情報（Load Information）] 列に表示されます。

ステップ 2 [デバイス タイプ（Device Type）] で、デフォルト ファームウェアを割り当てる電話モデルを指定します。

ステップ 3 横にある [ロード情報（Load Information）] フィールドに、ファームウェア ロードを入力します。

ステップ 4 （任意）[デバイス プール（Device Pool）] にデフォルトのデバイス プールを入力し、[電話テンプレート（Phone Template）]に該当する電話モデルのデフォルトの電話テンプレートを入力します。

ステップ 5 **[保存（Save）]** をクリックします。

電話のファームウェア ロードの設定

この手順を使用して、特定の電話にファームウェア ロードを割り当てます。[デバイスのデフォルト設定（Device Defaults Configuration）] ウィンドウに指定されているデフォルトとは異なるファームウェア ロードを使用する場合に、この手順を実行します。

（注） 多数の電話に1つのバージョンを割り当てる場合は、一括管理ツールを使用し、CSVファイルまたはクエリを使用して、[電話ロード名（Phone Load Name）] フィールドを設定できます。詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

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、個別の電話を選択します。

ステップ 3 [電話ロード名（Phone Load Name）] フィールドに、ファームウェアの名前を入力します。この電話では、ここで指定したファームウェア ロードによって、[デバイスのデフォルト設定（Device Defaults Configuration）] ウィンドウで指定されているデフォルトのファームウェア ロードが上書きされます。

ステップ 4 [電話の設定（Phone Configuration）] 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を含むヘルプは、オンライン ヘルプを参照してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [設定の適用（Apply Config）]をクリックして、変更したフィールドを電話にプッシュします。

ロード サーバの使用

電話が TFTP サーバ以外のサーバからファームウェアの更新をダウンロードするようにするには、電話の [電話の設定（Phone Configuration）] ページで「ロード サーバ」を設定できます。ロード サーバには、別の Cisco Unified Communications Manager またはサードパーティのサーバを指定できます。サードパーティのサーバは、電話が TCP ポート 6970 で HTTP を使用して（推奨）、または UDP ベースの TFTP プロトコルを使用して要求するすべてのファイルを提

供できる必要があります。DX ファミリの Cisco TelePresence デバイスなどの一部の電話モデルでは、ファームウェアのアップデートで HTTP のみをサポートしています。

（注） 多数の電話に 1 つのロード サーバを割り当てる場合は、一括管理ツールを使用し、CSV ファイルまたはクエリを使用して、[ロードサーバ（Load Server）] フィールドを設定できます。詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

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。

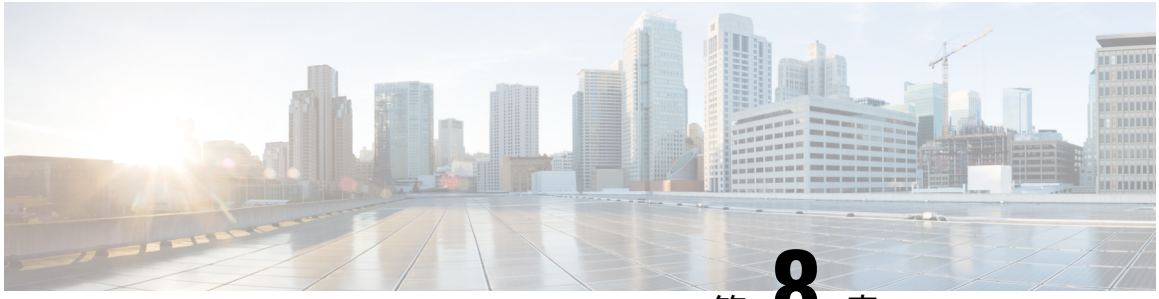
ステップ 2 [検索（Find）] をクリックし、個別の電話を選択します。

ステップ 3 [ロード サーバ（Load Server）] フィールドに、別のサーバの IP アドレスまたはホスト名を入力します。

ステップ 4 [電話の設定（Phone Configuration）] 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を含むヘルプは、オンライン ヘルプを参照してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [設定の適用（Apply Config）] をクリックして、変更したフィールドを電話にプッシュします。



第 8 章

インフラストラクチャ デバイスの管理

インフラストラクチャの管理の概要

この章では、ロケーション対応機能の一部として、スイッチと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 デバイスを管理するタスクについて説明します。ロケーション対応を有効にすると、Cisco Unified Communications Manager データベースには、各スイッチまたはアクセスポイントに現在関連付けられているエンドポイントのリストを含め、ネットワークのスイッチとアクセスポイントのステータス情報が保存されます。

エンドポイントからインフラストラクチャ デバイスへのマッピングは、Cisco Unified Communications Manager と Cisco Emergency Responder が発信者の物理的な場所を特定するのに役立ちます。たとえば、モバイルクライアントがローミング中に緊急通報を行っている場合、Cisco Emergency Responder はこのマッピングを使用して緊急サービスを送る場所を判断します。

データベースに保存されるインフラストラクチャ情報も、インフラストラクチャの使用状況をモニタするのに役立ちます。Unified Communications Manager インターフェイスから、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のデバイスを確認できます。現時点で特定のアクセスポイントまたはスイッチに関連付けられているエンドポイントのリストを表示することもできます。インフラストラクチャデバイスが使用されていない場合は、インフラストラクチャデバイスを非アクティブ化して追跡されないようにできます。

インフラストラクチャの管理の前提条件

Cisco Unified Communications Manager インターフェイス内でワイヤレス インフラストラクチャを管理するには、その前に、ロケーション認識機能を設定する必要があります。有線インフラストラクチャの場合、この機能はデフォルトで有効になっています。設定の詳細については、以下の章を参照してください。

『System Configuration Guide for Cisco Unified Communications Manager』の「Location Awareness」。

また、ネットワーク インフラストラクチャをインストールする必要もあります。詳細については、ワイヤレス LAN コントローラ、アクセス ポイント、スイッチなどのインフラストラクチャ デバイスに付属しているハードウェア ドキュメントを参照してください。

インフラストラクチャの管理のタスク フロー

次のタスクを実行して、ネットワーク インフラストラクチャ デバイスを監視および管理します。

手順

	コマンドまたはアクション	目的
ステップ 1	インフラストラクチャデバイスのステータスの表示 （98 ページ）	ワイヤレス アクセス ポイントまたはイーサネット スイッチの現在のステータスを、関連付けられているエンドポイントの一覧とともに取得します。
ステップ 2	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 （99 ページ）	使用されていないスイッチまたはアクセス ポイントがある場合は、そのデバイスに非アクティブのマークを付けます。そのインフラストラクチャ デバイスのステータスまたは関連付けられているエンドポイントの一覧が更新されなくなります。
ステップ 3	非アクティブ化されたインフラストラクチャ デバイス トラッキングのアクティブ化 （99 ページ）	非アクティブなインフラストラクチャ デバイスのトラッキングを開始します。Cisco Unified Communications Manager が、インフラストラクチャ デバイスのステータスおよび関連付けられているエンドポイントの一覧により、データベースの更新を開始します。

インフラストラクチャ デバイスのステータスの表示

この手順を使用して、ワイヤレス アクセス ポイントやイーサネット スイッチなどのインフラストラクチャ デバイスの現在のステータスを取得します。Cisco Unified Communications Manager インターフェイス内で、アクセス ポイントまたはスイッチのステータスおよび現在関連付けられているエンドポイントの一覧を表示できます。

手順

ステップ 1 Cisco Unified CM の管理で、**[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）] をクリックします。

ステップ 3 ステータスを表示するスイッチまたはアクセス ポイントをクリックします。
[スイッチおよびアクセス ポイントの設定（Switches and Access Point Configuration）] ウィンドウに、そのアクセスポイントまたはスイッチに現在関連付けられているエンドポイントの一覧を含む、現在のステータスが表示されます。

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

スイッチやアクセス ポイントなどの特定のインフラストラクチャ デバイスのトラッキングを削除するには、次の手順を使用します。使用されていないスイッチまたはアクセス ポイントで、この手順を実行できます。

（注） インフラストラクチャデバイスのトラッキングを削除すると、デバイスはデータベースに残ったまま、非アクティブになります。Cisco Unified Communications Manager は、その後、そのインフラストラクチャ デバイスに関連するエンドポイントの一覧も含めて、そのデバイスのステータスを更新しません。[スイッチとアクセス ポイント（Switches and Access Points）] ウィンドウの [関連リンク（Related Links）] ドロップダウンで、非アクティブなスイッチとアクセスポイントを表示できます。

手順

ステップ 1 Cisco Unified CM の管理で、**[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。

非アクティブ化されたインフラストラクチャ デバイス トラッキングのアクティブ化

この手順を使用して、非アクティブ化されたインフラストラクチャデバイスのトラッキングを開始します。スイッチまたはアクセス ポイントがアクティブになると、Cisco Unified

Communications Manager では、スイッチまたはアクセス ポイントに関連付けられているエンドポイントの一覧を含むステータスを動的にトラッキングし始めます。

始める前に

Location Awareness を設定する必要があります。詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Location Awareness」の章を参照してください。

手順

ステップ 1 Cisco Unified CM の管理で、**[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。

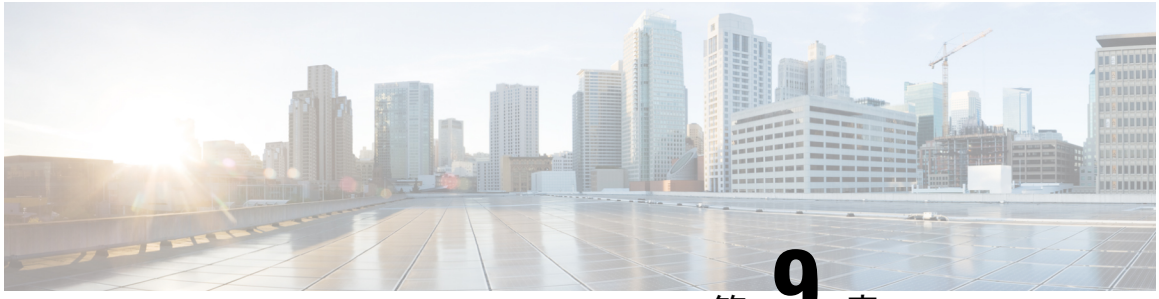
ステップ 2 [関連リンク（Related Links）] から、[非アクティブなスイッチおよびアクセス ポイント（Inactive Switches and Access Points）] を選択し、[移動（Go）] をクリックします。
[非アクティブなスイッチおよびアクセス ポイントの検索および表示（Find and List Inactive Switches and Access Points）] ウィンドウに、トラッキングされていないインフラストラクチャ デバイスが表示されます。

ステップ 3 トラッキングを開始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 4 [選択項目の再アクティブ化（Reactivate Selected）] をクリックします。

第 IV 部

システムの管理



第 9 章

システム ステータスのモニタ

クラスタ ノード ステータスの表示

この手順を使用して、クラスタ内のノードに関する情報を表示します。

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、**[表示（Show）]** > **[クラスタ（Cluster）]** を選択します。

ステップ 2 [クラスタ（Cluster）] ウィンドウのフィールドを調べます。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。

ハードウェア ステータスの表示

ハードウェア ステータスおよびシステム内のハードウェア リソースに関する情報を表示するには、この手順を実行します。

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、**[表示（Show）]** > **[ハードウェア（Hardware）]** を選択します。

ステップ 2 [ハードウェア ステータス（Hardware Status）] ウィンドウのフィールドを調べます。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。

ネットワーク ステータスの表示

イーサネットおよび DNS 情報など、システムのネットワーク ステータスを表示するには、この手順を実行します。

表示されるネットワーク ステータス情報は、ネットワーク耐障害性が有効になっているかどうかによって異なります。

- ネットワーク耐障害性が有効になっていると、イーサネット ポート 0 に障害が発生した場合、イーサネット ポート 1 が自動的にネットワーク通信を管理します。
- ネットワーク耐障害性が有効になっている場合、ネットワーク ポートのイーサネット 0、イーサネット 1、および Bond 0 のネットワーク ステータス情報が表示されます。
- ネットワーク耐障害性が有効になっていない場合、イーサネット 0 のステータス情報のみが表示されます。

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、**[表示（Show）]** > **[ネットワーク（Network）]** を選択します。

ステップ 2 [ネットワーク構成（Network Configuration）] ウィンドウのフィールドを調べます。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。

インストールされているソフトウェアの表示

ソフトウェアのバージョンおよびインストールされているソフトウェア パッケージに関する情報を表示するには、この手順を実行します。

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、**[表示（Show）]** > **[ソフトウェア（Software）]** を選択します。

ステップ 2 [ソフトウェア パッケージ（Software Packages）] ウィンドウのフィールドを調べます。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。

システム ステータスの表示

ロケール、稼働時間、CPU使用量、メモリ使用量などのシステム全体の状態を表示するには、この手順を実行します。

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、**[表示（Show）]** > **[システム（System）]** を選択します。

ステップ 2 [システム ステータス（System Status）] ウィンドウを調べます。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。

IP 設定の表示

この手順を使用して、システムで利用可能な登録済みポートの一覧を表示します。

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、**[表示（Show）]** > **[IP 設定（IP Preferences）]** を選択します。

ステップ 2 （任意） レコードをフィルタリングまたは検索するには、次のいずれかのタスクを実行します。

- 最初の一覧から検索パラメータを選択します。
- 2 番目の一覧から検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

ステップ 3 [検索（Find）] をクリックします。

ステップ 4 [システム ステータス（System Status）] ウィンドウに表示されるフィールドを調べます。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。

最終ログインの詳細の表示

エンドユーザ（ローカルまたはLDAPクレデンシャルを持つエンドユーザ）と管理者がCisco Unified Communications ManagerまたはIM and Presence ServiceのWebアプリケーションにログインすると、アプリケーションのメインウィンドウに、最後に成功したログインと最後に失敗したログインの詳細が表示されます。

SAML SSO機能を使用してログインするユーザには、最後に成功したシステムログイン情報だけが表示されます。ユーザが失敗したSAML SSOログイン情報をトラッキングするには、IDプロバイダー（IdP）アプリケーションを参照できます。

次のWebアプリケーションには、ログイン試行に関する情報が表示されます。

- Cisco Unified Communications Manager:
  - Cisco Unified CMの管理
  - Cisco Unifiedのレポート
  - Cisco Unifiedサービスアビリティ
- IM and Presence Service
  - Cisco Unified CM IM and Presenceの管理
  - Cisco Unified IM and Presenceのレポート
  - Cisco Unified IM and Presenceサービスアビリティ

Cisco Unified Communications Managerの次のWebアプリケーションでは、管理者だけがログインして最後のログイン詳細を表示できます。

- Disaster Recovery System
- Cisco Unified OS Administration

ノードの ping

pingユーティリティを使用して、ネットワーク内の別のノードにpingします。この結果は、デバイスの接続の確認やトラブルシューティングに役立ちます。

手順

ステップ 1 Cisco Unified Operating System Administrationで、**[サービス（Services）] > [Ping]** を選択します。

ステップ 2 [Pingの設定（Ping Configuration）] ウィンドウで、各フィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 3 [Ping] を選択します。

ping の結果が表示されます。

サービス パラメータの表示

クラスタ内のすべてのサーバで特定のサービスに属するサービスパラメータをすべて比較する必要がある場合があります。また、同期外れパラメータ（サーバ間で値が異なるサービスパラメータ）または提示された値から変更されているパラメータだけを表示する必要がある場合もあります。

次の手順を使用して、クラスタ内のすべてのサーバ上で特定のサービスに関するサービスパラメータを表示します。

手順

ステップ 1 **[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 ボックスで、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 ボックスで、クラスタ内のすべてのサーバ上でサービス パラメータを表示するサービスを選択します。

（注） [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウに、すべてのサービス（アクティブと非アクティブ）が表示されます。

ステップ 4 表示された [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウの [関連リンク（Related Links）] ドロップダウン リスト ボックスで [すべてのサーバに対するパラメータ（Parameters for All Servers）] を選択してから、[移動（Go）] をクリックします。

[すべてのサーバに対するパラメータ（Parameters for All Servers）] ウィンドウが表示されます。現在のサービスに関して、すべてのパラメータがアルファベット順に一覧表示されます。パラメータごとに、推奨値がパラメータ名の横に表示されます。各パラメータ名の下に、そのパラメータを含むサーバのリストが表示されます。各サーバ名の横に、このサーバのパラメータの現在値が表示されます。

特定のパラメータについて、対応するサービス パラメータ ウィンドウにリンクするサーバ名または現在のパラメータ値をクリックし、その値を変更します。[前へ（Previous）] と [次へ（Next）] をクリックすると、[すべてのサーバに対するパラメータ（Parameters for All Servers）] ウィンドウ間を移動できます。

ステップ 5 同期外れサービス パラメータを表示する必要がある場合は、[関連リンク（Related Links）] ドロップダウン リスト ボックスで、[すべてのサーバに対する同期外れパラメータ（Out of Sync Parameters for All Servers）] を選択してから、[移動（Go）] をクリックします。

[すべてのサーバに対する同期外れパラメータ（Out of Sync Parameters for All Servers）] ウィンドウが表示されます。現在のサービスに関して、サーバごとに値が異なるサービスパラメータがアルファベット順に表示されます。パラメータごとに、推奨値がパラメータ名の横に表示さ

れます。各パラメータ名の下に、そのパラメータを含むサーバのリストが表示されます。各サーバ名の横に、このサーバのパラメータの現在値が表示されます。

特定のパラメータについて、対応するサービス パラメータ ウィンドウにリンクするサーバ名または現在のパラメータ値をクリックして、その値を変更します。[前へ（Previous）] と [次へ（Next）] をクリックすると、[すべてのサーバに対する同期外れパラメータ（Out of Sync Parameters for All Servers）] ウィンドウ間を移動できます。

ステップ 6 推奨値から変更されたサービスパラメータを表示する必要がある場合は、[関連リンク（Related Links）] ドロップダウン リスト ボックスで、[すべてのサーバに対する変更済みパラメータ（Modified Parameters for All Servers）] を選択してから、[移動（Go）] をクリックします。

[すべてのサーバに対する変更済みパラメータ（Modified Parameters for All Servers）] ウィンドウが表示されます。現在のサービスに関して、推奨値とは異なる値を持つサービスパラメータがアルファベット順に表示されます。パラメータごとに、推奨値がパラメータ名の横に表示されます。各パラメータ名の下に、推奨値とは異なる値を持つサーバのリストが表示されます。各サーバ名の横に、このサーバのパラメータの現在値が表示されます。

特定のパラメータについて、対応するサービス パラメータ ウィンドウにリンクするサーバ名または現在のパラメータ値をクリックして、その値を変更します。[前へ（Previous）] と [次へ（Next）] をクリックすると、[すべてのサーバに対する変更済みパラメータ（Modified Parameters for All Servers）] ウィンドウ間を移動できます。

ネットワーク DNS の設定

DNS ネットワークを設定するには、この手順を使用します

（注） Cisco Unified CM Administration で、DHCP 設定ウィンドウによって DNS プライマリおよびセカンダリ サーバを割り当てることもできます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 DNS サーバを割り当てる場合は、パブリッシャ ノードに次の commandson のいずれかを実行します。

- プライマリ DNS サーバを割り当てるには、**set network dns primary <ip_address>** を実行します
- セカンダリ DNS サーバを割り当てるには、**set network dns secondary <ip_address>** を実行します

ステップ 3 追加の DNS オプションを割り当てるには、**set network dns options [timeout| seconds] [attempts| number] [rotate]** を実行します。

- timout で DNS タイムアウトを設定します
- second はタイムアウトの秒数です
- attempt は DNS 要求の試行回数を設定します
- number は試行回数を指定します
- rotate を指定すると、設定されている DNS サーバのローテーションが行われ、負荷が分散されます

たとえば、set network dns options timeout 60 attempts 4 rotate などとします

サーバは、このコマンドの実行後に再起動します。

第 10 章

使用状況レコードの表示

使用状況レコードの概要

Cisco Unified Communications Manager が提供するレコードを使用して、設定済みの項目がシステム内でどのように使用されているのかを確認することができます。設定済みの項目には、デバイスだけでなく、デバイス プール、日時グループ、ルート プランなどのシステム レベルの設定も含まれます。

依存関係レコード

依存関係レコードは、次の目的で使用します。

- システム レベルの設定（サーバ、デバイス プール、日時グループなど）に関する情報を調べる。
- 他のレコードを使用しているデータベース内のレコードを確認する。たとえば、特定のコーリング サーチ スペースを使用しているデバイス（CTI ルート ポイントや電話機など）を確認できます。
- レコードを削除する前に、レコード間の依存関係を明らかにする。たとえば、パーティションを削除する前に、依存関係レコードを使用して、そのパーティションにどのコーリング サーチ スペース（CSS）とデバイスが関連付けられているかを確認します。こうすることで、その依存関係を削除するように設定を再構成できます。

ルート プラン レポート

ルート プラン レポートでは、システム内で設定されている番号、ルート、パターンの一部またはすべてを確認できます。レポートを生成する際は、レポートの [パターン/電話番号（Pattern/Directory Number）] 列、[パーティション（Partition）] 列、または [ルート詳細（Route

Detail）]列のエントリをクリックすることで、該当する項目の設定ウィンドウにアクセスできます。

さらに、ルート プラン レポートでは、レポートのデータを.CSVファイルに保存して、他のアプリケーションにインポートすることもできます。.CSV ファイルには Web ページよりも詳細な情報が含まれます。具体的には、電話機の電話番号、ルートパターン、パターン使用状況、デバイス名、デバイスの説明などの情報です。

Cisco Unified Communications Manager は、内部コールのルーティングにも、外部公衆電話交換網（PSTN）コールのルーティングにもルート プランを使用します。ネットワークには複数のレコードが存在する可能性があるため、Cisco Unified Communications Manager Administration では、特定の基準に基づいて特定のルート プラン レコードを見つけることができます。

使用状況レポートのタスク

手順

	コマンドまたはアクション	目的
ステップ 1	ルート プラン レコードを表示し、これらのレコードを使用して未割り当ての電話番号を管理するには、次の手順を参照してください。 • ルート プラン レコードの表示（113 ページ） • ルート プラン レコードの保存（114 ページ） • 未割り当ての電話番号の削除（114 ページ） • 未割り当ての電話番号の更新（115 ページ）	特定のルート プラン レコードを検索し、レコードを CSV ファイルに保存し、未割り当ての電話番号を管理するには、これらの手順を使用してください。
ステップ 2	依存関係レコードを使用するには、次の手順を参照してください。 • 依存関係レコードの表示（117ページ）	システムレベルの設定に関する情報を見つけ、データベース内のレコード間の依存関係を表示するには、これらの手順を使用してください。

ルート プラン レポートのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ルート プラン レコードの表示（113ページ）。	ルート プラン レコードを表示し、カスタマイズされたルート プラン レポートを生成します。
ステップ 2	ルート プラン レコードの保存（114ページ）。	.csv ファイル形式でルート プラン レポートを表示します。
ステップ 3	未割り当ての電話番号の削除（114ページ）。	ルート プラン レポートから未割り当ての電話番号を削除します。
ステップ 4	未割り当ての電話番号の更新（115ページ）。	ルート プラン レポートから未割り当ての電話番号の設定を更新します。

ルート プラン レコードの表示

ここでは、ルート プラン レコードを表示する方法について説明します。ネットワーク内に複数のレコードがある可能性があるため、[Cisco Unified Communications Managerの管理（Cisco Unified Communications Manager Administration）] では、特定の基準に基づいて特定のルート プラン レコードを検索できます。カスタマイズされたルート プラン レポートを生成するには、次の手順を実行します。

手順

ステップ 1 **[コール ルーティング（Call Routing）] > [ルート プラン レポート（Route Plan Report）]** の順に選択します。

ステップ 2 データベースのすべてのレコードを検索するには、ダイアログボックスが空であることを確認して、ステップ 3 に進みます。

レコードをフィルタまたは検索するには、次の手順を実行します。

a) 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
b) 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
c) 必要に応じて、適切な検索テキストを指定します。

ステップ 3 [検索（Find）] をクリックします。

すべて、または条件を満たしているレコードが表示されます。1 ページあたりの項目の表示件数を変更するには、[Rows per Page] ドロップダウン リスト ボックスで別の値を選択します。

ステップ 4 表示されるレコードのリストから、表示するレコードへのリンクをクリックします。

ウィンドウに選択した項目が表示されます。

ルート プラン レコードの保存

このセクションでは、.csv ファイルでルート プラン レポートを表示する方法について説明します。

手順

ステップ 1 **[コール ルーティング（Call Routing）] > [ルート プラン レポート（Route Plan Report）]** の順に選択します。

ステップ 2 [ルート プラン レポート（Route Plan Report）] ウィンドウの [関連リンク（Related Links）] ドロップダウンリストから [ファイルで表示（View In File）] を選択し、[移動（Go）] をクリックします。

表示されたダイアログボックスで、ファイルを保存するか、別のアプリケーションにファイルをインポートすることができます。

ステップ 3 **[保存（Save）]** をクリックします。

別のウィンドウが表示され、任意の場所にこのファイルを保存できます。

（注） 別のファイル名での保存も可能ですが、ファイル名には .CSV 拡張子を含める必要があります。

ステップ 4 ファイルを保存する場所を選択し、[保存（Save）] をクリックします。この操作により、指定した場所にファイルが保存されます。

ステップ 5 保存した .CSV ファイルを探し、アイコンをダブルクリックして表示します。

未割り当ての電話番号の削除

このセクションでは、ルート プラン レポートから未割り当ての電話番号を削除する方法について説明します。電話番号は、Cisco Unified Communications Manager Administration の [電話番号の設定（Directory Number Configuration）] ウィンドウで設定または削除します。電話番号がデバイスから削除されたり、電話機が削除されたりしても、電話番号はそのまま Cisco Unified Communications Manager データベース内に残ります。データベースから電話番号を削除するには、[ルート プラン レポート（Route Plan Report）] ウィンドウを使用します。

手順

ステップ 1 **[コール ルーティング（Call Routing）] > [ルート プラン レポート（Route Plan Report）]** を選択します。

ステップ 2 [ルート プラン レポート（Route Plan Report）] ウィンドウで、3 つのドロップダウン リストを使用して、すべての未割り当て DN を列挙するルート プラン レポートを指定します。

ステップ 3 電話番号を削除する 3 つの方法があります。

a) 削除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たら、[削除（Delete）] をクリックします。

b) 削除する電話番号の横にあるチェック ボックスをオンにします。[選択項目の削除] をクリックします。

c) 見つかった未割り当ての電話番号をすべて削除するには、[見つかった項目をすべて削除（Delete All Found Items）] をクリックします。

電話番号を削除するかどうかを確認する警告メッセージが表示されます。

ステップ 4 電話番号を削除する場合は、[OK] をクリックします。削除要求をキャンセルする場合は、[キャンセル（Cancel）] をクリックします。

未割り当ての電話番号の更新

この項では、ルート プラン レポートから未割り当ての電話番号の設定を更新する方法について説明します。電話番号は、Cisco Unified Communications Manager Administration の [電話番号の設定（Directory Number Configuration）] ウィンドウで設定または削除します。デバイスから電話番号が削除されても、電話番号は Cisco Unified Communications Manager データベースに残っています。電話番号の設定を更新するには、[ルート プラン レポート（Route Plan Report）] ウィンドウを使用します。

手順

ステップ 1 **[コールルーティング（Call Routing）]** > **[ルート プラン レポート（Route Plan Report）]** を選択します。

ステップ 2 [ルート プラン レポート（Route Plan Report）] ウィンドウで、3 つのドロップダウン リストを使用して、未割り当ての電話番号をすべてリストするルート プラン レポートを指定します。

ステップ 3 更新する電話番号をクリックします。

（注） 電話番号およびパーティションを除く、電話番号のすべての設定を更新できます。

ステップ 4 コーリング サーチ スペースや転送オプションなどの必要な更新を行います。

ステップ 5 **[保存（Save）]** をクリックします。

[電話番号の設定（Directory Number Configuration）] ウィンドウが再度表示され、電話番号フィールドが空になります。

依存関係レコード 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	依存関係レコードの設定 （116 ページ）。	この手順を使用して、依存関係レコードを有効または無効にします。この手順は、通常よりも低い優先順位で実行され、ダイヤル プランの規模と複雑さ、CPU 速度、およびその他のアプリケーションの CPU 要件によっては完了までに時間がかかることがあります。
ステップ 2	依存関係レコードの表示 （117 ページ）。	依存関係レコードを有効にしたら、インターフェイスの設定ウィンドウからそれらのレコードにアクセスできるようになります。

依存関係レコードの設定

依存レコードを使用して、Cisco Unified Communications Manager データベース内のレコード間の関係を表示します。たとえば、パーティションを削除する前に、依存関係レコードを使用して、そのパーティションにどのコーリング サーチ スペース（CSS）とデバイスが関連付けられているかを確認します。

⚠

注意 依存関係レコードを使用すると、CPU使用率が高くなります。この手順は、標準以下の優先順位で動作し、ダイヤル プランのサイズと複雑さ、CPU 速度、および他のアプリケーションの CPU 要件によっては、完了までに時間がかかる場合があります。

依存関係レコードを有効にしたために、システムでCPU使用率の問題が発生している場合は、依存関係レコードを無効にすることができます。

手順

ステップ 1 Cisco Unified CM の管理で、**[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 [CCMAdmin パラメータ（CCMAdmin Parameters）] セクションにスクロールし、[依存関係レコードの有効化（Enable Dependency Records）] ドロップダウン リストで、次のオプションのいずれかを選択します。

- [True]：依存関係レコードを有効にします。
- [False]：依存関係レコードを無効にします。

選択したオプションに基づいて、依存関係レコードを有効または無効にした結果に関するメッセージを含むダイアログボックスが表示されます。このダイアログボックスで、[OK] をクリックする前に、メッセージをお読みください。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックします。
変更を確認する「更新に成功しました（`Update Successful`）」メッセージが表示されます。

依存関係レコードの表示

依存関係レコードを有効にすると、インターフェイスの設定ウィンドウからそれらにアクセスできます。

始める前に

依存関係レコードの設定 （116 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、表示するレコードの設定ウィンドウに移動します。

例：

デバイス プールの依存関係レコードを表示するには、**[システム（System）] > [デバイス プール（Device Pool）]** を選択します。

（注） [デバイスのデフォルト（Device Defaults）] ウィンドウと [エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウで依存関係レコードを表示することはできません。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 レコードのいずれかをクリックします。
設定ウィンドウが表示されます。

ステップ 4 [関連リンク（Related Links）] リスト ボックスで、[依存関係レコード（Dependency Records）] を選択し、[移動（Go）] をクリックします。

（注） 依存関係レコードを有効にしていない場合は、[依存関係レコード要約（Dependency Records Summary）] ウィンドウに、レコードに関する情報ではなくメッセージが表示されます。

[依存関係レコード要約（Dependency Records Summary）] ウィンドウには、データベース内の他のレコードによって使用されるレコードが表示されます。

ステップ 5 このウィンドウで、次の依存関係レコード ボタンのいずれかを選択します。

- [更新（Refresh）]：最新の情報でウィンドウを更新します。

- [閉じる（Close）]：[依存関係レコード（Dependency Records）] リンクをクリックした設定ウィンドウに戻らずにウィンドウを閉じます。
- [閉じて戻る（Close and Go Back）]：ウィンドウを閉じて、[依存関係レコード（Dependency Records）] リンクをクリックした設定ウィンドウに戻ります。

第 11 章

システムのバックアップ

バックアップの概要

定期的にバックアップを行うことを推奨します。ディザスタ リカバリ システム（DRS）を使用して、クラスタ内のすべてのサーバのデータを完全にバックアップできます。自動バックアップをセットアップすることも、任意の時点でバックアップを起動することもできます。

ディザスタ リカバリ システムで実行するバックアップは、クラスタ レベルであり、Cisco Unified Communications Manager クラスタ内のすべてのサーバのバックアップを 1 箇所に集め、バックアップ データを物理的なストレージ デバイスにアーカイブします。バックアップ ファイルは暗号化され、システム ソフトウェアによってだけ開くことができます。

DRS は、プラットフォームのバックアップ/復元の一環として、独自の設定（バックアップ デバイス設定およびスケジュール設定）を復元します。DRS は drfDevice.xml ファイルと drfSchedule.xml ファイルをバックアップおよび復元します。これらのファイルとともにサーバを復元するときは、DRS バックアップ デバイスおよびスケジュールを再設定する必要がありません。

システムデータを復元するときには、クラスタ内のどのノードを復元するかを選択できます。

ディザスタ リカバリ システムには、次の機能があります。

- バックアップおよび復元タスクを実行するためのユーザ インターフェイス。
- バックアップ機能を実行するための分散システム アーキテクチャ。
- スケジュール バックアップまたは手動（ユーザが起動する）バックアップ。
- リモート SFTP サーバへのバックアップのアーカイブ。

バックアップの前提条件

- バージョンの要件を満たしていることを確認してください。
  - すべての Cisco Unified Communications Manager クラスタ ノードは、同じバージョンの Cisco Unified Communications Manager アプリケ–ションを実行している必要があります。
  - すべての IM and Presence Service クラスタ ノードは、同じバージョンの IM and Presence Service アプリケーションを実行している必要があります。
  - バックアップ ファイルに保存されているソフトウェア バージョンが、クラスタ ノードで実行されるバージョンと同じでなければなりません。

  バージョンの文字列全体が一致している必要があります。たとえば、IM and Presence データベース パブリッシャ ノードがバージョン 11.5.1.10000-1 の場合、すべての IM and Presence サブスクライバ ノードは 11.5.1.10000-1 であり、バックアップ ファイルに保存されているバージョンも 11.5.1.10000-1 でなければなりません。現在のバージョンと一致しないバックアップ ファイルからシステムを復元しようすると、復元は失敗します。バックアップ ファイルに保存されているバージョンが、クラスタ ノードで実行されているバージョンと一致するよう、ソフトウェア バージョンをアップグレードしたら常にシステムをバックアップするようにしてください。

- DRS 暗号化は、クラスタ セキュリティ パスワードに依存することに留意してください。バックアップの実行中に、DRS は暗号化のためにランダム パスワードを生成し、そのランダム パスワードをクラスタ セキュリティ パスワードを使用して暗号化します。バックアップを実行した後、復元を行うまでの間にクラスタ セキュリティ パスワードが変更された場合、そのバックアップ ファイルを使用してシステムを復元するには、バックアップを実行した時点でのパスワードを把握していなければなりません。あるいは、セキュリティ パスワードを変更/リセットした直後にバックアップを作成するようにしてください。

- リモート デバイスをバックアップする必要がある場合は、必ず SFTP サーバを設定する必要があります。利用可能な SFTP サーバの詳細については、次の項を参照してください。リモート バックアップ用 SFTP サーバ （128 ページ）

バックアップ タスク フロー

次のタスクを実行して、バックアップを設定して実行します。バックアップの実行中は OS 管理タスクを実行しないでください。これは、ディザスタ リカバリ システムがプラットフォーム API をロックすることにより、すべての OS 管理要求をブロックするためです。ただし、CLI ベースのアップグレード コマンドしかプラットフォーム API ロッキング パッケージを使用しないため、ディザスタ リカバリ システムはほとんどの CLI コマンドを妨害しません。

手順

	コマンドまたはアクション	目的
ステップ 1	バックアップデバイスの設定（121ページ）	データをバックアップするデバイスを指定します。
ステップ 2	バックアップ ファイルのサイズの予測（122 ページ）	SFTP デバイス上で作成されるバックアップ ファイルのサイズを見積もります。
ステップ 3	次のいずれかのオプションを選択します。 • スケジュール バックアップの設定（123 ページ） • 手動バックアップの開始（125ページ）	スケジュールに従ってデータをバックアップするためのバックアップ スケジュールを作成します。 または、手動バックアップを実行します。
ステップ 4	現在のバックアップ ステータスの表示（126 ページ）	これはオプションです。バックアップのステータスをチェックします。バックアップの実行中、現在のバックアップ ジョブのステータスを確認できます。
ステップ 5	バックアップ履歴の表示（126ページ）	これはオプションです。バックアップ履歴の表示

バックアップ デバイスの設定

最大 10 個のバックアップ デバイスを設定できます。バックアップ ファイルを保存する場所を設定するには、次の手順を実行します。

始める前に

- バックアップ ファイルを保存するために SFTP サーバにディレクトリ パスへの書き込みアクセス権があることを確認します。
- DRS マスターエージェントがバックアップデバイスの設定を検証するときに、ユーザ名、パスワード、サーバ名とディレクトリ パスが有効であることを確認します。

（注） バックアップはネットワーク トラフィックが少なくなる時間帯にスケジューリングしてください。

手順

ステップ 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）] > [バックアップ デバイス（Backup Device）]** の順に選択します。

ステップ 2 [バックアップ デバイス リスト（Backup Device List）] ウィンドウで、次のいずれかを実行します。

- 新しいデバイスを設定するには、[新規追加（Add New）] をクリックします。
- 既存のバックアップ デバイスを編集するには、検索条件を入力し、[検索（Find）]、次に [選択項目の編集（Edit Selected）] をクリックします。
- バックアップ デバイスを削除するには、[バックアップ デバイス（Backup Device）] リストでバックアップ デバイスを選択してから [選択項目の削除（Delete Selected）] をクリックします。

バックアップ スケジュールにバックアップ デバイスとして設定されているバックアップ デバイスは削除できません。

ステップ 3 [バックアップ デバイス名（Backup device name）] フィールドにバックアップ名を入力します。

バックアップ デバイス名には、英数字、スペース（ ）、ダッシュ（-）、およびアンダースコア（_）だけを使用します。それ以外の文字は使用しないでください。

ステップ 4 [接続先の選択（Select Destination）] 領域の [ネットワーク ディレクトリ（Network Directory）] で、次を実行します。

- [ホスト名/IP アドレス（Host name/IP Address）] フィールドに、ネットワーク サーバのホスト名または IP アドレスを入力します。
- [パス名（Path name）] フィールドに、バックアップ ファイルを格納するディレクトリ パスを入力します。
- [ユーザ名（User name）] フィールドに、有効なユーザ名を入力します。
- [パスワード（Password）] フィールドに、有効なパスワードを入力します。
- [ネットワーク ディレクトリに保存するバックアップ数（Number of backups to store on Network Directory）] ドロップダウン リストから、バックアップの必要数を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

バックアップ ファイルのサイズの予測 （122 ページ）

バックアップ ファイルのサイズの予測

1 つまたは複数の選択した機能のバックアップ履歴が存在する場合に限り、Cisco Unified Communications Manager は、バックアップ tar のサイズを予測します。

計算されたサイズは正確な値ではなく、バックアップ tar の予測サイズです。サイズは前のバックアップの実際のバックアップ サイズに基づいて計算され、設定が前回のバックアップ以降変更された場合は異なることがあります。

この手順は、前回のバックアップが存在する場合にのみ使用でき、初めてシステムをバックアップする場合は使用できません。

SFTP デバイスに保存されているバックアップ tar のサイズを予測するには、次の手順に従ってください。

手順

ステップ 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）]** > **[手動バックアップ（Manual Backup）]** の順に選択します。

ステップ 2 [機能の選択（Select Features）] 領域でバックアップする機能を選択します。

ステップ 3 選択した機能のバックアップの予測サイズを表示するには、[サイズの予測（Estimate Size）] を選択します。

次のタスク

システムをバックアップするには、次のいずれかの手順を実行します。

- スケジュール バックアップの設定 （123 ページ）
- 手動バックアップの開始 （125 ページ）

スケジュール バックアップの設定

最大 10 個のバックアップ スケジュールを作成できます。各バックアップ スケジュールには、自動バックアップのスケジュール、バックアップする機能セット、保存場所など、独自のプロパティがあります。

バックアップ .tar ファイルはランダムに生成されるパスワードで暗号化されるということに注意してください。このパスワードは、クラスタ セキュリティ パスワードで暗号化され、バックアップ .tar ファイルとともに保存されます。このセキュリティ パスワードは忘れないように記憶しておくか、またはセキュリティ パスワードを変更またはリセットしたらすぐにバックアップを作成する必要があります。

注意 コール処理が中断してサービスに影響が及ばないように、バックアップはオフピーク時間中にスケジュールしてください。

始める前に

バックアップ デバイスの設定 （121 ページ）

手順

ステップ 1 ディザスタ リカバリ システムで、[バックアップ スケジューラ（Backup Scheduler）] を選択します。

ステップ 2 [スケジュール リスト（Schedule List）] ウィンドウで、新規スケジュールを追加するか、または既存のスケジュールを編集します。

- 新規スケジュールを作成するには、[新規追加（Add New）] をクリックします。
- 既存のスケジュールを設定するには、[スケジュール リスト（Schedule List）] 列でその名前をクリックします。

ステップ 3 [スケジューラ（scheduler）] ウィンドウで、[スケジュール名（Schedule Name）] フィールドにスケジュール名を入力します。

（注） デフォルトのスケジュールの名前は変更できません。

ステップ 4 [バックアップ デバイスの選択（Select Backup Device）] 領域でバックアップ デバイスを選択します。

ステップ 5 [機能の選択（Select Features）] 領域でバックアップする機能を選択します。少なくとも 1 つの機能を選択する必要があります。

ステップ 6 [バックアップの開始時刻（Start Backup at）] 領域でバックアップを開始する日付と時刻を選択します。

ステップ 7 [頻度（Frequency）] 領域でバックアップを行う頻度を選択します。頻度は、[一度（Once）]、[日次（Daily）]、[週次（Weekly）]、[月次（Monthly）] に設定できます。[週次（Weekly）] を選択した場合は、バックアップを行う週の曜日も選択できます。

ヒント バックアップ頻度を火曜日から土曜日までの [週次（Weekly）] に設定するには、[デフォルトの設定（Set Default）] をクリックします。

ステップ 8 これらの設定を更新するには、[保存（Save）] をクリックします。

ステップ 9 次のいずれかのオプションを選択します。

- 選択したスケジュールをイネーブルにするには、[選択されたスケジュールの有効化（Enable Selected Schedules）] をクリックします。
- 選択したスケジュールをディセーブルにするには、[選択されたスケジュールの無効化（Disable Selected Schedules）] をクリックします。
- 選択したスケジュールを削除するには、[選択項目の削除（Delete Selected）] をクリックします。

ステップ 10 スケジュールを有効にするには、[スケジュールの有効化（Enable Schedule）] をクリックします。

設定した時刻になると自動的に次のバックアップが実行されます。

（注） クラスタ内のすべてのサーバが、同じバージョンの Cisco Unified Communications Manager または Cisco IM and Presence サービスを実行し、ネットワークから到達可能であることを確認します。スケジュールされたバックアップの時刻にサーバに到達できないと、そのサーバはバックアップされません。

次のタスク

次の手順を実行します。

- バックアップ ファイルのサイズの予測 （122 ページ）
- （任意）現在のバックアップ ステータスの表示 （126 ページ）

手動バックアップの開始

始める前に

- バックアップ ファイルの格納場所としてネットワーク デバイスを使用していることを確認します。Unified Communications Manager の仮想化展開では、テープ ドライブによるバックアップ ファイルの保存はサポートされません。
- Cisco Unified Communications Manager または IM and Presence Service のインストールされているバージョンが、すべてのクラスタ ノードで同じであることを確認します。
- バックアップ プロセスは、リモート サーバに利用可能な容量がないためや、ネットワーク接続が中断されたために失敗することがあります。バックアップが失敗する原因となった問題に対処した後、新規のバックアップを開始する必要があります。
- ネットワークの中断がないことを確認してください。
- バックアップ デバイスの設定 （121 ページ）
- バックアップ ファイルのサイズの予測 （122 ページ）
- クラスタ セキュリティ パスワードのレコードがあることを確認します。このバックアップの完了後に、クラスタ セキュリティ パスワードを変更した場合は、パスワードを認識している必要があります。パスワードを認識していないと、バックアップ ファイルを使用してシステムを復元できなくなります。

（注） バックアップが実行されている間は、Disaster Recovery System がプラットフォーム API をロックしてすべての要求をブロックするため、Cisco Unified OS の管理または Cisco Unified IM and Presence OS の管理でタスクを実行することはできません。ただし、ディザスタ リカバリ システムは、CLI ベースのアップグレード コマンドだけがプラットフォーム API ロッキング パッケージを使用するため、ほとんどの CLI コマンドをブロックしません。

手順

ステップ 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）]** > **[手動バックアップ（Manual Backup）]** の順に選択します。

ステップ 2 [手動バックアップ（Manual Backup）] ウィンドウで、[バックアップ デバイス名（Backup Device Name）] 領域を選択します。

ステップ 3 [機能の選択（Select Features）] 領域から機能を選択します。

ステップ 4 [バックアップの開始（Start Backup）] をクリックします。

次のタスク

（任意）現在のバックアップ ステータスの表示 （126 ページ）

現在のバックアップ ステータスの表示

現在のバックアップ ジョブのステータスを確認するには、次の手順を実行します。

注意 リモート サーバへのバックアップが 20 時間以内に完了しないとバックアップ セッションがタイムアウトするため、新規バックアップを開始する必要があります。

手順

ステップ 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）]** > **[現在のステータス（Current Status）]** の順に選択します。

ステップ 2 バックアップ ログ ファイルを表示するには、ログファイル名リンクをクリックします。

ステップ 3 現在のバックアップをキャンセルするには、[バックアップのキャンセル（Cancel Backup）] をクリックします。

（注） 現在のコンポーネントがバックアップ操作を完了した後、バックアップがキャンセルされます。

次のタスク

バックアップ履歴の表示 （126 ページ）

バックアップ履歴の表示

バックアップ履歴を参照するには、次の手順を実行します。

手順

ステップ 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）] > [履歴（History）]** の順に選択します。

ステップ 2 [バックアップ履歴（Backup History）] ウィンドウで、ファイル名、バックアップ デバイス、完了日、結果、バージョン、バックアップされている機能、失敗した機能など、実行したバックアップを表示できます。

（注） [バックアップ履歴（Backup History）] ウィンドウには、最新の 20 個のバックアップ ジョブだけが表示されます。

バックアップの連携動作と制約事項

バックアップの制約事項

バックアップには、次の制約事項が適用されます。

表 *6:* バックアップの制約事項

制約事項	説明
クラスタ セキュリティ パスワード	クラスタ セキュリティ パスワードを変更したら、必ずバックアップを実行することを推奨します。 バックアップ暗号化では、バックアップ ファイルのデータを暗号化する際にクラスタ セキュリティ パスワードを使用します。バックアップ ファイルの作成後にクラスタ セキュリティ パスワードを編集すると、古いパスワードを忘れてしまった場合に、そのバックアップ ファイルを使用してデータを復元できなくなります。

制約事項	説明
証明書の管理	ディザスタ リカバリ システム（DRS）は、マスターエージェントとローカルエージェントとの間で SSL ベースの通信を使用して、Cisco Unified Communications Manager クラスタ ノード間のデータの認証および暗号化を行います。DRS は、IPSec 証明書を使用して、公開キー/秘密キーの暗号化を行います。証明書管理ページから IPSEC 信頼ストア（hostname.pem）ファイルを削除すると、DRS が想定どおりに機能しなくなることに注意してください。IPSEC 信頼ファイルを手動で削除するときは、IPSEC 証明書を IPSEC 信頼に必ずアップロードしてください。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『*Security Guide for Cisco Unified Communications Manager*』の「証明書管理」の項を参照してください。

リモート バックアップ用 SFTP サーバ

データをネットワーク上のリモート デバイスにバックアップするには、SFTP サーバを用意して必要な設定を行う必要があります。シスコは内部テストでは、Cisco TAC にサポートされている、シスコ提供の Cisco Prime Collaboration Deployment（PCD）上で SFTP サーバを使用します。SFTP サーバ オプションの概要については、次の表を参照してください。

以下の表示に記載されている情報を参考に、システムで使用する SFTP サーバ ソリューションを決定してください。

表 *7: SFTP* サーバ情報

SFTP サーバ	情報
Cisco Prime Collaboration Deployment の SFTP サーバ	このサーバはシスコが提供およびテストした SFTP サーバのみであり、Cisco TAC がサポートします。 バージョンの互換性は、使用している Unified Communications Manager および Cisco Prime Collaboration Deployment のバージョンに依存します。バージョン（SFTP）または Unified Communications Manager をアップグレードする前に、『*Cisco Prime Collaboration Deployment Administration Guide*』を参照して、互換性のあるバージョンであることを確認してください。

SFTP サーバ	情報
テクノロジー パートナーの SFTP サーバ	これらのサーバはサード パーティが提供およびテストしたものです。バージョンの互換性は、サードパーティによるテストに依存します。テクノロジー パートナーの SFTP サーバまたは Unified Communications Manager をアップグレードする場合、テクノロジー パートナーのページで、互換性のあるバージョンを確認してください。 https://marketplace.cisco.com
他のサードパーティの SFTP サーバ	これらのサーバはサード パーティが提供するものであり、Cisco TAC はこれらのサーバを正式にサポートしていません。 バージョンの互換性は、SFTP バージョンと Unified Communications Manager バージョンの互換性を確立するためのベスト エフォートに基づきます。 （注） これらの製品がシスコでテストされていない場合、シスコはその機能を保証することができません。Cisco TAC は、これらの製品をサポートしていません。完全にテストされてサポートされる SFTP ソリューションとしては、Cisco Prime Collaboration Deployment またはテクノロジー パートナーの SFTP サーバを利用してください。

暗号サポート

Unified Communications Manager 11.5 および以前のバージョンでは、Unified Communications Manager は SFTP 接続の次の CBC 暗号をアドバタイズします。

- aes128-cbc
- 3des-cbc
- blowfish-cbc

（注） バックアップ SFTP サーバが Unified Communications Manager との通信のためにこれらの CBC 暗号のいずれかをサポートしていることを確認します。

Unified Communications Manager 12.0 リリース以降では、CBC 暗号はサポートされていません。Unified Communications Manager は、次の CTR 暗号のみをサポートおよびアドバタイズします。

- aes256-ctr

- aes128-ctr
- aes192-ctr

（注） バックアップ SFTP サーバが Unified Communications Manager との通信のためにこれらの CTR 暗号のいずれかをサポートしていることを確認します。

第 12 章

システムの復元

復元の概要

ディザスタ リカバリ システム（DRS）には、システムを復元するプロセスを実行するためのガイドとなるウィザードが用意されています。

バックアップ ファイルは暗号化されており、それらを開いてデータを復元できるのは DRS システムのみです。ディザスタ リカバリ システムには、次の機能があります。

- 復元タスクを実行するためのユーザ インターフェイス。
- 復元機能を実行するための分散システム アーキテクチャ。

マスター エージェント

クラスタの各ノードで自動的にマスター エージェント サービスが起動されますが、マスター エージェントはパブリッシャ ノード上でのみ機能します。サブスクライバ ノード上のマスター エージェントは、何の機能も実行しません。

ローカル エージェント

サーバには、バックアップおよび復元機能を実行するローカルエージェントが搭載されています。

マスター エージェントを含むノードをはじめ、Cisco Unified Communications Manager クラスタ内の各ノードには、バックアップおよび復元機能を実行するために独自のローカルエージェントが必要です。

（注） デフォルトでは、ローカル エージェントは IM and Presence ノードをはじめ、クラスタ内の各ノードで自動的に起動されます。

復元の前提条件

- バージョンの要件を満たしていることを確認してください。
  - すべての Cisco Unified Communications Manager クラスタ ノードは、同じバージョンの Cisco Unified Communications Manager アプリケ-ションを実行している必要があります。
  - すべての IM and Presence Service クラスタ ノードは、同じバージョンの IM and Presence Service アプリケーションを実行している必要があります。
  - バックアップ ファイルに保存されているバージョンが、クラスタ ノードで実行されるバージョンと同じでなければなりません。

  バージョンの文字列全体が一致している必要があります。たとえば、IM and Presence データベース パブリッシャ ノードがバージョン 11.5.1.10000-1 の場合、すべての IM and Presence サブスクライバ ノードは 11.5.1.10000-1 であり、バックアップ ファイルに保存されているバージョンも 11.5.1.10000-1 でなければなりません。現在のバージョンと一致しないバックアップ ファイルからシステムを復元しようすると、復元は失敗します。
- サーバの IP アドレス、ホスト名、DNS 設定および導入タイプが、バックアップ ファイルに保存されている IP アドレス、ホスト名、DNS 設定および導入タイプと一致していることを確認します。
- バックアップを実行した後にクラスタ セキュリティ パスワードを変更した場合、元のパスワードのレコードを記録しておきます。元のパスワードが分からなければ、復元は失敗します。

復元タスク フロー

復元プロセス中、[Cisco Unified CM の管理（Cisco Unified Communications Manager OS Administration）] または [Cisco Unified CM IM and Presence OS の管理（Cisco Unified IM and Presence OS Administration）] に関するタスクを実行しないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	最初のノードのみの復元 （133 ページ）	（オプション）クラスタ内の最初のパブリッシャ ノードだけを復元する場合は、この手順を使用します。
ステップ 2	後続クラスタ ノードの復元 （135 ページ）	（オプション）クラスタ内のサブスクライバ ノードを復元する場合は、この手順を使用します。
ステップ 3	パブリッシャの再構築後の 1 回のステップでのクラスタの復元 （137 ページ）	（オプション）パブリッシャがすでに再構築されている場合、1 回のステップでクラスタ全体を復元するには、次の手順に従ってください。
ステップ 4	クラスタ全体の復元 （139 ページ）	（オプション）パブリッシャ ノードを含む、クラスタ内のすべてのノードを復元するには、この手順を使用します。主要なハード ドライブで障害またはアップグレードが発生した場合や、ハード ドライブを移行する場合には、クラスタ内のすべてのノードの再構築が必要になる場合があります。
ステップ 5	前回正常起動時の設定へのノードまたはクラスタの復元 （140 ページ）	（オプション）前回正常起動時の設定にノードを復元する場合に限り、この手順を使用します。ハード ドライブ障害やその他のハードウェア障害の後には使用しないでください。
ステップ 6	ノードの再起動 （141 ページ）	ノードを再起動するには、この手順を使用します。
ステップ 7	復元ジョブ ステータスのチェック （142 ページ）	（オプション）復元ジョブ ステータスを確認するには、この手順を使用します。
ステップ 8	復元履歴の表示 （142 ページ）	（オプション）復元履歴を表示するには、この手順を使用します。

最初のノードのみの復元

再構築後に最初のノードを復元する場合は、バックアップ デバイスを設定する必要があります。

この手順は、Cisco Unified Communications Manager の最初のノード（パブリッシャ ノードとも呼ばれます）に対して実行できます。その他の Cisco Unified Communications Manager ノードおよびすべての IM and Presence サービス ノードは、セカンダリ ノードまたはサブスクライバと見なされます。

始める前に

クラスタ内に IM and Presence サービス ノードがある場合は、最初のノードを復元するときに、ノードが実行されており、アクセス可能であることを確認してください。これは、この手順の実行中に有効なバックアップ ファイルを見つけるために必須です。

手順

ステップ 1 ディザスタ リカバリ システムから、**[復元（Restore）]** > **[復元ウィザード（Restore Wizard）]** を選択します。

ステップ 2 [復元ウィザード ステップ 1（Restore Wizard Step 1）] ウィンドウの [バックアップ デバイスの選択（Select Backup Device）] 領域で、復元する適切なバックアップ デバイスを選択します。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）] ウィンドウで、復元するバックアップ ファイルを選択します。

（注） バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）] ウィンドウで、[次へ（Next）] をクリックします。

ステップ 7 復元する機能を選択します。

（注） バックアップ対象として選択した機能が表示されます。

ステップ 8 復元するノードを選択します。

ステップ 9 [復元（Restore）] をクリックして、データを復元します。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 復元するノードの選択を求められたら、最初のノード（パブリッシャ）だけを選択します。

注意 このときに後続（サブスクライバ）ノードは選択しないでください。復元を試みても失敗します。

ステップ 12 （オプション）[サーバ名の選択（Select Server Name）] ドロップダウン リストから、パブリッシャ データベース復元元のサブスクライバ ノードを選択します。選択したサブスクライバ ノードが稼働しており、クラスタに接続されていることを確認してください。
ディザスタ リカバリ システムでバックアップ ファイルのすべてのデータベース以外の情報が復元され、選択した後続ノードから最新のデータベースが取り出されます。

（注） このオプションは、選択したバックアップファイルにCCMDBデータベース コンポーネントが含まれている場合にのみ表示されます。まず、パブリッシャ ノードだけが完全に復元されますが、ステップ14を実行し、後続のクラスタ ノードを再起動すると、ディザスタ リカバリ システムはデータベース レプリケーションを実行し、完全にすべてのクラスタ ノードのデータベースが同期されます。これにより、すべてのクラスタ ノードに最新のデータを使用していることが保障されます。

ステップ 13 [復元（Restore）] をクリックします。

ステップ 14 パブリッシャ ノードにデータが復元されます。復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

（注） 最初のノードを復元すると、Cisco Unified Communications Manager データベース全体がクラスタに復元されます。そのため、復元しているノードの数とデータベースのサイズによっては、数時間かかることがあります。復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

ステップ 15 [復元ステータス（Restore Status）] ウィンドウの [完了率（Percentage Complete）] フィールドに 100% と表示されたら、サーバを再起動します。クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

（注） Cisco Unified Communications Manager ノードだけを復元する場合は、Cisco Unified Communications Manager and IM and Presence Service サービス クラスタを再起動する必要があります。

IM and Presence サービスのパブリッシャ ノードのみを復元する場合は、IM and Presence サービス クラスタを再起動する必要があります。

次のタスク

- （オプション）復元のステータスを表示するには、次を参照してください： 復元ジョブ ステータスのチェック （142 ページ）
- ノードを再起動するには、次を参照してください： ノードの再起動 （141 ページ）

後続クラスタ ノードの復元

この手順は、Cisco Unified Communications Manager のサブスクライバ（後続）ノードにのみ適用されます。インストールされる最初の Cisco Unified Communications Manager ノードはパブリッシャ ノードです。その他すべての Cisco Unified Communications Manager ノードおよびすべての IM and Presence サービス ノードはサブスクライバ ノードです。

クラスタ内の 1 つ以上の Cisco Unified Communications Manager サブスクライバ ノードを復元するには、次の手順に従います。

始める前に

復元操作を実行する場合は事前に、復元のホスト名、IP アドレス、DNS 設定、および配置タイプが、復元するバックアップ ファイルのホスト名、IP アドレス、DNS 設定、および配置タイプに一致することを確認します。ディザスタ リカバリ システムでは、ホスト名、IP アドレス、DNS 設定、および配置タイプが異なると復元が行われません。

サーバにインストールされているソフトウェアのバージョンが復元するバックアップ ファイルのバージョンに一致することを確認します。ディザスタ リカバリ システムは、一致するソフトウェア バージョンのみを復元操作でサポートします。再構築後に後続ノードを復元している場合は、バックアップ デバイスを設定する必要があります。

手順

ステップ 1 ディザスタ リカバリ システムから、**[復元（Restore）] > [復元ウィザード（Restore Wizard）]** を選択します。

ステップ 2 [復元ウィザード ステップ 1（Restore Wizard Step 1）] ウィンドウの [バックアップ デバイスの選択（Select Backup Device）] 領域で、復元元のバックアップ デバイスを選択します。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）] ウィンドウで、復元するバックアップ ファイルを選択します。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）] ウィンドウで、復元する機能を選択します。

（注） 選択したファイルにバックアップされた機能だけが表示されます。

ステップ 7 [次へ（Next）] をクリックします。[復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウが表示されます。

ステップ 8 [復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウで、復元するノードを選択するよう求められたら、後続ノードのみを選択します。

ステップ 9 [復元（Restore）] をクリックします。

ステップ 10 後続ノードにデータが復元されます。復元ステータスの確認方法については、「次の作業」の項を参照してください。

（注） 復元プロセス中、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] または [ユーザ オプション（User Options）] に関するタスクを実行しないでください。

ステップ 11 [復元ステータス（Restore Status）] ウィンドウの [完了率（Percentage Complete）] フィールドに 100% と表示されたら、復元した 2 次サーバを再起動します。クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

（注） 最初の IM and Presence サービス ノードが復元されたら、IM and Presence サービスの後続ノードを再起動する前に、必ず最初の IM and Presence サービス ノードを再起動してください。

次のタスク

- （オプション）復元のステータスを表示するには、次を参照してください： 復元ジョブステータスのチェック （142 ページ）
- ノードを再起動するには、次を参照してください： ノードの再起動 （141 ページ）

パブリッシャの再構築後の 1 回のステップでのクラスタの復元

復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。パブリッシャがすでに再構築されている場合、または新しくインストールされた場合に、1 回のステップでクラスタ全体を復元する場合は、次の手順に従います。

手順

ステップ 1 ディザスタ リカバリ システムから、**[復元（Restore）] > [復元ウィザード（Restore Wizard）]** を選択します。

ステップ 2 [復元ウィザード ステップ 1（Restore Wizard Step 1）] ウィンドウの [バックアップ デバイスの選択（Select Backup Device）] 領域で、復元するバックアップ デバイスを選択します。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）] ウィンドウで、復元するバックアップ ファイルを選択します。

バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。

クラスタ全体を復元するクラスタのバックアップ ファイルだけを選択します。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）] ウィンドウで、復元する機能を選択します。

画面には、復元する機能のうち、バックアップ ファイルに保存された機能のみが表示されます。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウで、[1 ステップでの復元（One-Step Restore）] をクリックします。

このオプションは、復元対象として選択されたバックアップ ファイルがクラスタのバックアップ ファイルであり、復元対象として選択された機能に、パブリッシャとサブスクライバの両方

のノードに登録された機能が含まれている場合にのみ、[復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウに表示されます。詳細については、最初のノードのみの復元 （133 ページ）および後続クラスタ ノードの復元 （135 ページ）を参照してください。

（注） パブリッシャがクラスタ対応になりませんでした。「*1* ステップでの復元を開始できません（*Publisher has failed to become cluster aware. Cannot start one-step restore*）」というステータス メッセージが表示されたら、パブリッシャ ノードを復元してからサブスクライバ ノードを復元する必要があります。詳細については、「関連項目」を参照してください。

このオプションでは、パブリッシャがクラスタ対応になり、そのためには5分かかります。このオプションをクリックすると、ステータス メッセージに「「パブリッシャがクラスタ対応になるまで5分間待機してください。この期間にバックアップまたは復元処理を開始しないでください。（Please wait for 5 minutes until Publisher becomes cluster aware and do not start any backup or restore activity in this time period.）」」と表示されます。

この待ち時間の経過後に、パブリッシャがクラスタ対応になると、「「パブリッシャがクラスタ対応になりました」が表示されます。サーバを選択し、[復元（Restore）] をクリックしてクラスタ全体の復元を開始してください。（Please select the servers and click on Restore to start the restore of entire cluster）」」というステータス メッセージが表示されます。

この待ち時間の経過後、パブリッシャがクラスタ対応にならない場合、「パブリッシャがクラスタ対応にならなかったため、1 ステップでの復元を開始できません。通常の 2 ステップでの復元を実行してください。（Publisher has failed to become cluster aware. Cannot start one-step restore. Please go ahead and do a normal two-step restore.）」というステータス メッセージが表示されます。クラスタ全体を 2 ステップ（パブリッシャとサブスクライバ）で復元するには、最初のノードのみの復元 （133 ページ）と後続クラスタ ノードの復元 （135 ページ）で説明する手順を実行してください。

ステップ 9 復元するノードの選択を求められたら、クラスタ内のすべてのノードを選択します。

最初のノードを復元すると、ディザスタ リカバリ システムが自動的に後続ノードに Cisco Unified Communications Manager データベース（CCMDB）を復元します。そのため、復元しているノードの数とデータベースのサイズによっては、数時間かかることがあります。

ステップ 10 [復元（Restore）] をクリックします。
クラスタ内のすべてのノードでデータが復元されます。

ステップ 11 [復元ステータス（Restore Status）] ウィンドウの [完了率（Percentage Complete）] フィールドに 100% と表示されたら、サーバを再起動します。クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

次のタスク

- （オプション）復元のステータスを表示するには、次を参照してください： 復元ジョブステータスのチェック （142 ページ）
- ノードを再起動するには、次を参照してください： ノードの再起動 （141 ページ）

関連トピック

最初のノードのみの復元 （133 ページ）
後続クラスタ ノードの復元 （135 ページ）

クラスタ全体の復元

主要なハード ドライブで障害またはアップグレードが発生した場合や、ハード ドライブを移行する場合には、クラスタ内のすべてのノードの再構築が必要です。クラスタ全体を復元するには、次の手順を実行します。

ネットワーク カードの交換やメモリの増設など他のほとんどのハードウェア アップグレードでは、次の手順を実行する必要はありません。

手順

ステップ 1 ディザスタ リカバリ システムから、**[復元（Restore）] > [復元ウィザード（Restore Wizard）]** を選択します。

ステップ 2 [バックアップ デバイスの選択（Select Backup Device）] エリアで、復元する適切なバックアップ デバイスを選択します。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）] ウィンドウで、復元するバックアップ ファイルを選択します。

（注） バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）] ウィンドウで [次へ（Next）] をクリックします。

ステップ 7 [復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウで復元ノードの選択を求められたら、すべてのノードを選択します。

ステップ 8 [復元（Restore）] をクリックして、データを復元します。

最初のノードを復元すると、ディザスタ リカバリ システムが自動的に後続ノードに Cisco Unified Communications Manager データベース（CCMDB）を復元します。そのため、ノードの数とデータベースのサイズによっては、最大数時間かかることがあります。

すべてのノードでデータが復元されます。

（注） 復元プロセス中、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] または [ユーザ オプション（User Options）] に関するタスクを実行しないでください。

復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

ステップ 9 復元プロセスが完了したら、サーバを再起動します。サーバの再起動方法の詳細については、「次の作業」セクションを参照してください。

（注） 必ず最初のノードを再起動してから、後続ノードを再起動してください。

最初のノードが再起動し、Cisco Unified Communications Manager の復元後のバージョンが実行されたら、後続ノードを再起動します。

ステップ 10 レプリケーションはクラスタのリブート後に自動的にセットアップされます。『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の説明に従って 「utils dbreplication runtimestate」 CLI コマンドを使用して、すべてのノードで [レプリケーション ステータス（Replication Status）] の値を確認します。各ノードの値は 2 になっているはずです。

（注） クラスタのサイズによっては、後続ノードの再起動後に、後続ノードでのデータベース レプリケーションが完了するまでに時間がかかる場合があります。

ヒント レプリケーションが正しくセットアップされない場合は、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』の説明に従って「utils dbreplication rebuild」CLI コマンドを使用します。

次のタスク

- （オプション）復元のステータスを表示するには、次を参照してください。 復元ジョブ ステータスのチェック （142 ページ）
- ノードを再起動するには、次を参照してください： ノードの再起動 （141 ページ）

前回正常起動時の設定へのノードまたはクラスタの復元

前回正常起動時の設定にノードまたはクラスタを復元するには、次の手順に従います。

始める前に

- 復元ファイルに、バックアップ ファイルで設定されているホスト名、IP アドレス、DNS 設定、および配置タイプが含まれていることを確認します。
- サーバにインストールされている Cisco Unified Communications Manager のバージョンが復元するバックアップ ファイルのバージョンに一致することを確認します。
- この手順は、前回正常起動時の設定にノードを復元する場合にのみ使用してください。

手順

ステップ 1 ディザスタ リカバリ システムから、**[復元（Restore）] > [復元ウィザード（Restore Wizard）]** を選択します。

ステップ 2 [バックアップ デバイスの選択（Select Backup Device）] 領域で、復元する適切なバックアップ デバイスを選択します。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）] ウィンドウで、復元するバックアップ ファイルを選択します。

（注） バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）] ウィンドウで、[次へ（Next）] をクリックします。

ステップ 7 復元ノードを選択するように求められたら、該当するノードを選択します。
選択したノードにデータが復元されます。

ステップ 8 クラスタ内のすべてのノードを再起動します。後続の Cisco Unified Communications Manager ノードを再起動する前に、最初の Cisco Unified Communications Manager ノードを再起動します。クラスタに Cisco IM and Presence ノードもある場合は、最初の Cisco IM and Presence ノードを再起動してから、後続の IM and Presence ノードを再起動します。詳細については、「次の作業」の項を参照してください。

ノードの再起動

データを復元したら、ノードを再起動する必要があります。

パブリッシャ ノード（最初のノード）を復元したら、最初にパブリッシャ ノードを再起動する必要があります。サブスクラバ ノードは必ず、パブリッシャ ノードが再起動し、ソフトウェアの復元されたバージョンを正常に実行し始めた後で再起動してください。

注意 この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。

再起動する必要があるクラスタ内のすべてのノードでこの手順を実行します。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から、**[設定（Settings）] > [バージョン（Version）]** を選択します。

ステップ 2 ノードを再起動するには、[再起動（Restart）] をクリックします。

ステップ 3 レプリケーションはクラスタのリブート後に自動的に設定されます。**utils dbreplication runtimestate** CLI コマンドを使用して、すべてのノードで [レプリケーション ステータス（Replication Status）] 値を確認します。各ノードの値は 2 になっているはずです。CLI コマンドに関する情報は、後述の「関連項目」の項を参照してください。

レプリケーションが正しくセットアップされない場合は、『*Command Line Reference Guide for Cisco Unified Communications Solutions*』の説明に従って **utils dbreplication reset** CLI コマンドを使用します。CLI コマンドに関する情報は、後述の「関連項目」の項を参照してください。

（注） クラスタのサイズによっては、後続ノードの再起動後に、後続ノードでのデータベース レプリケーションが完了するまでに数時間かかる場合があります。

次のタスク

（オプション）復元のステータスを表示するには、復元ジョブ ステータスのチェック （142 ページ）を参照してください。

関連トピック

『Cisco Unified Communications Manager (CallManager) Command References』

復元ジョブ ステータスのチェック

次の手順に従って、復元ジョブ ステータスをチェックします。

手順

ステップ 1 ディザスタ リカバリ システムで、**[復元（Restore）] > [現在のステータス（Current Status）]** を選択します。

ステップ 2 [復元ステータス（Restore Status）] ウィンドウで、ログ ファイル名のリンクをクリックし、復元ステータスを表示します。

復元履歴の表示

復元履歴を参照するには、次の手順を実行します。

手順

ステップ 1 [Disaster Recovery System] で、**[復元（Restore）] > [履歴（History）]** を選択します。

ステップ 2 [復元履歴（Restore History）] ウィンドウで、ファイル名、バックアップ デバイス、完了日、結果、バージョン、復元された機能、失敗した機能など、実行した復元を表示できます。

[復元履歴（Restore History）] ウィンドウには、最新の 20 個の復元ジョブだけが表示されます。

データ認証

トレース ファイル

トラブルシューティングを行う際、またはログの収集中には、トレースファイルの保存先として次の場所が使用されます。

マスター エージェント、GUI、各ローカル エージェント、および JSch ライブラリのトレースファイルは次の場所に書き込まれます。

- マスター エージェントの場合、トレース ファイルは platform/drf/trace/drfMA0* にあります。
- 各ローカル エージェントの場合、トレース ファイルは platform/drf/trace/drfLA0* にあります。
- GUI の場合、トレース ファイルは platform/drf/trace/drfConfLib0* にあります。
- JSch の場合、トレース ファイルは platform/drf/trace/drfJSch* にあります。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html）を参照してください。

コマンドライン インターフェイス

ディザスタ リカバリ システムでは、次の表に示すように、バックアップおよび復元機能のサブセットにコマンドラインからアクセスできます。これらのコマンドの内容とコマンドラインインターフェイスの使用方法の詳細については、『*Command Line Interface（CLI）Reference Guide for Cisco Unified Presence*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html）を参照してください。

表 8: ディザスタ リカバリ システムのコマンドライン インターフェイス

コマンド	説明
utils disaster_recovery estimate_tar_size	SFTP/Local デバイスからのバックアップ tar の概算サイズを表示し、機能リストのパラメータを 1 つ要求します。

コマンド	説明
utils disaster_recovery backup	ディザスタ リカバリ システムのインターフェイスに設定されている機能を使用して、手動バックアップを開始します。
utils disaster_recovery jschLogs	JSch ライブラリのロギングを有効または無効にします。
utils disaster_recovery restore	復元を開始します。復元するバックアップ場所、ファイル名、機能、およびノードを指定するためのパラメータが必要です。
utils disaster_recovery status	進行中のバックアップ ジョブまたは復元ジョブのステータスを表示します。
utils disaster_recovery show_backupfiles	既存のバックアップ ファイルを表示します。
utils disaster_recovery cancel_backup	進行中のバックアップ ジョブをキャンセルします。
utils disaster_recovery show_registration	現在設定されている登録を表示します。
utils disaster_recovery device add	ネットワーク デバイスを追加します。
utils disaster_recovery device delete	デバイスを削除します。
utils disaster_recovery device list	すべてのデバイスを一覧表示します。
utils disaster_recovery schedule add	スケジュールを追加します。
utils disaster_recovery schedule delete	スケジュールを削除します。
utils disaster_recovery schedule disable	スケジュールを無効にします。
utils disaster_recovery schedule enable	スケジュールを有効にします。
utils disaster_recovery schedule list	すべてのスケジュールを一覧表示します。
utils disaster_recovery backup	ディザスタ リカバリ システムのインターフェイスに設定されている機能を使用して、手動バックアップを開始します。
utils disaster_recovery restore	復元を開始します。復元するバックアップ場所、ファイル名、機能、およびノードを指定するためのパラメータが必要です。
utils disaster_recovery status	進行中のバックアップ ジョブまたは復元ジョブのステータスを表示します。
utils disaster_recovery show_backupfiles	既存のバックアップ ファイルを表示します。

コマンド	説明
utils disaster_recovery cancel_backup	進行中のバックアップ ジョブをキャンセルします。
utils disaster_recovery show_registration	現在設定されている登録を表示します。

アラームおよびメッセージ

アラームおよびメッセージ

ディザスタ リカバリ システムは、バックアップまたは復元手順の実行時に発生するさまざまなエラーのアラームを発行します。次の表に、ディザスタ リカバリ システムのアラームの一覧を記載します。

表 *9:* ディザスタ リカバリ システムのアラームとメッセージ

アラーム名	説明	説明
DRFBackupDeviceError	DRF バックアップ プロセスでデバイスへのアクセスに関する問題が発生しています。	DRS バックアップ プロセスでデバイスへのアクセス中にエラーが発生しました。
DRFBackupFailure	シスコ DRF バックアップ プロセスが失敗しました。	DRS バックアップ プロセスでエラーが発生しました。
DRFBackupInProgress	別のバックアップの実行中は、新規バックアップを開始できません。	DRS は、別のバックアップの実行中は新規バックアップを開始できません。
DRFInternalProcessFailure	DRF 内部プロセスでエラーが発生しました。	DRS 内部プロセスでエラーが発生しました。
DRFLA2MAFailure	DRF ローカル エージェントが、マスター エージェントに接続できません。	DRS ローカル エージェントが、マスター エージェントに接続できません。
DRFLocalAgentStartFailure	DRF ローカル エージェントが開始されません。	DRS ローカル エージェントがダウンしている可能性があります。
DRFMA2LAFailure	DRF マスター エージェントがローカル エージェントに接続しません。	DRS マスター エージェントがローカル エージェントに接続できません。

アラーム名	説明	説明
DRFMABackupComponentFailure	DRF は、少なくとも 1 つのコンポーネントをバックアップできません。	DRS は、コンポーネントのデータをバックアップするように要求しましたが、バックアップ プロセス中にエラーが発生し、コンポーネントはバックアップされませんでした。
DRFMABackupNodeDisconnect	バックアップされるノードが、バックアップの完了前にマスター エージェントから切断されました。	DRS マスター エージェントが Cisco Unified Communications Manager ノードでバックアップ操作を実行しているときに、そのノードはバックアップ操作が完了する前に切断されました。
DRFMARestoreComponentFailure	DRF は、少なくとも 1 つのコンポーネントを復元できません。	DRS は、コンポーネントのデータを復元するように要求しましたが、復元プロセス中にエラーが発生し、コンポーネントは復元されませんでした。
DRFMARestoreNodeDisconnect	復元されるノードが、復元の完了前にマスター エージェントから切断されました。	DRS マスター エージェントが Cisco Unified Communications Manager ノードで復元操作を実行しているときに、そのノードは復元操作が完了する前に切断されました。
DRFMasterAgentStartFailure	DRF マスター エージェントが開始されませんでした。	DRS マスター エージェントがダウンしている可能性があります。
DRFNoRegisteredComponent	使用可能な登録済みコンポーネントがないため、バックアップが失敗しました。	使用可能な登録済みコンポーネントがないため、DRS バックアップが失敗しました。
DRFNoRegisteredFeature	バックアップする機能が選択されませんでした。	バックアップする機能が選択されませんでした。
DRFRestoreDeviceError	DRF 復元プロセスでデバイスへのアクセスに関する問題が発生しています。	DRS 復元プロセスは、デバイスから読み取ることができません。

アラーム名	説明	説明
DRFRestoreFailure	DRF 復元プロセスが失敗しました。	DRS 復元プロセスでエラーが発生しました。
DRFSftpFailure	DRF SFTP 操作でエラーが発生しています。	DRS SFTP 操作でエラーが発生しています。
DRFSecurityViolation	DRF システムが、セキュリティ違反となる可能性がある悪意のあるパターンを検出しました。	DRF ネットワーク メッセージには、コード インジェクションやディレクトリ トラバーサルなど、セキュリティ違反となる可能性がある悪意のあるパターンが含まれています。DRF ネットワーク メッセージがブロックされています。
DRFTruststoreMissing	ノードで IPsec 信頼ストアが見つかりません。	ノードで IPsec 信頼ストアが見つかりません。DRF ローカル エージェントが、マスター エージェントに接続できません。
DRFUnknownClient	パブリッシャの DRF マスター エージェントが、クラスタ外部の不明なサーバからクライアント接続要求を受け取りました。要求は拒否されました。	パブリッシャの DRF マスター エージェントが、クラスタ外部の不明なサーバからクライアント接続要求を受け取りました。要求は拒否されました。
DRFBackupCompleted	DRF バックアップが正常に完了しました。	DRF バックアップが正常に完了しました。
DRFRestoreCompleted	DRF 復元が正常に完了しました。	DRF 復元が正常に完了しました。
DRFNoBackupTaken	現在のシステムの有効なバックアップが見つかりませんでした。	アップグレード/移行または新規インストール後に、現在のシステムの有効なバックアップが見つかりませんでした。
DRFComponentRegistered	DRF により、要求されたコンポーネントが正常に登録されました。	DRF により、要求されたコンポーネントが正常に登録されました。
DRFRegistrationFailure	DRF 登録操作が失敗しました。	内部エラーが原因で、コンポーネントに対する DRF 登録操作が失敗しました。

アラーム名	説明	説明
DRFComponentDeRegistered	DRF は正常に要求されたコンポーネントの登録をキャンセルしました。	DRF は正常に要求されたコンポーネントの登録をキャンセルしました。
DRFDeRegistrationFailure	コンポーネントの DRF 登録解除リクエストが失敗しました。	コンポーネントの DRF 登録解除リクエストが失敗しました。
DRFFailure	DRF バックアップまたは復元プロセスが失敗しました。	DRF バックアップまたは復元プロセスでエラーが発生しました。
DRFRestoreInternalError	DRF 復元オペレーションでエラーが発生しました。復元は内部的にキャンセルされました。	DRF 復元オペレーションでエラーが発生しました。復元は内部的にキャンセルされました。
DRFLogDirAccessFailure	DRF は、ログディレクトリにアクセスできませんでした。	DRF は、ログディレクトリにアクセスできませんでした。
DRFDeRegisteredServer	DRF がサーバのすべてのコンポーネントを自動的に登録解除しました。	サーバが Unified Communications Manager クラスタから切断されている可能性があります。
DRFSchedulerDisabled	設定された機能がバックアップで使用できないため、DRF スケジューラは無効になっています。	設定された機能がバックアップで使用できないため、DRF スケジューラは無効になっています
DRFSchedulerUpdated	機能が登録解除されたため、DRF でスケジュールされたバックアップ設定が自動的に更新されます。	機能が登録解除されたため、DRF でスケジュールされたバックアップ設定が自動的に更新されます

ライセンス予約

ライセンス予約

Unified Communication Manager を有効にした特定のライセンス予約に対して復元操作を実行した後に、次の手順に従います。

表 *10*：ライセンス予約のディザスタ リカバリ システム

復元後の状態	CSSM 上の製品	ソリューション
未登録	可	シスコに連絡して CSSM から製品を削除し、製品から登録してください
	不可	何もする必要はありません
予約を実行中です	可	次のいずれかの手順を実行します 手順 1： **1.** CSSM から製品の承認コードを取得します。 **2.** 承認コード **ライセンス スマート予約の戻り値承認「<authorization-code>」**を指定して、以下の CLI を実行します 手順 2： **1.** シスコに連絡して CSSM から製品を削除してください
	不可	製品**ライセンス スマート予約キャンセル**から、CLI を実行します
REGISTERED	可	**1.** 製品から以下の CLI **ライセンス スマート予約戻り**を実行します。予約戻りコードがコンソールに出力されます。 **2.** 製品を削除するには、CSSM で予約戻りコードを入力します。
	不可	製品**ライセンス スマート予約戻り**から、CLI を実行します

復元の連携動作と制約事項

復元の制約事項

ディザスタ リカバリ システムを使用して Cisco Unified Communications Manager または IM and Presence Service を復元する場合、以下の制約事項が適用されます。

表 *11 :* 復元の制約事項

制約事項	説明
エクスポートの制限	制限されたバージョンの DRS バックアップは、制限されたバージョンにのみ復元できます。また、制限されていないバージョンのバックアップは、制限されていないバージョンにのみ復元できます。Cisco Unified Communications Manager の米国輸出無制限バージョンにアップグレードした場合、その後、このソフトウェアの米国輸出制限バージョンへのアップグレード、または新規インストールを実行できなくなります。
プラットフォームの移行	ディザスタ リカバリ システムを使用してプラットフォーム間で（たとえば、Windows から Linux へ、または Linux から Windows へ）データを移行することはできません。復元は、バックアップと同じ製品バージョンで実行する必要があります。Windows ベースのプラットフォームから Linux ベースのプラットフォームへのデータ移行については、『*Data Migration Assistant User Guide*』を参照してください。
HW の交換と移行	DRS 復元を実行してデータを新しいサーバに移行する場合、新しいサーバに古いサーバが使用していたのと同じ IP アドレスとホスト名を割り当てる必要があります。さらに、バックアップの取得時に DNS が設定されている場合、復元を実行する前に、同じ DNS 設定がある必要があります。 サーバの交換の詳細については、『*Replacing a Single Server or Cluster for Cisco Unified Communications Manager*』ガイドを参照してください。 また、ハードウェアの交換後は、証明書信頼リスト（CTL）クライアントを実行する必要もあります。後続ノード（サブスクライバ）サーバを復元しない場合には、CTL クライアントを実行する必要があります。他の場合、DRS は必要な証明書をバックアップします。詳細については、『*Cisco Unified Communications Manager Security Guide*』の「「Installing the CTL Client」」と「「Configuring the CTL Client 」」の手順を参照してください。

制約事項	説明
クラスタ間のエクステンション モビリティ（Extension Mobility Cross Cluster）	バックアップ時にリモート クラスタにログインしていた Extension Mobility Cross Cluster ユーザは、復元後もログインしたままとなります。

（注） Cisco Unified Communications サーバ コンポーネントの復元が正常に完了した後、Cisco Unified Communications Manager を Cisco Smart Software Manager または Cisco スマート ソフトウェア マネージャ サテライトに登録してください。バックアップを作成する前に製品がすでに登録されていたとしても、その製品を再登録してライセンス情報を更新する必要があります。

Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに製品を登録する方法の詳細については、ご使用のリリースの『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

トラブルシューティング

より小さい仮想マシンへの DRS 復元の失敗

問題

IM and Presence サービス ノードをディスク容量がより小さい VM に復元すると、データベースの復元が失敗することがあります。

原因

大きいディスク サイズから小さいディスク サイズに移行したときに、この障害が発生します。

解決策

2 個の仮想ディスクがある OVA テンプレートから、復元用の VM を展開します。

第 13 章

エンタープライズ パラメータの管理

エンタープライズ パラメータの概要

エンタープライズパラメータは、クラスタ全体ですべてのデバイスやサービスに適用されるデフォルト設定を提供します。たとえば、システムで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を設定します。

ユーザはエンタープライズパラメータを追加または削除できませんが、既存のエンタープライズ パラメータを更新することはできます。エンタープライズ パラメータの設定ウィンドウには、カテゴリ（CCMAdmin パラメータ、CCMUser パラメータ、CDR パラメータなど）ごとにエンタープライズ パラメータが一覧表示されます。

エンタープライズ パラメータの詳細な説明は、[エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウで確認できます。

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

エンタープライズ パラメータ情報の表示

[エンタープライズ パラメータ設定（Enterprise Parameter Configuration）] ウィンドウで、埋め込まれたコンテンツを通してエンタープライズ パラメータに関する情報にアクセスします。

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 次のいずれかの作業を実行します。

- 特定のエンタープライズパラメータの説明を表示するには、パラメータ名をクリックします。
- エンタープライズ パラメータの説明をすべて表示するには、[?] をクリックします。

エンタープライズ パラメータの更新

次の手順を使用して、[エンタープライズパラメータ設定（Enterprise Parameter Configuration）] ウィンドウを開き、システム レベル設定を構成します。

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

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 変更するエンタープライズ パラメータに必要な値を選択します。

ステップ 3 **[保存（Save）]** をクリックします。

次のタスク

デバイスへの設定の適用 （154 ページ）

デバイスへの設定の適用

次の手順を使用して、構成した設定でクラスタ内のすべての影響を受けるデバイスを更新します。

始める前に

エンタープライズ パラメータの更新 （154 ページ）

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 変更を確認してから、[保存（Save）] をクリックします。

ステップ 3 次のいずれかのオプションを選択します。

- システムでリブートするデバイスを判断するには、[設定の適用（Apply Config）] をクリックします。リブートする必要がないデバイスもあります。進行中のコールはドロップされる可能性がありますが、接続されたコールは、デバイス プールに SIP トランクが含まれていない限り、保持されます。
- クラスタ内のすべてのデバイスをリブートするには、[リセット（Reset）] をクリックします。この手順はオフピーク時間帯に実行することをお勧めします。

ステップ 4 確認ダイアログを読んでから、[OK] をクリックします。

デフォルト エンタープライズ パラメータの復元

エンタープライズ パラメータをデフォルト設定にリセットする場合は、次の手順を使用します。一部のエンタープライズパラメータには、設定ウィンドウの列に示すように、推奨値が含まれています、この手順では、これらの値をデフォルト設定として使用します。

手順

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

ステップ 2 [デフォルトに設定（Set to Default）] をクリックします。

ステップ 3 確認プロンプトを読み、[OK] をクリックします。

第 14 章

サーバの管理

サーバの管理の概要

この章では、Cisco Unified Communications Manager ノードのプロパティを管理する方法、プレゼンス サーバのステータスを表示する方法、および Unified Communications Manager サーバのホスト名を設定する方法を説明します。

クラスタからのノードの削除

プレゼンス冗長グループから IM and Presence サービス ノードを安全に削除する必要がある場合は、この手順に従います。

注意 ノードを削除すると、そのプレゼンス冗長グループの残りのノードで、ユーザに対するサービスが中断されます。この手順は必ず、メンテナンス期間中に実行してください。

手順

ステップ 1 **[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Groups）]**ページで、高可用性が有効な場合は無効にします。

ステップ 2 **[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [ユーザ管理（User Management）] > [プレゼンスユーザの割り当て（Assign Presence Users）]**ページで、削除するノードからすべてのユーザの割り当てを解除するか、移動します。

ステップ 3 プレゼンス冗長グループからノードを削除するには、プレゼンス冗長グループの [プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ページの [プレゼンスサーバ（Presence Server）] ドロップダウン リストから、[未選択（Not-Selected）] を選択します。ノードの割り当て解除の結果としてプレゼンス冗長グループ内のサービスが再起動されることを示す警告ダイアログ ボックスが表示されたら、[OK] を選択します。

ステップ 4 **[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [サーバ（Server）]**ページから、割り当て解除されたノードを削除します。このアクションを取り消せないことを示す警告ダイアログ ボックスが表示されたら、[OK] を選択します。

ステップ 5 割り当てを解除したノードのホスト VM またはサーバをシャットダウンします。

削除したサーバをクラスタに戻す

Unified Communications Manager Administration から後続のノード（サブスクライバ）を削除してそれをクラスタに戻す場合に、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[システム（System）] > [サーバ（Server）]** を選択してサーバを追加します。

ステップ 2 後続のノードを Cisco Unified Communications Manager Administration に追加したら、シスコが提供しているソフトウェア キットに付属しているご使用のバージョン用のディスクを使用して、サーバ上でインストールを実行します。

ヒント インストールするバージョンが、パブリッシャ ノード上で動作しているバージョンと一致することを確認します。パブリッシャ上で実行されているバージョンがインストール ファイルと一致しない場合は、インストール プロセス中に [インストール中にアップグレード（Upgrade During Install）] オプションを選択します。インストールの詳細については、『*Installation Guide for Cisco Unified Communications Manager and the IM and Presence Servic*』を参照してください。

ステップ 3 Cisco Unified CM をインストールしたら、その Cisco Unified CM のバージョンをサポートしているインストール マニュアルの説明に従って、後続のノードを設定します。

ステップ 4 Cisco Unified Reporting、RTMT、または CLI にアクセスして、データベース レプリケーションが既存のノード間で発生していることを確認します。必要に応じて、ノード間のデータベース レプリケーションを修復します。

インストール前のクラスタへのノードの追加

ノードをインストールする前に、Cisco Unified Communications Manager Administration を使用して、新しいノードをクラスタに追加します。ノードの追加時に選択するサーバタイプは、インストールしたサーバ タイプと一致する必要があります。

新しいノードをインストールする前に、Cisco Unified Communications Manager Administration を使用して、最初のノードで新しいノードを設定する必要があります。クラスタにノードをインストールするには、『*Cisco Unified Communications ManagerInstallation Guide*』を参照してください。

Cisco Unified Communications Manager のビデオ/音声サーバでは、Cisco Unified Communications Manager ソフトウェアの初期インストール中に追加した最初のサーバがパブリッシャ ノードに指定されます。後続のすべてのサーバ インストールまたは追加は、サブスクライバ ノードに指定されます。クラスタに追加した最初の Cisco Unified Communications Manager IM and Presence ノードが、IM and Presence Service データベース パブリッシャノードに指定されます。

（注） サーバの追加後は、Cisco Unified Communications Manager Administration を使用して、サーバ タイプを変更できなくなります。既存のサーバインスタンスを削除してから、再度、新しいサーバを追加して、正しいサーバ タイプ設定を選択する必要があります。

手順

ステップ 1 **[システム（System）] > [サーバ（Server）]** を選択します。

[サーバの検索/一覧表示（Find and List Servers）] ウィンドウが表示されます。

ステップ 2 [新規追加（Add New）] をクリックします。

[サーバの設定 - サーバを追加（Server Configuration - Add a Server）] ウィンドウが表示されます。

ステップ 3 [サーバ タイプ（Server Type）] ドロップダウン リスト ボックスで、追加するサーバ タイプを選択してから、[次へ（Next）] をクリックします。

- CUCM ビデオ/音声
- CUCM IM and Presence

ステップ 4 [サーバの設定（Server Configuration）] ウィンドウで、適切なサーバ設定を入力します。

サーバ設定フィールドの説明については、「Server Settings」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。

プレゼンス サーバのステータスの表示

IM and Presence Service ノードの重要なサービスのステータスと自己診断テスト結果を確認するには、Cisco Unified Communications Manager Administration を使用します。

手順

ステップ 1 **[システム（System）] > [サーバ（Server）]** を選択します。

[サーバの検索/一覧表示（Find and List Servers）] ウィンドウが表示されます。

ステップ 2 サーバの検索パラメータを選択し、[検索（Find）] をクリックします。

一致するレコードが表示されます。

ステップ 3 [サーバの検索/一覧表示（Find and List Servers）] ウィンドウに表示される IM and Presence サーバを選択します。

[サーバの設定（Server Configuration）] ウィンドウが表示されます。

ステップ 4 [サーバの設定（Server Configuration）] ウィンドウの IM and Presence サーバ情報のセクションで、プレゼンス サーバ ステータスのリンクをクリックします。

サーバの [ノードの詳細（Node Details）] ウィンドウが表示されます。

ホスト名の設定

次の表に、Unified Communications Manager サーバのホスト名を設定できる場所、ホスト名として指定できる文字数、および推奨されるホスト名の先頭文字と最終文字を示します。ホスト名を正しく設定しないと、Unified Communications Manager の一部のコンポーネント（オペレーティング システム、データベース、インストールなど）が期待通りに機能しない可能性があります。

⚠

注意 次の表に示すいずれかの場所でホスト名や IP アドレスを変更する前に、『*Changing the IP Address and Host Name for Cisco Unified Communications Manager*』を参照してください。設定後のホスト名や IP アドレスを正しく更新しないと、Unified Communications Manager に問題が発生することがあります。

表 *12 : Cisco Unified Communications Manager* におけるホスト名の設定

ホスト名の場所	可能な設定	指定できる文字数	推奨されるホスト名の先頭文字	推奨されるホスト名の最終文字
[ホスト名/IP アドレス（Host Name/ IP Address）] フィールド Cisco Unified Communications Manager Administration の **[システム（System）] > [サーバ（Server）]**	クラスタ内のサーバのホスト名を追加または変更できます。	2 ～ 63	英字	英数字
[ホスト名（Hostname）] フィールド Cisco Unified Communications Manager インストールウィザード	クラスタ内のサーバのホスト名を追加できます。	1 ～ 63	英字	英数字
[ホスト名（Hostname）] フィールド Cisco Unified Communications オペレーティングシステムの **[設定（Settings）] > [IP] > [イーサネット（Ethernet）]**	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1 ～ 63	英字	英数字
set network hostname hostname コマンドライン インターフェイス	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1 ～ 63	英字	英数字

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

いずれかの場所でホスト名を設定する前に、次の情報を確認してください。

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

  Unified Communications Manager パブリッシャ ノードをインストールした後は、パブリッシャのホスト名がこのフィールドに自動的に表示されます。Unified Communications Manager サブスクライバ ノードをインストールする前に、Unified Communications Manager パブリッシャ ノードでこのフィールドにサブスクライバ ノードの IP アドレスまたはホスト名を入力してください。

  このフィールドにホスト名を設定できるのは、Unified Communications Manager が DNS サーバにアクセスしてホスト名を IP アドレスに解決できる場合のみです。DNS サーバに Cisco Unified Communications Manager の名前とアドレスの情報が設定されていることを確認してください。

ヒント　DNS サーバに Unified Communications Manager の情報を設定するのに加えて、Cisco Unified Communications Manager のインストール時に DNS 情報を入力します。

- Unified Communications Manager パブリッシャ ノードのインストール時に、ネットワーク情報を設定するために（つまり、スタティック ネットワークを使用する場合に）パブリッシャ サーバのホスト名（必須）と IP アドレスを入力します。

  Unified Communications Manager サブスクライバ ノードのインストール時には、Unified Communications Manager パブリッシャ ノードのホスト名と IP アドレスを入力して、Unified Communications Manager がネットワークの接続性およびパブリッシャとサブスクライバ間の検証を確認できるようにしてください。さらに、サブスクライバ ノードのホスト名と IP アドレスも入力する必要があります。Unified Communications Manager のインストール時にサブスクライバ サーバのホスト名の入力を求められた場合は、Cisco Unified Communications Manager Administration の（[ホスト名/IP アドレス（Host Name/IP Address）] フィールドでサブスクライバ サーバのホスト名を設定した場合に）[サーバの設定（Server Configuration）] ウィンドウに表示される値を入力します。

Kerneldump ユーティリティ

Kerneldump ユーティリティにより、セカンダリ サーバを要求することなしに、該当するマシンでクラッシュ ダンプ ログをローカルに収集できます。

Unified Communications Manager クラスタでは、Kerneldump ユーティリティがサーバで有効であることを確認するだけで、クラッシュ ダンプ情報を収集できます。

（注） シスコでは、より効果的なトラブルシューティングを実現するため、Unified Communications Manager のインストール後に、Kerneldump ユーティリティが有効であることを確認するよう推奨しています。Kerneldump ユーティリティの設定をまだ行っていない場合は、Unified Communications Manager をサポート対象のアプライアンス リリースからアップグレードする前に行ってください。

重要 Kerneldump ユーティリティをイネーブル化またはディセーブル化を行うには、ノードのリブートが必要です。リブートが許容されるウィンドウ以外では、enable コマンドを実行しないでください。

Cisco Unified Communications オペレーティング システムのコマンドライン インターフェイス（CLI）を使用すると、Kerneldump ユーティリティのイネーブル化、ディセーブル化、ステータス確認を実行できます。

次の手順を利用して Kerneldump ユーティリティをイネーブル化します。

ユーティリティによって収集されるファイルの処理

Kerneldump ユーティリティから送信されたクラッシュ情報を表示するには、Cisco Unified Real-Time Monitoring Tool またはコマンドライン インターフェイス（CLI）を使用します。Cisco Unified Real-Time Monitoring Tool を使用して netdump ログを収集するには、[トレースおよびログ セントラル（Trace & Log Central）] の [ファイルの収集（Collect Files）] オプションを選択します。[システム サービス/アプリケーションの選択（Select System Services/Applications）] タブで、[Kerneldump ログ（Kerneldump logs）] チェックボックスをオンにします。Cisco Unified Real-Time Monitoring Tool を使用したファイルの収集の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

CLI を使用して kerneldump ログを収集するには、クラッシュ ディレクトリのファイルに対して「「file」」CLI コマンドを使用します。これらは 「activelog」 のパーティションの下にあります。ログ ファイル名は、kerneldump クライアントの IP アドレスで始まり、ファイルが作成された日付で終わります。ファイル コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

Kerneldump ユーティリティの有効化

次の手順を利用して Kerneldump ユーティリティを有効化します。カーネル クラッシュが発生した場合、ユーティリティは、クラッシュの収集とダンプのメカニズムを提供します。ローカル サーバまたは外部サーバにログをダンプするユーティリティを設定できます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 次のいずれかを実行します。

- ローカル サーバ上のカーネル クラッシュをダンプするには、`utils os kernelcrash enable` CLI コマンドを実行します。
- 外部サーバにカーネル クラッシュをダンプするには、外部サーバの IP アドレスを指定して `utils os kerneldump ssh enable <ip_address>` CLI コマンドを実行します。

ステップ 3 サーバをリブートします。

例

（注） kerneldump ユーティリティを無効にする必要がある場合、`utils os kernelcrash disable` CLI コマンドを実行してローカル サーバのコア ダンプを無効にし、`utils os kerneldump ssh disable <ip_address>` CLI コマンドを実行して外部サーバ上のユーティリティを無効にします。

次のタスク

コア ダンプの指示に従ってリアルタイム モニタリング ツールで電子メール アラートを設定します。詳細については、コア ダンプの電子メール アラートの有効化（164 ページ）を参照してください。

kerneldump ユーティリティおよびトラブルシューティングについては、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

コア ダンプの電子メール アラートの有効化

コア ダンプが発生するたびに管理者に電子メールを送信するようにリアルタイム モニタリング ツ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 **[システム（System）] > [ツール（Tools）] > [アラート セントラル）Alert Central）]** の順に選択します。

ステップ 2 [CoreDumpFileFound] アラートを右クリックし、[アラート/プロパティの設定（Set Alert/Properties）] を選択します。

ステップ 3 ウィザードの指示に従って優先条件を設定します。

a) [アラート プロパティ：電子メール通知（Alert Properties: Email Notification）] ポップアップで、[電子メールの有効化（Enable Email）] がオンになっていることを確認し、[設定（Configure）] をクリックしてデフォルトのアラート アクションを設定します。これにより管理者に電子メールが送信されます。

b) プロンプトに従って、受信者電子メール アドレスを [追加（Add）]します。このアラートがトリガーされると、デフォルトのアクションは、このアドレスへの電子メールの送信になります。

c) **[保存（Save）]** をクリックします。

ステップ 4 デフォルトの電子メール サーバを設定します。

a) **[システム（System）]** > **[ツール（Tools）]** > **[アラート（Alert）]** > **[電子メール サーバの設定（Config Email Server）]** の順に選択します。

b) 電子メール サーバの設定を入力します。

c) [OK] をクリックします。

第 V 部

セキュリティの管理

第 15 章

SAML シングル サインオンの管理

SAML シングル サインオンの概要

定義された一連の Cisco アプリケーションのうちの 1 つにサインインした後は、SAML シングル サインオン（SSO）を使用して、それらすべてのアプリケーションにアクセスできます。SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。これは、ユーザを認証するために、サービス プロバイダー（Cisco Unified Communications Manager など）が使用する認証プロトコルです。SAML では、ID プロバイダー（IdP）とサービスプロバイダーとの間でセキュリティ認証情報が交換されます。この機能は、さまざまなアプリケーションにわたり、共通の資格情報と関連情報を使用するための安全な機構を提供します。

SAML SSO は、IdP とサービス プロバイダーの間でのプロビジョニング プロセスの一部として、メタデータと証明書を交換することで、信頼の輪（CoT）を確立します。サービスプロバイダーは IdP のユーザ情報を信頼して、さまざまなサービスやアプリケーションへのアクセスを許可します。

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

iOS 上での Cisco Jabber の証明書ベースの SSO 認証のオプトイン制御

このリリースの Cisco Unified Communications Manager には、iOS での Cisco Jabber の SSO ログイン動作を ID プロバイダー（IdP）によって制御するためのオプトイン設定オプションが導入

されています。このオプションを使用すると、制御されたモバイル デバイス管理（MDM）環境内で、Cisco Jabber が IdP による証明書ベースの認証を実行できるようになります。

オプトイン制御を設定するには、Cisco Unified Communications Manager で [iOS の SSO ログイン動作（SSO Login Behavior for iOS）] エンタープライズ パラメータを使用します。

（注） このパラメータのデフォルト値を変更する前に、http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html で Cisco Jabber 機能のサポートおよびドキュメントを参照して、SSO ログイン動作と証明書ベースの認証に対する iOS 上での Cisco Jabber のサポートを確認してください。

この機能を有効にするには、iOS Cisco Jabber の SSO ログインの動作設定 （172 ページ）の手順を参照してください。

SAML シングル サインオンの前提条件

- Cisco Unified Communications Manager クラスタに DNS が設定されていること
- ID プロバイダー（IdP）サーバ
- IdP サーバによって信頼され、システムでサポートされる LDAP サーバ

SAML SSO 機能のテストは、SAML 2.0 を使用した以下の IdP で行われています。

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

サードパーティ アプリケーションは、次の設定要件を満たす必要があります。

- 必須属性の 「uid」 が IdP で設定されていること。この属性は、Cisco Unified Communications Manager の LDAP と同期されたユーザ ID に使用されている属性と一致している必要があります。

（注） Cisco Unified Communications Manager では現在のところ、ユーザ ID 設定の LDAP 属性として sAMAccountName オプションのみをサポートしています。

必須属性マッピングの設定の詳細については、IdP の製品マニュアルを参照してください。

- SAML SSO に参加するすべてのエンティティのクロックを同期させる必要があります。クロックの同期の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）の「「NTP Settings」」を参照してください。

SAML シングル サインオンの管理

SAML シングル サインオンの有効化

（注） 同期エージェントの確認テストに合格するまで、SAML SSO を有効にすることができません。

始める前に

- ユーザ データが Unified Communications Manager データベースに同期されていることを確認します。詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html で、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
- Cisco Unified CM IM and Presence サービスと Cisco Sync Agent サービスのデータ同期が完了していることを確認します。このテストのステータスをチェックするには、**[Cisco Unified CM IM and Presence Administration]** > **[診断（Diagnostics）]** > **[システム トラブルシューター（System Troubleshooter）]** を選択します。[Sync Agent が関連データ（デバイス、ユーザ、ライセンス情報など）を使用して同期したことを確認する（Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information）]「」 テストは、データ同期が正常に完了した場合にテスト合格の結果が示されています。
- Cisco Unified CM の管理へのアクセスを有効にするには、少なくとも 1 人の LDAP 同期ユーザが Standard CCM Super Users グループに追加されていることを確認します。詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html で、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
- IdP とサーバ間の信頼関係を設定するには、IdP から信頼メタデータ ファイルを取得し、それをすべてのサーバにインポートする必要があります。

手順

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

ステップ 2 [SAML SSO の有功化（Enable SAML SSO）] をクリックします。

ステップ 3 すべてのサーバ接続が再起動されることを通知する警告メッセージが表示されたら、[続行（Continue）] をクリックします。

ステップ 4 [参照（Browse）] をクリックし、IdP メタデータ ファイルを探してアップロードします。

ステップ 5 [IdP メタデータのインポート（Import IdP Metadata）] をクリックします。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [信頼メタデータ ファイルセットのダウンロード（Download Trust Metadata Fileset）] をクリックして、サーバ メタデータをシステムにダウンロードします。

ステップ 8 IdP サーバ上にサーバ メタデータをアップロードします。

ステップ 9 [次へ（Next）] をクリックして続行します。

ステップ 10 有効な管理者 ID のリストから、管理者権限を持つ LDAP 同期ユーザを選択します。

ステップ 11 [テストを実行（Run Test）] をクリックします。

ステップ 12 有効なユーザ名およびパスワードを入力します。

ステップ 13 成功メッセージが表示されたら、ブラウザ ウィンドウを閉じます。

ステップ 14 [完了（Finish）] をクリックし、Web アプリケーションが再起動するまで 1～2 分待ちます。

iOS Cisco Jabber の SSO ログインの動作設定

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

（注） [iOS 向け SSO ログイン動作（SSO Login Behavior for iOS）] パラメータには次のオプションが含まれます。

- [組み込みブラウザの使用（Use Embedded Browser）]：このオプションを有効にすると、Cisco Jabber は SSO の認証に、組み込みブラウザを使用します。このオプションにより、バージョン 9 より前の iOS デバイスのネイティブ Apple Safari ブラウザで、クロス起動なしの SSO を使用できるようになります。このオプションは、デフォルトで有効です。
- [ネイティブ ブラウザの使用（Use Native Browser）]：このオプションを有効にすると、Cisco Jabber は、iOS デバイスで Apple Safari フレームワークを使用し、MDM の導入で、ID プロバイダー（IdP）を利用する証明書ベースの認証を実行します。

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

ステップ 3 **[保存（Save）]** をクリックします。

アップグレード後の WebDialer 上での SAML シングル サインオンの有効化

次のタスクに従って、アップグレード後に Cisco WebDialer 上で SAML シングル サインオンを再度アクティブ化します。SAML シングル サインオンを有効化する前に Cisco WebDialer をアクティブ化すると、デフォルトで、Cisco WebDialer 上で SAML シングル サインオンが有効になりません。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco WebDialer サービスの非アクティブ化 （174 ページ）	Cisco WebDialer Web サービスがすでにアクティブになっている場合は、それを非アクティブにします。
ステップ 2	SAML シングル サインオンの無効化 （174 ページ）	SAML シングル サインオンがすでに有効になっている場合は、それを無効にします。
ステップ 3	Cisco WebDialer サービスのアクティブ化 （174 ページ）	
ステップ 4	SAML シングル サインオンの有効化 （171 ページ）	

Cisco WebDialer サービスの非アクティブ化

Cisco WebDialer Web サービスがすでにアクティブになっている場合は、それを非アクティブにします。

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（Servers）] ドロップダウン リストから、リストされている Cisco Unified Communications Manager サーバを選択します。

ステップ 3 [CTI サービス（CTI Services）] で、[Cisco WebDialer Web サービス（Cisco WebDialer Web Service）] 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。

次のタスク

SAML シングル サインオンの無効化 （174 ページ）

SAML シングル サインオンの無効化

SAML シングル サインオンがすでに有効になっている場合は、それを無効にします。

始める前に

Cisco WebDialer サービスの非アクティブ化 （174 ページ）

手順

CLI から、**utils sso disable** コマンドを実行します。

次のタスク

Cisco WebDialer サービスのアクティブ化 （174 ページ）

Cisco WebDialer サービスのアクティブ化

始める前に

SAML シングル サインオンの無効化 （174 ページ）

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（Servers）] ドロップダウン リストから、リストされている Cisco 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 WebDialer Web サービス（Cisco WebDialer Web 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 Cisco Unified Serviceability から、**[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。

WebDialer 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

SAML シングル サインオンの有効化 （171 ページ）

リカバリ URL へのアクセス

トラブルシューティングのために、SAML シングル サインオンをバイパスして、Cisco Unified Communications Manager Administration インターフェイスと Cisco Unified CM IM and Presence サービス インターフェイスにログインする場合に、リカバリ URL を使用します。たとえば、サーバのドメインまたはホスト名を変更する前に、リカバリ URL を有効にします。リカバリ URL にログインすると、サーバ メタデータの更新が容易になります。

始める前に

- 管理権限を持っているアプリケーション ユーザのみがリカバリ URL にアクセスできます。
- SAML SSO が有効になっている場合は、リカバリ URL がデフォルトで有効になります。CLI からリカバリ URL を有効/無効にすることができます。リカバリ URL を有効または無効にする CLI コマンドの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

手順

ブラウザで、「`https://hostname:8443/ssosp/local/login`」と入力します。

ドメインまたはホスト名変更後のサーバ メタデータの更新

ドメインまたはホスト名の変更後は、この手順を実行するまで、SAML シングル サインオンが機能しません。

（注） この手順を実行しても [SAML シングル サインオン（SAML Single Sign-On）] ウィンドウ にログインできない場合は、ブラウザのキャッシュをクリアしてもう一度ログインしてみてください。

始める前に

リカバリ URL が無効になっている場合、シングル サインオン リンクをバイパスするようには表示されません。リカバリ URL を有効にするには、CLI にログインして次のコマンドを実行します：**utils sso recovery-url enable**。

手順

ステップ 1 Web ブラウザのアドレス バーに次の URL を入力します。

```
https://<Unified CM-server-name>
```

`<Unified CM-server-name>` はホスト名またはサーバの IP アドレスです。

ステップ 2 [シングル サインオンをバイパスするリカバリURL（Recovery URL to bypass Single Sign-On (SSO)）] をクリックします。

ステップ 3 管理者ロールを持つアプリケーション ユーザのクレデンシャルを入力し、[ログイン（Login）] をクリックします。

ステップ 4 Cisco Unified CM の管理で、**[システム（System）]** > **[SAML シングル サインオン（SAML Single Sign-On）]** を選択します。

ステップ 5 [メタデータのエクスポート（Export Metadata）] をクリックしてサーバ メタデータをダウンロードします。

ステップ 6 サーバ メタデータ ファイルを IdP にアップロードします。

ステップ 7 [テストを実行（Run Test）] をクリックします。

ステップ 8 有効なユーザ ID とパスワードを入力します。

ステップ 9 成功のメッセージが表示されたら、ブラウザウィンドウを閉じます。

サーバ メタデータの手動プロビジョニング

ID プロバイダーで複数の UC アプリケーション用の単一接続をプロビジョニングするには、ID プロバイダーとサービス プロバイダー間の信頼の輪を設定しながら、サーバ メタデータを手

動でプロビジョニングする必要があります。信頼の輪の設定方法については、IdP製品のマニュアルを参照してください。

一般的なURL構文は次のとおりです。

```
https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>
```

手順

サーバメタデータを手動でプロビジョニングするには、Assertion Customer Service（ACS）URLを使用します。

例：

サンプルACS URL：

```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com"
index="0"/>
```

第 16 章

証明書の管理

証明書の概要

システムでは、自己署名証明書とサードパーティの署名付き証明書が使用されます。送信元から宛先までのデータ整合性を確保するために、デバイスのセキュア認証、データの暗号化、データのハッシュを行う際に、システム内のデバイス間で証明書を使用します。証明書を使用することにより、帯域幅、通信、操作のセキュアな転送が可能になります。

証明書を使用する際、意図した Web サイト、電話、FTP サーバなどのエンティティとの間でデータがどのように暗号化され共有されているかを理解し、それを定義することが最も重要な部分です。

システムが証明書を信頼するということは、システムにプレインストールされている証明書によって、適切な接続先と情報を共有していることが完全に確信されているということです。そうでない場合、システムはこれらのポイント間の通信を終了します。

証明書を信頼するには、サードパーティ認証局（CA）によって信頼がすでに確立されている必要があります。

まずデバイスが CA 証明書と中間証明書の両方を信頼できると認識していることが必要であり、そうであるならデバイスは Secure Socket Layer（SSL）ハンドシェイクというメッセージの交換によって提供されるサーバ証明書を信頼することができます。

（注） Tomcat 用の EC ベースの証明書がサポートされています。この新しい証明書を tomcat-ECDSA といいます。詳細については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』の「Enhanced TLS Encryption on IM and Presence Service」の章を参照してください。

Tomcat インターフェイスの EC 暗号はデフォルトで無効になっています。Cisco Unified Communications Manager または IM and Presence Service で [HTTPS 暗号（HTTPS Ciphers）] のエンタープライズパラメータを使用して、これらを有効にできます。このパラメータを変更すると、すべてのノードで Cisco Tomcat サービスを再起動する必要があります。

EC ベースの証明書の詳細については、Cisco Unified Communications Manager and IM and Presence Service リリース ノートの「ECDSA Support for Common Criteria for Certified Solutions」を参照してください。

サードパーティの署名付き証明書または証明書チェーン

アプリケーション証明書に署名した認証局の認証局ルート証明書をアップロードします。下位認証局がアプリケーション証明書に署名した場合は、下位認証局の認証局ルート証明書をアップロードする必要があります。すべての認証局証明書の PKCS#7 形式の証明書チェーンもアップロードできます。

認証局ルート証明書およびアプリケーション証明書は、同じ [証明書のアップロード（Upload Certificate）] ダイアログボックスを使用してアップロードできます。認証局ルート証明書または認証局証明書だけが含まれる証明書チェーンをアップロードする場合は、certificate type-trust 形式の証明書名を選択します。アプリケーション証明書またはアプリケーション証明書と認証局証明書が含まれる証明書チェーンをアップロードする場合は、証明書タイプだけが含まれている証明書名を選択します。

たとえば、Tomcat 認証局証明書または認証局証明書チェーンをアップロードする場合は [tomcat-trust] を選択します。Tomcat アプリケーション証明書またはアプリケーション証明書と認証局証明書が含まれる証明書チェーンをアップロードする場合は、[tomcat] または [tomcat-ECDSA] を選択します。

CAPF 認証局ルート証明書をアップロードすると、CallManager の信頼ストアにコピーされるため、認証局ルート証明書を個別に CallManager にアップロードする必要はありません。

（注） サードパーティの認証局署名付き証明書が正常にアップロードされると、署名付き証明書を取得するために使用された、最近生成した CSR が削除され、サード パーティの署名付き証明書（アップロードされている場合）を含む既存の証明書が上書きされます。

（注） tomcat-trust、CallManager-trust、および Phone-SAST-trust 証明書がクラスタの各ノードに自動的にレプリケートされます。

（注） DirSync サービスをセキュア モードで実行する場合に必要となるディレクトリの信頼証明書は、tomcat-trust にアップロードすることができます。

サード パーティ認証局証明書

サードパーティ認証局が発行するアプリケーション証明書を使用するには、署名付きのアプリケーション証明書と認証局ルート証明書の両方を認証局から取得するか、アプリケーション証明書と認証局証明書の両方が含まれている PKCS#7 証明書チェーン（Distinguished Encoding Rules [DER]）から取得する必要があります。これらの証明書の取得に関する情報は、認証局から入手してください。証明書を取得するプロセスは、認証局によって異なります。署名アルゴリズムでは RSA 暗号化が使用されている必要があります。

Cisco Unified Communications オペレーティング システムでは、プライバシー強化メール（PEM）エンコード形式で CSR が作成されます。システムは、DER および PEM エンコード形式の証明書と、PEM 形式の PKCS#7 証明書チェーンを受け入れます。認証局プロキシ機能（CAPF）以外のすべての証明書タイプの場合、それぞれのノードについて認証局ルート証明書およびアプリケーション証明書を取得してアップロードする必要があります。

CAPF の場合、最初のノードについてのみ認証局ルート証明書およびアプリケーション証明書を取得してアップロードします。CAPF および Unified Communications Manager の CSR には、認証局へのアプリケーション証明書要求に含める必要のある拡張情報が含まれています。認証局が拡張要求メカニズムをサポートしていない場合は、次の手順に従って X.509 拡張を有効にする必要があります。

- CAPF CSR では、次の拡張情報が使用されます。

```
X509v3 拡張キーの使用： TLS Web サーバ認証、IPSec エンド システム X509v3 キーの使用： デジタル署名、証明書署名
```

- Tomcat および Tomcat-ECDSA の CSR では、次の拡張情報が使用されます。

（注） Tomcat または Tomcat-ECDSA は、キー アグリーメントや IPsec エンド システム キーを使用する必要はありません。

```
X509v3 拡張キー使用： TLS Web サーバ認証、TLS Web クライアント認証、IPSec エンド システム X509v3 キー使用： デジタル署名、キー暗号化、データ暗号化、キー同意
```

- IPsec の CSR では、次の拡張情報が使用されます。

```
X509v3 拡張キー使用： TLS Web サーバ認証、TLS Web クライアント認証、IPSec エンド システム X509v3 キー使用： デジタル署名、キー暗号化、データ暗号化、キー同意
```

- Unified Communications Manager の CSR では、次の拡張情報が使用されます。

```
X509v3 拡張キー使用： TLS Web サーバ認証、TLS Web クライアント認証 X509v3 キー使用： デジタル署名、キー暗号化、データ暗号化、キー同意
```

- IM and Presence Service cup および cup-xmpp 証明書の CSR は、次の拡張機能を使用します。

```
X509v3 拡張キー使用：TLS Web サーバ認証、TLS Web クライアント認証、IPSec エンド システム X509v3 キー使用：デジタル署名、キー暗号化、データ暗号化、キー アグリーメント
```

（注） 使用する証明書に対してCSRを生成し、SHA256署名を使用してサードパーティ認証局に署名させることもできます。この署名付き証明書を Unified Communications Manager に再度アップロードすることで、Tomcat および他の証明書が SHA256 をサポートできるようになります。

CSR キーの用途拡張

次の表には、Unified Communications Manager と IM and Presence Service の CA 証明書の証明書署名要求（CSR）のキーの用途拡張が表示されています。

表 *13 : Cisco Unified Communications Manager CSR* キーの用途拡張

	マルチサーバ	キーの拡張用途			キーの用途				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント認証 (1.3.6.1.5.5.7.3.2)	IP セキュリティ末端システム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号化	キー証明書署名	鍵共有
CallManager CallManager-ECDSA	Y	Y	Y		Y	Y	Y		
CAPF（パブリッシャのみ）	N	Y			Y			Y	
ipsec ipsec-ECDSA	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
信頼検証サービス（TVS）	N	Y	Y		Y	Y	Y		

表 *14 : IM and Presence Service CSR* キーの用途拡張

	マルチサーバ	キーの拡張用途			キーの用途				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント認証 (1.3.6.1.5.5.7.3.2)	IP セキュリティ末端システム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号化	キー証明書署名	鍵共有
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		Y
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

証明書の表示

システムに属している証明書と信頼ストアの詳細を表示します。

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 証明書の一覧をフィルタするには、[検索（Find）] コントロールを使用します。

ステップ 3 証明書または信頼ストアの詳細を表示するには、証明書の .PEM または .DER ファイル名をクリックします。

ステップ 4 [証明書の一覧（Certificate List）] ウィンドウに戻るには、[関連リンク（Related Links）] リストの [検索/リストに戻る（Back To Find/List）] をクリックし、[移動（Go）] をクリックします。

証明書のダウンロード

手順

ステップ 1 [Cisco Unified OS Administration] から **[Security] > [Certificate Management]** を選択します。

ステップ 2 検索情報を指定し、[検索（Find）] をクリックします。

ステップ 3 証明書または証明書信頼リスト（CTL）のファイル名を選択します。

ステップ 4 [ダウンロード（Download）] をクリックします。

中間証明書のインストール

中間証明書をインストールするには、まずルート証明書をインストールして、署名付き証明書をアップロードする必要があります。この手順は、認証局から1つの署名付き証明書と複数の証明書が証明書チェーンで提供されている場合にのみ必要です。

ヒント ルート証明書の名前は、ルート証明書がアップロードされたときに生成された `.pem` ファイル名です。

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）] > [証明書の管理（Certificate Management）]** をクリックします。

ステップ 2 **[証明書のアップロード（Upload Certificate）]** をクリックします。

ステップ 3 [証明書の用途（Certificate Purpose）] ドロップダウンリストで [intelligenceCenter-srvr-trust] を選択して、ルート証明書をインストールします。

ステップ 4 [参照（Browse）] をクリックしてファイルに移動し、[開く（Open）] をクリックします。

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 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 7 **[証明書のアップロード（Upload Certificate）]** をクリックします。

ステップ 8 [証明書のアップロード（Upload Certificate）] ポップアップ ウィンドウの [証明書の名前（Certificate name）] ドロップダウンリストで [IntelligenceCenter-srvr] を選択し、ルート証明書の名前を入力します。

ステップ 9 次のいずれかの手順を実行して、アップロードするファイルを選択します。

- [ファイルのアップロード（Upload File）] テキストボックスに、ファイルのパスを入力します。
- [参照（Browse）] をクリックしてファイルに移動し、[開く（Open）] をクリックします。

ステップ 10 [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 11 顧客証明書をインストールしたら、FQDN を使用して Cisco Unified Intelligence Center の URL にアクセスします。IP アドレスを使用して Cisco Unified Intelligence Center にアクセスすると、

カスタム証明書を正常にインストールした後でも「ここをクリックしてログインを継続します（Click here to continue）」のメッセージが表示されます。「」

（注） tomcat 証明書をアップロードするときは、TFTP サービスを無効にし、その後有効にします。それ以外の場合は、TFTP は古いキャッシュの自己署名された tomcat 証明書を提供し続けます。

信頼証明書の削除

削除できる証明書は、信頼できる証明書だけです。システムで生成される自己署名証明書は削除できません。

注意 証明書を削除すると、システムの動作に影響する場合があります。証明書が既存のチェーンの一部である場合、証明書を削除すると証明書チェーンが壊れることがあります。この関係は、[証明書の一覧（Certificate List）] ウィンドウ内の関連する証明書のユーザ名とサブジェクト名から確認できます。この操作は取り消すことができません。

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）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 証明書の一覧をフィルタするには、[検索（Find）] コントロールを使用します。

ステップ 3 証明書のファイル名を選択します。

ステップ 4 [削除（Delete）] をクリックします。

ステップ 5 [OK] をクリックします。

（注）
- 削除する証明書が 「CAPF-trust」、「tomcat-trust」、「CallManager-trust」、または 「Phone-SAST-trust」 タイプの場合、証明書はクラスタ内のすべてのサーバで削除されます。
- 証明書を CAPF-trust にインポートする場合、それはその特定のノードでのみ有効になり、クラスタ全体で複製されることはありません。

証明書の再作成

証明書が期限切れの場合は、再作成します。電話機を再起動してサービスを再起動する必要があるため、営業時間後にこの手順を実行します。Cisco Unified OS の管理に 「cert」 タイプとしてリストされている証明書のみ再作成できます。

⚠

注意 証明書を再作成すると、システムの動作に影響する場合があります。証明書を再作成すると、サードパーティの署名付き証明書（アップロードされている場合）を含む既存の証明書が上書きされます。

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）] > [証明書の管理（Certificate Management）]** を選択します。

検索パラメータを入力して、証明書を検索して設定の詳細を表示します。すべての条件に一致したレコードが [Certificate List] ウィンドウに表示されます。

証明書の詳細ページで [再生成（Regenerate）] ボタンをクリックすると、同じキー長を持つ自己署名証明書が再生成されます。

3072 または 4096 の新しいキー長の自己署名証明書を再生成するには、[自己署名証明書の生成（Generate Self-Signed Certificate）] をクリックします。

ステップ 2 [自己署名証明書の新規作成（Generate New Self-Signed Certificate）] 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 [生成（Generate）] をクリックします。

ステップ 4 再作成された証明書の影響を受けるサービスをすべて再起動します。証明書名と説明の詳細については、関連項目のセクションを参照してください。

ステップ 5 CAPF 証明書または CallManager 証明書の再作成後に CTL クライアントを再実行します（設定している場合）。

（注） tomcat 証明書を再作成するときは、TFTP サービスを無効にし、その後有効にします。それ以外の場合は、TFTP は古いキャッシュの自己署名された tomcat 証明書を提供し続けます。

次のタスク

証明書を再作成したら、システムのバックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。バックアップに再作成した証明書が含まれていない状態で

システムの復元タスクを実行する場合は、システム内の各電話機のロックを手動で解除して、電話機を登録できるようにする必要があります。

関連トピック

証明書の名前と説明 （187 ページ）

証明書の名前と説明

次の表に、再作成可能なシステムのセキュリティ証明書と、再起動する必要がある関連サービスを示します。TFTP 証明書の再作成の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html の『*Cisco Unified Communications Manager Security Guide*』を参照してください。

表 *15*：証明書の名前と説明

名前	説明	関連サービス
tomcat tomcat-ECDSA	この自己署名ルート証明書は、HTTPS ノードのインストール中に作成されます。	Tomcat と TFTP
ipsec	この自己署名ルート証明書は、MGCP ゲートウェイおよび H.323 ゲートウェイとの IPsec 接続のインストール中に生成されます。	Cisco Disaster Recovery System（DRS）Local と Cisco DRF Master
CallManager	この自己署名ルート証明書は、Unified Communications Manager のインストール時に自動的にインストールされます。この証明書は、ノード名およびグローバル固有識別子（GUID）など、ノードの ID を提供します。	CallManager、CAPF、および CTI
CAPF	このルート証明書は、Cisco クライアント設定を完了すると、現在のノードまたはクラスタ内のすべてのノードにコピーされます。	CallManager と CAPF
TVS	自己署名ルート証明書です。	TVS

OAuth 更新ログイン用のキーの再生成

コマンドラインインターフェイスを使用して暗号キーと署名キーの両方を再生成するには、この手順を使用します。Cisco Jabber が Unified Communications Manager による OAuth 認証に使用する暗号キーまたは署名キーが侵害された場合にのみ、この作業を実行します。署名キーは非対称で RSA ベースであるのに対し、暗号キーは対称キーです。

（注）

- このタスクを完了すると、これらのキーを使用する現在のアクセス トークンと更新トークンは無効になります。
- エンドユーザへの影響を最小限に抑えるために、このタスクは営業時間外に完了することを推奨します。
- 暗号キーは、以下の CLI を使用してのみ再生成できますが、Cisco Unified OS の管理 GUI を使用して署名キーを再生成することもできます。**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択し、**AUTHZ** 証明書を選択して、[再作成（Regenerate）] をクリックします。

手順

ステップ 1 Unified Communications Manager 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 暗号キーを再生成するには、次の手順を実行します。

a) `set key regen authz encryption` コマンドを実行します。

b) `yes` と入力します。

ステップ 3 署名キーを再生成するには、次の手順を実行します。

a) `set key regen authz signing` コマンドを実行します。

b) `yes` と入力します。
Unified Communications Manager パブリッシャ ノードはキーを再生成し、IM and Presence サービスのローカル ノードを含む、Unified Communications Manager のすべてのクラスタ ノードに新しいキーを複製します。

次のタスク

すべての UC クラスタで新しいキーを再生成して同期する必要があります。

- IM and Presence 中央クラスタ：IM and Presence 集中型展開の場合、IM and Presence ノードはテレフォニーとは別のクラスタ上で実行されています。この場合、IM and Presence サービス一元管理クラスタの Unified Communications Manager パブリッシャ ノードでこの手順を繰り返します。

- Cisco Expressway または Cisco Unity Connection：これらのクラスタ上でもキーを再生成します。詳細については、Cisco Expressway および Cisco Unity Connection のマニュアルを参照してください。

証明書または証明書チェーンのアップロード

システムで信頼する新しい証明書または証明書チェーンを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 [Upload Certificate/Certificate chain] をクリックします。

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

ステップ 4 次のいずれかの手順を実行して、アップロードするファイルを選択します。

- [ファイルのアップロード（Upload File）] テキスト ボックスに、ファイルへのパスを入力します。
- [参照（Browse）] をクリックしてファイルに移動してから、[開く（Open）] をクリックします。

ステップ 5 ファイルをサーバに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。

（注） 証明書をアップロードしたら、影響を受けるサービスを再起動します。サーバが再起動したら、CCMAdmin または CCMUser GUI にアクセスして、新しく追加した証明書が使用されていることを確認できます。

サードパーティ証明書の認証局の管理

このタスク フローでは、サードパーティ証明書プロセスの概要を、各ステップへの参照とともに順番に説明します。お使いのシステムは、サードパーティ認証局が PKCS # 10 証明書署名要求（CSR）を使用して発行する証明書をサポートしています。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書署名要求の生成 （191 ページ）	証明書署名要求（CSR）を生成します。これは、公開キー、組織名、共通名、地域、および国などの証明書申請情報を含

	コマンドまたはアクション	目的
		む暗号化されたテキストのブロックです。認証局はこの CSR を使用して、ご使用のシステムの信頼できる証明書を生成します。
ステップ 2	証明書署名要求のダウンロード （191 ページ）	コンピュータに CSR をダウンロードして、認証局に証明書を送信できるようにします。
ステップ 3	認証局のドキュメントを参照してください。	認証局からアプリケーション証明書を取得します。
ステップ 4	認証局のドキュメントを参照してください。	認証局からルート証明書を取得します。
ステップ 5	信頼ストアへの認証局署名済み CAPF ルート証明書の追加 （191 ページ）	ルート証明書を信頼ストアに追加します。認証局の署名付き CAPF 証明書を使用している場合は、この手順を実行します。
ステップ 6	証明書または証明書チェーンのアップロード （189 ページ）	認証局ルート証明書をノードにアップロードします。
ステップ 7	CAPF または Cisco Unified Communications Manager の証明書を更新した場合は、新しい CTL ファイルを生成します。	『*Cisco Unified Communications Manager Security Guide*』（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。 サードパーティの署名付き CAPF または CallManager 証明書をアップロードしたら、CTL クライアント（設定している場合）を再実行します。
ステップ 8	サービスの再起動 （192 ページ）	新しい証明書の影響を受けるサービスを再起動します。すべての証明書タイプで、対応するサービスを再起動します（たとえば、Tomcat または Tomcat-ECDSA の証明書を更新した場合は Cisco Tomcat サービスを再起動します）。

証明書署名要求の生成

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

（注） 新しい CSR を生成すると、既存の CSR は上書きされます。

手順

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 [CSR の作成（Generate CSR）] をクリックします。

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

ステップ 4 [CSR の作成（Generate CSR）] をクリックします。

証明書署名要求のダウンロード

コンピュータに CSR をダウンロードして、認証局に証明書を送信できるようにします。

手順

ステップ 1 [Cisco Unified OS Administration] から **[Security] > [Certificate Management]** を選択します。

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

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

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

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

信頼ストアへの認証局署名済み CAPF ルート証明書の追加

認証局署名済みCAPF証明書を使用する場合は、次の手順に従って、ルート証明書をCallManager信頼ストアに追加します。

手順

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

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

ステップ 3 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] ポップアップ ウィンドウで、[証明書の用途（Certificate Purpose）] ドロップダウン リストから [CallManager の信頼性（CallManager-trust）] を選択し、認証局署名済み CAPF ルート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。

サービスの再起動

クラスタ内の特定のノードで機能またはネットワーク サービスを再起動する必要がある場合は、次の手順に従います。

手順

ステップ 1 再起動するサービスのタイプに応じて、次のいずれかのタスクを実行します。

- **[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。
- **[ツール（Tools）] > [コントロール センター - ネットワーク サービス（Control Center - Network Services）]** を選択します。

ステップ 2 [サーバ（Server）] ドロップダウンリストからシステム ノードを選択し、[移動（Go）] をクリックします。

ステップ 3 再起動するサービスの横にあるオプション ボタンをクリックし、[再起動（Restart）] をクリックします。

ステップ 4 再起動にはしばらく時間がかかることを示すメッセージが表示されたら、[OK] をクリックします。

Online Certificate Status Protocol（OCSP）による証明書失効（CRL）

Unified Communications Manager は、証明書失効の監視に Online Certificate Status Protocol（OCSP）の使用をサポートします。OCSP の Unified Communications Manager サポートを設定すると、システムは証明書がまだ有効であることを確認するために定期的なチェックを実行します。チェックは、証明書がアップロードされたときと、スケジュールされた時間に実行されます。

有効性検査

Unified Communications Manager は、証明書を検証するために代理信頼モデルを使用し、最初の試行が失敗した場合に、応答側の信頼モデルにフォールバックします。証明書のステータスを確認すると、以下が行われます。

- Unified Communications Manager はまず代理信頼モデルを使用し、OCSP 署名属性のルート CA または中間 CA をチェックします。
- これが失敗すると、Unified Communications Manager は応答側の信頼モデルにフォールバックします。システムは、信頼ストアから、証明書のキー使用セクションに署名 OID がある、OCSP 署名属性応答署名証明書を探します。
- 両方の試行が失敗した場合、証明書は取り消されています。

設定

OCSP のサポートは、Cisco Unified OS Administration の [証明書の取り消し（Certificate Revocation）] ウィンドウで設定できます。IPsec のリンクが設定されている場合は、OCSP を使用して IPsec のリンクに使用される証明書を検証するために、エンタープライズ パラメータのペアも設定する必要があります。

OCSP 応答の場合、Unified Communications Manager は、検証チェックを実行するために、ルートまたは中間 CA 証明書のいずれかを使用できます。あるいは、証明書を検証するために、OCSP サーバからの指定された OCSP 応答署名証明書を使用できます。これらは、Unified Communications Manager から外部的に設定する必要があります。

証明書モニタリング タスク フロー

次のタスクを行い、証明書ステータスと有効期限をモニタするようシステムを設定します。次の処理を自動的に行うようシステムを設定できます。

- 証明書の有効期限が近づいているときは、電子メールで通知する。
- 有効期限が切れた証明書を失効させる。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書モニタ通知の設定 （194 ページ）	証明書の自動モニタリングを構成します。システムは定期的に証明書ステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。
ステップ 2	OCSP による証明書失効の設定 （195 ページ）	Online Certificate Status Protocol（OCSP）を設定し、期限切れの証明書をシステムが自動的に失効させるようにします。

証明書モニタ通知の設定

Unified Communications Manager または IM and Presence サービスの自動証明書モニタリングを設定します。システムは定期的に証明書のステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。

（注） [Cisco Certificate Expiry Monitor] ネットワーク サービスを実行している必要があります。デフォルトでこのサービスは有効化されていますが、**[ツール（Tools）]** > **[コントロール センター - ネットワーク サービス（Control Center - Network Services）]** を選択し、[Cisco Certificate Expiry Monitor サービス（Cisco Certificate Expiry Monitor Service）] の状態が [実行中（Running）] であることを検証して Cisco Unified Serviceability でサービスが実行中であることを確認できます。

手順

ステップ 1 （Unified Communications Manager の証明書モニタリングのために）Cisco Unified OS の管理にログインするか、（IM and Presence サービスの証明書モニタリングのために）Cisco Unified IM and Presence の管理にログインします。

ステップ 2 **[セキュリティ（Security）]** > **[証明書モニタ（Certificate Management）]** を選択します。

ステップ 3 [通知開始時期（Notification Start Time）] フィールドに、数値を入力します。この値は、近づきつつある有効期限の通知を、有効期限の何日前にシステムが開始するかを表します。

ステップ 4 [通知頻度（Notification Frequency）] フィールドには、通知を行う頻度を入力します。

ステップ 5 これはオプションです。[電子メール通知を有効にする（Enable E-mail notification）] チェックボックスをオンにして、近づきつつある証明書有効期限に関する電子メールアラートをシステムに送信させます。

ステップ 6 [LSC モニタリングを有効にする（Enable LSC Monitoring）] チェック ボックスをオンにして、LSC 証明書を証明書ステータス チェックに含めます。

ステップ 7 [電子メール ID（E-mail IDs）] フィールドに、システムが通知を送信する電子メール アドレスを入力します。複数の電子メールアドレスは、セミコロンで区切って入力できます。

ステップ 8 [保存（Save）] をクリックします。

（注） 証明書モニタ サービスは、デフォルトで 24 時間ごとに 1 回だけ実行します。証明書モニタ サービスを再起動すると、サービスが開始され、24 時間後に実行する次のスケジュールが計算されます。証明書の有効期限が 7 日以内に近づいても、この周期は変化しません。このサービスは、証明書の有効期限が切れる 1 日前から、有効期限が切れた後も 1 時間おきに実行します。

次のタスク

Online Certificate Status Protocol（OCSP）を設定し、期限切れの証明書をシステムが自動的に失効させるようにします。詳細については、次を参照してください。OCSP による証明書失効の設定 （195 ページ）

OCSP による証明書失効の設定

オンライン証明書ステータスプロトコル（OCSP）を有効にして、証明書の状態を定期的にチェックし、期限切れの証明書を自動的に失効させます。

始める前に

システムに OCSP チェックに必要な証明書があることを確認します。OCSP 応答属性を設定されているルート CA 証明書または中間 CA 証明書を使用することができます。または、tomcat-trust へアップロードされている指定された OCSP 署名証明書を使用することができます。

手順

ステップ 1 （Unified Communications Manager の証明書失効のために）Cisco Unified OS の管理にログインするか、（IM and Presence サービスの証明書失効のために）Cisco Unified IM and Presence の管理にログインします。

ステップ 2 **[セキュリティ（Security）] > [証明書失効（Certificate Revocation）]** を選択します。

ステップ 3 [OCSP の有効化（Enable OCSP）] チェック ボックスをオンにして、次のタスクのいずれかを実行します。

- OCSP チェックの OCSP レスポンダを指定する場合は、[設定済み OCSP URI を使用する（Use configured OCSP URI）] ボタンを選択し、[OCSP 設定済み URI（OCSP Configured URI）] フィールドにレスポンダの URI を入力します。
- OCSP レスポンダ URI で証明書を設定する場合、[証明書からの OCSP URI を使用する（Use OCSP URI from Certificate）] ボタンを選択します。

ステップ 4 [失効チェックを有効にする（Enable Revocation Check）] チェック ボックスをオンにします。

ステップ 5 [チェック間隔（Check Every）] フィールドに失効チェックの間隔を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 これはオプションです。CTI、IPsec または LDAP リンクがある場合は、これらの長期性接続の OCSP 失効サポートを有効にするために、上記の手順に加えて次の手順も行う必要があります。

a) 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。

b) [証明書の失効や有効期限（Certificate Revocation and Expiry）] で、[証明書有効性チェック（Certificate Validity Check）] パラメーターを [True] に設定します。

c) [有効性チェック頻度（Validity Check Frequency）] パラメーターの値を設定します。

（注） **証明書失効**ウィンドウの [失効チェックを有効にする（Enable Revocation Check）] パラメーターの間隔値は、[有効チェック頻度（Validity Check Frequency）] エンタープライズ パラメーターの値よりも優先されます。

d) **[保存（Save）]** をクリックします。

証明書エラーのトラブルシュート

始める前に

IM and Presence サービス ノードから Unified Communications Manager サービスに、または、Unified Communications Manager ノードから IM and Presence サービス機能にアクセスしようとしてエラーが発生した場合は、tomcat-trust 証明書に問題があります。「サーバへの接続を確立できません（リモート ノードに接続できません）（Connection to the Server cannot be established (unable to connect to Remote Node)）」というエラー メッセージが、次の [サービスアビリティ（Serviceability ）] インターフェイス ウィンドウに表示されます。

- **[サービスのアクティブ化（Service Activation）]**
- **コントロール センター - 機能サービス**
- **コントロール センター - ネットワーク サービス**

この手順を使用して、証明書のエラーを解決します。最初のステップから開始し、必要に応じて進みます。最初のステップだけでエラーが解決される場合もあれば、すべてのステップを実行することが必要になる場合もあります。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] の **[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** で、必要な tomcat-trust 証明書が存在することを確認します。

必要な証明書がない場合は、再度確認するまで 30 分間待ちます。

ステップ 2 証明書を選択して情報を表示します。証明書の内容が、リモートノード上の対応する証明書の内容と一致することを確認します。

ステップ 3 CLI から、**utils service restart Cisco Intercluster Sync Agent** を実行して Cisco Intercluster Sync Agent サービスを再起動します。

ステップ 4 Cisco Intercluster Sync Agent サービスが再起動したら、**utils service restart Cisco Tomcat** を実行して Cisco Tomcat サービスを再起動します。

ステップ 5 30 分間待機します。前の手順で証明書のエラーが対処されず、tomcat-trust 証明書が存在する場合は、証明書を削除します。証明書を削除したら、ノードごとに Tomcat および Tomcat-ECDSA 証明書をダウンロードし、tomcat-trust 証明書としてピアにアップロードすることで、証明書を手動で交換する必要があります。

ステップ 6 証明書の交換が完了したら、**utils service restart Cisco Tomcat** を実行して、影響を受ける各サーバで Cisco Tomcat を再起動します。

第 17 章

一括証明書の管理

一括証明書の管理

クラスタ間で証明書のセットを共有する場合に、一括証明書管理を使用します。この手順は、Extension Mobility Cross Cluster などのクラスタ間で信頼を確立する必要があるシステム機能に必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書のエクスポート （200 ページ）	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。

	コマンドまたはアクション	目的
ステップ 2	証明書のインポート （201 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。 （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。

証明書のエクスポート

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（Save）] 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

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） 一括証明書管理機能を使用して証明書をインポートすると、電話機がリセットされます。

始める前に

[インポート（Import）] ボタンが表示されるには、次の操作を完了しておく必要があります。

- 2 つ以上のクラスタから SFTP サーバに証明書をエクスポートします。
- エクスポートした証明書を統合します。

手順

ステップ 1 Cisco Unified OS 管理画面で、**[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 [インポート（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

（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。
- TVS：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。

第 18 章

IPSec ポリシーの管理

IPsec ポリシーの概要

IPsec は、暗号セキュリティ サービスを使用した IP ネットワーク経由の非公開でセキュアな通信を保証するフレームワークです。IPsec ポリシーが IPsec セキュリティ サービスの設定に使用されます。このポリシーは、ネットワーク上のほとんどのトラフィック タイプにさまざまなレベルの保護を提供します。コンピュータ、部門（OU）、ドメイン、サイト、またはグローバル企業のセキュリティ要件を満たすように IPsec ポリシーを設定できます。

IPsec ポリシーの設定

（注）

- システムのアップグレード中、IPsec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPsec ポリシーを作成したり変更したりしないでください。
- IPsec には双方向プロビジョニングが必要です（ホストまたはゲートウェイごとに 1 ピア）。
- 一方の IPsec ポリシー プロトコルが 「ANY」、もう一方の IPsec ポリシー プロトコルが 「UDP」 または 「TCP」 に設定されている 2 つの Unified Communications Manager ノードに IPsec ポリシーをプロビジョニングする場合、「ANY」 プロトコルを使用するノードでの検証で検出漏れが発生する可能性があります。
- IPsec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

手順

ステップ 1 Cisco Unified OS の管理から **[セキュリティ（Security）] > [IPSec の設定（IPSec Configuration）]** の順に選択します。

ステップ 2 **[新規追加（Add New）]** をクリックします。

ステップ 3 [IPSEC ポリシーの設定（IPSEC Policy Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 （任意） IPsec を検証するには、**[サービス（Services）] > [Ping]** の順に選択し、[IPsec の検証（Validate IPsec）] チェックボックスをオンにして、[Ping] をクリックします。

IPSec ポリシーの管理

システムのアップグレード中、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを変更または作成しないでください。

⚠

注意 ホスト名、ドメイン、または IP アドレスを変更するために既存の IPSec 証明書に変更を加える際、証明書名を変更する場合は、IPSec ポリシーを削除して作り直す必要があります。証明書名を変更しない場合は、リモート ノードの作り直した証明書をインポートした後に、IPSec ポリシーを無効にして有効にする必要があります。

手順

ステップ 1 Cisco Unified OS の管理から **[セキュリティ（Security）] > [IPSec の設定（IPSec Configuration）]** の順に選択します。

ステップ 2 ポリシーを表示、イネーブル、またはディセーブルにするには、次の手順を実行します。

a) ポリシー名をクリックします。

b) ポリシーを有効または無効にするには、[ポリシーの有効化（Enable Policy）] チェックボックスをオンまたはオフにします。

c) [保存（Save）] をクリックします。

ステップ 3 1 つまたは複数のポリシーを削除するには、次の手順を実行します。

a) 削除するポリシーの横にあるチェックボックスをオンにします。

[すべてを選択（Select All）] をクリックするとすべてのポリシーを選択でき、[すべてをクリア（Clear All）] を選択するとすべてのチェックボックスをクリアできます。

b) [選択項目の削除（Delete Selected）] をクリックします。

第 19 章

クレデンシャル ポリシーの管理

クレデンシャル ポリシーと認証

認証機能は、ユーザの認証、クレデンシャル情報の更新、ユーザイベントとエラーのトラッキングとロギング、クレデンシャル変更履歴の記録、データ ストレージ用のユーザ クレデンシャルの暗号化または復号を行います。

システムは常に、アプリケーション ユーザ パスワードとエンド ユーザ PIN を Unified Communications Manager データベースに照合します。エンド ユーザ パスワードについては、社内ディレクトリまたはデータベースに照合して認証できます。

システムが社内ディレクトリと同期されていれば、Unified Communications Manager または Lightweight Directory Access Protocol（LDAP）のいずれかの認証機能によってパスワードを認証できます。

- LDAP 認証が有効にされている場合、ユーザ パスワードおよびクレデンシャル ポリシーは適用されません。これらのデフォルトは、ディレクトリ同期（DirSync サービス）で作成されたユーザに適用されます。
- LDAP 認証を無効にすると、システムはユーザ クレデンシャルをデータベースに照合して認証します。このオプションを使用する場合、クレデンシャル ポリシーを割り当て、認証イベントおよびパスワードを管理することができます。エンドユーザは、電話機のユーザ インターフェイスでパスワードと PIN を変更できます。

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

データベースにユーザが設定されると、システムはユーザ クレデンシャルの履歴をデータベースに格納して、ユーザがクレデンシャルの変更を要求されたときに以前の情報を入力できないようにします。

クレデンシャル ポリシーの JTAPI および TAPI のサポート

Cisco Unified Communications Manager Java テレフォニー アプリケーション プログラミング インターフェイス（JTAPI）およびテレフォニーアプリケーションプログラミングインターフェイス（TAPI）は、アプリケーションユーザに割り当てられたクレデンシャルポリシーをサポートするため、開発者はパスワードの有効期限、PIN の有効期限、およびクレデンシャル ポリシーの適用ためのロックアウト戻りコードに応答するアプリケーションを作成する必要があります。

アプリケーションは、アプリケーションが使用する認証モデルに関係なく、API を使用してデータベースまたは社内ディレクトリで認証します。

開発者向けの JTAPI および TAPI の詳細については、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。

クレデンシャル ポリシーの設定

クレデンシャル ポリシーは、アプリケーション ユーザとエンド ユーザに適用されます。パスワード ポリシーをエンド ユーザとアプリケーション ユーザに割り当て、PIN ポリシーをエンド ユーザに割り当てます。[クレデンシャル ポリシーのデフォルトの設定（Credential Policy Default Configuration）] に、これらのグループのポリシー割り当てが一覧表示されます。新しいユーザをデータベースに追加すると、システムがデフォルトポリシーを割り当てます。割り当てられたポリシーを変更したり、ユーザ認証イベントを管理したりできます。

手順

ステップ 1 Cisco Unified CM の管理から、**[ユーザの管理（User Management）] > [クレデンシャル ポリシー（Credential Policy）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- [検索（Find）] をクリックし、既存のクレデンシャル ポリシーを選択します。
- [新規追加（Add New）] をクリックして、新しいクレデンシャル ポリシーを作成します。

ステップ 3 [クレデンシャル ポリシーの設定（Credential Policy Configuration）] ウィンドウの各フィールドに入力します。フィールドとその設定の詳細については、オンラインヘルプを参照してください。

ステップ 4 **[保存（Save）]** をクリックします。

クレデンシャル ポリシー デフォルトの設定

インストール時に、Cisco Unified Communications Manager がスタティック デフォルト クレデンシャル ポリシーをユーザ グループに割り当てます。デフォルト クレデンシャルは提供しません。お使いのシステムが、新しいデフォルト ポリシーを割り当てたり、ユーザの新しいデフォルト クレデンシャルとクレデンシャル要件を設定したりするためのオプションを提供します。

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）]** > **[クレデンシャル ポリシーのデフォルト（Credential Policy Default）]** を選択します。

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

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

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

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

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

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

ステップ 7 [保存（Save）] をクリックします。

認証アクティビティのモニタ

最終ハック試行時刻やログイン試行失敗回数などの最新の認証結果が、システムによって表示されます。

システムは、次のクレデンシャル ポリシー イベントに関するログ ファイル エントリを生成します。

- 認証成功
- 認証失敗（不正なパスワードまたは不明）
- 次の原因による認証失敗

- 管理ロック
- ハッキング ロック（失敗したログオン ロックアウト）
- 期限切れソフト ロック（期限切れのクレデンシャル）
- 非アクティブ ロック（一定期間使用されていないクレデンシャル）
- ユーザによる変更が必要（ユーザが変更するように設定されたクレデンシャル）
- LDAP 非アクティブ（LDAP 認証へ切り替えたものの LDAP が非アクティブ）

- 成功したユーザ クレデンシャル更新
- 失敗したユーザ クレデンシャル更新

（注） エンド ユーザ パスワードに対して LDAP 認証を使用する場合は、LDAP は認証の成功と失敗だけを追跡します。

すべてのイベント メッセージに、文字列 「ims-auth」 と認証を試みているユーザ ID が含まれています。

手順

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

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

ステップ 3 [クレデンシャルの編集（Edit Credential）] をクリックし、ユーザの認証アクティビティを表示します。

次のタスク

Cisco Unified Real-Time Monitoring Tool（Unified RTMT）を使用してログ ファイルを表示できます。また、キャプチャしたイベントをレポートに収集できます。Unified RTMT の詳細な使用手順については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』（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。

クレデンシャル キャッシングの設定

クレデンシャル キャッシングを有効にすると、システム効率が向上します。システムは、ログイン要求ごとに、データベース ルックアップを実行したり、ストーアド プロシージャを呼び

出したりする必要がありません。キャッシング期間が切れるまで、関連するクレデンシャルポリシーが適用されません。

この設定は、ユーザ認証を呼び出すすべての Java アプリケーションに適用されます。

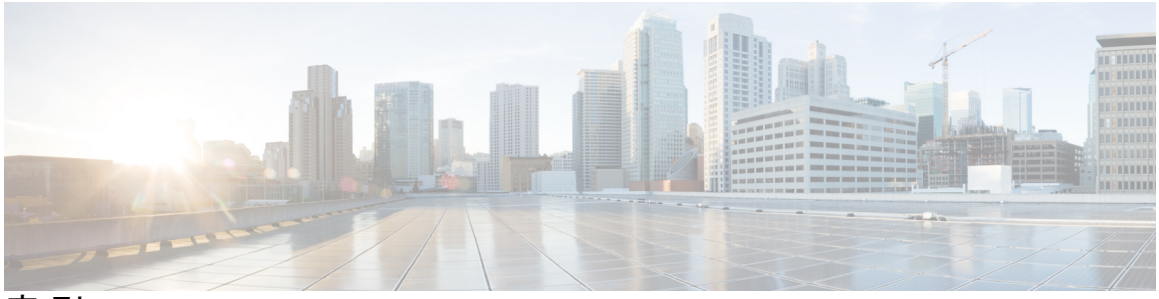
手順

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 必要に応じて、次のタスクを実行します。

- [キャッシングの有効化（Enable Caching）] エンタープライズ パラメータを [True] に設定します。このパラメータを有効にすると、Cisco Unified Communications Manager は、最大 2 分間、キャッシュされたクレデンシャルを使用します。
- システムがキャッシュされたクレデンシャルを認証に使用しないように、キャッシングを無効にするには、[キャッシングの有効化（Enable Caching）] エンタープライズ パラメータを [False] に設定します。LDAP 認証では、システムがこの設定を無視します。クレデンシャル キャッシングには、ユーザあたり少しの追加のメモリが必要です。

ステップ 3 **[保存（Save）]** をクリックします。



索 引