Cisco Unified Communications Manager リリース 12.5(1) セキュリティ ガイド

初版：2019 年 1 月 23 日

最終更新：2019 年 1 月 23 日

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

目 次

はじめに

目的

『*Cisco Unified Communications Manager* セキュリティ ガイド』は、システム管理者と電話管理者が次の作業を行う際に役立ちます。

- 認証の設定。
- 暗号化の設定。
- ダイジェスト認証の設定。
- HTTPS に関連付けられているサーバ認証証明書のインストール。
- Cisco CTL クライアントの設定。
- セキュリティ プロファイルの設定。
- サポートされている Cisco Unified IP Phone モデルでローカルで有効な証明書を設定、アップグレード、または削除するための Certificate Authority Proxy Function（CAPF）の設定。
- 電話のセキュリティ強化の設定。
- セキュリティのための Survivable Remote Site Telephony（SRST）リファレンスの設定。
- セキュリティのためのゲートウェイおよびトランクの設定。
- FIPS（連邦情報処理標準）140-2 モードの設定。

対象読者

このガイドでは、Cisco Unified Communications Manager のコール セキュリティ機能を設定する予定のシステム管理者と電話管理者向けのリファレンスおよび手順ガイドを提供します。

マニュアルの構成

次の表に、このマニュアルの主なセクションを示します。

表 *1*: マニュアルの概要

章	説明
セキュリティの基礎	
セキュリティの概要 （1 ページ）	セキュリティ用語、システム要件、連携動作と制限、インストール要件、および設定チェックリストの概要を説明します。認証と暗号化の種類についても説明されます。
Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS） （59 ページ）	HTTPS の概要と、信頼できるフォルダにサーバ認証証明書をインストールする方法について説明します。
デフォルトのセキュリティ設定 （73 ページ）	Cisco Unified IP Phone の自動セキュリティ機能を実現するデフォルトのセキュリティ機能について説明します。
Cisco CTL クライアントの設定 （103 ページ）	Cisco CTL クライアントのインストールと設定によって認証を設定する方法を説明します。
証明書	
電話とボイスメール ポートのセキュリティ	
電話のセキュリティ （181 ページ）	Unified Communications Manager と電話でどのようにセキュリティが使用されるかを説明します。電話のセキュリティ設定のために実行するタスクの一覧があります。
電話セキュリティ プロファイルの設定 （189 ページ）	Unified Communications Manager でセキュリティ プロファイルを設定して適用する方法を説明します。

章	説明
セキュア通知トーンおよび非セキュア通知トーンの設定 （211 ページ）	セキュア通知トーンを再生するよう電話を設定する方法を説明します。
アナログ エンドポイントに対する暗号化の設定 （217 ページ）	アナログエンドポイントへのセキュアなSCCP接続を設定する方法を説明します。
暗号化された電話設定ファイルの設定 （219 ページ）	Unified Communications Manager で暗号化された電話コンフィギュレーション ファイルを設定する方法を説明します。
SIP 電話のダイジェスト認証の設定 （233 ページ）	Unified Communications Manager Administration で SIP を実行している電話にダイジェスト認証を設定する方法を説明します。
電話のセキュリティ強化 （237 ページ）	Unified Communications Manager Administration を使用して電話のセキュリティを厳格化する方法を説明します。
セキュアな会議リソースの設定 （241 ページ）	セキュアな会議にメディア暗号化を設定する方法を説明します。
ボイス メッセージング ポートのセキュリティ設定 （257 ページ）	Unified Communications Manager Administration でボイス メール ポートのセキュリティを設定する方法を説明します。
セキュアなコールのモニタリングおよび録音のセットアップ （263 ページ）	セキュア コールのモニタリングと録音を設定する方法を説明します。
Cisco IP Phone の仮想プライベート ネットワーク	
CTI、JTAPI、および TAPI のセキュリティ	
CTI、JTAPI、および TAPI の認証および暗号化の設定 （285 ページ）	Unified Communications Manager でアプリケーション ユーザ CAPF プロファイルとエンドユーザ CAPF プロファイルを設定する方法を説明します。
SRST 参照、ゲートウェイ、トランク、および Cisco Unified Mobility Advantage サーバのセキュリティ	
セキュアな Survivable Remote Site Telephony （SRST）リファレンス （305 ページ）	Unified Communications Manager Administration でセキュリティのため SRST 参照を設定する方法を説明します。
ゲートウェイおよびトランクの暗号化の設定 （313 ページ）	Unified Communications Manager がセキュアなゲートウェイやトランクと通信する方法について説明します。IPSec に関する推奨事項と考慮事項について説明します。

章	説明
SIP トランク セキュリティ プロファイルの設定 （321 ページ）	Unified Communications Manager Administration で SIP トランク セキュリティ プロファイルを設定し、適用する方法を説明します。
SIP トランクのダイジェスト認証の設定 （339 ページ）	[Unified Communications Manager Administration] で SIP トランクにダイジェスト認証を設定する方法を説明します。
Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定 （345 ページ）	Unified Communications Manager Administration で Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルを設定する方法を説明します。
FIPS 140-2 モードの設定 （351 ページ）	Unified Communications Manager Administration で FIPS（連邦情報処理標準）140-2 モードを設定する方法を説明します。
Cisco V.150 Minimum Essential Requirements （MER） （353 ページ）	IP ネットワーク経由のモデムでのセキュアコールの発信を可能にする v. 150 の機能を設定する方法について説明します。

関連資料

各章には章トピックの関連資料の一覧が含まれています。

関連する Cisco IP Telephony アプリケーションと製品の詳細については、次のドキュメントを参照してください。

- 『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』
- 『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』
- 『*Cisco Unified Communications Manager Integration Guide for Cisco Unity*』
- 『*Cisco Unified Communications Manager Integration Guide for Cisco Unity Connection*』
- SRST 対応ゲートウェイに対応した Cisco Unified Survivable Remote Site Telephony（SRST）管理マニュアル
- 電話機モデルの *Cisco IP Phone Administration Guide*

表記法

（注）は、次のように表しています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒントは、次のように表しています。

ヒント 役立つ「ヒント」の意味です。

注意は、次のように表しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

マニュアルの入手、サポート、およびセキュリティガイドライン

マニュアルの入手方法、テクニカルサポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

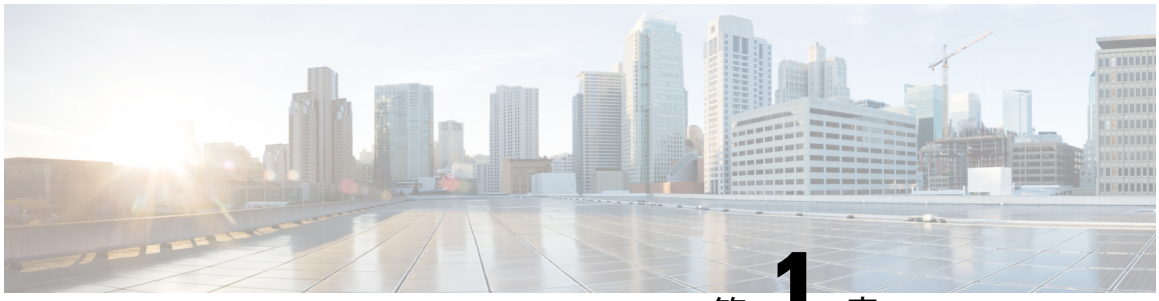
Cisco 製品のセキュリティ

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、http://www.access.gpo.gov/bis/ear/ear_data.html で参照できます。

第 部

セキュリティの基礎



第 1 章

セキュリティの概要

Unified Communications Manager システムにセキュリティ対策を実装すると、電話や Unified Communications Manager サーバの個人情報/ID の盗用、データ改ざん、コール シグナリング/メディア ストリーム改ざんを防止できます。

Cisco IP テレフォニー ネットワークでは、認証済み通信ストリームを確立および維持し、ファイルを電話に転送する前にそのファイルにデジタル署名して、Cisco Unified IP Phone 間のメディア ストリームとコール シグナリングを暗号化します。

用語および略語

次の表の定義は、Cisco IP テレフォニー ネットワークの認証、暗号化およびその他のセキュリティ機能を設定する際に適用されます。

表 *2:* 用語

用語	定義
アクセス コントロール リスト（ACL）	システム機能およびリソースにアクセスするための権限およびアクセス許可を定義するリスト。方式リストを参照してください。
認証	通信エンティティのアイデンティティを確認するプロセス。
許可	認証されたユーザ、サービス、またはアプリケーションに、要求されたアクションを実行するために必要なアクセス許可があるかどうかを指定するプロセス。Unified Communications Manager では、許可されたユーザに特定のトランク側 SIP 要求を制限するセキュリティ プロセスです。
認証ヘッダー	チャレンジに対する SIP ユーザ エージェントの応答。
証明書	証明書保持者名、公開キー、および証明書を発行する認証局のデジタル署名を含むメッセージ。
認証局（CA）	証明書を発行する信頼されたエンティティ：シスコまたはサードパーティのエンティティ。
認証局プロキシ機能（CAPF）	サポートするデバイスが Unified Communications Manager Administration を使用して、ローカルで有効な証明書を要求できるプロセス。
証明書信頼リスト（CTL）	CLI コマンドセット **utils cli** または CTL クライアントで作成され、Cisco Site Administrator Security Token（セキュリティ トークン）によって署名されたファイル。電話が信頼するサーバの証明書のリストを含みます。
Challenge	ダイジェスト認証において、SIP ユーザ エージェントに対しそのアイデンティティの認証を求める要求。

用語	定義
Cisco Site Administrator Security Token（セキュリティ トークン、etoken）	秘密キーと、Cisco Certificate Authority が署名する X.509v3 証明書を含むポータブル ハードウェア セキュリティ モジュール。ファイル認証に使用され、CTL ファイルの署名に使用される場合があります。 ハードウェア セキュリティ トークンは CTL クライアントにのみ必要です。CLI コマンド セット **utils ctl** はハードウェア セキュリティ トークンを必要としません。
デバイス認証	デバイスのアイデンティティを検証してエンティティが正当なものであることを接続の確立前に確認するプロセス。
ダイジェスト認証	デバイス認証の 1 つで、SIP ユーザ エージェントのアイデンティティを設定するために（特に）共有パスワードの MD5 ハッシュを使用します。
Digest User	SIP を実行している電話または SIP トランクが送信する許可要求に含まれているユーザ名。
デジタル署名	メッセージをハッシュし、その後署名者の秘密キーを使用してメッセージを暗号化することによって生成される値。受信者は署名者の公開キーを使用してメッセージとハッシュを復号化し、同じハッシュ関数を使って別のハッシュを作成し、次に 2 つのハッシュを比較し、メッセージが一致しており内容が変更されていないことを確認します。
DSP	デジタル シグナリング プロセッサ。
DSP ファーム	H.323 または MGCP ゲートウェイの DSP で提供される IP テレフォニー会議のネットワーク リソース。
暗号化	データを暗号文に変換するプロセス。情報の機密性を保持し、対象とする受信者のみがデータを読み取ることができるようにします。暗号化アルゴリズムと暗号キーが必要です。

用語	定義
ファイル認証	電話がダウンロードするデジタル署名ファイルを検証するプロセス。ファイルの作成後にファイルの改ざんが発生していないことを確認するため、電話で署名が検証されます。
H.323	インターネットの標準規格の 1 つで、一連の共通コーデック、コール設定とネゴシエーション手順、および基本的なデータ転送方法を定義します。
ハッシュ	ハッシュ関数を使用してテキスト文字列から生成される、通常は16進数の数値。これにより、データに対して 1 つの小さなデジタル「「フィンガープリント」」が作成されます。
Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS）	（少なくとも）HTTPS サーバのアイデンティティを確認する IETF 定義のプロトコル。暗号化を使用して、Tomcat サーバとブラウザ クライアントの間で交換される情報の機密性を確保します。
イメージ認証	電話がバイナリ イメージをロードする前に、そのバイナリ イメージの整合性と送信元を電話が検証するプロセス。
完全性	データの改ざんがエンティティ間で実行されていないことを確認するプロセス。
IPSec	エンドツーエンド セキュリティ用にセキュアな H.225、H.245、RAS シグナリング チャネルを提供する転送方式。
ローカルで有効な証明書（LSC）	CAPF が発行するデジタル X.509v3 証明書。電話または JTAPI/TAPI/CTI アプリケーションにインストールされます。
製造元でインストールされる証明書（MIC）	Cisco 認証局が署名し、サポートされている電話に Cisco Manufacturing によってインストールされるデジタル X.509v3 証明書。LSC が電話にインストールされると、CAPF の認証メカニズムとして使用されます。
中間者攻撃	Unified Communications Manager と電話との間で流れる情報を攻撃者が監視して改変できるようにするプロセス。

用語	定義
マルチポイント コントロール ユニット（MCU）	複数の H.323 エンドポイントを接続し、複数のユーザが IP ベースのビデオ会議に参加できるようにする柔軟なシステム。
MD5	暗号化で使用されるハッシュ関数。
メディア暗号化	暗号化手順によってメディアの機密性を保護するプロセス。メディア暗号化は IETF RFC 3711 で定義された Secure Real-Time Protocol（SRTP）を使用します。
メッセージ/データの改ざん	攻撃者が送信中にメッセージを変更しようとするイベント。コールの途中終了も含まれます。
方式リスト	許可プロセス中に SIP トランクに着信する可能性のある特定のカテゴリのメッセージを制限するツール。ランク側アプリケーションやデバイスで可能な SIP nonINVITE 方式を定義します。メソッド ACL とも呼ばれます。
混合モード	セキュア/非セキュア プロファイルおよび RTP/SRTP メディアを持つデバイスが Unified Communications Manager に接続できるようにするために設定する Unified Communications Manager のセキュリティ モード。
ナンス	サーバが各ダイジェスト認証要求に対して生成する一意のランダムな数値。MD5 ハッシュの生成に使用されます。
非セキュア モード	非セキュア プロファイルおよび RTP メディアを持つデバイスが Unified Communications Manager に接続できるようにするために設定する Unified Communications Manager のセキュリティ モード。
非セキュア コール	少なくとも 1 つのデバイスが認証も暗号化もされていないコール。
非セキュアなデバイス	UDP または TCP シグナリングと非セキュア メディアを使用するデバイス。
PKI	保護された公開キー配布、証明書と認証局など、公開キーの暗号化に必要な一連の要素からなる公開キー インフラストラクチャ。

用語	定義
公開/秘密キー	暗号化に使用されるキー。公開キーは幅広く使用可能ですが、秘密キーはそれぞれの所有者により保持されます。非対称暗号化では両方のキーが使用されます。
リプレイ アタック	攻撃者が実際のデバイスになりすまして、電話またはプロキシサーバを特定する情報をキャプチャし情報を再生するイベント。たとえば、プロキシサーバの秘密キーのなりすましなど。
RTP	リアルタイム転送プロトコル
Simple Certificate Enrollment Protocol（SCEP）	X.509証明書を発行する認証局との通信に使用されるプロトコル。
セキュアなコール	すべてのデバイスが認証され、シグナリングとメディア（音声ストリーム）が暗号化されているコール。
シグナリング認証	伝送中にシグナリング パケットに改ざんがなかったことを検証する TLS プロセス。
シグナリング暗号化	デバイスと Unified Communications Manager サーバの間で送信されるすべてのシグナリング メッセージの機密を保護するために暗号化手法を使用するプロセス。
SIP レルム	Unified Communications Manager がチャレンジに応答するために使用する文字列（名前）。
SRTP	Secure Real-Time Transport Protocol。ネットワーク上の音声会話のセキュリティを確保し、リプレイ アタックからの保護を提供するプロトコル。
SSL	インターネットでの電子メールなどのデータ通信を保護する暗号化プロトコル。後継のTLSと同等の機能を持ちます。
トランスポート レイヤ セキュリティ（TLS）	インターネットでの電子メールなどのデータ通信を保護する暗号化プロトコルで、機能としては SSL と同等です。
信頼リスト	デジタル署名なしの証明書リスト。

用語	定義
信頼ストア	Unified Communications Manager などのアプリケーションが明示的に信頼する X.509 証明書のリポジトリ。
X.509	PKI 証明書インポート用の ITU-T 暗号化規格であり、証明書の形式が含まれます。

システム要件

認証または暗号化に関するシステム要件は次のとおりです。

- 管理者パスワードは、クラスタ内の各サーバで異なる必要があります。
- Cisco CTL クライアントで使用されたユーザ名とパスワード（Unified Communications Manager サーバへのログイン用）は [Unified Communications Manager Administration] のユーザ名およびパスワード（[Unified Communications Manager Administration] へのログインに使用するユーザ名とパスワード）と一致する必要があります。
- ボイス メール ポートのセキュリティを設定する前に、この Cisco Unified Communications Manager リリースをサポートするバージョンの Cisco Unity または Unity Connection システムをインストールしていることを確認します。

機能一覧

Unified Communications Manager システムは、コール セキュリティに対してトランスポート層からアプリケーション層にかけてのマルチレイヤ アプローチを採用しています。

Transport Layer Security には、シグナリングの認証と暗号化のための TLS および IPSec が含まれ、音声ドメインへのアクセスの制御と防止が実現されます。SRTP によってメディアの認証と暗号化が付加され、音声会話と他のメディアのプライバシーと機密性が保護されます。

次の表は、機能のサポート状況と設定状況に応じて SCCP コール セッション中に Unified Communications Manager に実装可能な認証と暗号化機能の概要を示します。

表 *3 : SCCP* コールのセキュリティ機能

セキュリティ機能	回線側	トランク側
転送/接続/整合性	セキュア TLS ポート	IPSec 関連付け
デバイス認証	Unified Communications Manager や CAPF による TLS 証明書交換	IPSec 証明書交換または事前共有キー

セキュリティ機能	回線側	トランク側
シグナリング認証/暗号化	TLS モード：認証済みまたは暗号化済み	IPSec（認証ヘッダー、暗号化（ESP）、または両方）
メディア暗号化	SRTP	SRTP
許可	プレゼンス要求	プレゼンス要求
（注）　デバイスでサポートされる機能はデバイス タイプによって異なります。		

次の表に、機能のサポート状況と設定状況に応じて SIP コール セッション中に Unified Communications Manager に実装可能な認証と暗号化機能の概要を示します。

表 *4: SIP* コールのセキュリティ機能

セキュリティ機能	回線側	トランク側
転送/接続/整合性	セキュア TLS ポート	セキュア TLS ポート
デバイス認証	Unified Communications Manager や CAPF による TLS 証明書交換	IPSec 証明書交換または事前共有キー
ダイジェスト認証	各 SIP デバイスが一意のダイジェストユーザ クレデンシャルを使用します。	SIP トランク ユーザ エージェントは一意のダイジェスト クレデンシャルを使用します。
シグナリング認証/暗号化	TLS モード：認証済みまたは暗号化済み（Cisco Unified IP Phone 7942/7962 を除く）。	TLS モード：認証済みまたは暗号化済みモード
メディア暗号化	SRTP	SRTP
許可	プレゼンス要求	プレゼンス要求 方式リスト
（注）　デバイスでサポートされる機能はデバイス タイプによって異なります。		

セキュリティ アイコン

Unified Communications Manager は、コールに参加する Unified Communications Manager サーバおよびデバイスのセキュリティ レベルに応じてコールのセキュリティ ステータスを提供します。

セキュリティ アイコンをサポートする電話には、コールのセキュリティ レベルが表示されます。

- 電話は、シグナリング セキュリティ レベルが「認証済み」のコールに対してはシールド アイコンを表示します。シールドは Cisco IP デバイス間のセキュアな接続を示します。これは、デバイスのシグナリングが認証済みまたは暗号化されていることを意味します。
- 電話は、暗号化されたメディアのコールに対してはロック アイコンを表示します。これは、デバイスが暗号化シグナリングと暗号化メディアを使用していることを意味します。

（注） 一部の電話モデルでは、ロック アイコンのみが表示されます。

コールのセキュリティ ステータスは、ポイントツーポイント、クラスタ間およびクラスタ内、マルチホップ コールで変わることがあります。SCCP 回線、SIP 回線、および H.323 シグナリングでは、参加エンドポイントへのコール セキュリティ ステータスの変更の通知がサポートされています。セキュリティ アイコンに関連する制約については、セキュリティ アイコンおよび暗号化に関するトピックを参照してください。

コールの音声とビデオ部分がコールのセキュリティ ステータスのベースとなります。コールは、音声とビデオ部分の両方がセキュアである場合に限り、安全とみなされます。次の表で、セキュリティアイコンが表示されるかどうかと、どのアイコンが表示されるかを決定するルールについて説明します。

表 *5:* セキュリティ アイコンの表示規則

コールのメディア タイプとデバイス タイプ	シールドおよびロック アイコンの両方を表示する電話	ロック アイコンのみを表示する電話
セキュアな音声のみ	ロック	ロック
セキュアな音声と非セキュアなビデオ	シールド	なし
セキュアな音声とセキュアなビデオ	ロック	ロック
非セキュアな音声のみの認証済みデバイス	シールド	なし
非セキュアな音声とビデオがある認証済みデバイス	シールド	なし
非セキュアな音声のみの非認証デバイス	なし	なし
非セキュアな音声とビデオがある非認証デバイス	なし	なし

（注） 「Override BFCP Application Encryption Status When Designating Call Security Status」サービス パラメータは、パラメータ値が [True] で音声がセキュアであると、ロック アイコンを表示します。この状態は、他のすべてのメディア チャネルのセキュリティ ステータスを無視します。デフォルト パラメータ値は [False] です。

電話会議と割り込みコールでは、セキュリティ アイコンは会議のセキュリティ ステータスを表示します。

連携動作と制限事項

ここでは、連携動作と制限事項について説明します。

セキュアな会議機能に関する連携動作と制限事項の詳細については、関連項目を参照してください。

連携動作

このセクションでは、Unified Communications Manager アプリケーションと Cisco のセキュリティ機能の連携動作について説明します。

プレゼンス

SIP を実行している電話やトランクにプレゼンス グループ認証を追加するには、プレゼンス グループを設定して、プレゼンス要求を認証済みユーザに限定します。

プレゼンス グループ設定の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

SIP トランクでプレゼンス要求を許可するには、SIP トランクでのプレゼンス要求を許可するよう Unified Communications Manager を設定します。また必要な場合には、リモートデバイスやアプリケーションからの着信プレゼンス要求の受け入れと認証を行うよう Unified Communications Manager を設定します。

SIP トランク

SIP で開始された転送機能、および SIP トランクでの Web 転送やクリック ツー ダイヤルといったその他転送関連の高度な機能を使用するには、着信 Out-of-Dialog REFER 要求を受け入れるよう SIP トランク セキュリティ プロファイルを設定します。

イベント レポートのサポート（MWI サポートなど）を提供する場合、および（ボイス メッセージ サーバなどからの）コールごとの MTP 割り当てを減少させる場合は、Unsolicited NOTIFY SIP 要求を受け入れるよう SIP トランク セキュリティ プロファイルを設定します。

Unified Communications Manager が、SIP トランクの外部コールを外部デバイスまたは外部パーティに転送できるようにするには（在席転送の場合など）、REFERS および INVITES の Replaces

ヘッダー付き SIP 要求を受け入れるよう、SIP トランク セキュリティ プロファイルを設定します。

エクステンション モビリティ

エクステンションモビリティの場合、ユーザのログインとログアウトの際にSIPダイジェストクレデンシャルが変化します。異なるユーザには異なるクレデンシャルが設定されるためです。

CTI

CAPF プロファイルを設定した場合（各 Unified Communications Manager Assistant ノードに 1 つ）、Unified Communications Manager Assistant は CTI へのセキュアな接続をサポートします（Transport Layer Security 接続）。

CTI/JTAPI/TAPI アプリケーションのインスタンスが複数実行されている場合、CTI TLS をサポートするには、CTI Manager と JTAPI/TSP/CTI アプリケーション間のシグナリングおよびメディア通信ストリームを保護するために、すべてのアプリケーションインスタンスに一意のインスタンス ID（IID）を設定する必要があります。

デバイス セキュリティ モードが認証済みまたは暗号化済みの場合、Cisco Unity-CM TSP は Unified Communications Manager TLS ポートを介して Unified Communications Manager に接続します。セキュリティ モードが非セキュアの場合、Cisco Unity TSP は CTI Manager ポートを介して Unified Communications Manager に接続します。

機能制限

ここでは、シスコのセキュリティ機能に適用される制限事項について説明します。

認証および暗号化

認証機能および暗号化機能をインストールして設定する前に、次の制限事項を考慮してください。

- シグナリング暗号化またはメディア暗号化は、デバイス認証なしでは実装できません。デバイス認証をインストールするには、Cisco CTL Provider サービスを有効にしてから、Cisco CTL クライアントをインストールして設定します。
- 混合モードを設定している場合、Unified Communications Manager ではネットワーク アドレス変換（NAT）がサポートされません。

  メディア ストリームのファイアウォール トラバーサルを許可するために、ファイアウォールで UDP を有効にできます。UDP を有効にすると、ファイアウォールの信頼できる側にあるメディア ソースが、ファイアウォールを介してメディア パケットを送信することにより、ファイアウォールを通過する双方向のメディア フローを開くことができます。

ヒント　ハードウェア DSP リソースはこのタイプの接続を開始できないため、ファイアウォールの外側に置く必要があります。

シグナリング暗号化では、NAT トラバーサルがサポートされません。NAT を使用する代わりに、LAN 拡張 VPN の使用を検討してください。

割り込みと暗号化

割り込みと暗号化には次の制約事項が適用されます。

- 帯域幅の要件のため、Cisco IP Phone 7942 と 7962 は、アクティブな暗号化されたコールでの暗号化されたデバイスからの割り込みをサポートしません。割り込みの試行は失敗します。発信側の電話では、割り込みが失敗したことを示すトーンが再生されます。
- リリース 8.2 以前のリリースを実行中の暗号化された Cisco IP Phone は、認証済み参加者または非セキュア参加者としてのみアクティブな通話に割り込みできます。
- 発信者がセキュアな SCCP コールに割り込む場合、システムはターゲットデバイスで内部トーン再生メカニズムを使用し、ステータスはセキュアのままになります。
- 発信者がセキュアな SIP コールに割り込む場合、システムは保留トーンを再生し、トーンの間 Unified Communications Manager がコールを非セキュアとして分類します。

（注）　リリース 8.3 以降を実行中の、非セキュアまたは認証済み Cisco IP Phone は、暗号化されたコールに割り込むことができます。会議のセキュリティ ステータスは、セキュリティ アイコンによって表示されます。

ワイドバンド コーデックと暗号化

以下の情報は、暗号化向けに設定され、ワイドバンド コーデック地域が割り当てられている Cisco Unified IP Phone 7962 および 7942 に適用されます。TLS/SRTP 向けに設定された Cisco Unified IP Phone 7962 および 7942 にのみ適用されます。

暗号化されたコールを確立するため、Unified Communications Manager はワイドバンド コーデックを無視して、電話のコーデック リストからサポートされる別のコーデックを選択します。コールに参加する他のデバイスが暗号化向けに設定されていない場合、Unified Communications Manager はワイドバンド コーデックを使用して、認証済または非セキュア コールを確立することがあります。

メディア リソースと暗号化

Unified Communications Manager は、メディア リソースが使用されないセキュアな Cisco Unified IP Phone（SCCP または SIP）、セキュアな CTI デバイス/ルート ポイント、セキュアな Cisco MGCP IOS ゲートウェイ、セキュアな SIP トランク、セキュアな H.323 ゲートウェイ、セキュ

アな会議ブリッジ、およびセキュアな H.323/H.245/H.225 トランクの間での認証済みコールと暗号化コールをサポートしています。次の状況では Unified Communications Manager はメディア暗号化を提供しません。

- トランスコーダに関連するコール
- メディア ターミネーション ポイントに関連するコール

（注） MTP 暗号化は、非パススルー MTP でのみサポートされていません。

電話のサポートと暗号化

SCCP を実行している次の Cisco Unified IP Phone は暗号化をサポートします。6901、6911、6921、6941、6945、6961、7906G、7911G、7925G、7925G-EX、7926G、7931G、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7975G、8941、8945、および 9961。

SIP を実行している次の Cisco Unified IP Phone は暗号化をサポートします。6901、6911、6921、6941、6945、6961、7811、7821、7841、7861、7832、79 06G、7911G、7941G、7941G-GE、7942G、7961G、7961G-GE、7962G、7965G、7975G、8811、8821、8821-EX、8832、8841、8845、8851、8851NR、8865、8865NR、8941、8945、8961、9971、および 9971。

詳細は、暗号化とこのバージョンの Unified Communications Manager をサポートする『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

警告 セキュリティ機能を最大限に活用するため、Cisco IP Phone をファームウェアリリース 8.3 に更新することが推奨されます。リリース 8.3 はこの Unified Communications Manager リリースの暗号化機能をサポートします。以前のリリースを実行している暗号化済みの電話は、これらの機能を完全にサポートしてはいません。これらの電話は、認証済みまたは非セキュアな参加者として、セキュアな会議と割り込みコールにのみ参加することができます。

以前のリリースの Unified Communications Manager でファームウェアリリース 8.3 を実行している Cisco IP Phone は、会議または割り込みコールにおいて、会議のセキュリティ ステータスではなく、電話の接続のセキュリティ ステータスを表示します。また、会議リストなどのセキュアな会議機能をサポートしません。

電話のサポートと暗号化された設定ファイル

すべての電話が暗号化された設定ファイルをサポートするわけではありません。暗号化された設定ファイルをサポートするが、署名を検証しない電話もあります。暗号化された設定ファイルをサポートするすべての電話には、完全に暗号化された設定ファイルを受信するために Unified Communications Manager リリース 5.0 以降と互換性があるファームウェアが必要です。

セキュリティ アイコンおよび暗号化

セキュリティ アイコンおよび暗号化には次の制約事項が適用されます。

- コールの転送やコール保留時などのタスクを実行するときに、暗号化ロック アイコンが電話に表示されない場合があります。MOH など、これらのタスクに関連付けられたメディア ストリームが暗号化されていない場合、ステータスが暗号化から非セキュアに変わります。
- Unified Communications Manager は、H.323 トランクを通過中のコールに対してはシールド アイコンを表示しません。
- PSTN に関連するコールでは、セキュリティ アイコンはコールの IP ドメイン部分のみのセキュリティ ステータスを示します。
- TLS 転送タイプを使用する場合、SIP トランクが報告するセキュリティ ステータスは暗号化または非認証です。SRTP がネゴシエートされると、セキュリティ ステータスは暗号化になります。SRTP がネゴシエートされていない場合は、非認証のままになります。これにより、Unified Communications Manager のコール制御は、SIP トランクに関連するコールの全体的なセキュリティ レベルを特定できます。

  SIP トランクは、ミートミー会議または C 割り込みなどの発生時に参加者が認証されると、認証済みの状態をトランク経由で報告します。（SIP トランクは引き続き TLS/SRTP を使用します。）
- セキュアなモニタリングと録音のため、SIP トランクは SIP 回線によって現在使用されているように SIP トランクのセキュリティ アイコンの状態を送信するときに既存の Call Info ヘッダー メカニズムを使用します。これにより、SIP トランクのピアがコールの全体的なセキュリティ ステータスをモニタできるようになります。
- 一部の電話モデルでは、ロック アイコンしか表示されず、シールド アイコンが表示されません。

クラスタ セキュリティ モードとデバイス セキュリティ モード

（注） デバイス セキュリティ モードは、Cisco IP Phone または SIP トランクのセキュリティ機能を設定します。クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します。

クラスタ セキュリティ モードが非セキュアになると、デバイス セキュリティ モードは電話の設定ファイルで非セキュアになります。このような状況では、デバイス セキュリティ モードに認証済みまたは暗号化済みが指定されていた場合でも、電話と SRST 対応ゲートウェイまたは Unified Communications Manager との間に非セキュアな接続が作成されます。[SRST Allowed] チェックボックスなど、デバイス セキュリティ モード以外のセキュリティ関連の設定は無視されます。[Unified Communications Manager Administration] でセキュリティ設定が削除されることはありませんが、セキュリティは実現されません。

電話が SRST 対応ゲートウェイへのセキュアな接続を試行するのは、クラスタ セキュリティ モードが混合モードであり、電話設定ファイルのデバイス セキュリティ モードが認証済みまたは暗号化済みに設定され、[Trunk Configuration] ウィンドウで [SRST Allowed?] チェックボックスがオンであり、かつ電話設定ファイルに有効な SRST 証明書が存在する場合のみです。

ダイジェスト認証と暗号化

Unified Communications Manager では、SIP コールが 2 つ以上の独立したコール レッグとして定義されます。2 つの SIP デバイス間での標準の 2 者間通話の場合、2 つのコール レッグが存在します。1 つのレッグは発信元 SIP ユーザ エージェントと Unified Communications Manager の間（発信元コール レッグ）、もう 1 つのレッグは Unified Communications Manager と接続先 SIP ユーザ エージェントとの間です（終端コール レッグ）。各コール レッグが個別のダイアログを表します。ダイジェスト認証はポイントツーポイント プロセスであるため、各コール レッグでのダイジェスト認証は他のコール レッグから独立しています。SRTP 機能は、ユーザ エージェント間でネゴシエートされる機能に応じて、コール レッグごとに変更できます。

パケット キャプチャと暗号化

SRTP 暗号化を実装すると、サードパーティのスニフィング ツールが機能しません。適切な認証で承認された管理者は [Unified Communications Manager Administration] で設定を変更してパケット キャプチャを開始できます（パケット キャプチャをサポートしているデバイスの場合）。このリリースに対応した『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照し、Unified Communications Manager でのパケット キャプチャの設定に関する情報をご確認ください。

ベスト プラクティス

セキュリティの設定時には、次のベストプラクティスを強く推奨します。

- 必ず安全なラボ環境でインストール作業および設定作業を実行してから、広範囲のネットワークに展開します。
- リモート ロケーションにあるゲートウェイおよびその他のアプリケーション サーバに対して IPSec を使用します。

警告 IPSec を使用しない場合、セッション暗号キーがクリア テキストで転送されます。

- 電話料金の詐欺行為を防止するためには、『*System Configuration Guide for Cisco Unified Communications Manager*』で説明されている会議の機能拡張を設定します。同様に、コールの外部転送を制限する設定作業を実行します。この作業の実行方法については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

デバイスのリセット、サーバとクラスタのリブート、サービスの再起動

ここでは、Cisco Unified Serviceability でどのようなときにデバイスのリセット、サーバ/クラスタのリブート、サービスの再起動が必要になるかについて説明します。

次の注意事項を考慮してください。

- [Cisco Unified Communications Manager Administration] で単一のデバイスに別のセキュリティ プロファイルを適用した後は、そのデバイスをリセットします。
- 電話のセキュリティ強化作業を実施した場合、デバイスをリセットします。
- 混合モードから非セキュア モード（またはその逆）にクラスタのセキュリティ モードを変更した後は、デバイスをリセットします。
- Cisco CTL クライアントの設定後、または CTL ファイルの更新後は、すべてのデバイスを再起動します。
- CAPF エンタープライズ パラメータを更新した後は、デバイスをリセットします。
- TLS 接続ポートを更新した後は、Cisco CTL Provider サービスを再起動します。
- 混合モードから非セキュア モード（またはその逆）にクラスタのセキュリティ モードを変更した後は、Cisco CallManager サービスを再起動します。
- 関連する CAPF サービス パラメータを更新した後は、Cisco Certificate Authority Proxy Function サービスを再起動します。
- Cisco CTL クライアントの設定後、または CTL ファイルの更新後は、Cisco Unified Serviceability 内の Cisco CallManager サービスおよび Cisco TFTP サービスをすべて再起動します。クラスタ内でこれらのサービスを実行するすべてのサーバで、この作業を実行します。
- CTL Provider サービスを開始または停止した後は、Cisco CallManager サービスおよび Cisco TFTP サービスをすべて再起動します。
- セキュア SRST リファレンスの設定後は、従属デバイスをリセットします。
- Smart Card サービスを [Started] および [Automatic] に設定した場合、Cisco CTL クライアントをインストールした PC をリブートします。
- アプリケーションユーザ CAPF プロファイルに関連付けられたセキュリティ関連のサービス パラメータを設定した後は、Cisco IP Manager Assistant サービス、Cisco WebDialer Web サービスおよび Cisco Extended Functions サービスを再起動します。

Cisco CallManager サービスの再起動については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

電話の設定を更新した後に単一のデバイスをリセットするには、電話セキュリティ プロファイルの適用に関連したトピックを参照してください。

デバイスのリセット、サーバとクラスタのリブート、サービスのリセット

この項では、デバイスのリセット、Cisco Unified Serviceability でのサービスの再起動、またはサーバ/クラスタのリブートが必要となる場合について説明します。

クラスタのすべてのデバイスをリセットするには、次の手順を実行します。

始める前に

作業を進める前にデバイスのリセット、サーバとクラスタのリブートとサービスの再起動に関するガイドラインを参照してください。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[System]** > **[Cisco Unified CM]** を選択します。

[Find/List] ウィンドウが表示されます。

ステップ 2 [Find] をクリックします。

設定されている Unified Communications Manager サーバの一覧が表示されます。

ステップ 3 デバイスをリセットする Unified Communications Manager を選択します。

ステップ 4 [Reset] をクリックします。

ステップ 5 クラスタ内の各サーバでステップ 2 （17 ページ）とステップ 4 （17 ページ）を実行します。

割り込みによるメディア暗号化の設定

暗号化が設定されている Cisco Unified IP Phone 7962 および 7942 に割り込みを設定しようとすると、次のメッセージが表示されます。

注目 Cisco Unified IP Phone のモデル 7962 および 7942 に暗号化を設定する場合、暗号化されたコールに参加している間、それらの暗号化されたデバイスは割り込みリクエストを受け付けることができません。コールが暗号化されていると、割り込みの試行は失敗します。

[Unified Communications Manager Administration] で以下の作業を行うと、メッセージが表示されます。

- CTL クライアントの [Cluster Security Mode] パラメータを更新する。
- [Service Parameter] ウィンドウの [Builtin Bridge Enable] パラメータを更新する。

暗号化されたセキュリティ プロファイルが Cisco Unified IP Phone 7962 および 7942 に設定され、[Built In Bridge] 設定で **[Default]**（または [Default] と同等の設定）を選択した場合には、このメッセージは [Phone Configuration] ウィンドウに表示されません。ただし同じ制限が適用されます。

ヒント　変更を有効にするには、従属する Cisco IP デバイスをリセットする必要があります。

詳細については、割り込みと暗号化に関連する項目を参照してください。

CTLクライアント、SSL、CAPF、およびセキュリティトークンのインストール

認証サポートを実現するために、次のいずれかのオプションを選択できます。

1. [Unified Communications Manager Administration] から Cisco CTL クライアントをインストールします。Cisco CTL クライアント オプションの場合、少なくとも 2 つのセキュリティ トークンを入手する必要があります。
2. CLI コマンドセット **utils ctl** を使用します。この場合、セキュリティ トークンは不要です。このオプションの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

Unified Communications Manager をインストールすると、メディアおよびシグナリングの暗号化機能が自動的にインストールされます。

Unified Communications Manager によって、Unified Communications Manager 仮想ディレクトリ用のセキュア ソケット レイヤ（SSL）が自動的にインストールされます。

Cisco Certificate Authority Proxy Function（CAPF）では、[Unified Communications Manager Administration] の一部として自動的にインストールされます。

TLS および IPSec

転送セキュリティはデータのコーディング、パッキング、および送信を扱います。Unified Communications Manager は次のセキュアなトランスポート プロトコルを提供しています。

- Transport Layer Security（TLS）はセキュア ポートと証明書交換を使用して、2 つのシステム間またはデバイス間でセキュアで信頼できるデータ転送を実現します。TLS は音声ドメインへのアクセスを防ぐために、Unified Communications Manager 制御システム、デバイス、およびプロセス間の接続を保護および制御します。Unified Communications Manager は TLS を使用して SCCP を実行する電話へのセキュアな SCCP コール、および SIP を実行する電話またはトランクへの SIP コールを保護します。

- IP Security（IPSec）は、Unified Communications Manager とゲートウェイ間のセキュアで信頼できるデータ転送を実現します。IPSec は、 Cisco IOS MGCP および H.323 ゲートウェイにシグナリング認証および暗号化を実装します。

セキュア RTP（SRTP）サポートするデバイスにおいて、TLS および IPSec 転送サービスに次のセキュリティ レベルの SRTP を追加できます。SRTP はメディア ストリーム（音声パケット）を認証および暗号化し、Cisco Unified IP Phone の TDM またはアナログ音声ゲートウェイ ポートから発信または終了した音声会話が、音声ドメインへのアクセスを得ている可能性のある盗聴者から保護します。SRTP は、リプレイ アタックに対する保護を追加します。

Cisco Unified Communications Manager 9.0 以降はデュアル モード スマートフォンの TLS/SRTP サポートを提供しています。TLS は携帯電話については IP Phone と同じセキュアで信頼できるデータ転送モードを設定し、SRTP は音声会話を暗号化します。

証明書

証明書は、クライアントとサーバのアイデンティティを保護します。ルート証明書がインストールされた後、証明書はルート信頼ストアに追加され、デバイスとアプリケーション ユーザとの間を含め、ユーザとホストの間の接続を保護します。

管理者はサーバ証明書のフィンガープリントの参照、自己署名証明書の再生性、および信頼証明書の削除を Cisco Unified Communications Operating System GUI で実行できます。

管理者は、自己署名証明書の再生成と参照を CLI（コマンド ライン インターフェイス）でも実行できます。

CallManager 信頼ストアの更新と証明書の管理の詳細については、この Unified Communications Manager リリースに対応した『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

（注）

- Unified Communications Manager でサポートされている証明書の形式は PEM（.pem）および DER（.der）だけです。
- DER あるいは PEM の証明書のサポートされる最大サイズは 4096 ビットです。

（注） 2 つの証明書をアップロードする場合は、それらの共通名と有効期間は同じであるものの、シリアル番号と署名アルゴリズムは異なるものであることを確認してください。

たとえば、Cisco Unified Communications Manager tomcat-trust には、シリアル番号が 27:20:41:0c: 5b:08:69:80:42:62:4f:13:bd:16:06:6a、アルゴリズムが SHA1 のルート CA が存在します。シリアル番号が 7b:35:33:71:0b:7 c: 08:b2:47:b3:aa:f9:5 c: 0 d: ca:e4、アルゴリズムが SHA256 の証明書をアップロードしようとすると、証明書の管理処理は次のように実行されます。

1. 受信した証明書の妥当性が検証されます。
2. Tomcat 信頼フォルダから、共通名が同じである証明書が検索されます。
3. Tomcat 信頼フォルダの既存の証明書のシリアル番号と、アップロードしている受信証明書のシリアル番号がチェックされます。それらのシリアル番号が異なる場合は、両方の証明書の有効期限開始日を確認します。アップロードしている証明書の有効期限開始タイムスタンプが、既存の証明書の有効期限開始タイムスタンプよりも後である場合、Tomcat 信頼フォルダの中の既存の証明書が新しく受信した証明書で置き換えられます。そうでない場合、新しい証明書はアップロードされません。

SHA1 と SHA256 のアルゴリズムでは、件名または共通名が同じであれば、同じエンティティに属していることを意味しています。Unified Communications Manager のフレームワークでは、Unified Communications Manager サーバでそれらの 2 つのアルゴリズムを同時にサポートすることはしません。特定の信頼フォルダ内では、署名アルゴリズムが何であれ、いずれかのエンティティに属する 1 つの証明書のみがサポートされます。

電話の証明書タイプ

シスコは次の証明書タイプを電話で使用します。

- 製造元でインストールされる証明書（MIC）：Cisco Manufacturing はこの証明書をサポートされている電話に自動的にインストールします。製造元でインストールされる証明書は LSC インストールの Cisco Certificate Authority Proxy Function（CAPF）を認証します。製造元でインストールされる証明書を上書きしたり、削除することはできません。
- ローカルで有効な証明書（LSC）：このタイプの証明書は Cisco Certificate Authority Proxy Function（CAPF）に関連する必要な作業の実行後に、電話にインストールされます。デバイス セキュリティ モードを認証または暗号化に設定した後で、LSC は Unified Communications Manager と電話の間の接続を保護します。

ヒント　製造元でインストールされる証明書（MIC）をLSCのインストールでのみ使用することが推奨されます。シスコではCisco Unified Communications ManagerとのTLS接続の認証のためにLSCをサポートしています。MICルート証明書は侵害される可能性があるため、TLS認証またはその他の目的にMICを使用するように電話を設定するお客様は、ご自身の責任で行ってください。MICが侵害された場合シスコはその責任を負いません。

将来的な互換性の問題を回避するため、Unified Communications ManagerとのTLS接続にLSCを使用するためにCisco Unified IP Phone 6900シリーズ、7900シリーズ、8900シリーズ、9900シリーズをアップグレードし、MICルート証明書をCallManager信頼ストアから削除することが推奨されます。Unified Communications ManagerとのTLS接続にMICを使用する一部の電話モデルは登録できない場合があることに注意してください。

管理者はCallManager信頼ストアから次のMICルート証明書を削除する必要があります。

CAP-RTP-001

CAP-RTP-002

Cisco_Manufacturing_CA

Cisco_Root_CA_2048

Cisco_Manufacturing_CA_SHA2

Cisco_Root_CA_M2

ACT2_SUDI_CA

CAPF信頼ストアに残されたMICルート証明書は、証明書のアップグレードに使用されます。CallManager信頼ストアの更新および証明書の管理についての詳細は、このリリースに対応した『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

（注）　CallManager信頼ストアから証明書を削除した場合、UCMは電話機のMICを信頼しないため、セキュア オンボーディング機能は動作しません。

サーバ証明書のタイプ

Unified Communications Managerサーバでは次の自己署名（所有）証明書タイプが使用されます。

- HTTPS証明書（Tomcat）:自己署名ルート証明書は、HTTPSサーバのUnified Communications Managerインストール時に生成されます。Cisco Unity Connectionは、SMTPおよびIMAPサービスにこの証明書を使用します。
- CallManager証明書：自己署名ルート証明書はUnified Communications Managerサーバに Unified Communications Managerをインストールするときに、自動的にインストールされます。

- CAPF 証明書：Cisco CTL クライアント設定を完了すると、Unified Communications Manager のインストール時に生成されるこのルート証明書が、ご使用のサーバまたはクラスタ内のすべてのサーバにコピーされます。
- IPSec 証明書（ipsec_cert）：自己署名ルート証明書は、Unified Communications Manager のインストール時に、MGCP および H.323 ゲートウェイとの IPSec 接続用に生成されます。
- SRST 対応ゲートウェイの証明書：[Unified Communications Manager Administration] でのセキュアな SRST リファレンスの設定時に、Unified Communications Manager は SRST 対応ゲートウェイの証明書をゲートウェイから取得し Unified Communications Manager データベースに保存します。デバイスをリセットすると、証明書は電話の設定ファイルに追加されます。証明書はデータベースに格納されているため、証明書の管理ツールでこの証明書を管理することはできません。
- TVS 証明書：信頼検証サービス（TVS）をサポートする自己署名証明書です。
- Phone-SAST-trust 証明書：このカテゴリでは、システムが Cisco Unified IP Phone の VPN 証明書をインポートできます。これらの証明書は Midlet 信頼ストアに保存されます。
- 電話証明書信頼ストア（Phone-trust）：Unified Communications Manager はこの証明書タイプを使用して電話での HTTPS アクセスをサポートします。Cisco Unified Communications Operating System GUI を使用して証明書を Phone-trust ストアにアップロードできます。Cisco Unified IP Phone からの安全な Web アクセス（HTTPS）をサポートするため、Phone-CTL-trust にある証明書は CTL ファイルのメカニズムによって電話にダウンロードされます。電話の信頼証明書はサーバに残り、電話は TVS 経由でリクエスト可能です。

Unified Communications Manager は次のタイプの証明書を CallManager 信頼ストアにインポートします。

- Cisco Unity サーバまたは Cisco Unity Connection 証明書：Cisco Unity および Cisco Unity Connection はこの自己署名ルート証明書を使用して Cisco Unity SCCP および Cisco Unity Connection SCCP のデバイス証明書に署名します。Cisco Unity では、Cisco Unity Telephony Integration Manager（UTIM）がこの証明書を管理します。Cisco Unity Connection では、Cisco Unity Connection Administration がこの証明書を管理します。
- Cisco Unity および Cisco Unity Connection SCCP デバイス証明書：Cisco Unity および Cisco Unity Connection SCCP デバイスはこの署名付き証明書を使用して Unified Communications Manager との TLS 接続を確立します。
- 証明書の名前はボイス メール サーバ名に基づく証明書のサブジェクト名のハッシュを表しています。すべてのデバイス（またはポート）が、ルート証明書をルートとする証明書を発行します。
- SIP プロキシ サーバの証明書：CallManager 信頼ストアに SIP ユーザ エージェントの証明書が含まれ、SIP ユーザエージェントの信頼ストアに Cisco Unified Communications Manager 証明書が含まれる場合、SIP トランク経由で接続する SIP ユーザ エージェントは Unified Communications Manager に対して認証されます。

次の信頼ストアがあります。

- Tomcat および Web アプリケーション用の共通信頼ストア
- IPSec-trust
- CAPF-trust
- Userlicensing-trust
- TVS-trust
- Phone-SAST-trust
- Phone-CTL-trust

外部 CA からの証明書のサポート

Unified Communications Manager は PKCS#10 証明書署名要求（CSR）のメカニズムを利用してサードパーティ認証局（CA）との統合をサポートします。これは Cisco Unified Communications Operating System 証明書マネージャ GUI でアクセス可能です。現在サードパーティ CA を使用しているお客様は、Cisco CallManager、CAPF、IPSec、および Tomcat 証明書を発行するために CSR のメカニズムを使用する必要があります。

（注） マルチサーバ（SAN）CA 署名付き証明書を使用する際、マルチサーバ証明書は、パブリッシャにアップロードされる時点でクラスタに存在するノードのみに適用されます。したがって、ノードを再構築したり、クラスタに新しいノードを追加したりするたびに、新しいマルチサーバ証明書を生成して、クラスタにアップロードする必要があります。

システムを混合モードで実行すると、キー サイズが 4096 以上の CA 証明書を受け入れないエンドポイントもあります。CA 証明書を混合モードで使用するには、次のいずれかのオプションを選択してください。

- 証明書のキー サイズが 4096 未満の証明書の使用
- 自己署名証明書の使用

（注） このリリースの Unified Communications Manager は SCEP インターフェイスをサポートしません。

サードパーティの CA 署名付き証明書をプラットフォームにアップロードした後、CTL クライアントを実行して CTL ファイルを更新する必要があります。CTL クライアントの実行後、更新のために適切なサービスを再起動します。たとえば、Unified Communications Manager 証明書を更新するときは Cisco CallManager および Cisco TFTP サービスを再起動し、CAPF 証明書を更新するときは CAPF を再起動します。

（注） Cisco CallManager 証明書または CAPF 証明書をアップロードした後に、ITL ファイルを更新するために自動的に電話がリセットされる場合があります。

プラットフォームでの証明書署名要求（CSR）の生成については、この Unified Communications Manager リリースに対応した『Administration Guide for Cisco Unified Communications Manager』を参照してください。

認証、整合性、および許可

整合性および認証によって、次の脅威から保護されます。

- TFTP によるファイル操作（整合性）
- 電話と Unified Communications Manager との間で行われる呼処理シグナリングの変更（認証）
- で定義している中間者攻撃（認証） 表 2 : 用語 （2 ページ）
- 電話およびサーバの ID 盗難（認証）
- リプレイ アタック（ダイジェスト認証）

許可では、認証されたユーザ、サービス、またはアプリケーションが実行できるアクションを指定します。1 つのセッションで複数の認証方式と許可方式を実装できます。

イメージ認証

このプロセスは、電話へのロード前にバイナリ イメージ（ファームウェア ロード）が改ざんされることを防止します。イメージが改ざんされると、電話の認証プロセスが失敗し、イメージは拒否されます。イメージ認証は、Unified Communications Manager インストール時に自動的にインストールされた署名付きバイナリ ファイルを使用して実行されます。同様に、Web からダウンロードしたファームウェア アップデートでも、署名付きバイナリ イメージが提供されます。

デバイス認証

このプロセスは、通信デバイスのアイデンティティを検証し、エンティティが正当なものであることを確認します。

デバイス認証は、Unified Communications Manager サーバと、サポート対象の Cisco Unified IP Phone、SIP トランク、または JTAPI/TAPI/CTI アプリケーション（サポートされている場合）との間で発生します。これらのエンティティ間での認証済み接続は、それぞれのエンティティが相手側エンティティの証明書を受け入れた場合にのみ発生します。相互認証が、相互証明書交換のこのプロセスを表しています。

デバイス認証は、Cisco CTL ファイルの作成（Unified Communications Manager サーバ ノードとアプリケーションの認証時）、および Certificate Authority Proxy Function（電話と JTAPI/TAPI/CTI アプリケーションの認証時）に依存します。

ヒント SIP トランク経由で接続される SIP ユーザは、CallManager 信頼ストアに SIP ユーザ エージェント証明書が含まれ、SIP ユーザ エージェントの信頼ストアに Cisco Unified Communications Manager 証明書が含まれる場合に、Cisco Unified Communications Manager で認証されます。CallManager 信頼ストアの更新の詳細については、この Unified Communications Manager リリースに対応した『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ファイル認証

このプロセスは、設定ファイル、リング リスト ファイル、ロケール ファイル、および CTL ファイルなど、電話によってダウンロードされる、デジタル署名されたファイルを検証します。ファイルが作成後に改ざんされていないことを確認するため、電話によって署名が検証されます。サポートされるデバイスの一覧については、「「電話モデルのサポート」」を参照してください。

クラスタを混合モードに設定すると、リング リスト ファイル、ローカライズ ファイル、default.cnf.xml、リング リスト WAV ファイルなどのスタティック ファイルは TFTP サーバによって、.sgn フォーマットで署名されます。TFTP サーバは、ファイルのデータに発生した変更を検証するたびに、<device name>.cnf.xml フォーマットでファイルに署名します。

キャッシュが無効の場合、TFTP サーバは署名付きファイルをディスクに書き込みます。保存されたファイルが変更されたことが TFTP サーバによって確認された場合、TFTP サーバによってファイルが再度署名されます。ディスクの新しいファイルによって保存済みファイルが上書きされ、保存済みファイルは削除されます。電話が新しいファイルをダウンロードできるようになる前に、関連するデバイスを管理者が [Unified Communications Manager] で再起動する必要があります。

電話では、ファイルが TFTP サーバから受信されると、署名の検証によってファイルの整合性が確認されます。電話で認証済み接続を確立するには、次の条件への適合を確認します。

- 証明書が電話内に存在していること。
- CTL ファイルが電話に存在し、そのファイルに Unified Communications Manager エントリと証明書が存在していること。
- デバイスに認証または暗号化が設定されていること。

シグナリング認証

シグナリング整合性とも呼ばれるこのプロセスは、TLS プロトコルを使用して、伝送中にシグナリング パケットが改ざんされていないことを検証します。

シグナリング認証は証明書信頼リスト（CTL）ファイルの作成に依存します。

ダイジェスト認証

SIP トランクと電話のこのプロセスによって、Unified Communications Manager が Unified Communications Manager に接続されるデバイスのアイデンティティに対するチャレンジを実行できます。チャレンジが実施されると、デバイスはユーザ名とパスワードに類似したダイジェスト クレデンシャルを検証用に Unified Communications Manager に提出します。提出されたクレデンシャルが、データベース内でそのデバイスに対して設定されているクレデンシャルと一致した場合、ダイジェスト認証は成功となり、Unified Communications Manager によって SIP 要求が処理されます。

（注） クラスタ セキュリティ モードはダイジェスト認証に影響しないことに注意してください。

（注） あるデバイスのダイジェスト認証を有効にすると、登録する一意のダイジェスト ユーザ ID とパスワードが要求されます。

電話ユーザやアプリケーション ユーザには、Unified Communications Manager データベースで SIP ダイジェスト クレデンシャルを設定します。

- アプリケーションには、[Application User Configuration] ウィンドウでダイジェスト クレデンシャルを指定します。
- SIP を実行している電話には、[End User] ウィンドウでダイジェスト認証用のクレデンシャルを指定します。ユーザを設定した後にクレデンシャルを電話と関連付けるには、[Phone Configuration] ウィンドウで [Digest User]（エンドユーザ）を選択します。電話をリセットした後、クレデンシャルは TFTP サーバからその電話に提供される電話設定ファイル内に存在します。TFTP ダウンロードでダイジェスト クレデンシャルがクリアテキストで送信されないようにするには、暗号化された電話設定ファイルの設定に関連するトピックを参照してください。
- SIP トランクで受信したチャレンジの場合、レルム ユーザ名（デバイスまたはアプリケーション ユーザ）およびダイジェスト クレデンシャルを指定する SIP レルムを設定します。

外部電話やSIP実行中のトランクに対するダイジェスト認証を有効化してダイジェストクレデンシャルを設定する場合、Unified Communications Manager によってユーザ名、パスワード、レルムのハッシュを含むクレデンシャルのチェックサムが計算されます。システムでは、MD5 ハッシュの計算に、乱数であるナンス値が使用されます。値は Unified Communications Manager によって暗号化され、ユーザ名とチェックサムがデータベースに保存されます。

チャレンジを開始するために、Unified Communications Manager では SIP 401（Unauthorized）メッセージが使用されます。このメッセージのヘッダーにはナンスとレルムが含まれています。ナンス有効期間は、電話またはトランクの SIP デバイス セキュリティ プロファイルで設

定します。ナンス有効期間には、ナンス値が有効な時間を分単位で指定します。この時間が経過すると、その外部デバイスは Unified Communications Manager によって拒否され、新しい番号が生成されます。

（注） Unified Communications Manager は SIP トランク経由で着信した、回線側の電話やデバイスから発信された SIP コールに対してはユーザ エージェント サーバ（UAS）として動作し、SIP トランクに由来する SIP コールに対してはユーザ エージェント クライアント（UAC）として動作し、回線から回線へ、またはトランクからトランクへの接続に対してはバック ツーバック ユーザエージェント（B2BUA）として動作します。ほとんどの環境において、Unified Communications Manager は主に SCCP と SIP エンドポイントを接続する B2BUA として動作します。（SIP ユーザエージェントは、SIP メッセージを発信したデバイスまたはアプリケーションを表します。）

ヒント ダイジェスト認証では、整合性や機密性は提供されません。デバイスの整合性と機密性を確保するには、TLS をサポートするデバイスであれば、デバイスに TLS プロトコルを設定します。暗号化をサポートするデバイスであれば、デバイス セキュリティ モードを暗号化に設定します。暗号化された電話設定ファイルをサポートするデバイスであれば、ファイルに暗号化を設定します。

電話のダイジェスト認証

電話のダイジェスト認証を有効化すると、キープアライブ メッセージを除き、SIP を実行中の電話に対するすべての要求に対して Unified Communications Manager はチャレンジを実施します。Unified Communications Manager は回線側電話からのチャレンジに応答しません。

応答を受信すると、Unified Communications Manager はデータベースに保存されたユーザ名のチェックサムを、応答ヘッダー内のクレデンシャルに対して検証します。

SIP を実行中の電話は Unified Communications Manager レルムに存在します。このレルムはインストール時に [Unified Communications Manager Administration] で定義されます。電話へのチャレンジについて SIP レルムを設定するには、サービス パラメータ [SIP Station Realm] を使用します。各ダイジェスト ユーザには、レルムごとに 1 セットのダイジェスト クレデンシャルを設定できます。

ヒント エンドユーザのダイジェスト認証を有効にするが、ダイジェストクレデンシャルを設定しない場合、電話の登録が失敗します。クラスタ モードが非セキュアであり、かつダイジェスト認証が有効化されダイジェストクレデンシャルが設定されている場合、ダイジェストクレデンシャルが電話に送信され、Unified Communications Manager は依然としてチャレンジを開始します。

トランクのダイジェスト認証

トランクのダイジェスト認証を有効化すると、Unified Communications Manager は、SIP トランクを介して接続された SIP デバイスとアプリケーションからの SIP トランク要求に対してチャ

レンジを実施します。システムでは、チャレンジ メッセージ内で [Cluster ID] エンタープライズ パラメータが使用されます。SIP トランクを介して接続する SIP ユーザ エージェントは、[Unified Communications Manager] でデバイスまたはアプリケーションに設定された一意のダイジェスト クレデンシャルを使用して応答します。

Unified Communications Manager が SIP トランク要求を開始した場合、SIP トランクを介して接続された SIP ユーザ エージェントは Unified Communications Manager のアイデンティティにチャレンジを行えます。これらの着信チャレンジに対しては、要求されたクレデンシャルをユーザに提供するように SIP レルムを設定します。Unified Communications Manager が SIP 401（Unauthorized）または SIP 407（Proxy Authentication Required）メッセージを受信した場合、Unified Communications Manager はトランクを介して接続するレルムの暗号化パスワードおよびチャレンジ メッセージに指定されているユーザ名の暗号化されたパスワードをルックアップします。Unified Communications Manager によってパスワードが復号され、ダイジェストが計算され、応答メッセージ内に表現されます。

ヒント　レルムは、xyz.com のように SIP トランクを介して接続される領域を表し、要求の送信元を判別するのに役立ちます。

SIP レルムを設定するには、SIP トランクのダイジェスト認証の関連項目を参照してください。Unified Communications Manager にチャレンジを行うことができる SIP トランク ユーザ エージェントごとに、Unified Communications Manager で SIP レルム、ユーザ名、パスワードを設定する必要があります。各ユーザ エージェントには、レルムごとに 1 セットのダイジェスト クレデンシャルを設定できます。

認証

Unified Communications Manager では、許可プロセスを使用して、SIP が実行されている電話、SIP トランク、および SIP トランクの SIP アプリケーション要求からのメッセージについて、特定のカテゴリを制限します。

- SIP INVITE メッセージと in-dialog メッセージ、および SIP が実行されている電話の場合、Unified Communications Manager では、コーリング サーチ スペースおよびパーティションによって許可を与えます。
- 電話機からの SIP SUBSCRIBE 要求の場合、Unified Communications Manager では、プレゼンス グループへのユーザ アクセスに許可を与えます。
- SIP トランクの場合、Unified Communications Manager では、プレゼンス サブスクリプションおよび特定の非 INVITE SIP メッセージ（Out-of-Dialog REFER、Unsolicited NOTIFY、Replaces ヘッダー付き SIP 要求など）の許可を与えます。[SIP Trunk Security Profile Configuration] ウィンドウで、許可する SIP 要求をオンにする際に、許可を指定します。

SIP トランクのアプリケーションの許可を有効にするには、[SIP Trunk Security Profile] ウィンドウで [Enable Application Level Authorization] チェックボックスと [Enable Digest Authentication] チェックボックスをオンにしてから、[Application User Configuration] ウィンドウで許可する SIP 要求のチェックボックスをオンにします。

SIP トランクの許可とアプリケーション レベルの許可（認証）の両方を有効化した場合、最初に SIP トランクの許可が実行され、次に SIP アプリケーション ユーザの許可が実行されます。トランクの場合、Unified Communications Manager では、トランクのアクセス コントロール リスト（ACL）情報をダウンロードしてキャッシュします。ACL 情報は、着信 SIP 要求に適用されます。ACL で SIP 要求が許可されていない場合、コールは 403 Forbidden メッセージで失敗します。

ACL で SIP 要求が許可されている場合、Unified Communications Manager では、[SIP Trunk Security Profile] でダイジェスト認証が有効になっているかどうかを確認します。ダイジェスト認証が無効でアプリケーションレベルの認証も無効の場合、Unified Communications Manager では要求を処理します。ダイジェスト認証が有効な場合、Unified Communications Manager では、着信要求に認証ヘッダーが存在することを確認してから、ダイジェスト認証を使用して発信元アプリケーションを識別します。ヘッダーが存在しない場合、Unified Communications Manager では 401 メッセージでデバイスに対するチャレンジを行います。

アプリケーションレベルの ACL を適用する前に、Unified Communications Manager では、ダイジェスト認証で SIP トランク ユーザ エージェントを認証します。このため、アプリケーションレベルの許可（認証）を実行するには、事前に [SIP Trunk Security Profile] でダイジェスト認証を有効にする必要があります。

暗号化

ヒント　暗号化機能は、Unified Communications Manager をサーバにインストールするときに自動的にインストールされます。

ここでは、Unified Communications Manager のサポートする暗号化のタイプについて説明します。

セキュアエンドユーザログイン資格情報

Unified Communications Manager リリース 12.5(1) 以降、すべてのエンドユーザーログイン資格情報は強化されたセキュリティを提供するために SHA2 を使用してハッシュされています。Unified Communications Manager リリース 12.5(1) 以前は、エンド ユーザの ログイン クレデンシャルの [SHA1] のみを使用してハッシュされました。Unified Communications Manager リリース 12.5(1) には 「 古いクレデンシャルのアルゴリズムを持つユーザの Unified CM 」 レポートも含まれます。このレポートは、[Cisco Unified Reporting] ページで入手できます。このレポートを使用すると、管理者は、パスワードまたは PIN が SHA1 でハッシュされているすべてのエンドユーザをリストできます。

SHA1 でハッシュされているエンドユーザのパスワードまたは PIN はすべて、最初にログインが成功したときに自動的に SHA2 に移行されます。SHA1 でハッシュされている（古い）資格情報を持つエンドユーザは、次のいずれかの方法を使用して、自身の PIN またはパスワードを更新できます。

- 電話機のエクス テンション モビリティまたはディレクトリのアクセスにログインして、PIN を更新します。
- Cisco Jabber、Cisco Unified Communications セルフ ケアポータル、または Cisco Unified CM Administration にログインして、パスワードを更新します。

レポートを生成する方法の詳細についてを参照してください、 *Cisco Unified CM Administration Online Help* 。

シグナリング暗号化

シグナリング暗号化により、デバイスと Unified Communications Manager サーバ間で送信されるすべての SIP と SCCP シグナリング メッセージが暗号化されるようにできます。

シグナリング暗号化によって、相手に関連する情報、相手が入力した DTMF 番号、コール ステータス、メディア暗号キーなどの情報が、意図しないアクセスや不正なアクセスから保護されます。

クラスタを混合モードに設定している場合、Unified Communications Manager によるネットワーク アドレス変換（NAT）はサポートされません。NAT はシグナリング暗号化では動作しません。

ファイアウォールで UDP ALG を有効にし、メディア ストリームによるファイアウォール トラバーサルを許可できます。UDP ALG を有効にすると、ファイアウォールの信頼できる側のメディア ソースが、ファイアウォールを介してメディアパケットを送信することにより、ファイアウォールを通過する双方向のメディア フローを開くことができます。

ヒント　ハードウェア DSP リソースはこのタイプの接続を開始できないため、ファイアウォールの外側に置く必要があります。

シグナリング暗号化では、NAT トラバーサルがサポートされません。NAT を使用する代わりに、LAN 拡張 VPN の使用を検討してください。

メディア暗号化

Secure Real-Time Protocol（SRTP）を使用するメディア暗号化により、サポートされるデバイス間で対象の受信者だけがメディア ストリームを解釈できるようになります。メディア暗号化には、デバイスのメディアのマスター キー ペアの作成、デバイスへのキー配布、キーが転送される間のキー配布の保護などが含まれます。Unified Communications Manager では、SIP トランクに加えて、主に IOS ゲートウェイと、ゲートキーパー制御および非ゲートキーパー制御トランクの Unified Communications Manager H.323 トランク向けに SRTP がサポートされています。

（注） Cisco Unified Communications Manager では、デバイスおよびプロトコルの違いに応じて異なる方法でメディア暗号化キーが処理されます。SCCP を実行しているすべての電話は、Unified Communications Manager からメディア暗号化キーを取得します。この場合、TLS 暗号化シグナリング チャネルによって電話へのメディア暗号化キーのダウンロードが保護されます。SIP を実行している電話は、それ自体のメディア暗号化キーを生成して保存します。Unified Communications Manager システムによって導出されたメディア暗号化キーは、暗号化されたシグナリング パス経由で、H.323 用の IPSec で保護されたリンク、および SCCP と SIP 向けの MGCP または暗号化 TLS リンクを介してゲートウェイに安全に送信されます。

デバイスが SRTP をサポートしている場合、システムは SRTP 接続を使用します。1 つ以上のデバイスが SRTP をサポートしていない場合は、システムは RTP 接続を使用します。SRTP から RTP へのフォールバックは、セキュアなデバイスからセキュアではないデバイスへの転送、トランスコーディング、保留音などの場合に発生する可能性があります。

セキュリティ対応デバイスのほとんどにおいて、認証とシグナリング暗号化は、メディアを暗号化するための最小要件です。つまり、デバイスがシグナリング暗号化と認証をサポートしていない場合、メディア暗号化は行われません。Cisco IOS ゲートウェイおよびトランクでは、認証なしのメディア暗号化がサポートされています。SRTP 機能（メディア暗号化）を有効にする場合、Cisco IOS ゲートウェイおよびトランクに IPSec を設定する必要があります。

警告 Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイおよび H.323/H.245/H.225 トランクにおいて、セキュリティ関連情報が暗号化されずに送信されないようにすることは、IPSec 設定に依存しています。したがって、ゲートウェイおよびトランクに SRTP またはシグナリング暗号化を設定する前に、IPSec を設定することを強く推奨します。Unified Communications Manager は、IPSec 接続が正しく設定されていることを確認しません。IPSec を正しく設定しないと、セキュリティ関連情報が公開される可能性があります。

SIP トランクでは、セキュリティ関連情報が暗号化されない状態で送信されることがないようにするために、TLS が使用されます。

次の例は、SCCP および MGCP コールのメディア暗号化を示します。

1. デバイス A とデバイス B は、メディアの暗号化と認証をサポートしており、Unified Communications Manager に登録されています。
2. デバイス A がデバイス B に対してコールを発信すると、Unified Communications Manager はキーマネージャ機能に対しメディアセッションマスター値のセットを 2 つ要求します。
3. 両方のデバイスが 2 つのセットを受け取ります。 1 つはデバイス A からデバイス B へのメディア ストリーム用のセット、もう 1 つはデバイス B からデバイス A へのメディア ストリーム用のセットです。
4. デバイス A はマスター値の最初のセットを使用して、デバイス A からデバイス B へのメディア ストリームの暗号化と認証のためのキーを導出します。

5. デバイス A はマスター値の 2 番目のセットを使用して、デバイス B からデバイス A へのメディア ストリームの認証と復号のためのキーを導出します。
6. デバイス B はこれとは反対の操作手順でこれらのセットを使用します。
7. デバイスは、キーを受信した後に必要なキー導出を実行し、SRTP パケット処理が行われます。

（注） SIP を実行している電話と H.323 トランクまたはゲートウェイは、独自の暗号パラメータを生成し、Unified Communications Manager に送信します。

電話会議のメディア暗号化については、会議リソースの保護に関連する項目を参照してください。

AES 256 Encryption Support for TLS and SIP SRTP

Cisco Collaboration ソリューションは、Transport Layer Security（TLS）および Secure Real-time Transport Protocol（SRTP）を使用し、シグナリングとメディア暗号化を行います。現在、暗号化アルゴリズムとして、128 ビットの暗号キーを使用した Advanced Encryption Standard（AES）が使用されています。AES では、認証方式として Hash-based Message Authentication Code Secure Hash Algorithm-1（HMAC-SHA-1）も使用されます。これらのアルゴリズムは、変化していく不可欠なセキュリティとパフォーマンスのニーズを満たすために有効に拡張できません。セキュリティとパフォーマンスの要件の増大に対応するため、Next-Generation Encryption（NGE）での、暗号化、認証、デジタル署名、およびキー交換用のアルゴリズムとプロトコルが開発されています。また、AES 128 の代わりに、AES 256 暗号化のサポートが、NGE をサポートする TLS and Session Initiation Protocol（SIP）SRTP に提供されています。

AES 256 Encryption Support for TLS and SIP SRTP が、シグナリング暗号化とメディア暗号化での AES 256 暗号化のサポートに重点を置くために拡張されています。この機能は、Unified Communications Manager 上で実行されているアプリケーションが、SHA-2（Secure Hash Algorithm）標準規格および Federal Information Processing Standards（FIPS）に準拠する、AES-256 ベースの暗号を使用して TLS 1.2 接続を開始してサポートするために役立ちます。

この機能には、次の要件があります。

- SIP トランクおよび SIP 回線が開始する接続であること。
- Unified Communications Manager が SIP 回線と SIP トランクを通じた SRTP コール用にサポートする暗号化であること。

TLS での AES 256 および SHA-2 のサポート

Transport Layer Security（TLS）プロトコルでは、2 つのアプリケーション間の通信の認証、データの整合性、および機密性が提供されます。TLS 1.2 はセキュア ソケット レイヤ（SSL）プロトコル バージョン 3.0 をベースにしていますが、これら 2 つのプロトコルに相互の互換性はありません。TLS はクライアント/サーバ モードで動作し、一方がサーバとして機能し、もう一

方がクライアントとして機能します。SSL は Transmission Control Protocol（TCP）層とアプリケーション間のプロトコル層として位置付けられ、各クライアントとサーバ間にセキュアな接続を形成して、それらがネットワークを通じて安全に通信できるようにします。TLS が動作するためには、信頼性の高いトランスポート層プロトコルとして TCP が必要です。

Unified Communications Manager における、TLS 1.2 での AES 256 および SHA-2（Secure Hash Algorithm-2）のサポートは、SIP トランクおよび SIP 回線によって開始される接続を処理するための機能強化です。AES 256 および SHA-2 に準拠する、サポートされる暗号方式は次のとおりです。

- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256：暗号ストリングは ECDH-RSA-AES128-GCM-SHA256 です。
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384：暗号ストリングは ECDH-RSA-AES256-GCM-SHA384 です。

値は次のとおりです。

- TLS は、Transport Layer Security です
- ECDH は、アルゴリズムの楕円曲線 Diffie-Hellman です
- RSA は、アルゴリズムの Rivest Shamir Adleman です
- AES は、Advanced Encryption Standards です
- GCM は、Galois/Counter Mode です

新しくサポートされた暗号方式に加えて、Unified Communications Manager では、TLS_RSA_WITH_AES_128_CBC_SHA が引き続きサポートされています。この暗号方式の暗号ストリングは AES128-SHA です。

（注）
- Unified Communications Manager の証明書は、RSA に基づいています。
- Unified Communications Manager では、シスコの各エンドポイント（各電話）で、上記の TLS 1.2 用の新しい暗号方式はサポートされません。
- Unified Communications Manager において TLS 1.2 での AES 256 および SHA-2（Secure Hash Algorithm-2）のサポート機能強化を使用すると、Certificate Authority Proxy Function（CAPF）のデフォルトのキー サイズが 2048 ビットに増えます。

SRTP SIP コール シグナリングでの AES 256 のサポート

Secure Real-Time Transport Protocol（SRTP）では、Real-time Transport Protocol（RTP）の音声メディアとビデオ メディアの両方と、それらに付随する Real-time Transport Control Protocol（RTCP）ストリームに対して機密性およびデータの整合性を提供する方法を定義します。SRTP では、暗号化とメッセージ認証ヘッダーを使用して、この方法を実装します。SRTP では、暗号化は RTP パケットのペイロードだけに適用され、RTP のヘッダーには適用されません。た

だし、メッセージ認証は RTP のヘッダーと RTP のペイロードの両方に適用されます。また、メッセージ認証がヘッダー内の RTP のシーケンス番号に適用されるため、SRTP ではリプレイアタックに対する保護も間接的に提供されます。SRTP は、暗号化方法として 128 ビットの暗号キーによる Advanced Encryption Standard（AES）を使用します。また、認証方式として、Hash-based Message Authentication Code Secure Hash Algorithm-1（HMAC-SHA-1）も使用します。

Unified Communications Manager では、SIP 回線と SIP トランクを通じた SRTP コール用の暗号方式がサポートされます。これらの暗号方式は、AEAD_AES_256_GCM と AEAD_AES_128_GCM で、AEAD は Authenticated-Encryption with Associated-Data、GCM は Galois/Counter Mode です。これらの暗号方式は GCM に基づいています。これらの暗号方式が Session Description Protocol（SDP）内に存在する場合、AES 128 ベースの暗号方式および SHA-1 ベースの暗号方式に比べてより高い優先順位で処理されます。シスコの各エンドポイント（電話）では、Unified Communications Manager に SRTP のために追加した、これらの新しい暗号方式はサポートされません。

新たにサポートされる暗号方式に加えて、Unified Communications Manager では次の暗号方式が引き続きサポートされます。

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- F8_128_HMAC_SHA1_80

AES 256 暗号化は、次のコールでサポートされます。

- SIP 回線から SIP 回線へのコール シグナリング
- SIP 回線から SIP トランクへのシグナリング
- SIP トランクから SIP トランクへのシグナリング

Cisco Unified Communications Manager の要件

- SIP トランクと SIP 回線接続について TLS バージョン 1.2 がサポートされました。
- 暗号のサポート：TLS 1.2 接続時に、TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（暗号ストリング ECDHE-RSA-AES256-GCM-SHA384）および TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（暗号ストリング ECDHE-RSA-AES128-GCM-SHA256）が利用可能です。これらの暗号方式は GCM に基づいており、SHA-2 カテゴリに準拠しています。
- Unified Communications Manager は TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 暗号方式と TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 暗号方式を使用して TLS 1.2 を開始します。ピアが TLS 1.2 をサポートしていない場合、Unified Communications Manager は既存の AES128-SHA 暗号方式を使用した TLS 1.0 にフォールバックします。
- SIP 回線と SIP トランクを介した SRTP コールでは、GCM ベースの AEAD_AES_256_GCM 暗号方式と AEAD_AES_128_GCM 暗号方式がサポートされます。

連携動作と制限事項

- Unified Communications Manager の要件は、SIP 回線と SIP トランク、および基本的な SIP 間コールのみに適用されます。
- 非SIPプロトコルに基づくデバイスタイプでは、これまでのサポートされていた暗号による TLS バージョン使用時の動作が引き続きサポートされます。Skinny Call Control Protocol（SCCP）では、これまでにサポートされていた暗号による TLS 1.2 もサポートされています。
- SIP から非 SIP へのコールでは、引き続き AES 128 および SHA-1 ベースの暗号が使用されます。

AES 80 ビット認証サポート

Unified Communications Manager は、128 ビット暗号化キーと 80 ビット認証タグを保留音（MOH）、自動音声応答（IVR）、アナンシエータの暗号化アルゴリズムとして使用する Advanced Encryption Standard（AES）をサポートしています。デフォルトでは、80 ビット認証タグをサポートする電話は、MOH、IVR、アナンシエータを AES_CM_128_HMAC_SHA1_80 暗号化アルゴリズムを用いて再生します。

電話が IP 音声メディア ストリーミング（IPVMS）に安全に接続する際、AES_CM_128_HMAC_SHA1_80 暗号化アルゴリズムが優先的に使用されます。電話が 80 ビット認証をサポートしていない場合、AES_CM_128_HMAC_SHA1_32 暗号に戻ります。電話が 80 ビットまたは 32 ビットの認証タグのいずれかをサポートしていない場合は、Real-time Transport Protocol（RTP）でネゴシエーションを行います。

（注） SCCP 電話は 32 ビット認証タグしかサポートしていません。そのため、電話と IPVMS とのネゴシエーションは、AES_CM_128_HMAC_SHA1_32 暗号でのみ行われます。

電話 A が AES_CM_128_HMAC_SHA1_80 暗号化アルゴリズムをサポートし、電話 B が AES_CM_128_HMAC_SHA1_32 暗号化アルゴリズムをサポートしている場合、ユーザ A（電話 A）がユーザ B（電話 B）にダイヤルしユーザ B が保留にすると、ユーザ A は MOH に接続されます。電話 A は 80 ビット認証タグしかサポートしないため、電話 A と MOH のネゴシエーションは AES_CM_128_HMAC_SHA1_80 暗号を介して行われます。

ユーザ B（電話 B）がユーザ A（電話 A）にダイヤルし、ユーザ A が保留にする場合、電話 B は 32 ビット認証タグしかサポートしていないので、電話 B と MOH のネゴシエーションは AES_CM_128_HMAC_SHA1_32 暗号により行われます。

電話が 80 ビット認証タグをサポートする場合、電話と IVR またはアナンシエータとのネゴシエーションは AES_CM_128_HMAC_SHA1_80 で行われます。

次の表は、電話がサポートする暗号化アルゴリズムとネゴシエーション暗号を示しています。

表 *6:* 電話がサポートする暗号化アルゴリズムとネゴシエーション暗号

電話がサポートする暗号化アルゴリズム	ネゴシエーション暗号
AES_CM_128_HMAC_SHA1_32 と AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32	AES_CM_128_HMAC_SHA1_32
AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32 と AES_CM_128_HMAC_SHA1_80 以外	RTP に戻ります。

自己暗号化ドライブ

統一された CM は、自己暗号化ドライブ (SED) をサポートしています。これは、フル ディスク暗号化（FDE）とも呼ばれます。FDE は、ハードドライブで使用可能なすべてのデータを暗号化するために使用される暗号化方式です。このデータには、ファイル、オペレーティングシステム、およびソフトウェアプログラムが含まれます。ディスク上の使用可能なハードウェアは、すべての受信データを暗号化し、すべての送信データの暗号化を解除します。

ドライブがロックされると、暗号化キーが内部で作成され保存されます。このドライブに保存されているすべてのデータは、そのキーを使用して暗号化され、暗号化された形式で保存されます。FDE は、キー ID とセキュリティ キーで構成されます。

詳細については、https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/2-0/b_Cisco_UCS_C-series_GUI_Configuration_Guide_201/b_Cisco_UCS_C-series_GUI_Configuration_Guide_201_chapter_010011.html#concept_E8C37FA4A71F4C8F8E1B9B94305AD844を参照してください。

設定ファイルの暗号化

Unified Communications Manager は、ダイジェスト クレデンシャルや管理者パスワードといった機密データを、TFTP サーバからの設定ファイル ダウンロードの形で電話にプッシュします。

Unified Communications Manager において、データベース内では可逆暗号化を使用してこれらのクレデンシャルが保護されています。ダウンロードプロセス中のデータを保護するため、このオプションをサポートするすべての Cisco IP Phone において、暗号化された設定ファイルを設定することを推奨します。このオプションが有効にされると、デバイス設定ファイルだけがダウンロード用に暗号化されます。

（注） 状況によっては、機密データの電話へのダウンロードにクリアテキストを選択することもできます。たとえば、電話のトラブルシュートや自動登録などの場合が考えられます。

Unified Communications Managerは、暗号化キーを符号化してデータベースに保存します。TFTPサーバでは、対称暗号化キーを使用して設定ファイルの暗号化と復号が行われます。

- 電話に PKI 機能がある場合、Unified Communications Manager では電話の公開キーを使用して電話の設定ファイルを暗号化できます。
- 電話に PKI 機能がない場合、Unified Communications Manager と電話に一意の対称キーを設定する必要があります。

暗号化設定ファイルの設定は、[Unified Communications Manager Administration] の [Phone Security Profile] ウィンドウで有効化し、その後 [Phone Configuration] ウィンドウで電話に適用します。

暗号化された iX チャネル

Unified Communications Manager は、暗号化された iX チャンネルをサポートしています。IX チャネルは、ビデオ会議でのSIPフォン間でアプリケーションメディアを多重化するための信頼性の高いチャネルを提供します。暗号化された iX チャネルは、DTLS を使用して導入にセキュリティを追加し、アプリケーションメディアがiXチャネルを介して送信されるようにし、メディアを傍受しようとする中級者が見ることができないようにします。

[パススルーモード] の IOS MTP および RSVP エージェントは、暗号化された iX チャネルもサポートしています。

設定

ユニファイドコミュニケーションマネージャーの暗号化されたiXチャネルを有効にするには、次のことを実行する必要があります。

- 任意の中間 SIP トランクによって使用される [SIP プロファイル設定（SIP Profile Configuration）] の [**iX アプリケーション メディアを許可（Allow iX Application Media**）] チェックボックスをオンにします。この設定では、iXチャネルのネゴシエーションがオンになります。
- セキュア着信**アイコン表示ポリシー**サービスパラメータを設定して、セキュアロックアイコンを有効にします。デフォルトでは、[**BFCP および iX トランスポート以外の全メディアを暗号化すべき（All media except BFCP and iX transports must be encrypted**）] に設定されています。

暗号化モード

暗号化された電話機の場合、2 種類のセッション記述プロトコル (SDP) を使用して、ユニファイドコミュニケーションマネージャーがサポートしている暗号化チャネルの暗号化をサポートしています。この暗号化タイプは、エンドポイントがサポートするものであり、ユニファイドコミュニケーションマネージャーの設定可能な項目ではありません。

- **ベストエフォート方式**の暗号化: SDP オファーは暗号化された ix チャネルを目的としていますが、SIP ピアがサポートしていない場合は、暗号化されていない ix チャネルにフォー

ルバックします。このアプローチは、ソリューションで暗号化が必須ではない場合に使用することができます。

たとえば、暗号化はクラウドで必須であり、単一の企業ではありません。

ベストエフォート iX 暗号化

M = アプリケーション 12345 **UDP/UDT/IX ***

A = セットアップ: actpass

A = 指紋: SHA-1 < キー >

- **強制暗号化**: SDP オファーは、暗号化された iX チャネルに対してのみ使用できます。このオファーは、SIP ピアが iX チャネルの暗号化をサポートしていない場合には拒否されます。このアプローチは、エンドポイント間で暗号化が必須になっている展開で使用できます。

  たとえば、2 つの SIP デバイス間の暗号化は必須です。

  強制 iX 暗号化

  m = アプリケーション 12345 **UDP/DTLS/UDT/IX ***

  A = セットアップ: actpass

  A = 指紋: SHA-1 < キー >

デフォルトでは、すべての Cisco IP Phone はベストエフォート iX 暗号化を提供するように設定されています。ただし、Ciscoテレプレゼンスエンドポイントの製品固有の設定**内で**暗号化**モード**をオンに設定するか、または cisco Meeting Server の設定を再設定することによって、これを強制的に暗号化にすることができます。

非暗号化メディア

エンドポイントが完全なセキュア モードで導入されていない可能性がある場合は、Unified Communication Manager を使用して、会議のエンドポイントからのメディア パスでセキュア アクティブコントロールメッセージをネゴシエートできます。たとえば、エンドポイントがオフネットで、MRA モードの CUCM で登録されている場合などです。

前提条件

この機能の使用を開始する前に、次のことを確認してください。

- システムが輸出規制要件を満たしている
- 会議ブリッジへの SIP トランクがセキュアである

Unified CM は、セキュアでないエンドポイントまたはソフトフォンに対してセキュアアクティブ コントロール メッセージの DTLS 情報をネゴシエートし、次の方法でメッセージを受信できます。

- オンプレミスの登録済みエンドポイントまたはソフトフォンに対しては**ベストエフォート方式の暗号化 iX**

• オフプレミスの登録済みエンドポイントまたはソフトフォンに対しては**強制 iX 暗号化**

NMAP スキャン操作

すべての Windows または Linux プラットフォームで脆弱性スキャンを実行するには、Network Mapper（NMAP）スキャン プログラムを実行できます。NMAP はネットワーク調査やセキュリティ監査を行う、無料のオープン ソースのユーティリティです。

（注） NMAP DP スキャンは、完了までに最大 18 時間かかります。

シンタックス

nmap -n -vv -sU -p *<port_range> <ccm_ip_address>*

値は次のとおりです。

-n：DNS 解決なし。検出されたアクティブ IP アドレスに対して逆引き DNS 解決を行わないよう NMAP に指示します。NMAP 組み込みパラレル スタブ リゾルバを使用しても DNS の処理は遅くなる可能性があるため、このオプションを使用するとスキャン時間を削減できます。

-v：冗長性レベルを上げます。これにより、NMAP が出力する進行中のスキャンに関する情報が増えます。開いているポートは検出次第表示され、NMAP がスキャンに数分以上かかると推定した場合には完了までにかかる時間が表示されます。冗長度をさらに上げるには、このオプションを 2 回以上使用します。

-sU：UDP ポート スキャンを指定します。

-p：スキャンするポートを指定し、デフォルトをオーバーライドします。個々のポート番号と、ハイフンを使用したポート番号の範囲を使用できることにご注意ください（例：1-1023）。

ccm_ip_address：Cisco Unified Communications Manager の IP アドレス。

認証と暗号化のセットアップ

重要 この手順は CTL クライアントの暗号化オプションに適用されます。また、**utils ctl**CLI コマンドセットを使用して暗号化を設定することもできます。このオプションの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

次の手順は、認証および暗号化を実装するために必要なすべての手順を示します。指定されたセキュリティ機能のために行う必要がある作業を含む章の参考資料については、関連項目を参照してください。

- 新規インストールで認証と暗号化を実装するには、次の表を参照してください。
- ノードをセキュアクラスタに追加するには、ノードの追加方法および新しいノード用のセキュリティの設定方法を説明している『*Installing Cisco Unified Communications Manager*』を参照してください。

手順

ステップ 1 [Cisco Unified Serviceability] で Cisco CTL Provider サービスをアクティブにします。

クラスタの各 Unified Communications Manager サーバの Cisco CTL Provider サービスを必ずアクティブにします。

ヒント Unified Communications Manager のアップグレード前にこのサービスをアクティブにした場合は、サービスを再度アクティブにする必要はありません。アップグレード後にサービスは自動的にアクティブになります。

ステップ 2 ローカルで有効な証明書のインストール、アップグレード、トラブルシュート、または削除を行うには、[Cisco Unified Serviceability] で Cisco Certificate Authority Proxy サービスをアクティブにします。

最初のノードでのみ Cisco Certificate Authority Proxy サービスをアクティブにします。

ワンポイントアドバイス Cisco CTL クライアントをインストールして設定する前に、この作業を実行すれば、CAPF を使用するために CTL ファイルを更新する必要がなくなります。

ステップ 3 デフォルトのポート設定を使用しない場合は、TLS 接続用のポートを設定します。

ヒント Unified Communications Manager のアップグレードの前にこれらの設定項目を設定した場合は、設定項目はアップグレード中に自動的に移行されます。

ステップ 4 暗号化に Cisco CTL クライアントを使用している場合は、Cisco CTL クライアント用に設定するサーバについて、少なくとも 2 つのセキュリティ トークンとパスワード、ホスト名または IP アドレス、およびポート番号を入手します。

（注） **utils ctl** CLI オプションの場合、ハードウェア セキュリティ トークンは不要です。

ステップ 5 Cisco CTL クライアントをインストールします。

ヒント 今回のリリースの Unified Communications Manager にアップグレードした後で Cisco CTL ファイルを更新するには、今回のリリースの [Unified Communications Manager Administration] で利用可能なプラグインをインストールする必要があります。

ステップ 6 Cisco CTL クライアントを設定します。

ヒント Unified Communications Manager のアップグレード前に Cisco CTL ファイルを作成した場合、Cisco CTL ファイルはアップグレード中に自動的に移行されます。今回のリリースの Unified Communications Manager にアップグレードした後で Cisco CTL ファイルを更新するには、Cisco CTL クライアントの最新バージョンをインストールして設定する必要があります。

ステップ 7 電話セキュリティ プロファイルを設定します。

プロファイルを設定するときは、次の作業を実行します。

a) デバイスのセキュリティ モードを設定します。

ヒント デバイス セキュリティ モードは、Unified Communications Manager のアップグレード時に自動的に移行されます。以前のリリースの認証だけをサポートしていたデバイスに暗号化を設定する場合は、[Phone Configuration] ウィンドウで暗号化のセキュリティ プロファイルを選択する必要があります。

b) CAPF 設定を行います（SCCP および SIP を実行する一部の電話の場合）。

追加の CAPF 設定が [Phone Configuration] ウィンドウに表示されます。

c) SIP を実行する電話でダイジェスト認証を使用する場合は、[Enable Digest Authentication] チェックボックスをオンにします。

d) 暗号化された設定ファイルを有効にするには（SCCP および SIP を実行する一部の電話の場合）、[Encrypted Config] チェックボックスをオンにします。

e) 設定ファイルのダウンロードでダイジェスト クレデンシャルを除外するには、[Exclude Digest Credential in Configuration File] チェックボックスをオンにします。

ステップ 8 電話に電話セキュリティ プロファイルを適用します。

ステップ 9 電話に証明書を発行するように CAPF を設定します。

ヒント 今回のリリースの Unified Communications Manager へのアップグレード前に証明書の操作を実行し、CAPF をサブスクライバ サーバで実行した場合、CAPF データをパブリッシャ データベース サーバにコピーしてから、クラスタを今回のリリースの Cisco Unified Communications Manager にアップグレードする必要があります。

注意 Unified Communications Manager サブスクライバ サーバの CAPF データは Unified Communications Manager データベースに移行されないため、データをデータベースにコピーしなければ、データは失われます。データが失われても、CAPF ユーティリティを使用して発行したローカルで有効な証明書は電話に残ります。しかし、この証明書はもう有効でないため、今回のリリースの CAPF ユーティリティは証明書を再発行する必要があります。

次の手順は、省略可能です。

ステップ 10 サポートされている Cisco Unified IP Phone にローカルで有効な証明書がインストールされたことを確認します。

ステップ 11 SIP を実行する電話のダイジェスト認証を設定します。

ステップ 12 電話のセキュリティ強化作業を実行します。

ヒント 電話のセキュリティ強化設定を Unified Communications Manager のアップグレード前に設定した場合、デバイス設定はアップグレード中に自動的に移行されます。

ステップ 13 セキュリティ用の会議ブリッジ リソースを設定します。

ステップ 14 セキュリティ用のボイスメール ポートを設定します。

詳細については、このリリースの Unified Communications Manager の該当する Cisco Unity または Cisco Unity Connection 統合ガイドを参照してください。

ステップ 15 SRST リファレンスのセキュリティを設定します。

ヒント 前のリリースの Unified Communications Manager でセキュア SRST リファレンスを設定した場合、その設定は Unified Communications Manager のアップグレード中に自動的に移行されます。

ステップ 16 IPSec を設定します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 17 SIP トランク セキュリティ プロファイルを設定します。

ダイジェスト認証を使用する場合は、プロファイルの [Enable Digest Authentication] チェックボックスをオンにします。

トランクレベルの認証の場合、許可する SIP 要求の認証チェックボックスをオンにします。

トランクレベルの認証の後、アプリケーションレベルの許可を発生させる場合は、[Enable Application Level Authorization] チェックボックスをオンにします。

ダイジェスト認証をオンにしない限り、アプリケーションレベルの認証はオンにできません。

ステップ 18 SIP トランク セキュリティ プロファイルをトランクに適用します。

ステップ 19 トランクのダイジェスト認証を設定します。

ステップ 20 SIP トランク セキュリティ プロファイルで [Enable Application Level Authorization] チェックボックスをオンにした場合は、[Application User Configuration] ウィンドウの認証チェックボックスをオンにして、許可する SIP 要求を設定します。

ステップ 21 すべての電話をリセットします。

ステップ 22 すべてのサーバをリブートします。

暗号管理

Cipher management を使用すると、管理者は、各 TLS および SSH 接続で許可される一連のセキュリティ暗号を制御することができます。暗号管理では、弱い暗号を無効にして最小レベルのセキュリティを保証します。

[**Cipher Management**] ページには、デフォルト値はありません。代わりに、暗号化管理機能は、許可されている暗号を設定している場合にのみ有効になります。暗号管理ページで設定している場合でも、特定の弱い暗号は許可されません。

次の TLS インターフェイスおよび SSH インターフェイスで暗号を設定することができます。

- **すべての**tls: このフィールドに割り当てられている暗号は、ユニファイドコミュニケーションマネージャーおよびIMとプレゼンスのTLSプロトコルをサポートするすべてのサーバおよびクライアント接続に適用されます。
- **HTTPS TLS**: このフィールドに割り当てられる暗号は、ユニファイドコミュニケーションマネージャーおよびIMおよびプレゼンスのTLSプロトコルをサポートするポート443および8443上のすべてのCisco Tomcat接続に適用されます。**Https tls**および**すべての TLS**フィールドに暗号**を割り当てる場合、https tls**上で設定されて**いる暗号**がすべてのtls暗号を上書きします。
- **SIP TLS**: このフィールドに割り当てられる暗号は、ユニファイドコミュニケーションマネージャー上のTLSプロトコルをサポートするsip tlsインターフェイスを介して送受信されるすべての暗号化接続に適用されます。SCCPまたはCTIデバイスには適用されません。

  認証モードのSIPインターフェイスは、ナル-SHA暗号のみをサポートしています。SIPインターフェイスまたはすべてのインターフェイスで暗号化を設定した場合は、認証モードはサポートされなくなります。

  SIP TLSおよび**ALL TLS**フィールドで暗号を割り当てる場合、SIP TLSで設定した暗号は、ALL TLSs暗号を上書きします。
- **SSH の暗号化**: このフィールドに割り当てられる暗号は、ユニファイドコミュニケーションマネージャーおよびIMおよびプレゼンスのSSH接続に適用されます。
- **SSH キー交換**: このフィールドで割り当てられるキー交換アルゴリズムは、ユニファイドコミュニケーションマネージャーおよびIMとプレゼンスのSSHインターフェイスに適用されます。

カーブのネゴシエーション

次に、曲線のネゴシエーションの点を示します。

- ECDSAの暗号は、ECDSA証明書のキーサイズに基づいて、さまざまなECカーブとネゴシエートされます。
- RSAの暗号化は、証明書のキーサイズに関係なく、すべてのECカーブとネゴシエートされます。
- ECDSA証明書のキーサイズは、TLSネゴシエーションを発生させるための曲線サイズと同じである必要があります。

例：

クライアントがP-384 ECのカーブを提供する場合、384キー証明書とECDSAの暗号がネゴシエートされます。

曲線のネゴシエーションは、RSA暗号とECDSA暗号の両方のクライアント設定に基づいています。

例：

証明書のサイズが384ビットであり、クライアントのオファーリングがP-521の場合、P-384 P-256 ECのネゴシエーションが発生すると、P-521の曲線でTLSネゴシエーションが発生します。クライアントによって提供されるカーブは最初のP-521であり、P-384曲線もリストから利用できます。証明書サイズが384ビットであり、クライアントオファーリングがP-521、P-256の場合、P-384曲線がクライアントによって提供されないため、TLSネゴシエーションは行われません。

EC カーブでサポートされている暗号を次に示します。

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

推奨される暗号

警告 構成済みの暗号に、以下に示す推奨暗号が含まれていることを確認してください。含まれていない場合は、セキュアインターフェイスを介した他の製品との相互運用性に問題が発生する可能性があります。変更を有効にするには、**[暗号管理（Cipher Management）]** ページの値を変更したときに、影響を受けるサービスを再起動するかサーバをリブートします。

警告 SSH MACインターフェイスでsha2-512を設定すると、DRSとCDRの機能が影響を受けます。

暗号aes128-gcm@openssh.comの設定、"ssh Cipherの" フィールド内のaes256-gcm@openssh.com、またはssh kex "のsha2-nistp256アルゴリズムのみを設定すると、DRSとCDRの機能が失われます。

シスコでは、TLSおよびSSHインターフェイスの構成用に次の暗号ストリングを推奨しています。

TLS

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:
ECDHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA
```

SSH 暗号

```
aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
```

SSH MAC

```
hmac-sha2-256,hmac-sha1
```

FIPS 用の SSH KEX

```
ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1
```

非 FIPS 用の SSH KEX

```
ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha1,
diffie-hellman-group1-sha1,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1
```

暗号ストリングの設定

異なるセキュリティで保護されたインターフェイスで暗号文字列を設定するには、次の手順を実行します。

始める前に

- すべての **tls**、**SIP tls**、および**HTTPS tls**フィールドに必ず暗号文字列を OpenSSL cipher string 形式で入力してください。

  Ssh の**暗号化**、ssh MAC 、および**ssh キー交換**フィールドで、OpenSSH 形式の暗号またはアルゴリズムを入力してください。

- 推奨される暗号 （44 ページ）を確認してください。

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）]** > **[暗号の管理（Cipher Management）]** を選択します。

ステップ 2 **ALL TLS**、**SIP TLS**、**HTTP TLS**フィールドで暗号ストリングを設定するには、暗号ストリングを OpenSSL 暗号ストリング フォーマットで **[暗号ストリング（Cipher String）]** フィールドに入力します。

OpenSSL の暗号ストリング フォーマットの詳細については、https://www.openssl.org/docs/man1.0.2/apps/ciphers.htmlを参照してください。

（注） **[HTTPS TLS]** または **[SIP TLS]** フィールドの暗号ストリングを設定しない場合、デフォルトによりシステムは **ALL TLS** インターフェイスの設定を使用します。

（注） **All TLS**または**HTTPS TLS**フィールドで暗号文字列を設定しない場合、HTTPS TLS インターフェイスポート (8443) は、エンタープライズパラメータ (HTTPS 暗号) からの設定を取得します。

（注） **All TLS**または**SIP TLS**フィールドで暗号文字列を設定しない場合、SIP インターフェイスポート (5061) は、エンタープライズパラメータ (HTTPS 暗号) からの設定を暗号化モードで取得します。さらに、NULL-SHA 暗号を認証モードで取得します。

ステップ 3 **SSH 暗号化**、フィールドで暗号ストリングを設定するには、暗号ストリングを OpenSSL 暗号ストリング フォーマットで **[暗号ストリング（Cipher String）]** フィールドに入力します。

SSH 暗号化の OpenSSH の暗号ストリング フォーマットの詳細については、https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.htmlを参照してください。

[**Ssh cipher (ssh cipher)**] フィールドで暗号文字列を設定しなかった場合、デフォルトでは、次の暗号がすべての ssh 接続に適用されます。

FIPS モードで、次の様になります。

```
aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com
```

非 FIPS モードで、次のようになります。

```
aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com
```

ステップ 4 **[SSHキー交換（SSH Key Exchange）]** のキー交換アルゴリズムを設定するには、**[アルゴリズム文字列（Algorithm String）]** フィールドにアルゴリズム文字列を OpenSSH 文字列形式で入力します。

SSH キー交換用の OpenSSH アルゴリズム文字列形式の詳細については、https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.htmlを参照してください。

Ssh キー交換フィールドでキー交換アルゴリズムを設定しなかった場合、デフォルトでは、次のキー交換アルゴリズムがすべての ssh 接続に適用されます。

FIPS モードで、次の様になります。

```
diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

非 FIPS モードで、次のようになります。

```
diffie-hellman-group1-sha1, diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

ステップ 5 **[SSH MAC]** フィールドで MAC アルゴリズムを設定するには、**[アルゴリズム文字列（Algorithm String）]** フィールドにアルゴリズム文字列を OpenSSH 文字列形式で入力します。

SSH MAC の OpenSSH アルゴリズム文字列形式の詳細については、https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html を参照してください。

[**SSH MAC**)] フィールドで MAC アルゴリズムを設定しなかった場合、次の MAC アルゴリズムがデフォルトですべての SSH 接続に適用されます。

FIPS モードで、次の様になります。

```
hmac-sha1
```

非 FIPS モードで、次のようになります。

```
hmac-sha1
```

ステップ 6 **[保存（Save）]** をクリックします。

（注） 暗号化展開文字列および**アルゴリズム拡張文字列**フィールドを編集することはできません。

システムは、**All TLS**、**STP TLS**、**HTTPS TLS**、および**SSH 暗号化** における暗号化を検証し、**[実際の暗号方式（Actual Ciphers）]** フィールドに自動的に暗号方式を入力します。

[暗号ストリング（Cipher String）] フィールドに無効な暗号が入力されると、**[暗号化拡張文字列（Cipher Expansion String）]** フィールドに自動的な入力は行われず、以下のエラーが表示されます。

無効な暗号ストリングが入力されました

システムは、**[SSHキー交換（SSH Key Exchange）]** および **[SSH MAC]** フィールドのアルゴリズムを検証し、**[アルゴリズム拡張文字列（Algorithm Expansion String）]** フィールドに自動的にアルゴリズム文字列を入力します。

[アルゴリズム文字列（Algorithm String）] フィールドに無効なアルゴリズムが入力されると、**[アルゴリズム拡張文字列（Algorithm Expansion String）]** フィールドに自動的な入力は行われず、以下のエラーが表示されます。

無効なアルゴリズム文字列が入力されました

（注） [実際の暗号方式（Actual Ciphers）] または [実際のアルゴリズム（Actual Algorithms）] フィールドに自動的に入力される暗号またはアルゴリズムは、有効な暗号またはアルゴリズムです。システムは、**暗号拡張**文字列または**アルゴリズム拡張文字列**フィールドからの暗号またはアルゴリズムを選択します。

次のタスク

構成を保存すると、次のことを実行します。

- [**すべての TLS (All TLS)**] フィールドでの暗号化を設定した場合は、クラスタ内のすべてのノードをリブートして、暗号文字列を有効にします。
- [**HTTPS TLS (HTTPS TLS)**] フィールドでのみの暗号化を設定した場合は、すべてのノード上の Cisco Tomcat サービスを再起動して、暗号文字列を有効にします。

- **SIP TLS**フィールドでのみの暗号化を設定した場合は、すべてのノードでCisco CallManagerサービスを再起動して、暗号文字列を有効にします。
- **SSHの暗号**フィールドに暗号を設定した場合は、クラスタ内のすべてのノードをリブートして、暗号文字列を有効にします。
- **SSH キー交換**または**SSH MAC**フィールドで暗号を設定した場合は、クラスタ内のすべてのノードをリブートして、アルゴリズム文字列を有効にします。

関連トピック

推奨される暗号 （44 ページ）
暗号の制限 （48 ページ）
暗号の制限 （57 ページ）

暗号の制限

[Cipher **Management** configuration] ページでは任意の数の暗号を設定できますが、各アプリケーションには、そのインターフェイスでサポートされている暗号のリストがあります。たとえば、すべて**の TLS**インターフェイスで ECDHE または DHE または ECDSA ベースの暗号が表示される場合がありますが、Cisco Call Manager などのアプリケーションでは、このような暗号をサポートしていない場合があります。EC カーブまたは dhe アルゴリズムはこのアプリケーションのインターフェイスに対して有効になっていません。個々のアプリケーションアプリケーションの暗号のサポート （49 ページ）インターフェイスでサポートされている暗号のリストについては、以下のセクションを参照してください。

GUI での検証

暗号管理ページの暗号は、OpenSSL のガイドラインに従って検証されます。たとえば、次のように設定されている暗号があるとします。失敗しました。!MD5、暗号文字列は "不良" は暗号化されていないことを認識していても、有効であると見なされます。OpenSSL は、これを有効な文字列と見なします。AES128_SHA が AES128-SHA ではなく、ハイフンではなくアンダースコアを使用して設定されている場合、OpenSSL はこれを無効な暗号 (suite) として識別します。

認証モード (NULL 暗号)

アプリケーションインターフェイスがNULLの暗号を使用している場合は、**暗号管理**ページの**ALL TLS**または**SIP TLS** フィールドに暗号リストを設定することによって、NULL 暗号のサポートを無効にすることができます。

NULL 暗号を使用するアプリケーションインターフェイスの例は次のとおりです。

- **すべての TLS インターフェイス**: tls コンテキストの設定**ページ経由の**IM およびプレゼンスの SIP プロキシ。
- **SIP TLSインターフェイス:** sip または sccp で、いずれ**かのデバイス セキュリティ プロファイル**が認証済みモードに設定されている場合に、sip または sccp が経由します。

NULL 暗号を使用する必要がある場合は、これら 2 つのインターフェイスのいずれについても暗号を設定しないでください。

オーバーライド機能

[**Cipher Management**] ページの設定により、各アプリケーションと、暗号が設定されているその他の場所のデフォルト設定が上書きされます。つまり、[**Cipher Management**] ページで暗号が設定されていない場合は、すべてのインターフェイスの元の機能が保持されます。

たとえば、**エンタープライズパラメータ**「**TLS の暗号**」が、サポートされ「ているすべて」の暗号**を使用**して設定され「ていて、*cipher Management* ページが暗号によって構成されている場合、*AES256-GCM-SHA384: AES256-SHA256*」すべて**の TLS**インターフェイスで、すべてのアプリケーション SIP インターフェイスは「*AES256-gcm-SHA384: AES256-sha256*」暗号のみをサポートし、**エンタプライズは無視されますパラメータ**値。

アプリケーションの暗号のサポート

次の表は、アプリケーションインターフェイスと、TLS および SSH インターフェイスでサポートされているすべての対応する暗号およびアルゴリズムを示しています。

表 *7: TLS* 暗号のためのユニファイドコミュニケーションマネージャーの暗号サポート

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco CallManager	TCP/TLS	2443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: AES256-GCM-SHA384: AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: CAMELLIA128-SHA
DRS	TCP/TLS	4040	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco Tomcat	TCP/TLS	8443 / 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA
Cisco CallManager	TCP/TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-ECDSA-DES-CBC3-SHA
Cisco CTL Provider	TCP/TLS	2444	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:
Cisco Certificate Authority Proxy Function	TCP/TLS	3804	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
CTIManager	TCP/TLS	2749	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA
シスコ信頼検証サービス	TCP/TLS	2445	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA
Cisco Intercluster Lookup Service	TCP/TLS	7501	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:
安全な設定ダウンロード (HAPROXY)	TCP/TLS	6971、6972	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
認証済み UDS 連絡先の検索	TCP/TLS	9443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA:

表 *8 : Cisco* ユニファイドコミュニケーションマネージャー *IM &* プレゼンス暗号サポートが *TLS* の暗号でサポートされています

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco SIP Proxy	TCP/TLS	8083	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco SIP Proxy	TCP/TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA
Cisco XCP XMPP Federation Connection Manager	TCP/TLS	5269	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco SIP Proxy	TCP/TLS	5062	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA
Cisco XCP Client Connection Manager	TCP/TLS	5222	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco Tomcat	TCP/TLS	8443、443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA

表 *9 : SSH* 暗号の暗号サポート

サービス	暗号/アルゴリズム
SSH サーバ	• 暗号: aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC アルゴリズム： hmac-sha2-256 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1

サービス	暗号/アルゴリズム
SSH クライアント	• 暗号： aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC アルゴリズム： hmac-sha2-256 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1
DRS クライアント	• 暗号： aes128-ctr aes192-ctr aes256-ctr • MAC アルゴリズム： hmac-sha2-256 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1

サービス	暗号/アルゴリズム
SFTP クライアント	• 暗号： aes128-ctr aes192-ctr aes256-ctr • MAC アルゴリズム： hmac-sha2-256 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1

暗号の制限

[**Cipher Management**] ページでは、OpenSSL または OpenSSH でサポートされている暗号の設定を行うことができますが、重要なデータが偶発的に公開されることを回避するために、一部の暗号は Cisco のセキュリティ標準に基づいて内部的に無効化されています。

[**Cipher Management**] ページで暗号を設定すると、次の暗号が基本的に無効になります。

TLS を無効にした暗号

```
EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:ADH-DES-CBC-SHA:
DES-CBC-SHA:KRB5-DES-CBC-SHA:KRB5-DES-CBC-MD5:EXP-EDH-RSA-DES-CBC-SHA:
EXP-EDH-DSS-DES-CBC-SHA:EXP-ADH-DES-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:
EXP-KRB5-RC2-CBC-SHA:EXP-KRB5-DES-CBC-SHA:EXP-KRB5-RC2-CBC-MD5:EXP-KRB5-DES-CBC-MD5:
EXP-ADH-RC4-MD5:EXP-RC4-MD5:EXP-KRB5-RC4-SHA:EXP-KRB5-RC4-MD5:ADH-AES256-GCM-SHA384:
ADH-AES256-SHA256:ADH-AES256-SHA:ADH-CAMELLIA256-SHA:ADH-AES128-GCM-SHA256:ADH-AES128-SHA256:
ADH-AES128-SHA:ADH-SEED-SHA:ADH-CAMELLIA128-SHA:ADH-DES-CBC3-SHA:ADH-RC4-MD5:
AECDH-AES256-SHA:AECDH-AES128-SHA:AECDH-DES-CBC3-SHA:AECDH-RC4-SHA:AECDH-NULL-SHA:
DES-CBC3-MD5:IDEA-CBC-MD5:RC2-CBC-MD5:RC4-MD5:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:
ECDH-RSA-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:KRB5-RC4-SHA:
KRB5-RC4-MD5:IDEA-CBC-SHA:KRB5-IDEA-CBC-SHA:KRB5-IDEA-CBC-MD5:DHE-RSA-SEED-SHA:
DHE-DSS-SEED-SHA:SEED-SHA:KRB5-DES-CBC3-MD5:NULL-MD5:PSK-AES256-CBC-SHA:
PSK-AES128-CBC-SHA:PSK-3DES-EDE-CBC-SHA:ECDHE-RSA-NULL-SHA:ECDHE-ECDSA-NULL-SHA:
ECDH-RSA-NULL-SHA:ECDH-ECDSA-NULL-SHA:NULL-SHA256:NULL-SHA
```

SSH 無効暗号

```
3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

SSH が無効になっている KEX アルゴリズム

```
curve25519-sha256@libssh.org,gss-gex-sha1-,gss-group1-sha1-,gss-group14-sha1-
```

SSH が無効になっている MAC アルゴリズム

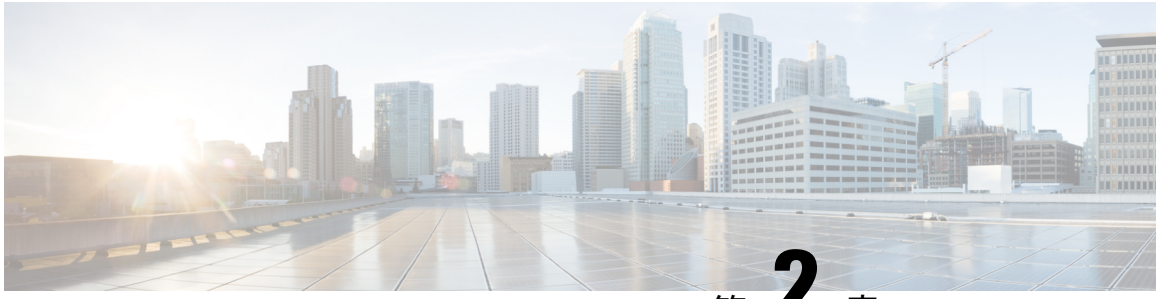
```
hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

詳細情報の入手先

関連するシスコのドキュメント

関連する Cisco IP Telephony アプリケーションと製品の詳細については、次のドキュメントを参照してください。

- 『*System Configuration Guide for Cisco Unified Communications Manager*』
- 『*Administration Guide for Cisco Unified Communications Manager*』
- 『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』
- 『*Cisco Unified Communications Manager Integration Guide for Cisco Unity*』
- 『*Cisco Unified Communications Manager Integration Guide for Cisco Unity Connection*』
- 『SRST 対応ゲートウェイに対応した *Cisco Unified Survivable Remote Site Telephony (SRST) Administration Guide*
- 『*Administration Guide for Cisco Unified Communications Manager*』
- 『*Cisco Unified Communications Manager Bulk Administration Guide*』
- 『*Cisco Unified Communications Manager*のトラブルシューティングガイド』
- 電話機モデルをサポートする *Cisco IP Phone* の管理ガイド



第 2 章

Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS）

この章では、Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS）について説明します。

HTTPS

HTTPS（Hypertext Transfer Protocol over Secure Sockets Layer（SSL））は、Microsoft Windows ユーザ向けにブラウザと Web サーバの間の通信を保護します。HTTPS は証明書を使用して、サーバのアイデンティティを保証し、ブラウザ接続を保護します。HTTPS では、インターネット経由での転送で公開キーを使用してユーザ ログインやパスワードなどのデータを暗号化します。

Unified Communications Manager は、HTTPS 接続の SSL および Transport Layer Security（TLS）をサポートしています。ご使用の Web ブラウザ バージョンが TLS をサポートしている場合、セキュリティ強化のために TLS を使用することを推奨します。セキュアな HTTPS 通信のために TLS を使用するには、Web ブラウザで SSL を無効にします。

HTTPS を有効にするには、接続プロセス中にサーバ識別用の証明書をダウンロードする必要があります。現在のセッションだけにサーバ証明書を使用するか、サーバでの現在のセッションと将来のセッションを保護するために信頼フォルダ（ファイル）に証明書をダウンロードすることができます。信頼フォルダには、すべての信頼済みサイトの証明書が保存されます。

Unified Communications Manager での Cisco Tomcat Web サーバ アプリケーションとの接続について、シスコでは次のブラウザをサポートしています。

- Microsoft Windows XP SP3 上で動作している場合は、Microsoft Internet Explorer（IE）7

- Microsoft Windows XP SP3 または Microsoft Vista SP2 上で動作している場合は、Microsoft Internet Explorer（IE）8
- Microsoft Windows XP SP3、Microsoft Vista SP2 または Apple MAC OS X 上で動作している場合は、Firefox 3.x
- Apple MAC OS X 上で動作している場合は、Safari 4.x

（注） Unified Communications Manager をインストールまたはアップグレードすると、HTTPS 自己署名証明書（Tomcat）が生成されます。この自己署名証明書は、Unified Communications Manager へのアップグレード時に自動的に移行されます。この証明書のコピーは .DER および .PEM 形式で作成されます。

自己署名証明書は、Cisco Unified Communications Operating System GUI を使用して再生成できます。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Unified Communications Manager で Cisco Tomcat との間で HTTPS を使用するアプリケーションを次の表に示します。

表 *10 : Unified Communications Manager HTTPS* アプリケーション

Unified Communications Manager HTTPS アプリケーション	**Web アプリケーション**
ccmadmin	Unified Communications Manager Administration
ccmservice	Cisco Unified Serviceability
cmplatform	オペレーティング システムの管理ページ
cmuser	Cisco Personal Assistant
ast	Real Time Monitoring Tool
RTMTReports	Real Time Monitoring Tool レポート アーカイブ
PktCap	パケット キャプチャに使用される TAC トラブルシューティング ツール
art	Unified Communications Manager CDR Analysis and Reporting
taps	Unified Communications Manager Auto-Register Phone Tool
dna	Dialed Number Analyzer
drf	Disaster Recovery System

Unified Communications Manager HTTPS アプリケーション	Web アプリケーション
SOAP	Unified Communications Manager データベースの読み取り/書き込み用の Simple Object Access Protocol API （注） セキュリティのため、SOAP を使用するすべての Web アプリケーションで HTTPS が必要です。SOAP アプリケーションの場合 HTTP はサポートされていません。HTTP を使用する既存のアプリケーションは実行に失敗します。ディレクトリ変更によって HTTPS に変換することはできません。

Cisco Unified IP Phone サービスの HTTPS

Unified Communications Manager、Cisco IP Phone、および Cisco Unified IP Phone の各サービスでは、HTTPS、暗号化、およびポート 8443 を使用したサーバのセキュアな識別がサポートされています。

TVS（信頼検証サービス）では証明書チェーンは確認されません。TVS が証明書を確認するためには、電話によって TVS に提示されるのと同じ証明書が Tomcat 信頼証明書ストア内に存在する必要があります。

TVS では、ルート証明書や中間証明書は確認されません。アイデンティティ証明書のみ、データベースに存在しない場合に確認されます。ルート証明書および中間証明書が提示された場合でも、検証は失敗します。

HTTPS をサポートする Cisco Unified IP Phone

次の Cisco IP Phone では、HTTPS がサポートされています。

- 6901、6911、6921、6941、6945、6961
- 7811、7821、7832、7841、7861
- 7906、7911、7925、7925-EX、7926、7931、7941、7941G-GE、7942、7945、7961、7962、7961G-GE、7965、7975
- 8811、8821、8831、8832、8841、8845、8851、8851NR、8861、8865、8865NR
- 8941、8945、8961
- 9951、9971

（注） このリストの 69xx 電話は、HTTPS クライアントとして動作可能ですが、HTTPS サーバとしての動作はできません。このリスト内の残りの電話は、HTTPS クライアントまたは HTTPS サーバとして動作可能です。

HTTPS をサポートする機能

次の機能で HTTPS がサポートされています。

- Cisco Extension Mobility（EM）
- Cisco Extension Mobility Cross Cluster（EMCC）
- Cisco Unified Communications Manager Manager Assistant（IPMA）
- Cisco Unified IP Phone サービス
- パーソナル ディレクトリ
- クレデンシャルの変更

Cisco Unified IP Phone サービスの設定

Unified Communications Manager リリース 8.0(1) 以降では、HTTPS をサポートするため、次の表に示すセキュア URL パラメータが電話の設定に含まれるようになりました。

セキュア URL の各パラメータを設定するには、[Unified Communications Manager Administration] から **[Device]** > **[Device Settings]** > **[Phone Services]** を選択します。詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

（注） [Cisco Unified Communications Manager Administration] の [Enterprise Parameters] セクションで Secured Phone URL パラメータを削除してリブートすると、デフォルトで URL パラメータが再度読み込まれます。リブートの後、[Secured Phone URL Parameters] セクションに移動し、正しい URL に変更して電話を再起動します。

表 *11* : セキュア *URL* の電話の設定

フィールド	説明
[Secure Service URL]	電話 Web サーバに対する要求を検証するために電話で使用されるセキュア URL を入力します。 （注） セキュア認証 URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルトでは、この URL はインストール中に設定された [Cisco Unified Communications Self Care Portal] ウィンドウにアクセスします。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255
[Secure Directory URL]	電話のディレクトリ情報の取得元となるサーバの URL を入力します。このパラメータには、ユーザが [Directory] ボタンを押したときにセキュアな Cisco IP Phone が使用する URL を指定します。 （注） セキュア ディレクトリ URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255

フィールド	説明
[Secure Idle URL]	電話が [Idle Timer] フィールドで指定された時間アイドルだったときに Cisco IP Phone に表示される情報のセキュア URL を入力します。たとえば、電話が 5 分間使用されなかったときに、LCD にロゴを表示できます。 （注） セキュア アイドル URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255
[Secure Information URL]	Cisco IP Phone がヘルプ テキストの情報を取得するサーバの場所を示す URL を入力します。この情報は、ユーザが電話の情報ボタン（i）またはヘルプ ボタン（?）ボタンを押したときに表示されます。 （注） セキュア情報 URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255

フィールド	説明
[Secure Messages URL]	メッセージ サーバのセキュア URL を入力します。ユーザが [Messages] ボタンを押すと、Cisco IP Phone はこの URL にアクセスします。 （注） セキュア メッセージ URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255
[Secure Services URL]	Cisco Unified IP Phone サービスのセキュア URL を入力します。これは、ユーザが [Services] ボタンを押したときにセキュア Cisco Unified IP Phone がアクセスする場所になります。 （注） セキュア サービス URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255

HTTPS をサポートするためのエンタープライズ パラメータの設定

HTTPS をサポートするため、Unified Communications Manager リリース 8.0(1) 以降では次の新しいエンタープライズ パラメータがサポートされています。

- [Secured Authentication URL]
- [Secured Directory URL]
- [Secured Idle URL]
- [Secured Information URL]
- [Secured Messaged URL]
- [Secured Services URL]

Internet Explorer 8 を使用して証明書を信頼できるフォルダに保存

ブラウザを再起動するたびに証明書をリロードしなくても安全なアクセスが行えるよう、Unified Communications Manager の証明書を Internet Explorer 8 にインポートしてください。Web サイトで証明書に対する警告が表示され、証明書が信頼ストアにない場合、Internet Explorer 8 は現在のセッションの間だけ証明書を記憶します。

サーバ証明書をダウンロードした後も、Internet Explorer 8 ではその Web サイトに対する証明書エラーが引き続き表示されます。このセキュリティの警告は、ブラウザの信頼ルート認証局の信頼できるストアにインポートされた証明書が含まれている場合には無視できます。

次の手順では、Internet Explorer 8 のルート証明書の信頼ストアに Unified Communications Manager の証明書をインポートする方法について説明します。

手順

ステップ 1 Tomcat サーバのアプリケーションを参照します（たとえば、Unified Communications Manager Administration のホスト名、localhost または IP アドレスをブラウザに入力します）。

ブラウザに「Certificate Error: Navigation Blocked」というメッセージが表示されます。これはこの Web サイトは信頼できないことを示しています。

ステップ 2 サーバにアクセスするには、[Continue to this website (not recommended)] をクリックします。

[Unified Communications Manager Administration] ウィンドウが表示され、ブラウザにアドレスバーと証明書のエラーのステータスが赤色で表示されます。

ステップ 3 サーバ証明書をインポートするには、[Certificate Error] ステータス ボックスをクリックして、ステータス レポートを表示します。レポートの [View Certificates] リンクをクリックします。

ステップ 4 証明書の詳細を確認します。

ステップ 5 [Certificate] ウィンドウで [General] タブを選択し、[Install Certificate] をクリックします。

証明書のインポート ウィザードが起動します。

ステップ 6 ウィザードを起動するには、[Next] をクリックします。

[Certificate Store] ウィンドウが表示されます。

ステップ 7 [Automatic] オプションが選択されていることを確認します。これを選択すると、ウィザードでこの証明書タイプの証明書ストアを選択できるようになります。[Next] をクリックします。

ステップ 8 設定を確認し、[Finish] をクリックします。

インポート操作に対してセキュリティ警告が表示されます。

ステップ 9 証明書をインストールするには、[Yes] をクリックします。

インポート ウィザードに「「The import was successful.」」と表示されます。

ステップ 10 [OK] をクリックします。**[View Certificates]** リンクを次にクリックしたときには、[Certificate Path] ウィンドウの **[Certification Path]** タブに「「This certificate is OK.」」と表示されます。

ステップ 11 信頼ストアにインポートした証明書が含まれていることを確認するには、Internet Explorer のツールバーの **[Tools]** > **[Internet Options]** をクリックして、**[Content]** タブを選択します。[Certificates] をクリックして、[Trusted Root Certifications Authorities] タブを選択します。インポートした証明書が見付かるまでリストをスクロールします。

証明書のインポート後、ブラウザには引き続きアドレスバーと証明書エラーのステータスが赤色で表示されます。このステータスは、ホスト名、localhost または IP アドレスを入力したり、ブラウザを更新または再起動した場合でも表示されます。

Internet Explorer 8 証明書のファイルへのコピー

証明書をファイルにコピーし、ローカルに保存しておけば、必要な時にいつでも証明書を復元できます。

次の手順を実行することで、標準の証明書保管形式で証明書をコピーできます。証明書の内容をファイルにコピーするには、次の手順を実行します。

手順

ステップ 1 [Certificate Error] ステータス ボックスをクリックします。

ステップ 2 [View Certificate] をクリックします。

ステップ 3 [Details] タブをクリックします。

ステップ 4 [Copy to File] ボタンをクリックします。

ステップ 5 [Certificate Export Wizard] が表示されます。[Next] をクリックします。

ステップ 6 次のリストに、選択可能なファイル形式を定義しています。エクスポートするファイルに使用するファイル形式を選択し、[Next] をクリックします。

a) [DER encoded binary X.509 (.CER)]：エンティティ間の情報転送で DER を使用します。
b) [Base-64 encoded X.509 (.CER)]：バイナリ添付ファイルをインターネット上でセキュアに送信できます。ファイルの文字化けを防ぐため、ASCII テキスト形式を使用します。
c) [Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)]：証明書自体と、選択した PC の認証パスにあるすべての証明書をエクスポートします。

ステップ 7 ファイルのコピーをエクスポートし、ファイル名を設定する場所を参照します。**[Save]** をクリックします。

ステップ 8 ファイル名とパスは [Certificate Export Wizard] ペインに表示されます。[Next] をクリックします。

ステップ 9 ファイルと設定が表示されます。[Finish] をクリックします。

ステップ 10 エクスポートの成功を示すダイアログボックスが表示されたら、[OK] をクリックします。

HTTPS による Firefox での初回の認証

Unified Communications Manager のインストールまたはアップグレード後に、[Unified Communications Manager Administration] またはその他の Unified Communications Manager SSL 対応仮想ディレクトリにユーザがブラウザクライアントから初めてアクセスすると、サーバを信頼するかどうかを尋ねる [Security Alert] 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が表示された場合、次のいずれかの作業を行う必要があります。

- **[I Understand The Risks]** をクリックすると、現在の Web セッションの間だけ証明書を信頼することになります。現在のセッションの間だけ証明書を信頼する場合は、アプリケーションにアクセスするたびに [Security Alert] ダイアログボックスが表示されます。つまり、信頼できるフォルダに証明書をインストールするまでこのダイアログボックスが表示されることになります。
- **[Get Me Out Of Here]** をクリックすると、操作がキャンセルされます。認証が行われないため、Web アプリケーションにアクセスできません。Web アプリケーションにアクセスするには、**[I Understand The Risks]** をクリックする必要があります。

Firefox 3.x を使用して証明書を信頼できるフォルダに保存

ブラウザ クライアントで HTTPS 証明書を信頼できるフォルダに保存するには、次の手順を実行します。

手順

ステップ 1 Tomcat サーバにアクセスします（たとえば、ブラウザに [Cisco Unified Communications Manager Administration] のホスト名、ローカルホスト、または IP アドレスを入力します）。

ステップ 2 [Security Alert] ダイアログボックスが表示されたら、[I Understand The Risks] をクリックします。

ステップ 3 [Add Exception] をクリックします。

[Add Exception] ダイアログボックスが表示されます。

ステップ 4 [Get Certificate] をクリックします。

ステップ 5 [Permanently store this exception] チェックボックスをオンにします。

ステップ 6 [Confirm Security Exception] をクリックします。

ステップ 7 次の手順を実行して証明書の詳細を表示します。

a) Firefox ブラウザで **[Tools]** > **[Options]** をクリックします。

[Options] ダイアログボックスが表示されます。

b) [Advanced] をクリックします。
c) [View Certificate] をクリックします。

[Certificate Manager] ダイアログボックスが表示されます。

d) 表示する証明書を強調表示して [View] をクリックします。

[Certificate Viewer] ダイアログボックスが表示されます。

e) [Details] タブをクリックします。
f) [Certificate Fields] フィールドで、表示するフィールドを強調表示します。

詳細は [Field Values] フィールドに表示されます。

g) [Certificate Viewer] ダイアログボックスで [Close] をクリックします。
h) [Certificate Viewer] ダイアログボックスで [OK] をクリックします。

Firefox 3.x 証明書のファイルへのコピー

証明書をファイルにコピーし、ローカルに保存しておけば、必要な時にいつでも証明書を復元できます。

次の手順を実行することで、標準の証明書保管形式で証明書をコピーできます。証明書の内容をファイルにコピーするには、次の手順を実行します。

手順

ステップ 1 Firefox ブラウザで **[Tools]** > **[Options]** をクリックします。

[Options] ダイアログボックスが表示されます。

ステップ 2 選択されていなければ、[Advanced] をクリックします。

ステップ 3 [Security] タブをクリックし、[View Certificates] をクリックします。

[Certificate Manager] ダイアログボックスが表示されます。

ステップ 4 [Servers] タブをクリックします。

ステップ 5 コピーする証明書を強調表示して [Export] をクリックします。

[Save Certificate to File] ダイアログボックスが表示されます。

ステップ 6 ファイルをコピーする場所に移動します。

ステップ 7 [Save as type] ドロップダウン リストで、ファイル タイプを次のオプションから選択します。

a) [X.509 Certificate (PEM)]：エンティティ間の情報転送で **PEM** を使用します。
b) [X.509 Certificate with chain (PEM)]：証明書チェーンを検証し、エンティティ間で情報を転送するために、プライバシー強化メール（Privacy Enhanced Mail）を使用します。

- [X.509 Certificate (DER)]：エンティティ間の情報転送で **DER** を使用します。

- [X.509 Certificate (PKCS#7)]：PKCS#7 は署名、データ暗号化のための標準規格です。署名されたデータを確認するには証明書が必要であるため、これを SignedData 構造に含めることができます。A .P7C ファイルは、署名するデータを持たない、退化した SignedData 構造です。
- [X.509 Certificate with chain (PKCS#7)]：証明書チェーンを検証し、エンティティ間で情報を転送するために、PKCS#7 を使用します。

ステップ 8 **[保存（Save）]** をクリックします。

ステップ 9 [OK] をクリックします。

HTTPS による Safari での初回の認証

Unified Communications Manager のインストールまたはアップグレード後に、[Unified Communications Manager Administration] またはその他の Unified Communications Manager SSL 対応仮想ディレクトリにユーザがブラウザクライアントから初めてアクセスすると、サーバを信頼するかどうかを尋ねる [Security Alert] 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が表示された場合、次のいずれかの作業を行う必要があります。

- [Yes] をクリックすると、現在の Web セッションの間だけ証明書を信頼することになります。現在のセッションの間だけ証明書を信頼する場合は、アプリケーションにアクセスするたびに [Security Alert] ダイアログボックスが表示されます。つまり、信頼できるフォルダに証明書をインストールするまでこのダイアログボックスが表示されることになります。
- **[Show Certificate]** > **[Install Certificate]** をクリックして、証明書のインストール作業を実行し、証明書を常に信頼することを示します。証明書を信頼できるフォルダにインストールすると、Web アプリケーションにアクセスするごとに [Security Alert] ダイアログボックスが表示されなくなります。
- [No] をクリックすると、操作がキャンセルされます。認証が行われないため、Web アプリケーションにアクセスできません。Web アプリケーションにアクセスするには、[Yes] をクリックするか、または **[Show Certificate]** > **[Install Certificate]** オプションを選択して証明書をインストールする必要があります。

（注） Unified Communications Manager へのアクセスに使用するアドレスは、証明書にある名前と一致する必要があります。一致しない場合は、デフォルトでメッセージが表示されます。信頼できるフォルダに証明書をインストールした後、ローカル ホストまたは IP アドレスを使用してその Web アプリケーションにアクセスすると、セキュリティ証明書の名前とアクセスするサイトの名前が一致しないことを示すセキュリティの警告が表示されます。

Safari 4.x を使用して証明書を信頼できるフォルダに保存

ブラウザ クライアントで HTTPS 証明書を信頼できるフォルダに保存するには、次の手順を実行します。

手順

ステップ 1 Tomcat サーバにアクセスします（たとえば、ブラウザに [Cisco Unified Communications Manager Administration] のホスト名、ローカルホスト、または IP アドレスを入力します）。

ステップ 2 [Security Alert] ダイアログボックスが表示されたら、[Show Certificate] をクリックします。

証明書のデータを確認する場合は、[Details] タブをクリックして、証明書の詳細を表示できます。設定のサブセットを表示するには（使用可能な場合）、次のオプションのいずれか 1 つを選択します。

a) [All]：すべてのオプションが [Details] ペインに表示されます。
b) [Version 1 Fields Only]：[Version]、[Serial Number]、[Signature Algorithm]、[Issuer]、[Valid From]、[Valid To]、[Subject]、および [Public Key] の各オプションが表示されます。
c) [Extensions Only]：[Subject Key Identifier]、[Key Usage]、および [Enhanced Key Usage] の各オプションが表示されます。
d) [Critical Extensions Only]：存在する場合は [Critical Extensions] が表示されます。
e) [Properties Only]：[Thumbprint algorithm] と [Thumbprint] オプションが表示されます。

ステップ 3 [Certificate] ペインの [Install Certificate] をクリックします。

ステップ 4 [Certificate Import Wizard] が表示されたら、[Next] をクリックします。

ステップ 5 [Place all certificates in the following store] オプション ボタンをクリックし、[Browse] をクリックします。

ステップ 6 [Trusted Root Certification Authorities] を参照し、選択して、[OK] をクリックします。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [完了（Finish）] をクリックします。

[Security Warning] ボックスに証明書の拇印が表示されます。

ステップ 9 証明書をインストールするには、[Yes] をクリックします。

インポートが正常に実行されたことを示す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 10 ダイアログボックスの右下隅にある [OK] をクリックします。

ステップ 11 証明書を信頼して、ダイアログボックスが今後表示されないようにするには、[Yes] をクリックします。

ヒント [Certificate] ペインの [Certification Path] タブをクリックして、証明書が正常にインストールされたことを確認できます。

ファイルへの Safari 4.x 証明書のコピー

証明書をファイルにコピーし、ローカルに保存しておけば、必要な時にいつでも証明書を復元できます。

次の手順を実行することで、標準の証明書保管形式で証明書をコピーできます。証明書の内容をファイルにコピーするには、次の手順を実行します。

手順

ステップ 1 [Security Alert] ダイアログボックスで、[Show Certificate] をクリックします。

ヒント Safari で、[Certificate Error] ステータス ボックスをクリックして、[Show Certificate] オプションを表示します。

ステップ 2 [Details] タブをクリックします。

ステップ 3 [Copy to File] ボタンをクリックします。

ステップ 4 [Certificate Export Wizard] が表示されます。[Next] をクリックします。

ステップ 5 次のリストに、選択可能なファイル形式を定義しています。エクスポートするファイルに使用するファイル形式を選択し、[Next] をクリックします。

a) [DER encoded binary X.509 (.CER)]：エンティティ間の情報転送で DER を使用します。

b) [Base-64 encoded X.509 (.CER)]：バイナリ添付ファイルをインターネット上でセキュアに送信できます。ファイルの文字化けを防ぐため、ASCII テキスト形式を使用します。

c) [Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)]：証明書自体と、選択した PC の認証パスにあるすべての証明書をエクスポートします。

ステップ 6 ファイルのコピーをエクスポートし、ファイル名を設定する場所を参照します。**[Save]** をクリックします。

ステップ 7 ファイル名とパスは [Certificate Export Wizard] ペインに表示されます。[Next] をクリックします。

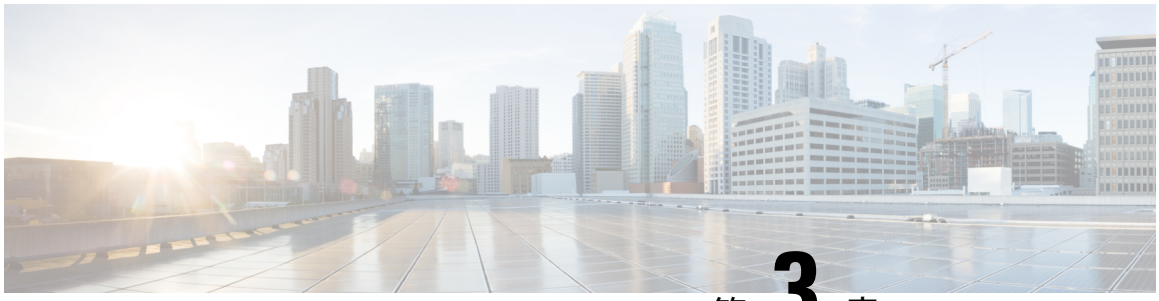
ステップ 8 ファイルと設定が表示されます。[Finish] をクリックします。

ステップ 9 エクスポートの成功を示すダイアログボックスが表示されたら、[OK] をクリックします。

HTTPS 設定に関する詳細情報の入手先

関連するシスコのドキュメント

- 『*Cisco Unified Serviceability Administration Guide*』
- 『*Administration Guide for Cisco Unified Communications Manager*』
- HTTPS に関して利用可能な Microsoft のドキュメント



第 3 章

デフォルトのセキュリティ設定

このセクションでは、デフォルトのセキュリティ設定について説明します。

デフォルトのセキュリティ機能

デフォルトのセキュリティとして、Cisco Unified IP Phone には次の自動化されたセキュリティ機能が用意されています。

- 電話設定ファイルの署名
- 電話設定ファイル暗号化のサポート
- Tomcat および他の Web サービスでの https の利用（MIDlet）

Unified Communications Manager リリース 8.0 以降では、CTL クライアントが実行されているかどうかにかかわらず、これらのセキュリティ機能がデフォルトで提供されています。

信頼検証サービス

信頼検証サービス（TVS）はSBDの主要コンポーネントです。TVSを使用するとCisco Unified IP PhoneはHTTPS確立時にEMサービス、ディレクトリ、MIDletなどのアプリケーションサーバを認証できます。

TVS には次の機能があります。

- 拡張性：Cisco IP Phone リソースは信頼する証明書の数の影響を受けません。
- 柔軟性：信頼証明書の追加や削除はシステムに自動的に反映されます。
- デフォルトのセキュリティ：非メディアおよびシグナリングセキュリティ機能はデフォルトのインストールに含まれており、ユーザの介入は必要ではありません。

（注） セキュアなシグナリングおよびメディアを有効にする場合は、CTLファイルを作成し、クラスタを混合モードに設定する必要があります。**utils ctl set-cluster mixed-mode** CLI コマンドを使用して、CTL ファイルの作成とセキュリティ モードの変更を一度に行うことができます。

TVS の説明

次の基本概念は信頼検証サービスを説明します。

- TVS は Unified Communications Manager サーバ上で動作し、Cisco IP Phone の代わりに証明書を認証します。
- 信頼できる証明書をすべてダウンロードするのではなく、Cisco IP Phone では TVS を信頼するだけで済みます。
- TVS 証明書およびいくつかのキー証明書が、初期信頼リストファイル（ITL）と呼ばれる新しいファイルにまとめられます。
- ITL ファイルはユーザの介入なしで自動的に生成されます。
- ITL ファイルは Cisco IP Phone によってダウンロードされ、そこから信頼情報がフローします。

初期信頼リスト

ITL ファイル

最初の信頼リスト (ITL) ファイルは、CTL ファイルと同じ形式になっています。ただし CTL ファイルよりも小さく、スリム化されたバージョンです。ITL ファイルには次の属性が適用されます。

- クラスタをインストールすると、システムが自動的にITLファイルをビルドします。内容が変更された場合、ITL ファイルは自動的に更新されます。
- ITL ファイルは eToken を必要としません。このファイルはソフト eToken（TFTP サーバの CallManager 証明書に関連付けられている秘密キー）を使用します。
- Cisco IP Phone は、起動時間中、リセット中、または CTL ファイルのダウンロード後に ITL ファイルをダウンロードします。

ITL ファイルの内容

ITL ファイルには次の証明書が含まれています。

- TFTP サーバの CallManager 証明書。この証明書によって、ITL ファイルの署名および電話設定ファイルの署名を認証できます。
- クラスタ内で、すべての TVS 証明書が利用可能です。これらの証明書によって、電話が TVS とセキュアに通信し、証明書の認証を要求することができます。
- CAPF 証明書：これらの証明書は、設定ファイルの暗号化をサポートしています。CAPF 証明書は必ずしも ITL ファイル内に存在する必要はありません（TVS で認証可能）が、CAPF 証明書によって CAPF への接続が簡易化されます。

ITL ファイルには証明書ごとに 1 つのレコードが含まれます。各レコードの内容は次のとおりです。

- 証明書
- Cisco IP Phone による検索を容易にするための、事前に抽出された証明書フィールド。
- 証明書の権限（TFTP、CUCM、TFTP+CCM、CAPF、TV、SAST）

TFTP サーバの CallManager 証明書は、2 つの異なる権限を持つ次の 2 つの ITL レコード内に存在します。

- TFTP 権限 または TFTP および CCM 権限：設定ファイルの署名を認証する。
- SAST 権限：ITL ファイルの署名を認証する。

ITL ファイルと CTL ファイルのインタラクション

Cisco IP Phone は、クラスタ セキュリティ モード（非セキュアまたは混合モード）を確認する際に CTL ファイルを使用します。CTL ファイルは、Unified Communications Manager レコードに Unified Communications Manager 証明書を含めることで、クラスタ セキュリティ モードを追跡します。

ITL ファイルにも、クラスタ セキュリティ モードを示す情報が含まれます。

ITLRecovery 証明書の証明書管理の変更

- ITLRecovery の有効期間が 5 年間から 20 年間に延長され、より長い期間にわたって同じ ITLRecovery 証明書が使用されるようになりました。

（注） Unified Communications Manager をアップグレードした場合、ITLRecovery 証明書の有効期間は引き続き 5 年のままです。Unified Communications Manager をアップグレードすると、新しいリリースに証明書がコピーされます。ただし、ITLRecovery 証明書を再生成するか、Unified Communications Manager の新規インストールを実行すると、ITLRecovery の有効期間が 20 年に延長されます。

- ITLRecovery 証明書を再生成する前に、警告メッセージが CLI と GUI の両方で表示されます。この警告メッセージでは、トークンレス CTL を使用している場合、および CallManager 証明書を再生成している場合には、CTL ファイルに更新された CallManager 証明書があり、その証明書がエンドポイントに対して更新されていることを確認することが指示されます。

連携動作と制限事項

Unified Communications Manager クラスタに 39 を超える証明書がある場合、Cisco IP Phone 上の ITL ファイル サイズが 64 キロバイトを超えます。ITL ファイル サイズが増加すると、電話での ITL の正常なロードに影響し、Unified Communications Manager での電話登録が失敗することになります。

Cisco Unified IP Phone の ITL ファイルの更新

電話機にインストールされている ITL ファイルで [デフォルトのセキュリティ（Security By Default）] を使用する Cisco Unified CM の集中型 TFTP では、TFTP 設定ファイルを検証しません。

（注） リモートクラスタから電話機を集中型TFTP構成に追加する前に、次の手順を実行してください。

手順

ステップ 1 中央 TFTP サーバで、**Prepare Cluster for Rollback to pre-8.0** エンタープライズ パラメータを有効にします。

ステップ 2 TVS および TFTP を再起動します。

ステップ 3 すべての電話をリセットし、ITL 署名検証を無効にする新しい ITL ファイルがダウンロードされることを確認します。

ステップ 4 [Secure https URLs] エンタープライズ パラメータで、HTTPS ではなく HTTP を使用するように設定します。

（注） Unified Communications Manager のリリース 10.5 以降では、[**クラスタの 8.0 以前へのロールバック準備（Prepare Cluster for Rollback to pre-8.0）**] エンタープライズ パラメータを有効にした後、電話が自動的にリセットされます。中央TFTPサーバのUnified Communications Managerバージョンについて、またこのパラメータを有効にする方法については、『*Cisco Unified Communications Manager* セキュリティ ガイド』の「8.0 より前のリリースにクラスタをロールバックする」のセクションを参照してください。

自動登録

自動登録は、混合モードと非セキュアモードの両方でサポートされます。また、デフォルトの設定ファイルに対する署名も行われます。「デフォルトのセキュリティ」がサポートされていない Cisco IP Phone には、署名されていないデフォルトの設定ファイルが提供されます。

Cisco Unified IP Phone サポート リストの取得

手順

ステップ 1 Cisco Unified Reporting のメイン ウィンドウで、[System Reports] をクリックします。

ステップ 2 [System Reports] リストで、[Unified CM Phone Feature List] をクリックします。

ステップ 3 [**機能（Feature）**] ドロップダウンリストから該当の機能を選択します。

ステップ 4 [Submit] をクリックします。

認定されたソリューション向けコモン クライテリアの ECDSA サポート

Unified Communications Manager は、楕円曲線デジタル署名アルゴリズム（ECDSA）証明書をサポートします。これらの証明書は、RSA ベースの証明書よりも堅牢であり、コモン クライテリア（CC）認定のある製品に必要となります。米国政府の Commercial Solutions for Classified Systems（CSfC）プログラムは、CC 認定が必要なので、Unified Communications Manager にはこれが含まれています。

ECDSA 証明書は、証明書マネージャ、SIP、Certificate Authority Proxy Function（CAPF）、Transport Layer Security（TLS）、トレース、エントロピー、HTTP、CTI Manager で既存の RSA 証明書とともに使用できます。

（注） ECDSA は、Unified Communications Manager と Tomcat についてのみサポートされています。

証明書マネージャでの ECDSA サポート

Unified Communications Manager リリース 11.0 の証明書マネージャでは、自己署名 ECDSA 証明書と ECDSA 証明書署名要求（CSR）の両方の生成がサポートされています。これより前の Unified Communications Manager では、**RSA** 証明書のみがサポートされていました。しかし、Unified Communications Manager リリース 11.0 以降では、既存の **RSA** 証明書に加えて **CallManager-ECDSA** 証明書がサポートされます。

CallManager 証明書と **CallManager-ECDSA** 証明書の両方が、共通の信頼ストアである CallManager-Trust を共有します。Unified Communications Manager によって、これらの証明書がこの信頼ストアにアップロードされます。

証明書マネージャでは、キー長の値が異なる ECDSA 証明書の生成がサポートされています。

Unified Communications Manager をインストールすると、自己署名証明書が生成されます。Unified Communications Manager リリース 11.0 には常時 ECDSA 証明書が存在し、この証明書が SIP インターフェイスで使用されます。セキュアなコンピュータ テレフォニー インテグレーション（CTI）マネージャ インターフェイスでも、ECDSA 証明書がサポートされます。CTI Manager と SIP サーバの両方で同じサーバ証明書が使用されるため、両方のインターフェイスが同期して動作します。

SIP での ECDSA サポート

Unified Communications Manager リリース 11.0 には SIP 回線と SIP トランク インターフェイス向けの ECDSA サポートが含まれています。Unified Communications Manager とエンドポイント電話またはビデオ デバイスとの間の接続は SIP 回線接続であるのに対し、2 つの Unified Communications Manager 間の接続は SIP トランク接続です。すべての SIP 接続では ECDSA 暗号方式がサポートされ、ECDSA 証明書が使用されます。

以下は、SIP が TLS（Transport Layer Security）接続を設定するシナリオです。

- SIP が TLS サーバとして機能する場合：Unified Communications Manager が着信するセキュア SIP 接続の TLS サーバとして機能する場合、SIP トランク インターフェイスは CallManager-ECDSA の証明書がディスクにあるかどうかを判断します。証明書がディスクにあり、選択された暗号スイートが **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** または **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** である場合、SIP トランク インターフェイスは CallManager-ECDSA を使用します。SIP トランク インターフェイスは ECDSA 暗号化スイートをサポートしないクライアントからの接続では RSA TLS 暗号スイートを引き続きサポートします。**[TLS Ciphers]** ドロップダウンリストには、Unified Communications Manager が TLS サーバとして機能するときにサポートされている暗号スイートの設定を許可するオプションがあります。
- SIP が TLS クライアントとして機能する場合：SIP トランク インターフェイスが TLS クライアントとして機能する場合、SIP トランク インターフェイスは Cisco Unified Communications Manager の [Enterprise Parameters] ウィンドウにある [TLS Ciphers] フィールド（[ECDSA ciphers] オプションも含む）に基づいて、要求された暗号化スイートのリストをサーバに送信します。[TLS Ciphers]。この設定は優先順位の高い順に TLS クライアント暗号化スイートのリストと、サポートされている暗号スイートを決定します。

（注） ECDSA クライアント証明書をサポートしていない以前のリリースの Unified Communications Manager と TLS 接続を確立する場合、この接続では RSA 暗号スイートが使用されます。TLS 接続で送信されるクライアント証明書は、選択した TLS 暗号に関連付けられている必要はありません。以前のリリースの Unified Communications Manager でも、TLS サーバが ECDSA クライアント証明書を受信して処理することがサポートされています。

Unified Communications Manager への接続に ECDSA 暗号を使用するデバイスでは、アイデンティティ信頼リスト（ITL ファイル）に CallManager-ECDSA 証明書が必要です。次に、デバイスは CallManager-ECDSA 証明書をローカル証明書ストアに組み込み、CallManager-ECDSA 証明書でセキュリティ保護された接続を信頼する必要があります。

CAPF での ECDSA サポート

Certificate Authority Proxy Function（CAPF）は、シスコのエンドポイントと Unified Communications Manager との間で証明書を交換する、シスコ独自のメソッドです。CAPF を使用するのはシスコのエンドポイントだけです。コモン クライテリア要件を達成するため、CAPF は CAPF バージョン 3 に更新され、クライアントに ECDSA ローカルで有効な証明書（LSC）を提供できるようになりました。顧客は LSC をローカルに作成します。LSC はメーカーが作成する製造者インストール証明書（MIC）の代替です。

CAPF バージョン 3 を使うことで、Unified Communications Manager サーバから電話、CTI アプリケーション、Jabber クライアントに対し、LSC で使用される EC キーの生成を指示できます。EC キーが生成されると、Unified Communications Manager は ECDSA LSC を生成して Cisco エンドポイントに送信するか、または ECDSA CSR を生成します。

エンドポイントで CAPF バージョン 3 がサポートされていない場合、[Cisco Unified CM Administration] からバックアップとして、必要な EC キー サイズと RSA キー サイズを設定して、[Phone Configuration] ウィンドウにある [EC Preferred, RSA Backup] オプションを選択できます。CAPF サーバが EC キー ペアに要求の送信を試行し、電話が EC キーをサポートしていないサーバと通信する場合、このバックアップ オプションが役立ちます。サーバは EC キー ペアの代わりに RSA キー ペアを生成するよう要求を送信します。

（注） Cisco エンドポイントが CAPF バージョン 3 をサポートしている場合、**Endpoint Advanced Encryption アルゴリズムのサポート**のパラメータを有効にした状態で [**電話の設定（Phone Configuration**）] で [**EC 優先、RSA バックアップ（EC Preferred, RSA Backup**）] オプションを選択しても、ECDSA ベースまたは RSA ベースの LSC は発行されません。Cisco エンドポイントが CAPF バージョン 3 をサポートしていない場合、**Endpoint Advanced Encryption アルゴリズムのサポート**のパラメータを有効または無効にすると、RSA ベースの LSC が発行されます。

（注） Endpoint **Advanced Encryption アルゴリズムのサポート**パラメータは、電話機が高度な TLS 暗号を使用して TFTP 設定ファイルをダウンロードすることを示します。デフォルトでは、EC の暗号が最も優先順位が高く設定されています。このソリューションは、MRA を使用しないオンプレミスの展開でのみサポートされています。

エントロピー

強力な暗号化には、エントロピーの堅牢なソースが必要です。エントロピーはデータのランダム性の指標であり、コモンクライテリア要件の最小しきい値の決定に役立ちます。暗号化などのデータ変換方式の効率もエントロピーの優れたソースの有無に依存します。ECDSA のような強力な暗号化アルゴリズムであっても、エントロピーの弱いソースを使用すれば、暗号化が容易に破られてしまいます。

Unified Communications Manager リリース 11.0 では、Unified Communications Manager のエントロピー ソースが向上しました。エントロピー モニタリング デーモンは設定が不要な組み込み機能です。ただし、Unified Communications Manager CLI によってオフにすることができます。

エントロピー モニタリング デーモン サービスの制御には、次の CLI コマンドを使用します。

CLI コマンド	説明
utils service start Entropy Monitoring Daemon	エントロピー モニタリング デーモン サービスを開始します。
utils service stop Entropy Monitoring Daemon	エントロピー モニタリング デーモン サービスを停止します。
utils service active Entropy Monitoring Daemon	エントロピー モニタリング デーモン サービスをアクティブにします。さらにカーネル モジュールがロードされます。
utils service deactive Entropy Monitoring Daemon	エントロピー モニタリング デーモン サービスを非アクティブ化します。さらにカーネル モジュールがアンロードされます。

コンフィギュレーション ダウンロードの HTTPS サポート

セキュアなコンフィギュレーション ダウンロードのため Unified Communications Manager リリース 11.0 では、以前のリリースでの HTTP および TFTP インターフェイスに加えて、HTTPS をサポートするように機能強化されました。必要な場合には、クライアントとサーバの両方が相互認証を使用します。ECDSA LSC および暗号化された TFTP コンフィギュレーションを使用して登録されたクライアントは、LSC を提示する必要があります。

HTTPS インターフェイスでは、サーバ証明書として CallManager と CallManager-ECDSA 証明書の両方が使用されます。

（注） CallManager、CallManager ECDSA、Tomcat 証明書を更新する場合、TFTP サービスを無効化してから再び有効化する必要があります。CallManager 証明書と CallManager-ECDSA 証明書の認証にはポート 6971 が使用され、Tomcat 証明書の認証にはポート 6972 が使用されます。

CTI Manager のサポート

コンピュータ テレフォニー インテグレーション（CTI）インターフェイスが、4 つの新しい暗号方式をサポートするよう強化されました。暗号スイートは
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256、
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384、
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256、および

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 です。これらの暗号スイートのサポートによって、CTI Manager インターフェイスでは、Unified Communications Manager 内に存在する場合に、**CallManager-ECDSA** 証明書の保有が必要となりました。SIP インターフェイスと同様、CTI Manager セキュア インターフェイスでサポートされる TLS 暗号方式の設定には、Unified Communications Manager 内のエンタープライズ パラメータ [TLS Ciphers] オプションが使用されます。

証明書の再生成

Unified Communications Manager 証明書の 1 つを再生成した場合、この項で説明する手順を実行する必要があります。

注意 証明書を再生成すると、システムの動作に影響する場合があります。証明書を再生成すると、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。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

CAPF 証明書の再生成

CAPF 証明書を再生成するには、次の手順を実行します。

（注） CAPF 証明書がパブリッシャにある場合は、電話が各自の ITL ファイルを更新するために自動的に再起動することがあります。

手順

ステップ 1 CAPF 証明書を再生成します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 2 CTL ファイルがある場合は、CTL クライアントを再実行する必要があります。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 3 CAPF サービスを再起動します。

詳細については、『*Cisco Unified Communications Manager Security Guide*』の「「Activating the Certificate Authority Proxy Function Service」」の項を参照してください。

TVS 証明書の再生成

TVS 証明書の再生成では手作業は必要はありません。

（注） TVS および TFTP 両方の証明書を再生成する場合は、TVS 証明書を再生成し、電話が再起動する場合は再起動が完了するまで待ってから、TFTP 証明書を再生成します。

TFTP 証明書の再生成

TFTP 証明書を再生成するには、次の手順を実行します。

（注） 複数の証明書を再生成する場合は、TFTP 証明書の再生成を最後に行う必要があります。電話が再起動する場合は再起動が完了するまで待ってから、TFTP 証明書を再生成します。この手順に従わないと、すべての Cisco IP Phone から ITL ファイルを手動で削除する必要が生じることがあります。

手順

ステップ 1 TFTP 証明書を再生成します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 2 TFTP サービスをアクティブにしたら、すべての電話が自動的に再起動するまで待ちます。

ステップ 3 クラスタが混合モードである場合は、CTL クライアントを実行します。

第 4 章「「CTL クライアントの設定」」を参照してください。

ステップ 4 クラスタが EMCC 導入に含まれる場合、証明書の一括プロビジョニングの手順を繰り返します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ITLRecovery 証明書の再生成

警告 ITLRecovery 証明書は電話機での有効期限が長く、CallManager 証明書も含まれているため、頻繁に再生成しないでください。

非セキュア クラスタの ITLRecovery 証明書の再生成

1. ITL ファイルが有効であることと、クラスタ内のすべての電話機が現在の ITL ファイルを信頼していることを確認します。
2. ITLRecovery 証明書を再生成します。

   各クラスタ内のパブリッシャに移動して ITLRecovery 証明書を再生成します。

   1. [Unified OS の管理（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。
   2. [検索（Find）] をクリックします。

      [証明書の一覧（Certificate List）] ウィンドウが表示されます。
   3. 表示された証明書の一覧から、[ITLRecovery.pem Certificate] リンクをクリックします。
   4. [**再生成（Regenerate**）] をクリックして ITLRecovery 証明書を再生成します。
   5. ポップアップ表示された確認メッセージで、[**OK**] をクリックします。
3. [証明書の管理（Certificate Management）] で `utils itl reset localkey` を使用して ITL ファイルに署名し、新しい ITL ファイルを受け入れます。
4. クラスタ内のすべての電話機を一括でリセットします。

（注） クラスタ内のすべての電話機が登録済みであることを確認してください。

5. 新しい ITLRecovery 証明書によって ITL ファイルが再署名されるように、TFTP サービスを再起動します。

   新しい ITLRecovery 証明書は、リセット中に電話機にアップロードされます。
6. 新しい ITL ファイルを取得するために、クラスタ内のすべての電話機に対して 2 回目の一括リセットを行います。
7. リセット後、新しい ITLRecovery 証明書が電話機にアップロードされます。

セキュア クラスタの ITLRecovery 証明書の再生成

トークンベースの ITL ファイルからトークンレスの ITL ファイルに移行する場合は、セキュリティ ガイドの「移行」の項を参照してください。

1. ITL ファイルが有効であることと、クラスタ内のすべての電話機が現在の ITL ファイルを信頼していることを確認します。
2. `show ctl` コマンドを使用して CTL ファイルを確認します。
3. ITLRecovery 証明書を再生成します。

   各クラスタ内のパブリッシャに移動して ITLRecovery 証明書を再生成します。

1. [Unified OS の管理（Unified OS Administration）] から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** > **[検索（Find）]** を選択します。
2. [**検索（Find）**] をクリックして、証明書の一覧を表示します。

   [証明書の一覧（Certificate List）] ウィンドウが表示されます。
3. 表示された証明書の一覧から、[ITLRecovery.pem Certificate] リンクをクリックします。
4. [**再生成（Regenerate）**] をクリックして ITLRecovery 証明書を再生成します。
5. ポップアップ表示された確認メッセージで、[**OK**] をクリックします。

4. [証明書の管理（Certificate Management）] で `utils ctl reset localkey` を使用して CTLFile に署名します。またこの操作により、新しい ITLRecovery 証明書で CTLFile が更新されます。
5. 新しい ITLRecovery 証明書に更新された新しい CTLFile を取得するために、クラスタ内のすべての電話機を一括でリセットします。

（注） クラスタ内のすべての電話機が登録済みであることを確認してください。

6. 新しい ITLRecovery 証明書によって CTLFile に再署名するため、`utils ctl update CTLFile` を使用して CTLFile を更新します。
7. 新しい ITLRecovery 証明書によって署名された新しい CTLFile を取得するために、クラスタ内のすべての電話機に対して 2 回目の一括リセットを行います。
8. リセット後、新しい ITLRecovery 証明書が電話機にアップロードされます。

Tomcat 証明書の再生成

CAPF 証明書を再生成するには、次の手順を実行します。

手順

ステップ 1 Tomcat 証明書を再生成します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 2 Tomcat および TFTP サービスを再起動します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 3 クラスタが EMCC 導入に含まれる場合、証明書の一括プロビジョニングの手順を繰り返します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

TFTP 証明書の再生成後のシステム バックアップ手順

ITL ファイルのトラストアンカーはソフトウェア エンティティ、つまり TFTP 秘密キーです。サーバがクラッシュすると、キーは失われ、電話は新しいITLファイルを検証できなくなります。

Unified Communications Manager リリース 10.0 では、TFTP 証明書と秘密キーの両方がディザスタ リカバリ システムによってバックアップされます。システムはバックアップ パッケージを暗号化して秘密キーを保護します。サーバがクラッシュすると、以前の証明書およびキーが復元されます。

TFTP 証明書が再生成されるたびに、新しいシステムのバックアップを作成する必要があります。バックアップ手順については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco Unified Communications Manager リリース 7.x からリリース 8.6 以降への更新アップグレード

クラスタをリリース 7.x から 8.6 以降にアップグレードするには、この手順に従ってください。

手順

ステップ 1 クラスタをアップグレードするための通常の手順に従ってください。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ヒント クラスタのすべてのノードを Unified Communications Manager リリース 8.6 以降にアップグレードした後、さらにこの手順に従ってご使用の Cisco Unified IP Phone をシステムに登録する必要があります。

ステップ 2 次のリリースのいずれかを混合モードで実行している場合、CTL クライアントの実行が必要です。

- Unified Communications Manager リリース 7.1(2)
  - 7.1(2) のすべての正規リリース
  - 007.001(002.32016.001) よりも前の 712 のすべての ES リリース

- Unified Communications Manager リリース 7.1(3)
  - 007.001(003.21900.003) = 7.1(3a)su1a よりも前の 713 のすべての正規リリース
  - 007.001(003.21005.001) よりも前の 713 のすべての ES リリース

（注） CTL クライアントの実行の詳細については、第 4 章「「CTL クライアントの設定」」を参照してください。

ステップ 3 Cisco IP Phone が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

注意 クラスタを復元できるようにするため、ディザスタ リカバリ システム（DRS）を使用してクラスタのバックアップを作成する必要があります。

ステップ 4 ご使用のクラスタをバックアップします。

DRS を使用してクラスタをバックアップするには、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

次のタスク

アップグレード後にパブリッシャが起動したら、CAR の移行が完了するまで再起動しないでください。このフェーズでは、古いバージョンに切り替えたり、DRS バックアップを実行することは許可されません。**[Cisco Unified Serviceability]** > **[Tools]** > **[CDR Analysis and Reporting]** を開いて CAR 移行の状態をモニタできます。

リリース 8.0 以前のクラスタへのロールバック

クラスタを Unified Communications Manager の旧リリース（リリース 8.0 よりも前）にロールバックする場合は、その前に [Prepare Cluster for Rollback to pre-8.0] エンタープライズ パラメータを使用したロールバックの準備が必要です。

クラスタをロールバックするための準備を行うには、クラスタの各サーバで次の手順に従います。

手順

ステップ 1 [Unified Communications Manager Administration]で 、**[System]** > **[Enterprise Parameters Configuration]** を選択します。

[Enterprise Parameters Configuration] ウィンドウが表示されます。

[Prepare Cluster for Rollback to pre-8.0] エンタープライズ パラメータを [True] に設定します。

（注） クラスタを Unified Communications Manager のバージョン 8.0 以前へロールバックする準備を行う場合のみ、このパラメータを有効にします。このパラメータが有効になっている間、HTTPS を使う電話サービス（たとえば、エクステンション モビリティなど）は機能しません。ただし、このパラメータが有効になっていても、基本的な電話の発信および受信は引き続き可能です。

ステップ 2 Cisco IP Phone が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

ステップ 3 クラスタの各サーバを以前のリリースに戻します。

クラスタを以前のバージョンに戻す方法の詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 4 クラスタが以前のバージョンに切り替わるまで待ちます。

ステップ 5 次のリリースのいずれかを混合モードで実行している場合、CTL クライアントの実行が必要です。

- Unified Communications Manager リリース 7.1(2)
  - 7.1(2) のすべての正規リリース
  - 007.001(002.32016.001) よりも前の 712 のすべての ES リリース
- Unified Communications Manager リリース 7.1(3)
  - 007.001(003.21900.003) = 7.1(3a)su1a よりも前の 713 のすべての正規リリース
  - 007.001(003.21005.001) よりも前の 713 のすべての ES リリース

（注） CTL クライアントの実行方法の詳細については、「「CTL クライアントの設定」」の章を参照してください。

ステップ 6 「[Prepare Cluster for Rollback to pre-8.0]」 エンタープライズ パラメータが [True] に設定されている場合、社内ディレクトリが機能するために以下の変更が必要です。

[Device] > [Device Settings] > [Phone Services] > [Corporate Directory] で、サービス URL を「Application:Cisco/CorporateDirectory」から「http://<ipaddr>:8080/ccmcip/xmldirectoryinput.jsp」へと変更します。

ステップ 7 「[Prepare Cluster for Rollback to pre-8.0]」 エンタープライズ パラメータが [True] に設定されている場合、パーソナル ディレクトリが機能するために以下の変更が必要です。

[Device] > [Device Settings] > [Phone Services] > [Personal Directory] で、サービス URL を「Application:Cisco/PersonalDirectory」から「http://<ipaddr>>:8080/ccmpd/pdCheckLogin.do?name=undefined」へと変更します。

戻した後のリリース 8.6 以降への再切り替え

クラスタをリリース 7.x に戻した後でリリース 8.6 以降のパーティションに再度切り替える場合は、次の手順を実行します。

手順

ステップ 1 クラスタを非アクティブのパーティションに再度切り替えるための手順に従います。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 2 次のいずれかのリリースを混合モードで使用していた場合は、CTL クライアントを実行する必要があります。

Unified Communications Manager リリース 7.1(2)

- 7.1(2) のすべての正規リリース
- 007.001(002.32016.001) よりも前の 712 のすべての ES リリース
- Unified Communications Manager リリース 7.1(3)
  - 007.001(003.21900.003) = 7.1(3a)su1a よりも前の 713 のすべての正規リリース
  - 007.001(003.21005.001) よりも前の 713 のすべての ES リリース

（注） CTL クライアントの実行方法の詳細については、「「CTL クライアントの設定」」の章を参照してください。

ステップ 3 [Unified Communications Manager Administration]で 、**[System]** > **[Enterprise Parameters Configuration]** を選択します。

[Enterprise Parameters Configuration] ウィンドウが表示されます。

[Prepare Cluster for Rollback to pre-8.6] エンタープライズ パラメータを [False] に設定します。

ステップ 4 Cisco Unified IP Phone が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

Cisco Unified Communications Manager および ITL ファイルによるクラスタ間での IP Phone の移行

Unified Communications Manager 8.0(1) 以降では、新しいデフォルトのセキュリティ機能と初期信頼リスト（ITL）ファイルが導入されました。この新機能により、異なる Unified CM クラスタ間の電話の移行では、必ず正しい手順で移行できるよう注意します。

⚠

注意 正しい手順に従わないと、数千台の電話のITLファイルを手動で削除しなければならない状況が発生する可能性があります。

新しい ITL ファイルをサポートする Cisco IP Phone では、Unified CM TFTP サーバからこの特別なファイルをダウンロードする必要があります。ITL ファイルが電話にインストールされると、設定ファイルおよびITLファイルの以降の更新では、以下のいずれかによる署名が必要となります。

- 電話に現在インストールされている TFTP サーバ証明書。
- TFTP の証明書。たとえば、いずれかのクラスタの検証済み TVS サービスなど。TVS サービスの証明書は ITL ファイルに示されているクラスタの中にあります。

この新しいセキュリティ機能により、電話を別のクラスタに移動する場合に、次の 3 つの問題が発生する可能性があります。

1. 新しいクラスタの ITL ファイルが現在の ITL ファイルの署名者によって署名されていないため、電話が新しい ITL ファイルや設定ファイルを受け入れることができない問題。
2. 電話の既存のITLにリストされているTVSサーバは、電話が新しいクラスタに移動すると接続できなくなる可能性があるという問題。
3. TVS サーバが証明書の検証のためにアクセス可能でも、古いクラスタ サーバには新しいサーバ証明書がない可能性があるという問題。

この 3 つの問題のうち 1 つ以上が発生した場合、考えられる解決策の 1 つは、クラスタ間を移動中のすべての電話からITLファイルを手作業で削除することです。ただし、この解決方法は電話の数が増えるにつれて大変な労力を必要とするため、望ましい解決策ではありません。

最も推奨されるオプションは、Cisco Unified CM エンタープライズ パラメータ [Prepare Cluster for Rollback to pre-8.0] を使用することです。このパラメータを [True] に設定すると、電話は空の TVS および TFTP 証明書セクションを含む特殊な ITL ファイルをダウンロードします。

電話に空の ITL ファイルがあると、（8.x 以前の Unified CM クラスタへの移行の場合）電話は署名のない設定ファイルをすべて受け入れます。また、（異なる Unified CM 8.x クラスタへの移行の場合）新しい ITL ファイルをすべて受け入れます。

空の ITL ファイルは、電話の **[Settings]** > **[Security]** > **[Trust List]** > **[ITL]** をチェックすることで確認できます。古いTVSやTFTPサーバが指定されていた場所には、空のエントリが表示されます。

新しい空の ITL ファイルをダウンロードできるまで、電話には古い Unified CM サーバにアクセスできる必要があります。

古いクラスタをオンラインにしておく場合は、デフォルトのセキュリティを復元するため、[Prepare Cluster for Rollback to pre-8.0] エンタープライズ パラメータを無効にします。

証明書の一括エクスポート

新旧のクラスタが同時にオンラインになっている場合には証明書の一括移行による方法を使用できます。

Cisco Unified IP Phone は、ダウンロードしたすべてのファイルを、ITL ファイルまたは ITL ファイルに指定されている TVS サーバと照合することに注意してください。電話を新しいクラスタに移動する必要がある場合、新しいクラスタが提示する ITL ファイルは、古いクラスタの TVS 証明書ストアの信頼を得る必要があります。

（注） 証明書の一括エクスポートは、電話の移行中、両方のクラスタがネットワークに接続され、オンラインである場合のみ機能します。

（注） 証明書一括インポート中、Cisco Extension Mobility Cross Cluster（EMCC）が動作を継続するには、訪問クラスタとホームクラスタの両方において付加的な ITLRecovery 証明書をインポートすることが必要です。[証明書の一括管理（Bulk Certificate Management）] の [証明書タイプ（Certificate Type）] ドロップダウン リストに、ITL_Recovery 証明書をインポートするための新しいオプションが追加されています。

証明書の一括エクスポートを使用するには、以下の手順を実行します。

手順

ステップ 1 [Cisco Unified Operating System Administration] から、**[Security]** > **[Bulk Certificate Management]** を選択します。

ステップ 2 新しい宛先クラスタ（TFTP のみ）から中央の SFTP サーバに証明書をエクスポートします。

ステップ 3 証明書の一括インターフェイスを使用して、SFTP サーバの証明書（TFTP のみ）を統合します。

ステップ 4 元のクラスタで証明書の一括機能を使用し、中央 SFTP サーバから TFTP 証明書をインポートします。

ステップ 5 DHCP オプション 150 またはその他の方式を使用して、電話を新しい宛先クラスタにポイントします。

電話は新しい宛先クラスタの ITL ファイルをダウンロードし、既存の ITL ファイルと照合することを試みます。証明書は既存の ITL ファイル内に存在しないため、電話は古い TVS サーバに新しい ITL ファイルの署名の確認を要求します。この要求を行うため、電話は古い元のクラスタの TCP ポート 2445 に TVS クエリを送信します。

証明書のエクスポート、統合、インポートが正常に行われると、TVS は成功を返し、電話のメモリにある ITL ファイルは新しくダウンロードされた ITL ファイルに置き換わります。

これで、電話は新しいクラスタから署名付き設定ファイルをダウンロードおよび認証できるようになりました。

自己署名証明書の生成

手順

ステップ 1 [Cisco Unified OS Administration] から **[Security]** > **[Certificate Management]** を選択します。[証明書リスト（Certificate List）] ウィンドウが表示されます。

ステップ 2 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。

ステップ 3 新しい自己署名証明書を生成するには、[Generate Self-Signed Certificate] をクリックします。[Generate New Self-Signed Certificate] ウィンドウが表示されます。

ステップ 4 [Certificate Purpose] ドロップダウン ボックスから、[CallManager-ECDSA] などのシステム セキュリティ証明書を選択します。

ステップ 5 [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、「関連項目」の項を参照してください。

ステップ 6 [Generate] をクリックします。

関連トピック

自己署名証明書のフィールド （93 ページ）

自己署名証明書のフィールド

表 *12 :* 自己署名証明書のフィールド

フィールド	説明
[Certificate Purpose]	ドロップダウンリストから必要なオプションを選択します。 次のいずれかのオプションを選択すると、[**キー タイプ（Key Type）**] フィールドが自動的に **RSA** に設定されます。 • tomcat • ipsec • ITLRecovery • CallManager • CAPF • TVS 次のいずれかのオプションを選択すると、[**キー タイプ（Key Type）**] フィールドが **EC**（楕円曲線）に自動的に設定されます。 • tomcat-ECDSA • CallManager-ECDSA
[Distribution]	ドロップダウンリストから Unified Communications Manager サーバを選択します。
共通名	[**Distribution**] ドロップダウンリストで選択した Unified Communications Manager サーバの名前が表示されます。

フィールド	説明
[Auto-populated Domains]	[**Certificate Purpose**] ドロップダウンリストから次のオプションのいずれかを選択した場合にのみ表示されます。 • tomcat • tomcat-ECDSA • CallManager • CallManager-ECDSA • TVS このフィールドには、1 つの証明書によって保護されるホストの名前がリスト表示されます。証明書の共通名はホスト名と同じです。**CallManager-ECDSA** 証明書と **tomcat-ECDSA** 証明書の両方には、ホスト名と異なる共通名があります。 このフィールドには、**CallManager-ECDSA** 証明書用の完全修飾ドメイン名が表示されます。
Key Type	このフィールドは秘密/公開キーのペアの暗号化と復号化に使用されるキー タイプを示します。 Unified Communications Manager は **EC** および **RSA** キー タイプをサポートしています。

フィールド	説明
[Key Length]	ドロップダウンリストから、次の値のいずれかを選択します。 • 1024 • 2048 • 3072 • 4096 キー長に応じて、自己署名証明書の要求によりハッシュアルゴリズムの選択肢が限定されます。ハッシュアルゴリズムの選択が限定されることで、キー長の強度以上のハッシュ アルゴリズム強度が確保されます。 • キー長の値が256の場合、サポートされるハッシュアルゴリズムは、SHA256、SHA384、またはSHA512です。 • キー長の値が384の場合、サポートされるハッシュアルゴリズムは、SHA384またはSHA512です。 （注） **キー長**の値が3072または4096の証明書を選択するのは、RSA 証明書の場合のみです。これらのオプションは、ECDSA 証明書については使用できません。 （注） CallManagerの[**Certificate Purpose**]で選択されたRSA **キー長**の値が2048を超えると、電話機のモデルによっては登録に失敗する場合があります。 詳細については、Cisco Unified Reporting Tool（CURT）の[**Unified CM Phone Feature List Report**]で、**3072/4096 RSA キー サイズ サポート**に対応した電話機モデルの一覧を確認できます。
Hash Algorithm	ドロップダウンリストからキー長以上の値を選択します。 （注） • [**Key Length**]フィールドで選択した値に基づいて、[**ハッシュ アルゴリズム（Hash Algorithm）**]ドロップダウンリストの値が変更されます。 • システムがFIPSモードで実行されている場合は、必ずハッシュ アルゴリズムとしてSHA256を選択する必要があります。

証明書署名要求の生成

特定の証明書タイプに対する新しい証明書署名要求を生成すると、アプリケーションはその証明書タイプの既存の証明書署名要求を上書きします。

Cisco Unified オペレーティング システムの管理から CSR を生成し、CA に示すことで、CA 署名の証明書をアップロードすることができます。CSR を生成するたびに、CSR と一緒に新しい秘密キーが生成されます。

秘密キーは、CSR を生成するときに選択した、サーバとサービスに一意なファイルです。セキュリティ コンプライアンスのため、この秘密キーは誰とも共有しないでください。秘密キーを誰かに渡すと、証明書のセキュリティが損なわれます。また、古い CSR を使用して証明書を作成する場合は、同じサービス用の新しい CSR を再生成しないでください。Unified Communications Manager は古い CSR と秘密キーを削除し、それらの両方を新しいものに置き換えて、古い CSR を使用不能にします。

（注） Unified Communications Manager リリース 11.0 以降では、TFTP またはすべての一括操作ユニットを選択した場合は、ECDSA 証明書は RSA 証明書に含まれるようになります。

手順

ステップ 1 [Cisco Unified OS Administration] から **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。
[証明書リスト（Certificate List）] ウィンドウが表示されます。

ステップ 2 [Generate CSR] をクリックします。
[Generate Certificate Signing Request] ウィンドウが表示されます。

ステップ 3 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。

ステップ 4 [Certificate Purpose] ドロップダウン ボックスから、[CallManager-ECDSA] などのシステム セキュリティ証明書を選択します。

ステップ 5 [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、「関連項目」の項を参照してください。

ステップ 6 [Generate] をクリックします。

関連トピック

証明書署名要求のフィールド （97 ページ）

証明書署名要求のフィールド

表 *13 :* 証明書署名要求のフィールド

フィールド	説明
[Certificate Purpose]	ドロップダウン ボックスから値を選択します。 • **CallManager** • **CallManager-ECDSA**

[Distribution]	Unified Communications Manager サーバを選択します。
	ECDSA の MultiServer にこのフィールドを選択すると、構文は次のとおりです。
	`Callmanager-ecdsa common name: <host-name>-EC-ms.<domain>`
	RSA の MultiServer にこのフィールドを選択すると、構文は次のとおりです。
	`Callmanager common name: <host-name>-ms.<domain>`

Common Name	デフォルトでは、**[Distribution]** フィールドで選択した Unified Communications Manager アプリケーションの名前が表示されます。
[Auto-populated Domains]	このフィールドは [Subject Alternate Names（SANs）] セクションに表示されます。1 つの証明書によって保護されるホストの名前をリストします。
[Parent Domain]	このフィールドは [Subject Alternate Names（SANs）] セクションに表示されます。デフォルトドメイン名を表示します。必要に応じてドメイン名を変更できます。
[Key Type]	このフィールドは秘密/公開キーのペアの暗号化と復号化に使用されるキー タイプを示します。 Unified Communications Manager は **EC** および **RSA** キー タイプをサポートしています。

フィールド	説明
[Key Length]	[Key Length] ドロップダウン ボックスから、値を 1 つ選択します。 キーの長さに応じて、CSR 要求によりハッシュ アルゴリズムの選択肢が限定されます。ハッシュ アルゴリズムの選択に制限が加わることで、キー長の強度以上のハッシュ アルゴリズム強度が確保されます。たとえばキー長が 256 の場合、サポートされるハッシュ アルゴリズムは、SHA256、SHA384、SHA512 です。同様にキー長が 384 の場合、サポートされるハッシュ アルゴリズムは SHA384 または SHA512 です。 （注） RSA 証明書については、[Key Length] の値が 3072 または 4096 の証明書のみを選択できます。これらのオプションは、ECDSA 証明書については使用できません。 （注） CallManager が [Certificate Purpose] で選択した RSA の [key length] が 2048 より大きいと、一部の電話モデルが登録に失敗する場合があります。Cisco Unified Reporting Tool（CURT）の [Unified CM Phone Feature List Report] で、3072/4096 RSA キー サイズ サポート機能をサポートする電話モデルの一覧を確認できます。
[Hash Algorithm]	楕円曲線のキー長と同じ強さのハッシュ アルゴリズムになるように、値を [Hash Algorithm] ドロップダウン ボックスから選択します。[Hash Algorithm] ドロップダウン ボックスから、値を 1 つ選択します。 （注） • [Key Length] フィールドで選択した値に基づいて [Hash Algorithm] フィールドの値は変化します。 • システムが FIPS モードで実行されている場合は、必ずハッシュアルゴリズムとして SHA256 を選択する必要があります。

連携動作と制限事項

• **TLS_ECDHE_ECDSA_WITH_AES256_SHA384**および TLS_ECDHE_ECDSA_WITH_AES128_SHA256 をサポートしない SIP デバイスは、引き続き TLS_ECDHE_RSA_WITH_AES_256_SHA384 、**TLS_ECDHE_ に接続できます RSA_WITH_AES_128_SHA256**、またはAES128_SHA。これらのオプションは、選択した TLS 暗号オプションによって異なります。[ECDSA only] オプションを選択すると、ECDSA

暗号化をサポートしないデバイスは SIP インターフェイスへの TLS 接続を確立できません。[ECDSA only] オプションを選択すると、このパラメータの値は **TLS_ECDHE_ECDSA_WITH_AES128_SHA256** および **TLS_ECDHE_ECDSA_WITH_AES256_SHA384** になります。

- CTI Manager のセキュア クライアントは、**TLS_ECDHE_RSA_WITH_AES_128_SHA256**、**TLS_ECDHE_RSA_WITH_AES_256_SHA384**、**TLS_ECDHE_ECDSA_WITH_AES_128_SHA256**、および **TLS_ECDHE_ECDSA_WITH_AES_256_SHA384** をサポートしていません。ただし、**AES128_SHA** を使用して接続できます。

ITL ファイルの一括リセットの実行

Unified Communications Manager クラスタのデバイスがロックされて、信頼のステータスを失った場合は、CLI コマンド **utils itl reset** を使用してアイデンティティ信頼リスト（ITL）ファイルの一括リセットを行います。このコマンドにより、新しい ITL リカバリ ファイルが生成されます。

ヒント Unified Communications Manager の新規インストールを実行した場合は、できるだけ早く ITL キーをエクスポートし、ディザスタ リカバリ システムによるバックアップを行います。

ITL リカバリ ペアをエクスポートする CLI コマンドは次のとおりです。

file get tftp *ITLRecovery.p12*

（キーのエクスポート先となる）SFTP サーバとパスワードの入力を求めるプロンプトが表示されます。

始める前に

この手順は必ず Unified Communications Manager パブリッシャで実行してください。必要に応じて、パブリッシャからキーをエクスポートします。

手順

ステップ 1 次のいずれかの手順を実行します。

- **utils itl reset localkey**の実行
- **utils itl reset remotekey**の実行

（注） **utils itl reset localkey**では、ローカルキーはパブリッシャ側にあります。このコマンドを発行しているとき、ITL回復キーをリセットしている間、ITLファイルはCallManagerキーによって一時的に署名されます。

ステップ 2 リセットが正常に行われたことを確認するには **show itl** を実行します。

ステップ 3 [Unified Communications Manager Administration] で、**[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。

ステップ 4 [リセット（Reset）] をクリックします。

デバイスが再起動されます。これで、CallManager キーで署名された ITL ファイルをダウンロードし、設定ファイルを受け入れる準備が整いました。

ステップ 5 TFTP サービスを再起動し、すべてのデバイスを再起動します。

（注） TFTP サービスを再起動すると、ITL ファイルが ITLRecovery キーによって署名され、ステップ 1 の変更がロールバックされます。

デバイスは ITLRecovery キーで署名されている ITL ファイルをダウンロードし、Unified Communications Manager に正しく再登録します。

ITLRecovery 証明書の有効期間の表示

手順

ステップ 1 [Cisco Unified OS Administration] から、**[Security] > [Certificate Management]** を選択します。[Certificate List] ウィンドウが表示されます。

ステップ 2 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。

ステップ 3 [ITLRecovery] リンクをクリックして、有効期間を確認します。

ステップ 4 [OK] をクリックします。

連絡先検索の認証設定タスク フロー

Unified Communications Manager で連絡先検索の認証をセットアップするには、次のタスクを実行します。この機能が設定されている場合、ユーザはディレクトリで他のユーザを検索する前にユーザ自身を認証する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	連絡先検索の認証の電話サポートの確認（101 ページ）	電話でこの機能がサポートされていることを確認します。Cisco Unified Reporting

	コマンドまたはアクション	目的
		で [Unified CM Phone Feature List] レポートを実行し、この機能をサポートしている電話モデルのリストを確認します。
ステップ 2	連絡先検索の認証の有効化 （101 ページ）	Unified Communications Manager で連絡先検索の認証を設定します。
ステップ 3	連絡先検索用のセキュアなディレクトリサーバの設定 （102 ページ）	電話のユーザがディレクトリで他のユーザを検索したときに示される URL を Unified Communications Manager で設定するには、次の手順を実行します。

連絡先検索の認証の電話サポートの確認

導入環境内の電話が連絡先検索の認証をサポートしていることを確認します。[Phone Feature List] レポートを実行して、この機能をサポートしているすべての電話モデルのリストを取得します。

手順

ステップ 1 Cisco Unified Reporting から [システム レポート(System Reports)] をクリックします。
ステップ 2 [ユニファイド CM 電話機能 (Unified CM Phone Feature)] を選択します。
ステップ 3 [ユニファイド CM 電話機能 (Unified CM Phone Feature)] レポートをクリックします。
ステップ 4 [製品 (Product)] フィールドはデフォルト値のままにします。
ステップ 5 [機能 (Feature)] ドロップダウンから [Authenticated Contact Search] を選択します。
ステップ 6 [Submit] をクリックします。`

次のタスク

連絡先検索の認証の有効化 （101 ページ）

連絡先検索の認証の有効化

電話ユーザの連絡先検索の認証を設定するには、Unified Communications Manager でこの手順に従います。

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 **utils contactsearchauthentication status** コマンドを実行し、このノードの連絡先検索の認証の設定を確認します。

ステップ 3 連絡先検索の認証の設定が必要な場合、

- 認証を有効にするには、**utils contactsearchauthentication enable** コマンドを実行します。
- 認証を無効にするには、**utils contactsearchauthentication disable** コマンドを実行します。

ステップ 4 すべての Unified Communications Manager クラスタ ノードでこの手順を繰り返します。

（注） 変更を有効にするには、電話をリセットする必要があります。

次のタスク

連絡先検索用のセキュアなディレクトリ サーバの設定 （102 ページ）

連絡先検索用のセキュアなディレクトリ サーバの設定

UDS がユーザ検索リクエストを送信するディレクトリ サーバ URL を Unified Communications Manager に設定するには、次の手順を使用します。デフォルトの値は `https://<cucm-fqdn-or-ip>:port/cucm-uds/users` です。

（注） デフォルトの UDS ポートは 8443 です。連絡先検索の認証が有効になると、デフォルトの UDS ポートは 9443 に切り替わります。その後、連絡先検索の認証を無効にした場合は、UDS ポートを手動で 8443 に戻す必要があります。

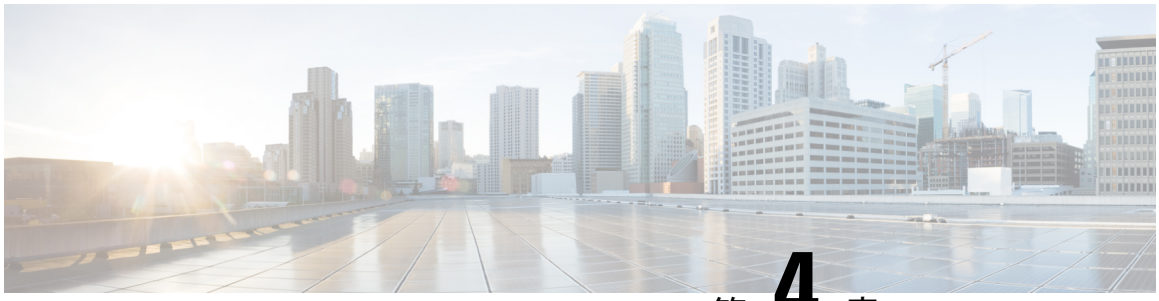
手順

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

ステップ 2 [Secure Contact Search URL] テキスト ボックスに、セキュアな UDS ディレクトリ要求の URL を入力します。

（注） URL には、Cisco TFTP サービスを実行していないノードを選択することを推奨します。Cisco TFTP と UDS サービスのいずれかのサービスが再起動すると、互いに悪影響が及ぶ可能性があります。

ステップ 3 **[保存 (Save)]** をクリックします。



第 4 章

Cisco CTL クライアントの設定

この章では、Cisco CTL クライアントの設定について説明します。

Cisco CTL の設定について

デバイス認証、ファイル認証およびシグナリング認証は、証明書信頼リスト（CTL）ファイルの作成に依存します。このファイルは、シスコの証明書信頼リスト(CTL)をインストールして設定すると作成されます。

（注）

- 混合モードを有効にするかまたは CTL ファイルを更新するには、エクスポート制御機能を許可するオプションを有効にする、Smart アカウントまたは仮想アカウントから受信した登録トークンを使用することにより、Unified Communications Manager で Smart ライセンス登録が完了していることを確認します。シスコ スマート ソフトウェア ライセンシングの設定方法の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『*System Configuration Guide for Cisco Unified Communications Manager*』の「「Smart Software Licensing」」の章を参照してください。
- CTL クライアントを実行しているものの、Unified Communications Manager がエクスポート制御機能に対応していない場合、*ClusterModeSecurityFailedExportControlNotAllow* というアラームが送信されます。

CTL ファイルには、次のサーバまたはセキュリティ トークンのエントリが含まれています。

- System Administrator Security Token（SAST）
- 同じサーバ上で実行されている Cisco CallManager サービスと Cisco TFTP サービス
- Certificate Authority Proxy Function（CAPF）
- TFTP サーバ（複数の場合あり）
- ASA ファイアウォール
- ITLRecovery

CTL ファイルには、サーバごとのサーバ証明書、公開キー、シリアル番号、署名、発行者名、サブジェクト名、サーバ機能、DNS 名 および IP アドレスが含まれています。

CTL ファイルを作成したら、Cisco CallManager サービスと Cisco TFTP サービスが実行されているすべてのノード上の [Cisco Unified Serviceability] でこれらのサービスを再起動する必要があります。電話が次回初期化されたときに、その電話ではこの CTL ファイルを TFTP サーバからダウンロードします。CTL ファイルに自己署名証明書が含まれた TFTP サーバのエントリがある場合、電話では .sgn 形式の署名付き設定ファイルを要求します。TFTP サーバに証明書が含まれていない場合、電話では署名なしのファイルを要求します。

Cisco CTL クライアントが CTL ファイルにサーバ証明書を追加した後、次の CLI コマンドを実行して CTL ファイルを更新できます。

utils ctl set-cluster mixed-mode
CTL ファイルを更新し、クラスタを混合モードに設定します。
utils ctl set-cluster non-secure-mode
CTL ファイルを更新し、クラスタを非セキュア モードに設定します。
utils ctl update CTLFile
クラスタ内の各ノードの CTL ファイルを更新します。

CTL ファイルにファイアウォールを設定すると、セキュアな Unified Communications Manager システムの一部として Cisco ASA ファイアウォールを保護できます。ファイアウォール証明書が「「CCM」」証明書として表示されます。

（注）
- パブリッシャ ノードで CLI コマンドを実行する必要があります。
- CallManager 証明書を再生成すると、ファイルの署名者が変更されることに注意してください。デフォルトのセキュリティをサポートしていない電話は、電話から CTL ファイルが手動で削除されない限り、新しい CTL ファイルを受け入れません。電話機の CTL ファイルの削除の詳細については、お使いの電話機モデルの『Cisco IP 電話 Administration Guide』を参照してください。

リカバリのために CTL ファイル内に 2 番目の SAST 権限を追加する

以前のリリースの Unified Communications Manager では、トークンレス（トークンなし）アプローチが使用されていました。このアプローチでは、エンドポイントで 1 つの Cisco Site Administrator Security Token（SAST）だけを信頼します。この SAST は CallManager 証明書です。このアプローチでは、証明書信頼リスト（CTL）ファイルに、CTL ファイルへの署名に使用された 1 つの SAST レコードだけが含まれていました。1 つの SAST だけが使用されていたため、SAST の署名者になんらかの更新が行われると、エンドポイントがロックアウトされました。SAST の署名者の更新が原因でエンドポイントまたはデバイスがロックアウトされるシナリオを次に示します。

- エンドポイントで、登録時に CallManager 証明書の使用によって署名された CTL ファイルを受け入れた場合。
- 管理者が CallManager 証明書を再生成して、CTL ファイルを更新した場合。この再生成は、更新した CTL ファイルが既存の CallManager 証明書ではなく、更新した CallManager 証明書によって署名されたことを意味しています。
- 更新した証明書がエンドポイントの信頼リストで取得できなかったため、エンドポイントではその更新した CallManager 証明書が信頼されなかった場合。このため、そのエンドポイントでは、その CTL ファイルをダウンロードするのではなく拒否しました。
- エンドポイントで、Transport Layer Security（TLS）を使用して ccm サービスと安全に接続しようとし、ccmservice がその更新した CallManager 証明書をエンドポイントに TLS 交換の一部として提供した場合。その更新した証明書がエンドポイントの信頼リストで取得できなかったので、エンドポイントではその CTL ファイルをダウンロードするのではなく拒否しました。
- エンドポイントが ccmservice と通信しなくなり、その結果ロックアウトされた場合。

エンドポイントのロックアウトからのリカバリを容易にするために、エンドポイントのトークンレス アプローチが拡張され、リカバリのために CTL ファイル内に 2 番目の SAST が追加されました。この機能では、トークンレス CTL ファイルに CallManager レコードと ITLRecovery レコードという 2 つの SAST トークンが含まれています。

ITLRecovery 証明書が、次の理由から他の証明書よりも優先して選択されます。

- ホスト名の変更など、二次的な理由で変化しないため。
- ITL ファイル内ですでに使用されているため。

CLI を使用した SIP OAuth 設定

CLI を使用して、クラスタ SIP OAuth モードを設定することができます。

（注） Cisco Unified Communications Manager での SIP OAuth モードの設定方法の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*、リリース *12.5(1)*』を参照してください。

次の点を考慮してください。

- クラスタ SIP OAuth モードが有効になっている場合、Cisco ユニファイドコミュニケーションマネージャーは、セキュアデバイスから OAuth トークンを受信した SIP 登録を受け入れることができます。

  有効にすると、Cisco ユニファイドコミュニケーションマネージャーのユーザインターフェイスを使用して設定可能な次の TLS ポートが開かれます。

  - **SIP OAuth ポート**
  - **SIP OAuth MRA ポート**

  [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、**[システム（System）]** > **[Cisco Unified CM]** > **Call Manager** ページを選択します。

- パラメータ変更を反映するには、すべてのノードで Cisco CallManager サービスを再起動してください。

この暗号化方法では次の CLI コマンドを使用します。

管理者: ユーティリティ sipOAuth モード
クラスタ内の SIP OAuth モードのステータスを確認します。

ユーティリティ sipOAuth モードの有効化
クラスタ内の SIP OAuth モードを有効にします。

ユーティリティ sipOAuth モードの無効化
クラスタ内の SIP OAuth モードを無効にします。

（注） パブリッシャ ノードでのみ CLI コマンドを実行すします。

Cisco CTL Provider サービスの有効化

Cisco CTL クライアントの設定後、Cisco CTL Provider サービスのセキュリティ モードは非セキュアから混合モードに変わり、サーバの証明書を CTL ファイルに伝送します。このサービスは、CTL ファイルをすべての Unified Communications Manager および Cisco TFTP サーバに伝送します。

このサービスを有効にし、Unified Communications Manager をアップグレードすると、Unified Communications Manager は、アップグレード後に自動的にサービスを再起動します。

ヒント クラスタ内のすべてのサーバで Cisco CTL Provider サービスを有効化する必要があります。

このサービスを有効化するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Serviceability で、**[Tools]** > **[Service Activation]** を選択します。

ステップ 2 [Servers] ドロップダウン リスト ボックスで、Cisco CallManager または Cisco TFTP サービスが有効になっているサーバを選択します。

ステップ 3 [Cisco CTL Provider] サービスのオプション ボタンをクリックします。

ステップ 4 [Save] をクリックします。

ヒント クラスタ内のすべてのサーバでこの手順を実行します。

（注） Cisco CTL Provider サービスを有効にする前に、CTL ポートを入力できます。デフォルトのポート番号を変更するには、TLS接続のためのポートの設定に関するトピックを参照してください。

ステップ 5 サービスがサーバで実行されていることを確認します。Cisco Unified Serviceability で、**[Tools]** > **[Control Center - Feature Services]** を選択し、サービスの状態を確認します。

CAPF サービス有効化

警告 Cisco CTL クライアントをインストールして設定する前に、Cisco Certificate Authority Proxy Function（CAOF）サービスを有効化すると、CAPF を使用するために CTL ファイルを更新する必要がなくなります。

セキュア ポートの設定

デフォルトポートが現在使用中の場合、またはファイアウォールを使用していてファイアウォール内のポートを使用できない場合に、異なる TLS ポート番号の設定が必要になることがあります。

- Cisco CTL Provider の TLS 接続用のデフォルト ポートは 2444 です。Cisco CTL Provider ポートでは、Cisco CTL クライアントからの要求をモニタします。このポートでは、CTL ファイルの取得、クラスタ セキュリティ モードの設定、TFTP サーバへの CTL ファイルの保存などの、Cisco CTL クライアントの要求を処理します。

（注） クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します。

- イーサネット電話ポートでは、SCCP を実行中の電話からの登録要求をモニタします。非セキュア モードでは、電話はポート 2000 を介して接続されます。混合モードでは、TLS 接続用の Unified Communications Manager ポートは、Unified Communications Manager のポート番号に 443 を加算（+）した番号になるため、Unified Communications Manager のデフォルトの TLS 接続ポートは 2443 になります。この設定は、ポート番号が使用中の場合、またはファイアウォールを使用していてファイアウォール内のポートを使用できない場合にのみ更新します。
- SIP セキュア ポートを使用すると、Unified Communications Manager で、SIP を実行中の電話からの SIP メッセージをリッスンできます。デフォルト値は 5061 です。このポートを変更した場合は、[Cisco Unified Serviceability] で Cisco CallManager サービスを再起動して、SIP を実行中の電話をリセットする必要があります。

ヒント ポートを更新した後、[Cisco Unified Serviceability] で Cisco CTL Provider サービスを再起動する必要があります。

ヒント　CTL ポートは、CTL クライアントが実行されている場所からデータ VLAN に対して開く必要があります。

デフォルト設定を変更するには、次の手順を実行します。

手順

ステップ 1　変更するポートに応じて、次の作業を実行します。

a) Cisco CTL Provider サービスの Port Number パラメータを変更するには、ステップ 2 （109 ページ）からステップ 6 （109 ページ）を実行します。

b) [Ethernet Phone Port] または [SIP Phone Secure Port] の設定を変更するには、ステップ 7 （109 ページ）からステップ 11 （109 ページ）を実行します。

ステップ 2　Cisco CTL Provider ポートを変更するには、[Unified Communications Manager Administration] で、**[System]** > **[Service Parameters]** を選択します。

ステップ 3　[Server] ドロップダウンリストで、Cisco CTL Provider サービスが実行されているサーバを選択します。

ステップ 4　[Service] ドロップダウン リスト ボックスで、[Cisco CTL Provider service] を選択します。

ヒント　サービスパラメータの詳細については、疑問符またはリンク名をクリックしてください。

ステップ 5　[Port Number] パラメータの値を変更するには、[Parameter Value] フィールドに新しいポート番号を入力します。

ステップ 6　[Save] をクリックします。

ステップ 7　[Ethernet Phone Port] または [SIP Phone Secure Port] の設定を変更するには、[Unified Communications Manager Administration] で **[System]** > **[Cisco Unified CM]** を選択します。

ステップ 8　『*Administration Guide for Cisco Unified Communications Manager*』の説明に従い、Cisco CallManager サービスが実行されているサーバを検索します。結果が表示されたら、そのサーバの [Name] リンクをクリックします。

ステップ 9　Unified Communications Manager の [Configuration] ウィンドウが表示されたら、[Ethernet Phone Port] フィールドまたは [SIP Phone Secure Port] フィールドに新しいポート番号を入力します。

ステップ 10　電話をリセットし、[Cisco Unified Serviceability] で Cisco CallManager サービスを再起動します。

ステップ 11　**[保存 (Save)]** をクリックします。

Cisco CTL クライアントの設定

重要 **utils ctl** CLI コマンド セットを使用して、暗号化を設定することができます。このオプションの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

（注）

- CLI コマンド **utils ctl set-cluster mixed-mode** は、混合モードでクラスタを設定します。混合モードを有効にするには、Unified Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されていること、およびスマート アカウントまたはバーチャルアカウントから受信した登録トークンでエクスポート制御機能の許可が有効になっており、そのトークンがこのクラスタに登録されていることを確認します。
- CLI コマンド **utils ctl update CTLFile** は、CTL ファイルを更新します。混合モードで CTLFile を更新するには、Unified Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されていること、およびスマート アカウントまたはバーチャルアカウントから受信した登録トークンでエクスポート制御機能の許可が有効になっており、そのトークンがこのクラスタに登録されていることを確認します。
- エクスポート制御機能を許可するオプションが有効になっている登録トークンに Unified Communications Manager が登録されていない場合、**utils ctl set-cluster mixed-mode** コマンドまたは **utils ctl update CTLFile** コマンドを実行すると、次のエラー メッセージが表示されます。

  `Command cannot be executed because the Unified Communications Manager cluster is not registered to a Smart/Virtual Account with Allow export-controlled functionality.`UCMクラスタを登録するときに、スマート/仮想アカウントから受信した製品トークンで[エクスポート制御機能を許可する]チェックボックスがオンになっていることを確認してください.

Cisco CTL CLI では、次のタスクが実行されます。

- クラスタまたはスタンドアロンサーバ用の Unified Communications Manager セキュリティ モードを設定します。

（注） Unified Communications Manager Administration の [Enterprise Parameters Configuration] ウィンドウで、Unified Communications Manager のクラスタ セキュリティ パラメータを混合モードに設定することはできません。Cisco CTL クライアントまたは CLI コマンドセット **utils ctl** からクラスタ セキュリティモードを設定できます。

- 証明書信頼リスト（CTL）を作成します。これは、セキュリティ トークン、Unified Communications Manager、ASA ファイアウォール、および CAPF サーバ用の証明書エントリが含まれたファイルです。

  CTL ファイルによって、電話接続用の TLS をサポートするサーバが示されます。クライアントは自動的に Unified Communications Manager、Cisco CAPF、および ASA ファイアウォールを検出し、これらのサーバの証明書エントリを追加します。

  （注） Cisco CTL クライアントは、スーパークラスタ サポートも提供します。スーパークラスタには、最大 16 のコールを処理するサーバ、1 つのパブリッシャ、2 つの TFTP サーバ、および最大 9 つのメディア リソース サーバが含まれます。

  ヒント CTL ファイルの更新は予定されたメンテナンスができます。これは、クラスタ内で Cisco CallManager を実行するすべてのサーバが動する必要があるためです。

  Cisco CTL の設定が完了すると、CTL は次のタスクを実行します。

  - CTL ファイルを Unified Communications Manager サーバに書き込みます。
  - CAPF capf.cer をクラスタ内のすべての Unified Communications Manager 後続ノード（最初のノード以外）に書き込みます。
  - PEM 形式の CAPF 証明書ファイルをクラスタ内のすべての Unified Communications Manager 後続ノード（最初のノード以外）に書き込みます。
  - すべての設定済み TFTP サーバにこのファイルを書き込みます。
  - すべての設定済み ASA ファイアウォールにこのファイルを書き込みます。
  - CTL ファイルを作成した時点で USB ポートに存在するセキュリティ トークンの秘密キーを使用して、CTL ファイルに署名します。

CTL ファイルの SAST 役割

（注） CTL ファイルに署名するには、次の表に記載されている*署名者が使用されます。

表 *14 : CTL* ファイルのシステム管理者セキュリティ トークン（*SAST*）役割

Cisco ユニファイド コミュニケーション マネージャ のバージョン	トークン ベースの CTL ファイルでの SAST 役割	Tokenless CTL ファイルでの SAST 役割
12.0(1)	トークン 1（署名者*） トークン 2 ITLRecovery CallManager	CallManager（署名者） ITLRecovery
11.5(x)	トークン 1（署名者） トークン 2 ITLRecovery CallManager	CallManager（署名者） ITLRecovery
10.5(2)	トークン 1（署名者） トークン 2	CallManager（署名者） ITLRecovery
10.5(1) （サポート外）	トークン 1（署名者） トークン 2	CallManager（署名者）
10.0(1) （サポート外）	トークン 1（署名者） トークン 2	CallManager（署名者）
9.1(2)	トークン 1（署名者） トークン 2	N/A

クラスタ間での電話の移行

クラスタ間で電話を移動するには、次の手順に従ってください。たとえば、クラスタ 1 からクラスタ 2 に移動するとします。

手順

ステップ 1 クラスタ 2 で、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 [検索（Find）] をクリックします。

ステップ 3 証明書の一覧で、ITLRecovery 証明書をクリックし、[.PEM ファイルのダウンロード（Download .PEM File）] または [.DER ファイルのダウンロード（Download .DER File）] のいずれかをクリックすることにより、いずれかのファイル形式の証明書をコンピュータにダウンロードします。
証明書の詳細が表示されます。

ステップ 4 証明書の一覧で、CallManager 証明書をクリックし、[.PEM ファイルのダウンロード（Download .PEM File）] または [.DER ファイルのダウンロード（Download .DER File）] のいずれかをクリックすることにより、いずれかのファイル形式の証明書をコンピュータにダウンロードします。
証明書の詳細が表示されます。

ステップ 5 クラスタ 1 で、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。
[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 6 [証明書チェーンのアップロード（Upload Certificate Chain）] をクリックすることにより、ダウンロードした証明書をアップロードします。

ステップ 7 [証明書の目的（Certificate Purpose）] ドロップダウン リストで、[電話と SAST 間の信頼（Phone-SAST-trust）] を選択します。

ステップ 8 [ファイルのアップロード（Upload File）] フィールドで、[ファイルの選択（Choose File）] をクリックし、手順 3 でダウンロードした ITLRecovery ファイルを参照し、[ファイルのアップロード（Upload File）] をクリックします。

アップロードされた ITLRecovery ファイルが、クラスタ 1 の [証明書リスト（Certificate List）] ウィンドウで [電話と SAST 間の信頼（Phone-SAST-Trust）] 証明書に対して表示されます。新しい ITL ファイルにクラスタ 2 の ITLRecovery 証明書がある場合は、コマンド `show itl` を実行します。

ステップ 9 クラスターの電話にローカルで有効な証明書（LSC）がある場合、クラスタ 1 からの CAPF 証明書をクラスタ 2 の CAPF 信頼ストアにアップロードしなければなりません。

ステップ 10 （任意） この手順は、クラスタが混合モードの場合にのみ適用可能です。CLI で **utils ctl update CTLFile** コマンドを実行することにより、CTL ファイルをクラスタ 1 で再生成します。

（注）
- `show ctl` CLI コマンドを実行することにより、クラスタ 2 の ITLRecovery 証明書と CallManager 証明書が、SAST としての役割で CTL ファイルに含められるようにします。
- 電話が新しい CTL ファイルおよび ITL ファイルを受け取っていることを確認します。更新された CTL ファイルには、クラスタ 2 の ITLRecovery 証明書が含まれています。

クラスタ 1 からクラスタ 2 に移行する電話が、クラスタ 2 の ITLRecovery 証明書を受け付けるようになります。

ステップ 11 クラスタ間で電話を移行します。

eToken ベースの CTL ファイルから Tokenless CTL ファイルへの移行

Tokenless CTL ファイルについては、ユニファイド コミュニケーション マネージャ リリース 12.0(1) で USB トークンを使用して生成されたアップロード済み CTL ファイルのダウンロードをエンドポイントで実行するよう、管理者が確認する必要があります。ダウンロード後、管理者は Tokenless CTL ファイルに切り替えることができます。次に、`utils ctl upgrade` CLI コマンドを実行することができます。

CTL ファイルの更新

（注） CLI コマンド セット **utils ctl** でクラスタ セキュリティを管理する場合は、この手順は必要ありません。

次の状況が発生したら CTL ファイルを更新する必要があります。

- 新しい Unified Communications Manager サーバをクラスタに追加する

  （注） ノードをセキュア クラスタに追加するには、ノードの追加方法および新しいノード用のセキュリティの設定方法を説明している『*Installing Unified Communications Manager*』を参照してください。

- Unified Communications Manager サーバの名前または IP アドレスを変更する
- 設定されたすべての TFTP サーバの IP アドレスまたはホスト名を変更する
- 設定されたすべての ASA ファイアウォールの IP アドレスまたはホスト名を変更する
- [Cisco Unified Serviceability] で Cisco Certificate Authority Function サービスを有効にする
- セキュリティ トークンを追加または削除する必要がある
- TFTP サーバを追加または削除する必要がある
- Unified Communications Manager サーバを追加または削除する必要がある
- ASA ファイアウォールを追加または削除する必要がある

- Unified Communications Manager サーバまたは Unified Communications Manager データを復元する
- CTL ファイルを含む Cisco ユニファイドコミュニケーションマネージャークラスタのすべてのノード上で、CallManager、CAPF、またはITL回復証明書を手動で再生成した場合は、[CTL] ウィザードを再実行する必要があります。この手順は、他の証明書の生成には必要ありません。
- Unified Communications Manaver を 7.1.5 以前のバージョンから 7.1.5 以降のバージョンに更新する
- バージョン 10.5 より前の Unified Communications Manager を 10.5 以降のバージョンに更新する場合は、移行に関する「ハードウェア eToken からトークンレスの解決策へ」のセクションを参照してください。
- サードパーティの CA 署名付き証明書をプラットフォームにアップロードした後。

（注） 混合モードの Unified Communications Manager クラスタでドメイン名が追加または変更された場合、その電話設定ファイルを有効にするには CTL ファイルを更新する必要があります。

ヒント ファイルの更新は、呼処理中断がもっとも少ない時期に行うことが推奨されます。

注意 セキュアな SIP または SCCP を使用して Unified Communications Manager が Unity Connection 10.5 以降と統合されている場合は、Unity Connection でセキュアなコールが停止することがあります。この問題を解決するには、Unity Connection で対応するポート グループをリセットする必要があります。

Unity Connection Administration インターフェイスでポート グループをリセットするには、**[Telephony Integrations]** > **[Port Group]** に移動し、リセットするポート グループを選択して、[Port Group Basics] ページで [Reset] をクリックします。

Cisco Unified Communications Manager セキュリティ モードの更新

クラスタ セキュリティ モードを設定するには、Cisco CTLを使用する必要があります。Unified Communications Manager のセキュリティ モードは、[Unified Communications Manager Administration] の [Enterprise Parameters Configuration] ウィンドウから変更することはできません。

（注） クラスタ セキュリティ モードでは、スタンドアロン サーバまたはクラスタのセキュリティ機能の設定を行います。

Cisco CTL クライアントの初期設定後にクラスタ セキュリティ モードを変更するには、CTL ファイルを更新する必要があります。

手順

ステップ 1 `utils ctl set-cluster mixed-mode` CLI コマンドを実行して、クラスタ セキュリティ モードをセキュアに変更します。

ステップ 2 `utils ctl set-cluster non-secure-mode` CLI コマンドを実行して、クラスタ セキュリティ モードを非セキュアに変更します。

Cisco CTL ファイルの詳細

（注） セキュリティ トークンが不要な **utils ctl** CLI コマンド セットを使用して暗号化を設定できます。このオプションの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

次の表に示すように、クラスタ セキュリティ モードを非セキュア モードまたは混合モードに設定できます。認証、シグナリング暗号化、およびメディア暗号化は混合モードでのみサポートされます。

（注） クラスタ セキュリティ モードでは、スタンドアロン サーバまたはクラスタのセキュリティ機能の設定を行います。

表 *15 : CTL* の設定

設定	説明
Unified Communications Managerサーバ	
Security Mode	

設定	説明
Unified Communications Manager クラスタの混合モードへの設定	混合モードでは、認証済み、暗号化済み、および非セキュアな Cisco IP Phone を Unified Communications Manager に登録できます。このモードでは、認証済みまたは暗号化済みのデバイスについて、Unified Communications Manager によってセキュアなポートの使用が確保されます。
Unified Communications Manager クラスタの非セキュア モードへの設定	非セキュア モードに設定すると、すべてのデバイスが非認証として登録され、Unified Communications Manager によってイメージ認証のみがサポートされます。 このモードを選択すると、CTL ファイル内にリストされているすべてのエントリの証明書が Cisco CTL クライアントによって削除されますが、CTL ファイルそのものは指定のディレクトリに引き続き存在します。未署名の設定ファイルが電話によって要求され、Unified Communications Manager に非セキュアとして登録されます。 **ヒント** デフォルトの非セキュアモードに電話を戻すには、電話およびすべての Unified Communications Manager サーバから CTL ファイルを削除する必要があります。
[CTL Entries]	
トークン	サーバまたはワークステーションに当初挿入したトークンをまだ削除していない場合は削除します。アプリケーションが次のトークンを要求したら、そのトークンを挿入して [OK] をクリックします。追加したセキュリティ トークンについての情報が表示されたら、[Add] をクリックします。すべてのセキュリティ トークンについて、これらの操作を繰り返します。
[Add TFTP Server]	証明書信頼リストに代替 TFTP サーバを追加するには、このボタンをクリックします。設定の詳細については、[Alternate TFTP Server] タブの設定が表示された後に [Help] ボタンをクリックします。設定を入力したら、[Next] をクリックします。

設定	説明
[Add Firewall]	証明書信頼リストにASAファイアウォールを追加するには、このボタンをクリックします。設定の詳細については、[Firewall] タブの設定が表示された後に [Help] ボタンをクリックします。設定を入力したら、[Next] をクリックします。

Cisco Unified Communications Manager セキュリティ モードの確認

クラスタ セキュリティ モードを確認するには、次の手順を実行します。

（注） クラスタ セキュリティ モードでは、スタンドアロン サーバまたはクラスタのセキュリティ機能の設定を行います。

手順

ステップ 1 Unified Communications Manager Administration で、**[システム（System）] > [エンタープライズ パラメータの設定（Enterprise Phone Configuration）]** を選択します。

ステップ 2 [Cluster Security Mode] フィールドを見つけます。フィールドの値が **1** と表示されている場合、混合モード用に Unified Communications Manager が正しく設定されています。（フィールド名をクリックすると追加情報を参照できます。）

ヒント Unified Communications Manager Administration でこの値を設定することはできません。Cisco CTL クライアントの設定後、この値が表示されます。

[automatic] または [started] への Smart Card サービスの設定

インストールされている Cisco CTL クライアントが Smart Card サービスの無効を検出した場合、Cisco CTL クライアント プラグインをインストールするサーバまたはワークステーションで SmartCard サービスを [automatic] と [started] に設定する必要があります。

ヒント　サービスが [started] および [automatic] に設定されていない限り、CTL ファイルにセキュリティトークンを追加できません。

ヒント　オペレーティング システムのアップグレード、サービス リリースの適用、Cisco Unified Communications Manager のアップグレードなどの後には、Smart Card サービスが実行中で自動になっていることを確認します。

サービスを [started] および [automatic] に設定するには、次の手順を実行します。

手順

ステップ 1　Cisco CTL クライアントをインストールしてあるサーバまたはワークステーションで、**[Start]** > **[Programs]** > **[Administrative Tools]** > **[Services]** または **[Start]** > **[Control Panel]** > **[Administrative Tools]** > **[Services]** を選択します。

ステップ 2　[Services] ウィンドウで、[Smart Card] サービスを右クリックして、[Properties] を選択します。

ステップ 3　[Properties] ウィンドウで [General] タブが表示されることを確認します。

ステップ 4　[Startup Type] ドロップダウン リスト ボックスから [Automatic] を選択します。

ステップ 5　[Apply] をクリックします。

ステップ 6　[Service Status] エリアで [Start] をクリックします。

ステップ 7　[OK] をクリックします。

ステップ 8　サーバまたはワークステーションをリブートし、サービスが実行されていることを確認します。

Cisco CTL クライアントの確認またはアンインストール

Cisco CTL クライアントをアンインストールしても、CTL ファイルが削除されません。同様に、クライアントをアンインストールしても、クラスタ セキュリティ モードと CTL ファイルは変更されません。アンインストールする場合は、CLI オプションを使用して Cisco CTL をアンインストールすることができます。

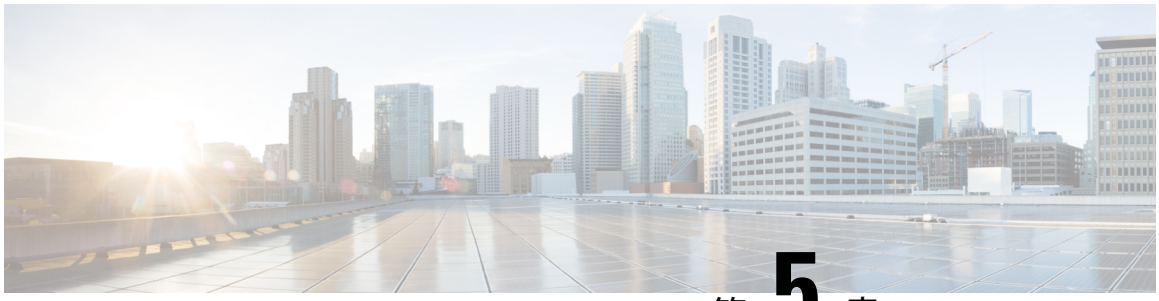
Cisco CTL クライアントがインストールされていることを確認するは、次の手順を実行します。

手順

ステップ 1　**[Start]** > **[Control Panel]** > **[Add or Remove Programs]** の順に選択します。

ステップ 2　[Cisco CTL Client] を見つけて、クライアントがインストールされていることを確認します。

ステップ 3 [Remove] をクリックして、クライアントをアンインストールします。



第 5 章

TLS の設定

TLS の概要

Transport Layer Security（TLS）はセキュア ポートと証明書交換を使用して、2 つのシステム間またはデバイス間でセキュアで信頼できるシグナリングとデータ転送を実現します。TLS は音声ドメインへのアクセスを防ぐために、ユニファイド コミュニケーション マネージャ 制御システム、デバイス およびプロセス間の接続を保護および制御します。

TLS の前提条件

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

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

- Cisco Unified Border Element（CUBE）
- Cisco Expressway
- Cisco TelePresence Conductor

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

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

TLS 設定タスク フロー

TLS 接続の Unified Communications Manager を構成するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	（任意）最小 TLS バージョンの設定 （123 ページ）。	デフォルトでは、Unified Communications Manager において、最小 TLS バージョンとして 1.0 がサポートされています。上位のバージョンの TLS がセキュリティ要件で求められる場合は、TLS 1.1 または 1.2 を使用するようにシステムを再設定します。
ステップ 2	（任意） TLS 暗号化の設定 （124 ページ）。	Unified Communications Manager でサポートされる TLS 暗号オプションを構成します。
ステップ 3	SIP トランクのセキュリティ プロファイルでの TLS の設定 （124 ページ）。	SIP トランクに TLS 接続を割り当てます。このプロファイルを使用するトランクでは、シグナリングのために TLS を使用します。また、セキュア トランクを使用することにより、会議ブリッジなどのデバイスに TLS 接続を追加することができます。
ステップ 4	SIP トランクへのセキュア プロファイルの追加 （125 ページ）。	トランクの TLS サポートを可能にするため、TLS 対応 SIP トランク セキュリ

	コマンドまたはアクション	目的
		ティ プロファイルを SIP トランクに割り当てます。また、セキュア トランクを使用することにより、会議ブリッジなどのリソースに接続することができます。
ステップ 5	電話セキュリティ プロファイルでの TLS の設定 （126 ページ）。	電話セキュリティ プロファイルに TLS 接続を割り当てます。このプロファイルを使用する電話では、シグナリングのために TLS を使用します。
ステップ 6	電話へのセキュア電話プロファイルの追加 （126 ページ）。	作成した TLS 対応プロファイルを電話に割り当てます。
ステップ 7	（任意）ユニバーサル デバイス テンプレートへのセキュア電話プロファイルの追加 （127 ページ）。	TLS対応の電話のセキュリティ プロファイルをユニバーサル デバイス テンプレートに割り当てます。LDAPディレクトリ同期がこのテンプレートで設定されている場合は、LDAP同期化を通じて電話のセキュリティをプロビジョニングできます。

最小 TLS バージョンの設定

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

始める前に

設定対象の TLS バージョンが、ネットワーク内のデバイスとアプリケーションでサポートされていることを確認します。詳細は、TLS の前提条件 （121 ページ）を参照してください。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

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

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

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

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

TLS 暗号化の設定

SIP インターフェイスの使用可能な最も強力な暗号化を選択することによって、弱い暗号化を無効にできます。TLS 接続を確立するために Unified Communications Manager でサポートされる暗号化を設定するには、この手順を使用します。

手順

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

ステップ 3 **[保存 (Save)]** をクリックします。

SIP トランクのセキュリティ プロファイルでの TLS の設定

SIP トランク セキュリティ プロファイルに TLS 接続を割り当てるには、次の手順を実行します。このプロファイルを使用するトランクでは、シグナリングのために TLS を使用します。

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）] > [セキュリティ（Security）] > [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして、新しい SIP トランク セキュリティ プロファイルを作成します。
- [検索（Find）] をクリックして検索し、既存のプロファイルを選択します。

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

ステップ 4 [デバイス セキュリティ モード（Device Security Mode）] フィールドの値を、[暗号化（Encrypted）] または [認証（Authenticated）] に設定します。

ステップ 5 [受信転送タイプ（Incoming Transport Type）] フィールドと [送信転送タイプ（Outgoing Transport Type）] フィールドの両方の値を、TLS に設定します。

ステップ 6 [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] ウィンドウの残りのフィールドにデータを入力します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ 7 **[保存 (Save)]** をクリックします。

SIP トランクへのセキュア プロファイルの追加

TLS 対応の SIP トランク セキュリティ プロファイルを SIP トランクに割り当てるには、次の手順を使用します。このトランクを使用することにより、会議ブリッジなどのリソースとのセキュア接続を作成できます。

始める前に

SIP トランクのセキュリティ プロファイルでの TLS の設定 （124 ページ）

手順

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

ステップ 2 [検索（Find）] をクリックして検索し、既存のトランクを選択します。

ステップ 3 [デバイス名（Device Name）] フィールドに、トランクのデバイス名を入力します。

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

ステップ 5 [SIP プロファイル（SIP Profile）] ドロップダウン リストで、SIP プロファイルを選択します。

ステップ 6 [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] ドロップダウン リスト ボックスから、前のタスクで作成した TLS 対応の SIP トランク プロファイルを選択します。

ステップ 7 [宛先（Destination）] 領域に、宛先 IP アドレスを入力します。最大 16 の宛先アドレスを入力できます。追加の宛先を入力するには、[+] ボタンをクリックします。

ステップ 8 [トランクの設定（Trunk Configuration）] ウィンドウのその他のフィールドを設定します。フィールドとその設定のヘルプについては、オンライン ヘルプを参照してください。

ステップ 9 **[保存（Save）]** をクリックします。

（注） トランクをセキュア デバイスに接続する場合、Unified Communications Manager にセキュア デバイスの証明書をアップロードする必要があります。証明書の詳細については、「証明書 （19 ページ）」の項を参照してください。

次のタスク

電話セキュリティ プロファイルでの TLS の設定 （126 ページ）。

電話セキュリティ プロファイルでの TLS の設定

電話セキュリティ プロファイルに TLS 接続を割り当てるには、次の手順を実行します。このプロファイルを使用する電話では、シグナリングのために TLS を使用します。

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）] > [セキュリティ（Security）] > [電話セキュリティ プロファイル（Phone Security Profile）]** の順に選択します。

ステップ 2 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして新しいプロファイルを作成します。
- [検索（Find）] をクリックして検索し、既存のプロファイルを選択します。

ステップ 3 新しいプロファイルを作成する場合は、電話モデルとプロトコルを選択し、[次へ（Next）] をクリックします。

（注） ユニバーサル デバイス テンプレートと LDAP 同期を使用して LDAP 同期を通じてセキュリティをプロビジョニングする場合は、[電話セキュリティ プロファイル タイプ（Phone Security Profile Type）] に [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 4 プロファイル名を入力します

ステップ 5 [デバイス セキュリティ モード（Device Security Mode）] ドロップダウン リスト ボックスで、[暗号化（Encrypted）] または [認証（Authenticated）] を選択します。

ステップ 6 （SIP 電話のみ）転送タイプには、TLS を選択します。

ステップ 7 [電話セキュリティ プロファイルの設定（Phone Security Profile Configuration）] ウィンドウの残りのフィールドを入力します。フィールドとその設定のヘルプについては、オンライン ヘルプを参照してください。

ステップ 8 **[保存 (Save)]** をクリックします。

電話へのセキュア電話プロファイルの追加

TLS 対応の電話セキュリティ プロファイルを電話に割り当てるには、次の手順を使用します。

（注） 一度に多数の電話にセキュア プロファイルを割り当てるには、一括管理ツールを使用することにより、それらのセキュリティ プロファイルの再割り当てを行います。

手順

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

ステップ 2 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして新しい電話機を作成します。
- [検索（Find）] をクリックして検索し、既存の電話機を選択します。

ステップ 3 電話の種類とプロトコルを選択し、[次（Next）] をクリックします。

ステップ 4 [デバイス セキュリティ プロファイル（Device Security Profile）] ドロップダウン リストから、作成したセキュア プロファイルを電話に割り当てます。

ステップ 5 次の必須フィールドに値を割り当てます。

- MAC アドレス
- [デバイスプール（Device Pool）]
- [SIPプロファイル（SIP Profile）]
- [オーナーのユーザID（Owner User ID）]
- 電話ボタンテンプレート（Phone Button Template）

ステップ 6 [電話の設定（Phone Configuration）] ウィンドウの残りのフィールドを入力します。フィールドとその設定のヘルプについては、オンライン ヘルプを参照してください。

ステップ 7 **[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 テンプレートへのセキュア電話プロファイルの追加 （127 ページ）

ユニバーサル デバイス テンプレートへのセキュア電話プロファイルの追加

TLS 対応の電話セキュリティ プロファイルをユニバーサル デバイス テンプレートに割り当てるには、次の手順を使用します。LDAP ディレクトリ同期が設定されている場合は、機能グループ テンプレートとユーザ プロファイルにより LDAP 同期にこのユニバーサル デバイス テンプレートを含めることができます。同期処理が発生すると、電話に対してセキュア プロファイルがプロビジョニングされます。

手順

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

ステップ 2 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして新しいテンプレートを作成します。
- [検索（Find）] をクリックして検索し、既存のテンプレートを選択します。

ステップ 3 [名前（Name）] フィールドに、テンプレートの名前を入力します。

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

ステップ 5 [デバイス セキュリティ プロファイル（Device Security Profile）] ドロップダウン リスト ボックスから、作成した TLS 対応セキュリティ プロファイルを選択します。

（注） [ユニバーサル デバイス テンプレート（Universal Device Template）] をデバイス タイプとする電話セキュリティ プロファイルが作成されていなければなりません。

ステップ 6 [SIP プロファイル（SIP Profile）] を選択します。

ステップ 7 [電話ボタン テンプレート（Phone Button Template）] を選択します。

ステップ 8 [ユニバーサル デバイス テンプレートの設定（Universal Device Template Configuration）] ウィンドウの残りのフィールドに入力します。フィールドとその設定のヘルプについては、オンライン ヘルプを参照してください。

ステップ 9 **[保存（Save）]** をクリックします。

次のタスク

LDAPディレクトリ同期処理に、ユニバーサルデバイステンプレートを含めます。LDAPディレクトリ同期の設定方法については、『*Cisco Unified Communications Manager* システム構成ガイド』の「「エンドユーザの構成」」の部分を参照してください。

TLS の連携動作と制約事項

TLS の相互作用

機能	データのやり取り
コモン クライテリア モード	コモン クライテリア モードは、最低限の TLS バージョンの設定と共に有効にすることができます。そのようにする場合、アプリケーションは、引き続きコモン クライテリアの要件に準拠し、アプリケーション レベルで TLS 1.0 セキュア接続を無効にすることになります。コモン クライテリア モードが有効な場合、アプリケーションで最低限の TLS バージョンを 1.1 または 1.2 のいずれかとして設定することができます。コモン クライテリア モードの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の中のコモン クライテリアへの準拠のトピックを参照してください。

TLS の制限

79xx、69xx、89xx、99xx、39xx、IP Communicator など、従来型の電話に Transport Layer Security（TLS）バージョン 1.2 を実装する際に発生する可能性のある問題を、次の表に示します。使用している電話で、このリリースのセキュア モードがサポートされているかどうかを確認するには、Cisco Unified Reporting の Phone Feature List Report を参照してください。従来型の電話の機能制限 および機能を実装するための回避策の一覧を、次の表に示します。

（注） 回避策は、影響を受ける機能が、実際のシステムで動作するように設計されています。しかし、その機能の TLS 1.2 コンプライアンスについては保証できません。

表 *16 : Transport Layer Security*（*TLS*）バージョン *1.2* の制約事項

機能	制限事項
暗号化モードの従来型の電話	暗号化モードの従来型の電話は動作しません。回避策はありません。
認証モードの従来型の電話	認証モードの従来型の電話は動作しません。回避策はありません。

機能	制限事項
HTTPS に基づくセキュア URL を使用する IP 電話サービス。	HTTPS に基づくセキュア URL を使用する IP 電話サービスは動作しません。 IP 電話サービスを使用するための回避策：基盤になっているすべてのサービス オプションに HTTP を使用します。たとえば、社内ディレクトリと個人用ディレクトリ。しかし、エクステンション モビリティなどの機能で、機密データを入力することが必要な場合、HTTP では安全ではないため、HTTP はお勧めしません。HTTP 使用には、次の欠点があります。 • 従来型の電話に HTTP、サポート対象の電話に HTTPS を設定する場合のプロビジョニングに関する課題。 • IP 電話サービスの復元力の欠如。 • IP 電話サービスを処理するサーバのパフォーマンスが低下する可能性。
従来型の電話でのエクステンションモビリティ クロス クラスタ（EMCC）	EMCC は、従来型の電話の TLS 1.2 でサポートされていません。 回避策：EMCC を有効にするため、次の作業を実行します。 1. HTTPS ではなく HTTP により EMCC を有効にします。 2. ユニファイド コミュニケーション マネージャ の全クラスタで混合モードをオンにします。 3. ユニファイド コミュニケーション マネージャ の全クラスタで同じ USB eToken を使用します。

機能	制限事項
従来型の電話でのローカルで有効な証明書（LSC）	LSC は、従来型の電話の TLS 1.2 でサポートされていません。結果として、LSC に基づく 802.1x および電話 VPN 認証はご利用いただけません。 802.1x のための回避策：古い電話では、MIC または EAP-MD5 によるパスワードに基づく認証。ただし、これらは推奨されません。 VPN のための回避策：エンドユーザのユーザ名とパスワードに基づく電話 VPN 認証を使用。
暗号化 Trivial File Transfer Protocol（TFTP）構成ファイル	暗号化 Trivial File Transfer Protocol（TFTP）構成ファイルは、メーカーのインストールした証明書（MIC）がある場合でも、従来型の電話の TLS 1.2 でサポートされません。 回避策はありません。
CallManager 証明書を更新すると、従来型の電話は信頼を失う	従来型の電話は、CallManager 証明書が更新された時点で信頼を失います。たとえば、証明書更新後、電話は新しい構成を取得できなくなります。これは、ユニファイドコミュニケーションマネージャ 11.5.1 だけで適用されます。 回避策：従来型の電話が信頼を失わないようにするため、次の手順を実行します。 **1.** CallManager 証明書を有効にする前に、[8.0 より前のリリースへロールバックするクラスタ（Cluster For Roll Back to Pre 8.0）] エンタープライズ パラメータを True に設定します。デフォルトでは、この設定により、セキュリティが無効になります。 **2.** 一時的に TLS 1.0 を許可します（ユニファイド コミュニケーション マネージャを複数回リブート）。

機能	制限事項
サポートされていないバージョンの Cisco ユニファイドコミュニケーションマネージャへの接続	上位の TLS バージョンをサポートしていない古いバージョンのユニファイドコミュニケーション マネージャ への TLS 1.2 接続は動作しません。たとえば、ユニファイドコミュニケーション マネージャリリース 9.x との TLS 1.2 SIP トランク接続は、そのリリースが TLS 1.2 をサポートしないため、動作しません。 次の回避策のいずれかを使用できます。 • 接続を有効にするための回避策：非セキュア トランクを使用。ただし、推奨されるオプションではありません。 • TLS 1.2 を使用しつつ接続を有効にするための回避策：TLS 1.2 をサポートしてていないバージョンから、サポートするリリースにアップグレードします。
Certificate Trust List（CTL）クライアント	CTL クライアントでは、TLS 1.2 がサポートされません。 次の回避策のいずれかを使用できます。 • CTL クライアントを使用する際に一時的に TLS 1.0 を許可し、クラスタをコモンクライテリア モードに移します。最小 TLS を 1.1 または 1.2 に設定します • コモン クライテリア モードで CLI コマンド **utils ctl set-cluster mixed-mode** を使用することにより、Tokenless CTL に移行します。最小 TLS を 1.1 または 1.2 に設定します
Address Book Synchronizer	回避策はありません。

Cisco ユニファイド コミュニケーション マネージャIM およびプレゼンスサービス のポートのうち Transport Layer Security Version 1.2 によって影響を受けるもの

ユニファイド コミュニケーション マネージャのポートのうち、TLS バージョン 1.2 によって影響を受けるものの一覧を、次の表に示します

表 *17 : Cisco* ユニファイド コミュニケーション マネージャ のポートのうち *Transport Layer Security Version 1.2* によって影響を受けるもの

Application	プロトコル	宛先/リスナー	通常モードで動作する Cisco ユニファイド コミュニケーション マネージャ			コモン クライテリア モードで動作する Cisco ユニファイド コミュニケーション マネージャ		
			最低 TLS バージョン 1.0	最低 TLS バージョン 1.1	最低 TLS バージョン 1.2	最低 TLS バージョン 1.0	最低 TLS バージョン 1.1	最低 TLS バージョン 1.2
Tomcat	HTTPS	443	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS v1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
SCCP-秒-SIG	Signalling Connection Control Part（SCCP）	2443	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
CTL-SERV	専用	2444	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
コンピュータテレフォニー インテグレーション（CTI）[こんぴゅーたてれふぉにーいんてぐれーしょん CTI]	Quick Buffer Encoding（QBE）[[illegible] QBE]	2749	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
CAPF-SERV	Transmission Control Protocol（TCP）	3804	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2

Application	プロトコル	宛先/リスナー	通常モードで動作する Cisco ユニファイド コミュニケーション マネージャ			コモン クライテリア モードで動作する Cisco ユニファイド コミュニケーション マネージャ		
			最低 TLS バージョン 1.0	最低 TLS バージョン 1.1	最低 TLS バージョン 1.2	最低 TLS バージョン 1.0	最低 TLS バージョン 1.1	最低 TLS バージョン 1.2
クラスタ間検索サービス（ILS）	N/A	7501	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
Administrative XML（AXL）	Simple Object Access Protocol（SOAP）	8443	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
高可用性プロキシ（HAProxy）	TCP	9443	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.2	TLS 1.2
SIP-SIG	Session Initiation Protocol（SIP）	5061（トランクで設定可能）	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
HA Proxy	[TCP]	6971、6972	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
Cisco Tomcat	HTTPS	8080、8443	8443：TLS 1.0、TLS 1.1、TLS 1.2	8443：TLS 1.1、TLS 1.2	8443：TLS 1.2	TLS 1.1	8443：TLS 1.1、TLS 1.2	8443：TLS 1.2
信頼検証サービス（TVS）	専用	2445	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2

インスタント メッセージングと Presence のポートのうち Transport Layer Security バージョン 1.2 による影響を受けるもの

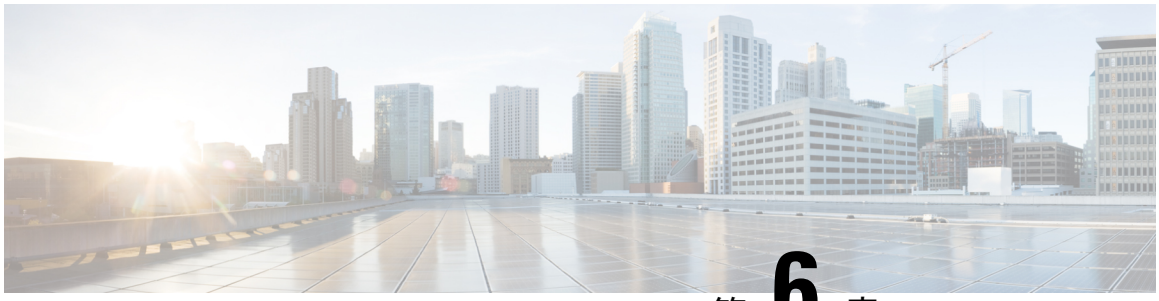
インスタント メッセージングと Presence のポートのうち、Transport Layer Security バージョン 1.2 による影響を受けるものの一覧を、次の表に示します。

表 *18* : インスタント メッセージングと *Presence* のポートのうち *Transport Layer Security* バージョン *1.2* による影響を受けるもの

宛先/リスナー	通常モードで動作するインスタント メッセージングと **Presence**			コモンクライテリア モードで動作するインスタント メッセージングと **Presence**		
	最低 **TLS** バージョン **1.0**	最低 **TLS** バージョン **1.1**	最低 **TLS** バージョン **1.2**	最低 **TLS** バージョン **1.0**	最低 **TLS** バージョン **1.1**	最低 **TLS** バージョン **1.2**
443	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
5061	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
5062	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
7335	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
8083	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
8443	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2

第 II 部

証明書



第 6 章

証明書概要

証明書の概要

証明書とは、証明書保持者名、公開キー、および証明書を発行する認証局のデジタル署名を含むファイルです。証明書は、証明書の所有者の身元を証明します。

ユニファイドコミュニケーションマネージャーは、公開キー基盤 (PKI) を使用する証明書を使用して、サーバとクライアントのアイデンティティを検証し、暗号化を有効化します。別のシステム (たとえば、電話機や media server) がユニファイドコミュニケーションマネージャーに接続しようとすると、そのシステム自身の身元を確認するために、その証明書がユニファイドコミュニケーションマネージャーに提示されます。適切なトラストストアに一致する証明書がある場合を除き、ユニファイドコミュニケーションマネージャーは他のシステムを信頼せず、アクセスが拒否されます。

ユニファイドコミュニケーションマネージャーは、次の2つの広範なクラスの証明書を使用します。

- 自己署名付き証明書: デフォルトでは、ユニファイドコミュニケーションマネージャーは自己署名付き証明書を使用します。これらは、サーバまたはクライアントの身元を確認するために、ユニファイドコミュニケーションマネージャーが証明書に署名する証明書です。ユニファイドコミュニケーションマネージャーは、自身の自己署名証明書を発行することも、または認証局のプロキシ機能を使用して、電話機の代理証明書を発行することもできます。
- CA 署名付き証明書: サードパーティ認証局 (CA) によって署名された証明書を使用するようにユニファイドコミュニケーションマネージャーを設定することもできます。認証署名要求 (CSR) は、ユニファイドコミュニケーションに代わって CA が証明書に署名するようにする必要があります。CA は要求を受信し、CA 署名された証明書を発行します。CA 署名付きの証明書を使用するには、最初に、ユニファイドコミュニケーションマネージャーに CA ルート証明書チェーンをインストールする必要があります。

（注） 通常、自己署名付き証明書は、社内のファイアウォールを通過しない内部接続に対して受け入れられます。ただし、WAN 接続の場合、またはパブリックインターネットを使用する接続の場合は、CA 署名付き証明書を使用する必要があります。

（注） X.509 の一般的な時間値。PKI 証明書は、グリニッジ標準時 (GMT) で表記されている**必要**があり、秒 (YYYYMMDDHHMMSSZ) を含める必要があります。秒の端数は許可されていません。このルールに違反する証明書は、ピアエンティティから提供されているか、またはトラストストアに読み込まれているかに関係なく、証明書の検証プロセスを失敗させる可能性があります。

CTL ファイル

Cisco Certificate Trust List は、Cisco CTL クライアントで混合モードを有効にするか、またはユーティリティ ctl CLI コマンドの 1 つを実行することによって作成されるファイルです (たとえば、ユーティリティ ctl update CTLFile)。混在モードが有効になっている場合、CTL ファイルは、TFTP サーバを経由して Cisco IP Phone にインストールされます。CTL ファイルには、認証局プロキシ機能のシステム証明書やその他の証明書など、信頼できる電話機の証明書のリストが含まれています。

CTL ファイルの設定方法の詳細については、「CTL Client セットアップ」の章を参照してください。

TLS

トランスポート回線シグナリング (TLS) は CA 署名された証明書を使用します。TLS が設定されている場合、もう一方のシステムは、最初の connection セットアップの一部として、その証明書をユニファイドコミュニケーションマネージャーに提示します。他のシステムの証明書がインストールされている場合は、他のシステムを信頼し、通信が行われます。他のシステムの証明書が存在しない場合、もう一方のシステムは信頼されず、通信は失敗します。

サードパーティー CA 署名付き証明書

デフォルトでは、ユニファイドコミュニケーションマネージャーはすべての接続に自己署名入りの証明書を使用します。ただし、証明書に署名するようにサードパーティ CA を設定することによって、セキュリティを追加できます。サードパーティ CA を使用するには、Cisco 統一 OS の管理に CA ルート証明書チェーンをインストールする必要があります。

一般に、自己署名付き証明書を使用した証明書をアップロード、ダウンロード、および表示するための同じタスクを使用できます。ただし、CA で署名された証明書を発行するには、CA が証明書を発行して署名できるように証明書署名要求 (CSR) を提出する必要があります。

設定

別のシステムで、ユニファイドコミュニケーションマネージャーに接続されている CA 署名済みの証明書を使用する場合は、Cisco 統一 OS の管理で次の手順を実行してください。

- 証明書を署名した CA のルート証明書をアップロードします。
- 他のシステムから CA 署名付き証明書をアップロードします。

ユニファイドコミュニケーションマネージャーの CA 署名証明書を使用する場合は、次のようにします。

- Cisco 統一 OS の管理では、CSR が、ユニファイドコミュニケーションマネージャーの CA 署名証明書を要求するようにします。
- Cisco 統一 OS 管理では、CA ルート証明書チェーンと CA 署名証明書の両方をダウンロードします。
- もう一方のシステムで、CA ルート証明書チェーンと CA 署名証明書の両方をアップロードします。

CA のルート証明書の取得と設定の方法の詳細については、証明機関のマニュアルを参照してください。

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 *19 : 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		Y	
ipsec	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 *20 : 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		

サーバ証明書のタイプ

Unified Communications Manager サーバでは次の自己署名（所有）証明書タイプが使用されます。

- HTTPS 証明書（Tomcat）:自己署名ルート証明書は、HTTPS サーバの Unified Communications Manager インストール時に生成されます。Cisco Unity Connection は、SMTP および IMAP サービスにこの証明書を使用します。
- CallManager 証明書：自己署名ルート証明書は Unified Communications Manager サーバに Unified Communications Manager をインストールするときに、自動的にインストールされます。
- CAPF 証明書：Cisco CTL クライアント設定を完了すると、Unified Communications Manager のインストール時に生成されるこのルート証明書が、ご使用のサーバまたはクラスタ内のすべてのサーバにコピーされます。
- IPSec 証明書（ipsec_cert）：自己署名ルート証明書は、Unified Communications Manager のインストール時に、MGCP および H.323 ゲートウェイとの IPSec 接続用に生成されます。
- SRST 対応ゲートウェイの証明書：[Unified Communications Manager Administration] でのセキュアな SRST リファレンスの設定時に、Unified Communications Manager は SRST 対応ゲートウェイの証明書をゲートウェイから取得し Unified Communications Manager データベースに保存します。デバイスをリセットすると、証明書は電話の設定ファイルに追加されます。証明書はデータベースに格納されているため、証明書の管理ツールでこの証明書を管理することはできません。
- TVS 証明書：信頼検証サービス（TVS）をサポートする自己署名証明書です。

- Phone-SAST-trust 証明書：このカテゴリでは、システムが Cisco Unified IP Phone の VPN 証明書をインポートできます。これらの証明書は Midlet 信頼ストアに保存されます。
- 電話証明書信頼ストア（Phone-trust）：Unified Communications Manager はこの証明書タイプを使用して電話での HTTPS アクセスをサポートします。Cisco Unified Communications Operating System GUI を使用して証明書を Phone-trust ストアにアップロードできます。Cisco Unified IP Phone からの安全な Web アクセス（HTTPS）をサポートするため、Phone-CTL-trust にある証明書は CTL ファイルのメカニズムによって電話にダウンロードされます。電話の信頼証明書はサーバに残り、電話は TVS 経由でリクエスト可能です。

Unified Communications Manager は次のタイプの証明書を CallManager 信頼ストアにインポートします。

- Cisco Unity サーバまたは Cisco Unity Connection 証明書：Cisco Unity および Cisco Unity Connection はこの自己署名ルート証明書を使用して Cisco Unity SCCP および Cisco Unity Connection SCCP のデバイス証明書に署名します。Cisco Unity では、Cisco Unity Telephony Integration Manager（UTIM）がこの証明書を管理します。Cisco Unity Connection では、Cisco Unity Connection Administration がこの証明書を管理します。
- Cisco Unity および Cisco Unity Connection SCCP デバイス証明書：Cisco Unity および Cisco Unity Connection SCCP デバイスはこの署名付き証明書を使用して Unified Communications Manager との TLS 接続を確立します。
- 証明書の名前はボイス メール サーバ名に基づく証明書のサブジェクト名のハッシュを表しています。すべてのデバイス（またはポート）が、ルート証明書をルートとする証明書を発行します。
- SIP プロキシ サーバの証明書：CallManager 信頼ストアに SIP ユーザ エージェントの証明書が含まれ、SIP ユーザ エージェントの信頼ストアに Cisco Unified Communications Manager 証明書が含まれる場合、SIP トランク経由で接続する SIP ユーザ エージェントは Unified Communications Manager に対して認証されます。

次の信頼ストアがあります。

- Tomcat および Web アプリケーション用の共通信頼ストア
- IPSec-trust
- CAPF-trust
- Userlicensing-trust
- TVS-trust
- Phone-SAST-trust
- Phone-CTL-trust

証明書の管理タスク

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（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 [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、[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 [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 （147 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 *21 :* 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

名前	説明	関連サービス
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 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 ノードを含み、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。

CTL ファイルの更新

この手順を使用して、CLI コマンドを使用してCTLファイルを更新します。混合モードが有効になっている場合は、新しい証明書をアップロードするたびに CTL ファイルを更新する必要があります。

（注） また、Cisco CTL クライアントを経由して CTL ファイルを更新することもできます。

手順

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

ステップ 2 `utils ctl update CTLfile` コマンドを実行します。CTL ファイルを再生すると、ファイルが TFTP サーバにアップロードされて、電話機に自動的に送信されます。

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。

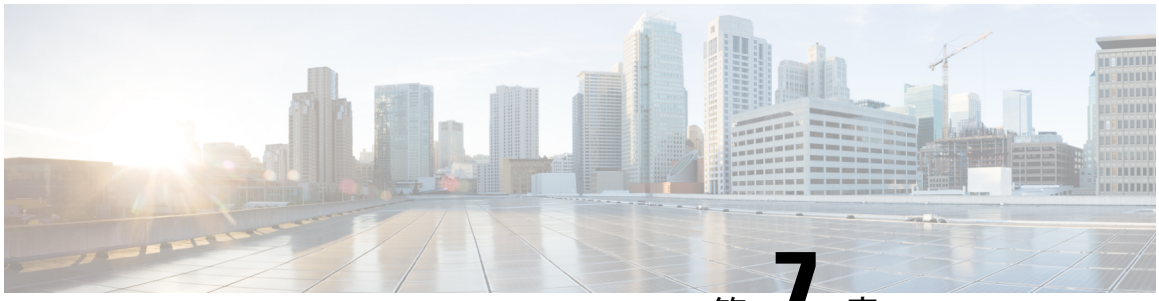
ステップ 2 証明書を選択して情報を表示します。証明書の内容が、リモート ノード上の対応する証明書の内容と一致することを確認します。

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 7 章

Certificate Authority Proxy Function

認証局プロキシ機能（CAPF）の概要

Cisco Certificate Authority Proxy Function (CAPF) は、ローカルの重要な証明書 (LSCs) を発行し、Cisco エンドポイントを認証する Cisco 専有サービスです。CAPF サービスは、ユニファイドコミュニケーションマネージャー上で実行され、次のタスクを実行します。

- サポートされる Cisco Unified IP Phone に対して LSC を発行する。
- 混合モードが有効になっている場合に、電話機を認証します。
- 電話機用の既存の LSCs をアップグレードします。
- 表示およびトラブルシューティングを行うために電話の証明書を取得する。

CAPF 実行モード

次のモードで動作するように CAPF を設定することができます。

- Cisco Authority プロキシ機能: ユニファイドコミュニケーションマネージャーの CAPF サービスは、CAPF サービス自体によって署名された LSCs を発行します。これは、デフォルトのモードです。
- [オンライン CA (Online CA)]: 外部オンライン CA が「電話用 LSC」として署名している場合は、このオプションを使用します。CAPF サービスは、自動的に外部 CA に接続されます。CSR が送信された場合、CA は署名して CA 署名した LSC を自動的に返します。
- オフライン CA: このオプションは、オフラインの外部 CA を使用して LSC for phone に署名する場合に使用します。このオプションでは、LSC を手動でダウンロードして CA に提

出してから、CA 署名の証明書の準備ができてからそれらをアップロードする必要があります。

（注） シスコでは、サードパーティ CA を使用して LSC に署名する必要がある場合、**オフライン** ca の代わりにオンライン ca オプションを使用して、プロセスが自動化されていて、問題が発生する可能性が低くなることを推奨します。

CAPF サービス証明書

統合コミュニケーションマネージャがインストールされている場合、CAPF サービスが自動的にインストールされ、CAPF 固有のシステム証明書が生成されます。セキュリティが適用されると、Cisco CTL クライアントは、すべてのクラスタノードに証明書をコピーします。

電話の証明書タイプ

シスコは次の X.509v3 証明書タイプを電話で使用します。

- ローカルで有効な証明書（LSC）：このタイプの証明書は Cisco Certificate Authority Proxy Function（CAPF）に関連する必要な作業の実行後に、電話にインストールされます。デバイス セキュリティ モードを認証または暗号化に設定した後で、LSC は Unified Communications Manager と電話の間の接続を保護します。

（注） オンライン CA の場合、LSC の有効性は CA に基づいています。また、CA が許可している限り使用できます。

- 製造元でインストールされる証明書（MIC）：Cisco Manufacturing は MIC をサポートされている電話モデルに自動的にインストールします。製造元でインストールされる証明書は LSC インストールの Cisco Certificate Authority Proxy Function（CAPF）を認証します。製造元でインストールされる証明書を上書きしたり、削除することはできません。

（注） 製造元でインストールされる証明書（MIC）を LSC のインストールでのみ使用することが推奨されます。シスコでは Unified Communications Manager との TLS 接続の認証のために LSC をサポートしています。MIC ルート証明書は侵害される可能性があるため、TLS 認証またはその他の目的に MIC を使用するように電話を設定するお客様は、ご自身の責任で行ってください。MIC が侵害された場合シスコはその責任を負いません。

CAPF 経由の LSC 生成

CAPF を設定し、設定されている認証文字列を電話機に追加すると、電話機と CAPF 間でキーと証明書の交換が行われます。以下が実行されます。

- 電話機は、設定された認証方法を使用して CAPF に対して自身を認証します。
- 電話機は公開/秘密キー ペアを生成します。
- 電話機は、署名されたメッセージの中で、公開キーを CAPF に転送します。
- 秘密キーは電話に残り、外部に公開されることはありません。
- 証明書はCAPFによって署名され、署名付きメッセージによって電話に送り返されます。

（注） 電話のユーザが証明書操作の中断や、電話の動作ステータスの確認を実行できることに注意してください。

（注） キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。証明書生成中にも電話は正常に機能しますが、TLS トラフィックが増加することで、電話での通話の処理に最小限の中断が発生する可能性があります。たとえば、インストールの最後に証明書がフラッシュへ書き込まれるとき、オーディオにノイズが発生する場合があります。

CAPF 前提条件

LSC 生成用の認証局のプロキシ機能を設定する前に、次の手順を実行します。

- サードパーティ CA を使用して LSCs に署名したい場合は、CA を外部に設定します。
- 電話機を認証する方法を計画します。
- LSCs を生成する前に、次のものを用意していることを確認してください。
  - Unified Communications Manager リリース 12.5 以降
  - 証明書に CAPF を使用するエンドポイント (Cisco IP Phone および Jabber を含む)。
  - Microsoft Windows Server 2012 および 2016
  - ドメイン名サービス（DNS）が設定されています
- 「CA ルートおよび HTTPS 証明書」をアップロードしてから、LSCs を生成する必要があります。セキュア SIP connection では、HTTPS 証明書は CAPF-トラストを通過し、CA ルート証明書は CAPF 信頼でコールマネージャーの信頼をたどります。インターネットイン

フォメーションサービス (IIS) は、HTTPS 証明書をホストします。CA ルート証明書は、証明書署名要求 (CSR) への署名に使用されます。

証明書をアップロードする必要がある場合のシナリオを次に示します。

表 *22:* 証明書のアップロードシナリオ

シナリオ	結果
CA ルートおよび HTTPS 証明書は同じです。	CA ルート証明書をアップロードする。
CA ルートと HTTPS の証明書は異なり、HTTPS 証明書は同じ CA ルート証明書によって発行されます。	CA ルート証明書をアップロードする。
中間 CA と HTTPS の証明書は異なり、CA ルート証明書によって発行されます。	CA ルート証明書をアップロードする。
CA ルートと HTTPS の証明書は異なり、同じ CA ルート証明書によって発行されます。	CA ルートおよび HTTPS 証明書をアップロードする。

（注） 複数の証明書を同時に生成するとコール処理中断の原因となるため、スケジュールされたメンテナンスの時間帯に CAPF を使用することを強く推奨します。

CAPF 設定タスク フロー

次のタスクを実行して、証明機関プロキシ機能 (CAPF) サービスがエンドポイント用 LSCs を発行するように設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	サードパーティの認証局のルート証明書のアップロード	LSC にサードパーティの CA 署名を適用する場合は、CA ルート証明書チェーンを CAPF 信頼ストアにアップロードします。その他の場合は、このタスクをスキップします。
ステップ 2	認証局（CA）ルート証明書のアップロード （158 ページ）	CA ルート証明書をコールマネージャー トラストストアにアップロードします。

	コマンドまたはアクション	目的
ステップ 3	オンライン認証局の設定 （159 ページ）	を使用して電話機 LSC 証明書を生成するには、次の手順を使用します。
ステップ 4	オフライン認証局の設定の設定	オフライン CA を使用して電話機 LSC 証明書を生成するには、次の手順を使用します。
ステップ 5	CAPF サービスをアクティブ化または再起動する	認証局のプロキシ機能のシステム設定を構成した後、必須の CAPF サービスがアクティブになっていることを確認します。
ステップ 6	次のいずれかの手順を使用して、ユニファイドコミュニケーションマネージャーの CAPF 設定を構成します。 • CAPD 設定をユニバーサル デバイス テンプレートで設定します。 （161 ページ） • バルク Admin による CAPF 設定の更新 （163 ページ） • 電話機の CAPF 設定の設定 （164 ページ）	次のオプションのいずれかを使用して、CAPF 設定を電話機の設定に追加します。 • まだ LDAP ディレクトリを同期していない場合、CAPF 設定をユニバーサルデバイステンプレートに追加し、初期 LDAP 同期を使用して設定を適用することができます。 • バルク管理ツールを使用すると、1 回の操作で多数の電話機に CAPF 設定を適用できます。 • CAPF 設定を電話機ごとに適用することができます。
ステップ 7	キープアライブ タイマーの設定 （165 ページ）	(ファイアウォールがタイムアウトしないように、CAPF エンドポイント接続のキープアライブ値を設定します。デフォルト値は 15 分です。

サードパーティの認証局のルート証明書のアップロード

外部 CA を使用して LSC 証明書に署名する場合は、CA ルート証明書を **CAPF 信頼**ストアおよび **callmanager 信頼**ストアにアップロードする必要があります。

（注） サードパーティ CA を使用して LSCs に署名しない場合は、このタスクをスキップできます。

手順

ステップ 1 [Cisco Unified 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 [Upload Certificate/Certificate chain] をクリックします。

ステップ 3 **[証明書目的（Certificate Purpose）]** ドロップダウンリストで、**[CallManager 信頼（CallManager-trust）]** を選択します。

ステップ 4 証明書の説明を [説明（Description）] に入力します。たとえば、**外部 LSC 署名 CA の証明書などです。**

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

ステップ 6 [アップロード（Upload）] をクリックします。

ステップ 7 このタスクを繰り返して、証明**書の目的で**使用**される発信者管理者の信頼に証明書をアップロードします。**

認証局（CA）ルート証明書のアップロード

クラスタ全体の証明書をアップロードし、クラスタ内のすべてのサーバに配布します。

手順

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

ステップ 2 [Upload Certificate/Certificate chain] をクリックします。

ステップ 3 **[証明書目的（Certificate Purpose）]** ドロップダウンリストで、**[CallManager 信頼（CallManager-trust）]** を選択します。

ステップ 4 **[説明（Description）]** フィールドに、証明書の説明を入力します。たとえば、**外部 LSC 署名 CA の証明書などです。**

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

ステップ 6 [アップロード（Upload）] をクリックします。

次のタスク

オンライン認証局の設定 （159 ページ）

オンライン認証局の設定

Unified Communications Manager でこの手順を実行して、オンライン認証局プロキシ機能を使用して電話機 LSC を生成します。

（注） オンライン CAPF は FIPS 対応モードではサポートされていません。

手順

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

ステップ 2 [**サーバ（Server**）] ドロップダウンリストから、Cisco CallManager サービスをアクティブ化したノードを選択します。

ステップ 3 [**サービス（Service**）] ドロップダウンリストから、[**Cisco 認証局プロキシ機能（アクティブ）（Cisco Certificate Authority Proxy Function (Active)**）] を選択します。サービス名の横に「Active」と表示されることを確認します。

ステップ 4 [**エンドポイントへの証明書発行者（Certificate Issuer to Endpoint**）] ドロップダウンリストから、[**オンラインCA（Online CA**）] を選択します。CA 署名付き証明書では、オンライン CA を使用することを推奨しています。

ステップ 5 [**証明書の有効期間（日数）（Duration Of Certificate Validity (in Days)**）] フィールドに、CAPF が発行した証明書が有効である日数を表す数値を、1 ～ 1825 の間で指定します。

ステップ 6 [**オンライン CA パラメータ（Online CA Parameters**）] 画面で次のパラメータを設定し、オンライン CA セクションに対する接続を作成します。

- オンライン CA ホスト名：サブジェクト名または共通名（CN）は、HTTPS 証明書の完全修飾ドメイン名（FQDN）と同じである必要があります。

  （注） 設定されているホスト名は、Microsoft CA で実行されているインターネット インフォメーション サービス（IIS）でホストされる HTTPS 証明書の共通名（CN）と同じです。

- オンライン CA ポート：オンライン CA のポート番号を入力します。たとえば「443」と入力します。
- オンラインCAテンプレート：テンプレートの名前を入力します。テンプレートはMicrosoft CA に作成されます。
- オンライン CA タイプ：デフォルトのタイプである Microsoft CA を選択します。
- オンライン CA ユーザ名：CA サーバのユーザ名を入力します。
- オンライン CA パスワード：CA サーバのユーザ名のパスワードを入力します。

残りの Cisco Certificate Authority Proxy Function サービスパラメータを入力します。必要に応じてパラメータをクリックすると

サービスパラメータのヘルプ システムを表示できます

ステップ 7 残りの Cisco Certificate Authority Proxy Function サービスパラメータを入力します。サービスパラメータのヘルプ システムを表示する必要がある場合は、パラメータ名をクリックします。

ステップ 8 **[保存（Save）]** をクリックします。

ステップ 9 変更内容を有効にするには、**Cisco Certificate Authority Proxy Function** サービスを再起動します。Cisco Certificate Enrollment service を自動的に再起動します。

次のタスク

CAPF サービスをアクティブ化または再起動する （161 ページ）

オフライン認証局の設定の設定

オフライン CA を使用して電話機 LSC 証明書を生成することを決定した場合は、次の高度なプロセスに従うことができます。

（注） オフライン CA オプションを使用すると、オンライン Ca よりも時間がかかり、手動による手順が多くなります。証明書の生成および送信プロセス中に問題 (たとえば、ネットワークの停止や電話機のリセットなど) が発生した場合は、プロセスを再起動する必要があります。

手順

ステップ 1 サードパーティ認証局からルート証明書チェーンをダウンロードします。

ステップ 2 Cisco Unified Communication Manager にルート証明書チェーンをインストールします。

ステップ 3 オフライン CA に対して **Certificate Issue to Endpoint**サービスパラメータを設定することで、オフラインの CA を使用するように Cisco Unified Communications Manager を設定します。

ステップ 4 お使いの電話機の LSC 用に **CSR** を生成します。

ステップ 5 認証局に**CSR** を送信します。

ステップ 6 **CSR** から署名付き証明書を取得します。

次のタスク

オフライン CA を使用して電話 lscs を生成する方法の詳細な例については、リンク https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/118779-configure-cucm-00.htmlを参照してください。

CAPF サービスをアクティブ化または再起動する

認証局のプロキシ機能のシステム設定を構成した後、必須の CAPF サービスがアクティブになっていることを確認します。Certificate Authority Proxy Function サービスがすでに有効である場合は、再起動します。

手順

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

ステップ 2 **[サーバ（Server）]** ドロップダウン リスト ボックスからパブリッシャ ノードを選択し、**[移動（Go）]** をクリックします。

ステップ 3 [**セキュリティサービス**] の下で、次の該当するサービスを確認します。

- **Cisco Certificate Enrollment Service**: オンライン CA を使用している場合は、このサービスを確認してください。それ以外の場合は、チェックボックスをオフのままにします。
- **Cisco Certificate Authority プロキシ機能**: このサービスをオフ (非アクティブ) にした場合は、それをチェックします。サービスがすでにアクティブ化されている場合は、そのサービスを再起動する必要があります (下記を参照してください)。

ステップ 4 いずれかの設定を編集した**場合は、[保存 (Save)] をクリックします。**

ステップ 5 **Cisco Certificate Authority Proxy Function** サービスがすでにチェックされている場合は（アクティブ）、再起動します。

a) **[関連リンク（Related Links）]** ドロップダウン リストから **[コントロールセンター-ネットワークサービス（Control Center - Network Services）]** を選択し、**[移動（Go）]** をクリックします。

b) [**セキュリティの**設定] の**下で、Cisco 認証**局プロキシ機能**サービスを確認し、[再起動 (Restart)] 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、個々の電話機に対して CAPF 設定を構成します。

- CAPD 設定をユニバーサル デバイス テンプレートで設定します。 （161 ページ）
- バルク Admin による CAPF 設定の更新 （163 ページ）
- 電話機の CAPF 設定の設定 （164 ページ）

CAPD 設定をユニバーサル デバイス テンプレートで設定します。

CAPF 設定をユニバーサルデバイステンプレートに設定するには、次の手順を実行します。テンプレートは、機能グループテンプレートの設定を使用して、LDAP ディレクトリ同期に適用

することができます。これを行うと、テンプレートのCAPF設定が、このテンプレートを使用する同期済みのすべてのデバイスに適用されます。

（注） Universalデバイステンプレートは、まだ同期されていないLDAPディレクトリにしか追加することができません。初期LDAP同期が発生した場合は、一括管理を使用して電話機を更新します。詳細については、バルク Admin による CAPF 設定の更新（163 ページ）を参照してください。

手順

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

ステップ 2 次のいずれかを実行します。

- [検索（Find）] をクリックし、既存のテンプレートを選択します。
- [新規追加（Add New）] をクリックします。

ステップ 3 **認証局プロキシ機能（CAPF）の設定**領域の拡張

ステップ 4 **[証明書の操作（Certificate Operation）]** ドロップダウン リストで、**[インストール/アップグレード（Install/Upgrade）]** を選択します。

ステップ 5 [**認証モード**] ドロップダウンメニューで、デバイスを認証する方法を選択します。

ステップ 6 認証文字列の使用を選択した場合は、**テキストボックス**に認証文字列を入力するか、**[**文字列の生成 ([文字列の生成])] をクリックして、システムによって文字列が生成されるようにします。

（注） また、この文字列はデバイス自体の赤で表示される必要があります。また、認証は失敗します。

ステップ 7 残りのフィールドで、キー情報を設定します。フィールドを含むヘルプは、オンラインヘルプを参照してください。

ステップ 8 [保存（Save）] をクリックします。

（注） このテンプレートを使用するデバイスは、この手順で割り当てたのと同じ認証方法で構成されていることを確認してください。それ以外の場合、デバイス認証は失敗します。電話機の認証を設定する方法の詳細については、電話機のマニュアルを参照してください。

次のタスク

プロファイルを使用しているデバイスにテンプレートの設定を適用するには、次のようにします。

- ユニバーサルデバイステンプレートを Feature Group テンプレートの設定に追加する
- 機能グループ テンプレートを、まだ同期されていない LDAP ディレクトリ設定に追加します。
- LDAP 同期を完了します。CAPF 設定は、同期されているすべてのデバイスに適用されます。

機能グループテンプレートとLDAP ディレクトリ同期の設定の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure End Users」セクションを参照してください。

バルク Admin による CAPF 設定の更新

この手順では、一括管理の**電話機**の更新電話クエリを使用して、多数の既存の電話機の CAPF 設定と lsc 証明書を 1 回の操作で構成します。

（注） まだ電話機をプロビジョニングしていない場合は、バルク管理**の [**電話機の挿入 (Insert phone)] メニューを使用して、CSV ファイルからの capf 設定で新しい電話機をプロビジョニングできます。電話を CSV ファイルから挿入する方法についての詳細は、 *Bulk Administration Guide for Cisco Unified Communications Manager* の「電話の挿入」の章を参照してください。

始める前に

電話機は、この手順で追加する認証方法と文字列と同じように設定されていることを確認します。そうでない場合、電話機はCAPF を認証できません。電話機で認証を設定する方法の詳細については、電話機のマニュアルを参照してください。

手順

ステップ 1 Cisco Unified CM の管理で、**[一括管理（Bulk Administration）] > [電話（Phones）] > [電話の更新（Update Phone）] > [クエリ（Query）]** の順に選択します。

ステップ 2 フィルタオプションを使用して、更新する電話機に検索を制限し、**[検索 (Find)] をクリックします**。

たとえば、[電話機の検索**場所**] ドロップダウンを使用して、LSC が特定の日付または特定のデバイスプール内のすべての電話機の前に期限切れになるすべての電話機を選択することができます。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 **ログアウト/リセット/再開** ([設定の**適用 (Config)**] ラジオボタン) を選択します。ジョブを実行すると、CAPF アップデートは更新されたすべての電話に適用されます。

ステップ 5 [**証明機関プロキシ関数 (capf)**]の情報で、**[**証明書の操作 (Certificate Operation)] チェックボックスをオンにします。

ステップ 6 [**証明書の操作 (Certificate Operation)**] ドロップダウンから、**[インストール /アップグレード]** を選択して、新しい LSC 証明書を電話機にインストールします。

ステップ 7 [**認証モード**] ドロップダウンから、LSC インストール時に電話機を認証する方法を選択します。

（注） 電話機は、同じ認証方法を使用するように設定されている必要があります。

ステップ 8 認証モードとして認証文字列で選択した場合は、次の手順のいずれかを実行します。

- 各デバイスに対して一意の認証文字列を使用する場合は、**各デバイスに対して一意の認証文字列を生成することを確認してください**。
- すべてのデバイスに同じ認証文字列を使用する場合は、[**認証文字列 (authentication string)**] テキストボックスに文字列を入力するか、**[文字列の生成 (string)]** をクリックします。

ステップ 9 **[電話の更新（Update Phones）]** ウィンドウで **[CAPF の情報（Certification Authority Proxy Function（CAPF）Information）]** セクションの残りのフィールドを入力します。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 10 **[ジョブ情報（Job Information）]** セクションで、**[今すぐ実行（Run Immediately）]**を選択します。

ステップ 11 （注） ジョブスケジューラを使用してジョブを後で実行する場合は、**[後で実行 (run in run)]** を選択することもできます。ジョブスケジューリングの詳細については、「*Bulk Administration Guide for Cisco Unified Communications Manager*」の「Manage Scheduled Jobs」の章を参照してください。

[送信（Submit）] をクリックします。

（注） この手順で [設定の適用 (Apply Configuration)] を選択しなかった場合は、更新されたすべての電話の [電話機の設定 (Phone Configuration)] ウィンドウで、[設定 (configuration)] を適用する必要があります。

次のタスク

オプション。 キープアライブ タイマーの設定 （165 ページ）

電話機の CAPF 設定の設定

個々の電話機の LSC 証明書の CAPF 設定を設定するには、次の手順を実行します。

（注） CAPF 設定を多数の電話機に適用するには、バルク管理または LDAP ディレクトリ同期を使用します。

始める前に

この手順で追加する認証方法と文字列を使用して、電話機が設定されていることを確認してください。そうでない場合、電話機はCAPFに自身を認証できなくなります。電話機で認証を設定する方法の詳細については、電話機のマニュアルを参照してください。

手順

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

ステップ 2 [検索（Find）] をクリックし、既存の電話機を選択します。**[CAPF の情報（Certification Authority Proxy Function (CAPF) Information）]** セクションに移動します。

ステップ 3 [**証明書の操作 (Certificate Operation)**] ドロップダウンから、**[インストール /アップグレード]** を選択して、新しい LSC 証明書を電話機にインストールします。

ステップ 4 [**認証モード**] ドロップダウンから、LSC インストール時に電話機を認証する方法を選択します。

（注） 電話機は、同じ認証方法を使用するように設定されている必要があります。

ステップ 5 **[認証文字列(Authentication string)]** で選択した場合は、テキスト文字列を入力するか、[文字列の生成 (generate string)] をクリックして、システムが文字列を生成するようにします。

ステップ 6 **[電話の設定（Phone Configuration）]** ウィンドウで **[CAPF の情報（Certification Authority Proxy Function（CAPF）Information）]** セクションの残りのフィールドを入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 7 **[保存 (Save)]** をクリックします。

キープアライブ タイマーの設定

ファイアウォールによって接続がタイムアウトしないように、次の手順を実行して、CAPF-エンドポイント接続のクラスターワイドキープアライブタイマーを設定します。デフォルト値は 15 分です。各間隔の後、CAPF サービスは電話機にキープアライブ信号を送信して、接続を開いた状態にします。

手順

ステップ 1 発行者ノードにログインするには、コマンドラインインターフェイスを使用します。

ステップ 2 `utils capt set keep_alive` CLI コマンドを実行します。

ステップ 3 5 ~ 60 (分) の間の数値を**入力**し、enter キーを押します。

CAPF の管理タスク

CAPF を設定し、LSC 証明書を発行した後、次のタスクを使用して LSC 証明書を継続的に管理します。

証明書ステータスのモニタリング

証明書のステータスを自動的に監視するようにシステムを設定することができます。証明書が期限切れに近づいたときにシステムから電子メールが送信され、期限切れ後に証明書が失効します。

証明書の監視の確認の設定方法の詳細については、「証明書の管理」の章の「証明書の監視と失効のタスクフロー」を参照してください。

古い LSC レポートの実行

次の手順を使用して、古い LSC レポートを Cisco ユニファイドレポートから実行します。古い LSCs は、エンドポイント CSR への応答として生成された証明書ですが、古くなった LSCS がインストールされる前に新しい CSR が生成されたため、インストールされませんでした。

（注） また、パブリッシャーノードで `utils capf stale-lsc list` CLI コマンドを実行することによって、古い LSC 証明書のリストを取得することもできます。

手順

ステップ 1 Cisco Unified Reporting から **[System Reports]** をクリックします。

ステップ 2 左側のナビゲーションバーで、[**古い LSCs**] を選択します。

ステップ 3 **[新規レポートの生成]** をクリックします。

保留中の CSR リストの表示

保留中の CAPF CSR ファイルのリストを表示するには、この手順を使用します。すべての CSR ファイルはタイムスタンプされます。

手順

ステップ 1 発行者ノードにログインするには、コマンドラインインターフェイスを使用します。

ステップ 2 `utils core active list` CLI コマンドを実行します。
保留中の CSR ファイルのタイムスタンプリストが表示されます。

古い LSC 証明書の削除

古い LSC 証明書をシステムから削除するには、次の手順を使用します。

手順

ステップ 1 発行者ノードにログインするには、コマンドラインインターフェイスを使用します。

ステップ 2 `[utils capf state-lsc delete all` CLI コマンド] を実行します。
古い LSC 証明書はすべてシステムから削除されます。

CAPF システムの連携動作と制限事項

機能	データのやり取り
[Authentication String]	電話の CAPF 認証方式については、アップグレードまたはインストールの後に同じ認証文字列を電話に入力する必要があります。入力されなかった場合、操作が失敗します。[TFTP Encrypted Config] エンタープライズ パラメータが有効な状態で認証文字列の入力に失敗した場合、電話の設定は失敗し、該当する認証文字列が電話に入力されるまで回復しません。
クラスタ サーバ クレデンシャル	CAPF が Unified Communications Manager クラスタのすべてのサーバを認証できるよう、クラスタ内のすべてのサーバで管理者のユーザ名とパスワードを同じものにする必要があります。

機能	データのやり取り
セキュアな電話機の移行	セキュアな電話が別のクラスタに移動されると、Unified Communications Manager はその電話が送信する LSC 証明書を信頼しなくなります。これは、その LSC 証明書が、CTL ファイル内に証明書が存在しない別の CAPF によって発行されたものであるためです。 セキュア電話を登録可能にするには、既存の CTL ファイルを削除します。その後、[Install/Upgrade] オプションを使用して新しい CAPF により新規 LSC 証明書をインストールし、新しい CTL ファイルのために電話をリセットします（または MIC を使用します）。[Phone Configuration] ウィンドウの [CAPF] セクションにある [Delete] オプションを使用して、電話を移動する前に既存の LSC を削除します。
Cisco Unified IP Phone 6900 シリーズ、7900 シリーズ、および 8900 シリーズ、および 9900	将来的な互換性の問題を回避するため、Unified Communications Manager との TLS 接続に LSC を使用するために Cisco Unified IP Phone 6900 シリーズ、7900 シリーズ、8900 シリーズ、9900 シリーズをアップグレードし、MIC ルート証明書を CallManager 信頼ストアから削除することが推奨されます。Cisco Unified Communications Manager との TLS 接続に MIC を使用する一部の電話モデルは登録できない場合があることに注意してください。 管理者は CallManager 信頼ストアから次の MIC ルート証明書を削除する必要があります。 • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048
停電	以下の情報は、通信障害や電源障害の発生時に適用されます。 • 電話での証明書インストールの実行中に通信障害が発生した場合、電話は証明書の取得を 30 秒間隔でさらに 3 回試行します。これらの値は設定できません。 • 電話による CAPF とのセッション試行中に電源障害が発生した場合、電話はフラッシュに保存されている認証モードを使用します。つまり、電話の再起動後に TFTP サーバから新しい設定ファイルをロードできなかった場合です。証明書操作が完了すると、システムはフラッシュの値をクリアします。

機能	データのやり取り
証明書の暗号化	Cisco Unified Communications Manager リリース 11.5(1)SU1 以降、CAPF サービスによって発行されるすべての LSC 証明書は、SHA-256アルゴリズムで署名されています。したがって、IP 電話 7900/8900/9900 シリーズのモデルは、SHA-256 署名済み LSC 証明書および外部 SHA2 アイデンティティ証明書（Tomcat、CallManager、CAPF、TVS など）をサポートします。署名の検証が必要な、その他の暗号化の操作では、SHA-1 のみがサポートされます。 （注） ソフトウェア メンテナンスが終了またはサポートが終了した電話モデルを使用する場合は、Unified Communications Manager の 11.5(1)SU1 より前のリリースの使用を強くお勧めします。

7942 および 7962 電話機を含む CAPF の例

ユーザまたは Unified Communications Manager によって電話がリセットされたときの CAPF と Cisco Unified IP Phone 7962 および 7942 とのインタラクションについては、以下の情報を考慮してください。

（注） 次の例では、LSC が電話に存在せず、CAPF 認証モードとして**既存の証明書**が選択されている場合、CAPF 証明書操作が失敗します。

例：非セキュア デバイス セキュリティ モード

この例では、[Device Security Mode] を **[Nonsecure]** に設定し、[CAPF Authentication Mode] を **[By Null String]** または **[By Existing Certificate (Precedence...)]** に設定した後、電話がリセットされます。リセットした電話は直ちにプライマリ Unified Communications Manager に登録され、設定ファイルを受信します。その後、電話によって LSC をダウンロードするための CAPF セッションが自動的に開始されます。電話で LSC をインストールした後、[Device Security Mode] を [Authenticated] または [Encrypted] に設定します。

例：認証済み/暗号化済みデバイス セキュリティ モード

この例では、**[Device Security Mode]** を **[Authenticated]** または **[Encrypted]** に設定し、[CAPF Authentication Mode] を **[By Null String]** または **[By Existing Certificate (Precedence...)]** に設定した後、電話がリセットされます。CAPF セッションが終了し LSC がインストールされるまで、電話はプライマリ Unified Communications Manager に登録されません。セッションが終了すると、電話が登録され、直ちに認証済みまたは暗号化済みモードで動作します。

この例では、電話が自動的に CAPF サーバに接続されないため、**[By Authentication String]** を設定できません。電話に有効な LSC がない場合、登録は失敗します。

IPv6 アドレッシングとの CAPF のインタラクション

CAPF は、IPv4、IPv6、またはその両方のタイプのアドレスを使用する電話に対し、証明書の発行とアップグレードを実行できます。IPv6 アドレスを使用する SCCP を実行する電話の証明書の発行またはアップグレードを実行するには、[Unified Communications Manager Administration] で [Enable IPv6] サービス パラメータを **[True]** に設定する必要があります。

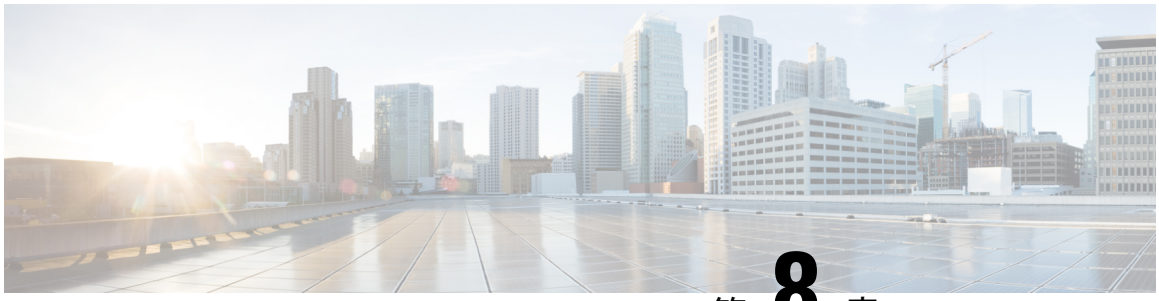
証明書取得のために電話が CAPF に接続されると、CAPF では [Enable IPv6] エンタープライズ パラメータの設定を使用して、その電話の証明書の発行またはアップグレードを実行するかどうかが決定されます。このエンタープライズ パラメータが **False** に設定された場合、CAPF は IPv6 アドレスを使用する電話からの接続を無視または拒否し、その電話は証明書を受け取りません。

IPv4、IPv6、またはその両方のタイプのアドレスを使用する電話から CAPF への接続方法について、次の表で説明します。

表 *23 : IPv6* または *IPv4* 電話から *CAPF* への接続方法

電話の IP モード	電話の IP アドレス	CAPF IP アドレス	電話から CAPF への接続方法
2 スタック	IPv4 と IPv6 が利用可能	IPv4、IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。IPv6 アドレスでは接続できない場合、電話は IPv4 アドレスを使用して接続を試みます。
2 スタック	IPv4	IPv4、IPv6	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv6	IPv4、IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。試行に失敗すると、電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4 と IPv6 が利用可能	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。

電話の IP モード	電話の IP アドレス	CAPF IP アドレス	電話から CAPF への接続方法
2 スタック	IPv4 と IPv6 が利用可能	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4	IPv6	電話は CAPF に接続できません。
2 スタック	IPv6	IPv4	電話は CAPF に接続できません。
2 スタック	IPv6	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv4、IPv6	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv6 スタック	IPv6	IPv4、IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv6	電話は CAPF に接続できません。
IPv6 スタック	IPv6	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv6 スタック	IPv6	IPv4	電話は CAPF に接続できません。



第 8 章

証明書のモニタリングと失効タスクのフロー

証明書モニタリングの概要

管理者は、証明書を管理できる必要があります。どの証明書をいつ更新する必要があるかを認識することがその一部です。Cisco Unified Communications Manager には、どの証明書が更新間近であり、期限がいつであるかを管理者が把握するために役立つ自動システムがあります。次の操作を実行するようにシステムを設定できます。

- 証明書が期限切れに近づいたときに、証明書のステータスを継続的に監視し、電子メールで送信します。
- 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。

オンライン証明書ステータス プロトコル（OCSP）による証明書失効（CRL）

Unified Communications Manager は、証明書失効をモニタリングするための OCSP をプロビジョニングします。スケジュールされた間隔、および証明書がアップロードされるたびにシステムが証明書のステータスをチェックし、有効性を確認します。

オンライン証明書状態プロトコル（OCSP）は、管理者がシステムの証明書要件を管理するのに役立ちます。OCSP を設定すると、証明書の有効性を確認したり期限切れの証明書をリアルタイムで無効化するための、シンプルかつ安全な自動メソッドを使用できます。

コモンクライテリア モードが有効になっている FIPS 展開の場合、OCSP はシステムのコモンクライテリア要件への準拠にも役立ちます。

有効性検査

Unified Communications Manager は、証明書のステータスを確認し、有効性を確認します。

証明書の検証は、次のように行われます。

- Unified Communications Manager は代理信頼モデル（DTM）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。ルート CA または中間 CA は、ステータスを確認するために OCSP 証明書に署名する必要があります。委任された信頼モデルが失敗すると、Unified Communications Manager が応答側の信頼モデル（TRP）にフォールバックし、指定された OCSP 応答の署名証明書を OCSP サーバから使用して証明書を検証します。

（注） 証明書の失効ステータスを確認するために、OCSP レスポンダが実行されている必要があります。

- **[証明書失効（Certificate Revocation）]** ウィンドウで OCSP オプションを有効にすると、最も安全な方法でリアルタイムに証明書失効をチェックすることができます。オプションから、証明書の OCSP URI を使用するか、または設定済みの OCSP URI を使用するかを選択します。OCSP の手動設定の詳細については、「OCSP による証明書失効の設定」を参照してください。

（注） リーフ証明書の場合、syslog、FileBeat、SIP、ILS、LBM などの TLS クライアントは、OCSP 要求を OCSP レスポンダに送信し、OCSP レスポンダからリアルタイムで証明書失効応答を受信します。

コモンクライテリア モードを有効にした状態で検証が実行されると、証明書に対して次のいずれかのステータスが返されます。

- **[良好（Good）]**：**良好**な状態とは、ステータスの問い合わせへの肯定的な応答を示します。この肯定的な応答は、少なくとも証明書が失効していないことを示しますが、必ずしもその証明書が発行済みであること、または、その応答が生成された時刻が証明書の有効期間内にあることを意味するものではありません。レスポンダが作成したアサーションに加えて、発行や有効性の肯定的なステートメントなど、レスポンダが作成した証明書のステータスに関する追加情報を伝送するためには、応答拡張を使用できます。
- **[失効（Revoked）]**：**失効** 状態とは、証明書が失効している（恒久的または一時的に保留されている）ことを示します。
- **[不明（Unknown）]**：**不明**状態とは、OCSP レスポンダが要求された証明書を認識していないことを示します。

（注） コモンクライテリアモードでは、**失効**と**不明**の両方の場合において接続に失敗しますが、コモンクライテリアモードが有効になっていない状態では応答が**不明**ステータスである場合、接続に成功します。

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自動的にモニタするようシステムを設定します。

- 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 （175 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 （176 ページ）	期限切れの証明書が自動的に失効するように OCSP を設定します。

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 （176 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。

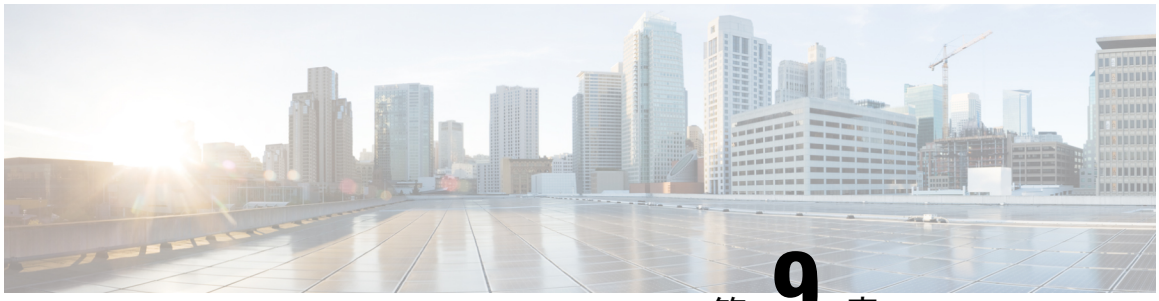
c) [有効性チェック頻度（Validity Check Frequency）] パラメーターの値を設定します。

（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。

第 III 部

Cisco IP Phone と Cisco ボイス メッセージング ポートのセキュリティ



第 9 章

電話のセキュリティ

この章では、電話のセキュリティについて説明します。

電話のセキュリティの概要

インストール時に、Unified Communications Manager は非セキュア モードで起動します。Unified Communications Manager のインストール後に電話が起動すると、すべてのデバイスは Unified Communications Manager に非セキュアとして登録されます。

Unified Communications Manager 4.0(1) 以降のリリースからアップグレードすると、電話はアップグレード前に有効にしたデバイスのセキュリティ モードで起動します。すべてのデバイスは選択したセキュリティ モードを使用して登録されます。

Unified Communications Manager のインストール時に、自己署名証明書が Unified Communications Manager および TFTP サーバで作成されます。また、自己署名証明書ではなくサードパーティの CA 署名付き証明書を Unified Communications Manager に使用するように選択できます。認証後、Unified Communications Manager は証明書を使ってサポートしているCisco Unified IP Phone を認証します。証明書が Unified Communications Manager および TFTP サーバに存在する場合は、Unified Communications Managerはそれぞれの Unified Communications Managerアップグレードで証明書を再発行しません。新しい証明書エントリで新しい CTL ファイルを作成する必要があります。

ヒント　サポートされていないシナリオまたは安全でないシナリオについては、連携動作と制限事項に関連する項目を参照してください。

Unified Communications Manager はデバイス レベルで認証と暗号化のステータスを維持しています。コールに関係するすべてのデバイスがセキュアとして登録されると、コール ステータスはセキュアとして登録されます。1 つのデバイスが非セキュアとして登録されると、発信者または受信者の電話がセキュアとして登録されていても、コールは非セキュアとして登録されます。

ユーザが Cisco Extension Mobility（EM; エクステンション モビリティ）を使用する場合、Unified Communications Manager はデバイスの認証ステータスと暗号化ステータスを保持します。Unified Communications Manager は、共有回線が設定される場合にもデバイスの認証ステータスおよび暗号化ステータスを保持します。

ヒント　暗号化された Cisco IP Phone に対して共有回線を設定するときには、回線を共有するすべてのデバイスで暗号化を設定します。つまり、暗号化をサポートするセキュリティ プロファイルを適用することで、すべてのデバイスのデバイス セキュリティ モードを暗号化に設定します。

信頼できるデバイス

Unified Communications Manager では Cisco IP Phone の電話モデルによってセキュリティ アイコンを有効にできます。セキュリティ アイコンは、コールがセキュアであるかどうか、接続されたデバイスが信頼できるかどうかを示します。

信頼できるデバイスとは、シスコ製デバイスか、シスコの信頼される接続のセキュリティ基準に合格したサードパーティ製デバイスを表します。これには、シグナリングおよびメディア暗号化、プラットフォーム ハードニング、保証などがあります。デバイスが信頼できる場合、セキュリティ アイコンが表示され、サポートされるデバイスでセキュア トーンが再生されます。さらに、デバイスはセキュア コールに関係する他の機能やインジケータも備えていることがあります。

デバイスをシステムに追加すると、Unified Communications Manager はデバイスが信頼できるかどうかを判断します。セキュリティ アイコンは情報目的でだけ表示され、管理者は直接設定できません。

Unified Communications Manager はアイコンおよびメッセージを Unified Communications Manager Administration に表示することでゲートウェイが信頼できるかを示します。

このセクションでは、Cisco IP Phone および Unified Communications Manager Administration の両方での信頼できるデバイスのセキュリティ アイコンの動作について説明します。

Cisco Unified Communications Manager Administration

[Unified Communications Manager Administration] の次のウィンドウには、デバイスが信頼されているかどうかが表示されます。

[Gateway Configuration]

ゲートウェイ タイプごとに、[Gateway Configuration] ウィンドウ（**[Device]** > **[Gateway]**）には、[Device Is Trusted] または [Device Is Not Trusted] と対応するアイコンが表示されます。

システムはデバイス タイプに基づいて、デバイスが信頼できるかどうかを判断します。ユーザはデバイスが信頼できるかどうかを設定できません。

[Phone Configuration]

電話デバイス タイプごとに、[Phone Configuration] ウィンドウ（**[Device]** > **[Phone]**）に [Device Is Trusted] または [Device Is Not Trusted] と対応するアイコンが表示されます。

システムはデバイス タイプに基づいて、デバイスが信頼できるかどうかを判断します。ユーザはデバイスが信頼できるかどうかを設定できません。

コールしたデバイスの信頼判定基準

ユーザがコールするデバイスのタイプは、電話に表示されるセキュリティ アイコンに影響します。システムは次の 3 つの基準に基づいて、コールがセキュアであるかどうかを判断します。

- コールのすべてのデバイスが信頼できるか。
- シグナリングはセキュア（認証されていて暗号化されている）か。
- メディアはセキュアか。

サポートされる Cisco IP Phone にロック セキュリティ アイコンが表示される前に、3 つの基準がすべて満たされている必要があることに注意してください。信頼できないデバイスが関与するコールでは、シグナリングおよびメディアのセキュリティに関係なく、コール全体のステータスは非セキュアなままで、電話機にロック アイコンが表示されません。たとえば、会議に信頼できないデバイスを含めた場合、システムは、そのコール レッグと会議自体を非セキュアと見なします。

電話モデルのサポート

Unified Communications Manager でセキュリティをサポートする電話モデルは、セキュアなシスコの電話とセキュアな推奨ベンダーの電話という 2 つのカテゴリに分類されます。セキュアなシスコの電話には、製造元でインストールされる証明書（MIC ）がプリインストールされ、Certificate Authority Proxy Function（CAPF）を使用したローカルで有効な証明書（LSC）の自動生成と交換をサポートします。セキュアなシスコの電話は、追加の証明書の管理なしで MIC を使用して Cisco Unified CM に登録できます。セキュリティ強化のために、CAPF を使用して

LSC を作成し、電話にインストールできます。詳細については、電話のセキュリティ設定とセットアップのトピックを参照してください。

セキュアな推奨ベンダーの電話には MIC がプリインストールされていないので、LSC の作成で CAPF をサポートしません。セキュアな推奨ベンダーの電話が Cisco Unified CM に接続するには、証明書がデバイスにあるか、デバイスによって生成される必要があります。電話のサプライヤが、電話の証明書を取得または生成する方法についての詳細を提供する必要があります。証明書を入手したら、OS 管理者証明書の管理インターフェイスを使用して、Cisco Unified CM に証明書をアップロードする必要があります。詳細については、推奨ベンダーの SIP 電話のセキュリティ セットアップに関するトピックを参照してください。

お使いの電話でサポートされるセキュリティ機能のリストについては、この Unified Communications Manager リリースに対応した電話管理およびユーザ マニュアル、またはファームウェア ロードに対応したファームウェアのマニュアルを参照してください。

Cisco Unified Reporting を使用して特定の機能をサポートする電話をリストすることもできます。Cisco Unified Reporting の詳細については、『Cisco Unified Reporting Administration Guide』を参照してください。

推奨ベンダーの SIP 電話のセキュリティ設定

推奨ベンダーのセキュアな電話とは、サードパーティ ベンダーによって製造されているが、COP ファイルを使用して Cisco Unified データベースにインストールされている電話です。推奨ベンダーの SIP 電話のセキュリティは、Unified Communications Manager が提供しています。セキュリティをサポートするには、COP ファイルで、推奨ベンダーの SIP 電話のセキュリティ暗号化およびセキュリティ認証を有効にする必要があります。これらの電話タイプは [Add a New Phone] ウィンドウのドロップダウンリストに表示されます。ダイジェスト認証はすべての推奨ベンダーの電話でサポートされていますが、TLS セキュリティはすべての推奨ベンダーの電話でサポートされているわけではありません。セキュリティ機能は電話のモデルにより異なります。電話セキュリティ プロファイルに 「[Device Security Mode]」 フィールドが含まれる場合、電話は TLS をサポートしています。

推奨ベンダーの電話が TLS セキュリティをサポートしている場合は、デバイス別の証明書と共有証明書の 2 つのモードが可能です。電話のサプライヤは電話で使用できるモードを指定し、証明書の生成または取得の手順を提供する必要があります。

デバイス別の証明書による推奨ベンダーの SIP 電話セキュリティ プロファイルのセットアップ

デバイス別の証明書を使用して推奨ベンダーの SIP 電話セキュリティ プロファイルを設定するには、次の手順を実行します。

手順

ステップ 1 OS管理の証明書管理インターフェイスを使用して、電話ごとに証明書をアップロードします。

ステップ 2 [Cisco Unified Administration] で、**[System]** > **[Security]** > **[Phone Security Profile]** の順に選択します。

ステップ 3 この電話のデバイス タイプの新しい電話セキュリティ プロファイルを設定し、[Device Security Mode] ドロップダウン リスト ボックスで [Encrypted] または [Authenticated] を選択します。

ステップ 4 CCMAdmin インターフェイスで新しい SIP 電話を設定するには、**[Device]** > **[Phone]** > **[Add New]** の順に選択します。

ステップ 5 [Phone Type] を選択します。

ステップ 6 必須フィールドに入力します。

ステップ 7 [Device Security Profile] ドロップダウン リスト ボックスで、作成したプロファイルを選択します。

推奨ベンダーの SIP 電話セキュリティ プロファイルの共有証明書の設定

共有証明書を使用して推奨ベンダーのSIP電話セキュリティプロファイルを設定するには、次の手順を実行します。

手順

ステップ 1 電話のベンダーの手順を使用して、サブジェクト代替名（SAN）の文字列を指定して証明書を生成します。SAN のタイプは DNS である必要があります。この手順で指定した SAN をメモしておきます。たとえば、X509v3 拡張の場合、次のようになります。

- サブジェクト代替名
- DNS:AscomGroup01.acme.com

（注） SAN のタイプは DNS である必要があります。そうでない場合、セキュリティは有効になりません。

ステップ 2 OS 管理の証明書管理インターフェイスを使用して、共有証明書をアップロードします。

ステップ 3 [Cisco Unified Administration] で、**[System]** > **[Security]** > **[Phone Security Profile]** の順に選択します。

ステップ 4 [Name]フィールドにサブジェクト代替名（SAN）の名前を入力します。これは、推奨ベンダーによって提供される証明書上の名前です。SAN がない場合は、証明書名を入力します。

（注） セキュリティ プロファイルの名前は、証明書の SAN と正確に一致している必要があります。一致しない場合、セキュリティは有効になりません。

ステップ 5 [Device Security Mode] ドロップダウン リスト ボックスで、[Encrypted] または [Authenticated] を選択します。

ステップ 6 [Transport type] ドロップダウン リスト ボックスで、[TLS] を選択します。

ステップ 7 CCMAdmin インターフェイスで新しい SIP 電話を設定するには、**[Device]** > **[Phone]** > **[Add New]** の順に選択します。

ステップ 8 [Phone Type] を選択します。

ステップ 9 各必須フィールドに入力します

ステップ 10 [Device Security Profile] ドロップダウン リスト ボックスで、作成したプロファイルを選択します。

電話のセキュリティ設定の表示

セキュリティをサポートする電話の特定のセキュリティ関連項目の設定とその確認を行うことができます。たとえば、電話にローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）がインストールされているかどうかを確認できます。セキュアメニューとアイコンの詳細については、ご使用の電話モデルに対応する『*Cisco IP Phone Administration Guide*』および『*Cisco IP Phone User Guide*』を参照してください。

Unified Communications Manager がコールを認証済みまたは暗号化済みと分類すると、コール状態を示すアイコンが電話に表示されます。Unified Communications Manager がどの時点でコールを認証済みまたは暗号化済みとして分類するかも決定します。

電話のセキュリティの設定

ここでは、サポートされている電話のセキュリティを設定する作業を説明します。

手順

ステップ 1 Cisco CTL クライアントが設定されていない場合はこれを設定し、Unified Communications Manager のセキュリティ モードが混合モードであることを確認します。

ステップ 2 電話にローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）がない場合は、Certificate Authority Proxy Function（CAPF）を使用して LSC をインストールします。

ステップ 3 電話セキュリティ プロファイルを設定します。

ステップ 4 電話に電話セキュリティ プロファイルを適用します。

ステップ 5 ダイジェスト クレデンシャルを設定した後、[Phone Configuration] ウィンドウでダイジェスト ユーザを選択してください。

ステップ 6 Cisco Unified IP Phone 7962 および 7942（SIP のみ）では、[End User Configuration] ウィンドウで設定したダイジェスト認証ユーザ名とパスワード（ダイジェストクレデンシャル）を入力します。

（注） このドキュメントでは、電話へのダイジェスト認証クレデンシャルの入力方法は説明していません。これらの作業の実行方法については、使用している電話のモデルに対応する*Cisco IP Phone Administration Guide*を参照してください。

このドキュメントでは、電話へのダイジェスト認証クレデンシャルの入力方法は説明していません。電話に認証名とパスワードを入力する方法については、ご使用の電話とバージョンの Unified Communications Manager に対応した『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 7 電話設定ファイルを暗号化します（暗号化機能をもつ電話のみ）。

ステップ 8 電話のセキュリティをより強化するには、電話設定を無効にします。

電話セキュリティの連携動作と制限事項

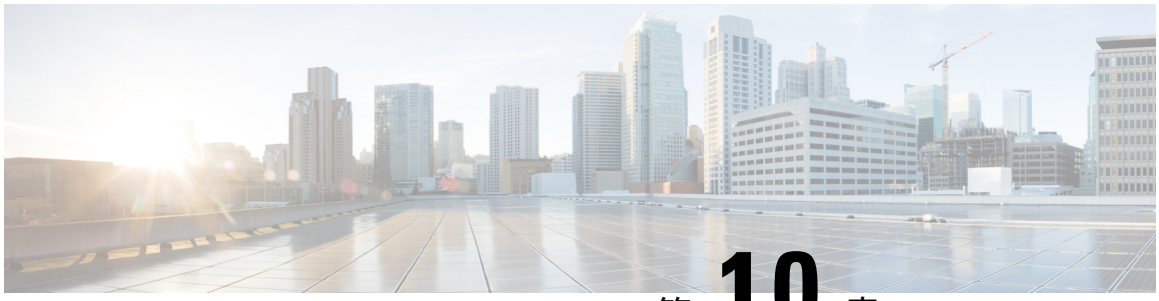
このセクションでは、電話セキュリティの連携動作と制限を示します。

機能	連携動作および制限事項
証明書の暗号化	Cisco Unified Communications Manager リリース 11.5(1)SU1 以降、CAPF サービスによって発行されるすべての LSC 証明書は、SHA-256 アルゴリズムで署名されています。したがって、Cisco Unified IP 電話 7900 シリーズ、8900 シリーズ、および 9900 シリーズのモデルは、SHA-256 署名済み LSC 証明書および外部 SHA2 アイデンティティ証明書（Tomcat、CallManager、CAPF、TVS など）をサポートします。署名の検証が必要な、その他の暗号化の操作では、SHA-1 のみがサポートされます。 （注） ソフトウェア メンテナンスが終了またはサポートが終了した電話モデルを使用する場合は、Unified Communications Manager の 11.5(1)SU1 より前のリリースの使用を強くお勧めします。

電話のセキュリティに関する詳細情報の入手先

関連するシスコのドキュメント

- 『*Administration Guide for Cisco Unified Communications Manager*』
- 『*Cisco Unified Communications Manager*のトラブルシューティングガイド』



第 10 章

電話セキュリティ プロファイルの設定

この章では、セキュリティ プロファイルの設定について説明します。

電話セキュリティ プロファイルの概要

Unified Communications Manager Administration は、電話の種類およびプロトコルのセキュリティ関連設定をセキュリティ プロファイルにグループ化し、単一のセキュリティ プロファイルを複数の電話に指定できるようにします。セキュリティ関連の設定には、デバイス セキュリティ モード、ダイジェスト認証、いくつかの CAPF 設定などがあります。[Phone Configuration] ウィンドウでセキュリティ プロファイルを選択する際に、構成済みの設定を電話に適用します。

Unified Communications Manager をインストールすると、自動登録用の事前に定義された非セキュアなセキュリティ プロファイル一式が提供されます。電話のセキュリティ機能を有効にするには、デバイス タイプとプロトコルに応じた新しいセキュリティ プロファイルを設定し、電話に適用する必要があります。

セキュリティ プロファイルの設定ウィンドウに表示されるのは、選択したデバイスとプロトコルでサポートされるセキュリティ機能だけです。

電話セキュリティ プロファイルの設定の前提条件

電話セキュリティ プロファイルを設定する前に、次の点を考慮してください。

- 電話を設定するときは、[**電話の設定（Phone Configuration**）] ウィンドウでセキュリティ プロファイルを選択します。デバイスがセキュリティまたはセキュア プロファイルをサポートしていない場合は、非セキュア プロファイルを適用します。
- 定義済みの非セキュア プロファイルは削除または変更できません。
- 現在デバイスに割り当てられているセキュリティ プロファイルは削除できません。
- 電話機に割り当てられているセキュリティプロファイルの設定を変更すると、再構成した設定が、その特定のプロファイルを割り当てられているすべての電話機に適用されます。
- デバイスに割り当てられているセキュリティ ファイルの名前を変更できます。事前にプロファイル名および設定を割り当てられている電話機は、新しいプロファイル名および設定を受け入れます。
- [**電話の設定（Phone Configuration**）] ウィンドウに、CAPF 設定、認証モード、およびキーサイズが表示されます。MIC または LSC に関連する証明書の操作には、CAPF 設定を設定する必要があります。[**電話の設定（Phone Configuration**）] ウィンドウで次のフィールドを直接更新できます。
  - セキュリティ プロファイルで CAPF 設定を更新すると、[電話の設定（Phone Configuration）] ウィンドウ上の設定も同様に更新されます。
  - [Phone Configuration] ウィンドウで CAPF 設定を更新し、一致するプロファイルが検出されると、Unified Communications Manager は、一致するプロファイルを電話に適用します。
  - [電話の設定（Phone Configuration）] ウィンドウで CAPF 設定を更新し、一致するプロファイルが検出されない場合は、Unified Communications Manager は新しいプロファイルを作成し、そのプロファイルを電話に適用します。
- アップグレード前にデバイス セキュリティ モードを設定済みの場合は、Unified Communications Manager が設定済みのモデルとプロトコルに基づいてプロファイルを作成し、デバイスにプロファイルを適用します。
- MIC は LSC のインストール時にのみ使用することを推奨します。シスコでは LSC による Cisco Unified Communications Manager との TLS 接続の認証をサポートしています。MIC ルート証明書は侵害される可能性があるため、TLS 認証またはその他の目的に MIC を使用するように電話を設定するユーザは、ご自身の責任で行ってください。MIC が侵害された場合シスコはその責任を負いません。
- TLS 接続に LSC を使用するには、Cisco IP Phone をアップグレードし、互換性の問題を回避するために MIC ルート証明書を CallManager 信頼ストアから削除することを推奨します。

電話セキュリティ プロファイルの検索

電話セキュリティ プロファイルを検索するには、次の手順を実行します。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[System]** > **[Security Profile]** > **[Phone Security Profile]** を選択します。

[Find and List Phone Security Profile] 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）照会のレコードも表示されることがあります。

ステップ 2 データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、ステップ 3 （191 ページ） 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。

（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、[Clear Filter] ボタンをクリックします。

ステップ 3 [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 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。

（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。

電話セキュリティ プロファイルのセットアップ

手順

ステップ 1 [Unified Communications Manager Administration] で、**[System] > [Security Profile]>[Phone Security Profile]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

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

[電話セキュリティ プロファイルの設定（Phone Security Profile Configuration）] ページが表示されます。

b) 既存のセキュリティ プロファイルをコピーするには、適切なプロファイルを検索し、コピーするセキュリティ プロファイルの横にある [**コピー（Copy**）] ボタンをクリックして続行します。

c) 既存のプロファイルを更新するには、適切なセキュリティ プロファイルを検索し、続行します。

[Add New] をクリックすると、各フィールドにデフォルト設定が入力された設定ウィンドウが表示されます。[Copy] をクリックすると、コピーした設定が入力された設定ウィンドウが表示されます。

ステップ 3 SCCP または SIP を実行している電話機の場合は、適切な設定を入力します。

ステップ 4 **[保存 (Save)]** をクリックします。

電話セキュリティ プロファイルの設定

次の表で、SCCP を実行している電話のセキュリティ プロファイル設定について説明します。

選択された電話タイプおよびプロトコルでサポートされる設定だけが示されています。

表 *24 : SCCP* を実行している電話のセキュリティ プロファイル

設定	説明
Name	セキュリティ プロファイルの名前を入力します。 新しいプロファイルを保存すると、電話タイプとプロトコルの [Phone Configuration] ウィンドウの [Device Security Profile] ドロップダウン リスト ボックスにその名前が表示されます。 **ヒント** セキュリティ プロファイル名にデバイス モデルとプロトコルを含めると、プロファイルの検索または更新時に正しいプロファイルを検索できます。
[Description]	セキュリティ プロファイルの説明を入力します。説明には、任意の言語で最大 50 文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

設定	説明
[Device Security Mode]	

設定	説明
	ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。 • [Non Secure]：電話には、イメージ認証、ファイル認証、デバイス認証を除くセキュリティ機能が存在していません。Unified Communications Manager への TCP 接続が開かれます。 • **[Authenticated]**：Unified Communications Managerは電話の整合性と認証を提供します。NULL/SHA を使用する TLS 接続がシグナリングに対して開きます。 • **[Encrypted]**：Unified Communications Manager は、トランクの整合性、認証、およびシグナリング暗号化を提供しています。 説明したように、次の暗号方式がサポートされています。 **TLS暗号方式** このパラメータは、Unified Communication Manager で SIP TLS 接続およびインバウンドの CTI Manager TLS CTI 接続を確立するためにサポートされる暗号を定義します。 最も強力：AES-256 SHA-384 のみ：RSA 優先 • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` （注） パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。このオプションを選択すると、電話機は認証モードで登録されません。 最も強力：AES-256 SHA-384 のみ：ECDSA 優先 • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` （注） パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。このオプションを選択すると、電話機は認証モードで登録されません。 中程度：AES-256 AES-128 のみ：RSA 優先 • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES128_GCM_SHA256`

設定	説明
	• TLS_ECDHE_ECDSA with AES128_GCM_SHA256 （注） このオプションを選択した場合、パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。このオプションを選択すると、電話機は認証モードで登録されません。 中程度：AES-256 AES-128 のみ：ECDSA 優先 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256 （注） このオプションを選択した場合、パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。このオプションを選択すると、電話機は認証モードで登録されません。 すべての暗号方式: RSA優先 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES128_GCM_SHA256 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_RSA with AES_128_CBC_SHA1 すべての暗号 ECDSA 優先 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256

設定	説明
	• TLS_RSA with AES_128_CBC_SHA1 （注） [認証済み] として選択されている [デバイスのセキュリティ プロファイル (トランク)] を使用して設定した場合、Ciscoユニファイドコミュニケーションマネージャーは、NULL_SHA 暗号を使用した TLS connection (データ暗号化なし) を開始します。 これらのトランクは、通知先デバイスが NULL_SHA 暗号をサポートしていない場合は、そのデバイスを登録したり、コールを発信したりしません。 NULL_SHA 暗号をサポートしていない通知先デバイスでは、[暗号化 (Encrypted)] として選択した [デバイスのセキュリティ プロファイル (トランク)] で設定する必要があります。このデバイス セキュリティ プロファイルを使用すると、トランクは、データの暗号化を可能にする追加の TLS 暗号を提供します。
[TFTP Encrypted Config]	このチェックボックスをオンにすると、Unified Communications Manager は TFTP サーバからの電話のダウンロードを暗号化します。

設定	説明
認証モード（Authentication Mode）	

設定	説明
	このフィールドでは、電話がCAPF証明書の処理時に使用する認証方法を選択できます。 ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。 • **[By Authentication String]**：ユーザが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 • **[By Null String]**：ユーザの介入なしで、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 このオプションでは、セキュリティは提供されません。このオプションはセキュアな閉じた環境の場合にのみ選択することを強く推奨します。 • **[By Existing Certificate (Precedence to LSC)]**：製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が電話に存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に MIC と LSC が存在する場合、LSC によって認証が行われます。電話機にLSCが存在しないが、MICが存在する場合、MICによって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • **既存証明書（MIC に優先権）（By Existing Certificate (Precedence to MIC)）**：電話にLSCまたはMICが存在する場合に、製造元でインストールされる証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機にMICが存在するかどうかに関係なく、LSCによって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。電話に証明書が存在しない場合にこのオプションを選択すると、操作は失敗します。

設定	説明
	（注） [Phone Security Profile] ウィンドウで設定される CAPF 設定は、[Phone Configuration] ウィンドウで設定される CAPF パラメータと相互に関係します。
[Key Order]	このフィールドは、CAPF のキーの並び方を指定します。ドロップダウン リストから、次のいずれかの値を選択します。 • **[RSA Only]** • **[EC Only]** • **[EC Preferred, RSA Backup]** （注） **[Key Order]**、**[RSA Key Size]**、および **[EC Key Size]** フィールドの値に基づいて電話を追加すると、デバイス セキュリティ プロファイルがその電話に関連付けられます。 **[EC Only]**値 を選択し、**[EC Key Size]** の値を [256] ビットにすると、デバイス セキュリティ プロファイルには値 **EC-256** が付加されます。
[RSA Key Size (Bits)]	ドロップダウン リスト ボックスから、**[512]**、**[1024]**、**[2048]**、**[3072]**、または**4096** のいずれかの値を選択します。 （注） CallManager が **[Certificate Purpose]** で選択した RSA の **[key length]** が 2048 より大きいと、一部の電話モデルが登録に失敗する場合があります。Cisco Unified Reporting Tool（CURT）の [Unified CM Phone Feature List Report] で、3072/4096 RSA キー サイズ サポート機能をサポートする電話モデルについて確認できます。
[EC Key Size (Bits)]	ドロップダウン リスト ボックスから、**[256]**、**[384]**、または **[521]** のいずれかの値を選択します。

次の表で、SIP を実行している電話のセキュリティ プロファイル設定について説明します。

表 *25 : SIP* を実行している電話のセキュリティ プロファイル

設定	説明
Name	セキュリティ プロファイルの名前を入力します。 新しいプロファイルを保存すると、電話タイプとプロトコルの [Phone Configuration] ウィンドウの [Device Security Profile] ドロップダウン リスト ボックスにその名前が表示されます。 **ヒント** セキュリティ プロファイル名にデバイス モデルとプロトコルを含めると、プロファイルの検索または更新時に正しいプロファイルを検索できます。
[Description]	セキュリティ プロファイルの説明を入力します。
[Nonce Validity Time]	ナンス値が有効な分数（秒単位）を入力します。デフォルト値は 600（10 分）です。この時間が経過すると、Unified Communications Manager は新しい値を生成します。 （注） ナンス値は、ダイジェスト認証をサポートする乱数であり、ダイジェスト認証パスワードの MD5 ハッシュを計算するときに使用されます。

設定	説明
[Device Security Mode]	ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。 • [Non Secure]：電話には、イメージ認証、ファイル認証、デバイス認証を除くセキュリティ機能が存在していません。Unified Communications Manager への TCP 接続が開かれます。 • **[Authenticated]**：Unified Communications Managerは電話の整合性と認証を提供します。NULL/SHA を使用する TLS 接続がシグナリングに対して開きます。 • **[Encrypted]**：Cisco Unified Communications Managerは電話の整合性、認証、および暗号化を提供します。シグナリングに AES128/SHA を使用する TLS 接続が開き、SRTP はすべての SRTP 対応ホップでのすべてのコールに対してメディアを伝送します。 （注） [認証済み] として選択されている [デバイスのセキュリティ プロファイル (トランク)] を使用して設定した場合、Ciscoユニファイドコミュニケーションマネージャーは、NULL_SHA 暗号を使用した TLS connection (データ暗号化なし) を開始します。 これらのトランクは、通知先デバイスが NULL_SHA 暗号をサポートしていない場合は、そのデバイスを登録したり、コールを発信したりしません。 NULL_SHA 暗号をサポートしていない通知先デバイスでは、[暗号化 (Encrypted)] として選択した [デバイスのセキュリティ プロファイル (トランク)] で設定する必要があります。このデバイス セキュリティ プロファイルを使用すると、トランクは、データの暗号化を可能にする追加の TLS 暗号を提供します。

設定	説明
[Transport Type]	[Device Security Mode] が [Non Secure] の場合は、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（一部のオプションは表示されないことがあります）。 • [TCP]：Transmission Control Protocol を選択し、パケットが送信時と同じ順序で受信されるようにします。このプロトコルを使用すると、パケットはドロップされませんが、プロトコルはセキュリティを提供しません。 • [UDP]：User Datagram Protocol を選択し、パケットがすばやく受信されるようにします。このプロトコルはパケットをドロップする可能性があり、パケットは送信された順序で受信されないことがあります。このプロトコルはセキュリティを提供しません。 • [TCP+UDP]：TCP と UDP を組み合わせて使用する場合は、このオプションを選択します。このオプションはセキュリティを提供しません。 [Device Security Mode] が [Authenticated] または [Encrypted] の場合、転送タイプは TLS になります。TLS によって、SIP 電話のシグナリングの整合性、デバイス認証、およびシグナリング暗号化（暗号化モードのみ）が実現されます。 プロファイルで [Device Security Mode] を設定できない場合は、転送タイプは UDP になります。
[Enable Digest Authentication]	このチェックボックスをオンにした場合、Unified Communications Manager は電話からのすべての SIP 要求に対してチャレンジを行います。 ダイジェスト認証ではデバイス認証、整合性、機密性は提供されません。これらの機能を使用するには、セキュリティ モードとして [Authenticated] または [Encrypted] を選択します。
[TFTP Encrypted Config]	このチェックボックスをオンにすると、Unified Communications Manager は TFTP サーバからの電話のダウンロードを暗号化します。このオプションはシスコ製電話専用です。 **ヒント** このオプションを有効化し、対称キーを設定してダイジェスト クレデンシャルと管理パスワードを保護することをお勧めします。

設定	説明
[OAuth 認証の有効化（Enable OAuth Authentication）]	[**デバイス セキュリティ プロファイル**] ドロップダウンリストから **[暗号化 (Encrypted)] を選択**すると、このチェックボックスが使用可能になります。 このチェック ボックスをオンにすると、Unified Communications Manager では、この電話のセキュリティ プロファイルと関連付けられているデバイスが SIP OAuth ポートを使用して登録できるようになります。デフォルトでは、このチェックボックスはオフになっています。 SIP OAuth を有効にするには、次のようにします。 • [Transport Type] が [TLS] の場合： • [デバイス セキュリティモード（Device Security Mode）]は **[** 暗号化（Encrypted）]です。 • ダイジェスト認証の無効化 • 暗号化設定は無効です。 （注） ユニファイドコミュニケーションマネージャーリリース 12.5 では、Jabber は SIP OAuth 認証をサポートしています。
[Exclude Digest Credentials in Configuration File]	このチェックボックスをオンにすると、Unified Communications Manager は TFTP サーバからの電話のダウンロードでダイジェスト クレデンシャルを除外します。このオプションは、Cisco IP Phone、7942、および 7962 (SIP のみ) に対応しています。

設定	説明
認証モード（Authentication Mode）	

設定	説明
	このフィールドでは、電話がCAPF証明書の処理時に使用する認証方法を選択できます。このオプションはシスコ製電話専用です。 ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。 • **[By Authentication String]**：ユーザが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、またはトラブルシューティングします。 • **[By Null String]**：ユーザの介入なしで、ローカルで有効な証明書をインストール/アップグレード、またはトラブルシューティングします。 このオプションではセキュリティが確保されません。したがって、このオプションはセキュアな閉じた環境の場合にのみ選択することを強く推奨します。 • **[By Existing Certificate (Precedence to LSC)]**：製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が電話に存在する場合に、ローカルで有効な証明書をインストール/アップグレード、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に LSC が存在しないが、MIC が存在する場合、MIC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • **既存証明書（MIC に優先権）（By Existing Certificate (Precedence to MIC)）**：電話に LSC または MIC が存在する場合に、製造元でインストールされる証明書をインストール/アップグレード、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。電話に証明書が存在しない場合にこのオプションを選択すると、操作は失敗します。

設定	説明
	（注） [Phone Security Profile] ウィンドウで設定される CAPF 設定は、[Phone Configuration] ウィンドウで設定される CAPF パラメータと相互に関係します。
[Key Size]	CAPF で使用されるこの設定では、ドロップダウン リスト ボックスから証明書のキー サイズを選択します。デフォルト設定は 1024 です。キー サイズのその他のオプションは 512 です。 デフォルトの設定より大きいキー サイズを選択すると、電話がキーの生成に必要なエントロピーを生成する時間が長くなります。キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。 （注） [Phone Security Profile] ウィンドウで設定される CAPF 設定は、[Phone Configuration] ウィンドウで設定される CAPF パラメータと相互に関係します。
[SIP Phone Port]	この設定は、UDP 転送を使用し SIP を実行する電話に適用されます。 UDP を使用して Unified Communications Manager からの SIP メッセージをリッスンする Cisco IP Phone（SIP のみ）のポート番号を入力します。デフォルト設定は 5060 です。 TCP または TLS を使用している電話ではこの設定が無視されます。

電話機へのセキュリティ プロファイルの適用

始める前に

電話の認証に証明書を使用するセキュリティ プロファイルを適用する前に、対象の電話にローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）が含まれていることを確認します。

電話のセキュリティ機能を有効にするには、デバイス タイプとプロトコルに応じた新しいセキュリティ プロファイルを設定し、電話に適用する必要があります。ただし、電話に証明書が含まれない場合は、次の作業を実行してください。

- [**電話の設定（Phone Configuration）**] ウィンドウで、非セキュア プロファイルを適用します。
- [Phone Configuration] ウィンドウで、CAPF 設定を行い、証明書をインストールします。
- [Phone Configuration] ウィンドウで、認証または暗号化のために設定されているデバイスのセキュリティ プロファイルを適用します。

デバイスに電話セキュリティ プロファイルを適用するには、次の手順を実行します。

手順

ステップ 1 [**電話の設定（Phone Configuration**）] ウィンドウの [**プロトコル固有情報（Protocol Specific Information**）] セクションに移動します。

ステップ 2 [Device Security Profile] ドロップダウンリストから、デバイスに適用するセキュリティ プロファイルを選択します。
電話のタイプおよびプロトコルに設定された電話セキュリティ プロファイルだけが表示されます。

ステップ 3 **[Save]** をクリックします。

ステップ 4 該当する電話に変更を適用するには、[Apply Config] をクリックします。

（注） セキュリティ プロファイルを削除するには、[**検索と一覧表示（Find and List**）] ウィンドウ上で該当するセキュリティ プロファイルの横にあるチェックボックスをオンにし、[**選択項目の削除（Delete Selected**）] をクリックします。

電話セキュリティ プロファイルと電話の同期

手順

ステップ 1 [Unified Communications Manager Administration] で、**[システム（System）] > [セキュリティ プロファイル（Security Profile）] > [電話セキュリティ プロファイル（Phone Security Profile）]** を選択します。
[**電話セキュリティ プロファイルの検索/一覧表示（Find and List Phone Security Profiles**）] ウィンドウが表示されます。

ステップ 2 使用する検索条件を選択し、[検索（Find）] をクリックします。
検索条件に一致する電話セキュリティ プロファイルの一覧がウィンドウに表示されます。

ステップ 3 該当の電話機を同期させる電話セキュリティ プロファイルをクリックします。
[**電話セキュリティ プロファイルの設定（Phone Security Profile Configuration**）] ウィンドウが表示されます。

ステップ 4 追加の設定変更を加えます。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 [設定の適用（Apply Config）] をクリックします。
[**設定情報の適用（Apply Configuration Information**）] ダイアログボックスが表示されます。

ステップ 7 [OK] をクリックします。

電話セキュリティ プロファイルの削除

この項では、Unified Communications Manager データベースから電話セキュリティ プロファイルを削除する方法について説明します。

始める前に

[Unified Communications Manager Administration] からセキュリティ プロファイルを削除する前に、デバイスに別のプロファイルを適用するか、そのプロファイルを使用するすべてのデバイスを削除する必要があります。プロファイルを使用しているデバイスを確認するには、[Security Profile Configuration] ウィンドウの [Related Links] ドロップダウン リスト ボックスで [Dependency Records] を選択し、[Go] をクリックします。

依存関係レコード機能がシステムで有効でない場合は、**[System]** > **[Enterprise Parameters Configuration]** に移動し、[Enable Dependency Records] 設定を [True] に設定します。依存関係レコード能に関連してCPU負荷が高くなることについての情報が表示されます。依存関係レコードを有効にするため、変更を保存します。依存関係レコードの詳細は、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

ステップ 1 削除するセキュリティ プロファイルを探します。

ステップ 2 複数のセキュリティ プロファイルを削除するには、[Find and List] ウィンドウで該当するセキュリティ プロファイルの横にあるチェック ボックスをオンにし、[Delete Selected] をクリックします。[Select All] をクリックし、次に [Delete Selected] をクリックすると、設定可能なすべてのレコードが削除されます。

ステップ 3 1 つのセキュリティ プロファイルを削除するには、次のいずれかの作業を実行します。

a) [Find and List] ウィンドウで、該当するセキュリティ プロファイルの横にあるチェック ボックスをオンにし、[Delete Selected] をクリックします。

ステップ 4 削除操作を確認するプロンプトが表示されたら、[OK] をクリックして削除するか、[Cancel] をクリックして削除の操作をキャンセルします。

電話セキュリティ プロファイルによる電話の検索

特定のセキュリティ プロファイルを使用している電話を検索するには、次の手順を実行します。

手順

ステップ 1 Unified Communications Manager Administrationで、**[Device]** > **[Phone]** を選択します。

ステップ 2 最初のドロップダウン リスト ボックスから、検索パラメータ [Security Profile] を選択します。

a) 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。

b) 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、[Clear Filter] ボタンをクリックします。

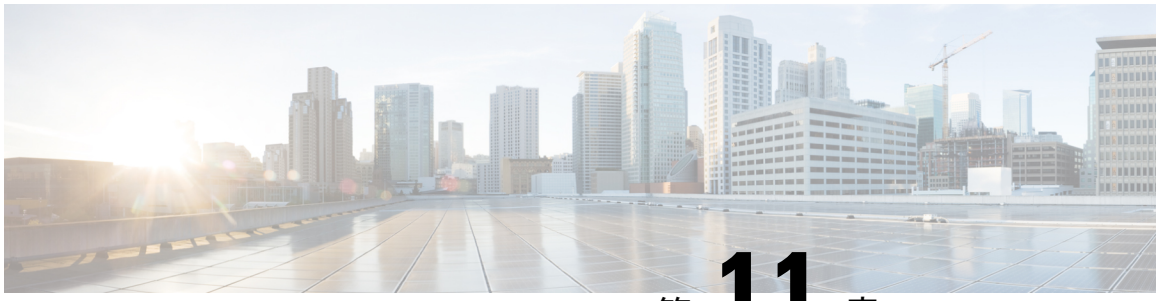
ステップ 3 [検索（Find）] をクリックします。

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 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。

（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。



第 11 章

セキュア通知トーンおよび非セキュア通知トーンの設定

この章では、セキュア通知トーンおよび非セキュア通知トーンの設定について説明します。システムは、通話が暗号化されているかどうかを示すために、保護対象の電話でセキュアおよび非セキュア通知トーンを再生します。

セキュア通知トーンと非セキュア通知トーンの概要

セキュア トーン機能では、暗号化されているコールの場合にセキュア通知トーンを再生するように電話を設定できます。このトーンは、コールが保護されており、機密情報が交換可能であることを示します。2 秒間のトーンでは、長いビープ音が 3 回鳴ります。コールが保護されている場合、着信側が応答するとすぐに保護対象の電話でトーンの再生が始まります。

コールが保護されていない場合、システムは、保護対象の電話で非セキュア通知トーンを再生します。非セキュア通知トーンでは、短いビープ音が 6 回鳴ります。ビデオ コールでは、最初にコールの音声部分に対するセキュア通知トーンが聞こえ、次に非セキュア メディア全体に対する非セキュア通知トーンが聞こえる場合があります。

セキュア通知トーンと非セキュア通知トーンに対応しているコールのタイプを次に示します。

- クラスタ間の IP-to-IP コール
- クラスタ間の保護されたコール
- 保護された MGCP E1 PRI ゲートウェイ経由の IP と時分割多重化（TDM）コール

（注） 保護対象の電話機の発信者にのみ、セキュア通知トーンと非セキュア通知トーンが聞こえます。保護されていない電話の発信者には、これらのトーンは聞こえません。ビデオ コールの場合、システムは、保護されたデバイスでセキュア通知トーンと非セキュア通知トーンを再生します。

保護されたデバイス

設定により、Unified Communications Manager で保護されたデバイスが指定されます。Unified Communications Manager では、サポートされている Cisco Unified IP Phone と MGCP E1 PRI ゲートウェイだけを保護されたデバイスとして設定できます。

Unified Communications Manager は、システムがコールの保護ステータスを判別すると、セキュア通知トーンと非セキュア通知トーンを再生するように MGCP IOS ゲートウェイに指示することもできます。

セキュア通知トーンと非セキュア通知トーンを使用できる次のタイプのコールを発信できます。

- クラスタ間の IP-to-IP コール
- システムが保護されたと判断するクラスタ間コール
- 保護された MGCP E1 PRI ゲートウェイ経由の IP から時分割多重化（TDM）へのコール

サポートされるデバイス

Cisco Unified Reporting を使用して、セキュア通知トーンおよび非セキュア通知トーンをサポートする Cisco IP Phone モデルを確認できます。Cisco Unified Reporting から、[Unified CM Phone Feature List] をクリックします。[Feature] プルダウン メニューから [Secure Tone] を選択します。その機能をサポートする製品のリストが表示されます。

Cisco Unified Reporting の詳細については、『*Cisco Unified Reporting Administration Guide*』を参照してください。

セキュア通知トーンと非セキュア通知トーンのヒント

この項では、セキュア通知トーン機能を使用することによる影響について説明します。

- 保護されたデバイスについての説明を次に示します。
  - SCCP または SIP を実行する電話機を保護対象デバイスとして設定できます。
  - 保護されたデバイスが暗号化されている非保護デバイスに発信する際はセキュア トーンが再生されますが、保護されたデバイスが非保護デバイスや暗号化されていないデバイスに発信する際は非セキュア トーンが再生されます。

- 保護された電話機間の発信で、メディアが暗号化されていない場合は、コールはドロップしません。システムは、コールに関係している電話機で非セキュア通知トーンを再生します。

- ビデオコールの場合、システムは、保護されたデバイスでセキュア通知トーンと非セキュア通知トーンを再生します。

（注） ビデオコールの場合、ユーザには、最初にコールの音声部分に対するセキュア通知トーンが聞こえ、次に非セキュアメディア全体に対する非セキュア通知トーンが聞こえます。

- Cisco IP Phone に表示されるロック アイコンは、メディアが暗号化されていることを示しますが、その電話が保護対象デバイスとして設定されていることを意味するわけではありません。ただし、保護されたコールを発信するにはロック アイコンが表示されている必要があります。

- 影響を受けるサービスと機能を次に示します。
  - 複数回線の補足サービス（コール転送、会議、コール待機など）は保護対象の電話でサポートされています。ユーザが保護されている電話機で補足サービスを呼び出すと、コールの最新のステータスを反映して、セキュア通知トーンまたは非セキュア通知トーンが再生されます。
  - Cisco Extension Mobility および複数ライン同時通話機能（Join Across Lines）サービスは、保護対象の電話では無効です。
  - 共有回線の設定は、保護対象の電話では使用できません。
  - 保留/再開および不在転送は保護対象のコールでサポートされます。

- 次に、MGCP E1 PRI ゲートウェイについての説明を示します。
  - SRTP 暗号化の MGCP ゲートウェイを設定する必要があります。次のコマンドを使用してゲートウェイを設定します。**mgcppackage-capabilitysrtp-packag**
  - MGCP ゲートウェイでは、[高度な IP サービス（Advanced IP Services）] または [高度な企業サービス（Advanced Enterprise Services）] イメージを指定する必要があります。

    たとえば、`c3745-adventerprisek9-mz.124-6.T.bin`など）。
  - MGCP PRI Setup メッセージ、Alert メッセージ、および Connect メッセージに独自の FacilityIE を使用することで、MGCP E1 PRI ゲートウェイとの間で保護ステータスが交換されます。
  - Unified Communications Manager キーは Cisco Unified IP Phone にだけセキュア通知トーンを再生します。ネットワークの PBX はコールのゲートウェイ側でトーンを再生します。

- Cisco Unified IP Phone と MGCP E1 PRI ゲートウェイの間のメディアが暗号化されていないと、コールはドロップされます。

（注） MGCP ゲートウェイの暗号化の詳細については、使用している Cisco IOS ソフトウェアのバージョンの『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』を参照してください。

セキュア通知トーンと非セキュア通知トーンの設定作業

セキュア トーンを再生するには、次の項目を必ず設定してください。

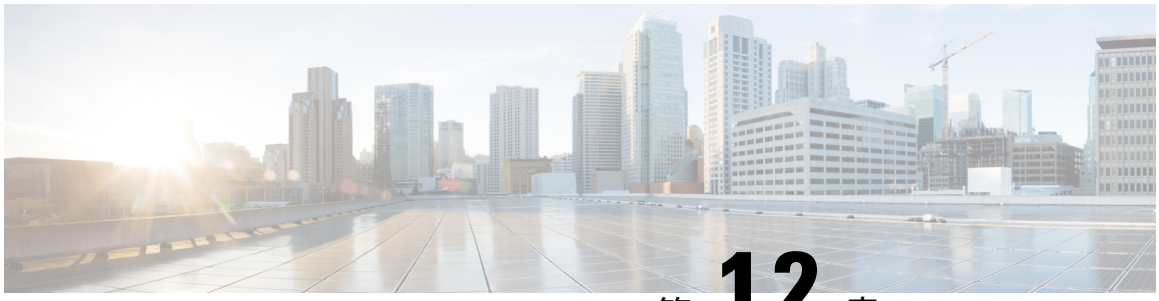
- **[Unified Communications Manager Administration]** で **[Device]** > **[Phone]** を選択すると表示される [Phone Configuration] ウィンドウで以下の項目を設定します。
  - ウィンドウの [デバイス情報（Device Information）] 部分の [ソフトキー テンプレート（Softkey Template）] ドロップダウン リストから、[標準保護電話（Standard Protected Phone）] を選択します。

（注） 保護された電話機用の補足サービス ソフトキーのないソフトキー テンプレートを使用する必要があります。

  - **[Join Across Lines]** オプション（同じくウィンドウの **[Device Information]** 部分内）では、**[Off]** を選択します。
  - [Protected Device] チェックボックス（同じくウィンドウの [Device Information] 部分内）をオンにします。
  - [Device Security Profile] ドロップダウンリスト（ウィンドウの [Protocol Specific Information] 部分内）から、[Phone Security Profile Configuration] ウィンドウで設定済みのセキュア電話プロファイルを選択します（**[System]** > **[Security Profile]** > **[Phone Security Profile]**）。
- [Phone Configuration] ウィンドウからディレクトリ番号を追加するときに表示される [Directory Number Configuration] ウィンドウに移動します。[Directory Number Configuration] ウィンドウの [Device DeviceName] 領域内の [Multiple Call/Call Waiting Settings] で、次のオプションを値 1 に設定します。
  - Maximum Number of Calls
  - ビジー トリガー

- [Cisco Unified Communications Manager Administration] で、**[System]** > **[Service Parameters]** を選択します。最初の [Service Parameter Configuration] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。2 つ目の [Service Parameter Configuration] ウィンドウで [Clusterwide Parameters (Feature - Secure Tone)] 領域を見つけ、[Play Secure Indication Tone] オプションを [True] に設定します。（デフォルト値は [False] です。）
- 保護された MGCP E1 PRI ゲートウェイを設定したら、[Unified Communications Manager Administration] で **[Device]** > **[Gateway]** > **[Add New]** を選択し、サポートされているゲートウェイを選択します。プロトコルとして [MCGP] を選択します。[Gateway Configuration] ウィンドウが表示されたら、次の設定項目を指定します。
  - [Global ISDN Switch Type] を [Euro] に設定します。
  - MGCP ゲートウェイのその他の設定を完了したら、[Save] をクリックし、ウィンドウのサブユニット 0 の右側に表示されるエンドポイントのアイコンをクリックします。[Enable Protected Facility IE] チェックボックスが表示されます。このチェックボックスをオンにします。

    この設定により、Cisco Unified IP Phone エンドポイントと、MGCP ゲートウェイに接続している保護対象 PBX 電話との間でコールの保護ステータスを渡すことができます。



第 12 章

アナログ エンドポイントに対する暗号化の設定

この章では、アナログエンドポイントに対する暗号化の設定について説明します。この機能により、アナログ電話から Cisco VG2xx Gateway へのセキュアな SCCP 接続を確立できます。ゲートウェイは SCCP シグナリング通信に Unified Communications Manager で Transport Layer Security（TLS）を使用し、音声通信には SRTP を使用します。証明書の管理などの既存の Unified Communications Manager TLS 機能が、セキュアな SCCP 通信に使用されます。

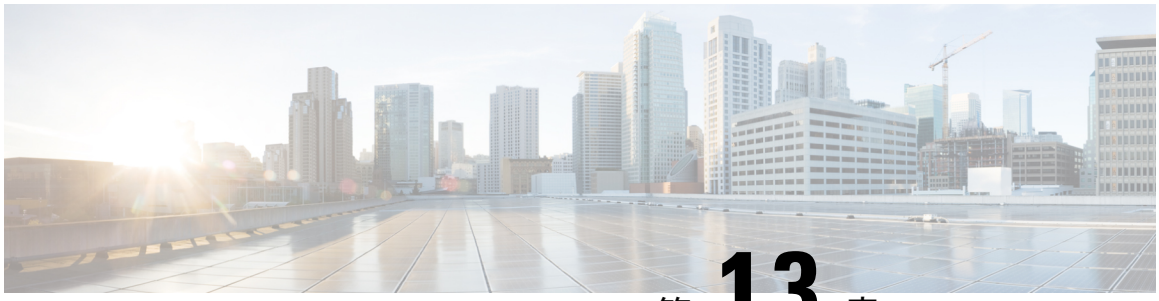
アナログ電話のセキュリティ プロファイル

アナログ電話への暗号化された接続を確立するには、[Device Security Mode] パラメータを [Authenticated] または [Encrypted] に設定して、アナログ電話用の電話セキュリティ プロファイルを作成する必要があります。電話セキュリティ プロファイルを作成するには、[Unified Communications Manager Administration] で、**[System]** > **[Security Profile]** > **[Phone Security Profile]** に移動します。

Cisco VG2xx ゲートウェイに接続されているアナログ電話を設定する場合は、[Device Security Profile] パラメータで、作成したセキュアなアナログプロファイルを選択します。[Device Security Profile] パラメータを設定するには、[Unified Communications Manager Administration] で **[Device]** > **[Phone]** に移動し、設定を行う電話の [Protocol Specific Information] セクションまでスクロールします。

セキュアなアナログ電話の証明書管理

セキュアなアナログ電話を機能させるために、Cisco VG2xx によって使用されているのと同じ CA 署名付き証明書を Cisco Unified Communications Manager にインポートする必要があります。証明書のインポートの詳細については、『*Administration Guide for Cisco Unified Communications Manager*』の第 6 章「「Security」」を参照してください。



第 13 章

暗号化された電話設定ファイルの設定

この章では、暗号化された電話設定ファイルの設定について説明します。セキュリティ関連の設定後、電話設定ファイルにはダイジェストパスワードや電話管理者のパスワードなどの機密情報が含まれるようになります。設定ファイルのプライバシーを確保するには、設定ファイルに暗号化を設定する必要があります。

暗号化された TFTP 設定ファイルの概要

この機能は、登録プロセスを実行している TFTP サーバから電話機がダウンロードする設定ファイルを暗号化することによって、デバイス登録中にデータを保護します。この設定ファイルには、ユーザ名、パスワード、IP アドレス、ポートの詳細、電話機の SSH クレデンシャルなどの機密情報が含まれている場合があり、暗号化しない場合、このような機密情報はクリアテキストで送信されます。データを保護するために、TFTP 設定ファイルを暗号化することを推奨します。

TFTP 設定ファイルを暗号化するには、[Cisco Unified CM Administration] に移動して、[**システム（System）**]>[**セキュリティ（Security）**]>[**電話セキュリティ プロファイル（Phone Security Profile）**] の順に選択し、[**TFTP 暗号化設定（TFTP Encrypted Config）**] チェックボックスをオンにします。

[TFTP 暗号化設定（TFTP Encrypted Config）] オプションを有効にした後、[Unified Communications Manager Administration] および電話機で必要なパラメータを設定してから [Cisco Unified Serviceability] で必要なサービスを再起動すると、TFTP サーバは次の作業を実行します。

1. ディスク上のプレーン テキストの設定ファイルをすべて削除します
2. 設定ファイルの暗号化バージョンの生成

電話が暗号化された電話設定ファイルをサポートしており、電話設定ファイルの暗号化に必要なタスクを行った場合は、暗号化バージョンの設定ファイルが必須です。

警告 TFTP 暗号化設定が False であるが、SIP を実行している電話でダイジェスト認証が True に設定されている場合、ダイジェスト クレデンシャルがクリア テキストで送信される可能性があります。

一部の電話は、暗号化された電話設定ファイルをサポートしていません。電話のモデルとプロトコルによって、設定ファイルの暗号化方法が決定します。サポートされる方式は、Unified Communications Manager の機能と暗号化設定ファイルをサポートするファームウェア ロードに依存します。電話のファームウェア ロードを、暗号化に対応していないバージョンにまでダウングレードすると、TFTP サーバは最低限の設定を行う平文の設定ファイルを送ります。この場合、電話が期待された機能を発揮できないことがあります。

キー情報のプライバシーを確実に維持できるように、暗号化された電話機設定ファイルに関連するタスクをセキュアな環境で実行することが強く推奨されます。

Unified Communications Manager は次の方式をサポートしています。

- 手動キー配布
- 電話の公開キーによる対称キー暗号化

手動キー配布と電話の公開キーによる対称キー暗号化のための設定情報は、混合モードが設定済みで、[Unified Communications Manager Administration] の [TFTP Encrypted Config] パラメータが有効になっていることを前提としています。

手動キー配布

手動キー配布を使用すると、電話リセット後に、Unified Communications Manager データベースに保存された 128 ビットまたは 256 ビットの対称キーを使用して電話設定ファイルが暗号化されます。電話モデルのキー サイズを判別する。

設定ファイルを暗号化するために、管理者はキーを手動で入力することも、Unified Communications Manager に **[Phone Configuration]** ウィンドウで生成させることもできます。データベースにキーが存在するようになった後、管理者またはユーザは電話のユーザインターフェイスにアクセスしてキーを電話に入力する必要があります。[Accept] ソフトキーを押すと、電話はすぐにキーをフラッシュに保存します。キーの入力以降、電話はリセット後に暗号化された設定ファイルを要求します。必要なタスクが実行された後、RC4 または AES 128 暗号化アルゴリズムを使用して、対称キーにより設定ファイルが暗号化されます。どの電話機が RC4 または AES 128 暗号化アルゴリズムを使用するかを確認するには、「暗号化をサポートする電話モデル （222 ページ）」を参照してください。

電話に対称キーが含まれる場合、その電話は暗号化された設定ファイルを常に要求します。Unified Communications Manager によって、TFTP サーバによって署名された暗号化設定ファイルが電話にダウンロードされます。すべての電話タイプで設定ファイルの署名者が検証されるわけではありません。

電話はフラッシュに保存された対称キーを使用して、ファイルの内容を復号します。復号に失敗すると、設定ファイルが電話に適用されません。

ヒント [TFTP Encrypted Config] の設定が無効にされた場合、管理者は電話の GUI で対称キーを削除する必要があります。これにより、次回リセットされたときに電話が暗号化されていない設定ファイルを要求します。

電話の公開キーによる対称キーの暗号化

製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が電話に含まれている場合、電話には公開キーと秘密キーのペアが含まれ、これらのキーはPKI暗号化に使用されます。

この方法を初めて使用する場合、電話は設定ファイルにある電話の証明書の MD5 ハッシュと LSC または MIC の MD5 ハッシュとを比較します。電話で問題が特定されない場合、電話はリセット後に暗号化された設定ファイルを TFTP サーバに要求します。電話が問題を特定した場合、たとえばハッシュが一致しない、電話に証明書がない、MD5 値がブランクであるなどの場合、電話は CAPF 認証モードが [By Authentication String] に設定されていない限り、CAPF とのセッションを開始しようとします（[By Authentication String] に設定されている場合は文字列の手動入力が必要です）。Certificate Authority Proxy Function（CAPF）は Cisco IP Phone を Unified Communications Manager に対して認証し、電話の証明書（LSC）を発行します。CAPF は、LSC または MIC から電話の公開キーを抽出し、MD5 ハッシュを生成し、Unified Communications Manager データベースに公開キーの値および証明書ハッシュを保存します。公開キーがデータベースに格納された後、電話はリセットされ、新しい設定ファイルが要求されます。

公開キーがデータベースに保存され電話がリセットされた後、データベースが TFTP に電話の公開キーが存在することを通知すると、対称キー暗号化プロセスが開始されます。TFTP サーバは 128 ビット対称キーを生成します。これにより、Advanced Encryption Standard（AES）128 暗号化アルゴリズムで設定ファイルが暗号化されます。次に、電話の公開キーで対称キーが暗号化され、設定ファイルの署名付きエンベロープヘッダーに含まれます。電話はファイルの署名を確認し、署名が有効であれば、電話は LSC または MIC の秘密キーを使用して暗号化された対称キーを復号化します。次に、対称キーによってファイルの内容が復号化されます。

設定ファイルを更新するたびに、TFTP サーバは自動的にファイルを暗号化するための新しいキーを生成します。

ヒント この暗号化方式をサポートする電話では、設定ファイルの暗号化設定フラグを使用して、暗号化ファイルを要求するかまたは非暗号化ファイルを要求するかを判断します。[TFTP Encrypted Config] 設定が無効な場合に、この暗号化方式をサポートする Cisco IP Phone が暗号化ファイル（.enc.sgn ファイル）を要求すると、Unified Communications Manager は [file not found error] エラーを電話に送信します。次に、電話は暗号化されていない署名付きファイル（.sgn ファイル）を要求します。

[TFTP Encrypted Config] 設定が有効な場合に、電話が何らかの理由で暗号化されていない設定ファイルを要求すると、TFTP サーバは最小限の設定を含む暗号化されていないファイルを提供します。電話は最小限の設定を受信した後、キーの不一致などのエラー状態を検出でき、CAPF でセッションを開始して電話の公開キーと Unified Communications Manager データベースを同期できます。エラー条件が解決されると、電話は次回リセットされるときに暗号化された設定ファイルを要求します。

暗号化をサポートする電話モデル

以下の Cisco Unified IP Phone では電話の設定ファイルを暗号化できます。

電話モデルとプロトコル	暗号化方式
Cisco Unified IP Phone 7800 または 6921	手動キー配布：暗号化アルゴリズム：RC4 キーサイズ：256 ビット ファイル署名のサポート：いいえ
Cisco ユニファイド IP Phone 7942 または 7962 (SIP のみ)	手動キー配布：暗号化アルゴリズム：Advanced Encryption Standard（AES）128 キーサイズ：128 ビット ファイル署名のサポート：SIP を実行するこれらの電話は、署名付きで暗号化された設定ファイルを受信しますが、署名情報を無視します。

電話モデルとプロトコル	暗号化方式
Cisco Unified IP Phone 6901、6911、6921、6941、6945、および 6961 Cisco Unified IP Phone 7975G。Cisco Unified IP Phone 7961G、7962G、または 7965G。Cisco Unified IP Phone 7941G、7942G、または 7945G。Cisco Unified IP Phone 7911G。Cisco Unified IP Phone 7906G Cisco Unified IP Phone 、7961G-GE、7941G-GE Cisco 統一 IP Phone 79 31g, (sccp のみ) CISCO 統一されたワイヤレス Ip Phone 79 25g, 79 25G-EX, 79 26g Cisco Unified IP Phone 8941 および 8945 Cisco Unified IP Phone 8961、9951、および 9971 Cisco IP Phone 7811、7821、7841、7861 Cisco IP Conference Phone 7832 Cisco IP Phones 8811、8841、8845、8851、8851NR、8861、8865、および 8865NR Cisco Unified IP Conference Phone 8831 Cisco Conference Phone 8832 Cisco Wireless IP Phone 8821	電話の公開キーによる対称キーの暗号化（PKI 暗号化）：暗号化アルゴリズム：AES 128 キーサイズ：128 ビット ファイル署名のサポート：はい （注） Cisco Unified IP Phone 6901 および 6911 はデフォルトでセキュリティをサポートしていないため、ITL ファイルを要求しません。したがって、暗号化された設定ファイルが Cisco IP Phone 6901 および 6911 で動作するための Cisco Certificate Authority Proxy Function（CAPF）の詳細を含む Cisco CTL ファイルを取得するため、Unified Communications Manager クラスタは、Cisco Unified IP Phone（6901 と 6911）ではセキュア（混合）モードに設定する必要があります。

暗号化された TFTP 設定ファイルのヒント

電話機がダウンロードする機密データを保護するために、[TFTP 暗号化設定（TFTP Encrypted Config）] フラグを有効化することを推奨します。電話に PKI 機能がない場合、 [Unified Communications Manager Administration] と電話で対称キーを設定する必要があります。電話と Unified Communications Manager のいずれかに対称キーが存在しない場合、または [TFTP Encrypted Config] フラグが設定されている場合に不一致が発生した場合、その電話は登録できません。

[Cisco Unified Communications Manager Administration] で暗号化された設定ファイルを設定する場合、以下の情報を検討してください。

- 暗号化された設定ファイルをサポートする電話でのみ、セキュリティ プロファイルに [TFTP Encrypted Config] フラグが表示されます。Cisco Unified IP Phone 7800、7942、7962（SCCP のみ）には暗号化された設定ファイルを設定できません。これらの電話は設定ファイルのダウンロード時に機密データを受信しないためです。

- [TFTP 暗号化設定（TFTP Encrypted Config）] のデフォルト設定は False（オフ）です。デフォルト設定である非セキュア プロファイルを電話に適用する場合、ダイジェスト クレデンシャルとセキュア パスワードはクリア テキストで送信されます。
- 公開キー暗号化を使用する Cisco IP Phone の場合、暗号化された設定ファイルを有効化するためにデバイス セキュリティ モードを認証済みまたは暗号化済みにすることを Unified Communications Manager が要求することはありません。Unified Communications Manager では、登録の間の公開キーのダウンロードに CAPF プロセスが使用されます。
- 環境がセキュアであるとわかっている場合、または PKI が有効でない電話への対称キーの手動設定を避けるために、暗号化されていない設定ファイルを電話にダウンロードすることを選択することも可能です。ただし、この方法は推奨されません。
- Cisco Unified IP Phone 7800、7942、7962（SIP のみ）の場合、[Unified Communications Manager Administration] では電話へのダイジェスト クレデンシャルを送信することができますが、この方法では暗号化された設定ファイルの使用に比べて使いやすいものの安全性は低くなります。[Exclude Digest Credentials in Configuration File] 設定を使用するこの方法は、最初に対称キーを設定して電話に入力する必要がないため、ダイジェスト クレデンシャルの初期化に役立ちます。

この方法の場合、ダイジェストクレデンシャルは暗号化されていない設定ファイルで電話に送られます。電話にクレデンシャルが存在するようになった後には、TFTP ファイル暗号化設定を無効のままにし、セキュリティ プロファイル ウィンドウの [設定ファイル内のダイジェスト信用証明書を除外（Exclude Digest Credentials in Configuration File）] フラグを有効化することで、その後のダウンロードからダイジェスト クレデンシャルを除外することを推奨します。

ダイジェスト クレデンシャルが電話に存在するようになり、着信ファイルにダイジェスト クレデンシャルが含まれないようになると、既存のクレデンシャルがそのまま使用されます。ダイジェスト クレデンシャルは、出荷時の状態へのリセットや新規クレデンシャル（空白を含む）の受信まで、電話にそのまま残ります。

電話またはエンドユーザのダイジェスト クレデンシャルを変更する場合、対応するセキュリティ プロファイル ウィンドウの [Exclude Digest Credentials] フラグを一時的に無効化し、新しいダイジェスト クレデンシャルを電話にダウンロードします。

電話設定ファイルの暗号化のタスク フロー

TFTP 設定ファイルに暗号化を設定するには、次のタスクを実行します。

始める前に

- クラスタ セキュリティが混合モードになっていることを確認します。
- クラスタ内の電話機のうち、手動キー暗号化および公開キー暗号化をサポートしている電話機を確認します。
- SHA-1 および SHA-512 をサポートしている電話機を確認します。

クラスタ全体で SHA-512 を有効にすると、この暗号をサポートしていない電話は機能しません。

手順

	コマンドまたはアクション	目的
ステップ 1	TFTP 暗号化の有効化 （225 ページ）	使用する電話の [TFTP Configuration File] オプションを有効にします。このオプションは電話セキュリティ プロファイルで有効にできます。
ステップ 2	SHA-512 署名アルゴリズムの設定 （226 ページ）	（任意）。TFTP ファイル暗号化を有効化すると、デフォルトの署名アルゴリズムとして SHA-1 が設定されます。強力な SHA-512 アルゴリズムを使用できるようシステムを更新するには、次の手順を実行します。
ステップ 3	手動キー配布の設定 （227 ページ）	手動のキーを使用する電話の場合は、手動キー配布を設定する必要があります。
ステップ 4	電話の対称キーの入力 （228 ページ）	手動のキーを使用する電話では、Unified Communications Manager にキーを入力します。
ステップ 5	LSC または MIC 証明書のインストールの確認 （229 ページ）	公開キーを使用する電話では、証明書のインストールを確認します。
ステップ 6	CTL ファイルの更新 （230 ページ）	TFTP 設定ファイルの更新が完了したら、CTL ファイルを再生成します。
ステップ 7	サービスの再起動 （230 ページ）	Cisco CallManager サービスおよび Cisco TFTP サービスを再起動します。
ステップ 8	電話のリセット （231 ページ）	暗号化された TFTP 設定ファイルの更新を完了したら、電話をリセットします。

TFTP 暗号化の有効化

TFTP サーバからダウンロードするファイルの暗号化を有効にするには、次の手順を使用します。このオプションは、特定のモデルの電話の電話セキュリティ プロファイル内で有効にできます。

手順

ステップ 1 [Cisco Unified CM Administration] で、**[System]** > **[Security]** > **[Phone Security Profile]** の順に選択します。

ステップ 2 [検索（**Find**）] をクリックし、電話セキュリティ プロファイルを選択します。

ステップ 3 [TFTP Encrypted Config] チェック ボックスをオンにします。

ステップ 4 **[Save]** をクリックします。

ステップ 5 クラスタで使用されている他の電話セキュリティプロファイルについて、ここまでの手順を繰り返します。

（注） 電話設定ファイルの暗号化を無効にするには、[Unified Communications Manager Administration] で電話セキュリティ プロファイルの [**TFTP 暗号化設定**（**TFTP Encrypted Config**）] チェックボックスをオフにし、変更を保存する必要があります。

SHA-512 署名アルゴリズムの設定

SHA-1 は TFTP ファイル暗号化のデフォルトのアルゴリズムです。

デジタル署名など、TFTP 設定ファイルに対してより堅牢な SHA-512 アルゴリズムを使用できるようシステムをアップグレードするには、以下の任意の手順を使用します。

（注） ご使用の電話が SHA-512 に対応していることを確認します。対応していない場合は、システム更新後に電話機が動作しなくなります。

始める前に

TFTP 暗号化の有効化 （225 ページ）

手順

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

ステップ 2 [セキュリティ パラメータ（**Security Parameters**）] セクションに移動します。

ステップ 3 [**TFTP ファイル署名アルゴリズム**（**TFTP File Signature Algorithm**）] ドロップダウンリストから、[**SHA-512**] を選択します。

ステップ 4 **[保存 (Save)]** をクリックします。

手動キー配布の設定

手動キーを使用する電話の場合は、手動キー配布を設定する必要があります。

始める前に

次に述べる手順では、以下の点を前提としています。

- 電話が Unified Communications Manager データベースに存在している。
- 互換性のあるファームウェア ロードが TFTP サーバに存在している。
- [Unified Communications Manager Administration] で、[TFTP 暗号化設定（TFTP Encrypted Config）] パラメータが有効に設定されている。
- 電話機が手動キー配布をサポートしている。

手順

ステップ 1 [Cisco Unified CM Administration] から、[**デバイス（Device）**] > [**電話機（Phone）**] の順に選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 [電話の設定（Phone Configuration）] ウィンドウが表示されたら、手動キー配布の設定を行います。

（注） この設定を行った後は、キーは変更できません。

ステップ 4 **[Save]** をクリックします。

ステップ 5 電話に対称キーを入力し、電話をリセットします。

これらの作業の実行方法については、使用している電話のモデルに対応する電話のアドミニストレーション ガイドを参照してください。

手動キー配布の設定

次の表に、[Phone Configuration] ウィンドウでの手動配布の設定について説明します。

表 *26 :* 手動キー配布の設定

設定	説明
[Symmetric Key]	対称キーに使用する 16 進数の文字列を入力します。有効な文字は、数字の 0～9、大文字（小文字）の A～F（または a～f）です。 キー サイズに対応した正確なビット数を入力するようにしてください。不正確な値は Cisco Unified Communications Manager に拒否されます。Cisco Unified Communications Manager では次のキー サイズがサポートされています: • Cisco Unified IP Phone 7905G および 7912G（SIP のみ）：256 ビット • Cisco ユニファイド IPPhone s の 7942 および 7962 (SIP のみ): 128 ビット キー設定後は、キーを変更しないでください。
[Generate String]	[Cisco Unified Communications Manager Administration] で 16 進数文字列を生成させる場合、[Generate String] ボタンをクリックします。 キー設定後は、キーを変更しないでください。
[Revert to Database Value]	データベースに存在する値を復元するには、このボタンをクリックします。

電話の対称キーの入力

前述の手順を使用して、Unified Communications Manager で電話機の手動キーを設定した場合は、次の手順を実行して電話機にキーを入力します。

手順

ステップ 1 電話の [Setting] ボタンを押します。

ステップ 2 設定がロックされている場合は、[Setting] メニューをスクロールし、[Unlock Phone] を強調表示して、[Select] ソフトキーを押します。電話のパスワードを入力して [Accept] ソフトキーを押します。

電話がパスワードを受け入れます。

ステップ 3 [Setting] メニューをスクロールし、[Security Configuration] を強調表示して、[Select] ソフトキーを押します。

ステップ 4 [Security Configuration] メニューで [Set Cfg Encrypt Key] オプションを強調表示し、[Select] ソフトキーを押します。

ステップ 5 暗号キーの入力を要求されたら、キーを入力します（16進数）。キーをクリアする必要がある場合は 32 桁のゼロを入力します。

ステップ 6 キーの入力が終了したら、[Accept] ソフトキーを押します。

電話が暗号キーを受け入れます。

ステップ 7 電話をリセットします。

電話のリセット後、電話は暗号化された設定ファイルを要求します。

LSC または MIC 証明書のインストールの確認

公開キーを使用する電話では、証明書のインストールを確認します。

（注） この手順は、PKI 暗号化を使用する Cisco Unified IP Phone に適用されます。ご使用の電話機が PKI 暗号化をサポートしているかどうかを確認するには、「暗号化された設定ファイルをサポートする電話機モデル」セクションを参照してください。

始める前に

次に述べる手順では、以下の点を前提としています。

- 電話が Unified Communications Manager データベースに存在している。
- [Unified Communications Manager Administration] で、[TFTP 暗号化設定（TFTP Encrypted Config）] パラメータが有効に設定されている。

手順

ステップ 1 製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が電話に存在することを確認します。

ヒント LSC または MIC が電話機に存在するかを Unified Communications Manager で確認するには、[電話の設定（Phone Configuration）] ウィンドウの CAPF 設定セクションにある [**トラブルシュート（Troubleshoot**）] オプションを選択します。証明書が電話に存在しない場合は、[Delete] と [Troubleshoot] オプションは表示されません。

ヒント　また、電話機の [セキュリティ設定（Security Configuration）] をチェックする方法でも、LSC または MIC が電話機に存在するかを確認することができます。詳細については、このバージョンの Unified Communications Manager に対応したCisco Unified IP Phone 用の『Cisco Unified IP Phone アドミニストレーション ガイド』を参照してください。

ステップ 2　証明書が存在しない場合、[電話の設定（Phone Configuration）] ウィンドウで認証局プロキシ機能（CAPF）を使用して、LSC をインストールします。LSC のインストール方法については、認証局プロキシ機能（CAPF）に関するトピックを参照してください。

ステップ 3　CAPF を設定したら、[Save] をクリックします。

ステップ 4　[Phone Configuration] ウィンドウで [Reset] をクリックします。電話機はリセット後、TFTP サーバから暗号化された設定ファイルを要求します。

CTL ファイルの更新

TFTP ファイル暗号化を有効にした後、CTL ファイルを再生成します。

手順

ステップ 1　コマンドライン インターフェイスにログインします。

ステップ 2　パブリッシャ ノードで **utils ctl update CTLfile** コマンドを実行します。

サービスの再起動

手順

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

ステップ 2　以下の 2 つのサービスを選択し、[**停止（Stop**）] をクリックします。

- Cisco CallManager
- Cisco TFTP

ステップ 3　これら2つのサービスが停止したら、両方を再度選択し、[**再起動（Restart**）] をクリックします。

電話のリセット

始める前に

暗号化された TFTP 設定ファイルの更新をすべて完了した後、必ず電話機をリセットしてください。

手順

ステップ 1 [Cisco Unified CM Administration] から、**[デバイス（Device）]** > **[電話（Phones）]** 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 [すべて選択（Select All）] をクリックします。

ステップ 4 [選択をリセットする（Reset selected）] をクリックします。

暗号化された TFTP 設定ファイルの無効化

電話設定ファイルの暗号化を無効にするには、対象の電話機に関連付けられている電話セキュリティ プロファイルで [TFTP 暗号化設定（TFTP Encrypted Config）] チェックボックスをオフにする必要があります。

警告 TFTP 暗号化設定が False であるが、SIP を実行している電話でダイジェスト認証が True に設定されている場合、ダイジェスト クレデンシャルがクリア テキストで送信される可能性があります。

設定の更新後、電話の暗号キーは Unified Communications Manager データベース内に残ります。

Cisco IP Phone 7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7975G は暗号化ファイル（.enc、.sgn ファイル）を必要とします。暗号化設定が false に変更された場合は、電話は暗号化されていない、署名されたファイル（.sgn ファイル）を要求します。

Cisco Unified IP Phone が SCCP および SIP で実行されている場合は、暗号化設定が無効に変更されたときに、暗号化されたファイルを要求します。次回リセットされたときに電話が暗号化されていない設定ファイルを要求するように設定するには、管理者が電話の GUI から対称キーを削除する必要があります。

- SCCP で実行される Cisco Unified IP Phone は、6901、6911、6921、6941、6945、6961、7906G、7911G、7925G、7925G-EX、7926G、7931G、7940G、7941G、7941G-GE、7942G、7945G、7960G、7961G、7961G-GE、7962G、7965G、7970G、7975G、8941、8945 です。

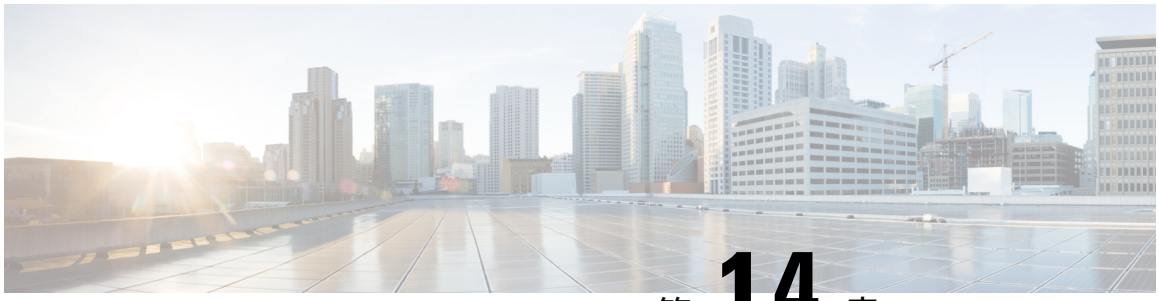
- SIP で実行される Cisco Unified IP Phone は、6901、6911、6921、6941、6945、6961、7906G、7911G、7941G、7941G-GE、7942G、7961G、7961G-GE、7962G、7965G、7975G、8941、8945、8961、9971、7811、78321、7841、7861、7832、8811、8841、8845、8851、8851NR、8861、8865、8865NE、8821、8831、8832、8832NR です。

ヒント　Cisco Unified IP Phone 7942 および 7962（SIP のみ）では、暗号化を無効にするために電話の GUI で対称キーのキー値として 32 バイトの 0 を入力します。Cisco Unified IP Phone （SIP のみ）では、暗号化を無効にするために電話の GUI で対称キーを削除します。これらの作業の実行方法については、使用している電話のモデルに対応する電話のアドミニストレーション ガイドを参照してください。

電話設定ファイルダウンロードからのダイジェストクレデンシャルの除外

初期設定後、電話に送信された設定ファイルからダイジェスト クレデンシャルを除外するには、電話に適用されているセキュリティ プロファイルの [Exclude Digest Credentials in Configuration File] チェック ボックスをオンにします。このオプションは、Ciscoユニファイド IP Phone s の 7800、7942、および 7962 (SIP のみ) でのみサポートされます。

ダイジェスト クレデンシャルを変更するために設定ファイルを更新する場合には、このチェック ボックスをオフにすることが必要となることがあります。



第 14 章

SIP 電話のダイジェスト認証の設定

この章では、SIP 電話機でのダイジェスト認証の設定について説明します。SIP を実行する電話機でのダイジェスト認証の動作の詳細については、「ダイジェスト認証 （26 ページ）」を参照してください。

電話のダイジェスト認証を有効化すると、SIP を実行中の電話に対するキープアライブメッセージを除くすべての要求に対して Unified Communications Manager はチャレンジを実施します。電話が提供するクレデンシャルの有効性を確認するために、Unified Communications Manager は **[End User Configuration]** ウィンドウでの設定に基づいて、エンド ユーザのダイジェスト クレデンシャルを使用します。

電話がエクステンション モビリティをサポートする場合、エクステンション モビリティ ユーザがログインすると、Unified Communications Manager は、**[End User Configuration]** ウィンドウでの設定に基づいて、エクステンション モビリティ エンドユーザのダイジェスト クレデンシャルを使用します。

SIP を実行しているシスコ以外の電話のダイジェスト認証の設定の詳細は、『*Administration Guide for Cisco Unified Communications Manager*』の付録 C を参照してください。

電話セキュリティ プロファイルからダイジェスト認証を有効化

電話セキュリティ プロファイルから電話機のダイジェスト認証を有効にするには、次の手順を使用します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[システム（System）] > [セキュリティ（Security）] > [電話セキュリティ プロファイル（Phone Security Profile）] の順に選択します。

ステップ 2 **[検索（Find）]** をクリックして、対象の電話機に関連付けられている電話セキュリティ プロファイルを選択します。

ステップ 3 **[ダイジェスト認証を有効化（Enable Digest Authentication）]** チェックボックスをオンにします。

ステップ 4 **[保存 (Save)]** をクリックします。

SIP Station レルムの設定

Cisco Unified Communications Manager が 401 Unauthorized メッセージへの応答として、SIP 電話機に対する認証確認の際に [レルム（Realm）] フィールドで使用する文字列を割り当てます。この設定は、電話機にダイジェスト認証が設定されている場合に適用されます。

（注） このサービス パラメータのデフォルトの文字列は「ccmsipline」です。

手順

ステップ 1 [Unified Communications Manager] で、**[System]** > **[Service Parameters]** を選択します。

ステップ 2 **[サーバ（Server）]** ドロップダウンリストから、Cisco CallManager サービスをアクティブ化したノードを選択します。

ステップ 3 **[サービス（Service）]** ドロップダウンリストから、Cisco CallManager サービスを選択します。サービス名の横に「「Active」」と表示されることを確認します。

ステップ 4 ヘルプの説明に従って、**SIP Realm Station** パラメータを更新します。パラメータのヘルプを表示するには、疑問符またはパラメータ名リンクをクリックします。

ステップ 5 **[保存 (Save)]** をクリックします。

電話ユーザへのダイジェストクレデンシャルの割り当て

電話機を所有するエンドユーザにダイジェストクレデンシャルを割り当てるには、次の手順を使用します。このクレデンシャルは、電話機による認証に使用されます。

.

手順

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

ステップ 2 [**検索（Find**）] をクリックして、電話機を所有しているエンドユーザを選択します。

ステップ 3 次のフィールドにクレデンシャルを入力します。

- Digest Credentials
- Confirm Digest Credentials

ステップ 4 **[保存 (Save)]** をクリックします。

エンド ユーザのダイジェスト クレデンシャルの設定

（注） ダイジェスト クレデンシャルの詳細を表示するには、[Cisco Unified Communications Manager Administration] に移動し、[**ユーザ管理（User Management**）] > [**エンドユーザ（End User**）] を選択します。ユーザ ID をクリックすると、[**エンドユーザの設定（End User Configuration**）] ウィンドウが表示されます。ダイジェスト クレデンシャルは、**[エンドユーザの設定（End User Configuration**）] ウィンドウの **[ユーザ情報（User Information**）] ペイン内に表示されます。

表 27 : Digest Credentials

設定	説明
Digest Credentials	英数字の文字列を入力します。
Confirm Digest Credentials	[Digest Credentials] の入力が正しいことを確認するために、このフィールドにクレデンシャルを再度入力します。

電話機へのダイジェスト認証の割り当て

この手順を使用して、ダイジェストユーザおよびダイジェスト認証が有効になっているセキュリティ プロファイルを電話機に関連付けます。

手順

ステップ 1 [Cisco Unified CM Administration] から、**[デバイス（Device）] > [電話機（Phone）]** の順に選択します。

ステップ 2 **[検索（Find）]** をクリックして、ダイジェスト認証を割り当てる電話を選択します。

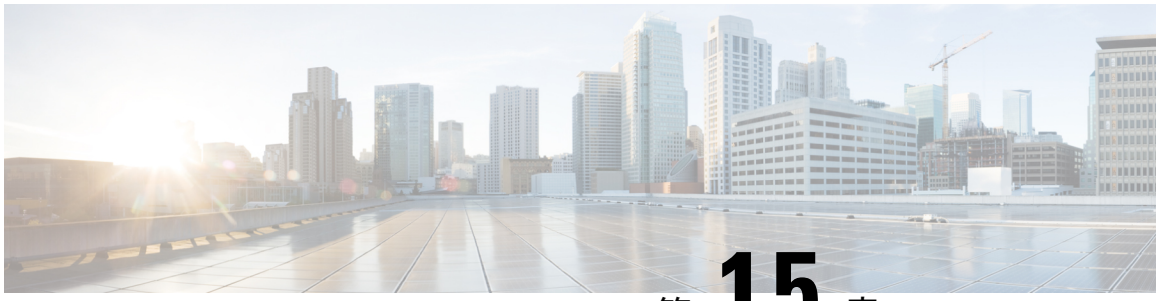
ステップ 3 **[ダイジェスト ユーザ（Digest User）]** ドロップダウンリストで、ダイジェスト クレデンシャルを割り当てたエンドユーザを割り当てます。

ステップ 4 ダイジェスト認証を有効にした電話セキュリティ プロファイルが **[デバイス セキュリティ プロファイル（Device Security Profile）]** ドロップダウンリストで割り当てられていることを確認します。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 [リセット（Reset）] をクリックします。

エンド ユーザを電話に関連付けたら、設定を保存し、電話をリセットします。



第 15 章

電話のセキュリティ強化

この章では、電話のセキュリティの強化について説明します。電話のセキュリティを強化するタスクは、[Unified Communications Manager Administration] の **[Phone Configuration]** ウィンドウで行います。

Gratuitous ARP の無効化

Cisco Unified IP Phone は、デフォルトでは Gratuitous ARP パケットを受け入れます。デバイスが使用する Gratuitous ARP パケットは、ネットワークにデバイスの存在を公表するために使用されます。ただし、攻撃者はこれらのパケットを使用して有効なネットワーク デバイスのスプーフィングを行えます。たとえば、デフォルトルータであると主張するパケットを攻撃者が送信する可能性があります。必要な場合、[Phone Configuration] ウィンドウで Gratuitous ARP を無効化できます。

（注） この機能を無効にしても、電話がデフォルト ルータを特定できなくなることはありません。

Web アクセスの無効化

電話の Web サーバ機能を無効にすると、統計および設定情報を提供する電話内部の Web ページへのアクセスがブロックされます。Cisco Quality Report Tool などの機能は、電話の Web ペー

ジにアクセスしないと正しく動作しません。また、Web サーバを無効にすると、CiscoWorks など、Web アクセスに依存するサービスアビリティ アプリケーションにも影響します。

Web サービスが無効であるかどうかを確認するため、電話は、サービスの無効/有効を示す設定ファイル内のパラメータを解析します。Web サービスが無効な場合、電話は HTTP ポート 80 をモニタリング用に開かず、電話内部 Web ページへのアクセスをブロックします。

PC 音声 VLAN へのアクセスの無効化

デフォルトでは、Cisco IP Phone はスイッチ ポート（上流に位置するスイッチに面したポート）で受信したすべてのパケットを PC ポートに転送します。[Phone Configuration] ウィンドウの [PC Voice VLAN Access] 設定を無効にすると、PC ポートから受信した音声 VLAN 機能を使用するパケットはドロップされます。さまざまな Cisco IP Phone がそれぞれ異なる方法でこの機能を使用しています。

- Cisco Unified IP Phone 7942 と 7962 は、PC ポートで送受信される、音声 VLAN のタグが付いたパケットをドロップします。

設定へのアクセスの無効化

デフォルトでは、Cisco IP Phone の [Applications] ボタンを押すと、電話の設定情報を含むさまざまな情報にアクセスできます。[Phone Configuration] ウィンドウで [Setting Access] パラメータ設定を無効にすると、通常は電話の [Applications] ボタンを押すと表示されるすべてのオプション（[Contrast]、[Ring Type]、[Network Configuration]、[Model Information]、[Status] などの設定）へのアクセスが拒否されます。

Unified Communications Manager Administration 内の設定を無効にすると、以前の設定は電話に表示されません。この設定を無効にすると、電話ユーザは [Volume] ボタンに関連した設定を保存できません。たとえば、ユーザは音量の設定を保存できません。

この設定を無効にすると、電話の既存の [Contrast]、[Ring Type]、[Network Configuration]、[Model Information]、[Status]、および [Volume] の現在の設定が自動的に保存されます。これらの電話機設定を変更するには、Unified Communications Manager Administration で [設定へのアクセス（Setting Access）] 設定を有効にします。

PC ポートの無効化

デフォルトでは、Unified Communications Manager は PC ポートを備えているすべての Cisco IP Phone で PC ポートを有効にします。必要な場合、[Phone Configuration] ウィンドウで [PC Port] 設定を無効にできます。PC ポートの無効化は、ロビーや会議室の電話の場合に役立ちます。

（注） PC ポートは一部の電話機で使用でき、ユーザは電話機にコンピュータを接続できます。この接続方法は、ユーザが 1 つの LAN ポートだけを必要とすることを意味します。

電話のセキュリティ強化の設定

手順

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

ステップ 2 電話機の検索条件を指定して **[検索（Find）]** をクリックし、すべての電話機を表示します。

ステップ 3 デバイス名をクリックします。
[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 次の製品固有のパラメータを見つけます。

a) PC Port
b) Settings Access
c) Gratuitous ARP
d) PC Voice VLAN Access
e) Web Access

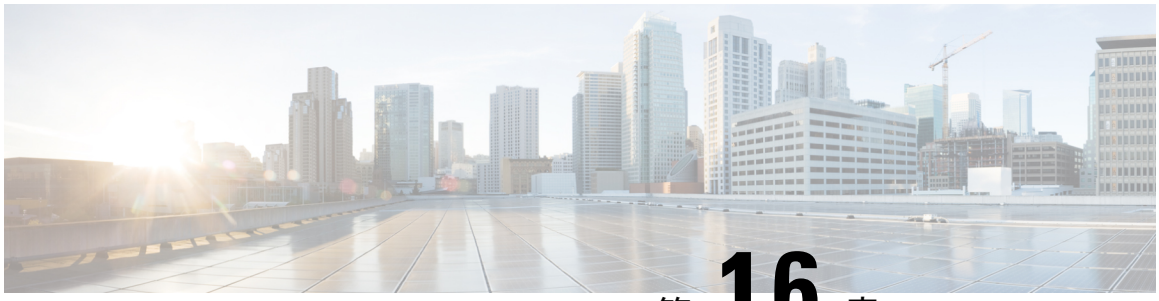
ヒント これらの設定に関する情報を確認するには、**[電話の設定（Phone Configuration）]** ウィンドウで各種パラメータの横に表示されているヘルプアイコンをクリックします。

ステップ 5 無効にする各パラメータのドロップダウンリストから、**[無効（Disabled）]** を選択します。スピーカーフォン、またはスピーカーフォンとヘッドセットを無効にするには、対応するチェックボックスをオンにします。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 [リセット（Reset）] をクリックします。

電話のセキュリティの強化に関する詳細情報の入手先



第 16 章

セキュアな会議リソースの設定

この章では、セキュアな会議リソースの設定について説明します。

セキュアな会議

セキュアな会議機能は、会議を保護するために認証と暗号化を提供します。会議に参加しているすべてのデバイスでシグナリングとメディアが暗号化されている場合に、会議は保護されているとみなされます。セキュアな会議機能は、セキュアな TLS または IPSec 接続での SRTP 暗号化をサポートします。

システムでは、会議の全体的なセキュリティ ステータスを示すセキュリティ アイコンが表示されます。この全体的なステータスは、参加しているデバイスの最も低いセキュリティ レベルにより決定します。たとえば、2 つの暗号化接続と 1 つの認証済み接続を含むセキュアな会議のセキュリティ ステータスは認証済みです。

セキュアなアドホック会議とミートミー会議を設定するには、セキュアな会議ブリッジを設定します。

- ユーザが認証済みまたは暗号化済みの電話から電話会議を開始すると、Unified Communications Manager はセキュアな会議ブリッジを割り当てます。
- ユーザが非セキュアな電話からコールを開始すると、Unified Communications Manager は非セキュアな会議ブリッジを割り当てます。

会議ブリッジ リソースを非セキュアとして設定すると、電話のセキュリティ設定にかかわらず、会議は非セキュアになります。

（注） Unified Communications Manager は会議を開始している電話のメディア リソース グループ リスト（MRGL）から会議ブリッジを割り当てます。セキュアな会議ブリッジを使用できない場合は、Unified Communications Manager は非セキュアな会議ブリッジを割り当て、会議は非セキュアになります。同様に、非セキュアな会議ブリッジを使用できない場合、Unified Communications Manager はセキュアな会議ブリッジを割り当て、会議は非セキュアになります。会議ブリッジが利用不可の場合、コールは失敗します。

ミートミー会議コールでは、会議を開始する電話はミートミー番号に設定された最小セキュリティ要件を満たす必要があります。セキュアな会議ブリッジを使用できないか、発信者のセキュリティ レベルが最小要件を満たさない場合、Unified Communications Manager は会議の試行を拒否します。

割り込みを使用する会議を保護するには、暗号化モードを使用するよう電話を設定します。デバイスが認証済みまたは暗号化済みの場合に [Barge] キーを押すと、Unified Communications Managerは割り込み相手とターゲットデバイスでの組み込みブリッジの間でセキュアな接続を確立します。システムは、割り込みコールに接続されているすべての参加者に対して会議のセキュリティ ステータスを示します。

（注） リリース 8.3 以降を実行している非セキュアまたは認証済みの Cisco Unified IP Phone は暗号化済みコールに割り込めるようになりました。

会議ブリッジの要件

ハードウェアによる会議ブリッジをネットワークに追加し、Unified Communications Manager Administration でセキュアな会議ブリッジを設定する場合、会議ブリッジをセキュアなメディア リソースとして登録できます。

（注） Unified Communications Manager の処理のパフォーマンスに対する影響を考え、ソフトウェアによる会議ブリッジでのセキュアな会議はサポートしていません。

H.323 または MGCP ゲートウェイでの会議を実現するデジタル シグナル プロセッサ（DSP）ファームが、IP テレフォニー会議のネットワーク リソースとして動作します。会議ブリッジは、Unified Communications Manager にセキュアな SCCP クライアントとして登録されます。

- 会議ブリッジのルート証明書が CallManager 信頼ストア内に存在し、Cisco CallManager 証明書が会議ブリッジの信頼ストアに存在する必要があります。
- セキュアな会議ブリッジのセキュリティ設定は、登録するUnified Communications Managerのセキュリティ設定と一致している必要があります。

会議ルータの詳細については、IOS ルータに付属するドキュメンテーションを参照してください。

Unified Communications Managerは、コールに対して会議リソースを動的に割り当てます。使用可能な会議リソースと有効化されたコーデックによって、ルータに許容される最大同時実行数のセキュアな会議が実現されます。ストリームの送受信は、参加するエンドポイントそれぞれに対して個別にキー設定されるため（このため参加者が会議を退出しても再度のキー設定は不要）、DSP モジュールに対するトータルでのセキュアな会議のキャパシティは、設定可能な非セキュア キャパシティの半分に等しくなります。

『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

セキュアな会議のアイコン

Cisco IP Phone は会議全体のセキュリティ レベルを示す会議セキュリティ アイコンを表示します。これらのアイコンは、ユーザ マニュアルに記載されているように、セキュアな 2 者間コールのステータス アイコンと一致します。

コールの音声とビデオ部分が会議のセキュリティ レベルのベースとなります。コールは、音声とビデオ部分がセキュアである場合に限り、安全とみなされます。

セキュアなアドホック会議とミートミー会議では、会議参加者の電話ウィンドウにある会議ソフトキーの横に会議のセキュリティ アイコンが表示されます。表示されるアイコンは、会議ブリッジおよびすべての参加者のセキュリティ レベルによって異なります。

- 会議ブリッジがセキュアで会議の全参加者が暗号化されている場合、ロック アイコンが表示されます。
- 会議ブリッジがセキュアで会議の全参加者が認証されている場合、シールド アイコンが表示されます。一部の電話モデルでは、シールド アイコンが表示されません。
- 会議ブリッジまたは会議のいずれかの参加者が非セキュアである場合に、コール状態アイコン（アクティブ、保留など）が表示されます。一部の古いモデルの電話では、アイコンは表示されません。

（注） 「Override BFCP Application Encryption Status When Designating Call Security Status」サービス パラメータは、パラメータ値が [True] で音声がセキュアであると、ロック アイコンを表示します。この状態は、他のすべてのメディア チャネルのセキュリティ ステータスを無視します。デフォルト パラメータ値は [False] です。

暗号化された電話がセキュアな会議ブリッジに接続すると、デバイスと会議ブリッジの間のメディア ストリーミングは暗号化されます。ただし、会議のアイコンは、他の参加者のセキュリティ レベルに応じて暗号化、認証済み、非セキュアのいずれかになります。非セキュア ステータスは、参加者のいずれかがセキュアでないか、または確認できないことを示します。

ユーザが [Barge] を押すと、[Barge] ソフトキーの横にあるアイコンが割り込み会議のセキュリティ レベルを示します。割り込むデバイスと割り込まれたデバイスが暗号化をサポートする場合、システムは 2 つのデバイス間のメディアを暗号化しますが、割り込み会議のステータスは、接続された参加者のセキュリティ レベルに応じて、非セキュア、認証済み、暗号化のいずれかになります。

セキュアな会議のステータス

会議のステータスは、参加者が会議に参加するときと退出するときに変わります。暗号化された会議は、認証済みまたは非セキュアな参加者がコールに接続すると、セキュリティ レベルが認証済みまたは非セキュアに戻ることがあります。同様に、認証済みまたは非セキュアな参加者がコールから退出すると、ステータスが上がることがあります。非セキュアな参加者が電話会議に接続すると、会議は非セキュアになります。

会議のステータスは、参加者が複数の会議を結合した場合、結合した会議のセキュリティ ステータスが変わった場合、保留にされた電話会議が別のデバイスで再開された場合、電話会議に割り込みがあった場合、または転送された電話会議が別のデバイスで完了した場合にも変化します。

（注） [Advanced Ad Hoc Conference Enabled] サービス パラメータは、会議、参加、直接転送、および転送などの機能を使用してアドホック会議をリンクできるかどうかを決定します。

Unified Communications Manager はセキュアな会議を維持するために以下のオプションを提供します。

- アドホック会議のリスト
- 最小セキュリティ レベルでのミートミー会議

アドホック会議のリスト

会議リストは、電話会議中に [ConfList] ソフトキーが押された場合に、参加者の電話に表示されます。会議リストには、会議のステータス、および暗号化されていない参加者を識別するための参加者ごとのセキュリティ ステータスが一覧表示されます。

会議リストには、[nonsecure]、[authenticated]、[encrypted]、[held] の各セキュリティ アイコンが表示されます。会議の開催者は、会議リストを使用して、セキュリティ ステータスの低い参加者を退席させることができます。

（注） [Advanced Ad Hoc Conference Enabled] サービス パラメータによって、会議の開催者以外の会議参加者が他の会議参加者を退席させることができるかどうかが決定されます。

参加者は、会議に参加すると、会議リストの一番上に追加されます。非セキュアな参加者を [ConfList] ソフトキーと [RmLstC] ソフトキーでセキュアな会議から削除する方法については、ご使用の電話のユーザ マニュアルを参照してください。

次の各項では、セキュアなアドホック会議と他の機能とのインタラクションについて説明します。

セキュアなアドホック会議と会議チェーン

ある 1 つのアドホック会議が別のアドホック会議にチェーンされると、そのチェーンされた会議は、メンバー「「Conference」」としてそれ自体のセキュリティ ステータスとともにリストに表示されます。会議全体のセキュリティ ステータスを判別するために、Unified Communications Manager に、チェーンされた会議のセキュリティ レベルが組み込まれます。

セキュアなアドホック会議と C 割り込み

ユーザが [cBarge] ソフトキーを押してアクティブな会議に参加すると、Unified Communications Managerではアドホック会議が作成され、割り込まれたデバイスのセキュリティ レベルとMRGLに従って会議ブリッジが割り当てられます。C割り込みのメンバー名が会議リストに表示されます。

セキュアなアドホック会議と割り込み

セキュアなアドホック会議の参加者が割り込まれた場合、割り込みコールのセキュリティ ステータスが会議リストの割り込み先参加者の横に表示されます。メディアが割り込み先参加者と会議ブリッジの間で実際に暗号化済みの場合に、割り込み元発信者の接続が認証済みであるために、割り込み先参加者のセキュリティアイコンが認証済みと表示されることがあります。

割り込み先参加者がセキュアだが非セキュアなアドホック会議に参加している場合に、アドホック会議のステータスがその後セキュアに変わると、割り込み元発信者のアイコンも更新されます。

セキュアなアドホック会議と参加

認証済みまたは暗号化済みの電話のユーザは、Cisco Unified IP Phone（SCCP が実行されている電話機のみ）の [Join] ソフトキーを使用して、セキュアなアドホック会議を作成またはそれに参加することができます。ユーザが [Join] を押してセキュリティ ステータスの不明な参加者を既存の会議に追加すると、Unified Communications Manager ではその会議のステータスを [unknown] にダウングレードします。[Join] を使用して新規メンバーを追加した参加者は会議の開催者になり、新規メンバーやその他の参加者を会議リストから退席させることができます（[Advanced Ad Hoc Conference Enabled] 設定が [True] になっている場合）。

セキュアなアドホック会議と保留/復帰

会議の開催者が参加者を追加するために電話会議を保留にすると、追加された参加者が電話に応答するまで、会議のステータスは不明（非セキュア）になります。その新規参加者が応答すると、会議リストで会議のステータスが更新されます。

共有回線上の発信者が保留中の電話会議を別の電話で復帰させる場合は、発信者が [Resume] を押したときに会議リストが更新されます。

最小セキュリティ レベルでのミートミー会議

管理者は、ミートミーのパターンまたは番号を非セキュア、認証済み、暗号化済みとして設定する場合、会議に最小セキュリティ レベルを指定できます。参加者は最小セキュリティ要件を満たしている必要があり、満たしていない場合はシステムが参加者をブロックし、コールをドロップします。このアクションはミートミー会議のコール転送、共有回線で再開されたミートミー会議コール、結合されたミートミー会議に適用されます。

ミートミー会議を開始する電話は、最小セキュリティ レベルを満たしている必要があります。満たしていない場合、システムによって試行が拒否されます。最小セキュリティ レベルとして認証済みまたは暗号化済みが指定されており、かつセキュアな会議ブリッジが使用できない場合、コールは失敗します。

会議ブリッジの最小レベルに非セキュアを指定すると、会議ブリッジはすべてのコールを受け入れ、会議のステータスは非セキュアになります。

ここでは、セキュアなミートミー会議とその他の機能のインタラクションについて説明します。

ミートミー会議とアドホック会議

ミートミー会議をアドホック会議に追加する場合、またはアドホック会議をミートミー会議に追加する場合、アドホック会議がミートミー会議の最小セキュリティ レベルを満たしている必要があります。満たしていない場合、コールはドロップされます。会議が追加されると、会議アイコンが変わる場合があります。

ミートミー会議と割り込み

割り込み発信者がミートミー会議参加者に割り込んだ場合、その発信者が最低セキュリティ要件を満たしていないと、割り込まれたデバイスのセキュリティ レベルは下がり、割り込み発信者と割り込まれたコールの両方がドロップされます。

ミートミー会議と保留/再開

共有回線の電話は、最小セキュリティ レベルを満たしていない限り、ミートミー会議を再開できません。電話が最小セキュリティ レベルを満たしていない場合、ユーザが [Resume] ボタンを押すと共有回線上のすべての電話がブロックされます。

Cisco Unified IP Phone のセキュアな会議とアイコンのサポート

次の Cisco Unified IP Phone では、セキュア会議とセキュア会議アイコンがサポートされています。

- Cisco Unified IP Phone 7942 および 7962（SCCP のみ、認証済みセキュア会議のみ）
- Cisco Unified IP Phone 6901、6911、6921、6941、6945、6961、7906G、7911G、7931G、7942、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7975G、8941、8945。（SCCP のみ）
- Cisco Unified IP Phone 6901、6911、6921、6941、6945、6961、7906G、7911G、7941G、7941G-GE、7942G、7961G、7961G-GE、7962G、7965G、7975G、8941、8945、8961、9971、9971。

  Cisco IP Phone 7811、7821、7841、7861、cisco ipphone 7832、cisco ip phone 8811、8841、8845、8851、8851NR、8861、8865、8865nr、cisco Wireless IP Phone 8821、統一 IP 会議電話機 8831、Cisco IP 会議電話 8832。

警告 セキュア会議機能を十分に活用するため、Cisco Unified IP Phone をリリース 8.3 以降にアップグレードすることを推奨します。このリリースでは、暗号化機能がサポートされています。以前のリリースを実行している暗号化済みの電話は、これらの機能を完全にサポートしてはいません。そのような電話は、認証済みまたは非セキュアな参加者としてのみセキュア会議に参加できます。

リリース 8.3 の Cisco Unified IP Phone で、以前のリリースの Cisco Unified Communications Manager が使用されている場合、電話会議の間、会議のセキュリティ ステータスではなく接続のセキュリティ ステータスが表示され、会議リストなどのセキュア会議機能もサポートされません。

Cisco Unified IP Phone に適用されるその他の制限については、Unified Communications Manager のセキュア会議の制限関連項目を参照してください。

セキュア電話会議とセキュリティ アイコンの詳細については、ご使用の電話の『*Cisco IP Phone Administration Guide*』および『*Cisco IP Phone User Guide*』を参照してください。

セキュアな会議の CTI サポート

Unified Communications Manager はライセンス済み CTI デバイスでのセキュアな会議をサポートしています。詳細については、このリリースの『*Unified Communications Manager JTAPI Developers Guide*』および『*Unified Communications Manager TAPI Developers Guide*』を参照してください。

トランクおよびゲートウェイでのセキュアな会議

Unified Communications Manager はクラスタ間トランク（ICT）、H.323 トランク/ゲートウェイ、および MGCP ゲートウェイを介したセキュアな会議をサポートしています。ただし、リリース 8.2 以前を実行する暗号化された電話は ICT および H.323 コールの場合 RTP に戻り、メディアは暗号化されません。

会議に SIP トランクが使用される場合、セキュアな会議のステータスは非セキュアになります。さらに、SIP トランク シグナリングはクラスタ外の参加者へのセキュアな会議通知をサポートしていません。

CDR データ

CDR データは、電話エンドポイントから会議ブリッジへの各コール レッグのセキュリティ ステータス、および会議自体のセキュリティ ステータスを示します。2 つの値が CDR データベースの内の 2 つの異なるフィールドを使用します。

ミートミー会議において最も低いセキュリティ レベル要件を満たさない加入の試みが拒否される場合、CDR データは終了原因コード 58 を示します（現在ベアラー機能を使用できません）。詳細については、『*CDR Analysis and Reporting Administration Guide*』を参照してください。

連携動作と制限事項

ここでは、次のトピックについて説明します。

- Cisco Unified Communications Manager のセキュアな会議とのインタラクション （249 ページ）
- Cisco Unified Communications Manager のセキュアな会議に関する制限事項 （250 ページ）

Cisco Unified Communications Manager のセキュアな会議とのインタラクション

このセクションでは、Unified Communications Manager とセキュア会議機能との間のインタラクションについて説明します。

- 会議をセキュアに保つため、セキュアなアドホック会議の参加者がコールを保留またはパークした場合は、[Suppress MOH to Conference Bridge] サービス パラメータが [False] に設定されている場合でも、システムは MOH を再生しません。セキュア会議のステータスは変わりません。
- クラスタ間環境では、セキュアなアドホック会議でクラスタ外の会議参加者が保留を押した場合に、そのデバイスへのメディア ストリームが停止し、MOH が再生され、メディア ステータスは不明に変わります。クラスタ外の参加者が MOH の保留コールを再開すると、会議のステータスがアップグレードされます。
- クラスタ間トランク（ICT）を介したセキュアなミートミー通話では、リモート ユーザが保留/再開のような電話の機能を作動させると、コールがクリアされ、メディア ステータスが不明に変わります。
- セキュアなアドホック会議の間に参加者の電話で再生される Unified Communications Manager のマルチレベル優先度およびプリエンプションの告知トーンや告知は、会議ステータスを非セキュアに変更します。
- 発信者がセキュアな SCCP 電話コールに割り込む場合、システムはターゲット デバイスで内部トーン再生メカニズムを使用し、会議ステータスはセキュアのままになります。
- 発信者がセキュアな SIP 電話コールに割り込む場合、システムは保留トーンを再生し、トーン再生中の会議ステータスは非セキュアのままになります。
- 会議がセキュアであり、RSVP が有効化されている場合、会議はセキュアなままになります。
- PSTN が関係する電話会議の場合、セキュリティ会議アイコンにはそのコールの IP ドメイン部分のみのセキュリティ ステータスが表示されます。
- 会議の長さの上限は、[Maximum Call Duration Timer] サービス パラメータでも制御できます。
- 会議ブリッジは、パケット キャプチャをサポートします。メディア ストリームが暗号化されている場合でも、パケット キャプチャ セッション中に、電話には会議について非セキュアのステータスが表示されます。
- システムに設定されたメディア セキュリティ ポリシーによって、セキュア会議の動作が変化する場合があります。たとえば、メディアセキュリティをサポートしていないエンドポイントとの電話会議に参加している場合でも、エンドポイントではシステムのメディア セキュリティ ポリシーに従ってメディア セキュリティが使用されます。

Cisco Unified Communications Manager のセキュアな会議に関する制限事項

このセクションでは、セキュア会議機能に関する Unified Communications Manager の制限事項について説明します。

- 暗号化された Cisco IP Phone でリリース 8.2 以前が実行されている場合、セキュア会議には認証済みまたは非セキュア参加者としてのみ参加できます。
- リリース 8.3 の Cisco Unified IP Phone で、以前のリリースの Unified Communications Manager が使用されている場合、電話会議の間、会議のセキュリティ ステータスではなく接続のセキュリティ ステータスが表示され、会議リストなどのセキュア会議機能もサポートされません。
- Cisco Unified IP Phone 7800 および 7911G では、会議リストがサポートされません。
- 帯域幅の要件のため、Cisco Unified IP Phone 7942 と 7962 は、アクティブな暗号化されたコールでの暗号化されたデバイスからの割り込みをサポートしません。割り込みの試行は失敗します。
- Cisco Unified IP Phone 7931G では、会議チェーンがサポートされません。
- SIP トランクを介して発信している電話は、デバイスのセキュリティ ステータスにかかわらず、非セキュアな電話として扱われます。
- セキュアな電話が SIP トランクを介してセキュアなミートミー会議に参加しようとした場合、コールは切断されます。SIP トランクでは SIP を実行中の電話に対する「「device not authorized」」メッセージの提供がサポートされていないため、電話がこのメッセージで更新されることはありません。さらに、SIP を実行中の 7962G 電話では、「「device not authorized」」メッセージがサポートされません。
- クラスタ間環境では、クラスタ外の参加者に会議リストが表示されません。ただし、クラスタ間の接続でサポートされていれば、接続のセキュリティ ステータスが [Conference] ソフトキーの隣に表示されます。たとえば、H.323 ICT 接続では、認証アイコンは表示されませんが（システムは認証済み接続を非セキュアとして扱う）、暗号化されている接続の暗号化アイコンは表示されます。

  クラスタ外の参加者は、クラスタ境界を越えて別のクラスタに接続する独自の会議を作成できます。システムは、接続された会議を基本的な 2 者間コールとして処理します。

会議リソースの保護のヒント

セキュアな会議ブリッジ リソースを設定する前に、次の点を考慮してください。

- セキュアな会議メッセージのカスタムテキストを電話に表示するには、ローカリゼーションを使用します。詳細については、Unified Communications Manager のロケール インストーラのマニュアルを参照してください。

- 会議または組み込みブリッジでは、電話会議を保護するために暗号化がサポートされている必要があります。
- セキュアな会議ブリッジ登録を有効にするには、クラスタ セキュリティ モードを混合モードに設定します。
- セキュアな会議ブリッジを確立するために、会議を開始する電話が認証済みまたは暗号化済みであることを確認します。
- 共有回線での会議の整合性を維持するためには、回線を共有するデバイスをさまざまなセキュリティ モードで設定しないでください。たとえば、暗号化済み電話が認証済みまたは非セキュアな電話と回線を共有するようには設定しないでください。
- クラスタ間で会議のセキュリティ ステータスを共有したい場合、ICT として SIP トランクを使用しないでください。
- クラスタ セキュリティ モードを混合モードに設定する場合、DSP ファームで設定されているセキュリティ モード（非セキュアまたは暗号化済み）は [Unified Communications Manager Administration] での会議ブリッジ セキュリティ モードに一致する必要があります。そうでないと、会議ブリッジは登録できません。両方のセキュリティ モードが暗号化済みと指定されていれば、会議ブリッジは暗号化済みとして登録されます。両方のセキュリティ モードが非セキュアと指定されていれば、会議ブリッジは非セキュアとして登録されます。
- クラスタ セキュリティ モードを混合モードに設定した場合で、会議ブリッジに適用したセキュリティ プロファイルが暗号化済み、会議ブリッジのセキュリティ レベルが非セキュアという場合は、Unified Communications Manager は会議ブリッジ登録を拒否します。
- クラスタ セキュリティ モードを非セキュア モードに設定する場合、DSP ファームのセキュリティ モードを非セキュアとして設定します。これにより会議ブリッジを登録できます。Unified Communications Manager Administration の設定が暗号化済みとして指定されていても、会議ブリッジは非セキュアとして登録します。
- 登録時に、会議ブリッジは認証に合格する必要があります。認証に合格するには、DSP ファーム システムに 1 つ以上の Unified Communications Manager の CallManager.pem 証明書が含まれ、Unified Communications Manager の CallManager の信頼性ストアに DSP ファーム システムと DSP 接続の証明書が含まれている必要があります。X.509 サブジェクト属性で指定された共通名は、associate **profile <profile-identifier> register <device-name>?** コマンドを使用して、Cisco Unified Communications Manager および DSP ファーム システムで定義された会議ブリッジ名から始まる必要があります。サブジェクト代替名属性はサポートされていません。たとえば、証明書サブジェクトの共通名が ?CN=example.cisco.com? の場合、Unified Communications Manager の会議ブリッジ名は ?example? で、DSP ファーム システム コマンドは **?associate profile <profile-identifier> register** example である必要があります。同じ DSP ファーム システムに複数のセキュアな会議ブリッジがある場合、それぞれ別々の証明書が必要です。
- 会議ブリッジの証明書が何らかの理由で期限切れまたは変更された場合は、Cisco Unified Communications Operating System Administration の証明書の管理機能を使用して信頼ストアの証明書を更新します。証明書が一致しないと TLS 認証が失敗し、また会議ブリッジが

動作しません。これは、会議ブリッジが Unified Communications Manager に登録できないためです。

- セキュアな会議ブリッジは、ポート 2443 で TLS 接続を介して Unified Communications Manager に登録されます。非セキュアな会議ブリッジは、ポート 2000 で TCP 接続を介して Unified Communications Manager に登録されます。
- 会議ブリッジのデバイス セキュリティ モードを変更するには、Unified Communications Manager デバイスのリセットと Cisco CallManager サービスの再起動が必要です。

セキュアな会議ブリッジのセットアップ

次の手順は、セキュアな会議をご使用のネットワークに追加するための手順を示します。

手順

ステップ 1 Cisco CTL クライアントをインストールし、混合モードに設定したことを確認します。

ステップ 2 信頼ストアへの Unified Communications Manager 証明書の追加も含め、Unified Communications Manager 接続用の DSP ファーム セキュリティを設定したことを確認します。DSP ファームのセキュリティ レベルを暗号化済みに設定します。

ご使用の会議ブリッジのマニュアルを参照してください。

ヒント DSP ファームは、ポート 2443 で Unified Communications Manager への TLS ポート接続を確立します。

ステップ 3 DSP ファーム証明書が CallManager 信頼ストア内にあることを確認してください。

証明書を追加するには、Cisco Unified Communications オペレーティング システムの証明書管理機能を使用して DSP 証明書を Unified Communications Manager 内の信頼ストアにコピーします。

証明書のコピーが終わったら、サーバで Cisco CallManager サービスを再起動します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』および『*Cisco Unified Serviceability Administration Guide*』を参照してください。

ヒント 証明書はクラスタ内の各サーバに必ずコピーし、クラスタ内の各サーバで Cisco CallManager サービスを再起動する必要があります。

ステップ 4 Unified Communications Manager の管理ページで、Cisco IOS Enhanced Conference Bridge を会議ブリッジ タイプとして設定し、暗号化済み会議ブリッジをデバイスのセキュリティ モードとして選択します。

ヒント 今回のリリースにアップグレードすると、Unified Communications Manager は自動的に非セキュアな会議ブリッジセキュリティ プロファイルを Cisco IOS Enhanced Conference Bridge 設定に割り当てます。

ステップ 5 ミートミー会議の最小セキュリティ レベルを設定します。

ヒント 今回のリリースにアップグレードすると、Unified Communications Manager は最小セキュリティ レベルとして非セキュアをすべてのミートミー パターンに自動的に割り当てます。

ステップ 6 セキュアな会議ブリッジのパケット キャプチャを設定します。

詳細については、『*Troubleshooting Guide for Unified Communications Manager*』を参照してください。

ヒント パケット キャプチャ モードをバッチ モードに設定し、キャプチャ層を SRTP に設定します。

Cisco Unified Communications Manager Administration でのセキュアな会議ブリッジの設定

[Unified Communications Manager Administration] でセキュアな会議ブリッジを設定するには、次の手順を実行します。会議ブリッジに暗号化を設定した後、Unified Communications Manager の各デバイスをリセットして、Cisco CallManager サービスを再起動する必要があります。

デバイス間の接続をセキュリティで保護するために、Unified Communications Manager と DSP ファームにそれぞれ証明書をインストールしたことを確認してください。

始める前に

はじめる前に

手順

ステップ 1 **[Media Resources]** > **[Conference Bridge]** を選択します。

ステップ 2 [Find and List Conference Bridges] ウィンドウで、Cisco IOS Enhanced Conference Bridge がインストールされていることを確認してから、セキュアな会議ブリッジのセットアップ（252 ページ）に進みます。

ステップ 3 デバイスがデータベース内に存在しない場合は、[Add New] をクリックして、Cisco Unified Communications Manager Administration でのセキュアな会議ブリッジの設定（253 ページ）に進みます。

ステップ 4 [Conference Bridge Configuration] ウィンドウで、[Conference Bridge Type] ドロップダウン リスト ボックスから [Cisco IOS Enhanced Conference Bridge] を選択します。『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って、[会議ブリッジ名（Conference Bridge Name）]、[説明（Description）]、[デバイス プール（Device Pool）]、[共通デバイス設定（Common Device Configuration）]、および [ロケーション（Location）] の設定を行います。

ステップ 5 [Device Security Mode] フィールドで、[Encrypted Conference Bridge] を選択します。
ステップ 6 **[保存（Save）]** をクリックします。
ステップ 7 [リセット（Reset）] をクリックします。

次のタスク

その他の会議ブリッジ設定タスクを実行するために、[Related Links] ドロップダウンリスト ボックスからオプションを選択して **[Go]** をクリックし、[Meet-Me Number/Pattern Configuration] ウィンドウまたは [Service Parameter Configuration] ウィンドウに移動できます。

ミートミー会議の最小セキュリティ レベルの設定

ミートミー会議の最小セキュリティ レベルを設定するには、次の手順を実行します。

手順

ステップ 1 **[Call Routing]** > **[Meet-Me Number/Pattern]** を選択します。
ステップ 2 [Find and List Conference Bridges] ウィンドウで、ミートミー番号/パターンが設定されていることを確認してから、セキュアな会議ブリッジのセットアップ （252 ページ）に進みます。
ステップ 3 ミートミー番号/パターンが設定されていない場合は、[Add New] をクリックして、ミートミー会議の最小セキュリティ レベルの設定 （254 ページ）に進みます。
ステップ 4 [Meet-Me Number Configuration] ウィンドウで、[Directory Number or Pattern] フィールドにミートミー番号または範囲を入力します。『*Feature Configuration Guide for Cisco Unified Communications Manager*』の説明に従って、[Description] と [Partition] の設定を行います。
ステップ 5 [Minimum Security Level] フィールドで、[Non Secure]、[Authenticated] または [Encrypted] を選択します。
ステップ 6 **[Save]** をクリックします。

次のタスク

セキュアな会議ブリッジをまだインストールしていない場合は、セキュアな会議ブリッジをインストールして設定します。

セキュアな会議ブリッジのパケット キャプチャの設定

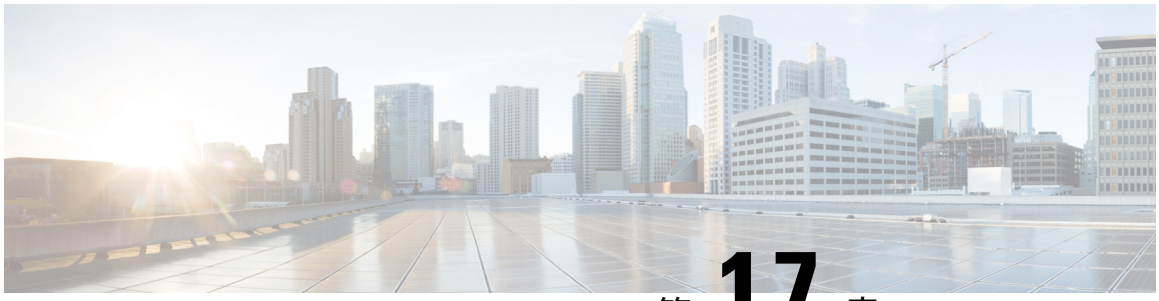
セキュアな会議ブリッジにパケット キャプチャを設定するには、[Service Parameter Configuration] ウィンドウでパケット キャプチャを有効にしてから、デバイス設定ウィンドウで、電話、ゲートウェイ、またはトランクに対してパケット キャプチャ モードをバッチ モードに設定し、キャ

プチャ層を SRTP に設定します。詳細については、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

メディア ストリームが暗号化されている場合でも、パケット キャプチャ セッション中に、電話には会議について非セキュアのステータスが表示されます。

セキュアな会議リソースに関する詳細情報の入手先

- システム要件 （7 ページ）
- 連携動作と制限事項 （10 ページ）
- 証明書 （19 ページ）
- 認証と暗号化のセットアップ （39 ページ）



第 17 章

ボイス メッセージング ポートのセキュリティ設定

この章では、ボイス メッセージング ポート セキュリティの設定について説明します。

ボイス メッセージング セキュリティ

Unified Communications Manager ボイス メッセージング ポートおよび SCCP を実行している Cisco Unity デバイス、または SCCP を実行している Cisco Unity Connection デバイスでセキュリティを設定するには、ポートのセキュアなデバイス セキュリティ モードを選択します。認証済みのボイス メール ポートを選択すると TLS 接続が開始され、相互証明書交換を使用してデバイスが認証されます（各デバイスが他のデバイスの証明書を受け入れます）。暗号化されたボイス メール ポートを選択すると、システムはまずデバイスを認証し、デバイス間で暗号化された音声ストリームを送信します。

Cisco Unity Connection 2.0 以降では、TLS ポート経由で Unified Communications Manager に接続します。デバイス セキュリティ モードが非セキュアになると、Cisco Unity Connection は、SCCP ポート経由で Unified Communications Manager に接続します。

（注） この章で使用されている用語「「サーバ」」は、Unified Communications Manager サーバを示します。「「ボイス メールサーバ」」は Cisco Unity サーバまたは Cisco Unity Connection サーバを示します。

ボイス メッセージング セキュリティの設定のヒント

セキュリティの設定の前に次の事項に注意してください。

- Cisco Unity では、Cisco Unity Telephony Integration Manager (UTIM) を使用してセキュリティ タスクを実行する必要があります。Cisco Unity Connection では、Cisco Unity Connection Administration を使用してセキュリティ タスクを実行する必要があります。これらのタスクの実行方法については、Cisco Unity 向け、または Cisco Unity Connection 向けの『Unified Communications Manager integration guide』を参照してください。
- Cisco Unity 証明書を信頼ストアに保存するには、この章で説明している手順に加え、Unified Communications Manager の証明書の管理機能を使用する必要があります。

  詳細については、以下の URL にある『*Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection*』の「「To Add Voice Messaging Ports in Cisco Unity Connection Administration」」の手順を参照してください。

  http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/integration/guide/cucm_sccp/guide/cucintcucmskinny230.html

  証明書をコピーした後、クラスタ内の各 Unified Communications Manager サーバで Cisco CallManager サービスを再起動する必要があります。
- Cisco Unity 証明書が期限切れになったか、何らかの理由で変更された場合は、『*Administration Guide for Cisco Unified Communications Manager*』の証明書の管理機能を使用して信頼ストアの証明書を更新します。証明書が一致しないと TLS 認証が失敗し、ボイス メッセージングが機能しません。これは、ボイス メッセージング機能が Unified Communications Manager に登録できないためです。
- ボイスメール サーバのポートを設定するときには、デバイス セキュリティ モードを選択する必要があります。
- Cisco Unity Telephony Integration Manager (UTIM) または Cisco Unity Connection Administration で指定する設定は、Unified Communications Manager Administration で設定されているボイス メッセージング ポートのデバイス セキュリティ モードと一致する必要があります。Cisco Unity Connection Administration の [Voice Mail Port Configuration] ウィンドウ（または [Voice Mail Port] ウィザード）で、ボイス メッセージング ポートにデバイス セキュリティ モードを適用します。

ヒント デバイス セキュリティ モードの設定が一致しないと、Unified Communications Manager でのボイスメール サーバ ポートの登録は失敗し、ボイスメール サーバは登録が失敗したポートへのコールに対応できません。

- ポートのセキュリティ プロファイルを変更するには、Unified Communications Manager デバイスのリセットとボイスメール サーバ ソフトウェアの再起動が必要です。Unified Communications Manager Administration で以前と異なるデバイス セキュリティ モードを使

用するセキュリティ プロファイルを適用するには、ボイスメール サーバの設定を変更する必要があります。

- [VoiceMail Port] ウィザードで既存のボイスメール サーバのデバイス セキュリティ モードを変更することはできません。既存のボイス メール サーバにポートを追加すると、現在プロファイルに設定されているデバイス セキュリティ モードは自動的に新しいポートに適用されます。

単一のボイス メッセージング ポートへのセキュリティ プロファイルの適用

単一のボイス メッセージング ポートにセキュリティ プロファイルを適用するには、次の手順を実行します。

この手順では、デバイスをデータベースに追加済みで、既存の証明証がない場合には、電話に新たな証明書をインストールしていることを前提としています。セキュリティ プロファイルを初めて適用した後、またはセキュリティ プロファイルを変更した場合は、デバイスをリセットする必要があります。

始める前に

セキュリティ プロファイルを適用する前に、ボイス メッセージングのセキュリティとボイス メッセージング ポートのセキュアなセットアップに関連するトピックを確認してください。

手順

ステップ 1 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って、ボイス メッセージング ポートを検索します。

ステップ 2 ポートの設定ウィンドウが表示されたら、[Device Security Mode] 設定を見つけます。ドロップダウン リスト ボックスから、ポートに適用するセキュリティ モードを選択します。データベースでは次のオプションが事前に定義されています。デフォルト値は、[Not Selected] に指定されています。

ステップ 3 **[保存（Save）]** をクリックします。

ステップ 4 [リセット（Reset）] をクリックします。

ボイスメールポートウィザードを使用するセキュリティプロファイルの適用

[Voice Mail Port] ウィザードの [Device Security Mode] 設定を新しいボイス メール サーバに適用するには、次の手順を使用します。

既存のボイス メール サーバのセキュリティ設定を変更するには、単一のボイス メール ポートへのセキュリティ プロファイルの適用に関するトピックを参照してください。

始める前に

セキュリティ プロファイルを適用する前に、ボイス メッセージングのセキュリティとボイス メッセージング ポートのセキュアなセットアップに関連するトピックを確認してください。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[Voice Mail]** > **[Cisco Voice Mail Port Wizard]** を選択します。

ステップ 2 ボイス メール サーバの名前を入力し、[Next] をクリックします。

ステップ 3 追加するポートの数を選択し、[Next] をクリックします。

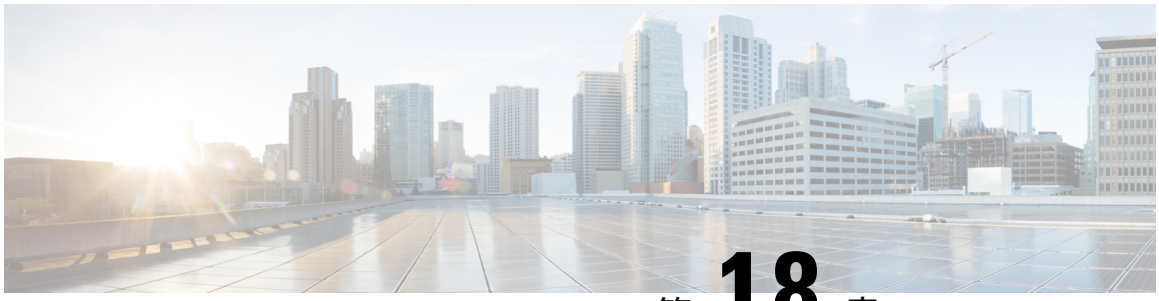
ステップ 4 [Cisco Voice Mail Device Information] ウィンドウで、ドロップダウン リスト ボックスから [Device Security Mode] を選択します。データベースでは次のオプションが事前に定義されています。デフォルト値は、[Not Selected] に指定されています。

ステップ 5 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って、他のデバイス設定を行います。[次へ（Next）] をクリックします。

ステップ 6 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って、設定プロセスを続けます。[Summary] ウィンドウが表示されたら、[Finish] をクリックします。

ボイスメッセージングセキュリティに関する詳細情報の入手先

- システム要件 （7 ページ）
- 認証と暗号化のセットアップ （39 ページ）
- 証明書 （19 ページ）



第 18 章

コール セキュア ステータス ポリシー

コール セキュア ステータス ポリシーについて

コール セキュア ステータス ポリシーでは、電話でのセキュア ステータス アイコンの表示が制御されます。ポリシーのオプションは次のとおりです。

- [All media except BFCP and iX application streams must be encrypted]

  これはデフォルト値です。コールのセキュリティ ステータスは、BFCP アプリケーション ストリームと iX アプリケーション ストリームの暗号化ステータスに左右されません。

- [All media except iX application streams must be encrypted]

  コールのセキュリティ ステータスは、iX アプリケーション ストリームの暗号化ステータスに左右されません。

- [All media except BFCP application streams must be encrypted]

  コールのセキュリティ ステータスは、BFCP の暗号化ステータスに左右されません。

- [All media in a session must be encrypted]

  コールのセキュリティ ステータスは、確立されている電話セッションのすべてのメディア ストリームの暗号化ステータスに左右されます。

- [Only Audio must be encrypted]

  コールのセキュリティ ステータスは、オーディオ ストリームの暗号化に左右されます。

（注） ポリシーに変更を加えると、電話でのセキュア アイコンの表示とセキュア トーンの再生に影響します。

コール セキュア ステータス ポリシーの設定

手順

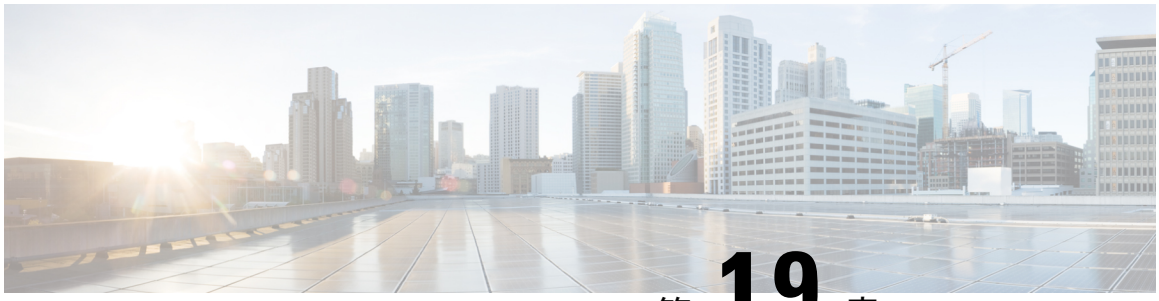
ステップ 1 『*Cisco Unified Communications Manager* システム コンフィギュレーション ガイド』の「サービス パラメータの設定」セクションに記載された説明に従って、[コール セキュア ステータス ポリシー（Call Secure Status Policy）] サービス パラメータを検索します。

ステップ 2 [Secure Call Icon Display Policy] ドロップダウンリストから、ポリシー オプションを選択します。

ビデオ コールとセキュア トーンへの影響に関する警告メッセージが表示されます。

ステップ 3 **[保存 (Save)]** をクリックします。

ウィンドウの内容が更新され、Unified Communications Manager によってサービス パラメータが変更内容で更新されます。



第 19 章

セキュアなコールのモニタリングおよび録音のセットアップ

この章では、セキュアなコールのモニタリングおよび録音のセットアップについて説明します。

セキュアコールのモニタリングと録音のセットアップについて

セキュア コールは、この項で説明するようにモニタリングおよび録音を行えます。

- スーパバイザは、セキュア コールまたは非セキュア コールに対してセキュアなモニタリング セッションを確立できます。
- 元のコールのコール セキュリティが、コール モニタリング要求の結果として、影響を受けたりダウングレードされたりすることは決してありません。
- モニタリング コールは、エージェントのデバイス機能と同じセキュリティ レベルで確立および維持できる場合に限り続行できます。
- エージェントとお客様間の元のコールには、モニタリング コールの暗号キーとは異なる暗号キーが必要です。モニタリングセッションでは、システムによってまずエージェントとお客様の混合音声が新しいキーで暗号化され、その後スーパバイザに送信されます。

（注） 認証された電話でのセキュアな録音またはセキュアでない録音はサポートされていません。

Unified Communications Manage は、安全でないレコーダーを使用しているときに、認証された電話の通話の録音をサポートしています。セキュアコールレコーダーを使用したコールの場合、レコーダーが SRTP フォールバックをサポートしている場合に限り録音が許可され、レコーダーに対するメディアストリームが RTP にフォールバックされます。

認証済みの電話機を使用したコールを録音するには:

- **電話を許可する**には、Cisco callmanager Service パラメータで**認証済みの電話録音**を設定します。この場合、コールは認証されますが、録音サーバへの接続は非認証であり、暗号化されません。
- **クラスタ SIPOAuth Mode**フィールドが Cisco callmanager enterprise パラメータであることを確認します。**[有効 (Enabled)]** に設定されていることを確認します。

セキュアなコールのモニタリングと録音のセットアップ

セキュアなコールのモニタリングと録音を設定するには、次の手順を実行します。

手順

ステップ 1 エージェントとスーパバイザの電話にセキュリティ機能をプロビジョニングします。

ステップ 2 次の設定を使用して、セキュアな SIP トランクを作成します。

- [Device Security Mode] を [Encrypted] に設定します。
- [Transmit Security Status] チェックボックスをオンにします。
- [SRTP Allowed] チェックボックスをオンにします。
- TLS SIP トランクをレコーダに設定します。

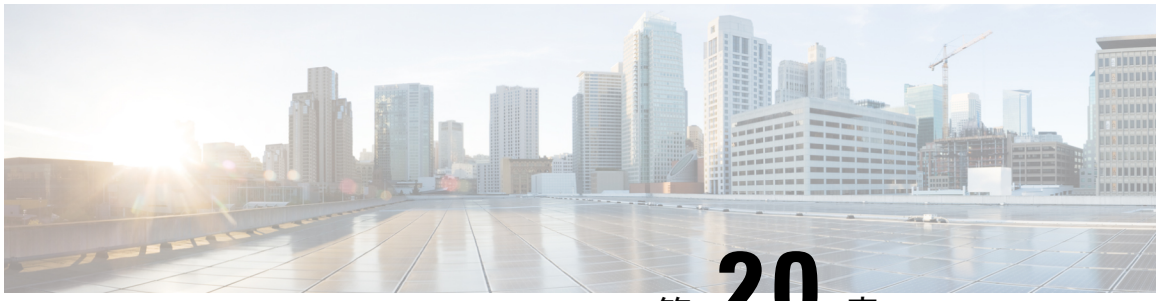
ステップ 3 非セキュアな場合と同様にモニタリングと録音を設定します。

a) エージェントの電話のビルトイン ブリッジを設定します。
b) エージェントの電話の DN ページを使用して、[Recording Option]（[Automatic Call Recording Enabled] と [Application Invoked Call Recording Enabled]）を設定します。
c) レコーダのルート パターンを作成します。
d) DN に通話録音プロファイルを追加します。
e) 必要に応じてモニタリング トーンと録音トーンをプロビジョニングします。

手順の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』の「「Monitoring and Recording」」の章を参照してください。

第 IV 部

Cisco Unified IP Phone のバーチャル プライベート ネットワーク



第 20 章

VPN クライアント

VPN クライアントの概要

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

（注） [VPN] メニューおよびこのメニューのオプションは、Unified Communications Manager の U.S. 輸出制限バージョンでは使用できません。

VPN クライアントの前提条件

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

VPN クライアント設定のタスク フロー

始める前に

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco IOS の前提条件の完了 （269 ページ）	Cisco IOS の前提条件を満たします。Cisco IOS VPN を設定するには、このアクションを実行します。
ステップ 2	IP Phone をサポートするための Cisco IOS SSL VPN の設定 （270 ページ）	IP Phone で VPN クライアントの Cisco IOS を設定します。Cisco IOS VPN を設定するには、このアクションを実行します。
ステップ 3	AnyConnect 用の ASA 前提条件への対応 （271 ページ）	AnyConnect の ASA 前提条件を満たします。ASA VPN を設定するには、このアクションを実行します。
ステップ 4	IP Phone での VPN クライアント用の ASA の設定 （272 ページ）	IP Phone で VPN クライアントの ASA を設定します。ASA VPN を設定するには、このアクションを実行します。
ステップ 5	VPN ゲートウェイごとに VPN コンセントレータを設定します。	リモート電話のファームウェアや設定情報をユーザがアップグレードする際の長い遅延を回避するには、ネットワーク内で TFTP サーバまたは Unified Communications Manager サーバの近くで VPN コンセントレータをセットアップします。これがネットワーク内で不可能な場合、代替 TFTP サーバまたはロード サーバを VPN コンセントレータの横にセットアップすることもできます。
ステップ 6	VPN コンセントレータの証明書のアップロード （275 ページ）	VPN コンセントレータの証明書をアップロードします。
ステップ 7	VPN ゲートウェイの設定 （275 ページ）	VPN ゲートウェイを設定します。
ステップ 8	VPN グループの設定 （277 ページ）	VPN グループを作成した後、設定した VPN ゲートウェイのいずれかをそのグループに追加できます。

	コマンドまたはアクション	目的
ステップ 9	次のいずれかの操作を行います。 • VPN プロファイルの設定 （278 ページ） • VPN 機能のパラメータの設定 （279 ページ）	VPN プロファイルを設定する必要があるのは、複数の VPN グループを使用している場合だけです。[VPN Profle] フィールドは、[VPN Feature Configuration] フィールドよりも優先されます。
ステップ 10	共通の電話プロファイルへの VPN の詳細の追加 （281 ページ）	共通の電話プロファイルに VPN グループおよび VPN プロファイルを追加します。
ステップ 11	Cisco Unified IP 電話 のファームウェアを、VPN をサポートしているバージョンにアップグレードします。	Cisco VPN クライアントを実行するには、サポートされている Cisco Unified IP 電話 でファームウェア リリース 9.0(2) 以降が稼動している必要があります。ファームウェアのアップグレード方法の詳細は、ご使用の Cisco Unified IP 電話 のモデルの Unified Communications Manager 向け『*Cisco Unified IP Phone Administration Guide*』を参照してください。
ステップ 12	サポートされている Cisco Unified IP 電話 を使用して、VPN 接続を確立します。	Cisco Unified IP 電話 を VPN に接続します。

Cisco IOS の前提条件の完了

手順

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

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

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

ステップ 2 SSL VPN ライセンスをアクティベートします。

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

手順

ステップ 1 Cisco IOS をローカルで設定します。

a) ネットワーク インターフェイスを設定します。

例：

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

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

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

例：

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

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

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

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

（注） この場所は Unified Communications Manager のバージョンによって変わります。

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

c) Cisco IOS ソフトウェア上にトラストポイントを作成します。

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

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

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

- 自己署名証明書を生成します。

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 1024 1024
```

```
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

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

  例:

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

- 生成した証明書を Unified Communications Manager に登録します。

  例:

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

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

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

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

例：

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

ステップ 5 VPN 機能を設定します。

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

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
```

AnyConnect 用の ASA 前提条件への対応

手順

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

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

ステップ 3 ライセンスをアクティベートします。

a) 次のコマンドを使用して、現在のライセンスの機能を確認してください。

show activation-key detail

b) 必要に応じて、追加の SSL VPN セッションと LINKSYS 電話が有効になっている新しいライセンスを取得します。

ステップ 4 デフォルト以外の URL を使用してトンネル グループが設定されていることを次のように確認してください。

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

デフォルト以外の URL を設定するときは、次のことを考慮してください。

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

IP Phone での VPN クライアント用の ASA の設定

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

手順

ステップ 1 ローカル設定

a) ネットワーク インターフェイスを設定します。

例：

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto
```

```
ciscoasa(config-if)# speed auto
ciscoasa(config-if)# no shutdown
ciscoasa#show interface ip brief (shows interfaces summary)
```

b) スタティック ルートとデフォルト ルートを設定します。

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

例：

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

c) DNS を設定します。

例：

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

ステップ 2 Unified Communications Manager と ASA に必要な証明書を生成および登録します。

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

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

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

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

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

c) ASA でトラストポイントを作成します。

例：

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

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

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

- 自己署名証明書を生成します。

  例：

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

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

  例:

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

- 生成した証明書を Unified Communications Manager に登録します。

  例:

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

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

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

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

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

ASA 証明書の設定

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

VPN コンセントレータの証明書のアップロード

VPN 機能をサポートするようにセットアップする際に、ASA で証明書を生成します。生成された証明書を PC またはワークステーションにダウンロードしてから、この項で説明されている手順を使用して Unified Communications Manager にアップロードします。Unified Communications Manager は、電話と VPN 間の信頼リストに証明書を保存します。

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

Cisco Unified IP 電話 は、製造元でインストールされる証明書（MIC）をデフォルトで送信します。CAPF サービスを設定すると、Cisco Unified IP 電話 はローカルで有効な証明書（LSC）を送信します。

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

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

手順

ステップ 1 Cisco Unified OS 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 **[証明書のアップロード（Upload Certificate）]** をクリックします。

[証明書のアップロード（Upload Certificate）] ダイアログボックスが表示されます。

ステップ 3 [証明書の目的（Certificate Purpose）] ドロップダウンリストで、[Phone-VPN-trust] を選択します。

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

ステップ 5 [ファイルのアップロード（Upload File）] をクリックします。

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

証明書管理の詳細については、「『Administration Guide for Cisco Unified Communications Manager』」を参照してください。

VPN ゲートウェイの設定

始める前に

VPN ゲートウェイごとに VPN コンセントレータが設定されていることを確認します。VPN コンセントレータの設定後、VPN コンセントレータの証明書をアップロードします。詳細については、VPN コンセントレータの証明書のアップロード （275 ページ）を参照してください。

手順

ステップ 1 [Cisco Unified CM Administration] から、以下を選択します。 **[拡張機能（Advanced Features）]** > **[VPN]** > **[VPN ゲートウェイ（VPN Gateway）]**。

ステップ 2 次のいずれかの作業を実行します。

a) 新しいプロファイルを設定するには、**[新規追加（Add New）]** をクリックします。
b) コピーする VPN ゲートウェイの横にある **[コピー（Copy）]** をクリックします。
c) 既存のプロファイルを更新するには、適切な VPN ゲートウェイを見つけて、設定を変更します。

ステップ 3 [VPN Gateway Configuration] ウィンドウでフィールドを設定します。詳細については、VPN クライアントの VPN ゲートウェイ フィールド （276 ページ）を参照してください。

ステップ 4 **[保存 (Save)]** をクリックします。

VPN クライアントの VPN ゲートウェイ フィールド

表 *28 : VPN* クライアントの *VPN* ゲートウェイ フィールド

フィールド	説明
[VPN Gateway Name]	VPN ゲートウェイの名前を入力します。
[VPN Gateway Description]	VPN ゲートウェイの説明を入力します。
[VPN Gateway URL]	ゲートウェイのメイン VPN コンセントレータの URL を入力します。 （注） VPN コンセントレータにグループ URL を設定し、この URL をゲートウェイ URL として使用する必要があります。 設定についての情報は、以下のような VPN コンセントレータのドキュメントを参照してください。 • 『*SSL VPN Client (SVC) on ASA with ASDM Configuration Example*』
[VPN Certificates in this Gateway]	上矢印キーと下矢印キーを使用して、ゲートウェイに証明書を割り当てます。ゲートウェイに証明書を割り当てないと、VPN クライアントはこのコンセントレータへの接続に失敗します。 （注） VPN ゲートウェイには最大 10 の証明書を割り当てることができます。各ゲートウェイに少なくとも 1 つの証明書を割り当てる必要があります。Phone-VPN-trust 権限に関係付けられた証明書だけが、使用可能な VPN 証明書のリストに表示されます。

VPN グループの設定

手順

ステップ 1 [Cisco Unified CM Administration] から、以下を選択します。 **[高度な機能（Advanced Features）]** > **[VPN]** > **[VPN グループ（VPN Group）]**。

ステップ 2 次のいずれかの作業を実行します。

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

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

c) 既存のプロファイルを更新するには、適切な VPN グループを見つけて、その設定を変更します。

ステップ 3 [VPN Group Configuration] ウィンドウ内の各フィールドを設定します。詳細については、「VPN クライアントの VPN ゲートウェイ フィールド （276 ページ）」のフィールド説明詳細を参照してください。

ステップ 4 **[保存 (Save)]** をクリックします。

VPN クライアントの VPN グループ フィールド

表 *29 : VPN* クライアントの *VPN* グループ フィールド

フィールド	定義
[VPN Group Name]	VPN グループの名前を入力します。
[VPN Group Description]	VPN グループの説明を入力します。
[All Available VPN Gateways]	スクロールして、すべての使用可能な VPN ゲートウェイを確認できます。
[Selected VPN Gateways in this VPN Group]	上矢印キーと下矢印キーを使用して、使用可能な VPN ゲートウェイをこの VPN グループの内外に移動します。 VPN クライアントで重大なエラーが発生し、特定の VPN ゲートウェイに接続できない場合は、リストの次の VPN ゲートウェイへの移動を試みます。 （注） 1 つの VPN グループに最大 3 つの VPN ゲートウェイを追加できます。また、VPN グループ内の証明書の合計数は 10 以下にする必要があります。

VPN プロファイルの設定

手順

ステップ 1 [Cisco Unified CM Administration] から、以下を選択します。 **[高度な機能（Advanced Features）]** > **[VPN]** > **[VPN プロファイル（VPN Profile）]**。

ステップ 2 次のいずれかの作業を実行します。

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

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

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

ステップ 3 [VPN Profile Configuration] ウィンドウで各フィールドを設定します。詳細については、「VPN クライアントの VPN プロファイル フィールド （278 ページ）」のフィールド説明詳細を参照してください。

ステップ 4 **[保存 (Save)]** をクリックします。

VPN クライアントの VPN プロファイル フィールド

表 *30 : VPN* プロファイル フィールドの詳細

フィールド	定義
[Name]	VPN プロファイルの名前を入力します。
[Description]	VPN プロファイルの説明を入力します。
[Enable Auto Network Detect]	このチェックボックスをオンにすると、VPN クライアントは、社内ネットワークの外にいることを検出した場合に限り動作します。 デフォルトで、ディセーブルになっています。
[MTU]	最大伝送ユニット（MTU）のサイズをバイト数で入力します。 デフォルト値：1290 バイト
[Fail to Connect]	このフィールドは、システムが VPN トンネルの作成中にログイン操作または接続操作が完了するまで待つ時間を指定します。 デフォルト：30 秒

フィールド	定義
[Enable Host ID Check]	このチェックボックスをオンにした場合は、ゲートウェイの証明書の subjectAltName または CN が、VPN クライアントの接続先の URL と一致している必要があります。 デフォルト：有効
[Client Authentication Method]	ドロップダウンリストからクライアント認証方法を選択します。 • [User and Password] • [Password only] • [Certificate (LSC or MIC)]
[Enable Password Persistence]	このチェックボックスをオンにすると、ログイン試行の失敗、ユーザによるパスワードの手動でのクリア、または電話機のリセットや電源切断が発生するまで、ユーザ パスワードが電話機に保存されます。

VPN 機能のパラメータの設定

手順

ステップ 1 [Cisco Unified CM Administration] から、以下を選択します。 **[高度な機能（Advanced Features）]** > **[VPN]** > **[VPN 機能設定（VPN Feature Configuration）]**。

ステップ 2 [VPN Feature Configuration] ウィンドウのフィールドを設定します。詳細については、VPN 機能のパラメータ （280 ページ）を参照してください。

ステップ 3 **[保存（Save）]** をクリックします。

次のタスク

次の作業を行います。

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

VPN 機能のパラメータ

表 *31 : VPN* 機能のパラメータ

フィールド	デフォルト
[Enable Auto Network Detect]	True の場合、VPN クライアントは、社内ネットワークの外にいることを検出した場合に限り動作します。 デフォルト：False
[MTU]	このフィールドは最大伝送ユニットを指定します。 デフォルト値は 1290 バイトです。 最小値：256 バイト 最大値：1406 バイト
[Keep Alive]	このフィールドは、システムがキープアライブ メッセージを送信するレートを指定します。 （注） Unified Communications Manager で指定した値よりも小さい値（ゼロ以外）を指定した場合、この値は VPN コンセントレータのキープアライブ設定によって上書きされます。 デフォルト：60 秒 最小値：0 最大値：120 秒
[Fail to Connect]	このフィールドは、システムが VPN トンネルの作成中にログイン操作または接続操作が完了するまで待つ時間を指定します。 デフォルト：30 秒 最小値：0 最大値：600 秒
[Client Authentication Method]	ドロップダウンリストからクライアント認証方法を選択します。 • [User and Password] • [Password only] • [Certificate (LSC or MIC)] デフォルト：User And Password

フィールド	デフォルト
[Enable Password Persistence]	[True] の場合、[Reset] ボタンまたは「**#**」 がリセットに使用されると、ユーザ パスワードは電話に保存されます。電話の電源が切断されたり、工場出荷時の状態にリセットされたりすると、パスワードは保存されず電話からクレデンシャルの入力が求められます。 デフォルト：False
[Enable Host ID Check]	[True] の場合、ゲートウェイの証明書の subjectAltName または CN が、VPN クライアントが接続する URL に一致する必要があります。 デフォルト：True

共通の電話プロファイルへの VPN の詳細の追加

手順

ステップ 1 [Cisco Unified CM Administration] から、以下を選択します。 **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）]**。

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

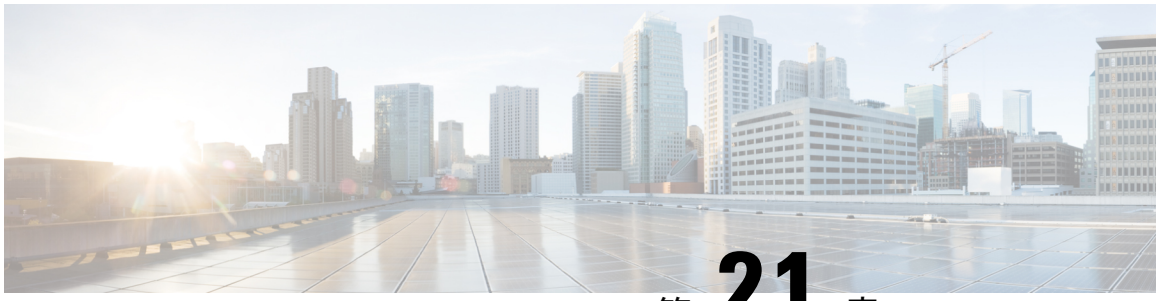
ステップ 3 [VPN情報（VPN Information）] セクションで、適切な [VPNグループ（VPN Group）] および [VPNプロファイル（VPN Profile）] を選択します。

ステップ 4 [保存（Save）]、[設定の適用（Apply Config）] の順にクリックします。

ステップ 5 [設定を適用（Apply Configuration）] ウィンドウで、**[OK]** をクリックします。

第 V 部

Cisco CTI、JTAPI、および TAPI アプリケーションのセキュリティ



第 21 章

CTI、JTAPI、および TAPI の認証および暗号化の設定

この章では、CTI、JTAPI、および TAPI アプリケーションを保護する方法の概要を説明します。また、CTI、TAPI、およびJTAPI アプリケーションの認証と暗号化の設定のため、[Unified Communications Manager Administration] で実行する必要がある作業についても説明します。

このドキュメントでは、[Unified Communications Manager Administration] で使用可能な Cisco JTAPI や TSP プラグインのインストール方法は説明しません。また、インストール中にセキュリティ パラメータを設定する方法についても説明しません。同様に、CTI で制御するデバイスまたは回線に制限を設定する方法も、このドキュメントでは説明しません。

CTI、JTAPI、および TAPI アプリケーションの認証

Unified Communications Manager を使用すれば、CTIManager と CTI/JTAPI/TAPI の各アプリケーションとの間のシグナリング接続およびメディア ストリームを保護できます。

（注） 次の情報は、Cisco JTAPI/TSP プラグインのインストール時にセキュリティ設定を定義したことを前提としています。また、Cisco CTL クライアント、または CLI コマンド セットの **utils ctl** で、クラスタ セキュリティ モードが混合モードに設定されていることも前提としています。この章で説明する作業を実行する際に、これらの設定が定義されていない場合、CTIManager とアプリケーションは非セキュア ポートのポート 2748 で接続されます。

CTIManager およびアプリケーションでは、相互に認証される TLS ハンドシェイク（証明書交換）によって他方のアイデンティティを確認します。TLS 接続が確立されると、CTIManager およびアプリケーションでは、TLS ポートのポート 2749 を介して QBE メッセージを交換します。

CTIManager では、アプリケーションとの認証を行うために、Unified Communications Manager の証明書（インストール時に Unified Communications Manager サーバに自動的にインストールされる自己署名証明書、またはプラットフォームにアップロードしたサードパーティの CA 署名付き証明書のいずれか）を使用します。

CLI コマンド セットの **utils ctl** または Cisco CTL クライアントによって CTL ファイルを生成した後、この証明書は CTL ファイルに自動的に追加されます。アプリケーションでは、CTL ファイルを TFTP サーバからダウンロードした後で、CTIManager への接続を試みます。

JTAPI/TSP クライアントでは、初めて CTL ファイルを TFTP サーバからダウンロードする際に CTL ファイルを信頼します。JTAPI/TSP クライアントでは CTL ファイルを検証しないため、このダウンロードはセキュアな環境で実行することを強く推奨します。JTAPI/TSP クライアントでは、後続の CTL ファイルのダウンロードを検証します。たとえば、CTL ファイルを更新すると、JTAPI/TSP クライアントでは、CTL ファイル内のセキュリティ トークンを使用して、ダウンロードした新しい CTL ファイルのデジタル署名の真正性を認証（確認）します。このファイルの内容には、Unified Communications Manager の証明書と CAPF サーバの証明書が含まれます。

JTAPI/TSP クライアントでは、CTL ファイルが改ざんされていると判断した場合、ダウンロードした CTL ファイルを取り替えません。つまり、クライアントでは、エラーをログに記録し、既存の CTL ファイル内の古い証明書を使用して TLS 接続の確立を試みます。CTL ファイルが変更または改ざんされている場合、正常に接続できないことがあります。CTL ファイルのダウンロードに失敗し、複数の TFTP サーバが存在する場合、このファイルをダウンロードするために別の TFTP サーバを設定できます。JTAPI/TAPI クライアントでは、次の場合、どのポートにも接続しません。

- 何らかの理由（CTL ファイルが存在しないなど）によって、クライアントで CTL ファイルをダウンロードできない場合。

- クライアントに既存の CTL ファイルがない場合。
- アプリケーション ユーザをセキュア CTI ユーザとして設定した場合。

アプリケーションでは、CTIManager との認証を行うために、Certificate Authority Proxy Function（CAPF）で発行する証明書を使用します。アプリケーションと CTIManager との間のすべての接続で TLS を使用するには、アプリケーションの PC で実行されているインスタンスごとに一意の証明書が必要です。1 つの証明書ですべてのインスタンスがカバーされるわけではありません。Cisco IP Manager Assistant サービスが実行されているノードに証明書がインストールされるようにするには、表 32 : アプリケーション ユーザおよびエンド ユーザの CAPF プロファイルの設定 （297 ページ）の説明に従って、[Unified Communications Manager Administration] で、それぞれの [Application User CAPF Profile Configuration] または [End User CAPF Profile Configuration] に一意のインスタンス ID を設定します。

ヒント アプリケーションをある PC からアンインストールして別の PC にインストールする場合、新しい PC のインスタンスごとに新しい証明書をインストールする必要があります。

アプリケーションで TLS を有効にするには、[Unified Communications Manager Administration] で、アプリケーション ユーザまたはエンド ユーザを Standard CTI Secure Connection ユーザ グループに追加する必要もあります。ユーザをこのグループに追加し、証明書をインストールすると、アプリケーションではユーザが TLS ポートを介して接続するようになります。

CTI、JTAPI、および TAPI アプリケーションの暗号化

ヒント 認証は暗号化の最小要件となります。つまり、認証が設定されなければ、暗号化を使用できません。

Unified Communications Manager Assistant、Cisco QRT、および Cisco Web Dialer は暗号化をサポートしていません。CTIManager サービスに接続する CTI クライアントでは、クライアントが音声パケットを送信する場合、暗号化がサポートされることがあります。

アプリケーションと CTIManager との間のメディア ストリームをセキュアにするため、Unified Communications Manager Administration の [標準 CTI に SRTP キー情報の受け入れを許可（Standard CTI Allow Reception of SRTP Key Material）] ユーザ グループにアプリケーション ユーザまたはエンド ユーザを追加します。これらのユーザが Standard CTI Secure Connection ユーザ グループにも存在する場合、およびクラスタ セキュリティ モードが混合モードである場合、CTIManager はアプリケーションとの TLS 接続を確立し、メディア イベントでキー情報をアプリケーションに提供します。

（注） クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ能力を設定します。

アプリケーションでは SRTP キー情報の記録や保存は行われませんが、アプリケーションはキー情報を使用して RTP ストリームを暗号化し、CTIManager からの SRTP ストリームを復号します。

アプリケーションが非セキュア ポートであるポート 2748 に何らかの理由で接続されると、CTIManager はキー情報を送信しません。制限が設定されているために CTI/JTAPI/TAPI からデバイスまたは電話番号のモニタリングや制御が行えない場合、CTIManager はキー情報を送信しません。

ヒント SRTP セッション キーを受け取るアプリケーションの場合、アプリケーション ユーザまたはエンドユーザが、Standard CTI Enabled、Standard CTI Secure Connection、Standard CTI Allow Reception of SRTP Key Material の 3 グループに存在している必要があります。

Unified Communications Manager では CTI ポートおよびルート ポイントとのセキュア コールを使用できますが、メディア パラメータはアプリケーションによって扱われるため、セキュア コールをサポートするようアプリケーションを設定する必要があります。

CTI ポートおよびルート ポイントは、ダイナミック登録またはスタティック登録によって登録されます。ポート/ルート ポイントによってダイナミック登録が使用されると、各コールに対してメディア パラメータが指定されます。スタティック登録が使用されると、メディア パラメータは登録時に指定され、コールごとに変更できません。CTI ポート/ルート ポイントが TLS 接続を介して CTIManager に登録するとき、デバイスはセキュアに登録され、アプリケーションがデバイス登録要求で有効な暗号化アルゴリズムを使用する場合、および他の参加者がセキュアである場合、メディアは SRTP を介して暗号化されます。

CTI アプリケーションは、すでに確立されているコールのモニタリングを開始するときには RTP イベントを受信しません。確立されたコールに対して、CTI アプリケーションは、コールのメディアがセキュアか非セキュアかを判断する DeviceSnapshot イベントを提供します。このイベントではキー情報が提供されません。

CTI、JTAPI、および TAPI アプリケーションの CAPF の機能

Unified Communications Manager と同時に自動的にインストールされる認証局プロキシ機能（CAPF）は、設定に応じて、CTI/TAPI/TAPI アプリケーションについて次のタスクを実行します。

- 認証文字列によって JTAPI/TSP クライアントを認証する。
- CTI/JTAPI/TAPI アプリケーション ユーザまたはエンド ユーザにローカルで有効な証明書（LSC）を発行する。
- 既存のローカルで有効な証明書をアップグレードする。
- 表示やトラブルシューティングのために証明書を取得する。

JTAPI/TSP クライアントが CAPF と対話するとき、クライアントは認証文字列を使用して CAPF に認証されます。その後、クライアントが公開キーと秘密キーのペアを生成し、署名付きメッセージによって公開キーを CAPF サーバに転送します。秘密キーはクライアントに残り、外部に公開されることはありません。証明書は CAPF によって署名され、署名付きメッセージによってクライアントに送り返されます。

アプリケーション ユーザとエンド ユーザには、それぞれ [Application User CAPF Profile Configuration] ウィンドウと [End User CAPF Profile Configuration] ウィンドウでの設定によって証明書を発行できます。Unified Communications Manager でサポートされる CAPF プロファイル間の相違点について、以下に説明します。

- アプリケーション ユーザ CAPF プロファイル：このプロファイルでは、CTIManager サービスとアプリケーションの間で TLS 接続をオープンできるようにするため、セキュアなアプリケーション ユーザに対してローカルで有効な証明書を発行できます。

  1 つのアプリケーション ユーザ CAPF プロファイルが、サーバのサービスまたはアプリケーションの 1 つのインスタンスに対応します。同じサーバで複数の Web サービスやアプリケーションをアクティブにする場合は、サーバのサービスごとに 1 つずつ、合計 2 つのアプリケーション ユーザ CAPF プロファイルを設定する必要があります。

  クラスタ内の 2 台のサーバでサービスまたはアプリケーションをアクティブにする場合、サーバごとに 1 つずつ、合計 2 つのアプリケーション ユーザ CAPF プロファイルを設定する必要があります。

- エンド ユーザ CAPF プロファイル：このプロファイルでは、CTI クライアントが TLS 接続を介して CTIManager サービスと通信できるよう、CTI クライアントに対してローカルで有効な証明書を発行できます。

ヒント JTAPI クライアントは、[JTAPI Preferences] ウィンドウで設定したパスに、Java Key Store 形式で LSC を保存します。TSP クライアントは、デフォルト ディレクトリまたは設定したパスに、暗号化形式で LSC を保存します。

以下の情報は、通信障害や電源障害の発生時に適用されます。

- 証明書インストールの実行中に通信障害が発生した場合、JTAPI クライアントは証明書の取得を 30 秒間隔でさらに 3 回試行します。この値は設定できません。

  TSP クライアントの場合、再試行回数と再試行タイマーを設定できます。TSP クライアントが一定時間内に証明書の取得を試行する回数を指定するには、次の値を設定します。どちらの値も、デフォルトは 0 です。最大 3 回までの再試行回数を、1（再試行 1 回）、2、3 で指定します。再試行間隔は 30 秒以内で設定できます。

- JTAPI/TSP クライアントと CAPF とのセッション試行中に電源障害が発生した場合、クライアントは電源復旧後に証明書のダウンロードを試行します。

CTI、JTAPI、および TAPI アプリケーションの CAPF システムのインタラクションおよび要件

CAPF には次の要件が存在します。

- アプリケーションユーザとエンドユーザの CAPF プロファイルを設定する前に、Cisco CTL クライアントのインストールと設定に必要なすべての作業を実行したことを確認します。[Enterprise Parameters Configuration] ウィンドウの [Cluster Security Mode] を 1 に設定します（混合モード）。
- CAPF を使用するには、最初のノードで Cisco Certificate Authority Proxy Function サービスをアクティブにする必要があります。
- 多くの証明書を同時に生成するとコール処理中断の原因となるため、スケジュールされたメンテナンスの時間帯に CAPF を使用することを強く推奨します。
- 証明書操作の全期間を通じて、最初のノードが正常に実行されていることを確認します。
- 証明書操作の全期間を通じて、CTI/JTAPI/TAPI アプリケーションが正常に機能していることを確認します。

CTI、JTAPI、および TAPI の保護

次の手順は、CTI、JTAPI および TAPI アプリケーションを保護するために実行する作業を示します。

手順

ステップ 1 CTI アプリケーションおよびすべての JTAPI/TSP プラグインがインストールされ、実行中であることを確認します。

ヒント　アプリケーション ユーザを Standard CTI Enabled グループに割り当てます。

詳細については、次の資料を参照してください。

- 『*Computer Telephony Integration, System Configuration Guide for Cisco Unified Communications Manager*』
- 『*Cisco JTAPI Installation Guide for Cisco Unified Communications Manager*』
- 『*Cisco TAPI Installation Guide for Cisco Unified Communications Manager*』
- 『*Administration Guide for Cisco Unified Communications Manager*』

ステップ 2 次の Unified Communications Manager セキュリティ機能がインストールされていることを確認します（インストールされていない場合は、これらの機能をインストールして設定します）。

- CTL クライアントがインストールされ、CTL ファイルが実行済みであり、CTL ファイルが作成されていることを確認します。

- CTL Provider サービスがインストールされ、サービスがアクティブであることを確認します。
- CAPF サービスがインストールされ、サービスがアクティブであることを確認します。必要に応じて、CAPF サービス パラメータを更新します。

  ヒント　CTL ファイルに CAPF 証明書を組み込むために、CAPF サービスを Cisco CTL クライアント用に実行する必要があります。電話で CAPF を使用したときにこれらのパラメータを更新済みの場合は、ここで再度パラメータを更新する必要はありません。

- クラスタ セキュリティ モードが混合モードに設定されていることを確認します。（クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します。）

  ヒント　クラスタ セキュリティ モードが混合モードでない場合、CTI/JTAPI/TAPI アプリケーションは CTL ファイルにアクセスできません。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 3　CTIManager およびアプリケーションで TLS 接続を使用する場合は、アプリケーション ユーザまたはエンド ユーザを Standard CTI Secure Connection ユーザ グループに追加します。

ヒント　CTI アプリケーションは、アプリケーション ユーザまたはエンド ユーザに割り当てることができますが、両方に割り当てることはできません。

ステップ 4　SRTP を使用する場合は、Standard CTI Allow Reception of SRTP Key Material ユーザ グループにアプリケーション ユーザまたはエンド ユーザを追加します。

ユーザはすでに Standard CTI Enabled および Standard CTI Secure Connection ユーザ グループに存在している必要があります。これらの 3 つのグループに存在しないアプリケーション ユーザまたはエンド ユーザは、SRTP セッション キーを受信できません。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』の権限設定に関連する項目を参照してください。

（注）　Unified Communications Manager Assistant、Cisco QRT、および Cisco Web Dialer は暗号化をサポートしていません。CTIManager サービスに接続する CTI クライアントでは、クライアントが音声パケットを送信する場合、暗号化がサポートされることがあります。

ステップ 5　Unified Communications Manager の管理でアプリケーション ユーザまたはエンド ユーザの CAPF プロファイルを設定します。

ステップ 6　CTI/JTAPI/TAPI アプリケーションの対応するセキュリティ関連パラメータを有効にします。

セキュリティ関連ユーザグループへのアプリケーションとエンド ユーザの追加

Standard CTI Secure Connection ユーザ グループと Standard CTI Allow Reception of SRTP Key Material ユーザ グループはデフォルトで [Unified Communications Manager Administration] に表示されます。これらのグループは削除できません。

CTIManager へのユーザ接続を保護するには、Standard CTI Secure Connection ユーザ グループにアプリケーション ユーザまたはエンド ユーザを追加する必要があります。CTI アプリケーションはアプリケーション ユーザまたはエンド ユーザに割り当てできますが、両方に割り当てることはできません。

アプリケーションと CTIManager でメディア ストリームを保護する場合は、アプリケーション ユーザまたはエンド ユーザを Standard CTI Allow Reception of SRTP Key Material ユーザ グループに追加する必要があります。

アプリケーション ユーザとエンド ユーザが SRTP を使用するには、TLS のベースラインの構成として機能する Standard CTI Enabled ユーザ グループと Standard CTI Secure Connection ユーザ グループに、これらのユーザが存在している必要があります。SRTP 接続には TLS が必要です。これらのグループにユーザを確保できたら、ユーザを Standard CTI Allow Reception of SRTP Key Material ユーザ グループに追加できます。SRTP セッション キーを受け取るアプリケーションの場合、アプリケーション ユーザまたはエンドユーザが、Standard CTI Enabled、Standard CTI Secure Connection、Standard CTI Allow Reception of SRTP Key Material の 3 グループに存在している必要があります。

Unified Communications Manager Assistant、Cisco QRT、Cisco Web Dialer は暗号化をサポートしていないため、Standard CTI Allow Reception of SRTP Key Material ユーザ グループにアプリケーション ユーザ、CCMQRTSecureSysUser、IPMASecureSysUser、WDSecureSysUser を追加する必要はありません。

ヒント ユーザ グループからのアプリケーション ユーザまたはエンド ユーザの削除については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。[Role Configuration] ウィンドウのセキュリティに関する設定については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[User Management]** > **[User Groups]** を選択します。

ステップ 2 すべてのユーザ グループを表示するには、[Find] をクリックします。

ステップ 3 目的に応じて、次のいずれかの作業を実行します。

a) Standard CTI Enabled グループにアプリケーション ユーザまたはエンド ユーザが存在することを確認します。
b) Standard CTI Secure Connection ユーザ グループにアプリケーション ユーザまたはエンド ユーザを追加するには、[Standard CTI Secure Connection] リンクをクリックします。
c) Standard CTI Allow Reception of SRTP Key Material ユーザ グループにアプリケーション ユーザまたはエンドユーザを追加するには、[Standard CTI Allow Reception of SRTP Key Material] リンクをクリックします。

ステップ 4 アプリケーション ユーザをグループに追加するには、ステップ 5 （293 ページ）～ステップ 7 （293 ページ）を実行します。

ステップ 5 [Add Application Users to Group] ボタンをクリックします。

ステップ 6 アプリケーション ユーザを検索するには、検索条件を指定し、[Find] をクリックします。

検索条件を指定せずに [Find] をクリックすると、すべてのオプションが表示されます。

ステップ 7 グループに追加するアプリケーションユーザのチェックボックス（複数可）をオンにし、[Add Selected] をクリックします。

[User Groups] ウィンドウにユーザが表示されます。

ステップ 8 グループにエンド ユーザを追加するには、ステップ 9 （293 ページ）～ステップ 11 （293 ページ）を実行します。

ステップ 9 [Add Users to Group] ボタンをクリックします。

ステップ 10 エンド ユーザを検索するには、検索条件を指定し、[Find] をクリックします。

検索条件を指定せずに [Find] をクリックすると、すべてのオプションが表示されます。

ステップ 11 グループに追加するエンド ユーザのチェックボックス（複数可）をオンにし、[Add Selected] をクリックします。

[User Groups] ウィンドウにユーザが表示されます。

Certificate Authority Proxy Function サービスのアクティブ化

Unified Communications Manager は Cisco Unified Serviceability の Certificate Authority Proxy Function サービスを自動でアクティブにしません。

CAPF 機能を使用するには、このサービスを最初のノード上でアクティブにする必要があります。

Cisco CTL クライアントをインストールして設定する前に、このサービスをアクティブにしなかった場合、CTL ファイルを更新する必要があります。

Cisco Certificate Authority Proxy Function サービスをアクティブにすると、CAPF 固有のキー ペアおよび証明書が CAPF によって自動的に生成されます。Cisco CTL クライアントでスタンドアロン サーバまたはクラスタ内のすべてのサーバにコピーする CAPF 証明書の拡張子は .0 です。CAPF 証明書が存在することを確認するには、Cisco Unified Communications オペレーティング システムの GUI で CAPF 証明書を表示します。

CAPF サービス パラメータの更新

[CAPF Service Parameter] ウィンドウには、証明書の有効年数、システムによるキー生成の最大再試行回数などの情報が表示されます。

Unified Communications Manager Administration で認証局プロキシ機能（CAPF）サービス パラメータがアクティブとして表示されるためには、Cisco Unified Serviceability で Certificate Authority Proxy Function サービスを有効化する必要があります。

ヒント　CAPF を電話に使用する際に CAPF サービス パラメータを更新する場合は、サービス パラメータを再度更新する必要はありません。

CAPF サービス パラメータを更新するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified Communications Manager Administration] で、**[System]** > **[Service Parameters]** を選択します。

ステップ 2　[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。

ヒント　クラスタ内の最初のノードを選択する必要があります。

ステップ 3　[Service] ドロップダウン リスト ボックスで、[Cisco Certificate Authority Proxy Function] サービスを選択します。サービス名の横に「「Active」」と表示されることを確認します。

ステップ 4　ヘルプの説明に従い、CAPF サービス パラメータを更新します。CAPF サービス パラメータのヘルプを表示するには、疑問符またはパラメータ名リンクをクリックします。

ステップ 5　変更を有効にするには、[Cisco Unified Serviceability] で Cisco Certificate Authority Proxy Function サービスを再起動します。

アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの検索

アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルを検索するには、次の手順を実行します。

手順

ステップ 1 [Unified Communications Manager Administration] で、アクセスするプロファイルに応じて次のいずれかのウィンドウを選択します。

a) **[ユーザ管理]** > **[Application User CAPF Profile]**。
b) **[ユーザ管理]** > **[End User CAPF Profile]**。

[Find and List] 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）照会のレコードも表示されることがあります。

ステップ 2 データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、ステップ 3 （295 ページ） 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。

- 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。

a) 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。
b) 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、[Clear Filter] ボタンをクリックします。

ステップ 3 [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 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。

（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。

アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの設定

JTAPI/TAPI/CTI の各アプリケーション用のローカルで有効な証明書をインストール、アップグレード、またはトラブルシューティングする場合は、表 32 : アプリケーション ユーザおよびエンド ユーザの CAPF プロファイルの設定 （297 ページ）を参照してください。

ヒント　アプリケーション ユーザ CAPF プロファイルを設定した後で、エンド ユーザ CAPF プロファイルを設定することを推奨します。

手順

ステップ 1　[Unified Communications Manager Administration] で、次のいずれかのオプションを選択します。

a) **[User Management]** > **[Application User CAPF Profile]**。
b) **[User Management]** > **[End User CAPF Profile]**。

[Find and List] ウィンドウが表示されます。

ステップ 2　次のいずれかの作業を実行します。

a) 新しい CAPF プロファイルを追加するには、[Find] ウィンドウで [Add New] をクリックします（プロファイルを表示してから、[Add New] をクリックすることもできます）。各フィールドにデフォルト設定が取り込まれた設定ウィンドウが表示されます。
b) 既存のプロファイルをコピーするには、適切なプロファイルを見つけ、[Copy] 列内にあるそのレコード用の [Copy] アイコンをクリックします（プロファイルを表示してから、[Copy] をクリックすることもできます）。表示されたプロファイルからの設定が取り込まれた設定ウィンドウが表示されます。
c) 既存のエントリを更新するには、適切なプロファイルを見つけて表示します。設定ウィンドウが表示され、現在の設定が示されます。

ステップ 3　表 32 : アプリケーション ユーザおよびエンド ユーザの CAPF プロファイルの設定 （297 ページ） に示すように、適切な設定を入力します。

ステップ 4　**[保存（Save）]** をクリックします。

ステップ 5　セキュリティを使用するアプリケーション ユーザおよびエンド ユーザごとに、この手順を繰り返します。

次のタスク

[Application User CAPF Profile Configuration] ウィンドウで CCMQRTSecureSysUser、IPMASecureSysUser、または WDSecureSysUser を設定した場合は、サービス パラメータを設定する必要があります。

CAPF の設定

次の表で、[Application User CAPF Profile Configuration] および [End User CAPF Profile Configuration] ウィンドウの CAPF 設定について説明します。

表 *32*：アプリケーション ユーザおよびエンド ユーザの *CAPF* プロファイルの設定

設定	説明
Application User	ドロップダウンリスト ボックスから、CAPF 操作用のアプリケーション ユーザを選択します。この設定には、設定されたアプリケーション ユーザが表示されます。 この設定は、[End User CAPF Profile Configuration] ウィンドウには表示されません。
[End User ID]	ドロップダウンリスト ボックスから、CAPF 操作用のエンド ユーザを選択します。この設定には、設定されたエンド ユーザが表示されます。 この設定は、[Application User CAPF Profile Configuration] ウィンドウには表示されません。
[Instance ID]	1 ～ 128 文字の英数字（a ～ z、A ～ Z、0 ～ 9）を入力します。インスタンス ID は、証明書操作のユーザを指定します。 1 つのアプリケーションに複数の接続（インスタンス）を設定できます。アプリケーションと CTIManager との接続を保護するため、アプリケーション PC（エンドユーザの場合）またはサーバ（アプリケーション ユーザの場合）で実行されるそれぞれのインスタンスに固有の証明書があることを確認します。 このフィールドは、Web サービスとアプリケーションをサポートする [CAPF Profile Instance ID for Secure Connection to CTIManager] サービス パラメータに関連します。

設定	説明
[Certificate Operation]	ドロップダウンリストボックスから、次のいずれかのオプションを選択します。 • [No Pending Operation]：証明書の操作が行われない場合に表示されます。（デフォルト設定） • [Install/Upgrade]：アプリケーションに新しい証明書をインストールするか、既存のローカルで有効な証明書をアップグレードします。
[Authentication Mode]	証明書の操作が [Install/Upgrade] の場合、認証モードとして [By Authentication String] が指定されます。つまり、ユーザ/管理者によって [JTAPI/TSP Preferences] ウィンドウに CAPF 認証文字列が入力された場合にのみ、ローカルで有効な証明書のインストール/アップグレードまたはトラブルシュートが CAPF によって実行されます。
[Authentication String]	手動で一意の文字列を入力するか、[Generate String] ボタンをクリックして文字列を生成します。 文字列が 4 ～ 10 桁であることを確認します。 ローカルで有効な証明書のインストールまたはアップグレードを実行する場合、アプリケーション PC の JTAPI/TSP 設定 GUI に管理者が認証文字列を入力することが必要です。この文字列は 1 回だけ使用できます。このインスタンスで使用した文字列を再び使用することはできません。
[Generate String]	CAPF が自動的に認証文字列を生成するよう設定するには、このボタンをクリックします。4 ～ 10 桁の認証文字列が [Authentication String] フィールドに表示されます。

設定	説明
[Key Order]	このフィールドは、CAPF のキーの並び方を指定します。ドロップダウン リストから、次のいずれかの値を選択します。 • **[RSA Only]** • **[EC Only]** • **[EC Preferred, RSA Backup]** （注） [Key Order]、[RSA Key Size]、および [EC Key Size] フィールドの値に基づいて電話を追加すると、デバイス セキュリティ プロファイルがその電話に関連付けられます。値 [EC Only] を選択し、[EC Key Size] の値を [256] ビットにすると、デバイス セキュリティ プロファイルには値 **EC-256** が付加されます。
[RSA Key Size (Bits)]	ドロップダウン リスト ボックスから、[512]、[1024]、[2048,]、[3072]、または [4096] のいずれかの値を選択します。
[EC Key Size (Bits)]	ドロップダウン リスト ボックスから、[256]、[384]、または [521] のいずれかの値を選択します。
[Operation Completes by]	このフィールドは操作を完了する必要がある期限の日時を指定します。このフィールドはすべての証明書操作に対応しています。 表示される値は、最初のノードに適用されます。 この設定は、証明書の操作を完了する必要がある期間のデフォルトの日数を指定する [CAPF Operation Expires in (days)] エンタープライズ パラメータと併用します。このパラメータはいつでも更新できます。
証明書の操作ステータス（Certificate Operation Status）	このフィールドには、保留中、失敗、成功といった証明書の操作の進行状況が表示されます。 このフィールドに表示される情報は変更できません。

アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルの削除

この項では、Unified Communications Manager データベースからアプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを削除する方法について説明します。

始める前に

[Unified Communications Manager Administration] でアプリケーション ユーザ CAPF プロファイルまたはエンドユーザ CAPF プロファイルを削除する前に、デバイスに別のプロファイルを適用するか、そのプロファイルを使用するすべてのデバイスを削除する必要があります。プロファイルを使用しているデバイスを確認するには、[Security Profile Configuration] ウィンドウの [Related Links] ドロップダウン リスト ボックスで [Dependency Records] を選択し、[Go] をクリックします。

依存関係レコード機能がシステムで有効でない場合は、依存関係レコード概要ウィンドウに、依存関係レコードを有効にするために実行できる操作が表示されます。また、依存関係レコード機能に関連して CPU 負荷が高くなることについての情報も表示されます。依存関係レコードの詳細は、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

ステップ 1 アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを探します。

ステップ 2 次のいずれかの作業を実行します。

a) 複数のプロファイルを削除するには、[Find and List] ウィンドウで該当するチェック ボックスの横にあるチェック ボックスをオンにし、[Delete Selected] をクリックします。[Select All] をクリックし、次に [Delete Selected] をクリックすると、設定可能なすべてのレコードが削除されます。

b) 1 つのプロファイルを削除するには、[Find and List] ウィンドウで該当するプロファイルの横にあるチェック ボックスをオンにし、[Delete Selected] をクリックします。

ステップ 3 削除操作を確認するプロンプトが表示されたら、[OK] をクリックして削除するか、[Cancel] をクリックして削除の操作をキャンセルします。

JTAPI/TAPI セキュリティ関連のサービス パラメータの設定

アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを設定した後、Cisco IP Manager Assistant サービスに対して、次のサービス パラメータを設定する必要があります。

- CTIManager Connection Security Flag
- CAPF Profile Instance ID for Secure Connection to CTIManager

サービス パラメータにアクセスするには、次の手順を実行します。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[System]** > **[Service Parameters]** を選択します。

ステップ 2 [Server] ドロップダウン リスト ボックスから、Cisco IP Manager Assistant サービスがアクティブになっているサーバを選択します。

ステップ 3 [Service] ドロップダウン リスト ボックスから、[Cisco IP Manager Assistant] サービスを選択します。

ステップ 4 パラメータが表示されたら、[CTIManager Connection Security Flag] パラメータおよび [CAPF Profile Instance ID for Secure Connection to CTIManager] パラメータを見つけます。

ステップ 5 疑問符またはパラメータ名のリンクをクリックすると表示されるヘルプの説明に従い、パラメータを更新します。

ステップ 6 **[Save]** をクリックします。

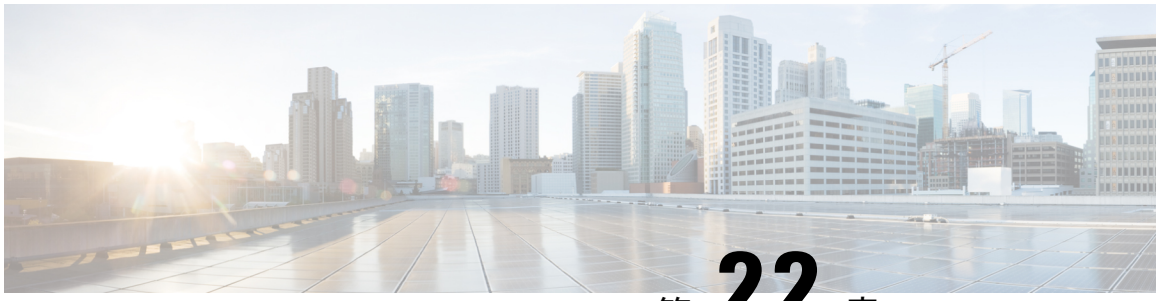
ステップ 7 サービスがアクティブになっているサーバごとに、この手順を繰り返します。

アプリケーションユーザまたはエンドユーザの証明書操作ステータスの表示

[JTAPI/TSP Preferences] GUI ウィンドウまたは（[Find/List] ウィンドウではなく）特定の [Application User CAPF Profile configuration] または [End User CAPF Profile configuration] ウィンドウで、証明書操作のステータスを確認できます。

第 VI 部

SRSTリファレンス、トランク、およびゲートウェイのセキュリティ



第 22 章

セキュアな Survivable Remote Site Telephony（SRST）リファレンス

この章では、SRST リファレンスについて説明します。

SRST セキュリティ

SRST 対応ゲートウェイは Unified Communications Manager がコールを完了できない場合に限定的な発信処理タスクを行います。

Secure SRST 対応ゲートウェイには自己署名証明書が含まれています。SRST 設定タスクを Unified Communications Manager Administrationで実行した後、 Unified Communications Manager はTLS接続を使用してSRST対応ゲートウェイで証明書プロバイダーサービスを認証します。Cisco Unified Communications Manager は次に SRST 対応ゲートウェイから証明書を取得し、この証明書を Unified Communications Manager データベースに追加します。

Unified Communications Manager Administration で従属デバイスをリセットすると、TFTP サーバは電話機の cnf.xml ファイルに SRST 対応ゲートウェイ証明書を追加し、そのファイルを電話機に送信します。その後、セキュアな電話は TLS 接続を使用して、SRST 対応ゲートウェイと相互に対話します。

ヒント 電話の設定ファイルには、単一の発行者からの証明書だけが含まれます。そのため、HSRP はサポートされません。

SRST セキュリティのヒント

セキュアな電話と SRST 対応ゲートウェイ間の接続を保護するには、次の条件が満たされていることを確認してください。

- SRST リファレンスに自己署名証明書が含まれている。
- Cisco CTL クライアントを介して混合モードに設定している。
- 電話に認証または暗号化を設定している。
- SRST リファレンスを [Unified Communications Manager Administration] で設定している。
- SRST 設定後に SRST 対応ゲートウェイと従属する電話をリセットしている。

（注） Unified Communications Manager は、電話の証明書情報を含む PEM 形式のファイルを SRST 対応ゲートウェイに提供します。

（注） ロースピードラインカード（LSC）の認証の場合、CAPF のルート証明書（CAPF.der）をダウンロードします。このルート証明書によりセキュア SRST は TLS ハンドシェイク中に電話の LSC を確認できます。

- クラスタ セキュリティ モードが非セキュアの場合、[Unified Communications Manager Administration] でデバイス セキュリティ モードが認証済みまたは暗号化であることが示されても、電話の設定ファイルではデバイスセキュリティモードが非セキュアなままです。このような状況では、電話は SRST 対応ゲートウェイおよび Unified Communications Manager で非セキュアな接続を試みます。

  （注） クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します。

- クラスタ セキュリティ モードが非セキュアの場合、システムはセキュリティ関連の設定（デバイスのセキュリティ モード、[Is SRST Secure?] チェックボックスなど）を無視します。設定がデータベースから削除されることはありませんが、セキュリティは提供されません。
- 電話が SRST 対応ゲートウェイへのセキュアな接続を試行するのは、クラスタ セキュリティ モードが混合モードに設定されており、電話の設定ファイルのデバイスセキュリティモードが認証済みまたは暗号化であり、[SRST Configuration] ウィンドウの [Is SRST Secure?] チェックボックスがオンになっており、有効な SRST 対応ゲートウェイの証明書が電話の設定ファイルにある場合だけです。

- 以前の Unified Communications Manager リリースでセキュア SRST リファレンスを設定していた場合、設定の移行はアップグレード中に自動的に行われます。
- 暗号化または認証済みモードの電話が SRST にフェールオーバーし、SRST での接続中に、クラスタ セキュリティ モードが混合モードから非セキュア モードに切り替わる場合、これらの電話は自動的に Unified Communications Manager にフォールバックしません。SRST ルータの電源をオフにし、これらの電話を Unified Communications Manager に強制的に再登録します。電話が Unified Communications Manager にフォールバックした後、SRST に電源を入れることができます。フェールオーバーとフォールバックは再び自動になります。

セキュアな SRST の設定

次の手順は、SRST のセキュリティ設定手順を示します。

手順

ステップ 1 デバイスが Unified Communications Manager とセキュリティに対応できるよう、SRST 対応ゲートウェイで必要なすべての作業を実行したことを確認します。

詳細は、このバージョンの Unified Communications Manager に対応した『*Cisco IOS SRST Version System Administrator Guide*』を参照してください。

ステップ 2 Cisco CTL クライアントのインストールおよび設定に必要なすべての作業を実行したことを確認します。

ステップ 3 電話に証明書が存在することを確認します。

詳細は、ご使用の電話のモデルの Cisco Unified IP Phone ドキュメンテーションを参照してください。

ステップ 4 電話に認証または暗号化を設定したことを確認します。

ステップ 5 SRST リファレンスのセキュリティ設定を行います。これには、[Device Pool Configuration] ウィンドウで SRST リファレンスを有効化することも含まれます。

ステップ 6 SRST 対応ゲートウェイと電話をリセットします。

セキュアな SRST リファレンスの設定

[Cisco Unified Communications Manager Administration][Unified Communications Manager Administration] で SRST リファレンスを追加、更新、または削除する前に、次の点を考慮してください。

- セキュアな SRST リファレンスの追加：初めて SRST リファレンスのセキュリティ設定を行う際に、表 33 : セキュア SRST リファレンスの設定 （310 ページ）で説明されているすべての項目を設定する必要があります。
- セキュアな SRST リファレンスの更新：[Unified Communications Manager Administration] で SRST の更新を実行しても、SRST 対応ゲートウェイの証明書は自動的には更新されません。証明書を更新するには、[Update Certificate] ボタンをクリックする必要があります。このボタンをクリックすると、証明書の内容が表示されるので、この証明書を受け入れるか拒否する必要があります。証明書を受け入れると、Unified Communications Manager では、Unified Communications Manager サーバ、またはクラスタ内の各 Unified Communications Manager サーバで、信頼できるフォルダ内にある SRST 対応ゲートウェイの証明書を置き換えます。
- セキュアな SRST リファレンスの削除：セキュアな SRST リファレンスを削除すると、Unified Communications Manager データベースおよび電話の cnf.xml ファイルから SRST 対応ゲートウェイの証明書が削除されます。

  SRST リファレンスの削除方法については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

セキュアな SRST リファレンスを設定するには、次の手順を実行します。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[System]** > **[SRST]** を選択します。

[Find and List] ウィンドウが表示されます。

ステップ 2 次のいずれかの作業を実行します。

a) 新しい SRST リファレンスを追加するには、[Find] ウィンドウで [Add New] をクリックします（プロファイルを表示してから、[Add New] をクリックすることもできます）。各フィールドにデフォルト設定が取り込まれた設定ウィンドウが表示されます。

b) 既存の SRST リファレンスをコピーするには、『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って適切な SRST リファレンスを見つけ、[Copy] 列内にあるそのレコード用の [Copy] アイコンをクリックします（プロファイルを表示してから、[Copy] をクリックすることもできます）。設定ウィンドウが表示され、設定された項目が示されます。

c) 既存の SRST リファレンスを更新するには、『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って適切な SRST リファレンスを見つけます。

設定ウィンドウが表示され、現在の設定が示されます。

ステップ 3 表 33 : セキュア SRST リファレンスの設定 （310 ページ）の説明に従ってセキュリティ関連の設定を入力します。

追加の SRST リファレンスの設定項目については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

[Find and List] ウィンドウが表示されます。

ステップ 4 [Is SRST Secure?] チェックボックスをオンにすると、[Update Certificate] ボタンをクリックして SRST 証明書をダウンロードする必要があることを示すメッセージがダイアログボックスに表示されます。[OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 データベース内の SRST 対応ゲートウェイの証明書を更新するには、[Update Certificate] ボタンをクリックします。

ヒント このボタンは、[Is SRST Secure?] チェック ボックスをオンにして [Save] をクリックした場合にだけ表示されます。

ステップ 7 証明書のフィンガープリントが表示されます。証明書を受け入れるには、[Save] をクリックします。

ステップ 8 [Close] をクリックします。

ステップ 9 [SRST Reference Configuration] ウィンドウで、[Reset] をクリックします。

次のタスク

[Device Pool Configuration] ウィンドウで SRST リファレンスを有効にしたことを確認します。

SRST リファレンスのセキュリティ設定

次の表では、[Unified Communications Manager Administration] で利用可能なセキュア SRST リファレンスの設定を説明します。

表 *33 :* セキュア *SRST* リファレンスの設定

設定	説明
[Is SRST Secure?]	SRST対応ゲートウェイに自己署名証明書が含まれることを確認した後で、このチェックボックスをオンにします。 SRSTを設定してゲートウェイおよび従属する電話をリセットすると、Cisco CTL プロバイダー サービスは SRST 対応ゲートウェイで証明書プロバイダー サービスに対して認証します。Cisco CTL クライアントは SRST 対応ゲートウェイから証明書を取得し、この証明書を Unified Communications Manager データベースに保存します。 ヒント SRST 証明書をデータベースおよび電話から削除するには、このチェックボックスをオフにして [Save] をクリックし、従属する電話をリセットします。
[SRST Certificate Provider Port]	このポートは SRST 対応ゲートウェイで証明書プロバイダー サービスの要求をモニタします。Unified Communications Manager は、このポートを使用して SRST 対応ゲートウェイから証明書を取得します。Cisco SRST 証明書プロバイダーのデフォルト ポートは2445 です。 SRST対応ゲートウェイでこのポートを設定した後、このフィールドにポート番号を入力します。 ヒント ポートが現在使用されているか、またはファイアウォールを使用していてファイアウォール内でポートを使用できない場合、異なるポート番号を設定する必要があります。ポート番号は 1024～49151 の範囲内である必要があります。範囲外の場合には「Port Numbers can only contain digits」というメッセージが表示されます。

設定	説明
[Update Certificate]	ヒント　このボタンは、[Is SRST Secure?] チェック ボックスをオンにして [Save] をクリックした場合にだけ表示されます。 証明書がデータベースにある場合、このボタンをクリックすると、Cisco CTL クライアントが Unified Communications Manager データベースに保存されている SRST 対応ゲートウェイの証明書を置き換えます（証明書がデータベースに存在する場合）。従属する電話をリセットすると、TFTP サーバは cnf.xml ファイル（および新しい SRST 対応ゲートウェイ証明書）を送信します。

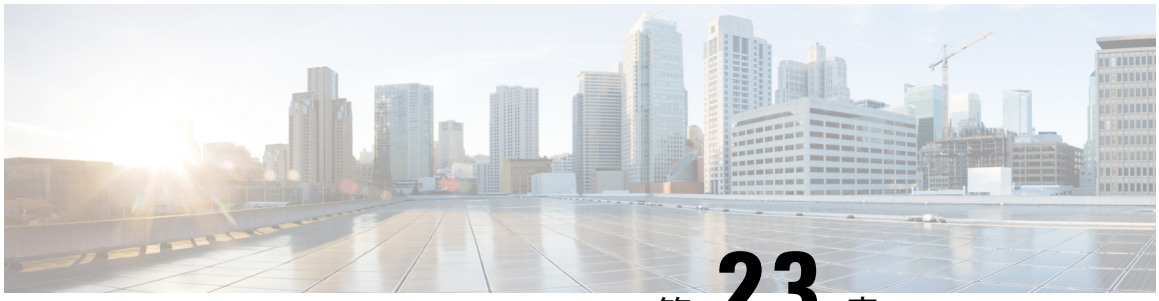
SRST リファレンスからのセキュリティの削除

セキュリティ設定後に SRST リファレンスを非セキュアにするには、[SRST Configuration] ウィンドウの [Is SRTS Secure?] チェック ボックスをオフにします。ゲートウェイのクレデンシャル サービスを無効にする必要があることを示すメッセージが表示されます。

ゲートウェイからの SRST 証明書の削除

SRST 証明書が SRST 対応ゲートウェイに存在しない場合は、Unified Communications Manager データベースおよび電話から、SRST 証明書を削除する必要があります。

この作業を実行するには、[SRST Secure?] チェック ボックスをオフにし、[SRST Configuration] ウィンドウで [Update] をクリックします。次に [Reset Decives] をクリックします。



第 23 章

ゲートウェイおよびトランクの暗号化の設定

この章では、ゲートウェイおよびトランクの暗号化の設定について説明します。

Cisco IOS MGCP ゲートウェイの暗号化

Unified Communications Manager は MGCP SRTP パッケージを使用するゲートウェイをサポートしています。ゲートウェイはこれを使用してセキュアな RTP 接続を介したパケットの暗号化と復号を行います。コールセットアップの間に交換される情報によって、ゲートウェイがコールに SRTP を使用するかどうかが決定されます。デバイスが SRTP をサポートしている場合、システムは SRTP 接続を使用します。1 つ以上のデバイスが SRTP をサポートしていない場合、システムは RTP 接続を使用します。SRTP から RTP へのフォールバック（またはその逆）は、安全なデバイスから安全ではないデバイスへの転送、会議、トランスコーディング、保留音などの場合に発生する可能性があります。

システムによって 2 つのデバイス間に SRTP コールがセットアップされると、Unified Communications Manager によってセキュアなコール用のマスター暗号化キーとソルトが生成され、SRTP ストリーム用のみゲートウェイに送信されます。ゲートウェイでは SRTCP ストリームのキーとソルトもサポートされていますが、Unified Communications Manager では送信されません。これらのキーは、MGCP シグナリング パスを介してゲートウェイに送信されます。このパスは IPSec を使用して保護する必要があります。Unified Communications Manager では IPSec 接続の有無が認識されませんが、IPSec が設定されていないとシステムではセッションキーが

クリア テキストでセッションに送信されます。セッション キーがセキュアな接続を介して送信されるよう、IPSec 接続が存在することを確認します。

ヒント SRTP に設定された MGCP ゲートウェイが、SCCP の動作している認証済み電話などの認証済みデバイスとのコールに関係している場合、シールドアイコンが電話に表示されます。Unified Communications Manager ではこれらのコールが認証済みとして分類されるためです。コールについてそのデバイスの SRTP 機能のネゴシエーションが成功すると、Unified Communications Manager ではそのコールが認証済みとして分類されます。MGCP ゲートウェイが、セキュリティ アイコンを表示できる電話に接続されている場合、コールが暗号化されているときは電話に鍵アイコンが表示されます。

H.323 ゲートウェイおよび H.323/H.225/H.245 トランクの暗号化

セキュリティをサポートする H.323 ゲートウェイおよびゲートキーパー、または非ゲートキーパー制御の H.225/H.323/H.245 トランクは、Cisco Unified Communications Operating System で IPSec アソシエーションを設定した場合、Unified Communications Manager に対して認証できます。Unified Communications Manager とこれらのデバイスの間での IPSec アソシエーション作成については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

H.323、H.225、および H.245 デバイスでは暗号キーが生成されます。これらのキーは、IPSec で保護されたシグナリング パスを介して Unified Communications Manager に送信されます。Unified Communications Manager は IPSec 接続が存在するかどうかを認識しませんが、IPSec が設定されていない場合、セッション キーは暗号化されずに送信されます。セッション キーがセキュアな接続を介して送信されるよう、IPSec 接続が存在することを確認します。

IPSec アソシエーションの設定に加えて、Unified Communications Manager Administration のデバイス設定ウィンドウにある [SRTP 許可（SRTP Allowed）] チェックボックスにマークを付ける必要があります。これは H.323 ゲートウェイ、H.225 トランク（ゲートキーパー制御）、クラスタ間トランク（ゲートキーパー制御）、およびクラスタ間トランク（非ゲートキーパー制御）の設定ウィンドウなどに存在します。このチェックボックスをオンにしない場合、Unified Communications Manager は RTP を使用してデバイスと通信します。このチェックボックスをオンにする場合、Unified Communications Manager は SRTP がデバイスに対して設定されているかどうかに応じて、セキュア コールと非セキュア コールを許可します。

注意 Unified Communications Manager Administration で [SRTP Allowed] チェックボックスをオンにする場合は、セキュリティ関連情報が暗号化されずに送信されることを防ぐために、IPSec を設定することを強く推奨します。

Unified Communications Manager は、IPSec 接続が正しく設定されたかどうかを確認しません。接続が正しく設定されていないと、セキュリティ関連情報が暗号化されずに送信されることがあります。

セキュア メディア パスまたはセキュア シグナリング パスを確立でき、デバイスが SRTP をサポートする場合、システムは SRTP 接続を使用します。セキュア メディア パスまたはセキュア シグナリング パスを確立できないか、1 つ以上のデバイスが SRTP をサポートしない場合、システムは RTP 接続を使用します。SRTP から RTP へのフォールバック（またはその逆）は、安全なデバイスから安全ではないデバイスへの転送、会議、トランスコーディング、保留音などの場合に発生する可能性があります。

ヒント コールがパススルー対応 MTP を使用し、リージョン フィルタリングの後でデバイスの音声機能が一致し、どのデバイスについても [MTP Required] チェックボックスがオンになっていない場合、Unified Communications Manager はそのコールをセキュアとして分類します。[MTP Required] チェックボックスがオンの場合、Unified Communications Manager はコールの音声パススルーを無効にし、コールを非セキュアとして分類します。MTP がコールに関係しない場合、Unified Communications Manager はデバイスの SRTP 機能に応じてそのコールを暗号化済みに分類することがあります。

Unified Communications Manager は、そのデバイスの [SRTP Allowed] チェックボックスがオンで、そのデバイスの SRTP 機能がコールに対して正常にネゴシエートされれば、コールを暗号化済みに分類します。 コールを暗号化済みとして分類します。前述の条件を満たさない場合、Unified Communications Manager はコールを非セキュアとして分類します。デバイスが、セキュリティ アイコンを表示できる電話に接続されている場合、コールが暗号化されているときは電話機に鍵アイコンが表示されます。

Unified Communications Manager は、トランクまたはゲートウェイ経由の発信 FastStart コールを非セキュアとして分類します。Unified Communications Manager Administration で [SRTP Allowed] チェックボックスをオンにした場合、Unified Communications Manager は **[Enable Outbound FastStart]** チェックボックスをオフにします。

Unified Communications Manager の一部の種類のゲートウェイおよびトランクでは、共有秘密キー（Diffie-Hellman キー）やその他の H.235 データを 2 つの H.235 エンドポイント間で透過的にパススルーさせることができます。このため、これら 2 つのエンドポイントではセキュア メディア チャネルを確立できます。

H.235 データのパススルーを有効にするには、次のトランクおよびゲートウェイの設定で、[H.235 pass through allowed] チェックボックスをオンにします。

- H.225 トランク

- ICT ゲートキーパー制御
- ICT 非ゲートキーパー制御
- H.323 ゲートウェイ

トランクとゲートウェイの設定の詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

SIP トランクの暗号化

SIP トランクは、シグナリングとメディア両方のセキュア コールをサポートできます。TLS がシグナリング暗号化を提供し、SRTP がメディア暗号化を提供します。

トランクのシグナリング暗号化を設定するには、SIP トランク セキュリティ プロファイルを設定する際に次のオプションを選択します（**[System]** > **[Security Profile]** > **[SIP Trunk Security Profile] ウィンドウ**）。

- [Device Security Mode] ドロップダウン リストから 「[Encrypted]」 を選択します。
- [Incoming Transport Type] ドロップダウン リストから 「[TLS]」 を選択します。
- [Outgoing Transport Type] ドロップダウン リストから 「[TLS]」 を選択します。

SIP トランク セキュリティ プロファイルを設定した後、プロファイルをトランクに適用します（**[Device]** > **[Trunk]** > **[SIP Trunk]** 設定ウィンドウ）。

トランクに対してメディア暗号化を設定するには、[SRTP Allowed] チェック ボックスをオンにします（[Device] > [Trunk] > [SIP Trunk] 設定ウィンドウも同様です）。

⚠

注意 このチェック ボックスをオンにする場合は、キーやその他のセキュリティ関連情報がコール ネゴシエーション中に公開されないように、暗号化された TLS プロファイルを使用することを強く推奨します。非セキュアプロファイルを使用する場合でも SRTP は機能しますが、キーはシグナリングおよびトレースで公開されます。この場合、Unified Communications Manager と接続先のトランク間でのネットワーク セキュリティを確保する必要があります。

セキュアなゲートウェイとトランクのセットアップ

この手順は、Cisco IOS MGCP ゲートウェイでセキュリティを設定する方法について説明しているマニュアル『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』とともに使用してください。

手順

ステップ 1 Cisco CTL クライアントをインストールし、設定したことを確認します。クラスタ セキュリティ モードが混合モードであることを確認します。

ステップ 2 電話に暗号化を設定したことを確認します。

ステップ 3 IPSec を設定します。

ヒント ネットワーク インフラストラクチャで IPSec を設定することも、Unified Communications Manager とゲートウェイまたはトランクとの間で IPSec を設定することもできます。IPSec を設定するために 1 つの方式を実装する場合、他の方式を実装する必要はありません。

ステップ 4 H.323 IOS ゲートウェイおよびクラスタ間トランクの場合、[Unified Communications Manager Administration] で [SRTP Allowed] チェックボックスをオンにします。

[SRTP Allowed] チェックボックスは、[Trunk Configuration] ウィンドウまたは [Gateway Configuration] ウィンドウに表示されます。これらのウィンドウを表示する方法については、『*Administration Guide for Cisco Unified Communications Manager*』のトランクおよびゲートウェイに関する章を参照してください。

ステップ 5 SIP トランクの場合、SIP トランク セキュリティ プロファイルを設定し、トランクに適用します（この処理を行っていない場合）。また、**[Device]** > **[Trunk]** > **[SIP Trunk]** の設定ウィンドウで 「[SRTP Allowed]」 チェックボックスを必ずオンにします。

注意 「[SRTP Allowed]」 チェックボックスをオンにする場合、コール ネゴシエーション中にキーやその他のセキュリティ関連情報が公開されないようにするために、暗号化された TLS プロファイルを使用することを強く推奨します。非セキュア プロファイルを使用すると、SRTP は機能しますが、キーはシグナリングおよびトレースで公開されます。この場合、Unified Communications Manager と接続先のトランク間でのネットワーク セキュリティを確保する必要があります。

ステップ 6 ゲートウェイのセキュリティ関連の設定タスクを実行します。

詳細については、『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』を参照してください。

ネットワーク インフラストラクチャ内の IPSec 設定

ここでは、IPSec の設定方法については説明しません。代わりに、ネットワーク インフラストラクチャで IPSec を設定する際の考慮事項と推奨事項について記載されています。ネットワーク インフラストラクチャ内で IPSec を設定する予定であり、Unified Communications Manager とデバイスの間では設定しない場合、IPSec の設定前に次の情報を検討してください。

- Unified Communications Manager 自体ではなく、インフラストラクチャの中で IPSec をプロビジョニングすることを推奨します。
- IPSec を設定する前に、既存の IPSec 接続または VPN 接続、プラットフォームの CPU への影響、帯域幅への影響、ジッタや遅延などのパフォーマンス メトリックについて考慮します。
- 『*Voice and Video Enabled IPSec Virtual Private Networks Solution Reference Network Design Guide*』を参照します。
- 『*Cisco IOS Security Configuration Guide, Release 12.2*』（またはそれ以降）を参照します。
- IPSec 接続のリモート エンドをセキュアな Cisco IOS MGCP ゲートウェイで終端します。
- テレフォニー サーバが存在するネットワークの信頼されている領域内のネットワーク デバイスでホストを終端します（ファイアウォールの背後、アクセス コントロール リスト（ACL）またはその他のレイヤ 3 デバイスなど）。
- ホスト側 IPSec 接続の終端に使用する機器は、ゲートウェイの数とそれらのゲートウェイに予想されるコールの量とによって決まります。たとえば、Cisco VPN 3000 シリーズ コンセントレータ、Catalyst 6500 IPSec VPN サービス モジュール、Cisco サービス統合型ルータなどがあります。
- セキュアなゲートウェイとトランクの設定の関連項目で指定されている順序で、手順を実行します。

注意 IPSec 接続を設定してその接続がアクティブであることを確認しないと、メディア ストリームのプライバシーが損なわれる可能性があります。

Cisco Unified Communications Manager とゲートウェイまたはトランクとの間の IPSec の設定

Unified Communications Manager と、この章で説明されているゲートウェイやトランクとの間の IPSec の設定に関する情報については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco Unified Communications Manager Administration を使用した SRTP の許可

[SRTP Allowed] チェックボックスは [Unified Communications Manager Administration] の以下の設定ウィンドウで表示されます。

- [H.323 Gateway Configuration] ウィンドウ
- [H.225 Trunk (Gatekeeper Controlled) Configuration] ウィンドウ
- [Inter-Cluster Trunk (Gatekeeper Controlled) Configuration] ウィンドウ
- [Inter-Cluster Trunk (Non-Gatekeeper Controlled) Configuration] ウィンドウ
- [SIP Trunk Configuration] ウィンドウ

H.323 ゲートウェイ、ゲートキーパー制御または非ゲートキーパー制御の H.323/H.245/H.225 トランク、SIP トランクの [SRTP Allowed] チェックボックスを設定するには、次の手順を実行します。

手順

ステップ 1 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って、ゲートウェイまたはトランクを検索します。

ステップ 2 ゲートウェイまたはトランクの設定ウィンドウを開いた後、[SRTP Allowed] チェックボックスをオンにします。

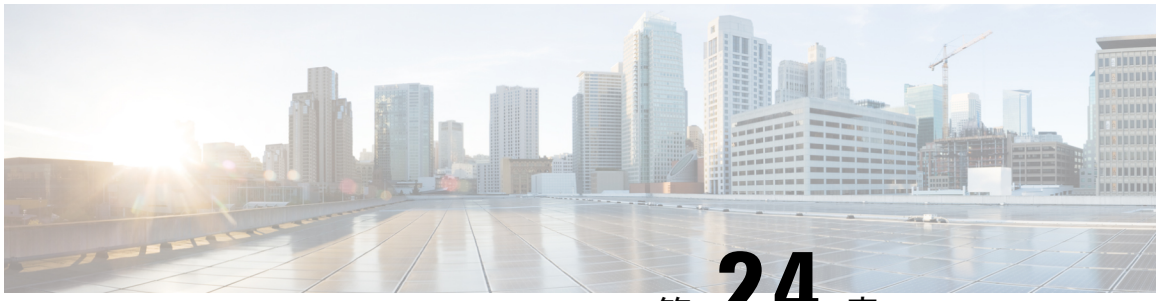
注意 SIP トランクの 「[SRTP Allowed]」 チェック ボックスをオンにする場合は、キーや他のセキュリティ関連の情報がネゴシエーション中に公開されることを防止するため、TLS 暗号化プロファイルの使用を強く推奨します。非セキュア プロファイルを使用すると、SRTP は機能しますが、キーはシグナリングおよびトレースで公開されます。この場合、Unified Communications Manager と接続先のトランク間でのネットワーク セキュリティを確保する必要があります。

ステップ 3 **[Save]** をクリックします。

ステップ 4 デバイスをリセットするには、[Reset] をクリックします。

ステップ 5 IPSec が H323 向けに正しく設定されたことを確認します。（SIP の場合は、TLS が正しく設定されたことを確認してください。）

ゲートウェイとトランクの暗号化に関する詳細情報の入手先



第 24 章

SIP トランク セキュリティ プロファイルの設定

この章では、SIP トランク セキュリティ プロファイルのセットアップについて説明します。

SIP トランク セキュリティ プロファイルの設定について

Unified Communications Manager Administration では、単一のセキュリティ プロファイルを複数の SIP トランクに割り当てることができるよう、SIP トランクのセキュリティ関連の設定項目をグループ化しています。セキュリティ関連の設定には、デバイス セキュリティ モード、ダイジェスト認証、着信転送タイプや発信転送タイプの設定などがあります。[Trunk Configuration] ウィンドウでセキュリティプロファイルを選択する際に、構成済みの設定を SIP トランクに適用します。

Unified Communications Manager をインストールすると、自動登録用の事前に定義された非セキュアな SIP トランク セキュリティ プロファイルが提供されます。SIP トランクのセキュリティ機能を有効にするには、新しいセキュリティ プロファイルを設定して、SIP トランクに適用します。トランクがセキュリティをサポートしない場合は、非セキュアプロファイルを選択してください。

セキュリティ プロファイルの設定ウィンドウに表示されるのは、SIP トランクでサポートされるセキュリティ機能だけです。

SIP トランク セキュリティ プロファイルの設定のヒント

[Unified Communications Manager Administration] で SIP トランク セキュリティ プロファイルを設定する際には以下の情報を考慮してください。

- SIP トランクを設定するときは、[Trunk Configuration] ウィンドウでセキュリティ プロファイルを選択する必要があります。デバイスがセキュリティをサポートしていない場合は、非セキュア プロファイルを選択します。
- 現在デバイスに割り当てられているセキュリティ プロファイルは削除できません。
- SIP トランクに割り当てられているセキュリティ プロファイルの設定を変更すると、再設定された設定が、そのプロファイルが割り当てられているすべての SIP トランクに適用されます。
- デバイスに割り当てられているセキュリティ ファイルの名前を変更できます。古いプロファイル名および設定が割り当てられている SIP トランクは、新しいプロファイル名および設定を受け入れます。
- Unified Communications Manager 5.0 以降のアップグレード前にデバイス セキュリティ モードを設定していた場合、Unified Communications Manager は SIP トランクのプロファイルを作成し、そのプロファイルをデバイスに適用します。

SIP トランク セキュリティ プロファイルの検索

SIP トランク セキュリティ プロファイルを検索するには、次の手順を実行します。

手順

ステップ 1 **[System]** > **[Security Profile]** > **[SIP Trunk Security Profile]** の順に選択します。

[Find and List] 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）照会のレコードも表示されることがあります。

ステップ 2 データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、ステップ 3 （323 ページ） 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) 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) 次に、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、[Clear Filter] ボタンをクリックします。

ステップ 3 [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 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。

（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。

SIP トランク セキュリティ プロファイルの設定

SIP トランク セキュリティ プロファイルを追加、更新、またはコピーするには、次の手順を実行します。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[System]** > **[Security Profile]** > **[SIP Trunk Security Profile]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

a) 新しいプロファイルを追加するには、[Find] ウィンドウで [Add New] をクリックします

（プロファイルを表示してから、[Add New] をクリックすることもできます）。

各フィールドにデフォルト設定が取り込まれた設定ウィンドウが表示されます。

b) 既存のセキュリティ プロファイルをコピーするには、適切なプロファイルを見つけ、[Copy] 列内にあるそのレコード用の [Copy] アイコンをクリックします

（プロファイルを表示してから、[Copy] をクリックすることもできます）。

設定ウィンドウが表示され、設定された項目が示されます。

c) 既存のプロファイルを更新するには、SIP トランク セキュリティ プロファイルの検索 （322 ページ）の説明に従い、適切なセキュリティ プロファイルを見つけて表示します。

設定ウィンドウが表示され、現在の設定が示されます。

ステップ 3 表 34 : SIP トランク セキュリティ プロファイルの設定 （324 ページ） に示すように、適切な設定を入力します。

ステップ 4 **[Save]** をクリックします。

次のタスク

セキュリティ プロファイルを作成した後、それをトランクに適用します。

SIP トランクにダイジェスト認証を設定した場合は、トランクの [SIP Realm] ウィンドウと、その SIP トランクを介して接続されるアプリケーションの [Application User] ウィンドウで、ダイジェスト クレデンシャルを設定する必要があります（まだ設定していない場合）。

SIP トランクを介して接続されるアプリケーションに対してアプリケーションレベルの許可（認証）を有効にした場合は、[Application User] ウィンドウで、そのアプリケーションに許可される方式を設定する必要があります（まだ設定していない場合）。

SIP トランク セキュリティ プロファイルの設定

次の表は、SIP トランク セキュリティ プロファイルの設定を示します。

表 *34 : SIP* トランク セキュリティ プロファイルの設定

設定	説明
Name	セキュリティ プロファイルの名前を入力します。新しいプロファイルを保存すると、[Trunk Configuration] ウィンドウの [SIP Trunk Security Profile] ドロップダウン リスト ボックスにその名前が表示されます。
[Description]	セキュリティ プロファイルの説明を入力します。説明には、任意の言語で最大 50 文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

設定	説明
[Device Security Mode]	ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。 • [Non Secure]：イメージ認証以外のセキュリティ機能は適用されません。TCP または UDP 接続が Unified Communications Manager に対して開きます。 • **[Authenticated]**：Unified Communications Manager はトランクの整合性と認証を提供します。NULL/SHA を使用する TLS 接続が開きます。 • **[Encrypted]**：Cisco Unified Communications Manager は、トランクの整合性、認証、およびシグナリング暗号化を提供しています。AES128/SHA を使用する TLS 接続がシグナリング用に開きます。 （注） [認証済み] として選択されている [デバイスのセキュリティ プロファイル (トランク)] を使用して設定した場合、Cisco ユニファイド コミュニケーション マネージャーは、NULL_SHA 暗号を使用した TLS connection (データ暗号化なし) を開始します。 これらのトランクは、通知先デバイスが NULL_SHA 暗号をサポートしていない場合は、そのデバイスを登録したり、コールを発信したりしません。 NULL_SHA 暗号をサポートしていない通知先デバイスでは、[暗号化 (Encrypted)] として選択した [デバイスのセキュリティ プロファイル (トランク)] で設定する必要があります。このデバイス セキュリティ プロファイルを使用すると、トランクは、データの暗号化を可能にする追加の TLS 暗号を提供します。

設定	説明
[Incoming Transport Type]	[Device Security Mode] が [Non Secure] の場合、転送タイプは TCP+UDP になります。 [Device Security Mode] が [Authenticated] または [Encrypted] の場合、転送タイプは TLS になります。 （注） Transport Layer Security（TLS）プロトコルは Unified Communications Manager とトランクとの間の接続を保護します。
[Outgoing Transport Type]	ドロップダウン リスト ボックスから適切な発信転送モードを選択します。 [Device Security Mode] が [Non Secure] の場合、TCP または UDP を選択します。 [Device Security Mode] が [Authenticated] または [Encrypted] の場合、転送タイプは TLS になります。 （注） TLS により、SIP トランクのシグナリング整合性、デバイス認証、およびシグナリングの暗号化が実現します。 ヒント Unified Communications Manager システムと TCP の再使用をサポートしない IOS ゲートウェイとの間の SIP トランクを接続する場合、出力転送タイプとして UDP を使用する必要があります。

設定	説明
[Enable Digest Authentication]	ダイジェスト認証を有効にする場合に、このチェックボックスをオンにします。このチェックボックスをオンにすると、Unified Communications Manager はトランクからのすべての SIP 要求に対してチャレンジを行います。 ダイジェスト認証ではデバイス認証、整合性、機密性は提供されません。これらの機能を使用するには、セキュリティ モードとして [Authenticated] または [Encrypted] を選択します。 **ヒント** TCP または UDP 転送を使用しているトランクで SIP トランク ユーザを認証するには、ダイジェスト認証を使用します。
[Nonce Validity Time]	ナンス値が有効な分数（秒単位）を入力します。デフォルト値は 600（10 分）です。この時間が経過すると、Unified Communications Manager は新しい値を生成します。 （注） ナンス値は、ダイジェスト認証をサポートする乱数であり、ダイジェスト認証パスワードの MD5 ハッシュを計算するときに使用されます。

設定	説明
安全な証明書の件名またはサブジェクトの別名	このフィールドは、着信転送タイプおよび発信転送タイプに TLS を設定した場合に適用されます。 デバイス認証では、SIP トランク デバイスのセキュアな証明書のサブジェクトまたはサブジェクト代替名を入力します。Unified Communications Manager クラスタがある場合、または TLS ピアに SRV ルックアップを使用する場合は、単一のトランクは複数のホストに解決されることがあります。このように解決された場合、トランクに複数のセキュアな証明書のサブジェクトまたはサブジェクト代替名が設定されます。X.509 のサブジェクト名が複数存在する場合、スペース、カンマ、セミコロン、コロンのいずれかを入力して名前を区切ります。 このフィールドには、最大 4096 文字を入力できます。 **ヒント** サブジェクト名はソース接続の TLS 証明書に対応します。サブジェクト名が、サブジェクト名とポートで一意であることを確認します。異なる SIP トランクに同じサブジェクト名と着信ポートの組み合わせを割り当てることはできません。例: ポート 5061 の SIP TLS trunk1 は、セキュリティ保護された証明書の件名またはサブジェクト代替名 my_cm1, my_cm2 を持っています。ポート 5071 の SIP TLS trunk2 には、セキュリティで保護された証明書のサブジェクトまたはサブジェクト代替名 my_cm2, my_cm3 があります。ポート 5061 の SIP TLS trunk3 は、セキュリティで保護された証明書の件名またはサブジェクト代替名my_ccm4を含むことができますが、安全な証明書のサブジェクトまたはサブジェクト代替名 my_cm1 を含めることはできません。

設定	説明
[Incoming Port]	着信ポートを選択します。0 ～ 65535 の範囲で一意のポート番号を入力します。着信 TCP および UDP SIP メッセージ用のデフォルト ポート値は 5060 です。着信 TLS メッセージ用の SIP セキュア ポートのデフォルト ポート値は 5061 です。入力した値は、このプロファイルを使用するすべての SIP トランクに適用されます。 **ヒント** TLS を使用するすべての SIP トランクは同じ着信ポートを共有できます。TCP + UDP を使用するすべての SIP トランクは同じ着信ポートを共有できます。同じポートで、SIP TLS 転送トランクと SIP 非 TLS 転送トランク タイプとを混在させることはできません。

設定	説明
[Enable Application Level Authorization]	アプリケーション レベルの認証は、SIP トランクを介して接続されるアプリケーションに適用されます。 このチェックボックスをオンにする場合、[Enable Digest Authentication] チェックボックスもオンにして、トランクのダイジェスト認証を設定する必要があります。Unified Communications Manager は許可されているアプリケーション方式を確認する前に、SIP アプリケーション ユーザを認証します。 アプリケーション レベルの許可が有効な場合、トランク レベルの許可が最初に発生してからアプリケーション レベルの許可が発生するため、Unified Communications Manager は [Application User Configuration] ウィンドウで SIP アプリケーション ユーザに対して許可されたメソッドより先に、（このセキュリティ プロファイル内の）トランクに対して許可されたメソッドをチェックします。 **ヒント** アプリケーションのアイデンティティを信頼しないか、またはアプリケーションが特定のトランクで信頼されていない場合は、アプリケーション レベルの許可の使用を検討してください。つまり、アプリケーション要求は想定外の別のトランクから送信される場合もあります。

設定	説明
[Accept Presence Subscription]	Unified Communications Manager が SIP トランク経由でのプレゼンス サブスクリプション要求を受け入れるようにするには、このチェックボックスをオンにします。 [Enable Application Level Authorization] チェックボックスをオンにしたら、[Application User Configuration] ウィンドウに移動し、この機能について許可するすべてのアプリケーション ユーザの [Accept Presence Subscription] チェックボックスをオンにします。 アプリケーション レベルの許可が有効になっている場合に、アプリケーション ユーザの [Accept Presence Subscription] チェックボックスをオンにし、トランクのこのチェックボックスをオンにしない場合、トランクに接続された SIP ユーザ エージェントに 403 エラー メッセージが送信されます。
[Accept Out-of-Dialog Refer]	Unified Communications Manager が SIP トランク経由で着信する非 INVITE、Out-of-Dialog REFER 要求を受け入れるようにするには、このチェックボックスをオンにします。 [Enable Application Level Authorization] チェックボックスをオンにしたら、[Application User Configuration] ウィンドウに移動し、このメソッドについて許可するすべてのアプリケーション ユーザの [Accept Out-of-Dialog refer] チェックボックスをオンにします。
[Accept unsolicited notification]	Unified Communications Manager が SIP トランク経由で着信する非 INVITE、Unsolicited NOTIFY メッセージを受け入れるようにするには、このチェックボックスをオンにします。 [Enable Application Level Authorization] チェックボックスをオンにしたら、[Application User Configuration] ウィンドウに移動し、このメソッドについて許可するすべてのアプリケーション ユーザの [Accept Unsolicited Notification] チェックボックスをオンにします。

設定	説明
[Accept replaces header]	Unified Communications Manager が既存の SIP ダイアログに代わる新規の SIP ダイアログを許可するようにするには、このチェックボックスをオンにします。 [Enable Application Level Authorization] チェックボックスをオンにしたら、[Application User Configuration] ウィンドウに移動し、このメソッドについて許可するすべてのアプリケーション ユーザの [Accept Header Replacement] チェックボックスをオンにします。
[Transmit Security Status]	Unified Communications Manager が関連付けられた SIP トランクからのコールのセキュリティ アイコン ステータスを SIP ピアに送信するようにするには、このチェックボックスをオンにします。 デフォルトでは、このチェックボックスはオフになっています。

設定	説明
[SIP V.150 Outbound SDP Offer Filtering]	ドロップダウン リスト ボックスから、次のフィルタ処理オプションのいずれかを選択します。 • [Use Default Filter]：SIP トランクは [SIP V.150 Outbound SDP Offer Filtering] サービス パラメータに示されているデフォルト フィルタを使用します。このサービス パラメータを検索するには、[Unified Communications Manager Administration] で **[System]** > **[Service Parameters]** > **[Clusterwide Parameters (Device-SIP)]** に進みます。 • [No Filtering]：SIP トランクは、アウトバウンド オファーで V.150 SDP 回線のフィルタリングを行いません。 • [Remove MER V.150]：SIP トランクは、アウトバウンド オファーで V.150 MER SDP 回線を削除します。トランクが MER V.150 よりも前の Unified Communications Manager に接続する際のあいまいさを低減するには、このオプションを選択します。 • [Remove Pre-MER V.150]：SIP トランクは、アウトバウンド オファーで非 MER 対応 V.150 回線をすべて削除します。クラスタがプレ MER 回線でオファーを処理できない MER 準拠デバイスのネットワークに含まれる際のあいまいさを低減するには、このオプションを選択します。

設定	説明
[SIP V.150 Outbound SDP Offer Filtering]	ドロップダウン リスト ボックスから、次のフィルタ処理オプションのいずれかを選択します。 • [Use Default Filter]：SIP トランクは [SIP V.150 Outbound SDP Offer Filtering] サービス パラメータに示されているデフォルト フィルタを使用します。このサービス パラメータを検索するには、[Unified Communications Manager Administration] で **[System]** > **[Service Parameters]** > **[Clusterwide Parameters (Device-SIP)]** に進みます。 • [No Filtering]：SIP トランクは、アウトバウンド オファーで V.150 SDP 回線のフィルタリングを行いません。 • [Remove MER V.150]：SIP トランクは、アウトバウンド オファーで V.150 MER SDP 回線を削除します。トランクが MER V.150 よりも前の Unified Communications Manager に接続する際のあいまいさを低減するには、このオプションを選択します。 • [Remove Pre-MER V.150]：SIP トランクは、アウトバウンド オファーで非 MER 対応 V.150 回線をすべて削除します。クラスタがプレ MER 回線でオファーを処理できない MER 準拠デバイスのネットワークに含まれる際のあいまいさを低減するには、このオプションを選択します。 （注） セキュアなコールの接続を確立するためには SIP の IOS を V.150 に設定する必要があります。IOS を Cisco Unified Communication Manager で設定する際の詳細については、http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t4/mer_cg_15_1_4M.html をご覧ください。

SIP トランク セキュリティ プロファイルの適用

[Trunk Configuration] ウィンドウでトランクに SIP トランク セキュリティ プロファイルを適用します。デバイスにセキュリティ プロファイルを適用するには、次の手順を実行します。

手順

ステップ 1 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って、トランクを検索します。

ステップ 2 [トランク設定（Trunk Configuration）] ウィンドウが表示されたら、[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] 設定を探します。

ステップ 3 セキュリティ プロファイルのドロップダウン リスト ボックスから、デバイスに適用するセキュリティ プロファイルを選択します。

ステップ 4 **[Save]** をクリックします。

ステップ 5 トランクをリセットするには、[Apply Config] をクリックします。

次のタスク

ダイジェスト認証を有効にしたプロファイルを SIP トランクに適用した場合は、[SIP Realm] ウィンドウでダイジェスト クレデンシャルを設定する必要があります。

アプリケーション レベルの認証を有効にしたプロファイルを適用した場合は、[Application User] ウィンドウでダイジェスト クレデンシャルと、適切な認証方法を設定する必要があります（まだ設定していない場合）。

SIP トランク セキュリティ プロファイルと SIP トランクの同期

設定変更が行われた SIP トランク セキュリティ プロファイルと SIP トランクを同期させるには、次の手順を実行します。この手順では、最小限の割り込みで未適用の設定が適用されます。（たとえば、影響を受けるデバイスの一部では、リセットまたは再起動が不要な場合があります。）

手順

ステップ 1 **[System]** > **[Security Profile]** > **[SIP Trunk Security Profile]** の順に選択します。

[Find and List SIP Trunk Security Profiles] ウィンドウが表示されます。

ステップ 2 使用する検索条件を選択します。

ステップ 3 [検索（Find）] をクリックします。

ウィンドウに検索条件と一致する SIP トランク セキュリティ プロファイルのリストが表示されます。

ステップ 4 該当する SIP トランクと同期させる SIP トランク セキュリティ プロファイルをクリックします。[SIP Trunk Security Profile Configuration] ウィンドウが表示されます。

ステップ 5 追加の設定変更を加えます。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 [設定の適用（Apply Config）] をクリックします。

[Apply Configuration Information] ダイアログが表示されます。

ステップ 8 [OK] をクリックします。

SIP トランク セキュリティ プロファイルの削除

この項では、Unified Communications Manager データベースから SIP トランク セキュリティ プロファイルを削除する方法について説明します。

始める前に

[Unified Communications Manager Administration] からセキュリティ プロファイルを削除する前に、デバイスに別のプロファイルを適用するか、そのプロファイルを使用するすべてのデバイスを削除する必要があります。プロファイルを使用しているデバイスを検索するには、[SIP Trunk Security Profile Configuration] ウィンドウの [Related Links] ドロップダウン リスト ボックスで [Dependency Records] を選択し、[Go] をクリックします。

依存関係レコード機能がシステムで有効でない場合は、依存関係レコード概要ウィンドウに、依存関係レコードを有効にするために実行できる操作が表示されます。また、依存関係レコード機能に関連して CPU 負荷が高くなることについての情報も表示されます。依存関係レコードの詳細は、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

ステップ 1 削除する SIP トランク セキュリティ プロファイルを探します。

ステップ 2 次のいずれかの作業を実行します。

a) 複数のセキュリティ プロファイルを削除するには、[Find and List] ウィンドウで次のいずれかの作業を実行します。

- 削除するセキュリティ プロファイルの隣にあるチェック ボックスをオンにして、[Delete Selected] をクリックします。

- [Select All] をクリックし、次に [Delete Selected] をクリックすると、設定可能なすべてのレコードが削除されます。

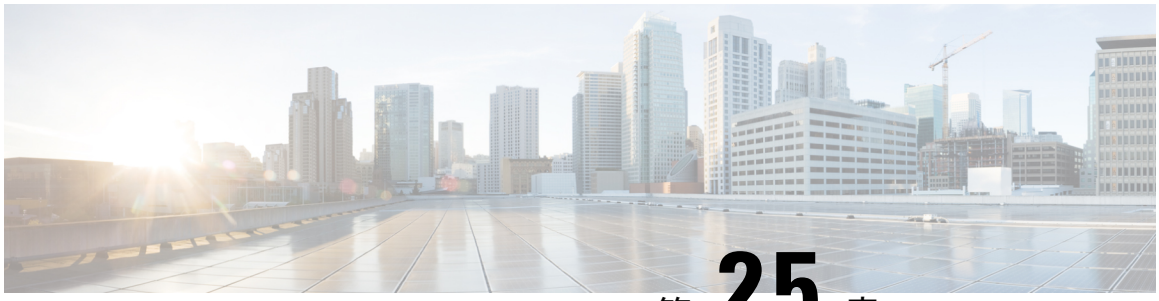
b) 1 つのセキュリティ プロファイルを削除するには、[Find and List] ウィンドウで次のいずれかの作業を実行します。

- 削除するセキュリティ プロファイルの隣にあるチェック ボックスをオンにして、[Delete Selected] をクリックします。
- セキュリティ プロファイルの [Name] リンクをクリックします。特定の [Security Profile Configuration] ウィンドウが表示されたら、[Delete Selected] をクリックします。

ステップ 3 削除操作を確認するプロンプトが表示されたら、[OK] をクリックして削除するか、[Cancel] をクリックして削除の操作をキャンセルします。

SIP トランク セキュリティ プロファイルに関する詳細情報の入手先

- 認証 （28 ページ）
- 連携動作 （10 ページ）
- ダイジェスト認証 （26 ページ）



第 25 章

SIP トランクのダイジェスト認証の設定

この章では、SIP トランクのダイジェスト認証の設定について説明します。SIP トランクにダイジェスト認証を設定する場合、Unified Communications Manager は SIP トランクで SIP 要求を受信すると、SIP ユーザ エージェントのアイデンティティでチャレンジを実施します。次に SIP ユーザ エージェントは、Unified Communications Manager が SIP 要求をトランクに送信する際に、Unified Communications Manager のアイデンティティでチャレンジを実施できます。SIP トランクでのダイジェスト認証の動作の詳細については、「ダイジェスト認証 （26ページ）」を参照してください。

SIP トランクのダイジェスト認証の設定

ここでは、SIP トランクのダイジェスト認証を設定する作業を説明します。

手順

ステップ 1 SIP トランク セキュリティ プロファイルを設定します。[Enable Digest Authentication] チェックボックスがオンであることを確認します。

ステップ 2 SIP トランク セキュリティ プロファイルをトランクへ適用します。

ステップ 3 設定されていない場合は、エンタープライズ パラメータ、クラスタ ID を設定します。

このパラメータは SIP トランクで SIP 要求を送信する SIP ユーザ エージェント識別のための Unified Communications Manager チャレンジをサポートします。

ステップ 4 Unified Communications Manager が SIP トランクで SIP 要求を送信する SIP ユーザ エージェントのアイデンティティのチャレンジを行う場合は、[Application User Configuration] ウィンドウでアプリケーション ユーザのダイジェスト クレデンシャルを設定します。

ステップ 5 Unified Communications Manager がトランク ピアからのチャレンジに応答する場合は、SIP レルムを設定します。

ダイジェスト認証のエンタープライズパラメータの設定

ダイジェスト認証用にエンタープライズ パラメータ、クラスタ ID を設定するには、[Unified Communications Manager Administration] で、**[System]** > **[Enterprise Parameters]** を選択します。クラスタ ID パラメータを検索し、パラメータのヘルプの説明に従って値を更新します。このパラメータは SIP トランクで SIP 要求を送信する SIP ユーザ エージェント識別のための Unified Communications Manager チャレンジをサポートします。

ヒント パラメータのヘルプにアクセスするには、[Enterprise Parameters Configuration] ウィンドウに表示される疑問符またはパラメータのリンクをクリックします。

ダイジェスト クレデンシャルのセットアップ

Unified Communications Manager が SIP ユーザ エージェントのアイデンティティのチャレンジを行う場合は、[Unified Communications Manager Administration] の [Application User Configuration] ウィンドウでアプリケーション ユーザのダイジェスト クレデンシャルを設定します。Unified Communications Manager は、これらのクレデンシャルを使用して、SIP トランクで要求を送信する SIP ユーザ エージェントのアイデンティティを確認します。

アプリケーション ユーザにダイジェスト クレデンシャルを設定するには、次の手順を実行します。

手順

ステップ 1 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って、アプリケーション ユーザを探します。

ステップ 2 アプリケーション ユーザのリンクをクリックします。

ステップ 3 個別の [Application User Configuration] ウィンドウが表示されたら、表 36 : SIP レルム セキュリティ プロファイル （343 ページ）に従い適切な設定値を入力します。

ステップ 4 **[保存 (Save)]** をクリックします。

アプリケーションユーザのダイジェストクレデンシャルの設定

次の表に、[Unified Communications Manager Administration] の **[Application User Configuration]** ウィンドウ内にあるダイジェスト クレデンシャルの設定について説明します。

表 *35* : ダイジェスト認証クレデンシャル

設定	説明
Digest Credentials	英数字の文字列を入力します。
Confirm Digest Credentials	[Digest Credentials] の入力が正しいことを確認するために、このフィールドにクレデンシャルを再度入力します。

SIP レルムの検索

SIP レルムを検索するには、次の手順を実行します。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[User Management]** > **[SIP Realm]** を選択します。

[Find and List] 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）照会のレコードも表示されることがあります。

ステップ 2 データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、ステップ 3 （341 ページ） 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。

（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、[Clear Filter] ボタンをクリックします。

ステップ 3 [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 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。

（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。

次のタスク

まだ設定していない場合は、[Cluster ID] エンタープライズ パラメータを設定します。

SIP レルムの設定

Unified Communications Manager が 1 つ以上のトランク ピアからのチャレンジに対して応答する場合は、Unified Communications Manager に対してチャレンジを行う可能性のある各 SIP トランク ユーザ エージェントに、SIP レルムを設定する必要があります。

SIP レルムを追加または更新するには、次の手順を実行します。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[User Management]** > **[SIP Realm]** を選択します。

ステップ 2 表 36 : SIP レルム セキュリティ プロファイル （343 ページ） に示すように、適切な設定を入力します。

ステップ 3 **[Save]** をクリックします。

ステップ 4 追加または更新する必要があるすべてのレルムについてこの手順を実行します。

次のタスク

ダイジェスト認証が正常に実行されるようにするため、Unified Communications Manager と同一の設定が SIP ユーザ エージェントに対して設定されていることを確認します。

SIP レルム設定

Unified Communications Manager がトランク ピアによってチャレンジされる際に、SIP レルムがトランク側のクレデンシャルを提供します。

次の表に、SIP レルムの設定を示します。

表 *36 : SIP* レルム セキュリティ プロファイル

設定	説明
Realm	SIP トランクに接続するレルムのドメイン名を入力します（例：SIPProxy1_xyz.com）。英数字、ピリオド、ダッシュ、アンダースコア、スペースを使用できます。
User	このレルム内の SIP ユーザエージェントのユーザ名を入力します。たとえば、Unified Communications Manager サーバ名を入力します。SIP トランクは、このユーザ名を使用して Unified Communications Manager にチャレンジします。
Digest Credentials	Unified Communications Manager がこのレルムとユーザに対するチャレンジに応答するために使用するパスワードを入力します。
Confirm Digest Credentials	確認のため、パスワードを再入力します。

SIP レルムの削除

このセクションでは、Unified Communications Manager データベースから SIP レルムを削除する方法について説明します。

手順

ステップ 1 削除する SIP レルムを探します。

ステップ 2 次のいずれかの作業を実行します。

a) 複数の SIP レルムを削除するには、[Find and List] ウィンドウで次のいずれかの作業を実行します。

- 削除するレルムの隣にあるチェック ボックスをオンにして、[Delete Selected] をクリックします。

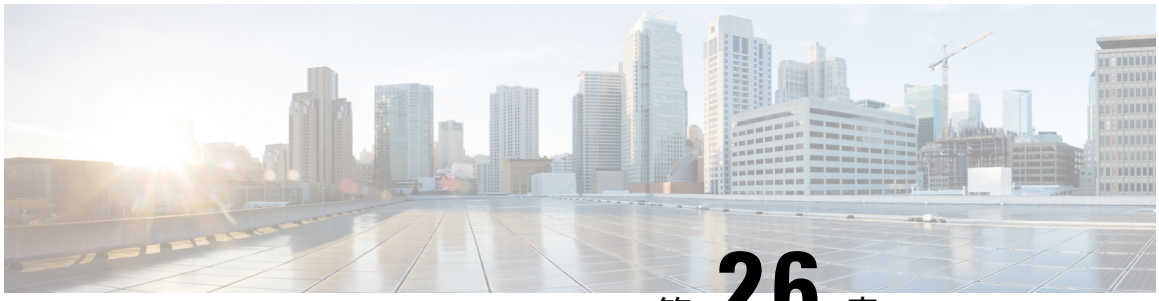
  [Select All] をクリックし、次に [Delete Selected] をクリックすると、設定可能なすべてのレコードが削除されます。

b) 単一の SIP レルムを削除するには、[Find and List] ウィンドウで次のいずれかの作業を実行します。

- 削除するレルムの隣にあるチェック ボックスをオンにして、[Delete Selected] をクリックします。

  レルムの [Name] リンクをクリックします。特定の [SIP Realm Configuration] ウィンドウが表示されたら、[Delete Selected] をクリックします。

ステップ 3 削除操作を確認するプロンプトが表示されたら、[OK] をクリックして削除するか、[Cancel] をクリックして削除の操作をキャンセルします。



第 26 章

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定

この章では、Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルのセットアップについて説明します。

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定について

Unified Communications Manager Administration では、単一のセキュリティ プロファイルを複数の Mobile Communicator クライアントに割り当てることができるよう、セキュリティ関連の設定項目をグループ化しています。セキュリティ関連の設定には、デバイス セキュリティ モード、着信転送タイプ、X.509 のサブジェクト名などがあります。[Cisco Unified Communications Manager Administration] で Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルを設定すると、このプロファイルがその Cisco Unified Communications Manager の設定済み Mobile Communicator クライアントすべてに自動で適用されます。

セキュリティ プロファイルの設定ウィンドウに表示されるのは、Cisco Unified Mobility Advantage サーバでサポートされるセキュリティ機能だけです。

（注） Cisco Unified Mobility Advantage サーバを Unified Communications Manager Assistant Administration で設定することはできません。Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定については、ご使用の Cisco Unified Mobility Advantage のマニュアルを参照してください。Unified Communications Manager で設定する Cisco Unified Mobility Advantage のセキュリティ プロファイルが、Cisco Unified Mobility Advantage サーバ上のセキュリティ プロファイルと必ず一致するようにしてください。Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの検索

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルを検索するには、次の手順を実行します。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[System] > [Security Profile]** > **[CUMA Server Security Profile]** を選択します。

[Find and List CUMA Server Security Profile] 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）照会のレコードも表示されることがあります。

ステップ 2 データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、ステップ 3 （346 ページ） 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。

（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、[Clear Filter] ボタンをクリックします。

ステップ 3 [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 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。

（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。

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定

セキュリティ プロファイルを追加、更新、またはコピーするには、次の手順を実行します。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[System]** > **[Security Profile]** > **[CUMA Server Security Profile]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

a) 新しいプロファイルを追加するには、[Find] ウィンドウで [Add New] をクリックし、Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定 （345 ページ）に進みます。

b) 既存のセキュリティプロファイルをコピーするには、適切なプロファイルを見つけて、コピーするセキュリティ プロファイルの横に表示されている [Copy] ボタンをクリックしてから、Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定 （345 ページ）に進みます。

c) 既存のプロファイルを更新するには、適切なセキュリティ プロファイルを検索し、Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定 （345 ページ）に進みます。

[Add New] をクリックすると、各フィールドにデフォルト設定が入力された設定ウィンドウが表示されます。[Copy] をクリックすると、コピーした設定が入力された設定ウィンドウが表示されます。

ステップ 3 XXX の説明に従って、適切な設定を入力します。 表 37 : セキュリティ プロファイル設定 （348 ページ）

ステップ 4 **[保存 (Save)]** をクリックします。

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定について、次の表で説明します。

表 *37*：セキュリティ プロファイル設定

設定	説明
Name	セキュリティ プロファイルの名前を入力します。 **ヒント** セキュリティ プロファイル名にデバイス モデルを含めると、プロファイルの検索または更新時に正しいプロファイルを検索できます。
Description	セキュリティ プロファイルの説明を入力します。説明には、任意の言語で最大 50 文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。
[Device Security Mode]	ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。 • [Non Secure]：Cisco Unified Mobility Advantage サーバには、イメージ認証以外のセキュリティ機能はありません。Unified Communications Manager への TCP 接続が開かれます。 • [Authenticated]：Unified Communications Manager によって Cisco Unified Mobility Advantage サーバの整合性と認証が提供されます。NULL/SHA を使用する TLS 接続がシグナリングに対して開きます。 • [Encrypted]：Unified Communications Manager によって Cisco Unified Mobility Advantage サーバの整合性、認証、および暗号化が提供されます。シグナリング用に AES128/SHA を使用する TLS 接続が開き、SRTP によってすべてのモバイル コールのメディアが伝送されます。

設定	説明
Transport Type	[Device Security Mode] が [Non Secure] の場合、ドロップダウン リスト ボックスから次のオプションを選択します。 • [TCP]：Transmission Control Protocol を選択し、パケットが送信時と同じ順序で受信されるようにします。このプロトコルを使用すると、パケットはドロップされませんが、プロトコルはセキュリティを提供しません。 [Device Security Mode] が [Authenticated] または [Encrypted] の場合、転送タイプはTLSになります。TLSによって、シグナリングの整合性、デバイス認証、およびシグナリング暗号化（暗号化モードのみ）が実現されます。
安全な証明書の件名またはサブジェクトの別名	（[Device Security Mode] が [Authenticated] または [Encrypted] の場合は必須）。このフィールドは、転送タイプに TLS を設定した場合に適用されます。 Secure Certificate Subject または Subject Alternate Name は暗号化における公開キー インフラストラクチャについての国際電気通信連合電気通信標準化部門の標準規格です。サブジェクト名はソース接続のTLS証明書に対応します。 X.509 のサブジェクト名が複数存在する場合、スペース、カンマ、セミコロン、コロンのいずれかを入力して名前を区切ります。 このフィールドには、最大 4096 文字を入力できます。

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイル クライアント アプリケーション

Mobile Communicator クライアントのデバイス設定ウィンドウに 「[Device Security Profile]」フィールドが存在しない場合、クライアントに Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルを手動で適用する必要はありません。

[Unified Communications Manager Administration] で Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルを設定すると、このプロファイルがそのUnified Communications Managerの設定済み Mobile Communicator クライアントすべてに自動で適用されます。

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの削除

この項では、Unified Communications Manager データベースから Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルを削除する方法について説明します。

手順

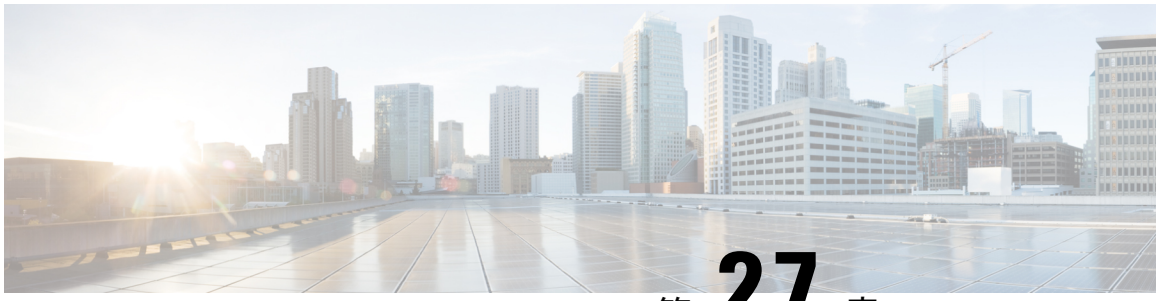
ステップ 1 削除するセキュリティ プロファイルを探します。

ステップ 2 セキュリティ プロファイルを削除するには、次の作業を実行します。

a) [Find and List] ウィンドウで、該当するセキュリティ プロファイルの横にあるチェック ボックスをオンにし、[Delete Selected] をクリックします。

ステップ 3 削除操作を確認するプロンプトが表示されたら、[OK] をクリックして削除するか、[Cancel] をクリックして削除の操作をキャンセルします。

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルに関する詳細情報の入手先



第 27 章

FIPS 140-2 モードの設定

この章では、FIPS 140-2 モードの設定について説明します。

FIPS モードは、一部の 12.x バージョンではサポートされていません

FIPS モードは 12.5(1)SU1 でサポートされています。ただし FIPS モードは、Cisco Unified Communications Manager および IM and Presence Service のリリース 12.0(x) と 12.5(1) ではサポートされていません。FIPS モード、強化されたセキュリティ モード、またはコモンクライテリア モードを有効化した以前のリリースからアップグレードする場合、リリース 12.0(x) または 12.5(1) へのアップグレードを行う前にこれらのモードを無効にするか、または代わりに 12.5(1)SU1 にアップグレードする必要があります。TFTP およびその他のサービスは、FIPS モードが有効になっている 12.0(x) または 12.5(1) では機能しません。

FIPS モードは、一部の 12.x バージョンではサポートされていません

第 28 章

Cisco V.150 Minimum Essential Requirements（MER）

V.150 の概要

V.150 Minimum Essential Requirements 機能により、IP ネットワーク経由でモデムから安全なコール発信が可能になります。この機能は、モデムとテレフォニーデバイスが従来の公衆電話交換網（PSTN）で稼働している大規模なインストール ベースに対しダイヤルアップ モデムを使用します。V.150.1 勧告では、PSTN 上のモデムおよびテレフォニー デバイスと IP ネットワーク間でのモデム経由でのデータのリレー方法について、具体的に定義されています。V.150.1 は、ダイヤルアップ モデム コールをサポートしている IP ネットワークでのモデムの使用に関する ITU-T 勧告です。

Cisco V.150.1 Minimum Essential Requirements 機能は、国家安全保障局（NSA）の SCIP-216 Minimum Essential Requirements（MER）for V.150.1 勧告の要件に準拠しています。SCIP-216 勧告により既存の V.150.1 要件が簡素化されました。

Cisco V.150.1 MER 機能は次のインターフェイスをサポートしています。

- Media Gateway Control Protocol（MGCP）T1（PRI と CAS）および E1（PRI）トランク
- Session Initiation Protocol（SIP）トランク
- アナログ ゲートウェイ ポイント向けの Skinny Client Control Protocol（SCCP）
- Secure Communication Interoperability Protocol-End Instruments（SCIP-EI）

Cisco V.150.1 MER の前提条件

システムですでに基本的なコール制御機能がセットアップされている必要があります。コール制御システムをセットアップする手順については、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_0_1/sysConfig/CUCM_BK_C733E983_00_cucm-system-configuration-guide.html にある『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

Unified Communications Manager の次のいずれかのリリースがインストールされている必要があります。

- 最小バージョンはリリース 10.5(2) SU3 です。
- 11.0 の最小バージョンは 11.0(1) SU2 です（2016 年春に公開）。
- 11.5(1) 以降のすべてのリリースではこの機能がサポートされています。
- Cisco IOS リリース 15.6(2)T 以降が必要です。

V.150 は、メディア ターミネーション ポイント（MTP）ではサポートされていません。V.150 コールを処理するデバイス、トランク およびゲートウェイから MTP を削除することが推奨されます。

V.150 設定のタスク フロー

Unified Communications Manager で V.150 のサポートを追加するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	メディア リソース グループ設定のタスク フロー（355 ページ）を行うには、次のサブタスクを実行します。 • 非 V.150 エンドポイントのメディア リソース グループの設定（356 ページ） • 非 V.150 エンドポイントのメディア リソース グループ リストの設定（356 ページ） • V.150 エンドポイントのメディア リソース グループの設定（357 ページ） • V.150 エンドポイントのメディア リソース グループ リストの設定（357 ページ）	V.150 デバイスおよび非 V.150 デバイスのメディア リソース グループおよびメディア リソース グループ リストを追加します。

	コマンドまたはアクション	目的
ステップ 2	Cisco V.150（MER）に対応したゲートウェイの設定 （358 ページ）	ゲートウェイに V.150 機能を追加します。
ステップ 3	#unique_394	MGCP ゲートウェイ全体で V.150 サポートを使用するには、ポートインターフェイスに V.150 サポートを追加します。
ステップ 4	#unique_395	SCCP ゲートウェイ全体で V.150 サポートを使用するには、ポートインターフェイスに V.150 サポートを追加します。
ステップ 5	電話での V.150 サポートの設定 （359 ページ）	V.150 コールを発信する電話に V.150 サポートを追加します。
ステップ 6	SIP トランク設定のタスク フロー （360 ページ）を行うには、次のサブタスクのいずれかまたは両方を実行します。 • クラスタ全体の V.150 フィルタの設定 （361 ページ） • SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加 （362 ページ）	V.150 コールに使用する SIP トランクに V.150 サポートを追加します。

メディア リソース グループ設定のタスク フロー

2 つのメディア リソース グループ セット（非 V.150 コール用の MTP リソースからなるメディア リソース グループと、V.150 コール用の MTP リソースが含まれないメディア リソース グループ）を設定するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	非 V.150 エンドポイントのメディア リソース グループの設定 （356 ページ）	非 V.150 エンドポイントで使用する MTP を含むメディア リソース グループを設定します。
ステップ 2	非 V.150 エンドポイントのメディア リソース グループ リストの設定 （356 ページ）	非 V.150 エンドポイントの MTP メディア リソースが含まれているメディア リソース グループ リストを設定します。
ステップ 3	V.150 エンドポイントのメディア リソース グループの設定 （357 ページ）	セキュア V.150 コール用の MTP リソースが含まれていないメディア リソース グループを設定します。

	コマンドまたはアクション	目的
ステップ 4	V.150 エンドポイントのメディア リソース グループ リストの設定（357 ページ）	メディア リソース グループに必要なリソースを追加した後で、MTP のない非 V.150 エンドポイント用のメディア リソース グループ リストを設定します。

非 V.150 エンドポイントのメディア リソース グループの設定

非 V.150 エンドポイントの MTP リソースのメディア リソース グループを新たに追加するには、次の手順に従います。

手順

ステップ 1 Cisco Unified CM Administration で **[Media Resources]** > **[Media Resource 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)]** フィールドに、メディア リソース グループ名として「「Do not use with V.150 devices」」と入力します。

ステップ 4 [Available Media Resources] フィールドで MTP デバイスだけを選択し、下矢印キーをクリックします。
選択されたデバイスが [Selected Media Resources] フィールドに表示されます。

ステップ 5 **[保存 (Save)]** をクリックします。

次のタスク

非 V.150 エンドポイントのメディア リソース グループ リストの設定 （356 ページ）

非 V.150 エンドポイントのメディア リソース グループ リストの設定

非 V.150 エンドポイントの MTP リソースのメディア リソース グループ リストを新たに追加するには、次の手順に従います。

始める前に

非 V.150 エンドポイントのメディア リソース グループの設定 （356 ページ）

手順

ステップ 1 Cisco Unified CM Administration で **[Media Resources]** > **[Media Resource Group List]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **[名前(Name)]** フィールドに、メディア リソース グループ リストの名前として「「Non-V.150」」と入力します。

ステップ 4 **[Available Media Resources]** フィールドで、「「Do not use with V.150 Devices」」という名前の V.150 MER リソース グループを選択し、下矢印キーをクリックします。
選択されたデバイスが [Selected Media Resources] フィールドに表示されます。

ステップ 5 **[保存 (Save)]** をクリックします。

V.150 エンドポイントのメディア リソース グループの設定

V.150 デバイスに対し、MTP リソースのない新しいメディア リソース グループを追加するには、次の手順に従います。

手順

ステップ 1 Cisco Unified CM Administration で **[Media Resources]** > **[Media Resource 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)]** フィールドに、メディア リソース グループ名として「「For use with V.150 devices」」と入力します。

ステップ 4 [Available Media Resources] フィールドで MTP リソースを除く複数のデバイスを選択し、下矢印キーをクリックします。
選択されたデバイスが [Selected Media Resources] フィールドに表示されます。

ステップ 5 **[保存 (Save)]** をクリックします。

次のタスク

V.150 エンドポイントのメディア リソース グループ リストの設定 （357 ページ）

V.150 エンドポイントのメディア リソース グループ リストの設定

V.150 デバイスの MTP リソースのメディア リソース グループ リストを追加するには、次の手順に従います。

始める前に

V.150 エンドポイントのメディア リソース グループの設定 （357 ページ）

手順

ステップ 1 Cisco Unified CM Administration で **[Media Resources]** > **[Media Resource Group List]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **[名前(Name)]** フィールドに、メディア リソース グループ リストの名前として「「V.150」」と入力します。

ステップ 4 **[Available Media Resources]** フィールドで、「「For V.150 Devices」」という名前の V.150 MER リソース グループを選択し、下矢印キーをクリックします。
選択されたメディア リソース グループが [Selected Media Resources] フィールドに表示されます。

ステップ 5 **[保存 (Save)]** をクリックします。

Cisco V.150（MER）に対応したゲートウェイの設定

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [ゲートウェイタイプ (Gateway Type)] ドロップダウン リストからゲートウェイを選択します。

ステップ 4 [次へ（Next)] をクリックします。

ステップ 5 [Protocol] ドロップダウン リストから、プロトコルを選択します。

ステップ 6 ゲートウェイに対して選択するプロトコルに応じて、次のいずれかを実行します。

- MGCP の場合は、[Domain Name] フィールドに、ゲートウェイで設定されているドメイン名を入力します。
- SCCP の場合は、[MAC Address (Last 10 Characters)] フィールドにゲートウェイ MAC アドレスを入力します。

ステップ 7 **[Unified Communications Manager Group]** ドロップダウン リストから **[Default]** を選択します。

ステップ 8 [Configured Slots、VICs and Endpoints] 領域で次の手順を実行します。

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

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

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

ステップ 9 [VPN Gateway Configuration] ウィンドウでその他のフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 10 **[保存（Save）]** をクリックします。

次のタスク

次のいずれかを実行します。

- #unique_394または
- #unique_395

電話での V.150 サポートの設定

電話に V.150 のサポートを追加するには、次の手順を使用します。V.150 をサポートする電話のタイプは次のとおりです。

- Cisco 7962：Cisco 7962 として登録されているサード パーティ SCCP エンドポイント
- 7961G-GE：Cisco 7961G-GE として登録されているサード パーティ SCCP エンドポイント
- サード パーティ AS-SIP エンドポイント

始める前に

必ず目的の電話番号と同じユーザ ID を使用してエンド ユーザを作成してください。

サードパーティ AS-SIP SIP エンドポイントの [エンド ユーザ設定（End User Configuration）] ウィンドウの [ダイジェスト クレデンシャル（Digest Credentials）] フィールドを必ず設定してください。

新しいエンド ユーザの設定方法の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『*System Configuration Guide for Cisco Unified Communications Manager*』の「「Provision End Users Manually」」の章を参照してください。

手順

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

ステップ 2 次のいずれかの手順を実行します。

- 既存の電話で V.150 を設定するには、[検索（Find）] をクリックして電話を選択します。
- 新しい電話で V.150 を設定するには、[新規追加（Add New）] をクリックします。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウンリストから、V.150 をサポートする電話のタイプを選択し、[次へ（Next)] をクリックします。

ステップ 4 Cisco 7962 として登録されているサードパーティ SCCP エンドポイントの場合：[Device Protocol] ドロップダウン リストから [SCCP] を選択し、[次へ（Next)] をクリックします。

ステップ 5 [Media Resource Group List] ドロップダウン メニューから [V.150] を選択します。

ステップ 6 サード パーティ AS-SIP SIP エンドポイントのみ。次のフィールドを設定します。

- [Digest User] ドロップダウンからこの電話のエンドユーザを選択します。このエンドユーザがダイジェスト認証に使用されます。
- [メディア ターミネーション ポイント必須（Media Termination Point Required）] チェックボックスはオフのままにします。
- [音声とビデオ コールの Early Offer サポート（Early Offer support for voice and video calls）] 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。
[Apply Config] のメッセージ ウィンドウが表示されます。

ステップ 8 [設定の適用（Apply Config）] をクリックします。

ステップ 9 [OK] をクリックします。

SIP トランク設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	V.150 の SIP プロファイルの設定 （360 ページ）	SIP プロファイルで SIP トランクの SIP Best Effort Early Offer サポートを設定します。
ステップ 2	クラスタ全体の V.150 フィルタの設定 （361 ページ）	オプション。クラスタ全体での SIP V.150 SDP オファー フィルタリングのデフォルト設定を行います。
ステップ 3	SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加 （362 ページ）	特定の SIP トランクに割り当て可能な SIP トランク セキュリティ プロファイル内で V.150 フィルタを設定します。
ステップ 4	V.150 の SIP トランクの設定 （362 ページ）	V.150 コールを処理する SIP トランクで V.150 サポートを設定します。

V.150 の SIP プロファイルの設定

SIP プロファイルで SIP トランクの SIP Best Effort Early Offer サポートを設定するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified CM の管理で、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIP プロファイル（SIP Profile）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

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

ステップ 3 [名前(Name)] フィールドに、V.150 の SIP 名を入力します。

ステップ 4 [説明（Description)] フィールドに、V.150 の説明を入力します。

ステップ 5 [Early Offer Support for Voice and video class] ドロップダウンリストから [Select Best Effort (no MTP inserted)] を選択します。

ステップ 6 必要なその他の設定値を入力します。フィールドとその設定オプションの詳細については、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。

クラスタ全体の V.150 フィルタの設定

クラスタ全体での SIP V.150 SDP オファー フィルタリングのデフォルト設定には、次の手順を使用します。

（注） SIP トランク セキュリティ プロファイル内の [SIP V.150 SDP Offer Filtering] 値に、クラスタ全体のサービス パラメータ設定とは異なる値を設定すると、このセキュリティ プロファイル設定により、そのセキュリティ プロファイルを使用するトランクのクラスタ全体のサービス パラメータ設定がオーバーライドされます。

手順

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

ステップ 2 [サーバ（Server）] ドロップダウン リストからアクティブなサーバを選択します。

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

ステップ 4 [Clusterwide Parameters (Device- SIP)] セクションで [SIP V.150 SDP Offer Filtering] サービス パラメータの値を設定します。

ステップ 5 ドロップダウン リストから [SIP V.150 SDP Offer Filtering] を選択します。

ステップ 6 目的のフィルタリング アクションを指定します。

ステップ 7 **[保存 (Save)]** をクリックします。

次のタスク

SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加 （362 ページ）

SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加

SIP トランク セキュリティ プロファイル内で V.150 フィルタを割り当てるには、次の手順を実行します。

（注） SIP トランク セキュリティ プロファイルの [SIP V.150 SDP Offer Filtering] に、クラスタ全体のサービス パラメータとは異なる値を設定すると、このセキュリティ プロファイル設定は、そのセキュリティ プロファイルを使用するトランクのクラスタ全体のサービス パラメータ設定をオーバーライドします。

始める前に

クラスタ全体の V.150 フィルタの設定 （361 ページ）

手順

ステップ 1 [Cisco Unified CM Administration] から **[システム(System)]** > **[セキュリティ（Security）]** > **[SIP Trunk Security Profile]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存の SIP トランク セキュリティ プロファイルの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、リストから既存のプロファイルを選択します。
- 新しい SIP トランク セキュリティ プロファイルを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [SIP V.150 SDP Offer Filtering] ドロップダウン リストの値を設定します。

（注） デフォルト設定では、クラスタ全体のサービス パラメータ [SIP V.150 Outbound SDP Offer Filtering] の値が使用されます。

ステップ 4 [SIP Trunk Security Profile Configuration] ウィンドウのその他のフィールドをすべて設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 **[保存 (Save)]** をクリックします。

次のタスク

V.150 の SIP トランクの設定 （362 ページ）

V.150 の SIP トランクの設定

SIP トランクの設定を行うには、次の手順に従います。

始める前に

SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加 （362 ページ）

手順

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

ステップ 2 次のいずれかの手順を実行します。

- 新しいプロファイルを作成するには、[Add New] をクリックします。
- 既存のトランクを選択するには、[Find] をクリックして SIP トランクを選択します。

ステップ 3 新しいトランクの場合は次の手順に従います。

- [Trunk Type] ドロップダウンリストから [SIP Trunk] を選択します。
- [Protocol Type] ドロップダウンリストから、[SIP] を選択します。
- [Trunk Service Type] ドロップダウン リストから [None(Default)] を選択します。
- [次へ（Next)] をクリックします。

ステップ 4 [名前(Name] フィールドに SIP トランク名を入力します。

ステップ 5 [説明(Description)] フィールドに SIP トランクの説明を入力します。

ステップ 6 **[Media Resource Group List]** ドロップダウンリストから、「「V.150」」という名前のメディア リソース グループ リストを選択します。

ステップ 7 SIP トランクの宛先アドレスを設定します。

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

b) 宛先が DNS SRV レコードの場合は [Destination Address is an SRV] チェック ボックスをオンにします。

c) 宛先を追加するには、[+] ボタンをクリックします。SIP トランクには最大 16 個の宛先を追加できます。

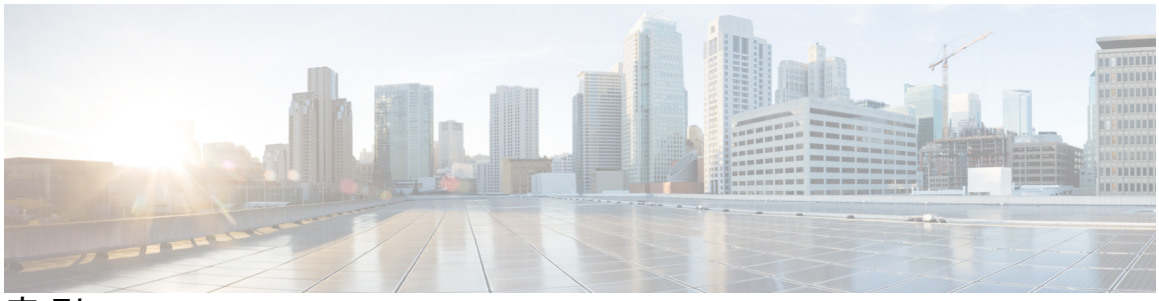
ステップ 8 [SIP Trunk Security Profile] ドロップダウンリストから、このトランクに設定した SIP トランク セキュリティ プロファイルを割り当てます。

ステップ 9 [SIP Profile] ドロップダウンリストから、[Best Effort Early Offer] 設定でセットアップした SIP プロファイルを割り当てます。

ステップ 10 [Media Termination Point Required] チェックボックスはオフのままにします。

ステップ 11 [Trunk Configuration] ウィンドウのその他のフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 12 **[保存 (Save)]** をクリックします。



索引

き

こ

し

せ

た

て

と

に

ふ

ほ

め

ゆ

れ

ろ

わ