Cisco Unified Communications Manager リリース 12.5（1）SU2 セキュリティガイド

First Published: 2020-02-03

Last Modified: 2021-09-27

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

CONTENTS

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タスクを実行するのに役立つものです。

- 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 電話モデル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、または削除するには、Certificate Authority Proxy Function (capf) を設定します。
- 電話機のセキュリティ強化を設定します。
- 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にゲートウェイとトランクを設定します。
- FIPS (連邦情報処理標準) 140-2 モードを設定します。

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。

組織

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	セキュリティ用語、システム要件、連携動作と制限事項、インストール要件、および設定チェックリストの概要を示します。では、さまざまなタイプの認証と暗号化について説明します。
Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS）	HTTPS の概要を示し、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	には、Cisco Unified IP 電話の自動セキュリティ機能を提供するデフォルトのセキュリティ機能に関する情報が記載されています。
Cisco CTL クライアントの設定	CiscoCTL クライアントをインストールして設定することによって認証を設定する方法について説明します。
TLS セットアップ	
証明書	
証明書概要	
電話とボイスメール ポートのセキュリティ	
電話機のセキュリティ	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	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	セキュア通知トーンを再生するように電話機を設定する方法について説明します。
アナログエンドポイント設定への暗号化	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について説明します。
暗号化された電話設定ファイルの設定	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	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	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	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セキュリティの設定	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	セキュアコールのモニタリングと録音を設定する方法について説明します。
CiscoIPPhones 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 の認証と暗号化の設定	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	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。
ゲートウェイとトランクの暗号化の設定	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	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	[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	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	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 の最小必須要件 (MER)	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、章のトピックの関連資料のリストが含まれています。

関連する CiscoIP 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* 電話 の管理ガイド

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、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http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.htmlで示されています。

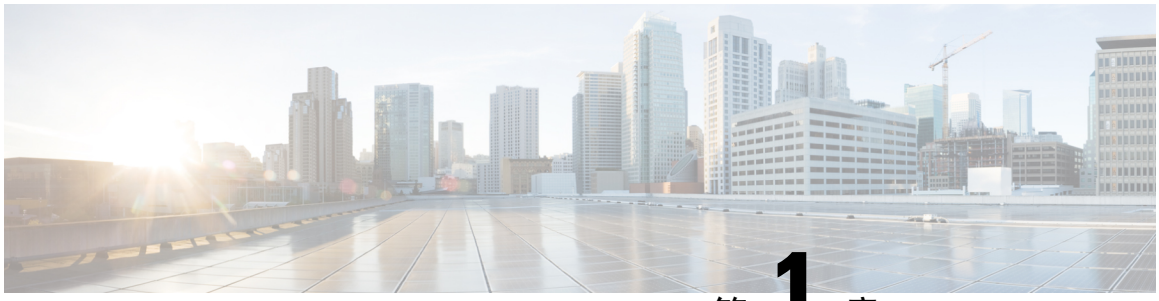
シスコ製品のセキュリティの概要

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したものとみなされます。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

セキュリティの基本



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。

CiscoIP 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 電話 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、CiscoIPtelephony 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ときに適用されます。

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と権限を定義するリスト。方式リストを参照してください。
認証（Authentication）	通信エンティティの id を確認するプロセス。
承認	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。
証明局（CA）	証明書を発行する信頼できるエンティティ: 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	ダイジェスト認証では、SIP ユーザエージェントに対して id を認証するよう要求します。

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、シスコの認証局が署名する 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 ファイルに署名するため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	共有パスワードの MD5 ハッシュが SIP ユーザエージェントの id を確立するために使用される、デバイス認証の形式。
[ダイジェストユーザ（Digest User）]	SIP または SIP トランクを実行している電話が送信する認証要求に含まれるユーザ名。
デジタル署名（Digital Signature）	メッセージをハッシュしてから、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用して別のハッシュを生成し、2つのハッシュを比較して、メッセージが一致し、コンテンツがそのままであることを確認します。
DSP	デジタル シグナリング プロセッサ。
DSP ファーム	H.323 またはシスコの CP ゲートウェイで Dsp によって提供される IP テレフォニー会議用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。これにより、情報の機密性が確保され、目的の受信者だけがデータを読み取ることができるようになります。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、ファイルの改ざんが発生しないように、電話機でシグニチャを検証します。
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。
hash	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保証する IETF 定義のプロトコル。暗号化を使用することにより、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が確保されます。
イメージ認証	電話機にロードする前に、バイナリイメージの整合性とソースを検証するプロセス。
整合性	エンティティ間でデータの改ざんが発生しなかったことを保証するプロセス。
IPSec	エンドツーエンドのセキュリティのためにセキュアな h.323、.H、および RAS シグナリングチャネルを提供するトランスポート。
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。電話機または JTAPI/TAPI/CTI アプリケーションにインストールされている。
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。メディア暗号化では、IETFRFC3711 で定義されているように、Secure Real Time Protocol (SRTP) を使用します。
メッセージ/データの改ざん	攻撃者が転送中にメッセージを変更しようとした場合に発生するイベント。これには、コールの終了が含まれます。
方式リスト	承認プロセス中に SIP トランクで受信できるメッセージの特定のカテゴリを制限するツール。トランク側のアプリケーションまたはデバイスに対して許可される SIP 非 Invite 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。
Nonce	ダイジェスト認証要求ごとにサーバが生成する一意のランダムな番号。MD5 ハッシュを生成するために使用されます。
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または暗号化されていないコール。
非セキュアなデバイス	UDP または TCP シグナリングおよび非セキュアメディアを使用するデバイス。

用語	定義
PKI	公開キーインフラストラクチャ。公開キーの暗号化に必要な一連の要素 (セキュアな公開キーの配布、証明書、および認証局を含む) で構成されます。
公開/秘密キー	暗号化で使用されるキー。公開キーを利用できますが、秘密鍵は、それぞれの所有者に流通する非対称暗号化は、両方のキーを使用します。
リプレイ アタック	攻撃者が、電話またはプロキシサーバを識別する情報をキャプチャし、実際のデバイスであると偽装して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を偽装します。
RTP	リアルタイム トランスポート 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 コール	すべてのデバイスが認証され、シグナリングが暗号化され、メディア (音声ストリーム) が暗号化されるコール。
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。
Transport Layer Security（TLS）	インターネット上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。機能的には SSL と同等です。

用語	定義
信頼リスト（Trust List）	デジタル署名のない証明書リスト。
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 証明書をインポートするための ITU-T 暗号化規格。証明書の形式が含まれています。

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、クラスタ内のすべてのサーバで異なる場合があります。
- 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。

関連トピック

CAPF システム インタラクションと要件

機能リスト

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、音声ドメインへのアクセスを制御および防止するためのシグナリング認証と暗号化のための TLS と IPSec が含まれています。SRTP は、音声会話やその他のメディアのプライバシーと機密性を保護するために、メディア認証と暗号化を追加します。

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
トランスポート/接続/整合性	セキュアな TLS ポート	IPSec 関連付け

セキュリティ機能	回線側	トランク側
デバイス認証	Unified Communications Manager や CAPF による TLS 証明書交換	IPSec 証明書の交換または事前共有キー
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)、またはその両方]
メディア暗号化	SRTP	SRTP
承認	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* コールセキュリティ機能

セキュリティ機能	回線側	トランク側
トランスポート/接続/整合性	セキュアな 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 証明書の交換または事前共有キー
ダイジェスト認証	各 SIP デバイスは、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 電話 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
承認	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機には、コールのセキュリティレベルが表示されます。

- 電話機には、認証済みのシグナリングセキュリティレベルのコールのシールドアイコンが表示されます。シールドは、Cisco IP デバイス間のセキュアな接続を識別します。これは、デバイスに認証済みまたは暗号化済みのシグナリングがあることを意味します。
- 電話機には、暗号化されたメディアを含むコールのロックアイコンが表示されます。これは、デバイスが暗号化された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） 一部の電話機モデルでは、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、クラスタ間、およびマルチホップコールで変更できます。SCCP 回線、SIP 回線、および h.323 シグナリングは、参加しているエンドポイントに対するコールセキュリティステータスの変更に関する通知をサポートします。セキュリティアイコンに関連付けられている制限については、セキュリティアイコンと暗号化に関連するトピックを参照してください。

コールの音声およびビデオ部分は、コールのセキュリティステータスに基づいています。音声とビデオの両方の部分がセキュアである場合にのみ、コールの安全を考慮してください。次の表では、セキュリティアイコンが表示されるかどうか、および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ルール

コール内のメディアタイプとデバイスタイプ	シールドアイコンとロックアイコンの両方を表示する電話機	ロックアイコンのみを表示する電話機
セキュアな音声のみ	ロック	ロック
セキュアでないビデオでのセキュアな音声	シールド	なし
セキュアなビデオによるセキュアな音声	ロック	ロック
非セキュア音声のみを使用する認証済みデバイス	シールド	なし
非セキュアな音声およびビデオを備えた認証済みデバイス	シールド	なし

コール内のメディアタイプとデバイスタイプ	シールドアイコンとロックアイコンの両方を表示する電話機	ロックアイコンのみを表示する電話機
非セキュア音声のみを使用する非認証デバイス	なし	なし
非セキュアな音声およびビデオを備えた未認証デバイス	なし	なし

（注） 「コールセキュリティステータスを指定した場合の BFCP アプリケーション暗号化ステータスのオーバーライド」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場合に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。

会議および割り込みコールの場合、[セキュリティ (security)] アイコンに会議のセキュリティステータスが表示されます。

関連トピック

セキュアな会議アイコン, on page 255

連携動作と制限事項

ここでは、インタラクションと制限事項について説明します。

セキュア会議機能に関連付けられているインタラクションと制限については、「関連項目」を参照してください。

関連トピック

連携動作, on page 10
[Restrictions（機能制限）], on page 11
セキュアな会議リソースの設定, on page 253

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シスコ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

認可されたユーザに送信されるプレゼンス要求を制限するために、プレゼンスグループを設定します。SIP を実行している電話機およびトランクに対して、プレゼンスグループの許可を追加できます。

プレゼンスグループの設定の詳細については、Cisco Unified Communications Manager 機能設定ガイドを参照してください。

SIP トランク上のプレゼンス要求を許可および受け入れるように Unified Communications Manager を設定します。必要に応じて、リモートデバイスまたはアプリケーションからの着信プレゼンス要求を受け入れ、認証するように Unified Communications Manager を設定します。

SIP Trunk

SIP で開始される転送機能や他の高度な転送関連機能を使用するには、SIP トランク セキュリティ プロファイルを設定して、着信要求、Out-of-dialog 要求、REFER 要求を受け入れます。たとえば、Web 転送やクリックツーダイヤルがあります。

イベントをレポートしたり（MWI サポート）、（音声メッセージングサーバからの）コールごとの MTP 割り当てを減らしたりするには、非要請通知 SIP 要求を受け入れるように SIP トランク セキュリティ プロファイルを設定します。

REFERS および INVITES のヘッダーを置き換える SIP 要求を受け入れるように 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 は SIP トランクの外部コールを外部デバイスまたはパーティに転送できるようになりました。

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、ユーザがログインおよびログアウトする際に、異なるエンドユーザが別のログイン情報を保有しているため、SIP ダイジェストログイン情報が変更されます。

コンピュータ テレフォニー インテグレーション（CTI）

Cisco Unified Communications Manager Assistant は、CAPF プロファイルを（Cisco Unified Communications Manager Assistant ノードごとに 1 つ）設定している場合に CTI へのセキュアな接続をサポートします（トランスポート層セキュリティ接続）。

CTI TLS サポートでは、CTI/JTAPI/TAPI アプリケーションの複数のインスタンスが実行されている場合に、すべてのアプリケーションインスタンスに固有の InstanceID（IID）を設定する必要があります。IID 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します。

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になっている場合、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と同じ場合、Cisco Unity TSP は CTI Manager ポートを介して Unified Communications Manager に接続します。

[Restrictions（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約事項について説明します。

関連トピック

認証および暗号化, on page 12

割り込みと暗号化, on page 12
クラスタおよびデバイスのセキュリティモード, on page 15
ダイジェスト認証と暗号化, on page 15
メディアリソースと暗号化, on page 13
パケット キャプチャと暗号化, on page 16
電話機のサポートと暗号化, on page 13
電話機のサポートと暗号化されたセットアップファイル, on page 14
セキュリティ アイコン, on page 9
ワイドバンドコーデックと暗号化, on page 13

認証および暗号化

認証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。

- デバイス認証なしでシグナリングまたはメディア暗号化を実装することはできません。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、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。

  ファイアウォールでUDPを有効にして、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ことができます。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介して双方向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存在する必要があります。

シグナリング暗号化は、NAT トラバーサルをサポートしていません。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 電話 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 電話 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 電話 は、暗号化されたコールに割り込むことができます。[セキュリティ (security)] アイコンは、会議のセキュリティステータスを示します。

関連トピック

セキュアな会議アイコン, on page 255

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 電話 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 電話 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 電話 （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。

- トランスコーダが関係するコール
- メディアターミネーションポイントを含むコール

（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。

電話機のサポートと暗号化

SCCP を実行している次の Cisco Unified IP 電話 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 電話 は暗号化をサポートします。6901、6911、6921、6941、6945、6961、7811、7821、7841、7861、7832、7906G、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 電話 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。これらの電話機は、認証済みまたは非セキュアの参加者としてのみ、セキュアな会議および割り込みコールに参加できます。

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 電話 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。

電話機のサポートと暗号化されたセットアップファイル

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。一部の電話機は暗号化された設定ファイルをサポートしていますが、ファイルシグニチャを検証しません。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。

関連トピック

電話機モデルのサポート, on page 191

セキュリティアイコンと暗号化

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。

- コールの転送や保留などのタスクを実行すると、暗号化ロックアイコンが電話機に表示されないことがあります。MOH など、これらのタスクに関連付けられているメディアストリームが暗号化されていない場合、ステータスは [暗号化 (encrypted)] から [非セキュア (not)] 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 を含むコールの場合、セキュリティアイコンには、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が表示されます。
- TLS 転送タイプを使用している場合、SIP トランクは暗号化された、または認証されていないセキュリティステータスを報告します。SRTP がネゴシエートされると、セキュリティステータスが暗号化されます。それ以外の場合は、認証されません。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。

会議やc割り込みなどのイベント中にパーティが認証されると、SIPトランクはトランク経由で認証済みステータスを報告します。(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に、sip トランクは sip 回線で現在使用されているように、sipトランクを介してセキュリティアイコンステータスを送信するために既存のコール情報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。
- 一部の電話機モデルでは、シールドアイコンではなく、ロックアイコンのみが表示されます。

関連トピック

セキュアな会議アイコン, on page 255

クラスタおよびデバイスの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 電話 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。

電話機は、クラスタセキュリティモードが混合である場合にのみ、SRST対応ゲートウェイへのセキュアな接続を試行します。電話機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済みに設定されていて、SRST が許可されているかどうかを確認します。[トランクの設定 (Trunk Configuration)] ウィンドウでチェックボックスがオンになっており、有効な SRST 証明書が電話機の設定ファイルに存在します。

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）。各コールレッグは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、各コールレッグのダイジェスト認証は他のコールレッグから独立したままになります。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暗号化が実装されている場合、サードパーティスニッフィングツールは機能しません。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

Unified Communications Manager のセキュリティを設定する際には、次のベストプラクティスをお勧めします。

- 大規模なネットワークに導入する前に、安全なラボ環境でセキュリティのインストールと設定を必ず行ってください。
- 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 IPSec を使用します。

警告 IPSec の使用に失敗した場合は、セッション暗号キーがクリアテキストで送信されます。

- 電話料金の詐欺行為の防止するため、電話会議の機能拡張を設定します。詳細については、Cisco Unified Communications Manager システム設定ガイドを参照してください。

  コールの外部転送を制限するため、設定タスクを実行します。詳細については、Cisco Unified Communications Manager 機能設定ガイドを参照してください。

関連トピック

割り込みセットアップによるメディア暗号化, on page 18
デバイス、サーバ、クラスタ、およびサービスのリセット, on page 17

デバイスのリセット、サーバとクラスタのリブート、およびサービスの再起動

ここでは、デバイスをリセットする必要がある場合、サーバ/クラスタを再起動する場合、またはシスコユニファイドサービスを再起動する必要がある場合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で別のセキュリティプロファイルを適用した後、単一のデバイスをリセットします。
- 電話機のセキュリティ強化タスクを実行する場合は、デバイスをリセットします。

- クラスタセキュリティモードを混合モードから非セキュアモード (またはその逆) に変更した後で、デバイスをリセットします。
- Cisco CTL クライアントを設定した後、または CTL ファイルを更新した後に、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、デバイスをリセットします。
- TLS 接続のポートを更新した後、Cisco CTL Provider サービスを再起動します。
- クラスタセキュリティモードを混合モードから非セキュアモード (またはその逆) に変更した後、Cisco CallManager サービスを再起動します。
- 関連付けられた CAPF サービスパラメータを更新した後、Cisco Certificate Authority Proxy Function サービスを再起動します。
- Cisco CTL クライアントを設定した後、または CTL ファイルを更新した後に、シスコユニファイドサービスのすべての Cisco CallManager および cisco TFTP サービスを再起動します。クラスタ内でこれらのサービスを実行しているすべてのサーバで、次の作業を実行します。
- CTL プロバイダーサービスを開始または停止した後、すべての Cisco CallManager および Cisco TFTP サービスを再起動します。
- セキュア SRST 参照を設定した後、依存デバイスをリセットします。
- スマートカードサービスを開始および自動に設定した場合は、Cisco CTL クライアントをインストールした PC を再起動します。
- 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ているセキュリティ関連のサービスパラメータを設定した後、Cisco IP Manager Assistant サービス、Cisco Web Dialer 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。

電話機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するトピックを参照してください。

関連トピック

電話機へのセキュリティ プロファイルの適用 , on page 219

デバイス、サーバ、クラスタ、およびサービスのリセット

このセクションでは、Cisco Unified Serviceability で、デバイス、サーバ、クラスタ、およびサービスをリセットするシナリオについて説明します。

クラスタ内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。

手順

Step 1 Unified Communications Managerから、**[システム（System）]** > **[CiscoUnifiedCM]** を選択します。

Step 2 [検索（Find）] をクリックします。

設定されている Unified Communications Manager サーバの リストが表示されます。

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

Step 4 [リセット（Reset）] をクリックします。

Step 5 クラスタ内のサーバごとにステップ 2 とステップ 4 を実行します。

関連トピック

デバイスのリセット、サーバとクラスタのリブート、およびサービスの再起動, on page 16

割り込みセットアップによるメディア暗号化

暗号化用に Cisco Unified IP 電話 7962 および 7942 の割り込みを設定し、 Cisco Unified Communications Manager Administration で次のタスクを実行します。

- CTL クライアントで [クラスタセキュリティモード（Cluster Security Mode）] パラメータを更新します。
- [サービスパラメータ（Service Parameter）] ウィンドウで、[有効な組み込みブリッジ（Builtin Bridge Enable）] サービスパラメータを更新します。

タスクが完了すると、次のメッセージが表示されます。

注目 Cisco Unified IP 電話 モデル 7962 および 7942 の暗号化を設定する場合、暗号化されたデバイスは、暗号化されたコールに参加しているときに割り込みリクエストを受け入れ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。

Cisco Unified IP 電話7962 および 7942 （暗号化されたセキュリティ プロファイルで設定済み）では、[電話の設定（Phone Configuration）] ウィンドウにメッセージが表示 されません。[組み込みブリッジ（Built In Bridge）] 設定に **[デフォルト（Default）]** を選択するか、または [Default] と同等のデフォルト設定を選択します。いずれの選択にも同じ制限が適用されます。

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

関連トピック

割り込みと暗号化, on page 12

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

認証サポートを取得するには、次のいずれかのオプションを使用できます。

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

トランスポートセキュリティは、データのコーディング、パッキング、および送信を処理します。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、 CiscoIOS 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。

SRTP をサポートするデバイスで次のレベルのセキュリティを確保するために、セキュア RTP (SRTP) を TLS および IPSec トランスポートサービスに追加できます。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、CiscoUnifiedIPPhones 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、リプレイ攻撃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、IP 電話 と同じようにセキュアで信頼性の高いデータ転送モードを確立し、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を表示し、自己署名証明書を再生成し、 Cisco Unified Communications オペレーティングシステムの GUI で信頼証明書を削除することができます。

管理者は、コマンドラインインターフェイス (CLI) で自己署名証明書を再生成して表示することもできます。

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、共通名と同じ有効期間があるものの、シリアル番号と署名アルゴリズムが異なっていることを確認してください。

たとえば、`27:20:41: 0c: 5b:08:69:80:42:62: 4f:13: bd:16:06: 6a`のシリアル番号と SHA1 アルゴリズムが Cisco Unified Communications Manager tomcat 信頼に存在するルート CA です。`7b:35:33:71: 0b: 7c:08: b2:47: b3: aa: f9: 5c: 0d: ca: e4`シリアル番号と SHA256 アルゴリズムを使用して証明書をアップロードしようとすると、証明書の管理は次のように行われます。

1. 着信証明書の有効性が確認されます。
2. 同じ共通名の証明書が、tomcat trust フォルダで検索されます。
3. Tomcat trust フォルダに存在する証明書のシリアル番号と、アップロードする着信証明書がチェックされます。シリアル番号が異なる場合は、両方の証明書の有効期限の開始日が確認されます。着信証明書の有効開始タイムスタンプが既存の証明書の有効開始タイムスタンプよりも後の場合、既存の証明書は tomcat trust フォルダ内の新しい着信証明書に置き換わります。それ以外の場合、新しい着信証明書はアップロードされません。

SHA1 アルゴリズムと SHA256 アルゴリズムの両方に同じサブジェクト名または共通名があります。これは、それらが同じエンティティに属していることを意味します。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。シグニチャアルゴリズムに関係なく、特定の信頼フォルダでは、どのエンティティにも属する1つの証明書のみがサポートされます。

関連トピック

電話機の証明書タイプ, on page 21
サーバ証明書のタイプ, on page 23
外部 CA からの証明書のサポート, on page 24

電話機の証明書タイプ

電話機証明書は、電話機を認証するための一意の識別子です。これは、IP 攻撃に対するセキュリティにとって重要です。

電話機の証明書は次のとおりです。

表 *6:*

電話機の証明書	説明
製造元でインストールされる証明書（MIC）	MIC は Cisco Manufacturing CA によって署名され、署名された証明書はサポートされている Cisco Unified IP 電話 に自動的にインストールされます。 MICは、ローカルで有効な証明書（LSC）のインストールまたは暗号化された設定ファイルのダウンロードに対して、シスコ認証局プロキシ機能（CAPF）で認証します。管理者は証明書を変更、削除、または無効にできないため、有効期限が切れた後は使用できません。
ローカルで有効な証明書（LSC）	Cisco Unified IP 電話 は、セキュアモードで動作するために LSC を必要とし、認証と暗号化に使用されます。これらは CAPF、オンラインまたはオフライン CA により署名され、MIC よりも優先されます。 CAPF に関連付けられている必要なタスクを実行すると、サポートされている電話機にこの証明書がインストールされます。認証または暗号化を使用するようにデバイス セキュリティ モードを設定した後に、LSC により、Unified Communications Manager と電話機間の接続のセキュリティが確保されます。

ヒント 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、Unified Communications Manager との TLS 接続の認証用に LSC をサポートしています。電話の設定で TLS 認証などの目的でMICを使用した場合、MICルート証明書は容易に侵害されるため、当社は何ら責任を負いません

Unified Communications Manager への TLS 接続に LSC を使用するには、Cisco Unified IP 電話 6900、7900、8900、および9900シリーズをアップグレードします。今後の互換性の問題を回避するために、Unified Communications Manager 信頼ストアから MIC ルート証明書を削除します。

（注） Unified Communications Manager への TLS 接続に MIC を使用する一部の電話機モデルは、登録できない場合があります。

管理者は Unified Communications Manager 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。Unified Communications Manager 信頼ストアの更新と証明書の管理については、Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。

（注） CallManger 信頼ストアから Cisco Manufacturing 証明書を削除すると、電話機の製造元でインストールされた証明書（MIC）を検証できないため、セキュアオンボーディング機能は動作しません。

関連トピック

認証と暗号化のセットアップ, on page 42

サーバ証明書のタイプ

サーバ証明書は、基本的にサーバを識別するための証明書です。サーバ証明書は、コンテンツを暗号化および復号化する論拠の役目を果たします。

Unified Communications Manager サーバ内の自己署名証明書（所有）証明書タイプは次のとおりです。

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

表 7: 証明書タイプと説明

証明書タイプ	説明
Cisco Unity サーバまたは Cisco Unity Connection 証明書	Cisco Unity と 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 デバイス証明書に署名します。Cisco unityの場合、 Cisco Unity TELEPHONY Integration Manager (UTIM) はこの証明書を管理します。Cisco Unity Connection の場合は、Cisco Unity Connection の管理機能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証明書を使用して、Unified Communications Manager との TLS 接続を確立します。
SIP プロキシサーバ証明書	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 Unified Communications Manager 証明書が含まれている場合、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。

（注） 証明書名は、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ます。すべてのデバイス (またはポート) は、ルート証明書をルートとする証明書を発行します。

次の追加の信頼ストアが存在します。

- tomcat および web アプリケーションの共通信頼ストア
- IPSec-trust
- CAPF-trust
- Userlicensing: 信頼
- TVS-trust
- Phone-SAST-trust
- Phone-CTL-trust

Cisco Unity Connection の CA 信頼証明書の詳細については、Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。これらの信頼証明書は、電子メール、予定表情報、連絡先を取得するための Exchange または Meeting Place Express へのセキュアな接続を確保します。

外部 CA からの証明書のサポート

Unified Communications Manager は、PKCS#10 Certificate Signing Request（CSR; 証明書署名要求）メカニズムを使用して、サードパーティの認証局（CA）との統合をサポートします。このメカニズムには、Unified Communications Manager の GUI でアクセスできます。

現在、サードパーティ CA を使用しているお客様は、CSR メカニズムを使用して次の証明書を発行する必要があります。

- Unified Communications Manager
- CAPF
- IPSec
- Tomcat
- 信頼検証サービス（TVS）

（注） マルチサーバ（SAN）の CA 署名付き証明書は、証明書が発行元にアップロードされた場合にのみクラスタ内のノードに適用されます。新しいマルチサーバ証明書を生成します。新しいノードを追加したり、再作成するたびにクラスタにアップロードします。

システムを混合モードで実行すると、一部のエンドポイントでは、キーサイズが4096以上の CA 証明書を受け入れることができない場合があります。混合モードで CA 証明書を使用するには、次のいずれかのオプションを選択します。

- 証明書のキーサイズが 4096 未満の証明書を使用します。
- 自己署名証明書を使用します。

（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。

（注） 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 クライアントを実行した後、該当するサービスを再起動して更新します。

例：

- Unified Communications Manager 証明書を更新する際 に、TFTP サービスと Unified Communications Manager サービスを再起動します。
- CAPF 証明書を更新するときに CAPF を再起動します。

Unified Communications Manager 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（CSRs）の生成方法については、Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。

関連トピック

Cisco CTL クライアントの設定, on page 113
デフォルトのセキュリティ設定, on page 79

認証、整合性、および許可

整合性と認証は、次の脅威から保護します。

- TFTP ファイルの操作 (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）
- 頭字語で定義している中間者攻撃（認証）
- 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）

認可は、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ことを指定します。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。

関連トピック

認証, on page 30
デバイス認証, on page 26
ダイジェスト認証, on page 28
ファイル認証, on page 27
イメージ認証, on page 26
シグナリング認証, on page 27

イメージ認証

このプロセスでは、電話機にロードする前に、ファームウェアロードのバイナリイメージの改ざんを防止します。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にも、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 電話、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。相互認証では、相互証明書交換のこのプロセスについて説明します。

デバイス認証は、CiscoCTL 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。

関連トピック

Certificate Authority Proxy Function
Cisco CTL クライアントの設定, on page 113

電話機モデルのサポート, on page 191

ファイル認証

このプロセスは、電話機がダウンロードするデジタル署名されたファイルを検証します。たとえば、設定、リングリスト、ロケール、およびCTLファイルなどです。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、TFTPサーバは、呼出音リスト、ローカライズされたca.cnf、およびリングリストwavファイル(sgn形式)などの静的ファイルに署名します。Tftpサーバは、ファイルに対してデータの変更が発生したことを確認するたびに、<デバイス名>のファイルに署名します。

キャッシュが無効になっている場合、TFTPサーバは署名された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をTFTPサーバが確認すると、TFTPサーバはファイルを再署名します。ディスク上の新しいファイルは、削除された保存済みファイルを上書きします。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。

電話機は、TFTPサーバからファイルを受信すると、ファイルの署名を検証することによってファイルの整合性を検証します。電話機で認証済み接続を確立するには、次の基準が満たされていることを確認します。

- 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。
- 認証または暗号化のためにデバイスを設定しました。

関連トピック

Cisco CTL クライアントの設定, on page 113
電話機モデルのサポート, on page 191

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。

関連トピック

Cisco CTL クライアントの設定, on page 113

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は影響しないことに注意してください。

（注） デバイスのダイジェスト認証を有効にすると、デバイスには一意のダイジェストユーザ ID とパスワードを登録する必要があります。

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。

- アプリケーションの場合は、[アプリケーションユーザの設定 (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の場合は、[エンドユーザ (End User)] ウィンドウでダイジェスト認証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に関連付けるには、[電話の設定 (Phone Configuration)] ウィンドウでダイジェストユーザ (エンドユーザ) を選択します。電話をリセットした後、ログイン情報は TFTP サーバから電話機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課題については、SIP レルムを設定します。これにより、レルムのユーザ名 (デバイスまたはアプリケーションユーザ) とダイジェストクレデンシャルが指定されます。

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。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、nonce の有効期間を設定します。Nonce の有効期間は、nonce 値が有効なままになる分数を指定します。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 メッセージを発信する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、デバイスが TLS をサポートしている場合は、デバイスの TLS プロトコルを設定します。デバイスが暗号化をサポートしている場合は、デバイスセキュリティモードを暗号化として設定します。デバイスが暗号化された電話設定ファイルをサポートしている場合は、ファイルの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。SIP レルムは、サービスパラメータ [SIP Station Realm] を使用して電話にチャレンジするように設定します。各ダイジェストユーザは、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持つことができます。

ヒント エンドユーザのダイジェスト認証を有効にしても、ダイジェストクレデンシャルを設定しない場合、電話機は登録に失敗します。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、SIP トランクを介して接続するドメイン (xyz.com など) を表します。これは、要求の送信元を識別するのに役に立ちます。

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に関連するトピック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持つことができます。

関連トピック

SIP 電話のダイジェスト認証の設定, on page 245
暗号化された電話設定ファイルの設定, on page 231
SIP トランクのダイジェスト認証の設定, on page 349

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。許可された SIP 要求をウィンドウで確認す

る場合は、[SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] ウィンドウで承認を指定します。

SIP トランク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 [Digest Authentication] チェックボックスをオンにします。次に、[Application User Configuration] ウィンドウで [allowed SIP request] チェックボックスをオンにします。

SIP トランク認証とアプリケーションレベル認証の両方をイネーブルにすると、最初に sip トランクに対して認証が行われ、次に SIP アプリケーションユーザに対して許可が行われます。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禁止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。したがって、アプリケーションレベルの認証を実行するには、その前に、SIP トランクセキュリティプロファイル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。

関連トピック

設定ファイルの暗号化, on page 38
メディア暗号化, on page 32
シグナリング暗号化, on page 32

セキュア エンド ユーザ ログイン クレデンシャル

Unified Communications Manager リリース 12.5(1) 以降、すべてのエンドユーザ ログイン クレデンシャルは、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

ルは、SHA1 のみを使用してハッシュされていました。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 の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すべてのパスワードまたは PIN は、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）クレデンシャル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。

レポートの生成方法の詳細については、*Cisco Unified CM Administration* のオンライン ヘルプを参照してください。

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 を有効にして、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ことができます。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存在する必要があります。

シグナリング暗号化は、NAT トラバーサルをサポートしていません。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

セキュアリアルタイムプロトコル(SRTP)を使用するメディア暗号化により、目的の受信者だけがサポートされているデバイス間で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。

デバイスは、SRTP を使用できる場合、ネゴシエーション時にステートを示す必要があります。デバイスがキャッシュされた以前のネゴシエーション SDP を同じコール内の異なるデバイスと使用する場合、CUCM は SRTP をサポートしません。

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。少なくとも1つのデバイスが 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。CiscoIOS ゲートウェイとトランクは、認証なしでメディア暗号化をサポートします。CiscoIOS ゲートウェイおよびトランクの場合は、SRTP 機能 (メディア暗号化) を有効にするときに IPSec を設定する必要があります。

警告 ゲートウェイとトランクの SRTP またはシグナリング暗号化を設定する前に、Cisco では、Cisco IOS の転送 CP ゲートウェイ、h.323 ゲートウェイ、および h.323/トランクを使用して ipsec を設定することを強く推奨します。セキュリティ関連情報がクリアテキストで送信されないようにするために、IPSec 設定に依存します。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、セキュリティ関連の情報が公開される可能性があります。

SIP トランクは TLS に依存して、セキュリティ関連の情報がクリアテキストで送信されないようにします。

次の例では、SCCP コールと転送 CP 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つのセットを受信します。1セットはメディアストリーム用、デバイス A はデバイス B、メディアストリームの場合はデバイス B (デバイス A) 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、メディアストリーム (デバイス A) を暗号化および認証するキーを導出します。
5. マスター値の2番目のセットを使用して、デバイス A はメディアストリーム (デバイス B) を認証および復号化するキーを導出します。
6. デバイス B は、逆の動作シーケンスでこれらのセットを使用します。
7. デバイスがキーを受信すると、デバイスは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。

電話会議で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トピックを参照してください。

関連トピック

セキュアな会議リソースの設定, on page 253

TLS および SIP SRTP に対する AES 256 暗号化のサポート

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、128ビット暗号キーを使用した Advanced Encryption Standard (AES) は、暗号化暗号として使用されています。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、必要な変化するセキュリティとパフォーマンスのニーズに合わせて効果的に拡張することはできません。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、TLS および NGE をサポートするセッション開始プロトコル (SIP) SRTP の AES 128 の代わりに、AES 256 暗号化サポートが提供されます。

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 トランクと SIP 回線が開始する接続。
- 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、伝送制御プロトコル (TCP) レイヤとアプリケーションの間のプロトコル層として配置され、クライアントとサーバ間のセキュアな接続を形成し、ネットワークを介して安全に通信できるようにします。TLS を動作させるには、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 AES128 で、...
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384: 暗号ストリングは AES256 です。 SHA384 です。

定義:

- TLS は、Transport Layer Security です
- ECDH は楕円曲線 Diffie-hellman (アルゴリズム) です。
- RSA is Rivest Shamir Adleman (アルゴリズム)
- 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) は、リアルタイムトランスポートプロトコル (RTP) の音声およびビデオメディアと、それに対応するリアルタイムトランスポート制御プロトコル (RTCP) ストリームの両方に機密性とデータの整合性を提供する方法を定義します。SRTP は、暗号化およびメッセージ認証ヘッダーを使用してこの方式を実装します。SRTP では、暗号化は rtp パケットのペイロードにのみ適用され、RTP 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。これらの暗号暗号方式は AEAD_AES_256_GCM と AEAD_AES_128_GCM であり、AEAD は関連データを使用して認証され、GCM は Galois/Counter モードです。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) に存在する場合、AES 128 および SHA-1 ベースの暗号方式よりも高いプライオリティで処理されます。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ています。

- 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 トランクおよび SIP 回線接続での TLS バージョン1.2 のサポートを使用できます。
- 暗号サポート: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (暗号ストリング ECDHE-AES256 SHA384) および TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (暗号ストリング ECDHE-AES128): TLS 1.2 接続が確立されたときに使用可能になります。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 回線および SIP トランクを介した SRTP コールは、GCM ベースの AEAD_AES_256_GCM と AEAD_AES_128_GCM の暗号方式をサポートします。

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は、サポートされている暗号を使用した TLS バージョンの既存の動作を引き続きサポートします。Skinny Call Control Protocol (SCCP) は、以前にサポートされていた暗号方式を使用した TLS 1.2 もサポートしています。
- Sip から非 SIP へのコールでは、引き続き AES 128 および SHA-1 ベースの暗号方式が使用されます。

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機は、AES_CM_128_HMAC_SHA1_80 crypto 暗号方式を使用して MOH、IVR、および警報を再生します。

電話機が IP Voice Media Streaming (IPVMS) に安全に接続すると、AES_CM_128_HMAC_SHA1_80 crypto cipher に優先順位が付与されます。電話機が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 *8*：電話機能とネゴシエートされた暗号方式の比較

電話がサポートする暗号化アルゴリズム	ネゴシエートされた暗号
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

Unified Communications Manager 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、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』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 電話 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。このオプションを有効にすると、デバイスコンフィギュレーション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、暗号化されていない電話機に機密データをダウンロードすることを選択することもできます。たとえば、電話機のトラブルシューティングなどです。

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。

関連トピック

暗号化された TFTP 設定ファイルの概要, on page 231
電話機モデルのサポート, on page 191

暗号化された iX チャネル

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

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

設定

Unified Communications Managerの暗号化された iX チャネルを有効にするには、次のことを実行する必要があります。

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

号化すべき（**All media except BFCP and iX transports must be encrypted**）] に設定されています。

暗号化モード

暗号化された電話機の場合、2 種類のセッション記述プロトコル (SDP) を使用して、Unified Communications Managerがサポートしている暗号化チャネルの暗号化をサポートしています。この暗号化タイプは、エンドポイントがサポートするものであり、Unified Communications Managerの設定可能な項目ではありません。

- **ベストエフォート方式**の暗号化: SDP オファーは暗号化された ix チャネルを目的としていますが、SIP ピアがサポートしていない場合は、暗号化されていない ix チャネルにフォールバックします。このアプローチは、ソリューションで暗号化が必須ではない場合に使用することができます。

  たとえば、暗号化はクラウドで必須であり、単一の企業ではありません。

  ベストエフォート iX 暗号化

  M = アプリケーション 12345 **UDP/UDT/IX** *

  A = セットアップ: actpass

  A = 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 電話 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

Unified Communications Managerは、エンドポイントが完全にセキュアなモードで展開されていない場合に、会議のエンドポイントからのメディアパス内のセキュアなアクティブコントロールメッセージのネゴシエーションを有効にします。たとえば、エンドポイントがオフネットで、モバイルおよびリモートアクセスモードで Unifird CM に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。

- システムは輸出規制要件に準拠しています。
- 会議ブリッジへの SIP トランクはセキュアです。

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への**ベストエフォート暗号化 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への**強制 IX 暗号化**

NMAP スキャン操作

Windows または Linux プラットフォームでネットワークマッパー (NMAP) スキャンプログラムを実行して、脆弱性スキャンを実行できます。NMAP は、ネットワーク調査またはセキュリティ監査のための無料のオープンソースユーティリティを表します。

（注） NMAP DP スキャンが完了するまでに最大18時間かかる場合があります。

構文

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

定義：

-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、進行中のスキャンに関する詳細情報が NMAP によって出力されます。開いているポートが検出されると、システムは開いているポートを表示します。NMAP がスキャンに数分以上かかると推定した場合は、完了時間の推定値を提供します。このオプションは、冗長性をさらに高めるために2回以上使用してください。

-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、デフォルトを上書きします。個々のポート番号は、ハイフンで区切られた範囲であることに注意してください (たとえば、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。

次の手順では、認証と暗号化を実装するために実行する必要があるすべてのタスクについて説明します。指定されたセキュリティ機能に対して実行する必要があるタスク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。

- 新規インストールの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

Step 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。サービスは、アップグレード後に自動的にアクティブになります。

Step 2 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、トラブルシューティング、または削除するには、シスコのユニファイドサービスで 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タスクを実行することで、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。

Step 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。

Step 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。

Step 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。

Step 6 CiscoCTL 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。

Step 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には、次のタスクを実行します。

a) デバイス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のみがサポートされているデバイスの暗号化を設定する場合は、[電話の設定 (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 を実行している一部の電話機の場合)。

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

c) SIP を実行している電話にダイジェスト認証を使用する予定の場合は、[ダイジェスト認証を有効にする (Enable Digest Authentication)] チェックボックスをオンにします。

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

e) コンフィギュレーション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。

Step 8 電話機に電話セキュリティプロファイルを適用します。

次の手順はオプションです。

Step 9 （任意） ローカルで有効な証明書がサポートされている Cisco Unified IP 電話 にインストールされていることを確認します。

Step 10 （任意） SIP を実行している電話のダイジェスト認証を設定します。

Step 11 （任意） 電話機のセキュリティ強化タスクを実行します。

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。

Step 12 （任意） セキュリティ用の会議ブリッジ リソースを設定します。

Step 13 （任意） セキュリティのために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。

Step 14 （任意） 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。

Step 15 （任意） 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。

Step 16 （任意） 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予定の場合は、プロファイルの [ダイジェスト認証の有効化 (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は、許可されている SIP 要求の [authorization] 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にアプリケーションレベルの認証を実行する場合は、[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。

Step 17 （任意） 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。

Step 18 （任意） トランクのダイジェスト認証を設定します。

Step 19 （任意） SIP トランクセキュリティプロファイルの [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 [Authorization] チェックボックスをオンにして、許可された SIP 要求を設定します。

Step 20 （任意） すべての電話をリセットします。

Step 21 （任意） すべてのサーバをリブートします。

関連トピック

Certificate Authority Proxy Function サービスの有効化
Cisco CTL Provider サービスの有効化, on page 117
電話機へのセキュリティ プロファイルの適用 , on page 219
SIP トランクセキュリティプロファイルの適用, on page 346
認証, on page 30
Cisco CTL クライアントのインストール
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, on page 18
SIP 電話のダイジェスト認証の設定, on page 245
SIP トランクのダイジェスト認証の設定, on page 349
暗号化された TFTP 設定ファイルのヒント, on page 235
暗号化された電話設定ファイルの設定, on page 231

ゲートウェイおよびトランクの暗号化の設定, on page 327
電話の認証文字列の入力
ネットワーク インフラストラクチャ内の IPSec 設定, on page 332
電話のセキュリティ強化, on page 249
電話セキュリティプロファイルの設定の前提条件, on page 202
デバイス、サーバ、クラスタ、およびサービスのリセット, on page 17
セキュアな会議リソースの設定, on page 253
セキュアな Survivable Remote Site Telephony（SRST）リファレンス, on page 319
CAPF のセットアップ
Cisco CTL クライアントの設定, on page 113
Cisco CTL クライアントのアップグレードと Cisco CTL ファイルの移行
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, on page 350
電話セキュリティ プロファイルの設定, on page 201
セキュア ポートの設定, on page 118
SIP トランク セキュリティ プロファイルの設定, on page 335
システム要件, on page 7
ボイス メッセージング ポートのセキュリティ設定, on page 269

暗号管理

暗号の管理はオプションの機能で、すべてのTLSおよびSSH接続で許可されるセキュリティ暗号のセットを制御できます。暗号管理を使用すると、弱い暗号を無効にして最小レベルのセキュリティを有効にすることができます。

[**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（Cipher Management）]** 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。

- [All TLS（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、Unified Communications Manager および IM and Presence Service 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、Unified Communications Manager および IM and Presence Service 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。

（注） **[HTTPS TLS]** および **[すべての TLS（All 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（All 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 暗号（SSH Ciphers）]：このフィールドに割り当てられる暗号は、Unified Communications Manager および IM and Presence Service の SSH 接続に適用されます。

- [SSH キー交換（SSH Key Exchange）]：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、Unified Communications Manager および IM and Presence Service 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。

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

このセクションでは、推奨される暗号を一覧にします。構成済みの暗号に、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。推奨される暗号を設定した後で変更を有効にするには、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-sha2-512,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-group16-sha512, diffie-hellman-group14-sha256
```

非 FIPS 用の SSH KEX

```
ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256,
diffie-hellman-group14-sha1, diffie-hellman-group16-sha512, diffie-hellman-group14-sha256
```

暗号ストリングの設定

- [すべての TLS（All TLS）]、[SIP TLS]、および [HTTPS TLS] フィールドに必ず暗号ストリングを OpenSSL 暗号ストリング形式で入力してください。
- また、**[SSH 暗号（SSH Ciphers）]**、**[SSH MAC]**のアルゴリズム、および**[SSH キー交換（SSH Key Exchange）]** フィールドには、OpenSSH 形式で暗号またはアルゴリズムも入力してください。
- 推奨される暗号 （47 ページ）を確認してください。

異なるセキュアなインターフェイスで暗号ストリングを設定するには、「暗号の制限事項」セクションを参照してください。

手順

Step 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。
[暗号の管理（Cipher Management）] ページが表示されます。

Step 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。

Step 3 次のフィールドに暗号ストリングを設定しない場合に発生する状況を以下に示します。

- **[すべての TLS（All TLS）] または [HTTPS TLS]** フィールド：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（Enterprise parameters）]**（HTTPS 暗号）ページから設定を実行します。
- [すべての TLS（All TLS）] または [SIP TLS] フィールド：SIP インターフェイスポート（5061）は、暗号化モードの [エンタープライズパラメータ]（TLS 暗号）ページと認証モードの NULL-SHA 暗号から設定を取得します。

（注） **[HTTPS TLS]** または **[SIP TLS]** フィールドに暗号ストリングを設定しない場合、システムはデフォルトで **[ALL TLS（すべての TLS）]** フィールドから設定を取得します。

OpenSSL 暗号ストリングの形式の詳細については、https://www.openssl.org/docs/man1.0.2/apps/ciphers.htmlを参照してください。

Step 4 **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 暗号の OpenSSH 暗号ストリング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暗号（SSH Ciphers）]フィールドに暗号ストリング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
```

Step 5 **[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（SSH Key Exchange）]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
```

Step 6 **[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
```

Step 7 **[保存（Save）]** をクリックします。

（注） **[暗号拡張文字列（Cipher Expansion String）]**および**[アルゴリズム拡張文字列（Algorithm Expansion String）]**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、以下のエラーメッセージが表示されます。

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、以下のエラーメッセージが表示されます。

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（Cipher Expansion String）]** または **[アルゴリズム拡張文字列（Algorithm Expansion String）]**フィールドから暗号またはアルゴリズムを選択します。

対応するフィールドに暗号を設定した場合は、それぞれのサービスをリブートまたは再起動する必要があります。

表 *9*: 設定された暗号と対応するアクション

設定された暗号フィールド	操作
All TLS	暗号ストリングを有効にするために、クラスタ内のすべてのノードをリブートします。
HTTPS TLS	暗号ストリングを有効にするため、すべてのノードで Cisco Tomcat サービスを再起動します。
SIP TLS	暗号ストリングを有効にするために、すべてのノードで Unified Communications Manager を再起動します。
SSH 暗号	暗号ストリングを有効にするために、クラスタ内のすべてのノードをリブートします。

設定された暗号フィールド	操作
SSH キー交換 または SSH MAC	アルゴリズム文字列を有効にするために、クラスタ内のすべてのノードをリブートします。

（注） 暗号は、**[暗号の管理（Cipher Management）]**ページの**[暗号ストリング（Cipher String）]**フィールドに入力して有効にできます。これらの暗号を入力しない場合は、アプリケーションでサポートされているデフォルトの暗号すべてが有効になります。ただし、**[暗号の管理（Cipher Management）]**ページの**[暗号ストリング（Cipher String）]**フィールドに暗号ストリングを入力しない場合は、特定の弱い暗号を無効にすることもできます。

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、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、Unified Communications Manager などのアプリケーションでは、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ではないため、このような暗号をサポートしていない場合があります。個々のアプリケーションインターフェイスでサポートされている暗号のリストの詳細については、「アプリケーションの暗号のサポート （52 ページ）」セクションを参照してください。

GUI での検証

[暗号管理（Cipher Management）] 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 ではなく、AES128_SHA が設定されている場合（ハイフンの代わりに下線を使用）、OpenSSL はこれを無効な暗号スイートとして識別します。

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（TLS Context Configuration）] ページ経由のIM and Presence の Unified Communications Manager 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（Device Security Profile）] が [認証済み（Authenticated）] 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

[暗号管理（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。

[エンタープライズパラメータ（Enterprise Parameter）]「**[TLS の暗号（TLS Ciphers）]**」 が、「*[*サポートされているすべての暗号（*ALL Supported Ciphers*）*]*」 を使用して設定されていて、**[暗号管理（Cipher Management）]** ページが、**[すべての TLS（All TLS）]** インターフェイスの「*AES256-GCM-SHA384:AES256-SHA256*」暗号によって設定されている場合、すべてのアプリケーション SIP インターフェイスは 「*AAES256-GCM-SHA384:AES256-SHA256*」 暗号のみをサポートし、**[エンタプライズパラメータ（Enterprise Parameter）]** の値は無視されます。

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 ***10 : 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 ***11 : Unified Communications Manager IM & Presence*** 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	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

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 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 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 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 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

表 *12 : 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 • 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： aes256-ctr aes256-cbc aes128-ctr aes128-cbc aes256-ctr blowfish-cbc • MAC アルゴリズム： hmac-md5 hmac-sha2-256 hmac-sha1 hmac-sha1-96 hmac-md5-96 • KEX アルゴリズム： ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group1-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
エンドユーザ（Linux OS）	SHA-512 – Hashing (salted)
DRS バックアップ/ RTMT SFTP	AES-128 – Encryption
アプリケーションユーザ	AES-256 – Encryption

暗号の制限

[暗号管理（Cipher Management）] ページでは、OpenSSL または OpenSSH がサポートする暗号を設定できます。ただし、暗号の一部は、偶発的なデータが偶発的に公開されることを回避するために、Cisco のセキュリティ標準に基づいて内部的に無効になっています。

[**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

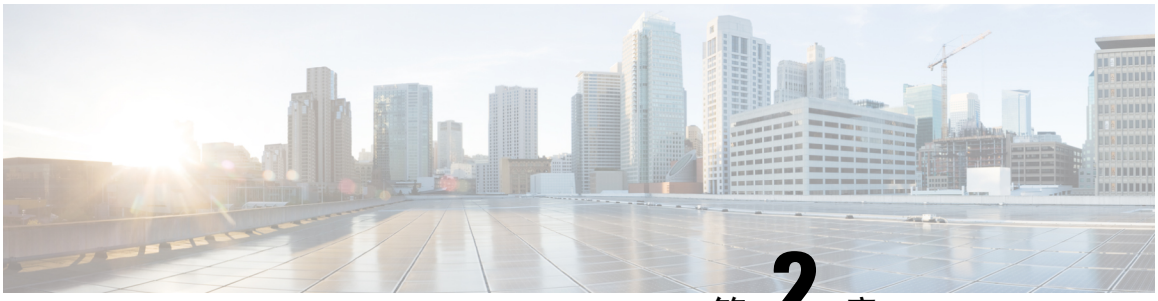
```
hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

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 CiscoIP 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* 一括管理ガイド
- 『*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* 電話 の管理ガイド



第 2 章

Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS）

この章では、セキュアソケットレイヤを介したハイパーテキスト転送プロトコル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 ID を保証し、ブラウザ接続をセキュアにします。HTTPS は、インターネット経由の転送時に、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。Web ブラウザのバージョンが TLS をサポートしている場合は、TLS を使用してセキュリティを向上させることを推奨します。セキュアな HTTPS 通信に 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 *13 : 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（Web Application）**
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 [英語]
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 {"title": "Japanese"}	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（Web Application）
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に、SOAP を使用しているすべての Web アプリケーションには HTTPS が必要です。シスコでは、SOAP アプリケーションの HTTP をサポートしていません。HTTP を使用する既存のアプリケーションは失敗します。ディレクトリを変更することによって HTTPS に変換することはできません。

Cisco Unified IP 電話 サービスの HTTPS

Unified Communications Manager、Cisco IP 電話、および Cisco Unified IP 電話 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。

TV (信頼検証サービス) は、証明書チェーンを検証しません。TV が証明書を確認するには、電話機によって TV に提示されたものと同じ証明書が tomcat 信頼証明書ストアに含まれている必要があります。

TVは、ルート証明書または中間証明書を確認します。アイデンティティ証明書は、データベースに存在しない場合にのみ検証されます。ルート証明書と中間証明書が存在する場合でも、。検証に失敗しました。

HTTPS をサポートする Cisco Unified IP 電話

次の Cisco IP 電話 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） このリスト内の69xx 電話は、HTTPS クライアントとして機能できますが、HTTPS サーバとして機能することはできません。このリスト内の残りの電話機は、HTTPS クライアントまたはHTTPS サーバとして動作できます。

HTTPS をサポートする機能

次の機能は、HTTPS をサポートしています。

- Cisco Extension Mobility（EM）
- Cisco Extension Mobility Cross Cluster（EMCC）
- Cisco Unified Communications Manager Manager Assistant（IPMA）
- Cisco Unified IP 電話 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（Change Credentials）

Cisco Unified IP 電話 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 [エンタープライズパラメータ (Enterprise Parameter)] セクションでセキュアな電話の URL パラメータを削除してから再起動すると、URL パラメータはデフォルトで再入力されます。再起動後に、[セキュアな電話の URL パラメータ (セキュア電話の URL Parameters)] セクションに移動し、URL に対して正しい変更を行い、電話機を再起動します。

表 *14 :* セキュア *Url* の電話機の構成時の設定

フィールド	説明
[セキュア認証URL（Secure Authentication URL）]	電話 Web サーバに対する要求を検証するために電話機で使用するセキュア 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。 この URL はデフォルトでは、インストール時に設定される Cisco Unified Communications の [セルフケアポータル（Self Care Portal）] ウィンドウにアクセスします。 デフォルトの設定を受け入れるには、このフィールドを空白にします。 最大長：255
[セキュアディレクトリ URL（Secure Directory URL）]	電話機がディレクトリ情報を取得する際の取得元サーバのセキュア 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 電話 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。 デフォルトの設定を受け入れるには、このフィールドを空白にします。 最大長：255

フィールド	説明
[セキュアアイドルURL（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 電話 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 分間使用されていない場合、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
[セキュア情報URL（Secure Information URL）]	Cisco IP 電話 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、ユーザが電話機の情報（i）ボタンまたは疑問符（?）ボタンを押すと表示されます。 （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
[セキュアメッセージURL（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 電話 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
[セキュアサービスURL（Secure Services URL）]	Cisco Unified IP 電話 サービスのセキュア URL を入力します。ユーザが [サービス（Services）] ボタンを押すと、Cisco Unified IP 電話 はこのセキュア URL にアクセスします。 （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。

- [保護された認証URL（Secured Authentication URL）]
- [保護されたディレクトリURL（Secured Directory URL）]
- Secured Idle URL
- [保護された情報URL（Secured Information URL）]
- [Secured Messaged URL]

• [保護されたサービス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する

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。ブラウザの信頼できるルート認証局信頼ストアにインポートされた証明書が含まれている場合は、セキュリティ警告を無視できます。

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

Step 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）。

ブラウザに証明書エラー: Navigation ブロックメッセージが表示され、この web サイトが信頼できないことを示します。

Step 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。

Step 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。

Step 4 証明書の詳細を確認します。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

関連トピック

HTTPS 設定に関する詳細情報の入手先, on page 77

Internet Explorer 8 証明書をファイルにコピーする

証明書をファイルにコピーしてローカルに保存すると、必要な場合は常に証明書を復元できます。

次の手順を実行すると、標準の証明書の保存形式を使用して証明書がコピーされます。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

Step 1 [Certificate Error status] ボックスをクリックします。

Step 2 [証明書の表示（View Certificates）] をクリックします。

Step 3 [詳細（Details）] タブをクリックします。

Step 4 **[ファイルにコピー]** ボタンをクリックします。

Step 5 [Certificate Export Wizard] が表示されます。[次へ（Next）] をクリックします。

Step 6 次のリストは、選択可能なファイル形式を定義しています。エクスポートされたファイルに使用するファイル形式を選択します。[**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): インターネットを介して安全なバイナリ添付ファイルを送信します。は ASCII テキスト形式を使用して、ファイルの破損を防止します。
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。

Step 7 ファイルのコピーをエクスポートする場所を参照し、ファイルに名前を付けます。[保存（Save）] をクリックします。

Step 8 ファイル名とパスが [Certificate Export Wizard] ペインに表示されます。[次へ（Next）] をクリックします。

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

Step 10 [Successful export] 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。

関連トピック

HTTPS 設定に関する詳細情報の入手先, on page 77

HTTPS を使用した Firefox の初回認証

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、次のいずれかのタスクを実行する必要があります。

- **[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ごとに [セキュリティの警告（Security Alert）] ダイアログボックスが表示されます。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。

関連トピック

Internet Explorer 8 証明書をファイルにコピーする, on page 71
Safari 4.x を使用して証明書を信頼できるフォルダに保存する, on page 75

Firefox 3.x を使用して証明書を信頼できるフォルダに保存します。

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

手順

Step 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）。

Step 2 [セキュリティ警告 (Security Alert)] ダイアログボックスが表示されたら、[**リスクを理解**する (I)] をクリックします。

Step 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。

Step 4 [Get Certificate] をクリックします。

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

Step 6 [セキュリティ例外の確認（Confirm Security Exception）] をクリックします。

Step 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) [詳細設定（Advanced）] をクリックします。

c) [証明書の表示（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。

d) 表示する証明書を強調表示し、[**表示 (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) [詳細（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。

[フィールド値 (Field Values)] フィールドに詳細が表示されます。

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。

ファイルに 3. x 証明書をコピー Firefox

証明書をファイルにコピーしてローカルに保存すると、必要な場合は常に証明書を復元できます。

次の手順を実行すると、標準の証明書の保存形式を使用して証明書がコピーされます。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

Step 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。

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

Step 3 [**Encryption**] 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。

Step 4 [Servers] タブをクリックします。

Step 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。

Step 6 ファイルをコピーする場所に移動します。

Step 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)]: プライバシー強化メールを使用して、証明書チェーンを検証し、エンティティ間で情報を転送します。

- [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、データの署名または暗号化のための標準規格です。署名されたデータを検証するために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)]: pkcs＃7 を使用して、証明書チェーンを確認し、エンティティ間で情報を転送します。

Step 8 [保存（Save）] をクリックします。

Step 9 [OK] をクリックします。

関連トピック

HTTPS 設定に関する詳細情報の入手先, on page 77

HTTPS を使用した Safari の初回認証

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、次のいずれかのタスクを実行する必要があります。

- [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ごとに [セキュリティの警告（Security Alert）] ダイアログボックスが表示されます。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 [セキュリティの警告（Security Alert）] ダイアログボックスが表示されなくなります。
- [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。

関連トピック

Internet Explorer 8 証明書をファイルにコピーする, on page 71
Firefox 3.x を使用して証明書を信頼できるフォルダに保存します。, on page 72

Safari 4.x を使用して証明書を信頼できるフォルダに保存する

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

手順

Step 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）。

Step 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。

証明書データを確認することを選択した場合は、[**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)、次のいずれかのオプションを選択します。

a) すべて (all): すべてのオプションが [詳細 (Details)] ペインに表示されます。
b) バージョン1のフィールドのみ:バージョン、シリアル番号、署名アルゴリズム、発行元、有効な From、有効な To、Subject、および公開キーオプションが表示されます。
c) [拡張のみ (Extensions Only)]: サブジェクトキー識別子、キーの使用状況、および拡張キー使用法のオプションが表示されます。
d) [Critical Extensions Only]: 重要な内線番号 (存在する場合) が表示されます。
e) [プロパティのみ (Properties Only)]: サムプリントアルゴリズムとサムプリントオプションが表示されます。

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

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

Step 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。

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

Step 7 [次へ（Next）] をクリックします。

Step 8 [Finish] をクリックします。

セキュリティ警告ボックスには、ユーザの証明書サムプリントが表示されます。

Step 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。

Step 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。

Step 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 証明書が正常にインストールされたことを確認するには、[Certificate] ペインの [certificate **Path**] タブをクリックします。

Safari 4.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てローカルに保存すると、必要な場合は常に証明書を復元できます。

次の手順を実行すると、標準の証明書の保存形式を使用して証明書がコピーされます。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

Step 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。

Step 2 [詳細（Details）] タブをクリックします。

Step 3 **[ファイルにコピー]** ボタンをクリックします。

Step 4 [Certificate Export Wizard] が表示されます。[次へ（Next）] をクリックします。

Step 5 次のリストは、選択可能なファイル形式を定義しています。エクスポートされたファイルに使用するファイル形式を選択します。[**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): インターネットを介して安全なバイナリ添付ファイルを送信します。は ASCII テキスト形式を使用して、ファイルの破損を防止します。
c) 暗号化メッセージ構文標準 PKCS #7 証明書 (.P7B): 証明書および証明書のすべての証明書を、選択した PC にエクスポートします。

Step 6 ファイルのコピーをエクスポートする場所を参照し、ファイルに名前を付けます。[保存（Save）] をクリックします。

Step 7 ファイル名とパスが [Certificate Export Wizard] ペインに表示されます。[次へ（Next）] をクリックします。

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

Step 9 [Successful export] 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。

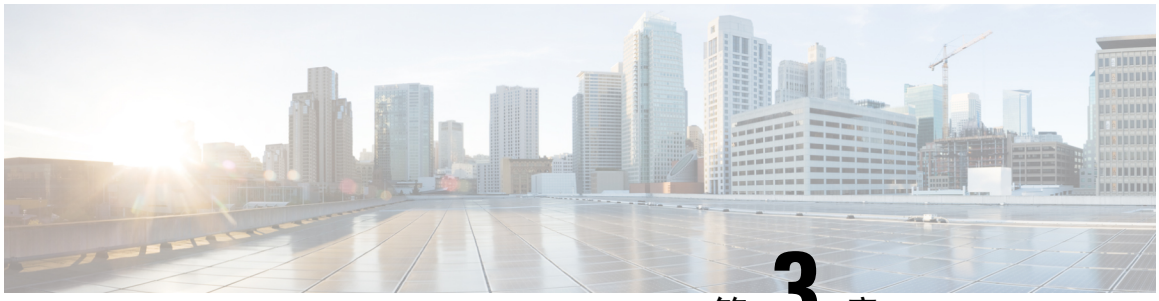
関連トピック

HTTPS 設定に関する詳細情報の入手先, on page 77

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 で入手可能な Microsoft のドキュメンテーション



第 3 章

デフォルトのセキュリティ設定

ここでは、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

デフォルトでは、セキュリティはCisco Unified IP 電話 s に対して次の自動セキュリティ機能を提供します。

- 電話機の設定ファイルの署名
- 電話機の設定ファイルの暗号化のサポート

- 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

ネットワーク内に多数の電話機があり、Cisco Unified IP 電話 のメモリも限られています。したがって、Unified Communications Manager は TVS を介してリモート信頼ストアとして動作するため、各電話機に証明書信頼ストアを配置する必要はありません。Cisco Unified IP 電話 は CTL ファイルまたは ITL ファイルを使用して署名または証明書を検証できないため、検証のために TVS サーバに問い合わせることもできます。したがって、中央信頼ストアを持つことは、信頼ストアをすべての Cisco Unified IP 電話 に持つよりも管理が簡単です。

TVS を使用すると、HTTPS を確立しているときに、Cisco Unified IP 電話 で EM サービス、ディレクトリ、および MIDlet などのアプリケーションサーバを認証できます。

TV には、次の機能があります。

- 拡張性：Cisco Unified IP 電話 のリソースは、信頼する証明書の数に影響されません。
- 柔軟性: 信頼証明書の追加または削除は、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 ファイルを作成してから、クラスタを混合モードに設定する必要がありますCTL ファイルを作成し、クラスタを混合モードに設定するには、CLI コマンド **utils ctl set-cluster mixed-mode** を使用します。

TVS を説明する基本的な概念を次に示します。

- TVS は、Unified Communications Manager サーバ 上で実行され、Cisco IP 電話に代わって証明書を認証します。
- Cisco Unified IP 電話 は、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、TVS を信頼する必要があるだけです。
- 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 Unified IP 電話 によりダウンロードされ、信頼はそこからフローします。

TV の説明

TVS を説明する基本的な概念を次に示します。

- TVS は Unified Communications Manager サーバ上で動作し、Cisco IP 電話 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 電話では TVS を信頼するだけで済みます。
- 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 電話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

初期信頼リスト（ITL）ファイルは、エンドポイントが Unified Communications Manager を信頼できるよう、最初のセキュリティに使用されます。ITL は明示的に有効にするセキュリティ機能を必要としません。ITL ファイルは、TFTP サービスがアクティブになり、クラスタがインストールされると自動的に作成されます。Unified Communications Manager の TFTP サーバの秘密キーは、ITL ファイルの署名に使用されます。

Unified Communications Manager クラスタまたはサーバが非セキュアモードの場合、ITL ファイルはサポートされている Cisco Unified IP 電話 ごとにダウンロードされます。CLI コマンド **admin:show itl** を使用して、ITL ファイルの内容を表示できます。

Cisco Unified IP 電話 は、次のタスクを実行するために ITL ファイルが必要です。

- CAPF とセキュアに通信する。設定ファイル暗号化をサポートするための前提条件です。
- 設定ファイルの署名を認証する。
- TVS を使用する EM サービス、ディレクトリ、MIDlet などのアプリケーション サーバを認証します。

Cisco IP 電話 に CTL ファイルがまだ存在していない場合、最初の ITL ファイルが自動的に信頼されます。テレビは、署名者に対応する証明書を返すことができる必要があります。

Cisco IP 電話 に既存の CTL ファイルがある場合、ITL ファイルの署名の認証にその CTL ファイルが使用されます。

（注） SHA-1 または MD5 アルゴリズム値は、初期信頼リスト（ITL）ファイルの値に変更があった場合にのみ変更されます。ITL ファイルのチェックサム値を使用すると、Cisco IP 電話 と Unified Communications Manager クラスタの間にある ITL ファイルの差異を特定できます。ITL ファイルのチェックサム値は、ITL ファイルを変更した場合にのみ変更されます。

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、これはより小さく、スリムのバージョンです。

ITL ファイルには次の属性が適用されます。

- TFTP サービスがアクティブ化され、クラスタをインストールすると、システムによって ITL ファイルが自動的に作成されます。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。
- リセット中、再起動中、または CTL ファイルのダウンロード後に、Cisco Unified IP 電話 は ITL ファイルをダウンロードします。

ITL ファイルには次の証明書が含まれています。

- ITLRecovery 証明書：この証明書は ITL ファイルに署名します。
- TFTP サーバの CallManager 証明書：この証明書を使用すると、ITL ファイル署名と電話機設定ファイル署名を認証できます。
- クラスタ上で使用可能なすべての TVS 証明書：これらの証明書を使用すると、電話機は TVS と安全に通信し、証明書認証を要求できます。
- CAPF 証明書: これらの証明書は、コンフィギュレーションファイルの暗号化をサポートします。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 電話 によるルックアップ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。

初期信頼リストファイル

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、これはより小さく、スリムのバージョンです。

ITL ファイルには次の属性が適用されます。

- システムは、クラスタのインストール時に自動的に ITL ファイルを作成します。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。

- リセット中、再起動中、または CTL ファイルのダウンロード後に、Cisco Unified IP 電話 は 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：この証明書を使用すると、ITL ファイル署名と電話機設定ファイル署名を認証できます。
- クラスタ上で使用可能なすべての TVS 証明書：これらの証明書を使用すると、電話機は TVS と安全に通信し、証明書認証を要求できます。
- CAPF 証明書: これらの証明書は、コンフィギュレーションファイルの暗号化をサポートします。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 電話 によるルックアップ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 と CTL ファイルの相互作用

Cisco IP 電話 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 ファイルには、クラスタセキュリティモードの指示も含まれています。

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、CLI と GUI の両方に警告メッセージが表示されます。この警告メッセージは、トークンレス CTL を使用しており、CallManager 証明書を再生成する場合に、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更新されていることを確認するために表示されます。

ITLRecovery 証明書

ITLRecovery Certificate 機能では、新しい **ITL ファイルステータス**ドロップダウンリストが導入され、管理者は古い ITL を持つ電話機を識別して、それらの電話機に必要なアクションを実行できるようになりました。

一部の電話機は、ITL ファイルが更新されたときに最新の ITL ファイルを取得せず、古いものを保持します（CM 証明書の更新など）。システムは、不一致の ITL ファイルがある電話機の集中型レポートをユーザインターフェイスに表示します。

次に、さまざまな ITLRecovery シナリオを示します。

TFTP Service Activaton:

- TFTP サービスがアクティブになると、生成された ITL ファイルのハッシュがサーバのホスト名とともに DB に保存されます。ITL が TFTP コードで更新されるたびに更新されます。
- TFTP ホスト名がすでにテーブルに存在する場合は、生成された ITL ハッシュが保存されている値と比較されます。
  - ITL ハッシュが同じでない場合、新しい ITL ハッシュが DB で更新されます。
  - ITL ハッシュが同じ場合、TFTP ログに「Tftp Itl hash not changed」と表示されます。

デバイス登録と ITLFile のダウンロード

- 電話機がUnified Communications Managerに登録されると、サーバに存在する ITLFile の詳細（サーバのホスト名、ハッシュ、タイムスタンプ）が DB に存在しません。
- 電話機がUnified Communications Managerに登録されると、電話機に適用された ITL ファイルの詳細を含む SIP アラームが送信されます。これは、DB に保存されている ITL ファイルのハッシュと比較されます。
  - ITL ハッシュが同じ場合、デバイスハッシュ情報は新しいタイムスタンプで更新されます。

- ITL ハッシュが同じでない場合、報告された ITL ハッシュとタイムスタンプがデバイスに対して更新されます。

- 電話機の登録が解除されると、そのデバイスの信頼ハッシュ情報が削除されます。

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 電話 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 電話 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を使用している Unified Communication Manager との集中型 TFTP では、TFTP 設定ファイルは検証されません。

リモートクラスタからの電話機が集中型 TFTP 展開に追加される前に、次の手順を実行します。

手順

Step 1 中央 TFTP サーバで、Enterprise パラメータ **Prepare cluster for PRE CM-8.0 rollback** を有効にします。

Step 2 TVS および TFTP を再起動します。

Step 3 すべての電話機をリセットして、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ていることを確認します。

Step 4 HTTPS ではなく HTTP を使用するように、エンタープライズパラメータセキュア https Url を設定します。

（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 バージョンと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 より前のリリースへのクラスタのロールバック」セクションを参照してください。

自動登録

システムは混合モードと非セキュアモードの両方で自動登録をサポートします。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 電話 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。

ITL ファイルステータスの取得

電話機の ITL ファイルステータスを取得するには、次の手順を使用します。

Procedure

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

Step 2 **[電話機を探す（Find Phone where）]** ドロップダウンリストで **[ITL ファイルステータス（ITL File Status）]** を選択し、条件を選択します。

フィールド	説明
一致	サーバと電話機の ITL ハッシュが同じ
MisMatch	サーバの ITL ハッシュが電話機の ITL ハッシュと異なる
未インストール	電話機が新しい CUCM サーバへの登録に失敗し、以前のサーバにバウンスする
不明	電話機またはサーバの ITL ハッシュが不明

Step 3 [検索（Find）] をクリックします。

Cisco Unified IP 電話 サポートリストの取得

Cisco Unified Reporting ツールを使用して、デフォルトでセキュリティをサポートするシスコエンドポイントのリストを生成します。

手順

Step 1 [Cisco Unified Reporting] から [システムレポート（System Reports）] をクリックします。

Step 2 [システムレポート（System Reports）] リストで、[Unified CM 電話機能一覧（Unified CM Phone Feature List）] をクリックします。

Step 3 **[製品（Product）]** ドロップダウンリストから、**[デフォルトのセキュリティ（Security By Default）]** を選択します。

Step 4 [送信（Submit）] をクリックします。
特定の電話でサポートされている機能のリストを含むレポートが生成されます。

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。Secure Computer Telephony Integration (CTI) Manager インターフェイスは、ECDSA 証明書もサポートしています。CTI Manager と SIP サーバの両方が同じサーバ証明書を使用しているため、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 接続は、ECDSA 暗号方式をサポートし、ECDSA 証明書を使用します。

SIP が (Transport Layer Security) TLS 接続を行うシナリオを次に示します。

- 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存在する場合、選択した暗号スイートが**TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**または**TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**場合、SIP トランクインターフェイスは CallManager ECDSA 証明書を使用します。SIP トランクインターフェイスは、ECDSA 暗号スイートをサポートしていないクライアントからの接続に対して 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 [**エンタープライズパラメータ (Enterprise Parameters)**] ウィンドウの [**Tls 暗号 (tls cipher)**] フィールド (**ECDSA 暗号**オプションも含む) に基づいて、要求された暗号スイートのリストをサーバに送信します。[TLS Ciphers]。この設定により、TLS クライアント暗号スイートリストおよびサポートされている暗号スイートが優先順に決定されます。

（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、CallManager ECDSA 証明書によって保護されている接続を信頼するために、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む必要があります。

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。Cisco エンドポイントのみが CAPF を使用します。一般的な基準要件を達成するために、CAPF は CAPF バージョン3に更新されます。これにより、クライアントは ECDSA ローカルで有効な証明書 (LSC) で提供されるようになります。カスタマーがローカルで LSC を作成します。LSC は製造元が作成した製造元でインストールされた証明書 (MIC) に代わるものです。

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。

エンドポイントに CAPF バージョン3のサポートがない場合は、必要な EC キーサイズと RSA キーサイズを設定し、Cisco ユニファイド CM Administration からバックアップとして [**電話の設定 (Phone Configuration)**] ウィンドウで [**ec キー優先 (rsa Backup)**] オプションを選択できます。このバックアップオプションは、CAPF サーバが ec キーペアに要求を送信しようとし、電話機が EC キーをサポートしていないサーバと通信する場合に便利です。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をサポートしていて、**エンドポイントの Advanced Encryption Algorithm Support**パラメータを有効にせずに、**電話の設定**で**EC 優先、rsa バックアップ**オプションを選択した場合、ECDSA または RSA ベースの lscs 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、**エンドポイントの Advanced Encryption Algorithm support**パラメータを有効または無効にすると、RSA ベースの lscs 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

強力な暗号化を行うには、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尺度であり、一般的な基準要件の最小しきい値を決定するのに役に立ちます。暗号化や暗号化などのデータ変換技術は、その有効性を高めるためにエントロピーの適切なソースに依存しています。ECDSA などの強力な暗号化アルゴリズムでエントロピーの弱いソースが使用されている場合は、暗号化が簡単に切断される可能性があります。

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を制御するには、次の CLI コマンドを使用します。

CLI コマンド	説明
ユーティリティサービス開始エントロピーモニタリングデーモン	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。
ユーティリティサービス停止エントロピーモニタリングデーモン	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。
ユーティリティサービスアクティブエントロピーモニタリングデーモン	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。
ユーティリティサービス deactive エントロピーモニタリングデーモン	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。必要に応じて、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 lscs および暗号化された TFTP 設定を使用して登録されたクライアントは、lscs を提示する必要があります。

HTTPS インターフェイスは、CallManager と CallManager ECDSA 証明書の両方をサーバ証明書として使用します。

（注） CallManager、CallManager ECDSA、または tomcat 証明書を更新する場合は、TFTP サービスを非アクティブ化してから再アクティブ化する必要があります。ポート6971は CallManager および CallManager ECDSA 証明書の認証に使用されますが、ポート6972は tomcat 証明書の認証に使用されます。

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) インターフェイスは、4つの新しい暗号方式をサポートするように強化されています。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、電話機が自動的に再起動して ITL ファイルを更新することがあります。これは、[証明書の更新時の電話の連携（Phone Interaction on Certificate Update）] パラメータが自動的にリセットされる場合に適用されます。

手順

Step 1 CAPF 証明書を再生成します。

Step 2 CTL ファイルがある場合は、CTL ファイルを更新する必要があります。

詳細については、『Cisco Unified Communications Manager Security Guide』の「証明書の再生成」セクションを参照してください。

Step 3 CAPF 証明書が再生成されると、CAPF サービスが自動的に再起動されます。

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

（注） TV と TFTP の両方の証明書を再生成する場合は、TV 証明書を再生成し、可能な電話機の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。これは、[証明書の更新時の電話の連携（Phone Interaction on Certificate Update）] パラメータが自動的にリセットされる場合に適用されます。

手順

Step 1 TVS 証明書の再生成

Step 2 CTL ファイルがある場合は、CTL ファイルを更新する必要があります。

詳細については、『Cisco Unified Communications Manager Security Guide』 の「証明書の再生成」セクションを参照してください。

Step 3 TVS 証明書が再生成されると、TVS サービスが自動的に再起動されます。

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予定の場合は、最後にTFTP証明書を再生成する必要があります。TFTP証明書を再生成する前に、可能な電話機の再起動が完了するまで待ちます。この手順に従わないと、すべての Cisco IP 電話 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。これは、[証明書の更新時の電話の連携（Phone Interaction on Certificate Update）] パラメータが自動的にリセットされる場合に適用されます。

手順

Step 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。

Step 2 TFTPサービスが有効化されている場合は、すべての電話機が自動的に再起動するまで待ちます。

Step 3 クラスタが混合モードの場合は、CTL ファイルを更新します。

Step 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 この証明書の有効期限が電話機で長いため、ITLRecovery 証明書は頻繁に再生成しないでください。また、この証明書には CallManager 証明書も含まれています。

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、および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かどうかを確認します。
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、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。

      [証明書リスト（Certificate List）] ウィンドウが表示されます。
   3. 表示された証明書のリストから、ITLRecovery pem 証明書のリンクをクリックします。
   4. ITLRecovery 証明書を再生成するには、**[再生成 (再生成)]** をクリックします。
   5. 確認メッセージポップアップで、**[OK]**をクリックします。
3. CallManager 証明書のユーティリティ `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してリセットします。

（注） クラスタ内のすべての電話機が登録されていることを確認してください。

5. TFTP サービスを再起動して、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. クラスタ内のすべての電話機を一括してリセットし、新しい ITL ファイルを取得します。
7. リセット後に、新しい ITLRecovery 証明書を使用して電話機が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 ITL ファイルに移行する場合は、『security guide』の「migration」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、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。

      [証明書リスト（Certificate List）] ウィンドウが表示されます。
   3. 表示された証明書のリストから、ITLRecovery pem 証明書のリンクをクリックします。
   4. ITLRecovery 証明書を再生成するには、[**再生成 (再生成)**] をクリックします。
   5. 確認メッセージポップアップで、[**OK]**をクリックします。
4. CallManager 証明書で、CTLFile にユーティリティ `ctl reset localkey\`を使用して署名します。これにより、新しい ITLRecovery 証明書を使用して CTLFile も更新されます。
5. クラスタ内のすべての電話機を一括してリセットし、新しいITLRecovery証明書を使用して新しい CTLFile をピックアップします。

（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。
- ITLRecoveryを再生成すると、システム全体の証明書が有効化に使用される場合、クラスタの SAML SSO ログインに影響します。

6. 新しい ITLRecovery Certificate CTLFile `ctl Update CTLFile`によって再署名されるように、を更新します。
7. クラスタ内のすべての電話機を一括してリセットし、新しいITLRecovery証明書によって署名された新しい CTLFile をピックアップします。
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

Tomcat 証明書を再生成するには、次の手順を実行します。

手順

Step 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。

Step 2 Tomcat サービスの再起動

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

Step 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である TFTP 秘密キーです。サーバがクラッシュすると、キーが失われ、電話機は新しい 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、秘密キーの秘密を保持するためにバックアップパッケージを暗号化します。サーバがクラッシュすると、以前の証明書と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 以降へのアップグレードの更新

クラスタをリリース7.xからリリース8.6以降にアップグレードするには、次の手順を実行します。

手順

Step 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 電話 をシステムに登録する必要があります。

Step 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) のすべての通常リリース
  - 007.001 (002.32016.001) より前の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) より前の713のすべての通常リリース = 7.1 (3a) su1a
  - 007.001 (003.21005.001) より前の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。

Step 3　Cisco IP 電話 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　クラスタを回復できるようにするには、ディザスタリカバリシステム(DRS) を使用してクラスタをバックアップする必要があります。

Step 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したりすることはできません。CAR 移行ステータスをモニタするには、**Cisco ユニファイドサービスの** > > **CDR Analysis and Reporting**に移動します。

8.0 より前のリリースへのクラスタのロールバック

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

Step 1 Unified Communications Manager で、**[システム（System）] > [エンタープライズパラメータ設定（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。

Step 2 Cisco IP 電話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。

Step 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。

Step 4 クラスタが以前のバージョンへの切り替えを完了するまで待ちます。

Step 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) のすべての通常リリース
  - 007.001 (002.32016.001) より前の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) より前の713のすべての通常リリース = 7.1 (3a) su1a
  - 007.001 (003.21005.001) より前の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。

Step 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。

Step 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。

復帰後のリリース8.6 以降へのスイッチバック

クラスタをリリース7.x に戻した後にリリース8.6 またはそれ以降のパーティションに切り替える場合は、次の手順に従います。

手順

Step 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。

Step 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) のすべての通常リリース
- 007.001 (002.32016.001) より前の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) より前の713のすべての通常リリース = 7.1 (3a) su1a
  - 007.001 (003.21005.001) より前の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。

Step 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。

Step 4 Cisco Unified IP 電話 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 と ITL ファイルを使用したクラスタ間での IP フォンの移行

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。この新機能を使用する場合は、異なるユニファイドCMクラスタ間で電話を移動する際には注意が必要です。また、移行のための適切な手順に従っていることを確認してください。

⚠

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 電話 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。

- 電話機に現在インストールされている TFTP サーバ証明書
- クラスタのいずれかで TV サービスを検証できる TFTP 証明書。ITL ファイルにリストされているクラスタ内の TV サービスの証明書を確認できます。

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のままにする予定の場合は、[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て、デフォルトでセキュリティを復元します。

関連トピック

8.0 より前のリリースへのクラスタのロールバック, on page 96

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 電話 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

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

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

Step 3 証明書の一括処理用のインターフェイスを使用して SFTP サーバで証明書（TFTP のみ）を統合します。

Step 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。

Step 5 DHCPオプション150、またはその他の方法を使用して、電話機に新しい宛先クラスタを指定します。

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。電話機はTCPポート2445の古いクラスタにTVSクエリを送信してこの要求を行います。

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。

これで電話機は新しいクラスタから署名付きのコンフィギュレーション ファイルをダウンロードし、検証できるようになります。

自己署名証明書の生成

手順

Step 1 [Cisco Unified OS Administration] から **[Security]** > **[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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 6 [生成（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, on page 102

自己署名証明書のフィールド

表 *15 :* 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、[**Key Type**] フィールドは自動的に**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、[**Key Type**] フィールドは自動的に**EC** (楕円曲線) に設定されます。 • tomcat-ECDSA • CallManager-ECDSA
ディストリビューション	ドロップダウンリストから Unified Communications Manager サーバを選択します。
[Auto-populated Domains]	[証明書の目的 (**Certificate** by)] ドロップダウンリストを使用して、次のいずれかのオプション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ているホスト名が一覧表示されます。証明書の共通名は、ホスト名と同じです。両方、**CALLMANAGER ecdsa**と**tomcat の**両方の証明書には、ホスト名とは異なる共通の名前があります。 このフィールドには、**CALLMANAGER ECDSA**証明書の完全修飾ドメイン名が表示されます。

フィールド	説明
キー タイプ	このフィールドには、公開キーと秘密キーのペアの暗号化および復号化に使用されるキーのタイプがリストされます。 Unified Communications Manager は **EC** および **RSA** キー タイプをサポートしています。
キーの長さ（Key Length）	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。 • 1024 • 2048 • 3072 • 4096 キーの長さによっては、自己署名証明書要求によってハッシュアルゴリズムの選択肢が制限されます。ハッシュアルゴリズムを限定して選択した場合は、キー長の強度以上のハッシュアルゴリズム強度を使用できます。 • キー長の値が256の場合、サポートされてい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、サポートされてい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の証明書は、RSA 証明書に対してのみ選択されます。これらのオプションは、ECDSA 証明書では使用できません。 （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。

フィールド	説明
Hash Algorithm	ドロップダウンリストからキーの長さ以上の値を選択します。 （注） • [**ハッシュアルゴリズム (Hash Algorithm)**] ドロップダウンリストの値は、[**キー長 (Key Length)**] フィールドで選択した値に基づいて変わります。 • 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して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。

CA 署名付き証明書をアップロードするには、Cisco ユニファイドオペレーティングシステムの管理から CSR を生成し、CA に提示します。CSR を生成するたびに、CSR とともに新しい秘密キーが生成されます。

秘密キーは、CSR の生成時に選択したサーバとサービスに固有のファイルです。セキュリティコンプライアンスのために、この秘密キーを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

Step 1 [Cisco Unified OS Administration] から **[Security]** > **[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。

Step 2 [CSR の作成（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。

Step 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。

Step 4 [証明書の目的 (**Certificate** by)] 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。

Step 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。

Step 6 [生成（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, on page 105

証明書署名要求のフィールド

表 *16 :* 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**

ディストリビューション	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>`

	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、サブジェクト代替名 (SANs) セクションに表示されます。単一の証明書によって保護されるホスト名が一覧表示されます。
[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。
キー タイプ	このフィールドは、公開キーと秘密キーのペアの暗号化と復号化に使用されるキーのタイプを示します。 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
キーの長さ（Key Length）	[**Key Length**] ドロップダウンボックスから、値の1つを選択します。 キーの長さによっては、CSR要求によってハッシュアルゴリズムの選択肢が制限されます。ハッシュアルゴリズムを限定して選択することで、キー長の強度以上のハッシュアルゴリズム強度を使用できます。たとえば、キーの長さが256の場合、サポートされているハッシュアルゴリズムはSHA256、SHA384、またはSHA512です。同様に、384のキー長の場合、サポートされてい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の証明書は、RSA証明書に対してのみ選択できます。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） 一部の電話機モデルでは、CallManagerの[証明書の目的（Certificate Purpose）]に対して選択されたRSAの[キーの長さ（key length）]が2048を超える場合、登録に失敗します。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	[**ハッシュアルゴリズム (Hash algorithm)**] ドロップダウンボックスから値を選択して、楕円曲線のキー長としてより強力なハッシュアルゴリズムを設定します。[**ハッシュアルゴリズム (Hash Algorithm)**] ドロップダウンボックスから、値の1つを選択します。 （注） • [**ハッシュアルゴリズム (Hash Algorithm)**] フィールドの値は、[**キー長 (Key Length)**] フィールドで選択した値に基づいて変わります。 • 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**] オプションを選択した場合、ecdsa 暗号をサポートしていないデバイスは、SIP インターフェイスへの TLS 接続を確立できません。[**ECDSA only**] オプションを選択した場合、このパラメータの値は **TLS_ECDHE_ECDSA_WITH_AES128_SHA256** と **TLS_ECDHE_ECDSA_WITH_AES256_SHA384** になります。

- CTI Manager 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

この手順を実行できるのは、Unified Communications Manager パブリッシャのみからであることを確認してください。

電話機が ITL ファイル 署名者を信頼できなくなり、かつ TFTP サービスによってローカルに提供された ITL ファイルを認証できないか、TVS を使用して認証できない場合は、ITL ファイルの一括リセットが実行されます。

一括リセットを実行するには、CLI コマンド **utils itl reset** を使用します。このコマンドは新しい ITL リカバリファイルを生成し、電話機と CUCM の TFTP サービス間の信頼を再確立します。

ヒント Unified Communications Manager をインストールする場合は、CLI コマンド **file get tftp** *ITLRecovery.p12* を使用して ITL リカバリペアをエクスポートしてから、DR を介してバックアップを実行します。（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も表示されます。

手順

Step 1 次のいずれかの手順を実行します。

- **utils itl reset localkey** を実行します。
- **utils itl reset remotekey** を実行します。

（注） **utils itl reset localkey** の場合、ローカルキーはパブリッシャにあります。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。

Step 2 **show itl** を実行してリセットが正常に行われたことを確認します。

Step 3 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

Step 4 [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。

Step 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 キーで署名された 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。

CTL ローカルキーのリセット

Unified Communications Manager クラスタ上のデバイスがロックされ、信頼されたステータスが失われる場合は、CLI コマンド **ctl reset localkey** を使用して Cisco Trust List（CTL）ファイルのリセットを実行します。このコマンドにより、新しい CTL ファイルが生成されます。

手順

Step 1 **utils ctl reset localkey** の実行

（注） **utils ctl 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すると、CTL ファイルは ITLRecovery キーによって一時的に署名されます。

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

Step 3 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。
[エンタープライズパラメータの設定（Enterprise Parameters Configuration）] ページが表示されます。

Step 4 [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 CTL 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。

Step 5 **utils ctl update CTLFile** を実行して、ステップ 1 の変更をロールバックする必要なサービスを再起動します。

デバイスが再起動されます。これで、ITLRecovery キーで署名された CTL 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。

デバイスは、必要なキーを使用して署名された CTL ファイルをダウンロードし、Unified Communications Manager に再度正しく登録します。

ITLRecovery 証明書の有効期間の表示

ITLRecovery 証明書は電話機での有効期間が長いです。[証明書ファイルデータ（Certificate File Data）] ペインに移動し、有効期間または他の ITLRecovery 証明書の詳細を表示できます。

手順

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

Step 2 証明書を検索し、設定の詳細を表示するには、必要な検索パラメータを入力します。
条件に一致する証明書のリストが [証明書リスト（Certificate List）] ページに表示されます。

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

ITLRecovery 証明書の詳細が [証明書ファイルデータ（Certificate File Data）] ペインに表示 されます。

有効期間は現在の年から 20 年です。

連絡先検索認証タスクフロー

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
Step 1	連絡先検索の認証の電話サポートの確認（110 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 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。
Step 2	連絡先検索の認証の有効化（110 ページ）	Unified Communications Manager で連絡先検索の認証を設定します。

	コマンドまたはアクション	目的
Step 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（111 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

Step 1 Cisco Unified Reporting から [システム レポート(System Reports)] をクリックします。

Step 2 **[ユニファイド CM 電話機能 (Unified CM Phone Feature)]** を選択します。

Step 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。

Step 4 [製品 (Product)] フィールドはデフォルト値のままにします。

Step 5 **[機能 (Feature)]** ドロップダウンから **[Authenticated Contact Search]** を選択します。

Step 6 [送信（Submit）] をクリックします。

連絡先検索の認証の有効化

電話ユーザの連絡先検索認証を設定するには、Unified Communications Manager で次の手順を使用します。

手順

Step 1 コマンドライン インターフェイスにログインします。

Step 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。

Step 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。

Step 4 すべての Unified Communications Manager のクラスタノードに対して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。

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。

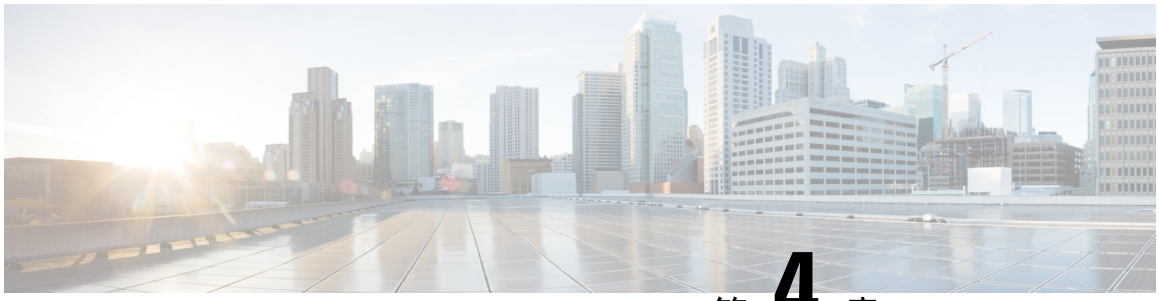
手順

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

Step 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。

Step 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）
- 同じサーバで実行されている CiscoCallManager および CiscoTFTP 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。

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。
- ITLRecovery 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。

リカバリのための CTL ファイルへの2番目の SAST ロールの追加

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 ファイルに署名するために使用された1つの SAST レコードだけが含まれていました。1つの SAST のみが使用されているため、SAST 署名者の更新によってエンドポイントのロックアウトが発生しました。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。

- エンドポイントは、登録時に CallManager 証明書を使用して署名された CTL ファイルを受け入れました。
- 管理者が CallManager 証明書を再生成し、CTL ファイルを更新しました。これは、更新された CTL ファイルが既存の CallManager 証明書ではなく、更新された CallManager 証明書によって署名されたことを暗示しています。
- 更新された証明書がエンドポイントの信頼リストで使用できなかったため、エンドポイントは更新された CallManager 証明書を信頼しませんでした。そのため、エンドポイントは、CTL ファイルをダウンロードする代わりに拒否しました。
- エンドポイントは、Transport Layer Security (TLS) を介して ccm サービスに安全に接続しようとしました。 ccmservice は更新された CallManager 証明書を TLS 交換の一部としてエンドポイントに提供しました。更新された証明書は、エンドポイントの信頼リストでは使用できなかったため、エンドポイントはその 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2つの SAST トークン (CallManager レコードと ITLRecovery レコード) が含まれています。

ITLRecovery 証明書は、次の理由により他の証明書よりも選択されます。

- ホスト名の変更などの二次的な理由によって変更されることはありません。
- すでに ITL ファイルで使用されています。

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 *14*』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 Unified Communications Manager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 クライアントを設定すると、Cisco CTL Provider サービスによってセキュリティモードが非セキュアモードから混合モードに変更され、サーバ証明書が CTL ファイルに転送されます。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 CiscoCTL 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

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

Step 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。

Step 3　**CiscoCTL Provider** サービスのオプションボタンをクリックします。

Step 4　[保存（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）　CiscoCTL Provider サービスをアクティブにする前に、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場合は、TLS 接続用のポートの設定に関連するトピックを参照してください。

Step 5　サービスがサーバ上で実行されていることを確認します。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。

関連トピック

セキュア ポートの設定, on page 118
CTL クライアントの設定に関する詳細情報の入手先

Cisco CAPF サービスのアクティベーション

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 サービスをアクティブにすると、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。

関連トピック

Certificate Authority Proxy Function サービスの有効化

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。

- TLS 接続の Cisco CTL プロバイダーのデフォルトポートは2444に相当します。Cisco CTL プロバイダーポートは、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、Cisco CTL クライアント要求を処理します。

（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は、SCCP を実行している電話機からの登録要求をモニタします。非セキュアモードでは、電話機はポート2000を介して接続します。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。このポートを変更する場合は、 Cisco Unified Serviceability の CiscoCallManager サービスを再起動し、SIP を実行している電話機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 クライアントが実行されているデータ VLAN に対して CTL ポートを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

Step 1　変更するポートに応じて、次のタスクを実行します。

a) Cisco CTL Provider サービスのポート番号パラメータを変更するには、Step 2 （119 ページ）～ Step 6 （119 ページ）を実行します。

b) イーサネット電話ポートまたは SIP 電話のセキュアポートの設定をStep 7 （119 ページ）変更 Step 11 （119 ページ）するには、~ を実行します。

Step 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。

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

Step 4　[サービス (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。

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

（注）　12.X 以降では、[パラメータ値（Parameter Value）] フィールドの [ポート番号（Port Number）] パラメータの値を変更できません。

Step 6　**[保存（Save）]** をクリックします。

Step 7　[イーサネット電話ポート（Ethernet Phone Port）] または [SIP 電話セキュアポート（SIP Phone Secure Port）] の設定を変更するには、[Unified Communications Manager Administration] で **[システム（System）] > [CiscoUnifiedCM]** を選択します。

Step 8　『*Administration Guide for Cisco Unified Communications Manager*』の説明に従い、CiscoCallManager 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 **[名前（Name）]** リンクをクリックします。

Step 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。

Step 10　電話機をリセットし、Cisco Unified Serviceability の CiscoCallManager サービスを再起動します。

Step 11　[保存（Save）] をクリックします。

関連トピック

CTL クライアントの設定に関する詳細情報の入手先

Cisco CTL クライアントのセットアップ

重要 < x xid = "i 7000.1.1" id = "x253"/> **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） また、Cisco CTL クライアントは、最大16の呼処理サーバ、1台のパブリッシャ、2つの TFTP サーバ、最大9個のメディアリソースサーバをサポートします。

  ヒント TFTP サービスを再起動し、クラスタ内でこれらの
  いるすべてのサーバで CallManager する必要がある
  されたメンテナンス期間中に CTL ファイルを更新

  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。
  - 設定されているすべての TFTP サーバにファイルを書き込みます。
  - 設定されているすべての ASA ファイアウォールにファイルを書き込みます。
  - Ctl ファイルを作成したときに、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。

関連トピック

Cisco CTL ファイルの詳細, on page 126
デバイス、サーバ、クラスタ、およびサービスのリセット, on page 17
Cisco CTL クライアントのアップグレードと Cisco CTL ファイルの移行
詳細情報の入手先, on page 61

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 *17 : 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 Unified Communications Manager 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	ITLRecovery（署名者） CallManager
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

Step 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。

Step 2 [検索（Find）] をクリックします。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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**ユーティリティ ctl**を使用してクラスタセキュリティを管理する場合、この手順は必要ありません。

次のシナリオが発生した場合は、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
- 設定されている任意の TFTP サーバの IP アドレスまたはホスト名を変更する場合
- 設定されている 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場合
- シスコユニファイドサービスで Cisco Certificate Authority Function サービスを有効にした場合
- 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場合
- TFTP サーバを追加または削除する必要がある場合
- 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
- 10.5 より前のユニファイドコミュニケーションマネージャバージョンからバージョン10.5 以降に更新する場合は、「ハードウェア eTokens からトークンレスソリューションへの移行」の項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 シスコでは、最小限のコール処理の中断が発生した場合に、ファイルを更新することを強く推奨しています。

注意 ユニファイドコミュニケーションマネージャが、セキュアな SIP または SCCP を使用して Unity Connection 10.5 以降と統合されている場合、セキュアコールは Unity Connection での動作を停止する可能性があります。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 インターフェイスを使用してポートグループをリセットするには、[Telephony] [統合 > **ポートグループ**] に移動し、リセットするポートグループを選択して、[**ポートグループの基本**] ページで [**リセット**] をクリックします。

関連トピック

CTL ファイル エントリの削除
Cisco CTL クライアントの設定, on page 113
詳細情報の入手先, on page 61

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

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

Step 1 CLI コマンドの`monitorctl set クラスタ混合モード`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。

Step 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。

関連トピック

CTL ファイルの更新, on page 124

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。混合モードのみが、認証、暗号化されたシグナリング、および暗号化されたメディアをサポートしています。

（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 *18 : CTL* の構成時の設定

設定	説明
Unified Communications Managerサーバ	
セキュリティ モード（**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 電話 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 エントリ	
置換可能なトークン	サーバまたはワークステーションに最初に挿入したトークンを削除していない場合は、削除します。アプリケーションからプロンプトが表示されたら、次のトークンを挿入し、[**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、これらのタスクを繰り返します。
[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、代替 TFTP サーバのタブ設定を表示した後に [**ヘルプ (Help)**] ボタンをクリックしてください。設定を入力したら、[**次へ (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。

関連トピック

Cisco CTL クライアントの設定のヒント
詳細情報の入手先, on page 61

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

Step 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。

Step 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。この値は、Cisco CTL クライアントを設定した後に表示されます。

関連トピック

CTL クライアントの設定に関する詳細情報の入手先

開始または自動のスマートカードサービスのセットアップ

Cisco CTL クライアントのインストールでスマートカードサービスが無効になっていることが検出された場合は、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スマートカードサービスを自動に設定し、起動する必要があります。

ヒント　サービスが [開始 (on)] および [自動 (automatic)] に設定されていない場合、CTL ファイルにセキュリティトークンを追加することはできません。

ヒント　オペレーティングシステムをアップグレードし、サービスリリースを適用し、 Cisco Unified Communications Managerをアップグレードした後、スマートカードサービスが開始され、自動であることを確認します。

サービスを開始および自動に設定するには、次の手順を実行します。

手順

Step 1　Cisco CTL クライアントをインストールしたサーバまたはワークステーションで、[スタート] [プログラム] [＞ ＞ **管理ツール** ＞] [サービス]、または [**スタート** ＞ **] [コントロールパネル]** ＞ **[管理ツール]** ＞ **[サービス]** を選択します。

Step 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。

Step 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。

Step 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。

Step 5　**[適用（Apply）]** をクリックします。

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

Step 7　[OK] をクリックします。

Step 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。

関連トピック

CTL クライアントの設定に関する詳細情報の入手先

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 ファイルは削除されません。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。これを選択した場合は、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には、次の手順を実行します。

手順

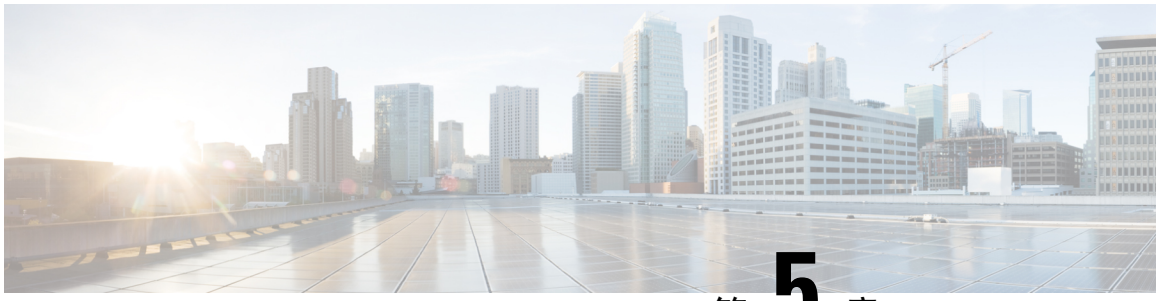
Step 1 **[Start]** > **[Control Panel]** > **[Add or Remove Programs]** の順に選択します。

Step 2 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には、 **CISCO CTL クライアント**を見つけます。

Step 3 クライアントをアンインストールするには、[**Remove**] をクリックします。

関連トピック

CTL クライアントの設定に関する詳細情報の入手先



第 5 章

TLS セットアップ

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
Step 1	最小 TLS バージョンの設定（133 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。
Step 2	（任意） TLS 暗号化の設定 （134 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。
Step 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 （134 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。
Step 4	SIP トランクへのセキュア プロファイルの追加 （135 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

	コマンドまたはアクション	目的
		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。
Step 5	電話セキュリティ プロファイルでの TLS の設定 （135 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。
Step 6	電話へのセキュア電話プロファイルの追加（136 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。
Step 7	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 （137 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。

設定対象の TLS バージョンが、ネットワーク内のデバイスとアプリケーションでサポートされていることを確認します。詳細については、「TLS の前提条件 （131 ページ）」を参照してください。

手順

Step 1 コマンド ライン インターフェイスにログインします。

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

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

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

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

TLS 暗号化の設定

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

手順

Step 1 Cisco Unified CM 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。

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

Step 3 [保存（Save）] をクリックします。

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

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

手順

Step 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。

Step 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。

Step 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。

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

Step 5 **[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。

Step 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。

Step 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。

Step 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。

Step 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」セクションを参照してください。

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

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [セキュリティ（Security）] > [電話セキュリティプロファイル（Phone Security Profile）]** の順に選択します。

Step 2 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。

Step 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。

Step 4 プロファイル名を入力します

Step 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。

Step 6 （SIP 電話のみ）転送タイプには、**TLS** を選択します。

Step 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。

Step 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

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

Step 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。

Step 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。

Step 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。

Step 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）

Step 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。

Step 7 [保存（Save）] をクリックします。

ユニバーサル デバイス テンプレート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

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[ユーザ管理（User Management）] > [ユーザ/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）]**

Step 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。

Step 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。

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

Step 5 **[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 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。

Step 6 **[SIP プロファイル（SIP Profile）]** を選択します。

Step 7 **[電話ボタン テンプレート（Phone Button Template）]** を選択します。

Step 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。

Step 9 [保存（Save）] をクリックします。

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

TLS の連携動作と制約事項

この章では、TLS のインタラクションと制限事項について説明します。

TLS の相互作用

表 *19 : TLS* の相互作用

機能	連携動作
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 *20 : 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。
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.** すべての Unified Communications Manager クラスタで混合モードをオンにします。 **3.** すべての Unified Communications Manager クラスタに同じ USB eToken を使用します。
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。

機能	制限事項
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）。
サポートされていないバージョンの Cisco Unified Communications Manager への接続	より高い TLS バージョンをサポートしていない Unified Communications Manager の古いバージョンへの TLS 1.2 接続は動作しません。たとえば、Unified Communications Manager リリース 9.x への TLS 1.2 SIP トランク接続は動作しません。このリリースでは TLS 1.2 がサポートされていないためです。 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

機能	制限事項
Address Book Synchronizer	回避策はありません。

Cisco Unified Communications ManagerIM 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

次の表に、TLS バージョン 1.2 の影響を受ける Unified Communications Manager ポートを示します。

表 *21 : Cisco Unified Communications Manager* 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

アプリケーション	プロトコル	宛先/リスナー	通常モードで動作する Cisco Unified Communications Manager			コモン クライテリア モードで動作する Cisco Unified Communications Manager		
			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

アプリケーション	プロトコル	宛先/リスナー	通常モードで動作する Cisco Unified Communications Manager			コモン クライテリア モードで動作する Cisco Unified Communications Manager		
			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
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）[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
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

アプリケーション	プロトコル	宛先/リスナー	通常モードで動作する Cisco Unified Communications Manager			コモン クライテリア モードで動作する Cisco Unified Communications Manager		
			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
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

次の表は、Transport Layer Security バージョン 1.2 の影響を受ける IM and Presence Service ポートを示します。

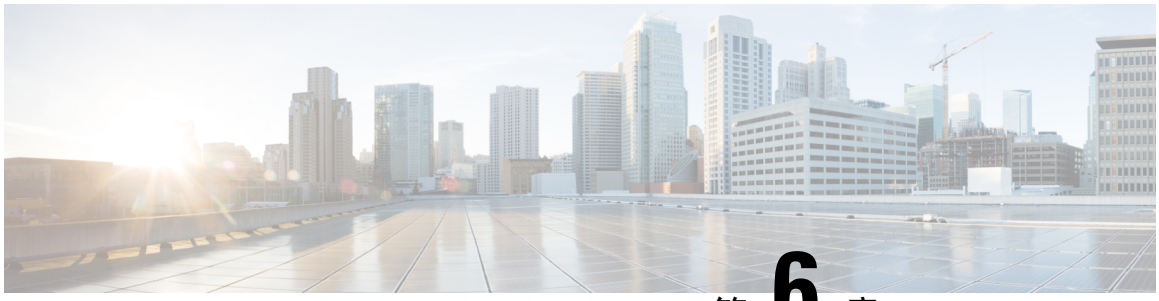
表 *22 :* インスタント メッセージングと *Presence* のポートのうち *Transport Layer Security* バージョン *1.2* による影響を受けるもの

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

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**
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 電話 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

CA で署名された証明書は、デジタル証明書に署名および発行する信頼できるサードパーティ証明書です。

デフォルトでは、Unified Communications Manager はすべての接続に自己署名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、CA ルート証明書チェーンを Cisco Unified Communications Manager Administration にインストールします。

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。証明書をアップロード、ダウンロード、および表示する方法の詳細については、「**自己署名証明書**」セクションを参照してください。

構成

Unified Communications Manager に接続している別のシステムからの CA で署名された証明書を使用する場合は、 Cisco Unified Communications Manager Administration で次の手順を実行します。

- 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。

CA で署名された証明書を Unified Communications Manager で使用する場合は、次の手順に従います。

- Cisco Unified Communications Manager Administration で CA で署名された証明書を要求するには、CSR を完了します。
- CA ルート証明書チェーンと CA で署名された証明書の両方を次のページでダウンロードします。 Cisco Unified Communications Manager Administration
- CA ルート証明書チェーンと CA で署名された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。

証明書署名要求のキー用途拡張

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 *23 : 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		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）	Y	Y	Y		Y	Y	Y		

表 *24 : 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

サーバ証明書は、基本的にサーバを識別するための証明書です。サーバ証明書は、コンテンツを暗号化および復号化する論拠の役目を果たします。

Unified Communications Manager サーバ内の自己署名証明書（所有）証明書タイプは次のとおりです。

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

表 *25 :* 証明書タイプと説明

証明書タイプ	説明
Cisco Unity サーバまたは Cisco Unity Connection 証明書	Cisco Unity と 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 デバイス証明書に署名します。Cisco unityの場合、 Cisco Unity TELEPHONY Integration Manager (UTIM) はこの証明書を管理します。Cisco Unity Connection の場合は、Cisco Unity Connection の管理機能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。

証明書タイプ	説明
SIP プロキシサーバ証明書	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 Unified Communications Manager 証明書が含まれている場合、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。

（注） 証明書名は、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ます。すべてのデバイス (またはポート) は、ルート証明書をルートとする証明書を発行します。

次の追加の信頼ストアが存在します。

- tomcat および web アプリケーションの共通信頼ストア
- IPSec-trust
- CAPF-trust
- Userlicensing: 信頼
- TVS-trust
- Phone-SAST-trust
- Phone-CTL-trust

Cisco Unity Connection の CA 信頼証明書の詳細については、Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。これらの信頼証明書は、電子メール、予定表情報、連絡先を取得するための Exchange または Meeting Place Express へのセキュアな接続を確保します。

証明書の管理タスク

証明書の表示

証明書の一覧を共通名、有効期限、キータイプ、使用法に基づいて並べ替えて表示するには、[証明書の一覧（Certificate List）] ページでフィルタオプションを使用します。フィルタオプションにより、データの並べ替え、表示、管理を効率的に行うことができます。

Unified Communications Manager リリース 14 以降では、アイデンティティ証明書または信頼証明書の一覧を並べ替えて表示するときの基準として、使用法オプションを選択できます。

手順

Step 1 Cisco Unified OS の管理から、[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。
[Certificate List] ページが表示されます。

Step 2 [証明書の一覧の検索条件（Find Certificate List where）] ドロップダウンリストから目的のフィルタオプションを選択し、[検索（Find）] フィールドに検索項目を入力して、[検索（Find）] ボタンをクリックします。

たとえば、アイデンティティ証明書だけを表示するには、[証明書の一覧の検索条件（Find Certificate List where）] ドロップダウンリストから [使用法（Usage）] を選択し、[検索（Find）] フィールドにアイデンティティを入力して、[検索（Find）] ボタンをクリックします。

証明書のダウンロード

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

手順

Step 1 [Cisco Unified OS Administration] から **[Security]** > **[Certificate Management]** を選択します。

Step 2 検索情報を指定し、[検索（Find）] をクリックします。

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

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している場合にのみ必要です。

手順

Step 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。

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

Step 3 ルート証明書をインストールするには、**[証明書の目的（Certificate Purpose）]** ドロップダウンリストから適切な信頼ストアを選択します。

Step 4 選択した証明書の目的の説明を入力します。

Step 5 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。

Step 6 [アップロード（Upload）] をクリックします。

Step 7 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。また、証明書が既存のチェーンの一部である場合、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します。この操作は取り消すことができません。

手順

Step 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。

Step 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。

Step 3 証明書のファイル名を選択します。

Step 4 [削除（Delete）] をクリックします。

Step 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」 証明書タイプの場合、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

証明書が期限切れになる前に、証明書を再生成することを推奨します。RTMT（Syslog Viewer）で警告が発行され、証明書の期限が近くなると電子メールで通知が送信されます。

ただし、期限切れの証明書を再生成することもできます。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、営業時間後にこのタスクを実行します。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

Step 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。

Step 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。フィールドおよびその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 3 [生成（Generate）] をクリックします。

Step 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。

Step 5 CAPF 証明書、ITLRecovery 証明書、または CallManager 証明書の再生成後に CTL ファイルを更新します（設定している場合）。

（注） 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。

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 *26*：証明書の名前と説明

名前	説明	関連サービス
tomcat tomcat-ECDSA	この証明書は、SIP Oauth モードが有効な場合に Web サービス、Cisco DRF サービス、および Cisco CallManager サービスで使用されます。	Cisco Tomcatサービス、Cisco CallManagerサービス、HAProxyサービス、およびCisco Disaster Recovery System（DRS）ローカルおよびマスターサービス。
CallManager CallManager-ECDSA	SIP、SIP トランク、SCCP、TFTP などに使用されます。	CallManager - HAProxy サービス CallManager-ECDSA - Cisco CallManager サービス
CAPF	Unified Communications Manager パブリッシャで実行されている CAPF サービスで使用されます。この証明書は、エンドポイントに LSC を発行するために使用されます（オンラインおよびオフライン CAPF モードを除く）。	該当なし
信頼検証サービス（TVS）	これは信頼検証サービスで使用され、サーバ証明書が変更された場合に、電話機のセカンダリ信頼検証メカニズムとして機能します。	該当なし

（注） [セキュリティパラメータ（Security Parameter）] セクションには、新しいエンタープライズパラメータとして [証明書更新時の電話機の動作（Phone Interaction on Certificate Update）] が導入され、TVS、CAPF、TFTP のいずれかの証明書が更新されたときに、電話機のリセットを手動で行うか自動で行うかを設定できます。デフォルトでは、このパラメータは電話機を自動的にリセットするように設定されています。

OAuth 更新ログイン用のキーの再生成

コマンドライン インターフェイスを使用して暗号キーと署名キーの両方を再生成するには、この手順を使用します。Cisco Jabber が Unified Communications Manager との OAuth 認証に使用する暗号キーまたは署名キーが侵害された場合にのみ、この作業を実行します。署名キーは非対称で RSA ベースであるのに対し、暗号キーは対称キーです。

このタスクを完了すると、これらのキーを使用する現在のアクセス トークンと更新トークンは無効になります。

エンドユーザへの影響を最小限に抑えるために、このタスクは営業時間外に完了することを推奨します。

暗号キーは、以下の CLI を使用してのみ再生成できますが、パブリッシャノードの Cisco Unified OS の管理 GUI を使用して署名キーを再生成することもできます。**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択し、**AUTHZ** 証明書を選択して、**[再作成（Regenerate）]** をクリックします。

手順

Step 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。

Step 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。

Step 3 署名キーを再生成するには、次の手順を実行します。

a) `set key regen authz signing` コマンドを実行します。
b) 「`yes`」と入力します。
Unified Communications Manager パブリッシャ ノードがキーを再生成し、IM and Presence サービスのローカル ノードを含めたすべての Unified Communications Manager クラスタ ノードに新しいキーを複製します。

すべての UC クラスタで新しいキーを再生成して同期する必要があります。

- IM and Presence 中央クラスタ：IM and Presence 集中型展開の場合、IM and Presence ノードはテレフォニーとは別のクラスタ上で実行されています。この場合、IM and Presence Service の

中央クラスタの Unified Communications Manager パブリッシャ ノードで、この手順を繰り返します。

- Cisco Expressway または Cisco Unity Connection：これらのクラスタ上でもキーを再生成します。詳細については、Cisco Expressway および Cisco Unity Connection のマニュアルを参照してください。

（注） 次のシナリオでは、Cisco XCP 認証サービスを再起動する必要があります。

- Authz 証明書を再生成する場合
- IM and Presenc e管理コンソールで集中型展開に新しいエントリを作成する場合

証明書署名要求の生成

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

（注） 新しい CSR を生成すると、既存の CSR は上書きされます。

手順

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

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

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

Step 4 [生成（Generate）] をクリックします。

証明書署名要求のダウンロード

CSR を生成した後にダウンロードし、認証局に提出する準備をします。

手順

Step 1 [Cisco Unified OS Administration] から **[Security] > [Certificate Management]** を選択します。

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

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

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

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

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 ルート証明書を使用 する場合は、ルート証明書を Unified Communications Manager 信頼ストアに追加します。

手順

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

Step 2 [Upload Certificate/Certificate chain] をクリックします。

Step 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、[証明書の目的（Certificate Purpose）] ドロップダウンリストから [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。

Step 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。

手順

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

Step 2 `utils ctl update CTLfile` コマンドを実行します。CTL ファイルを再生成すると、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

Step 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。

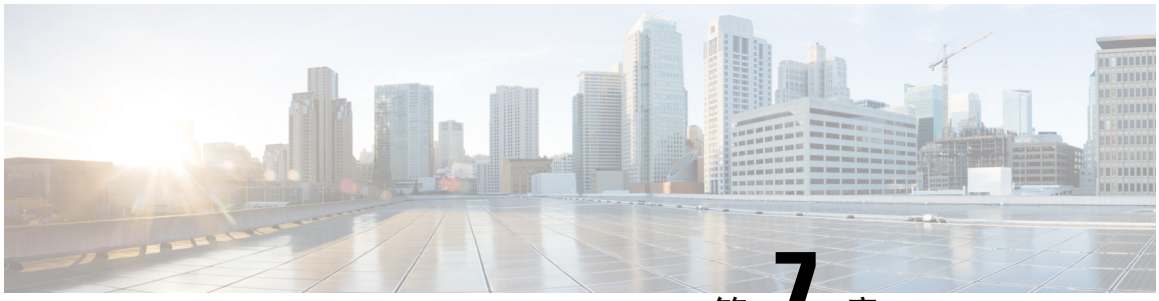
Step 2 証明書を選択して情報を表示します。証明書の内容が、リモート ノード上の対応する証明書の内容と一致することを確認します。

Step 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。

Step 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。

Step 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。

Step 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 認証局プロキシ機能（CAPF）は、ローカルで有効な証明書（LSC）を発行し、Cisco エンドポイントを認証する Cisco 専有サービスです。CAPF サービスは、Unified Communications Manager 上で実行され、次のタスクを実行します。

- サポートされる Cisco Unified IP 電話 に対して LSC を発行する。
- 混合モードが有効になっている場合に電話機を認証する。
- 電話機用の既存の LSC をアップグレードする。
- 表示とトラブルシューティングのために電話機証明書を取得する。

CAPF の実行モード

CAPF は、次のモードで動作するように設定することができます。

- Cisco Authority プロキシ機能：Unified Communications Manager の CAPF サービスが、CAPF サービス自体によって署名された LSC を発行します。これがデフォルトのモードです。
- オンライン CA：外部オンライン CA によって電話機用の LSC に署名する場合は、このオプションを使用します。CAPF サービスは自動的に外部 CA に接続します。CSR が送信されると CA が署名し、CA で署名された LSC が自動的に返されます。
- オフライン CA：オフラインの外部 CA によって電話機用の LSC に署名する場合は、このオプションを使用します。このオプションでは、LSC を手動でダウンロードし、CA に提出して、CA で署名された証明書の準備ができたら、それらをアップロードする必要があります。

（注） サードパーティ CA を使用して LSC に署名する必要がある場合、シスコでは、オフライン CA ではなくオンライン CA のオプションを使用することを推奨します。オンライン CA ではプロセスが自動化されるため、はるかに高速で、問題が発生する可能性も低くなります。

CAPF サービス証明書

統合コミュニケーションマネージャがインストールされている場合、CAPF サービスが自動的にインストールされ、CAPF 固有のシステム証明書が生成されます。セキュリティが適用されると、Cisco CTL クライアントは、すべてのクラスタノードに証明書をコピーします。

電話機の証明書タイプ

シスコは次の X.509v3 証明書タイプを電話で使用します。

- ローカルで有効な証明書（LSC）：このタイプの証明書は Cisco Certificate Authority Proxy Function（CAPF）に関連する必要な作業の実行後に、電話にインストールされます。デバイス セキュリティ モードを認証または暗号化に設定した後で、LSC は Unified Communications Manager と電話の間の接続を保護します。

（注） オンライン CA の場合、LSC の有効性は CA に基づいています。また、CA が許可している限り使用できます。

- 製造元でインストールされる証明書（MIC）：Cisco Manufacturing は MIC をサポートされている電話モデルに自動的にインストールします。製造元でインストールされる証明書は LSC インストールの Cisco Certificate Authority Proxy Function（CAPF）を認証します。製造元でインストールされる証明書を上書きしたり、削除することはできません。

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

CAPF 経由の LSC 生成

CAPF を設定した後、電話機に設定されている認証文字列を追加します。キーと証明書の交換は、電話機と CAPF の間で行われ、以下が発生します。

- 電話機は、設定された認証方法を使用して CAPF に対して自身を認証します。
- 電話機は公開/秘密キー ペアを生成します。
- 電話機は、署名されたメッセージの中で、公開キーを CAPF に転送します。
- 秘密キーは電話に残り、外部に公開されることはありません。
- 証明書は CAPF によって署名され、署名付きメッセージによって電話に送り返されます。

（注） 電話のユーザが証明書操作の中断や、電話の動作ステータスの確認を実行できることに注意してください。

（注） キーの生成を低い優先順位で設定すると、アクションの発生中に、電話機が機能します。電話機は証明書生成中に機能しますが、TLS トラフィックが追加された場合、電話機でのコールプロセスの中断が最小限に抑えられる可能性があります。たとえば、インストールの最後に証明書がフラッシュに書き込まれると、音声信号が発生することがあります。

CAPF 前提条件

LSC 生成用の認証局のプロキシ機能を設定する前に、次の手順を実行します。

- サードパーティ CA を使用して LSCs に署名したい場合は、CA を外部に設定します。
- 電話機を認証する方法を計画します。
- LSC を生成する前に、次の条件を満たしていることを確認してください。
  - Unified Communications Manager リリース 12.5 以降
  - 証明書に CAPF を使用するエンドポイント（Cisco IP 電話 および Jabber を含む）
  - Microsoft Windows Server 2012 および 2016
  - ドメインネームサービス（DNS）が構成されている
- LSC を生成する前に、CA ルート証明書と HTTPS 証明書をアップロードする必要があります。セキュア SIP 接続では、HTTPS 証明書は CAPF 信頼を通過し、CA ルート証明書は CAPF 信頼と CallManager 信頼を通過します。インターネット インフォメーション サービス（IIS）は、HTTPS 証明書をホストします。CA ルート証明書は、証明書署名要求 (CSR) への署名に使用されます。

  証明書をアップロードする必要がある場合のシナリオを次に示します。

表 *27:* 証明書のアップロードシナリオ

シナリオ	結果
CA ルート証明書と HTTPS 証明書が同じ。	CA ルート証明書をアップロードする。
CA ルート証明書と HTTPS 証明書が異なり、HTTPS 証明書は同じ CA ルート証明書によって発行される。	CA ルート証明書をアップロードする。
中間 CA 証明書と HTTPS 証明書が異なり、CA ルート証明書によって発行される。	CA ルート証明書をアップロードする。
CA ルート証明書と HTTPS 証明書が異なり、同じ CA ルート証明書によって発行される。	CA ルート証明書と HTTPS 証明書をアップロードする。

（注） 複数の証明書を同時に生成するとコール処理中断の原因となるため、スケジュールされたメンテナンスの時間帯に CAPF を使用することを強く推奨します。

認証局プロキシ機能の設定タスクフロー

次のタスクを実行して、証明機関プロキシ機能 (CAPF) サービスがエンドポイント用 LSCs を発行するように設定します。

手順

	コマンドまたはアクション	目的
Step 1	サードパーティの認証局のルート証明書のアップロード	LSC にサードパーティの CA 署名を適用する場合は、CA ルート証明書チェーンを CAPF 信頼ストアにアップロードします。その他の場合は、このタスクをスキップします。
Step 2	認証局（CA）ルート証明書のアップロード （166 ページ）	CA ルート証明書を Unified Communications Manager 信頼ストアにアップロードします。
Step 3	オンライン認証局の設定 （166 ページ）	電話機の LSC 証明書を生成するには、次の手順を使用します。

	コマンドまたはアクション	目的
Step 4	オフライン認証局の設定の設定	オフライン CA を使用して電話機 LSC 証明書を生成するには、次の手順を使用します。
Step 5	CAPF サービスのアクティブ化または再起動	CAPF システム設定を構成した後、必須の CAPF サービスをアクティブにします。
Step 6	次のいずれかの手順を使用 して、Unified Communications Manager で CAPF 設定を構成します。 • ユニバーサル デバイス テンプレートでの CAPD 設定の構成（169 ページ） • 一括管理による CAPF 設定の更新（171 ページ） • 電話機の CAPF 設定の構成（172 ページ）	次のオプションのいずれかを使用して、CAPF 設定を電話機の設定に追加します。 • まだ LDAP ディレクトリを同期していない場合、CAPF 設定をユニバーサルデバイステンプレートに追加し、初期 LDAP 同期を使用して設定を適用します。 • 一括管理ツールを使用すると、1 回の操作で多数の電話機に CAPF 設定を適用できます。 • CAPF 設定を電話機ごとに適用することができます。
Step 7	キープアライブ タイマーの設定（173 ページ）	（オプション）ファイアウォールがタイムアウトしないように、CAPF エンドポイント接続のキープアライブ値を設定します。デフォルト値は 15 分です。

サードパーティの認証局のルート証明書のアップロード

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

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

手順

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

Step 2 [Upload Certificate/Certificate chain] をクリックします。

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

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

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

Step 6 [アップロード（Upload）] をクリックします。

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

認証局（CA）ルート証明書のアップロード

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

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

Step 2 [Upload Certificate/Certificate chain] をクリックします。

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

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

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

Step 6 [アップロード（Upload）] をクリックします。

オンライン認証局の設定

オンライン CAPF を使用 して電話機 LSC を生成するには、Unified Communications Manager でこの手順を使用します。

（注） FIPS 対応モードは、オンライン CAPF および CAPFips3 をサポートしません。

手順

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

Step 2 **[サーバ（Server）]** ドロップダウンリストから、[Cisco Certificate Authority Proxy Function（アクティブ）（Cisco Certificate Authority Proxy Function (Active)）] サービスをアクティブにしたノードを選択します。

Step 3 **[サービス（Service）]** ドロップダウン リストから、[Cisco Certificate Authority Proxy Function（アクティブ）（Cisco Certificate Authority Proxy Function (Active)）] を選択します。サービス名の横に「Active」と表示されることを確認します。

Step 4 [エンドポイントへの証明書発行者（Certificate Issuer to Endpoint）] ドロップダウンリストから、[オンラインCA（Online CA）] を選択します。CA 署名付き証明書の場合、オンライン CA を使用することを推奨します。

Step 5 [証明書の有効期間（日数）（Duration Of Certificate Validity (in Days)）] フィールドに、CAPF が発行した証明書が有効である日数を表す数値を、1 ～ 1825 の間で指定します。

Step 6 [オンラインCAパラメータ（Online CA Parameters）] セクションで、次のパラメータを設定して、オンライン CA セクションへの接続を作成します。

- [オンラインCAホスト名（Online CA Hostname）]：サブジェクト名または共通名（CN）は、HTTPS 証明書の完全修飾ドメイン名（FQDN）と同じである必要があります。

  （注） 設定されたホスト名は、Microsoft CA で実行されているインターネットインフォメーション サービス（IIS）によってホストされる HTTPS 証明書の共通名（CN）と同じです。

- [オンラインCAポート（Online CA Port）]：オンライン CA のポート番号を入力します。たとえば、443 のように指定します。
- [オンラインCAテンプレート（Online CA Template）]：テンプレートの名前を入力します。Microsoft CA がテンプレートを作成します。
- [オンラインCAタイプ（0Online CA Type）]：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（Online CA Username）]：CA サーバのユーザ名を入力します。
- [オンラインCAパスワード（Online CA Password）]：CA サーバのユーザ名のパスワードを入力します。

Step 7 残りの CAPF サービスパラメータを完了します。サービスパラメータのヘルプシステムを表示するには、パラメータ名をクリックします。

Step 8 [保存（Save）] をクリックします。

Step 9 変更内容を有効にするには、**Cisco Certificate Authority Proxy Function** を再起動します。Cisco Certificate Enrollment サービスが自動的に再起動します。

現在のオンライン CA の制限

- オンライン CA 操作の場合、EST サーバは CUCM から TVS 証明書を使用します。TVS 証明書が CA で署名されている場合、オンライン CA は動作しません。
- CA サーバが英語以外の言語を使用している場合、オンライン CA 機能は動作しません。CA サーバは英語でのみ応答します。

- オンライン CA 機能は、CA での mTLS 認証をサポートしていません。
- LSC 操作にオンライン CA を使用している場合、LSC 証明書に「デジタル署名」と「キー暗号化」のキー使用法が指定されていないと、デバイスのセキュア登録は失敗します。
- LSC 操作にオンライン CA を使用している場合、LSC 証明書に「デジタル署名」と「キー暗号化」が指定されていないと、デバイスのセキュア登録は失敗します。

オフライン認証局の設定の設定

オフライン CA を使用して電話機 LSC 証明書を生成することを決定した場合は、次の高度なプロセスに従うことができます。

（注） オフライン CA オプションを使用すると、オンライン CA よりも時間がかかり、手動による手順が非常に多くなります。証明書の生成および送信プロセス中に問題（たとえば、ネットワークの停止や電話機のリセットなど）が発生した場合は、プロセスを再起動する必要があります。

手順

Step 1 サードパーティ認証局からルート証明書チェーンをダウンロードします。

Step 2 ルート証明書チェーンを Unified Communications Manager 内の必要な信頼（CallManager 信頼 CAPF 信頼）にアップロードします。

Step 3 [エンドポイントへの証明書の発行（Certificate Issue to Endpoint）] サービスパラメータを [オフライン CA（Offline CA）] に設定して、オフライン CA を使用するように Unified Communications Manager を設定します。

Step 4 お使いの電話機の LSC 用に **CSR** を生成します。

Step 5 認証局に**CSR** を送信します。

Step 6 **CSR** から署名付き証明書を取得します。

オフライン CA を使用して電話機 LSC を生成する方法の詳細な例については、「CUCM サードパーティ CA 署名済み LSC の作成およびインポートの設定」を参照してください。

CAPF サービスのアクティブ化または再起動

CAPF システム設定を構成した後、必須の CAPF サービスをアクティブにします。CAPF サービスがすでにアクティブ化されている場合は、再起動します。

手順

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

Step 2 [サーバ（Server）] ドロップダウン リストからパブリッシャ ノードを選択し、[移動（Go）] をクリックします。

Step 3 [セキュリティサービス（Security Services）] ペインで、適用されるサービスを確認します。

- **Cisco Certificate Enrollment Service**：オンライン CA を使用している場合は、このサービスをオンにし、そうでない場合はオフのままにします。
- **Cisco Certificate Authority Proxy Function**：オフになっている（非アクティブ）場合は、このサービスをオンにします。このサービスがすでにアクティブ化されている場合は、再起動します。

Step 4 設定を編集した場合は、[保存（Save）] をクリックします。

Step 5 **Cisco Certificate Authority Proxy Function** サービスがすでにチェックされている場合は（アクティブ）、再起動します。

a) **[関連リンク（Related Links）]** ドロップダウンリストから **[コントロールセンター - 機能サービス（Control Center - Feature Services）]** を選択し、**[移動（Go）]** をクリックします。

b) [セキュリティ設定（Security Settings）] ペインで、[Cisco Certificate Authority Proxy Function] サービスをオンにして、[再起動（Restart）] をクリックします。

Step 6 次の手順のいずれかを実行して、個々の電話機に対して CAPF 設定を構成します。

a) ユニバーサル デバイス テンプレートでの CAPD 設定の構成 （169 ページ）

b) 一括管理による CAPF 設定の更新 （171 ページ）

c) 電話機の CAPF 設定の構成 （172 ページ）

ユニバーサル デバイス テンプレートでの CAPD 設定の構成

CAPF 設定をユニバーサルデバイステンプレートに設定するには、次の手順を実行します。テンプレートは、機能グループテンプレートの設定を使用して、LDAP ディレクトリ同期に適用することができます。テンプレートの CAPF 設定は、このテンプレートを使用する同期のすべてのデバイスに適用されます。

（注） ユニバーサルデバイステンプレートは、まだ同期されていない LDAP ディレクトリにしか追加することができません。初期 LDAP 同期が発生した場合は、一括管理を使用して電話機を更新します。詳細については、「一括管理による CAPF 設定の更新（171 ページ）」を参照してください。

手順

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

Step 2 次のいずれかを実行します。

- [検索（Find）] をクリックして、既存のテンプレートを選択します。
- [新規追加（Add New）] をクリックします。

Step 3 [認証局プロキシ機能（CAPF）の設定（Certificate Authority Proxy Function (CAPF) Settings）] 領域を展開します。

Step 4 [証明書の操作（Certificate Operation）] ドロップダウンリストで、[インストール/アップグレード（Install/Upgrade）] を選択します。

Step 5 [認証モード（Authentication Mode）] ドロップダウンリストメニューから、デバイスを認証するためのオプションを選択します。

Step 6 認証文字列の使用を選択した場合は、[認証文字列（Authentication String）] テキストボックスに文字列を入力するか、または [文字列を生成（Generate String）] をクリックして、システムによって文字列が生成されるようにします。

（注） この文字列がデバイス上で設定されていない場合、認証は失敗します。

Step 7 残りのフィールドで、キー情報を設定します。フィールドの詳細については、オンラインヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

（注） このテンプレートを使用するデバイスは、この手順で割り当てたのと同じ認証方式で設定されていることを確認してください。それ以外の場合、デバイス認証は失敗します。電話機の認証を設定する方法の詳細については、電話機のマニュアルを参照してください。

Step 9 次の手順に従って、このプロファイルを使用しているデバイスにテンプレートの設定を適用します。

a) ユニバーサル デバイス テンプレートを [機能グループテンプレートの設定（Feature Group Template Configuration）] に追加します。
b) 同期されていない LDAP ディレクトリ設定に機能グループテンプレートを追加します。
c) LDAP 同期を完了します。CAPF 設定は、同期されているすべてのデバイスに適用されます。

機能グループテンプレートと LDAP ディレクトリの設定の詳細については、『Cisco Unified Communications Manager システム設定ガイド』の「エンドユーザの設定」の項を参照してください。

一括管理による CAPF 設定の更新

Bulk Administrationの**電話機の更新**クエリを使用して、1 回の操作で多数の既存の電話機に CAPF 設定と LSC 証明書を設定します。

（注） まだ電話機をプロビジョニングしていない場合は、一括管理の [電話機の挿入（Insert phone）] メニューを使用して、CSV ファイルからの CAPF 設定で新しい電話機をプロビジョニングできます。CSV ファイルから電話機を挿入する方法の詳細については、『Cisco Unified Communications Manager 一括管理ガイド』の「電話機の挿入」セクションを参照してください。

電話機は、この手順で追加する文字列と認証方式と同じ文字列と認証方式で設定されていることを確認します。それ以外の場合、お使いの電話機は CAPF に対して認証しません。電話機で認証を設定する方法の詳細については、電話ドキュメンテーションを参照してください。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[一括管理（Bulk Administration）] > [電話機（Phones）] > [電話機の更新（Update Phones）] > [クエリ（Query）]**

Step 2 フィルタオプションを使用して、更新する電話機に検索を制限し、[検索（Find）] をクリックします。

たとえば、[電話機の検索場所（Find phones where）] ドロップダウンリストを使用して、特定の日付の前に LSC の有効期限が切れる電話機や、特定のデバイスプールにある電話機をすべて選択します。

Step 3 [次へ（Next）] をクリックします。

Step 4 [ログアウト/リセット/リスタート（Logout/Reset/Restart）] セクションで、[設定の適用（Apply Config）] ラジオボタンを選択します。ジョブを実行すると、CAPF アップデートは更新されたすべての電話に適用されます。

Step 5 [認証局プロキシ機能（CAPF）情報（Certification Authority Proxy Function (CAPF) Information）] で、[証明書の操作（Certificate Operation）] チェックボックスをオンにします。

Step 6 [証明書の操作（Certificate Operation）] ドロップダウンリストから、[インストール/アップグレード（Install/Upgrade）] を選択して、新しい LSC 証明書を電話機にインストールします。

Step 7 [認証モード（Authentication Mode）] ドロップダウンリストから、LSC のインストール時に電話機を認証する方法を選択します。

（注） 電話機で同じ認証方式を設定します。

Step 8 [認証モード（Authentication Mode）]として [認証文字列による（By Authentication String）] を選択した場合は、次の手順のいずれかを実行します。

- 各デバイスに対して一意の認証文字列を使用する場合は、[各デバイスに対して一意の認証文字列を生成する（Generate unique authentication string for each device）] をオンにします。
- すべてのデバイスに同じ認証文字列を使用する場合は、[認証文字列（Authentication String）] テキストボックスに文字列を入力するか、[文字列の生成（Generate String）] をクリックします。

Step 9 [電話の更新（Update Phones）] ウィンドウの [認証局プロキシ機能（CAPF）情報（Certification Authority Proxy Function (CAPF) Information）] セクションで、残りのフィールドを入力します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

Step 10 [ジョブ情報（Job Information）] セクションで、[今すぐ実行（Run Immediately）]を選択します。

（注） スケジュールされた時刻にジョブを実行する場合は、[後で実行（Run Later）] を選択します。ジョブのスケジュール設定の詳細については、『Cisco Unified Communications Manager 一括管理ガイド』の「スケジュールされたジョブの管理」セクションを参照してください。

Step 11 [送信（Submit）] をクリックします。

（注） この手順で [設定の適用（Apply Config）] オプションを選択しなかった場合は、[電話機の設定（Phones Configuration）] ウィンドウですべての更新された電話機に設定を適用します。

電話機の CAPF 設定の構成

個々の電話機の LSC 証明書の CAPF 設定を設定するには、次の手順を実行します。

（注） LDAP 設定を多数の電話機に適用するには、一括管理または CAPF ディレクトリ同期を使用します。

この手順で追加するのと同じ文字列と認証方式で電話機を設定します。それ以外の場合、電話機は CAPF に対してそれ自体を認証しません。電話機で認証を設定する方法の詳細については、電話ドキュメンテーションを参照してください。

手順

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

Step 2 既存の電話機を選択するには、[検索（Find）] をクリックします。[電話の設定（Phone Configuration）] ページが表示されます。

Step 3 [認証局プロキシ機能（CAPF）情報（Certification Authority Proxy Function (CAPF) Information）] ペインに移動します。

Step 4 [証明書の操作（Certificate Operation）] ドロップダウンリストから、[インストール/アップグレード（Install/Upgrade）] を選択して、新しい LSC 証明書を電話機にインストールします。

Step 5 [認証モード（Authentication Mode）] ドロップダウンリストから、LSC のインストール時に電話機を認証する方法を選択します。

（注） 電話機は、同じ認証方式を使用するように設定する必要があります。

Step 6 [認証文字列による（By Authentication String）] を選択した場合は、テキスト文字列を入力するか、[文字列の生成（Generate String）] をクリックして文字列を生成します。

Step 7 [電話の設定（Phone Configuration）] ページの [認証局プロキシ機能（CAPF）情報（Certification Authority Proxy Function (CAPF) Information）] ペインで、残りのフィールドに詳細を入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

キープアライブ タイマーの設定

ファイアウォールによって接続がタイムアウトしないように、次の手順を実行して、CAPF-エンドポイント接続のクラスターワイド キープアライブ タイマーを設定します。デフォルト値は 15 分です。各間隔の後、CAPF サービスは電話機にキープアライブ信号を送信して、接続を開いた状態にします。

手順

Step 1 コマンド ライン インターフェイスを使用して、パブリッシャノードにログインします。

Step 2 `utils capt set keep_alive` CLI コマンドを実行します。

Step 3 5 ～ 60（分）の間の数値を入力し、**Enter** キーを押します。

CAPF の管理タスク

CAPF を設定し、LSC 証明書を発行した後、次のタスクを使用して LSC 証明書を継続的に管理します。

証明書ステータスのモニタリング

証明書のステータスを自動的に監視するようにシステムを設定することができます。証明書が期限切れに近づいたときにシステムから電子メールが送信され、期限切れ後に証明書が失効します。

証明書の監視の確認の設定方法の詳細については、「証明書の管理」の章の「証明書の監視と失効のタスクフロー」を参照してください。

古い LSC レポートの実行

次の手順を使用して、古い LSC レポートを Cisco ユニファイドレポートから実行します。古い LSC とは、エンドポイント CSR への応答として生成された証明書ですが、その LSC がインストールされる前にエンドポイントによって新しい CSR が生成されたため、インストールされなかったものです。

（注） パブリッシャーノードで `utils capf stale-lsc list` CLI コマンドを実行して、古い LSC 証明書のリストを取得することもできます。

手順

Step 1 Cisco Unified Reporting から、[システムレポート（System Reports）] を選択します。

Step 2 左側のナビゲーションバーで、[古いLSC（Stale LSCs）] を選択します。

Step 3 [新規レポートの作成（Generate a new Report）] をクリックします。

保留中の CSR リストの表示

保留中の CAPF CSR ファイルのリストを表示するには、この手順を使用します。すべての CSR ファイルはタイムスタンプされます。

手順

Step 1 コマンド ライン インターフェイスを使用して、パブリッシャノードにログインします。

Step 2 `utils core active list` CLI コマンドを実行します。
保留中の CSR ファイルのタイムスタンプリストが表示されます。

古い LSC 証明書の削除

古い LSC 証明書をシステムから削除するには、次の手順を使用します。

手順

Step 1 コマンド ライン インターフェイスを使用して、パブリッシャノードにログインします。

Step 2 `utils capf stale-lsc delete all` CLI コマンドを実行します。

古い LSC 証明書はすべてシステムから削除されます。

CAPF システムの連携動作と制限事項

機能	連携動作
認証文字列	電話の CAPF 認証方式については、アップグレードまたはインストールの後に同じ認証文字列を電話に入力する必要があります。入力されなかった場合、操作が失敗します。[TFTP Encrypted Config]エンタープライズパラメータが有効な状態で認証文字列の入力に失敗した場合、電話の設定は失敗し、該当する認証文字列が電話に入力されるまで回復しません。
クラスタ サーバ クレデンシャル	CAPF が Unified Communications Manager クラスタのすべてのサーバを認証できるよう、クラスタ内のすべてのサーバで管理者のユーザ名とパスワードを同じものにする必要があります。
セキュアな電話機の移行	セキュアな電話が別のクラスタに移動されると、Unified Communications Manager はその電話が送信する LSC 証明書を信頼しなくなります。これは、その LSC 証明書が、CTL ファイル内に証明書が存在しない別の CAPF によって発行されたものであるためです。 セキュアな電話機を登録できるようにするには、既存の CTL ファイルを削除します。その後、[Install/Upgrade] オプションを使用して新しい CAPF を使用して新しい LSC 証明書をインストールし、電話機を新しい CTL ファイルにリセット (または MIC を使用) することができます。電話機を移動する前に既存の LSC を削除するには、[電話の設定 (Phone Configuration)] ウィンドウの [CAPF] セクションの [削除 (Delete)] オプションを使用します。

機能	連携動作
Cisco Unified IP 電話 6900 シリーズ、7900 シリーズ、および 8900 シリーズ、および 9900	将来的な互換性の問題を回避するため、Unified Communications Manager との TLS 接続に LSC を使用するために Cisco Unified IP 電話 6900 シリーズ、7900 シリーズ、8900 シリーズ、9900 シリーズをアップグレードし、MIC ルート証明書を CallManager 信頼ストアから削除することが推奨されます。Cisco Unified Communications Manager との TLS 接続に MIC を使用する一部の電話モデルは登録できない場合があることに注意してください。 管理者は、CallManager 信頼ストアから次の MIC ルート証明書を削除する必要があります。 • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048
停電	以下の情報は、通信障害や電源障害の発生時に適用されます。 • 電話機で証明書のインストールが行われている間に通信障害が発生した場合、電話機は30秒間隔で証明書の取得を3回試行します。これらの値は設定できません。 • 電話機が CAPF とのセッションを試行している間に電源障害が発生した場合、電話機はフラッシュに保存されている認証モードを使用します。つまり、電話機の再起動後に、電話機が TFTP サーバから新しい設定ファイルをロードできない場合です。証明書の操作が完了すると、システムはフラッシュの値をクリアします。
証明書の暗号化	Cisco Unified Communications Manager リリース 11.5(1)SU1 以降、CAPF サービスによって発行されるすべての LSC 証明書は、SHA-256 アルゴリズムで署名されています。したがって、IP 電話 7900/8900/9900 シリーズのモデルは、SHA-256 署名済み LSC 証明書および外部 SHA2 アイデンティティ証明書（Tomcat、CallManager、CAPF、TVS など）をサポートします。署名の検証が必要な、その他の暗号化の操作では、SHA-1 のみがサポートされます。 （注） ソフトウェア メンテナンスが終了またはサポートが終了した電話モデルを使用する場合は、Unified Communications Manager の 11.5(1)SU1 より前のリリースの使用を強くお勧めします。

7942 および 7962 電話機での CAPF の例

ユーザまたはUnified Communications Managerによって電話がリセットされたときのCAPFとCisco Unified IP 電話 7962 および 7942 とのインタラクションについては、以下の情報を考慮してください。

（注） 以下の例では、電話機に LSC が存在せず、CAPF 認証モードとして [既存の証明書（By Existing Certificate）] が選択されている場合、CAPF 証明書操作が失敗します。

例：非セキュア デバイス セキュリティ モード

この例では、[Device Security Mode] を **[Nonsecure]** に設定し、[CAPF Authentication Mode] を **[By Null String]** または **[By Existing Certificate (Precedence...)]** に設定した後、電話がリセットされます。リセットした電話は直ちにプライマリ Unified Communications Manager に登録され、設定ファイルを受信します。その後、電話機は CAPF とのセッションを自動的に開始して LSC をダウンロードします。電話機が LSC をインストールした後、デバイスセキュリティモードを [認証済み (Authenticated)] または [暗号化 (Encrypted)] に設定します。

例：認証済み/暗号化済みデバイス セキュリティ モード

この例では、**[Device Security Mode]** を **[Authenticated]** または **[Encrypted]** に設定し、[CAPF Authentication Mode] を **[By Null String]** または **[By Existing Certificate (Precedence...)]** に設定した後、電話がリセットされます。CAPF セッションが終了し LSC がインストールされるまで、電話はプライマリ Unified Communications Manager に登録されません。セッションが終了すると、電話機が登録され、すぐに認証モードまたは暗号化モードで実行されます。

この例では、電話が自動的にCAPFサーバに接続されないため、**[By Authentication String]** を設定できません。電話に有効な LSC がない場合、登録は失敗します。

IPv6 アドレッシングとの CAPF のインタラクション

CAPFは、IPv4、IPv6、または両方のタイプのアドレスを使用する電話機に証明書を発行し、アップグレードすることができます。IPv6 アドレスを使用する SCCP を実行する電話の証明書の発行またはアップグレードを実行するには、[Unified Communications Manager Administration] で [Enable IPv6] サービス パラメータを **[True]** に設定する必要があります。

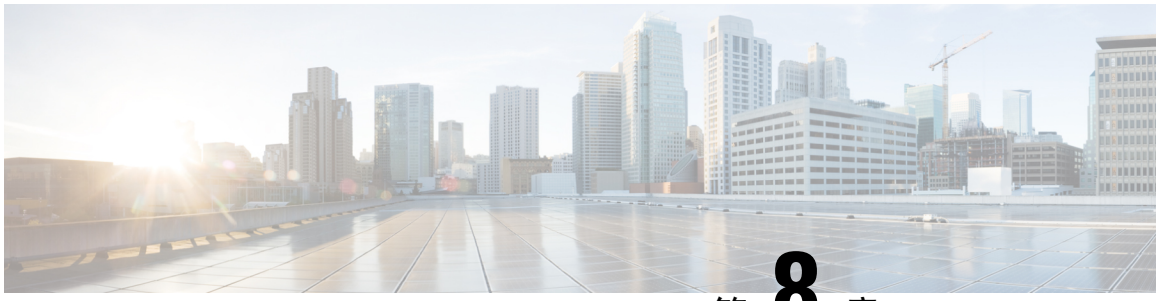
電話機が CAPF に接続して証明書を取得すると、CAPF は [IPv6 を有効にする (Enable IPv6)] エンタープライズパラメータの設定を使用して、電話機に証明書を発行するか、またはアップグレードするかを決定します。エンタープライズパラメータが**False**に設定されている場合、CapfはIPv6アドレスを使用する電話機からの接続を無視または拒否し、電話機は証明書を受信しません。

次の表では、IPv4、IPv6、または両方のタイプのアドレスを持つ電話機が CAPF に接続する方法について説明します。

表 *28 : IPv6* または *IPv4* 電話機の *CAPF* への接続方法

電話機の IP モード	電話機の IP アドレス	CAPF IP アドレス	電話機から CAPF への接続方法
2つのスタック	IPv4 と IPv6 が利用可能	IPv4、IPv6	電話機は、IPv6 アドレスを使用して CAPF に接続します。電話機が IPv6 アドレスを介して接続できない場合は、IPv4 アドレスを使用して接続を試みます。
2 スタック	IPv4	IPv4、IPv6	電話機は、CAPF に接続するために IPv4 アドレスを使用します。
2 スタック	IPv6	IPv4、IPv6	電話機は、IPv6 アドレスを使用して CAPF に接続します。試行に失敗した場合、電話機は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4 と IPv6 が利用可能	IPv6	電話機は、および IPv6 アドレスを使用して CAPF に接続します。
2つのスタック	IPv4 と IPv6 が利用可能	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4	IPv6	電話機が CAPF に接続できない。
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。

電話機の IP モード	電話機の IP アドレス	CAPF IP アドレス	電話機から CAPF への接続方法
IPv4 スタック	IPv4	IPv4、IPv6	電話機は、CAPF に接続するために IPv4 アドレスを使用します。
IPv6 スタック	IPv6	IPv4、IPv6	電話機は、IPv6 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv6	電話機が CAPF に接続できない。
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

証明書モニタリングの概要

管理者は、自動化されたシステムが Unified Communications Manager および IM and Presence Service サービスに含まれている場合、証明書を 追跡および更新できる必要があります。証明書モニタリングは、管理者が証明書のステータスを継続的に知り、証明書の有効期限が近づいたときに電子メールで通知を受信するのに役立ちます。

• 証明書モニタリングの設定 （181 ページ）

証明書モニタリングの設定

Cisco Certificate Expiry Monitor ネットワークサービスが実行されている必要があります。このサービスはデフォルトで有効になりますが、Cisco Unified Serviceability でサービスが実行されていることを確かめるには、**[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）]** のステータスが **[実行中（Running）]** であることを確認します。

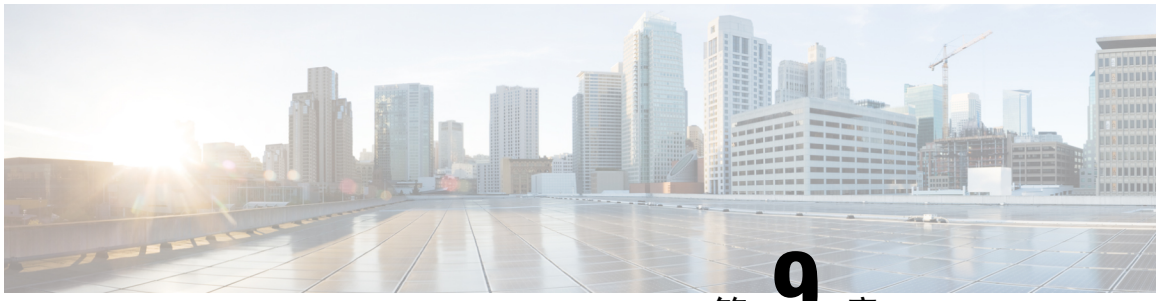
手順

Step 1 Cisco Unified OS Administration で、**[セキュリティ（Security）] > [証明書モニタ（Certificate Monitor）]** を選択します。

Step 2 設定の詳細を入力または選択します。

Step 3 **[保存（Save）]** をクリックして、設定を保存します。

（注） デフォルトで、証明書モニタサービスは 24 時間ごとに 1 回実行されます。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、この頻度は変わりません。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。



第 9 章

証明書失効の概要

このセクションでは、証明書失効について説明します。Cisco UCM は、証明書失効をモニタするためにオンライン証明書ステータスプロトコル（OCSP）をプロビジョニングします。証明書がアップロードされるたびに、スケジュールされたタイムラインで、システムはそのステータスをチェックして有効性を確認します。

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。

• 証明書失効の設定 （183 ページ）

証明書失効の設定

[有効性検証（Validation Checks）] では、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。

証明書の検証手順は次のとおりです。

- 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、OCSP 証明書に署名してステータスを確認する必要があります。
- 代理信頼モデルが失敗した場合は、レスポンダの信頼モデル（TRP）に戻ります。次に、Unified Communications Manager は OCSP サーバからの指定された OCSP 応答署名証明書を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には、OCSP 応答側が実行されている必要があります。

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。

（注） syslog、FileBeat、SIP、ILS、LBM など、TLS クライアントは OCSP からリアルタイムで失効応答を受信します。

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 応答属性で設定されたルート CA 証明書または中間 CA 証明書、または tomcat-trust にアップロードされた、指定 OCSP 署名証明書を使用できます。

手順

Step 1 Cisco Unified OS Administration で、**[セキュリティ（Security）] > [証明書失効（Certificate Revocation）]** を選択します。

Step 2 **[ANATの有効化（Enable OCSP）]** チェックボックスを選択します。

Step 3 証明書に OCSP レスポンダ URI が設定されている場合は、[証明書からの OCSP URI を使用する（Use OCSP URI from Certificate）] オプションをクリックします。

または

Step 4 OCSP チェックに OCSP レスポンダを指定する場合は、[設定された OCSP URI を使用（Use Configured OCSP URI Option）] をクリックします。

Step 5 レスポンダの [OCSP の設定済み URI] を入力します。

Step 6 失効チェックを有効にするには、[失効チェックの有効化（Enable Revocation Check）] チェックボックスをオンにします。

Step 7 失効ステータスを確認する**頻度**を入力し、[時間（Hours）] または [Days（日）] から**時間間隔**をクリックします。

Step 8 [保存（Save）] をクリックします。

（注） シスコサービスのリストを再起動して、リアルタイム OCSP を有効にするように求める、アラートがポップアップ表示されます。このポップアップは、**[OCSP の有効化（Enable OCSP）]** チェックボックスをオンにした場合、または以降の変更を保存した場合にのみ表示されます。

OCSP レスポンダは、検証とコモンクライテリアモードがオンの場合に、次のいずれかのステータスを返します。

- [良好（Good）]：OCSP レスポンダがステータスの照会に対して肯定的な応答を送信していることを示します。証明書は失効しませんが、証明書が発行されたという意味でも、応答時間が証明書の有効期間内にあるという意味でもありません。Response 拡張機能は、発行、有効性など、証明書のステータスに関してレスポンダが行ったより多くの要求を伝えます。
- [失効（Revoked）]：証明書が永久的または一時的に失効（保留）ステータスにあることを示します。
- [不明（Unknown）]：OCSP レスポンダが要求された証明書について認識していないことを示しています。

警告　コモンクライテリアモードを有効にした場合、接続は **[失効済み（Revoked）]** および **[不明（Unknown）]** のケースで失敗します。コモンクライテリアモードを無効にすると、接続は **[不明（Unknown）]** のケースで成功します。

Step 9　（任意）CTI、IPsec または LDAP リンクがある場合は、これらの長期的に中断しない接続の 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 Administration から、**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** を選択します。
b) [証明書失効と有効期限（Certificate Revocation and Expiry）] ペインに移動します。
c) [証明書有効性チェック（Certificate Validity Check）] パラメータを [有効（Enabled）] に設定します。
d) [有効性チェック頻度（Validity Check Frequency）] パラメータの値を入力します。

（注）　**[証明書失効（Certificate Revocation）]** ページの **[失効チェックの有効化（Enable Revocation Check）]** パラメータの間隔値は、**[有効性チェックの頻度（Validity Check Frequency）]** エンタープライズパラメータの値よりも優先されます。

e) [保存（Save）] をクリックします。

第 III 部

Cisco IP 電話と Cisco ボイス メッセージング ポートのセキュリティ

第 10 章

電話機のセキュリティ

この章では、電話機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 電話 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を含む新しい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、または非セキュアなシナリオについては、連携動作と制限事項に関連するトピック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ている場合、コールステータスはセキュアとして登録されます。一方のデバイスが非セキュアとして登録されている場合、発信者または受信者の電話機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 電話 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。

関連トピック

連携動作と制限事項, on page 10

信頼できるデバイス

Unified Communications Manager では Cisco IP 電話 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 電話 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 の管理

[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。

電話の設定

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。

デバイスが信頼決定基準と呼ばれる

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定します。

- 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。

サポート対象の Cisco Unified IP 電話 にロック セキュリティ アイコンが表示される前に、これら 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を含むコールでは、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セキュアでないままで、電話機にロック アイコンが表示されません。たとえば、会議で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セキュアでないものと見なします。

電話機モデルのサポート

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機には、製造元でインストールされる証明書 (MIC) が事前にインストールされており、認証局プロキシ機能 (CAPF) を使用して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ています。セキュアなシスコの電話機は、追加の証明書の管理なしで MIC を使用して Cisco ユニファイド CM に登録できます。セキュリティを強化するために、CAPF を使用して電話機に

LSC を作成してインストールすることができます。詳細については、電話セキュリティのセットアップと設定に関連する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機には、MIC が事前にインストールされておらず、LSCs を生成するための CAPF がサポートされていません。セキュアな推奨ベンダーの電話機が Cisco ユニファイド CM に接続するためには、デバイスに証明書を提供するか、デバイスによって生成される必要があります。電話機のサプライヤは、電話機の証明書を取得または生成する方法の詳細を提供する必要があります。証明書を取得したら、OS 管理証明書管理インターフェイスを使用して Cisco ユニファイド 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設定に関連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。

また、シスコのユニファイドレポートを使用して、特定の機能をサポートしている電話機を一覧表示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。

関連トピック

電話機のセキュリティの設定, on page 194
推奨ベンダーの SIP 電話セキュリティのセットアップ, on page 192
電話機のセキュリティ設定の表示, on page 194

推奨ベンダーの SIP 電話セキュリティのセットアップ

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ためには、COP ファイル内の推奨ベンダーの SIP 電話のセキュリティ暗号化または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、[新しい電話の追加(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。すべての推奨ベンダーの電話はダイジェスト認証をサポートしていますが、すべての推奨ベンダーの電話が TLS セキュリティをサポートするわけではありません。セキュリティ機能は、電話機のモデルに基づいています。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機が TLS セキュリティをサポートしている場合は、デバイスごとの証明書と共有証明書の2つのモードが考えられます。電話機のサプライヤは、電話機に適用されるモード、および電話機の証明書の生成または取得の手順を指定する必要があります。

推奨ベンダーの SIP 電話セキュリティプロファイルのデバイスごとの証明書の設定

デバイスごと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

Step 1 OS 管理証明書管理インターフェイスを使用して、各電話機の証明書をアップロードします。

Step 2 [Cisco Unified Administration] で、**[System]** > **[Security]** > **[Phone Security Profile]** の順に選択します。

Step 3 この電話のデバイスタイプに対して新しい電話セキュリティプロファイルを設定し、**[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で **[暗号化（Encrypted）]** または **[認証済み（Authenticated）]** を選択します。

Step 4 CCMAdmin インターフェイスで新しい SIP 電話を設定するには、**[デバイス (Device)]** > **[電話 (Phone)]** > **[追加 (Add new]** の順に選択します。

Step 5 [Phone Type] を選択します。

Step 6 必須フィールドに入力します。

Step 7 **[デバイスのセキュリティプロファイル（Device Security Profile）]** ドロップダウンリストで、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セットアップ

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

Step 1 電話機のベンダーの指示を使用して、サブジェクト代替名 (SAN) 文字列を使用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 extensions の場合は次のようになります。

- サブジェクト代替名
- DNS:AscomGroup01.acme.com

（注） SAN は DNS タイプである必要があります。または、セキュリティが有効になっていません。

Step 2 OS 管理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。

Step 3 [Cisco Unified Administration] で、**[System]** > **[Security]** > **[Phone Security Profile]** の順に選択します。

Step 4 **[名前 (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、優先ベンダーから提供された証明書の名前です。または、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と完全に一致する必要があります。そうしないと、セキュリティが有効になりません。

Step 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で、**[暗号化（Encrypted）]** または **[認証済み（Authenticated）]** を選択します。

Step 6 [転送タイプ（Transport type）] ドロップダウンリストで、**[TLS]** を選択します。

Step 7 CCMAdmin インターフェイスで新しい SIP 電話を設定するには、**[デバイス (Device)]** > **[電話 (Phone)]** > **[追加 (Add new]** の順に選択します。

Step 8 [Phone Type] を選択します。

Step 9 各必須フィールドに入力します

Step 10 **[デバイスのセキュリティプロファイル（Device Security Profile）]** ドロップダウンリストで、作成したプロファイルを選択します。

関連トピック

電話セキュリティ プロファイルの設定, on page 201

電話機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機の特定のセキュリティ関連の設定を構成して表示することができます。たとえば、電話機にローカルで有効な証明書または製造元でインストールされた証明書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* 電話 の管理ガイド および *Cisco IP* 電話 ユーザ ガイド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。

関連トピック

連携動作と制限事項, on page 10
セキュリティ アイコン, on page 9

電話機のセキュリティの設定

次の手順では、サポートされている電話のセキュリティを設定するタスクについて説明します。

手順

Step 1 まだ設定していない場合は、Cisco CTL クライアントを設定し、Unified Communications Manager 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。

Step 2 電話機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た証明書 (MIC) が含まれていない場合は、Certificate Authority Proxy Function (CAPF) を使用して LSC をインストールします。

Step 3 電話セキュリティ プロファイルを設定します。

Step 4 電話に電話セキュリティ プロファイルを適用します。

Step 5 ダイジェストクレデンシャルを設定した後、[電話の設定 (Phone Configuration)] ウィンドウからダイジェストユーザを選択します。

Step 6 Cisco Unified IP 電話 7962 または 7942（SIP のみ）で、[エンドユーザ設定（End User Configuration）] ウィンドウで設定したダイジェスト認証のユーザ名とパスワード（ダイジェストログイン情報）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* 電話アドミニストレーション ガイド』を参照してください。

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。このタスクの実行方法については、お使いの電話機モデルをサポートする Cisco Unified Communications Manager アドミニストレーション ガイド およびこのバージョンの Unified Communications Manager を参照してください。

Step 7 電話機がこの機能をサポートしている場合は、電話機の設定ファイルを暗号化します。

Step 8 電話機を強化するには、電話機の設定を無効にします。

関連トピック

電話機へのセキュリティ プロファイルの適用 , on page 219
Certificate Authority Proxy Function
Cisco CTL クライアントの設定, on page 113
暗号化された電話設定ファイルの設定, on page 231
エンドユーザのダイジェストクレデンシャルの設定, on page 247
電話のセキュリティ強化, on page 249
電話セキュリティ プロファイルの設定, on page 201
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, on page 247
電話機へのダイジェスト認証の割り当て, on page 248

電話セキュリティの連携動作と制限事項

ここでは、電話機のセキュリティに関する対話と制限について説明します。

表 *29* : 電話セキュリティの連携動作と制限事項

機能	連携動作および制限事項
証明書の暗号化	Unified Communications Manager リリース 11.5(1) SU1 から、CAPF サービスで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 シリーズは、SHA-256 で署名された 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した電話モデルまたはサポート終了電話モデルを使用する場合は、Unified Communications Manager11.5(1)SU1 リリースより前のバージョンを使用することを推奨します。

電話機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』

関連トピック

連携動作と制限事項, on page 10
認証、整合性、および許可, on page 25
暗号化, on page 31
認証と暗号化のセットアップ, on page 42
Certificate Authority Proxy Function
電話機のセキュリティの設定, on page 194
電話セキュリティ プロファイルの設定, on page 201
暗号化された電話設定ファイルの設定, on page 231
電話のセキュリティ強化, on page 249

TFTP OAuth の概要

この機能により、Unified Communications Manager のセキュリティが強化されます。セキュリティを向上させるために、Unified Communications Manager は SIP OAuth 対応の電話機をチェックし、TFTP OAuth を使用して設定ファイル要求を認証および承認します。Unified Communications Manager

は、エンドポイントによって提示されたトークンを確認し、有効なものだけにコンフィギュレーションファイルを提供します。

TFTP OAuth は次をサポートします。

- TFTP ファイルのダウンロードは、認証された電話に対してのみ、セキュリティで保護されたポートを介して行われていることを確認します。
- CAPF 操作は、セキュアなファイル転送には必須ではありません。

次の電話機モデルは、TFTP OAuth をサポートしています。

- 7811
- 7821
- 7832
- 7841
- 7861
- 8811
- 8832
- 8841
- 8845
- 8851
- 8851NR
- 8861
- 8865
- 8865NR

TFTP OAuth タスクフロー

始める前に

- Cisco CallManager エンタープライズパラメータの **[クラスタ SIPOAuth モード（Cluster SIPOAuth Mode）]** フィールドが **[有効（Enabled）]** に設定されていることを確認します。CLI から SIP OAuth を有効にする方法の詳細については、CLI を使用した SIP OAuth 設定を参照してください。

手順

	コマンドまたはアクション	目的
Step 1	電話セキュリティプロファイルでデバイスセキュリティモードを設定する	電話セキュリティプロファイルでデバイスセキュリティモードを設定します。
Step 2	Phone Edge TrustへのCA証明書のアップロード	CA 証明書は、Cisco Tomcat 証明書を Phone Edge Trust に発行するために使用されます。

電話セキュリティプロファイルでデバイスセキュリティモードを設定する

この手順を使用して、電話機のセキュリティプロファイルで**デバイスセキュリティモード（Device Security Mode）**を設定します。これは、その電話機の**[電話機のセキュリティプロファイル（Phone Security Profile）]**内でデバイスセキュリティモードを**[暗号化（Encrypted）]**に設定している場合にのみ必要です。

手順

Step 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。

Step 2 次のいずれかを実行します。

- 既存の電話セキュリティプロファイルを検索する
- [新規追加（Add New）] をクリックします。

Step 3 [電話セキュリティプロファイル情報（Phone Security Profile Information）] セクションの **[デバイスセキュリティモード（Device Security Mode）]** ドロップダウンリストから、**[暗号化（Encrypted）]** を選択します。

Step 4 **[転送タイプ（Transport type）]** ドロップダウンリストで、**[TLS]** を選択します。

Step 5 [OAuth 認証の有効化（Enable OAuth Authentication）] チェックボックスをオンにします。

Step 6 **[保存（Save）]** をクリックします。

Step 7 電話セキュリティプロファイルを電話に関連付けます。電話セキュリティ電話を適用する方法の詳細については、Cisco Unified Communications Manager セキュリティ ガイドの「セキュリティプロファイルを電話に適用する」セクションを参照してください。

（注） 変更を有効にするには、スマートフォンをリセットしてください。

（注） [SIP OAuth モード（SIP OAuth Mode）] が有効な場合、**[ダイジェスト認証を有効化（Enable Digest Authentication）]** および **[TFTP 暗号化設定（TFTP Encrypted Config）]** オプションはサポートされません。電話機は、**https(6971)**を介して TFTP 設定ファイルを安全にダウンロードし、認証にトークンを使用します。

Phone Edge TrustへのCA証明書のアップロード

この手順を使用して、Tomcat 署名付き証明書のルート証明書を Phone EdgeTrust にアップロードします。

（注） この手順は Cisco Phone に対してのみ実行され、Cisco Jabber には適用されません。

手順

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

Step 2 [Upload Certificate/Certificate chain] をクリックします。

Step 3 **[証明書/証明書チェーンのアップロード]** ウィンドウで、**[証明書の目的]** ドロップダウンリストから **[電話-エッジ-信頼]** を選択します。

Step 4 **[ファイルのアップロード]** フィールドで、**[参照]** をクリックして証明書をアップロードします。

Step 5 [アップロード（Upload）] をクリックします。

第 11 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、デバイスのセキュリティ モード、ダイジェスト認証およびいくつかの CAPF 設定が含まれます。[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する際に、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。電話機のセキュリティ機能を有効にするには、デバイスタイプとプロトコルに応じた新しいセキュリティプロファイルを設定し、電話機に適用する必要があります。

選択されたデバイスとプロトコルがサポートするセキュリティ機能のみが、[セキュリティ プロファイル設定（security profile settings）] ウィンドウで表示されます。

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、次の情報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。
- 事前定義された非セキュアプロファイルを削除または変更することはできません。
- デバイスに現在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。
- すでに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、その特定のプロファイルが割り当てられているすべての電話に、再設定された設定が適用されます。
- 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。以前のプロファイル名と設定で割り当てられた電話機は、新しいプロファイル名と設定を前提としています。
- CAPF 設定、認証モード、およびキーサイズは、[電話の設定 (**Phone Configuration**)] ウィンドウに表示されます。Mic または LSCs に関連する証明書操作の CAPF 設定を構成する必要があります。これらのフィールドは、[電話の**設定 (Phone Configuration**)] ウィンドウで直接更新できます。
  - セキュリティプロファイルの CAPF 設定を更新すると、[電話の設定 (Phone Configuration)] ウィンドウでも設定が更新されます。
  - [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 電話 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。

関連トピック

証明書, on page 20

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

Step 1 Cisco 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。

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

Step 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、Step 3 （203 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。条件を削除するには、**[-]** ボタンをクリックして最後に追加された条件を削除するか、または**[フィルタのクリア（Clear Filter）]** をクリックして、追加されたすべての検索条件を削除します。

Step 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、[ページあたりの行数（Rows per Page）] ドロップダウンリストで別の値を選択します。

Step 4 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

（注） ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

ウィンドウに、選択したレコードが表示されます。

関連トピック

セキュリティ プロファイルに関する詳細情報の入手先

電話セキュリティプロファイルのセットアップ

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

Step 1 Cisco 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。

Step 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。

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見つけて続行します。

[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。[コピー（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。

Step 3 SCCP または SIP を実行している電話機の適切な設定を入力します。

Step 4 [保存（Save）] をクリックします。

関連トピック

電話セキュリティプロファイルの検索, on page 203
セキュリティ プロファイルに関する詳細情報の入手先

電話セキュリティ プロファイルの設定

次の表では、SCCP を実行している電話のセキュリティ プロファイルに関する設定について説明します。

選択した電話のタイプおよびプロトコルがサポートする設定のみ表示します。

表 *30 : 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
名前	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 [電話の設定（Phone Configuration）] ウィンドウの [デバイスのセキュリティプロファイル（Device Security Profile）] ドロップダウンリスト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。

設定	説明
説明	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
[デバイスセキュリティモード（Device Security Mode）]	

設定	説明
	ドロップダウンリストから、次のオプションのいずれかを選択します。 • [非セキュア（Non Secure）]：イメージ、ファイル、デバイス認証を除くセキュリティ機能は電話機に存在しません。TCP 接続で Unified Communications Manager が利用できます。 • [認証済（Authenticated）]： Unified Communications Managerは電話機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。 • [暗号化（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 Communications 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` 中 - AES-256 AES-128のみ: RSA優先 （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。 • `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`

設定	説明
	（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（Authenticated）] として選択されている [デバイスセキュリティプロファイル（Device Security Profile）] を使用してトランクを設定した場合、Unified Communications Manager は、NULL_SHA 暗号を使用した TLS 接続（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がオンの場合、Unified Communications Manager は電話機が TFTP サーバからダウンロードするファイルを暗号化します。

設定	説明
[認証モード（Authentication Mode）]	

設定	説明
	このフィールドでは、電話機がCAPF証明書の操作時に使用する認証方法を選択できます。 ドロップダウン リスト 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、閉鎖された安全な環境だけで選択することをお勧めします。 • **[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。このオプションを選択して、電話機に証明書が

設定	説明
	存在しない場合、操作は失敗します。 （注） [電話セキュリティ プロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
[キーの順序（Key Order）]	このフィールドは、CAPF のキーの順序を指定します。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 のみ（RSA Only）]** • **[ECのみ（EC Only）]** • **[EC 優先、RSA バックアップ（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の一覧を確認できます。
[ECキーサイズ（ビット）（EC Key Size (Bits)）]	ドロップダウンリストから、**256**、**384**、または**521**のいずれかの値を選択します。

次の表では、SIP を実行している電話のセキュリティ プロファイルに対する設定について説明します。

表 *31 : 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
名前	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 [電話の設定（Phone Configuration）] ウィンドウの [デバイスのセキュリティプロファイル（Device Security Profile）] ドロップダウンリスト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。
説明	セキュリティ プロファイルの説明を入力します。
ナンス確認時間（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
[デバイスセキュリティモード（Device Security Mode）]	ドロップダウンリストから、次のオプションのいずれかを選択します。 • [非セキュア（Non Secure）]：イメージ、ファイル、デバイス認証を除くセキュリティ機能は電話機に存在しません。TCP 接続で Unified Communications Manager が利用できます。 • [認証済（Authenticated）]： Unified Communications Managerは電話機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。 • [暗号化（Encrypted）]： Unified Communications Managerは電話機の整合性、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（Authenticated）] として選択されている [デバイスセキュリティプロファイル（Device Security Profile）] を使用してトランクを設定した場合、Unified Communications Manager は、NULL_SHA 暗号を使用した TLS 接続（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
転送タイプ	[デバイスセキュリティモード（Device Security Mode）] が **[非セキュア（Non Secure）]** の場合は、ドロップダウンリストから次のオプションのいずれかを選択します（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、パケットが送信したとき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場合があります。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。 [デバイスセキュリティモード（Device Security Mode）] が [認証（Authenticated）] または [暗号化（Encrypted）] の場合、TLS では [転送タイプ（Transport Type）] を指定します。TLS は、SIP 電話に対し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（暗号化モードに限る）を提供します。 プロファイルで [デバイス セキュリティ モード（Device Security Mode）] を設定できない場合は、転送タイプとして UDP を指定します。
[ダイジェスト認証の有効化（Enable Digest Authentication）]	このチェックボックスをオンにすると、Unified Communications Manager は、電話機からのすべての SIP 要求で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、認証または暗号化のセキュリティモードを選択します。
TFTP 暗号化（TFTP Encrypted Config）	このチェックボックスがオンの場合、Unified Communications Manager は電話機が TFTP サーバからダウンロードするファイルを暗号化します。このオプションはシスコ製電話機に限り使用できます。 **ヒント** このオプションを有効にして、対称キーを設定し、ダイジェストログイン情報と管理者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、電話セキュリティプロファイルに関連付けられているデバイスを SIP OAuthポートに登録することが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） Unified Communications Manager リリース12.5以降、Jabber デバイスは SIP OAuth 認証に対応しています。
[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 は電話機が TFTP サーバからの電話ダウンロードのダイジェストログイン情報を削除します。このオプションは、Cisco IP 電話、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、電話機がCAPF証明書の操作時に使用する認証方法を選択できます。このオプションはシスコ製電話機に限り使用できます。 ドロップダウンリストから、次のオプションのいずれかを選択します。 • **[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、セキュアな閉じた環境の場合にだけこのオプションを選択することをお勧めします。 • **[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。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 （注） [電話セキュリティ プロファイル（Phone Security Profile）] ウィ

設定	説明
	ンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
[キー サイズ（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 サイズのもう 1 つのオプションは、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、電話機でキーの生成に必要なエントロピーを生成するのに時間がかかります。キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。 （注） [電話セキュリティ プロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
SIP 電話ポート（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 Unified IP 電話（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機はこの設定を無視します。

関連トピック

設定ファイルの暗号化, on page 38
ダイジェスト認証, on page 28
SIP 電話のダイジェスト認証の設定, on page 245
暗号化された電話設定ファイルの設定, on page 231
電話セキュリティプロファイルの設定の前提条件, on page 202
詳細情報の入手先, on page 61

電話機へのセキュリティ プロファイルの適用

電話機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、特定の電話機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た証明書 (MIC) が含まれていることを確認してください。

電話機のセキュリティ機能を有効にするには、デバイス タイプとプロトコルに応じた新しいセキュリティ プロファイルを設定し、電話機に適用する必要があります。ただし、電話機に証明書が含まれていない場合は、次のタスクを実行します。

- [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。
- [電話の設定 (Phone Configuration)] ウィンドウで、capf 設定を構成することによって証明書をインストールします。
- [電話の設定 (Phone Configuration)] ウィンドウで、認証または暗号化用に設定されたデバイス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

Step 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。

Step 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。
電話機タイプとプロトコルに対してのみ設定されている電話セキュリティプロファイルが表示されます。

Step 3 [保存（Save）] をクリックします。

Step 4 該当する電話に変更を適用するには、[**設定の適用 (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、[**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。

関連トピック

Certificate Authority Proxy Function
SIP 電話のダイジェスト認証の設定, on page 245
セキュリティ プロファイルに関する詳細情報の入手先

電話機のセキュリティプロファイルと電話機の同期

電話セキュリティプロファイルに複数の電話を同期させるには、次の手順を実行します。

手順

Step 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。

Step 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。

Step 3 該当する電話機を同期する電話セキュリティプロファイルをクリックします。

Step 4 追加の設定変更を加えます。

Step 5 [保存（Save）] をクリックします。

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

Step 7 [OK] をクリックします。

関連トピック

セキュリティ プロファイルに関する詳細情報の入手先

電話セキュリティ プロファイルの削除

Unified Communications Managerでセキュリティプロファイルを削除する前に、別のプロファイルをデバイスに適用するか、該当プロファイルを使用するすべてのデバイスを削除してください。

プロファイルを使用するデバイスを確認するには、ステップ 1 を実行します。

手順

Step 1 [セキュリティプロファイルの設定（Security Profile Configuration）] ウィンドウで、[関連リンク（Related Links）] ドロップダウンリストから [依存関係レコード（Dependency Records）] を選択し、[移動（Go）] をクリックします。

依存関係レコード機能がシステムで有効になっていない場合は、**[システム] > [エンタープライズ パラメータ設定 (system Enterprise Parameters Configuration)]** に移動し、[依存関係レコードの有効化 (Enable dependency Records)] 設定を **[True]** に変更依存関係レコード機能に関連する高 CPU 使用率に関する情報がメッセージに表示されます。依存関係レコードを有効にするには、変更を保存します。依存関係レコードの詳細については、次を参照してください。Cisco Unified Communications Manager システム設定ガイド

ここでは、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。

Step 2 削除するセキュリティプロファイルを検索します。

Step 3 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ます。次に、[**Delete Selected**] をクリックします。この選択で設定可能なすべてのレコードを削除するには、[すべて選択（Select All）] をクリックして、[選択項目の削除（Delete Selected）] をクリックします。

Step 4 単一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行います。

a) [**Find And List**] ウィンドウで、適切な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ます。次に、[**Delete Selected**] をクリックします。

Step 5 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。

関連トピック

電話セキュリティプロファイルの検索, on page 203
セキュリティ プロファイルに関する詳細情報の入手先

電話機のセキュリティプロファイルを使用した電話機の検索

特定のセキュリティプロファイルを使用する電話機を検索するには、次の手順を実行します。

手順

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

Step 2 最初のドロップダウンリストから、検索パラメータ **[セキュリティプロファイル（Security Profile）]** を選択します。

a) ドロップダウンリストで、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） 追加の検索条件を追加するには、**[+]** をクリックします。条件を追加した場合、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、[-] 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] をクリックします。

Step 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、[ページあたりの行数（Rows per Page）] ドロップダウンリストで別の値を選択します。

Step 4 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

（注） ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

ウィンドウに、選択したレコードが表示されます。

関連トピック

セキュリティ プロファイルに関する詳細情報の入手先

第 12 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と非セキュア通知トーンの設定について説明します。システムは保護された電話機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、コールが暗号化されているかどうかを示します。

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。

保護されるデバイス

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 電話 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ている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 と時分割多重化（TDM）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 電話 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。[機能 (Feature)] プルダウンメニューで、[**セキュア トーン (Secure トーン)**] 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

ここでは、セキュア通知トーン機能を使用した場合の影響について説明します。

- 次に、保護されたデバイスに関する情報を示します。
  - 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。
  - 保護されていないデバイスをコールする保護されたデバイスはセキュアトーンを再生しますが、保護されていないデバイスや暗号化されていないデバイスをコールする保護されたデバイスは、セキュアでないトーンを再生します。

- 保護された電話が別の保護された電話機にコールを発信し、メディアが暗号化されていない場合、コールはドロップされません。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 電話 に表示されるロック アイコンは、メディアが暗号化されていることを示しますが、その電話が保護対象デバイスとして設定されていることを意味するわけではありません。ただし、保護された発信にはロック アイコンが表示されている必要があります。

- 次のサービスと機能が影響を受けます。

  - マルチライン補足サービス (コール転送、会議、コール待機など) は、保護対象の電話機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、保護対象の電話機では使用できません。

  - 保護されたコールでは保留/再開および不在転送がサポートされます。

- 次に、これらの情報を次に示します。

  - 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`のようになります。

  - 保護ステータスは、COCP PRI Setup、Alert、および Connect の各メッセージで独自の FacilityIE を使用して、交換用の CP E1 PRI ゲートウェイと交換されます。

  - Unified Communications Manager キーは Cisco Unified IP 電話 にだけセキュア通知トーンを再生します。ネットワーク内の PBX は、コールのゲートウェイ側にトーンを再生します。

  - Cisco Unified IP 電話 と MGCP E1 PRI ゲートウェイの間のメディアが暗号化されていないと、コールはドロップされます。

（注） メディア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に対応した『 *Cisco IOS* のメディアおよびシグナリングの認証と暗号化機能』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**] チェックボックスをオンにします (ウィンドウの [**device Information**] 部分にもあります)。
  - [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]**）。
- [**電話の設定 (Phone configuration**)] ウィンドウで電話番号を追加したときに表示される [電話番号の設定 **(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。
  - [コールの最大数（Maximum Number of Calls）]
  - [ビジー トリガー（Busy Trigger）]
- [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番目の**サービスパラメータ設定**ウィンドウで、クラスタ**全体のパラメータ (機能セキュアトーン)**エリアを見つけ、[**セキュア通知トーンを再生 (Play Secure**インジケータ)] 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。[**ゲートウェイの設定 (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。
  - 残りの設定を完了したら、[**保存 (Save)**] をクリックします。次に、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 (endpoint)] 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 電話 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 13 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の設定への暗号化について説明します。この機能を使用すると、アナログ電話のセキュアな SCCP 接続を Cisco VG2xx ゲートウェイに作成できます。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。

- アナログ電話セキュリティプロファイル（229 ページ）
- セキュアなアナログ電話の証明書管理（229 ページ）

アナログ電話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、デバイスセキュリティモードのパラメータを [**認証済み (Authenticated)**] または [**暗号化 (encrypted)**] に設定したアナログ電話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。

関連トピック

電話セキュリティ プロファイルの設定, on page 201

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 14 章

暗号化された電話設定ファイルの設定

この章では、暗号化された電話機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を行った後、電話機の設定ファイルには、ダイジェストパスワードや電話管理者パスワードなどの機密情報が含まれています。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

TFTP 設定は、電話機が登録プロセスを実行する際に TFTP サーバから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、デバイスの登録プロセス中にデータを保護します。このファイルには、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 ログイン情報などの機密情報が含まれます。この機能が設定されていない場合、設定ファイルはクリアテキストで送信されます。この機能を導入すると、登録プロセス中に攻撃者がこの情報を傍受できなくなります。この情報は暗号化解除され、クリアテキストで送信されます。したがって、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。

警告 SIP 電話でダイジェスト認証オプションを有効にし、TFTP で暗号化設定オプションを無効にした場合は、ダイジェストログイン情報がクリアテキストで送信されます。

TFTP の設定後、TFTP サーバは次の手順を実行します。

- ディスク上のクリアテキストの設定ファイルをすべて削除します
- 暗号化されたバージョンのコンフィギュレーションファイルを生成します。

電話機が暗号化された電話設定ファイルをサポートし、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、電話機は設定ファイルの暗号化バージョンを要求します。

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ません。電話機のモデルとプロトコルによって、コンフィギュレーションファイルを暗号化するためにシステムが使用する方法が決定されます。サポートされる方式は、Unified Communications Manager の機能と、暗号化された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暗号化されていない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。

暗号化キーの配布

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を推奨します。

Unified Communications Manager は、次の方式をサポートします。

- 手動キー配布
- 電話の公開キーによる対称キーの暗号化

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 暗号化設定（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。

関連トピック

手動キー配布, on page 232
電話機の公開キーによる対称キーの暗号化, on page 233
電話機モデルのサポート, on page 191
暗号化された TFTP 設定ファイルの無効化, on page 243

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。キーがデータベースに存在する場合、管理者またはユーザは電話機のユーザインターフェイスにアクセスして、電話にキーを入力する必要があります。[**承認 (Accept)**] ソフトキーを押すとすぐに、電話機はフラッシュにキーを保存します。キーを入力すると、電話機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。必要なタスクが発生すると、対称キーは RC4 または AES 128 暗号化アルゴリズムを使用してコンフィギュレーションファイルを暗号化します。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機モデル（234 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コンフィギュレーションファイルの署名者が検証されるわけではありません。

電話機は、フラッシュに保存されている対称キーを使用して、ファイルの内容を復号化します。復号化に失敗した場合、設定ファイルは電話機に適用されません。

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。

関連トピック

電話機モデルのサポート, on page 191

電話機の公開キーによる対称キーの暗号化

電話機に製造元でインストールされる証明書 (MIC) またはローカルで有効な証明書 (LSC) が含まれている場合、電話機にはPKI暗号化に使用される公開キーと秘密キーのペアが含まれています。

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。電話機が問題を特定しない場合、電話機がリセットされた後、電話機は TFTP サーバから暗号化された設定ファイルを要求します。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 電話 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存在し、電話機がリセットされると、データベースが TFTP に電話機の公開キーが存在することを通知した後に、対称キー暗号化プロセスが開始されます。TFTP サーバは、Advanced Encryption Standard (AES) 128 暗号化アルゴリズムを使用してコンフィギュレーションファイルを暗号化する 128 ビットの対称キーを生成します。次に、電話の公開キーによって対称キーが暗号化されます。このキーには、コンフィギュレーションファイルの署名付きエンベロープヘッダーが含まれています。電話機はファイルの署名を検証し、署名が有効であれば、電話機は 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します。対称キーは、ファイルの内容を復号化します。

コンフィギュレーションファイルを更新するたびに、TFTP サーバは自動的に新しいキーを生成してファイルを暗号化します。

ヒント この暗号化方式をサポートする電話の場合、電話機はコンフィギュレーションファイルの暗号化設定フラグを使用して、暗号化または暗号化されていないファイルを要求するかどうかを決定します。[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 電話が暗号化ファイル（.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、電話機は暗号化されていない署名されたファイル (...) を要求します。

TFTP 暗号化設定が有効になっていても、電話機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した場合、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。エラー状態が解決された場合、電話機は、次回のリセット時に暗号化された設定ファイルを要求します。

関連トピック

Certificate Authority Proxy Function について
電話機モデルのサポート, on page 191

暗号化をサポートする電話機モデル

次のCisco Unified IP 電話 の電話機設定ファイルを暗号化できます。

電話機のモデルとプロトコル	[暗号化方式（Encryption Method）]
Cisco Unified IP 電話 7800 または 6921	手動キー配布: 暗号化アルゴリズム: RC4Key サイズ: 256 ビット ファイル署名のサポート: いいえ
Cisco Unified IP 電話 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) 128Key サイズ：128 ビット ファイル署名のサポート: SIP を実行している電話機は、署名された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。

電話機のモデルとプロトコル	[暗号化方式（Encryption Method）]
Cisco Unified IP 電話 6901、6911、6921、6941、6945 および 6961 Cisco Unified IP 電話 79 g、Cisco Unified IP 電話 7961g、7961G、または 7965G;Cisco Unified IP 電話 79 41G、79 42g、または 7945G;Cisco Unified IP 電話 7911G;Cisco Unified IP 電話 の 79 06g Cisco Unified IP 電話 、7961G-GE、7941G-GE Cisco Unified IP 電話 7931G, (SCCP のみ) Cisco Unified ワイヤレス IP 電話 7925G, 7925G-EX, 7926G Cisco Unified IP 電話 8941 および 8945 Cisco Unified IP 電話 8961、9951、および 9971 Cisco IP 電話 7811、7821、7841、7861 Cisco IP 会議用電話 7832 Cisco IP 電話s 8811、8841、8845、8851、8851NR、8861、8865、および 8865NR Cisco Unified IP 会議用電話 8831 Cisco 会議用電話 8832 Cisco ワイヤレス IP 電話 8821	電話機の公開キーによる対称キーの暗号化：暗号化アルゴリズム：AES128Key サイズ：128 ビット ファイル署名のサポート: はい （注） Cisco Unified IP 電話 6901 および6911 は、デフォルトでは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 電話 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 電話（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

電話機のダウンロードで機密データを保護するには、TFTP暗号化設定ファイルを有効にすることをお勧めします。電話に PKI 機能がない場合、[Unified Communications Manager Administration] と電話で対称キーも設定する必要があります。対称キーが電話機または Unified Communications Managerのいずれかに存在しない場合、またはTFTP暗号化設定ファイルの設定時に不一致が発生した場合、電話機は登録できません。

Unified Communications Manager で暗号化された設定ファイルを設定する場合は、次の点を考慮してください。

- 暗号化された設定ファイルをサポートしている電話機にのみ、[電話機のセキュリティプロファイルの設定（Phone Security Profile Configuration）] ページ)に [TFTP 暗号化設定（TFTP Encrypted Config）] チェックボックスが表示されます。暗号化された設定ファイルを Cisco Unified IP 電話 の 7800、7942、および 7962（SCCP のみ）に設定することはできません。これらの電話機は設定ファイルのダウンロードで機密データを受信しないからです。

- デフォルトでは、[TFTP 暗号化設定（TFTP Encrypted Config）] チェックボックスはオフになっています。このデフォルト設定、非セキュアプロファイルを電話機に適用した場合、ダイジェストログイン情報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 Unified IP 電話 の場合、Unified Communications Manager では [デバイスセキュリティモード（Device Security Mod）] を [認証済み (Authenticated)] または [暗号化(Encrypted)] に設定して暗号化された設定ファイルを有効にする必要はありません。Unified Communications Manager は、登録中の公開鍵をダウンロードするために CAPF プロセスを使用します。
- 環境が安全である場合や、PKI が有効になっていない電話機に対称キーを手動で設定しないようにする場合は、暗号化されていない設定ファイルを電話機にダウンロードできます。ただし、この方法を使用することはお勧めしません。
- Cisco Unified IP 電話 の 7800、7942、および 7962（SIP のみ）では、Unified Communications Manager は暗号化された設定ファイルを使用するよりも簡単で、安全性が低いダイジェストログイン情報を電話機に送信する方法を提供します。[ダイジェストログイン設定ファイルを除外（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、ダイジェストログイン情報の初期化に役立ちます。この方法では、暗号化されていないコンフィギュレーションファイルで、電話機にダイジェストクレデンシャルを送信します。ログイン情報が電話機に入力された後は、[TFTP 暗号化設定（TFTP Encrypted Config）] オプションを無効にしてから、[電話機のセキュリティ プロファイルの設定（Phone Security Profile Configuration）] ページの [設定ファイルのダイジェストクレデンシャルを除外する（Exclude Digest Credential in Configuration File）] を有効にすることをお勧 めします。これにより、今後のダウンロードからダイジェストログイン情報が除外されます。
- ダイジェストログイン情報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ログイン情報が含まれないようになると、既存のログイン情報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、電話機が工場出荷時の状態にリセットされるか、または新しいクレデンシャル (空白を含む) を受信するまで、そのまま残ります。電話機またはエンドユーザのダイジェストログイン情報を変更する場合は、対応する [電話機のセキュリティプロファイル情報（Phone Security Profile Information）] ページの [設定ファイルでのダイジェストログイン情報の除外（Exclude Digest Credential in Configuration File）] を一時的に無効にして、新しいダイジェストログイン情報を電話機にダウンロードします。

電話機の設定ファイルの暗号化のタスクフロー

TFTP 設定ファイルの暗号化を設定するには、クラスタのセキュリティが混合モードで設定されていることを確認し、手動キー暗号化と公開キー暗号化をサポートするクラスタ内の電話機を確認し、SHA-1 と SHA-512 をサポートする電話機を確認し、以下のタスクを完了します。

（注） SHA-512 クラスタ全体を有効にし、電話機がサポートしていない場合、これらの電話機は機能しません。

手順

	コマンドまたはアクション	目的
Step 1	TFTP 暗号化の有効化 （237 ページ）	電話機の [TFTP 設定ファイル (TFTP Configuration File)] オプションを有効にします。電話セキュリティプロファイルでこのオプションを有効にすることができます。
Step 2	SHA-512 署名アルゴリズムの設定 （238 ページ）	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。より強力な SHA-512 アルゴリズムを使用するようにシステムを更新するには、次の手順を使用します。
Step 3	LSC または MIC 証明書のインストールの確認 （241 ページ）	公開キーを使用する電話機の場合は、証明書のインストールを確認します。
Step 4	CTL ファイルの更新 （242 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。
Step 5	サービスの再起動 （242 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。
Step 6	電話のリセット （243 ページ）	暗号化されたTFTP設定ファイルの更新が完了したら、電話機をリセットします。

TFTP 暗号化の有効化

この TFTP 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。TFTP サーバからダウンロードするファイルのTFTP暗号化を有効にするには、次の手順を実行します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[システム（System）] > [セキュリティ（Security）] > [電話セキュリティプロファイル（Phone Security Profile）]**

Step 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。

Step 3 **[TFTP Encrypted Config]** チェックボックスをオンにします。

Step 4 [保存（Save）] をクリックします。

Step 5 クラスタで使用されている他のすべての電話セキュリティプロファイルに対して、これら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、 Cisco Unified Communications Manager Administrationの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して、変更内容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。次のオプションの手順を使用して、デジタル署名などの TFTP 設定ファイルにより強力な SHA-512 アルゴリズムを使用するようにシステムをアップグレードできます。

（注） ご使用の電話機が SHA-512 をサポートしていることを確認してください。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。

手順

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

Step 2 [セキュリティパラメータ（Security Parameters）] ペインに移動します。

Step 3 [**TFTP File Signature Algorithm**] ドロップダウンリストから、[**SHA-512**] を選択します。

Step 4 [保存（Save）] をクリックします。

この手順を完了するには、ポップアップウィンドウに一覧表示されている影響を受けるサービスを再起動します。

手動キー配布の設定

手動キーを使用する電話機の場合は、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。
- お使いの電話機は、手動キー配布をサポートしています。

手順

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

Step 2 [検索（Find）] をクリックします。

Step 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） 設定を行った後は、キーを変更しないようにしてください。

Step 4 [保存（Save）] をクリックします。

Step 5 電話機に対称キーを入力し、電話機をリセットします。

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 *32 :* 手動キー配布の構成時の設定

設定	説明
[対称キー（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 電話 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 キーが設定された後は、変更しないようにしてください。
[文字列を生成（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。
[データベース値を復元（Revert to Database Value）]	データベース内の値を復元する場合は、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で電話機の手動キーを設定した場合は、次の手順を使用して電話機にキーを入力します。

手順

Step 1 電話の [Setting] ボタンを押します。

Step 2 設定がロックされている場合は、[**設定 (Settings)**] メニューを下にスクロールして、[**電話のロック解除 (Unlock Phone)**] を強調表示し、 **[選択**電話機のパスワードを入力し、[**承認 (Accept)**] ソフトキーを押します。

電話機はパスワードを受け入れます。

Step 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。

Step 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。

Step 5 暗号キーの入力を求められたら、キー (16 進数) を入力します。キーをクリアする必要がある場合は、32のゼロの数字を入力します。

Step 6 キーの入力が完了したら、[**承認 (Accept)**] ソフトキーを押します。

電話機は暗号キーを受け入れます。

Step 7 電話機をリセットします。

電話機がリセットされると、電話機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機の場合は、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 電話に適用されます。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モデル」の項を参照して

次の手順は、電話機が Unified Communications Manager データベースに存在し、Unified Communications Manager で [TFTP 暗号化設定（TFTP Encrypted Config）] パラメータを有効にしていることを前提としています。

手順

Step 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。

Step 2 [Cisco Unified CM Administration] から、**[デバイス（Device）] > [電話機（Phone）]** の順に選択します。
電話機のリストが表示されます。

Step 3 [デバイス名（Device Name）] をクリックします。
[電話の設定（Phone Configuration）] ページが表示されます。

ヒント **[電話の設定（Phone Configuration）]** ページの [CAPF 設定（CAPF settings）] セクションで **[トラブルシュート（Troubleshoot）]** オプションを選択して、Unified Communications Managerの電話機に LSC または MIC が存在するかどうかを確認します。証明書が電話機に存在しない場合、[削除（Delete）] および [トラブルシュート（Troubleshoot）] オプションは表示されません。

ヒント　電話機のセキュリティ設定を確認することによって、電話機に LSC または MIC が存在することを確認することもできます。詳細については、 Unified Communications Manager のこのバージョンをサポートするCisco Unified IP 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。

Step 4　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、Certificate Authority Proxy Function に関連するトピックを参照してください。

Step 5　CAPF を設定したら、[保存（Save）] をクリックします。

Step 6　[リセット（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

Unified Communications Manager の変更を行った後、CTL ファイルを更新します。TFTP ファイル暗号化を有効にしているので、CTL ファイルを再生成する必要があります。

手順

Step 1　コマンドライン インターフェイスにログインします。

Step 2　パブリッシャ ノードで **utils ctl update CTLfile** コマンドを実行します。

サービスの再起動

暗号化された TFTP 設定ファイルの更新を完了したら、Cisco TFTP サービスと Cisco CallManager サービスを再起動して変更を有効にしてください。

手順

Step 1　[Cisco Unified Serviceability] から選択します。**[ツール（Tools）] > [コントロールセンター - 機能サービス（Control Center - Feature Services）]**

Step 2　次の 2 つのサービスを選択します。

- Cisco CallManager
- Cisco TFTP

Step 3　[再起動（Restart）] をクリックします。ただし、CallManager 証明書を再生成または更新した後は、TFTP サービスを手動で再起動する必要はありません。

電話のリセット

すべての暗号化されたTFTP設定ファイルの更新が完了したら、電話機をリセットしてください。

手順

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

Step 2 [検索（Find）] をクリックします。

Step 3 [すべて選択（Select All）] をクリックします。

Step 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

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、ダイジェストログイン情報がクリアテキストで送信される可能性があります。

設定を更新した後、電話機の暗号キーは Unified Communications Manager データベースに残ります。

Cisco Unified IP 電話7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、 7962G、7965G、 および 7975G は暗号化ファイル（.enc、.sgn ファイル）を要求します。暗号化設定が **False** に更新された場合は、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 電話 は、SCCP および SIP 上で実行されている場合に、暗号化設定が **False**に更新されると、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、電話の GUI から対称キーを削除します。

- Cisco Unified IP 電話SCCP で実行される Cisco Unified IP 電話 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。
- Cisco Unified IP 電話SIP で実行される Cisco Unified IP 電話 は、6901、6911、6921、6941、6945、6961、7906G、7911G、7941G、7941G-GE、7942G、7961G、7961G、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。

手順

	コマンドまたはアクション	目的
Step 1	電話機設定ファイルの暗号化を無効にするには、電話機に関連付けられている電話機の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ます。	
Step 2	Cisco Unified IP 電話 7942 および 7962（SIP のみ）の場合は、電話画面で対称キーのキー値として「32-byte 0」を入力して暗号化を無効にします。	
Step 3	Cisco Unified IP 電話（SIP のみ）の場合は、電話画面で対称キーを削除して暗号化を無効にします。	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

初期設定後に電話機に送信される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、電話機に適用され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 電話 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の変更のコンフィギュレーションファイルを更新するには、このチェックボックスをオフにする必要があります。

関連トピック

暗号化された TFTP 設定ファイルのヒント, on page 235
暗号化された電話ファイルのセットアップに関する詳細情報の入手先

第 15 章

SIP 電話のダイジェスト認証の設定

この章では、SIP 電話のダイジェスト認証の設定について説明します。SIP を実行している電話でダイジェスト認証がどのように機能するダイジェスト認証 （28 ページ）かの詳細については、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でのダイジェスト認証の有効化

電話セキュリティプロファイルを使用して電話のダイジェスト認証を有効にするには、次の手順を実行します。

手順

Step 1 [Cisco Unified CM 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。

Step 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。

Step 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。

Step 4 [保存（Save）] をクリックします。

関連トピック

電話セキュリティ プロファイルの設定, on page 201
SIP ステーションレルムの設定, on page 246
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, on page 247
エンドユーザのダイジェストクレデンシャルの設定, on page 247
電話機へのダイジェスト認証の割り当て, on page 248

SIP ステーションレルムの設定

401の不正なメッセージへの応答でSIP電話がチャレンジされた場合に、Cisco Unified Communications Managerが使用する文字列を[レルム (Realm)]フィールドに割り当てます。これは、電話機がダイジェスト認証用に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

Step 1 Unified Communications Managerから、**[System（システム）] > [Service Parameters（サービスパラメータ）]** を選択します。

Step 2 **[サーバ（Server）]** ドロップダウンリストから、CiscoCallManager サービスをアクティブ化したノードを選択します。

Step 3 **[サービス（Service）]** ドロップダウンリストから、CiscoCallManager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。

Step 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のリンクをクリックします。

Step 5 [保存（Save）] をクリックします。

関連トピック

ダイジェスト認証に関する詳細情報の入手先

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

この手順を使用して、電話を所有しているエンドユーザにダイジェストログイン情報を割り当てます。電話機は、ログイン情報を使用して認証します。

手順

Step 1 Cisco Unified Communications Manager Administration で、**[ユーザ管理（User Management）] > [エンドユーザ（End User）]** を選択します。

Step 2 [検索 **(Find)**] をクリックして、電話を所有しているエンドユーザを選択します。

Step 3 次のフィールドにクレデンシャルを入力します。

- ダイジェスト クレデンシャル（Digest Credentials）
- [ダイジェストクレデンシャルの確認（Confirm Digest Credentials）]

Step 4 [保存（Save）] をクリックします。

関連トピック

エンドユーザのダイジェストクレデンシャルの設定, on page 247
ダイジェスト認証に関する詳細情報の入手先

エンドユーザのダイジェストクレデンシャルの設定

ダイジェストログイン情報の詳細を表示するには、次の手順を実行します。

Cisco Unified Communications Manager の管理ページから、[ユーザ管理（User Management）] > [エンドユーザ（End User）] を選択し、[ユーザ ID（User 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)]** ペインで使用できます。

表 ***33 :*** ダイジェスト クレデンシャル（***Digest Credentials***）

設定	説明
ダイジェスト クレデンシャル（Digest Credentials）	英数字の文字列を入力します。

設定	説明
[ダイジェストクレデンシャルの確認（Confirm Digest Credentials）]	[ダイジェストクレデンシャル（Digest Credentials）] の入力が正しいことを確認するために、このフィールドに再度クレデンシャルを入力します。

関連トピック

電話機へのダイジェスト認証の割り当て, on page 248

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とダイジェスト認証に対応した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

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

Step 2 **[検索 (Find)]** をクリックして、ダイジェスト認証を割り当てる電話を選択します。

Step 3 **[ダイジェストユーザ (Digest User)]** ドロップダウンリストから、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。

Step 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から割り当てられていることを確認します。

Step 5 [保存（Save）] をクリックします。

Step 6 [リセット（Reset）] をクリックします。

エンドユーザを電話機に関連付けた後、設定を保存し、電話機をリセットします。

関連トピック

ダイジェスト認証に関する詳細情報の入手先

第 16 章

電話のセキュリティ強化

この章では、電話機のセキュリティ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

デフォルトでは、 Cisco Unified IP 電話 s は 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をスプーフィングすることができます。たとえば、攻撃者は、デフォルトルータであると主張するパケットを送信する可能性があります。これを選択した場合は、[**電話の設定 (Phone Configuration)**] ウィンドウで、無償 ARP を無効にすることができます。

（注） この機能を無効にしても、電話機がデフォルトルータを特定することはできません。

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 サービスが無効になっているかどうかを確認するために、電話機は設定ファイルのパラメータを解析して、サービスが無効になっているか、有効になっているかを示します。Web サービスが無効になっている場合、電話機はモニタリング目的で HTTP ポート80を開かず、電話機の内部 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 電話 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 電話 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 電話 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。

アクセスの無効化の設定

デフォルトでは、Cisco IP 電話 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 [音量 (Volume)] ボタンに関連付けられている設定を保存できません。たとえば、ユーザはボリュームを保存できません。

この設定を無効にすると、現在のコントラスト、呼出音タイプ、ネットワーク設定、モデル情報、ステータス、および電話機に存在するボリューム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 ポートのディセーブル化

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 電話 で PC ポートを有効にします。これを選択した場合は、[電話の設定 (Phone Configuration)] ウィンドウで [PC ポート (PC Port)] 設定を無効にすることができます。PC ポートを無効にすると、ロビーまたは会議室の電話機で役立ちます。

（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

電話のセキュリティ強化は、接続のセキュリティを強化するために電話機に適用できるオプションの設定で構成されています。次の 3 つの設定ウィンドウのいずれかを使用して設定を適用できます。

- 電話の設定 - [電話の設定（Phone Configuration）] ウィンドウを使用して、個々の電話に設定を適用します。
- 共通の電話プロファイル - [共通の電話プロファイル（Common Phone Profile）] ウィンドウを使用して、このプロファイルを使用するすべての電話機に設定を適用します。
- 企業電話 - [企業電話（Enterprise Phone）] ウィンドウを使用して、企業全体のすべての電話機に設定を適用します。

（注） これらの各ウィンドウに競合する設定が表示される場合、電話が正しい設定を判断するために使用する優先順位は次のとおりです。1) 電話の設定、2) 共通の電話プロファイル、3) 企業電話。

電話のセキュリティ強化を設定するには、次の手順を実行します。

手順

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

Step 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。

Step 3 デバイス名をクリックします。

Step 4 次の製品固有のパラメータを見つけます。

a) [PC ポート（PC Port）]
b) [設定アクセス（Settings Access）]
c) [無償 ARP（Gratuitous ARP）]
d) [PC の音声 VLAN へのアクセス（PC Voice VLAN Access）]
e) [Web アクセス（Web Access）]

ヒント これらの設定の情報を確認するには、**[電話の設定 (Phone Configuration)]** ウィンドウのパラメータの横に表示される [ヘルプ (help)] アイコンをクリックします。

Step 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。スピーカフォンまたはスピーカ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。

Step 6 [保存（Save）] をクリックします。

Step 7 [リセット（Reset）] をクリックします。

関連トピック

電話機のセキュリティ強化に関する詳細情報の入手先, on page 252

電話機のセキュリティ強化に関する詳細情報の入手先

関連トピック

Gratuitous ARP の無効化, on page 249
Web アクセスの無効化, on page 249
PC 音声 VLAN へのアクセスの無効化, on page 250
アクセスの無効化の設定, on page 250
PC ポートのディセーブル化, on page 250

第 17 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。会議は、すべての参加デバイスが暗号化されたシグナリングとメディアを持っている場合、セキュアと見なされます。セキュアな会議機能は、セキュアな TLS または IPSec 接続を介した SRTP 暗号化をサポートします。

システムには、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。これは、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って決定されます。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には、認証済みの会議セキュリティステータスがあります。

セキュアなアドホック会議と会議室の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。会議ブリッジが使用できない場合、コールは失敗します。

会議コールの場合、会議を開始する電話機は、会議番号に設定されている最小のセキュリティ要件を満たしている必要があります。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、割り込みコールで接続されているすべての通話者に対して会議のセキュリティ ステータスを提供します。

（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 電話 は暗号化済みコールに割り込めるようになりました。

関連トピック

最小セキュリティレベルの会議の開催, on page 258

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なコーデックは、ルータごとに許可される同時のセキュアな会議の最大数を提供します。送信ストリームと受信ストリームは、参加している各エンドポイントに個別にキーが割り当てられるため (参加者が会議を退室したときにキー再生成は必要ありません)、DSP モジュールの合計セキュア会議容量は、非セキュアな容量の1分に相当します。を設定できます。

『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

セキュアな会議アイコン

Cisco IP 電話 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、電話機のユーザマニュアルで説明されているように、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。

コールの音声およびビデオ部分によって、会議のセキュリティレベルの基準が提供されます。音声とビデオの両方の部分がセキュアである場合にのみ、コールはセキュアと見なされます。

アドホックおよび会議のセキュアな会議では、会議の参加者の電話ウィンドウの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、会議ブリッジと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、会議のすべての参加者が暗号化されている場合は、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、会議のすべての参加者が認証されている場合は、シールドアイコンが表示されます。一部の電話機モデルでは、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、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。または、一部の古い電話機モデルでは、アイコンが表示されません。

（注） 「コールセキュリティステータスを指定した場合の BFCP アプリケーション暗号化ステータスのオーバーライド」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場合に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。

暗号化された電話機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が暗号化されます。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、または非セキュアにすることができます。非セキュアステータスは、いずれかの当事者がセキュアでないか、または検証できないことを示します。

ユーザが [割り込み (割り込み)] を押すと、[割り込み (割り込み)] ソフトキーの横に表示されるアイコンによって割り込み会議のセキュリティレベルが提供されます。割り込みデバイスと割り込まれたデバイスが暗号化をサポートしている場合、システムは2つのデバイス間でメディアを暗号化しますが、接続されている通話者のセキュリティレベルに応じて、割り込み会議のステータスは非セキュア、認証済み、または暗号化済み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、参加者が会議に出入りしたときに変更できます。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、認証済みまたは非セキュアのセキュリティレベルに戻ることができます。同様に、認証済みまたは非セキュアな参加者がコールを切断した場合、ステータスはアップグレードされます。非セキュアな参加者が電話会議に接続すると、その会議は非セキュアとしてレンダリングされます。

会議の状態は、参加者が会議をチェーンするとき、チェーン会議のセキュリティステータスが変更されたとき、別のデバイスで保留中の会議コールが再開されたとき、会議コールが割り込まれたしたとき、または転送されたときに変更することもできます。会議コールは別のデバイスに対して完了します。

（注） Advanced Ad Hoc 会議が有効になっているサービスパラメータは、会議、参加、直接転送、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の会議の開催

関連トピック

アドホック会議のリスト, on page 257
最小セキュリティレベルの会議の開催, on page 258

アドホック会議のリスト

会議コール中にConfListソフトキーを押すと、参加している電話機に会議リストが表示されます。会議のリストには、会議のステータスと各参加者のセキュリティステータスが表示され、暗号化されていない参加者を識別します。

会議リストには、非セキュア、認証済み、暗号化済み、保留中のセキュリティアイコンが表示されます。会議の開始者は、会議リストを使用して、セキュリティステータスが低い参加者を退出させることができます。

（注） 高度なアドホック会議の有効化サービスパラメータは、会議の開催者以外の会議参加者が会議参加者を追放できるかどうかを決定します。

参加者が会議に参加すると、会議リストの先頭に追加されます。ConfList および RmLstC ソフトキーを使用してセキュアな会議から非セキュアな参加者を削除するには、お使いの電話機のユーザマニュアルを参照してください。

ここでは、他の機能とのセキュアなアドホック会議の相互作用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した場合は、割り込みターゲットの横にある会議リストに割り込みコールのセキュリティステータスが表示されます。割り込みの発信者には認証済みの接続があるため、割り込みターゲットと会議ブリッジの間でメディアが暗号化されている場合、割り込みターゲット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。

割り込みターゲットがセキュアだが非セキュアなアドホック会議では、アドホック会議のステータスが [セキュア (secure)] に変わると、[割り込み発信者 (割り込み caller)] 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ユーザは、 Cisco Unified IP 電話 (sccp を実行している電話機のみ) で [参加 (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参加できま

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。参加している新しいメンバーを追加した参加者は会議の開催者になり、会議リストから新しいメンバーまたは他の参加者を取り出します (高度なアドホック会議が有効になっている設定が True の場合)。

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会議コールを保留にすると、追加された参加者がコールに応答するまで、会議のステータスは [不明 (unknown)] (非セキュア) のままになります。新しい参加者が応答すると、会議リストの会議ステータスが更新されます。

共有回線の発信者が別の電話で開催中の会議コールを再開すると、発信者が [再開 (Resume)] を押すと会議リストが更新されます。

最小セキュリティレベルの会議の開催

管理者は、ミーティングのパターンまたは番号を非セキュア、認証済み、または暗号化済みとして設定するときに、会議の最小セキュリティレベルを指定できます。参加者は最小のセキュリティ要件を満たしている必要があります。または、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、会議コールの転送、共有回線での会議コールの再開、およびチェーン会議に適用されます。

会議室の会議を開始する電話機が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。一致しない場合、システムはその試行を拒否します。最小セキュリティレベルで認証済みまたは暗号化済みが指定されていて、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として非セキュアを指定した場合、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、他の機能とのセキュアな会議の連携動作について説明します。

会議とアドホック会議

会議をアドホック会議に追加したり、会議にアドホック会議を追加したりするには、アドホック会議が会議の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。または、コールがドロップされます。会議アイコンは、会議が追加されたときに変更されることがあります。

ミートミー会議と割り込み

発信者が会議参加者を割り込むときに、割り込みの発信者が最小のセキュリティ要件を満たしていない限り、割り込まれたデバイスのセキュリティレベルがダウングレードし、割り込みの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。

会議の開催と保留/再開

電話機が最小セキュリティレベルを満たしていない限り、共有回線上の電話機が会議の開催を再開することはできません。電話機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 [再開 (Resume)] 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。

関連トピック

ミートミー会議の最小セキュリティ レベルの設定, on page 266

Cisco Unified IP 電話 セキュアな会議とアイコンのサポート

これらのCisco Unified IP 電話はセキュアな会議とセキュアな会議のアイコンをサポートしています。

- Cisco Unified IP 電話 7942 および 7962（SCCP のみ、認証済みセキュア会議のみ）
- Cisco Unified IP 電話 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 電話 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 電話 7811、7821、7841、7861、Cisco IP電話 7832、Cisco IP 電話 8811、8841、8845、8851、8851NR、8861、8865、8865nr、Cisco ワイヤレス IP 電話 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 電話 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された電話は、これらの新機能を完全にはサポートしていません。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 電話 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 電話 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* 電話 の管理ガイド および *Cisco IP* 電話 ユーザ ガイドを参照してください。

関連トピック

[Restrictions（機能制限）], on page 11

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。

トランクとゲートウェイを介したセキュアな会議

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 トランクが含まれている場合、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、オフクラスタ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、電話機の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 ステータスを提供します。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

この項では、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（260 ページ）
• セキュアな会議による Cisco Unified Communications Manager の制約事項（261 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。

- 会議を安全に保つために、セキュアなアドホック会議の参加者がコールを保留にするか、コールをパークする場合、[MOH を会議ブリッジに抑制 (hold MOH to call 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。セキュアな会議のステータスは変更されません。
- 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、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が unknown に変わります。クラスタ外の参加者が MOH を使用して保留中の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ることがあります。
- クラスタ間トランク (ICT) を介したセキュアな MeetMe コールは、リモートユーザが保留/再開などの電話機能を起動し、メディアステータスが unknown に変更されたかどうかをクリアします。
- 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、RSVP が有効になっている場合、会議はセキュアなままになります。
- PSTN を含む電話会議の場合、セキュリティ会議アイコンには、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が表示されます。
- Maximum Call Duration Timer サービスパラメータは、会議の最大継続時間も制御します。
- 会議ブリッジはパケットキャプチャをサポートしています。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、電話機には会議の非セキュアステータスが表示されます。
- システムに設定されているメディアセキュリティポリシーによって、セキュアな会議の動作が変更されることがあります。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、エンドポイントはシステム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を使用します。

セキュアな会議による Cisco Unified Communications Manager の制約事項

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 電話 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 電話 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 電話 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 電話 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 電話の 79 31g は、会議のチェーンをサポートしていません。
- SIP トランクを介してコールしている電話は、デバイスのセキュリティステータスに関係なく、非セキュアな電話機として扱われます。
- セキュアな電話機が SIP トランクを介してセキュアな会議に参加しようとすると、コールはドロップされます。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の会議リストは表示されません。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会議ソフトキーの横に表示されます。たとえば、h.323 ICT 接続の場合、認証アイコンは表示されません (システムは認証された接続を非セキュアとして扱う) が、暗号化された接続の暗号化アイコンが表示されます。

  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者間コールとして扱います。

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、次の情報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機で表示する場合は、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は、会議コールを保護するために暗号化をサポートする必要があります。
- セキュアな会議ブリッジの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調達するために、会議を開始する電話機が認証または暗号化されていることを確認します。

- 共有回線で会議の整合性を維持するには、異なるセキュリティモードで回線を共有するデバイスを設定しないでください。たとえば、認証済みまたは非セキュアな電話機を使用して回線を共有するように暗号化された電話機を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する場合は、SIP トランクを ICTs として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 Subject 属性で指定された共通名は、Cisco Unified Communications Manager で定義された会議ブリッジ名から開始し、関連付け**プロファイル < プロファイル識別子 > register < device Name >?**コマンドを使用して DSP ファームシステムで指定する必要があります。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 ファームシステム上に複数のセキュアな会議ブリッジがある場合、それぞれに個別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 CiscoCallManager 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

次の手順では、ネットワークにセキュアな会議を追加するために使用するタスクについて説明します。

手順

Step 1 CiscoCTL クライアントが混合モードにインストールされ、設定されていることを確認します。

Step 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に設定します。

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。

Step 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 CiscoCallManager 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CiscoCallManager サービスを再起動する必要があります。

Step 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。

Step 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。

Step 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、階層をSRTPにキャプチャします。

関連トピック

Cisco CTL クライアントの設定, on page 113
会議リソースの保護のヒント, on page 262
ミートミー会議の最小セキュリティ レベルの設定, on page 266
セキュアな会議ブリッジのパケット キャプチャの設定, on page 267
Cisco Unified Communications Manager Administration でのセキュアな会議ブリッジの設定, on page 265

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、CiscoCallManager 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

Step 1　**[Media Resources]** > **[Conference Bridge]** を選択します。

Step 2　[会議ブリッジの検索と一覧表示] ウィンドウで、Cisco IOS Enhanced 会議ブリッジがインストールされてセキュアな会議ブリッジのセットアップ（264 ページ）いることを確認し、に進みます。

Step 3　デバイスがデータベースに存在しない場合は、[新規追加 **(Add New)**] をクリックします。にCisco Unified Communications Manager Administration でのセキュアな会議ブリッジの設定（265 ページ）進みます。

Step 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、会議ブリッジの名前、説明、デバイスプール、共通デバイス設定、およびロケーション設定を構成します。

Step 5　[Device Security Mode] フィールドで、[**Encrypted 会議ブリッジ**] を選択します。

Step 6　[保存（Save）] をクリックします。

Step 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。

関連トピック

セキュアな会議リソースに関する詳細情報の入手先, on page 267

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

Step 1 **[Call Routing]** > **[Meet-Me Number/Pattern]** を選択します。

Step 2 [会議ブリッジの検索/一覧表示 (Find and List bridge bridge)] ウィンドウで、会議番号/パターンセキュアな会議ブリッジのセットアップ（264 ページ）が設定されていることを確認し、に進みます。

Step 3 Meet a の番号/パターンが設定されていない場合は、**[新規追加 (Add New)]** をクリックします。にミートミー会議の最小セキュリティ レベルの設定（266 ページ）進みます。

Step 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、説明とパーティションの設定を行います。

Step 5 [Minimum Security Level] フィールドで、[**Non Secure**]、[**Authenticated**]、または [**Encrypted**] を選択します。

Step 6 [保存（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。

関連トピック

Cisco Unified Communications Manager Administration でのセキュアな会議ブリッジの設定, on page 265
セキュアな会議リソースに関する詳細情報の入手先, on page 267

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のパケットキャプチャを設定するには、[**サービスパラメータ設定 (Service Parameter Configuration)**] ウィンドウでパケットキャプチャを有効にします。次に、[デバイス設定 (device configuration)] ウィンドウで、パケットキャプチャモードをバッチモードに設定し、電話、ゲートウェイ、またはトランクの SRTP に階層をキャプチャします。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 （20 ページ）
- 認証と暗号化のセットアップ （42 ページ）

関連トピック

システム要件, on page 7
連携動作と制限事項, on page 10
証明書, on page 20
認証と暗号化のセットアップ, on page 42
セキュアな会議, on page 253
会議ブリッジの要件, on page 254
セキュアな会議アイコン, on page 255
セキュアな会議のステータス, on page 256
Cisco Unified IP 電話 セキュアな会議とアイコンのサポート, on page 259
セキュアな会議の CTI サポート, on page 260
トランクとゲートウェイを介したセキュアな会議, on page 260
連携動作と制限事項, on page 260
会議リソースの保護のヒント, on page 262
セキュアな会議ブリッジのセットアップ, on page 264
セキュアな会議ブリッジのパケット キャプチャの設定, on page 267

セキュアな会議リソースに関する詳細情報の入手先

第 18 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のセキュリティ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

セキュリティを設定する前に、次の情報を考慮してください。

- 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 CiscoCallManager 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。

セキュアなボイスメッセージングポートのセットアップ

次の手順では、ボイスメッセージングポートのセキュリティを設定するために使用するタスクについて説明します。

手順

Step 1 CiscoCTL クライアントが混合モードにインストールされ、設定されていることを確認します。

Step 2 電話機が認証または暗号化用に設定されていることを確認します。

Step 3 Cisco Unified Communications Operating System Administration の証明書管理機能を使用して Cisco Unity 証明書を Unified Communications Manager サーバの信頼ストアにコピーし、CiscoCallManager 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 クラスタにある各 Unified Communications Manager サーバの Cisco CTL Provider サービスをアクティブにします。次に、すべてのサーバで CiscoCallManager サービスを再起動します。

Step 4 Unified Communications Manager の管理ページで、ボイス メッセージング ポートのデバイス セキュリティ モードを設定します。

Step 5 Cisco Unity または Cisco Unity Connection のボイス メッセージング ポートのセキュリティ関連設定タスクを実行します。たとえば、Cisco Unity が Cisco TFTP サーバを指すように設定します。

詳細については、Cisco Unity または *Cisco Unity Connection*の『Unified Communications Manager Integration Guide』を参照してください。

Step 6 Unified Communications Manager の管理ページでデバイスをリセットし、Cisco Unity ソフトウェアを再起動します。

詳細については、Cisco Unity または Cisco Unity Connection の『Unified Communications Manager Integration Guide』を参照してください。

関連トピック

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, on page 272

ボイスメールポートウィザードを使用したセキュリティプロファイルの適用, on page 273
Cisco CTL クライアントの設定, on page 113
電話機のセキュリティ, on page 189
電話セキュリティ プロファイルの設定, on page 201
ボイスメッセージングセキュリティの設定のヒント, on page 270

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、証明書がまだ存在していない場合に、デバイスをデータベースに追加し、電話機に証明書をインストールした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セキュリティとセキュアなボイスメッセージングポートの設定に関連するトピックを確認してください。

手順

Step 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。

Step 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を予め定義しています。デフォルト値は、[Not Selected] に指定されています。

Step 3 [保存（Save）] をクリックします。

Step 4 [リセット（Reset）] をクリックします。

関連トピック

ボイスメッセージングセキュリティ, on page 269
ボイスメッセージングセキュリティの設定のヒント, on page 270
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, on page 273

ボイスメールポートウィザードを使用したセキュリティプロファイルの適用

この手順を使用して、新しいボイスメールサーバの [ボイスメールポート (Voice Mail Port)] ウィザードで [デバイスセキュリティモード (Device Security Mode)] 設定を適用します。

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に関連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セキュリティとセキュアなボイスメッセージングポートの設定に関連するトピックを確認してください。

手順

Step 1 [Unified Communications Manager Administration] で、**[Voice Mail]** > **[Cisco Voice Mail Port Wizard]** を選択します。

Step 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。

Step 3 追加するポートの数を選択します。[**Next**] をクリックします。

Step 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**デバイス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を予め定義しています。デフォルト値は、[Not Selected] に指定されています。

Step 5 『 *Administration Guide for Cisco Unified Communications Manager* 』の説明に従って、その他のデバイス設定を行います。[次へ（Next）] をクリックします。

Step 6 『 *Administration Guide for Cisco Unified Communications Manager* 』の説明に従って、設定プロセスを続行します。[Summary] ウィンドウが表示されたら、[Finish] をクリックします。

関連トピック

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, on page 272
ボイスメッセージングセキュリティ, on page 269
ボイスメッセージングセキュリティの設定のヒント, on page 270
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, on page 273

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（42 ページ）
- 証明書（20 ページ）

関連トピック

システム要件, on page 7
連携動作と制限事項, on page 10
証明書, on page 20
認証と暗号化のセットアップ, on page 42
ボイスメッセージングセキュリティ, on page 269
ボイスメッセージングセキュリティの設定のヒント, on page 270

第 19 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は、電話機のセキュアステータスアイコンの表示を制御します。ポリシーのオプションは次のとおりです。

- BFCP および iX アプリケーションストリームを除くすべてのメディアが暗号化されている必要があります。

  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 および iX アプリケーションストリームの暗号化ステータスに依存しません。

- IX アプリケーションストリームを除くすべてのメディアが暗号化されている必要があります

  コールのセキュリティステータスは、暗号化ステータスiXアプリケーションストリームに依存しません。

- BFCPアプリケーションストリームを除くすべてのメディアが暗号化されている必要があります

  コールのセキュリティステータスは、BFCP 暗号化ステータスに依存しません。

- セッション内のすべてのメディアが暗号化されている必要があります

  コールのセキュリティステータスは、確立された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よって異なります。

- 音声のみを暗号化する必要があります

  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よって異なります。

（注） ポリシーの変更は、電話機のセキュアな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

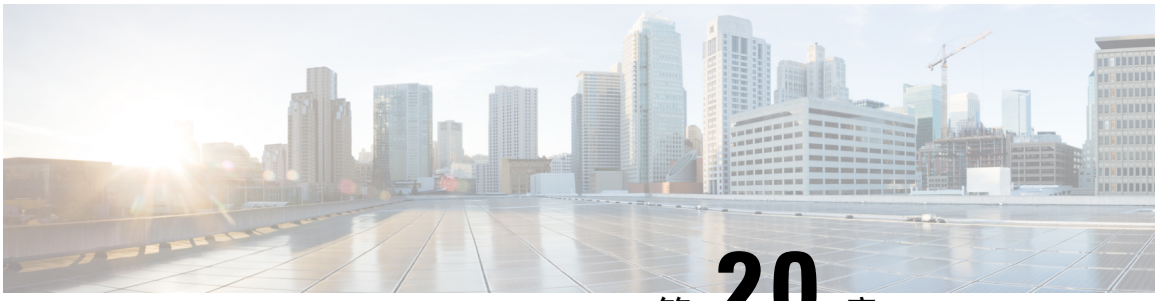
Step 1 Cisco Unified Communications Manager については、『 *System Configuration Guide* 』の「Configure service Parameters」の項の説明に従って、[Call Secure Status Policy] サービスパラメータを検索します。

Step 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を示す警告メッセージが表示されます。

Step 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 20 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と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。

- セキュリティ保護された、またはセキュリティ保護されていないコールに対して、セキュリティ保護されたモニタリングセッションを確立できます。
- コールモニタリング要求の結果として、元のコールのコールセキュリティが影響を受けたり、ダウングレードされたりすることはありません。
- 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のみ、続行が許可されます。
- エージェントとカスタマー間の元のコールには、モニタリングコール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、システムはエージェントと顧客の混合音声を、最初に新しいキーを使用して暗号化してから、上司に送信します。

（注） Unified Communications Manager は、安全でないレコーダを使用中に、認証済みコールのコール録音をサポートします。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

Step 1 エージェントおよび上司の電話機でセキュアな機能をプロビジョニングします。

Step 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。

- [デバイスのセキュリティモード（Device Security Mode）] を [暗号化（Encrypted）] に設定します。
- [セキュリティステータスを送信（Transmit Security Status）] チェックボックスをオンにします。
- [SRTP を許可する（SRTP Allowed）] チェックボックスをオンにします。
- [TLS SIP トランク（TLS SIP trunk）] をレコーダに設定します。

Step 3 非セキュアなモニタリングおよび録音と同じ方法で、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組み込みブリッジを設定します。
b) エージェントの電話の [ディレクトリ番号（Directory Number）] ページを使用して、[録音オプション（Recording Option）]（[通話録音の自動有効化（Automatic Call Recording Enabled）] と [アプリケーションから呼び出されたコール録音が有効（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) ディレクトリ番号にコール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。

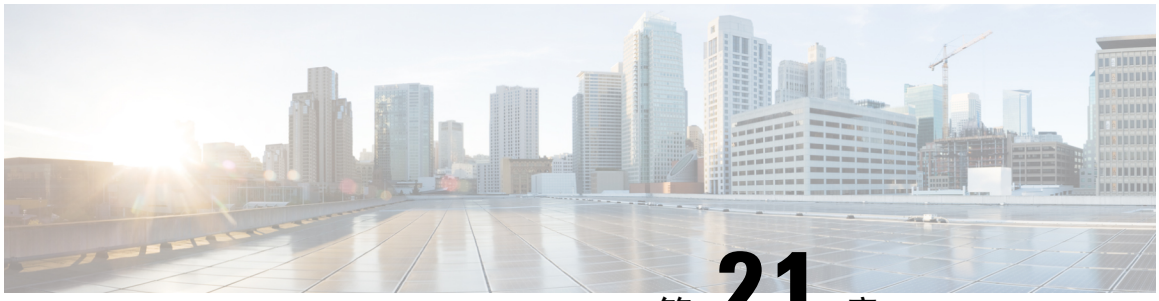
詳細な情報と手順については、Cisco Unified Communications Manager 機能設定ガイドの「モニタリングと録音」「」の章を参照してください。

関連トピック

電話機のセキュリティの設定, on page 194
SIP トランク セキュリティ プロファイルの設定, on page 335

第 IV 部

Cisco Unified IP 電話 のバーチャル プライベート ネットワーク



第 21 章

VPN クライアント

VPN クライアントの概要

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

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

VPN クライアント設定のタスク フロー

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

手順

	コマンドまたはアクション	目的
Step 1	Cisco IOS の前提条件の完了 （285 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。
Step 2	IP 電話 をサポートするための Cisco IOS SSL VPN の設定 （285 ページ）	IP 電話 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。

	コマンドまたはアクション	目的
Step 3	AnyConnect 用の ASA 前提条件への対応（287 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。
Step 4	IP 電話 での VPN クライアント用の ASA の設定 （288 ページ）	IP 電話 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。
Step 5	VPN ゲートウェイごとに VPN コンセントレータを設定します。	ユーザがリモート電話のファームウェアや設定情報をアップグレードするときに遅延が長くなるのを回避するため、VPN コンセントレータはネットワーク内の TFTP サーバまたは Unified Communications Manager サーバの近くにセットアップします。これがネットワーク内で不可能な場合、代替 TFTP サーバまたはロードサーバを VPN コンセントレータの横にセットアップすることもできます。
Step 6	VPN コンセントレータの証明書のアップロード （290 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。
Step 7	VPN ゲートウェイの設定 （291 ページ）	VPN ゲートウェイを設定します。
Step 8	VPN グループの設定 （292 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。
Step 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 （293 ページ） • VPN 機能のパラメータの設定 （295 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。
Step 10	共通の電話プロファイルへの VPN の詳細の追加 （296 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。
Step 11	Cisco Unified IP 電話 のファームウェアを、VPN をサポートしているバージョンにアップグレードします。	To run the Cisco VPN client, a supported Cisco Unified IP 電話 must be running firmware release 9.0（2） or higher. ファームウェアのアップグレードの詳細については、ご使用の Cisco Unified IP 電話 モデルの Unified Communications Manager に関する *Cisco Unified IP* 電話 アドミニストレーション ガイドを参照してください。

	コマンドまたはアクション	目的
Step 12	サポートされている Cisco Unified IP 電話を使用して、VPN 接続を確立します。	Cisco Unified IP 電話 を VPN に接続します。

Cisco IOS の前提条件の完了

次の手順を使用して、Cisco IOS の前提条件を完了します。

手順

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

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

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

Step 2 SSL VPN ライセンスをアクティベートします。

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

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

手順

Step 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
```

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

Step 3 からUnified Communications Managercapf 証明書をインポートします。

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

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

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

c) Cisco IOS ソフトウェア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 からインポートした証明書で置き換えます。

- 自己署名証明書を生成します。

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

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

例：

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

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

例：

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

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

Step 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
```

Step 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。例：

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
```

AnyConnect 用の ASA 前提条件への対応

AnyConnect の前提条件を完了するには、次の手順を使用します。

手順

Step 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。

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

Step 3 ライセンスをアクティベートします。

a) 次のコマンドを実行して、現在のライセンスの機能を確認してください。

show activation-key detail

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

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

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

デフォルト以外の URL を設定するときは、次のことを考慮してください。

- ASA の IP アドレスにパブリック DNS エントリが含まれている場合、これを完全修飾ドメイン名（FQDN）に置き換えることができます。
- You can only use a single URL （FQDN or IP address） on the VPN gateway in Unified Communications Manager.
- 証明書 CN またはサブジェクト代行名が必要な場合は、グループ URL の FQDN または IP アドレスを一致させます。

- ASA 証明書の CN や SAN が FQDN や IP アドレスと一致しない場合は、Unified Communications Manager のホスト ID チェックボックスをオフにします。

IP 電話 での VPN クライアント用の ASA の設定

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

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

手順

Step 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
```

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

から次の証明書をUnified Communications Manager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 電話 の認証。

- CAPF：LSC を使用した IP 電話 の認証。

これらUnified Communications Managerの証明書をインポートするには、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 からインポートした証明書で置き換えます。

- 自己署名証明書を生成します。

  例：

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

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

  例：

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

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

  例：

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

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

Step 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。例：

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

ASA 証明書の設定

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

VPN コンセントレータの証明書のアップロード

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

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

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

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

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

手順

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

Step 2 **[証明書のアップロード]**をクリックします。

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

Step 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。

Step 5 [ファイルのアップロード（Upload File）] をクリックします。

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

詳細については、「証明書の管理」の 章を参照 してください。

VPN ゲートウェイの設定

VPN ゲートウェイごとに VPN コンセントレータが設定されていることを確認します。VPN コンセントレータの設定後、VPN コンセントレータの証明書をアップロードします。詳細については、VPN コンセントレータの証明書のアップロード（290 ページ）を参照してください。

VPN ゲートウェイを設定するには、この手順を使用します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[拡張機能（Advanced Features）] > [VPN] > [VPN ゲートウェイ（VPN Gateway）]** を選択します。

Step 2 次のいずれかの操作を行います。

a) **[新規追加（Add New）]** をクリックして、新しいプロファイルを設定します。
b) コピーする VPN ゲートウェイの横にある **[コピー（Copy）]**をクリックします。
c) 適切な VPN ゲートウェイを見つけて、設定を変更し、既存のプロファイルを更新します。

Step 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 クライアント用 VPN ゲートウェイのフィールド（291 ページ）を参照してください。

Step 4 [保存（Save）] をクリックします。

関連トピック

VPN ゲートウェイの検索

VPN クライアント用 VPN ゲートウェイのフィールド

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

表 34 : VPN クライアント用 VPN ゲートウェイのフィールド

フィールド	説明
[VPN ゲートウェイ名（VPN Gateway Name）]	VPN ゲートウェイの名前を入力します。
[VPN ゲートウェイの説明（VPN Gateway Description）]	VPN ゲートウェイの説明を入力します。

フィールド	説明
[VPN ゲートウェイの URL（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） グループ URL で VPN コンセントレータを設定し、この URL をゲートウェイの 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。電話 VPN 信頼ロールに関係付けられた証明書だけが、使用可能な VPN 証明書のリストに表示されます。

VPN グループの設定

VPN グループを設定するには、この手順を使用します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[拡張機能（Advanced Features）] > [VPN] > [VPN グループ（VPN Group）]** を選択します。

Step 2 次のいずれかの操作を行います。

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

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

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

Step 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 クライアント用 VPN ゲートウェイのフィールド（291 ページ）、フィールドの説明の詳細について、を参照してください。

Step 4 [保存（Save）] をクリックします。

関連トピック

VPN グループの検索
VPN クライアント用 VPN グループのフィールド, on page 293

VPN クライアント用 VPN グループのフィールド

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

表 *35 : VPN* クライアント用 *VPN* グループのフィールド

フィールド	定義
[VPN グループ名（VPN Group Name）]	VPN グループの名前を入力します。
[VPN グループの説明（VPN Group Description）]	VPN グループの説明を入力します。
[使用可能なすべての VPN ゲートウェイ（All Available VPN Gateways）]	スクロールして、使用可能なすべての VPN ゲートウェイを確認します。
[この VPN グループ内で選択された VPN ゲートウェイ（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 クライアントで重要なエラーが発生し、特定の VPN ゲートウェイに接続できない場合は、リストの次の VPN ゲートウェイへの移動を試みます。 （注） 1 つの VPN グループに最大 3 つの VPN ゲートウェイを追加できます。また、VPN グループ内の証明書の合計数は 10 以下にする必要があります。

VPN プロファイルの設定

VPN プロファイルを設定するには、この手順を使用します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[拡張機能（Advanced Features）] > [VPN] > [VPN プロファイル（VPN Profile）]** を選択します。

Step 2 次のいずれかの操作を行います。

a) **[新規追加（Add New）]** をクリックして、新しいプロファイルを設定します。
b) 既存のプロファイルをコピーする VPN プロファイルの横にある **[コピー (copy)]** をクリックします。
c) 既存のプロファイルを更新するには、該当するフィルタを [Find VPN Profile Where] で指定し、[検索（Find）] をクリックして設定を変更します。

Step 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 クライアント用 VPN プロファイルのフィールド（294 ページ）、フィールドの説明の詳細について、を参照してください。

Step 4 [保存（Save）] をクリックします。

関連トピック

VPN プロファイルの検索

VPN クライアント用 VPN プロファイルのフィールド

この表では、VPN プロファイルフィールドの詳細について説明します。

表 *36 : 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。
説明	VPN プロファイルの説明を入力します。
[自動ネットワーク検出の有効化（Enable Auto Network Detect）]	このチェックボックスをオンにすると、企業ネットワークの外にいることが検出された場合に限り、VPN クライアントが動作します。 デフォルトで、ディセーブルになっています。
[最大伝送ユニット（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
[接続に失敗（Fail to Connect）]	このフィールドは、システムが VPN トンネルを作成している間に、ログイン操作または接続操作が完了するのを待機する時間を指定します。 デフォルト：30 秒
[ホストIDチェックを有効化（Enable Host ID Check）]	このチェックボックスをオンにする場合、ゲートウェイ証明書 subjectAltName または CN は、VPN クライアントの接続先の URL と一致する必要があります。 デフォルト：有効
[クライアント認証方式（Client Authentication Method）]	ドロップダウン リストから、クライアントの認証方式を選択します。 • [ユーザおよびパスワード（User and Password）] • パスワードのみ • [証明書（LSC または MIC）（Certificate (LSC or MIC)）]

フィールド	定義
[Enable Password Persistence]	このチェックボックスをオンにすると、ログインの失敗、ユーザによる手動のパスワードのクリア、電話のリセット、または電源が切れるまで、ユーザのパスワードは電話に保存されます。

VPN 機能のパラメータの設定

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[拡張機能（Advanced Features）] > [VPN] > [VPN 機能設定（VPN Feature Configuration）]**。

Step 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 （295 ページ）を参照してください。

Step 3 [保存（Save）] をクリックします。

次の作業を行います。

- 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。ファームウェアのアップグレード方法の詳細については、ご使用の Cisco Unified IP 電話 モデルの*Cisco Unified IP* 電話 アドミニストレーション ガイドを参照してください。
- サポートされている Cisco Unified IP 電話 を使用して、VPN 接続を確立します。

VPN 機能のパラメータ

VPN 機能パラメータの説明を表に示します。

表 37 : VPN 機能のパラメータ

フィールド	デフォルト
[自動ネットワーク検出の有効化（Enable Auto Network Detect）]	[はい（True）] の場合、企業ネットワークの外にいることが検出された場合に限り、VPN クライアントが動作します。 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。 最小値は 256 バイトです。 最大値は 1406 バイトです。

フィールド	デフォルト
[キープ アライブ（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） この値がゼロ以外であり、かつ Unified Communications Manager で指定された値よりも小さい場合、VPN コンセントレータのキープ アライブ設定によってこの設定が上書きされます。 デフォルト：60 秒 最小値：0 最大値：120 秒
[接続に失敗（Fail to Connect）]	このフィールドは、システムが VPN トンネルを作成している間に、ログイン操作または接続操作が完了するのを待機する時間を指定します。 デフォルト：30 秒 最小値：0 最大値：600 秒
[クライアント認証方式（Client Authentication Method）]	ドロップダウン リストから、クライアントの認証方式を選択します。 • [ユーザおよびパスワード（User and Password）] • パスワードのみ • [証明書（LSC または MIC）（Certificate (LSC or MIC)）] デフォルト：[ユーザおよびパスワード（User and Password）]
[パスワードの永続化を有効にする（Enable Password Persistence）]	[はい（True）]の場合、リセットするために[リセット（Reset）]ボタンまたは「**#**」が使用されると、ユーザ パスワードは電話機で保存されます。電話機の電源が失われるか、または工場出荷時の設定にリセットすると、パスワードは失われ、電話機でクレデンシャル用の音声ガイダンスが流れます。 デフォルト：False
[ホストIDチェックを有効化（Enable Host ID Check）]	[はい（True）] の場合、ゲートウェイ証明書 subjectAltName または CN は、VPN クライアントの接続先の URL と一致する必要があります。 デフォルト：[はい（True）]

共通の電話プロファイルへの VPN の詳細の追加

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

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）]**。

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

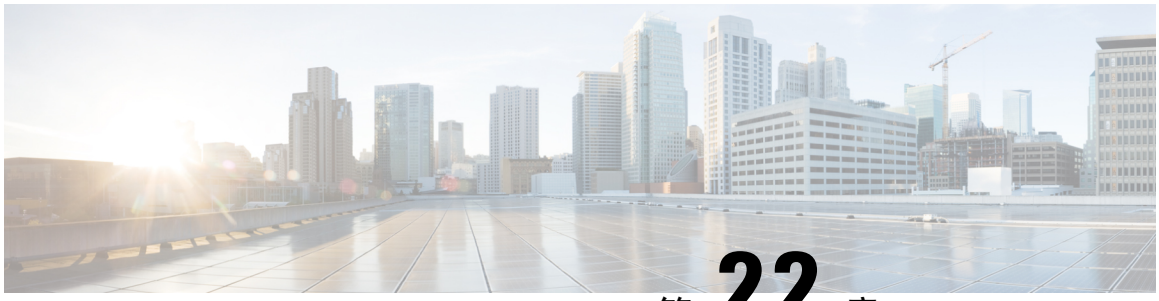
Step 3 [VPN情報（VPN Information）] セクションで、適切な [VPNグループ（VPN Group）] および [VPNプロファイル（VPN Profile）] を選択します。

Step 4 [保存（Save）]、[設定の適用（Apply Config）] の順にクリックします。

Step 5 設定の適用ウィンドウで [**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 22 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について説明します。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 CiscoJTAPI 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、このドキュメントでは、CTI 制御デバイスまたは回線の制限を設定する方法については説明しません。

CTI、JTAPI、および TAPI アプリケーションの認証

Unified Communications Manager を使用して、CTIManager と CTI/JTAPI/TAPI 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） Cisco JTAPI/TSP プラグインのインストール中に、セキュリティ設定を構成したとします。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 とアプリケーションは、相互に認証された TLS ハンドシェイク (証明書交換) によって他方の当事者の id 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。

アプリケーションとの認証を行うために、CTIManager は、Unified Communications Manager 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されたサードパーティの CA 署名付き証明書）を使用します。

CLI コマンドセットの**monitorctl**または Cisco ctl クライアントを使用して 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 クライアントが最初に TFTP サーバから CTL ファイルをダウンロードするときに、JTAPI/TSP クライアントは 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推奨します。JTAPI/TSP クライアントは、その後の CTL ファイルのダウンロードを確認します。たとえば、CTL ファイルを更新した後、JTAPI/TSP クライアントは、CTL ファイルのセキュリティトークンを使用して、ダウンロードする新しい CTL ファイルのデジタル署名を認証します。ファイルの内容には、Unified Communications Manager 証明書と CAPF サーバ証明書が含まれます。

CTL ファイルが侵害された場合、JTAPI/TSP クライアントはダウンロードした CTL ファイルを置き換えません。クライアント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 接続を確立しようとします。CTL ファイルが変更されたか、または侵害された場合、接続は失敗する可能性があります。CTL ファイルのダウンロードが失敗し、複数の TFTP サーバが存在する場合は、ファイルをダウンロードするように別の TFTP サーバを設定できます。JTAPI/TAPI クライアントは、次の状況ではどのポートにも接続しません。

- クライアントは何らかの理由で CTL ファイルをダウンロードできません。たとえば、CTL ファイルは存在しません。
- クライアントには、既存の CTL ファイルがありません。
- アプリケーションユーザをセキュアな CTI ユーザとして設定しました。

アプリケーションは、CTIManager を使用して認証するために、認証局プロキシ機能（CAPF）によって発行され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つの証明書がすべてのインスタンスをカバーしていません。Cisco Unified Communications 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、「CAPF の設定項目」の説明に従って、 Cisco Unified Communications Manager Administration で、それぞれの [アプリケーションユーザ CAPF プロファイルの設定（Application User CAPF Profile Configuration）] または [エンドユーザ CAPF プロファイルの設定（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。

また、アプリケーションの TLS を有効にするには、Unified Communications Manager 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があります。このグループにユーザを追加して証明書をインストールすると、アプリケーションによって、ユーザが TLS ポート経由で接続することが保証されます。

関連トピック

CAPF の設定項目, on page 307
Cisco CTL クライアントの設定, on page 113

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して機能します。つまり、認証を設定していない場合、暗号化を使用することはできません。

Unified Communications Manager、Cisco QRT、および Cisco Web Dialer は暗号化をサポートしません。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 間のメディアストリームを保護するには、Unified Communications Manager でアプリケーション ユーザまたはエンドユーザを [標準 CTI SRTP キー情報の受信許可（Standard CTI Allow Reception of SRTP Key Material）] ユーザグループに追加します。これらのユーザが Standard CTI Secure Connection ユーザグループにも存在し、クラスタセキュリティモードが混合モードになっている場合、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アプリケーションに主要な資料を提供します。

（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。

アプリケーションは SRTP キー資料を記録したり保存したりしませんが、アプリケーションはキーマテリアルを使用して RTP ストリームを暗号化し、CTIManager から SRTP ストリームを復号化します。

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。制限を設定したために CTI/JTAPI/TAPI がデバイスまたは電話番号をモニタまたは制御できない場合、CTIManager はキー情報を送信しません。

ヒント アプリケーションが SRTP セッションキーを受信するには、アプリケーションまたはエンドユーザが、Standard CTI Enabled、Standard CTI Secure Connection、および Standard CTI で SRTP キー情報の受信を許可する3つのグループに存在している必要があります。

Unified Communications Managerは、CTIports およびルートポイントで送受信されるセキュアコールを円滑にしますが、アプリケーションがメディアパラメータを処理するため、セキュアコールをサポートするようにアプリケーションを設定する必要があります。

CTIports/ルートポイントは、ダイナミックまたはスタティック登録によって登録します。ポート/ルートポイントがダイナミック登録を使用している場合、各コールに対してメディアパラメータが指定されます。スタティック登録の場合、メディアパラメータは登録時に指定され、コールごとに変更することはできません。CTIports/ルートポイントが TLS 接続を介して CTIManager に登録されると、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し、他方がセキュアである場合は、SRTP を介してメディアが暗号化されます。

CTI アプリケーションが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、アプリケーションは RTP イベントを受信しません。確立されたコールの場合、CTI アプリケーションは DeviceSnapshot イベントを提供します。これは、コールのメディアがセキュアか非セキュアかを定義します。このイベントは、キー素材を提供しません。

CTI、JTAPI、および TAPI アプリケーションの CAPF の機能

認証局プロキシ機能（CAPF）は Unified Communications Manager とともに自動的にインストールされ、設定に応じて次の CTI/TAPI/TAPI アプリケーション用のタスクを実行します。

- 認証文字列を使用して JTAPI/TSP クライアントに対して認証を行います。
- 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）を発行します。
- 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またはエンドユーザに証明書を発行するには、[Application User CAPF Profile Configuration] ウィンドウまたは [End User CAPF Profile Configuration] ウィンドウでそれぞれ設定を行います。次に、Unified Communications Manager がサポートする CAPF プロファイルの違いについて説明します。

- **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、複数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 キーストア形式で 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、暗号化された形式で LSC を保存します。

次の情報は、通信または電源障害が発生した場合に適用されます。

- 証明書のインストールが行われている間に通信障害が発生した場合、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 クライアントでは、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、割り当てられた時間に証明書を取得しようとする回数を指定して、これらの値を設定します。両方の値について、デフォルトは0です。1(1回の再試行)、2、または3を指定することで、最大3回の再試行を設定できます。再試行ごとに30秒以内に設定できます。

- JTAPI/TSP クライアントが CAPF とのセッションを試行している間に電源障害が発生した場合、クライアントは電源が回復した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 システムインタラクションと要件

CAPF には次の要件があります。

- 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、[エンタープライズパラメータ設定（Enterprise Parameters Configuration）] ウィンドウの [クラスタセキュリティモード（Cluster Security Mode）] を 1（混合モード）に設定します。
- CAPF を使用するには、パブリッシャノードで Cisco 認証局プロキシ機能サービスをアクティブに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プロセス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 を使用することを推奨します。

- 証明書操作の全期間を通じて、パブリッシャノードが正常に実行されていることを確認します。
- 証明書の操作全体で CTI/JTAPI/TAPI アプリケーションが機能していることを確認します。

Certificate Authority Proxy Function サービスのアクティブ化

Unified Communications Managerは、Cisco Unified Serviceability で認証局プロキシ機能サービスを自動的にはアクティブ化しません。

CAPF 機能を使用するには、最初のノードでこのサービスを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ていない場合は、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 証明書は、CAPF 証明書が存在することを検証として、Cisco Unified Communications オペレーティングシステムの GUI に表示されます。

関連トピック

CTL ファイルの更新, on page 124

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 アプリケーション用の重要な証明書をローカルでインストール/アップグレード/トラブルシューティングする場合は、「CAPF の設定項目」を参考にしてください。

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てからエンドユーザ CAPF プロファイルを設定することを推奨します。

手順

Step 1　Cisco Unified Communications Manager Administration で、次のいずれかのオプションを選択します。

a) **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アプリケーションユーザ CAPF プロファイル（Application User CAPF Profile）]**
b) **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [エンドユーザ CAPF プロファイル（End User CAPF Profile）]**

Step 2　次のいずれかの操作を行います。

a) 既存のプロファイルを編集するには、[検索（Find）]をクリックし、既存のプロファイルを編集します。
b) 新しいプロファイルを作成するには、[新規追加（Add New）] をクリックします。
c) 既存のプロファイルから新しいプロファイルに設定をコピーするには、**[検索（Find）]** をクリックし、目的の設定がある既存のプロファイルを選択します。[コピー（Copy）]をクリックして、それらの設定を含む新しいプロファイルに名前を付けます。必要に応じて新しいプロファイルを編集します。

Step 3 「CAPF の設定項目」の説明に従って、適切な設定を入力します。

Step 4 [保存（Save）] をクリックします。

Step 5 この手順を繰り返して、さらに CAPF プロファイルを作成します。ユーザに必要な数のプロファイルを作成します。
[アプリケーションユーザ CAPF プロファイルの設定（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。

関連トピック

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
JTAPI/TAPI セキュリティ関連のサービスパラメータのセットアップ, on page 315
CTI、JTAPI、TAPI 認証に関する詳細情報の入手先

CAPF の設定項目

次の表で、**[アプリケーション ユーザ CAPF プロファイルの設定（Application User CAPF Profile Configuration）]** および **[エンド ユーザ CAPF プロファイルの設定（End User CAPF Profile Configuration）]** ウィンドウの CAPF の設定項目について説明します。

表 *38 :* 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項目

設定	説明
Application User	ドロップダウンリストから、**CAPF 操作のアプリケーションユーザ**を選択します。この設定には、設定されたアプリケーションユーザが表示されます。 この設定は、[エンドユーザ CAPF プロファイル（End User CAPF Profile Configuration）] ウィンドウには表示されません。
エンド ユーザ ID（End User ID）	ドロップダウンリストから、**CAPF 操作のエンドユーザ**を選択します。この設定は設定済みのエンドユーザを示します。 この設定は、[アプリケーションユーザ CAPF プロファイルの設定（Application User CAPF Profile Configuration）] ウィンドウには表示されません。

設定	説明
[インスタンス ID（Instance ID）]	1 ～ 128 文字の英数字（a ～ z、A ～ Z、0 ～ 9）を入力します。インスタンス ID は、証明書を操作するユーザを識別します。 アプリケーションの複数の接続先（インスタンス）を設定できます。アプリケーションと CTIManager 間の接続を保護するには、アプリケーション PC（エンドユーザ用）またはサーバ（アプリケーション ユーザ用）上で実行される各インスタンスが固有の証明書を持ってい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。
[証明書の操作（Certificate Operation）]	ドロップダウン リストから、次のオプションのいずれかを選択します。 • **[保留中の操作なし（No Pending Operation）]**：証明書の操作が発生しない場合に表示されます。（デフォルト設定） • [インストール/アップグレード（Install/Upgrade）]：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。
[認証モード（Authentication Mode）]	証明書の操作が [インストール/アップグレード（Install/Upgrade）] の場合、認証モードとして [認証文字列（By Authentication String）] が指定されます。つまり、ユーザ/管理者によって [JTAPI/TSP 設定（JTAPI/TSP Preferences）] ウィンドウに CAPF 認証文字列が入力された場合にのみ、ローカルで有効な証明書のインストール/アップグレードまたはトラブルシューティングが CAPF によって実行されます。
[認証文字列（Authentication String）]	手動で一意の文字列を入力するか、[文字列の生成（Generate String）] ボタンをクリックして文字列を生成します。 4 桁から 10 桁の文字列が含まれてい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（JTAPI/TSP preferences）]** 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 回の使用のみをサポートしており、文字列をインスタンスで使用した後は、再び使用できません。
文字列の生成（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、[文字列の生成（Generate String）] ボタンをクリックします。[認証文字列（Authentication String）] フィールドに 4 桁から 10 桁の認証文字列が表示されます。

設定	説明
[キーの順序（Key Order）]	このフィールドは、CAPF のキーの順序を指定します。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 のみ（RSA Only）]** • **[ECのみ（EC Only）]** • **[EC 優先、RSA バックアップ（EC Preferred, RSA Backup）]** （注） [キーの順序（Key Order）]、[RSAキーサイズ（RSA Key Size）]、および [ECキーサイズ（EC Key Size）] の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 プロファイルはその電話に関連付けられます。値 [ECのみ（EC Only）] と [ECキーサイズ（EC Key Size）] で 256 ビットの値を選択した場合、デバイス セキュリティ プロファイルには [EC-256] の値が追加されます。
[RSAキーサイズ（ビット）（RSA Key Size (Bits)）]	ドロップダウンリストから、**512**、**1024**、**2048**、**3072**、または**4096**のいずれかの値を選択します。
[ECキーサイズ（ビット）（EC Key Size (Bits)）]	ドロップダウンリストから、**256**、**384**、または**521**のいずれかの値を選択します。
操作完了期限（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 操作有効期間（日数）（CAPF Operation Expires in (days)）] エンタープライズ パラメータと併用します。このパラメータはいつでもアップデートできます。
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。

関連トピック

CAPF システム インタラクションと要件
JTAPI/TAPI セキュリティ関連のサービスパラメータのセットアップ, on page 315
詳細情報の入手先, on page 61

CAPF サービス パラメータの更新

[サービスパラメータ（Service Parameter）] ウィンドウには、Cisco Certificate Authority Proxy Function のオプション設定があります。CAPF証明書の証明書発行者、オンラインCA接続設定、証明書の有効期間、キーサイズなどの設定を構成できます。

Cisco Unified Communications Manager Administration で CAPF サービスパラメータをアクティブとして表示するには、Cisco Unified Serviceability で[認証局プロキシ機能（Certificate Authority Proxy Function）] サービスを有効にします。

ヒント　電話機にCAPFを使用したときにCAPFサービスパラメータを更新した場合は、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

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

Step 2　**[サーバ（Server）]** ドロップダウン リストからサーバを選択します。

ヒント　クラスタ内のパブリッシャノードを選択する必要があります。

Step 3　**[サービス（Service）]** ドロップダウンリストで、**[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。

Step 4　オンラインヘルプの説明に従って、**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。

Step 5　変更内容を有効にするには、Cisco Unified Serviceability で、**Cisco Certificate Authority Proxy Function** サービスを再起動します。

（注）　認証局プロキシ機能の設定方法の詳細については、「**認証局プロキシ機能**」の章を参照してください。

関連トピック

CTI、JTAPI、TAPI 認証に関する詳細情報の入手先

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

Cisco 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、別のプロファイルをデバイスに適用するか、該当プロファイルを使用するすべてのデバイスを削除してください。プロファイルを使

用しているデバイスを確認するには、[セキュリティ プロファイルの設定（Security Profile Configuration）] ウィンドウの [関連リンク（Related Links）] ドロップダウンリストで [依存関係レコード（Dependency Records）] を選択し、[移動（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については、Cisco Unified Communications Manager システム設定ガイドを参照してください。

ここでは、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 Unified Communications Manager データベースから削除する方法を説明します。

手順

Step 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 プロファイルを検索します。

Step 2 次のいずれかの操作を行います。

a) 複数のプロファイルを削除するには、[**Find And List**] ウィンドウの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ます。次に、[**Delete Selected**] をクリックします。この選択で設定可能なすべてのレコードを削除するには、[すべて選択（Select All）] をクリックして、[選択項目の削除（Delete Selected）] をクリックします。

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ます。次に、[**Delete Selected**] をクリックします。

Step 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。

関連トピック

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
CTI、JTAPI、TAPI 認証に関する詳細情報の入手先

CTI、JTAPI、および TAPI の保護

次の手順では、CTI/JTAPI/TAPI アプリケーションを保護するために実行するタスクについて説明します。

手順

Step 1 CTI アプリケーションと JTAPI/TSP プラグインがインストールされ、実行されてい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。

- *Unified Communications Manager*の*Cisco JTAPI* インストールガイド
- *Unified Communications Manager*の*Cisco TAPI* インストールガイド

Step 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ていることを確認し、CTL ファイルを実行して作成します。
- CTL プロバイダーサービスがインストールされ、サービスがアクティブ化されてい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化されてい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 Capf サービスは、CTL ファイルに CAPF 証明書を含めるために、Cisco CTL クライアントに対して実行する必要があります。電話機に CAPF を使用したときにこれらのパラメータを更新した場合は、パラメータを再度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。

Step 3 エンドユーザとアプリケーションユーザを、必要な権限を含むアクセス制御グループに割り当てます。ユーザを次のすべてのグループに割り当てます。これにより、ユーザは CTI 接続で **TLS** および **SRTP** を使用できます。

- 標準 CTI 対応
- 標準 CTI セキュア接続
- 標準 CTI SRTP 重要素材の受信許可

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のいずれか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。

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。アプリケーションまたはエンドユーザは、これら3つのグループに存在しない場合、SRTP セッションキーを受信できません。詳細については、ユーザアクセス制御グループの設定に関連するトピックを参照してください。

（注） Cisco Unified Communications Manager Assistant、Cisco QRT、および Cisco Web Dialer は暗号化をサポートしません。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。

Step 4 エンドユーザとアプリケーションユーザの CAPF プロファイルを設定します。詳細については、「**認証局プロキシ機能**」の章を参照 してください。

Step 5 CTI/JTAPI/TAPI アプリケーションで、対応するセキュリティ関連のパラメータを有効にします。

関連トピック

Cisco CTL クライアントの設定, on page 113
CAPF サービス パラメータの更新
セキュリティ関連のアクセス制御グループへのアプリケーションとエンドユーザの追加, on page 313
CTI、JTAPI、および TAPI アプリケーションの CAPF の機能, on page 304
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, on page 306
CAPF の設定項目, on page 307
JTAPI/TAPI セキュリティ関連のサービスパラメータのセットアップ, on page 315

セキュリティ関連のアクセス制御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 ユーザグループおよび 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 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のいずれか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。

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。

アプリケーションとエンドユーザが SRTP を使用できるようになるには、そのユーザは、TLS のベースライン設定として機能する 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。SRTP 接続には TLS が必要です。ユーザがこれらのグループに存在する場合は、標準 CTI にユーザを追加して、SRTP キーマテリアルユーザグループの受信を許可することができます。アプリケーションが SRTP セッションキーを受信するには、アプリケーションまたはエンドユーザが、**Standard CTI Enabled**、**Standard CTI Secure Connection**、および **Standard CTI で SRTP キー情報の受信を許可する**3つのグループに存在している必要があります。

Cisco Unified Communications Manager Assistant、CiscoQRT、および Cisco Web Dialer が暗号化をサポートしていないため、アプリケーションユーザ（CCMQRTSecureSysUser、IPMASecureSysUser、および WDSecureSysUser）を標準 CTI SRTP 重要素材の受信許可ユーザグループに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、Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。**[ロールの設定（Role Configuration）]** ウィンドウでのセキュリティ関連の設定については、Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。

手順

Step 1　Cisco Unified Communications Manager Administrationから、**[ユーザ管理（User Management）] > [ユーザグループ（User Group）]** を選択します。

Step 2　すべての**ユーザグループ**を表示するには、[検索（Find）] をクリックします。

Step 3　実行する内容に応じて、次のいずれかの作業を行います。

a) アプリケーションまたはエンドユーザが Standard CTI Enabled グループに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、[標準 CTI セキュア接続（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、[標準CTI SRTP重要素材の受信許可（Standard CTI Allow Reception of SRTP Key Material）] リンクをクリックします。

Step 4　アプリケーション ユーザをグループに追加するには、手順 5 ~ 7 を実行します。

Step 5　[グループにアプリケーションユーザを追加（Add Application Users to Group）] をクリックします。

Step 6　アプリケーションユーザを検索するには、検索条件を指定します。次に、**[検索 (Find)]** をクリックします。

検索条件を指定せずに [検索 (Find)] をクリックすると、使用可能なすべてのオプションが

Step 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。

ユーザが [ユーザグループ（User Group）] ウィンドウに表示されます。

Step 8　エンドユーザをグループに追加するには、ステップ 9 ～ 11 を実行します。

Step 9　[グループにユーザを追加（Add Users to Group）] をクリックします。

Step 10　エンドユーザを検索するには、検索条件を指定します。次に、**[検索 (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。

Step 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。

ユーザが [ユーザグループ（User Group）] ウィンドウに表示されます。

関連トピック

CTI、JTAPI、TAPI 認証に関する詳細情報の入手先

JTAPI/TAPIセキュリティ関連のサービスパラメータのセットアップ

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

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

Step 2 **[サーバ**（**Server**）**]** ドロップダウンリストから、[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。

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

Step 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。

Step 5 疑問符またはパラメータ名のリンクをクリックしたときに表示されるヘルプの説明に従って、パラメータを更新します。

Step 6 [保存（Save）] をクリックします。

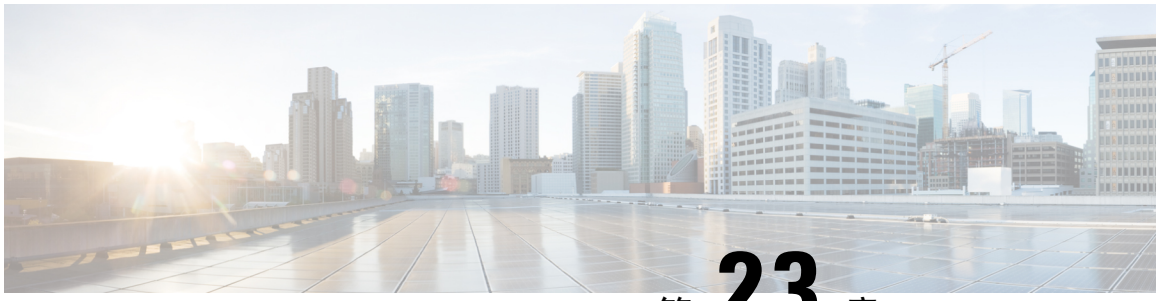
Step 7 サービスがアクティブになっているサーバごとに、この手順を繰り返します。

アプリケーションまたはエンドユーザの証明書の操作ステータスの表示

特定の [アプリケーションユーザ CAPF プロファイル設定（Application User CAPF Profile configuration）] または [エンドユーザ CAPF プロファイル設定（End User CAPF Profile configuration）] ウィンドウで、または（[検索/一覧表示（Find/List）] ウィンドウではなく） [JTAPI/TSP 設定（JTAPI/TSP Preferences）] GUI ウィンドウで、証明書操作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 23 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 電話機の設定ファイルには、1つの発行者からの証明書のみが含まれています。そのため、システムは HSRP をサポートしていません。

SRST のセキュリティのヒント

セキュアな電話機と SRST 対応ゲートウェイ間の接続を保護するために、次の基準が満たされていることを確認します。

- SRST リファレンスには、自己署名証明書が含まれています。
- Cisco CTL クライアントを使用して混合モードを設定しました。
- 認証または暗号化のために電話機を設定しました。
- 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） LSC 認証の場合は、CAPF 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機の 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と同等の場合、システムはセキュリティ関連の設定を無視します。たとえば、デバイスセキュリティモードの場合は SRST セキュアですか。チェックボックスなどをオンにします。設定はデータベースから削除されませんが、セキュリティは提供されません。
- 電話機は、クラスタセキュリティモードが混合モードになっている場合にのみ、SRST 対応ゲートウェイへのセキュアな接続を試行します。電話設定ファイルのデバイスセキュリティモードが authenticated または encrypted に設定されている場合は、SRST セキュアですか。[**Srst 設定 (Srst Configuration)**] ウィンドウでチェックボックスがオンになっており、有効な srst 対応ゲートウェイ証明書が電話機の設定ファイルに存在しています。

- 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、セキュリティのために SRST 設定プロセスを実行するタスクを示しています。

手順

Step 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『*CiscoIOS SRST Version System Administrator Guide*』を参照してください。

Step 2 CiscoCTL クライアントをインストールして設定するために必要なすべてのタスクを実行したことを確認します。

Step 3 電話に証明書が存在することを確認します。

詳細については、ご使用の電話機モデルのCisco Unified IP 電話 のマニュアルを参照してください。

Step 4 電話機が認証または暗号化用に設定されていることを確認します。

Step 5 [デバイスプールの設定 (Device Pool Configuration)] ウィンドウでの SRST リファレンスの有効化を含む、セキュリティのための SRST リファレンスを設定します。

Step 6 SRST 対応のゲートウェイと電話をリセットします。

関連トピック

電話機へのセキュリティ プロファイルの適用 , on page 219
Cisco CTL クライアントの設定, on page 113
セキュア SRST リファレンスのセットアップ, on page 322

セキュア SRST リファレンスのセットアップ

[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 39：セキュア SRST リファレンスの設定（324 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

Step 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。

Step 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、**[新規追加 (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] 列でそのレコードの [**copy**] アイコンをクリックします。(プロファイルを表示し、**[コピー (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。

Step 3 表 39：セキュア SRST リファレンスの設定（324 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。

SRST リファレンスの追加設定の詳細については、 *Cisco Unified Communications Manager* のアドミニストレーションガイドを参照してください。

[Find and List] ウィンドウが表示されます。

Step 4 [Is SRST Secure?] をオンにした後、チェックボックスをオンにすると、[証明書の更新 (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という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。

Step 5 [保存（Save）] をクリックします。

Step 6 データベース内の SRST 対応ゲートウェイ証明書を更新するには、[**証明書の更新 (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。

Step 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。

Step 8 [閉じる（Close）] をクリックします。

Step 9 [SRST Reference Configuration] ウィンドウで、[**Reset**] をクリックします。

次のタスク

[**デバイスプールの設定 (Device Pool Configuration)**] ウィンドウで srst リファレンスが有効になっていることを確認します。

関連トピック

SRST セキュリティに関する詳細情報の入手先

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 *39* : セキュア *SRST* リファレンスの設定

設定	説明
セキュアSRST（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、ゲートウェイおよび従属する電話をリセットすると、CiscoCTL Provider サービスは、SRST 対応のゲートウェイ上の証明書プロバイダサービスに対して認証を行います。CiscoCTL 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 証明書 プロバイダー ポート（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。CiscoSRST 証明書プロバイダのデフォルトポートは 2445 です。 SRST 対応のゲートウェイ上でこのポートを設定したら、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は、別の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 の範囲内に存在する必要があります。それ以外の場合は、次のメッセージが表示されます: ポート番号には数字のみを含めることができます。

設定	説明
証明書を更新する（Update Certificate）	ヒント　このボタンは、[セキュア SRST（Is SRST Secure?）] チェックボックスをオンにして [保存（Save）] をクリックした場合のみ表示されます。 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、CiscoCTL 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 対応のゲートウェイ証明書）を電話に送信します。

関連トピック

SRST のセキュリティのヒント, on page 320
詳細情報の入手先, on page 61

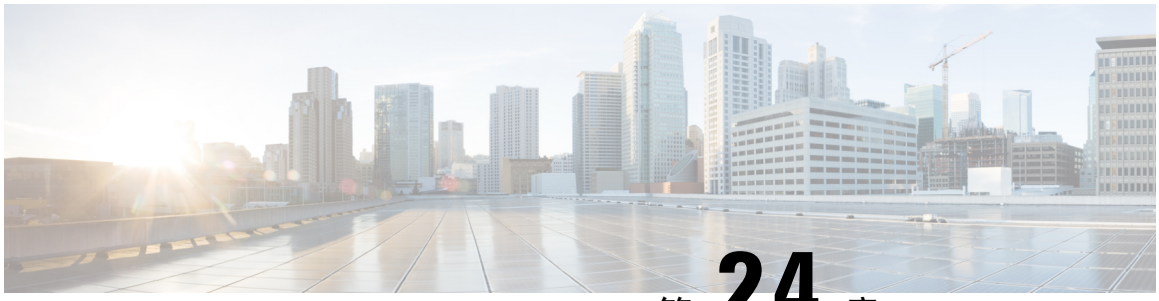
SRST リファレンスからのセキュリティの削除

セキュリティを設定した後に SRST リファレンスを非セキュアにするには、[Is SRST Secure?] チェックボックスをオフにします。[SRST 設定 (SRST Configuration)] ウィンドウのチェックボックスをオンにします。ゲートウェイのクレデンシャルサービスをオフ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。

このタスクを実行するには、[**IS Srst Secure?**] チェックボックスをオフにして、[Srst Configuration] ウィンドウで [**Update**] をクリックします。次に、[**Reset Devices**] をクリックします。



第 24 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、ゲートウェイと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。MGCP SRTP パッケージは、ゲートウェイがセキュア RTP 接続上でパケットを暗号化および復号化するときに使用されます。コールセットアップ中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まります。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。少なくとも1つのデバイスが 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。

システムが 2 台のデバイス間で暗号化 SRTP コールを設定する場合、Unified Communications Manager はセキュアコール用のマスター暗号化キーと salt を生成し、SRTP ストリーム専用のゲートウェイに送信します。Unified Communications Manager は SRTCP ストリーム用のキーと salt を送信しませんが、ゲートウェイはこれらもサポートします。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 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、システムはゲートウェイにセッションキーをクリアテキストで送信します。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 用に設定されている MGCP ゲートウェイが、認証済みデバイス（たとえば、SCCP を実行している認証済み電話機）とのコールに関与している場合、 Unified Communications Managerがコールを認証済みとして分類するため、電話機に保護アイコンが表示されます。 Unified Communications Managerは、デバイスの SRTP 機能がコールのネゴシエートに成功した場合、コールを暗号化として分類します。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。

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。コマンド **mgcppackage-capabilitysrtp-package** を使用してゲートウェイを設定します。
- 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。
- 保護ステータスは、COCP PRI Setup、Alert、および Connect の各メッセージで独自の FacilityIE を使用して、交換用の CP E1 PRI ゲートウェイと交換されます。
- Unified Communications Manager は、Cisco Unified IP 電話 でのみセキュア通知トーンを再生します。ネットワーク内の PBX は、コールのゲートウェイ側にトーンを再生します。
- Cisco Unified IP 電話 と MGCP E1 PRI ゲートウェイの間のメディアが暗号化されていないと、コールはドロップされます。

（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。

H.323 ゲートウェイおよび h.323/h.323/.h トランク暗号化 (h.323)

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。接続を正しく設定しないと、セキュリティ関連の情報がクリアテキストで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 data] の通過を有効にするには、次のトランクおよびゲートウェイの構成時の設定で [**h.235 パススルーを許可**する] チェックボックスをオンにします。

- 「-225 Trunk」
- 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の両方でセキュアなコールをサポートできます。TLS はシグナリング暗号化を提供し、SRTP は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 ([**システム** > **セキュリティプロファイル** > **(sip trunk security profile)**] ウィンドウで) を設定するときに、次のオプションを選択します。

- **[デバイス セキュリティ モード（Device Security Mode）]** ドロップダウンリストから、「[暗号化済（Encrypted）]」 を選択します。
- **[着信転送タイプ（Incoming Transport Type）]** ドロップダウンリストから 「[TLS]」 を選択します。
- **[発信転送タイプ（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ら、そのプロファイルをトランクに適用します ([**Device** > **trunk** > **sip trunk** configuration] 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を許可（SRTP Allowed）]** チェックボックスをオンにします（**[デバイス（Device）][トランク][SIP トランク（SIP Trunk）]** 設定ウィンドウでも同様です）。

⚠

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とトランクの接続先間でネットワークのセキュリティを確保する必要があります。

関連トピック

SIP トランク セキュリティ プロファイルの設定, on page 335

セキュアゲートウェイとトランクのセットアップ

この手順は、 *CiscoIOS* のメディアおよびシグナリングの認証および暗号化機能と組み合わせて使用します。これにより、セキュリティのためにCiscoIOS MGCP ゲートウェイを設定する方法に関する情報が提供されます。

手順

Step 1 **ctls ctl** コマンドを実行してクラスタを混合モードに設定したことを確認します。

Step 2 電話機が暗号化用に設定されていることを確認します。

Step 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。

Step 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 で [SRTPを許可する（SRTP Allowed）] チェックボックスをオンにします。

[SRTPを許可する（SRTP Allowed）]チェックボックスは、[トランクの設定（Trunk Configuration）]ウィンドウまたは[ゲートウェイの設定（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、Cisco Unified Communications Manager アドミニストレーション ガイド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。

Step 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、**[デバイス（Device）] > [トランク（Trunk）] > [SIP トランク（SIP Trunk）]** の設定ウィンドウで **[SRTP を許可する（SRTP allowed）]** チェックボックスを必ずオンにします。

注意 **[SRTP を許可する（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とトランクの接続先間でネットワークのセキュリティを確保する必要があります。

Step 6 ゲートウェイで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。

関連トピック

Cisco CTL クライアントの設定, on page 113
Unified Communications Manager とゲートウェイまたはトランク間の IPsec の設定, on page 333
ネットワーク インフラストラクチャ内の IPSec 設定, on page 332
電話機のセキュリティ, on page 189
デフォルトのセキュリティ機能, on page 79
SIP トランク セキュリティ プロファイルの設定, on page 335

ネットワーク インフラストラクチャ内の IPSec 設定

このセクションでは、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。

- Ciscoでは、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、ジッターや遅延などの評価指標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 CiscoIOS 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た球体内のネットワークデバイスでホストの終端を終端します。たとえば、ファイアウォール、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デバイスの背後にあります。
- 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。
- セキュアゲートウェイとトランクの設定に関連するトピック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。

Unified Communications Manager とゲートウェイまたはトランク間の 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 を許可する（SRTP Allowed）] チェックボックスは、Unified Communications Managerの次の設定ウィンドウに表示されます。

- H.323 ゲートウェイの設定ウィンドウ
- [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 トランクの設定 (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

Step 1 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。

Step 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 を許可する（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 を許可する（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ないように TLS 暗号化プロファイルの使用を推奨します。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とトランクの接続先間でネットワークのセキュリティを確保する必要があります。

Step 3 [保存（Save）] をクリックします。

Step 4 デバイスをリセットするには、[Reset] をクリックします。

Step 5 IPSec が H323 に対して正しく設定されていることを確認します。(SIP の場合は、TLS が正しく設定されていることを確認してください)。

関連トピック

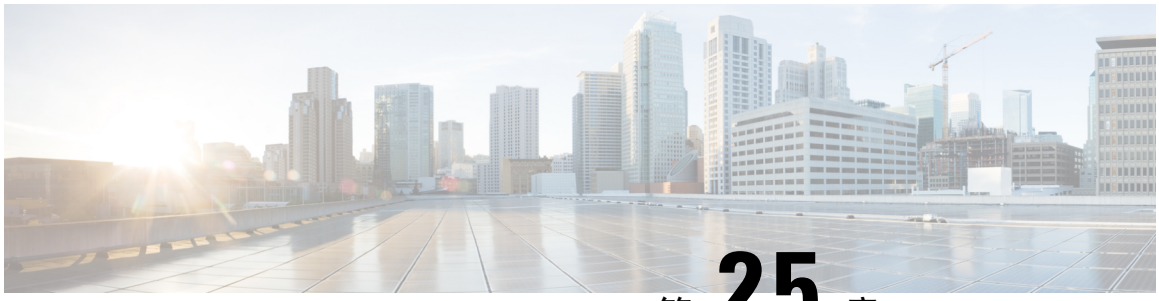
ゲートウェイとトランクの暗号化に関する詳細情報の入手先, on page 334

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

- 認証、整合性、および許可 （25 ページ）
- 暗号化 （31 ページ）

関連トピック

認証、整合性、および許可, on page 25
暗号化, on page 31
Cisco IOS MGCP ゲートウェイの暗号化, on page 327
H.323 ゲートウェイおよび h.323/h.323/.h トランク暗号化 (h.323), on page 328
SIP トランクの暗号化, on page 330
セキュアゲートウェイとトランクのセットアップ, on page 331
ネットワーク インフラストラクチャ内の IPSec 設定, on page 332
Unified Communications Manager とゲートウェイまたはトランク間の IPsec の設定, on page 333



第 25 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設定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項目には、デバイス セキュリティ モード、ダイジェスト認証、着信/発信転送タイプの設定があります。[トランクの設定（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、自動登録用の定義済み非セキュア 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、それを 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は、SIP トランクがサポートするセキュリティ機能だけが表示されます。

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場合は、[トランクの設定 (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。
- すでに 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、そのプロファイルが割り当てられているすべての SIP トランクに再設定された設定が適用されます。
- 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と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と設定を前提としています。
- 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

Step 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）クエリーのレコードも表示されることがあります。

Step 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、Step 3 （337 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。

Step 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、**[ページあたりの行数（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。

Step 4 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

（注） ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

選択した項目がウィンドウに表示されます。

関連トピック

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, on page 348

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

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

Step 2 次のいずれかの操作を行います。

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（336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。

Step 3 「SIP トランク セキュリティ プロファイルの設定」の説明に従って、適切な設定を入力します。

Step 4 [保存（Save）] をクリックします。

セキュリティプロファイルを作成したら、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、SIP トランクを介して接続されているアプリケーションの [**Sip レルム (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 (まだ設定していない場合)。SIP トランクを介して接続されてい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を有効にした場合は、[**アプリケーションユーザ (Application User)**] ウィンドウでアプリケーションに許可されているメソッドを設定する必要があります (まだ実行していない場合)。

関連トピック

SIP トランクセキュリティプロファイルの適用, on page 346
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, on page 348

SIP トランク セキュリティ プロファイルの設定

次の表では、[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] の設定項目について説明します。

表 *40 : SIP* トランク セキュリティ プロファイルの設定項目

設定	説明
名前	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、[トランクの設定（Trunk Configuration）] ウィンドウの [SIP トランク セキュリティ プロファイルの設定（SIP Trunk Security Profile）] ドロップダウンリストにその名前が表示されます。
説明	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
[デバイスセキュリティモード（Device Security Mode）]	ドロップダウンリストから、次のオプションのいずれかを選択します。 • [非セキュア（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 接続で Unified Communications Manager が利用できます。 • [認証済み（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。 • [暗号化（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（Authenticated）]** として選択されている [デバイスセキュリティプロファイル（Device Security Profile）] を使用してトランクを設定した場合、Unified Communications Manager は、NULL_SHA 暗号を使用した TLS 接続（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接続先デバイスでは、トランクを **[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（Device Security Profile）] オプション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。
[Incoming Transport Type]	[デバイスセキュリティモード（Device Security Mode）] が [非セキュア（Non Secure）] の場合、転送タイプは TCP+UDP になります。 [デバイスセキュリティモード（Device Security Mode）] が [認証済（Authenticated）] または [暗号化（Encrypted）] の場合、TLS で転送タイプが指定されます。 （注） Transport Layer Security（TLS）プロトコルによって、 Unified Communications Managerとトランク間の接続が保護されます。

設定	説明
[発信転送タイプ（Outgoing Transport Type）]	ドロップダウン リストから適切な発信転送モードを選択します。 [デバイスセキュリティモード（Device Security Mode）] が [非セキュア（Non Secure）] の場合は、[TCP] または [UDP] を選択します。 [デバイスセキュリティモード（Device Security Mode）] が [認証済（Authenticated）] または [暗号化（Encrypted）] の場合、TLS で転送タイプが指定されます。 （注） TLS により、SIP トランクのシグナリング完全性、デバイス認証、およびシグナリング暗号化が保証されます。 ヒント TCP 接続の再利用をサポートしていない Unified Communications Manager システムと IOS ゲートウェイ間で SIP トランクを接続する場合は、発信トランスポートタイプとして UDP を使用する必要があります。
[ダイジェスト認証の有効化（Enable Digest Authentication）]	ダイジェスト認証を有効にするには、このチェックボックスをオンにします。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、完全性、および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 [認証済（Authenticated）] または [暗号化（Encrypted）] を選択してください。 ヒント TCP または UDP 転送を使用しているトランクでの 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てください。
ナンス確認時間（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 クラスタを使用している場合、または TLS ピアに SRV ルックアップを使用している場合は、1 つのトランクが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、4096 文字まで入力できます。 **ヒント** サブジェクト名は、送信元接続 TLS 証明書に対応します。サブジェクト名とポートごとにサブジェクト名が一意になるようにしてください。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。
[着信ポート（Incoming Port）]	着信ポートを選択します。0 ～ 65535 の範囲の一意のポート番号値を 1 つ入力します。着信 TCP および UDP SIP メッセージのデフォルト ポート値として 5060 が指定されます。着信 TLS メッセージのデフォルトの保護されたSIPポートには5061が指定されます。ここで入力した値は、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、TLS SIP転送トランクと TLS 以外の SIP 転送トランク タイプを混在させることはできません。

設定	説明
[アプリケーション レベル認証を有効化（Enable Application Level Authorization）]	アプリケーション レベルの認証が、SIP トランクを介して接続された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、[ダイジェスト認証を有効化（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 [アプリケーションユーザの設定（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** アプリケーションを信頼性を識別できない場合、または特定のトランクでアプリケーションが信頼されない場合（つまり、予期したものとは異なるトランクからアプリケーション要求が着信する場合）には、アプリケーション レベル認証の使用を考慮してください。
[プレゼンスの SUBSCRIBE の許可（Accept Presence Subscription）]	Unified Communications Manager が SIP トランク経由で着信するプレゼンスサブスクリプション要求を受け付けるようにする場合は、このチェックボックスをオンにします。 [アプリケーション レベル認証を有効化（Enable Application level authorization）] チェックボックスをオンにした場合は、[アプリケーション ユーザの設定（Application User Configuration）] ウィンドウに移動し、この機能に関して許可されるアプリケーション ユーザの [プレゼンスの SUBSCRIBE の許可（Accept Presence Subscription）] チェックボックスをオンにします。 アプリケーション レベルの認証が有効な場合、[プレゼンスの SUBSCRIBE の許可（Accept Presence Subscription）] チェックボックスがアプリケーション ユーザに関してオンに設定され、トランクに関してはオンに設定されない場合、トランクに接続される 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。

設定	説明
Out-of-Dialog REFER の許可（Accept Out-of-dialog REFER）	Unified Communications Manager が SIP トランク経由で着信する非インバイトの Out-of-Dialog REFER 要求を受け付けるようにする場合は、このチェックボックスをオンにします。 [アプリケーション レベル認証を有効化（Enable Application level authorization）] チェックボックスをオンにした場合は、[アプリケーション ユーザの設定（Application User Configuration）] ウィンドウに移動し、この方式に関して許可されるアプリケーション ユーザの [Out-of-Dialog REFER の許可（Accept Out-of-dialog REFER）] チェックボックスをオンにします。
[Unsolicited NOTIFY の許可（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。 [アプリケーション レベル認証を有効化（Enable Application level authorization）] チェックボックスをオンにした場合は、[アプリケーション ユーザの設定（Application User Configuration）] ウィンドウに移動し、この方式に関して許可されるアプリケーション ユーザの [Unsolicited NOTIFY の許可（Accept Unsolicited Notification）] チェックボックスをオンにします。
[ヘッダー置き換えの許可（Accept Replaces Header）]	Unified Communications Manager が既存の SIP ダイアログを置き換える新しい SIP ダイアログを受け付けるようにする場合は、このチェックボックスをオンにします。 [アプリケーション レベル認証を有効化（Enable Application level authorization）] チェックボックスをオンにした場合は、[アプリケーション ユーザの設定（Application User Configuration）] ウィンドウに移動し、この方式に関して許可される [ヘッダー置き換えの許可（Accept Header Replacement）] チェックボックスをオンにします。
[セキュリティ ステータスを送信（Transmit Security Status）]	Unified Communications Manager が、関連付けられた SIP トランクから SIP ピアにコールのセキュリティ アイコン ステータスを送信するようにする場合は、このチェックボックスをオンにします。 デフォルトでは、このボックスはオフになっています。

設定	説明
[SIP V.150アウトバウンドSDPオファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）]	ドロップダウンリストから、次のフィルタ処理オプションのいずれかを選択します。 • [デフォルトのフィルタを使用（Use Default Filter）]：SIP トランクは、[SIP V.150 アウトバウンド SDP オファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）] サービス パラメータで指定されたデフォルト フィルタを使用します。このサービスパラメータを見つけるには、 Cisco Unified Communications Manager Administration で、**[システム（System）] > [サービスパラメータ（Service Parameters）] > [クラスタ全体のパラメータ（デバイス-SIP）（Clusterwide Parameters (Device-SIP)）]** の順に移動します。 • [フィルタなし（No Filtering）]：SIP トランクは、アウトバウンド オファー内の V.150 SDP 行のフィルタリングを実行しません。 • [MER V.150 を削除（Remove MER V.150）]：SIP トランクは、アウトバウンド オファー内の V.150 MER SDP 行を削除します。 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アウトバウンドSDPオファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）]	ドロップダウンリストから、次のフィルタ処理オプションのいずれかを選択します。 • [デフォルトのフィルタを使用（Use Default Filter）]：SIP トランクは、[SIP V.150 アウトバウンド SDP オファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）] サービス パラメータで指定されたデフォルト フィルタを使用します。このサービスパラメータを見つけるには、 Cisco Unified Communications Manager Administration で、**[システム（System）] > [サービスパラメータ（Service Parameters）] > [クラスタ全体のパラメータ（デバイス-SIP）（Clusterwide Parameters (Device-SIP)）]** の順に移動します。 • [フィルタなし（No Filtering）]：SIP トランクは、アウトバウンド オファー内の V.150 SDP 行のフィルタリングを実行しません。 • [MER V.150 を削除（Remove MER V.150）]：SIP トランクは、アウトバウンド オファー内の V.150 MER SDP 行を削除します。 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。MER より前の行を使用するオファーを処理できない MER 準拠デバイスからなるネットワークにクラスタが含まれている場合、あいまいさを減らすには、このオプションを選択します。 （注） セキュアなコール接続を確立するには、V.150 用に SIP で IOS を設定する必要があります。IOS をUnified Communications 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。

関連トピック

認証, on page 30
ダイジェスト認証, on page 28
SIP トランクのダイジェスト認証の設定, on page 349
SIP トランク セキュリティ プロファイルの設定のヒント, on page 336
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, on page 348

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

Step 1 Cisco Unified Communications Manager アドミニストレーション ガイドの説明に従って、トランクを検索します。

Step 2 [**Trunk Configuration**] ウィンドウが表示されたら、[**SIP trunk Security Profile**] の設定を見つけます。

Step 3 **セキュリティプロファイル**の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。

Step 4 [保存（Save）] をクリックします。

Step 5 トランクをリセットするには、[**Apply Config**] をクリックします。
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、トランクの [SIP レルム（SIP Realm）] ウィンドウでダイジェストログイン情報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するプロファイルを適用した場合は、[**アプリケーションユーザ (Application User)**] ウィンドウでダイジェストクレデンシャルと許可された認可方式を設定する必要があります (まだ実行していない場合)。

関連トピック

SIP レルムの設定, on page 353
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, on page 348

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

SIP トランクを設定変更を行った SIP トランクセキュリティプロファイルと同期するには、次の手順を実行します。これにより、最も影響の少ない方法で未処理の設定が適用されます。（たとえば、影響を受けるデバイスの一部では、リセットまたは再起動が不要な場合があります。）

手順

Step 1 **[System] > [Security Profile] > [SIP Trunk Security Profile]** の順に選択します。

Step 2 使用する検索条件を選択します。

Step 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。

Step 4 該当する SIP トランクを同期する 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。

Step 5 追加の設定変更を加えます。

Step 6 [保存（Save）] をクリックします。

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

[設定情報の適用（Apply Configuration Information）] ダイアログが表示されます。

Step 8 [OK] をクリックします。

関連トピック

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, on page 348

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

Step 1 削除する SIP トランクセキュリティプロファイルを検索します。

Step 2 次のいずれかの操作を行います。

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タスクを実行します。

- 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。
- この選択で設定可能なすべてのレコードを削除するには、[すべて選択（Select All）] をクリックして、[選択項目の削除（Delete Selected）] をクリックします。

b) 単一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タスクを実行します。

- 削除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ます。次に、[**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。特定のセキュリティプロファイルの設定ウィンドウが表示されたら、[**選択項目の削除 (Delete Selected)**] をクリックします。

Step 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。

関連トピック

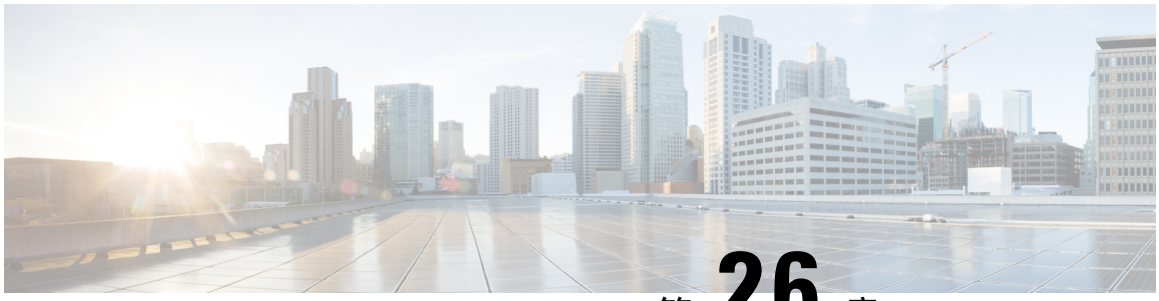
SIP トランクセキュリティプロファイルの検索, on page 336
SIP トランクセキュリティプロファイルに関する詳細情報の入手先, on page 348

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 （30 ページ）
- 連携動作 （10 ページ）
- ダイジェスト認証 （28 ページ）

関連トピック

SIP トランク セキュリティ プロファイルの設定について, on page 335
SIP トランク セキュリティ プロファイルの設定のヒント, on page 336
認証, on page 30
連携動作, on page 10
ダイジェスト認証, on page 28



第 26 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 トランクのダイジェスト認証の仕組みの詳細についてはダイジェスト認証（28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

次の手順では、SIP トランクのダイジェスト認証を設定するタスクについて説明します。

手順

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

関連トピック

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, on page 351
SIP トランクセキュリティプロファイルの適用, on page 346
SIP レルムの設定, on page 353
ダイジェスト認証, on page 28
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, on page 350
ダイジェストクレデンシャルの設定, on page 350
SIP トランク セキュリティ プロファイルの設定, on page 335
SIP レルムの設定項目, on page 353

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、[**エンタープライズパラメータの設定 (Enterprise Parameters Configuration**)] ウィンドウに表示される疑問符をクリックするか、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設定

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

Step 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。

Step 2 アプリケーション ユーザのリンクをクリックします。

Step 3 特定の [**アプリケーションユーザの設定 (Application User Configuration)**] ウィンドウが表示さ表 42 : SIP レルム セキュリティ プロファイル（353 ページ）れたら、の説明に従って適切な設定を入力します。

Step 4 [保存（Save）] をクリックします。

関連トピック

SIP レルムの設定項目, on page 353
SIP トランク ダイジェスト認証に関する詳細情報の入手先

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 *41* : ダイジェスト認証クレデンシャル

設定	説明
ダイジェスト クレデンシャル（Digest Credentials）	英数字の文字列を入力します。
[ダイジェストクレデンシャルの確認（Confirm Digest Credentials）]	[ダイジェストクレデンシャル（Digest Credentials）] の入力が正しいことを確認するために、このフィールドに再度クレデンシャルを入力します。

関連トピック

SIP トランク ダイジェスト認証に関する詳細情報の入手先

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

Step 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）クエリーのレコードも表示されることがあります。

Step 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、Step 3（352 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。

Step 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、**[ページあたりの行数（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。

Step 4 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

（注） ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

選択した項目がウィンドウに表示されます。

次のタスク

まだ実行していない場合は、[Cluster ID] エンタープライズパラメータを設定します。

関連トピック

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, on page 350
SIP トランク ダイジェスト認証に関する詳細情報の入手先

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

Step 1 [Unified Communications Manager Administration] で、**[User Management]** > **[SIP Realm]** を選択します。

Step 2 表 42 : SIP レルム セキュリティ プロファイル（353 ページ）に示すように、適切な設定を入力します。

Step 3 **[保存（Save）]** をクリックします。

Step 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。

関連トピック

SIP レルムの検索, on page 351
SIP トランク ダイジェスト認証に関する詳細情報の入手先

SIP レルムの設定項目

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 *42 : SIP* レルム セキュリティ プロファイル

設定	説明
レルム	SIP トランクに接続するレルムのドメイン名（SIPProxy1_xyz.com など）を入力します。使用できる文字は、英数字、ピリオド、ダッシュ、アンダースコア、およびスペースです。

設定	説明
ユーザ	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。
[ダイジェストクレデンシャルの確認（Confirm Digest Credentials）]	確認のため、パスワードを再入力します。

関連トピック

SIP トランク ダイジェスト認証に関する詳細情報の入手先

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

Step 1 削除する SIP レルムを検索します。

Step 2 次のいずれかの操作を行います。

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タスクを実行します。

- 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。

  この選択で設定可能なすべてのレコードを削除するには、[すべて選択（Select All）]をクリックして、[選択項目の削除（Delete Selected）] をクリックします。

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タスクを実行します。

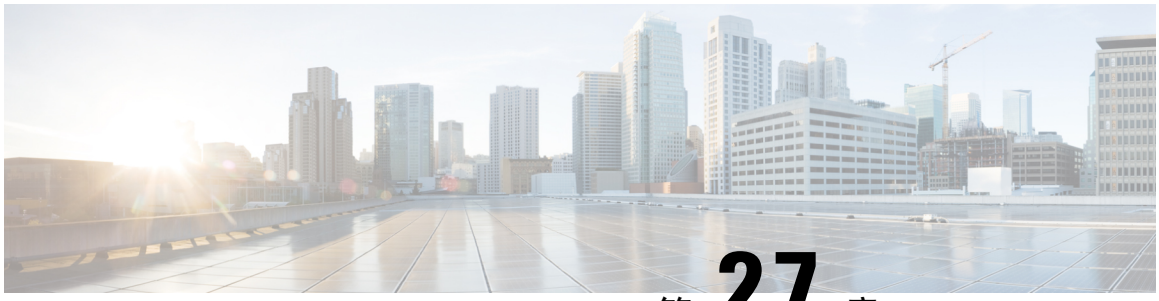
- 削除するレルムの隣にあるチェック ボックスをオンにして、[Delete Selected] をクリックします。

  レルムの [**名前 (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。

Step 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。

関連トピック

SIP レルムの検索, on page 351
SIP トランク ダイジェスト認証に関する詳細情報の入手先



第 27 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 Unity Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルについては、『*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 アドバンテージサーバ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

Step 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）クエリーのレコードも表示されることがあります。

Step 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、Step 3 （358 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。

Step 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、[ページあたりの行数（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。

Step 4 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

（注） ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

選択した項目がウィンドウに表示されます。

関連トピック

Cisco Unified Mobility アドバンテージサーバセキュリティプロファイルに関する詳細情報の入手先, on page 362

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

Step 1 [Unified Communications Manager Administration] で、**[System]** > **[Security Profile]** > **[CUMA Server Security Profile]** を選択します。

Step 2 次のいずれかの操作を行います。

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（357 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（357 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Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定（357 ページ）見つけて、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。

Step 3 XXX の説明に従って、適切な設定を入力します。 表 43 : セキュリティ プロファイルの設定項目（360 ページ）

Step 4 [保存（Save）] をクリックします。

関連トピック

Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの設定項目, on page 360

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの検索, on page 358
Cisco Unified Mobility アドバンテージサーバセキュリティプロファイルに関する詳細情報の入手先, on page 362

Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの設定項目

次の表で、Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの設定項目について説明します。

表 *43*：セキュリティ プロファイルの設定項目

設定	説明
名前	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。
説明	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。
[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 ボックスから、次のいずれかのオプションを選択します。 • **[非セキュア（Non Secure）]**：イメージ認証を除くセキュリティ機能は Cisco Unified Mobility Advantage サーバに適用されていません。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。シグナリングに対して AES128/SHA を使用する TLS 接続が開き、SRTP はすべてのモバイル コールに対してメディアを伝送します。

設定	説明
[転送タイプ（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、パケットが送信したとき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。 [デバイス セキュリティ モード（Device Security Mode）] が **[認証済み（Authenticated）]** または **[暗号化（Encrypted）]** の場合、TLS では [転送タイプ（Transport Type）] を指定します。TLS は、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（暗号化モードに限る）を提供します。
安全な証明書の件名またはサブジェクトの別名	（[デバイス セキュリティ モード（Device Security Mode）] が [認証済み（Authenticated）] または [暗号化（Encrypted）] の場合にのみ、必須。）このフィールドは、転送タイプとして TLS を選択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、4096 文字まで入力できます。

関連トピック

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの検索, on page 358
詳細情報の入手先, on page 61

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。

関連トピック

Cisco Unified Mobility アドバンテージサーバセキュリティプロファイルに関する詳細情報の入手先, on page 362

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

Step 1 削除するセキュリティ プロファイルを探します。

Step 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、適切な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ます。次に、[**Delete Selected**] をクリックします。

Step 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。

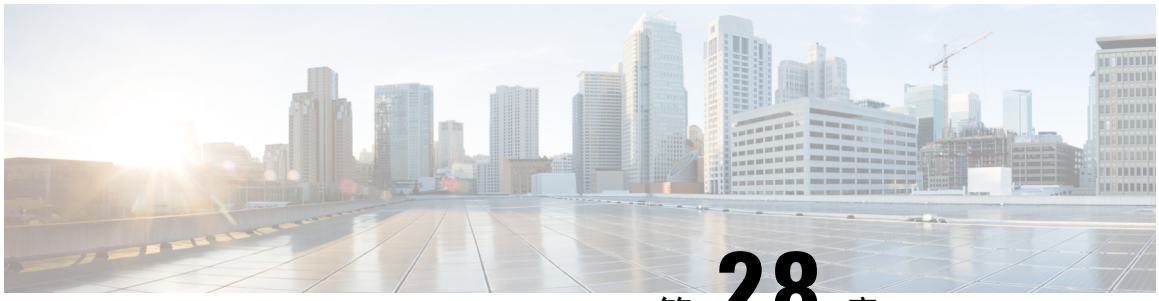
関連トピック

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの検索, on page 358
Cisco Unified Mobility アドバンテージサーバセキュリティプロファイルに関する詳細情報の入手先, on page 362

Cisco Unified Mobility アドバンテージサーバセキュリティプロファイルに関する詳細情報の入手先

関連トピック

Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルについて, on page 357
Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの設定項目, on page 360



第 28 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 140-2 の設定

⚠

注意 FIPS モードは、FIPS 準拠のリリースだけでサポートされます。Unified Communications Managerの FIPS 非準拠のバージョンにアップグレードする前に、必ず FIPS モードを無効にしてください。

FIPS 準拠のリリースと、そのリリースの証明書を確認するには、https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html の *FIPS 140* のドキュメントを参照してください。

連邦情報処理標準（FIPS）は、米国およびカナダ政府の認証規格です。暗号化モジュールで順守する必要がある要件が規定されています。

Unified Communications Manager の特定のバージョンは、米国の National Institute of Standards（NIST）に従って FIPS 140-2 に準拠しています。これらは FIPS モード、レベル 1 に準拠して動作できます。

Unified Communications Manager

- 再起動
- スタートアップ時に認定のセルフテストを実行する
- 暗号モジュールの整合性チェックを実行する
- キー情報を再生成する

FIPS 140-2 モードを有効にすると、この時点で、Unified Communications Manager は FIPS 140-2 モードで動作しています。

FIPS の要件には、次のものが含まれます。

- スタートアップ時のセルフテストの実行
- 一連の承認済み暗号機能に対する制限

FIPS モードでは、次の FIPS 140-2 レベル 1 検証済み暗号化モジュールが使用されます。

- CiscoSSL 1.0.2n.6.2.194 with FIPS Module CiscoSSL FOM 6_2_0
- CiscoJ 5.2.1
- RSA CryptoJ 6_2_3
- Openssh 7.5.9
- Libreswan
- NSS

次の FIPS 関連作業を実行できます。

- FIPS 140-2 モードの有効化
- FIPS 140-2 モードの無効化
- FIPS 140-2 モードのステータスの確認

（注）
- デフォルトでは、システムは非FIPSモードになっているため、有効にする必要があります。
- クラスタ上で FIPS、コモンクライテリア、または強化されたセキュリティモードにアップグレードする前に、セキュリティパスワードの長さが最小 14 文字である必要があります。旧バージョンが FIPS を有効にしていた場合でもパスワードを更新します。

FIPSモードで自己署名証明書または証明書署名要求（CSR）を生成する場合は、SHA256ハッシュアルゴリズムを使用して証明書を暗号化する必要があり、SHA1 を選択できません。

IPsec の要件

このリリースでは、Libreswanライブラリサポートは、IPsecのOpenswanライブラリのサポートに置き換えられています。このサポートには、既存の機能に対する変更はありません。

証明書ベースの認証を Libreswan ライブラリで機能させるには、送信元と宛先の両方の証明書が CA 署名付き証明書である必要があります。さらに、同じ認証局 (CA) がこれらの証明書に署名する必要があります。Libreswan ライブラリへの移行には、次の制限事項があります。

- 自己署名証明書を使用した証明書ベースの認証を使用してIPsecが設定されているユニファイドコミュニケーションマネージャをアップグレードすると、アップグレードは失敗します。アップグレードを正常に実行するには、CA 署名付き証明書を使用して IPsec ポリシーを再設定します。

- 証明書ベースの認証を使用しており、IPsecを設定するために自己署名証明書を使用している場合、IPsec は動作を停止します。
- 証明書ベースの認証を使用しており、IPsec を設定するための送信元と宛先に対して異なる CA で署名された CA 署名付き証明書を使用している場合、IPsec は動作を停止します。
- Unified Communications Manager では、DH グループ キー値が 1、2、または 5 の IPsec ポリシーは無効になっています。ただし、DH グループキー値 1、2、または 5 を使用して IPSec ポリシーを設定し、FIPS モードが有効になっている場合は、ユニファイド コミュニケーション マネージャへのアップグレードがブロックされます。

FIPS 140-2 モードの有効化

Unified Communications Managerで FIPS 140-2 モードを有効にする前に、次の点を検討してください。

- 非 FIPS モードから FIPS モードに切り替えた場合は、MD5 および DES プロトコルは機能しません。
- 単一サーバクラスタでは、証明書が再生成されるため、FIPS モードを有効にする前に、CTL クライアントを実行するか、または [Prepare Cluster for Rollback to pre-8.0] エンタープライズ パラメータを適用する必要があります。これらの手順のいずれかを実行しない場合は、FIPS モードを有効にした後に手動で ITL ファイルを削除する必要があります。
- クラスタでは、すべてのノードが FIPS モードまたは非 FIPS モードである必要があります。異なるモードの各ノードは許可されません。たとえば、FIPS モードのノード A と非 FIPS モードのノード B は許可されません。
- FIPS モードをサーバで有効にした後は、サーバがリブートし、電話が正常に再登録されるまで待機してから、次のサーバで FIPS を有効にしてください。

⚠

注意 FIPS モードを有効にする前に、システム バックアップを実行することを強く推奨します。FIPS のチェックが起動時に失敗した場合は、システムが停止し、復元するにはリカバリ CD が必要になります。

手順

Step 1 CLI セッションを開始します。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の「「CLI セッションの開始」」セクションを参照してください。

Step 2 CLI で **utils fips enable** を入力します。

14 文字未満のパスワードを入力すると、次のプロンプトが表示されます。

```
FIPS、コモンクライテリア、強化されたセキュリティモードなどのセキュリティモードを有効にするには、クラスタセキュリティパスワードは 14 文字以上使用する必要があります。すべてのノードで「set password user security」CLI コマンドを使用してクラスタ セキュリティ パスワードを更新し、このコマンドを再試行します。
**************************************************************************
 コマンドの実行に失敗しました（Executed command unsuccessfully）
```

14 文字を超えるパスワードを入力すると、次のプロンプトが表示されます。

```
セキュリティ警告：この操作により、1)CallManager 2)Tomcat 3)IPsec 4)TVS 5)CAPF 6)SSH 7)ITLRecovery の証明書が再生成されます。上記のコンポーネント用にアップロードされたサードパーティの CA 署名付き証明書を再アップロードする必要があります。（The operation will regenerate certificates for 1)CallManager 2)Tomcat 3)IPsec 4)TVS 5)CAPF 6)SSH 7)ITLRecovery Any third party CA signed certificates that have been uploaded for the above components will need to be re-uploaded.）システムが混合モードで動作している場合は、ctl ファイルを更新するために CTL クライアントを再実行する必要があります。クラスタ内に他のサーバがある場合は、このノードの FIPS 操作が完了してシステムがバックアップおよび実行されるまで待機して、他のノードの FIPS 設定を変更しないでください。エンタープライズパラメータの [TFTP ファイル署名アルゴリズム（TFTP File Signature Algorithm）] に Unified Communications Manager の現行バージョンの FIPS 準拠ではない値 [SHA-1] が設定されている場合は、完全に FIPS にするために、パラメータ値を SHA-512 に変更することを推奨します。SHA-512 を署名アルゴリズムとして設定するには、クラスタにプロビジョニングされているすべての電話機が SHA-512 署名付き設定ファイルを検証できる必要がある場合があります。そうでない場合、電話機の登録が失敗する可能性があります。詳細については、『Cisco Unified Communications Manager Security Guide』を参照してください。これにより、システムが FIPS モードに変更され、再起動します。
********************************************************************************** 警告：続行したら、Ctrl+C キーを押さないでください。開始後にこの操作をキャンセルすると、システムは一貫性のない状態になります。リカバリするには、システムをリーブートし、「utils fips status」を実行する必要があります。（Once you continue do not press Ctrl+C. Canceling this operation after it starts will leave the system in an inconsistent state; rebooting the system and running "utils fips status" will be required to recover.）
**********************************************************************************
Do you want to continue (yes/no)?
```

Step 3 **Yes** と入力します。

次のメッセージが表示されます。

```
証明書を生成しています...オペレーティングシステムで FIPS モードを設定しています。FIPS mode enabled successfully. システムのバックアップが実行されると、システムを再起動した後に、これを強くお勧めします。システムは数分で再起動します。
```

Unified Communications Manager が自動的にリブートされます。

（注）
- 証明書および SSH キーは、FIPS 要件に応じて、自動的に再生成されます。
- 単一のサーバ クラスタを使用しており、[Prepare Cluster for Rolback to pre 8.0] エンタープライズ パラメータを適用してから FIPS 140-2 モードを有効にした場合は、すべての電話がサーバに正常に登録されたことを確認してから、このエンタープライズ パラメータを無効にする必要があります。

（注） FIPS モードでは、Unified Communications Manager は Racoon 検証済み（非 FIPS 検証）の代わりに、Libreswan（FIPS 検証済）を使用します。Raccoon のセキュリティポリシーに、FIPS で承認されていない機能が含まれている場合、CLI コマンドは、FIPS で承認された機能を使用してセキュリティポリシーを定義し直すよう表示して中止されます。詳細については、Cisco Unified Communications Manager アドミニストレーション ガイドの「IPsec の管理」に関連するトピックを参照してください。

FIPS 140-2 モードの無効化

FIPS 140-2 モードを Unified Communications Manager で無効にする前に、次の点を考慮してください。

- 単一または複数のサーバクラスタでは、CTL クライアントを実行することを推奨します。CTL クライアントが単一のサーバクラスタで実行されていない場合は、FIPS モードを無効にした後で、手動で ITL ファイルを削除する必要があります。
- 複数サーバのクラスタでは、各サーバを個別に無効にする必要があります。これは、FIPS モードはクラスタ全体ではなくサーバごとに無効になるためです。

FIPS 140-2 モードを無効にするには、次の手順を実行します。

手順

Step 1 CLI セッションを開始します。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の「Starting a CLI Session」の項を参照してください。

Step 2 CLI で、**utils fips disable** と入力します。

Unified Communications Manager がリブートされ、非 FIPS モードに戻ります。

（注） 証明書と SSH キーは自動的に再生成されます。

FIPS 140-2 モードのステータス確認

FIPS 140-2 モードが有効になっているかどうかを確認するには、CLI からモードステータスを確認します。

FIPS 140-2 モードのステータスを確認するには、次の手順を実行します。

手順

Step 1 CLI セッションを開始します。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の「Starting a CLI Session」の項を参照してください。

Step 2 CLI に **utils fips status** と入力します。

FIPS 140-2 モードが有効になっていることを確認するために、次のメッセージが表示されます。

```
admin: システムが FIPS モードで動作している状態の fips ステータス。自己診断テストのステータス:-S T A R T----------------------FIPS selftests ランの実行時間が N 3 の開始時刻: Thu Apr 28 15:59:24 PDT 2011 NSS の自己診断テストが成功しました。カーネル暗号テストに合格しました。オペレーティングシステムの OpenSSL 自己診断テストに合格しました。Libreswan 自己診断テストに合格しました。OpenSSL の自己診断テストに合格しました。CryptoJ 自己診断テストに合格しました...
```

FIPS 140-2 モードサーバのリブート

FIPS 140-2 モードで Unified Communications Manager サーバがリブートすると、リブート後に各 FIPS 140-2 モジュールで FIPS のスタートアップ時のセルフテストがトリガーされます。

注意 これらのセルフテストのいずれかが失敗すると、Unified Communications Managerサーバが停止します。

（注） 対応する CLI コマンドを使用して FIPS を有効または無効にすると、Unified Communications Manager サーバが自動的に再起動されます。リブートを開始することもできます。

注意 一時的なエラーによってスタートアップセルフテストに失敗した場合は、 Unified Communications Managerサーバの再起動によって問題が修正されます。ただし、起動時のセルフテスト エラーが解消されない場合は、FIPS モジュールに重大な問題があるため、リカバリ CD の使用が唯一の選択肢となります。

強化されたセキュリティ モード

強化されたセキュリティモードはFIPS対応システムで稼働します。強化されたセキュリティモードで動作するために、Unified Communications Manager と IM and Presence Service の両方を有効にすることで、次のセキュリティとリスク管理制御を備えるシステムを有効にすることができます。

- ユーザのパスワードとパスワードの変更に関して厳格化されたクレデンシャル ポリシーが適用されます。
- デフォルトでは、連絡先検索の認証機能が有効です。
- リモート監査ログ用のプロトコルが TCP または UDP に設定されている場合は、デフォルトのプロトコルが TCP に変更されます。リモート監査ログのプロトコルが TLS に設定されている場合、デフォルトのプロトコルは TLS のままです。コモン クライテリア モードでは、厳密なホスト名検証が使用されます。そのため、サーバには、証明書と一致する完全修飾ドメイン名（FQDN）を設定する必要があります。

Unified Communications Manager が FIPS モードの場合、バックアップデバイスとして設定するデバイスは FIPS 準拠である必要があります。キー交換アルゴリズム**diffie-hellman-group1-sha1**は FIPS モードではサポートされていません。非 FIPS モードのUnified Communications Manager で **diffie-hellman-group1-sha1** アルゴリズムを設定すると、FIPS モードを有効にすると、このアルゴリズムは SSH キー交換から自動的に削除されます。

クレデンシャル ポリシーの更新

強化されたセキュリティモードを有効にすると、新しいユーザパスワードとパスワード変更に関してより厳格なクレデンシャルポリシーが有効になります。強化されたセキュリティモードを有効にした後で、管理者は一連の CLI コマンド **set password ***** を使用して、次の要件のいずれかを変更できます。

- パスワードの長さは 14 ～ 127 文字です。
- パスワードには少なくとも 1 つの小文字、1 つの大文字、1 つの数字 および 1 つの特殊文字が含まれている必要があります。
- 過去 24 回以内に使用したパスワードを再使用することはできません。
- パスワードの最短有効期間は 1 日、最長有効期間は 60 日です。
- 新たに生成されるパスワードの文字列では、古いパスワードの文字列と少なくとも 4 文字が異なる必要があります。

強化されたセキュリティ モードの設定

強化されたセキュリティ モードを有効にする前に、FIPS を有効にしてください。

すべての Unified Communications Manager または IM and Presence Service クラスタノードでこの手順を使用して、強化されたセキュリティモードを設定します。

（注） 拡張セキュリティモードを有効にした後で、Unified Communications Manager パブリッシャのパスワードを変更する場合は、IM and Presence Service パブリッシャのサービスが「STARTED」状態（「Cisco IM and Presence Data Monitor」サービスおよび SyncAgent）であることを確認する必要があります。

手順

Step 1 コマンドライン インターフェイスにログインします。

Step 2 **utils EnhancedSecurityMode status** コマンドを実行し、強化されたセキュリティモードが有効であるかどうかを確認します。

Step 3 Unified Communications Manager クラスタノードで次のいずれかのコマンドを実行します。

- 強化されたセキュリティ モードを有効にするには、**utils EnhancedSecurityMode enable** コマンドを実行します。
- 強化されたセキュリティ モードを無効にするには、**utils EnhancedSecurityMode disable** コマンドを実行します。

Step 4 拡張セキュリティモードを有効にした後、Cisco Unified CM の管理ユーザインターフェイスで、14 文字を含む新しいパスワードに変更します。

Unified Communications Manager パブリッシャで拡張セキュリティモードを有効にした後、次の手順を実行します。

1. Unified Communications Manager サブスクライバで拡張セキュリティモードを有効にします。
2. IM and Presence Service パブリッシャで拡張セキュリティモードを有効にします。
3. IM and Presence Service サブスクライバで拡張セキュリティモードを有効にします。

（注） **utils EnhancedSecurityMode enable** CLI コマンドまたは **utils EnhancedSecurityMode disable** CLI コマンドをすべてのノードで同時に実行しないでください。

コモン クライテリア モード

コモンクライテリアモードでは、Unified Communications Manager と IM and Presence Service サービスの両方がコモンクライテリアのガイドラインに準拠できます。コモンクライテリアモードは、各クラスタ ノードで次に示す CLI コマンドを使用して設定できます。

- ユーティリティ `fips_common_criteria` 有効
- ユーティリティ `fips_common_criteria disable`
- ユーティリティ `fips_common_criteria` ステータス

コモン クライテリア構成のタスク フロー

- 一般的な基準モードを有効にするには、FIPS モードが実行されている必要があります。FIPS がまだ有効になっていない場合、コモンクライテリアモードを有効にしようとすると FIPS を有効にするよう求められます。FIPS を有効にすると、証明書を再生成する必要があります。詳細については、FIPS 140-2 モードの有効化 （365 ページ）を参照してください。
- コモンクライテリアモードでは、証明書ベースの IPSec ポリシーの IPSec ポリシーを設定する前に、クラスタおよびノード間で証明書交換操作が必須です。
- X.509 v3 証明書は、共通基準モードで必要です。X.509 v3 証明書は、次の通信プロトコルとして TLS 1.2 を使用する場合にセキュアな接続を有効にします。
  - リモート監査ログ
  - FileBeat クライアントと logstash サーバ間の接続を確立しています。

Unified Communications Manager と IM and Presence Service をコモンクライテリアモードに設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
Step 1	TLSの有効化 （371 ページ）	TLS は、共通基準モードを設定するための前提条件です。
Step 2	コモン クライテリア モードの構成 （372 ページ）	Unified Communications Manager と IM and Presence Service のすべてのクラスタノードでコモンクライテリアモードを設定します。

TLSの有効化

TLS 1.2 バージョンまたは TLS バージョン1.1 は、共通基準モードの要件です。TLS バージョン1.0 を使用したセキュア接続は、共通基準モードを有効にした後は許可されません。

- TLS 接続の確立中に、ピア証明書の`Extendedkeyusage`拡張機能が適切な値についてチェックされます。
  - ピアがサーバの場合、ピア証明書には、 `Extendedkeyusage`拡張機能として`serverauth`が必要です。
  - ピアがクライアントである場合、ピア証明書には、 `Extendedkeyusage`拡張として`clientauth`が必要です。

`Extendedkeyusage`拡張がピア証明書に存在しない場合、または正しく設定されていない場合は、接続が閉じられます。

TLS バージョン 1.2 をサポートするには、次の手順を実行します。

手順

Step 1 Soap UI バージョン5.2.1 をインストールします。

Step 2 Microsoft Windows プラットフォームで実行している場合は、次のようにします。

a) `C:\Program Files\SmartBear\SoapUI-5.2.1\bin`に移動します。

b) `] Vmoptions]`ファイルを編集して、追加`-dsoapui. https. プロトコル = tlsv 1.2、TLSv1、SSLv3`を編集し、ファイルを保存します。

Step 3 Linux で実行している場合は、`bin/soaup. sh`ファイルを編集して`JAVA_OPTS = "$JAVA _OPTS-dsoapui. https. プロトコル = SSLv3, tlsv 1.2"`を追加し、ファイルを保存します。

Step 4 OSX を実行している場合は、次のようになります。

a) [アプリケーション (applications)]/[コンテンツ `(Contents)`] に移動します。

b) `] Vmoptions]`を編集して、追加`-dsoapui. https. プロトコル = tlsv 1.2、TLSv1、SSLv3`を編集し、ファイルを保存します。

Step 5 SoapUI ツールを再起動し、AXL テストを続行します。

コモン クライテリア モードの構成

Unified Communications Manager と IM and Presence Service サービスのコモンクライテリアモードを設定するには、次の手順を使用します。

手順

Step 1 コマンドライン インターフェイス プロンプトにログインします。

Step 2 `utils fips_common_criteria status` コマンドを実行し、システムがコモンクライテリアモードで実行されているかどうかを確認します。

Step 3 クラスタ ノードで次のいずれかのコマンドを実行します。

- 共通基準モードを有効にするには、[コマンドユーティリティ `(enable)`] fips_common_criteria 実行します。
- 共通基準モードを無効にするには、[コマンドユーティリティ `(disable)`] fips_common_criteria 実行します。

  共通基準モードが無効になっている場合は、最小 TLS バージョンを設定するためのプロンプトが表示されます。

（注） これらのコマンドをすべてのノードで同時に実行しないでください。

Step 4 単一のクラスタ全体でコモンクライテリアモードを有効にするには、すべてのUnified Communications Manager および IM and Presence Service クラスタノードでこの手順を繰り返します。

（注）
- CTL クライアントは TLS 1.1 プロトコルと TLS 1.2 プロトコルをサポートしていないので、サーバがコモンクライテリアモードである場合、CTL クライアントはUnified Communications Managerノードに接続しません。
- 一般的な基準モードでは、TLS 1.1 または TLS 1.2 (DX シリーズおよび 88 XX シリーズの電話機など) をサポートする電話機モデルのみがサポートされています。7975や9971などの TLSv 1.0 のみをサポートする電話機モデルは、共通基準モードではサポートされていません。
- 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。

Step 5 ノード間で ICSA がすでに設定されているマルチクラスタ設定で共通基準モードを有効にするには、次の順序で各ノードの共通基準モードを有効にします。

1. Unified Communications Manager - クラスタ 1（パブリッシャ）
2. IM and Presence Service - クラスタ 1（パブリッシャ）
3. IM and Presence Service - クラスタ 1（1 つ以上のサブスクライバ）
4. Unified Communications Manager - クラスタ 2（パブリッシャ）
5. IM and Presence Service - クラスタ 2（パブリッシャ）
6. IM and Presence Service - クラスタ 2（1 つ以上のサブスクライバ）

Step 6 証明書の同期に失敗した場合は、次を参照してください。

CiscoSSH サポート

Unified Communications Manager は CiscoSSH をサポートします。システムで FIPS モードを有効にすると、CiscoSSH は自動的に有効になります。追加設定は不要です。

CiscoSSH サポート

CiscoSSH は、次のキー交換アルゴリズムをサポートします。

- **Diffie-Hellman-Group14-SHA1**
- **Diffie-Hellman-Group-Exchange-SHA256**

- **Diffie-Hellman-Group-Exchange-SHA1**

CiscoSSH は、Unified Communications Manager サーバで次の暗号をサポートしています。

- **AES-128-CTR**
- **AES-192-CTR**
- **AES-256-CTR**
- **AES-128-GCM@openssh.com**
- **AES-256-GCM@openssh.com**
- **AES-128-CBC**（リリース 12.0(1) 以降をサポート）
- **AES-192-CBC**（リリース 12.0(1) 以降をサポート）
- **AES-256-CBC**（リリース 12.0(1) 以降をサポート）

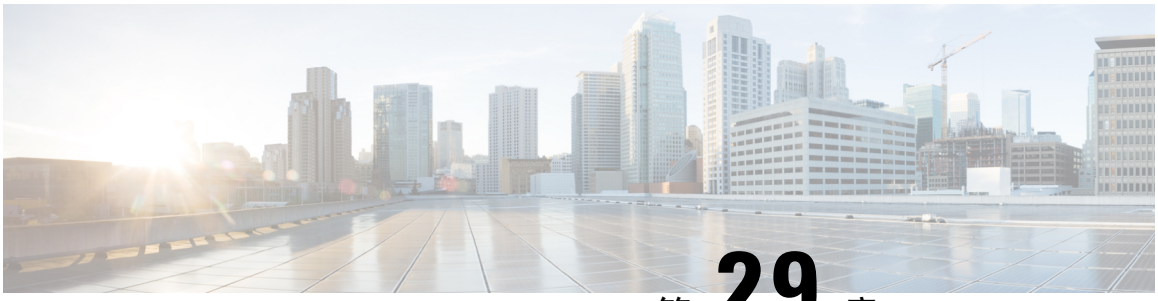
CiscoSSH は、クライアントの次の暗号方式をサポートします。

- **AES-128-CTR**
- **AES-192-CTR**
- **AES-256-CTR**
- **AES-128-GCM@openssh.com**
- **AES-256-GCM@openssh.com**
- **AES-128-CBC**
- **AES-192-CBC**
- **AES-256-CBC**

FIPS モードの制約事項

機能	機能制限
SNMP v3	FIPS モードでは、MD5 または DES を使用した SNMP v3 はサポートされていません。FIPS モードが有効になっているときに SNMP v3 が設定されている場合は、認証プロトコルとして**SHA**を設定し、プライバシープロトコルとして**AES128**を設定する必要があります。
証明書のリモート登録	FIPS モードでは、証明書のリモート登録はサポートされていません。

機能	機能制限
SFTP サーバ	デフォルトでは、JSCH ライブラリは SFIPS 接続に ssh-rsa を使用していましたが、FIPS モードは ssh-rsa をサポートしません。CentOS の最近の更新により、JSCH ライブラリは、変更後の FIPS 値に応じて 、**ssh-rsa**（SHA1withRSA）または **rsa-sha2-256**（SHA256withRSA）の両方をサポートします。具体的には、次の選択を行います。 （注） • FIPS モードは **rsa-sha2-256** のみをサポートします。 • 非 FIPS モードは、ssh-rsa と **rsa-sha2-256** の両方をサポートします。 **rsa-sha2-256**（SHA256WithRSA）のサポートは OpenSSH 6.8 バージョン以降でのみ利用可能です。FIPS モードでは、OpenSSH 6.8 バージョン以降で実行されている SFIPS サーバだけが **rsa-sha2-256**（SHA256WithRSA）をサポートします。



第 29 章

Cisco V.150 Minimum Essential Requirements（MER）

V.150 の概要

「V. 150 最低必須要件」機能を使用すると、IP ネットワーク経由のモデムで安全なコールを行うことができます。この機能では、ダイヤルアップモデムを使用して、従来の公衆交換電話網(PSTN)上で動作するモデムとテレフォニーデバイスを大規模に設置します。V.150.1 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。呼制御システムの設定方法については、Cisco Unified Communications Manager システム設定ガイドを参照してください。

Unified Communications Manager の場合、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 に V.150 サポートを追加するには、次のタスクを完了します。

手順

	コマンドまたはアクション	目的
Step 1	メディア リソース グループ設定のタスク フロー（379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 （380 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（381 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（381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 （382 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。
Step 2	Cisco V.150（MER）に対応したゲートウェイの設定 （382 ページ）	ゲートウェイにV.150機能を追加します。

	コマンドまたはアクション	目的
Step 3	V.150 MGCP ゲートウェイ ポート インターフェイスの設定 （383 ページ）	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。
Step 4	V.150 SCCP ゲートウェイ ポート インターフェイスの設定 （384 ページ）	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。
Step 5	電話での V.150 サポートの設定 （384 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。
Step 6	SIP トランク設定のタスク フロー （385 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。 • V.150 の SIP プロファイルの設定 （386 ページ） • クラスタ全体の V.150 フィルタの設定 （386 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 （387 ページ） • V.150 の SIP トランクの設定 （388 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。
Step 7	V.150 MER 機能を使用するには、この機能をサポートするようにゲートウェイで IOS を設定する必要もあります。	IOS ゲートウェイ設定の詳細については、http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t4/mer_cg_15_1_4M.html を参照してください。

メディア リソース グループ設定のタスク フロー

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。呼制御システムの設定方法については、Cisco Unified Communications Manager システム設定ガイドを参照してください。

Unified Communications Manager の場合、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 の場合、最小バージョンは 11.0(1) SU2 です。
- 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。

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
Step 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 （380 ページ）	V.150 以外のエンドポイントに対して、MTP を使用してメディアリソースグループを設定できます。
Step 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 （381 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。
Step 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 （381 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。
Step 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 （382 ページ）	セキュアV.150エンドポイントに必要なリソースをメディアリソースグループに追加した後で、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

Step 1 Cisco Unified Communications Manager Administrationから、**[メディアリソース（Media Resources）]** > **[メディアリソースグループ（Media Resource Group）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 **[名前(Name)]** フィールドに、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。

Step 4 [使用可能なメディア リソース（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。
選択したデバイスが **[選択したメディアリソース (selected Media Resources)]** フィールドに表示されます。

Step 5 [保存（Save）] をクリックします。

非 V.150 エンドポイントのメディア リソース グループ リストの設定

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 （380 ページ）

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。

手順

Step 1 Cisco Unified Communications Manager Administrationから、**[メディアリソース（Media Resources）]** > **[メディアリソースグループリスト（Media Resource Group List）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 **[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。

Step 4 [使用可能なメディアリソース（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。
選択したデバイスが **[選択したメディアリソース (selected Media Resources)]** フィールドに表示されます。

Step 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

Step 1 Cisco Unified Communications Manager Administrationから、**[メディアリソース（Media Resources）]** > **[メディアリソースグループ（Media Resource Group）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 **[名前(Name)]** フィールドに、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。

Step 4 [使用可能なメディアリソース（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。
選択したデバイスが **[選択したメディアリソース (selected Media Resources)]** フィールドに表示されます。

Step 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 リストの設定

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（381 ページ）

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。

手順

Step 1 Cisco Unified Communications Manager Administrationから、**[メディアリソース（Media Resources）]** > **[メディアリソースグループリスト（Media Resource Group List）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 **[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。

Step 4 [使用可能なメディアリソース（Available Media Resources）] フィールドで、[V.150 デバイス用（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。

Step 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

Cisco V.150（MER）のゲートウェイを設定するには、次の手順を使用します。

手順

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

Step 2 [新規追加（Add New）] をクリックします。

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

Step 4 [次へ（Next)] をクリックします。

Step 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。

Step 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。

Step 7 **[Unified Communications Manager Group]** ドロップダウン リストから **[Default]** を選択します。

Step 8 [設定済みのスロット、VIC、およびエンドポイント（Configured Slots、VICs and Endpoints）] 領域で次の手順を実行します。

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

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

c) [保存（Save）] をクリックします。
ポートアイコンが表示されます。各**ポートアイコン**は、ゲートウェイで利用可能な**ポートインターフェイス**に対応します。対応する**ポートアイコン**をクリックすることによって、任意の**ポートインターフェイス**を設定できます。

Step 9 [ゲートウェイの設定（Gateway Configuration）] ウィンドウでその他のフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 10 [保存（Save）] をクリックします。

V.150 MGCP ゲートウェイ ポート インターフェイスの設定

V.150 MGCP ゲートウェイ ポート インターフェイスを設定するには、次の手順を使用します。

手順

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

Step 2 既存のゲートウェイの設定を変更するための検索条件を入力し、[Find] をクリックします。

Step 3 [設定されたスロット、VIC およびエンドポイント（Configured Slots, VICs, and Endpoints）] 領域で、V.150 MER 用のポートを設定するモジュールとサブユニットを見つけ、該当するポートアイコンをクリックします。

Step 4 [Device Protocol] ドロップダウンリストから [Digital Access T1] または [Digital Access PRI] を選択し、[Next] をクリックします。

（注） [Device Protocol] ドロップダウンリストが表示されるのは、[Configured Slots、VICs、and Endpoints] 領域で T1 ポートが選択されている場合だけです。

[Gateway Configuration] ウィンドウにポート インターフェイス設定が表示されます。

Step 5 **「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。

Step 6 [V150 (subset)] チェックボックスをオンにします。

Step 7 必要に応じて残りのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

Step 9 （任意）ゲートウェイで追加のポート インターフェイスを設定するには、[Related Links] ドロップダウンリストから [Back to MGCP Configuration] を選択し、[Go] をクリックします。異なるポートインターフェイスを選択できます。

V.150 SCCP ゲートウェイ ポート インターフェイスの設定

V.150 SCCP ゲートウェイ ポート インターフェイスを設定するには、次の手順を使用します。

手順

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

Step 2 既存の SCCP ゲートウェイの設定を変更するための検索条件を入力し、[Find] をクリックします。

Step 3 [設定されたスロット、VIC およびエンドポイント（Configured Slots, VICs, and Endpoints）] 領域で、V.150 MER 用のポートを設定するモジュールとサブユニットを見つけ、該当するポートアイコンをクリックします。

Step 4 「**「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。

Step 5 **[Product Specific Configuration Layout]** 領域で **[Latent Capability Registration Setting]** ドロップダウンリストが表示される場合は、**[Modem Relay]** または **[Modem Relay and Passthrough]** を選択します。

Step 6 必要に応じて残りのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 7 [保存（Save）] をクリックします。

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

手順

Step 1 必須: 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ます。

Step 2 必須: 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 [ダイジェストログイン情報（Digest Credentials）] フィールドを設定します。

新しいエンドユーザの設定方法の詳細については、の「「エンドユーザの手動プロビジョニング」」の章を参照してください。Cisco Unified Communications Manager システム設定ガイド

Step 3 Cisco Unified Communications Manager Administrationから、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

Step 4 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。

Step 5 [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。

Step 6 Cisco 7962 として登録されたサードパーティの SCCP エンドポイントの場合は、[デバイスプロトコル（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。

Step 7 **[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。

Step 8 サードパーティの AS-SIP SIP エンドポイントの場合のみ、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。

Step 9 [保存（Save）] をクリックします。

Step 10 [設定の適用（Apply Config）] をクリックします。

Step 11 [OK] をクリックします。

SIP トランク設定のタスク フロー

SIP トランクタスクフローを設定するには、次の手順を使用します。

手順

	コマンドまたはアクション	目的
Step 1	V.150 の SIP プロファイルの設定（386 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。

	コマンドまたはアクション	目的
Step 2	クラスタ全体のV.150フィルタの設定（386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。
Step 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（387 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。
Step 4	V.150 の SIP トランクの設定（388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

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

Step 2 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。

Step 3 [名前(Name)] フィールドに、V.150 の SIP 名を入力します。

Step 4 [説明（Description)] フィールドに、V.150 の説明を入力します。

Step 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。

Step 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。

Step 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

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

Step 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。

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

Step 4 [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。

Step 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。

Step 6 目的のフィルタリング アクションを指定します。

Step 7 [保存（Save）] をクリックします。

SIP トランク セキュリティ プロファイルへの 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。

手順

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

Step 2 次のいずれかの操作を行います。

- 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。

Step 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。

Step 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。

Step 5 [保存（Save）] をクリックします。

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。

手順

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

Step 2 次のいずれかの手順を実行します。

- 新しいプロファイルを作成するには、[Add New] をクリックします。
- 既存のトランクを選択するには、**[検索（Find）]** をクリックして SIP トランクを選択します。

Step 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。

Step 4 [名前(Name] フィールドに SIP トランク名を入力します。

Step 5 [説明(Description)] フィールドに SIP トランクの説明を入力します。

Step 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。

Step 7 SIP トランクの宛先アドレスを設定します。

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

b) 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) 接続先を追加するには、[+] 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。

Step 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。

Step 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。

Step 10 [Media Termination Point Required] チェックボックスはオフのままにします。

Step 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。

Step 12 [保存（Save）] をクリックします。

INDEX

C

E

H

I

J

M

N

S

T