Cisco Unified Communications Manager
セキュリティ ガイド

Cisco Unified Communications Manager Security Guide

リリース 8.5(1)

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco および Cisco ロゴは、米国シスコシステムズ社や米国および他の国の関連会社の商標です。シスコの商標の一覧は、www.cisco.com/go/trademarks で参照できます。本書に記載されているサードパーティの商標は、それぞれの所有者の財産です。「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1005R)

Cisco Unified Communications Manager セキュリティ ガイド
Copyright © 2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2010-2011, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

はじめに

ここでは、このマニュアルの目的、対象読者、構成、および表記法、そして関連資料の入手方法について説明します。

次のトピックについて取り上げます。

目的

『*Cisco Unified Communications Manager セキュリティ ガイド*』は、システム管理者および電話機管理者が次の作業を実行する際に役立ちます。

- 認証を設定する。
- 暗号化を設定する。
- ダイジェスト認証を設定する。
- HTTPS に関連付けられているサーバ認証証明書をインストールする。
- Cisco CTL クライアントを設定する。
- セキュリティ プロファイルを設定する。
- サポートされている Cisco Unified IP Phone モデルのローカルで有効な証明書をインストール、アップグレード、または削除できるように Certificate Authority Proxy Function（CAPF）を設定する。
- 電話機のセキュリティを強化する。
- Survivable Remote Site Telephony（SRST）参照先についてセキュリティを設定する。
- ゲートウェイおよびトランクについてセキュリティを設定する。

対象読者

このマニュアルで説明しているリファレンスおよび手順のガイドは、Cisco Unified Communications Manager のコール セキュリティ機能の設定を担当するシステム管理者および電話機管理者を対象としています。

マニュアルの構成

表 1 は、このマニュアルの構成を示しています。

表 1　　このマニュアルの構成

章	説明
セキュリティの基礎	
第 1 章「セキュリティの概要」	セキュリティの用語、システム要件、相互作用と制限、インストール要件、および設定用チェックリストの概要を説明します。また、さまざまなタイプの認証と暗号化についても説明します。
第 2 章「HTTP over SSL（HTTPS）の使用方法」	HTTPS の概要を説明します。また、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も説明します。
第 3 章「デフォルトのセキュリティ」	自動セキュリティ機能を Cisco Unified IP Phone に提供するデフォルトのセキュリティについて説明します。
第 4 章「Cisco CTL クライアントの設定」	Cisco CTL クライアントをインストールおよび設定することにより認証を設定する方法を説明します。
第 5 章「証明書の設定」	証明書の設定について説明します。
電話機およびボイスメール ポートのセキュリティ	
第 6 章「電話機のセキュリティの概要」	Cisco Unified Communications Manager および電話機でのセキュリティの使用方法について説明し、電話機でセキュリティを設定するために実行するタスクのリストを示します。
第 7 章「電話機セキュリティ プロファイルの設定」	Cisco Unified Communications Manager の管理ページでセキュリティ プロファイルを設定し、電話機に適用する方法を説明します。
第 8 章「セキュア インディケーション トーンと非セキュア インディケーション トーンの設定」	セキュア インディケーション トーンを再生するよう電話機を設定する方法を説明します。
第 9 章「アナログ エンドポイントの暗号化の設定」	アナログ電話機で Cisco VG2xx Gateway へのセキュアな SCCP 接続を作成する方法について説明します。
第 10 章「Certificate Authority Proxy Function の使用方法」	Certificate Authority Proxy Function の概要を説明します。また、サポートされている電話機のローカルで有効な証明書をインストール、アップグレード、削除、またはトラブルシュートする方法も説明します。

表 1　　このマニュアルの構成（続き）

章	説明
第 11 章「暗号化された電話機設定ファイルの設定」	暗号化された電話機設定ファイルを Cisco Unified Communications Manager の管理ページで設定する方法を説明します。
第 12 章「SIP 電話機のダイジェスト認証の設定」	SIP を実行する電話機に Cisco Unified Communications Manager の管理ページでダイジェスト認証を設定する方法を説明します。
第 13 章「電話機のセキュリティ強化」	Cisco Unified Communications Manager の管理ページを使用して電話機のセキュリティを強化する方法を説明します。
第 14 章「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。
第 15 章「ボイスメール ポートのセキュリティ設定」	Cisco Unified Communications Manager の管理ページでボイスメール ポートのセキュリティを設定する方法を説明します。
第 16 章「セキュア コールのモニタリングと録音の設定」	セキュア コールのモニタリングと録音を行う方法について説明します。
CTI、JTAPI、および TAPI のセキュリティ	
第 17 章「バーチャル プライベート ネットワークの設定」	バーチャル プライベート ネットワークを設定する方法について説明します。
第 18 章「VPN ゲートウェイの設定」	VPN ゲートウェイを設定する方法について説明します。
第 19 章「VPN グループの設定」	VPN グループを設定する方法について説明します。
第 20 章「VPN プロファイルの設定」	VPN プロファイルを設定する方法について説明します。
第 21 章「VPN 機能設定」	VPN 機能を設定する方法について説明します。
第 22 章「CTI、JTAPI、および TAPI の認証と暗号化の設定」	Cisco Unified Communications Manager の管理ページでアプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルを設定する方法を説明します。
SRST 参照先、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	
第 23 章「セキュア SRST（Survivable Remote Site Telephony）参照先の設定」	Cisco Unified Communications Manager の管理ページで SRST 参照先についてセキュリティを設定する方法を説明します。
第 24 章「ゲートウェイおよびトランクの暗号化の設定」	Cisco Unified Communications Manager がセキュアなゲートウェイまたはトランクと通信する方法、および IPSec に関する推奨事項と考慮事項について説明します。
第 25 章「SIP トランク セキュリティ プロファイルの設定」	Cisco Unified Communications Manager の管理ページで SIP トランクのセキュリティ プロファイルを設定し、適用する方法を説明します。

表 1　　このマニュアルの構成（続き）

章	説明
第 26 章「SIP トランクのダイジェスト認証の設定」	Cisco Unified Communications Manager の管理ページでダイジェスト認証を SIP トランクに設定する方法を説明します。
第 27 章「Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの設定」	Cisco Unified Communications Manager の管理ページで 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について説明します。

関連資料

各章に、その章のトピックについての関連マニュアルのリストを記載しています。

Cisco IP テレフォニー関連のアプリケーションと製品の詳細は、次の資料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 対応ゲートウェイをサポートする Cisco Unified Survivable Remote Site Telephony（SRST）の管理マニュアル
- ご使用の電話機モデルをサポートしているファームウェア リリース ノート

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*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。

マニュアルの入手方法、テクニカル 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、次の URL 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が示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

PART 1

セキュリティの基礎

CHAPTER 1

セキュリティの概要

Cisco Unified Communications Manager システムにセキュリティ機構を実装すると、電話機や Cisco Unified Communications Manager サーバの ID 盗難、データ改ざん、コール シグナリングやメディア ストリームの改ざんを防止することができます。

Cisco IP テレフォニー ネットワークは、認証された通信ストリームの確立および維持、電話機にファイルを転送する前のファイルへのデジタル署名、Cisco Unified IP Phone 間でのメディア ストリームおよびコール シグナリングの暗号化を行います。

この章は、次の内容で構成されています。

用語と略語

表 1-1 に示す定義は、Cisco IP テレフォニー ネットワークで認証、暗号化、および他のセキュリティ機能を設定する場合に適用されます。

表 1-1　用語

用語	定義
Access Control List（ACL; アクセス コントロール リスト）	システムの機能およびリソースにアクセスするためのアクセス権を定義するリスト。メソッド リストを参照。
Certificate Authority（CA; 認証局）	証明書を発行する信頼されたエンティティ。シスコまたはサードパーティのエンティティなど。
Certificate Authority Proxy Function（CAPF）	サポートされているデバイスが Cisco Unified Communications Manager の管理機能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。
Certificate Trust List（CTL; 証明書信頼リスト）	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）で署名したファイル。電話機が信頼するサーバの証明書リストを含みます。
Cisco Site Administrator Security Token（セキュリティ トークン、etoken）	秘密鍵と、Cisco Certificate Authority の署名する X.509v3 証明書が含まれるポータブル ハードウェア セキュリティ モジュール。ファイルの認証に使用され、CTL ファイルに署名します。
DSP	Digital Signaling Processor（デジタル シグナル プロセッサ）。
DSP ファーム	H.323 または MGCP 対応ゲートウェイの DSP で提供される IP テレフォニー会議のネットワーク リソース。
H.323	インターネット規格の一種。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式を定義します。
Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS; HTTP over SSL）	HTTPS サーバの ID を（少なくとも）保証する IETF が定義したプロトコル。暗号化を使用して、Tomcat サーバとブラウザ クライアントとの間で交換される情報の機密を確保します。
IPSec	エンドツーエンド セキュリティ用に、セキュアな H.225、H.245、RAS シグナリング チャネルを提供する転送方式。
Locally Significant Certificate（LSC; ローカルで有効な証明書）	CAPF が発行し、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デジタル X.509v3 証明書。
Man-in-the-Middle（中間者）攻撃	Cisco Unified Communications Manager と電話機との間で流れる情報を、攻撃者が監視して改変できるプロセス。
Manufacture Installed Certificate（MIC; 製造元でインストールされる証明書）	Cisco Certificate Authority によって署名され、サポートされている電話機にシスコの製造過程でインストールされた X.509v3 デジタル証明書。LSC が電話機にインストールされる際の CAPF の認証メカニズムとして使用します。
MD5	暗号化で使用されるハッシュ関数。
Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）	複数の H.323 エンドポイントと接続して、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なる柔軟なシステム。
PKI	Public Key Infrastructure（公開鍵インフラストラクチャ）。セキュリティ保護された公開鍵の配布、証明書や認証局など、公開鍵の暗号化に必要な要素のセットで構成されます。

表 1-1　用語（続き）

用語	定義
RTP	Real-Time Transport Protocol（リアルタイム転送プロトコル）。
Simple Certificate Enrollment Protocol（SCEP）	X.509 証明書を発行する認証局との通信に使用されるプロトコル。
SIP レルム	Cisco 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	ネットワークで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セキュアなリアルタイム転送プロトコル。
SSL	データ通信（インターネットでの電子メールなど）のセキュリティを確保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。
System Administrator Security Token（SAST）	CTI/JTAPI/TAPI アプリケーションでは、CTL ダウンロード用の CTL ファイルへの署名に使用するトークン。
Transport Layer Security（TLS）	データ通信（インターネットでの電子メールなど）のセキュリティを確保する暗号化プロトコル。機能的には SSL と同等です。
X.509	PKI 認証のインポートに使用する ITU-T 暗号化規格で、証明書の形式を含んでいます。
暗号化	データを暗号文に変換するプロセス。情報の機密性を保持し、対象とする受信者だけがデータを読み取ることができるようにします。暗号化アルゴリズムと暗号鍵が必要です。
イメージ認証	電話機にバイナリ イメージをロードする前に、電話機がバイナリ イメージの整合性と発信元を検証するプロセス。
許可	認証されたユーザ、サービス、またはアプリケーションに、要求されたアクションの実行に必要なアクセス権があるかどうかを指定するプロセス。Cisco Unified Communications Manager では、許可されたユーザに一部のトランク側 SIP 要求を制限するセキュリティ プロセス。
許可ヘッダー	チャレンジに対する SIP ユーザ エージェントの応答。
公開鍵/秘密鍵	暗号化に使用される鍵。公開鍵は広く一般に流通するが秘密鍵は該当する所有者が保持します。非対称暗号化では、両方の鍵を使用します。
混合モード	Cisco Unified Communications Manager のセキュリティ モードで、セキュア/非セキュアのプロファイルを持つデバイスおよび RTP/ SRTP メディアが Cisco Unified Communications Manager に接続できるようにする設定を行います。
シグナリング暗号化	デバイスと Cisco Unified Communications Manager サーバの間で送信されるすべてのシグナリング メッセージの機密保持を行うために、暗号化手法を使用するプロセス。
シグナリング認証	転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する TLS プロセス。
証明書	証明書の保持者名、公開鍵、およびこの証明書を発行する認証局のデジタル署名が含まれているメッセージ。
信頼ストア	Cisco Unified Communications Manager などのアプリケーションによって明示的に信頼された X.509 証明書のリポジトリ。
信頼リスト	デジタル署名なしの証明書リスト。
整合性	エンティティ間でデータの改ざんが行われなかったことを確認するプロセス。

表 1-1　用語（続き）

用語	定義
セキュア コール	すべてのデバイスが認証され、シグナリングとメディア（ボイス ストリーム）が暗号化されているコール。
ダイジェスト認証	デバイス認証の形式。（特に）共有パスワードの MD5 ハッシュを使用して、SIP ユーザ エージェントの ID を確認します。
ダイジェスト ユーザ	SIP を実行する電話機または SIP トランクが送信する許可要求に含まれているユーザ名。
チャレンジ	ダイジェスト認証において、SIP ユーザ エージェントの ID を認証するための SIP ユーザ エージェントに対する要求。
デジタル署名	メッセージをハッシュ変換し、その後、署名者が自身の秘密鍵で暗号化して生成される値。メッセージの受信者は署名者の公開鍵でハッシュ変換を行ってこれを復号化します。これによって同じハッシュ関数で別のハッシュ値が生成されます。この 2 つのハッシュを比較してメッセージが一致し、内容が損なわれていないことを確認します。
デバイス認証	接続前に、デバイスの ID を検証し、このエンティティが主張内容と一致することを確認するプロセス。
ナンス	一意のランダムな数値で、サーバが各ダイジェスト認証要求に対して生成します。MD5 ハッシュを生成するために使用されます。
認証	通信中のエンティティの ID を検証するプロセス。
ハッシュ	ハッシュ関数を使用してテキスト文字列から生成される、主に 16 進数で表される数字。これによって、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」を作成します。
非セキュア コール	少なくとも 1 台のデバイスが認証も暗号化もされていないコール。
非セキュア デバイス	UDP または TCP 方式のシグナリングと非セキュア メディアを使用するデバイス。
非セキュア モード	Cisco Unified Communications Manager のセキュリティ モードで、非セキュア プロファイルを持つデバイスおよび RTP メディアが Cisco Unified Communications Manager に接続できるようにする設定を行います。
ファイル認証	電話機でダウンロードするデジタル署名されたファイルを検証するプロセス。電話機は署名を検証して、ファイルが作成後に改ざんされていないことを確認します。
メソッド リスト	許可プロセス中に、SIP トランクに着信する可能性のある一定のカテゴリのメッセージを制限するツール。トランク側アプリケーションまたはデバイスに対して SIP 非インバイト メソッドを許可するかどうかを定義します。メソッド ACL とも呼ばれます。
メッセージ/データ改ざん	攻撃者が、転送中のメッセージを変更しようとするイベント。コールの途中終了も含まれます。
メディア暗号化	暗号化手順によってメディアの機密を保護するプロセス。メディア暗号化では、IETF RFC 3711 で定義された Secure Real Time Protocol（SRTP）を使用します。
リプレイ アタック	攻撃者が、電話機またはプロキシ サーバを識別する情報をキャプチャし、実際のデバイスを偽装しながら情報を再送するイベント。たとえば、プロキシ サーバの秘密鍵を偽装します。

システム要件

認証および暗号化には、次のシステム要件があります。

- Cisco Unified Communications Manager は、このマニュアルで示すセキュリティ機能の最小要件として機能します。
- クラスタのサーバごとに、異なる管理者パスワードを使用できます。
- Cisco CTL クライアントで使用するユーザ名およびパスワード（Cisco Unified Communications Manager サーバへのログインに使用）は、Cisco Unified Communications Manager の管理ページのユーザ名およびパスワード（Cisco Unified Communications Manager の管理ページへのログインに使用するユーザ名およびパスワード）と一致する必要があります。
- LSC は、Cisco Unified Communications Manager との TLS 接続の認証用のすべての電話機にインストールされています。Certificate Authority Proxy Function（CAPF）については、「CAPF システムの相互作用および要件」（P.10-4）を参照してください。
- ボイスメール ポートのセキュリティを設定する前に、今回のリリースの Cisco Unified Communications Manager をサポートする Cisco Unity または Cisco Unity Connection システムのバージョンがインストールされていることを確認します。

機能一覧

Cisco Unified Communications Manager システムは、トランスポート層からアプリケーション層まで、複数層によるコール セキュリティへのアプローチを使用します。

トランスポート層セキュリティには、音声ドメインへのアクセスを制御および防止するためにシグナリングの認証と暗号化を行う TLS および IPSec が含まれます。SRTP は、メディア認証および暗号化をセキュア プライバシーに追加し、音声会話およびその他のメディアに機密性を追加します。

表 1-2 に、サポートされる機能および設定された機能に応じて SCCP コール セッション中に Cisco Unified Communications Manager が実装できる認証および暗号化の機能の概要を示します。

表 1-2　SCCP コールのセキュリティ機能

セキュリティ機能	回線側	トランク側
転送 / 接続 / 整合性	セキュア TLS ポート	IPSec アソシエーション
デバイス認証	Cisco Unified Communications Manager と CAPF のいずれかまたは両方との TLS 証明書交換	IPSec 証明書交換、または事前共有鍵
シグナリング認証 / 暗号化	TLS モード：認証または暗号化	IPSec（認証ヘッダー、暗号化（ESP）、または両方）
メディア暗号化	SRTP	SRTP
許可	プレゼンス要求	プレゼンス要求
注：デバイスがサポートする機能はデバイス タイプによって異なります。		

表 1-3 に、サポートされる機能および設定された機能に応じて SIP コール セッション中に Cisco Unified Communications Manager が実装できる認証および暗号化の機能の概要を示します。

表 1-3　SIP コールのセキュリティ機能

セキュリティ機能	回線側	トランク側
転送/接続/整合性	セキュア TLS ポート	セキュア TLS ポート
デバイス認証	Cisco Unified Communications Manager および CAPF のいずれかまたは両方との TLS 証明書交換	IPSec 証明書交換、または事前共有鍵
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	SIP トランク ユーザ エージェントは一意のダイジェスト信用証明書を使用
シグナリング認証/暗号化	TLS モード：認証または暗号化（Cisco Unified IP Phone 7940G/7960G を除く）	TLS モード：認証または暗号化モード
メディア暗号化	SRTP	SRTP
許可	プレゼンス要求	プレゼンス要求 メソッド リスト

注：デバイスがサポートする機能はデバイス タイプによって異なります。

セキュリティ アイコン

Cisco Unified Communications Manager は、コールに参加する Cisco Unified Communications Manager サーバとデバイスに設定されているセキュリティ レベルに応じたセキュリティのステータスをコールに提供します。

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。

- シグナリング セキュリティ レベルが「認証」のコールに対しては、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、デバイスのシグナリングが認証または暗号化されていることを意味します。
- 暗号化メディアのコールに対しては、電話機にロック　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 アイコンしか表示されません。

コールのセキュリティ ステータスは、ポイント間、クラスタ内、クラスタ間、マルチホップ コールで変わる場合があります。SCCP 回線、SIP 回線、および H.323 シグナリングでは、コールのセキュリティ ステータスが変更した場合、参加しているエンドポイントへの通知をサポートしています。コールのパスに SIP トランクが含まれる場合、コール セッションのステータスは非セキュアになります。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」（P.1-11）を参照してください。

コールの音声とビデオは、コールのセキュリティ ステータスの基盤になります。音声とビデオの両方が安全である場合に限り、コールは安全であると見なされます。表 1-4 で、セキュリティ アイコンを表示するかどうかを判断する規則と、表示されるアイコンについて説明します。

表 1-4　セキュリティ アイコンの表示規則

コールのメディア タイプとデバイス タイプ	シールド 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
セキュアな音声（非セキュアなビデオを含む）	シールド	なし
セキュアな音声（セキュアなビデオを含む）	ロック	ロック
認証されたデバイス（非セキュアな音声のみ含む）	シールド	なし
認証されたデバイス（非セキュアな音声とビデオを含む）	シールド	なし
認証されていないデバイス（非セキュアな音声のみ含む）	なし	なし
認証されていないデバイス（非セキュアな音声とビデオを含む）	なし	なし

会議コールおよび割り込みコールでは、セキュリティ アイコンは会議のセキュリティ ステータスを表示します。詳細については、「セキュアな会議のアイコン」（P.14-3）を参照してください。

相互作用および制限

この項では、次のトピックについて取り上げます。

- 「相互作用」（P.1-7）
- 「制限」（P.1-8）

セキュアな会議の機能に関する相互作用と制限の詳細については、「セキュアな会議リソースの設定」（P.14-1）を参照してください。

相互作用

ここでは、シスコのセキュリティ機能が Cisco Unified Communications Manager アプリケーションと相互に作用する方法について説明します。

プレゼンス

SIP を実行する電話機およびトランクにプレゼンス グループ許可を追加するには、プレゼンス要求を許可ユーザに制限するプレゼンス グループを設定します。

（注）　プレゼンス グループの設定の詳細については、『*Cisco Unified Communications Manager 機能およびサービス ガイド*』を参照してください。

SIP トランクでプレゼンス要求を許可するには、Cisco Unified Communications Manager で SIP トランクでのプレゼンス要求を受け入れるように設定します。また、必要に応じて、Cisco Unified Communications Manager でリモート デバイスおよび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て認証できるように設定します。

SIP トランク

SIP 発信転送機能、および Web Transfer やクリック ツー ダイヤルなどの高度な転送関連機能を SIP トランクで使用するには、Cisco Unified Communications Manager で着信 Out-of-Dialog REFER 要求を受け付けるように設定する必要があります。

イベント レポートをサポートし（MWI サポートなど）、1 コールあたりの MTP 割り当て（ボイスメール サーバからなど）を削減するには、Cisco Unified Communications Manager で Unsolicited NOTIFY SIP 要求を受け付けるように設定する必要があります。

Cisco Unified Communications Manager が、SIP トランクの外部コールを外部デバイスまたはパーティに転送できるようにするには（有人転送など）、Cisco Unified Communications Manager で REFER およびインバイトの REPLACE ヘッダー付き SIP 要求を受け付けるように設定します。

エクステンション モビリティ

エクステンション モビリティでは、エンド ユーザごとに異なるクレデンシャルが設定されるため、ユーザがログインまたはログアウトしたときに、SIP ダイジェスト信用証明書が変更されます。

CTI

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

CTI/JTAPI/TAPI アプリケーションの複数のインスタンスが実行中の場合、CTI TLS をサポートするには、管理者が、アプリケーション インスタンスごとに一意のインスタンス ID（IID）を設定し、CTI Manager と JTAPI/TSP/CTI アプリケーションとの間のシグナリングおよびメディア通信ストリームを保護する必要があります。

デバイス セキュリティ モードが認証済みまたは暗号化済みになっている場合、Cisco Unity-CM TSP は Cisco Unified Communications Manager TLS ポートを介して Cisco Unified Communications Manager に接続します。セキュリティ モードが非セキュアになっている場合は、Cisco Unity TSP は、Cisco Unified Communications Manager ポートを介して Cisco Unified Communications Manager に接続します。

制限

次の項で、シスコのセキュリティ機能に適用される制限について説明します。

- 「認証と暗号化」（P.1-9）
- 「割り込みと暗号化」（P.1-9）
- 「ワイドバンド コーデックと暗号化」（P.1-9）
- 「メディア リソースと暗号化」（P.1-10）
- 「電話機のサポートと暗号化」（P.1-10）
- 「電話機のサポートおよび暗号化された設定ファイル」（P.1-10）
- 「セキュリティ アイコンと暗号化」（P.1-11）
- 「クラスタおよびデバイス セキュリティ モード」（P.1-11）
- 「ダイジェスト認証と暗号化」（P.1-12）
- 「パケット キャプチャと暗号化」（P.1-12）

認証と暗号化

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、次の制限を考慮してください。

- 混合モードに設定すると、自動登録機能は動作しません。
- デバイス認証がないとシグナリング暗号化またはメディア暗号化を実装できません。デバイス認証をインストールするには、Cisco CTL Provider サービスを有効にし、Cisco CTL クライアントをインストールして設定してください。
- 混合モードに設定している場合、Cisco Unified Communications Manager は Network Address Translation（NAT; ネットワーク アドレス変換）をサポートしません。

  ファイアウォールで UDP を有効にすると、メディア ストリームによるファイアウォールの通過が許可されます。UDP を有効にすると、ファイアウォールの信頼できる側にあるメディア ソースが、ファイアウォールを介してメディア パケットを送信することにより、ファイアウォールを通過する双方向のメディア フローを開くことができます。

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

  シグナリング暗号化では NAT トラバーサルをサポートしません。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。
- SRTP は、音声パケットのみを暗号化します。

割り込みと暗号化

割り込みと暗号化には、次の制限が適用されます。

- 帯域幅要件のため、Cisco Unified IP Phone 7940G および 7960G は、アクティブな暗号化済みコールへの暗号化済みデバイスからの割り込みをサポートしません。割り込みを試みると失敗します。割り込みが失敗したことを示すトーンが発信者の電話機で再生されます。
- リリース 8.2 またはそれ以前を実行している暗号化が設定されている Cisco Unified IP Phone は、認証済みまたは非セキュアの参加者としてのみ、アクティブなコールに割り込むことができます。
- 発信者がセキュアな SCCP コールに割り込むと、システムは割り込み先のデバイスで内部のトーン再生メカニズムを使用し、ステータスはセキュアなままとなります。
- 発信者がセキュアな SIP コールに割り込むと、システムは保留音を再生し、Cisco Unified Communications Manager は再生中にこのコールを非セキュアと分類します。

（注） リリース 8.3 以降を実行している非セキュアまたは認証済みの Cisco Unified IP Phone は、暗号化済みコールに割り込むことができます。セキュリティ アイコンによって会議のセキュリティ ステータスが示されます。詳細については、「セキュアな会議のアイコン」（P.14-3）を参照してください。

ワイドバンド コーデックと暗号化

次の情報は、暗号化が設定されていて、ワイドバンドのコーデック リージョンに関連付けられた Cisco Unified IP Phone 7960G または 7940G に適用されます。これは、TLS/SRTP 用に設定された Cisco Unified IP Phone 7960G または 7940G 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、Cisco Unified Communications Manager はワイドバンド コーデックを無視して、サポートされる別のコーデックを電話機が提示するコーデック リストから選択します。コールのもう一方のデバイスで暗号化が設定されていない場合、Cisco Unified Communications Manager はワイドバンド コーデックを使用して認証済みおよび非セキュア コールを確立できます。

メディア リソースと暗号化

Cisco Unified Communications Manager はメディア リソースを使用しないセキュア Cisco Unified IP Phone（SCCP または SIP）、セキュア CTI デバイス/ルート ポイント、セキュア Cisco MGCP IOS ゲートウェイ、セキュア SIP トランク、セキュア H.323 ゲートウェイ、セキュア会議ブリッジ、およびセキュア H.323/H.245/H.225 トランク間で、認証および暗号化されたコールをサポートします。Cisco Unified Communications Manager では、次の場合にメディア暗号化を使用できません。

- トランスコーダに関連するコール
- メディア ターミネーション ポイントに関連するコール
- 保留音に関連するコール（セキュア会議ブリッジのコールを除く）

電話機のサポートと暗号化

一部の Cisco Unified IP Phone（Cisco Unified IP Phone 7912G など）は、暗号化コールをサポートしません。暗号化はサポートしても、証明書の署名の検証はサポートしない電話機もあります。暗号化とこのバージョンの Cisco Unified Communications Manager をサポートする Cisco Unified IP Phone の詳細については、Cisco Unified IP Phone のアドミニストレーション ガイドを参照してください。

SCCP を実行する Cisco Unified IP Phone 7906G、7911G、7931G、7940G、7941G、7941G-GE、7942G、7945G、7960G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、および 7975G は、暗号化をサポートします。SIP を実行する Cisco Unified IP Phone 7906G、7911G、7941G、7941G-GE、7942G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、および 7975G は、暗号化をサポートします。

警告　**セキュリティ機能を最大限に活用するには、Cisco Unified IP Phone をリリース 8.3 にアップグレードすることをお勧めします。リリース 8.3 は、今回のリリースの Cisco Unified Communications Manager で暗号化機能をサポートします。それよりも前のリリースを実行している暗号化済みの電話機では、これらの新機能が完全にはサポートされません。これらの電話機では、セキュアな会議コールおよび割り込みコールに対し、認証済みか非セキュアな参加者としてだけ参加できます。**

Cisco Unified IP Phone で Cisco Unified Communications Manager の以前のリリースとともにリリース 8.3 を実行している場合、会議コールまたは割り込みコール中に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ます。また、会議リストなどのセキュアな会議機能はサポートされません。

電話機のサポートおよび暗号化された設定ファイル

暗号化された設定ファイルをサポートしない電話機もあります。また、暗号化された設定ファイルはサポートするが、署名の検証をサポートしない電話機もあります。Cisco Unified IP Phone 7905G および 7912G を除き、暗号化された設定ファイルをサポートする電話機にはすべて、完全に暗号化された設定ファイルを受信するために、Cisco Unified Communications Manager リリース 5.0 以降と互換性のあるファームウェアが必要です。Cisco Unified IP Phone 7905G および 7912G は、既存のセキュリティ メカニズムを使用します。このメカニズムはこの機能のために新しいファームウェアを必要としません。暗号化された設定ファイルの電話機でのサポートについては、「サポートされる電話機のモデル」（P.11-4）を参照してください。

セキュリティ アイコンと暗号化

セキュリティ アイコンと暗号化には、次の制限が適用されます。

- コールの転送またはコールの保留などのタスクを実行するときに、暗号化ロック　アイコンが電話機に表示されないことがあります。MOH など、こうしたタスクに関連付けられたメディア ストリームが暗号化されていない場合、ステータスは暗号化済みから非セキュアに変化します。
- Cisco Unified Communications Manager は、H.323 トランクおよび SIP トランクで転送されるコールに対してはシールド アイコンを表示しません。
- PSTN に関連するコールの場合、セキュリティ アイコンで表示されるセキュリティ ステータスはコールの IP ドメイン部分についてのみです。
- 転送タイプに TLS が使用されている場合、SIP トランクからレポートされるセキュリティ ステータスは、暗号化済みまたは非認証になります。SRTP がネゴシエートされると、セキュリティ ステータスは暗号化済みになります。ネゴシエートされない場合は非認証のままです。これによって、Cisco Unified Communications Manager のコール制御は、SIP トランクに関連するコールの全体的なセキュリティ レベルを特定できます。

  SIP トランクは、ミートミー会議や C 割り込みなどのイベント中に参加者が認証された場合、認証済みステータスをトランク経由でレポートします（SIP トランクは引き続き TLS または SRTP を使用します）。
- セキュアなモニタリングおよび録音のため、SIP トランクは、SIP トランク経由でセキュリティ アイコン ステータスを送信するときに、SIP 回線で現在使用されているように、既存の Call Info ヘッダー メカニズムを使用します。その結果、コールの全体的なセキュリティ ステータスを SIP トランク ピアから監視できます。
- 暗号化済み電話機からの SIP トランク経由のコールが、そのクラスタ内の暗号化済み電話機に転送された場合、コールは暗号化されず、それらの暗号化済み電話機が同じセキュア クラスタ内に存在してもロック アイコンは表示されません。
- 一部の電話機モデルでは、ロック アイコンしか表示されず、シールド アイコンが表示されません。

セキュアな会議でのセキュリティ アイコンの表示の詳細については、「セキュアな会議のアイコン」（P.14-3）を参照してください。

クラスタおよびデバイス セキュリティ モード

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

クラスタ セキュリティ モードが非セキュアと示される場合、デバイス セキュリティ モードは電話機の設定ファイルで非セキュアになっています。この場合、電話機は、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ても、SRST 対応のゲートウェイおよび Cisco Unified Communications Manager と非セキュア接続を確立します。デバイス セキュリティ モード以外のセキュリティ関連設定（[SRST を許可 (SRST Allowed)] チェックボックスなど）も無視されます。セキュリティ設定は Cisco Unified Communications Manager の管理ページで削除されませんが、セキュリティは提供されません。

電話機が SRST 対応ゲートウェイへのセキュア接続を試行するのは、クラスタ セキュリティ モードがセキュアで、電話機設定ファイル内のデバイス 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おり、[トランクの設定 (Trunk Configuration)] ウィンドウで [SRST を許可 (SRST Allowed?)] チェックボックスがオンになっていて、電話機の設定ファイル内に有効な SRST 証明書が存在する場合だけです。

ダイジェスト認証と暗号化

Cisco Unified Communications Manager は、複数の異なるコール レッグを持つコールとして、SIP コールを定義します。通常、2 つの SIP デバイスで 2 者が通話するとき、2 つの異なるコール レッグが存在します。1 つは、発信 SIP ユーザ エージェントと Cisco Unified Communications Manager の間（発信コール レッグ）で、もう 1 つは Cisco Unified Communications Manager と宛先 SIP ユーザ エージェントの間（着信コール レッグ）です。各コール レッグは、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 プロセスなので、各コール レッグの認証は別のコール レッグから独立しています。SRTP 機能は、ユーザ エージェント間でネゴシエーション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、サードパーティのスニファは動作しません。適切な認証で許可された管理者は、Cisco Unified Communications Manager の管理ページ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するデバイスの場合）。Cisco Unified Communications Manager でのパケット キャプチャの設定については、今回のリリースをサポートする『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

ベスト プラクティス

シスコでは、次のベスト プラクティスを強く推奨します。

- 必ず安全なテスト環境でインストールおよび設定タスクを実行してから、広範囲のネットワークに展開します。
- リモートのロケーションのゲートウェイその他のアプリケーション サーバには IPSec を使用します。

警告　これらのインスタンスで IPSec を使用しない場合、セッション暗号鍵が暗号化されずに転送されます。

- 通話料金の不正を防止するため、『*Cisco Unified Communications Manager システム ガイド*』に説明されている電話会議の機能拡張を設定します。同様に、コールの外部転送を制限する設定作業を実行することができます。この作業の実行方法については、『*Cisco Unified Communications Manager 機能およびサービス ガイド*』を参照してください。

この項では、次のトピックについて取り上げます。

- 「デバイスのリセット、サービスの再起動またはリブート」（P.1-12）
- 「メディア暗号化の設定と割り込み」（P.1-13）

デバイスのリセット、サービスの再起動またはリブート

ここでは、デバイスのリセット、Cisco Unified サービスアビリティでのサービスの再起動、あるいはサーバまたはクラスタのリブートが必要になる場合について説明します。

次のガイドラインを考慮します。

- Cisco Unified Communications Manager の管理ページで別のセキュリティ プロファイルを適用した後、1 台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作業を実行した場合は、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）に変更した後は、デバイスをリセットします。

- Cisco CTL クライアントの設定後、または CTL ファイルの更新後は、すべてのデバイスを再起動します。
- CAPF エンタープライズ パラメータを更新した後は、デバイスをリセットします。
- TLS 接続用のポートを更新した後は、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）に変更した後は、Cisco CallManager サービスを再起動します。
- Cisco Certificate Authority Proxy Function サービスに関連する CAPF サービス パラメータを更新した後は、このサービスを再起動します。
- Cisco CTL クライアントの設定後、または CTL ファイルの更新後は、Cisco Unified サービスアビリティで Cisco CallManager サービスおよび Cisco TFTP サービスをすべて再起動します。この作業は、これらのサービスを実行するクラスタ内のすべてのサーバで実行します。
- CTL Provider サービスを開始または停止した後は、Cisco CallManager サービスおよび Cisco TFTP サービスをすべて再起動します。
- セキュア SRST 参照先の設定後は、従属デバイスをリセットします。
- Smart Card サービスを「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 をリブートします。
- アプリケーション ユーザ CAPF プロファイルに関連付けられ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は、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。

電話機設定の更新後に単一のデバイスをリセットするには、「電話機セキュリティ プロファイルの適用」（P.7-10）を参照してください。

クラスタ内のデバイスをすべてリセットするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで [システム (System)] > [Cisco Unified CM] の順に選択します。

検索と一覧表示ウィンドウが表示されます。

ステップ 2　[検索 (Find)] をクリックします。

設定済みの Cisco Unified Communications Manager サーバのリストが表示されます。

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

ステップ 4　[リセット (Reset)] をクリックします。

ステップ 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。

メディア暗号化の設定と割り込み

「割り込みと暗号化」（P.1-9）に加えて、次の情報も参照してください。

暗号化が設定されている Cisco Unified IP Phone 7960G および 7940G に対して割り込みを設定しようとすると、次のメッセージが表示されます。

If you configure encryption for Cisco Unified IP Phone models 7960 and 7940, those encrypted devices cannot accept a barge request when they are participating in an encrypted call.When the call is encrypted, the barge attempt fails.

メッセージが表示されるのは、Cisco Unified Communications Manager の管理ページで次の作業を実行したときです。

- [エンタープライズパラメータ設定(Enterprise Parameters Configuration)] ウィンドウで、Cluster Security Mode パラメータを更新する。
- [サービスパラメータ設定(Service Parameter Configuration)] ウィンドウで、Builtin Bridge Enable パラメータを更新する。

Cisco Unified IP Phone 7960G および 7940G に暗号化されたセキュリティ プロファイルを設定し、[ビルトインブリッジ(Built In Bridge)] 設定で [オン(On)] を選択した場合（デフォルト設定は [デフォルト(Default)]）、このメッセージは [電話の設定(Phone Configuration)] ウィンドウに表示されません。ただし同じ制限が適用されます。

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

インストール

認証のサポートを可能にするには、プラグインの Cisco CTL クライアントを Cisco Unified Communications Manager の管理ページからインストールします。Cisco CTL クライアントをインストールするためには、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。

Cisco Unified Communications Manager のインストール時に、メディアおよびシグナリング暗号化機能が自動的にインストールされます。

Cisco Unified Communications Manager は、Cisco Unified Communications Manager 仮想ディレクトリに SSL（Secure Sockets Layer）を自動的にインストールします。

Cisco Certificate Authority Proxy Function（CAPF）は、Cisco Unified Communications Manager の管理機能の一部として自動的にインストールされます。

TLS と IPSec

転送セキュリティは、データの符号化、パッキング、および送信を扱います。Cisco Unified Communications Manager は、次のセキュア転送プロトコルを提供します。

- Transport Layer Security（TLS）: セキュアなポートおよび証明書交換を使用して、2 つのシステムまたはデバイス間で、信頼性の高いセキュアなデータ転送を実現します。TLS は、Cisco Unified Communications Manager で制御されたシステム、デバイス、およびプロセス間の接続を保護および制御し、音声ドメインへのアクセスを防止します。Cisco Unified Communications Manager は、TLS を使用して、SCCP を実行する電話機への SCCP コール、および SIP を実行する電話機またはトランクへの SIP コールを保護します。
- IP Security（IPSec）: Cisco Unified Communications Manager とゲートウェイの間で、信頼性の高いセキュアなデータ転送を実現します。IPSec は、Cisco IOS MGCP ゲートウェイおよび H.323 ゲートウェイに対してシグナリング認証および暗号化を実装します。

Secure RTP（SRTP; セキュア RTP）をサポートするデバイスの次のレベルのセキュリティとして、TLS および IPSec 転送サービスに SRTP を追加できます。SRTP は、メディア ストリーム（音声パケット）を認証および暗号化し、Cisco Unified IP Phone および TDM またはアナログ音声ゲートウェイ ポートで開始または終了する音声会話を、音声ドメインへのアクセス権を取得した盗聴者から保護します。さらに、SRTP はリプレイ アタックからの保護も提供します。

証明書

証明書は、クライアントとサーバの ID 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、ユーザとホスト間（デバイスおよびアプリケーション ユーザを含む）の接続のセキュリティを確保します。

管理者は Cisco Unified Communications オペレーティング システムの GUI で、サーバ証明書のフィンガープリントの表示、自己署名証明書の再生成、および信頼証明書の削除ができます。

また、管理者は、コマンドライン インターフェイス（CLI）で自己署名証明書の再生成および表示ができます。

CallManager 信頼ストアの更新と証明書の管理の詳細については、今回のリリースの Cisco Unified Communications Manager をサポートする『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

（注） Cisco Unified Communications Manager は、PEM（.pem）形式および DER（.der）形式の証明書のみサポートします。

この項では、次のトピックについて取り上げます。

- 「電話機の証明書の種類」（P.1-15）
- 「サーバの証明書の種類」（P.1-16）
- 「外部 CA からの証明書のサポート」（P.1-17）

電話機の証明書の種類

シスコでは次の種類の証明書を電話機で使用します。

- Manufacture-Installed Certificate（MIC; 製造元でインストールされる証明書）：この証明書は、サポートされている電話機にシスコの製造過程で自動的にインストールされます。製造元でインストールされる証明書は、LSC のインストールにおける Cisco Certificate Authority Proxy Function（CAPF）に対する認証を行います。MIC は上書きすることも削除することもできません。
- Locally Significant Certificate（LSC; ローカルで有効な証明書）：この種類の証明書は、Cisco Certificate Authority Proxy Function（CAPF）に関連する必要な作業を実行した後で、サポートされている電話機にインストールされます。設定の作業については、「設定用チェックリストの概要」（P.1-25）を参照してください。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、Cisco 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 製造元でインストールされる証明書（MIC）は、LSC のインストールの場合にのみ使用することをお勧めします。シスコでは、Cisco Unified Communications Manager との TLS 接続の認証用に 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 認証用またはその他の目的のために MIC を使用するように電話機を設定するお客様は、ご自身の責任で行ってください。MIC が侵害されてもシスコは責任を負いかねます。

Cisco Unified Communications Manager との TLS 接続で LSC を使用するには Cisco Unified IP Phone 7906G、7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、および 7975G をアップグレードし、CallManager 信頼ストアから MIC ルート証明書を削除して今後の互換性の問題を回避することをお勧めします。Cisco 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

CAPF 信頼ストアに格納されている MIC ルート証明書は、証明書のアップグレードに使用されます。CallManager 信頼ストアの更新と証明書の管理の詳細については、今回のリリースをサポートする『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

サーバの証明書の種類

Cisco Unified Communications Manager サーバでは、次の種類の自己署名証明書を使用します。

- HTTPS 証明書（Tomcat）：この自己署名ルート証明書は、Cisco Unified Communications Manager をインストールするときに、HTTPS サーバに対して生成されます。Cisco Unity Connection は、この証明書を SMTP サービスおよび IMAP サービスに使用します。
- CallManager 証明書：この自己署名ルート証明書は、Cisco Unified Communications Manager サーバに Cisco Unified Communications Manager をインストールすると自動的にインストールされます。
- CAPF 証明書：このルート証明書は、Cisco Unified Communications Manager のインストール中に生成され、Cisco CTL クライアントの設定が完了した後で、ユーザのサーバまたはクラスタ内のすべてのサーバにコピーされます。
- IPSec 証明書（ipsec_cert）：この自己署名ルート証明書は、Cisco Unified Communications Manager のインストール中に、MGCP および H.323 ゲートウェイとの IPSec 接続に対して生成されます。
- SRST 対応ゲートウェイ証明書：Cisco Unified Communications Manager の管理ページのセキュア SRST 参照先を設定するときに、Cisco Unified Communications Manager は、ゲートウェイから SRST 対応ゲートウェイ証明書を取得し、Cisco Unified Communications Manager データベースに格納します。デバイスをリセットすると、証明書は電話機設定ファイルに追加されます。証明書はデータベースに格納されるため、この証明書を証明書管理ツールで管理することはできません。
- TVS 証明書：これらは Trust Verification Service（TVS; 信頼検証サービス）をサポートする自己署名証明書です。
- 電話と VPN 間の信頼性証明書：このカテゴリを使用すると、Cisco Unified IP Phone の VPN 証明書をインポートできます。これらの証明書は MIDlet 信頼ストアに格納されます。
- Phone Certificates 信頼ストア（Phone-trust）：Cisco Unified Communications Manager は、電話機で HTTPS アクセスをサポートするためにこの証明書の種類を使用します。証明書は、Cisco Unified Communications オペレーティング システムの GUI を使用して、電話機の信頼ストアにアップロードできます。その後この証明書は、CTL ファイル メカニズムによって電話機にダウンロードされ、Cisco Unified IP Phone からのセキュアな Web アクセス（HTTPS）をサポートします。

Cisco Unified Communications Manager は、次の種類の証明書を CallManager 信頼ストアにインポートします。

- Cisco Unity サーバまたは Cisco Unity Connection 証明書：Cisco Unity および Cisco Unity Connection は、この自己署名ルート証明書を使用して、Cisco Unity SCCP および Cisco Unity Connection SCCP デバイス証明書に署名します。Cisco Unity の場合、Cisco Unity Telephony Integration Manager（UTIM）が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、Cisco Unified Communications Manager との TLS 接続を確立します。

  証明書名は、ボイスメール サーバ名に基づく証明書の件名のハッシュを表しています。すべてのデバイス（またはポート）が、ルート証明書をルートとする証明書を発行します。

- SIP Proxy 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 Cisco 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、Cisco Unified Communications Manager に対して認証されます。

存在する追加の信頼ストアを次に示します。

- Tomcat および Web アプリケーションの共通信頼ストア：Tomcat の信頼性証明書は、社内ディレクトリ（Active Directory または Netscape Directory）から Tomcat 信頼ストアにアップロードされます。信頼する証明書のアップロード後は、Cisco Tomcat サービスおよび Cisco DirSync サービスを再起動する必要があります。

外部 CA からの証明書のサポート

Cisco 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、Cisco Unified Communications オペレーティング システムの [証明書の管理 (Certificate Management)] の GUI でアクセスできます。現在サードパーティの CA を使用しているお客様は、この CSR メカニズムを使用して、Cisco Unified Communications Manager、CAPF、IPSec、および Tomcat の証明書を発行する必要があります。

（注）　今回のリリースの Cisco Unified Communications Manager は、SCEP インターフェイス サポートを提供しません。

サードパーティの CA 署名付き証明書をプラットフォームにアップロードした後、CTL クライアントを実行して、CTL ファイルを更新してください。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。たとえば、Cisco Unified Communications Manager 証明書を更新する場合は Cisco CallManager サービスと Cisco TFTP サービスを再起動し、CAPF 証明書を更新する場合は CAPF を再起動します。更新の手順については、「Cisco CTL クライアントの設定」（P.4-1）を参照してください。

プラットフォームでの証明書署名要求（CSR）の生成の詳細については、今回のリリースの Cisco Unified Communications Manager をサポートする『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

認証、整合性、および許可の概要

整合性および認証によって、次の脅威から保護します。

- TFTP ファイルの操作（整合性）
- 電話機と Cisco Unified Communications Manager との間で行われるコール処理シグナリングの変更（認証）
- 表 1-1 で定義した Man-in-the-Middle（中間者）攻撃（認証）
- 電話機およびサーバの ID 盗難（認証）
- リプレイ アタック（ダイジェスト認証）

許可は、認証されたユーザ、サービス、またはアプリケーションが実行できるアクションを指定します。単一セッションで複数の認証および許可の方式を実装できます。

認証、整合性、および許可の詳細については、次の項を参照してください。

- 「イメージ認証」（P.1-18）
- 「デバイス認証」（P.1-18）
- 「ファイル認証」（P.1-19）
- 「シグナリング認証」（P.1-19）
- 「ダイジェスト認証」（P.1-19）
- 「許可」（P.1-21）

イメージ認証

このプロセスは、バイナリ イメージ（ファームウェア ロード）が電話機でロードされる前に改ざんされるのを防ぎます。イメージが改ざんされると、電話機は認証プロセスで失敗し、イメージを拒否します。イメージ認証は、Cisco Unified Communications Manager のインストール時に自動的にインストールされる署名付きバイナリ ファイルを使用して行われます。同様に、Web からダウンロードするファームウェア アップデートでも署名付きバイナリ イメージが提供されます。

デバイス認証

このプロセスでは、通信デバイスの ID を検証し、このエンティティが主張内容と一致することを確認します。サポートされるデバイスのリストについては、「サポートされる電話機のモデル」（P.6-3）を参照してください。

デバイス認証は、Cisco Unified Communications Manager サーバとサポートされる Cisco Unified IP Phone、SIP トランク、または JTAPI/TAPI/CTI アプリケーション（サポートされる場合）の間で発生します。認証された接続は、各エンティティが他のエンティティの証明書を受け付けたときにのみ、これらのエンティティの間で発生します。この相互証明書交換プロセスが、相互認証と呼ばれるプロセスです。

デバイス認証は、「Cisco CTL クライアントの設定」（P.4-1）で説明する Cisco CTL ファイルの作成（Cisco Unified Communications Manager サーバ ノードおよびアプリケーションの認証の場合）、および「Certificate Authority Proxy Function の使用方法」（P.10-1）で説明する Certificate Authority Proxy Function（電話機および JTAPI/TAPI/CTI アプリケーションの認証の場合）に依存します。

ヒント　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、Cisco Unified Communications Manager に対して認証されます。CallManager 信頼ストアの更新の詳細については、今回のリリースの Cisco Unified Communications Manager をサポートする『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

ファイル認証

このプロセスでは、電話機で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、呼出音一覧、ロケール、CTL ファイルなどがあります。電話機は署名を検証して、ファイルが作成後に改ざんされていないことを確認します。サポートされるデバイスのリストについては、「サポートされる電話機のモデル」（P.6-3）を参照してください。

クラスタを非セキュア モードに設定した場合、TFTP サーバはどのファイルにも署名しません。クラスタを混合モードに設定した場合、TFTP サーバは呼出音一覧、ローカライズ、デフォルトの .cnf.xml、呼出音一覧 wav ファイルなど、.sgn 形式のスタティック ファイルに署名します。TFTP サーバは、ファイルのデータが変更されたことを確認するたびに、<device name>.cnf.xml 形式のファイルに署名します。

キャッシングが無効になっている場合、TFTP サーバは署名付きファイルをディスクに書き込みます。TFTP サーバは、保存されたファイルが変更されたことを確認すると、再度そのファイルに署名します。ディスク上に新しいファイルを置くと、保存されていたファイルは上書きされて削除されます。電話機で新しいファイルをダウンロードするには、事前に、Cisco Unified Communications Manager の管理ページで、影響を受けるデバイスを再起動しておく必要があります。

電話機は、TFTP サーバからファイルを受信すると、ファイルの署名を確認して、ファイルの整合性を検証します。電話機で認証された接続を確立するには、次の基準を満たしてください。

- 証明書が電話機に存在する必要がある。
- CTL ファイルが電話機にあり、そのファイルに Cisco Unified Communications Manager エントリおよび証明書が存在する必要がある。
- デバイスに認証または暗号化を設定した。

（注）　ファイル認証は Certificate Trust List（CTL; 証明書信頼リスト）ファイルの作成に依存します。これについては、「Cisco CTL クライアントの設定」（P.4-1）で説明します。

シグナリング認証

このプロセスはシグナリング整合性とも呼ばれ、TLS プロトコルを使用して、転送中のシグナリング 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 Certificate Trust List（CTL; 証明書信頼リスト）ファイルの作成に依存します。これについては、「Cisco CTL クライアントの設定」（P.4-1）で説明します。

ダイジェスト認証

この SIP トランクおよび電話機用のプロセスによって、Cisco Unified Communications Manager は、Cisco Unified Communications Manager に接続しているデバイスの ID でチャレンジができます。チャレンジが行われるときは、デバイスは自身のダイジェスト信用証明書（ユーザ名やパスワードのようなもの）を Cisco Unified Communications Manager に提示して検証を受けます。提示された信用証明書がそのデバイス用としてデータベースに設定済みの信用証明書と一致した場合、ダイジェスト認証は成功し、Cisco Unified Communications Manager は SIP 要求を処理します。

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

（注）　デバイスでダイジェスト認証を有効にする場合、デバイスを登録するには一意のダイジェスト　ユーザ ID およびパスワードが必要になります。

ユーザは Cisco Unified Communications Manager データベースに電話機ユーザまたはアプリケーション ユーザの SIP ダイジェスト信用証明書を設定します。

- 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信用証明書を指定します。
- SIP を実行する電話機の場合は、[エンドユーザの設定(End User Configuration)] ウィンドウで、ダイジェスト認証信用証明書を指定します。ユーザを設定した後でクレデンシャルを電話機に関連付けるには、[電話の設定(Phone Configuration)] ウィンドウで [ダイジェストユーザ(Digest User)]（エンドユーザ）を選択します。電話機をリセットした後、クレデンシャルは、TFTP サーバが電話機に提供する電話機設定ファイルに存在するようになります。ダイジェスト信用証明書が TFTP ダウンロードで暗号化されずに送信されることがないようにする方法については、「暗号化された電話機設定ファイルの設定」を参照してください。
- ユーザは、チャレンジを SIP トランク上で受信するための SIP レルムを設定します。SIP レルムは、レルム、ユーザ名（デバイスまたはアプリケーション ユーザ）およびダイジェスト信用証明書を指定します。

SIP を実行する外部の電話機またはトランクのダイジェスト認証を有効にし、ダイジェスト信用証明書を設定した場合、Cisco Unified Communications Manager は、ユーザ名、パスワード、およびレルムのハッシュを含む信用証明書チェックサムを計算します。システムはナンス値（ランダムな数値）を使用して、MD5 ハッシュを計算します。Cisco Unified Communications Manager は値を暗号化し、ユーザ名とチェックサムをデータベースに格納します。

チャレンジを開始する場合、Cisco Unified Communications Manager は、ヘッダーにナンスとレルムを含む SIP 401（Unauthorized）メッセージを使用します。ユーザは、SIP デバイスのセキュリティ プロファイルで電話機またはトランクのナンス確認時間を設定します。ナンス確認時間は、ナンス値が有効な時間数（分単位）を指定するものです。この時間を超えると、Cisco Unified Communications Manager は外部デバイスを拒否して新しい番号を生成します。

（注）　Cisco Unified Communications Manager は、回線側電話機またはデバイスから発信され、SIP トランク経由で到達した SIP コールのユーザ エージェント サーバ（UAS）、SIP トランクに向けて発信された SIP コールのユーザ エージェント クライアント（UAC）、または、回線対回線接続またはトランク対トランク接続のバックツーバック ユーザ エージェント（B2BUA）として機能します。ほとんどの環境では、Cisco Unified Communications Manager は主に、SCCP および SIP エンドポイントを接続する B2BUA として機能します（SIP ユーザ エージェントは、SIP メッセージを発信したデバイスまたはアプリケーションを表します）。

ヒント　ダイジェスト認証は、整合性や信頼性を提供しません。デバイスの整合性および信頼性を保証するには、デバイスに TLS プロトコルを設定します（デバイスが TLS をサポートする場合）。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 モードを暗号化に設定します。デバイスが暗号化された電話機設定ファイルをサポートする場合は、ファイルの暗号化を設定します。

電話機のダイジェスト認証

電話機に対してダイジェスト認証が有効になっている場合、Cisco Unified Communications Manager は、SIP を実行する電話機に対し、キープアライブ メッセージ以外のすべての要求でチャレンジを行います。Cisco Unified Communications Manager は回線側の電話機からのチャレンジには応答しません。

応答を受信した後、Cisco Unified Communications Manager は、データベースに格納されているユーザ名のチェックサムと、応答ヘッダーのクレデンシャルと比較して検証します。

SIP を実行する電話機は Cisco Unified Communications Manager のレルムに存在し、これは Cisco Unified Communications Manager の管理機能のインストール時に定義されます。電話機のチャレンジ用の SIP レルムは、サービス パラメータ SIP Station Realm で設定します。各ダイジェスト ユーザは、レルムごとにダイジェスト信用証明書のセットを 1 つ持つことができます。詳細については、「SIP 電話機のダイジェスト認証の設定」を参照してください。

ヒント　エンド ユーザのダイジェスト認証を有効にしたが、ダイジェスト信用証明書は設定しなかった場合、電話機は登録できません。クラスタ モードが非セキュアで、ダイジェスト認証を有効にし、ダイジェスト信用証明書を設定した場合、ダイジェスト信用証明書は電話機に送信されますが、Cisco Unified Communications Manager でもチャレンジが開始されます。

トランクのダイジェスト認証

トランクに対してダイジェスト認証が有効になっている場合、Cisco Unified Communications Manager は、SIP トランク経由で接続する SIP デバイスおよびアプリケーションからの SIP トランク要求でチャレンジを行います。システムはチャレンジ メッセージで Cluster ID エンタープライズ パラメータを使用します。SIP トランクを通じて接続する SIP ユーザ エージェントは、Cisco Unified Communications Manager の管理ページで設定したデバイスまたはアプリケーション用の一意のダイジェスト信用証明書で応答します。

Cisco Unified Communications Manager が SIP トランク要求を開始すると、SIP トランクを介して接続する SIP ユーザ エージェントは Cisco Unified Communications Manager の ID をチャレンジできます。これらの着信するチャレンジに対して、管理者は SIP レルムを設定して要求されたクレデンシャルをユーザに提供します。Cisco Unified Communications Manager が SIP 401（Unauthorized）メッセージまたは SIP 407（Proxy Authentication Required）メッセージを受信すると、Cisco Unified Communications Manager は、トランク経由で接続するレルムおよびチャレンジ メッセージで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。Cisco Unified Communications Manager は、パスワードを復号化し、ダイジェストを計算し、これを応答メッセージで表します。

ヒント　レルムは SIP トランク経由で接続するドメイン（xyz.com など）を表し、要求の発信元の識別に役立ちます。

SIP レルムの設定方法の詳細については、「SIP トランクのダイジェスト認証の設定」（P.26-1）を参照してください。SIP レルムとユーザ名およびパスワードは、Cisco Unified Communications Manager に対してチャレンジができる SIP トランク ユーザ エージェントごとに Cisco Unified Communications Manager で設定する必要があります。各ユーザは、レルムごとにダイジェスト信用証明書のセットを 1 つ持つことができます。

許可

Cisco Unified Communications Manager は、許可プロセスを使用して、SIP を実行する電話機、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、一定のカテゴリを制限します。

- SIP インバイト メッセージと in-dialog メッセージ、および SIP を実行する電話機の場合、Cisco Unified Communications Manager はコーリング サーチ スペースおよびパーティションを通じて許可を与えます。
- 電話機からの SIP SUBSCRIBE 要求の場合、Cisco Unified Communications Manager 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、Cisco Unified Communications Manager はプレゼンス サブスクリプションおよび非インバイト SIP メッセージ（Out-of-Dialog REFER、Unsolicited NOTIFY、Replaces ヘッダー付き SIP 要求など）の許可を与えます。[SIP 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、許可する SIP 要求のチェックボックスをオンにして、許可を指定します。

SIP トランクのアプリケーションの許可を有効にするには、[SIP 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 [アプリケーションレベル認証を有効化 (Enable Application Level Authorization)] チェックボックスと [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てから、[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウで許可する SIP 要求のチェックボックスをオンにします。

SIP トランクの許可とアプリケーション レベルの許可の両方を有効にすると、最初に SIP トランクの許可が発生し、次に SIP アプリケーション ユーザの許可が発生します。トランクの場合、Cisco Unified Communications Manager 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 が SIP 要求を許可しない場合、コールは 403 Forbidden メッセージで失敗します。

ACL が SIP 要求を許可する場合、Cisco Unified Communications Manager 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)] でダイジェスト認証が有効かどうかを確認します。ダイジェスト認証が有効でなく、アプリケーションレベルの許可が有効でない場合、Cisco Unified Communications Manager は要求を処理します。ダイジェスト認証が有効な場合、Cisco Unified Communications Manager 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、Cisco Unified Communications Manager 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、Cisco Unified Communications Manager 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。そのため、アプリケーションレベルの許可を発生させるには、事前に [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)] でダイジェスト認証を有効にする必要があります。

暗号化の概要

ヒント　暗号化の機能は、Cisco Unified Communications Manager をサーバにインストールすると自動的にインストールされます。

ここでは、Cisco Unified Communications Manager がサポートする暗号化の種類について説明します。

- 「シグナリング暗号化」（P.1-22）
- 「メディア暗号化」（P.1-23）
- 「設定ファイルの暗号化」（P.1-24）

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 Cisco Unified Communications Manager サーバとの間で送信されるすべての SIP および SCCP シグナリング メッセージが確実に暗号化されます。

シグナリング暗号化は、各側に関連する情報、各側で入力された DTMF 番号、コール ステータス、メディア暗号鍵などについて、予期しないアクセスや不正アクセスから保護します。

クラスタを混合モードに設定した場合、Cisco Unified Communications Manager による Network Address Translation（NAT; ネットワーク アドレス変換）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 を有効にすると、メディア ストリームによるファイアウォールの通過が許可されます。UDP ALG を有効にすると、ファイアウォールの信頼できる側にあるメディア ソースが、ファイアウォールを介してメディア パケットを送信することにより、ファイアウォールを通過する双方向のメディア フローを開くことができます。

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

シグナリング暗号化では NAT トラバーサルをサポートしません。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。

SIP トランクは、シグナリング暗号化をサポートしますが、メディア暗号化はサポートしません。

メディア暗号化

メディア暗号化は Secure Real-Time Protocol（SRTP）を使用し、対象とする受信者だけが、サポートされるデバイス間のメディア ストリームを解釈できるようになります。サポートには、オーディオ ストリームだけが含まれます。メディア暗号化には、デバイス用のメディア マスター鍵ペアの作成、デバイスへの鍵配送、鍵転送中の配送の保護が含まれます。Cisco Unified Communications Manager は主に、IOS ゲートウェイ用、およびゲートキーパー制御トランクと非ゲートキーパー制御トランクの Cisco Unified Communications Manager H.323 トランク用に、また SIP トランクにおいて、SRTP をサポートします。

（注）　Cisco Unified Communications Managerは、デバイスおよびプロトコルに応じてメディア暗号鍵を異なる方法で処理します。SCCP を実行する電話機はすべて、Cisco Unified Communications Manager からメディア暗号鍵を取得します。この場合、メディア暗号鍵は、TLS で暗号化されたシグナリング チャネルによって電話機に安全にダウンロードされます。SIP を実行する電話機は、自身のメディア暗号鍵を生成して保存します。Cisco Unified Communications Manager システムで導出されたメディア暗号鍵は、暗号化されたシグナリング パス経由で、H.323 および MGCP では IPSec で保護されたリンクを通じて、SCCP および SIP では暗号化された TLS リンクを通じてゲートウェイに安全に送出されます。

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。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 デバイスから非セキュア デバイスへの転送、トランスコーディング、保留音などで発生する場合があります。

セキュリティがサポートされているほとんどのデバイスで、認証およびシグナリング暗号化は、メディア暗号化の最小要件となります。つまり、デバイスがシグナリング暗号化および認証をサポートしていない場合、メディア暗号化を行うことができません。Cisco IOS ゲートウェイおよびトランクは、認証なしのメディア暗号化をサポートします。SRTP 機能（メディア暗号化）を有効にする場合は、Cisco IOS ゲートウェイおよびトランクに対して IPSec を設定する必要があります。

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

SIP トランクは、TLS を使用して、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ぎます。

次の例で、SCCP および MGCP コールのメディア暗号化を示します。

1. メディア暗号化および認証をサポートするデバイス A とデバイス B があり、Cisco Unified Communications Manager に登録されています。
2. デバイス A がデバイス B に対してコールを行うと、Cisco Unified Communications Manager はキー マネージャ機能からメディア セッション マスター値のセットを 2 つ要求します。
3. 両方のデバイスで 2 つのセットを受信します。1 つはデバイス A からデバイス B へのメディア ストリーム用、もう 1 つはデバイス B からデバイス A へのメディア ストリーム用です。
4. デバイス A は最初のマスター値セットを使用して、デバイス A からデバイス B へのメディア ストリームを暗号化して認証する鍵を取得します。
5. デバイス A は 2 番目のマスター値セットを使用して、デバイス B からデバイス A へのメディア ストリームを認証して復号化する鍵を取得します。
6. これとは反対の操作手順で、デバイス B がこれらのセットを使用します。
7. 両方のデバイスは、鍵を受信した後に必要な鍵導出を実行し、SRTP パケット処理が行われます。

（注）　SIP を実行する電話機および H.323 トランク / ゲートウェイは、独自の暗号パラメータを生成し、Cisco Unified Communications Manager に送信します。

会議コールのメディア暗号化の詳細については、「セキュアな会議リソースの設定」（P.14-1）を参照してください。

設定ファイルの暗号化

Cisco Unified Communications Manager は、TFTP サーバからの設定ファイルのダウンロードで、機密データ（ダイジェスト信用証明書や管理者パスワードなど）を電話機に送出します。

Cisco Unified Communications Manager は、可逆暗号化を使用して、データベース内でこれらのクレデンシャルを保護します。ダウンロード プロセス中にこ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 Unified IP Phone（「サポートされる電話機のモデル」（P.11-4）を参照）で、暗号化された設定ファイルを設定することをお勧めします。このオプションが有効になっていると、デバイス設定ファイルだけがダウンロード用に暗号化されます。

（注）　状況によっては（たとえば、電話機のトラブルシューティングを行う場合や、自動登録中など）、暗号化されていない状態で機密データを電話機にダウンロードすることを選択することもできます。

Cisco Unified Communications Manager は、暗号鍵を符号化し、データベースに格納します。TFTP サーバは、対称暗号鍵を使用して、設定ファイルを暗号化および復号化します。

- 電話機に PKI 機能が備わっている場合、Cisco Unified Communications Manager は、電話機の公開鍵を使用して、電話機設定ファイルを暗号化できます。
- 電話機に PKI 機能が備わっていない場合は、Cisco Unified Communications Manager および電話機で一意の対称キーを設定する必要があります。

Cisco Unified Communications Manager の管理ページの [電話セキュリティプロファイルの設定(Phone Security Profile Configuration)] ウィンドウで、暗号化された設定ファイルの設定を有効にします。その後、[電話の設定 (Phone Configuration)] ウィンドウで、この設定を電話機に適用します。

詳細については、「電話機設定ファイルの暗号化について」（P.11-1）を参照してください。

NMAP スキャンの実行

Network Mapper（NMAP）スキャン プログラムは、脆弱性スキャンを実行するすべての Windows または Linux プラットフォームで実行できます。NMAP は、ネットワーク調査やセキュリティ監査に使用できる、無償かつオープン ソースのユーティリティです。

（注）　NMAP DP スキャンが完了するまで、最大で 18 時間かかることがあります。

構文

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

オプションおよびパラメータ：

-n：DNS 解決を行いません。NMAP が検出したアクティブな IP アドレスに対してリバース DNS 解決を行わないように指定します。NMAP で組み込みの並列なスタブ リゾルバを使用しても DNS の処理が遅くなる場合があるため、このオプションを使用するとスキャン時間を大幅に削減できます。

-v：冗長性レベルを上げます。冗長性レベルを上げると、NMAP で出力される進行中のスキャン情報が多くなります。開いているポートは検出され次第表示され、NMAP がスキャンに数分以上かかると予測した場合には推定完了時間が表示されます。このオプションを 2 回以上使用すると、冗長性がさらに上がります。

-sU：UDP ポートのスキャンを指定します。

-p：スキャンするポートを指定します（デフォルト値が上書きされます）。個々のポート番号の指定も、ハイフンを使用したポート番号の範囲の指定（例：1-1023）もできます。

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

設定用チェックリストの概要

表 1-5 に、認証および暗号化を実装するために必要なすべての作業を示します。また、各章には指定されたセキュリティ機能のために実行が必要な作業のチェックリストが含まれる場合もあります。

- 新規インストールで認証と暗号化を実装する手順については、表 1-5 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手順については、『*Installing Cisco Unified Communications Manager Release 6.1(1)*』を参照してください。このマニュアルには、ノードを追加する方法、および新しいノードにセキュリティを設定する方法が記載されています。

表 1-5　認証および暗号化の設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	Cisco Unified サービスアビリティで Cisco CTL Provider サービスをアクティブにします。 クラスタ内の各 Cisco Unified Communications Manager サーバで Cisco CTL Provider サービスを必ずアクティブにします。 **ヒント** Cisco Unified Communications Manager のアップグレード前にこのサービスをアクティブにした場合は、サービスを再度アクティブにする必要はありません。アップグレード後にサービスは自動的にアクティブになります。	「Cisco CTL Provider サービスのアクティブ化」（P.4-5）

表 1-5　認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 2	Cisco Unified サービスアビリティで Cisco Certificate Authority Proxy サービスをアクティブにし、ローカルで有効な証明書のインストール、アップグレード、トラブルシューティング、または削除を行います。 最初のノードでのみ Cisco Certificate Authority Proxy サービスをアクティブにします。 **ワンポイントアドバイス**　Cisco CTL クライアントをインストールして設定する前にこの作業を実行すれば、CAPF を使用するために CTL ファイルを更新する必要がなくなります。	「Certificate Authority Proxy Function サービスのアクティブ化」（P.10-6）
ステップ 3	デフォルトのポート設定を使用しない場合は、TLS 接続用のポートを設定します。 **ヒント**　これらの設定を Cisco Unified Communications Manager のアップグレード前に設定した場合、設定はアップグレード時に自動的に移行されます。	「TLS 接続用ポートの設定」（P.4-6）
ステップ 4	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。	「Cisco CTL クライアントの設定」（P.4-10）
ステップ 5	Cisco CTL クライアントをインストールします。 **ヒント**　今回のリリースの Cisco 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 Cisco Unified Communications Manager の管理機能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。	• 「システム要件」（P.1-5） • 「インストール」（P.1-14） • 「Cisco CTL クライアントのインストール」（P.4-8） • 「Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行」（P.4-9）
ステップ 6	Cisco CTL クライアントを設定します。 **ヒント**　Cisco 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時に自動的に移行されます。今回のリリースの Cisco 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。	• 「Cisco CTL クライアントの設定」（P.4-10） • 「Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行」（P.4-9）

表 1-5　認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 7	電話機のセキュリティ プロファイルを設定します。プロファイルを設定するときは、次の作業を実行します。 • デバイスのセキュリティ モードを設定します。 **ヒント** デバイス セキュリティ モードは、Cisco Unified Communications Manager のアップグレード時に自動的に移行されます。以前のリリースの認証だけをサポートしていたデバイスに暗号化を設定する場合は、[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。 • CAPF 設定を定義します（SCCP および SIP を実行す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。 • SIP を実行する電話機でダイジェスト認証を使用する場合は、[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。 • 暗号化された設定ファイルを有効にするには（SCCP および SIP を実行する一部の電話機の場合）、[TFTP暗号化(TFTP Encrypted Config)] チェックボックスをオンにします。 • 設定ファイルのダウンロードでダイジェスト信用証明書を除外するには、[設定ファイル内のダイジェスト信用証明書を除外(Exclude Digest Credentials in Configuration File)] チェックボックスをオンにします。	「電話機セキュリティ プロファイルの設定」(P.7-4) 「電話機セキュリティ プロファイルの設定のヒント」(P.7-2) 「暗号化された電話機設定ファイルの設定」(P.11-1) 「暗号化された設定ファイルの設定のヒント」(P.11-4)
ステップ 8	電話機に電話機セキュリティ プロファイルを適用します。	「電話機セキュリティ プロファイルの適用」(P.7-10)
ステップ 9	電話機に証明書を発行するように CAPF を設定します。 **ヒント** 今回のリリースの Cisco Unified Communications Manager へのアップグレード前に証明書の操作を実行して CAPF をサブスクライバ サーバで実行した場合、CAPF データをパブリッシャ データベース サーバにコピーしてから、クラスタを今回のリリースの Cisco Unified Communications Manager にアップグレードする必要があります。 ⚠ **注意** Cisco Unified Communications Manager サブスクライバ サーバの CAPF データは Cisco Unified Communications Manager データベースに移行されません。したがって、データをデータベースにコピーしないと、データは失われます。データが失われても、CAPF ユーティリティを使用して発行したローカルで有効な証明書は電話機に残ります。しかし、この証明書はもう有効でないため、今回のリリースの CAPF ユーティリティは証明書を再発行する必要があります。	• 「システム要件」(P.1-5) • 「CAPF の設定用チェックリスト」(P.10-5)

表 1-5　認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 10	サポートされている Cisco Unified IP Phone にローカルで有効な証明書がインストールされたことを確認します。	• 「システム要件」（P.1-5） • 「電話機での認証文字列の入力」（P.10-11）
ステップ 11	SIP を実行する電話機のダイジェスト認証を設定します。	• 「SIP 電話機のダイジェスト認証の設定」（P.12-1）
ステップ 12	電話機のセキュリティ強化作業を実行します。 **ヒント** 電話機のセキュリティ強化設定を Cisco 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時に自動的に移行されます。	• 「電話機のセキュリティ強化」（P.13-1）
ステップ 13	セキュリティ用の会議ブリッジを設定します。	• 「セキュアな会議リソースの設定」（P.14-1）
ステップ 14	セキュリティ用のボイスメール ポートを設定します。	• 「ボイスメール ポートのセキュリティ設定」（P.15-1） • 今回のリリースの Cisco Unified Communications Manager に該当する Cisco Unity または Cisco Unity Connection のインテグレーション ガイド
ステップ 15	SRST 参照先のセキュリティを設定します。 **ヒント** 前のリリースの Cisco Unified Communications Manager でセキュア SRST 参照先を設定した場合は、Cisco Unified Communications Manager のアップグレード時にその設定が自動的に移行されます。	• 「セキュア SRST（Survivable Remote Site Telephony）参照先の設定」（P.23-1）
ステップ 16	IPSec を設定します。	• 「ゲートウェイおよびトランクの暗号化の設定」（P.24-1） • 「ネットワーク インフラストラクチャで IPSec を設定する場合の注意事項」（P.24-5） • 『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』 • 『*Cisco Unified Communications Operating System Administration Guide*』

表 1-5　認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 17	SIP トランク セキュリティ プロファイルを設定します。 ダイジェスト認証を使用する場合は、プロファイルの [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。 トランクレベルの許可の場合、許可する SIP 要求の許可チェックボックスをオンにします。 トランクレベルの許可の後、アプリケーションレベルの許可を発生させる場合は、[アプリケーションレベル認証を有効化(Enable Application Level Authorization)] チェックボックスをオンにします。 ダイジェスト認証をオンにしない場合、アプリケーションレベルの許可はオンにできません。	• 「SIP トランク セキュリティ プロファイルの設定」（P.25-1） • 「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」（P.26-2）
ステップ 18	SIP トランク セキュリティ プロファイルをトランクに適用します。	• 「SIP トランク セキュリティ プロファイルの適用」（P.25-8）
ステップ 19	トランクのダイジェスト認証を設定します。	• 「SIP トランクのダイジェスト認証の設定」（P.26-1）
ステップ 20	SIP トランク セキュリティ プロファイルで [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)] ウィンドウの許可チェックボックスをオンにして、許可する SIP 要求を設定します。	• 「SIP トランク セキュリティ プロファイルの設定」（P.25-1） • 「許可」（P.1-21）
ステップ 21	すべての電話機をリセットします。	「デバイスのリセット、サービスの再起動またはリブート」（P.1-12）
ステップ 22	すべてのサーバをリブートします。	「デバイスのリセット、サービスの再起動またはリブート」（P.1-12）

参考情報

シスコの関連マニュアル

Cisco IP テレフォニー関連のアプリケーションと製品の詳細は、次の資料を参照してください。

- 『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』
- 『*Cisco Unified Communications Operating System Administration Guide*』
- 『*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 対応ゲートウェイをサポートする Cisco Unified Survivable Remote Site Telephony（SRST）の管理マニュアル
- 『*Disaster Recovery System Administration Guide*』
- 『*Cisco Unified Communications Manager Bulk Administration ガイド*』
- 『*Troubleshooting Guide for Cisco Unified Communications Manager*』
- ご使用の電話機モデルをサポートしているファームウェア リリース ノート

CHAPTER 2

HTTP over SSL（HTTPS）の使用方法

この章は、次の内容で構成されています。

HTTPS の概要

Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS; HTTP over SSL）は、Microsoft Windows ユーザのために、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、ブラウザ接続を保護します。HTTPS は公開鍵を使用して、インターネット経由で転送されるデータ（ユーザのログインやパスワードを含む）を暗号化します。

HTTPS を有効にするには、接続プロセス中にサーバを識別する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でサーバ証明書を受け入れることができます。また、信頼できるフォルダ（ファイル）に証明書をダウンロードすると、そのサーバとの現在のセッションおよび将来のセッションを保護することができます。信頼できるフォルダには、すべての信頼できるサイトの証明書が格納されています。

シスコは、Cisco Unified Communications Manager 内の Cisco Tomcat Web サーバ アプリケーションへの接続で次のブラウザをサポートしています。

- Microsoft Internet Explorer（IE）7（Microsoft Windows XP SP3 で実行されている場合）
- Microsoft Internet Explorer（IE）8（Microsoft Windows XP SP3 または Microsoft Vista SP2 で実行されている場合）
- Firefox 3.x（Microsoft Windows XP SP3、Microsoft Vista SP2、または Apple MAC OS X で実行されている場合）
- Safari 4.x（Apple MAC OS X で実行されている場合）

（注）　Cisco 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。自己署名証明書は、アップグレード中に自動的に Cisco Unified Communications Manager に移行されます。この証明書のコピーは、.DER 形式および .PEM 形式で作成されます。

自己署名証明書は、Cisco Unified Communications オペレーティング システムの GUI を使用して再生成できます。詳細については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

表 2-1 に、Cisco Unified Communications Manager 内の、Cisco Tomcat で HTTPS を使用するアプリケーションを示します。

表 2-1　Cisco Unified Communications Manager の HTTPS アプリケーション

Cisco Unified Communications Manager の HTTPS アプリケーション	Web アプリケーション
ccmadmin	Cisco Unified Communications Manager の管理
ccmservice	Cisco Unified サービスアビリティ
cmplatform	オペレーティング システムの管理
cmuser	Cisco Personal Assistant
ast	Real-Time Monitoring Tool
RTMTReports	Real-Time Monitoring Tool レポート アーカイブ
PktCap	パケット キャプチャに使用する TAC トラブルシューティング ツール
art	Cisco Unified Communications Manager CDR Analysis and Reporting
taps	Cisco Unified Communications Manager Auto-Register Phone Tool
dna	Dialed Number Analyzer
drf	ディザスタ リカバリ システム
SOAP	Cisco Unified Communications Manager データベースに対して読み書きを行うための Simple Object Access Protocol API （注）　セキュリティのために、SOAP を使用するすべての Web アプリケーションで HTTPS が必要です。シスコは、SOAP アプリケーションで HTTP をサポートしません。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、このようなアプリケーションを HTTPS に変換することはできません。

Cisco Unified IP Phone サービスでの HTTPS

リリース 8.0 よりも前の Cisco Unified Communications Manager では、Cisco Unified IP Phone および Cisco Unified IP Phone サービスで HTTPS 通信がサポートされておらず、ポート 8080 で「クリア テキスト」を使用して通信が行われていました。

Cisco Unified Communications Manager リリース 8.0 では、Cisco Unified IP Phone および Cisco Unified IP Phone サービスで、HTTPS、暗号化、およびポート 8443 によるサーバの安全な識別がサポートされています。

サポートされるデバイス

HTTPS をサポートしている Cisco Unified IP Phone は、次のとおりです。

- 7906
- 7911
- 7931
- 7941
- 7961
- 7970
- 7942
- 7945
- 7962
- 7965
- 7975

サポートされる機能

HTTPS をサポートしている機能は、次のとおりです。

- Cisco Extension Mobility（EM; エクステンション モビリティ）
- Cisco Extension Mobility Cross Cluster（EMCC; クラスタ間のエクステンション モビリティ）
- Cisco Unified Communications Manager の Manager Assistant（IPMA）
- Cisco Unified IP Phone サービス
- パーソナル ディレクトリ
- クレデンシャル変更

Cisco Unified IP Phone サービスの設定内容

Cisco Unified Communications Manager リリース 8.0(1) では、HTTPS をサポートするために、電話機の設定内容に表 2-2 に示すセキュア URL パラメータが含まれています。

セキュア URL パラメータを設定するには、Cisco Unified Communications Manager の管理ページから [デバイス(Device)] > [デバイスの設定(Device Settings)] > [IP Phone サービス(Phone Services)] の順に選択します。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「Cisco Unified IP Phone サービスの設定」の章を参照してください。

表 2-2　セキュア URL 用の電話機の設定内容

フィールド	説明
[セキュア認証 URL(Secure Authentication URL)]	電話機の Web サーバに対する要求を検証するために、この電話機が使用するセキュア URL を入力します。 **（注）** [セキュア認証 URL(Secure Authentication URL)] の値を指定しないと、デバイスでは非セキュア URL が使用されます。セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。 デフォルトでは、この URL は、インストール時に設定された [Cisco Unified CM のユーザ オプション(Cisco Unified CM User Options)] ウィンドウにアクセスします。 デフォルト値を受け入れるには、このフィールドをブランクのままにします。 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となるサーバのセキュア URL を入力します。このパラメータには、ディレクトリ ボタンを押したときに、セキュリティで保護された Cisco Unified IP Phone が使用する URL を指定します。 **（注）** [セキュアディレクトリ URL(Secure Directory URL)] の値を指定しないと、デバイスでは非セキュア URL が使用されます。セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。 デフォルト値を受け入れるには、このフィールドをブランクのままにします。 最大長：255
[セキュアアイドル URL(Secure Idle URL)]	[アイドルタイマー (Idle Timer、秒)] フィールドの指定に従って電話機がアイドル状態になったときに、Cisco Unified IP Phone のディスプレイに表示する情報のセキュア URL を入力します。たとえば、電話機が 5 分間使用されなかったときに、LCD 上にロゴを表示できます。 **（注）** [セキュアアイドル URL(Secure Idle URL)] の値を指定しないと、デバイスでは非セキュア URL が使用されます。セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。 デフォルト値を受け入れるには、このフィールドをブランクのままにします。 最大長：255

表 2-2　セキュア URL 用の電話機の設定内容（続き）

フィールド	説明
[セキュア情報URL(Secure Information URL)]	Cisco Unified IP Phone がヘルプ テキスト情報を検索できるサーバの場所を示すセキュア URL を入力します。この情報は、ユーザが情報（[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(Secure Information URL)] の値を指定しないと、デバイスでは非セキュア URL が使用されます。セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。 デフォルト値を受け入れるには、このフィールドをブランクのままにします。 最大長：255
[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。ユーザがメッセージ ボタンを押すと、Cisco Unified IP Phone はこの URL に接続されます。 **（注）** [セキュアメッセージURL(Secure Messages URL)] の値を指定しないと、デバイスでは非セキュア URL が使用されます。セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。 デフォルト値を受け入れるには、このフィールドをブランクのままにします。 最大長：255
[セキュアサービスURL(Secure Services URL)]	Cisco Unified IP Phone サービスのセキュア URL を入力します。これは、ユーザがサービス ボタンを押すと、セキュリティ保護された Cisco Unified IP Phone が接続される場所です。 **（注）** [セキュアサービスURL(Secure Services URL)] の値を指定しないと、デバイスでは非セキュア URL が使用されます。セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。 デフォルト値を受け入れるには、このフィールドをブランクのままにします。 最大長：255

エンタープライズ パラメータの設定内容

HTTPS をサポートするために、Cisco Unified Communications Manager リリース 8.0(1) では次の新しいエンタープライズ パラメータをサポートしています。

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

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

ブラウザを再起動するたびに証明書をリロードせずに、アクセスを保護するには、必ず Cisco Unified Communications Manager の証明書を Internet Explorer 8 にインポートします。証明書の警告が表示された Web サイトへのアクセスを続行する場合、その証明書が信頼ストアに存在しないときは、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 は引き続き Web サイトの証明書エラーを表示します。ブラウザの [信頼されたルート証明機関] 信頼ストアにインポート済み証明書が含まれている場合は、このセキュリティ警告を無視できます。

Internet Explorer 8 のルート証明書信頼ストアに Cisco Unified Communications Manager 証明書をインポートする手順は、次のとおりです。

手順

ステップ 1　Tomcat サーバのアプリケーションを参照します（たとえば、ブラウザに Cisco Unified Communications Manager の管理ページのホスト名、ローカルホスト、または IP アドレスを入力します）。

ブラウザに、この Web サイトが信頼されていないことを示す「証明書のエラー：ナビゲーションはブロックされました」というメッセージが表示されます。

ステップ 2　サーバにアクセスするには、[このサイトの閲覧を続行する (推奨されません)。] をクリックします。

[Cisco Unified Communications Manager の管理] 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] ステータスが赤色で表示されます。

ステップ 3　サーバ証明書をインポートするには、[証明書のエラー] 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。レポートで [証明書の表示] リンクをクリックします。

ステップ 4　証明書の詳細を確認します。

ステップ 5　[証明書] ウィンドウで [全般] タブを選択し、[証明書のインストール] をクリックします。

[証明書のインポート ウィザード] が起動します。

ステップ 6　[次へ] をクリックして、ウィザードを開始します。

[証明書ストア] ウィンドウが表示されます。

ステップ 7　[自動] オプション（ウィザードがこの証明書タイプの証明書ストアを選択できる）が選択されていることを確認し、[次へ] をクリックします。

ステップ 8　設定を確認し、[完了] をクリックします。

インポート操作に関するセキュリティ警告が表示されます。

ステップ 9　[はい] をクリックして、証明書をインストールします。

インポート ウィザードに「インポートに成功しました」と表示されます。

ステップ 10　[OK] をクリックします。次回 [証明書の表示] リンクをクリックすると、[証明書] ウィンドウの [証明書のパス] タブに「この証明書は問題ありません」と表示されます。

ステップ 11　インポートした証明書が信頼ストアにあることを確認するには、Internet Explorer のツールバーで [ツール] > [インターネット オプション] をクリックし、[コンテンツ] タブを選択します。[証明書] をクリックし、[信頼されたルート証明機関] タブを選択します。リストをスクロールして、インポートした証明書を見つけます。

証明書のインポート後も引き続き、ブラウザにアドレス バーと [証明書のエラー] ステータスが赤色で表示されます。ホスト名、ローカルホスト、または IP アドレスを再入力しても、ブラウザをリフレッシュまたは再起動しても、このステータスは変わりません。

追加情報

「関連項目」（P.2-12）を参照してください。

証明書のファイルへのコピー

証明書をファイルにコピーし、ローカルに保管することによって、必要なときにいつでも証明書を復元することができます。

次の手順を実行すると、標準の証明書保管形式で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

ステップ 1　[証明書のエラー] ステータス ボックスをクリックします。

ステップ 2　[証明書の表示] をクリックします。

ステップ 3　[詳細設定] タブをクリックします。

ステップ 4　[ファイルにコピー] ボタンをクリックします。

ステップ 5　[証明書のエクスポート ウィザード] が表示されます。[次へ] をクリックします。

ステップ 6　ファイル形式を定義する次のリストから選択することができます。エクスポート ファイルに使用するファイル形式を選択して、[次へ] をクリックします。

- [DER encoded binary X.509 (.CER)] : DER を使用してエンティティ間で情報を転送します。
- [Base-64 encoded X.509 (.CER)] : 保護されたバイナリ添付ファイルをインターネット経由で送信します。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。
- [Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)] : 証明書と、認証パス内のすべての証明書を、選択した PC にエクスポートします。

ステップ 7　ファイルのコピーをエクスポートする場所に移動して、ファイルの名前を指定します。[保存] をクリックします。

ステップ 8　ファイル名とパスが [証明書のエクスポート ウィザード] ペインに表示されます。[次へ] をクリックします。

ステップ 9　ファイルと設定が表示されます。[終了] をクリックします。

ステップ 10　エクスポートが正常に行われたことを示すダイアログボックスが表示されたら、[OK] をクリックします。

追加情報

「関連項目」（P.2-12）を参照してください。

Firefox での HTTPS の使用方法

Cisco Unified Communications Manager をインストールまたはアップグレードした後に、初めて Cisco Unified Communications Manager の管理ページまたは他の Cisco Unified Communications Manager SSL 対応仮想ディレクトリにブラウザ クライアントからアクセスすると、サーバを信頼するかどうかを確認するセキュリティ警告のダイアログボックスが表示されます。

ダイアログボックスが表示されたら、次の作業のいずれか 1 つを実行する必要があります。

- [危険性を理解した上で接続するには] をクリックして、現在の Web セッションに対してだけ証明書を信頼します。現在のセッションに対してだけ証明書を信頼すると、セキュリティ警告のダイアログボックスは、信頼できるフォルダに証明書をインストールするまで、アプリケーションにアクセスするたびに表示されます。
- [スタートページに戻る] をクリックして、操作を取り消します。認証は行われず、Web アプリケーションにアクセスすることはできません。Web アプリケーションにアクセスするには、[危険性を理解した上で接続するには] をクリックする必要があります。

次の各項では、Firefox ブラウザで HTTPS を使用する方法について説明します。

- 「Firefox 3.x を使用して証明書を信頼できるフォルダに保存する方法」（P.2-8）
- 「証明書のファイルへのコピー」（P.2-9）

Firefox 3.x を使用して証明書を信頼できるフォルダに保存する方法

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

手順

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

ステップ 2　セキュリティ警告のダイアログボックスが表示されたら、[危険性を理解した上で接続するには] をクリックします。

ステップ 3　[例外を追加] をクリックします。

[セキュリティ例外の追加] ダイアログボックスが表示されます。

ステップ 4　[証明書を取得] をクリックします。

ステップ 5　[次回以降にもこの例外を有効にする] チェックボックスをオンにします。

ステップ 6　[セキュリティ例外を承認] をクリックします。

ステップ 7　証明書の詳細を表示するには、次の手順に従います。

a. Firefox ブラウザから、[ツール] > [オプション] をクリックします。

[オプション] ダイアログボックスが表示されます。

b. [詳細] をクリックします。

c. [証明書を表示] をクリックします。

[証明書マネージャ] ダイアログボックスが表示されます。

d. 表示する証明書を強調表示して、[表示] をクリックします。

[証明書ビューア] ダイアログボックスが表示されます。

e. [詳細] タブをクリックします。

f. [証明書のフィールド] フィールドで、表示するフィールドを強調表示します。

[フィールドの値] フィールドに詳細が表示されます。

g. [証明書ビューア] ダイアログボックスで、[閉じる] をクリックします。

h. [証明書マネージャ] ダイアログボックスで、[OK] をクリックします。

証明書のファイルへのコピー

証明書をファイルにコピーし、ローカルに保管することによって、必要なときにいつでも証明書を復元することができます。

次の手順を実行すると、標準の証明書保管形式で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

ステップ 1　Firefox ブラウザから、[ツール] > [オプション] をクリックします。

[オプション] ダイアログボックスが表示されます。

ステップ 2　まだ選択されていない場合は、[詳細] をクリックします。

ステップ 3　[暗号化] タブをクリックして、[証明書を表示] をクリックします。

[証明書マネージャ] ダイアログボックスが表示されます。

ステップ 4　[サーバ証明書] タブをクリックします。

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

[証明書をファイルに保存] ダイアログボックスが表示されます。

ステップ 6　ファイルのコピー先に移動します。

ステップ 7　[ファイルの種類] ドロップダウン リストで、次のオプションからファイル タイプを選択します。

- [X.509 証明書（PEM）] : **PEM** を使用してエンティティ間で情報を転送します。
- [証明書パスを含む X.509 証明書（PEM）] : プライバシー エンハンスト 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 証明書（DER）] : **DER** を使用してエンティティ間で情報を転送します。

- [X.509 証明書（PKCS#7）]：PKCS#7 は、データの署名または暗号化の標準です。署名されたデータの検証に必要になるため、証明書を SignedData 構造に含めることができます。.P7C ファイルは、署名が必要なデータを持たない縮退した SignedData 構造です。
- [証明書パスを含む X.509 証明書（PKCS#7）]：PKCS#7 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。

ステップ 8　[保存] をクリックします。

ステップ 9　[OK] をクリックします。

追加情報

「関連項目」（P.2-12）を参照してください。

Safari での HTTPS の使用方法

Cisco Unified Communications Manager をインストールまたはアップグレードした後に、初めて Cisco Unified Communications Manager の管理ページまたは他の Cisco Unified Communications Manager SSL 対応仮想ディレクトリにブラウザ クライアントからアクセスすると、サーバを信頼するかどうかを確認する [セキュリティの警告] ダイアログボックスが表示されます。

ダイアログボックスが表示されたら、次の作業のいずれか 1 つを実行する必要があります。

- [はい] をクリックして、現在の Web セッションについてだけ証明書を信頼するように選択します。現在のセッションに対してだけ証明書を信頼すると、[セキュリティの警告] ダイアログボックスは、信頼できるフォルダに証明書をインストールするまで、アプリケーションにアクセスするたびに表示されます。
- [証明書を表示] > [証明書のインストール] の順にクリックして、証明書のインストール作業を実行します。この場合、常に証明書を信頼することになります。信頼できるフォルダに証明書を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たびに [セキュリティの警告] ダイアログボックスが表示されることはありません。
- [いいえ] をクリックして、操作を取り消します。認証は行われず、Web アプリケーションにアクセスすることはできません。Web アプリケーションにアクセスするには、[はい] をクリックするか、または [証明書を表示] > [証明書のインストール] オプションを使用して証明書をインストールする必要があります。

（注）　Cisco Unified Communications Manager へのアクセスに使用するアドレスは、証明書に記載されてい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 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が、アクセスしているサイトの名前と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。

次の各項では、Safari で HTTPS を使用する方法について説明します。

- 「Safari 4 を使用して証明書を信頼できるフォルダに保存する方法」（P.2-11）
- 「証明書のファイルへのコピー」（P.2-11）

Safari 4 を使用して証明書を信頼できるフォルダに保存する方法

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

手順

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

ステップ 2　[セキュリティの警告] ダイアログボックスが表示されたら、[証明書を表示] をクリックします。

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

- [すべて] : すべてのオプションが [詳細] ペインに表示されます。
- [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]、[発行者]、[有効期間の開始]、[有効期間の終了]、[サブジェクト]、および [公開キー] の各オプションが表示されます。
- [拡張機能のみ] : [サブジェクト キー識別子]、[キー使用法]、および [拡張キー使用法] の各オプションが表示されます。
- [重要な拡張機能のみ] : 存在する場合は [重要な拡張機能] が表示されます。
- [プロパティのみ] : [拇印アルゴリズム] と [拇印] オプションが表示されます。

ステップ 3　[証明書] ペインの [証明書のインストール] をクリックします。

ステップ 4　[証明書のインポート ウィザード] が表示されたら、[次へ] をクリックします。

ステップ 5　[証明書をすべて次のストアに配置する] オプション ボタンをクリックし、[参照] をクリックします。

ステップ 6　[信頼されたルート証明機関] を参照し、選択して、[OK] をクリックします。

ステップ 7　[次へ] をクリックします。

ステップ 8　[完了] をクリックします。

[セキュリティ警告] ボックスに証明書の拇印が表示されます。

ステップ 9　[はい] をクリックして、証明書をインストールします。

インポートが正常に行われたことを示すメッセージが表示されます。[OK] をクリックします。

ステップ 10　ダイアログボックスの右下に表示される [OK] をクリックします。

ステップ 11　証明書を信頼して、今後このダイアログボックスを表示しないようにするには、[はい] をクリックします。

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

証明書のファイルへのコピー

証明書をファイルにコピーし、ローカルに保管することによって、必要なときにいつでも証明書を復元することができます。

次の手順を実行すると、標準の証明書保管形式で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

ステップ 1　[セキュリティの警告] ダイアログボックスで、[証明書を表示] をクリックします。

ヒント　Safari の場合は、[証明書のエラー] ステータス ボックスをクリックして、[証明書を表示] オプションを表示します。

ステップ 2　[詳細] タブをクリックします。

ステップ 3　[ファイルにコピー] ボタンをクリックします。

ステップ 4　[証明書のエクスポート ウィザード] が表示されます。[次へ] をクリックします。

ステップ 5　ファイル形式を定義する次のリストから選択することができます。エクスポート ファイルに使用するファイル形式を選択して、[次へ] をクリックします。

- [DER encoded binary X.509 (.CER)] : DER を使用してエンティティ間で情報を転送します。
- [Base 64 encoded X.509 (.CER)] : 保護されたバイナリ添付ファイルをインターネット経由で送信します。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。
- [Cryptographic Message Syntax Standard-PKCS #7 証明書 (.P7B)] : 証明書と、認証パス内のすべての証明書を、選択した PC にエクスポートします。

ステップ 6　ファイルのコピーをエクスポートする場所に移動して、ファイルの名前を指定します。[保存] をクリックします。

ステップ 7　ファイル名とパスが [証明書のエクスポート ウィザード] ペインに表示されます。[次へ] をクリックします。

ステップ 8　ファイルと設定が表示されます。[終了] をクリックします。

ステップ 9　エクスポートが正常に行われたことを示すダイアログボックスが表示されたら、[OK] をクリックします。

追加情報

「関連項目」（P.2-12）を参照してください。

参考情報

関連項目

「証明書」（P.1-15）

シスコの関連マニュアル

- 『*Cisco Unified Serviceability Administration Guide*』
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』
- 入手可能な HTTPS 関連の Microsoft の資料

CHAPTER 3

デフォルトのセキュリティ

ここでは、次の内容について説明します。

概要

デフォルトのセキュリティは、次の自動セキュリティ機能を Cisco Unified IP Phone に提供します。

- 電話機設定ファイルの署名
- 電話機設定ファイルの暗号化に対するサポート
- Tomcat および他の Web サービス（MIDlet）での https

Cisco Unified Communications Manager リリース 8.0 では、CTL クライアントを実行せずに、これらのセキュリティ機能をデフォルトで使用できます。

（注） セキュアなシグナリングおよびメディアについては、引き続き CTL クライアントを実行して、ハードウェア eToken を使用することが必要です。

信頼検証サービス

Trust Verification Service（TVS; 信頼検証サービス）は、デフォルトのセキュリティの主要コンポーネントです。TVS を使用すると、HTTPS を確立しているときに、Cisco Unified IP Phone 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。

TVS で提供される機能は次のとおりです。

- スケーラビリティ：Cisco Unified IP Phone 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が、システム内で自動的に反映されます。
- デフォルトのセキュリティ：メディアおよびシグナリングのセキュリティ以外の機能はデフォルトのインストールに含まれており、ユーザ操作は必要ありません。

（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には、CTL クライアントが必要です。

TVS の概要

信頼検証サービスの基本概念は次のとおりです。

- TVS は Cisco Unified Communications Manager サーバで稼動して、Cisco Unified IP Phone の代わりに証明書を認証します。
- 信頼できる証明書をすべてダウンロードするのではなく、Cisco Unified IP Phone では TVS を信頼するだけで済みます。
- TVS 証明書およびいくつかのキー証明書が、Identity Trust List（ITL; ID 信頼リスト）という新しいファイルにまとめられます。
- ITL ファイルは、ユーザ操作なしで自動的に生成されます。
- ITL ファイルは、Cisco Unified IP Phone によってダウンロードされ、ここから信頼情報が取得されます。

初期信頼リスト

次のタスクを実行するには、Cisco Unified IP Phone に Initial Trust List（ITL; 初期信頼リスト）が必要です。

- 設定ファイルの署名の認証
- CAPF との安全な通話（設定ファイルの暗号化をサポートするための前提条件）
- TVS に対する信頼（特に https 証明書の認証）

Cisco Unified IP Phone に既存の CTL ファイルがない場合、最初の ITL ファイルが（CTL ファイルの場合と同様に）自動的に信頼されます。後続の ITL ファイルが同じ TFTP 秘密鍵で署名されているか、または TVS で署名者に応じた証明書を返すことができる必要があります。

Cisco Unified IP Phone に既存の CTL ファイルがある場合は、その CTL ファイルを使用して ITL ファイルの署名を認証します。

ITL ファイル

ITL ファイルには、初期信頼リストが格納されます。ITL ファイルは CTL ファイルと同じ形式で、基本的には CTL ファイルの小型版または縮小版です。ITL ファイルに適用される属性は、次のとおりです。

- CTL ファイルとは異なり、ITL ファイルはクラスタのインストール時にシステムによって自動的に作成され、内容の変更が必要になった場合には、自動的に更新されます。
- ITL ファイルに eToken は不要です。このファイルはソフト eToken（TFTP 秘密鍵）を使用します。
- ITL ファイルは、ブート時またはリセット時に CTL ファイル（ある場合）がダウンロードされた後すぐに、Cisco Unified IP Phone によってダウンロードされます。

ITL ファイルの内容

ITL ファイルには、次の証明書が含まれます。

- TFTP サーバの証明書。この証明書を使用すると、ITL ファイルの署名および電話機設定ファイルの署名を認証できます。
- クラスタ内のすべての TVS 証明書。この証明書を使用すると、電話機は TVS と安全に通信して証明書認証を要求できます。
- CAPF 証明書。この証明書を使用すると、設定ファイルの暗号化をサポートできます。ITL ファイルに必須というわけではありませんが（TVS で認証できる）、CAPF 証明書によって CAPF への接続が簡易化されます。

CTL ファイルと同様に、ITL ファイルには証明書ごとに 1 つのレコードが格納されます。各レコードの内容は次のとおりです。

- 証明書
- Cisco Unified IP Phone による簡易検索のために事前抽出された証明書フィールド
- 証明書権限（TFTP、CUCM、TFTP+CCM、CAPF、TVS、SAST）

TFTP 証明書は、次の 2 つの異なる権限を持つ 2 つの ITL レコードに含まれています。

- TFTP または TFTP+CCM 権限：設定ファイルの署名を認証します。
- SAST 権限：ITL ファイルの署名を認証します。

ITL ファイルと CTL ファイルの相互作用

Cisco Unified IP Phone では、クラスタのセキュリティ モード（非セキュアまたは混合モード）を確認するのに依然として CTL ファイルを使用します。CTL ファイルは、Cisco Unified Communications Manager のレコードに Cisco Unified Communications Manager の証明書を格納することで、クラスタ セキュリティ モードを追跡します。

ITL ファイルにも、クラスタ セキュリティ モードを示す情報が格納されます。

自動登録

クラスタが非セキュア モードの場合、システムによって自動登録がサポートされます。また、デフォルトの設定ファイルに対する署名も行われます。デフォルトのセキュリティをサポートしていない Cisco Unified IP Phone には、署名されていないデフォルトの設定ファイルが提供されます。

（注）　混合モードでは、自動登録はサポートされません。

サポートされている Cisco Unified IP Phone

Cisco Unified Reporting を使用すると、デフォルトのセキュリティをサポートしている Cisco Unified IP Phone のリストを取得できます。Cisco Unified Reporting を使用するには、次の手順に従います。

手順

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

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

ステップ 3　[Feature] プルダウン メニューから、適切な機能を選択します。

ステップ 4　[Submit] をクリックします。

Cisco Unified Reporting の使用方法の詳細については、『*Cisco Unified Reporting Administration Guide*』を参照してください。

証明書の再生成

Cisco Unified Communications Manager の証明書の 1 つを再生成する場合には、この項の手順を実行する必要があります。

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。

	手順	追加情報
ステップ 1	CAPF 証明書を再生成します。	『*Cisco Unified Communications Operating System Administration Guide*』の第 6 章「Security」を参照してください。
ステップ 2	CAPF サービスを再起動します。	「Certificate Authority Proxy Function サービスのアクティブ化」を参照してください。
ステップ 3	現在 TFTP サービスが稼動しているサーバで、このサービスを再起動します。	「TFTP サーバでの Cisco TFTP サービスの再起動」（P.3-6）を参照してください。
ステップ 4	Cisco Unified IP Phone をリセットします。	「すべての Cisco Unified IP Phone のリセット」（P.3-10）を参照してください。

TVS 証明書の再生成

TVS 証明書を再生成するには、次の手順を実行します。

（注）　クラスタ内のすべての TVS 証明書を再生成する場合、これらの手順は、すべての証明書を再生成した後に実行できます。

（注）　TVS および TFTP の両方の証明書を再生成する場合は、常にこれらの手順を実行してから TFTP 証明書を再生成します。この手順に従わないと、すべての Cisco Unified IP Phone から手動で ITL ファイルを削除することが必要になる場合があります。

	手順	追加情報
ステップ 1	TVS 証明書を再生成します。	『*Cisco Unified Communications Operating System Administration Guide*』の第 6 章「Security」を参照してください。
ステップ 2	現在 TFTP サービスが稼動しているサーバで、このサービスを再起動します。	詳細については、「TFTP サーバでの Cisco TFTP サービスの再起動」（P.3-6）を参照してください。
ステップ 3	Cisco Unified IP Phone をリセットします。	詳細については、「すべての Cisco Unified IP Phone のリセット」（P.3-10）を参照してください。

TFTP 証明書の再生成

TFTP 証明書を再生成するには、次の手順に従います。

（注） クラスタ内のすべての TFTP 証明書を再生成する場合、これらの手順は、すべての証明書を再生成した後に実行できます。

（注） TFTP および TVS の両方の証明書を再生成する場合は、常にこれらの手順を実行してから TVS 証明書を再生成します。この手順に従わないと、すべての Cisco Unified IP Phone から手動で ITL ファイルを削除することが必要になる場合があります。

	手順	追加情報
ステップ 1	TFTP 証明書を再生成します。	『*Cisco Unified Communications Operating System Administration Guide*』の第 6 章「Security」を参照してください。
ステップ 2	クラスタが混合モードの場合は、CTL クライアントを実行します。	第 4 章「Cisco CTL クライアントの設定」を参照してください。
ステップ 3	現在 Cisco TFTP サービスが稼動しているサーバで、このサービスを再起動します。	詳細については、「TFTP サーバでの Cisco TFTP サービスの再起動」（P.3-6）を参照してください。
ステップ 4	クラスタが混合モードの場合、次のサービスが起動されているときにはこれらのサービスを再起動します。 • Cisco CallManager • Cisco CTL Provider • Cisco CTL Manager	『*Cisco Unified Serviceability Administration Guide*』の第 11 章「Configuring Services」を参照してください。
ステップ 5	Cisco Unified IP Phone をリセットします。	詳細については、「すべての Cisco Unified IP Phone のリセット」（P.3-10）を参照してください。
ステップ 6	クラスタが EMCC 構成の一部の場合は、一括証明書プロビジョニングの手順を繰り返します。	『*Cisco Unified Communications Operating System Administration Guide*』の第 6 章「Security」を参照してください。

TFTP 証明書再生成後のシステムのバックアップ

ITL ファイルの信頼アンカーは、TFTP 秘密鍵というソフトウェア エンティティです。サーバがクラッシュすると鍵が失われ、電話機は新しい ITL ファイルを検証できなくなります。

Cisco Unified Communications Manager リリース 8.0 では、TFTP 証明書と秘密鍵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。秘密鍵を保護するために、バックアップ パッケージは暗号化されます。サーバがクラッシュすると、以前の証明書および鍵が復元されます。

TFTP 証明書が再生成された場合は、常に新しいシステム バックアップを作成する必要があります。バックアップの手順については、『*Disaster Recovery System Administration Guide*』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 8.0 へのアップグレード

クラスタをリリース 7.x からリリース 8.0 にアップグレードするには、次の手順に従います。

手順

ステップ 1　通常のクラスタ アップグレード手順に従います。詳細については、『*Cisco Unified Communications Operating System Administration Guide*』の第 7 章「Software Upgrades」を参照してください。

ヒント　クラスタ内のすべてのノードを Cisco Unified Communications Manager リリース 8.0 にアップグレードした後、ここに示す手順に従って Cisco Unified IP Phone をシステムに登録する必要があります。

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

Cisco Unified Communications Manager リリース 7.1(2)

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

Cisco Unified Communications Manager リリース 7.1(3)

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

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

TFTP サーバでの Cisco TFTP サービスの再起動

ステップ 3　Cisco Unified サービスアビリティで、[Tools] > [Control Center - Feature Services] の順に選択します。

[Control Center - Feature Services] ウィンドウが表示されます。

ステップ 4　Cisco Tftp サービスが稼動している各ノードで、このサービスを再起動します。

ステップ 5　TFTP がファイルを再作成するまで、5 分間待ちます。

すべての Cisco Unified IP Phone のリセット

（注）　電話機の設定を確実に最新の状態にするには、クラスタ内のすべての Cisco Unified IP Phone をリセットする必要があります。

ステップ 6　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウが表示されます。

ステップ 7　[リセット (Reset)] をクリックします。

ステップ 8　Cisco Unified IP Phone が Cisco Unified Communications Manager に登録されるまで、10 分間待ちます。

クラスタのバックアップ

注意　クラスタを回復できるようにするには、Disaster Recovery System（DRS; ディザスタ リカバリ システム）を使用してクラスタをバックアップしておく必要があります。

ステップ 9　DRS を使用してクラスタをバックアップする方法については、『*Disaster Recovery System Administration Guide*』を参照してください。

8.0 よりも前のリリースへのクラスタのロールバック

クラスタを 8.0 よりも前の Cisco Unified Communications Manager のリリースにロールバックする前に、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て、クラスタをロールバックするための準備を行う必要があります。

注意　クラスタをロールバックするための準備を行わずに 8.0 よりも前の Cisco Unified Communications Manager のリリースにダウングレードすると、デフォルトのセキュリティを使用している Cisco Unified IP Phone は、Cisco Unified Communications Manager への登録時に CTL、ITL、および署名付き設定ファイルを要求するループに入ります。この状態の Cisco Unified IP Phone は設定ファイルの変更を認識できないため、システム内の個々の Cisco Unified IP Phone で、手動で ITL ファイルを削除することが必要になる場合があります。

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

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウが表示されます。

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 8.0 よりも前の Cisco Unified Communications Manager のリリースにロールバックする準備を行っている場合に限り、このパラメータを有効にします。https を使用する電話機サービス（エクステンション モビリティなど）は、このパラメータが有効になっている間は動作しません。ただし、このパラメータが有効になっていても、基本的な電話コールの発信および受信は引き続き実行できます。

すべてのノードでの Cisco 信頼検証サービスの再起動

（注）　この手順で示されている順番に従って、サービスを再起動する必要があります。

ステップ 2　Cisco Unified サービスアビリティで、[Tools] > [Control Center - Network Services] の順に選択します。

[Control Center - Network Services] ウィンドウが表示されます。

ステップ 3　Cisco 信頼検証サービスを再起動するには、ウィンドウの下部にある [Restart] ボタンをクリックします。

ステップ 4　クラスタ内のすべてのノードで Cisco 信頼検証サービスを再起動します。

TFTP サーバでの Cisco TFTP サービスの再起動

ステップ 5　Cisco Unified サービスアビリティで、[Tools] > [Control Center - Feature Services] の順に選択します。

[Control Center - Feature Services] ウィンドウが表示されます。

ステップ 6　Cisco Tftp サービスが稼動している各ノードで、このサービスを再起動します。

ステップ 7　TFTP がファイルを再作成するまで、5 分間待ちます。

すべての Cisco Unified IP Phone のリセット

（注）　電話機の設定を確実に最新の状態にするには、クラスタ内のすべての Cisco Unified IP Phone をリセットする必要があります。

ステップ 8　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウが表示されます。

ステップ 9　[リセット (Reset)] をクリックします。

ステップ 10　Cisco Unified IP Phone が Cisco Unified Communications Manager に登録されるまで、10 分間待ちます。

以前のリリースへのクラスタの復元

ステップ 11　クラスタ内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、『*Cisco Unified Communications Operating System Administration Guide*』の第 7 章「Software Upgrades」を参照してください。

ステップ 12　クラスタが以前のバージョンに切り替わるまで待ちます。

ステップ 13　次のいずれかのリリースを混合モードで使用している場合、CTL クライアントを実行する必要があります。

Cisco Unified Communications Manager リリース 7.1(2)

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

Cisco Unified Communications Manager リリース 7.1(3)

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

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

TFTP サーバでの Cisco TFTP サービスの再起動

ステップ 14　Cisco Unified サービスアビリティで、[Tools] > [Control Center - Feature Services] の順に選択します。

[Control Center - Feature Services] ウィンドウが表示されます。

ステップ 15　Cisco Tftp サービスが稼動している各ノードで、このサービスを再起動します。

ステップ 16　TFTP がファイルを再作成するまで、5 分間待ちます。

すべての Cisco Unified IP Phone のリセット

ステップ 17　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウが表示されます。

ステップ 18　[リセット (Reset)] をクリックします。

ステップ 19　Cisco Unified IP Phone が Cisco Unified Communications Manager に登録されるまで、10 分間待ちます。

リリース 8.0 への切り替え

クラスタをリリース 7.x に戻した後でリリース 8.0 パーティションに切り替える場合は、この項の手順に従います。

手順

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

ステップ 2　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウが表示されます。

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

ステップ 3　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、CTL クライアントを実行する必要があります。

Cisco Unified Communications Manager リリース 7.1(2)

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

Cisco Unified Communications Manager リリース 7.1(3)

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

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

すべてのノードでの Cisco 信頼検証サービスの再起動

（注）　この手順で示されている順番に従って、サービスを再起動する必要があります。

ステップ 4　Cisco Unified サービスアビリティで、[Tools] > [Control Center - Network Services] の順に選択します。

[Control Center - Network Services] ウィンドウが表示されます。

ステップ 5　Cisco 信頼検証サービスを再起動するには、ウィンドウの下部にある [Restart] ボタンをクリックします。

ステップ 6　クラスタ内のすべてのノードで Cisco 信頼検証サービスを再起動します。

TFTP サーバでの Cisco TFTP サービスの再起動

ステップ 7　Cisco Unified サービスアビリティで、[Tools] > [Control Center - Feature Services] の順に選択します。

[Control Center - Feature Services] ウィンドウが表示されます。

ステップ 8　Cisco Tftp サービスが稼動している各ノードで、このサービスを再起動します。

ステップ 9　TFTP がファイルを再作成するまで、5 分間待ちます。

すべての Cisco Unified IP Phone のリセット

（注）　電話機の設定を確実に最新の状態にするには、クラスタ内のすべての Cisco Unified IP Phone をリセットする必要があります。

ステップ 10　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウが表示されます。

ステップ 11　[リセット (Reset)] をクリックします。

ステップ 12　Cisco Unified IP Phone が Cisco Unified Communications Manager に登録されるまで、10 分間待ちます。

CHAPTER 4

Cisco CTL クライアントの設定

この章は、次の内容で構成されています。

Cisco CTL クライアントの概要

デバイス認証、ファイル認証、およびシグナリング認証は、Certificate Trust List（CTL; 証明書信頼リスト）ファイルの作成に依存します。このファイルは、USB ポートのある単一の Windows ワークステーションまたはサーバに Cisco Certificate Trust List（CTL）クライアントをインストールおよび設定したときに作成されます。

（注）　Cisco CTL クライアント用としてサポートされている Windows のバージョンは、Windows 2000、Windows XP、および Windows Vista です。Terminal Services は、Cisco CTL クライアントのインストールに使用しないでください。シスコは、Cisco Technical Assistance Center（TAC）がリモートでトラブルシューティングおよび設定作業を行えるように Terminal Services をインストールしています。

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

- System Administrator Security Token（SAST）
- 同一のサーバで実行される Cisco CallManager サービスおよび Cisco TFTP サービス
- Certificate Authority Proxy Function（CAPF）
- TFTP サーバ（複数可）
- ASA ファイアウォール

CTL ファイルには、各サーバのサーバ証明書、公開鍵、シリアル番号、署名、発行者名、件名、サーバ機能、DNS 名、および IP アドレスが含まれます。

CTL ファイルを作成したら、Cisco CallManager サービスおよび Cisco TFTP サービスを実行するすべてのノードで、Cisco Unified サービスアビリティを使用してこれらのサービスを再起動する必要があります。次回、電話機を初期化するときには、CTL ファイルが TFTP サーバからダウンロードされます。CTL ファイルに自己署名証明書を持つ TFTP サーバ エントリが含まれている場合、電話機は .sgn 形式の署名付き設定ファイルを要求します。どの TFTP サーバにも証明書がない場合、電話機は署名なし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すると、CTL クライアントの GUI にこの証明書を表示できます。

ファイアウォールを CTL ファイルに設定すると、セキュアな Cisco 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。Cisco CTL クライアントは、ファイアウォール証明書を「CCM」証明書として表示します。

Cisco Unified Communications Manager の管理は、etoken を使用して、Cisco CTL クライアントと Cisco CTL Provider との間の TLS 接続を認証します。

CTL クライアント 5.0 プラグインのインストールに関する特記事項

CTL クライアント 5.0 または 5.2 プラグインにアップグレードする場合、最初に eToken Run Time Environment 3.00 を削除する必要があります。次の手順に従います。

手順

ステップ 1　次の URL から Windows Installer Cleanup ユーティリティをダウンロードします。

http://support.microsoft.com/kb/290301

ステップ 2　このユーティリティを PC にインストールします。

ステップ 3　ユーティリティを実行します。

ステップ 4　プログラムのリストから eToken rte3.0 を見つけて削除します。

ステップ 5　CTL クライアントのインストールに進みます。

インストールに関する Windows 2000 ユーザ向けの特記事項

Windows 2000 を実行するワークステーションまたはサーバを使用している場合、CTL クライアント プラグインを正しくインストールするために Windows Installer 3.0 アップデートをダウンロードする必要があります。Windows Installer 3.0 は次の URL で入手できます。

http://www.microsoft.com/downloads/details.aspx?familyid=5FBC5470-B259-4733-A914-A956122E08E8&displaylang=en

（注）　Windows 2000 には Windows Installer 2.0 が付属しています。

Windows Installer 3.0 には検証が必要です。手順に従って PC を検証してください。次に Windows Installer 3.0 をインストールし、必要に応じてマシンをリブートします。その後、CTL クライアントのインストールに進みます。

Cisco CTL クライアントの設定のヒント

Cisco Unified Communications Manager の管理ページで Cisco CTL クライアントを設定する場合は、次の点を考慮してください。

- 電話機はサイズの大きい CTL ファイルを受け入れることができないため、Cisco CTL クライアントは CTL ファイルのサイズを 32 KB に制限します。CTL ファイルのサイズに影響を与えるのは、次の要因です。
  - クラスタ内のノードの数

    ノードの数が多ければ、CTL ファイルにより多くの証明書が必要になります。
  - TLS プロキシで使用されているファイアウォールの数

    TLS プロキシ機能を備えたファイアウォールは、ノードと同じであるため、CTL ファイルに含まれます。
  - 外部の Certificate Authority（CA; 認証局）が CAPF 証明書および CallManager 証明書に署名しているかどうか

    外部の CA が署名した証明書（CAPF/CallManager）はデフォルトの自己署名証明書よりもかなり大きいため、CTL ファイルに含めることができる証明書の最大数が制限されることがあります。

これらの要因は、32 KB の CTL ファイルに含めることができる証明書の最大数を直接制限するため、セキュアな Cisco Unified Communications Manager 配備内に含めることができるノードまたはファイアウォールの最大数を示します。

- Cisco Unified Communications Manager ノードのホスト名が、Cisco CTL クライアントがインストールされているリモート PC で解決可能であることを確認します。解決可能でない場合、Cisco CTL クライアントは正しく動作しません。
- Cisco CTL Provider サービスをアクティブにする必要があります。クラスタ環境がある場合は、クラスタ内のすべてのサーバで Cisco CTL Provider サービスをアクティブにする必要があります。
- CTL ファイルを作成または更新したら、これらのサービスを実行するすべての Cisco Unified Communications Manager サーバおよびクラスタ内のすべての TFTP サーバで Cisco Unified サービスアビリティを使用して、Cisco CallManager サービスおよび Cisco TFTP サービスを再起動する必要があります。
- Cisco CTL クライアントに、代替 TFTP サーバまたは集中 TFTP サーバなどのクラスタ外サーバのエントリが含まれている場合、これらのサーバでも Cisco CTL Provider サービスを実行する必要があります。
- Cisco CTL クライアント GUI の代替 TFTP サーバのセクションで、別のクラスタに存在する Cisco TFTP サーバを指定します。[Alternate TFTP Server] タブの設定値を使用して、代替 TFTP サーバおよび集中 TFTP サーバを Cisco CTL クライアントに設定します。

（注） クラスタ外の（代替および集中）TFTP サーバの設定方法の詳細については、『*Cisco Unified Communications Manager システム ガイド*』の「Cisco TFTP」を参照してください。

- 集中 TFTP 設定では、混合モードで動作するすべてのクラスタ外 TFTP サーバで、マスター TFTP サーバまたはマスター TFTP サーバの IP アドレスをクラスタ外 CTL ファイルに追加する必要があります。マスター TFTP サーバで、マスター TFTP サーバ用に設定された代替ファイル リスト内のすべての代替 TFTP サーバの設定ファイルを処理します。集中 TFTP 設定のクラスタすべてで同じセキュリティ モードを使用する必要はありません。各クラスタで独自のモードを選択できます。

Cisco CTL クライアントの設定用チェックリスト

表 4-1 に、初めて Cisco CTL クライアントをインストールおよび設定する場合に実行する設定作業のリストを示します。Cisco Unified Communications Manager をアップグレードするときの CTL ファイル設定の詳細については、「Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行」（P.4-9）を参照してください。

表 4-1　Cisco CTL クライアントの設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	クラスタ内のすべてのサーバがオンラインになっており、CTL クライアントが実行されている PC からアクセスできることを確認します。サーバがホスト名を使用して設定されている場合は、ホスト名を ping して到達可能性を確認します。	
ステップ 2	クラスタ サーバのすべてのホスト名が、パブリッシャ サーバに設定されている DNS サーバで定義されていることを確認します。	

表 4-1　Cisco CTL クライアントの設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 3	Cisco Unified サービスアビリティで Cisco CTL Provider サービスをアクティブにします。 クラスタ内の各 Cisco Unified Communications Manager サーバで Cisco CTL Provider サービスをアクティブにします。 **ヒント** Cisco Unified Communications Manager のアップグレード前にこのサービスをアクティブにした場合は、サービスを再度アクティブにする必要はありません。アップグレード後にサービスは自動的にアクティブになります。	「Cisco CTL Provider サービスのアクティブ化」（P.4-5）
ステップ 4	Cisco Unified サービスアビリティで Cisco Certificate Authority Proxy サービスをアクティブにします。 **ヒント** クラスタ内の最初のノードでのみ Cisco Certificate Authority Proxy サービスをアクティブにします。 **ワンポイントアドバイス** Cisco CTL クライアントをインストールして設定する前にこの作業を実行すれば、CAPF を使用するために CTL ファイルを更新する必要がなくなります。	「Certificate Authority Proxy Function サービスのアクティブ化」（P.10-6）
ステップ 5	デフォル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** これらの設定を Cisco Unified Communications Manager のアップグレード前に設定した場合、設定は自動的に移行されます。	「TLS 接続用ポートの設定」（P.4-6）
ステップ 6	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。	「Cisco CTL クライアントの設定」（P.4-10）
ステップ 7	Cisco CTL クライアントをインストールします。	• 「システム要件」（P.1-5） • 「インストール」（P.1-14） • 「Cisco CTL クライアントのインストール」（P.4-8）
ステップ 8	Cisco CTL クライアントを設定します。	「Cisco CTL クライアントの設定」（P.4-10）

Cisco CTL Provider サービスのアクティブ化

Cisco CTL クライアントの設定後、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。その後、このサービスによって、CTL ファイルがすべての Cisco Unified Communications Manager および Cisco TFTP サーバに転送されます。

サービスをアクティブにしてから Cisco Unified Communications Manager をアップグレードした場合、Cisco Unified Communications Manager によってサービスはアップグレード後に自動的に再度アクティブになります。

ヒント　クラスタ内のすべてのサーバで Cisco CTL Provider サービスをアクティブにする必要があります。

サービスをアクティブにするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified サービスアビリティで、[Tools] > [Service Activation] の順に選択します。

ステップ 2　[Server] ドロップダウン リスト ボックスで、Cisco CallManager サービスまたは Cisco TFTP サービスをアクティブにしたサーバを選択します。

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

ステップ 4　[Save] をクリックします。

ヒント　クラスタ内のすべてのサーバで、この手順を実行します。

（注）　Cisco CTL Provider サービスを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 接続用ポートの設定」（P.4-6）を参照してください。

ステップ 5　サービスがサーバで実行されていることを確認します。サービスの状態を確認するには、Cisco Unified サービスアビリティで [Tools] > [Control Center–Feature Services] の順に選択します。

追加情報

「関連項目」（P.4-21）を参照してください。

Cisco CAPF サービスのアクティブ化

このサービスのアクティブ化については、「Certificate Authority Proxy Function サービスのアクティブ化」（P.10-6）を参照してください。

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

TLS 接続用ポートの設定

デフォルトのポートが現在使用中の場合や、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は、異なる TLS ポート番号の設定が必要になることもあります。

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

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

- Ethernet Phone ポートは、SCCP を実行する電話機からの登録要求を監視します。非セキュア モードの場合、電話機はポート 2000 を介して接続されます。混合モードの場合、Cisco Unified Communications Manager の TLS 接続用ポートは Cisco Unified Communications Manager ポート番号に 443 を加算（+）した番号になるため、Cisco Unified Communications Manager のデフォルトの TLS 接続は 2443 になります。ポート番号が現在使用中の場合や、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、この設定を更新します。
- SIP セキュア ポートを使用すると、Cisco Unified Communications Manager は、SIP を実行する電話機からの SIP メッセージを傍受できます。デフォルト値は 5061 です。このポートを変更した場合は、Cisco Unified サービスアビリティで Cisco CallManager サービスを再起動し、SIP を実行す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は、Cisco Unified サービスアビリティで Cisco CTL Provider サービスを再起動する必要があります。

CTL ポートは、CTL クライアントが実行されているデータ VLAN に対して開いている必要があります。Cisco Unified Communications Manager にシグナルを戻すために TLS を実行している電話機も CTL クライアントが使用するポートを使用します。これらのポートは、電話機が認証済みステータスまたは暗号化済みステータスに設定されているすべての VLAN に対して必ず開いてください。

デフォルト設定を変更するには、次の手順を実行します。

手順

ステップ 1　変更するポートに応じて、次の作業を実行します。

- Cisco CTL Provider サービスの Port Number パラメータを変更するには、ステップ 2 ～ステップ 6 を実行します。
- [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、ステップ 7 ～ステップ 11 を実行します。

ステップ 2　Cisco CTL Provider ポートを変更するには、Cisco Unified Communications Manager の管理ページで [システム(System)] > [サービスパラメータ(Service Parameters)] の順に選択します。

ステップ 3　[サーバ(Server)] ドロップダウン リスト ボックスで、Cisco CTL Provider サービスを実行しているサーバを選択します。

ステップ 4　[サービス(Service)] ドロップダウン リスト ボックスで、**Cisco CTL Provider** サービスを選択します。

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

ステップ 5　Port Number パラメータの値を変更するには、[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。

ステップ 6　[保存(Save)] をクリックします。

ステップ 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、Cisco Unified Communications Manager の管理ページで [システム(System)] > [Cisco Unified CM] の順に選択します。

ステップ 8　『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の説明に従い、Cisco CallManager サービスを実行しているサーバを検索します。結果が表示されたら、サーバの [名前(Name)] リンクをクリックします。

ステップ 9　[Cisco Unified Communications Manager の設定(Cisco Unified CM Configuration)] ウィンドウが表示されたら、[イーサネット電話ポート(Ethernet Phone Port)] フィールドまたは [SIP 電話セキュアポート(SIP Phone Secure Port)] フィールドに新しいポート番号を入力します。

ステップ 10　電話機をリセットし、Cisco Unified サービスアビリティで Cisco CallManager サービスを再起動します。

ステップ 11　[保存(Save)] をクリックします。

追加情報

「関連項目」（P.4-21）を参照してください。

Cisco CTL クライアントのインストール

次のイベントが発生するときには、クライアントを使用して CTL ファイルを更新する必要があります。

- クラスタ セキュリティ モードの最初の設定時
- CTL ファイルの最初の作成時
- Cisco Unified Communications Manager のインストール後
- Cisco Unified Communications Manager サーバまたは Cisco Unified Communications Manager データの復元後
- Cisco Unified Communications Manager サーバの IP アドレスまたはホスト名の変更後
- セキュリティ トークンの追加後または削除後
- ASA ファイアウォールの追加後または削除後
- TFTP サーバの追加後または削除後
- Cisco Unified Communications Manager サーバの追加後または削除後
- サードパーティの CA 署名証明書をプラットフォームにアップロードした後

ヒント　クライアントをインストールしようとしているサーバまたはワークステーションで、Smart Card サービスが「開始」および「自動」に設定されていない場合、インストールは失敗します。

Cisco CTL クライアントをインストールするには、次の手順を実行します。

手順

ステップ 1　『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の説明に従い、クライアントをインストールしようとする Windows ワークステーションまたはサーバから Cisco Unified Communications Manager の管理ページに移動します。

ステップ 2　Cisco Unified Communications Manager の管理ページで、[アプリケーション(Application)] > [プラグイン(Plugins)] の順に選択します。

[プラグインの検索と一覧表示 (Find and List Plugins)] ウィンドウが表示されます。

ステップ 3　[かつプラグインタイプが次に等しい(and Plugin Type equals)] ドロップダウン リスト ボックスから [インストール(Installation)] を選択し、[検索(Find)] をクリックします。

ステップ 4　[Cisco CTL Client] を見つけます。

ステップ 5　ファイルをダウンロードするには、ウィンドウの左側の、Cisco CTL クライアント プラグイン名のちょうど反対側にある [ダウンロード(Download)] をクリックします。

ステップ 6　[保存] をクリックして、ファイルを任意の場所に保存します。

ステップ 7　インストールを開始するには、[Cisco CTL Client]（ファイルを保存した場所によってアイコンまたは実行ファイルになります）をダブルクリックします。

（注）　[ダウンロードの完了] ボックスで [ファイルを開く] をクリックすることもできます。

ステップ 8　Cisco CTL クライアントのバージョンが表示されるので、[Next] をクリックします。

ステップ 9　インストール ウィザードが表示されます。[Next] をクリックします。

ステップ 10　使用許諾契約に同意して [Next] をクリックします。

ステップ 11　クライアントをインストールするフォルダを選択します。必要な場合は、[Browse] をクリックしてデフォルトの場所を変更することができます。場所を選択したら、[Next] をクリックします。

ステップ 12　インストールを開始するには、[Next] をクリックします。

ステップ 13　インストールが完了したら、[Finish] をクリックします。

追加情報

「関連項目」（P.4-21）を参照してください。

Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行

Cisco Unified Communications Manager リリース 5.x から 6.x にアップグレードした後で CTL ファイルを変更するには、アップグレード前にインストールしていた Cisco CTL クライアントをアンインストールし、最新の Cisco CTL クライアントをインストールし（「Cisco CTL クライアントのインストール」（P.4-8）を参照）、CTL ファイルを再生成する必要があります。アップグレード前にサーバの削除や追加を実行しなかった場合は、アップグレード後に Cisco CTL クライアントを再設定する必要はありません。Cisco Unified Communications Manager のアップグレードにより、CTL ファイル内のデータは自動的に移行されます。

Cisco Unified Communications Manager 4.x からリリース 6.x にアップグレードし、セキュリティがクラスタ上で有効になっている場合は、アップグレード前にインストールしていた Cisco CTL クライアントをアンインストールし、最新の Cisco CTL クライアントをインストールして CTL ファイルを再生成する必要があります。アップグレードされたクラスタのセキュリティを有効にするには、次の手順に従います。

手順

ステップ 1　既存の Cisco CTL クライアントをアンインストールします。

ステップ 2　新しい Cisco CTL クライアントをインストールします（「Cisco CTL クライアントのインストール」（P.4-8）を参照）。

ステップ 3　以前に使用した USB キーのうち少なくとも 1 つを使用して Cisco CTL クライアントを実行します（「Cisco CTL クライアントの設定」（P.4-10）を参照）。

ステップ 4　これらのサービスを実行するすべての Cisco Unified Communications Manager サーバおよびクラスタ内のすべての TFTP サーバで Cisco Unified サービスアビリティを使用して、Cisco CallManager サービスおよび Cisco TFTP サービスを再起動する必要があります。

追加情報

「関連項目」（P.4-21）を参照してください。

Cisco CTL クライアントの設定

ヒント　Cisco CTL クライアントは、スケジューリングされたメンテナンス期間中に設定します。これは、クラスタ内で Cisco CallManager サービスおよび Cisco TFTP サービスを実行するすべてのサーバでこれらのサービスを再起動する必要があるためです。

Cisco CTL クライアントは、次のタスクを実行します。

- Cisco Unified Communications Manager クラスタのセキュリティ モードを設定します。

（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。

ヒント　Cisco Unified Communications Manager の管理ページの [エンタープライズパラメータ設定（Enterprise Parameters Configuration）] ウィンドウで Cisco Unified Communications Manager クラスタのセキュリティ パラメータを混合モードに設定することはできません。クラスタ セキュリティ モードを設定するには、Cisco CTL クライアントを設定する必要があります。詳細については、「Cisco CTL クライアントの設定内容」（P.4-15）を参照してください。

- Certificate Trust List（CTL; 証明書信頼リスト）を作成します。これは、セキュリティ トークン、Cisco 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 Cisco Unified Communications Manager、Cisco CAPF、および ASA ファイアウォールを検出して、これらのサーバの証明書エントリを追加します。

  設定時に挿入したセキュリティ トークンによって CTL ファイルが署名されます。

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

始める前に

ヒント　Cisco Unified Communications Manager をアップグレードするときの CTL ファイル設定の詳細については、「Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行」（P.4-9）を参照してください。

Cisco CTL クライアントを設定する前に、Cisco CTL Provider サービスおよび Cisco Certificate Authority Proxy Function サービスを Cisco Unified サービスアビリティでアクティブにしたことを確認します。少なくとも 2 つのセキュリティ トークンを入手します。これらのセキュリティ トークンは、シスコの認証局が発行します。シスコから取得したセキュリティ トークンを使用する必要があります。トークンを一度に 1 つずつサーバまたはワークステーションの USB ポートに挿入します。サーバに USB ポートがない場合、USB PCI カードを使用することができます。

次のパスワード、ホスト名または IP アドレス、ポート番号を取得します。

- Cisco Unified Communications Manager の管理ユーザ名とパスワード

ヒント　管理ユーザ名は、エンドユーザではなく、アプリケーション ユーザである必要があり、また、スーパーユーザ権限を持つスーパーユーザ グループのメンバーでなければなりません。

- セキュリティ トークンの管理者パスワード
- ASA ファイアウォールの管理ユーザ名とパスワード

これらの説明については、表 4-2（P.4-16）を参照してください。

ヒント　Cisco CTL クライアントをインストールする前に、サーバへのネットワーク接続を確認します。ネットワーク接続が確立されていることを確認するには、『*Cisco Unified Communications Operating System Administration Guide*』の説明に従って ping コマンドを実行します。クラスタ環境では、クラスタ内のすべてのサーバにネットワーク接続できることを確認してください。

複数の Cisco CTL クライアントをインストールした場合、Cisco Unified Communications Manager では一度に 1 台のクライアントの CTL 設定情報しか受け入れません。ただし、設定作業は同時に 5 台までの Cisco CTL クライアントで実行できます。あるクライアントで設定作業を実行している間、その他のクライアントで入力した情報は Cisco Unified Communications Manager によって自動的に保存されます。

Cisco CTL クライアントの設定が完了すると、CTL クライアントは次のタスクを実行します。

- CTL ファイルを Cisco 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 Cisco 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 Cisco Unified Communications Manager 後続ノード（最初のノード以外）に書き込みます。
- すべての設定済み TFTP サーバにこのファイルを書き込みます。
- すべての設定済み ASA ファイアウォールにこのファイルを書き込みます。

- CTL ファイルを作成した時点で USB ポートに存在するセキュリティ トークンの秘密鍵を使用して、CTL ファイルに署名します。

クライアントを設定するには、次の手順を実行します。

手順

ステップ 1　購入したセキュリティ トークンを少なくとも 2 つ入手します。

ステップ 2　次の作業のいずれかを実行します。

- インストールしたワークステーションまたはサーバのデスクトップにある [Cisco CTL Client] アイコンをダブルクリックします。
- [スタート] > [プログラム] > [Cisco CTL Client] の順に選択します。

ステップ 3　表 4-2 の説明に従って Cisco Unified Communications Manager サーバの設定内容を入力し、[Next] をクリックします。

ステップ 4　表 4-2 の説明に従って、[Set Cisco Unified Communications Manager Cluster to Mixed Mode] をクリックし、[Next] をクリックします。

ステップ 5　設定する内容に応じて、次の作業を実行します。

- セキュリティ トークンを追加するには、ステップ 6 ～ステップ 12 を参照します。
- Cisco CTL クライアント設定を完了するには、ステップ 17 ～ステップ 21 を参照します。

注意　クライアントを初めて設定する場合、少なくとも 2 つのセキュリティ トークンが必要です。アプリケーションが要求しない限り、トークンを挿入しないでください。ワークステーションまたはサーバに USB ポートが 2 つある場合は、2 つのセキュリティ トークンを同時に挿入しないでください。

ステップ 6　アプリケーションが要求したら、現在 Cisco CTL クライアントを設定しているワークステーションまたはサーバで使用可能な USB ポートにセキュリティ トークンを 1 つ挿入して、[OK] をクリックします。

ステップ 7　挿入したセキュリティ トークンについての情報が表示されます。[Add] をクリックします。

ステップ 8　検出された証明書エントリがペインに表示されます。

ステップ 9　他のセキュリティ トークン（複数も可能）を証明書信頼リストに追加するには、[Add Tokens] をクリックします。

ステップ 10　サーバまたはワークステーションに挿入したトークンを取り外していない場合は、取り外します。アプリケーションが要求したら、次のトークンを挿入して [OK] をクリックします。

ステップ 11　2 番目のセキュリティ トークンについての情報が表示されます。[Add] をクリックします。

ステップ 12　すべてのセキュリティ トークンについて、ステップ 9 ～ステップ 11 を繰り返します。

ステップ 13　証明書エントリがペインに表示されます。

ステップ 14　表 4-2（P.4-16）の説明に従って、設定内容を入力します。

ステップ 15　[Next] をクリックします。

ステップ 16　表 4-2 の説明に従って設定内容を入力し、[Next] をクリックします。

ステップ 17　すべてのセキュリティ トークンおよびサーバを追加したら、[Finish] をクリックします。

ステップ 18　表 4-2 の説明に従ってセキュリティ トークンのユーザ パスワードを入力し、[OK] をクリックします。

ステップ 19　クライアントによって CTL ファイルが作成されると、各サーバのウィンドウに、サーバ、ファイル ロケーション、および CTL ファイルのステータスが表示されます。[Finish] をクリックします。

ステップ 20　スタンドアロン サーバまたはクラスタのすべてのデバイスをリセットします。詳細については、「デバイスのリセット、サービスの再起動またはリブート」（P.1-12）を参照してください。

ステップ 21　Cisco Unified サービスアビリティで、Cisco CallManager サービスおよび Cisco TFTP サービスを再起動します。

ヒント　これらのサービスを実行するすべての Cisco Unified Communications Manager サーバとクラスタ内のすべての TFTP サーバで、これらのサービスを再起動します。

ステップ 22　CTL ファイルを作成したら、USB ポートからセキュリティ トークンを取り外します。すべてのセキュリティ トークンを安全な場所に格納します。

追加情報

「関連項目」（P.4-21）を参照してください。

CTL ファイルの更新

次の場合に、CTL ファイルを更新する必要があります。

- 新しい Cisco Unified Communications Manager サーバをクラスタに追加した場合

（注）　ノードをセキュア クラスタに追加する手順については、『*Installing Cisco Unified Communications Manager Release 6.1(1)*』を参照してください。このマニュアルには、ノードを追加する方法、および新しいノードにセキュリティを設定する方法が記載されています。

- Cisco Unified Communications Manager サーバの名前または IP アドレスを変更した場合
- いずれかの設定済み TFTP サーバの IP アドレスまたはホスト名を変更した場合
- いずれかの設定済み 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した場合
- Cisco Unified サービスアビリティで 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
- Cisco Unified Communications Manager サーバを追加または削除する必要がある場合
- ASA ファイアウォールを追加または削除する必要がある場合
- Cisco Unified Communications Manager サーバまたは Cisco Unified Communications Manager データを復元した場合
- サードパーティの CA 署名証明書をプラットフォームにアップロードした後

ヒント　ファイルの更新は、コール処理がほとんど中断されないときに実行することを強く推奨します。

CTL ファイルにある情報を更新するには、次の手順を実行します。

手順

ステップ 1　最新の CTL ファイルを設定するために挿入したセキュリティ トークンを 1 つ入手します。

ステップ 2　インストールしたワークステーションまたはサーバのデスクトップにある [Cisco CTL Client] アイコンをダブルクリックします。

ステップ 3　表 4-2 の説明に従って Cisco Unified Communications Manager サーバの設定内容を入力し、[Next] をクリックします。

ヒント　このウィンドウでは、Cisco Unified Communications Manager サーバについて更新します。

ステップ 4　CTL ファイルを更新するには、表 4-2 の説明にあるように [Update CTL File] をクリックし、[Next] をクリックします。

注意　すべての CTL ファイルを更新するには、すでに CTL ファイルに存在するセキュリティ トークンを（1 つ）USB ポートに挿入する必要があります。クライアントでは、このトークンを使用して CTL ファイルの署名を検証します。Cisco CTL クライアントによって署名が検証されるまで、新しいトークンは追加できません。ワークステーションまたはサーバに USB ポートが 2 つある場合は、両方のセキュリティ トークンを同時に挿入しないでください。

ステップ 5　現在 CTL ファイルを更新しているワークステーションまたはサーバで使用可能な USB ポートにまだセキュリティ トークンを挿入していない場合は、いずれかのセキュリティ トークンを挿入してから [OK] をクリックします。

ステップ 6　挿入したセキュリティ トークンについての情報が表示されます。[Next] をクリックします。

検出された証明書エントリがペインに表示されます。

ヒント　このペインでは、Cisco Unified Communications Manager、Cisco TFTP、または ASA ファイアウォールのエントリを更新できません。Cisco Unified Communications Manager エントリを更新するには、[Cancel] をクリックし、ステップ 2 ～ステップ 6 をもう一度実行します。

ステップ 7　既存の Cisco CTL エントリを更新するか、あるいはセキュリティ トークンを追加または削除する際は、次の点を考慮してください。

- サーバ設定の更新手順または新しいセキュリティ トークンの追加手順については、「Cisco CTL クライアントの設定」（P.4-10）を参照してください。
- セキュリティ トークンを削除するには、「CTL ファイル エントリの削除」（P.4-15）を参照してください。

ステップ 8　CTL ファイルの更新が終了したら、Cisco Unified サービスアビリティで、Cisco CallManager サービスおよび Cisco TFTP サービスを再起動します。

ヒント　これらのサービスを実行するすべてのクラスタ内のすべてのノードで TFTP サービスおよび Cisco CallManager サービスを再起動してください。

追加情報

「関連項目」（P.4-21）を参照してください。

CTL ファイル エントリの削除

Cisco CTL クライアントの [CTL Entries] ウィンドウに表示される一部の CTL エントリは、いつでも削除することができます。クライアントを開いて、[CTL Entries] ウィンドウを表示するプロンプトに従い、削除する項目を強調表示してから **[Delete Selected]** をクリックしてエントリを削除します。

Cisco Unified Communications Manager、Cisco TFTP、ASA ファイアウォール、または Cisco CAPF を実行するサーバを、CTL ファイルから削除することはできません。

CTL ファイルには常に 2 つのセキュリティ トークン エントリが存在している必要があります。ファイルからセキュリティ トークンをすべて削除することはできません。

追加情報

「関連項目」（P.4-21）を参照してください。

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

クラスタのセキュリティ モードを設定するには、Cisco CTL クライアントを使用する必要があります。Cisco Unified Communications Manager セキュリティ モードは、Cisco Unified Communications Manager の管理ページの [エンタープライズパラメータ設定(Enterprise Parameters Configuration)] ウィンドウで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。

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。[Cluster Security Mode] ウィンドウに移動して、モードの設定を変更し、[Next]、[Finish] の順にクリックします（「CTL ファイルの更新」（P.4-13）および表 4-2 を参照）。

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 モードに変更した場合、CTL ファイルはサーバに存在したままですが、CTL ファイルに証明書は含まれません。CTL ファイルに証明書が存在しないため、電話機は署名なし設定ファイルを要求し、非セキュアとして Cisco Unified Communications Manager に登録されます。

Cisco CTL クライアントの設定内容

クラスタのセキュリティ モードは、表 4-2 の説明にあるように、非セキュア モードまたは混合モードのいずれかに設定できます。混合モードだけが認証、シグナリング暗号化、およびメディア暗号化をサポートしています。

（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。

表 4-2 を使用して、初めての Cisco CTL クライアント設定、CTL ファイルの更新、または混合モードから非セキュア モードへの変更を行うことができます。

- 設定のヒントについては、「Cisco CTL クライアントの設定のヒント」（P.4-3）を参照してください。
- 関連する情報および手順については、「関連項目」（P.4-21）を参照してください。

表 4-2　CTL クライアントの設定内容

設定	説明
[Cisco Unified Communications Manager Server]	
[Hostname or IP Address]	最初のノードのホスト名または IP アドレスを入力します。
[Port]	この Cisco Unified Communications Manager サーバで実行されている Cisco CTL Provider サービスの CTL ポート番号を入力します。デフォルトのポート番号は 2444 です。
[Username and Password]	最初のノードでスーパーユーザの管理者権限を持つアプリケーションユーザのユーザ名とパスワードと同じものを入力します。
[Security Mode]	
[Set Cisco Unified Communications Manager Cluster to Mixed Mode]	混合モードでは、認証済みで暗号化済み、および非セキュアの Cisco Unified IP Phone を Cisco Unified Communications Manager に登録することができます。このモードでは、認証済みまたは暗号化済みのデバイスでセキュア ポートが使用されることを Cisco Unified Communications Manager が保証します。 **（注）** 混合モードに設定すると、Cisco Unified Communications Manager によって自動登録は無効になります。
[Set Cisco Unified Communications Manager Cluster to Non-Secure Mode]	非セキュア モードに設定すると、すべてのデバイスは非認証として登録され、Cisco Unified Communications Manager はイメージ認証のみサポートします。 このモードを選択すると、Cisco CTL クライアントは CTL ファイルにあるすべてのエントリの証明書を削除しますが、CTL ファイルは引き続き指定したディレクトリに存在します。電話機は署名なし設定ファイルを要求し、非セキュアとして Cisco Unified Communications Manager に登録されます。 **ヒント** 電話機をデフォルトの非セキュア モードに戻すには、電話機およびすべての Cisco 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。 このモードでは自動登録を使用できます。
[Update CTL File]	CTL ファイルの作成後にこのファイルを変更するには、このオプションを選択する必要があります。このオプションを選択すると、Cisco Unified Communications Manager のセキュリティ モードは変更されません。
[CTL Entries]	
[Add Tokens]	証明書信頼リスト（CTL）にセキュリティ トークンを追加するには、このボタンをクリックします。 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取り外していない場合は、取り外します。アプリケーションが要求したら、次のトークンを挿入して [OK] をクリックします。追加したセキュリティ トークンについての情報が表示されたら、[Add] をクリックします。すべてのセキュリティ トークンについて、これらの作業を繰り返します。
[Add TFTP Server]	CTL に代替 TFTP サーバを追加するには、このボタンをクリックします。設定の詳細については、[Alternate TFTP Server] タブの設定値が表示された後で [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。

表 4-2　CTL クライアントの設定内容（続き）

設定	説明
[Add Firewall]	CTL 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] タブの設定値が表示された後で [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。
[Alternate TFTP Server]	
[Hostname or IP Address]	TFTP サーバのホスト名または IP アドレスを入力します。 代替 TFTP サーバには、別のクラスタに存在する Cisco TFTP サーバを指定します。代替 TFTP サーバの設定に 2 つの異なるクラスタを使用する場合は、両クラスタが使用するクラスタ セキュリティ モードが同じであることが必要です。これは、Cisco CTL クライアントを両方のクラスタにインストールして設定する必要があることを意味します。さらに、同じバージョンの Cisco Unified Communications Manager が両方のクラスタで動作している必要があります。 TFTP サービス パラメータ FileLocation 内のパスが、クラスタ内のすべてのサーバで同じであることを確認してください。 詳細については、「Cisco CTL クライアントの設定のヒント」（P.4-3）を参照してください。
[Port]	今回のリリースの Cisco Unified Communications Manager では不要です。
[Username and Password]	今回のリリースの Cisco Unified Communications Manager では不要です。
[Firewall]	
[Hostname or IP Address]	ファイアウォールのホスト名または IP アドレスを入力します。
[Port]	設定できません。デフォルトのポートである 2444 番の Cisco Unified Communications Manager ポートを使用します。
[Username and Password]	設定できません。Cisco Unified Communications Manager のインストール時に設定した管理者名とパスワードがシステムによって使用されます。
[Security Token]	
[User Password]	Cisco CTL クライアントを初めて設定するときは、デフォルト パスワードの **Cisco123** を大文字と小文字を区別して入力し、証明書の秘密鍵を取得して CTL ファイルが署名済みであることを確認します。

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

クラスタのセキュリティ 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。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで [システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

ステップ 2　[Cluster Security Mode] フィールドを見つけます。フィールド内の値が **1** と表示される場合、Cisco Unified Communications Manager は混合モードに正しく設定されています（詳細については、フィールド名をクリックしてください）。

ヒント　この値は Cisco Unified Communications Manager の管理ページで設定することができません。この値が表示されるのは、Cisco CTL クライアントの設定後です。

追加情報

「関連項目」（P.4-21）を参照してください。

Smart Card サービスの開始および自動の設定

Cisco CTL クライアント インストールにより、Smart Card サービスが無効であると検出された場合は、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、Smart Card サービスを「自動」および「開始」に設定する必要があります。

ヒント　サービスが「開始」および「自動」に設定されていない場合は、セキュリティ トークンを CTL ファイルに追加できません。

オペレーティング システムのアップグレード、サービス リリースの適用、Cisco Unified Communications Manager のアップグレードなどを行ったら、Smart Card サービスが「開始」および「自動」になってい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

ステップ 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] の順に選択します。

ステップ 2　[サービス] ウィンドウで、**Smart Card** サービスを右クリックし、[プロパティ] を選択します。

ステップ 3　[プロパティ] ウィンドウに [全般] タブが表示されていることを確認します。

ステップ 4　[スタートアップの種類] ドロップダウン リスト ボックスから、[自動] を選択します。

ステップ 5　[適用] をクリックします。

ステップ 6　[サービスの状態] 領域で、[開始] をクリックします。

ステップ 7　[OK] をクリックします。

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

追加情報

「関連項目」（P.4-21）を参照してください。

セキュリティ トークン パスワード（etoken）の変更

この管理パスワードは、証明書の秘密鍵を取得し、CTL ファイルが署名されることを保証します。各セキュリティ トークンには、デフォルト パスワードが付属しています。セキュリティ トークン パスワードはいつでも変更できます。Cisco CTL クライアントによりパスワードの変更を求めるプロンプトが表示されたら、設定を続行する前にパスワードを変更する必要があります。

パスワード設定の関連情報を検討するには、[Show Tips] ボタンをクリックします。何らかの理由でパスワードを設定できない場合は、表示されるヒントを検討してください。

セキュリティ トークン パスワードを変更するには、次の手順を実行します。

手順

ステップ 1　Cisco CTL クライアントを Windows サーバまたはワークステーションにインストールしたことを確認します。

ステップ 2　Cisco CTL クライアントをインストールした Windows サーバまたはワークステーションの USB ポートにセキュリティ トークンが挿入されていなければ挿入します。

ステップ 3　[スタート] > [プログラム] > [etoken] > [Etoken Properties] の順に選択します。次に、[etoken] を右クリックし、[Change etoken password] を選択します。

ステップ 4　[Current Password] フィールドに、最初に作成したトークン パスワードを入力します。

ステップ 5　新しいパスワードを入力します。

ステップ 6　確認のため、新しいパスワードを再入力します。

ステップ 7　[OK] をクリックします。

追加情報

「関連項目」（P.4-21）を参照してください。

Cisco Unified IP Phone 上の CTL ファイルの削除

注意　セキュアな実験環境でこの作業を実行することをお勧めします。特に、Cisco Unified Communications Manager サーバから CTL ファイルを削除する予定がない場合にお勧めします。

次の状況が発生した場合は、Cisco Unified IP Phone 上の CTL ファイルを削除してください。

- CTL ファイルに署名したセキュリティ トークンをすべて紛失した。
- CTL ファイルに署名したセキュリティ トークンが漏洩した。
- 電話機をセキュア環境からストレージ領域などに移動する。
- 電話機を、非セキュア クラスタ、または異なるドメインの別のセキュア クラスタへと移動する。
- 電話機を、未知のセキュリティ ポリシーを持つ領域からセキュアな Cisco Unified Communications Manager へと移動する。
- 代替 TFTP サーバ アドレスを、CTL ファイル内に存在しないサーバへと変更する。

Cisco Unified IP Phone 上の CTL ファイルを削除するには、表 4-3 の作業を実行します。

表 4-3　Cisco Unified IP Phone 上の CTL ファイルの削除

Cisco Unified IP Phone モデル	作業
Cisco Unified IP Phone 7960G および 7940G	IP Phone 上の [セキュリティ設定] メニューで、[CTL ファイル]、[解除] または **# を押して、[削除] を押します。
Cisco Unified IP Phone 7970G および同等モデル	次の方法のどちらかを実行します。 • [セキュリティ設定] メニューのロックを解除します（『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』を参照）。CTL オプションの下にある [削除] ソフトキーを押します。 • [設定] メニューにある [削除] ソフトキーを押します。 （注）　[設定] メニューにある [削除] ソフトキーを押すと、CTL ファイル以外の情報も削除されます。詳細については、『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』を参照してください。

追加情報

「関連項目」（P.4-21）を参照してください。

Cisco CTL クライアントのバージョンの特定

使用している Cisco CTL クライアントのバージョンを特定するには、次の手順を実行します。

手順

ステップ 1　次の作業のいずれかを実行します。

- デスクトップ上の [Cisco CTL Client] アイコンをダブルクリックします。
- [スタート] > [プログラム] > [Cisco CTL Client] の順に選択します。

ステップ 2　Cisco CTL クライアント ウィンドウの左上隅にあるアイコンをクリックします。

ステップ 3　[About Cisco CTL Client] を選択します。クライアントのバージョンが表示されます。

追加情報

「関連項目」（P.4-21）を参照してください。

Cisco CTL クライアントの確認とアンインストール

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。必要であれば、Cisco CTL クライアントをアンインストールし、クライアントを別の Windows ワークステーションまたはサーバにインストールして、同じ CTL ファイルを引き続き使用することができます。

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

手順

ステップ 1　[スタート] > [コントロール パネル] の順に選択します。

ステップ 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 Client] を見つけます。

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

追加情報

「関連項目」（P.4-21）を参照してください。

参考情報

関連項目

- 「システム要件」（P.1-5）
- 「Cisco CTL クライアントの概要」（P.4-2）
- 「Cisco CTL クライアントの設定用チェックリスト」（P.4-4）
- 「Cisco CTL Provider サービスのアクティブ化」（P.4-5）
- 「Cisco CAPF サービスのアクティブ化」（P.4-6）
- 「TLS 接続用ポートの設定」（P.4-6）
- 「Cisco CTL クライアントのインストール」（P.4-8）
- 「Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行」（P.4-9）
- 「Cisco CTL クライアントの設定」（P.4-10）
- 「CTL ファイルの更新」（P.4-13）
- 「CTL ファイル エントリの削除」（P.4-15）
- 「Cisco Unified Communications Manager セキュリティ モードの更新」（P.4-15）
- 「Cisco CTL クライアントの設定内容」（P.4-15）
- 「Cisco Unified Communications Manager のセキュリティ モードの確認」（P.4-17）
- 「Smart Card サービスの開始および自動の設定」（P.4-18）
- 「Cisco Unified IP Phone 上の CTL ファイルの削除」（P.4-19）
- 「Cisco CTL クライアントのバージョンの特定」（P.4-20）
- 「Cisco CTL クライアントの確認とアンインストール」（P.4-20）
- 「Certificate Authority Proxy Function の使用方法」（P.10-1）

シスコの関連マニュアル

『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』

『*Troubleshooting Guide for Cisco Unified Communications Manager*』

CHAPTER 5

証明書の設定

この章は、次の内容で構成されています。

証明書の設定の概要

[証明書の設定 (Certificate Configuration)] ウィンドウを使用して、システム上の証明書を表示します。[証明書の設定 (Certificate Configuration)] ウィンドウのフィールドは、[キャッシュの有効期間 (Duration in Cache)] を除いてすべて読み取り専用です。

証明書の検索

証明書を検索するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで [システム (System)] > [セキュリティ (Security)] > [証明書 (Certificate)] の順に選択します。

[証明書の検索と一覧表示 (Find and List Certificates)] ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

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

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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

（注）　検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3　[検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　表示されたレコード リストから、目的のレコードのリンクをクリックします。

（注）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

証明書の設定の表示

[証明書の管理(Certificate Management)] ウィンドウのフィールドは、[キャッシュの有効期間(Duration in Cache)] を除いてすべて読み取り専用です。

表 5-1　VPN プロファイルの設定値

フィールド	定義
[件名 (Subject Name)]（読み取り専用）	証明書の件名を表示します。
[発行者名 (Issuer Name)]（読み取り専用）	証明書の発行者名を表示します。
[シリアル番号 (Serial Number)]（読み取り専用）	シリアル番号（MAC アドレス）を表示します。
[IPv4 アドレス (IPv4 Address)]（読み取り専用）	IPv4 アドレスを表示します。
[IPv6 アドレス (IPv6 Address)]（読み取り専用）	IPv6 アドレスを表示します。
[キャッシュの有効期間 (Duration in Cache)]	証明書を電話機のキャッシュに保存する期間を時間単位で入力します。値にゼロを指定した場合、証明書をキャッシュしないことを示します。システムのデフォルト値を受け入れるには、ブランクのままにします。 最大値：720 時間
[選択された権限 (Selected Roles)]	証明書に現在関連付けられている権限を表示します。
[選択されたサービス (Selected Services)]	証明書に現在関連付けられているサービスを表示します。

PART 2

Cisco Unified IP Phone および Cisco ボイスメール ポートのセキュリティ

CHAPTER 6

電話機のセキュリティの概要

この章は、次の内容で構成されています。

電話機のセキュリティ機能について

インストール時は、Cisco Unified Communications Manager は非セキュア モードで起動します。Cisco Unified Communications Manager のインストール後、電話機を起動すると、デバイスはすべて非セキュアとして Cisco Unified Communications Manager に登録されます。

Cisco Unified Communications Manager 4.0(1) またはそれ以降のリリースからアップグレードした後は、アップグレード前に有効にしたデバイス セキュリティ モードで電話機が起動します。デバイスはすべて、選択されたセキュリティ モードを使用して登録されます。

Cisco Unified Communications Manager をインストールすると、Cisco Unified Communications Manager および TFTP サーバに自己署名証明書が作成されます。自己署名証明書ではなく、Cisco Unified Communications Manager のサードパーティの CA 署名付き証明書を使用することもできます。認証を設定した後、Cisco Unified Communications Manager はこの証明書を使用して、サポートされた Cisco Unified IP Phone を認証します。証明書が Cisco Unified Communications Manager および TFTP サーバに存在していれば、Cisco Unified Communications Manager はそれぞれの Cisco Unified Communications Manager のアップグレード時に証明書を再発行しません。新しい証明書エントリで新しい CTL ファイルを作成する必要があります。

ヒント サポートされていないシナリオまたは安全でないシナリオについては、「相互作用および制限」（P.1-7）を参照してください。

Cisco Unified Communications Manager は認証および暗号化のステータスをデバイス レベルで維持します。コールに関係するすべてのデバイスがセキュアとして登録されると、コール ステータスはセキュアとして登録されます。いずれか 1 つのデバイスが非セキュアとして登録されると、発信者または受信者の電話機がセキュアとして登録されても、そのコールは非セキュアとして登録されます。

ユーザが Cisco エクステンション モビリティを使用する場合、Cisco Unified Communications Manager はデバイスの認証および暗号化ステータスを保持します。また、シェアドラインが設定されている場合も、Cisco Unified Communications Manager はデバイスの認証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 Unified IP Phone に対してシェアドラインを設定する場合は、回線を共有するすべてのデバイスを暗号化用に設定します。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して、すべてのデバイスのデバイス セキュリティ モードを暗号化済みに設定します。

信頼できるデバイス

Cisco Unified Communications Manager を使用すると、Cisco Unified IP Phone の電話機モデルごとにセキュリティ 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、および接続される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、信頼できる接続に関するシスコのセキュリティ基準を満たしている、シスコ製デバイスまたはサードパーティ製デバイスです。このセキュリティ基準には、シグナリング暗号化またはメディア暗号化、プラットフォームのセキュリティ強化、および保証が含まれますが、これだけではありません。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、サポート対象のデバイスでセキュア トーンが再生されます。また、そのデバイスで、セキュア コールに関連する他の機能またはインジケータも使用できます。

Cisco Unified Communications Manager は、デバイスをシステムに追加したときに、その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 アイコンは情報提供を目的として表示されるだけなので、管理者はこのアイコンを直接設定できません。

また、Cisco Unified Communications Manager は、Cisco Unified Communications Manager の管理ページにアイコンおよびメッセージを表示し、ゲートウェイが信頼できるかどうかも示します。

ここでは、Cisco Unified IP Phone および Cisco Unified Communications Manager の管理ページでの、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

Cisco Unified Communications Manager の管理ページの次のウィンドウに、デバイスが信頼できるかどうかが示されます。

[ゲートウェイの設定 (Gateway Configuration)]

ゲートウェイ タイプごとに、[ゲートウェイの設定 (Gateway Configuration)] ウィンドウ（[デバイス (Device)] > [ゲートウェイ (Gateway)]）に、[デバイスは信頼済み (Device is trusted)] または [デバイスは信頼されていない (Device is not trusted)] が対応するアイコンとともに表示されます。

デバイス タイプに基づいて、信頼できるデバイスかどうかがシステムによって判断されます。ユーザは、信頼できるデバイスかどうかを設定できません。

[電話の設定 (Phone Configuration)]

電話機のデバイス タイプごとに、[電話の設定 (Phone Configuration)] ウィンドウ（[デバイス (Device)] > [電話 (Phone)]）に、[デバイスは信頼済み (Device is trusted)] または [デバイスは信頼されていない (Device is not trusted)] が対応するアイコンとともに表示されます。

デバイス タイプに基づいて、信頼できるデバイスかどうかがシステムによって判断されます。ユーザは、信頼できるデバイスかどうかを設定できません。

Cisco Unified IP Phone

ユーザがコールするデバイスのタイプは、電話機に表示されるセキュリティ アイコンに影響します。次の 3 つの基準を考慮して、コールがセキュアであるかどうかが判断されます。

- コールのすべてのデバイスが信頼できるデバイスであるかどうか。
- シグナリングがセキュアであるかどうか（認証および暗号化されているかどうか）。
- メディアがセキュアであるかどうか。

サポート対象の Cisco Unified IP Phone 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がコールに含まれている場合、シグナリングおよびメディアのセキュリティに関係なく、コール全体のステータスは非セキュアになり、電話機にロック アイコンは表示されません。たとえば、信頼できないデバイスを会議に加えると、そのコール レッグだけでなく会議そのものも非セキュアであると見なされます。

サポートされる電話機のモデル

使用している電話機でサポートされるセキュリティ機能の一覧については、今回のリリースの Cisco Unified Communications Manager をサポートする電話機の管理マニュアルおよびユーザ マニュアル、または、使用しているファームウェア ロードをサポートするファームウェアのマニュアルを参照してください。

Cisco Unified Reporting を使用して、特定の機能をサポートしている電話機のリストを表示することもできます。Cisco Unified Reporting の使用方法の詳細については、『*Cisco Unified Reporting Administration Guide*』を参照してください。

電話機のセキュリティ設定の確認

セキュリティをサポートする電話機に、特定のセキュリティ関連設定を構成して表示することができます。たとえば、電話機にインストールされている証明書がローカルで有効な証明書（LSC）か製造元でインストールされる証明書（MIC）かを確認できます。セキュリティ メニューおよびアイコンの詳細については、使用している電話機モデルおよび今回のバージョンの Cisco Unified Communications Manager をサポートする Cisco Unified IP Phone の管理マニュアルおよびユーザ マニュアルを参照してください。

Cisco Unified Communications Manager がコールを認証済みまたは暗号化済みとして分類すると、コールの状態を示すアイコンが電話機に表示されます。Cisco Unified Communications Manager がどのようなときにコールを認証済みまたは暗号化済みとして分類するかについては、「セキュリティ アイコン」（P.1-6）および「相互作用および制限」（P.1-7）を参照してください。

電話機のセキュリティ設定用チェックリスト

サポートされる電話機のセキュリティを設定する作業を表 6-1 で説明します。

表 6-1　電話機のセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	Cisco CTL クライアントを設定し、Cisco Unified Communications Manager セキュリティ モードを混合モードにしていない場合、設定します。	「Cisco CTL クライアントの設定」（P.4-1）
ステップ 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る証明書（MIC）が含まれていない場合、Certificate Authority Proxy Function（CAPF）を使用して LSC をインストールします。	「Certificate Authority Proxy Function の使用方法」（P.10-1）

表 6-1　電話機のセキュリティ設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 3	電話機のセキュリティ プロファイルを設定します。	「電話機セキュリティ プロファイルの設定」（P.7-1）
ステップ 4	電話機のセキュリティ プロファイルを電話機に適用します。	「電話機セキュリティ プロファイルの適用」（P.7-10）
ステップ 5	SIP を実行する電話機がダイジェスト認証をサポートする場合、[エンドユーザの設定 (End User Configuration)] ウィンドウで、ダイジェスト信用証明書を設定します。	• 「[エンドユーザの設定 (End User Configuration)] ウィンドウでのダイジェスト信用証明書の設定」（P.12-3） • 「エンド ユーザのダイジェスト信用証明書の設定内容」（P.12-3）
ステップ 6	ダイジェスト信用証明書を設定した後、[電話の設定 (Phone Configuration)] ウィンドウで、[ダイジェストユーザ (Digest User)] を選択します。	「[電話の設定 (Phone Configuration)] ウィンドウでのダイジェスト ユーザの設定」（P.12-4）
ステップ 7	Cisco Unified IP Phone 7960G または 7940G（SIP のみ）で、[エンドユーザの設定 (End User Configuration)] ウィンドウで設定したダイジェスト認証ユーザ名およびパスワード（ダイジェスト信用証明書）を入力します。	このマニュアルでは、電話機でダイジェスト認証信用証明書を入力する手順については説明しません。この作業の実行方法については、ユーザの電話機モデルと今回のバージョンの Cisco Unified Communications Manager をサポートする Cisco Unified IP Phone のアドミニストレーション ガイドを参照してください。
ステップ 8	電話機設定ファイルを暗号化します（電話機がこの機能をサポートする場合）。	「暗号化された電話機設定ファイルの設定」（P.11-1）
ステップ 9	電話機の設定を無効にして電話機のセキュリティを強化します。	「電話機のセキュリティ強化」（P.13-1）

参考情報

関連項目

- 「相互作用および制限」（P.1-7）
- 「認証、整合性、および許可の概要」（P.1-17）
- 「暗号化の概要」（P.1-22）
- 「設定用チェックリストの概要」（P.1-25）
- 「Certificate Authority Proxy Function の使用方法」（P.10-1）
- 「電話機のセキュリティ設定用チェックリスト」（P.6-3）
- 「電話機セキュリティ プロファイルの設定」（P.7-1）
- 「暗号化された電話機設定ファイルの設定」（P.11-1）
- 「電話機のセキュリティ強化」（P.13-1）

シスコの関連マニュアル

- 『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』
- 『*Troubleshooting Guide for Cisco Unified Communications Managerr*』

CHAPTER 7

電話機セキュリティ プロファイルの設定

この章は、次の内容で構成されています。

電話機セキュリティ プロファイルの概要

Cisco Unified Communications Manager の管理では、電話機タイプおよびプロトコルに対するセキュリティ関連の設定がセキュリティ プロファイルとしてまとめられ、1 つのセキュリティ プロファイルを複数の電話機に割り当てることができます。セキュリティ関連の設定には、デバイス セキュリティ モード、ダイジェスト認証、一部の CAPF 設定などがあります。[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ことで、構成済み設定を電話機に適用します。

Cisco Unified Communications Manager をインストールすると、自動登録用の事前定義済み非セキュア セキュリティ プロファイルのセットが提供されます。電話機でセキュリティ機能を有効にするには、そのデバイス タイプおよびプロトコルの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。

選択したデバイスおよびプロトコルがサポートするセキュリティ機能だけが、セキュリティ プロファイル設定ウィンドウに表示されます。

電話機セキュリティ プロファイルの設定のヒント

Cisco Unified Communications Manager の管理ページで電話機セキュリティ プロファイルを設定する場合は、次の点を考慮してください。

- 電話機を設定する場合は、[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 プロファイルを適用します。
- 事前定義済みの非セキュア プロファイルは、削除することも変更することもできません。
- 現在デバイスに割り当てられているセキュリティ プロファイルを削除することはできません。
- 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、再構成した設定が、そのプロファイルを割り当てられているすべての電話機に適用されます。
- デバイスに割り当てられているセキュリティ ファイルの名前を変更できます。古いプロファイル名および設定を割り当てられている電話機は、新しいプロファイル名および設定を受け入れます。
- 電話機セキュリティ プロファイルの CAPF 設定（認証モードおよび鍵サイズ）は、[電話の設定 (Phone Configuration)] ウィンドウにも表示されます。Manufacture-Installed Certificate（MIC; 製造元でインストールされる証明書）または Locally Significant Certificate（LSC; ローカルで有効な証明書）に関連する証明書操作の CAPF 設定を定義する必要があります。[電話の設定 (Phone Configuration)] ウィンドウで、これらのフィールドを直接更新できます。
  - セキュリティ プロファイルで CAPF 設定を更新すると、[電話の設定 (Phone Configuration)] ウィンドウで設定が更新されます。
  - [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見つかった場合、Cisco Unified Communications Manager は一致するプロファイルを電話機に適用します。
  - [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見つからなかった場合、Cisco Unified Communications Manager は新しいプロファイルを作成して電話機に適用します。
- Cisco Unified Communications Manager 5.0 以降へのアップグレード前にデバイス セキュリティ モードを設定した場合は、Cisco Unified Communications Manager が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。
- Manufacturer-Installed Certificate（MIC; 製造元でインストールされる証明書）は、LSC のインストールでのみ使用することをお勧めします。シスコでは、Cisco Unified Communications Manager との TLS 接続の認証用に 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 認証用またはその他の目的のために MIC を使用するように電話機を設定するお客様は、ご自身の責任で行ってください。MIC が侵害されてもシスコは責任を負いかねます。

  Cisco Unified Communications Manager との TLS 接続で LCS を使用するには Cisco Unified IP Phone モデル 7906G、7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、797G、7971G、7971G-GE、および 7975G をアップグレードし、CallManager 信頼ストアから MIC ルート証明書を削除して今後の互換性の問題を回避することをお勧めします。詳細については、「証明書」（P.1-15）を参照してください。

電話機セキュリティ プロファイルの検索

電話機セキュリティ プロファイルを検索するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[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)] の順に選択します。

[電話セキュリティプロファイルの検索と一覧表示 (Find and List Phone Security Profile)] ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

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

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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

（注）　検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3　[検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　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）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

追加情報

「関連項目」（P.7-13）を参照してください。

電話機セキュリティ プロファイルの設定

セキュリティ プロファイルを追加、更新、またはコピーするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[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)] の順に選択します。

ステップ 2　次の作業のいずれかを実行します。

- 新しいプロファイルを追加するには、検索ウィンドウの [新規追加 (Add New)] をクリックし、ステップ 3 に進みます。
- 既存のセキュリティ プロファイルをコピーするには、「電話機セキュリティ プロファイルの検索」（P.7-3）の説明に従い、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 [コピー (Copy)] ボタンをクリックし、ステップ 3 に進みます。
- 既存のプロファイルを更新するには、「電話機セキュリティ プロファイルの検索」（P.7-3）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、ステップ 3 に進みます。

[新規追加 (Add New)] をクリックすると、各フィールドのデフォルト設定を示し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、設定をコピーした設定ウィンドウが表示されます。

ステップ 3　SCCP を実行する電話機の場合は表 7-1、SIP を実行する電話機の場合は表 7-2 の説明に従い、適切な設定を入力します。

ステップ 4　[保存 (Save)] をクリックします。

次の作業

セキュリティ プロファイルを作成した後、「電話機セキュリティ プロファイルの適用」（P.7-10）の説明に従い、電話機に適用します。

SIP を実行する電話機の電話機セキュリティ プロファイルでダイジェスト認証を設定した場合は、[エンドユーザの設定 (End User Configuration)] ウィンドウでダイジェスト信用証明書を設定する必要があります。その後、[電話の設定 (Phone Configuration)] ウィンドウの [ダイジェストユーザ (Digest User)] 設定を使用して、ユーザを電話機に関連付ける必要があります。

追加情報

「関連項目」（P.7-13）を参照してください。

電話機セキュリティ プロファイルの設定内容

表 7-1 では、SCCP を実行する電話機のセキュリティ プロファイルの設定内容について説明します。

表 7-2 では、SIP を実行する電話機のセキュリティ プロファイルの設定内容について説明します。

選択した電話機タイプおよびプロトコルがサポートしている設定だけが表示されます。

- 設定のヒントについては、「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）を参照してください。
- 関連する情報および手順については、「関連項目」（P.7-13）を参照してください。

表 7-1　SCCP を実行する電話機のセキュリティ プロファイル

設定	説明
[名前(Name)]	セキュリティ プロファイルの名前を入力します。 新しいプロファイルを保存すると、該当する電話機タイプおよびプロトコルの [電話の設定(Phone Configuration)] ウィンドウにある [デバイスセキュリティプロファイル(Device Security Profile)] ドロップダウン リスト ボックス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、プロファイルを検索または更新する場合の適切なプロファイルの検出に役立ちます。
[説明(Description)]	セキュリティ プロファイルの説明を入力します。説明には、任意の言語で最大 50 文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。
[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、次のオプションのいずれかを選択します。 • [非セキュア(Non Secure)]：電話機にイメージ認証以外のセキュリティ機能はありません。TCP 接続で Cisco Unified Communications Manager が利用できます。 • [認証のみ(Authenticated)]：Cisco Unified Communications Manager は電話機の整合性と認証を提供します。シグナリング用に、NULL/SHA を使用する TLS 接続を開始します。 • [暗号化(Encrypted)]：Cisco 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。シグナリング用に AES128/SHA を使用する TLS 接続を開始し、すべての電話機コールのメディアを SRTP で搬送します。
[TFTP暗号化(TFTP Encrypted Config)]	このチェックボックスがオンの場合、Cisco Unified Communications Manager は電話機が TFTP サーバからダウンロードする設定ファイルを暗号化します。詳細については、「設定ファイルの暗号化」（P.1-24）および「暗号化された電話機設定ファイルの設定」の手順（P.11-1）を参照してください。

表 7-1　SCCP を実行する電話機のセキュリティ プロファイル（続き）

設定	説明
[認証モード (Authentication Mode)]	このフィールドでは、電話機が CAPF 証明書操作中に使用する認証方式を選択できます。 ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 • [認証ストリング (By Authentication String)] : ユーザが電話機に CAPF 認証文字列を入力した場合だけ、ローカルで有効な証明書をインストール、アップグレード、削除、またはトラブルシューティングします。 • [Null ストリング (By Null String)] : ユーザが介入することなく、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を一切提供しません。したがって、このオプションは安全な閉じた環境の場合にだけ選択することを強く推奨します。 • [既存の証明書 (LSC の優先)(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）が電話機に存在する場合、LSC 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。LSC が電話機に存在する場合、MIC が電話機に存在するかどうかに関係なく、認証は LSC を介して行われます。MIC と LSC が電話機に存在する場合、認証は LSC を介して行われます。電話機に LSC が存在せず、MIC が存在する場合、認証は MIC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 MIC と LSC は電話機で同時に存在できるものの、電話機は常に 1 つの証明書だけを使用して CAPF を認証します。優先されるプライマリ証明書が何らかの理由で侵害された場合、あるいは他の証明書を介して認証する場合には、認証モードを更新する必要があります。 • [既存の証明書 (MIC の優先)(By Existing Certificate (Precedence to MIC))] : LSC または MIC が電話機に存在する場合、LSC 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。MIC が電話機に存在する場合、LSC が電話機に存在するかどうかに関係なく、認証は MIC を介して行われます。電話機に LSC だけが存在し MIC が存在しない場合、認証は LSC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 **（注）** [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 パラメータと相互に関係があります（詳細については、「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）を参照してください）。[電話の設定 (Phone Configuration)] ウィンドウで CAPF 設定を定義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*』を参照してください。

表 7-1　SCCP を実行する電話機のセキュリティ プロファイル（続き）

設定	説明
[キーサイズ(Key Size、ビット)]	CAPF で使用されるこの設定では、ドロップダウン リスト ボックスから証明書の鍵サイズを選択します。デフォルト設定値は 1024 です。これ以外のオプションには、512 と 2048 があります。 デフォルト設定値よりも大きな鍵サイズを選択すると、電話機で鍵生成に必要なエントロピーを生成するためにさらに時間がかかります。鍵生成を低いプライオリティで設定すると、アクションの実行中も電話機の機能を利用できます。電話機モデルによっては、鍵生成の完了に 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の設定(Phone Security Profile Configuration)] 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 パラメータと相互に関係があります（詳細については、「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）を参照してください）。[電話の設定(Phone Configuration)] ウィンドウで CAPF 設定を定義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*』を参照してください。

表 7-2　SIP を実行する電話機のセキュリティ プロファイル

設定	説明
[名前(Name)]	セキュリティ プロファイルの名前を入力します。 新しいプロファイルを保存すると、該当する電話機タイプおよびプロトコルの [電話の設定(Phone Configuration)] ウィンドウにある [デバイスセキュリティプロファイル(Device Security Profile)] ドロップダウン リスト ボックス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、プロファイルを検索または更新する場合の適切なプロファイルの検出に役立ちます。
[説明(Description)]	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)]	ナンス値が有効な時間を秒単位で入力します。デフォルト値は 600（10 分）です。この時間が経過すると、Cisco 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ランダム値で、ダイジェスト認証パスワードの MD5 ハッシュの計算に使用されます。
[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 ボックスから、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)]：電話機にイメージ認証以外のセキュリティ機能はありません。TCP 接続で Cisco Unified Communications Manager が利用できます。 • [認証のみ(Authenticated)]：Cisco Unified Communications Manager は電話機の整合性と認証を提供します。シグナリング用に、NULL/SHA を使用する TLS 接続を開始します。 • [暗号化(Encrypted)]：Cisco 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。シグナリング用に AES128/SHA を使用する TLS 接続を開始し、すべての SRTP 対応ホップ上のすべての電話機コールのメディアを SRTP で搬送します。

表 7-2　SIP を実行する電話機のセキュリティ プロファイル（続き）

設定	説明
[転送タイプ (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)] である場合は、ドロップダウン リスト ボックスから次のオプションのいずれかを選択します（表示されないオプションもあります）。 • [TCP]：パケットを送信された順に受信するには、Transmission Control Protocol を選択します。このプロトコルは、パケットがドロップされないことを保証しますが、セキュリティは提供されません。 • [UDP]：パケットを高速に受信するには、User Datagram Protocol を選択します。このプロトコルは、パケットをドロップすることがあり、送信された順に受信するとは限りません。セキュリティは提供されません。 • [TCP + UDP]：TCP と UDP を組み合わせて使用するには、このオプションを選択します。このオプションでは、セキュリティは提供されません。 [デバイスセキュリティモード (Device Security Mode)] が [認証のみ (Authenticated)] または [暗号化 (Encrypted)] である場合、TLS が転送タイプとなります。TLS では、SIP 電話機のシグナリング整合性、デバイス認証、およびシグナリング暗号化（暗号化モードのみ）が提供されます。 プロファイルでデバイス セキュリティ モードを設定できない場合、転送タイプは UDP になります。
[ダイジェスト認証を有効化 (Enable Digest Authentication)]	このチェックボックスをオンにすると、Cisco 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、および信頼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 [認証のみ (Authenticated)] または [暗号化 (Encrypted)] を選択します。 **（注）** ダイジェスト認証の詳細については、「ダイジェスト認証」(P.1-19) および「SIP 電話機のダイジェスト認証の設定」(P.12-1) を参照してください。
[TFTP 暗号化 (TFTP Encrypted Config)]	このチェックボックスがオンの場合、Cisco Unified Communications Manager は電話機が TFTP サーバからダウンロードする設定ファイルを暗号化します。このオプションは、シスコ製電話機専用です。 **ヒント** このオプションを有効にして、対称キーを設定し、ダイジェスト信用証明書と管理者パスワードを保護することをお勧めします。 詳細については、「設定ファイルの暗号化」（P.1-24）および「暗号化された電話機設定ファイルの設定」（P.11-1）を参照してください。
[設定ファイル内のダイジェスト信用証明書を除外 (Exclude Digest Credentials in Configuration File)]	このチェックボックスがオンの場合、Cisco Unified Communications Manager は電話機が TFTP サーバからダウンロードする設定ファイル内のダイジェスト信用証明書を削除します。このオプションは、Cisco Unified IP Phone 7905G、7912G、7940G、および 7960G（SIP のみ）用です。 詳細については、「設定ファイルの暗号化」（P.1-24）および「暗号化された電話機設定ファイルの設定」（P.11-1）を参照してください。

表 7-2　SIP を実行する電話機のセキュリティ プロファイル（続き）

設定	説明
[認証モード (Authentication Mode)]	このフィールドでは、電話機が CAPF 証明書操作中に使用する認証方式を選択できます。このオプションは、シスコ製電話機専用です。 ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 • [認証ストリング (By Authentication String)] : ユーザが電話機に CAPF 認証文字列を入力した場合だけ、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。 • [Null ストリング (By Null String)] : ユーザが介入することなく、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は一切提供されません。したがって、このオプションは安全な閉じた環境の場合にだけ選択することを強く推奨します。 • [既存の証明書 (LSC の優先)(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）が電話機に存在する場合、LSC 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。LSC が電話機に存在する場合、MIC が電話機に存在するかどうかに関係なく、認証は LSC を介して行われます。電話機に LSC が存在せず、MIC が存在する場合、認証は MIC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 MIC と LSC は電話機で同時に存在できるものの、電話機は常に 1 つの証明書だけを使用して CAPF を認証します。優先されるプライマリ証明書が何らかの理由で侵害された場合、あるいは他の証明書を介して認証する場合には、認証モードを更新する必要があります。 • [既存の証明書 (MIC の優先)(By Existing Certificate (Precedence to MIC))] : LSC または MIC が電話機に存在する場合、LSC 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。MIC が電話機に存在する場合、LSC が電話機に存在するかどうかに関係なく、認証は MIC を介して行われます。電話機に LSC だけが存在し MIC が存在しない場合、認証は LSC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 **（注）** [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 パラメータと相互に関係があります（詳細については、「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）を参照してください）。[電話の設定 (Phone Configuration)] ウィンドウで CAPF 設定を定義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*』を参照してください。

表 7-2　SIP を実行する電話機のセキュリティ プロファイル（続き）

設定	説明
[キーサイズ(Key Size、ビット)]	CAPF で使用されるこの設定では、ドロップダウン リスト ボックスから証明書の鍵サイズを選択します。デフォルト設定値は 1024 です。これ以外のオプションには、512 と 2048 があります。 デフォルト設定値よりも大きな鍵サイズを選択すると、電話機で鍵生成に必要なエントロピーを生成するためにさらに時間がかかります。鍵生成を低いプライオリティで設定すると、アクションの実行中も電話機の機能を利用できます。電話機モデルによっては、鍵生成の完了に 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の設定(Phone Security Profile Configuration)] 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 パラメータと相互に関係があります（詳細については、「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）を参照してください）。[電話の設定(Phone Configuration)] ウィンドウで CAPF 設定を定義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*』を参照してください。
[SIP 電話ポート(SIP Phone Port)]	この設定は、UDP 転送を使用し SIP を実行する電話機に適用されます。 UDP を使用する Cisco Unified IP Phone（SIP のみ）が、Cisco Unified Communications Manager からの SIP メッセージの傍受に使用する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 を使用する電話機は、この設定を無視します。

電話機セキュリティ プロファイルの適用

[電話の設定(Phone Configuration)] ウィンドウで、電話機セキュリティ プロファイルを電話機に適用します。

始める前に

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、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る証明書（MIC）が含まれていることを確認します。

電話機に証明書が含まれていない場合は、次の手順を実行します。

1. [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。
2. [電話の設定(Phone Configuration)] ウィンドウで、CAPF 設定で設定された証明書をインストールします。この作業の実行の詳細については、「Certificate Authority Proxy Function の使用方法」（P.10-1）を参照してください。
3. [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したデバイス セキュリティ プロファイルを適用します。

デバイスに電話機セキュリティ プロファイルを適用するには、次の手順を実行します。

手順

ステップ 1　『*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、電話機を検索します。

ステップ 2　[電話の設定(Phone Configuration)] ウィンドウが表示されたら、[デバイスセキュリティプロファイル(Device Security Profile)] を見つけます。

ステップ 3　[デバイスセキュリティプロファイル(Device Security Profile)] ドロップダウン リスト ボックスから、デバイスに適用するセキュリティ プロファイルを選択します。該当する電話機タイプおよびプロトコル用に設定されている電話機セキュリティ プロファイルだけが表示されます。

ステップ 4　[保存(Save)] をクリックします。

ステップ 5　該当する電話機に変更を適用するには、[設定の適用] をクリックします。

次の作業

SIP を実行する電話機にダイジェスト認証を設定した場合は、[エンドユーザの設定(End User Configuration)] ウィンドウで、ダイジェスト信用証明書を設定する必要があります。次に、[電話の設定(Phone Configuration)] ウィンドウで、[ダイジェストユーザ(Digest User)] 設定を定義する必要があります。ダイジェスト ユーザおよびダイジェスト信用証明書の設定の詳細については、「SIP 電話機のダイジェスト認証の設定」（P.12-1）を参照してください。

追加情報

「関連項目」（P.7-13）を参照してください。

電話機セキュリティ プロファイルと影響を受ける電話機の同期

電話機を、設定変更が行われた電話機セキュリティ プロファイルと同期させるには、次の手順を実行します。この手順では、できる限り簡潔な方法で主な設定内容を適用します（たとえば、影響を受ける電話機の一部では、リセットまたは再起動する必要がない場合があります）。

手順

ステップ 1　[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)] の順に選択します。

[電話セキュリティプロファイルの検索と一覧表示 (Find and List Phone Security Profiles)] ウィンドウが表示されます。

ステップ 2　使用する検索条件を選択します。

ステップ 3　[検索(Find)] をクリックします。

ウィンドウに検索条件と一致する電話機セキュリティ プロファイルのリストが表示されます。

ステップ 4　該当する電話機と同期させる電話機セキュリティ プロファイルをクリックします。[電話セキュリティプロファイルの設定(Phone Security Profile Configuration)] ウィンドウが表示されます。

ステップ 5　設定の変更を行います。

ステップ 6　[保存(Save)] をクリックします。

ステップ 7　[設定の適用] をクリックします。

[設定情報の適用] ダイアログボックスが表示されます。

ステップ 8　[OK] をクリックします。

追加情報

「関連項目」（P.7-13）を参照してください。

電話機セキュリティ プロファイルの削除

ここでは、Cisco Unified Communications Manager データベースから電話機セキュリティ 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

Cisco Unified Communications Manager の管理ページからセキュリティ 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。該当プロファイルを使用しているデバイスを検索するには、セキュリティプロファイルの設定ウィンドウの [関連リンク (Related Links)] ドロップダウン リスト ボックスから [依存関係レコード (Dependency Records)] を選択して、[移動 (Go)] をクリックします。

システムで依存関係レコード機能が有効になっていない場合は、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択し、[Enable Dependency Records] 設定を [True] に変更します。依存関係レコード機能を使用すると、CPU 使用率が高くなるという情報を示すメッセージが表示されます。変更内容を保存して、依存関係レコードをアクティブにします。依存関係レコードの詳細については、『*Cisco Unified Communications Manager システム ガイド*』を参照してください。

手順

ステップ 1　「電話機セキュリティ プロファイルの検索」（P.7-3）の手順に従って、セキュリティ プロファイルを検索します。

ステップ 2　複数のセキュリティ プロファイルを削除するには、検索と一覧表示ウィンドウで、適切なチェックボックスの横に表示されているチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックします。[すべてを選択 (Select All)] をクリックしてから [選択項目の削除 (Delete Selected)] をクリックすると、この選択で設定可能なすべてのレコードを削除できます。

ステップ 3　単一のセキュリティ プロファイルを削除するには、次の作業のどちらかを実行します。

- 検索と一覧表示ウィンドウで、適切なセキュリティ プロファイルの横に表示されているチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックします。

ステップ 4　削除操作の確認を要求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、[キャンセル (Cancel)] をクリックして削除操作を取り消します。

追加情報

「関連項目」（P.7-13）を参照してください。

電話機セキュリティ プロファイルを使用している電話機の検索

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

ステップ 1　Cisco Unified Communications Manager の管理ページで、[デバイス (Device)] > [電話 (Phone)] の順に選択します。

ステップ 2　最初のドロップダウン リスト ボックスから、検索パラメータの [セキュリティプロファイル (Security Profile)] を選択します。

- 2 番目のドロップダウン リスト ボックスから検索パターンを選択します。
- 必要に応じて適切な検索テキストを指定します。

（注）　検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3　[検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　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）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

追加情報

「関連項目」（P.7-13）を参照してください。

参考情報

関連項目

- 「ダイジェスト認証」（P.1-19）
- 「設定ファイルの暗号化」（P.1-24）
- 「電話機セキュリティ プロファイルの概要」（P.7-1）
- 「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）
- 「電話機セキュリティ プロファイルの検索」（P.7-3）
- 「電話機セキュリティ プロファイルの設定」（P.7-4）
- 「電話機セキュリティ プロファイルの設定内容」（P.7-4）
- 「電話機セキュリティ プロファイルの適用」（P.7-10）
- 「電話機セキュリティ プロファイルと影響を受ける電話機の同期」（P.7-11）
- 「電話機セキュリティ プロファイルの削除」（P.7-12）
- 「電話機セキュリティ プロファイルを使用している電話機の検索」（P.7-12）
- 「暗号化された電話機設定ファイルの設定」（P.11-1）
- 「SIP 電話機のダイジェスト認証の設定」（P.12-1）
- 「電話機のセキュリティ強化」（P.13-1）

シスコの関連マニュアル

『*Cisco Unified Communications Manager アドミニストレーション ガイド*』

『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』

CHAPTER 8

セキュア インディケーション トーンと非セキュア インディケーション トーンの設定

コールが暗号化されているかどうかを示すために、保護対象の電話機でセキュア インディケーション トーンと非セキュア インディケーション トーンが再生されます。

この章は、次の内容で構成されています。

概要

保護対象の電話機でセキュア インディケーション トーンが再生されるのは、コール全体のステータスが保護対象と規定されている場合、つまりコールが暗号化されているとシステムで判別される場合です。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すものです。このトーンでは、長いビープ音が 3 回鳴ります。コール全体のステータスが保護対象と規定されている場合、着信側が応答するとすぐに、保護対象の電話機でトーンの再生が開始されます。

コール全体のステータスが保護されていない場合は、保護対象の電話機で非セキュア インディケーション トーンが再生されます（短いビープ音が 6 回鳴ります）。

（注） 保護対象の電話機の発信者にのみ、セキュア インディケーション トーンと非セキュア インディケーション トーンが聞こえます。保護されていない電話機の発信者には、これらのトーンは聞こえません。

保護対象デバイス

設定を行って、Cisco Unified Communications Manager の保護対象デバイスを指定します。Cisco Unified Communications Manager で保護対象デバイスとして設定できるのは、サポート対象の Cisco Unified IP Phone および MGCP E1 PRI ゲートウェイのみです。

システムでコールの保護ステータスの判別が行われたときに、Cisco Unified Communications Manager は MGCP IOS ゲートウェイでセキュア インディケーション トーンと非セキュア インディケーション トーンを再生することもできます。

セキュア インディケーション トーンと非セキュア インディケーション トーンを使用できるコールは、次のとおりです。

- クラスタ内 IP 間コール
- システムで保護対象と判別されるクラスタ間コール
- 保護対象 MGCP E1 PRI ゲートウェイ経由の IP と Time Division Multiplexing（TDM; 時分割多重）間のコール

保護対象デバイスとして設定可能な Cisco Unified IP Phone モデルを決定する方法については、「サポートされるデバイス」（P.8-2）を参照してください。

サポートされるデバイス

Cisco Unified Reporting を使用すると、セキュア インディケーション トーンと非セキュア インディケーション トーンをサポートする Cisco Unified IP Phone モデルを確認できます。Cisco Unified Reporting で、[Unified CM Phone Feature List] をクリックします。[Feature] プルダウン メニューから [Secure Tone] を選択します。その機能をサポートしている製品のリストが表示されます。

Cisco Unified Reporting の使用方法の詳細については、『*Cisco Unified Reporting Administration Guide*』を参照してください。

セキュア インディケーション トーンと非セキュア インディケーション トーンに関する重要情報

ここでは、セキュア インディケーション トーン機能の使用による影響について説明します。

- 保護対象デバイスに関する情報を次に示します。
  - 保護対象デバイスとして設定できるのは、SCCP または SIP を実行する電話機です。
  - 保護対象デバイスは、保護対象でないデバイス（暗号化デバイスと非暗号化デバイスの両方）にコールできます。この場合、コールは保護対象でないと規定され、非セキュア インディケーション トーンが再生されます。
  - 保護対象の電話機が別の保護対象電話機にコールを発信したが、メディアが暗号化されていない場合、そのコールは切断されません。この場合、コールを行っている電話機で非セキュア インディケーション トーンが再生されます。
- ビデオ コールの場合、保護対象デバイスでセキュア インディケーション トーンと非セキュア インディケーション トーンが再生されます。

（注） ビデオ コールでは、コールの音声部分について最初にセキュア インディケーション トーンが聞こえ、それから非セキュア メディア全体について非セキュア インディケーション トーンが聞こえることがあります。

- Cisco Unified IP Phone に表示されるロック アイコンは、メディアが暗号化されていることを示しますが、その電話機が保護対象デバイスとして設定されていることを示すものではありません。ただし、保護されたコールを発信するには、ロック アイコンが表示されている必要があります。

- サービスおよび機能への影響は次のとおりです。
  - 複数回線の補足サービス（コール転送、会議、コール待機など）は、保護対象の電話機で無効になっています。保護対象の電話機で補足サービスを呼び出すと、コールの更新ステータスを反映して、セキュア インディケーション トーンまたは非セキュア インディケーション トーンが再生されます。
  - Cisco エクステンション モビリティ サービスおよび Join Across Line サービスは、保護対象の電話機で無効になっています。
  - シェアドライン設定は、保護対象の電話機で使用できません。
  - 保留 / 復帰および不在転送は、保護対象コールでサポートされていません。
- MGCP E1 PRI ゲートウェイに関する情報を次に示します。
  - MGCP ゲートウェイは SRTP 暗号化に対応するよう設定する必要があります。このゲートウェイは、**mgcp package-capability srtp-package** コマンドを使用して設定します。
  - MGCP ゲートウェイでは、Advanced IP Services イメージまたは Advanced Enterprise Services イメージ（たとえば c3745-adventerprisek9-mz.124-6.T.bin）を指定する必要があります。
  - MGCP E1 PRI ゲートウェイとの保護ステータスの交換は、MGCP PRI Setup メッセージ、Alert メッセージ、および Connect メッセージの独自の FacilityIE を使用して行われます。
  - Cisco Unified Communications Manager がセキュア インディケーション トーンを再生するのは、Cisco Unified IP Phone に対してのみです。コールのゲートウェイ エンドに対してトーンを再生するのは、ネットワーク内の PBX です。
  - Cisco Unified IP Phone と MGCP E1 PRI ゲートウェイとの間のメディアが暗号化されていない場合、コールは切断されます。

（注） MGCP ゲートウェイに関する暗号化の詳細については、使用中の Cisco IOS ソフトウェア 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。

設定要件

セキュア トーンの再生については、次に示す項目を設定する必要があります。

- [電話の設定 (Phone Configuration)] ウィンドウ（Cisco Unified Communications Manager の管理ページで [デバイス (Device)] > [電話 (Phone)] を選択して移動）で、次の項目を設定します。
  - ウィンドウの [デバイス情報 (Device Information)] 部分に表示されている [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、[Standard Protected Phone] を選択します。

（注） 保護対象の電話機には、補足サービス ソフトキーのない新しいソフトキー テンプレートを使用する必要があります。

  - [回線をまたいで参加 (Join Across Lines)] オプション（同じウィンドウの [デバイス情報 (Device Information)] 部分に表示）で、[オフ (Off)] を選択します。
  - [保護されたデバイス (Protected Device)] チェックボックス（同じウィンドウの [デバイス情報 (Device Information)] 部分に表示）をオンにします。

  - [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（同じウィンドウの [プロトコル固有情報(Protocol Specific Information)] 部分に表示）から、[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（[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)]）で設定済みのセキュアな電話機のプロファイルを選択します。

- [電話の設定(Phone Configuration)] ウィンドウで電話番号を追加するときに [電話番号の設定(Directory Number Configuration)] ウィンドウが表示されるので、このウィンドウに移動します。[電話番号の設定(Directory Number Configuration)] ウィンドウの [デバイス < *デバイス名* > の複数コール / コール待機設定(Multiple Call/Call Waiting Settings on Device <DeviceName>)] 領域で、次の 2 つのオプションの値を 1 に設定します。
  - [コール最大数(Maximum Number of Calls)]
  - [ビジートリガー(Busy Trigger)]
- Cisco Unified Communications Manager の管理ページで、[システム(System)] > [サービスパラメータ(Service Parameters)] を選択します。最初の [サービスパラメータ設定(Service Parameter Configuration)] ウィンドウでサーバを選択し、Cisco CallManager サービスを選択します。2 番目の [サービスパラメータ設定(Service Parameter Configuration)] ウィンドウで [Clusterwide Parameters (Feature - Secure Tone)] 領域を見つけて、[Play Secure Indication Tone] オプションを [True] に設定します（デフォルト値は [False] です）。
- 保護対象の MGCP E1 PRI ゲートウェイを設定する場合は、Cisco Unified Communications Manager の管理ページで [デバイス(Device)] > [ゲートウェイ(Gateway)] > [新規追加(Add New)] を選択し、サポート対象ゲートウェイを選択します。プロトコルには [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、次のように設定します。
  - [Global ISDN Switch Type] を [Euro] に設定します。
  - MGCP ゲートウェイのその他の設定を完了したら、[保存(Save)] をクリックし、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 アイコンをクリックします。[保護されたファシリティIEの有効化(Enable Protected Facility IE)] チェックボックスが表示されます。このチェックボックスをオンにします。

    この設定により、Cisco Unified IP Phone エンドポイントと、MGCP ゲートウェイに接続している保護対象 PBX 電話機との間で、コールの保護ステータスを渡すことが可能になります。

CHAPTER 9

アナログ エンドポイントの暗号化の設定

この機能を使用すると、アナログ電話機で Cisco VG2xx Gateway へのセキュアな SCCP 接続を作成できます。このゲートウェイは、SCCP シグナリング通信には Cisco 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。Cisco Unified Communications Manager の既存の TLS 機能（証明書の管理など）は、セキュアな SCCP 通信で使用されます。

この章は、次の内容で構成されています。

電話機セキュリティ プロファイル

アナログ電話機で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 (Device Security Mode)] パラメータを [認証のみ (Authenticated)] または [暗号化 (Encrypted)] に設定して、アナログ電話機用の電話機セキュリティ プロファイルを作成する必要があります。電話機セキュリティ プロファイルを作成するには、Cisco Unified Communications Manager の管理ページで [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)] の順に選択します。

電話機セキュリティ プロファイルの作成の詳細については、『*Cisco Unified Communications Manager セキュリティ ガイド*』の第 7 章「電話機セキュリティ プロファイルの設定」を参照してください。

Cisco VG2xx ゲートウェイに接続されているアナログ電話機を設定する場合は、[デバイスセキュリティプロファイル (Device Security Profile)] パラメータに対して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。[デバイスセキュリティプロファイル (Device Security Profile)] パラメータを設定するには、Cisco Unified Communications Manager の管理ページで [デバイス (Device)] > [電話 (Phone)] にナビゲートして、設定を行う電話機の [プロトコル固有情報 (Protocol Specific Information)] セクションまでスクロールします。

証明書の管理

セキュアなアナログ電話機の機能を利用するには、同じ CA 署名付き証明書を、Cisco VG2xx Gateway で使用する 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、『*Cisco Unified Communications Operating System Administration Guide*』の第 6 章「Security」を参照してください。

CHAPTER 10

Certificate Authority Proxy Function の使用方法

この章は、次の内容で構成されています。

Certificate Authority Proxy Function の概要

Certificate Authority Proxy Function（CAPF）は Cisco Unified Communications Manager とともに自動的にインストールされ、設定に応じて次のタスクを実行します。

- 既存の Manufacturing Installed Certificate（MIC; 製造元でインストールされる証明書）、Locally Significant Certificate（LSC; ローカルで有効な証明書）、ランダム生成された認証文字列、または安全性の低いオプションの「null」認証によって認証します。
- ローカルで有効な証明書を、サポートされている Cisco Unified IP Phone に対して発行します。
- 電話機にある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。
- 電話機の証明書を表示およびトラブルシューティングするために取得します。

インストール中に、CAPF に固有の証明書が生成されます。CAPF 証明書は Cisco CTL クライアントによってクラスタ内のすべての Cisco Unified Communications Manager サーバにコピーされ、拡張子 .0 を使用します。CAPF 証明書が存在することを確認するには、Cisco Unified Communications オペレーティング システムの GUI で、CAPF 証明書を表示します。

Cisco Unified IP Phone と CAPF の相互作用

CAPF と相互に作用するとき、電話機は認証文字列、既存の MIC または LSC 証明書、または「null」を使用して CAPF に対して自分を認証し、公開鍵と秘密鍵のペアを生成し、署名付きメッセージで公開鍵を CAPF サーバに転送します。秘密鍵はそのまま電話機に残り、外部に公開されることはありません。CAPF は、電話機証明書に署名し、その証明書を署名付きメッセージで電話機に返送します。

次の情報は、通信または電源の障害が発生した場合に適用されます。

- 電話機で証明書をインストールしているときに通信障害が発生すると、電話機は 30 秒間隔であと 3 回、証明書を取得しようとします。これらの値は設定することができません。
- 電話機で CAPF とのセッションを試行しているときに電源障害が発生すると、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。これは、電話機がリブート後に 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にあたります。証明書の操作が完了すると、フラッシュ内の値はシステムによってクリアされます。

ヒント　電話機ユーザが電話機で証明書操作を中断したり、操作ステータスを確認できることに注意してください。

ヒント　鍵生成を低いプライオリティで設定すると、アクションの実行中も電話機の機能を利用できます。鍵生成の完了には 30 分以上かかります。

証明書生成中も電話機は機能しますが、TLS トラフィックが増えることにより、最小限の範囲ですがコール処理が中断される場合があります。たとえば、インストールの終了時に証明書がフラッシュに書き込まれる際に音声が乱れることがあります。

証明書用に 2048 ビットの鍵を選択すると、電話機の起動およびフェールオーバー中に電話機、Cisco Unified Communications Manager、およびセキュア SRST 対応ゲートウェイとの間で接続を確立するのに 60 秒以上かかる場合があります。最高のセキュリティ レベルを必要としている場合を除き、2048 ビットの鍵は設定しないでください。

次に、ユーザまたは Cisco Unified Communications Manager によって電話機がリセットされたときに CAPF が Cisco Unified IP Phone 7960G および 7940G とどのように相互に作用するかについて説明します。

（注）　次の例では、LSC が電話機内にまだ存在しない場合や、CAPF 情報の [認証モード(Authentication Mode)] に [既存の証明書(By Existing Certificate)] が選択されている場合に、CAPF 証明書操作が失敗します。

例：非セキュアのデバイス セキュリティ モード

この例では、[デバイスセキュリティモード(Device Security Mode)] を [非セキュア(Nonsecure)] に、CAPF 情報の [認証モード(Authentication Mode)] を [Null ストリング(By Null String)] または [既存の証明書(... の優先)(By Existing Certificate (Precedence...))] に設定した後に電話機がリセットされます。電話機は、リセット後すぐにプライマリ Cisco Unified Communications Manager に登録し、設定ファイルを受け取ります。次に、電話機は自動的に CAPF とのセッションを開始し、LSC をダウンロードします。LSC のインストール後、電話機は [デバイスセキュリティモード(Device Security Mode)] を [認証のみ(Authenticated)] または [暗号化(Encrypted)] に設定します。

例：認証のみまたは暗号化デバイス セキュリティ モード

この例では、[デバイスセキュリティモード(Device Security Mode)] を [認証のみ(Authenticated)] または [暗号化(Encrypted)] に、CAPF 情報の [認証モード(Authentication Mode)] を [Null ストリング(By Null String)] または [既存の証明書(... の優先)(By Existing Certificate (Precedence...))] に設定した後に電話機がリセットされます。CAPF セッションが終了して電話機が LSC をインストールするまで、電話機はプライマリ Cisco Unified Communications Manager に登録しません。セッションが終了すると、電話機は登録を行い、すぐに認証済みまたは暗号化済みモードで動作します。

この例では、電話機は CAPF サーバに自動的に接続しないので、[認証ストリング(By Authentication String)] を設定することはできません。電話機に有効な 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 の相互作用

CAPF は、IPv4、IPv6、またはその両方のタイプのアドレスを使用する電話機に証明書を発行したり、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 が実行されている電話機に対して証明書を発行またはアップグレードするには Cisco Unified Communications Manager の管理 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 Enable IPv6 エンタープライズ パラメータの設定を使用して、電話機に対して証明書を発行するか、アップグレードするかを決定します。このエンタープライズ パラメータが **False** に設定されると、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。

表 10-1 で、IPv4、IPv6、またはその両方のタイプのアドレスを使用する電話機で CAPF に接続する方法を説明します。

表 10-1　IPv6 または IPv4 電話機から 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
デュアルスタック	IPv4 および IPv6 対応	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 アドレスで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。
デュアルスタック	IPv4	IPv4、IPv6	電話機は IPv4 アドレスを使用して CAPF に接続します。
デュアルスタック	IPv6	IPv4、IPv6	電話機は IPv6 アドレスを使用して CAPF に接続します。接続に失敗すると、電話機は IPv4 アドレスを使用して CAPF に接続します。
デュアルスタック	IPv4	IPv4	電話機は IPv4 アドレスを使用して CAPF に接続します。

表 10-1　IPv6 または IPv4 電話機から CAPF への接続方法（続き）

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
デュアルスタック	IPv4 および IPv6 対応	IPv6	電話機は IPv6 アドレスを使用して CAPF に接続します。
デュアルスタック	IPv4 および IPv6 対応	IPv4	電話機は IPv4 アドレスを使用して CAPF に接続します。
デュアルスタック	IPv4	IPv6	電話機は CAPF に接続できません。
デュアルスタック	IPv6	IPv4	電話機は CAPF に接続できません。
デュアルスタック	IPv6	IPv6	電話機は IPv6 アドレスを使用して CAPF に接続します。
IPv4	IPv4	IPv4、IPv6	電話機は IPv4 アドレスを使用して CAPF に接続します。
IPv6	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	IPv4	IPv4	電話機は IPv4 アドレスを使用して CAPF に接続します。
IPv4	IPv4	IPv6	電話機は CAPF に接続できません。
IPv6	IPv6	IPv6	電話機は IPv6 アドレスを使用して CAPF に接続します。
IPv6	IPv6	IPv4	電話機は CAPF に接続できません。

CAPF システムの相互作用および要件

CAPF には、次の要件があります。

- CAPF を使用する前に、Cisco CTL クライアントのインストールおよび設定に必要なすべての作業を実行したことを確認します。CAPF を使用するには、最初のノードで Cisco Certificate Authority Proxy Function サービスをアクティブにする必要があります。
- 証明書のアップグレードまたはインストール操作で、電話機に対して CAPF 認証方式を [認証ストリング (By Authentication String)] にした場合、操作後に同じ認証文字列を電話機に入力する必要があります。入力しなかった場合、操作が失敗します。TFTP Encrypted Configuration エンタープライズ パラメータが有効で、認証文字列を入力しなかった場合、電話機に障害が発生し、電話機に入力された認証文字列が一致するまで復帰しないことがあります。
- スケジューリングされたメンテナンス画面で CAPF を使用することを強く推奨します。これは、同時に多数の証明書が生成されると、コール処理が中断される場合があるためです。
- Cisco Unified Communications Manager クラスタ内のすべてのサーバで、同じ管理者ユーザ名とパスワードを使用する必要があります。これで、CAPF はクラスタ内のすべてのサーバに認証を受けることができます。
- 証明書操作の間、最初のノードが実行中で正しく機能していることを確認します。
- 証明書操作の間、電話機が正しく機能していることを確認します。
- 保護された電話機が別のクラスタに移動された場合、Cisco Unified Communications Manager はその電話機が送信する LSC 証明書を信頼しません。これは、その LSC 証明書が別の CAPF によって発行されたものであり、その CAPF の証明書が CTL ファイルに存在しないためです。保護された電話機が登録できるようにするには、「Cisco Unified IP Phone 上の CTL ファイルの削除」（P.4-19）に従って、既存の CTL ファイルを削除します。その後、[インストール/アップグレード

（Install/Upgrade）] オプションを使用して、新しい CAPF で新しい LSC 証明書をインストールし、新しい CTL ファイルのために電話機をリセットできます（または MIC を使用できます）。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 セクションで [削除 (Delete)] オプションを使用します。

ヒント Cisco IP Telephony Backup and Restore System（BARS）を使用して、CAPF データおよびレポートをバックアップすることができます。これは Cisco Unified Communications Manager によって情報が Cisco Unified Communications Manager データベースに格納されるためです。

Cisco Unified サービスアビリティでの CAPF の設定

次の作業を Cisco Unified サービスアビリティで実行します。

- Cisco Certificate Authority Proxy Function サービスをアクティブにします。
- CAPF 用のトレース設定を行います。

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

CAPF の設定用チェックリスト

表 10-2 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する場合に実行する作業のリストを示します。

表 10-2　CAPF の設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	ローカルで有効な証明書が電話機に存在するかどうかを確認します。 CAPF データを Cisco Unified Communications Manager パブリッシャ データベース サーバにコピーする必要があるかどうかを確認します。 **ヒント** Cisco Unified Communications Manager 4.0 で CAPF ユーティリティを使用していて、CAPF データが Cisco Unified Communications Manager データベースに存在することを確認した場合は、Cisco Unified Communications Manager 4.0 で使用していた CAPF ユーティリティを削除できます。	• 使用している電話機モデルとこのバージョンの Cisco Unified Communications Manager をサポートする電話機のマニュアル • このバージョンの Cisco Unified Communications Manager をサポートする『*Data Migration Assistant User Guide*』
ステップ 2	Cisco Certificate Authority Proxy Function サービスが実行されていることを確認します。 **ヒント** このサービスは、すべての CAPF 操作時に実行されている必要があります。またこのサービスは、CTL ファイルに CAPF 証明書を組み込むために、Cisco CTL クライアントでも実行されている必要があります。	「Certificate Authority Proxy Function サービスのアクティブ化」（P.10-6）

表 10-2　CAPF の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 3	Cisco CTL クライアントのインストールおよび設定に必要なすべての作業を実行したことを確認します。CAPF 証明書が Cisco CTL ファイル内に存在することを確認します。	「Cisco CTL クライアントの設定」（P.4-10）
ステップ 4	必要に応じて、CAPF サービス パラメータを更新します。	• 「CAPF サービス パラメータの更新」（P.10-7） • 「CAPF による電話機の証明書のインストール、アップグレード、トラブルシューティング、または削除」（P.10-7）
ステップ 5	電話機のローカルで有効な証明書をインストール、アップグレード、またはトラブルシューティングするには、Cisco Unified Communications Manager の管理ページを使用します。	• 「CAPF による電話機の証明書のインストール、アップグレード、トラブルシューティング、または削除」（P.10-7） • 「[電話の設定 (Phone Configuration)] ウィンドウの CAPF 設定」（P.10-8） • 「LSC ステータスまたは認証文字列に基づく電話機の検索」（P.10-9）
ステップ 6	証明書の操作が必要な場合は、認証文字列を電話機に入力します。	「電話機での認証文字列の入力」（P.10-11）

Certificate Authority Proxy Function サービスのアクティブ化

Cisco Unified Communications Manager は、Cisco Unified サービスアビリティで Certificate Authority Proxy Function サービスを自動的にはアクティブ化しません。

Cisco CTL クライアントをインストールして設定する前にこのサービスをアクティブにしなかった場合は、「CTL ファイルの更新」（P.4-13）の説明に従って CTL ファイルを更新する必要があります。このサービスは、最初のノードでのみアクティブにします。

サービスをアクティブにするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified サービスアビリティで、[Tools] > [Service Activation] の順に選択します。

ステップ 2　[Server] ドロップダウン リスト ボックスから、Certificate Authority Proxy Function サービスをアクティブにするサーバを選択します。

ステップ 3　[Certificate Authority Proxy Function] チェックボックスをオンにします。

ステップ 4　[Save] をクリックします。

追加情報

「関連項目」（P.10-12）を参照してください。

CAPF サービス パラメータの更新

CAPF サービスのパラメータを設定するウィンドウには、証明書の有効年数、システムによる鍵生成の最大再試行回数、鍵のサイズなどの情報が表示されます。

CAPF サービス パラメータが、Cisco Unified Communications Manager の管理ページでアクティブのステータスとして表示されるようにするには、「Certificate Authority Proxy Function サービスのアクティブ化」（P.10-6）の説明に従って Certificate Authority Proxy Function サービスをアクティブにする必要があります。

CAPF サービス パラメータを更新するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [サービスパラメータ (Service Parameters)] を選択します。

ステップ 2　[サーバ (Server)] ドロップダウン リスト ボックスから、サーバを選択します。

ヒント　クラスタ内の最初のノードを選択する必要があります。

ステップ 3　[サービス (Service)] ドロップダウン リスト ボックスから、Cisco Certificate Authority Proxy Function サービスを選択します。

ステップ 4　パラメータごとに表示されるヘルプの説明に従い、CAPF サービス パラメータを更新します。

（注）　CAPF サービス パラメータのヘルプを表示するには、疑問符またはパラメータ名リンクをクリックします。

ステップ 5　変更内容を有効にするには、Cisco Certificate Authority Proxy Function サービスを再起動する必要があります。

追加情報

「関連項目」（P.10-12）を参照してください。

CAPF による電話機の証明書のインストール、アップグレード、トラブルシューティング、または削除

CAPF を使用するときに、表 10-3 を参照してください。

Certificate Authority Proxy Function を使用するには、次の手順を実行します。

手順

ステップ 1　『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の説明に従って、電話機を検索します。

ステップ 2　検索結果が表示された後、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する電話機を見つけて、その電話機の [デバイス名(Device Name、回線)] リンクをクリックします。

ステップ 3　表 10-3 の説明に従って、設定内容を入力します。

ステップ 4　[保存(Save)] をクリックします。

ステップ 5　[リセット(Reset)] をクリックします。

追加情報

「関連項目」（P.10-12）を参照してください。

[電話の設定(Phone Configuration)] ウィンドウの CAPF 設定

表 10-3 は、Cisco Unified Communications Manager の管理ページの [電話の設定(Phone Configuration)] ウィンドウにある CAPF 設定について説明しています。

- 設定のヒントについては、「CAPF システムの相互作用および要件」（P.10-4）を参照してください。
- 関連する情報および手順については、「関連項目」（P.10-12）を参照してください。

表 10-3　CAPF 設定

設定	説明
[証明書の操作(Certificate Operation)]	ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 • [保留中の操作なし(No Pending Operation)]：証明書の操作が発生しないときに表示されます（デフォルトの設定）。 • [インストール/アップグレード(Install/Upgrade)]：電話機にローカルで有効な証明書を新しくインストールするか、あるいは既存の証明書をアップグレードします。 • [削除(Delete)]：電話機に存在するローカルで有効な証明書を削除します。 • [トラブルシューティング(Troubleshoot)]：ローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）を取得します。取得することで、CAPF トレース ファイルで証明書のクレデンシャルを確認できます。電話機に両方の種類の証明書が存在する場合、Cisco Unified Communications Manager は証明書の種類ごとに 1 つずつ、2 つのトレース ファイルを作成します。 **ヒント** [トラブルシューティング(Troubleshoot)] オプションを選択すると、LSC または MIC が電話機に存在することを確認できます。電話機に証明書が存在しない場合、[削除(Delete)] オプションと [トラブルシューティング(Troubleshoot)] オプションは表示されません。

表 10-3　CAPF 設定（続き）

設定	説明
[認証文字列 (Authentication String)]	[認証ストリング (By Authentication String)] オプションを選択した場合に、このフィールドは適用されます。文字列を手動で入力するか、あるいは [文字列を生成 (Generate String)] ボタンをクリックして文字列を生成します。文字列は 4 ～ 10 桁にしてください。 ローカルで有効な証明書をインストール、アップグレード、またはトラブルシューティングするには、電話機ユーザまたは管理者が電話機に認証文字列を入力する必要があります。詳細については、「電話機での認証文字列の入力」（P.10-11）を参照してください。
[文字列を生成 (Generate String)]	CAPF で自動的に認証文字列を生成する場合は、このボタンをクリックします。4 ～ 10 桁の認証文字列が [認証文字列 (Authentication String)] フィールドに表示されます。
[操作の完了期限 (Operation Completes By)]	このフィールドは、すべての証明書操作オプションをサポートし、操作を完了する必要がある期限の日付と時刻を指定します。 表示される値は、最初のノードに適用されます。
[証明書の操作ステータス (Certificate Operation Status)]	このフィールドは証明書操作の進行状況を表示します。たとえば、<操作のタイプ> pending、failed、successful などです（操作のタイプには、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という証明書操作オプションが表示されます）。このフィールドに表示される情報は変更できません。

LSC ステータスまたは認証文字列に基づく電話機の検索

証明書操作ステータスまたは認証文字列に基づいて電話機を検索するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[デバイス (Device)] > [電話 (Phone)] の順に選択します。

検索と一覧表示ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

ステップ 2　最初のドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。

- [LSC ステータス (LSC Status)] : このオプションを選択すると、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、削除、またはトラブルシューティングに CAPF を使用する電話機のリストが表示されます。
- [認証文字列 (Authentication String)] : このオプションを選択すると、[認証文字列 (Authentication String)] フィールドで指定された認証文字列を持つ電話機のリストが返されます。

ステップ 3　2 番目のドロップダウン リスト ボックスから、検索パターンを選択します。

ステップ 4　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、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 5　[検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 6　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）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

追加情報

「関連項目」（P.10-12）を参照してください。

CAPF レポートの生成

必要に応じて CAPF レポートを生成し、証明書操作のステータス、認証文字列、セキュリティ プロファイル、認証モードなどを表示できます。レポートには、デバイス名、デバイスの説明、セキュリティ プロファイル、認証文字列、認証モード、LSC ステータスなどが含まれます。

CAPF レポートを生成するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[デバイス (Device)] > [電話 (Phone)] の順に選択します。

検索と一覧表示ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

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

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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

（注）　検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3　[検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　[関連リンク (Related Links)] ドロップダウン リスト ボックスで、[ファイルでの CAPF レポート (CAPF Report in File)] を選択し、[移動 (Go)] をクリックします。

ステップ 5　ファイルを任意の場所に保存します。

ステップ 6　Microsoft Excel を使用して .csv ファイルを開きます。

追加情報

「関連項目」（P.10-12）を参照してください。

電話機での認証文字列の入力

認証ストリング モードを選択して認証文字列を生成した場合、ローカルで有効な証明書をインストールするには、電話機に認証文字列を入力する必要があります。

ヒント　認証文字列は 1 回の使用に限って適用されます。[電話の設定 (Phone Configuration)] ウィンドウまたは CAPF レポートに表示される認証文字列を入手します。

始める前に

電話機に認証文字列を入力する前に、次の条件を満たしていることを確認します。

- CAPF 証明書が CTL ファイル内に存在する。
- 「Certificate Authority Proxy Function サービスのアクティブ化」（P.10-6）の説明に従って、Cisco Certificate Authority Proxy Function サービスをアクティブにした。
- 最初のノードが機能していて、実行中である。証明書のインストールごとにサーバが実行していることを確認する。
- デバイスが登録済みである。
- 署名付きイメージが電話機に存在する（使用している電話機モデルをサポートする Cisco Unified IP Phone の管理マニュアルを参照してください）。

手順

ステップ 1　電話機の設定ボタンを押します。

ステップ 2　設定がロックされている場合は、**#（アスタリスク、アスタリスク、シャープ記号）を押してロックを解除します。

ステップ 3　下方にスクロールして [設定] メニューに移動します。[セキュリティ設定] を強調表示し、[選択] ソフトキーを押します。

ステップ 4　下方にスクロールして [セキュリティ設定] メニューに移動します。[LSC] を強調表示し、[更新] ソフトキーを押します。

ステップ 5　認証文字列の入力を要求するプロンプトが表示された場合、システムから提供された文字列を入力して [送信] ソフトキーを押します。

電話機は現在の CAPF の設定に応じて、証明書をインストール、更新、削除、または取得します。

電話機に表示されるメッセージを確認すると、証明書の操作の進捗を監視することができます。[送信] を押すと、LSC オプションの下に「処理中」というメッセージが表示されます。電話機は、公開鍵と秘密鍵のペアを生成し、情報を電話機に表示します。電話機が正常に手順を完了すると、成功したことを示すメッセージが電話機に表示されます。電話機に失敗のメッセージが表示されるのは、誤った認証文字列を入力したか、電話機のアップグレードを有効にしなかった場合です。

[中止] オプションを選択すると、いつでも手順を停止できます。

追加情報

「関連項目」（P.10-12）を参照してください。

電話機での認証文字列の確認

[設定] > [モデル情報] の順に選択して LSC の設定が [インストール済み] か [未インストール] のどちらであるかを確認すれば、電話機に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。

追加情報

「関連項目」（P.10-12）を参照してください。

参考情報

関連項目

- 「Certificate Authority Proxy Function の概要」（P.10-1）
- 「Cisco Unified IP Phone と CAPF の相互作用」（P.10-2）
- 「CAPF システムの相互作用および要件」（P.10-4）
- 「Cisco Unified サービスアビリティでの CAPF の設定」（P.10-5）
- 「CAPF の設定用チェックリスト」（P.10-5）
- 「Certificate Authority Proxy Function サービスのアクティブ化」（P.10-6）
- 「CAPF サービス パラメータの更新」（P.10-7）
- 「CAPF による電話機の証明書のインストール、アップグレード、トラブルシューティング、または削除」（P.10-7）
- 「[電話の設定 (Phone Configuration)] ウィンドウの CAPF 設定」（P.10-8）
- 「LSC ステータスまたは認証文字列に基づく電話機の検索」（P.10-9）
- 「CAPF レポートの生成」（P.10-10）

- 「電話機での認証文字列の入力」（P.10-11）
- 「電話機での認証文字列の確認」（P.10-12）

シスコの関連マニュアル

『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』

『*Cisco Unified Serviceability Administration Guide*』

CHAPTER 11

暗号化された電話機設定ファイルの設定

セキュリティ関連の設定を構成した後、電話機設定ファイルには、ダイジェスト パスワードや電話機管理者パスワードなど、機密性が高い情報が含まれます。設定ファイルの機密性を守るために、設定ファイルを暗号化するように設定する必要があります。

この章は、次の内容で構成されています。

電話機設定ファイルの暗号化について

電話機が Cisco Unified Communications Manager からダウンロードする設定ファイル内のダイジェスト信用証明書およびセキュア パスワードを保護するには、[電話セキュリティプロファイルの設定(Phone Security Profile Configuration)] ウィンドウで [TFTP暗号化(TFTP Encrypted Config)] オプションを有効にして、Cisco Unified Communications Manager の管理で追加作業を実行する必要があります。

[TFTP暗号化(TFTP Encrypted Config)] オプションを有効にして Cisco Unified Communications Manager の管理ページおよび電話機で、必要なパラメータを設定し、Cisco Unified サービスアビリティで必要なサービスを再起動すると、TFTP サーバは次の作業を実行します。

1. ディスク上のクリア テキストの設定ファイルをすべて削除します。
2. 暗号化されたバージョンの設定ファイルを生成します。

電話機が暗号化された電話機設定ファイルをサポートしている場合に、電話機設定ファイルの暗号化に必要な作業を実行すると、電話機は設定ファイルの暗号化されたバージョンを要求します。

警告　**SIP を実行する電話機のダイジェスト認証が有効になっていて、TFTP 暗号化設定が無効になっている場合、ダイジェスト信用証明書は暗号化されずに送信されます。詳細については、「電話機設定ファイルの暗号化の無効化」（P.11-9）を参照してください。**

「サポートされる電話機のモデル」（P.11-4）で説明するように、暗号化された電話機設定ファイルをサポートしない電話機があります。電話機モデルとプロトコルによって、設定ファイルの暗号化に使用される方式が決まります。サポートされる方式は、Cisco 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。暗号化された設定ファイルをサポートしないバージョンに電話機ファームウェアをダウングレードした場合、TFTP サーバは、最小限の設定内容を含む暗号化されていない設定ファイルを提供します。その結果、電話機が期待されるとおりに動作しない可能性があります。

鍵情報の機密性を維持するために、暗号化された電話機設定ファイルに関する作業は、セキュアな環境で実行することを強く推奨します。

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

- 鍵の手動配布
- 電話機の公開鍵による対称キーの暗号化

「鍵の手動配布」および「電話機の公開鍵による対称キーの暗号化」の項の情報は、混合モードに設定し、Cisco Unified Communications Manager の管理で TFTP Encrypted Config パラメータを有効にしたことを前提とします。

鍵の手動配布

ヒント　この方式をサポートする電話機のリストについては、「サポートされる電話機のモデル」（P.11-4）を参照してください。

鍵の手動配布では、電話機がリセットされた後、Cisco Unified Communications Manager データベースに格納されている 128 ビットまたは 256 ビットの対称キーによって、電話機設定ファイルが暗号化されます。使用中の電話機モデルの鍵サイズを確認するには、「サポートされる電話機のモデル」（P.11-4）を参照してください。

設定ファイルを暗号化するには、[電話の設定 (Phone Configuration)] ウィンドウで、管理者が手動で鍵を入力するか、Cisco Unified Communications Manager が鍵を生成するように要求できます。データベースに鍵が存在するようになった後、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、電話機に鍵を入力する必要があります。[Accept] ソフトキーを押すとすぐに、鍵は電話機のフラッシュに格納されます。鍵を入力した後、電話機をリセットすると、電話機は暗号化された設定ファイルを要求します。必要な作業を実行した後、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、設定ファイルを暗号化します。電話機が RC4 と AES 128 のどちらの暗号化アルゴリズムを使用するかを確認するには、「サポートされる電話機のモデル」（P.11-4）を参照してください。

電話機に対称キーが含まれている場合、電話機は必ず暗号化された設定ファイルを要求します。Cisco Unified Communications Manager は、TFTP サーバが署名した暗号化された設定ファイルを電話機にダウンロードします。すべての電話機タイプが設定ファイルの署名者を検証するわけではありません。詳細については、「サポートされる電話機のモデル」（P.11-4）を参照してください。

電話機は、フラッシュに格納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 暗号化 (TFTP Encrypted Config)] 設定を無効にした場合、管理者は、次にリセットしたときに暗号化されていない設定ファイルを電話機が要求するように、電話機 GUI から対称キーを削除する必要があります。

電話機の公開鍵による対称キーの暗号化

ヒント　この方式をサポートする電話機のリストについては、「サポートされる電話機のモデル」（P.11-4）を参照してください。

Certificate Authority Proxy Function（CAPF）の詳細については、「Certificate Authority Proxy Function の概要」（P.10-1）を参照してください。Certificate Authority Proxy Function（CAPF）は、Cisco Unified Communications Manager に対する Cisco Unified IP Phone を認証し、電話機の証明書（LSC）を発行します。

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 暗号化で使用される公開鍵と秘密鍵のペアが含まれています。

この方式を初めて使うとき、設定ファイルの電話機証明書の MD5 ハッシュと、LSC または MIC の MD5 ハッシュが比較されます。電話機で問題が検出されない場合、電話機は、リセット後に暗号化された設定ファイルを TFTP サーバに要求します。電話機で問題が検出された場合（ハッシュが一致しない、電話機に証明書が含まれていない、MD5 値がブランクであるなど）、CAPF 認証モードが [認証ストリング (By Authentication String)] でなければ、電話機は CAPF とのセッションを開始しようとします（[認証ストリング (By Authentication String)] の場合は、文字列を手動で入力する必要があります）。CAPF は、電話機の公開鍵を LSC または MIC から抽出し、MD5 ハッシュを生成し、公開鍵および証明書ハッシュの値を Cisco Unified Communications Manager データベースに格納します。公開鍵がデータベースに格納された後、電話機はリセットされ、新しい設定ファイルが要求されます。

公開鍵がデータベースに存在するようになり、電話機がリセットされた後、電話機用の公開鍵があることをデータベースが TFTP に通知すると、対称キー暗号化処理が開始されます。TFTP サーバは 128 ビット対称キーを生成します。これによって、設定ファイルは Advanced Encryption Standard（AES; 高度暗号化規格）128 暗号化アルゴリズムで暗号化されます。次に、電話機の公開鍵で対称キーが暗号化され、設定ファイルの署名付きエンベロープ ヘッダーに含まれます。電話機は、ファイルの署名を検証し、署名が有効である場合は、LSC または MIC の秘密鍵を使用して、暗号化された対称キーを復号化します。次に、対称キーによって、ファイルの内容が復号化されます。

設定ファイルを更新するたびに、TFTP サーバは、ファイルを暗号化する新しい鍵を自動的に生成します。

ヒント　この暗号化方式をサポートする電話機は、設定ファイルの暗号化設定フラグを使用して、暗号化されたファイルと暗号化されていないファイルのどちらを要求するかを決定します。[TFTP 暗号化 (TFTP Encrypted Config)] 設定が無効の場合、この暗号化方式をサポートする Cisco Unified IP Phone が暗号化されたファイル（.enc.sgn ファイル）を要求すると、Cisco Unified Communications Manager はファイルが見つからないというエラーを電話機に送信します。次に、電話機は、暗号化されていない署名付きファイル（.sgn ファイル）を要求します。

[TFTP 暗号化 (TFTP Encrypted Config)] 設定が有効の場合、何らかの理由で電話機が暗号化されていない設定ファイルを要求すると、TFTP サーバは最小限の設定内容を含む暗号化されていないファイルを提供します。電話機は、最小限の設定を受信した後、エラー状態（鍵の不一致など）を検出でき、CAPF とのセッションを開始して電話機の公開鍵を Cisco Unified Communications Manager データベースと同期させることができます。エラー状態が解消された場合、電話機は次回リセット時に暗号化された設定ファイルを要求します。

サポートされる電話機のモデル

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

電話機モデルとプロトコル	暗号化方式
Cisco Unified IP Phone 7905G または 7912G（SIP のみ）	鍵の手動配布： 暗号化アルゴリズム：RC4 鍵サイズ：256 ビット ファイル署名のサポート：なし
Cisco Unified IP Phone 7940G または 7960G（SIP のみ）	鍵の手動配布： 暗号化アルゴリズム：高度暗号化規格（AES）128 鍵サイズ：128 ビット ファイル署名のサポート：SIP を実行するこれらの電話機は、署名付きで暗号化された設定ファイルを受信するが、署名情報を無視
Cisco Unified IP Phone 7970G、7971G、または 7975G Cisco Unified IP Phone 7961G、7962G、または 7965G Cisco Unified IP Phone 7941G、7942G、または 7945G Cisco Unified IP Phone 7911G Cisco Unified IP Phone 7906G Cisco Unified IP Phone 7971G-GE、7961G-GE、7941G-GE Cisco Unified IP Phone 7931G（SCCP のみ）	電話機の公開鍵による対称キーの暗号化（PKI 暗号化）： 暗号化アルゴリズム：AES 128 鍵サイズ：128 ビット ファイル署名のサポート：あり

暗号化された設定ファイルの設定のヒント

[TFTP 暗号化(TFTP Encrypted Config)] フラグを有効にして、電話機がダウンロードする設定ファイル内の機密データを保護することをお勧めします。電話機に PKI 機能が備わっていない場合は、Cisco Unified Communications Manager の管理および電話機で対称キーを設定する必要もあります。[TFTP 暗号化(TFTP Encrypted Config)] フラグが設定されている場合、電話機または Cisco Unified Communications Manager で対称キーが欠落していたり、不一致が発生したりすると、電話機は登録できません。

Cisco Unified Communications Manager の管理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する電話機のセキュリティ プロファイルだけに [TFTP 暗号化(TFTP Encrypted Config)] フラグが表示されます。Cisco Unified IP Phone 7905G、7912G、7940G、および 7960G（SCCP のみ）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ため、これらの電話機に暗号化された設定ファイルを設定することはできません。
- [TFTP 暗号化(TFTP Encrypted Config)] のデフォルト設定は、無効（オフ）です。デフォルトの非セキュア プロファイルを電話機に適用すると、ダイジェスト信用証明書およびセキュア パスワードは暗号化されない状態で送信されます。

- 公開鍵暗号化を使用する Cisco Unified IP Phone の場合、Cisco Unified Communications Manager で、暗号化された設定ファイルを有効にするために、デバイス セキュリティ モードを認証済みまたは暗号化済みに設定する必要はありません。Cisco 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。
- ご使用の環境がセキュアであることがわかっている場合、または PKI が有効でない電話機に対称キーを手動で設定することを避ける場合は、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することもできます。ただし、この方法はお勧めできません。
- Cisco Unified IP Phone 7905G、7912G、7940G、および 7960G（SIP のみ）の場合、Cisco Unified Communications Manager の管理に、ダイジェスト信用証明書を電話機に送信する方式として、暗号化された設定ファイルを使用するよりも簡単であるが安全性の低い方式が用意されています。この方式は、[設定ファイル内のダイジェスト信用証明書を除外(Exclude Digest Credentials in Configuration File)] 設定を使用します。これは、まず対称キーを設定して電話機に入力するという作業が不要であるため、ダイジェスト信用証明書の初期化に便利です。

  この方式では、暗号化されていない設定ファイルで電話機にダイジェスト信用証明書を送信します。電話機でクレデンシャルが受信された後、対応するセキュリティ プロファイル ウィンドウで TFTP ファイルの暗号化設定を無効のままにして、[設定ファイル内のダイジェスト信用証明書を除外(Exclude Digest Credentials in Configuration File)] フラグを有効にすることをお勧めします。これによって、次回以降のダウンロードでダイジェスト信用証明書が除外されます。

  これらの電話機にすでにダイジェスト信用証明書が存在しており、着信ファイルにダイジェスト信用証明書が含まれていない場合、既存のクレデンシャルが所定の場所に残ります。電話機が工場出荷時の設定にリセットされるか、新しいクレデンシャル（ブランクを含む）が受信されるまで、ダイジェスト信用証明書は元の状態のまま残ります。

  電話機ユーザまたはエンド ユーザのダイジェスト信用証明書を変更した場合は、対応するセキュリティ プロファイル ウィンドウでダイジェスト信用証明書を除外するフラグを一時的に無効にして、新しいダイジェスト信用証明書を電話機にダウンロードします。

暗号化設定ファイルの設定用チェックリスト

表 11-1 を使用して、Cisco Unified Communications Manager の管理で暗号化された設定ファイルの設定手順を進めます。

表 11-1　暗号化設定ファイルの設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	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。 **（注）** クラスタ セキュリティ モードは、クラスタまたはスタンドアロン サーバのセキュリティ機能を設定します。	「Cisco CTL クライアントの設定」（P.4-1）
ステップ 2	[電話セキュリティプロファイルの設定(Phone Security Profile Configuration)] で [TFTP 暗号化(TFTP Encrypted Config)] チェックボックスをオンにします。必ず、このプロファイルを電話機に適用します。	• 「暗号化された設定ファイルの設定のヒント」（P.11-4） • 「電話機設定ファイルの暗号化の有効化」（P.11-6） • 「電話機セキュリティ プロファイルの適用」（P.7-10）

表 11-1　暗号化設定ファイルの設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 3	鍵の手動配布をサポートする電話機、および電話機の公開鍵による対称キーの暗号化（PKI 暗号化）をサポートする電話機を確認します。	「サポートされる電話機のモデル」（P.11-4）
ステップ 4	使用中の電話機が鍵の手動配布をサポートする場合は、鍵の手動配布の作業を実行します。	• 「暗号化された設定ファイルの設定のヒント」（P.11-4） • 「鍵の手動配布の設定」（P.11-6） • 「鍵の手動配布の設定内容」（P.11-7）
ステップ 5	使用中の電話機が鍵の手動配布をサポートする場合は、電話機に対称キーを入力し、電話機をリセットします。	「電話機での対称キーの入力」（P.11-8）
ステップ 6	使用中の電話機が、電話機の公開鍵による対称キーの暗号化（PKI 暗号化）をサポートしている場合、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）が電話機に存在することを確認します。	• 「LSC 証明書または MIC 証明書がインストールされていることの確認」（P.11-8） • 「Certificate Authority Proxy Function の使用方法」（P.10-1）

電話機設定ファイルの暗号化の有効化

TFTP サーバは、設定ファイルを構築するときに、データベースに問い合わせます。電話機に適用されている電話機セキュリティ プロファイルで TFTP 暗号化フラグが設定されている場合、TFTP サーバは暗号化された設定ファイルを構築します。

TFTP 暗号化フラグにアクセスするには、「電話機セキュリティ プロファイルの検索」（P.7-3）の説明に従って、電話機の適切なデバイス セキュリティ プロファイルを見つけます。設定ファイルの暗号化を有効にするには、[TFTP 暗号化 (TFTP Encrypted Config)] チェックボックスをオンにします。

追加情報

「関連項目」（P.11-10）を参照してください。

鍵の手動配布の設定

使用中の電話機が鍵の手動配布をサポートしているかどうかを確認するには、「サポートされる電話機のモデル」（P.11-4）を参照してください。

次に述べる手順では、以下の点を前提としています。

- 電話機が Cisco Unified Communications Manager データベースに存在する。
- 互換性のあるファームウェア ロードが TFTP サーバに存在する。
- Cisco Unified Communications Manager の管理で TFTP Encrypted Config パラメータを有効にしている。

手順

ステップ 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、電話機を検索します。

ステップ 2　[電話の設定 (Phone Configuration)] ウィンドウが表示された後、表 11-2 の説明に従って、鍵の手動配布設定を定義します。この設定を行った後は、鍵は変更できません。

ステップ 3　[保存 (Save)] をクリックします。

ステップ 4　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、使用中の電話機モデルをサポートする電話機のアドミニストレーション ガイドを参照してください。

追加情報

「関連項目」（P.11-10）を参照してください。

鍵の手動配布の設定内容

表 11-2 で、[電話の設定 (Phone Configuration)] ウィンドウに表示される手動配布の設定内容について説明します。

- 設定のヒントについては、「暗号化された設定ファイルの設定のヒント」（P.11-4）を参照してください。
- 関連する情報および手順については、「関連項目」（P.11-10）を参照してください。

表 11-2　鍵の手動配布の設定内容

設定	説明
[対称キー (Symmetric Key)]	対称キーとして使用する 16 進文字の文字列を入力します。数字の 0 ～ 9 と、大文字または小文字の英字（A ～ F または a ～ f）を使用できます。 鍵サイズに対応した正しいビットを入力してください。そうでない場合、Cisco Unified Communications Manager は入力された値を拒否します。Cisco Unified Communications Manager は、次の鍵サイズをサポートします。 • Cisco Unified IP Phone 7905G および 7912G（SIP のみ）：256 ビット • Cisco Unified IP Phone 7940G および 7960G（SIP のみ）：128 ビット 鍵を設定した後は、変更できません。
[文字列を生成 (Generate String)]	Cisco Unified Communications Manager の管理ページで 16 進文字列を生成するには、[文字列を生成 (Generate String)] ボタンをクリックします。 鍵を設定した後は、変更できません。
[データベース値を復元 (Revert to Database Value)]	データベースに存在する値に復元する場合は、このボタンをクリックします。

電話機での対称キーの入力

Cisco Unified Communications Manager の管理で鍵の手動配布を設定した後、電話機に対称キーを入力するには、次の手順を実行します。

手順

ステップ 1　電話機の設定ボタンを押します。

ステップ 2　設定がロックされている場合は、[設定] メニューを下方にスクロールし、電話のロック解除を強調表示して [選択] ソフトキーを押します。電話機のパスワードをキー入力し、[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。

ステップ 3　[設定] メニューを下方にスクロールし、[セキュリティ設定] を強調表示し、[選択] ソフトキーを押します。

ステップ 4　[セキュリティ設定] メニューで、[Set Cfg Encrypt Key] オプションを強調表示し、[選択] ソフトキーを押します。

ステップ 5　暗号鍵の入力を要求されたら、鍵（16 進）を入力します。鍵をクリアする必要がある場合、ゼロを 32 回入力します。

ステップ 6　鍵の入力が終了したら、[Accept] ソフトキーを押します。

電話機は暗号鍵を受け入れます。

ステップ 7　電話機をリセットします。

電話機のリセット後、電話機は暗号化された設定ファイルを要求します。

LSC 証明書または MIC 証明書がインストールされていることの確認

この手順は、PKI 暗号化を使用する Cisco Unified IP Phone に適用されます。使用中の電話機が、電話機の公開鍵による対称キーの暗号化（PKI 暗号化）方式をサポートするかどうかを確認するには、「サポートされる電話機のモデル」（P.11-4）を参照してください。

次の手順では、Cisco Unified Communications Manager データベースに電話機が存在し、Cisco Unified Communications Manager の管理で TFTP Encrypted Config パラメータを有効にしたことを前提としています。

手順

ステップ 1　製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が電話機に存在することを確認します。

ヒント　[電話の設定 (Phone Configuration)] ウィンドウの CAPF セクションで [トラブルシューティング (Troubleshoot)] オプションを選択することにより、LSC または MIC が電話機に存在することを Cisco Unified Communications Manager の管理で確認できます。電話機に証明書が存在しない場合、[削除 (Delete)] オプションと [トラブルシューティング (Troubleshoot)] オプションは表示されません。

電話機のセキュリティ設定を調べる方法でも、電話機に LSC または MIC が存在するかどうか確認できます。詳細については、このバージョンの Cisco Unified Communications Manager をサポートする Cisco Unified IP Phone のアドミニストレーション ガイドを参照してください。

ステップ 2　証明書が存在しない場合は、[電話の設定(Phone Configuration)] ウィンドウの CAPF 機能を使用して、LSC をインストールします。LSC をインストールする方法については、「Certificate Authority Proxy Function の使用方法」（P.10-1）を参照してください。

ステップ 3　CAPF 設定を定義した後、[保存(Save)] をクリックします。

ステップ 4　[電話の設定(Phone Configuration)] ウィンドウで、[リセット(Reset)] をクリックします。電話機は、リセット後、暗号化された設定ファイルを TFTP サーバに要求します。

追加情報

「関連項目」（P.11-10）を参照してください。

電話機設定ファイルが暗号化されていることの確認

電話機設定ファイルを暗号化するときは、次の形式が使用されます。

- Cisco Unified IP Phone 7905G および 7912G（SIP のみ）：LD <MAC>.x
- Cisco Unified IP Phone 7940G および 7960G（SIP のみ）：SIP<MAC>.cnf.enc.sgn
- Cisco Unified IP Phone 7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、および 7975G：SEP<MAC>.cnf.xml.enc.sgn

電話機で設定ファイルにアクセスするには、暗号化をサポートする Cisco Unified IP Phone と今回のリリースの Cisco Unified Communications Manager 用の Cisco Unified IP Phone アドミニストレーション ガイドを参照してください。

電話機設定ファイルの暗号化の無効化

電話機設定ファイルの暗号化を無効にするには、Cisco Unified Communications Manager の管理の電話機セキュリティ プロファイルで [TFTP 暗号化(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。

警告　**SIP を実行する電話機のダイジェスト認証が有効になっていて、TFTP 暗号化設定が無効になっている場合、ダイジェスト信用証明書は暗号化されずに送信されます。**

設定を更新した後、電話機の暗号鍵は Cisco Unified Communications Manager データベースに残ります。

Cisco Unified IP Phone 7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、および 7975G が暗号化されたファイル（.enc.sgn ファイル）を要求している場合、暗号化設定を更新して無効にすると、電話機は暗号化されていない署名付きファイル（.sgn ファイル）を要求します。

Cisco Unified IP Phone 7940G/7960G/7905G/7912G（SIP のみ）が暗号化されたファイルを要求している場合、暗号化設定を更新して無効にしたときは、次に電話機がリセットされたときに暗号化されていない設定ファイルを要求するように、管理者が電話機 GUI で対称キーを削除する必要があります。

ヒント　Cisco Unified IP Phone 7940G および 7960G（SIP のみ）では、電話機 GUI で対称キーとして 32 バイトの 0 を入力して、暗号化を無効にします。Cisco Unified IP Phone 7905G および 7912G（SIP のみ）では、電話機 GUI 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、使用中の電話機モデルをサポートする電話機のアドミニストレーション ガイドを参照してください。

電話機設定ファイルのダウンロードからのダイジェスト信用証明書の除外

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信用証明書を除外するには、電話機に適用されるセキュリティ プロファイルの [設定ファイル内のダイジェスト信用証明書を除外 (Exclude Digest Credentials in Configuration File)] チェックボックスをオンにします。Cisco Unified IP Phone 7905G、7912G、7940G、および 7960G（SIP のみ）だけが、このオプションをサポートしています。

ダイジェスト信用証明書を変更した場合は、このチェックボックスをオフにして、設定ファイルを更新する必要があります。詳細については、「暗号化された設定ファイルの設定のヒント」（P.11-4）を参照してください。

追加情報

「関連項目」（P.11-10）を参照してください。

参考情報

関連項目

- 「電話機設定ファイルの暗号化について」（P.11-1）
- 「サポートされる電話機のモデル」（P.11-4）
- 「暗号化された設定ファイルの設定のヒント」（P.11-4）
- 「暗号化設定ファイルの設定用チェックリスト」（P.11-5）
- 「電話機設定ファイルの暗号化の有効化」（P.11-6）
- 「鍵の手動配布の設定」（P.11-6）
- 「鍵の手動配布の設定内容」（P.11-7）
- 「電話機での対称キーの入力」（P.11-8）
- 「LSC 証明書または MIC 証明書がインストールされていることの確認」（P.11-8）
- 「電話機設定ファイルが暗号化されていることの確認」（P.11-9）
- 「電話機設定ファイルの暗号化の無効化」（P.11-9）
- 「電話機設定ファイルのダウンロードからのダイジェスト信用証明書の除外」（P.11-10）
- 「Certificate Authority Proxy Function の使用方法」（P.10-1）
- 「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）

シスコの関連マニュアル

- 『*Cisco Unified Communications Manager Bulk Administration ガイド*』
- 電話機のモデルおよびプロトコルに対応した Cisco Unified IP Phone アドミニストレーション ガイド

CHAPTER 12

SIP 電話機のダイジェスト認証の設定

電話機のダイジェスト認証を有効にしている場合、Cisco Unified Communications Manager は、SIP を実行するすべての電話機の要求（キープアライブ メッセージ以外）でチャレンジを行います。Cisco Unified Communications Manager は、[エンドユーザの設定(End User Configuration)] ウィンドウで設定されたエンド ユーザのダイジェスト信用証明書を使用して、電話機が提供するクレデンシャルを検証します。

電話機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 ユーザがログインしたときに、Cisco Unified Communications Manager は、[エンドユーザの設定(End User Configuration)] ウィンドウで設定されたエクステンション モビリティ エンド ユーザのダイジェスト信用証明書を使用します。

SIP を実行する電話機でのダイジェスト認証の動作の詳細については、「ダイジェスト認証」（P.1-19）を参照してください。

SIP を実行するシスコ以外の電話機にダイジェスト認証を設定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*』の付録 C を参照してください。

この章は、次の内容で構成されています。

SIP 電話機ダイジェスト認証の設定用チェックリスト

SIP を実行する電話機にダイジェスト認証を設定する作業を表 12-1 で説明します。

表 12-1　SIP 電話機ダイジェスト認証の設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	SIP を実行する電話機のセキュリティ プロファイルを設定します。[ダイジェスト認証を有効化(Enable Digest Authentication)] チェックボックスがオンになっていることを確認します。	「電話機セキュリティ プロファイルの設定」（P.7-1）

表 12-1　SIP 電話機ダイジェスト認証の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 2	SIP を実行する電話機にセキュリティ プロファイルを適用します。	「電話機セキュリティ プロファイルの設定」（P.7-1）
ステップ 3	デフォルト設定を更新する場合は、ダイジェスト認証に関連するサービス パラメータ（SIP Station Realm サービス パラメータなど）を設定します。	「ダイジェスト認証サービス パラメータの設定」（P.12-2）
ステップ 4	[エンドユーザの設定(End User Configuration)] ウィンドウで、ダイジェスト信用証明書を設定します。	• 「[エンドユーザの設定(End User Configuration)] ウィンドウでのダイジェスト信用証明書の設定」（P.12-3） • 「エンド ユーザのダイジェスト信用証明書の設定内容」（P.12-3）
ステップ 5	[電話の設定(Phone Configuration)] ウィンドウで [ダイジェストユーザ(Digest User)] を選択します。 SIP を実行する電話機 Cisco Unified IP Phone 7970G、7971G、7971G-GE、7975G、7961G、7961G-GE、7962G、7965G、7945G、7941G、7941G-GE、7942G、7945G、7911G では、ダイジェスト ユーザを選択すると、電話機設定ファイルにダイジェスト信用証明書が含まれます。	「[電話の設定(Phone Configuration)] ウィンドウでのダイジェスト ユーザの設定」（P.12-4）
ステップ 6	Cisco Unified IP Phone 7940G または 7960G（SIP のみ）では、[エンドユーザの設定(End User Configuration)] ウィンドウで設定したダイジェスト信用証明書を入力します。	電話機で認証名およびパスワードを入力する方法については、このバージョンの Cisco Unified Communications Manager をサポートする『*Cisco Unified IP Phone Administrator Guide*』を参照してください。

ダイジェスト認証サービス パラメータの設定

電話機のチャレンジ用の SIP レルムは、サービス パラメータ SIP Station Realm で設定します。インストール時に、Cisco Unified Communications Manager にはデフォルト設定の「ccmsipline」が含まれています。パラメータの詳細については、[サービスパラメータ設定(Service Parameter Configuration)] ウィンドウに表示されている疑問符またはパラメータ名リンクをクリックします。

ダイジェスト認証サービス パラメータ（SIP Realm Station パラメータなど）を更新するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[システム(System)] > [サービスパラメータ(Service Parameters)] を選択します。

ステップ 2　[サーバ(Server)] ドロップダウン リスト ボックスから、Cisco CallManager サービスをアクティブにしたノードを選択します。

ステップ 3　[サービス(Service)] ドロップダウン リスト ボックスから、Cisco CallManager サービスを選択します。サービス名の横に「Active」と表示されていることを確認します。

ステップ 4　ヘルプの説明に従って、**SIP Realm Station** パラメータを更新します。パラメータのヘルプを表示するには、疑問符またはパラメータ名リンクをクリックします。

ステップ 5　[保存(Save)] をクリックします。

追加情報

「関連項目」（P.12-4）を参照してください。

[エンドユーザの設定 (End User Configuration)] ウィンドウでのダイジェスト信用証明書の設定

次の手順では、Cisco Unified Communications Manager データベースにエンド ユーザが存在することを前提としています。エンド ユーザのダイジェスト信用証明書を設定するには、次の手順を実行します。

手順

ステップ 1　『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の説明に従って、エンド ユーザを検索します。

ステップ 2　目的の [エンドユーザの設定 (End User Configuration)] ウィンドウが表示されたら、表 12-2 の説明に従って、適切な文字列を入力します。

ステップ 3　[保存 (Save)] をクリックします。

ステップ 4　その他のエンド ユーザにダイジェスト信用証明書を設定するには、この手順を繰り返します。

次の作業

[エンドユーザの設定 (End User Configuration)] ウィンドウでダイジェスト信用証明書を設定した後、[電話の設定 (Phone Configuration)] ウィンドウにアクセスして、電話機のダイジェスト ユーザを選択します。

ダイジェスト ユーザを選択した後、Cisco Unified IP Phone 7960G または 7940G（SIP のみ）で、[エンドユーザの設定 (End User Configuration)] ウィンドウから取得したダイジェスト認証信用証明書を入力します。

追加情報

「関連項目」（P.12-4）を参照してください。

エンド ユーザのダイジェスト信用証明書の設定内容

表 12-2 で、Cisco Unified Communications Manager の管理ページの [エンドユーザの設定 (End User Configuration)] ウィンドウに表示されるダイジェスト信用証明書の設定について説明します。関連する手順については、「[電話の設定 (Phone Configuration)] ウィンドウでのダイジェスト ユーザの設定」（P.12-4）を参照してください。

表 12-2　ダイジェスト信用証明書

設定	説明
[ダイジェスト信用証明書 (Digest Credentials)]	英数字文字列を入力します。
[ダイジェスト信用証明書の確認 (Confirm Digest Credentials)]	ダイジェスト信用証明書を正しく入力したことを確認するために、このフィールドにクレデンシャルを入力します。

[電話の設定(Phone Configuration)] ウィンドウでのダイジェスト ユーザの設定

ダイジェスト ユーザを電話機と関連付けるには、次の手順を実行します。

手順

ステップ 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、電話機を検索します。

ステップ 2　目的の [電話の設定(Phone Configuration)] ウィンドウが表示されたら、[ダイジェストユーザ(Digest User)] 設定を見つけて、電話機と関連付けるエンド ユーザを選択します。

ステップ 3　[保存(Save)] をクリックします。

ステップ 4　[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ら、設定を保存し、電話機をリセットします。

追加情報

「関連項目」（P.12-4）を参照してください。

参考情報

関連項目

- 「ダイジェスト認証」（P.1-19）
- 「電話機セキュリティ プロファイルの設定」（P.7-1）
- 「SIP 電話機ダイジェスト認証の設定用チェックリスト」（P.12-1）
- 「ダイジェスト認証サービス パラメータの設定」（P.12-2）
- 「[エンドユーザの設定(End User Configuration)] ウィンドウでのダイジェスト信用証明書の設定」（P.12-3）
- 「エンド ユーザのダイジェスト信用証明書の設定内容」（P.12-3）
- 「[電話の設定(Phone Configuration)] ウィンドウでのダイジェスト ユーザの設定」（P.12-4）

シスコの関連マニュアル

『*Cisco SIP IP Phone Administrator Guide*』

CHAPTER 13

電話機のセキュリティ強化

電話機のセキュリティを強化するには、Cisco Unified Communications Manager の管理ページの [電話の設定 (Phone Configuration)] ウィンドウで作業を実行する必要があります。この章は、次の内容で構成されています。

Gratuitous ARP の無効化

デフォルトで Cisco Unified IP Phone は Gratuitous ARP パケットを受け入れます。デバイスによって使用される Gratuitous ARP パケットは、ネットワーク上にデバイスがあることを宣言します。しかし、攻撃者はこうしたパケットを使用して有効なネットワーク デバイスのスプーフィングを行うことができます。たとえば、攻撃者はデフォルト ルータを宣言するパケットを送信できます。必要に応じて、[電話の設定 (Phone Configuration)] ウィンドウで [Gratuitous ARP] を無効にすることができます。

（注） この機能を無効化しても、電話機はデフォルト ルータを識別することができます。

Web アクセスの無効化

電話機の 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機の内部 Web ページにアクセスできなくなります。電話機の Web ページにアクセスできないと、Cisco 品質レポート ツールなどの機能が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があります。

Web サービスが無効かどうかを判別するため、電話機はサービスの無効 / 有効を示す設定ファイル内のパラメータを解析します。Web サービスが無効であれば、電話機はモニタリング用に HTTP ポート 80 を開かず、電話機の内部 Web ページに対するアクセスをブロックします。

[PC Voice VLAN Access] 設定の無効化

デフォルトで Cisco Unified IP Phone はスイッチ ポート（上流のスイッチを向くポート）で受信したすべてのパケットを PC ポートに転送します。[電話の設定 (Phone Configuration)] ウィンドウで [PC Voice VLAN Access] 設定を無効にすると、ボイス VLAN 機能を使用する PC ポートから受信したパケットは廃棄されます。Cisco Unified IP Phone の各機種で、それぞれ異なる方法でこの機能が使用されています。

- Cisco Unified IP Phone 7940G および 7960G は、PC ポートで送受信される、ボイス VLAN のタグが付いたパケットをすべて廃棄します。
- Cisco Unified IP Phone 7970G は、PC ポートで送受信され、802.1Q タグが含まれる VLAN 上のパケットをすべて廃棄します。
- Cisco Unified IP Phone 7912G はこの機能を実行できません。

[Setting Access] 設定の無効化

デフォルトでは、Cisco Unified IP Phone の設定ボタンを押すと、電話機の設定情報を含むさまざまな情報にアクセスできます。[電話の設定 (Phone Configuration)] ウィンドウで [Setting Access] 設定を無効にすると、電話機で設定ボタンを押したときに通常は表示されるすべてのオプションにアクセスできなくなります。オプションには、[コントラスト (Contrast)]、[呼出音タイプ (Ring Type)]、[ネットワークの設定 (Network Configuration)]、[モデル情報 (Model Information)]、および [ステータス (Status)] 設定があります。

これらの設定は、Cisco Unified Communications Manager の管理で設定を無効にすると、電話機に表示されません。設定を無効にした場合、電話機ユーザは音量ボタンに関連付けられた設定を保存できません。たとえば、ユーザは音量を保存できなくなります。

この設定を無効にすると、電話機の現在のコントラスト、呼出音タイプ、ネットワークの設定、モデル情報、ステータス、および音量の設定が自動的に保存されます。これらの電話機設定を変更するには、Cisco Unified Communications Manager の管理で [Setting Access] 設定を有効にする必要があります。

[PC Port] 設定の無効化

デフォルトで Cisco Unified Communications Manager は PC ポートのあるすべての Cisco Unified IP Phone 上で PC ポートを有効にします。必要に応じて、[電話の設定 (Phone Configuration)] ウィンドウで [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、ロビーや会議室の電話機で役立ちます。

電話機設定のセキュリティ強化

注意　次の手順を実行すると、電話機の機能が無効になります。

電話機の機能を無効にするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[デバイス (Device)] > [電話 (Phone)] の順に選択します。

ステップ 2　電話機の検索対象を指定して [検索 (Find)] をクリックするか、電話機すべてのリストを表示するために [検索 (Find)] をクリックします。

ステップ 3　デバイス名をクリックして、デバイスの [電話の設定 (Phone Configuration)] ウィンドウを開きます。

ステップ 4　次の製品固有のパラメータを探します。

- PC Port
- Settings Access
- Gratuitous ARP
- PC Voice VLAN Access
- Web Access

ヒント　これらの設定に関する情報を確認するには、[電話の設定 (Phone Configuration)] ウィンドウでパラメータの横に表示されている疑問符をクリックします。

ステップ 5　無効にする各パラメータのドロップダウン リスト ボックスから、[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。

ステップ 6　[保存 (Save)] をクリックします。

ステップ 7　[リセット (Reset)] をクリックします。

追加情報

詳細については、「関連項目」（P.13-3）を参照してください。

参考情報

関連項目

- 「Gratuitous ARP の無効化」（P.13-1）
- 「Web アクセスの無効化」（P.13-1）
- 「[PC Voice VLAN Access] 設定の無効化」（P.13-2）
- 「[Setting Access] 設定の無効化」（P.13-2）
- 「[PC Port] 設定の無効化」（P.13-2）
- 「電話機設定のセキュリティ強化」（P.13-2）

シスコの関連マニュアル

『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』

CHAPTER 14

セキュアな会議リソースの設定

この章は、次の内容で構成されています。

セキュアな会議の概要

セキュアな会議機能では、会議の安全を確保するための認証と暗号化を提供します。接続されているすべてのデバイスでシグナリングおよびメディアが暗号化されている場合、会議は安全であると見なされます。セキュアな会議機能は、セキュアな TLS または IPSec 接続での SRTP 暗号化をサポートしています。

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 アイコンが用意されています。セキュリティ ステータスは、接続されているデバイスのうち最も低いセキュリティ レベルで決まります。たとえば、2 つの暗号化済み接続と 1 つの認証済み接続を含むセキュアな会議の場合、会議のセキュリティ ステータスは、認証済みになります。

セキュアなアドホック会議とミートミー会議を設定するには、セキュアな会議ブリッジを設定します。

- 認証済みまたは暗号化済みの電話機からユーザが会議コールを開始すると、Cisco Unified Communications Manager はセキュアな会議ブリッジを割り当てます。
- 非セキュアな電話機からユーザがコールを開始すると、Cisco 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、電話機のセキュリティ設定に関わらず、会議は非セキュアになります。

（注）　Cisco Unified Communications Manager は、会議を開始している電話機の Media Resource Group List（MRGL; メディア リソース グループ リスト）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が使用不可である場合、Cisco 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が使用不可である場合、Cisco Unified Communications Manager はセキュアな会議ブリッジを割り当て、会議はセキュアになります。使用可能な会議ブリッジがない場合、コールは失敗します。

ミートミー会議コールの場合、会議を開始する電話機は、ミートミー番号用に設定された最小セキュリティ要件も満たしている必要があります。使用可能なセキュアな会議ブリッジがない場合や開催者のセキュリティ レベルが最小要件を満たしていない場合、Cisco Unified Communications Manager は会議の試行を拒否します。詳細については、「最小セキュリティ レベルでのミートミー会議」（P.14-5）を参照してください。

割り込みを使用する会議の安全を確保するには、暗号化済みモードを使用するよう電話機を設定します。デバイスが認証済みまたは暗号化済みである場合に割り込みキーを押すと、Cisco Unified Communications Manager によって割り込み側と発信先デバイスのビルトイン ブリッジとの間に安全な接続が確立されます。システムは、割り込みコールに接続されているすべての参加者に対して会議のセキュリティ ステータスを示します。

（注）　リリース 8.3 以降を実行している非セキュアまたは認証済みの Cisco Unified IP Phone は、暗号化済みコールに割り込むことができるようになりました。

会議ブリッジの要件

会議ブリッジは、ハードウェア会議ブリッジをネットワークに追加して Cisco Unified Communications Manager の管理でセキュアな会議ブリッジを設定する際に、セキュアなメディア リソースとして登録できます。

（注）　Cisco Unified Communications Manager の処理のパフォーマンスに影響が及ぶため、ソフトウェア会議ブリッジ上のセキュアな会議はサポートされていません。

H.323 または MGCP ゲートウェイで会議を提供する Digital Signal Processor（DSP; デジタル シグナル プロセッサ）ファームは、IP テレフォニー会議のネットワーク リソースとして機能します。会議ブリッジは、セキュアな SCCP クライアントとして Cisco Unified Communications Manager に登録されます。

- 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 Unified Communications Manager 証明書が会議ブリッジの信頼ストア内に存在している必要があります。
- セキュアな会議ブリッジのセキュリティ設定が、登録する Cisco Unified Communications Manager 内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、ご使用のルータに添付されている IOS ルータ マニュアルを参照してください。

Cisco Unified Communications Manager は、会議リソースをコールに動的に割り当てます。使用可能な会議リソースと有効なコーデックで、ルータごとに同時に使用可能なセキュアな会議の最大数が提供されます。送信ストリームと受信ストリームで、参加するエンドポイントごとにキーが個別に生成される（したがって、参加者が会議を離れるときにキーを再生成する必要がない）ので、DSP モジュールに対するセキュアな会議全体の容量は、設定可能な非セキュア容量の半分になります。

詳細については、『*Cisco Unified Communications Manager システム ガイド*』の「会議デバイスの概要」を参照してください。

セキュアな会議のアイコン

Cisco Unified IP Phone は、会議全体のセキュリティ レベルを示す会議セキュリティ アイコンを表示します。電話機のユーザ マニュアルで説明されているように、これらのアイコンは、安全な 2 者間のコールのステータス アイコンと同じです。

コールの音声とビデオ部分は、会議のセキュリティ レベルの基盤となります。音声とビデオの両方の部分が安全である場合に限り、コールは安全であると見なされます。

セキュアなアドホック会議およびミートミー会議の場合、会議のセキュリティ アイコンは、会議参加者の電話機のウィンドウで会議ソフトキーの横に表示されます。表示されるアイコンは、会議ブリッジおよびすべての参加者のセキュリティ レベルによって異なります。

- 会議ブリッジがセキュアですべての会議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すべての会議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いずれかの会議参加者が非セキュアである場合は、コール状態アイコン（アクティブ、保留中など）が表示されるか、旧式の電話機モデルではアイコンが表示されません。

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場合は、デバイスと会議ブリッジの間のメディア ストリームが暗号化されますが、会議のアイコンは、相手側のセキュリティ レベルに応じて、暗号化済み、認証済み、または非セキュアになります。非セキュア ステータスは、参加者のいずれかが非セキュアであるか、または確認できないことを意味します。

ユーザが [割込み] を押すと、[割込み] ソフトキーの横に表示されるアイコンが、割り込み会議のセキュリティ レベルを示します。割り込むデバイスと割り込まれるデバイスが暗号化をサポートしている場合、システムは両デバイス間のメディアを暗号化しますが、割り込み会議のステータスは、接続された参加者のセキュリティ レベルに応じて、非セキュア、認証済み、または暗号化済みになります。

セキュアな会議の保守

会議のステータスは、参加者が加わったときと退席したときに変わります。認証済みまたは非セキュアの参加者がコールに接続すると、暗号化された会議のセキュリティ レベルは認証済みまたは非セキュアに下がる場合があります。同様に、認証済みまたは非セキュアの参加者がコールを切断すると、ステータスは上がる場合があります。非セキュアの参加者が会議コールに接続すると、会議は非セキュアになります。

参加者が会議を結合した場合、結合した会議のセキュリティ ステータスが変わった場合、保留された会議コールが別のデバイスで再開された場合、会議コールに割り込みが入った場合、転送された会議コールが別のデバイスで終了した場合も、会議のステータスが変わる可能性があります。

（注）　Advanced Ad Hoc Conference Enabled サービス パラメータは、会議、参加、直接転送、転送などの機能を使用してアドホック会議を互いにリンクさせることができるかどうかを決定します。

Cisco Unified Communications Manager には、セキュアな会議を保守するため、次のオプションが用意されています。

- 「アドホック会議の会議リスト」（P.14-4）
- 「最小セキュリティ レベルでのミートミー会議」（P.14-5）

アドホック会議の会議リスト

会議リストは、会議コール中に [参加者] ソフトキーが押された場合に、参加者の電話機に表示されます。会議リストは、会議のステータスを示し、また、暗号化されていない参加者を特定するために各参加者のセキュリティ ステータスを示します。

会議リストは、非セキュア、認証済み、暗号化済み、保留中のセキュリティ アイコンを表示します。会議の開始者は、会議リストを使用して、セキュリティ ステータスの低い参加者を退席させることができます。

（注）　Advanced Ad Hoc Conference Enabled サービス パラメータは、会議の開始者以外の参加者が他の参加者を退席させることができるかどうかを決定します。

参加者は、会議に参加すると、会議リストの一番上に追加されます。非セキュアな参加者を [参加者] ソフトキーと [ドロップ] ソフトキーでセキュアな会議から削除する方法は、ご使用の電話機のユーザ マニュアルを参照してください。

次の各項では、セキュアなアドホック会議とその他の機能と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の結合

アドホック会議が別のアドホック会議に結合されると、結合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。Cisco Unified Communications Manager は、会議全体のセキュリティ ステータスを判別するため、結合された会議のセキュリティ レベルを組み込みます。

セキュアなアドホック会議と C 割り込み

ユーザが [C 割込] ソフトキーを押してアクティブな会議に参加すると、Cisco Unified Communications Manager はアドホック会議を作成し、割り込まれる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を割り当てます。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に割り込みがあった場合は、会議リストで割り込み元の横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。割り込み元と会議ブリッジの間のメディアが暗号化済みであっても、割り込み発信者の接続が認証済みであるために、割り込み元のセキュリティ アイコンが認証済みとなる場合もあります。

割り込み元がセキュアでアドホック会議が非セキュアである場合に、アドホック会議のステータスが後からセキュアに変更されると、割り込み発信者のアイコンも更新されます。

セキュアなアドホック会議と参加

認証済みまたは暗号化済みの電話機ユーザは、Cisco Unified IP Phone（SCCP を実行する電話機のみ）の [参加] ソフトキーを使用して、セキュアなアドホック会議を作成またはそれに参加することができます。ユーザが [参加] 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、Cisco Unified Communications Manager は会議のステータスを「不明」にダウングレードします。[参加] を使用して新規メンバーを追加した参加者は、会議の開始者になり、新規メンバーやその他の参加者を会議リストから退席させることができます（Advanced Ad Hoc Conference Enabled 設定が有効になっている場合）。

セキュアなアドホック会議と保留 / 復帰

会議の開始者が参加者を追加するため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（非セキュア）になります。新規参加者が応答すると、会議リストで会議のステータスが更新されます。

シェアドライン上の発信者が保留中の会議コールを別の電話機で復帰する場合は、発信者が [復帰] を押したときに会議リストが更新されます。

最小セキュリティ レベルでのミートミー会議

管理者は、ミートミーのパターンまたは番号を非セキュア、認証済み、または暗号化済みとして設定する際に、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、最小セキュリティ要件を満たしている必要があります。これを満たしていないと、システムは参加者をブロックして、コールを切断します。このアクションは、ミートミー会議コール転送、シェアドラインで復帰されたミートミー会議コール、結合したミートミー会議に適用されます。

ミートミー会議を開始する電話機は、最小セキュリティ レベルを満たしている必要があります。これを満たしていないと、システムは試行を拒否します。最小セキュリティ レベルが認証済みまたは暗号化済みを指定していて、セキュアな会議ブリッジが使用不可である場合、コールは失敗します。

会議ブリッジの最小レベルに非セキュアを指定すると、会議ブリッジはすべてのコールを受け入れ、会議のステータスは非セキュアになります。ミートミー会議の安全を確保する方法は、「ミートミー会議の最小セキュリティ レベルの設定」（P.14-11）を参照してください。

次の各項では、セキュアなミートミー会議とその他の機能との相互作用について説明します。

ミートミー会議とアドホック会議

ミートミー会議をアドホック会議に追加したりアドホック会議をミートミー会議に追加したりするには、アドホック会議がミートミー会議の最小セキュリティ レベルを満たしている必要があります。これを満たしていないと、コールは切断されます。会議が追加されると、会議アイコンが変わります。

ミートミー会議と割り込み

ある発信者がミートミー会議の参加者に割り込んだ場合にその割り込み発信者が最小セキュリティ要件を満たしていないと、割り込まれたデバイスのセキュリティ レベルがダウングレードし、割り込み発信者と割り込まれたコールの両方が切断されます。

ミートミー会議と保留 / 復帰

シェアドラインの電話機は、最小セキュリティ レベルを満たしていない限り、ミートミー会議を復帰できません。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にユーザが [復帰 (Resume)] を押すと、シェアドライン上のすべての電話機がブロックされます。

Cisco Unified IP Phone のサポート

次の Cisco Unified IP Phone は、セキュアな会議とセキュアな会議アイコンをサポートしています。

- Cisco Unified IP Phone 7940G および 7960G（SCCP のみ、認証済みのセキュアな会議のみ）
- Cisco Unified IP Phone 7906G、7911G、および 7931G（SCCP のみ）
- Cisco Unified IP Phone 7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、および 7975G

警告　**セキュアな会議機能をフルに活用するため、暗号化機能をサポートするリリース 8.3 に Cisco Unified IP Phone をアップグレードすることをお勧めします。それより前のリリースを実行している暗号化済みの電話機では、これらの新機能が完全にはサポートされません。これらの電話機では、認証済みまたは非セキュアの参加者としてだけセキュアな会議に参加できます。**

Cisco Unified Communications Manager の以前のリリースとともにリリース 8.3 を実行している Cisco Unified IP Phone では、会議コール中に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ます。また、会議リストなどのセキュアな会議機能はサポートされません。

Cisco Unified IP Phone に当てはまる制限の詳細については、「制限」（P.14-8）を参照してください。

セキュアな会議コールとセキュリティ アイコンの詳細については、ご使用の電話機のユーザ ガイドと、今回の Cisco Unified Communications Manager リリースをサポートする『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』を参照してください。

CTI サポート

Cisco 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、今回のリリースの『*Cisco Unified Communications Manager JTAPI Developers Guide*』および『*Cisco Unified Communications Manager TAPI Developers Guide*』を参照してください。

トランクおよびゲートウェイでのセキュアな会議

Cisco Unified Communications Manager は、クラスタ内トランク（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 以前を実行している暗号化済みの電話機は、ICT および H.323 コールの場合は 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。また、SIP トランク シグナリングは、クラスタ外の参加者へのセキュアな会議通知をサポートしていません。

CDR データ

CDR データは、会議自体のセキュリティ ステータスに加えて、電話機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 ステータスも示します。CDR データベース内では、2 つの値が 2 つの異なるフィールドを使用します。

最小セキュリティ レベル要件を満たしていない参加試行をミートミー会議が拒否した場合、CDR データは終了原因コード 58（ベアラ機能を現在使用できない）を示します。詳細については、『*CDR Analysis and Reporting Administration Guide*』を参照してください。

相互作用および制限

この項では、次のトピックについて取り上げます。

- 「相互作用」（P.14-7）
- 「制限」（P.14-8）

相互作用

この項では、Cisco Unified Communications Manager とセキュアな会議機能との相互作用について説明します。

- 会議の安全を保つため、Suppress MOH to Conference Bridge サービス パラメータが False に設定されている場合でも、セキュアなアドホック会議の参加者がコールを保留にしたりコールをパークしたとき、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わりません。
- クラスタ間環境では、クラスタ外の会議参加者がセキュアなアドホック会議で保留を押すと、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、メディアのステータスが不明に変わります。クラスタ外の参加者が MOH 付きの保留コールを再開すると、会議のステータスは上がります。
- リモート ユーザが保留 / 復帰などの電話機能を起動すると、メディアのステータスが不明に変わり、クラスタ間トランク（ICT）でのセキュアなミートミー コールは消去されます。
- Cisco Unified Communications Manager Multilevel Precedence and Preemption 用のアナンシエータのトーンやアナウンスメントがセキュアなアドホック会議中に参加者の電話機で再生されると、会議のステータスは非セキュアに変わります。
- 発信者がセキュアな SCCP 電話機コールに割り込んだ場合、システムは発信先デバイスで内部トーン再生メカニズムを使用し、会議のステータスはセキュアに保たれます。
- 発信者がセキュアな SIP 電話機コールに割り込んだ場合、システムは保留トーンを再生し、その間、会議のステータスは非セキュアになります。
- 会議がセキュアで RSVP が有効である場合、会議はセキュアに保たれます。
- PSTN を含む会議コールでは、コールの IP ドメイン部分のセキュリティ ステータスだけがセキュリティ会議アイコンで示されます。
- Maximum Call Duration Timer サービス パラメータは、最大会議期間も制御します。
- 会議ブリッジは、パケット キャプチャをサポートします。メディア ストリームが暗号化済みであっても、パケット キャプチャ セッション中、電話機は会議について非セキュア ステータスを示します。
- ご使用のシステムに対して設定されているメディア セキュリティ ポリシーがセキュアな会議の動作を変える場合があります。たとえば、エンドポイントは、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会議コールに参加している場合でも、システムのメディア セキュリティ ポリシーに従ってメディア セキュリティを使用します。

制限

この項では、セキュアな会議機能での Cisco Unified Communications Manager の制限について説明します。

- リリース 8.2 以前を実行している暗号化済みの Cisco Unified IP Phone は、認証済みまたは非セキュアの参加者としてしかセキュアな会議に参加できません。
- Cisco Unified Communications Manager の以前のリリースとともにリリース 8.3 を実行している Cisco Unified IP Phone では、会議コール中に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ます。また、会議リストなどのセキュアな会議機能はサポートされません。
- Cisco Unified IP Phone 7905G および 7911G は会議リストをサポートしていません。
- 帯域幅要件のため、Cisco Unified IP Phone 7940G および 7960G は、アクティブな暗号化済みコールへの暗号化済みデバイスからの割り込みをサポートしません。割り込みを試みると失敗します。
- Cisco Unified IP Phone 7931G は会議の結合をサポートしていません。
- SIP トランクを介して発信している電話機は、そのデバイスのセキュリティ ステータスにかかわらず、非セキュアの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ミートミー会議に参加しようとすると、コールは切断されます。SIP トランクは、SIP を実行する電話機への「認証されていないデバイス」のメッセージの提供をサポートしていないので、電話機はこのメッセージで更新されません。また、SIP を実行する 7960G 電話機も「認証されていないデバイス」のメッセージをサポートしていません。
- クラスタ間では、クラスタ外の参加者に対して会議リストは表示されませんが、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 ステータスは [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が（システムは認証済み接続を非セキュアとして扱います）、暗号化済み接続に対する暗号化アイコンは表示されます。

  クラスタ外の参加者は、クラスタ境界を越えて別のクラスタへ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 通話者間コールとして扱います。

会議リソースのセキュリティを確保するための設定のヒント

セキュアな会議ブリッジのリソースを設定する前に、次の情報を考慮に入れてください。

- セキュアな会議メッセージ用のカスタム 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、Cisco Unified Communications Manager Locale Installer のマニュアルを参照してください。
- 会議またはビルトイン ブリッジは、会議コールの安全を確保するため、暗号化をサポートしている必要があります。
- セキュアな会議ブリッジ登録を有効にするには、クラスタのセキュリティ モードを混合モードに設定します。
- セキュアな会議ブリッジを確立するため、会議を開始する電話機が認証済みまたは暗号化済みであることを確認してください。
- シェアドラインでの会議の整合性を保つため、回線を共有するデバイスを別々のセキュリティ モードで設定することはしないでください。たとえば、暗号化済みの電話機が認証済みまたは非セキュアな電話機と回線を共有するように設定することはしないでください。
- 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 ICT として使用しないでください。

- クラスタのセキュリティ モードを混合モードに設定する場合は、DSP ファーム用に設定されたセキュリティ モード（非セキュアまたは暗号化済み）が Cisco Unified Communications Manager の管理の会議ブリッジのセキュリティ モードと一致している必要があります。一致していないと、会議ブリッジは登録されません。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。
- クラスタのセキュリティ モードを混合モードに設定し、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で会議ブリッジのセキュリティ レベルが非セキュアである場合、Cisco Unified Communications Manager は会議ブリッジの登録を拒否します。
- クラスタのセキュリティ モードを非セキュア モードに設定する場合は、会議ブリッジが登録されるよう、DSP ファームのセキュリティ モードを非セキュアに設定してください。Cisco Unified Communications Manager の管理での設定が暗号化済みであっても、会議ブリッジは非セキュアとして登録されます。
- 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 ファームに Cisco Unified Communications Manager 証明書が含まれ、Cisco Unified Communications Manager に DSP ファーム システムの証明書と DSP 接続の証明書が含まれている必要があります。会議ブリッジが確実に認証に合格するためには、X.509 証明書名に会議ブリッジ名が含まれている必要があります。
- 会議ブリッジの証明書が失効したか、または何らかの理由で変更された場合は、Cisco Unified Communications オペレーティング システムの管理の証明書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 認証は失敗し、会議ブリッジは Cisco Unified Communications Manager に登録できないため機能しません。
- セキュアな会議ブリッジは、ポート 2443 で TLS 接続を介して Cisco Unified Communications Manager に登録されます。非セキュアの会議ブリッジは、ポート 2000 で TCP 接続を介して Cisco Unified Communications Manager に登録されます。
- 会議ブリッジのデバイスのセキュリティ モードを変更するには、Cisco Unified Communications Manager デバイスをリセットして Cisco CallManager サービスを再起動する必要があります。

セキュアな会議ブリッジの設定用チェックリスト

ネットワークにセキュアな会議を追加するときには、表 14-1 を参照してください。

表 14-1　セキュアな会議ブリッジの設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	Cisco CTL クライアントを混合モードでインストールして設定したことを確認します。	「Cisco CTL クライアントの設定」（P.4-1）
ステップ 2	信頼ストアへの Cisco Unified Communications Manager 証明書の追加も含め、Cisco Unified Communications Manager 接続用の DSP ファーム セキュリティを設定したことを確認します。DSP ファームのセキュリティ レベルを暗号化済みに設定します。 **ヒント** DSP ファームは、ポート 2443 で Cisco Unified Communications Manager への TLS ポート接続を確立します。	ご使用の会議ブリッジのマニュアルを参照してください。

表 14-1　セキュアな会議ブリッジの設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 3	DSP ファーム証明書が CallManager 信頼ストア内にあることを確認してください。 証明書を追加するには、Cisco Unified Communications オペレーティング システムの証明書管理機能を使用して DSP 証明書を Cisco Unified Communications Manager 内の信頼ストアにコピーします。 証明書のコピーが終わったら、サーバで Cisco CallManager サービスを再起動します。 **ヒント** 証明書はクラスタ内の各サーバにコピーし、クラスタ内の各サーバで Cisco CallManager サービスを再起動してください。	• 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』 • 『*Cisco Unified Serviceability Administration Guide*』
ステップ 4	Cisco Unified Communications Manager の管理で、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、Cisco 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。	• 「会議リソースのセキュリティを確保するための設定のヒント」（P.14-8） • 「Cisco Unified Communications Manager の管理でのセキュアな会議ブリッジの設定」（P.14-10）
ステップ 5	ミートミー会議の最小セキュリティ レベルを設定します。 **ヒント** 今回のリリースにアップグレードすると、Cisco Unified Communications Manager は自動的に非セキュアな最小セキュリティ レベルをすべてのミートミー パターンに割り当てます。	「ミートミー会議の最小セキュリティ レベルの設定」（P.14-11）
ステップ 6	（オプション）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。 **ヒント** パケット キャプチャ モードをバッチ モードに設定し、キャプチャ層を SRTP に設定します。	「セキュアな会議ブリッジのパケット キャプチャの設定」（P.14-12） 『*Troubleshooting Guide for Cisco Unified Communications Manager*』

Cisco Unified Communications Manager の管理でのセキュアな会議ブリッジの設定

Cisco Unified Communications Manager の管理ページ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。会議ブリッジの暗号化を設定した後、Cisco Unified Communications Manager デバイスをリセットして、Cisco CallManager サービスを再起動する必要があります。

始める前に

デバイス間の接続を安全にするため、Cisco Unified Communications Manager と DSP ファームに証明書をインストールしたことを確認してください。

手順

ステップ 1　[メディアリソース(Media Resources)] > [会議ブリッジ(Conference Bridge)] を選択します。

ステップ 2　[会議ブリッジの検索と一覧表示(Find and List Conference Bridges)] ウィンドウで、Cisco IOS Enhanced Conference Bridge がインストールされていることを確認し、ステップ 4 に進みます。

データベース内にデバイスが存在しない場合は、[新規追加(Add New)] をクリックし、ステップ 3 に進みます。

ステップ 3　[会議ブリッジの設定(Conference Bridge Configuration)] ウィンドウで、[会議ブリッジタイプ(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。『*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、会議ブリッジ名、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を設定します。

ステップ 4　[デバイスセキュリティモード(Device Security Mode)] フィールドで、[Encrypted Conference Bridge] を選択します。

ステップ 5　[保存(Save)] をクリックします。

ステップ 6　[リセット(Reset)] をクリックします。

次の作業

その他の会議ブリッジ設定タスクを実行するため、[関連リンク(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 [移動(Go)] をクリックし、[ミートミー番号の設定(Meet-Me Number Configuration)] ウィンドウまたは [サービスパラメータ設定(Service Parameter Configuration)] ウィンドウに移動します。

追加情報

「関連項目」（P.14-12）を参照してください。

ミートミー会議の最小セキュリティ レベルの設定

ミートミー会議の最小セキュリティ レベルを設定するには、次の手順を実行します。

手順

ステップ 1　[コールルーティング(Call Routing)] > [ミートミー番号/パターン(Meet-Me Number/Pattern)] を選択します。

ステップ 2　[会議ブリッジの検索と一覧表示(Find and List Conference Bridges)] ウィンドウで、ミートミー番号/パターンが設定されていることを確認し、ステップ 4 に進みます。

ミートミー番号/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、ステップ 3 に進みます。

ステップ 3　[ミートミー番号の設定(Meet-Me Number Configuration)] ウィンドウで、[電話番号またはパターン(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。『*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、説明とパーティションの値を設定します。

ステップ 4　[最小セキュリティレベル(Minimum Security Level)] フィールドで、[非セキュア(Non Secure)]、[認証のみ(Authenticated)] または [暗号化(Encrypted)] を選択します。

ステップ 5　[保存(Save)] をクリックします。

次の作業

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、「Cisco Unified Communications Manager の管理でのセキュアな会議ブリッジの設定」（P.14-10）の説明に従って、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。

追加情報

「関連項目」（P.14-12）を参照してください。

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てから、デバイス設定ウィンドウで電話機、ゲートウェイ、またはトランクに対してパケット キャプチャ モードをバッチ モードに設定し、キャプチャ層を SRTP に設定します。詳細については、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

メディア ストリームが暗号化済みであっても、パケット キャプチャ セッション中、電話機は会議について非セキュア ステータスを示します。

参考情報

関連項目

- 「システム要件」（P.1-5）
- 「相互作用および制限」（P.1-7）
- 「証明書」（P.1-15）
- 「設定用チェックリストの概要」（P.1-25）
- 「セキュアな会議の概要」（P.14-1）
- 会議ブリッジの要件
- 「セキュアな会議のアイコン」（P.14-3）
- 「セキュアな会議の保守」（P.14-3）
- 「Cisco Unified IP Phone のサポート」（P.14-6）
- 「CTI サポート」（P.14-6）
- 「トランクおよびゲートウェイでのセキュアな会議」（P.14-6）
- 「相互作用および制限」（P.14-7）
- 「会議リソースのセキュリティを確保するための設定のヒント」（P.14-8）
- 「セキュアな会議ブリッジの設定用チェックリスト」（P.14-9）
- 「Cisco Unified Communications Manager の管理でのセキュアな会議ブリッジの設定」（P.14-10）
- 「ミートミー会議の最小セキュリティ レベルの設定」（P.14-11）
- 「セキュアな会議ブリッジのパケット キャプチャの設定」（P.14-12）

シスコの関連マニュアル

- 『*Cisco Unified Communications Manager システム ガイド*』の「会議ブリッジ」
- 『*Cisco Unified Communications Manager システム ガイド*』の「トランスコーディング、会議、および MTP 用の Cisco DSP リソース」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「会議ブリッジの設定」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「ミートミー番号/パターンの設定」
- 『*Cisco Unified Communications Operating System Administration Guide*』
- 『*Troubleshooting Guide for Cisco Unified Communications Manager*』
- 『*CDR Analysis and Reporting Administration Guide*』
- 『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』
- 今回のリリースの Cisco Unified Communications Manager およびご使用の Cisco Unified IP Phone の Cisco IP Phone ユーザ ガイドおよびリリース ノート

CHAPTER 15

ボイスメール ポートのセキュリティ設定

この章は、次の内容で構成されています。

ボイスメールのセキュリティの概要

Cisco Unified Communications Manager ボイスメール ポートおよび SCCP を実行する Cisco Unity デバイスまたは SCCP を実行する Cisco Unity Connection デバイスにセキュリティを設定するには、ポートに対して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 接続が開始されます。この接続では、相互証明書交換（各デバイスが相手のデバイスの証明書を受け入れる）を使用して、デバイスが認証されます。暗号化済みのボイスメール ポートを選択すると、システムはまずデバイスを認証してから、デバイス間で暗号化されたボイス ストリームを送信します。

- Cisco Unity または Cisco Unity Connection 1.2 以前で、デバイス セキュリティ モードが認証済みまたは暗号化済みになっている場合、Cisco Unity Unified CM TSP は、TLS ポートを介して Cisco 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っている場合、Cisco Unity Unified CM TSP は、SCCP ポートを介して Cisco Unified Communications Manager に接続します。
- Cisco Unity Connection 2.0 以降では、TLS ポートを介して Cisco 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っている場合、Cisco Unity Connection は、SCCP ポートを介して Cisco Unified Communications Manager に接続します。

（注） この章では、「サーバ」という用語は Cisco Unified Communications Manager サーバを意味します。「ボイスメール サーバ」という用語は Cisco Unity サーバまたは Cisco Unity Connection サーバを意味します。

ボイスメール 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、次の点を考慮してください。

- Cisco Unity 4.0(5) 以降とこのバージョンの Cisco Unified Communications Manager を実行する必要があります。
- Cisco Unity Connection 1.2 以降とこのバージョンの Cisco Unified Communications Manager を実行する必要があります。
- Cisco Unity の場合、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 の場合、Cisco Unity Connection の管理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 または Cisco Unity Connection 用の、該当する Cisco Unified Communications Manager インテグレーション ガイドを参照してください。
- この章で説明する手順に加えて、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、Cisco Unity 証明書を信頼ストアに保存する必要があります。この作業の実行の詳細については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

  証明書をコピーした後、クラスタ内の各 Cisco Unified Communications Manager サーバで Cisco CallManager サービスを再起動する必要があります。
- Cisco Unity 証明書が失効したか、または何らかの理由で変更された場合は、Cisco Unified Communications オペレーティング システムの管理の証明書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 認証は失敗し、ボイスメールは Cisco Unified Communications Manager に登録できないため機能しません。
- ボイスメール サーバのポートを設定する場合は、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 の管理で指定する設定は、Cisco Unified Communications Manager の管理で設定されているボイスメール ポートのデバイス セキュリティ モードと一致している必要があります。Cisco Unity Connection の管理の [ボイスメールポートの設定 (Voice Mail Port Configuration)] ウィンドウ（または ボイスメール ポート ウィザード）で、ボイスメール 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場合は、ボイスメール サーバのポートが Cisco Unified Communications Manager に登録できず、ボイスメール サーバはそれらのポートでコールを受け入れることができません。

- ポートのセキュリティ プロファイルを変更するには、Cisco Unified Communications Manager デバイスをリセットしてボイスメール サーバ ソフトウェアを再起動する必要があります。Cisco Unified Communications Manager の管理で、以前のプロファイルと異なるデバイス 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場合は、ボイスメール サーバの設定を変更する必要があります。
- ボイスメール ポート 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 モードが自動的に新規ポートに適用されます。

ボイスメール ポートのセキュリティ設定用チェックリスト

ボイスメール ポートのセキュリティを設定するときには、表 15-1 を参照してください。

表 15-1　ボイスメール ポートのセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	Cisco CTL クライアントを混合モードでインストールして設定したことを確認します。	「Cisco CTL クライアントの設定」（P.4-1）
ステップ 2	電話機に認証または暗号化を設定したことを確認します。	「電話機のセキュリティの概要」（P.6-1） 「電話機セキュリティ プロファイルの設定」（P.7-1）
ステップ 3	Cisco Unified Communications オペレーティング システムの管理の証明書管理機能を使用して、Cisco Unified Communications Manager サーバの信頼ストアに Cisco Unity 証明書をコピーします。次に、Cisco CallManager サービスを再起動します。 **ヒント** クラスタにある各 Cisco 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 Cisco CallManager サービスを再起動します。	• 「ボイスメール セキュリティの設定のヒント」（P.15-2） • 『*Cisco Unified Communications Operating System Administration Guide*』 • 『*Cisco Unified Serviceability Administration Guide*』
ステップ 4	Cisco Unified Communications Manager の管理で、ボイスメール ポートのデバイス セキュリティ モードを設定します。	• 「単一ボイスメール ポートへのセキュリティ プロファイルの適用」（P.15-3） • 「ボイスメール ポート ウィザードでのセキュリティ プロファイルの適用」（P.15-4）
ステップ 5	Cisco Unity または Cisco Unity Connection のボイスメール 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。	Cisco Unity または Cisco Unity Connection 用の Cisco Unified Communications Manager インテグレーション ガイド
ステップ 6	Cisco Unified Communications Manager の管理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。	• Cisco Unity または Cisco Unity Connection 用の Cisco Unified Communications Manager インテグレーション ガイド • 「単一ボイスメール　ポートへのセキュリティ プロファイルの適用」（P.15-3）

単一ボイスメール ポートへのセキュリティ プロファイルの適用

単一のボイスメール ポートにセキュリティ プロファイルを適用するには、次の手順を実行します。

この手順では、デバイスはデータベースに追加済みで、証明書が存在しない場合は証明書が電話機にインストール済みであることを前提としています。セキュリティ プロファイルを初めて適用した後、またはセキュリティ プロファイルを変更した場合、デバイスをリセットする必要があります。

セキュリティ プロファイルを適用する前に、次の項を検討してください。

- 「ボイスメールのセキュリティの概要」（P.15-1）
- 「ボイスメール セキュリティの設定のヒント」（P.15-2）
- 「ボイスメール ポートのセキュリティ設定用チェックリスト」（P.15-3）

手順

ステップ 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、ボイスメール ポートを検索します。

ステップ 2　ポートの設定ウィンドウが表示されたら、[デバイスセキュリティモード(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。このオプションは、データベースで事前定義されています。デフォルト値は [-- 選択されていません --] です。

ステップ 3　[保存(Save)] をクリックします。

ステップ 4　[リセット(Reset)] をクリックします。

追加情報

「関連項目」（P.15-5）を参照してください。

ボイスメール ポート ウィザードでのセキュリティ プロファイルの適用

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方法は、「単一ボイスメール ポートへのセキュリティ プロファイルの適用」（P.15-3）を参照してください。

セキュリティ プロファイルを適用する前に、次の項を検討してください。

- 「ボイスメールのセキュリティの概要」（P.15-1）
- 「ボイスメール セキュリティの設定のヒント」（P.15-2）
- 「ボイスメール ポートのセキュリティ設定用チェックリスト」（P.15-3）

ボイスメール ポート ウィザードで新規ボイスメール サーバにデバイス セキュリティ モードの設定を適用するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[ボイスメール(Voice Mail)] > [Cisco ボイスメールポートウィザード(Cisco Voice Mail Port Wizard)] を選択します。

ステップ 2　ボイスメール サーバの名前を入力し、[次へ(Next)] をクリックします。

ステップ 3　追加するポートの数を選択して、[次へ(Next)] をクリックします。

ステップ 4　[Cisco ボイスメールデバイス情報(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。このオプションは、データベースで事前定義されています。デフォルト値は [-- 選択されていません --] です。

ステップ 5　『*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、その他のデバイス設定を実行します。[次へ(Next)] をクリックします。

ステップ 6　『*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、設定プロセスを続行します。要約ウィンドウが表示されたら、[終了(Finish)] をクリックします。

追加情報

「関連項目」（P.15-5）を参照してください。

参考情報

関連項目

- 「システム要件」（P.1-5）
- 「相互作用および制限」（P.1-7）
- 「証明書」（P.1-15）
- 「設定用チェックリストの概要」（P.1-25）
- 「ボイスメールのセキュリティの概要」（P.15-1）
- 「ボイスメール セキュリティの設定のヒント」（P.15-2）
- 「単一ボイスメール ポートへのセキュリティ プロファイルの適用」（P.15-3）
- 「ボイスメール ポート ウィザードでのセキュリティ プロファイルの適用」（P.15-4）

シスコの関連マニュアル

- 今回の Cisco Unified Communications Manager リリースに対応した Cisco Unity または Cisco Unity Connection 用の『*Cisco Unified Communications Manager Integration Guide*』
- 『*Cisco Unified Communications Operating System Administration Guide*』

CHAPTER 16

セキュア コールのモニタリングと録音の設定

この章は、次の内容で構成されています。

セキュア コールのモニタリングと録音の概要

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できます。

- スーパーバイザは、セキュア コールまたは非セキュア コールに対してセキュアなモニタリング セッションを確立できます。
- 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。
- エージェントのデバイスの機能と同じセキュリティ レベルで確立および維持できる場合に限り、モニタリング コールを続行できます。
- エージェントとお客様間の元のコールは、モニタリング コールとは異なる暗号鍵を使用している必要があります。モニタリング セッションでは、スーパーバイザに送信する前に、最初に新しい鍵でエージェントとお客様の混合音声が暗号化されます。

（注） 認証された電話機でのセキュアな録音はサポートされていません。

セキュア コールのモニタリングと録音の設定

セキュア コールのモニタリングと録音を設定するには、次の手順を使用します。

表 16-1　セキュア コールのモニタリングと録音の設定

	手順	注
ステップ 1	エージェントおよびスーパーバイザの電話機にセキュア機能をプロビジョニングします。	「電話機のセキュリティ設定用チェックリスト」（P.6-3）を参照してください。
ステップ 2	次の設定を使用してセキュア SIP トランクを作成します。 • [デバイスセキュリティモード(Device Security Mode)] を [暗号化(Encrypted)] に設定します。 • [送信セキュリティステータス(Transmit Security Status)] チェックボックスをオンにします。 • [SRTP を許可(SRTP Allowed)] チェックボックスをオンにします。 • TLS SIP トランクをレコーダに設定します。	詳細については、「SIP トランク セキュリティ プロファイルの設定」の章を参照してください。
ステップ 3	非セキュアなモニタリングおよび録音の場合と同様に、モニタリングおよび録音を設定します。 • エージェントの電話機にビルトイン ブリッジを設定します。 • エージェントの電話機の DN ページを使用して、[録音オプション(Recording Option)] を設定します（[自動コール録音が有効(Automatic Call Recording Enabled)] または [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)]）。 • レコーダ用のルート パターンを作成します。 • コール録音プロファイルを DN に追加します。 • 必要に応じて、モニタリングと録音のトーンをプロビジョニングします。	詳細な手順については、『*Cisco Unified Communications Manager 機能およびサービス ガイド*』の「モニタリングと録音」の章を参照してください。

PART 3

Cisco Unified IP Phone のバーチャル プライベート ネットワーク

CHAPTER 17

バーチャル プライベート ネットワークの設定

Cisco Unified IP Phone の Cisco VPN クライアントはシスコの他の在宅勤務用製品を補完するもので、お客様が在宅勤務者に関連する問題を解決するのに役立ちます。

- 導入しやすい：すべての設定を CUCM の管理で設定できます。
- 使いやすい：企業内で電話機を設定した後、その電話機を家に持ち帰ってブロードバンド ルータに差し込むだけで、難しい設定メニューを使用せずに即座に接続できます。
- 管理しやすい：電話機は、ファームウェア アップデートおよび設定変更をリモートで受け取ることができます。
- 安全：VPN トンネルは、音声および Cisco Unified IP Phone サービスだけに適用されます。PC ポートに接続されている PC により、VPN クライアント ソフトウェアを使用して専用のトンネルが認証および確立されます。

サポートされるデバイス

Cisco Unified Reporting を使用すると、Cisco Unified IP Phone でサポートされる VPN クライアントを確認できます。Cisco Unified Reporting で、[Unified CM Phone Feature List] をクリックします。[Feature] のプルダウン メニューから [Virtual Private Network Client] を選択します。その機能をサポートしている製品のリストが表示されます。

Cisco Unified Reporting の使用方法の詳細については、『*Cisco Unified Reporting Administration Guide*』を参照してください。

VPN 機能の設定

サポートされている Cisco Unified IP Phone の VPN 機能を設定するには、次に示す手順を実行します。

表 17-1　VPN の設定用チェックリスト

設定手順		注意および関連手順
ステップ 1	VPN ゲートウェイごとに VPN コンセントレータをセットアップします。	設定情報については、次のような VPN コンセントレータのマニュアルを参照してください。 • 『*SSL VPN Client (SVC) on ASA with ASDM Configuration Example*』 http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008071c428.shtml **（注）** ASA ソフトウェアはバージョン 8.0.4 以降である必要があります。また、「AnyConnect Cisco VPN Phone」ライセンスがインストールされている必要があります。 **（注）** ユーザがリモート電話機でファームウェアまたは設定情報をアップグレードする際の長時間にわたる遅延を回避するために、VPN コンセントレータをネットワーク内の TFTP または Cisco Unified Communications Manager サーバの近くにセットアップすることをお勧めします。ネットワークでこのような設定を実現できない場合は、VPN コンセントレータの隣にある代替の TFTP またはロード サーバをセットアップできます。 • 『*SSL VPN Client (WebVPN) on IOS with SDM Configuration Example*』 http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008072aa61.shtml **（注）** IOS ソフトウェアはバージョン 15.1(2)T 以降である必要があります。フィーチャ セット/ライセンス：2900 モデルの場合は「Universal (Data & Security & UC)」、SSL VPN ライセンスがアクティブになっている 2800 モデルの場合は「Advanced Security」。 **（注）** ユーザがリモート電話機でファームウェアまたは設定情報をアップグレードする際の長時間にわたる遅延を回避するために、VPN コンセントレータをネットワーク内の TFTP または Cisco Unified Communications Manager サーバの近くにセットアップすることを推奨します。ネットワークでこのような設定を実現できない場合は、VPN コンセントレータの隣にある代替の TFTP またはロード サーバをセットアップできます。
ステップ 2	VPN コンセントレータの証明書をアップロードします。	第 18 章「VPN ゲートウェイの設定」
ステップ 3	VPN ゲートウェイを設定します。	第 18 章「VPN ゲートウェイの設定」
ステップ 4	VPN　ゲートウェイを使用して VPN グループを作成します。	第 19 章「VPN グループの設定」
ステップ 5	VPN プロファイルを設定します。	第 20 章「VPN プロファイルの設定」

表 17-1　VPN の設定用チェックリスト（続き）

設定手順		注意および関連手順
ステップ 6	VPN グループおよび VPN プロファイルを共通の電話プロファイルに追加します。	Cisco Unified Communications Manager の管理ページで、[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)] の順に選択します。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「共通電話プロファイルの設定」の章を参照してください。 **（注）** VPN プロファイルを共通の電話プロファイルに関連付けていない場合、VPN は [VPN 機能設定(VPN Feature Configuration)] ウィンドウで定義されているデフォルト設定を使用します。
ステップ 7	Cisco Unified IP Phone のファームウェアを、VPN をサポートしているバージョンにアップグレードします。	Cisco VPN クライアントを実行するには、サポートされている Cisco Unified IP Phone でファームウェア リリース 9.0(2) 以降が稼動している必要があります。ファームウェアのアップグレード方法の詳細については、使用している Cisco Unified IP Phone モデルの『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』を参照してください。 **（注）** ファームウェア リリース 9.0(2) にアップグレードする前に、サポートされている Cisco Unified IP Phone でファームウェア リリース 8.4(4) 以降が稼動している必要があります。
ステップ 8	サポートされている Cisco Unified IP Phone を使用して、VPN 接続を確立します。	Cisco Unified IP Phone の設定および VPN 接続の確立の詳細については、使用している Cisco Unified IP Phone モデルの『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』を参照してください。

IOS の設定要件

IP Phone で VPN クライアントの IOS 設定を作成する場合は、次の手順を実行します。

ステップ 1　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。

フィーチャ セット / ライセンス：Universal (Data & Security & UC) for IOS ISR-G2

フィーチャ セット / ライセンス：Advanced Security for IOS ISR

ステップ 2　SSL VPN ライセンスをアクティブにします。

IP Phone での VPN クライアントの IOS の設定

IP Phone で VPN クライアントの IOS を設定するには、次の手順を実行します。

ステップ 1　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. スタティック ルートとデフォルト ルートを設定します。

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

例：

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

ステップ 2　Cisco Unified Communications Manager と IOS に必要な証明書を生成および登録します。

次の証明書を Cisco Unified Communications Manager からインポートする必要があります。

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

これらの Cisco Unified Communications Manager 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 Communications Manager OS の管理 Web ページで次を選択します。

b. [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します（注意 : この場所は、UCM のバージョンによって異なる場合があります）。

c. Cisco_Manufacturing_CA と CAPF の証明書を見つけます。.pem ファイルをダウンロードし、.txt ファイルで保存します。

d. IOS でトラストポイントを作成します。

例：

```
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 行から END 行までコピーし、貼り付けます。他の証明書でこの手順を繰り返します。

e. 次の IOS 自己署名証明書を生成して Cisco Unified Communications Manager に登録するか、または CA からインポートする証明書と置き換えます。

- 自己署名証明書を生成します。

例：

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name> <exportable
-optional>
Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 1024 1024
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

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

  例：

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

- 生成した証明書を Cisco 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 CUCM の証明書の管理にアップロードします。

ステップ 3　AnyConnect を 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、flash にインストールします。

例：

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

ステップ 4　VPN 機能を設定します。設定の参考として、次に示すサンプル IOS 設定を利用できます。

（注）　電話機で証明書とパスワード認証の両方を使用する場合は、電話機の MAC アドレスを持つユーザを作成します。ユーザ名では大文字と小文字が区別されます。次の例を参考にしてください。

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
```

サンプル IOS 設定

IP Phone で VPN クライアントの IOS 設定を独自に行う場合の一般的なガイドラインとして、次に示すサンプル設定を利用できます。設定の各エントリは変更される場合があります。

```
Current configuration : 4648 bytes
!
! Last configuration change at 13:48:28 CDT Fri Mar 19 2010 by test
!
version 15.2
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
no service password-encryption
!
! hostname of the IOS
hostname vpnios
!
boot-start-marker

! Specifying the image to be used by IOS - boot image
boot system flash c2800nm-advsecurityk9-mz.152-1.4.T
```

```
boot-end-marker
!
!
logging buffered 21474836
!
aaa new-model
!
!
 aaa authentication login default local
 aaa authentication login webvpn local
 aaa authorization exec default local
 !
 aaa session-id common
 !
 clock timezone CST -6
 clock summer-time CDT recurring
 !
 crypto pki token default removal timeout 0
 !

! Define trustpoints
 crypto pki trustpoint iosrcdnvpn-cert
  enrollment selfsigned
  serial-number
  subject-name cn=iosrcdnvpn-cert
  revocation-check none
  rsakeypair iosrcdnvpn-key 1024
 !
 crypto pki trustpoint CiscoMfgCert
  enrollment terminal
  revocation-check none
  authorization username subjectname commonname
 !
 crypto pki trustpoint CiscoRootCA
  enrollment terminal
  revocation-check crl
  authorization username subjectname commonname
 !
 !
! Certificates
 crypto pki certificate chain iosrcdnvpn-cert
  certificate self-signed 04
 crypto pki certificate chain CiscoMfgCert
  certificate ca 6A6967B3000000000003
 crypto pki certificate chain CiscoRootCA
  certificate ca 5FF87B282B54DC8D42A315B568C9ADFF
 crypto pki certificate chain test
  certificate ca 00
 dot11 syslog
 ip source-route
 !
 !
 ip cef
 !
 !
 !
 ip domain name nw048b.cisco.com
 no ipv6 cef
 !
 multilink bundle-name authenticated
 !
!
 voice-card 0
 !
```

```
 !
 !
 license udi pid CISCO2821 sn FTX1344AH76
 archive
  log config
   hidekeys
 username admin privilege 15 password 0 vpnios
 username test privilege 15 password 0 adgjm
 username usr+ privilege 15 password 0 adgjm
 username usr# privilege 15 password 0 adgjm
 username test2 privilege 15 password 0 adg+jm
 username CP-7962G-SEP001B0CDB38FE privilege 15 password 0 adgjm
 !
 redundancy
 !
!
!--- Configure interface. Generally one interface to internal network and one outside
 interface GigabitEthernet0/0
  description "outside interface"
  ip address 10.89.79.140 255.255.255.240
  duplex auto
  speed auto
 !
 interface GigabitEthernet0/1
  description "Inside Interface"
  ip address dhcp
  duplex auto
  speed auto
 !
!--- Define IP local address pool
 ip local pool webvpn-pool 10.8.40.200 10.8.40.225
 ip default-gateway 10.89.79.129
 ip forward-protocol nd
 ip http server
 ip http authentication local
 ip http secure-server
 ip http timeout-policy idle 60 life 86400 requests 10000
 !
 !
!--- Define static IP routes
ip route 0.0.0.0 0.0.0.0 10.89.79.129
ip route 10.89.0.0 255.255.0.0 10.8.40.1
 !
 no logging trap
 access-list 23 permit 10.10.10.0 0.0.0.7
!
 control-plane
 !
line con 0
  exec-timeout 15 0
 line aux 0
! telnet access
 line vty 0 4
  exec-timeout 30 0
  privilege level 15
  password vpnios
  transport input telnet
 line vty 5 15
  access-class 23 in
  privilege level 15
  transport input all
 !
 exception data-corruption buffer truncate
 scheduler allocate 20000 1000
```

```
 !

! webvpn gateway configuration
 webvpn gateway VPN_RCDN_IOS
  hostname vpnios
  ip address 10.89.79.140 port 443
! ssl configuration
  ssl encryption aes128-sha1
  ssl trustpoint iosrcdnvpn-cert
  inservice
  !
! webvpn context for User and Password authentication
 webvpn context UserPasswordContext
  title "User-Password authentication"
  ssl authenticate verify all
  !
  !
  policy group UserPasswordGroup
    functions svc-enabled
    hide-url-bar
    timeout idle 3600
    svc address-pool "webvpn-pool"
    svc default-domain "nw048b.cisco.com"
    svc split include 10.89.75.0 255.255.255.0
    svc dns-server primary 64.101.128.56
    svc dtls
  default-group-policy UserPasswordGroup
  gateway VPN_RCDN_IOS domain UserPasswordVPN
  inservice
 !
 !
! webvpn context for Certificate (username pre-filled) and Password authentication
 webvpn context CertPasswordContext
  title "certificate plus password"
  ssl authenticate verify all
  !
  !
  policy group CertPasswordGroup
    functions svc-enabled
    hide-url-bar
    timeout idle 3600
    svc address-pool "webvpn-pool"
    svc default-domain "nw048b.cisco.com"
    svc dns-server primary 64.101.128.56
    svc dtls
  default-group-policy CertPasswordGroup
  gateway VPN_RCDN_IOS domain CertPasswordVPN
  authentication certificate aaa
  username-prefill
  ca trustpoint CiscoMfgCert
  inservice
 !
 !
! webvpn context for certificate only authentication
 webvpn context CertOnlyContext
  title "Certificate only authentication"
  ssl authenticate verify all
  !
  !
  policy group CertOnlyGroup
    functions svc-enabled
    hide-url-bar
    timeout idle 3600
    svc address-pool "webvpn-pool"
```

```
   svc default-domain "nw048b.cisco.com"
   svc dns-server primary 64.101.128.56
   svc dtls
 default-group-policy CertOnlyGroup
 gateway VPN_RCDN_IOS domain CertOnlyVPN
 authentication certificate
 ca trustpoint CiscoMfgCert
 inservice
!
end
```

ASA の設定要件

IP Phone で VPN クライアントの ASA 設定を作成する場合は、次の手順を実行します。

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

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

ステップ 3　ライセンスをアクティブにします。

a. 現行ライセンスの機能を表示します。
show activation-key detail

b. 追加の SSL VPN セッションと Linksys 電話機が有効になっている新しいライセンスについては、http://www.cisco.com/go/license を参照してください。VPN 機能をサポートする場合は、「Any Connect Cisco VPN phone」ライセンスを選択します。

IP Phone での VPN クライアントの ASA の設定

IP Phone で VPN クライアントの ASA を設定するには、次の手順を実行します。

ステップ 1　次のローカル設定を行います。

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. 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
```

c. DNS を設定します。

例：

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

ステップ 2　Cisco Unified Communications Manager と IOS に必要な証明書を生成および登録します。

次の証明書を Cisco Unified Communications Manager からインポートする必要があります。

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

これらの Cisco Unified Communications Manager 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 Communications Manager OS の管理 Web ページで次を選択します。

b. [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します（注意 : この場所は、UCM のバージョンによって異なる場合があります）。

c. Cisco_Manufacturing_CA と CAPF の証明書を見つけます。.pem ファイルをダウンロードし、.txt ファイルで保存します。

d. IOS でトラストポイントを作成します。

例：

```
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 行から END 行までコピーし、貼り付けます。他の証明書でこの手順を繰り返します。

e. 次の IOS 自己署名証明書を生成して Cisco Unified Communications Manager に登録するか、または CA からインポートする証明書と置き換えます。

- 自己署名証明書を生成します。

例：

```
Router> enable
Router# configure terminal
Router(config)#  crypto key generate rsa general-keys label <name> <exportable
-optional>
Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 1024 1024
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

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

例：

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

- 生成した証明書を Cisco 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 CUCM の証明書の管理にアップロードします。

ステップ 3　VPN 機能を設定します。設定の参考として、次に示すサンプル IOS 設定を利用できます。

（注） 電話機で証明書とパスワード認証の両方を使用する場合は、電話機の MAC アドレスを持つユーザを作成します。ユーザ名では大文字と小文字が区別されます。次の例を参考にしてください。

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
username CP-7975G-SEP001AE2BC16CB attributes vpn-group-policy GroupPhoneWebvpn
service-type remote-access
```

サンプル ASA 設定

IP Phone で VPN クライアントの ASA 設定を独自に行う場合の一般的なガイドラインとして、次に示すサンプル設定を利用できます。設定の各エントリは変更される場合があります。

```
ciscoasa(config)# show running-config
: Saved
:

!--- ASA version
ASA Version 8.2(1)
!
!--- Basic local config on ASA
hostname ciscoasa
domain-name nw048b.cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard

!--- Configure interface. Generally one interface to internal network and one outside
!--- Ethernet0/0 is outside interface with security level 0
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 10.89.79.135 255.255.255.0

!--- Ethernet0/1 is inside interface with security level 100
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address dhcp
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
```

```
!
interface Ethernet0/3
 shutdown
 no nameif
 security-level 100
 no ip address
!
interface Management0/0
 shutdown
 nameif management
 security-level 100
 no ip address
 management-only
!

!--- Boot image of ASA
boot system disk0:/asa821-k8.bin
ftp mode passive

!--- Clock settings
clock timezone CST -6
clock summer-time CDT recurring

!--- DNS configuration
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 64.101.128.56
 domain-name nw048b.cisco.com


!--- Enable interface on the same security level so that they can communicate to each
other
same-security-traffic permit inter-interface
!--- Enable communication between hosts connected to same interface
same-security-traffic permit intra-interface
pager lines 24

!--- Logging options
logging enable
logging timestamp
logging console debugging
no logging message 710005
mtu outside 1500
mtu inside 1500
mtu management 1500

!--- Define IP local address pool
ip local pool Webvpn_POOL 10.8.40.150-10.8.40.170 mask 255.255.255.192
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside

!--- ASDM image
asdm image disk0:/asdm-623.bin
no asdm history enable
arp timeout 14400

!--- Static routing
route outside 0.0.0.0 0.0.0.0 10.89.79.129 1
route inside 10.89.0.0 255.255.0.0 10.8.40.1 1
route inside 0.0.0.0 0.0.0.0 10.8.40.1 tunneled

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
```

```
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.1.0 255.255.255.0 inside
http redirect outside 80
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

!--- ASA certs
!--- trustpoints and certificates
crypto ca trustpoint ASA_VPN_Cert
 enrollment self
 keypair ASA_VPN_Cert_key
 crl configure
crypto ca trustpoint CiscoMfgCert
 enrollment terminal
 crl configure
crypto ca trustpoint UCM_CAPF_Cert
 enrollment terminal
 no client-types
 crl configure
crypto ca certificate chain ASA_VPN_Cert
 certificate 02d5054b
  quit

crypto ca certificate chain CiscoMfgCert
 certificate ca 6a6967b3000000000003
  quit

crypto ca certificate chain UCM_CAPF_Cert
 certificate ca 6a6967b3000000000003
  quit
telnet timeout 5
ssh scopy enable
ssh timeout 5
console timeout 0

!--- configure client to send packets with broadcast flag set
dhcp-client broadcast-flag
!--- specifies use of mac-addr for client identifier to outside interface
dhcp-client client-id interface outside
!
tls-proxy maximum-session 200
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

!--- configure ssl
ssl encryption aes128-sha1
ssl trust-point ASA_VPN_Cert
ssl certificate-authentication interface outside port 443

!--- VPN config
!--- Configure webvpn
webvpn
 enable outside
 default-idle-timeout 3600
```

```
 svc image disk0:/anyconnect-win-2.1.0148-k9.pkg 1
 svc enable

!--- Group-policy
group-policy GroupPhoneWebvpn internal
group-policy GroupPhoneWebvpn attributes
 banner none
 vpn-simultaneous-logins 10
 vpn-idle-timeout none
 vpn-session-timeout none
 vpn-tunnel-protocol IPSec svc webvpn
 default-domain value nw048b.cisco.com
 address-pools value Webvpn_POOL
 webvpn
  svc dtls enable
  svc keep-installer installed
  svc keepalive 120
  svc rekey time 4
  svc rekey method new-tunnel
  svc dpd-interval client none
  svc dpd-interval gateway 300
  svc compression deflate
  svc ask none default webvpn

!--- Configure user attributes
username test password S.eA5Qq5kwJqZ3QK encrypted
username test attributes
 vpn-group-policy GroupPhoneWebvpn
 service-type remote-access

!—Configure username with Phone MAC address for certificate+password method
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
username CP-7975G-SEP001AE2BC16CB attributes
 vpn-group-policy GroupPhoneWebvpn
 service-type remote-access

!--- Configure tunnel group for username-password authentication
tunnel-group VPNphone type remote-access
tunnel-group VPNphone general-attributes
 address-pool Webvpn_POOL
 default-group-policy GroupPhoneWebvpn
tunnel-group VPNphone webvpn-attributes
 group-url https://10.89.79.135/VPNphone enable

!--- Configure tunnel group with certificate only authentication
tunnel-group CertOnlyTunnelGroup type remote-access
tunnel-group CertOnlyTunnelGroup general-attributes
 default-group-policy GroupPhoneWebvpn
tunnel-group CertOnlyTunnelGroup webvpn-attributes
 authentication certificate
 group-url https://10.89.79.135/CertOnly enable

!--- Configure tunnel group with certificate + password authentication
tunnel-group CertPassTunnelGroup type remote-access
tunnel-group CertPassTunnelGroup general-attributes
 authorization-server-group LOCAL
 default-group-policy GroupPhoneWebvpn
 username-from-certificate CN
tunnel-group CertPassTunnelGroup webvpn-attributes
 authentication aaa certificate
 pre-fill-username ssl-client
 group-url https://10.89.79.135/CertPass enable

!
```

```
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:cd28d46a4f627ed0fbc82ba7d2fee98e
: end
```

CHAPTER 18

VPN ゲートウェイの設定

VPN ゲートウェイを設定するには、最初に、VPN コンセントレータの証明書をアップロードしてから、VPN ゲートウェイを設定する必要があります。

この章は、次の内容で構成されています。

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 ASA をセットアップする場合は、ASA で証明書を生成することをお勧めします。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、この項の手順を使用して Cisco Unified Communications Manager にアップロードします。Cisco Unified Communications Manager は、証明書を電話と VPN 間の信頼リストに保存します。

ASA は SSL ハンドシェイク中にこの証明書を送信し、Cisco Unified IP Phone 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。

Cisco Unified IP Phone はデフォルトでその Manufacturer Installed Certificate（MIC; 製造元でインストールされる証明書）を送信します。CAPF サービスを設定している場合には、Cisco Unified IP Phone はその Locally Significant Certificate（LSC; ローカルで有効な証明書）を送信します。

デバイス レベルの証明書認証を使用する場合は、Cisco Unified IP Phone が信頼されるように、ルート MIC または CAPF 証明書を ASA にインストールする必要があります。

Cisco Unified Communications オペレーティング システムを使用して、証明書を Cisco Unified Communications Manager にアップロードします。次の手順に従って、VPN コンセントレータの証明書をアップロードします。

手順

ステップ 1 Cisco Unified Communications オペレーティング システムの管理から、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。

[証明書の一覧 (Certificate List)] ウィンドウが表示されます。

ステップ 2 [証明書のアップロード (Upload Certificate)] をクリックします。

[証明書のアップロード (Upload Certificate)] ポップアップ ウィンドウが表示されます。

ステップ 3 [証明書の名前 (Certificate Name)] プルダウン メニューから、[電話と VPN 間の信頼性 (Phone-VPN-trust)] を選択します。

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

ステップ 5　[ファイルのアップロード (Upload File)] をクリックします。

ステップ 6　アップロードするファイルをさらに選択するか、または [閉じる (Close)] をクリックします。

証明書管理の詳細については、『*Cisco Unified Communications Operating System Administration Guide*』の第 6 章「Security」を参照してください。

VPN ゲートウェイの設定

この項は、次の内容で構成されています。

VPN ゲートウェイの検索

VPN ゲートウェイを検索するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[拡張機能 (Advanced Features)] > [VPN] > [VPN ゲートウェイ (VPN Gateway)] の順に選択します。

[VPN ゲートウェイの検索と一覧表示 (Find and List VPN Gateways)] ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

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

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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

（注）　検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3　[検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　表示されたレコード リストから、目的のレコードのリンクをクリックします。

（注）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

VPN ゲートウェイの設定

VPN ゲートウェイを追加、更新、またはコピーするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[拡張機能 (Advanced Features)] > [VPN] > [VPN ゲートウェイ (VPN Gateway)] の順に選択します。

ステップ 2　次の作業のいずれかを実行します。

- 新しいプロファイルを追加するには、検索ウィンドウの [新規追加 (Add New)] をクリックし、ステップ 3 に進みます。
- 既存の VPN ゲートウェイをコピーするには、「VPN ゲートウェイの検索」（P.18-2）の説明に従い、適切なプロファイルを見つけて、コピーする VPN ゲートウェイの横に表示されている [コピー (Copy)] ボタンをクリックし、ステップ 3 に進みます。
- 既存のプロファイルを更新するには、「VPN ゲートウェイの検索」（P.18-2）の説明に従い、適切な VPN ゲートウェイを見つけて、ステップ 3 に進みます。

[新規追加 (Add New)] をクリックすると、各フィールドのデフォルト設定を示し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、設定をコピーした設定ウィンドウが表示されます。

ステップ 3　表 18-1 の説明に従って、適切な設定を入力します。

ステップ 4　[保存 (Save)] をクリックします。

表 18-1　VPN ゲートウェイの設定値

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。

表 18-1　VPN ゲートウェイの設定値（続き）

フィールド	説明
[VPN ゲートウェイの URL(VPN Gateway URL)]	ゲートウェイ内の主要な VPN コンセントレータの URL を入力します。 （注）　VPN コンセントレータに 1 つのグループ URL を設定し、この URL をゲートウェイ URL として使用する必要があります。 設定情報については、次のような VPN コンセントレータのマニュアルを参照してください。 • 『*SSL VPN Client (SVC) on ASA with ASDM Configuration Example*』 http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008071c428.shtml
[この場所の VPN 証明書 (VPN Certificates in this Location)]	上矢印キーおよび下矢印キーを使用して、証明書をゲートウェイに割り当てます。証明書をゲートウェイに割り当てなかった場合、VPN クライアントはそのコンセントレータへの接続に失敗します。 （注）　最大 10 の証明書を 1 つの VPN ゲートウェイに割り当てることができます。また、各ゲートウェイに少なくとも 1 つの証明書を割り当てる必要があります。電話と VPN 間の信頼性権限に関係付けられた証明書だけが、使用可能な VPN 証明書のリストに表示されます。

CHAPTER 19

VPN グループの設定

この章では、VPN グループの作成手順について説明します。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このグループに追加できます。

この章は、次の内容で構成されています。

VPN グループの検索

VPN グループを検索するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、[拡張機能 (Advanced Features)] > [VPN(VPN)] > [VPN グループ (VPN Group)] の順に選択します。

[VPN グループの検索と一覧表示 (Find and List VPN Groups)] ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

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

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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

（注） 検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3 [検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4 表示されたレコード リストから、目的のレコードのリンクをクリックします。

（注）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

VPN グループの設定

VPN グループを追加、更新、またはコピーするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[拡張機能 (Advanced Features)] > [VPN(VPN)] > [VPN グループ (VPN Group)] の順に選択します。

ステップ 2　次の作業のいずれかを実行します。

- 新しいプロファイルを追加するには、検索ウィンドウの [新規追加 (Add New)] をクリックし、ステップ 3 に進みます。
- 既存の VPN グループをコピーするには、「VPN グループの検索」（P.19-1）の説明に従い、適切なプロファイルを見つけて、コピーする VPN グループの横に表示されている [コピー (Copy)] ボタンをクリックし、ステップ 3 に進みます。
- 既存のプロファイルを更新するには、「VPN グループの設定」（P.19-2）の説明に従い、適切な VPN グループを見つけて、ステップ 3 に進みます。

[新規追加 (Add New)] をクリックすると、各フィールドのデフォルト設定を示し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、設定をコピーした設定ウィンドウが表示されます。

ステップ 3　表 19-1 の説明に従って、適切な設定を入力します。

ステップ 4　[保存 (Save)] をクリックします。

表 19-1　VPN グループの設定値

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。

表 19-1　VPN グループの設定値（続き）

フィールド	定義
[使用可能なすべての VPN ゲートウェイ (All Available VPN Gateways)]	スクロールして、使用可能なすべての VPN ゲートウェイを表示します。
[この VPN グループ内で選択されたゲートウェイ (Selected VPN Gateways in this VPN Group)]	上矢印ボタンと下矢印ボタンを使用して、使用可能な VPN ゲートウェイをこの VPN グループに入れたりグループから外したりします。 VPN クライアントで重大なエラーが発生して、特定の VPN ゲートウェイに接続できない場合、VPN クライアントはリスト内の次の VPN ゲートウェイに接続しようとします。 **（注）** 1 つの VPN グループに最大 3 つの VPN ゲートウェイを追加できます。また、VPN グループ内の証明書数は、合計で 10 までです。

CHAPTER 20

VPN プロファイルの設定

この章は、次の内容で構成されています。

VPN プロファイルの概要

[VPN プロファイル (VPN Profile)] ウィンドウを使用して、[共通の電話プロファイルの設定 (Common Phone Profile Configuration)] ウィンドウで Cisco Unified IP Phone に割り当てるプロファイルを作成します。

VPN プロファイルの検索

VPN プロファイルを検索するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、[拡張機能 (Advanced Features)] > [VPN(VPN)] > [VPN プロファイル (VPN Profile)] の順に選択します。

[VPN プロファイルの検索と一覧表示 (Find and List VPN Profiles)] ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

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

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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

（注）　検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3　[検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　表示されたレコード リストから、目的のレコードのリンクをクリックします。

（注）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

VPN プロファイルの設定

VPN プロファイルを追加、更新、またはコピーするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[拡張機能 (Advanced Features)] > [VPN(VPN)] > [VPN プロファイル (VPN Profile)] の順に選択します。

ステップ 2　次の作業のいずれかを実行します。

- 新しいプロファイルを追加するには、検索ウィンドウの [新規追加 (Add New)] をクリックし、ステップ 3 に進みます。
- 既存のプロファイルをコピーするには、「VPN プロファイルの検索」（P.20-1）の説明に従い、適切なプロファイルを見つけて、コピーする VPN プロファイルの横に表示されている [コピー (Copy)] ボタンをクリックし、ステップ 3 に進みます。
- 既存のプロファイルを更新するには、「VPN　プロファイルの検索」（P.20-1）の説明に従い、適切な VPN プロファイルを見つけて、ステップ 3 に進みます。

[新規追加 (Add New)] をクリックすると、各フィールドのデフォルト設定を示し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、設定をコピーした設定ウィンドウが表示されます。

ステップ 3　表 20-1 の説明に従って、適切な設定を入力します。

ステップ 4　[保存 (Save)] をクリックします。

表 20-1　VPN プロファイルの設定値

フィールド	定義
[名前(Name)]	VPN プロファイルの名前を入力します。
[説明(Description)]	VPN プロファイルの説明を入力します。
[自動ネットワーク検出を有効化(Enable Auto Network Detect)]	このチェックボックスをオンにすると、VPN クライアントは、社内ネットワーク外にあることが検出された場合に限り実行できます。 デフォルト：[無効(Disabled)]
[MTU]	Maximum Transmission Unit（MTU; 最大伝送ユニット）のサイズをバイト単位で入力します。 デフォルト：1290 バイト
[接続の失敗(Fail to Connect)]	VPN トンネルの作成中に、ログインまたは接続操作が完了するまで待機する時間を指定します。 デフォルト：30 秒
[ホスト ID チェックを有効化(Enable Host ID Check)]	このチェックボックスがオンの場合、ゲートウェイ証明書の subjectAltName または CN が、VPN クライアントの接続先の URL と一致している必要があります。 デフォルト：[有効(Enabled)]
[クライアント認証方式(Client Authentication Method)]	ドロップダウン リストから、クライアント認証方式を選択します。 • [ユーザーおよびパスワード(User and password)] • [パスワードのみ(Password only)] • [証明書(Certificate)]（LSC または MIC）
[永続的パスワードを有効化(Enable Password Persistence)]	このチェックボックスをオンにすると、ログイン試行の失敗、ユーザによるパスワードの手動でのクリア、または電話機のリセットや電源切断が発生するまで、ユーザ パスワードが電話機に保存されます。

CHAPTER 21

VPN 機能設定

この章では、VPN 機能設定パラメータについて説明します。この章の構成は、次のとおりです。

概要

[VPN 機能設定 (VPN Feature Configuration)] ウィンドウには、VPN プロファイルを共通の電話プロファイルと関連付けていない場合に、システムで使用される VPN 機能の共通設定値が含まれています。VPN プロファイルを共通の電話プロファイル設定の一部として定義している場合、VPN プロファイルは [VPN 機能設定 (VPN Feature Configuration)] の設定よりも優先されます。

VPN 機能設定パラメータ

VPN 機能設定パラメータを編集するには、次の手順に従います。

ステップ 1 Cisco Unified Communications Manager の管理ページで、[拡張機能 (Advanced Features)] > [VPN] > [VPN 機能設定 (VPN Feature Configuration)] の順に選択します。

[VPN 機能設定 (VPN Feature Configuration)] ウィンドウが表示されます。

ステップ 2 表 21-1 に従って、推奨値を受け入れるか、または新しい値を入力します。

ステップ 3 [保存 (Save)] をクリックします。

表 21-1　VPN 機能設定パラメータ

フィールド	デフォルト
[Enable Auto Network Detect]	[True] の場合、VPN クライアントは、社内ネットワーク外にあることが検出された場合に限り実行できます。 デフォルト：[False]
[MTU]	最大伝送ユニットを指定します。 デフォルト：1290 バイト 最小値：256 バイト 最大値：1406 バイト
[Keep Alive]	キープアライブ メッセージを送信する間隔を指定します。 （注）　Cisco Unified Communications Manager で指定した値よりも小さい値（ゼロ以外）を指定した場合、この値は VPN コンセントレータのキープアライブ設定によって上書きされます。 デフォルト：60 秒 最小値：0 最大値：120 秒
[Fail to Connect]	VPN トンネルの作成中に、ログインまたは接続操作が完了するまで待機する時間を指定します。 デフォルト：30 秒 最小値：0 最大値：600 秒
[Client Authentication Method]	ドロップダウン リストから、クライアント認証方式を選択します。 • [User and password] • [Password only] • [Certificate]（LSC または MIC） デフォルト：[User and password]
[Enable Password Persistence]	[True] の場合、ログイン試行の失敗、ユーザによるパスワードの手動でのクリア、または電話機のリセットや電源切断が発生するまで、ユーザ パスワードが電話機に保存されます。 デフォルト：[False]
[Enable Host ID Check]	[True] の場合、ゲートウェイ証明書の subjectAltName または CN が、VPN クライアントの接続先の URL と一致している必要があります。 デフォルト：[True]

PART 4

Cisco CTI、JTAPI、および TAPI アプリケーションのセキュリティ

CHAPTER 22

CTI、JTAPI、および TAPI の認証と暗号化の設定

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について簡単に説明します。また、CTI、TAPI、および JTAPI アプリケーションの認証と暗号化を設定するために、Cisco Unified Communications Manager の管理で実行する必要がある作業についても説明します。

このマニュアルでは、Cisco Unified Communications Manager の管理で使用できる Cisco JTAPI または TSP プラグインのインストール方法や、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は説明していません。同じく、このマニュアルでは、CTI で制御するデバイスまたは回線に制限を設定する方法も説明しません。

この章は、次の内容で構成されています。

CTI、JTAPI、および TAPI アプリケーションの認証について

Cisco 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。

ヒント　次の情報では、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定義したことを前提としています。また、Cisco CTL クライアントでクラスタ 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を前提としています。この章で説明する作業を実行するときに、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 ポートであるポート 2748 で接続されます。

CTIManager および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 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は、TLS ポート、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、Cisco Unified Communications Manager 証明書（インストール時に Cisco 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。Cisco CTL クライアントをインストールして 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。アプリケーションは、CTIManager への接続を試行する前に、TFTP サーバから CTL ファイルをダウンロードします。

JTAPI/TSP クライアントは、初めて CTL ファイルを TFTP サーバからダウンロードするときに CTL ファイルを信頼します。JTAPI/TSP クライアントは CTL ファイルを検証しないため、ダウンロードはセキュアな環境で実行することを強く推奨します。後続の CTL ファイルのダウンロードは、JTAPI/TSP クライアントで確認されます。たとえば、CTL ファイルの更新後、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、ダウンロードした新しい 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、Cisco 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ていると判断された場合、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 ファイルにある古い証明書を使用して、TLS 接続の確立を試行します。CTL ファイルが変更または侵害されている場合、正常に接続できない可能性があります。CTL ファイルのダウンロードに失敗し、複数の TFTP サーバが存在する場合、「Cisco CTL クライアントの設定」（P.4-1）で説明するように、別の TFTP サーバでファイルをダウンロードするように設定できます。JTAPI/TAPI クライアントは、次の条件下では、どのポートにも接続しません。

- 何らかの理由でクライアントが CTL ファイルをダウンロードできない（CTL ファイルが存在しないなど）。
- クライアントに既存の CTL ファイルがない。
- アプリケーション ユーザをセキュア CTI ユーザとして設定した。

CTIManager との認証を行うために、アプリケーションは、Certificate Authority Proxy Function（CAPF）が発行する証明書を使用します。アプリケーションと CTIManager とのすべての接続で TLS を使用するには、アプリケーション PC で実行されるインスタンスごとに一意の証明書が必要です。1 つの証明書ですべてのインスタンスがカバーされるわけではありません。Cisco IP Manager Assistant サービスを実行しているノードに証明書がインストールされるようにするには、表 22-2 の説明に従い、Cisco Unified Communications Manager の管理でそれぞれのアプリケーション 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 の各インスタンスに対して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、Cisco Unified Communications Manager の管理でアプリケーション ユーザまたはエンド ユーザを Standard CTI Secure Connection ユーザ グループに追加する必要があります。ユーザをこのグループに追加し、証明書をインストールすると、アプリケーションはユーザを TLS ポート経由で接続させます。

CTI、JTAPI、および TAPI アプリケーションの暗号化について

ヒント　認証は、暗号化の最小要件です。つまり、認証を設定していない場合、暗号化は使用できません。

Cisco Unified Communications Manager Assistant、Cisco QRT、および Cisco WebDialer は暗号化をサポートしていません。CTIManager サービスに接続する CTI クライアントは、クライアントが音声パケットを送信する場合、暗号化をサポートすることがあります。

アプリケーションと CTIManager の間のメディア ストリームを安全にするには、Cisco Unified Communications Manager の管理でアプリケーション ユーザまたはエンド ユーザを 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 グループにも存在する場合や、クラスタ セキュリティ モードが混合モードと等しい場合、CTIManager はアプリケーションとの TLS 接続を確立し、メディア イベント内でアプリケーションに鍵関連情報を提供します。

（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機能を設定します。

アプリケーションは SRTP 鍵関連情報を記録または格納しませんが、鍵関連情報を使用して RTP ストリームを暗号化し、CTIManager からの SRTP ストリームを復号化します。

何らかの理由でアプリケーションが非セキュア ポートであるポート 2748 に接続した場合、CTIManager は鍵関連情報を送信しません。制限を設定しなかったために CTI/JTAPI/TAPI がデバイスまたはディレクトリ メンバーを監視または制御できない場合、CTIManager は鍵関連情報を送信しません。

ヒント　アプリケーションで SRTP セッション鍵を受信するには、アプリケーション ユーザまたはエンド ユーザが Standard CTI Enabled、Standard CTI Secure Connection、および Standard CTI Allow Reception of SRTP Key Material の 3 つのグループに存在する必要があります。

Cisco Unified Communications Manager は、CTI ポートおよびルート 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、アプリケーションがセキュア コールをサポートするように設定する必要があります。

CTI ポートやルート ポイントは、ダイナミック登録またはスタティック登録で登録されます。ポートやルート ポイントがダイナミック登録を使用する場合、メディア パラメータはコールごとに指定されます。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。CTI ポートやルート ポイントが TLS 接続を介して CTIManager に登録される場合、デバイスは安全に登録されます。このとき、アプリケーションが有効な暗号化アルゴリズムを使用し、相手がセキュアであれば、メディアは SRTP で暗号化されます。

CTI アプリケーションが、すでに確立されているコールの監視を開始するとき、アプリケーションは RTP イベントを受信しません。確立されたコールに対して、CTI アプリケーションは、コールのメディアがセキュアか非セキュアかを定義する DeviceSnapshot イベントを提供します。このイベントには、鍵関連情報は含まれません。

CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要

Certificate Authority Proxy Function（CAPF）は Cisco 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。

- 認証文字列によって JTAPI/TSP クライアントを認証します。
- 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します。
- 証明書を表示およびトラブルシューティングするために取得します。

JTAPI/TSP クライアントが CAPF と相互に作用するとき、クライアントは認証文字列を使用して CAPF を認証します。次に、クライアントは公開鍵と秘密鍵のペアを生成し、署名付きメッセージで公開鍵を CAPF サーバに転送します。秘密鍵はそのまま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。CAPF は、証明書に署名し、その証明書を署名付きメッセージでクライアントに返送します。

[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)] ウィンドウまたは [エンドユーザ CAPF プロファイルの設定 (End User CAPF Profile Configuration)] ウィンドウで設定内容を設定し、それぞれ、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します。次に、Cisco 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 : このプロファイルを使用すると、ローカルで有効な証明書を発行して、アプリケーション ユーザの安全を確保することができます。これによって、CTIManager サービスとアプリケーションの間で TLS 接続が開かれます。

  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 サービスまたはアプリケーションをアクティブにする場合は、サーバのサービスごとに 1 つずつ、合計 2 つのアプリケーション ユーザ CAPF プロファイルを設定する必要があります。

  クラスタ内の 2 つ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は、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：このプロファイルを使用すると、CTI クライアントにローカルで有効な証明書を発行することができます。これによって、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になります。

ヒント　JTAPI クライアントは LSC を Java Key Store 形式で、JTAPI の初期設定ウィンドウで設定したパスに格納します。TSP クライアントは LSC を暗号化形式で、デフォルト ディレクトリまたは設定したパスに格納します。

次の情報は、通信または電源の障害が発生した場合に適用されます。

- 証明書をインストールしているときに通信障害が発生すると、JTAPI クライアントは 30 秒間隔であと 3 回、証明書を取得しようとします。この値は設定することができません。

  TSP クライアントの場合は、再試行回数と再試行タイマーを設定できます。これらの値は、TSP クライアントが一定の時間内に証明書の取得を試行する回数を指定することで設定します。どちらの値も、デフォルトは 0 です。最大 3 回の再試行回数を設定でき、1（1 回だけ再試行）、2、または 3 を指定します。それぞれについて、再試行の時間を 30 秒以下で設定できます。

- 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復帰した後で、証明書のダウンロードを試行します。

CTI、JTAPI、および TAPI アプリケーションに対する CAPF システムの相互作用および要件

CAPF には、次の要件があります。

- アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルを設定する前に、Cisco CTL 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作業を実行したことを確認します。[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウの Cluster Security Mode が 1（混合モード）であることを確認してください。
- CAPF を使用するには、最初のノードで Cisco Certificate Authority Proxy Function サービスをアクティブにする必要があります。
- 同時に多数の証明書が生成されると、コール処理が中断される場合があるため、スケジューリングされたメンテナンス画面で CAPF を使用することを強く推奨します。
- 証明書操作の間、最初のノードが実行中で正しく機能していることを確認します。
- 証明書操作の間、CTI/JTAPI/TAPI アプリケーションが正しく機能していることを確認します。

CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト

表 22-1 に、CTI/JTAPI/TAPI アプリケーションを保護するために実行する作業のリストを示します。

表 22-1　CTI/JTAPI/TAPI のセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	CTI アプリケーションおよびすべての JTAPI/TSP プラグインがインストールされ、実行中であることを確認します。 **ヒント** アプリケーション ユーザは Standard CTI Enabled グループに割り当てます。	• 『*Cisco Unified Communications Manager システム ガイド*』の「コンピュータ テレフォニー統合」 • 『*Cisco JTAPI Installation Guide for Cisco Unified Communications Manager*』 • 『*Cisco TAPI Installation Guide for Cisco Unified Communications Manager*』 • 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』
ステップ 2	次の Cisco 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 ファイルが作成されるように、CTL クライアントがインストールされ、CTL ファイルが実行されていることを確認します。 • 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であることを確認します。 • CAPF サービスがインストールされ、サービスがアクティブであることを確認します。必要に応じて、CAPF サービス パラメータを更新します。 **ヒント** CAPF サービスは、CTL ファイルに CAPF 証明書を組み込むために、Cisco CTL クライアントで実行されている必要があります。電話機で 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、ここでパラメータを更新する必要はありません。 • クラスタ セキュリティ モードが混合モードに設定されていることを確認します（クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します）。 **ヒント** クラスタ セキュリティ モードが混合モードでない場合、CTI/JTAPI/TAPI アプリケーションは CTL ファイルにアクセスできません。	• 「Cisco CTL クライアントの設定」(P.4-1) • 「CAPF サービス パラメータの更新」(P.22-9) • 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』
ステップ 3	CTIManager およびアプリケーションで TLS 接続を使用する場合は、アプリケーション ユーザまたはエンド ユーザを Standard CTI Secure Connection ユーザ グループに追加します。 **ヒント** CTI アプリケーションは、アプリケーション ユーザまたはエンド ユーザに割り当てることができますが、両方に割り当てることはできません。	「セキュリティ関連ユーザ グループへのアプリケーション ユーザとエンド ユーザの追加」(P.22-7)

表 22-1　CTI/JTAPI/TAPI のセキュリティ設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 4	SRTP を使用する場合は、Standard CTI Allow Reception of SRTP Key Material ユーザ グループにアプリケーション ユーザまたはエンド ユーザを追加します。 ユーザはすでに Standard CTI Enabled および Standard CTI Secure Connection ユーザ グループに存在している必要があります。これらの 3 つのグループに存在しないアプリケーション ユーザまたはエンド ユーザは、SRTP セッション鍵を受信できません。 Cisco Unified Communications Manager Assistant、Cisco QRT、および Cisco WebDialer は暗号化をサポートしていません。CTIManager サービスに接続する CTI クライアントは、クライアントが音声パケットを送信する場合、暗号化をサポートすることがあります。	「セキュリティ関連ユーザ グループへのアプリケーション ユーザとエンド ユーザの追加」（P.22-7） 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「権限の設定」
ステップ 5	Cisco Unified Communications Manager の管理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 プロファイルを設定します。	• 「CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要」（P.22-4） • 「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」（P.22-11） • 「アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルの CAPF 設定ウィンドウ」（P.22-12）
ステップ 6	CTI/JTAPI/TAPI アプリケーションの対応するセキュリティ関連パラメータを有効にします。	「JTAPI/TAPI セキュリティ関連サービス パラメータ」（P.22-14）

セキュリティ関連ユーザ グループへのアプリケーション ユーザとエンド 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 Cisco Unified Communications Manager の管理に表示されます。これらのグループは削除できません。

CTIManager へのユーザ接続の安全を確保にするには、アプリケーション ユーザまたはエンド ユーザを Standard CTI Secure Connection ユーザ グループに追加する必要があります。CTI アプリケーションは、アプリケーション ユーザまたはエンド ユーザに割り当て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。

アプリケーションおよび CTIManager でメディア ストリームを保護するには、アプリケーション ユーザまたはエンド ユーザを Standard CTI Allow Reception of SRTP Key Material ユーザ グループに追加する必要があります。

アプリケーション ユーザおよびエンド ユーザが SRTP を使用する前に、そのユーザが Standard CTI Enabled ユーザ グループおよび Standard CTI Secure Connection ユーザ グループに存在している必要があります。これが、TLS の基本設定になります。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、ユーザを Standard CTI Allow Reception of SRTP Key Material ユーザ グ

ループに追加できます。アプリケーションで SRTP セッション鍵を受信するには、アプリケーション ユーザまたはエンド ユーザが Standard CTI Enabled、Standard CTI Secure Connection、および Standard CTI Allow Reception of SRTP Key Material の 3 つのグループに存在する必要があります。

Cisco Unified Communications Manager Assistant、Cisco QRT、および Cisco WebDialer は暗号化をサポートしないため、アプリケーション ユーザである CCMQRTSecureSysUser、IPMASecureSysUser、および WDSecureSysUser を Standard CTI Allow Reception of SRTP Key Material 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。[権限の設定 (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

ステップ 1　Cisco Unified Communications Manager の管理ページで、[ユーザ管理 (User Management)] > [ユーザ グループ (User Groups)] の順に選択します。

ステップ 2　すべてのユーザ グループを表示するには、[検索 (Find)] をクリックします。

ステップ 3　目的に応じて、次のいずれかを実行します。

- アプリケーション ユーザまたはエンド ユーザが Standard CTI Enabled グループに存在することを確認します。
- [Standard CTI Secure Connection] リンクをクリックして、アプリケーション ユーザまたはエンド ユーザを Standard CTI Secure Connection ユーザ グループに追加します。
- [Standard CTI Allow Reception of SRTP Key Material] リンクをクリックして、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 グループに追加します。

ステップ 4　アプリケーション ユーザをグループに追加するには、ステップ 5 ～ステップ 7 を実行します。

ステップ 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)] ボタンをクリックします。

ステップ 6　アプリケーション ユーザを検索するには、検索条件を指定し、[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表示されます。

ステップ 7　グループに追加するアプリケーション ユーザのチェックボックスをオンにして、[選択項目の追加 (Add Selected)] をクリックします。

[ユーザグループの設定 (User Group Configuration)] ウィンドウにユーザが表示されます。

ステップ 8　エンド ユーザをグループに追加するには、ステップ 9 ～ステップ 11 を実行します。

ステップ 9　[グループにエンドユーザを追加 (Add End Users to Group)] ボタンをクリックします。

ステップ 10　エンド ユーザを検索するには、検索条件を指定し、[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表示されます。

ステップ 11　グループに追加するエンド ユーザのチェックボックスをオンにして、[選択項目の追加 (Add Selected)] をクリックします。

[ユーザグループの設定 (User Group Configuration)] ウィンドウにユーザが表示されます。

追加情報

「関連項目」（P.22-15）を参照してください。

Certificate Authority Proxy Function サービスのアクティブ化

Cisco Unified Communications Manager は、Cisco Unified サービスアビリティで Certificate Authority Proxy Function サービスを自動的にはアクティブ化しません。Certificate Authority Proxy Function サービスのアクティブ化については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

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なかった場合は、「CTL ファイルの更新」（P.4-13）の説明に従って 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 に固有の鍵ペアおよび証明書が CAPF によって自動生成されます。CAPF 証明書は Cisco CTL クライアントによってスタンドアロン サーバまたはクラスタ内のすべてのサーバにコピーされ、拡張子 .0 を使用します。CAPF 証明書が存在することを確認するには、Cisco Unified Communications オペレーティング システムの GUI で、CAPF 証明書を表示します。

CAPF サービス パラメータの更新

CAPF サービスのパラメータを設定するウィンドウには、証明書の有効年数、システムによる鍵生成の最大再試行回数、鍵のサイズなどの情報が表示されます。

Cisco Unified Communications Manager の管理で 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 サービスアビリティで Certificate Authority Proxy Function サービスをアクティブ化する必要があります。

ヒント　電話機で 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、ここでサービス パラメータを更新する必要はありません。

CAPF サービス パラメータを更新するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [サービスパラメータ (Service Parameters)] を選択します。

ステップ 2　[サーバ (Server)] ドロップダウン リスト ボックスから、サーバを選択します。

ヒント　クラスタ内の最初のノードを選択する必要があります。

ステップ 3　[サービス (Service)] ドロップダウン リスト ボックスから、Cisco Certificate Authority Proxy Function サービスを選択します。サービス名の横に「Active」と表示されていることを確認します。

ステップ 4　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。

ステップ 5　変更内容を有効にするには、Cisco Unified サービスアビリティで Cisco Certificate Authority Proxy Function サービスを再起動する必要があります。

追加情報

「関連項目」（P.22-15）を参照してください。

アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの検索

アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルを検索するには、次の手順に従います。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、アクセスするプロファイルに応じて、次のオプションのいずれかを選択します。

- [ユーザ管理(User Management)] > [アプリケーションユーザCAPFプロファイル(Application User CAPF Profile)]
- [ユーザ管理(User Management)] > [エンドユーザCAPFプロファイル(End User CAPF Profile)]

検索と一覧表示ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

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

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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

（注）　検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア(Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3　[検索(Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　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）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

追加情報

「関連項目」（P.22-15）を参照してください。

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 アプリケーションのローカルで有効な証明書をインストール、アップグレード、またはトラブルシューティングする場合は、表 22-2 を参照してください。

ヒント　エンド ユーザ CAPF プロファイルを設定する前に、アプリケーション ユーザ CAPF プロファイルを設定することをお勧めします。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで次のいずれかのオプションを選択します。

- [ユーザ管理 (User Management)] > [アプリケーションユーザ CAPF プロファイル (Application User CAPF Profile)]
- [ユーザ管理 (User Management)] > [エンドユーザ CAPF プロファイル (End User CAPF Profile)]

検索と一覧表示ウィンドウが表示されます。

ステップ 2　次のいずれかを実行します。

- 新しい CAPF プロファイルを追加するには、検索ウィンドウで [新規追加 (Add New)] をクリックします（プロファイルを表示してから、[新規追加 (Add New)] 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、各フィールドのデフォルト設定が示されます。
- 既存のプロファイルをコピーするには、「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」（P.22-10）の説明に従って適切なプロファイルを見つけ、[コピー (Copy)] 列内にあるそのレコード用の [コピー (Copy)] ボタンをクリックします（プロファイルを表示してから、[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、表示されたプロファイルからの設定が示されます。
- 既存のエントリを更新するには、「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」（P.22-10）の説明に従い、適切なプロファイルを見つけて表示します。設定ウィンドウが表示され、現在の設定が示されます。

ステップ 3　表 22-2 の説明に従って、適切な設定を入力します。

ステップ 4　[保存 (Save)] をクリックします。

ステップ 5　セキュリティを使用するアプリケーション ユーザおよびエンド ユーザごとに、この手順を繰り返します。

次の作業

[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 を設定する場合は、「JTAPI/TAPI セキュリティ関連サービス パラメータ」（P.22-14）の説明に従って、サービス パラメータを設定する必要があります。

追加情報

「関連項目」（P.22-15）を参照してください。

アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルの CAPF 設定ウィンドウ

表 22-2 に、[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)] ウィンドウでの CAPF 設定を示します。

- 設定のヒントについては、「CTI、JTAPI、および TAPI アプリケーションに対する CAPF システムの相互作用および要件」（P.22-5）を参照してください。
- 関連する情報および手順については、「関連項目」（P.22-15）を参照してください。

表 22-2　アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルの設定内容

設定	説明
[アプリケーションユーザ (Application User)]	ドロップダウン リスト ボックスから、CAPF オペレーション用のアプリケーション ユーザを選択します。これによって、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 プロファイルの設定 (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 ボックスから、CAPF オペレーション用のエンド ユーザを選択します。これによって、設定されたエンド ユーザが表示されます。 この設定は、[アプリケーションユーザ CAPF プロファイルの設定 (Application User CAPF Profile Configuration)] ウィンドウには表示されません。
[インスタンス ID (Instance Id)]	1 ～ 128 字の英数字（a ～ z、A ～ Z、0 ～ 9）を入力します。インスタンス ID は、証明書操作のためユーザを識別します。 1 つのアプリケーションに対して複数の接続（インスタンス）を設定できます。アプリケーションと CTIManager との接続の安全を確保するには、アプリケーション PC（エンド ユーザの場合）またはサーバ（アプリケーション ユーザの場合）で実行されるインスタンスごとに一意の証明書があることを確認します。 このフィールドは、Web サービスおよびアプリケーションをサポートする CAPF Profile Instance ID for Secure Connection to CTIManager サービス パラメータに関係があります。このパラメータにアクセスする方法については、「JTAPI/TAPI セキュリティ関連サービス パラメータ」（P.22-14）を参照してください。
[証明書の操作 (Certificate Operation)]	ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 • [保留中の操作なし (No Pending Operation)]：証明書の操作が発生しないときに表示されます（デフォルトの設定）。 • [インストール / アップグレード (Install/Upgrade)]：アプリケーションのローカルで有効な証明書を新しくインストールするか、あるいは既存の証明書をアップグレードします。

表 22-2　アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルの設定内容（続き）

設定	説明
[認証モード (Authentication Mode)]	証明書のインストールまたはアップグレード操作の認証モードは [認証ストリング (By Authentication String)] です。これは、ユーザまたは管理者が JTAPI/TSP の初期設定ウィンドウで CAPF 認証文字列を入力したときにだけ、ローカルで有効な証明書がインストール、アップグレード、またはトラブルシューティングされることを意味します。
[認証文字列 (Authentication String)]	一意の文字列を手動で入力するか、あるいは [文字列を生成 (Generate String)] ボタンをクリックして文字列を生成します。 文字列は 4 ～ 10 桁にしてください。 ローカルで有効な証明書をインストールまたはアップグレードするには、アプリケーション PC の JTAPI/TSP の初期設定ウィンドウで、管理者が認証文字列を入力する必要があります。この文字列は、1 回だけ使用できます。あるインスタンスに文字列を使用した場合、その文字列をもう一度使用することはできません。
[文字列を生成 (Generate String)]	CAPF で自動的に認証文字列を生成する場合は、このボタンをクリックします。4 ～ 10 桁の認証文字列が [認証文字列 (Authentication String)] フィールドに表示されます。
[キーサイズ (Key Size、ビット)]	ドロップダウン リスト ボックスから、証明書の鍵のサイズを選択します。デフォルト設定値は 1024 です。これ以外のオプションには、512 と 2048 があります。 鍵生成を低いプライオリティで設定すると、アクションの実行中もアプリケーションの機能を利用できます。鍵生成が完了するまで、30 分以上の時間がかかることがあります。 証明書に 2048 ビットの鍵を選択した場合、アプリケーションと Cisco Unified Communications Manager の間で接続を確立するために、60 秒以上の時間がかかることがあります。最高のセキュリティ レベルを使用する場合を除き、2048 ビットの鍵は設定しないでください。
[操作の完了期限(Operation Completes By)]	このフィールドは、すべての証明書操作をサポートし、操作を完了する必要がある期限の日付と時刻を指定します。 表示される値は、最初のノードに適用されます。 この設定は、証明書操作を完了する必要があるデフォルトの日数を指定する CAPF Operation Expires in (days) エンタープライズ パラメータとともに使用します。このパラメータはいつでも更新できます。
[証明書の操作ステータス (Certificate Operation Status)]	このフィールドは、pending、failed、successful など、証明書操作の進行状況を表示します。 このフィールドに表示される情報は変更できません。

アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルの削除

ここでは、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 Cisco Unified Communications Manager データベースから削除する方法を説明します。

始める前に

Cisco Unified Communications Manager の管理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。該当プロファイルを使用しているデバイスを検索するには、セキュリティプロファイルの設定ウィンドウの [関連リンク (Related Links)] ドロップダウン リスト ボックスから [依存関係レコード (Dependency Records)] を選択して、[移動 (Go)] をクリックします。

システムで依存関係レコード機能が有効になっていない場合は、レコードの [依存関係レコード要約 (Dependency Records Summary)] ウィンドウに、依存関係レコードを有効にすると実行できるアクションを示すメッセージが表示されます。また、依存関係レコード機能を使用すると、CPU 使用率が高くなるという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 ガイド*』を参照してください。

手順

ステップ 1　「アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの検索」(P.22-10) の説明に従い、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。

ステップ 2　次の作業のいずれかを実行します。

- 複数のプロファイルを削除するには、検索と一覧表示ウィンドウで、適切なチェックボックスの横に表示されているチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックします。この選択に対するすべての設定可能なレコードを削除するには、[すべてを選択 (Select All)] をクリックしてから [選択項目の削除 (Delete Selected)] をクリックします。
- 単一のプロファイルを削除するには、検索と一覧表示ウィンドウで、適切なプロファイルの横に表示されているチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックします。

ステップ 3　削除操作の確認を要求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、[キャンセル (Cancel)] をクリックして削除操作を取り消します。

追加情報

「関連項目」（P.22-15）を参照してください。

JTAPI/TAPI セキュリティ関連サービス パラメータ

アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを設定した後、Cisco IP Manager Assistant サービスに対して、次のサービス パラメータを設定する必要があります。

- CTIManager Connection Security Flag
- CAPF Profile Instance ID for Secure Connection to CTIManager

サービス パラメータにアクセスするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [サービスパラメータ (Service Parameters)] を選択します。

ステップ 2　[サーバ (Server)] ドロップダウン リスト ボックスから、Cisco IP Manager Assistant サービスがアクティブになっているサーバを選択します。

ステップ 3　[サービス (Service)] ドロップダウン リスト ボックスから、**Cisco IP Manager Assistant** サービスを選択します。

ステップ 4　パラメータが表示されたら、CTIManager Connection Security Flag パラメータおよび CAPF Profile Instance ID for Secure Connection to CTIManager パラメータを見つけます。

ステップ 5　疑問符またはパラメータ名リンクをクリックすると表示されるヘルプの説明に従い、パラメータを更新します。

ステップ 6　[保存 (Save)] をクリックします。

ステップ 7　サービスがアクティブになっているサーバごとに、この手順を繰り返します。

アプリケーション ユーザまたはエンド ユーザに対する証明書操作のステータスの表示

特定のアプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルの設定ウィンドウ（検索と一覧表示ウィンドウではありません）、または JTAPI/TSP の初期設定ウィンドウで、証明書操作のステータスを表示できます。

参考情報

関連項目

- 「Cisco CTL クライアントの設定」（P.4-1）
- 「CTI、JTAPI、および TAPI アプリケーションの認証について」（P.22-2）
- 「CTI、JTAPI、および TAPI アプリケーションの暗号化について」（P.22-3）
- 「CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要」（P.22-4）
- 「CTI、JTAPI、および TAPI アプリケーションに対する CAPF システムの相互作用および要件」（P.22-5）
- 「CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト」（P.22-6）
- 「セキュリティ関連ユーザ グループへのアプリケーション ユーザとエンド ユーザの追加」（P.22-7）
- 「Certificate Authority Proxy Function サービスのアクティブ化」（P.22-9）
- 「CAPF サービス パラメータの更新」（P.22-9）
- 「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」（P.22-10）
- 「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」（P.22-11）
- 「アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルの CAPF 設定ウィンドウ」（P.22-12）

- 「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」（P.22-14）
- 「JTAPI/TAPI セキュリティ関連サービス パラメータ」（P.22-14）
- 「アプリケーション ユーザまたはエンド ユーザに対する証明書操作のステータスの表示」（P.22-15）

シスコの関連マニュアル

- 『*Cisco JTAPI Installation Guide for Cisco Unified Communications Manager*』
- 『*Cisco TAPI Installation Guide for Cisco Unified Communications Manager*』
- 『*Cisco Unified Communications Manager システム ガイド*』の「コンピュータ テレフォニー統合」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』

PART 5

SRST 参照先、トランク、およびゲートウェイのセキュリティ

CHAPTER 23

セキュア SRST（Survivable Remote Site Telephony）参照先の設定

この章は、次の内容で構成されています。

SRST のセキュリティの概要

SRST 対応ゲートウェイは、Cisco Unified Communications Manager がコールを完了できない場合に、制限付きのコール処理タスクを提供します。

セキュア 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。Cisco Unified Communications Manager の管理で SRST 設定作業を実行した後、Cisco 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 SRST 対応ゲートウェイから証明書を取得して、その証明書を Cisco Unified Communications Manager データベースに追加します。

Cisco Unified Communications Manager の管理で従属デバイスをリセットすると、TFTP サーバは SRST 対応ゲートウェイの証明書を電話機の cnf.xml ファイルに追加してファイルを電話機に送信します。これで、保護された電話機は TLS 接続を使用して SRST 対応ゲートウェイと対話します。

ヒント 電話機設定ファイルには、単一の発行者からの証明書だけが含まれます。そのため、HSRP はサポートされません。

SRST のセキュリティ設定のヒント

次の基準が満たされていることを確認します。これらが満たされていると、保護された電話機と SRST 対応ゲートウェイとの間で接続の安全が確保されます。

- SRST 参照先に自己署名証明書が含まれている。
- Cisco CTL クライアントを介して混合モードを設定した。
- 電話機に認証または暗号化を設定した。
- Cisco Unified Communications Manager の管理で SRST 参照先を設定した。
- SRST の設定後に、SRST 対応ゲートウェイおよび従属する電話機をリセットした。

（注） Cisco Unified Communications Manager は、SRST 対応ゲートウェイ向けに、電話機の証明書情報を含む PEM 形式のファイルを提供します。

LSC 認証では、CAPF ルート証明書（CAPF.der）をダウンロードしてください。このルート証明書では、セキュア SRST が 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になっている場合は、Cisco Unified Communications Manager の管理でデバイス セキュリティ モードが認証済みまたは暗号化済みと示されていても、電話機の設定ファイルのデバイス セキュリティ モードは非セキュアのままです。このような場合、電話機は、クラスタ内で SRST 対応ゲートウェイおよび Cisco Unified Communications Manager サーバとの非セキュア接続を試行します。

（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。

- クラスタ セキュリティ モードが非セキュアになっている場合は、デバイス セキュリティ モードや [セキュア SRST(Is SRST Secure?)] チェックボックスなど、セキュリティ関連の設定が無視されます。設定がデータベースから削除されることはありませんが、セキュリティは提供されません。
- 電話機が SRST 対応ゲートウェイへのセキュア接続を試行するのは、クラスタ セキュリティ モードが混合モードで、電話機設定ファイル内のデバイス 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おり、[SRST 参照先の設定 (SRST Reference Configuration)] ウィンドウで [セキュア SRST(Is SRST Secure?)] チェックボックスがオンになっていて、電話機の設定ファイル内に有効な SRST 証明書が存在する場合だけです。
- 前のリリースの Cisco Unified Communications Manager でセキュア SRST 参照先を設定した場合は、アップグレード時にその設定が自動的に移行されます。
- 暗号化済みまたは認証済みモードの電話機が 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 モードに切り替わった場合、これらの電話機は自動的には Cisco Unified Communications Manager にフォールバックされません。SRST ルータの電源を切り、強制的にこれらの電話機を Cisco Unified Communications Manager に再登録する必要があります。電話機が Cisco Unified Communications Manager にフォールバックした後、管理者は SRST の電源を投入でき、フェールオーバーおよびフォールバックが再び自動になります。

SRST のセキュリティ設定用チェックリスト

表 23-1 を使用して、SRST のセキュリティ設定手順を進めます。

表 23-1　SRST のセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	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。すべてを実行すると、デバイスが Cisco Unified Communications Manager およびセキュリティをサポートします。	このバージョンの Cisco Unified Communications Manager をサポートする『*Cisco IOS SRST Version System Administrator Guide*』。これは、次の URL で入手できます。 http://www.cisco.com/univercd/cc/td/doc/product/voice/srst/srst33/srst33ad/index.htm
ステップ 2	Cisco CTL クライアントのインストールおよび設定に必要なすべての作業を実行したことを確認します。	「Cisco CTL クライアントの設定」（P.4-1）
ステップ 3	電話機に証明書が存在することを確認します。	使用中の電話機モデルの Cisco Unified IP Phone マニュアルを参照してください。
ステップ 4	電話機に認証または暗号化を設定したことを確認します。	「電話機セキュリティ プロファイルの適用」（P.7-10）
ステップ 5	SRST 参照先のセキュリティ設定を行います。これには、[デバイスプール設定 (Device Pool Configuration)] ウィンドウで SRST 参照先を有効にする作業も含まれます。	「セキュア SRST 参照先の設定」（P.23-3）
ステップ 6	SRST 対応ゲートウェイと電話機をリセットします。	「セキュア SRST 参照先の設定」（P.23-3）

セキュア SRST 参照先の設定

Cisco Unified Communications Manager の管理で SRST 参照先を追加、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 SRST 参照先の追加：初めて SRST 参照先のセキュリティ設定を行う場合、表 23-2 で説明するすべての項目を設定する必要があります。
- セキュア SRST 参照先の更新：Cisco Unified Communications Manager の管理で 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更新されません。証明書を更新するには、[証明書の更新 (Update Certificate)] ボタンをクリックする必要があります。クリックすると証明書の内容が表示され、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、Cisco Unified Communications Manager は Cisco Unified Communications Manager サーバまたはクラスタ内の各 Cisco Unified Communications Manager サーバで、信頼できるフォルダにある SRST 対応ゲートウェイの証明書を置き換えます。
- セキュア SRST 参照先の削除：セキュア SRST 参照先を削除すると、Cisco Unified Communications Manager データベースおよび電話機の 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 参照先の削除方法は、『*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。

セキュア SRST 参照先を設定するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [SRST] を選択します。

検索と一覧表示ウィンドウが表示されます。

ステップ 2　次のいずれかを実行します。

- 新しい SRST 参照先を追加するには、検索ウィンドウで [新規追加 (Add New)] をクリックします（プロファイルを表示してから、[新規追加 (Add New)] 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、各フィールドのデフォルト設定が示されます。
- 既存の SRST 参照先をコピーするには、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の説明に従って適切な SRST 参照先を見つけ、[コピー (Copy)] 列内にあるそのレコード用の [コピー (Copy)] アイコンをクリックします（プロファイルを表示してから、[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、設定内容が示されます。
- 既存の SRST 参照先を更新するには、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の説明に従って適切な SRST 参照先を見つけます。設定ウィンドウが表示され、現在の設定が示されます。

ステップ 3　表 23-2 の説明に従い、セキュリティ関連の設定を入力します。

その他の SRST 参照先設定内容の説明については、『*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。

ステップ 4　[セキュア SRST(Is SRST Secure?)] 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。

ステップ 5　[保存 (Save)] をクリックします。

ステップ 6　データベース内の SRST 対応ゲートウェイの証明書を更新するには、[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、[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)] をクリックした後にだけ表示されます。

ステップ 7　証明書のフィンガープリントが表示されます。証明書を受け入れるには、[保存 (Save)] をクリックします。

ステップ 8　[閉じる (Close)] をクリックします。

ステップ 9　[SRST 参照先の設定 (SRST Reference Configuration)] ウィンドウで、[リセット (Reset)] をクリックします。

次の作業

[デバイスプール設定 (Device Pool Configuration)] ウィンドウで SRST 参照先が有効になったことを確認します。

追加情報

「関連項目」（P.23-6）を参照してください。

SRST 参照先のセキュリティの設定内容

表 23-2 で、セキュア SRST 参照先に対して Cisco Unified Communications Manager の管理で使用できる設定について説明します。

- 設定のヒントについては、「SRST のセキュリティ設定のヒント」（P.23-2）を参照してください。
- 関連する情報および手順については、「関連項目」（P.23-6）を参照してください。

表 23-2　セキュア SRST 参照先の設定内容

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、このチェックボックスをオンにします。 SRST を設定してゲートウェイおよび従属する電話機をリセットすると、Cisco CTL Provider サービスは SRST 対応ゲートウェイで証明書プロバイダー サービスに認証を受けます。Cisco CTL クライアントは SRST 対応ゲートウェイから証明書を取得して、その証明書を Cisco Unified Communications Manager データベースに格納します。 **ヒント** データベースおよび電話機から SRST 証明書を削除するには、このチェックボックスをオフにして [保存(Save)] をクリックし、従属する電話機をリセットします。
[SRST 証明書プロバイダ ポート(SRST Certificate Provider Port)]	このポートは、SRST 対応ゲートウェイ上で証明書プロバイダー サービスに対する要求を監視します。Cisco Unified Communications Manager はこのポートを使用して SRST 対応ゲートウェイから証明書を取得します。Cisco SRST 証明書プロバイダーのデフォルト ポートは 2445 です。 SRST 対応ゲートウェイ上でこのポートを設定した後、このフィールドにポート番号を入力します。 **ヒント** ポートが現在使用中の場合や、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は、異なるポート番号の設定が必要になることもあります。ポート番号は、1024 ～ 49151 の範囲に存在する必要があります。この範囲外にある場合、「ポート番号に使用できるのは数字だけです」というメッセージが表示されます。
[証明書の更新(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)] をクリックした後にだけ表示されます。 このボタンをクリックすると、Cisco CTL クライアントは Cisco Unified Communications Manager データベースに格納されている既存の 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)。従属する電話機をリセットした後、TFTP サーバは cnf.xml ファイルを（新しい SRST 対応ゲートウェイの証明書とともに）電話機に送信します。

SRST 参照先からのセキュリティの解除

セキュリティ設定後に SRST 参照先を非セキュアにするには、[SRST 参照先の設定(SRST Reference Configuration)] ウィンドウで、[セキュア SRST(Is SRST Secure?)] チェックボックスをオフにします。ゲートウェイ上のクレデンシャル サービスを無効にする必要がある旨のメッセージが表示されます。

SRST 証明書がゲートウェイから削除された場合

SRST 証明書が SRST 対応のゲートウェイから削除された場合は、その SRST 証明書を Cisco Unified Communications Manager データベースと IP Phone から削除する必要があります。

この作業を実行するには、[SRST 参照先の設定(SRST Reference Configuration)] ウィンドウで、[セキュア SRST(Is SRST Secure?)] チェックボックスをオフにして [更新(Update)] をクリックし、[複数のデバイスのリセット(Reset Devices)] をクリックします。

参考情報

関連項目

- 「SRST のセキュリティの概要」（P.23-1）
- 「SRST のセキュリティ設定のヒント」（P.23-2）
- 「SRST のセキュリティ設定用チェックリスト」（P.23-3）
- 「セキュア SRST 参照先の設定」（P.23-3）
- 「SRST 参照先のセキュリティの設定内容」（P.23-5）
- 「SRST 参照先からのセキュリティの解除」（P.23-6）
- 「SRST 証明書がゲートウェイから削除された場合」（P.23-6）

シスコの関連マニュアル

- 『*Cisco IOS SRST System Administrator Guide*』
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』

CHAPTER 24

ゲートウェイおよびトランクの暗号化の設定

この章は、次の内容で構成されています。

Cisco IOS MGCP ゲートウェイの暗号化の概要

Cisco 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。コール設定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判別されます。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。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（およびその逆の）フォールバックは、セキュア デバイスから非セキュア デバイスへの転送、電話会議、トランスコーディング、保留音などで発生する場合があります。

システムが 2 つのデバイス間で暗号化済み SRTP コールを設定すると、Cisco Unified Communications Manager はセキュア コールのためのマスター暗号鍵とソルトを生成し、SRTP ストリームの場合にのみゲートウェイに送信します。ゲートウェイでもサポートされている SRTCP ストリームの場合、Cisco Unified Communications Manager は鍵とソルトを送信しません。これらの鍵は 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。これは、IPSec を使用してセキュリティを設定する必要があります。Cisco 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鍵を暗号化せずに送信します。セッション鍵がセキュア接続を介して送信されるように、IPSec 接続が存在することを確認します。

ヒント　SRTP 用に設定された MGCP ゲートウェイが、認証されたデバイス（SCCP を実行する認証された電話機など）とのコールに関わる場合、Cisco Unified Communications Manager はこのコールを認証済みとして分類するため、電話機にシールド アイコンが表示されます。コールに対してデバイスの SRTP 機能が正常にネゴシエートされると、Cisco Unified Communications Manager は、このコールを暗号化済みとして分類します。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機に接続されている場合、コールが暗号化されていると、電話機にロック アイコンが表示されます。

H.323 ゲートウェイおよび H.323/H.225/H.245 トランクの暗号化の概要

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 オペレーティング システムで IPSec アソシエーションを設定した場合、Cisco Unified Communications Manager に対して認証ができます。Cisco Unified Communications Manager とこれらのデバイスとの間で IPSec アソシエーションを作成する方法については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

H.323、H.225、および H.245 デバイスは暗号鍵を生成します。これらの鍵は、IPSec で保護されたシグナリング パスを介して Cisco Unified Communications Manager に送信されます。Cisco 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、セッション鍵は暗号化されずに送信されます。セッション鍵がセキュア接続を介して送信されるように、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、Cisco Unified Communications Manager の管理のデバイス設定ウィンドウで [SRTP を許可(SRTP Allowed)] チェックボックスをオンにする必要があります。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）、クラスタ間トランク（非ゲートキーパー制御）などのデバイス設定ウィンドウがあります。このチェックボックスをオンにしない場合、Cisco 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した場合、Cisco Unified Communications Manager は、デバイスに対して SRTP が設定されているかどうかに応じて、セキュア コールまたは非セキュア コールを発生させます。

注意　Cisco Unified Communications Manager の管理ページで [SRTP を許可(SRTP Allowed)] チェックボックスをオンにした場合は、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。

Cisco Unified Communications Manager は、IPSec 接続が正しく設定されているかどうかを確認しません。接続が正しく設定されていない場合、セキュリティ関連情報が暗号化されずに送信されることがあります。

セキュア メディア パスまたはセキュア シグナリング パスを確立でき、デバイスが SRTP をサポートする場合、システムは SRTP 接続を使用します。セキュア メディア パスまたはセキュア シグナリング パスを確立できない、または 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（およびその逆の）フォールバックは、セキュア デバイスから非セキュア デバイスへの転送、電話会議、トランスコーディング、保留音などで発生する場合があります。

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、どのデバイスに対しても [メディアターミネーションポイントが必須(Media Termination Point Required)] チェックボックスがオンになっていない場合、Cisco Unified Communications Manager はこのコールをセキュアに分類します。[メディアターミネーションポイントが必須(Media Termination Point Required)] チェックボックスがオンの場合、Cisco 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に分類します。コールに関連する MTP がない場合、デバイスの SRTP 機能によっては、Cisco Unified Communications Manager がそのコールを暗号化済みに分類することがあります。

SRTP が設定されているデバイスでは、デバイスに対する [SRTP を許可(SRTP Allowed)] チェックボックスがオンで、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た場合、Cisco Unified Communications Manager はコールを暗号化済みに分類します。この基準を満たさない場合、Cisco Unified Communications Manager は、コールを非セキュアに分類します。デバイスがセキュリティ アイコンを表示できる電話機に接続されている場合、コールが暗号化されていると、電話機にロック アイコンが表示されます。

Cisco Unified Communications Manager は、トランクまたはゲートウェイによるアウトバウンド FastStart コールを非セキュアに分類します。Cisco Unified Communications Manager の管理ページで、[SRTP を許可(SRTP Allowed)] チェックボックスをオンにした場合、Cisco Unified Communications Manager は [アウトバウンド FastStart を有効にする(Enable Outbound FastStart)] チェックボックスを無効にします。

Cisco 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、共有秘密鍵（Diffie-Hellman 鍵）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通過させることができます。このため、これら 2 つのエンドポイントではセキュア メディア チャネルを確立できます。

H.235 データを通過できるようにするには、次のトランクおよびゲートウェイの設定で [H.235 パススルー使用可能(H.235 Pass Through Allowed)] チェックボックスをオンにします。

- H.225 トランク
- ICT ゲートキーパー制御
- ICT 非ゲートキーパー制御
- H.323 ゲートウェイ

トランクおよびゲートウェイの設定については、『*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。

SIP トランクの暗号化の概要

SIP トランクは、シグナリングとメディア両方についてセキュア コールをサポートできます。シグナリング暗号化は TLS によって、メディア暗号化は SRTP によって提供されます。

トランクに対してシグナリングの暗号化を設定するには、SIP トランク セキュリティ プロファイルを設定するときに、次のオプションを選択します（[システム(System)] > [セキュリティプロファイル(Security Profile)] > [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）。

- [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
- [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
- [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

SIP トランク セキュリティ プロファイルを設定した後、プロファイルをトランクに適用します（[デバイス (Device)] > [トランク (Trunk)] > SIP トランクの設定ウィンドウ）。

トランクに対してメディア暗号化を設定するには、[SRTP を許可 (SRTP Allowed)] チェックボックスをオンにします（同様に [デバイス (Device)] > [トランク (Trunk)] > SIP トランクの設定ウィンドウ）。

注意　この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鍵やその他のセキュリティ関連情報が公開されないようにするために、暗号化された TLS プロファイルを使用することを強く推奨します。非セキュア プロファイルを使用する場合でも SRTP は機能しますが、シグナリングおよびトレースで鍵が公開されます。この場合、Cisco Unified Communications Manager とトランクの接続先の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。

SIP トランク セキュリティ プロファイルの設定の詳細については、「SIP トランク セキュリティ プロファイルの設定」の章を参照してください。

ゲートウェイおよびトランクのセキュリティ設定用チェックリスト

表 24-1 を、Cisco IOS MGCP ゲートウェイでセキュリティを設定する方法について説明しているマニュアル『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』とともに使用してください。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a0080357589.html

表 24-1　MGCP ゲートウェイのセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	Cisco CTL クライアントをインストールし、設定したことを確認します。クラスタ セキュリティ モードが混合モードであることを確認します。	「Cisco CTL クライアントの設定」（P.4-1）
ステップ 2	電話機に暗号化を設定したことを確認します。	「電話機のセキュリティの概要」（P.6-1）
ステップ 3	IPSec を設定します。 **ヒント** ネットワーク インフラストラクチャで IPSec を設定することも、Cisco 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。どちらかの方法で IPSec を設定した場合、もう 1 つの方法を使用する必要はありません。	• 「ネットワーク インフラストラクチャで IPSec を設定する場合の注意事項」（P.24-5） • 「Cisco Unified Communications Manager とゲートウェイまたはトランクとの間で IPSec を設定する場合の注意事項」（P.24-6）
ステップ 4	H.323 IOS ゲートウェイおよびクラスタ間トランクの場合、Cisco Unified Communications Manager の管理ページで [SRTP を許可 (SRTP Allowed)] チェックボックスをオンにします。	[SRTP を許可 (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。

表 24-1　MGCP ゲートウェイのセキュリティ設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 5	SIP トランクの場合、SIP トランク セキュリティ プロファイルを設定し、トランクに適用します（この処理を行っていない場合）。また、[デバイス(Device)] > [トランク(Trunk)] > SIP トランクの設定ウィンドウで、[SRTP を許可(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(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鍵やその他のセキュリティ関連情報が公開されないようにするために、暗号化された TLS プロファイルを使用することを強く推奨します。非セキュア プロファイルを使用する場合でも SRTP は機能しますが、シグナリングおよびトレースで鍵が公開されます。この場合、Cisco Unified Communications Manager とトランクの接続先の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。	• 「SIP トランクの暗号化の概要」（P.24-3） • 「SIP トランク セキュリティ プロファイルの設定」（P.25-3）
ステップ 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。	• 『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』

ネットワーク インフラストラクチャで IPSec を設定する場合の注意事項

このマニュアルでは、IPSec の設定方法は説明しません。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を示します。IPSec をネットワーク インフラストラクチャで設定し、Cisco Unified Communications Manager とデバイスとの間では設定しない場合は、IPSec の設定前に、次のことを検討してください。

- シスコは、Cisco Unified Communications Manager 自体ではなくインフラストラクチャで IPSec をプロビジョニングすることをお勧めします。
- IPSec を設定する前に、既存の IPSec 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、ジッタまたは待ち時間、およびその他のパフォーマンス上のメトリックを考慮してください。
- 『*Voice and Video Enabled IPSec Virtual Private Networks Solution Reference Network Design Guide*』を参照してください。これは、次の URL で入手できます。

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf
- 『*Cisco IOS Security Configuration Guide, Release 12.2*』（またはそれ以降）を参照してください。これは、次の URL で入手できます。

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080087df1.html
- セキュア Cisco IOS MGCP ゲートウェイで接続のリモート エンドを終了します。

- テレフォニー サーバがあるネットワークの信頼されている領域内で、ネットワーク デバイスのホスト エンドを終了します。たとえば、ファイアウォール内のアクセス コントロール リスト（ACL）またはその他のレイヤ 3 デバイスです。
- ホスト エンド IPSec 接続を終了するために使用する装置は、ゲートウェイの数やゲートウェイへの予期されるコール ボリュームによって異なります。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、または Cisco サービス統合型ルータを使用できます。
- 「ゲートウェイおよびトランクのセキュリティ設定用チェックリスト」（P.24-4）に示されている順序どおりに手順を実行してください。

注意　IPSEC 接続を設定して接続がアクティブであることを確認しないと、メディア ストリームの機密性が損なわれる可能性があります。

Cisco Unified Communications Manager とゲートウェイまたはトランクとの間で IPSec を設定する場合の注意事項

この章で説明する Cisco Unified Communications Manager とゲートウェイまたはトランクとの間での IPSec の設定については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

[SRTP を許可 (SRTP Allowed)] チェックボックスの設定

[SRTP を許可 (SRTP Allowed)] チェックボックスは、Cisco Unified Communications Manager の管理の次の設定ウィンドウに表示されます。

- H.323 のゲートウェイ設定ウィンドウ
- H.225 トランク（ゲートキーパー制御）のトランク設定ウィンドウ
- クラスタ間トランク（ゲートキーパー制御）のトランク設定ウィンドウ
- クラスタ間トランク（非ゲートキーパー制御）のトランク設定ウィンドウ
- SIP トランク設定ウィンドウ

H.323 ゲートウェイ、および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 トランクまたは SIP トランクに対して [SRTP を許可 (SRTP Allowed)] チェックボックスを設定するには、次の手順を実行します。

手順

ステップ 1　『*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、ゲートウェイまたはトランクを検索します。

ステップ 2　ゲートウェイまたはトランクの設定ウィンドウが開いたら、[SRTP を許可 (SRTP Allowed)] チェックボックスをオンにします。

注意　SIP トランクに対して [SRTP を許可 (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鍵やその他のセキュリティ関連情報が公開されないようにするために、暗号化された TLS プロファイルを使用することを強く推奨します。非セキュア プロファイルを使用する場合でも SRTP は機能しますが、シグナリングおよびトレースで鍵が公開されます。この場合、Cisco Unified Communications Manager とトランクの接続先の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。

ステップ 3　[保存 (Save)] をクリックします。

ステップ 4　[リセット (Reset)] をクリックして、デバイスをリセットします。

ステップ 5　H323 について IPSec が正しく設定されたことを確認します（SIP については、TLS が正しく設定されたことを確認します）。

追加情報

「関連項目」（P.24-7）を参照してください。

参考情報

関連項目

- 「認証、整合性、および許可の概要」（P.1-17）
- 「暗号化の概要」（P.1-22）
- 「Cisco IOS MGCP ゲートウェイの暗号化の概要」（P.24-1）
- 「H.323 ゲートウェイおよび H.323/H.225/H.245 トランクの暗号化の概要」（P.24-2）
- 「SIP トランクの暗号化の概要」（P.24-3）
- 「ゲートウェイおよびトランクのセキュリティ設定用チェックリスト」（P.24-4）
- 「ネットワーク インフラストラクチャで IPSec を設定する場合の注意事項」（P.24-5）
- 「Cisco Unified Communications Manager とゲートウェイまたはトランクとの間で IPSec を設定する場合の注意事項」（P.24-6）

シスコの関連マニュアル

- 『*Cisco Unified Communications Operating System Administration Guide*』
- 『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』
- 『*Cisco IOS Security Configuration Guide, Release 12.2*』（またはそれ以降）
- 『*Voice and Video Enabled IPSec Virtual Private Networks Solution Reference Network Design Guide*』

CHAPTER 25

SIP トランク セキュリティ プロファイルの設定

この章は、次の内容で構成されています。

SIP トランク セキュリティ プロファイルの概要

Cisco Unified Communications Manager の管理では、SIP トランクに対するセキュリティ関連の設定がグループ化され、1 つのセキュリティ 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ます。セキュリティ関連の設定には、デバイス セキュリティ モード、ダイジェスト認証、着信転送タイプや発信転送タイプの設定などがあります。[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ことで、構成済みの設定を SIP トランクに適用します。

Cisco Unified Communications Manager をインストールすると、自動登録用の事前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、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ていない場合は、非セキュア プロファイルを選択します。

SIP トランクがサポートするセキュリティ機能だけが、セキュリティ プロファイル設定ウィンドウに表示されます。

SIP トランク セキュリティ プロファイルの設定のヒント

Cisco Unified Communications Manager の管理で SIP トランク セキュリティ プロファイルを設定する場合は、次の点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 プロファイルを適用します。
- 現在デバイスに割り当てられているセキュリティ プロファイルを削除することはできません。
- 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、再構成した設定が、そのプロファイルを割り当てられているすべての SIP トランクに適用されます。
- デバイスに割り当てられているセキュリティ ファイルの名前を変更できます。古いプロファイル名および設定を割り当てられている SIP トランクは、新しいプロファイル名および設定を受け入れます。
- Cisco Unified Communications Manager 5.0 以降へのアップグレード前にデバイス セキュリティ モードを設定した場合は、Cisco Unified Communications Manager が SIP トランクの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。

SIP トランク セキュリティ プロファイルの検索

SIP トランク セキュリティ プロファイルを検索するには、次の手順を実行します。

手順

ステップ 1　[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)] の順に選択します。

検索と一覧表示ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

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

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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

（注）　検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3　[検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　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）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

追加情報

「関連項目」（P.25-11）を参照してください。

SIP トランク セキュリティ プロファイルの設定

SIP トランク セキュリティ プロファイルを追加、更新、またはコピーするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[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)] の順に選択します。

ステップ 2　次の作業のいずれかを実行します。

- 新しいプロファイルを追加するには、検索ウィンドウで [新規追加 (Add New)] をクリックします（プロファイルを表示してから、[新規追加 (Add New)] 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、各フィールドのデフォルト設定が示されます。
- 既存のセキュリティ プロファイルをコピーするには、「SIP トランク セキュリティ プロファイルの検索」（P.25-2）の説明に従って適切なプロファイルを見つけ、[コピー (Copy)] 列内にあるそのレコード用の [コピー (Copy)] アイコンをクリックします（プロファイルを表示してから、[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、設定内容が示されます。
- 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」（P.25-2）の説明に従い、適切なセキュリティ プロファイルを見つけて表示します。設定ウィンドウが表示され、現在の設定が示されます。

ステップ 3　表 25-1 の説明に従って、適切な設定を入力します。

ステップ 4　[保存 (Save)] をクリックします。

次の作業

セキュリティ プロファイルを作成した後、「SIP トランク セキュリティ プロファイルの適用」（P.25-8）の説明に従い、トランクに適用します。

SIP トランクにダイジェスト認証を設定した場合は、トランクの [SIP レルムの設定 (SIP Realm Configuration)] ウィンドウと、SIP トランクを介して接続されるアプリケーションの [アプリケーションユーザの設定 (Application User Configuration)] ウィンドウで、ダイジェスト信用証明書を設定する必要があります（まだ設定していない場合）。

SIP トランクを介して接続されるアプリケーションのアプリケーションレベル許可を有効にした場合は、[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウで、そのアプリケーションに許可される方式を設定する必要があります（まだ設定していない場合）。

追加情報

「関連項目」（P.25-11）を参照してください。

SIP トランク セキュリティ プロファイルの設定内容

表 25-1 で、SIP トランク セキュリティ プロファイルの設定内容について説明します。

- 設定のヒントについては、「SIP トランク セキュリティ プロファイルの設定のヒント」（P.25-2）を参照してください。
- 関連する情報および手順については、「関連項目」（P.25-11）を参照してください。

表 25-1　SIP トランク セキュリティ プロファイルの設定内容

設定	説明
[名前(Name)]	セキュリティ プロファイルの名前を入力します。新しいプロファイルを保存すると、[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(SIP Trunk Security Profile)] ドロップダウン リスト ボックスに名前が表示されます。
[説明(Description)]	セキュリティ プロファイルの説明を入力します。説明には、任意の言語で最大 50 文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。
[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を適用しません。TCP または UDP 接続で Cisco Unified Communications Manager が利用できます。 • [認証のみ(Authenticated)]：Cisco 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 接続を開始します。 • [暗号化(Encrypted)]：Cisco Unified Communications Manager はトランクの整合性、認証、および暗号化を提供します。シグナリング用に、AES128/SHA を使用する TLS 接続を開始します。
[着信転送タイプ(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)] である場合、[TCP+UDP] が転送タイプとなります。 [デバイスセキュリティモード(Device Security Mode)] が [認証のみ(Authenticated)] または [暗号化(Encrypted)] である場合、[TLS] が転送タイプとなります。 **（注）** Transport Layer Security（TLS）プロトコルによって、Cisco Unified Communications Manager とトランクとの間の接続が保護されます。

表 25-1　SIP トランク セキュリティ プロファイルの設定内容（続き）

設定	説明
[発信転送タイプ(Outgoing Transport Type)]	ドロップダウン リスト ボックスから、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)] である場合、[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 [認証のみ(Authenticated)] または [暗号化(Encrypted)] である場合、[TLS] が転送タイプとなります。 **（注）** TLS は、SIP トランクのシグナリング整合性、デバイス認証、およびシグナリング暗号化を実現します。 **ヒント** TCP 接続の再利用をサポートしていない Cisco Unified Communications Manager システムと IOS ゲートウェイの間で SIP トランクを接続する場合は、発信転送タイプとして UDP を使用する必要があります。詳細については、『*Cisco Unified Communications Manager システム ガイド*』の「セッション開始プロトコル（SIP）の概要」を参照してください。
[ダイジェスト認証を有効化(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、Cisco Unified Communications Manager は、トランクからのすべての SIP 要求でチャレンジを行います。 ダイジェスト認証は、デバイス認証、整合性、および信頼性を提供しません。これらの機能を使用するには、セキュリティ モード [認証のみ(Authenticated)] または [暗号化(Encrypted)] を選択します。 ダイジェスト認証の詳細については、「ダイジェスト認証」（P.1-19）および「SIP トランクのダイジェスト認証の設定」（P.26-1）を参照してください。 **ヒント** TCP 転送または UDP 転送を使用しているトランク上の 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)]	ナンス値が有効な時間を秒単位で入力します。デフォルト値は 600（10 分）です。この時間が経過すると、Cisco 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ランダム値で、ダイジェスト認証パスワードの MD5 ハッシュの計算に使用されます。

表 25-1　SIP トランク セキュリティ プロファイルの設定内容（続き）

設定	説明
[X.509 の件名 (X.509 Subject Name)]	このフィールドは、[着信転送タイプ (Incoming Transport Type)] および [発信転送タイプ (Outgoing Transport Type)] に TLS を設定した場合に適用されます。 デバイス認証のために、SIP トランク デバイスの X.509 証明書の件名を入力します。Cisco Unified Communications Manager クラスタがある場合、または TLS ピアに対して SRV ルックアップを使用する場合、単一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。その結果、トランクに複数の X.509 の件名が設定されます。複数の X.509 の件名がある場合は、スペース、カンマ、セミコロン、コロンのいずれか 1 つを使用して、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** 件名は、送信元接続の TLS 証明書に対応します。件名が、件名とポートで一意であることを確認してください。同じ件名と着信ポートの組み合わせを、異なる SIP トランクに割り当てることはできません。 例 : ポート 5061 の SIP TLS trunk1 の [X.509 の件名 (X.509 Subject Name)] は、my_cm1, my_cm2 です。ポート 5071 の SIP TLS trunk1 の [X.509 の件名 (X.509 Subject Name)] は、my_cm2, my_cm3 です。この場合、ポート 5061 の SIP TLS trunk3 の [X.509 の件名 (X.509 Subject Name)] は my_ccm4 にできますが、my_cm1 にはできません。
[着信ポート (Incoming Port)]	着信ポートを選択します。1024 ～ 65535 の一意のポート番号を入力します。着信 TCP および UDP の SIP メッセージのデフォルト ポート値は、5060 です。着信 TLS メッセージの保護されたデフォルト SIP ポートは、5061 です。入力した値は、このプロファイルを使用するすべての SIP トランクに適用されます。 **ヒント** TLS を使用するすべての SIP トランクが、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 トランクが、同じ着信ポートを共有できます。同じポートで、TLS の SIP 転送トランクと、TLS 以外の SIP 転送トランク タイプを混合することはできません。 **ヒント** 通常のトラフィック時に SIP トランク UDP ポート上で単一の IP アドレスからの着信パケット レートが、設定済みの SIP Trunk UDP Port Throttle Threshold を超える場合は、そのしきい値を再設定してください。SIP トランクと SIP ステーションが同じ着信 UDP ポートを共有している場合、2 つのサービス パラメータ値の大きいほうの値に基づいて Cisco Unified Communications Manager はパケットのスロットリングを行います。このパラメータに対する変更を有効にするには、Cisco CallManager サービスを再起動する必要があります。

表 25-1　SIP トランク セキュリティ プロファイルの設定内容（続き）

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許可は、SIP トランクを介して接続されるアプリケーションに適用されます。 このチェックボックスをオンにする場合は、[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、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。Cisco 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は、まずトランクレベルの許可が発生してから、アプリケーション レベルの許可が発生します。つまり、Cisco 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 ユーザに許可されている方式よりも先に、（このセキュリティ プロファイルで）トランクに許可されている方式を確認します。 **ヒント** アプリケーションの ID を信頼しない場合、またはアプリケーションが特定のトランクで信頼されていない場合は、アプリケーションレベルの許可の使用を検討してください。アプリケーション要求は、予期しないトランクから着信することがあります。 トランクのダイジェスト認証設定の詳細については、「SIP トランクのダイジェスト認証の設定」（P.26-1）を参照してください。許可の詳細については、「許可」（P.1-21）および 「相互作用」（P.1-7）を参照してください。[アプリケーションユーザの設定(Application User Configuration)] ウィンドウでアプリケーション レベルの許可を設定する方法の詳細については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照してください。
[プレゼンスの SUBSCRIBE の許可(Accept Presence Subscription)]	Cisco 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、この機能について許可す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許可が有効で、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)] チェックボックスがオンで、トランクのチェックボックスがオフの場合、トランクに接続されている 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。

表 25-1　SIP トランク セキュリティ プロファイルの設定内容（続き）

設定	説明
[Out-of-Dialog REFER の許可(Accept Out-of-Dialog REFER)]	Cisco 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、この方式について許可す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)]	Cisco Unified Communications Manager が SIP トランク経由で着信する非インバイトの Unsolicited NOTIFY メッセージ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、この方式について許可す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。
[Replaces ヘッダーの許可(Accept Replaces Header)]	Cisco 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、この方式について許可するアプリケーション ユーザの [REPLACE ヘッダの許可(Accept Replaces Header)] チェックボックスをオンにします。
[送信セキュリティステータス(Transmit Security Status)]	Cisco 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、このチェックボックスはオフになっています。

SIP トランク セキュリティ プロファイルの適用

[トランクの設定(Trunk Configuration)] ウィンドウで、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。デバイスにセキュリティ プロファイルを適用するには、次の手順を実行します。

手順

ステップ 1　『*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。

ステップ 2　[トランクの設定(Trunk Configuration)] ウィンドウが表示されたら、[SIP トランクセキュリティプロファイル(SIP Trunk Security Profile)] 設定を見つけます。

ステップ 3　セキュリティ プロファイルのドロップダウン リスト ボックスから、デバイスに適用するセキュリティ プロファイルを選択します。

ステップ 4　[保存(Save)] をクリックします。

ステップ 5　[設定の適用(Apply Config)] をクリックして、トランクをリセットします。

次の作業

SIP トランクにダイジェスト認証を有効にするプロファイルを適用した場合は、トランクの [SIP レルムの設定(SIP Realm Configuration)] ウィンドウでダイジェスト信用証明書を設定する必要があります。「SIP レルムの設定」（P.26-4）を参照してください。

アプリケーションレベルの許可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の設定(Application User Configuration)] ウィンドウで、ダイジェスト信用証明書と可能な許可方式を設定する必要があります（まだ設定していない場合）。

追加情報

「関連項目」（P.25-11）を参照してください。

SIP トランク セキュリティ プロファイルと影響を受ける SIP トランクの同期

SIP トランクを設定変更が行われた SIP トランク セキュリティ プロファイルと同期させるには、次の手順を実行します。この手順では、できる限り簡潔な方法で主な設定内容を適用します（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を実行する必要がない場合があります）。

手順

ステップ 1　[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)] の順に選択します。

[SIP トランクセキュリティプロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles)] ウィンドウが表示されます。

ステップ 2　使用する検索条件を選択します。

ステップ 3　[検索(Find)] をクリックします。

ウィンドウに検索条件と一致する SIP トランク セキュリティ プロファイルのリストが表示されます。

ステップ 4　該当する SIP トランクと同期させる SIP トランク セキュリティ プロファイルをクリックします。[SIP トランクセキュリティプロファイルの設定(SIP Trunk Security Profile Configuration)] ウィンドウが表示されます。

ステップ 5　設定の変更を行います。

ステップ 6　[保存(Save)] をクリックします。

ステップ 7　[設定の適用(Apply Config)] をクリックします。

[設定情報の適用 (Apply Configuration Information)] ダイアログボックスが表示されます。

ステップ 8　[OK] をクリックします。

追加情報

「関連項目」（P.25-11）を参照してください。

SIP トランク セキュリティ プロファイルの削除

ここでは、Cisco 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

Cisco Unified Communications Manager の管理でセキュリティ 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。該当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 トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] ウィンドウの [関連リンク (Related Links)] ドロップダウン リスト ボックスから [依存関係レコード (Dependency Records)] を選択して、[移動 (Go)] をクリックします。

システムで依存関係レコード機能が有効になっていない場合は、レコードの [依存関係レコード要約 (Dependency Records Summary)] ウィンドウに、依存関係レコードを有効にすると実行できるアクションを示すメッセージが表示されます。また、依存関係レコード機能を使用すると、CPU 使用率が高くなるという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 ガイド*』を参照してください。

手順

ステップ 1　「SIP トランク セキュリティ プロファイルの検索」（P.25-2）の手順に従って、セキュリティ プロファイルを検索します。

ステップ 2　次のいずれかを実行します。

- 複数のセキュリティ プロファイルを削除するには、検索と一覧表示ウィンドウで、次のいずれかを実行します。
  - 削除するセキュリティ プロファイルの横に表示されているチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックします。
  - この選択に対するすべての設定可能なレコードを削除するには、[すべてを選択 (Select All)] をクリックしてから [選択項目の削除 (Delete Selected)] をクリックします。
- 単一のセキュリティ プロファイルを削除するには、検索と一覧ウィンドウで、次のいずれかを実行します。
  - 削除するセキュリティ プロファイルの横に表示されているチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックします。
  - セキュリティ プロファイルの [名前 (Name)] リンクをクリックします。指定したセキュリティ プロファイルの設定ウィンドウが表示されたら、[削除 (Delete)] をクリックします。

ステップ 3　削除操作の確認を要求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、[キャンセル (Cancel)] をクリックして削除操作を取り消します。

追加情報

「関連項目」（P.25-11）を参照してください。

参考情報

関連項目

- 「SIP トランク セキュリティ プロファイルの概要」（P.25-1）
- 「SIP トランク セキュリティ プロファイルの設定のヒント」（P.25-2）
- 「SIP トランク セキュリティ プロファイルの検索」（P.25-2）
- 「SIP トランク セキュリティ プロファイルの設定」（P.25-3）
- 「SIP トランク セキュリティ プロファイルの設定内容」（P.25-4）
- 「SIP トランク セキュリティ プロファイルの適用」（P.25-8）
- 「SIP トランク セキュリティ プロファイルと影響を受ける SIP トランクの同期」（P.25-9）
- 「SIP トランク セキュリティ プロファイルの削除」（P.25-10）
- 「許可」（P.1-21）
- 「相互作用」（P.1-7）
- 「ダイジェスト認証」（P.1-19）

シスコの関連マニュアル

『*Cisco Unified Communications Manager アドミニストレーション ガイド*』

『*Cisco Unified Communications Manager システム ガイド*』

CHAPTER 26

SIP トランクのダイジェスト認証の設定

SIP トランクにダイジェスト認証を設定すると、Cisco Unified Communications Manager は、SIP トランクで SIP 要求を受信したときに、SIP ユーザ エージェントの ID でチャレンジを行うことができます。Cisco Unified Communications Manager がトランクへ SIP 要求を送信した場合は、SIP ユーザ エージェントが Cisco Unified Communications Manager の ID でチャレンジを行うことができます。SIP トランクでのダイジェスト認証の動作の詳細については、「ダイジェスト認証」（P.1-19）を参照してください。

この章は、次の内容で構成されています。

SIP トランクのダイジェスト認証の設定用チェックリスト

SIP トランクにダイジェスト認証を設定する作業を表 26-1 で説明します。

表 26-1　SIP トランクのセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	SIP トランクのセキュリティ プロファイルを設定します。[ダイジェスト認証を有効化(Enable Digest Authentication)] チェックボックスがオンになっていることを確認します。	• 「SIP トランク セキュリティ プロファイルの設定」（P.25-3） • 「ダイジェスト認証」（P.1-19）
ステップ 2	SIP トランク セキュリティ プロファイルをトランクに適用します。	「SIP トランク セキュリティ プロファイルの適用」（P.25-8）

表 26-1　SIP トランクのセキュリティ設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 3	Cluster ID エンタープライズ パラメータを設定します（設定していない場合）。 このパラメータにより、Cisco Unified Communications Manager は、SIP トランクで SIP 要求を送信する SIP ユーザ エージェントの ID でチャレンジを行えるようになります。	「ダイジェスト認証のエンタープライズ パラメータの設定」（P.26-2）
ステップ 4	Cisco Unified Communications Manager は、SIP トランクで SIP 要求を送信する SIP ユーザ エージェントの ID でチャレンジを行い、[アプリケーションユーザの設定 (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信用証明書を設定します。	• 「[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウでのダイジェスト信用証明書の設定」（P.26-2） • 「アプリケーション ユーザのダイジェスト信用証明書の設定内容」（P.26-3）
ステップ 5	Cisco Unified Communications Manager がトランク ピアからのチャレンジに応答した場合は、SIP レルムを設定します。	• 「ダイジェスト認証」（P.1-19） • 「SIP レルムの設定」（P.26-4） • 「SIP レルムの設定内容」（P.26-5）

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

Cluster ID エンタープライズ パラメータをダイジェスト認証用に設定するには、Cisco Unified Communications Manager の管理ページで、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。Cluster ID パラメータを見つけ、パラメータのヘルプの説明に従って値を更新します。このパラメータにより、Cisco Unified Communications Manager は、SIP トランクで SIP 要求を送信する SIP ユーザ エージェントの ID でチャレンジを行えるようになります。

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設定 (Enterprise Parameters Configuration)] ウィンドウに表示されている疑問符をクリックするか、パラメータのリンクをクリックします。

[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウでのダイジェスト信用証明書の設定

Cisco Unified Communications Manager が SIP ユーザ エージェントの ID でチャレンジを行う場合は、Cisco Unified Communications Manager の管理の [アプリケーションユーザの設定 (Application User Configuration)] ウィンドウで、アプリケーション ユーザのダイジェスト信用証明書を設定する必要があります。Cisco Unified Communications Manager は、これらの信用証明書を使用して、SIP トランクで要求を送信する SIP ユーザ エージェントの ID を確認します。

アプリケーション ユーザのダイジェスト信用証明書を設定するには、次の手順を実行します。

手順

ステップ 1　『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の説明に従って、アプリケーション ユーザを検索します。

ステップ 2　アプリケーション ユーザのリンクをクリックします。

ステップ 3　目的の [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れたら、表 26-3 の説明に従って、適切な文字列を入力します。

ステップ 4　[保存 (Save)] をクリックします。

追加情報

「関連項目」（P.26-6）を参照してください。

アプリケーション ユーザのダイジェスト信用証明書の設定内容

表 26-3 では、Cisco Unified Communications Manager の管理の [アプリケーションユーザの設定 (Application User Configuration)] ウィンドウに表示されるダイジェスト信用証明書の設定について説明します。関連する情報および手順については、「関連項目」（P.26-6）を参照してください。

表 26-2　ダイジェスト認証クレデンシャル

設定	説明
[ダイジェスト信用証明書 (Digest Credentials)]	英数字文字列を入力します。
[ダイジェスト信用証明書の確認 (Confirm Digest Credentials)]	ダイジェスト信用証明書を正しく入力したことを確認するために、このフィールドにクレデンシャルを入力します。

SIP レルムの検索

SIP レルムを検索するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[ユーザ管理 (User Management)] > [SIP レルム (SIP Realm)] の順に選択します。

検索と一覧表示ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

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

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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

（注）　検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3　[検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　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）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

次の作業

Cluster ID エンタープライズ パラメータをまだ設定していない場合は、「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」（P.26-2）の説明に従って設定します。

追加情報

「関連項目」（P.26-6）を参照してください。

SIP レルムの設定

Cisco Unified Communications Manager が 1 つまたは複数のトランク ピアからのチャレンジに応答する場合は、Cisco Unified Communications Manager でチャレンジを実行できる SIP トランク ユーザ エージェントの SIP レルムを設定する必要があります。

SIP レルムを追加または更新するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[ユーザ管理 (User Management)] > [SIP レルム (SIP Realm)] の順に選択します。

ステップ 2　次のいずれかを実行します。

- 新しい SIP レルムを追加するには、検索ウィンドウで [新規追加 (Add New)] をクリックします (SIP レルムを表示してから、[新規追加 (Add New)] 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、各フィールドのデフォルト設定が示されます。

- 既存のレコードをコピーするには、「SIP レルムの検索」（P.26-3）の説明に従って適切なレコードを見つけ、[コピー (Copy)] 列内にあるそのレコード用の [コピー (Copy)] アイコンをクリックします（SIP レルムを表示してから、[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、設定内容が示されます。
- 既存のレコードを更新するには、「SIP レルムの検索」（P.26-3）の説明に従い、適切な SIP レルムを見つけて表示します。設定ウィンドウが表示され、現在の設定が示されます。

ステップ 3　表 26-3 の説明に従って、適切な設定を入力します。

ステップ 4　[保存 (Save)] をクリックします。

ステップ 5　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。

次の作業

ダイジェスト認証を成功させるために、Cisco Unified Communications Manager で設定した内容と SIP ユーザ エージェントで設定した内容が同じであることを確認します。

追加情報

「関連項目」（P.26-6）を参照してください。

SIP レルムの設定内容

Cisco Unified Communications Manager がトランク ピアによるチャレンジを受ける場合は、SIP レルムがトランク側のクレデンシャルを提供します。

表 26-3 で、SIP レルムの設定内容を説明します。関連する情報および手順については、「関連項目」（P.26-6）を参照してください。

表 26-3　SIP レルム セキュリティ プロファイル

設定	説明
[レルム (Realm)]	SIP トランクに接続されるレルムのドメイン名を入力します（SIPProxy1_xyz.com など）。英数字、ピリオド、ダッシュ、アンダースコア、スペースを使用できます。
[ユーザ (User)]	このレルム内の SIP ユーザ エージェントのユーザ名を入力します。たとえば、Cisco 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、この Cisco Unified Communications Manager でチャレンジを実行します。
[ダイジェスト信用証明書 (Digest Credentials)]	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 Cisco Unified Communications Manager が使用するパスワードを入力します。
[ダイジェスト信用証明書の確認 (Confirm Digest Credentials)]	確認のためパスワードを再入力します。

SIP レルムの削除

ここでは、Cisco Unified Communications Manager データベースから SIP レルムを削除する方法について説明します。

手順

ステップ 1　「SIP レルムの検索」（P.26-3）の手順に従って、SIP レルムを検索します。

ステップ 2　次のいずれかを実行します。

- 複数の SIP レルムを削除するには、検索と一覧表示ウィンドウで、次のいずれかを実行します。
  - 削除するレルムの横に表示されているチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックします。
  - この選択に対するすべての設定可能なレコードを削除するには、[すべてを選択 (Select All)] をクリックしてから [選択項目の削除 (Delete Selected)] をクリックします。
- 単一の SIP レルムを削除するには、検索と一覧表示ウィンドウで、次のいずれかを実行します。
  - 削除するレルムの横に表示されているチェックボックスをオンにして、[選択項目の削除 (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。指定した [SIP レルムの設定 (SIP Realm Configuration)] 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。

ステップ 3　削除操作の確認を要求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、[キャンセル (Cancel)] をクリックして削除操作を取り消します。

追加情報

「関連項目」（P.26-6）を参照してください。

参考情報

関連項目

- 「ダイジェスト認証」（P.1-19）
- 「SIP トランクのダイジェスト認証の設定用チェックリスト」（P.26-1）
- 「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」（P.26-2）
- 「[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウでのダイジェスト信用証明書の設定」（P.26-2）
- 「アプリケーション ユーザのダイジェスト信用証明書の設定内容」（P.26-3）
- 「SIP レルムの検索」（P.26-3）
- 「SIP レルムの設定」（P.26-4）
- 「SIP レルムの設定内容」（P.26-5）
- 「SIP レルムの削除」（P.26-6）

CHAPTER 27

Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの設定

この章は、次の内容で構成されています。

Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの概要

Cisco Unified Communications Manager の管理では、セキュリティ関連の設定がグループ化され、1 つのセキュリティ 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、および X.509 の件名などがあります。Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルを Cisco Unified Communications Manager の管理で設定すると、その Cisco Unified Communications Manager の設定済みの Mobile Communicator クライアントすべてに、このプロファイルが自動的に適用されます。

Cisco Unified Mobility Advantage サーバがサポートするセキュリティ機能だけが、セキュリティ プロファイル設定ウィンドウに表示されます。

（注） Cisco Unified Mobility Advantage サーバは Cisco Unified Communications Manager の管理で設定することができません。Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルのセットアップについては、Cisco Unified Mobility Advantage のマニュアルを参照してください。Cisco Unified Communications Manager で設定する Cisco Unified Mobility Advantage セキュリティ プロファイルは、Cisco Unified Mobility Advantage サーバ上のセキュリティ プロファイルと一致させる必要があります。Cisco Unity Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定については、『*Cisco Unified Communications Manager セキュリティ ガイド*』を参照してください。

Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの検索

Cisco Unified Mobility Advantage 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

ステップ 1　Cisco Unified Communications Manager の管理ページで、[システム(System)] > [セキュリティプロファイル(Security Profile)] > [CUMA サーバセキュリティプロファイル(CUMA Server Security Profile)] の順に選択します。

[CUMA サーバセキュリティプロファイルの検索と一覧表示 (Find and List CUMA Server Security Profiles)] ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

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

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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

（注）　検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア(Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3　[検索(Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数(Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　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）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

追加情報

「関連項目」（P.27-6）を参照してください。

Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの設定

セキュリティ プロファイルを追加、更新、またはコピーするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [セキュリティプロファイル (Security Profile)] > [CUMA サーバセキュリティプロファイル (CUMA Server Security Profile)] の順に選択します。

ステップ 2　次のいずれかを実行します。

- 新しいプロファイルを追加するには、検索ウィンドウの [新規追加 (Add New)] をクリックし、ステップ 3 に進みます。
- 既存のセキュリティ プロファイルをコピーするには、「Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの検索」（P.27-2）の説明に従い、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 [コピー (Copy)] ボタンをクリックし、ステップ 3 に進みます。
- 既存のプロファイルを更新するには、「Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの検索」（P.27-2）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、ステップ 3 に進みます。

[新規追加 (Add New)] をクリックすると、各フィールドのデフォルト設定を示し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、設定をコピーした設定ウィンドウが表示されます。

ステップ 3　表 27-1 の説明に従って、適切な設定を入力します。

ステップ 4　[保存 (Save)] をクリックします。

追加情報

「関連項目」（P.27-6）を参照してください。

Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの設定内容

表 27-1 で、Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの設定について説明します。

- 設定のヒントについては、「Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの検索」（P.27-2）を参照してください。
- 関連する情報および手順については、「関連項目」（P.27-6）を参照してください。

表 27-1　Cisco Unified Mobility Advantage サーバのセキュリティ プロファイル

設定	説明
[名前 (Name)]	セキュリティ プロファイルの名前を入力します。 **ヒント** セキュリティ プロファイル名にデバイス モデルを含めると、プロファイルを検索または更新する場合に適切なプロファイルを検出するのに役立ちます。
[説明 (Description)]	セキュリティ プロファイルの説明を入力します。説明には、任意の言語で最大 50 文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。
[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、次のオプションのいずれかを選択します。 • [非セキュア (Non Secure)] : Cisco Unified Mobility Advantage サーバにイメージ認証以外のセキュリティ機能はありません。TCP 接続で Cisco Unified Communications Manager が利用できます。 • [認証のみ (Authenticated)] : Cisco Unified Communications Manager は Cisco Unified Mobility Advantage サーバの整合性と認証を提供します。シグナリング用に、NULL/SHA を使用する TLS 接続を開始します。 • [暗号化 (Encrypted)] : Cisco Unified Communications Manager は Cisco Unified Mobility Advantage サーバの整合性、認証、および暗号化を提供します。シグナリング用に AES128/SHA を使用する TLS 接続を開始し、すべてのモバイル コールのメディアを SRTP で搬送します。
[転送タイプ (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)] である場合は、ドロップダウン リスト ボックスから次のオプションを選択します。 • [TCP] : パケットを送信された順に受信するには、Transmission Control Protocol を選択します。このプロトコルは、パケットがドロップされないことを保証しますが、セキュリティは提供しません。 [デバイスセキュリティモード (Device Security Mode)] が [認証のみ (Authenticated)] または [暗号化 (Encrypted)] である場合、TLS が転送タイプとなります。TLS は、シグナリング整合性、デバイス認証、およびシグナリング暗号化（暗号化モードのみ）を提供します。
[X.509 の件名 (X.509 Subject Name)]	([デバイスセキュリティモード (Device Security Mode)] の設定値が [認証のみ (Authenticated)] または [暗号化 (Encrypted)] である場合に必要）このフィールドは、転送タイプとして TLS を設定した場合に適用されます。 X.509 は、国際電気通信連合電気通信標準化部門による、暗号法の公開鍵インフラストラクチャ規格です。件名は、送信元接続の TLS 証明書に対応します。 複数の X.509 の件名がある場合は、スペース、カンマ、セミコロン、またはコロンのいずれか 1 つを使用して、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。

Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの適用

[デバイスセキュリティプロファイル(Device Security Profile)] フィールドは、Mobile Communicator クライアントのデバイス設定ウィンドウには存在しません。つまり、Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルをクライアントに手動で適用する必要はありません。

Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルを Cisco Unified Communications Manager の管理で設定すると、その Cisco Unified Communications Manager の設定済みの Mobile Communicator クライアントすべてに、このプロファイルが自動的に適用されます。

追加情報

「関連項目」（P.27-6）を参照してください。

Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの削除

ここでは、Cisco Unified Communications Manager データベースから Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルを削除する方法について説明します。

手順

ステップ 1　「Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの検索」（P.27-2）の手順に従って、セキュリティ プロファイルを検索します。

ステップ 2　セキュリティ プロファイルを削除するには、次の手順を実行します。

- 検索と一覧表示ウィンドウで、適切なセキュリティ プロファイルの横に表示されているチェックボックスをオンにして、[選択項目の削除(Delete Selected)] をクリックします。

ステップ 3　削除操作の確認を要求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、[キャンセル(Cancel)] をクリックして削除操作を取り消します。

追加情報

「関連項目」（P.27-6）を参照してください。

参考情報

関連項目

- 「Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの概要」（P.27-1）
- 「Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの検索」（P.27-2）
- 「Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの検索」（P.27-2）
- 「Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの設定」（P.27-3）
- 「Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの設定内容」（P.27-3）
- 「Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの適用」（P.27-5）
- 「Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルの削除」（P.27-5）

INDEX

C

E

H

I

J

M

N

S

T

あ

い

か

き

こ

し

せ

た

て

と

に

ふ

ほ

め

ろ

わ