はじめに

目的

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

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

- FIPS（連邦情報処理標準）140-2 モードの設定。

対象読者

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

マニュアルの構成

次の表に、このマニュアルの主なセクションを示します。

表 *1*：マニュアルの概要

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

章	説明
電話セキュリティ プロファイルの設定	[Cisco Unified Communications Manager Administration] でセキュリティ プロファイルを設定して電話に適用する方法を説明します。
セキュア通知トーンおよび非セキュア通知トーンの設定	セキュア通知トーンを再生するよう電話を設定する方法を説明します。
アナログエンドポイントに対する暗号化の設定	アナログ エンドポイントへのセキュアな SCCP 接続を設定する方法を説明します。
Certificate Authority Proxy Function	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での、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、トラブルシューティングの方法を説明します。
暗号化された電話設定ファイルの設定	[Cisco Unified Communications Manager Administration] で暗号化された電話設定ファイルを設定する方法を説明します。
SIP 電話のダイジェスト認証の設定	[Cisco Unified Communications Manager Administration] で SIP を実行している電話にダイジェスト認証を設定する方法を説明します。
電話のセキュリティ強化	[Cisco Unified Communications Manager Administration] を使用して電話のセキュリティを厳格化する方法を説明します。
セキュアな会議リソースの設定	セキュアな会議にメディア暗号化を設定する方法を説明します。
ボイス メッセージング ポートのセキュリティ設定	[Cisco Unified Communications Manager Administration] でボイス メール ポートのセキュリティを設定する方法を説明します。
セキュアなコールのモニタリングおよび録音のセットアップ	セキュア コールのモニタリングと録音を設定する方法を説明します。
Cisco IP Phone の仮想プライベート ネットワーク	
CTI、JTAPI、および TAPI のセキュリティ	

章	説明
CTI、JTAPI、および TAPI の認証および暗号化の設定	[Cisco Unified Communications Manager Administration] でアプリケーションユーザ CAPF プロファイルとエンドユーザ CAPF プロファイルを設定する方法を説明します。
SRST 参照、ゲートウェイ、トランク、および Cisco Unified Mobility Advantage サーバのセキュリティ	
セキュアな Survivable Remote Site Telephony（SRST）リファレンス	[Cisco Unified Communications Manager Administration] でセキュリティのため SRST 参照を設定する方法を説明します。
ゲートウェイおよびトランクの暗号化の設定	Cisco Unified Communications Manager がセキュアなゲートウェイやトランクと通信する方法について説明します。IPSec に関する推奨事項と考慮事項について説明します。
SIP トランク セキュリティ プロファイルの設定	[Cisco Unified Communications Manager Administration] で SIP トランク セキュリティ プロファイルを設定し、適用する方法を説明します。
SIP トランクのダイジェスト認証の設定	[Cisco Unified Communications Manager Administration] で SIP トランクにダイジェスト認証を設定する方法を説明します。
Cisco Unified Mobility Advantage サーバのセキュリティ プロファイルの設定	[Cisco Unified Communications Manager Administration] で Cisco Unified Mobility Advantage サーバ セキュリティ プロファイルを設定する方法を説明します。
FIPS 140-2 モードの設定	[Cisco Unified Communications Manager Administration] で FIPS（連邦情報処理標準）140-2 モードを設定する方法を説明します。

関連資料

各章には章トピックの関連資料の一覧が含まれています。

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

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

- 『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』
- 『*Cisco Unified Communications Manager Integration Guide for Cisco Unity*』
- 『*Cisco Unified Communications Manager Integration Guide for Cisco Unity Connection*』
- SRST 対応ゲートウェイに対応した Cisco Unified Survivable Remote Site Telephony（SRST）管理マニュアル
- ご使用の電話モデルに対応したファームウェア 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」の意味です。

注意は、次のように表しています。

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

マニュアルの入手、サポート、およびセキュリティガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、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も示されています。 http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

シスコ製品のセキュリティ

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化

技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および現地国の法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意したものと見なされます。米国および現地の法律を順守できない場合は、本製品を至急送り返してください。

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