はじめに

目的

Cisco Unified Communications Manager セキュリティガイドは、システム管理者と電話管理者が次のタスクを実行するのに役立つものです。

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

対象読者

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

組織

次の表に、このマニュアルの主なセクションを示します。

表 *1:* マニュアルの概要

章	説明
セキュリティの基礎	
セキュリティの概要	セキュリティ用語、システム要件、連携動作と制限事項、インストール要件、および設定チェックリストの概要を示します。では、さまざまなタイプの認証と暗号化について説明します。
Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS）	HTTPS の概要を示し、信頼できるフォルダにサーバ認証証明書をインストールする方法について説明します。
デフォルトのセキュリティ設定	には、Cisco Unified IP 電話の自動セキュリティ機能を提供するデフォルトのセキュリティ機能に関する情報が記載されています。
Cisco CTL クライアントの設定	CiscoCTL クライアントをインストールして設定することによって認証を設定する方法について説明します。
TLS セットアップ	
証明書	
証明書概要	
電話とボイスメール ポートのセキュリティ	
電話機のセキュリティ	Unified Communications Manager と電話でどのようにセキュリティが使用されるかを説明します。電話のセキュリティ設定のために実行するタスクの一覧があります。
電話セキュリティ プロファイルの設定	Unified Communications Manager でセキュリティ プロファイルを設定して適用する方法を説明します。

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

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

関連資料

各章には、章のトピックの関連資料のリストが含まれています。

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

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

表記法

（注）は、次のように表しています。

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

ヒントは、次のように表しています。

ヒント 役立つ「ヒント」の意味です。

注意は、次のように表しています。

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

マニュアルの入手、サポート、およびセキュリティガイドライン

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

シスコ製品のセキュリティの概要

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

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