



はじめに

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

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

- [このマニュアルについて \(i ページ\)](#)
- [対象読者 \(iii ページ\)](#)
- [表記法 \(iv ページ\)](#)
- [法令順守 \(iv ページ\)](#)

このマニュアルについて

このセキュリティガイドには、短い説明を含む次の部分が含まれています。

表 1: 部分と説明

パート	説明
CUCM セキュリティの概要	<p>セキュリティの概要に関する次のトピックの情報を提供します。</p> <ul style="list-style-type: none">• システム要件• 一般的なアイコン• ベストプラクティス <p>また、システム内のセキュリティを設定する概要も提供しています。</p>

パート	説明
基本的なシステムセキュリティ	<p>システムで基本的なセキュリティを設定するための次のトピックに関する情報を提供します。</p> <ul style="list-style-type: none">• 証明書• セキュリティモード• 暗号管理• セキュアトーンとアイコン• TFTP 暗号化• 電話機のセキュリティ• トランクとゲートウェイの SIP セキュリティ• TLS セットアップ
ユーザセキュリティ	<p>システムでユーザセキュリティを設定するための次のトピックに関する情報を提供します。</p> <ul style="list-style-type: none">• ID の管理<ul style="list-style-type: none">• ユーザ アクセス制御• クレデンシャル ポリシー• ディレクトリアクセス<ul style="list-style-type: none">• 連絡先検索認証の設定• 連絡先検索用のセキュアなディレクトリ サーバの設定

パート	説明
高度なシステムセキュリティ	<p>システムで高度なセキュリティを設定するための次のトピックに関する情報を提供します。</p> <ul style="list-style-type: none">• FIPS モード• 強化されたセキュリティ モード• コモン クライテリア モード• Cisco V.150 最低要件• ECDSA と RSA• IPsec ポリシー• CTI の認証と暗号化の設定• JTAPI、および TAPI• セキュアなコールのモニタリングおよび録音• VPN クライアント
付録	<p>システムをセキュリティで保護するための次のトピックに関する情報を提供します。</p> <ul style="list-style-type: none">• 追加のセキュリティの設定• 用語および略語• 連携動作と制限事項• Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS)• トラブルシューティング情報• リモートアカウント• ログの詳細• 一般的な脆弱性と PSIRT• OS の強化

対象読者

このガイドの対象読者は次のとおりです。

- システム管理者
- 電話管理者

Unified Communications Manager のコールセキュリティ機能を設定します。

表記法

このセクションでは、ガイドに続くドキュメントの表記方法について説明します。

(注) は、次のように表しています。



(注) 重要または追加情報の注釈です。

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。

強いレベルの注意は、次のように表しています。



注意 読者は注意する必要がありますという意味です。このような状況では、手順を慎重に読んでください。それ以外の場合、機器に損傷を与えたり、データを失ったりする可能性があります。

弱いレベルの注意は、次のように表しています。



注目 読者は注意を払ってくださいという意味です。このような状況では、手順を慎重に読んでください。それ以外の場合、機器に損傷を与えたり、データを失ったりする可能性があります。

警告



警告 読者は指示に従わなければならないという意味です。このような状況では、手順を慎重に読んでください。それ以外の場合、機器に損傷を与えたり、データを失ったりする可能性があります。

法令順守

Unified Communications Manager (セキュリティ) 製品には、暗号化機能とインポート、エクスポート情報が含まれています。情報の転送および使用は、米国および他の国に適用される法律に準拠

しています。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見なされます。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を参照してください。

翻訳について

このドキュメントは、米国シスコ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。